Creating a Cellular Device Investigation Toolkit: Basic Hardware and Software Specifications

SEARCH High-Tech Crime Training Services
Rev. May 2009

Keith Daniels
(keith.daniels@search.org)

Lauren Wagner
(lauren.wagner@search.org)

The following is a description of the basic hardware and software specifications required to recover data from cellular devices. The High-Tech Crime Training Services staff of SEARCH Group, Inc., in cooperation with law enforcement agencies throughout the United States, developed these specifications.

The field of cellular device data recovery is constantly changing. It is necessary that a budget include money for equipment and software upgrades.

The products listed here are not intended to be part of an exclusive or exhaustive list; they are merely examples of products available in this field. Where prices are listed, those numbers are approximate. If you would like specific purchase recommendations or have suggestions of hardware and software to add to the list, please contact SEARCH Training Services staff at 916/392-2550.

SEARCH

THE NATIONAL CONSORTIUM FOR JUSTICE
INFORMATION AND STATISTICS

7311 Greenhaven Drive, Suite 145 • Sacramento, California 95831

Phone: (916) 392-2550 • Fax: (916) 392-8440 • Internet: www.search.org

TOOLKIT COMPONENTS

You will need to have either a laptop or a desktop computer to retrieve information from the cell phone. Using a laptop has a number of advantages, including being able to take it into the field and work on phones onsite.

The computer you use should have USB 2.0 and FireWire. A USB (universal serial bus) connector is necessary for the cables to connect to the phone. FireWire is needed to connect a DVR (digital video recorder) to the computer to capture data that is not otherwise retrievable.

Cables (including Bluetooth and IR) are the most important components connecting the cell phone to the computer. If you cannot connect to the cell phone, you will have to use a DVR or a ZRT to gather the information.

HARDWARE

Cellebrite UFED System
$3,999
http://www.cellebrite.com

This standalone device assists in criminal investigations and is used to extract electronic evidence from mobile phones and PDAs. Supports 95% of all cellular phones in the market today. Field extraction of data ensures that a suspect's phone can be examined before the individual has a chance to destroy or erase data. Subsequent annual upgrade kits are $899.

Secure ViewKit for Forensics
$2,701
http://www.datapilot.com

Kit includes DataPilot Secure View Software CD; extended universal cable set; individual cables; SIM card reader; Bluetooth adapter, IRDA connector; and hardware key. All mobile content of varying formats, including recent calls, contacts, calendar, to dos, SMS, pictures and video can be acquired from the majority of handsets. Kit comes with 2-year free software updates to support new phones and all required cables. If you order via telephone, mention that you are working with **J. Martinez**. A yearly maintenance fee is $1600.

Device Seizure and Device Seizure ToolBox
$1,595
http://www.paraben-forensics.com/catalog/

Device Seizure gathers data from supported phones and devices. Device Seizure ToolBox is the cables for the supported phones. They are available individually at a cost of $895 for Device Seizure and $749 for the Device Seizure ToolBox. A one-year maintenance subscription is $180.

.XRY
$9,490 One year Kit License
http://www.teeltech.com

Retrieves all information stored on a mobile telephone and creates a report. Subsequent annual licenses are $4620.

USB reader for SIM cards
(GSM phones)
(Model ACR38T-IBS)
$35.05
http://www.smartcardfocus.com/

All GSM (Global System for Mobile Communications) phones have a SIM (Subscriber Identity Module) card and need a reader to read and retrieve the data off the card.

iGo
http://www.igo.com

The iGo Solution Finder locates power adapters and tips. Purchase one power adapter for $30; individual tips as needed for $10.

DC Lab Power Supply 0-15V/3A Digital Display with Backlight
$79.95
http://www.vellemanusa.com

This wall plug-in device charges cell phone batteries and will run a cell phone without a battery.

Neutrino
$1,750
http://www.guidancesoftware.com

This is a mobile phone acquisition tool that integrates with EnCase® v6, allowing you to analyze both mobile phone and computer evidence at the same time. Initial purchase price listed here includes a one-year maintenance/subscription fee. Subsequent annual fees are $1,000.

Paraben's CSI Stick
$199
http://www.paraben-forensics.com/catalog/

A portable cell phone forensic and data gathering tool.

SOFTWARE

SEARCH Investigative Toolbar
Free
http://www.searchinvestigative.ourtoolbar.com
This invaluable tool provides investigative links contained visually on either Firefox or Internet Explorer. This tool includes a cookie cleaner, a history cleaner, and a cache cleaner.

BitPim
Free
www.bitpim.org

BitPim fully supports only a limited number of CDMA phone models. It can pull the file system of most CDMA phones.

Oxygen Forensic Suite 2
$999
http://www.oxygen-forensic.com

A mobile forensic software for analysis of cell phones, smartphones and PDAs.
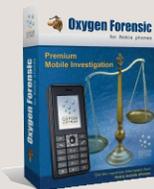
Oxygen Phone Manager (Forensic Edition)
$299
http://www.opm-2.com/

This program works with many Nokia phones and a limited number of Samsung phones.

Paraben's Sim Card Seizure
$129
http://www.paraben-forensics.com/catalog/

Recover deleted sms/text messages and perform comprehensive analysis of SIM card data.

MOBILedit! Forensic
$399
http://www.mobiledit.com/

MOBILedit! primarily deals with GSM phones. The latest version will support some CDMA (code division multiple access) phones.

TULP2G
http://tulp2g.sourceforge.net
This is a forensic software framework for extraction and decoding of data stored in electronic devices.

Nextel iDEN Phonebook Manager
Free
http://idenphones.motorola.com/iden/support/software/organizer_upd.jsp

This is the phone manager for Nextel phones. It can be used to retrieve information off cell phones.

Media Downloader for iDEN-compatible Phones
Free
http://idenphones.motorola.com/iden/support/software/html/media_download.html

If the phone has the Media Center or My Pictures feature, this software can be used to download the media (videos and pictures).

floAt's Mobile Agent
Free
http://fma.sourceforge.net/index2.htm

This is a phone editing tool that allows users to easily manage all of the personal data stored in their phones. This product will work on some Sony Ericsson phones.

VISUAL/AUDIO CAPTURE

Digital Video Camera
$250 to $450

Any good quality digital video camera will work along with a desktop tripod. We have used the Canon VR700 with good results. You will need a FireWire cable and a FireWire connection on your computer and Windows Movie Maker.

Desktop Tripod
$40

Vise
$20

ZRT
$950
http://www.fernico.com

ZRT streamlines the process of taking high-resolution photographs of screen displays and merges these photos into custom-designed report templates.

Audacity
Free
http://audacity.sourceforge.net/

This product is used to record conversations from a cell phone to another device.

CELL PHONE SIGNAL CONTAINMENT

Signal Disruption Bag
Varies from $29.99 to $150

A signal disruption bag is a device you can place a cell phone into so that it cannot receive any signals. This prevents changes from taking place in the phone due to receiving a signal. These bags are not perfect. Consider wrapping the cell phone in three layers of aluminum foil and then placing it in the bag or an arson can.

Arson Cans
Free

Arson cans are available through your local fire department or fire marshal. For cell phone investigative purposes, you must use arson cans, not empty paint cans.

Aluminum Foil

Most cell phones wrapped in three layers of aluminum foil are unable to receive a signal.

Cell Phone Signal Disruption Device
Varies up to $500
http://www.globalgadgetuk.com/yo50.htm

These devices will disrupt the local cell phone signals by preventing the phone from using the control channels to communicate with the cell tower. Using this device will generate .6 watts of power (using 2 antennas). It should disrupt all signals within about 10 meters. However, this may not work because some cell phones have antenna that put out more than .5 watts of power and can overpower the disrupter.

> **NOTE**: Use of cell phone signal disruption devices may be in violation of federal law. Check with your legal advisor before using.

Cellular Device Data Recovery
Preparation Considerations and Troubleshooting

Keith I. Daniels
Computer Training Specialist

and

Lauren Wagner
Computer Training Specialist

HOW TO USE THIS GUIDE

Agencies should develop their own procedures and policies. It is **imperative** that once procedures are developed, they be adhered to for every data recovery effort. Taking shortcuts may result in data not being recovered or potential evidence being excluded from the case.

This guide is intended to provide recommendations, troubleshooting strategies and issue resolution regarding cellular device data recovery. It does not replace or supersede any policies, procedures, rules and ordinances applicable to your jurisdiction's data recovery activities. The contents of this guide should be considered as suggestions only. It is not legal counsel and should not be interpreted as a legal service.
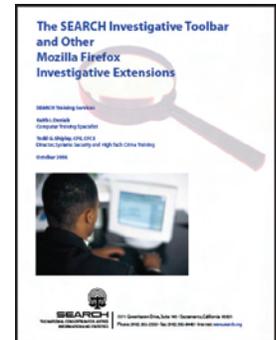
Mobile device data recovery is not always a straightforward process. The purpose of this guide is to provide the data recovery specialist with a basic knowledge of equipment setup and troubleshooting issues that may be encountered during the process. This is not an exhaustive guide, as considerations and issues may vary by device, make, model and software used. Furthermore, many of the suggestions provided in this guide may have to be repeated to successfully obtain the data required.

The process for recovering data from cellular handheld devices may require the specialist to utilize more than a single program or tool. In fact, several different programs or tools may be required to facilitate locating and retrieving all pertinent data. Some of these programs and tools may be forensically sound, while others may not. It is for this reason that we suggest using the term "data recovery" rather than "forensics" to describe the entire process.

Computer and Workspace Considerations

The following suggestions will enhance your ability to successfully begin the process of data recovery:

- A clear workspace with sufficient space.
- A standalone computer, preferably one specific to mobile device data recovery.
- To avoid potential conflicts, the computer should be limited to as few installed programs as possible.
- Microsoft Outlook should not be installed on the computer, because some of the programs may write information to or from it.
- Update software as often as possible. Make note of the date and time of these updates and the version number.
- Do not use an external USB hub unless it has a separate power supply.
- Install the Firefox Web browser and the SEARCH Investigative Toolbar for Firefox or Internet Explorer on the machine. For instructions, download *The SEARCH Investigative Toolbar and Other Mozilla Firefox Investigative Extensions* document from the SEARCH Website at **http://www.search.org/files/pdf/toolbarfirefox.pdf**. The **Cell** dropdown menu on this toolbar provides access to links that are of investigative importance.
- Create a file structure that can be copied or replicated for later cases.

Pre-examination Considerations

Prior to conducting data recovery from a handheld device, you should take a number of preparatory steps. This helps to ensure that data of potential evidentiary value will be gathered and presented in an effective and timely manner. (You may be working with an investigator who has collected the device and is investigating the case.) These steps are:

STEP 1: Review documented legal authorization before attempting any data recovery.

STEP 2: Triage with the investigator to establish exactly what data is to be recovered; this must be documented.

STEP 3: Have the investigator complete a Handheld Device Evidence Processing Request form (similar to the one included in Appendix A).

STEP 4: Begin a Seized Handheld Device Analysis Worksheet (similar to the one included in Appendix B).

STEP 5: Complete the Handheld Device Analysis Control Sheet (similar to the one included in Appendix C). This sheet is a running list of devices that you have previously conducted data recovery from. This becomes a good court reference that can be used to show your previous experience in this area; it also acts as a database in the event that a device of similar make and model is investigated.

STEP 6: Document the condition of the device, particularly possible damage.

STEP 7: Capture images of the front and back of the device.

STEP 8: If the device is off, remove the battery. Capture images of the device behind the battery.

STEP 9: Obtain information about the device: make, model, ESN, etc. Add this information to your Seized Handheld Device Analysis Worksheet (Appendix B).

STEP 10: Establish that the handheld device has a charged battery. This may involve using a voltmeter. Note: The voltage is usually indicated on the inside of the battery, as are the positive and negative connections (+ -).

STEP 11: If required, charge the device with an appropriate charger. If using a variable-level battery charger, do not charge the battery to a higher capacity than listed either on the battery or documentation. Set the charger to a level lower than the maximum capacity of the battery.
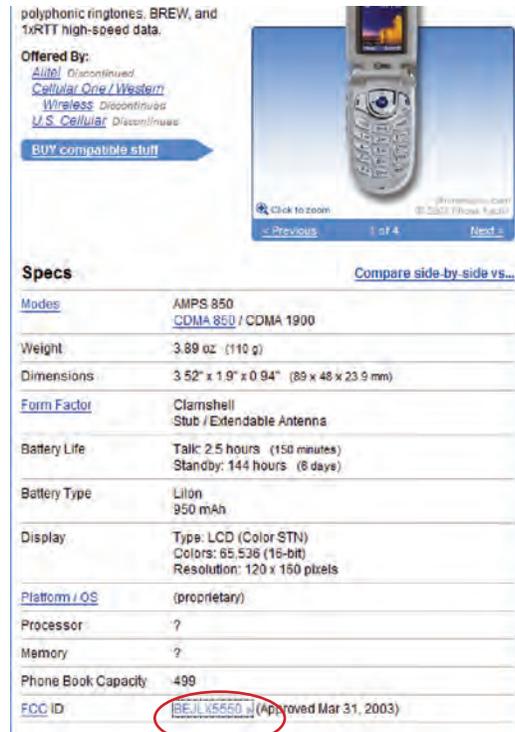
Step 12: Utilizing the SEARCH Investigative Toolbar (for instructions, see white paper at **http://www.search.org/files/pdf/toolbarfirefox.pdf**), navigate to **www.phonescoop.com** and research the device by entering the make and model into the search bar and clicking **Jump**, as illustrated in Figure 1.

Figure 1. Phone Scoop Search Bar

STEP 13: Capture the Phone Scoop page using Snagit in scrolling mode.

STEP 14: From Phone Scoop, locate and download the manual for the device, as shown in Figures 2 and 3. For the manual you require, scroll down to the FCC ID field and click on the device model, as shown in Figure 2.

Figure 2. Locate Device Model

STEP 15: The FCC requires the manual for every phone to be sent to them for documentation. Clicking on **Detail** under the Display Exhibits heading (Figure 3) provides the download page.

Figure 3. Access Download Page for Device Manual

STEP 16: Place the manual and Phone Scoop snags into the evidence folder.

STEP 17: Review any databases that may prove useful to aid in the data recovery.

STEP 18: Locate which connection method will provide communication with the device: cabling, infrared, Bluetooth, etc.

STEP 19: Establish what data can be recovered for the particular device make and model by reviewing the Web site of each piece of software that is available to you.

STEP 20: Select the software to be utilized first.

STEP 21: Attempt to make a connection between the device and the software.

Connect the Device and Troubleshoot

Choose the correct cable that will connect the device to the computer for potential data recovery. Connect it to the computer. Drivers may or may not install automatically.

- Open the program that came with the cabling that you are using to connect the device to the computer.
- Turn on the device.
- Attempt to establish connection with the device using the procedure outlined by the software.
- If connection is not made, there are several procedures to try:
  o Check that the cable and device are connected properly.
  o Establish the integrity of the cable end that connects to the device and check for possible damage.
  o Unplug the cable from the USB port on the computer and re-insert it into the same port.
  o Unplug the cable and re-insert it into another USB port. This will reload the driver.
  o Turn off the phone, remove the battery and wait for at least 30 seconds to drain any resident capacitor. This is particularly true with Motorola phones.
  o Turn off the computer, disconnect any cables and cold-boot the computer.
  o **Repeat all previous steps at least once, and possibly as many as five or more times.**

Use Device Manager to Create a Shortcut for Easy Access

What is Device Manager?

Device Manager is one of the most useful diagnostic tools in the Windows operating system. It lets you see all of the devices attached to your computer, and which resources they are each using. When a piece of hardware is not working, the offending hardware is highlighted where the user can deal with it. The list of hardware can be sorted by various criteria.

Regardless of the recovery software you are using, it is valuable to establish which port the cabling and software is using to communicate. DataPilot, for example, has a Device Manager button, but others may not.

Frequently utilizing Windows Device Manager can be invaluable in troubleshooting handheld device data recovery. Establishing connectivity with the device can be the most difficult hurdle to cross. Utilizing Device Manager can aid in this process. It is useful to create a shortcut to Device Manager and run it from the taskbar, providing easy access to this valuable tool.

To accomplish this, right-click an empty space on the desktop; click on **New**, then click on **Shortcut**, as shown in Figure 4.
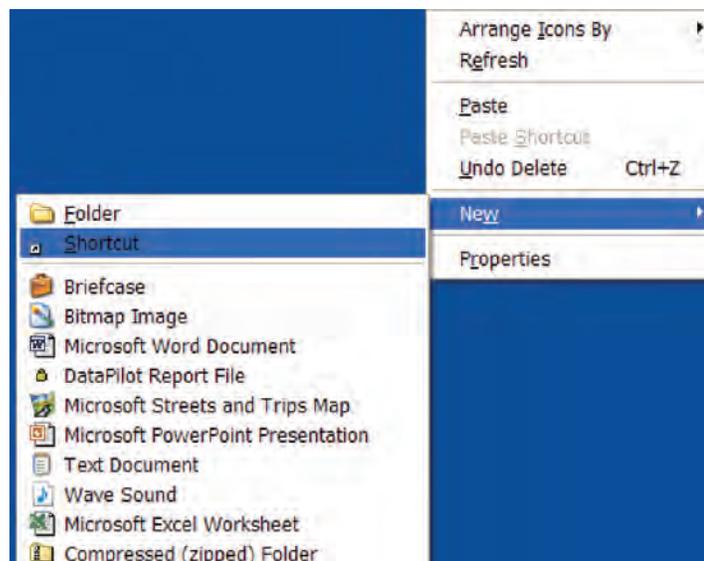

Figure 4. Device Manager Shortcut

A 'Create Shortcut' screen will appear (Figure 5). Enter **DEVMGMT.MSC** in the "Type the location of the item" box and click **Next.**
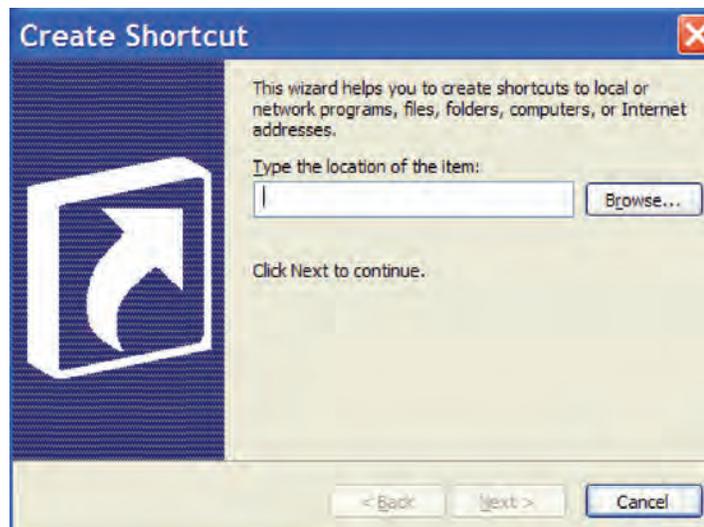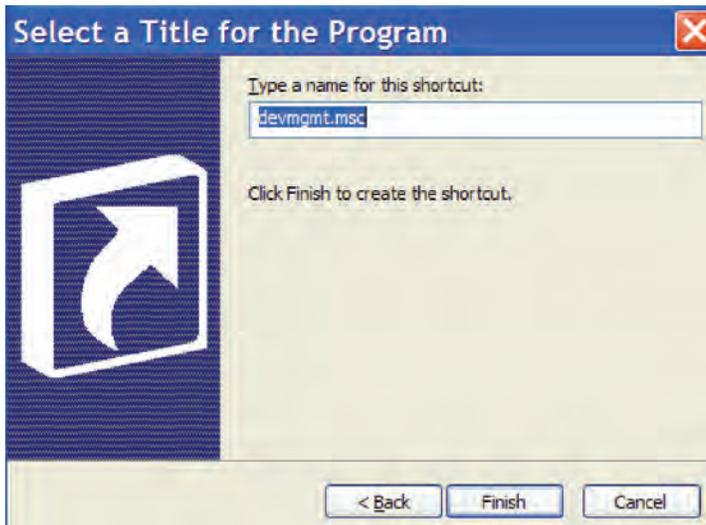

Figure 5. Create Shortcut Screen

The 'Select a Title' screen (Figure 6) asks you to type a name for the shortcut you're creating. Enter **Device Manager** in the "Type a name for this shortcut" box and click **Finish**.

Figure 6. Device Manager Title Screen

A shortcut icon should appear on the desktop (Figure 7). Drag this icon onto the taskbar at the bottom of the screen for quick access during the troubleshooting process. To gain access, single-click the icon.

Figure 7. Device Manager shortcut on desktop

The manual way to get to the Device Manager is to right-click on **My Computer>Properties>Hardware>Device Manager.**

Troubleshooting Considerations

External devices communicate with the computer by COM ports (communication ports). For example, most people have a serial port on their computer. These are used to attach peripheral hardware. The serial port is always COM1. If you are using a serial cable, you will have to make sure you change the port to COM1.

In addition to the COM ports that devices can communicate on, there has to be a program that will take the data coming in and allow your computer to deal with it in a coherent fashion. That requires a device driver. Whenever you install a new device, a device driver is installed. Some device drivers come with Windows. For example, the device driver allows you to use external hard drives and thumb drives. Other devices have their own device driver. If you installed the hardware properly, when you insert the cable for the first time, it should detect the cable and load the proper drivers. If you are using COM1, no drivers are loaded. If you load a device driver once on USB 1, when you plug it in a second time it will not require a second install (unless you uninstall the drivers, which is discussed later). If you install the same device on USB 2 (or any different USB port), you will have to install the device driver for that USB port.

Installing Drivers for Cables

Figure 8. Installing drivers for cables

Figure 9. Installing drivers for cables

Figure 10. Installing drivers for cables

With Device Manager open, click the Plus (+) beside **Ports (COM & LPT)** to open it (Figure 11).
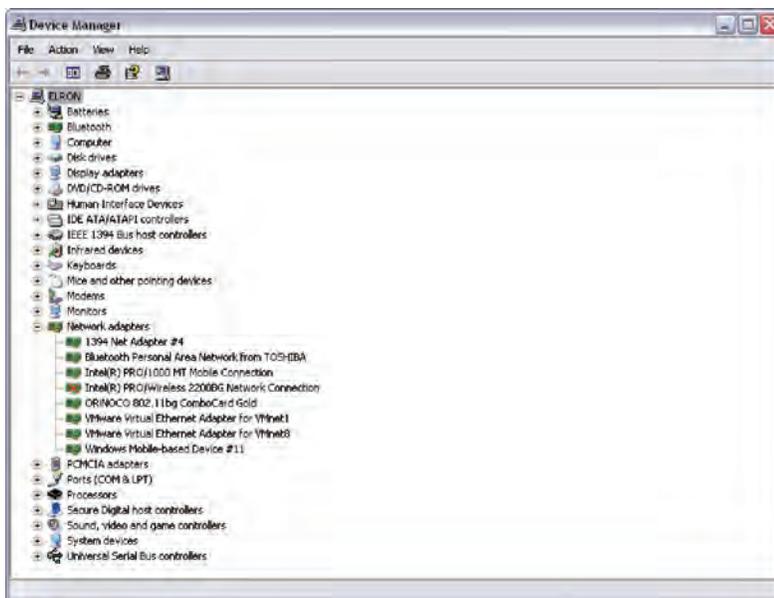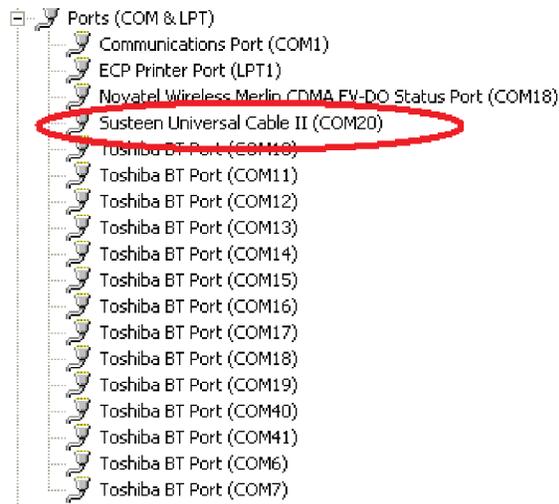

Figure 11. Installing drivers for cables

When you are using cables plugged into your USB port, the easiest way to see what port your cable is on is to look at the Port section.

If you are using DataPilot cables, it is pretty easy to see what COM port they are using.

Figure 12. Installing drivers for cables

Figure 12 shows that the Susteen cable is on COM20. When you first install the cable (whatever cables you are using), look at the lower-right corner of the computer to see what hardware is detected. If you are using DataPilot, it often will show up as Susteen Universal Cable II. This indicates what you would look for in the COM ports.

When you plug the device into the cable for the first time, the new hardware wizard may come up. For example, if you plug in a Samsung or Motorola phone, the new hardware wizard will activate and you will install a Susteen USB modem. This will tell you that instead of looking for Susteen Universal Cable, you will have to look for the Susteen USB Modem. This will allow you to properly identify the correct COM port. Without using the correct COM port, you will never access the phone.

Troubleshooting may require that you uninstall the drivers. This will force Windows to reload them when you plug in the device. This is done from within Device Manager and right-clicking on the appropriate port that you wish to uninstall.

Click on **Uninstall**. Leave the device in until you uninstall the driver. Then remove the device and cold-boot the computer (turn it off, as opposed to using the **Restart** option). When it is successfully rebooted, insert the device and Windows should reinstall the drivers for you.

A Final Word

Each of the software tools that you use for device data recovery will have different nuances. Practice with the tool to find other workarounds. This process can be frustrating and discouraging, but "If at first you don't succeed, try, try and try again."

For other important investigative papers, visit the SEARCH High-tech Crime Publications page at **http://www.search.org/programs/hightech/publications.asp**. Contact the authors at **keith@search.org** or **lauren@search.org**.

Appendix A

Electronic version available on request

Case Number _____

Handheld Device
Evidence Processing Request

Detective _____ **Badge** _____

Date Seized _____ **Report #** _____

Suspect Name _____ **Item #** _____

Check all items taken:

☐ **Handheld Device**   ☐ **Separate Sim Card(s)**   ☐ **Holder/case**

☐ **Charger**   ☐ **Other Media**   ☐ **Software**

☐ **Data Cable**   ☐ **Sim Card Reader**

SEARCH
The National Consortium for Justice Information and Statistics

Appendix B

Electronic version available on request

Seized Handheld Device Analysis Worksheet

Case Number _____

Case Details:

Investigative Section _____
Investigator _____
Case Agent _____
Evidence Item Number _____

Date Received for Analysis _____
Date of Analysis _____
Type of Case _____
Primary Offense _____

Device Details:

Handheld Device Owner _____ (if known)
Handheld Device Condition _____ (visible damage)
Manufacturer _____
Model _____
Serial Number _____
IMEI / ESN _____
Cell Telephone Number ( ) _____
Service Provider _____
PIN Number _____
SIM Card Number _____

IMSI Number _____
Direct Connect Number _____
Type of Device:

☐ CDMA
☐ TDMA
☐ GSM
☐ Other _____

Device Time _____
Atomic Time _____

Device Features:

Custom Ringtones ☐	Memo/Note/To Do ☐	SMS ☐	Data Capable ☐
Ringtone ID ☐	Fixed Dialed Numbers ☐	MMS ☐	Multiple Language Support ☐
Camera Enabled ☐	Phonebook ☐	EMS ☐	Voice Memo ☐
Picture ID Capable ☐	Call Log ☐	USB ☐	Multiple numbers per name support ☐
Video Capable ☐	Last Number Dialed ☐	Hard Drive ☐	Forwarding Enabled ☐
Voice Recorder ☐	Custom Graphics ☐	Voice Command ☐	Bluetooth ☐
Calendar ☐	Expansion Card ☐	GPS Capable ☐	

(over)

Device Particulars:				

Handset Locked	☐ Y ☐ N	PUK Obtained ☐ Y ☐ N Note _____
"Airplane" Mode Capable	☐ Y ☐ N	Enabled? If yes, date _____
Custom Banner	☐ Y ☐ N	If yes, describe _____
Welcome Note	☐ Y ☐ N	If yes, describe _____
Device on when received	☐ Y ☐ N	Device examined for physical damage Y ☐ N ☐
Device Password	_____	
Charger Tip	_____	
Cable	_____	
Program	_____	

Battery Details:

Removed Battery	☐ Y ☐ N	Battery Make _____
Device charged by seizing officer	☐ Y ☐ N	Battery Serial Number _____
		Battery Voltage Capacity _____
		Results from Battery test with voltmeter _____

Notes:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Appendix C

Electronic version available on request

Handheld Device Analysis
Control Sheet

	Date	Case No.	Device Make	Model	DataPilot	Cellebrite	BitPim	Cell Seizure	Oxygen	Other	Manually	SIM	Yes	No
								Software Used					Complete	
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														

Francis X. Aumand III
Chairman

Ronald P. Hawley
Executive Director

Kelly J. Peters
Deputy Executive Director

SEARCH
7311 Greenhaven Drive, Suite 145 • Sacramento, CA 95831
(916) 392-2550 • (916) 392-8440 (fax) • www.search.org

Cellular Device Data Recovery
Preparation Considerations and Troubleshooting

Keith I. Daniels
Computer Training Specialist

and

Lauren Wagner
Computer Training Specialist

HOW TO USE THIS GUIDE

Agencies should develop their own procedures and policies. It is **imperative** that once procedures are developed, they be adhered to for every data recovery effort. Taking shortcuts may result in data not being recovered or potential evidence being excluded from the case.

This guide is intended to provide recommendations, troubleshooting strategies and issue resolution regarding cellular device data recovery. It does not replace or supersede any policies, procedures, rules and ordinances applicable to your jurisdiction's data recovery activities. The contents of this guide should be considered as suggestions only. It is not legal counsel and should not be interpreted as a legal service.

Mobile device data recovery is not always a straightforward process. The purpose of this guide is to provide the data recovery specialist with a basic knowledge of equipment setup and troubleshooting issues that may be encountered during the process. This is not an exhaustive guide, as considerations and issues may vary by device, make, model and software used. Furthermore, many of the suggestions provided in this guide may have to be repeated to successfully obtain the data required.

The process for recovering data from cellular handheld devices may require the specialist to utilize more than a single program or tool. In fact, several different programs or tools may be required to facilitate locating and retrieving all pertinent data. Some of these programs and tools may be forensically sound, while others may not. It is for this reason that we suggest using the term "data recovery" rather than "forensics" to describe the entire process.

Computer and Workspace Considerations

The following suggestions will enhance your ability to successfully begin the process of data recovery:

- A clear workspace with sufficient space.
- A standalone computer, preferably one specific to mobile device data recovery.
- To avoid potential conflicts, the computer should be limited to as few installed programs as possible.
- Microsoft Outlook should not be installed on the computer, because some of the programs may write information to or from it.
- Update software as often as possible. Make note of the date and time of these updates and the version number.
- Do not use an external USB hub unless it has a separate power supply.
- Install the Firefox Web browser and the SEARCH Investigative Toolbar for Firefox or Internet Explorer on the machine. For instructions, download *The SEARCH Investigative Toolbar and Other Mozilla Firefox Investigative Extensions* document from the SEARCH Website at **http://www.search.org/files/pdf/toolbarfirefox.pdf**. The **Cell** dropdown menu on this toolbar provides access to links that are of investigative importance.
- Create a file structure that can be copied or replicated for later cases.

Pre-examination Considerations

Prior to conducting data recovery from a handheld device, you should take a number of preparatory steps. This helps to ensure that data of potential evidentiary value will be gathered and presented in an effective and timely manner. (You may be working with an investigator who has collected the device and is investigating the case.) These steps are:

STEP 1: Review documented legal authorization before attempting any data recovery.

STEP 2: Triage with the investigator to establish exactly what data is to be recovered; this must be documented.

STEP 3: Have the investigator complete a Handheld Device Evidence Processing Request form (similar to the one included in Appendix A).

STEP 4: Begin a Seized Handheld Device Analysis Worksheet (similar to the one included in Appendix B).

STEP 5: Complete the Handheld Device Analysis Control Sheet (similar to the one included in Appendix C). This sheet is a running list of devices that you have previously conducted data recovery from. This becomes a good court reference that can be used to show your previous experience in this area; it also acts as a database in the event that a device of similar make and model is investigated.

STEP 6: Document the condition of the device, particularly possible damage.

STEP 7: Capture images of the front and back of the device.

STEP 8: If the device is off, remove the battery. Capture images of the device behind the battery.

STEP 9: Obtain information about the device: make, model, ESN, etc. Add this information to your Seized Handheld Device Analysis Worksheet (Appendix B).

STEP 10: Establish that the handheld device has a charged battery. This may involve using a voltmeter. Note: The voltage is usually indicated on the inside of the battery, as are the positive and negative connections (+ -).

STEP 11: If required, charge the device with an appropriate charger. If using a variable-level battery charger, do not charge the battery to a higher capacity than listed either on the battery or documentation. Set the charger to a level lower than the maximum capacity of the battery.

Step 12: Utilizing the SEARCH Investigative Toolbar (for instructions, see white paper at **http://www.search.org/files/pdf/toolbarfirefox.pdf**), navigate to **www.phonescoop.com** and research the device by entering the make and model into the search bar and clicking **Jump**, as illustrated in Figure 1.

Figure 1. Phone Scoop Search Bar

STEP 13: Capture the Phone Scoop page using Snagit in scrolling mode.

STEP 14: From Phone Scoop, locate and download the manual for the device, as shown in Figures 2 and 3. For the manual you require, scroll down to the FCC ID field and click on the device model, as shown in Figure 2.

Figure 2. Locate Device Model

STEP 15: The FCC requires the manual for every phone to be sent to them for documentation. Clicking on **Detail** under the Display Exhibits heading (Figure 3) provides the download page.

Figure 3. Access Download Page for Device Manual

STEP 16: Place the manual and Phone Scoop snags into the evidence folder.

STEP 17: Review any databases that may prove useful to aid in the data recovery.

STEP 18: Locate which connection method will provide communication with the device: cabling, infrared, Bluetooth, etc.

STEP 19: Establish what data can be recovered for the particular device make and model by reviewing the Web site of each piece of software that is available to you.
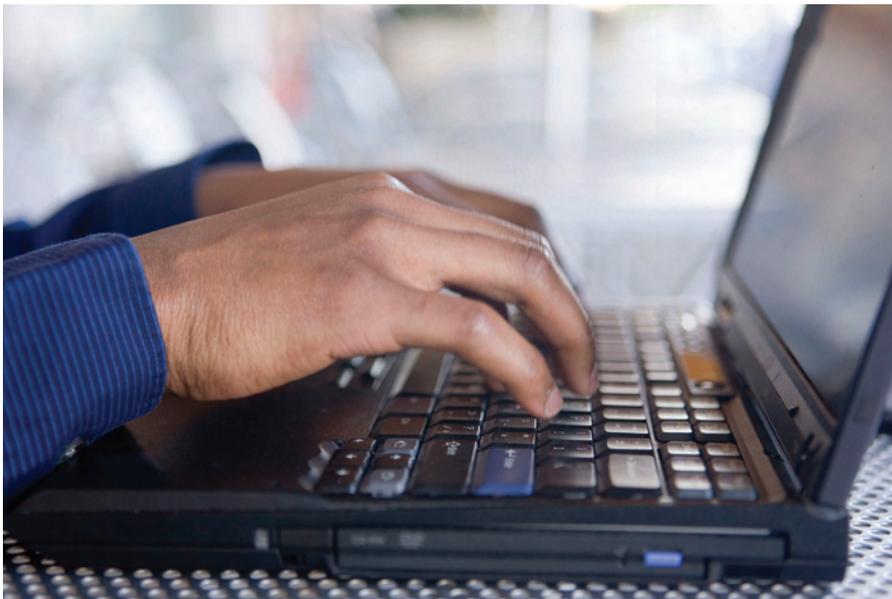
STEP 20: Select the software to be utilized first.

STEP 21: Attempt to make a connection between the device and the software.

Connect the Device and Troubleshoot

Choose the correct cable that will connect the device to the computer for potential data recovery. Connect it to the computer. Drivers may or may not install automatically.

- Open the program that came with the cabling that you are using to connect the device to the computer.
- Turn on the device.
- Attempt to establish connection with the device using the procedure outlined by the software.
- If connection is not made, there are several procedures to try:
  o Check that the cable and device are connected properly.
  o Establish the integrity of the cable end that connects to the device and check for possible damage.
  o Unplug the cable from the USB port on the computer and re-insert it into the same port.
  o Unplug the cable and re-insert it into another USB port. This will reload the driver.
  o Turn off the phone, remove the battery and wait for at least 30 seconds to drain any resident capacitor. This is particularly true with Motorola phones.
  o Turn off the computer, disconnect any cables and cold-boot the computer.
  o **Repeat all previous steps at least once, and possibly as many as five or more times.**

Use Device Manager to Create a Shortcut for Easy Access

What is Device Manager?

Device Manager is one of the most useful diagnostic tools in the Windows operating system. It lets you see all of the devices attached to your computer, and which resources they are each using. When a piece of hardware is not working, the offending hardware is highlighted where the user can deal with it. The list of hardware can be sorted by various criteria.

Regardless of the recovery software you are using, it is valuable to establish which port the cabling and software is using to communicate. DataPilot, for example, has a Device Manager button, but others may not.

Frequently utilizing Windows Device Manager can be invaluable in troubleshooting handheld device data recovery. Establishing connectivity with the device can be the most difficult hurdle to cross. Utilizing Device Manager can aid in this process. It is useful to create a shortcut to Device Manager and run it from the taskbar, providing easy access to this valuable tool.

To accomplish this, right-click an empty space on the desktop; click on **New**, then click on **Shortcut**, as shown in Figure 4.
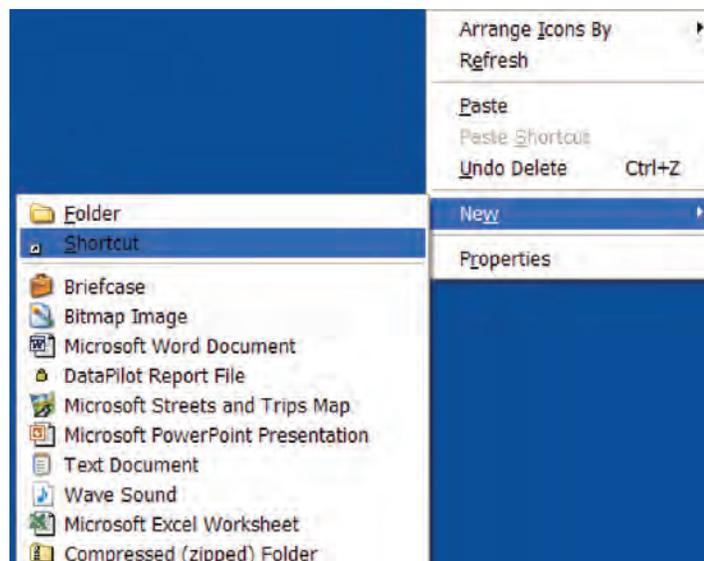

Figure 4. Device Manager Shortcut

A 'Create Shortcut' screen will appear (Figure 5). Enter **DEVMGMT.MSC** in the "Type the location of the item" box and click **Next.**
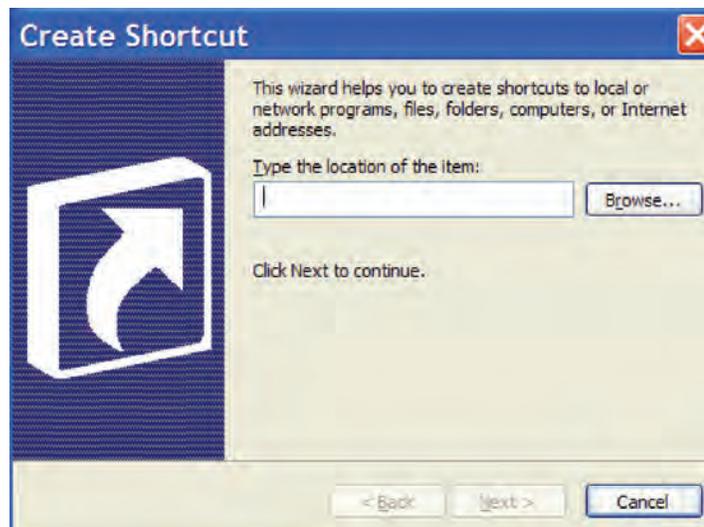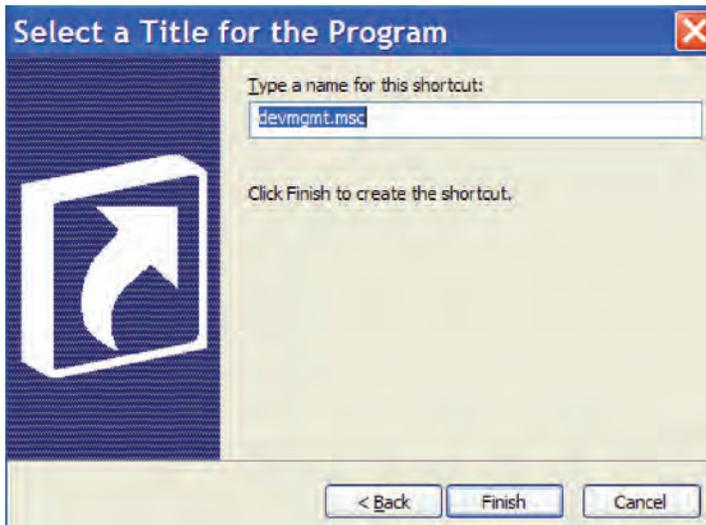

Figure 5. Create Shortcut Screen

The 'Select a Title' screen (Figure 6) asks you to type a name for the shortcut you're creating. Enter **Device Manager** in the "Type a name for this shortcut" box and click **Finish**.

Figure 6. Device Manager Title Screen

A shortcut icon should appear on the desktop (Figure 7). Drag this icon onto the taskbar at the bottom of the screen for quick access during the troubleshooting process. To gain access, single-click the icon.

Figure 7. Device Manager shortcut on desktop

The manual way to get to the Device Manager is to right-click on **My Computer>Properties>Hardware>Device Manager.**

Troubleshooting Considerations

External devices communicate with the computer by COM ports (communication ports). For example, most people have a serial port on their computer. These are used to attach peripheral hardware. The serial port is always COM1. If you are using a serial cable, you will have to make sure you change the port to COM1.

In addition to the COM ports that devices can communicate on, there has to be a program that will take the data coming in and allow your computer to deal with it in a coherent fashion. That requires a device driver. Whenever you install a new device, a device driver is installed. Some device drivers come with Windows. For example, the device driver allows you to use external hard drives and thumb drives. Other devices have their own device driver. If you installed the hardware properly, when you insert the cable for the first time, it should detect the cable and load the proper drivers. If you are using COM1, no drivers are loaded. If you load a device driver once on USB 1, when you plug it in a second time it will not require a second install (unless you uninstall the drivers, which is discussed later). If you install the same device on USB 2 (or any different USB port), you will have to install the device driver for that USB port.

Installing Drivers for Cables

Figure 8. Installing drivers for cables

Figure 9. Installing drivers for cables

Figure 10. Installing drivers for cables

With Device Manager open, click the Plus (+) beside **Ports (COM & LPT)** to open it (Figure 11).
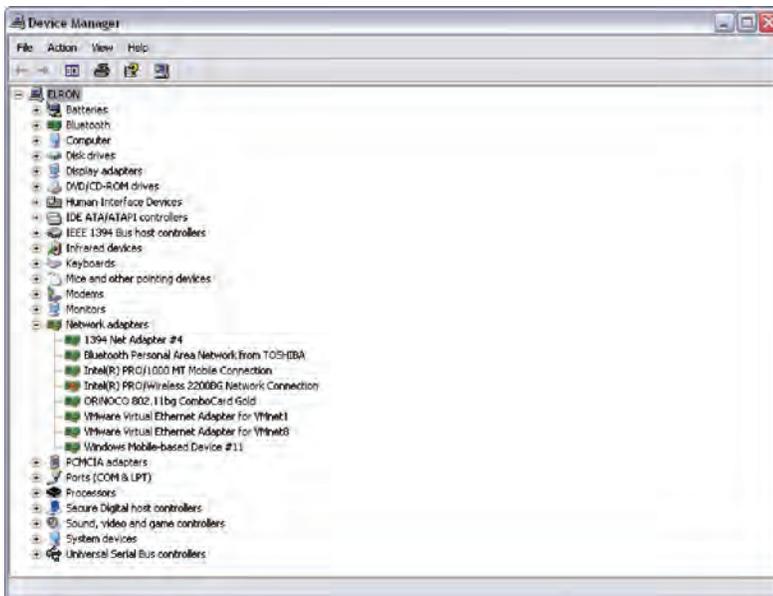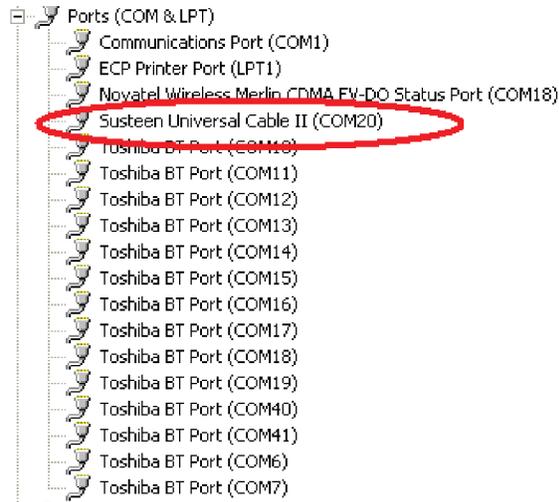

Figure 11. Installing drivers for cables

When you are using cables plugged into your USB port, the easiest way to see what port your cable is on is to look at the Port section.

If you are using DataPilot cables, it is pretty easy to see what COM port they are using.

Figure 12. Installing drivers for cables

Figure 12 shows that the Susteen cable is on COM20. When you first install the cable (whatever cables you are using), look at the lower-right corner of the computer to see what hardware is detected. If you are using DataPilot, it often will show up as Susteen Universal Cable II. This indicates what you would look for in the COM ports.

When you plug the device into the cable for the first time, the new hardware wizard may come up. For example, if you plug in a Samsung or Motorola phone, the new hardware wizard will activate and you will install a Susteen USB modem. This will tell you that instead of looking for Susteen Universal Cable, you will have to look for the Susteen USB Modem. This will allow you to properly identify the correct COM port. Without using the correct COM port, you will never access the phone.

Troubleshooting may require that you uninstall the drivers. This will force Windows to reload them when you plug in the device. This is done from within Device Manager and right-clicking on the appropriate port that you wish to uninstall.

Click on **Uninstall**. Leave the device in until you uninstall the driver. Then remove the device and cold-boot the computer (turn it off, as opposed to using the **Restart** option). When it is successfully rebooted, insert the device and Windows should reinstall the drivers for you.

A Final Word

Each of the software tools that you use for device data recovery will have different nuances. Practice with the tool to find other workarounds. This process can be frustrating and discouraging, but "If at first you don't succeed, try, try and try again."

For other important investigative papers, visit the SEARCH High-tech Crime Publications page at **http://www.search.org/programs/hightech/publications.asp**. Contact the authors at **keith@search.org** or **lauren@search.org**.

Appendix A

Electronic version available on request

Case Number _____

Handheld Device
Evidence Processing Request

Detective _____ **Badge** _____

Date Seized _____ **Report #** _____

Suspect Name _____ **Item #** _____

Check all items taken:

☐ **Handheld Device**　　☐ **Separate Sim Card(s)**　　☐ **Holder/case**

☐ **Charger**　　　　　　☐ **Other Media**　　　　　☐ **Software**

☐ **Data Cable**　　　　　☐ **Sim Card Reader**

SEARCH
The National Consortium for Justice Information and Statistics

Appendix B

Electronic version available on request

Seized Handheld Device Analysis Worksheet

Case Number _____

Case Details:

Investigative Section _____
Investigator _____
Case Agent _____
Evidence Item Number _____

Date Received for Analysis _____
Date of Analysis _____
Type of Case _____
Primary Offense _____

Device Details:

Handheld Device Owner _____
(if known)
Handheld Device Condition _____
(visible damage)
Manufacturer _____
Model _____
Serial Number _____
IMEI / ESN _____
Cell Telephone Number ( ) _____
Service Provider _____
PIN Number _____
SIM Card Number _____

IMSI Number _____
Direct Connect Number _____
Type of Device:
- [ ] CDMA
- [ ] TDMA
- [ ] GSM
- [ ] Other _____

Device Time _____
Atomic Time _____

Device Features:

Custom Ringtones [ ]	Memo/Note/To Do [ ]	SMS [ ]	Data Capable [ ]
Ringtone ID [ ]	Fixed Dialed Numbers [ ]	MMS [ ]	Multiple Language Support [ ]
Camera Enabled [ ]	Phonebook [ ]	EMS [ ]	Voice Memo [ ]
Picture ID Capable [ ]	Call Log [ ]	USB [ ]	Multiple numbers per name support [ ]
Video Capable [ ]	Last Number Dialed [ ]	Hard Drive [ ]	Forwarding Enabled [ ]
Voice Recorder [ ]	Custom Graphics [ ]	Voice Command [ ]	Bluetooth [ ]
Calendar [ ]	Expansion Card [ ]	GPS Capable [ ]	

(over)

Device Particulars:

Handset Locked	☐ Y ☐ N	PUK Obtained ☐ Y ☐ N Note _____
"Airplane" Mode Capable	☐ Y ☐ N	Enabled? If yes, date _____
Custom Banner	☐ Y ☐ N	If yes, describe _____
Welcome Note	☐ Y ☐ N	If yes, describe _____
Device on when received	☐ Y ☐ N	Device examined for physical damage Y ☐ N ☐
Device Password	_____	
Charger Tip	_____	
Cable	_____	
Program	_____	

Battery Details:

Removed Battery	☐ Y ☐ N	Battery Make _____
Device charged by seizing officer	☐ Y ☐ N	Battery Serial Number _____
		Battery Voltage Capacity _____
		Results from Battery test with voltmeter _____

Notes:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Appendix C

Electronic version available on request

Handheld Device Analysis
Control Sheet

	Date	Case No.	Device Make	Model	DataPilot	Cellebrite	BitPim	Cell Seizure	Oxygen	Other	Manually	SIM	Yes	No
									Software Used				Complete	
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														
20														
21														
22														
23														
24														
25														

Francis X. Aumand III
Chairman

Ronald P. Hawley
Executive Director

Kelly J. Peters
Deputy Executive Director

SEARCH
7311 Greenhaven Drive, Suite 145 • Sacramento, CA 95831
(916) 392-2550 • (916) 392-8440 (fax) • www.search.org