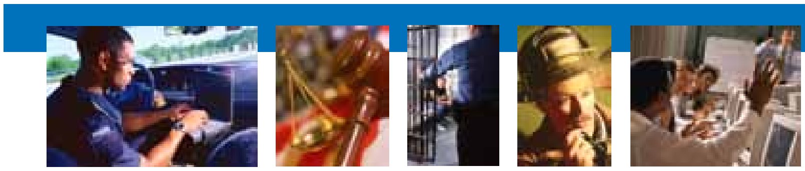


SEARCH TRAINING SERVICES

April 2013

Cellular Device Data Recovery
Preparation Considerations and Troubleshooting

Lauren Wagner
High-Tech Crime 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.

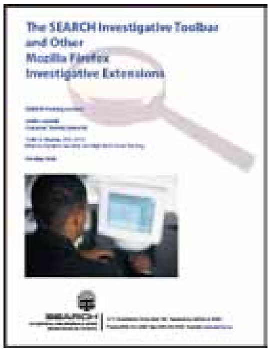
The process for recovering data from cellular handheld devices may require the specialist to utilize more than a single program or tool. In fact, several different programs or tools may be required to facilitate locating and retrieving all pertinent data. Some of these programs and tools may be forensically 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.

SEARCH, The National Consortium for Justice Information and Statistics
7311 Greenhaven Drive, Suite 270 • Sacramento, California 95831 • (916) 392-2550 • www.search.org

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.



The SEARCH Investigative Toolbar and Other Mozilla Firefox Investigative Extensions

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.

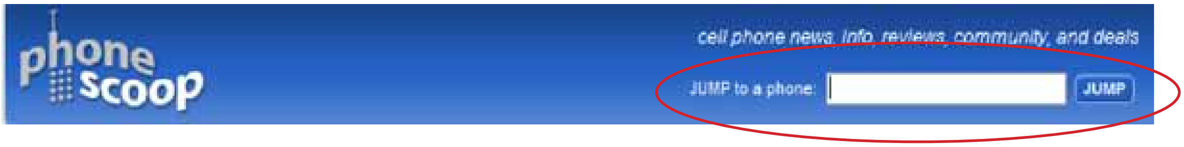
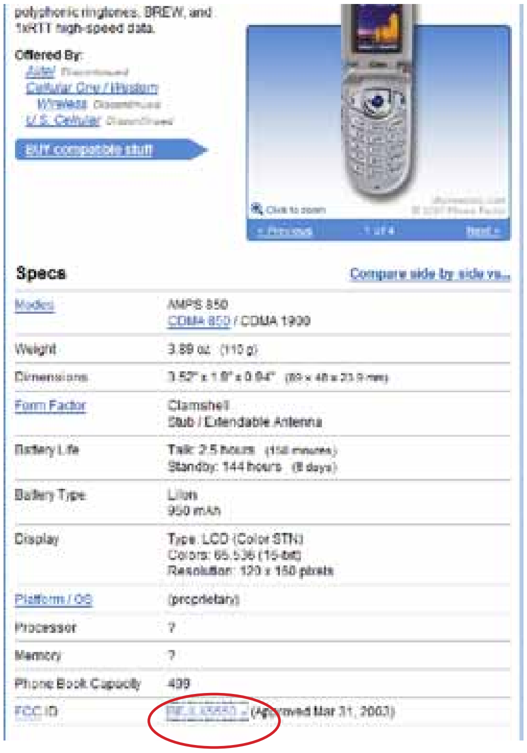


Figure 1. Phone Scoop Search Bar

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.



polyphonic ringtones, BREW, and 1xRTT high-speed data.

Offered By:
Alltel Discontinued
Cellular One / Western Wireless Discontinued
U.S. Cellular Discontinued

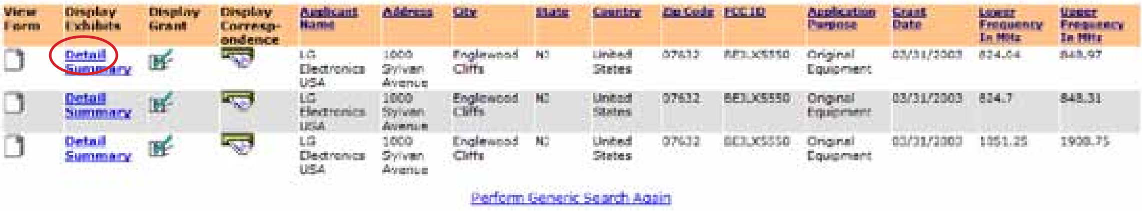
Specs

Compare side by side vs...

Modes	AMPS 850 CDMA 850 / CDMA 1900
Weight	3.89 oz. (110 g)
Dimensions	3.52" x 1.8" x 0.94" (89 x 46 x 23.9 mm)
Form Factor	Clamshell Stub / Extendable Antenna
Battery Life	Talk: 2.5 hours (150 minutes) Standby: 144 hours (6 days)
Battery Type	LiIon 950 mAh
Display	Type: LCD (Color STN) Colors: 65,536 (16-bit) Resolution: 120 x 160 pixels
Platform / OS	(proprietary)
Processor	?
Memory	?
Phone Book Capacity	499
FCC ID	[illegible] (Approved Mar 31, 2003)

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.



View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Grant Date	Lower Frequency In MHz	Upper Frequency In MHz
☐	Detail Summary	✓	✉	LG Electronics USA	1000 Sylvan Avenue	Englewood Cliffs	NJ	United States	07632	BEJLX5550	Original Equipment	03/31/2003	824.04	848.97
☐	Detail Summary	✓	✉	LG Electronics USA	1000 Sylvan Avenue	Englewood Cliffs	NJ	United States	07632	BEJLX5550	Original Equipment	03/31/2003	824.7	848.31
☐	Detail Summary	✓	✉	LG Electronics USA	1000 Sylvan Avenue	Englewood Cliffs	NJ	United States	07632	BEJLX5550	Original Equipment	03/31/2003	1851.25	1908.75

Perform Generic Search Again

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.

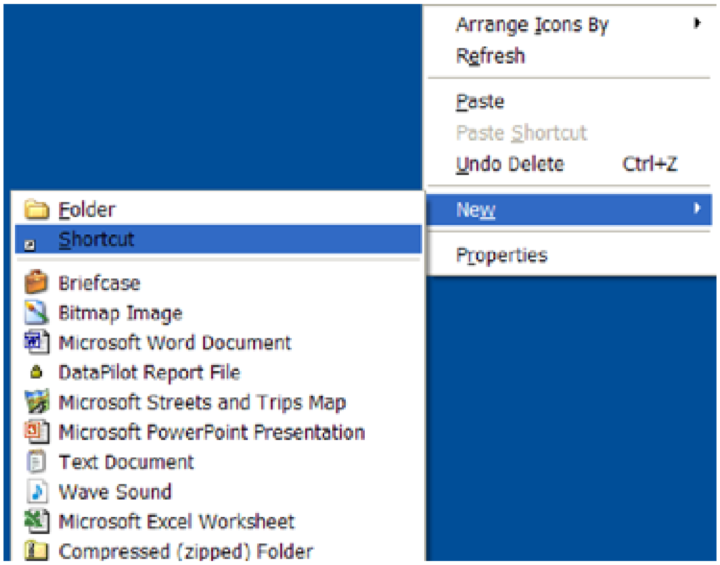
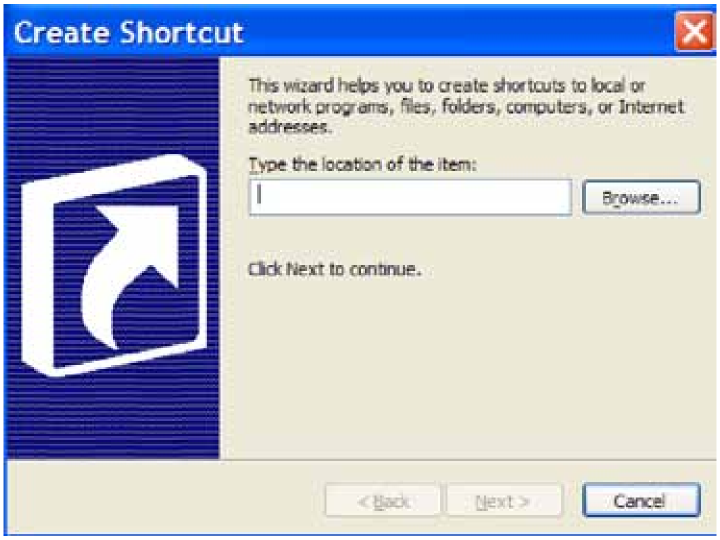


Figure 4. Device Manager Shortcut

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



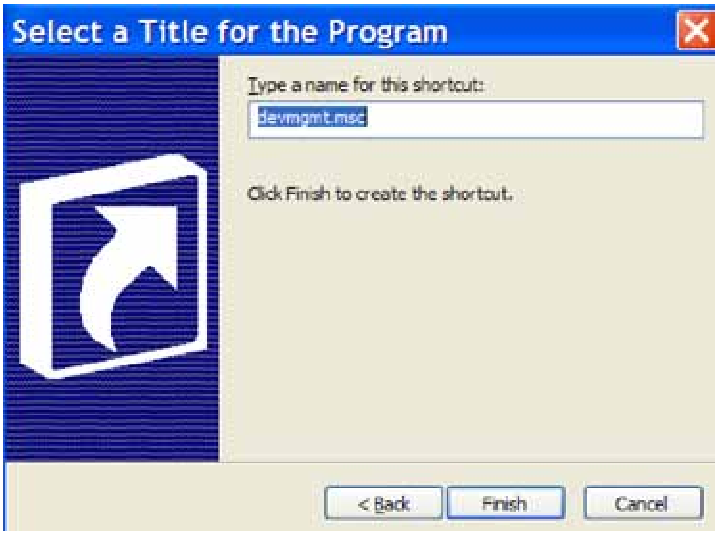
This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

Type the location of the item:

Click Next to continue.

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**.



Select a Title for the Program

Type a name for this shortcut:

devmgmt.msc

Click Finish to create the shortcut.

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.

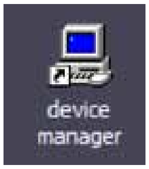


Figure 7. Device Manager shortcut on desktop

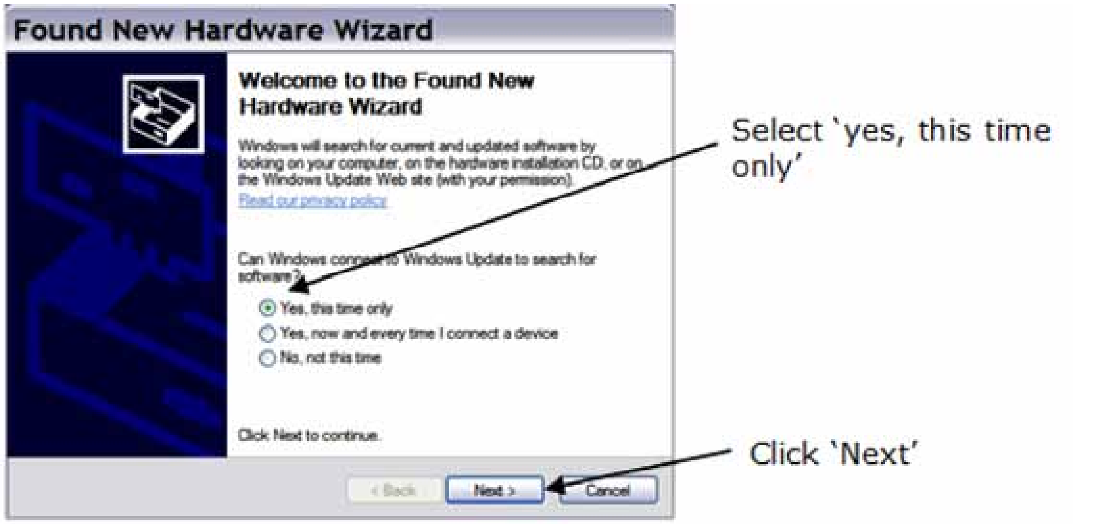
The manual way to get to the Device Manager is to right-click on **My Computer>Properties>Hardware>Device Manager.**

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



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

Can Windows connect to Windows Update to search for software?

● Yes, this time only

○ Yes, now and every time I connect a device

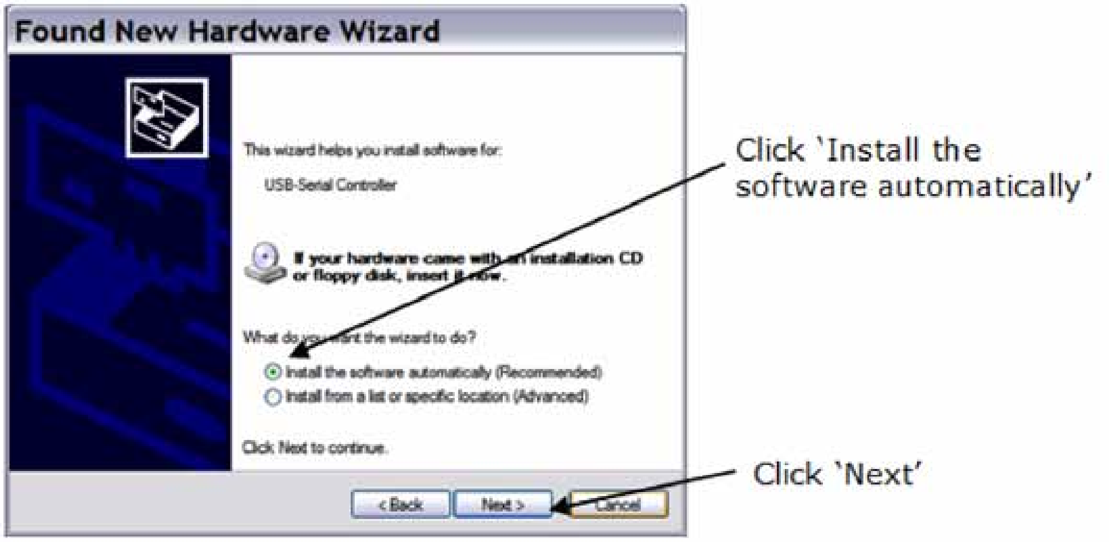
○ No, not this time

Click Next to continue.

Select 'yes, this time only'

Click 'Next'

Figure 8. Installing drivers for cables



Found New Hardware Wizard

This wizard helps you install software for:

USB-Serial Controller

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

● Install the software automatically (Recommended)

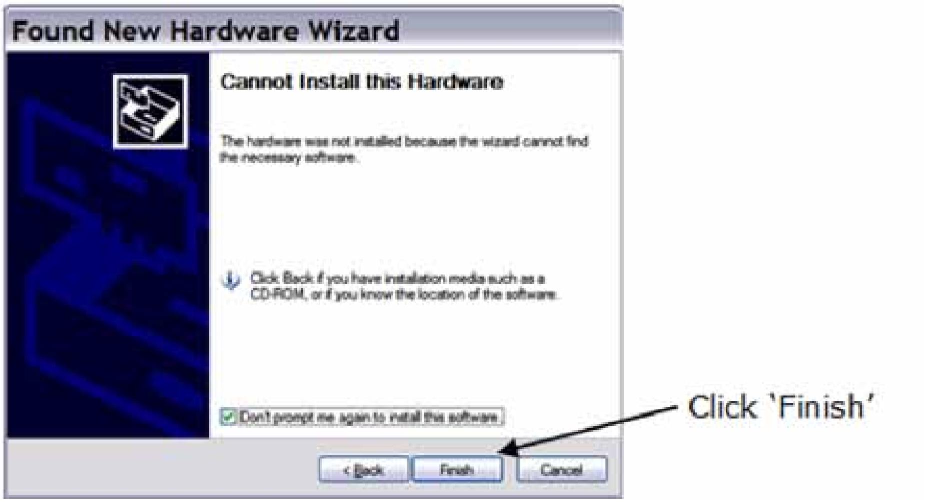
○ Install from a list or specific location (Advanced)

Click Next to continue.

Click 'Install the software automatically'

Click 'Next'

Figure 9. Installing drivers for cables



Found New Hardware Wizard

Cannot Install this Hardware

The hardware was not installed because the wizard cannot find the necessary software.

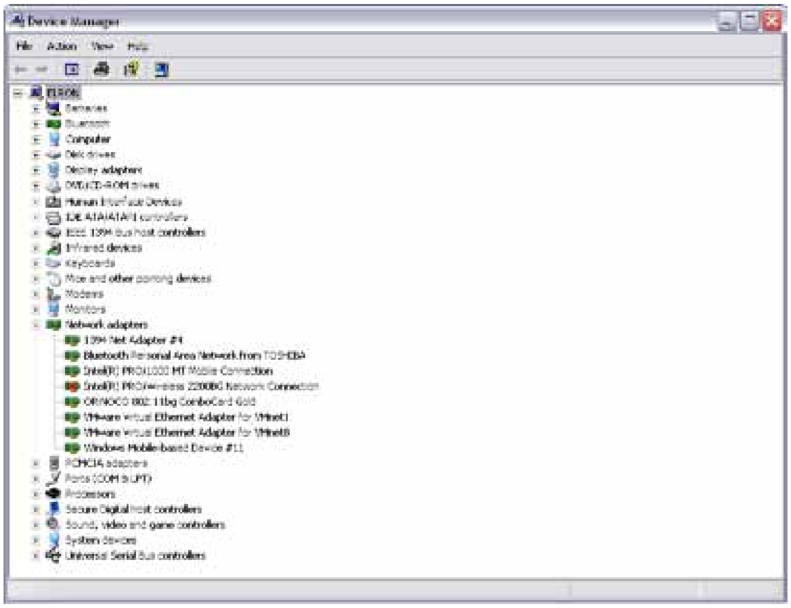
Click Back if you have installation media such as a CD-ROM, or if you know the location of the software.

☑ Don't prompt me again to install this software.

Click 'Finish'

Figure 10. Installing drivers for cables

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

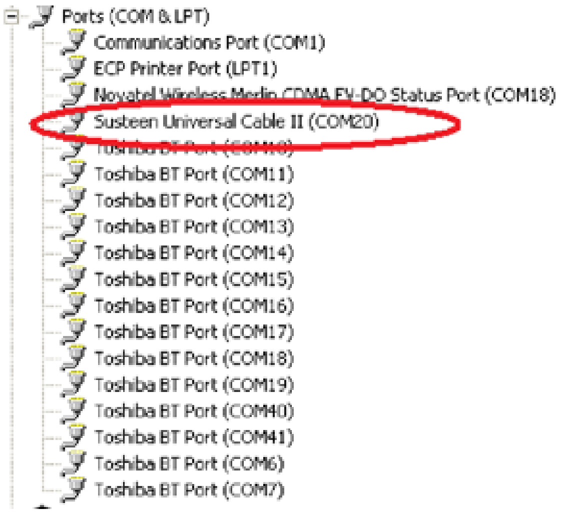


- ELRON
  - Batteries
  - Bluetooth
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - IEEE 1394 Bus host controllers
  - Infrared devices
  - Keyboards
  - Mice and other pointing devices
  - Modems
  - Monitors
  - Network adapters
    - 1394 Net Adapter #4
    - Bluetooth Personal Area Network from TOSHIBA
    - Intel(R) PRO/1000 MT Mobile Connection
    - Intel(R) PRO/Wireless 2200BG Network Connection
    - ORiNOCO 802.11bg ComboCard Gold
    - VMware Virtual Ethernet Adapter for VMnet1
    - VMware Virtual Ethernet Adapter for VMnet8
    - Windows Mobile-based Device #11
  - PCMCIA adapters
  - Ports (COM & LPT)
  - Processors
  - Secure Digital host controllers
  - Sound, video and game controllers
  - System devices
  - Universal Serial Bus controllers

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.



Ports (COM & LPT)
Communications Port (COM1)
ECP Printer Port (LPT1)
Novatel Wireless Merlin CDMA EV-DO Status Port (COM18)
Susteen Universal Cable II (COM20)
Toshiba BT Port (COM10)
Toshiba BT Port (COM11)
Toshiba BT Port (COM12)
Toshiba BT Port (COM13)
Toshiba BT Port (COM14)
Toshiba BT Port (COM15)
Toshiba BT Port (COM16)
Toshiba BT Port (COM17)
Toshiba BT Port (COM18)
Toshiba BT Port (COM19)
Toshiba BT Port (COM40)
Toshiba BT Port (COM41)
Toshiba BT Port (COM6)
Toshiba BT Port (COM7)

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**.

Appendix A

Electronic version available on request

Handheld Device Evidence Processing Request

Case Number____________________________________

Detective____ Badge ______________________________________

Date Seized ____ Report # ____________________________________

Suspect Name _______________________________________ Item # ______________________________________

Check all items taken:

- □ Handheld Device
- □ Charger
- □ Data Cable
- □ Separate SIM Card(s)
- □ Other Media
- □ SIM Card Reader
- □ Holder/case
- □ Software

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

Examiner ________________________

Case Agent ________________________

Investigative Section ________________________

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 ________________________

Cell Telephone Number ________________________

Service Provider ________________________

Serial Number ________________________

IMEI/ESN ________________________

IMSI Number ________________________

SIM Card Number ________________________

Type of Device □ CDMA □ GSM □ Other ________________________

Device Time ________________________

Atomic Time ________________________

(Over)

Device Particulars

Handset Locked □ Y □ N

PUK Obtained □ Y □ N PUK ____________________

Pin/Password ____________________

Pattern lock

● ● ●
● ● ●
● ● ●

Other ____________________

Airplane Mode Enabled □ Y □ N If yes, date ____________________

Device examined for physical damage □ Y □ N

Software Used/Versions and Special Instructions for Connections

Notes

Appendix C

Electronic version available on request

Handheld Device Analysis Control Sheet

					Software Used								Complete	
	Date	Case No.	Manufacturer	Model	Cellebrite Logical	DataPilot	BitPim	Paraben	Cellebrite Physical	Other	Manual	SIM	Yes	No
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														

This project was supported by Cooperative Agreement #2007-DD-BX-K041 by the Bureau of Justice Assistance, U.S. Department of Justice. Points of view or opinions contained in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

SEARCH
7311 Greenhaven Drive, Suite 270 • Sacramento, CA 95831
(916) 392-2550 • (916) 392-8440 (fax) • www.search.org