.

Information in this document is subject to change without notice.

END-USER LICENSE AGREEMENT FOR SHARP TECHNOLOGY INC. SOFTWARE

IMPORTANT - READ CAREFULLY: This SHARP TECHNOLOGY INC. End-User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single entity) and SHARP TECHNOLOGY INC. for the SHARP TECHNOLOGY INC. "HackTracer" software product, which includes computer software and may include associated media, printed materials, and “online” or electronic documentation (“SOFTWARE PRODUCT”). The SOFTWARE PRODUCT also includes any updates and supplements to the original SOFTWARE PRODUCT provided to you by SHARP TECHNOLOGY INC. Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

Software PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following rights:

You may install, use, access, display, run, or otherwise interact with (“RUN”) one copy of the SOFTWARE PRODUCT, or any prior version for the same operating system, on a single computer, workstation, terminal, or other digital electronic device (“COMPUTER”). The primary user of the COMPUTER on which the SOFTWARE PRODUCT is installed may make a second copy for his or her exclusive use on a portable computer.

• Reservation of Rights. All rights not expressly granted are reserved by SHARP TECHNOLOGY INC.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

• Not for Resale Software. If the SOFTWARE PRODUCT is labeled “Not For Resale” or “NFR,” then, notwithstanding other sections of this EULA, your use of the SOFTWARE PRODUCT is limited to use for demonstration, test, or evaluation purposes and you may not resell, or otherwise transfer for value, the SOFTWARE PRODUCT.

• Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

• Separation of Components. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one COMPUTER.

• Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of SHARP TECHNOLOGY INC.

• Rental. You may not rent, lease, or lend the SOFTWARE PRODUCT.

• Support Services. SHARP TECHNOLOGY INC. may provide you with support services related to the SOFTWARE PRODUCT (“Support Services”). Use of Support Services is governed by the SHARP TECHNOLOGY INC. policies and programs described in the user manual, in “online” documentation, and/or in other SHARP TECHNOLOGY INC.-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this EULA. With respect to technical information you provide to SHARP TECHNOLOGY INC. as part of the Support Services, SHARP TECHNOLOGY INC. may use such information for its business purposes, including for product support and development. SHARP TECHNOLOGY INC. will not utilize such technical information in a form that personally identifies you.

• Software Transfer. The initial licensee of the SOFTWARE PRODUCT may make a one-time permanent transfer of this EULA and SOFTWARE PRODUCT only directly to an end user. This transfer must include all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, this EULA, and, if applicable, the Certificate of Authenticity). Such transfer may not be by way of consignment or any other indirect transfer. The transferee of such one-time transfer must agree to comply with the terms of this EULA, including the obligation not to further transfer this EULA and SOFTWARE PRODUCT.

• Termination. Without prejudice to any other rights, SHARP TECHNOLOGY INC. may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

3. COPYRIGHT. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and “applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by SHARP TECHNOLOGY INC. or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. If this SOFTWARE PRODUCT contains documentation which is provided only in electronic form, you may print one copy of such electronic documentation. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

4. DUAL-MEDIA SOFTWARE. You may receive the SOFTWARE PRODUCT in more than one medium. Regardless of the type or size of medium you receive, you may use only one medium that is appropriate for your single COMPUTER. You may not RUN the other medium on another COMPUTER. You may not loan, rent, lease, or otherwise transfer the other medium to another user, except as part of the permanent transfer (as provided above) of the SOFTWARE PRODUCT.

5. BACKUP COPY. After installation of one copy of the SOFTWARE PRODUCT pursuant to this EULA, you may keep the original media on which the SOFTWARE PRODUCT was provided by SHARP TECHNOLOGY INC. solely for backup or archival purposes. If the original media is required to use the SOFTWARE PRODUCT on the COMPUTER, you may make one copy of the SOFTWARE PRODUCT solely for backup or archival purposes. Except as expressly provided in this EULA, you may not otherwise make copies of the SOFTWARE PRODUCT or the printed material accompanying the SOFTWARE PRODUCT.

MISCELLANEOUS

If you acquired this SOFTWARE PRODUCT in the United States, this EULA is governed by the laws of the State of Texas. You shall comply with all applicable export laws, restrictions, and regulations of any United States or foreign agency or authority. You agree not to export or re-export, or allow the export or re-export of any product, technology, or information you obtain or learn under this EULA (or any direct product thereof) from the country in which you installed and are using the PRODUCT in violation of any such laws, restrictions, or regulations. The PRODUCT is a "commercial item," "commercial computer software," and/or "commercial computer software documentation" as defined under U.S. law in FAR section 2.101, DFAR section 252.227-7014(a)(1) and DFAR section 252.227-7014(a)(1), or otherwise. Consistent with DFAR section 227.7202 and FAR Section 12.212, any use, modification, reproduction, release, performance, display, disclosure or distribution of the PRODUCT by the U.S. government shall be governed solely by the terms of this EULA and shall be prohibited except to the extent expressly permitted in this EULA.

LIMITED WARRANTY

LIMITED WARRANTY FOR SOFTWARE PRODUCTS ACQUIRED IN THE US AND CANADA. SHARP TECHNOLOGY INC. warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Support Services provided by SHARP TECHNOLOGY INC. shall be substantially as described in applicable written materials provided to you by SHARP TECHNOLOGY INC., and

SHARP TECHNOLOGY INC. support engineers will make commercially reasonable efforts to solve any problem issues. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you. To the extent allowed by applicable law, implied warranties on the SOFTWARE PRODUCT, if any, are limited to ninety (90) days.

CUSTOMER REMEDIES. SHARP TECHNOLOGY INC.'s and its suppliers' entire liability and your exclusive remedy shall be, at SHARP TECHNOLOGY INC.'s option, either (a) return of the price paid, if any, or (b) repair or replacement of the SOFTWARE PRODUCT that does not meet SHARP TECHNOLOGY INC.'s Limited Warranty and which is returned to SHARP TECHNOLOGY INC. with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by SHARP TECHNOLOGY INC. are available without proof of purchase from an authorized international source.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, SHARP TECHNOLOGY INC. and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide Support Services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, in no event shall SHARP TECHNOLOGY INC. or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide Support Services, even if SHARP TECHNOLOGY INC. has been advised of the possibility of such damages. In any case, SHARP TECHNOLOGY INC.'s entire liability under any provision of this EULA shall be limited to the greater of the amount actually paid by you for the SOFTWARE PRODUCT or U.S.$5.00; provided, however, if you have entered into a SHARP TECHNOLOGY INC. Support Services Agreement, SHARP TECHNOLOGY INC.'s entire liability regarding Support Services shall be governed by the terms of that agreement. Because some states and jurisdictions do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

END USER LICENSE AGREEMENT FOR NEOWORX INC. SOFTWARE

NeoWorx inc. warrants that it is sole owner of the software and has full power and authority to grant this license herein without consent of any other party.

This software is licensed, not sold. The fee you pay entitles you to use the software, not to own it.

The software contained in this package (hereafter referred to as "the Software") is copyrighted material owned by NeoWorx inc. Payment of the single copy license fee authorizes one named person to use the Software on one computer provided this copyright is not violated and provided the rules outlined herein are observed.

One person may use the Software on any single computer. This license can not be transferred. You must pay for additional copies of the Software if more than one person uses it at one time, or if the Software is used on two or more computers. Neither concurrent use on two or more computers, nor use by more than a single individual on a network is permitted without authorization and payment of other license fees.

You may make copies of the software for backup purposes, as long as all such copies, along with the original, are kept in your possession or control.

You may not make any changes or modifications to the Software, including, but not limited to, de-compiling, disassembling, or otherwise reverse engineering it. You may not rent or lease it to others. You may not use it on a computer network if more than one user can use it on more than one computer during any one twenty-four hour span of time.

NeoWorx hereby disclaims all warranties relating to this software, whether express or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose. NeoWorx will not be liable for any special, incidental, consequential, indirect or similar damages due to loss of data or any other reason, even if NeoWorx or an agent of NeoWorx has been advised of the possibility of such damages. In no event shall NeoWorx's liability for any damages ever exceed the price paid for the license to use the software, regardless of the form of the claim. The person using the software bears all risk as to the quality and performance of the software.

U.S. GOVERNMENT RESTRICTED RIGHTS

Use, duplication, or disclosure by the Government is subject to standard shrink-wrapped software restrictions.

Disclaimer of Warranty

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OR MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.

INTRODUCTION

Welcome to Hack Tracer. If you're reading this, you are probably concerned about the security of your computer while you are on the Internet. You may have experienced an attack that compromised your computer or you may have heard horror stories about what happened to someone else or you may just be playing it safe. No matter the reason that brought you here, you are about to install a tiny little program that will give your system big time protection.

Why do I need protection?

Any time you are online, you are tied into the World Wide Web and you are a part of the web. Your computer is potentially just as accessible as any web site you are visiting. It has an IP address which is used to route traffic to you. Your Internet service provider (ISP) assigns that address to you on a temporary basis during your online session. As soon as you sign off, your ISP can immediately reassign the address you just had to another user who has signed on. You must have an IP address in order to use the web. When you browse a web page or send E-mail, data traffic has to be able to find it's way back to you. Some DSL cable modem and ISDN connections may have permanently assigned IP addresses.

So how does someone find ***your*** machine among the many millions that may be online at any given moment? Usually, ***dumb luck.***

Hackers looking for users to victimize make use of scanner programs that enable them to search rapidly through hundreds of DNS addresses looking for an open door. You might compare it to a door-to-door salesman walking down a street and ringing doorbells hoping to find someone home. In this case it might be more accurate to think of the hacker as a burglar looking for an open window or an unlocked door.

Hack Tracer is a personal firewall designed to protect your computer from a possible unwanted intrusion and it includes a sophisticated trace module that can tell you the source of the intrusion. In other words, Hack Tracer locks the windows and the doors and it tells you who was trying to get in.

The thought of someone trying to get into your computer without your knowledge can seem pretty scary. The reality is that most apparent "intrusions" can be classified as harmless. And as a Hack Tracer user you will be surprised to discover just how often someone tries to unexpectedly reach your computer.

There are a broad variety of sources and reasons for these types of "friendly" intrusions.

When you first sign on to the Internet, you might find yourself the target for data that was intended for the last user who had your DNS address. Technically, that's an intrusion because you are receiving something you didn't ask for.

When you are registering software online or completing a survey or application, you might find that the computer at the other end is querying your computer. Most software companies now


make it a policy to ask your permission before obtaining information from your computer, but this may not always be the case.

An online service might ask your computer to tell it what web browser you're using. That information can prove very helpful in making decisions affecting web site redesign. It would not be wise to upgrade a site if the majority of users have older web browsers that would be incapable of seeing fancy applets or multiple frame pages.

Your computer routinely has to contact different computers on the Internet to find the addresses of web sites or other computers that you are trying to contact. This type of traffic is called a DNS query. In some cases there may be traffic related to configuration of your Internet connection, and there may be traffic between your computer and your ISP that allows your ISP to determine if you are still connected.

As you can see, most of these instances are harmless, or at worst, simply nosey.

With Hack Tracer you'll be protected from the unwanted friendly probes, the nosey, and, most important of all, the burglars.

Hack Tracer is NOT an anti-virus program. It cannot detect, it cannot protect you from, and it cannot remove or quarantine traditional computer viruses or the newer types of worms or Trojan horses. These make their way onto your system from an infected floppy disk or as a seemingly innocent E-mail attachment, but always at your unknowing invitation. ***You still need "anti-virus" protection***, you still need to update it regularly to protect yourself from new viruses, and you need to practice common sense when it comes to accepting software from others. Never accept software directly from someone you meet on an online chat forum, no matter how cool they say the program is. This is basic online safety.

GETTING STARTED

SYSTEM REQUIREMENTS

Your computer should be *Pentium class with at least 32 MB of RAM*. More memory is recommended.

Hack Tracer will work in any version of Windows 95 or 98. Windows NT and 2000 are not supported by this version.

Hack Tracer is intended for use on standalone IBM compatible computers that are connected to the Internet via analog modems, cable modems, DSL or ISDN connections. If you want to use Hack Tracer on a computer that is part of a large LAN (more than 5 computers) make certain it is OK with your system administrator before installing.

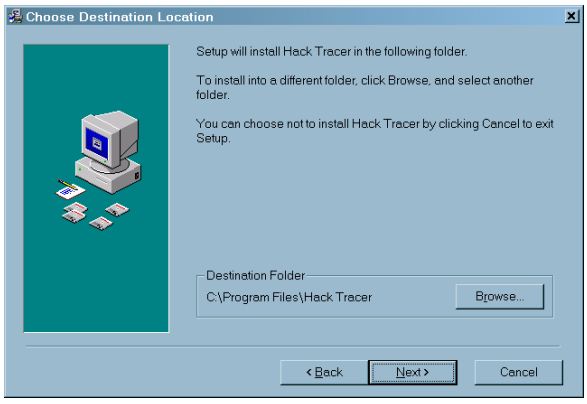
Hack Tracer will protect your system while it is connected to the Internet regardless of whether you are using a browser, sending or receiving E-mail, using a newsgroup reader, an FTP program or web authoring software. If you're online, Hack Tracer is protecting you from unwanted connections.

INSTALLATION

To install Hack Tracer, run the HackTracer.EXE file.

You will be warned to close all Windows programs before running the Setup program. If necessary, click on *Cancel*, close all running programs, and then restart the Hack Tracer installation.

The first thing the installation program will ask you is if you want to view an online document with further help information. Make sure you are connected to the Internet and they press 'Yes' to view this page. The page may contain help information that is more up to date than this printed documentation. The page will offer additional guidance in installing and setting up the program.



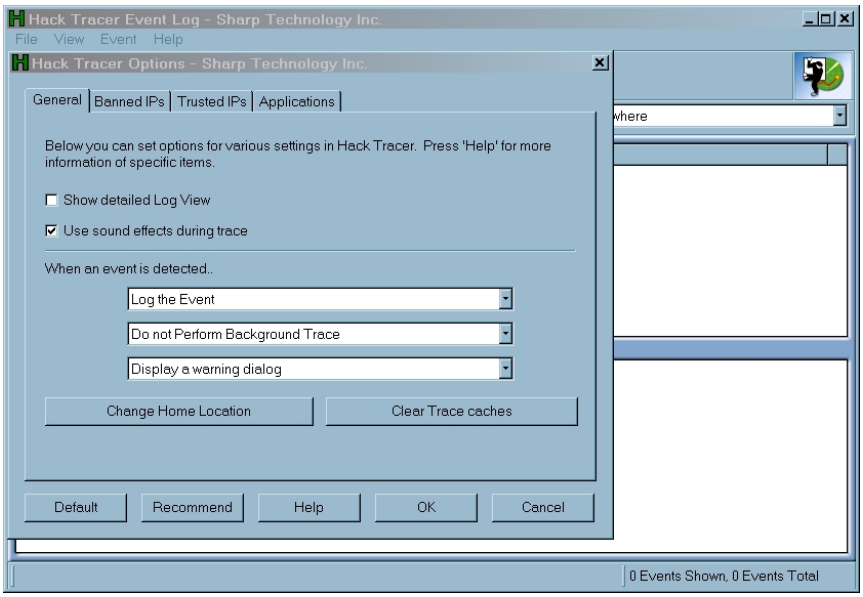
The default installation location for Hack Tracer is C:\Program Files\Hack Tracer. If you want to install it in another location, click on the Browse button and customize the installation location to suit your needs.

A progress meter will indicate how the installation is progressing. On most systems this will only take a few seconds.

Your system must be restarted to complete the installation. You can defer this to a later time by clicking Cancel, but remember that ***Hack Tracer cannot begin to protect your system until you have restarted your computer.***

Configuring Hack Tracer

When your system restarts the Hack Tracer Options and Event Log window will appear as shown. You will be offered another online help page with the latest details on the initial setup of Hack Tracer. Make sure you are connected to the Internet before you select 'Yes' to view this help page.

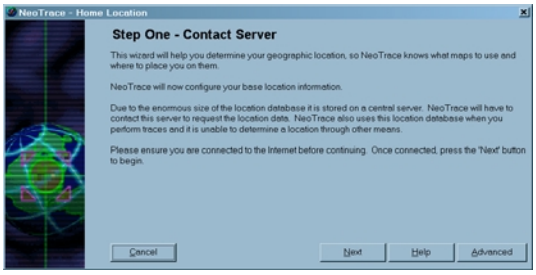


You can safely accept the default settings at this time. When you are more familiar with Hack Tracer you can begin to modify these settings to suit your personal preferences. The various setting choices are explained in detail later in this manual.

Setting your home location

There is one setting which you should make, however, and that is your home location. You can either make it now or wait for the program to ask you to set it the first time you attempt to track an event.

The Hack Tracer NeoTrace Express (NTX) module needs to know where you are located in order to generate proper trace maps. Click on the Change Home Location button to launch a Wizard that will walk you through setting your home location. The process involves automatically connecting with the NeoTrace home site to obtain precise coordinates for your home location from an enormous online location database.



The Home Location Wizard will launch.

If you are not already on line, you will be prompted to connect to the Internet.

The Wizard will link automatically to the Hack Tracer/NeoTrace web site.

In Step Two you will be asked to select your country from a drop down scrollable list. After you select your country, enter any other information the Wizard requests. The Wizard will access the database and determine the appropriate latitude and longitude data for your location.

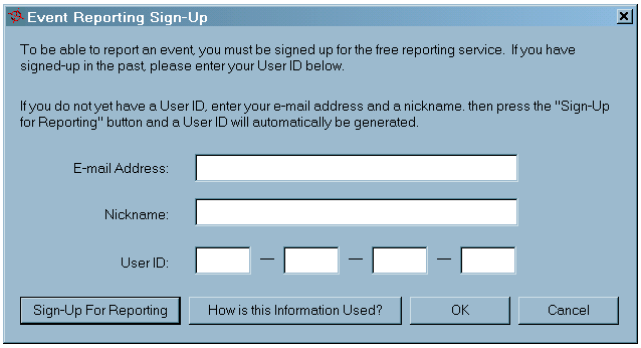
City location data is not yet available for all countries. If a specific location for your hometown or city is not available, a default location for your country (typically the capital), will be returned.

The Wizard will inform you that the location data has been transferred to your computer.

Click on ***Finish*** to close the Wizard and return to the Options Window.

Event Reporting Sign-Up

The first time you report an event using the 'Report This' button or link in Hack Tracer you will be asked to sign up.



Your event data will be submitted to a centralized reporting system that aggregates unwelcome traffic information and analyses it for patterns. When the pattern indicates someone who is creating problems or potentially dangerous the proper authorities and service providers can be notified from this central service.

In order to sign up to use the reporting service you need to uniquely identify yourself with your email address. This address will only be used to notify you of important events related to the reporting system and your security.

That's it. You are now ready to surf the web safe from hackers.

HOW DO I…?

How do I protect my computer from hackers?

If you're installing Hack Tracer you are already taking the first and most important step in protecting yourself from Hackers.

Always practice safe computing. ***Never*** accept files directly from people you meet online. ***Never*** open an unexpected E-mail attachment. Set your security options (if any) on your E-mail to a high setting. ***Never*** share passwords with anyone. ***Never*** divulge personal information in chat sessions with people you don't know.

Much of this is common sense but from time to time it's easy to become complacent and be lulled into a false sense of security. The so-called "Love Bug" virus which swept around the world overnight was a good example of a costly Internet-borne virus that was opened and spread by millions of people who saw a familiar name in the "From" field and proceeded to open their little "surprise package" without giving it a second thought. By the time they had a second thought, it was already too late.

How do I understand what the alert messages mean?

When Hack Tracer detects an intrusion it will alert you in one of several ways depending on how you have set up your event alert options.

The most dramatic alert message is the one displayed at right that pops up right in the middle of your screen.

The meaning of these alerts is entirely dependent on the nature of the event. Later on in this manual we will discuss the various types of probes that can take place and the significance of the particular port being probed. You can click on the "More Information" link in the Events Details box to open a web page with further explanation. This web-based help system allows you to view expanded information and help that is specific to the event in question.

When you first set up Hack Tracer you will probably want to maximize the event alerts so that you can better understand the nature and frequency of these unsolicited intrusions. In time, as you get used to Hack Tracer's ability to fend off these intrusions you'll probably opt for silent background operation with an occasional peek at the event log to see just who and what Hack Tracer has been protecting you from.

How do I configure the behavior of Hack Tracer?

Hack Tracer's behavior is fully configurable in the Options dialog.

• You decide if and how you will be alerted to an intrusion event. Options include a sound, a blinking icon on the task bar, a pop-up intruder alert in the middle of your screen or quiet background operation.

• You decide what Hack Tracer will do when there is an intrusion. Options here include logging the event and performing a trace in background,

• You can set up a list of banned IPs, in effect barring them from ever communicating with your computer.

• You can establish a list of Trusted IPs which are granted complete access to your system.

• You may also designate particular applications which can interact with your system without restriction. These include interactive games such as Quake.

These configuration options are described in detail later on in this manual.

How do I fight back against hackers?

Fighting hackers is not your job. It's ours. You don't have to fight back and in any case, you shouldn't. If you counter-attack, that action is every bit as illegal as the hacker's original attack on you.

Hack Tracer is stopping these intruders before they get in your door. No harm has been done to your system and when all is said and done the majority of intrusion events do not come from hackers.

Hack Tracer has automatically captured the critical information detailing the intrusion attempt and Hack Tracer provides you with a quick and easy way to report your attack to HackerWatch headquarters.

Your intrusion report is cataloged and correlated with thousands of other reports. When the data establishes a distinct hacker pattern, HackerWatch reports the alleged hacker to appropriate Internet authorities.

How do I report hackers to authorities?

It's as easy as one, two, three and HackerWatch headquarters does all the hard work for you.

First, be sure to register for HackerWatch as soon as you install your Hack Tracer software. The simple procedure for signing up is explained above at the end of the installation section.

Two, keep your HackerWatch ID number handy. You will need it just once, the first time you sign in to report a suspicious intrusion.


Three, click on ***Report It*** in the event detection window OR simply open the Hack Tracer Event Log, highlight the suspected hack attempt in the upper Event Log window, and click on ***Report This Event*** in the lower Event Detail window (shown at right).

Hack Tracer will automatically contact HackerWatch headquarters where the event will be recorded for screening, correlation and notification of authorities. The HackerWatch report page (shown at right) will acknowledge your report and indicate the number of events you have reported to-date. The HackerWatch site may also display information specific to your intrusion attempt if it is available.

How do I check for News and Hack Tracer updates?

Simply click the **NEWS** icon on the Event Log Icon bar. You will be connected to Hack Tracer headquarters and get the latest news on Hack Tracer and other critical news regarding hacking and computer viruses. If you are not already online, you will be asked to connect to your ISP.

In the pull down **Help** menu click on **Check for Updates...** to automatically check the Hack Tracer site for an updated version of the software. If you are not already online, you may be asked to connect to your ISP.

How do I trace back to a hacker?

Hack Tracer includes a special version of the award-winning ***NeoTrace*** software. This special version is called NeoTrace Express or NTX. If configured to do so, Hack Tracer will do an immediate background trace. If you have Hack Tracer configured to pop up an ***Event Detected*** window, you can click on **Track It!** to launch the NeoTrace Express function.

Why would I want to turn on background tracing?

If the source of the event is connected on a dial-up connection with a temporary IP that computer may not be there to trace to later. Tracing at the time the event occurs ensures an accurate trace.

The flip side of this is that the assumed hacker *may* be able to detect the trace.

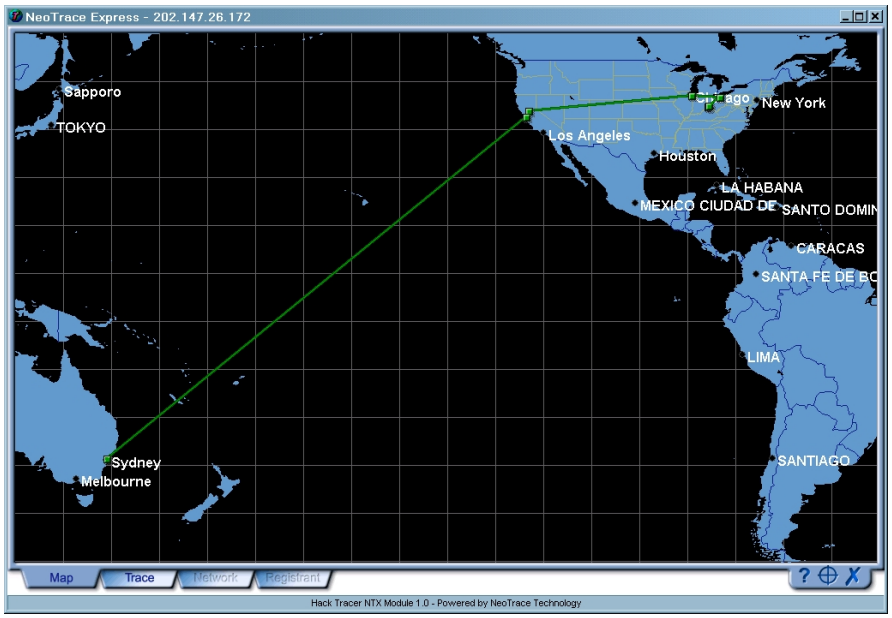
NeoTrace Express will display a graphic representation of the trace process. Clicking on the Trace tab below the map displays a detailed list of all the Internet nodes between you and the intrusion source. The Network tab displays detailed information about the source and the Registrant tab brings up Internet registration information pertinent to the source IP address.

NeoTrace Express functionality is explained in detail later in this manual.

What do Hackers want from me?

What hackers want from you and what they can potentially do to you varies widely from a simple "ding-dong-ditch" (the equivalent of ringing someone's doorbell and then running away) to grand-theft-auto.

The good news is that in the vast majority of cases the intent and the possible damage are minimal. The bad news is that the nuisance attacks can desensitize us to the threat, and a large number of nuisance attacks can add up to a very big problem.



There are just as many predators and wackos on the Internet as there are in the real world. The world of cyberspace offers these people a feeling of anonymity and action at a distance. An attack worked through a computer lends the villain a sense of security and makes it a sort of game for many of them. It becomes a technical challenge to see if they can hack a computer or disrupt a web site. They may actually be unaware of the amount of trouble they are causing.

Personal computers are easy pickings for hackers when compared to commercial and government sites. Personal computers are generally not behind a firewall, run non-secure operating systems, and, by definition, are set up by amateurs. If you set up your personal computer with the default software and do nothing to protect it, it's like buying a car and parking it all over town with the doors unlocked. You're inviting trouble.

The most common type of hacker you will encounter is a "script kiddie." This derisive phrase has been coined to describe people using software tools to attempt to find "holes," possible points of entry into your computer. These software tools will automatically scan ranges of IP addresses probing for and noting possible entry points. The hacker can then go back and make a more determined effort at breaking into the computer.

One of the things that these "script kiddies" search for is known Trojans that are already on your computer. (A Trojan, named after the "Trojan Horse," is a computer program that offers a means to perform unwanted actions on your computer; Trojans are similar to a virus, are generally more complex and much larger than the typical virus program, and they are often disguised as a useful

program.) Where did you get this Trojan that the "script kiddie" finds? From someone you met online or from a friend who thought they were giving you a cool utility.

If your computer is sitting there like an unlocked car, a hacker can access your system in much the same way you can access a drive in another computer on a LAN. They can read or copy any file on your system. They can obtain your social security number if you have archived your tax records. They can look at your money management program and online banking records. They can deposit a Trojan or a virus on your hard drive. They can change or delete data and passwords.

The payload of a Trojan may range from simply deleting files on your hard drive, to stealing passwords or allowing remote control of your computer. This latter category is now the most commonplace and certainly the most feared. These programs can allow a remote operator to gain access to your computer and perform actions on it, deleting files, making changes, even viewing your screen and running software remotely. A computer with a Trojan of this nature on it will often appear to be 'possessed,' and indeed in a way it is.

Unprotected systems are vulnerable to having a Trojan placed on them by a hacker who stumbles across your unprotected system during a routine scan. Once Hack Tracer is installed, a Trojan can only be placed in your system by *you*! If you install a Trojan on your system after you install Hack Tracer, you are punching a hole in the protection given you by Hack Tracer. The Trojan will open a door in your firewall and Hack Tracer will ignore it because the Trojan makes it look as though you are authorizing the access.

We can only repeat our earlier warnings: ***Never*** accept files directly from people you meet online. ***Never*** open an unexpected E-mail attachment. Set your security options (if any) on your E-mail to a high setting. ***Never*** share passwords with anyone. ***Never*** divulge personal information in chat sessions with people you don't know.

Data destruction and data theft are the two main things you need to worry about from hacker attacks. Data theft could include stealing your account names and passwords. This could gain them access to your screen name, your E-mail, your Internet dial-up account, your web site accounts. If they discover a web site account that has your stored credit card information and also a facility to change your mailing address they would potentially be able to order items from that site. If there are data files on your computer that contain your credit card or banking information, your taxes, etc. they are potentially subject to theft.

What we are describing here are worse case scenarios. Keep in mind that the majority of intrusions are harmless and even most hack attacks are just minor nuisances.

With Hack Tracer installed on your computer, these troublemakers cannot even tell that there is a computer at your IP address. Think of yourself as living in an invisible house surrounded with a 30-foot high electrified fence topped with razor-wire.

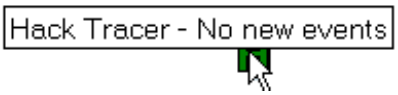
Hack Tracer's bells and whistles

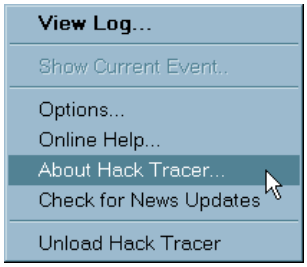
The Hack Tracer Tray Icon

Hack Tracer places a small icon on your Windows Taskbar. It tells you that Hack Tracer is alive and well and ready to protect you whenever you're online.

This task bar icon will blink when an intrusion event occurs if you have the options configured to do that.

If you place your cursor over the icon it will report the number of new events since you last checked the event log or "No new events" if none have occurred.





If you right click on the task bar icon, you will be presented with the popup menu shown at right offering you access to all Hack Tracer features including checking for News and Updates online.

Unload Hack Tracer temporarily disables the firewall protection. Clicking on Hack Tracer Tray utility in the program group restores protection.

The Hack Tracer Options Window

The Options dialog allows you to set up Hack Tracer to meet your needs and to change those settings at any time with a few simple clicks.

Setting your Home Location

Set your home location by simply clicking on the Change NeoTrace Home Location button bar. This launches the home location wizard. This process is described in detail and fully illustrated back in the installation/setup section.

General Options

Show detailed Log View

The default is *unchecked*. The default log shows the Date and Time of the event, the source IP address, the host name at that source IP address, and Event Information. Checking *Show detailed Log View* adds two fields to your log information: the Destination Port and the Source (Src.) Port. The significance of the information captured in these fields is fully explained in the Event Log section.

Use sound effects during trace

The default is *checked*. When the NeoTrace Express module is launched, a map appears and a distinctive ping sound signals the identification of each Internet node as NeoTrace Express searches the cyber trail leading back to the source of the intrusion.

Check for new version of program

The default is *unchecked*. If you check this box, Hack Tracer will automatically check its home site for the availability of a newer version of the program. If a new version is available, you will be prompted to view further information. If automatic checking is selected the check will be performed approximately once per month. You can check for updates yourself at any time by clicking on Check for Updates in the pull down Help menu of the Events Log.

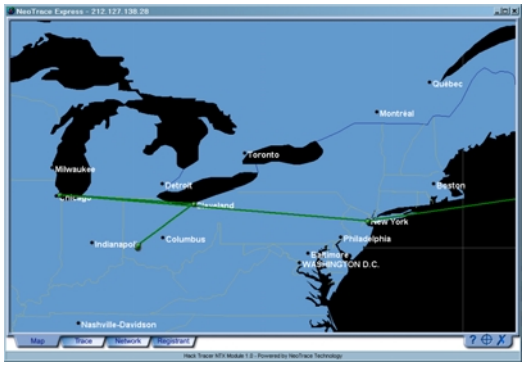
When an Event is Detected...

Hack Tracer responds to an intrusion event in a variety of user determined ways. The default options are shown above.

Log the Event

The default action is *Log the Event*. Hack Tracer captures all of the critical information regarding the intrusion and enters it in the event log. A *Do Not Log the Event* choice is the alternative choice, in which case no logging will be performed.

Tracing the Event



The default action is *Do not Perform Background Trace*. Tracing the source of an event is left up to the user. The alternative choice here is *Perform a Background Trace*. With this option selected, Hack Tracer immediately launches a "quiet" version of NeoTrace Express and performs a detailed source trace. See the NeoTrace Express section to understand what the NeoTrace process tells you.
The benefit to having a background trace performed immediately is that you may be able to gather information that will not be available later. If the event source is a computer connected through a modem, this connection will likely be gone by the time you manually investigate. Turning on background tracing is the surest means of getting accurate trace data.

Event notification

The default is *Display a warning dialog.* When Hack Tracer detects an intrusion the Intrusion Event dialog box will pop up in the center of your monitor. During your initial "get-acquainted" period, most users want this sort of "in your face" warning. Once you get used to the idea that the majority of events are harmless, you will probably want to de-escalate to one of the other alert alternatives: *Flash the Tray Icon* or simply *Keep Quiet*. Responding to an event notification is discussed in detail later in this manual.

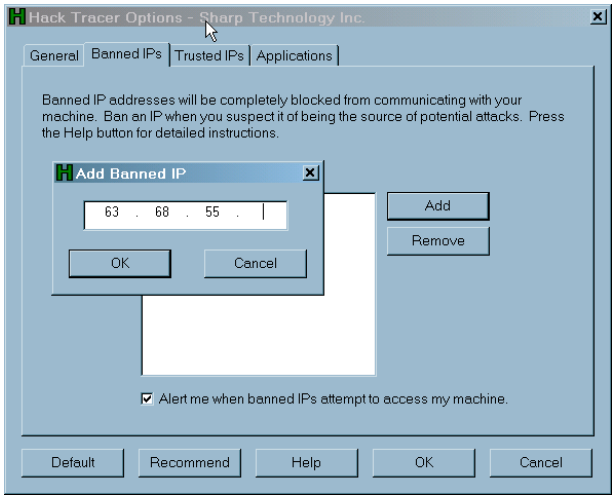
Clearing Trace Caches

Hack Tracer and NeoTrace Express record the information received from the DNS (node name), WhoIs (node owner) and LOC (location) lookups. To clear the entire cache simply press the *Clear Trace Caches* button.

Setting the remaining options

Banned IPs

The banned IPs window allows you to create a list of IP addresses that you want permanently barred from communicating with your computer. Simply click on Add and enter the complete IP address. Note the check box at the bottom of the dialog box where you can request an alert whenever a banned IP attempts to contact your system.



Users at IP addresses in your banned list will be completely unable to communicate with your computer. Note that you will also be completely unable to communicate with them as well since no returned data will be allowed into your system.

You have a choice of whether you want attempted traffic from banned IPs to be logged. To set this option toggle the checkbox at the bottom of the Banned IPs.

Trusted IPs

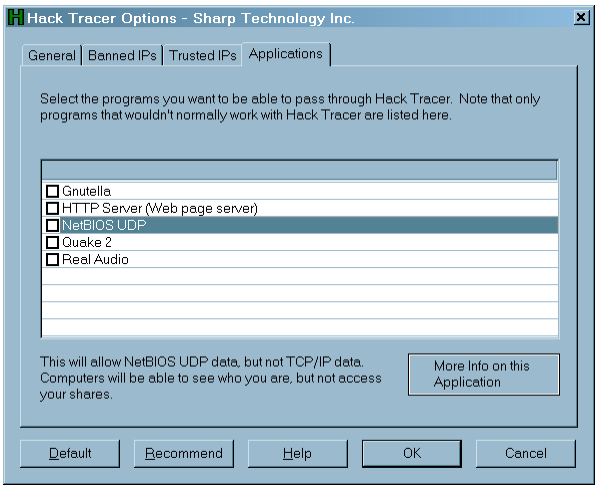
Trusted IPs are computers that you do not want blocked. Traffic from any IP address on the Trusted list will be treated as though Hack Tracer were not installed on your computer.

To create a Trusted IP entry, simply click on Add and enter the full IP address in the popup window.

For users at these IP addresses the access to your computer will be as though you have no firewall installed.

By default Hack Tracer will treat any computers on your LAN as Trusted. If you do not want Hack Tracer to behave in this fashion you should uncheck the box at the bottom of the Trusted IPs Dialog.

Applications



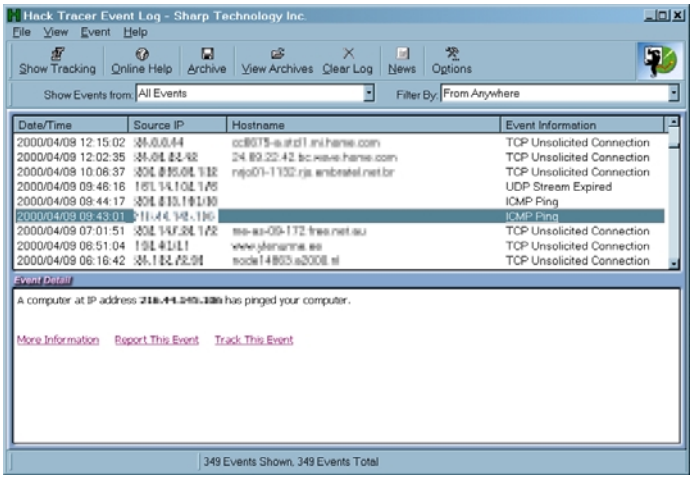
Certain applications require unencumbered access in and out of your system. These types of applications behave like a 'server' in that they need to accept connections that are not expected ahead of time. Applications that fall into this category may include games and chat programs. Most game and chat programs are designed to not require special firewall configuration.

Known applications with this requirement have been pre-entered. Check only those which you actually use.

Additional application configuration information can be found in the online help. This may include additional application configuration files that you can download.

The Hack Tracer Event Log

The Hack Tracer Event Log is the heart of the Hack Tracer program. From here you can access program options, launch a trace, get more information about an event, and report an event. The event log listing and the event detail window provide you with precise information about every intrusion event.

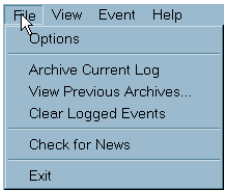


The pull down menus

The File menu

Options: Opens the Options dialog box which was described in detail above.

Archive Current Log: This function clears the current event log and saves its entire content to an event log file (.elog). *Note: the archive functions are described in more detail immediately after this section.*



View Previous Archives: Opens an Explorer window and shows you all of the previously saved archive files.

Clear Logged Events: This function clears the current log without saving it in an archive file. There is a warning message that asks you to confirm this choice before the log is cleared.

Check for News: Contacts Hack Tracer headquarters and checks for news updates. If you are not online, you will be prompted to connect to your ISP.

Exit: Closes the Event Log window.

The View Menu

The View Menu options allow you to filter which events from the log are displayed. Changing the view option does not alter the data in the log, it merely expands or limits which items are displayed.

Show All Events: All events in the current log are displayed.

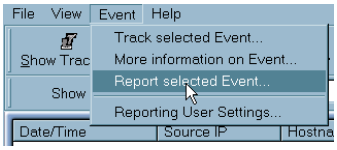
Show Last 7 Days: Only those events in the current log that occurred in the last seven days are displayed. *Other events do not show, but are not deleted.*

A note about screen shots: in most of the screen images in this doc the IP addresses and host names have been deliberately obscured.

Show Today's Events: Only those events in the current log that occurred in the last 24 hours. *Other events do not show, but are not deleted.*

The Event Menu

Track selected Event: Launches NeoTrace Express and tracks whatever event is currently highlighted in the log window.



More Information on Event: Opens a web page that may contain additional details about the port and/or IP address involved in the event.

Report selected Event: Submits the highlighted event to the HackerWatch reporting system.

The Help Menu

All of the help for Hack Tracer and NeoTrace Express is stored online. This means that in order to view online help information you must be connected to the Internet. Using centralized online help enables us to provide you with the very latest available information and links to additional helpful material.

Contents: Displays the Help file table of contents.

Check for Updates: Connects to Hack Tracer headquarters and checks for a newer version of the program. *Note: If you have* Check for new version of program *selected in the Options dialog box, Hack Tracer will automatically perform this check approximately once each month.*

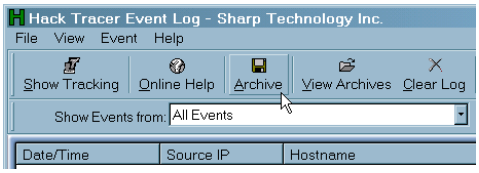
Simulate Attack: Connects to Hack Tracer headquarters and links you to a site which will test your ports and report on the effectiveness of Hack Tracer in protecting your system. If you are not online you will be prompted to connect.

Hack Tracer Homepage: Takes you to a web site with information on Hack Tracer.

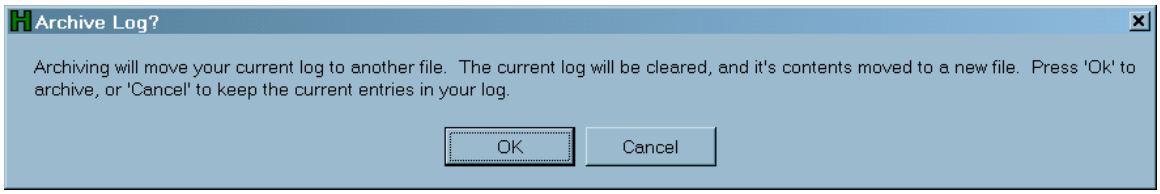
About Hack Tracer: Displays copyright and current version information.

Archiving functions

Hack Tracer's log archiving functions are accessible from the pull down File menu (described above) or the icon button bar (described below). The archive feature allows you periodically save your event logs as well as retrieve old logs for review. It is good practice to archive your log periodically. This will keep the number of events to a manageable level and make it easier for you to spot suspicious patterns of activity. It also helps you to clear out older events that are no longer of interest.

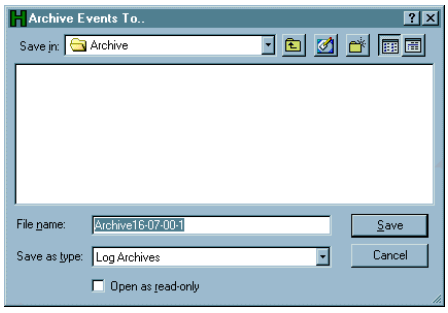


When you click on Archive Current Log in the pull down File menu OR click on the Archive icon in the button bar (shown at right), you will get a warning



message (shown below) advising you that the contents of the current log are about to be removed.

If you click OK, an Explorer window will appear. Hack Tracer offers you a default file name as well as a default location for your archive file. The default location is a folder called Archive within the Hack Tracer folder. We recommend that you keep the default location. The log file name includes the current date in day-month-year sequence. A file saved on July 16, 2000 would be saved as "archive16-07-00-1.elog" If you saved another archive file on the same date the date code would end with "-2."



Clicking Cancel either in the initial warning window or in the Explorer window stops the archiving process and leaves your current log untouched.

Clicking on View Previous Archives in the pull down File menu OR clicking on the View Archives icon in the button bar will open an Explorer window listing all of the archive files in the default location. Click on an archive file to load it into the event window.

The selected archive file will replace the current log in the Event Log window and the View Archives button *will remain depressed*. When you are done reviewing the archive file, click on the depressed View Archive button. The data being viewed by the Log Viewer will return to the current event log.

Button Bar

The button bar below the drop down menu bar offers quick access to the most commonly used Hack Tracer functions.

Show Tracking: Launches NeoTrace Express and tracks the currently highlighted event.

Online Help: Connects you to the Hack Tracer web site and the complete online help facility.

Archive: This function clears the current event log and saves its entire content to an event log file (.elog). *Note: the archive functions are described in detail in the preceding section.*

View Archives: Opens an Explorer window and shows you all of the previously saved archive files in the default location. You may open and view any archive file. While viewing an archive file, this button will appear to be depressed. When you are done with the archive file click on the depressed button. Your archive file will vanish and the current log will reappear in the Event Log window.

Clear Log: This function clears the current log without saving it in an archive file. There is a warning message that asks you to confirm this choice before the log is cleared.

News: Contacts Hack Tracer headquarters and checks for news updates. If you are not online, you will be prompted to connect to your ISP.

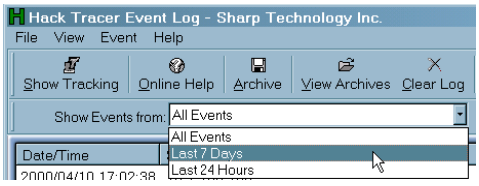
Options: Opens the previously described Options dialog box.

Clicking on the Hack Tracer logo art at the right side of the button bar connects you to the Hack Tracer home page. If you are not online, you will be prompted to connect.

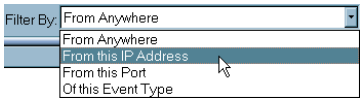
Selection list / Filter

Just below the button bar there are two drop down selection lists that serve as log view filters.

Show Events From: this menu offers you a choice of All Events, events in the Last 7 days, and events in the Last 24 hours. *While other events may vanish, given your choice, they are still in the current log.*



Filter By: This drop down menu offers *From Anywhere* (i.e. the entire log), *From this IP Address* (will limit list to those events which originated with the currently highlighted IP address), *From this Port* (will limit list to those events which attempted to contact the currently highlighted port), and *Of this Event Type* (will limit list to those events which were of the same type as the currently highlighted event). Events which vanish when the event filter is applied remain in the current log.



The Event Window

The default Event Window shows the Date and Time of the event, the source IP, the registered Hostname at that address (if available) and the event type.

The detailed view (which may be turned on in the Options dialog box) adds the Destination Port and Source Port information for the event to the columns displayed.

Destination and Source Ports

The destination and source ports are significant because different applications listen and transmit on different ports. Ports are assigned to standard protocols like SMTP or HTTP so that programs know what port to try a connection on. So the destination port for TCP packets indicates the application or server they are looking for. In the case of UDP packets the source port has more significance.

In most cases, the event detail window will provide specific information regarding the port which was probed. It may also list known hacker uses for the port.

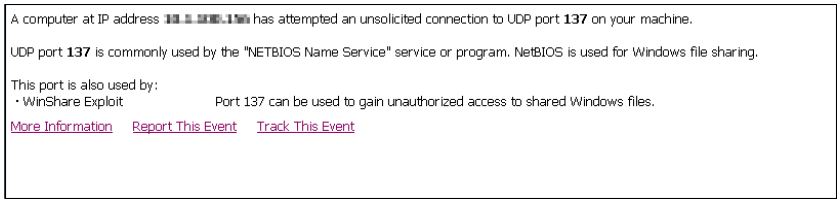
Adjusting and sorting columns

Column width may be adjusted by moving the cursor over the heading bar until it changes shape. Simply click and drag.

The data in the event log can be sorted into almost any order you desire with a simple click of your mouse. In the example at right, the user has clicked at the top of the Destination Port column to sort the events in ascending order based on the port number. A second click would reverse the sort going from highest value to lowest. You may sort date and time, source IP, event type, etc.

Event details

The lower window in the Event Log shows details of any event highlighted in the upper window. It may, as in the example shown below, list known instances of attacks that have been known to access a particular port.



At the bottom of the detail window there are three links: *More Information, Report This Event* and *Track This Event.*

More Information accesses the Hack Tracer site to see if additional information is available on this type of intrusion event.

Click on Report this Event to contact the HackerWatch reporting site and upload an automatic report on this event. Log in is fully automated and you will be told how many reports you have submitted to-date.

Status Bar

At the bottom of the Event Log is a status bar. If you are online, your current IP address will be generally shown at lower left together with your machine name (if it has one) and NetMask address. At the right side of the status bar you will see a summary of the current log. If you are using a filter you can expect to see a difference between the events shown and the total number of events in the current log.

Using NeoTrace Express (NTX)

When you installed Hack Tracer, one of the first things you ran was the Location Wizard. In order to accurately show the trace path on its default map view, NeoTrace Express needs that information.

Running a Trace

When you click on *Track It* in the **Event Detected** window OR click the *Show Tracking* button in the **Event Log** window, Hack Tracer launches NeoTrace Express.

The trace begins immediately. Unless you disabled the sound in the Options setup window, you will hear a series of beeping sounds and the display will begin updating. The default opening display map shows the entire globe. You can zoom in (left click) or zoom out (right click) on the map during or after the trace.

The process may seem a bit confusing at first. The sounds tell you that the trace is progressing. The green node dots appearing on the map won't make sense until the trace is completed.

If your home location is properly entered, the map trace will originate there and end at the registered location where your intrusion event originated. The number of "nodes" on the map varies considerably and will give you some idea of the complexity of the Internet.

You can stop a trace before completion by hitting the '***X***' button at the lower right corner of the NeoTrace Express window.

Trace

Click on the Trace tab to reveal a complete list of all the Internet nodes between you and the source of your intrusion event. While performing the trace, NeoTrace Express has collected all the information available about the nodes along the route. The default Node display shows the name or IP address of each node and the ping time to that node. The number of nodes can vary from a few to two dozen or more.

The node or nodes closest to your node (you will always be node 1) are probably recognizable as belonging to your Internet Service Provider (ISP). Smaller ISPs pass their traffic off to interstate or international carriers while some very large ISPs carry their own traffic cross country.

"Ping time," the column headed RT (Return Time), indicates the length of time it takes for a packet of data to travel from your computer to that distant computer and back in microseconds (ms). The time only indicates the round trip to that one computer and is not directly related to the time on previous nodes.

The Ping time is greatly affected by the amount of traffic on your connection. If you see a sudden and dramatic worsening of ping times it is usually due to a web page transfer, file download or E-mail poll. The slower your connection the larger the effect traffic will have on the ping time.

Sudden jumps in the ping time when tracing overseas generally indicates the point where the traffic moves over a long distance connection. Usually the node on the short end of the jump is the last node in your country, and the next node is the first node in the next country. This is particularly apparent in traces that cross the Pacific or Atlantic.

If you find this information interesting you may want to consider acquiring a full-featured version of NeoTrace which can be utilized for tracing to any Internet IP address worldwide and not just those causing intrusion alerts on your system.

Network and Registrant

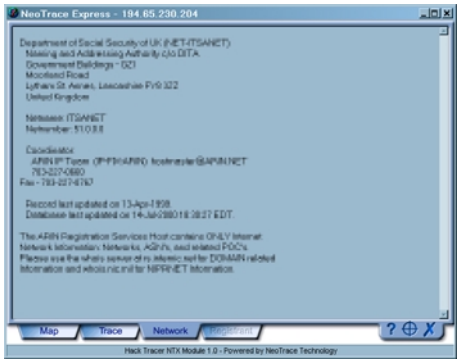
The next two tabs in the NeoTrace Express window reveal what is known as the WhoIs information (literally "Who is...?). The accuracy of this information is generally good for IP addresses in most of North America and Europe.

The format for the information returned from international servers may be a bit different, quite long, and not as easy to understand.

Unfortunately the majority of countries do not have WhoIs servers available. This makes retrieval of information on them impossible.

Network

The Network information tells you the name and location of the servers that are responsible for providing the DNS info for the domain or IP address which originated your intrusion event.



Registrant

The registrant information, if complete, will contain the following data:

1. Company name and address.
2. Domain name (for example, neoworx.com).
3. Contact information for administrative, billing and technical needs.
4. Date information detailing the creation date and the most recent update of this information.

The actual location of a computer will frequently not match the information provided by the WhoIs results. The mailing address may be for a separate location or a post office box, and in many cases another company may host the web site or other server. Fortunately for you, pinning down the exact location for the source of a hacker intrusion is not your concern. If you report the intrusion to HackerWatch headquarters and the trace information you obtained is complete, the data should be more than enough for authorities to locate the source of the intrusion.

Navigating the Map

Take a few moments to learn how to navigate the map view.

Zooming and scrolling the Map View

To scroll the map hold down the left mouse button and drag on the map. The map will move according to how far you moved the mouse. To zoom click the left mouse button without dragging to zoom in, and click the right mouse button to zoom out.

Understanding the Map View

The Map View is a geographical representation of the trace from your computer to another computer connected to the Internet. The location of your computer is set with the Home Location Wizard, if your computer does not appear in the correct place on the map it is because you have not set your location correctly.

There are several types of map node icons used to represent nodes on the trace map. The icon shape indicates the reliability of the location information. In the case of nodes in the middle portion of the trace they are only placed on the map if an accurate location is known. The target/end node however may be placed *even if verified information is not available*. This means that while nodes in the middle portion of the trace are placed reliably, the end node location may not be. Obviously dots in the middle of a straight line represent unknown locations and are provided only as indicators of the nodes relative position in the trace and not as the actual node location.

Due to the dependency of the Map View on lookups of geographic data this view is the slowest to provide useful information in the initial stages of a trace. You may want to view the Trace display tab while the trace is in progress.

Trouble-shooting

Nearly all the features of Hack Tracer require that you be connected to the Internet. If you encounter a problem you have not seen before, first ensure that your Internet connection is still working.

Disabling and uninstalling Hack Tracer

To temporarily disable Hack Tracer, click on the tray icon and then click on Unload Hack Tracer. You will be warned that you are disabling your system's online protection. To reactivate Hack Tracer click on Hack Tracer Tray Utility in the Hack Tracer program group.

If you should decide to uninstall Hack Tracer click on Uninstall Hack Tracer in the Hack Tracer program group. After the uninstall routine has run you will be asked to reboot your system to complete the process.

Failure to Boot

It is theoretically possible for unplanned interaction between Hack Tracer and another application (such as another firewall or email monitoring program) to cause your system to not be able to boot normally. Symptoms would be either a lock up on boot or a 'Blue Screen of Death' error, also known as an Access Violation.

In the unlikely event you experience this type of problem you should reboot your computer and perform a 'safe mode' boot. Press F8 during the boot process to get a menu from which you can choose the safe mode boot. After the computer has booted in safe mode you should then uninstall either Hack Tracer or the other application that is causing the conflict.

Support Options

Use the online help to view topics of interest and the FAQ (Frequently Asked Questions). Since the online help can be updated at any time it is likely to contain information not found in the PDF or printed manual.

To view options for human-assisted support visit the Hack Tracer home page.

An Intruder Alert

What does it mean?

In most cases it means nothing because, as we have pointed out repeatedly, most intrusions are benign. Remember that Hack Tracer is protecting you and that you have nothing to worry about. Examine the log event carefully and try to determine if the intrusion was a real hack attempt.

Look at the host name for the source IP. If it's your Internet service provider or came from an organization whose site you visiting, it can be dismissed as a benign or nosey probe. If the host name is blank but the event information column shows “UDP stream expired” it was probably data being sent to you after you stopped a page load or moved to another site without canceling a data request. Again, a benign event.

If you do not recognize the host name or you are certain it is from an IP address that you were not visiting, you may well have experienced a real hack attempt.

What should I do about it?

If you are reasonably certain that the intrusion attempt was not friendly, report it. Contact the HackerWatch site. If you have not previously registered, take a moment to do so.

Hack Tracer will automatically provide the HackerWatch database with the most critical information needed to pinpoint the source and the type of intrusion you experienced. This information is regularly reviewed to determine activity patterns. If an event or series of events are determined to be real hacker attacks, they will be reported to internet authorities for further action.

What information does my system provide to HackerWatch?

The loss of privacy that can occur when everything is computerized is disturbing. When you report a hacker intrusion to HackerWatch we do collect some data from your computer and this is fully explained right here.

Hack Tracer does not report any personal information of yours to our server. We collect all of the information specific to your intrusion event: the date and time, the IP address of the intruder, the node name. This gives us enough information to uniquely identify the source of your incursion and we can report this information to authorities.

It makes us happy to know that there are many thousands of people using and benefiting from this program, and the information you supply will help make the Internet a safer place.

GLOSSARY OF TERMS

BPS (Bits-Per-Second) The speed at which data is transmitted in bits-per-second. A 28.8 modem can move 28,800 bits per second.

Browser
A program that is used to look at various kinds of Internet resources.

Cookie
A Cookie most commonly refers to a piece of information sent by a Web Server to a user's Web Browser. The Browser software sends it back to the Server whenever the browser makes additional requests from the Server. When you visit a site you have previously visited and are welcomed by name, thank (or blame) a cookie that told them who you are.
When a Web Server attempts to send a cookie to your computer, you may get an Intruder warning from Hack Tracer

Country Codes
In the course of tracing intrusion attempts you will sooner or later encounter a country code. The country code is a two-letter tag at the end of a site URL which identifies the country where the site is located. See the on-line help for a detailed list of country codes.

Domain Name System/Server (DNS)
The Domain Name System simplifies Internet navigation. Computers on the internet can only be found at their numerical IP address (e.g., 206.216.115.4). An address like "neoworx.com" makes sense to a human but a DNS server must match it up to its real IP address. The DNS server databases are updated regularly as new domain names are registered.

Domain Name
An Internet site's unique name, which can consist of two or more parts separated by dots (neoworx.com, whitehouse.gov, www.chubu.ac.jp).

DSL
DSL or Digital Subscriber Line is an increasingly popular method of connecting to the Internet over regular phone lines. DSL offers the advantage of a relatively high speed connection at prices substantially lower than ISDN connections. In theory DSN has a download speed limit of 9 megabits per second and an upload limit of 640 kilobits per second. In reality, and dependent of your provider's equipment as well as your system equipment, you can expect anything from about 1.5 megabit download/128 kilobit upload (Asymmetric DSL) to 384 kilobits in both directions (Symmetric DSL).

E-mail


Electronic Mail, messages sent via the Internet or within a company LAN or WAN. E-mail attachments in the form of EXE (executable) files or VBS (Visual Basic script) files have become increasingly popular as a means of transmitting viruses and Trojans.

Finger
Software that allows you find out more information about an Internet user such as their real name and if they are logged on to a network or the Internet.

Firewall
Hardware and/or software designed to keep unauthorized outsiders from tampering with a computer system. That system may be a standalone computer, a small LAN or a company-wide network or WAN with thousands of users. Hack Tracer is a software firewall effective in protecting standalone computers and small networks..

FTP
FTP or File Transfer Protocol is used to move files between Internet sites. When you "download" a file from a site, e.g. a virus program update, you are using FTP. Public FTP sites from which you can download program or driver updates are usually anonymous FTP servers that permit anonymous logins. Private FTP sites normally require a Login name as well as a password and those who use them regularly, usually make use of specialized FTP programs.

Hit
A "hit" is a single request from a web browser for a single item from a web server. A single web page with text and graphics will require multiple hits in order to acquire the complete page. The number of hits required to get the entire page, the size of graphic files, the speed of your connection and the transfer speed of all the various nodes between your browser and the web site all add up to a page that appears in seconds or one that comes in very slowly.

HTTP
HyperText Transfer Protocol moves hypertext (HTML) files on the Internet from the server you are visiting to the browser you are viewing with.

Internet
The Internet consists of a huge number of inter-connected networks that use the TCP/IP protocols for the location and transfer of data. The Internet evolved from a linking of university and college computers (in the late 1960s and early 1970s) funded by the U.S. Department of Defense and called the ARPANET. The Internet today is a global network of almost 100,000 independent networks.

Intranet
A private network, usually inside an organization, that functions very much like the Internet. It has become common practice to permit access to such Intranets from standalone computers used by students or employees off-campus or off-site. Firewalls, login procedures and passwords are designed to provide security.


IP Number

The Internet Protocol Number or IP address is a unique number consisting of four parts separated by dots (e.g. 63.227.89.66). Every computer of the Internet from the largest server to a laptop communicating through a cell phone has a unique IP number. Not every computer has a domain name but everyone has an IP.

ISDN

Integrated Services Digital Network is yet another way of moving data at high speed over existing phone lines (see DSL). ISDN is widely available and with increasing pressure from DSL providers, cost is coming down. While a 128,000 Bps rate is theoretically possible, most users find that reality is in the 56,000 to 64,000 Bps range.

ISP

Internet Service Provider. This is the service you subscribe to in order to connect with the Internet. It may be a small local company with a few thousand subscribers, a regional company (e.g. uswest.net) or a nationwide mega-provider like A.O.L. or AT&T WorldNet. Most ISPs sell you a connection, nothing more. They provide no security whatsoever and if your system is hacked and subsequently damaged or destroyed, they don't owe you the time of day. On the other hand if you are a hacker or violate any of the fine print in your ISP service agreement, they can cut off your Internet access before you can say World Wide Web.

LAN

Local Area Network. Two or more computers that are linked together and able to share programs, data and/or peripherals

MIME

Multipurpose Internet Mail Extensions, MIME, is the standard format used for transmitting files attached to E-mail messages (pictures, sound files, video files, executables, etc.). The attachment is encoded when it leaves your computer and is decoded and restored to its original form at the receiving end. The specific encoding/decoding format for a given file varies with the file type. Once in a great while you may receive a MIME format attachment, essentially an attachment that was not properly encoded or decoded. If you open it and look at it, it will appear to be indecipherable gobbledygook.

Modem

MOdulator/DEModulator. Your modem takes data you are sending and modulates it so that it can be transmitted over an analog voice phone line. Your modem accepts incoming modulated data and demodulates it so that it is usable by your computer. The earliest modems required the user to place the telephone handset into a cradle with padded apertures for the two ends of the handset. Speeds were in the range of 300 to 1,200 Bps. With improvements in error correction, modems today under ideal conditions can transmit data at over 50,000 Bps. over a single phone line. DSL and ISDN connections offer even higher speeds. These days the term modem is frequently used to describe external network connection devices that don't actually perform any modulation or demodulation, such as DSL and Cable modems which are actually digital end-to-end.


Network
When you connect two or more computers, you create a network. When you connect two or more networks you create an internet (lower case "i").

Node
A single computer connected to a network. When you ask Hack Tracer to perform a trace, the NeoTrace Express trace list shows you all of the nodes between your computer and the source of your intrusion event. The nodes simply served as connection points in passing along the data.

Packet Switching
This is the method used to move data on the Internet. The data you are sending or receiving is broken up into pieces, each piece carrying the IP address of where it is going and where it is coming from. Billions of these pieces are passing through the Internet at any given time and the major node servers are sorting these pieces and routing them at incredible speeds. The E-mail you are reading or the web page you are looking at has been reassembled and delivered to your monitor after traveling across town or around the world and, best of all, you don't have to give it a moments thought.

Password
A code (usually alphanumeric) you use to gain access to your computer or to a given program or to a web site.

PING
Packet Internet Groper is a program used to determine whether a specific IP address is accessible. A packet is sent to the specified address and the program waits for a reply. Programs like NeoTrace and NeoTrace Express use PING to identify and/or troubleshoot Internet connections. In addition to identifying the target site, these programs also note all of the nodes the data passed through between the two ends of the connection. The most popular shareware PING utility is the full-featured version of NeoTrace.

Port
A place where information goes into and/or out of a computer, e.g. a conventional analog modem is connected to a serial port. The port numbers in TCP/IP communications are virtual values used to separate traffic into application-specific streams. The ports (destination and source) captured in the Hack Tracer Event Log are significant because different applications listen and transmit on different ports. Ports are assigned to standard protocols like SMTP or HTTP so that programs know what port to try a connection on. The destination port for TCP packets indicates the application or server being looked for. In the case of UDP packets the source port has more significance.

PPP
Point to Point Protocol allows a computer to use a regular phone line and modem to make TCP/IP connections to the Internet.

Server


A computer or software that provides specific services to software running on other computers. The “mail server” at your ISP is software that handles all of the incoming and outgoing mail for all of your ISP's users. A server on a LAN is hardware that constitutes the primary node on the network. It may also have software which provides specific services, data or other capabilities to all of the client computers attached to it.

SLIP
Serial Line Internet Protocol used to connect a computer to the Internet by way of a phone line. PPP is replacing SLIP because it is more efficient.

SMTP
Simple Mail Transfer Protocol is a set of rules governing the sending and receiving of E-mail on the Internet.

SNMP
Simple Network Management Protocol is a set of standards governing communication with devices connected to a TCP/IP network. This communication takes the form of Protocol Data Units or “PDU’s.”

SSL
Secure Sockets Layer, a protocol created by Netscape Communications to enable encrypted, secure communications across the Internet. Internet banking, securities and e-commerce sites commonly use SSL.

TCP/IP
Transmission Control Protocol/Internet Protocol, the protocols that make the Internet possible and that make it possible for your computer to be part of the Internet.

Top Level Domains
Top Level Domains (TLDs) are the most common domain name extensions. The most familiar of these is the ubiquitous “DOT COM” but there are others in common usage:

COM	US Commercial
EDU	US Educational
GOV	US Government
INT	International
MIL	US Military
NET	Network
ORG	Non-Profit Organization

Trojan Horse
A type of computer worm or virus which comes to you disguised as a desirable program. The name is based on the famous Trojan Horse which was left outside the walls of Troy by a departing army which appeared to have given up its plans of conquest. The horse, which concealed a band of soldiers, was brought into the walled city by its unwary inhabitants. The


soldiers opened the gates of the city in the middle of the night and Troy was destroyed by the returning troops.

URL
Uniform Resource Locator, the standard format for Internet addresses.

USENET
More commonly called Newsgroups, USENET is a decentralized worldwide community made up of almost 20,000 discussion groups covering almost every conceivable area of interest. Rule of thumb: don't accept software from someone you meet in a newsgroup or chat room!

VPN
Virtual Private Network, a network which makes use of the Internet to connect computers that are in different locations. Communication is encrypted for security.

WAN
Wide Area Network, a network of computers that covers an area larger than a single building or campus. In the past WANs have been private networks connecting geographically separated offices of the same organization. WANs are rapidly being replaced by the Internet and the wide use of VPNs.

WWW
The World Wide Web or just “The Web.” Many people think of this in terms of what is accessible to their browser but in reality the web now encompasses all of the resources that make up the Internet including such things as FTP sites, USENET, and much more.

Index