Social Media Investigation:
Mobile Device Forensics Tools Capabilities

STEPHANIE KARTIKAMUTIARA BRENNADIVA

(Police First Inspector, Bachelor of Ed, Bachelor of Science)

A thesis submitted to the graduate faculty of Design and Creative Technologies
Auckland University of Technology
in partial fulfilment of the
requirements for the degree of
Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand
2018

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief. It contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

Stephanie K Brennadiva

Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies in the School of Engineering, Computer and Mathematical Sciences at Auckland University of Technology, New Zealand under supervision from Dr Brian Cusack. First and foremost, I thank Allah the most gracious and the most merciful, for giving me the opportunity, strength, and determination to complete my thesis. It is my pleasure to take this opportunity to thank all of you and apologise to those I do not mention by name here; Nevertheless, I highly valued your kind support.

I would like to express my deepest gratitude to my supervisor, Dr Brian Cusack, for all the guidance and support during my thesis journey. Likewise, I would like to thank Dr Alastair Nisbet for providing me with the knowledge in the fields of security and digital forensics. I would also like to thank my Institution (Indonesian National Police) for providing the work systems, documents, and all the tools for my research. In addition, I would like to thank for the support from my good classmates in the Master of Information Security and Digital Forensics programme at AUT. They have been my mentors and companions on this challenging journey. I also would like to express my gratitude for all the support and fun shared by my fellow friends in Auckland and Indonesia.

Finally, I would like to express my profound gratitude to my parents, my grandmother, my older sister, my twin sister, my uncle, my aunt and all my extended family for their tremendous support throughout of my study journey.

Abstract

The significant development of social media in recent years has an impact on increasing the number of social media platforms and device users around the world. The majority of social media users access their platform via smartphones and have continuous access from location and time. The recent features provided by social media platforms allow the uploaded files such as videos and photos to last a short period of time before disappearing. This is one of the concerns for social media investigators and evidence collection. For instance, a cybercriminal who utilised social media to spread threats or sell illegal drugs and substances, can post a secret code through photos and videos, and know the potential evidence is gone. For that reason, it is a necessity to educate investigators and to figure out the capability of mobile device forensics tools before use. Crimes can and are committed using social media and these social media-related crime cases require examining and retrieving potential evidence from social media applications such as Facebook, Twitter, and Instagram. Usually, the mobile device is the first physical point of entry for evidence.

This thesis reviewed and compared two widely used mobile device forensics tools, namely, MSAB XRY and Cellebrite UFED, with the aim to understand which of those tools possess the greatest useful practical capability for professional practice in handling cyber-crime cases related to social media. The two selected mobile device forensics tools were evaluated in a systematic and forensically sound manner in the research. Four case scenarios were developed, and each case consists of specific data such as social media status (posts), chat messages, photos, and videos. Social media evidence was planted on three Android smartphones: Samsung J5 Prime, Samsung S4 mini, and OPPO A57. To discover which of the chosen forensic tools is better performing in a social media investigation, the testing rating method was implemented. This research will explore the capabilities of mobile forensic tool devices in social media investigations by posing the main research question as follows:

> ***"What are the capabilities of the chosen mobile devices forensics tools (i.e., Cellebrite UFED and MSAB XRY) when examining Social Media applications on Android smartphones in a social media-related crimes investigation?"***

The research found that Cellebrite UFED performed better as a mobile device forensic tool than MSAB XRY in the tests described in chapter 3. Several factors contributed to the result such as MSAB XRY 7.6 is unable to examine the OPPO A57 smartphone due to the Android smartphone not yet being on the extractable list for the tool. In contrast, Cellebrite UFED is capable of examining all three smartphones. Moreover, Cellebrite UFED also has more extraction options for file system extraction, which is required most for social media-related cybercrime cases. The research findings also show that Cellebrite UFED surpassed MSAB XRY when retrieving evidence such as social media status (post), photos, and videos from all three social media applications on all three Android smartphones.

The results are helpful for investigators who are alerted to different capabilities in different tools, and also the importance of selecting the best performing tool for any investigation. The findings also suggest that an investigator should not only assess capability before embarking on a social media related investigation but also consider the best combination of tools to use. Each tool has strengths and weaknesses and the selection where one tool compensates for another is the best option. The consideration of cost is also important where time, tools and training have to be optimised to fit the investigation budget. Social media forensic tool capabilities are still developing so an investigator must assess current limitations and issues of the chosen mobile device forensic tool prior to use, and the tool developers need to recognise the limitation of the tools and improve the capability for examining social media applications on smartphones.

Table of Contents

List of Tables

List of Figures

Chapter One

INTRODUCTION

1.0 INTRODUCTION

In 2018, over half of the world's population is now an internet user. With 42 percent of internet users are active social media users and these figures are expected to grow. Moreover, 91 percent of social media users are using the applications via their smartphones to access their selected social media platforms (Kemp, 2018). According to Valentine (2018), social media users are most likely to use social media platforms as a source to stay up to date with current entertainment, news, and events and as a place to share their personal details or content and stay engaged with others (their friends, colleagues, and another people with similar interests). However, since social media allows people to interact with anonymous users and all the people around the world with various backgrounds, social media platforms have become an attractive vehicle to perpetrate cybercrimes. A growing number of criminals are utilising social media to achieve their goals (Lambert, 2017).

According to FBI's IC3 Report (2018) social media was used as tool to facilitate crimes such as phishing, pharming, terrorism, government impersonation, identity theft, extortion, confidence fraud, child pornography, romance fraud, and harassment/threats of violence with 19,986 prosecuted felonies in 2017. Furthermore, mobile devices are increasingly the focus of criminal investigations, such as those used by organised crime and terrorist groups. For those cyber related offenses, valid and forensically sound evidence is crucially needed. One of the methods required is by using mobile device forensics tools for acquiring potential evidences in social media on the smartphones. While the increase in the number of users in social media has resulted in an increased number of crimes, there are limited studies focused on identifying the existing tools' capabilities in extracting social media applications evidence on smartphones. The purpose of this thesis is to gain information regarding digital forensics tools capabilities, and particularly mobile device forensic tools whilst handling social media crime cases. By using existing mobile forensics tools, it will help to identify limitations and cautions in the investigation process.

Chapter one is structured to introduce the thesis and to summarise its contribution. The motivation of this research will be presented in section 1.1. In section 1.2, the objectives of thesis will be outlined. In section 1.3, the contribution of thesis is defined by identifying the problems, the research question, and the findings. This section provides an overview of the thesis. Lastly, the structure of the thesis is outlined in section 1.4, in order to present briefly the flow of the thesis content.

1.1 MOTIVATION

The motivation of the author for conducting this thesis came from working for several years in law enforcement and particularly in the criminal investigation department. The author observed that the common evidence that is frequently found in recent years in the crime scenes is mobile device related and specifically smartphones. Many conventional crimes are now related to digital media and better described as cybercrimes. Due to the greater, smarter, and better communication capabilities of smartphones they are a tool of choice. Also the range of applications on a smartphone allow all manner of communication to occur including secure communications. They have better screen resolution for images, faster connections, and a vast amount of multipurpose tools for voice, text and image communication. The majority of people spend over two hours a day of their time on smartphones, with around 66 percent of that time on social media applications (Chaffey, 2018).

The social media platforms have become a pleasant place to interact with other people all around the world. Individuals can moderately post and share everything in social media including their personal information, location, and relationships. The social media users also can communicate with new people with a same interest, common problems and hobbies, and with no limit of age. They can easily find any content in social media such as recent news, education materials and entertainment. However, there are also people that have employed social media platforms to commit malicious acts such as recruit members (terrorism), cyber bullying, drug dealing, cyber financial fraud, love scams, child abuse and human exploitation. This puts social media information as one of the significant sources of evidence in criminal investigation. Nevertheless, social media forensics investigation is a relatively challenging field of digital forensics, due to the lack of specially designed tools and inadequate knowledge of some investigators relating to social media investigation.

The most widely used mobile device forensics tools that are utilised for investigating social media and mobile devices in law enforcement field are commercial tools, namely, MSAB XRY and Cellebrite UFED. Both tools have become the main tools when investigating mobile devices. Year by year, the number of mobile devices for crime cases to be investigated is increasing significantly. The mobile devices in almost every case are forensically examined by one of those two mobile forensic tools. Notwithstanding that the investigator may not understand which one is the most suitable or the related capabilities they are accepted as standard. There has been only few research reports that cover the choice of social media applications in investigation, particularly comparative mobile device forensic tools capabilities. In this thesis two tools' performance are to be compared when examining three social media apps on three android smartphones. With the purpose of identifying performance of those two smartphones forensics tools’ capabilities in social media investigation, and putting in the investigator mind the need to assess the choice of tool or combination of tools prior to use.

1.2 AIM OF THESIS

The first and foremost aim of this thesis is to evaluate and compare the chosen existing mobile device forensic tools capabilities when investigating social media applications in Android smartphones with the test scenarios developed herein. With a better understanding regarding the mobile device forensic tools capabilities when investigating social media applications on Android smartphones, the author hopes that it will benefit in combating social media-related cases, upgrade the investigators skills, address social media investigation problems, and also can stimulate mobile device forensics tools development companies to improve the quality of existing tools for handling social media-related crime cases.

In the following section, the research contribution includes the research question, sub-questions, hypotheses, and the summary of findings are reported in order to provide an overview of the thesis.

1.3 CONTRIBUTION OF THESIS

The prime purpose of this thesis is to test, evaluate and compare the capabilities of two mobile device forensics tools namely, MSAB XRY and Cellebrite UFED in extracting evidences from three social media applications: Facebook, Twitter and Instagram; on three Android smartphones (Samsung J5 Prime, Samsung S4 mini and OPPO A57).

The several issues and problems in social media investigation such as difficulty to assemble credible forensic evidence, lack of comprehension and understanding of investigators related to social media crime cases, jurisdictional and law differences, lack of specially designed tools for social media forensics and unavailability of international standard procedures in social media forensic investigation, lead to the designing of the research methodology and the research question.

There are six phases in this research. The research phases begins with the pre-phase step where, the mobile device forensics tools and smartphones that will be used in this thesis are selected. The working hypothesis also is developed. The next phase, the test case scenarios are developed. Each case consists of specific planted data (social media features) such as Social media status (posts), chat messages, photos, and videos. In phase 2, the testing case scenario are implemented and applied on the three chosen smartphones. In phase 3, the two selected mobile devices forensic tools are being utilised to examine all three Android smartphones. Phase 4, has the test results and findings being analysed. Lastly, in phase 5, the capabilities of both mobile forensic tools are assessed and compared using the prescribed tool ranking method. The tool ranking method is being utilised to determine and compare the capabilities of both selected forensics tools. The results obtained were analysed to answer the research question, sub-questions and the hypotheses. The main research question proposed for this research is:

"What are the capabilities of the chosen mobile devices forensics tools (i.e., Cellebrite UFED and MSAB XRY) when examining Social Media applications on Android smartphones in a social media-related crimes investigation?"

The associated sub-questions are formulated in order to address the main research question:

The Sub Question 1: *What extraction type of mobile device forensics tools are pre-eminent for collecting evidence from Social Media on Android phones?*

The Sub Question 2: *Are the chosen mobile device forensics tools capable to examine all three selected Android smartphones?*

The Sub Question 3: *Which tool is the best performer for Social Media investigations?*

Three hypotheses are also developed for each of the sub questions, as follows:

Hypothesis 1: *File system extraction of Cellibrite UFED is the best extraction type when gathering evidence from social media apps on Android smartphones.*

Hypothesis 2: *The both selected mobile forensics tools are able to examine all three chosen Android smartphones.*

Hypothesis 3: *Cellebrite UFED will perform better than MSAB XRY.*

The result findings obtained in this thesis show that Cellebrite UFED is better than MSAB XRY in extracting social media apps evidence in three selected Android smartphones.

1.4 THESIS STRUCTURE

This thesis is composed of 5 chapters. Chapter One “Introduction”, Chapter Two “Literature Review”, Chapter Three “Research Methodology”, Chapter Four “Research Findings”, and Chapter Five “Discussion and Conclusion”. Also there are formalities and references in the respective sections.

Chapter One introduces the objective of the thesis and motivations for the thesis as well as the thesis contribution. Chapter two presents a literature review. The literature reviewed in Chapter two include: digital forensics, social media, mobile forensic investigation tools, social media-related crimes, and the problems and issues related to social media forensics. The social media are introduced and explained at the beginning of the chapter and is followed by a general overview of digital forensics. The basic phases of forensic investigation also will be discussed in chapter two. The chapter then reviews two chosen mobile device forensic tools that can be utilised to collect potential evidence from social media applications on smartphones and several social media-related crimes will be identified. Chapter two concludes with a summary of problems, challenges and issues associated with a social media forensic investigation.

In Chapter three, the research methodology of this thesis will be discussed. At the beginning of chapter 3, the research question, sub-questions and hypothesis of this thesis are defined and then the data required to answering those questions specified. The testing design and testing methodology including data collection procedures are also presented to outline the processes in the research. Lastly, the limitations of the research are identified.

Chapter four reports the research findings and comparison results of the two selected smartphones forensics tools' capabilities in examining three social media apps on three Android smartphones. The tool ranking method is used to determine the capabilities of both mobile forensic tools and is explained at the beginning of chapter four. In chapter four, collected data and findings are analysed and the summary of findings presented in tables and charts to visualise the relationships in the research findings.

Chapter five discusses the research findings and the analyses the results presented in chapter four. Based on the findings summary provided in chapter four, the research question and sub-questions identified in chapter three are answered, and also the validity of proposed hypotheses are addressed in this chapter five. Then, chapter five concludes the thesis, as well as describing some possible directions and recommendations for further research. A list of all the references used in this research follows.

Chapter Two
LITERATURE REVIEW

2.0 INTRODUCTION

The number of internet users has dramatically increased. According to Kemp (2018), the global internet users rose by seven percent in 2018. In 2017 the global internet users were estimated to be 3.773 billion and it increased to 4.021 billion, up 248 million in 2018. Furthermore, the majority of the global population is interconnected with others using the internet, particularly social media, which has seen enormous growth in use in recent years. Active social media users in 2018 grew by 13 percent, up to an impressive 407 million versus 2017, from 2.789 billion to 3.196 billion. As has been noted, more than 3 billion people are now utilising the social media platforms, with the majority of those users are using the applications via their mobile devices to access their selected platforms (Kemp, 2018).

In their early development, social media began as websites that were accessible only through a laptop or desktop. Nevertheless, the evolution of smartphones leads to social media released mobile application versions. This advancement is beneficial to users' online activity, so that they might access their social media account easier and more conveniently across time and space (Aldhafferi, Watson, & Sajeev, 2013). Individuals are more likely to share information about their lives routinely and voluntarily such as date of birth, personal phone number, home and school address, users’ personal activities and having conversations with other users (private talk or regular talk).

Due to the large amounts of information in social media, some people might perform illicit activities, misuse and exploit that information (Ge, Peng, & Chen, 2014). Furthermore, social media not only can be used to commit crimes but also the criminals might leave a trail of digital artefacts, for instance, messages, photos, geotagging and so forth. Since the information and data of social media are located in the cyber place and might be left in the devices, digital forensic investigators have to carry distinct knowledge, ability, and skills to deal with social media-related crimes. Performing social media forensics is tough and, in some cases, an investigator may face numerous difficulties. There are several investigating tools that have been developed for mobile device forensics. However, forensic investigators might not always understand which tool that is the right one for gathering evidence from certain phone such as Android phones.

The research objective of chapter 2 is to critically review the recent literature related to four main areas; namely, digital forensics, social media, investigation tools, and social media-related crimes. In this chapter, some possible issues and potential research questions will be identified. In section 2.1 the definition of "social media" and numerous social media applications that have been used widely will be explained. Thereafter, Section 2.2 discusses a general overview of digital forensics, and digital forensics investigation such as mobile phone forensics and social media forensics. A number of mobile forensic investigation tools are reviewed in detail in section 2.3. Several social media-related crimes are discussed in section 2.4. Lastly, in section 2.5, the problems and issues related to social media forensics will be identified.

2.1 SOCIAL MEDIA

The definition of social media according to Oxford dictionaries is "websites and applications that enable individuals to interact, create and share content or to participate in social networking". Moreover, Balusamy, Varma, and Grandhi (2017) states that social media is "the collective of online communications channels dedicated to community-based input, interaction, content-sharing, and collaboration". Facebook, Twitter, Instagram, Path, and LinkedIn are prominent instances of social media. Based on many sources, it can be said that the main function of social media is as a place for people interaction in public or private communication without consideration of distance and time limitations.

There are several definitions of social media that are listed Fuchs (2017) in table 2.1.

Table 2.1: Definition of Social Media

Source	**Definition**
Standage (2013, p.3).	Social media is a place where information is transferred from one user to another individual with the purpose to form a circulated community
Van Dijck (2013, p.11)	Social media as "The very word ‘social' associated with media implies that platforms are user-centred and that they facilitate communal activities, just as the term “participatory” emphasizes human collaboration. Indeed, social media can be seen as online facilitators or enhancer of human networks – webs of people that promote connectedness as a social value”.
Boyd (2014, p.6)	Social media is Internet-based services that enable users to diffuse and create their own content.
Hunsinger & Senft (2014, p.1)	Network information services that designed with a purpose for in-depth support for social interaction, collaborative work, and opportunities.
Meikle (2016)	Social media is a particular internet communication platform that allow the merging of personal and public communication. For instance, Facebook and Twitter, Instagram and Pinterest, blogger and YouTube, Reddit and Tumblr and so forth.

According to Chaffey (2018), the most popular social media platforms used in 2017 are Facebook, YouTube, Instagram, Twitter, and Snapchat. Each social media has its own key features. The significant increase of social media user in each platform is because there are entirely new purposes of using social media. It used to be for simply communication, to share and stay connected with family and other people. However, nowadays social media can be used as a place for financial purposes such as for advertisers, selling goods and users can also directly interact with a company regarding products (costumers review).

2.2 DIGITAL FORENSICS

The origin of forensic emerges from the practice of medical forensics with meaning "of or used in law courts" (Oxford Dictionary, 1999, p. 305). The term "Forensic" has become more familiar to the IT community and law enforcement, as the number of malicious activities using electronics such as a computer has increased (Reith, Carr, & Gunsch, 2002, p. 10). Therefore, the new term has been introduced as digital forensics. Moreover, there are different areas that digital forensics covers which include Internet forensics, network forensics, mobile phone forensics and the new areas which recently emerged; cloud forensics and Social Media Forensics.

Even though the definition can change when the perception of digital forensics changes. The meaning of digital forensics can have some common elemental components. McKemmish (1999) defined digital forensic as "the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable". In recent years, owning a Facebook or Twitter account is becoming a common phenomenon. Most government institution and business organisations are connected with their colleges and share their public and private activities freely on social media and these days with the improvement of mobile phones such as smartphones, most individuals are likely to utilise a smartphone for their social media activities. In this context, all information that has been posted on social media is easy to view. The information might be used by malicious people to conduct illegal activities. The following section gives a brief introduction to mobile phone forensics and social media forensics.

2.2.1 Mobile Phone Forensics

Ayers, Brothers, and Jansen (2014) define mobile phone forensics as, "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods". This is not an easy criterion to attain because of the constant release of upgrades and rapid changes of mobile devices' operating systems versions, hardware, software and features requiring a mobile forensic tools company to continually update and keep up the forensic tools capability and compatibility with the newest models of mobile devices. Conducting mobile device forensics is considerably arduous. Due to the software variability, operating systems of mobile devices are different, which makes a universal standard tool for mobile devices such as smartphones, nearly impossible.

Kent, Chevalier, Grance, and Dang (2006) suggested Four Step Forensics Process (FSFP) that can be used as one of the basic digital forensics investigation models. FSFP contains four phase processes: Collection, Examination, Analysis, and Reporting as can be seen in Figure 2.1:

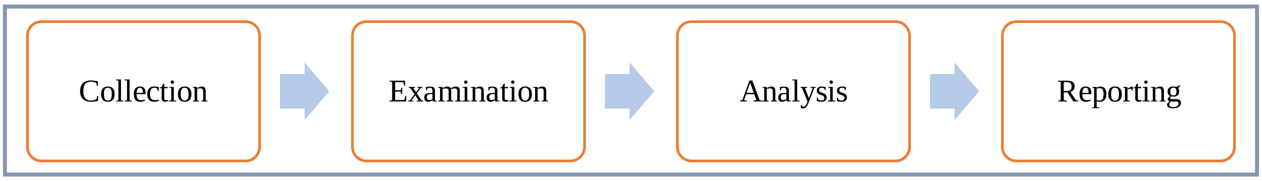


Figure 2.1: FSFP Forensic Investigation Model

The collection phase utilises seizure, identifying the potential source of data and acquisition of data in a forensic manner. The examination involves both manual and computerised techniques to identify and extract data that are relevant to the case. The analysis phase is the process of analysing extracted data to discover relevant evidence that can be used for unravelling cases. The last phase of reporting, presents the data gathered by the forensics investigator in a human-readable format written report for presentation in court.

The examination phase may be the most critical stage in forensics. Each mobile device and smartphone has distinct characteristics. There are two types of extraction (acquisitions) techniques commonly used: physical acquisition and logical acquisition. In physical acquisition, the information from the device is extracted by accessing its flash memory. This creates a bit-by-bit copy of the device (entire flash memory) and supports deleted file recovery. However, it is difficult to execute due to it requiring specialised hardware and software, and most mobile devices are typically sealed and do not support physical extraction unless the device has been rooted. A few tools can enable debugging of the root mode of the locked device; nevertheless, those few tools have a low number of supporting guides and are considerably complex to use. In contrast, logical acquisition extracts the information that is accessible and non-deleted in mobile devices operating system such as Android and IOS (Chintalapati, 2015).

2.3 MOBILE FORENSICS INVESTIGATING TOOLS

In the investigation process for combating cybercrimes that utilise smartphones and other mobile devices, gathering evidence in a forensic manner is required but challenging. With the general users of mobile devices and the intense use of social media applications on smartphones, the amount of smartphone evidence in each case can be an extremely high. For each case, many devices may be involved and the load escalates as many cases are investigated. This creates time costs and the necessity of having skilled workers. For that reason, finding a more effective way of processing devices for evidence is beneficial to the investigation.

Technology has significantly contributed to criminal investigation. Various tools have been used to assist the forensics investigation including identification and examination processes. The tools enable forensic investigators to examine the evidence more effectively and in a forensically sound manner. Pollitt (2013) stated that digital investigation without proper tool is no longer practical as systems have become more complicated and hard drive capacity on electronic devices are growing exponentially. The immense volumes of information and data that is on social media platforms could take time to sort through and to preserve relevant evidence adequately. It also might be challenging when carrying out the initial phases in the forensic process on seizure and acquisition of digital artefacts on mobile devices (Casey, 2011).

One of the vital elements that digital forensics investigators needed in order to perform an effective forensics investigation is to have knowledge of the right tool for each criminal case scenario. The knowledge will help to retrieve effectively and accurately relevant information such as communications, the timeline of evidence, associations, and geolocation information. The knowledge can save time and avoid alteration of evidence (Conti et al., 2012). Digital forensic tools that are utilised for investigation must be reliable and relevant in order to make evidence legally admissible in the court. In the following section, tools, which can be used for social media forensics investigation on Android phones will be evaluated and some information about their capabilities and limitations will be provided. Currently, the two main mobile forensics tools that have been used in most police institution around the world are Cellebrite UFED and MSAB XRY. The following table 2.2 shows the brief overview of two mobile devices digital forensic tools: MSAB XRY and Cellebrite UFED.

Table 2.2: Mobile device Forensics tools

Name	Description
MSAB XRY	MSAB provides products for extraction, analysing, and reporting. MSAB XRY has two extraction methods, namely, XRY Logical and XRY Physical. XRY Logical is the extraction method that is frequently used as it enables the investigator to access and recover live and file system data from mobile device immediately on the crime scene and this extraction method is one of the quickest extraction methods. On the other hand, XRY Physical can supports extraction of internal memory and removable media without changing the target device. XRY Physical recovers raw data from the target smartphone by bypassing the operating system and offers the chance to go deeper and recover deleted data from the target smartphone. The physical extraction is separated into two distinct stages: the initial dump stage, where raw data is recovered from the smartphone, and decoding stage, where the tool can automatically reconstruct the data into meaningful information. All the XRY extraction data results are in the proprietary XRY file format that can ensure the data and the integrity of evidence all the way to court.
Cellebrite UFED	Cellebrite UFED is a commercial mobile digital forensic tool that performs physical, logical, file system, and password acquisition on a wide range of devices and platforms, such as Android smartphones. It also performs decoding, analysis, and reporting.

These two tools are selected due they are relevant to the research and are used by law enforcement agencies and educational institutions. More detailed information regarding MSAB XRY and Cellebrite UFED can be found in following subsections 2.3.1 and 2.3.2.

2.3.1 MSAB XRY

One of commonly used mobile forensics tool by Police, Law Enforcement, Military, Government Intelligence Agencies and Forensic Laboratories to investigate crime is XRY (Walnycky, Baggili, Marrington, Moore, & Breitinger, 2015). XRY Mobile Forensic Tools is a product by Swedish company MSAB and designed for Windows. This forensic tool is a purpose-built software be equipped with all the necessary hardware to recover mobile devices data in the forensically secure manner and this tool is exclusively available for intelligence institutions, law enforcement, and military agencies.

XRY has been designed and developed to make the mobile devices forensic process much easier for the user. The user interface of XRY is simple to navigate and it provides a user-friendly wizard designed step by step process guide and a device manual that contains several lists of mobile devices that have been tested, untested and currently cannot be recovered from mobile devices. These features of XRY are useful for saving the valuable time of investigation as it provides some information regarding types of data that can be recovered from each mobile device listed.

The main use of XRY is to perform secure digital forensic extractions include logical and physical extraction of a wide variety of mobile devices such as feature phones, smartphones, GPS navigation units, 4G modems, augmented devices, portable music players, and tablets (MSAB, 2017). XRY logical extraction is a rapid extraction method that automatically recovers live file data system from mobile devices by directly communicating with the operating system of the device. Even though the result of this extraction method is equivalent with the result of manually examining screen by screen displayed data in a mobile device, the automation records all the data by capturing and screenshotting it. The logical extraction is preferable due to the extraction result being saved in proprietary XRY file format. This file format is a secure format that can preserve and guard the integrity of the recovered evidence in forensically sound manner. In addition, XRY physical extraction is an extraction method that allows examiners to dump and recover all memory and raw data from the device. This memory dump consists of complex data structures, encrypted, protected and deleted data information. Similar to XRY logical extraction, the extraction results of XRY physical extraction are also all in proprietary XRY file format (Trivedi, 2015).

The XRY mobile forensic tool not only has the ability for logical and physical extraction but also can be used to recover data information from cloud applications and non-standard mobile devices. According to MSAB, the newest version of XRY can extract more data in less time and adequately preserve the integrity of evidence from mobile digital devices. It also has a new capability in term of extracting and analysing drone data. Although XRY can be utilised in most mobile devices, there is still a large number of unsupported mobile digital devices. This might happen because of the constant changes of mobile devices especially smartphones. This issue may hinder the progress of the criminal investigation. To avoid the negative effect of this issue investigators should be more aware and familiar with the capability of forensic tools that are being employed in the investigation.

2.3.2 CELLEBRITE UFED

Another widely used tool for logical and physical extraction and analysis of mobile devices forensics is the Cellebrite ‘Universal Forensics Extraction Device’ (UFED). Cellebrite UFED is a hand-held device with optional desktop software, data cables, adapters and other peripherals. The UFED additionally has an integrated Subscriber Identity Module (SIM) reader. UFED is sold specifically only to approved corporates and governments institutions and organisations. This tool has the ability to extract both physical and logical data of mobile devices including the ability to decipher encrypted, password protected information and to recover deleted data information. Various mobile operating systems (OSs) can be extracted by this tool, including iOS, Android, and Windows Mobile, and thousands of models of phones, tablets, drones and GPS devices (Bhusari & Sahu, 2013).

When conducting a criminal investigation with the aim to acquire all possible evidence, the tools, and devices that are employed should secure the integrity of the data and also apply the extraction process in a forensically sound manner that is thoroughly and quick. The cellebrite UFED enables the retrieval of subject data such as phonebook contacts, all types of multimedia content, SMS and MMS messages, call logs, electronic serial numbers (ESN), International Mobile Equipment Identity (IMEI) and SIM location information from both non-volatile memory and volatile storage via logical ("all visible stored data on mobile devices"), file system (e.g., directories and files), or physical extractions (i.e.: hex dump, a bit-for-bit copy of a mobile device's entire storage). Physical extraction enables it to recover deleted information, decipher encrypted data, and acquire information from password-protected mobile applications such as Facebook, Skype, WhatsApp and browser-saved passwords. The UFED's physical extraction functionality can also overcome devices' password locks, as well as SIM PIN numbers. Moreover, all cable connectors from subject (source) side act as a write-blocker and read-only boot loaders keep data from being altered or deleted during a physical extraction. The feature is considered as one advantage for using cellebrite UFED for mobile device forensics investigation (Cellebrite, 2017).

2.4 SOCIAL MEDIA-RELATED CRIMES

A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-money offences, such as creating viruses on other computers or posting confidential business information on the Internet.

Most cybercrimes cannot be placed into a single crime category, which makes a statistical recording of this activity limited at best. The Internet Crime Complaint Centre (IC3) compiles and releases annual reports on the statistics and cybercrime facts. Using statistics and facts, analysts prepare reports on cybercrime trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data in public and private sectors. This also helps in the creation of tools and strategies to combat cybercriminals. Internet-connected activities are as vulnerable to crime and can lead to victimization as effectively as common physical crimes. The types of crimes that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and are provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves and their families through safe online practices.

Brunty, Miller, and Helenek (2014) outlined in which social media may be used by criminals: identity theft, burglary, social engineering, phishing, malware, cyberstalking, scamming, frauds, blackmailing, spamming, cyberbullying, exploitation, sexual assault, prostitution, organized crime, and cyberterrorism. Patton et al. (2014) also explained several types of violence that mostly happen via social media: child sex exploitation, cyber-bullying/victimisation, Electronic dating aggression/cyber-stalking, gang violence, and cyber-suicide. Furthermore, Poonia (2014) classifies types of cyber-crime into four major categories as follows:

- Crime Against Individuals

Cybercrimes carried out against individual person incorporate such sorts of violations such as transmission of Children, Harassment of anyone with the utilization of a computer, for instance, Cyber Defamation, Hacking, Trafficking, E-mail satirising, IRC Crime (Internet Transfer Chat), Net Extortion, Malicious code, Dissemination, Posting, Phishing, Credit Card Fraud and Scattering of revolting material including Software Theft. The potential mischief of such a crime to individuals is intense.

- Crime Against Property

The second type of Cyber-crimes classification relate to Cybercrimes against all types of property. These offences include digital devices vandalism (devastation of others' property), Threatening, Intellectual Property Crimes, and Salami Attacks. This sort of crime is typically prevailing in the financial organisation or with the end goal of carrying out money-related violations. A significant characteristic of this sort of offence is that the visibility is small to the point that it would typically go in secret.

- Crime Against Organisation

The third kind of Cyber-crimes classification is that, Cybercrimes against an institution. Cyber Terrorism is one distinct sort of crime in this kind. The development of cyber world and internet has exposed that the standard of Cyberspace is being utilised by people and a number of groups pressure international governments and likewise to threaten the people of a nation. By employing many features on the internet such as social media, they can persuade people to join, recruiting persons around the world, to spread the fear to a country, raise funds and collect financial support for the purpose of committing terrorist attacks.

- Crime Against Society

The fourth form of Cyber-crimes is Cybercrimes against society. In this category fraud, digital psychological oppression, web jacking, contaminating the youth through indecent, financial Crimes, cyber terrorism, Sale of Illegal Articles, Data Diddling, Salami Attacks, forgery of currency notes, check sheets and so forth can be counterfeit utilising computers, high tech devices and smart scanners and printers. Web Jacking programmers obtain entrance and control over the site of another, and they change the substance of a site for meeting political targets or for cash.

2.5 SUMMARY OF ISSUES AND PROBLEMS

Literature shows that the concept of social media forensics in the digital forensic area has developed rapidly in the past decades, and there are a lot of concerns and problems that are associated with social media forensics. There is no accepted model of professional standards or standardised tools that the investigator can use in this area.

It is important to explore the implications of social media and develop standard tools and guidelines for social media forensic investigation. Although some software companies like MSAB XRY and Cellebrite UFED can be used for social media forensics investigation, there is no central body or disciplinary board which can be used as a role model for the social media investigation process. Having a clear guideline and tools that forensic investigators can follow will be of great value for our society.

Technologies change all the time, and tools, which can help forensic experts to do their job, will also require rapid development. While it is positive news that technologies will help forensic experts to do a better performance, digital forensic experts also need to develop their skills and knowledge as a parallel with rapidly changing technologies in order to maintain themselves as a professional digital forensic expert.

There are many other challenges remaining in digital forensics investigations particularly when dealing with social media-related crimes. The following sub-sections summarise selected problems and issues associated with social media forensics.

2.5.1 Problem 1: Difficult to Assemble Credible Forensic Evidence

A forensic investigator like any other detective has to find and verify evidence in order to pursue a criminal inquiry. Digital evidence, particularly of social media, relies on experts knowing what to look for and where, the artefacts reside, before recreating digital events or tracking illicit activity and leads that can be used as evidence. This process is not as easy as casually looking into someone social media's account. The acquiring process of social media should use forensically sound tools and techniques. This process can be exceptionally challenging due to in recent years most people access their social media via applications in their smartphones. Smartphones are unique. Each of them may need particular requirements for forensic processes to function. Acquiring accurate and relevant evidence also might risk data being lost which frequently occurs in social media forensic investigations (Casey, 2011).

Preserving evidence is one of the essentials in social media forensics. To collect artefacts, investigators begin by identifying the origin of the social media account of criminals. Approximately six million Facebook users utilise their mobile-phone numbers as a user account (Cross, 2013). This is one of the difficulties, in finding the real person behind the social media account as it can be hosted by an unregistered provider. In some countries, the use of sims cards is not regulated. This has led to an increase in the number of unregistered sim cards users, for instance in Indonesia. Taking advantage of the lack of control criminals might use the sim card as a tool to create multiple and many fake social media accounts. Due to the accounts being unregistered, many of the suspects are untraceable. Therefore, it is recommended that mobile phone sim cards should be registered. If governments work together to develop a policy that mandates any mobile phone provider to register every number purchased by consumers, this can prevent untraceable cybercrime criminals.

2.5.2 Problem 2: Lack of Comprehension and Understanding from Investigators Related to Social Media Crime Cases

Social media forensics is different from computer forensics as the evidence exists not only in physical devices but also in cyber-space. Some investigators have found it hard to investigate social media-related crimes. According to a study by LexisNexis in 2012, 80 percent of law enforcement professionals were self-taught in social media forensics. A smaller number stated that their investigative knowledge was gathered through working with their colleagues. Approximately 10 percent claimed that their knowledge of social media was attained from formal training and around 33 percent reported that they did not have sufficient knowledge to use social media as an evidentiary tool (as cited in Brunty et al., 2014). As social media continues to grow globally and become more and more complex, it is paramount that the law enforcement community creates opportunities and training so that their investigators can comprehend and remain up-to-date with current social media investigative techniques and methodologies. However, to be fully capable in investigating social media-related crime cases, an investigator also needs to possess a better understanding of the forensics tools that are to be used in social media crime investigation. This would have an impact on the number of solved social media crime cases.

2.5.3 Problem 3: Jurisdictional and Law Differences

Internet Service Providers and servers are located all over the world. Social media information and data may require big data analysis and can be located in a cloud and may be spread over many providers, servers, and users (Nelson, Phillips, & Stuart, 2014). For many social media-related crime cases, to find the perpetrators, investigators need data of social media accounts that can be obtained from the social media providers. For cases related to the risk of death and imminent harm to a child, or any emergency situation such as a terrorist threat or attempted suicide, most social media platforms are willing to ‘spring' – or share with law enforcement agencies of social media information immediately. However, obtaining the information is again not easy. The legal counsel of the social media service providers may reject and deny requests by local law enforcement officers and other authorities since the legal agreement does not stipulate the required legal terms of reference (Brunty et al., 2014).

In order to preserve forensically sound data, the process of requesting data from social media service providers requires cautious attention. Social media data records will contain information and potential evidence. The record will contain the IP address history; that is the unique numbers that identify a computer on the internet and phone numbers as requested (Cross & Shinder, 2008). Some requests might be rejected by social media providers, owing to jurisdictional and law differences. For example, in some countries, such as Indonesia, defamation is a criminal offence. Yet for some providers of social media in the US, to obtain social media records such as IP addresses cannot be gained due to defamation in the US is not a criminal offence (Burden & Palmer, 2003). If IP addresses and other information related to the suspect cannot be gathered, the case will remain unsolved. To tackle these cases related to defamation, would be possible if there were international agreements with providers regarding social media records across jurisdictional and law differences.

2.5.4 Problem 4: Lack of Specially Designed Tools for Social Media Forensics

Several digital forensics tools have been developed, however, there are no dedicated forensic tools or techniques designed exclusively for social media forensic investigation. Whilst working with social media, forms of forensics differ widely owing to; a lack of physical access, the remote nature of the evidence and the level of trust in the authenticity and integrity amongst the online community. Another problem with undertaking social media forensics is whether the remote data or data ownership is forensically sound and whether the distributed and 'elastic' data chain of custody, and large data volumes can be deciphered (Dykstra & Sherman, 2012).

The immense volume of information on social media apps takes time to sort through for preserving relevant evidence. It can also be challenging when carrying out the initial phases of the forensic process in the seizure and acquisition of digital artefacts (Casey, 2011). Huber et al., (2011) have developed a solution to this retrieval process from social media services by using a hybrid system in combination with a web crawling component with a custom add-on for social media that harvests date from social media. The datasets that are collected contain profile information and associated 'metadata'. The use of this open source software (social snapshots) reduced significantly, the time taken to scan social media with access to additional and hidden information. This software might be used in the future to improve efficiencies at the acquisition stage in social media forensics. However, in order to execute the collection and analysis of the social media evidence properly and in a forensically sound manner, other tools and techniques need to be utilised and developed so that the forensic investigator can perform effectively and efficiently when dealing with evidence from social media particularly when investigating social media applications on smartphones.

2.5.5 Problem 5: Unavailability of International Standard Procedure in Social Media Forensic Investigation

Social media forensics has remained ineffectual as there is no agreed international standard for social media forensics investigation. Beebe (2009) has said that digital forensics largely lacks any standardisation of process (Garfinkel, 2010) with regards to procedures or management. According to the Oxford dictionary, a standard implies a measure, norm, or model for comparative evaluation. Having a standard can set up a protocol that everyone recognises and can adapt. With the increase in cybercrime, particularly international social media-related cases, the development and enhancement of digital forensics and social media forensics is a necessity. It is now vital to draw up a suitable international standard for the procedure, codes of ethics, and standardised techniques for social media forensic investigation. By doing so it is hoped that this will minimise issues, problems, and constraints in social media forensics investigation and lessening challenges while investigating transnational social media-related cases.

2.5.6 Problem 6: Shortage of tools and monitoring of handling multiple social media public activities.

Although the argument of privacy versus safety is always a controversial one, even when it comes to monitoring social media for law enforcement purposes (Cross, 2013). It is necessary for monitoring particularly of multiple social media channels. Social media penetrates the lives of its members; it is available at any hour of the day on any device. Malicious people do not have office hours and they can carry on their illicit activity at any time of day. Criminals can work on a global scale having multiple social media accounts on more than one site. While monitoring of activity is essential in many countries they do not have any monitoring, especially for multiple social media activities. Social media platforms, as a result, are used by terrorist groups, human traffickers, prostitution networks, child pornography rings and so forth, on both an international and domestic scale. With the ability to monitoring multiple social media platforms, it is becoming possible to effectively to give attention to illegal activity early (pre-emptive actions) and detect suspicious activity. The potential for uncovering posts, tweets, pictures, videos or other probative evidence can be identified and the criminal associates affiliated with persons of interest can be apprehended.

2.6 CONCLUSION

A thorough analysis of literature that is related to social media forensics has been made in this literature review chapter. An information on the current state of knowledge and trends associated with social media was discussed. It is noted that the most of users now are utilising the apps via their smartphone to access their social media platforms. The social media not only provides opportunity in positive purposes such as the financial sector, where it can be used as a publishing and marketing instrument, but also social media can be utilised by some people for negative and illicit intentions, that for example, can be media content offences or a target of crime.

As can be seen in the prior section of the literature review, statistics indicate an increase of social media users year on year and also major improvements in social media features. These have resulted in emerging benefits and also challenges for the users and law enforcement institutions especially in term of social media-related crime investigation. In cybercrime investigation, especially social media-enabled crime investigation, investigating social media in a smartphone can be exceptionally complex due to variable hardware (even though the same smartphone’s brand and same OS, they are all unique). Hence, investigating mobile devices is likely to be more intricate than other digital devices such as a computer. Even though nowadays there are several available tools and techniques that can be used for investigating mobile devices such as smartphones, an investigator cannot randomly use those tools and techniques. Investigators are required to utilise the right tools and techniques, in order to ensure social media and the smartphones investigation process is effective and forensically sound. Moreover, social media features are also developing constantly. An investigator, has to understand which are the effective tools and techniques for undertaking social media-enabled crime cases that utilise social media applications in smartphones. Section 2.3 introduced mobile device forensic tools that are extensively used in law enforcement institutions. Two mobile device forensic tools were chosen for detailed study, to establish each forensic tools' capability in a social media investigation.

As social media platforms are significantly growing in functionality and there is a vast development of smartphones, continuous monitoring and sufficient knowledge will be required in order to investigate social media applications in smartphones satisfactorily. It is proposed that this research will focus on the comparison of smartphones forensic tools capability in investigating social media applications in Android smartphones. In chapter 3, the proposed testing methodology and design of the study will be defined, and the research limitations also will be identified.

Chapter Three

RESEARCH METHODOLOGY

3.0 INTRODUCTION

The literature review completed in Chapter 2 provides information about social media, mobile phone forensics, and investigating tools that can be used to collect evidence from social media applications on mobile devices in a forensically sound manner. The literature also highlighted social media-related crimes and several issues that surround the topic of investigating cybercrime cases, especially social media-enabled crimes that require gathering social media evidence. There are challenges in assembling credible forensic evidence from mobile devices due to the advanced technology of smartphones (Sathe & Dongre, 2018), jurisdictional and law differences and the lack of understanding of investigation requirements related to social media crime cases (Wall, 2015).

The aim of Chapter 3 is to decide a research question and to develop a pertinent research method to answer the question. Two chosen mobile devices forensic tools from the literature review will be tested and analysed for identifying the most effective tool for investigating social media-related crime cases. Namely, Cellebrite UFED and MSAB XRY.

The research question of this study and hypothesis derived from section 2.5 will be elaborated in section 3.1. In section 3.2 the proposed design of the study will be outlined to facilitate answering the research question and sub-questions. The testing design including data collection procedures will be explained in section 3.3, followed by the testing methodology in section 3.4. In section 3.5 the research limitations will be identified and discussed. The chapter concludes in section 3.6.

3.1 THE RESEARCH QUESTION AND HYPOTHESIS

The literature review in Chapter 2 provides a background of theoretical knowledge in regard to the chosen research area of evidence collection of social media applications on Android phones with the aim to ameliorate investigation process on social media-related crime cases. An assorted body of literature has been elaborated, starting with social media forensics in general, social media-enabled crimes, challenges and issues associated with social media forensics investigation process.

The research question was developed based on the literature review in chapter 2. First, it is quite common to find mobile phones as a source of evidence, as most people even offenders are using smartphones for communication. Smartphones have applications with performance that is nearly as good as a computer (Pierce, 2018). Second, people nowadays are always connected with the internet and social media everywhere, every time, every day without a need to login in to a computer (Brown, 2015). By using their smartphones and the applications (such as social media apps) they can commit malicious acts and criminal activities such as drug trafficking, scams, online threats/stalking, child abuse (sexual exploitation), cyberbullying, cyberterrorism (terrorism recruitment, spread threat and terror, and terrorist financing) (Hayes & Luther, 2018). Therefore, the investigator has to evaluate, test and compare existing mobile device forensics tools that are utilised for investigating smartphones and work out the best choices. Research shows that currently the most used propriety tools are Cellebrite UFED and MSAB XRY (Hassan & Pantaleon, 2017).

The research question addresses the chosen mobile forensic tools ability to provide a substantial contribution to investigation processes when dealing with social media-related crimes. Sub-questions can concern what features of each tool that offer the best way to collect meaningful evidence from social media in Android phones.

This research will explore mobile forensic tools capabilities by posing the following main research question:

> ***What are the capabilities of the chosen mobile devices forensics tools (i.e., Cellebrite UFED and MSAB XRY) when examining Social Media applications on Android smartphones in a social media-related crimes investigation?***

As reviewed in chapter 2, forensic work plays a significant role in cybercrime investigation. The main focus of this study is to examine (1) the accuracy and completeness of evidence collection from social media apps on Android smartphones (2) to assess the ability to find probative artefacts from social media applications on Android phones by using Cellebrite UFED and MSAB XRY, and (3) to evaluate both smartphone forensics tools by comparing the performance when collecting social media evidence.

In order to answer the main research question, associated sub-questions are formulated:

> **The Sub Question 1:** *What extraction type of mobile device forensics tools are pre-eminent for collecting evidence from Social Media on Android phones?*
> **The Sub Question 2:** *Are the chosen mobile device forensics tools capable to examine all three selected Android smartphones?*
> **The Sub Question 3:** *Which tool is the best performer for Social Media investigations?*

The key findings from the research testing will be used to evaluate the questions. From the analysed, possibilities can be explored to combine all the strengths of existing tools to maximise the effectiveness of the Social Network Forensic investigation process. The result of the capability comparison of the chosen tools would then enable the investigator to evaluate whether the tool chosen meets the requirements demanded by their scenario, and to improve the efficiency of the investigation process. Answering above sub-questions will indicate ways which those combined strengths from existing tools can be structured by methodology to satisfy both forensic examiners and thus the court of law.

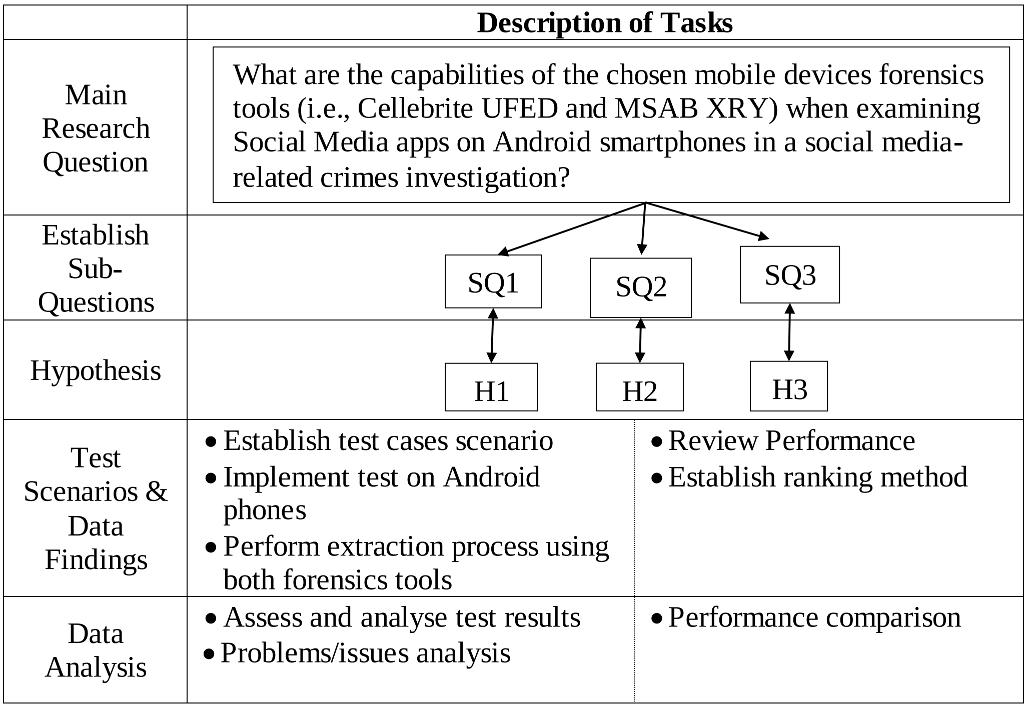
A number of hypotheses have also been developed for each of the sub-questions. The hypotheses have been devised in order to link with each sub-question and to inform the main research question.

Hypothesis 1: *File system extraction of Cellibrite UFED is the best extraction type when gathering evidence from social media applications on Android smartphones.*

Hypothesis 2: *The both selected mobile forensics tools are able to examine all three chosen Android smartphones.*

Hypothesis 3: *Cellebrite UFED will perform better than MSAB XRY.*

By aiming to answer the designed research questions and validate the proposed hypotheses that are related to each sub-question, a research flow chart was developed for guiding the main phases of evaluation for the two selected mobile forensics tools.



	Description of Tasks	
Main Research Question	What are the capabilities of the chosen mobile devices forensics tools (i.e., Cellebrite UFED and MSAB XRY) when examining Social Media apps on Android smartphones in a social media-related crimes investigation?	
Establish Sub-Questions	SQ1 SQ2 SQ3	
Hypothesis	H1 H2 H3	
Test Scenarios & Data Findings	• Establish test cases scenario • Implement test on Android phones • Perform extraction process using both forensics tools	• Review Performance • Establish ranking method
Data Analysis	• Assess and analyse test results • Problems/issues analysis	• Performance comparison

Figure 3.1: Research Flow Chart

Figure 3.1 presents the flowchart outlining the main research question, sub-questions and the links to associated tool evaluation phases.

3.2 DESIGN OF STUDY

The aim of the study is to conduct research concerning capabilities of selected mobile forensics tools to develop potential and crucial data evidence from social media applications on smartphones in relation to social media-enabled crime investigations. By evaluating each tool information may be gained to improve the investigation processes. The two selected mobile device forensic tools that were identified in chapter two will be assessed and compared through an analysis of the data results. Those two digital forensic tools will be used to examine three different Android smartphones. Namely, Samsung S4 Mini, Samsung J5 Prime, and Oppo A57. On each Android smartphone, the social media applications Facebook, Twitter, and Instagram will be installed. After that, the designed test scenarios will be implemented, then the examination process initiated with the chosen forensics tools.

In this study, there is a need to collect, analyse, and interpret quantitative and qualitative data in one study, a mixed methodology consists of quantitative and qualitative data will be used to perform an analytical comparison between MSAB XRY and Cellebrite UFED. The quantitative data will consist of how many instances of specified planted social media status (posts), photos, chat messages, and videos in Android smartphones that can be gathered by the selected mobile forensic tool. The qualitative data will generate a more comprehensive understanding that will help to answer the research question. By applying the mixed methodology, it will help the author to address research questions and also in-depth evaluation of the tools' capabilities can be reported.

The research design phases are shown in the following figure 3.2.

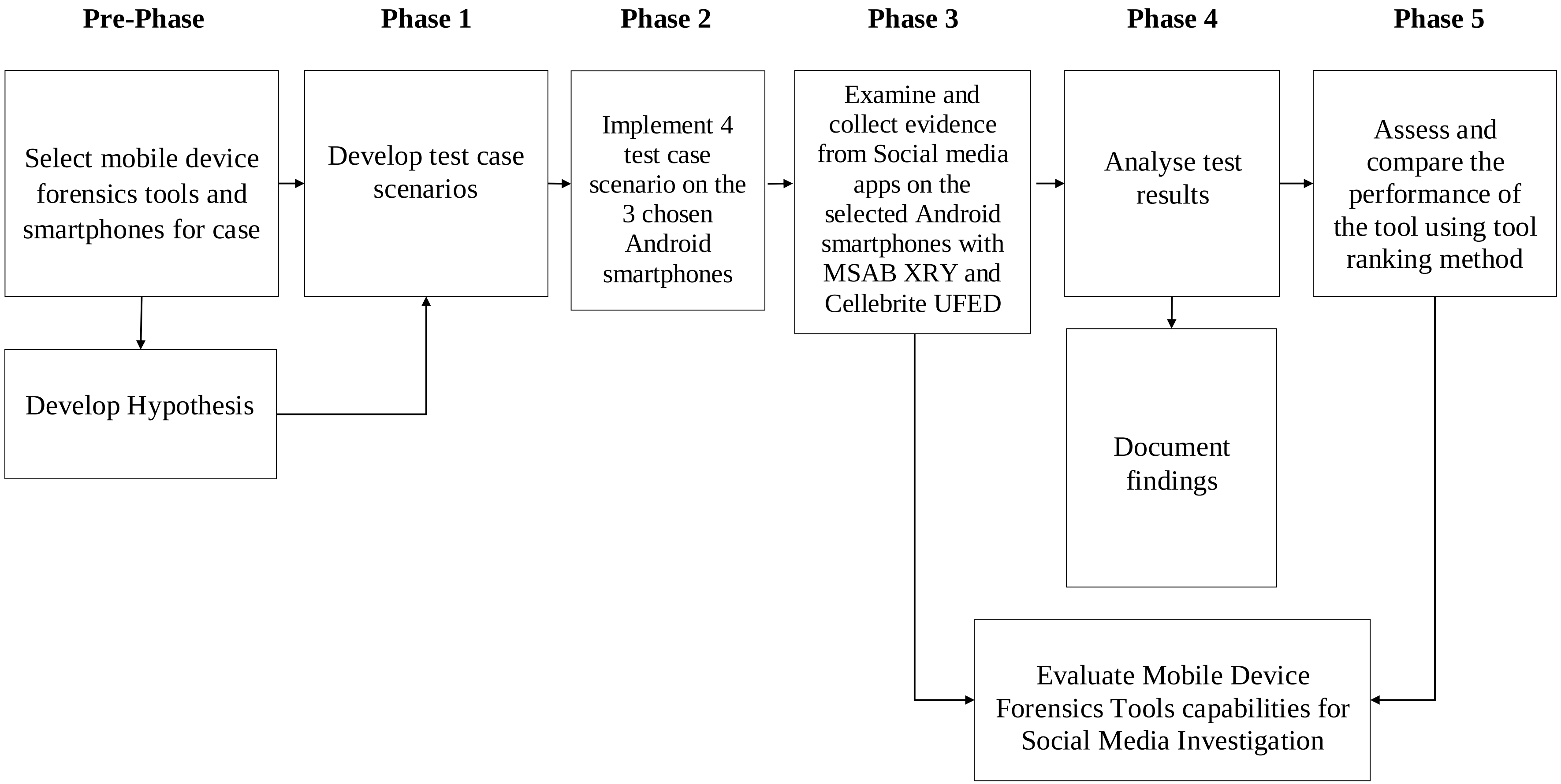

Pre-Phase
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Select mobile device forensics tools and smartphones for case
Develop test case scenarios
Implement 4 test case scenario on the 3 chosen Android smartphones
Examine and collect evidence from Social media apps on the selected Android smartphones with MSAB XRY and Cellebrite UFED
Analyse test results
Assess and compare the performance of the tool using tool ranking method
Develop Hypothesis
Document findings
Evaluate Mobile Device Forensics Tools capabilities for Social Media Investigation

Figure 3.2: Research Design Phases

3.3 TESTING DESIGN

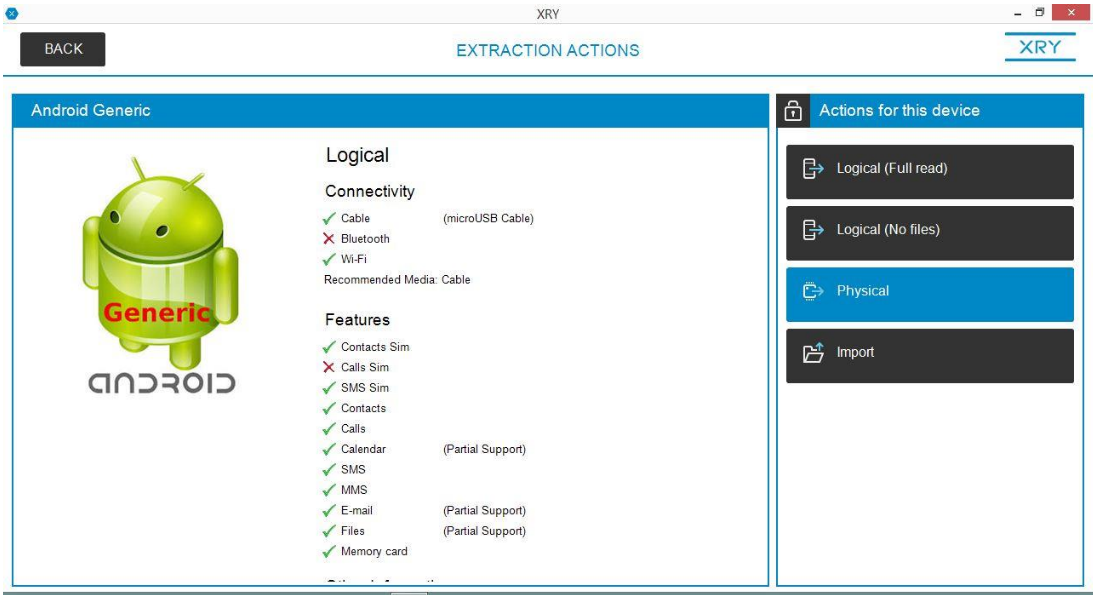
The testing consists of three phases: 1) preparation, 2) data collection, and 3) data analysis. The detailed preparation, data collection, and data analysis phases are explained in the following sections.

3.3.1 Preparation

In this research, all smartphones will be wiped before the evidence is planted. The step minimises and eliminates unused excess data that can hamper the extraction process. After the wiping process, all social media applications (Facebook, Twitter and Instagram) are installed on all smartphones. Then, the evidence is planted and after that, the smartphones are examined by utilising MSAB XRY and Cellebrite UFED, independently and under the same conditions.

3.3.2 Data Collection

The top two most used of mobile forensics tools are utilised in the data acquisition phase i.e. MSAB XRY and Cellebrite UFED. Each tool has their own characteristics. Even though all smartphones all used the Android operating system when they were examined different cables had to be selected to connect each tool. MSAB XRY that is used in this research is XRY version 7.6 that was launched in December 2017 and is able to process two extraction types, namely logical extraction and physical extraction. On the other hand, Cellebrite UFED that is employed in this research is UFED touch 2, UFED 4PC and UFED Physical Analyzer 7.1 and has more extraction type options, such as logical extraction, file system extraction, and physical extraction. More detail of the extraction type option of both mobile forensic tools can be seen in figure 3.3 and figure 3.4.



Logical

Connectivity

- ✓ Cable (microUSB Cable)
- ✗ Bluetooth
- ✓ Wi-Fi

Recommended Media: Cable

Features

- ✓ Contacts Sim
- ✗ Calls Sim
- ✓ SMS Sim
- ✓ Contacts
- ✓ Calls
- ✓ Calendar (Partial Support)
- ✓ SMS
- ✓ MMS
- ✓ E-mail (Partial Support)
- ✓ Files (Partial Support)
- ✓ Memory card

Figure 3.3: MSAB XRY Extraction Types Option

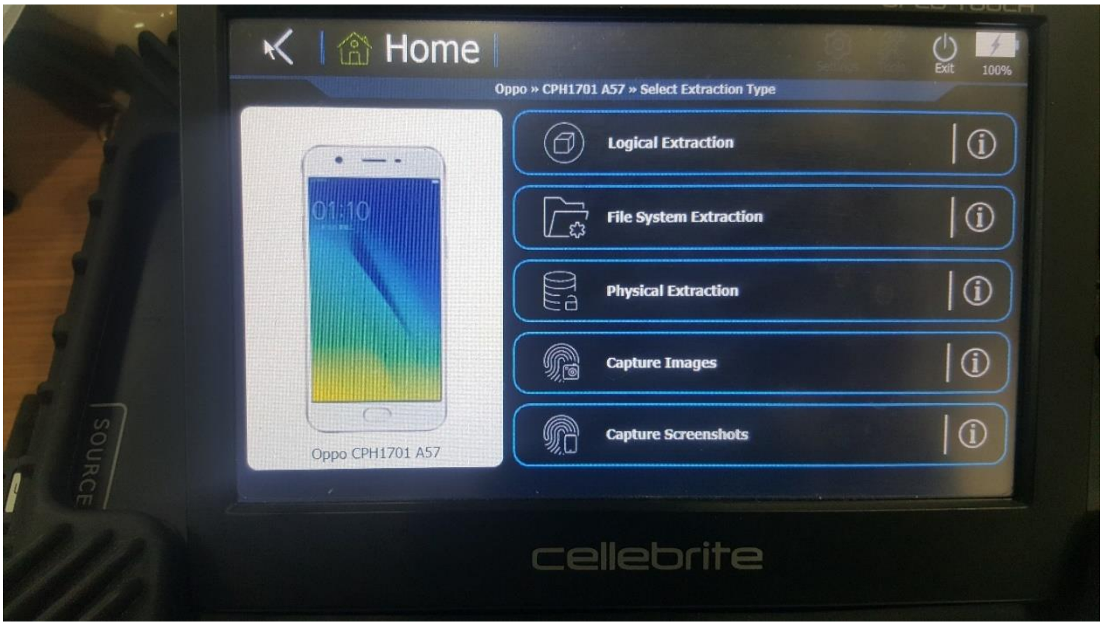


Figure 3.4: Cellebrite UFED Extraction Types Option

3.3.3 Data Analysis

Achieving reliable outputs and results, with precise data analysis procedures are necessary for trustworthy findings. Data analysis begins with the first step of determining the total number of social media application artefacts. In order to ascertain this, all the social media applications are being examined by utilising two mobile devices forensic tools. The second step is running the smartphones digital forensic tools. Each forensic tool is used to parse and examine the smartphones. The third step is analysing the output and results for determining each tool capability. By finding the capabilities further investigations can benefit by knowing the limitations. Figure 3.5 shows the data analysis procedures.

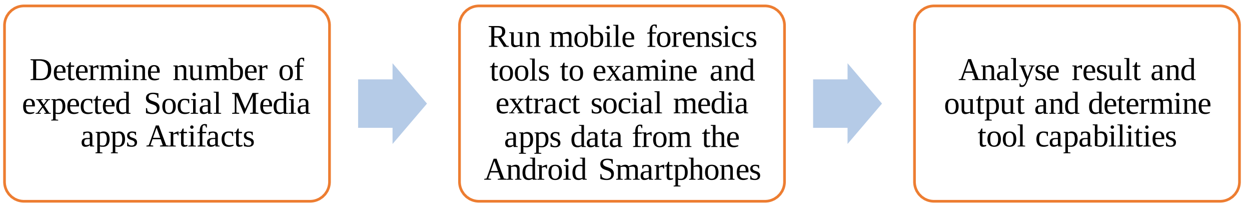

Determine number of expected Social Media apps Artifacts
Run mobile forensics tools to examine and extract social media apps data from the Android Smartphones
Analyse result and output and determine tool capabilities

Figure 3.5: Data Analysis Procedure

3.4 TESTING METHODOLOGY

A mobile devices digital forensic tools methodology is being used to conduct the research regarding the capabilities of two chosen mobile device forensic tools for extracting android social media applications, with data information such as videos, photos, and other artefacts of social media activity on Android phones. The aim of knowing this information is to assist investigation processes to become more efficient. Figure 3.6 displays the testing procedure used to evaluate the capabilities of two mobile device digital forensic tools.

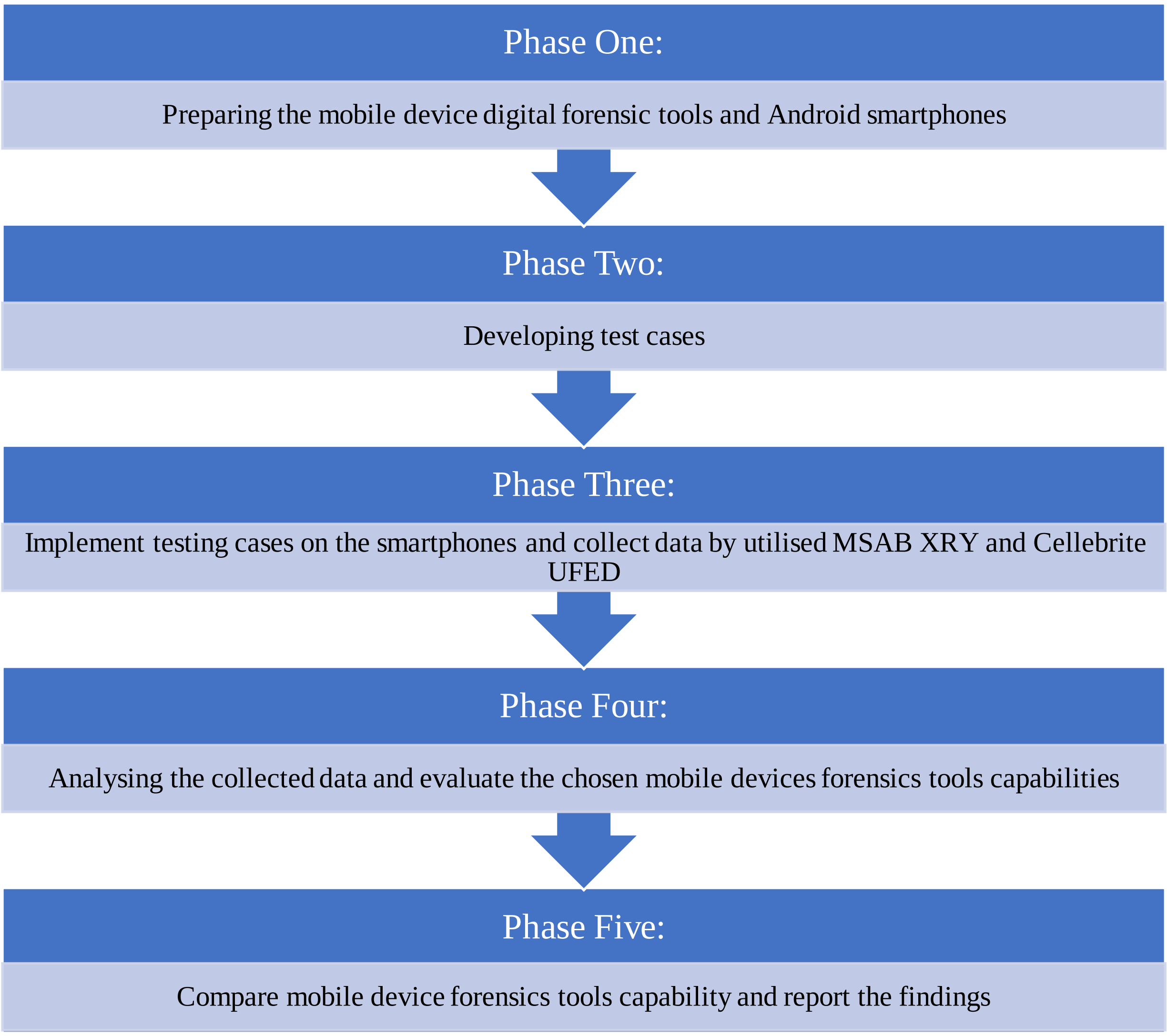

Phase One:
Preparing the mobile device digital forensic tools and Android smartphones
Phase Two:
Developing test cases
Phase Three:
Implement testing cases on the smartphones and collect data by utilised MSAB XRY and Cellebrite UFED
Phase Four:
Analysing the collected data and evaluate the chosen mobile devices forensics tools capabilities
Phase Five:
Compare mobile device forensics tools capability and report the findings

Figure 3.6: Tool Testing Methodology Overview

3.4.1 Test Scenarios

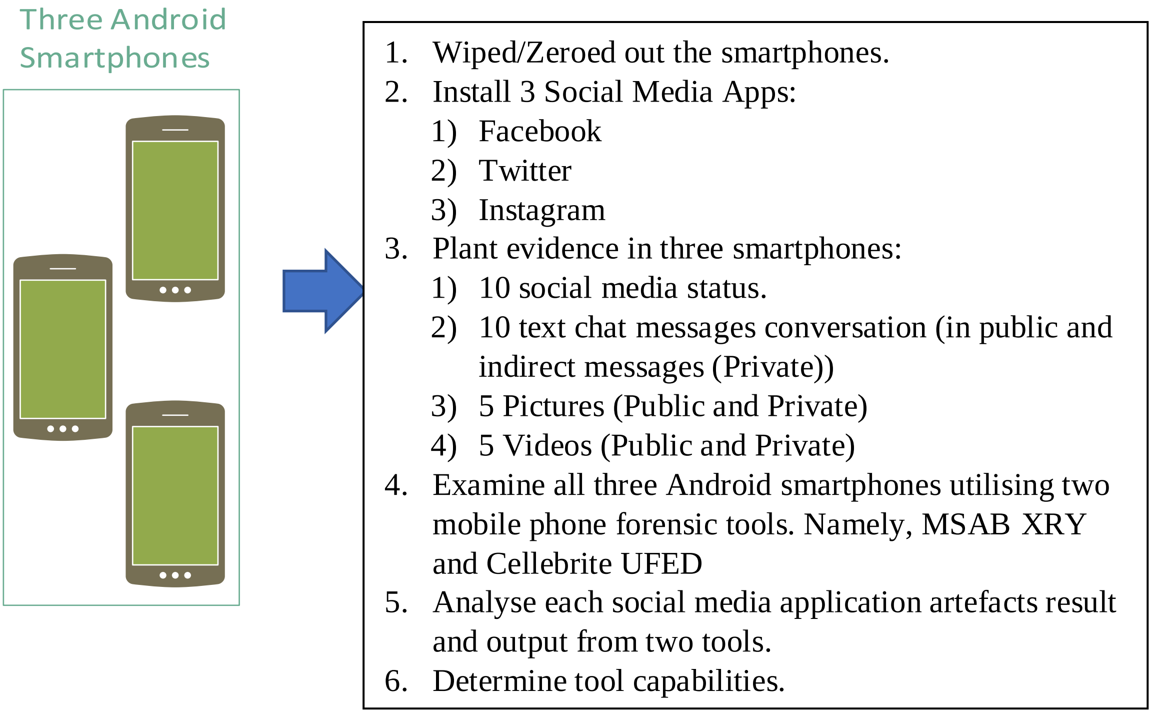
The following tool testing scenarios are developed based on social media feature data that is most likely be classified as potential evidence. A total of four test scenarios are identified as significant for data collection. They will also provide the information to determine actions, relationships and events. The feature data mostly can be found in all selected social media platforms, which are social media status (posts), chat messages, photos, and videos. The feature data plays a major role in the social media investigation process. More detail each feature data set is shown in table 3.1. Table 3.1 shows the identified test scenarios with their particular test scenario number and description of the functionality of each test that is based on four main social media data features. Each test case represents the artefacts that need to be collected from each test by utilising both smartphone forensic tools.

Table 3.1: Test Cases of Social Media Apps Features on Android Smartphones.

Test Case	Test Case Name	Test Tool Functionality
TC01	Social Media Status (posts) Analysis	Identifying the key actors in a particular case with all the names included in a particular post and finding out about the nature of the relationship among the key actors.
TC02	Chat messages Analysis	Examine and provide detail of all chat conversation messages from all selected social media apps.
TC03	Photos Analysis	Identify availability of all photos that have been uploaded in public and private in Instagram, Facebook and Twitter.
TC04	Videos Analysis	Examine all videos in Instagram, Facebook and Twitter that have been uploaded in public and private.

3.4.2 Test Procedures Overview

Building up a robust and forensically viable testing environment is necessary in order to obtain a forensically sound result. In this subsection, the practical considerations are reviewed of the testing procedure from the beginning: wiping out the smartphones until the final step: evaluation and determination of the best mobile forensic tools for dealing a social media enabled crime cases. Figure 3.7 displays the test procedures overview. The first four steps are classified as the pre-extraction procedure. From the figure, it can be seen that the test started with the three selected Android smartphones being wiped before the test begins. The next step is three social media apps are installed (all of which are the most recent version). The next step is planting designed evidence on those three Android smartphones. After that, all Android smartphones are extracted using MSAB XRY and Cellebrite UFED. The results from those tests are analysed and the results can be used for addressing the research questions.



1. Wiped/Zeroed out the smartphones.
2. Install 3 Social Media Apps:
   1) Facebook
   2) Twitter
   3) Instagram
3. Plant evidence in three smartphones:
   1) 10 social media status.
   2) 10 text chat messages conversation (in public and indirect messages (Private))
   3) 5 Pictures (Public and Private)
   4) 5 Videos (Public and Private)
4. Examine all three Android smartphones utilising two mobile phone forensic tools. Namely, MSAB XRY and Cellebrite UFED
5. Analyse each social media application artefacts result and output from two tools.
6. Determine tool capabilities.

Figure 3.7: Test Procedures Overview

3.5 LIMITATIONS OF RESEARCH

The research evaluates two prominent mobile digital forensic tools' capability in the case of social media investigation on smartphones. When social media are involved in a crime, the investigator needs to choose digital forensic tools to examine, gather, and analyse the evidence from digital devices such as tablets, computers, and smartphones. Each of those devices is unique. They have been developed in their own particular ways. For that reason, for an investigator it is necessary to understand which digital forensic tools are capable to be used for investigating social media-enabled case evidence. Nowadays, the most frequent digital device that has evidence in a social media-enabled case is smartphones. Dealing with smartphones is not a simple task due to each of them having unique characteristics. Not only the evidence is distinctive but also the mobile forensic tool that is used for examination of smartphones has its own functionalities and limitations. In order to appropriately perform a forensically sound investigation, it is essential to identify those characteristics and limitations.

The first limitation of the proposed research is that only two mobile phone forensics tools have been selected due to known reputation. A number of other mobile phone forensic tools are available, and they can also be used for social media forensics, however, the focus of this research is on the top two smartphone forensics tools in use. The second limitation is that this research focuses solely on one smartphone operating system, namely, Android operating system. This research might not represent the overall capability of each forensic tool, but it does provide qualified information regarding their capability when investigating social media enabled crime cases.

Another limitation of the proposed research is extra matters. The retrieved data is possibly different on a case-by-case basis. First, each model of a smartphone may not be the same as the same model of smartphone that is manufactured in a different country, and with the one that was used in this research. Second, the additional hardware of the tool such as cables also must be taken into consideration because if there is some tiny problem with the cable during the extraction process, the extraction process might be unsuccessful or immediately abortive. Third, the testing environment has been designed for the specific purpose of this study. Therefore, it might not be completely representative of all social media investigation environments.

3.6 CONCLUSION

Literature review in Chapter 2 indicated that there is needed to look into an effective way to extract social media evidence from smartphones. Digital forensic investigators are required to understand numerous different tools and techniques to gather potential evidence, and researching the capability of available forensic tools will enhance the quality of the investigation process.

In subsection 3.1, the main research question, sub-questions, and hypothesis have been defined. The research questions and hypothesis are the key focus of this research. Subsection 3.2 discussed the research design that will be used to address all the research questions. The proposed research will look at the capability of mobile phone forensic tools for retrieving social media as potential evidence data. There are three testing phases for this proposed research outlined in subsection 3.3. In subsection 3.4, the testing methodology including test cases and testing procedures was outlined. The limitations of this research are discussed in subsection 3.5, providing information that must be taken into consideration. The next chapter four will present the evidence collected by applying the methodology of this chapter. The research findings also provide comparison results of the chosen smartphones forensics tools that can show the tools' capability when investigating social media applications in Android smartphones. The research will inform investigators and give a clearer view of dealing with particular android smartphones when conducting social media investigations. Also for future improvement to address the identified flaws that tool developers may use.

Chapter Four
RESEARCH FINDINGS

4.0 INTRODUCTION

A mobile phone forensics tool that can gather most of the social media evidence in a smartphone is required for social media investigation. Social media platforms in the form of applications on smartphones such as Facebook, Twitter, and Instagram have become primary everyday communication, and nowadays have functionality and features that are changing relentlessly. Those changes generate a significant increase in the amount of potential sources of social media evidence and make investigators to work extra hard because there is enormous amounts of data that should be examined on smartphones. These concerns require the investigator to understand the capability of available forensic tools when examining social media applications on smartphones in order to critically analyse the evidence and to improve the effectiveness of the social media investigation. Chapter 3 provided the main research question and sub-questions based on the issues identified in chapter 2. The research design phases and testing methodology was formulated to answer the research questions.

The aims of chapter 4 are to report the research findings and the comparison results of the chosen smartphone forensics tools by implementing a test rating method. The data are being used to evaluate the capability of both tools. This chapter 4 consists of three major sections. Section 4.1 sets up the tool ranking method that can help determine which tools is more capable when examining social media artefacts in Android smartphones. The summarised collected data and the testing result is presented in section 4.2. In section 4.3, the analysis report of each tool is presented and compared to find out the most capable social media forensics tool.

4.1 TEST RATING METHOD

In regard to distinguishing the most capable social media forensics tool between MSAB XRY and Cellebrite UFED, the data findings of each tool will be compared. Each case consists of specific planted data (social media features) such as social media status (posts), photos, chat messages, and videos. In this chapter, the extraction data result from each case will be shown in tables. Each table contains information about retrieved data compared to the total number of artefacts that were planted in the smartphones. The test rating method is also implemented to discover which of the chosen forensic tools that is better in social media investigation.

A rating scale is applied to rate all four test scenarios to determine each of forensic tool capability in a social media investigation. The details of all test scenarios can be seen in chapter 3.4.1. The rating scale is from 0 to 3. If a tool fails to recover any data in smartphones, it is rated a 0. A rating of 1 indicates some data was found, but insufficient for robust acceptance. A rating of 2 indicates the tool meets the search data requirement. A rating of 3 indicates the tool is able to recover most of the expected data and the tool provides an exceptional data result. More details of the forensic tool rating scale can be seen in table 4.1.

The following table 4.1 displays the test rating scale consists of the associated description, rating standard and percentile grouping.

Table 4.1: Mobile phone forensics test rating scale

Rating	Description	Rating Standard	Percentage Found
0	Miss	Unable to find any evidence	0%
1	Below	Sometimes able to find evidence but not adequate	1% - 30%
2	Meet	Able to meet the search data requirement	31%-60%
3	Above	Able to meet the requirement and provide excellent results	61% -100%

It is necessary to know the expected data from the smartphones before a tool rank test can be performed so that each tool's data results can be compared against the expected data quantity. In order to have determine the accuracy of the test result, prepared social media status (posts), chat messages, photos, and videos have been posted on each social media application. The findings from the tests of two mobile phone forensic tools for each test scenario are summarised and discussed in section 4.2 below.

4.2 TEST FINDINGS

MSAB XRY and Cellebrite UFED have produced examination results in their own specific file extension xry format as files and ufdr files, respectively. There are three smartphones that were used in this research: Samsung S4 Mini, Samsung J5 Prime and OPPO A57. The following sub-sections show the extraction result of the two selected smartphones forensics tools.

4.2.1 Overall Extraction Process

Two mobile phone forensic tools are utilised to extract social media artefacts from three smartphones that were specified earlier. Before the extraction process all three smartphones had the pre-extraction procedure performed. The pre-extraction procedure has been identified in chapter 3.4.2, figure 3.2. First, all three smartphones were wiped. Next, three social media applications (Facebook, Twitter, and Instagram) were installed and then the prepared social media evidence such as social media status (posts), chat messages conversation, pictures, and videos were planted on all three smartphones. After the whole pre-extraction procedure was completed, the extraction process was carried out.

Two smartphones forensic tools that were used in this research have distinctive extraction options. MSAB XRY has two extraction types which are logical extraction and physical extraction. Whereas, Cellebrite UFED has more extraction types such as logical Extraction, file system extraction, and physical extraction. A summary of extraction types of MSAB XRY and Cellebrite UFED is illustrated in figure 4.1 as follows:

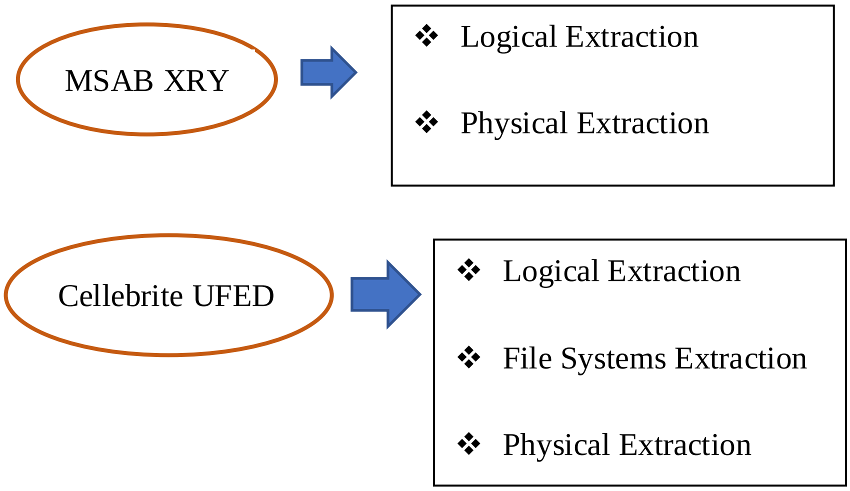


Figure 4.1: Extraction Types

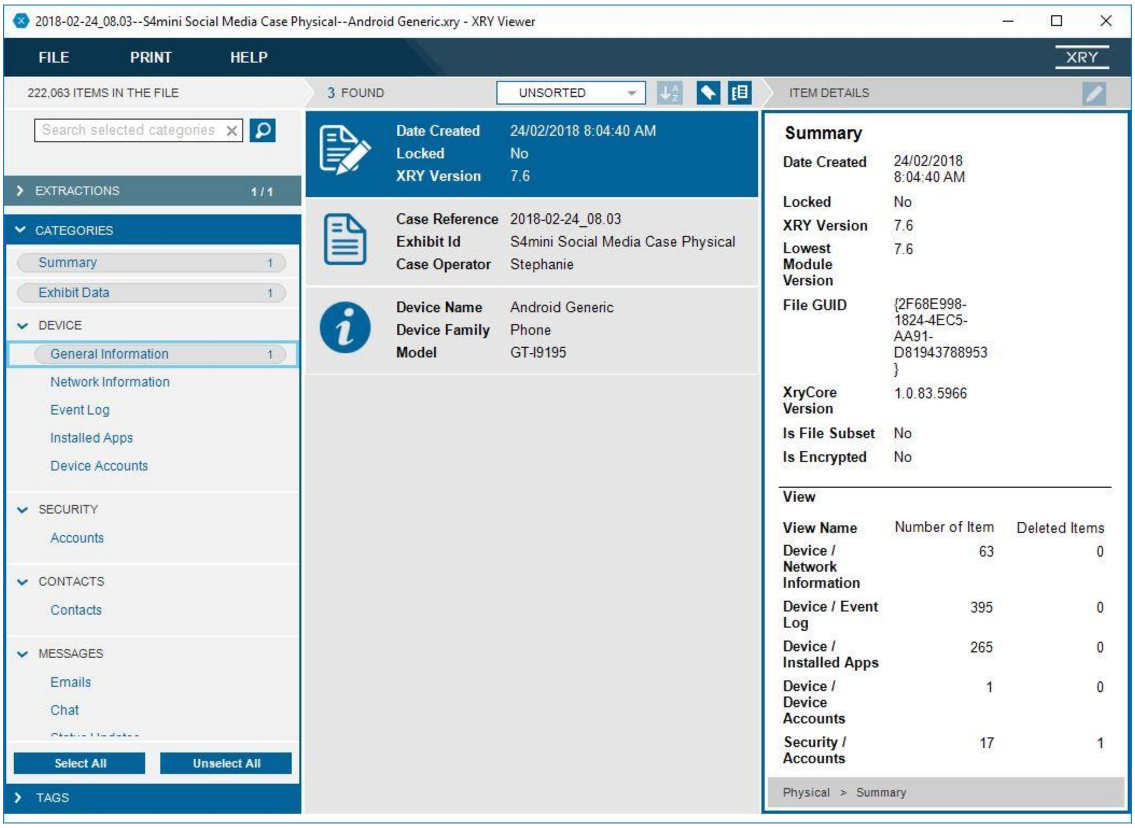
The first tool that was employed is MSAB XRY version 7.6 seen in figure 4.1. This tool can perform two types of mobile devices extraction such as physical extraction and logical extraction. However, in fact, this tool can only process the physical extraction in the older type of smartphones. Among three smartphones that were used in this research (Samsung S4 Mini, Samsung J5 Prime and OPPO A57), only Samsung S4 mini (released in 2013-2014) that can be physically extracted by MSAB XRY and for Samsung J5 prime and OPPO A57 that were released in 2016 and 2017, respectively. MSAB XRY can only logically extract Samsung J5 Prime and still cannot examine OPPO A57 due to the phone is not yet on the extractable list in this mobile device forensic tool.

On the other hand, mobile device forensic tool Cellebrite UFED 7.1 offered more variation of extraction options such as physical extraction, file system extraction, and logical extraction. There is also a sub extractions process under file system extraction. Similar with MSAB XRY, Cellebrite UFED also has limitation for extracting from recent smartphones. In this research, Samsung S4 mini is the only smartphone that can be physically extracted by Cellebrite UFED and both phones (Samsung J5 Prime and OPPO A57) that were released in recent years can only be logically extracted and the file system extracted. A summary of the list of smartphones that were used in this research can be seen in the following table 4.2.

Table 4.2: List of Smartphones that used in this research

	MSAB XRY	Cellebrite UFED
Samsung S4 Mini	✓ (Logical & Physical Extraction)	✓ (Logical, File System & Physical Extraction)
Samsung J5 Prime	✓ (Logical Extraction)	✓ (Logical & File System Extraction)
OPPO A57	✗	✓ (Logical & File System Extraction)

In terms of capability, by looking at the number of smartphones that can be extracted, Cellebrite UFED surpasses MSAB XRY due to Cellebrite UFED can examine OPPO smartphone that cannot be extracted by XRY. Both smartphone forensic tools cannot perform multiple extractions simultaneously and can extract one smartphone each time. The time required for the process of extraction varies. There is no fixed time benchmark given and this is influenced by many factors. During the extraction process, each smartphone has to use a particularly designed cable that is assigned by the forensic tool. The erroneous use of a cable might alter the extraction result. Each extraction generates the result in a particular file extension that can only be opened with specific software reader for each forensic tool. Figure 4.2 and figure 4.3 show the screenshot of the example of MSAB XRY and Cellebrite UFED reports.



2018-02-24_08.03--S4mini Social Media Case Physical--Android Generic.xry - XRY Viewer

222,063 ITEMS IN THE FILE

3 FOUND

Date Created 24/02/2018 8:04:40 AM
Locked No
XRY Version 7.6

Case Reference 2018-02-24_08.03
Exhibit Id S4mini Social Media Case Physical
Case Operator Stephanie

Device Name Android Generic
Device Family Phone
Model GT-I9195

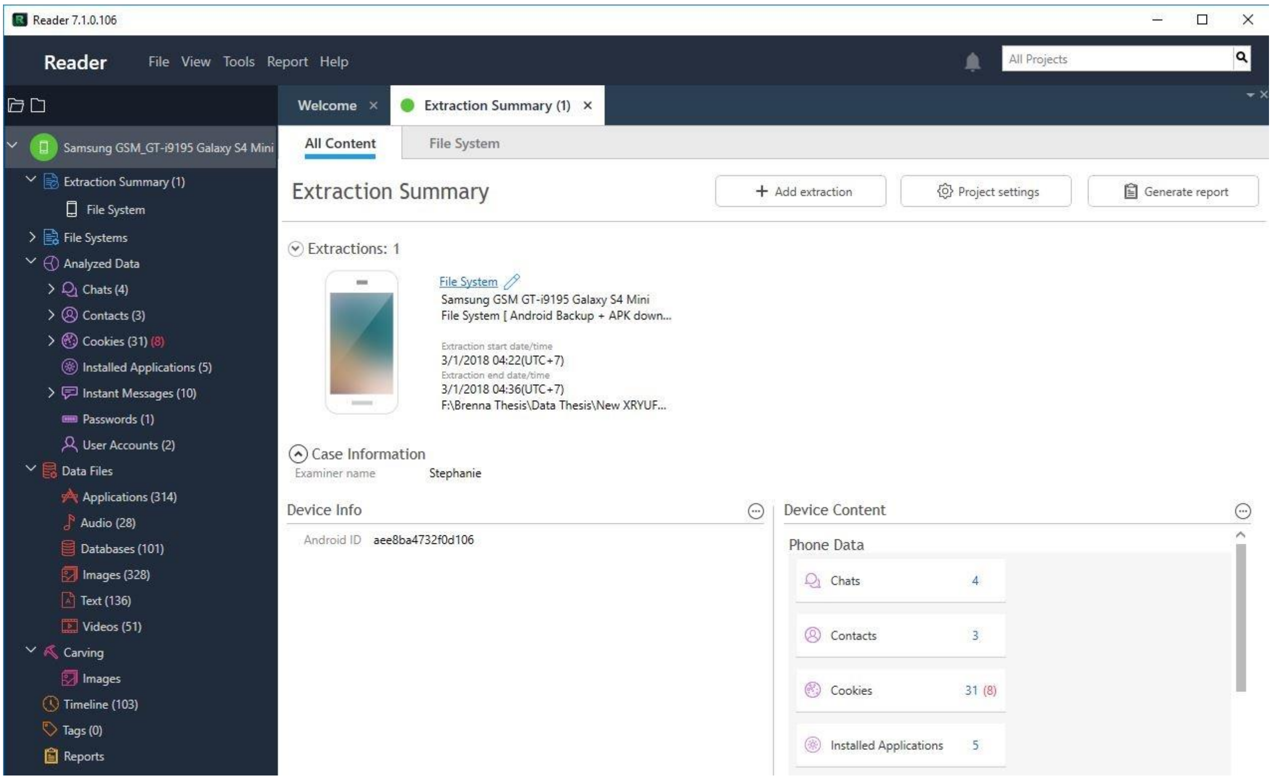
Summary

Date Created 24/02/2018 8:04:40 AM
Locked No
XRY Version 7.6
Lowest Module Version 7.6
File GUID {2F68E998-1824-4EC5-AA91-D81943788953}
XryCore Version 1.0.83.5966
Is File Subset No
Is Encrypted No

View

View Name	Number of Item	Deleted Items
Device / Network Information	63	0
Device / Event Log	395	0
Device / Installed Apps	265	0
Device / Device Accounts	1	0
Security / Accounts	17	1

Figure 4.2: An Example of MSAB XRY Extraction Report



Reader 7.1.0.106

Extraction Summary

Extractions: 1

File System
Samsung GSM GT-i9195 Galaxy S4 Mini
File System [Android Backup + APK down...
Extraction start date/time
3/1/2018 04:22(UTC+7)
Extraction end date/time
3/1/2018 04:36(UTC+7)
F:\Brenna Thesis\Data Thesis\New XRYUF...

Case Information
Examiner name Stephanie

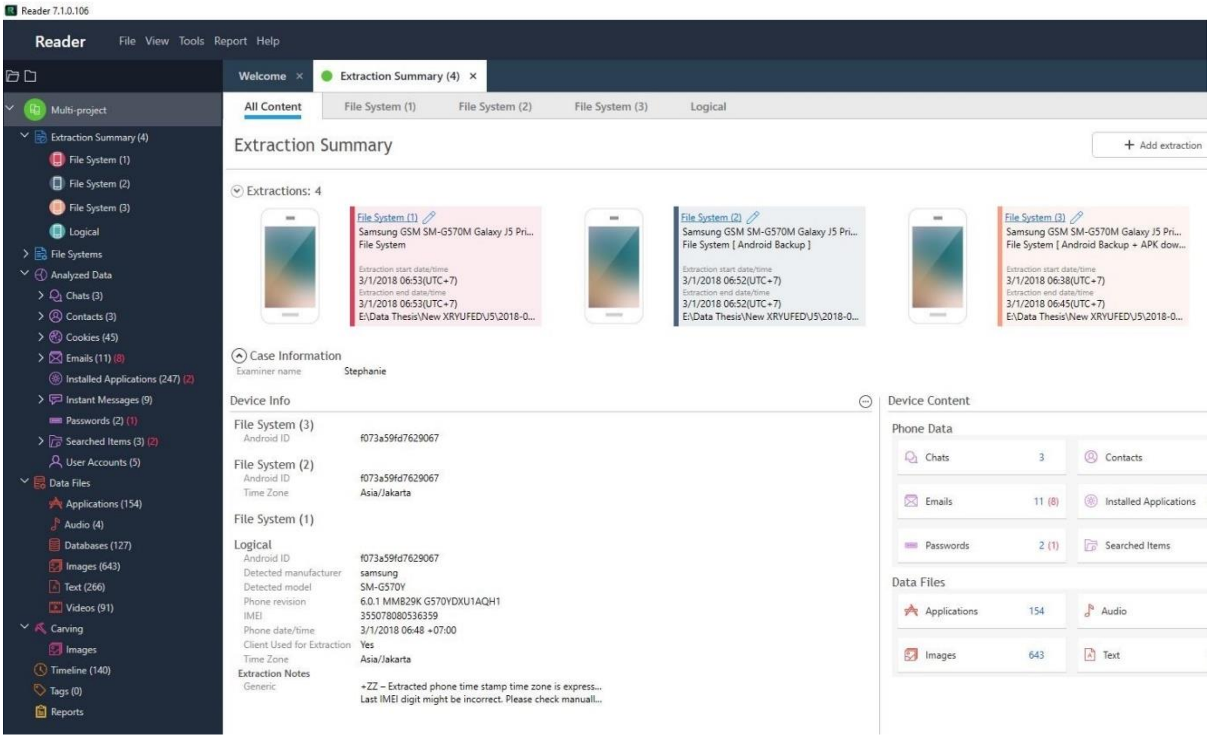
Device Info
Android ID aee8ba4732f0d106

Device Content
Phone Data

Chats	4
Contacts	3
Cookies	31 (8)
Installed Applications	5

Figure 4.3: An Example of Cellebrite UFED Extraction Report

In the matter of extraction reports, Cellebrite UFED has more functions than MSAB XRY such as the multiple report viewer. This function allows the investigator to look and analyse all extractions reports of one smartphone concurrently in one report. Figure 4.4 illustrates the screenshot of Cellebrite UFED multiple extraction reports in one file.



Extraction Summary

Extractions: 4

File System (1)
Samsung GSM SM-G570M Galaxy J5 Pri...
File System
Extraction start date/time
3/1/2018 06:53(UTC+7)
Extraction end date/time
3/1/2018 06:53(UTC+7)
E:\Data Thesis\New XRYUFED\J5\2018-0...

File System (2)
Samsung GSM SM-G570M Galaxy J5 Pri...
File System [Android Backup]
Extraction start date/time
3/1/2018 06:52(UTC+7)
Extraction end date/time
3/1/2018 06:52(UTC+7)
E:\Data Thesis\New XRYUFED\J5\2018-0...

File System (3)
Samsung GSM SM-G570M Galaxy J5 Pri...
File System [Android Backup + APK dow...
Extraction start date/time
3/1/2018 06:38(UTC+7)
Extraction end date/time
3/1/2018 06:45(UTC+7)
E:\Data Thesis\New XRYUFED\J5\2018-0...

Case Information
Examiner name Stephanie

Device Info

File System (3)
Android ID f073a59fd7629067

File System (2)
Android ID f073a59fd7629067
Time Zone Asia/Jakarta

File System (1)

Logical
Android ID f073a59fd7629067
Detected manufacturer samsung
Detected model SM-G570Y
Phone revision 6.0.1 MMB29K G570YDXU1AQH1
IMEI 355078080536359
Phone date/time 3/1/2018 06:48 +07:00
Client Used for Extraction Yes
Time Zone Asia/Jakarta
Extraction Notes
Generic +ZZ – Extracted phone time stamp time zone is express...
Last IMEI digit might be incorrect. Please check manuall...

Device Content

Phone Data
Chats 3
Contacts
Emails 11 (8)
Installed Applications
Passwords 2 (1)
Searched Items

Data Files
Applications 154
Audio
Images 643
Text

Figure 4.4: An Example of Cellebrite UFED Multiple Extraction reports

In the following sub-sections, the social media applications test scenario extraction findings of both forensic tools are discussed and explained.

4.2.2 Social Media Status (Posts) Analysis

Social media status (posts) analysis is important in social media investigation as it can provide critical information that can help to identify connection and relationships between the key actors of a case. Social media status (posts) mostly represents people's current thought and emotional related status (posts). They are not only in text form but also pictures and videos. This feature commonly is used as media to communicate with others or strangers because they are equipped with a comment option in each status (posts). For instance, it can be used by malicious people to approach innocent children in child sex abuse crime cases. This test analysis involved testing whether both forensic tools can extract social media status (posts) on all three social media apps (Facebook, Twitter, and Instagram) on three Android smartphones (Samsung S4 Mini, Samsung J5 Prime, and OPPO A57).

Table 4.3: Social Media Status (posts) test result summary

		MSAB XRY	**Cellebrite UFED**	**Expected**
Facebook	Samsung S4 Mini	0 (0%)	0 (0%)	10
	Samsung J5 Prime	0 (0%)	0 (0%)	10
	OPPO A57	-	0 (0%)	10
Rating		**0** (0%)	**0** (0%)	-
Twitter	Samsung S4 Mini	2 (20%)	10 (100%)	10
	Samsung J5 Prime	0 (0%)	9 (90%)	10
	OPPO A57	-	9 (90%)	10
Rating		**1** (6.67%)	**3** (93.3%)	-
Instagram	Samsung S4 Mini	0 (0%)	0 (0%)	10
	Samsung J5 Prime	0 (0%)	0 (0%)	10
	OPPO A57	-	0 (0%)	10
Rating		**0** (0%)	**0** (0%)	-
Total Rating		**1 (2.22%)**	**2 (31.11%)**	

In table 4.3, it can be seen that social media status (posts) in all three social media applications are difficult to gather by available mobile device forensics tools. MSAB XRY forensic tool that can only examine two smartphones out of three smartphones, namely, Samsung S4 Mini and Samsung J5 Prime, and can only collect two social media status (posts) updates of 10 planted status (posts) that it collected from smartphone S4 Mini via physical extraction. Similarly, Cellebrite UFED also experiences difficulty in collecting social media status (posts) from three social media applications (Facebook, Twitter, and Instagram). Through three extraction types such as logical, physical and file system extraction, only file system extraction can gather social media status (posts) information. Table 4.3 shows social media status (posts) on Facebook and Instagram were unsuccessfully recovered by both tools. Only social media status (posts) on Twitter can be recovered by both tools MSAB XRY and Cellebrite UFED. MSAB XRY was able to collect 2 of 10 social media status (posts) on twitter in the Samsung S4 Mini. In contrast, Cellebrite UFED was successful gathering most of social media status (posts) by collecting 10 of 10 in Samsung S4 Mini, 9 of 10 in Samsung J5 Prime and 9 of 10 in OPPO A57.

In order to have a clearer explanation of each tool social media status (posts) recovered capability, the summary of the test results in a chart is illustrated in figure 4.5. The following figure 4.5 depicts the hit-rate percentage of successfully collected social media status (posts) in three social media apps by two selected smartphone forensic tools.

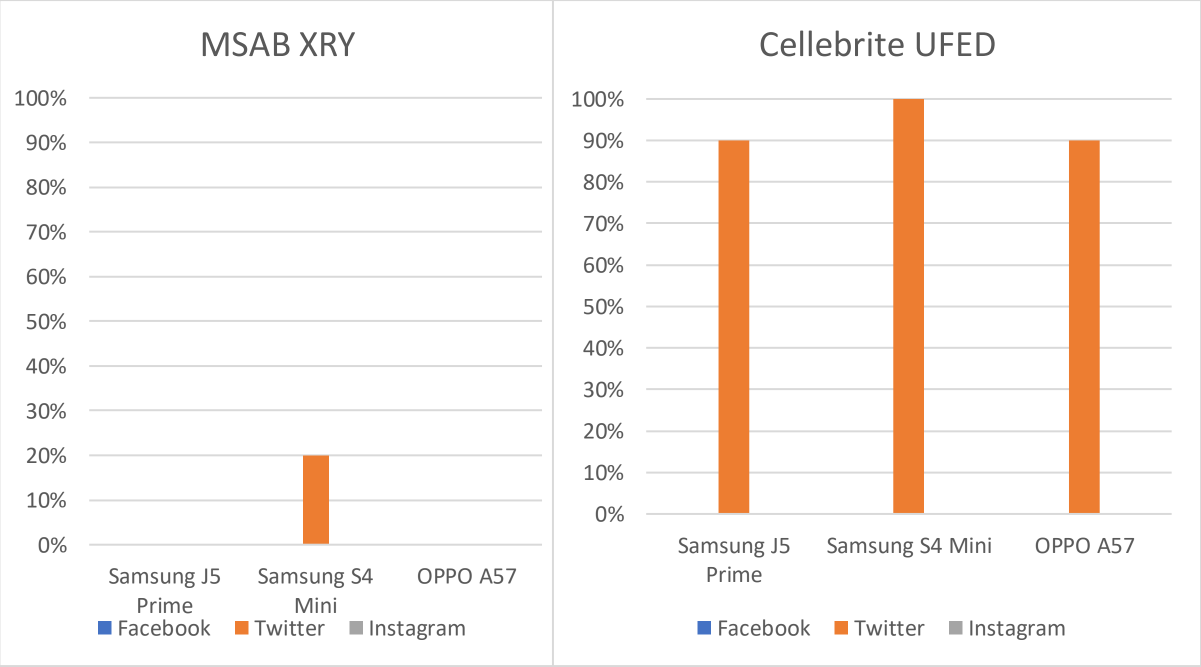


Figure 4.5: Social Media Status (posts) hit-rate by MSAB XRY and Cellebrite UFED

As can be seen from figure 4.5, both tools were unable to recover any status (posts) on Facebook and Instagram with zero per cent of recovered data as a result. On the other hand, Twitter status (posts) updates can be retrieved by both tools, with 20 percent of recovered Twitter status (posts) in Samsung S4 Mini by MSAB XRY. Cellebrite UFED was able to recover status (posts) on Twitter in Samsung J5 Prime, Samsung S4 Mini and OPPO A57 by 90 percent, 100 percent, and 90 percent, respectively.

4.2.3 Chat Messages Analysis

Besides social media status (posts), the chat messages feature also one of the important elements that is crucial in social media investigation. There are two types of chat messages feature nowadays in social media applications. For instance, private chat messages and public chat messages. The private chat messages feature in some social media has the ability to self-destruct within 24 hours. This feature might be one of the recent obstacles in social media crime cases investigation. Table 4.4 illustrates chat messages on three social media apps that can be recovered by MSAB XRY and Cellebrite UFED.

Table 4.4: Chat Messages test result summary

		MSAB XRY	**Cellebrite UFED**	**Expected**
Facebook	Samsung S4 Mini	9 (90%)	10 (100%)	10
	Samsung J5 Prime	10 (100%)	10 (100%)	10
	OPPO A57	-	10 (100%)	10
Rating		**3** (63.3%)	**3** (100%)	-
Twitter	Samsung S4 Mini	10 (100%)	10 (100%)	10
	Samsung J5 Prime	9 (90%)	10 (100%)	10
	OPPO A57	-	9 (90%)	10
Rating		**3** (63.3%)	**3** (96.67%)	-
Instagram	Samsung S4 Mini	10 (100%)	10 (100%)	10
	Samsung J5 Prime	9 (90%)	10 (100%)	10
	OPPO A57	-	10 (100%)	10
Rating		**3** (63.3%)	**3** (100%)	-
Total Rating		**3 (63.3%)**	**3 (98.89%)**	

In table 4.4, it can be seen that chat messages in social media apps on all three smartphones mostly can be retrieved by MSAB XRY and Cellebrite UFED. Cellebrite UFED was able to retrieve almost all chat messages on Facebook, Twitter, and Instagram from all three smartphones (Samsung S4 Mini, Samsung J5 Prime and

OPPO 57) with 10 of 10 recovered chat messages from both Facebook and Instagram, and only miss one chat messages of ten Twitter chat messages from OPPO A57. On the other hand, MSAB XRY was able to recover 9 of 10 chat messages on Facebook, 10 of 10 chat messages on Twitter, and 10 of 10 chat messages on Instagram from Samsung S4 Mini. Moreover, MSAB XRY was also able to recover most of the chat messages on Facebook, Twitter and Instagram. It missed one chat messages on Twitter and one chat messages on Instagram from Samsung J5 Prime. However, due to MSAB UFED cannot examine OPPO A57, it affects the capability percentage of MSAB XRY.

Figure 4.6 shows the proportion hit-rate of the retrieved chat messages on Facebook, Twitter, and Instagram from the Android smartphones by MSAB XRY and Cellebrite UFED. MSAB XRY found 100 percent of chat messages on Facebook, 90 percent of chat messages in Twitter, and 90 percent of chat messages in Instagram from Samsung J5 Prime. In addition, MSAB XRY also found a similar result from Samsung S4 Mini with 90 percent of Facebook chat messages, 100 percent of Twitter chat messages, and 100 percent of Instagram chat messages. Likewise, Cellebrite UFED was able to recover all three social media chat messages from all three smartphones in the range between 90 percent and 100 percent. One hundred percent of Facebook chat message, Twitter chats messages, and Instagram chat messages were fully recovered from both Samsung J5 Prime and Samsung S4 Mini. Furthermore, from OPPO A57 100 percent of Facebook chat messages, 90 percent Twitter chat messages, and 100 percent of Instagram chat messages were recovered by Cellebrite UFED.

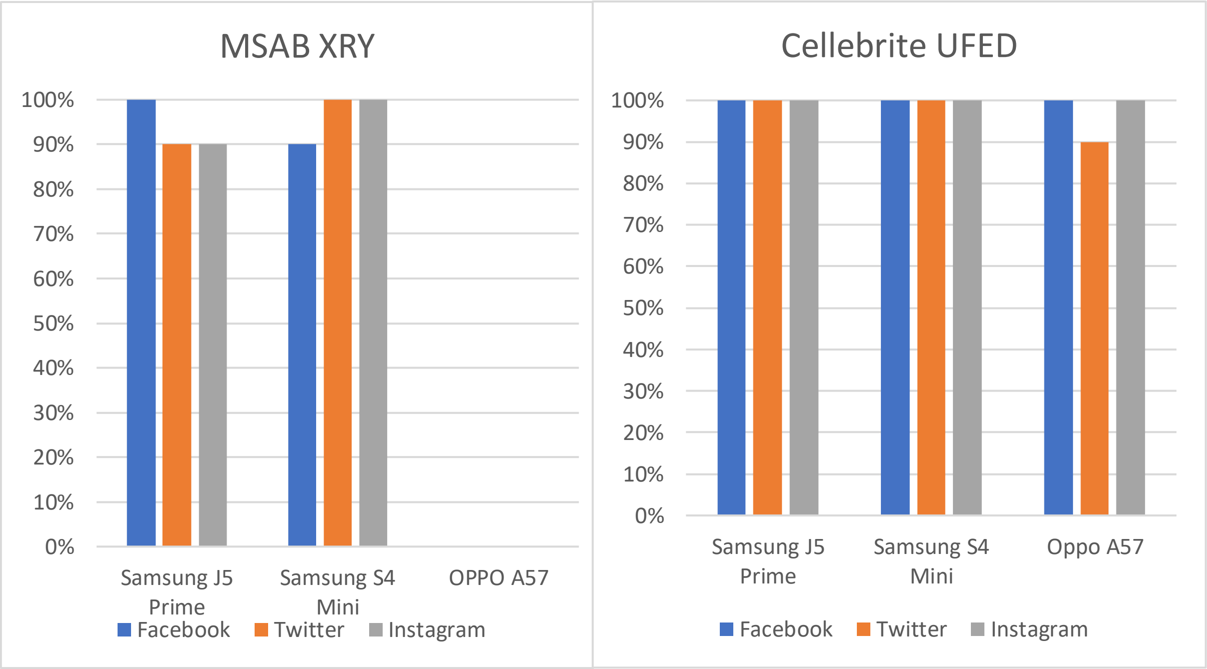


Figure 4.6: Chat Messages hit-rate by MSAB XRY and Cellebrite UFED

4.2.4 Photos Analysis

Photos analysis is vital in a social media investigation. The most uploaded data in social media is photos. A number of case-related information can be found in the pictures that have been uploaded to social media such as modified time, created date and time, and location of where the pictures were taken. According to Pew Research Centre (2018), the most prevalent social media platforms in 2018 is Instagram (Murnane, 2018). This social media platforms as the most popular social media apps is focus on a photo and video-sharing. In recent times, this social media platform launched new content that enables the uploaded file last a short period of time before disappearing. This has become one of the concerns for a social media investigator. For example, a person that wants to share a secret code of some designated crime can easily clear out the potential evidence because of that feature. For that reason, a strong, fast improvement and most capable forensics tools is a must in social media investigation nowadays.

Table 4.5 illustrates social media photos that were recovered by MSAB XRY and Cellebrite UFED. As can be seen from the table, even though MSAB XRY was able to recover almost all of expected social media photos from Samsung S4 Mini with 5 of 5 Facebook photos, 4 of 5 Twitter photos, and 4 of 5 Instagram photos. MSAB XRY was only able to recover less when examining Samsung S4 Mini with the result between 2 and 3 of 5 expected social media photos from Samsung J5 Prime. Similarly, Cellebrite UFED also can recover at least two-fifths of social media photos with a total rating higher than MSAB XRY due to Cellebrite UFED was capable to retrieve photos from OPPO A57.

Table 4.5: Photos extraction test result summary

		MSAB XRY	Cellebrite UFED	Expected
Facebook	Samsung S4 Mini	5 (100%)	4 (80%)	5
	Samsung J5 Prime	2 (40%)	2 (40%)	5
	OPPO A57	-	2 (40%)	5
Rating		**2** (46.67%)	**2** (53.33%)	-
Twitter	Samsung S4 Mini	4 (80%)	5 (100%)	5
	Samsung J5 Prime	2 (40%)	4 (80%)	5
	OPPO A57	-	2 (40%)	5
Rating		**2** (46.67%)	**3** (73.3%)	-
Instagram	Samsung S4 Mini	4 (80%)	5 (100%)	5
	Samsung J5 Prime	3 (60%)	3 (60%)	5
	OPPO A57	-	2 (40%)	5
Rating		**2** (53.3%)	**3** (66.67%)	-
Total Rating		**2 (48.87%)**	**3 (64.44%)**	

Figure 4.7 displays the percentage hit-rate of the retrieved photos on Facebook, Twitter, and Instagram Applications from three Android smartphones by MSAB XRY and Cellebrite UFED. As can be seen in the figure 4.7, MSAB XRY located more photos from Samsung S4 Mini than from Samsung J5 Prime. MSAB XRY collected 60 percent of photos in Instagram and 40 percent of photos on Facebook and Twitter from Samsung J5 Prime. Whereas from Samsung S4 Mini, MSAB XRY can recover approximately more than half of the photos from all three social media applications.

On the other hand, photos on Twitter in Samsung J5 Prime that can be found by Cellebrite UFED was double (80 percent) that of MSAB XRY, which was only 40 percent. In addition, retrieved photos from the Samsung S4 mini that was located by Cellebrite UFED is relatively similar, and it was found by MSAB XRY, between 80 percent and 100 percent. While, photos on all three social media platforms applications (Facebook, Twitter, and Instagram) were successfully recovered from OPPO A57 by Cellebrite UFED. It had a result of 40 percent.

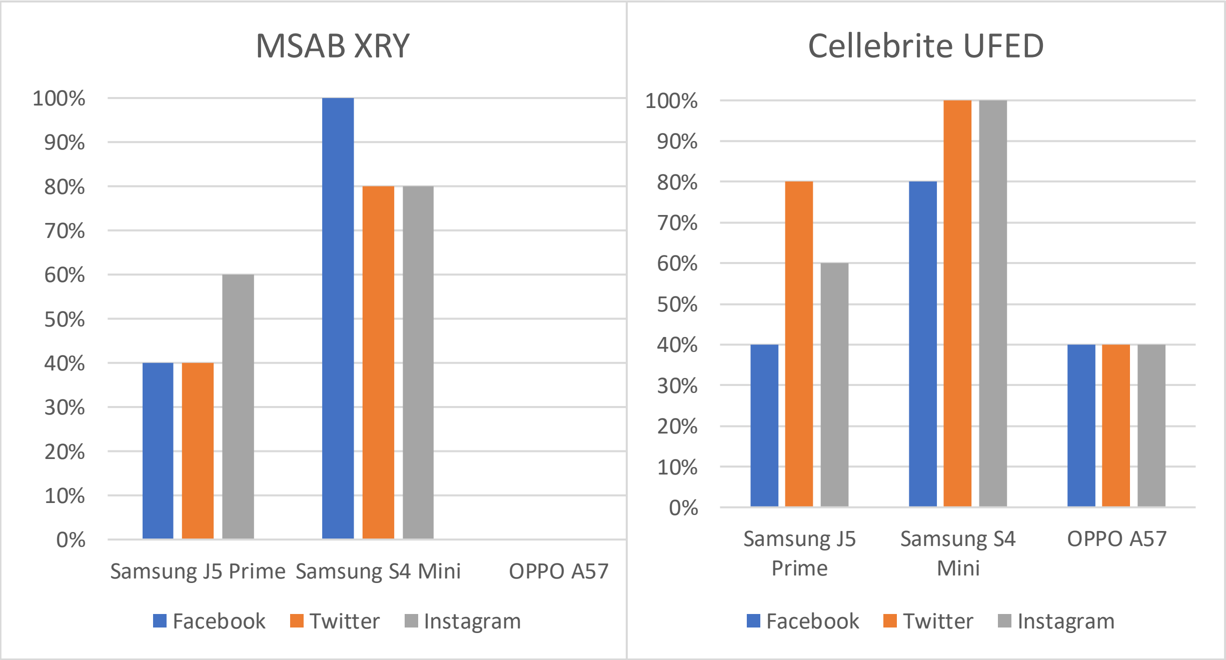


Figure 4.7: Photos hit-rate by MSAB XRY and Cellebrite UFED

4.2.5 Videos Analysis

There has been an explosive growth in video usage in social media in recent years. This is because of the newest features of social media. The new feature allows the videos that have been posted to disappear after 24 hours. This may create a new challenge in social media investigation. For instance, in child abuse cases, a video uploaded of a child abuse victim that can be used as evidence can vanish without trace or a hint of drugs or murder cases also can fade with no trace. This situation requires an investigator to have a broad knowledge which forensic tools that suitable to support in that type of circumstances in social media investigation.

Table 4.6 shows social media videos that were retrieved by MSAB XRY and Cellebrite UFED. MSAB XRY was able to recover 3 of 5 videos on Facebook and Twitter also 4 of 5 videos on Instagram from Samsung S4 Mini. Moreover, this smartphone forensic tool found videos from Samsung J5 Prime with 2 of 5 videos on Facebook, 1 of 5 videos on Twitter, and 3 of 5 videos on Instagram. On the contrary, Cellebrite UFED was able to retrieve more videos on Facebook and Instagram than videos on Twitter. The videos on Twitter can only be found from Samsung S4 Mini and OPPO A57 with 1 video and 2 videos, respectively. None of the videos on Twitter in Samsung J5 Prime were successfully retrieved by Cellebrite UFED. This mobile forensic tool was able to recover 4 of 5 Facebook videos from Samsung S4 Mini, 5 of 5 Facebook videos from Samsung J5 Prime, and 2 of 5 Facebook videos from OPPO A57. Moreover, it was found 5 of 5 videos on Instagram in Samsung S4 Mini and Samsung J5 Prime, while 4 of 5 Instagram videos was found from OPPO A57.

Table 4.6: Videos extraction test result summary

		XRY	**UFED**	**Expected**
Facebook	Samsung S4 Mini	3 (60%)	4 (80%)	5
	Samsung J5 Prime	2 (40%)	5 (100%)	5
	OPPO A57	-	2 (40%)	5
Rating		**2** (33.33%)	**3** (73.33%)	-
Twitter	Samsung S4 Mini	3 (60%)	1 (20%)	5
	Samsung J5 Prime	1 (20%)	0 (0%)	5
	OPPO A57	-	2 (40%)	5
Rating		**1** (26.67%)	**1** (20%)	-
Instagram	Samsung S4 Mini	4 (80%)	5 (100%)	5
	Samsung J5 Prime	3 (60%)	5 (100%)	5
	OPPO A57	-	4 (80%)	5
Rating		**2** (46.67%)	**3** (93.33%)	-
Total Rating		**2 (35.67%)**	**3 (62.23%)**	

Figure 4.8 shows the percentage hit-rate of the retrieved videos on Facebook, Twitter, and Instagram Applications from three Android smartphones by MSAB XRY and Cellebrite UFED. As can be seen in the figure 4.8, MSAB XRY was able to locate all three social media videos from Samsung S4 Mini in the range between 60 percent and 80 percent. Furthermore, MSAB XRY collected 40 percent of videos on Facebook, 20 percent videos on Twitter and 60 percent of videos on Instagram from the Samsung J5 Prime.

On the other hand, although Cellebrite UFED was able to retrieve videos on Facebook and on Instagram in Samsung J5 Prime and Samsung S4 Mini in the range between 60 percent and 80 percent. This tool cannot perform well in term of extracting videos on Twitter in both smartphones. Cellebrite UFED can only recover no more than 20 percent of videos. Additionally, Cellebrite UFED recovered 40 percent of videos on both Facebook and Twitter from OPPO A57. Whereas, 80 percent of videos on Instagram were successfully recovered from OPPO A57 by Cellebrite UFED.

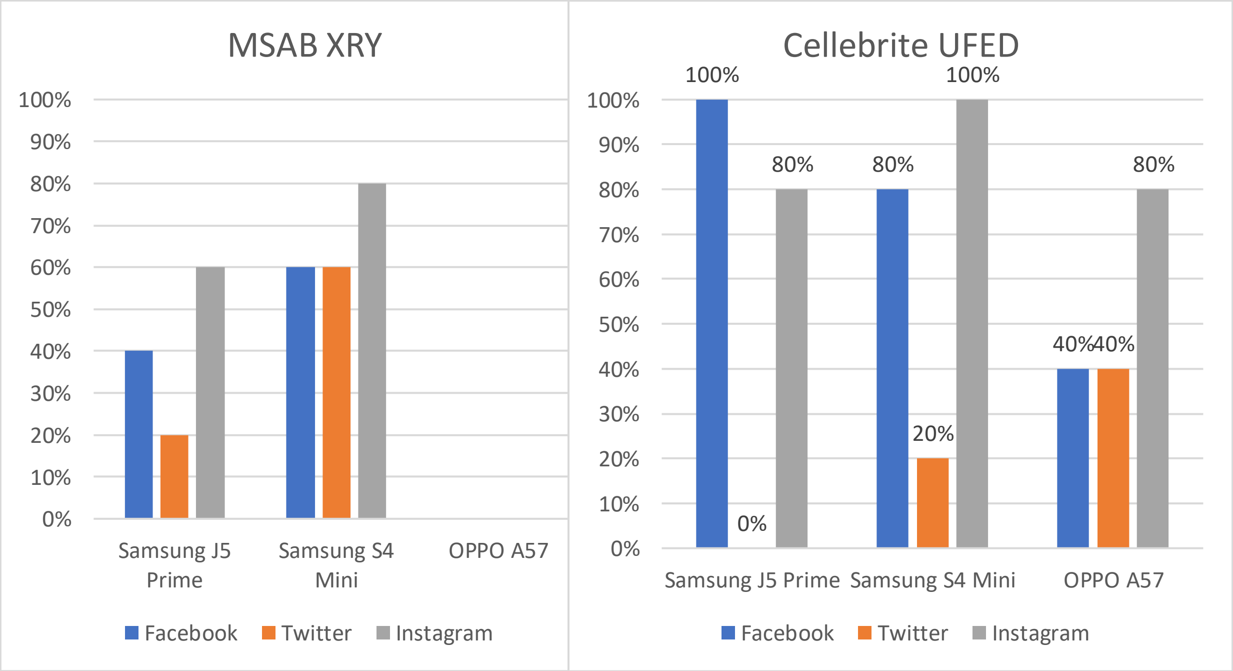


Figure 4.8: Videos hit-rate by MSAB XRY and Cellebrite UFED

4.3 ANALYSIS OF THE TESTING RESULTS

The testing results for each scenario presented in section 4.2 are analysed in this section. After a thorough analysis of data obtained from two particular smartphones forensic tools, the result shows that each smartphone forensic tool has their own ability when analysing social media applications (Facebook, Twitter, and Instagram) in three different smartphones that were released in three different years. Various extraction types that are available in each forensic tool are used to identify the capability of each tool when extracting social media evidence in three social media applications on three different Android phones. As shown in Figure 4.1, MSAB XRY has two extraction types, namely, logical extraction and physical extraction. Whereas, Cellebrite UFED has three extraction types, namely, logical extraction, physical extraction, and file system extraction. Based on the Cellebrite UFED extraction data results most social media evidence (four test scenario) are obtained by utilising file system extraction. The greatest differences between Cellebrite UFED and MSAB XRY is MSAB XRY cannot examine OPPO A57 due to the phone is not yet on the extractable list in this mobile device forensic tool at the time of the research (in Feb 2018 by XRY 7.6).

4.3.1 Smartphones of Results

Table 4.7 shows a detailed social media applications investigation categorised in Android smartphones that were used in this research. As shown in the table, MSAB XRY was able to recover social media evidence in three different social media apps such as Facebook, Twitter, and Instagram from two out of three Android smartphones that were used in this study. Despite OPPO A57 cannot be extracted by MSAB XRY 7.6, this forensic tool can perform moderately well when extracting Samsung S4 Mini with total rating 3 (64 percent). It means this tool can meet the requirement and provide acceptable results. This finding occurred because Samsung S4 Mini is the only smartphones that were used in the research that can make use of all extraction types in MSAB XRY.

Table 4.7: Summary of smartphone results examined by MSAB XRY

Android Smartphones	**Scenario**	**MSAB XRY Results**			**Rating**	**Result**
		Facebook	**Twitter**	**Instagram**		
1. Samsung S4 Mini	1. Social media status (posts)	**0** (0%)	**2** (20%)	**0** (0%)	**1** (6.67%)	**Below**
	2. Chat messages	**9** (90%)	**10** (100%)	**10** (100%)	**3** (96.67%)	**Above**
	3. Photos	**5** (100%)	**4** (80%)	**4** (80%)	**3** (86.67%)	**Above**
	4. Videos	**3** (60%)	**3** (60%)	**4** (80%)	**3** (66.67%)	**Meet**
Total Rating					**3 (64.17%)**	**Above**
2. Samsung J5 Prime	1. Social media status (posts)	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**Miss**
	2. Chat messages	**10** (100%)	**9** (90%)	**9** (90%)	**3** (93.33%)	**Above**
	3. Photos	**2** (40%)	**2** (40%)	**3** (60%)	**2** (46.67%)	**Meet**
	4. Videos	**2** (40%)	**1** (20%)	**3** (60%)	**2** (40%)	**Meet**
Total Rating					**2 (45%)**	**Meet**
3. OPPO A57	1. Social media status (posts)	-	-	-	-	**Miss**
	2. Chat messages	-	-	-	--	**Miss**
	3. Photos	-	-	-	-	**Miss**
	4. Videos	-	-	-	-	**Miss**
Total Rating					**-**	**Miss**

Similar to table 4.7, study results regarding social media application investigation on three Android phones by utilising Cellebrite UFED are shown in table 4.8. It can be seen from the table that all three smartphones were successfully extracted by Cellebrite UFED with the proportion of data result from all smartphones more than 50 percent. The highest rating value is achieved by Samsung S4 Mini, this smartphone was managed to utilise all three extraction types of Cellebrite UFED including physical extraction.

However, the other phones were only able to employ two extraction types such as logical extraction and file system extraction. Although only one phone can be physically extracted by this forensic tool, there is no massive gap between those three phones. This might be because of the extraction method that plays an important role when examining social media applications is not a physical extraction method but file system extraction method. The file system extraction option in Cellebrite UFED has several abilities. One is the extraction method is able to compose the tool to concentrate more on the application that has been installed on the smartphones. For instance, social media applications, messaging applications, and so forth.

Table 4.8: Summary of smartphone results examined by UFED Cellebrite

Android Smartphones	**Scenario**	**Cellebrite UFED Results**			**Rating**	**Result**
		Facebook	**Twitter**	**Instagram**		
1. Samsung S4 Mini	1. Social media status (posts)	**0** (0%)	**10** (100%)	**0** (0%)	**2** (33.33%)	**Meet**
	2. Chat messages	**10** (100%)	**10** (100%)	**10** (100%)	**3** (100%)	**Above**
	3. Photos	**4** (80%)	**5** (100%)	**5** (100%)	**3** (93.33%)	**Above**
	4. Videos	**4** (80%)	**1** (20%)	**5** (100%)	**2** (66.67%)	**Above**
Total Rating					**3 (73.33%)**	**Above**
2. Samsung J5 Prime	1. Social media status (posts)	**0** (0%)	**9** (90%)	**0** (0%)	**1** (30%)	**Below**
	2. Chat messages	**10** (100%)	**10** (100%)	**10** (100%)	**3** (100%)	**Above**
	3. Photos	**2** (40%)	**4** (80%)	**3** (60%)	**2** (60%)	**Meet**
	4. Videos	**5** (100%)	**0** (0%)	**5** (100%)	**2** (66.67%)	**Above**
Total Rating					**2 (64.17%)**	**Above**
3. OPPO A57	1. Social media status (posts)	**0** (0%)	**9** (90%)	**0** (0%)	**1** (30%)	**Below**
	2. Chat messages	**10** (100%)	9 (90%)	**10** (100%)	**3** (96.67%)	**Above**
	3. Photos	**2** (40%)	**2** (40%)	**2** (40%)	**2** (40%)	**Meet**
	4. Videos	2 (40%)	**2** (40%)	**4** (80%)	**2** (53.33%)	**Meet**
Total Rating					**2 (55%)**	**Meet**

4.3.2 MSAB XRY of Results

In order to show more the performance of MSAB XRY in analysing social media, the results are summarised as follows in table 4.9.

Table 4.9: Summary of MSAB XRY capability results

Scenario	**Android Smartphones**	**MSAB XRY Results**			**Rating**	**Result**
		Facebook	**Twitter**	**Instagram**		
1. Social media status (posts)	1. Samsung S4 Mini	**0** (0%)	**2** (20%)	**0** (0%)	**1** (6.67%)	**Below**
	2. Samsung J5 Prime	**0** (0%)	**0** (0%)	**0** (0%)	**0** (0%)	**Miss**
	3. OPPO A57	-	-	-	-	**Miss**
Total Rating					**1 (2.22%)**	**Below**
2. Chat messages	1. Samsung S4 Mini	**9** (90%)	**10** (100%)	**10** (100%)	**3** (96.67%)	**Above**
	2. Samsung J5 Prime	**10** (100%)	**9** (90%)	**9** (90%)	**3** (93.33%)	**Above**
	3. OPPO A57	-	-	-	-	**Miss**
Total Rating					**3 (63.33%)**	**Above**
3. Photos	1. Samsung S4 Mini	**5** (100%)	**4** (80%)	**4** (80%)	**3** (86.67%)	**Above**
	2. Samsung J5 Prime	**2** (40%)	**2** (40%)	**3** (60%)	**2** (46.67%)	**Meet**
	3. OPPO A57	-	-	-	-	**Miss**
Total Rating					**2 (44.45%)**	**Meet**
4. Videos	1. Samsung S4 Mini	**3** (60%)	**3** (60%)	**4** (80%)	**3** (66.67%)	**Meet**
	2. Samsung J5 Prime	**2** (40%)	**1** (20%)	**3** (60%)	**2** (40%)	**Meet**
	3. OPPO A57	-	-	-	-	**Miss**
Total Rating					**2 (35.56%)**	**Meet**
MSAB XRY capability results – Final Rating					**2 (36.39%)**	**MEET**

It can be seen from table 4.9 that MSAB XRY is strong in term of examining chat messages in social media applications on Android smartphones with a total ranking 3 (63 percent) and also relatively good when examining photos and videos in social media application on the three selected phones with total ranking 2 (44 percent) and 2 (36 percent), respectively. However, in term of examining social media status (posts), MSAB XRY performed poorly. Therefore, to dealing with this problem, the forensic tool needs an update or some extra toolkit content that can increase the performce ability of the forensic tool when dealing with social media-enabled crime cases.

4.3.3 Cellebrite UFED of Results

The following table 4.10 illustrates a summary of Cellebrite UFED performance when analysing three social media apps (Facebook, Twitter, and Instagram) in three Android smartphones (Samsung S4 Mini, Samsung J5 Prime, and OPPO A57).

Table 4.10: Summary of Cellebrite UFED capability results

Scenario	**Android Smartphones**	**Cellebrite UFED Results**			**Rating**	**Result**
		Facebook	**Twitter**	**Instagram**		
1. Social media status (posts)	1. Samsung S4 Mini	**0** (0%)	**10** (100%)	**0** (0%)	**2** (33.33%)	**Meet**
	2. Samsung J5 Prime	**0** (0%)	**9** (90%)	**0** (0%)	**1** (30%)	**Below**
	3. OPPO A57	**0** (0%)	**9** (90%)	**0** (0%)	**1** (30%)	**Below**
Total Rating					**2 (31.11%)**	**Meet**
2. Chat messages	1. Samsung S4 Mini	**10** (100%)	**10** (100%)	**10** (100%)	**3** (100%)	**Above**
	2. Samsung J5 Prime	**10** (100%)	**10** (100%)	**10** (100%)	**3** (100%)	**Above**
	3. OPPO A57	**10** (100%)	9 (90%)	**10** (100%)	**3** (96.67%)	**Above**
Total Rating					**3 (98.89%)**	**Above**
3. Photos	1. Samsung S4 Mini	**4** (80%)	**5** (100%)	**5** (100%)	**3** (93.33%)	**Above**
	2. Samsung J5 Prime	**2** (40%)	**4** (80%)	**3** (60%)	**2** (60%)	**Meet**
	3. OPPO A57	**2** (40%)	**2** (40%)	**2** (40%)	**2** (40%)	**Meet**
Total Rating					**3 (64.44%)**	**Above**
4. Videos	1. Samsung S4 Mini	**4** (80%)	**1** (20%)	**5** (100%)	**3** (66.67%)	**Above**
	2. Samsung J5 Prime	**5** (100%)	**0** (0%)	**5** (100%)	**3** (66.67%)	**Above**
	3. OPPO A57	**2** (40%)	**2** (40%)	**4** (80%)	**2** (53.33%)	**Meet**
Total Rating					**3 (62.22%)**	**Above**
Cellebrite UFED capability results – Final Rating					**3 (64.17%)**	**ABOVE**

According to the results presented in table 4.10, Cellebrite UFED is performing well when investigating social media applications in Android smartphones. It can recover almost all of social media chat messages with total ranking 3 (99 percent) and above half of photos and videos in social media can be retrieved with total ranking 3 for both, (64 percent) and (62 percent), respectively. However, this mobile device forensic tool reported cannot retrieve social media status (posts) adequately.

4.4 RESEARCH RESULTS

In this section, the test analysis result of the selected mobile device forensic tools is compared and presented in one chart and one table. The aim is to illustrate clearly the testing results from each of the four testing scenarios and comparing both smartphone forensic tools ability in investigating social media applications based on the testing scenario analysis. A summary of the test scenario findings from section 4.2 and comparison analysis results of both smartphones forensic tools are discussed. More detail of the two smartphone forensic tools performance results are presented in the following sub-section.

4.4.1 Test Scenario Result Summary

In order to distinguish which of two selected mobile device forensic tools functioned better in term of social media investigation, all the findings are summarised in table 4.11.

Table 4.11: Summary of the test scenario findings

Scenario	**MSAB XRY**		**Cellebrite UFED**	
	Score	**Rating**	**Score**	**Rating**
Social media status (posts)	**2.22%**	**1 (Below)**	**31.11%**	**2 (Meet)**
Chat messages	**63.33%**	**3 (Above)**	**98.89%**	**3 (Above)**
Photos	**44.45%**	**2 (Meet)**	**64.44%**	**3 (Above)**
Videos	**35.56%**	**2 (Meet)**	**62.22%**	**3 (Above)**
Total - Weighted	**36.39%**	**2**	**64.17%**	**3**
Ranking	**2nd**		**1st**	

It can be seen that from the table 4.11 above that Cellebrite UFED achieved higher performance test result in the cases than MSAB XRY. The MSAB XRY achieved varied rates with one Rating 1 (Below classification, two rating 2 (Meet classification), and one rating 3 (Above classification for retrieved social media chat messages). On the other hand, Cellebrite UFED attained only one rating 2 (Meet classification for retrieved social media status (posts) and the rest were rated as rating 3 (Above classification). As has been noted, overall score performance of MSAB XRY is 36 percent and Cellebrite UFED is 64 percent. It can be said that in the social media investigation, Cellebrite UFED performed better than MSAB XRY.

4.4.2 Comparison of Smartphone Forensics Tools

Four test scenarios were designated to compare the two mobile device forensics tools capabilities for the purpose of investigating social media applications evaluated in this research. The ratings for all tools have been plotted on a Radar-chart (figure 4.9). The radar-chart is utilised to show the relationship and illustrate more clearly the comparison results of two chosen mobile devices forensic tools' capabilities, namely, MSAB XRY and Cellebrite UFED in social media-enabled crimes investigation.

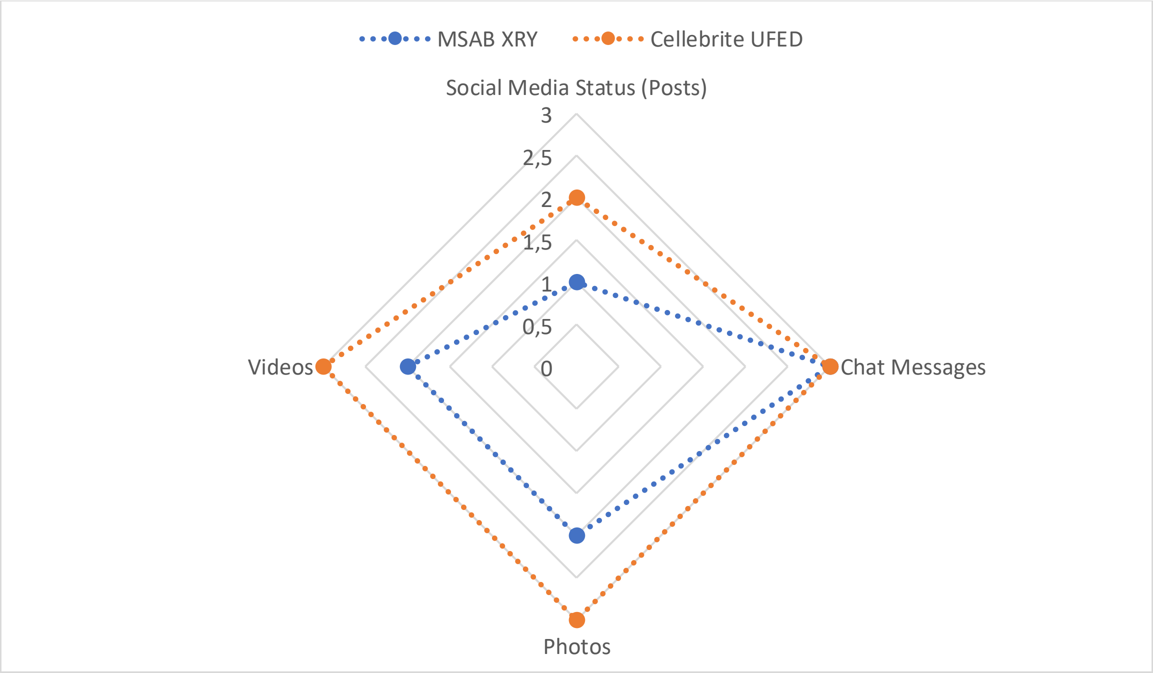


Figure 4.9: Comparison of Social Media Extraction Capability of Smartphone Forensic Tools

In figure 4.9, the ratings range from 0 (Miss) to 3 (Above) is shown to provide a clearer interpretation of the test result. Several trends have been identified based on the comparison results. For example, Cellebrite UFED consistently achieved high ratings when examining chat messages, photos, and videos of social media apps (Facebook, Twitter, and Instagram) in selected Android smartphones (Samsung S4 Mini, Samsung J5 Prime, and OPPO A57) with 3 ratings. As can be seen from figure 4.9, in spite of Cellebrite UFED and MSAB XRY attained same high ratings in chat messages analysis (3 ratings), Cellebrite UFED overbear MSAB XRY in three other test scenarios such as social media status (posts), photos, and videos.

4.5 CONCLUSION

Chapter four stated the results and analysis of the research findings and also visually presents discovered relationships in the findings based on the test scenarios. The main focus of chapter 4 is on reporting the test results and presenting the tool assessment results in a visual format with the purpose to provide clearer visualisation of each smartphone forensic tool's capability and limitations in a social media investigation. Chapter 4 also presents the comparison data results between MSAB XRY and Cellebrite UFED that can allow the investigator to identify and then utilise the forensics tool effectively. Hence, by understanding each of tool's ability, it can reduce the investigation time and improve the extraction of evidence.

The test rating method was specified in section 4.1 in order to clarify and explain each part of the extraction results. Field-testing was conducted with a total of 4 test scenarios for evaluating the top two mobile device forensic tool capabilities. Each test scenario is presented with a table and a chart that summaries the testing analysis results that is shown in section 4.2. In section 4.3, the analysis of testing results are depicted into three sections, a summary of the capability of each tool when examining three different Android smartphones is presented in section 4.3.1 and summaries of each individual tool extraction results can be found in section 4.3.2 for MSAB XRY and 4.3.3 for Cellebrite UFED. A detailed comparison of results between MSAB XRY and Cellebrite XRY is shown in chapter 4.4.

In social media-related crime investigation process, understanding the capability of each forensic tool can help the investigator to work more effective when examining social media applications. As has been noted in the prior section, the mobile device forensic tools that are evaluated in this research namely, MSAB XRY 7. 4 and Cellebrite UFED 7.1, performed variably the test scenarios. The recent version of each tool can be expected to improve and therefore can examine a greater variety of smartphones. The next chapter, Chapter five, will comprehensively answer the research questions and hypotheses based on the findings presented in chapter four. Chapter five also will provide a detailed discussion and analysis of the findings presented in chapter four.

Chapter Five

DISCUSSION AND CONCLUSION

5.0 INTRODUCTION

The findings and results for each test scenario and comparison results between the two chosen mobile device forensics tools' capabilities are reported and presented in both a descriptive and a visual manner in chapter four. In chapter five, the findings reported in chapter four will be used to answer the research question, the sub-questions and test the hypotheses from chapter three. The discussion of the findings and the recommendation for future research will also be presented in this chapter five.

Chapter five consists of five major sections. Section 5.1 answers the research sub-questions and tests the research hypotheses outlined in chapter 3 (section 3.1) by utilised the findings reported in chapter 4. Furthermore, the main research question is answered in section 5.2. Then, the discussion of the result findings is discussed in section 5.3. Lastly, the recommendation for future research will be delivered in the final section 5.4.

5.1 SUB-QUESTIONS AND HYPOTHESES TEST

A total of associated three sub research questions were developed in order to answering the main research question of this thesis. In this section, the sub research questions and hypotheses that was outlined in chapter 3 are answered with the data from the findings from chapter 4.

The first sub question stated in chapter three is:

Sub-Question 1: *What extraction type of mobile device forensics tools is pre-eminent for collecting evidence from Social Media on Android phones?*

To answer this research question, the associated hypothesis 1 was tested according to the findings in chapter four. It is shown in table 5.1.

Table 5.1: The Result of Hypothesis Testing for Hypothesis 1

Hypothesis 1	
File system extraction of Cellibrite UFED is the best extraction type when gathering evidence from social media applications on Android smartphones.	
Argument For:	**Argument Against:**
File system extraction is useful for understanding the application usage such as social media applications on smartphones. Moreover, it also has an option to choose particular social media applications that are required to be examined (Subsection 4.3.1).	The other extraction types, such as physical extraction, also have capability to recover social media evidence. To be able to mine all the data it can get, including data from the unallocated/deleted space of the smartphones, is an advantage (Section 2.3).
Justification:	
The hypothesis 1 is true because from the result findings; it is acknowledged that both of mobile forensics tools are capable to extract social media potential evidence on smartphones, especially Cellebrite UFED. It is reported in the test findings in chapter 4 that most of the planted social media evidence were collected by utilising the file system extraction of Cellebrite UFED on all three chosen Android smartphones (Subsection 4.3.3, Table 4.10). However, physical extraction also must be considered due the only smartphones (Samsung S4 mini) that can be physically extracted by both forensics tools, obtained the highest rate and percentage among other Android smartphones (Subsection 4.3.1, Table 4.8).	

According to the result of testing analysis shown in section 4.3, this sub research question 1 can be answered in the following manner:

"*The most pre-eminent extraction type of mobile device forensics tools for collecting social media evidence from selected smartphones is file system extraction. For instance, in this research, as can be seen in table 4.8, most of the designed social* *media evidence from all three smartphones were collected by file system extraction of Cellebrite UFED with the completeness percentage are all above 50 percent."*

The second sub question as posted in chapter three is:

> **Sub-Question 2:** *Are the chosen mobile device forensics tools capable to examine all three selected Android smartphones?*

To answer this research question, the associated hypothesis 2 was tested according to the findings in chapter four. It is shown in table 5.2.

Table 5.2: The Result of Hypothesis Testing for Hypothesis 2

<table>
<tr><th colspan="2">Hypothesis 2</th></tr>
<tr><td colspan="2"><i>The selected mobile forensics tools able to examine all three chosen Android smartphones.</i></td></tr>
<tr><td><b>Argument For:</b></td><td><b>Argument Against:</b></td></tr>
<tr><td>The developers claim that both mobile forensic devices: MSAB XRY 7.6 and Cellebrite UFED 7.1, have increased support for the latest mobile devices, including iOS, drones, and Android devices (Section 2.3).</td><td>Both tools are capable to analyse most of android smartphones. It is found that Cellebrite UFED is able to examine all three smartphones. On the other hand, MSAB XRY 7. 6 is not fully capable to analyse all the Android smartphones (Section 4.3).</td></tr>
<tr><td colspan="2"><b>Justification:</b></td></tr>
<tr><td colspan="2">The hypothesis 2 is false because from the findings it is acknowledged that only Cellebrite UFED is able to examine all three selected Android Smartphones (Section 4.3, Table 4.8). It is shown in section 4.3 that MSAB XRY is unable to examine OPPO A57 (Table 4.8) due to the Android smartphone is not yet on the extractable list in this mobile device forensics tool.</td></tr>
</table>

According to the result of testing analysis shown in section 4.3, this sub research question 2 can be answered in the following manner:

"*The chosen mobile device forensics tools are not capable to examine all three selected Android smartphones. Due to one of the forensics tools, namely, MSAB XRY 7.6 is not able to examine the OPPO A57 Android smartphone."*

The third sub question as posted in chapter three is

Sub-Question 3: *Which tool is better for Social Media investigation?*

To answer this research question, the associated hypothesis 3 was tested according to the findings in chapter four. It is shown in table 5.3

Table 5.3: The Result of Hypothesis Testing for Hypothesis 3

Hypothesis 3	
Cellebrite UFED will perform better than MSAB XRY.	
Argument For:	**Argument Against:**
Cellebrite UFED has more extraction type options such as logical extraction, file system extraction, and physical extraction (Section 4.2, Table 4.1). It allows the forensic tool to gather more social media evidence.	MSAB XRY is capable of gathering most of social media evidence from a wide variety of mobile devices such as feature phones, smartphones, GPS navigation units, 4G modems, augmented devices, portable music players, and tablets (Subsection 2.3.1).
Justification:	
The hypothesis 3 is true because from the findings in chapter 4; it is known that Cellebrite UFED has achieved a higher percentage of social media evidence such as social media status (posts), photos and videos. Only when collecting chat messages, Cellebrite UFED attained the same high ratings with MSAB XRY (Section 4.4, Figure 4.9).	

According to the result of testing analysis shown in section 4.3, this sub research question 3 can be answered in the following manner:

"*Cellebrite UFED is a better mobile device forensics tool for social media investigation. Because the forensics tool is able to reach a higher percentage than MSAB XRY in overall tests of the research (Section 4.4, Table 4.11) and Cellebrite UFED also has function that facilitates the investigator to look and analyses all extraction reports of one smartphone concurrently in one report (Section 4.2, Table 4.4)*".

5.2 THE RESEARCH QUESTION

This section addresses the main research question that was developed in section 3.1. The main research question defined in chapter 3, section 3.1 is:

“What are the capabilities of the chosen mobile devices forensics tools (i.e., Cellebrite UFED and MSAB XRY) when examining Social Media applications on Android smartphones in a social media-related crimes investigation?”

The aim of this thesis is to evaluate and compare the chosen existing mobile device forensic tools capabilities when investigating three social media apps (Facebook, Twitter, and Instagram) in three Android smartphones (Samsung J5 Prime, Samsung S4 Mini, and OPPO A 57). In order to answer the main research question, three sub questions and three associated hypotheses have been derived. Four testing scenarios are designed for testing the capability of the mobile forensics tools in collecting social media evidence on Android smartphones. The research findings presented in chapter four and answers of the sub-questions in section 5.1 are utilised to answer the main research question.

As can be seen in section 4.2, 4.3 and 4.4, the chosen mobile device forensics tools are able to collect social media evidence such as social media status (posts), chat messages, photos and videos. Each of mobile device forensic tools has different capability when examining social media applications on Android smartphones. MSAB XRY is able to examine only two out of three Android smartphones (Table 4.2). According to Table 4.7, this forensics tool is capable to perform moderately well when extracting Samsung S4 Mini artefacts with the total successful recovered evidence approximately 64 percent and it is also able to extract social media evidence in the Samsung J5 Prime with around 45 percent of the total social media evidence collected. Table 4.9 presented the total percentage (rating) of MSAB XRY when collecting each of social media evidence. MSAB XRY is strong in terms of collecting chat messages with a total percentage of successfully collected chat messages of 63 percent. When collecting photos and videos, MSAB XRY attains 44 percent and 36 percent of the successfully collected photos and videos evidence, respectively. However, in term of collecting social media status (posts), MSAB XRY can only retrieved 2 percent of planted social media status (posts) from only two smartphones. Lastly, as shown in table 4.11, due to this limitation the mobile device forensics tool is unable to examine OPPO A57. It has an overall performance score of MSAB XRY is 37 percent when collecting social media evidence on Android smartphones.

On the other hand, based on table 4.2, it can be seen that Cellebrite UFED is able to examine all three selected Android smartphones. According to Table 4.8, this forensics tool is capable for extracting all three selected smartphones with the proportion of successfully collected social media evidence at approximately 50 percent. Cellebrite UFED performs well when examining the Samsung S4 Mini with the percentage of successfully retrieved social media evidence is 73 percent. This tool also performs strongly when examining Samsung J5 Prime and OPPO A57 with the percentage of successfully recovered social media evidence is 64 percent and 55 percent, respectively. Table 4.10 presented the summary of the Cellebrite UFED capability result including the total percentage of each social media evidence that is successfully collected. From the table 4.10, it is shown that this forensics tool is almost collecting all planted chat messages evidence with the total percentage of successfully recovered chat messages is 99 percent. Moreover, Cellebrite UFED was able to gather successfully evidence when collecting photos and videos, with the total percentage of both social media evidence is 64 percent and 62 percent, respectively. Nevertheless, Cellebrite UFED performs less well when collecting social media status (posts) evidence in all smartphones with only 31 percent of successfully collected social media status (posts). Lastly, as shown in table 4.11, Cellebrite UFED attained a higher total percentage of successfully collected evidence than MSAB XRY in all test cases in this research, with the overall performance score of Cellebrite UFED is 64 percent when collecting social media evidence on Android smartphones.

5.3 DISCUSSION OF FINDINGS

In the prior sections 5.1 and 5.2, the research questions and the associated hypotheses were answered and tested. Based on the findings presented in chapter four, the limitation of this research will be identified in this section 5.3. It is identified from table 4.2 that the current mobile device forensics tools (MSAB XRY 7.6 and Cellebrite UFED 7.1) that are used in this thesis have limitations when extracting from recent smartphones. Both forensics tools are unable to fully perform all the available extraction types that they are presented. For Samsung J5 prime and OPPO A57 that were released in 2016 and 2017, respectively, MSAB XRY can only logically extract Samsung J5 Prime and still cannot examine OPPO A57 due to the fact the phone is not yet on the extractable list in this mobile device forensic tool, at the time of testing. Similarly, Cellebrite UFED also cannot fully make use of the extraction types. Cellebrite UFED can use all the extraction types when examine Samsung S4 Mini that was released in 2013-2014. For other Android smartphones that are released in recent years such as Samsung J5 Prime and OPPO A57, Cellebrite UFED can only utilise two out of three extraction types that this tool has, namely, Logical extraction and File System extraction.

With the emergence of new features of social media platforms such as the feature that has the ability to self-destruct within 24 hours in the form of photos and videos, employing the most capable mobile device forensics tool is a necessity. As shown in table 4.11, both mobile device forensics tools cannot fully retrieve the social media evidence in the form of photos and videos. MSAB XRY is able to collect 44 percent of planted photos and 36 percent of planted videos. On the other hand, Cellebrite UFED is able to retrieve 64 percent of planted videos and 62 percent, respectively. The average percentage of successfully collected photos evidence and videos evidence is 54 percent and 63 percent, respectively. With the less than 65 percent of photos and videos that can be collected by the current forensics tools, it is likely that it will difficult handling the new social media features with the current MSAB XRY version 7.6 and Cellebrite UFED version 7.1. To examine the recent social media features better and improved mobile device forensics tools are needed for use to undertake gathering those social media data or the latest version of both chosen mobile forensics tools are required to be updated.

The most challenging social media evidence to collect in this thesis is social media status (posts). It is reported in chapter four Table 4.3 that both of mobile device forensics tools are struggling to retrieve the social media evidence with the total percentage of successfully collected social media status (posts) is 2 percent by MSAB XRY and 31 percent by Cellebrite UFED. It is a need to discover the best forensics tool and technique to adequately recover social media status (posts) due to most of the social media users frequently using this media feature and the cybercriminals may also employ this feature in committing crimes. By utilising the most suitable mobile forensics tool when collecting social media status (posts) evidence, it is expected a significant increase in the solved social media-related crime cases.

5.4 RECOMMENDATION FOR FURTHER RESEARCH

Even though the research conducted in this thesis has accomplished addressing its purpose and the research questions outlined in section 3.1, there are many uncovered areas that require additional study and research in the future. The further studies recommended include comparing mobile device forensics tools' capability when extracting social media evidence on others operating system smartphones, such as iOS and Windows smartphones. This includes assessing the available mobile device forensics tools' ability with the aim to retrieve the other social media features and other social media platforms that have not been discussed in this thesis, Also evaluating other available mobile forensics tools' ability in social media-related crime cases investigation such as oxygen Forensics should be done.

Further study could be undertaken in comparison of mobile device forensics tools' capabilities when extracting social media evidence on various smartphones. In this thesis, the research shows that the chosen mobile device forensics tools are able to recover social media evidence from Android smartphones. However, the smartphones that are evidence in crime cases are not only Android phones, there are many other brands, series and operating system types that also can be found in crime scenes and as an evidence of criminal cases. Greater understanding about the mobile forensics tools' capability to examine several types of smartphones is expected to make the social media investigation process more useful.

In order to comprehend more fully social media and improve the quality of social media investigations, assessing the available mobile device forensics tools' ability with the purpose to collect the other social media features and other social media platforms that have not been discussed in this thesis, is necessary. This thesis shows that the selected mobile device forensics tools are capable to retrieve potential social media evidence such as social media status (posts), chat messages, photos, and videos in three different social media platforms namely, Facebook, Twitter, and Instagram. Nevertheless, social media nowadays has more numerous features that are likely be also utilised more by social media users and other social media platforms also used by individuals. With the aim to improve the investigation process, understanding the mobile forensics tools' capability in investigating recent social media features and other available social media platforms is essential.

Further study in evaluating other available mobile forensics tools' ability in social media-related crime cases investigation such as oxygen Forensics could also be done. In this thesis, the research findings show that the both chosen mobile forensics tools namely, MSAB XRY and Cellebrite UFED are suitable for social media investigation. However, both forensics tools are reported as not fully able to collect social media evidence from smartphones. By evaluating other available mobile forensics tools' ability such as oxygen Forensics, may possibly help in finding a digital forensics tool that is better in recovering social media evidence on smartphones.

REFERENCES

Aldhafferi, N., Watson, C., & Sajeev, A. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. *arXiv preprint arXiv:1305.2770*.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics. *National Institute of Standards and Technology (NIST) Special Publication*, 800-101. https://dx.doi.org/10.6028/NIST.SP. 800-101r1

Balusamy, B., Varma, V. T. S., & Grandhi, S. S. M. Y. (2017). Social Network Web Mining: Web Mining Techniques for Online Social Network Analysis. In *Web Data Mining and the Development of Knowledge-Based Decision Support Systems* (pp. 284-310). IGI Global. https://dx.doi.org/10.4018/978-1-5225-1877-8.ch015

Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. In *IFIP International Conference on Digital Forensics* (pp. 17-36). Springer, Berlin, Heidelberg.

Bhusari, M. V. K., & Sahu, M. A. M. (2013). Smartphone attacks and security challenges. *International Journal of Computer Science and Management Research, 2*(5), 2473-2476.

Brown, N. (2015). Smartphones and Social Media – Where Will it Take Us. Retrieved from https://socialmediaweek.org/blog/2015/05/smartphones-and-social-media-where-will-it-take-us/.

Brunty, J., & Helenek, K. (2014). *Social media investigation for law enforcement*. New York, NY: Routledge.

Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime—A new breed of criminal? *Computer Law & Security Review, 19*(3), 222-227.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Waltham, MA: Academic press.

Cellebrite. (2017). UFED Ultimate. Retrieved from https://www.cellebrite.com/en/products/ufed-ultimate/.

Chaffey, D. (2018). The most popular social networks worldwide 2018. Retrieved from https://www.smartinsights.com/digital-marketing-strategy/popular-social-networks-worldwide-chartoftheday/.

Chintalapati, P. (2015). Mobile Forensics-Data Acquisition Methods. Retrieved from http://securitycommunity.tcs.com/infosecsoapbox/articles/2015/11/04/mobile-forensics-data-acquisition-methods/.

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation, 9*, S90-S98.

Fuchs, C. (2017). *Social media: A critical introduction*. London, UK: Sage Pub..

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64-S73.

Ge, J., Peng, J., & Chen, Z. (2014). Your privacy information are leaking when you surfing on the social networks: A survey of the degree of online self-disclosure (DOSD). *IEEE* Symposium conducted at the IEEE 13th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC), 2014.

Hassan, M., & Pantaleon, L. (2017). An investigation into the impact of rooting android device on user data integrity. In *Emerging Security Technologies (EST),* 2017 Seventh International Conference on (pp. 32-37). IEEE.

Hayes, R. M., & Luther, K. (2018). # FutureCrime: What Is Crime in the Age of New Media?. In # *Crime* (pp. 153-191). Palgrave Macmillan, Cham.

Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., & Weippl, E. (2011). Social snapshots: Digital forensics for online social networks. In *Proceedings of the 27th annual computer security applications conference* (pp. 113-122). New York, NY: ACM.

Kemp, S. (2018). Digital in 2018: World's internet users pass the 4 billion mark. Retrieved from https://wearesocial.com/blog/2018/01/global-digital-report-2018.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication, 10,* 800-886. Gaithersburg, MD.

Lambert, J. (2017). How social media is changing the way people commit crimes and how police fight it. Retrieved from http://foxbaltimore.com/news/cover-story/how-social-media-is-changing-how-people-commit-crimes.

McKemmish, R. (1999). *What is forensic computing?* : Australian Institute of Criminology Canberra.

Murnane, K. (2018). Which Social Media Platform Is The Most Popular In The US?. Retrieved from http://forbes.com/sites/kevinmurnane/2018/03/03/which-social-media-platform-is-the-most-popular-in-the-us

MSAB. (2017). XRY - the first choice for digital evidence extraction. Retrieved from https://www.msab.com/download/product_sheets/en/XRY_The_First_Choice_Digital.pdf.

Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations*. Boston, MA: Cengage Learning.

Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior*, 35, 548-553.

Pierce, D. (2018). Your Smartphone Is the Best Computer You Own. Retrieved from https://www.wsj.com/articles/your-phone-is-the-best-computer-you-ownso-use-it-more-1527084001.

Pollitt, M. M. (2013). Triage: A practical solution or admission of failure. *Digital Investigation*, 10(2), 87-88. https://doi.org/10.1016/j.diin.2013.01.002

Poonia, A. S. (2014). Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN*, 2278-6856.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1-12.

Sathe, S. C., & Dongre, N. M. (2018). Data acquisition techniques in mobile forensics. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 280-286). IEEE.

Shinder, D. L., & Cross, M. (2008). *Scene of the Cybercrime (Second Edition)*. Burlington, MA: Syngress Pub.

Soltani, S., & Seno, S. A. H. (2017). A survey on digital evidence collection and analysis. In *Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on (pp. 247-253)*. IEEE.

Valentine, O. (2018). Top 10 Reasons for Using Social Media. Retrieved from https://blog.globalwebindex.com/chart-of-the-day/social-media/.

Vimal, K., & Trivedi, A. (2015). A memory management scheme for enhancing performance of applications on Android*IEEE.* Symposium conducted at 2015 IEEE Recent Advances in the meeting of the Intelligent Computational Systems (RAICS).

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. D*igital Investigation*, *14*, S77-S84.

Zheleva, E., Terzi, E., & Getoor, L. (2012). Privacy in social networks. *Synthesis Lectures on Data Mining and Knowledge Discovery, 3*(1), 1-85.