

Forensic Analysis in Mobile Environments

Introduction

Unit 4

1 Introduction to Forensic Analysis

2 Methodology

Stages of the Forensic Analysis

The Forensic Report

3 Basic Tools

4 Methods of Data Acquisition

- Methods of Data Acquisition

- Maximising Data Acquisition

- Acquisition on Android

- Acquisition on iOS

- Acquisition on Windows Phone

- Acquisition on BlackBerry

- 5 Types of Data Acquisition
 - Forensic Image of an Android Device
 - Image of an SD card
 - Forensic Image of an iOS Device
 - Logical Acquisition of an Android Device
 - Memory Acquisition of an Android Device
- 6 Data Analysis
- 7 Analysis Laboratory
 - Introduction to the Laboratory
 - Presentation of the Case
 - Creation of the Case
 - Information Extraction
 - Analysis
 - Report
- 8 Research exercises
 - Assessment test



A person wearing a light blue button-down shirt is seated at a dark wooden desk. They are holding a black pen and writing in a small, open notebook. A laptop is partially visible to the right of the notebook. The background is a solid orange wall. A semi-transparent dark blue banner is overlaid across the middle of the image, containing the title text in white.

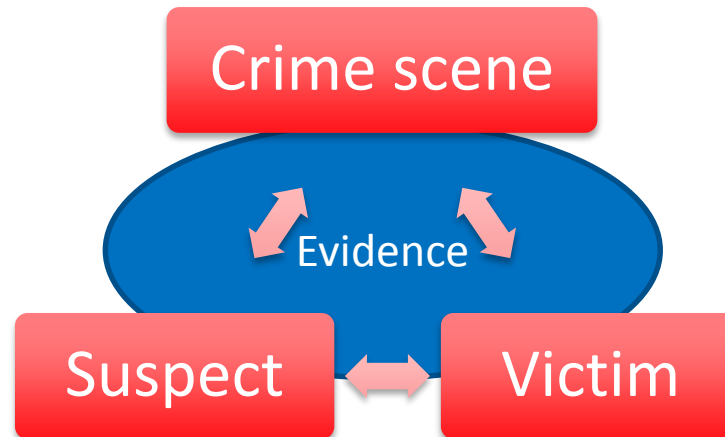
Introduction to Forensic Analysis

◆◆◆ Introduction to Forensic Analysis

Locard's Exchange Principle

Any physical interaction between two objects implies the transfer of material from one to the other

- Such principle was developed by Edmond Locard in 1934.
- It is the precursor of the forensic analysis as scientific field.
 - The criminal leaves evidences in the crime scene when committing it.
 - The analyst may modify evidences during the acquisition or analysis process.



◆◆◆ Introduction to Forensic Analysis

Definition

- Forensic Analysis in IT environments:
 - Forensic Analysis is the set of procedures for evidence gathering and analysis aimed at discovering the causes of an incident in which a computer system is involved.
- Depending on the type of incident occurred, the process of forensic analysis is performed with different purposes:
 - If the incident is related to a criminal activity or the security forces and judicial bodies are involved, the aim of the analysis is to present evidences in a court.
 - In case it is a computer security incident, the procedures carried out (such as the forensic analysis) will be aimed at responding efficiently against the incident.
- The forensic analysis process carried out in an organization in the event of a computer incident, is compatible with the legal process that may be lead from the incident itself and, on many occasions, it is useful to clarify events and authors.

◆◆◆ Introduction to Forensic Analysis

Objectives

- Generally, the objectives of a forensic analysis can be divided into two:
 - To understand what has happened in a computer system. According to the type of investigation, the events to study may be different:
 - In case of a computer intrusion: get to know procedures carried out to access the system as well as the scope of damages.
 - In the case of crimes that have not been committed via computer, it is useful to learn information regarding the owner of the device (e.g.: to check an alibi).
 - To know the responsible for each event discovered during the analysis.
 - This task can be very complex due to the techniques existing for providing anonymity to attackers (botnets, Tor, etc.).

◆◆◆ Introduction to Forensic Analysis

Motivation

- Forensics IT is an essential part of the response against incidents processes:
 - It is applied after a security crime or incident.
 - It enables the reconstruction of events or actions that have lead to a security incident in order to improve protection processes existing in an organization.
- Computer forensics can also be used actively in the context of an organisation in order to:
 - Audit security properties of a given system (maintenance of privacy, transmission of sensitive data, etc.).
 - Review the compliance of security regulations and standards.
 - Verify that users comply with the procedures required for the destruction of sensitive data in a system.



Special Features in the Mobile Environment I

- One of the main problems of computer forensics is the fact that it should be always adapted to the constant creation of new devices:
 - Computer forensics dealt, from its origins, with crimes committed via computer means. Therefore, investigations were focused on workplaces, servers and networks.
 - When mobile phones came out, new forms of data (such as SMS and calls) appeared. It connected computer forensics to crimes committed outside the electronic environment.
 - When smartphones appeared, the range of collectable information from a device increased (messages, emails, locations, etc.).
 - The new smart devices (wearable, vehicles, home automation, etc.) provide even more information that can be useful for a judicial inquiry.
- Each of these types of devices has a set of special features that make the forensic analysis a hard task to perform.

Special Features in the Mobile Environment II

- Specifically, the analysis of mobile environments and smartphones implies a challenge, due to the following reasons:
 - **Different operative systems:** even though Android is the most used operative system, there are others that also have an important market share and, thus, should be known in depth in order to perform the process of taking evidences. iOS, Windows Phone and BlackBerry OS are some examples.
 - **Legal considerations:** it is essential to comply with the current regulations during the whole process, in order to maintain the evidences' legal validity if necessary.
 - **Anti-forensic techniques:** just like in the case of computers, it is possible to carry out actions in order to make evidence identification more difficult during a forensic process. For example: evidence destruction, concealment, or falsification.

◆◆◆ Introduction to Forensic Analysis

Special Features in the Mobile Environment III

- Mobile operative systems provide protection and encryption systems by default that make data acquisition and analysis more difficult:
 - The **code lock** of a device avoids access to the device, even using a cable in some systems.
 - The **remote wipe** allows a user to erase all the evidences of a device without having physical access to it.
 - The **disk encryption** makes it possible for attackers to read memories via physical access to the chip.
- There are millions of applications available for all types of devices. Each of them, with a different information storage mechanism.



◆◆◆ Introduction to Forensic Analysis

Relevant Evidences in the Mobile Environment

Contacts	Emails	Music files
Call history	Browsing history	Documents
SMS	Photographs	Calendar
MMS	Video	Trusted networks
Search history	Keyboard cache	Location history
Messaging applications' conversations	Posts on social networks	Data removed from the phone
Accounts	Applications installed	Device sensors' data



Methodology

A close-up, slightly blurred photograph of a person's hand holding a blue pen, writing on a document. The person is wearing a grey, textured sweater. In the background, a white mug of coffee sits on a wooden desk. The scene is softly lit, creating a warm, focused atmosphere. A semi-transparent grey box is overlaid on the center of the image, containing the title text.

Stages of the Forensic Analysis

◆◆◆ Stages of the Forensic Analysis

Introduction

- The process of forensic analysis is based on a methodology and some tools that are accepted by the community.
- Such methodology used during the forensic analysis of computer systems has been inherited from traditional forensic processes.
- Tools used should comply with two essential requirements:
 - **Repeatability:** ability to repeat exactly the same results from the same initial conditions, in separate successive executions, using the same method and tools.
 - **Reproducibility:** ability to obtain the same results from the same initial conditions, using the same method, but different means (by using different tools or developing them completely).
- It is said that a forensic procedure is “forensically sound” if the process for evidence collecting, handling, storage and analysis ensures that evidences have not been modified during the analysis process.

◆◆◆ Stages of the Forensic Analysis

Guides

- Even though there is no standardised methodology focused on the forensic analysis of mobile devices, there are different guides that may be useful in the process:
 - [Guidelines on Mobile Device Forensics](#) by NIST.
 - [Developing Process for Mobile Device Forensics](#) by SANS.
 - [Best Practices for Mobile Phone Forensics](#) by the Scientific Working Group on Digital Evidence (SWGDE).
 - [Good Practice Guide for Mobile Phone Seizure & Examination](#) by the Interpol.
 - [ISO/IEC 27037:2012](#), *Guidelines for identification, collection, acquisition and preservation of digital evidence*.
 - [RFC 3227](#), it does not mention mobile devices directly, but it is a de facto standard in the process of computer forensics.

◆◆◆ Stages of the Forensic Analysis

Outline

The forensic analysis process is divided into five stages.



In order to perform the analysis process correctly, it is recommended to take notes during all the stages of the analysis.

Such notes (the more detailed, the better) may include:

- Screenshots.

- Location of evidences discovered.

- Handwriting notes.

- Use of noting system within the forensic application itself.

Preparation

Acquisition

Management
of evidences

Exam

Analysis

Presentation

◆◆◇ Stages of the Forensic Analysis

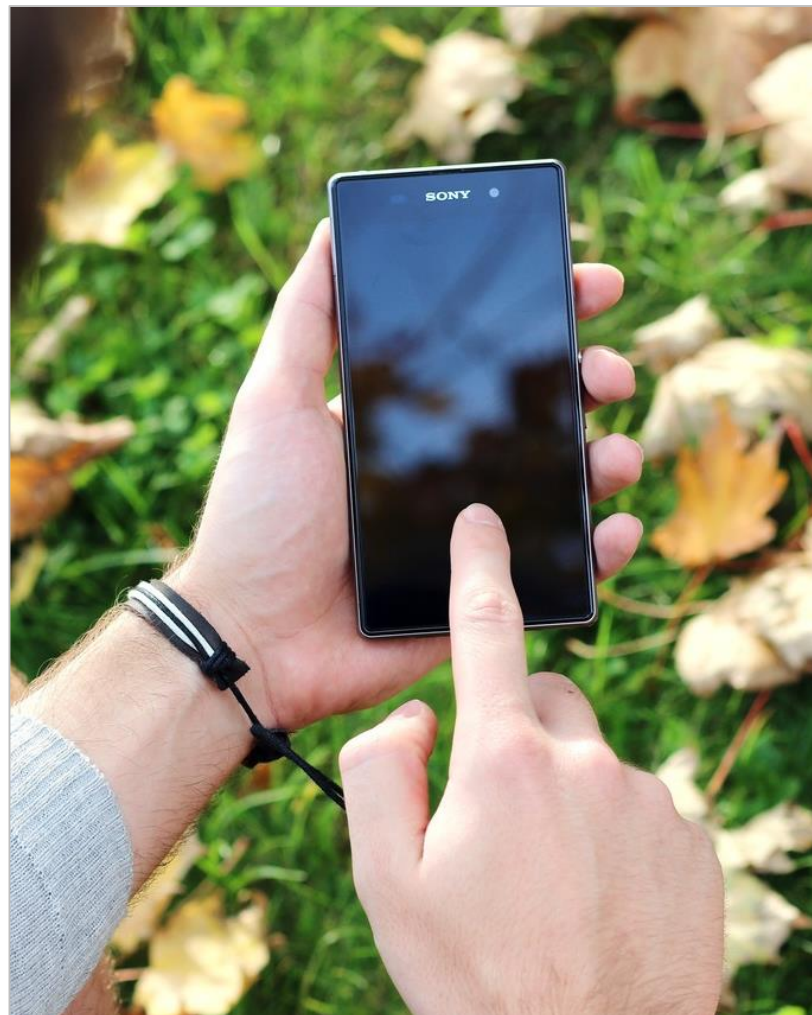
Preparation

- This stage is executed previously to the analysis process.
- It implies identifying the physical elements to be analysed, as well as evidences that will be searched in each of the analysable elements.
- Such elements depend on the objective of the forensic analysis:
 - The analysis of an intrusion via mobile device will require, for example, the analysis of the device's storage in order to find evidences of illegal access to the systems.
 - The analysis of a device in order to check an alibi will require, for example, the analysis of the device's storage in order to check locations in which the device's owner has been to.
- On some occasions this task is performed together with the acquisition of evidences due to the necessity of a rapid response against the incident in order to avoid the elimination of evidences.
 - For example, during the seizure of a mobile device, the first task performed is the initial preservation of the evidence by placing it in a Faraday cage, in order to isolate it from external signals.

◆◆◆ Stages of the Forensic Analysis

Order of Evidence Acquisition

- The **acquisition process** should be performed taking into consideration evidences' volatility.
- First, it is necessary to collect the most volatile evidences.
- A possible order of acquisition is described below, according to volatility and applying the ones in bold to mobile devices ([RFC 3227](#)):
 - **Registers or caches.**
 - Routing tables, **processes list and memory.**
 - Temporary files system.
 - **Disk.**
 - Remote monitoring system.
 - Network topology and physical configuration.
 - **External, physical means.**



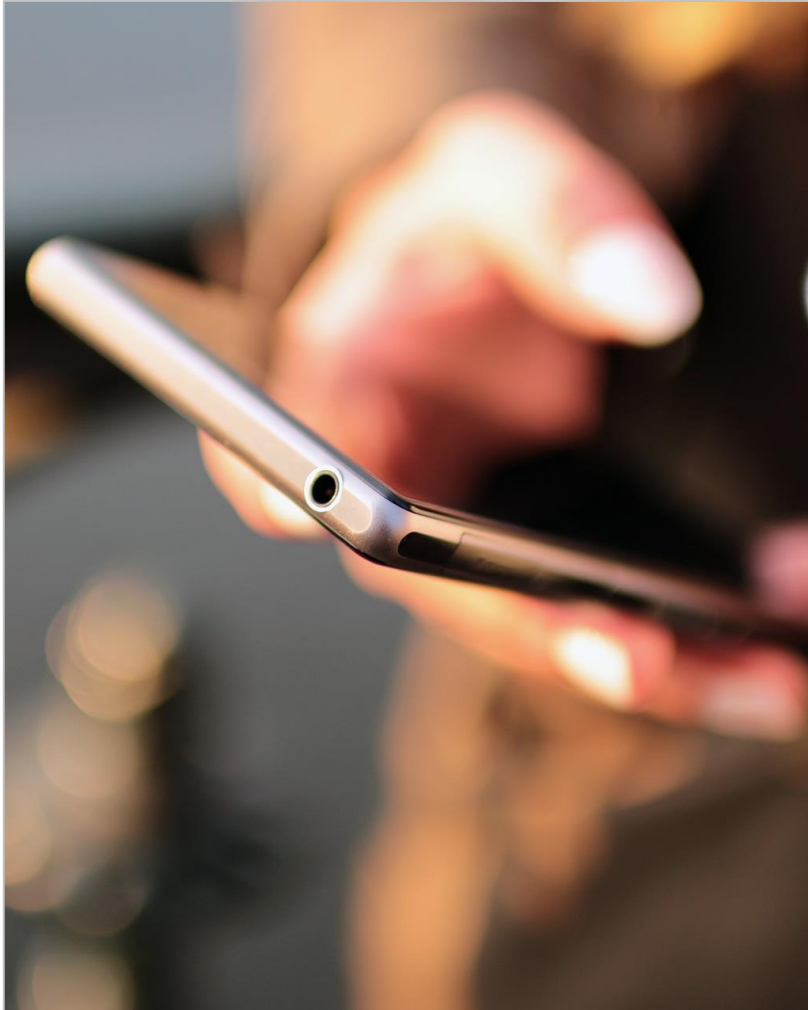
◆◆◆ Stages of the Forensic Analysis

Acquisition I

- The **acquisition process** implies obtaining or capturing the evidences mentioned in the preparation stage.
- Evidences can be divided into two groups according to their lifetime:
 - **Volatile:** evidences that are created and destroyed during the execution of the system (memory, network packets, temporary files, etc.). They may include encryption passwords, processes in execution that have been removed from the disk or other interesting data.
 - **Non-volatile:** evidences that can be obtained from the device once it has been turned off (mainly, storage devices).
- If it is possible, a forensic duplicate should be always made:
 - It implies performing a bit-by-bit copy of the information from the source.
 - Once the copy has been obtained, its hash is necessary to validate that it is an exact copy.
 - It can be compressed in order to optimise storage.
 - Generally, it is made via specific hardware.

◆◆◆ Stages of the Forensic Analysis

Acquisition II



- Different tools and techniques should be used according to the status of the device and the type of evidence involved:
 - If the device is turned on and unlocked, it is possible to use techniques for network monitoring or core dumping in order to obtain evidences in real time.
 - Some of these techniques slightly modify the analysed system. The validity of the evidences depends on the amount of changes caused by the acquisition tool.
 - For example, the dd program for core dumping should be loaded on the memory that will be dumped for its execution.
 - In case the device is in Sleep Mode, the information acquisition can be performed in situ or at the laboratory, after the seizure.

◆◆◆ Stages of the Forensic Analysis

Acquisition III

- For each evidence collected, it is essential:
 - To specify tools and procedures used to obtain it.
 - To specify the exact **evidence** collected:
 - **Network traffic**: duration, start time, type of packets, data obtained, etc.
 - **Hard disk**: rate of recovery, recovery method, etc.
- Use some mechanisms to ensure that data obtained are not modified and, in case they are, changes should be able to be traced:
 - Generally, a summary of data obtained should be made by using a summary function (SHA-256).
 - According to the aim of the investigation, the summary may be signed with a private key of the investigator.



◆◆◆ Stages of the Forensic Analysis

Chain of Custody and Evidence Management

- Evidence management is an essential process for the validation of the whole process of forensic analysis.
- If evidences are well managed, the chain of custody is respected and thus, evidences will not be compromised.
- The chain of custody includes the set of procedures aimed at gathering, translating and guarding evidences related to the investigation.
- The chain of custody is aimed at ensuring that evidences are authentic, undamaged, and not modified.
- The chain of custody allows the user:
 - To trace the physical elements corresponding to a specific evidence.
 - To identify the origin of a physical element used as evidence.
 - To ensure that the access to an evidence is monitored and recorded.
 - To document all the processes performed to extract evidences.
 - To prove that processes mentioned above are reproducible and replicable.

◆◆◆ Stages of the Forensic Analysis

Exam

- The exam involves the identification of evidences by using the information obtained in the acquisition stage.
- In the analysis of a disk:
 - Examine the file system and partitions.
 - Existing and deleted files.
 - Unused spaces and blocks after the end-of-file mark.
 - Obtain metadata, categorise files and discard the irrelevant ones.
- In the network analysis:
 - Discard irrelevant packets.
- In the memory analysis:
 - Discard irrelevant processes.
 - Extract relevant information from the processes.

◆◆◆ Stages of the Forensic Analysis

Analysis

- The **analysis** implies obtaining conclusions from the evidences acquired.
- It is the most complex stage of the process and the one that provides more freedom; therefore, it varies according to the analyst.
- In some cases, the analysis of evidences may create a new testing and extraction stage in order to make new evidences visible.
- It is conducted through an iterative process:
 - **Create an hypothesis** based on the information related available.
 - **Prove the hypothesis** with the evidences existing. The possible existence of counterevidences should also be taken into account.
 - Example:
 - **Hypothesis:** the individual was at the crime scene at a given time.
 - **Evidences:** the device's history of locations shows that the individual was 15 km away.
 - **Anti-forensic techniques:** the device was modified and the date of last modification of the location history file is inconsistent with the date of the event.

◆◆◆ Stages of the Forensic Analysis

Presentation

- The presentation stage implies describing the proved events as well as evidences that corroborate them.
- Generally, it means writing a forensic report.
- The forensic report will be read by non-technical staff (judges, executives, etc.), therefore, it should be clear and include a language adapted to the profile of the reader.
- In case that it is written for a legal process, it may be necessary to defend it in front of the judge.





The Forensic Report

◆◆◆ The Forensic Report

Structure

- Generally, a forensic analysis should include the following sections:
 - Summary of the case.
 - Used tools.
 - Evidence acquisition.
 - Evidence processing.
 - Evidence analysis.
 - Conclusions.
- Depending on the objective and its area, it may be necessary to adjust the structure of the forensic report.



◆◆◆ The Forensic Report

Summary of the Case

- This section should mention:
 - Reasons to conduct the forensic analysis.
 - How evidences have come to the analyst (chain of custody).
 - Who has requested the forensic analysis.
 - The most important dates regarding the report.
 - Date of request, evidences reception and time spent in the creation of the report.
- In some cases, this section also includes a summary of the main results of the analysis. It is important to be careful when writing the information in order not to influence the reader.



◆◆◆ The Forensic Report

Used Tools

- This section should describe all the third parties' tools used in the analysis.
- The following information should be specified for each tool:
 - Version of the tool used (including the platform).
 - Manufacturer.
 - Task that tools have been used for.
- In case any specific tool has been developed for the analysis, it should be mentioned in this section. In addition, an annex should be included in which the necessity and validity of the tool should be proved.
- From some points of view, this part could be divided into subsections of the report sections presented below.

◆◆◆ The Forensic Report

Evidence Acquisition

- This section should describe the process of interaction with evidences.
- To this end, it is necessary to document the following steps as in-depth as possible:
 - The **moment** in which the analyst comes into contact with the evidences.
 - The **status** of the evidences when they are received by the analyst (including photographs and a description of serial numbers of the devices in case they have any).
 - **Processes executed** to preserve each evidence received.
 - They should include the configuration of devices or environments in which evidences will be preserved.
 - **Integrity markers** of all the copies and evidences collected.
 - Some tools use MD5, but it is advisable to use higher standards such as SHA-256, since MD5 presents collisions or combinations of standards.
- The content of this section should prove that the integrity of evidences have not been compromised and the chain of custody has been respected.

Evidence Processing

- The steps executed for the extraction of information that is not explicitly found on the evidences are described in this section:
 - Removed blocks of the files system.
 - Files or data after end-of-file marks.
- The following steps should be documented:
 - The process carried out to move from a forensic image to a working copy. It is necessary to ensure that the original copy is not modified and the working copy is identical to the original one, bit by bit.
 - Processes executed for each evidence element extracted from the working copy.
 - Each evidence should conduct the analyst to the original data unambiguously.

◆◆◆ The Forensic Report

Analysis

- This section of the forensic analysis includes evidences analysed that are relevant for the specific case.
- Evidences that confirm or refute hypothesis involved in the analysis process are presented and explained.
- For each analysed hypothesis:
 - The initial hypothesis as well as the previous information that leads to it are explained.
 - Devices and evidences used during the analysis in order to verify or refute the hypothesis should be listed.
 - A conclusion on the final verification of the defined hypothesis is stated.
- Hypothesis that are not corroborated during the analysis should be also included in the report if they are relevant to the case.
- It is advisable that all the elements necessary to understand the process of verification of the hypothesis (screenshots, logs, etc.) are included.

◆◆◆ The Forensic Report

Conclusions

- This section includes conclusions reached by the analyst after the performance of all the forensic analysis tasks.
- The ultimate goal of a forensic analysis is to describe facts objectively.
- All the conclusions listed in this section should be supported by evidences obtained and described in the report.
- It is also recommendable to remind the reader the reasons why the forensic report was made.



A close-up, slightly blurred photograph of a workshop. In the foreground, a wooden workbench holds a metal compass and a divider. To the right, a black metal stand with a circular base is visible. In the background, there are stacks of books and a piece of light-colored material, possibly leather or paper. A semi-transparent blue rectangle is overlaid across the middle of the image, containing the text "Basic Tools".

Basic Tools

Introduction

- Even though the analysis largely depends on the platform of the analysed device, there is a set of basic tools that could be useful during the whole process of forensic analysis.
- In this section, the main useful tools and programs that may be required during the different stages of a forensic analysis will be presented.
- Generally, commercial-grade forensic suites include various of such tools integrated in a unique product, and this fact facilitates the analysis tasks:
 - **EnCase Forensic** (Guidance Software) - <https://www.guidancesoftware.com>
 - **Oxygen Forensics** (Oxygen Forensics) - <http://www.oxygen-forensic.com/>
 - **Forensic ToolKit** (Access Data) - <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
 - **UFED** (Cellebrite) - <http://www.cellebrite.com/Mobile-Forensics/Applications>

Acquisition - dd

- `dd` is a console tool available in most UNIX systems.
- `dd` is able to read and write on devices directly via the low-level driver without needing to pass through the operative system.
- This feature makes this tool especially interesting to create raw copies of hard disks, flash and RAM memories, since it copies data provided by the low-level driver of the copied device bit by bit.
 - In the case of RAM memory, it should be loaded on it in order to be executed; therefore, it is modified (the utility trace in memory is minimal).
- In order to execute it, it is only necessary to:

```
> dd if=/dev/disk of=myCD.iso bs=2048 conv=noerror,sync
```

Source device	Destination	Block size	Conversion options
---------------	-------------	------------	--------------------
- `dd` is included in Santoku Linux, Android and jailbroken iOS devices.

Analysis – Hexadecimal Viewer

- During the forensic analysis, sometimes, it will be necessary to analyse data files in raw format.
- It is impossible to inspect such files with text editors, since many characters that are not displayed are not printable.
- An hexadecimal editor displays the content of a file with two different views:
 - One shows the data conversion to hexadecimal.
 - The other one displays printable characters in case there is any.
- This way, it is possible to conduct searches and even replace the content of a binary file by editing its printable characters or values in hexadecimal (as needed) directly.
- Existing hexadecimal editors:
 - **iHex** (Mac OS X) – Available on the App Store.
 - **Bless** (Linux) - <http://home.gna.org/bless/downloads.html>
 - **HxD** (Windows) - <https://mh-nexus.de/en/hxd/>

◆◆◆ Basic Tools

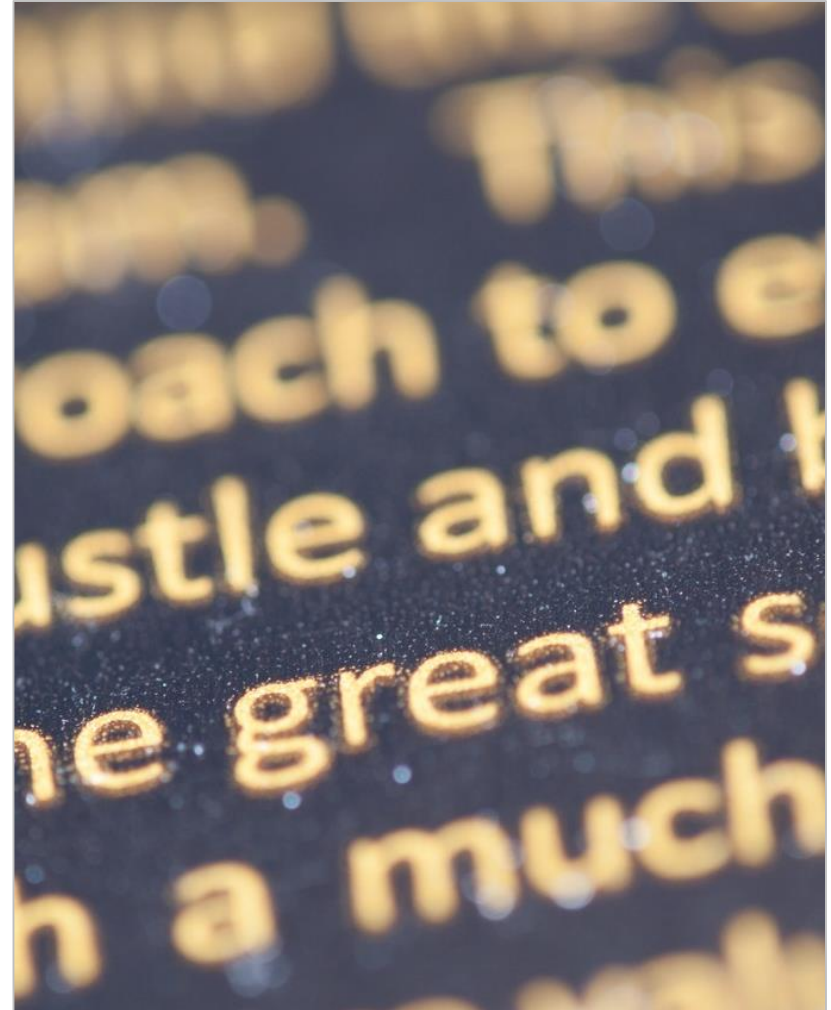
Analysis – SQLite Editor

- SQLite is a quite popular database motor used by most mobile applications for the persistence of data.
- SQLite databases are stored in files with sqlite extension; however, they may also use other extensions such as db, sqllitedb, sqlite3, etc.).
- An SQLite viewer allows the user to inspect the content of such kind of files.
- There are several SQLite editors available for all platforms:
 - **DB Browser**, is a free software project available for all platforms - <http://sqlitebrowser.org>
 - **Sqliteman** – Available in Santoku Linux.



Analysis – Text Editor

- The text editor is useful to access the information stored in text files during the analysis.
- This information may include the following elements among others:
 - XML files.
 - Configuration files.
 - Files with text used by applications.
- Nowadays, there are several editors available for all platforms:
 - **Atom** (multiplatform) - <https://atom.io>
 - **Leafpad** – Available in Santoku Linux.



Analysis - Console Tools

- Apart from the tools mentioned before, there are several console tools that can be useful for the forensic analyst:
 - **Grep**: tool for the search of regular expressions.
 - **Strings**: it identifies printable text chains in a binary file.
 - **Exiftool**: it extracts metadata from a picture.
- Such tools are installed in any Linux distribution (including Santoku).



Sleuth Kit and Autopsy

- **The Sleuth Kit** (TSK) is a set of console tools and a library that enables the analysis of disk images and the recovery of files from such images.
- **Autopsy** is an interface used by Sleuth Kit to manage cases. The analyst may create a new forensic case, load images of acquisitions, create MD5 hashes of different elements of the image, browse the files structure or image blocks, add notes on the forensic analysis that is conducted, etc.
- Sleuth Kit and Autopsy are available in Santoku Linux. In order to open them, it is only necessary to execute it in console (due to the installation, it is necessary to execute it in root mode).
 - > autopsy
- There is a more recent version, but it is only available for Windows environments
 - <http://www.sleuthkit.org>



Methods of Data Acquisition

A woman with long brown hair, wearing a beige trench coat, is looking down at a white smartphone in her hands. She has pink nail polish. The background is a blurred urban scene with modern buildings and a blue sky. A semi-transparent dark grey rectangle is overlaid on the image, containing the text "Types of Data Acquisition" in white.

Types of Data Acquisition

◆◆◆ Methods of Data Acquisition

Introduction I

- Once the evidences to acquire are listed, it is necessary to obtain data related to the devices that will be included in the forensic analysis.
- The method used to acquire the device's data may vary according to:
 - The platform from which data will be obtained (Android, iOS, Windows Phone, BlackBerry, etc.).
 - The specific version of hardware and software as well as the device's configuration (version of the device, current unlock configuration, etc.).
 - The status of the device when it was found (turned on or off, locked or unlocked, etc.).
 - The type of data to acquire and their volatility (data captured in persistent storage or in memory).
- According to the variable mentioned above, it is possible to perform three types of acquisition: manual, logical, and physical.

◆◆◆ Methods of Data Acquisition

Manual Acquisition

- The user interacts with the device to access its data. Data acquisition is performed with screenshots or photographs of the device's screen.
- Such type of acquisition has several advantages:
 - + It does not require additional tools.
 - + It allows users to extract information in a context that is easy to understand by unspecialised readers.
- However, it also includes certain disadvantages:
 - It is only possible to access data that are visible on the screen.
 - It may modify the status of the device.
 - Data processing time is longer.

◆◆◆ Methods of Data Acquisition

Logical Acquisition

- It implies copying files and directories from the device's file system.
- The following elements are used to this aim:
 - Access APIs to the file system of the analysed device. The device's operative system will copy the requested files and directory to other device.
 - APIs of the acquisition tool's operative system. The unit connects to the device to analyse. Data of the analysed system will still be read by the analysed device's firmware.
- Advantages:
 - + It is easy to obtain and, generally, it does not require specialised hardware.
 - + In some cases it is possible to perform it from other device (tested): therefore, APIs of the analysed device are not used.
- Disadvantages:
 - It does not copy deleted files or information that have been hidden on the file system.
 - It depends on access permissions to the system's files.

◆◆◆ Methods of Data Acquisition

Physical Acquisition

- It implies the physical copy of the physical storage device bit by bit.
- It requires full access to the storage device.
- Generally the storage system of a mobile device is brazed to the rest of components and is not accessible physically.
- Furthermore, given the security measures included in mobile operative systems, on many occasions, it is necessary to execute exploits on the system, in order to perform the low-level copy.
- Advantages:
 - + It enables access to all the blocks of the physical support copied, including removed files and blocks that are not marked as used.
- Disadvantages:
 - Usually, it is the most complex process and is not always possible to perform.

◆◆◆ Methods of Data Acquisition

Types of Storage

- The physical acquisition depends on the mobile device's types of storage:
 - The NAND flash memory is the most used one for storing in mobile devices. It may be written and read in blocks.
 - It is mainly used for the operative system storage, system data partition and other removable memories.
 - The NOR memory is another kind of flash memory optimised for the execution of code. It allows the user to read and execute bytes independently.
 - In the last few years, the use of NOR memories –contrary to NAND memories– for generic purposes has decreased.
 - Memory cards use NAND memories. They are generally formatted in FAT32.
 - iOS devices do not allow the use of SD cards. Windows Phone, Android and Blackberry devices allow the use of such SD cards, but it depends on the device model.

Modification of the Acquired Device

- In an ideal environment, the acquisition of data from the device should not modify its physical status.
- Unfortunately, it is not always possible.
- The device's status may be affected according to its characteristics, the type of acquisition performed and tools used:
 - Date and time of access to files.
 - Removal or creation of new files.
 - Modification of the device's memory to load dump applications.
- For the analysis to be valid, it is necessary to document all the types of acquisition performed and consequences of each of them on the analysed device:
 - The manual acquisition will create screenshot files.
 - The logical acquisition may modify the date of access to files.



Maximising Data Acquisition

◆◆◆ Maximising Data Acquisition

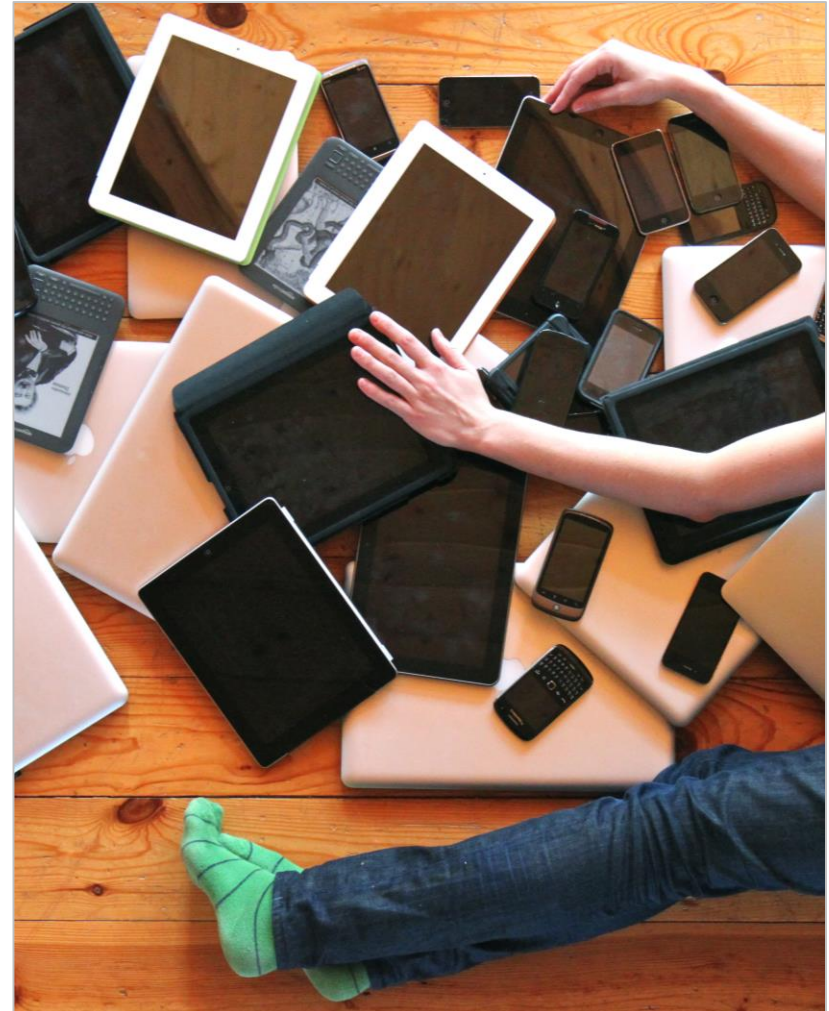
Introduction

- The amount of data accessible on a mobile device largely depends on the status of such device:
 - **Unlocked:** it is possible to access the device until it is blocked due to inactivity.
 - **Locked** with a code or other authentication system: It is necessary to introduce an access code (a fingerprint or similar) to access the device.
 - **Turned off:** in order to access the device, it is necessary to turn it on.
- In order to maximise the amount of data that can be obtained in a device it is essential to follow a group of initial steps. Even though specific steps may vary in each platform, this set of procedures may be performed on any device, regardless the operative system or manufacturer.

◆◆◆ Maximising Data Acquisition

Unlocked Device

- If the device has been seized being unlocked, the following steps should be followed:
 - Isolate the device from the network, turn the Aeroplane Mode on and extract the SIM card. It is advisable to introduce it in a place that shields the device from external electromagnetic radiation (Faraday cage).
 - Activate all the possible options that enables physical access to the device:
 - Deactivate the lock code (if possible).
 - Activate the debugging via USB.
 - Deactivate lock after idle time (always active).
 - Obtain all the removable devices: SD and SIM cards or backups in associated devices (computers).



◆◆◆ Maximising Data Acquisition

Locked Device

- If the device is locked, we only have the following options:
 - Isolate the device from the network, extract the SIM card or place it in a Faraday cage.
 - Check whether the device has debugging via USB activated. In case the USB connection is activated, we may be able to load bootloaders to modify the device's start system and thus, enable physical access to it.
 - If the device has not the USB debugging option deactivated, conduct an attack to extract the lock code (smudge attack or brute force).
 - Obtain all the removable devices: SD and SIM cards or backups in associated devices (computers).
 - If the device is turned off, it is possible to extract the removable media directly and turn the phone on.

A group of green Android robots standing in a row, with the text "Data Acquisition on Android" overlaid in the center.

Data Acquisition on Android

Manual Acquisition

- It is only possible if the phone is unlocked.
- List all the applications existing and take screenshots of the relevant elements.
- In order to access data from some applications it may be necessary to connect the device to the Internet. It should be considered as a last resort, since the device may be locked remotely.
- Apart from applications, it is important to access settings and capture information on each of the existing accounts on the device.
- The method used to take screenshots may be different according to the system version. Generally, screenshots may be taken by pressing the home button and the volume down button at the same time.

◆◆◆ Data Acquisition on Android

Logical Acquisition

- It may be performed via adb, with the following command:

```
> adb backup -apk -shared -system -all -f file.backup
```

Include APK from
Third parties'
Applications

Include
removable
storage

Include
system
Applications

Include all
The applications

Output file

- Applications that do not allow backups will not be copied.
- Once the backup has been obtained, it can be extracted by using:
 - Android Backup Extractor - <https://sourceforge.net/projects/adbextractor/>
- And the command:

```
> java -jar abe.jar unpack file.backup file.tar
```
- It is also possible via apps (information on the phone will only be accessible via permissions):
 - AFLocal – Available in Santoku Linux.

◆◆◆ Data Acquisition on Android

Physical Acquisition

- It is only possible to perform in case we have administrator access to the device or via physical access and a connection to the JTAG interface of the memory chip.
- If the device is rooted, it is possible to perform it with dd.
- First, it is necessary to search the path to the flash memory:
 - > `cat /proc/partitions`
 - The first entry (generally, mmcblk0) corresponds to the whole flash memory.
- Discover the block size of the system:
 - > `df /data`
- Execute dd with the information obtained on the Blksize column:
 - > `dd if=/dev/block/mmcblk0 of=/sdcard/blk0.img bs=4096`
 - *conv=notrunc,noerror,sync*
- If the disk image is stored in the SD card, it is necessary to ensure that the introduced card has been erased properly (all 0s).

Physical Acquisition - Memory

- The implementation of dd for Android is not properly prepared to read the device's RAM memory.
- The device's memory may be obtained by using Linux Memory Extractor (LiME), a tool that is responsible for:
 - Discovering the physical addresses of the RAM's address ranges by inspecting the kernel.
 - Transforming physical addresses into virtual.
 - Copying the content of virtual addresses to a network socket or the SD card in order to be extracted.
- LiME is a kernel extension that should be loaded via adb (the process will be studied during a laboratory).
- The acquisition of separated processes' RAM memory is also possible in devices that are in production process (or the emulator) via Android Device Monitor.

Data Acquisition on iOS



◆◆◆ Data Acquisition on iOS

Manual Acquisition

- It is only possible if the phone is unlocked.
- To unlock de lock code it is necessary to know the established one, therefore, it is advisable to deactivate the automatic lock.
- List all the applications existing and take screenshots of the relevant elements.
- In order to access data from some applications it may be necessary to connect the device to the Internet. It should be considered as a last resort, since the device may be locked remotely.
- It is possible to access the diagnostic data sent to applications developers in the privacy settings.

◆◆◆ Data Acquisition on iOS

Logical Acquisition

- It may only be performed if the phone is unlocked or has no lock code.
- On iOS9, select “Trust this computer”.
- Via iTunes:
 - The device is connected to iTunes and the backup is performed.
 - If the backup is encrypted, a brute force attack should be conducted in order to decrypt it:
 - There are payment tools to perform this task (<https://www.elcomsoft.com/eppb.html>).
- Via idevicebackup (idevicebackup2):
 - Available in two different versions of Snatoku, according to iOS version:
 - `> idevicebackup backup directory`
 - If the device is jailbroken, it is possible to install the SSH server or the device application to open an SSH connection to other computer.
- If iCloud is used, Apple account credentials associated to the device are required.

◆◆◆ Data Acquisition on iOS

Logical Acquisition

- Via applications such as iFunBox or iPhone Explorer:
 - The support depends on the operative system version.
 - It enables access to the sandbox of each application.
 - If the device is jailbroken, it is possible to access all the files system.
- The information extracted through such methods does not include:
 - Emails.
 - Location history.
 - Applications cache.
 - Executable files.



◆◆◆ Data Acquisition on iOS

Physical Acquisition

- If the device is jailbroken, the procedure to perform it is similar to Android's:
 - Execute the following command from the analyst's computer:
> `ssh root@ip dd if=/dev/rdisk0 bs=1M | dd of=ios-root.img`
 - Execute dd on the iPhone via SSH and redirect the output of the command to the image on the analyst's computer (with the dd command again).
 - Since the creation of iPhone 3GS, this tool is not very useful, since the device's flash memory is encrypted.
- Via commercial applications such as:
 - Lantern by Katana Forensics - <https://katanaforensics.com>
 - Mobile Phone Examiner by Access Data - <http://accessdata.com>
 - Encase.
 - FTK.
 - Such type of tools are able to extract the encryption key and decrypt the resulting image.

Data Acquisition on Windows Phone



◆◆◆ Data Acquisition on Windows Phone

Manual Acquisition

- It is only possible if the phone is unlocked.
- To unlock de lock code it is necessary to know the existing one, therefore, it is advisable to deactivate the automatic lock.
- List all the applications existing and take screenshots of the relevant elements.
- In order to access data from some applications it may be necessary to connect the device to the Internet. It should be considered as a last resort, since the device may be locked remotely.
- Apart from applications, through the phone settings, it is also possible to access last connected Wi-Fi networks and other relevant configuration data of the phone.

◆◆◆ Data Acquisition on Windows Phone

Logical Acquisition



- Before Windows Phone 7.5 it could be performed via the Windows Phone Device Manager application.
- From Windows Phone 8.0, the device's storage is not accessible via USB connection.
- Acquisition is only possible via the backup tool on cloud, by using the credentials of the account associated with the device.

◆◆◆ Data Acquisition on Windows Phone

Physical Acquisition



- There are no forensic applications that support the physical extraction of Windows Phone devices.
- The only possible option is the acquisition through the JTAG interface of the flash memory. If the device is encrypted (business use), this task is not very useful.



Data Acquisition on BlackBerry

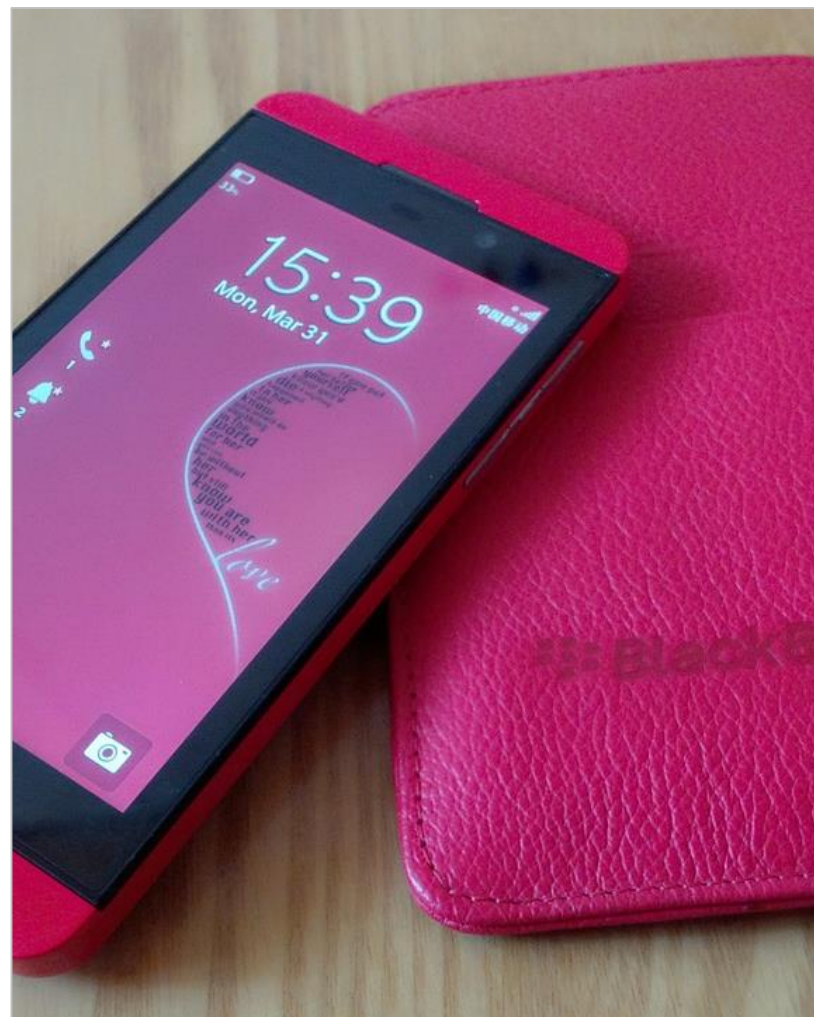
Manual Acquisition

- It is only possible if the phone is unlocked.
- To unlock de lock code it is necessary to know the existing one, therefore, it is advisable to deactivate the automatic lock.
- List all the applications existing and take screenshots of the relevant elements.
- In order to access data from some applications it may be necessary to connect the device to the Internet. It should be considered as a last resort, since the device may be locked remotely.
- Apart from applications, through the phone settings, it is also possible to access last connected Wi-Fi networks and other relevant configuration data of the phone.

◆◆◆ Data Acquisition on BlackBerry

Logical Acquisition

- Apart from the device, the SD card can also be encrypted (in case the model has an SD slot).
- The only available method is the use of access credentials of BlackBerry Link account of the associated device. It is possible to download the backup of the device in order to analyse it with the appropriate forensic tools from the account itself.



◆◆◆ Data Acquisition on BlackBerry

Physical Acquisition

- Elements stored in BlackBerry devices are encrypted, therefore, it is not useful to extract the device physically to conduct the forensic analysis.





Data Acquisition Laboratory

Introduction

- In this part of the unit, a series of laboratories aimed at showing information extraction techniques for mobile devices will be performed.
- Specifically, the following activities will be carried out:
 - Acquisition of a forensic image of an Android Device.
 - Acquisition of an image of an SD card.
 - Acquisition of a forensic image of an iOS Device.
 - Logical Acquisition of an Android Device.
 - Memory Acquisition of an Android Device.
- In this case, laboratories will be described as a set of steps to follow at the same time that they are displayed on the screen.

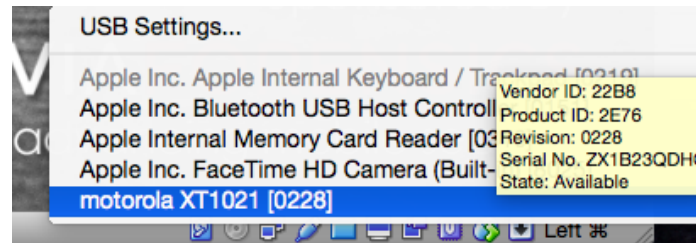
A photograph of a smartphone with a white keyboard and earbuds on a wooden desk. The smartphone screen is orange and displays a white icon of a person with a speech bubble, and the text "Google play" is visible at the bottom. A semi-transparent text box is overlaid on the image.

Forensic Image of an Android Device

◆◆◆ Forensic Image of an Android Device

Connection of the Device

- A rooted device is required in order to perform this laboratory.
- The device's image will be acquired via USB connection; therefore, it has to be connected to the analysis computer.
- Since the image will be performed in Santoku, connect the device to the virtual machine in VirtualBox.



- In Settings, select the 2.0 or 3.0 USB option, according to the device. To do this, it is necessary to download a VirtualBox extension.
 - <https://www.virtualbox.org/wiki/Downloads>

◆◆◆ Forensic Image of an Android Device

Preparation of the Acquisition

- Once connected in Santoku, open a shell on the device and switch to the root user:

```
santoku@santoku-VirtualBox:~$ adb shell
shell@condor_ums:/ $ su
root@condor_ums:/ #
```

- Since the only partition that can be modified by the user is the one in `data`, use `mount` to discover the corresponding device:

```
root@condor_ums:/ # mount | grep data
/dev/block/platform/msm_sdcc.1/by-name/system /system ext4 ro,seclabel,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/userdata /data ext4 rw,seclabel,nosuid,nodev,noatime,nodiratime,disca
d,nobarrier,noauto_da_alloc,data=ordered 0 0
```

- Then, find out the size of the block:

```
root@condor_ums:/ # df /data
Filesystem      Size      Used    Free  Blksize
/data           2.2G      1.2G    941.7M    4096
```

◆◆◆ Forensic Image of an Android Device

Acquisition of the Image

- The acquisition requires an empty SD card in the device.
- Depending on the Android version and the device, the card will be installed on a directory.

```
root@condor_ums:/ # mount | grep sdcard
/dev/block/vold/179:65 /mnt/media_rw/sdcard1 vfat rw,dirsync,nosuid,nodev,n
mask=0007,dmask=0007,allow_utime=0020,codepage=cp437,iocharset=iso8859-1,sh
ro 0 0
/dev/fuse /storage/sdcard1 fuse rw,nosuid,nodev,relatime,user_id=1023,group
other 0 0
root@condor_ums:/ #
```

- In order to perform the acquisition, execute dd with the corresponding parameters.

```
> dd if=/dev/block/platform/msm_sdcc.1/by-name/userdata  
of=/storage/sdcard1/user.img bs=4096
```
- Once the image has been performed from the console of the analysis computer.

```
> adb pull /storage/sdcard1/user.img
```
- Then, the image of the user's partition is obtained.

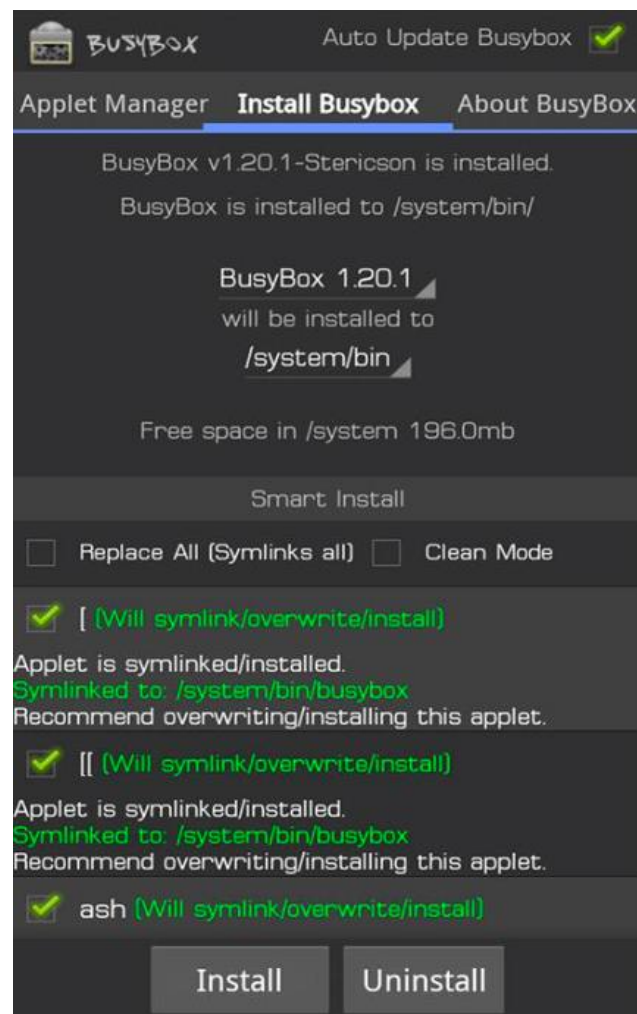


Image of an SD Card

◆◆◆ Image of an SD card

Installation of Busybox

- In order to acquire images from SD cards, another device is required to store the captured image.
- With BusyBox, it is possible to redirect data created by dd, directly to a port where they are received by the analysis computer.
- You can install BusyBox via Google Play:
 - <https://play.google.com/store/apps/details?id=stericson.busybox>
- Once installed, execute and install it without accepting advertising messages.



◆◆◆ Image of an SD Card

Acquisition of the Image

- Find out the device corresponding to the memory card:

```
root@condor umts:/ # mount | grep sdcard
/dev/block/vold/179:65 /mnt/media_rw/sdcard1 vfat rw,dirsync,nosuid,nodev,n
mask=0007,dmask=0007,allow_utime=0020,codepage=cp437,iocharset=iso8859-1,sh
ro 0 0
/dev/fuse /storage/sdcard1 fuse rw,nosuid,nodev,relatime,user_id=1023,group
_other 0 0
root@condor_umts:/ #
```

- Since the image cannot be stored in the SD card, transmit it to the analysis computer through a socket. To this end, write the following command in a new terminal on the analysis computer:

```
santoku@santoku-VirtualBox:~$ adb forward tcp:8888 tcp:8888
```

- This way, we make sure that all the elements that reach adb via the 8888 port, are transmitted to the analysis computer through the same port.
- Execute:
 - > `dd if=/dev/block/vold/179:65 | busybox nc -l -p 8888`
- Then, the information is received by the analysis computer through the following command:

```
santoku@santoku-VirtualBox:~$ nc 127.0.0.1 8888 > sd_image.dd
santoku@santoku-VirtualBox:~$
```


A close-up, side-profile shot of a person with long brown hair holding a silver iPhone. The phone's screen is lit up, showing a grid of colorful app icons. The person is wearing a light-colored, possibly white, long-sleeved shirt. The background is a blurred indoor setting, likely a home or office, with a desk and some electronic equipment visible. A semi-transparent dark grey rectangular box is overlaid across the middle of the image, containing the text 'Forensic Image of an iOS Device' in white.

Forensic Image of an iOS Device

◆◆◆ Forensic Image of an iOS Device

Extraction of the Image

- As on Android, the image acquisition of the device requires administrator permissions and thus, jailbreak.
- In this case, the acquisition of the device's image is performed via an SSH connection; therefore, the device has to be connected to the same Wi-Fi network as the analysis computer.
 - The installation of such kind of tools was explained in the third unit of this course.
- In order to perform the extraction, it is only necessary to execute the following command:

```
> ssh root@ip_iphone dd if=/dev/rdisk0 bs=1M | dd of=imagen-ios.img
```
- Once finished the command, a full image of the device will be obtained.
- If the device used is an iPhone 3GS or newer, the image will be encrypted; therefore, it will not be useful. It is necessary to use a commercial tool.

Logical Acquisition of an Android Device



◆◆◇ Logical Acquisition on Android

Installation of AFLogical

- In this laboratory, the AFLogical tool will be used for the logical acquisition of evidences.
- AFLogical is an Android application that includes the permissions required to extract all the information that is accessible through permissions of an Android system:
 - Call history.
 - Contacts.
 - SMS and MMS messages and attached files.
- Since it is executed through a normal application, a rooted phone is not required.
- In order to install it from a command line on Santoku:

```
> aflogical-ose
```
- It will install and execute the application.

◆◆◆ Logical Acquisition on Android

Execution of AFLogical

- Once the application is executed, it is necessary to select the information that is going to be extracted on the device.
- Once obtained the information on the device, continue on the console in order to transfer data to our device.

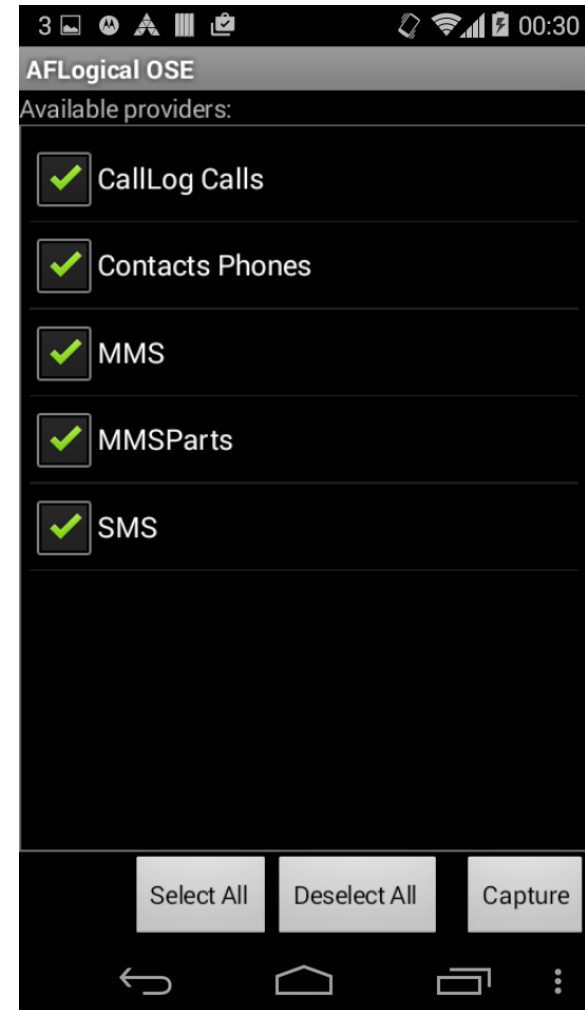
```
santoku@santoku-VirtualBox:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:

697 KB/s (28794 bytes in 0.040s)
  pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

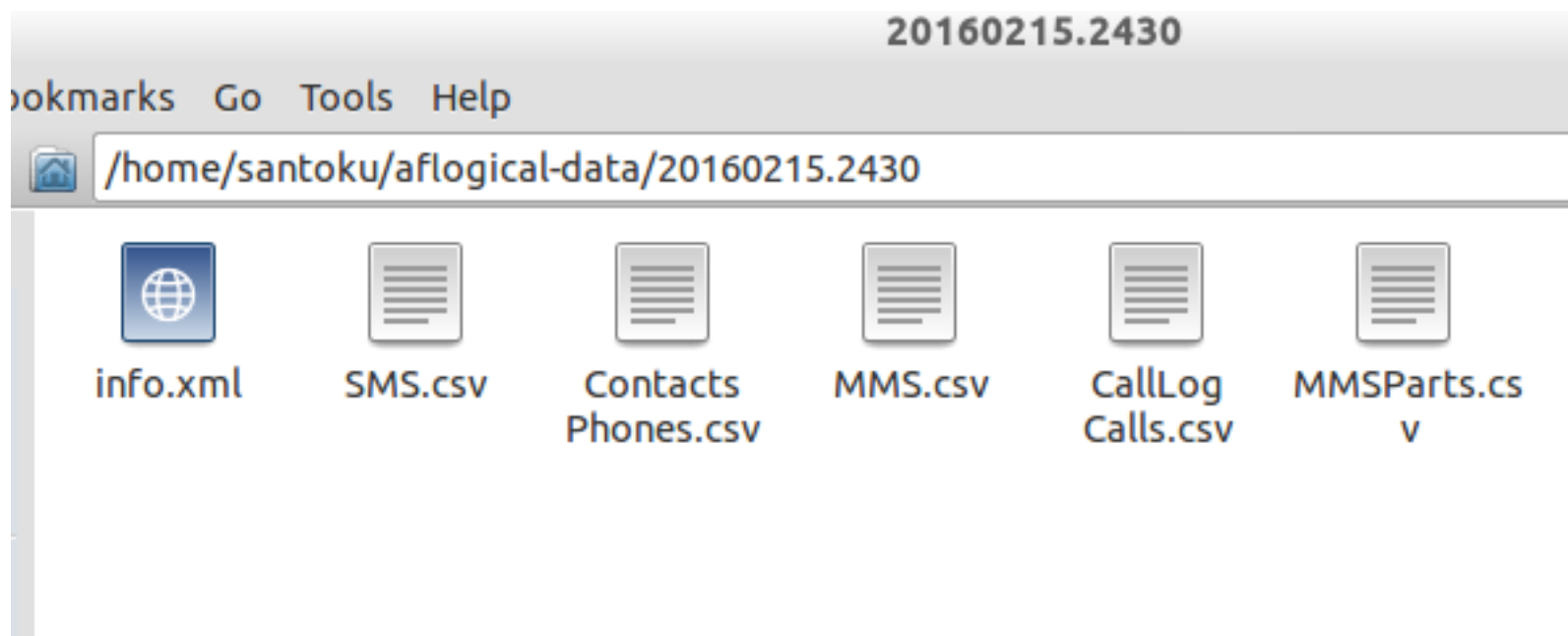
pull: building file list...
pull: /sdcard/forensics/20160215.2430/SMS.csv -> /home/santoku/aflogical-data/20
160215.2430/SMS.csv
pull: /sdcard/forensics/20160215.2430/MMS.csv -> /home/santoku/aflogical-data/20
160215.2430/MMS.csv
```



◆◆◆ Logical Acquisition on Android

Results

- The results can be inspected by using the file browser of Santoku Linux.



The background of the slide is a close-up photograph of an Android phone's home screen. It features a scenic wallpaper of a forest path with sunlight filtering through the trees. Several app icons are visible: Google Maps (a colorful pin), YouTube (a red play button), a white circular icon with five dots, the Google Chrome logo (a four-colored wheel), the Gmail icon (a white envelope with a red border), and a green speech bubble icon. At the bottom, a white square icon representing the recent apps button is visible. A semi-transparent grey rectangle is overlaid on the center of the screen, containing the title text.

Memory Acquisition of an Android Device

◆◆◇ Memory Acquisition on Android

Installation and Execution of LiME

- As in previous laboratories, on this occasion a rooted device is required.
- First, it is necessary to download and compile LiME.
 - Installation guide: <https://github.com/504ensicsLabs/LiME/tree/master/doc>
- Once compiled, it is necessary to copy the module to the device that is going to be used to acquire the memory:

```
> adb push lime.ko /storage/sdcard1/lime.ko
```
- Modify the ports to redirect the LiME output:

```
> adb forward tcp:4444
```
- Open a shell:

```
> adb shell
```
- Access a root and execute the kernel module:

```
> su  
  
> insmod /sdcard/lime.ko "path=/storage/sdcard1/ram.lime  
format=lime"
```

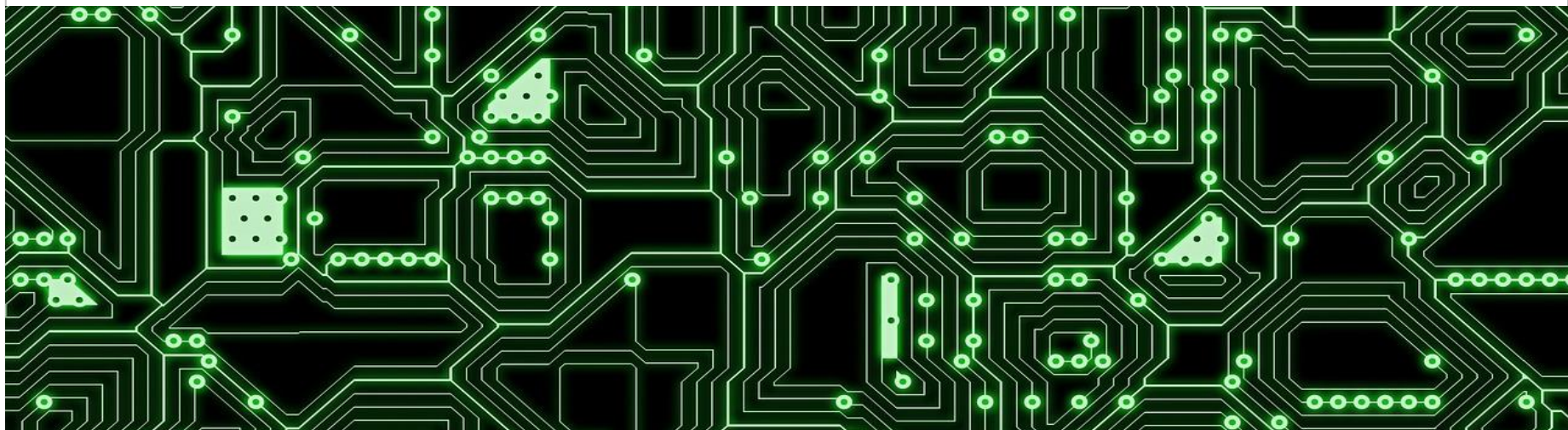
◆◆◆ Memory Acquisition on Android

Transmission of the Image

- The image is created in lime format in the sd card of the system.
- To obtain it on the analysis computer, use adb.

```
> adb pull /storage/sdcard1/ram.lime
```
- The image obtained may be analysed with volatility. It is necessary to have it installed in Santoku:

```
> sudo apt-get install volatility
```



A blurred background image of a laptop screen showing a data analysis dashboard. The dashboard includes a line graph with a legend for 'New Visitor' and 'Returning Visitor', and a pie chart showing a 27.8% segment. The text 'Data Analysis' is overlaid in white on a blue semi-transparent rectangle.

Data Analysis

Data of Interest Formats

```
78 // ... strlen( realpath($_SERVER['DOCUMENT_ROOT']) )) . '?_CAPTCHA=' .
79 // ... ltrim(preg_replace('/\\\\\\\\/', '/', $image_src), '/');
80 $_SESSION['_CAPTCHA']['config'] = serialize($captcha_config);
81 return array(
82     'code' => $captcha_config['code'],
83     'image_src' => $image_src
84 );
85 }
86
87
88 if( !function_exists('hex2rgb') ) {
89     function hex2rgb($hex_str, $return_string = false) {
90         $hex_str = preg_replace("/[^0-9A-Fa-f]/", '', $hex_str); // Gets a proper hex string
91         $rgb_array = array();
92         if( strlen($hex_str) == 6 ) {
93             $color_val = hexdec($hex_str);
94             $rgb_array['r'] = 0xFF & ($color_val >> 0x10);
95             $rgb_array['g'] = 0xFF & ($color_val >> 0x8);
96             $rgb_array['b'] = 0xFF & $color_val;
97         } elseif( strlen($hex_str) == 3 ) {
98             $rgb_array['r'] = hexdec(str_repeat(substr($hex_str, 0, 1), 2));
99             $rgb_array['g'] = hexdec(str_repeat(substr($hex_str, 1, 1), 2));
100             $rgb_array['b'] = hexdec(str_repeat(substr($hex_str, 2, 1), 2));
101         } else {
102             return false;
103         }
104         return $return_string ? implode($separator, $rgb_array) : $rgb_array;
105     }
106 }
107
108 // Draw the image
109 if( isset($_GET['captcha']) ) {
```

Introduction I

- During the analysis stage, evidences acquired are reviewed and studied.
- Given the huge amount of information stored in nowadays mobile phones, it is not advisable to use a strategy that extracts all the available information from the device without order or justification.
- According to the origin of evidences and the specific case, a series of hypothesis should be stated.
- Such hypothesis will be proved or refuted through the analysis of data established in the exam stage, and additional data that may be required during the analysis.
- During the rest of the section, the following elements will be described:
 - The main types of data that can be found on a device.
 - The way of analysing them, according to the type of evidence acquired.
 - The main type of data of interest on the principal platforms.

◆◆◆ Data of Interest Format

Introduction II

- Regardless the platform or the operative system, many applications use the same formats to store persistent information.
- Getting to know the structure and components of such kinds of files may be useful to identify the existence of information stored in a specific format, even if the file has been removed from the system.
- The most interesting types of files, from the point of view of the forensic analysis are specified below:
 - XML files.
 - SQLite databases storage files.
 - Photographs and their metadata (EXIF).
 - Plain text files and strings included in them.

◆◆◆ Data of Interest Format

XML Files

- XML files (eXtensible Markup Language) are text files that include information structured by marks.
- They are mainly used to storage preferences.
- XML only defines the structure of the file, but not its content.
 - According to the platform, the content of the files will be different.
 - They generally begin with the following line:
 - `<?xml version="1.0" encoding="UTF-8"?>`
- Generally, XML files have an xml extension, but they can also be found with other extensions (plist on iOS, for example).
 - Plist files also include a header and have specific tags:
 - `<plist version="1.0">`
 - `<key><dict><integer>`

◆◆◆ Data of Interest Format

SQLite Files

- SQLite files are organised in fixed size pages that are filled in from the bottom.
- As on a file system, when the content of the page is not required, it is marked as empty, but is not removed (efficiency). Some editors allow the user to inspect such content:
 - Sqlite Viewer - <http://www.sqliteviewer.org>
- The storage is made in files with different extensions. Sqlite and db are the most used ones:
 - In some cases, changes in a database are stored in a file with the same name, but with the “-journal” or “-wal” extension added.
 - In order to reconstruct all the information of the database, it is necessary to access both files.
- Regardless its extension, all the SQLite files begin with the `SQLite format 3` string for the version 3 of the format. It can be used to find sqlite files removed from the system.

◆◆◆ Data of Interest Format

Photographs - EXIF



- EXIF corresponds to Exchangeable image file format.
- The EXIF format allows the user to add a series of metadata to photographs and videos captured with all kinds of cameras.
- In the case of mobile phones, apart from the model of the device and the configuration of the camera, EXIF data may also provide information on the location in which the picture was taken.
- Such kind of information may be very relevant to establish timelines and locate the device in places related to the events that are investigated.

Text Files

- Text files store all type of non-encrypted information:
 - Note texts.
 - Configuration of applications, etc.
- Since the contents of the text files are stored in the device without encryption, it is possible to conduct searches to find data.
- It enables the extraction of data from existing files, but it also facilitates the search for information in removed blocks.
- On many occasions, the keys and the type of word searched will be related to the specific case that is investigated.
- Some keys that may be interesting include:
 - Password, pass, pass= password=.
 - User, location.
 - Personal names, places, etc.

A close-up photograph of a person's hand moving a white chess piece on a wooden chessboard. The person's face, wearing glasses, is blurred in the background. The chessboard has alternating light and dark squares, and various wooden pieces are visible.

Type of Analysis According to the Evidence Acquired

Analysis of Executable Binary Files

- Depending on the type of case, it may be necessary to analyse the binary executable files of a device:
 - Intrusion via malware.
 - Need for extraction of data from a specific application.
- Specifically, the following elements may be interesting in a forensic investigation:
 - Credentials stored by the application.
 - Data of the application such as history of conversations (Whatsapp), history of purchases, etc.
 - Interaction of the application with the system's APIs.
- Once the elements of interest are identified, they will be analysed by using the techniques described in Unit 3.
- In order to validate the forensic analysis, it is necessary to document and validate the process of extraction of information, in case it has not been previously documented by other investigators.

File System Analysis

- It implies analysing the different mechanisms and data of interest that may be found in the file system of a device.
- The location of the different elements will depend on the platform, version, device, etc. This analysis is beneficial due to the general consistency in all the devices of the same platform and version.
- The analysis of the file system is generally performed by mounting the acquired images in read-only mode.
- This way, it is possible to navigate the files structure of the system in order to search data or mechanisms of interest.
- Depending on the data acquisition system, once installed the disk, it may also be possible to conduct an analysis of the space that is not used by it.

Analysis of Deleted Space - File Carving

- Generally, on traditional file systems, removing a file only marks as available the disk blocks in which the file was stored.
- The content of the blocks remains intact until they are requested by the file system.
- Depending on the type of file, size, and status of the blocks in which it was stored, it may be possible to recover its content.
- In order to analyse the deleted space it is important to take into consideration the type of files to recover.
- Depending on the type of file and information to recover, the procedure will be one or another.

Analysis of Deleted Space - File Carving

- Most files of interest have a specific header beginning:
 - `SQLite Format 3` (in ASCII notation) for sqlite files.
 - `%PDF` (in ASCII notation) for pdf files.
 - `\211PNG\r\n` (in ASCII notation) for png files.
 - `FFD8` (in hexadecimal) for jpeg files.
- At the same time, the size of the file is described on its header:
 - If the file is smaller than the block size, a search will not be necessary.
 - If the file is bigger, the search will be conducted first in contiguous blocks and then, in other blocks of the disk, in case it was not successful (using different heuristics).
- Fortunately, there are tools (such as Scalpel, available in Santoku) that perform this task automatically.
- On some occasions, it is not necessary to recover the whole file. For example, in order to retrieve a password, it is possible to conduct string searches such as password, pass, etc. Such kind of search can be performed with the console program strings (available in Santoku) or an hexadecimal editor.

Memory Analysis

- It implies analysing a memory dump:
 - The dump may include the whole memory of the device.
 - Or only a process.
- There are two types of analysis:
 - Brute force analysis: the memory is analysed as a stream of bytes. It allows the user to search strings and other data. However, the analysis of variables, code, etc. is more complex.
 - Organised: it uses a memory map to interpret the different values and the structure of the image file captured. It allows the user to distinguish the parts of the code and the memory data. As in the file system, the organisation of the device's memory depends on the device and the operative system version used.
- If, due to device restrictions, the extraction is made to the SD card, it is important to ensure that the SD card has been copied. This rule violates the acquisition order from volatile to less volatile. However, in some cases it is necessary.

Backup Analysis

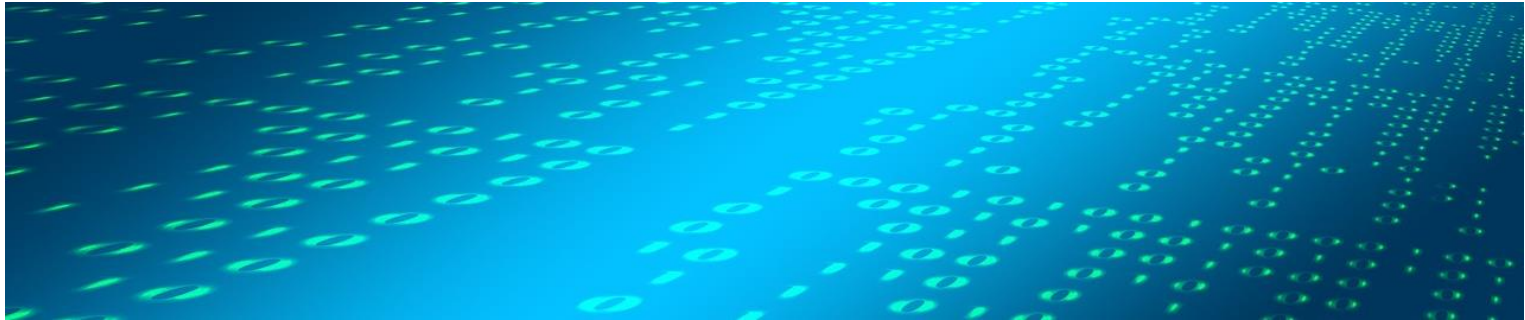
- It implies analysing backups performed on a device:
 - Through a computer that the device has been connected to.
 - Through the backup services on the cloud.
- The structure and location of files stored in the backup is different from the physical structure of the device.
- In order to check the accuracy of data stored in the backup, it is possible to use a device in order to dump the copy.
- In case the backup has been encrypted, it will be necessary to discover the password:
 - Phone Password Breaker allows the user to extract the password used, via brute force attacks - <https://www.elcomsoft.com/eppb.html>
 - Such types of tools are not able to extract encrypted backups from BlackBerry 10 devices. For such cases, BlackBerry Link credentials are required.

Analysis on Different Platforms



Files of interest for each mobile platform will be reviewed below. Elements such as memory, backup, or file system will be analysed depending on the platform.

Furthermore, it will be possible to apply unassigned blocks search techniques on each of the studied platforms, as it was mentioned in this section.



The image features the green Android robot character on the right side, set against a dark background with out-of-focus blue and orange light circles (bokeh). A semi-transparent grey rectangle is positioned in the center, containing the text "Analysis on Android".

Analysis on Android

General Aspects

- Generally, the information analysed on an Android device will be presented in the following form:
 - **SharedPreferences files:** XML files that store key-value pairs.
 - **SQLite databases with different extensions:** ContentProviders of the system are generally stored in sqlite files.
 - **Non-encrypted text files.**
 - **Binary files:** images.
- Files can be stored in:
 - Internal storage of the device (protected from other applications' access in case it is not rooted).
 - External storage of the device (easily accessible by the rest of applications).

File System

- Android's file system is divided into various partitions:
 - **bootloader**: read-only partition. The first code executed when the phone is turned on. Loads Android's kernel.
 - **boot**: includes Android's kernel.
 - **splash**: saves the image that is displayed when the device is initiated.
 - **userdata**: stores all the user's data (applications, pictures, etc.).
 - **System**: includes libraries, system's applications and Android's framework.
 - **Cache**: it stores files used temporarily by the applications (including the Dalvik virtual machine).
- All the processes have access to certain restricted directories (including the adb process).

◆◆◆ Analysis on Android

Directories of Interest – Applications of the System

- System applications on Android are located in ***/system/app***
- This partition is read-only. It only stores APK and odex files (code of the application prepared to be executed in the virtual machine).
- Data created by applications are stored in ***/data/data/***

```
root@condor_umts:/data/data # ls -las
total 552
drwxr-x--x u0_a3    u0_a3          1970-02-26 01:42 com.android.backupconfirm
drwxr-x--x bluetooth bluetooth      1970-02-26 01:44 com.android.bluetooth
drwxr-x--x u0_a49    u0_a49          1970-02-26 01:43 com.android.browser.provider
drwxr-x--x u0_a50    u0_a50          1970-02-26 01:43 com.android.calculator2
drwxr-x--x u0_a6     u0_a6          1970-02-26 01:44 com.android.calendar
drwxr-x--x u0_a51    u0_a51          1970-02-26 01:44 com.android.cellbroadcastreceiver
drwxr-x--x u0_a52    u0_a52          1970-02-26 01:43 com.android.certinstaller
drwxr-x--x u0_a53    u0_a53          2016-02-13 18:02 com.android.chrome
drwxr-x--x u0_a9     u0_a9          1970-02-26 01:42 com.android.contacts
drwxr-x--x u0_a12    u0_a12          2016-02-13 15:43 com.android.defcontainer
drwxr-x--x u0_a14    u0_a14          1970-02-26 01:44 com.android.deskclock
drwxr-x--x u0_a16    u0_a16          1970-02-26 01:44 com.android.dialer
drwxr-x--x u0_a55    u0_a55          1970-02-26 01:43 com.android.documentsui
drwxr-x--x u0_a47    u0_a47          1970-02-26 01:43 com.android.dreams.basic
drwxr-x--x u0_a79    u0_a79          1970-02-26 01:43 com.android.dreams.phototable
drwxr-x--x u0_a18    u0_a18          1970-02-26 01:44 com.android.email
drwxr-x--x u0_a57    u0_a57          1970-02-26 01:44 com.android.exchange
drwxr-x--x u0_a19    u0_a19          2016-02-13 16:16 com.android.externalstorage
drwxr-x--x u0_a65    u0_a65          1970-02-26 01:43 com.android.htmlviewer
```

```
root@condor_umts:/ # cd /system/app/
3c_main.apk
3c_main.odex
AonIntLT.apk
AonIntLT.odex
BasicDreams.apk
BasicDreams.odex
Bluetooth.apk
Bluetooth.odex
BluetoothExt.apk
BluetoothExt.odex
Books.apk
BrowserProviderProxy.apk
Bug2GoStub.apk
Calculator.apk
Calculator.odex
CellBroadcastReceiver.apk
CellBroadcastReceiver.odex
CertInstaller.apk
CertInstaller.odex
Chrome.apk
```

◆◆◇ Analysis on Android

Directories of Interest – Applications of the System

- **APK files** are stored in */data/app*

```
[root@condor_umts:/data/app # ls -las
total 105028
-rw-r--r-- system system 32940855 2016-02-13 20:35 com.facebook.katana-1.apk
-rw-r--r-- system system 46874450 2016-02-13 20:39 com.snapchat.android-1.apk
-rw-r--r-- system system 27726782 2016-02-13 20:37 com.spotify.music-1.apk
```

- **Sandboxes** are located in */data/data/*

```
drwxr-x--x u0_a74 u0_a74 1970-02-26 01:43 com.motorola.motosignature.app
drwxr-x--x u0_a84 u0_a84 1970-02-26 01:43 com.motorola.pgmsystem2
drwxr-x--x radio radio 1970-02-26 01:43 com.motorola.programmenu
drwxr-x--x u0_a38 u0_a38 1970-02-26 01:45 com.motorola.setup
drwxr-x--x u0_a41 u0_a41 2016-02-13 17:48 com.motorola.so
drwxr-x--x u0_a45 u0_a45 1970-02-26 01:44 com.motorola.wappushi
drwxr-x--x system system 1970-02-26 01:44 com.qualcomm.atfwd
drwxr-x--x u0_a67 u0_a67 1970-02-26 01:43 com.qualcomm.interfacepermissions
drwxr-x--x system system 1970-02-26 01:43 com.qualcomm.location
drwxr-x--x u0_a85 u0_a85 1970-02-26 01:43 com.qualcomm.qcom_qmi
drwxr-x--x radio radio 1970-02-26 01:44 com.qualcomm.qcrilmsgtunnel
drwxr-x--x system system 1970-02-26 01:44 com.qualcomm.qualcommsettings
drwxr-x--x system system 1970-02-26 01:44 com.qualcomm.services.location
drwxr-x--x u0_a89 u0_a89 2016-02-13 15:43 com.qualcomm.timeservice
drwxr-x--x u0_a86 u0_a86 1970-02-26 01:43 com.quickoffice.android
drwxr-x--x u0_a95 u0_a95 2016-02-13 20:37 com.spotify.music
drwxr-x--x u0_a93 u0_a93 2016-02-13 18:02 eu.chainfire.supersu
drwxrwx--- media media 1970-02-26 01:42 media
drwxr-x--x bluetooth bluetooth 1970-02-26 01:43 orq.codeaurora.bluetooth
```

- It is possible to verify how each application is associated to a specific user.

Structure of an Application's Sandbox

- The directory of each Android application is structured into the following folders (not all of them are included in all the applications):
 - **files**: it stores files that the application may create and require during its execution. It may be useful to store pictures or other elements used by the application.
 - **lib**: it stores links to directories in which libraries specifically compiled for the platform required by the application are stored.
 - **shared_prefs**: it stores Shared Preferences files created by the application.
 - **databases**: it stores the sqlite files (providers) that the application uses.
 - **cache**: temporary files used by the application.

```
[root@condor_umts:/data/data/com.spotify.music # ls
app_MixpanelAPI.Images.DecideChecker
app_MixpanelAPI.Images.ViewCrawler
cacert.pem
cache
code_cache
databases
files
lib
shared_prefs
_
```

◆◆◇ Analysis on Android

Data of Interest – Photographs

- The directory that stores photographs on Android largely depends on the manufacturer and the type of exact ROM:
 - */storage/emulated/DCIM*, if the device has not an SD card.
 - */storage/sdcardX/DCIM*, if the device has an SD card.
- Depending on the use of the phone, there may be pictures in both locations.
- Inside the DCIM folder, pictures taken with the device camera are stored in the Camera folder.

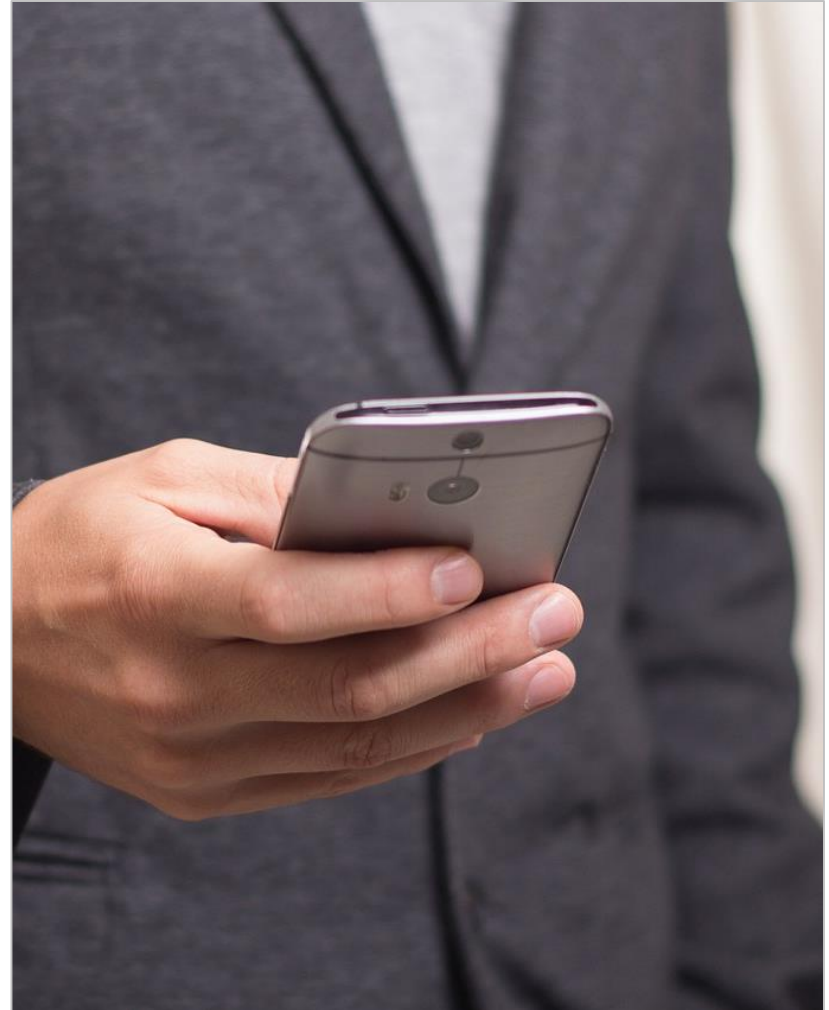
```
[root@condor_umts:/storage/emulated/0/DCIM # ls
Camera
[root@condor_umts:/storage/emulated/0/DCIM # cd Camera
[root@condor_umts:/storage/emulated/0/DCIM/Camera # ls
IMG_20160213_201017879.jpg
IMG_20160213_201022555.jpg
root@condor_umts:/storage/emulated/0/DCIM/Camera # █
```

- Regardless the storage device, pictures may be accessed from the analyst's computer itself via USB connection (or the image of the SD card).

◆◆◇ Analysis on Android

Data of Interest – Keyboard Cache

- Android stores the words selected by the user as a part of the predictive system of the keyboard in a **Content Provider**:
/data/data/com.android.providers.userdictionary/database/user_dict.db
- Words written in password fields are not stored in this dictionary.
- It does not include timestamps.



Data of Interest – Passwords and Settings

- In case it has been configured, the lock code is stored in:
 - */Data/system/gesture.key*, if it is a lock pattern:
 - Each dot of the pattern has a number assigned (beginning with 0 from the upper-left dot).
 - A summary of the link between the byte value of the pattern is made (e.g.: 01254).
 - Given the scarce number of possible combinations, it is easy to obtain it by creating all the combinations in SHA1.
 - <http://forensics.spreitzenbarth.de/2012/02/28/cracking-the-pattern-lock-on-android/>
 - */Data/system/password.key*, if it is a numeric code:
 - It stores the summary of the numeric code together with a seed in SHA and MD5 (both concatenated).
 - The location in which the seed is stored depends on the Android version:
 - */data/data/com.android.providers.settings/databases/settings.db*
 - */data/system/locksettings.db*
 - In both files it is stored in *lockscreen.password_salt*
 - Once the seed and the final hash are obtained, it is possible to perform a dictionary attack in order to obtain the original PIN or password.
 - <http://forensics.spreitzenbarth.de/2015/08/12/breaking-the-screenlock-a-short-update/>

◆◆◇ Analysis on Android

Wi-Fi Networks Connected

- Data related to Wi-Fi networks that the device has had access to are stored in */data/misc/Wi-Fi*
- The wpa_supplicant.conf file stores information related to the configuration of Wi-Fi access points.
- Apart from the list of last Wi-Fi networks that the device has been connected to, access passwords to them can also be found. Among such data, we may also find access keys to corporate environments.

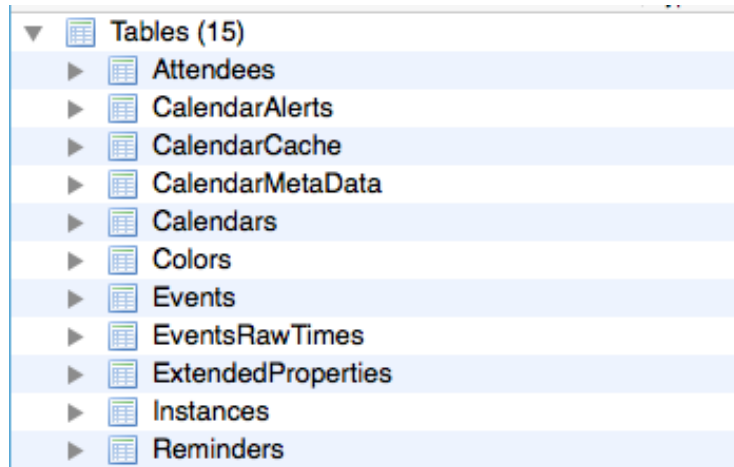
```
root@condor_umts:/data/misc/wifi # cat wpa
wpa_supplicant.conf wpa_supplicant/
lt wpa_supplicant.conf
mot_wpa_conf_version=3
ctrl_interface=/data/misc/wifi/sockets
disable_scan_offload=1
driver_param=use_p2p_group_interface=1
update_config=1
device_name=condor_retgb
manufacturer=motorola
model_name=XT1021
model_number=XT1021
serial_number=ZX1B23QDHQ
device_type=10-0050F204-5
config_methods=physical_display virtual_push_button
p2p_disabled=1
p2p_no_group_iface=1
country=US

networks={
  ssid="SK   iBA"
  psk="
  key_mgmt=WPA-PSK
  priority=1
}
```


◆◆◇ Analysis on Android

Data of Interest – Calendar

- The system's list of events is stored in a Content Provider located in:
/data/data/com.android.providers.calendar/databases/calendar.db
- Such database includes information on events, participants, reminders and alerts.



- The information of this figure may be especially interesting, since it includes the calendar that the user has synchronised with the Google account.

Data of Interest – Text Messages

- Text messages are stored in a Content Provider located in:
 - */data/data/com.android.providers.telephony/databases/mmssms.db*
- Text messages are stored in the SMS table.

sms			CREATE TABLE sms (_id..
_id	INTEGER		`_id' INTEGER
thread_id	INTEGER		`thread_id' INTEGER
address	TEXT		`address' TEXT
person	INTEGER		`person' INTEGER
date	INTEGER		`date' INTEGER
date_sent	INTEGER		`date_sent' INTEGER D..
protocol	INTEGER		`protocol' INTEGER
read	INTEGER		`read' INTEGER DEFA...
status	INTEGER		`status' INTEGER DEFA..
type	INTEGER		`type' INTEGER
reply_path_present	INTEGER		`reply_path_present' IN...
subject	TEXT		`subject' TEXT
body	TEXT		`body' TEXT
service_center	TEXT		`service_center' TEXT
failure_cause	INTEGER		`failure_cause' INTEGE...
locked	INTEGER		`locked' INTEGER DEF...
sub_id	INTEGER		`sub_id' INTEGER DEF...
stack_type	INTEGER		`stack_type' INTEGER ...
error_code	INTEGER		`error_code' INTEGER ...
seen	INTEGER		`seen' INTEGER DEFA...

- The provider also offers other tables to access messages by threads.
- MMS' URIs are located in the “attachments” table.

Data of Interest – Browser

- On Android, the browser depends by default on the manufacturer and the operative system version:
 - */data/data/com.android.chrome* for Chrome:
 - Data of interest are stored in the *app_chrome/Default/* folder.
 - Files of interest in the same folder:
 - *Login Data*: Sqlite file with access credentials to web pages.
 - *Cookies*: Sqlite file with cookies of visited webs.
 - *Bookmarks*: Json file with favourite websites saved in the browser.
 - *History*: Sqlite file with the history of visited websites.
 - *Web Data*: Sqlite file with forms auto-filled information.
 - */data/data/com.android.browser* for browsers by default that are not Chrome.
 - The database of stored passwords is located in:
/data/data/com.android.browser/databases/webview.db

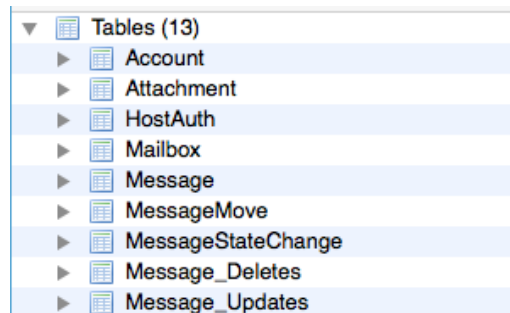
Data of Interest – Contacts and Calls

- Contacts and calls of the device are stored in the **ContentProvider** located in:
/data/data/com.android.providers.contacts/
- The location may vary depending on the manufacturer and the telephone company.
- The database that stores such information is located in **databases/contacts2.db**
 - Contacts are stored in contacts tables: *raw_contacts* and *deleted_contacts*.
 - Recent calls are stored in the **call** table.
- Furthermore, all the pictures associated to contacts on the phone are stored in the **photos** folder.
- The list of recent calls of the device is stored in the same file *databases/contacts2.db*, in the *call* table.

◆◆◆ Analysis on Android

Data of Interest – Email

- As in the case of the browser, it will depend on the type of account that the user has configured.
- Regarding Gmail, there is one database for each account:
 - */data/data/com.google.android.gm/databases/mailstore.[ACCOUNT].db*
 - It includes tables such as:
 - Conversations.
 - Attachments.
 - Messages.
- The rest of email accounts are located in the Content Provider:
 - */data/data/com.android.email/databases/EmailProvider.db*



◆◆◆ Analysis on Android

Data of Interest – Geographical Data

- Geographical data on Android are mainly stored in Google Maps.
- Its folder is stored in `/data/data/com.google.android.apps.maps`
- There are multiple data of interest in such folder:
 - The cache folder stores images with parts of the maps and Street View images previously reviewed.
 - In the `databases/gmm_myplaces.db` file, places that the user has selected as favourite in the application are stored.

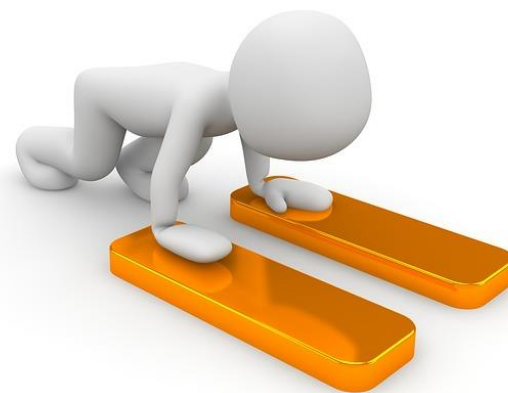




Analysis on iOS

General Aspects

- Generally, the information analysed on an iOS device will be presented in the following form:
 - Plist files:
 - XML files that store key-value pairs.
 - Preferences of the applications stored via *NSUserDefaults* are stored with this format.
 - SQLite databases with different extensions.
 - Non-encrypted text files.
 - Binary files: images.
 - Plain text files.



File System

- iOS file system (HFS+) provides the date of last modification, access, change, and creation. Such dates are provided in the form of seconds passed since January 1, 2001.
- The system is divided into two partitions:
 - **Firmware Partition:** read-only, except for update processes. It stores system files and applications of the operative system.
 - **User's partition:** it stores applications and data created while the phone is being used.
- From iPhone 3GS, all iOS devices include an AES motor by default that encrypts data stored in the flash memory; therefore, the physical read of the device is not useful, unless the encryption key is available.
















Directories of Interest – Applications of the System

- All data of applications installed by default are stored in:
/private/var/mobile/Library

▶ Accounts	-- 02/06/2014, 19:46
▶ AddressBook	-- 02/06/2014, 19:47
▶ adi	-- 31/01/2016, 21:59
▶ AggregateDictionary	-- 28/12/2015, 19:50
▶ ApplePushService	-- 02/06/2014, 19:47
▶ Application Support	-- 28/12/2015, 19:49
▶ ApplicationSync	-- Today, 00:27
▶ Assets	-- 01/02/2016, 03:22
▶ BackBoard	-- Today, 22:37
▶ BulletinBoard	-- 01/02/2016, 01:41
▶ Caches	-- Today, 22:32
▶ Calendar	-- 28/12/2015, 19:49
▶ Carrier Bundle.bundle	-- 28/12/2015, 19:51
▶ CarrierDefault.bundle	-- 02/06/2014, 19:46
▶ com.apple.itunesstored	-- Today, 00:27
▶ com.apple.nsnetworkd	-- 04/02/2016, 20:39
▶ ConfigurationProfiles	-- Today, 00:13
▶ ConfigurationProfilesAp...essibilityParameters.plist	181 B 02/06/2014, 19:46
▶ Cookies	-- Today, 00:13
▶ Cydia	-- 28/12/2015, 20:18
▶ DataAccess	-- 13/01/2016, 21:08
▶ Duet	-- 28/12/2015, 19:50
▶ FairPlay	-- 28/12/2015, 19:50
▶ IdentityServices	-- 02/06/2014, 19:47
▶ Keyboard	-- 04/02/2016, 20:40
▶ Logs	-- Today, 00:01
▶ Mail	-- 01/02/2016, 01:42

Directories of Interest – Applications of the System

- Third parties' applications are stored in: */private/var/mobile/Applications*

▶  1B79EF4A-4F35-4A80-9E47-487743AC1CD3	-- 02/06/2014, 19:47
▶  6CD73469-98F1-4FB9-BE24-6FE273E4567E	-- 02/06/2014, 19:47
▶  303D7F2A-BB68-4640-91EB-2676F1739F42	-- 02/06/2014, 19:47
▶  592AD005-2D16-4968-9406-2AC5015A3FFF	-- Today, 00:15
▶  631FFD33-5D49-4E18-86F9-09C4E632F2DE	-- 08/02/2016, 13:29
▶  864EB949-E1AD-4039-8C17-158D16150EAF	-- 02/06/2014, 19:46
▶  1322E7DE-C499-4185-B986-8E83E7440AFC	-- 31/01/2016, 22:05
▶  64653523-6D05-4D5E-89B4-71417F51B82A	-- 02/06/2014, 19:47
▶  A5FEC033-54E7-4CBF-8A11-E066F8AC6B05	-- 08/02/2016, 13:29
▶  A35FBD93-B22E-42E5-8996-6138D66CD711	-- 02/06/2014, 19:47
▶  AB3718E2-B24B-4841-A3DD-9FC01DFBF56F	-- 02/06/2014, 19:46
▶  AE326639-4687-476B-B0E1-C2FF684E2D99	-- 31/01/2016, 21:53
▶  AFE689B8-1EB8-4718-AB91-6AF6772024A9	-- 02/06/2014, 19:46
▶  CCB0CA51-5230-4FFF-A12E-C4BCF06BFF0A	-- 02/06/2014, 19:46
▶  F212F15B-AB35-438F-A884-3C20FB206C27	-- 31/01/2016, 23:25

- Each application is identified with a 32-characters UUID (the same for the same application in different devices).

Structure of an Application's Sandbox

- Each application includes, at least, the following directories:
 - **Documents**: it stores files created and used by the application.
 - **Library**: it stores configuration files created via iOS' API and cache files.
 - **tmp**: temporary files that are created during the execution of an application.

▼	1B79EF4A-4F35-4A80-9E47-487743AC1CD3	-- 02/06/2014, 19:47
▶	Documents	-- 02/06/2014, 19:47
▶	Library	-- 02/06/2014, 19:47
▶	tmp	-- 02/06/2014, 19:47
▶	Web.app	-- 02/06/2014, 19:47
▼	6CD73469-98F1-4FB9-BE24-6FE273E4567E	-- 02/06/2014, 19:47
▶	Documents	-- 02/06/2014, 19:47
▶	Library	-- 02/06/2014, 19:47
▶	StoreKitUIService.app	-- 02/06/2014, 19:47
▶	tmp	-- 02/06/2014, 19:47

- As it was verified during the security analysis of an application, it is possible that sensitive data (such as credentials) are stored in those folders.

Data of Interest – Photographs

- Pictures of the device are stored in the directory: *private/var/mobile/media/DCIM*

▼ 100APPLE	-- Today, 22:56
IMG_0001.PNG	57.1 KB 31/01/2016, 20:52
IMG_0002.JPG	1.5 MB Today, 22:55
IMG_0003.JPG	1.8 MB Today, 22:56

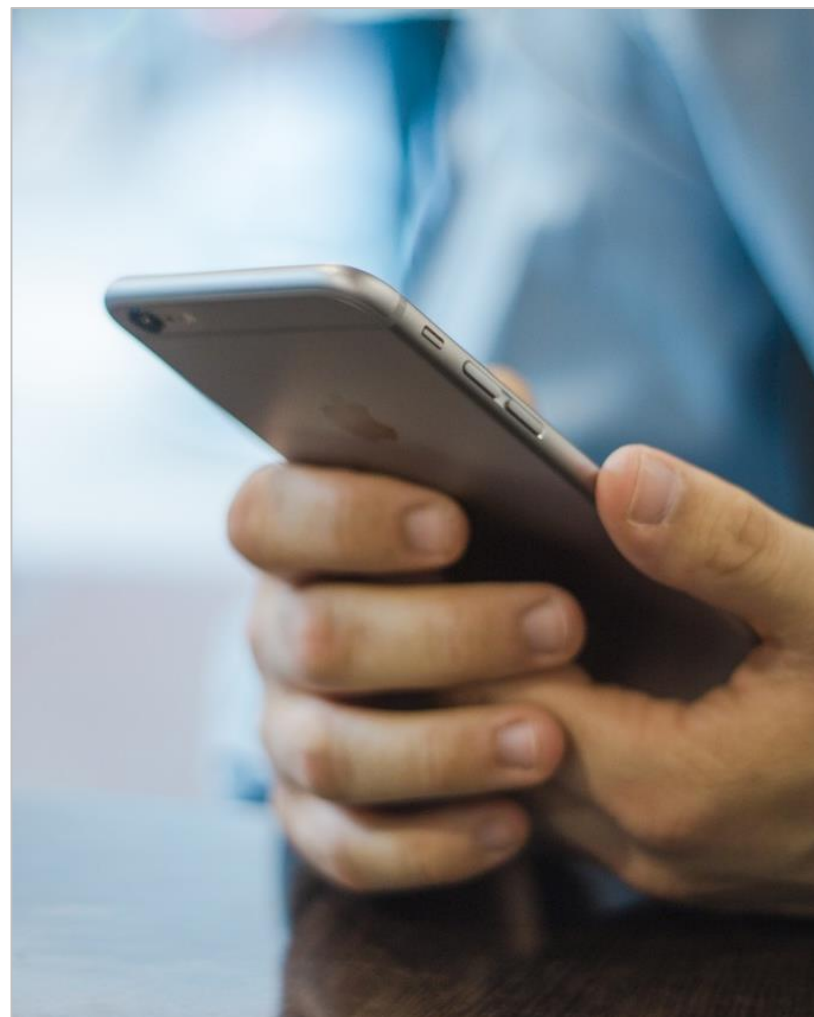
- The 100Apple folder stores pictures taken with the device itself in such directory.
- Photographs taken are assigned consecutive numbers. If a number of the sequence is missing, it has been removed from the phone.
- Screenshots are in the same folder, but in PNG format.
- EXIF data of pictures may be quite interesting regarding the analysis.

IMG_0001.PNG	57.1 KB 31/01/2016, 20:52
IMG_0002.JPG	1.5 MB Today, 22:55
IMG_0003.JPG	1.8 MB Today, 22:56
IMG_0004.PNG	1.0 MB Today, 23:00

◆◆◆ Analysis on iOS

Data of Interest – Keyboard Cache

- iOS stores a file with words written by the user during the normal use of the device
/private/var/mobile/Library/Keyboard/dynamic-text.dat
- It collects words typed in any application that receives input of the keyboard.
- Words written in password fields are not stored in this dictionary.
- It does not include timestamps.
- The *UserDictionary.sqlite* file stores the corrections that the user has made to the system's dictionary.



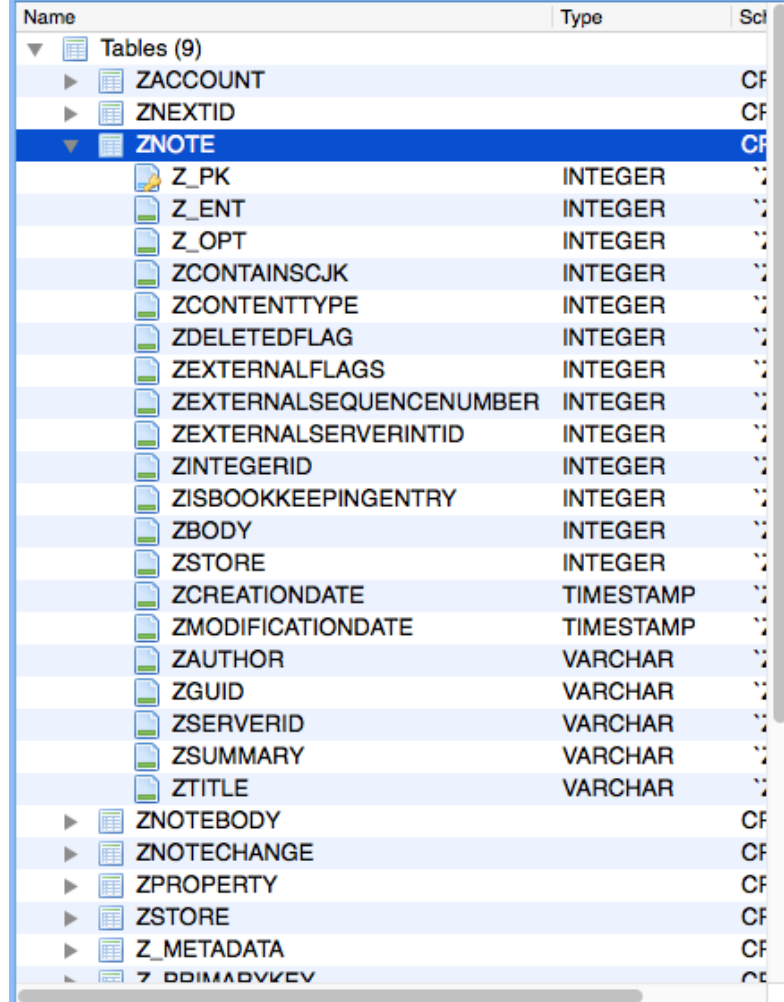
Data of Interest – Keychain

- iOS applications can use the Keychain service to store passwords in the device.
- Different genp, cert, inet and key tables containing information on passwords used by the device can be found in this file.
- In several cases, the information stored in such file is encrypted; therefore, it is necessary to use forensic tools such as iPhone Password Breaker by Elcomsoft in order to decrypt the files.

◆◆◆ Analysis on iOS

Data of Interest – Notes

- Data existing on the notes application (and other similar ones included in the system) may be highly useful during the forensic analysis.
- Data of the notes application are stored in:
 - */private/var/mobile/Library/Notes/notes.sqlite*
- The sqlite file tables include information such as date of creation and last modification of the note.
- From iOS 9.3 version, notes can be encrypted by using the Keychain and the user's lock code.



The screenshot displays a SQLite database browser interface. The 'Tables (9)' section is expanded, showing a list of tables. The 'ZNOTE' table is selected and highlighted in blue. Below it, the columns of the 'ZNOTE' table are listed, including their data types and primary key status. The columns are: Z_PK (INTEGER, PRIMARY KEY), Z_ENT (INTEGER), Z_OPT (INTEGER), ZCONTAINSCJK (INTEGER), ZCONTENTTYPE (INTEGER), ZDELETEDFLAG (INTEGER), ZEXTERNALFLAGS (INTEGER), ZEXTERNALSEQUENCENUMBER (INTEGER), ZEXTERNALSERVERINTID (INTEGER), ZINTEGERID (INTEGER), ZISBOOKKEEPINGENTRY (INTEGER), ZBODY (INTEGER), ZSTORE (INTEGER), ZCREATIONDATE (TIMESTAMP), ZMODIFICATIONDATE (TIMESTAMP), ZAUTHOR (VARCHAR), ZGUID (VARCHAR), ZSERVERID (VARCHAR), ZSUMMARY (VARCHAR), and ZTITLE (VARCHAR). Below the 'ZNOTE' table, other tables are listed: ZNOTEBODY, ZNOTECHANGE, ZPROPERTY, ZSTORE, Z_METADATA, and Z_METADATA.

Name	Type	Sql
Tables (9)		
▶ ZACCOUNT		CF
▶ ZNEXTID		CF
▼ ZNOTE		CF
Z_PK	INTEGER	PK
Z_ENT	INTEGER	
Z_OPT	INTEGER	
ZCONTAINSCJK	INTEGER	
ZCONTENTTYPE	INTEGER	
ZDELETEDFLAG	INTEGER	
ZEXTERNALFLAGS	INTEGER	
ZEXTERNALSEQUENCENUMBER	INTEGER	
ZEXTERNALSERVERINTID	INTEGER	
ZINTEGERID	INTEGER	
ZISBOOKKEEPINGENTRY	INTEGER	
ZBODY	INTEGER	
ZSTORE	INTEGER	
ZCREATIONDATE	TIMESTAMP	
ZMODIFICATIONDATE	TIMESTAMP	
ZAUTHOR	VARCHAR	
ZGUID	VARCHAR	
ZSERVERID	VARCHAR	
ZSUMMARY	VARCHAR	
ZTITLE	VARCHAR	
▶ ZNOTEBODY		CF
▶ ZNOTECHANGE		CF
▶ ZPROPERTY		CF
▶ ZSTORE		CF
▶ Z_METADATA		CF
▶ Z_METADATA		CF

Data of Interest – Text Messages

- Unlike emails and other corporate messaging applications, SMS are only accessible from the device.
- On iOS, the message database is located in:
 - `/private/var/mobile/Library/SMS/sms.db`
- The most relevant tables in such files are described below:
 - `Messages` includes sent and received messages.
 - `msg_pieces` includes elements sent with messages (videos and pictures).
- iMessage messages are stored in the same database. Attached files are stored in the Attachments folder of the SMS directory.

◆◆◆ Analysis on iOS

Data of Interest – Cookies

- They are stored in a binary file in:
 - `/private/var/mobile/Library/Cookies/Cookies.binarycookies`
- It includes a header and cookies separated on different pages.

Field	Size	Description
Header	4 bytes	“COOK”
No of pages	4 bytes	In <i>Little Endian</i>
Size of the page	4 bytes	In <i>Little Endian</i>
Page	Variable	<i>Cookies:</i>
Queue	8 bytes	Checksum of the file content

- It requires a specialised program or an hexadecimal viewer.

◆◆◆ Analysis on iOS

Data of Interest – Searches and Favourites

- They are stored in the following folder:
/private/var/mobile/Library/Safari
- Bookmarks are stored in an Sqlite file:
Bookmarks.db
- Recent searches are stored in a plist file: *SearchEngines.plist*



Data of Interest – Contacts and Calls

- Contacts of the phone are stored in:
 - */private/var/mobile/Library/AddressBook*
- There are two especially interesting tables:
 - *ABPerson*: it stores names and personal details of the contact.
 - *ABMultiValue*: it stores phone numbers, email addresses and other accounts of such individual. It is directly related to *ABPerson* values through a Foreign Key.
- The history of calls is stored in:
 - */private/var/Library/CallHistory/call_history.db*
- It includes the phone number, duration of the call and the reference to the contact.
- It also indicates whether the call is incoming or outgoing.

Data of Interest – Geographical Data

- On iOS, the location daemon of the system stores the information related to location in the following folder:
 - */private/var/root/Library/Caches/locationd*
- Depending on the iOS version, the name of contents and files used in such folder may vary:
 - *consolidated.db*
 - *Cache_encryptedA.db*
- Such files store geographical information related to multiple aspects of the device, including the last Wi-Fi points that the device has been connected to, location of cells and last locations requested by the device's applications.

Other Data of Interest

- The Preferences directory stores multiple information files of interest:
 - *com.apple.accountsettings.plist*: information on email accounts.
 - *com.apple.AppStore.plist*: last search of applications on the AppleStore.
 - *com.apple.facetime.plist*: information on the use of Facetime.
- Voicemails are stored in the following file:
/mobile/Library/Voicemail/voicemail.db



Other Data of Interest – Backups

- Each backup performed by iTunes is stored in a folder with the device's UDID.
- Differential backups are stored in folders with the same UDID and date.
- iTunes security folders include the following files of interest:
 - *Status.plist*: date and information on the performed backup.
 - *Manifest.plist*: includes information of third parties' applications installed and configuration data of the system's applications.
 - *Info.plist*: information of the device such as IMEI, SIM serial, etc.

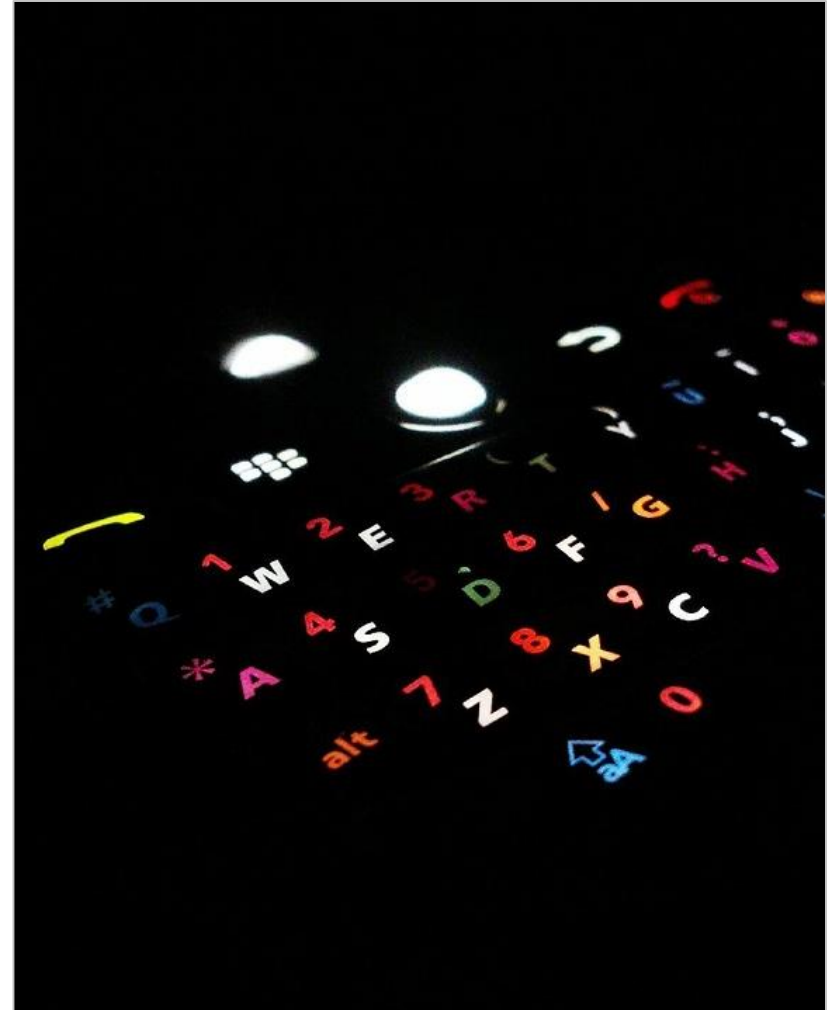


BlackBerry Analysis

◆◆◆ Analysis on BlackBerry

General Aspects

- Generally, the information analysed on a BlackBerry 10 device will be presented in the following form:
 - Sqlite databases with .db and .dat extensions.
 - XML files.
 - .Ini files.
 - Binary files: (.bin): images.
 - Plain text and other configuration files (.conf).



◆◆◆ Analysis on BlackBerry

Files

- Generally and, due to the security restrictions existing on BlackBerry 10, the analysis is always conducted on a backup of the device.
- The backup of a BlackBerry 10 device includes three tar files:
 - **App**: includes applications installed in the device.
 - **Media**: includes data created during the use of the device (including data created by the applications).
 - **Settings**: contains configuration data of the device, applications and accounts.



◆◆◇ Analysis on BlackBerry

Directories of Interest – Applications

- All the applications of the system are stored in the app folder.
- Applications may have two types of name:
 - *Com.[app name].gYABG[alphanumeric characters]*
 - *sys.[app name].gYABG[alphanumeric characters]*
- The com prefix is used for third parties' applications and the sys prefix, for system applications.
- At the end of the name, a set of random alphanumeric characters is added.
- Data of some applications of the system, such as calendar, contacts, etc. are located in:
 - */settings/accounts/1000/sysdata/pim*
 - “Pim” is an acronym for Personal Information Manager.

◆◆◆ Analysis on BlackBerry

Data of Interest – Photographs

- Photographs taken by the device's camera are stored in `/media/camera` if there is no SD card on the device. In case there is an SD card, photographs are stored in the `/sdcard/camera` card folder. Videos are stored in the same way, but in the `videos` folder.
- Pictures stored by other applications are stored in the corresponding folder, inside the `media` folder.
- Screenshots are always stored in the `/media/camera` folder of the device, in PNG format and without EXIF information.

◆◆◆ Analysis on BlackBerry

Data of Interest

- The calendar of the device is stored in:
 - */settings/accounts/1000/sysdata/pim/db/1-pm.db*
 - Events are stored in the CalendarEvent table. Timestamps are stored in GMT.
- Contacts of the device are stored in:
 - */settings/accounts/1000/sysdata/pim/db/2-pm.db*
- The history of calls is stored in:
 - */settings/accounts/1000/sysdata/pim/db/8-pm.db*
 - The history is stored in Call and CallDetail tables. Timestamps are stored in GMT.
- Reminders of the device are stored in:
 - */settings/accounts/1000/sysdata/pim/db/18-pm.db*

◆◆◇ Analysis on BlackBerry

Data of Interest – Text Messages

- Messages are stored in:
 - */settings/var/db/text_messagingsettings/messages.db*
- The content of the messages can be found in the Attachments table.
- In order to know whether a message is incoming or outgoing it is necessary to inspect the inbound field of the Messages table. The value 0 means “sent” and the value 1, “received”.
- The database of BlackBerry Messenger is located in:
 - */app/sys.bbm.gYABgLOJBR2Vz7FzS.kdgJchuag/appdata/data/master.db*
- Such database also records voice and video calls made via BMM (only the event is recorded).

◆◆◇ Analysis on BlackBerry

Data of Interest – BlackBerry Hub

- BlackBerry Hub centralises information on calls, messages on the voicemail, emails, sms, social network feeds, calendar events, and notifications.
- Even though the information included in the hub may be accessed through different means, it is important to use it during the analysis, since it provides a timeline of all the events occurred on the device.
- The database is located in:
/sys.pim.messages.gYABgJ8jn83Ok_NEWYpIPYozt5w/appdata/data/unfied.db
- In such database, there is an input for each event that includes:
 - The type of application and event created (application, calendar, notification, etc.).
 - The text displayed in the hub.
 - The date of the event in in the form of seconds since January 1, 1970.

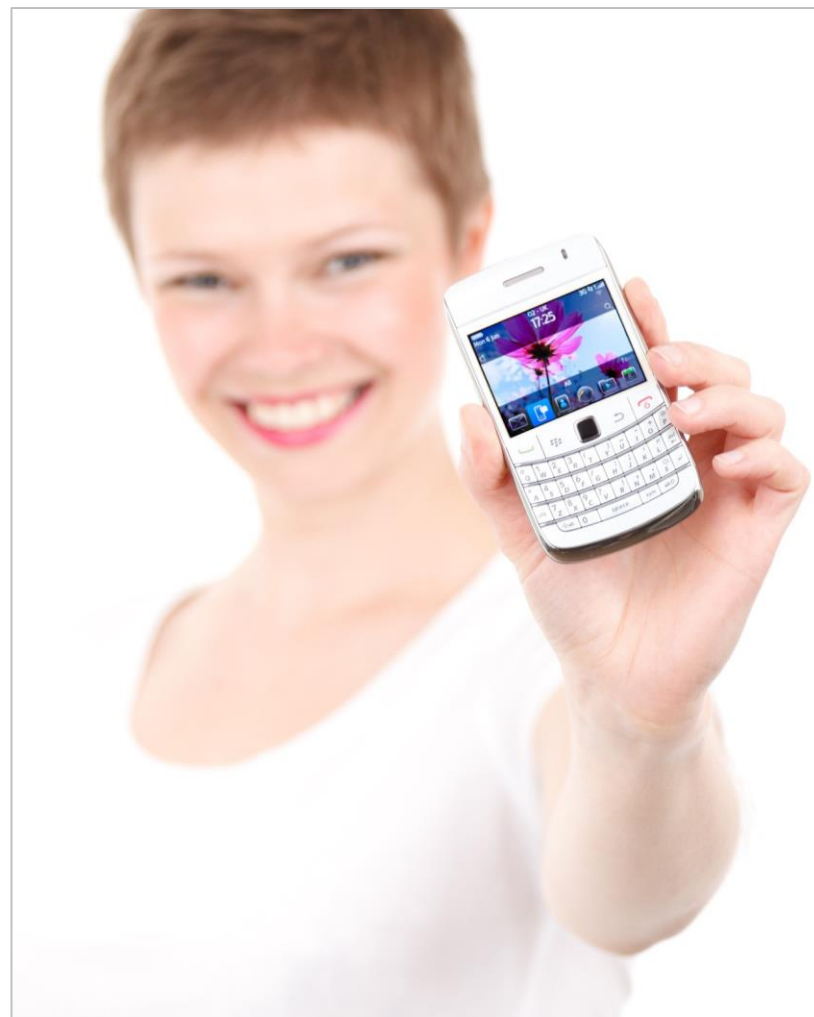
Data of Interest – History and Bookmarks

- Relevant files related to the browser are stored in:
 - */app/sys.browser.gYABgJYFHAzbeFMPCCpYWBtHAm0/appdata/data/chrome/database/local-0*
- The Databases.db file leads to files (variable according to the model) that include browsing history and bookmarks.
- There are two tables of interest in each of such files:
 - *history*: includes an input for each page of the browsing history. URLs are provided with identifiers.
 - *urls*: it maps the URLs to the identifiers mentioned in the last table. Includes a field the last date in which the URL was visited.

◆◆◆ Analysis on BlackBerry

Data of Interest – Browsing Cache and Cookies

- Further relevant data regarding the use of the browser can be found in:
 - `/app/sys.browser.gYABgJYFHAzbeFM PCCpYWBtHAm0/appdata/data/webviews`
- The `cookieCollection.db` file stores the browsing cookies.
- The cache folder stores temporary files of the Internet.
- The database folder stores specific databases of each site that has requested the use of storage via HTML 5.



Windows Phone Analysis



General Aspects

- Since Windows 10 Mobile operative system has been in the market for a short time and it has a small market share, this operative system is not documented enough in the context of the computer forensics.
- In any case, its structure has multiple similarities with the general structure of Windows systems and, above all, with Windows 10:
 - It includes the use of a registry of the storage of configurations and information of the system.
 - Use of NFTS partitions.
 - Structure of directories of the system.
- Mechanisms and data of interest that have been documented until date for Windows Phone 8 are described in the following slides.

◆◆◆ Windows Phone Analysis

Data of Interest – Photographs

- Photographs and videos recorded by the camera are stored in the directory:
 - *Users\Public\Pictures\CameraRoll*
- The format of photographs is:
 - *WP_YYYYMMDD_###.jpg*
 - Where
 - WP is the acronym for Windows Phone.
 - YYYYMMDD means year (Y), month (M) and day (D) when the picture was taken.
 - ### is a self/incremented sequential number.
- In case that the phone has an SD card installed, photographs can also be located in the SD card, in the same format.
- Pictures saved from other sources are stored in:
 - *Users\Public\Pictures\SavedPictures*

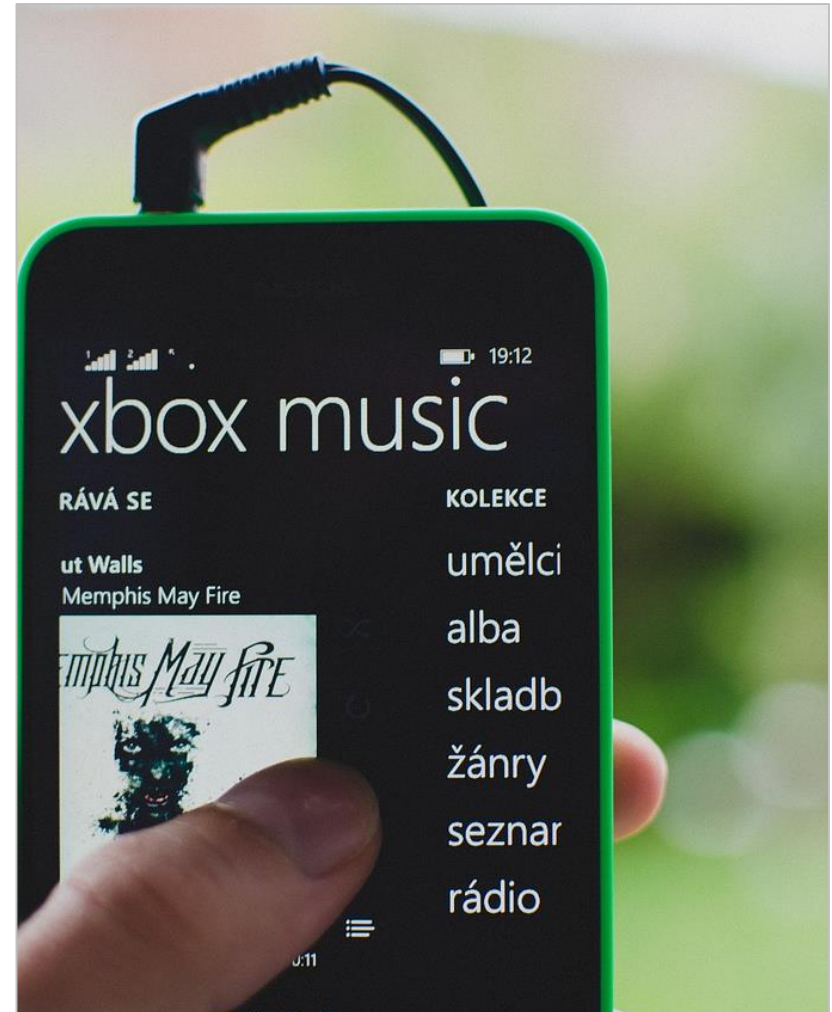
Data of Interest – History of Calls and Messages

- The history of calls is stored in a file with no extension:
 - *Users\WPCOMMSERVICES\APPDATA\Local\UserData\phone*
 - All the calls existing in such file ends with the following string: *B1776703-738E-437D-B891- 44555CEB6669*.
- SMS messages are located in:
 - *Users\WPCOMMSERVICES\APPDATA\Local\Unistore\store.vol*
- Files attached to MMS messages may be located in:
 - *SharedData\Comms\Unistore\Data*
 - This directory stores images, text and other multimedia files with .dat extension (the encryption of information maintains the original format and only modifies the extension).

◆◆◆ Windows Phone Analysis

Data of Interest – Web Browsing

- The browsing history and cookies are stored in:
 - *Users\DefApps\APPDATA\INETNETEXPLORER\NetCache*
- The history that has not been included yet in the file mentioned before is stored in:
 - *Users\DefApps\APPDATA\Local\Microsoft\Windows\WebCache\01.dat*
- Favourites of the device are stored in:
 - *SharedData\InternetExplorer\Favorites*



Data of Interest – Notes

- System notes are stored in the application One Note, included in the Office suite.
- The directory of installation of the application and its data can be found in:
 - *Users\DefApps\APPDATA\OFFICE\Temp\OneNote*
- Additionally, the applications cache may also store information that has not been stored in the persistent part of the application yet:
 - *Users\DefApps\APPDATA\OFFICE\Temp\OneNote\OneNoteRuntimeCache\OneNoteRuntimeCache_Files*

Data of Interest – Keyboard Cache

- The keyboard cache as well as elements used for the automatic filling of forms are stored in the following folder:
 - *SharedData\Input\nutral*
- Inside this folder we can find two files:
 - **ihds.dat**: it stores words typed by the user when writing on the keyboard in any of the applications of the phone.
 - **livehds.dat**: it stores data previously introduced in forms for the later automatic fill-in.



Analysis Laboratory

A fluorescence microscopy image showing a grid of cells. The top row features five cells with bright, distinct fluorescence in cyan, green, yellow, cyan, and green. The bottom row shows a larger field of cells with more diffuse, blue and cyan fluorescence. A semi-transparent dark gray rectangle is centered over the image, containing the title text.

Introduction to the Laboratory

◆◆◆ Introduction to the Laboratory

Analysis of an Android Device's Image.

- In this laboratory, the forensic analysis of an Android image will be conducted.
- The laboratory exercise will be based on a simulation in which you should assume the role of a forensic investigator in a fictional case.
- **The ultimate goal of the analysis is to write a forensic report that will be discussed in the corresponding forum.**
- The laboratory is divided into tasks:
 - At the end of each task, the solution will be available, so that you can continue working in case you still have difficulties.
 - **In order to take as much advantage as possible out of the laboratory, try to fully complete the task before checking the solution.**
- It is possible that you find more evidences than the ones listed in the solutions provided during the analysis.



This situation is normal, due to the huge amount of evidences that mobile devices create. Time and space restrictions do not allow us to show all of them in a solution. We encourage you to use the forum in order to share evidences that are not documented in the solutions.


◆◆◆ Introduction to the Laboratory

Preparation of Autopsy

- During the laboratory, we will use Santoku Linux; therefore, we recommend you to download all the material required for the realisation of the laboratory from the Santoku's virtual machine itself.
- Some tools that will be used in the laboratory are mentioned below:
 - Autopsy.
 - Sqliteman.
 - Exiftool.
- In the case of Autopsy, there is a small bug in the Santoku version that has to be fixed before starting the task. To do this, it is only necessary to write the following commands on the console:

```
> sudo ln -s /usr/bin/icat /usr/bin/icat-sleuthkit
> sudo ln -s /usr/bin/ils /usr/bin/ils-sleuthkit
```

 - It allows sleuthkit to use icat and ils to show information of the files.

A close-up photograph of a person's hands writing on a document. The person is wearing a light blue button-down shirt. Their right hand holds a black and silver pen, and their left hand rests on the document. The document is white with some faint, illegible text. A semi-transparent dark grey rectangular box is overlaid on the center of the image, containing the text "Presentation of the Case" in white.

Presentation of the Case

◆◆◆ Presentation of the Case

Context

- Due to some information revealed to the police by a confident, it is known that some Spanish-speaking criminals may be preparing robberies in the city of London.
- After a first robbery in one of the most prestigious jewellery shops of the city, one of the criminals let his face uncovered and his image is captured by one of the cameras of the city. Four criminals are involved in the robbery.
- Following the suspect through the cameras of the city, the police identify him in a house that seems to be his current residence.
- After a raid in the house of the alleged offender, an Android device that the user was using in the moment of the raid was found.

◆◆◆ Presentation of the Case

Status of the Device

- The seized device had no lock system configured and was rooted.
- The device had no SD card inserted.
- Taking advantage of the device's current status, an expert from the police performed the following tasks right after the seizure:
 - Format an 8GB-SD card for the acquisition of forensic data.
 - Connect the seized device to a forensic analysis computer via USB cable.
 - Use `adb` and the `dd` command to dump the physical content of the disk partition that has been established in `/data` (user's data partition) to the SD card.
 - Extract the image captured from the SD card to the analyst's computer through the `adb pull` command.
 - The MD5 hash of the obtained image is `235fdf8cdba7584ac5c8a10fc9e11c56`.

◆◆◆ Presentation of the Case

Statement

- The image obtained has been sent to our laboratory for the analysis.
- A forensic analysis of the found image is requested and it should include:
 - The location of possible future targets of the criminal group.
 - Names or any other elements that may identify possible accomplices of the suspect.
 - Additional information (accounts names, etc.) that, after obtaining the corresponding court order, may provide more information on the suspect and its activities.





Creation of the Case

◆◆◇ Creation of the Case

Load on Autopsy

- The main tool that will be used during this exercise is Autopsy.
- In order to launch Autopsy, the following command has to be written in a Santoku Linux' console (it has to be executed as administrator in this installation).

> sudo autopsy

```
santoku@santoku-VirtualBox:~$ sudo autopsy

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

Evidence Locker: /var/lib/autopsy
Start Time: Mon Feb 15 13:23:09 2016
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

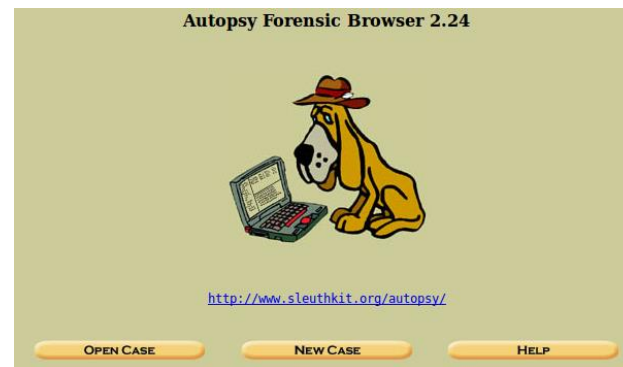
Keep this process running and use <ctrl-c> to exit
```

- Open the browser and write the address provided.

◆◆◆ Creation of the Case

Open a New Case

- In the browser window, click on “New Case”.
- Fill in the form with the case's data.



1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="Mi nombre"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

◆◆◆ Creation of the Case

Add Devices

- A new window will describe the case and configuration directories.
- Since, in this case, only one device will be analysed, click “Add Host”.

Creating Case: AndroidRobo

Case directory (/var/lib/autopsy/AndroidRobo/) created
Configuration file (/var/lib/autopsy/AndroidRobo/case.aut) created

We must now create a host for this case.

ADD HOST

◆◆◇ Creation of the Case

Details of the Device

- Add details of the device:

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

◆◆◆ Creation of the Case

Add the Image

- Select “Add Image”:

Adding host: Android to case AndroidRobo

Host Directory (/var/lib/autopsy/AndroidRobo/Android/) created

Configuration file (/var/lib/autopsy/AndroidRobo/Android/host.aut) created

We must now import an image file for this host

ADD IMAGE

- And “Add Image File”:

No images have been added to this host yet

Select the Add Image File button below to add one

ADD IMAGE FILE

CLOSE HOST

HELP

FILE ACTIVITY TIME LINES

IMAGE INTEGRITY

HASH DATABASES

VIEW NOTES

EVENT SEQUENCER

◆◆◆ Creation of the Case

Add the Image

- Write the location of the file in our file system.
- As it was specified in the description of the case, the image is a partition of the disk, therefore, we should select the corresponding option.
- In order not to copy or move the whole file, select Symlink.

ADD A NEW IMAGE

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

☐ Disk ☒ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☒ Symlink ☐ Copy ☐ Move

NEXT

CANCEL **HELP**

◆◆◇ Creation of the Case

Integrity of the Image

- As forensic analysts, we should make sure that the image corresponds exactly to the one obtained during the phone dump.
- To do this, we have the MD5 hash, therefore, we should verify its integrity before including it in the analysis.

235fdf8cdba7584ac5c8a10fc9e11c56

Local Name: images/data.img

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☐ Ignore the hash value for this image.

☐ Calculate the hash value for this image.

☒ Add the following MD5 hash value for this image:

☒ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ext4)

Mount Point: File System Type:

ADD **CANCEL** **HELP**

◆◆◆ Creation of the Case

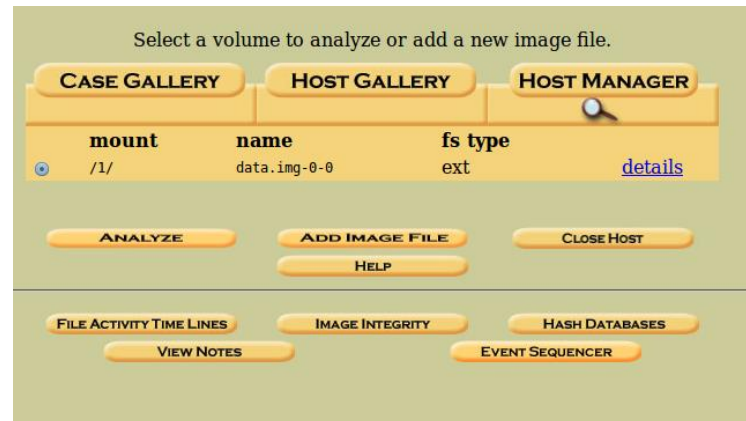
Verification of the Integrity

- Once the integrity of the image has been verified, we should obtain a result similar to the one presented below.

```
Calculating MD5 (this could take a while)
Current MD5: 235FDF8CDBA7584AC5C8A10FC9E11C56
Integrity Check Passed
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Volume image (0 to 0 - ext - /1/) added with ID vol1
```

OK

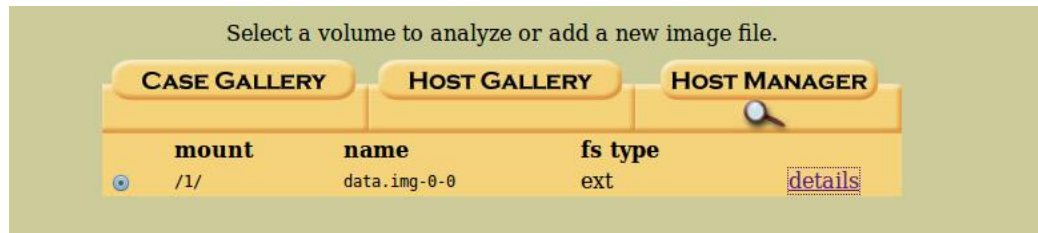
- Furthermore, it is important to take into consideration the image loaded in the case involved.



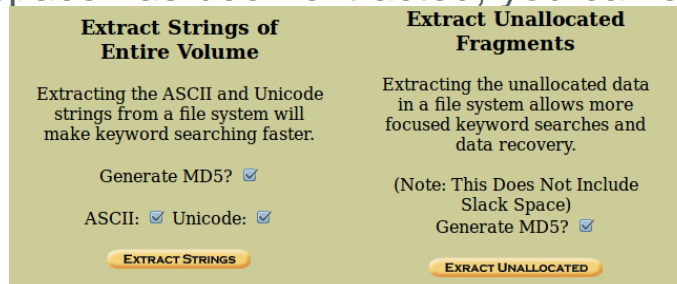
◆◆◆ Creation of the Case

Initial Analysis

- In order to facilitate the extraction of future evidences, the following tasks should be performed:
 - Analyse the space of the device.
 - Create a strings index to conduct searches efficiently.
- To do this, open the details of the image in the case's window.



- Then, select “Extract Strings” and “Extract Unallocated”.
 - Once the removed space has been extracted, you can also extract its strings.



A person is seen from behind, sitting at a wooden table and typing on a silver laptop. The laptop screen is black. To the left of the laptop is a black smartphone. In front of the laptop is a black notebook with a pen resting on it. To the right of the laptop is a white coffee cup on a saucer. The background is blurred, showing an outdoor setting with trees and a path. A semi-transparent dark grey rectangle is overlaid on the image, containing the text "Information Extraction" in white.

Information Extraction

Determine the First Elements to Examine

- Once the image of Autopsy has been loaded, the first thing to do is to decide what information included in the image is interesting regarding the case involved. To do this, it is important to take into consideration the objective of the forensic report requested.

Task

Create a list that includes elements of interest for the case concerned.

Expected result

A list that includes information taken from the device that may allow analysts to reach conclusions on the possible future targets, accomplices of the suspect or additional information to continue with the investigations.

Determine the First Elements to Examine

- The report requested is aimed at collecting information on three specific elements:
 - Possible **location** of new targets.
 - **Personal connections** of the suspect with other accomplices.
 - Additional information on his **online presence**.
- The following elements may be interesting regarding new targets:
 - Information of location applications. Coordinate pairs stored in applications may provide analysts data of interest.
 - Wi-Fi points that the device has been connected to. If Wi-Fi connections were public, it is possible to find the specific place in which the device has been located.
 - Messages that include information on locations. Information exchanged with other people regarding locations that may be relevant for the analysis.

Determine the First Elements to Examine

- The following elements may be interesting regarding personal connections:
 - Phone book, since it describes people that the suspect has regular contact with.
 - History of calls, since it describes people that the suspect has had contact with recently.
 - Messages received via SMS and other messaging/email applications, since they provide information on personal relations with each person.
- Regarding the online presence of the suspect:
 - Suspect's usernames (and credentials, if possible) in other online services. They will allow analysts to access additional information to determine involvement of the suspect in the events occurred.
- Since some information elements may be created by different applications, the analyst should also create an inventory of applications installed on the device.

List of Elements to Examine

- List of installed applications, paying special attention to those applications related to:
 - Location.
 - Messaging.
 - Network services (social networks, etc.).
- Places included in location applications.
- Wi-Fi networks that the device has been connected to.
- Phone book.
- Call history.
- Messages content and recipients from messaging applications installed on the device.
- List of access credentials for social networks of applications installed on the device.
- Pictures that include relevant information on any of the elements mentioned above.

◆◆◆ Information Extraction

Extraction of Information Elements

- Once all the elements to extract during the analysis are listed, extract them.
- Each of the following tasks is focused on the extraction of one of the elements mentioned in the previous table.
- In order to start the analysis stage, you should have extracted the information related to each of them.
- During the analysis stage, the analyst may need to extract new information elements. This task is common within the forensic analysis processes.
- Regarding the creation of the forensic analysis, it is important to take notes on all the steps and processes carried out during the tasks.



Extraction of the List of Applications

- The first step to take in order to reduce the rest of tasks, is to identify applications installed on the device.

Task

Write a list that includes the applications installed on the device, paying special attention to applications that may include information regarding location, messages or access to social networks.

Expected result

A list of applications that specifies the type of information that can be extracted from each of them.

Extraction of the List of Applications

- Applications installed on an Android device are located in: */data/data*
- The image obtained in the case comes from the data partition; therefore, it will be only necessary to inspect the content of the data folder in order to discover the applications installed.
- In Autopsy, go to data and check the applications list.
- Among that amount of applications, there are some interesting ones. For example:

d / d	com.quickoffice.android/	18:43:03 (GMT) 2016-02-14 18:07:42 (GMT)	23:43:17 (GMT) 1970-02-25 23:43:16 (GMT)	18:43:03 (GMT) 2016-02-14 18:07:42 (GMT)	4096	10086	10086	72241
d / d	com.skype.raider/	2016-02-14 14:42:01 (GMT)	2016-02-13 18:40:40 (GMT)	2016-02-14 14:42:01 (GMT)	4096	10097	10097	73230
d / d	com.snapchat.android/	2016-02-14 14:42:00 (GMT)	2016-02-13 18:39:40 (GMT)	2016-02-14 14:42:00 (GMT)	4096	10096	10096	73355
d / d	com.spotify.music/	2016-02-14 14:42:00 (GMT)	2016-02-13 18:37:53 (GMT)	2016-02-14 14:42:00 (GMT)	4096	10095	10095	73419
d / d	com.whatsapp/	2016-02-14 14:42:02 (GMT)	2016-02-13 18:41:44 (GMT)	2016-02-14 14:42:02 (GMT)	4096	10099	10099	73421

Extraction of the List of Applications

- In the list of applications, verify that one of them has been removed from the device.

Personal task: investigate the utility of such application. If appropriate, add the analysis of the application to the report.

		15:48:30 (GMT)	23:43:01 (GMT)	15:48:30 (GMT)					
d / d	com.motorola.wappushsi/	1970-02-25	1970-02-25	1970-02-25	4096	10045	10045	72133	
		23:44:42 (GMT)	23:43:04 (GMT)	23:44:42 (GMT)					
✓ d / r	com.pinellascodeworks.securewipe	2016-02-14	2016-02-14	2016-02-14	20480	10021	10021	73691	
		14:50:04 (GMT)	14:50:04 (GMT)	14:50:04 (GMT)				(realloc)	
d / d	com.qualcomm.atfwd/	1970-02-25	1970-02-25	1970-02-25	4096	1000	1000	72261	
		23:44:46 (GMT)	23:43:18 (GMT)	23:44:46 (GMT)					
d / d	com.qualcomm.interfacepermissions/	1970-02-25	1970-02-25	1970-02-25	4096	10067	10067	72195	
		23:43:10 (GMT)	23:43:10 (GMT)	23:43:10 (GMT)					

- The list of applications is quite large:
 - We should take into consideration the fact that all the applications are stored in this folder, including applications installed by default on the system.
 - All of them should be listed, but it is important to specify which ones are directly related to the case.

Extraction of the List of Applications

- List of applications of interest I:
 - com.quickoffice.android - QuickOffice
 - It may store relevant documents.
 - com.skype.raider - Skype
 - It may store contacts, pictures, messages, and locations.
 - com.snapchat.android – Snapchat
 - It may store contacts, pictures, messages, and locations.
 - com.whatsapp
 - It may store contacts, pictures, messages, and locations.
 - com.instagram.android
 - It may store contacts, pictures, messages, and locations.
 - com.google.android.gm
 - It may store relevant emails.
 - com.android.browser
 - It stores browsing data.

Extraction of the List of Applications

- List of applications of interest II:
 - com.google.android.apps.maps
 - It may store locations.
 - com.facebook.katana
 - It may store contacts, pictures, messages, and locations.
 - com.android.email
 - It may store relevant emails.
 - com.android.chrome
 - It stores browsing data.
- Furthermore, there are providers (mentioned before) relevant for the forensic analysis:
 - com.android.providers.calendar
 - com.android.providers.telephony
 - com.android.providers.contacts

Data of Interest Format

- Once the list of relevant applications of the device has been recovered, analyse them in order to find relevant data for the investigation.
- Once relevant data of each application have been extracted, the analyst can perform the analysis tasks.
- The information extracted during this process should be properly documented and tagged in order to facilitate the later analysis tasks.
- In most cases, the validity of information extracted during this process has been corroborated by the community, as in the case of data involved during the study of the analysable elements.
- In case that it is necessary to extract information on applications or services that are not documented, it would be necessary to verify that the extracted information corresponds to the device's. Such type of validation will not be covered during this laboratory.

History of Calls and Contacts

Task

Find and extract the information related to the phone's history of calls and contacts.

Expected result

The file that identifies calls made from the device.

◆◆◆ Information Extraction

History of Calls and Contacts

- The history of calls and contacts of the device are located in:
 - `/data/com.android.providers.contacts/databases/contacts2.db`
- Extract the file (its journal is empty).
 - Take notes of all the process in order to document it in the report.

The screenshot shows a file explorer window with a list of files. The file `contacts2.db` is circled in red. To the right, a Firefox download dialog is open for the file `...ta.com.android.providers.contacts.databases.contacts2.db`. The dialog shows the file's origin as `http://localhost:9999` and asks "What should Firefox do with this file?". The "Save File" option is selected. The "OK" button is circled in red. At the bottom of the file explorer, there are links for "ASCII (display - report)", "Hex (display - report)", "ASCII Strings (display - report)", "Export", and "Add Note". The "Export" link is circled in red.

File Name	Timestamp	Timestamp
<code>./</code>	2016-02-14 18:07:55 (GMT)	1970-02-01 23:44:10 (GMT)
<code>contacts2.db</code>	2016-02-14 15:02:18 (GMT)	1970-02-01 23:44:10 (GMT)
<code>contacts2.db-journal</code>	2016-02-14 15:02:18 (GMT)	1970-02-01 23:44:10 (GMT)
<code>contacts2.db-mj0F6E4D94B</code>	2016-02-14 18:07:55 (GMT)	2016-02-14 18:07:55 (GMT)
<code>profile.db</code>	2016-02-13 21:07:29 (GMT)	1970-02-01 23:44:10 (GMT)
<code>profile.db-journal</code>	2016-02-13 21:07:29 (GMT)	1970-02-01 23:44:10 (GMT)

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)

Text Messages

Task

Find and extract information related to text messages of the device.

Expected result

A file that describes the text messages of the device.

Information Extraction

Text Messages

- Text messages of the device are located in:
 - `/data/com.android.providers.telephony/databases/mmssms.db`
- Extract the file (and its journal).
 - Take notes of all the process in order to document it in the report.

The screenshot shows a file manager interface with a table of files. The file `mmssms.db` is circled in red. To the right, a Firefox download dialog is open for the file `...a.com.android.providers.telephony.databases.mmssms.db`. The dialog shows the file is unknown and from `http://localhost:9999`. The 'What should Firefox do with this file?' section has 'Save File' selected. The 'OK' button in the dialog is also circled in red. At the bottom of the file manager, there are links for 'ASCII (display - report)', 'Hex (display - report)', 'ASCII Strings (display - report)', 'Export', and 'Add Note'. The 'Export' link is circled in red. The file type is identified as 'SQLite 3.x database, user version 58'.

File Name	Timestamp 1	Timestamp 2
./	1970-02-25 23:44:28 (GMT)	1970-02-25 23:44:19 (G
dlut.db	1970-02-25 23:44:20 (GMT)	1970-02-25 23:44:19 (G
dlut.db-journal	1970-02-25 23:44:20 (GMT)	1970-02-25 23:44:19 (G
mmssms.db	2016-02-14 15:25:12 (GMT)	1970-02-25 23:44:28 (G
mmssms.db-journal	2016-02-14 15:25:12 (GMT)	1970-02-25 23:44:28 (G
telephony.db	2016-02-14 14:43:59 (GMT)	1970-02-25 23:44:20 (G
telephony.db-journal	2016-02-14 14:43:59 (GMT)	1970-02-25 23:44:20 (GMT)

2016-02-14 18:02:20 (GMT) 8720 1001 1

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note

File Type: SQLite 3.x database, user version 58

Wi-Fi Networks

Task

Find and extract information related to Wi-Fi networks that the device has connected to.

Expected result

A file that describes Wi-Fi networks that the device has been connected to.

◆◆◆ Information Extraction

Wi-Fi Networks

- Information on Wi-Fi networks that the device has been connected to is located in:
 - `/misc/Wi-Fi/wpa_supplicant.conf`
- In this case, it is possible to access the information of the file, even before extracting it.
- Extract the file.
 - Take notes of all the process in order to document it in the report.

The screenshot shows a file manager interface with a list of files on the left and a Firefox download dialog on the right. The file list includes:

File Name	Size	Modified
p2p_supplicant.conf	14:42:06 (GMT)	2016-02-14
sockets/	14:42:06 (GMT)	2016-02-14
softap.conf	1970-02-25	23:44:16 (GMT)
wcnss_qcom_wlan_cal.bin	2009-01-02	11:00:04 (GMT)
wpa_supplicant.conf	2016-02-14	14:42:06 (GMT)
wpa_supplicant/	1970-02-25	23:42:44 (GMT)

The file `wpa_supplicant.conf` is circled in red. The Firefox dialog shows the file `vol1-1.misc.wifi.wpa_supplicant.conf` with the message "which is: unknown from: http://localhost:9999". The dialog asks "What should Firefox do with this file?" and has options: "Open with" (selected, Leafpad (default)), "Save File", and "Do this automatically for files like this from now on." The "OK" button is circled in red. At the bottom, a status bar shows "ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note" and "File Type: data".

Locations on Maps Application

Task

Find and extract the information related to the locations registered on the maps application.

Expected result

A file that identifies locations registered on maps application.

Information Extraction

Locations on Maps Application

- Access the maps application's folder in order to search information related to locations:
 - `/data/com.google.android.apps.maps/`
- In the cache/http folder, we can find two images.

52a6786d8aab81daefa5bd8117265422.0	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:21 (GMT)	5591	10059	10059	80306
52a6786d8aab81daefa5bd8117265422.1	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:21 (GMT)	23084	10059	10059	80307
52a6786d8aab81daefa5bd8117265422.1.tmp	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:20 (GMT)	2016-02-14 15:00:21 (GMT)	23084	10059	10059	80307 (realloc)
cdbcca21c9097e1d4198f169434eef5a.0	2016-02-14 15:00:19 (GMT)	2016-02-14 15:00:19 (GMT)	2016-02-14 15:00:21 (GMT)	5621	10059	10059	80037
cdbcca21c9097e1d4198f169434eef5a.1	2016-02-14 15:00:21 (GMT)	2016-02-14 15:00:19 (GMT)	2016-02-14 15:00:21 (GMT)	22569	10059	10059	80300

- Apart from extracting them, it is possible to add notes on them to facilitate the creation of the report.

Enter a note for `/1/data/com.google.android.apps.maps/cache/http/52a6786d8aab81daefa5bd8117265422.1 (80307)`:

A note works like a bookmark and allows you to later find this data more easily.

Imagen de interés

☒ Add a Standard Note

Add a Sequencer Event:

A sequencer event will be sorted based on the time so that event reconstruction will be easier

☐ M-Time (Sun Feb 14 16:00:21 2016)
☐ A-Time (Sun Feb 14 16:00:20 2016)
☒ C-Time (Sun Feb 14 16:00:21 2016)

OK

Locations on Maps Application

- Apart from extracting them, it is possible to add notes on them in order to facilitate the creation of the report.
 - It is possible to add not only informational texts, but also dates and thus, create an events timeline.

Enter a note for /1/data/com.google.android.apps.maps/cache/http/52a6786d8aab81daefa5bd8117265422.1 (80307):

A note works like a bookmark and allows you to later find this data more easily.

Imagen de interés

☒ Add a Standard Note

Add a Sequencer Event:

A sequencer event will be sorted based on the time so that event reconstruction will be easier

☐ M-Time (Sun Feb 14 16:00:21 2016)
☐ A-Time (Sun Feb 14 16:00:20 2016)
☒ C-Time (Sun Feb 14 16:00:21 2016)

OK

◆◆◆ Information Extraction

Locations on Maps Application

- We can find a list with applications used to share locations in *files/share_history.xml*:
 - Gmail.
 - Snapchat.
- Locations that have been shared will be checked later.
- In the databases folder, there may be relevant databases.
Save and note them.

[gmm_myplaces.db](#)

[gmm_myplaces.db-journal](#)

[gmm_storage.db](#)

[gmm_storage.db-journal](#)

Photographs

Task

Find and extract pictures included on the device's image.

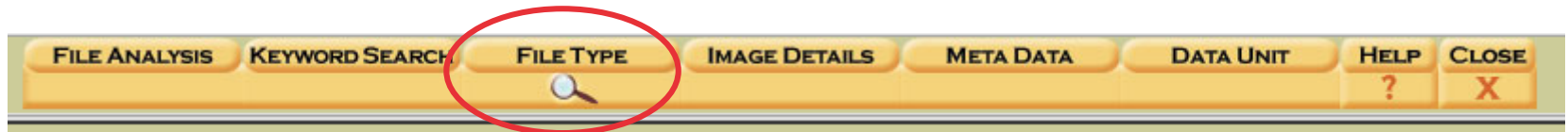
Expected result

A file of pictures included on the device's image.

◆◆◆ Information Extraction

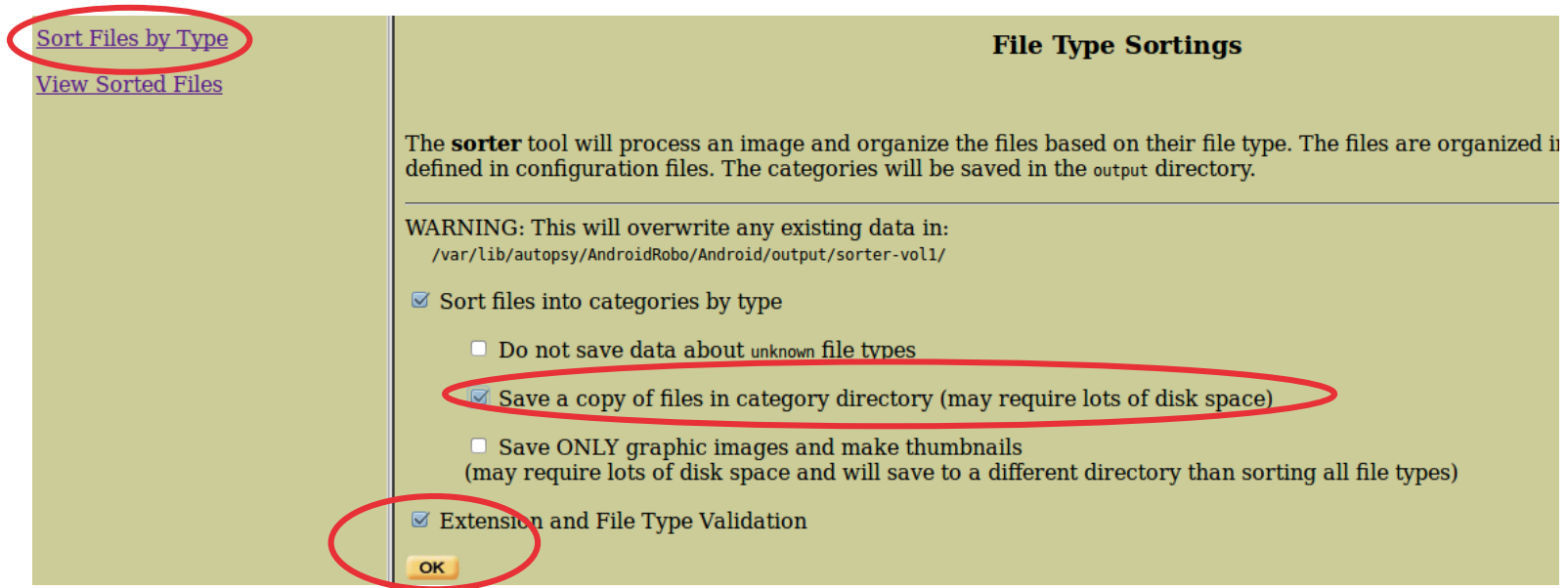
Photographs

- First, access the directory in which photographs are saved by default in order to inspect its content:
 - */media*
- Check that there are relevant images in:
 - */media/0/WhatsApp/Media/WhatsApp Images/*
 - */media/0/DCIM/Camera/*
 - */media/0/Pictures/Screenshots/*
- Autopsy also allows users to search all the images included in the image automatically.
- In File Type.



Photographs

- Select the “Sort Files by Type” option and, after selecting the options showed in the Autopsy screenshot, it will extract all the relevant types of files.



- Once created the list of files, it is possible to access it by using the URL displayed in the “View Sorted Files” option.

Photographs

Files (3801)

Files Skipped (1002)

- Non-Files (1002)
- Reallocated Name Files (786)
- 'ignore' category (0)

Extensions

- [Extension Mismatches](#) (156)

Categories (2013)

- [archive](#) (28)
- [audio](#) (2)
- [compress](#) (2)
- [crypto](#) (0)
- [data](#) (625)
- [disk](#) (0)
- [documents](#) (306)
- [exec](#) (183)
- [images](#) (117) ([thumbnails](#))
- [system](#) (0)
- [text](#) (172)
- [unknown](#) (578)
- [video](#) (0)

- [Page 1](#)
- [Page 2](#)

Image Thumbnails - Page 2



Emails

Task

Find and extract emails included on the device's image.

Expected result

The email database included on the device's image.

Information Extraction

Emails

- There are two email applications on the device:
 - `/data/com.android.email/`
 - `/data/com.google.android.gm/`
- Verify the content of the databases and check that there is no additional relevant content regarding the same application, except for the code of creation of tables. Therefore, add the notes necessary for the later creation of the report.

r / r	EmailProvider.db	2016-02-14 14:42:40 (GMT)	1970-02-25 23:44:32 (GMT)	2016-02-14 14:42:40 (GMT)	131072
r / r	EmailProvider.db-journal	2016-02-14 14:42:40 (GMT)	1970-02-25 23:44:32 (GMT)	2016-02-14 14:42:40 (GMT)	0
✓ r / r	EmailProvider.db- mjB722619EE	2016-02-14 15:01:24 (GMT)	2016-02-14 15:01:24 (GMT)	2016-02-14 15:01:24 (GMT)	36824
r / r	EmailProviderBackup.db	1970-02-25 23:44:33 (GMT)	1970-02-25 23:44:32 (GMT)	2016-02-14 14:42:39 (GMT)	131072
r / r	EmailProviderBackup.db-	1970-02-25	1970-02-25	2016-02-14	8720

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * A
File Type: SQLite 3.x database, user version 124

ASCII String Contents Of File: /1/data/com.android.email/databases/EmailProvider.db

```
SQLite format 3
;triggermessage_count_message_insertMessageCREATE TRIGGER message_count_message_insert after insert on Message begin update Mailbox s
Utriggerunread_message_readMessageCREATE TRIGGER unread_message_read before update of flagRead on Message when OLD.flagRead!=NEW.flag
ytriggerunread_message_moveMessageCREATE TRIGGER unread_message_move before update of mailboxKey on Message when OLD.flagRead=0 begin
Striggerunread_message_deleteMessageCREATE TRIGGER unread_message_delete before delete on Message when OLD.flagRead=0 begin update Ma:
Striggerunread_message_insertMessageCREATE TRIGGER unread_message_insert before insert on Message when NEW.flagRead=0 begin update Ma:
qtriggermessage_deleteMessageCREATE TRIGGER message_delete before delete on Message begin delete from Attachment where messageKey=ol
indexmessage_syncServerIdMessage
CREATE INDEX message_syncServerId on Message (syncServerId)\
```

◆◆◆ Information Extraction

Emails

- In the case of the Gmail application there are database files that make reference to a Gmail account. Note them as important and download them.

<u>internal.johntoppysmith@gmail.com.db</u>	14:201
<u>internal.johntoppysmith@gmail.com.db-journal</u>	14:201
<u>mailstore.johntoppysmith@gmail.com.db</u>	14:201
<u>mailstore.johntoppysmith@gmail.com.db-shm</u>	15:201
<u>mailstore.johntoppysmith@gmail.com.db-wal</u>	15:201

Web Browsing Data

Task

Find and extract web browsing data included on the device's image.

Expected result

The browsing history database included on the device's image.

◆◆◆ Information Extraction

Emails

- The analysed image has only one browser installed in:
 - */data/com.google.chrome/*
- Inspect the content and note all the files included in the internal folder in order to analyse them:
 - *app_chrome/Default*



A vertical list of files and folders, each preceded by a blue underlined text icon. The items are: Archived History, Archived History-journal, Bookmarks, Bookmarks.bak, Cookies, Cookies-journal, DeltaFileLevelDb/, Favicons, Favicons-journal, History, and History Provider Cache.

- [Archived History](#)
- [Archived History-journal](#)
- [Bookmarks](#)
- [Bookmarks.bak](#)
- [Cookies](#)
- [Cookies-journal](#)
- [DeltaFileLevelDb/](#)
- [Favicons](#)
- [Favicons-journal](#)
- [History](#)
- [History Provider Cache](#)

Information Related to Social Networks

Task

Find and extract information that may be relevant and related to social network applications on the device.

Expected result

Database files, pictures and other files included in applications' caches related to social networks

Information Related to Social Networks

- In order to perform this task, it is necessary to inspect the content of all the applications that are related to social networks.
- Access all the applications and note the relevant files included in each of them.
- Applications to analyse are presented below:
 - com.quickoffice.android – QuickOffice.
 - com.skype.raider – Skype.
 - com.snapchat.android – Snapchat.
 - com.whatsapp
 - com.instagram.android
 - com.facebook.katana
- The contents of such applications will be analysed during the analysis stage in order to look for evidences.

A photograph of a wooden desk with a laptop, glasses, and a mouse. The desk is made of thick, rustic wood. A silver laptop is closed and has a pair of black-rimmed glasses resting on it. A white computer mouse is on the desk to the right of the laptop. In the background, a white chair is visible. The word "Analysis" is overlaid in white text on a semi-transparent dark grey rectangle in the center of the image.

Analysis

Analysis Tasks

- During this part of the laboratory, contents mentioned before will be inspected. In addition, we will add notes regarding the information found.
- The objective of this task is to obtain the information required to write the report properly.
- To this end, we assume that:
 - The device has been used by the members of a criminal group in order to exchange some type of information on their targets.
- Data required to continue the investigations are described below:
 - Information on the possible accomplices in the events occurred.
 - Locations of possible future targets.
 - Information on accounts logged on the device, with the aim of acquiring them later, by using a court order.

Information on the Accomplices

Task

Analyse data obtained to establish a list of frequent contacts in the device as well as the type of information that has been exchanged.

Expected result

A part of the forensic report that specifies contacts of interest found on the device as well as messages that have been exchanged.

◆◆◆ Analysis

Information on the Accomplices

- When analysing the call table of the contacts2.db calls database

Full View

Item View

Script Output

	_id	number	presentation	date	duration	type	new	name	num
1	1	444	1	1455393591600	119	2	1	{null}	
2	2	07484157148	1	1455401147692	0	2	1	{null}	
3	3	07454127148	1	1455401158993	0	2	1	{null}	
4	4	+448444827777	1	1455465631810	1	2	1	{null}	

- and navigating the contacts table, we can conclude that:
 - The following sentence has been executed to reduce the number of columns: `Select display_name, sync1 from raw_contacts`

display_name	
J	https://www.google.com/m8/feeds/contacts/joh
J	447401089370@s.whatsapp.net
j.thebest@gmail.com	https://www.google.com/m8/feeds/contacts/joh

Information on the Accomplices

- The inspection of the messages database (mmssms.db) provides the following information.
 - The following sentence has been executed to simplify the output obtained and to facilitate its reading: `Select address, person, body from sms`

	address	person	
			You can also tap on this link to verify your phone: v.whatsapp.com/4929
8	Snapchat	{null}	Snapchat Code: 727829. Happy Snapping!
9	7401 089370	{null}	Movil nuevo. Aun no me hago con el. La app de Snapchat esta muy bien
10	+447401089370	1	Hola John! Móvil nuevo :) aunque aún no me hago con el. Snapchat esta
11	7401 089370	{null}	Siii
12	+447401089370	1	También estoy llegando. No tengo tarifa de datos ya

Information on Accomplices and other Phones

- After the information analysed from the SMS, contacts and telephones databases, we can conclude that the device made calls to four different numbers. This information will be complemented with social networks:
 - 444 seems to be an information number of the telephone company.
 - Two phone calls have been made to very similar mobile phone numbers; however, any of them was answered.
 - The Internet search does not provide any useful information.
 - Various suspicious messages have been sent to a contact that has the following phone number: 7401089370.
 - A call has been made to the number +448444827777.
 - An Internet search shows that the number belongs to the United Kingdom Historic Royal Palaces service.
 - There is a contact whose email address is: j.thebest@gmail.com.
 - Text messages to register in services such as Snapchat and WhatsApp.

Information on Locations

Task

Analyse the information on places that the device may have been to.

Expected result

A part of the report that specifies locations found and the importance that they have in the investigation.

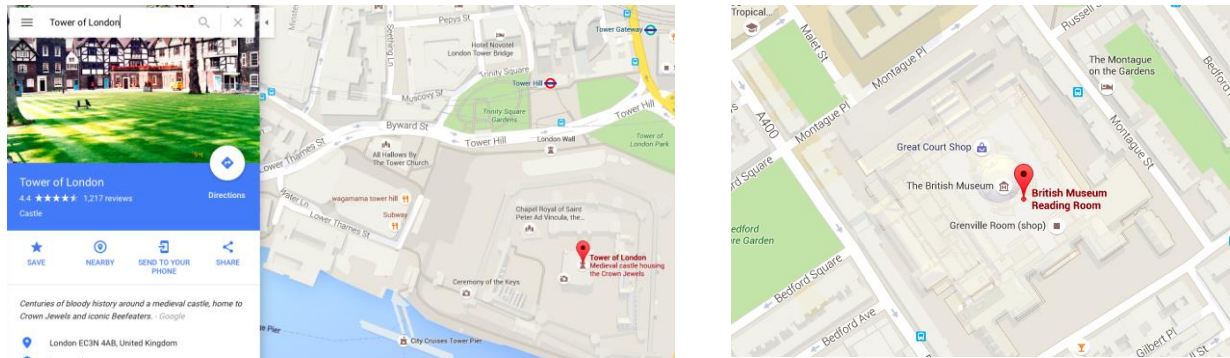
Information on Locations

- If we analyse the ggm_myplaces.db database, we can observe that there are two entries in the table with URLs that belong to Google maps.

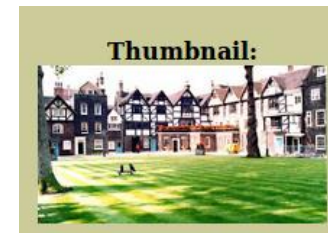
Full View Item View Script Output		
	corpus	key_string
1	1	http://maps.google.com/?q=British+Museum+Reading+Room,+Great+Russell+St,+London+WC1B
2	1	http://maps.google.com/?cid=12159518736249087079

Information on Locations

- Check the results provided by the URLs and verify that they are linked to two specific locations of the city of London.



- The phone number found in the history of calls is the contact phone of the Tower of London.
- In addition, when analysing one of the files found in the application's cache, we can observe that the image is the same as the one displayed in the figure:
 - `cache/http/52a6786d8aab81daefa5bd8117265422.1`



Information on Locations

- Then, analyse the content of the Wi-Fi networks file and check that it includes data of a connection (including a password), but the name of the access point does not provide any information of the location apart from the country (Great Britain).

```
-----8-----  
p2p_disabled=1  
p2p_no_group_iface=1  
country=GB  
  
network={  
    ssid="SKY565BA"  
    psk="EABATUTD"  
    key_mgmt=WPA-PSK  
    priority=1  
}  
00000030000000e00000
```

- Note all the discoveries made in this task in order to write the report later.

Information on Locations

- Pictures taken by the camera do not show the GPS coordinates among the EXIF information.

```
santoku@santoku-VirtualBox:~/Downloads$ exiftool /var/lib/autopsy/AndroidRobo/Android/output/sorter-voll/images/data.img-104106.jpg
ExifTool Version Number      : 9.46
File Name                    : data.img-104106.jpg
Directory                    : /var/lib/autopsy/AndroidRobo/Android/output/sorter-voll/images
File Size                    : 809 kB
File Modification Date/Time  : 2016:02:16 23:13:28+01:00
File Access Date/Time       : 2016:02:16 23:15:36+01:00
File Inode Change Date/Time  : 2016:02:16 23:13:28+01:00
File Permissions             : rw-r--r--
File Type                    : JPEG
MIME Type                    : image/jpeg
Exif Byte Order              : Big-endian (Motorola, MM)
Make                         : Motorola
Camera Model Name            : XT1021
X Resolution                  : 72
```

- However, the content shows that they have been taken in a museum with important pieces of art.
 - According to the location information obtained before, we can conclude that the British Museum is the place involved.
- Note all the discoveries made in this task in order to write the report later.



Information on Accounts

Task

Analyse data on each of the relevant applications found on the device in order to establish a list of frequent contacts and the type of information that has been sent by using them.

Expected result

A part of the forensic report that specifies relevant information found on each of the analysed applications and whether information is related to the previously analysed data.

Information on Accounts

- In this task, the information included in the rest of applications installed on the device will be analysed.
- As it was mentioned before, the analysis of such applications should be validated with control devices:
 - For each application, evidences should be created in the control device, and it should be verified that they really correspond to the facts directly observed on the phone.
 - In this task it is assumed that the validation of the meaning of data has already been made.
 - If desired, the student may validate data.
- In this section of the analysis, only a part of the possible results to obtain is displayed.

The revision of the possible set of additional evidences is an extra task for the student.

Information on Accounts – Spotify

- After an initial analysis, it is verified that the accounts have not been used; therefore, they do not include relevant information:
 - Facebook.
 - Instagram.
 - Skype.
- After analysing Spotify, a file that includes the user and the account authentication token is found.
 - *data/com.spotify.music/files/settings/prefs*

```
autologin.canonical_username="johntoppysmith"  
autologin.username="johntoppysmith"  
autologin.saved_credentials="{\"johntoppysmith\":[\"johntoppysmith\", \"ajpHPT8ErZCWmrR3x0NUPmbfsSKbL+krHEWhyqKJqrjlqbDUobsfu065eWVKXEIn\"]}"  
language="en_GB"  
autologin.blob="ajpHPT8ErZCWmrR3x0NUPmbfsSKbL+krHEWhyqKJqrjlqbDUobsfu065eWVKXEIn"  
core.clock_delta=-1
```

◆◆◆ Analysis

Information on Accounts - Gmail

- Gmail emails can be analysed in the following file:
 - *databases/mailstore.johntoppysmith@gmail.com.db*
- Its content shows a series of messages to the contact j.thebest@gmail.com, in which the location of the museum is shared and some pieces of jewellery are mentioned. The following consultation has been made to facilitate the reading of the result:

- *Select toAddresses, snippet from messages*

4	John Smith <johntoppysmith@gmail.com>	Hi John tips to get the most out of Gmail Bring your
5	"johntoppysmith" <johntoppysmith@gmail.com>	Hey johntoppysmith! Before you start Snapping, it's a
6	"" <j.thebest@gmail.com>	British Museum Reading Room Great Russell St Lond
7	"" <j.thebest@gmail.com>	Ya he llegado
8	"" <j.thebest@gmail.com>	Despues iremos a ver las joyas

- Given the evidences found until date, they may possibly be related to the Tower of London.

Information on Accounts - Whatsapp

- Databases of Whatsapp are analysed. The application's conversations are stored in: */databases/msgstore.db*
- The following entries can be found when analysing the content. The following consultation has been made to facilitate the reading:

- *Select key_remote_jid, data, latitude, longitude from messages*

	key_remote_jid	data	latitude	longitude
1		-1 {null}	0	0
2	447401089370@s.whatsapp.net	Hola!	0	0
3	447401089370@s.whatsapp.net	{null}	51.52393464	-0.07597850985
4	447401089370@s.whatsapp.net	Voy de camino	0	0
5	447401089370@s.whatsapp.net	{null}	0	0
6	447401089370@s.whatsapp.net	{null}	51.5211384	-0.1149357
7	447401089370@s.whatsapp.net	Genial!	0	0

- It is verified that there is a communication via chat messages with the same number used to exchange SMS messages.
- Two locations have been shared. After looking for coordinates, a conclusion is reached:
 - The first coordinate corresponds to the following address: 10 Redchurch ST, London E2 7DD.
 - The second one corresponds to the following address: A401, London WC1X 8NX.

Information on Accounts - Snapchat

- It is possible to analyse the main database file of Snapchat:
 - *databases/tcspahn.db*
- It is verified that the “J” contact has also been contacted through Snapchat.

Full View Item View Script Output				
	_id	Username	DisplayName	PhoneNumber
1	1	jorge.anonimo	J	
2	2	johntoppysmith		
3	3	teamsnapchat	Team Snapchat	

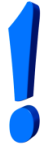
- It was not possible to access files deleted by Snapchat.
 - It may be due to the use of the application com.pinellascodeworks.secureswipe that allows users to securely delete unused blocks on the internal memory.



Report

Introduction

- As a last step to complete the laboratory, the student should write a report that includes evidences found and conclusions reached after the analysis.
- In order to write the report, you can use all the notes and information gathered during the analysis, including information provided in the solution of each stage.
- In the following slides, there is a description of the general structure that is expected from the report.



Such structure is quite similar to the one mentioned in this unit, but, in addition, some clues and guides regarding the specific case involved will be provided.

- Once finished, it is recommended to upload the report to the corresponding section of the forum, where you will also be able to read and compare reports made by other students.

Summary of the Case

- In this section you should describe:
 - A title page that includes your user identifier for the forum.
 - Specific precedents of the case. Statement of the case described with your own words.
 - The status of evidences that were sent to you. Size and description of the evidences file received including the data that enable its verification by third parties.
 - Limitations of the analysis that you are conducting, taking into consideration the status and the set of evidences received. Take into consideration that you do not have access to the real device and you are only analysing one of the device's partitions.
 - What you are asked to verify or corroborate as a forensic analyst.
- Since the case is a simulation, it is not necessary to include:
 - Who has requested the forensic analysis.
 - The most important dates regarding the report.
 - Personal data of the analyst.

Used Tools

- You should describe all the tools used.
- Apart from the ones presented during the resolution of the exercise:
 - Autopsy.
 - Sqliteman.
 - Firefox.
 - Exiftool.
- You should add any additional tools that have been used. Remember that, for each of them, you should specify:
 - Version of the tool used (including the platform).
 - Manufacturer.
 - Task it has been used for.
- If you have used any recent or unknown tool, you should include a validation test of it.

Evidence Acquisition

- You should include the process followed to add the obtained image to Autopsy.
- This section of the report will not be very significant for this simulation, since the process will be very similar for all the students.




Evidence Processing

- In this section, you should explain the way of extracting the different evidence files used to prove your reasoning during the analysis stage.
- In case you have performed any operation to retrieve files in the removed space, you should describe the process carried out.
- In addition, for each information element extracted from the image, you should obtain its MD5 summary and add it to the forensic analysis:
 - Each extracted evidence should conduct the analyst to the original data unambiguously.
 - Furthermore, this way, you will also be able to verify that the rest of students have analysed exactly the same evidences.

Analysis and Conclusions

- Based on the information extracted in the last section, you should discuss about the events that are proved by using the information included in the analysed image.
- In this case, arguments and hypothesis are managed by the people that have requested the analysis; therefore, our work is limited in this sense.
- Each conclusion extracted from the analysis should be justified by an evidence that has been identified during the extraction and analysis process.
- It is possible that you cannot confirm categorically some statements due to the scarce number of evidences; therefore, you should limit your statements to what evidences indicate.



Research exercise

◆◆◇ Research exercise

Description

- In this exercise the student should conduct a research and write the results obtained on the subject's forum, in order to discuss them with the rest of students.
- During this unit, we have reviewed and studied the limitations that some security technologies included in mobile devices suppose for the forensic analysis.
- In this exercise, you should investigate one of the technologies mentioned below:
 - Disk encryption.
 - Backups encryption.
 - Code lock of the device.
 - Remote lock.

Description

- You explain the following specifications for the selected technology:
 - Platforms that implement it.
 - From which version?
 - Scope of the result of the forensic analysis (for each platform).
 - How long may the analysis take?
 - Recommendations to reduce its impact during its impact in the analysis process.
 - Can it be avoided in any way during the seizure or at any other moment of the analysis?
 - (Commercial or regular) tools that allow analysts to mitigate the impact during the forensic analysis process.

A hand holding a pen is writing on a notebook. In the foreground, a black calculator and a textbook are visible. The textbook contains math problems, including arithmetic series and sigma notation. A blue semi-transparent banner is overlaid on the image, containing the text "Assessment Test".

Assessment Test

Thank you for your attention

