Anglia Ruskin University

Mobile Forensics: OpenSource Investigation

SID: 1914301

MOD002691 Final Project Report

BSc (Hons) Cyber security

Submitted: April 2023

Anglia Ruskin University, Cambridge

Table of Contents

Table of Tables

Table of Figures

1.0 Abstract

Society is growing in terms of technological development; this includes the use of mobile devices consisting in Android as the most popular Operating System. Android can be seen in diverse devices such as televisions, tablets, consoles and even cars. Therefore, the need for mobile forensics investigators capable of analysing Android is also growing. The aim of a mobile forensic investigator is to analyse the digital evidence that can be contained in a mobile device and perform an investigation without affecting the integrity of the data, this is an essential step, as evidence needs to be admissible in court. Although with the rapid development of technology, digital evidence is often overlooked or mishandled. This can be due to poor training or even lack of funding in the digital forensics field. As such, training mobile forensic investigators can be a complex and expensive process due to the fees of commercial tools. Thus, the aim of this research is the creation of a tutorial that can guide mobile forensics students and non-technical people into creating their own isolated virtual environment. This will allow students to perform a mobile forensic analyse with the use of two open-source tools and comparing the outcomes for dual-verification. With this research, students will also gain basic knowledge on how to create a virtual environment, how two different open-source tools function, how to perform a basic analyse on an Android device such as the HTC Desire 626s provided by the NIST database and where to find the data extracted from the device.

2.0 Introduction

2.1 Background

The Digital Forensics has expanded its field to include the complex and specialized branch of Mobile Forensics. This is due to the fact that the everyday life now includes the use of technology. As such, this field focus on the extraction, preservation and accurate analyse of digital evidence from a mobile device, such as smartphones, tablets and even wearables. (Rick Ayers, Sam Brothers, Wayne Jansen, May, 2014) also supports that *"Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. Mobile device forensics is an evolving specialty in the field of digital forensics".*

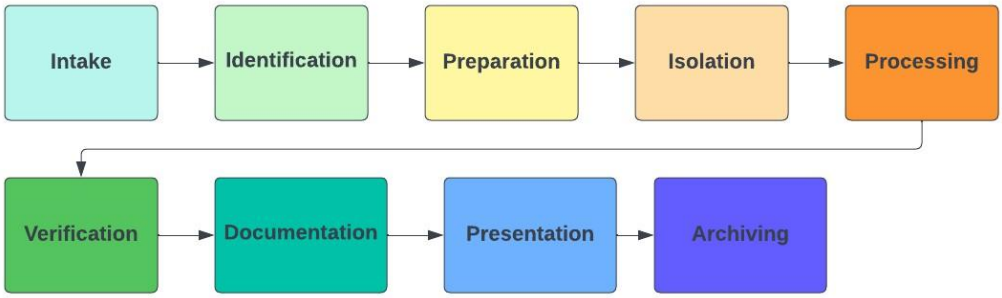


Figure 1 Mobile phone evidence extraction process (Satish Bommisetty, July 2014)

It is important that in a court, mobile devices that have failed to undergo a methodical and legitimate forensic examination will not be considered as valid evidence. Furthermore, for the evidence to be internationally accepted, it is vital that forensic laboratories comply with ISO 17025 standards, which guarantees the accuracy and reliability of results and demonstrates the competence of the laboratory in question (ISO standards, N.D).

This is crucial, as potentially critical information relevant to the case may be stored on the poorly analysed mobile device, which can jeopardize the outcome of a case. The case of Casey Anthony is an example of how, according to (Craig Wilson, July 2011) the credibility of the Digital Forensics team was put into question. As the defence realized the massive discrepancy in the results of both tools used. One tool, NetAnalysis, showed that one visit was done to a website related to chloroform, while the second tool showed a massive difference of 84 visits done to the same website.

Because of these inconsistencies, digital evidence did not play a part in the Casey Anthony trial. Which raises the questions of what went wrong. Was it lack of training and resources from the Digital Forensics team? Could open-source mobile forensics software have been used as part of the dual verification tool?

To extract and analyse digital evidence from mobile devices, there are several choices provided such as the free and community developed Open-source software and the commercialized tools developed by professionals. However, each has advantages and disadvantages, such as:

	Open-Source software	Commercial software
Advantages	• No licensing fees. • Bugs and issues easily fixed through the community. • Tools are customizable according to needs. • User friendly GUI • Free to use and users have access to the source code as to which they can modify it and distribute	• Technical support • Higher quality • Reduction of time required to gather evidence – automation. • Regular updates
Disadvantages	• Requires the user to be familiar with Linux because most opensource applications are only compatible with Linux. • Lack of technical support • Not as easy to use	• Expensive software for digital laboratories • Expensive annual License fee • Less flexibility – Automated functions • Data can still be missed. One tool may not offer support for • a specific mobile device, therefore requiring another expensive software. • Can be discontinued and affect businesses

Table 1 Differences between Open-Source and Commercial software (XiphCyber, May 2022)

Open-source tools for mobile forensics are increasingly growing and becoming more popular despite the disadvantages. Users who are willing to invest time into learning these tools will have a good starting point into learning mobile forensics.

Although, according to (Maxim Chernyshev, November 2017) the scarcity of technical support such as lack of documentation, training courses or even a poor communication with the developer, could be a big obstacle faced by those who are looking to learn open-source mobile forensics tools. This can limit the ability to apply the skills on real-life scenarios and even

demotivate learners who face these challenges. In addition, commercial tools are quite often expensive and require an annual fee to be paid which also creates another barrier in learning mobile forensics. This highlights the need for the creation of guides regarding open-source tools, tutorials, explanations on testing environments and how to assist learners in using dualverification to verify the integrity of the results obtained.

The demand for trustworthy open-source tools for higher education and even police training is the main factor behind this research. The goal is that not only DF students but even nontechnical people, will be able to conduct mobile forensics investigations through open-source tools. This will give them transferrable skills that they may employ in a workplace environment where commercial software is used. It is an interesting and dynamic field, where resources are provided to students and even non-technical people that have interest in mobile forensics, can obtain mobile data and conduct any type of investigations. These tools also offer real-time approach to the results obtained, and the ability to view the results of these analysis creates an extra layer of excitement and can lead to insightful outcomes related to the investigation.

2.2 Scope of the Project

The scope of this project is to develop a guide using an Android dataset from NIST and use two open-source tools to conduct an investigation. In which, the reader will also be able to follow along and reproduce the same steps. This guide will outline the steps on how extracted data from mobile devices can be used to determine an individual's whereabouts and activity at a specific moment. *Table 2* lists examples of potential evidence that may hold information related to investigations and that will be explored in this paper. To do so, this research has also reproduced the steps of how to create a Windows 10 forensics lab using two types of hypervisors.

The focus of this research will solely fall on the most popular mobile device operating system, the Android. As a result, other devices such as Blackberry, iOS and Windows will not be explored in this study. This is due to the complexity of other OS, the limitation of the scope and timeframe of this paper.

In terms of data, due to the limitations of the datasets provided by NIST, modern Android devices will also not be explored. As this research is a guide for non-technical students to follow, in order to perform a basic analyse of a mobile device, the same data must also be

available to download. Due to the already extracted data provided by NIST, the extraction through the use of these tools will not be an aim in this paper.

Evidence	Data to be analysed
• Internet browser	URLs, SQL databases
• SMS and MMS	Outgoing SMS and MMS
• Phone calls and logs	Call history and deleted information
• Twitter	Outgoing tweets
• GPS	Geotags
• Deleted files	Deleted cache, pictures
• Device information	Model, IMEI and IMSI, phone number

Table 2 Examples of potential evidence sources from a modern mobile device

2.3 Hypothesis

"How open-source mobile forensics may be of used in investigations and how they can facilitate the learning process of mobile forensics?"

This hypothesis is specifically dedicated to mobile forensics open-source tools and how can these also facilitate the extensive learning process of mobile forensics investigations and compact them into faster approaches for basic investigations that require quick results. This idea is reinforced by an article (Owen Bowcott, May 2018) in which outlines how digital evidence in cases is being overlooked and often mishandled by police officers due to the lack of funding in Digital forensics, an increase of digital evidence and the lack of expertise.

2.4 Aims & Objectives

For a clearer understanding of the research process, the aims have been divided into smaller, more detailed chapters. Each chapter will consist of a specific aim and include related objectives. This will grant readers with the knowledge on the type of information gained through mobile forensics and a breakdown on the forensics guide.

Understanding the type of information obtained through mobile forensics analysis and how can it be used by a non-technical person

Mobile data can be collected from various types of devices and operating systems, including Android phones, Blackberries, Apple iPhones, Android tablets and iPads, wearables, and more. This is due to the widespread use of mobile phones as the preferred choice for user interaction,

surpassing the use of Desktops/Laptops. *Figure 2* illustrates the increase of mobile phone usage compared to the Desktop and laptop usage in the year of 2022.

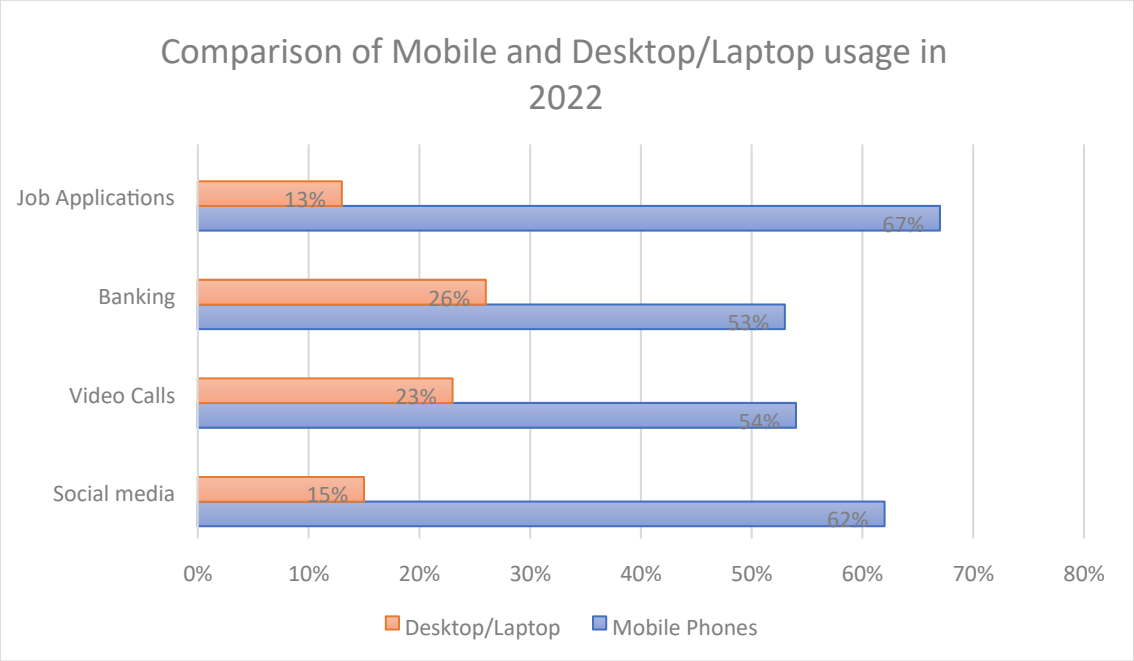


Figure 2 Comparison of Mobile and Desktop/Laptop usage (Hiley, February 2023)

As such, these devices are not only being used for pleasure activities but also for criminal activities such as human trafficking, fraud, child pornography, harassment, and accessibility to narcotics. Therefore, it is essential that investigators and layman must understand what type of information they will be extracting. Smartphones provide a vast amount of data from call history, contacts, text message, e-mail, browser history, chat logs, GPS (Jeff Lessard, January 2010).

The information gathered through mobile analysis can be used in multiple purposes for diverse types of laymen such as lawyers, private investigators, law enforcement and even for military use. As an example, the military forces can use mobile forensics to detect and deter communication between terrorist organisations that may share propaganda videos or even trigger any type of mechanisms for IEDs *(Improvised Explosive Devices)* (MSAB, N.D).

As the mobile forensics field is in constant development, it is essential that mobile forensics investigators stay up to date with the current techniques and tools used for the data extraction and examination in this field. To provide more information on the challenges, (Hoog, May 2014) explains how it is essential to understand the different types of mobile acquisition as they can retrieve essential data to the examiner. As such a classification method was created by

the mobile forensics' examiner and researcher Sam Brother. This classification aids the mobile examiner to compare the different tools and provides a framework. Although these methods do become more technical, time consuming and expensive. The examiner must only perform the extraction that they were trained on as digital evidence can be permanently destroyed if procedures are not followed.

	Method	Challenges	Data collected
Manual Extraction	Data viewed directly from the device's screen and data is manually documented through a digital camera	Impossible to recover deleted information and data modification	Captures what is shown on the device
Logical Extraction	Connected through a cable to the forensics workstation. The Forensic tool the communicates with the mobile device's OS requesting data from the System through API (Application Programming Interface)	Not available on all devices. It can also not be performed on a locked phone as it requires USB debugging.	Call logs, SMS, MMS, Images, Videos, Audio files, contacts, calendars, app data. Live data can be retrieved, although it will not retrieve any deleted data.
Physical Extraction/Hex Dump	Extracts all the data stored in a phone which provides the examiner with more data compared to the previous extraction types. This connects the phone through a cable, extracts the memory data into a raw disk image. Requires an expert to analyse this data extraction result as it is in binary format	Extensive but least support method. The extraction is also dependable on the operating system and security measurements of the device.	Deleted data such as images, videos, installed apps, location information, emails can be recovered
Chip-off	Data acquired directly from the chip and data is extracted through a chip reader. Due to the wide variety of chips used, this extraction requires the investigator to have great knowledge on this type of extraction	Without prior knowledge regarding the chips, the investigator can damage the chip and the data inside it.	Ensures that the investigator has obtained all the data stored in a device. Usually used if the device has suffered physical damage such as water or fire damage

Micro Read	Examining the data manually and interpreting the data seen on the memory chip	Time consuming, costly and requires extensive knowledge on Flash memory and file system. No commercial tools available	Used for high profile cases such as national security crisis and only used after all other extractions have been used

Table 3 Types of extraction used in mobile forensics (Hoog, May 2014), (Special Counsel, March 2016), (O' Reilly, N.D), (Mobile Forensics Solution, N.D) and (Privacy International, OCtober 2019)

Digital Forensics curriculum and best applied to the creation of a mobile forensics guide

Due to the necessity for communication and its growth in society, digital and mobile forensics are becoming more popular topics. Although interest in teaching these subjects has increased, there is a lack of consistency in the curricula created for these subjects. (Khushi Gupta, June 2022) points out some of the challenges faced by educators and students regarding the creation and implementation of DF labs such as:

- the lack of educators in the field which leads to students not being provided with the essential skills needed for employers.
- The creation of lab exercises is also a long process and often found tedious, therefore there is lack of practical exercises and mainly theory is provided and relied upon.

While there are many studies that provide insight in Digital forensics curriculum and tested frameworks applied to undergraduate students, there seems to be a lack of fully dedicated studies into creating a framework just for mobile forensics. As such, this research will adapt and apply knowledge gained through other studies related to digital forensics curriculum and apply it to mobile forensics.

One study conducted by (Kevin S. Floyd, April 2014) supports the idea that active learning, such as hands-on exercises, increases student's knowledge in the subject for a longer time than just learning theory. In addition, to theory-based education, it is essential to combine this knowledge with practical exercises such as digital forensic labs.

Design of the forensic guide and how this software can be used by non-technical learners

To begin this guide, it is essential to define the type of testbed environment that will be used for mobile data analysis. Thus, a user must comprehend the definition of a testbed and its purpose.

(Testim, November 2019) defines that a testbed is an environment that is used to simulate a real-world scenario served to test and analyse data. Creating a test environment has many advantages and is an essential step, as these provide with an appropriate evaluation of the performance of an application that is being tested. Furthermore, it isolates the code and verifies the behaviour of an application, assuring that the host's system does not interfere with the performance of the application tested. A testbed also consists of specific hardware, software, OS, network configuration, the product under test and any other application and system software, as this allows for the tester to be certain that this application will behave the same way as in a standard environment.

Testbed environment

The types of operating systems that will be used to create a testbed environment must be determined to be compatible with the appropriate tools for the selected data that will be extracted.

Windows 10 will be deployed as this operating system is the most popular OS used and up to date. This popularity is due that most people are familiarized with Windows XP, windows 7 and Windows 8. Research conducted by (Petroc Taylor, February 2023) also confirms that up until January 2023, windows 10 was still running in 69% of most computers while the new Windows 11 is only being run in 18% of the devices. The remainder 17% are held by its competitor, Apple MacOS and iOS.

Running an isolated copy of windows 10 is a necessity and as such, the installation of a virtual machine is a requirement. There are many ways that this can be achieved depending on the type of hypervisors software being used.

Virtual machines installed directly on the Host OS are called hypervisor type 2, these share the hardware and resources with the host. Contrarily, type 1 hypervisors are installed directly on the machine, and all the resources, including processors, RAM, storage are reserved for the virtual machines are reserved for the virtual machine.

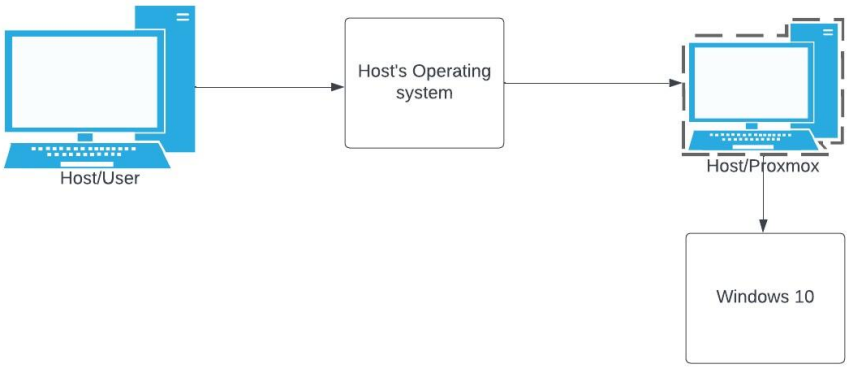


Figure 3 Virtual Machine hypervisor type 2

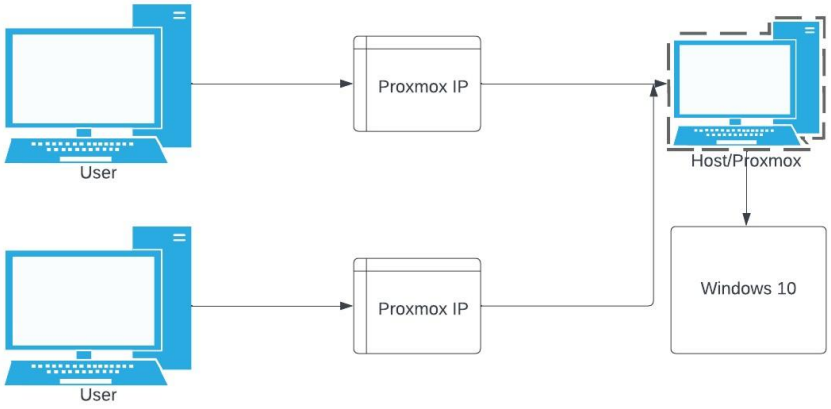


Figure 4 Hypervisor type 1

According to (Anand, February 2021) Hypervisors such as Proxmox and ESXi are composed by lightweight operating systems without a desktop environment and are easily accessed through a Web interface and SSH. Compared to Type 2 hypervisors, these sorts of hypervisors also do not need any kind of maintenance. However, Type 1's primary drawback is the inability to access the host as a workstation because of the lack of environment.

Now that this has been considered, the user can choose the optimal hypervisor type depending on their requirements and the specs of their components.

As such there are numerous Type 1 hypervisors available, including KVM Linux, Proxmox, and VMware ESXi. For the purpose of this research, Proxmox was the chosen hypervisor, as (Anand, February 2021) states it is a user-friendly open-source platform that supports small and enterprise-level virtualization and has an intuitive dashboard. While comparing it to VMware ESXi that is only free for 60 days. The free license also has certain limitation such as a maximum of 2 physical CPUs in the host machine, and only 8 vCPUs in the virtual machine itself. *Table 4*

shows the minimum system requirements for the installation of Proxmox and the hypervisor type 2, VirtualBox.

System requirements of VirtualBox and Proxmox		
RAM	• 2GB/4GB	• 2GB
Disk Space	• 25GB • Recommended more space to work on Forensic evidence	• 32GB
Processor	• X86 64-bit CPU • Most recent Intel or AMD CPU will also work	• Intel EMT64 or AMD64
Operating system	• Windows Server 2008 or 2008 R2 (64-bit) • Windows 7/8/8.1 (64-bit) • Windows 10 RTM build 10240 (64-bit) • Windows server 2012/2012 R2/ 2016 (64-bit) • Mac host (64-bit) • 10.13 (High Sierra) • 10.14(Mojave) • 10.15 (Catalina) • Does not work on new M1 hardware	• Not needed as it runs directly on the machine

Table 4 System requirements for the installation of VirtualBox (Cyberstart, N.D) and Proxmox (Proxmox, N.D)

As mentioned above, Windows 10 will be the chosen OS due to its popularity, considering that one of the chosen tools, Avilla Forensics is also only compatibility with Windows 10 and Windows 11. More information about this tool can be found in *section 8*.

Having now established the type of hypervisor installation, the operating system that will be running and tools that will perform the analysis of data. It is crucial to ensure that the testing environment, this including the Virtual Machine is in working condition.

Testing the functionality of the testbed environment

It is vital to verify if the environment is functional to ensure a secure and isolated environment for the creation of a mobile forensics' lab. Testing the functionality of the virtual environment is an essential step, although this is often overlooked. Not testing the virtual environment can lead to potential inaccuracies or even compromising the results. A study conducted by (Lozenzo Martignoni, July 2010) reinforces the idea that little efforts has been invested into testing these types of environments. This led to the creation of a prototype named "KEmuFUzzer" which was used to test VM's such as VirtualBox, VMware, QEMU and BOSCHS.

The authors begin by defining the two primary classes of virtual machines, including the process virtual machine, which may run a single process, and the system virtual machine, which can run an entire operating system. It is also explained that throughout the development of modern and complexed system architectures, creating a Virtual Machine that fully replicates the physical host is a challenging process and that efficiency has become the main priority. Thus, the lack of standardization in testing these environments. The authors conducted a several testing methods on the VM that included a snapshot of the VM before the tests were ran so that this can be reverted to a previous state if necessary. Additionally, the use of fully automated testing tools based on fuzzing and differential analysis, specifically designed for virtual machines were employed.

According to (Synopsys, N.D) this means that to find vulnerabilities, invalid or even unexpected data input must be injected into the system. The behaviour of the system is then recorded during initial tests, and it is then submitted to more examination in order to create effective exams. Fuzzing is beneficial to a system as:

- it provides a good picture of the quality of security of the system and software under examination.
- Hackers also use this technique to find any vulnerabilities which can help developers to avoid any zero-day exploits.
- It is an automated system which requires no manual intervention and therefore it is as low costly budget.
- Fuzzing can also detect vulnerabilities that were not detected by manual audits.

As such, to prevent any interference with lab results, it is essential to submit the testing environment to testing. Which can be done using Open-source fuzzing tools such as OSS-Fuzz which supports the analysis in a Virtual Machine.

Design of user's guide based on previous theory: Testbed approach

This section will outline the steps taken for the creation of the testing environment mentioned above. The installation of the OS's and tools. Finally, a description of how to access the data set employed for the analysis in this guide.

Steps	Task	Notes
1. User must decide the type of Hypervisor	Depending on user's needs and computer components, user must decide between Type 1 or Type 2 Hypervisor	• Proxmox Download Link • VirtualBox
2. Installation of Hypervisor	User must install the hypervisor according to the Type. If Type 1 was the chosen one, user must install the hypervisor in a separate host system. If Type 2 is the chosen one, then this can be installed in the user's current system	**To take into consideration:** Installing Proxmox will erase the system's environment
3. OS and tools	Installation of Windows Operating system. The installation of Avilla forensics is required.	• **Windows 10** • **Avilla Forensics** • **Autopsy**
4. Dataset	Download of the NIST CFREDs Dataset for analysis.	• **Mobile Device Images**
5. Analyse of dataset in Windows 10	Analysing the same dataset through Avilla Forensics and Autopsy. The goal here is to obtain the same results found in both tools and compare them.	

Table 5 Design of the mobile forensics guide

NIST (National Institute of Standards and Technology) will be the main source of data used for the analyse in both open-source tools for comparison of results. With NIST, students can explore the different types of databases related to digital and mobile forensics as these are also widely used for training purposes. This database is referred to as CFReDS. According to (NIST, N.D) the CFReDS are datasets that can assist an investigator in tool testing, developing familiarity with the tools and training. These datasets are designed to simulate real-world scenarios that include diverse artifacts that can be explored by students. Furthermore, it guarantees the reliability of the forensic tool in use.

2.5 Theoretical limitations of the project

This research made it clear that mobile forensics is a new and developing field. One of the main limitations in this field is the lack of limited access of research but also, the lack of a set framework to adhere to. This is due to new technologies that are constantly emerging and making these obsolete. To worsen this limitation, the increase of number of mobile devices purchased are predominantly composed by Android and IOs as these are becoming the popular choice in the market. As a result, it will be more difficult to analyse other operating systems, like Windows, and there will not be any recommendations available to do so.

To perform the lab exercises provided in this guide, the users must also have the required system requirements to perform these. Therefore, hardware and costs could possibly become a limitation.

Regarding dataset, although NIST was mentioned as a provider of datasets. There seem to be a lack of up-to-date datasets for mobile forensics. Thus, there is the need for the creation of more datasets that will include the newest Android phones with recent OS versions and Applications.

To conclude, one of the main limitations is also the lack of documentation and support from any of Open-source tools to provide a reliable mobile analyse.

2.6 Assumptions

This research assumes that despite the rapid changes in mobiles and the challenges faced by law enforcement to keep up with these changes, mobile forensics can be applied to all mobile devices independent of the Operating System. This is due to the rapid development in this field and the need of identifying digital evidence to be applied in court (Abdulalem Ali, April, 2017). It is also assumed that due to the constant changes, communities have also kept up and developed open-source tools capable of extracting and analysing data from the most recent devices. This assumption is supported by the fact that, during the creation of this research, Avilla Forensics tool was constantly being updated, which demonstrated the dedication from an open-source community in staying updated with the new technologies.

Although, most open-source tools do not have great documentation or even support from its creators, which can become a challenge to non-technical people to use it (XiphCyber, May 2022).

2.7 Summary of the chapter

To summarise, this research was conducted due to the advances in the use of mobile devices for communication. Although, these are also being used to commit crimes. Therefore, Digital forensics has expanded its branch into mobile forensics, where the extraction preservation, analysis and presentation of digital evidence is essential in the outcome of a case.

Since it is a very recent and still growing field, there is a lack of training, resources and even funding to invest in the future of mobile forensics investigators. Due to the high price of commercial tools' annual fees and tools itself, communities took a stand in creating opensource tools for mobile forensics. Although there are disadvantages regarding these tools such as the lack of technical support, this can allow users who are willing to learn to have a good starting point in this field and apply it further into the work environment.

The scope of this project is precisely that. The creation of a guide composed by mobile forensics Labs, for anyone who is willing to learn mobile forensics using Open-source tools and to be able to analyse essential artefacts such as: Internet browser, SMS, phone calls and logs, deleted files, GPS and social medias. With the creation of this guide, the hypothesis of how open-source mobile forensic tool can facilitate the learning process in this field, especially for beginners and people who interest in mobile forensics.

To do so, the aim of this research was split into the creation of a functional testbed that is composed by the user's choice of the type of hypervisor 1 or 2. In these hypervisors, users can install Windows 10 which will provide compatibility with Avilla Forensics and for comparison of results, Autopsy must also be installed.

For extracted data, a dataset was downloaded from NIST. This dataset is composed by data extracted from an Android phone, this was the chosen OS due to its popularity and growth in society compared to other OS.

There are some limitations that should be taken into consideration in the creation of a mobile forensics guide, such as the lack of framework to follow as the technologies are constantly evolving, the lack of tools to analyse other OS since Android and IOs are becoming the most popular. And it is also essential the required components recommended in this guide to perform the installation of the lab.

3.0 Literature review

The creation of guides for digital forensics has been an already research and discussed, therefore, the use of previous research will serve as a guide into the decision making of the methodology used in this project.

3.1 Creation of guides

The following papers in *table 6* were relevant in the decision making of how guides for mobile and digital forensics were created, the challenges met and outcomes.

Title/Reference	Method/Objective	Findings/Conclusions
EvilPlant: An Efficient digital forensics challenge creation, manipulation, and distribution solution (Mark Scanlon, January 2017).	Limitations on the creation and distribution of digital forensic challenges to students that are time consuming and costly. This requires a much more efficient way in distributing these images. Therefore, the authors created a web platform that allows the recreation and the easy distribution of digital forensic labs. These labs can have their data modify and the difficulty of level can be changed. This will also allow the users to share the challenges across the digital forensics community, provide scores and instant feedback to students.	• This method would eliminate plagiarism due to the ability of customize the challenges. It can also be applied to digital forensics investigators allowing them to be tested to for the same skills while working on different challenges. • Validation of tools. The ability to reconstruct the devices state by orderly integrating the packages into the base of device that were created on the previous snapshot of the device. • Reconstruction of the device for the analysis of Malware.
This research was beneficial as it allowed to set the initial idea of the structure of the testbed, such as the decision of using Proxmox for convenient access to the labs. In the use of this method in university environment, students would be able to login through SSH into Proxmox, which is composed with different types of labs with various levels of difficulties.		

Digital Forensics Lab Design: A Framework (Khushi Gupta, June 2022)	This research highlights the difficulties faced by educators and students regarding the creation and implementation of DF labs such as the costs of the hardware and software, the time-consumption spend in the creation of the lab files, the dynamic field making it hard to keep tool and labs updated. Students also use different OS which can have different or even tools with different settings and configuration procedures. This framework suggests the following lab documentation:	• Having a set framework and guidance for students will allow them to develop knowledge in the tools used, as well as the understanding of a digital forensics' investigation. • This research also adds the missing framework for the implementation of labs in the literature.
	• Lab Scenario – background story which acts as a starting point leading into the investigation. • Learning objectives – purpose of the lab • Estimated completion time – helps students pace themselves. • Tools used – overview of tools used which allows the users to collect the tools before starting the lab • Initial setup – lab environment, tools and configurations • Lab tasks and report writing • Feedback	
The development of a framework is essential it sets the standards for the creation of any STEM labs. The framework used will be an essential add-on to this project because it will establish a benchmark that can be followed during the implementation of this and any other future guides.		

Table 6 Literature review: Creation of guides for a mobile forensics investigation

3.2 Testbed

The testing environment is a crucial step as this will isolate the data being analysed from the host files. This ensures the integrity of the results. To do so, it is essential to build the testing environment using virtual machines. *Table 7* exemplifies how this was applied into previous research.

Title/Reference	Method/Objective	Findings/Conclusions

Computer Forensics Analysis in a Virtual Environment (Derek Bem, 2007)	This research's objective is to show the examination made on the VMWare application and how it differs from the host system, therefore VMWare by itself cannot produce court admissible evidence. The authors proposed a new approach involving two environments (Conventional and Virtual) that will be used simultaneously and independently. The author also explain how a virtual machine is a software that allows users to create different environments which	The authors concluded that the cooperation between both professionals would speed up the investigation time and achieve faster results. Having computer technicians conduct the initial investigations on a virtual machine will also keep the real evidences from being compromised in case of any mistakes. The authors end this research by stating that using a virtual machine to conduct an
	are composed by simulated set of hardware and even software. These environments can be controlled independently although they require additional resources from the host machine, plus these types of software are complex and therefore come with limitations. This research also proposes that two types of computer personnel should be used to conduct a forensic investigation: Computer technician that will deal with the VM and a copy of the original Forensic Image which will then report any findings to the Professional investigator.	investigation can also serve as initial training,. A person with little computer forensics experience is not immediately given all the responsibilities of a fully trained Investigator, but they will be introduced to the process in an environment that will not compromise evidence and the case.
Using this research to point out the benefits of the virtualization environment and how they can be applied to training. It also provides a clear understanding of how a virtual machine is composed and the main differences of how the investigations are conducted in the virtual machine versus how they are conducted in the protected copy of the evidence.		

Table 7 Literature review: Virtual machines what are they and benefits of using for digital forensics investigations

3.3 Chosen OS

It is essential to define which operating system of the mobile device was to be analysed, as seen in the research in *table 8*, these require specific tools for specific Operating Systems.

Title/Reference	Method/Objective	Findings/Conclusions

A Novel Framework for Mobile Forensics Investigation Process (Mohammed Moreb, March 2023)	According to this research, Android is the most popular OS while iOS is considered the second most popular. (Mohammed Moreb, March 2023) has developed a new methodology framework which integrated all the needed steps and data sources in order to construct a crime case. This framework aims to retrieve data commonly found in devices such as call logs, SMS, GPS, app data and stored files.	Provides a comprehensive framework applied to Android mobile devices that includes guidance on how to perform the analysis on an Android phone.
This research stresses that Android is one of the most popular OS chosen by consumers. Therefore, it has a user base and higher chances of crimes being committed through the use of Android. **(Mohammed Moreb, March 2023)** also points out the base evidence that can be found while analysing an Android device, which will also be analysed in this project.		

Table 8 Literature review: Popularity of the Android Operating System

3.4 Current Open-source Mobile Forensics software

The research in *table 9* was used as a guide for a better understanding of the differences between open-source and commercial tools.

Title/Reference	Method/Objective	Findings/Conclusions
Comparative Analysis of Commercial and Open-Source Mobile Device Forensic Tools (Radhika Padmanabhan, March 2017)	This study aims to find out if opensource tools have the capability of replacing commercial forensic tools. Based on the following parameters: functionality, usability, cost, support, compatibility and reliability, the authors analyse 2 commercial and 2 open-source tools to determine the best tool for a forensic investigator	This research concludes that opensource have more prominent features such as the creation of an environment where users can easily share resources, these tools also offer the flexibility of working with either a GUI or the command line. However, commercial tools are much quicker and accurate during the extraction and analysis of data. The author also states that these are the two characters that mostly separates open-source and commercial tools, that in the future there will be shifting towards the use of open-source tools.
This research has help for a better understanding of how essential Open-source tools are and the main differences between them and commercial tools.		

Table 9 Literature review: Open-source tools vs Commercial tools in mobile forensics

There is an immense diversity of mobile devices that operate on various operating systems such as iOS, Android, Blackberry and Windows. Due to this diversity, this research will focus on devices running Android. Comparing these devices with iOS, they are often found to be more affordable and more popular, making these devices the main source for malicious activities. According to (Hoog, July 2011), the widespread usage of Android in tablets and smartphones will eventually lead to the use of this OS in cars, televisions, GPS units, game consoles, and even netbooks. As a result, Android will very certainly be discovered in forensics investigations more often than any other type of OS.

Table 10 lists the open-source mobile forensics tools available for Android, the operating systems on which they run on, the different types of results the user can obtain, and a download link of the software.

Software	Environment	Features	Link
Sleuth Kit (TSK)	• Windows • Unix	• Uses command-line instructions.	https://www.sleuthkit.org/sleuthkit/ download.php
Autopsy	• Linux • OS X • Windows	• GUI version of TSK • Timeline analysis • Hash Filtering • Web Artifacts and Data Carving	https://www.autopsy.com/downloa d/
FTK Imager	• Windows • Linux	• Fast scanning and processing of data to • identify evidence Friendly GUI	https://www.exterro.com/ftk-imager
AndroGuard	• Windows • Linux • OSX	• Python based tool • Reverse engineering on Android apps • .apk file analysis which allows for malware and vulnerabilities can be done	https://github.com/androguard/andr oguard
Oxygen Forensics Viewer	• Windows	• Open-source version of Oxygen • Forensics Detective Used to view and analyse device data deleted and recovered through Oxygen Forensics Detective	https://www.oxygenforensic.com/en/products/freeviewer

Avilla Forensics	• Windows	• Both Android and iOS • Friendly GUI • Data extraction from WhatsApp, Messenger, Twitter, Instagram, Web browsers and Geolocation	https://github.com/AvillaDaniel/Avill aForensics

Table 10 Examples of open-source software and types of environments that they run on (Avilla, N.D), (Forensics, May 2020), (Infosec, April 2018), (PhoenixTS, January 2016) and (Carrier, N.D)

4.0 Methodology

This research consists in the process of creating an instructional material in which it targets a specific audience such as digital forensic student or layman with interest in exploring the field of mobile forensics using open-source tools. After careful consideration, it was determined that ADDIE (Analysis, Design, Development, Implementation and Evaluation) methodology would be the best choice to apply to this research.

According to (Quigley, N.D) ADDIE divides into 5 essential steps:

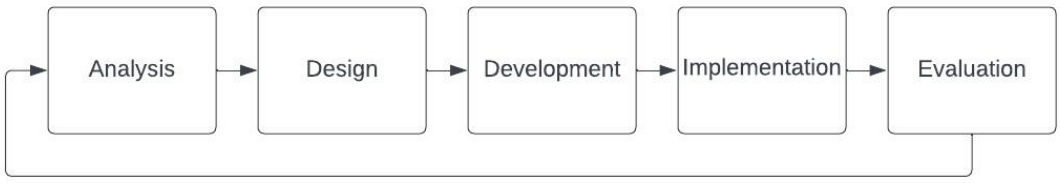


Figure 5 ADDIE methodology

4.1 Analysis

The current situation must be analysed in order to understand the goal of the research and to fill any existing gaps in the previous research and training. Questions such as "How to improve the situation and achieve goals through training?" is the main foundation for the rest of the process (Quigley, N.D). As such, this research has achieved this step with the research seen above, where it was stated that a lack of resources is provided in order to train future mobile forensics investigators, but also, the high cost of commercial tools. Therefore, training could be achieved with open-source tools.

4.2 Design and development

In this stage, it is essential to establish a structure which will apply all the knowledge from the previous sections in order to create a prototype of the guide. The remainder of this research will also adhere to this structure.

Storyboard one

The first storyboard *(Table 11)* explains the approach taken in the decision of the hypervisors for the virtualization environment.

Goal
The first goal is to define the hypervisor to be used by the users.
Approach
Based on the user's components and needs, users must pick between the hypervisor type 1 or hypervisor type 2.
Platforms
• Proxmox as hypervisor type 1 • VirtualBox as hypervisor type 2
Course outline
Users will be guided through the installation of box types of hypervisors
Learning objective
• To understand the differences between the hypervisors and the different utilities • To understand why an isolated environment is needed when conducting forensic investigations and tool testing

Table 11 Hypervisors

Storyboard two

Hypervisors will then require the installation of Operating Systems. *Table 12* takes on the method used in this guide for the installation of the chosen OS.

Goal
Installation of Windows 10
Approach
The operating system will be individually installed in the previously chosen hypervisor
Platforms
• Windows 10

Course outline
Users will be guided through the installation of the chosen OS
Learning objective
• Due to its popularity, Users will be comfortably using a familiar OS to perform an investigation, which already requires a huge learning curve.

Table 12 Operating System

Storyboard three

Table 13 provides the outcomes of the tool section and a brief explanation of what data each tools will be analysing.

Goal
Decision of tools to be able to analyse the dataset in both operating systems
Approach
Each tool will be used by the user depending on what type of data will be analysed
Platforms
• Autopsy will be used to analyse call logs, SMS, deleted files, media such as images, E-mail. • Avilla Forensics will be used to analyse the same data as above
Course outline
Users will be guided through all steps on the analyses in all tools referenced above.
Learning objective
• Using different types of tools will help users become more versatile and increase their tool expertise • It will also help users in understanding how to use dual verification to match results

Table 13 Tools

Storyboard four

It is also essential to establish where the data will be provided from. Therefore, *table 14* gives a brief overview on where to retrieve this and the process taken to convert this data for further analysis.

Goal
Deciding the Dataset
Approach

Using NIST, it is essential to decided which dataset would be used as good example for this guide. Although, there are a lack of datasets composed with recent Android devices, for the purpose of this guide a HTCH Desire 626 dataset was used.
Platforms
• https://cfreds.nist.gov/ was used to download the chosen dataset
Course outline
Users will be guided on how to search for datasets, how to download them and extract them, and how to import them into the tools
Learning objective
• Gained knowledge on the different types of datasets in NIST

Table 14 Dataset

5.0 Implementation

The objectives and the essential criteria have now been established; therefore, the mobile forensic investigation can begin. To do so, the user must start with the installation of the hypervisors that will cater the user's needs and components. As such, this section is divided into two subchapters, where a step-by-step guide for both installations can be followed.

5.1 Hypervisors

Hypervisors are vital for the virtualization of environments, knowing the differences between hypervisors can help the user understand which fits their needs. (Vissarion Yfantis, April 2020) explains that hypervisors provide two major features such as partitioning, which allows independent software payloads to run at the same time on the same hardware, but also resource distribution. (Vissarion Yfantis, April 2020) also explains that there are two types of hypervisors:

- **Type 1/Bare-metal/Native Hypervisor:** The software of the hypervisors is directly installed in the Host's hardware. The advantages of this type of hypervisors are the scalability, optimization of physical resources since there are no other software interfering and better allocation of resources. These hypervisors are usually used in enterprises and for large-scale deployments.
- **Type 2/Embedded/Hosted hypervisors:** An application that is built into the host's operating system. This type of hypervisor is easy to step up, although due to its dependency on the OS, if this crashes, then the hypervisor will also crash.

The installation of the preferred hypervisor will be dependent on the user's needs and hardware. Therefore, the following sections will be a guide on the installation of both hypervisors.

VirtualBox

According to (Oracle, N.D) VirtualBox is one of the most popular open-source virtualization software. It allows the reduction of IT costs as it also reduces the number of required desktop and server configurations. It also supports a wide variety of operating system such as Windows, Linux and MacOS, making this hypervisor compatible with most workstation.

Download and Installation of VirtualBox

Users must download the correct installation file according to the host machine.

1. To download the file, users must open a web browser and open https://www.virtualbox.org/wiki/Downloads
2. Double clicking on the file will launch the VirtualBox setup
3. In the custom setup screen, users must select the location where they wish to install VirtualBox in
4. During the network interfaces, this setup will install a virtual network adapter.
5. VirtualBox will begin to install

Proxmox VE

Proxmox VE is an open-source server management platform applied to business virtualization. It integrates Linux containers, networking, and many other features into one platform. These containers and virtual machines are easy to manage but there also disaster recovery tools built-into the platform.

Proxmox was the preferred hypervisor software for this research as according to (Crull, January 2022) Proxmox is one of the most popular ways to achieve virtualization, as it is completely free to use, and it is user friendly. A subscription can also be purchased which provides with tech help and other features, although, Proxmox free version will run everything that is necessary.

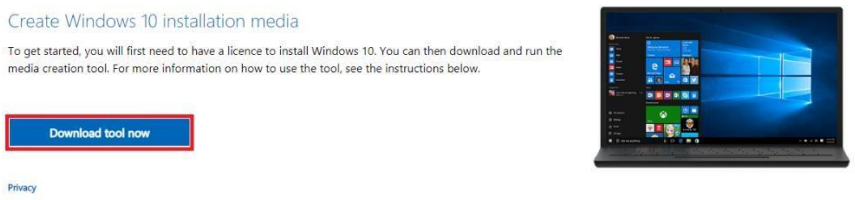
Download and installation of Proxmox

Steps taken for the installation of Proxmox:

1. Proxmox VE ISO must be downloaded from the website: https://www.proxmox.com/en/downloads
2. ISO must then burn into a CD/DVD or a bootable USB flash drive must be created using the Rufus tool
3. The USB drive must be plugged into the host/server desired for the installation of Proxmox.
4. The installation should automatically start, although if that is not the case, the boot order in the BIOS must be changed.
5. During the installation, it is necessary to create a root password.
6. Once the installation is complete, Proxmox can be accessed through another computer by entering the IP address of the server into the web browser

5.2 Operating system: Windows 10

Having the hypervisors installed, downloading the Windows 10 ISO is a simple and quick process. *Table 15* provides all the steps taken from the download of the media creation tool and the download of the Windows 10 ISO.

Step 1. Download of the media creation tool	To download the ISO, users must first download the media creation tool, this can be found in the following link: *https://www.microsoft.com/en-gb/softwaredownload/windows10*
	

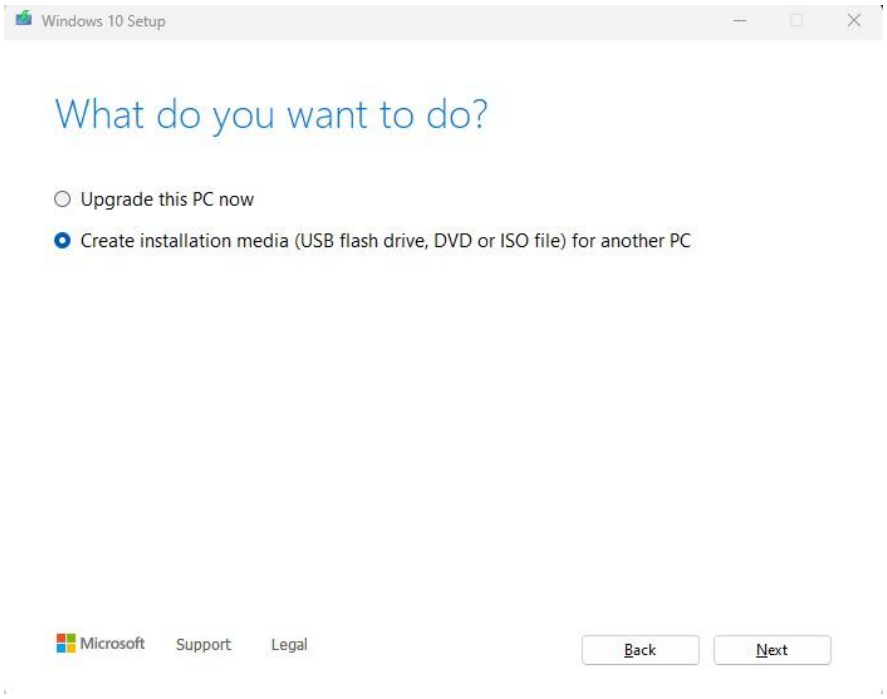
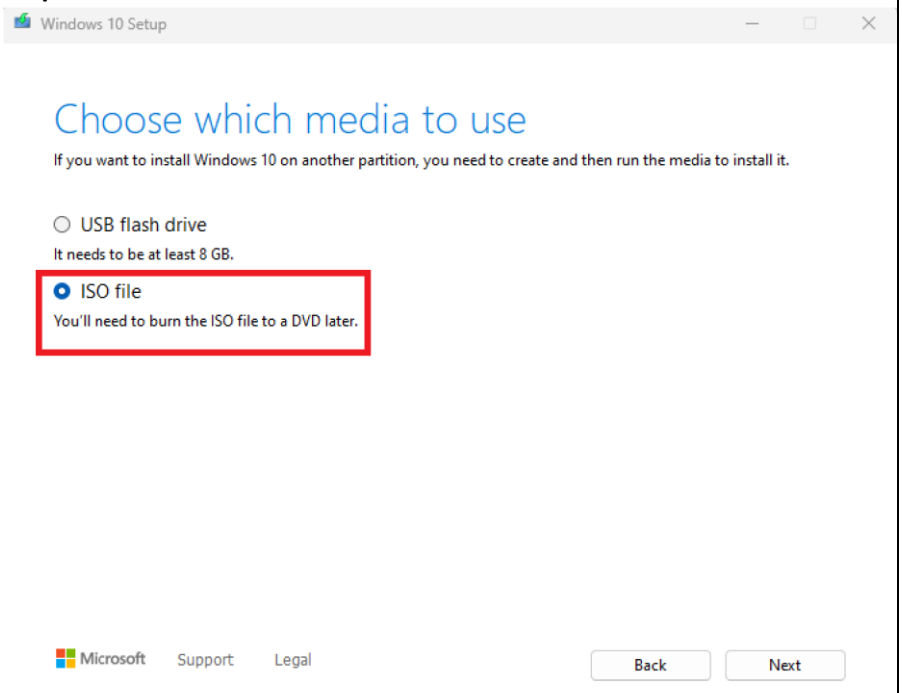
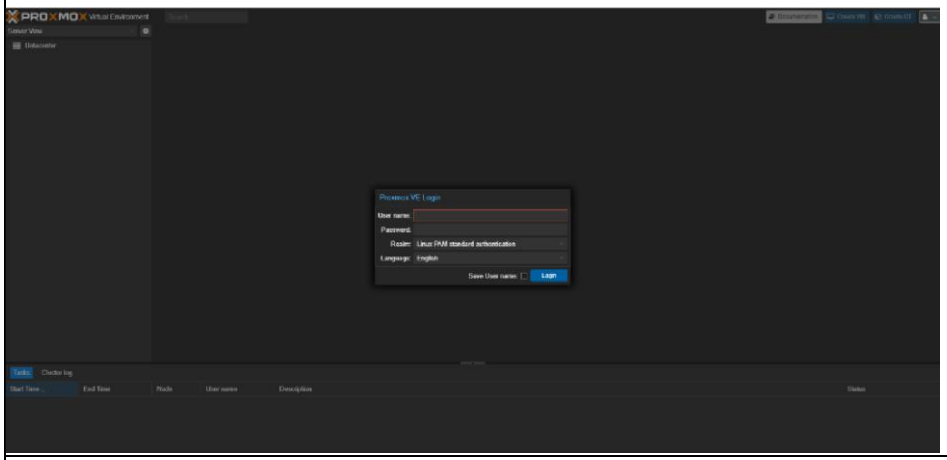
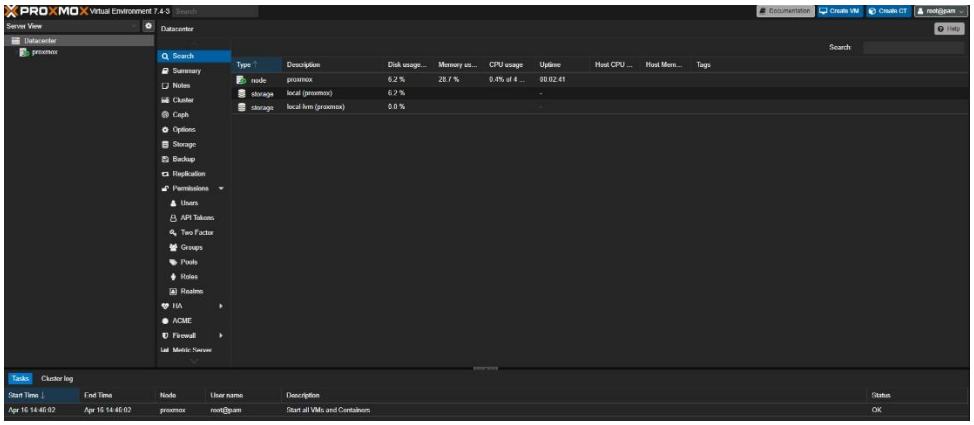
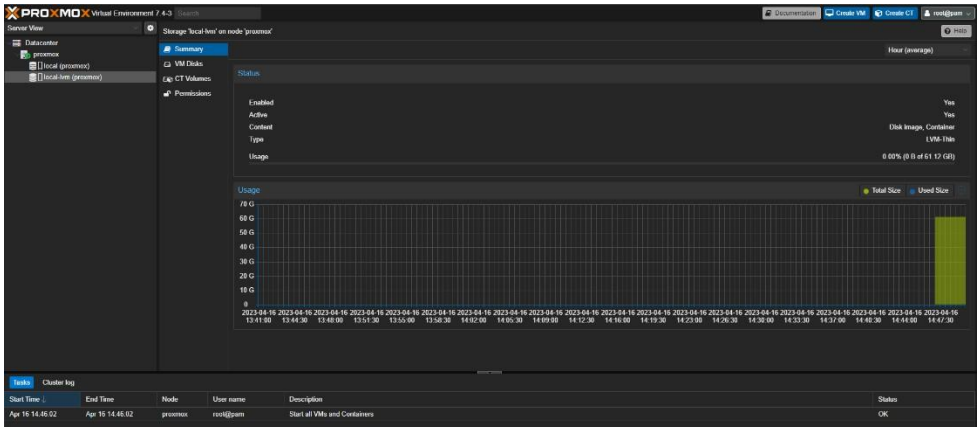
Step 2 Creating installation media 	Virtual Machines require the ISO file, thus, users must select the second option to enable the download of the ISO.
Step 3 Download of the ISO 	The download will begin, and the ISO will be available for import in the Virtual Machines.

Table 15 Download of Windows 10 ISO

Windows 10 installation in Proxmox

Step 1 login 	Using a web browser, the user must log-in into Proxmox using the IP address setup during the installation phase, the username: **root** and the password created during the installation.
 **Step 2 Overview of Proxmox initial page**	

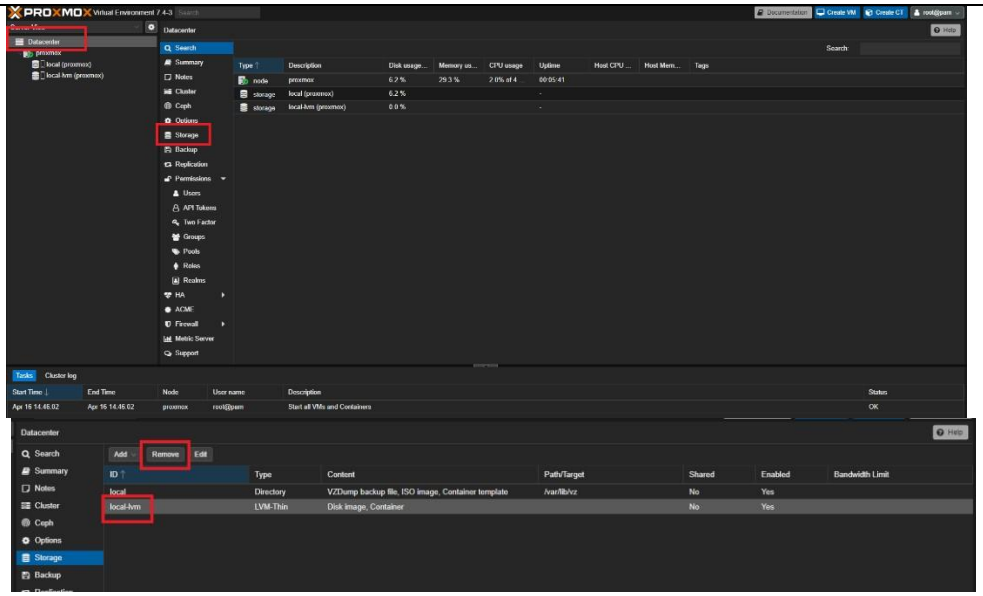


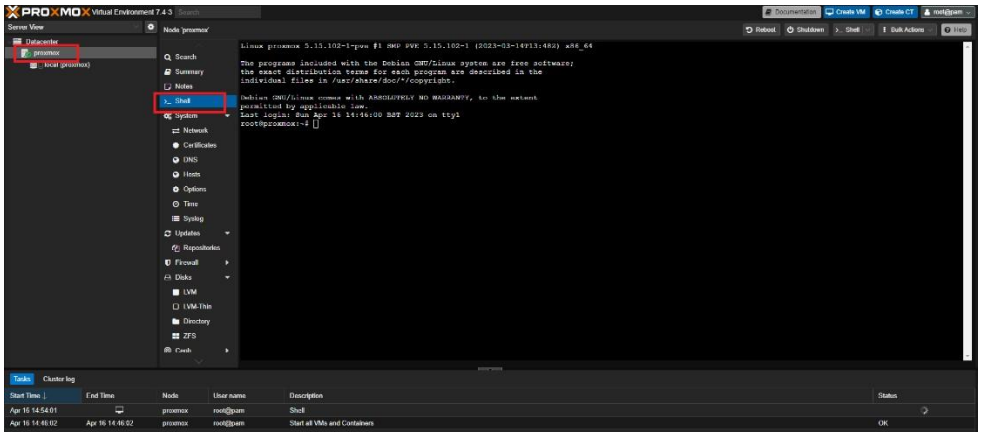
Step 3. Deleting local-lvm to allocate more space

As seen, local-lvm is using 61GB. This can be deleted to allocate more space into the local partition.

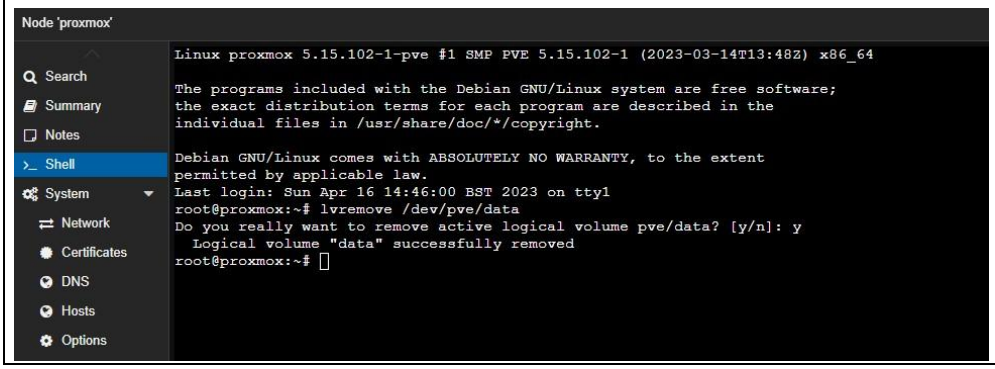
Step 4. Storage

In storage, users can delete the local-lvm.





Step 5. Using Shell to allocate the extra space



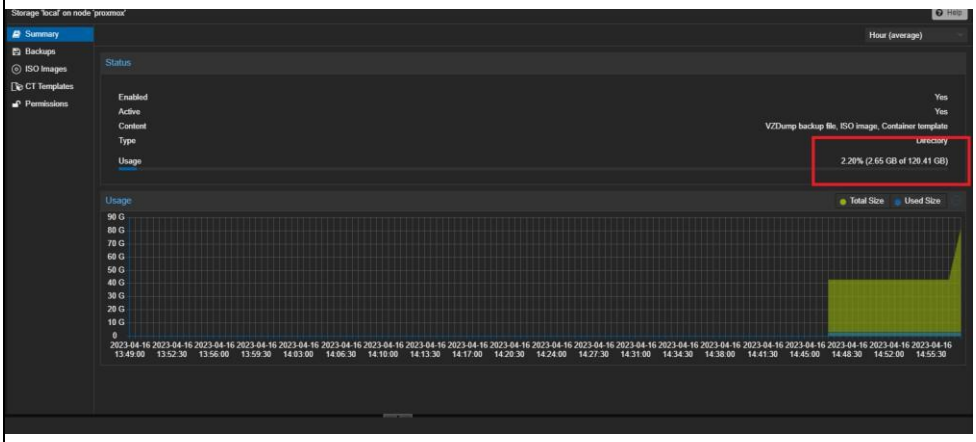
Using the shell command users must input the 3 following commands:

1. *lvremove /dev/pve/data* this will completely remove the local-lvm so that the space can be allocated to the local drive
2. *lveresize -l +100%FREE /dev/pve/root* this command will resize the local partition
3. *resize2fs /dev/mapper/pveroot this command will ingrate the allocate space into the newly resize partition.*

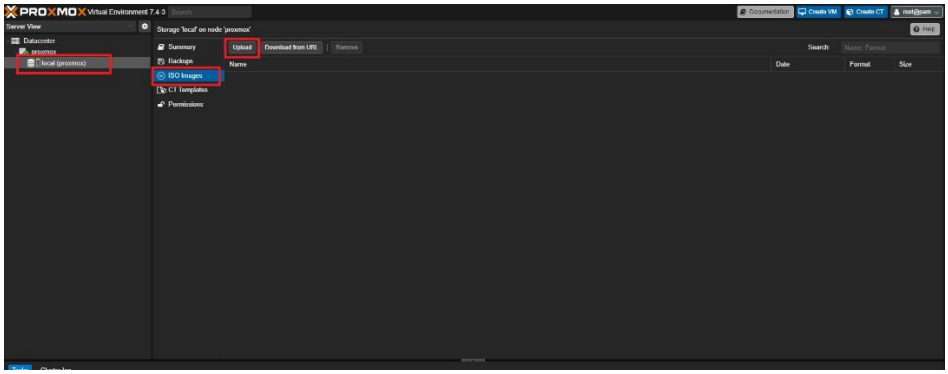
```
root@proxmox:~# lvresize -l +100%FREE /dev/pve/root
  Size of logical volume pve/root changed from 40.56 GiB (10384 extents) to <114.24 GiB (29245 extents).
  Logical volume pve/root successfully resized.
root@proxmox:~#
```

```
root@proxmox:~# resize2fs /dev/mapper/pve-root
resize2fs 1.46.5 (30-Dec-2021)
Filesystem at /dev/mapper/pve-root is mounted on /; on-line resizing required
old_desc_blocks = 6, new_desc_blocks = 15
The filesystem on /dev/mapper/pve-root is now 29946880 (4k) blocks long.

root@proxmox:~#
```

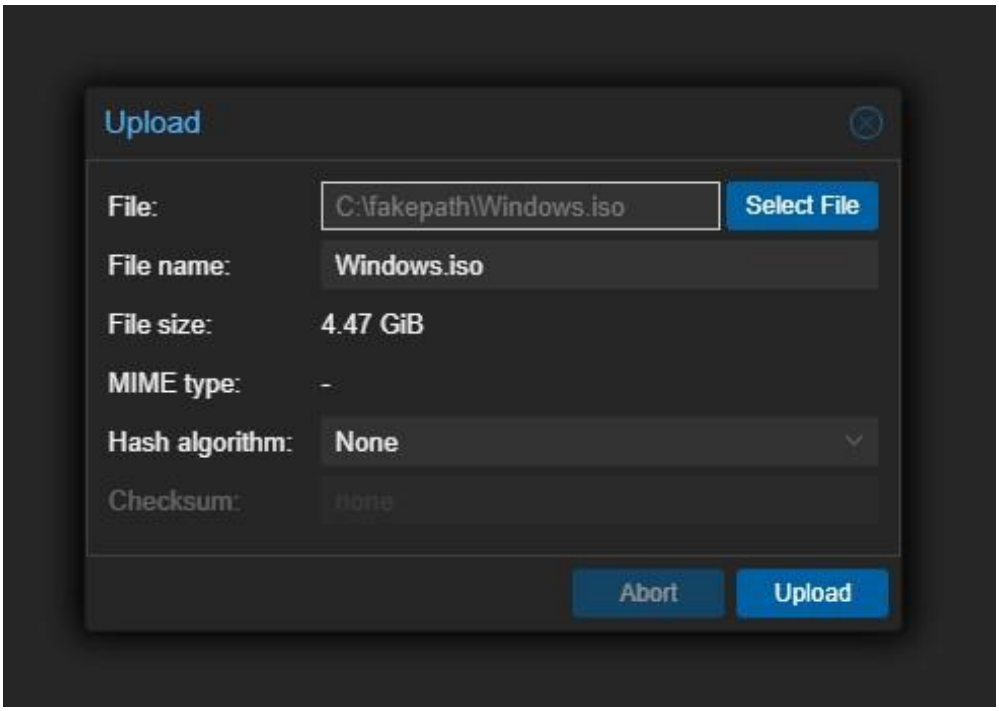


As seen in the last image, the space in local has now increased

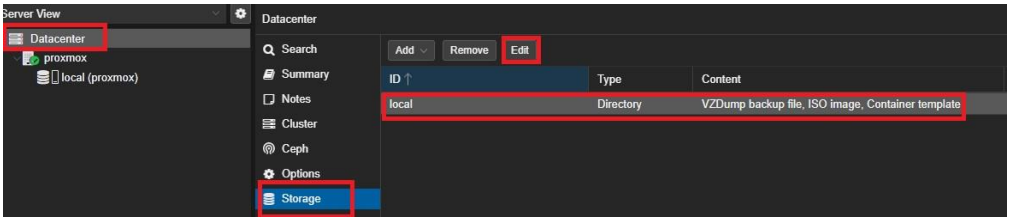


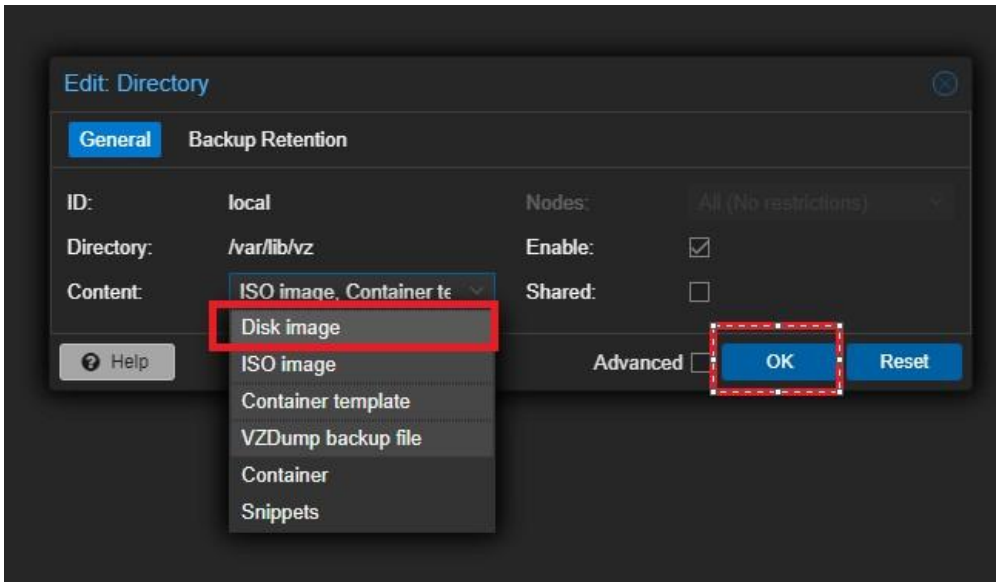
Step 6. Importing ISO

The ISO of the desired virtual machine now needs to imported into Proxmox


Upload
File:
C:\fakepath\Windows.iso
Select File
File name:
Windows.iso
File size:
4.47 GiB
MIME type:
-
Hash algorithm:
None
Checksum:
Abort
Upload

Step 7. Specify the type of content that can be allowed in the directory



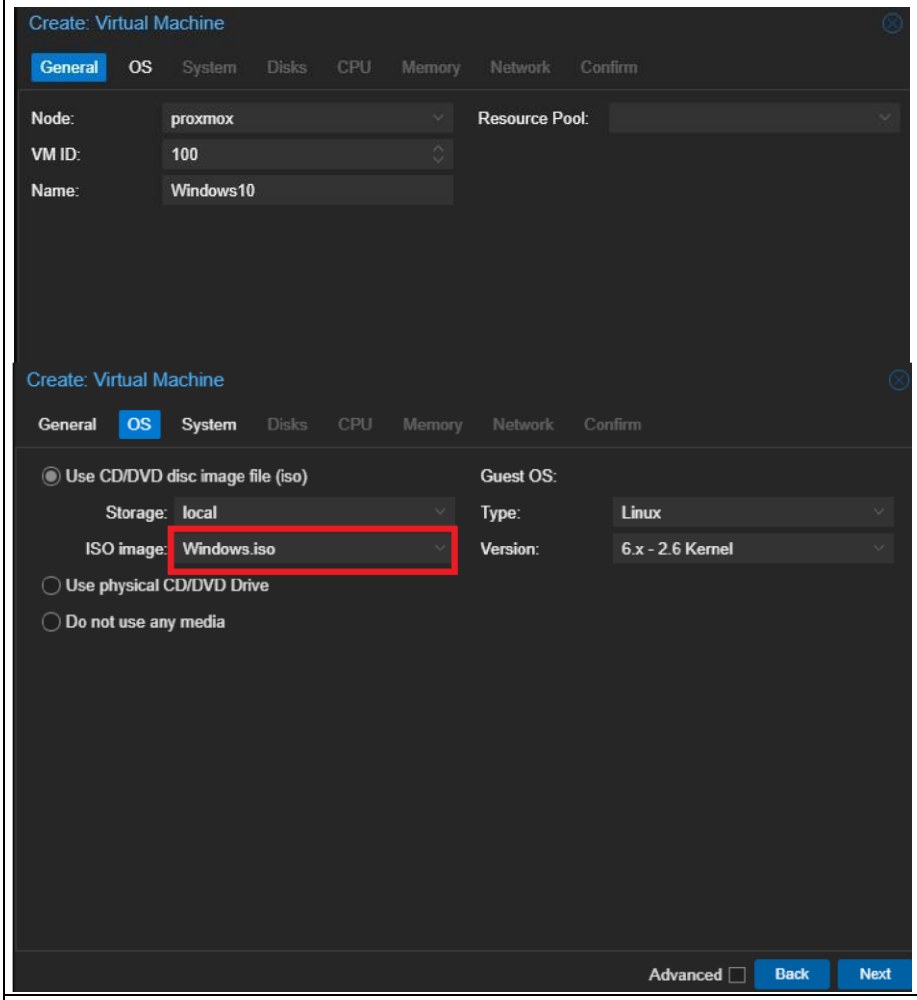


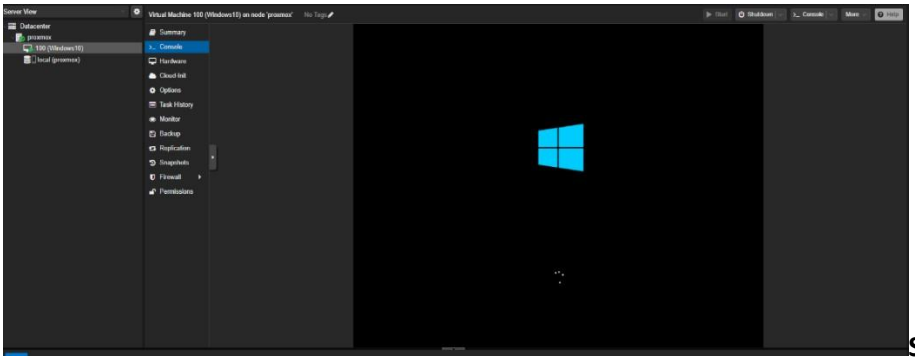
This step is crucial in order to be able to create the virtual machine.

Creating Virtual Machine

Step 8.

Follow the steps to create the virtual machine





Step 9

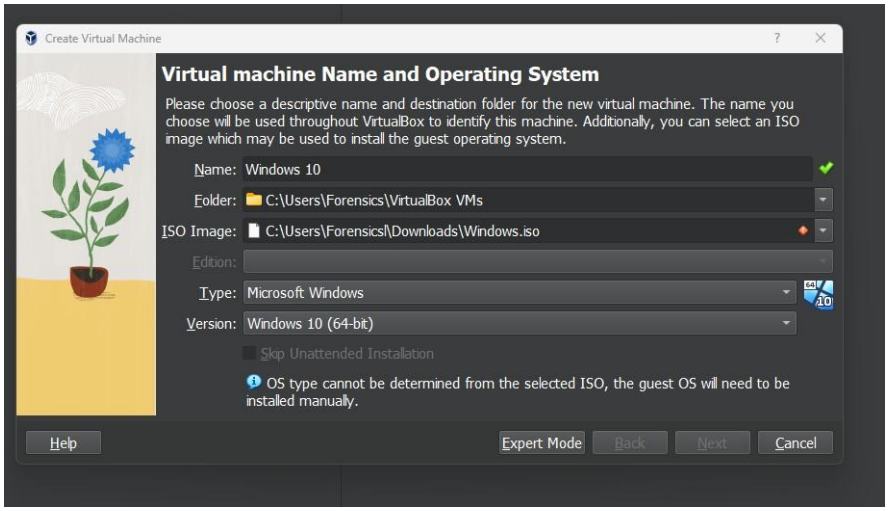
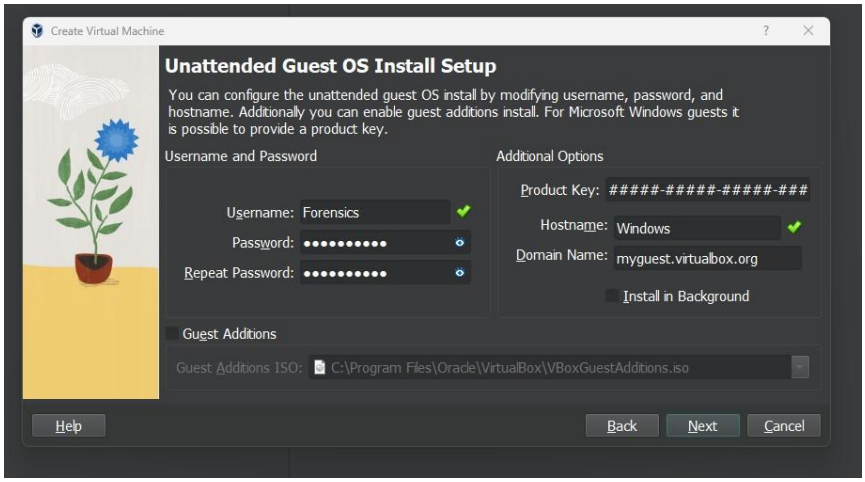
Windows 10 Virtual Machine

Windows 10 will begin the installation and user must follow the steps. Installation of the tools and dataset can be found under section 6.2, 7.0 and 8.0

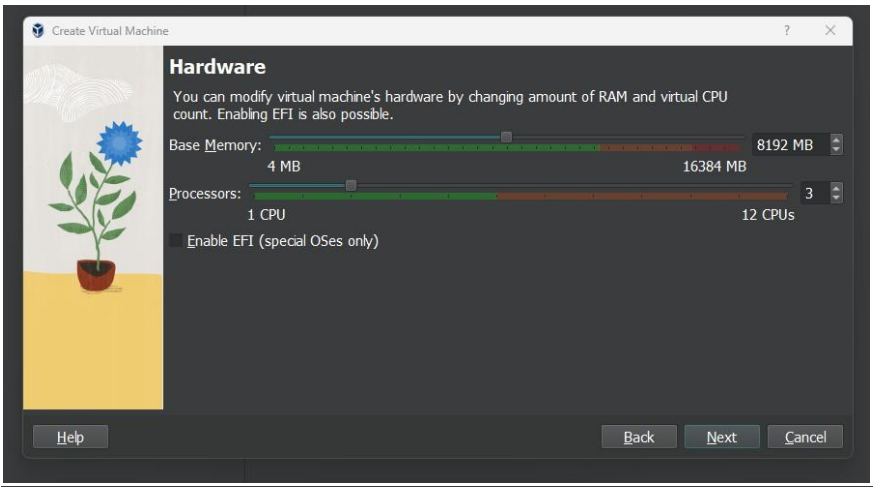
Table 16 Installation of WIndows 10 in Proxmox

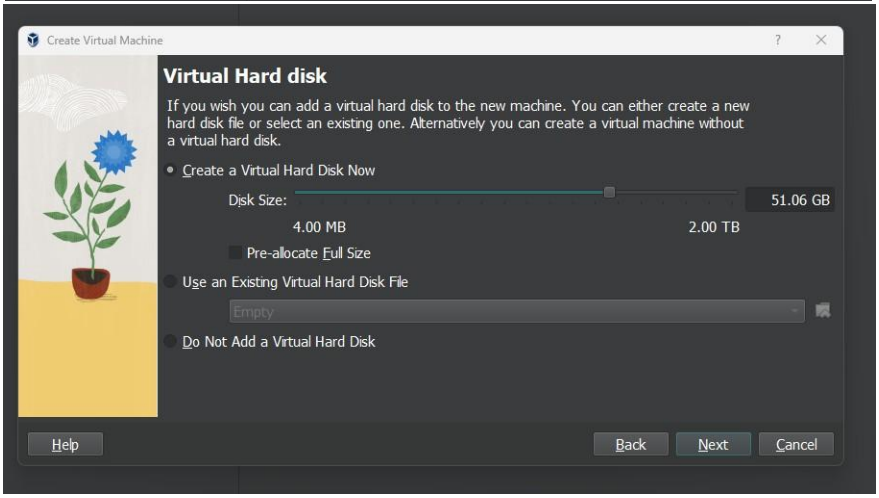
Windows 10 Installation in VirtualBox

In VirtualBox the installation of Windows 10 is quite similar. *Table 17* shows the steps taken for the installation of the operating system in VirtualBox.

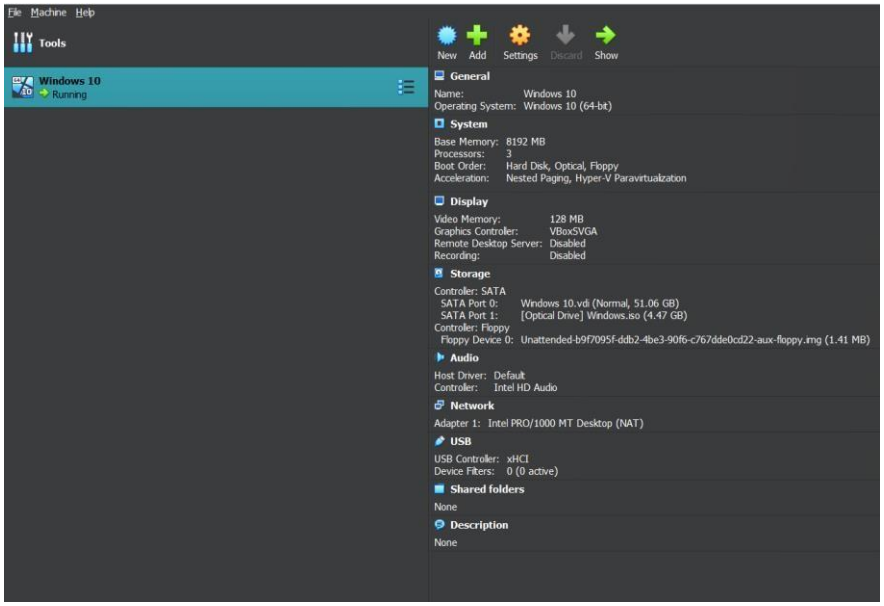
Step 1. Overview of VirtualBox 	By clicking on "New", this will begin the process of installing a brand-new virtual machine in the system
Step 2. Selecting the ISO 	The correct ISO image, in this case Windows 10, must be imported.
Step 3. Creating password 	The guest must be configured in order to proceed with the installation. Therefore, a new password and username must be created. It is also recommended to change the Hostname so that the installation can proceed.

Step 4. Hardware	It is essential to select the correct amount of RAM divided between the host machine and the virtual machine, as well as the CPU. This will determine the speed of the virtual machine. Regarding the Hard drive, this must be enough to allocate the Operating System, tools and any desired datasets.





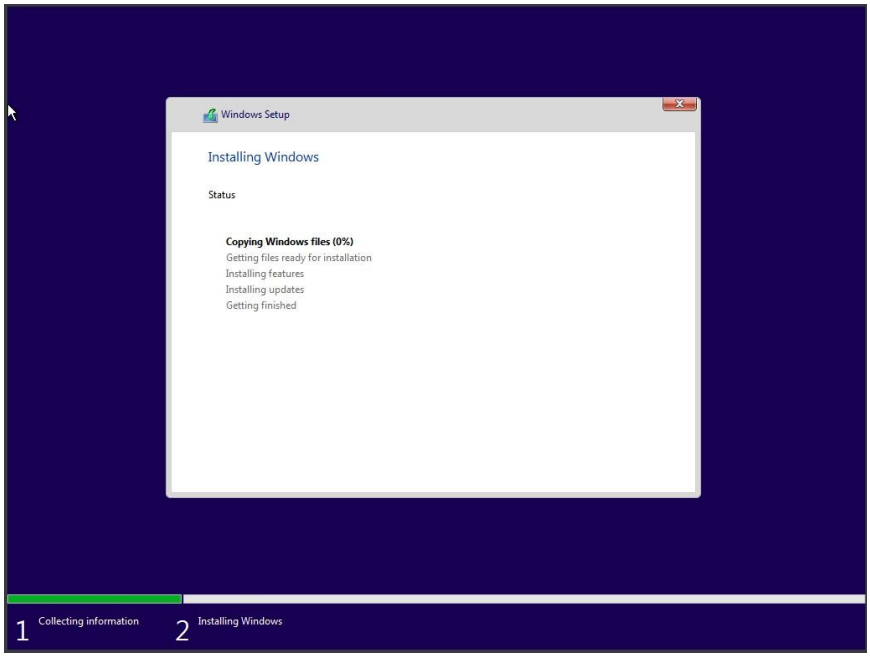
Step 5. Virtual Machines



As seen, the virtual machine was created. The user can see the specs of the VM and can even alter it. Windows 10 should automatically launch and the installation will begin.

Step 6. Installing Windows

To install Windows 10, users will have to follow the instructions presented on the screen. Windows allows users to use an



inactivated Window 10 without any sort of restrictions for one month after the installation. Therefore, users looking to only experiment mobile forensics in a Windows 10 Virtual Machine can do so even without the activation key, although for only one month.

Step 7. Installation of tools	Now that Windows is installed, the tools and the dataset must be downloaded from the respective websites. This is explained in the following sections: 6.2, 7.0 and 8.0.

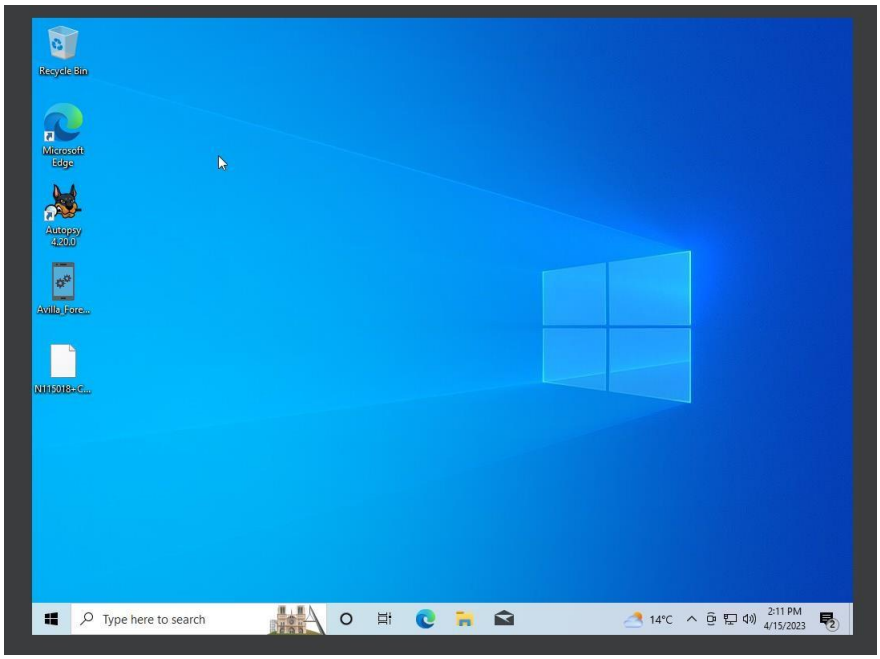


Table 17 Installation of Windows 10 in VirtualBox

6.0 Data

6.1 Android file system hierarchy

According to (Satish Bommisetty, July 2014) knowing the android file hierarchy can assist the investigator to narrow down the investigation into specific folders. This is because Android uses Linux kernel, and it is also split into several partitions *(Figure 6).*

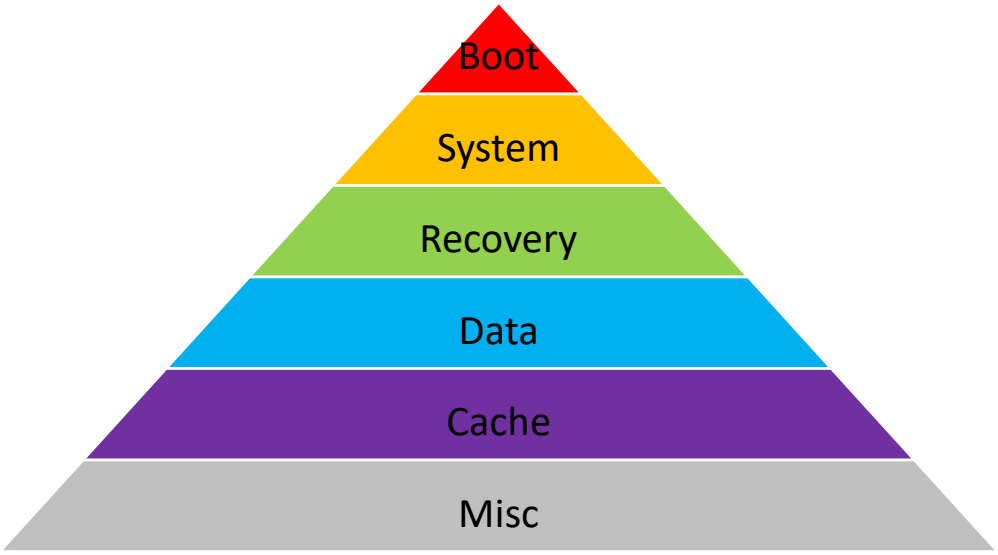


Figure 6 Android File System hierarchy

(Satish Bommisetty, July 2014) further explains each partition:

- **Boot**: This partition contains essential information and files that allow the phone to boot. It contains data such as Kernel information and RAM. Capturing RAM can be essential for the investigation as according to (Forensics, N.D) it can contain any programs running on the system, network connections, evidence of malware, registry hives, usernames and passwords, decrypted files and keys.
- **System**: Since this folder also contains system-related information, it should never be deleted as this will make the device unbootable.
- **Recovery**: A folder that contains backup information that allows the device to boot into recovery mode.
- **Data**: This folder contains mostly data related to the user activity such as contacts, SMS, dialled numbers, images, videos.
- **Cache:** Stores frequently accessed data. This is also essential for an investigation, as in this partition, data that can no longer be found in the data partition may be found in here. As an example, cache is used to store contents from a website or even programmes.
- **Misc:** Miscellaneous settings can be found in this folder. Stores information such as state of the device, hardware settings, USB settings.

6.2 NIST Dataset

NIST (*Figure 7*) provides a collection of datasets that are publicly available and can be used for tool testing and research purposes. These datasets can vary depending on the need of the user, there are datasets related to cyber security, malware investigation, digital forensics and even hacking cases. These datasets can be found under https://cfreds.nist.gov/.

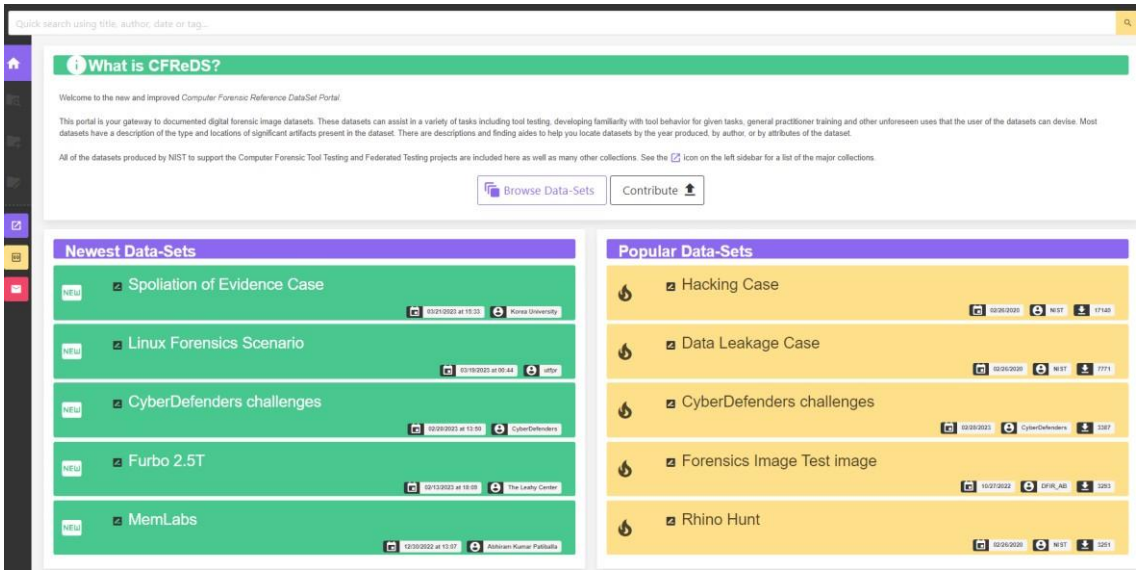


Figure 7 NIST main page

To conduct a mobile forensics investigation, users can simply search for mobile devices images and download a file of their choice. In this case, an image of an HTC Desire 626s was downloaded. This device image was the results of a chip-off extraction. As explained above, a chip-off extraction is the extraction of data directly through the memory and then its contents are turned into Forensics images.

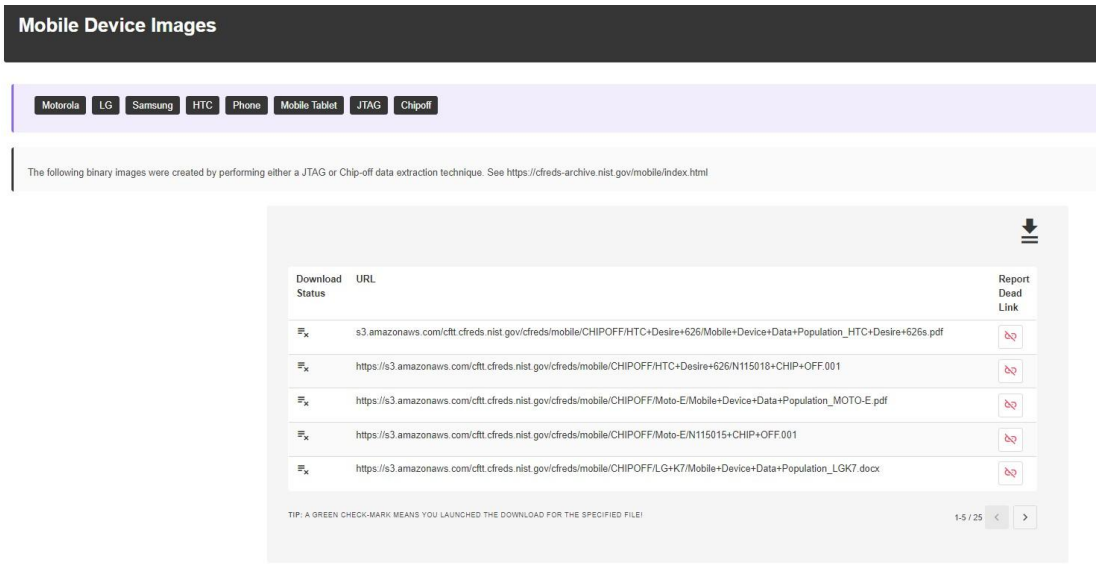


Figure 8 Mobile device images: https://cfreds.nist.gov/all/NIST/MobileDeviceImages

Data found in HTC Desire 626s Image

Users can find a .pdf file (*Figure 9*) related to the HTC 626s image that can be used at the end of the investigation. This is pdf file provides information on the type of data that can be found

such as the device model, IMEI and IMSI, contacts, SMS, call logs, deleted entries, e-mails and attachments, web history and apps (Facebook, LinkedIn, Instagram).

Appendix A – Mobile Device Population Data

Appendix A – contains an example/template of a dataset used for populating the internal memory of a mobile device. The format contains data element categories and sub-categories within each root data element.

HTC Desire 626s
IMEI: 352678079162076
ICCID: 8901260472997564858
IMSI: 31060479756485
Phone Number: 15868232570

Handset Internal Memory:

<Address Book>

<Long Name (50 chars), Mobile Number>

John Jacob Jingle Heimer Schmidt That's My Name Too Whenever I Go Out The People Always Shout John Jacob Jingle Heimer Schmidt
, 8988675309

<Regular Name, Mobile Number, email, website, picture>

Jimi Hendrix, 7691234560, hendrix@experienced.com, website: www.jimihendrix.com

<Special Character Name, Home Number>

*, 8887771212

<Blank Name, Work Number>

, 8785551111

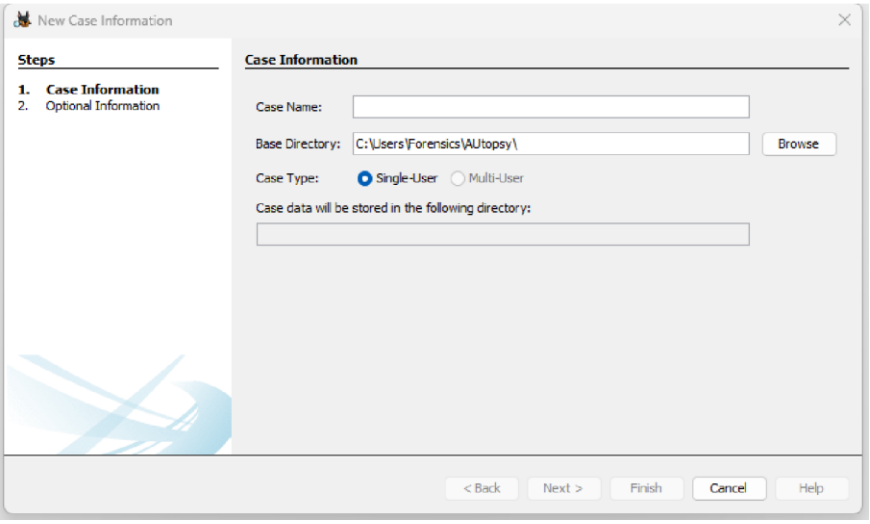
Figure 9 Example of data provided in the PDF file of the HTC dataset

7.0 Autopsy

Autopsy is a very popular digital forensics open-source tool. It is also the graphical version of The Sleuth Kit, a tool that is often used in other open-source software. This tool has a friendly interface, and it is also used by law enforcement, corporate examiners and even the military. In this research, Autopsy was used in conjunction with SQLite to analyse databases such as the contacts database. Users can download this tool by following the link: *https://www.autopsy.com/download/*

7.1 Import NIST dataset into Autopsy

Table 18 was created to aid in the guidance of each step on how to import the NIST dataset for further analysis.

Step 1. The case 	Once Autopsy is launched, users will be able to decide between creating a new or opening a case that was already imported into autopsy.
Step 2. Case Information 	As this is the first time importing the extracted data, a new case must be created, and case information is required.

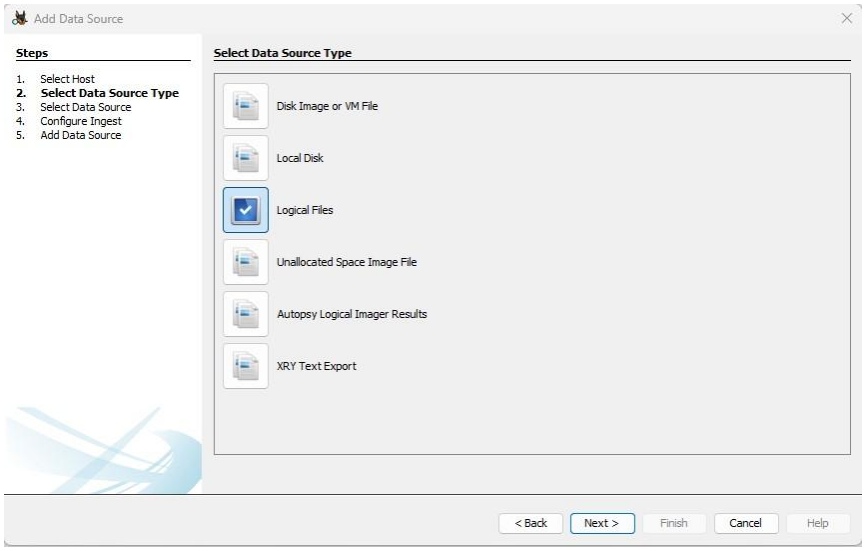
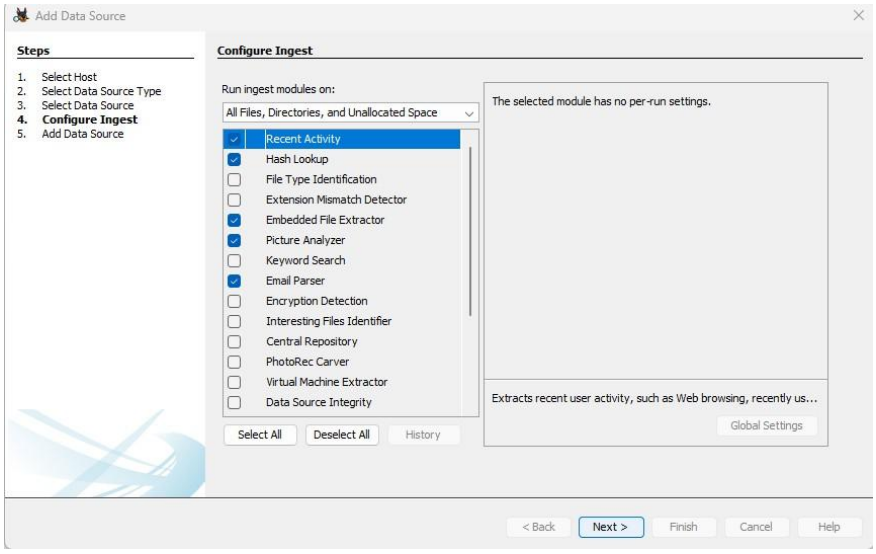
Step 3. Data source type 	**Disk image or VM File –** used to analyse data obtained from a sector-by-sector copy of the local disk or even data extracted from a virtual machine **Local Disk –** Local drive can be analysed without having a copy of it made. Must be attached through a USB and a write blocker. **Logical files –** Files or folders in the local machine. Use to analyse a collection of files **Unallocated Spaced Image File –** Autopsy can analyse unallocated space, useful in the search for deleted files **Autopsy logical Imager results** – extracts data and creates a Forensic image of the logical files in a storage device **XRY Text Export –** Used to extract data from mobile devices
Step 4. 	After selecting the correct data source, in this case the Logical file, and selecting the dataset for analysis, it is essential to configure the correct ingest. As this will determine the time that autopsy will take to analyse the data.
Step 5. Autopsy will begin to import all data. It is essential to let the ingest run and only begin the investigation once all data has been imported to not miss any crucial information.	

Table 18 Steps on how to import the NIST dataset into Autopsy

7.2 Tool Layout

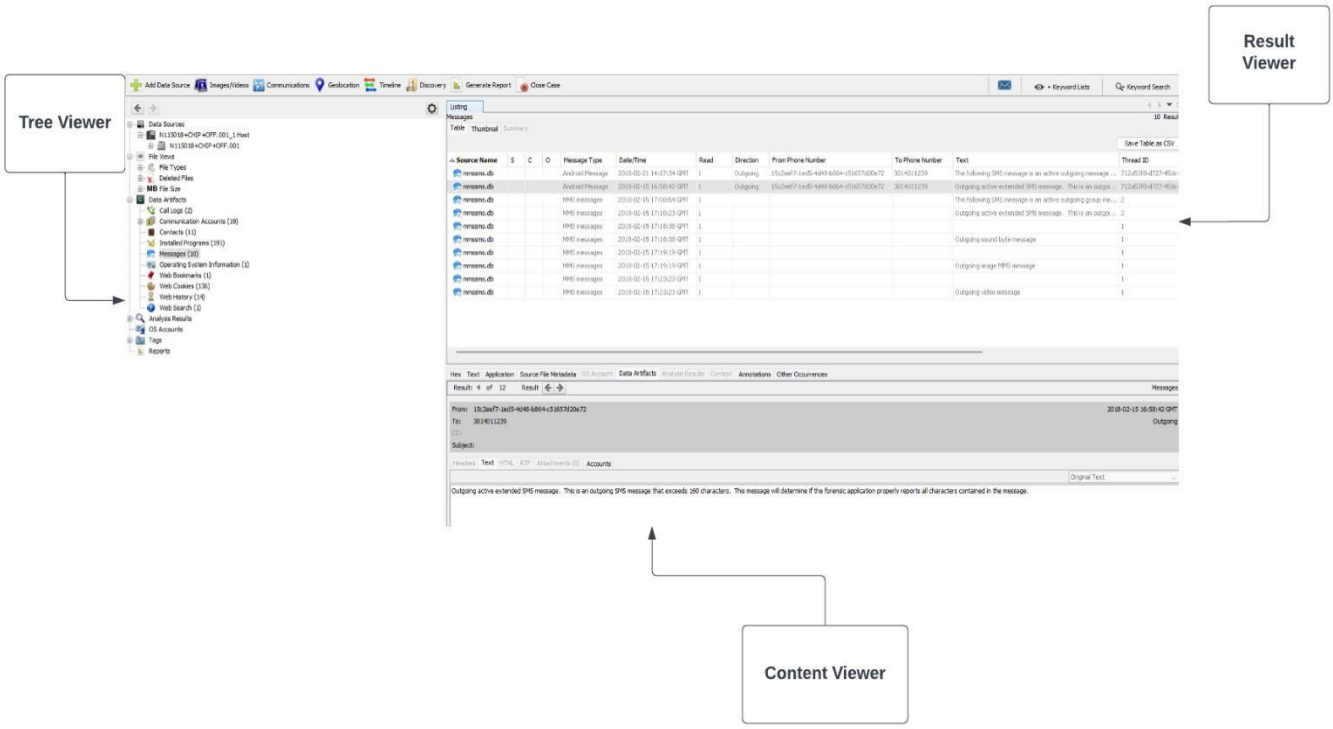


Figure 10 Autopsy tool layout

Tree Viewer
The tree is located on the left-hand side and contains the results of the ingest. This tree is split into four areas: 1. **Data source:** contains the file systems of the imported data source. Multiple data sources can be added. 2. **Views:** Specific files, such as .mp3, .wav and even deleted files, from all sources can be found here 3. **Results:** Results such as e-mail messages, tags, hash set, GPS, web history, can be found here 4. **Reports:** Generated reports can be found here
Result Viewer
Located in the right-hand side, displays the different types of data stored in each file.
Content Viewer
Located in the bottom right of the software. It contains any results associated with the selected item in the results viewer

Table 19 Autopsy tool layout (Sleuth kit, N.D)

7.3 Analysis of Dataset

To begin this analysis, the identification of the mobile device is an essential step as this will confirm the model number and IMEI that match the suspect's or victim's device.

The identification of the model can be found in diverse folders of the device. There are many folders that can be explored such as the System, Cache and one of the most important folders: the user Data. This folder contains most of the data related to the usage of the phone, such as call logs, App data, media files, download files, messaging, emails. And in some cases, applications will save the model of phone in the registry, which can be used to extract the model for analysis.

Identification of Mobile Device

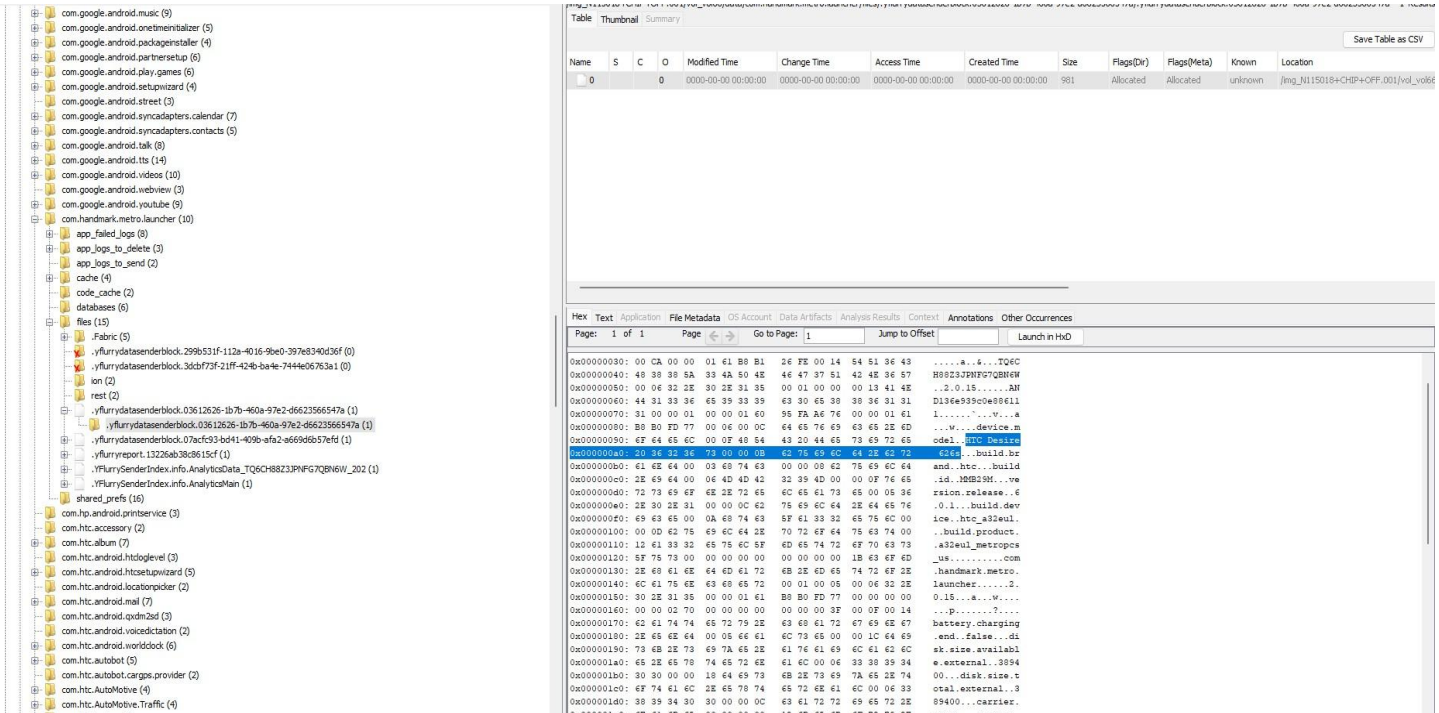
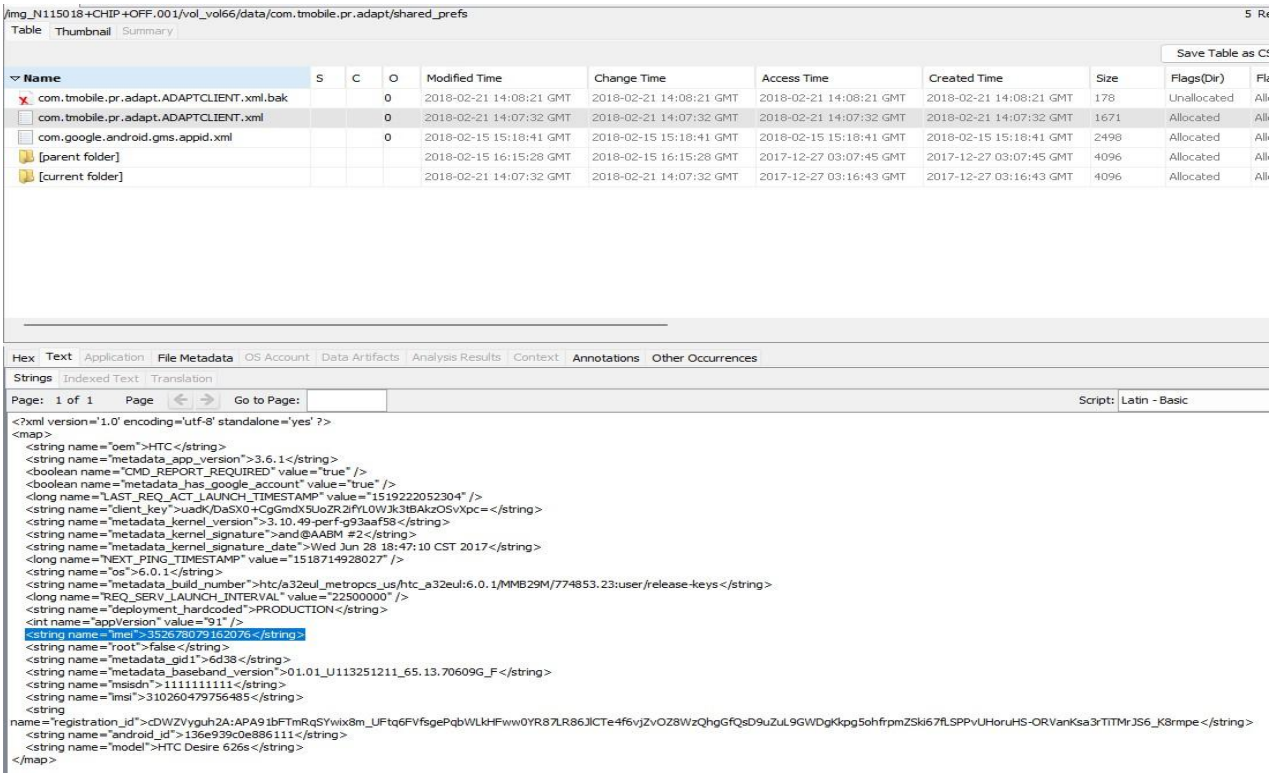
Device Model
Evidence: Device Model – HTC Desire 626s
Folder: /vol66/data/com.handmark.metro.launcher/files/.yflurrydatasenderblock.03612626-1b7b-460a-97e2-d6623566547a

Notes: The model number can be found in the Hex code, although this is not enough to confirm the suspect's device.
Output: Text version clearly showing the device model, brand, version and build but also disk size and battery

Table 20 Autopsy Analyse: Identification of device model

IMEI and IMSI
Evidence: IMEI and IMSI
Folder: */vol66/data.com.tmobile.pr.adapt/shared_prefs/com.tmobile.pr.adapt.ADAPTCLIENT.xml*



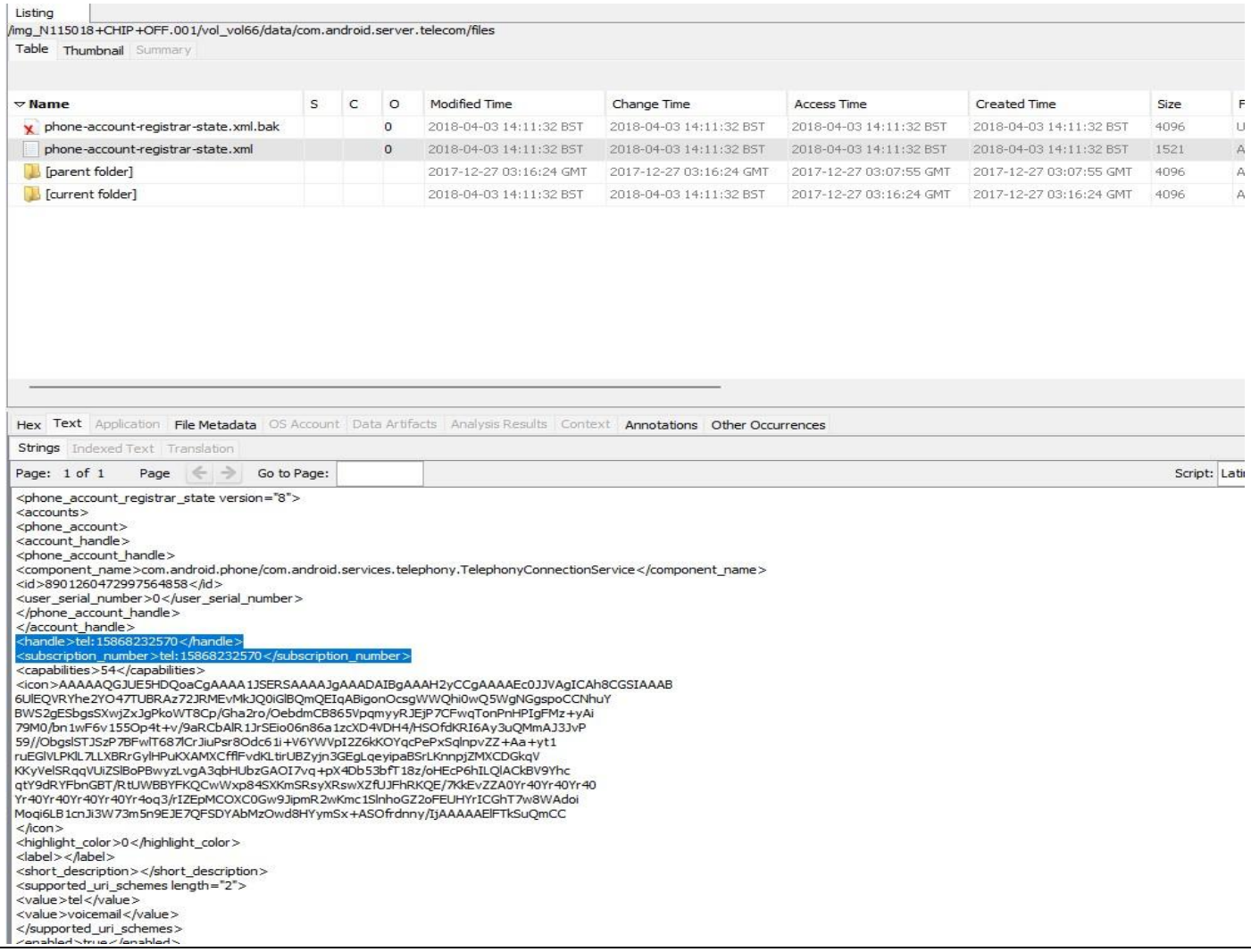
Notes: The IMEI is A 15-17 digit code used to identify every mobile device. This code is also used by telecomunnication services to block any stolen devices from initiating calls (TechTarget, December 2020).

Output: In the picture above, the model of the device is identified as HTC Desire 626s, the IMEI as 352678079162076 and the IMSI: 310260479756485.

```
<string name="imei">352678079162076</string>
<string name="root">false</string>
<string name="metadata_gid1">6d38</string>
<string name="metadata_baseband_version">01.01_U113251211_65.13.70609G_F</string>
<string name="msisdn">1111111111</string>
<string name="imsi">310260479756485</string>
<string
ame="registration_id">cDWZVyguh2A:APA91bFTmRqSYwix8m_UFtq6FVfsgePqbWLkHFww0YR87LF
<string name="android_id">136e939c0e886111</string>
<string name="model">HTC Desire 626s</string>
/map>
```

Table 21 Autopsy Analyse: Identification of IMEI and IMSI

Phone Number
Evidence: Phone number
Folder: /vol66/com.android.server.telecom/files/phone-account-registrar-state.xml



Notes: Phone account registration showing when the account was created, and the phone number registered to.

Output: Confirmation of mobile number - 15868232570

<id>8901260472997564858</id>
<user_serial_number>0</user_serial_number>
</phone_account_handle>
</account_handle>
<handle>tel:15868232570</handle>
<subscription_number>tel:15868232570</subscription_number>
<capabilities>54</capabilities>
<icon>AAAAAQGJUE5HDQoaCgAAAA1JSERSAAAAJgAAADAIBgAAAH2yCCgAAAAEc0JJVAgICAh8CGSIAAAB
6UlEQVRYhe2YO47TUBRAz72JRMEvMkJQ0iGlBQmQEIqABigonOcsgWWQhi0wQ5WgNGgspoCCNhuY
BWS2gESbgsSXwjZxJgPkoWT8Cp/Gha2ro/OebdmCB865VpqmyyRJEjP7CFwqTonPnHPIgFMz+yAi
79M0/bn1wF6v155Op4t+v/9aRCbAlR1JrSEio06n86a1zcXD4VDH4/HSOfdKRI6Ay3uQMmAJ3JvP
59//ObgslSTJSzP7BFwlT687lCrJiuPsr8Odc61i+V6YWVpI2Z6kKOYqcPePxSqlnpvZZ+Aa+yt1
ruEGlVLPKlL7LLXBRrGylHPuKXAMXCffFvdKLtirUBZyjn3GEgLqeyipaBSrLKnnpjZMXCDGkqV
KKyVelSRqqVUiZSlBoPBwyzLvgA3qbHUbzGAOI7vq+pX4Db53bfT18z/oHEcP6hILQlACkBV9Yhc
qtY9dRYFbnGBT/RtUWBBYFKQCwWxp84SXKmSRsyXRswXZfUJFhRKQE/7KkEvZZA0Yr40Yr40
Yr40Yr40Yr40Yr4oq3/rIZEpMCOXC0Gw9JipmR2wKmc1SlnhoGZ2oFEUHYrICGhT7w8WAdoi
Moqi6LB1cnJi3W73m5n9EJE7QFSDYAbMzOwd8HYymSx+ASOfrdnny/IjAAAAAElFTkSuQmCC

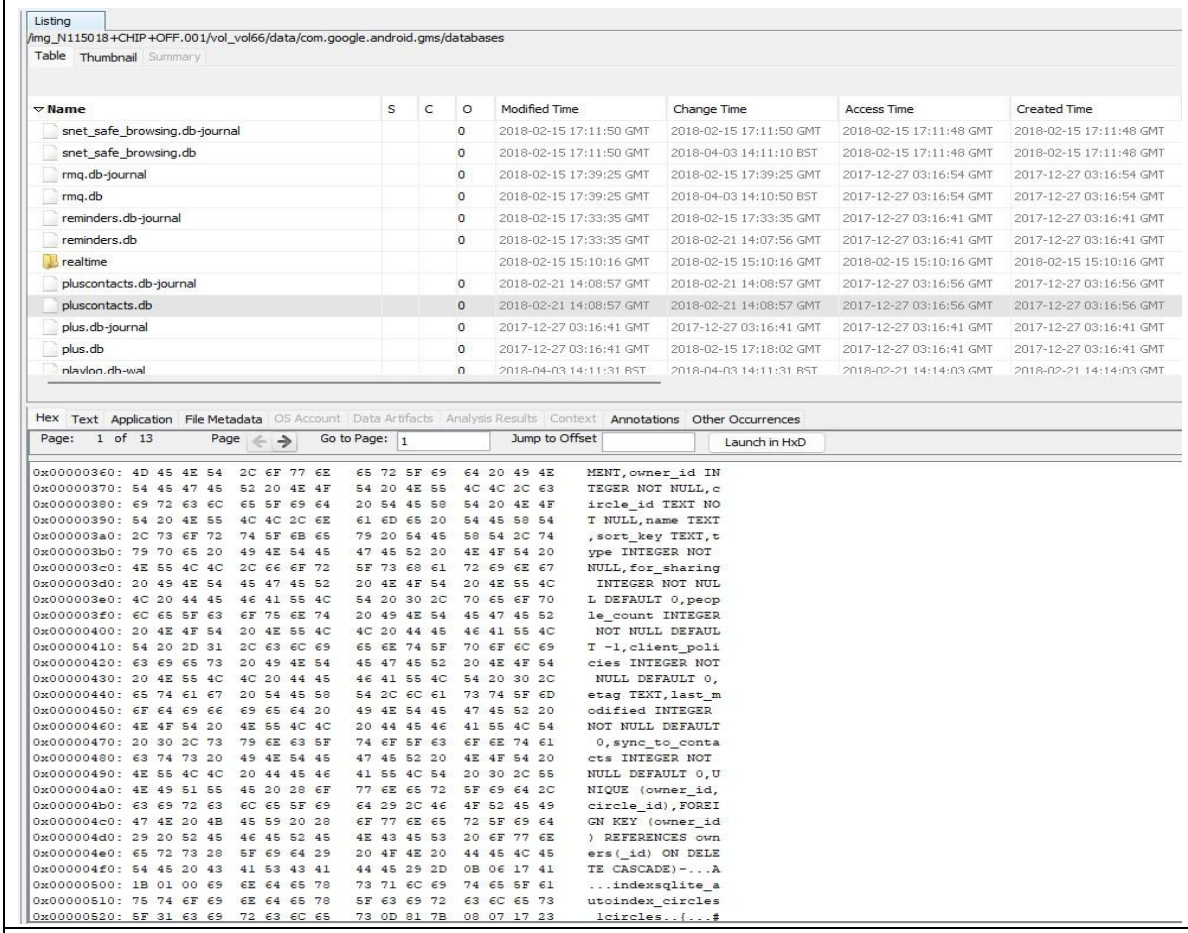
Table 22 Autopsy Analyse: Suspect's Phone number

Traditional Phone-based Evidence

Plus Contacts

Evidence: Plus contacts database

Folder: /vol66/data/com.google.android.gms.databases/pluscontacts.db



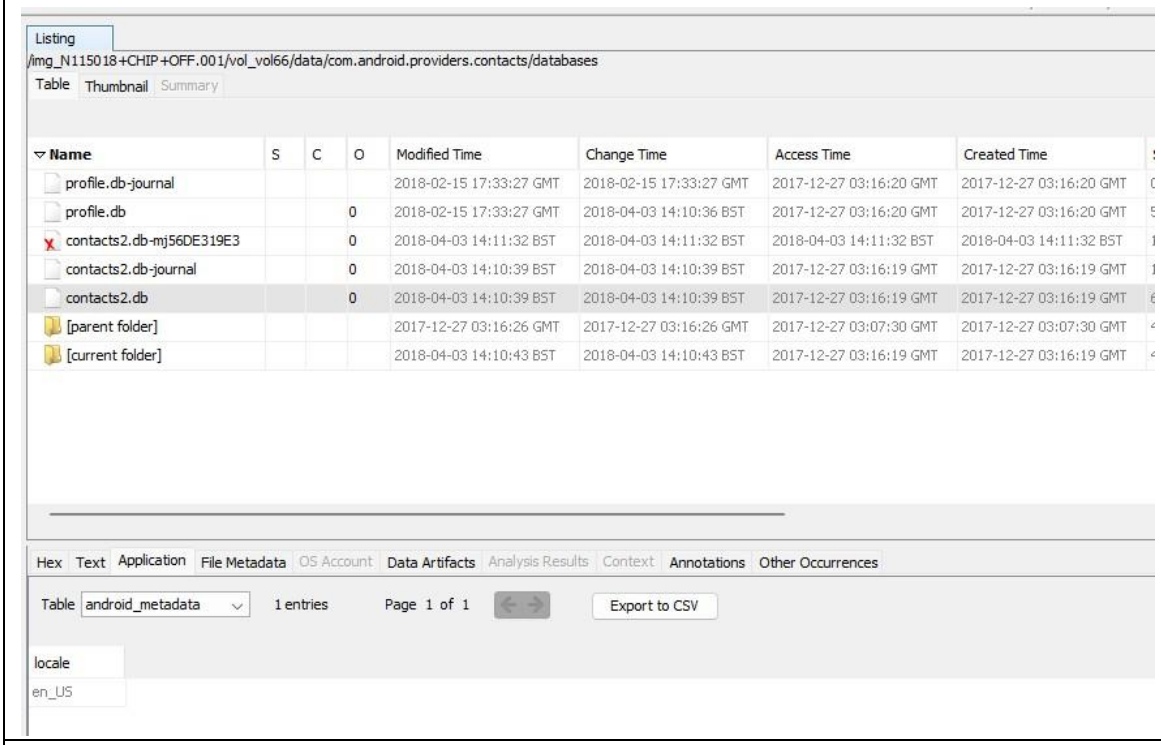
Notes: The database was extracted and analysed through SQLite

Output: List of contacts that include phone number and e-mails

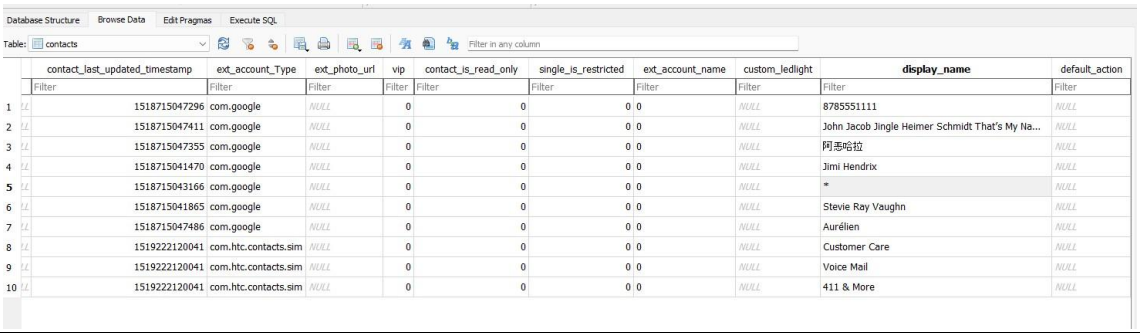
_id	container_id	item_type	is_edge_key	value	value2	value_type	custom_label	affinity1	affinity2
1	1	0	NULL	c3267096521791622711	NULL	NULL	NULL	NULL	NULL
2	1	2	0	8887771212	+18887771212	3	mobile	NULL	NULL
3	2	0	NULL	c520897731255403082	NULL	NULL	NULL	NULL	NULL
4	2	2	0	8785551111	+18785551111	3	mobile	NULL	NULL
5	3	0	NULL	c60008374675620458 56	NULL	NULL	NULL	NULL	NULL
6	3	2	0	+86 35 8 763 30 07	+863587633007	3	mobile	NULL	NULL
7	4	0	NULL	c5102245260360992690	NULL	NULL	NULL	NULL	NULL
8	4	2	0	8988675309	NULL	3	mobile	NULL	NULL
9	5	0	NULL	c4956517292728292689	NULL	NULL	NULL	NULL	NULL
10	5	1	0	hendrix@experienced.com	NULL	1	home	0.0	NULL
11	5	2	0	7691234560	NULL	3	mobile	NULL	NULL
12	5	4	0	www.jimihendrix.com	NULL	NULL	NULL	NULL	NULL
13	6	0	NULL	c7314956050578411 22	NULL	NULL	NULL	NULL	NULL
14	6	2	0	+33 22 6 555 20 20	+33226555202	3	mobile	NULL	NULL
17	8	0	NULL	c6796806989030074738	NULL	NULL	NULL	NULL	NULL
18	8	1	0	stevie@srv.com	NULL	2	work	0.0	NULL
19	8	2	0	1234567890	NULL	3	mobile	NULL	NULL
20	9	0	NULL	c926414797239820190	NULL	NULL	NULL	NULL	NULL
21	9	2	0	(987) 876-7654	NULL	-1		NULL	NULL
22	10	0	NULL	103681920312758735827	NULL	NULL	NULL	NULL	NULL
23	10	1	1	cfttmobile1@gmail.com	NULL	-1	NULL	0.0	NULL

Table 23 Autopsy Analyse: contacts plus data extraction

Contacts
Evidence: Contacts
Folder: /vol66/data/com.android.providers.contacts/databases



Notes: Although, only exporting this database did not reveal all the saved contacts and therefore, a second database was extracted. This the main database for contacts.
Output: contacts were found but also the * could indicate a delete value from the database



	contact_last_updated_timestamp	ext_account_Type	ext_photo_url	vip	contact_is_read_only	single_is_restricted	ext_account_name	custom_ledlight	display_name	default_action
1	1518715047296	com.google	NULL	0	0	0	0	NULL	8785551111	NULL
2	1518715047411	com.google	NULL	0	0	0	0	NULL	John Jacob Jingle Heimer Schmidt That's My Na...	NULL
3	1518715047355	com.google	NULL	0	0	0	0	NULL	阿丽哈拉	NULL
4	1518715041470	com.google	NULL	0	0	0	0	NULL	Jimi Hendrix	NULL
5	1518715043166	com.google	NULL	0	0	0	0	NULL	*	NULL
6	1518715041865	com.google	NULL	0	0	0	0	NULL	Stevie Ray Vaughn	NULL
7	1518715047486	com.google	NULL	0	0	0	0	NULL	Aurélien	NULL
8	1519222120041	com.htc.contacts.sim	NULL	0	0	0	0	NULL	Customer Care	NULL
9	1519222120041	com.htc.contacts.sim	NULL	0	0	0	0	NULL	Voice Mail	NULL
10	1519222120041	com.htc.contacts.sim	NULL	0	0	0	0	NULL	411 & More	NULL

Table 24 Autopsy Analyse: Contacts2.db extracted

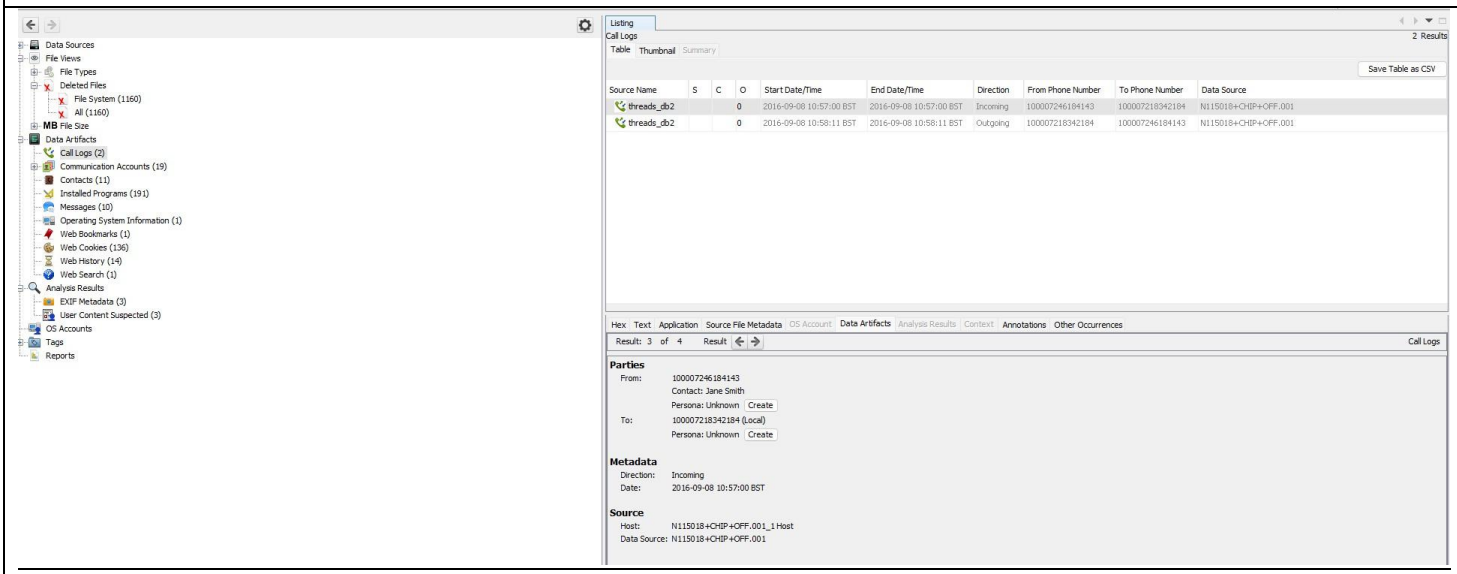
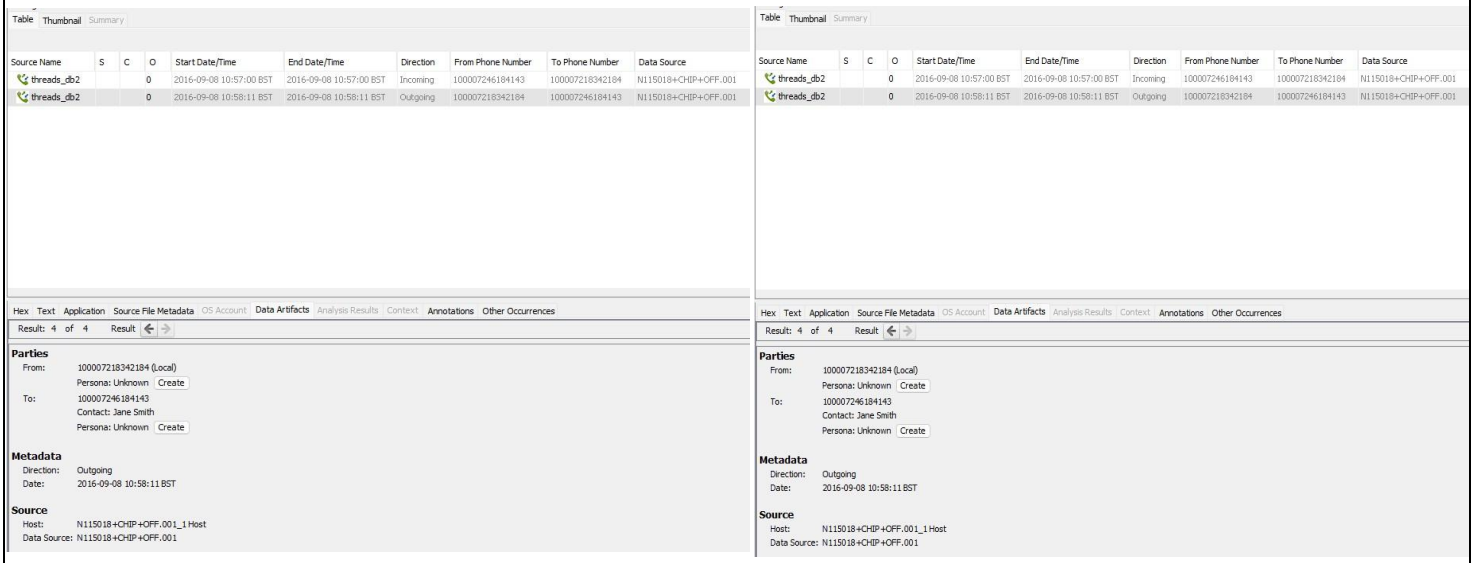
Call logs
Evidence: Call logs
Folder: Data artifacts

Notes: The call logs in Autopsy can be extracted under the Data artifacts.
Output: As seen below, it extracts outgoing and incoming calls


Table 25 Autopsy Analyse: Call logs output

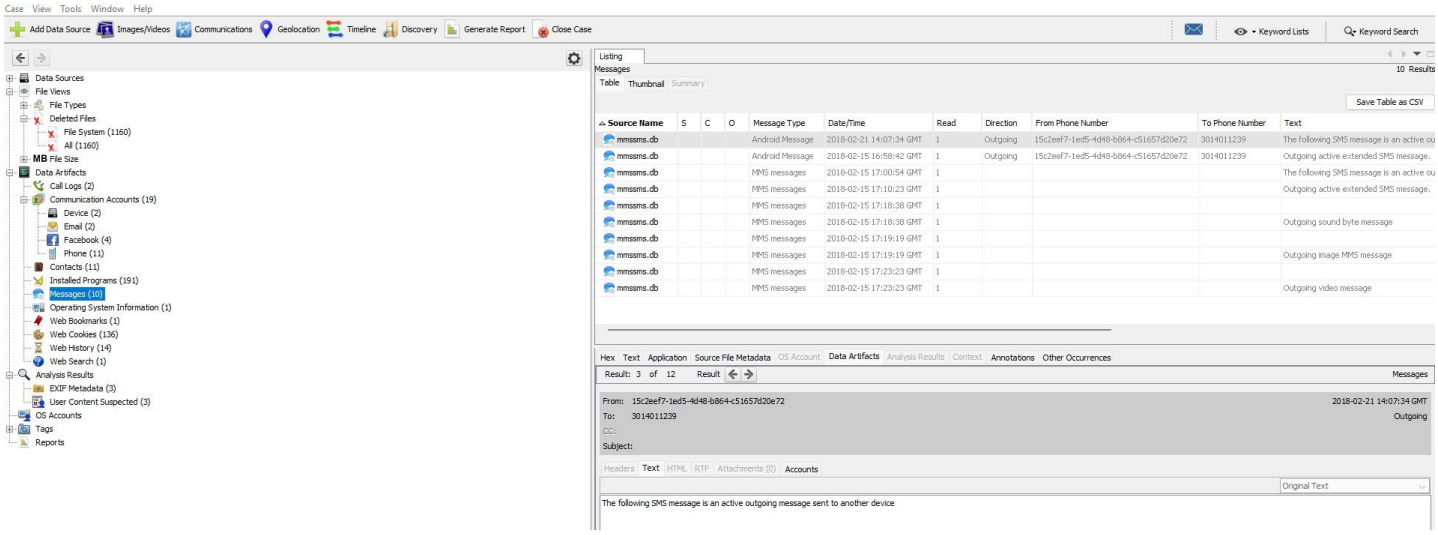
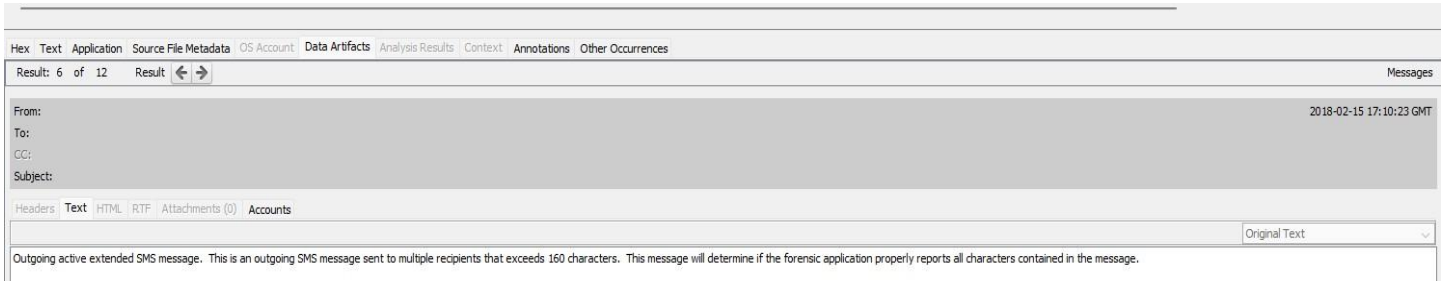
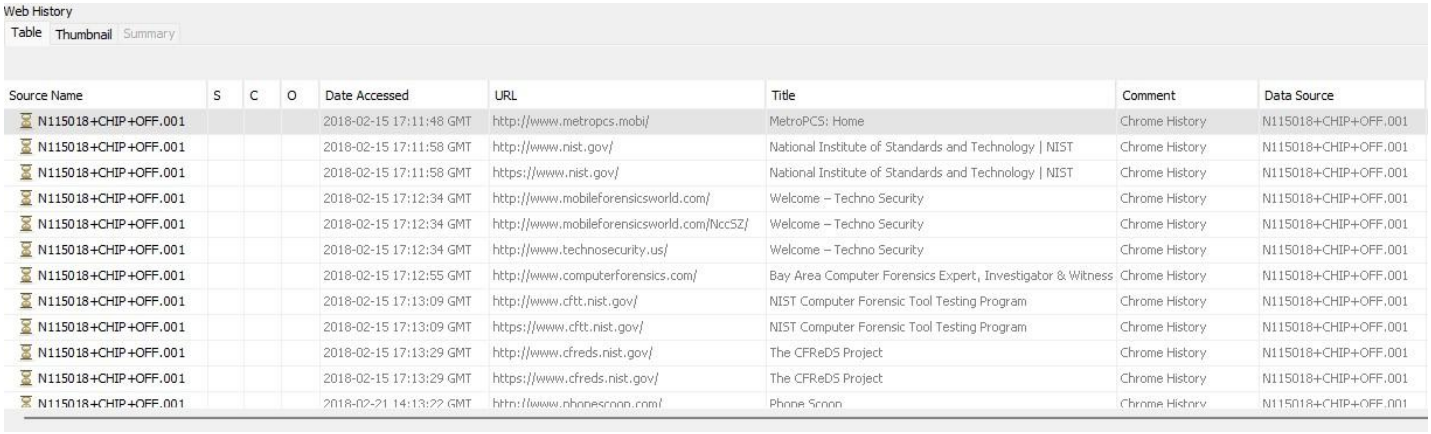
SMS/MMS
Evidence: SMS and MMS
Folder: Data Artifacts

Notes: Outgoing SMS and MMS
Output: example of SMS extracted from the mobile device


Table 26 Autopsy Analyse: SMS and MMS output

Web History

Evidence: Web History

Folder: Data Artifacts



Source Name	S	C	O	Date Accessed	URL	Title	Comment	Data Source
N115018+CHIP+OFF.001				2018-02-15 17:11:48 GMT	http://www.metropcs.mobi/	MetroPCS: Home	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:11:58 GMT	http://www.nist.gov/	National Institute of Standards and Technology | NIST	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:11:58 GMT	https://www.nist.gov/	National Institute of Standards and Technology | NIST	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:12:34 GMT	http://www.mobileforensicsworld.com/	Welcome – Techno Security	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:12:34 GMT	http://www.mobileforensicsworld.com/NccSZ/	Welcome – Techno Security	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:12:34 GMT	http://www.technosecurity.us/	Welcome – Techno Security	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:12:55 GMT	http://www.computerforensics.com/	Bay Area Computer Forensics Expert, Investigator & Witness	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:13:09 GMT	http://www.cftt.nist.gov/	NIST Computer Forensic Tool Testing Program	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:13:09 GMT	https://www.cftt.nist.gov/	NIST Computer Forensic Tool Testing Program	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:13:29 GMT	http://www.cfreds.nist.gov/	The CFReDS Project	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-15 17:13:29 GMT	https://www.cfreds.nist.gov/	The CFReDS Project	Chrome History	N115018+CHIP+OFF.001
N115018+CHIP+OFF.001				2018-02-21 14:13:22 GMT	http://www.phonescoop.com/	Phone Scoop	Chrome History	N115018+CHIP+OFF.001

Notes: Visited websites URLs in Google Chrome

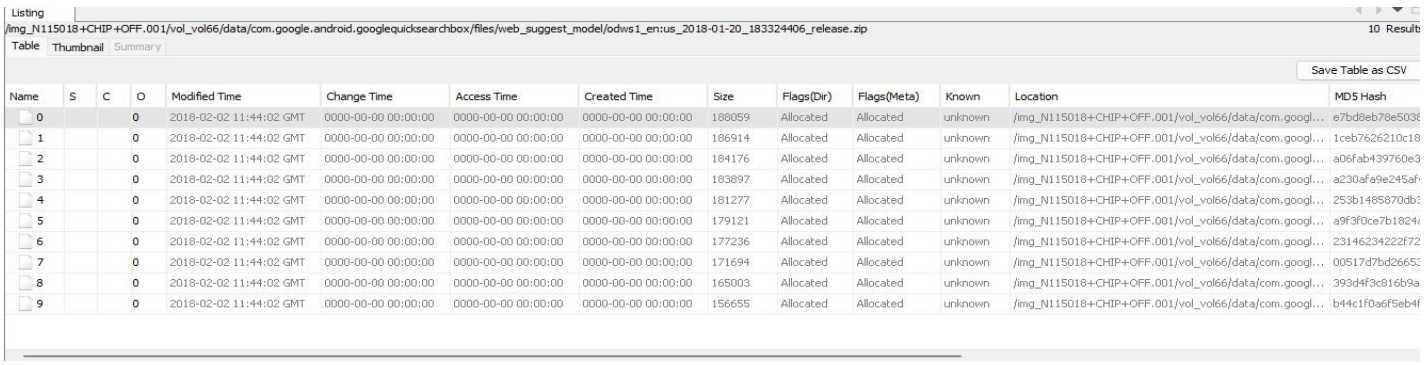
Output: example of visited website showing the access date and time and URL

Table 27 Autopsy Analyse: Visited websites

Google Quick Search

Evidence: Google quick search

Folder: /vol66/data/com.google.android.googlequicksearchbox/files/web_suggest_model/odws1_en:us_2018_01-20_183324406_release.zip


Listing
/img_N115018+CHIP+OFF.001/vol_vol66/data/com.google.android.googlequicksearchbox/files/web_suggest_model/odws1_en:us_2018-01-20_183324406_release.zip
10 Results
Table Thumbnail Summary
Save Table as CSV

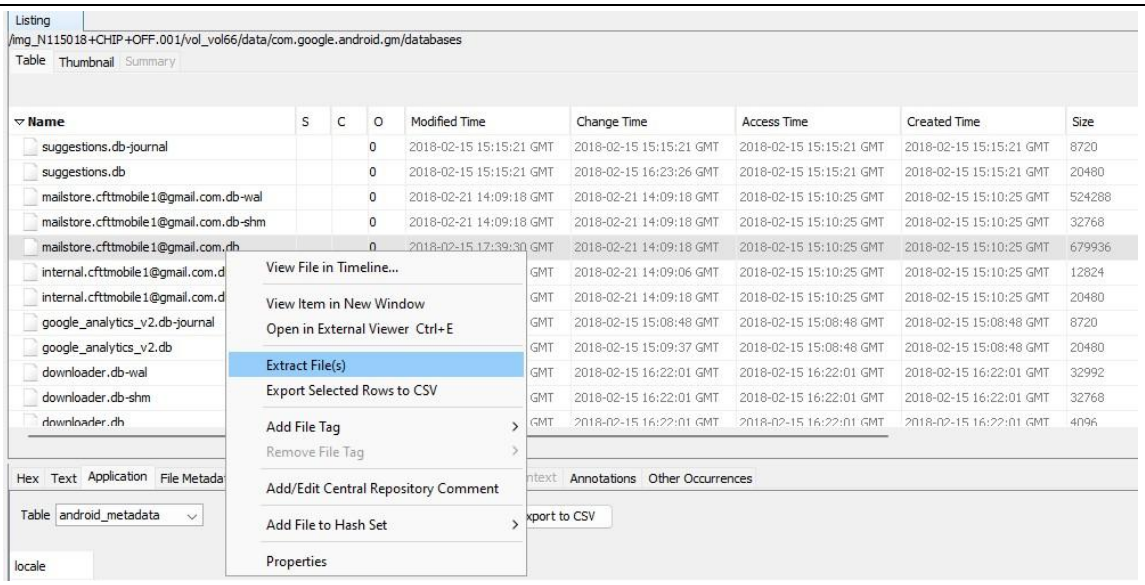
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
0			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	188059	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	e7bd8eb78e503
1			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	186914	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	1ceb7626210c18
2			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	184176	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	a06fab439760e3
3			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	183897	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	a230afa9e245af
4			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	181277	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	253b1485870db3
5			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	179121	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	a9f3f0ce7b1824
6			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	177236	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	23146234222f72
7			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	171694	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	00517d7bd26653
8			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	165003	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	393d4f3c816b9a
9			0	2018-02-02 11:44:02 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	156655	Allocated	Allocated	unknown	/img_N115018+CHIP+OFF.001/vol_vol66/data/com.googl...	b44c1f0a6f5eb4f

Notes: All quick searches stored in the device as a zip file. These can be directly open in Autopsy

Output: Once open, a list of the quick searches is available. This can be used to determine if a crime was premeditated.

Table 28 Autopsy Analyse: Google quick search output

Email-s
Evidence: Received E-mails
Folder: /vol66/data/com.google.android.gmm/databases/mailstore.ctfmobile1@gmail.com.db



Notes: emails database can also be extracted and analysed through SQLite

Output: extraction of all received e-mails showing a snippet of the e-mails and the subject

Table: conversations

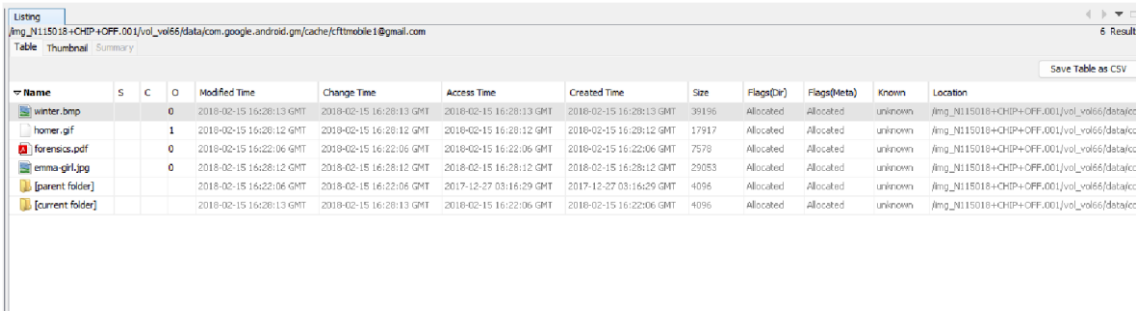
	_id	queryId	subject	snippet	fromAddress	fromProtoBuf	fromCompact	personalLevel	labelIds
1	1592434019732748317	0	#WeMetOnTwitter	Happy Valentine's Day, John Smith! ...	NULL	NULL	NULL	2	,52,-510,14,1,6,5,42,
2	1592410923213877993	0	John, you have 1 new notification	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,6,5,42,
3	1592382257099034208	0	John, 5 data science courses for you	Develop your skills on LinkedIn Learning John ...	NULL	NULL	NULL	2	,56,69,5,42,52,-510,14,1,6,
4	1592375138558169316	0	The problem with working hard	John Smith The problem with working hard ...	NULL	NULL	NULL	2	,52,-510,14,1,6,5,42,
5	1592315529912170386	0	Security alert	cftt mobile1 New device signed in to ...	NULL	NULL	NULL	2	,52,1,41,-508,5,
6	1592273737180967571	0	Check your Google Account security status	cftt mobile1 Stay safer online with the new ...	NULL	NULL	NULL	2	,52,1,41,-508,5,
7	1592260169589756740	0	John, you have 91 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,6,5,42,
8	1592231791986481149	0	Eun Yang Tweeted: Finally! Woohoo! 🎉??🎻 💃	Indira Lakshmanan, Chelsea Janes, Joy Reid, a n...	NULL	NULL	NULL	2	,52,-510,14,1,6,5,42,
9	1592214119063534089	0	New login to Twitter from Android	We noticed a recent login for your account ...	NULL	NULL	NULL	2	,52,44,14,1,41,-508,5,
10	1592198112850881299	0	Chare.wav		NULL	NULL	NULL	2	,8,
11	1592182085681485165	0	John, see who you already know on LinkedIn	You know more people on LinkedIn than you thin...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
12	1592168190153554705	0	John, you have 4 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
13	1592142527418137465	0	John, do you know these people on LinkedIn?	Adding connections makes building relationships ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
14	1592112594981854029	0	Maria Elena Carrillo, Yarlis Barrios Beltran and 8 others are ...	Add the people you know to see their photos and...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
15	1592077052056508838	0	John, you have 6 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
16	1592021344422381941	0	John, you have 8 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
17	1592019808300359537	0	Alice Stevenson, Michelle Jordan and 8 others are new friend...	Add the people you know to see their photos and...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
18	1591987585590472615	0	John, you have 4 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
19	1591981910865993096	0	Let the #WinterGames begin	Follow Team USA and your favorite athletes ...	NULL	NULL	NULL	2	,52,14,1,43,5,-509,
20	1591980925097956464	0	Maggie Haberman Tweeted: In the case of this particular ...	Andrea Swalec, Washington Post, NBCSports ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
21	1591954983267110008	0	Follow EasyBuyMobiles, A Viral Team and Hallie Nolan on ...	A Viral Team, Hallie Nolan also Tweeted. Who to...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
22	1591934868976202108	0	John, you have 4 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
23	1591890228775858616	0	Ted Leonsis Tweeted: Capital One Arena is part of the ...	Michael Tubbs, Doug Kammerer, Chris Long, Joe ...	NULL	NULL	NULL	2	,52,-510,14,1,5,42,
24	1591865595790526151	0	John, we're glad you're back!	Here's three quick steps to get started using your...	NULL	NULL	NULL	2	,52,17,14,1,42,
25	1591838626954015448	0	John, you have 6 new notifications	A lot has happened on Facebook since you last ...	NULL	NULL	NULL	2	,52,17,14,1,42,
26	1545487767691671918	1	gibson.txt		NULL	NULL	NULL	2	,17,-2,1,41,19,7,20,
27	1545487675735835686	1	forensics.pdf		NULL	NULL	NULL	2	,17,-2,1,41,19,7,20,
28	1545487598156294665	1	french.mp3		NULL	NULL	NULL	2	,17,-2,1,41,19,7,20,
29	1545487536384287494	1	chare.wav		NULL	NULL	NULL	2	,17,-2,1,41,19,7,20,

Table 29 Autopsy Analyse: E-mails output

Email Attachments and Downloads

Evidence: Received Attachments

Folder: vol66/data/com.google.android.com/cache/ctftmobile1@gmail.com/Attachments



Notes: A list of attachments can also be found in the conversation Database. To do so, the database must be extracted and the filter changed to “Attachments”

Output: Images extracted from cache

Notes: User can also explore the Download folder to confirm the files that were previously downloaded on the device

Folder: vol66/media/0/Download

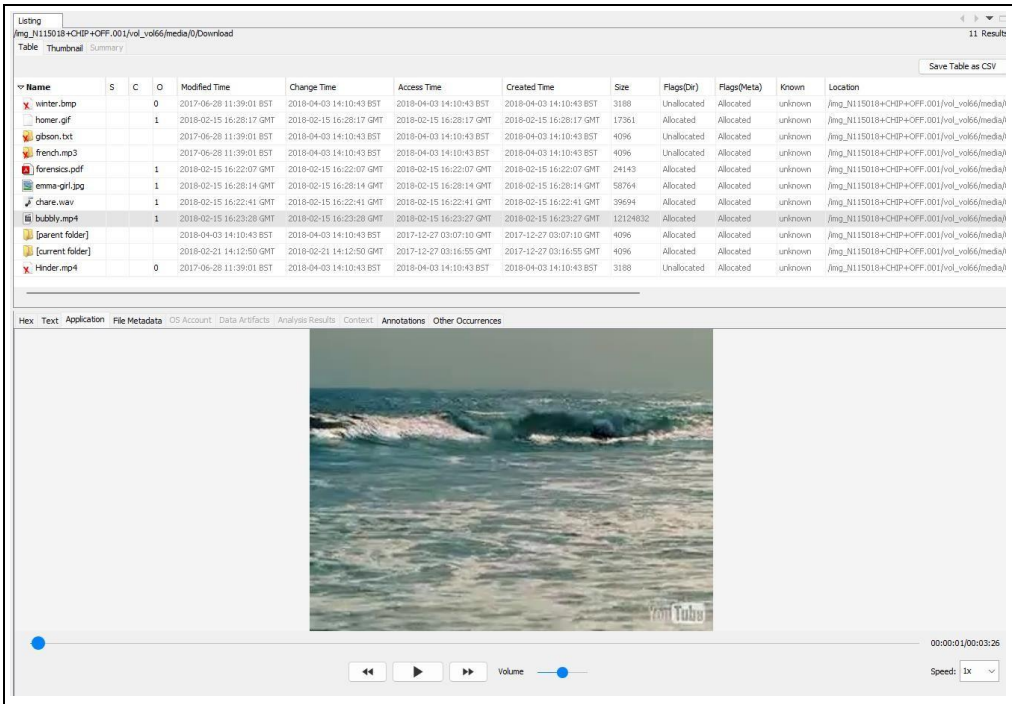
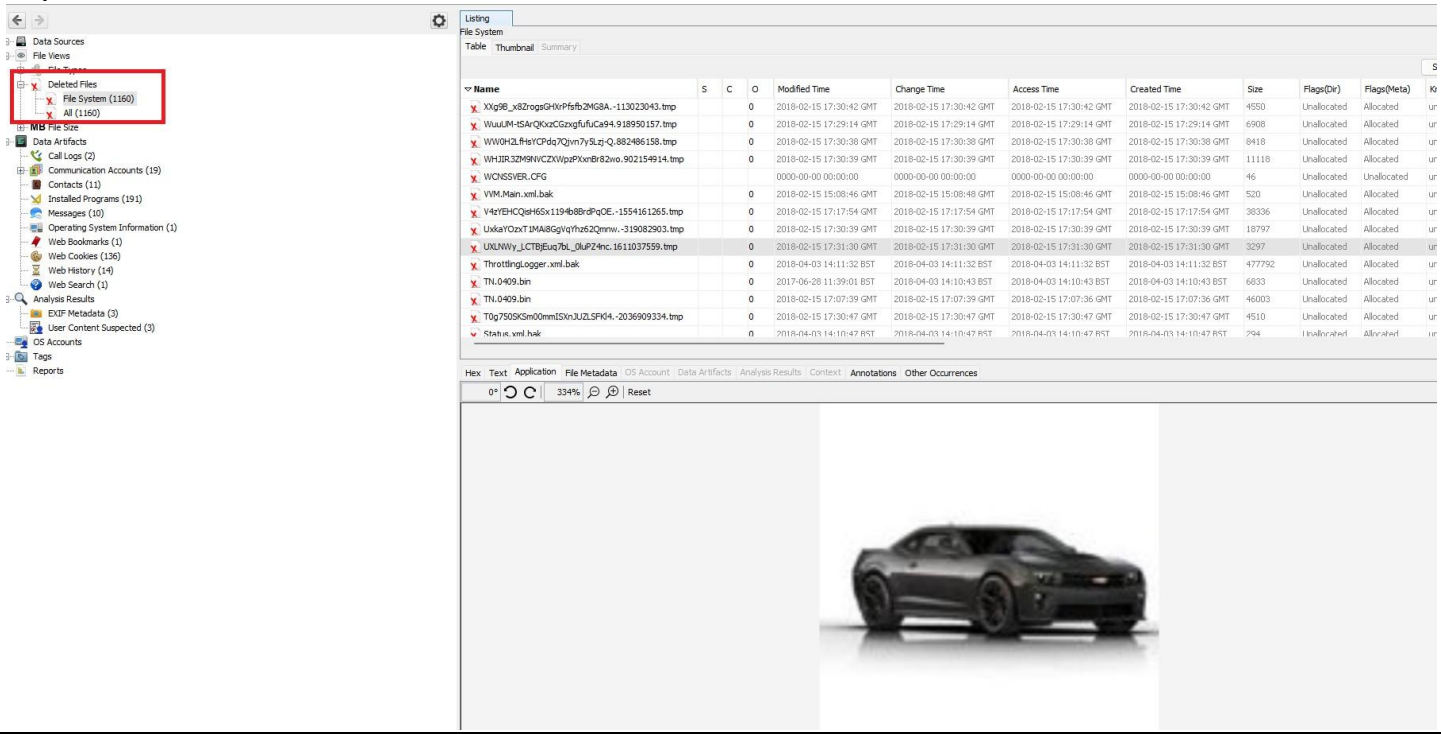


Table 30 Autopsy Analyse: E-mail attachments and downloads

Deleted Files
Evidence: Deleted twitter cache file
Folder: Deleted File Systems
Output

Evidence: Deleted facebook cache image

Folder: Deleted File Systems

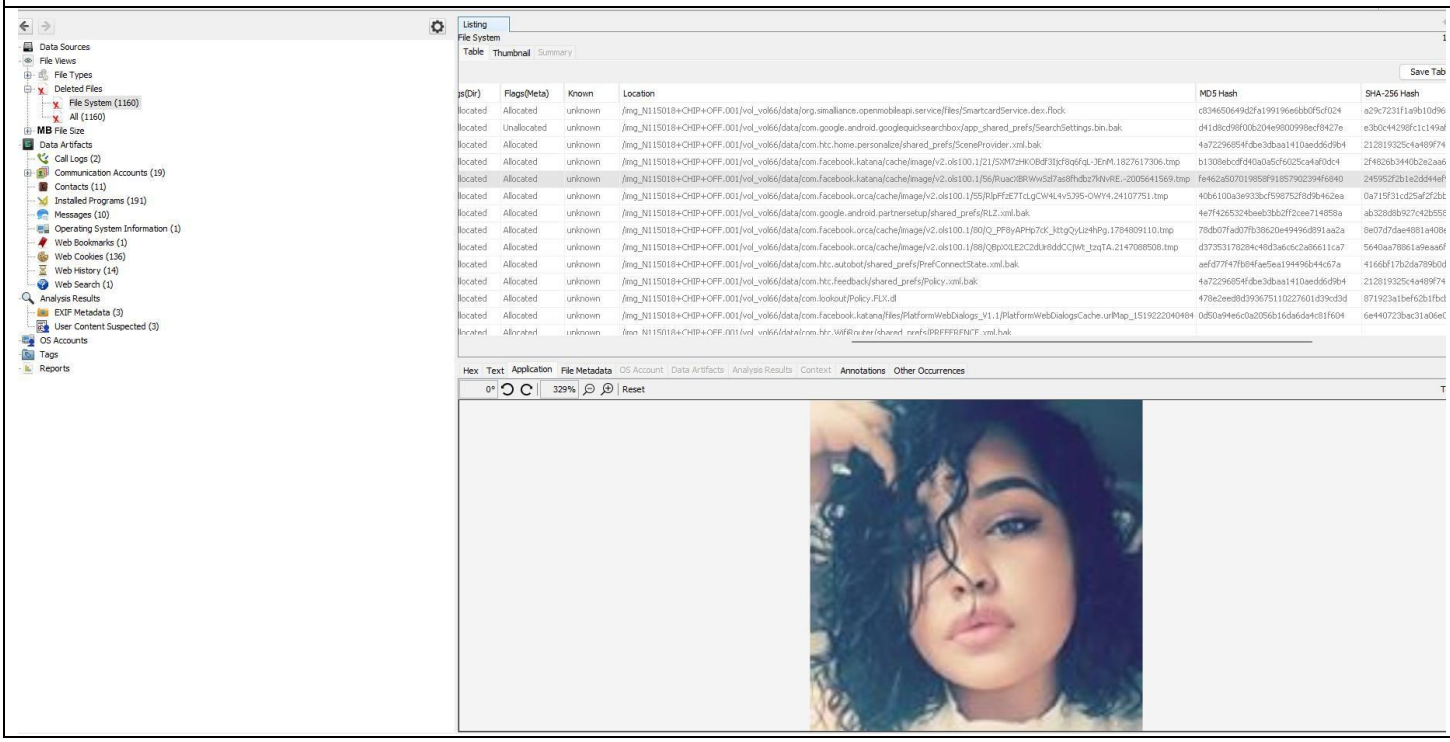
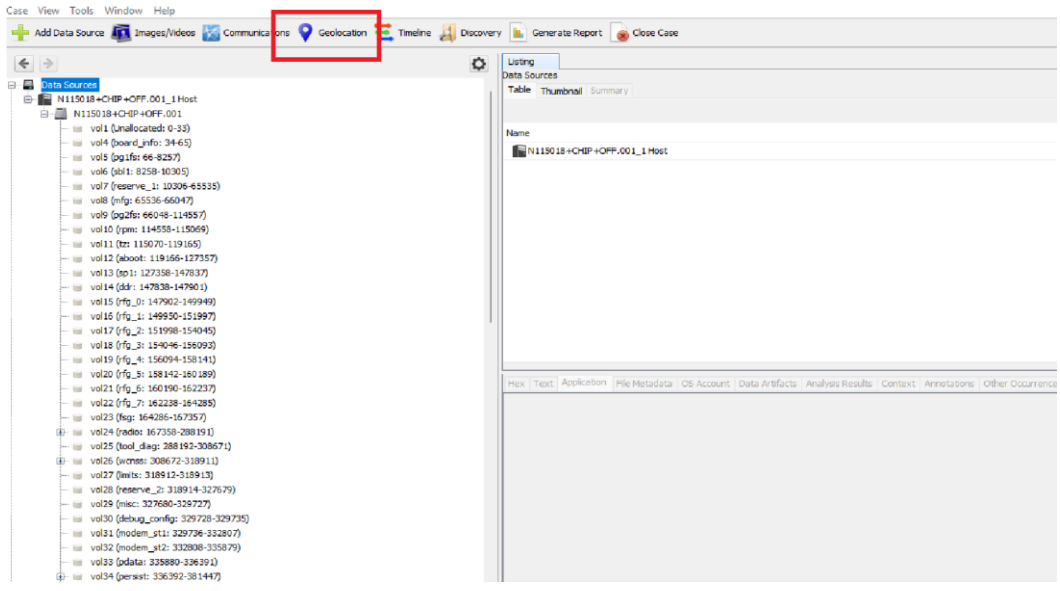


Table 31 Autopsy Analyse: Deleted files

GPS

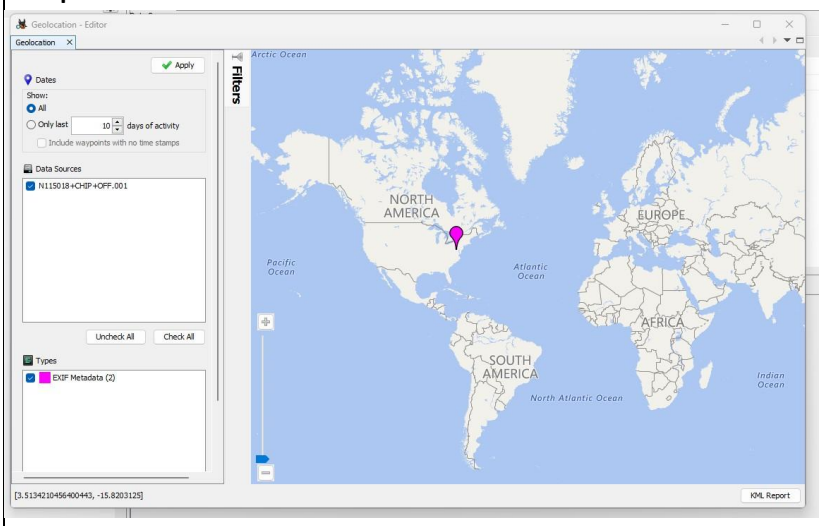
Evidence: Mobile device Geolocation

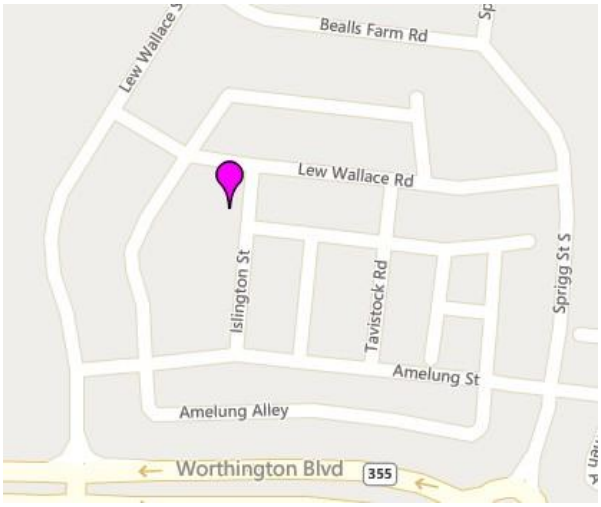
Folder: Geolocation can be found in Autopsy's layout



Notes: This Dataset provided by NIST only recorded one GPS entry

Output


Geolocation - Editor
Geolocation
Apply
Dates
Show:
All
Only last
10
days of activity
Include waypoints with no time stamps
Data Sources
N115018+CHIP+OFF.001
Uncheck All
Check All
Types
EXIF Metadata (2)
Filters
Arctic Ocean
NORTH AMERICA
EUROPE
Pacific Ocean
Atlantic Ocean
AFRICA
SOUTH AMERICA
North Atlantic Ocean
Indian Ocean
[3.513421045640044 3, -15.8203125]
KML Report


Bealls Farm Rd
Lew Wallace Rd
Islington St
Tavistock Rd
Spriggs St
Amelung St
Amelung Alley
Worthington Blvd
355

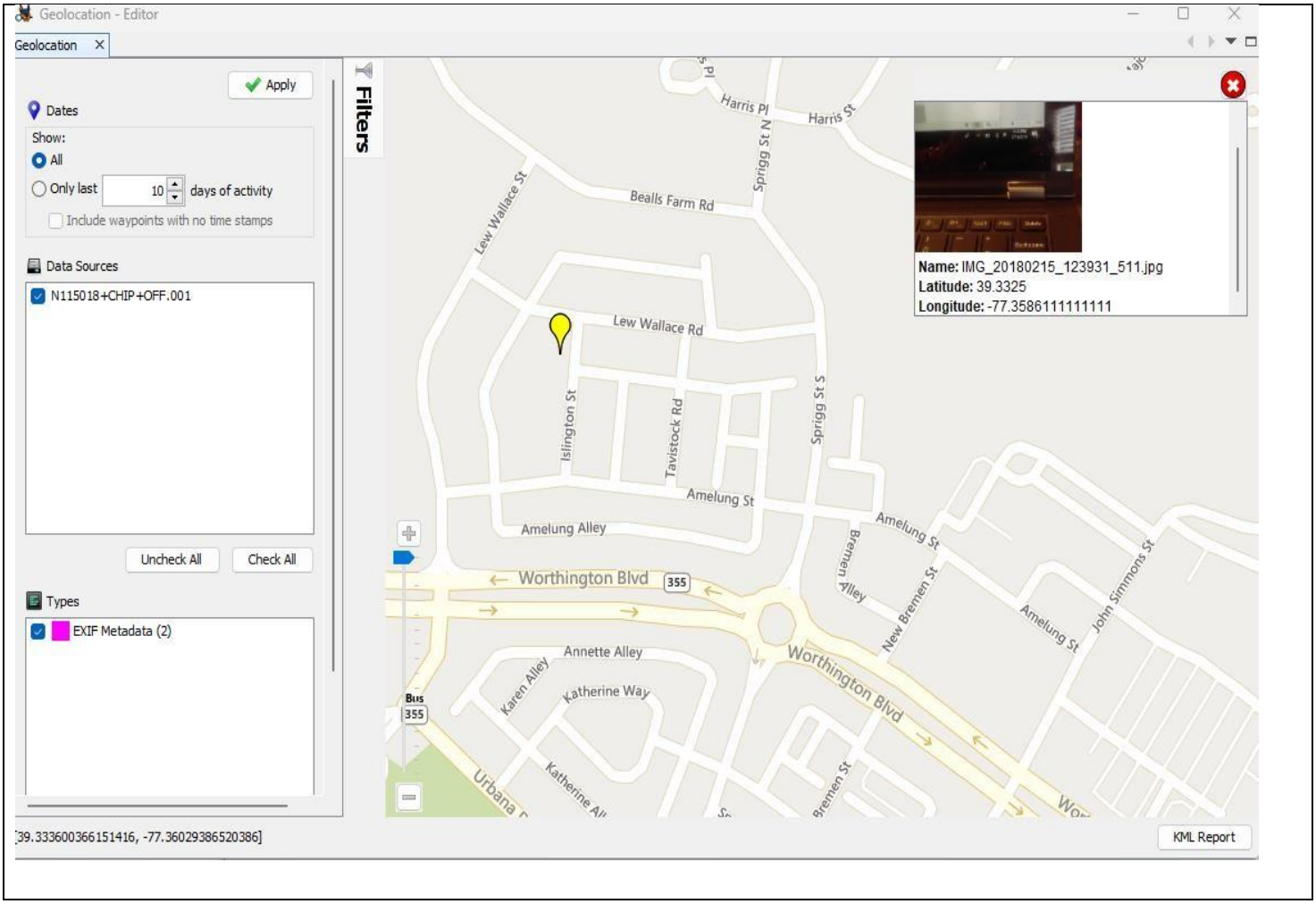
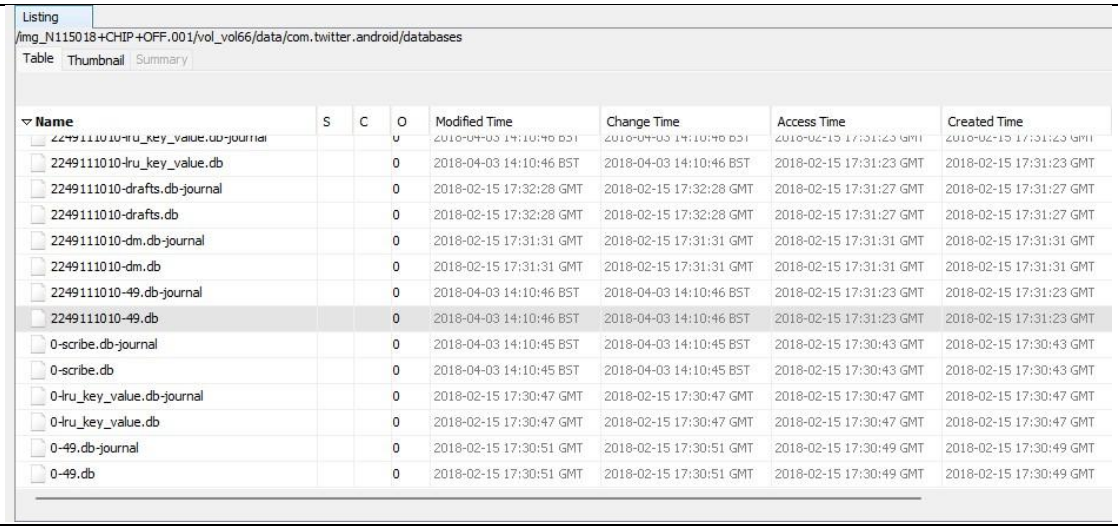


Table 32 Autopsy Analyse: GPS output

Application Based evidence

Twitter
Evidence: Outgoing tweets
Folder: /vol66/data/com.twitter.android/databases/2249111010-49.db



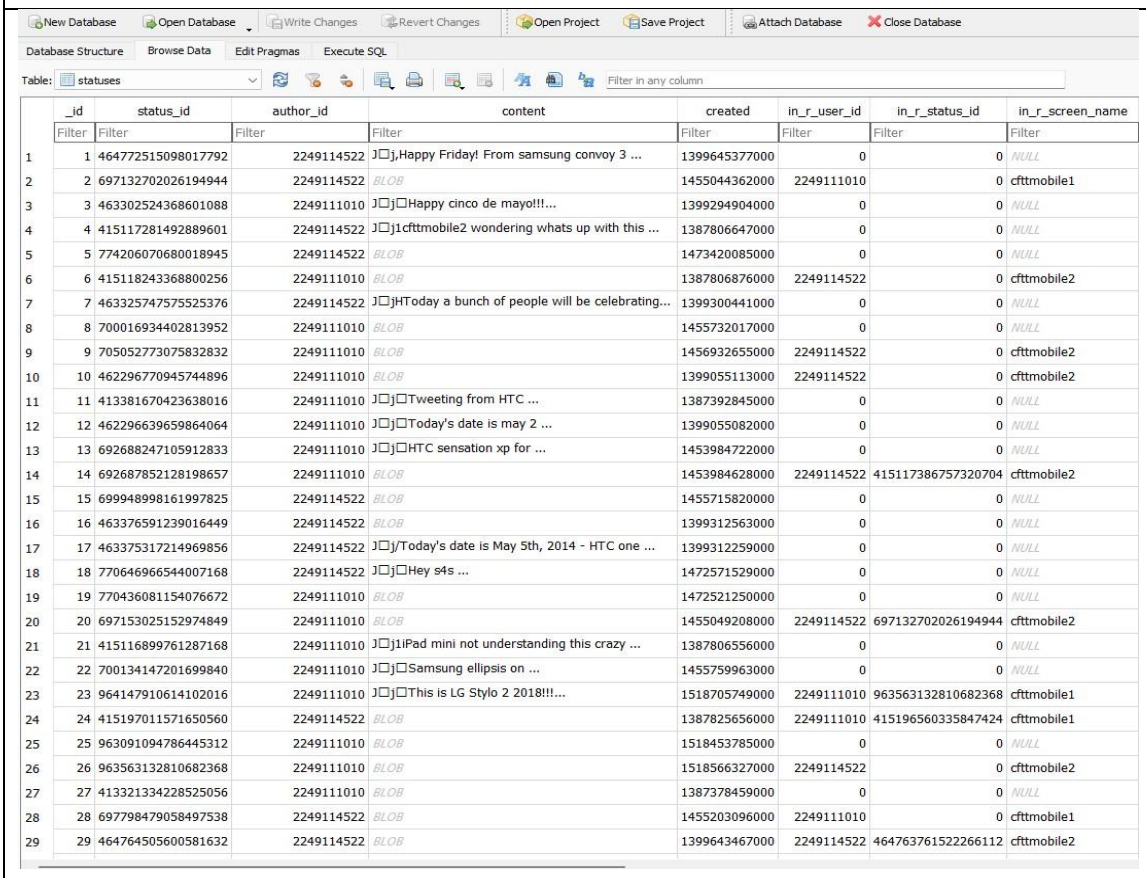
Listing

/img_N115018+CHIP+OFF.001/vol_vol66/data/com.twitter.android/databases

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
2249111010-lru_key_value.db-journal			0	2018-04-03 14:10:46 BST	2018-04-03 14:10:46 BST	2018-02-15 17:31:23 GMT	2018-02-15 17:31:23 GMT
2249111010-lru_key_value.db			0	2018-04-03 14:10:46 BST	2018-04-03 14:10:46 BST	2018-02-15 17:31:23 GMT	2018-02-15 17:31:23 GMT
2249111010-drafts.db-journal			0	2018-02-15 17:32:28 GMT	2018-02-15 17:32:28 GMT	2018-02-15 17:31:27 GMT	2018-02-15 17:31:27 GMT
2249111010-drafts.db			0	2018-02-15 17:32:28 GMT	2018-02-15 17:32:28 GMT	2018-02-15 17:31:27 GMT	2018-02-15 17:31:27 GMT
2249111010-dm.db-journal			0	2018-02-15 17:31:31 GMT	2018-02-15 17:31:31 GMT	2018-02-15 17:31:31 GMT	2018-02-15 17:31:31 GMT
2249111010-dm.db			0	2018-02-15 17:31:31 GMT	2018-02-15 17:31:31 GMT	2018-02-15 17:31:31 GMT	2018-02-15 17:31:31 GMT
2249111010-49.db-journal			0	2018-04-03 14:10:46 BST	2018-04-03 14:10:46 BST	2018-02-15 17:31:23 GMT	2018-02-15 17:31:23 GMT
2249111010-49.db			0	2018-04-03 14:10:46 BST	2018-04-03 14:10:46 BST	2018-02-15 17:31:23 GMT	2018-02-15 17:31:23 GMT
0-scribe.db-journal			0	2018-04-03 14:10:45 BST	2018-04-03 14:10:45 BST	2018-02-15 17:30:43 GMT	2018-02-15 17:30:43 GMT
0-scribe.db			0	2018-04-03 14:10:45 BST	2018-04-03 14:10:45 BST	2018-02-15 17:30:43 GMT	2018-02-15 17:30:43 GMT
0-lru_key_value.db-journal			0	2018-02-15 17:30:47 GMT	2018-02-15 17:30:47 GMT	2018-02-15 17:30:47 GMT	2018-02-15 17:30:47 GMT
0-lru_key_value.db			0	2018-02-15 17:30:47 GMT	2018-02-15 17:30:47 GMT	2018-02-15 17:30:47 GMT	2018-02-15 17:30:47 GMT
0-49.db-journal			0	2018-02-15 17:30:51 GMT	2018-02-15 17:30:51 GMT	2018-02-15 17:30:49 GMT	2018-02-15 17:30:49 GMT
0-49.db			0	2018-02-15 17:30:51 GMT	2018-02-15 17:30:51 GMT	2018-02-15 17:30:49 GMT	2018-02-15 17:30:49 GMT

Output: Content of the tweets and confirmation of the account that sent them



New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: statuses — Filter in any column

	_id	status_id	author_id	content	created	in_r_user_id	in_r_status_id	in_r_screen_name
1	1	464772515098017792	2249114522	J□j,Happy Friday! From samsung convoy 3 ...	1399645377000	0	0	NULL
2	2	697132702026194944	2249114522	BLOB	1455044362000	2249111010	0	cfttmobile1
3	3	463302524368601088	2249111010	J□j□Happy cinco de mayo!!!...	1399294904000	0	0	NULL
4	4	415117281492889601	2249114522	J□j1cfttmobile2 wondering whats up with this ...	1387806647000	0	0	NULL
5	5	774206070680018945	2249114522	BLOB	1473420085000	0	0	NULL
6	6	415118243368800256	2249111010	BLOB	1387806876000	2249114522	0	cfttmobile2
7	7	463325747575525376	2249114522	J□jHToday a bunch of people will be celebrating...	1399300441000	0	0	NULL
8	8	700016934402813952	2249111010	BLOB	1455732017000	0	0	NULL
9	9	705052773075832832	2249111010	BLOB	1456932655000	2249114522	0	cfttmobile2
10	10	462296770945744896	2249111010	BLOB	1399055113000	2249114522	0	cfttmobile2
11	11	413381670423638016	2249111010	J□j□Tweeting from HTC ...	1387392845000	0	0	NULL
12	12	462296639659864064	2249111010	J□j□Today's date is may 2 ...	1399055082000	0	0	NULL
13	13	692688247105912833	2249111010	J□j□HTC sensation xp for ...	1453984722000	0	0	NULL
14	14	692687852128198657	2249111010	BLOB	1453984628000	2249114522	415117386757320704	cfttmobile2
15	15	699948998161997825	2249114522	BLOB	1455715820000	0	0	NULL
16	16	463376591239016449	2249114522	BLOB	1399312563000	0	0	NULL
17	17	463375317214969856	2249114522	J□j/Today's date is May 5th, 2014 - HTC one ...	1399312259000	0	0	NULL
18	18	770646966544007168	2249114522	J□j□Hey s4s ...	1472571529000	0	0	NULL
19	19	770436081154076672	2249111010	BLOB	1472521250000	0	0	NULL
20	20	697153025152974849	2249111010	BLOB	1455049208000	2249114522	697132702026194944	cfttmobile2
21	21	415116899761287168	2249111010	J□j1iPad mini not understanding this crazy ...	1387806556000	0	0	NULL
22	22	700134147201699840	2249111010	J□j□Samsung ellipsis on ...	1455759963000	0	0	NULL
23	23	964147910614102016	2249111010	J□j□This is LG Stylo 2 2018!!!...	1518705749000	2249111010	963563132810682368	cfttmobile1
24	24	415197011571650560	2249114522	BLOB	1387825656000	2249111010	415196560335847424	cfttmobile1
25	25	963091094786445312	2249111010	BLOB	1518453785000	0	0	NULL
26	26	963563132810682368	2249111010	BLOB	1518566327000	2249114522	0	cfttmobile2
27	27	413321334228525056	2249111010	BLOB	1387378459000	0	0	NULL
28	28	697798479058497538	2249114522	BLOB	1455203096000	2249111010	0	cfttmobile1
29	29	464764505600581632	2249114522	BLOB	1399643467000	2249114522	464763761522266112	cfttmobile2

Table 33 Autopsy Analyse: Twitter output

8.0 Avilla Forensics

Avilla Forensics is an open-source tool created by the teacher of mobile forensics and police agent in the state of Sao Paulo, Brazil. This tool can be found on the project's GitHub located at: https://github.com/AvillaDaniel/AvillaForensics. To download the software, the user can find the link by scroll to the bottom of page where main software will be found in a Google Drive link. This workstation is composed by many open-source tools such as SQLite, Android Debug Bridge, IPED and many others. Even though, it does not require installation, this workstation must be launched with administrator rights to ensure that all features of the tool are fully working.

8.2 Tool layout

Once the tool is launched, the user is greeted with a brief explanation on how to execute the tool and a donation option to carry supporting the project. It is crucial for a mobile forensics investigator to familiarize themselves with the layout of any mobile forensics' tools. Understanding these layouts and what each tool can provide allows the investigator to efficiently navigate and acquire the data needed for the investigation. *Table 32* provides an explanation on all the tools available inside of Avilla Forensics.

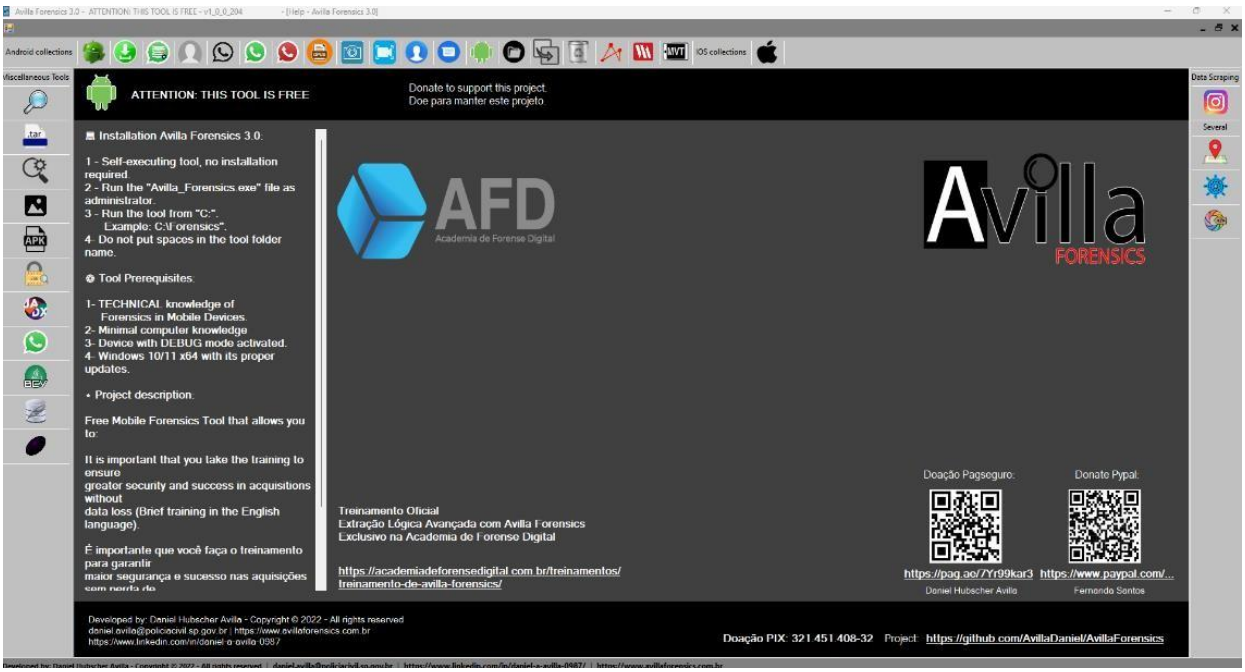
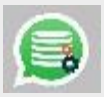
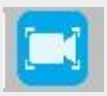


Figure 11 Avilla Forensics

Icon	Name	Function
	Backup ADB	This function allows to test for connectivity between the phone and the application. Android Debug Bridge is a tool that is implemented into Avilla Forensics that allows for the backup of the data stored in the device. This data includes app data, media files, system, and user data.
	APK Downgrade	With this tool the chosen application for analysis is downgraded for an older version. Newer versions of the application might have vulnerabilities that were patched up, therefore, downgrading to an older version of the application allows investigators to exploit that area to retrieve data.
	MGStore Decrypt	A tool used to decrypt databases encrypted with crypt14 and crypt15
	Contacts List + Avatar Photo + Deleted Contacts	This tool allows for the extraction of WhatsApp data such as the contact list, the avatar photos and even the deleted contacts.
	Download and .ENC decryptor	A decryptor used for generic encoded files.
	WhatsApp chat generator	Generates chat logs based on avatars and conversations
	OPUS audio WhatsApp transcription	Transcribes the audio speech of a WhatsApp voice message into a text format
	Screenshot	Takes a screenshot of the mobile phone screen
	Mirror Device	Once the mobile phone is plugged, this tools mirrors the device and the investigator can proceed with a manual extraction

	SMS and contacts extraction	Extracts SMS and contacts of the mobile phone into an excel sheet. Requires the phone to be connected to the workstation
	Misc Collections	Collection of data such as the IMEI, Dump of the system, Accounts, screen and Backup Dump, contacts, SMS, users,
		Android version, Bluetooth, Audios and videos and many more
	Android Trash	Collects deleted data from the android device
	IPED	Digital Evidence Processor and Indexer designed by the Federal Brazilian Police. This tool can handle large volumes of data such that were extracted for analysis
	Converter Backup .AB to .Tar	Integrated tool that converts extracted AB folders from mobile devices into .TAR. An essential process that allows tools such as IPED or Autopsy to view the data inside these folders
	Android QuickScan	Allows the investigator to perform a quick scan of the whole android to search for determined file such as .wav, mpeg, jpeg, pdf, 7zip, etc
	Image finder – BETA	A tool that is in Beta stage. This tool is used to search for a determined image based on the file type
	APK installer	Installs APK's directly into the mobile phone
	Hash calculator	Calculates the MD5, SH1, SH256, SHA238, SHA512 of a folder
	Jadx	A tool used for reverse-engineering and allows for the analyse of code of an APK file.
	WhatsApp Viewer	Allows investigators to view WhatsApp databases that are often found encrypted

	ByteCode Viewer	This tool is used to analyse the Bytecode of a compiled program
	SQLite Studio	A user-friendly tool that allows the creation, modification and viewing of SQLite databases

Table 32 Explanation of tools integrated in Avilla Forensics

8.3 Importing NIST dataset into Avilla Forensics

Before starting any analysis, the extracted data must be imported into each tool. Although, tools have different procedures for importing data. Therefore, *table* 33 provides guidelines on how to do this step in Autopsy and Avilla Forensics.

For data that was already extracted, users can use the IPED tool to perform the analysis. According to (GitHub, N.D) IPED or Digital Evidence Processor and Indexer (*Figure 12*) is an open-source tool developed by the digital forensics' experts from the Brazilian Federal Police since 2012, having its code officially published in GitHub in 2019. This tool is one of the examples of how the Sleuth Kit's library is very present in multiple open-source tools.

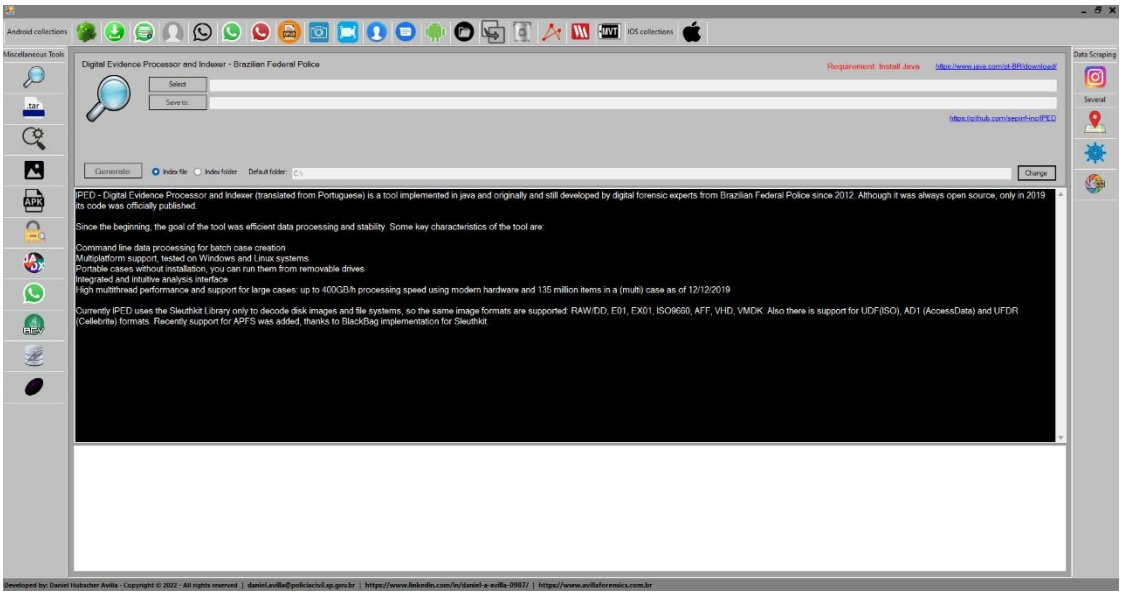
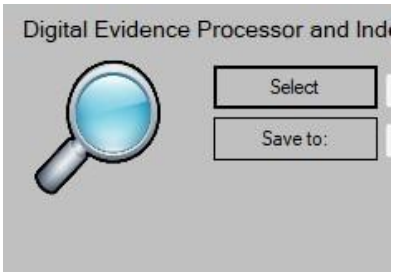
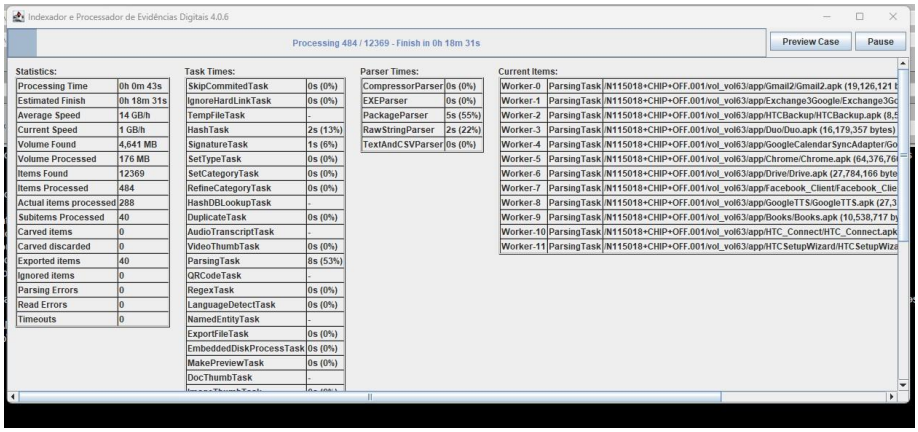
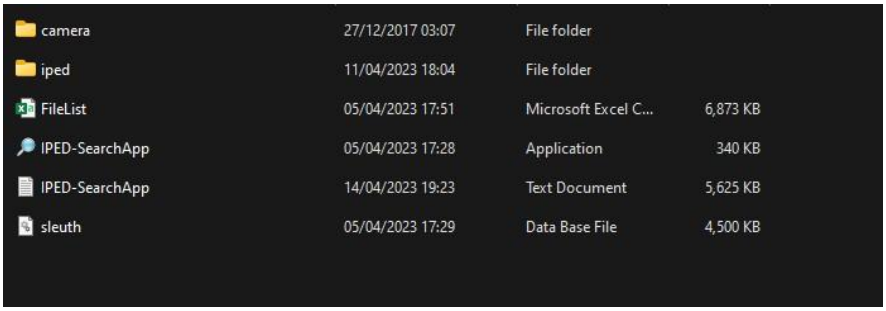


Figure 12 Overview of IPED tool

Step 1. Select the dataset 	Using the select code, users must select the NIST dataset. The data exported by the IPED tool must be saved to a specific folder. Once the dataset is select and a specific folder was crated for the data. The IPED can now generate the report.
Step 2. Generating report	At this point, IPED will launch and this process might take some time.
	
Step 3. IPED folder 	To carry on the same analyse, the user just has to load the folder related to the case and launch IPED-SearchAPP

Step 4. Overview of IPED	Once the process is finished, IPED will reveal all the data in the extracted dataset. At this stage, the analyse can now begin.

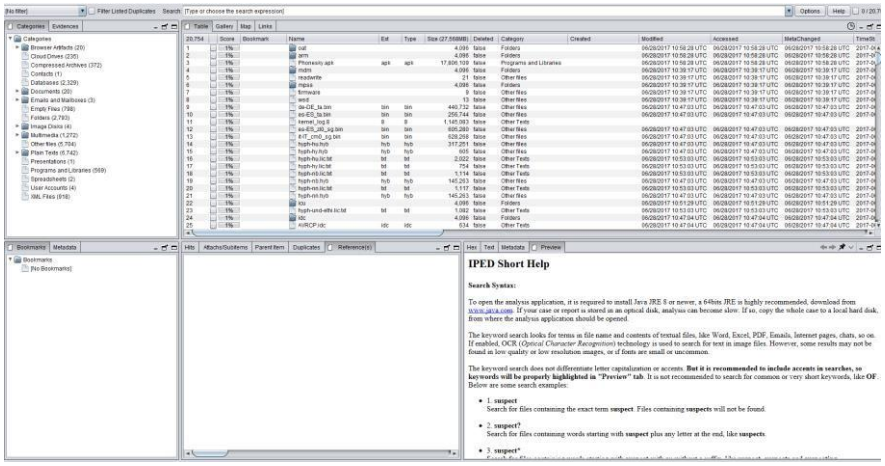
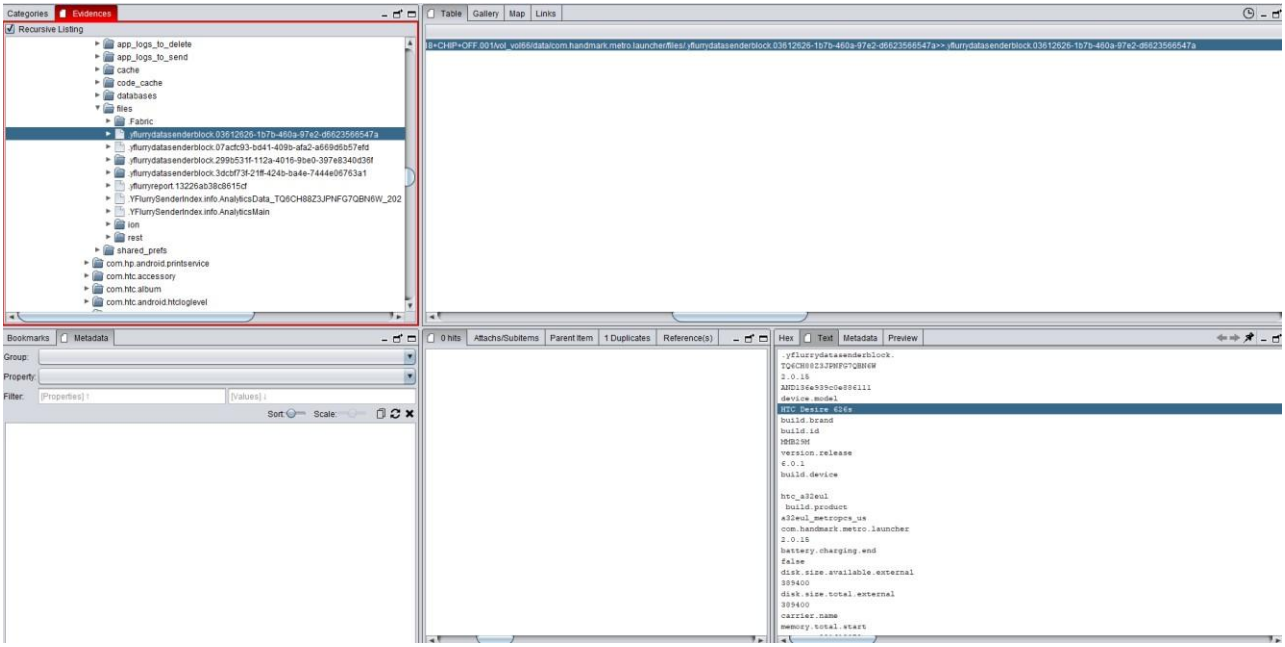


Table 33 Import NIST dataset into IPED

8.4. Analyse of Dataset through Avilla Forensics/IPED

Device Model
Evidence: Device Model – HTC Desire 626s
Folder: /vol66/data/com.handmark.metro.launcher/files/.yflurrydatasenderblock.03612626-1b7b-460a-97e2-d6623566547a

Output: Text showing the device model, brand, version and build but also disk size and battery

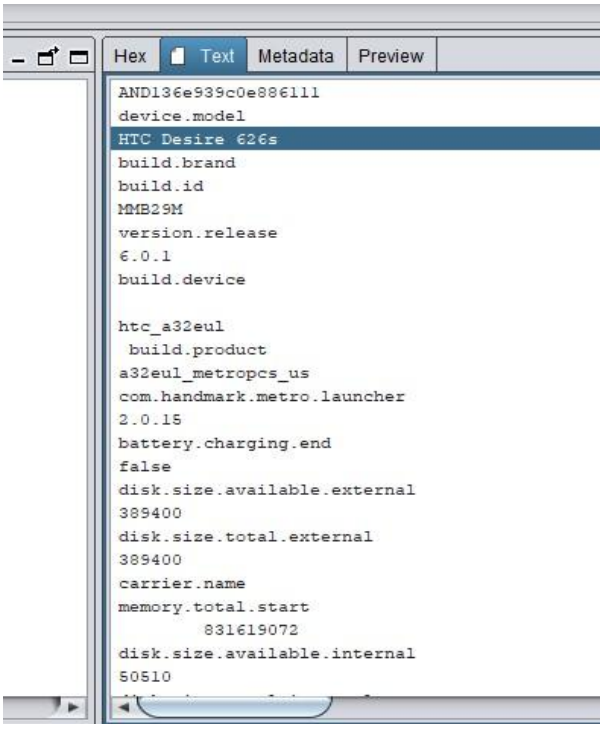
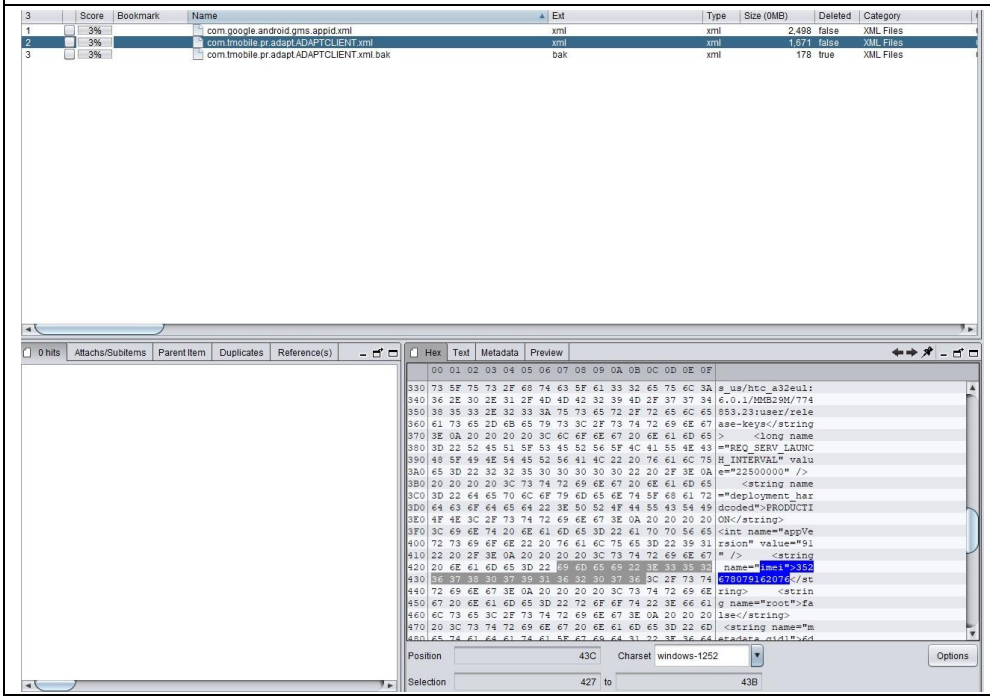


Table 34 Avilla Forensics Analyse: Device Model

IMEI and IMSI
Evidence: IMEI and IMSI
Folder: /vol66/data.com.tmobile.pr.adapt/shared_prefs/com.tmobile.pr.adapt.ADAPTCLIENT.xml



Output: The string in HEX confirms which one is the IMEI and the IMSI

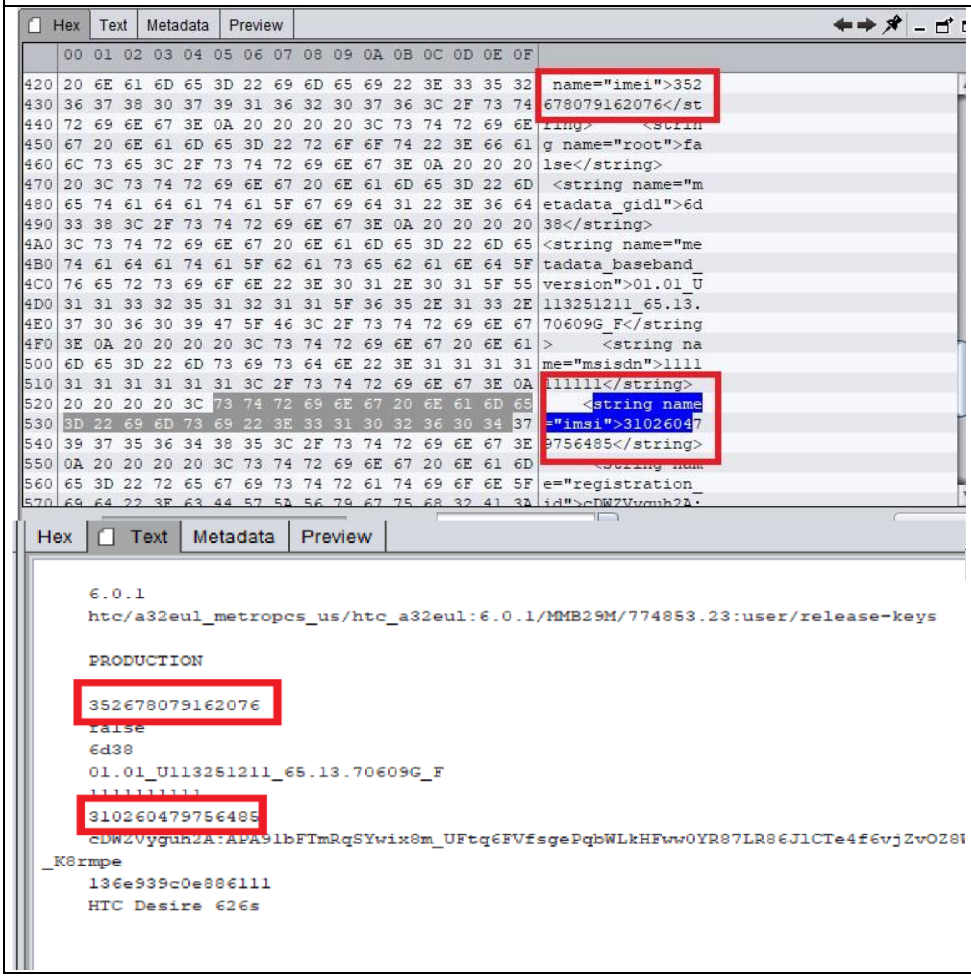
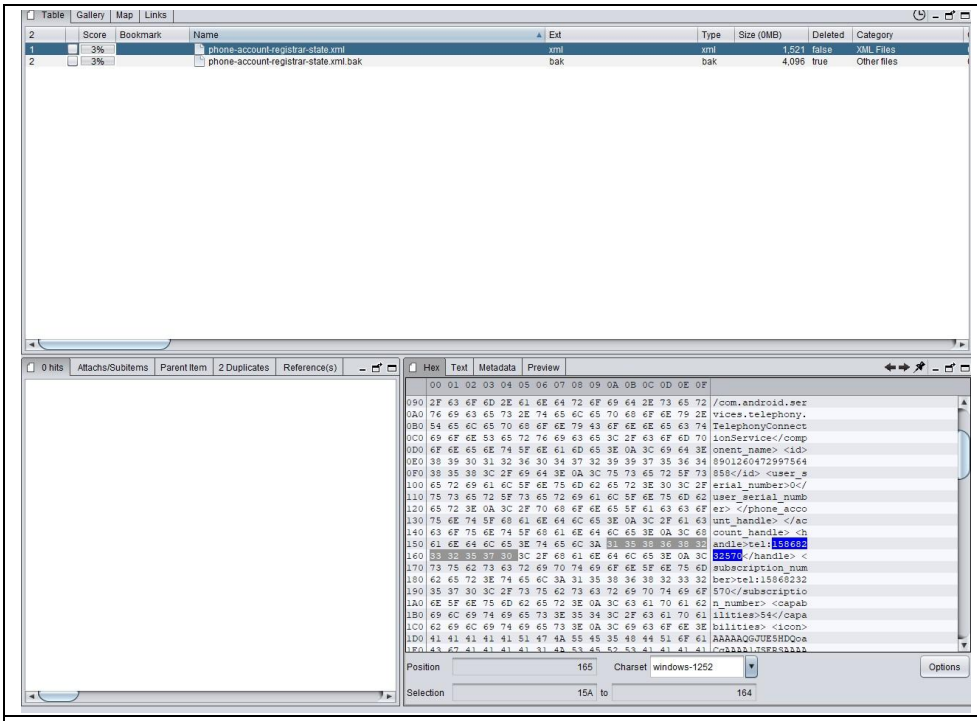


Table 35 Avilla Forensics Analyse: IMEI and IMSI

Phone Number
Evidence: Phone number
Folder: /vol66/com.android.server.telecom/files/phone-account-registrar-state.xml



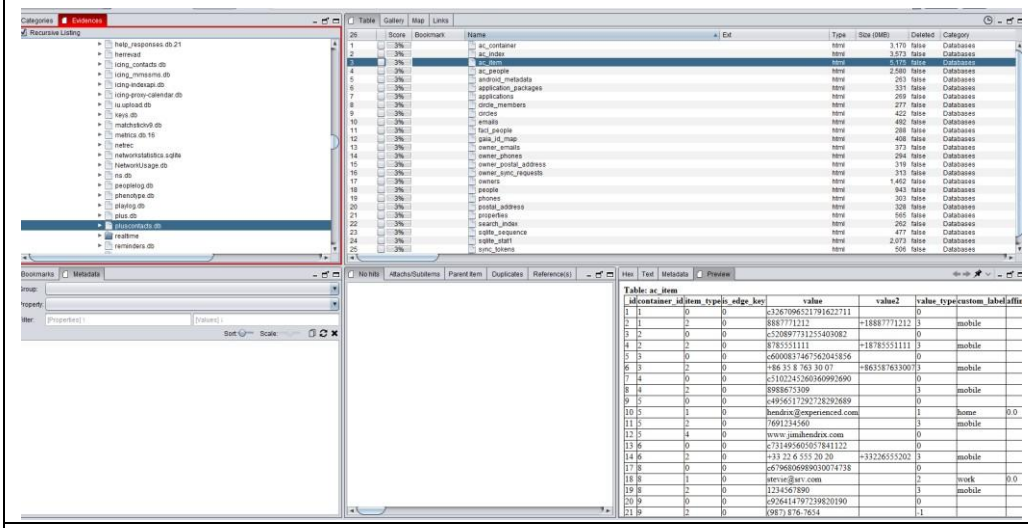
Output

Table 36 Avilla Forensics Analyse: Phone number

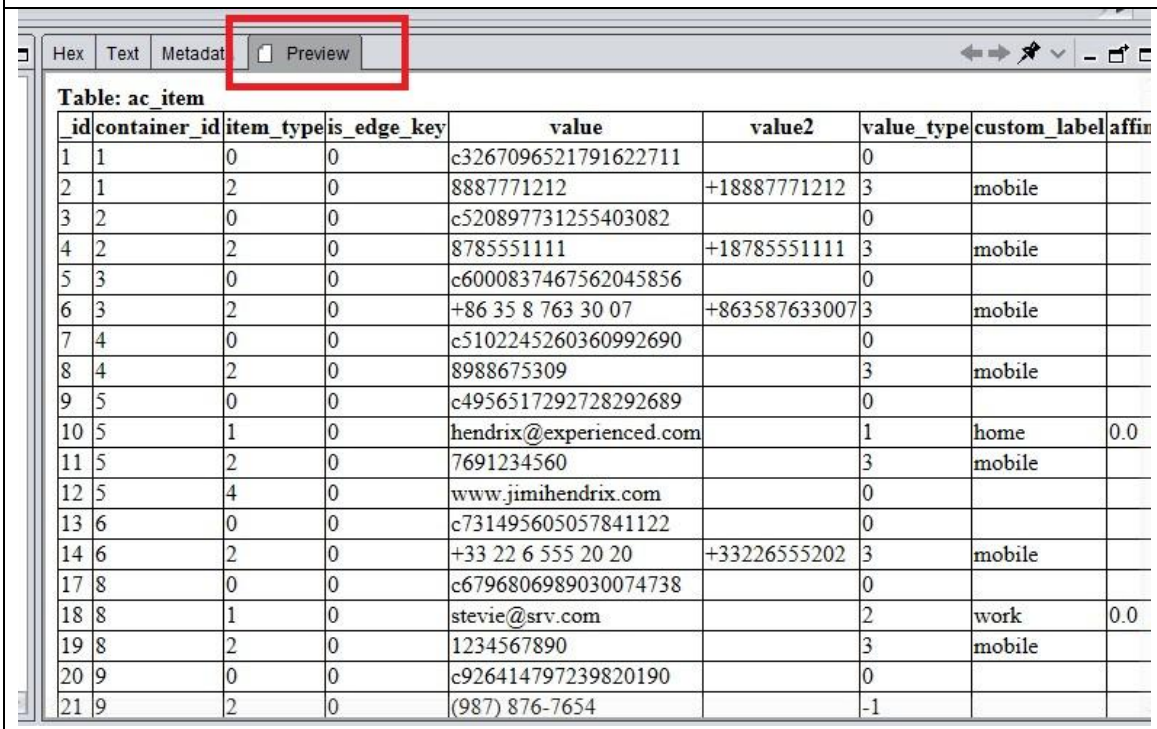
Contacts

Evidence: Plus Contacts and contacts2.db

Folder: /vol66/data/com.google.android.gms.databases//vol66/data/com.android.providers.contacts/databases



Output: Extraction of one database containing contacts such as e-mails and mobile numbers



Hex | Text | Metadat | Preview

Table: ac_item

_id	container_id	item_type	is_edge_key	value	value2	value_type	custom_label	affin
1	1	0	0	c3267096521791622711		0		
2	1	2	0	8887771212	+18887771212	3	mobile	
3	2	0	0	c520897731255403082		0		
4	2	2	0	8785551111	+18785551111	3	mobile	
5	3	0	0	c6000837467562045856		0		
6	3	2	0	+86 35 8 763 30 07	+8635876330073	mobile		
7	4	0	0	c5102245260360992690		0		
8	4	2	0	8988675309		3	mobile	
9	5	0	0	c4956517292728292689		0		
10	5	1	0	hendrix@experienced.com		1	home	0.0
11	5	2	0	7691234560		3	mobile	
12	5	4	0	www.jimihendrix.com		0		
13	6	0	0	c731495605057841122		0		
14	6	2	0	+33 22 6 555 20 20	+33226555202	3	mobile	
17	8	0	0	c6796806989030074738		0		
18	8	1	0	stevie@srv.com		2	work	0.0
19	8	2	0	1234567890		3	mobile	
20	9	0	0	c926414797239820190		0		
21	9	2	0	(987) 876-7654		-1		

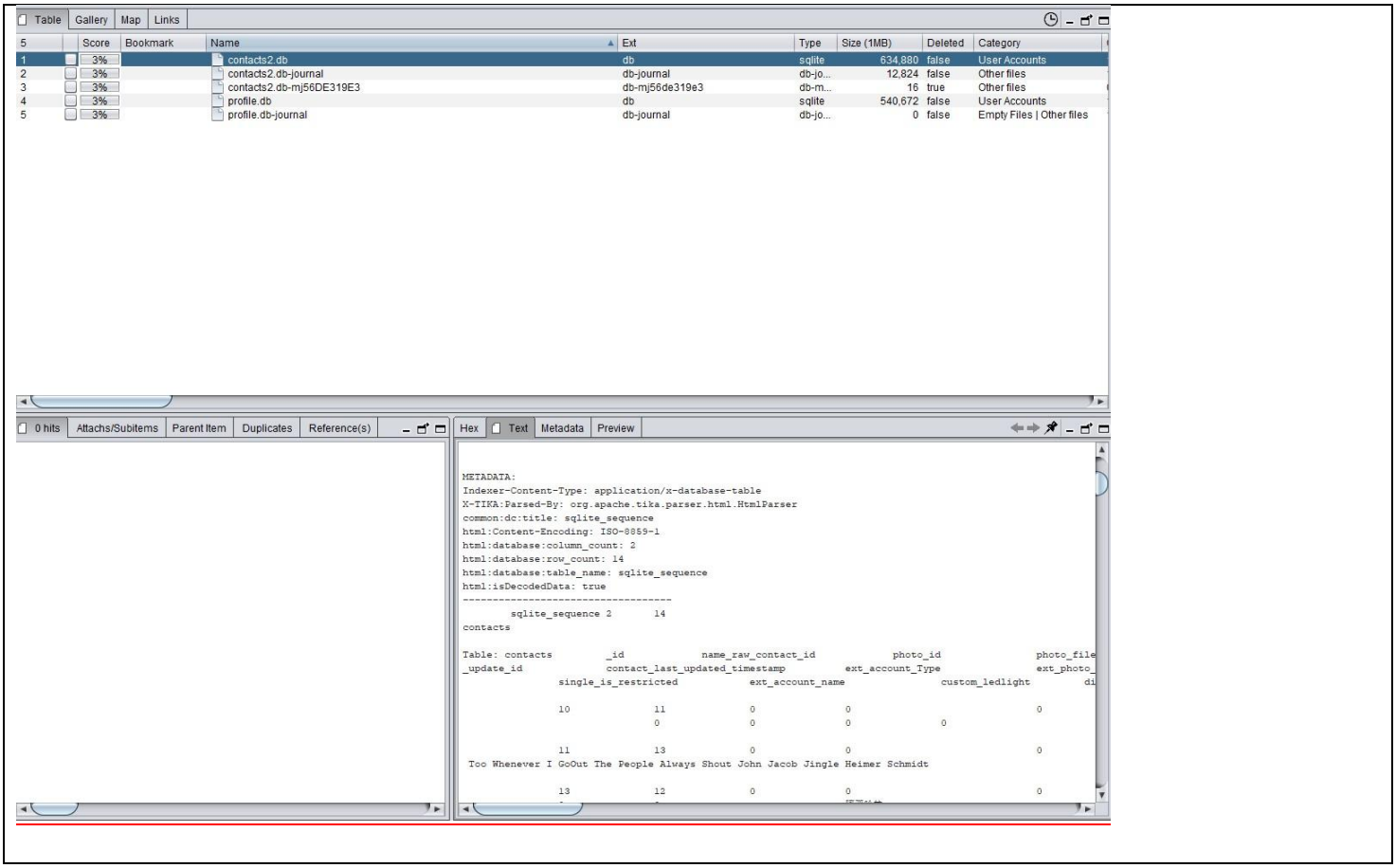


Table 37 Avilla Forensics Analyse: Plus contacts and Contacts2 database

SMS and MMS
Evidence: SMS and MMS
Folder: vol66/data/com.android.providers.telephony/databases/mmssms.db/words

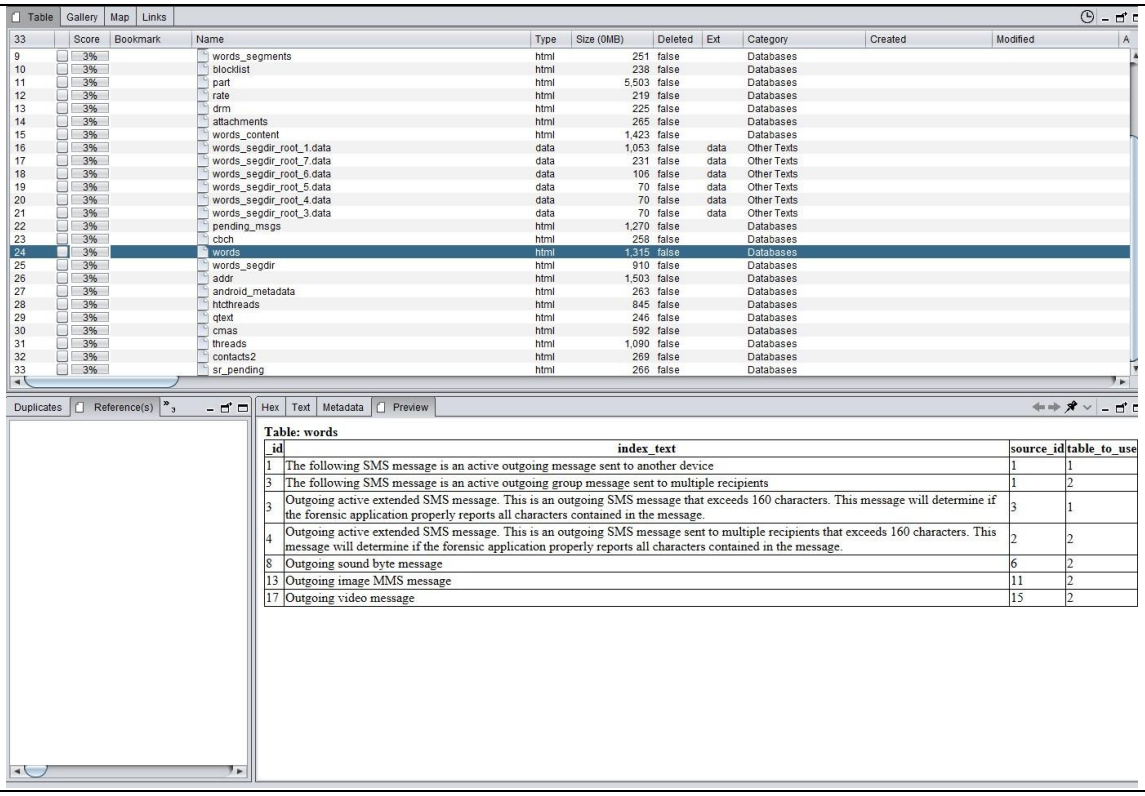


Table: words

id	index_text	source_id	table_to_use
1	The following SMS message is an active outgoing message sent to another device	1	1
3	The following SMS message is an active outgoing group message sent to multiple recipients	1	2
3	Outgoing active extended SMS message. This is an outgoing SMS message that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.	3	1
4	Outgoing active extended SMS message. This is an outgoing SMS message sent to multiple recipients that exceeds 160 characters. This message will determine if the forensic application properly reports all characters contained in the message.	2	2
8	Outgoing sound byte message	6	2
13	Outgoing image MMS message	11	2
17	Outgoing video message	15	2

Output: Outgoing text messages and MMS. In the same database, a table with pending messages can also be exported

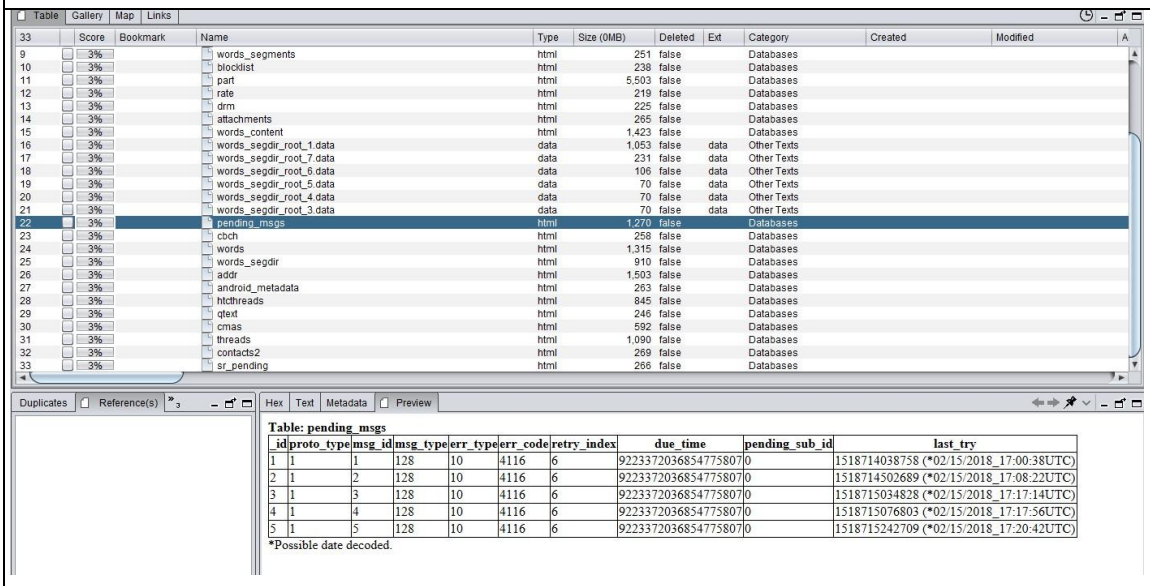


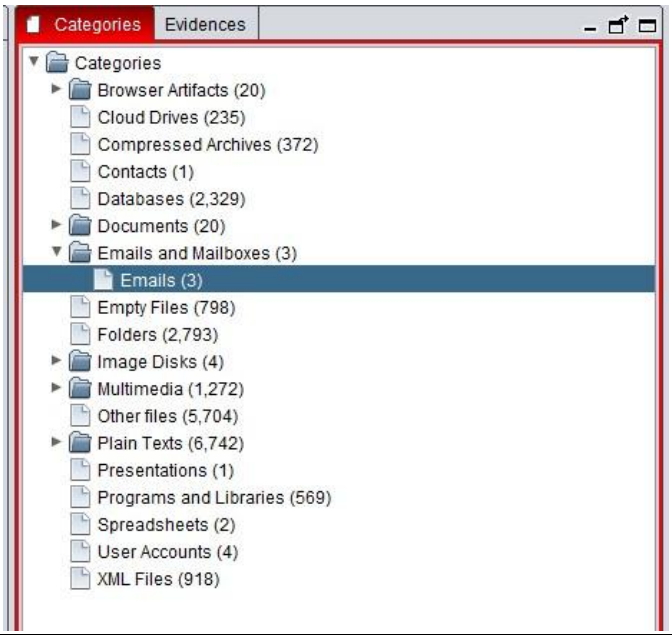
Table: pending_msgs

_id	proto_type	msg_id	msg_type	err_type	err_code	retry_index	due_time	pending_sub_id	last_try
1	1	1	128	10	4116	6	92233720368547758070	0	1518714038758 (*02/15/2018_17:00:38UTC)
2	1	2	128	10	4116	6	92233720368547758070	0	1518714502689 (*02/15/2018_17:08:22UTC)
3	1	3	128	10	4116	6	92233720368547758070	0	1518715034828 (*02/15/2018_17:17:14UTC)
4	1	4	128	10	4116	6	92233720368547758070	0	1518715076803 (*02/15/2018_17:17:56UTC)
5	1	5	128	10	4116	6	92233720368547758070	0	1518715242709 (*02/15/2018_17:20:42UTC)

*Possible date decoded.

Table 38 Avilla Forensics: SMS and MMS

E-mails
Evidence: E-mails
Folder: under categories



Output: Outgoing text messages and MMS. In the same database, a table with pending messa

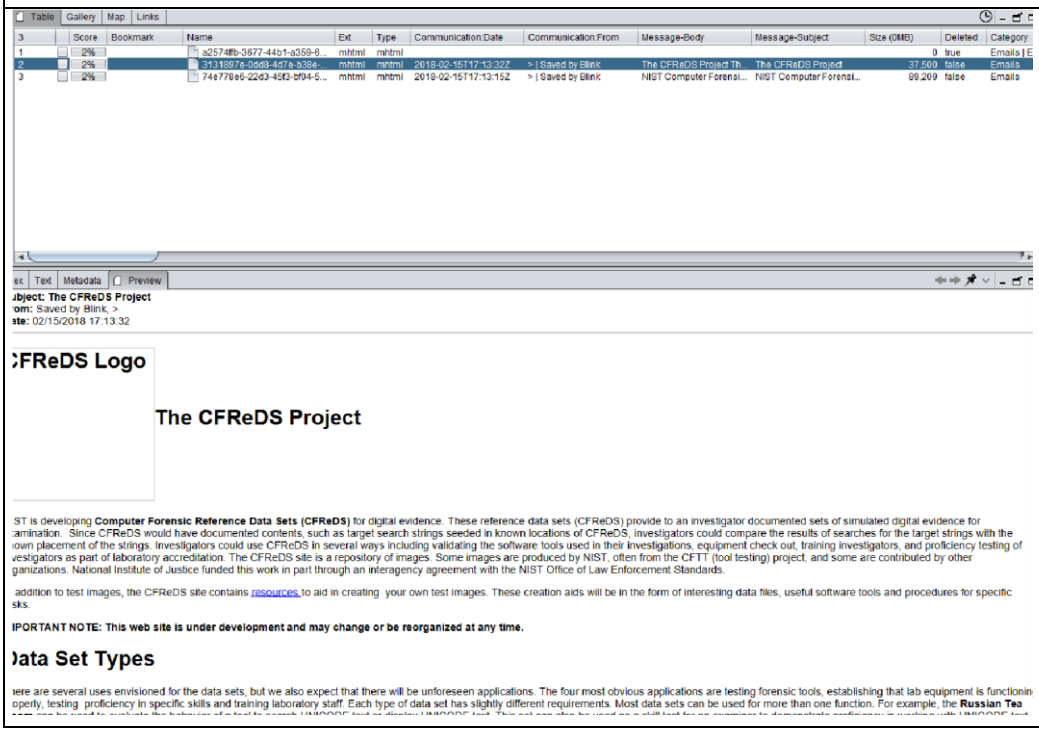
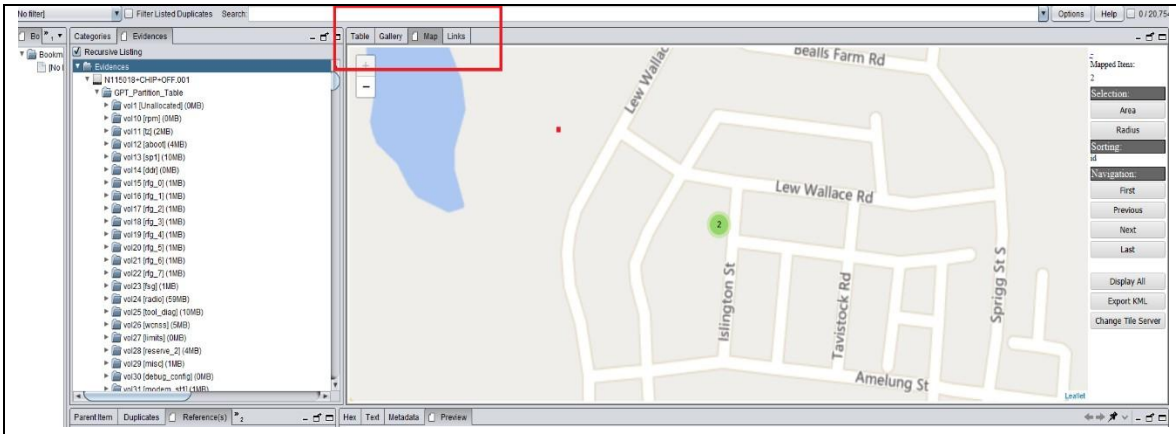
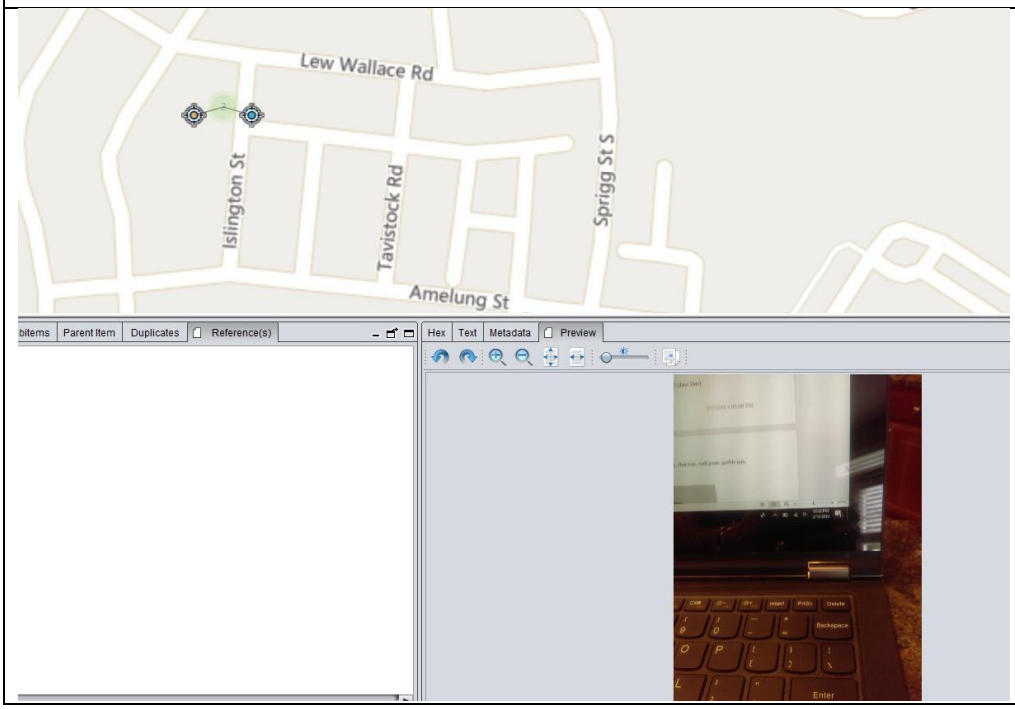


Table 39 Avilla Forensics: E-mails

GPS
Evidence: GPS
Folder: under categories



Output: By clicking on the pinpoint, this will split into 2 geolocations revealing two images associated with that location



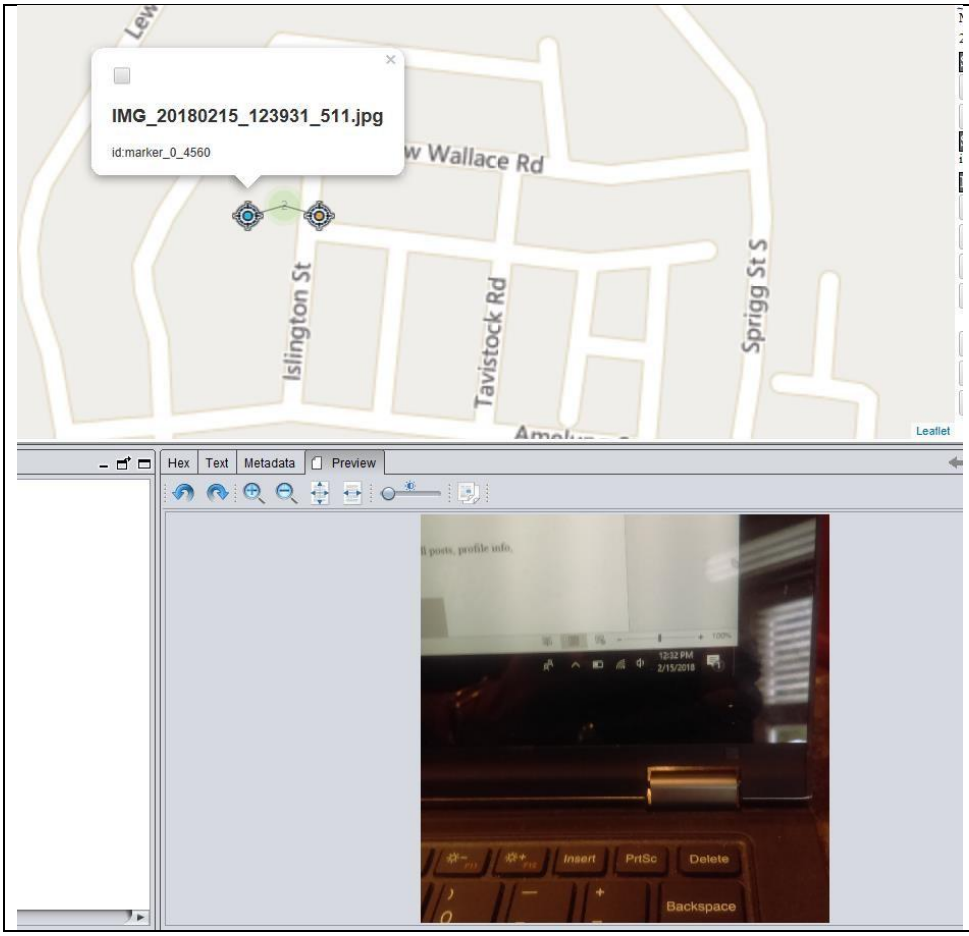


Table 40 Avilla Forensics: GPS

Deleted Files
Evidence: Deleted Facebook and Twitter cache
Folder: Filter can be created for all the deleted files

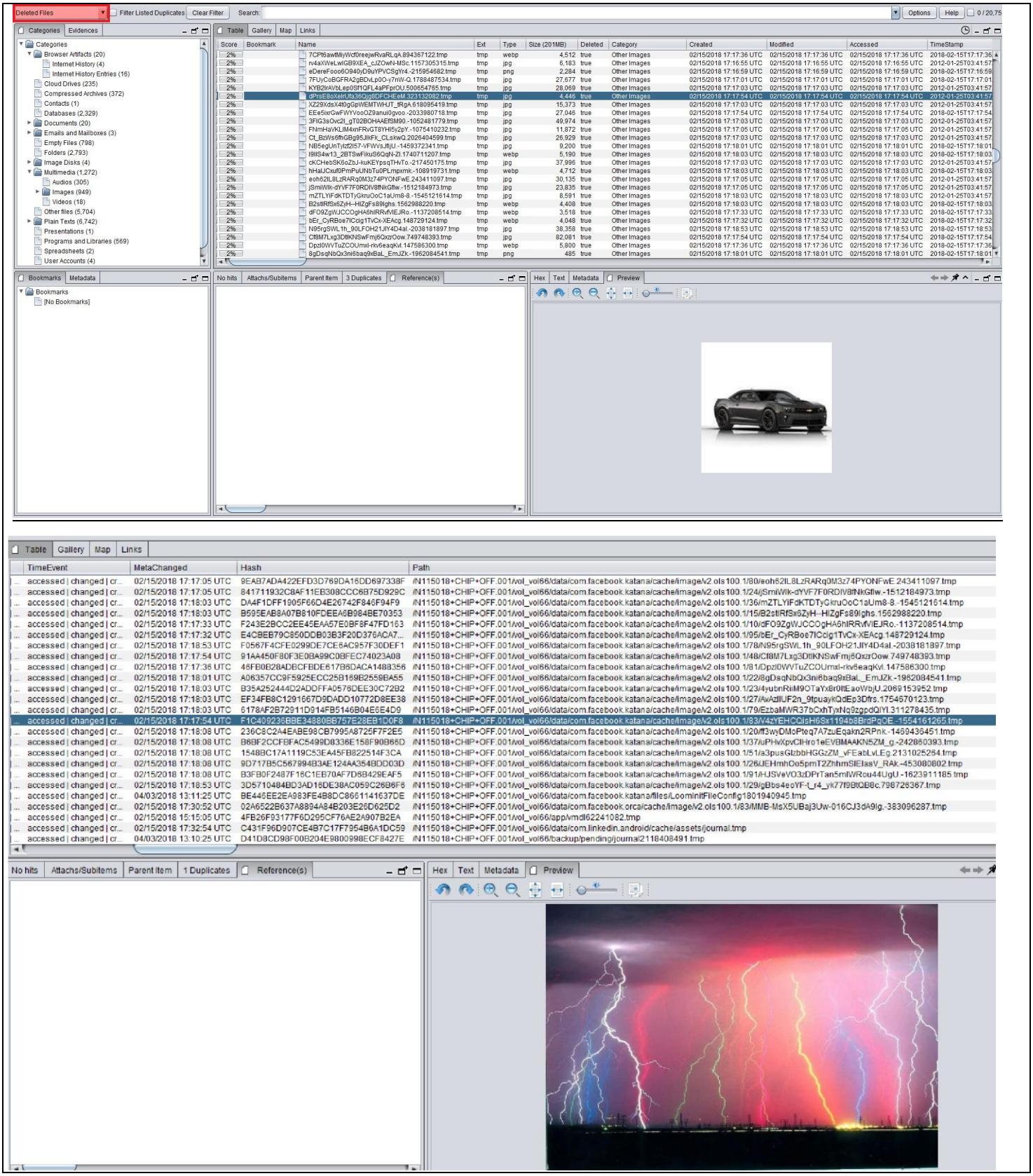


Table 41 Avilla Forensics: Deleted Files

9.0 Comparison of Results

In the field of digital and mobile forensics, it is essential the analysis and comparison of results of different forensic tools. This can ensure the trustworthiness of the procedure; the tool was first used for the analyse of data and the accuracy of the mobile forensic investigator. As such, for the comparison of results, both tools were compared in terms of functionality and user interface, support, and compatibility.

The data was analysed in two different tools, the objective of this action is to identify any inconsistencies in the results of the analysis. To conclude this research, the MD5 of the dataset was created through the command line and through Avilla Forensic's hash calculator and compared.

9.1 Tools

Both Autopsy and Avilla Forensics are open-source tools that do not require any sort of subscription or fee. Although, Avilla Forensics is a tool that is still being developed and users can provide monetary support towards this project through donations. It was identified during this research three types of measurements of comparison for Autopsy and Avilla Forensics:

1. **Compatibility:** While Autopsy works in a wide range of operating system such as Linux, Windows and MacOS. Avilla can only be launched in a Windows 10 or Windows 11 host. In terms of what type of data sources can these two tools analyse, Autopsy has the capability to perform analysis beyond mobile devices, such as Hard-drives, File systems, memory dumps and even Windows registry hives. While Avilla Forensics is a workstation purely designed for the analyse of mobile devices. In his current state, the workstation is mainly developed for the analyse of Android devices, although there are some tools integrated in the workstation to perform iOS collections.
2. **Support:** Autopsy was first released in 2008 and became popular throughout the years and the community for autopsy has grown. It became an extremely popular tool for digital forensics. This resulted in communities developing their own support system for any type of troubleshooting related to the tool. While Avilla Forensics is a recent workstation that is still being developed, it is not as well known in the Digital Forensics field like Autopsy is. Therefore, the support for Autopsy, at the moment, is much bigger than Avilla Forensics.
3. **User interface and functionality:** Both tools are user friendly due to their intuitive layouts as both provide GUI interfaces. Although, during this research, Autopsy seemed

to have a much cleaner and less heavy layout compared to Avilla Forensics. In terms of loading of the data for analysis, Autopsy was much quicker to load the results. While with Avilla every change of file in the IPED, required the tool to load the results causing a slight delay during the analysis.

While Autopsy is one tool with many capabilities for extraction and analyse of data, Avilla Forensics is a conjunction of different open-source tools such as SQLite, ADB, .tar converter, Hash calculator, and many others. Unlike Autopsy, Avilla does not require installation on the host, making it a light workstation and a perfect tool for computers with lower hardware capabilities. This was seen during the analysis of the dataset in Proxmox, as there was a limitation of hardware in the host machine which caused some slowness in Autopsy. While this was not felt during the analysis using Avilla Forensics as this workstation was much more lightweight than Autopsy.

9.2 Data

The comparison of the found data is an essential step towards the integrity of the investigation results but also towards the use of open-source tools to conduct simple investigations. As seen in the results above and *Table 42* most of the extracted data was found during the analyse on both tools. Although, some discrepancies were also found, such as the lack of capability to locate the call logs and outgoing tweets, and the extra image and Geo-location found in Avilla Forensics.

Although these discrepancies exist, both tools could analyse the same data and obtaining the same results, showing that students can use two open-source tools such as Avilla Forensics and Autopsy to obtain and learn more about the dual-verification process.

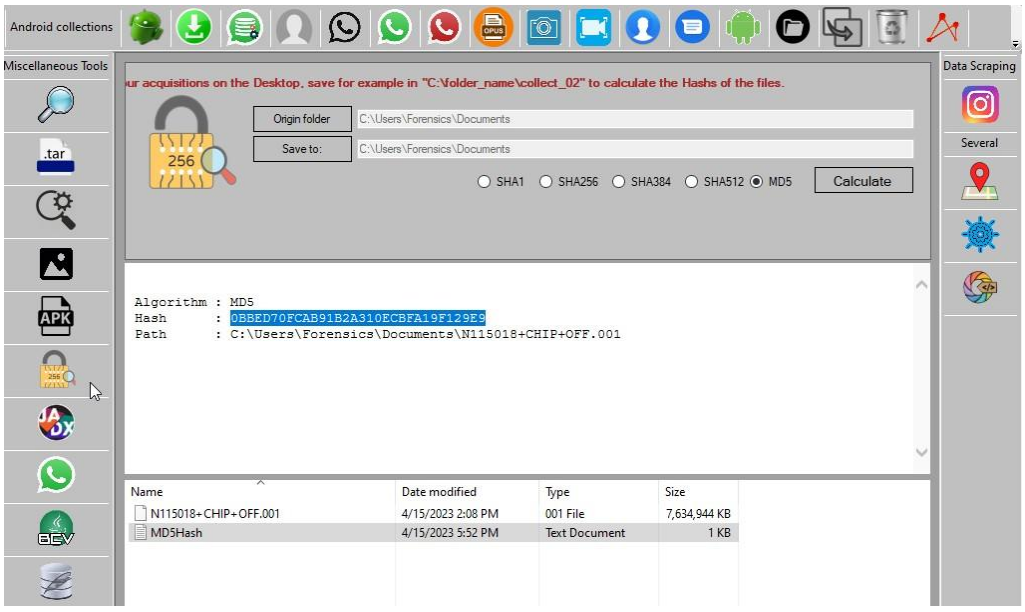
Artifact type	Avilla Forensics	Autopsy	Note
Device Model	✓	✓	
IMEI and IMSI	✓	✓	
Phone Number	✓	✓	
Plus Contacts	✓	✓	
Contacts database	✓	✓	
Call Logs		✓	Call logs in Avilla Forensics were not located
SMS/MMS	✓	✓	

Web History	✓	✓	
Google Quick search	✓	✓	
E-mails	✓	✓	
Attachments	✓	✓	
GPS	✓	✓	Avilla found 2 geolocations with 2 different images associated to it. Although, Autopsy only found one image
Deleted Files	✓	✓	
Application based evidence - Twitter		✓	Tweet folder was not located in Avilla Forensics

Table 42 Comparison of results

9.3 MD5

Dual verification is the process of verifying the accuracy and integrity of the extracted data. This process assures that the investigators can enhance the credibility of the findings done through the investigation of the mobile device. This can be achieved through the creation of the MD5 of the file through both tools and comparing it. Although, Autopsy does not provide a hash calculator, therefore, the MD5 was created using the certutil tool in the command line. While Avilla Forensics provides a hash calculator tool. *Table 43* provides the steps taken to create the MD5 for both tools and comparing them at the end.



Creating the hash calculator in Avilla Forensics is an extremely quick process. Once the dataset image is imported, the tool creates a Text document with the MD5 but it also shows the hash in the tool itself.

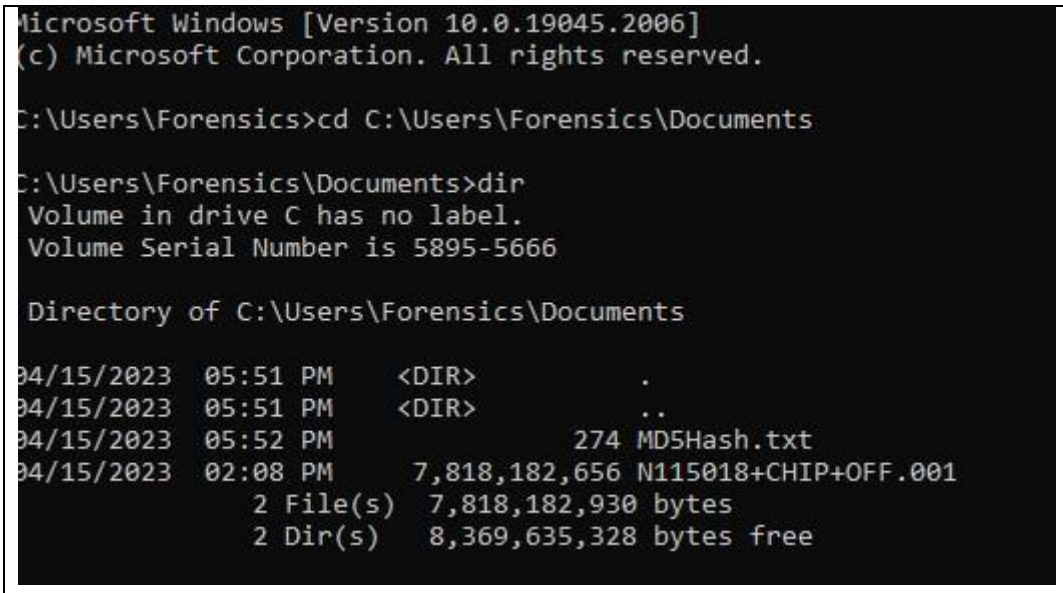
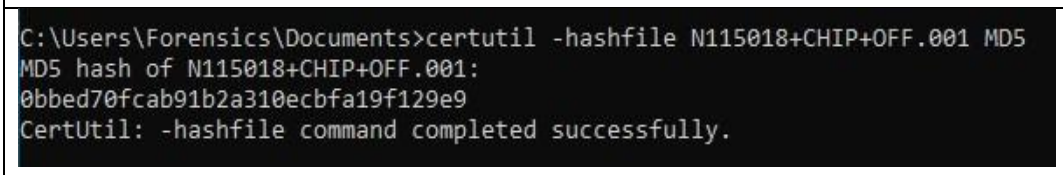
<table>
<tr><td> 
</td><td>One of the options to create the MD5 for comparison is through the Command Line in Windows. Users must navigate to the folder using the CD command.</td></tr>
<tr><td> 
</td><td>Once users are in the correct folder containing the dataset, the certutil tool can be used to create the MD5. This is done using the following command: certutil -hashfile <filename.extension> MD5</td></tr>
<tr><td colspan="2">As observed, both MD5 contain matching hash values. This assures that the data extracted and to be analysed through both tools contains the same information, this not only adds an extra layer of credibility to the findings but also reinforces the integrity of the investigation.</td></tr>
</table>

Table 43 Dual Verification

10.0 Conclusion

In conclusion, this study has highlighted the importance of having trained mobile forensics investigators and how open-source tools can provide students with insight of how to begin a mobile device investigation, an understanding of the data hierarchy and where to look for the required data.

These tools can be essential for very basic training on how to perform an investigation and they can incentive students and mobile forensics enthusiasts, these tools must also be compared with a commercial tool used by law enforcements to assess the main differences and to assess how much of the knowledge gain is transferable into the commercial tools.

As seen during this research, there is a lack of resources for mobile forensics labs for students, therefore, this guide composed by the creation of a sterile environment and dual-verification using two different tools for the analyse of a dataset provided by NIST is a step forward in the creation of more guide solely dedicated to mobile forensics analysis.

10.1 Summary of Project

During the research for the literature review, it was seen that mobile forensics is the most recent field in the Digital Forensics branch, therefore, there is a lack of guides for this field but also due to the constant development of technology, it becomes a complex and slow task to create consistent labs for students to follow. Although, there is an abundant amount of opensource tools that can provide students with the ability to perform basic mobile forensic analysis and gain knowledge through them. Therefore, two tools were used for this purpose.

During the literature review, research was made on the different types of tools, the decision was based of in popularity and tool functionality. Autopsy was the chosen tool due to its popularity and community size. While, Avilla Forensics, a more recent workstation and less known, was chosen due to its versatility and user interface.

The methods used for this research were also based in the creation of a sterile environment using Virtual machines to avoid any modification or hindrance of the data being analysed. This also creates a fully dedicated environment solely with the purpose for mobile forensic investigations. The creation of these sterile environments was seen in many Digital Forensics research papers for institutional purposes.

Using the inspiration of such research papers, two types of environments were created with the use of VirtualBox and Proxmox. These open-source hypervisors were chosen due to their capabilities offered to the user even as a free tool. By having the two types of hypervisors available, allows the student to make a decision as to which hypervisor best applies to their needs. This can also motivate the student to further purse the addition of more mobile forensics labs into their own virtual environment, but to also further analyse much more complex datasets.

Due to its popularity and being the most familiarized operating system being used in the moment of this research, Windows 10 will be the chosen operating system to be deployed into the virtual machines.

Therefore, due to the already daunting task of learning the complexity of a mobile forensic analyse, it was decided that allowing the user to work on an environment already familiarized with was the best choice.

As this is a step-by-step guide of a mobile forensics analyse, it was essential that the data being analysed in this research was also made available to the user. Therefore, the dataset was an image provided by NIST. The chosen dataset was also based on the device's operating system. As seen during this research, Android is currently the most used Operating system in a mobile device, with the possibility of making other O.S such as Blackberry and Windows obsolete. It was also seen that Android could possibly be implemented in other day-to-day devices such as cars, televisions, GPS units and game consoles, therefore, increasing the capability of analysis on an Android device will become an essential skill in the future.

This research provides the steps on how to install each tool, the layouts, and how to import the data into to the tools for analyse. These tools are then compared based of functionality, user interface and compatibility. As an example, it was seen that Autopsy is currently a much heavier tool compared with Avilla Forensics, therefore, for computers with lower hardware capabilities can run Avilla Forensics without issues as this workstation does not require installation. This workstation also provides multiple tools that are fully dedicated to Android device analysis, although, user must also be aware that this tool is still under development.

In the comparison of data, the model, IMEI, IMSI, call logs, contacts, SMS and MMS, e-Mails, GPS can be found in the analyse of both tools. This shows that the use of open-source tools can be used for further education on mobile forensics, although the learnt skills must be compared with the skills learn using a commercial tool.

The main limitation found in this research were the lack of datasets with the most recent mobile device operating systems to use in comparison with the dataset used in this paper. A preferred android device could have been used to perform an extraction of data using both tools, although due to the given time limit, this was not possible and therefore, not included in this research.

10.2 Future works

For future works and addition to the composition of a mobile forensics' lab for students, this would include the creation of a dataset formed by the most recent versions of Android in a recent mobile device. This would be used to compare different models and how the Android

file hierarchy changes according to the version of Android, the make of the device and the model.

Although only Windows 10 was used in the creation of this guide, it is also essential that future investigators are trained in Linux systems, as Android being Linux-based. Therefore, the addition of Linux Operating system to the testing environment and the creation of Linux labs would massively increase students' knowledge on the different types of Operating Systems.

To conclude this section and highlighting the lack of datasets, one of the objectives would be the creation of an approved dataset for NIST and making it available for anyone interest in mobile forensics investigation to download it and perform the analyse themselves.

References

Abdulalem Ali, S. A. R. S. H. O. A. M. F. S., April, 2017. *A metamodel for mobile forensics.* [Online]
Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0176223
[Accessed 16 March 2023].

Anand, February 2021. *Proxmox vs ESXi: 9 Compelling reasons why my choice was clear.* [Online]
Available at: https://www.smarthomebeginner.com/proxmox-vs-esxi/ [Accessed
25 March 2023].

Avilla, D., N.D. *Avilla Forensics.* [Online]
Available at: https://github.com/AvillaDaniel/AvillaForensics [Accessed
17 February 2023].

Carrier, B., N.D. *Autopsy.* [Online]
Available at: https://www.sleuthkit.org/autopsy/ [Accessed
17 February 2023].

Carrier, B., N.D. *The Sleuth Kit.* [Online]
Available at: https://www.sleuthkit.org/sleuthkit/docs.php [Accessed
17 February 2023].

Costa, C. d. S., 2018. *Pericia Forense em Dispositivos moveis, estudo de caso: Smartphone moto G6 com Android 8.0.* [Online]
Available at: https://dspace.doctum.edu.br/bitstream/123456789/249/1/TCC%20-%20C%c3%8dCERO%20DE%20SALES%20COSTA.pdf
[Accessed 24 February 2023].

Craig Wilson, July 2011. *Digital Evidence Discrepancies – Casey Anthony Trial.* [Online] Available at: https://www.digital-detective.net/digital-evidence-discrepancies-casey-anthonytrial/
[Accessed 29 January 2023].

Crull, C., January 2022. *Budget Proxmox Server for Homelabs.* [Online]
Available at: https://www.storagereview.com/review/budget-proxmox-server-for-homelabs
[Accessed 14 April 2023].

Cyberstart, N.D. *Installing and setting up VirtualBox (Intel Mac and Windows users).* [Online]
Available at: https://help.cyberstart.com/help/installing-and-setting-up-virtualbox-intel-macusers
[Accessed 24 February 2023].

Derek Bem, E. H., 2007. *Computer Forensics Analysis in a Virtual Environment.* [Online]
Available at:
https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=068a0bda4f62d3447947800c2630b09893c69a62
[Accessed 18 March 2023].

Forensics, M., N.D. *MAGNET RAM Capture.* [Online]
Available at: https://www.magnetforensics.com/resources/magnet-ram-

capture/#:~:text=Evidence%20that%20can%20be%20found,on%20the%20local%20hard%20disk.
[Accessed 12 April 2023].

Forensics, O., May 2020. *OXygen Forensics Viewer: See it all, wherever you are.* [Online]
Available at: https://blog.oxygen-forensic.com/oxygen-forensic-viewer-see-it-all-whereveryou-are/
[Accessed 17 February 2023].

Francesco Servida, N.D. *Samsung Galaxy S10 - Android 10 (DFRWS 2021).* [Online] Available at:
https://cfreds.nist.gov/all/FrancescoServida%2FDFRWS/SamsungGalaxyS10Android10DFRWS2021
[Accessed 16 March 2023].

GitHub, N.D. *IPED.* [Online]
Available at: https://github.com/sepinf-inc/IPED [Accessed
14 April 2023].

Hiley, C., February 2023. *UK mobile phone statistics, 2023.* [Online]
Available at: https://www.uswitch.com/mobiles/studies/mobile-statistics/#uk-mobile-phoneuser-statistics
[Accessed 13 February 2023].

Hongmei Chi, E. L. J. C. C. a. D. E., N.D. *Design and Implementation of Digital Forensics Labs: A case study for teaching digital forensics to undergraduate students.* [Online] Available at: http://www.elearning.famu.edu/cis/year2009-Chi-Jones-etal-CATE.pdf [Accessed
20 February 2023].

Hoog, A., July 2011. *Android FOrensics: Investigation, Analysis and Mobile Security for Google Android.* Rockland: Elsevier Science & Technology Book.

Hoog, A., May 2014. *iPhone and iOS forensics: Investigation, analysis and mobile security for Apple iPhone, iPad and iOS Devices.* Waltham: Syngress.

Horsman, G., February 2019. *Tool testing and reliability issues in the field of digital forensics.* [Online]
Available at: https://pdf.sciencedirectassets.com/273059/1-s2.0-S1742287618X00085/1-s2.0-S1742287618303062/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEIH%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJGMEQCIFhSVHe8VUAnYlqjdAkTEuwcTDhOZgt8vTA9tcsV6XI9AiA9LziWboRoRqyd [Accessed 18 March 2023].

Infosec, April 2018. *Android Penetration Tools Walkthrough Series: Androguard.* [Online]
Available at: https://resources.infosecinstitute.com/topic/android-penetration-toolswalkthrough-series-androguard/ [Accessed 17 February 2023].

ISO standards, N.D. *ISO/IEC 17025 testing and calibration laboratories.* [Online]
Available at: https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html
[Accessed 30 January 2023].

Jahan Hassan, A. D. B. R., August 2022. *Virtual Laboratories in Tertiary Education: Case Study Analysis by learning theories.* [Online]
Available at: https://www.mdpi.com/2227-7102/12/8/554 [Accessed 18 March 2023].

Jeff Lessard, G. K., January 2010. *Android forensics: Simplifying cell phone examinations.* [Online]
Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7480&context=ecuworks [Accessed 13 February 2023].

Kevin S. Floyd, J. Y., April 2014. *Development of a Digital Forensics Lab to support active learning.* [Online]
Available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=sais2014 [Accessed 18 February 2023].

Khushi Gupta, A. N. N. S. C. V., June 2022. *Digital Forensics Lab Design: A Framework.* [Online]
Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9800799 [Accessed 18 February 2023].

Lozenzo Martignoni, R. P. G. F. R. D. B., July 2010. *Testing system virtual machines.* [Online]
Available at: https://dl.acm.org/doi/pdf/10.1145/1831708.1831730 [Accessed 16 March 2023].

Mark Scanlon, X. D. D. L., January 2017. *EviPlant: An efficient digital forensic challenge creation, manipulation.* [Online]
Available at: https://arxiv.org/ftp/arxiv/papers/1704/1704.08990.pdf [Accessed 18 March 2023].

Maxim Chernyshev, S. Z. Z. B. A. A. W., November 2017. *Mobile Forensics: Advances, challenges, and research opportunities.* [Online]
Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8123468 [Accessed 29 January 2023].

Mobile Forensics Solution, N.D. *Chip-Off Examinations.* [Online] Available at: http://mobileforensicsolutions.tech/chip-off-examinations/ [Accessed 17 February 2023].

Mohammed Moreb, S. S. B. A., March 2023. *A Novel Framework for Mobile FOrensics Investigation Process.* [Online]
Available at: https://assets.researchsquare.com/files/rs-2611927/v1/d45fcf81-88f7-43ff-b8a28cdf0e50bc53.pdf?c=1678288076 [Accessed 18 March 2023].

MSAB, N.D. *Technological innovations and the road ahead for mobile forensics.* [Online]
Available at: https://www.msab.com/reports/technological-innovations-and-the-road-aheadfor-mobile-forensics/
[Accessed 13 February 2023].

NIST, N.D. *What is CFReDS?.* [Online] Available at: https://cfreds.nist.gov/ [Accessed 24 February 2023].

O' Reilly, N.D. *Micro read.* [Online]
Available at: https://www.oreilly.com/library/view/practical-mobileforensics/9781788839198/ac5758e4-e433-46e9-b396-c5cd29638a82.xhtml [Accessed 17 February 2023].

Oracle, N.D. *Oracle VM VirtualBox.* [Online]
Available at: https://www.oracle.com/uk/virtualization/virtualbox/ [Accessed 12 April 2023].

Owen Bowcott, May 2018. *Police mishandling digital evidence, forensic experts warn.* [Online]
Available at: https://www.theguardian.com/law/2018/may/15/police-mishandling-digitalevidence-forensic-experts-warn [Accessed 2 February 2023].

Petroc Taylor, February 2023. *Windows operating systems market share of desktop PCs worldwide 2017-2023.* [Online]
Available at: https://www.statista.com/statistics/993868/worldwide-windows-operatingsystem-market-share/#:~:text=Windows%2010%20is%20the%20most,around%2018%20percent%20of%20devices.
[Accessed 12 April 2023].

PhoenixTS, January 2016. *Incident Response Tools: FTK for Linux.* [Online] Available at: https://phoenixts.com/blog/forensics-tools-ftk-linux/#:~:text=Yes%2C%20you%20can%20opt%20for,searching%2C%20and%20its%20carving%20abilities.
[Accessed 17 February 2023].

Privacy International, OCtober 2019. *A technical look at Phone Extraction.* [Online]
Available at: https://privacyinternational.org/long-read/3256/technical-look-phone-extraction
[Accessed 17 February 2023].

Proxmox, N.D. *System requirements.* [Online]
Available at: https://www.proxmox.com/en/proxmox-ve/requirements [Accessed 24 February 2023].

Quigley, E., N.D. *ADDIE: 5 Steps To Effective Training.* [Online] Available at: https://www.learnupon.com/blog/addie-5-steps/ [Accessed 19 March 2023].

Radhika Padmanabhan, K. L. M. G. D. S. M. S., March 2017. *Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools.* [Online]
Available at: https://ieeexplore.ieee.org/document/7880238 [Accessed 18 March 2023].

Rick Ayers, Sam Brothers, Wayne Jansen, May, 2014. *Guidelines on Mobile Device Forensics.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf
[Accessed 29 January 2023].

Ritika Lohiya, P. J. P. S., May 2015. *Survey on Mobile Forensics.* [Online] Available at:

https://www.researchgate.net/publication/277907742_Survey_on_Mobile_Forensics [Accessed 17 February 2023].

Rivera, P. J. A., N.D. *Mobile Digital Forensic Tool using Santoku Linux.* [Online] Available at: https://prcrepository.org/xmlui/bitstream/handle/20.500.12475/401/Articulo%20Final_Pedro%20Acevedo.pdf?sequence=1&isAllowed=y [Accessed 24 February 2023].

Rune Nordvik, R. S. K. F. S. A. F. T., May 2021. *Reliability validation for file system interpretation.* [Online] Available at: https://reader.elsevier.com/reader/sd/pii/S2666281721000822?token=8C87F91CBA27CAE7AFFCE985C7028FBC26BA0151B03E244A61975F4C20BBAA0E867744590ABDB353639394478DD97E15&originRegion=eu-west-1&originCreation=20230318205714 [Accessed 18 March 2023].

Satish Bommisetty, R. T. H. M., July 2014. In: M. H. A. S. Sarang Chari, ed. *Practical Mobile Forensics.* Birmingham: Packt Publishing, p. 167.

Satish Bommisetty, R. T. H. M., July 2014. Practical Mobile Forensics. In: M. H. A. S. Sarang Chari, ed. Birmingham: Packt Publishing ltd., p. 12.

Sleuth kit, N.D. *Autopsy User Documentation.* [Online]
Available at: https://sleuthkit.org/autopsy/docs/user-docs/3.1/uilayout_page.html [Accessed 14 April 2023].

Special Counsel, March 2016. *3 Methods of Mobile Device Extractions and the Data each contains.* [Online]
Available at: https://blog.specialcounsel.com/ediscovery/three-types-of-mobile-deviceextractions-and-what-each-contains/ [Accessed 17 February 2023].

Synopsys, N.D. *Fuzz testing.* [Online]
Available at: https://www.synopsys.com/glossary/what-is-fuzz-testing.html#:~:text=Fuzz%20testing%20or%20fuzzing%20is,as%20crashes%20or%20information%20leakage.
[Accessed 16 March 2023].

TechTarget, December 2020. *IMEI (International Mobile Equipment Identity).* [Online]
Available at: https://www.techtarget.com/whatis/definition/IMEI-International-MobileEquipment-Identity
[Accessed 13 April 2023].

Testim, November 2019. *What Is a Test Environment? A Guide to Managing Your Testing.* [Online]
Available at: https://www.testim.io/blog/test-environment-guide/ [Accessed 22 February 2023].

Vissarion Yfantis, April 2020. *What Is a Hypervisor and What Are Its Benefits? | Parallels Explains.* [Online]
Available at: https://www.parallels.com/blogs/ras/hypervisor/ [Accessed 13 April 2023].

XiphCyber, May 2022. *Open-source vs proprietary software: Which is better?.* [Online] Available at: https://xiphcyber.com/articles/open-source-vs-proprietary-software [Accessed 29th January 2023].

Appendices

Appendix A- Academic Poster