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

SEARCH High-Tech Crime Training Services
Rev. October 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**. 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

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.

Secure ViewKit for Forensics

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**.

Device Seizure and Device Seizure ToolBox

http://www.paraben-forensics.com/catalog/

Device Seizure gathers data from supported phones and devices. Device Seizure ToolBox includes the cables for the supported phones.

.XRY

http://www.teeltech.com

Retrieves all information stored on a mobile telephone and creates a report.

USB reader for SIM cards
(GSM phones)
(Model ACR38T-IBS)
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.

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

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

Neutrino
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.

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

A portable cell phone forensic and data gathering tool.

SOFTWARE

SEARCH Investigative Toolbar
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
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
http://www.oxygen-forensic.com

A mobile forensic software for analysis of cell phones, smartphones and PDAs.

Oxygen Phone Manager (Forensic Edition)
http://www.opm-2.com/

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

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

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

MOBILedit! Forensic
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
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
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
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

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

Vise

ZRT

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

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

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

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

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.