

==Phrack Inc.==

Volume Four, Issue Forty, File 1 of 14

Issue 40 Index

P H R A C K 4 0

August 1, 1992

~ Baby's Got Back! ~

Welcome to the special 40th Anniversary issue of Phrack Magazine! A month later, we are just barely recovering from the fun at the amazingly successful SummerCon '92. It was the largest turnout ever seen at a SummerCon and the full details can be found in a special report by Knight Lightning and myself with help from Holistic Hacker and Dr. Williams.

Brian Oblivion, whose name is regularly seen in the pages of Phrack returns with part two of his file on Cellular Telephony (part one seen in Phrack 38). Also relating to telephones in this issue is "The Fine Art of Telephony" by Crimson Flash. This equally in depth and detailed file focuses of RC/MAC, FACS, and MARCH.

Even though the arrogant bastards at Southwestern Bell and BT Tymnet boast about their great security, it appears that they had almost nothing to do with the tracking down and apprehension of the MOD in New York. As a few of us already know, MOD was brought in by hackers. Gee, imagine that.

I'm not going to play politics and make judgments about this, instead I'll let you read all about it in Phrack World News, Part 2 and then you can draw your own conclusions.

Since we're on the subject of Tymnet, I felt it appropriate <grin> to include 3 articles on the subject by Toucan Jones. A special "kissy, kissy" to Dale Drew (aka The Dictator aka Blind Faith aka Bartman) for his help and assistance in getting us this valuable information. Could a file on TRW be 'round the corner? Hmmmmmm could be. :-)

Starting with this issue, Mind Mage will be assisting with Phrack Loopback as our Technical Advisor. He will handle questions regarding technical problems both for publication or for private response. Feel free to send your questions to phracksub@stormking.com and they will be forwarded and answered.

This issue's Loopback has a very special message from Jester Sluggo as he gives notice of his official retirement from the hacking community. Sluggo remembers the past and give advice about the future; I continue my pursuit on the so-called professionals in the anti-virus community and exposes their real agenda; and, Sarlo takes us on a tour of the 1992 Consumer Electronics Show in Chicago and there is lots more.

The Racketeer (Rack of The Hellfire Club) takes the reigns of the continuing Network Miscellany column and Rambone returns with the latest on what is happening in the underground world of computer software traders in Pirates Cove.

Taran King is back for a special Phrack Pro-Phile with Lex Luthor, the founder of the Legion of Doom and perhaps the most legendary underground hacker ever.

"If it's older than a week, then we won't have it online."

You are invited to check out a great new BBS called Planet 10. If you have half a brain, you might even get access. Planet 10 is run by Control C and features messages and xfers that are timed to expire after 1 week maximum. Give it a call at (313)683-9722.

"Phrack is a bad influence..."

-- TriZap, July 1992 :-)

DISPATER, Phrack Editor

<phracksub@stormking.com> or <phrack@well.sf.ca.us>

Editor-In-Chief : Dispater
Eleet Founders : Taran King and Knight Lightning
Technical Consultant : Mind Mage
Network Miscellany : The Racketeer [HFC]
Pirates Cove : Rambone
News : Datastream Cowboy
Photography : Restricted Data Transmissions
Publicity : AT&T, BellSouth, and the United States Secret Service
Creative Stimulus : Camel Cool, Jolt Cola, and Taco Bell
Shampoo : Mudge
Other Helpers : Apollo, Brian Oblivion, Control C, Dr. Williams,
Dokkalfar, The Gatsby, Gentry, Guido Sanchez, Holistic
Hacker, Jester Sluggo, Legacy Irreverent, Lex Luthor,
Mr. Bigg, Nihil, The Omega, The Pope, The Public,
Sarlo, TriZap, Tuc, Voyager, and White Knight

We're Back and We're Phrack!

"Phrack. If you don't get it, you don't get it."

"Whaddya mean I don't support the system? I go to court when I have to!"

-- Phrack 40 --

Table Of Contents

~~~~~

|                                                     |     |
|-----------------------------------------------------|-----|
| 1. Introduction by Dispater                         | 06K |
| 2. Phrack Loopback by Dispater and Mind Mage        | 50K |
| 3. Phrack Pro-Phile on Lex Luthor by Taran King     | 36K |
| 4. Network Miscellany by The Racketeer [HFC]        | 32K |
| 5. Pirates Cove by Rambone                          | 57K |
| 6. Cellular Telephony, Part II by Brian Oblivion    | 72K |
| 7. The Fine Art of Telephony by Crimson Flash       | 65K |
| 8. BT Tymnet, Part 1 of 3 by Toucan Jones           | 57K |
| 9. BT Tymnet, Part 2 of 3 by Toucan Jones           | 55K |
| 10. BT Tymnet, Part 3 of 3 by Toucan Jones          | 91K |
| 11. SummerCon 1992 by Knight Lightning and Dispater | 35K |
| 12. PWN/Part 1 by Datastream Cowboy                 | 50K |
| 13. PWN/Part 2 by Datastream Cowboy                 | 48K |
| 14. PWN/Part 3 by Datastream Cowboy                 | 48K |

Total: 702K

"Phrack. The magazine the PHONE COMPANY doesn't want you to read!"

==Phrack Inc.==

[-=:< Phrack Loopback >:=-]

By Dispater & Mind Mage

Phrack Loopback is a forum for you, the reader, to ask questions, air problems, and talk about what ever topic you would like to discuss. This is also the place Phrack Staff will make suggestions to you by reviewing various items of note; magazines, software, catalogs, hardware, etc.

In this issue:

|                                    |                                        |
|------------------------------------|----------------------------------------|
| Retirement of a Hacker             | : Jester Sluggo                        |
| Truth Is Out Of Style              | : Dispater                             |
| Tim Foley Virus                    | : Guido Sanchez                        |
| The Hacker Files (from DC Comics)  | : Newsbytes                            |
| Sneakers (from Universal Pictures) | : Press Release                        |
| Pirates v. AT&T: Posters           | : Legacy Irreverent and Captain Picard |
| Telco Trashing Yields Big Rewards  | : Anonymous                            |
| Anonymous Mail On IBM VM Systems?  | : Apollo                               |
| WWIV Link Hack                     | : Mr. Bigg                             |
| The Day Bell System Died           | : Anonymous                            |
| The 1992 Consumer Electronics Show | : Sarlo                                |

---

```
      x  x  x
      |  |  |
    +-----+
    | Retirement |
    |   of a    |
    |   Hacker  |
    +---+-----+---+
    | by Jester Sluggo |
    +---+-----+---+
    | Released: July 9, 1992 |
    +-----+-----+
```

I would like to begin by saying "Hello" to all readers of this file, but unfortunately it will be my last time. I've been a member of the "hacker underground" for over a decade and am one of the few extremely lucky hackers who has successfully hacked a great number of computer systems, phone systems, and other technologies, yet has never been caught. I wish to take this last opportunity to reflect on my experiences, and express many personal views, because although there are feelings of sadness, it is my pleasure to announce my formal retirement from this "underground" community.

My decision to retire has been a carefully planned path which began several years ago. During the early 1980's, the innocence of hacking and exploring computer systems for my quest of knowledge was a great thrill. Every system was like an unexplored door which lead to unlimited opportunities; various computer systems, operating systems, languages, networks, software, and data.

But it was in the later part of the 1980's when I began to realize that I had to focus my interests, knowledge and experience towards a legitimate career. It's nearly impossible to earn a living solely within the resources of the hacker underground, and the idea of abusing technology for monetary gain is against the (unwritten) code of hacker ethics. Also at this time, the innocence of exploring various systems was being replaced by the realities of ruining my entire future at such a young age if I was caught and convicted by the United States' legal system.

The media and law-enforcement agencies have almost always been biased against hackers, and these are two powerful entities that influence society. Hackers

have always been presented in a negative context, whereas their discoveries, efforts, creativeness, and hard work have been ignored except among fellow hackers. In a way, it's similar to how the U.S. government and corporations support research and development: A group of researchers discover, explore, refine, or exploit a certain technology over a period of many years, yet their efforts go unnoticed unless their research results in a product acceptable to society. The researcher's results are shared, respected, and challenged among the scientific community and journals long before they ever result in a product (if they ever result in a product). In the same way that researchers and scientists relentlessly pursue their interests, I pursued answers to my curiosities and interests.

It is the groups that want to control the society (the legal system, and police) which have labeled "hackers" as notorious people. Hackers can use technology to access a variety of information which was previously accessible only to these groups, and these controllers are afraid of losing their advantages and control. Currently in US, the FBI is afraid of losing their ability to easily tap fiber optics so they're proposing to make it mandatory for central offices to make it easier for them. If people knew how common illegal wiretaps occur, they'd be upset at the abuse of power. Police are making illegal search and seizures, and district attorneys are filing outrageous affidavits to protect their control of power and access to information.

It was in the middle to late 1980's when the legal system and law enforcement agencies increased efforts to severely penalize hackers, when the risk of getting caught began to outweigh the excitement of discovering. It is unbelievably difficult to carry the burden of a "serious" criminal record throughout one's life when you're 20 years old (or for that matter 16 years old), as well as the eternal monetary debt which comes with these consequences. In the 1970's, the founders of Apple computer were caught selling Blue Boxes while they were in college and got off with a minimal fine. With today's laws, the potential jail time, monetary damages, and lawyer fees, the system would have wasted and banned the brilliance of Steve Wozniak and Steve Jobs. Apple Computer (and microcomputers) might not have been born (IBM would have loved that).

Technology has changed faster than the legal system and society can adapt, so for now, unapproved exploring of these technologies has been declared a serious offense. Society trusts the legal systems' judgement, but even in 1992 law-makers are just barely beginning to understand technology: "Is software patentable (do not confuse with copyrightable), and to what degree?", "What privacy and freedom of speech should we have with electronic mail and communications?" Don't let unqualified law makers make decisions about technology-related issues that will affect you, without them knowing what you have to say.

So it was in the late 1980's when I began preparing for my retirement. I outlined a set of goals and a plan to achieve them. Unfortunately this plan required several years to fulfill, but I knew it was the right time of my life to begin this ambitious plan. The goals I wanted to achieve were:

- 1) Pass the knowledge I've gained onto others.
- 2) Keep the "hacker" movement active.
- 3) Prepare myself to be legitimately successful so that I can help to influence society's views about technology as a member of the society.

Due to the increasing danger of getting caught, and to become successful, I was forced to hide from the mainstream hacker community and make my actions and efforts unknown. The first two goals were closely related and took slightly longer to complete than my original plan. However, they were a much greater financial sacrifice than I ever imagined. The third goal will probably require

the rest of my lifetime, but it's a challenge I accept.

To complete goals 1 and 2, I've spent the last 5 years preparing a "tomb" of information and knowledge used within the hacker community. Not all of the information is complete, but neither is the seed that grows to become a tree. Anyone with a telephone can guess ("hack" according to the media and law enforcement) 4-digit passwords to telephone calling cards or PBX out-dial lines, but I wanted "real" hackers. I talked and met with 100's of hackers world-wide to find the right individuals who can responsibly learn and append to this "tomb" -- people who have the desire, respect, effort and ability to encourage new generations of hackers. This group has been selected and trained, and I feel they are some of the best prospects. Their international mixing should give them an almost unlimited number of opportunities, and some protection. I wish them the best of all luck in their endless journey of learning and knowledge.

To become legitimately successful meant getting a respectable job. Obviously, with my interests, I knew it would have to be in the high technology industries. Unfortunately, getting a job interview or a job offer with these companies is difficult because the Human Resources departments always shun the hiring of hackers. This is ironic, because many of the engineers and programmers within these companies are made of ex-hackers, or people who share a similar intense interest in technology. Also, since some of the best experiences of a hacker are discovered non-legitimately they can't be presented on a resume.

My first step towards completing this goal was instinctive; to keep my excitement and enjoyment focused intensely on technology. This may sound strange, but many hackers know friends who "burn out" on hacking or working in the high-tech companies, and I didn't want to 'burn out' at 20 years of age, so I had to slow down my hacking activity.

The next step was getting a college education, which I've completed. College is not the answer to everything... in fact it's not the answer to anything, however, college is an experience I wish everyone could experience -- it's a unique experience. A college degree will not guarantee a job, but it might get you past the Human Resources department. If you have the chance to attend college, don't miss this chance. I realize employers prefer experienced workers over inexperienced "fresh" college graduates, but if you have a focused interest on a certain technology, then you will find a way to keep updating yourself while suffering through college. And like me, you will find the college degree combined with the results of your focused efforts will open the best job opportunities to you. Be focused and patient... it worked for me!

I am currently working on the inside of a technology-related company, enjoying the work I do for a living. In fact, sometimes I think to myself, "Wow, I get paid for doing this!?" It's a thrill to be doing what I do, yet I must work hard, and continue working hard to achieve the highest position I am able to reach to make the most of my abilities. In doing this, I hope someday to give something back to the non-hacking society which may show them that hackers are constructive to society, thus, changing their negative view which has labeled hackers synonymous to "criminals." I would like to see mature, legitimately-successful hackers, form an interest group to help cultivate the energy of the younger hackers.

Although I am retiring from the community, I can never retire the curiosity and intense interest I have about technology. Instead, I now focus these aspects legitimately into my daily work and will continue to do so. I've immensely enjoyed my involvement in the hacking community and will always treasure it. I also hope to eventually persuade people to accept hackers and to not persecute them. This last goal is the most ambitious goal, but I feel it's the most important goal, because those groups that control society are wasting a group of young and talented individuals who could be inventors of future

technologies. Now, I will formally say "goodbye" to my friends in the hacking community... but not for the last time.

Persevere,

Jester Sluggo

---

## "Truth Is Out Of Style"

An Investigative Report Into Computer Security Corruption

by Dispater

It seems that these days the anti-virus industry/community has brainwashed the public into thinking that any use of a modem will put you in contact with an unfathomable array of dangers. It sounds like something your mom said, when she didn't want you to stay out after dark doesn't it?

As it turns out the anti-virus community has all the moral fiber of television evangelists. As they preach on about the horrors of accessing information (without purchasing one of their products), they are engaging in the activity that they claim should be made a federal offense, in Congress. That is the "distribution of computer viruses. Not only have they been involved in this type of activity since they industry began, but now there is a self proclaimed "elite" [smirk] group of so-called professionals within the industry that wish to keep a monopoly on the virus trade, by ruining the reputation and lives of independent researchers. So in a way, we now have a "virus cartel" within the computer security industry.

### The Little Black Book of Computer Viruses

~~~~~

The Little Black Book of Computer Viruses is a printed text that has been around for a few years, but is finally making waves with people who think Prodigy and CompuServe are the best networks ever invented. Anyway, this book contains printed out versions of viruses. Gee, viruses are SO difficult for people to get their hands on aren't they? Well, one of the information dinosaurs got his name in print for condemning such immorality.

"Professional virus fighters such as Alan Solomon at S&S International are madder than angry hornets over the publication. They are encouraging anti-black book campaigns that include PICKETING THE AUTHOR'S HOUSE, boycotting shops that sell the book, petitioning Congress, and even bringing in lawyers."

-- ComputerWorld, June 29, 1992, page 4 (emphasis added)

Well isn't it interesting to note that while Mr. Solomon is encouraging personal and economic harassment of Mr. Ludwig, his close friend and business associate, Sarah Gordon is doing the dirty work for him.

The Con

~~~~~

The National Computer Security Association's 1st Annual Conference on Viruses took place in Washington, D.C. this past June. Alan Solomon and Sarah Gordon were there in full force. Gordon has often been referred to as being Solomon's sidekick and nowhere did she live up to this distinctive title more than at this conference.

At the conference, Gordon purchased not one, but two copies of Ludwig's book and then immediately ran to the conference organizer to make a dramatic scene over how immoral it was for Mr. Ludwig to be selling such a thing. As it turns

out this is not the first time Sarah Gordon has engaged in such hypocritical behavior.

Another interesting thing to note at the conference is the fact that one evening, Knight Lightning and a couple of others noticed some people sitting around a room and walked in out of curiosity to what was going on. As it turned out what was going on was a "midnight meeting" of sorts. KL and friends were asked to leave because "it was not appropriate that <they> be here." Why wasn't it appropriate? It's because what these people were doing was discussing the ways they were going to "take down bulletin boards" and damage people's career's who distribute viruses.

Sometime after this conference, I learned about their plan to use "the media to ruin these sysops. For example, to use influence with the media to call attention to this type of activity." These people even went so far as to compile a list of BBSes that they wish to "take down."

#### The Hit List

~~~~~

Phrack received anonymous mail containing the BBS "hit list" that the self-proclaimed "elite" group of modem vigilantes put together to target first. Upon our receipt of this list, Phrack staff members contacted the sysops of these boards and as a result, many of the numbers have since been changed.

+1-206-481-2728	The Festering Pit of Vile Excretions [This phone number belongs to a construction company called Custom Building Co.]
+1-213-274-1333	West Coast Technologies (Tymnet 311021300023)
+1-213-274-2222	DII
+1-213-PRI-VATE\)BBS-A-Holic
+1-ITS-PRI-VATE/	
+1-301-PRI-VATE\)Digital Underground
+1-301-913-5915/	
+1-301-948-7761	Cornerstone III []
+1-305-669-1347	The Penthouse
+1-516-466-4620\)Hamburger Heaven: this was down for software problems, was titled Sentinel's Gate
+1-517-PRI-VATE/	The Final Frontier
+1-602-491-0703	Pirate's Guild
+1-708-541-1069	Night Eyes
+1-717-367-3501	Pirate's Cove
+1-818-831-3189	Silicon Central
+1-901-756-4756	The Welfare Department [This is an insurance companies phone number]
+1-213-274-1333	West Coast Technologies (Tymnet 311021300023)
+1-213-274-aaaa	DII
+1-313-LIM-ITED	Canterbury Woods
+1-409-372-5511	The Crowbar Hotel
+1-514-PRI-VATE\)The Sacred Reich
+1-514-975-9362/	
+1-516-328-0847	The Grave of the Lost
+1-516-541-6324	Realm of Heroes
+1-708-459-7267	Hell Pit
+1-713-464-9013	South of Heaven
+1-818-831-3189	Pirate's Cove
+1-819-PRI-VATE	Brain Damage

It is unclear as to whom is directly responsible for the organization of this

group or who is responsible for creating and distributing the list, however there were representatives from CERT, ISPNews, and several other well known individuals who are self-proclaimed security experts as well as a slew of nobodies who wish to make a name for themselves.

The Hell Pit BBS

~~~~~

The Hell Pit is a BBS system in Chicago and operated by a sysop named Kato. Kato has a legitimate curiosity (as if a curiosity needs to be validated) about the inner-workings of viruses. I shall let him relate his experience:

"I have been running The Hell Pit BBS for the past 3 years. It's gone through many phases in that time, but the most recent has been my affection for computer viruses. I became interested in viruses about one and a half years ago and I set up a virus file base on my system. At first I had a mere 5 or 6 viruses that I had collected from a system in the area. My collection has grown to about 700 IBM computer viruses."

"It seems to be their objective to shut down my bulletin board system and therefore eliminate my virus database. Considering these anti-virus personnel claim to be interested in aspects of computer security, I find their tactics highly questionable. There was recently a NCSA anti-virus conference. I learned from sources that one of the people attending the conference [Sarah Gordon] had committed certain acts on my BBS. This person claimed to have called up, uploaded 3 fake viruses, gained access to my virus database and then downloaded several viruses. This is their proof that I do not adequately control virus access on my system. The anti-virus personnel do not allow me to defend myself."

"Anti-virus personnel themselves have committed the same mistakes as I did, probably much more often. There is no set of rules that determines what makes someone an anti-virus authority. Certain people that seem to fit the mold are allowed to exchange viruses with anti-virus personnel. What are the criteria for these people? Is there any? It has been my experience that if you get involved with the right circles, you are considered an anti-virus authority. However, there are many places in the anti-virus community for viruses to leak out. For one thing, you can never be certain who you are dealing with. Just because someone is smart and claims to hold an anti-virus attitude is no guarantee that that person isn't an "in the closet" virus writer.

"At anti-virus conferences such as the NCSA anti-virus conference, guests were exchanging viruses like they were baseball cards. That isn't what I would consider controlling access."

"They do help a lot of people with computer troubles. However, to criticize me for not properly controlling access to my collection of viruses is being hypocritical."

"If anyone would like to call my system to check things out, feel free. I have a lot more to offer than just computer viruses. I have a good number of text files and some pretty active message bases. The Hell Pit BBS - (708) 459-7267" - Kato

#### Conclusions

~~~~~

It seems there is a move afoot in the anti-virus community to rid the world of bulletin board systems that disseminate viruses openly and freely. The anti-virus professionals believe that they must "defend the world" from this type of activity. Even though during a recent conference in Washington, D.C., it was disclosed that an anti-virus researcher recently uploaded three (3) viruses

onto a virus BBS (Hell Pit). Why was this done? To "expose the fact that the sysop was not as careful as he claims to be." The person that did this was then able to download viruses which was against the policy the sysop claimed was in place (of course this statement is based upon the integrity of the anti-virus community and their integrity is obviously suspect).

So, the anti-virus community set-up this sysop and made an example of him in a national conference without allowing him the opportunity to defend himself. In fact, the sysop may still be totally unaware that this event has even occurred, until now that is.

These anti-virus researchers were openly exchanging copies of viruses for "research purposes only." It seems okay for them to disseminate viruses in the name of research because of their self-proclaimed importance in the anti-virus community, but others that threaten their elite (NOT!) status are subject to be framed and have examples made of them.

Do As I Say, Not As I Do

~~~~~

This type of activity raises a very interesting question. Who gives private sector computer security employees or consultants carte blanche to conduct this type of activity? Especially when they have the gall to turn around and label hackers as criminals for doing the exact same thing. The answer is not who, but what; money and ego. Perhaps the most frightening aspect of this whole situation is that the true battle being fought here is not over viruses and bulletin board systems, but instead the free dissemination of information. For a group of individuals so immersed in this world, there is a profound ignorance of the concepts of First Amendment rights.

Phrack Magazine is ready to stand tall and vigorously keep a close watch and defend against any incursion of these rights. We've been around a long time, we know where the bodies are buried, our legion of followers and readers have their eyes and ears open all across the country. Those of you in the security industry be warned because every time you slip up, we will be there to expose you.

Dispater

---

Tim Foley Virus

~~~~~

By Guido Sanchez

Right after I moved from 512 to 708, I had the misfortune to realize that Steve Jackson Games, a company whose games I readily buy and play, had a BBS up in my home town called the Illuminati BBS. This was my misfortune as I could have called it locally in Texas, but now instead had to spend my phone bill on it from Illinois.

A good year after the Secret Service assault of Steve Jackson Games, after most of the "evidence" was returned with nifty little green stickers on it, a text file was put up on the BBS called FOLEY.TXT, a simple copy of the lawsuit that Steve Jackson Games had filed against the government, also known as JACKSUIT.TXT, distributed by the EFF I believe.

[Editor's Note: We have been unable to confirm that EFF ever released a file called JACKSUIT.TXT, however details of the EFF's participation in the Steve Jackson Games lawsuit can be found in EFFector Online 1.04.]

It was called FOLEY.TXT obviously because of Timothy Foley, a big-shot government guy [actually an agent for the U.S. Secret Service] who is one of

the defendants in the case. I downloaded the file, and zipped it into a file called, surprisingly enough, FOLEY.ZIP.

Within the next week, I was gleefully spreading information as usual, and uploaded the FOLEY.ZIP file along with a batch of viral files to a local BBS with a beginning virus base. The theory here is to spread viruses about, accessible to all so that wonderful little Anti-Viral programmers cannot succeed.

Unfortunately, the FOLEY.ZIP file was put into the viral file base, and before I could warn the sysop to move it into the appropriate file base, about 8 lame warezwolves had downloaded it and by the end of the week it was widely spread around the 708 NPA.

The moral of this story? None really, it's just an amusing vignette of what can happen when people become involved in the intense bartering of information that takes place via modem, and can get ridiculed if they're not sure of their commodity. That's all this huge business is, everyone is a courier. Whether they're pirated files, adult files, sound files, viruses, or text files; 90% of the time they're just downloaded from one 1.2 gig board and uploaded to the next one for more credits to download more files, etc.

It's a great big cycle, just like life. So, to risk sounding cliché, my rally to all is this: "Slow down! Sit back and pick the roses, eat them, digest them, and eventually <hopefully> excrete them!" Mr. Warhol, my fifteen minutes are up. The soapbox is now free.

The Hacker Files

June 22, 1992

~~~~~

By Barbara E. McMullen & John F. McMullen (Newsbytes)

NEW YORK -- DC Comics has announced the introduction of a new twelve-issue series, "The Hacker Files." DC spokesperson Martha Thomases said that the first issue will ship on June 23rd.

The series, created by science fiction author Lewis Shiner, deals with the adventures of "super-hacker" Jack Marshall who, prior to the events chronicled in the series, unjustly lost his job at Digitronix and now operates as a free-lance consultant.

The first story line, covering the first four issues of the series, deals with Marshall's attempt to uncover those responsible for jamming ARPANET (Network of Advanced Research Projects Agency) and causing NORAD's Space Surveillance Center inside Cheyenne Mountain, Wyoming to malfunction, bringing the United States to the brink of nuclear war.

In the course of his investigation, Marshall, AKA "Hacker," is assisted by a number of members of the hacker community -- "Master Blaster," "Sue Denim," and "Spider" (Master Blaster, whose real name is Mikey is a student at New York City's Bronx High School of Science).

Fiction comes close to reality when it appears that the person responsible for the virus that caused the damage is Roger P. Sylvester, a student at Columbia University and the son of a high ranking official at the National Security Agency (NSA); on November 2, 1988 Robert T. Morris, Jr., a Cornell student and son of NSA's chief computer scientist, caused the crippling of the Internet through his release of the "Internet Worm."

Shiner told Newsbytes, "The similarity of the characters was, of course done intentionally -- you might even note the somewhat subtle connection of the names: 'Sylvester The Cat' and 'Morris The Cat.' I did it partially to show those somewhat knowledgeable about computers that the plot was not made out of

whole cloth but was the result of a good deal of research."

Shiner continued, "When reading comics, I look for information density and I tried to make the Hacker Files rich in that regard. I'm hoping to attract some computer-literate young people to comics -- comics were one of the earliest forms of expression to make great use of computers and I hope, with the Hacker Files, to involve more computer types in the medium."

Shiner also told Newsbytes that his experience as a programmer with a small Dallas software firm provided him with an ongoing interest in computer and communications technology. He added, "The firm was sold to EDS (Electronic Data Services), Ross Perot's firm, and, with long hair and jeans, I didn't fit into the EDS mold so I left and concentrated on writing."

---

"Sneakers" by Universal Pictures

June 24, 1992

~~~~~

Taken from PR Newswire

Follow A Team of High-Tech Security Experts
Into The Complex World of Computer Crime

"I was trying to break into Protovision. I wanted to get the programs for their new games." -- David Lightman (Matthew Broderick, "WarGames").

"The world isn't run by weapons anymore, or energy or money. It's run by little ones and zeros. Little bits of data. It's all just electrons." -- Cosmo (Ben Kingsley, "Sneakers").

In 1984, screenwriters Walter F. Parkes and Lawrence Lasker received an Academy Award nomination for their script which followed the adventures of a young high school hacker (Matthew Broderick) whose computer made contact with the mainframe computers at North American Air Defense Command (NORAD).

A critical and box office success, "WarGames" was the first major motion picture to explore the emerging worlds of computer games, hacking, crashing and data piracy. It soon found a legion of fans who had also discovered the vast frontiers available through their personal computer.

Eight years later, Parkes and Lasker along with writer-director Phil Alden Robinson ("Field of Dreams") have collaborated on "Sneakers," a Universal Pictures release which follows a team of high-tech security experts into the complex world of computer crime. The caper film, directed by Robinson, stars Robert Redford, Dan Aykroyd, Ben Kingsley, River Phoenix, Sidney Poitier, David Strathairn, James Earl Jones, and Mary McDonnell.

Parkes and Lasker first heard the term "sneakers" at a computer convention in 1981 as a nickname for IBM's kid programmers. Months later, they met the editor of a small computer magazine who had a very different definition of the word. "Sneakers," their source explained, is a term that is synonymous with "black hatters" and "tiger teams," or individuals who are hired to break into places in order to test the security of the installation.

Teaming up with Robinson, the trio wrote the basic outline of a story about a team of sneakers whose questionable pasts had brought them together. Robinson then embarked on some extensive research, but what had begun as basic fact-finding about computer outlaws soon evolved into clandestine meetings with underground hackers, FBI men, cryptologists, wire tappers, professional penetrators and an endless stream of cyberpunks who were the pioneers in system break-ins.

The "Sneakers" research led to meetings with numerous characters, ranging from the notorious Captain Crunch (John Draper) to renowned mathematician Leonard

Adelman, called the father of public-key encryption. Using computer encryption as a plot device, the writers were able to concoct an intricate "what if" story which explored the possibility of a "black box" that could potentially crack the code of any electronic information in the world.

"'Sneakers' has to do with a new age... the information age," said Redford. "It's quite possible that a war in the future will be a war of information. Whoever has it, wins."

Coming to theaters this September.

Pirates v. AT&T: Posters

~~~~~

Special thanks to Legacy Irreverent and Captain Picard

On May 24 1992, two lone pirates, Legacy (of CyberPunk System) and Captain Picard (of Holodeck) had finally had enough of AT&T. Together, they traveled to the AT&T Maintenance Facility (just west of Goddard, Kansas) and claimed the property in the name of pirates and hackers everywhere.

They hoisted the Jolly Roger skull and crossbones high on the AT&T flagpole, where it stayed for two days until it was taken down by security.

This event was photographed and videotaped by EGATOBAS Productions, to preserve this landmark in history. And now you can witness the event. For a limited time they are offering full color posters and t-shirts of the Jolly Roger Pirate flag flying high over AT&T, with the AT&T logo in plain view, with the caption; "WE CAME, WE SAW, WE CONQUERED."

|         |                                  |            |
|---------|----------------------------------|------------|
| Prices: | 11" x 17" Full Color poster..... | \$ 7.00 US |
|         | 20" x 30" Full Color poster      | \$20.00 US |
|         | T-shirts                         | \$20.00 US |

If you are interested in purchasing, simply send check or money order for the amount, plus \$1.00 US for postage and handling to:

CyberPunk System  
P.O. Box 771027  
Wichita, KS 67277-1072

Be sure to specify size on T-shirt.

A GIF of this is also available from CyberPunk System, 1:291/19, 23:316/0, 72:708/316, 69:2316/0. FREQ magicname PIRATE

---

#### Telco Trashing Yields Big Rewards

July 20, 1992

~~~~~

by Anonymous

A few days ago, I was faced with a decision about what to do that fine evening: Try and make amends with my girlfriend or go dumpster diving down at the Bell Central Office. Well I guess I am a true lamer since I opted for the telco, but my choice did not go unrewarded as I found a nice little treasure.

The building is a old 1940's brick place with almost no security whatsoever, not even a guard on Sunday nights. So, it was no problem to jump the barbed wire fence that surrounded the truck lot where the dumpster was located. After rooting around through the dumpster for something worth my while, I came across a medium sized box that apparently had been used by one of the employees for moving since written on the were the words "pots and pans, kitchen."

Naturally intrigued by this strange box in a telco dumpster, I opened it and found quite a surprise! There, staring up at me, was a binder with a label stuck on it that read "Phrack 23." Inside I found the entire collection of Phrack 1-39, Informatik 1-4, and LOD/H Technical Journals 1 and 2 (apparently they were too cheap to print out the rest). They were poorly printed on a laser printer (or well printed on a ink jet), but they were much better than the cheesy job I had done printing out mine. :-)

Apparently someone at the telco is a phreaker that infiltrated the ranks of South Central Bell or they have been reading up on the latest and greatest in the phreaker/hacker community.

Perhaps not as valuable as a list of COSMOS passwords or dialups, but still it was quite a find.

Anonymous Mail On IBM VM Systems?

~~~~~

Date: Tue, 28 Apr 92 14:54:58 EST

From: Apollo

Subject: Anonymous Mail

To: Phrack Staff

Dear Phrack Staff,

I was reading a past Phrack issue and noticed that you can send anonymous mail from a UNIX system. I know that there is a way to send it from a VM system. However, the people at my node don't want anonymous mail sent, so they do not tell us how it's done. Can someone PLEASE tell me how I can send anonymous mail via a VM system?

-- Apollo --

From: Mind Mage

Subject: Anonymous Mail

To: Apollo

I assume that you know you can telnet to any VM system on the Internet and send anonymous mail using port 25 and a commands that are very similar to that of the UNIX SMTP.

If you want to send it from your particular system, you can try telneting to port 25 of your own machine and doing it from there.

Mind Mage

---

WWIV Link Hack

~~~~~

By Mr. Bigg (Rebel*-Jedi)

Not that many people care but here is a nice little trick I happened to come across and feel like sharing.

Hack for WWIV Systems Using Multi-Net v1.0 Mod
Usually used for LinkNet

Main Login: @-!NETWORK!-@

Link Login: 1 (or whoever is sysop)

//edit config.dat

find system password in file

abort editing

//dos

enter system password

Viola, access to Dos :)

Lamely enough there is no password. Check for users when using this mod.

The Day Bell System Died

~~~~~

Sung to the tune of American Pie (with apologies to Don McLean)

Long, long, time ago,  
I can still remember,  
When the local calls were "free".  
And I knew if I paid my bill,  
And never wished them any ill,  
That the phone company would let me be...

But Uncle Sam said he knew better,  
Split 'em up, for all and ever!  
We'll foster competition:  
It's good capital-ism!

I can't remember if I cried,  
When my phone bill first tripled in size.  
But something touched me deep inside,  
The day... Bell System... died.

And we were singing...

Bye, bye, Ma Bell, why did you die?  
We get static from Sprint and echo from MCI,  
"Our local calls have us in hock!" we all cry.  
Oh Ma Bell why did you have to die?  
Ma Bell why did you have to die?

Is your office Step by Step,  
Or have you gotten some Crossbar yet?  
Everybody used to ask...  
Oh, is TSPS coming soon?  
IDDD will be a boon!  
And, I hope to get a Touch-Tone phone, real soon...

The color phones are really neat,  
And direct dialing can't be beat!  
My area code is "low":  
The prestige way to go!

Oh, they just raised phone booths to a dime!  
Well, I suppose it's about time.  
I remember how the payphones chimed,  
The day... Bell System... died.

And we were singing...

Bye, bye, Ma Bell, why did you die?  
We get static from Sprint and echo from MCI,  
"Our local calls have us in hock!" we all cry.  
Oh Ma Bell why did you have to die?  
Ma Bell why did you have to die?

Back then we were all at one rate,  
Phone installs didn't cause debate,

About who'd put which wire where...  
Installers came right out to you,  
No "phone stores" with their ballyhoo,  
And 411 was free, seemed very fair!

But FCC wanted it seems,  
To let others skim long-distance creams,  
No matter 'bout the locals,  
They're mostly all just yokels!

And so one day it came to pass,  
That the great Bell System did collapse,  
In rubble now, we all do mass,  
The day... Bell System... died.

So bye, bye, Ma Bell, why did you die?  
We get static from Sprint and echo from MCI,  
"Our local calls have us in hock!" we all cry.  
Oh Ma Bell why did you have to die?  
Ma Bell why did you have to die?

I drove on out to Murray Hill,  
To see Bell Labs, some time to kill,  
But the sign there said the Labs were gone.  
I went back to my old CO,  
Where I'd had my phone lines, years ago,  
But it was empty, dark, and ever so forlorn...

No relays pulsed,  
No data crooned,  
No MF tones did play their tunes,  
There wasn't a word spoken,  
All carrier paths were broken...

And so that's how it all occurred,  
Microwave horns just nests for birds,  
Everything became so absurd,  
The day... Bell System... died.

So bye, bye, Ma Bell, why did you die?  
We get static from Sprint and echo from MCI,  
"Our local calls have us in hock!" we all cry.  
Oh Ma Bell why did you have to die?  
Ma Bell why did you have to die?

We were singing:

Bye, bye, Ma Bell, why did you die?  
We get static from Sprint and echo from MCI,  
"Our local calls have us in hock!" we all cry.  
Oh Ma Bell why did you have to die?

---

The 1992 Consumer Electronics Show  
~~~~~  
By Sarlo

The Consumer Electronic Show is the annual event held in Chicago, Illinois, that gives a sneak peek at the electronic products to come to market, as well as products that are currently on the market.

The show is usually closed to the public. This year however, for a MEASLY \$10 fee, the common shmoe can waltz his ignorant ass right up to the door, get a

green stamp on his hand, and walk up to several displays, oohing and ahhhing, and gape like landed fish at the wonderous booths set up by various participating companies such as AT&T, most major bell companies, IBM, Prodigy, dozens of cellular manufacturers, Nintendo, Sega, and more software producers than I really have the patience to list.

I take a taxi to the McCormick center, a convention haven, and enter through the underground entrance. I walk down the nondescript hallway, noting that for a center that is supposed to be housing the latest in the future technology, nothing was that awe-inspiring. Expecting a lame show with shoddy video graphics, I purchased my ticket, got my hand stamped and entered the doors.

Into an enormous room, filling my senses with an array of Lights and Sound. You could almost smell the silicon as I made my way down the aisle displaying the giant Phillips Digital Compact Cassettes screen. Not being a huge fan of stereo equipment, I head over to the Sharp Electronics Display. It was a turn in the right direction, as it brought me face to face with one of the clearest and, per the name, sharpest video displays I have seen in my life. Their LCD big-screen televisions, displaying a aquarium scene. Even close up, distortion of the images were at a minimum. Along the north wall, a smaller, gutted version of the LCD display was shown, giving electronics buffs a firsthand look at the inner workings of the viewscreens. Turning a corner, I came face to face with their dual-projection wallscreen television. Instead of ghost images and a fuzzy, indistinct picture, I found that it may have very well be the highest quality video projection system I have ever come in contact with.

Cellular Mania

~~~~~

The highlight of the Cellular Phone section was the Motorola Cordless/Cellular display area with a large sign showing the spokesperson for Motorola, the eye-catching slogan above him:

"Cordless Phone Eavesdroppers Are Everywhere."

Immediately catching my interest, I wandered over to check out the smaller print:

"But with my Motorola Secure Clear (tm) Cordless Phone, my private conversations stay private."

Secure Clear, as the literature explains it, is an exclusive technology that assures you that no eavesdroppers will be able to use another cordless phone, scanner or baby monitor to listen to your cordless conversations.

As most of us know, security codes and multi-channels don't always prevent eavesdropping. With the latest technology these days, security codes, one of 65,000 possible codes that are randomly assigned every time you set the handset into the base, keeps someone from using your phone base as an outgoing phonenumber.

Using the Auto Channel Scan (ACS), the Secure Clear Cordless Phones automatically skip any channels that register noise or interference. Three guesses what Sarlo is getting himself for Christmas.

For more information on this or any other Motorola product, call their Consumer Products Division at (800)331-6456.

On other notes, Technophone had a wide variety of cellular accessories, including a Desk stand, spare batteries, an in-car charger, a new life of antennae, QuickCharge AC chargers, and a hands-free unit for safe operation in a car.

Omni Cellular had one of their Model "A" V833k Portable Hand-Helds open for a



demonstration, giving a static-free conversation with one of the salesmen. Many of the features of this phone were:

- o 90 Minutes of Talk Time
- o 10 hours of Stand-by Time.
- o and a sturdy design built right here in the USA.

Other features included Auto-Power Shutoff, Electronic Lock, 50 number memory, and signal strength indicator.

East Building Hipster Hi-Jinx

~~~~~

Growing bored, I headed over to the map. Searching it, I found, almost literally, my green light. On their illuminated map display, the green section of the map beamed out to me.

"Computers"

Hauling ass to the door, stopping for a quick inspection of my bags by the security guard, I strolled over to the east building (purchasing a way-keen CES-92 T-Shirt along the way), I burst into the building with a renewed vigor.

Right smack-dab in the front of the entrance there is the awful stench of men in business suits and cheap computer services. Right away, I knew I had found the Prodigy display.

With free trials and the salesmen prodding the consumers to subscribe to their system, I decided to take a look.

"Where else can you get such a great service, allowing you access to such a wide variety of things such as an online message service, up-to-date news, an online encyclopedia, and thousands of interesting users, people just like yourselves?" The Online-Conman peddled his wares to the unsuspecting consumers, not only misinforming them as to think that Prodigy is a useful service at all, but to actually have the gall to shove a PS/1 in their faces and tell them it's a quality computer.

"Umm... what about any Public Access Unix Site with an Internet or Usenet feed," I asked. The clod then got on his high-horse and addressed me.

"Perhaps. But most Public Unix's, or bulletin boards, for that matter don't have high-quality graphics to accompany the information." The man had definitely done his homework. But apparently IBM and Sears soaped the man's brains out thoroughly enough to the point where he actually bought the bull that they were forcing down peoples throats.

"Yea," I said. "But most public access sites don't waste a quarter of your screen space with worthless advertisements. I wasn't aware that pretty pictures made the news or messages any more informative, either. But I might also point out that they don't charge you a extra amount of money for every message over the 30th one, read your mail or censor your public posts, or, many times, even charge you a fee at all, other than possibly an optional subscription fee, around \$50 a YEAR at most, nor do they have small datafiles that collects information from the fat table from the subscribers." As I was speaking, the salesman was trying to interrupt me, finally succeeding at this point.

"Well, I can see you have a lot of questions," the salesman evades rather well. "So I'm sure this gentleman over here will be glad to answer any of your questions, while I can take this lady's question...Yes?"

I was approached by another salesman who asked me what questions I needed

answered. I said none, seeing as I didn't have much interest in his system anyhow, and that I was just seeing how good the Prodigy salespeople worked under pressure. He said he would be glad to answer any questions I had, but if I were only there to harass people, to please take it elsewhere.

Then it was off to the various other setups. Magazines were on display and free for the taking here, including Mobile Office, Various Nintendo/Game System magazines, and Audio Equipment. Walking down one of the back isles, I heard a bit of conversation that caught my ears.

Star Trek Straight To Your Home

~~~~~

"Computer. Recognize Picard, Jean-Luc. Kitchen Lights ON, Turn ON the VCR and hit RECORD. Close the Curtains, and turn on the Extasy Channel. Prepare to record "Chicks with Dicks."

- Jean Luc Picard

Stardate 1992.4, 2:45 A.M.

Such a Scenario is something you would think you could find only on Star Trek, right? Wrong. With the Mastervoice, the "Ultimate in Home Automation", the mastervoice is much like your own personal butler, telling the correct time, activating and operating any device in your household, and even with it's own alarm system. All of this, at the command of your voice.

Mastervoice can be designed to be used by up to four people, can be trained in any language. It distinguishes who is speaking, obeys the commands, but also speaks back to you -- in a HUMAN sounding voice. Male or Female. You can add or delete voices from it's recognition systems, you can also create new response words as well.

Featuring control over lights, stereo, TV, coffee maker, heating and cooling systems. It also has a Household Noise Override that allows you to have stupid children racing around your home in an obnoxious manner without disturbing the unit.

Plus, it is also a speakerphone/telephone with stored numbers. At the sound of your voice, it will dial or answer incoming calls and allow you to carry on a conversation without ever having to touch the system. It also interfaces with your PC for memory storage or control operations.

Built in infrared sensor and intrusion detection systems are another highlight of this demonstration. As it recognizes up to four voices, you can assign a password for each voice, being anything from "I am home" to "Supercalafragilisticexpialidoshes". If all fails, it can call the police for you. Nutty as all hell.

Mastervoice operates thru carrier current modules. This model, as one of the top of the line voice-recognition home-use systems, it is up there in the \$4,000 plus range, but seeing all the stuff it does, it's well worth the price.

Skipping the Game Module Section (Nintendo/Sega/TurboGraphix/etc) entirely, I ran into an interesting palmtop known as the Psion Series 3, and their new interlink software. Windows Compatable, the palmtop not only has communication software for a link between your PC and Palmtop, but also will support standard Hayes and Hayes compatible modems. Sporting a qwerty style keyboard and a romcard port, 128k and a 40 column screen, the Series 3 may be limited, but provides an acceptable amount of access to other online services. Though for now, a Windows based software package is only available, at the time of this writing, there will be DOS and UNIX compatible packages available to the public in 5 to 6 months.

==Phrack Pro-Phile==

Written and Created by Taran King (1986)

Welcome to Phrack Pro-Phile. Phrack Pro-Phile is created to bring info to you, the users, about old or highly important/controversial people. This month, I bring you perhaps the most famous all underground hackers and the founder of the Legion of Doom.

Lex Luthor

---

Personal

~~~~~

Handle: Lex Luthor

Call me: I really no longer identify with "Lex Luthor" and don't ever expect me to use the handle again with regards to calling boards so you CAN call me "Johnson."

Past handles: I was too status conscious to have more than one handle. All my effort went into just one persona.

Handle origin: From the Superfriends/Justice League of America (ABC TV) cartoon series where the Legion of Doom (LOD) kicked their asses until the series writers thought up some lame way for them to win, but of course, LOD always escaped to fight another day.

Date of Birth: You should know better than that.

Height: You should know better than that.

Weight: Approximately 610 Newtons plus or minus a few.

Eye color: With or without colored contact lenses?

Hair color: With or without my wig disguise?

Computer: Apple //+ collecting dust and a soon to be obsolete IBM 286.

Email address: lex@stormking.com

The Interview Of Lex Luthor!

~~~~~

by Taran King

TK = Taran King

LL = Lex Luthor

TK: So Lex, why have you finally relented to a Pro-Phile/interview when I have been after you to do one for about 5 years now?

LL: Well, I have to admit that I am still reluctant. This whole issue of computer security/insecurity, hacking/phreaking, philes/electronic publishing, etc. is still quite controversial and I would prefer to concentrate on strictly legitimate activities. Especially areas where the importance of opinions are negligible and the importance of facts are paramount, as in Science and Engineering. However, I realize that Phrack won't be around forever, so I thought that if I had any last words left to say I'd better say it now so here I am.

TK: How did you get started into hacking/phreaking?

LL: It was easy. I had a delicious shake for breakfast, one for lunch and oh sorry. No really, it WAS easy. I had a friend who bought an Apple and I used to go over to his house and watch him play Ultima I, a fantasy/adventure game. After drooling over Ultima long enough, I took all my savings and bought a system, which was in excess of \$1000 at the time. Being penniless, I had nothing else to do but learn the machine. My

friend then purchased a modem and started calling boards. I followed suit. He was interested in cracking software and became rather well known using the handle "The Punk". After he gave me some codes for various LD companies I started calling around. A short while later, I noticed that there were boards, sections of boards, and most importantly INFORMATION that I was not permitted to use/see. I was unhappy about being excluded especially from RACS III (Tuc eventually came around though) and took it upon myself to learn what was involved in accessing these systems and getting more information. I realized as most have, that providing information that others do not possess allowed me to be noticed and therefore gain more information. By the way, I still play Ultima, I BOUGHT Ultima VI two years ago but am just getting around to playing it now.

TK: What was more important to you, getting noticed or getting information?

LL: The information was undoubtedly the goal. I realize now, as many hackers and phreaks have in retrospect, that I am an INFORMATION JUNKIE. The notoriety was simply the means to be trusted with more information and knowledge. Unfortunately back then I was unaware that most of the information that I sought was available LEGALLY. I was blinded by the information itself, and did not concentrate on the \*methods of obtaining information\*. Now with the advent of CD rom databases, and also online databases, the information is readily found. The problem is that the service providers are pricing the disks and online time out of the reach of common people, which of course puts me back to square one in a way.

TK: Why do you need information?

LL: Look, if there is one thing that prevents people from doing things or pursuing their dreams, it's INFORMATION. Not money, not guts, not anything. With the right information just about everything else can be obtained with the exception of health and happiness I suppose.

TK: Give me an example.

LL: Okay. If you have ever been up late watching TV and 'ol Dave Del Dotto or Carlton Sheets or whomever gets on and is trying to sell you their "courses" on Real Estate, Buying at Government Auctions, etc. then you know what I am talking about. These guys made millions simply by obtaining information that the majority of people were not aware of and put it to use, they could have been anybody.

TK: What types of information do you look for?

LL: Although I always look to learn new ways of how to obtain information in general, i.e., what new databases are available and how to use them, etc. I am currently concentrating on scientific data since I am working on my Master's Thesis and a comprehensive literature search is required to prevent me from duplicating what has already been accomplished. The "don't re-invent the wheel" philosophy.

TK: You mention a thesis, what schooling have you had/are pursuing?

LL: I don't want to be too specific, however, I have an undergraduate engineering degree and am currently in the process of completing dual Master's degrees, one in Quantum Physics and the other in Engineering.

TK: Sounds heavy, but why be vague, you must have a computer-type or electrical engineering degree?

LL: No, and I get that a lot from old friends: "You are so good with computers, why aren't you doing that?" My interest in computers now is

simply to make them calculate equations and do simulations of physical systems. And to help me get more information.

TK: Let's get back to the H/P subject, there's a few people who have always contended that you and the guys in LOD really didn't know much of anything, is that true?

LL: Well I can't speak much about the old members, but their expertise satisfied me and other members (we would usually vote on new members, I wasn't a dictator you know). As for me, I realized early on that only certain people can be trusted with certain information, and certain types of information can be trusted to no one. Giving out useful things to irresponsible people would inevitably lead to whatever thing it was being abused and no longer useful. I was very possessive of my information and frequently withheld things from my articles. By not providing much data, some people may conclude that I didn't know anything at all. Its just that I didn't release it to just anyone and that dismayed various people probably to the point of lashing out at me and LOD.

#### Some People to Mention

~~~~~

Taran King: You were always hounding me for a Phrack Pro-Phile. Hope you are enjoying it.

Knight Lightning: Great guy, but how did he get so famous even though he never even broke into the E911 computer? Sad to see him get screwed by overzealous "professionals." Wish I had some money to donate to his defense fund.

The Blue Archer: Always wanted to meet him. I never got a chance to meet him face to face although I have known him for 8 years. To be honest, he was better at getting into systems than I was.

Tuc: Always willing to bend over backwards to help you out. I still use the briefcase he bought me in NYC many years ago.

Paul Muad'Dib: The one in New York. He is one of the smartest people I've ever met. I hope he is doing something worthwhile.

Bioc Agent 003: Talked to him quite a number of times and met him at TAP meetings, but we never got to be friends.

Cheshire Catalyst: I still owe him \$20. He lent it to me in NYC.

Control-C: A wildman with the women. I hope he gives me his STARGATE videogame when he gets tired of it. I don't play it every day like him, but I still can kick his ass.

Phantom Phreaker: He has a spiritual side to him that most people never realize.

The Videosmith: A fun person with talent. I was sad to see him leave the scene so early. Met with him in his home state two years ago just to say hello.

Dr. Who: Here is a guy who loved hacking and exploring systems. I mean he really enjoyed it. He got quite good at it too.

Telenet Bob: Met him up in Massachusetts at Dr. Who's conference.

Jester Sluggo: Met him up in Massachusetts along with The Sprinter. Obviously he knew more than he let on even way back then.

Compu-Phreak: I liked listening to his pirate radio station while he operated it. The FCC never did catch on.

Silver Spy: A very smart guy with a future. Someone who knows when to stop, but was a little bit panicky at times.

Erik Bloodaxe: Part of the original LOD group. I think he always wanted my job. I consider him a friend even though we had our misunderstandings.

Mark Tabas: Part of the original LOD group and sysop of Farmers of Doom (FOD) for the short time it was up. I hope he isn't in any trouble again.

Flash Hoser: A fellow information junkie in the Great White North (GWN).

Gary Seven: Probably one of the least known yet talented hackers around except that I mentioned him in the acknowledgement section of many of my files. He has since quit.

Digital Logic: Ran a good board for quite a while. An idealist who could give a great speech. Too bad no one would listen.

The Ronz!: Old friend who no one ever heard of unless they called Digital Logic's Data Service BBS.

Al Capone: Should have been born a few years earlier so he could have gotten into hacking when it was fun. He got into it too late and the risk became a little too high for him.

Quasi Moto: Sysop of Plovernet. Was a good sysop, but not much of a hacker. Still talk to him on the net.

King Blotto: Known him a long time. Glad he never put me on TeleTrial!

The Mentor: A fantastic writer. He ran a great board (Phoenix Project). The last time I talked to him was a few years ago, but he wasn't very talkative. I think he fell for the 'ol Lex is a rat rumors.

The Leftist: I hitched a ride with him to one of the SummerCons in St. Louis. Haven't talked to him since his trouble began, I hope he's cleaned up his act. I thought he was cool until I heard he was making stuff up about me to the investigators.

The Prophet: A kindlier gentler hacker. Sorry to see him get screwed by the system.

The Urvile: Met him at SummerCon '89. Definitely seemed to be the type who you could trust not to screw you over.

Sir Francis Drake: Met him at SummerCon '87. I'm glad I got a chance to.

Sir Knight: What a character.

Shooting Shark: I appreciate the favorable comments he made about me in HIS Phrack Pro-Phile.

A Few Other Things

~~~~~

While I'm on the subject of people, there is one thing that I have not see

published in any form, and that's a "Where are they now" type of thing for ex-hacks/phreaks. Just so people know, there are a number of us who are doing quite well at lawful pursuits.

For example:

|                     |                                                           |
|---------------------|-----------------------------------------------------------|
| Silver Spy          | - Completing a Master's Degree in Electrical Engineering. |
| Knight Lightning    | - Working to become a lawyer.                             |
| The Unknown Soldier | - A high level manager at a successful software company.  |
| The Mentor          | - Creating games at a well known game company.            |
| Jester Sluggo       | - Working for a 'high technology' company.                |
| The Disk Jockey     | - Working in the computer business.                       |
| Gary Seven          | - Chief engineer at a radio station.                      |

#### The Interview With Lex Continues

~~~~~

TK: In an early issue of Phrack you were referred to by the following:
"There is paranoia and beyond paranoia there is Lex." How do you respond to that?

LL: Ha Ha, I remember that one. Well of course there is some truth to it. And the saying, "better paranoid than sorry." is true as you can see since I am not behind bars... not that I ever did anything illegal of course, ahem. I should mention that I met two individuals early in my hacking career that had a significant influence on me, and both are the absolute epitome of paranoid.

One was "Eliott Ness" who was probably in his late 30's to 40's by the sound of his voice. He used to call LOD, I met him on a local board. He was extremely knowledgeable, but always knew when to stop giving general information, never gave out ANY personal information, and never communicated for any length of time.

The other guy was "Number 6" from TAP meetings in NYC. I met him a few times. Six was another older gentleman. He was very calm until anyone showed up with a camera. Then he "went off" until the camera threat was negated. This guy had a way of extracting information out of you without you even realizing what he was up to.

As I recall people would ask him a question and he would simply turn it around and say, "well, what do you think (or know) about so and so" and the hapless phreak would spill his guts with Six taking notes and sometimes making corrections to what the phreak said much to the phreak's surprise. But Six never really gave out much information although it was completely apparent to me that he knew a great deal just by the way he carried himself.

A few phreaks would try to follow him after the TAP meetings, but he always lost them without ever letting on that he knew he was being followed. It should be mentioned that paranoia can destroy you (as the song goes). A number of times I ran into real problems trying to escape from suspected problems that probably weren't anything to worry about.

TK: What memorable H/P BBSes do you recall?

LL: OSUNY: Caught the tail end when I first started. I was impressed.

Plovernet: That BBS was crazy. Constantly busy since it had hundreds of active users and Quasi Moto let everyone post whatever they wanted and never deleted messages unless there was no disk space left. We helped start the "philes" trend there also. It was easy to spot who knew what they were talking about so I

invited them onto the LOD BBS. Some of the people on the LOD BBS were then asked to join the now infamous LOD group.

TK: (*Interrupts*) Did you ever think the group you started would become a household name in security and hack/phreak circles?

LL: Although I knew the guys in the group were good hacks/phreaks, I had no clue of where it was leading. Since we did not tolerate destructive/malicious behavior nor things like credit card fraud I did not think there was much risk in the group as a whole getting any real attention. Of course, all that changed with time.

TK: Sorry for the interruption. Please continue.

LL: Metal Shop Private: The users were idealistic and good natured which was refreshing. I liked it most because it was a good source of information/files and we were the first to see new Phrack issues.

Farmers Of Doom: Mark Tabas did a fantastic job with this one. It was quite busy, but did not remain up very long.

Phoenix Project: Again, another fantastic job. The Mentor had some rather unconventional ideas like letting security people on, which I thought was a good idea.

RACS III: Tuc didn't give me the time of day at first, but eventually I got on. Then he took it down.

Pirates Cove: The board in 516 (Long Island, NY). One of the classics. It's where I met Emmanuel Goldstein and invited him onto Plovernet to help sell 2600 subscriptions.

Catch-22: Absolutely positively the most secure BBS I ever encountered. Besides passwording subboards along with requiring users to have a high enough security level to access them, it made use of many concepts from the "basic security model" introduced by Lampson and later augmented by Graham and Dorothy Denning. Of course Silver Spy and I had no clue what an access matrix was and things of that nature. A duress password was implemented so if someone got nailed they could enter the password, not compromise the system, yet appear as to be cooperating with the authorities who we presumably thought would ask the hacker to call. It was never used but nice to have.

BlottoLand: Good board for a while, but he let too many of his "loyal subjects" on the system who were locals and they eventually overran it.

TK: Do you REALLY think you are ELITE or what?

LL: I really don't know how anyone got the idea that I considered myself elite. The only people who said I thought I was elite were those who I never met or talked to. Contrary to some people's belief, I never considered myself as elite. I was just a guy who liked to pass information on to others so I wrote some files. The files did help me get access to more information by making me more well known. When I read the newspaper, I'm one of those annoying people who keeps interrupting your breakfast to tell you details about all the neat stories.

TK: Speaking about the group, what do you think about Erik Bloodaxe and others starting ComSec Data Security?

LL: When I first called Bloodaxe after I saw them in the papers/magazines he thought I would be mad, maybe that he took my idea or something. I told him I am familiar with the computer security consulting business and don't want any part of it. It's too tough to get people to pay money for something that they cannot get a verifiable return on their investment. Besides, getting them to trust you with their inner most secrets is extremely difficult.

I told ComSec to write articles about security until their fingers fell off. Legitimize themselves as soon as they can. There was too much prejudice out there against them with ComputerWorld leading the pack. I really think they could have helped some companies if given a chance. But I don't think they had enough knowledge about the whole security picture, i.e., Physical Security, Environmental Systems (fire suppression, UPS, etc), Administrative Security (Hiring/firing policies, etc.), what goes on in big IBM shops MVS, CICS, ROSCOE, etc. There is a lot involved.

TK: How did you feel when Knight Lightning and Phrack erroneously insinuated that you might have informed on other hackers, maybe even the Atlanta Legion of Doom members a few years ago?

LL: Well as you now know, Craig (KL) has seen all the documents and records from his trial and many documents from the Atlanta case and there was no mention whatsoever of me in regards to providing information, being a witness, testifying, etc.

Although I haven't talked to the Atlanta guys since before their trial I am sure they know I had absolutely nothing to do with what happened to them. The real story has since come out. If there is one thing I hate, it's being accused of something you didn't do.

If someone does something they are accused of, he should be man enough to admit it. I have said this before a number of times, I have never provided information to anyone about other hacks/phreaks that directly nor indirectly led to them being visited, arrested, or prosecuted. It's just not my way. What goes around comes around and that kind of boomerang is something I knew I didn't want to play with.

My success in avoiding trouble is fairly straightforward: Most of all it was secrecy and misdirection (ala Stainless Steel Rat), avoiding phone company computers especially those in which I was a customer of (i.e., my local RBOC) because if you get THEM pissed at you, they'll get you one way or another. Also, lots of LUCK and not intentionally making any enemies although there have been a few hackers mad at me whom I never even talked to and I have no idea as to why they didn't care for me.

TK: Do you have any advice for people out there who may want to begin hacking or phreaking?

LL: I am not one to dictate what people should or should not do, but I wouldn't if I were them. The technology to prevent and detect security breaches and then to track down their source is ever improving. The Cuckoo's Egg (by Cliff Stoll) provides a good example of that. But that shouldn't even come into the picture.

I think they should examine objectively why they want to do it. Then make an honest attempt at finding other legal ways to accomplish whatever they were trying to do. I don't care how you justify it, it's dishonest. Forget about the law part of it. It just causes other people problems. I didn't know how much until my school's systems were hacked and I was unable to read my e-mail for a week. I was angry and thought to myself that I'd like to get my hands on that asshole hacker. Then I laughed for quite awhile realizing what I was thinking and the irony of it all.

Poetic justice I suppose. None of my data was touched, but I was denied service and denial of service can be just as damaging. As for the challenge of it, well I can't deny that that was very addicting, but there are many legal ways to challenge yourself.

TK: What conventions/involvements outside of phone calls have you done?

LL: TAP meetings were probably the first. Then a Con in Massachusetts, the Con in Philly with Videosmith et al. and of course the few SummerCons (1987 and 1989) in St. Louis. There were some computer security conferences that were interesting also. Those helped to sensitize me to the "other side."

TK: I remember at SummerCon '89 that you were accidentally caught on video tape for about 2 seconds and requested that it be erased, which it was. What is the deal with cameras?

LL: It may sound a little odd, but I don't think anyone has the right to take another person's picture without their permission. Especially when the person who is on film has no idea where the picture will end up.

I predict within 5-10 years maximum that states will start using video cameras to digitize your picture when you go for a new driver's license. The digitized image will be stored with the rest of your personal information and probably be available to people like private investigators and others who gain access to the information illegally. With ISDN, Multi-Media, etc., it will be possible to "set up" people very easily by altering images via computers, etc. to make them look like they are doing just about anything you can think of. When things like that start to happen I will not look crazy but smart, at least to my friends who think my avoidance of cameras is abnormal.

Most Memorable Experience

~~~~~

TK: What are your most memorable experiences (funny things that happened to you during your phreaking/hacking or not so funny)?

LL: Dr. Who in Massachusetts had a conference in which me, Tuc, and The Videosmith drove up at 4 AM in Tuc's VW Beetle hydroplaning all the way due to the rain, and dead tired. We were all in a silly mood and had a lot of laughs.

Also, the time when I was in NYC with Paul Muad'Dib and we had no money to eat. He was the first person I know of who had any real knowledge of phone company switching systems. He engineered a switch in Manhattan to put call forwarding on a pay phone. Once this was done, all the money put into the phone would remain in the phone but would not drop into the coin box. Those who put money in didn't really have to since the phone was converted to a POTS (Plain Old Telephone Service). Alas, humans are creatures of habit. So after a couple of hours (since it was a busy phone) he had the guy put the phone back to the way it was. When this was done, all the money held in the phone was returned. It was like hitting the jackpot in Las Vegas. We then proceeded to McDonald's.

The story about me running around naked in a Motel 6 parking lot that Control-C has tried to get people to believe is, of course, grossly exaggerated. His girlfriend hooked me up with a friend of her's. Dan and his girl were in another room. He called me to come over, but I was in my underwear. We had been drinking so I ran the 8 feet or so to his room (we were on the 2nd floor with a solid balcony so no one from the ground could see anyway), I said hello and then ran back to my room to go another round.

Probably my favorite memory is relatively recent. J.J. Bloombecker, Director of the National Center for Computer Crime Data, spoke at my school. I sat in the very back as usual (I hate to have anyone sitting behind me, anywhere) in a room of about 40 people and listened to his speech which basically was to promote his book, "Spectacular Computer Crimes." I spoke to him but never let on who I really was. He talked about Craig's (Knight Lightning) case and then he went on about whomever named LOD, the Legion of Doom, should have named them something like the "Legion of Ineffectual Pansies." The reason being that, what prosecutor in his/her right mind would go to a judge and say how dangerous a group of ineffectual pansies are.

I sat there trying not to blush and thinking that of all the hundreds of people he said that to, he probably never expected to say it to the person who really named the group.

I did meet Donn B. Parker, whom I consider the father of computer security, twice. The first time I just shook his hand. The second time was relatively recently and we spoke for 20 minutes or so. I never told him who I really was, not that he would know anyway. But I complimented him enough so even if he found out, he couldn't have gotten too mad at me.

TK: What were some of your memorable accomplishments (newsletters/files/etc.)?

LL: The REAL accomplishments (non-files) will remain anonymous, but my favorite files were the IBM VM/CMS series because they were well written along with the Attacking, Defeating, and Bypassing Physical Security Devices series. Before I wrote a file I scoured boards and other traditional sources for the information I sought. If I came up empty handed, I researched it and wrote about it myself.

Although the COSMOS files helped me get started, they were a complete joke. They provided enough information to be dangerous and didn't help my standing with the RBOC's. The VAX/VMS files got better as they progressed, but except for some of Part III they didn't provide much that wasn't available in manuals. I enjoy writing, but it usually takes me many revisions to get it just right. As for newsletters, the LOD/H Technical Journal is another thing that I was involved in.

TK: What is the story behind the LOD/H Technical Journal?

LL: The LOD/H Technical Journal almost never was. As you are aware, LOD had gotten a group of files together to be published in PHRACK as an "all LOD issue," but some of the members thought we should put out our own stuff. The idea grew on me and I said okay. I should let it be known that you helped us out for the first issue by spell checking it and performing some editing and critique. But we were only able to produce 4 issues since it was difficult in getting quality non-plagiarized or non-highly paraphrased material.

After the third issue, I realized that I was probably not doing anyone any favors by exposing security holes and weaknesses in systems. Some people may not believe hearing this from ME, but I don't agree with those hackers who think they are doing people a service by exposing their system vulnerabilities. Nobody needs someone checking their door at night to see if its locked. And although the old door analogy isn't exactly the same as the pseudo-physical computer login, its close enough. Sorry about getting off the subject a little.

TK: That's okay. Why did you quit the H/P community?

LL: I wrote a letter to 2600 Magazine about a year ago that goes into it a

little. Between that and what I've said here, it should be fairly apparent. In brief, I realized I was mainly in it for the purpose of getting information. It got too dangerous and I decided to direct my energy to graduating instead of how to defeat security systems. The thought processes involved in hacking and those in solving problems in Engineering Design are remarkably similar and I think my hacking experience makes me a much better designer and problem solver. Not that I am advertising for a job or anything...

#### Lex's Favorite Things

~~~~~

- Women: Without Diseases.
- Cars: So fast that you are terrified to put the pedal all the way down to the floor.
- Foods: Anything that does not contain pesticides, herbicides, heavy metals, radioactive elements, toxic chemicals, harmful microorganisms, artificial colors, or preservatives. I guess that rules out fish, produce, meat, processed foods, drinking water, and so on. In other words there's nothing left to eat. In all seriousness, I do like great big salads and if I was rich I would have an awesome wine cellar.
- Music: Heavy Metal, some Punk, and Classical.
- Authors: Richard P, Feynman, Isaac Asimov, Stephen Hawking, Jane Roberts, Budd Hopkins, Jacques Valee, Bruce Sterling, K. Eric Drexler, and Matthew Lesko.
- Books: I liked the Cuckoo's Egg, anything about physics, and non-kook metaphysical books. The only thing I collect these days are books. I have hundreds of them.
- Games: Atari's ASTERIODS DELUXE was probably the most difficult videogame ever (even though it's more than ten years old) and which I am one of the best there is at playing it. When it comes to this, I admit I AM Elite. There's almost no one on this planet who can beat me. Defender and Stargate are also great. They don't make games like they used to. And of course, the Ultima series.
- Actors: Dana Carvey, Bill Moyers, Patrick Stewart (ST:TNG), Jonathan Frakes (ST:TNG), Andy Griffith (Matlock), and too many movie stars to mention.

The Interview Concludes

~~~~~

- TK: Is there anyone specifically that you want to say a few things to?
- LL: To all those who subscribe to the "Once a thief, always a thief" mentality and to those few die-hard law people who would love to get their hands on me and other ex-hackers: Don't bother, people are basically good and can be "rehabilitated" without going to prison.
- LL: The other thing that I have never understood about the hack/phreak community is some of the obsession with tracking people down. I could understand it a little better when the reason was to check out others to make sure they were not feds.
- I never compiled lists of who I talked to with anything except their handle, first name, and phone number. I never CNA'd them for their last names, or tried to find out where they worked.
- But some guys just had to know everything about everyone. Don't they have anything better to do? I was careful yes, but not to the point of invading everyone's privacy especially when the person stated they just wanted to be left alone. I am not saying I NEVER invaded another's privacy, but I don't now and almost never did it in the past.

I left an Internet mailing address at the beginning of this Pro-Phile so people can contact me. I don't mind talking to people, but I just don't think it's fair to harass and threaten people who don't want to be bothered. I am open to useful and constructive conversations via email, but I really don't think it's necessary to compile individual's personal information. I never did it and will never understand why people do it.

Besides, it's no great accomplishment to find people these days. The ways of getting information are numerous and many are legal, so how much skill does it really take to get someone's info? Almost none. Anyone can do it... on just about anyone they want.

TK: What do you think about the future of the hack/phreak world or telecom communications in general?

LL: As for the hack/phreak aspect, every time I think hacking is dead and people would have to be deranged to break into computers or make phone calls illegally for free, I read about another hapless person or group of people who have done it. Don't they realize there are better and easier ways of going about whatever they are doing? Don't they realize that the technology to CATCH you is such that you have lost the fight before you even get started?

Yes there will be new technologies that will help both sides, but there is the law of diminishing returns. As for what hackers should be doing, if anything they should keep an eye on our right to privacy. If it weren't for hackers, TRW would still be screwing people over (worse than they do now) and would have never apologized for not correcting invalid credit information.

TK: And of course the question that no Phrack Pro-Phile does without...

Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks?

LL: Absolutely NOT. I don't judge people on how they look anymore (yes I used to). As The Mentor so eloquently put it in his Hacker Manifesto (Phrack 7 and again in Phrack 14), of which this is, but a lame paraphrase, it's more important to relate to people on what they know and on their ideas than what they look like or what color their skin is, etc. And the vast majority have non-geeky ideas.

TK: Thanks for your time, Lex.

LL: Thank you for letting me ramble on for so long.

---

==Phrack Inc.==

Volume Four, Issue Forty, File 4 of 14

Network Miscellany

\*\*\*\*\*  
< How to Acquire Information on Internet Computers >  
\*\*\*\*\*

Compiled from Internet Sources

by The Racketeer  
of The Hellfire Club

Network Miscellany created by Taran King

Generally speaking, information is everything. A lot of hacking any computer on a network is being able to gather information about the machine and its vulnerabilities. This file is about using the available resources on the Internet network in order to gain important information about any perspective sites.

A large amount of information has been printed in Phrack recently about the Internet, most of it copied straight from manuals and in my opinion lacking hacking flair. Therefore, I'm going to take you straight into the heart of the heart of the matter with this file on acquiring information!

Now, the Internet is notorious for not having an instruction manual. Most people who find out what the Internet is learn from their friends. It used to be that there was only one real landmark on the Internet, and that was the SIMTEL-20 FTP archive. Now, the Internet is probably the largest free network in existence. In fact, it's a hacker's paradise!

Unfortunately, you have to know about "public" sites on the network before you can use them. Likewise, how are you going to hack an organization if you don't know any machines on it? Sort of like trying to complain to Packard-Bell about your computer equipment not working when the bastards don't supply their name, address, or phone number. You are going to have to find another way to get that information if you want to get anything done.

There is not any one particular way to learn about a site. In fact, you'll have to combine several unusual methods of gathering information in order to obtain anything resembling a "complete picture." However, using the combinations of techniques described in this file, you can maneuver through any network on the Internet and learn about the machines within.

The first stop on this journey is the ARPANet Network Information Center (frequently called "NIC" by experienced network users). NIC's purpose is simply to keep track of all the network connections, fields, domains, and hosts that people wish to be told about.

To connect to NIC, you would issue a command from your Internet connected machine similar to this:

```
.----- command
\ /
[lycaeum][1]> telnet nic.ddn.mil
```

This will (within a short period of time) route you to the Network Information Center and grant you access. There isn't a straight forward login/logout system on NIC like other Unix computers; it will just connect you to the Information System upon connection. The message you will get will be similar to this:

```
*  -- DDN Network Information Center --
*
*  For TAC news, type:          TACNEWS <return>
*  For user and host information, type:  WHOIS <return>
*  For NIC information, type:        NIC <return>
*
*  For user assistance call (800) 235-3155 or (415) 859-3695
*  Report system problems to ACTION@NIC.DDN.MIL or call (415) 859-5921

SRI-NIC, TOPS-20 Monitor 7(21245)-4
@ <prompt>
```

Great, now we are in. Essentially, since NIC is just a great big telephone book, we need to let our fingers do the walking. Let's demonstrate a few simple commands as I go after one of the government contract giants, the

corporation known as UNISYS. Let's start by entering WHOIS.

@WHOIS

SRI-NIC WHOIS 3.5(1090)-1 on Tue, 22 Aug 91 15:49:35 PDT, load 9.64

Enter a handle, name, mailbox, or other field, optionally preceded by a keyword, like "host sri-nic". Type "?" for short, 2-page details, "HELP" for full documentation, or hit RETURN to exit.

---> Do ^E to show search progress, ^G to abort a search or output <---

Whois:

Okay, now we are in the database. Since Unisys is our target, let's go ahead and ask it about "Unisys."

Whois: unisys

|                                 |                                     |                |
|---------------------------------|-------------------------------------|----------------|
| Cartee, Melissa (MC142)         | unisys@email.ncsc.navy.mil          | (904) 234-0451 |
| Ebersberger, Eugen (EE35)       | UNISYS@HICKAM-EMH.AF.MIL            | (808) 836-2810 |
| Lichtscheidl, Mark J. (MJL28)   | UNISYS@BUCKNER-EMH1.ARMY.MIL        | (DSN) 634-4390 |
| Naval Warfare Assessment Center | (UNISYS) UNISYS.NWAC.SEA06.NAVY.MIL |                |

137.67.0.11

|                       |                          |                |
|-----------------------|--------------------------|----------------|
| Navratil, Rich (RN74) | UNISYS@COMISO-PIV.AF.MIL | (ETS) 628-2250 |
|-----------------------|--------------------------|----------------|

There are 28 more matches. Show them? y --> of course

|                                       |                               |                 |
|---------------------------------------|-------------------------------|-----------------|
| Peterson, Randy A. (RP168)            | UNISYS@AVIANO-SBLC.AF.MIL     | (ETS) 632-7721  |
| Przybylski, Joseph F. (JP280)         | UNISYS@AVIANO-SBLC.AF.MIL     | (ETS) 632-7721  |
| UNISYS Corporation (BIGBURD)          | BIGBURD.PRC.UNISYS.COM        | 128.126.10.34   |
| UNISYS Corporation (GVLV2)            | GVL.UNISYS.COM                | 128.126.220.102 |
| UNISYS Corporation (MONTGOMERY-PIV-1) | MONTGOMERY-PIV-1.AF.MIL       | 26.5.0.204      |
| Unisys Corporation (NET-MRC-NET)      | MRC-NET                       | 192.31.44.0     |
| Unisys Corporation (NET-SDC-PRC-CR)   | UNISYS-ISF-11                 | 192.26.24.0     |
| Unisys Corporation (NET-SDC-PRC-LBS)  | UNISYS-ISF-9                  | 192.26.22.0     |
| UNISYS Corporation (NET-SDC-PRC-NET)  | UNISYS-ISF-7                  | 192.12.195.0    |
| Unisys Corporation (NET-SDC-PRC-SA)   | UNISYS-ISF-10                 | 192.26.23.0     |
| Unisys Corporation (NET-SDC-PRC-SW)   | UNISYS-ISF-8                  | 192.26.21.0     |
| Unisys Corporation (NET-UNISYS-CULV)  | UNISYS-CULV                   | 192.67.92.0     |
| Unisys Corporation (NET-UNISYS-PRC)   | UNISYS-PRC                    | 128.126.0.0     |
| Unisys Corporation (NET-UNISYS-RES1)  | UNISYS-RES1                   | 192.39.11.0     |
| Unisys Corporation (NET-UNISYS-RES2)  | UNISYS-RES2                   | 192.39.12.0     |
| Unisys Corporation (NET-UNISYS2)      | UNISYS-B2                     | 129.221.0.0     |
| Unisys Corporation (STARS)            | STARS.RESTON.UNISYS.COM       | 128.126.160.3   |
| Unisys Corporation (UNISYS-DOM)       | UNISYS.COM                    |                 |
| Unisys Linc Development Centre        | (NET-LINC) LINC               | 143.96.0.0      |
| UNISYS (ATC-SP)                       | ATC.SP.UNISYS.COM             | 129.218.100.161 |
| Unisys (FORMAL)                       | FORMAL.CULV.UNISYS.COM        | 192.67.92.30    |
| UNISYS (KAUAI-MCL)                    | KAUAI.MCL.UNISYS.COM          | 128.126.180.2   |
| UNISYS (MCLEAN-UNISYS)                | MCLEAN-UNISYS.ARMY.MIL        | 26.13.0.17      |
| UNISYS (NET-UNISYS-RES3)              | UNISYS-RES3                   | 192.67.128.0    |
| Unisys (NET-UNISYS-SP)                | UNISYS-SP                     | 129.218.0.0     |
| UNISYS (SALTLCY-UNISYS)               | SALTLCY-UNISYS.ARMY.MIL       | 26.12.0.120     |
| UNISYS (SYS-3)                        | SYS3.SLC.UNISYS.COM           | 129.221.15.85   |
| Wood, Roy (RW356)                     | UNISYS@LAKENHEATH-SBLC.AF.MIL |                 |
|                                       | 0044-0638-522609              | (DSN) 226-2609  |

As you can see, the details on these computers get fairly elaborate. The first "column" is the matching information, second column is the network name or title, then it is followed by a phone number or IP port address. If the phone number has an area code, then it is of a standard phone nature; however, if it is (DSN) then it's on the "Data Security Network," aka Autovon (the military phone system).

Now, as you can tell from the above list, there are several UNISYS accounts at military machines -- including a military machine NAMED after Unisys (mclean-

unisys.army.mil). This stands to reason since Unisys deals mostly in military computer equipment. Since it is a secretive military group, you'd figure an outsider shouldn't be able to gain much information about them.

Here is what happens if you center on a specific person:

Whois: cartee  
Cartee, Melissa (MC142) unisys@email.ncsc.navy.mil  
7500 McElvey Road  
Panama City, FL 32408  
(904) 234-0451  
MILNET TAC user

Record last updated on 18-Apr-91.

Hmm.. Very interesting. This user obviously has access to military computers since she has a TAC card, and goes under the assumed identity as "Unisys" in general. Could this person be a vital link to the Unisys/U.S. Defense connection? Quite possibly. More likely she is a maintenance contact, since she can use her TAC card to contact multiple (confined) military networks.

I've gone ahead and requested specific information about kauai.mcl.unisys.com, which as far as I know is a focal point for the Unisys Networks. Of course, the information on this machine is non-classified (or if it IS classified, Unisys will probably be chewed out by Uncle Sam). Notice all the great information it gives:

Whois: kauai.mcl.unisys.com  
UNISYS (KAUAI-MCL)  
Building 8201, 10th Floor Computer Room  
8201 Greensboro Drive  
McLean, VA 22102

Hostname: KAUAI.MCL.UNISYS.COM  
Nicknames: MCL.UNISYS.COM  
Address: 128.126.180.2  
System: SUN-3/180 running SUNOS

Coordinator:  
Meidinger, James W. (JWM3) jim@BURDVAX.PRC.UNISYS.COM  
(215) 648-2573

domain server

Record last updated on 05-Aug-91.

No registered users.

Aha! The Coordinator on this machine doesn't use it! There are no registered users! Namely, if you wanted to hack it, you aren't screwing with the higher ups (this is good). Since when does Unisys buy computers from other companies? Can't they just grab a few off the assembly line or something? The computer is stationed in McLean, Virginia! That's where the CIA is! Could Unisys be developing computers for the international espionage scene? Obviously, there is a great deal of information to be sucked out of this machine.

How? The answer was listed there. The machine is a DOMAIN SERVER. That means this computer holds the network information used to identify all the computer systems on its network and all we need to do right now is figure out a way to squeeze that information out! But first, let's see if our hunch was correct in assuming the bigwigs are far away by checking out the head honcho, "Mr. Meidinger."



Whois: jim@burdvax.prc.unisys.com

Meidinger, James W. (JWM3)

jim@BURDVAX.PRC.UNISYS.COM

Unisys Corporation

Computer Resources

Room g311

P.O. Box 517

Paoli, PA 19301-0517

(215) 648-2573

Record Last Updated on 04-Jul-90.

Yup, Mr. Meidinger is far away -- Pennsylvania, to be exact. Not exactly keyboard's length away, is he? Besides, being in the "Computer Resources" department, I'd suspect he is just an accountant. Accountants are to computing as beavers are to trees (unless, of course, they actually like computers, which isn't a foregone conclusion in the business world).

I'm going to skip the rest of the information on NIC, since it has been overkilled in this particular magazine anyway. The only hint I have is to read CERT's and DDN's news blurbs, since they give out some interesting information which would be useful and educational. Besides, messing around with the CIA's hired goons sounds much more fun.

Now is the time for a little bit of a lesson in critical reasoning: the Internet isn't exactly a "free to the public" network, meaning you just can't attach your computer to a machine on the Internet and expect it to work all of a sudden. You need to configure your machine around the computers in the network domain you are linking into, and if you have their permission, then everything is cool. But once you're configured, and your router and/or server has been notified of your existence, does that mean anyone else has that information? The answer is yes, although that info won't be forwarded to a place like NIC -- it will have to be obtained another way.

All packets of data on the Internet need to be routed to and from valid computer hosts. Therefore, all of this information is stored on the network's gateway. But the routing information stored is simply in numeric format, such as 128.126.160.3. At least, that is as understandable as it gets, since Ethernet addresses are even more elaborate and in binary.

However, as Internet users know, there is more than a single way of describing a computer. "telnet 128.126.160.3" would be one way of connecting to a computer, or "telnet aviary.stars.reston.unisys.com" would be another way of connecting to the same computer. These names are chosen by the owner of the network, and are described through the use of "domain servers."

As you recall, kauai.mcl.unisys.com was listed by NIC as a domain server. This means that the names of the computer systems on that network are stored on that particular host. Of course, that's not the only thing. The domain server presents the computer name and IP number to the connecting machine allowing you to connect to the computer by using a "domain style name." Ultimately, everything is converted to IP numbers.

Most network software allows compatibility with domain servers, meaning if you want to connect to nic.ddn.mil, and you specify a command "telnet nic.ddn.mil" then you will connect to nic.ddn.mil. Sadly, this isn't true of all computers (which require IP numbers only), but at least it is true enough that the general user is likely to have such computer resources.

Reaching back to the Dark Ages, there is a computer program that allows machines that don't directly interpret domain style addresses to IP addresses to still find out what the name of a machine is. This program is called "nslookup" and is usually found in the Unix operating system (at least, I haven't used it anywhere else -- it might only work on Unix).

"nslookup" stands for Name Server Lookup (there has been some debate, it seems, if a domain server is really a name server, or visa versa; in fact, both describe what they do well enough to have conflict). Regardless, let's go ahead and work on learning how to use nslookup.

```
[lycaeum][2]> nslookup
Default Name Server:  lycaeum.hfc.com
Address:  66.6.66.6
```

Now, going back to that NIC information we got earlier, let's continue to hack on poor old Unisys, which is giving up its info every step we make. We determined that the kauai.mcl.unisys.com was a domain server, so let's jump ahead to that by changing our server to their server (after all, the computers we are after aren't on our machine).

```
> server kauai.mcl.unisys.com
Default Server:  kauai.mcl.unisys.com
Address:  128.126.180.2
```

Okay, now we have connected to the server. This isn't a constant connection, by the way. It will only establish a connection for the brief instant that it takes for it to execute commands. It doesn't require a password or an account to get this information off of a nameserver.

Let's start off by having it give us a list of everything about Unisys that this server knows. "Everything" is pretty much a good place to start, since we can't go wrong. If we come up with nothing, then that's what's available. The basic command to list machines is "ls" like the Unix directory command.

```
> ls unisys.com
[kauai.mcl.unisys.com]
Host of domain name      Internet address
unisys.com               server = burdvax.prc.unisys.com      3600
burdvax.prc.unisys.com   128.126.10.33                       3600
unisys.com               server = kronos.nisd.cam.unisys.com  3600
kronos.nisd.cam.unisys.com 128.170.2.8                         3600
unisys.com               server = kauai.mcl.unisys.com       3600
kauai.mcl.unisys.com     128.126.180.2                       43200
unisys.com               server = io.isf.unisys.com          3600
io.isf.unisys.com        128.126.195.20                      3600
reston.unisys.com        server = aviary.stars.reston.unisys.com 3600
aviary.star.reston.unisys.com 128.126.160.3                      3600
aviary.star.reston.unisys.com 128.126.162.1                      3600
reston.unisys.com        server = kauai.mcl.unisys.com       3600
kauai.mcl.unisys.com     128.126.180.2                       43200
rosslyn.unisys.com       server = aviary.stars.reston.unisys.com 3600
aviary.stars.reston.unisys.com 128.126.160.3                      3600
aviary.stars.reston.unisys.com 128.126.162.1                      3600
rosslyn.unisys.com       server = kauai.mcl.unisys.com       3600
kauai.mcl.unisys.com     128.126.180.2                       43200
rmtc.unisys.com          server = rmtcfl.rmtc.unisys.com     3600
rmtcfl.rmtc.unisys.com   192.60.8.3                         3600
rmtc.unisys.com          server = gvlv2.gvl.unisys.com       3600
gvlv2.gvl.unisys.com     128.126.220.102                    3600
sp.unisys.com             server = dsslan.sp.unisys.com       3600
dsslan.sp.unisys.com     129.218.32.11                      3600
sp.unisys.com            server = sys3.slc.unisys.com        3600
sys3.slc.unisys.com      129.221.15.85                      3600
cam.unisys.com           server = kronos.nisd.cam.unisys.com  3600
kronos.nisd.cam.unisys.com 128.170.2.8                        3600
cam.unisys.com           server = burdvax.prc.unisys.com     3600
```

|                            |                                     |        |       |
|----------------------------|-------------------------------------|--------|-------|
| burdvax.prc.unisys.com     | 128.126.10.33                       | 3600   |       |
| prc.unisys.com             | server = burdvax.prc.unisys.com     |        | 3600  |
| burdvax.prc.unisys.com     | 128.126.10.33                       | 3600   |       |
| prc.unisys.com             | server = kronos.prc.unisys.com      |        | 3600  |
| kronos.prc.unisys.com      | 128.170.2.8                         | 3600   |       |
| prc.unisys.com             | server = walt.prc.unisys.com        |        | 3600  |
| walt.prc.unisys.com        | 128.126.2.10                        | 3600   |       |
| walt.prc.unisys.com        | 128.126.10.44                       | 3600   |       |
| culv.unisys.com            | server = formal.culv.unisys.com     |        | 3600  |
| formal.culv.unisys.com     | 192.67.92.30                        | 3600   |       |
| culv.unisys.com            | server = kronos.nisd.cam.unisys.com |        | 3600  |
| kronos.nisd.cam.unisys.com | 128.170.2.8                         | 3600   |       |
| slc.unisys.com             | server = sys3.slc.unisys.com        |        | 3600  |
| sys3.slc.unisys.com        | 129.221.15.85                       | 3600   |       |
| slc.unisys.com             | server = dsslan.sp.unisys.com       |        | 3600  |
| dsslan.sp.unisys.com       | 129.218.32.11                       | 3600   |       |
| slc.unisys.com             | server = nemesis.slc.unisys.com     |        | 3600  |
| nemesis.slc.unisys.com     | 128.221.8.2                         | 3600   |       |
| bb.unisys.com              | server = sunnc.wwt.bb.unisys.com    |        | 3600  |
| sunnc.wwt.bbs.unisys.com   | 192.39.41.2                         | 3600   |       |
| bb.unisys.com              | server = burdvax.prc.unisys.com     |        | 3600  |
| burdvax.prc.unisys.com     | 128.126.10.33                       | 3600   |       |
| isf.unisys.com             | server = orion.ISF.unisys.com       |        | 3600  |
| orion.ISF.unisys.com       | 128.126.195.7                       | 3600   |       |
| isf.unisys.com             | 128.126.195.1                       | 3600   |       |
| isf.unisys.com             | server = burdvax.prc.unisys.com     |        | 3600  |
| burdvax.prc.unisys.com     | 128.126.10.33                       | 3600   |       |
| isf.unisys.com             | server = io.isf.unisys.com          |        | 3600  |
| io.isf.unisys.com          | 128.126.195.20                      | 3600   |       |
| gvl.unisys.com             | 128.126.220.102                     | 172800 |       |
| gvl.unisys.com             | server = gvlv2.gvl.unisys.com       |        | 3600  |
| gvlv2.gvl.unisys.com       | 128.126.220.102                     | 3600   |       |
| gvl.unisys.com             | server = burdvax.prc.unisys.com     |        | 3600  |
| burdvax.prc.unisys.com     | 128.126.10.33                       | 3600   |       |
| mcl.unisys.com             | 128.126.180.2                       | 43200  |       |
| mcl.unisys.com             | server = kauai.mcl.unisys.com       |        | 43200 |
| kauai.mcl.unisys.com       | 128.126.180.2                       | 43200  |       |
| mcl.unisys.com             | server = burdvax.prc.unisys.com     |        | 43200 |
| burdvax.prc.unisys.com     | 128.126.10.33                       | 3600   |       |
| mcl.unisys.com             | server = kronos.nisd.cam.unisys.com |        | 43200 |
| kronos.nisd.cam.unisys.com | (dlen = 1152?)                      | 4096   |       |

ListHosts: error receiving zone transfer:

result: NOERROR, answers = 256, authority = 0, additional = 3.

Bummer, an error. Funny, it claims there isn't an error, yet it screwed up the kronos address and knocked me out. Apparently, this domain server is screwed. Oh well, I guess that's really their problem because in the information it gave us, it was able to provide all the answers we needed to figure out the next step!

Quick analysis of the above information shows that most of the servers were connected to at LEAST two other servers. Quite impressive: A fault-tolerant TCP/IP network. Since it is fault tolerant, we can go ahead and use a different machine to poke into the "mcl.unisys.com" domain. Since "mcl" stands for McLean, that's where we want to go.

Remember that NIC told us that kauai.mcl.unisys.com had an alias? It was also called "mcl.unisys.com". Looking at the above list, we see toward the bottom that mcl.unisys.com is also domain served by the computers burdvax.prc.unisys.com and kronos.nisd.cam.unisys.com. Let's connect to one of them and see what we can gather!

Whenever a server starts acting screwy like kauai was doing, I make it a habit

of using IP numbers when they are available. I'm going to connect to burdvax.prc.unisys.com through its IP address of 128.126.10.33.

```
> server 128.126.10.33
Default server: [128.126.10.33]
Address: 128.126.10.33
```

Now that we are connected, let's see the network information again, but this time let's try something different and possibly more useful. This time we will use the -h command, which happens to describe the computer type (CPU) and the operating system it runs on (OS) which will give us a better idea of what we are dealing with.

```
> ls -h mcl.unisys.com
```

| Host or domain name      | CPU           | OS       |       |       |
|--------------------------|---------------|----------|-------|-------|
| maui.mcl.Unisys.COM      | SUN-2/120     | UNIX     | 43200 |       |
| cisco.mcl.Unisys.COM     | CISCO GATEWAY | CISCO    |       | 43200 |
| kauai.mcl.Unisys.COM     | SUN-3/180     | UNIX     | 43200 |       |
| voyager.mcl.Unisys.COM   | SUN-4/330     | UNIX     | 43200 |       |
| dial.mcl.Unisys.COM      | SUN-3/260     | UNIX     | 43200 |       |
| astro.mcl.Unisys.COM     | SUN-3/60      | UNIX     | 43200 |       |
| hotrod.mcl.Unisys.COM    | Unisys 386    | SCO/UNIX |       | 43200 |
| oahu.mcl.Unisys.COM      | VAX-11/785    | UNIX     | 43200 |       |
| lanai.mcl.Unisys.COM     | SUN-3/160     | UNIX     | 43200 |       |
| mclean_is.mcl.Unisys.COM | 386           | NOVELL   |       | 43200 |

WOW! Look at all those Suns! I guess Unisys has no faith in their own computers or something! If only President Bush could see this display of a company backing their product! In fact, the only Unisys computer in this whole lot is a cheesy 386 clone which probably is some guy's desktop machine.

Once again, there is some fascinating information here. Let's run through it really quick:

Maui is a Sun 2, which is a really old RISC computer. You don't see many of these around but they still can be useful for storing stuff on. But then again, it probably is faster than a PC!

Oahu is a Vax-11 which is apparently running Ultrix. This may be where Unisys hoards all their programmers since it isn't being used for serious networking (at least, as far as we can tell).

Mclean\_is happens to be the file server for a PC network. We can't really tell from this point how many computers are on this network, but it could be possible it is used for public information trade, where secretaries or receptionists use it to confirm trade and scheduling.

Hotrod is also a 386, made by Unisys even! Oddly, it is running a copy of SCO Unix, which means it is, no doubt, a personal computer someone uses for Unix programming. If Unisys were itself a part of the government, I'd think this computer would have been a kludged bidding contract which they got stuck with because they were aiming for lowest bid and were unfortunately not very picky.

Voyager is an interesting machine, which is apparently the most modern on this network. Since it is a Sun-4 computer (probably IPX) it would be a high-speed graphics workstation. This could be the machine where many CAD applications are stored and worked on. Another possibility is that Sun 4 computers were extremely expensive when they purchased this network of Suns, and they purchased this one machine to be the file server to the other Sun 3s and the Sun 2. If you were to gain access to one of the other machines, it's possible you would have access to all of them.

Cisco is just a standard Cisco Router/Gateway box, linking that particular

network to the Internet.

Kauai is a messed up domain server, big deal. It might work on the same network as Astro and Lanai.

Dial is a Sun-3. Is there something in a name? This could be the telecommunications dial-in for the network. Maybe the same computer system has a dialout attached to it. It might even be possible that "dial" has a guest account for people logging in so that they can easily connect to other computers on the same network (probably not).

Astro and Lanai are also Sun 3 computers. It isn't quite obvious what their purpose is. Essentially, we have the impression that they were all purchased about the same time (explaining the large number of Sun-3 computers in this network) and it is quite possible they are just linked up to the Sun 4 in a file sharing network. It is also possible they are older and fundamental to the operation of Unisys's communication platform at this particular site.

There is one flaw that makes using the -h switch somewhat unreliable: Sometimes people realize you can do this and take the time to remove or never include the information about the individual machines on the network. Therefore, it is always best for you to do a "ls <domain>" and check everything out in case a computer has been removed. Using "telnet" to connect to the computer is usually a foolproof method of finding out what computer it is they are talking about.

```
> ls mcl.unisys.com
[[128.126.10.33]]
Host or domain name      Internet address
mcl.Unisys.COM           server = kauai.mcl.unisys.com      3600
kauai.mcl.unisys.com     128.126.180.2                    3600
mcl.Unisys.COM           server = burdvax.prc.unisys.com    3600
burdvax.prc.unisys.com   128.126.10.33                    3600
mcl.Unisys.COM           server = kronos.nisd.cam.unisys.com 3600
kronos.nisd.cam.unisys.com 128.170.2.8                      3600
mcl.Unisys.COM           128.126.180.2                    43200
maui.mcl.Unisys.COM      128.126.180.3                    43200
cisco.mcl.Unisys.COM     128.126.180.10                   43200
kauai.mcl.Unisys.COM     128.126.180.2                    3600
voyager.mcl.Unisys.COM   128.126.180.37                   43200
dial.mcl.Unisys.COM      128.126.180.36                   43200
LOCALHOST.mcl.Unisys.COM 127.0.0.1                        43200
astro.mcl.Unisys.COM     128.126.180.7                    43200
hotrod.mcl.Unisys.COM    128.126.180.125                  43200
oahu.mcl.Unisys.COM      128.126.180.1                    43200
lanai.mcl.Unisys.COM     128.126.180.6                    43200
mclean_is.mcl.Unisys.COM 128.126.180.9                    43200
```

Well, running down the list, it appears that there aren't any more computers important to this domain that we don't know already. LOCALHOST is just another way of saying connect to where you are, so that isn't a big deal. Hotrod being separate from the rest of the machines seems apparent since its IP address is x.x.x.125, which is quite separate from the others. Even though this doesn't have to be, it seems it is a wiring kludge -- probably for an office like I surmised.

The next step? Go ahead and hack away! This is where all those system hacks people trade on the net and all those CERT Advisories become useful. If you become good hacking a single machine (Suns, for example), using nslookup will help you identify those machines and make it easier for you to hack.

Looking for annex computers, libraries, guest machines, and other such computers also becomes easy when you use nslookup, because the names and

computer types are there for your convenience. Checking on sites by selecting interesting "special purpose" machines with nslookup first can yield good results. People have called this "netrunning," and it sounds like as good a name as any.

Of course, the other big problem when dealing with domain servers is trying to identify them. The largest list of domain servers can be found off of the Department of Defense Network Listing (usually called hosts.txt) which is available almost everywhere on the Internet through anonymous FTP. Here is a rundown on how to get the file:

```
[lycaeum][3]> ftp wuarchive.wustl.edu
```

```
220 wuarchive.wustl.edu FTP server (Version 6.24 Fri May 8 07:26:32 CDT 1992) ready.
```

```
Remote host connected.
```

```
Username (wuarchive.wustl.edu:rack): anonymous
```

```
331 Guest login ok, send your complete e-mail address as password.
```

```
Password (wuarchive.wustl.edu:anonymous):
```

```
230- This is an experimental FTP server. If your FTP client crashes or
230- hangs shortly after login please try using a dash (-) as the first
230- character of your password. This will turn off the informational
230- messages that may be confusing your FTP client.
```

```
230-
```

```
230- This system may be used 24 hours a day, 7 days a week. The local
230- time is Wed Jun 3 20:43:23 1992.
```

```
230-
```

```
230-Please read the file README
```

```
230- it was last modified on Mon Mar 2 08:29:25 1992 - 93 days ago
```

```
230-Please read the file README.NFS
```

```
230- it was last modified on Thu Feb 20 13:15:32 1992 - 104 days ago
```

```
230 Guest login ok, access restrictions apply.
```

```
ftp> get /network_info/hosts.txt
```

```
200 PORT command successful.
```

```
150 Opening ASCII mode data connection for /network_info/hosts.txt (1088429 bytes).
```

```
226 Transfer complete.
```

```
Transferred 1109255 bytes in 182.95 seconds (6063.29 bytes/sec, 5.92 KB/s).
```

```
ftp> quit
```

```
221 Goodbye.
```

Now let's convert it to a file we can use effectively: let's take out of that huge list of only the machines that are domain servers:

```
[lycaeum][4]> grep -i domain hosts.txt > domains
```

Okay, now that we have done that, let's prove that this is a way of finding a domain server without connecting to anyplace. Let's just use the grep command to search the file for a server in the mcl.unisys.com domain:

```
[lycaeum][5]> grep -i mcl.unisys.com domains
```

```
HOST : 128.126.180.2 : KAUAI.MCL.UNISYS.COM,MCL.UNISYS.COM : SUN-3/180 :
```

```
SUNOS : TCP/TELNET,TCP/FTP,TCP/SMTP,UDP/DOMAIN :
```

```
[lycaeum][6]>
```

And there you have another way. Everything we looked at is here: IP number, the name, the "alias," the computer type, the operating system, and a brief list of network protocols it supports, including the domain server attribute. However, none of the other machines on the mcl.unisys.com network were displayed. The DoD isn't a complete list of network machines, only the network machines that are vital to the functioning of the Internet (in the last year,

this list has grown from about 350K to 1.1 megabytes -- and this only reflects the "new" networks, not including the addition of new machines onto old networks; the Internet is definitely "in;" I believe it was estimated 25% growth per month!).

Obviously, this is very effective when going after university sites. It seems they have too many machines to take good care of security on. Essentially, the DoD list contains much the same information as NIC does, and is about a million times more discreet. I'm not sure if NIC is fully logged, but it does have a staff Head of Security (\*snicker\*).

Well, that will pretty much wrap it up for this file. Hope some of it was useful for you.

---

==Phrack Inc.==

Volume Four, Issue Forty, File 5 of 14

Pirates Cove

By Rambone

Welcome back to Pirates Cove. My apologies for not providing you with this column in Phrack 39. However, in this issue we take a look at some recent busts of pirate boards and the organization most to blame for it all... the Software Publishers Association. Plus we have news and information about Vision-X, game reviews, BAD Magazine, and more. Enjoy.

-----  
FBI Raids Computer Pirate; SPA Follows With Civil Lawsuit June 11, 1992  
~~~~~

BOSTON -- The Federal Bureau of Investigation raided [on June 10] "Davy Jones Locker," a computer bulletin board located in Millbury, Massachusetts, which has allegedly been illegally distributing copyrighted software programs.

The Davy Jones bulletin board was a sophisticated computer bulletin board with paying subscribers in 36 states and 11 foreign countries.

A computer bulletin board allows personal computer users to access a host computer by a modem-equipped telephone to exchange information including messages, files, and computer programs. The system operator (or sysop) is generally responsible for materials posted to the bulletin board.

For a fee of \$49 for three months or \$99 for one year, subscribers to Davy Jones Locker were given access to a special section of the bulletin board that contained copies of more than 200 copyrighted programs including popular business and entertainment packages. Subscribers could "download" or receive these programs for use on their own computers without having to pay the copyright owner anything for them.

The business programs offered were from a variety of well-known software companies, including: AutoDesk, Borland International, Broderbund, Central Point System, Clarion Software, Fifth Generation, Fox Software, IBM, Intuit, Lotus Development, Micrografx, Microsoft, Software Publishing Corp., Symantec, Ventura Software, WordPerfect and X-Tree Co. Entertainment programs included Flight Simulator by Microsoft, and Leisure Suit Larry by Sierra.

Seized in the raid on Davy Jones Locker were computers, telecommunications equipment, as well as financial and other records.

"The SPA applauds the FBI's action today," said Ilene Rosenthal, director of

litigation for the Software Publishers Association (SPA). "This is one of the first instances that we are aware of where the FBI has shut down a pirate bulletin board for distributing copyrighted software. It clearly demonstrates a trend that the government is recognizing the seriousness of software copyright violation. It is also significant that this week the Senate passed S.893, a bill that would make the illegal distribution of copyrighted software a felony."

For the past four months, the Software Publishers Association has been investigating the Davy Jones Locker bulletin board and had downloaded business and entertainment programs from the board. The programs obtained from Davy Jones Locker were then cross-checked against the original copyrighted materials. In all cases, they were found to be identical.

Subscribers to Davy Jones Locker not only downloaded copyrighted software, but were also encouraged to contribute additional copyrighted programs to the bulletin board.

The system operator limited subscribers to four hours on the bulletin board each day. He also limited the amount of software a subscriber could download to his or her own computer each day. Those who "uploaded" or transmitted new copyrighted software to the bulletin board for further illegal distribution were rewarded with credits good for additional on-line time or for additional software.

"Imagine a video store that charges you a membership fee and then lets you make illegal duplicates of copyrighted movies onto blank video tapes," explains Ilene Rosenthal, SPA director of litigation. "But it limits the number of movies you can copy unless you bring in new inventory -- copies of new movies not already on the shelves. That was the deal at Davy Jones Locker."

Davy Jones Locker was an international concern with paid subscribers in the United States and 11 foreign countries including Australia, Canada, Croatia, France, Germany, Iraq, Israel, Netherlands, Spain, Sweden and the United Kingdom.

Whether it's copied from a program purchased at a neighborhood computer store or downloaded from a bulletin board thousands of miles away, pirated software adds to the cost of computing. According to SPA, software pirates throughout the world steal between \$10 and \$12 billion of copyrighted software each year.

"Many people may not realize that software prices are higher, in part, to make up for losses to the pirates," says Ken Wasch, executive director of the SPA. "Pirate bulletin boards not only distribute business software, but also hurt the computer game publishers by distributing so many of their programs illegally. In addition they ruin the reputation of the hundreds of legitimate bulletin boards which serve an important function to computer users."

The Software Publishers Association is the principal trade association of the personal computer software industry. Its 900 members represent the leading publishers in the business, consumer and education software markets. The SPA has offices in Washington, D.C., and Paris La Defense, France.

CONTACT: Software Publishers Association, Washington, D.C.
Terri Childs or Ilene Rosenthal, 202/452-1600

PC Bulletin Board Hit by FBI Raid

June 14, 1992

~~~~~

By Josh Hyatt (Boston Globe) (Chicago Tribune, Section 7, Page 3)

BOSTON -- In one of the first reported crackdowns of its kind, six FBI agents



raided a computer bulletin board based in a Millbury, Massachusetts, home last week. Authorities said the bulletin board's operator had been illegally distributing copyrighted software.

Executing a criminal search warrant, the agents seized several computers, six modems and a program called PC Board, which was used to run the bulletin board. Authorities also seized documents that listed users of the service.

No arrests were made, according to the Software Publisher's Association, a trade group that brought the case to the FBI's attention. The association estimates that, as of March, the bulletin board had distributed \$675,000 worth of copyrighted software; software pirates, it says, annually steal as much as \$12 billion this way.

The FBI will not comment on the case except to confirm that a raid had taken place and that the investigation is continuing. The alleged operator of the bulletin board, Richard Kenadek, could not be reached for comment.

Around the same time as the raid, the software association filed a civil lawsuit against Kenadek, charging him with violating copyright laws. Ilene Rosenthal, the group's director of litigation, said that "the man had incriminated himself" through various computerized messages.

"There's plenty of evidence to show that he was very aware of everything on his bulletin board," she said.

Bulletin boards let personal computer users access a host computer via modems. Typically, participants exchange information regarding everything from computer programs to tropical fish. They may also, for example, obtain upgrades of computer programs.

The association said its own four-month investigation revealed that this bulletin board, called Davy Jones Locker, contained copies of more than 200 copyrighted programs.

Rosenthal said users also were encouraged to contribute copyrighted software programs for others to download or copy.

According to Rosenthal, subscribers paid a fee, \$49 for three months or \$99 for one year. She said Davy Jones Locker had nearly 400 paying subscribers in 36 states and 11 foreign countries.

---

Cracking Down On Computer Counterfeiters

July 1992

~~~~~

By B.A. Nilsson (PC-Computing Magazine) (Page 188)

Popular bonding rituals usually aren't criminal. Admire a friend's new car, and you're likely to swap a few stories and a can of STP. You may be invited to take the car for a spin. You can pass recipes back and forth or lend your copy of the latest best-seller to a fellow fan.

Sharing computer programs is another common practice among friends. It's great to help someone who's daunted by the challenge of learning to use a new machine, and sometimes that includes a gift of some of your favorite software. "Here. Why don't you get started with WordPerfect?" And, later, inevitably, "The Norton Utilities will get that file back for you."

Copying a set of disks is so simple and such a private action that you'd hardly think it's also illegal. The legality part is easy to overlook. The copyright notice is a complicated critter, often printed on the seal of the software package that is torn away as you dig for those floppy disks. You may not even be the one who ripped the original package open (in which case, you're yet

another who's ripped the program off).

But whether or not you're aware of it, unless you either broke the shrink-wrap or received the package with all disks, documentation, and licensing information intact, you're breaking the law. The good news is that if you're an individual with pirated software on your home computer, you probably won't get caught. But if you're a boss with an angry employee, the Software Publishers Association (SPA) may get tipped off. When the SPA comes to call on your business, it's with U.S. marshals and lots of official paperwork. And the association has an annoyingly good history of winning its copyright-infringement cases.

Perspectives on Piracy

"Computers give us a kind of technical sophistication that never used to exist," says Ken Wasch, the voluble head of the SPA. "In the old days, if you wanted to make your own copy of something like a pencil, you'd need a complicated manufacturing center. But the very fact that you can run a computer program means that you can make a flawless copy of it. This is the only industry in the world that empowers every customer to be a manufacturing subsidiary."

The regulations are spelled out again and again in the software manuals: You're allowed to make one or two copies of the program for backup purposes. Other rules vary slightly from company to company. Some license agreements demand that the software package be used only with a single machine; others, most notably Borland's, let you use the program on as many computers as you wish, provided no two copies of the program are run concurrently, just as a book can be read by only one person at a time.

"If all software developers took the same approach as Borland International, people wouldn't steal so much," says avowed pirate Ed Teach.

(Note: The names and locations of all interviewed pirates have been changed.)

"Borland gives you that book license. Of course, they'll drive you insane with upgrades. They wholesale the software, then make their money on all the subsequent releases."

Teach is the systems administrator for a residential health-care company in the Southeast. "I believe in piracy," he says. "I like to borrow something to play with it. If I like it, I'll buy it."

He dismisses demos and limited versions of programs as inadequate for the testing he prefers; similarly, he considers the typical 30-day return agreement too restrictive. "It's not a realistic time period for an evaluation," Teach says. "I just got a copy of FormTool Pro, and it's a powerful program with a very steep learning curve. I can't devote myself to it and learn what I'd need to know in 30 days."

Teach has spent six years recommending and configuring programs for his company. He does not fit the image of a lawbreaker, and he believes that what he does is morally justified. "I buy the software eventually. My company bought licenses to use WordPerfect 5.1 after starting with a pirated copy of the program. Everything on the company machines is legit."

Copying wasn't always so easy. Old-timers remember the copy-protection schemes that pervaded the computer industry, requiring key disks or special initialization procedures. But users unanimously demanded an end to it, and when Lotus, the last significant holdout, gave in, that era was over. Today you find protection only on games and niche-market programs.

How much has the end of copy protection cost software companies? It's

impossible to figure accurately. In August 1991, the indefatigable Software Publishers Association released figures on corporate-use losses that suggest both a staggering financial loss and a possible decline in piracy. In 1987, 1.31 DOS-based software programs were sold for every office computer. The expected proportion is three packages per computer, meaning that more than half of the programs in use were probably pirated. In 1990, the number of legitimate packages jumped to 1.78. But prices have gone up, too, so that the dollar losses haven't changed much: The 1987 liability was \$2.3 billion, and the number rose to \$2.4 billion in 1990.

The numbers for private-use piracy, on the other hand, can't be calculated. If all the computer users who have never pirated software got together, they wouldn't need a very large hall. Wasch concedes that it's difficult to actually catch and prosecute the individual pirate. "Nobody is actually doing time for piracy," he says, citing the exception of a retailer who was caught running what amounted to a pirated-software storefront.

The Software Police

Although the SPA is targeting home abuse in a current study, Wasch believes that the greatest financial losses are due to corporate piracy. And corporate pirates are easier to apprehend because an angry employee is frequently willing to turn in the boss. "We get about 20 calls a day," says Wasch, who set up a special number (800-388-7478) for reporting piracy. "Ninety percent of the calls we follow up on come from disgruntled employees."

It's the kind of visit most of us have only seen in the movies, and it's usually an unexpected one. A receptionist with one targeted company was so shocked by the arrival of the SPA posse that she asked if it was a "Candid Camera" stunt.

Founded in 1984 as an educational and promotional group, the SPA evolved into a software police force five years ago as more and more software vendors joined. Now almost 800 are in the fold. The SPA began to woo whistle-blowers in earnest about two years ago, after a tip led to the successful bust of a large corporation in the Midwest.

"Business is too good," Wasch says. "We're doing far more lawsuits and far more audits than ever before, and the numbers are continuing to grow."

If your corporation is busted by the SPA, hope that it's done by mail. "What happens then is that we write the CEO a letter explaining that we want to do an audit," Wasch says. "If we find illegal software, the company pays twice: Once for the pirated copy, once for a new one."

"That's a lot better for the company. The fine is much lower, and they don't face the adverse publicity that results from a lawsuit. Still, 60 percent of them promise they won't destroy software before they report it, and then they go and do it anyway."

That was the case with a recent SPA visit to a medium-size defense contractor in Washington, DC. "They agreed to an audit, and then they tried to wipe pirated programs off all the hard disks," Wasch says. "But we knew. Why do they think we called them in the first place? Someone on the inside was talking. I couldn't believe they'd sit there and lie to us about it, we had them over a barrel!"

The increasingly ominous specter of the SPA breaking down the door is making more companies go legit, but some continue to spout excuses. "I don't want to break the law, but I also don't want to go out of business," says Howell Davis, the CEO of an accounting firm in a New England capital. "We can't afford to work without computers, but I can't pay the high price of registering every copy of every program we use. I had to borrow a lot of money to get this

business off the ground, and I think of this as just another form of borrowing. It's another loan I'll repay when I can afford to."

Some corporate pirates operate with a sense of entitlement.

"Nobody's going to catch us," says Charles Vane, the managing director of a nonprofit theater company in the Northwest, "and nobody should even be trying to. We're on the brink of bankruptcy. Companies should be giving us software packages as a gesture of support for the arts." He admits that almost all of the software his theater uses is pirated. "We have some nice programs, including an accounting package developed for Ernst & Young that we swiped and a copy of SuperCalc with a bunch of extra modules. And WordPerfect, of course," Vane says.

Where do the packages originate? "Our board members get them for us," Vane says. "Of course, that means we can't be choosy. We have to wait until a particular program comes our way. And what they like to give us the most are games. We have a kazillion games."

Games and piracy are natural partners. Games themselves encourage piracy. Unlike business-oriented programs, they engender intense, short-lived relationships. Or as pirate-BBS operator John Rackam puts it, "Games get boring. That's why you see so many of them on the pirate boards."

Online Piracy

Rackam runs a BBS straight out of "The Man from U.N.C.L.E." It looks like any other medium-size board in the country, with a standard collection of shareware and message bases. Gain special access which only takes \$50 and a friend's recommendation and you pass through the secret door into a 600MB collection of the latest applications, including 10 zipped files of the complete dBASE IV, 11 of AutoCAD, and 6 of MS-DOS 5.0.

"Most of the people who use my board are collectors," he says. "They have to have the latest copy of everything." Rackam isn't deterred by the threat of getting caught. "I don't think it's going to happen to me. I'm not doing anything that's really terrible. I mean, I'm not hacking up bodies or anything. I make no money off this. The fee is just for keeping up my equipment. I consider myself a librarian."

Novell takes a dim view of that attitude, as evidenced by an August 1991 raid of two California bulletin board systems accused of distributing Novell NetWare files. Such systems are another target the SPA would like to hit, and Wasch is looking for FBI cooperation.

That makes the Humble Guys Network ripe for the picking. Study the high-resolution GIF file of these buccaneers, and you see a collection of ordinary-looking folks who happen to traffic in pirated game software. The founder, a hacker who called himself Candy Man, has since skipped the country; now The Slave Lord, a student at a southern college, is at the helm.

"The whole point of the network is to get games before the stores have them," says Bill Kidd, a computer consultant in Manhattan. "This is like proof of manhood, how fast you can get them." Kidd professes little personal involvement with piracy, but he knows where the bodies are buried.

"First there are the suppliers who can get a program from a manufacturer well before it's released," Kidd says. "Often the supplier works for the manufacturer. The game goes to the head person, who delivers it to the crackers. They're the ones who remove the copy protection. From there it goes to the couriers, and each has a list of pirate BBS's. The program then makes it all over the country in minutes."

Speed is an obsession. These pirates are armed with 9,600-bit-per-second modems and a must-have-it-now mentality. "The week before MS-DOS 5.0 hit the stores," says Kidd, "most of the pirate boards had already deleted it because they had been offering beta versions six months before."

As far as revenues are concerned, pirate bulletin boards may be more of a nuisance than a threat. "Those people are never really going to buy that software," says John Richards, a product manager with Lotus. "Nominally, it's bad, but it's not as if they're buying one copy of 1-2-3 to put on the office workstation for ten users."

Pirates at Home

While an office environment allows for regular, rigorous audits, the home user gets away with pirating software. Peer under the hoods of a few hard disks, and you're liable to find something illicit.

"It can happen innocently enough," says Symantec's Rod Turner. As general manager of the Peter Norton Group, Turner has the distinction of overseeing one of the most frequently pirated pieces of software: The Norton Utilities. "Someone puts a copy of the software on someone else's machine to test it out and leaves it behind. The other user assumes it's there legitimately," Turner says.

"Often, someone gets software from a friend who got it at work," says Tony Geer, service manager at Computer Directions, a retail outlet in Albany, New York. Geer looks at hundreds of user-configured hard disks every month. "Someone buys a machine from us, then turns around and calls us to say that he's got all this software now, could we tell him how to run it," Geer says. "What am I supposed to do? The customer wants me to spend hours on the phone teaching him or he gets mad. When I tell him he has to buy the program, too, he gets annoyed."

Geer also receives a huge number of requests for pirated software. "A lot of users think that we can load up their hard disks with programs, even though they know they ought to be paying for them and just want to duck the fee."

A few requests come from the truly naive, Geer says. "I'll get a call for software support and I'll ask, 'What did the manual say?' I didn't get a manual," the person tells me. "A friend gave this to me." And then I have to explain that software isn't free."

High software prices are a common user complaint. Former WordPerfect executive vice president W.E."Pete" Peterson thinks the \$495 list price of WordPerfect's best-selling word processing program is justified, however. "WordPerfect sells about 150,000 copies a month at that price, so quite a few users think the price is justified, too," says Peterson. "A computer costs anywhere from a few hundred to a few thousand dollars. Without the software, the computer is worthless. WordPerfect goes to a lot of work to write and support the software."

The latter includes a costly policy of toll-free phone support, handled by operators who would just as soon not ask for a registration number. It's an expensive way of showing trust, but it has paid off in excellent public relations.

"We try to sympathize with people," says Jeff Clark, public relations director at XyQuest, the company that publishes XyWrite, a word processing program popular among journalists. "We sell replacement manuals as a service to registered users, but there's a call at least once a week from someone who's obviously trying to get manuals to go with a pirated copy."

The challenge then is to educate the caller, who may not even know that a law

has been broken. "All we ask of a registered user is to run the program on one machine at a time," Clark explains. "If you're using it at work, yes, you can use it at home. But don't buy one copy to use in an office of eight people."

"A lot of people seem to think copying disks is OK because it's easy to do," says Turner, who is also chairman of the SPA's companion organization, the Business Software Alliance, which fights international piracy. "Then they call our tech line, and we're in the delicate position of telling them they're using a product illegally."

Microsoft is even more benevolent. "We like to know where the pirated copy originated," says Bill Pope, associate general counsel for the company. "It's not always possible to learn over the phone who's pirating something, because we don't require that registration cards be returned. But if we do identify a pirated copy, we'll help the user get it legally, and we may even supply a free copy of the program if we can learn where it came from."

A highly publicized amnesty program was launched by the XTree Company in July of 1982. For \$20, anyone with a pirated copy of an XTree program was allowed to buy a license for the entry-level version of the program, thus getting access to the upgrade path. Response was enthusiastic during the 90-day period, but the offer won't be repeated. "You can't offer amnesty over and over," says Michael Cahlin, who markets the XTree products. "You lose the respect of dealers and users who paid full price for it."

Turner is more blunt about it. "Amnesty encourages piracy. I don't think it's been successful."

While the SPA will continue to make headlines with Untouchables-style raids of corporate offices, Wasch also acknowledges that education is the key to fighting piracy. A 12-minute, SPA-produced videotape entitled It's Just Not Worth the Risk spells out the message as a congenial corporate manager is made wise to the ways of the company pirate.

"That tape has been a huge success," says Wasch. "American Express bought 300 copies, and Kimberly-Clark just ordered 100. We've distributed about 10,000 of them so far."

A self-audit kit, also available from the SPA, includes a program that determines what software is in use on your PC as well as sample corporate memos and employee agreement forms to promote piracy awareness.

Seeing the Light

Fear of being caught keeps many people honest, but some pirates will wait until they're forced to walk the plank before giving up.

John Rackam says his BBS users are innocent. "They can't afford the software, and they shouldn't have to pay," he says. "They're downloaders. They un-ARC it and say, This is nice!' Then they never use it again."

Charles Vane believes that software companies should give nonprofit organizations like his theater a break. "If they give us packages, we'll give them publicity. We'll print it in the program, we'll post it in the lobby. It's an upscale crowd that comes through here. We just don't have the luxury of money. I bought one program, ReportWriter, because it was cheap and good."

For casual users, piracy may simply be a phase. "I own 90 percent of the programs I use," says systems administrator Ed Teach. "That's a big reverse from about four years ago, when 90 percent of them were bootlegs."

And there's always the problem of well-meaning friends. Henry Every, a journalist at a Florida newspaper, received pirated programs from friends when

he bought his first computer five years ago.

"I had all these programs and no idea how to use them," Every says. "Fortunately, the bookstore had guides that were even better than the manuals, and I became something of a power user. Then I became the guy that a friend of a friend would call for help with his machine. Next thing I know, I'm the one giving away pirate copies.

"But I won't do it anymore. I'm sick and tired of getting those calls all hours of the day and night asking me how to use the damn things."

No Excuses Accepted

"When I'm sitting across the table from them and they're looking really dog-faced, when I can see the whites of their eyes, it's hard to pull the trigger," says Ken Wasch, the head of the Software Publishers Association. "Nevertheless," he says, "I pull the trigger."

Wasch is not a tender man when it comes to dealing with software pirates. He has no patience for the typical excuses given by those who copy and use unlicensed software, and he offers the following responses to the common complaints he hears from the outlaws:

* The price is too high.

"Hey I don't own a Mercedes Benz. Why? The price is too high. If you can't afford it, don't use it."

* It's better to test the real thing than a crippled or demo version.

"The demos are normally very good. They limit the number of records, or they don't save to the disk, or something. It's enough."

* I'll pay for it later.

"I doubt it."

* I won't get caught.

Wasch laughs. When he does so, you can't help but hope that he's laughing with you, not at you. "Sooner or later . . ."

How Microsoft Foiled the Pirates

Imitation is flattering only when you don't lose money over it. Many software packages are copied by clever pirates who duplicate disks, manuals, even packaging. Microsoft has been hit often enough by counterfeiters that recent software releases, including the Windows 3.1 and MS-DOS 5.0 upgrade packages, were specially designed to be bootleg-proof.

"Every component part was carefully designed or hand-picked for that reason," says Kristi Bankhead, who works with Microsoft's general counsel on piracy issues. "To the user, it should just look like an attractive box, but it allows us to tell at once if it's legitimate or not."

That strategy paid off in March when FBI agents raided a quartet of Silicon Valley companies that were pulling in up to \$600,000 a month distributing bogus copies of MS-DOS and Windows.

Key components of the official, bootleg-proof box designs are colorful artwork and the use of holograms. On the MS-DOS 5.0 upgrade box, a silver circle on

the side offers an iridescent image of the logo. A second hologram, a small rectangle on the side of the program manual shows through an expensive die-cut hole on the other side of the box. The interlocked letters D-O-S are printed in a four-color process that results in complicated mixtures that defy reproduction. Even the way the box is folded and the flaps are glued and tucked is unique, it's not a common style, and counterfeiters must either spend time and money to copy it or risk quick discovery.

Even as the DOS upgrade package was being readied for market last year, police detectives uncovered a Los Angeles based pirate ring that was already working on full-scale knockoffs of it. "We got them while they were in the process of completing the DOS 5.0 artwork," said Bankhead, "but we could tell how bad it would look. For instance, they were using a piece of foil for the hologram, and it had no three-dimensional image."

Top 10 Pirate BBS Downloads

1. Windows 3.1 (Microsoft)
2. Excel 4.0 (Microsoft)
3. Norton Utilities 6.0 (Symantec)
4. WordPerfect for Windows 5.1 (WordPerfect)
5. Stacker 2.0 (Stac Electronics)
6. AutoMap (AutoMap)
7. Procomm Plus 2.0 (Datastorm Technologies)
8. PC Tools Deluxe 7.1 (Central Point Software)
9. QEMM-386 6.0 (Quarterdeck Office Systems)
10. WordPerfect 5.1 (WordPerfect)

It looks familiar. It's very close to a recent Top 10 list of legitimate programs. That's not surprising, since popular programs are also the most-often swiped.

The list above was compiled from a survey of pirate BBS's, with help from John Rackam. He explains that activity is so brisk the profile changes from week to week, with games being the most transitory items (which is why they're impossible to track). Because non-disclosure doesn't exist in the pirate world and exchanging beta copies of software is a pirate tradition, Windows 3.1 won a strong position even before its official release. By the way, there's only a cursory interest in OS/2 2.0, which is ominous news for IBM if pirate interest is any barometer of sales.

Software Publishers Association: Nazis or Software Police?

~~~~~

##### An Investigative Report by Rambone

The Software Publishers Association (SPA) is the principal trade association of the microcomputer software industry. Founded in 1984 by 25 firms, the SPA now has more than 750 members, which include major businesses, consumer and education software companies, and smaller firms with annual revenues of less than \$1 million. The SPA is committed to promoting the industry and protecting the interests of its membership.

The SPA has two membership categories: Full and Associate. Software firms that produce, release, develop or license microcomputer software and are principally responsible for the marketing and sales of that software are eligible to apply for full membership status. Firms that develop software, but do not publish are also eligible. Associate membership is open to firms that do not publish software, but provide services to software companies. These members include vendors, consultants, market research firms, distributors and hardware manufacturers.

#### Lobbying



The SPA provides industry representation before the U.S. Congress and the executive branch of government and keeps members up-to-date on events in Washington, D.C., that effect them. The fight against software piracy is among its top priorities. The SPA is the industry's primary defense against software copyright violators both in the United States and abroad. Litigation and an ongoing advertising campaign are ways in which the SPA strives to protect the copyrights of its members.

This is the impression that the SPA wants to give the general public, and for the most part, I have no problem with it. During a lengthy conversation with Terri Childs of SPA, I was informed of several things. The association's main source of information is from their hot-line and the calls are usually from disgruntled employees just waiting to get back at their former bosses. An example of this is a company that had bought one copy of Microsoft Works, and with over 100 employees, they all seemed to be using the same copy. One particular secretary had gotten fired, for what reason I do not know, so she called the SPA police and spilled her beans. Once that happened the SPA got the balls rolling by instructing the Federal Marshals to get a warrant and storm the building like they own the place. With a nifty little program they have that searches the machines for illegal copies of the software, they came up with the programs not registered to that machine. \*Bam!\*, caught like a dead rat in a cage. The SPA declined to comment on what has happened to that company since the raid, but they did say the company would be fined "X" amount of dollars for each illegal copy.

Ms. Childs was very helpful though, she explained the idea behind the association, and what they stand for. I was very impressed with what she had to say. However, when I brought up the case concerning the Davy Jones Locker bust. She told me she was not qualified to answer questions involving that case and directed me to Elaine Rosenthat. So a few hours later I called her, and for a few brief moments she seemed to be quite helpful, but then decided to put me on a speaker phone with the founder of the "Association," Ken Wasch.

>From the start I knew I would not get a straight answer out of him. The first thing I asked him is if someone not in SPA obtained an account to get onto DJL, and then gave it to them with log captures from the BBS. He would not give me a straight answer, just that SPA was able to obtain the information. I then asked him what actions are being taken toward DJL and received another run around.

Finally, I asked what type of fine would be likely to be handed down in this case. He refused to give me an answer.

But I did learn one very interesting little fact from all of this. The money obtained by this incident and others like it do not go to the software companies who the SPA claims to be protecting. Instead it goes right into the coffers of the SPA itself! I guess they like to try those Mercedes.

And here is a few more interesting little tidbits about the SPA. Not only do they fine the companies for having illegal software and then pocket the money, but the annual charge for membership on the software companies can range anywhere from \$700 to \$100,000! It seems to me that it is much more profitable to eradicate piracy than to participate in doing it.

For those of you currently operating or considering operating a pirate bulletin board, I would suggest that you not charge your users for access. Even if you claim that the money is only for hardware upgrades, in the long run, if you get busted, the money you collected will be evidence that suggests you were selling copyrighted software for financial gain.

~~~~~

By Rambone

There seems to be a fallacy in the pirate world that all BBS software is untouchable. However, about a month ago a few people associated with the Oblivion team took apart .93 (a version number of Vision-X) and found backdoors. The unfortunate problem with this is that the V-X team put those backdoors in so they could trace down which Beta site was giving out Beta copies. Well, they found the backdoors and called up several boards and used them.

1. The story from the people who hacked the boards is this, one of the two involved was irate because he wrote a registration for .93 so anyone could run it, whether they paid for the software or not. When the V-X team found out about it, they blacklisted him from being able to logon into any V-X system. This was done hard-coded, so no sysop could let him in with that handle. Anyway, the story is they got into several of the BBSes, and even dropped to DOS to look around, but did not have any intentions on destroying data. Basically, they wanted to expose the weaknesses of the software. The problem started when they posted the backdoors on a national net, which means that now any lamer could use this backdoor for their own purpose. According to the Oblivion guys, they did not destroy the data, but some of the lamers that saw the backdoors on the net did. They regret posting the backdoors. They didn't realize that there are some people who are malicious enough to destroy data.
2. The Vision-X team are positive that the people who did take down the BBSes were the Oblivion team, some say they even admitted to doing it. There is a major paradox in these stories, and at this point it doesn't look like anyone will ever be able to get the entire truth about what had happened.

Backdoors have never been a good idea, even if the authors are positive they will never be found. The recent barrage of system crashing prove that the backdoors will indeed be found eventually. On the flip side of the coin, even if backdoors in BBS software are found, they should be left alone to be used for their original intent. Most authors who put the backdoors into the systems do it to protect their investment and hardwork. Most BBS programmers these days work on the software for the benefit of the modem community, and expect a little money in return for their hard work. It is wrong for sysops to use it without permission. You guys need to stop being cheap asses, and support a software you want support from. What is the point of running a cracked piece of software since you cannot get support from the authors and not get the net they are involved in. The nominal amount of money involved is a good investment in the future of your bbs.

"BAD" Magazine Lives Up To Its Name

~~~~~

By Rambone

I had never read Bad Magazine until recently. Everywhere discussion about it had erupted, all I saw were comments that it was a waste of harddrive space. However, when Bad's eighth issue surfaced, I heard that there were a few disparaging remarks made about me and a spew of other loose information.

So I went ahead and took a look at it, and what I found was one lie after another. I have never seen a magazine so full of shit as BAD #8. Apparently they seemed to think I mentioned them in Phrack magazine, "Bad Magazine got their first mention in the magazine Phrack." The funny thing is, the only mention of BAD Magazine ever to appear in Phrack before now was a remark attributed to The Grim Reaper that I reprinted.

I could care less about a pathetically lame magazine such as BAD and I never

mentioned them and never intended on mentioning them until they raised the issue by taking a pot shot at me.

"The Boys of Phrack however did not do their homework when mentioning this though." This is a quote from BAD regarding comments made about Vision-X, which the article was not even about. What they don't know is that I personally called The Grim Reaper and talked to him before putting anything in Phrack about his bust. That's what the point of the article was about, not about some lame magazine named BAD and what they did. They deemed me responsible for not backing up my facts, when in fact, I backed them all up. Grim Reaper's comments about Vision-X was not my concern, it was his bust for credit card abuse that I was interested in learning about. The remarks concerning BAD were made by TGR, so it would appear that "the boys at BAD" did not do THEIR homework!

"Rambone obviously does not get much exposure to the pirate world." Yet another ridiculous and unsubstantiated remark.. You boys definitely did not do your homework, you better start asking around a little more before making irresponsible accusations. The last words I will say about this is when people put a magazine together, they should try and find writers who will investigate facts instead of fabricating them. If they actually read my article, they would have known that I did not say a word about their magazine, but rather quoted The Grim Reaper. With writers such as those at BAD, I would not suggest anyone waste their time reading it, unless you are into tabloids like National Inquirer, but then at least some of their articles have a basis in fact.

---

#### Games

~~~~~

Game Of The Month : Links 386 Pro

: -*~ Release Information ~*-	:	-*~ Game Information ~*-	:
: Cracker	None	: Publisher	MICROPLAY
: Protection Type	None	: Graphics	SVGA Minimum
: Supplier	The Witch King	: Sound	All
: Date of Release	07/13/92	: Rating [1-10]	10

Sorry guys for reprinting the information file, but I got lazy <g>.

With the advent of the Super VGA Monitors, and the prices becoming more resonable, companies are starting to come out with special games to take advantage of SVGA mode. Most of these games still will play in VGA mode so don't fret.

One of the latest to date, and probably the best is Links 386 Pro, which the title indicates, at least a 386 is required. The installation of the game is one of the most impressive I have ever seen, they cover every aspect of your hardware to take full advantage of it. One of the harder things to swallow is that you must have at least 512k of memory on your VGA card, and it must comply by the VESA standard. If it does, the instalation is smart enough to try and find one for you.

The game it's self is a major improvement over it's predecessor, Links. The graphics are much improved, which was a feat in itself, and many more options and bugs had been taken care of. The company also listened to its customers and added many new features that were suggested.

When first loading up 386 pro, you are greated by a backview of a course instead of the boring blank screen in the original. From there, you can just about set up anything under the moon, from your club selection, to fairway conditions, and techture of the greens. You can even select the wind

conditions. One of the most impressive features besides the outstanding graphics is the option to have multiple windows open while playing the game.

Let's say you are at the first hole, about to drive one down the fairway, if you can make it there, you can also have another window up overlooking the fairway waiting to see where the ball is going to drop. This is just one of many windows you can open, four at the most. After playing it for quite sometime, I would only suggest one or two though.

If you are contiplating buying a game to take advantage of your SVGA monitor, look no further than Links 386 Pro. It's the wave of the future, and it's here now.

No Longer Buy Console, Copy Them

~~~~~

Special Thanks Snow Dog

The following is an information excerpt on the GameDoctor. Basically, you can buy a machine called the GameDoctor hook it up to your PC and copy the rom data over to your HD in a compresed format. From there, you can send it over the nets, through the modem, or bring it to a friend's house. You hook the GameDoctor up to your PC, hook your console game to the GameDoctor and transfer the compressed data file onto a blank cartridge. Wow, instant Super Mario brothers. There will be a more in-depth review of this machine in the next issue, for now, here's a little taste.

Snow Dog writes:

The machines are external SCSI interface machines, about the size of a super NES but wider, and fitted for japanese (super famicom) cartridges. They are made by electronics nippon, known as NEC in the States, and friend has one that works on both his Amiga 2000 and his 486-33 (SCSI is universal).

They include five disks of Famicom OS, which you can use on a logical harddisk partition of around six megs since SNES games are measured in MegaBITS and will NEVER get bigger than four meg or so, but the OS needs room. Controllers et. al. plug into the copier units.

If you take an SNES or Genesis cart out of their shell and put it in a SF shell, you can copy them too. It works like teledisk, and Altered Reality in (303)443-1524 has console gamefile support. All you do is download it and use your own console copier to put it on a cart, or at your option if it is a SNES or Famico game, play it off your OS. Genesis games don't work in the SF OS so you need to copy them to cartridge.

There are Japanese copiers specifically for Mega Drive (Genesis) that will do the same except that the OS is Sega-specific and you'll need to copy SNES games. There is also a NEC PC Engine (turbo graphics and super graphics) copier because they made the bloody system, but it is proprietary and it will only work with the turbo format.

I have never seen or worked with an internal model, but there is an internal 5.25" full height model in the NEC catalog...I ordered the catalog after I saw an advertisement for it in the back of Electronic Gaming Monthly, and a rather rich friend of mine went and bought the system. He also bought the \$130 Japanese Street fighter II and copied it for all of us. How nice of him! Of course we had to buy the cartridges and pay him \$20, but he made a \$100 profit. Good deal for him!

---

Okay, that is it for now. Greetings go out to Cool Hand, Ford Perfect, Lestat, RifleMan, The CrackSmith, AfterMath, both Night Rangers, Kim Clancy, Bar

Manager, Butcher, Venom, and all the couriers who help make things happen.  
Special thanks to Tempus for one kick ass ansi!  
Until next time, keep playing.

==Phrack Inc.==

Volume Four, Issue Forty, File 6 of 14

```
*****
*
*                               Cellular Telephony
*                               Part II
*
*                               by
*                               Brian Oblivion
*
* Courtesy of:      Restricted-Data-Transmissions (RDT)
*                  "Truth Is Cheap, But Information Costs."
*
*
*
*                               June 1, 1992
*****
```

In Phrack 38, I discussed the history of cellular telephony, monitoring techniques, and a brief description of its predecessors. In Part II, I'll describe the call processing sequences for land-originated and mobile-originated calls, as well as the signaling formats for these processes. I apologize for the bulk of information, but I feel it is important for anyone who is interested in how the network communicates. Please realize that there was very little I could add to such a cut and dried topic, and that most is taken verbatim from Industry standards, with comments and addendum salt and peppered throughout.

## Call-Processing Sequences

### Call-Processing Sequence for Land-Originated Calls

| MTSO                                                      | Cell Site | Mobile Unit                                            |
|-----------------------------------------------------------|-----------|--------------------------------------------------------|
|                                                           | 1 --      | Transmits setup channel data on paging channel         |
|                                                           | 2 --      | Scans and locks on paging channel                      |
| Receives incoming call --- 3<br>and performs translations |           |                                                        |
| Sends paging message ----- 4<br>to cell site              |           |                                                        |
|                                                           | 5 --      | Reformats paging message                               |
|                                                           | 6 --      | Sends paging message to mobile unit via paging channel |
|                                                           | 7 --      | Detects Page                                           |
|                                                           | 8 --      | Scans and locks on access channel                      |
|                                                           | 9 --      | Seizes setup channel                                   |
|                                                           | 10 --     | Acquires sync                                          |
|                                                           | 11 --     | Sends service request                                  |

|                           |                                                                             |
|---------------------------|-----------------------------------------------------------------------------|
|                           | 12 -- Reformats service request                                             |
|                           | 13 -- Performs directional locate                                           |
|                           | 14 -- Sends service request to MTSO                                         |
| Selects voice channel --- | 15                                                                          |
| Sends tx-on command to -- | 16                                                                          |
| cell site                 |                                                                             |
|                           | 17 -- Reformats channel designation message                                 |
|                           | 18 -- Sends channel designation message to mobile unit via access channel   |
|                           | 19 -----Tunes to voice channel                                              |
|                           | 20 -----Transponds SAT                                                      |
|                           | 21 -- Detects SAT                                                           |
|                           | 22 -- Puts on-hook on trunk                                                 |
| Detects off-hook -----    | 23                                                                          |
| Sends alert order -----   | 24                                                                          |
|                           | 25 -- Reformats alert order                                                 |
|                           | 26 -- Sends alert order to mobile unit via blank-and-burst on voice channel |
|                           | 27 -----Alerts User                                                         |
|                           | 28 -----Sends 10-kHz tone                                                   |
|                           | 29 -- Detects 10-kHz tone                                                   |
|                           | 30 -- Puts on-hook on trunk                                                 |
| Detects on-hook -----     | 31                                                                          |
| Provides audible ring --- | 32                                                                          |
|                           | 33 -- Detects absence of 10-kHz tone                                        |
|                           | 34 -- Puts off-hook on trunk                                                |
| Detects off-hook -----    | 35                                                                          |
| Removes audible ring ---- | 36                                                                          |
| and completes connection  |                                                                             |

Time

#### Call-Processing Sequence for Mobile-Originated Calls

| MTSO                       | Cell Site                                                                 | Mobile Unit                       |
|----------------------------|---------------------------------------------------------------------------|-----------------------------------|
| -----                      | -----                                                                     | -----                             |
|                            | 1 -- Transmits setup channel data on paging channel                       |                                   |
|                            | 2 -----                                                                   | Scans and locks-on paging channel |
|                            | 3 -----                                                                   | User initiates call               |
|                            | 4 -----                                                                   | Scans and locks-on access channel |
|                            | 5 -----                                                                   | Seizes setup channel              |
|                            | 6 -----                                                                   | Acquires sync                     |
|                            | 7 -----                                                                   | Sends service request             |
|                            | 8 -- Reformats service request                                            |                                   |
|                            | 9 -- Performs directional Locate                                          |                                   |
|                            | 10 -- Sends service request to MTSO                                       |                                   |
| Selects voice channel ---- | 11                                                                        |                                   |
| Sends tx-on command to --- | 12                                                                        |                                   |
| cell site                  |                                                                           |                                   |
|                            | 13 -- Reformats channel designation message                               |                                   |
|                            | 14 -- Sends channel designation message to mobile unit via access channel |                                   |
|                            | 15 -----                                                                  | Tunes to voice channel            |
|                            | 16 -----                                                                  | Transponds SAT                    |
|                            | 17 -- Detects SAT                                                         |                                   |
|                            | 18 -- Puts off-hook on trunk                                              |                                   |
| Detects off-hook -----     | 19                                                                        |                                   |

Completes call through --- 20  
network Time

Let me review the frequency allocation for Wireline and non-Wireline systems. Remember that the Wireline service is usually provided by the area's telephone company, in my area that company is NYNEX. The non-Wireline companies are usually operated by other carriers foreign to the area, in my area we are serviced by Cellular One (which is owned by Southwestern Bell). Each company has its one slice of the electro-magnetic spectrum. The coverage is not continuous, remember that there are also 800 MHz trunked business systems that also operate in this bandwidth. Voice channels are 30 KHz apart and the Data channels are 10 KHz apart.

| Frequency Range   | Use                                           |
|-------------------|-----------------------------------------------|
| 870.000 - 879.360 | Cellular One (mobile input 825.000 - 834.360) |
| 880.650 - 890.000 | NYNEX (mobile input 835.650 - 845.500)        |
| 890.000 - 891.500 | Cellular One (mobile input 845.000 - 846.500) |
| 891.500 - 894.000 | NYNEX (mobile input 846.500 - 849.000)        |
| 879.390 - 879.990 | Cellular One (data)                           |
| 880.020 - 880.620 | NYNEX (data)                                  |

The data streams are encoded NRZ (Non-return-to-zero) binary ones and zeroes are now zero-to-one and one-to-zero transitions respectively. This is so the wideband data can modulate the transmitter via binary frequency shift keying, and ones and zeroes into the modulator MUST now be equivalent to nominal peak frequency deviations of 8 KHz above and below the carrier frequency.

#### PUTTING IT ALL TOGETHER - Signaling on the Control Channels

The following information will be invaluable to the hobbyist that is monitoring cellular telephones via a scanner and can access control channel signals. All information released below is EIA/TIA -- FCC standard. There are a lot of differences between cellular phones, but all phones must interface into the mobile network and talk fluently between each other and cell sites. Therefore, the call processing and digital signaling techniques are uniform throughout the industry.

#### MOBILE CALL PROCESSING

##### Calling:

Initially, the land station transmits the first part of its SID to a mobile monitoring some control channel, followed by the number of paging channels, an ESN request, then mobile registration, which will either be set to 0 or 1. When registration is set to one, the mobile will transmit both MIN1 and MIN2 during system access, another 1 for discontinuous (DTX) transmissions, read control-filler (RCF) should be set to 1, and access functions (if combined with paging operations) require field setting to 1, otherwise CPA (combined paging access) goes to 0.

##### Receiving:

As the mobile enters the Scan Dedicated Control Channels Task, it must examine signal strengths of each dedicated control channel assigned to System A if enabled. Otherwise System B control channels are checked. The values assigned in the NAWC (Number of Additional Words Coming) system parameter overhead message train will determine for the mobile if all intended information has been received. An EDN field is used as a crosscheck, and control-filler messages are not to be counted as part of the message. Should a correct BCH

code be received along with a non-recognizable overhead message, it must be part of the NAWC count train but the equivalent should not try and execute the instructions.

Under normal circumstances, mobiles are to tune to the strongest dedicated control channel, receive a system parameter transmission, and, within 3 seconds, set up the following:

- o Set SID's 14 most significant bits to SID1 field value.
- o Set SID's least significant bit to 1, if serving system status enables, or to zero if not.
- o Set paging channels N to 1 plus the value of N-1 field.
- o Set paging channel FIRSTCHP as follows:
  - If SIDs = SIDp then FIRSTCHPs = FIRSTCHPp (which is an 11-bit paging channel).
  - If SIDs = SIDp and serving system is enabled, set FIRSTCHPs to initial dedicated channel for system B.
  - If SIDs = SIDp and serving system is disabled, set FIRSTCHPs to first dedicated control channel for system B.
- o Set LASTCHPs to value of FIRSTCHPs + Ns -1.
- o Should the mobile come equipped for autonomous registration, it must:
  - o Set registration increment (REGINCRs) to its 450 default value.
  - o Set registration ID status to enabled.

I know that was a little arcane sounding but it's the best you can do with specifications. Data is data, there is no way to spruce it up. From here on out a mobile must begin the Paging Channel Selection Task. If this cannot be completed on the strongest dedicated channel, the second strongest dedicated channel may be accessed and the three second interval commenced again. Incomplete results should result in a serving system status check and an enabled or disabled state reversed, permitting the mobile to begin the Scan. Dedicated control Channels Task when channel signal strengths are once more examined.

Custom local operations for mobiles may be sent and include roaming mobiles whose home systems are group members. A new access channel may be transmitted with a new access field set to the initial access channel. Autonomously registered mobiles may increment their next registered ID by some fixed value, but the global action message must have its REGINCR field adequately set. Also, so that all mobiles will enter the Initialization Task and scan dedicated control channels, a RESCAN global action message must be transmitted.

Mobile stations may be required to read a control-filler message before accessing any system on a reverse control channel.

System access for mobiles is sent on a forward control channel in the following manner. Digital Color Code (DCC) identifies the land is carried with the system parameter overhead message overload class fields are set to zero among the restricted number, and the remainder set to 1. Busy-to-idle status (BIS) access parameters go to zero when mobiles are prevented from checking on the reverse control channel and the message must be added to the overhead. When mobiles can't use the reverse control channel for seizure messages attempts or busy signals, access attempt parameters must also be included in the overhead. And when a land station receives a seizure precursor matching its digital color



code with 1 or no bit errors, busy idle bits signals on the forward control channel must be set to busy within 1.2 milliseconds from the time of the last bit seizure. Busy-idle bit then must remain busy until a minimum of 30 msec following the final bit of the last word of the message has been received, or a total of 175 msec has elapsed.

### Channel Confirmation

Mobiles are to monitor station control messages for orders and respond to both audio and local control orders even though land stations are not required to reply. MIN bits must be matched. Thereafter, the System Access Task is entered with a page response, as above, and an access timer started.

This time runs as follows:

- o 12 seconds for an origination
- o 6 seconds for page response
- o 6 seconds for an order response
- o 6 seconds for a registration

The last try code is then set to zero, and the equipment begins the Scan Access Channels Task to find two channels with the strongest signals which it tunes and enters the Retrieve Access Attempts Parameters Task.

This is where both maximum numbers of seizure attempts and busy signals are each set to 10. A read control-filler bit (RCF) will then be checked: If the RCF equals zero, the mobile then reads a control-filler message, sets DCC and WFOM (wait for overhead message train before reverse control channel access) to the proper fields and sets the proper fields and sets the appropriate power level. Should neither the DCC field nor the control-filler message be received and access time has expired, the mobile station goes to Serving System Determination Task. But within the allowed access time, the mobile station enters the Alternate Access Channel Task. BIS is then set to 1 and the WFOM bit is checked. If WFOM equals 1, the station enters the Update Overhead Information Task; if WFOM equals 0, a random delay wait is required of 0 to 200 msec, +/- 1 msec. Then, the station enters the Seize Reverse Control Channel Task.

Service Requesting is next. This task requires that the mobile continue to send its message to the land station according to the following instructions:

- o Word A is required at all times.
- o Word B has to be sent if last try access LT equals 1 or if E requires MIN1 and/or MIN2, and the ROAM status is disabled, or if the station has been paged with a 2-word control message.
- o Word C is transmitted with S (serial number) being 1
- o Word D required if the access is an origination
- o Word E transmitted when the access is an origination and between 9 and 16 digits are dialed. When the mobile has transmitted its complete message, an unmodulated carrier is required for another 25 milliseconds before carrier turnoff. After words A through E have been sent, the next mobile task depends on the type of access.

Order confirmation requires entry into the Serving System Determination Task.

Origination means entry into the Await Message Task.

Page response, is the same as Origination.

Registration requires Await Registration Confirmation, which must be completed within 5 seconds or registration failure follows. The same is true for Await Message since an incomplete task in 5 seconds sends the mobile into the Serving System Determination Task. Origination or Page response requires mobile update of parameters delivered in the message. If R equals 1, the mobile enters the

Autonomous Registration Task, otherwise, it goes to the Initial Voice Channel Confirmation Task. Origination access may be either an intercept or reorder, and in these instances, mobiles enter the Serving System Determination Task. The same holds true for a page response access. But if access is an origination and the user terminates his call during this task, the call has to be released on a voice channel and not control channel.

If a mobile station is equipped for Directed Retry and if a new message is received before all four words of the directed retry message, it must go to the Serving System Determination Task. There the last try code (LT) must be set according to the ORDQ (order qualifier) field of the message as follows:

If 000, LT sets to 0  
If 0001, LT sets to 1

Thereafter, the mobile clears the list of control channels to be scanned in processing Directed Retry (CCLIST) and looks at each CHANPOS (channel position) field contained in message words three and four. For nonzero CHANPOS field, the mobile calculates a corresponding channel number by adding CHANPOS to FIRSTCHA minus one. Afterwards, the mobile has then to determine if each channel number is within the set designated for cellular systems. A true answer requires adding this/these channel(s) to the CCLIST.

#### Awaiting Answers

Here, an alert timer is set for 65 seconds (0 to +20 percent). During this period the following events may take place:

- o Should time expire, the mobile turns its transmitter off and enters the Serving System Determination Task.
- o An answer requires signaling tone turnoff and Conversation Task entry.
- o If any of the messages listed hereafter are received within 100 milliseconds, the mobile must compare SCC digits that identify stored and proper SAT frequencies for the station to the PSCC (present SAT color code). If not equivalent, the order is ignored. If correct, then the following actions taken for each order:

Handoff: Signaling extinguished for 500 msec, signal tone off, transmitter off, power lever adjusted, new channel tuned, new SAT, new SCC field, transmitter on, fade timer reset, and signaling tone on. Wait for an answer.

Alert: Reset alert timer for 65 seconds and stay in Waiting for Answer Task.

Stop Alert: Extinguish signaling tone and enter Waiting for Order Task.

Release: Signaling tone off, wait 500 msec, then enter Release Task.

Audit: Confirm message to land station, then stay in Waiting for Answer Task.

Maintenance: Reset alert timer for 65 seconds and remain in Waiting for Answer Task.

Change Power: Adjust transmitter to power level required and send confirmation to land station. Remain in Waiting for Answer Task.

Local Control: If local control is enabled and order received, examine LC

field and determine action.

Orders other than the above for this type of action are ignored.

### Conversation

In this mode, a release-delay timer is set for 500 mSec. If Termination is enabled, the mobile sets termination status to disabled and waits 500 mSec before entering Release Task. The following actions may then execute:

- o Upon call termination, the release delay timer has to be checked. If time has expired, the Release Task is entered; if not expired, the mobile must wait until expiration and then enter Release Task.
- o Upon user requested flash, signaling tone turned on for 400 mSec. But should a valid order tone be received during this interval, the flash is immediately terminated and the order processed. The flash, of course, is not then valid.
- o Upon receipt of the following listed orders and within 100 mSec, the mobile must compare SCC with PSCC, and the order is ignored if the two are not equal. But if they are the same, the following can occur:

Handoff: Signaling tone on for 50 mSec, then off, transmitter off, power level adjusted, new channel tuned, adjust new SAT, set SCC to SCC field message value, transmitter on, fade timer reset, remain in Conversation Task.

Send Called Address: Upon receipt within 10 seconds of last valid flash, called address sent to land station. Mobile remains in Conversation Task. Otherwise, remain in Conversation Task.

Alert: Turn on signaling tone, wait 500 mSec, then enter Waiting for Answer Task.

Release: Check release delay timer. If time expired, mobile enters Release Task; but if timer has not finished, then mobile must wait and then enter Release Task when time has expired.

Audit: Order confirmation sent to land station while remaining in Conversation Task.

Maintenance: Signaling tone on, wait 500 mSec, then enter Waiting for Answer Task.

Change Power: Adjust transmitter to power level required by order qualification code and send confirmation to land station. Remain in Conversation Task.

Local Control: If local control is enabled and local control order received, the LC field is to be checked for subsequent action and confirmation.

Orders other than the above for this type of action are ignored.

### Release

In the release mode the following steps are required:

- o Signaling tone sent for 1.8 sec. If flash in transmission when

- signaling tone begun, it must be continued and timing bridged so that action stops within 1.8 sec.
- o Stop signaling tone.
  - o Turn off transmitter.
  - o The mobile station then enters the Serving System Determination Task.

The above is the Cellular System Mobile/Land Station Compatibility Specification. The following shall be Signaling Formats which are also found in the above document. I converted all these tables by HAND into ASCII so appreciate them. It wasn't the easiest thing to do. But I must say, I definitely understand the entire cellular operation format.

There are two types of continuous wideband data stream transmissions. One is the Forward Control Channel which is sent from the land station to the mobile. The other is the Reverse Control Channel, which is sent from the mobile to the land station. Each data stream runs at a rate of 10 kilobit/sec, +/- 1 bit/sec rate. The formats for each of the channels follow.

#### - Forward Control Channel

The forward control channel consists of three discrete information streams. They are called stream A, stream B and the busy-idle stream. All three streams are multiplexed together. Messages to mobile stations with the least significant bit of their MIN number equal to "0" are sent on stream A, and those with a "1" are sent on stream B.

The busy-idle stream contains busy-idle bits, which are used to indicate the status of the reverse control channel. If the busy-idle bit = "0" the reverse control channel is busy, if it equals "1" it is idle. The busy-idle bit is located at the beginning of each dotting sequence, word sync sequence, at the beginning of the first repeat of word A and after every 10 message bits thereafter.

Mobile stations achieve synchronization with the incoming data via a 10 bit dotting sequence (1010101010) and an 11 bit word sync sequence (11100010010). Each word contains 40 bits, including parity and is repeated 5 times after which it is then referred to as a "block". For a multiword message, the second word block and subsequent word blocks are formed the same as the first word block including the dotting and sync sequences. A "word" is formed when the 28 content bits are encoded into a (40, 28; 5) BCH (Bose-Chaudhuri-Hocquenghem) code. The left-most bit shall be designated the most-significant bit.

The Generator polynomial for the (40, 28;5) BCH code is:

$$G_B(X) = X^{12} + X^{10} + X^8 + X^5 + X^4 + X^3 + X^0$$

Each FOCC message can consist of one or more words. Messaging transmitted over the forward control channel are:

- Mobile station control message
- Overhead message
- Control-filler message

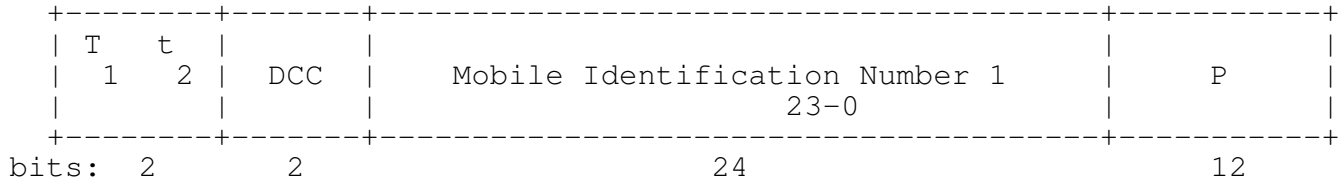
Control-filler messages may be inserted between messages and between word blocks of a multiword message.

Message Formats: Found on either stream A or B

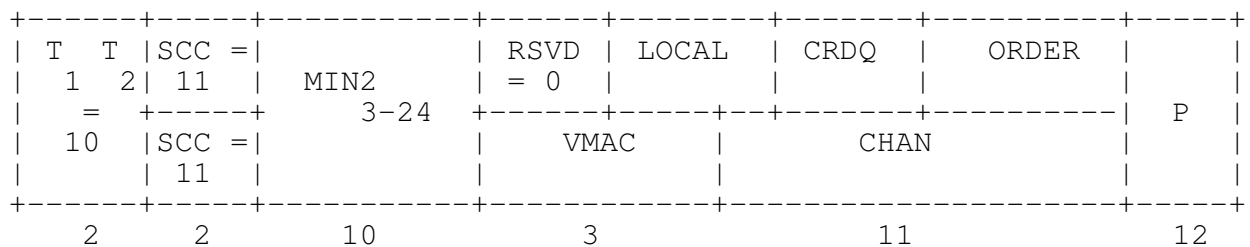
## - Mobile Station Control Message

The mobile station control message can consist of one, two, or four words.

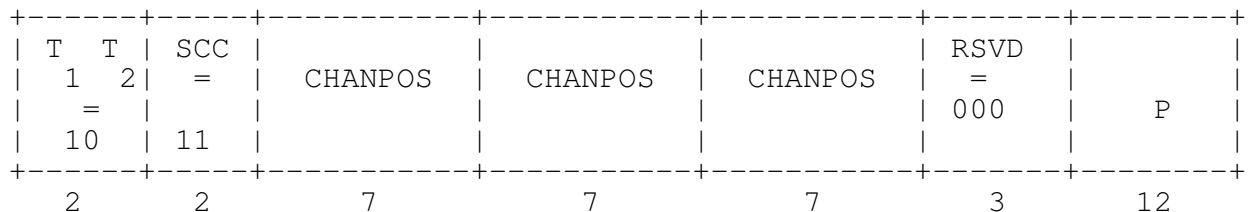
### Word 1 (abbreviated address word)



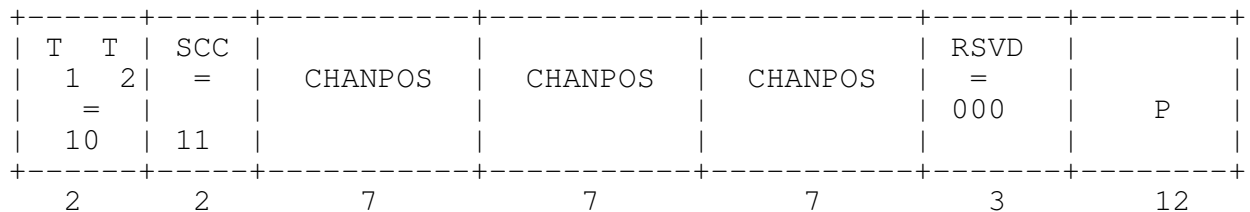
### Word 2 (Extended Address Word)



### Word 3 (First Directed-Retry Word)



### Word 4 (Second Directed-Retry Word)



The interpretation of the data fields:

- T T - Type field. If only Word 1 is send, set to 00 in Word 1.
- SCC - SAT color code (discussed previously)
- ORDER - Order field. Identifies the order type (see table below)
- ORDQ - Order qualifier field. Qualifies the order to a specific action
- LOCAL - Local control field. This field is specific to each system. The ORDER field must be set to local control for this field to be interpreted.
- VMAC - Voice Mobile Attenuation Code field. Indicates the mobile station power level associated with the designated voice channel.

CHAN - Channel number field. Indicates the designated voice channel.  
 CHANPOS- CHANnel POSition field. Indicates the position of a control channel relative to the first access channel (FIRSTCHA).  
 RSVD - Reserved for future use, all bits must be set as indicated.  
 P - Parity field.

#### Coded Digital Color Code

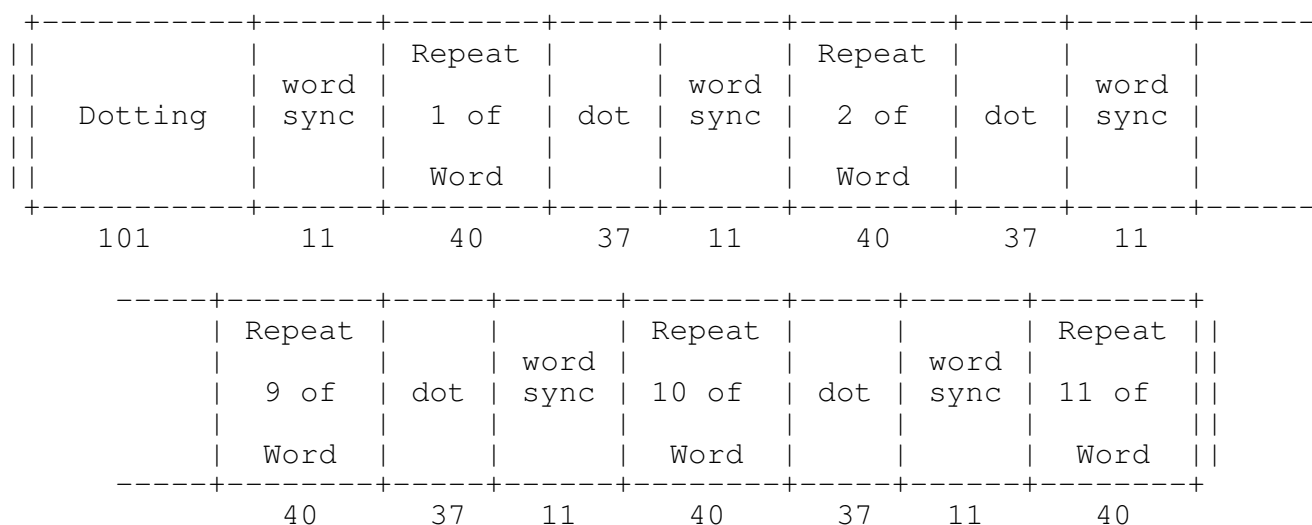
| Received DCC | 7-bit Coded DCC |
|--------------|-----------------|
| 00           | 0000000         |
| 01           | 0011111         |
| 10           | 1100011         |
| 11           | 1111100         |

#### Order and Order Qualification Codes

| Order Code                   | Order Qualification Code | Function                                            |
|------------------------------|--------------------------|-----------------------------------------------------|
| 00000                        | 000                      | page (or origination)                               |
| 00001                        | 000                      | alert                                               |
| 00011                        | 000                      | release                                             |
| 00100                        | 000                      | reorder                                             |
| 00110                        | 000                      | stop alert                                          |
| 00111                        | 000                      | audit                                               |
| 01000                        | 000                      | send called-address                                 |
| 01001                        | 000                      | intercept                                           |
| 01010                        | 000                      | maintenance                                         |
| 01011                        | 000                      | charge power to power level 0                       |
| 01011                        | 001                      | charge power to power level 1                       |
| 01011                        | 010                      | charge power to power level 2                       |
| 01011                        | 011                      | charge power to power level 3                       |
| 01011                        | 100                      | charge power to power level 4                       |
| 01011                        | 101                      | charge power to power level 5                       |
| 01011                        | 110                      | charge power to power level 6                       |
| 01011                        | 111                      | charge power to power level 7                       |
| 01100                        | 000                      | directed retry - not last try                       |
| 01100                        | 001                      | directed retry - last try                           |
| 01101                        | 000                      | non-autonomous registration - don't reveal location |
| 01101                        | 001                      | non-autonomous registration - make location known   |
| 01101                        | 010                      | autonomous registration - don't reveal location     |
| 01101                        | 011                      | autonomous registration - make location known       |
| 11110                        | 000                      | local control                                       |
| All other codes are reserved |                          |                                                     |

#### Forward Voice Channel

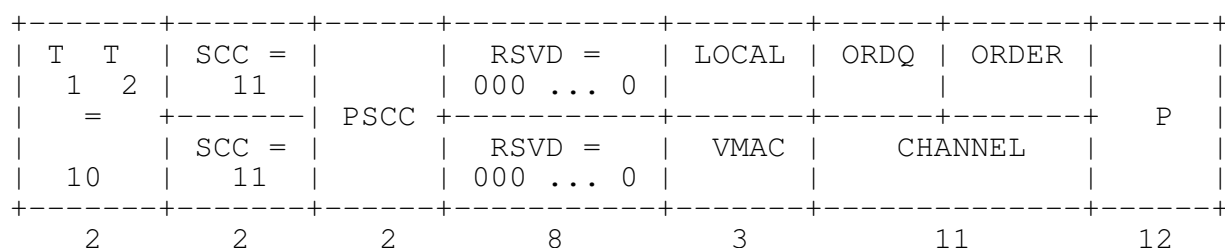
The forward voice channel (FVC) is a wideband data stream sent by the land station to the mobile station. This data stream must be generated at a 10 kilobit/Sec +/- .1 bit/Sec rate. The Forward Voice Channel format follows:



A 37-bit dotting sequence and an 11-bit word sync sequence are sent to permit mobile stations to achieve synchronization with the incoming data, except at the first repeat of the word, where the 101-bit dotting sequence is used. Each word contains 40 bits, including parity, and is repeated eleven times together with the 37-bit dotting and 11-bit word sync; it is then referred to as a word block. A word block is formed by encoding the 28 content bits into a (40, 28) BCH code that has a distance of 5 (40, 28; 5). The left-most bit (as always) is designated the most-significant bit. The 28 most significant bits of the 40-bit field shall be the content bits. The generator polynomial is the same as that used for the forward control channel.

The mobile station control message is the only message transmitted over the forward voice channel. The mobile station control message consists of one word.

#### Mobile Station Control Message:



#### Interpretation of the data fields:

- T   T   - Type field. Set to '10'.  
1   2
- SCC   - SAT color code for new channel (see SCC table)
- PSCC   - Present SAT color code. Indicates the SAT color code associated with the present channel.
- ORDER   - Order field. Identifies the order type. (see Order table)
- ORDQ   - Order qualifier field. Qualifies the order to a specific action (see Order table)
- LOCAL   - Local Control field. This field is specific to each system. The ORDER field must be set to local control (see Order table) for this field to be interpreted.
- VMAC   - Voice mobile attenuation code field. Indicates the mobile station power level associated with the designated voice channel.

RSVD - Reserved for future use; all bits must be set as indicated.  
P - Parity field.

### Reverse Control Channel

The Reverse Control Channel (RECC) is a wideband data stream sent from the mobile station to the land station. This data stream runs at a rate of 10 kilobit/sec, +/- 1 bit/sec rate. The format of the RECC data stream follows:

|       | +  | -----   | +  | ----- | + | ----- | +   | -----      | +   | -----       | +   | -----      | + | ----- | + | ----- | + | ----- | + |
|-------|----|---------|----|-------|---|-------|-----|------------|-----|-------------|-----|------------|---|-------|---|-------|---|-------|---|
|       |    | Dotting |    | Word  |   | Coded |     | first word |     | Second word |     | Third word |   |       |   |       |   |       |   |
|       |    |         |    | sync  |   | DCC   |     | repeated   |     | repeated    |     | repeated   |   |       |   |       |   |       |   |
|       |    |         |    |       |   |       |     | 5 times    |     | 5 times     |     | 5 times    |   |       |   |       |   |       |   |
| bits: | 30 |         | 11 |       | 7 |       | 240 |            | 240 |             | 240 |            |   |       |   |       |   |       |   |

Dotting = 01010101...010101

Word sync = 11100010010

All messages begin with the RECC seizure precursor which is composed of a 30 bit dotting sequence (1010...101), and 11 bit word sync sequence (11100010010), and the coded digital color code.

Each word contains 48 bits, including parity, and is repeated five times after which it is referred to as a word block. A word is formed by encoding 36 content bits into a (48, 36) BCH code that has a distance of 5, (48 36; 5). The left most bit shall be designated the most-significant bit. The 36 most significant bits of the 48 bit field shall be the content bits.

The generator polynomial for the code is the same for the (40,28;5) code used on the forward channel.

Each Reverse Control Channel message can consist of one of the five words. The types of messages to be transmitted over the reverse control channel are as follows:

- o Page Response Message
- o Origination Message
- o Order Confirmation Message
- o Order Message

These messages are made up of combination of the following five words:

#### Word A - Abbreviated Address Word

|  | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | +  |
|--|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|----|
|  |   | F     |   |       |   |       |   | RSVD  |   | S     |   |       |   |       |   |       |   |       |    |
|  |   | =     |   | NAWC  |   | T     |   | S     |   | E     |   | =     |   | C     |   |       |   | P     |    |
|  |   | 1     |   |       |   |       |   | 0     |   | M     |   |       |   |       |   |       |   |       |    |
|  | 1 |       | 3 |       | 1 |       | 1 |       | 1 |       | 1 |       | 4 |       |   | 24    |   |       | 12 |

#### Word B - Extended Address Word

|  | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + |
|--|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|
|  |   | F     |   |       |   |       |   |       |   |       |   | RSVD  |   |       |   |       |   |       |   |



|   |      |       |      |       |    |       |       |    |
|---|------|-------|------|-------|----|-------|-------|----|
| = | NAWC | LOCAL | ORDQ | LOCAL | LT | =     | MIN 2 | P  |
| 0 |      |       |      |       |    | 00..0 | 33-24 |    |
| 1 | 3    | 5     | 3    | 5     | 1  | 8     | 10    | 12 |

Word C - Electronic Serial Number Word

|   |      |  |  |  |  |              |  |  |  |    |  |
|---|------|--|--|--|--|--------------|--|--|--|----|--|
| F |      |  |  |  |  |              |  |  |  |    |  |
| = | NAWC |  |  |  |  | SERIAL (ESN) |  |  |  | P  |  |
| 1 |      |  |  |  |  |              |  |  |  |    |  |
| 1 | 3    |  |  |  |  | 32           |  |  |  | 12 |  |

Word D - First Word of the Called-Address

|   |      |       |       |     |     |     |     |       |       |    |
|---|------|-------|-------|-----|-----|-----|-----|-------|-------|----|
| F |      | 1st   | 2nd   |     |     |     |     | 7th   | 8th   |    |
| = | NAWC | DIGIT | DIGIT | ... | ... | ... | ... | DIGIT | DIGIT | P  |
| 1 |      |       |       |     |     |     |     |       |       |    |
| 1 | 3    | 4     | 4     | 4   | 4   | 4   | 4   | 4     | 4     | 12 |

Word E - Second Word of the Called-Address

|   |      |       |       |     |     |     |     |       |       |    |
|---|------|-------|-------|-----|-----|-----|-----|-------|-------|----|
| F | NAWC | 9th   | 10th  |     |     |     |     | 15th  | 16th  |    |
| = | =    | DIGIT | DIGIT | ... | ... | ... | ... | DIGIT | DIGIT | P  |
| 0 | 000  |       |       |     |     |     |     |       |       |    |
| 1 | 3    | 4     | 4     | 4   | 4   | 4   | 4   | 4     | 4     | 12 |

The interpretation of the data fields is as follows:

- F - First word indication field. Set to '1' in first word and '0' in subsequent words.
- NAWC - Number of additional words coming field.
- T - T field. Set to '1' to identify the message as an origination or an order; set to '0' to identify the message as an order response or page response.
- S - Send serial number word. If the serial number word is sent, set to '1'; if the serial number word is not sent, set to '0'.
- SCM - The station class mark field
- ORDER - Order field. Identifies the order type.
- ORDQ - Order qualifier field. Qualifies the order confirmation to a specific action.
- LOCAL - Local control field. This field is specific to each system. The ORDER field must be set to locate control for this field to be interpreted.
- LT - Last-try code field.

|        |                                                                                       |
|--------|---------------------------------------------------------------------------------------|
| MIN1   | - Mobile Identification number field part one.                                        |
| MIN2   | - Mobile Identification number field part two.                                        |
| SERIAL | - Electronic Serial Number field. Identifies the serial number of the mobile station. |
| DIGIT  | - Digit field (see table below)                                                       |
| RSVD   | - Reserved for future use; all bits must be set as indicated.                         |
| P      | - Parity field.                                                                       |

Called-address Digit Codes

| Digit | Code | Digit | Code |
|-------|------|-------|------|
| 1     | 0001 | 7     | 0111 |
| 2     | 0010 | 8     | 1000 |
| 3     | 0011 | 9     | 1001 |
| 4     | 0100 | 0     | 1010 |
| 5     | 0101 | *     | 1011 |
| 6     | 0110 | #     | 1100 |
|       |      | Null  | 0000 |

NOTE :

1. The digit 0 is encoded as binary 10, not binary zero.
2. The code 0000 is the null code, indicated no digit present
3. All other four-bit sequences are reserved, and must not be transmitted.

Examples of encoding called-address information into the called address words follow:

If the number 2# is entered, the word is as follows:

[illegible]

If the number 13792640 is entered, the word is as follows:

|      |      |      |      |      |      |      |      |      |   |
|------|------|------|------|------|------|------|------|------|---|
| NOTE | 0001 | 0011 | 0111 | 1001 | 0010 | 0110 | 0100 | 1010 | P |
|------|------|------|------|------|------|------|------|------|---|

As you can see the numbers are coded into four bits and inserted sequentially into the train. Notice that when the number is longer than 8 numbers it is broken into two different Words.

If the number 6178680300 is entered, the words are as follows:

Word D - First Word of the Called-Address

[illegible]

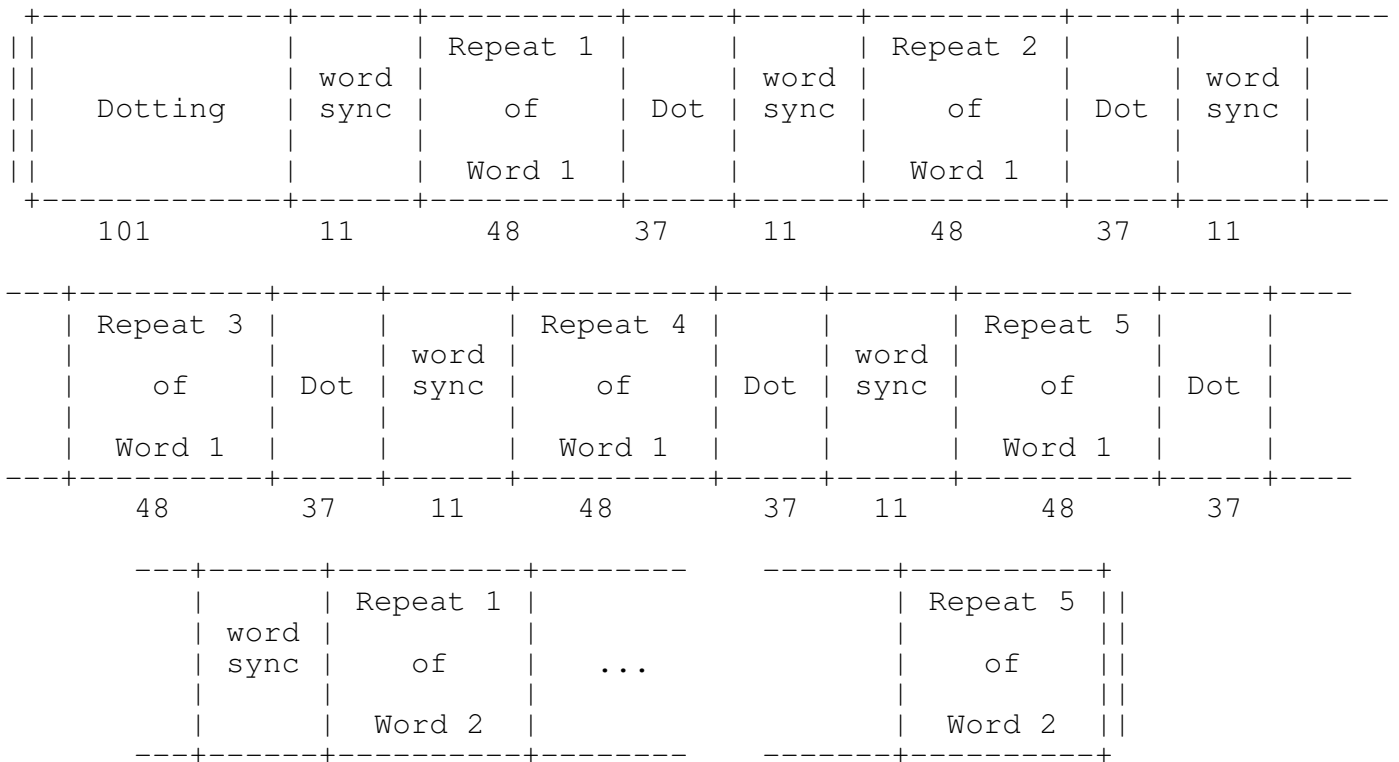
## Word E - Second Word of the Called-Address

[illegible]

NOTE = four bits which depend on the type of message

### Reverse Voice Channel

The reverse voice channel (RVC) is a wideband data stream sent from the mobile station to the land station. This data stream must be generated at a 10 kilobit/second +/- 1 bit/sec rate. The format is presented below.



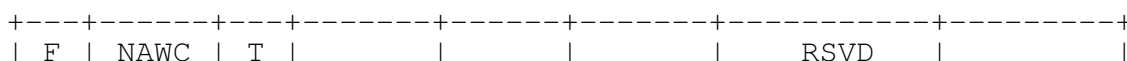
A 37-bit dotting sequence and an 11-bit word sync sequence are sent to permit land stations to achieve synchronization with the incoming data, except at the first repeat of word 1, where a 101-bit dotting sequence is used. Each word contains 48 bits, including parity, and is repeated five times together with the 37-bit dotting and 11-bit word sync sequences; it is then referred to as a word block. For a multi-word message, the second word block is formed the same as the first word block including the 37-bit dotting and 11-bit word sync sequences. A word is formed by encoding the 36 content bits into a (48, 36) BCH code that has a distance of 5, (48, 36; 5). The left-most bit (earliest in time) shall be designated the most-significant bit. The 36 most-significant bits of the 48-bit field shall be the content bits. The generator polynomial for the code is the same as for the (40, 28; 5) code used on the forward control channel.

Each RVC message can consist of one or two words. The types of messages to be transmitted over the reverse voice channel are as follows:

- o Order Confirmation Message
- o Called-Address Message

The message formats are as follows:

### Order Confirmation Message:



|   |    |   |       |      |       |           |    |
|---|----|---|-------|------|-------|-----------|----|
| = | =  | = | LOCAL | ORDQ | ORDER | =         | P  |
| 1 | 00 | 1 |       |      |       | 000 ... 0 |    |
| 1 | 2  | 1 | 5     | 3    | 5     | 19        | 12 |

### Called-Address Message

#### Word 1 - First Word of the Called-Address

|   |      |   |       |       |     |     |     |     |       |       |    |
|---|------|---|-------|-------|-----|-----|-----|-----|-------|-------|----|
| F | NAWC | T | 1st   | 2nd   |     |     |     |     | 7th   | 8th   | P  |
| = | =    | = | Digit | Digit | ... | ... | ... | ... | Digit | Digit |    |
| 1 | 01   | 0 |       |       |     |     |     |     |       |       |    |
| 1 | 2    | 1 | 4     | 4     | 4   | 4   | 4   | 4   | 4     | 4     | 12 |

#### Word 2 - Second Word of the Called-Address

|   |      |    |       |       |     |     |     |    |       |       |    |
|---|------|----|-------|-------|-----|-----|-----|----|-------|-------|----|
| F | NAWC | T  | 9th   | 10th  |     |     |     |    | 15th  | 16th  | P  |
| = | =    | =  | Digit | Digit | ... | ... | ... | .. | Digit | Digit |    |
| 0 | 00   | 0D |       |       |     |     |     |    |       |       |    |
| 1 | 2    | 1  | 4     | 4     | 4   | 4   | 4   | 4  | 4     | 4     | 12 |

The fields are descriptions a the me as those for the Reverse Control channel above.

### Overhead Message

A three-bit OHD field is used to identify the overhead message types. Overhead message type codes are listed in the table below. They are grouped into the following functional classes:

- o System parameter overhead message
- o Global action overhead message
- o Registration identification message
- o Control-filler message

Overhead messages are send in a group called an overhead message train. The first message of the train must be the system parameter overhead message. The desired global action messages and/or a registration ID message must be appended to the end of the system parameter overhead message. The total number of words in an overhead message train is one more than the value of the NAWC field contained in the first word of the system parameter overhead message. The last word in the train must be set to '0'. For NAWC-counting purposes, inserted control-filler messages must not be counted as part of the overhead message train.

The system parameter overhead message must be sent every .8 +/- .3 seconds on each of the following control channels:

- o combined paging-access forward channel.
- o Separate paging forward control channel
- o Separated access forward control channel when the control-filler

message is sent with the WFOM bit set to '1'.

The global action messages and the registration identification message are sent on an as needed basis.

- o The system parameter for overhead message consists of two words.

#### 0 Word 1

|    |   |     |      |      |      |     |    |
|----|---|-----|------|------|------|-----|----|
| T  | T |     |      | RSVD |      | OHD |    |
| 1  | 2 |     |      | =    | NAWC | =   | P  |
| 11 |   | DCC | SID1 | 000  |      | 110 |    |
| 2  | 2 |     | 14   | 3    | 4    | 3   | 12 |

#### Word 2

|    |   |     |   |   |      |      |      |
|----|---|-----|---|---|------|------|------|
| T  | T |     |   |   |      |      | RSVD |
| 1  | 2 |     |   |   |      |      | =    |
| 11 |   | DCC | S | E | REGH | REGR | DTX  |
| 2  | 2 |     | 1 | 1 | 1    | 1    | 1    |

|       |     |     |          |     |  |     |    |
|-------|-----|-----|----------|-----|--|-----|----|
|       |     |     |          |     |  | OHD |    |
|       |     |     |          |     |  | =   | P  |
| N - 1 | RCF | CPA | CMAx - 1 | END |  | 111 |    |
| 5     | 1   | 1   | 7        | 1   |  | 3   | 12 |

#### Overhead Message Types

| Code | Order                              |
|------|------------------------------------|
| 000  | Registration ID                    |
| 001  | Control-filler                     |
| 010  | reserved                           |
| 011  | reserved                           |
| 100  | global action                      |
| 101  | reserved                           |
| 110  | Word 1 of system parameter message |
| 111  | Word 2 of system parameter message |

The interpretation of the data fields:

T T - Type field. Set to '11' indicating an overhead word.

1 2

OHD - Overhead message type field. The OHD field of Word 1 is set to '110' indicating the first word of the system parameter overhead message. The OHD field of Word 2 is set to '111' indicating the second word of the system parameter overhead





|   |   |   |    |   |   |    |
|---|---|---|----|---|---|----|
| 2 | 2 | 4 | 16 | 1 | 3 | 12 |
|---|---|---|----|---|---|----|

The interpretation of the data fields are as follows:

|         |   |                                                                                                                          |
|---------|---|--------------------------------------------------------------------------------------------------------------------------|
| T       | T | - Type field. Set to '11' indicating overhead word.                                                                      |
| 1       | 2 |                                                                                                                          |
| ACT     |   | - Global action field (see table below).                                                                                 |
| BIS     |   | - Busy-idle status field.                                                                                                |
| DCC     |   | - Digital Color Code.                                                                                                    |
| OHD     |   | - Overhead Message type field. Set to '100' indicating the global action message.                                        |
| REGINCR |   | - Registration increment field.                                                                                          |
| NEWACC  |   | - News access channel starting point field.                                                                              |
| MAXBUSY |   | - Maximum busy occurrences field (page response).                                                                        |
| - PGR   |   |                                                                                                                          |
| MAXBUSY |   | - Maximum busy occurrences field (other accesses).                                                                       |
| - OTHER |   |                                                                                                                          |
| MAXSZTR |   | - Maximum seizure tries field (page response).                                                                           |
| - PRG   |   |                                                                                                                          |
| MAXSZTR |   | - Maximum seizure tries field (other accesses).                                                                          |
| - OTHER |   |                                                                                                                          |
| OLCN    |   | - Overload class field (N = 0 to 15)                                                                                     |
| END     |   | - End indication field. Set to '1' to indicate the last word of the overhead message train; set to '0' if not last word. |
| RSVD    |   | - Reserved for future use, all bits must be set as indicated.                                                            |
| LOCAL   |   | - May be set to any bit pattern.                                                                                         |
| CONTROL |   |                                                                                                                          |
| P       |   | - Parity field.                                                                                                          |

The registration ID message consists of one word. When sent, the message must be appended to a system parameter overhead message in addition to any global action messages.

|   |       |   |       |   |       |   |       |   |       |   |       |   |
|---|-------|---|-------|---|-------|---|-------|---|-------|---|-------|---|
| + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + |
|   | T     |   | T     |   |       |   |       |   | OHD   |   |       |   |
|   | 1     |   | 2     |   |       |   |       |   |       |   |       |   |
|   | =     |   |       |   | DCC   |   | REGID |   | END   |   | =     |   |
|   |       |   |       |   |       |   |       |   |       |   | P     |   |
|   | 11    |   |       |   |       |   |       |   | 000   |   |       |   |
| + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + | ----- | + |
|   | 2     |   | 2     |   | 20    |   | 1     |   | 3     |   | 12    |   |

The interpretation of the data fields:

|       |   |                                                                                                            |
|-------|---|------------------------------------------------------------------------------------------------------------|
| T     | T | - Type field. Set to '11' indicating overhead word.                                                        |
| DCC   |   | - Digital color code field.                                                                                |
| OHD   |   | - Overhead message type field. Set to '000' indicating the registration ID message.                        |
| REGID |   | - Registration ID field.                                                                                   |
| END   |   | - End indication field. Set to '1' to indicate last word of the overhead message train; set to '0' if not. |
| P     |   | - Parity field.                                                                                            |

The control-filler message consists of one word. It is sent whenever there is no other message to be sent on the forward control channel. It may be inserted between messages as well as between word blocks of a multiword message. The control-filler message is chosen so that when it is sent, the 11-bit word sequence will not appear in the message stream, independent of the busy-idle bit status.

The control-filler message is also used to specify a control mobile



attenuation code (CMAC) for use by mobile stations accessing the system on the reverse control channel, and a wait-for-overhead-message bit (WFOM) indicating whether or not mobile stations must read an overhead message train before accessing the system.

|   |   |     |        |      |      |    |      |   |      |      |     |    |   |
|---|---|-----|--------|------|------|----|------|---|------|------|-----|----|---|
| T | T |     |        |      | RVSD |    | RVSD |   |      |      | OHD |    |   |
| 1 | 2 |     |        |      | =    | 11 | =    | 1 | WFOM | 1111 | =   |    | P |
|   |   | DCC | 010111 | CMAC |      |    |      |   |      |      |     |    |   |
|   |   |     |        |      | 00   |    | 00   |   |      |      | 001 |    |   |
| 2 | 2 | 2   | 6      | 3    | 2    | 2  | 2    | 1 | 1    | 4    | 3   | 16 |   |

Interpretation of the data fields:

- T 1 2 - Type field. Set to '11' indicating overhead word.
- DCC - Digital color code field.
- CMAC - Control mobile attenuation field. Indicates the mobile station power level associated with the reverse control channel.
- RVSD - Reserved for future use; all bits must be set as indicated.
- WFOM - Wait-for-overhead-message field.
- OHD - Overhead message type field. Set to '001' indicating the control-filler word.
- P - Parity field.

#### Data Restrictions

The 11-bit sequence (11100010010) is shorter than the length of a word, and therefore can be embedded in a word. Normally, embedded word-sync will not cause a problem because the next word sent will not have the word-sync sequence embedded in it. There are, however, three cases in which the word-sync sequence may appear periodically in the FOCC stream. They are as follows:

- o the overhead message
- o the control-filler message
- o Mobile station control messages with pages to mobile stations with certain central office codes.

These three cases are handled by:

1. Restricting the overhead message transmission rate to about once per second
2. designing the control-filler message to exclude the word-sync sequence, taking into account the various busy-idle bits
3. Restricting the use of certain office codes

If the mobile station control message is examined with the MIN1 separated into NXX-X-XXX as described earlier (where NXX is the central office code, N represents a number from 2 - 9, and X represents a number from 0-9) the order and order qualifications table can be used to deduce when the word-sync word would be sent. If a number of mobile stations are paged consecutively with the same central office code, mobile stations that are attempting to synchronize to the data stream may not be able to do so because of the presence of the false word sync sequence. Therefore, the combinations of central office codes and groups of line numbers appearing in the following table must not be used for mobile stations.

# RESTRICTED CENTRAL OFFICE CODES

| T<br>1 | T<br>2 | DCC | NXX           | X    | XXX | Central<br>Office<br>Code | Thousands<br>Digit |
|--------|--------|-----|---------------|------|-----|---------------------------|--------------------|
| 01     |        | 11  | 000100(1)0000 | ...  | ... | 175                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0001 | ...  | ... | 176                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0010 | ...  | ... | 177                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0011 | ...  | ... | 178                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0100 | ...  | ... | 179                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0101 | ...  | ... | 170                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0110 | ...  | ... | 181                       | 0 to 9             |
| 01     |        | 11  | 000100(1)0111 | ...  | ... | 182                       | 0 to 9             |
| 0Z     |        | 11  | 100010(0)1000 | ...  | ... | 663                       | 0 to 9             |
| 0Z     |        | 11  | 100010(0)1001 | ...  | ... | 664                       | 0 to 9             |
| 0Z     |        | 11  | 100010(0)1010 | ...  | ... | 665                       | 0 to 9             |
| 0Z     |        | 11  | 100010(0)1011 | ...  | ... | 666                       | 0 to 9             |
| 0Z     |        | Z1  | 110001(0)0100 | ...  | ... | 899                       | 0 to 9             |
| 0Z     |        | Z1  | 110001(0)0101 | ...  | ... | 800                       | 0 to 9             |
| 0Z     |        | ZZ  | 111000(1)0010 | ...  | ... | 909                       | 0 to 9             |
| 00     |        | ZZ  | 011100(0)1001 | 0ZZZ | ... | 568                       | 1 to 7             |
| 00     |        | ZZ  | 111100(0)1001 | 0ZZZ | ... | 070                       | 1 to 7             |
| 00     |        | ZZ  | 001110(0)0100 | 10ZZ | ... | 339                       | 8,9,0              |
| 00     |        | ZZ  | 011110(0)0100 | 10ZZ | ... | 595                       | 8,9,0              |
| 00     |        | ZZ  | 101110(0)0100 | 10ZZ | ... | 851                       | 8,9,0              |
| 00     |        | ZZ  | 111110(0)0100 | 10ZZ | ... | 007                       | 8,9,0              |
| 0Z     |        | ZZ  | 000011(1)0100 | 0010 | ... | 150                       | 2                  |
| 0Z     |        | ZZ  | 000111(1)0001 | 0010 | ... | 224                       | 2                  |
| 0Z     |        | ZZ  | 001011(1)0001 | 0010 | ... | 288                       | 2                  |
| 0Z     |        | ZZ  | 001111(1)0001 | 0010 | ... | 352                       | 2                  |
| 0Z     |        | ZZ  | 010011(1)0001 | 0010 | ... | 416                       | 2                  |
| 0Z     |        | ZZ  | 010111(1)0001 | 0010 | ... | 470                       | 2                  |
| 0Z     |        | ZZ  | 011011(1)0001 | 0010 | ... | 544                       | 2                  |
| 0Z     |        | ZZ  | 011111(1)0001 | 0010 | ... | 508                       | 2                  |
| 0Z     |        | ZZ  | 100011(1)0001 | 0010 | ... | 672                       | 2                  |
| 0Z     |        | ZZ  | 100111(1)0001 | 0010 | ... | 736                       | 2                  |
| 0Z     |        | ZZ  | 101011(1)0001 | 0010 | ... | 790                       | 2                  |
| 0Z     |        | ZZ  | 101111(1)0001 | 0010 | ... | 864                       | 2                  |
| 0Z     |        | ZZ  | 110011(1)0001 | 0010 | ... | 928                       | 2                  |
| 0Z     |        | ZZ  | 110111(1)0001 | 0010 | ... | 992                       | 2                  |
| 0Z     |        | ZZ  | 111011(1)0001 | 0010 | ... | 056                       | 2                  |
| 0Z     |        | ZZ  | 111111(1)0001 | 0010 | ... | ...                       | 2                  |

1. In each case, Z represents a bit that may be 1 or 0.
2. Some codes are not used as central office codes in the US at this time. They are included for completeness.
3. The bit in parentheses is the busy-idle bit.

Well there is your signaling in a nutshell. Please note I hardly have the most up-to-date signalling data. Basically what was presented here was a skeleton, the bare bones without all the additions. There are some additions that are system specific. As I get updates I'll be sure to share them with the rest of you. I would be interested in any feedback, so, if you have something to say, send it to:

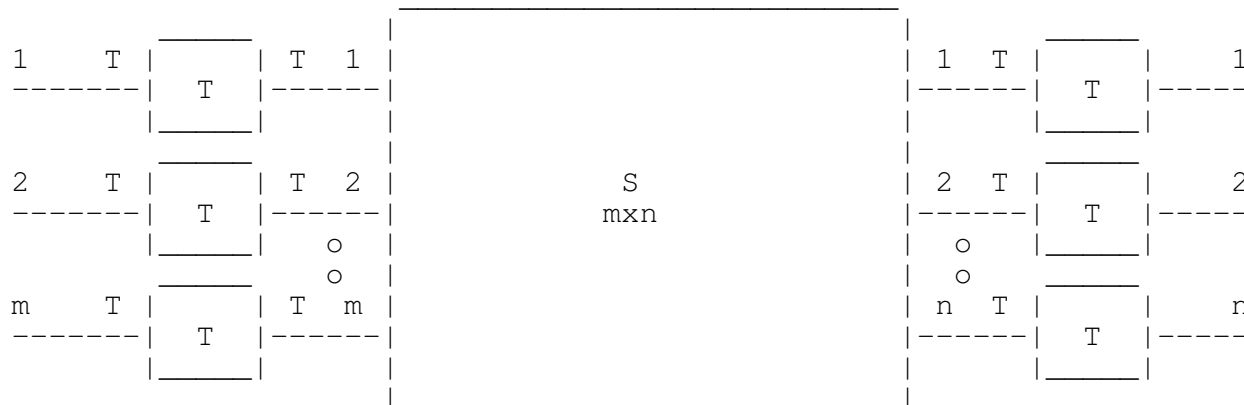
oblivion@atdt.org





Analog Signal (You Talking) / / \ \ Analog Signal\_\_|

Blow Up / of the Switch



The basic design of most of the switches today is a Time-Space-Time (TST) topology. In the Time-Space-Time in the arrangement shown, time slot interchangers will interchange information between external channels and internal (space array) channels.

This is just a quick run through to gives you a general idea about switches without going into math and more technical ideas. For a better understanding, get "Fundamentals of Digital Switching" by John C. McDonald. This book is well written and describes ideas that I cannot get into.

#### C. RCMAC

~~~~~

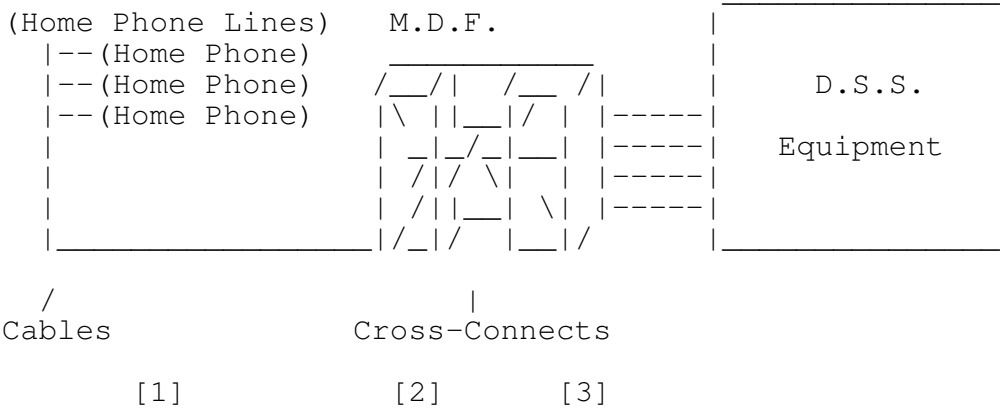
The Recent Change Memory Administration Center's (RCMAC) purpose is to make changes to the software in various Electronic Switching Systems (ESS). An ESS uses a Stored Program Control (SPC) to provide telephone service. Since people with phones and their services change often, the ESS uses a memory called Recent Change. This Recent Change area of memory is used on a standby basis until the information can be updated into the semipermanent memory area of the ESS. It is in the templar area that changes (or Recent Change Messages) are typed and held for updating into the semipermanent memory area (Recent Change Memory).

The following Switching Systems (switches for short) that have Recent Change:

- 1/1AESS
- 2/2BESS
- 3ESS
- 5ESS
- Remote Switching System (RSS)
- #5ETS
- DMS100/200/250/300

Here is a typical hookup. As you follow the diagram below, you will see:

- [1] Telephone subscriber connected to the Central Office by cables.
- [2] At the Central Office, each subscriber is connected to the Main Distributing Frame.
- [3] The Cable and Pair is now connected to the Office Equipment (OE) at another location on the MDF.



1. Office Equipment

The Office Equipment (OE) is identified by a unique numbering plan. The equipment numbers identify the equipment location within the system. The Equipment Numbers also vary from one type of equipment to another.

You also may find the OE (Office Equipment) referred to as the LEN (Line Equipment Number). It is called a REN (Remote Equipment Number) in a case of RSS (Remote Switching System).

Each telephone number is assigned to a specific equipment location where they bid for dial tone.

Here is an example of different types of Office Equipment:

1/1AESS

```

OE 0 0 4 - 1 0 1 - 3 1 2
| | /      | | |      | | /
| |      | | |      | |
| |      | | |      | Level
| |      | | |      | Switch
| |      | | |      | Concentrator
| |      | |      | Bay
| |      | |      | Line Switch Frame
| |      | |      | Line Link
Control Group
  
```

#2ESS

```

OE 0 1 1 - 2 1 4 0
| | /      | | | /
| |      | | |
| |      | | | Switch and Level
| |      | | | Concentrator
| |      | | | Concentrator Group
| |      | | | Link Trunk Network
Control Group
  
```

#3ESS

```

OE 0 0 1 - 2 1 4 0
| | /      | | | |
| |      | | | Level
| |      | | | Switch
| |      | | | Switch Group
| |      | | | Concentrator
| |      | | | Concentrator Group
Control Group
  
```

Others

```

1XB      = XXXX-XXX-XX
1XB      = XXXX-XXXX-XX
5XB      = XXX-XX-XX
SXS      = XXXX-XXX
DMS-10   = XXX-X-XX-X
5ESS     = XXXX-XXX-XX
5ESS     = XXXX-XX-XX
RSS      = XXXX-X-XXXX
DMS-1/200 = XXX-X-XX-XX
  
```

2. How Does All This Fit Into RCMAC?

RCMAC (Recent Change Memory Administration Center) is responsible for updating any Service Order activity. This action will change a customer line or service in the Recent Change memory of the SPC switches.

3. Function of RCMAC

~~~~~

The three basic functions performed in RCMAC are:

- a. Coordination of Recent Change Source Documentation
- b. Processing of Recent Change Requests
- c. Administrative Responsibilities and Interface Groups

In more detail:

#### - Coordination of Recent Change Source Documentation

The first function is the coordination of Source Documents. The main source of RC (Recent Change) is the Service Orders. Service Orders are changes in a subscriber's service. RCMAC, in addition to the input of the service order in the switches, is responsible for other activities such as:

- Simulated Facilities (SFG)
- Route Indexes
- Traffic Registers (TR)
- Subscriber Line Usages (SLU)
- Service Observing Assignment (SOB)
- MARCH (MIZAR) RPM Updates

Terminal Communications to the switches and/or MARCH (MIZAR) typically use the AT&T Datakit. RCMAC also is responsible for "HOT" requests from the I.C. (Installation Center) and other transmissions from the I.C.

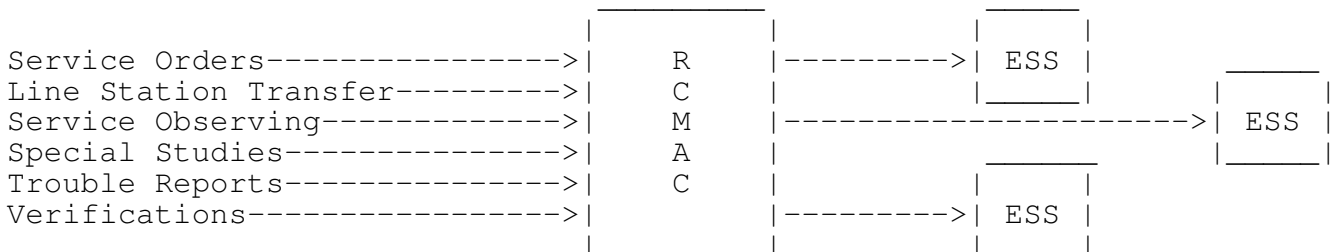
#### - Processing of Recent Change Requests

The second function of RCMAC is processing of RC messages. This involves inputting and editing RC messages in the switches. When RCMAC inputs messages, they are making a change to their customer's service. The customer's service is dependent on the prompt, accurate processing of RC source documents (Service Orders).

The due date (sometimes referred to as the Frame Due Date) remarks and time interval assigned to the order will govern the release of RC input to ESS. Due date is important because this is the date that the Service Order has to be completed (going through the FACS system, frame work done, and RC message inputted into the switch).

#### Recent Change Requests

The RCMAC receives documentation for changes to the temporary memory areas of the various types of ESS equipment. These changes may come in many forms and from many different sources.



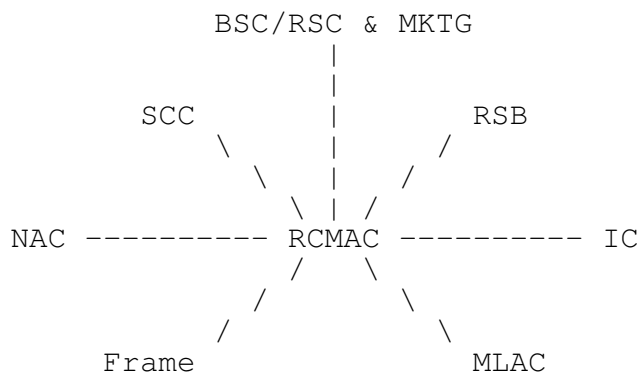
Some Recent Changes requests are Service Orders, Line Equipment Transfers (LET), Service Observing Requests (SOB), Special Studies (SLU), Trouble Reports and Verification (follow local procedure). In short, it is taking this information and making the correct changes into the SPC switches.

## - Administrative Responsibilities and Interface Groups

- Control of errors.
- Monitor activity.
- Prepare administrative reports.
- Coordination of RCMAC operations and interface with other departments.
- Restore RC area of the switches in the event that RC memory is damaged due to machine failure.

## Operational Interface

RCMAC must coordinate activities with many work groups to achieve accurate and quick RC for the ESSes.



To help understand this better, here is a short description of each group that interfaces with RCMAC:

### SCC (Switching Control Center)

- Technical assistance to RCMAC
- Provide emergency coverage (off hours) for RCMAC. This includes service affecting problems. They also coordinate any updates in the ESS programs with RCMAC.

NAC (Network Administration Center) provides RCMAC with:

- Line Class Codes (LCC) like 1FR (1-party Flat Rate).
- List of numbers that must be changed (in ESS memory) from one intercept route index to another, prior to reassignment.
- Translation Assignments; Example: Simulated Facilities Group (SFG).
- Area Transfer/Dial for Dial Assignment.
- Service Observing assignment.
- Subscriber Line Usages (SLU) study assignment.
- Customer Line Overflow study assignment.
- RPM updates for DMS 100 change in COSMOS tables USOC/NXX/Ltg.

Frame (Frame Jeopardy Reports) Central Office (FCC) will interface with RCMAC for Line Equipment transfers.

- Problems encountered by the frame group when completing Service Orders may be coordinated with the MLAC (Loop Assignment Center), or when appropriate will be called directly to RCMAC (i.e. No Dial Tone on a new connect).

### Business/Residence Service Center (BSC/RSC) and Marketing (MKTG)

- The BSC/RSC and MKTG determine what kind of service the customer wants, generates Service Orders, and coordinates with RCMAC regarding special services to customers.



Repair Service Bureau (RSB) or Single Point of Contact (SPOC)

- Customer trouble reports may involve RC inputs; the RCMAC would work closely with RSB or SPOC to clear such troubles.
- RCMAC is responsible for analyzing, investigating and resolving customer trouble caused by RC input.

Installation Center (IC) and/or Maintenance Center (MC)

- The IC/MC group is responsible for the administration function associated with the completion and control of Service Order load. This invokes all orders whether they require field work or no field work.
- This Group is responsible for ensuring all service orders are taken care of on the proper due date.

Mechanized Loop Assignment Center (MLAC) or LAC

- Assigns Service Orders for RCMAC.
- Assigns customers loops (this group is not in all BOCs).

#### D. The FACS Environment

~~~~~

To better understand RCMAC, Source Document flow, and a typical BOC as a whole, the FACS (Facility Administration Control System) is an important part of this.

Systems in a FACS environment

PREMIS - PREMises Information System

This system is divided into three parts: the main PREMIS database, PREMLAC (Loop Assignment) and PREMLAS (Loop Assignment Special circuit). This contains customer and address inventory and assigns numbers.

SOAC - Service Order Analysis and Control

This system receives Service Orders from SORD and interprets and determines facility requirements. The system requests and receives assignments from LFACS and COSMOS and forwards orders to MARCH, forwards assignments to SORD, and also maintains Service Order history and manages changes.

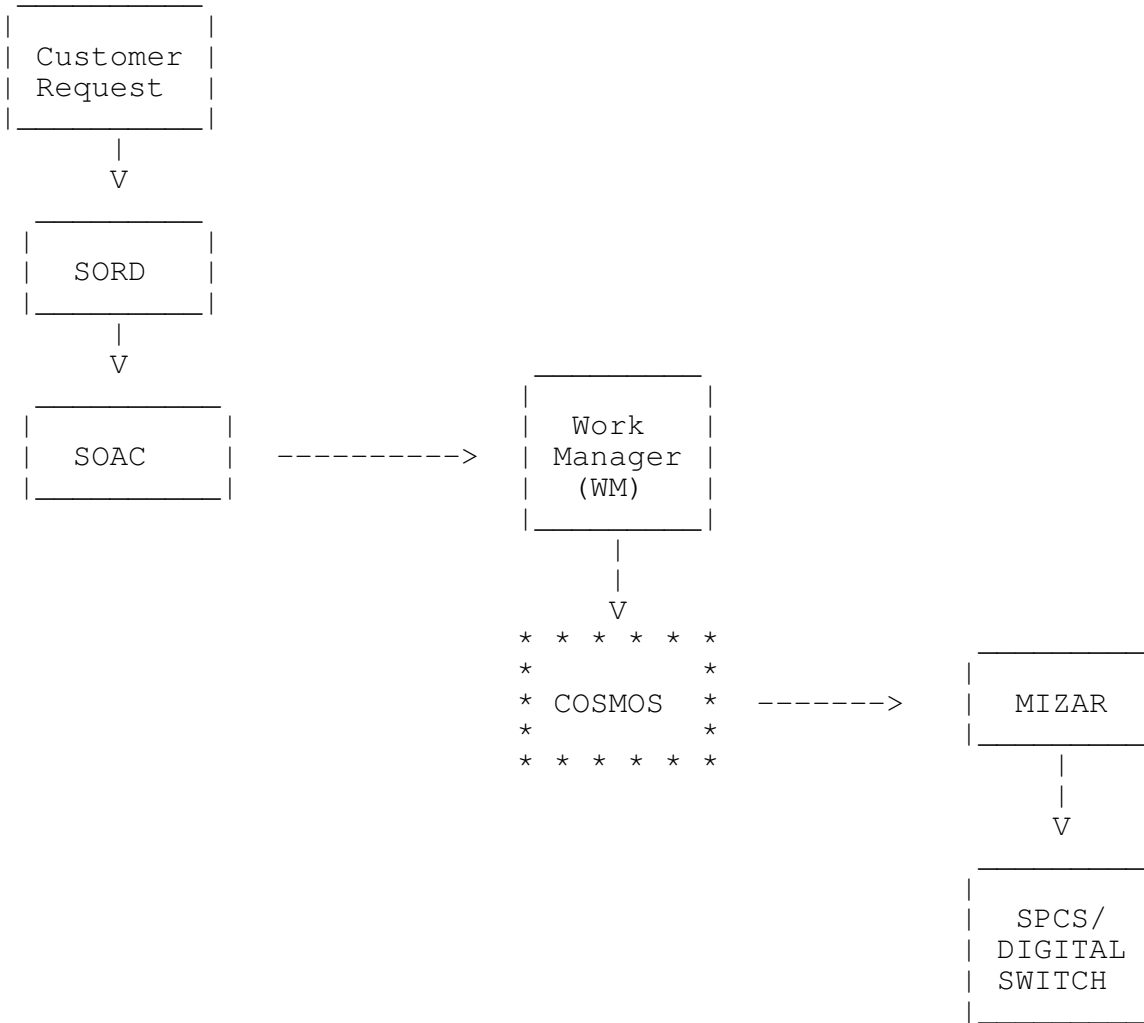
LFACS - Loop FACS contains all loop facilities inventory and responds to requests for assignment.

COSMOS - Computer System for Mainframe OperationS contains all the OE inventory and responds for OE request.

SORD - Service Order and Distribution distributes Service Orders throughout the system.

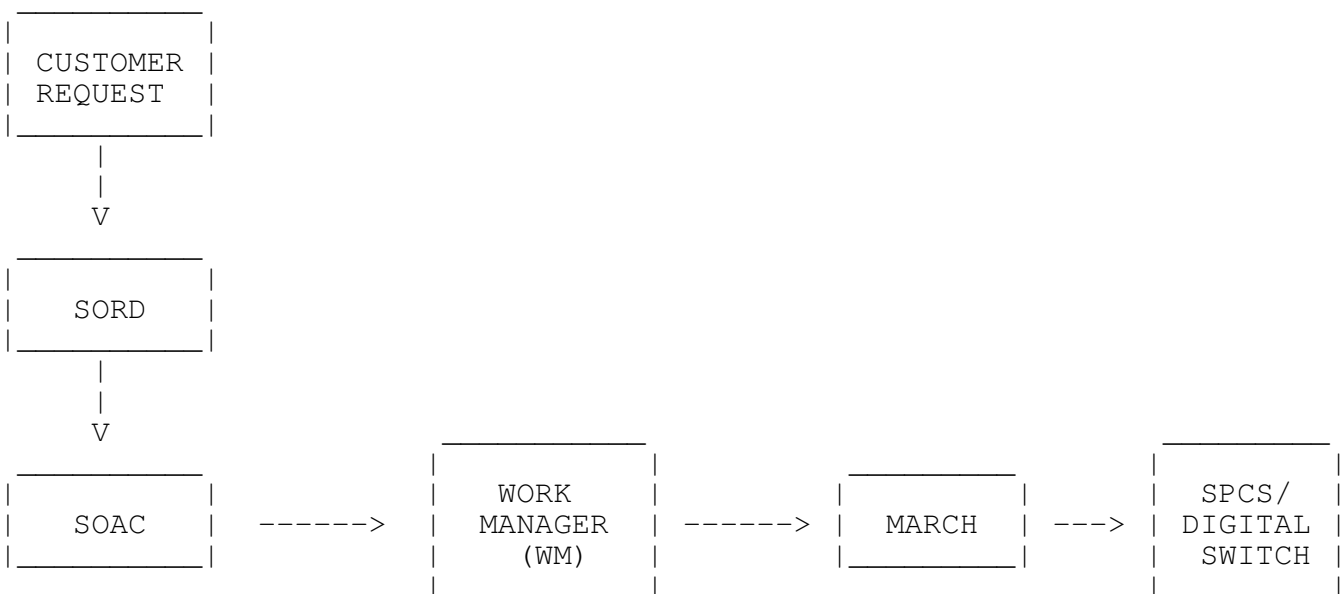
MARCH - MARCH is the Mizar upgrade which will come into play when the Stromberg-Carlson (SxS and XBAR) is upgraded to Generic 17.1 (the software interface is called NAC). Though there is a problem with the interface between MARCH and COSMOS (because the Generic Interface is not supported by COSMOS), templates are used for MAN, AGE, LETS, etc. Anyway, MARCH plays a big part in this system. MARCH, aside from what was talked about above, has a basic function of keeping RCMAC up to date on the switches (MSR user transaction). It is an RC message manager which will allow one to modify messages (ORE), show usages (MAR) and logs all transmissions.

~~~~~  
PHASE I - COSMOS/MIZAR



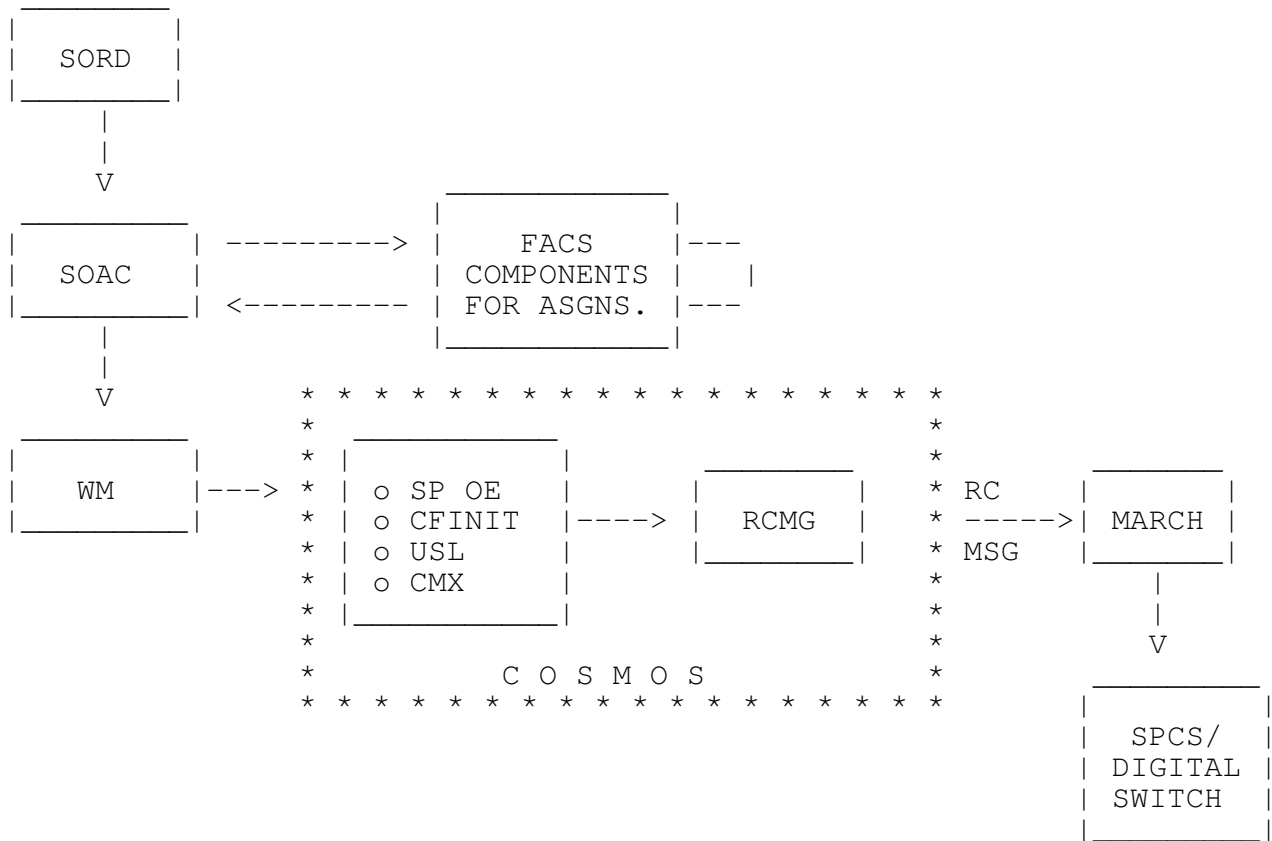
---

PHASE II - SOAC/MARCH



... Then There Was MLAC

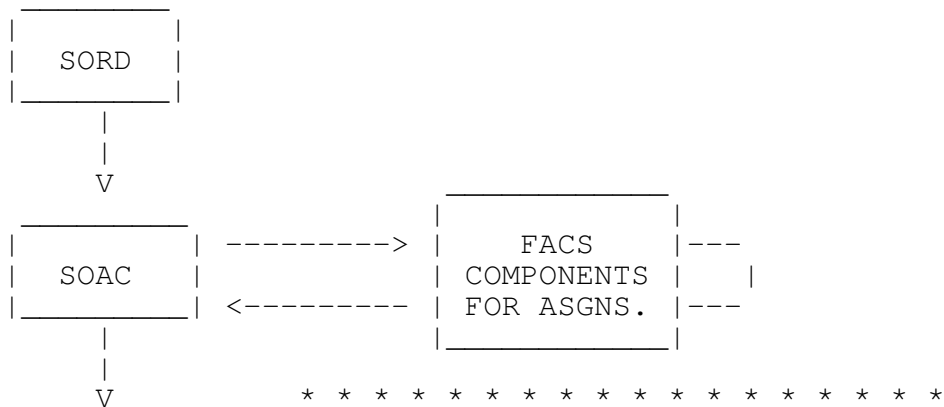
With conversion to FACS, a shift in the service order provisioning process was made from manual input by the LAC and NAC to mechanized data flow from SOAC to COSMOS (via Work Manager). Tables used for Recent Change (CFINIT, USL, and CXM) and spare OE assignments reside in COSMOS, along with the Recent Change Message Generator (RCMG). The LAC and NAC are now involved only on an exception basis (This will be explained in more detail later on).

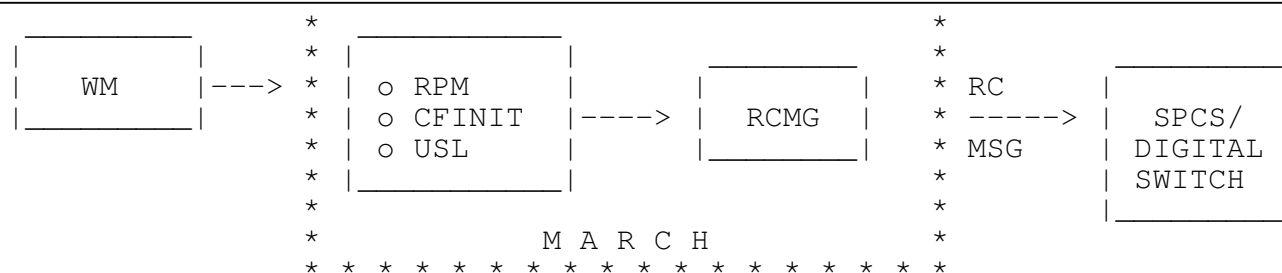


. . . NOW THERE IS SOAC/MARCH

With the SOAC/MARCH application (FACS/MARCH configuration), the primary source of service order data continues to be SOAC. COSMOS is taken out of the Recent Change business with this application (except, like the LAC and NAC, on an exception basis) and becomes just another FACS Component. The tables that resided in COSMOS or Recent Change are now duplicated in MARCH.

Instead of retrieving, storing, and passing on already-formatted Recent Change messages, MARCH now generates the Recent Change from the data passed from SOAC, as did COSMOS previously.





## E. Getting Ready For Recent Change Message

~~~~~  
STARTING WITH SORD

Service Orders (SORD) contain FIDs and USOCs (Universal Service Order Codes [these codes tell the type of service the customer may have or get]) followed by data specific to a customer's service request (SORD accesses PREMIS for telephone number and address data; other entries are made by the Service Representative). The order is then passed to SOAC.

THEN TO SOAC

SOAC uses internal tables to read the FIDs and USOCs passed by SORD to determine what information is required from the various components of FACS. SOAC then accesses the appropriate FACS components (LFACS for Cable Pair assignment; COSMOS for OE assignment) and gathers the required data.

Once all the data has been collected, SOAC passes the information to the Work Manager. Data is either passed as is or translated by SOAC (again using internal tables) into language acceptable to the receiving systems (i.e., COSMOS and MARCH).

SOAC passes information intended for MARCH in one of two ways:

TP-Flow-Through Translation Packets

Translation Packets (TPs) contain fully translatable data from which MARCH can generate a Recent Change message. Determination is made by SOAC based on the interface capabilities and its ability to read, translate as required, and pass data.

Service Order Image

Service Order Images are sent to MARCH if SOAC is not able to pass all required data. Images require additional information, either input manually or retrieved from COSMOS before Recent Change messages are generated.

WORK MANAGER - THE TRAFFIC COP

The primary function of Work Manager is to read the service order and determine where the data must be sent. Decisions include:

COSMOS System	MARCH System
COSMOS Wire Center	MARCH Switch
COSMOS Control Group	Serving RCMA

Work Manager passes the service order data to MARCH on a real time basis (orders that were previously held in COSMOS until requested by Frame Due Date [FDD] are now held in MARCH), either as a TP or an Image.

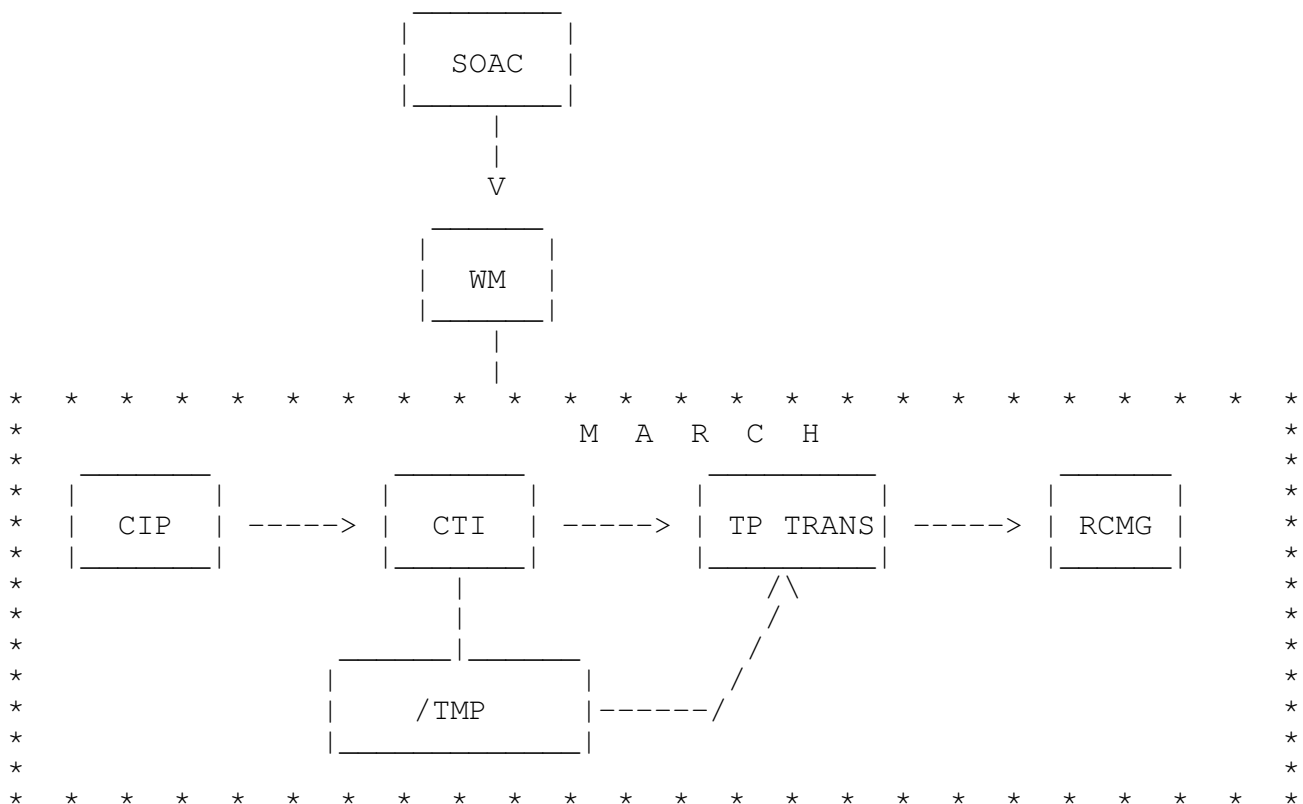
1. When MARCH Receives A Translation Packet (TP)

~~~~~

- (1) A Translation Packet, passed from SOAC via Work Manager is received in MARCH by the CIP, Communication Interface Program.
- (2) When data is received by the CIP, it calls up the CTI or Job Control Module. The Job Control Module or CTI writes the data that is received to a temporary file and informs TP Trans (Translation Translator) that an order has been received. It also controls the number of simultaneous jobs submitted to TPTrans.
- (3) TPTrans analyzes the order in the temporary file, does appropriate FID conversion (such as stripping out dashes), reformats the order, and passes it to the Recent Change Message Generator (RCMG).
- (4) RCMG performs all Recent Change message generation and, upon completion, writes the order into a MARCH pending file (Pending Header or Review file).

In addition to the data passed from SOAC, RCMG uses the following data in MARCH to translate into switch-acceptable messages:

|                |                                  |
|----------------|----------------------------------|
| NXX            | Switch Specific Parameters (RPM) |
| USOC (RPM)     | CCF Keywords (CFINIT)            |
| USOC/NXX (RPM) | Review Triggers (RVT)            |
|                | Release Times (SRM)              |



## 2. When MARCH Receives A Service Order Image

~~~~~

- (1) A Service Order Image, passed from SOAC via Work Manager is received in MARCH by the CIP, Communication Interface Program.
- (2) When the image is received by the CIP, it calls up the CTI or Job Control Module. The Job Control Module or CTI writes the data that is received to a temporary file and informs TP TRANS (Translation Translator) that an

Though it is trivial to understand just how all these system work, here is a rough overview of MARCH. To Cover MARCH, this will first cover the background processing.

F. MARCH Background Processing

~~~~~

##### RECENT CHANGE PARAMETER (RPM)

In conjunction with ORI Patterns and Recent Change Templates, the RPM determines how information from SOAC is changed and/or manipulated to create acceptable switch Recent Change messages.

RCMA Supervisor has overall responsibility for the RPM. Although specific categories may be maintained by Staff Manager, it is overviewed by RCMAC as a whole.

This includes Line Class Code (LCC) conversion data previously under the sole responsibility of the NAC in COSMOS. It requires a change of procedures for the RCMA to ensure proper LCC information is passed on the RPM and updated appropriately.

Initial USOC is LCC conversion data and will be copied into MARCH from the COSMOS USOC Table.

##### SWITCH RELEASE MANAGER (SDR)

With SOAC/MARCH, it no longer determines the types of orders to be pulled from COSMOS, and thus establishes the date and time orders are to be released to the switch, coming both from SOAC and from COSMOS.

It is based on Package Type (PKT) and Package Category (PKC)

##### SWINIT TRANSACTION

Contains switch-specific data for MARCH to communicate with SOAC (via Work Manager), COSMOS, and the switch.

Establishes the call times for COSMOS.

- RCP by Order Number for Service Order Images.
- Suspends, Restores, and Nonpayment Disconnects.
- Automated AGE Requests (as applicable).
- Automated MAN Report.

##### SDR - SWITCH DATA REPORT

SDR is a report transaction intended for use by the RCMA Associate.

The Switch Data Report provides a printout of the SWINIT information that was populated from the Perpetrations Questionnaire submitted by the RCMA Supervisor (see Order Description part of this file).

##### MOI of an Order in History

Orders in the History Header (HH) file will reflect the history source. The history source indicated how the order was written to the history file.

#### G. User Transaction in MARCH

~~~~~

Most Commonly Used MARCH Commands

.-----.				
Transaction	Name	Function	Search keys	Prompts

MSR <CR>	MARCH Status Report	office status	. <CR> sw address	----
MOI <CR>	MARCH Order Inquiry	status of order, tn, file	fn rv fn rj fn hh/adt xx-xx so n12345678 tn xxxxxxxx	----
ONC <CR>	On Line COSMOS	Access COSMOS	-----	login password
ONS <CR>	On Line Switch	Access Switch	-----	Switch logon
ORE <CR>	Order Edit	Edit Header or message text of MARCH file	fn rv fn rj so n12345678 tn xxxxxxxx	----
ORE -G <CR>	Order Edit Global	edit multiple files	2 Search keys Required	----
ORI <CR>	Order Input	Build MARCH file	-----	Patterns
ORS <CR>	Order Send	Send to Switch immediately	so n12345678 tn xxxxxxxx	----
TLC <CR>	Tail COSMOS	watch MARCH pull orders	-----	----
TLS <CR>	Tail Switch	Watch orders sent to switch	-----	-----
VFY <CR>	Verify	Request Verify	-----	rltm,type tn,oe,hml
VFD <CR>	Verify Display	Show Completed verifies	-----	----
VFS <CR>	Verify Status	Show pending verities	-----	

Here is a detailed explanation of some of the commands:

MOI - MARCH ORDER INQUIRY

MOI is a conversational inquiry transaction intended for use by the RCMAC Clerk.

MOI is used to inquire on Recent Change messages in a pending file(s): Pending Header, Review, Reject, and/or History Header. It may be used to inquire on one message, an entire order, several messages in more than one file, or all orders in a file, determined by the search keys entered.

ONS - ON line Switch

Each switch has its own login sequence.

Login

- 1) Give a Hard Break
- 2) At the "?" prompt type "login"
- 3) There will be an "Enter User Name" prompt. Enter the user name.
- 4) Then "Enter Password" with a row of @, *, & and # covering the password.
- 5) Once on, type "SERVORD" and you are on the RC channel of the switch.

Logout

- 1) Type "LOGOUT" and CONTROL-P

1AESS

Login

- 1) Set Echo on, Line Feeds on and Caps Lock on.
- 2) End each VFY message with " . CONTROL-D" and each RC message with " ! CONTROL-D".

Logout

- 1) Hit CONTROL-P

5ESS

Login

- 1) Type "rcv:menu:apprc" at the "<" prompt.

Logout

- 1) Type "Q" and hit CONTROL-P

ONC - On Line COSMOS

- 1) You will see "login:" so type in username and then there will be a "Password:" prompt to enter password.

ORE - Order Edit

ORE Commands are used to move between windows and to previous and subsequent headers and text within an editing session. Commands may be input at any point in the ORE session regardless of the cursor location. They are capital letters requiring use of the shift key or control commands. Here are the movement commands:

Commands ~~~~~	Description ~~~~~
N (ext header)	Replaces the data on the screen with the next header and associated text that matches the search keys entered.
M (ore text)	Replaces the data in the message text window with the next message associated with the existing header (for multiple text message).
P (revious header)	Replaces data in the header windows with the header you looked at previously (in the same editing session).
B (ackup text)	Replaces data in the message text window with the text you looked at previously (in the same editing session).
S (earch window)	Moves the cursor to the search window permitting additional search keys to be entered.
Control-D	Next Page
Control-U	Previous Page
<	Move cursor from text window to header.
>	Moves to text window from header.
Q (uit)	Quit

ORE -G

ORE -G is a conversational transaction intended for use by the RCMA

associate.

ORE -G is used to globally edit Recent Change messages existing in a MARCH pending file: Pending Header, Review, and Reject. Editing capabilities include adding information on an order.

ORE -G is also used to change header information and to remove messages.

ORI - ORder Input

ORder Input enables one to input an order and change orders. The changes that can be made are in the telephone number, OE, so on. This command is too complex to really get into here.

VFY - Verify

This is used to manually input verify messages into MARCH, thus to the switches.

MSR - MARCH Status Report

This used to count the amount of service orders stored in SOAC. It also shows the amount of change messages that have been sent to the switch.

H. Service Order Forms

~~~~~

In my time, I have come across a lot of printouts that have made no sense to me. After several months, I could start to understand some of the codes. Here are what some of the common service orders are and what they are for.

#### SORD Service Order:

```
|
|
|TN          CUS TD      DD      APT MAC ACC AO      CS  SLS      HU
|415-343-8765 529 T      DUE      W          AS OF 1FR ABCDE4W
|ORD          SU      EX      STA APP CD      IOP CT TX RA SP CON AC
|C14327658      SMIUX      R          R
|ACNA  R
|WA          343# EXETER, SMT
|WN          IDOL, BILLY
|---S&E
|I1          ESL
|O1          1FR/TN 343-8321/ADL
|          /PIC 10288
|O1          ESL/FN 3438321
|---BILL
|MSN  IDOL, BILLY
|MSTN 555-1212
|---RMKS
|RMK   BLAH
|
|          /**** END
|
|
```

```
|
| [1]          [2]          [3]          [9]
| |          |          |          |
|TN          CUS TD      DD      APT MAC ACC AO      CS  SLS      HU
|407-343-8765 529 T      DUE      W          AS OF 1FR ABCDE4W
|
```

```

| [8]
| |
| ORD          SU    EX      STA APP CD      IOP CT TX RA SP CON AC
|C14327658      SMIUX      R              R
|ACNA  R
|
| [4]
| |
|WA      343# EXETER, SMT
|
| [6]
| |
|WN      AT&T
|---S&E
|I1      ESL
|O1      1FR/TN 343-8321/ADL      [5]
|        /PIC 10288
|O1      ESL/FN 3438321      /
|---BILL
|
| [6]
| |
| MSN      IDOL, BILLY
|
| [7]
| |
| MSTN      555-1212
|---RMKS
|RMK      BLAH
|
|        /**** END

```

- [1] Telephone Number. Format is XXX-XXX-XXXX.
- [2] Customer number.
- [3] Due Date.
- [4] Work Address.
- [5] The S&E field:

ACTION CODE -- This is the code at the far left-most side of the page. These codes end with a 1 or a 0. The 1 says to add this feature and the 0 says to not do the feature. There are several different action codes. Here is a list:

| Action Code | Used to                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------|
| ~~~~~       | ~~~~~                                                                                                   |
| I           | Add features                                                                                            |
| O           | Remove features                                                                                         |
| C-T         | Change designated number of rings, "forward to" number, or both on Busy/Delay call forwarding features. |
| E-D         | Enter or Delete a feature for record purposes only.                                                     |
| R           | Recap CCS USOC to advise                                                                                |

Here is a list of some common USOCs (features):

|     |                      |
|-----|----------------------|
| ESC | Three Way Calling    |
| ESF | Speed Calling        |
| ESL | Speed Calling 8 Code |
| ESM | Call Forwarding      |
| ESX | Call Waiting         |
| EVB | Busy Call Forward    |

|       |                            |
|-------|----------------------------|
| EVC   | Bust Call Forward Extended |
| EVD   | Delayed Call Forwarding    |
| HM1   | Intercom Plus              |
| HMP   | Intercom Plus              |
| MVCCW | Commstar II Call Waiting   |

[6] Billing name  
[7] Billing number  
[8] Service Order Number  
[9] Class of Service or LCC (See appendix 1)

#### SDR File Header Information Order (MARCH)

|                         |                         |
|-------------------------|-------------------------|
| 1. Switchname           | 7. Package Type         |
| 2. Header File Name     | 8. Package Category     |
| 3. Current Date & Time  | 9. Reject Reason        |
| 4. Service Order Number | 10. Release Date & Time |
| 5. Service Order Type   | 11. Accept Date & Time  |
| 6. Telephone Number     | Reject Date & Time      |
|                         | 12. Input Source        |

#### History Header File

|                       |                                 |                                      |
|-----------------------|---------------------------------|--------------------------------------|
| [1]<br> <br>sw: swad0 | [2]<br> <br>history header file | [3]<br> <br>fri may 31 07:50:12 1992 |
|-----------------------|---------------------------------|--------------------------------------|

[4]- so=janet3                      tn=                      pkt-in                      pkc=other  
[11]- act=05-30 0750              src=ori                      |                      |                      |  
history text=                      [6]                      [7]                      [8]  
rc:sclist:                      [12]  
ord 31235  
cx =031235  
adn 2  
! ~

#### Reject File

|               |                  |                               |
|---------------|------------------|-------------------------------|
| [1]- sw:swad2 | [2]- reject file | [3]- fri may 30 11:22:01 1992 |
|---------------|------------------|-------------------------------|

[4]- so=c238                      [5]- ver=7    tn=5551212    -[6]  
[9]- rj reason=ot              rldt=05-30 1059              rjdt=05-30 :106    src=cosmos  
message test=                      |                      |                      |  
rc:line:chg:                      [10]                      [11]                      [12]  
ord 87102  
"=238-7102'  
"ord c231"  
"restoration from ssv-db"  
tn 555 1212  
lcc 1mr  
! ~  
ve data=  
  , er  
  
m 07 rc18 0 87102 0 4 valar  
  new 00001605 err 00000307  
  05/30/92 11:07:16

I. COSMOS Service Order From The SOI Command  
~~~~~

WC%
WC% SOI
H ORD N73322444

DEC 19, 1992 10:12:21 AM
SERVICE ORDER ASSIGNMENT INQUIRY

ORD N73322444-A OT(NC) ST(AC-) FACS(YES)
DD(12-20-92) FDD(12-20-92) EST(11-16:14) SG(G) DT(XX) OC(COR)
MDF WORK REQ(YES) MDF COMPL(NO) LAC COMPL(NO) RCP(NO)
WPN 9446 WLST 1= P 2= 3= 4= 5= 6= 7= 8=
COORDINATION REQUIRED
RMK FAT TBCC,RO D77901070
RMK FAT TBCC,RO D77901070

CP 48-0942
ST SF PC FS WK DATE 11-28-89 RZ 13
LOC PF01008

OE 012-25-006
ST SF PC FS WK DATE 11-12-91 CZ 1MB US 1MS FEA TNNL
PIC 10288
LCC BB1
CCF ESX
LOC PF01007

TN 571-5425
ST WK PD FS WK DATE 12-03-91 TYPE X
**ORD D77901070-C OT CD ST AC- DD 12-20-92 FDD 12-20-92

** SOI COMPLETED
WC%

WC%
WC% SOI

H ORD N73322444

[1]- DEC 19, 1992 10:12:21 AM
[2]- SERVICE ORDER ASSIGNMENT INQUIRY

[3] [4] [5]
| | |
ORD N73322444-A OT(NC) ST(AC-) FACS(YES)
[7] [8] [6] [9]
| | | |
DD(12-20-92) FDD(12-20-92) EST(11-16:14) SG(G) DT(XX) OC(COR)
[10] [11] [12] [13]
| | | |
MDF WORK REQ(YES) MDF COMPL(NO) LAC COMPL(NO) RCP(NO)

WPN 9446 WLST 1= P 2= 3= 4= 5= 6= 7= 8=
COORDINATION REQUIRED
RMK FAT TBCC,RO D77901070
RMK FAT TBCC,RO D77901070

[35]
|

CP	48-0942					
	[34]		[35]	[36]		[37]
	ST SF	PC	FS WK	DATE 11-28-89	RZ	13
	LOC PF01008 -[39]					
OE	012-25-006 -[19]					
	[20]		[21]	[22]	[23]	[24]
	ST SF	PC	FS WK	DATE 11-12-91	CS 1MB	US 1MS
						[25]
						FEA TNNL
	PIC 10288					
	LCC BB1 -[27]					
	CCF ESX -[26]					
	LOC PF01007 -[32]					
TN	571-5425 -[14]					
	[15]	[16]	[17]		[18]	
	ST WK	PD FS WK	DATE 12-03-91	TYPE	X	
	[38]		[28]	[29]	[30]	[31]
	**ORD D77901070-C		OT CD	ST AC-	DD 12-20-92	FDD 12-20-92
**	SOI COMPLETED -[40]					
WC%	-[41]					

- [1] Date and Time the SOI was Requested in COSMOS
 - [2] Title of Output Message
 - [3] Order Number
 - [4] Order Type
 - [5] Status of Order
 - [6] EST (11-16:14) When Service Order was Established into COSMOS
 - [7] Due Date
 - [8] Frame Due Date
 - [9] Segment Group
 - [10] Main Distributing Frame Work Required
 - [11] Main Distributing Frame Work Complete
 - [12] Loop Assignment Center Completed
 - [13] FACS Y
- >-- The order has downloaded from SOAC to MARCH (MARCH)
- RCP N
- [14] Telephone Number
 - [15] Present State of Telephone Number
 - [16] Future Status of Telephone Number
 - [17] Date of Last Activity on Telephone Number
 - [18] Type of Telephone Number
 - [19] Line Equipment
 - [20] Present Status of Line Equipment
 - [21] Future Status of Phone Line
 - [22] Date of Last Activity on Line Equipment

- [23] Class of Service
- [24] USOC
- [25] Features
- [26] Custom Calling Feature
- [27] Line Class Code
- [28] Order Type that is Clearing Telephone Number
- [29] Status of Order that is Clearing Telephone Number
- [30] Due Date
- [31] Frame Due Date
- [32] Location of Line Equipment on Frame
- [33] Cable and Pair
- [34] Present Status of Cable and Pair
- [35] Future Status of Cable and Pair
- [36] Date of Last Activity on Cable and Pair
- [37] Resistance Zone
- [38] Order Number Clearing Cable
- [39] Location of Cable and Pair on Frame
- [40] SOI Complete Message
- [41] Wire Center and Prompt Symbol to Indicate Computer is Ready for Another Transaction
- [42] Primary Independent Carrier is 10288 (AT&T's Ten Triple X Code)

J. MSR - MARCH Status Report (MARCH)

~~~~~

switch name

| =====                  |                          |           |            |
|------------------------|--------------------------|-----------|------------|
| march status report    |                          |           |            |
| sw:switch name         | tue oct 30 11:14:48 1992 |           |            |
| pending work functions |                          |           |            |
| =====                  |                          |           |            |
|                        | past due                 | due today | future due |
| use moi for:           | 0                        | 0         | 0          |
| reject file            | 0                        | 1         | 270        |
| review file            | 0                        | 0         | 0          |
| held release status    | 28                       | 14        | 44         |
| normal release status  | 0                        | 7         | 184        |
| =====                  |                          |           |            |
| use pac for:           | 0                        | 15        |            |
| change notices         | 0                        | 3         |            |
| unknown switch notices | 0                        | 0         |            |
| =====                  |                          |           |            |

\*\* msr completed

switch name

|                |                               |     |      |
|----------------|-------------------------------|-----|------|
| =====          |                               |     |      |
| [1]            | march status report           |     |      |
|                | [2]- tue oct 30 11:14:48 1992 |     |      |
| sw:switch name | pending work functions        |     |      |
| =====          |                               |     |      |
|                | [3]                           | [5] | [12] |
|                |                               |     |      |

|                        | past due | due today | future due |
|------------------------|----------|-----------|------------|
| use moi for:           | 0        | 2 -[6]    | 0          |
| reject file            | 0        | 1 -[7]    | 0          |
| held release status    | 5 -[4]   | 6 -[8]    | 0          |
| normal release status  | 0        | 3 -[9]    | 3 -[13]    |
| use pac for:           | 0        | 15 -[10]  |            |
| change notices         | 0        | 3 -[11]   |            |
| unknown switch notices | 0        | 0         |            |
| =====                  |          |           |            |
| ** msr completed       |          |           |            |

- [1] Office MSR request in (switch name/address)
- [2] Date and time of request
- [3] Past due service order column
- [4] Past due service order on hold
- [5] Due today service order column
- [6] Order due today in the reject file
- [7] Orders due today in review file
- [8] Orders due today on hold
- [9] Orders due today with a normal release status
- [10] PAC service orders which have been changed
- [11] PAC switch advisory notices encountered today
- [12] Future due service order column
- [13] Order due in the future with a normal release status

#### K. Other Notes

~~~~~

LCC or Line Class Code is, in short, what kind of line the Bell customer may have. They are the phone line type ID. These IDs are used by the SCC (Switching Control Center) and the switches as an ID to what type of billing you have. Here is a list of some common LCCs that a standard BOC uses.

Note: This is not in stone. These may change from area to area.

1FR - One Flat Rate
1MR - One Measured Rate
1PC - One Pay Phone
CDF - DTF Coin
PBX - Private Branch Exchange (Direct Inward Dialing ext.)
CFD - Coinless ANI7 Charge-a-Call
INW - InWATS
OWT - OutWATS
PBM - 0 HO/MO MSG REG (No ANI)
PMB - LTG = 1 HO/MO Regular ANI6

L. Recommended Reading

~~~~~

Agent Steal's file in LODTJ #4  
Acronyms 1988 [from Metal Shop Private BBS] (Phrack 20, File 11)  
Lifting Ma Bell's Cloak Of Secrecy by VaxCat (Phrack 24, File 9)



Volume Four, Issue Forty, File 8 of 14

-- John Guinasso, director of global network security for Tymnet parent BT North America in Information Week (July 13, 1992, Page 15).

Welcome to Tymnet!

- A. BT Tymnet Access Location Index
- B. BT-GNS Access Within Regional Bell Operating Companies
  - 1. Bell Atlantic
  - 2. BellSouth
  - 3. Pacific Bell
  - 4. Southwestern Bell
  - 5. Southern New England Telephone
- C. Database or Timesharing Companies on Tymnet
- D. Service Classifications For Database or Timesharing Companies Using Tymnet
- E. Summary of Global Network Services By Country
- F. Terminal Identifiers
- G. Login Options

- ## H. BT-GNS Worldwide Asynchronous Outdial Service

- ## I. BT-GNS Worldwide Access Sorted By Node

### A. BT Tymnet Access Location Index

~~~~~

Country	Abbrev.	Country	Abbrev.
ANTIGUA	ATG	HONG KONG	HKG
ARGENTINA	ARG	ISREAL	ISR
AUSTRALIA	AUS	ITALY	ITA
AUSTRIA	AUT	JAMAICA	JAM
BAHAMAS	BHS	JAPAN	JPN
BAHRAIN	BHR	KOREA	KOR
BARBADOS	BRB	NETHERLANDS	NLD

BELGIUM	BEL	NORTHERN MARIANAS	SAP
BERMUDA	BMU	PANAMA	PAN
CANADA	CAN	PERU	PER
CAYMAN ISLANDS	CAY	PHILIPPINES	PHL
COLUMBIA	COL	PURERTO RICO	PRI
DENMARK	DNK	SWEDEN	SWE
DOMINICAN RPUBLIC	DOM	SWITZERLAND	CHE
EGYPT	EGY	TRINIDAD AND TOBAGO	TTO
FRANCE	FRA	UNITED KINGDOM	GBR
GREECE	CRC	URUGUAY	URY
GUAM	GUM	USA	USA
GUATEMALA	GTM	VIRGIN ISLANDS	VIR
HONDURAS	HND	WEST GERMANY	DDR

B. BT-GNS Access Within Regional Bell Operating Companies

TYMNET has gateways into many of the Regional Bell Operating Companies' packet networks. For specifics on how to access these networks, please refer to the information listed at the end of this listing.

NODE	CITY	PROV			DIALUP ACCESS				ACCESS NO.	M N P	COMMENTS
		ST	CNTRY	DENS	100's bps						
					3	12	24	96			
02275	Birmingham	AL	USA	MED	B	B	C		205/822-8629	N	@PLSK
03306	Berkeley	CA	USA	MED	B	B			510/548-2121	N	@PPS
03306	Berkeley	CA	USA	MED			C		510/548-5743	N	@PPS
06272	El Segundo	CA	USA	MED	B	B			310/640-8548	N	@PPS
06272	El Segundo	CA	USA	MED			C		310/640-0350	N	@PPS
06272	Fullerton	CA	USA	MED	B	B			714-441-2777	N	@PPS
06272	Fullerton	CA	USA	MED			C		714/441-1839	N	@PPS
06272	Inglewood	CA	USA	MED	B	B			310/216-7667	N	@PPS
06272	Inglewood	CA	USA	MED			C		310/216-4469	N	@PPS
06272	Los Angeles	CA	USA	MED	B	B			213/480-1677	N	@PPS
06272	Los Angeles-Downtn.	CA	USA	MED	B	B			213/687-3727	N	@PPS
03306	Mountain View	CA	USA	MED	B	B			415/960-3363	N	@PPS
03306	Mountain View	CA	USA	MED			C		415/961-2102	N	@PPS
03306	Oakland	CA	USA	MED	B	B	C		510/893-9889	N	@PPS
03306	Palo Alto	CA	USA	MED	B	B			415/325-4666	N	@PPS
03306	Palo Alto	CA	USA	MED			C		415/323-2019	N	@PPS
06272	Pasadena	CA	USA	MED	B	B			818-356-0780	N	@PPS
06272	Pasadena	CA	USA	MED			C		818/356-0487	N	@PPS
03306	San Francisco	CA	USA	MED	B	B			415/362-2280	N	@PPS
03306	San Francisco	CA	USA	MED	B	B	C		415/543-8275	N	@PPS
03306	San Francisco	CA	USA	MED	B	B			415/626-5380	N	@PPS
03306	San Francisco	CA	USA	MED	B	B	C		415/626-7477	N	@PPS
03306	San Francisco	CA	USA	MED			C		415/362-7579	N	@PPS
03306	San Jose	CA	USA	MED	B	B			408-920-0888	N	@PPS
03306	San Jose	CA	USA	MED			C		408/298-0584	N	@PPS
06272	Santa Ana	CA	USA	MED	B	B			714-972-9844	N	@PPS
06272	Santa Ana	CA	USA	MED			C		714/972-2314	N	@PPS
06272	Van Nuys	CA	USA	MED	B	B			818-780-1066	N	@PPS
06272	Van Nuys	CA	USA	MED			C		818/780-5468	N	@PPS
02727	Bridgeport	CT	USA	MED	B	B	C		203/366-6972	N	@CONNNET
02727	Bristol	CT	USA	MED	B	B	C		203/589-5100	N	@CONNNET
02727	Canaan	CT	USA	MED	B	B	C		203/824-5103	N	@CONNNET
02727	Clinton	CT	USA	MED	B	B	C		203/669-4243	N	@CONNNET
02727	Danbury	CT	USA	MED	B	B	C		203/743-2906	N	@CONNNET
02727	Danielson	CT	USA	MED	B	B	C		203/779-1880	N	@CONNNET
02727	Hartford/Middletown	CT	USA	MED	B	B	C		203/724-6219	N	@CONNNET
02727	Meriden	CT	USA	MED	B	B	C		203/237-3460	N	@CONNNET

02727	New Haven	CT	USA	MED	B	B	C	203/776-1142	N	@CONNNET
02727	New London	CT	USA	MED	B	B	C	203/443-0884	N	@CONNNET
02727	New Milford	CT	USA	MED	B	B	C	203/355-0764	N	@CONNNET
02727	Norwalk	CT	USA	MED	B	B	C	203/866-5305	N	@CONNNET
02727	Norwich/New London	CT	USA	MED	B	B	C	203/443-0884	N	@CONNNET
02727	Old Greddwich	CT	USA	MED	B	B	C	203/637-8872	N	@CONNNET
02727	Old Saybrook	CT	USA	MED	B	B	C	203/388-0778	N	@CONNNET
02727	Seymour	CT	USA	MED	B	B	C	203/881-1455	N	@CONNNET
02727	Stamford	CT	USA	MED	B	B	C	203/324-9701	N	@CONNNET
02727	Storrs	CT	USA	MED	B	B	C	203/429-4243	N	@CONNNET
02727	Stratford/Bridgeport	CT	USA	MED	B	B	C	203/366-6972	N	@CONNNET
02727	Torrington	CT	USA	MED	B	B	C	203/482-9849	N	@CONNNET
02727	Waterbury	CT	USA	MED	B	B	C	203/597-0064	N	@CONNNET
02727	Willimantic	CT	USA	MED	B	B	C	203/456-4552	N	@CONNNET
02727	Windsor	CT	USA	MED	B	B	C	203/688-9330	N	@CONNNET
02727	Windsor Lcks/Enfield	CT	USA	MED	B	B	C	203/623-9804	N	@CONNNET
06254	Washington	DC	USA	MED	B	B		202/328-0619	N	@PDN
06254	Washington	DC	USA	MED	B	B		202/479-7214	N	@PDN
06254	Washington	DC	USA	MED	B	B		202/546-5549	N	@PDN
06254	Washington (Downtown	DC	USA	MED	B	B		202/393-6003	N	@PDN
06254	Washington (Midtown)	DC	USA	MED	B	B		202/293-4641	N	@PDN
03526	Dover	DE	USA	MED	B	B	C	410/734-9465	N	@PDN
03526	Georgetown	DE	USA	MED	B	B	C	302/856-7055	N	@PDN
03526	Newark	DE	USA	MED	B	B	C	302/366-0800	N	@PDN
03526	Wilmington	DE	USA	MED			C	302/655-1144	N	@PDN
03526	Wilmington	DE	USA	MED	B	B		302/428-0030	N	@PDN
04125	Boca Raton	FL	USA	MED	B	B		407/392-4801	N	@PLSK
04125	Ft. Pierce	FL	USA	MED	B	B		407/461-0996	N	@PLSK
07064	Jacksonville	FL	USA	MED	B	B	C	904/354-1032	N	@PLSK
04125	Miami	FL	USA	MED	B	B	C	305/661-0437	N	@PLSK
04125	Plantation	FL	USA	MED	B	B	C	305/791-5663	N	@PLSK
07064	St. Augustine	FL	USA	MED	B	B		904/825-1101	N	@PLSK
04125	Stuart	FL	USA	MED	B	B		407/288-0185	N	@PLSK
04125	W. Hollywood	FL	USA	MED	B	B		305/962-8226	N	@PLSK
04125	W. Palm Beach	FL	USA	MED	B	B	C	407/842-8990	N	@PLSK
10200	Athens	GA	USA	MED	B	B	C	404/613-1289	N	@PLSK
10200	Atlanta	GA	USA	MED	B	B		404/261-4633	N	@PLSK
10200	Atlanta	GA	USA	MED	B	B	C	404/266-9403	N	@PLSK
10200	Columbus	GA	USA	MED	B	B		404/324-5771	N	@PLSK
10200	Rome	GA	USA	MED	B	B		404/234/6542	N	@PLSK
05443	Hays	KS	USA	MED	B	B		913/625-8100	N	@MRLK
05443	Hutchinson	KS	USA	MED	B	B		316/669-1052	N	@MRLK
05443	Kansas City	KS	USA	MED	B	B		316/225-9951	N	@MRLK
05443	Lawrence	KS	USA	MED	B	B		913/841-5580	N	@MRLK
05443	Manhattan	KS	USA	MED	B	B		913/539-9291	N	@MRLK
05443	Parsons	KS	USA	MED	B	B		316/421-0620	N	@MRLK
05443	Salina	KS	USA	MED	B	B		913/825-4547	N	@MRLK
05443	Topeka	KS	USA	MED	B	B		913/235-1909	N	@MRLK
05443	Wichita	KS	USA	MED	B	B		316/269-1996	N	@MRLK
06254	Bethesda	MD	USA	MED	B	B		301/986-9942	N	@PDN
06254	Colesville	MD	USA	MED	B	B	C	301/989-9324	N	@PDN
06254	Hyattsville	MD	USA	MED	B	B		301/779-9935	N	@PDN
06254	Laurel	MD	USA	MED	B	B	C	301/490-9971	N	@PDN
06254	Rockville	MD	USA	MED	B	B		301/340-9903	N	@PDN
06254	Silver Spring	MD	USA	MED	B	B		301/495-9911	N	@PDN
04766	Bridgeton/St. Louis	MO	USA	MED	B	B		314/622-0900	N	@MRLK
04766	St. Louis	MO	USA	MED	B	B		314/622-0900	N	@MRLK
11060	Chapel Hill	NC	USA	MED	B	B		919/933-2580	N	@PLSK
11060	Durham	NC	USA	MED	B	B		919/687-0181	N	@PLSK
11060	Raleigh	NC	USA	MED	B	B	C	919/664-8077	N	@PLSK
07771	Bernardsville	NJ	USA	MED	B	B	C	908/766-7138	N	@PDN
07771	Clinton	NJ	USA	MED	B	B		908/730-8693	N	@PDN
07771	Dover	NJ	USA	MED	B	B	C	201/361-9211	N	@PDN

07771	Eatontown/Red Bank	NJ	USA	MED	B	B	C	908/758-8000	N	@PDN
07771	Elizabeth	NJ	USA	MED	B	B	C	908/289-5100	N	@PDN
07771	Englewood	NJ	USA	MED	B	B	C	201/871-3000	N	@PDN
07771	Freehold	NJ	USA	MED	B	B	C	908/780-8890	N	@PDN
07771	Hackensack	NJ	USA	MED	B	B	C	201/343-9200	N	@PDN
07771	Jersey City	NJ	USA	MED	B	B	C	201/659-3800	N	@PDN
07771	Livingston	NJ	USA	MED	B	B	C	201/533-0561	N	@PDN
07771	Long Branch/Red Bank	NJ	USA	MED	B	B	C	908/758-8000	N	@PDN
07771	Madison	NJ	USA	MED	B	B	C	201/593-0004	N	@PDN
07771	Metuchen	NJ	USA	MED	B	B	C	908/906-9500	N	@PDN
07771	Middletown	NJ	USA	MED	B	B	C	908/957-9000	N	@PDN
07771	Morristown	NJ	USA	MED	B	B	C	201/455-0437	N	@PDN
07771	New Boundland	NJ	USA	MED	B	B	C	201/697-9380	N	@PDN
07771	New Brunswick	NJ	USA	MED	B	B	C	908/247-2700	N	@PDN
07771	Newark	NJ	USA	MED	B	B	C	201/623-0083	N	@PDN
07771	Passaic	NJ	USA	MED	B	B	C	201/473-6200	N	@PDN
07771	Paterson	NJ	USA	MED	B	B	C	201/345-7700	N	@PDN
07771	Phillipsburg	NJ	USA	MED	B	B	C	908/454-9270	N	@PDN
07771	Pompton Lakes	NJ	USA	MED	B	B	C	201/835-8400	N	@PDN
07771	Red Bank	NJ	USA	MED	B	B	C	908/758-8000	N	@PDN
07771	Ridgewood	NJ	USA	MED	B	B	C	201/445-4800	N	@PDN
07771	Somerville	NJ	USA	MED	B	B	C	908/218-1200	N	@PDN
07771	South River	NJ	USA	MED	B	B	C	908/390-9100	N	@PDN
07771	Spring Lake	NJ	USA	MED	B	B	C	908/974-0850	N	@PDN
07771	Toms River	NJ	USA	MED	B	B	C	908/286-3800	N	@PDN
07771	Washington	NJ	USA	MED	B	B	C	908/689-6894	N	@PDN
07771	Wayne/Paterson	NJ	USA	MED	B	B	C	201/345-7700	N	@PDN
06510	Ada	OK	USA	MED	B	B		405/436-0252	N	@MRLK
06510	Altus	OK	USA	MED	B	B		405/477-0321	N	@MRLK
06510	Alva	OK	USA	MED	B	B		405/327-1441	N	@MRLK
06510	Ardmore	OK	USA	MED	B	B		405/223-8086	N	@MRLK
	Bartlesville	OK	USA	MED	B	B		918/336-6901	N	@MRLK
06510	Clinton	OK	USA	MED	B	B		405/323-8102	N	@MRLK
06510	Durant	OK	USA	MED	B	B		405/924-2680	N	@MRLK
06510	Enid	OK	USA	MED	B	B		405/242-8221	N	@MRLK
06510	Lawton	OK	USA	MED	B	B		405/248-8772	N	@MRLK
	Mcalester	OK	USA	MED	B	B		918/426-0900	N	@MRLK
	Miami	OK	USA	MED	B	B		918/540-1551	N	@MRLK
	Muskogee	OK	USA	MED	B	B		918/683-1114	N	@MRLK
06510	Oklahoma City	OK	USA	MED	B	B		405/236-0660	N	@MRLK
06510	Ponca City	OK	USA	MED	B	B		405/762-9926	N	@MRLK
	Sallisaw	OK	USA	MED	B	B		918/775-7713	N	@MRLK
06510	Shawnee	OK	USA	MED	B	B		405/273-0053	N	@MRLK
06510	Stillwater	OK	USA	MED	B	B		405/377-5500	N	@MRLK
	Tulsa	OK	USA	MED	B	B		918/583-6606	N	@MRLK
06510	Woodward	OK	USA	MED	B	B		405/256-9947	N	@MRLK
03526	Allentown	PA	USA	MED	B	B		215/435-0266	N	@PDN
	Altoona	PA	USA	MED			C	814/949-0505	N	@PDN
	Altoona	PA	USA	MED	B	B		814/946-8639	N	@PDN
03526	Ambler	PA	USA	MED	B	B		215/283-2170	N	@PDN
10672	Ambridge	PA	USA	MED	B	B		412/266-9610	N	@PDN
10672	Carnegie	PA	USA	MED	B	B		412/276-1882	N	@PDN
10672	Charleroi	PA	USA	MED	B	B		412/483-9100	N	@PDN
03526	Chester Heights	PA	USA	MED	B	B		215/358-0820	N	@PDN
03526	Coatesville	PA	USA	MED	B	B		215/383-7212	N	@PDN
10672	Connellsville	PA	USA	MED	B	B		412/628-7560	N	@PDN
03526	Downington/Coates.	PA	USA	MED	B	B		215/383-7212	N	@PDN
03562	Doylestown	PA	USA	MED	B	B		215/340-0052	N	@PDN
03562	Germantown	PA	USA	MED	B	B		215-843-4075	N	@PDN
10672	Glenshaw	PA	USA	MED	B	B		412/487-6868	N	@PDN
10672	Greensburg	PA	USA	MED	B	B		412/836-7840	N	@PDN
	Harrisburg	PA	USA	MED			C	717/238-0450	N	@PDN
	Harrisburg	PA	USA	MED	B	B		717/236-3274	N	@PDN

10672	Indiana	PA	USA	MED	B	B	412/465-7210	N	@PDN
03526	King of Prussia	PA	USA	MED	B	B	215/270-2970	N	@PDN
03526	Kirklyn	PA	USA	MED	B	B	215/789-5650	N	@PDN
03526	Lansdowne	PA	USA	MED	B	B	215/626-9001	N	@PDN
10672	Latrobe	PA	USA	MED	B	B	412/537-0340	N	@PDN
	Lemoyne/Harrisburg	PA	USA	MED	B	B	717/236-3274	N	@PDN
10672	McKeesport	PA	USA	MED	B	B	412/673-6200	N	@PDN
10672	New Castle	PA	USA	MED	B	B	412/658-5982	N	@PDN
10672	New Kensington	PA	USA	MED	B	B	412/337-0510	N	@PDN
03526	Norristown	PA	USA	MED	B	B	215/270-2970	N	@PDN
03526	Paoli	PA	USA	MED	B	B	215/648-0010	N	@PDN
	Philadelphia	PA	USA	MED			215/625-0770	N	@PDN
	Philadelphia	PA	USA	MED	B	B	215/923-7792	N	@PDN
10672	Pittsburgh	PA	USA	MED			412/261-9732	N	@PDN
10672	Pittsburgh	PA	USA	MED	B	B	412-687-4131	N	@PDN
10672	Pittsburgh	PA	USA	MED	B	B	412/281-8950	N	@PDN
10672	Pottstown	PA	USA	MED	B	B	215/327-8032	N	@PDN
03526	Quakertown	PA	USA	MED	B	B	215/538-7032	N	@PDN
03526	Reading	PA	USA	MED	B	B	215/375-7570	N	@PDN
10672	Rochester	PA	USA	MED	B	B	412/728-9770	N	@PDN
03526	Scranton	PA	USA	MED			717/341-1860	N	@PDN
03526	Scranton	PA	USA	MED	B	B	717/348-1123	N	@PDN
10672	Sharon	PA	USA	MED	B	B	412/342-1681	N	@PDN
03526	Tullytown	PA	USA	MED	B	B	215/547-3300	N	@PDN
10672	Uniontown	PA	USA	MED	B	B	412/437-5640	N	@PDN
03562	Valley Forge	PA	USA	MED	B	B	215/270-2970	N	@PDN
10672	Washington	PA	USA	MED	B	B	412/223-9090	N	@PDN
03526	Wayne	PA	USA	MED	B	B	215/341-9605	N	@PDN
10672	Wilkinsburg	PA	USA	MED	B	B	412/241-1006	N	@PDN
06254	Alexandria	VA	USA	MED	B	B	703/683-6710	N	@PDN
06254	Arlington	VA	USA	MED	B	B	703/524-8961	N	@PDN
06254	McLean	VA	USA	MED	B	B	703/848-2941	N	@PDN

B=BELL 103/113 (300 bps) or BELL 212A (1200 bps) compatible modems
C=CCITT V.21(300 bps) or CCITT V.22 bis(2400 bps) or CCITT V.32 compatible modems.

B1. Bell Atlantic
~~~~~  
@PDN BELL ATLANTIC - NETWORK NAME IS PUBLIC DATA NETWORK (PDN)

(CONNECT MESSAGE)  
...<CR> (SYNCHRONIZES DATA SPEEDS)

WELCOME TO THE BPA/DST PDN

\*.T <CR> (TYMNET ADDRESS)

131069 (ADDRESS CONFIRMATION - TYMNET DNIC)  
COM (CONFIRMATION OF CALL SET-UP)

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

-----  
B2. BellSouth  
~~~~~  
@PLSK BELLSOUTH - NETWORK NAME IS PULSELINK

(CONNECT MESSAGE)

... <CR> (SYNCHRONIZES DATA SPEEDS)
(DOES NOT ECHO TO THE TERMINAL)

CONNECTED
PULSELINK

13106 (TYMNET ADDRESS)
(DOES NOT ECHO TO THE TERMINAL)

PULSELINK: CALL CONNECTED TO 1 3106

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

B3. Pacific Bell
~~~~~

@PPS PACIFIC BELL - NETWORK NAME IS PUBLIC PACKET SWITCHING (PPS)  
  
(CONNECT MESSAGE)

...<CR> (SYNCHRONIZES DATA SPEEDS)>  
(DOES NOT ECHO TO THE TERMINAL)

ONLINE 1200  
WELCOME TO PPS: 415-XXX-XXXX  
131069 (TYMNET ADDRESS)  
(DOES NOT ECHO UNTIL TYMNET RESPONDS)

-GWY 0XXXX- TYMNET: PLEASE LOG IN: (HOST # WITHIN DASHES)

-----  
B4. Southwestern Bell  
~~~~~

@MRLK - SOUTHWESTERN BELL TELEPHONE- NETWORK NAME IS MICROLINK II(R)

(CONNECT MESSAGE)
(PLEASE TYPE YOUR TERMINAL IDENTIFIER)

A (YOUR TERMINAL IDENTIFIER)

WELCOME TO MICROLINK II
-XXXX:01-030-
PLEASE LOG IN:
.T <CR> (USERNAME TO ACCESS TYMNET)

HOST: CALL CONNECTED

-GWY 0XXXX- TYMNET: PLEASE LOG IN:

B5. Southern New England Telephone
~~~~~

@CONNNET - SOUTHERN NEW ENGLAND TELEPHONE - NETWORK NAME IN CONNNET  
  
(CONNECT MESSAGE)

HH<CR> (SYNCHRONIZES DATA SPEEDS)  
(DOES NOT ECHO TO THE TERMINAL)  
  
CONNNET

.T<CR> (MUST BE CAPITAL LETTERS)  
26-SEP-88 18:33 (DATA)  
031069 (ADDRESS CONFIRMATION)  
COM (CONFIRMATION OF CALL SET-UP)

-GWY OXXXX-TYMNET: PLEASE LOG IN:

-----  
C. Database or Timesharing Companies on Tymnet

~~~~~  
APCUG "GLOBALNET" BBS
Bloodstock Research Information
BRS Information Technologies
BT, North America (Dialcom)
Cartermill, Inc.
Charles Schwab and Company, Inc.
Chemical Abstracts Services (CAS)
Commercial SABRE
Commodity Systems, Inc.
CompuServe, Inc.
Compusource
Computer Intelligence
Connect, Inc.
Creative Automation Co.
Delphi
Dialog Information Services, Inc.
Digital Equipment Corp.
Diversified Network Applications, Inc.
Dow Jones & Company, Inc.
Dun and Bradstreet
Electronic Data Systems Corp.
Export Network, Inc.
Gibson Information Systems (GIS)
Global Interconnect Communications, Inc.
Idioma Translation
Interactive Data Corp.
Jeppesen DataPlan
Mead Data Central
Metro On-Line Services, Ltd.
National Library of Medicine (NLM)
NewsNet, Inc.
Nikkei Telecom Japan
Nuclear Power Experience
OCR Services, Inc.
Official Airline Guide (OAG)
ORBIT Search Service
Power Computing Company
Rand McNally - TDM, Inc.
Real Estate Investment Network
SeniorNet
Southeast Regional Data Center (SERDAC)
SPEED>S Corporation
The Jockey Club Information Systems
TRW Business Credit Division
TRW Information Services
USA TODAY Sports Center
West Publishing Company (WEST)
Xerox Computer Services (XCS)

D. Service Classifications For Database or Timesharing Companies Using Tymnet

MAJOR CATEGORIES:

Business	Investments
Communications	Legal
Computers	Livestock
Economics	Marketing
Education	Medicine
Electronic Mail	Natural Resources
Environment	Real Estate
Finance	Safety
Games	Science
General Interest	Sports
Government	Trade
Health Care	Transportation
Insurance	Travel
International	

OTHER CATEGORIES

Accounting	Law
Airlines	Management
Asia	Manufacturing
Aviation	Market Analysis
Batch (Processing)	Mines
Car	Network
Chats	News
Chemistry	Nuclear Power
Commodities	Outsourcing
Computing	Patents
Conferences	PC
Corporate	Racing
Credit (Business or Consumer)	Records
Data (Processing)	Registration
Direct Marketing	Research
Disaster Recovery	Reservations
DMV	RJE
Electric Power	Route Planning
Engineering	Schedules
Export	SEC
Fax Services	Securities
Fictitious Names	Software
Flight Plans	Tax
Hotel	Timesharing
Horses	Translation
Information	UCC
Instruction	User Group
IRS (Internal Revenue Service)	Vendors
Japan	Weather
Languages	

BT TYMNET's Global Network Service (GNS) combines three level of international services:

1. BT TYMNET GLOBAL NETWORK CONNECTION SERVICE
2. ENHANCED GLOBAL CONNECTION SERVICE
3. BASIC GLOBAL CONNECTION SERVICE

BT TYMNET GLOBAL NETWORK CONNECTION SERVICE (TGN) is currently offered in the

following countries:

Australia	Netherlands
Belgium	New Zealand
Canada	Spain
Denmark	Sweden
France	Switzerland
Germany	United Kingdom
Italy	United States
Japan	

BT TYMNET GLOBAL NETWORK CONNECTION SERVICE are BT TYMNET owned and operated sites and equipment. Global, Regional and local support is provided end-to-end by BT TYMNET's trained and experienced technical staff, in place worldwide since 1977. Round the clock coverage for trouble reporting and response on critical problems is provided. BT TYMNET Global Network Service enhanced pricing, local currency billing and end-user billing is available.

ENHANCED GLOBAL CONNECTION SERVICE (EGC) complement the service described above and is currently available from the following locations:

Alaska (USA)*	Israel
Antigua	Italy
Argentina	Jamaica
Australia	Korea
Austria	Netherland Antilles
Bahama	Panama
Bahrain	Peru
Barbados	Philippines
Belgium	Puerto Rico*
Bermuda	Saudi Arabia
Cayman Islands	Sweden
Denmark	Switzerland
Dominican Republic	Tortola
France	Trinidad and Tobago
Germany	United Kingdom
Guam*	US Virgin Islands
Guatemala	
Honduras	
Hong Kong	

* USA Domestic services and rates apply

ENHANCED GLOBAL CONNECTION SERVICE is offered by a local Telecommunication Administration equipped with BT TYMNET technology. In many instances the administration is using BT TYMNET's Network Supervisors to operate the packet service in their area.

All ENHANCED GLOBAL CONNECTION SERVICE locations offer direct TYM2 (TYMNET's proprietary) protocol connection to the BT TYMNET Public Network and thus may offer BT TYMNET's comprehensive array of enhanced protocol services. Most currently offer BT TYMNET asynchronous access and X.25 service. Naturally, a close affinity exists between BT TYMNET and ENHANCED GLOBAL CONNECTION SERVICE providers so a very high degree of service and support exists in these locations. TYMUSA, a universal dial-up service which is billed back to the customer's home office, is offered from all the above locations.

BASIC GLOBAL CONNECTION SERVICE (BGC) completes the full range of international connectivity and is currently available from the following locations:

Antigua	Greenland*	Panama
---------	------------	--------

Argentina	Gudaelope*	Peru
Australia	Guam & Saipan	Philippines
Austria	Guatemala	Portugal
Bahamas	Honduras	Puerto Rico
Bahrain	Hong Kong	Qatar
Barbados	Hungary	Reunion Island
Belgium	Iceland	Saudi Arabia
Bermuda	India	San Marino*
Brazil	Indonesia	Senegal*
Canada	Ireland	Singapore
Cayman Islands	Israel	South Africa
Chile	Italy	South Korea
China	Ivory Coast	Spain
Colombia	Jamaica	Sweden
CostaRica	Japan	Switzerland
Curacao	Kuwait	Taiwan
Cyprus*	Luxembourg	Thailand
Denmark	Macau*	Tortola (BVI)*
Djibouti*	Malaysia	Trinidad & Tobago
Dominican Republic	Malta*	Tunisia*
Egypt	Mauritius*	Turkey
Faroe Islands*	Mexico	UAE
Finland	Mozambique*	US Virgin Islands
France	Nth. Antilles*	USSR
French Antilles	Netherlands	United Kingdom
French Guiana	New Caledonia*	United States
French Polynesia*	New Zealand	Uruguay
Gabon	Northern Marianas	Vanuatu*
Gambia	Norway	Yugoslavia*
Germany		Zimbabwe
Greece		

* Information will be available on the next update

BASIC GLOBAL CONNECTION SERVICE providers connect their networks to BT TYMNET exclusively via X.75 protocol gateways. The CCITT recommendation X.75 is closely related to the better known CCITT X.25 recommendation and provides a reliable communication channel for interworking between Public Data Networks.

As a supplier of network technology to US IRC's and foreign carriers for more than 10 years, BT TYMNET has a wealth of experience with the X.75 standard and actively participates in its development. BT TYMNET X.75 software has evolved into a sophisticated product providing numerous advanced features not found in other X.75 implementations. BT TYMNET maintains and supports more X.75 gateway links than any other network in the world.

All of BT TYMNET's X.75 gateways are supported by BT TYMNET's International Network Services (INS) group which ensures that all the gateways are configured to provide a uniform interface to BT TYMNET regardless of the origination network.

E. Summary of Global Network Services By Country

Note: TYMNET GLOBAL NETWORK (TGN) use BT TYMNET's assigned DNIC of 3106. The other DNICs listed in the table below are the DNICs of the ENHANCED GLOBAL CONNECTION (EGC) and BASIC GLOBAL CONNECTION (BGC) service providers.

COUNTRY	TGN	DNIC/Network	>>	EGC	BGC
Alaska		3135/Alascom	>>	X	

Antigua		3443/Aganet	>> X	
Argentina		7220/ARPAC	>> X	
Argentina		7222/ARPAC	>>	X
Australia	X	BT TYMNET	>>	
Australia		5052/AUSPAC	>>	X
Australia		5053/MIDAS	>>	X
Austria		2322/DATEX-P	>>	X
Austria		2329/RADIO AUST	>> X	
Bahamas		3640/BaTelCo	>> X	
Bahrain		4263/BAHNET	>> X	
Barbados		3423/IDAS	>> X	
Belgium	X	BT TYMNET	>>	
Belgium		2062/DCS	>>	X
Belgium		206/DCS	>>	X
Belgium		2069/DCS	>>	X
Bermuda		3503/Bermudanet	>> X	
Brazil		7240/Interdata	>>	X
Brazil		7241/Renpac	>>	X
Cameroun		6261/Campac	>>	X
Canada	X	BT TYMNET	>>	
Canada		3020/Datapac	>>	X
Canada		3025/Globedat	>>	X
Canada		3028/CNCP-PACKET Network	>>>> >>	X
Canada		3029/CNCP-INFO SWITCH	>>>> >>	X
Cayman Islands		3463/IDAS	>> X	
Chile		3104/Entel	>>	X
Chile		7302/Entel	>>	X
Chile		7303/Chile-PAC	>>	X
Chile		7305/VTR	>>	X
China		4600/PTELCOM	>>	X

China		4602/CHINAPAK >>	X
Columbia		7320/DAPAQ >>	X
Columbia		7322/COLDAPAQ >>	X
Costa Rica		7122/RACSAPAC >>	X
Costa Rica		7129/RACSAPAC >>	X
Cyprus		2802/Cytapac >>	X
Cyprus		2803/Cytapac >>	X
Cyprus		2808/Cytapac >>	X
Cyprus		2809/Cytapac >>	X
Denmark	X	BT TYMNET >>	
Denmark		2382/Datapak >>	X
Denmark		2383/Datapak >>	X
Djibouti		6328/Djipac >>	X
Dominican Rep		3700/UDTS-I >> X	
Egypt		6020/ARENTO >>	X
Egypt		6023/EGYPTNET >>	X
Faroe Islands		2881/Faroepac >>	X
Finland		2442/Datapak >>	X
France	X	BT TYMNET >>	
France		2080/Transpac >>	X
France		2081/NTI >>	X
Fr Antillies		3400/Dompac >>	X
Fr Guiana		7420/Dompac >>	X
Fr. Polynesia		5470/Tompac >>	
Gabon		6282/Gabonpac >>	X
Germany F.R	X	BT TYMNET >>	
Germany F.R		2624/DATEX-P >>	X
Greece		2022/Helpak >>	X
Greece		2023/Hellaspac >>	X
Greenland		2901/KANUPAX >>	X
Guadeloupe		3441/ >>	X
Guam		5351/PCINET >> X	

Guatemala		7043/GAUTEL	>> X	
Honduras		7080/HONDUTEL	>> X	
Hong Kong		4542/INTELPAC	>> X	
Hong Kong		4545/DATAPAC	>>	X
Hong Kong		4546/DATAPAC	>>	X
Hungary		2160/NEDEX	>>	X
Hungary		2161/DATEX	>>	X
Iceland		2740/Icepak	>>	X
India		4042/GPSS	>>	X
Indonesia		5101/SKDP	>>	X
Ireland		2724/Eirpac	>>	X
Israel		4251/Isranet	>>	X
Italy	X	BT TYMNET	>>	
Italy		2222/Darbo-Ital	>>	X
Italy		2227/Italcable	>>	X
Ivory Coast		6122/SYTRANPAC	>>	X
Jamaica		3380/Jamintel	>> X	
Japan		4400/Global VAN	>>	X
Japan		4404/JAIS	>>	X
Japan	X	4406/NIS- BT TYMNET	>> >>	
Japan		4407/	>>	X
Japan		4401/NTT DDX	>>	X
Japan		4408/Venus-P	>>	X
Japan		4410/NI+CI	>>	X
Japan		4411/K-NET	>>	X
Korea Rep		4501/DACOM-NET	>>	X
Kuwait		4190/	>>	X
Kuwait		4263/KUPAC	>>	X
Lebanon		4155/RADUS	>>	X
Luxembourg		2704/Luxpac-X.25	>>>	X
Luxembourg		2709/Luxpac-Pad	>>	X

Macau		4550/Macoupac	>>	X
Madagascar		6360/	>>	X
Malaysia		5021/Maynet	>>	X
Malta		2782/Maltapac	>>	X
Mauritius		6170/MauriData	>>	X
Mauritius		6171/MauriData	>>	X
Mexico		3340/TELEPAC	>>	X
Morocco			>>	X
Mozambique		6435/	>>	X
Namibia		6490/Swanet	>>	
Niger		6142/	>>	
Netherlands	X	BT TYMNET	>>	
Netherlands		2041/Datanet-1	>>	X
Netherlands		2044/DABAS	>>	X
Netherlands		2049/Datanet-1 Memocom	>> >>	X
N. Antilles		3620/LANDSRAIDO	>> X	
N. Marianas		5351/PCInet	>> X	
New Caledonia		5460/Tompac	>>	X
New Zealand	X	3106/BT TYMNET	>>	
New Zealand		5301/Pacnet	>>	X
Norway		2422/Datapak	>>	X
Panama		7141/INTEL	>> X	
Panama		7142/INTELPAQ	>>	X
Peru		3104/IMPACS	>> X	
Peru		7160/ENTEL	>>	X
Philippines		5152/Philcom	>> X	
Philippines		5154/GMCR	>> X	
Philippines		5156/ETPI	>> X	
Philippines		5151/CAPWIRE	>>	X
Polynesia		5470/Tompac	>>	X
Portugal		2680/Telepac	>>	X

Portugal		2682/CPRM	X
Puerto Rico		3300/WorldCom	X
Puerto Rico		3301/PRTC	X
Qatar		4271/DOHPAC	X
Reunion		6470/Dompac	X
San Marino		2922/X NET SMR	X
Saudi Arabia		4201/Alwaseet	
Saudi Arabia		4263/Bahnet	X
Senegal		6081/Serpac	
Singapore		5250/	X
Singapore		5252/Telepac	X
South Africa		6550/Saponet	X
South Africa		6559/Saponet	X
Spain	X	BT TYMNET	
Spain		2141/TIDA	X
Spain		2145/Iberpac	X
Sweden	X	BT TYMNET	
Sweden		2401/Datapak	X
Sweden		2402/Datapak	X
Sweden		2403/Datapak	X
Switzerland	X	BT TYMNET	
Switzerland		2284/Telepac	X
Taiwan		4877/ITA	X
Taiwan		4872/PACNET	X
Taiwan		4873/DCI Telepac	X
Thailand		5200/IDAR	X
Thailand		5201/Cateng	
Tortola, BVI		3483/	X
Trinidad		3740/Textel	X
Trinidad		3745/Datanett	X
Tunisia		6050/RED25	X

Turkey		2860/	>>	X
Turkey		2862/IGX	>>	X
Turkey		2863/Turpac	>>	X
Turks BWI		3763/	>> X	
UAE		4241/	>>	X
UAE		3104/IMPACS	>>	X
UAE		4243/EMDAN	>>	X
U. Kingdom	X	BT TYMNET	>>	
U. Kingdom		2350/Mercury	>>	X
U. Kingdom		2351/Mercury	>>	X
U. Kingdom		2341/BTI IPSS	>>	X
U. Kingdom		2355/JAIS-Japan	>>	X
U. Kingdom		2342/BT PSS	>>	X
U. Kingdom		2352/Hull	>>	X
United States	X	3106/BT TYMNET	>>	
Uruguay		7482/Antel	>>	X
USSR		2502/Iasnet	>>	X
U.S. Virgin I		3320/UDTS-I	>> X	
Vanuatu		5410/Viapac	>>	X
Yugoslavia		2201/Yupac	>>	X
Zimbabwe		6482/Zimnet	>>	X

F. Terminal Identifiers

~~~~~

A terminal identifier indicates to the network the characteristics of your terminal. Most terminals can use the "A" terminal identifier. However, if your terminal requires a carriage return delay, for example, then the "I" or the "E" identifier should be used.

At 'please type your terminal identifier' please enter:

- A for PC's and CRT terminals (SAVE parity)
- C for 300 baud Impact Printer Terminals
- E for Thermal Printer Terminals like the SILENT 700 series
- F for BETA transaction terminals
- G for the GE Terminet at 1200 baud
- I for 300 baud Thermal Printer Terminals
- K for EVEN/ODD parity terminals (future implementation)
- O for MARK/SPACE parity terminals (BBS access)



Y for 300 baud Transaction terminals

-----

## G. Login Options

~~~~~

At the 'please log in:' prompt the user can specify control characters to set the network to the needs of the user. For example when you are connected to a database and the data is coming in so fast you can backpressure the data by typing ^S. The network however will only react on this command if you specified ^R at the logon step.

^E - control E - Enter Full Duplex mode (future implementation)
^H - control H - Enter Half Duplex mode - disable echo!!
^I - control I - Build optimal circuit for Interactive traffic
^P - control P - Force EVEN Parity
^R - control R - Enable host backpressure X-on X-off
^U - control U - Force terminal data to uppercase
^V - control V - Build optimal circuit for Volume traffic
^W - control W - Erase login up to last terminator
^X - control X - Enable terminal backpressure X-on X-off
^Z - control Z - Disconnect/Logoff
ESC - escape - Discard login and get NEW please log in prompt
BREAK - break - Switch to CCITT X.3 X.28 X.29 PAD (selected nodes)

==Phrack Inc.==

Volume Four, Issue Forty, File 9 of 14

BT Tymnet British Telecom Part 2 of 3 Presented by Toucan Jones August 1, 1992
--

Welcome Back to Tymnet!

PART 1

- A. BT Tymnet Access Location Index
- B. BT-GNS Access Within Regional Bell Operating Companies
 - 1. Bell Atlantic
 - 2. BellSouth
 - 3. Pacific Bell
 - 4. Southwestern Bell
 - 5. Southern New England Telephone
- C. Database or Timesharing Companies on Tymnet
- D. Service Classifications For Database or Timesharing Companies Using Tymnet
- E. Summary of Global Network Services By Country
- F. Terminal Identifiers
- G. Login Options

PART 2

- H. BT-GNS Worldwide Asynchronous Outdial Service

PART 3

I. BT-GNS Worldwide Access Sorted By Node

H. BT-GNS Worldwide Asynchronus Outdial Service

- OUTDIAL -		PROV			DIALUP ACCESS				M			
HOST	CITY	ST	CNTRY	DENS	100's bps				AREA	CODE	P	COMMENTS
					3	12	24	96				
7651	Anniston	AL	USA	LOW	B	B	C		205		Y	
4101	Birmingham	AL	USA	HIGH	B	B	C		205		Y	
2517	Dothan	AL	USA	LOW	B	B	C		205		Y	
5641	Florence	AL	USA	LOW	B	B	C		205		Y	
8287	Gadsden	AL	USA	LOW	B	B	C		205		Y	
737	Huntsville	AL	USA	MED	B	B	C		205		Y	
8829	Mobile	AL	USA	MED	B	B	C		205		Y	
3245	Montgomery	AL	USA	LOW	B	B	C		205		Y	
2439	Northport	AL	USA	LOW	B	B	C		205		Y	
1751	Opelika	AL	USA	LOW	B	B	C		205		Y	
2439	Tuscaloosa/Northport	AL	USA	LOW	B	B	C		205		Y	
15360	Fayetteville	AR	USA	LOW	B	B	C		501		Y	
1297	Ft. Smith	AR	USA	LOW	B	B	C		501		Y	
2725	Hot Springs	AR	USA	LOW	B	B	C		501		Y	
2794	Jonesboro	AR	USA	LOW	B	B	C		501		Y	
10690	Little Rock	AR	USA	MED	B	B	C		501		Y	
10690	Little Rock	AR	USA	MED	B	B	C		501		Y	
7380	Pine bluff	AR	USA	LOW	B	B	C		501		Y	
15360	Springdale/Fayettevl	AR	USA	LOW	B	B	C		501		Y	
6112	Flagstaff	AZ	USA	LOW	B	B	C		602		Y	
9532	Mesa/Phoenix	AZ	USA	HIGH	B	B	C		602		Y	
9532	Mesa/Phoenix	AZ	USA	HIGH	B	B	C		602		Y	
9532	Phoenix	AZ	USA	HIGH	B	B	C		602		Y	
9532	Phoenix	AZ	USA	HIGH	B	B	C		602		Y	
3232	Tucson	AZ	USA	MED	B	B	C		602		Y	
3232	Tucson	AZ	USA	MED	B	B	C		602		Y	
3530	Yuma	AZ	USA	LOW	B	B	C		602		Y	
8963	Alameda/Oakland	CA	USA	HIGH	B	B	C		510		Y	
2940	Alhambra	CA	USA	MED	B	B	C		818		Y	
2940	Alhambra	CA	USA	MED	B	B	C		818		Y	
9184	Anaheim/Newprt Beach	CA	USA	HIGH	B	B	C		714		Y	
9184	Anaheim/Newprt Beach	CA	USA	HIGH	B	B	C		714		Y	
4457	Antioch	CA	USA	LOW	B	B	C		510		Y	
2940	Arcadia/Alhambra	CA	USA	MED	B	B	C		818		Y	
2940	Arcadia/Alhambra	CA	USA	MED	B	B	C		818		Y	
3664	Bakersfield	CA	USA	LOW	B	B	C		805		Y	
9182	Belmont/Redwood City	CA	USA	HIGH	B	B	C		415		Y	
8963	Berkeley/Oakland	CA	USA	HIGH	B	B	C		510		Y	
9206	Beverly Hills/Shr Ok	CA	USA	MED	B	B	C		818		Y	
2841	Burbank	CA	USA	LOW	B	B	C		818		Y	
3486	Burlingame/So. S.F.	CA	USA	LOW	B	B	C		415		Y	
9206	Canoga Park/Shrm Oak	CA	USA	MED	B	B	C		818		Y	
7859	Cathedral City	CA	USA	LOW	B	B	C		619		Y	
7801	Chico	CA	USA	LOW	B	B	C		916		Y	
6294	Colton	CA	USA	MED	B	B	C		714		Y	
9202	Concord/Walnut Creek	CA	USA	LOW	B	B	C		510		Y	
9202	Concord/Walnut Creek	CA	USA	LOW	B	B	C		510		Y	
5415	Corona	CA	USA	LOW	B	B	C		714		Y	
4309	Covina/Diamond Bar	CA	USA	MED	B	B	C		714		Y	
7276	Davis	CA	USA	LOW	B	B	C		916		Y	
4309	Diamond Bar	CA	USA	MED	B	B	C		714		Y	
06824	El Centro	CA	USA	LOW	B	B	C		619		Y	
2940	El Monte/Alhambra	CA	USA	MED	B	B	C		818		Y	

2940	El Monte/Alhambra	CA	USA	MED	B	B	C	818	Y
9203	El Segundo	CA	USA	MED	B	B	C	310	Y
09203	El Segundo	CA	USA	MED	B	B	C	310	Y
4304	Escondido/Vista	CA	USA	MED	B	B	C	619	Y
981	Eureka	CA	USA	LOW	B	B	C	707	Y
03513	Fairfield	CA	USA	LOW	B	B	C	707	Y
3513	Fairfield	CA	USA	LOW	B	B	C	707	Y
7399	Fremont	CA	USA	MED	B	B	C	510	Y
3996	Fresno	CA	USA	LOW	B	B	C	209	Y
3996	Fresno	CA	USA	LOW	B	B	C	209	Y
2841	Glendale/Burbank	CA	USA	LOW	B	B	C	818	Y
8963	Hayward/Oakland	CA	USA	HIGH	B	B	C	510	Y
3173	Inglewood/Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Inglewood/Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Inglewood/Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Inglewood/Vernon	CA	USA	HIGH	B	B	C	213	Y
9184	Irvine/Newport Beach	CA	USA	HIGH	B	B	C	714	Y
9184	Irvine/Newport Beach	CA	USA	HIGH	B	B	C	714	Y
5991	Lancaster	CA	USA	LOW	B	B	C	805	Y
9205	Long Beach	CA	USA	MED	B	B	C	310	Y
6616	Los Alamos/St. Maria	CA	USA	LOW	B	B	C	805	Y
6450	Los Altos/San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	Los Altos/San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	Los Altos/San Jose	CA	USA	HIGH	B	B	C	408	Y
3173	Los Angeles/Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Los Angeles/Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Los Angeles/Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Los Angeles/Vernon	CA	USA	HIGH	B	B	C	213	Y
9203	Mar Vista/El Segundo	CA	USA	MED	B	B	C	310	Y
9203	Mar Vista/El Segundo	CA	USA	MED	B	B	C	310	Y
9203	MarinaDelRey/El Sgnd	CA	USA	MED	B	B	C	310	Y
03501	Marysville	CA	USA	LOW	B	B	C	916	Y
14085	Merced	CA	USA	LOW	B	B	C	209	Y
2120	Modesto	CA	USA	LOW	B	B	C	209	Y
10401	Monterey	CA	USA	LOW	B	B	C	408	Y
10401	Monterey	CA	USA	LOW	B	B	C	408	Y
5134	Moorpark	CA	USA	LOW	B	B	C	805	Y
13891	Napa	CA	USA	LOW	B	B	C	707	Y
9184	Newport Beach	CA	USA	HIGH	B	B	C	714	Y
9184	Newport Beach	CA	USA	HIGH	B	B	C	714	Y
9205	Norwalk/Long Beach	CA	USA	MED	B	B	C	310	Y
8963	Oakland	CA	USA	HIGH	B	B	C	510	Y
4309	Ontario/Diamond Bar	CA	USA	MED	B	B	C	714	Y
4112	Oxnard/Port Hueneme	CA	USA	MED	B	B	C	805	Y
9202	Pacheco/Walnut Creek	CA	USA	LOW	B	B	C	510	Y
9202	Pacheco/Walnut Creek	CA	USA	LOW	B	B	C	510	Y
7859	Palm Sprngs/Cath Cty	CA	USA	LOW	B	B	C	619	Y
9182	Palo Alto/Redwd City	CA	USA	HIGH	B	B	C	415	Y
2940	Pasadena/Alhambra	CA	USA	MED	B	B	C	818	Y
2940	Pasadena/Alhambra	CA	USA	MED	B	B	C	818	Y
9202	Pleasnthill/Walnt Ck	CA	USA	LOW	B	B	C	510	Y
9202	Pleasnthill/Walnt Ck	CA	USA	LOW	B	B	C	510	Y
4309	Pomona/Diamond Bar	CA	USA	MED	B	B	C	714	Y
4112	Port Hueneme	CA	USA	MED	B	B	C	805	Y
5416	Poway	CA	USA	LOW	B	B	C	619	Y
4972	Redding	CA	USA	LOW	B	B	C	916	Y
9182	Redwood City	CA	USA	HIGH	B	B	C	415	Y
6294	Riverside/Colton	CA	USA	MED	B	B	C	714	Y
9179	Sacramento	CA	USA	HIGH	B	B	C	916	Y
3655	Salinas	CA	USA	LOW	B	B	C	408	Y
6294	San Bernadino/Colton	CA	USA	MED	B	B	C	714	Y
4447	San Clemente	CA	USA	LOW	B	B	C	714	Y
9183	San Diego	CA	USA	HIGH	B	B	C	619	Y

9183	San Diego	CA	USA	HIGH	B	B	C	619	Y
9206	San Fernando/Shr Oak	CA	USA	MED	B	B	C	818	Y
9533	San Francisco	CA	USA	HIGH	B	B	C	415	Y
9533	San Francisco	CA	USA	HIGH	B	B	C	415	Y
9533	San Francisco	CA	USA	HIGH	B	B	C	415	Y
6450	San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	San Jose	CA	USA	HIGH	B	B	C	408	Y
2979	San Luis Obispo	CA	USA	LOW	B	B	C	805	Y
3486	San Mateo/So. S.F.	CA	USA	LOW	B	B	C	415	Y
9205	San Pedro/Long Beach	CA	USA	MED	B	B	C	310	Y
8094	San Rafael	CA	USA	LOW	B	B	C	415	Y
9184	Santa Ana/Newprt Bch	CA	USA	HIGH	B	B	C	714	Y
9184	Santa Ana/Newprt Bch	CA	USA	HIGH	B	B	C	714	Y
6295	Santa Barbara	CA	USA	MED	B	B	C	805	Y
6450	Santa Clara/San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	Santa Clara/San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	Santa Clara/San Jose	CA	USA	HIGH	B	B	C	408	Y
3182	Santa Cruz	CA	USA	MED	B	B	C	408	Y
6116	Santa Maria	CA	USA	LOW	B	B	C	805	Y
9203	Santa Monica/El Sgnd	CA	USA	MED	B	B	C	310	Y
4111	Santa Rosa	CA	USA	LOW	B	B	C	707	Y
9206	Sherman Oaks	CA	USA	MED	B	B	C	818	Y
3486	So. San Francisco	CA	USA	LOW	B	B	C	415	Y
3208	Stockton	CA	USA	LOW	B	B	C	209	Y
6450	Sunnyvale/San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	Sunnyvale/San Jose	CA	USA	HIGH	B	B	C	408	Y
6450	Sunnyvale/San Jose	CA	USA	HIGH	B	B	C	408	Y
14338	Upland	CA	USA	LOW	B	B	C	714	Y
3830	Vallejo	CA	USA	LOW	B	B	C	707	Y
9206	Van Nuys/Sherman Oak	CA	USA	MED	B	B	C	818	Y
4112	Ventura/Port Hueneme	CA	USA	MED	B	B	C	805	Y
3173	Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Vernon	CA	USA	HIGH	B	B	C	213	Y
3173	Vernon	CA	USA	HIGH	B	B	C	213	Y
3598	Visalia	CA	USA	LOW	B	B	C	209	Y
4304	Vista	CA	USA	MED	B	B	C	619	Y
4309	W.Covina/Diamond Bar	CA	USA	MED	B	B	C	714	Y
9202	Walnut Creek	CA	USA	LOW	B	B	C	510	Y
9202	Walnut Creek	CA	USA	LOW	B	B	C	510	Y
9206	West L.A./Shrmn Oaks	CA	USA	MED	B	B	C	818	Y
7276	Woodland/Davis	CA	USA	LOW	B	B	C	916	Y
2584	Aurora/Denver	CO	USA	HIGH	B	B	C	303	Y
2584	Aurora/Denver	CO	USA	HIGH	B	B	C	303	Y
2584	Boulder/Denver	CO	USA	HIGH	B	B	C	303	Y
2584	Boulder/Denver	CO	USA	HIGH	B	B	C	303	Y
2660	Colorado Springs	CO	USA	MED	B	B	C	719	Y
2660	Colorado Springs	CO	USA	MED	B	B	C	719	Y
2584	Denver	CO	USA	HIGH	B	B	C	303	Y
2584	Denver	CO	USA	HIGH	B	B	C	303	Y
8737	Fort Collins	CO	USA	LOW	B	B	C	303	Y
6115	Grand Junction	CO	USA	LOW	B	B	C	303	Y
7743	Greeley	CO	USA	LOW	B	B	C	303	Y
14753	Pueblo	CO	USA	LOW	B	B	C	719	Y
9128	Bloomfield	CT	USA	HIGH	B	B	C	203	Y
9128	Bloomfield	CT	USA	HIGH	B	B	C	203	Y
6472	Bridgeport	CT	USA	MED	B	B	C	203	Y
7962	Fairfield/Westport	CT	USA	MED	B	B	C	203	Y
9128	Hartford/Bloomfield	CT	USA	HIGH	B	B	C	203	Y
3165	Meriden	CT	USA	LOW	B	B	C	203	Y
3165	Middletown/Meriden	CT	USA	LOW	B	B	C	203	Y
11036	New Haven	CT	USA	MED	B	B	C	203	Y

7955	New London	CT	USA	LOW	B	B	C	203	Y
7962	Norwalk/Westport	CT	USA	MED	B	B	C	203	Y
7955	Norwich/New London	CT	USA	LOW	B	B	C	203	Y
8071	Somers	CT	USA	LOW	B	B	C	203	Y
9129	Stamford	CT	USA	HIGH	B	B	C	203	Y
6472	Stratford/Bridgeport	CT	USA	MED	B	B	C	203	Y
3073	Waterbury	CT	USA	LOW	B	B	C	203	Y
7962	Westport	CT	USA	MED	B	B	C	203	Y
2262	Washington/Fairfax	DC	USA	HIGH	B	B	C	703	Y
2262	Washington/Fairfax	DC	USA	HIGH	B	B	C	703	Y
2262	Washington/Fairfax	DC	USA	HIGH	B	B	C	703	Y
2262	Washington/Fairfax	DC	USA	HIGH	B	B	C	703	Y
2262	Washington/Fairfax	DC	USA	HIGH	B	B	C	703	Y
12900	Dover	DE	USA	LOW	B	B	C	302	Y
10800	Georgetown	DE	USA	LOW	B	B	C	302	Y
1784	Newark/Wilmington	DE	USA	MED	B	B	C	302	Y
1784	Wilmington	DE	USA	MED	B	B	C	302	Y
5656	Boca Raton/Delray	FL	USA	LOW	B	B	C	407	Y
3326	Boynton Bch/WPalm Bch	FL	USA	MED	B	B	C	407	Y
4637	Clearwater	FL	USA	MED	B	B	C	813	Y
3720	Cocoa	FL	USA	LOW	B	B	C	407	Y
3720	Cocoa	FL	USA	LOW	B	B	C	407	Y
5656	Delray	FL	USA	LOW	B	B	C	407	Y
9453	Fort Meyers	FL	USA	LOW	B	B	C	813	Y
4701	Fort Pierce	FL	USA	LOW	B	B	C	407	Y
7123	Ft. Lauderdale	FL	USA	MED	B	B	C	305	Y
10351	Gainesville	FL	USA	LOW	B	B	C	904	Y
7123	Hollywood/Ft. Lauderdale	FL	USA	MED	B	B	C	305	Y
5797	Jacksonville	FL	USA	MED	B	B	C	904	Y
5797	Jacksonville	FL	USA	MED	B	B	C	904	Y
09914	Key West	FL	USA	LOW	B	B	C	305	Y
9900	Kissimmee	FL	USA	LOW	B	B	C	407	Y
820	Lakeland	FL	USA	LOW	B	B	C	813	Y
7096	Longwood/Orlando	FL	USA	MED	B	B	C	407	Y
3720	Melbourne/Cocoa	FL	USA	LOW	B	B	C	407	Y
3720	Melbourne/Cocoa	FL	USA	LOW	B	B	C	407	Y
3720	Merritt Isle/Cocoa	FL	USA	LOW	B	B	C	407	Y
3720	Merritt Isle/Cocoa	FL	USA	LOW	B	B	C	407	Y
6582	Miami	FL	USA	HIGH	B	B	C	305	Y
6582	Miami	FL	USA	HIGH	B	B	C	305	Y
11124	Naples	FL	USA	LOW	B	B	C	813	Y
7220	Ocala	FL	USA	LOW	B	B	C	904	Y
7096	Orlando	FL	USA	MED	B	B	C	407	Y
10699	Ormond Beach	FL	USA	LOW	B	B	C	904	Y
3407	Panama City	FL	USA	LOW	B	B	C	904	Y
3193	Pensacola	FL	USA	LOW	B	B	C	904	Y
7123	Pompano Bch/Ft. Lauderdale	FL	USA	MED	B	B	C	305	Y
9902	Port St. Lucie	FL	USA	LOW	B	B	C	407	Y
3112	Sarasota	FL	USA	LOW	B	B	C	813	Y
3112	Sarasota	FL	USA	LOW	B	B	C	813	Y
4637	St. Petersburg/Clearwater	FL	USA	MED	B	B	C	813	Y
12790	Tallahassee	FL	USA	MED	B	B	C	904	Y
5518	Tampa	FL	USA	HIGH	B	B	C	813	Y
6181	Vero Beach	FL	USA	LOW	B	B	C	407	Y
3326	West Palm Beach	FL	USA	MED	B	B	C	407	Y
820	Winterhaven/Lakeland	FL	USA	LOW	B	B	C	813	Y
5774	Albany	GA	USA	LOW	B	B	C	912	Y
8795	Atlanta/Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Atlanta/Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Atlanta/Doraville	GA	USA	HIGH	B	B	C	404	Y
433	Augusta/Martinez	GA	USA	LOW	B	B	C	404	Y
433	Augusta/Martinez	GA	USA	LOW	B	B	C	404	Y
14525	Columbus	GA	USA	LOW	B	B	C	404	Y

8795	Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Doraville	GA	USA	HIGH	B	B	C	404	Y
3711	Macon/Warner Robins	GA	USA	LOW	B	B	C	912	Y
8795	Marietta/Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Marietta/Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Marietta/Doraville	GA	USA	HIGH	B	B	C	404	Y
433	Martinez	GA	USA	LOW	B	B	C	404	Y
8795	Norcross/Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Norcross/Doraville	GA	USA	HIGH	B	B	C	404	Y
8795	Norcross/Doraville	GA	USA	HIGH	B	B	C	404	Y
1386	Rome	GA	USA	LOW	B	B	C	404	Y
3327	Savannah	GA	USA	LOW	B	B	C	912	Y
3711	Warner Robins	GA	USA	LOW	B	B	C	912	Y
1745	Ames	IA	USA	LOW	B	B	C	515	Y
5964	Cedar Falls/Waterloo	IA	USA	LOW	B	B	C	319	Y
8755	Cedar Rapids	IA	USA	LOW	B	B	C	319	Y
5296	Davenport/RockIsland	IA	USA	MED	B	B	C	309	Y
9854	Des Moines	IA	USA	MED	B	B	C	515	Y
3275	Dubuque	IA	USA	LOW	B	B	C	319	Y
5290	Iowa City	IA	USA	LOW	B	B	C	319	Y
5374	Marshalltown	IA	USA	LOW	B	B	C	515	Y
08985	Ottomwa	IA	USA	LOW	B	B	C	515	Y
14315	Sioux City	IA	USA	LOW	B	B	C	712	Y
5964	Waterloo	IA	USA	LOW	B	B	C	319	Y
200	Boise	ID	USA	MED	B	B	C	208	Y
10239	Coeur D'Alene	ID	USA	LOW	B	B	C	208	Y
3660	Idaho Falls	ID	USA	LOW	B	B	C	208	Y
3207	Pocatello	ID	USA	LOW	B	B	C	208	Y
1436	Twin Falls	ID	USA	LOW	B	B	C	208	Y
11496	Bloomington	IL	USA	LOW	B	B	C	309	Y
13595	Bradley	IL	USA	LOW	B	B	C	815	Y
9753	Champaign/Urbana	IL	USA	LOW	B	B	C	217	Y
8257	Chicago	IL	USA	HIGH	B	B	C	312	Y
8257	Chicago	IL	USA	HIGH	B	B	C	312	Y
4630	Cicero/Maywood	IL	USA	LOW	B	B	C	708	Y
1119	Danville	IL	USA	LOW	B	B	C	217	Y
8900	Decatur	IL	USA	LOW	B	B	C	217	Y
8944	Downrs Grove/Gln Eln	IL	USA	MED	B	B	C	708	Y
8944	Downrs Grove/Gln Eln	IL	USA	MED	B	B	C	708	Y
3905	Elgin	IL	USA	LOW	B	B	C	708	Y
4630	Forest Park/Maywood	IL	USA	LOW	B	B	C	708	Y
2514	Freeport	IL	USA	LOW	B	B	C	815	Y
8944	Glen Ellyn	IL	USA	MED	B	B	C	708	Y
8944	Glen Ellyn	IL	USA	MED	B	B	C	708	Y
14576	Joliet	IL	USA	LOW	B	B	C	815	Y
13595	Kankakee/Bradley	IL	USA	LOW	B	B	C	815	Y
780	Lake Bluff	IL	USA	LOW	B	B	C	708	Y
7005	Lake Zurich/Palatine	IL	USA	LOW	B	B	C	708	Y
13640	Lansing	IL	USA	LOW	B	B	C	708	Y
780	Librtyvle/Lake Bluff	IL	USA	LOW	B	B	C	708	Y
4630	Maywood	IL	USA	LOW	B	B	C	708	Y
10945	Northfield	IL	USA	LOW	B	B	C	708	Y
3001	O'Fallon	IL	USA	LOW	B	B	C	618	Y
7005	Palatine	IL	USA	LOW	B	B	C	708	Y
3614	Peoria	IL	USA	LOW	B	B	C	309	Y
14553	Quincy	IL	USA	LOW	B	B	C	217	Y
5296	Rock Island	IL	USA	MED	B	B	C	309	Y
6048	Rockford	IL	USA	MED	B	B	C	815	Y
5403	Springfield	IL	USA	MED	B	B	C	217	Y
9753	Urbana	IL	USA	LOW	B	B	C	217	Y
8944	Wheaton/Glen Ellyn	IL	USA	MED	B	B	C	708	Y
8944	Wheaton/Glen Ellyn	IL	USA	MED	B	B	C	708	Y

9323	Bloomington	IN	USA	LOW	B	B	C	812	Y
2444	Elkhart	IN	USA	LOW	B	B	C	219	Y
3426	Evansville	IN	USA	LOW	B	B	C	812	Y
3423	Ft. Wayne	IN	USA	LOW	B	B	C	219	Y
14286	Gary	IN	USA	LOW	B	B	C	219	Y
14286	Gary	IN	USA	LOW	B	B	C	219	Y
14286	Hammond/Gary	IN	USA	LOW	B	B	C	219	Y
14286	Hammond/Gary	IN	USA	LOW	B	B	C	219	Y
14286	Highland/Gary	IN	USA	LOW	B	B	C	219	Y
14286	Highland/Gary	IN	USA	LOW	B	B	C	219	Y
9349	Indianapolis	IN	USA	HIGH	B	B	C	317	Y
2646	Kokomo	IN	USA	LOW	B	B	C	317	Y
3157	Lafayette	IN	USA	LOW	B	B	C	317	Y
4632	Marion	IN	USA	LOW	B	B	C	317	Y
5129	Mishawaka/South Bend	IN	USA	MED	B	B	C	219	Y
5129	South Bend	IN	USA	MED	B	B	C	219	Y
2893	Terre Haute	IN	USA	LOW	B	B	C	812	Y
8615	Kansas City/Mission	KS	USA	HIGH	B	B	C	913	Y
8615	Kansas City/Mission	KS	USA	HIGH	B	B	C	913	Y
14347	Lawrence	KS	USA	LOW	B	B	C	913	Y
3408	Leavenworth	KS	USA	LOW	B	B	C	913	Y
2799	Manhattan	KS	USA	LOW	B	B	C	913	Y
8615	Mission	KS	USA	HIGH	B	B	C	913	Y
8615	Mission	KS	USA	HIGH	B	B	C	913	Y
3416	Salina	KS	USA	LOW	B	B	C	913	Y
8615	Shawnee/Mission	KS	USA	HIGH	B	B	C	913	Y
8615	Shawnee/Mission	KS	USA	HIGH	B	B	C	913	Y
1672	Topeka	KS	USA	LOW	B	B	C	913	Y
8013	Wichita	KS	USA	MED	B	B	C	316	Y
16213	Bowling Green	KY	USA	LOW	B	B	C	502	Y
3718	Frankfort	KY	USA	LOW	B	B	C	502	Y
9987	Lexington	KY	USA	MED	B	B	C	606	Y
8678	Louisville	KY	USA	MED	B	B	C	502	Y
1087	Owensboro	KY	USA	LOW	B	B	C	502	Y
02291	Paducah	KY	USA	LOW	B	B	C	502	Y
14288	Alexandria	LA	USA	LOW	B	B	C	318	Y
6999	Baton Rouge	LA	USA	MED	B	B	C	504	Y
6999	Baton Rouge	LA	USA	MED	B	B	C	504	Y
8525	Lafayette	LA	USA	LOW	B	B	C	318	Y
15174	Lake Charles	LA	USA	LOW	B	B	C	318	Y
2480	Monroe	LA	USA	LOW	B	B	C	318	Y
3654	New Orleans	LA	USA	HIGH	B	B	C	504	Y
03654	New Orleans	LA	USA	HIGH	B	B	C	504	Y
03654	New Orleans	LA	USA	HIGH	B	B	C	504	Y
3539	Shreveport	LA	USA	LOW	B	B	C	318	Y
10404	Slidell	LA	USA	LOW	B	B	C	504	Y
7044	Bedford	MA	USA	LOW	B	B	C	617	Y
8796	Boston	MA	USA	HIGH	B	B	C	617	Y
8796	Boston	MA	USA	HIGH	B	B	C	617	Y
753	Brockton/Randolph	MA	USA	LOW	B	B	C	617	Y
8796	Cambridge/Boston	MA	USA	HIGH	B	B	C	617	Y
8796	Cambridge/Boston	MA	USA	HIGH	B	B	C	617	Y
3003	Fall River/Somerset	MA	USA	LOW	B	B	C	508	Y
10677	Fitchburg/Leominster	MA	USA	LOW	B	B	C	508	Y
10148	Groton	MA	USA	LOW	B	B	C	508	Y
3948	Holyoke/Springfield	MA	USA	MED	B	B	C	413	Y
3948	Holyoke/Springfield	MA	USA	MED	B	B	C	413	Y
3948	Holyoke/Springfield	MA	USA	MED	B	B	C	413	Y
11063	Kingston	MA	USA	LOW	B	B	C	617	Y
10020	Lawrence	MA	USA	LOW	B	B	C	508	Y
10677	Leominster	MA	USA	LOW	B	B	C	508	Y
531	Lowell	MA	USA	LOW	B	B	C	508	Y
07745	Lynn	MA	USA	LOW	B	B	C	617	Y

4001	Manchester	MA	USA	LOW	B	B	C	508	Y
432	Marlborough	MA	USA	LOW	B	B	C	508	Y
4216	New Bedford	MA	USA	LOW	B	B	C	508	Y
2478	Pittsfield	MA	USA	LOW	B	B	C	413	Y
753	Randolph	MA	USA	LOW	B	B	C	617	Y
3003	Somerset	MA	USA	LOW	B	B	C	508	Y
3948	Springfield	MA	USA	MED	B	B	C	413	Y
3948	Springfield	MA	USA	MED	B	B	C	413	Y
3948	Springfield	MA	USA	MED	B	B	C	413	Y
11108	Taunton	MA	USA	LOW	B	B	C	508	Y
7044	Woburn/Bedford	MA	USA	LOW	B	B	C	617	Y
3456	Worcester	MA	USA	LOW	B	B	C	508	Y
14437	Aberdeen	MD	USA	LOW	B	B	C	410	Y
10587	Annapolis	MD	USA	LOW	B	B	C	410	Y
4600	Baltimore	MD	USA	HIGH	B	B	C	410	Y
4600	Baltimore	MD	USA	HIGH	B	B	C	410	Y
2262	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703	Y
2262	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703	Y
2262	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703	Y
2262	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703	Y
2262	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703	Y
999	Cumberland	MD	USA	LOW	B	B	C	301	Y
10832	Frederick/Myersville	MD	USA	LOW	B	B	C	301	Y
10832	Hagerstown/Myersvill	MD	USA	LOW	B	B	C	301	Y
10832	Myersville	MD	USA	LOW	B	B	C	301	Y
1758	Rockville	MD	USA	LOW	B	B	C	301	Y
10209	Salisbury	MD	USA	LOW	B	B	C	410	Y
9686	Auburn	ME	USA	LOW	B	B	C	207	Y
7486	Augusta	ME	USA	LOW	B	B	C	207	Y
10860	Bangor	ME	USA	LOW	B	B	C	207	Y
9686	Lewiston/Auburn	ME	USA	LOW	B	B	C	207	Y
4217	Portland	ME	USA	LOW	B	B	C	207	Y
07252	Presque Isle	ME	USA	LOW	B	B	C	207	Y
6438	Ann Arbor	MI	USA	MED	B	B	C	313	Y
10147	Battle Creek	MI	USA	LOW	B	B	C	616	Y
4231	Benton Harbor	MI	USA	LOW	B	B	C	616	Y
894	Burton	MI	USA	LOW	B	B	C	313	Y
4316	Cadillac	MI	USA	LOW	B	B	C	616	Y
8794	Detroit	MI	USA	HIGH	B	B	C	313	Y
8794	Detroit	MI	USA	HIGH	B	B	C	313	Y
894	Flint/Burton	MI	USA	LOW	B	B	C	313	Y
4766	Freeland	MI	USA	LOW	B	B	C	517	Y
4017	Grand Rapids	MI	USA	MED	B	B	C	616	Y
5747	Jackson	MI	USA	LOW	B	B	C	517	Y
3195	Kalamazoo	MI	USA	MED	B	B	C	616	Y
9992	Lansing	MI	USA	MED	B	B	C	517	Y
7225	Marquette	MI	USA	LOW	B	B	C	906	Y
4766	Midland/Freeland	MI	USA	LOW	B	B	C	517	Y
4357	Muskegon	MI	USA	LOW	B	B	C	616	Y
4847	Plymouth	MI	USA	MED	B	B	C	313	Y
10342	Pontiac	MI	USA	LOW	B	B	C	313	Y
4620	Port Huron	MI	USA	LOW	B	B	C	313	Y
10754	Roseville	MI	USA	LOW	B	B	C	313	Y
4766	Saginaw/Freeland	MI	USA	LOW	B	B	C	517	Y
3424	Southfield	MI	USA	MED	B	B	C	313	Y
4231	St. Joe/Benton Hrbr	MI	USA	LOW	B	B	C	616	Y
6066	Traverse City	MI	USA	LOW	B	B	C	616	Y
10933	Duluth	MN	USA	LOW	B	B	C	218	Y
13488	Hibbing	MN	USA	LOW	B	B	C	218	Y
1648	Mankato	MN	USA	LOW	B	B	C	507	Y
3494	Minneapolis	MN	USA	HIGH	B	B	C	612	Y
3494	Minneapolis	MN	USA	HIGH	B	B	C	612	Y
10597	Rochester	MN	USA	LOW	B	B	C	507	Y

10597	Rochester	MN	USA	LOW	B	B	C	507	Y
14283	St. Cloud	MN	USA	LOW	B	B	C	612	Y
3494	St. Paul/Minneapolis	MN	USA	HIGH	B	B	C	612	Y
3494	St. Paul/Minneapolis	MN	USA	HIGH	B	B	C	612	Y
8978	Bridgeton/St. Louis	MO	USA	HIGH	B	B	C	314	Y
8978	Bridgeton/St. Louis	MO	USA	HIGH	B	B	C	314	Y
8856	Cape Girardeau	MO	USA	LOW	B	B	C	314	Y
6017	Columbia	MO	USA	LOW	B	B	C	314	Y
8978	Hazelwood	MO	USA	HIGH	B	B	C	314	Y
8615	Independence/Mission	MO	USA	HIGH	B	B	C	913	Y
8615	Independence/Mission	MO	USA	HIGH	B	B	C	913	Y
2564	Jefferson City	MO	USA	LOW	B	B	C	314	Y
1928	Joplin	MO	USA	LOW	B	B	C	417	Y
8615	Kansas City/Mission	MO	USA	HIGH	B	B	C	913	Y
8615	Kansas City/Mission	MO	USA	HIGH	B	B	C	913	Y
6182	Rolla	MO	USA	LOW	B	B	C	314	Y
5681	Springfield	MO	USA	LOW	B	B	C	417	Y
6192	St. Joseph	MO	USA	LOW	B	B	C	816	Y
8978	St. Louis	MO	USA	HIGH	B	B	C	314	Y
8978	St. Louis	MO	USA	HIGH	B	B	C	314	Y
14342	Gulfport	MS	USA	LOW	B	B	C	601	Y
1164	Hattiesburg	MS	USA	LOW	B	B	C	601	Y
6301	Jackson	MS	USA	LOW	B	B	C	601	Y
6301	Jackson	MS	USA	LOW	B	B	C	601	Y
6491	Meridian	MS	USA	LOW	B	B	C	601	Y
14882	Pascagoula	MS	USA	LOW	B	B	C	601	Y
9901	Tupelo	MS	USA	LOW	B	B	C	601	Y
10874	Vicksburg	MS	USA	LOW	B	B	C	601	Y
3504	Billings	MT	USA	LOW	B	B	C	406	Y
7946	Bozeman	MT	USA	LOW	B	B	C	406	Y
7862	Butte	MT	USA	LOW	B	B	C	406	Y
04506	Great Falls	MT	USA	LOW	B	B	C	406	Y
5136	Helena	MT	USA	LOW	B	B	C	406	Y
274	Asheville	NC	USA	LOW	B	B	C	704	Y
9986	Chapel Hill/Durham	NC	USA	HIGH	B	B	C	919	Y
9986	Chapel Hill/Durham	NC	USA	HIGH	B	B	C	919	Y
6793	Charlotte	NC	USA	HIGH	B	B	C	704	Y
6793	Charlotte	NC	USA	HIGH	B	B	C	704	Y
9986	Durham	NC	USA	HIGH	B	B	C	919	Y
9986	Durham	NC	USA	HIGH	B	B	C	919	Y
10985	Fayetteville	NC	USA	LOW	B	B	C	919	Y
3703	Gastonia	NC	USA	LOW	B	B	C	704	Y
2964	Greensboro	NC	USA	MED	B	B	C	919	Y
2004	Greenville	NC	USA	LOW	B	B	C	919	Y
1737	High Point	NC	USA	LOW	B	B	C	919	Y
7821	Kannapolis	NC	USA	LOW	B	B	C	704	Y
9324	Rocky Mount	NC	USA	LOW	B	B	C	919	Y
14364	Wilmington	NC	USA	LOW	B	B	C	919	Y
7068	Winston-Salem	NC	USA	MED	B	B	C	919	Y
7068	Winston-Salem	NC	USA	MED	B	B	C	919	Y
14444	Bismark	ND	USA	LOW	B	B	C	701	Y
5251	Fargo	ND	USA	LOW	B	B	C	701	Y
7233	Grand Forks	ND	USA	LOW	B	B	C	701	Y
4281	Minot	ND	USA	LOW	B	B	C	701	Y
14994	Minot	ND	USA	LOW	B	B	C	701	Y
6997	Grand Island	NE	USA	LOW	B	B	C	308	Y
9856	Lincoln	NE	USA	LOW	B	B	C	402	Y
2521	Omaha	NE	USA	MED	B	B	C	402	Y
7212	Concord	NH	USA	LOW	B	B	C	603	Y
6651	Durham	NH	USA	LOW	B	B	C	603	Y
3627	Hanover	NH	USA	LOW	B	B	C	603	Y
4027	Manchester	NH	USA	LOW	B	B	C	603	Y
1347	Nashua	NH	USA	MED	B	B	C	603	Y

1696	North Hampton	NH	USA	LOW	B	B	C	603	Y
1554	Peterborough	NH	USA	LOW	B	B	C	603	Y
1347	Salem/Nashua	NH	USA	MED	B	B	C	603	Y
883	Atlantic City	NJ	USA	LOW	B	B	C	609	Y
8693	Camden/Pennsauken	NJ	USA	MED	B	B	C	609	Y
8693	Cherry hill/Pennskn	NJ	USA	MED	B	B	C	609	Y
6334	Eatontown/Red Bank	NJ	USA	LOW	B	B	C	908	Y
6334	Eatontown/Red Bank	NJ	USA	LOW	B	B	C	908	Y
7618	Elizabeth/Newark	NJ	USA	HIGH	B	B	C	201	Y
7618	Elizabeth/Newark	NJ	USA	HIGH	B	B	C	201	Y
6319	Englewood Cliffs	NJ	USA	MED	B	B	C	201	Y
7618	Jersey City/Newark	NJ	USA	HIGH	B	B	C	201	Y
7618	Jersey City/Newark	NJ	USA	HIGH	B	B	C	201	Y
6334	Long Branch/Red Bank	NJ	USA	LOW	B	B	C	908	Y
6334	Long Branch/Red Bank	NJ	USA	LOW	B	B	C	908	Y
4378	Lyndhurst/Union City	NJ	USA	HIGH	B	B	C	201	Y
3820	Morristown	NJ	USA	LOW	B	B	C	201	Y
7618	Newark	NJ	USA	HIGH	B	B	C	201	Y
7618	Newark	NJ	USA	HIGH	B	B	C	201	Y
2312	Paterson	NJ	USA	MED	B	B	C	201	Y
8693	Pennsauken	NJ	USA	MED	B	B	C	609	Y
3319	Piscataway	NJ	USA	HIGH	B	B	C	908	Y
6334	Red Bank	NJ	USA	LOW	B	B	C	908	Y
2312	Ridgewood/Paterson	NJ	USA	MED	B	B	C	201	Y
8920	South Brunswick	NJ	USA	HIGH	B	B	C	609	Y
730	Trenton	NJ	USA	LOW	B	B	C	609	Y
4378	Union City	NJ	USA	HIGH	B	B	C	201	Y
7618	Union/Newark	NJ	USA	HIGH	B	B	C	201	Y
7618	Union/Newark	NJ	USA	HIGH	B	B	C	201	Y
14708	Vineland	NJ	USA	LOW	B	B	C	609	Y
2312	Wayne/Paterson	NJ	USA	MED	B	B	C	201	Y
661	Albuquerque	NM	USA	MED	B	B	C	505	Y
6630	Las Cruces	NM	USA	LOW	B	B	C	505	Y
14541	Rosewell	NM	USA	LOW	B	B	C	505	Y
4604	Santa Fe	NM	USA	LOW	B	B	C	505	Y
2140	Carson City	NV	USA	MED	B	B	C	702	Y
2140	Carson City	NV	USA	MED	B	B	C	702	Y
13943	Las Vegas	NV	USA	MED	B	B	C	702	Y
13943	Las Vegas	NV	USA	MED	B	B	C	702	Y
2140	Reno/Carson City	NV	USA	MED	B	B	C	702	Y
2140	Reno/Carson City	NV	USA	MED	B	B	C	702	Y
9192	Albany	NY	USA	MED	B	B	C	518	Y
5312	Binghamton	NY	USA	LOW	B	B	C	607	Y
9194	Buffalo	NY	USA	MED	B	B	C	716	Y
582	Centereach/Lk Grove	NY	USA	MED	B	B	C	516	Y
6612	Corning	NY	USA	LOW	B	B	C	607	Y
15117	Elmira	NY	USA	LOW	B	B	C	607	Y
09193	Hempstead	NY	USA	MED	B	B	C	516	Y
9193	Hempstead	NY	USA	MED	B	B	C	516	Y
8811	Huntington/Melville	NY	USA	MED	B	B	C	516	Y
11191	Ithaca	NY	USA	LOW	B	B	C	607	Y
8861	Kingston	NY	USA	LOW	B	B	C	914	Y
582	Lake Grove	NY	USA	MED	B	B	C	516	Y
8811	Melville	NY	USA	MED	B	B	C	516	Y
9193	Mineola/Hempstead	NY	USA	MED	B	B	C	516	Y
9193	Mineola/Hempstead	NY	USA	MED	B	B	C	516	Y
10615	New City	NY	USA	LOW	B	B	C	914	Y
1059	New York	NY	USA	HIGH	B	B	C	212	Y
1059	New York	NY	USA	HIGH	B	B	C	212	Y
1059	New York	NY	USA	HIGH	B	B	C	212	Y
1059	New York	NY	USA	HIGH	B	B	C	212	Y
3480	Niagara Falls	NY	USA	LOW	B	B	C	716	Y
6019	Perinton/Pittsford	NY	USA	HIGH	B	B	C	716	Y

6019	Pittsford	NY	USA	HIGH	B	B	C	716	Y
2930	Poughkeepsie	NY	USA	LOW	B	B	C	914	Y
6019	Rochester/Pittsford	NY	USA	HIGH	B	B	C	716	Y
582	Ronkonkoma/Lake Grve	NY	USA	MED	B	B	C	516	Y
9192	Schenectady/Albany	NY	USA	MED	B	B	C	518	Y
4710	Syracuse	NY	USA	MED	B	B	C	315	Y
1101	Utica	NY	USA	LOW	B	B	C	315	Y
08109	Watertown	NY	USA	LOW	B	B	C	315	Y
8571	White Plains	NY	USA	HIGH	B	B	C	914	Y
8571	White Plains	NY	USA	HIGH	B	B	C	914	Y
8740	Akron	OH	USA	MED	B	B	C	216	Y
8740	Akron	OH	USA	MED	B	B	C	216	Y
8160	Canton	OH	USA	LOW	B	B	C	216	Y
1785	Cincinnati	OH	USA	HIGH	B	B	C	513	Y
1785	Cincinnati	OH	USA	HIGH	B	B	C	513	Y
4222	Cleveland	OH	USA	HIGH	B	B	C	216	Y
4222	Cleveland	OH	USA	HIGH	B	B	C	216	Y
9347	Columbus	OH	USA	HIGH	B	B	C	614	Y
9511	Dayton	OH	USA	MED	B	B	C	513	Y
8859	Elyria	OH	USA	LOW	B	B	C	216	Y
1427	Findly	OH	USA	LOW	B	B	C	419	Y
4622	Lima	OH	USA	LOW	B	B	C	419	Y
6022	Mansfield	OH	USA	LOW	B	B	C	419	Y
13471	Springfield	OH	USA	LOW	B	B	C	513	Y
7313	Steubenville/Wntsvl	OH	USA	LOW	B	B	C	614	Y
1190	Toledo	OH	USA	MED	B	B	C	419	Y
1190	Toledo	OH	USA	MED	B	B	C	419	Y
11131	Warren	OH	USA	LOW	B	B	C	216	Y
7313	Wintersville	OH	USA	LOW	B	B	C	614	Y
4909	Youngstown	OH	USA	LOW	B	B	C	216	Y
7231	Ardmore	OK	USA	LOW	B	B	C	405	Y
10816	Enid	OK	USA	LOW	B	B	C	405	Y
16218	Lawton	OK	USA	LOW	B	B	C	405	Y
9165	Oklahoma City	OK	USA	HIGH	B	B	C	405	Y
6605	Tulsa	OK	USA	HIGH	B	B	C	918	Y
06605	Tulsa	OK	USA	HIGH	B	B	C	918	Y
2820	Bend	OR	USA	LOW	B	B	C	503	Y
8603	Corvallis	OR	USA	LOW	B	B	C	503	Y
9857	Eugene	OR	USA	LOW	B	B	C	503	Y
7883	Medford	OR	USA	LOW	B	B	C	503	Y
9164	Portland	OR	USA	HIGH	B	B	C	503	Y
9164	Portland	OR	USA	HIGH	B	B	C	503	Y
3174	Salem	OR	USA	LOW	B	B	C	503	Y
9857	Springfield/Eugene	OR	USA	LOW	B	B	C	503	Y
3432	Allentown/Bethlehem	PA	USA	MED	B	B	C	215	Y
7025	Altoona	PA	USA	LOW	B	B	C	814	Y
3432	Bethlehem	PA	USA	MED	B	B	C	215	Y
3896	Butler	PA	USA	LOW	B	B	C	412	Y
182	Coatesville	PA	USA	LOW	B	B	C	215	Y
182	Downington/Coatsvllle	PA	USA	LOW	B	B	C	215	Y
3338	Erie	PA	USA	LOW	B	B	C	814	Y
13069	Greensburg	PA	USA	LOW	B	B	C	412	Y
1707	Harrisburg/Lemoyne	PA	USA	MED	B	B	C	717	Y
8376	Johnstown	PA	USA	LOW	B	B	C	814	Y
508	KingofPrussa/Norstwn	PA	USA	MED	B	B	C	215	Y
7853	Lancaster	PA	USA	LOW	B	B	C	717	Y
13069	Latrobe/Greensburg	PA	USA	LOW	B	B	C	412	Y
1707	Lemoyne	PA	USA	MED	B	B	C	717	Y
14610	Mt. Penn	PA	USA	LOW	B	B	C	215	Y
7851	New Castle	PA	USA	LOW	B	B	C	412	Y
508	Norristown	PA	USA	MED	B	B	C	215	Y
9581	Philadelphia	PA	USA	HIGH	B	B	C	215	Y
9581	Philadelphia	PA	USA	HIGH	B	B	C	215	Y

9581	Philadelphia	PA	USA	HIGH	B	B	C	215	Y
7408	Pittsburgh	PA	USA	HIGH	B	B	C	412	Y
1572	Scranton	PA	USA	LOW	B	B	C	717	Y
8907	Secane	PA	USA	LOW	B	B	C	215	Y
3765	State College	PA	USA	LOW	B	B	C	814	Y
508	Valley Forge/Norstwn	PA	USA	MED	B	B	C	215	Y
7941	Wilkes Barre	PA	USA	LOW	B	B	C	717	Y
11157	Williamsport	PA	USA	LOW	B	B	C	717	Y
4382	York	PA	USA	LOW	B	B	C	717	Y
6425	Middletown	RI	USA	LOW	B	B	C	401	Y
6425	Newport/Middletown	RI	USA	LOW	B	B	C	401	Y
9130	Pawtucket/Providence	RI	USA	HIGH	B	B	C	401	Y
9130	Pawtucket/Providence	RI	USA	HIGH	B	B	C	401	Y
9130	Providence	RI	USA	HIGH	B	B	C	401	Y
9130	Providence	RI	USA	HIGH	B	B	C	401	Y
9130	Warwick/Providence	RI	USA	HIGH	B	B	C	401	Y
9130	Warwick/Providence	RI	USA	HIGH	B	B	C	401	Y
11293	Woonsocket	RI	USA	LOW	B	B	C	401	Y
2917	Aiken	SC	USA	LOW	B	B	C	803	Y
9907	Charleston	SC	USA	LOW	B	B	C	803	Y
9993	Columbia	SC	USA	MED	B	B	C	803	Y
9993	Columbia	SC	USA	MED	B	B	C	803	Y
9993	Columbia	SC	USA	MED	B	B	C	803	Y
8860	Florence	SC	USA	LOW	B	B	C	803	Y
3380	Greenville	SC	USA	MED	B	B	C	803	Y
3380	Greenville	SC	USA	MED	B	B	C	803	Y
935	Myrtle Beach	SC	USA	LOW	B	B	C	803	Y
14407	Spartanburg	SC	USA	LOW	B	B	C	803	Y
8872	Pierre	SD	USA	LOW	B	B	C	605	Y
2171	Rapid City	SD	USA	LOW	B	B	C	605	Y
8819	Sioux Falls	SD	USA	LOW	B	B	C	605	Y
1836	Blountville	TN	USA	LOW	B	B	C	615	Y
2937	Chattanooga	TN	USA	MED	B	B	C	615	Y
5720	Clarkesville	TN	USA	LOW	B	B	C	615	Y
3175	Jackson	TN	USA	LOW	B	B	C	901	Y
8502	Johnson City	TN	USA	LOW	B	B	C	615	Y
8328	Kingsport	TN	USA	LOW	B	B	C	615	Y
13895	Knoxville	TN	USA	MED	B	B	C	615	Y
13895	Knoxville	TN	USA	MED	B	B	C	615	Y
1551	Memphis	TN	USA	MED	B	B	C	901	Y
1551	Memphis	TN	USA	MED	B	B	C	901	Y
9141	Nashville	TN	USA	HIGH	B	B	C	615	Y
9141	Nashville	TN	USA	HIGH	B	B	C	615	Y
9141	Nashville	TN	USA	HIGH	B	B	C	615	Y
9683	Oakridge	TN	USA	LOW	B	B	C	615	Y
9114	Sevierville	TN	USA	LOW	B	B	C	615	Y
6980	Abilene	TX	USA	LOW	B	B	C	915	Y
8736	Amarillo	TX	USA	LOW	B	B	C	806	Y
9337	Arlington/Fort Worth	TX	USA	MED	B	B	C	817	Y
1306	Austin	TX	USA	HIGH	B	B	C	512	Y
1306	Austin	TX	USA	HIGH	B	B	C	512	Y
1306	Austin	TX	USA	HIGH	B	B	C	512	Y
7758	Baytown	TX	USA	LOW	B	B	C	713	Y
5115	Brownsville	TX	USA	LOW	B	B	C	512	Y
14871	Bryan	TX	USA	LOW	B	B	C	409	Y
4497	College Statn/Bryan	TX	USA	LOW	B	B	C	409	Y
11966	Corpus Christi	TX	USA	MED	B	B	C	512	Y
2948	Dallas	TX	USA	HIGH	B	B	C	214	Y
2948	Dallas	TX	USA	HIGH	B	B	C	214	Y
2948	Dallas	TX	USA	HIGH	B	B	C	214	Y
5990	Denton	TX	USA	LOW	B	B	C	817	Y
210	El Paso	TX	USA	MED	B	B	C	915	Y
210	El Paso	TX	USA	MED	B	B	C	915	Y

9337	Fort Worth	TX	USA	MED	B	B	C	817	Y
3615	Galveston	TX	USA	LOW	B	B	C	409	Y
13481	Harlingen	TX	USA	LOW	B	B	C	512	Y
4562	Houston	TX	USA	HIGH	B	B	C	713	Y
4562	Houston	TX	USA	HIGH	B	B	C	713	Y
4562	Houston	TX	USA	HIGH	B	B	C	713	Y
4562	Houston	TX	USA	HIGH	B	B	C	713	Y
4562	Houston	TX	USA	HIGH	B	B	C	713	Y
9861	Killeen	TX	USA	LOW	B	B	C	817	Y
3715	Laredo	TX	USA	LOW	B	B	C	512	Y
948	Longview	TX	USA	LOW	B	B	C	903	Y
4435	Lubbock	TX	USA	LOW	B	B	C	806	Y
12022	Mcallen	TX	USA	LOW	B	B	C	512	Y
8254	McKinney	TX	USA	LOW	B	B	C	214	Y
04905	Midland	TX	USA	LOW	B	B	C	915	Y
9322	Nederland/Pt. Arthur	TX	USA	LOW	B	B	C	409	Y
2326	Odessa/Midland	TX	USA	LOW	B	B	C	915	Y
9322	Port Arthur	TX	USA	LOW	B	B	C	409	Y
8511	San Angelo	TX	USA	LOW	B	B	C	915	Y
9169	San Antonio	TX	USA	HIGH	B	B	C	512	Y
09169	San Antonio	TX	USA	HIGH	B	B	C	512	Y
9169	San Antonio	TX	USA	HIGH	B	B	C	512	Y
6248	Sherman	TX	USA	LOW	B	B	C	903	Y
14777	Temple	TX	USA	LOW	B	B	C	817	Y
8871	Texarkana	TX	USA	LOW	B	B	C	903	Y
3615	Texas City/Galveston	TX	USA	LOW	B	B	C	409	Y
3826	Tyler	TX	USA	LOW	B	B	C	903	Y
10996	Victoria	TX	USA	LOW	B	B	C	512	Y
9859	Waco	TX	USA	LOW	B	B	C	817	Y
6862	Wichita Falls	TX	USA	LOW	B	B	C	817	Y
07936	Ogden	UT	USA	LOW	B	B	C	801	Y
534	Salt Lake City	UT	USA	HIGH	B	B	C	801	Y
534	Salt Lake City	UT	USA	HIGH	B	B	C	801	Y
2262	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703	Y
8531	Charlottesville	VA	USA	LOW	B	B	C	804	Y
2262	Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Fairfax	VA	USA	HIGH	B	B	C	703	Y
2262	Fairfax	VA	USA	HIGH	B	B	C	703	Y
8215	Hampton	VA	USA	MED	B	B	C	804	Y
10149	Harrisonburg	VA	USA	LOW	B	B	C	703	Y
2839	Lynchburg	VA	USA	LOW	B	B	C	804	Y
4975	Manassas	VA	USA	LOW	B	B	C	703	Y
413	Midlothian/Richmond	VA	USA	MED	B	B	C	804	Y
413	Midlothian/Richmond	VA	USA	MED	B	B	C	804	Y
8459	Newport News	VA	USA	MED	B	B	C	804	Y
6986	Norfolk	VA	USA	MED	B	B	C	804	Y
14706	Petersburg	VA	USA	LOW	B	B	C	804	Y
6986	Portsmouth/Norfolk	VA	USA	MED	B	B	C	804	Y
6986	Portsmouth/Norfolk	VA	USA	MED	B	B	C	804	Y
413	Richmond	VA	USA	MED	B	B	C	804	Y
413	Richmond	VA	USA	MED	B	B	C	804	Y
4026	Roanoke	VA	USA	LOW	B	B	C	703	Y

6986	Virginia Bch/Norfolk	VA	USA	MED	B	B	C	804	Y
6986	Virginia Bch/Norfolk	VA	USA	MED	B	B	C	804	Y
4557	Williamsburg	VA	USA	LOW	B	B	C	804	Y
3435	Burlington	VT	USA	LOW	B	B	C	802	Y
1827	Auburn	WA	USA	LOW	B	B	C	206	Y
9170	Bellevue/Seattle	WA	USA	HIGH	B	B	C	206	Y
9170	Bellevue/Seattle	WA	USA	HIGH	B	B	C	206	Y
9170	Bellevue/Seattle	WA	USA	HIGH	B	B	C	206	Y
8373	Bellingham	WA	USA	LOW	B	B	C	206	Y
773	Bremerton	WA	USA	LOW	B	B	C	206	Y
1827	Enumclaw/Auburn	WA	USA	LOW	B	B	C	206	Y
5133	Everett	WA	USA	LOW	B	B	C	206	Y
2944	Longview	WA	USA	LOW	B	B	C	206	Y
2508	Olympia	WA	USA	LOW	B	B	C	206	Y
6113	Port Angeles	WA	USA	LOW	B	B	C	206	Y
5298	Pullman	WA	USA	LOW	B	B	C	509	Y
2116	Richland	WA	USA	MED	B	B	C	509	Y
2116	Richland	WA	USA	MED	B	B	C	509	Y
9170	Seattle	WA	USA	HIGH	B	B	C	206	Y
9170	Seattle	WA	USA	HIGH	B	B	C	206	Y
9170	Seattle	WA	USA	HIGH	B	B	C	206	Y
159	Spokane	WA	USA	MED	B	B	C	509	Y
906	Tacoma	WA	USA	LOW	B	B	C	206	Y
5447	Vancouver	WA	USA	LOW	B	B	C	206	Y
8931	Yakima	WA	USA	LOW	B	B	C	509	Y
8868	Appleton	WI	USA	LOW	B	B	C	414	Y
5314	Beloit	WI	USA	LOW	B	B	C	608	Y
9167	Brookfield	WI	USA	HIGH	B	B	C	414	Y
9786	Eau Claire	WI	USA	LOW	B	B	C	715	Y
3421	Green Bay	WI	USA	LOW	B	B	C	414	Y
5314	Janesville/Beloit	WI	USA	LOW	B	B	C	608	Y
6966	Kenosha	WI	USA	LOW	B	B	C	414	Y
4633	La Crosse	WI	USA	LOW	B	B	C	608	Y
2635	Madison	WI	USA	LOW	B	B	C	608	Y
9167	Milwaukee/Brookfield	WI	USA	HIGH	B	B	C	414	Y
5966	Oshkosh	WI	USA	LOW	B	B	C	414	Y
6966	Racine/Kenosha	WI	USA	LOW	B	B	C	414	Y
1792	Sheboygan	WI	USA	LOW	B	B	C	414	Y
5144	Wausau	WI	USA	LOW	B	B	C	715	Y
5465	West Bend	WI	USA	LOW	B	B	C	414	Y
3431	Charleston	WV	USA	LOW	B	B	C	304	Y
6594	Huntington	WV	USA	LOW	B	B	C	304	Y
890	Morgantown	WV	USA	LOW	B	B	C	304	Y
12924	Parkersburg	WV	USA	LOW	B	B	C	304	Y
890	Westover/Morgantown	WV	USA	LOW	B	B	C	304	Y
6681	Wheeling	WV	USA	LOW	B	B	C	304	Y
10537	Casper	WY	USA	LOW	B	B	C	307	Y
4213	Cheyenne	WY	USA	LOW	B	B	C	307	Y
1752	Laramie	WY	USA	LOW	B	B	C	307	Y

B=BELL 103/113 (300 bps) or BELL 212A (1200 bps) compatible modems.

C=CCITT V.21(300 bps) or CCITT V.22 bis(2400 bps) or CCITT V.32 compatible modems.

==Phrack Inc.==

Volume Four, Issue Forty, File 10 of 14

	BT Tymnet	
	British Telecom	

Part 3 of 3

Presented by Toucan Jones

August 1, 1992

Welcome Back to Tymnet Again!

PART 1

- A. BT Tymnet Access Location Index
- B. BT-GNS Access Within Regional Bell Operating Companies
 - 1. Bell Atlantic
 - 2. BellSouth
 - 3. Pacific Bell
 - 4. Southwestern Bell
 - 5. Southern New England Telephone
- C. Database or Timesharing Companies on Tymnet
- D. Service Classifications For Database or Timesharing Companies Using Tymnet
- E. Summary of Global Network Services By Country
- F. Terminal Identifiers
- G. Login Options

PART 2

- H. BT-GNS Worldwide Asynchronous Outdial Service

PART 3

- I. BT-GNS Worldwide Access Sorted By Node

I. BT-GNS Worldwide Access Sorted By Node

NODE	CITY	PROV ST	CNTRY	DENS	DIALUP ACCESS 100'S BPS				ACCESS NO.	M N P	COMMENTS
					3	12	24	96			
	Porto Alegre		BRA	BGC	C				(011) 15331	N	BGC Access
	Porto Alegro		BRA	BGC	C				(011) 15311	N	BGC Access
	Cartago		CRI	BGC	C	C			51-2000	N	BGC Access
	C. Quesada		CRI	BGC	C	C			46-2000	N	BGC Access
	Heredia		CRI	BGC	C	C			38-2000	N	BGC Access
	Kuwait City		KUW	BGC	C				143	N	BGC Access
	Rio		BRA	BGC	C				(021)2538153	N	BGC Access
	Cairo		EGY	BGC	C				(2)3907102	N	BGC Access
	Sao Paolo		BRA	BGC	C				(011) 1531	N	BGC Access
	Antofaganta		CHI	BGC	C	C			(083)251634	Y	BGC Access
	Iguigue		CHI	BGC	C	C			(051)27907	Y	BGC Access
	La Serena		CHI	BGC	C	C			(051)215751	Y	BGC Access
	Punta Arenas		CHI	BGC	C	C			(061)28018	Y	BGC Access
	Santiago		CHI	BGC	C	C			(02)6987788	Y	BGC Access
	Talca		CHI	BGC	C	C			(041)234814	Y	BGC Access
	Temuco		CHI	BGC	C	C			(045)231476	Y	BGC Access
	Valdivia		CHI	BGC	C	C			(061)28018	Y	BGC Access
	Valparaiso		CHI	BGC	C	C			(032)258052	Y	BGC Access
	Beijing		CNA	BGC	C				3014443	N	BGC Access
	Alajvela		CRI	BGC	C	C			41-2000	N	BGC Access
	Liberia		CRI	BGC	C	C			66-2000	N	BGC Access
	Cairo		EGY	BGC	C				(2) 390-9111	N	BGC Access
	Orste		CRI	BGC	C	C			20-2000	N	BGC Access

Limon		CRI	BGC	C	C		58-2000	N	BGC	Access
Puntapbnas		CRI	BGC	C	C		61-2000	N	BGC	Access
San Jose		CRI	BGC	C	C		57-2000	N	BGC	Access
S.Isidro		CRI	BGC	C	C		71-2000	N	BGC	Access
Cairo		EGY	BGC		C		(2) 390-7203	N	BGC	Access
Bombay		IND	BGC		C		(22) 275-916	N	BGC	Access
Bombay		IND	BGC			C	(22) 275-847	N	BGC	Access
Adak	AK	USA	ALAS	B	B	C	907/592-2557	N		
Anchorage	AK	USA	ALAS			C	907/258-6607	Y		
Anchorage	AK	USA	ALAS	B	B		907/258-7222	N		
Barrow	AK	USA	ALAS	B	B		907/852-2425	N	Stat	Mux
Bethel	AK	USA	ALAS	B	B		907/543-2411	N	Stat	Mux
Cantwell	AK	USA	ALAS	B	B	C	907/768-2700	N		
Cordova	AK	USA	ALAS	B	B		907/424-3744	N		
Craig	AK	USA	ALAS	B	B	C	907/826-2948	N		
Dead horse	AK	USA	ALAS	B	B		907/659-2777	N		
Delta Junction	AK	USA	ALAS	B	B		907/895-5070	N		
Dillingham	AK	USA	ALAS	B	B		907/842-2688	N	Stat	Mux
Dutch Harbor	AK	USA	ALAS	B	B	C	907/581-1820	N		
Fairbanks	AK	USA	ALAS			C	907/452-5848	Y		
Fairbanks	AK	USA	ALAS	B	B		907/456-3282	N		
Glennallen	AK	USA	ALAS	B	B		907/822-5231	N		
Haines	AK	USA	ALAS	B			907/766-2171	N		
Healy	AK	USA	ALAS	B	B	C	907/683-1350	N		
Homer	AK	USA	ALAS	B	B		907/235-5239	N		
Juneau	AK	USA	ALAS			C	907/789-1976	Y		
Juneau	AK	USA	ALAS	B	B		907/789-7009	N		
Kenai	AK	USA	ALAS	B	B		907/262-1990	N		
Ketchikan	AK	USA	ALAS	B	B		907/225-1871	N	Stat	Mux
King Salmon	AK	USA	ALAS	B	B		907/246-3049	N		
Kodiak	AK	USA	ALAS	B	B		907/486-4061	N	Stat	Mux
Kotzebue	AK	USA	ALAS	B	B		907/442-2602	N		
Mcgrath	AK	USA	ALAS	B	B		907/524-3256	N	Stat	Mux
Menana	AK	USA	ALAS	B			907/832-5214	N		
Nome	AK	USA	ALAS	B	B		907/443-2256	N	Stat	Mux
Northway	AK	USA	ALAS	B	B		907/778-2301	N	Stat	Mux
Palmer/Wasilla	AK	USA	ALAS	B	B		907/745-0200	N		
Petersburg	AK	USA	ALAS	B			907/772-3878	N		
Prudhoe Bay	AK	USA	ALAS	B	B		907/659-2777	N		
Seward	AK	USA	ALAS	B	B		907/224-3126	N	Stat	Mux
Sitka	AK	USA	ALAS	B	B		907/747-5887	N	Stat	Mux
Skagway	AK	USA	ALAS	B			907/983-2170	N		
Soldotna/Kenai	AK	USA	ALAS	B	B		907/262-1990	N		
St. Paul	AK	USA	ALAS	B	B		907/546-2320	N	Stat	Mux
Tanana	AK	USA	ALAS	B	B		907/366-7167	N	Stat	Mux
Tok	AK	USA	ALAS	B			907/883-4747	N		
Unalaska/Dutch Hbr.	AK	USA	ALAS	B	B	C	907/581-1820	N		
Valdez	AK	USA	ALAS	B	B		907/835-4987	N	Stat	Mux
Wasilla	AK	USA	ALAS	B	B		907/745-0200	N		
Whittier	AK	USA	ALAS	B	B		907/472-2467	N	Stat	Mux
Wrangell	AK	USA	ALAS	B			907/874-2394	N		
Yakutat	AK	USA	ALAS	B	B		907/784-3453	N	Stat	Mux
Kuwait City		KUW	BGC		C		142	N	BGC	Access
Kuwait City		KUW	BGC			C	141	N	BGC	Access
Kuala Lumpur		MAL	BGC	C			(30) 2328800	N	BGC	Access
Kuala Lumpur		MAL	BGC		C		(30) 2328855	N	BGC	Access
Penang		MAL	BGC	C			(04) 375588	N	BGC	Access
Penang		MAL	BGC		C		(04) 360088	N	BGC	Access
Kota Kinabalu		MAL	BGC	C			(088) 218800	N	BGC	Access
Kota Kinabalu		MAL	BGC		C		(088) 218855	N	BGC	Access
Petaling		MAL	BGC	C	C		(03) 7926600	N	BGC	Access
Ipoh		MAL	BGC	C			(05) 548533	N	BGC	Access
Abu Dhabi		UAE	BGC			C	(4) 400-2763	N	BGC	Access

	Surabaya		IND	BGC	C		21242	N	BGC	Access
	Jakarta		IND	BGC	C		3805476	N	BGC	Access
	Abu Dhabi		UAE	BGC		C	(4) 4002764	N	BGC	Access
	Izmir		TUR	BGC		C	145-20	N	BGC	Access
	Abu Dhabi		UAE	BGC	C		(4) 400-2760	N	BGC	Access
	Jakarta		IND	BGC		C	3805445	N	BGC	Access
	Jakarta		IND	BGC	C		3805477	N	BGC	Access
	Bandung		IND	BGC	C		57441	N	BGC	Access
	Abidjan		IVC	BGC	C	C	612211	N	BGC	Access
	Lisbon		POR	BGC		C	(06) 7174	N	BGC	Access
	Kuantan		MAL	BGC	C		(09) 508800	N	BGC	Access
	Istanbul		TUR	BGC		C	511 4083	N	BGC	Access
	Coimbra		POR	BGC		C	(03) 7173	N	BGC	Access
	Khon Kaen		THA	BGC		C	(2) 245-581	N	BGC	Access
	Abu Dhabi		UAE	BGC		C	(4) 400-2761	N	BGC	Access
	Abidjan		IVC	BGC		C	612210	N	BGC	Access
	Coimbra		POR	BGC	C		(03) 7172	N	BGC	Access
	Bangkok		THA	BGC	C		(2) 233-9905	N	BGC	Access
	Jakarta		IND	BGC		C	370208	N	BGC	Access
	Jakarta		IND	BGC		C	370195	N	BGC	Access
	Medan		IND	BGC	C		510977	N	BGC	Access
	Semarang		IND	BGC	C	C	20008	N	BGC	Access
	Porto		POR	BGC		C	(05) 7173	N	BGC	Access
	Porto		POR	BGC	C		(05) 7172	N	BGC	Access
	Porto		POR	BGC		C	(05) 7173	N	BGC	Access
	Medan		IND	BGC	C		511977	N	BGC	Access
	Medan		IND	BGC		C	512977	N	BGC	Access
	Medan		IND	BGC		C	513977	N	BGC	Access
	Ipoh		MAL	BGC		C	(05) 548444	N	BGC	Access
	Lisbon		POR	BGC		C	(06) 7172	N	BGC	Access
	Pattaya		THA	BGC		C	(2) 425-313	N	BGC	Access
	Coimbra		POR	BGC		C	(03) 7173	N	BGC	Access
	Ankara		TUR	BGC		C	310 4805	N	BGC	Access
	Lisbon		POR	BGC		C	(06) 7173	N	BGC	Access
	St. Thomas		VIR	3		B	809/776-7084	N	TYMUSA	
	St. Thomas		VIR	3		B	809/774-7099	N	TYMUSA	
	Bangkok		THA	BGC		C	(2) 233-2312	N	BGC	Access
	Rio		BRA	BGC	C		(021)2538151	N	BGC	Access
	San Pedro		CRI	BGC	C	C	53-2000	N	BGC	Access
	Chiengmai		THA	BGC		C	(2) 248-719	N	BGC	Access
	Athens		GRC	BGC		C	(1) 884-8428	N	BGC	Access
	Kuantan		MAL	BGC		C	(09) 508855	N	BGC	Access
	Reykjavik		ICE	BGC		C	006	N	BGC	Access
	Hong Kong		HKG	PAC		C	05-877-2553	N	BISYNC	
1663	Annapolis	MD	USA	LOW	B	B	C	410/224-0520	Y	
02026	Marshalltown	IA	USA	LOW	B	B	C	515/753-0670	Y	
02027	Milan		ITA	E2	B	C	C	(2) 66983004	N	
02040	Geneva		CHE	E1	C	C	C	(22) 782-9329	Y	
02045	Albany	NY	USA	MED	B	B	C	518/458-9724	Y	
02045	Schenectady/Albany	NY	USA	MED	B	B	C	518/458-9724	Y	
02050	Casper	WY	USA	LOW	B	B	C	307/234-4211	Y	
02051	Cincinnati	OH	USA	HIGH			C	513/489-2435	N	TYM-X25
02051	Cincinnati	OH	USA	HIGH			C	513/489-2664	N	TYM-X25
02057	Sevierville	TN	USA	LOW	B	B	C	615/453-0401	Y	
02066	Indianapolis	IN	USA	HIGH	B	B		317/631-1002	N	
02071	Las Cruces	NM	USA	LOW	B	B	C	505/525-3401	Y	
02074	Eugene	OR	USA	LOW	B	B	C	503/343-0044	Y	
02076	Oakland	CA	USA	HIGH			C	510/635-1662	N	TYM-X25
02076	Alameda/Oakland	CA	USA	HIGH			C	510/635-1662	N	TYM-X25
02076	Berkeley/Oakland	CA	USA	HIGH			C	510/635-1662	N	TYM-X25
02076	Hayward/Oakland	CA	USA	HIGH			C	510/635-1662	N	TYM-X25
02124	Yakima	WA	USA	LOW	B	B	C	509/248-1462	Y	
02145	Norristown	PA	USA	MED			C	215/666-1984	N	

02155	Bloomington	IN	USA	LOW	B	B	C	812/332-0544	Y	
02156	Dallas	TX	USA	HIGH	B	B	C	214/630-5516	Y	
02163	Cheyenne	WY	USA	LOW	B	B	C	307/638-0403	Y	
02235	Seattle	WA	USA	HIGH	B	B	C	206/281-7141	Y	
02235	Bellevue/Seattle	WA	USA	HIGH	B	B	C	206/281-7141	Y	
02246	Birmingham	AL	USA	HIGH	B	B		205/942-4141	N	
02253	Boston	MA	USA	HIGH				C 617/439-7628	N	TYM-X25
02253	Cambridge/Boston	MA	USA	HIGH				C 617/439-7628	N	TYM-X25
02256	Elgin	IL	USA	LOW	B	B	C	708/888-8113	Y	
02261	Burlington	VT	USA	LOW	B	B	C	802/862-1000	Y	
02265	Albuquerque	NM	USA	MED	B	B	C	505/242-8931	Y	
02301	Eau Claire	WI	USA	LOW	B	B	C	715/833-0121	Y	
02304	New York	NY	USA	HIGH				C 212/269-4640	Y	
02326	Ormond Beach	FL	USA	LOW	B	B	C	904/673-0034	Y	
02331	Seattle	WA	USA	HIGH	B	B	C	206/281-7141	Y	
02331	Bellevue/Seattle	WA	USA	HIGH	B	B	C	206/281-7141	Y	
02340	Newark	NJ	USA	HIGH				C 201/824-4201	Y	
02340	Elizabeth/Newark	NJ	USA	HIGH				C 201/824-4201	Y	
02340	Jersey City/Newark	NJ	USA	HIGH				C 201/824-4201	Y	
02340	Union/Newark	NJ	USA	HIGH				C 201/824-4201	Y	
02344	Knoxville	TN	USA	MED	B	B	C	615/694-0156	Y	
02346	Norristown	PA	USA	WATS	B	B	C	800/###-####	Y	
02347	Grand Junction	CO	USA	LOW	B	B	C	303/241-1643	Y	
02354	Baltimore	MD	USA	HIGH	B	B		410/547-8100	N	
02357	Bloomfield	CT	USA	HIGH	B	B		203/242-7140	N	
02357	Hartford/Bloomfield	CT	USA	HIGH	B	B		203/242-7140	N	
02364	Mesa/Phoenix	AZ	USA	HIGH	B	B		602/254-5811	N	
02364	Phoenix	AZ	USA	HIGH	B	B		602/254-5811	N	
02367	Champaign/Urbana	IL	USA	LOW	B	B	C	217/344-3400	Y	
02367	Urbana	IL	USA	LOW	B	B	C	217/344-3400	Y	
02376	Lima	OH	USA	LOW	B	B	C	419/228-6343	Y	
02377	Minneapolis	MN	USA	HIGH				C 612/338-0845	Y	
02377	St. Paul/Minneapolis	MN	USA	HIGH				C 612/338-0845	Y	
02402	Hattiesburg	MS	USA	LOW	B	B	C	601/582-0286	Y	
02413	Birmingham	GBR	E1		C	C	C	(21632) 6636	Y	
02414	Aurora/Denver	CO	USA	HIGH	B	B		303/830-9210	N	
02414	Boulder/Denver	CO	USA	HIGH	B	B		303/830-9210	N	
02414	Denver	CO	USA	HIGH	B	B		303/830-9210	N	
02423	All Cities	CAY	3		B	B		809/949-7100	N	TYMUSA
02432	Chattanooga	TN	USA	MED	B	B	C	615/265-1020	Y	
02435	Williamsburg	VA	USA	LOW	B	B	C	804/229-6786	Y	
02440	Brookfield	WI	USA	HIGH	B	B		414/785-1614	N	
02440	Milwaukee/Brookfield	WI	USA	HIGH	B	B		414/785-1614	N	
02443	Burbank	CA	USA	LOW	B	B	C	818/841-4795	Y	
02443	Glendale/Burbank	CA	USA	LOW	B	B	C	818/841-4795	Y	
02446	Texarkana	TX	USA	LOW	B	B	C	903/792-4521	Y	
02450	KingofPrussa/Norstwn	PA	USA	MED	B	B	C	215/666-9190	Y	
02450	Valley Forge/Norstwn	PA	USA	MED	B	B	C	215/666-9190	Y	
02453	Dallas	TX	USA	HIGH	B	B		214/638-8888	N	
02465	Downrs Grove/Gln Eln	IL	USA	MED	B	B		708/790-4400	N	
02465	Glen Ellyn	IL	USA	MED	B	B		708/790-4400	N	
02465	Wheaton/Glen Ellyn	IL	USA	MED	B	B		708/790-4400	N	
02472	Paris	FRA	E1		C	C	C	(1) 47728080	Y	
02475	White Plains	NY	USA	HIGH	B	B	C	914/761-9590	Y	
02477	Alkmaar	NLD	E1		C	C	C	C (72) 155190	Y	
02503	Bellevue/Seattle	WA	USA	HIGH	B	B		206/285-0109	N	
02503	Seattle	WA	USA	HIGH	B	B		206/285-0109	N	
02517	Nashville	TN	USA	HIGH	B	B	C	615/889-5790	Y	
02521	Jacksonville	FL	USA	MED				C 904/724-5994	Y	
02544	Washington/Fairfax	DC	USA	HIGH	B	B		703/691-8200	N	
02544	Bethesda/Fairfax	MD	USA	HIGH	B	B		703/691-8200	N	
02544	Alexandria/Fairfax	VA	USA	HIGH	B	B		703/691-8200	N	
02544	Arlington/Fairfax	VA	USA	HIGH	B	B		703/691-8200	N	

02544	Fairfax	VA	USA	HIGH	B	B		703/691-8200	N	
02545	Washington/Fairfax	DC	USA	HIGH	B	B		703/691-8200	N	
02545	Bethesda/Fairfax	MD	USA	HIGH	B	B		703/691-8200	N	
02545	Alexandria/Fairfax	VA	USA	HIGH	B	B		703/691-8200	N	
02545	Arlington/Fairfax	VA	USA	HIGH	B	B		703/691-8200	N	
02545	Fairfax	VA	USA	HIGH	B	B		703/691-8200	N	
02557	Tyler	TX	USA	LOW	B	B	C	903/581-8652	Y	
02560	Neuchatel		CHE	E1	C	C	C	(38) 338606	Y	
02565	Boise	ID	USA	MED	B	B		208/343-0404	N	
02566	Pierre	SD	USA	LOW	B	B	C	605/224-7700	Y	
02570	Dayton	OH	USA	MED	B	B		513/898-0124	N	
02571	Aurora/Denver	CO	USA	HIGH			C	303/830-9032	N	TYM-X25
02571	Boulder/Denver	CO	USA	HIGH			C	303/830-9032	N	TYM-X25
02606	Elizabeth/Newark	NJ	USA	HIGH	B	B		201/824-1212	N	
02606	Jersey City/Newark	NJ	USA	HIGH	B	B		201/824-1212	N	
02606	Newark	NJ	USA	HIGH	B	B		201/824-1212	N	
02606	Union/Newark	NJ	USA	HIGH	B	B		201/824-1212	N	
02610	Fairfield	CA	USA	LOW	B	B	C	707/421-0106	Y	
02613	Chapel Hill/Durham	NC	USA	HIGH	B	B		919/549-8952	N	
02613	Durham	NC	USA	HIGH	B	B		919/549-8952	N	
02614	Lancaster	CA	USA	LOW	B	B	C	805/945-4962	Y	
02616	Manchester	MA	USA	LOW	B	B	C	508/526-1506	Y	
02630	Sherman	TX	USA	LOW	B	B	C	903/868-0089	Y	
02631	Anaheim/Newprt Beach	CA	USA	HIGH	B	B		714/756-8341	N	
02631	Irvine/Newport Beach	CA	USA	HIGH	B	B		714/756-8341	N	
02631	Newport Beach	CA	USA	HIGH	B	B		714/756-8341	N	
02631	Santa Ana/Newprt Bch	CA	USA	HIGH	B	B		714/756-8341	N	
02635	Richland	WA	USA	MED	B	B	C	509/375-3367	Y	
02640	Peterborough	NH	USA	LOW	B	B	C	603/924-7090	Y	
02644	Anaheim/Newprt Beach	CA	USA	HIGH			C	714/752-1493	Y	
02644	Irvine/Newport Beach	CA	USA	HIGH			C	714/752-1493	Y	
02644	Newport Beach	CA	USA	HIGH			C	714/752-1493	Y	
02644	Santa Ana/Newprt Bch	CA	USA	HIGH			C	714/752-1493	Y	
02653	Stamford	CT	USA	HIGH	B	B		203/965-0000	N	
02655	Colton	CA	USA	MED	B	B		714/370-1200	N	
02655	Riverside/Colton	CA	USA	MED	B	B		714/370-1200	N	
02655	San Bernadino/Colton	CA	USA	MED	B	B		714/370-1200	N	
02657	Pawtucket/Providence	RI	USA	HIGH			C	401/751-8030	Y	
02657	Pawtucket/Providence	RI	USA	HIGH	B	B	C	401/273-0200	Y	
02657	Providence	RI	USA	HIGH			C	401/751-8030	Y	
02657	Providence	RI	USA	HIGH	B	B	C	401/273-0200	Y	
02657	Warwick/Providence	RI	USA	HIGH			C	401/751-8030	Y	
02657	Warwick/Providence	RI	USA	HIGH	B	B	C	401/273-0200	Y	
02665	San Diego	CA	USA	HIGH	B	B	C	619/296-8747	Y	
02666	Jackson	MI	USA	LOW	B	B	C	517/788-9191	Y	
02674	Tupelo	MS	USA	LOW	B	B	C	601/841-0090	Y	
02703	St. Laurent	QU	CAN	CANH	C	C	C	514/747-2996	Y	
02703	Montreal/St. Laurent	QU	CAN	CANH	C	C	C	514/747-2996	Y	
02704	San Francisco	CA	USA	WATS	B	B	C	800/###-####	Y	
02704	San Jose	CA	USA	WATS	B	B	C	800/###-####	Y	
02711	Kingsport	TN	USA	LOW	B	B	C	615/378-5746	Y	
02712	Houston	TX	USA	HIGH	B	B	C	713/496-1332	Y	
02720	La Crosse	WI	USA	LOW	B	B	C	608/784-9099	Y	
02723	Baton Rouge	LA	USA	MED	B	B		504/924-5102	N	
02737	Salt Lake City	UT	USA	HIGH	B	B		801/364-0780	N	
02743	Jackson	MS	USA	LOW	B	B	C	601/355-9741	Y	
02752	Stamford	CT	USA	HIGH			C	203/324-2297	Y	
02753	San Antonio	TX	USA	HIGH	B	B		512/225-8002	N	
02770	Tucson	AZ	USA	MED	B	B	C	602/297-2239	Y	
02771	Wheeling	WV	USA	LOW	B	B	C	304/233-7676	Y	
03001	Dallas	TX	USA	HIGH	B	B		214/638-8888	N	
03031	Aurora	IL	USA	LOW	B	B		708/844-0700	N	
03031	St. Charles/Aurora	IL	USA	LOW	B	B		708/844-0700	N	

03035	San Francisco	CA	USA	WATS	B	B	C		800/###-####	Y	
03611	Nashville	TN	USA	HIGH				C	615/889-4044	Y	
03611	Nashville	TN	USA	HIGH	B	B	C		615/889-5790	Y	
03614	Mankato	MN	USA	LOW	B	B	C		507/387-7313	Y	
03623	Erie	PA	USA	LOW	B	B	C		814/456-8501	Y	
03624	Raleigh	NC	USA	LOW	B	B	C		919/829-0536	Y	
03627	Belfast		GBR	E1				C	(232) 234467	Y	
03630	Idaho Falls	ID	USA	LOW	B	B	C		208/522-3624	Y	
03635	Lafayette	LA	USA	LOW	B	B	C		318/234-8255	Y	
03643	Harrisburg/Lemoyne	PA	USA	MED	B	B			717/763-6481	N	
03643	Lemoyne	PA	USA	MED	B	B			717/763-6481	N	
03650	Chicago	IL	USA	HIGH	B	B	C		312/922-6571	Y	
03651	Green Bay	WI	USA	LOW	B	B	C		414/432-3064	Y	
03652	Trenton	NJ	USA	LOW	B	B	C		609/394-1900	Y	
03653	Ft. Wayne	IN	USA	LOW	B	B	C		219/422-2581	Y	
03654	Southfield	MI	USA	MED	B	B	C		313/424-8024	Y	
03656	Evansville	IN	USA	LOW	B	B	C		812/464-8181	Y	
03661	Charleston	WV	USA	LOW	B	B	C		304/345-9575	Y	
03662	Allentown/Bethlehem	PA	USA	MED	B	B	C		215/865-6978	Y	
03662	Bethlehem	PA	USA	MED	B	B	C		215/865-6978	Y	
03663	Mesa/Phoenix	AZ	USA	HIGH				C	602/258-4528	Y	
03663	Phoenix	AZ	USA	HIGH				C	602/258-4528	Y	
03664	Phoenix	AZ	USA	HIGH				C	602/257-0629	N	TYM-X25
03664	Phoenix	AZ	USA	HIGH			C		602/257-0736	N	TYM-X25
03666	Lansing	MI	USA	MED	B	B			517/482-5721	N	
03673	Carson City	NV	USA	MED	B	B	C		702/885-8411	Y	
03673	Reno/Carson City	NV	USA	MED	B	B	C		702/885-8411	Y	
03675	Worcester	MA	USA	LOW	B	B	C		508/791-9000	Y	
03677	Joplin	MO	USA	LOW	B	B	C		417/781-8718	Y	
03704	Niagara Falls	NY	USA	LOW	B	B	C		716/285-2561	Y	
03705	Albany	NY	USA	MED	B	B			518/458-8300	N	
03705	Schenectady/Albany	NY	USA	MED	B	B			518/458-8300	N	
03706	San Francisco	CA	USA	HIGH	B	B			415/974-1300	N	
03707	Philadelphia	PA	USA	HIGH				C	215/629-0567	Y	
03712	Ottomwa	IA	USA	LOW	B	B	C		515/682-0857	Y	
03720	Winston-Salem	NC	USA	MED	B	B	C		919/765-1221	Y	
03725	Los Altos/San Jose	CA	USA	HIGH				C	408/432-0804	Y	
03725	San Jose	CA	USA	HIGH				C	408/432-0804	Y	
03725	Santa Clara/San Jose	CA	USA	HIGH				C	408/432-0804	Y	
03725	Sunnyvale/San Jose	CA	USA	HIGH				C	408/432-0804	Y	
03726	Billings	MT	USA	LOW	B	B	C		406/252-4880	Y	
03731	Shreveport	LA	USA	LOW	B	B	C		318/688-5840	Y	
03733	Brussels		BEL	E1		C	C		(2) 725-5060	Y	
03733	Brussels		BEL	E1				C	02-7255015	N	HSA
03737	Clearwater	FL	USA	MED				C	813/443-4515	Y	
03752	Rosemont	IL	USA	HIGH	B	B	C		708/698-9800	Y	
03774	Port Angeles	WA	USA	LOW	B	B	C		206/452-6800	Y	
03775	Newark	OH	USA	LOW	B	B	C		614/345-8953	Y	
04000	Longwood/Orlando	FL	USA	MED	B	B			407/841-0020	N	
04000	Orlando	FL	USA	MED	B	B			407/841-0020	N	
04003	Agana Heights		GUM	*		C	C		671/477-2222	N	
04003	Guatemala City		GTM	2		B			(2) 345-999	N	TYMUSA
04003	Guatemala City		GTM	2		B			(2) 345-599	N	TYMUSA
04003	All Cities		HND	2		B	B		320-544	N	TYMUSA
04003	Afula		ISR	3		B	B	C	(6) 596658	N	TYMUSA
04003	Ashdod		ISR	3		B	B	C	(8) 542999	N	TYMUSA
04003	Bezeq		ISR	3		B	B	C	(57) 36029	N	TYMUSA
04003	Eilat		ISR	3		B	B	C	(59) 75147	N	TYMUSA
04003	Hadera		ISR	3		B	B	C	(6) 332409	N	TYMUSA
04003	Haifa		ISR	3		B	B	C	(4) 525421	N	TYMUSA
04003	Haifa		ISR	3		B	B	C	(4) 673235	N	TYMUSA
04003	Haifa		ISR	3		B	B	C	(4) 674203	N	TYMUSA
04003	Haifa		ISR	3		B	B	C	(4) 674230	N	TYMUSA

04003	Herzeliya	ISR	3	B	B	C	(52)	545251	N	TYMUSA
04003	Jerusalem	ISR	3	B	B	C	(2)	242675	N	TYMUSA
04003	Jerusalem	ISR	3	B	B	C	(2)	246363	N	TYMUSA
04003	Jerusalem	ISR	3	B	B	C	(2)	248551	N	TYMUSA
04003	Jerusalem	ISR	3	B	B	C	(2)	814396	N	TYMUSA
04003	Nahariya	ISR	3	B	B	C	(4)	825393	N	TYMUSA
04003	Netanya	ISR	3	B	B	C	(53)	348588	N	TYMUSA
04003	Rehovot	ISR	3	B	B	C	(8)	469799	N	TYMUSA
04003	Tel Aviv	ISR	3	B	B	C	(3)	203435	N	TYMUSA
04003	Tel Aviv	ISR	3	B	B	C	(3)	546-3837	N	TYMUSA
04003	Tel Aviv	ISR	3	B	B	C	(3)	751-2504	N	TYMUSA
04003	Tel Aviv	ISR	3	B	B	C	(3)	751-3799	N	TYMUSA
04003	Tel Aviv	ISR	3	B	B	C	(3)	752-0110	N	TYMUSA
04003	Tiberias	ISR	3	B	B	C	(6)	790274	N	TYMUSA
04003	Tzfat	ISR	3	B	B	C	(6)	973282	N	TYMUSA
04003	All Cities	JAM	2	B	B		809/924-9915	N	TYMUSA	
04003	Curacao	NDA	3	C	C		(9)	239251	N	TYMUSA
04003	Curacao & St. Martin	NDA	3	C	C		0251	N	TYMUSA	
04003	All Cities	PAN	3			C	636-727	N	TYMUSA	
04003	All Cities	PAN	3	B	B		639-055	N	TYMUSA	
04003	Manila	PHL	2	B	B		(2)	815-1553	N	TYMUSA
04003	Manila	PHL	2	B	B		(2)	815-1555	N	TYMUSA
04003	Manila	PHL	2	B	B		(2)	817-1581	N	TYMUSA
04003	Manila	PHL	2	B	B		(2)	817-1791	N	TYMUSA
04003	Manila	PHL	2	B	B		(2)	817-1796	N	TYMUSA
04003	Manila	PHL	2	C			(2)	521-7901	N	TYMUSA
04003	Manila	PHL	2	C			(2)	817-8811	N	TYMUSA
04003	Manila	PHL	2	C			(2)	819-1009	N	TYMUSA
04003	Manila	PHL	2	C			(2)	819-1011	N	TYMUSA
04003	Manila	PHL	2	C			(2)	819-1550	N	TYMUSA
04003	Mayaguez/Ponce	PRI	*	B	B		809/462-4213	N		
04003	San Juan	PRI	*			C	809/724-6070	N		
04003	San Juan	PRI	*	B	B		809/725-1882	N		
04003	San Juan	PRI	*	B	B		809/725-4343	N		
04003	San Juan	PRI	*	C	C		809/725-3501	N		
04003	San Juan	PRI	*	C	C		809/725-4702	N		
04003	Alkobar	SAU	5			C	(3)	8981025	N	TYMUSA
04003	Jeddah	SAU	5			C	(2)	6691377	N	TYMUSA
04003	Jeddah	SAU	5			C	(2)	6690708	N	TYMUSA
04003	Riyadh	SAU	5			C	(1)	4631038	N	TYMUSA
04003	Riyadh	SAU	5			C	(1)	4658803	N	TYMUSA
04003	All Cities	TTO	2	C	C		809/627-0854	N	TYMUSA	
04003	All Cities	TTO	2	C	C		809/627-0855	N	TYMUSA	
04003	Aberdeen	GBR	1	C	C	C	(224)	210701	Y	TYMUSA
04003	Birmingham	GBR	1	C	C	C	(21)	633-3474	Y	TYMUSA
04003	Bristol	GBR	1	C	C	C	(272)	211545	Y	TYMUSA
04003	Cambridge	GBR	1	C	C	C	(223)	460127	Y	TYMUSA
04003	Cardiff	GBR	1	C	C	C	(222)	344184	Y	TYMUSA
04003	Chelmsford	GBR	1	C	C	C	(245)	491323	Y	TYMUSA
04003	Edinburgh	GBR	1	C	C	C	(31)	313-2137	Y	TYMUSA
04003	Exeter	GBR	1	C	C	C	(392)	421565	Y	TYMUSA
04003	Glasgow	GBR	1	C	C	C	(41)	204-1722	Y	TYMUSA
04003	Hastings	GBR	1	C	C	C	(424)	722788	Y	TYMUSA
04003	Ipswich	GBR	1	C	C	C	(473)	210212	Y	TYMUSA
04003	Kings Lynn	GBR	1	C	C	C	(553)	691090	Y	TYMUSA
04003	Leamington	GBR	1	C	C	C	(926)	451419	Y	TYMUSA
04003	Leeds	GBR	1	C	C	C	(532)	440024	Y	TYMUSA
04003	Liverpool	GBR	1	C	C	C	(51)	255-0230	Y	TYMUSA
04003	London (Clerkenwell)	GBR	1	C	C	C	(71)	490-2200	Y	TYMUSA
04003	Luton	GBR	1	C	C	C	(582)	481818	Y	TYMUSA
04003	Manchester	GBR	1	C	C	C	(61)	834-5533	Y	TYMUSA
04003	Newcastle	GBR	1	C	C	C	(91)	261-6858	Y	TYMUSA
04003	Nottingham	GBR	1	C	C	C	(???)	506005	Y	TYMUSA

04003	Oxford		GBR	1	C	C	C	(865)	798949	Y	TYMUSA
04003	Plymouth		GBR	1	C	C	C	(752)	603302	Y	TYMUSA
04003	Reading		GBR	1	C	C	C	(734)	500722	Y	TYMUSA
04003	Ayr		GBR	1	C	C	C	(292)	611822	Y	TYMUSA
04003	Belfast		GBR	1	C	C	C	(232)	331284	Y	TYMUSA
04003	Benbecula		GBR	1	C	C	C	(870)	2657	Y	TYMUSA
04003	Brechin		GBR	1	C	C	C	(356)	25782	Y	TYMUSA
04003	Brecon		GBR	1	C	C	C	(874)	3151	Y	TYMUSA
04003	Brighton		GBR	1	C	C	C	(273)	550046	Y	TYMUSA
04003	Campbeltown		GBR	1	C	C	C	(586)	52298	Y	TYMUSA
04003	Canterbury		GBR	1	C	C	C	(227)	762950	Y	TYMUSA
04003	Carlisle							612/333-2799		N	
04325	Hempstead	NY	USA	MED	B	B	C	516/485-7422		Y	
04325	Mineola/Hempstead	NY	USA	MED	B	B	C	516/485-7422		Y	
04327	Salem	OR	USA	LOW	B	B	C	503/370-4314		Y	
04330	Lubbock	TX	USA	LOW	B	B	C	806/797-0765		Y	
04340	Brownsville	TX	USA	LOW	B	B	C	512/548-1331		Y	
04343	Dallas	TX	USA	HIGH	B	B	C	214/630-5516		Y	
04353	Beverly Hills/Shr Ok	CA	USA	MED	B	B	C	818/789-9557		Y	
04353	Canoga Park/Shrm Oak	CA	USA	MED	B	B	C	818/789-9557		Y	
04353	San Fernando/Shr Oak	CA	USA	MED	B	B	C	818/789-9557		Y	
04353	Sherman Oaks	CA	USA	MED	B	B	C	818/789-9557		Y	
04353	Van Nuys/Sherman Oak	CA	USA	MED	B	B	C	818/789-9557		Y	
04353	West L.A./Shrmn Oaks	CA	USA	MED	B	B	C	818/789-9557		Y	
04355	Detroit	MI	USA	HIGH			C	313/965-4982		N	TYM-X25
04360	San Diego	CA	USA	HIGH	B	B		619/296-3370		N	
04372	Norristown	PA	USA	WATS	B	B	C	800/###-####		Y	
04375	Concord	NH	USA	LOW	B	B	C	603/228-4732		Y	
04376	Merced	CA	USA	LOW	B	B	C	209/383-7593		Y	
04403	Oklahoma City	OK	USA	HIGH	B	B	C	405/495-9201		Y	
04411	Belmont/Redwood City	CA	USA	HIGH	B	B	C	415/361-8701		Y	
04411	Palo Alto/Redwd City	CA	USA	HIGH	B	B	C	415/361-8701		Y	
04411	Redwood City	CA	USA	HIGH	B	B	C	415/361-8701		Y	
04430	Newark/Wilmington	DE	USA	MED	B	B		302/652-2060		N	
04430	Wilmington	DE	USA	MED	B	B		302/652-2060		N	
05177	Huntsville	AL	USA	MED	B	B	C	205/882-1519		Y	
05201	Greenville	SC	USA	MED	B	B	C	803/271-9213		Y	
05205	Eindhoven		NLD	E1	C	C	C	(4902)	45530	Y	
05206	White Plains	NY	USA	HIGH	B	B		914/328-7730		N	
05211	Eatontown/Red Bank	NJ	USA	LOW	B	B	C	908/758-0337		Y	
05211	Long Branch/Red Bank	NJ	USA	LOW	B	B	C	908/758-0337		Y	
05211	Red Bank	NJ	USA	LOW	B	B	C	908/758-0337		Y	
05215	Hibbing	MN	USA	LOW	B	B	C	218/262-3824		Y	
05221	Florence	AL	USA	LOW	B	B	C	205/760-0030		Y	
05241	Inglewood/Vernon	CA	USA	HIGH	B	B		213/587-0030		N	
05241	Los Angeles/Vernon	CA	USA	HIGH	B	B		213/587-0030		N	
05241	Vernon	CA	USA	HIGH	B	B		213/587-0030		N	
05242	Inglewood/Vernon	CA	USA	HIGH	B	B		213/587-0030		N	
05242	Los Angeles/Vernon	CA	USA	HIGH	B	B		213/587-0030		N	
05242	Vernon	CA	USA	HIGH	B	B		213/587-0030		N	
05250	Quincy	IL	USA	LOW	B	B	C	217/223-9531		Y	
05253	Clarkesville	TN	USA	LOW	B	B	C	615/645-8877		Y	
05256	Durham	NH	USA	LOW	B	B	C	603/868-1502		Y	
05260	Spokane	WA	USA	MED	B	B		509/624-1549		N	
05264	Rocky Mount	NC	USA	LOW	B	B	C	919/937-4828		Y	
05277	Philadelphia	PA	USA	HIGH	B	B	C	215/592-8750		Y	
05304	Fort Pierce	FL	USA	LOW	B	B	C	407/466-5661		Y	
05307	Peoria	IL	USA	LOW	B	B	C	309/637-5961		Y	
05325	Colton	CA	USA	MED	B	B	C	714/422-0222		Y	
05325	Riverside/Colton	CA	USA	MED	B	B	C	714/422-0222		Y	
05325	San Bernadino/Colton	CA	USA	MED	B	B	C	714/422-0222		Y	
05333	Bloomfield	CT	USA	HIGH			C	203/286-0712		N	TYM-X25
05333	Hartford/Bloomfield	CT	USA	HIGH			C	203/286-0712		N	TYM-X25

05341	Alameda/Oakland	CA	USA	HIGH	B	B	C	510/633-1896	Y	
05341	Berkeley/Oakland	CA	USA	HIGH	B	B	C	510/633-1896	Y	
05341	Hayward/Oakland	CA	USA	HIGH	B	B	C	510/633-1896	Y	
05341	Oakland	CA	USA	HIGH	B	B	C	510/633-1896	Y	
05350	Antioch	CA	USA	LOW	B	B	C	510/754-8222	Y	
05363	Brussels		BEL	E1				206/221-0450	N	DCS GATEWAY
05365	Wausau	WI	USA	LOW	B	B	C	715/848-6171	Y	
05366	Pontiac	MI	USA	LOW	B	B	C	313/338-8384	Y	
05402	Dallas	TX	USA	HIGH			C	214/634-0833	N	TYM-X25
05402	Dallas	TX	USA	HIGH			C	214/634-0834	N	TYM-X25
05402	Dallas	TX	USA	HIGH			C	214/634-0834	N	TYM-X25
05410	Minneapolis	MN	USA	HIGH			C	612/332-2580	N	TYM-X25
05410	St. Paul/Minneapolis	MN	USA	HIGH			C	612/332-2580	N	TYM-X25
05410	Minneapolis	MN	USA	HIGH			C	612/332-2680	N	TYM-X25
05410	St. Paul/Minneapolis	MN	USA	HIGH			C	612/332-2680	N	TYM-X25
05415	Wichita Falls	TX	USA	LOW	B	B	C	817/723-2386	Y	
05417	Marseille		FRA	E1	C	C	C	(91) 259933	Y	
05431	Opelika	AL	USA	LOW	B	B	C	205/742-9040	Y	
06515	Charlotte	NC	USA	HIGH			C	704/329-0104	Y	
06522	Pawtucket/Providence	RI	USA	HIGH	B	B	C	401/273-0200	Y	
06522	Providence	RI	USA	HIGH	B	B	C	401/273-0200	Y	
06522	Warwick/Providence	RI	USA	HIGH	B	B	C	401/273-0200	Y	
06525	New Orleans	LA	USA	HIGH	B	B	C	504/525-2014	Y	
06532	New Orleans	LA	USA	HIGH	B	B		504/522-1370	N	
06544	Piscataway	NJ	USA	HIGH	B	B	C	908/562-8550	Y	
06560	Rostock		FRG	E1	C	C	C	(81) 36622404	Y	
06562	Dublin		IRL	E2	C	C	C	(1) 67 98 924	Y	
06564	Everett	WA	USA	LOW	B	B	C	206/258-1018	Y	
06567	Vicksburg	MS	USA	LOW	B	B	C	601/638-1551	Y	
06570	Pittsburgh	PA	USA	HIGH			C	412/642-2271	N	
06574	Miami	FL	USA	HIGH	B	B	C	305/599-2900	Y	
06577	Boston	MA	USA	HIGH	B	B	C	617/439-3531	Y	
06577	Cambridge/Boston	MA	USA	HIGH	B	B	C	617/439-3531	Y	
06605	San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
06605	Santa Clara/San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
06605	Sunnyvale/San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
06614	Akron	OH	USA	MED	B	B	C	216/376-8330	Y	
06626	Lexington	KY	USA	MED	B	B		606/266-0019	N	
06641	Kingston	MA	USA	LOW	B	B	C	617/582-1200	Y	
06651	Aurora/Denver	CO	USA	HIGH			C	303/830-8530	Y	
06651	Boulder/Denver	CO	USA	HIGH			C	303/830-8530	Y	
06651	Denver	CO	USA	HIGH			C	303/830-8530	Y	
06667	Reading/Mt. Penn	PA	USA	MED	B	B	C	215/796-9000	Y	
06667	Mt. Penn	PA	USA	LOW	B	B	C	215/796-9000	Y	
06670	Barcelona		ESP	E2	C	C	C	(3) 4155082	Y	
06673	Aberdeen	MD	USA	LOW	B	B	C	410/273-0872	Y	
06674	Houston	TX	USA	HIGH	B	B		713/556-6700	N	
06675	State College	PA	USA	LOW	B	B	C	814/234-3853	Y	
06704	Houston	TX	USA	HIGH	B	B		713/556-6700	N	
06715	Midlothian/Richmond	VA	USA	MED	B	B		804/330-2465	N	
06715	Richmond	VA	USA	MED	B	B		804/330-2465	N	
06733	Los Angeles/Vernon	CA	USA	HIGH			C	213/588-4712	N	TYM-X25
06733	Inglewood/Vernon	CA	USA	HIGH			C	213/588-4712	N	TYM-X25
06733	Vernon	CA	USA	HIGH			C	213/588-4712	N	TYM-X25
06733	Los Angeles/Vernon	CA	USA	HIGH			C	213/588-4639	N	TYM-X25
06733	Inglewood/Vernon	CA	USA	HIGH			C	213/588-4639	N	TYM-X25
06733	Vernon	CA	USA	HIGH			C	213/588-4639	N	TYM-X25
06754	Kitchener	ON	CAN	CANL	C	C	C	519/742-7613	Y	
06755	Coatesville	PA	USA	LOW	B	B	C	215/383-0440	Y	
06755	Downington/Coatsvllle	PA	USA	LOW	B	B	C	215/383-0440	Y	
06762	Marquette	MI	USA	LOW	B	B	C	906/228-3780	Y	
06771	Ft. Smith	AR	USA	LOW	B	B	C	501/782-2486	Y	
06774	Topeka	KS	USA	LOW	B	B	C	913/234-3070	Y	

07001	Boston	MA	USA	HIGH	B	B		617/439-3400	N	
07001	Cambridge/Boston	MA	USA	HIGH	B	B		617/439-3400	N	
07005	Detroit	MI	USA	HIGH			C	313/964-1225	Y	
07024	Longview	TX	USA	LOW	B	B	C	903/236-7475	Y	
07025	Madison	WI	USA	LOW	B	B	C	608/242-0227	Y	
07026	Madison	WI	USA	LOW	B	B	C	608/242-0227	Y	
07031	Albany	GA	USA	LOW	B	B	C	912/888-9282	Y	
07042	Nashua	NH	USA	MED	B	B	C	603/882-0435	Y	
07042	Salem/Nashua	NH	USA	MED	B	B	C	603/882-0435	Y	
07043	Sarasota	FL	USA	LOW	B	B	C	813/952-9000	Y	
07057	New York	NY	USA	HIGH			C	212/797-2792	N	TYM-X25
07057	New York	NY	USA	HIGH			C	212/797-2790	N	TYM-X25
07075	Cincinnati	OH	USA	HIGH	B	B		513/530-9019	N	
07100	Los Altos/San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
07100	San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
07100	Santa Clara/San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
07100	Sunnyvale/San Jose	CA	USA	HIGH	B	B	C	408/432-8618	Y	
07102	Hutchinson	KS	USA	LOW	B	B	C	316/663-2192	Y	
07107	Barre/Montpelier	VT	USA	LOW	B	B		802/229-4508	N	
07107	Montpelier	VT	USA	LOW	B	B		802/229-4508	N	
7117	Fremont	CA	USA	MED	B	B	C	510/490-7366	Y	
07126	Rolla	MO	USA	LOW	B	B	C	314/364-2084	Y	
07140	Cincinnati	OH	USA	HIGH			C	513/489-1032	Y	
07143	Portland	OR	USA	HIGH			C	503/225-1918	Y	
07144	Portland	OR	USA	HIGH	B	B	C	503/222/2151	Y	
07145	Portland	OR	USA	HIGH			C	503/225-1918	Y	
07145	Portland	OR	USA	HIGH	B	B	C	503/222-2151	Y	
07147	Portland	OR	USA	HIGH	B	B		503/222-0900	N	
07150	Boca Raton/Delray	FL	USA	LOW	B	B	C	407/272-7900	Y	
07150	Delray	FL	USA	LOW	B	B	C	407/272-7900	Y	
07157	Rosewell	NM	USA	LOW	B	B	C	505/623-3591	Y	
07162	Perinton/Pittsford	NY	USA	HIGH			C	716/586-4100	Y	
07162	Perinton/Pittsford	NY	USA	HIGH			C	716/586-4858	N	TYM-X25
07162	Rochester/Pittsford	NY	USA	HIGH			C	716/586-4100	Y	
07162	Pittsford	NY	USA	HIGH			C	716/586-4100	Y	
07162	Pittsford	NY	USA	HIGH			C	716/586-4858	N	TYM-X25
07162	Rochester/Pittsford	NY	USA	HIGH			C	716/586-4858	N	TYM-X25
07162	Perinton/Pittsford	NY	USA	HIGH			C	716/586-4829	N	TYM-X25
07162	Pittsford	NY	USA	HIGH			C	716/586-4829	N	TYM-X25
07162	Rochester/Pittsford	NY	USA	HIGH			C	716/586-4829	N	TYM-X25
07175	Myrtle Beach	SC	USA	LOW	B	B	C	803/448-1619	Y	
07177	Copenhagen	DNK	E2		C	C	C	31-18-63-33	Y	
07205	Los Altos/San Jose	CA	USA	HIGH	B	B		408/432-3430	N	
07205	San Jose	CA	USA	HIGH	B	B		408/432-3430	N	
07205	Santa Clara/San Jose	CA	USA	HIGH	B	B		408/432-3430	N	
07205	Sunnyvale/San Jose	CA	USA	HIGH	B	B		408/432-3430	N	
07210	Fall River/Somerset	MA	USA	LOW	B	B	C	508/676-3087	Y	
07210	Somerset	MA	USA	LOW	B	B	C	508/676-3087	Y	
07214	Middletown	RI	USA	LOW	B	B	C	401/849-1660	Y	
07214	Newport/Middletown	RI	USA	LOW	B	B	C	401/849-1660	Y	
07220	Bridgeport	CT	USA	MED	B	B		203/579-1479	N	
07220	Stratford/Bridgeprt	CT	USA	MED	B	B		203/579-1479	N	
07221	Atlantic City	NJ	USA	LOW	B	B	C	609/345-4050	Y	
07223	Dayton	OH	USA	MED	B	B	C	513/898-0696	Y	
07226	Ogden	UT	USA	LOW	B	B	C	801/393-5280	Y	
07227	Mexico C(Xochimilco)	MEX	MX		B	B	B	(5) 6754911	N	
07227	Mexico C(Xochimilco)	MEX	MX		B	B	B	(5) 6754072	N	
07227	Mexico C(Xochimilco)	MEX	MX		B	B	B	(5) 6754635	N	
07227	Mexico C(Xochimilco)	MEX	MX		B	B	B	(5) 6753173	N	
07227	Mexico C(Xochimilco)	MEX	MX		B	B	B	(5) 6753372	N	
07227	Mexico C(Xochimilco)	MEX	MX		B	B	B	(5) 6753629	N	
07236	White Plains	NY	USA	HIGH	B	B	C	914/761-9590	Y	
07240	White Plains	NY	USA	HIGH			C	914/761-5377	Y	

07241	Greenville	NC	USA	LOW	B	B	C		919/758-0102	Y	
07242	High Point	NC	USA	LOW	B	B	C		919/883-6121	Y	
07246	San Francisco	CA	USA	HIGH				C	415/896-5578	N	TYM-X25
07247	San Antonio	TX	USA	HIGH	B	B	C		512/222-9877	Y	
07250	Curacao		NDA	3	C	C			(9)239251	N	TYMUSA
07250	Curacao		NDA	3	C	C			0251 (LOCAL)		TYMUSA
07270	Gibraltar		GIB	E2	C	C	C		(350) 41000	Y	
07272	Greenville	SC	USA	MED				C	803/370-9014	Y	
07301	Rome	GA	USA	LOW	B	B	C		404/234-0102	Y	
07302	San Francisco	CA	USA	HIGH	B	B	C		415/543-0691	Y	
07303	Danville	IL	USA	LOW	B	B	C		217/442-1452	Y	
07306	Davenport/RockIsland	IA	USA	MED	B	B	C		309/788-3713	Y	
07306	Rock Island	IL	USA	MED	B	B	C		309/788-3713	Y	
07313	Melbourne		AUS	PAC	C	C	C		(3)416-2146	Y	
07320	San Francisco	CA	USA	HIGH	B	B	C		415/543-0691	Y	
07322	Greeley	CO	USA	LOW	B	B	C		303/352-0960	Y	
07331	Levittown	PA	USA	LOW	B	B			215/943-3700	N	
07332	Pittsfield	MA	USA	LOW	B	B	C		413/499-0971	Y	
07336	Ardmore	OK	USA	LOW	B	B	C		405/226-1260	Y	
07340	Grand Forks	ND	USA	LOW	B	B	C		701/746-0344	Y	
07344	Lynn	MA	USA	LOW	B	B	C		617/592-0207	Y	
07346	San Francisco	CA	USA	HIGH	B	B	C		415/543-0691	Y	
07364	Corning	NY	USA	LOW	B	B	C		607/962-4481	Y	
07370	Spartanburg	SC	USA	LOW	B	B	C		803/579-7088	Y	
07375	Hanover	NH	USA	LOW	B	B	C		603/643-4011	Y	
07404	Long Beach	CA	USA	MED	B	B	C		310/436-6033	Y	
07404	Norwalk/Long Beach	CA	USA	MED	B	B	C		310/436-6033	Y	
07404	San Pedro/Long Beach	CA	USA	MED	B	B	C		310/436-6033	Y	
07406	Akita		JPN	PAC		C	C		0188-65-5733	N	
07406	Akita		JPN	PAC		C			0188-65-5735	N	
07406	Atsugi		JPN	PAC		C	C		0462-21-0404	N	
07406	Atsugi		JPN	PAC		C			0462-21-5331	N	
07406	Atsugi		JPN	PAC		C	C	C	0462-22-7154	Y	
07406	Chiba		JPN	PAC		C	C		0472-96-3581	N	
07406	Chiba		JPN	PAC		C	C	C	0472-96-0279	Y	
07406	Fukui		JPN	PAC		C	C		0776-35-8840	N	
07406	Fukui		JPN	PAC		C			0776-34-3308	N	
07406	Fukuoka		JPN	PAC		C	C		092-474-7196	N	
07406	Fukuoka		JPN	PAC		C			092-474-7076	N	
07406	Fukuoka		JPN	PAC		C	C	C	092-461-2769	Y	
07406	Hamamatsu		JPN	PAC		C			0534-56-7355	N	
07406	Hamamatsu		JPN	PAC		C	C		0534-56-7231	N	
07406	Hiroshima		JPN	PAC		C	C		082-243-9270	N	
07406	Hiroshima		JPN	PAC		C	C	C	082-241-6857	Y	
07406	Kagoshima		JPN	PAC		C	C		0992-22-8954	N	
07406	Kanazawa		JPN	PAC		C	C		0762-24-2341	N	
07406	Kanazawa		JPN	PAC		C	C	C	0762-24-7792	Y	
07406	Kobe		JPN	PAC		C	C		078-333-0552	N	
07406	Kobe		JPN	PAC		C			078-333-0587	N	
07406	Kouriyama		JPN	PAC		C	C		0249-38-5396	N	
07406	Kumamoto		JPN	PAC		C	C		096-354-3065	N	
07406	Kumamoto		JPN	PAC		C			096-355-5233	N	
07406	Kyoto		JPN	PAC		C	C		075-431-6203	N	
07406	Kyoto		JPN	PAC		C			075-431-6205	N	
07406	Matsuyama		JPN	PAC		C	C		0899-32-4207	N	
07406	Matsuyama		JPN	PAC		C			0899-32-2975	N	
07406	Matsuyama		JPN	PAC		C	C	C	0899-32-2865	Y	
07406	Mito		JPN	PAC		C	C		0292-24-4213	N	
07406	Morioka		JPN	PAC		C	C		0196-54-7315	N	
07406	Morioka		JPN	PAC		C	C	C	0196-22-3885	Y	
07406	Nagasaki		JPN	PAC		C	C		0958-28-6077	N	
07406	Nagoya		JPN	PAC		C	C		052-981-3221	N	
07406	Nagoya		JPN	PAC		C			052-911-1621	N	

07406	Nagoya	JPN	PAC	C	C	C	052-991-4521	Y	
07406	Naha	JPN	PAC		C	C	0988-61-3414	N	
07406	Naha	JPN	PAC	C			0988-61-4002	N	
07406	Niigata	JPN	PAC		C	C	025-241-5410	N	
07406	Niigata	JPN	PAC	C	C	C	025-241-5409	Y	
07406	Ohita	JPN	PAC		C	C	0975-38-2160	N	
07406	Okayama	JPN	PAC		C	C	0862-31-4993	N	
07406	Okayama	JPN	PAC	C			0862-32-6760	N	
07406	Osaka	JPN	PAC		C		06-271-9029	N	
07406	Osaka	JPN	PAC		C	C	06-271-6876	N	
07406	Osaka	JPN	PAC	C			06-271-9028	N	
07406	Osaka	JPN	PAC	C	C	C	06-264-9951	Y	
07406	Sapporo	JPN	PAC		C	C	011-281-4421	N	
07406	Sapporo	JPN	PAC	C			011-281-4343	N	
07406	Sapporo	JPN	PAC	C	C	C	011-210-5962	Y	
07406	Sendai	JPN	PAC		C	C	022-231-5355	N	
07406	Sendai	JPN	PAC	C	C	C	022-231-5741	Y	
07406	Shizuoka	JPN	PAC		C	C	0542-84-3398	N	
07406	Shizuoka	JPN	PAC	C	C	C	0542-84-3393	Y	
07406	Takamatsu	JPN	PAC		C	C	0878-23-0501	N	
07406	Takamatsu	JPN	PAC	C			0878-23-0502	N	
07406	Takasaki	JPN	PAC		C	C	0273-23-9739	N	
07406	Tokuyama	JPN	PAC		C	C	0834-32-0991	N	
07406	Tokyo	JPN	PAC		C		03-3555-9526	N	
07406	Tokyo	JPN	PAC		C	C	03-3555-9696	N	N
07406	Tokyo	JPN	PAC	C			03-3555-9525	N	
07406	Tokyo	JPN	PAC	C	C	C	03-3288-6461	Y	
07406	Toyama	JPN	PAC		C	C	0764-41-7769	N	
07406	Toyama	JPN	PAC	C			0764-41-7578	N	
07406	Tsuchiura	JPN	PAC		C	C	0298-55-6121	N	
07406	Urawa	JPN	PAC		C	C	048-833-9341	N	
07406	Utsunomiya	JPN	PAC		C	C	0286-34-8251	N	
07406	Utsunomiya	JPN	PAC	C	C	C	0286-37-4378	Y	
07406	Yokohama	JPN	PAC		C	C	045-453-7637	N	
07406	Yokohama	JPN	PAC	C			045-453-7757	N	
07406	Yokohama	JPN	PAC	C	C	C	045-453-7758	Y	
07406	Yonago	JPN	PAC		C	C	0859-32-3201	N	
07406	Nagasaki	JPN	PAC	C			0958-28-6088	N	
07406	Nagano	JPN	PAC		C	C	0262-34-3900	N	
07406	Tokyo	JAP	PAC			C	03-3262-7517	N	TYM-X25
07406	Tokyo	JAP	PAC			C	03-5275-3829	Y	NEW NUMBER
07407	Buenos Aires	ARG	2		C		(1) 40-01-91	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-92	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-93	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-94	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-95	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-96	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-97	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-98	N	TYMUSA
07407	Buenos Aires	ARG	2		C		(1) 40-01-99	N	TYMUSA
07414	Warren	OH	USA	LOW	B	B	C	216/392-2555	Y
07417	San Francisco	CA	USA	HIGH				C	415/495-7220
07432	Lyndhurst/Union City	NJ	USA	HIGH	B	B	C		201/864-8468
07432	Union City	NJ	USA	HIGH	B	B	C		201/864-8468
07434	Davis	CA	USA	LOW	B	B	C		916/758-3551
07434	Woodland/Davis	CA	USA	LOW	B	B	C		916/758-3551
07437	Austin	TX	USA	HIGH	B	B	C		512/448-1096
07447	Butte	MT	USA	LOW	B	B	C		406/494-6682
07450	Dallas	TX	USA	HIGH				C	214/637-3012
07454	Terre Haute	IN	USA	LOW	B	B	C		812/232-0112
07455	Lafayette	IN	USA	LOW	B	B	C		317/423-4616
07456	Dubuque	IA	USA	LOW	B	B	C		319/582-3599
07457	Minot	ND	USA	LOW	B	B	C		701/838-2140

07460	Beloit	WI	USA	LOW	B	B	C	608/362-4655	Y	
07460	Janesville/Beloit	WI	USA	LOW	B	B	C	608/362-4655	Y	
07463	Hot Springs	AR	USA	LOW	B	B	C	501/623-3576	Y	
07464	Jonesboro	AR	USA	LOW	B	B	C	501/935-7957	Y	
07465	Cadillac	MI	USA	LOW	B	B	C	616/775-9242	Y	
07466	Muskegon	MI	USA	LOW	B	B	C	616/739-3453	Y	
07467	Port Huron	MI	USA	LOW	B	B	C	313/982-0301	Y	
07472	Mansfield	OH	USA	LOW	B	B	C	419/529-3303	Y	
07520	Atlanta/Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	
07520	Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	
07520	Marietta/Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	
07520	Norcross/Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	
07522	San Angelo	TX	USA	LOW	B	B	C	915/658-4590	Y	
07524	San Antonio	TX	USA	HIGH	B	B	C	512/222-9877	Y	
07525	Boston	MA	USA	HIGH	B	B		617/439-3400	N	
07525	Cambridge/Boston	MA	USA	HIGH	B	B		617/439-3400	N	
07533	Inglewood/Vernon	CA	USA	HIGH			C	213/588-8128	Y	
07533	Los Angeles/Vernon	CA	USA	HIGH			C	213/588-8128	Y	
07533	Vernon	CA	USA	HIGH			C	213/588-8128	Y	
07540	Calgary	AB	CAN	CANH	C	C	C	403/232-6653	Y	
07542	Sacramento	CA	USA	HIGH			C	916/442-0992	N	
07543	Sacramento	CA	USA	HIGH			C	916/442-0851	N	TYM-X25
07547	Taunton	MA	USA	LOW	B	B	C	508/824-3816	Y	
07571	Salisbury	MD	USA	LOW	B	B	C	410/860-0480	Y	
07600	Bowling Green	KY	USA	LOW	B	B	C	502/781-5711	Y	
07602	All Cities		ATG	3	B	B		809/462-0210	N	TYMUSA
07603	All Cities		ATG	3	B	B		809/462-0210	N	TYMUSA
07607	Gastonia	NC	USA	LOW	B	B	C	704/867-2203	Y	
07617	Corpus Christi	TX	USA	MED	B	B	C	512/289-7305	Y	
07622	Manassas	VA	USA	LOW	B	B	C	703/330-9070	Y	
07625	Lowell	MA	USA	LOW	B	B	C	508/452-5112	Y	
07631	Auburn	WA	USA	LOW	B	B	C	206/735-3975	Y	
07631	Enumclaw/Auburn	WA	USA	LOW	B	B	C	206/735-3975	Y	
07636	Santa Fe	NM	USA	LOW	B	B	C	505/471-0606	Y	
07646	Monroe	LA	USA	LOW	B	B	C	318/388-8810	Y	
07650	Kokomo	IN	USA	LOW	B	B	C	317/453-7818	Y	
07651	Appleton	WI	USA	LOW	B	B	C	414/730-8029	Y	
07652	Corona	CA	USA	LOW	B	B	C	714/737-5510	Y	
07653	Poway	CA	USA	LOW	B	B	C	619/679-0200	Y	
07655	Norristown	PA	USA	WATS	B	B	C	800/###-####	Y	
07656	Norristown	PA	USA	WATS	B	B	C	800/###-####	Y	
07663	Birmingham		GBR	E1	C	C	C	(21) 632-6636	Y	
07675	Dundas	ON	CAN	CANH	C	C	C	416/628-5908	Y	
07676	Newport News	VA	USA	MED	B	B	C	804/596-0898	Y	
07677	Fitchburg/Leominster	MA	USA	LOW	B	B	C	508/537-6451	Y	
07677	Leominster	MA	USA	LOW	B	B	C	508/537-6451	Y	
07703	Inglewood/Vernon	CA	USA	HIGH	B	B	C	213/587-7514	Y	
07703	Los Angeles/Vernon	CA	USA	HIGH	B	B	C	213/587-7514	Y	
07703	Vernon	CA	USA	HIGH	B	B	C	213/587-7514	Y	
07712	Vero Beach	FL	USA	LOW	B	B	C	407/569-8207	Y	
07714	Meridian	MS	USA	LOW	B	B	C	601/482-4335	Y	
07717	Baytown	TX	USA	LOW	B	B	C	713/420-3389	Y	
07720	Miami	FL	USA	HIGH			C	305/599-9996	N	TYM-X25
07720	Miami	FL	USA	HIGH			C	305/599-9997	N	TYM-X25
07721	Freeport	IL	USA	LOW	B	B	C	815/232-7111	Y	
07723	Dothan	AL	USA	LOW	B	B	C	205/794-7954	Y	
07724	Miami	FL	USA	HIGH			C	305/592-2357	Y	
07725	Panama City	FL	USA	LOW	B	B	C	904/769-0709	Y	
07726	Leavenworth	KS	USA	LOW	B	B	C	913/651-8094	Y	
07730	Salina	KS	USA	LOW	B	B	C	913/825-4845	Y	
07731	Cicero/Maywood	IL	USA	LOW	B	B	C	708/345-9100	Y	
07731	Forest Park/Maywood	IL	USA	LOW	B	B	C	708/345-9100	Y	
07731	Maywood	IL	USA	LOW	B	B	C	708/345-9100	Y	

07733	Marion	IN	USA	LOW	B	B	C	317/662-1928	Y	
07735	Attleboro	MA	USA	LOW	B	B		508/226-6441	N	
07737	Lynchburg	VA	USA	LOW	B	B	C	804/846-0213	Y	
07743	Holyoke/Springfield	MA	USA	MED	B	B	C	413/787-0048	Y	
07743	Springfield	MA	USA	MED	B	B	C	413/787-0048	Y	
10021	Houston	TX	USA	HIGH	B	B	C	713/496-1332	Y	
10021	Houston	TX	USA	HIGH				C	713/589-7593	N TYM-X25
10021	Houston	TX	USA	HIGH				C	713/589-7591	N TYM-X25
10027	Kannapolis	NC	USA	LOW	B	B	C	704/932-4131	Y	
10031	Bedford	MA	USA	LOW	B	B	C	617/271-0420	Y	
10031	Woburn/Bedford	MA	USA	LOW	B	B	C	617/271-0420	Y	
10033	Bend	OR	USA	LOW	B	B	C	503/389-0146	Y	
10034	Baltimore	MD	USA	HIGH				C	410/659-7460	Y
10040	Columbus	OH	USA	HIGH				C	614/224-0436	N TYM-X25
10040	Columbus	OH	USA	HIGH			C	614/224-0427	N TYM-X25	
10052	Napa	CA	USA	LOW	B	B	C	707/257-6810	Y	
10061	Buffalo	NY	USA	MED	B	B		716/893-1306	N	
10066	Williamsport	PA	USA	LOW	B	B	C	717/321-8520	Y	
10070	New York	NY	USA	HIGH				C	212/269-4640	Y
10071	York	PA	USA	LOW	B	B	C	717/852-8186	Y	
10075	Blountville	TN	USA	LOW	B	B	C	615/323-1962	Y	
10100	Corvallis	OR	USA	LOW	B	B	C	503/757-6341	Y	
10103	Ann Arbor	MI	USA	MED				C	313/973-0166	Y
10105	Camden/Pennsauken	NJ	USA	MED	B	B	C	609/665-5902	Y	
10105	Cherry hill/Pennskn	NJ	USA	MED	B	B	C	609/665-5902	Y	
10105	Pennsauken	NJ	USA	MED	B	B	C	609/665-5902	Y	
10110	Newark	NJ	USA	HIGH				C	201/824-4130	N TYM-X25
10110	Elizabeth/Newark	NJ	USA	HIGH				C	201/824-4130	N TYM-X25
10110	Jersey City/Newark	NJ	USA	HIGH				C	201/824-4130	N TYM-X25
10110	Union/Newark	NJ	USA	HIGH				C	201/824-4130	N TYM-X25
10110	Elizabeth/Newark	NJ	USA	HIGH			C	201/824-4128	N TYM-X25	
10110	Jersey City/Newark	NJ	USA	HIGH			C	201/824-4128	N TYM-X25	
10110	Newark	NJ	USA	HIGH			C	201/824-4128	N TYM-X25	
10110	Union/Newark	NJ	USA	HIGH			C	201/824-4128	N TYM-X25	
10113	Fairfield/Westport	CT	USA	MED	B	B	C	203/454-2129	Y	
10113	Norwalk/Westport	CT	USA	MED	B	B	C	203/454-2129	Y	
10113	Westport	CT	USA	MED	B	B	C	203/454-2129	Y	
10122	Hull/Ottawa	ON	CAN	CANH	C	C	C	613/563-2910	N	
10122	Ottawa	ON	CAN	CANH	C	C	C	613/563-2910	N	
10124	Cologne		FRG	E1	C	C	C	(221)210196	N	
10130	Sacramento	CA	USA	HIGH	B	B	C	916/447-7434	Y	
10151	Portland	OR	USA	HIGH				C	503/225-1233	N TYM-X25
10153	South Brunswick	NJ	USA	HIGH				C	609/452-8011	N TYM-X25
10153	South Brunswick	NJ	USA	HIGH				C	609/452-8388	Y
10153	Princeton/So. Brnswk	NJ	USA	HIGH				C	609/452-8011	N TYM-X25
10153	Princeton/So. Brnswk	NJ	USA	HIGH				C	609/452-8388	Y
10170	Johnstown	PA	USA	LOW	B	B	C	814/539-5059	Y	
10171	Jamestown	NY	USA	LOW	B	B		716/488-0794	N	
10172	Somers	CT	USA	LOW	B	B	C	203/763-3521	Y	
10204	Austin	TX	USA	HIGH	B	B	C	512/448-1096	Y	
10211	Atlanta/Doraville	GA	USA	HIGH				C	404/455-9285	N TYM-X25
10211	Marietta/Doraville	GA	USA	HIGH				C	404/455-9285	N TYM-X25
10211	Norcross/Doraville	GA	USA	HIGH				C	404/455-9285	N TYM-X25
10211	Doraville	GA	USA	HIGH				C	404/455-9285	N TYM-X25
10211	Atlanta/Doraville	GA	USA	HIGH			C	404/455-7540	N TYM-X25	
10211	Doraville	GA	USA	HIGH			C	404/455-7540	N TYM-X25	
10211	Marietta/Doraville	GA	USA	HIGH			C	404/455-7540	N TYM-X25	
10211	Norcross/Doraville	GA	USA	HIGH			C	404/455-7540	N TYM-X25	
10212	Hamilton	OH	USA	LOW	B	B		513/874-1744	N	
10213	Ocala	FL	USA	LOW	B	B	C	904/732-3707	Y	
10217	Atlanta/Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	
10217	Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	
10217	Marietta/Doraville	GA	USA	HIGH	B	B	C	404/451-3362	Y	

10217	Norcross/Doraville	GA	USA	HIGH	B	B	C		404/451-3362	Y	
10233	Cleveland	OH	USA	HIGH	B	B	C		216/861-6709	Y	
10234	Cleveland	OH	USA	HIGH			C	C	216/696-0363	N	TYM-X25
10242	San Jose	CA	USA	HIGH				C	408/954-8481	N	TYM-X25
10242	Los Altos/San Jose	CA	USA	HIGH				C	408/954-8481	N	TYM-X25
10242	Santa Clara/San Jose	CA	USA	HIGH				C	408/954-8481	N	TYM-X25
10242	Sunnyvale/San Jose	CA	USA	HIGH				C	408/954-8481	N	TYM-X25
10242	San Jose	CA	USA	HIGH			C		408/954-8476	N	TYM-X25
10242	Los Altos/San Jose	CA	USA	HIGH			C		408/954-8476	N	TYM-X25
10242	Santa Clara/San Jose	CA	USA	HIGH			C		408/954-8476	N	TYM-X25
10242	Sunnyvale/San Jose	CA	USA	HIGH			C		408/954-8476	N	TYM-X25
10243	Huntington	WV	USA	LOW	B	B	C		304/529-2091	Y	
10250	Inglewood/Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10250	Los Angeles/Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10250	Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10254	Atlanta/Doraville	GA	USA	HIGH				C	404/451-1546	Y	
10254	Doraville	GA	USA	HIGH				C	404/451-1546	Y	
10254	Marietta/Doraville	GA	USA	HIGH				C	404/451-1546	Y	
10254	Norcross/Doraville	GA	USA	HIGH				C	404/451-1546	Y	
10255	Laredo	TX	USA	LOW	B	B	C		512/727-8308	Y	
10256	Hampton	VA	USA	MED	B	B	C		804/727-0572	Y	
10261	Sheboygan	WI	USA	LOW	B	B	C		414/457-6128	Y	
10264	Pittsburgh	PA	USA	HIGH				C	412/642-7703	N	TYM-X25
10264	Pittsburgh	PA	USA	HIGH			C		412/642-2386	N	TYM-X25
10267	Springfield	MA	USA	MED	B	B	C		413/787-0048	Y	
10267	Holyoke/Springfield	MA	USA	MED	B	B	C		413/787-0048	Y	
10274	Tucson	AZ	USA	MED	B	B	C		602/297-2239	Y	
10301	Abilene	TX	USA	LOW	B	B	C		915/676-0091	Y	
10305	Gadsden	AL	USA	LOW	B	B	C		205/543-3550	Y	
10307	Ann Arbor	MI	USA	MED	B	B	C		313/973-7935	Y	
10317	Kenosha	WI	USA	LOW	B	B	C		414/553-9044	Y	
10317	Racine/Kenosha	WI	USA	LOW	B	B	C		414/553-9044	Y	
10320	Iowa City	IA	USA	LOW	B	B	C		319/354-3633	Y	
10325	Inglewood/Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10325	Los Angeles/Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10325	Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10334	Monterey	CA	USA	LOW	B	B	C		408/375-2644	Y	
10337	Louisville	KY	USA	MED	B	B			502/499-7110	N	
10346	Portsmouth/Norfolk	VA	USA	MED	B	B	C		804/857-0148	Y	
10346	Virginia Bch/Norfolk	VA	USA	MED	B	B	C		804/857-0148	Y	
10346	Norfolk	VA	USA	MED	B	B	C		804/857-0148	Y	
10355	Longwood/Orlando	FL	USA	MED				C	407/839-0555	Y	
10355	Orlando	FL	USA	MED				C	407/839-0555	Y	
10361	Alexandria/Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
10361	Arlington/Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
10361	Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
10361	Washington/Fairfax	DC	USA	HIGH	B	B	C		703/352-3136	Y	
10361	Bethesda/Fairfax	MD	USA	HIGH	B	B	C		703/352-3136	Y	
10363	El Segundo	CA	USA	MED	B	B	C		310/643-4228	Y	
10363	Mar Vista/El Segundo	CA	USA	MED	B	B	C		310/643-4228	Y	
10363	MarinaDelRey/El Sgnd	CA	USA	MED	B	B	C		310/643-4228	Y	
10363	Santa Monica/El Sgnd	CA	USA	MED	B	B	C		310/643-4228	Y	
10402	Rockville	MD	USA	LOW	B	B	C		301/294-4522	Y	
10404	Lyon		FRA	E1	C	C	C		(7) 8478144	Y	
10430	Inglewood/Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10430	Los Angeles/Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10430	Vernon	CA	USA	HIGH	B	B	C		213/587-7514	Y	
10436	Concord/Walnut Creek	CA	USA	LOW	B	B	C		510/935-1507	Y	
10436	Pacheco/Walnut Creek	CA	USA	LOW	B	B	C		510/935-1507	Y	
10436	Pleasnthill/Walnt Ck	CA	USA	LOW	B	B	C		510/935-1507	Y	
10436	Walnut Creek	CA	USA	LOW	B	B	C		510/935-1507	Y	
10464	Quebec City	QU	CAN	CANH	C	C	C		418/647-1116	Y	
10467	Colorado Springs	CO	USA	MED	B	B	C		719/590-1003	Y	

10470	Arlington/Fort Worth	TX	USA	MED	B	B	C	817/332-9397	Y	
10470	Fort Worth	TX	USA	MED	B	B	C	817/332-9397	Y	
10472	Windsor	NY	USA	LOW	B	B		914/561-9103	N	
10506	Johnson City	TN	USA	LOW	B	B	C	615/928-9544	Y	
10516	Charlottesville	VA	USA	LOW	B	B	C	804/977-5661	Y	
10526	Houston	TX	USA	HIGH	B	B	C	713/496-1332	Y	
10542	McKinney	TX	USA	LOW	B	B	C	214/542-2641	Y	
10543	Akron	OH	USA	MED	B	B		216/376-6227	N	
10552	Salem	OR	USA	LOW	B	B	C	503/370-4314	Y	
10560	Muncie	IN	USA	LOW	B	B	C	317/281-9021	Y	
10567	Durham	NC	USA	HIGH	B	B	C	919/549-9025	Y	
10567	Chapel Hill/Durham	NC	USA	HIGH	B	B	C	919/549-9025	Y	
10570	Bozeman	MT	USA	LOW	B	B	C	406/585-9719	Y	
10574	Hilo	HI	USA	MED	B	B	C	808/935-5717	N	
10601	Augusta	ME	USA	LOW	B	B	C	207/622-3083	Y	
10602	Cape Girardeau	MO	USA	LOW	B	B	C	314/335-1518	Y	
10603	Elyria	OH	USA	LOW	B	B	C	216/324-7156	Y	
10604	Florence	SC	USA	LOW	B	B	C	803/664-0550	Y	
10605	Kingston	NY	USA	LOW	B	B	C	914/336-2790	Y	
10612	Montreal/St. Laurent	QU	CAN	CANH	C	C	C	514/747-2996	Y	
10612	St. Laurent	QU	CAN	CANH	C	C	C	514/747-2996	Y	
10615	Secane	PA	USA	LOW	B	B	C	215/543-3045	Y	
10621	Princeton/So. Brnswk	NJ	USA	HIGH	B	B		609/452-1018	N	
10621	South Brunswick	NJ	USA	HIGH	B	B		609/452-1018	N	
10622	South Brunswick	NJ	USA	HIGH	B	B	C	609/452-9529	Y	
10622	Princeton/So. Brnswk	NJ	USA	HIGH	B	B	C	609/452-9529	Y	
10631	Honolulu	HI	USA	MED	B	B		808/545-7610	N	
10632	Honolulu	HI	USA	MED			C	808/528-5300	Y	
10665	Tulsa	OK	USA	HIGH	B	B	C	918/585-2706	Y	
10666	Tulsa	OK	USA	HIGH	B	B	C	918/585-2706	Y	
10673	Springfield	MO	USA	LOW	B	B	C	417/881-6225	Y	
10703	Tortola		VGB	3	C	C	C	809/494-3993	N	TYMUSA
10705	Atlanta/Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
10705	Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
10705	Marietta/Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
10705	Norcross/Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
10710	New York	NY	USA	HIGH	B	B		212/943-4700	N	
10713	Houston	TX	USA	HIGH			C	713/870-8381	Y	
10726	Winnipeg	MB	CAN	CANH					N	
10727	Lawton	OK	USA	LOW	B	B	C	405/353-6987	Y	
10730	Grand Island	NE	USA	LOW	B	B	C	308/382-3176	Y	
10750	Steubenville/Wntsvl	OH	USA	LOW	B	B	C	614/284-0020	Y	
10750	Wintersville	OH	USA	LOW	B	B	C	614/284-0020	Y	
10753	El Segundo	CA	USA	MED	B	B	C	310/643-4228	Y	
10753	Mar Vista/El Segundo	CA	USA	MED	B	B	C	310/643-4228	Y	
10753	MarinaDelRey/El Sgnd	CA	USA	MED	B	B	C	310/643-4228	Y	
10753	Santa Monica/El Sgnd	CA	USA	MED	B	B	C	310/643-4228	Y	
11003	Bangor	ME	USA	LOW	B	B	C	207/990-0529	Y	
11010	Southfield	MI	USA	MED			C	313/557-2106	Y	
11012	Lincoln	NE	USA	LOW	B	B	C	402/464-6235	Y	
11013	Eugene	OR	USA	LOW	B	B	C	503/343-0044	Y	
11013	Springfield/Eugene	OR	USA	LOW	B	B	C	503/343-0044	Y	
11014	Waco	TX	USA	LOW	B	B	C	817/776-0880	Y	
11015	Killeen	TX	USA	LOW	B	B	C	817/526-8118	Y	
11026	Slidell	LA	USA	LOW	B	B	C	504/646-2900	Y	
11030	Atlanta/Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
11030	Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
11030	Marietta/Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
11030	Norcross/Doraville	GA	USA	HIGH	B	B		404/451-2208	N	
11035	Clearwater	FL	USA	MED	B	B	C	813/441-1621	Y	
11035	St. Petersbrg/Clrwrtr	FL	USA	MED	B	B	C	813/441-1621	Y	
11052	Eureka	CA	USA	LOW	B	B	C	707/445-3021	Y	
11053	Provo	UT	USA	LOW	B	B		801/373-2192	N	

11054	Corpus Christi	TX	USA	MED				C	512/289-1981	Y	
11061	Hong Kong		HKG	HK	C	C	C		877-2602	N	
11063	Cumberland	MD	USA	LOW	B	B	C		301/777-9320	Y	
11067	Auburn	ME	USA	LOW	B	B	C		207/795-6013	Y	
11067	Lewiston/Auburn	ME	USA	LOW	B	B	C		207/795-6013	Y	
11074	London		GBR	E1	C	C	C		(81)566-7260	Y	
11100	Naples	FL	USA	LOW	B	B	C		813/434-8080	Y	
11105	Memphis	TN	USA	MED	B	B	C		901/527-8122	Y	
11107	Vancouver	BC	CAN	HIG				C	604/682-6054	N	TYM-X25
11110	Dusseldorf		FRG	E1	C	C	C		(211)596871	Y	
11114	Calgary	AB	CAN	CANH				C	403/264-5472	Y	
11120	El Paso	TX	USA	MED	B	B	C		915/533-1453	Y	
11121	El Paso	TX	USA	MED	B	B	C		915/533-1453	Y	
11123	Buffalo	NY	USA	MED	B	B	C		716/893-1014	Y	
11130	Houston	TX	USA	HIGH	B	B	C		713/496-1332	Y	
11141	Amsterdam		NLD	E1					2041290546	N	DN-1
11144	Grand Rapids	MI	USA	MED				C	616/458-9252	N	
11150	Chicago	IL	USA	WATS	B	B	C		800/###-####	Y	
11151	Chicago	IL	USA	WATS	B	B	C		800/###-####	Y	
11152	Chicago	IL	USA	WATS	B	B	C		800/###-####	Y	
11156	Alexandria/Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
11156	Arlington/Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
11156	Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
11156	Washington/Fairfax	DC	USA	HIGH	B	B	C		703/352-3136	Y	
11156	Bethesda/Fairfax	MD	USA	HIGH	B	B	C		703/352-3136	Y	
11160	Chicago	IL	USA	WATS				C	800/###-####	Y	
11161	Winston-Salem	NC	USA	MED	B	B	C		919/765-1221	Y	
11162	Charleston	SC	USA	LOW	B	B	C		803/553-0860	Y	
11207	O'Fallon	IL	USA	LOW	B	B	C		618/632-3993	Y	
11223	London		GBR	E1	C	C	C		(71)489-8571	N	
11224	Monterey	CA	USA	LOW	B	B	C		408/375-2644	Y	
11225	London		GBR	E1	C	C	C		(71)489-8571	N	
11231	Lancaster	PA	USA	LOW	B	B	C		717/569-1081	Y	
11236	Lansing	MI	USA	MED	B	B	C		517/484-5344	Y	
11237	Columbia	SC	USA	MED	B	B	C		803/254-7563	Y	
11240	Greenville	SC	USA	MED	B	B	C		803/271-9213	Y	
11241	Mobile	AL	USA	MED	B	B	C		205/460-2515	Y	
11242	Lake Zurich/Palatine	IL	USA	LOW	B	B	C		708/991-7171	Y	
11242	Palatine	IL	USA	LOW	B	B	C		708/991-7171	Y	
11251	Denton	TX	USA	LOW	B	B	C		817/565-0552	Y	
11252	Vancouver	WA	USA	LOW	B	B	C		206/574-0427	Y	
11257	Little Rock	AR	USA	MED	B	B	C		501/666-6886	Y	
11266	Fort Collins	CO	USA	LOW	B	B	C		303/224-9819	Y	
11267	Amarillo	TX	USA	LOW	B	B	C		806/355-7088	Y	
11270	San Rafael	CA	USA	LOW	B	B	C		415/453-2087	Y	
11271	Cathedral City	CA	USA	LOW	B	B	C		619/324-0920	Y	
11271	Palm Sprngs/Cath Cty	CA	USA	LOW	B	B	C		619/324-0920	Y	
11272	Moorpark	CA	USA	LOW	B	B	C		805/523-0203	Y	
11273	San Clemente	CA	USA	LOW	B	B	C		714/240-9424	Y	
11274	Mishawaka/South Bend	IN	USA	MED	B	B	C		219/234-6410	Y	
11274	South Bend	IN	USA	MED	B	B	C		219/234-6410	Y	
11275	Bridgeport	CT	USA	MED	B	B	C		203/332-7256	Y	
11275	Stratford/Bridgeport	CT	USA	MED	B	B	C		203/332-7256	Y	
11276	Syracuse	NY	USA	MED	B	B	C		315/433-1593	Y	
11277	Alexandria/Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
11277	Arlington/Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
11277	Fairfax	VA	USA	HIGH	B	B	C		703/352-3136	Y	
11277	Washington/Fairfax	DC	USA	HIGH	B	B	C		703/352-3136	Y	
11277	Bethesda/Fairfax	MD	USA	HIGH	B	B	C		703/352-3136	Y	
11300	Toledo	OH	USA	MED	B	B	C		419/255-7705	Y	
11301	Harrisburg/Lemoyne	PA	USA	MED	B	B	C		717/975-9881	Y	
11301	Lemoyne	PA	USA	MED	B	B	C		717/975-9881	Y	
11304	Newark/Wilmington	DE	USA	MED	B	B	C		302/652-2036	Y	

11304	Wilmington	DE	USA	MED	B	B	C		302/652-2036	Y	
11305	Lyndhurst/Union City	NJ	USA	HIGH				C	201/617-9069	Y	
11305	Union City	NJ	USA	HIGH				C	201/617/9069	Y	
11305	Union City	NJ	USA	HIGH				C	201/617-9110	N	TYM-X25
11305	Lyndhurst/Union City	NJ	USA	HIGH				C	201/617-9110	N	TYM-X25
11305	Lyndhurst/Union City	NJ	USA	HIGH			C		201/617-9103	N	TYM-X25
11305	Union City	NJ	USA	HIGH			C		201/617-9103	N	TYM-X25
11306	Holyoke/Springfield	MA	USA	MED	B	B	C		413/787-0048	Y	
11306	Springfield	MA	USA	MED	B	B	C		413/787-0048	Y	
11307	Rockford	IL	USA	MED	B	B	C		815/633-2080	Y	
11313	Little Rock	AR	USA	MED				C	501/666-1224	Y	
11314	Alameda/Oakland	CA	USA	HIGH				C	510/638-7904	Y	
11314	Berkeley/Oakland	CA	USA	HIGH				C	510/638-7904	Y	
11314	Hayward/Oakland	CA	USA	HIGH				C	510/638-7904	Y	
11314	Oakland	CA	USA	HIGH				C	510/638-7904	Y	
11315	Oakridge	TN	USA	LOW	B	B	C		615/482-1466	Y	
11321	Northport	AL	USA	LOW	B	B	C		205/758-1116	Y	
11321	Tuscaloosa/Northport	AL	USA	LOW	B	B	C		205/758-1116	Y	
11322	Augusta/Martinez	GA	USA	LOW	B	B	C		404/855-0442	Y	
11322	Martinez	GA	USA	LOW	B	B	C		404/855-0442	Y	
11323	Owensboro	KY	USA	LOW	B	B	C		502/685-0959	Y	
11326	Toronto	ON	CAN	CANH				C	416/361-3028	Y	
11326	Toronto	ON	CAN	CANH			C	C	416/361-3383	N	TYM-X25
11331	Midlothian/Richmond	VA	USA	MED	B	B	C		804/330-2673	Y	
11331	Richmond	VA	USA	MED	B	B	C		804/330-2673	Y	
11346	Ft. Lauderdale	FL	USA	MED				C	305/779-3445	Y	
11346	Ft. Lauderdale	FL	USA	MED	B	B	C		305/467-1870	Y	
11346	Hollywd/Ft. Laudrdle	FL	USA	MED				C	305/779-3445	Y	
11346	Hollywd/Ft. Laudrdle	FL	USA	MED	B	B	C		305/467-1870	Y	
11346	Pompno Bch/Fr. Ldrdl	FL	USA	MED	B	B	C		305/467-1870	Y	
11346	Pompno Bch/Ft. Ldrdl	FL	USA	MED				C	305/779-3445	Y	
11356	Asheville	NC	USA	LOW	B	B	C		704/253-8945	Y	
11361	London		GBR	E1	C	C	C		(81)566-7260	Y	
11362	Stamford	CT	USA	HIGH	B	B	C		203/327-2974	Y	
11371	Santa Barbara	CA	USA	MED	B	B			805/564-2354	N	
11372	Santa Barbara	CA	USA	MED	B	B	C		805/965-1612	Y	
11376	New Orleans	LA	USA	HIGH				C	504/524-1738	Y	
11402	Modesto	CA	USA	LOW	B	B	C		209/527-0150	Y	
11405	Marlborough	MA	USA	LOW	B	B	C		508/481-0026	Y	
11447	Seattle	WA	USA	HIGH	B	B	C		206/281-7141	Y	
11447	Bellevue/Seattle	WA	USA	HIGH	B	B	C		206/281-7141	Y	
11451	Battle Creek	MI	USA	LOW	B	B	C		616/964-9303	Y	
11452	Harrisonburg	VA	USA	LOW	B	B	C		703/433-6333	Y	
11453	Groton	MA	USA	LOW	B	B	C		508/448-9361	Y	
11460	Chicago	IL	USA	HIGH				C	312/427-1506	N	TYM-X25
11460	Chicago	IL	USA	HIGH			C		312/427-1453	N	TYM-X25
11465	Munich		FRG	E1	C	C	C		(89)129-6081	Y	
11471	Clarksburg	WV	USA	LOW	B	B	C		304/624-1451	Y	
11500	Salt Lake City	UT	USA	HIGH				C	801/364-7605	Y	
11500	Salt Lake City	UT	USA	HIGH				C	801/364-7439	N	TYM-X25
11500	Salt Lake City	UT	USA	HIGH			C		801/364-7451	N	TYM-X25
11646	Hazelwood	MO	USA	HIGH	B	B	C		314/731-8283	Y	
11646	St. Louis	MO	USA	HIGH	B	B	C		314/731-8283	Y	
11646	Bridgeton/St. Louis	MO	USA	HIGH	B	B	C		314/731-8283	Y	
11652	Tampa	FL	USA	HIGH				C	813/933-7095	N	TYM-X25
11652	Tampa	FL	USA	HIGH			C		813/933-7303	N	TYM-X25
11671	Rochester	MN	USA	LOW	B	B	C		507/282-0830	Y	
11702	Georgetown	DE	USA	LOW	B	B	C		302/856-1788	Y	
11716	Greensburg	PA	USA	LOW	B	B	C		412/838-1920	Y	
11716	Latrobe/Greensburg	PA	USA	LOW	B	B	C		412/838-1920	Y	
11727	Huntsville	AL	USA	MED				Y	205/882-9199	Y	
11730	Alhambra	CA	USA	MED	B	B	C		818/308-1800	Y	
11730	Arcadia/Alhambra	CA	USA	MED	B	B	C		818/308-1800	Y	

11730	El Monte/Alhambra	CA	USA	MED	B	B	C		818/308-1800	Y
11730	Pasadena/Alhambra	CA	USA	MED	B	B	C		818/308-1800	Y
11732	Zurich		CHE	E1	C	C	C		(1) 837-0301	Y
11736	Leeds		GBR	E1			C		(532) 341838	Y
11741	Duluth	MN	USA	LOW	B	B	C		218/722-0655	Y
11743	Northfield	IL	USA	LOW	B	B	C		708/501-4536	Y
11744	Bristol		GBR	E1			C		(272) 255392	Y
11745	Hamburg		FRG	E1	C	C	C		(40)251-4037	Y
11752	West Bend	WI	USA	LOW	B	B	C		414/334-1755	Y
11753	St. Cloud	MN	USA	LOW	B	B	C		612/656-1280	Y
11754	Victoria	TX	USA	LOW	B	B	C		512/576-9200	Y
11764	Portsmouth/Norfolk	VA	USA	MED	B	B	C		804/857-0148	Y
11764	Virginia Bch/Norfolk	VA	USA	MED	B	B	C		804/857-0148	Y
11764	Norfolk	VA	USA	MED	B	B	C		804/857-0148	Y
12026	Columbia	MO	USA	LOW	B	B	C		314/875-5570	Y
12031	Presque Isle	ME	USA	LOW	B	B	C		207/764-4167	Y
12044	New Haven	CT	USA	MED				C	203/789-1848	Y
12045	Memphis	TN	USA	MED				C	901/521-1303	Y
12054	Fayetteville	NC	USA	LOW	B	B	C		919/424-9610	Y
12063	St. Louis	MO	USA	HIGH	B	B	C		314/731-8283	Y
12063	Bridgeton/St. Louis	MO	USA	HIGH	B	B	C		314/731-8283	Y
12066	Nashville	TN	USA	HIGH	B	B	C		615/889-5790	Y
12101	Belleville/O'Fallon	IL	USA	LOW	B	B	C		618/632-3993	Y
12150	Gary	IN	USA	LOW	B	B	C		219/884-7450	Y
12150	Hammond/Gary	IN	USA	LOW	B	B	C		219/884-7450	Y
12150	Highland/Gary	IN	USA	LOW	B	B	C		219/884-7450	Y
12151	Gary	IN	USA	LOW	B	B	C		219/884-7450	Y
12151	Hammond/Gary	IN	USA	LOW	B	B	C		219/884-7450	Y
12151	Highland/Gary	IN	USA	LOW	B	B	C		219/884-7450	Y
12161	Rotterdam		NLD	E1	C	C	C	C	(10) 4530099	Y
12161	Rotterdam		NLD	E1			C		(10) 4524923	N HSA
12161	Rotterdam		NLD	E1	C	C	C	C	(10) 4532002	Y
12201	Washington/Fairfax	DC	USA	HIGH	B	B			703/691-8200	N
12201	Bethesda/Fairfax	VA	USA	HIGH	B	B			703/691-8200	N
12201	Alexandria/Fairfax	VA	USA	HIGH	B	B			703/691-8200	
12201	Arlington/Fairfax	VA	USA	HIGH	B	B			703/691-8200	
12201	Fairfax	VA	USA	HIGH	B	B			703/691-8200	
12263	Lakeland	FL	USA	LOW	B	B	C		813/858-6970	Y
12263	Winterhaven/Lakeland	FL	USA	LOW	B	B	C		813/858-6970	Y
12314	Freeland	MI	USA	LOW	B	B	C		517/695-6751	Y
12314	Midland/Freeland	MI	USA	LOW	B	B	C		517/695-6751	Y
12314	Saginaw/Freeland	MI	USA	LOW	B	B	C		517/695-6751	Y
12361	Aurora/Denver	CO	USA	HIGH	B	B	C		303/832-3447	Y
12361	Boulder/Denver	CO	USA	HIGH	B	B	C		303/832-3447	Y
12361	Denver	CO	USA	HIGH	B	B	C		303/832-3447	Y
12371	Bremen		FRG	E1	C	C	C		(421) 170997	Y
12425	El Centro	CA	USA	LOW	B	B	C		619/352-5823	Y
12456	Fairfield	CA	USA	LOW	B	B	C		707/421-0106	Y
12460	Victorville	CA	USA	LOW	B	B	C		619/955-7050	Y
12513	Tallahassee	FL	USA	MED				C	904/422-0016	Y
12513	Tallahassee	FL	USA	MED	B	B	C		904/422-0149	Y
12514	Jacksonville	FL	USA	MED	B	B	C		904/721-8559	Y
12516	Watertown	NY	USA	LOW	B	B	C		315/788-1816	Y
12533	Lancaster	CA	USA	LOW	B	B	C		805/945-4962	Y
12534	Maui	HI	USA	LOW	B	B	C		808/661-7688	Y
12600	Meriden	CT	USA	LOW	B	B	C		203/686-1238	Y
12600	Middletown/Meriden	CT	USA	LOW	B	B	C		203/686-1238	Y
12601	Aiken	SC	USA	LOW	B	B	C		803/648-0237	Y
12611	London	ON	CAN	CANL	C	C	C		519/641-8362	Y
12620	Honolulu	HI	USA	MED			C		808/528-5300	Y
12621	Paducah	KY	USA	LOW	B	B	C		502/443-1086	Y
12622	Dover	DE	USA	LOW	B	B	C		302/678-3569	Y
12624	Marysville	CA	USA	LOW	B	B	C		916/749-8015	Y

12626	Great Falls	MT	USA	LOW	B	B	C	406/727-9510	Y	
12642	Los Gatos	CA	USA	LOW	B	B	C	408/356-1818	Y	
12650	Paris		FRA	E1	C	C	C	(1) 47728080	Y	
12720	Birmingham	AL	USA	HIGH	B	B	C	205/942-7898	Y	
12732	Midland	TX	USA	LOW	B	B	C	915/561-8401	Y	
12732	Odessa/Midland	TX	USA	LOW	B	B	C	915/561-8401	Y	
12742	Zanesville	FL	USA	LOW	B	B	C	614/454-2893	Y	new svc
12755	Bismark	ND	USA	LOW	B	B	C	701/223-5165	Y	
13010	Houston	TX	USA	HIGH	B	B	C	713/496-1332	Y	
13026	Spokane	WA	USA	MED	B	B	C	509/747-3011	Y	
13103	Sarasota	FL	USA	LOW	B	B	C	813/952-9000	Y	
13104	Goteborg		SWE	E2	C	C	C	(31) 450630	Y	
13110	Rochester	MN	USA	LOW	B	B	C	507/282-0830	Y	
13120	Dallas	TX	USA	HIGH	B	B	C	214/630-5516	Y	
13121	Downrs Grove/Gln Eln	IL	USA	MED	B	B	C	708/790-4955	Y	
13121	Glen Ellyn	IL	USA	MED	B	B	C	708/790-4955	Y	
13121	Wheaton/Glen Ellyn	IL	USA	MED	B	B	C	708/790-4955	Y	
13123	Knoxville	TN	USA	MED	B	B	C	615/694-0156	Y	
13132	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703/352-3136	Y	
13132	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703/352-3136	Y	
13132	Fairfax	VA	USA	HIGH	B	B	C	703/352-3136	Y	
13132	Washington/Fairfax	DC	USA	HIGH	B	B	C	703/352-3136	Y	
13132	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703/352-3136	Y	
13133	Alexandria/Fairfax	VA	USA	HIGH	B	B	C	703/352-3136	Y	
13133	Arlington/Fairfax	VA	USA	HIGH	B	B	C	703/352-3136	Y	
13133	Fairfax	VA	USA	HIGH	B	B	C	703/352-3136	Y	
13133	Washington/Fairfax	DC	USA	HIGH	B	B	C	703/352-3136	Y	
13133	Bethesda/Fairfax	MD	USA	HIGH	B	B	C	703/352-3136	Y	
13134	Baton Rouge	LA	USA	MED	B	B	C	504/291-0967	Y	
13154	Brookfield	WI	USA	HIGH	B	B	C	414/785-0630	Y	
13154	Milwaukee/Brookfield	WI	USA	HIGH	B	B	C	414/785-0630	Y	
13156	Alexandria	LA	USA	LOW	B	B	C	318/445-1800	Y	
13164	Sioux City	IA	USA	LOW	B	B	C	712/255-3834	Y	
13171	Upland	CA	USA	LOW	B	B	C	714/985-1153	Y	
13172	Gulfport	MS	USA	LOW	B	B	C	601/864-9441	Y	
13173	Lawrence	KS	USA	LOW	B	B	C	913/843-4870	Y	
13177	Wilmington	NC	USA	LOW	B	B	C	919/392-7913	Y	
13213	Edmunton	AB	CAN		C	C	C	403/484-4404	Y	
13214	Indianapolis	IN	USA	HIGH	B	B	C	317/632-6408	Y	
13215	Petersburg	VA	USA	LOW	B	B	C	804/861-1788	Y	
13216	Vineland	NJ	USA	LOW	B	B	C	609/692-8943	Y	
13224	Frankfurt		FRG	E1	C	C	C	(69) 507-6736	Y	
13226	Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13226	Elizabeth/Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13226	Jersey City/Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13226	Union/Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13227	Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13227	Elizabeth/Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13227	Jersey City/Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13227	Union/Newark	NJ	USA	HIGH	B	B	C	201/824-3044	Y	
13230	Miami	FL	USA	HIGH	B	B	C	305/599-2900	Y	
13231	Hempstead	NY	USA	MED	B	B	C	516/485-7422	Y	
13231	Mineola/Hempstead	NY	USA	MED	B	B	C	516/485-7422	Y	
13233	New York	NY	USA	HIGH	B	B	C	212/809-9660	Y	
13234	New York	NY	USA	HIGH	B	B	C	212/809-9660	Y	
13235	New York	NY	USA	HIGH	B	B	C	212/809-9660	Y	
13236	New York	NY	USA	HIGH	B	B	C	212/809-9660	Y	
13240	Tampa	FL	USA	HIGH	B	B	C	813/933-6210	Y	
13242	Morristown	NJ	USA	LOW	B	B	C	201/539-1222	Y	
13244	Pueblo	CO	USA	LOW	B	B	C	719/543-9712	Y	
13245	Norristown	PA	USA	MED	B	B	C	215/666-9190	Y	
13246	Salt Lake City	UT	USA	HIGH	B	B	C	801/533-8152	Y	
13247	Baton Rouge	LA	USA	MED	B	B	C	504/291-0967	Y	

13251	Newport Beach	CA	USA	HIGH	B	B	C	714/852-8141	Y
13251	Anaheim/Newprt Beach	CA	USA	HIGH	B	B	C	714/852-8141	Y
13251	Irvine/Newport Beach	CA	USA	HIGH	B	B	C	714/852-8141	Y
13251	Santa Ana/Newprt Bch	CA	USA	HIGH	B	B	C	714/852-8141	Y
13252	Newport Beach	CA	USA	HIGH	B	B	C	714/852-8141	Y
13252	Anaheim/Newprt Beach	CA	USA	HIGH	B	B	C	714/852-8141	Y
13252	Irvine/Newport Beach	CA	USA	HIGH	B	B	C	714/852-8141	Y
13252	Santa Ana/Newprt Bch	CA	USA	HIGH	B	B	C	714/852-8141	Y
13253	Longwood/Orlando	FL	USA	MED	B	B	C	407/841-0217	Y
13253	Orlando	FL	USA	MED	B	B	C	407/841-0217	Y
13256	Temple	TX	USA	LOW	B	B	C	817/773-2545	Y
13273	Downrs Grove/Gln Eln	IL	USA	MED	B	B	C	708/790-4955	Y
13273	Glen Ellyn	IL	USA	MED	B	B	C	708/790-4955	Y
13273	Wheaton/Glen Ellyn	IL	USA	MED	B	B	C	708/790-4955	Y
13300	New Orleans	LA	USA	HIGH	B	B	C	504/525-2014	Y
13301	New Orleans	LA	USA	HIGH	B	B	C	504/525-2014	Y
13314	Frederick/Myersville	MD	USA	LOW	B	B	C	301/293-9504	Y
13314	Hagerstown/Myersvill	MD	USA	LOW	B	B	C	301/293-9504	Y
13314	Myersville	MD	USA	LOW	B	B	C	301/293-9504	Y
13334	Toulouse		FRA	E1	C	C	C	(61) 300291	Y
13341	Hull/Ottawa	ON	CAN	CANH	C	C	C	613/563-2910	N
13341	Ottawa	ON	CAN	CANH	C	C	C	613/563-2910	N
13344	Bellingham	WA	USA	LOW	B	B	C	206/671-7750	Y
13345	Springfield	OH	USA	LOW	B	B	C	513/322-8855	Y
13346	Kankakee/Bradley	IL	USA	LOW	B	B	C	815/935-2352	Y
13346	Bradley	IL	USA	LOW	B	B	C	815/935-2352	Y
13354	Chico	CA	USA	LOW	B	B	C	916/343-4401	Y
13357	Bryan	TX	USA	LOW	B	B	C	409/823-1090	Y
13364	Missoula	MT	USA	LOW	B	B	C	406/542-0472	Y
13365	Pascagoula	MS	USA	LOW	B	B	C	601/769-0121	Y
13430	Minot	ND	USA	LOW	B	B	C	701/838-2140	Y
13446	Red Bank	NJ	USA	LOW	B	B	C	908/758-0337	Y
13446	Eatontown/Red Bank	NJ	USA	LOW	B	B	C	908/758-0337	Y
13446	Long Branch/Red Bank	NJ	USA	LOW	B	B	C	908/758-0337	Y
13450	Elmira	NY	USA	LOW	B	B	C	607/737-9065	Y
13451	Rome		ITA	E2	B	C	C	(6) 8550340	Y
13452	Turin		ITA	E2	B	C	C	(11) 2480125	Y
13524	Fayetteville	AR	USA	LOW	B	B	C	501/442-0234	Y
13524	Springdale/Fayettevl	AR	USA	LOW	B	B	C	501/442-0234	Y
13535	Honolulu	HI	USA	MED			C	808/528-5300	Y
13541	Colorado Springs	CO	USA	MED	B	B	C	719/590-1003	Y
13552	Bakersfield	CA	USA	LOW	B	B	C	805/325-0371	Y
13553	Harrisburg/Lemoyne	PA	USA	MED	B	B	C	717/975-9881	Y
13553	Lemoyne	PA	USA	MED	B	B	C	717/975-9881	Y
13554	Richland	WA	USA	MED	B	B	C	509/375-3367	Y
13557	Port Arthur	TX	USA	LOW	B	B	C	409/721-3400	Y
13557	Nederland/Pt. Arthur	TX	USA	LOW	B	B	C	409/721-3400	Y
13572	Springfield	MO	USA	LOW	B	B	C	417/881-6225	Y
13573	Austin	TX	USA	HIGH	B	B	C	512/448-1096	Y
13576	Fresno	CA	USA	LOW	B	B	C	209/442-4328	Y
13577	Shreveport	LA	USA	LOW	B	B	C	318/688-5840	Y
13601	Birmingham	AL	USA	HIGH	B	B	C	205/942-7898	Y
13602	Birmingham	AL	USA	HIGH	B	B	C	205/942-7898	Y
13603	Louisville	KY	USA	MED	B	B	C	502/499-9825	Y
13614	Long Beach	CA	USA	MED	B	B	C	310/436-6033	Y
13614	Norwalk/Long Beach	CA	USA	MED	B	B	C	310/436-6033	Y
13614	San Pedro/Long Beach	CA	USA	MED	B	B	C	310/436-6033	Y
13616	Little Rock	AR	USA	MED	B	B	C	501/666-6886	Y
13617	Philadelphia	PA	USA	HIGH	B	B	C	215/592-8750	Y
13620	Mobile	AL	USA	MED	B	B	C	205/460-2515	Y
13623	Akron	OH	USA	MED	B	B	C	216/376-8330	Y
13624	Toledo	OH	USA	MED	B	B	C	419/255-7705	Y
13626	Memphis	TN	USA	MED	B	B	C	901/527-8122	Y

13641	Burton	MI	USA	LOW	B	B	C	313/743-8350	Y
13643	Madrid		ESP	E2	C	C	C	(1) 7661900	Y
13645	Lansing	MI	USA	MED	B	B	C	517/484-5344	Y
13646	Fort Worth	TX	USA	MED	B	B	C	817/332-9397	Y
13646	Alington/Fort Worth	TX	USA	MED	B	B	C	817/332-9397	Y
13650	Columbia	SC	USA	MED	B	B	C	803/254-7563	Y
13651	Columbia	SC	USA	MED	B	B	C	803/254-7563	Y
13653	Ft. Wayne	IN	USA	LOW	B	B	C	219/422-2581	Y
13655	Huntsville	AL	USA	MED	B	B	C	205/882-1519	Y

* Node 4003 is listed for many different countries. It represents the Enhanced Global Connection Service which includes nodes: 2576, 3512, 3513, and 4003.

B=BELL 103/113 (300 bps) or BELL 212A (1200 bps) compatible modems

C=CCITT V.21(300 bps) or CCITT V.22 bis(2400 bps) or CCITT V.32 compatible modems

==Phrack Inc.==

Volume Four, Issue Forty, File 11 of 14

"Told ya...Should a killed me last year!"

by Knight Lightning & Dispater

Special Thanks: Dr. Williams, Holistic Hacker, Nihil, and The Pope

SummerCon '92
 June 26-28, 1992
 Executive International Hotel

"SummerCon... What is it? In many ways, SummerCon is much more than just a convention that attracts America's greatest phreaking and hacking personalities. SummerCon is a state of mind.

Hackers by nature are urged on by a hidden sense of adventure to explore the unknown, to challenge the unchallenged, to reach out and experiment with anything and everything. The realization that we are not alone in our quest sometimes comes as a great gift and the opportunity to meet one's heroes, partners, and idols can be the most awe-inspiring aspect of the hacker community -- this is what SummerCon is all about.

On the surface, SummerCon looks like a handful of youths hanging out at a hotel in St. Louis, Missouri. To me, it is more like one of those madcap movies you see on late night Home Box Office or something. No real point or direction, rebels without cause, all in the name of frantic fun and games. The atmosphere surrounding SummerCon is that of

a dream world where once a year you can escape to a fantasy where ingenuity is king and you have friends around you at every moment. SummerCon itself may only last a weekend, but the friendships last a lifetime."

-- Knight Lightning, Phrack 28, File 8 (PWN Special on SummerCon '89)

SummerCon! At last, a return to the original idea behind the event. It was great! It was crazy! It was a party! It was everything it should have been and more.

When Taran King, Forest Ranger, and Knight Lightning first conceived the idea of SummerCon in late 1986, they probably never imagined that they would all three still be involved six years later or just how popular their high-school dream would become.

It seemed as though nothing could top SummerCon '89. It was a great turnout of 23 people, there was a serious conference, there was also sorts of mischief and mayhem, and all in all, everyone had a great time. In 1990, SummerCon coincidentally took place on the same weekend on which the United States government dropped charges on Knight Lightning. The turnout was less than ten people and the conference was anything, but a success.

In 1991, SummerCon tried something new. The theme that year was CyberView and it had a special focus on civil liberties issues. The turnout was average, but something was missing. Finally, in 1992, the spirit of SummerCon was reborn anew.

Setting Up For SummerCon '92

~~~~~

Setting up SummerCon this year was a tricky situation. Knight Lightning had moved to Washington, D.C., Dispatier didn't live in St. Louis, Taran King was working full time, and Forest Ranger was nowhere to be found. Luckily, there was Rambone. With help from Taran King, Rambone set forth to make sure that the hotel accommodations and the conference room arrangements were taken care of and without his help, SummerCon might possibly not have happened.

All sorts of other arrangements had to be made as well. We wanted this year's conference to be very special and so for the first time ever, we decided to embark on the risky enterprise of designing and selling Phrack/SummerCon t-shirts. Knight Lightning and Dispatier worked together on the design work and Dispatier took care of the art and manufacturing. For those who haven't seen or heard about these shirts before, a brief description is in order.

---

#### Phrack/SummerCon '92 T-Shirts

~~~~~

There were only a very limited number of shirts made for the conference and they were sold out. A re-order was issued, mostly for people who attended the conference (but didn't get a shirt because of the small supply). A few shirts were reserved for people that were unable to attend. Unlike the Legion of Doom, Internet World Tour shirts, Phrack has no plans at this time to sell shirts to the general public. If there is a change in policy, we will let the readers know immediately.

The shirts are standard white, short-sleeved t-shirts with no pockets.

Front: On the left breast there is a picture resembling Oliver Wendall Jones (the computer hacker from the comic strip Bloom County). He is swinging his sword while standing at ground zero inside the cross hairs

of a rifle. Circling above him are the words, "SummerCon '92" and below him, "June 26-28 St. Louis, MO."

Back:

PHRACK
M a g a z i n e

When You Care Enough
To Indict The Very Best

PHRACK: 1 Secret Service: 0

911's A JOKE!

The information contained
herein should not be disclosed
to unauthorized persons. It is
meant solely for use by authorized
employees of the BELLSOUTH Corporation
or any of its subsidiaries.

Executive International Hotel... Not A Best Western Anymore?

~~~~~  
All parties concerned decided that we should return to the site where our best conferences had been held, the Executive International Best Western Hotel, but we had a surprise waiting for us when we arrived for the conference. It turned out that the Executive International was no longer a Best Western, in fact they had gone bankrupt. To make matters worse, the bank that foreclosed on the property failed as well -- in other words, the Executive International was now owned by the United States Government!

- - - - -  
SummerCon Begins

~~~~~  
There was so much going on and there were so many people at the conference, that there is no possible way to give a play-by-play of events at SummerCon.

Knight Lightning arrived the Thursday before and Dispatser flew in in the wee hours of the morning on Friday. When KL arrived with TK at the hotel around 1 PM, the conference was already in full swing with groups of guys from Texas and Boston congregated outside the hotel wearing Phrack t-shirts and already trading war stories. Perhaps the biggest surprise was the arrival of Doc Holiday, who no one had been able to contact to invite -- of course the surprise was more on Erik Bloodaxe than anyone else.

More and more people arrived during the day, and as they did, a strange sensation was shared among the alumni from SummerCon's past. True, Tuc and Lex Luthor weren't here, but outside of that, this was already looking like a reunion of all the people from all the SummerCons that had been before.

Lucifer 666 was running around with Control C, The Disk Jockey was seen cruising the downtown bar scene with Forest Ranger and Tom Brokaw, Erik Bloodaxe and Doc Holiday called some of the girls they had met from the previous year's convention. Everything was happening so fast, it was hard to keep track of, so we didn't try. We just had fun.

About 1/3 of the people at SummerCon went to see "Batman Returns." In light of the trip at the SummerCon of 1989, it seemed like a good idea. Others hung out poolside, roaming the hotel and its adjoining office complex, and still others

raided the free buffet at the Radison Hotel down the street.

The Washington, D.C. contingent of SummerCon guests were content to sit in their room most the evening and explore Internet sites in the St. Louis area. Some went trashing, some hit the bars looking for women, and some sat in the room occupied by Restricted Data Transmissions (RDT) for some good information exchange.

Meanwhile, an underage hacker named Pyro (gee that's an original name) was the first to meet the pride and joy of Springfield, Illinois. Both of these young women claimed to be age 16 and Pyro was the first to experience some of their womanhood. One of "girls" was named Dena and she was in the mood for some action as well. Clawing at almost every guy at the hotel, she refused to leave. She finally disappeared into a room and was not heard from again until the next morning.

SummerCon: The Conference

~~~~~

The previous evening's activities had taken their toll. When 12 noon came around, most of the hackers weren't even awake yet, let alone prepared for the conference session. The meeting was re-scheduled to 1 PM, but in the meantime Knight Lightning passed out copies of Security Insider Report (from Interpact), information about InterTek, a ComputerWorld article by Chris 'Erik Bloodaxe' Goggans (this article also appears in PWN 40/1), while Mr. Icom did the same with back issues of Cybertek. Emmanuel Goldstein was busy selling the new black 2600 t-shirts and passing out back issues of 2600 Magazine. Copies of a recent article about hackers doing computer security from the Boston Business Journal were also to be found compliments of RDT. RDT was also responsible for making this year's SummerCon buttons. Holistic Hacker made some as well. Thanks to all parties concerned for your great work and efforts.

Although it wasn't exactly made available for everyone to take a close look at, Knight Lightning proudly showed off his pre-release copy of THE HACKER CRACKDOWN by Bruce Sterling. This book, which will be available in hardback to the public on October 15, 1992, looks to be one of the most popular literary works on the world of hackers ever. It focuses on the raids in the Atlanta-LOD/Phrack/E911 case and Operation Sun Devil. It is believed that Knight Lightning himself appears on the cover of the book.

With the gavel-like banging of a lineman test set, Knight Lightning formally called the meeting to order at about 1:15 PM. He expressed his appreciation for the massive attendance (there were at least 60 people actually at the SummerCon meeting). Rambone made a quick note about the activities of the previous night as laughter and jokes about the "cyber-nymphs" erupted from all around the room.

Disputer took the floor for a moment to welcome everyone as well and then expressed his gratitude to the members of RDT for all of their help in producing Phrack issues during the past year. A discussion about who owned the hotel began briefly and then the first conference speaker was called to the floor.

- - - - -

#### 1. The Gatsby

"I'm sure you're all familiar by now with the media stories of the '1000-member ring of hackers' that supposedly have been invading the credit bureaus of CBI/Equifax, but the story isn't true and there is a lot more going on."

Gatsby explained that a hacker named The Prisoner (aka Multiplexor) from Indianapolis (and apparently also to some extent from Long Island) flew to San

Diego to see a girl, supposedly on a carded ticket.

While in San Diego, he allegedly broke into computers at Zale's Jewlery store and pulled credit card info from their point-of-sales system. After he vacated the rented room he had been staying in, he foolishly left behind the credit card printouts and his former landlord (whom he owed money to) discovered them and called the San Diego Police Department.

Sometime later, Multiplexor was met at his new accommodations at the Sleepy Time Motel in San Diego by the police. The FBI was brought into the case and he was kept at the Marriott Hotel for two weeks, all expenses paid! While under government supervision, Multiplexor logged into several systems, including Scantronics BBS.

During the course of the investigation, a hacker known as The Crypt Keeper came forward to tell what he knew about the hacker underground. He eventually would give the police access to Scantronics BBS logs he had in his possession after using The Gatsby's password to login to the system.

These logs were used by the police to gain search warrants for Scantronics BBS and its now unhappy former sysop, Kludge.

[The full details, police reports, warrants, and an interview with The Crypt keeper appears in Phrack World News 40/1.]

## 2. Agent Steal

Agent Steal gave a very informative talk about his dealings with Kevin Poulson, know to some as Dark Dante. AS related some of the experiences and adventures that the two of them had been through several years ago and talked about how Kevin used to break into central offices on a daily bases. Poulsen even had special equipment set up in his apartment to prevent him from being traced. Poulsen of course was the subject of a federal indictment and appeared on an episode of Unsolved Mysteries. He has since been taken into custody and is awaiting trial.

Agent Steal himself had spent a short time in prison on some bogus charges that were brought against him to elicit his help in prosecuting Poulsen. He refused to assist, but he eventually was released anyway. He said that he was looking forward to something different now, but he may have been referring to the Ozzy Osbourne concert later that night in St. Louis. Agent Steal is working on a book about his adventures with Poulsen called "Data Thief" and he expects it to be published in the near future.

## 3. Emmanuel Goldstein, 2600 Magazine, Editor

"Many people mistrust the government and big business, and they want to know how to fight back."

Emmanuel Goldstein spoke about the First Amendment and why 2600 Magazine has been able to exist and grow over the years despite the events that haunted Phrack in 1990. During 2600's eight years in existence, the magazine has never once been directly harassed by the government. The main reason he believes that Phrack was hit and 2600 left alone is because 2600 is a printed (hardcopy) publication.

However, 2600 is in need of good writers and will print anything, leaked or sent to them, it doesn't matter. 2600 has never been sued, although they are often threatened with legal action [See PWN 40/3 for the latest threats against 2600 from Bellcore]. 2600 has a subscription list of 1500 and a newstand of 3000.



He also spoke about some of their press releases that were issued in order to alert people about insecure systems, but that the information is never acted upon until something happens. People always like to blame the magazine for giving the details on how to do something (such as opening Fed Ex drop boxes), but never take action to correct the problems the magazine exposes.

A few people had questions for Emmanuel. For example, he was asked, "How do you morally justify hacking and the type of information published in 2600?" He responded by pointing out that 2600 only prints information about security flaws which need to be addressed and fixed.

Emmanuel was also asked if there was any fallout from the Simplex lock hacking article which described how to hack Simplex locks with out any tools and in less than 20 minutes (often less than 3 minutes). Given that Simplex locks are widely used at universities and Federal Express drop boxes, one would expect some sort of action. Emmanuel replied that he was surprised that there hadn't been much of a response or any action taken against 2600 because of the article. However, based on what many readers have told him, it seems that nobody has even changed the default combinations!

#### 4. Control C [Legion of Doom]

Control C has been a hacker surrounded by a lot of controversy over the years, from his days with the Legion of Doom through his employment and termination from Michigan Bell security.

He addressed the circumstances that led to his finding work with Michigan Bell. In 1987, Control C had started to log into Michigan Bell computers almost on a daily basis for the purpose of becoming better acquainted with C programming. During one 4 hour session, Michigan Bell Security traced his call back to Chicago (where he had been in school at the time). The next day, ^C had moved back to Detroit and he received a call from some gentlemen who wanted to invite him to lunch.

When he showed up, he was greeted by Michigan Bell Security personnel and the country sheriff's department. The result was a job where his main responsibility was to find flaws in their computer security by any means necessary. Over the years, Control C found well over 100 different holes and other weaknesses in their systems.

As time went on and key people left and were replaced by staff with more conservative attitudes, a new vice president (and former police officer) came in and decided it was no longer fashionable to employ a hacker. Control C was informed that he must leave despite the need for his services.

Shortly after Control C agreed to depart, the Secret Service became involved. They wanted to bring charges on ^C for the original break-ins at Michigan Bell that led to his employment. It didn't matter that Michigan Bell had signed documents that they would not bring charges. It didn't prevent the Secret Service from coming after him in 1990 (right during the same time as the E911 Phrack case and LOD-Atlanta cases began).

Control C was requested to take a polygraph. However, the timing was not good and ^C's lawyer request a new time. Now more than a year and a half since the request was made, ^C has not heard back from the Secret Service. Today ^C has moved on to a new vocation.

#### 5. Signal Surfer

Signal Surfer voiced his concerns about the bad reputation hackers have in the computer industry when in reality, most people in the industry are hackers in

the first place. He expressed an interest in trying to get people together to work on changing the stereotype of the modern hacker and helping hackers find legitimate jobs in the computer field.

#### 6. Predat0r, TAP Magazine, Editor; Blitzkrieg BBS, Sysop

Predat0r gave a short update on the current status of TAP and tried to explain why he hadn't produced an issue in over a year. Legal problems (something about being accused of stealing a laptop computer) that were taking up his time and resources were at fault. However, he says that those issues have been resolved and that TAP will start publishing again with issue #106 sometime this fall.

He gave his promise that he would not just fold the magazine and rip everyone off who had sent him money.

#### 7. Mr. Icom, Cybertek, Editor

Similar to Predat0r, Mr. Icom expressed his apologies for having been somewhat delinquent in getting new issues of his magazine out. He claimed that issue #7 would be released in the near future.

#### 8. Erik Bloodaxe (Chris Goggans) [Legion of Doom] [Comsec Data Security, Inc.]

It was only a year ago at SummerCon '91 that Erik Bloodaxe, Doc Holiday, and Malefactor proudly announced the formation of Comsec. Now, the following year, it seemed that events had come full circle. What had happened to Comsec? Why did it go out of business? What is the deal? That's what everyone wanted to know and what Goggans was prepared to discuss.

One of the factors that contributed to the failure of Comsec was operating costs associated with creating the company in the first place. Unfulfilled promises of investment in the company from people like Kenyon "Malefactor" Shulman and a whisper campaign against them by others in the computer security industry and a criminally negligent press hurt them badly, so much in fact they could not recover.

Goggans continued his tale of corruption and unfair play in the security community. For example, there was an agreement between Goggans and ISPNews about Goggans writing a regular column in their bi-monthly publication. However, after he submitted his first article, the newly formed editorial board decided against allowing it to be published. They said it was common for the editorial board to not allow sensitive articles in their magazine. But when ISPNews was asked what other contributors had their articles reviewed like this, they could produce no names. It should also be pointed out that among the members of the editorial board is one William J. Cook, formally an assistant United States Attorney in Chicago -- the same prosecutor who is responsible for the cases against Phrack co-founder Craig Neidorf (Knight Lightning), Shadow Hawk, Steve Jackson Games, Len Rose, The Mentor, and Chris Goggans himself!

But it didn't end there! Someone on the editorial advisory board (without permission from Goggans) forwarded his article to the head of security for SprintNet. Goggans received a threatening letter from SprintNet that called his article potentially libelous and claimed that it contained inaccuracies and proprietary company information.

But waitasec if the article contains confidential information then how could it be innaccurate? And if it's inaccurate then how could it divulge useful security flaws in their security?

Most recently, Goggans wrote an article for ComputerWorld (see PWN 40/1) about hackers and computer security. It addresses Tymnet and Telenet security issues. He discussed how hackers exploit these networks and how they can be stopped. He read the article aloud in full. It was typical of most security articles -- detailed, technically rounded, and somewhat dry. There were no big security revelations or tips.

He then went on to read some of the editorial replies of people responding to his article in subsequent issues of ComputerWorld. The audience did not approve of their negative response.

Finally, the discussion turned to the situation with MOD. Goggans talked about the persistent harassment he had been subjected to by Phiber Optik and other members of his alleged New York based organization.

Goggans said that in addition to the usual childish prank calls he would often receive, MOD obtained his credit information including his credit card numbers and posted them on bulletin boards and IRC. They were also responsible for changing his residential home telephone long distance service from U.S. Sprint to AT&T so they could more easily obtain his long distance calling records.

He was not alone -- other partners at Comsec and Doc Holiday's (Scott Chasin) mother were also harassed. Harassing a hacker is one thing, but going after a man's family and livelihood is clearly stepping beyond the bounds of a hacker's code of ethics. Something had to be done about the problem, so Comsec decided to end MOD's reign of criminal obnoxiousness by any means necessary.

There was a debate as to the proper way to handle this situation. Goggans revealed that he eventually turned to the FBI for assistance, who were surprising helpful. Some people at SummerCon were critical of his admission.

Emmanuel Goldstein was the most outspoken of those who responded. "If we start resorting to asking the FBI to resolve our problems, then that is a worse violation than what MOD did to you. The more appropriate response would be to use the same tricks to get back at them."

Emmanuel also gave an example of what he meant. One day, his office started receiving lots of calls from people who wanted trips to Europe. It turned out that an answering machine at a travel agency had been left with an outgoing message that told callers to contact both John Maxfield and Emmanuel Goldstein and gave out both their numbers. Maxfield solved the problem by calling the feds... 2600 hacked the answering machine and changed the message to something more innocuous.

However clever Emmanuel's ideas might be, Goggans stated that, "legitimate business people cannot resort to illegal means to correct such a situation. We had no other alternatives."

The debate continued for 30 minutes until, eventually, Knight Lightning stepped in, pointed out that this discussion could go on forever, and that it was time to start closing up shop.

## 9. DrunkFux, HoHoCon, Director

Before the meeting was officially concluded, dFx had a few things to discuss concerning how the guests had been conducting themselves in the hotel and he wanted to relate an experience he had at HoHoCon '91.

"The rowdiness at HoHoCon made last night at SummerCon look like a daycamp."

Drunkfux explained that the managers at the hotel for HoHoCon blamed the

conferences guests for all sorts of damage, and threatened to hold dFx financially responsible. The manager even threatened to bill his credit card for the damage. dFx responded by calling his credit card company and they informed him that what the hotel had threatened to do was illegal and they would be more than happy to prosecute the Hilton Hotel if they attempted to bill dFx for such charges.

The Hilton staff claimed that some conference guests set fire to part of a hallway, but refused to show dFx the damage when asked. dFx's attorney (a relative who had gotten involved at this point) asked if any fire alarms had gone off. The reply was no. The attorney then informed the Hilton staff that he would be happy to sue them on behalf of the conference guests for endangering their lives by placing them in accommodations with defective fire alarms. The Hilton staff changed their story.

Another claim against the HoHo'ers was that they had engaged in and allowed underage drinking. The attorney pointed out that the hotel's own bartenders were responsible for serving many of them and if Hilton's claim was true, he would be forced to call the state and have the hotel's liquor license revoked. The Hilton staff changed their story.

This sequence of point/counter-point repeated itself a few times until all claims were dropped.

A few days later, the two hotel managers who had previously accused dFx of damage went to his house to personally apologize. They gave him coupons for free nights the next time he stays at one of their hotels. dFx recorded the meeting on videotape and he joked around about putting the scene into gifs and distributing it to a BBS near you!

---

#### Afterwards

~~~~~

After the official meeting, many guests left the hotel to eat, trash, and explore the city. Frosty and some of the other GCMS-MechWarriors started a game of Hacker (Steve Jackson Games) in the conference room. Many people soon wandered over to Northwest Plaza Mall; where the trouble began.

Rule #4

~~~~~

About 10 or more people (including Emmanuel Goldstein, The Conflict, Erik Bloodaxe, Doc Holiday, and Signal Surfer) had entered the Northwest Plaza mall and a couple of them had baseball caps on... backwards.

A few minutes later, they were approached by mall security who told them that wearing their hats backwards was a violation of Rule #4 and was not allowed. Specifically the security guard said, "All clothing must be worn in the way it was meant to be worn." Go figure, aren't hats supposed to be worn on your head? This was more than Emmanuel and the others would take. They marched right into Sears and Emmanuel bought everyone (who didn't already have a hat) a bright red St. Louis Cardinals baseball cap.

Now all of them had their hats on backwards and they started strolling around the mall soon catching the eye of another always-alert rent-a-cop, mall security guard. After telling them to turn their hats around (and dropping his walkie-talkie in his attempt to call for backup), the security guard was approached by Emmanuel who wanted to discuss this Rule #4.

Another guard mumbled something about how a case on the matter had already gone to the appellate court, but he neglected to mention the outcome and we have been unable to find any details about case.

The security guards (now in full force) told Emmanuel this policy was in fact posted at all entrances and then they threw everyone out of the mall. Emmanuel says that he circled the mall noting that the rule was actually only posted at 2 of the 12 entrances. Another interesting rule was #6, which made it illegal to have a cellular phone, beeper, or any other device capable of making sounds in the mall. Erik Bloodaxe had broken this rule when he had played "Mary Had A Little Lamb" on Signal Surfers cellular phone.

## Nightfall

~~~~~

Towards the late afternoon about half of the Con ventured to the St. Louis waterfront on the Mississippi (Laclede's Landing) where the riverboats, bars and the Arch is found.

Holistic Hacker showed videos in his room including:

"ESS Phun"	- A humorous raid of a Bell Central Office by three hackers.
"Unsolved Mysteries"	- The Kevin Poulsen episode.
"Rudolph the Heavy-Metal Reindeer"	- No explanation.
"Good Morning America"	- See Doc Holiday EAT his own hand!
"Now It Can Be Told"	- Phiber Optik, Emmanuel Goldstein, and Knight Lightning on Geraldo.
"SummerCon '89"	- Highlights of SummerCon '89.
"SummerCon '91"	- Highlights of SummerCon '91.

Later in the evening, things just went out of control. Smoke bombs were going off, power outages were occurring, rooms were filling up with trash found in dumpsters at major computer and telecommunications office buildings. Dena was back stalking new prey (and found it).

Agent Steal and DrunkFux went to the Ozzy Osbourne concert while Erik Bloodaxe and Doc Holiday went out with the girls from last year's conference. They didn't make it back to the hotel until the next morning <wink wink>.

Security guards were running around threatening to send people to jail for no specific reason other than being disruptive.

The only serious discussions that night took place in the RDT room.

Sunday

~~~~~

The guests slowly began waking up just before mandatory checkout time from the hotel. As they gathered in the lobby and outside for last minute discussions and group photos, the group began to slowly dwindle in size. A few had to catch flights right away, a few would be staying until Monday morning, but everyone promised to return next year.

-----  
PWN ^^ PWN ^^ PWN { SummerCon '92 } PWN ^^ PWN ^^ PWN  
PWN ^^ PWN ^^ PWN { Guest List! } PWN ^^ PWN ^^ PWN

|                |                 |                  |
|----------------|-----------------|------------------|
| Agent Steal    | Erik Bloodaxe   | The Not          |
| Albatross      | Father Crime    | Omega            |
| Apollo Phoebus | Forest Ranger   | OPii             |
| Aragorn        | Frosty          | Phaedrus         |
| Black Phoenix  | Gateway         | Phantom Phreaker |
| Brian Oblivion | The Gatsby      | The Pope         |
| Bucky          | Golgo 13        | Predat0r         |
| The Butler     | Holistic Hacker | The Public       |

|                    |                  |               |
|--------------------|------------------|---------------|
| Coder Decoder      | Hunter           | Pyro          |
| Colin              | Junkmaster       | Rambone       |
| The Conflict       | Just Dave        | Sarlo         |
| Control C          | Knight Lightning | Scooter       |
| Count Zero         | Krynn            | The Serpent   |
| Cray-Z Phreaker    | Lord MacDuff     | Signal Surfer |
| Crimson Death      | Louis Cypher     | Slack Master  |
| Dark Angel         | Lucifer 666      | Slave Driver  |
| Dark Creeper       | Magic Man        | Taran King    |
| Disk Jockey        | Minor Threat     | Tom Brokaw    |
| Dispater           | Mr. Icom         | Video Vance   |
| Doc Holiday        | Mucho Maas       | Voyager       |
| Dr. Cypher         | Mudge            | Weapons       |
| Dr. Williams       | Nat X            | White Knight  |
| Drab Jester        | Night Ranger     | Wind Runner   |
| Drunkfux           | Nihil            |               |
| Emmanuel Goldstein | Norris           |               |

A total of 73 people and they are what made it worth remembering!

#### A Few Things We Learned At SummerCon

~~~~~

By The Pope and Nihil

- Don't try to buy beer at stores that have gas pumps.
- How correctly wear a baseball hat.
- "Playing" cellular phones is illegal.
- All mall security officers are imported from Mississippi.
- The showers at the Executive Internation only have two temperatures: freeze and scald.
- Frosty bought a lifetime supply knee-high tube socks before they went out of style in the 1970's.
- How to pick up underage girls.
- Control C should have chosen the alias "No Control C."
- After being awake for 43 hours (and drinking for 30), OPii's accent disappears.
- Hanging out with Crimson Death and Phantom Phreaker means worrying about being drug tested at work Monday morning.
- Hanging out with Crimson Death, Phantom Phreaker, and Erik Bloodaxe will teach you how to defeat Monday morning's drug test.
- Erik Bloodaxe and The Pope are the Siskel and Ebert of pornographic films.
- Agent Steal has big hair.
- Taran King has perfect hair.
- DO NOT get into a car with Voyager and The Public.

==Phrack Inc.==

Volume Four, Issue Forty, File 12 of 14

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN	
PWN	PWN
PWN	Phrack World News
PWN	PWN
PWN	Issue 40 / Part 1 of 3
PWN	PWN
PWN	Compiled by Datastream Cowboy
PWN	PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN	

By Knight Lightning and The Gatsby
Special Thanks to Bruce Bigelo (San Diego Union-Tribune)

"Multiplexor and The Crypt Keeper Spill Guts"

A lot of stories have been circulating in the press over the past two months about hordes of credit card stealing computer hackers that were disrupting the economy of the United States. It all began with rumors about Multiplexor, a small time hacker that was thought to have spent some time in Long Island, New York and supposedly is from Indiana. The story was that Multiplexor had carded a plane ticket to San Diego to see a girl or meet some friends, but when he landed, he was met by the police instead.

Where that information or the supposed "1,000 member hacker ring" theory came from, we might never know, but we know do know the facts in this case thanks to police reports and warrant affidavits supplied by the court and acquired by The Gatsby with help.

That information and more is now available.

For purposes of understanding the following, "SEMENICK" and "MARCOV" are both the same person. You might know him better under the names of Multiplexor or The Prisoner. Later in this file, you will see references to a person named Kevin Marcus who is better known to some as The Crypt Keeper.

SAN DIEGO POLICE DEPARTMENT Investigators Follow-Up Report

CASE NUMBER: N/A
DATE: March 23, 1992
TIME: 1300 Hours
SUBJECT: Damage Assessment of and Intelligence gathering on Illegal entry (Hacking) Computer Systems and the Illegal use of Credit Cards.
SUSPECT: SEMENICK, John Edward AKA: MARCOV, Eric Edward
VICTIM: Zales Jewelry Store
LOCATION: 4465 La Jolla Village Drive, San Diego, CA
DETECTIVE: Dennis W. Sadler (I.D.# 2486)

On March 31, 1992, I received a ARJIS 4 form from Officer Smyth (I.D.# 3871) regarding some papers found by a Mr. Maurice Osborne at his residence.

Mr. Osborne had asked an individual by the name of Eric MARCOV, who had rented a room from him, to leave. After MARCOV left the house, Mr. Osborne discovered some papers with what appeared to be credit card information on them. Mr. Osborne called the police and reported what he found.

Officer Smyth collected the papers and wrote the attached report. After reviewing these papers, I learned that they did in fact contain some personal information on individuals which included the person's name, address, credit card number, card expiration date, and social security number. It appeared that the person who wrote these notes was possibly using this credit card information illegally.

I contacted Mr. Osborne by phone on March 31st. He verified the contents of the report and he stated that he feels MARCOV may still be in town. On April 2nd, I was contacted by Mr. Osborne who learned that MARCOV was staying at a motel in the beach area named Sleepy Time.

On April 2, 1992, while in the beach area, I came across the Sleepy Time Motel. I contacted the motel manager, William Gainok. I asked Mr. Gainok if he had a person registered there by the name of Eric MARCOV. He said that he did and

that Marcov was in room number 108.

At approximately 8:40 am, I knocked on the door to room number 108. A white male answered the door. I asked him if he was Eric MARCOV. He said yes. I identified myself as a San Diego Police Detective and told him that I needed to talk to him about some questionable credit card activity.

As he opened the motel room door, I saw more papers like <those> given to me by Mr. Osborne laying on the floor near the door with more credit card information on them. After being invited into the motel room, I asked MARCOV if he knew why I was here. He said I think so. I asked MARCOV why he thought so. He said the credit cards.

At this point, I was only interviewing MARCOV regarding the papers found at Mr. Osborne's residence. I had no active case or any evidence indicating that MARCOV was involved in, or a suspect of any criminal or illegal activity.

I asked MARCOV if he had any I.D. on him. He said that he did not. MARCOV gave me the following information; Eric Edward MARCOV, DOB 05-15-74, then changed the year to 73. He said he was 18 going on 19. He did not know his social security number. When asked if he had a drivers' license, he said that he has never had one. MARCOV appeared to be between the age of 17 to 19 years old.

While asking him about papers, he started talking about computers and gaining information from various systems. He talked for about 10 minutes. After that, I decided to call the FBI because hacking was involved in obtaining the credit card information and numbers, plus the information was coming from out of state. MARCOV also sounded like he knew a lot about computer hacking and was involved in it himself.

At 8:58 am, I called the local office of the FBI and told them what I had and asked if they would be interested in talking with MARCOV. I asked MARCOV prior to calling the FBI, if he would be willing to talk with them about his computer activities. He agreed to talk with them.

A short later Special Agent Keith Moses called me back at the motel. I explained to him what I had and what MARCOV was willing to talk about. After going over the case with Moses, he agreed to come out and talk with MARCOV.

Both Moses and I interviewed MARCOV regarding his hacking activities and knowledge. MARCOV was extensively involved in the hacking community during the last four years and had some superior knowledge about what was happening in the hacker world. We later learned that he had been arrested for computer crimes in early 1991 in Indianapolis. We attempted to contact the investigators that worked that case, but we never received any calls back after numerous attempts.

During the interview, I attempted to confirm MARCOV's true identity. I asked him for his parents' information. He said he did not remember their home phone numbers, but they had a phone. He also could not remember their home addresses. I asked him for his parents' employment information. He said that his father worked for a local (his home town) turbine company.

I called the information number for the local phone company and then called the company to verify this information. However, the company's personnel office could not locate any employee matching the name given to me by MARCOV. MARCOV also gave me the school and year he graduated. I called the local school district's administrative office and discovered they had no record of MARCOV attending or graduating from their school system.

I confronted him with this information and he finally gave me his true information. His true name was John Edward SEMENICK, DOB 05-15-75. I located

his father's work number and contacted him. He was very uninterested about his son's whereabouts or condition. When asked if he would supply an airline or bus ticket for transportation home, he said he would not. His father further stated that when his son decided to come home, he'll have to find his own way. SEMENICK's parents are divorced and he lives with his father. However, we learned that his mother had filed a runaway report with the local sheriff's office.

I contacted his mother and she seemed a little more concerned, but said she would not provide a ticket or funds for his return. I asked both parents if while John was in San Diego would they have any problems if their son assisted us in our investigation. I explained to them that he was not facing any known criminal charges at that point and that the information he would be giving us would be for damage assessment and intelligence gathering purposes on hackers

Both parents stated that they had no problem with him assisting us if he was not being charged. Because SEMENICK was a juvenile and a runaway report was filed on him, we contacted the U.S. Attorney's office, the District Attorney's Juvenile Division, and the Juvenile Hall Probation Intake Officer for advice.

They advised us that there was no problem with him giving us information. SEMENICK was booked into Juvenile hall as a runaway and then released to a halfway home for the evening. The intake officer explained to us that because his parents would not send for him, they would only keep him for one evening and then he would be let go on his own again the next day.

After SEMENICK went through the runaway process and was being released, we picked him back up. The FBI agreed and furnished the funds to put SEMENICK up in a hotel, give him living expenses, and then provide transportation for him home. SEMENICK was put up in a suite at the Mission Valley Marriott. He was allowed to do what he wanted while staying at the hotel and to see his friends at any time.

During SEMENICK's stay at the Marriott, either myself or Agent Moses stayed in the hotel room next to SEMENICK's. During the three day stay at the hotel, SEMENICK was able to provide us with some very useful information and intelligence. It was not enough to make any arrest, but we obtained some very valuable information. We were not able to independently verify the information by another source.

During the period of April 3rd to April 5th, 1992, SEMENICK contacted numerous persons by phone who were involved in computer hacking. SEMENICK willingly and voluntarily signed an FBI consent form giving us permission to record his phone calls during the course of our investigation. There were numerous tape recorded phone conversations involving at least 4 separate individuals.

During this same period of time, information in data format was also downloaded from another individual's computer located on the East Coast to the computer we had set up. The information we received during the download was current credit records just obtained from CBI credit reporting company by this person, a CBI manual written in part by "Kludge" a San Diego hacker, and numerous other files/documents involving illegal activity such as "carding." "Carding" is a term used by the hacker community regarding the illegal or fraudulent use of credit cards or credit card numbers by hackers nationwide.

SEMENICK stated that he had been a member of a local BBS called Scantronics when he was an active hacker. He stated that the board is run by a guy named "KLUDGE" and contains hundreds of files and documents. He said that most of these files and documents contained on "KLUDGE's" computer are "how to" manuals. This means that they instruct the person who obtains them through Scantronics BBS on how to do various things both legal and illegal. Some of the illegal activities that are covered on this BBS is carding, phone hacking, ATM fraud, and credit bureau information.

We obtained three documents written by or put out by either "KLUDGE" or Scantronics BBS.

THIS INVESTIGATION IS ONGOING AT THIS TIME AND FURTHER INFORMATION AND EVIDENCE WILL BE ADDED.

SAN DIEGO POLICE DEPARTMENT
Investigators Follow-Up Report

CASE NUMBER: N/A
DATE: April 30, 1992
TIME: 0700 Hours
SUBJECT: Computer Hacking
SUSPECT: N/A
VICTIM: N/A
LOCATION: N/A
DETECTIVE: Dennis W. Sadler (I.D.# 2486)

On April 16, 1992, I was contacted by Kevin Marcus. Marcus learned that we were investigating individuals who were illegally logging (hacking) into various computer systems nationwide. Marcus runs a local computer bulletin board system (BBS) called The Programmer's Paradise. Marcus was concerned about the illegal activities had had seen on various local BBSs and contacted me.

Marcus also said that he had received computer messages from a person who goes by the name (handle) of Knight Lightning in New York who asked him if he heard anything about our investigation. Knight Lightning told Marcus that on April 3rd a reporter from San Diego by the name of Bigelo had contacted and talked to him about our ongoing investigation.

-- -- -- -- --

Enclosure 1:

Date: Fri, 10 Apr 1992 18:14:11 -500
To: knight@eff.org
From: Craig Neidorf <knight@eff.org>
Subject: Runaway Teen Hacker Picked Up?

I was just contacted by a reporter in San Diego about a hacker case.

Apparently there is a teenage hacker from Indiana who ran away from home to California to see some girl there. The local police and the FBI supposedly picked him up on April 3rd and he remains in their custody uncharged while he is telling them all sorts of information on hacker rings across the nation.

Does anyone have any clues as to who this kid is or what's going on?

:Knight Lightning

-- -- -- -- --

Enclosure 2:

Date: Thu, 16 Apr 1992 22:25:17 -0400
From: Craig Neidorf <knight@eff.org>
To: tck@netlink.cts.com
Subject: Re: Hi.

Bruce Bigelo, Union Tribune. Left his number at the office. Nothing going on, but I understand that you called him.

Craig

-- -- -- -- -- -- --

Marcus offered to assist us. I asked if he knew of a BBS called Scantronics. He said that he did and that he had been a member of that BBS and view the files on that board in the past to see what the board carried. Marcus is a computer science major at a local college and is doing research in the anti-virus field. Marcus stated that the board carried a lot of technical data, but had nothing regarding his subject. Marcus also belongs to other local and out-of-state BBSs where he talks with other individuals with his same interest.

Marcus stated that he was last on Scantronics BBS about a month ago and he had seen numerous computer files that involved CBI and carding. Carding is a term used by hackers who are involved in the illegal or fraudulent use of credit cards and their numbers. These credit card numbers are obtained from credit reporting companies such as CBI and TRW, by illegally accessing (hacking) their way into those company computers and reading or copying private individuals credit reports and information.

Most copies of credit reports from these companies will show a person's name, current and previous addresses, social security number, employer, salary, and all current credit history including all credit cards and their account numbers. They <the hackers> then use these credit card numbers to obtain goods.

If one of the hackers used an account number he found on a credit report that he illegally pulled from the credit reporting company, the victim would most likely not find out that their card had been illegally used until the next billing cycle which could be as much as 45 days after the illegal transaction took place. According to the credit card industry, this is one of the most risk free and safest way to commit credit card fraud.

Marcus said that the person's name who ran this BBS was Jeremy. He did not know his last name, but the handle he is known by is "KLUDEGE." I asked if he knew the phone number to this BBS and he gave me 423-4852. The BBS phone number, the operator's first name, and <the operator's> handle matched the information we had learned earlier.

Marcus also gave me two disks <that> contained some files which had been downloaded (left on his BBS) by other persons on his system. He regularly checks his board and removes or deletes files regarding questionable or illegal activity such as carding.

I viewed both of these disks and they contained some very interesting files. These files included various topics <such as> an auto theft manual, CBI manual, TRW manual, American Express card info, and many other files which if downloaded or copied by another person, that person could easily gain illegal access to various credit reporting companies and commit various other illegal types of activity.

I told Marcus if he came across any further information regarding this type of activity or further information about the BBS called Scantronics to please contact me.

On April 17, 1992, I met Marcus and he said that he had logged onto Scantronics last night by using an access number a friend gave him. This same friend had let him use his access number to gain access to this BBS on many prior occasions. He did this on his own, without any direction whatsoever from me or any other law enforcement official.

Marcus handed me a 5 1/4" computer disk and said that it contained some file

listings and a list of all validated users. Marcus also stated that the disk contained a copy of the messages that were sent to him through his BBS by the person in New York regarding our investigation [those messages displayed above from Knight Lightning].

He asked me if I wanted him to log on and see for myself what was on "KLUDGE's" BBS. I told him that I would have to consult with the D.A.'s office first. However, I was unable to get a hold of our D.A. liaison. I told <Marcus> that I'd get back with him later.

After talking to D.A. Mike Carlton, I advised Marcus not to go into Scantronics BBS unless it was for his own information. However he said that if he came across any further information during his normal course of running his own BBS, he would notify me.

-- -- -- -- --

[The police report also contained 60 pages of printouts of postings and text files found on Scantronics BBS. It is also made very clear that Kevin Marcus (aka The Crypt Keeper) accessed Scantronics BBS by using the password and account number of The Gatsby. Files include:

- "Credit Bureau Information" which sounds harmless enough to begin with and turns out is actually a reprint of an article from the September 27, 1992 issue of Business Week Magazine
- "Advanced Carding" by The Disk Jockey, which dates back to 1987.
- "The Complete CBI Manual of Operations" by Video Vindicator and Kludge, dated October 10, 1991.

Aftermath

~~~~~

On April 23, 1992, a search warrant was issued in the municipal court of the State of California in the county of San Diego which authorized the seizure of:

- A. All telephone company subscriber information to include service start date, copy of most current billing statement, current credit information, and location of telephone service to the following telephone numbers; (619)XXX-XXXX and (619)XXX-XXXX and any other telephone number information in any chain of call forwarding, to or from the listed phone numbers.
- B. All telephone company records which includes subscriber information, service start date, copy of most current billing statement, current credit information, and location of telephone service phone numbers to which calls are being forwarded to or from, from the listed phone numbers.

#### CERTIFICATION TO DEFER NOTIFICATION TO SUBSCRIBER

The Court finds there is substantial probable cause to believe notification to the subscriber whose activities are recorded in the records described above would impede or destroy this investigation. Accordingly, the court certifies the request of the San Diego Police Department that notification to the subscriber be deferred pending further order of this court.

On April 30, 1992, a search warrant was issued in the municipal court of the State of California in the county of San Diego which authorized the search of Kludge's residence and the seizure of:

All computer equipment and paraphernalia use in computer hacking, or apart of the BBS known as Scantronics which includes, but is not limited to

monitor(s), keyboard(s), CPU(s), which may or may not contain hard disk drive(s), floppy drive(s), tape drive(s), CD rom drive(s), modem(s), fax/modem(s), all hard copies (paper copies) of any computer files which have been stored or currently stored on/in a computer system, all documents whether in hard or data form which show how to operate any computer program or computer file, all memory storage devices which may include hard disk drive(s), 5 1/4" and 3 1/2" computer memory storage disks, all computer memory storage and computer back up tapes, and all computer CD rom disks capable of computer data storage; and, documents and effects which tend to show dominion and control over said premises and computer system, including fingerprints, records, handwritings, documents and effects which bear a form of identification such as a person's name, photograph, social security number, or driver's license number and keys.

The warrant was used immediately and Scantronics BBS and much more was seized.

-----  
The Crypt Keeper Responds

~~~~~  
Date: Wed, 17 Jun 92 09:13:50 PDT
From: tck@bend.UCSD.EDU (Kevin Marcus)
To: knight@eff.org
Subject: Hmm.

I'll start at the beginning...

On April 3rd, I arrived at my workplace (a computer store) around 3 pm. Multiplexor is sitting in the back with some FBI agent and Detective Dennis Sadler. The reason they chose my store for technical support is because Dennis and one of my managers are very good friends.

I saw what was happening, and I saw Multiplexor call up Kludge's board and try to log on, but alas he was not validated. Nonetheless, that same day I told Gatsby and Kludge what was up, because they are/were my friends and I didn't want something bad to happen to them.

A few days later, my boss suggested that I tell Dennis that I was on Kludge's board awhile ago, but that I was not anymore because they might have found something on me. So the next time I saw him (he comes in about once a week, still), I told him that I was on the board awhile ago, but that I wasn't anymore. He asked a few stupid questions and I didn't really say a whole bunch about.

He eventually found out that I had warned Kludge about his board. I am not really sure how, I sure as heck didn't tell him. He then told me that I nearly blew their investigation and for interfering with an investigation the maximum penalty was like 5 years or something like that. He was getting ready to arrest me and take me down to the county courthouse when my boss was able to convince him that I was a good kid, not looking for trouble, and that I would get him something to re-strengthen. So, even though Dennis didn't tell me specifically to get something from Kludge's board, he told me that what he needed to get his case back up to par was an idea of what was on the board, like a buffering of his system.

That night I called up Gatsby and got his password from him. I called and buffered. The next time that I saw him [Sadler], I told him what I had done. He wanted to know how I got on Kludge's board, and I told him through a friend's account. He asked me which friend, and I said "The Gatsby." He then started asking me a bunch of questions about Gatsby such as, "What is his real name?" And, at first I said that I didn't want to tell him, and then he said that I was withholding evidence and he could bust me on that alone. So I told him his name and that he lived in XXXXX (a suburb of San Diego). They already

had him and Kludge in phone conversations over Kludge's line since it was taped for a while so they knew who he was in the first place.

If Sadler didn't have anything hanging over my head, such as interfering with an investigation, and/or withholding evidence, then I would not have said jack, more than likely. My first contact with him was on suggestion of my boss, who is a good friend of his, and he might have told my boss something which made him worry and think that I would be arrested for something, I do not know.

Now, if I was a nark, then I can assure you that a LOT more people would have gone down. I have a plethora of information on who is who, who is where, who does what, etc. and, even though it's old, I bet a lot of it is true. If I wanted there to be another Operation Sun-Devil, then I would have given all of that information to him. But I didn't, because that is not at all what I had wanted. I didn't want anyone to get busted (including myself) for anything.

If I were a nark, then I would probably have given him a lot more information, wouldn't you think?

I sure do.

I am not asking anyone to forget about it. I know that I screwed up, but there is not a whole bunch about it that I can do right now.

When Sadler was here asking me questions, it didn't pop into my mind that I should tell him to wait and then go and call my attorney, and then a few minutes later come back and tell him whatever my lawyer said. I was scared.

Hackers Aren't The Real Enemy

June 8, 1992

~~~~~

By Chris Goggans (ComputerWorld) (Page 37)

(Goggans is a 23-year old hacker who is currently seeking employment with anyone who won't make him cut his hair.)

For years articles have been published about people who call themselves "hackers." These have been written by people who have investigated hackers, who have been the targets of hackers, who secure systems against hackers and who claim to know hackers. As a member of the so-called "computer underground," I would like to present the hacker's point of view.

I hope you will put aside any personal bias you may have toward people who call themselves hackers because it is probably based on media reports rather than real contact.

I also hope you won't refuse to read this because you have a problem with my ethics. Over the past 11 years, operating under the pseudonym Erik Bloodaxe, I had opportunities to become rich beyond the dreams of avarice and wreak great havoc on the world's computer networks. Yet I have done neither. I have looked behind doors that were marked "employees only" but have never disrupted the operation of business. Voyeurism is a far cry from rape.

Illegal, but not criminal

Undeniably, the actions of some hackers are illegal, but they are still hardly criminal in nature. The intention of most of these individuals is not to destroy or exploit systems but merely to learn in minute detail how they are used and what they are used for. The quest is purely intellectual, but the drive to learn is so overwhelming that any obstacle blocking its course will be circumvented. Unfortunately, the obstacles are usually state and federal laws on unauthorized computer access.

The overwhelming difference between today's hackers and their 1960s MIT namesakes is that many of my contemporaries began their endeavors too young to have ready access to computer systems. Few 13-year-olds find themselves with system privileges on a VAX through normal channels.

My own first system was an Atari 8-bit computer with 16K of memory. I soon realized that the potential of such a machine was extremely limited. With the purchase of a modem, however, I was able to branch out and suddenly found myself backed by state-of-the-art computing power at remote sites across the globe. Often, I was given access by merely talking to administrators about the weak points in their systems, but most often my only access was whatever account I may have stumbled across.

Many people find it hard to understand why anyone would risk prosecution just to explore a computer system. I have asked myself that same question many times and cannot come up with a definitive answer. I do know that it is an addiction so strong that it can, if not balanced with other activities, lead to total obsession. Every hacker I know has spent days without sleep combing the recesses of a computer network, testing utilities and reading files. Many times I have become so involved in a project that I have forgotten to eat.

Hackers share almost no demographic similarities: They are of all income levels, races, colors and religions and come from almost every country. There are some shared characteristics, however. Obsessive-compulsive behavior (drug or alcohol abuse, gambling, shoplifting) is one. Others have a history of divorce in their families, intelligence scores in the gifted to genius level, poor study habits and a distrust of any authority figure. Most hackers also combine inherent paranoia and a flair for the romantic -- which is apparent in the colorful pseudonyms in use throughout the hacker community.

In most cases, however, once hackers reach college age -- or, at minimum, the age of legal employment -- access to the systems they desire is more readily available through traditional means, and the need to break a law to learn is curtailed.

Popular media has contributed greatly to the negative use of the word "hacker." Any person found abusing a long-distance calling card or other credit card is referred to as a hacker. Anyone found to have breached computer security on a system is likewise referred to as a hacker and heralded as a computer whiz, despite the fact that even those with the most basic computer literacy can breach computer security if they put their minds to it.

Although the media would have you believe otherwise, all statistics show that hackers have never been more than a drop in the bucket when it comes to serious computer crime. In fact, hackers are rarely more than a temporary nuisance, if they are discovered at all. The real danger lies in the fact that their methods are easily duplicated by people whose motives are far more sinister. Text files and other information that hackers write on computer systems can be used by any would-be corporate spy to help form his plan of attack on a company.

Given that almost everyone is aware of the existence and capabilities of hackers -- and aware of how others can go through the doors hackers open -- the total lack of security in the world's computers is shocking.

#### Points of entry

The primary problem is poor systems administration. Users are allowed to select easily guessed passwords. Directory permissions are poorly set. Proper process accounting is neglected. Utilities to counter these problems exist for every operating system, yet they are not widely used.

Many systems administrators are not provided with current information to help

them secure their systems. There is a terrible lack of communication between vendors and customers and inside the corporate community as a whole.

Rather than inform everyone of problems when they are discovered, vendors keep information in secret security databases or channel it to a select few through electronic-mail lists. This does little to help the situation, and, in fact, it only makes matters worse because many hackers have access to these databases and to archives of the information sent in these mailing lists.

Another major problem in system security comes from telecommunications equipment. The various Bell operating companies have long been the targets of hackers, and many hackers know how to operate both corporate and central office systems better than the technicians who do so for a living.

Increased use of computer networks has added a whole new dimension of insecurity. If a computer is allowed to communicate with another on the same network, every computer in the link must be impenetrable or the security of all sites is in jeopardy. The most stunning examples of this occur on the Internet. With such a wide variety of problems and so little information available to remedy them, the field of computer security consulting is growing rapidly. Unfortunately, what companies are buying is a false sense of security. The main players seem to be the national accounting firms. Their high-cost audits are most often procedural in nature, however, and are rarely conducted by individuals with enough technical expertise to make recommendations that will have a real and lasting effect.

Ultimately, it is the responsibility of the systems administrators to ensure that they have the proper tools to secure their sites against intrusion. Acquiring the necessary information can be difficult, but if outsiders can get their hands on this information, so can the people who are paid to do the job.

---

## THE GREAT DEBATE

Phiber Optik v. Donn Parker

Cyberpunk Meets Mr. Security

June 1992

~~~~~

By Jonathan Littman (PC Computing Magazine) (Page 288)

The boy cautiously approached the table and asked the tall, distinguished bald gentleman in the gray suit if he could join him. The boy's conference name tag read Phiber Optik; the gentleman's read Donn Parker. One was a member of the Legion of Doom, the infamous sect of teenage hackers charged with fraud, conspiracy, and illegal computer access in 1990; the other was a legendary security expert.

The unlikely pair had been brought together by an unusual gathering, the nation's first Computers, Freedom, and Privacy conference, held in the San Francisco Bay Area on the last weekend of March 1991. They were part of an eclectic mix of G-men, Secret Service agents, prosecutors, privacy advocates, and hackers who had come to see the other side up close.

Only weeks before, Optik's laptop computer had been seized by state police in an investigation begun by the Secret Service. Optik and fellow hackers Acid Phreak and Scorpion were among the first to come under the scrutiny of the Secret Service in the days of Operation Sun Devil, a 14-city sweep in the spring of 1990 that resulted in 42 seized computers, 23,000 confiscated disks, and four arrests.

The criminal charges brought against Optik and his cohort included illegal computer access and trading in stolen access codes. Optik, a juvenile at the time of his initial questioning, spent a day in jail and was later convicted of

a misdemeanor for theft of services.

Parker knew the story well. Over the last two decades, the former Lutheran Sunday school teacher has interviewed dozens of criminals to whom computers were simply the tools of the trade. Along the way, he earned a worldwide reputation as the bald eagle of computer crime. Parker speaks frequently to law-enforcement agencies and corporations as a consultant to SRI International, a leading research and management firm based in Menlo Park, California. His books *Fighting Computer Crime* and *Crime by Computer*, countless articles, and a large Justice Department study on computer ethics have established him as the foremost authority on the hacker psyche.

PARKER: How do you view the ethics of getting into someone's computer system?

OPTIK: I know what your point of view is because I've read your papers and I've listened to you talk. I know that you think any entry, you know, any unauthorized entry, is criminal.

I can't say I agree with that. I do agree that anyone who's an impressionable teenager, who's on the scene and wants to break into as many computers as is humanly possible to prove a point, has the potential to do damage, because they're juveniles and have no idea what they're doing, and they're messing around in places that they have no business being.

At the time, I was 17 years old and still a minor. There was no way I was going to be able to buy a Unix, a VAX, my own switching system. These are the things I'm interested in learning how to program. It would not have been possible to access this type of computer development environment had I not learned how to break into systems. That's the way I see it.

PARKER: What are you doing at this conference? What's your purpose?

OPTIK: Basically I want to be exposed to as many people as possible and hear as many people's views as I can.

PARKER: What's your ultimate purpose then-what would you like to do as far as a career? Do you think this is a way for you to get into a career?

OPTIK: Well, of course, I hope to enter the computer industry. Just by being here, I hope to talk to people like you, the many people who are professionals in the field, hear their views, have them hear my views.

See, the thing I regret the most is that there is this communication gap, a lack of dialogue between people who proclaim themselves to be hackers and people who are computer professionals. I think if there were a better dialogue among the more respectable type of hackers and the computer professionals, then it would be a lot more productive.

PARKER: How do you tell the difference between a more responsible type of hacker?

OPTIK: I realize that it's a very big problem. I can see that it's pretty impossible to tell, and I can clearly understand how you come to the conclusions that you initially state in your paper about how hackers have been known to cheat, lie, and exaggerate. I experienced that firsthand all the time. I mean, these people are generally like that. Just keep in mind that a large number of them aren't really hardcore hackers -- they're impressionable teenagers hanging out. It's just that the medium they're using to hang out is computers.

I don't consider myself part of that crowd at all. I got into

computers early on. Like when I was entering junior high school. I was really young, it must have been preteen years. I'm talking about 12 or 13 years old when I got a computer for Christmas.

I didn't immediately go online. I'm not one of these kids today that get a Commodore 64 with a modem for Christmas because they got good grades on their report card. The reason I would have called myself a hacker is, I was hacking in the sense of exploring the world inside my computer, as far as assembly language, machine language, electronics tinkering, and things of that nature. That truly interested me.

The whole social online thing I could really do without because that's where these ideas come from. You know, this whole negative, this bad aftertaste I get in my mouth when I hear people put down the whole hacking scene. It's because of what they're hearing, and the reason they're hearing this is because of the more outspoken people in this "computer underground" and the twisted coverage in the media, which is using this whole big hype to sell papers.

And the people who are paying the price for it are people like me; and the people who are getting a twisted view of things are the professionals, because they're only hearing the most vocal people. It's another reason why I'm here, to represent people like myself, who want other people to know there are such things as respectable hackers. You know hacking goes beyond impressionable young teenage delinquents.

PARKER: How would you define hacking?

OPTIK: It's this overall wanting to understand technology, to be able to communicate with a machine on a very low level, to be able to program it. Like when I come upon a computer, it's like my brain wants to talk to its microprocessor. That's basically my philosophy.

PARKER. And does it matter to you who actually owns the computer?

OPTIK: Usually it does. Oh, at first it didn't matter. The mere fact of getting into Unix, and learning Unix, was important enough to warrant me wanting to be on the system. Not because of information that was in there. I really don't care what the information is.

You know there's that whole Cyberpunk genre that believes information should be free. I believe in computer privacy wholly. I mean if someone wants something to be private, by all means let it be private. I mean, information is not meant for everyone to see if you design it as being private. That's why there is such a thing as security.

If someone wants to keep something private, I'm not going to try to read it. It doesn't interest me. I couldn't care less what people are saying to each other on electronic mail. I'm there because I'm interested in the hardware.

PARKER: How is anyone else going to know that you're not interested in reading their private mail?

OPTIK: That's a problem I have to deal with. There's not a real solution in the same way that there's no way that you're really going to be able to tell whether someone's malicious or not. Hackers do brag, cheat, and exaggerate. They might tell you one thing and then stab you in the back and say something else.

PARKER: I've interviewed over 120 so-called computer criminals.

OPTIK: Right.

PARKER: I've interviewed a lot of hackers, and I've also interviewed a lot of people engaged in all kinds of white-collar crime.

OPTIK: Yeah.

PARKER: And it seems to me that the people I have talked with that have been convicted of malicious hacking and have overcome and outgrown that whole thing have gone into legitimate systems programming jobs where there is great challenge, and they're very successful. They are not engaged in malicious hacking or criminal activity, and they're making a career for themselves in technology that they love.

OPTIK: Right.

PARKER: Why couldn't you go that route? Why couldn't you get your credentials by going to school like I did and like everybody else did who functions as a professional in the computer field, and get a challenging job in computer technology?

OPTIK: I certainly hope to get a challenging job in computer technology. But I just feel that where I live, and the way the school system is where I am, it doesn't cater to my needs of wanting to learn as much about technology as fast as I want to learn.

PARKER: Yeah, but one of the things you have to learn, I guess, is patience, and you have to be willing to work hard and learn the technology as it's presented.

OPTIK: You know, you just have to remember that by being able to go places that people shouldn't, I'm able to learn things about technology that schools don't teach. It's just that programs in local colleges where I am, they couldn't even begin to grasp things that I've experienced.

PARKER: OK, so you want instant gratification then.

OPTIK: It's not so much gratification . . .

PARKER: You're not willing to spend four years in a--

OPTIK: I certainly am willing to go to college.

PARKER: Uh huh.

OPTIK: I definitely intend to go to college; I just don't expect to learn very much concerning technology. I do expect to learn some things about technology I probably didn't know, but I don't expect to be exposed to such a diverse amount of technology as in my teenage years.

PARKER: OK, well, I can see impatience and a lack of opportunity to do all that stuff very quickly, but--

OPTIK: I wouldn't go so far as to call it impatience. I'd call it an eagerness to learn.

PARKER: Eagerness to learn can be applied in the establishment process of education in all kinds of ways. You can excel in school.

OPTIK: I was never Mr. Academia, I can tell you that right off the bat. I don't find much of interest in school. Usually I make up for it by reading technology manuals instead.

PARKER: How are you going to spend four years in school if you've already

decided you're really not suited to be in school?

OPTIK: Well, it's not so much school as it is that I feel constrained being in high school and having to go through junior high school and high school because of the way the educational program are tailored to like, you know --

PARKER: Well, if you hold this direction that you're going right now, you could very well end up as a technician repairing equipment, maintaining computers, and you could very well end up in a dead-end job.

In order to break into a higher level of work, you need a ticket, you need a degree, you have to prove that you have been able to go to school and get acceptable grades. The route that you're going doesn't seem to me to lead to that.

Now there are some people who have managed to overcome that, OK -- Geoff Goodfellow. Steve Wozniak. But those people are 1 out of 100,000. All the other 99,000-odd people are technicians. They're leading reasonable lives, making a reasonable income, but they're not doing very big things. They're keeping equipment running.

OPTIK: Yeah.

PARKER: And if you have all this curiosity and all this drive and this energy (which is what it takes), and you go a route that gets you to a position where you can do real, exciting, advanced research . . . I mean, I've talked to a lot of hackers. I'm thinking of one in Washington, D.C., who was convicted of a computer crime. He went back to school, he's got his degree, and he has a very top systems programming job. He said he finally reached a point where he decided he had to change the way he was going about this, because the way things were going, the future for him was pretty bleak.

And it seems to me, hopefully, you may come to a realization that to do important things, exciting things, ultimately you've got to learn the computer-science way of presenting operating systems, and how to write programs of a very large, complex nature.

Have you ever done that, have you ever written a really big computer program?

OPTIK: I've written this . . .

PARKER: There's a discipline involved that has to do with learning how to be an engineer. It takes a tremendous amount of education and discipline. And it sounds to me like you lack the discipline. You want instant gratification, you want to be an expert now. And you end up being an expert all right, but in a very narrow range of technology.

You learn the Novell LAN, you learn some other aspect, you learn about a telephone company's switching system. That doesn't lead to a career in designing and developing systems. That leads to a career in maintaining the kind of hardware that you've been hacking.

And it seems to me you've got to go back and learn the principles. What are the basic principles of an operating system? What are the basic principles of access control? Until you've gone back and learned those basics, you're flying by the seat of your pants, and just picking up odds and ends of stuff that you can grab quickly.

OPTIK: I don't see it so much as grabbing things quickly. I've put a lot of time into studying very detailed things. It's not so much popping in

and popping out and whatever I find I'm glad I found it. I do spend a lot of time studying manuals and things.

PARKER: Manuals are not going to do it. All you do in learning a manual is learn the current equipment and how it works. If you studied Donald Kanuth's volumes on computer science programming and computer sciences, you would learn the theory of computer programming, you would learn the operating system theory, you would learn the theory that is the foundation on which all of these systems are built.

OPTIK: But that's the thing I guess I don't do. I was never much concerned with theory of operation. I was always concerned with how things work, and how I can use them. Like how to program. I'll admit I was never much into theory. It never interested me. Like with what I do-theory really doesn't play any role at the present time. Of course, that's subject to change at any time. I'm rather young . . .

A FRIEND WHISPERED in Optik's ear that it was time to go. Still locked in debate, the hacker and the security man left the table and walked together toward the escalator. In profile, at the bottom of the moving stairs, they were an odd couple: Optik with his shiny, jet black hair, Parker with his shiny dome.

Parker was speaking calmly, warning Optik that one day hacking wouldn't seem so boundless, that one day his opportunities wouldn't seem quite so vast. Optik fidgeted, glancing away. Conference attendees filed up the escalator.

"I don't want to be a hacker forever," blurted Optik.

The next afternoon the bank of hotel phones was crowded with business people and conference attendees punching in to get their messages and make their calls. There was Optik, wedged between the suits, acoustic coupler slipped over the phone receiver, a laptop screen flickering before his eyes, his hands flitting over the keys.

He was still young.

==Phrack Inc.==

Volume Four, Issue Forty, File 13 of 14

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN	
PWN	PWN
PWN	Phrack World News
PWN	PWN
PWN	Issue 40 / Part 2 of 3
PWN	PWN
PWN	Compiled by Datastream Cowboy
PWN	PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN	

MOD Indicted

July 8, 1992

~~~~~

Taken from U.S. Newswire

The following is the press release issued by the United States Attorney's Office in the Southern District of New York.

Group of "Computer Hackers" Indicted  
First Use of Wiretaps in Such a Case

NEW YORK -- A group of five "computer hackers" has been indicted on charges of

computer tampering, computer fraud, wire fraud, illegal wiretapping, and conspiracy, by a federal grand jury in Manhattan, resulting from the first investigative use of court-authorized wiretaps to obtain conversations and data transmissions of computer hackers.

A computer hacker is someone who uses a computer or a telephone to obtain unauthorized access to other computers.

The indictment, which was filed today, alleges that Julio Fernandez, a/k/a "Outlaw," John Lee, a/k/a "Corrupt," Mark Abene, a/k/a "Phiber Optik," Elias Ladopoulos, a/k/a "Acid Phreak," and Paul Stira, a/k/a "Scorpion," infiltrated a wide variety of computer systems, including systems operated by telephone companies, credit reporting services, and educational institutions.

According to Otto G. Obermaier, United States Attorney for the Southern District of New York, James E. Heavey, special agent in charge, New York Field Division, United States Secret Service, William Y. Doran, special agent in charge, Criminal Division, New York Field Division, Federal Bureau of Investigation, and Scott Charney, chief of the Computer Crime Unit of the Department of Justice, the indictment charges that the defendants were part of a closely knit group of computer hackers self-styled "MOD," an acronym used variously for "Masters of Disaster" and "Masters of Deception" among other things.

The indictment alleges that the defendants broke into computers "to enhance their image and prestige among other computer hackers; to harass and intimidate rival hackers and other people they did not like; to obtain telephone, credit, information and other services without paying for them; and to obtain passwords, account numbers and other things of value which they could sell to others."

The defendants are also alleged to have used unauthorized passwords and billing codes to make long distance telephone calls and to be able to communicate with other computers for free.

Some of the computers that the defendants allegedly broke into were telephone switching computers operated by Southwestern Bell, New York Telephone, Pacific Bell, U.S. West and Martin Marietta Electronics Information and Missile Group. According to the indictment, such switching computers each control telephone service for tens of thousands of telephone lines.

In some instances, the defendants allegedly tampered with the computers by adding and altering calling features. In some cases, the defendants allegedly call forwarded local numbers to long distance numbers and thereby obtained long distance services for the price of a local call. Southwestern Bell is alleged to have incurred losses of approximately \$370,000 in 1991 as a result of computer tampering by defendants Fernandez, Lee, and Abene.

The indictment also alleges that the defendants gained access to computers operated by BT North America, a company that operates the Tymnet data transfer network. The defendants were allegedly able to use their access to Tymnet computers to intercept data communications while being transmitted through the network, including computer passwords of Tymnet employees. On one occasion, Fernandez and Lee allegedly intercepted data communications on a network operated by the Bank of America.

The charges also allege that the defendants gained access to credit and information services including TRW, Trans Union and Information America. The defendants allegedly were able to obtain personal information on people including credit reports, telephone numbers, addresses, neighbor listings and social security numbers by virtue of their access to these services. On one occasion Lee and another member of the group are alleged to have discussed obtaining information from another hacker that would allow them to alter credit

reports on TRW. As quoted in the indictment, Lee said that the information he wanted would permit them "to destroy people's lives... or make them look like saints."

The indictment further charges that in November 1991, Fernandez and Lee sold information to Morton Rosenfeld concerning how to access credit services. The indictment further alleges that Fernandez later provided Rosenfeld's associates with a TRW account number and password that Rosenfeld and his associates used to obtain approximately 176 TRW credit reports on various individuals. (In a separate but related court action, Rosenfeld pleaded guilty to conspiracy to use and traffic in account numbers of TRW. See below).

According to Stephen Fishbein, the assistant United States attorney in charge of the prosecution, the indictment also alleges that members of MOD wiped out almost all of the information contained within the Learning Link computer operated by the Educational Broadcasting Corp. (WNET Channel 13) in New York City. The Learning Link computer provided educational and instructional information to hundreds of schools and teachers in New York, New Jersey and Connecticut. Specifically, the indictment charges that on November 28, 1989, the information on the Learning Link was destroyed and a message was left on the computer that said: "Happy Thanksgiving you turkeys, from all of us at MOD" and which was signed with the aliases "Acid Phreak," "Phiber Optik," and "Scorpion." During an NBC News broadcast on November 14, 1990, two computer hackers identified only by the aliases "Acid Phreak" and "Phiber Optik" took responsibility for sending the "Happy Thanksgiving" message.

Obermaier stated that the charges filed today resulted from a joint investigation by the United States Secret Service and the Federal Bureau of Investigation. "This is the first federal investigation ever to use court-authorized wiretaps to obtain conversations and data transmissions of computer hackers," said Obermaier. He praised both the Secret Service and the FBI for their extensive efforts in this case. Obermaier also thanked the Department of Justice Computer Crime Unit for their important assistance in the investigation. Additionally, Obermaier thanked the companies and institutions whose computer systems were affected by the defendants' activities, all of whom cooperated fully in the investigation.

Fernandez, age 18, resides at 3448 Steenwick Avenue, Bronx, New York. Lee (also known as John Farrington), age 21, resides at 64A Kosciusko Street, Brooklyn, New York. Abene, age 20, resides at 94-42 Alstytne Avenue, Queens, New York. Elias Ladopoulos, age 22, resides at 85-21 159th Street, Queens, New York. Paul Stira, age 22, resides at 114-90 227th Street, Queens, New York. The defendants' arraignment has been scheduled for July 16, at 10 AM in Manhattan federal court.

The charges contained in the indictment are accusations only and the defendants are presumed innocent unless and until proven guilty. Fishbein stated that if convicted, each of the defendants may be sentenced to a maximum of five years imprisonment on the conspiracy count. Each of the additional counts also carries a maximum of five years imprisonment, except for the count charging Fernandez with possession of access devices, which carries a maximum of ten years imprisonment. Additionally, each of the counts carries a maximum fine of the greater of \$250,000, or twice the gross gain or loss incurred.

-----

In separate but related court actions, it was announced that Rosenfeld and Alfredo De La Fe [aka Renegade Hacker] have each pleaded guilty in Manhattan Federal District Court to conspiracy to use and to traffic in unauthorized access devices in connection with activities that also involved members of MOD.

Rosenfeld pled guilty on June 24 before Shirley Wohl Kram, United States District Judge. At his guilty plea, Rosenfeld admitted that he purchased

account numbers and passwords for TRW and other credit reporting services from computer hackers and then used the information to obtain credit reports, credit card numbers, social security numbers and other personal information which he sold to private investigators. Rosenfeld added in his guilty plea that on or about November 25, 1991, he purchased information from persons named "Julio" and "John" concerning how to obtain unauthorized access to credit services. Rosenfeld stated that he and his associates later obtained additional information from "Julio" which they used to pull numerous credit reports. According to the information to which Rosenfeld pleaded guilty, he had approximately 176 TRW credit reports at his residence on December 6, 1991.

De La Fe pled guilty on June 19 before Kenneth Conboy, United States District Judge. At his guilty plea, De La Fe stated that he used and sold telephone numbers and codes for Private Branch Exchanges ("PBXs"). According to the information to which De La Fe pleaded guilty, a PBX is a privately operated computerized telephone system that routes calls, handles billing, and in some cases permits persons calling into the PBX to obtain outdial services by entering a code. De La Fe admitted that he sold PBX numbers belonging to Bugle Boy Industries and others to a co-conspirator who used the numbers in a call sell operation, in which the co-conspirator charged others to make long distance telephone calls using the PBX numbers. De La Fe further admitted that he and his associates used the PBX numbers to obtain free long distance services for themselves. De La Fe said that one of the people with whom he frequently made free long distance conference calls was a person named John Farrington, who he also knew as "Corrupt."

Rosenfeld, age 21, resides at 2161 Bedford Avenue, Brooklyn, N.Y. Alfredo De La Fe, age 18, resides at 17 West 90th Street, N.Y. Rosenfeld and De La Fe each face maximum sentences of five years, imprisonment and maximum fines of the greater of \$250,000, or twice the gross gain or loss incurred. Both defendants have been released pending sentence on \$20,000 appearance bonds. Rosenfeld's sentencing is scheduled for September 9, before Shirley Wohl Kram. De La Fe's sentencing is scheduled for August 31, before Conboy.

-----

#### Contacts:

Federico E. Virella Jr., 212-791-1955, U.S. Attorney's Office, S. N.Y.  
Stephen Fishbein, 212-791-1978, U.S. Attorney's Office, S. N.Y.  
Betty Conkling, 212-466-4400, U.S. Secret Service  
Joseph Valiquette Jr., 212-335-2715, Federal Bureau of Investigation

Editor's Note: The full 23 page indictment can be found in Computer Underground Digest (CUD), issue 4.31 (available at [ftp.eff.org/pub/cud/cud](ftp://ftp.eff.org/pub/cud/cud)).

---

EFF Issues Statement On New York Computer Crime Indictments

July 9, 1992

~~~~~  
Cambridge, MA -- The Electronic Frontier Foundation (EFF) issued a statement concerning the indictment of MOD for alleged computer-related crimes.

This statement said, in part, that EFF's "staff counsel in Cambridge, Mike Godwin is carefully reviewing the indictment."

EFF co-founder and president Mitchell Kapor said "EFF's position on unauthorized access to computer systems is, and has always been, that it is wrong. Nevertheless, we have on previous occasions discovered that allegations contained in Federal indictments can also be wrong, and that civil liberties can be easily infringed in the information age. Because of this, we will be examining this case closely to establish the facts."

When asked how long the complete trial process might take, assistant U.S. attorney Fishbein said "I really couldn't make an accurate estimate. The length of time period before trial is generally more a function of the defense's actions than the prosecution's. It could take anywhere from six months to a year.

Feds Tap Into Major Hacker Ring

July 13, 1992

~~~~~

By Mary E. Thyfault (InformationWeek) (Page 15)

Law enforcement officials are taking the gloves off-and plugging their modems in-in the battle against computer crime.

In one of the largest such cases ever, a federal grand jury in Manhattan indicted five computer "hackers" -- part of a group that calls itself MOD, for Masters of Deception -- on charges of computer tampering, computer fraud, wire fraud, illegal wiretapping, and conspiracy.

Some of the hackers are accused of stealing phone service and selling information on how to obtain credit reports. The victims (a dozen were named in the indictments, but numerous others are likely to have been hit as well) include three Baby Bells, numerous credit bureaus, and BankAmerica Corp.

For the first time, investigators used court-authorized wiretaps to monitor data transmissions over phone lines. The wiretapping comes as the FBI is unsuccessfully lobbying Congress to mandate that telecom equipment and service companies build into new technology easier ways for securities agencies to tap into computer systems.

Ironically, the success of this wiretap, some say, may undermine the FBI's argument. "They did this without the equipment they claim they need," says Craig Neidorf, founder of hacker newsletter Phrack.

If convicted, the alleged hackers-all of whom are under 22 years old-could face 55 years each and a fine of \$250,000, or twice the gross gain or loss incurred. One charged with possessing an access device could face an additional five years.

The vulnerability of the victims' networks should be surprising, but experts say corporations continue to pay scant attention to security issues. For instance, despite the fact that the credit bureaus are frequent targets of hackers and claim to have made their networks more secure, in this case, most of the victims didn't even know they were being hit, according to the FBI.

Two of the victims, value-added network service provider BT Tymnet and telco Southwestern Bell, both take credit for helping nab the hacker ring. "We played an instrumental role in first recognizing that they were there," says John Guinasso, director of global network security for Tymnet parent BT North America. "If you mess with our network and we catch you -- which we always do -- you will go down."

---

Second Thoughts On New York Computer Crime Indictments

July 13, 1992

~~~~~

By John F. McMullen (Newsbytes)

NEW YORK -- On Wednesday, July 9th, I sat at a press briefing in New York City's Federal Court Building during which law enforcement officials presented details relating to the indictment of 5 young computer "hackers". In describing the alleged transgressions of the indicted, United States Assistant Attorney Stephen Fishbein wove a tale of a conspiracy in which members of an evil sounding group called the "Masters of Destruction" (MOD) attempted to

wreck havoc with the telecommunications system of the country.

The accused were charged with infiltrating computer systems belonging to telephone companies, credit bureaus, colleges and defense contractors -- Southwestern Bell, BT North America, New York Telephone, ITT, Information America, TRW, Trans Union, Pacific Bell, the University of Washington, New York University, U.S. West, Learning Link, Tymnet and Martin Marietta Electronics Information and Missile Group. They were charged with causing injury to the telephone systems, charging long distance calls to the universities, copying private credit information and selling it to third parties -- a long list of heinous activities.

The immediate reaction to the indictments were predictably knee-jerk. Those who support any so-called "hacker"-activities mocked the government and the charges that were presented, forgetting, it seems to me, that these charges are serious -- one of the accused could face up to 40 years in prison and \$2 million in fines; another -- 35 years in prison and \$1.5 million in fines. In view of that possibility, it further seems to me that it is a wasteful diversion of effort to get all excited that the government insists on misusing the word "hacker" (The indictment defines computer hacker as "someone who uses a computer or a telephone to obtain unauthorized access to other computers.") or that the government used wiretapping evidence to obtain the indictment (I think that, for at least the time being that the wiretapping was carried out under a valid court order; if it were not, the defendants' attorneys will have a course of action).

On the other hand, those who traditionally take the government and corporate line were publicly grateful that this threat to our communications life had been removed -- they do not in my judgement properly consider that some of these charges may have been ill-conceived and a result of political considerations.

Both groups, I think, oversimplify and do not give proper consideration to the wide spectrum of issues raised by the indictment document. The issues range from a simple black-and-white case of fraudulently obtaining free telephone time to the much broader question of the appropriate interaction of technology and law enforcement.

The most clear cut cases are the charges such as the ones which allege that two of the indicted, Julio Fernandez a/k/a "Outlaw" and John Lee a/k/a "Corrupt" fraudulently used the computers of New York University to avoid paying long distance charges for calls to computer systems in El Paso, Texas and Seattle, Washington. The individuals named either did or did not commit the acts alleged and, if it is proven that they did, they should receive the appropriate penalty (it may be argued that the 5 year, \$250,000 fine maximum for each of the counts in this area is excessive, but that is a sentencing issue not an indictment issue).

Other charges of this black-and-white are those that allege that Fernandez and/or Lee intercepted electronic communications over networks belonging to Tymnet and the Bank of America. Similarly, the charge that Fernandez, on December 4, 1991 possessed hundreds of user id's and passwords of Southwestern Bell, BT North America and TRW fits in the category of "either he did it or he didn't."

A more troubling count is the charge that the indicted 5 were all part of a conspiracy to "gain access to and control of computer systems in order to enhance their image and prestige among other computer hackers; to harass and intimidate rival hackers and people they did not like; to obtain telephone, credit, information, and other services without paying for them; and to obtain passwords, account numbers and other things of value which they could sell to others."

To support this allegation, the indictment lists 26, lettered A through Z, "Overt Acts" to support the conspiracy. While this section of the indictment lists numerous telephone calls between some of the individuals, it mentions the name Paul Stira a/k/a "Scorpion" only twice with both allegations dated "on or about" January 24, 1990, a full 16 months before the next chronological incident. Additionally, Stira is never mentioned as joining in any of the wiretapped conversation -- in fact, he is never mentioned again! I find it hard to believe that he could be considered, from these charges, to have engaged in a criminal conspiracy with any of the other defendants.

Additionally, some of the allegations made under the conspiracy count seem disproportionate to some of the others. Mark Abene a/k/a "Phiber Optik" is of possessing proprietary technical manuals belonging to BT North America while it is charged that Lee and Fernandez, in exchange for several hundred dollars, provided both information on how to illegally access credit reporting bureaus and an actual TRW account and password to a person, Morton Rosenfeld, who later illegally accessed TRW, obtained credit reports on 176 individuals and sold the reports to private detective (Rosenfeld, indicted separately, pled guilty to obtaining and selling the credit reports and named "Julio" and "John" as those who provided him with the information). I did not see anywhere in the charges any indication that Abene, Stira or Elias Ladopoulos conspired with or likewise encouraged Lee or Fernandez to sell information involving the credit bureaus to a third party

Another troubling point is the allegation that Fernandez, Lee, Abene and "others whom they aided and abetted" performed various computer activities "that caused losses to Southwestern Bell of approximately \$370,000." The \$370,000 figure, according to Assistant United States Attorney Stephen Fishbein, was developed by Southwestern Bell and is based on "expenses to locate and replace computer programs and other information that had been modified or otherwise corrupted, expenses to determine the source of the unauthorized intrusions, and expenses for new computers and security devices that were necessary to prevent continued unauthorized access by the defendants and others whom they aided and abetted."

While there is precedent in assigning damages for such things as "expenses for new computers and security devices that were necessary to prevent continued unauthorized access by the defendants and others whom they aided and abetted." (the Riggs, Darden & Grant case in Atlanta found that the defendants were liable for such expenses), many feel that such action is totally wrong. If a person is found uninvited in someone's house, they are appropriately charged with unlawful entry, trespassing, burglary -- whatever the statute is for the transgression; he or she is, however, not charged with the cost of the installation of an alarm system or enhanced locks to insure that no other person unlawfully enters the house.

When I discussed this point with a New York MIS manager, prone to take a strong anti-intruder position, he said that an outbreak of new crimes often results in the use of new technological devices such as the nationwide installation of metal detectors in airports in the 1970's. While he meant this as a justification for liability, the analogy seems rather to support the contrary position. Air line hijackers were prosecuted for all sorts of major crimes; they were, however, never made to pay for the installation of the metal detectors or absorb the salary of the additional air marshalls hired to combat hijacking.

I think the airline analogy also brings out the point that one may both support justifiable penalties for proven crimes and oppose unreasonable ones -- too often, when discussing these issues, observers choose one valid position to the unnecessary exclusion of another valid one. There is nothing contradictory, in my view, to holding both that credit agencies must be required to provide the highest possible level of security for data they have collected AND that persons invading the credit data bases, no matter how secure they are, be held

liable for their intrusions. We are long past accepting the rationale that the intruders "are showing how insecure these repositories of our information are." We all know that the lack of security is scandalous; this fact, however, does not excuse criminal behavior (and it should seem evident that the selling of electronic burglar tools so that someone may copy and sell credit reports is not a public service).

The final point that requires serious scrutiny is the use of the indictment as a tool in the on-going political debate over the FBI Digital Telephony proposal. Announcing the indictments, Otto G. Obermaier, United States Attorney for the Southern District of New York, said that this investigation was "the first investigative use of court-authorized wiretaps to obtain conversations and data transmissions of computer hackers." He said that this procedure was essential to the investigation and that "It demonstrates, I think, the federal government's ability to deal with criminal conduct as it moves into new technological areas." He added that the interception of data was possible only because the material was in analog form and added "Most of the new technology is in digital form and there is a pending statute in Congress which seeks the support of telecommunications companies to allow the federal government, under court authorization, to intercept digital transmission. Many of you may have read the newspaper about the laser transmission which go through fiber optics as a method of the coming telecommunications method. The federal government needs the help of Congress and, indeed, the telecommunications companies to able to intercept digital communications."

The FBI proposal has been strongly attacked by the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF) and Computer Professionals for Social Responsibility (CPSR) as an attempt to institutionalize, for the first time, criminal investigations as a responsibility of the communications companies; a responsibility that they feel belongs solely to law-enforcement. Critics further claim that the proposal will impede the development of technology and cause developers to have to "dumb-down" their technologies to include the requested interception facilities. The FBI, on the other hand, maintains that the request is simply an attempt to maintain its present capabilities in the face of advancing technology.

Whatever the merits of the FBI position, it seems that the indictments either would not have been made at this time or, at a minimum, would not have been done with such fanfare if it were not for the desire to attempt to drum up support for the pending legislation. The press conference was the biggest thing of this type since the May 1990 "Operation Sun Devil" press conference in Phoenix, Arizona and, while that conference, wowed us with charges of "hackers" endangering lives by disrupting hospital procedures and being engaged in a nationwide, 13 state conspiracy, this one told us about a bunch of New York kids supposedly engaged in petty theft, using university computers without authorization and performing a number of other acts referred to by Obermaier as "anti-social behavior" -- not quite as heady stuff!

It is not to belittle these charges -- they are quite serious -- to question the fanfare. The conference was attended by a variety of high level Justice Department, FBI and Secret Service personnel and veteran New York City crime reporters tell me that the amount of alleged damages in this case would normally not call for such a production -- New York Daily News reporter Alex Michelini publicly told Obermaier "What you've outlined, basically, except for the sales of credit information, this sounds like a big prank, most of it" (Obermaier's response -- "Well, I suppose you can characterize that as a prank, but it's really a federal crime allowing people without authorization to rummage through the data of other people to which they do not have access and, as I point out to you again, the burglar cannot be your safety expert. He may be inside and laugh at you when you come home and say that your lock is not particularly good but I think you, if you were affected by that contact, would

be somewhat miffed"). One hopes that it is only the fanfare surrounding the indictments that is tied in with the FBI initiative and not the indictments themselves.

As an aside, two law enforcement people that I have spoken to have said that while the statement that the case is "the first investigative use of court-authorized wiretaps to obtain conversations and data transmissions of computer hackers," while probably true, seems to give the impression that the case is the first one in which data transmission was intercepted. According to these sources, that is far from the case -- there have been many instances of inception of data and fax information by law enforcement officials in recent years.

I know each of the accused in varying degrees. The one that I know the best, Phiber Optik, has participated in panels with myself and law enforcement officials discussing issues relating to so-called "hacker" crime. He has also appeared on various radio and television shows discussing the same issues. His high profile activities have made him an annoyance to some in law enforcement. One hopes that this annoyance played no part in the indictment.

I have found Phiber's presence extremely valuable in these discussions both for the content and for the fact that his very presence attracts an audience that might never otherwise get to hear the voices of Donald Delaney, Mike Godwin, Dorothy Denning and others addressing these issues from quite different vantage points. While he has, in these appearances, said that he has "taken chances to learn things", he has always denied that he has engaged in vandalous behavior and criticized those who do. He has also called those who engage in "carding" and the like as criminals (These statements have been made not only in the panel discussion, but also on the occasions that he has guest lectured to my class in "Connectivity" at the New School For Social Research in New York City. In those classes, he has discussed the history of telephone communications in a way that has held a class of professionals enthralled by over two hours.

While my impressions of Phiber or any of the others are certainly not a guarantee of innocence on these charges, they should be taken as my personal statement that we are not dealing with a ring of hardened criminals that one would fear on a dark night.

In summary, knee-jerk reactions should be out and thoughtful analysis in! We should be insisting on appropriate punishment for lawbreakers -- this means neither winking at "exploration" nor allowing inordinate punishment. We should be insisting that companies that have collected data about us properly protect -- and are liable for penalties when they do not. We should not be deflected from this analysis by support or opposition to the FBI proposal before Congress -- that requires separate analysis and has nothing to do with the guilt or innocence of these young men or the appropriate punishment should any guilt be established.

New York Hackers Plead Not Guilty

July 17, 1992

~~~~~  
New York City -- At an arraignment in New York Federal Court on Thursday, July 16th, the five New York "hackers," recently indicted on charges relating to alleged computer intrusion, all entered pleas of not guilty and were released after each signed a personal recognizance (PRB) bond of \$15,000 to guarantee continued appearances in court.

As part of the arraignment process, United States District Judge Richard Owen was assigned as the case's presiding judge and a pre-trial meeting between the judge and the parties involved.

Charles Ross, attorney for John Lee, told Newsbytes "John Lee entered a not guilty plea and we intend to energetically and aggressively defend against the

charges made against him."

Ross also explained the procedures that will be in effect in the case, saying "We will meet with the judge and he will set a schedule for discovery and the filing of motions. The defense will have to review the evidence that the government has amassed before it can file intelligent motions and the first meeting is simply a scheduling one."

Majorie Pearce, attorney for Stira, told Newsbytes "Mr. Stira has pleaded not guilty and will continue to plead not guilty. I am sorry to see the government indict a 22 year old college student for acts that he allegedly committed as a 19 year old."

The terms of the PRB signed by the accused require them to remain within the continental United States. In requesting the bond arrangement, Assistant United States Attorney Stephen Fishbein referred to the allegations as serious and requested the \$15,000 bond with the stipulation that the accused have their bonds co-signed by parents. Abene, Fernandez and Lee, through their attorneys, agreed to the bond as stipulated while the attorneys for Ladopoulos and Stira requested no bail or bond for their clients, citing the fact that their clients have been available, when requested by authorities, for over a year. After consideration by the judge, the same \$15,000 bond was set for Ladopoulos and Stira but no co-signature was required.

---

Young Working-Class Hackers Accused of High-Tech Crime

July 23, 1992

~~~~~

By Mary B.W. Tabor with Anthony Ramirez (The New York Times) (Page B1, B7)

Computer Savvy, With an Attitude

Late into the night, in working-class neighborhoods around New York City, young men with code names like Acid Phreak and Outlaw sat hunched before their glowing computer screens, exchanging electronic keys to complex data-processing systems. They called themselves the Masters of Deception. Their mission: to prove their prowess in the shadowy computer underworld.

Compulsive and competitive, they played out a cybernetic version of "West Side Story," trading boasts, tapping into telephone systems, even pulling up confidential credit reports to prove their derring-do and taunt other hackers. Their frequent target was the Legion of Doom, a hacker group named after a gang of comic-book villains. The rivalry seemed to take on class and ethnic overtones, too, as the diverse New York group defied the traditional image of the young suburban computer whiz.

But Federal prosecutors say the members of MOD, as the group called itself, went far beyond harmless pranks.

Facing Federal Charges

On July 16, five young men identified by prosecutors as MOD members pleaded not guilty to Federal charges including breaking into some of the nation's most powerful computers and stealing confidential data like credit reports, some of which were later sold to private investigators. Prosecutors call it one of the most extensive thefts of computer information ever reported.

The indictment says the men entered the computer systems of Southwestern Bell, TRW Information Services and others "to enhance their image and prestige among other computer hackers; to harass and intimidate rival hackers and other people they did not like; to obtain telephone, credit, information and other services without paying for them; and to obtain passwords, account numbers and other things of value which they could sell to others."

With modems that link their terminals to other computers over ordinary telephone lines, young hackers have been making mischief for years. But as the nation relies more and more on vast networks of powerful computers and as personal computers become faster and cheaper, the potential for trouble has soared. For example, Robert Tappan Morris, a Cornell student, unleashed a program in 1988 that jammed several thousand computers across the country.

A Polyglot Group

But the world of computer hackers has been changing. Unlike the typical hackers of old -- well-to-do suburban youths whose parents could afford costly equipment -- the Masters of Deception are a polyglot representation of blue-collar New York: black, Hispanic, Greek, Lithuanian and Italian. They work their mischief often using the least expensive computers.

One of the young men, 21-year-old John Lee, who goes by the name Corrupt, has dreadlocks chopped back into stubby "twists," and lives with his mother in a dilapidated walk-up in Bedford-Stuyvesant, Brooklyn. He bounced around programs for gifted students before dropping out of school in the 11th grade. Scorpion -- 22-year-old Paul Stira of Queens -- was his class valedictorian at Thomas A. Edison High School in Queens. Outlaw -- Julio Fernandez, 18, of the Bronx -- first studied computers in grade school.

They met not on street corners, but via computer bulletin boards used to swap messages and programs.

With nothing to identify them on the boards except their nicknames and uncanny abilities, the young men found the computer the great democratic leveler.

Questions of Profit

There may be another difference in the new wave of hackers. While the traditional hacker ethic forbids cruising computer systems for profit, some new hackers are less idealistic. "People who say that," said one former hacker, a friend of the MOD who insisted on anonymity, "must have rich parents. When you get something of value, you've got to make money."

Mr. Lee, Mr. Fernandez, Mr. Stira and two others described as MOD members -- 20-year-old Mark Abene (Phiber Optik), and 22-year-old Elias Ladopoulos (Acid Phreak), both of Queens -- were charged with crimes including computer tampering, computer and wire fraud, illegal wiretapping and conspiracy. They face huge fines and up to five years in prison on each of 11 counts.

The youths, on advice of their lawyers, declined to be interviewed.

Prosecutors say they do not know just how and when youthful pranks turned to serious crime. Other hackers said the trouble began, perhaps innocently enough, as a computer war with ethnic and class overtones.

The Masters of Deception were born in a conflict with the Legion of Doom, which had been formed by 1984 and ultimately included among its ranks three Texans, one of whom, Kenyon Shulman, is the son of a Houston socialite, Carolyn Farb.

Banished From the Legion

Mr. Abene had been voted into the Legion at one point. But when he began to annoy others in the group with his New York braggadocio and refusal to share information, he was banished, Legion members said.

Meanwhile, a hacker using a computer party line based in Texas had insulted Mr. Lee, who is black, with a racial epithet.

By 1989, both New Yorkers had turned to a new group, MOD, founded by Mr.

Ladopoulos. They vowed to replace their Legion rivals as the "new elite."

"It's like every other 18- or 19-year-old who walks around knowing he can do something better than anyone else can," said Michael Godwin, who knows several of the accused and is a lawyer for the Electronic Frontier Foundation of Cambridge, Massachusetts, which provides legal aid for hackers. "They are offensively arrogant."

Hacker groups tend to rise and fall within six months or so as members leave for college, meet girls or, as one former hacker put it, "get a life." But the MOD continued to gather new members from monthly meetings in the atrium of the Citicorp Building in Manhattan and a computer bulletin board called Kaos. According to a history the group kept on the computer network, they enjoyed "mischievous pranks," often aimed at their Texas rivals, and the two groups began sparring.

Texas-New York Sparring

But in June 1990, the three Texas-based Legion members, including Mr. Shulman, Chris Goggans and Scott Chasin, formed Comsec Data Security, a business intended to help companies prevent break-ins by other hackers.

Worried that the Texans were acting as police informers, the MOD members accused their rivals of defaming them on the network bulletin boards. Several members, including Mr. Abene, had become targets of raids by the Secret Service, and MOD members believed the Texans were responsible, a contention the Texans respond to with "no comment."

But the sparring took on racial overtones as well. When Mr. Lee wrote a history of the MOD and left it in the network, Mr. Goggans rewrote it in a jive parody.

The text that read, "In the early part of 1987, there were numerous amounts of busts in the U.S. and in New York in particular" became "In de early time part uh 1987, dere wuz numerous amounts uh busts in de U.S. and in New Yo'k in particular."

Mr. Goggans said that it was not meant as a racist attack on Mr. Lee. "It was just a good way to get under his skin," he said.

Exposing Identities

MOD's activities, according to the indictment and other hackers, began to proliferate.

Unlike most of the "old generation" of hackers who liked to joyride through the systems, the New Yorkers began using the file information to harass and intimidate others, according to prosecutors. Everything from home addresses to credit card numbers to places of employment to hackers' real names -- perhaps the biggest taboo of all -- hit the network.

In the indictment, Mr. Lee and Mr. Fernandez are accused of having a conversation last fall in which they talked about getting information on how to alter TRW credit reports to "destroy people's lives or make them look like saints."

The prosecutors say the youths also went after information they could sell, though the indictment is not specific about what, if anything, was sold. The only such information comes from another case earlier this month in which two other New York City hackers, Morton Rosenfeld, 21, of Brooklyn, and Alfredo de la Fe, 18, of Manhattan, pleaded guilty to a conspiracy to use passwords and other access devices obtained from MOD. They said they had paid "several hundred dollars" to the computer group for passwords to obtain credit reports

and then resold the information for "several thousand dollars" to private investigators.

News Media Attention

Competition for attention from the news media also heated up. The former Legion members in Comsec had become media darlings, with articles about them appearing in Time and Newsweek. Mr. Abene and Mr. Ladopoulos also appeared on television or in magazines, proclaiming their right to probe computer systems, as long as they did no damage.

In one highly publicized incident, during a 1989 forum on computers and privacy sponsored by Harper's magazine, John Perry Barlow, a freelance journalist and lyricist for the Grateful Dead, went head to head with Mr. Abene, or Phiber Optik. Mr. Barlow called the young hacker a "punk."

According to an article by Mr. Barlow -- an account that Mr. Abene will not confirm or deny -- Mr. Abene then retaliated by "downloading" Mr. Barlow's credit history, displaying it on the computer screens of Mr. Barlow and other network users.

Skirmishes Subside

"I've been in redneck bars wearing shoulder-length curls, police custody while on acid, and Harlem after midnight, but no one has ever put the spook in me quite as Phiber Optik did at that moment," Mr. Barlow wrote. "To a middle-class American, one's credit rating has become nearly identical to his freedom."

In recent months, hackers say, the war has calmed down. Comsec went out of business, and several Masters of Deception were left without computers after the Secret Service raids.

Mr. Abene pleaded guilty last year to misdemeanor charges resulting from the raids. On the night before his arrest this month, he gave a guest lecture on computers at the New School for Social Research.

Mr. Lee says he works part time as a stand-up comic and is enrolled at Brooklyn College studying film production.

Mr. Stira is three credits shy of a degree in computer science at Polytechnic University in Brooklyn. Mr. Fernandez hopes to enroll this fall in the Technical Computer Institute in Manhattan. Mr. Ladopoulos is studying at Queens Community College.

No trial date has been set.

But the battles are apparently not over yet. A couple of days after the charges were handed up, one Legion member said, he received a message on his computer from Mr. Abene. It was sarcastic as usual, he said, and it closed, "Kissy, kissy."

[Editor's Note: Article included photographs of Phiber Optik, Scorpion, Corrupt, and Outlaw.]

Frustrated Hackers May Have Helped Feds In MOD Sting

July 20, 1992

~~~~~

By James Daly (ComputerWorld) (Page 6)

NEW YORK -- Are hackers beginning to police themselves? The five men recently charged with cracking into scores of complex computer systems during the last two years may have been fingered by other hackers who had grown weary of the

group's penchant for destruction and vindictiveness, members of the hacker community said.

The arrest of the defendants, whom federal law enforcement officials claimed were members of a confederation variously called the "Masters of Deception" and the "Masters of Disaster" (MOD), was cause for celebration in some quarters where the group is known as a spiteful fringe element.

"Some of these guys were a big pain," said one source who requested anonymity for fear that unindicted MOD members would plot revenge. "They used their skills to harass others, which is not what hacking is all about. MOD came with a 'you will respect us' attitude, and no one liked it."

Said another: "In the past few months, there has been a lot of muttering on the [bulletin] boards about these guys."

In one episode, MOD members reportedly arranged for the modem of a computer at the University of Louisville in Kentucky to continually dial the home number of a hacker bulletin board member who refused to grant them greater access privileges. A similar threat was heard in Maryland.

In the indictment, the defendants are accused of carrying on a conversation in early November 1991 in which they sought instructions on how to add and remove credit delinquency reports "to destroy people's lives . . . or make them look like a saint." Unlike many other hacker organizations, the members of MOD agreed to share important computer information only among themselves and not with other hackers.

Officials Mum

Who exactly helped the FBI, Secret Service and U.S. Attorney General's Office prepare a case against the group is still anyone's guess. Assistant U.S. Attorney Stephen Fishbein is not saying. He confirmed that the investigation into the MOD began in 1990, but he would not elaborate on how or why it was launched or who participated. FBI and Secret Service officials were equally mute.

Some observers said that if the charges are true, the men were not true "hackers" at all.

"Hacking is something done in the spirit of creative playfulness, and people who break into computer security systems aren't hackers -- they're criminals," said Richard Stallman, president of the Cambridge, Massachusetts-based Free Software Foundation, a public charity that develops free software. The foundation had several files on one computer deleted by a hacker who some claimed belonged to the MOD.

The MOD hackers are charged with breaking into computer systems at several regional telephone companies, Fortune 500 firms including Martin Marietta Corp., universities and credit-reporting concerns such as TRW, Inc., which reportedly had 176 consumer credit reports stolen and sold to private investigators. The 11-count indictment accuses the defendants of computer fraud, computer tampering, wire fraud, illegal wiretapping and conspiracy.

But some hackers said the charges are like trying to killing ants with a sledgehammer. "These guys may have acted idiotically, but this was a stupid way to get back at them," said Emmanuel Goldstein, editor of 2600, a quarterly magazine for the hacker community based in Middle Island, New York.

Longtime hackers said the MOD wanted to move into the vacuum left when the Legion of Doom began to disintegrate in late 1989 and early 1990 after a series of arrests in Atlanta and Texas. Federal law enforcement officials have

described the Legion of Doom as a group of about 15 computer enthusiasts whose members re-routed calls, stole and altered data and disrupted telephone services.

==Phrack Inc.==

Volume Four, Issue Forty, File 14 of 14

|     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN | PWN |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |
| PWN |     |     |     |     |     |     |     |     |     |     |     | PWN |     |

Bellcore Threatens 2600 Magazine With Legal Action July 15, 1992

~~~~~  
THE FOLLOWING CERTIFIED LETTER HAS BEEN RECEIVED BY 2600 MAGAZINE. WE WELCOME ANY COMMENTS AND/OR INTERPRETATIONS.

Leonard Charles Suchyta
General Attorney
Intellectual Property Matters

Emanuel [sic] Golstein [sic], Editor
2600 Magazine
P.O. Box 752
Middle Island, New York 11953-0752

Dear Mr. Golstein:

It has come to our attention that you have somehow obtained and published in the 1991-1992 Winter edition of 2600 Magazine portions of certain Bellcore proprietary internal documents.

This letter is to formally advise you that, if at any time in the future you (or your magazine) come into possession of, publish, or otherwise disclose any Bellcore information or documentation which either (i) you have any reason to believe is proprietary to Bellcore or has not been made publicly available by Bellcore or (ii) is marked "proprietary," "confidential," "restricted," or with any other legend denoting Bellcore's proprietary interest therein, Bellcore will vigorously pursue all legal remedies available to it including, but not limited to, injunctive relief and monetary damages, against you, your magazine, and its sources.

We trust that you fully understand Bellcore's position on this matter.

Sincerely,

LCS/sms

LCS/CORR/JUN92/golstein.619

Emmanuel Goldstein Responds
~~~~~



Major security hole in telephone network creates "self-serve" monitoring feature allowing anyone to listen in on any telephone conversation they choose. Weakness involves feature called Busy Line Verification (BLV), which allows phone companies to "break into" conversation at any time. BLV is used most often by operators entering conversation to inform callers of emergency message. But BLV feature can be used by anyone with knowledge of network's weakness to set up ad hoc 'wiretap' and monitor conversations, said Emmanuel Goldstein, editor of 2600 Magazine, which published article in its Winter 1991 issue.

2600 Magazine is noted for finding and exposing weaknesses of telecommunications. It's named for frequency of whistle, at one time given away with Cap'n Crunch cereal, which one notorious hacker discovered could, when blown into telephone receiver, allow access to open 800 line. Phone companies have since solved that problem.

Security risks are outlined in article titled "U.S. Phone Companies Face Built-In Privacy Hole" that quotes from internal Bellcore memo and Bell Operating Co. documents: "'A significant and sophisticated vulnerability' exists that could affect the security and privacy of BLV." Article details how, after following 4 steps, any line is susceptible to secret monitoring. One document obtained by 2600 said: "There is no proof the hacker community knows about the vulnerability."

When Bellcore learned of article, it sent magazine harsh letter threatening legal action. Letter said that if at any time in future magazine "comes into possession of, publishes, or otherwise discloses any Bellcore information" organization will "vigorously pursue all legal remedies available to it including, but not limited to, injunctive and monetary damages." Leonard Suchyta, Bellcore General Attorney for Intellectual Property Matters, said documents in magazine's possession "are proprietary" and constitute "a trade secret" belonging to Bellcore and its members -- RBOCs. He said documents are "marked with 'Proprietary' legend" and "the law says you can't ignore this legend, its [Bellcore's] property." Suchyta said Bellcore waited so long to respond to publication because "I think the article, as we are not subscribers, was brought to our attention by a 3rd party." He said this is first time he was aware that magazine had published such Bellcore information.

But Goldstein said in reply letter to Bellcore: "This is not the first time we have done this. It will not be the last." He said he thinks Bellcore is trying to intimidate him, "but they've come up against the wrong publication this time." Goldstein insisted that documents were leaked to his magazine: "While we don't spread the documents around, we will report on what's contained within." Suchyta said magazine is obligated to abide by legend stamped on documents. He said case law shows that the right to publish information hinges on whether it "has been lawfully acquired. If it has a legend on it, it's sort of hard to say it's lawfully acquired."

Goldstein said he was just making public what already was known: There's known privacy risk because of BLV weakness: "If we find something out, our first instinct is to tell people about it. We don't keep things secret." He said information about security weaknesses in phone network "concerns everybody." Just because Bellcore doesn't want everyone to know about its shortcomings and those of telephone network is hardly reason to stifle that information, Goldstein said. "Everybody should know if their phone calls can be listened in on."

Suchyta said that to be considered "valuable," information "need not be of super, super value," like proprietary software program "where you spent millions of dollars" to develop it. He said information "could well be your own information that would give somebody an advantage or give them some added value they wouldn't otherwise have had if they had not taken it from you." Goldstein said he was "sympathetic" to Bellcore's concerns but "fact is, even

when such weaknesses are exposed, [phone companies] don't do anything about them." He cited recent indictments in New York where computer hackers were manipulating telephone, exploiting weaknesses his magazine had profiled long ago. "Is there any security at all [on the network]?" he said. "That's the question we have to ask ourselves."

Letter from Bellcore drew burst of responses from computer community when Goldstein posted it to electronic computer conference. Lawyers specializing in computer law responded, weighing in on side of magazine. Attorney Lance Rose said: "There is no free-floating 'secrecy' right . . . Even if a document says 'confidential' that does not mean it was disclosed to you with an understanding of confidentiality -- which is the all-important question." Michael Godwin, general counsel for Electronic Frontier Foundation, advocacy group for the computer community, said: "Trade secrets can qualify as property, but only if they're truly trade secrets. Proprietary information can (sort of) qualify as property if there's a breach of a fiduciary duty." Both lawyers agreed that magazine was well within its rights in publishing information. "If Emmanuel did not participate in any way in encouraging or aiding in the removal of the document from Bellcore . . . that suggests he wouldn't be liable," Godwin said.

-----  
Bellcore And 2600 Dispute Publishing Of Article

July 27, 1992

~~~~~

By Barbara E. McMullen & John F. McMullen (Newsbytes)

MIDDLE ISLAND, NY -- Eric Corley a/k/a "Emmanuel Goldstein", editor and publisher of 2600 Magazine: The Hacker Quarterly, has told Newsbytes that he will not be deterred by threats from Bellcore from publishing material which he considers important for his readership.

Earlier this month, Corley received a letter (addressed to "Emanuel Golstein") from Leonard Charles Suchyta, General Attorney, Intellectual Property Matters at Bellcore taking issue with the publication by 2600 of material that Suchyta referred to as "portions of certain Bellcore proprietary internal documents."

The letter continued "This letter is to formally advise you that, if at any time in the future you (or your magazine) come into possession of, publish, or otherwise disclose any Bellcore information or documentation which either (i) you have any reason to believe is proprietary to Bellcore or has not been made publicly available by Bellcore or (ii) is marked "proprietary," "confidential," "restricted," or with any other legend denoting Bellcore's proprietary interest therein, Bellcore will vigorously pursue all legal remedies available to it including, but not limited to, injunctive relief and monetary damages, against you, your magazine, and its sources."

While the letter did not mention any specific material published by 2600, Corley told Newsbytes that he believes that Suchyta's letter refers to an article entitled "U.S. Phone Companies Face Built-In Privacy Hole".that appears on page 42 of the Winter 1991 issue. Corley said "What we published was derived from a 1991 internal Bellcore memo as well as Bell Operating Company documents that were leaked to us. We did not publish the documents. However, we did read what was sent to us and wrote an article based upon that. The story focuses on how the phone companies are in an uproar over a 'significant and sophisticated vulnerability' that could result in BLV (busy line verification) being used to listen in on phone calls."

The 650-word article said, in part, "By exploiting a weakness, it's possible to remotely listen in on phone conversations at a selected telephone number. While the phone companies can do this any time they want, this recently discovered self-serve monitoring feature has created a telco crisis of sorts."

The article further explained how people might exploit the security hole,

saying "The intruder can listen in on phone calls by following these four steps:

- "1. Query the switch to determine the Routing Class Code assigned to the BLV trunk group.
- "2. Find a vacant telephone number served by that switch.
- "3. Via recent change, assign the Routing Class Code of the BLV trunks to the Chart Column value of the DN (directory number) of the vacant telephone number.
- "4. Add call forwarding to the vacant telephone number (Remote Call Forwarding would allow remote definition of the target telephone number while Call Forwarding Fixed would only allow the specification of one target per recent change message or vacant line)."

"By calling the vacant phone number, the intruder would get routed to the BLV trunk group and would then be connected on a "no-test vertical" to the target phone line in a bridged connection."

The article added "According to one of the documents, there is no proof that the hacker community knows about the vulnerability. The authors did express great concern over the publication of an article entitled 'Central Office Operations - The End Office Environment' which appeared in the electronic newsletter Legion of Doom/Hackers Technical Journal. In this article, reference is made to the 'No Test Trunk'."

The article concludes "even if hackers are denied access to this "feature", BLV networks will still have the capability of being used to monitor phone lines. Who will be monitored and who will be listening are two forever unanswered questions."

Corley responded to Suchyta's letter on July 20th, saying "I assume that you're referring to our revelation of built-in privacy holes in the telephone infrastructure which appeared on Page 42. In that piece, we quoted from an internal Bellcore memo as well as Bell Operating Company documents. This is not the first time we have done this. It will not be the last.

"We recognize that it must be troubling to you when a journal like ours publishes potentially embarrassing information of the sort described above. But as journalists, we have a certain obligation that cannot be cast aside every time a large and powerful entity gets annoyed. That obligation compels us to report the facts as we know them to our readers, who have a keen interest in this subject matter. If, as is often the case, documents, memoranda, and/or bits of information in other forms are leaked to us, we have every right to report on the contents therein. If you find fault with this logic, your argument lies not with us, but with the general concept of a free press.

"And, as a lawyer specializing in intellectual property law, you know that you cannot in good faith claim that merely stamping "proprietary" or "secret" on a document establishes that document as a trade secret or as proprietary information. In the absence of a specific explanation to the contrary, we must assume that information about the publicly supported telephone system and infrastructure is of public importance, and that Bellcore will have difficulty establishing in court that any information in our magazine can benefit Bellcore's competitors, if indeed Bellcore has any competitors.

"If in fact you choose to challenge our First Amendment rights to disseminate important information about the telephone infrastructure, we will be compelled to respond by seeking all legal remedies against you, which may include sanctions provided for in Federal and state statutes and rules of civil procedure. We will also be compelled to publicize your use of lawsuits and the threat of legal action to harass and intimidate.

Sincerely,

Emmanuel Goldstein"

Corley told Newsbytes "Bellcore would never have attempted this with the New York Times. They think that it would, however, be easy to shut us up by simple threats because of our size. They are wrong. We are responsible journalists; we know the rules and we abide by them. I will, by the way, send copies of the article in question to anyone who request it. Readers may then judge for themselves whether any boundaries have been crossed."

Corley, who hosts the weekly "Off the Hook" show on New York City's WBAI radio station, said that he had discussed the issue on the air and had received universal support from his callers. Corley also told Newsbytes, that, although he prefers to be known by his nomme de plume (taken from George Orwell's 1984), he understands that the press feels bound to use his actual name. He said that, in the near future, he will "end the confusion by having my name legally changed."

Bellcore personnel were unavailable for comment on any possible response to Corley's letter.

Interview With Ice Man And Maniac

July 22, 1992

~~~~~

By Joshua Quittner (New York Newsday) (Page 83)

Ice Man and Maniac are two underground hackers in the New England area that belong to a group known as Micro Pirates, Incorporated. They agreed to be interviewed if their actual identities were not revealed.

[Editor's Note: They are fools for doing this, especially in light of how Phiber Optik's public media statements and remarks will ultimately be used against him.]

Q: How do you define computer hacking?

Maniac: Hacking is not exploration of computer systems. It's more of an undermining of security. That's how I see it.

Q: How many people are in your group, Micro Pirates Incorporated?

Ice Man: Fifteen or 14.

Maniac: We stand for similar interests. It's an escape, you know. If I'm not doing well in school, I sit down on the board and talk to some guy in West Germany, trade new codes of their latest conquest. Escape. Forget about the real world.

Ice Man. It's more of a hobby. Why do it? You can't exactly stop. I came about a year-and-a-half ago, and I guess you could say I'm one of the ones on a lower rung, like in knowledge. I do all the -- you wouldn't call it dirty work -- phone calls. I called you -- that kind of thing.

Q: You're a "social engineer"?

Ice Man: Social engineering -- I don't know who coined the term. It's using conversation to exchange information under false pretenses. For example, posing as a telecommunications employee to gain more knowledge and insight into the different [phone network] systems.

Q: What social engineering have you done?

Maniac: We hacked into the system that keeps all the grades for the public



school system. It's the educational mainframe at Kingsborough Community College. But we didn't change anything.

Ice Man: They have the mainframe that stores all the schedules, Regents scores, ID numbers of all the students in the New York high school area. You have to log in as a school, and the password changes every week.

Q: How did you get the password?

Ice Man: Brute force and social engineering. I was doing some social engineering in school. I was playing the naive person with an administrator, asking all these questions toward what is it, where is it and how do you get in.

Q: I bet you looked at your grades. How did you do?

Ice Man: High 80s.

Q. And you could have changed Regents scores?

Ice Man: I probably wouldn't have gotten away with it, and I wouldn't say I chose not to on a moral basis. I'd rather say on a security basis.

Q: What is another kind of social engineering?

Maniac: There's credit-card fraud and calling-card fraud. You call up and say, "I'm from the AT&T Corporation. We're having trouble with your calling-card account. Could you please reiterate to us your four-digit PIN number?" People, being kind of God-fearing -- as AT&T is somewhat a God -- will say, "Here's my four-digit PIN number."

Q: Hackers from another group, MOD, were arrested recently and charged with, among other things, selling inside information about how to penetrate credit bureaus. Have you cleaned up your act?

Maniac: We understand the dangers of it now. We're not as into it. We understand what people go through when they find out a few thousand dollars have been charged to their credit-card account.

Q: Have you hacked into credit bureaus?

Ice Man: We were going to look up your name.

Maniac: CBI [Credit Bureau International, owned by Equifax, one of the largest national credit bureaus], is pretty insecure, to tell you the truth.

Q: Are you software pirates, too?

Maniac: Originally. Way back when.

Ice Man: And then we branched out and into the hacking area. Software piracy is, in the computer underground, the biggest thing. There are groups like THG and INC, which are international. THG is The Humble Guys. INC is International Network of Crackers, and I've recently found out that it's run by 14 and 15-year-olds. They have people who work in companies, and they'll take the software and they'll crack it -- the software protection -- and then distribute it.

Q: Are there many hacking groups in New York?

Maniac: Three or four. LOD [the Legion of Doom, named by hacker Lex Luthor], MOD, MPI and MOB [Men of Business].

Q: How do your members communicate?

Ice Man: The communication of choice is definitely the modem [to access underground electronic bulletin boards where members leave messages for each other or "chat" in real time]. After that is the voice mail box [VMB]. VMBs are for communications between groups.

A company, usually the same company that has beepers and pagers and answering services, has a voice-mail-box service. You call up [after hacking out an access code that gives the user the ability to create new voice mail boxes on a system] and can enter in a VMB number. Occasionally they have outdial capabilities that allow you to call anywhere in the world. I call about five every day. It's not really my thing.

Q: Is your group racially integrated?

Ice Man: Half of them are Asian. Also we have, I think, one Hispanic. I never met him. Race, religion -- nobody cares. The only thing that would alienate you in any way would be if you were known as a lamer. If you just took, took, took and didn't contribute to the underground. It's how good you are, how you're respected.

Maniac: We don't work on a racial basis or an ethnic basis. We work on a business basis. This is an organized hobby. You do these things for us and you get a little recognition for it.

Ice Man: Yeah. If you're a member of our group and you need a high-speed modem, we'll give you one, on a loan basis.

Q: How does somebody join MPI?

Maniac: They have to contact either of us on the boards.

Ice Man: And I'll go through the whole thing [with them], validating them, checking their references, asking them questions, so we know what they're talking about. And if it's okay, then we let them in. We have members in 516, 718, 212, 201, 408, and 908. We're talking to someone in Florida, but he's not a member yet.

Q: Are any MPI members in other hacking groups?

Ice Man: I know of no member of MPI that is in any other group. I wouldn't call it betrayal, but it's like being in two secret clubs at one time. I would want them faithful to my group, not any other group. There is something called merging, a combination of both groups that made them bigger and better. A lot of piracy groups did that.

Q: Aren't you concerned about breaking the law?

Maniac: Breaking the law? I haven't gotten caught. If I do get caught, I won't be stupid and say I was exploring -- I'm not exploring. I'm visiting, basically. If you get caught, you got to serve your time. I'm not going to fight it.

---

FBI Unit Helps Take A Byte Out Of Crime

July 15, 1992

~~~~~

By Bill Gertz (The Washington Times) (Page A4)

FBI crime busters are targeting elusive computer criminals who travel the world by keyboard, telephone and computer screen and use such code names as "Phiber Optik," "Masters of Disaster," "Acid Phreak" and "Scorpion."

"Law enforcement across the board recognizes that this is a serious emerging crime problem, and it's only going to continue to grow in the future," said Charles L. Owens, chief of the FBI's economic crimes unit.

Last week in New York, federal authorities unsealed an indictment against five computer hackers, ages 18 to 22, who were charged with stealing long-distance phone service and credit bureau information and who penetrated a wide variety of computer networks.

The FBI is focusing its investigations on major intrusions into banking and government computers and when the objective is stealing money, Mr. Owens said in an interview.

FBI investigations of computer crimes have doubled in the past year, he said, adding that only about 11 percent to 15 percent of computer crimes are reported to law enforcement agencies. Because of business or personal reasons, victims often are reluctant to come forward, he said.

Currently, FBI agents are working on more than 120 cases, including at least one involving a foreign intelligence agency. Mr. Owens said half of the active cases involve hackers operating overseas, but he declined to elaborate.

The FBI has set up an eight-member unit in its Washington field office devoted exclusively to solving computer crimes.

The special team, which includes computer scientists, electrical engineers and experienced computer system operators, first handled the tip that led to the indictment of the five hackers in New York, according to agent James C. Settle, who directs the unit.

Computer criminals, often equipped with relatively unsophisticated Commodore 64 or Apple II computers, first crack into international telephone switching networks to make free telephone calls anywhere in the world, Mr. Settle said.

Hackers then can spend up to 16 hours a day, seven days a week, breaking into national and international computer networks such as the academic-oriented Internet, the National Aeronautics and Space Administration's Span-Net and the Pentagon's Milnet.

To prevent being detected, unauthorized computer users "loop and weave" through computer networks at various locations in the process of getting information.

"A lot of it is clearly for curiosity, the challenge of breaking into systems," Mr. Settle said. "The problem is that they can take control of the system."

Also, said Mr. Owens, computer hackers who steal such information from commercial data banks may turn to extortion as a way to make money.

Mr. Settle said there are also "indications" that computer criminals are getting involved in industrial espionage.

The five hackers indicted in New York on conspiracy, computer-fraud, computer tampering, and wire-fraud charges called themselves "MOD," for Masters of Deception or Masters of Disaster.

The hackers were identified in court papers as Julio Fernandez, 18, John Lee, 21, Mark Abene, 20, Elias Ladopoulos, 22, and Paul Stira, 22. All live in the New York City area.

Mr. Fernandez and Mr. Lee intercepted data communications from a computer network operated by the Bank of America, court papers said.

They also penetrated a computer network of the Martin Marietta Electronics Information and Missile Group, according to the court documents.

The hackers obtained personal information stored in credit bureau computers, with the intention of altering it "to destroy people's lives or make them look like saints," the indictment stated.

And Today's Password Is...

May 26, 1992

~~~~~

By Robert Matthews (The Daily Telegraph) (page 26)

### "Ways Of Keeping Out The Determined Hacker"

One of the late Nobel Prize-winning physicist Richard Feynman's favorite stories was how he broke into top-secret atomic bomb files at Los Alamos by guessing that the lock combination was 271828, the first six digits of the mathematical constant "e". Apart from being amusing, Feynman's anecdote stands as a warning to anyone who uses dates, names or common words for their computer password.

As Professor Peter Denning, of George Mason University, Virginia, points out in American Scientist, for all but the most trivial secrets, such passwords simply aren't good enough. Passwords date back to 1960, and the advent of time-sharing systems that allowed lots of users access to files stored on a central computer. It was not long before the standard tricks for illicitly obtaining passwords emerged: Using Feynman-style educated guessing, standing behind computer users while they typed in their password or trying common system passwords like "guest" or "root". The biggest security nightmare is, however, the theft of the user-password file, which is used by the central computer to check any password typed in.

By the mid-1970s, ways of tackling this had been developed. Using so-called "one-way functions", each password was encrypted in a way that cannot be unscrambled. The password file then contains only apparently meaningless symbols, of no obvious use to the would-be hacker. But, as Denning warns, even this can be beaten if passwords are chosen sloppily. Instead of trying to unscramble the file, hackers can simply feed common names and dates -- or even the entire English dictionary -- through the one-way function to see if the end result matches anything on the scrambled password file. Far from being a theoretical risk, this technique was used during the notorious Project Equalizer case in 1987, when KGB-backed hackers in Hanover broke the passwords of Unix-based computers in America.

Ultimately, the only way to solve the password problem is to free people of their fear of forgetting more complex ones. The long-term solution, says Denning, probably lies with the use of smart-card technology. One option is a card which generates different passwords once a minute, using a formula based on the time given by an internal clock. The user then logs on using this password. Only if the computer confirms that the password corresponds to the log-on time is the user allowed to continue. Another smart-card technique is the "challenge-response" protocol. Users first log on to their computer under their name, and are then "challenged" by a number appearing on the screen. Keying this into their smart card, a "response number" is generated by a formula unique to each smart card. If this number corresponds to the response expected from a particular user's smart card, the computer allows access. A number of companies are already marketing smart-card systems, although the technology has yet to become popular.

In the meantime, Denning says that avoiding passwords based on English words would boost security. He highlights one simple technique for producing non-standard words that are nonetheless easy to remember: "Pass-phrases". For this, one merely invents a nonsensical phrase like "Martin says Unix gives gold

forever", and uses the first letter of each word to generate the password: MSUGGF. Such a password will defeat hackers, even if the password file is stolen, as it does not appear in any dictionary. However, Denning is wary of giving any guarantees. One day, he cautions, someone may draw up a computerized dictionary of common phrases. "The method will probably be good for a year or two, until someone who likes to compile these dictionaries starts to attack it."

---

Outgunned "Computer Cops" Track High-Tech Criminals

June 8, 1992

~~~~~  
By Tony Rogers (Associated Press)

BOSTON -- The scam was simple. When a company ordered an airline ticket on its credit card, a travel agent entered the card number into his computer and ordered a few extra tickets.

The extra tickets added up and the unscrupulous agent sold them for thousands of dollars.

But the thief eventually attracted attention and authorities called in Robert McKenna, a prosecutor in the Suffolk County district attorney's office. He is one of a growing, but still outgunned posse of investigators who track high-tech villains.

After the thief put a ticket to Japan on a local plumbing company's account, he was arrested by police McKenna had posing as temporary office workers. He was convicted and sentenced to a year in prison.

But the sleuths who track high-tech lawbreakers say too many crimes can be committed with a computer or a telephone, and too few detectives are trained to stop them.

"What we've got is a nuclear explosion and we're running like hell to escape the blast. But it's going to hit us," said Chuck Jones, who oversees high-tech crime investigations at the California Department of Justice.

The problem is, investigators say, computers have made it easier to commit crimes like bank fraud. Money transfers that once required signatures and paperwork are now done by pressing a button.

But it takes time to train a high-tech enforcer.

"Few officers are adept in investigating this, and few prosecutors are adept in prosecuting it," Jones said.

"You either have to take a cop and make him a computer expert, or take a computer expert and make him a cop. I'm not sure what the right approach is."

In recent high-tech crimes:

- Volkswagen lost almost \$260 million because of an insider computer scam involving phony currency exchange transactions.
- A former insurance firm employee in Fort Worth, Texas, deleted more than 160,000 records from the company's computer.
- A bank employee sneaked in a computer order to Brinks to deliver 44 kilograms of gold to a remote site, collected it, then disappeared.

Still, computer cops have their successes.

The Secret Service broke up a scheme to make counterfeit automatic teller

machine cards that could have netted millions.

And Don Delaney, a computer detective for the New York State Police, nabbed Jaime Liriano, who cracked a company's long-distance phone system.

Many company phone systems allow employees to call an 800 number, punch in a personal identification number and then make long-distance calls at company expense.

Some computer hackers use automatic speed dialers -- known as "demon dialers" -- to dial 800 numbers repeatedly and try different four-digit numbers until they crack the ID codes. Hackers using this method stole \$12 million in phone service from NASA.

Liriano did it manually, calling the 800 number of Data Products in Wallingford, Connecticut, from his New York City apartment. He cracked the company's code in two weeks.

Liriano started selling the long distance service -- \$10 for a 20-minute call anywhere -- and customers lined up inside his apartment.

But Delaney traced the calls and on March 10, he and his troopers waited outside Liriano's apartment. On a signal from New York Telephone, which was monitoring Liriano's line, the troopers busted in and caught him in the act.

Liriano pleaded guilty to a misdemeanor of theft of services, and was sentenced to three years' probation and community service.

Data Products lost at least \$35,000. "And we don't know what he made," Delaney said of Liriano.

Who Pays For Calls By Hackers?

June 12, 1992

~~~~~

By Kent Gibbons (The Washington Times) (Page C1)

ICF International Inc. doesn't want to pay \$82,000 for unauthorized calls by hackers who tapped the company's switchboard.

AT&T says the Fairfax engineering firm owns the phone system and is responsible for the calls, mostly to Pakistan.

Now their dispute and others like it are in Congress' lap. A House subcommittee chairman believes a law is needed to cap the amount a company can be forced to pay for fraudulent calls, the same way credit card users are protected.

Edward Markey, the Massachusetts Democrat who held hearings on the subject said long-distance carriers and local telephone companies should absorb much of those charges.

Victims who testified said they didn't know about the illegal calls until the phone companies told them, sometimes weeks after strange calling patterns began. But since the calls went through privately owned switchboards before entering the public telephone network, FCC rules hold the switchboard owners liable.

"This is one of the ongoing dilemmas caused by the breakup of AT&T," Mr. Markey said. Before the 1984 Bell system breakup, every stage of a call passed through the American Telephone & Telegraph Co. network and AT&T was liable for fraudulent calls.

Estimates of how much companies lose from this growing form of telephone fraud

range from \$300 million to more than \$2 billion per year.

The range is so vast because switchboard makers and victims often don't report losses to avoid embarrassment or further fraud, said James Spurlock of the Federal Communications Commission.

Long-distance carriers say they have stepped up their monitoring of customer calls to spot unusual patterns such as repeated calls to other countries in a short period. In April, Sprint Corp. added other protective measures, including, for a \$100 installation charge and \$100 monthly fee, a fraud liability cap of \$25,000 per incident.

AT&T announced a similar plan last month.

Robert Fox, Sprint assistant vice president of security, said the new plans cut the average fraud claim from more than \$20,000 in the past to about \$2,000 during the first five months of this year.

But the Sprint and AT&T plans don't go far enough, Mr. Markey said.

ICF's troubles started in March 1988. At the time, the portion of ICF that was hit by the fraud was an independent software firm in Rockville called Chartways Technologies Inc. ICF bought Chartways in April 1991.

As with most cases of fraud afflicting companies with private phone systems, high-tech bandits broke into the Chartways switchboard using a toll-free number set up for the company's customers.

Probably aided by a computer that randomly dials phone numbers, the hackers got through security codes to obtain a dial tone to make outside calls.

The hackers used a fairly common feature some companies offer out-of-town employees to save on long-distance calls. Ironically, Chartways never used the feature because it was too complicated, said Walter Messick, ICF's manager of contract administration.

On March 31, AT&T officials told Chartways that 757 calls were made to Pakistan recently, costing \$42,935.

The phone bill arrived later that day and showed that the Pakistan calls had begun 11 days before, Mr. Messick said.

Because of the Easter holiday and monitoring of calls by Secret Service agents, ICF's outside-calling feature was not disconnected until April 4. By then, ICF had racked up nearly \$82,000 in unauthorized calls.

A year ago, the FCC's Common Carrier Bureau turned down ICF's request to erase the charges. The full commission will hear an appeal this fall.

---

Dutch Hackers Feel Data Security Law Will Breed Computer Crime      July 7, 1992  
~~~~~  
By Oscar Kneppers (ComputerWorld Netherland)

HAARLEM, the Netherlands -- Dutch hackers will be seriously reprimanded for breaking and entering computer systems, if a new law on computer crime is passed in the Netherlands.

Discussed recently in Dutch parliament and under preparation for more than two years, the proposed law calls hacking "a crime against property." It is expected to be made official in next spring at the earliest and will consist of the following three parts:

- The maximum penalty for hackers who log on to a secured computer system would be six months' imprisonment.
- If they alter data in the system, they could spend up to four years in prison.
- Those who illegally access a computer system that serves a "common use" -- like that in a hospital or like a municipal population database -- could soon risk a prison sentence of six years.

This pending law does not differentiate between computer crimes committed internally or externally from an office. For example, cracking the password of a colleague could lead to prosecution.

Hackers believe this law will only provoke computer crime, because the hackers themselves will no longer offer "cheap warnings" to a computer system with poor security.

Rop Gonggrijp, who is sometimes called the King of Hacking Holland, and is currently editor-in-chief of Dutch computer hacker magazine "Hack-tic" warns that this law could produce unexpected and unwanted results.

"Students who now just look around in systems not knowing that it [this activity] is illegal could then suddenly end up in jail," he said. Gonggrijp equates hacking to a big party, where you walk in uninvited.

Gonggrijp is concerned about the repercussions the new law may have on existing hackers. He said he thinks the current relationship between computer hackers and systems managers in companies is favorable. "[Hackers] break into, for example, an E-mail system to tell the systems manager that he has to do something about the security. If this law is introduced, they will be more careful with that [move]. The cheap warning for failures in the system will, therefore, no longer take place, and you increase chances for so-called real criminals with dubious intentions," he added.

According to a spokesman at the Ministry of Justice in The Hague, the law gives the Dutch police and justice system a legal hold on hackers that they currently lack.

"Computer criminals [now] have to be prosecuted via subtle legal tricks and roundabout routes. A lot of legal creativity was [previously] needed. But when this law is introduced, arresting the hackers will be much easier," he said.

The Dutch intelligence agency Centrale Recherche Informatiedienst (CRI) in The Hague agreed with this. Ernst Moeskes, CRI spokesman, said, "It's good to see that we can handle computer crime in a directed way now."

PWN Quicknotes

~~~~~

1. Printer Avoids Jail In Anti-Hacking Trial (By Melvyn Howe, Press Association Newsfile, June 9, 1992) -- A printer avoided a jail sentence in Britain's first trial under anti-hacking legislation. Freelance typesetter Richard Goulden helped put his employers out of business with a pirate computer program -- because he said they owed him L2,275 in back pay. Goulden, 35, of Colham Avenue, Yiewsley, west London, was conditionally discharged for two years after changing his plea to guilty on the second day of the Southwark Crown Court hearing. He was ordered to pay L1,200 prosecution costs and L1,250 compensation to the company's liquidators. Goulden had originally denied the charge of unauthorized modification of computer material under the 1990 Computer Misuse Act. After his change of plea Judge John Hunter told him: "I think it was plain



at a very early stage of these proceedings that you had no defence to this allegation." Mr. Warwick McKinnon, prosecuting, told the jury Goulden added a program to a computer belonging to Ampersand Typesetters, of Camden, north-west London, in June last year which prevented the retrieval of information without a special password. Three months later the company "folded". Mr Jonathan Seitler, defending, said Goulden had changed his plea after realizing he had inadvertently broken the law.

---

2. ICL & GM Hughes In Joint Venture To Combat Computer Hackers (Extel Examiner, June 15, 1992) -- General Motors Corporation unit, Hughes STX, and ICL have set up a joint venture operation offering ways of combating computer hackers. Hughes STX is part of GM's GM Hughes Electronics Corporation subsidiary. ICL is 80% owned by Fujitsu. Industry sources say the venture could reach \$100 million in annual sales within four years.
- 

3. Another Cornell Indictment (Ithaca Journal, June 17, 1992) -- Mark Pilgrim, David Blumenthal, and Randall Swanson -- all Cornell students -- have each been charged with 4 felony counts of first-degree computer tampering, 1 count of second-degree computer tampering, and 7 counts of second-degree attempted computer tampering in connection with the release of the MBDF virus to the Internet and to various BBSs.

David Blumenthal has also been charged with two counts of second-degree forgery and two counts of first-degree falsifying business records in connection with unauthorized account creation on Cornell's VAX5 system. He was also charged with a further count of second-degree computer tampering in connection with an incident that occurred in December of 1991.

---

4. Computer Watchdogs Lead Troopers To Hacker (PR Newswire, July 17, 1992) -- Olympia, Washington -- State Patrol detectives served a search warrant at an East Olympia residence Thursday evening, July 16, and confiscated a personal computer system, programs and records, the Washington State Patrol said.

The resident, who was not on the premises when the warrant was served, is suspected of attempts to break into computer files at the Department of Licensing and the State Insurance Commissioner's office.

The "hacker's" attempts triggered computerized security devices which alerted officials someone was attempting to gain access using a telephone modem. Patrol detectives and computer staff monitored the suspect's repeated attempts for several weeks prior to service of the warrant.

Placement of a telephone call by a non-recognized computer was all that was required to trigger the security alert. The internal security system then stored all attempted input by the unauthorized user for later retrieval and use by law enforcement. Integrity of the state systems was not breached.

The investigation is continuing to determine if several acquaintances may be linked to the break in. Charges are expected to be filed as early as next week in the case.

CONTACT: Sgt. Ron Knapp of the Washington State Patrol, (206)459-6413

---

5. UPI reports that the 313 NPA will split to a new 810 NPA effective August 10, 1994.

Oakland, Macomb, Genesee, Lapeer, St. Clair and Sanilac counties as well as small sections of Saginaw, Shiawassee and Livingston counties will go into 810. Wayne, Washtenaw, Monroe, and small parts of Jackson and Lenawee

counties will remain in 313. The city of Detroit is in Wayne County and won't change.

---