MIT World Peace University

Digital Forensics and Investigation
Third Year B. Tech, Semester 5

Tools for Digital Forensics and Investigation for Mobile Devices.

Lab Assignment 1

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

August 14, 2023

Contents

1 Aim

To Learn about the different tools used in Digital Forensics and Investigation for Mobile Devices.

2 Objectives

1. Understand the need for Digital Forensics and Investigation for Mobile Devices.
2. Find out the tools available in the market for Forensics in Mobile Devices.
3. Experiment with some simple tools.

3 Theory

3.1 Definitions

Definition 1. ***Digital Forensics*** *is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.*

Definition 2. ***Mobile Forensics*** *is a sub-branch of Digital Forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.*

3.2 Need for Mobile Forensics

1. **Digital Evidence Collection:** Mobile devices store a vast amount of digital evidence, including call logs, messages, app data, and location information. Forensics enables systematic extraction and preservation of this evidence for legal investigations.
2. **Criminal Investigations:** Mobile devices often contain crucial evidence in criminal cases, such as text messages, images, and GPS data. Forensic analysis aids law enforcement agencies in reconstructing timelines and uncovering relevant details.
3. **Cybersecurity Incidents:** Mobile devices can be compromised in cyberattacks, leading to data breaches or unauthorized access. Forensics helps identify attack vectors, assess the extent of compromise, and prevent future incidents.
4. **Fraud Detection:** Mobile forensics assists in detecting financial fraud by analyzing communication records, app usage, and location data to establish patterns of fraudulent activities.
5. **Employee Misconduct:** Employers can use mobile forensics to investigate cases of data theft, policy violations, or other employee misconduct, ensuring a secure workplace environment.
6. **Disaster Recovery:** Mobile forensics aids in recovering data from damaged or compromised devices, helping individuals and organizations restore lost information.
7. **Legal Proceedings:** Mobile device data can be presented as evidence in court. Forensic procedures validate the authenticity of data, ensuring its admissibility in legal proceedings.

4 Forensic Tool Types

An examiner can use various mobile forensic tools depending on the objective of the examination and the type of mobile device involved. Experts use the Mobile Forensic Tool Leveling System (Fig. 2) to assess the tool's capability in data acquisition. As the level in the pyramid increases, forensic tools become more expensive, methods become more invasive, and technical requirements also increase. Each level is briefly discussed below:

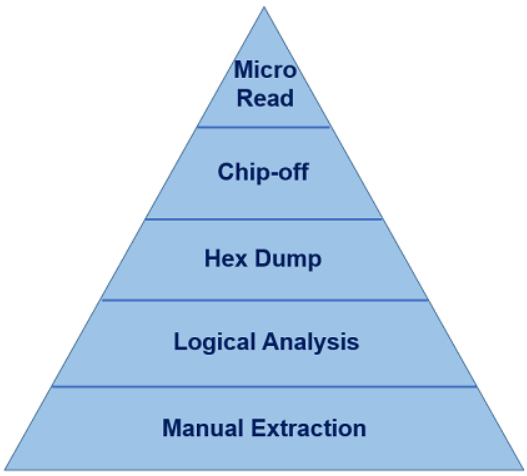

Figure 1:

1. "Manual Extraction" - It involves physical analysis of the device and photographic documentation of the data present in it. Some of the tools used for manual analysis are Project-A-Phone and Fernico ZRT.

2. "Logical Analysis" - It requires connecting the data cable to the handset and extracting data using cell phone extraction software such as Oxygen Forensic Suite and Lantern.

3. "Physical Analysis (Hex Dump)" - It involves connecting the device to the forensic workstation and pushing a bootloader to instruct the device to dump the memory to the computer. The data dumped into the computer is then subjected to further analysis. Some common tools used for hex dump include XACT and Pandora's Box.

4. "Physical Analysis (Chip-Off)" - It involves removing the memory chip from the device and using a separate reader to review and analyze the data. Another way is to use a second mobile device to read data. Some tools used for this process are the iSeasamo Phone Opening Tool and the FEITA Digital inspection station.

5. "Physical Analysis (Micro Read)" - It entails using a high-powered electron microscope to view, analyze, and interpret data on memory chips.

5 Process

Cell phone digital forensics requires gathering data in forensically sound conditions. Forensically sound refers to data collection without alteration or destruction during the investigative process, whether on purpose or by accident. The compilation, analysis, handling, and storage of data must

have been done in a manner acceptable by law. Mobile forensics requires legal and technical expertise in observing the forensic process discussed in the succeeding sections.

5.1 Preparation

The preparation stage involves researching information about the specific device and the appropriate tools to be used. It also requires the preparation of the machine and the devices needed for the examination (e.g., cables, extraction software, drivers, etc.).

5.2 Isolation

The isolation stage involves cutting off the device's connection from data or cellular access such as Bluetooth and Wi-Fi to preserve the data. Disabling network connectivity is essential because most mobile devices can be remotely controlled by the user, who may lock or completely wipe the information. Incoming calls and texts may also potentially modify existing data.

Figure 2: Phone kept in a rfid Safe bag, to prevent remote access, and isolate it completely.

6 Tools

6.1 Processing

In the processing stage, tools prepared in the previous steps can now be used to extract data from the mobile device. Depending on the circumstance and the objective of the examination, more intrusive tools can be used to extract data during the initial or final stage of the processing.

6.2 Verification

The verification stage requires the examiner to check whether the data obtained from the device is accurate. It is an essential step because, in some cases, the data in the mobile device is erroneous or incomplete.

7 Tools

7.1 SANS Sift

The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu based Live CD which includes all the tools you need to conduct an in-depth forensic or incident response investigation. It supports analysis

of Expert Witness Format (E01), Advanced Forensic Format (AFF), and RAW (dd) evidence formats. SIFT includes tools such as log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.

7.2 Prodiscover Forensics

ProDiscover Basic is a simple digital forensic investigation tool that allows you to image, analyse and report on evidence found on a drive. Once you add a forensic image you can view the data by content or by looking at the clusters that hold the data. You can also search for data using the Search node based on the criteria you specify.

7.3 The Sleuth Kit (+Autopsy)

The Sleuth Kit is an open source digital forensics toolkit that can be used to perform in-depth analysis of various file systems. Autopsy is essentially a GUI that sits on top of The Sleuth Kit. It comes with features like Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching out of the box, with the ability to add other modules for extended functionality.

Figure 3: The Sleuth Kit + Autopsy webpage.

7.4 FTK Imager

FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images or memory dumps. Using FTK Imager you can also create SHA1 or MD5 hashes of files, export files and folders from forensic images to disk, review and recover files that were deleted from the Recycle Bin (providing

that their data blocks haven't been overwritten), and mount a forensic image to view its contents in Windows Explorer.

7.5 Linux 'dd'

dd comes by default on the majority of Linux distributions available today (e.g. Ubuntu, Fedora). This tool can be used for various digital forensic tasks such as forensically wiping a drive (zero-ing out a drive) and creating a raw image of a drive.

7.6 CAINE

(Computer Aided INvestigative Environment) is Linux Live CD that contains a wealth of digital forensic tools. Features include a user-friendly GUI, semi-automated report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.

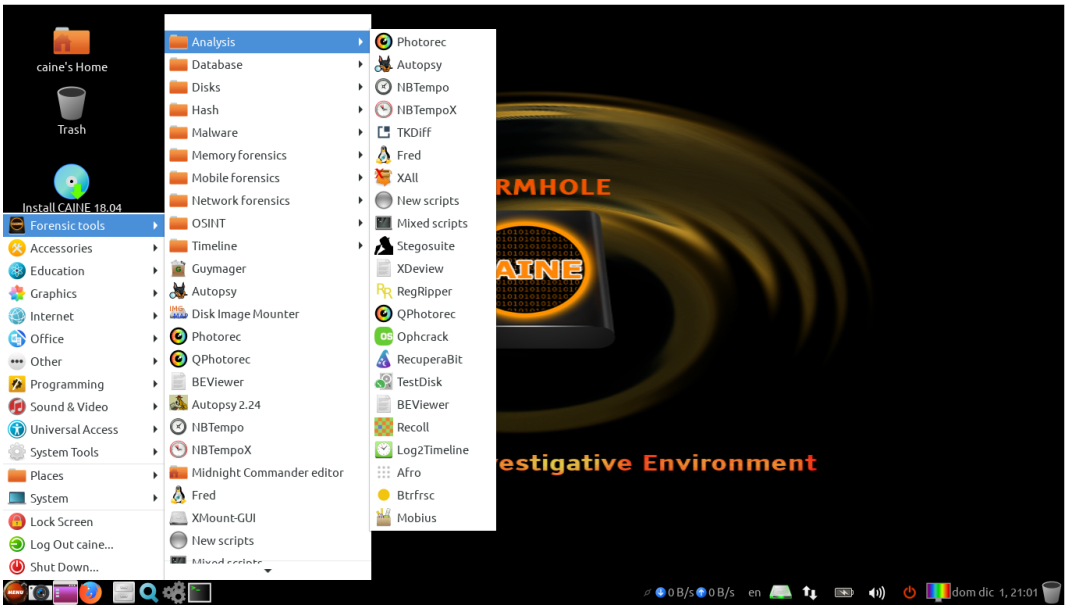

Figure 4:

7.7 Oxygen Forensic Suite 2013 Standard

If you are investigating a case that requires you to gather evidence from a mobile phone to support your case, Oxygen Forensics Suite (Standard Edition) is a tool that will help you achieve this. Features include the ability to gather Device Information (Manufacturer, OS Platform, IMEI, Serial Number, etc.), Contacts, Messages (Emails, SMS, MMS, etc.) and recovery of deleted messages, Call Logs, and Calendar and Task information. It also comes with a file browser which allows you to access and analyse user photos, videos, documents and device databases.

Figure 5: Oxygen Forensic Suite 2014

7.8 Free Hex Editor Neo

Free Hex Editor Neo is a basic hex editor that was designed to handle very large files. While a lot of the additional features are found in the commercial versions of Hex Editor Neo, I find this tool useful for loading large files (e.g. database files or forensic images) and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.

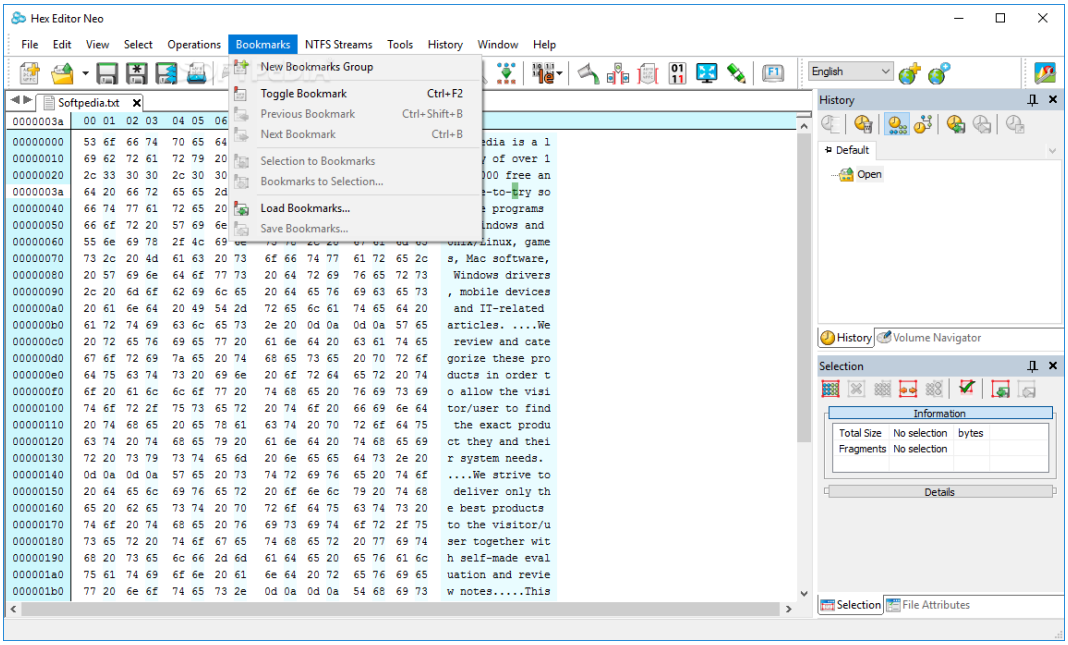

Figure 6:

7.9 Mandiant RedLine

RedLine offers the ability to perform memory and file analysis of a specific host. It collects information about running processes and drivers from memory, and gathers file system metadata, registry data, event logs, network information, services, tasks, and Internet history to help build an overall threat assessment profile.

Figure 7:

7.10 P2 eXplorer

P2 eXplorer is a forensic image mounting tool that allows you to mount a forensic image as a physical disk and view the contents of that image in Windows Explorer or load it into an external forensic analysis tool. P2 eXplorer supports images in RAW, DD, IMG, EX01, SMART and SafeBack format, amongst others.

8 Experiments

For Experimentation and basic testing, we have used Andriller.

8.1 Andriller

Andriller is a software utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices. It has features, such as powerful Lockscreen cracking for Pattern, PIN code, or Password; custom decoders for Apps data from Android (some Apple iOS and Windows) databases for decoding communications. Extraction and decoders produce reports in HTML and Excel formats.

8.2 Screenshots

These are the reports generated by Andriller. The first one is from Parth's Phone and the second one is from Krish's Phone. USB Debugging had to be turned on for this to work.

[Andriller Report]

Type	Data
Serial	hqnzin75pvkzdezh
Status	device
Permisson	shell
Wifi Mac	04:c8:07:31:0f:fc
Local_Time	2023-08-02 06:19:46 India Standard Time
Device_Time	2023-08-02 11:49:46 IST
Accounts	• com.google: kpt.krishna***@gmail.com • com.google: thadesarkrish***aj@gmail.com • com.google: krishpt9***ail.com • com.google: mit.krishna***@gmail.com • com.google: littlekin***gmail.com • com.xiaomi: 1697***558 • org.telegram.messenger: 1102***145 • com.truecaller.account: True***ler • com.duolingo: Duo***go • digilocker: e3294b61-e22f-58c6-8e55-06916a6***7a@elibom.digitallocker.gov.in • com.microsoft.skydrive: Krishnaraj.k***outlook.com • com.dropbox.android.account: kpt.krishna***@gmail.com • co.sensara.miremote: 98a1be9c-d1b8-4e3***e7b-a3f1f72a1636 • com.github.android: Kris***rajT • com.whatsapp: Wha***pp • com.samsung.health.auth: kpt.krishna***@gmail.com • com.reddit.account: Reddit f***Android • com.reddit.account: kpt***ish • com.reddit.account: Reddit ***ognito

 # andriller.com # (This field is editable in Preferences)

Figure 8: Krishnaraj's Phone

[Andriller Report]

Type	Data
Serial	X8PZX4WSUGFUEIRW
Status	device
Permisson	shell
Wifi Mac	52:58:95:3e:c4:28
Local_Time	2023-08-02 06:22:04 India Standard Time
Device_Time	2023-08-02 11:52:04 IST
Accounts	• com.google: parthzarekar@gmail.com • com.google: bten4444@gmail.com • com.google: parthzarekar4@gmail.com • com.google: zarekarhome506@gmail.com • com.oneplus.account: I1630167491720 • com.oneplus.account: 879****0288 • com.whatsapp: WhatsApp • org.telegram.messenger: 1963751589 • com.twitter.android.auth.login: Parth26421831 • com.truecaller.account: Truecaller • com.facebook.auth.login: 100043358384688 • com.facebook.messenger: Messenger • com.reddit.account: Reddit for Android • com.reddit.account: New-Willingness7250 • com.microsoft.office: Office • com.adobe.creativesdk.foundation.auth.adobeID.DC: parthzarekar@gmail.com • com.duolingo: Duolingo • com.github.android: Parth4123 • com.google: 1032210846@mitwpu.edu.in
Application	Shared Storage (0)

 # andriller.com # (This field is editable in Preferences)

Figure 9: Parth's Phone

8.3 Andriller in Action

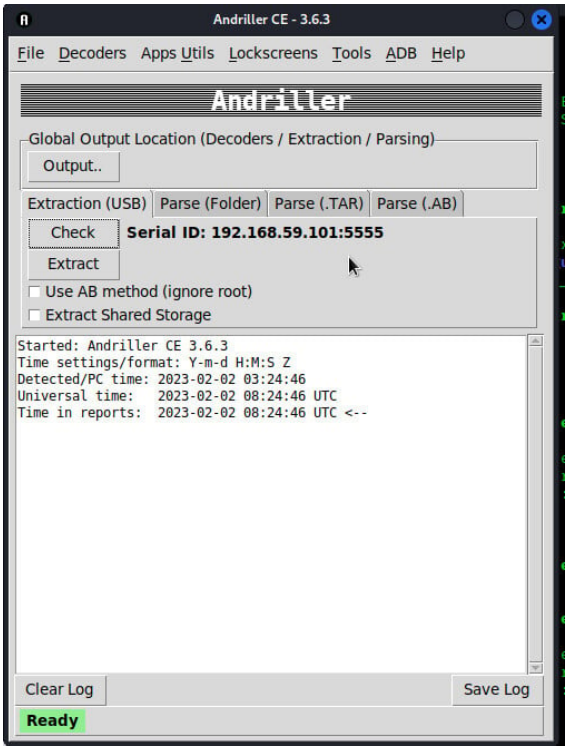

Figure 10: Andriller extracting information, Demo, not experimental.

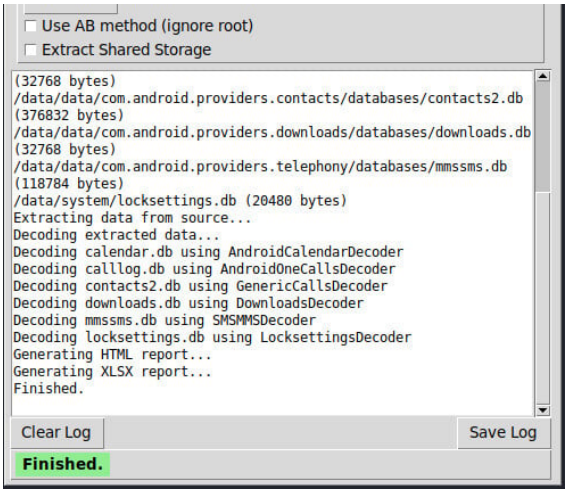

Figure 11: Andriller finishes extrating, Demo, not experimental.

9 Results

We were able to extract some very basic information from the devices.

1. We obtained the email ids logged in on the device.

2. We obtained android files for almost all apps.
3. We also got the db files for many notable apps like Instagram, contacts etc. This was the most significant part of the experiment.

10 Platform

Operating System: Windows 11
IDEs or Text Editors Used: Visual Studio Code
Compilers or Interpreters: Python 3.10.1

11 Conclusion

Thus, we were able to learn about the different tools used in Digital Forensics and Investigation for Mobile Devices. We also performed a very basic extraction from ours and our Friend's mobile devices, and managed to get some very basic information from it.

References

[1] *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.*
Academic Press.

[2] *File System Forensic Analysis.*
Addison-Wesley.

[3] *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation.*
Elsevier.

[4] Vskills - Digital Forensic Tools
VSkills