Mobile Forensics Tools

Technical Report · May 2015

DOI: 10.13140/RG.2.2.14945.63842

1 author:

Devharsh Trivedi
Stevens Institute of Technology
27 PUBLICATIONS **9** CITATIONS

SEE PROFILE

CSL Assignment
Mobile Forensics Tools

Devharsh Trivedi
14MCEI25

April 19, 2015

1 Mobile device forensics

Mobile forensics tools tend to consist of both a hardware and software component. Mobile phones come with a diverse range of connectors, the hardware devices support a number of different cables and perform the same role as a write blocker in computer devices.

Name	Platform	License	Version	Description
Cellebrite Mobile Forensics[7]	Windows	proprietary		Universal Forensics Extraction Device - Hardware and Software
Secure View Mobile Forenscis Software[7]	Windows	proprietary		Hardware/Software package
Radio Tactics Aceso[7]	Windows	proprietary		"All-in-one" unit with a touch screen
Paraben Device Seizure[7]	Windows	proprietary		Hardware/Software package
MicroSystemation XRY/XACT[7]	Windows	proprietary		Hardware/Software package, specializes in deleted data
Oxygen Forensic Suite (former Oxygen Phone Manager[7])	Windows	proprietary		Smart forensics for smartphones
MOBILedit! Forensic[7]	Windows	proprietary		Hardware-Connection kit/Software package
NowSecure Forensics[8]	Santoku Linux (bare metal or in a VM on Mac OSX VMWare Fusion or Windows VMWare Player)	proprietary	2.9	Automated filesystem, backup, and logical acquisitions of SMS, apps, contacts and more
MPE+ Mobile Phone Examiner Plus[7]	Windows	proprietary		Universal Cell phone and Smart phone Forensics Extraction and Analysis Tool - Hardware and Software

2 MicroSystemation XRY

MicroSystemation XRY (http://www.msab.com) is one of the market leaders in mobile device acquisition. MicroSystemation sell products to capture mobile phones and other small-scale devices logically via USB, infrared, and Bluetooth. XRY also has an additional component, XACT, that expands capability by performing physical acquisition via the JTAG interface. XACT also allows for the acquisition of specifi c models of GPS receiver. Figure 20.14 shows the XRY acquisition interface.

2.1 XRY Logical

XRY Logical is a software based solution for any Windows based PC, complete with the necessary hardware for forensic investigations of mobile devices. XRY is the standard in mobile device forensics and the first choice among law enforcement agencies worldwide.

Currently supporting +1000 different telephone models, including most GSM telephones and many 3G telephones, .XRY creates an encrypted file containing a copy of the information stored on the telephone. The solution pulls an impressive amount of information from the phone, including, telephone books with names, numbers, etc., SMS messages that have been sent, received and archived, pictures, calendar Information, sound files, and some SIM data as well. .XRY software is

sold with a communication hub that includes Bluetooth for connectivity without cables. A cable kit is available, as are individual cables.

2.2 XRY Physical

XRY Physical is a software package for the physical recovery of data from mobile devices. The memory dump from each individual device is a complex data structure, so Micro Systemation has developed XRY Physical to make it easier to navigate this wealth of information.

XRY Physical provides mobile phone forensics specialists with the tools they need to perform highly sophisticated "physical" data acquisitions from confiscated phones or memory cards and allows for the recovery of deleted information. The new XRY Physical lets forensics specialists push investigations even further by performing physical data acquisitions a process generating hex dumps from phone memory and allowing the recovery of deleted information.

3 Cellebrite Universal Forensic Extraction Device (UFED)

Cellebrite Universal Forensic Extraction Device (UFED) (http://www.cellebrite.com) is a self-contained, portable mobile phone logical acquisition device. The system is self-powered and copies data to a USB disk or to a second phone. Cellebrite UFED was designed in Israel. The Cellebrite UFED is shown in Figure 20.15. Cellebrite also have an additional component, UFED Physical Pro, that allows physical acquisition of mobile phones and other small-scale devices. UFED systems are also available in a fi eld-ready ruggedized form.

UFED Touch Ultimate, enables the most technologically advanced extraction, decoding, analysis and reporting of mobile data. It performs physical, logical, file system and password extraction

of all data (even if deleted) from the widest range of devices including legacy and feature phones, smartphones, portable GPS devices, tablets and phones manufactured with Chinese chipsets.

The Cellebrite UFED and UFED Physical Pro 2 forensic tools currently support the most phones of any tool on the market, with over 3,200 mobile devices capable of being analyzed. In addition to data extraction, such as phonebooks, call logs, SMS messages, pictures and file systems, the UFED tool can extract phone lock codes from many devices. The UFED Physical Pro 2 tool is capable of acquiring and decoding the physical memory from several hundred devices, including the iPhone and other iOS Devices. Characterized by their ease-of-use, multiple language support and extensive phone coverage, the UFED tools are used widely around the world.

4 Logicube CellDEK

Logicube CellDEK (http://www.logicubeforensics.com) is a system designed to acquire data from mobile phones and other small-scale devices such as GPS receivers. CellDEK conducts logical extraction of data via USB, infrared, and Bluetooth.

The portable CellDEK is compatible with 1800 cell phones, PDAs, and satellite navigation devices. This cell phone data extraction device is a self-contained system with a touch-screen display and allows the user to identify devices by brand, model number, dimensions and/or photographs. When the device type is selected a smart adapter feature then illuminates the correct USB adapter.

Connectivity by infra-red and Bluetooth are also built-in. Up to 40 adapters may be stored in the systems built-in rack.

The portable CellDEK is compatible with 500+ of the most popular cell phones and PDA's. Built to perform in the field (not just in the lab), investigators can immediately gain access to vital information, saving days of waiting for a report from a crime lab. This advanced cell phone data extraction device is a self-contained system that features a touch-screen display allowing the user to quickly identify devices by brand, model number, dimensions and/or photographs.

5 MOBILedit! Forensic

MOBILedit! Forensic (http://mobiledit.com) is another logical data acquisition tool. MOBILedit! Forensic can be purchased as a software-only tool or as part of a kit including cables and infrared reader.

MOBILedit Forensic supports thousands of different phones including common feature phones from manufacturers like Samsung, HTC, Nokia, Sony, LG and Motorola. It also supports all smartphone operating systems including Android, iPhone, Blackberry, Symbian, Windows Mobile, Windows Phone, Bada, Meego or Mediatek (Chinese phones).

MobilEdit Forensic software analyzes a comprehensive collection of GSM phones, and a growing number of CDMA phones. The latest version incorporates a HEX viewer for analyzing CDMA phones in low level, and more flexible reporting and output options. The software is sold individually, or with a complete cable kit. Individual cables are not offered by MobilEdit Forensic.

MOBILedit! Forensic is the world's most trusted phone investigation tool. Highly rated by the National Institute of Standards and Technology, MOBILedit! Forensic is the primary mobile

device investigation tool used in over 70 countries. Simply connect a phone and MOBILedit! Forensic extracts all content and generates a forensic report ready for courtroom presentation. These tamper-proof, flawless reports are used in hundreds of courtrooms every day.

- Analyze phones via Bluetooth, IrDA or cable connection
- Analyze phonebook, last dialed numbers, missed calls, received calls, SMS messages, multimedia messages, photos, files, phone details, calendar, notes, tasks and more
- Large quantity of phones supported
- Direct SIM analyzer through SIM readers
- Reads deleted messages from the SIM card
- Secure and tamper-proof using MD5 hash
- Preferred/forbidden networks
- Hex dump viewer

6 iXAM

iXAM (http://www.ixam-forensics.com) is a forensic acquisition system specifically for the Apple iPhone and Apple iPod Touch. iXAM acquires data via the USB interface, but has full physical

extraction of data. iXAM is a niche system, only providing acquisition of a small number of devices from a single manufacturer. Figure 20.16 shows iXAM acquiring an Apple iPhone.

iXAM - an iPhone, iPod Touch and iPad forensic imaging and data analysis suite comprising two key applications to allow fast and comprehensive forensic examination and reporting of user and system data stored on these unique devices.

iXAM - Forensic data imaging tool: Uses a proprietary method which requires no modification to the device Operating System and leaves absolutely no trace on the target device. This tool has 2 extraction modes to allow investigators to perform the appropriate level of examination based on importance of the device and the time available.

Forensic Imaging Mode: A full byte for byte physical memory space image of either the user or system partition, including unallocated memory space. Includes audit logging &MD5/SHA1 hash validation of every memory block.

Logical Imaging Mode: Allows an investigator to perform targeted acquisition of specific key live data sets, but still using a physical imaging technique to download the data.

iXAMiner - Decoding and reporting tool: Enables investigators to interpret and present the results of a data acquisition performed using iXAM.

7 References

- https://community.spiceworks.com/security/mobile-forensics/reviews
- CHAPTER 20, Digital Evidence on Mobile Devices, Eoghan Casey and Benjamin Turnbull
- www.mobileforensicscentral.com/mfc/products_software.asp
- http://nanoforensic.com/index.php?option=com_content&view=article&id=50&Itemid=86
- https://en.wikipedia.org/wiki/List_of_digital_forensics_tools#Mobile_device_forensics