ASSIGNMENT 2

CS6503: Digital Forensics

Dr Dax Roberts

Andrew Graff
2231290

Table of Contents

Introduction

Kia ora, in this report I am presented with a real-life case study that involves an interception of a package by NZ Police. The package contained illegal substances that has required a forensic analysis investigation to identify, collect, and prepare to analyse data from multiple electronic sources.

There are two major components of this report; the first component will be a discussion of a methodology I have selected to apply forensic data analysis and an insight into the different phases involved. Further to this component, we will be identifying the different sources of electronic and digital evidence with tools to help assist the collection of data, analysis of data and maintaining integrity.

The second component ventures more thoroughly into our findings of each phase and the undertaking of these methods with a hands-on approach by applying it to the case study. An application of hardware and software tools have been explored in great depth to assist the forensics processes along with supporting documentation and a case summary.

Forensic analysis is a rapidly changing and evolving field with the increased use of mobile devices being a major key evidence for digital forensic examination.

Methodology Discussion

There are several different methodologies for evidence collection an analysis. Digital forensics processes today are still quite familiar to the modern physical forensics given the history and existence of practices long before technology arrived. These approaches have been implemented in our current models of digital forensic analysis. There is an intricate play between physical and digital evidence. “A digital footprint might lead investigators to physical evidence, such as a weapon or a hidden stash of document. Conversely, physical evidence might confirm the authenticity of digital communications” (Das, 2023).

A methodology I have selected for this report is the Digital Forensics Model consisting of five phases. The reason for this selection is because of the various electronic and digital evidence presented for analysis in the case. A specific mobile phone is identified to being a key evidence and likely to be directly involved in the criminal matter. The mobile phone will contain some valuable information for digital forensic analysis with possible leads to better understand the scale of the crime and connections to prevent any further harm.

The phases of this methodology are basic principles that are applied for general digital forensics investigations. Some phases can be recognised in other methodologies. One of the earliest digital forensic methodologies developed was the computer forensic investigative process by Pollitt in 1984.

Pollitt’s methodology consisted of four main phases. These phases were acquisition, identification, evaluation and admission. The sequence of how digital evidence was collected here was to handle it in a way it that it meets reliability and was legally acceptable. These were generally forensic focussed and did not include the preparation, planning aspect as per the methodology we selected for this case.

Pollitt discusses the rapidly growing field of Digital Forensic and is hopeful of the new generation to be “aware of the history and pioneering spirit that propelled the early years”, (Pollitt, 2010).

This adds to my reasoning for selecting the Digital Crime Scene Investigation and the phase of its methodology as follows,

- **Identification** – identifying the electronic/digital devices or resources that contain data. This can be working with clients to gather details of what happened and the evidence for collection.

- **Extraction and Preservation** – Securely storing seized devices in a safe location. Once the device has been obtained, data will be cloned for evidence analysis in the next phase. Duplicating all relevant data and ensuring the integrity of the captured data through tools and techniques.

- **Analysis** – Performing a deep dive (exhaustive investigation) by extracting relevant data and examining any information as evidence. This process can involve data recovery from any deleted, damaged or encrypted files using different techniques.

  Some tools used here would be Autopsy and FTK imager (file or data carving) this software tool can capture, identifying and recovering deleted files. A cryptographic hash value is automatically created to verify image integrity via FTK imager. This will ensure integrity of the data collected to confirm data has not been tampered. Redline is another data integrity tool available to use.

- **Documentation** - A timeline of the sequential steps of what has taken place. A post analysis result outlining the findings of the valuable information extracted and documented in a formal way for clients to understand. This process will visualize the entire investigation and draw conclusions.

- **Presentation** – Formal proceedings commence by using all the information and findings of the investigation to present to those of interest. This will contain discoveries and what is learned to assist with client proceedings.

This methodology is not only helpful for law enforcement agencies, but can also be applied for identifying cyber-attacks, frauds, data leaks for other corporations (ERMProtect Staff, 2024).

After the Digital Crime Scene Investigation phase, a specific report would be developed for our client. This would be a case summary and used by law enforcement agencies and lawyers in the court of law.

“A proper forensic report is not a legal document – it is a technical and scientific document. It does not contain arguments; it contains facts, namely immutable truths found within 1s and 0s of digital evidence” (Garrie, 2016).

Case summary is the most pivotal part of digital forensic examination that will determine the outcome of criminal investigations. It will contain a listing of evidence collected and a detailed description of the evidence. Different types of evidence are commonly computers/laptops or mobile devices. This listed step by step concept is known as the chain of custody.

“Chain of custody is a legal term referring to the order and manner in which physical or electronic evidence in criminal and civil investigations has been handled”, (Longley, 2022).

Once items are descripted, an analysis is performed on the evidence using applicable tools with findings reported. This section will have an inspection of each item artifact, and all the actions involved to perform the analysis.

Timekeeping, troubleshooting, tools etc used in the process with observations recorded and conducted that are all directly relevant to the investigation. As these reports are technical, it will need to be explained in a way that any person could understand.

The case summary document requires formatting, information accuracy of what has been provided, address of the examining organization, case identifiers, dates of report and signed final with also definitions of any acronyms or abbreviations used. Figures and tables include a caption numbering.

Case Study Application

The Police have provided the below details of the situation. A digital forensic investigation is prompted due to a package containing illegal substances addressed to one of the residences of the flat. As a digital forensic analyst, an examination is required for an analysis on the electronic/digital evidence.

It is initially analysed that the key evidence is a mobile phone owned by the direct recipient of the package.

- ***Flat of 5 students not studying cyber security***
- ***Each flat mate lockable bedroom (laptop or desktop per room)***
- ***Each flat mate owns mobile phone***
- ***Three flat mates have external hard drives for data back up and two also have cloud back up***
- ***One flat mate uses cloud back up no external hard drive***
- ***One router/modem in shared area (all are accessing/both wired and wireless)***
- ***Games console owned by one flat mate, in common area that all flatmates can access***
- (initial analysis) One router/modem default admin password has not been changed
- (initial analysis) One router/modem shows wireless strength is strong that someone directly outside the flat could access the router/modem
- (initial analysis) One mobile belongs to named recipient of the intercepted package

Digital Crime Scene Investigation Phase

Identification

Below is an identified number of electronic/digital evidence devices that may contain data of interest. These have been categorised and itemized below. A chain of custody as follows.

- ***Total of 5 Computers/Laptops***. 4 laptops all connected via flat Wi-Fi connection and 1 computer connected by wired ethernet connection. All computer/laptops currently running Windows 11 and actively being used hours prior to collection.
- ***Total of 5 Mobile Devices***. All mobiles are connected to the flat Wi-Fi. One of the 5 mobile devices is key evidence which belongs to the named recipient of the package. 4 mobile devices are Android models, 1 Apple and 1 Samsung model mobile devices active use prior to collection.
- ***Total of 3 External Hard Drives and Total of 3 Cloud back-ups.*** (Two flat mates both own an external hard drive and cloud back up, one flat mate only owns cloud backup, and one flat mate only owns an external hard drive).
- ***One Wireless Router*** (Main router being used by all flat mates)
- ***One Console (Xbox One)*** wired connection to the router. All flat mates have sign-ins/profile on this console.
-

Electronic/Digital Devices			
Electronic/Digital Devices	**Serial number/Model**		
1 x Computer A	A00601201	Dell	Flat mate A
1 x Laptop B	A35612487	HP	Flat mate B
1 x Laptop C	A02696644	HP	Flat mate C
1 x Laptop D	A12312302	HP	Flat mate D
1 x Laptop E	A23035465	Lenovo	Flat mate E
1 x Mobile A	2231290	Android	Flat mate A
1 x Mobile B	IO43222	Android	Flat mate B
1 x Mobile C	IO43212	Android	Flat mate C
1 x Mobile D	IO43215	Apple	Flat mate D
1 x Mobile E	IO43297	Samsung	Flat mate E
1 x External Hard Drive A	DS110001	Toshiba	Flat mate A
1 x External Hard Drive B	DS120023	Toshiba	Flat mate B
1 x External Hard Drive C	DS213000	Seagate	Flat mate C
1 x Cloud Back-up A	E12	AWS	Flat mate A
1 x Cloud Back-up B	E13	AWS	Flat mate B
1 x Cloud Back-up D	E14	iCloud	Flat mate D
1 x Router	FR12Z	TP-Link	Full Access
1 x Xbox One	A1ZX03	Microsoft	Flat mate E/Full Access

Extraction and Preservation

All devices have been identified and now require a process called preservation to preserve the collected evidence. One way this can be done is performing an immediate image capture of all collected evidence. This will duplicate/clone the data and provide a hash value to ensure the integrity of the evidence (at the time of its collection). Third party will be able to match this data against the generated hash value at any time during process and most importantly at the end of investigation to ensure there has been no tampering of data.

Hardware tools that will be used for digital evidence collection:

Tableau Tx1

A tool helpful for forensic data acquisition. This tool can connect to many different electronic devices, offering functionalities complimenting the versatility of the forensic imaging tool. “The increasing diversity, size and sophistication of digital media makes evidence collection a challenge. Digital investigators need a versatile solution that can acquire data from any storage type, including network shares, that is easy to use and navigate that can help close cases faster, reduce case backlogs and increase investigative capacity”, (OpenText, 2018).

The computer and laptops hard drive evidence will be plugged into the Tx1, capturing the image of the data and use of write blockers to prevent any data written to the evidence.

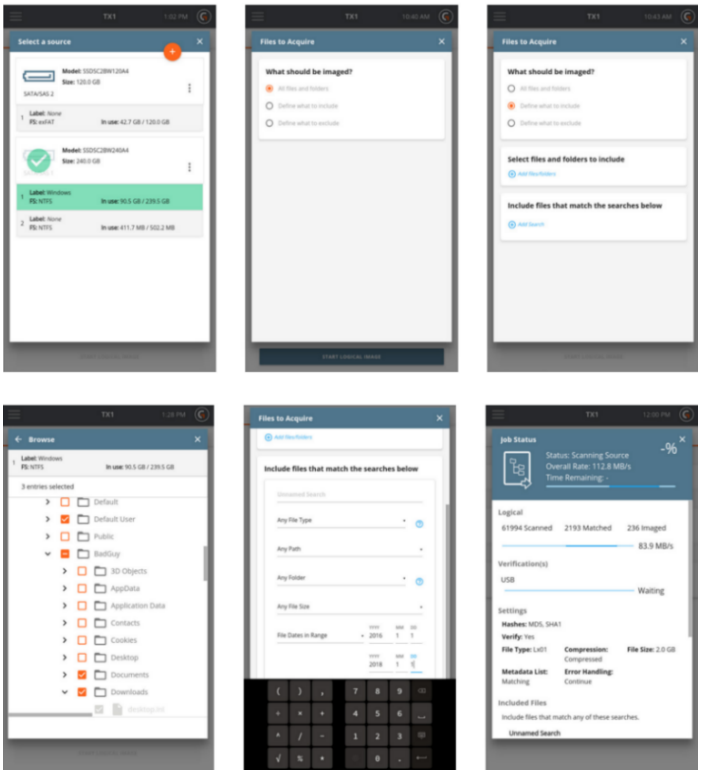


Figure 1. TX1

Logicube Falcon-NEO2

This hardware tool will duplicate the storage device collected for the 3 external hard drives collected whilst still preserving the integrity of the original data. The collected evidence data can be quite large especially analysing 3 external hard drives. The Falcon-NEO2 would be the appropriate approach to effectively image capture these storage devices in a timely manner.

“The Falcon-NEO2 can encrypt the storage drives, which improves the security of the harvested evidence. It achieves imaging speeds of up to 115GB/min on a SAS-3 SSD to SAS-3 E01 captures”, (Thackray et al., 2023).

Figure 2. NEO2

Cellebrite UFED (Universal Forensics Extraction Device)

The mobile phone may be locked or encrypted becoming difficult to analyse useful information for evidence. A powerful tool that can clone/capture the data from the mobile phones collected for evidence. A tool only obtained working with a law enforcement agency.

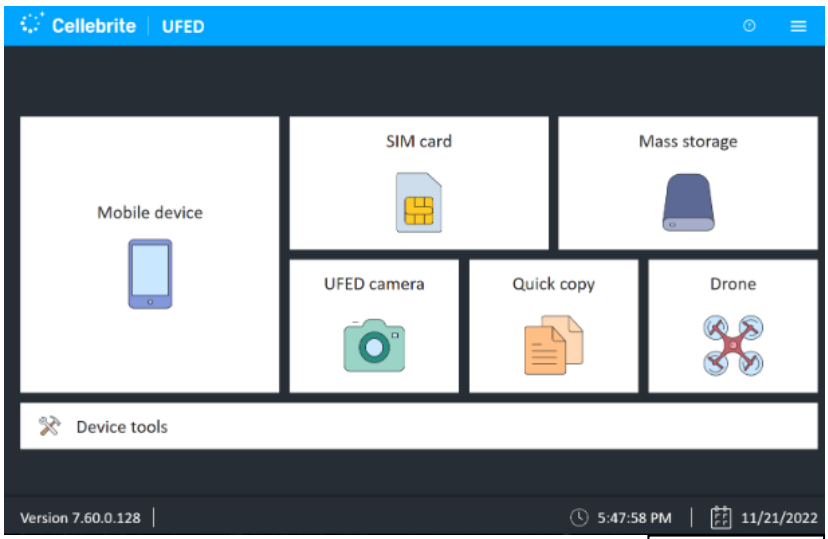


Figure 3. UFED

UFED has “advanced extraction techniques, UFED can retrieve various types of data, such as call logs, messages, contracts, multimedia files, app data, and more” (Pelorustechnologies, 2023).

This hardware tool can process all the mobile phones and target the key mobile evidence in question. The extraction of the call logs etc will provide information of what messages were exchanged and open doors to where and how the package arrived in the country.

A total of 18 electronic/digital evidence has been identified with data extracted. All electronic/digital evidence has been successfully captured (cloned) and hashed for data integrity. These devices are preserved in a secured in lock up for the next analysis phase.

Electronic/Digital Devices		**Hashing MD5/SHA1**
1 x Computer A	Stored in Room 1. Shelf A.	952a0a785507724c46aa0dddfe0b1674
1 x Laptop B	Stored in Room 1. Shelf A.	ede2d49caeb6ed3dcaf8731530e77aef
1 x Laptop C	Stored in Room 1. Shelf A.	cc321d0d18f411c0d7123cb3382dc65d
1 x Laptop D	Stored in Room 1. Shelf A.	b4bdf81426be83a57ae0c1ada2c5488a
1 x Laptop E	Stored in Room 1. Shelf A.	648df2f51128db70bebd658e69a24983
1 x Mobile A	Stored in Room 1. Shelf B.	97844615296381fb27bfb76a272e52df44bc35d8
1 x Mobile B	Stored in Room 1. Shelf B.	3db8a99a0933719305e0932a0095ccefd954628a
1 x Mobile C	Stored in Room 1. Shelf B.	e862a109c5852f2772b6af6bdf4ff55cc6ef67eb
1 x Mobile D	Stored in Room 1. Shelf B.	91a989b133ab828435b2671ad6b78a6716ab6343
1 x Mobile E	Stored in Room 1. Shelf B.	9d12afc2c98a81be02c50f6d8a026e142e40c62d
1 x External Hard Drive A	Stored in Room 1. Shelf C.	27ae19f613ee4cbf1d90c81a84200a76e77189fa
1 x External Hard Drive B	Stored in Room 1. Shelf C.	2fff809166bfd1c10e37413ecaffc4a8a4795bf1
1 x External Hard Drive D	Stored in Room 1. Shelf C.	ae00e3b67aeb2107d1532ebecb8d9e8b6df87962
1 x Cloud Back-up A	Stored on Server A	aa99407f64d0eaaa77bfb7bb242d4a8f9c13db26

1 x Cloud Back-up B	Stored on Server B	0a4764794e8ee8c66fd6bc08d4066ba6e13079b8
1 x Cloud Back-up C	Stored on Server C	f75b267609bbc29963ffb24d57f9d5014f7f31bd
1 x Router	Stored in Room 1. Box A.	77eb1db6cb81b3cb088d36ab7aae8f230dcfaa28
1 x Xbox One	Stored in Room 1. Box B.	5b56e33500970431ddce6d030d28a6fe005589ad
Total Electronic/Digital Evidence:**18**	***Locked and secured.***	

Analysis

Software tools available such as the FTK imager tool or Magnet Process Capture can do a basic analysis of the data from the extracted cloned information. The data that was captured from the electronic evidence/devices will be analysed and explored. If data is corrupted, deleted or damaged data this software tool can likely recover this information.

At the time of collecting evidence, a computer may have been immediately shutdown in attempt to evade any suspicious activity.

Magnet Process Capture is a great tool to quickly review a computer. This tool allows for processes to be extracted or viewed in volatile memory. Once the memory of selected processes is captured from our computer evidence, we can perform carving techniques to extract the data.

FTK imager can carve (extract structured data out of raw data) files from a RAM capture. “It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation”, (Warlock, 2018).

A screenshot shown below is of a file carved from a windows memory dump (file containing all information stored in RAM before system failure). An image was recovered from recognizing jpeg header and footer file numbers. A selection of the correct file numbers was extracted from the raw data and exported, uncovering an image.

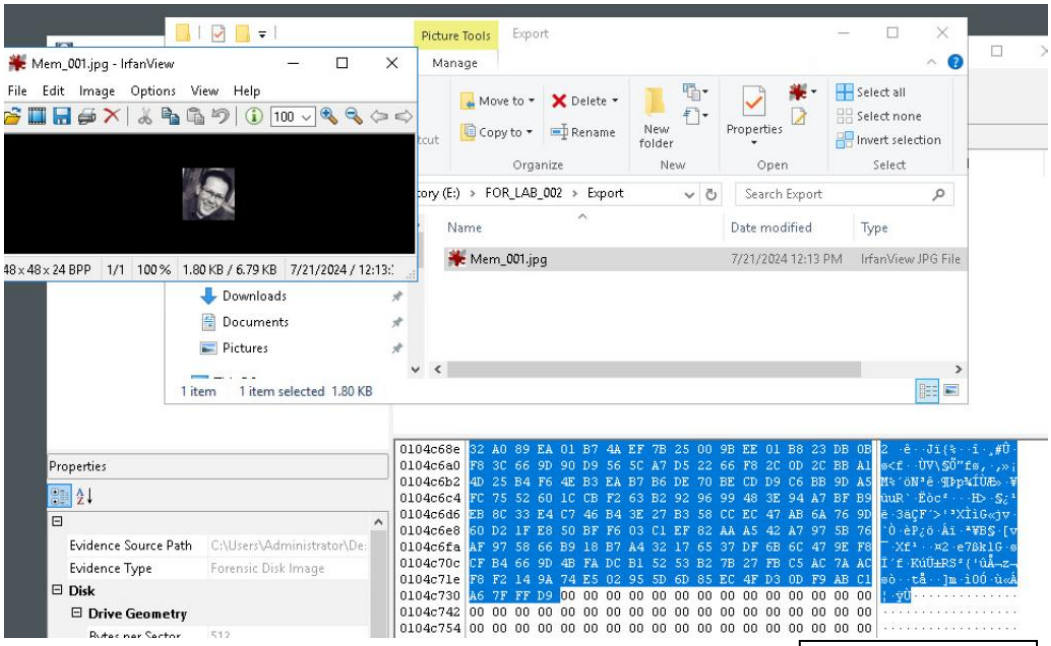


Figure 4. FTK imager

The procedure will be performed on the computers or laptops kept in evidence to help reconstruct any fragments of data.

Mobile device analysis allows to extract information using UFED and detail a report from the information gathered. Providing communication data such as call log times, text message exchanges, and also user and device content. Other tools such as SPF Pro (SmartPhone Forensic System Professionals) can extract deleted data.

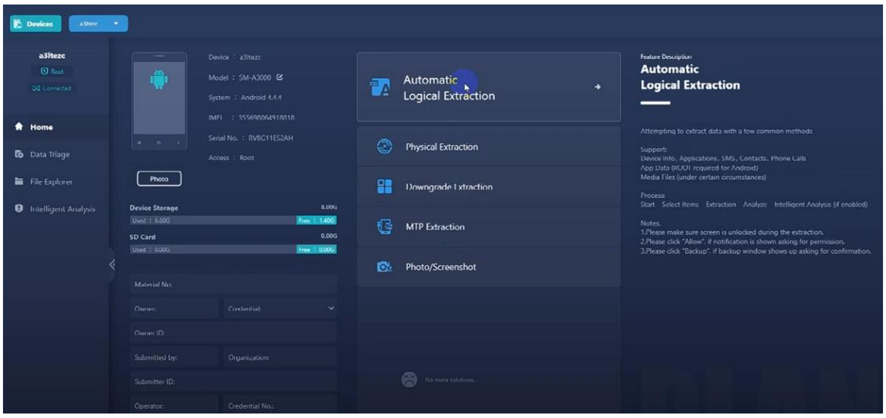
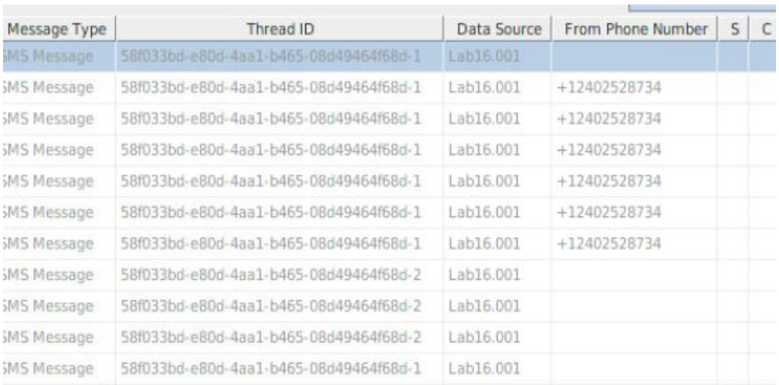


Figure 5. SPF

Another software tool to be used and will be involved in developing the case summary is the Autopsy tool to provide more information about the key mobile device evidence. The information extracted to be used for analysis will be databases in search of configuration files to see if any backups directly on the mobile device.

Mapping location information will be examined in search of mobile users' activity of movements using Google Maps and being able to track original destination points. Mobile information and sim card history to examine if any other numbers were used on the device.

Communications extracting call logs, text messages, emails (connected email address) and attachments of images. The mobile device link to the Wi-Fi and details of this connection.



Message Type	Thread ID	Data Source	From Phone Number	S	C
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001			
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001	+12402528734		
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001	+12402528734		
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001	+12402528734		
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001	+12402528734		
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001	+12402528734		
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001	+12402528734		
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-2	Lab16.001			
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-2	Lab16.001			
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-2	Lab16.001			
SMS Message	58f033bd-e80d-4aa1-b465-08d49464f68d-1	Lab16.001			

Figure 6. Autospy

Network forensics to analyse the TP Link Modem. The modem is electronic evidence because of the responsibility it has to connect two different networks. It acts as a tool to send packets of data through a network or internet, a transfer of sources between the end device and internet (routing). An initial analysis of the modem discovered the default admin password had not been changed.

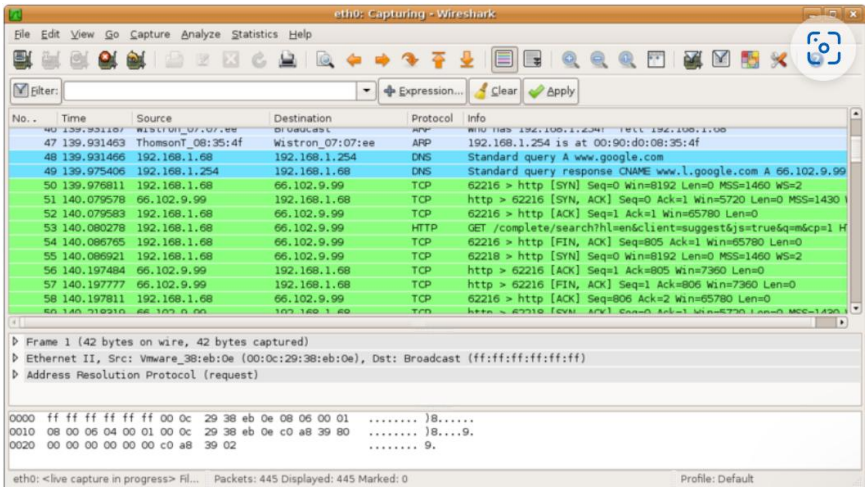


Figure 7. Wireshark

"Evidence is captured from the network and interpreted based on the knowledge from network forensics. This research has some purpose that are to find out what data is obtained during the network is connect and then collect and analyse data from computer networks" (Hildayanti and Riadi, 2019).

Tools used for Network forensics are Netcut and Wireshark. Wireshark will find forensics information through the network usage and can provide details of the IP of access, what, when and where the flat mate accesses the network. Wireshark operates as an open source "packet sniffer" (monitoring network traffic). Netcut is involved in the process to break and divert internet connection.

Forensic analysis of the Xbox One Console. This gaming equipment uses NTFS (new technology file system) files system. The Xbox One hard drive will be forensically imaged using FTK. This will allow for examination of any logging information or data relating to involvement of the parcel.

Documentation

June 5: Parcel intercepted containing illegal substances

June 7: Police seize all electronic/digital devices for forensic data investigation

June 7: All 18 electronic/digital evidence identified, cloned, hashed and stored in a secure location. The devices have been documented, recorded and itemized in the forensic evidence register in preparation of analysis.

- 1 x Computer and 4 x Laptop – hard drives removed and cloned for analysis via Tableau TX1 equipment
- 3 x External hard drive – cloned and write blocker added using Logicube Neo2
- 5 x Mobile – relevant data duplicated via UFED (details and communication exchanges and data recorded)
- 1 x Modem – analysed using Netcut and Wireshark to observe traffic flow and interception
- 1 x Console – analysed using FTK imager to clone and identify any communications via online network
- 3 x Cloud Data Backup – persevered in an encrypted secure server storage

June 10: Analysis of data extraction using FTK image to uncover any deleted or damaged files from electronic digital evidence devices

July 3: Mobile analysis on the “Mobile A” indicates suspicious activity of call logs to an unknown overseas number, in-sync with the timestamp of email exchanges from “Computer A”, verifying this in accordance with the network traffic flow via “Modem”

Wireshark at the respective times. The plain text pinpoints the conversation between the buyer and seller.

FTK imager unearths a deleted image from the “Computer A” device of the parcel prior to delivery from an unknown domain. This image matches the parcel that was intercepted by NZ Police.

July 15: Complete forensic analysis report performed on key mobile device evidence

August 28: All relevant data analysed, documented and prepared for formal presentation.

Presentation

It is within scientific reason, the data obtained from the digital/electronic evidence seized at the address of interest have concluded a number of substantial facts pin-pointing the involvement and relation of the parcel to the person responsible.

All relevant information is from the mobile device and computer owned by the named recipient of the package entailing conversations of an unknown overseas number. The data from the computer with plain text email conversation between “buyer and seller”. A deleted image was recovered from the computer during the email exchanges of an image that matches the intercepted parcel.

Extraction of images, call logs, email messages, Wi-Fi connections, attachments in connection with the package have been documented using a forensic tool also further concludes above.

The timestamp of conversations and emails prior to the arrival of the package confirms a narrative between the sending of the parcel up until the interception.

The case summary provides an in-depth analysis of the mobile device with supporting documentation.

Case Summary (Mobile Device)

NZ Police have contacted the Digital Forensics team to analyse data from an Android mobile device. A forensic examination is required on the mobile device to extract any relevant data that may provide vital information around the intercepted parcel containing illegal substances.

Evidence

Physical Evidence:

(1) 1 x Samsung Android Mobile Phone (Serial 2231290)

Objectives:

Extract any relevant information of the Android phone showing in direct relations and involvement of the parcel.

Targeted investigation is on the mobile device as the key evidence. The mobile device owner is the named recipient of the parcel.

Search for any connections of outside sources such as sellers/organisers/manufacturer responsible for the shipping of the product. Collect and extract any evidential data in the process.

Capture and detail each action and steps taken using digital forensic tools that are gathering the evidence.

Mobile Device Forensics Examination:

1. June 15 – Samsung Android Mobile Phone was received for forensic analysis. Mobile device has been listed as evidence, item has been photographed, all identifiers documented such as serial numbers, model and make. Unique markings and any damages recorded. These have all been carefully performed to protect the chain of custody.

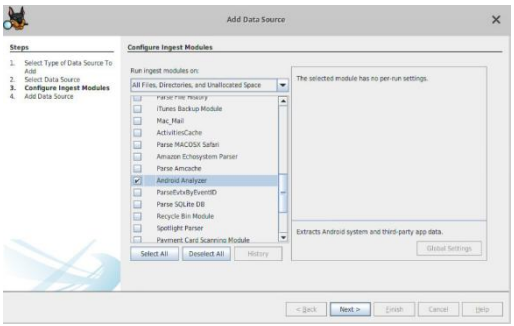
2. The following tool will be used in accordance with extraction of data

    1. FTK Imager version 4.3.0.18
    2. Autopsy version 4.13

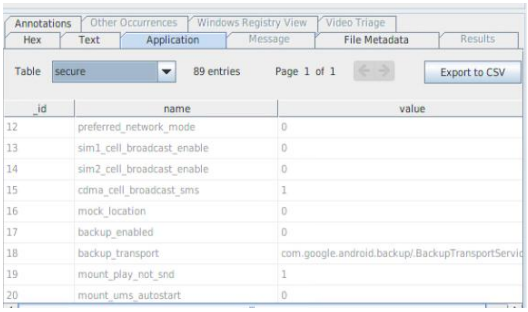
3. A physical image is captured using FTK imager of the device to begin extracting data. The physical image in this context is a bit-by-bit copy of the device to acquire as much data including data in deleted space.

4. Autopsy software tool is being used for the examination and analysis. The physical image has been captured to proceed with the extraction of relevant data.

5. A new case is created for Autopsy report and the disk image of the Samsung Android evidence file has been added as data source for analysis. The ingest modules selected for the analysis are Android Analyzer and Exit Parser.

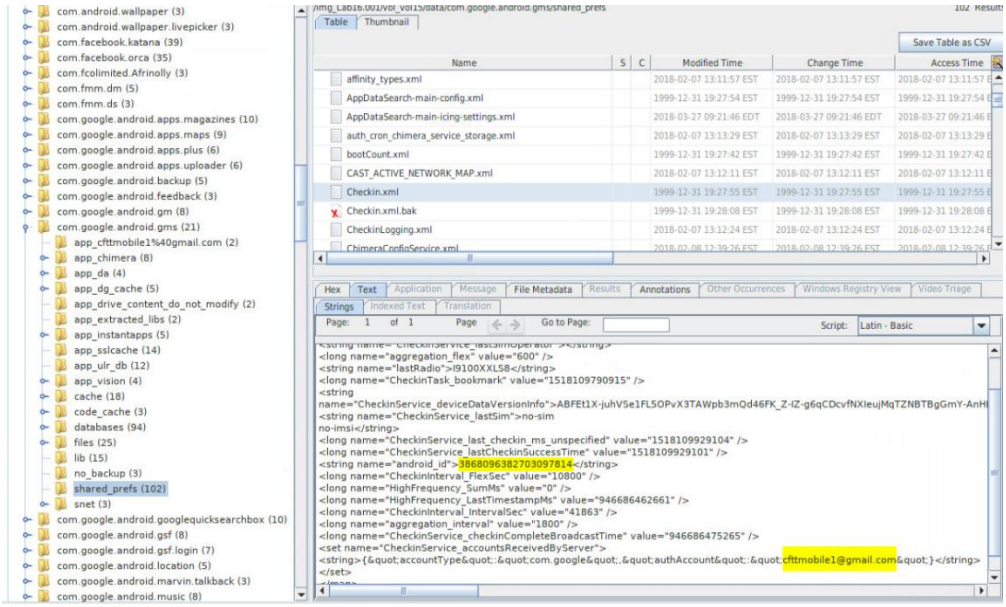


6. Databases and config. files are searched on the mobile device. It is confirmed back ups enabled on the device, and locking settings were enabled at the time of extraction.



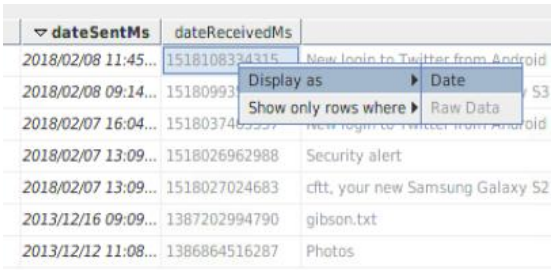
Configuration settings

7. Email and IMEI (International Mobile Equipment Identity) associated with the device is located. These are highlighted.

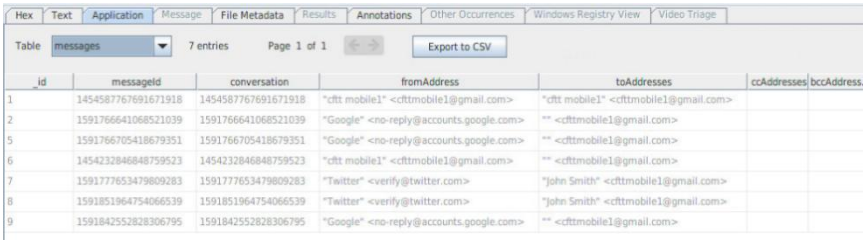


IMEI and email address

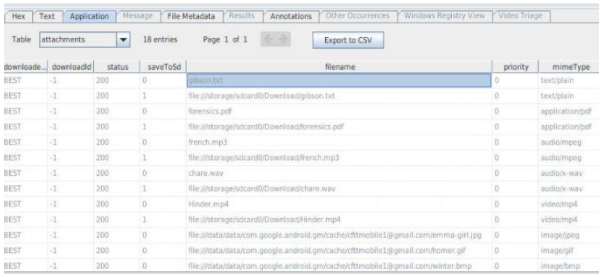
8. Communication logs have been searched and extracted. Email messages showing sender and receiver including times and dates have been found, attachments to emails, call logs including phone numbers and text messages (sms) are documented.



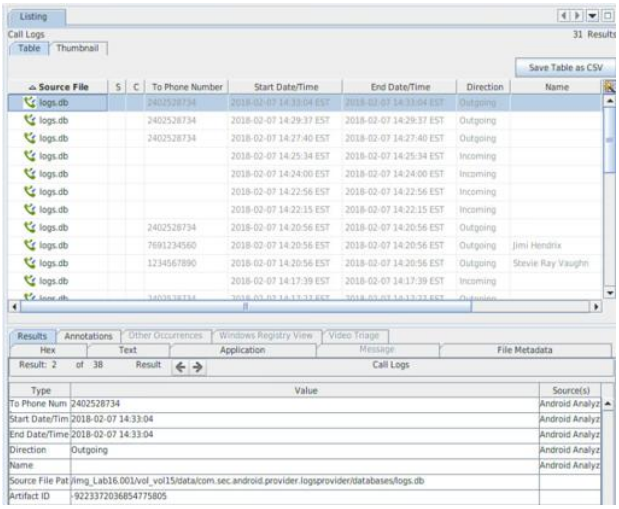
Dates of Messages and exchanges



Email exchanges

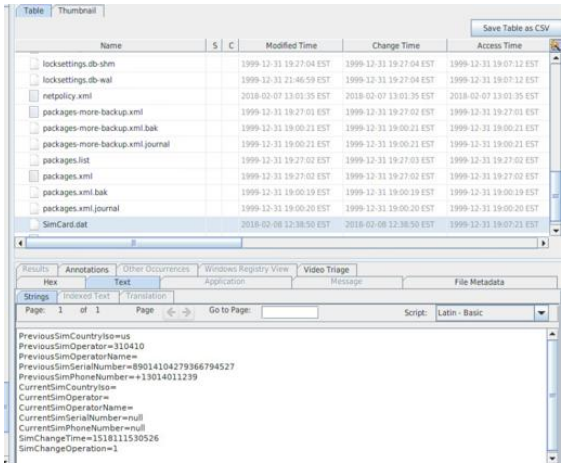


File attachments

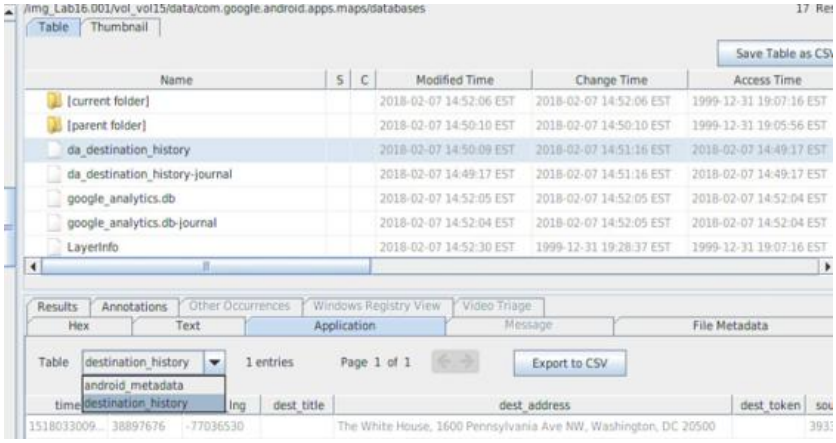


Call logs

9. Sim card information and google map/location (including destination and arrival points) of the mobile device have been extracted.

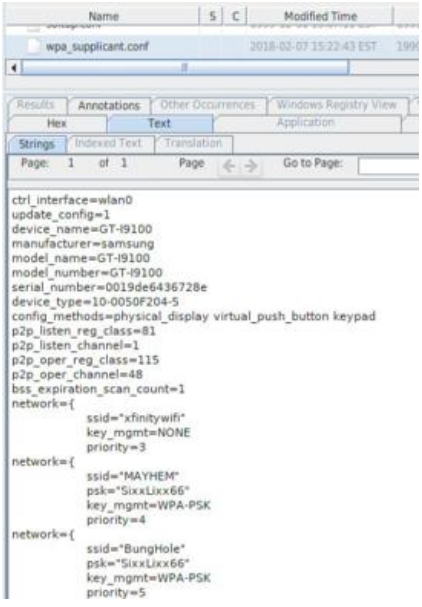


Sim card



Google maps

10. Mobile device Wi-Fi connection details have also been extracted along with information of the network.



Wifi connection details

Relevant Findings

The extraction of the Samsung Mobile Device has provided us with some valuable information. We have identified the device had multiple sim cards used, and the numbers associated. The numbers could be of interest and have been registered to identify links to the overseas channel these are supported by the call logs on file.

The email and IMEI number directly linked and identities the device has been recorded. IMEI number can be further checked on databases to see if this has been used in relation to other activities. The email of the user is explored, and messages uncovered showing the exchanges as matching on the computer.

The Wi-Fi connection details the mobile has been identified, recording the multiple locations of interest of the connection and timeframe of communications during the arrangement process between “buyer and seller”.

References

(Das, 2023).	Das, S. (2023, September 14). Unveiling the Significance of Digital vs. Physical Evidence in Investigations. *Medium.* Unveiling the Significance of Digital vs. Physical Evidence in Investigations | by Sourabh Kumar Das | Medium
(ERMProtect Staff, 2024).	ERMProtect Staff. What Are the 5 Stages of a Digital Forensics Investigation? What Are the 5 Stages of a Digital Forensics Investigation? - ERMProtect Cybersecurity
(Garrie, 2016).	Garrie, D. (2016, August 15). The Neutral Corner: Understanding a Digital Forensics Report. Understanding a Digital Forensics Report (thomsonreuters.com)
(Hildayanti and Riadi, 2019).	Hildayant, N., Riadi, Im. (2019, May 19). *Forensics Analysis of Router On Computer Networks Using Live Forensics Method.* International Journal of Cyber-Security and Digital Forensics. (PDF) Forensics Analysis of Router On Computer Networks Using Live Forensics Method (researchgate.net)
(Longley, 2022).	Longley, R. (2022, July 13). *What is Chain of Custody? Definition and Examples.* Thought Co. What Is Chain of Custody? (thoughtco.com)
(OpenText, 2018).	OpenText. (2018). OpenText Tableau Forensic Imager (TX1) *Product Overview.* OpenText | Tableau Forensic Imager (TX1) - Product overview (digitoforense.cl)
(Pelorustechnologies, 2023).	Pelorustechnologies. (2023, May 25). *"Exploring the Power of Cellebrite UFED in Digital Forensics".* Medium. "Exploring the Power of Cellebrite UFED in Digital Forensics" | by Pelorustechnologies | Medium
(Pollitt, 2010).	Pollitt, M. (2010). A history of digital forensics. In *Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised*

	Selected Papers 6 (pp. 3-15). Springer Berlin Heidelberg.
(Thackray et al., 2023).	Thackray, J., Fellow, C., Dip, FSS. (2023, September 23). A Practitioners Experience and Assessment. Logicube | Falcon-Neo_Review2
(Warlock, 2018).	Warlock. (2018, February 4). *File Carving.* Digital Forensics. File carving | Infosec (infosecinstitute.com)

Images

Figure 1. TX1	Image source: OpenText | Tableau Forensic Imager (TX1) - Product overview (digitoforense.cl)
Figure 2. NEO2	Image source: How To Image To A Network Repository With Logicube's Forensic Falcon-NEO - Forensic Focus
Figure 3. UFED	Image source: Cellebrite UFED | Access and Collect Mobile Device Data
Figure 4. FTK Imager	Image source: Original screenshot from Lab 2 Netlab.
Figure 5. SPF	Image source: SmartPhone Forensic System Professional | Mobile Forensics (salvationdata.com)
Figure 6. Autopsy	Image source: Original screenshot from Lab 16
Figure 7. Wireshark	Image source: Wireshark vs Netcat for Network Protocol Analysis | UpGuard