Cracking the Code: Digital Forensic Analysis of Social Media Applications on Virtual Android Devices

MSc Research Project
MSc in Cybersecurity

Bhavesh Dalvi
Student ID: x23206080

School of Computing
National College of Ireland

Supervisor: Dr. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Bhavesh Rajesh Dalvi

Student ID: x23206080

Programme: MSc in Cybersecurity **Year:** 2024-25

Module: MSc Research Project

Supervisor: Dr. Imran Khan

Submission Due Date: 29.01.2025

Project Title: Cracking the code: Digital Forensic Analysis of social media applications on virtual android devices

Word Count: 10541 **Page Count:** 27

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: BR Dalvi

Date: 28.01.2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Cracking the Code: Digital Forensic Analysis of Social Media Applications on Virtual Android Devices

Bhavesh Dalvi
x23206080

Abstract

The last few decades have seen a tremendous rise in the use of smartphones and social media applications, thanks to the rapid growth and inventions around technology and internet. Social media platforms like Instagram, X, WhatsApp have become an integral part of one's life in the 21st century as they have drastically changed the dynamics of networking and socialising. These social media applications have a positive as well as a negative side to it. The positive side being that these applications are extensively used by the public for networking, information and entertainment purposes, while the negative flip side of it being that these applications are emerging as a potential source for performing crimes like cyberbullying, cyberstalking, fraudulent transactions, spreading hate messages, impersonation, cyberterrorism etc. This research intends to utilize digital forensic techniques to perform forensic analysis of social media data on android platforms to identify potential sources of digital artifacts that could aid in investigating crimes. The research utilizes the Android studio software to configure virtual android devices on which the social media applications would be installed and then data would be extracted and analysed using forensic tools and techniques in accordance with the NIST framework to ensure its applicability and admissibility in real world situations. The research uses forensic techniques to analyse and recover digital artifacts like text messages, multimedia, call logs etc. The study highlights the use of digital forensics in analysing social media data for solving modern day crimes.

1 Introduction

The tremendous expansion of internet and technology has led to an exponential growth in the usage of social media platforms. These platforms have grown quite popular among the masses due to its appealing nature and attractive new trends and features. The social media market has broadened largely by developing applications that fulfil almost all kinds of user needs and provides them satisfaction. Today, there are multiple social media applications and platforms that provide features of instant messaging, content creation, networking and connecting with strangers, and being a source of acquiring information and cherishing moments of entertainment. These features of social media applications along with other benefits have attracted more than half of the world's population. As per reports an estimated 5.07 billion people around the world use social media platforms of different kinds (Connell, 2024). This paper focuses on some of the leading social media platforms in the form of Instagram, X (previously known as Twitter) and WhatsApp. The study was aimed around these three social media giants because they are quite popular and highly utilized applications amongst people from different age groups. Also, these applications were originally developed with different initiatives and hence compliment each other quite well in terms of serving purpose and feature introductions.

Instagram is widely used photo sharing and messaging platform available over multiple operating systems and browsers. It is used for sharing photos, videos, connecting and interacting with strangers, content creation, audio and video calling, online shopping etc. Instagram has around 2.4 billion users worldwide (Mortensen, 2024). The next social media application is X (previously known as twitter). It is a messaging application and a microblogging site. It allows users to connect with different people, share ideas in the form of tweets, post comments, likes and make voice and video calls. As of early 2024, the X application had nearly 600 million active users (Mahajan, 2024). Lastly, WhatsApp is a widely used instant messaging platform that is available across multiple operating systems. It is used to connect with people, share messages, multimedia, interact with users via voice and video calling features, perform transactions etc. WhatsApp is the most widely used messaging platform with close 2 billion active monthly users (Ceci, 2024).

The increased usage of social media applications can also be accounted towards the exponential use in mobile phones. Due to technological advancements, what we have today in our packets is nothing short of an engineering marvel. These smartphone devices are convenient to use and have high computing powers, which is why they are quite popular among the masses. And what makes it more appealing is the fact that one can install and run their favourite social media applications on these mobile devices and stay connected with the online world at any given time. There are various mobile devices running on different operating systems like Android, iOS, Blackberry OS etc. However, people have slightly greater preference towards the android operating devices due to its user-friendly interface and efficient operating system, which is also evident from the smartphone market statistics which show that android has 70% market share today as compared to iOS’s 29% market share (Szczygieł, 2024).

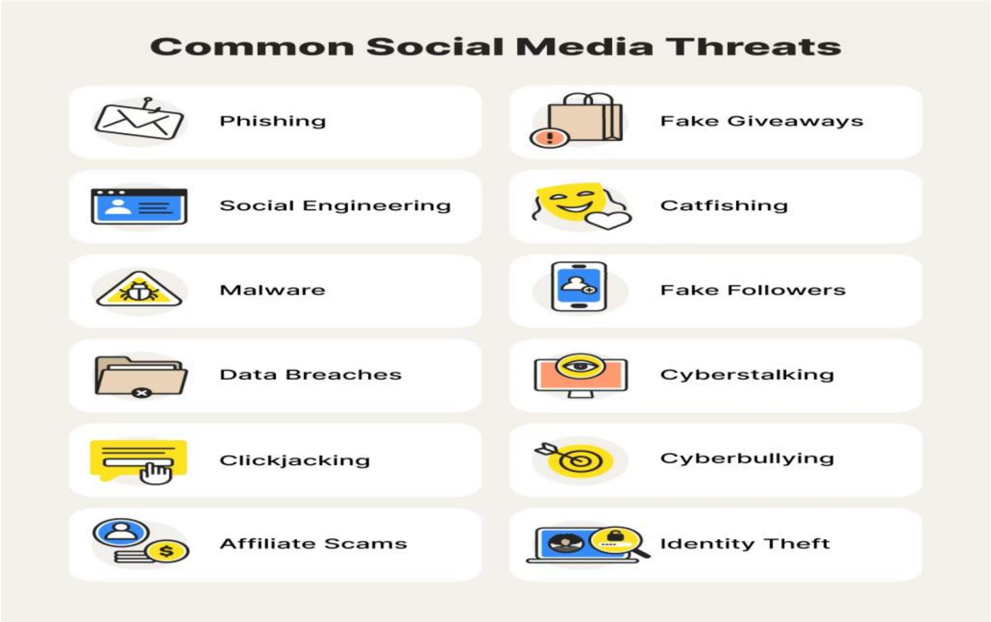

Figure 1: Common Threats and Attacks through Social Media

But as we know, every coin has two sides. Similarly, the advancement in smartphone devices and social media applications have both positive and negative impacts on our daily life. As good the benefits of social media platforms are, there is also a negative side or disadvantage of it. Lately, social media platforms have become a potential source of performing cyber or online crimes such as cyberbullying, identity theft, performing fraudulent transactions, cyberstalking, phishing, cyberterrorism, online scams, spreading of fake news and hate speeches etc. This has disturbed the harmony among online users and created a sense of fear while using these applications. Lately, tackling crimes occurring through these platforms has been a trending topic and has led to increased popularity of digital forensic techniques.

Digital forensics is a sub-domain within cybersecurity that applies the learnings of computer science, tools and techniques to collect, preserve, extract and analyse digital sources of data residing in electronic devices like mobile phones, laptops, pen-drives etc (Badman and Forrest, 2024). This research aims to make use of digital forensics techniques in accordance with the NIST framework to extract and analyse social media data residing in the internal storage of virtual android devices and understand its role in solving a crime investigation. The research utilizes different industry recognized tools and techniques in the entire process and recovers important digital artifacts in the form of text messages, call logs, personal information, multimedia etc.

This section sets the tone for the work to be followed. The section helps to understand the motivation behind the study, the work that would be done in the study and the summary about the expected results. The report structure is as mentioned below:

Related Work: It gives an idea about the literature review done around the topic in the past

Research Methodology: It gives an idea about the research approach and the information on different frameworks, tools and test case scenarios

Design Step: It gives an idea about the design that would be implemented as a part of this research

Implementation: It gives information on the derived results and its significance

Evaluation: This section critically evaluates our work based on the research question and objectives

Conclusion and Future work: This section provides an overview on the entire study with scope of future research/work.

1.1 Research Question and Objectives

The research question is “How digital forensics can make use of social media data obtained from a smartphone device to aid investigators in the overall crime investigation process?”

The objectives that we aim to attain through this research are as follows:

- To understand the structuring, storage and management of social media data in the internal storage of an android device
- To perform digital forensic process with industry recognized and legally accepted tools and techniques in accordance with universally accepted frameworks
- Extract and analyse social media data from android devices and look for potential sources of digital evidence/artifacts

- To analyse and provide practical applications and use-cases of the digital artifacts in real-world situations to aid in crime investigation process

2 Related Work

This research aims to understand the data storage and management structure in android devices with respect to the social media data, the various forensic tools and frameworks that can be utilized to perform forensically sound extraction of digital evidence belonging to popular social media applications of Instagram, X and WhatsApp from a virtual android device and analysing the evidence to discover any sources of potential cybercrimes along with potential sources of artifacts or digital evidence that can be utilized by investigators in solving a crime investigation. Digital forensics is quite a popular and emerging field among cyber enthusiasts and hence there are many research papers available around the topic of digital forensics of social media applications on mobile devices.

This section aims to provide a summary reflecting on the past work done around the topic along with critical analysis of each past research that motivated us towards choosing this area of research.

2.1 Summary Table of Past Research

Project Reference	Design Technique	Brief Summary
(Alisabeth and Pramadi, 2020)	Virtual android device using Genymotion	The authors performed forensic analysis of data extracted from Instagram application on android devices and analyzed the potential sources of artifacts.
(Pambayun and Riadi, 2020)	Digital Forensics using Oxygen Forensics and Json Viewer software on a physical android device	The authors make use of oxygen forensics and Json viewer software to extract and analyze crime related data from Instagram application on a physical android device and then compare the results.
(Gunawan, Mallitania and Sugiantoro, 2024)	Virtual android device using Genymotion	The authors analyze the digital artifacts extracted from WhatsApp, Instagram and Telegram applications on virtual android device.
(Azhar and Shortall, 2015)	Digital forensics using Oxygen Forensics and Cellebrite UFED on 3 physical mobile devices operating on different OS.	The authors try to recover and analyze digital artifacts from WhatsApp application on Android, iOS and Windows operating physical mobile devices.
(Zakarneh,	Digital Forensics using	The authors try to solve a fictional crime

2021)	ADB Backup and Final Mobile Forensic tool on a physical android device	scenario by analyzing digital artifacts extracted from WhatsApp on a physical android device in accordance with NIST framework.
(Arram, Owda and Shadeed, 2022)	Digital forensics of WhatsApp application on a non-rooted physical android device	The authors try to perform digital forensics of WhatsApp application on a non-rooted android device to extract evidence and analyze its usefulness in an investigation.
(Liu, Sun, Wu and Zhang, 2018)	Digital forensics of Twitter application on both a physical android and customized virtual android device	The authors aim to perform digital forensics of Twitter application on both a physical android and customized virtual android device to access and analyze the local data and remote online data of the Twitter user.
(Nurhairani and Raidi, 2019)	Digital Forensics of Twitter application on a rooted and non-rooted android device	The authors aim to extract and analyze twitter data from a rooted and non-rooted device to identify hate speech and compare the results.
(Awan, 2015)	Digital forensics of social media applications on physical mobile devices	The authors aim to extract and analyze social media data from android, iOS, Windows and blackberry operating physical devices.

Table 1: Literature Review Summary

2.2 Critical Analysis of Past Research

In the paper (Alisabeth and Pramadi, 2020) published in the IOP conference series, the authors analysed the digital artifacts generated from the Instagram application on a virtual android device. The research utilised the Genymotion software to create a virtual android device to install Instagram application and configure the test data on it. Once the setup and test data were configured it was extracted and analysed using the SQLite database. Post analysis, the authors highlighted the potential sources of digital artifacts of Instagram application that could be gathered from the device’s storage along with their details and potential use. However, the research report lacked details about the framework that was used in the digital forensics process. This motivated us to study and explore the different universally accepted industry framework that can be utilised in our research study.

In the paper (Pambayun and Riadi, 2020) published on ResearchGate, the authors focused their research on analyzing the text messages and photos/videos shared between users on Instagram application to identify any cybercrime or hate message. A physical android device was used in this process which had Instagram application and test data configured on it. Once the setup of the phone was ready, the data related to the Instagram application was extracted from the phone’s memory using the Oxygen Forensics software. The extracted data contained various databases, JSON files and multimedia which were analyzed using Oxygen Forensics software and the JSON viewer software. The results indicated successful retrieval of the text messages displaying some kind of crimes and abuse in it. The photos and videos were retrieved using the Oxygen forensics software but the same was not possible using the JSON viewer software. The entire digital forensics process was carried out in accordance with the Digital Forensics Research Workshop Framework. The study highlighted the importance of using digital forensics process and at the same time provided a comparative analysis between different techniques used in the process. However, the study only focused on one aspect of digital evidence, that is the text messages while not providing more details on other potential sources of digital artifacts and their use cases which could be of help in a crime investigation.

In the paper (Gunawan, Mallitania and Sugiantoro, 2024) published on IEEE, the authors aimed to understand the structure of data storage in android devices, their potential security impacts and analyzed the digital evidence acquired from WhatsApp, Instagram and Telegram applications installed on virtual android devices. The authors made use of the National Institute of Standards and Technology Framework to carry out the entire digital forensics process. By using a customized virtual android device in Genymotion software, all the applications were installed on it and the experiment setup was configured. Post creating this, using Kali Purple Linux and Digital Evidence and Forensic Toolkit the data was extracted from the virtual device and analyzed for potential digital artifacts respectively. The results reflected on the identification and tracing of the different artifact sources like multimedia, contact details, text messages, profile information etc. along with focus on how the phone’s memory stores social media related data and how digital forensics can play an important role in extracting and utilizing this information for investigation purposes.

In the paper (Azhar and Shortall, 2015) published on IEEE, the authors aimed at performing forensic analysis of WhatsApp data residing in the storage of phones running on Android, iOS and Windows operating systems. As a part of this research, three physical mobile devices running on different operating systems having WhatsApp application installed on it were used. A physical tool UFED by Cellebrite and Oxygen Forensics software was used to extract data from the device and analyze it for digital evidence. The results indicated that the digital evidence/artifacts related to text messages and media of the WhatsApp application were successfully retrieved from the device storage of Android and iOS mobile phones, however due to the strict security features of Windows operating systems the authors were not able to recover all the data. In such cases, the authors proposed a way of performing live forensics in accordance with the ACPO guidelines to recover maximum data. The study gave a good understanding of how data extraction and analysis of WhatsApp application can be performed on different operating systems and how artifacts can be used in investigations.

In the paper (Zakarneh, 2021) published on ResearchGate, the authors focused on analyzing digital evidence extracted from WhatsApp application on a physical android device by making use of ADB backup software, Final mobile forensic tool and NIST framework. The authors tried to create a fictional crime scenario and explored how digital evidence like text messages and multimedia data extracted from the WhatsApp application could prove beneficial in solving the overall investigation. The research was successfully able to retrieve digital evidence in the form of text messages, multimedia data, user information, call logs, documents etc., which was then analyzed to see its importance in crime investigation.

In the paper (Arram, Owda and Shadeed, 2022) published on ResearchGate, the authors focused on performing digital forensics of WhatsApp application on a non-rooted physical android device. The study made use of multiple different extractions, imaging and analysis software for successful retrieval of digital evidence from the device without rooting it. The study states that when a device is rooted one gets access to the application data and files stored in the local storage of the device, which is not quite possible in a non-rooted device. So, this paper suggests ways to perform a forensic extraction of data from a non-rooted device in accordance with accepted frameworks such that meaningful artifacts are analyzed and their potential usefulness in solving crime investigations are explored. The study also focuses on attempts to access the encrypted database of WhatsApp which stores messages and multimedia data belonging to WhatsApp users. The results gave a good idea of the potential data artifacts that could be recovered from the application on a non-rooted device.

In the paper (Liu, Sun, Wu and Zhang, 2018) published on IEEE, the authors tried a unique way of accessing and analyzing the local and the remote online data of the twitter application running on a physical android and a customized virtual android device. Initially, the authors utilized a physical android device, installed the twitter application and created the test data for experiment purposes. After this, the authors extracted the data from the local storage of the device (local data) through standard digital forensic procedures. After data extraction was done, the data was analyzed and the locations of the potential sources of digital artifacts were listed. Then, the Genymotion android emulator was used for the creation of a customized virtual android device. The virtual android device was customized to have the same IMEI and android number as that of the physical device. The twitter application was installed in the virtual device. The extracted data from the physical device was loaded into the virtual device via the ADB commands. It was observed by the authors that they were able to login to the application using the cache and the other data available from the extracted dump. After this they extracted the data from the virtual device and analyzed it too. The aim of this research was to understand the structure of data storage in android devices, analyze the local data in the device's storage and with the help of the local data login to the twitter application on the virtual device and access the remote online services and analyze that data too. The authors tried to show that the application and the device works in an active passive state. When the application was on the physical device and the internet connectivity was turned off for forensic extraction, there might be some data that might have not synced and stored in the database. This can sometimes lead to incomplete data. Also, one cannot directly login back or use the application on that device as it may tamper the data. This acts as a part of live forensics, which is the last resort in any digital forensic investigation and is done by taking appropriate permissions. So, to avoid that an alternative was provided in this paper to access the local and remote online services/data of the application.

In the paper (Nurhairani and Raidi, 2019) published on ResearchGate, the authors aim at performing digital forensics of Twitter application's data residing in the storage of a physical android phone to analyze and find any hate speech that could potentially help in solving a cyber investigation. The authors create a fictional scenario wherein two users of which one is a victim using twitter application on a non-rooted device and other is a criminal using twitter application on a rooted device are having a conversation over twitter. It is considered that some kind of hate speech is directed from the criminal to the victim via the direct message feature of twitter application. Using the NIJ method, the authors try to perform digital forensics on both the devices to extract and analyze the twitter data for any hate speech. The authors make use of various forensic tools like RootExplore and SQLiteManager. After extraction and analysis, it was observed that all the data was retrieved from the rooted device and the text messages indicating hate speech were identified which could potentially be of great help in an investigation. However, only an APK file was retrieved from the non-rooted device. This led to failure in identification of hate speech message on the non-rooted device. The study showed that the digital forensic process can be performed with much ease and better results could be achieved on a rooted android device.

In the paper (Awan, 2015) published on IEEE, the authors aimed to perform digital forensics to extract and analyze social media data from the internal storage of four different physical devices running on android, iOS, windows and blackberry operating systems. The social media applications that were tested as a part of this research were Facebook, Twitter and LinkedIn. The authors carried out the entire digital forensics process in accordance with the NIST framework, so that it is accepted according to legal and regulatory terms. After extraction of the data, it was analyzed for presence of digital artifacts. The directories of the potential sources of digital evidence in each of the applications were laid out as a part of the results discovered from the analysis. From the research, it was concluded that digital artifacts can be recovered and analyzed from Android, iOS and Windows operating devices but none of the evidence was recovered from the Blackberry operating devices.

3 Research Methodology

This section will discuss the entire approach that has been followed in this research as a response to the question of ‘How digital forensics can make use of social media data obtained from a smartphone device to aid investigators in the overall crime investigation process?’ The study of different papers around digital forensics of social media applications on mobile devices gave us a deep understanding of the entire process and its outcome and motivated us to further contribute to the area.

Most of the published papers around this topic focused on performing digital forensics on physical mobile devices, only a few of them utilized the concept of virtual devices. This motivated us to explore the digital forensics process on a custom based virtual android device as it could be utilized in real-world scenarios to provide better visualization and understanding of the entire process in a court proceeding. Also, technology keeps getting updated every single day, hence this paper tries to prove the applicability of the entire digital forensic process by analysing the digital evidence on latest versions of android devices and the social media applications. Last but not least, this research tries to combine the understandings acquired from the past study and provide a comprehensive overview by focusing on analysing the text messages between users on all three social media platforms to identify any scenario of crime or hate speech, analysing the potential sources of digital artifacts related to social media that could be recovered from the device's storage and their potential use cases in real-world scenarios to aid in the overall crime investigation process.

3.1 Digital Forensics

A crime investigation is meaningless without the involvement of forensics. The traditional forensics relied on chemical and biological forensic methods to aid investigators in the overall crime investigation process. But with the advent of internet and technology, the dynamics of crimes have changed over the last few years. There has been a notable shift towards cybercrimes and crimes conducted over mobile devices and social media platforms. This has led to the emergence of another field within the forensics domain known as Digital Forensics. Digital Forensics is the art of applying concepts of computer science and technology to collect, recover and analyse digital evidence from mobile devices, computers, laptops etc., in a forensically sound process that is legally accepted in court proceedings (Badman and Forrest, 2024). Digital forensics has various applications which range from solving cybercrimes like ransomware attacks to resolving civil and criminal investigations by analysing evidence from digital devices. The paper intends to use the knowledge of digital forensics to analyse data of social media residing in the internal storage of a virtual device and analyse its practical implications to help solve a crime investigation in real-world.

3.2 NIST Framework

The National Institute of Science and Technology (NIST) framework was developed by the United States National Institute of Technology and Framework in 2014. It comprises of a set of guidelines and protocols that organizations should follow to improve their cyber posture and increase their resiliency towards the cybersecurity risks/threats (SubRosa, 2024) . The NIST model clearly identifies an ideal digital forensic procedure in its special publication 800-61 (Revision 2), which provides an outline for investigators to perform a digital forensics process in a forensically sound manner that is as per industry standards and will hold admissible in legal court proceedings. This research aimed at utilizing the NIST framework for its entire digital forensic process as it is a universally accepted framework and can ensure that all the work is done in an accurate manner that maintains the integrity of the evidence and holds its value in legal proceedings. The NIST framework consists of four stages as mentioned below:

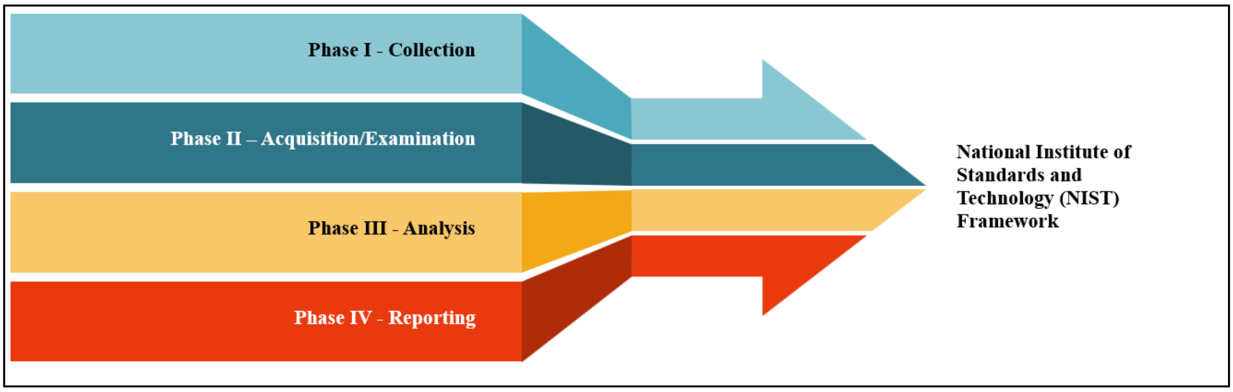
Phase I - Collection
Phase II – Acquisition/Examination
Phase III - Analysis
Phase IV - Reporting
National Institute of Standards and Technology (NIST) Framework

Figure 2: NIST Framework

1. **Collection:** This stage represents the process of identification and collection of the potential sources of evidence that would form the basis for the entire digital forensic process. In our research, the collection phase of NIST framework will focus on identifying and preserving the virtual android device that has the applications and social media data residing on it. This is an important step as it ensures that the data integrity is maintained, and the evidence (device) is not tampered.
2. **Examination/Acquisition:** This stage deals with the acquisition of the data from the chosen mobile device in an accurate and a forensically sound manner to maintain its integrity, availability and admissibility in a court proceeding. In our research, we have utilized an approach by using forensics tools to extract and create forensic images of the data to ensure its integrity and availability. The acquisition process would be explained in detail in the upcoming sections.
3. **Analysis:** This stage deals with the analysis of the extracted data using advanced forensic tools and techniques to discover digital artifacts and evidence that could be of potential interest to investigators in solving a crime investigation. Investigators make use of various tools like Oxygen Forensics, Cellebrite UFED, EnCase, Autopsy to perform the analysis process. The analysis process is explained in detail in the upcoming sections.
4. **Reporting:** This is the final stage of the NIST framework wherein a detailed and a comprehensive report documenting all the digital artifacts and evidence discovered from the analysis phase is prepared, such that it gives an accurate presentation of the entire digital forensic process.

3.3 Forensic Tools and Techniques

The NIST framework lists out guidelines for investigators which state the use of industry approved and legally accepted forensic tools and techniques to carry out the entire process in a forensically sound manner. In this subsection we analyse the different forensic tools and techniques available in the market and the justification behind selection of the tools. We will discuss the tools in accordance with the different stages of the NIST framework.

1. **Collection Stage – Android Studio software:** Android Studio is an Integrated Development Environment for app designing, development and testing purposes. Android Studio is used in this research to create a virtual android device for configuring the test environment on which the social media applications and test data would be setup. Android Studio is a free open-source software that has feature of configuring and running multiple customised virtual devices simultaneously. We explored multiple other emulator softwares like Genymotion, Noxplayer, BrowserStack etc. However, on critical analysis it was observed that each of them had certain limitations or drawbacks such as the Genymotion software did not allow multiple instances of emulator devices or rooting of android 13 and above devices in its trail version. The BrowserStack software allowed limited time access to the virtual device post which it would be deleted and the Noxplayer software had a lot of bugs and lagging issues. Therefore, it was identified that Android Studio would be the best fit for our research project.

2. **Examination/Acquisition Stage – FTKImager tool:** FTKImager is an open-source forensic tool that is mostly used for creation of forensic images and analysis of digital evidence/data. The FTKImager tool is used in this research to acquire the data from the virtual device and create forensic or logical images of it to maintain the data integrity and availability. There were multiple other tools such as Encase, Autopsy and Volatility for data extraction and forensic imaging. However, the Encase software is a paid commercial software, while Volatility tool is used majorly to perform memory forensics during events of malware attack. Since, we would be using the Autopsy tool during the analysis stage we decided to choose another software and selected the FTKImager tool.
3. **Analysis Stage – Autopsy software:** Autopsy is an open-source software used for performing digital forensics. It is a high-end computational software that has user-friendly interface and can be utilized to analyse forensic images or data for potential artifacts, deleted data and in-depth examination of different files and folders. There are multiple other softwares available for forensic analysis of digital data such as Cellebrite UFED, Oxygen Forensics, Encase etc. Even though these other mentioned softwares are good but they all are commercial paid softwares, that are used by investigators for examination and analysis purposes. However, as a part of our research, we selected the Autopsy tool for analysis of digital artifacts as it was an ideal fit considering the kind of features and results, we get with the autopsy tool and that too without paying a penny.

3.3.1 Accuracy or Recovery Success Rate of Forensic tools

As a part of the research work, we focused on the use of four different tools or software namely the Android Studio, Android debug bridge (ADB Commands). FTKImager and Autopsy. However, the Android studio was used only for the creation of the virtual environment. We used the other three tools as a part of the forensics process. This section mentions the accuracy or recovery success rate of these tools. It is a challenging task to determine the exact recovery success rate of these tools, because it varies with respect to the source of evidence, the type of data or files, its state, compatibility etc. Therefore, we will provide the different areas or conditions under which these tools provide accurate results.

The Android Debug Bridge (ADB) tool is used to extract the data from the virtual android device. The ADB tool performs efficiently and provides accurate results when working with rooted devices, wherein they have full access to all areas of the device. It can successfully recover application data, user files, logs, temporary and deleted files, multimedia. The recovery rate of the ADB tool will be hindered to some extent when working with non-rooted or encrypted devices or devices whose USD Debugging is disabled.

The FTKImager is a widely used tool in the forensics world. It provides high accuracy when dealing with data recovery or file analysis, forensic imaging and mounting, data integrity checks, file carving. The recovery success rate of FTKImager tools is quite high when dealing with unaltered data in normal state, fragmented data or even while dealing with deleted data. The recovery rate can be hindered when working with encrypted devices, damaged devices or overwritten data (Agboola, Osamor, Olajide , 2024).

Autopsy is one of the most widely used tool in the forensics world for data recovery and analysis. The Autopsy tool provides good compatibility when dealing with different sources of evidence like mobile devices, hard drives, laptops/computers etc. It provides high accuracy while dealing with data and file analysis, file carving, integrity checks, reporting. It has high recovery success rate when dealing with normal untampered data, deleted artifacts, temporary files, cache data, damaged data. The recovery rate is hindered when dealing with encrypted devices or fragmented data (Agboola, Osamor, Olajide , 2024).

3.4 Test Scenarios and Evaluation Parameters

This research aims to perform digital forensic analysis of social media data residing in the internal storage of virtual android devices, to look for potential sources of digital evidence/artifacts that could aid in investigation process. For implementation and evaluation of this research we consider the following test scenarios on all the three applications:

1. Two users are having a conversation using the direct message or text message feature of the three social media applications. This conversation remains private between the two users only. Consider that there is some kind of illegal activity/crime or hate message that has occurred between the two users through these text messages. The text messages would be accounted for as a potential source of digital evidence that could help shed light on whether crime or hate speech had occurred or not.
2. The second scenario would be to perform general activities on the application from a criminal’s perspective like uploading posts, tweets, likes, comments etc. and treating them as potential sources of digital evidence to verify if that data could be retrieved from the internal storage of the virtual device.
3. The last step which would not be treated as scenario but rather a critical analysis is to see how these recover digital artifacts could potentially aid investigators in solving a crime investigation (practical or real-world use-cases of the digital artifacts in solving an investigation)

The study will be evaluated based on the analysed results. The deciding factor for evaluation would be whether the research is able to accurately extract and identify evidence related to the crime activity or hate speech that occurred through the text messages, and whether the study is able to identify and recover maximum potential sources of digital artifacts and state its practical applications in aiding investigation process in real-world scenarios. The evaluation of the results would be done in detail in the upcoming sections.

4 Design Specification

This section details about the design specification for conducting the entire digital forensic process in this research. The design specification is divided into three stages:

4.1 Configuring the Test Environment

The research focuses on virtual android devices to store and extract social media data from. Therefore, as discussed in the above sections we utilize the Android Studio software to create customised virtual android devices for testing purposes. We have chosen to work with rooted virtual android devices in our research. This is done to achieve two objectives, first being that in most of the cases, a criminal would prefer to have a rooted device to perform illegal activities and second being that a rooted device provides with more access and leverage in performing the forensics process.

Android Studio Version: v2024.2

The below table provides a summary about the configuration and version details of the virtual android devices and the three social media applications in use.

Application	Application Version and Release Date	Virtual Device Name	Virtual Device Android version	Virtual Device configuration
Instagram	v278.0.0.22.117, Sept 24, 2024	Google Pixel 6	Android 9.0 API 28	Rooted device with 2GB RAM, 6GB internal storage and 512MB of external storage
X	v10.55.0, Aug 21, 2024	Google Pixel 6	Android 14.0 API 34	Rooted device with 2GB RAM, 6GB internal storage and 512MB of external storage
WhatsApp	v2.24.20.81, Oct 08, 2024	Google Pixel 5	Android 14.0 API 34	Rooted device with 2GB RAM, 6GB internal storage and 512MB of external storage

Table 2: Details of the social media applications

For creating the test environment to install these applications on a virtual android device, multiple permutations and combinations of different android versions and different versions of these applications were tried and tested. After multiple failed attempts, we were successfully able to find a combination of the application version and the virtual device's android version to setup the test environment, where focus was made to ensure that the latest android version and latest versions of the applications released in the past four months would be used. However, due to certain configurational requirements and security reasons, we were unable to install and test the Instagram application on the latest android versions. The following procedures were followed to install the applications and setup the test data for forensic analysis purposes. These procedures are mostly common for all three social media applications:

- Once the virtual devices were configured and booted, we started the process of installing the applications in them
- All three social media applications were downloaded from the ApkPure website. The ApkPure websites consists of apk files and packages of android applications with their previous versions and configuration details
- The applications were installed onto the virtual device via the drag and drop method
- Once the virtual device was setup and the required applications were installed, the process of test data creation for forensic analysis was initiated.
- Two test user accounts were created for each of the social media application wherein one user was considered as a suspect and the other user as a victim. The social media applications on the virtual device were logged in through the suspect's credentials/details, since our focus is on analysing the suspect's device
- The basic configurations and profile details of the suspect's user account were setup such as profile picture, personal details, adding a description (for Instagram), setting up the status (for WhatsApp) etc
- On Instagram and X applications, a follow request was sent by the suspect to the victim and other random users too. The follow request was accepted by the victim and a connection was setup (Followers and Following list)
- On WhatsApp application, the contact details of the victim were saved by the suspect, and a hello message was sent to the victim as part of initiating a conversation
- Now using the direct message feature on Instagram and X and the private conversation/ messages feature on WhatsApp, sample text messages and conversations indicating crime and hate speeches were shared between the two users on all these applications.
- Apart from that photos and videos were shared between the two users along with audio recordings, voice and video calls
- In the Instagram application, multiple posts, reels and story were uploaded by the suspect. The uploaded posts contained captions, comments and location details of the user/suspect
- In the X application, the user uploaded multiple posts and tweets and even performed retweets
- In WhatsApp application, the user used the story feature to upload multiple stories
- The user performed multiple searches as a part of search history on the Instagram and X application.
- On the Instagram and X application the user performed activity like posting comments, sharing likes and bookmarking posts etc
- On WhatsApp application, the suspect created a group which had the victim user and another random user. The group was used to carry out illegal activities and share wrongful material in the form of text messages or multimedia
- All the three applications were assigned different permissions such as access to camera, location, storage, microphone, contacts etc

These activities were performed on the three applications installed in the respective virtual android devices in Android Studio to create the test data that would be extracted and analysed for potential sources of digital evidence/artifacts that could assist in solving an investigation.

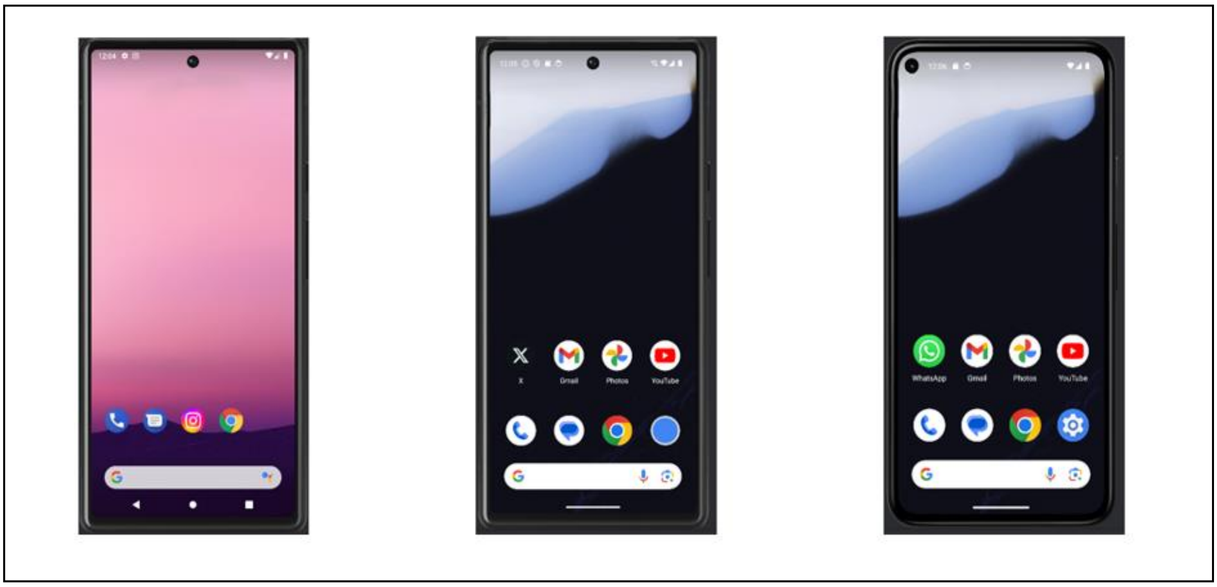

Figure 3: Social media applications installed on virtual android devices in Android Studio

4.2 Data Acquisition and Processing

This stage details about the entire extraction and forensic imaging process of the digital data of social media applications residing in the internal storage of the virtual android devices. The following steps were performed in this stage which were common for all three applications:

- For this stage, the ADB commands and the FTKImager software/tool were used
- The ADB commands were used in the terminal of the Android Studio software to connect to the virtual device and successfully extract the social media data from the internal and the external storage of the virtual android device onto the local folder of our laptop.
- Post extraction, the data was backed up and forensic imaging was performed using the FTKImager tool to ensure data integrity and availability
- The extracted data from the internal and external storage of the device was then fed to the FTKImager tool, which in return created a disk image of the data (.ad1 extension) and verified the integrity of the data by computing and comparing its hash value to ensure that there is no data tampering
- The next step involved mounting this disk image file on a logical drive to create a forensic image of the data. This was done using the FTKImager tool
- This forensic image of the data would then be analysed using the autopsy tool to locate potential sources of digital evidence in the next stage

FTKImager software version: v4.7.3.81

4.3 Analysis

This stage details about the analysis process that is carried out on the extracted social media data to locate for potential sources of digital evidence/artifacts that can aid in crime investigations. The autopsy tool is used in this stage to analyse the extracted social media data. The following steps were performed as a part of the analysis stage which were common for all three social media applications:

- Once the forensic image of each of the extracted data was taken, the next step involved the analysis of the data for which the autopsy tool was utilised
- In the autopsy tool the basic details required for building up a new case are inputted
- Then the forensic image of the data or the logic drive image of each social media application is fed to the autopsy tool for analysis purpose. The internal and the external storage data of each individual application is fetched in the same autopsy report under different data source tags.
- Once, the forensic image is analysed by the autopsy tool, it gives a listing and details of all the files and folders within the image along with the social media data that is of interest to us
- The final analysis results for each application will be discussed in detail in next section

Autopsy software version: v4.21.0

5 Implementation

This section describes in detail the final analysis results that have been generated for each of the three social media applications through the applied digital forensic process. These results will provide an overview of the entire process, the potential outcomes and implications and a thorough understanding of whether these results were successful in fulfilling the objectives that were set out in the research or not.

The Autopsy tool analyses the forensic images of the extracted data for all three applications and provides us with a detailed analysis report. This analysis report helps us to clearly identify the internal and external data storage and management structure in android devices with respect to the social media data. It helps us to analyse how much of the test data were we able to extract and recover successfully and how these recovered digital artifacts could potentially help investigators in solving a crime or cyber investigation. We will try to understand and analyse the results based on the test scenarios laid out in Section 3.4. According to Section 3.4, the implementation and evaluation of this research project would be based on three scenarios/test cases that are, analysing the text message conversations between users to identify any criminal activity or hate speech, analysing how much of the social media data can be recovered from the internal storage of the device and lastly analysing the potential use cases of the recovered digital artifacts. Therefore, on analysing the results based on these scenarios, we observe the following things.

After performing rigorous examination and analysis of the extracted data for each of the social media application on the Autopsy tool, we observe that we were able to successfully access and recover the text messages and private conversations that occurred between the users. These recovered text messages or conversations indicated presence of some illegal activities or hate speeches. This was a clear indication of some criminal activity that could potentially act as a great source of evidence in solving a crime investigation. Such text messages/conversations involving hate speech and sharing of illegal photos/videos between users was successfully recovered and identified on all three applications.

The next scenario involved analysis of how social media data is stored in the internal storage of the android device and how much of this test data could be recovered using the proposed digital forensic method. The autopsy tool provided us with a directory listing of all the data that resides in the internal and external storage of the device. This helped us understand and explore how social media data is stored in the storage of the virtual device and what data is stored in the internal memory and what is stored on the external memory (SDCard) of the device. We will now analyse the data that was successfully recovered for each of the application and what could potentially act as a source of digital evidence/artifact in an investigation process.

Application Name	**Digital Evidence/Artifacts**		
	Name	**Path**	**Content**
Instagram	Profile details and user information	/data/user/0/com.instagram.android/databases/direct.db-wal	Contains personal information about the user like username, email address, phone number, user bio/description etc
	Followed accounts	/data/user/0/com.instagram.android/databases/direct.db-wal	Contains only the information on number of followed and following accounts
	Direct messages/ Text conversations	/data/user/0/com.instagram.android/databases/direct.db	Contains information of text messages or private conversations occurring between users
	Video/Voice calls	/data/user/0/com.instagram.android/databases/direct.db-wal	Contains information about the call logs between users
	Shared posts/multimedia with users	/data/user/0/com.instagram.android/databases/direct.db-wal	Contains information about the posts that are shared with users via the direct message feature
	Search history	/data/user/0/com.instagram.android/databases/ig_msys_database_17842650819366744	Contains information about the search history performed by the user
	Timestamp / Logs	/data/user/0/com.instagram.android/databases/time_in_app_70827974743.db	Contains information on the last logging and other activity
X	Posts / Tweets	/data/com.twitter.android/da	Contains information

		tabases/1861368657680769024-drafts.db	about the uploaded posts/ tweets by the user
	Search history	/data/com.twitter.android/databases/1861368657680769024-search.db	Contains information about the search history performed by the user
	Direct messages / Text conversations	/data/com.twitter.android/databases/1861368657680769024-drafts.db-wal	Contains information of text messages or private conversations occurring between users
	Retweets	/data/com.twitter.android/databases/1861368657680769024-66.db	Contains history of retweets
	Comments	/data/com.twitter.android/databases/1861368657680769024-drafts.db-wal	Contains information about the comments made by the user on different posts/tweets
	Multimedia shared	/sdcard/Pictures/Twitter	Contains information about the photos and videos shared between users
	Location	/data/com.twitter.android/databases/1861368657680769024-drafts.db-wal	Contains location history of the user
	Timestamp/ Logs	/data/com.twitter.android/databases/0-lru_key_value.db	Contains information on the last logging and other activity
WhatsApp	Profile details and user account information	/data/data/com.whatsapp/databases/msgstore.db /data/data/com.whatsapp/databases/contacts2.db	Contains personal information about the user like username, email address, phone number
	Contacts	/data/data/com.whatsapp/databases/wa.db	Contains information about the other users and their contact details
	Shared multimedia (photos/videos) sent and received	/data/data/com.whatsapp/files/.Shared (For shared multimedia) /sdcard/Pictures/.thumbnails (For received multimedia)	Contains information about the photos and videos sent and received between users and groups
	Call history	/data/data/com.whatsapp/databases/msgstore.db	Contains information about the call logs

			between users
	Profile pictures	/data/data/com.whatsapp/cache/Profile Pictures	Contains the profile pictures of the user and others
	Story	/sdcard/Pictures/.story	Contains information about the user's story
	Status	/data/data/com.whatsapp/files/status	Contains information about the user account and other account's status
	Text Messages	/data/data/com.whatsapp/databases/msgstore.db	Contains information of text messages or private conversations occurring between users and group participants
	Payment details	/data/data/com.whatsapp/databases/payments.db	Contains information about transactions or bank information
	Pages and communities followed	/data/data/com.whatsapp/databases/msgstore.db-wal	Contains information about followed pages and communities
	Location	/data/data/com.whatsapp/shared_prefs/com.whatsapp_prefernces.xml	Contains location history of the user
	Timestamp / Logs	/data/data/com.whatsapp/files/Logs/whatsapp-2024-11-26.1.log.gz /data/data/com.whatsapp/shared_prefs/time_spent_prefs.xml	Contains information on the last logging and other activity

Table 3: Summary of digital artifacts extracted from social media application

The evidence (in the form of screenshots) for each of the test case scenarios and digital artifacts is recorded and presented in a separate file named as the artifacts ICT file which will be shared along with the main report. Kindly refer to the same for analysing the screenshots.

These are the results that were analysed from the digital data of social media extracted from the virtual android devices. The last scenario which focuses on the potential use-cases and practical application of the digital artifacts in solving crime investigations will be discussed in the Evaluation Section.

6 Evaluation

This section provides a comprehensive analysis and evaluation of the applied forensic process and the acquired results to verify whether the objectives of the research were met. The evaluation of this study will be based on the parameters/scenarios depicted in the Section 3.4 of this research paper. The evaluation of this study will provide us with a thorough answer to the research question "How digital forensics can make use of social media data obtained from a smartphone device to aid investigators in the overall crime investigation process?"

Based on the mentioned scenarios/test cases in Section 3.4 and the results acquired from the autopsy tool in Section 5 of the report, it can be clearly stated that the study is able to correctly identify the presence of hate speech or illegal activities performed on all three social media applications by analysing the digital artifacts of text messages/private conversations extracted from the internal storage of the virtual android device by using digital forensic processes in accordance with the NIST framework.

Now, based on the second test case/ scenario in Section 3.4 and the results acquired from the autopsy tool in Section 5 of the report, it can be stated that the study has done an ideal job of extracting and recovering digital artifacts/evidence of social media applications residing in the internal storage of the virtual device by applying digital forensic processes in accordance with the NIST framework. The reason for stating that it has performed an ideal job was because there were various issues encountered while extracting and analysing the digital evidence which did not lead to full recovery of the data belonging to certain social media applications. To be precise, the research was unable to extract the information or profile details and call history of the user account on X application. Also, the research was unable to extract and recover information related to uploaded posts, reels, story and location history of the user account on Instagram application. There might be various reasons as to why this occurred but two of the most significant reasons that we could analyse post this research were that firstly the past literature review done around this topic was performed on lower/earlier versions of the android device and the application. However, with new advances in technology the newer versions of android device and the application may have stringent security policies and configurations which would deny storing or extracting certain kind of data from the phone's memory. The other reason could be that the forensic tools that we have utilised in the research may have limited data extraction capabilities due to which not all the data was recovered. However, since the other premier forensic tools were paid commercial software, it caused a limitation towards exploring them. The list of recovered and non-recovered data for each of the respective applications is mentioned in the table below.

Artifacts	Instagram	X	WhatsApp
Multimedia (Photos/Videos)	Not Recovered	Recovered	Recovered
Posts/Tweets/Story	Not Recovered	Recovered	Recovered
Location history	Not Recovered	Recovered	Recovered

User information / Profile details	Recovered	Not Recovered	Recovered
Text Messages/ Private Conversations	Recovered	Recovered	Recovered
Call logs	Recovered	Not Recovered	Recovered
Search history	Recovered	Recovered	Not Applicable

Table 4: Summary of digital artifacts extracted from social media application

The above summary table indicates that most of the data related to the WhatsApp application was extracted and recovered successfully from the internal storage of the virtual device through the digital forensic process. The final stage of the evaluation process involves mentioning of the use-cases or practical applications of the acquired digital evidence/artifacts in real-world situations such that it could help in solving crime investigations. The use-cases or practical applications of the artifacts are as mentioned in the below table.

Artifacts	Content	Potential use cases or applications
Posts/ Tweets/ Story	Includes content uploaded on social media	This information can be used to understand and study the behavioural patterns and lifestyle of the suspect and could be useful in analysing whether the suspect could commit a certain crime or not
Text messages/ Private Conversations	Includes conversations that happen between users or within a group and includes texts, multimedia etc	This information can be utilised by investigators to identify the presence of any criminal activity, wrongful acts, hate speech or events related to cyberbullying etc. and can potentially help in solving an investigation
Location history	Information about the user's location (device's location)	This vital information can be utilised by the investigators to track the activity of the user and analyse their involvement near a crime scene
User details/ Profile information	Includes personally identifiable information like name, username, email address, phone number etc	This information could prove to be very helpful to the investigators in situations where they have no clue on the suspect but have found a mobile device. By analysing personal information of a user like name, phone number etc they can move a step ahead in their investigation process
Multimedia (Photos/Audio/ Video)	Includes photos, audio and video recordings uploaded or shared	This could contain evidence of any wrongful acts committed by the user in digital formats and could potentially act as a breakthrough in the investigation

Call history	Information about the call logs	This information can be used by investigators to a keep a track on the suspect's contacts who might be involved in the crime and analyse the call activity that has happened over social media in the form of transcripts or logs
Search history	Information about the searches made by the user	This information can be used to analyse and study the behavioural pattern of the suspect and could be useful in analysing whether the suspect could commit a certain crime or not. It can also be helpful in analysing incidents of cyberstalking
Logs and Timestamps	Information about the course of events	This information could be used by the investigators to track the activities performed by the user on social media application and verify their involvement during the moments of crime commitment
Payment and Transaction history	Information of transactions and bank data	This provides vital information about the transactions and bank related information of the user. This could potentially be of great help to investigators to detect any unusual transaction activity, fraudulent transactions or details of ransom payments
Access permissions	Includes access that an application has towards the device like (camera, storage, location, microphone, contacts)	The data that the application stores in the form of access permissions could potentially contain important piece of information or evidence

Table 5: Use-Cases and Practical Applications of Digital Artifacts

The evidence in the form of screenshots for the above artifacts and other results is recorded and presented in a separate file named as the artifacts ICT file which will be shared along with the main report. Kindly refer to the same for analysing the screenshots.

Thus, it can be concluded from the evaluation of the entire process and results that the study presented in this paper has done a good job of answering the research question and proposing a solution that can be utilized by investigators in real-world situations during a crime investigation or during court proceedings.

6.1 Discussion

This section provides a brief overview of the entire research that has been conducted and the results generated as part of it. The study was conducted to understand and analyse how the social media data extracted from the internal storage of virtual android devices can be utilized to solve a crime or cyber investigation. The study was performed using universally accepted forensic tools and techniques in accordance with industry recognized and legally accepted NIST framework, so that the overall process and the acquired results could mimic a real-world digital forensic process. The experiment had an ideal design which led to successful configuration of test environment, accurate and forensically sound data extraction and an efficient analysis process. There were a few exceptions where all the data was not being recovered from certain applications due to reasons mentioned before and can be considered as a part of future research work, but the overall study had fruitful results. Since, the study was performed in accordance with universal and legal standards, it could be utilized in real-world scenarios to investigate a suspect's device.

The study conducted here is very much like real world digital forensic processes apart from a few changes such as in real-world forensic analysis, a faraday bag is used to collect and preserve the physical electronic devices, commercial tools and software are used for the entire forensic process. The study or the approach can also be followed for digital forensic process over the iOS operating mobile devices with few notable changes. These changes are due to the structure and functioning of the iOS devices. The iOS devices store the application data in closed sandboxed file systems or directories which are not directly accessible. One needs specialised tools for that, or the best possible solution is to perform jailbreaking on the iOS devices. Once this is achieved, the remaining extraction and analysis process is like the one followed over the android platforms. The study helps to understand the digital forensics domain and contribute towards it.

7 Conclusion and Future Work

The objective of the research project was to understand how android devices perform storage and management of social media data within their internal storage and how this data can be extracted and analysed using digital forensic processes to aid investigators in the crime investigation process. The study conducted in this paper proposed a design and solution that was efficient in answering the research question and providing fruitful results. The study conducted in this paper was in accordance with the universally accepted frameworks and utilized industry recognized and legally accepted forensic tools and techniques. This ensures the applicability of the solution/study in real world scenarios. The study was successful in identifying hate speech or crime activities occurring through social media which acted as a great source of digital evidence during the investigation, while the study also focused on analysing the potential sources of artifacts and their applications/use-cases in real world situations.

There is a lot of scope for future work around this topic or domain. As a part of this research project we worked on android operating systems, however there are multiple operating systems available in the market today and carrying out a digital forensic analysis of social media applications on other operating systems would be a topic of my interest. I would also like to perform the forensic analysis of social media applications on non-rooted devices to understand the technicalities and challenges and learn new workarounds and techniques to solve and analyse them.

References

Agboola, V., Osamor, J. and Olajide, F. (2024) ‘Evaluating the efficiency of FTK, Autopsy, and mobile forensic tools: A comparative study in criminal investigations’, in *International Journal of Intelligent Computing Research.* United Kingdom, 2024, Available at: https://10.20533/ijicr.2042.4655.2024.0156 [Accessed 26 January 2025]

Alisabeth,C. and Pramadi,Y.R. (2020) ‘Forensic Analysis of Instagram on Android’, in *IOP Conference Series: Materials Science and Engineering*. Jakarta, Indonesia, 3-4 August 2020, Available at: https://doi.org/10.1088/1757-899X/1007/1/012116 [Accessed 04 October 2024]

Arram, L.A., Owda, M and Shadeed, M. (2022) ‘Forensic Analysis of WhatsApp Artifacts in Android without Root’, in *Advances in Science Technology and Engineering Systems Journal*. April 2022, Available at: https://doi.org/10.25046/aj070212 [Accessed 06 October 2024]

Awan, F.A. (2015) ‘Forensic Examination of Social Networking Applications on Smartphones’ , in *Conference on Information Assurance and Cyber Security (CIACS)*. Rawalpindi, Pakistan, December 2015, Available at: https://doi.org/10.1109/CIACS.2015.7395564 [Accessed 10 October 2024]

Azhar, M.A.H.B and Shortall, A. (2015) ‘Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms’, in *Sixth International Conference on Emerging Security Technologies (EST).* Braunschweig, Germany, 3-5 September 2015, Available at: https://doi.org/10.1109/EST.2015.16 [Accessed 06 October 2024]

Badman, A. and Forrest, A. (2024) *What is digital forensics? | IBM*, *www.ibm.com*. Available at: https://www.ibm.com/topics/digital-forensics/ [Accessed 06 December 2024]

Ceci, L. (2024) *Topic: WhatsApp* (2018) *www.statista.com*. Available at: https://www.statista.com/topics/2018/whatsapp/ [Accessed 06 December 2024]

Connell, A. (2024) *30+ Social Media Usage And Industry Statistics (2024)*. Available at: https://adamconnell.me/social-media-statistics/ [Accessed 06 December 2024]

Liu, X., Sun, W., Wu, S. and Zhang, Y. (2018) ‘Forensics on Twitter and WeChat Using a Customised Android Emulator’, in *IEEE 4th International Conference on Computer and Communications (ICCC)*. Chengdu, China, 7-10 December 2018, Available at: https://doi.org/10.1109/CompComm.2018.8781056 [Accessed 10 October 2024]

Mahajan, V. (2024) *50+ X (Twitter) Statistics & Facts Need to Know in 2025* (2024) *Notta.ai*. Available at: https://www.notta.ai/en/blog/twitter-statistics [Accessed 06 December 2024]

Millatina, D., Gunawan, E.H. and Sugiantoro, B. (2024) ‘Forensic Analysis of WhatsApp, Instagram, and Telegram on Virtual Android Device’, in *12th International Symposium on Digital Forensics and Security (ISDFS).* San Antonio, TX, USA, 29-30 April 2024, Available at: https://doi.org/10.1109/ISDFS60797.2024.10527308 [Accessed 04 October 2024]

Mortensen, O. (2024) *How many users on Instagram? Statistics & facts (2024)*, *SEO.AI*. Available at: https://seo.ai/blog/how-many-users-on-instagram [Accessed 06 December 2024]

Nurhairani, H. and Riadi, I. (2019) ‘Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method’ in *International Journal of Computer Applications*. December, 2019, Available at: https://www.researchgate.net/profile/Imam-Riadi-2/publication/338067201 [Accessed 10 October 2024]

Pambayun,S. and Riadi, I. (2020) ‘Investigation on Instagram Android-based using Digital Forensics Research Workshop Framework’, in *International Journal of Computer Applications.* December 2020, Available at: https://www.researchgate.net/publication/347441116 [Accessed 04 October 2024]

Subrosa. (2024) *Understanding the NIST Digital Forensics Framework: Advancing Cybersecurity Practices.* Available at: https://subrosacyber.com/en/blog/nist-digital-forensics-framework [Accessed 06 December 2024]

Szczygieł, B. (2024) *iPhone vs Android Users: Key Differences*, *www.netguru.com*. Available at: https://www.netguru.com/blog/iphone-vs-android-users-differences [Accessed 06 December 2024]

Zakarneh, S. (2021) ‘Forensic Investigation of WhatsApp on Android Smartphone’s’, in *International Journal of Science, Engineering and Technology*. August 2021, Available at: https://www.researchgate.net/profile/Shadi-Zakarneh-2/publication/354103749 [Accessed 06 October 2024]