

**ANDROID FORENSICS FOR CYBERCRIME
INVESTIGATION IN MYANMAR**

NAING LINN HTUN

UNIVERSITY OF COMPUTER STUDIES, YANGON

DECEMBER, 2021

Android Forensics for Cybercrime Investigation in Myanmar

Naing Linn Htun

University of Computer Studies, Yangon

A thesis submitted to the University of Computer Studies, Yangon in partial
fulfillment of the requirements for the degree of
Doctor of Philosophy

December, 2021

Statement of Originality

I hereby confirm that the work involved in this dissertation is an original research result and has not been presented to a higher degree in any other institution or university.

I also followed this study with my knowledge and beliefs that do not include material previously published or written by others, except for the appropriate references are made in the text of the dissertation.

17-12-2021

.....
Date



.....
Naing Linn Htun

ACKNOWLEDGEMENTS

Through this work, I have the opportunity to express my sincere regards and appreciation to all the people who assisted and guided me to make this dissertation.

First of all, I would like to express very special thanks to Dr. Mie Mie Khin, the Rector, the University of Computer Studies, Yangon, for allowing me to develop and giving me general guidance in this dissertation. I would like to mention my special appreciation and thanks to Dr. Mie Mie Thet Thwin, former Rector of University of Computer Studies, Yangon, for her kindly support and encouragement during the period of my Ph.D. study.

Second, I would like to express my deep gratitude to my supervisor, Dr. Khaing Khaing Wai, Professor, the University of Computer Studies, Yangon, for her consistent support and motivation during my Doctoral degree studies. She provided me with guidance and knowledge, and led me in the right direction during the time of writing this dissertation.

Third, I would like to offer my sincere gratitude to my course coordinator of Ph.D 10th Batch, Dr. Thin Lai Lai Thein, Professor, the University of Computer Studies, Yangon, for her excellent guidance, patience and taking care of me throughout my Ph.D life. Then, I also would like to express my respectful gratitude to Daw Aye Aye Khine, Associate Professor, Head of English Department, for her valuable supports from the language point of view and pointed out the correct usage in my dissertation. I would like to extend my special thanks to my co-supervisor, Dr. Cho Cho San, Lecturer, University of Computer Studies, Yangon, for her suggestions and comments.

Then, I would like to extend my special thanks and acknowledge to Prof. Dr. Mie Mie Su Thwin and Prof. Dr. Khine Khine Oo who gave me kindly support, motivation, encouragement, and valuable suggestions in this dissertation.

I also would like to thank my beloved parents for their help and support during each step of my life. They taught me the value of hard work and an education. Without them, I may never have gotten to where I am today. Also, I would like to show my deepest gratitude for their financial support, encouragement and endless trust during the time of my Doctoral degree studies.

Furthermore, I would like to thank my friends of Ph.D 10th Batch, who have accompanied me throughout my journey. And, I also want to thank all members of our laboratory for their help and support of my research in the laboratory.

Finally, special thanks to my committee members: Dr. Aung Htein Maw, Professor, University of Information Technology and Dr. Win Pa Pa, Professor, University of Computer Studies, Yangon who kindly agreed to serve on my committee.

This dissertation is dedicated to my father, mother and elder sisters. Their love, encouragement, trust and understanding made everything I have possible.

ABSTRACT

Mobile phone technology is changing rapidly, and there are a growing number of different device models with different operating systems around the world. In particular, Android mobile devices are becoming much more attractive than any other platforms, not only in Myanmar's mobile market but also in other developing countries. It can offer flexibility and convenience for communication, entertainments, sharing and storing data, using social media network, and others. People use smartphones for different purposes, such as for their personality and business. On the other hand, if the smartphones were involved in a crime, the evidence data may be on devices. In such cases, investigators should have adequate investigation processes, procedures, frameworks, and forensics tools to obtain evidence data.

In this dissertation, the workable process flow has been proposed for the forensics investigation on Android devices which consists of seven stages. They are (1) Preparation, (2) Determine Scope of Crime Scene, (3) Secure Evidence Devices Collection, (4) Documentation and Preservation, (5) Examination and Analysis, (6) Presentation and (7) Review. A detailed analysis framework has also been proposed for Examination and Analysis stage. It is divided into two main parts – Live Forensics and Static Forensics because if the investigator does not notice the Live Forensics, the data on memory can be easily lost.

Finally, an applicable tool (ANDROSICS) with many useful features has been proposed that would support the analysis framework. It consists of five main parts – (i) data acquisition and collection, (ii) examination and analysis (iii) Bruteforcing (iv) reporting, and (v) management process. In data acquisition and collection stage, it provides to extract both volatile and non-volatile data on Android devices. This stage generates the four types of data such as Portable Network Graphics (.png) file from the screenshot, Android Backup (.ab) file from backup process, ANDROSICS file (.andro6) from volatile data and Image file (.img) file from non-volatile data. In the examination and analysis phase, it can check the integrity of all collected data in prior stages. Afterwards, the investigator can analyze the device information, corrupted files, potential data in SQLite database files on and on. In Bruteforcing, it can crack the password of device screen locks, zip files, Microsoft Office files and pdf files. Investigator can also create custom wordlist with many rules in this stage. In the reporting stage, it supports to generate the report files for all data in investigation

processes. As the management process, it protects the tampering of authorized users, Login access for authorized users and Logs for all activities.

Besides, the data collection process was evaluated and implemented on some popular brands of android devices in Myanmar. They are Huawei, Samsung and Oppo devices with different versions. And the ANDROSICS tool is compared with some other opensource tools and overview research work comparison is based on the related papers. In any case, since this research work is dedicated to our country, it is hoped that it will be useful for android forensics investigation because well-defined process flow, framework, localization tool is not available in our country yet.

Keywords: Cybercrime Investigation, Mobile Device Forensics, Android Platform, Live Forensics, Static Forensics, Data Acquisition, Bruteforcing.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	i
ABSTRACT	iii
TABLE OF CONTENTS	v
LIST OF FIGURES	ix
LIST OF TABLES	xii
1. INTRODUCTION	1
1.1 Evolution of Mobile Device Forensics	2
1.2 Problem Statement	2
1.3 The Need for Mobile Device Forensics	3
1.3.1 Use of Mobile Phones to Store and Transmit Personal Information	4
1.3.2 Using the Mobile Smartphones in Online Transactions	4
1.3.3 Law Enforcement, Criminals and Mobile Devices	4
1.4 Motivation of Android Forensic	4
1.5 Challenges faced by Android Forensics	7
1.6 Position of the Research	7
1.7 Organization of the Research	8
2. BACKGROUND THEORY AND LITERATURE REVIEW	9
2.1 Cybercrimes	9
2.2 Type of Cybercrimes	9
2.2.1 Hacking	9
2.2.2 Theft	9
2.2.3 Cyber Stalking	10
2.2.4 Malicious Software	10
2.2.5 Child soliciting and Abuse	10
2.3 Digital Evidence and Nature of Digital Evidence	10
2.4 Cyber Security and Digital Forensics	11
2.5 Basic Branches of Digital Forensics	12
2.5.1 Network Forensics	13
2.5.2 Computer Forensics	13
2.5.3 Mobile Device Forensics	13
2.5.4 Database Forensics	14
2.5.5 Memory Forensics	14

2.6 Challenges faced by Digital Forensics	14
2.7 Nature of Forensics	15
2.7.1 Dead/Offline Acquisition	15
2.7.2 Live Acquisition	15
2.8 Mobile Device Forensics	16
2.9 Nature of Android Operating System	18
2.10 Android Mobile Device Forensic	19
2.11 Commercial Mobile Device Forensic Tools	19
2.11.1 OSAF	20
2.11.2 Oxygen	20
2.11.3 Autopsy	20
2.11.4 XRY	20
2.11.5 Andriller	21
2.11.6 UFED	21
2.11.7 MOBILedit	21
2.12 The Literature Reviews	22
2.12.1 Mobile Device Forensics	22
2.12.2 Process Model and Framework for Android Forensics	23
2.12.3 Tools for Android Forensics	24
2.13 Comparative Study of Android Forensics Tool Suites	27
2.14 Summary	29
3. THE PROPOSED METHODOLOGY	30
3.1 Process Flow for Mobile Device Forensics	30
3.1.1 Preparation	31
3.1.2 Determine Scope of Crime Scene	32
3.1.3 Secure Evidence Devices Collection	32
3.1.4 Documentation and Preservation	33
3.1.5 Examination and Analysis	34
3.1.6 Presentation	34
3.1.7 Review	34
3.2 Analysis Framework for Android Forensics Investigation	34
3.3 Proposed ANDROSICS Tool Suite	36
3.3.1 Data Collection Process	37

3.3.2 Examination and Analysis	40
3.3.3 Brute Force	42
3.3.4 Report	42
3.3.5 Management	42
3.3.6 Other Provided Features for Android Forensics	43
3.4 Summary	43
4. IMPLEMENTATION AND EXPERIMENTAL RESULTS	44
4.1 Testing Environment	44
4.1.1 USB Debugging Mode Preparation	45
4.1.2 Tamper Protection	46
4.1.3 Case Ticket Creation	47
4.2 Data Collection Process	48
4.3 Examination and Analysis	52
4.3.1 Data Viewer	53
4.3.2 Backup File to Zip Format	54
4.3.3 File Type Analyzer	55
4.3.3.1 Sample Scenario for Evaluation	58
4.3.3.2 Evaluation of File Analyzer feature using ANDROSICS	61
4.3.4 SQLite Reader	62
4.4 Brute Force Techniques	63
4.4.1 Wordlist Creator	63
4.4.2 Screen Lock Decoder	66
4.4.2.1 Pattern Lock	67
4.4.2.2 Pin Code (Personal Identification Number)	69
4.4.2.3 Password Lock	71
4.4.3 Zip/Rar Password Cracker	73
4.4.4 Microsoft Office Password Cracker	77
4.4.5 PDF Password Cracker	77
4.5 Reporting	78
4.5.1 Main Report	79
4.5.2 Data Viewer Report	82
4.5.3 File Analyzer Report	82
4.5.4 SQLite Database Report	84

4.6 Management	85
4.7 Additional Features	89
4.7.1 Android Device Management	89
4.7.2 Cryptography	90
4.8 Comparison	96
4.9 Sample Scenario	99
4.10 Summary	102
5. CONCLUSION AND FUTURE WORK	103
5.1 Benefit of the Research	105
5.2 Limitation of the Research	105
5.3 Future Work	106
AUTHOR'S PUBLICATIONS	107
BIBLIOGRAPHY	108

LIST OF FIGURES

Figure 1.1	Fishbone Diagram for Loss of Evidence in Cyber-crime Investigation	3
Figure 1.2	Smartphones Platform Usage in Myanmar (2016)	5
Figure 1.3	Smartphones Platform Usage in Myanmar (2016-2020)	6
Figure 1.4	Smartphone Vendor Market Share Myanmar 2017	7
Figure 2.1	Cyber Security and Digital Forensics	11
Figure 2.2	Forensics Process Flow (NIST)	12
Figure 2.3	Basis Branches of Digital Forensics	13
Figure 2.4	Smartphone Component Consideration	17
Figure 2.5	Architecture of Android Operating System	18
Figure 2.6	Android Partitions	19
Figure 3.1	The Overview of Proposed Methodology	30
Figure 3.2	Proposed Process Flow for Android Forensics in Cybercrime Investigation	31
Figure 3.3	Changing Settings for Control Access	33
Figure 3.4	Analysis Framework for Android Forensics Investigation	35
Figure 3.5	Features of Proposed ANDROSICS Tool for Android Forensics in Cybercrime Investigation	37
Figure 3.6	Dump System Service List	39
Figure 3.7	PNG Signature and Chunk	41
Figure 4.1	USB Debugging Mode Preparation in Jellybean Version	45
Figure 4.2	USB Debugging Mode Preparation in Oreo Version	46
Figure 4.3	Tamper Protection for ANDROSICS Tool	46
Figure 4.4	Creating and Analyzing a Case Ticket	47
Figure 4.5	Live Data Acquisition on Samsung Device	48
Figure 4.6	Active Mode Instruction Box	49
Figure 4.7	Backup Process on Android Device	50
Figure 4.8	Backup Process	50
Figure 4.9	Streaming Live Log Data.....	51
Figure 4.10	Notice of Super Capture Feature	51

Figure 4.11	Imaging Process Flow	52
Figure 4.12	Imaging Feature in Androsics Tool	52
Figure 4.13	(a) Examination and Analysis Process on Huawei Device Data	53
Figure 4.13	(b) Examination and Analysis Process on Samsung Device Data	53
Figure 4.14	Data Viewer Feature	54
Figure 4.15	(a) Backup File Converter without Backup File	54
Figure 4.15	(b) Backup File Converter with Backup File	55
Figure 4.16	(a) Four types of Status for File with Extension	57
Figure 4.16	(b) Three types of Status for File with no Extension	57
Figure 4.17	(a) Four File Formats in Five Files based on ZIP File	59
Figure 4.17	(b) Using File Analyzer Feature from Androsics for Evaluation	59
Figure 4.18	(a) True Negative – Extension Changes from ZIP to PNG	59
Figure 4.18	(b) False Negative – both Change Extension and Header Code	60
Figure 4.18	(c) True Negative - Delete Extension of ZIP File	60
Figure 4.18	(d) False Positive and True Positive of ZIP File	60
Figure 4.19	(a) Two Files with no Extension Format	61
Figure 4.19	(b) True Positive and False Negative in File with no Extension	61
Figure 4.20	(a) Evaluation on APK File Format	62
Figure 4.20	(b) Evaluation on JPG File Format	62
Figure 4.21	SQLite Database Reader	63
Figure 4.22	Windows View of Androsics Wordlist Creator	66
Figure 4.23	Android Phone with Pattern Lock	67
Figure 4.24	Three Types of Pattern Lock Decoding Process	69
Figure 4.25	The Appearance of Pin Lock on Android Smartphone	70
Figure 4.26	Pin Lock Decoder Feature	71
Figure 4.27	Salt Number in settings.db	71
Figure 4.28	Android Phone with Password Lock	72
Figure 4.29	Device Policies File Screenshot	72
Figure 4.30	Password Lock Decoder in ANDROSICS tool	73

Figure 4.31	Evaluation on ZArchiver Application	74
Figure 4.32	Evaluation on BreeZip Application via Microsoft Store	75
Figure 4.33	Evaluation on WinRAR Application	75
Figure 4.34	The Detail Process of Zip/Rar Password Cracking Process	76
Figure 4.35	The Appearance of Zip/Rar Password Cracker in Androsics Tool	76
Figure 4.36	Microsoft Office File Password Cracker in Androsics Tool	77
Figure 4.37	PDF File Password Cracker Feature in Androsics	78
Figure 4.38	Main Report Screenshot	81
Figure 4.39	Account Information Report (Sample Screenshot)	82
Figure 4.40	File Summary Report (Sample Screenshot)	83
Figure 4.41	Specific File Report (Sample Screenshot)	83
Figure 4.42	Overview Report of SQLite Database Reader	84
Figure 4.43	Specific Report of SQLite Database Reader	85
Figure 4.44	Tamper Protection with Secret Key	86
Figure 4.45	User Account Login Feature	86
Figure 4.46	User Management Feature	87
Figure 4.47	Case Access Logs	88
Figure 4.48	Detail Logs	88
Figure 4.49	Wireless Debugging through ADB	89
Figure 4.50	Command Box	90
Figure 4.51	Hash Calculator	91
Figure 4.52	Encode and Decode Feature	91
Figure 4.53	Substitution Cipher	92
Figure 4.54	Encryption Feature	92
Figure 4.55	Decryption Feature	93
Figure 4.56	Hex Viewer	94
Figure 4.57	Steganography (LSB)	94
Figure 4.58	The Detail Process of PNG Dimension Fixer	95
Figure 4.59	The Appearance of Image Dimension Fixer in Androsics Tool	95

Figure 4.60	View of Application Lists in SQLite Database Reader	100
Figure 4.61	The Appearance of Map My Run Application	101
Figure 4.62	Evidence Data in Database File of Map My Run Application	101
Figure 4.63	Evidence Data in Database File of Google Maps Application	101
Figure 4.64	The Configuration of Timeline Tracking Feature	102

LIST OF TABLES

Table 1.1	Detail Description of Smartphones Platform usage in Myanmar 2016	5
Table 1.2	Detail Description of Smartphones Platform usage in Myanmar (2016-2020)	6
Table 2.1	Comparative Study of Open-Source Tools for Android Forensics	28
Table 2.2	Evaluation on Samsung Galaxy (GT-S5300) v2.3.6	28
Table 2.3	Evaluation on HTC Desire 300 v4.1.2	29
Table 3.1	Technical Expected Requirements in Preparation	32
Table 3.2	Four Type of File Formats from Data Collection Process	37
Table 3.3	The Overview of File Type Analysis	41
Table 4.1	The Detail Description of Testing Environment	44
Table 4.2	Case Information of a Ticket	47
Table 4.3	Profile Data of Evidence Device	49
Table 4.4	Classified for File Type Analyzer	55
Table 4.5	Possible Statuses of Some Text-Based File Types	58
Table 4.6	Permutation and Combination Algorithms for Generating Password ..	64
Table 4.7	Input Characters Groups	64
Table 4.8	Rules of Wordlist Creator	65
Table 4.9	Execution Time and Integrity on Three Types of Pattern Lock Decoder	68
Table 4.10	Different Types of Zip Application for Testing	74
Table 4.11	Testing Environment for PDF Password Cracker	78
Table 4.12	Sample of Data Collection Report	80
Table 4.13	Comparison of Some Forensics Tools and Proposed ANDROSICS	96
Table 4.14	Comparison of Other Tools based on the Features of ANDROSICS ...	98
Table 4.15	Crime Investigation Environment	99
Table 4.16	Main Directory of Map My Run and Google Maps Application	100
Table 5.1	Interesting Directories for Evidence Information	104
Table 5.2	Interesting Artifacts Data for Evidence Information	104

CHAPTER 1

INTRODUCTION

With the development of daily life and business at the speed of electronic communication, most civil and criminal investigations involve some kind of digital elements. As mobile phones become more prevalent and play a major role in society, these devices are more likely to be part of these investigations. There are four ways to connect a mobile phone to a crime [24]: (1) It can be used as a communication tool in the process of committing crimes (2) It can be a storage device that provides evidence of a crime (3) It may include victim information (4) It may be a means of crime. Thus, criminal investigators need to be familiar with mobile phones and understand the complexity of mobile devices forensics.

Mobile device forensics is an area of digital forensics that is related to extract and analyze all data from the evidence devices under forensically sound conditions. Digital investigators no longer need to try to read people's minds because people's interests, financial information, personal information, hidden secrets, and even their life affair are all on their smartphones. Nowadays, people cannot do their life activities joyfully without having their smartphones for even a day. Since they store the confidential data on their smartphones, data is sometimes more valuable than their devices. If an important person lost his mobile phone and the bad guy got it, the data inside the phone can lead to a crime. On the other hand, if the investigator seized the mobile phone related to the crime, the data on the mobile devices has become very important as the evidence in investigation processes.

Nowadays, the number of smartphone users is increasing significantly year by year. There are four mobile operators and a lot of internet service providers in Myanmar. Some people have more than one smartphone with dual SIM (Subscriber Identification Module) cards. It is necessary for the adequate process flow, framework, and forensics tools. Therefore, this thesis proposed suitable process flow, applicable framework, and ANDROSICS tool for Android forensics. Because according to mobile usage in Myanmar, Android smartphones are used more than any other smartphone. Additionally, investigator can use commercial tools, open-source tools and local own tools but the local own tool is not available yet.

1.1 Evolution of Mobile Device Forensics

Forensics is a field of science that including data acquisition, recovery process and investigation of material found on digital evidence devices, often related with computer crime. In the middle of the 1980s, with the rise of cybercrime, the judiciary began enacting legislation to deal with the ever-increasing cases of cybercrime. That is why, forensics investigator considered the investigation and analysis process for digital devices based on computer crime. NIST (National Institute Standards and Technology) highlighted that its proposed Forensic procedures and guidelines should be in line with the law relating to organizational policies in 2006. Organizations should include legal advisors, investigators, and technical experts in the development of procedures and guidelines as a quality assurance measure.

For mobile devices forensics investigation, many researchers have been searching and exploring the different ways to tackle the crimes that they proposed guidelines, methodologies, frameworks, tools, and techniques. NIST provides basic elements of mobile forensics process flow and information required for mobile forensics tools in 2014. This process contains five steps - preservation, acquisition, examination, analysis, and reporting [8].

1.2 Problem Statement

Figure 1.1 illustrates the possible causes that generate the loss of digital evidence of mobile devices in cyber-crime investigation. With the growth of technology, if people do not have the security awareness, it may lead to some problems in our digital world. Among them, people have to care about the disturbance of insiders. There are three types of insiders. If the security awareness is accessible, the practicable policies and laws regarding to the cyber-criminal activities can be drawn. Many knowledgeable experts are also necessitated to draw the well-defined policies. If the clear policy is not available, this can conduct the problem. Even though the well-defined policies and laws are available, the procedures are still required to follow up these defined policies. Whenever the chiseled procedures cannot be built, it may cause the loss of evidence in cyber-crime investigation process.

In addition, the materials are also needed to support in digital forensic process. Materials include the powerful machines, money, faraday bag, mobile devices, PCs, USB cable, power bank, memory sticks and so on. As the rapidly development in

technology, the modern mobile devices include the anti-forensics features in different perspectives such as block the permission of access, constraints. Many commercial forensic tools are expensive and will not be able to effort for the developing countries like Myanmar. Sometimes, it may lead to the sanction problem depending on the countries. Furthermore, some open-source tools are not convinced and there is no guarantee. Most of the trial tools cannot get all functions with fully access. In the digital era, every country should have a forensic tool suite based on their countrywide policies and laws to collect the useful evidence for cyber-crime investigation activities. Definitely, there is no digital forensics tools in Myanmar. Thus, in this dissertation aims to build the compact and standardize mobile device forensics guidelines and proposes a framework for developing country like Myanmar. Then, this dissertation implements the Android forensics tool suite (ANDROSICS) based on the proposed forensics process flow and framework for Myanmar.

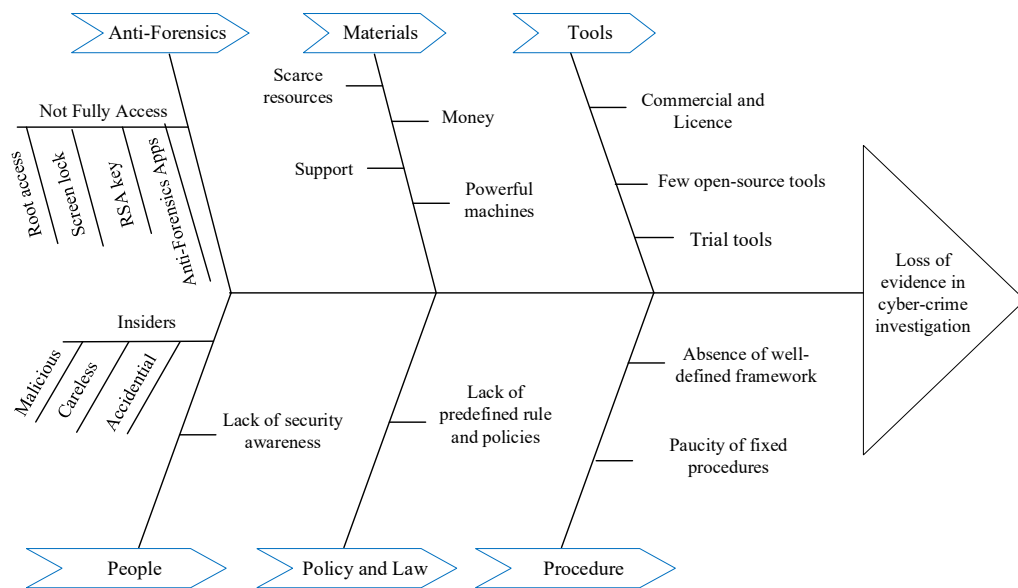


Figure 1.1 Fishbone Diagram for Loss of Evidence in Cyber-crime Investigation

1.3 The Need for Mobile Device Forensics

There are many aspects to consider in mobile device forensics. This section describes the need for mobile device forensics by highlighting the following [36]:

1.3.1 Use of mobile phones to store and transmit personal information

Mobile smartphones applications are developing rapidly. Spreadsheets, Word processors and database-based applications have already been ported to the smartphone devices. The ability to print, store and view electronic documents are performed by these devices. The mobile phone's ability to send and receive SMS (Short Message Service) messages also transformed mobile devices into a message center. People use their smartphones in social media communication with the use of internet.

1.3.2 Using the mobile smartphones in online transactions

Wireless Application Protocol (WAP) has changed the way mobile phones are used in online transactions. Further improvements in security and connectivity of mobile devices and networks technologies have enabled the smartphones to be used securely in online transactions such as airline reservation, hotel reservation, online shopping, stock trading, mobile banking and so on. As part of mobile technology development, the idea of mobile device forensics came to our mind and so this dissertation is a milestone to achieve the objectives.

1.3.3 Law enforcement, criminals and mobile devices

The gap between the law enforcement and cybercrime is still considerable when it comes to the utilization of mobile phone technologies. Mobile phones were used by criminal organizations as a tool to evade capture and facilitate everyday operations. On the other hand, law enforcement and digital forensics still lag behind when it comes to dealing with the digital evidence obtained from mobile devices.

1.4 Motivation of Android Forensic

According to the statistics of mobile device users in Myanmar, 2016, ninety-two percent of smartphone users (27.7 million) are used the Android platform, around five percent (1.5 million) are used iOS and almost three percent (0.9 million) are used the other platforms. The detailed statistics are described in Table 1.1 and summary are shown in Figure 1.2 [45].

Table 1.1 Detail description of smartphones platform usage in Myanmar (2016)

Platform	Android	iOS	Other
Percentage	91.56	5.247	0.204
Total Number	27768000	1572000	954000

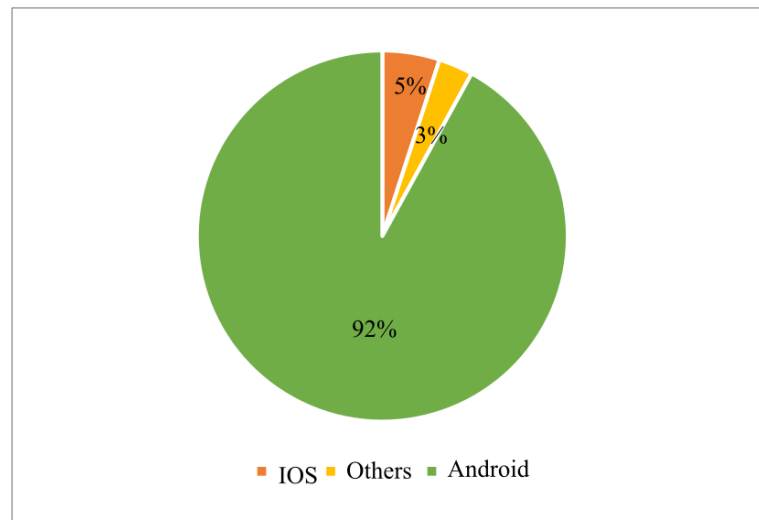


Figure 1.2 Smartphones Platform Usage in Myanmar (2016)

Furthermore, the usage of mobile devices in Myanmar are analyzed within five years from 2016 to 2020 as described in Table 1.2. Based on this analysis, it can clearly be seen that the percentage of Android smartphone users in Myanmar are significantly higher than iOS and other smartphone operating systems. In Figure 1.3 can obviously see the usage of different smartphones platform for five years (2016-2020). At the beginning of this thesis, the analysis of mobile usage of 2014-2016 is done, but so far Android platforms are still the most used in Myanmar, 2020. Thus, this dissertation aims to propose the compact and optimal guidelines for Android mobile device forensic process in Myanmar. After that, the analysis framework has been proposed based on the proposed Android forensic process flow. Finally, the ANDROSICS tool suite is implemented that is technically suitable for the proposed framework and process flow for Android mobile forensics. However, there is no one tool that can fit for all forensic solutions.

Table 1.2 Detailed description of smartphones platform usage in Myanmar (2016-2020)

Year	Android	iOS	Linux	Windows
2016 July	91.56	5.247	0.204	0.079
2017 July	85.23	6.137	0.107	0.055
2018 July	89.581	6.892	0.035	0.032
2019 July	90.341	9.162	0.025	0.016
2020 July	89.684	10.12	0.023	0.012
Average	89.2792	7.5116	0.0788	0.0388

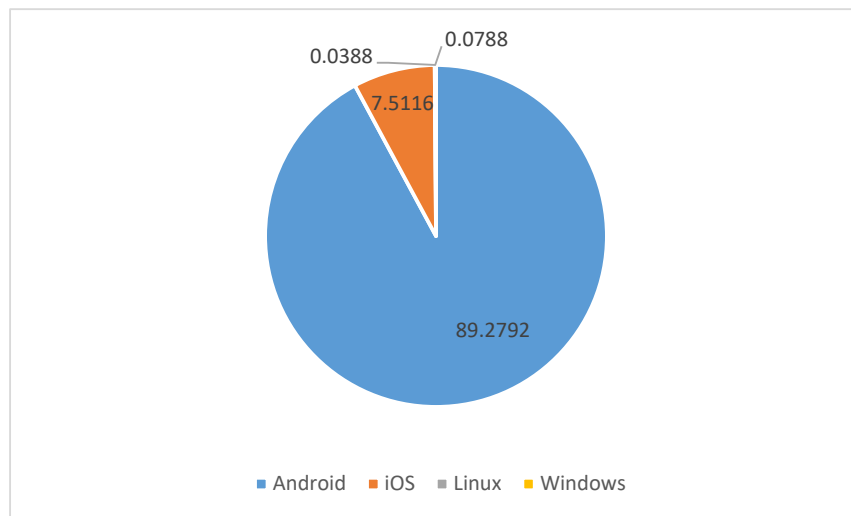


Figure 1.3 Smartphones Platform Usage in Myanmar (2016-2020)

For selecting the testing devices, the author studied which mobile brands are the most used in the smartphone market of Myanmar in 2017. Among them, Huawei mobile device is highest percentage and Samsung mobile device is the second most common of all. The detailed statistical analysis is illustrated in Figure 1.4. Based on the above statistic, the author decided to use them for testing devices in this thesis.

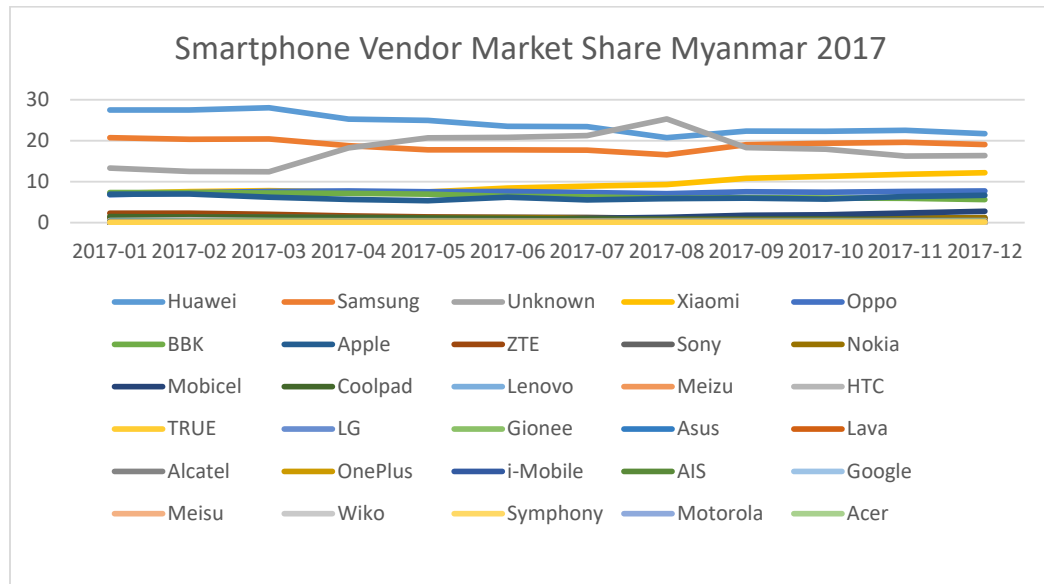


Figure 1.4. Smartphone Vendor Market Share Myanmar 2017

1.5 Challenges faced by Android Forensics

There are challenges and issues faced by criminal investigators in forensics on Android smartphones.

- **Android Emulator** cannot support some of main features and processes for testing forensics investigation.
- **Stock Firmware** is wide range of versions and it have different nature depend on mobile brands.
- **Custom Firmware** is a fully standalone version and developers customized or modified any features as they like.
- **Commercial Tools** are very expensive, and we cannot afford to do practical tests for forensics process.

1.6 Position of the Research

There is no precise or well-defined cyber laws and forensic investigation procedure in most of the developing countries like Myanmar. Some of the existing process flows are complex and have necessitated factors due to the rapidly changing of technology. Nowadays, in developing countries should have their own forensic process flow and framework corresponding to their home countries. Especially, there is no precise cyber laws and procedures in Myanmar at the present time.

Thus, it is necessary to do many researches on forensics in order to develop in the cyber forensics' activities. This research has proposed the appropriate forensic process flow and framework in forensics investigation for Myanmar. Moreover, an Android forensic tool suite (ANDROSICS) has been implemented which is technically suitable for doing the investigation process. It can be believed that this research will be a partly support research in cybercrime investigation process in Myanmar.

This research emphasizes on to extract many useful artifact data from Android smartphone devices. Then, the extracted data are stored in the encryption format to prevent the access or read the data from unauthorized access users. In addition, the focus on developing theoretically necessary features is described, based on the results of discussions with the Cyber Police Department in Nay Pyi Taw.

1.7 Organization of the Research

This dissertation is organized with five chapters, the introduction of Android forensics with motivation is mentioned in this Section. A brief explanation of background theory and literature reviews are described in Section II. The proposed Methodology is explained in Section III. The implementation setup and evaluation of proposed ANDROSICS tool suite is discussed in Section IV. The last section will present about conclusion and future work of this research.

CHAPTER II

BACKGROUND THEORY AND LITERATURE REVIEW

This chapter discusses the concepts of cybercrimes, cyber-attacks, fundamental of Android forensics and literature review in the development of android forensics methodologies such as process flows, analysis frameworks, acquisition methods, tools and techniques.

2.1 Cybercrimes

Cybercrimes can be defined as the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones.

2.2 Type of Cybercrimes

When any crime is committed over the Internet, it is referred to as a cyber-crime. There are many types of cyber-crimes and the most common ones are explained below:

2.2.1 Hacking

This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

2.2.2 Theft

This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber-crime and there are laws that prevent people from illegal downloading.

2.2.3 Cyber Stalking

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

2.2.4 Malicious Software

These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

2.2.5 Child soliciting and Abuse

This is also a type of cyber-crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

2.3 Digital Evidence and Nature of Digital Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cellphones, and digital fax machines.

The main characteristics of digital evidence are – it is latent as fingerprints and DNA, can transcend national borders with ease and speed; highly fragile and can be easily altered, damaged, or destroyed; and also, time sensitive. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. When dealing with digital evidence, the principles that should be applied are – actions taken to secure and collect digital evidence should not change that evidence; persons conducting the examination of digital evidence should be trained for this purpose; and activity relating to the seizure, examination, storage, or transfer of digital evidence should be fully documented, preserved, and available for review.

2.4 Cyber Security and Digital Forensics

The characteristics of cyber security and digital forensics are closely similar. The main difference is the nature of their process. Cyber security process is running before the crime and especially do the protection prior happening the crime. The digital forensics is about the investigation after a cyber-attack or crime has been taken place. The study of the evidences from attacks on digital systems in order to learn what has occurred, how to prevent it from recurring, and the extent of the damage. Figure 2.1 shows the nature of cyber security and digital forensics.

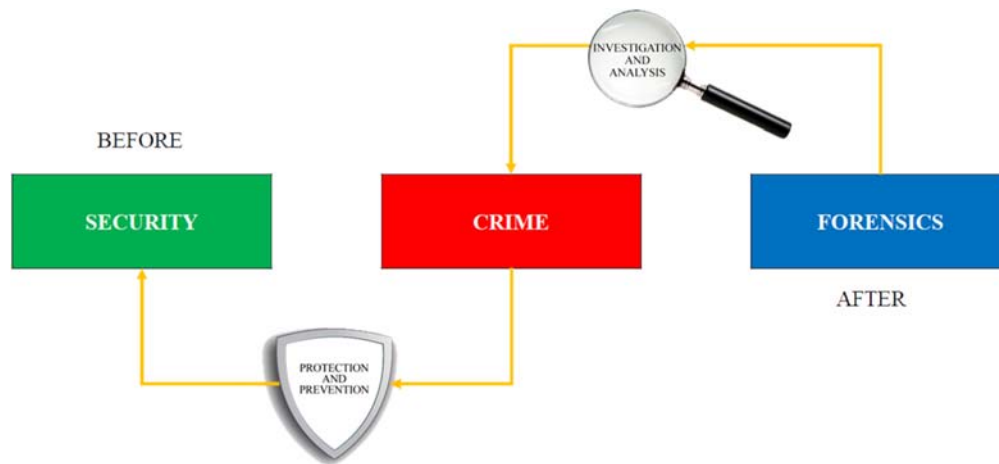


Figure 2.1 Cyber Security and Digital Forensics

The fundamentals of most common digital investigation, which contain digital evidence, digital forensics tools, and scientific methods. Digital evidence is defined as any digital information that is stored, transmitted or produced from electronic devices and software (e.g., pictures, downloaded files, logs, email, browser history file, etc.). Digital forensics tools include proprietary tools, open-source tools and own tools. The investigators need to choose the proper tools for their investigation and apply the scientific methods such as investigating phenomena, acquiring new knowledge, or correcting and integrating previous knowledge [17][20].

Basically, digital forensics process encompasses with four key elements that are established by National Institute of Standard and Technology (NIST) as shown in Figure 2.2. Generally, most of the researchers and forensic organizations are doing researches and proposed the modified process flows in different perspective based on NIST process flow for forensics investigation. However, the following five stages are common in their proposed digital forensics process.

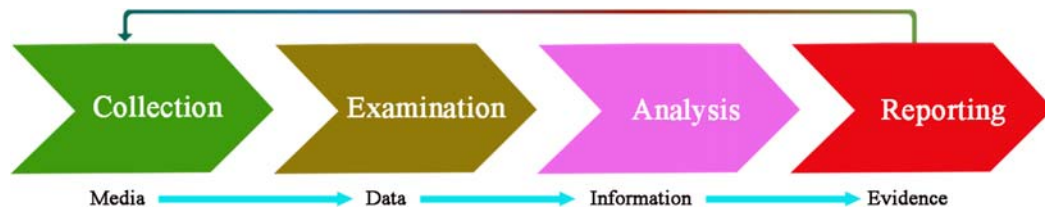


Figure 2.2 Forensics Process Flow (NIST)

- ***The identification and acquiring of digital evidence:*** Knowing what evidence is present, where it is stored and how it is stored is vital in determining which processes are to be employed to facilitate its recovery. In addition, the Cyber forensic examiner must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it. After the evidence is identified the cyber forensics examiner/ investigator should image/ clone the hard disk or the stored media.
- ***The preservation of digital evidence:*** It is a critical element in the forensic process. Any examination of the electronically stored data can be carried out in the least intrusive manner. Alteration to data that is of evidentiary value must be accounted for and justified.
- ***The analysis of digital evidence:*** The extraction, processing and interpretation of digital data is generally regarded as the main element of cyber forensics. Extraction produces a binary junk, which should be processed, to make it human readable.
- ***Report the findings:*** It means giving the findings, in a simple lucid manner, so that any person can understand. The report should be in simple terms, giving the description of the items, process adopted for analysis and chain of custody, the hard and soft copy of the findings, glossary of terms on and on.
- ***The presentation of digital evidence:*** It involves deposing evidence in the court of law regarding the findings and the credibility of the processes employed during analysis.

2.5 Basic Branches of Digital Forensics

The branch of Cyber forensics can be classified into various sub-branches. Some of these sub-branches are illustrated in Figure 2.3 [12].

2.5.1 Network Forensics

Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

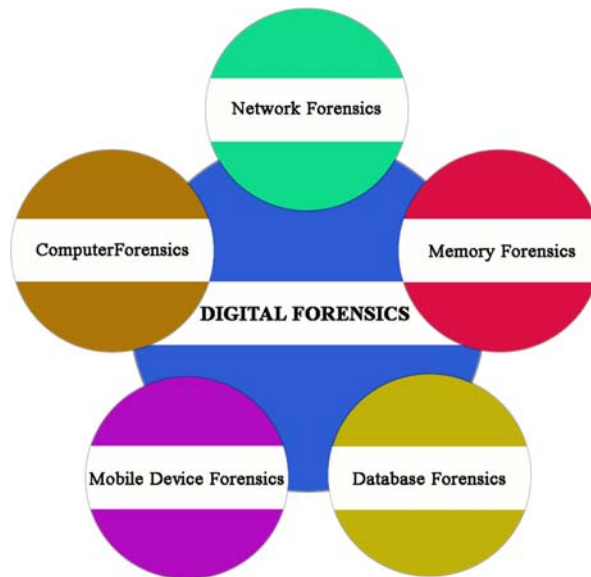


Figure 2.3 Basis Branches of Digital Forensics

2.5.2 Computer Forensics

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

2.5.3 Mobile Device Forensics

Mobile device forensics deals with examining and analyzing mobile devices like mobile phones, pagers to retrieve addresses book, call logs (Missed, Dialed, Received), Paired Device History, Incoming/Out Going SMS/MMS, Videos, Photos, Audio on and on. Mobile device forensics is a part of digital forensics that the recovery of digital evidence data from a suspected mobile device.

2.5.4 Database Forensics

Database Forensics is a branch of digital forensic science relating to the forensic study of databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.

2.5.5 Memory Forensics

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in the memory dump of a computer. Information security professionals conduct the memory forensics to investigate and identify the attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data. Memory forensics deals with the collecting data from system memory such as system registers, cache, RAM in raw form and then carving the data from raw dump.

2.6 Challenges faced by Digital Forensics

There are major challenges faced by the digital forensics:

- The increase of PC and usage of mobile devices in daily life
- The extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes the difficulties in prosecution
- The large amount of storage space leads to the difficulties in investigation job
- Any technological changes require an upgrade or changes to solutions

There are some major benefits of digital forensics:

- It ensures the integrity of the computer system.
- It produces evidence in the court, which can lead to the punishment of the culprit
- It helps the companies to capture important information if their computer systems or networks are compromised
- Efficiently tracks down cybercriminals from anywhere in the world
- It helps to protect the money and valuable time of individual or organization
- It allows to extract, process and interpret the factual evidence, so it proves the cybercriminal action in the court

2.7 Nature of Forensics

Forensic investigations seek to uncover evidence and analyze it to gain a full understanding of a crime scene, the motives of the criminal's identity. Due to the smartphones and internet have become ubiquitous in our daily lives, the cyber realm increasingly contains the potential evidence for all types of criminal investigations. Traditional cyber forensics have focused on dead-box analysis, however, there is an emerging methodology for live-box analysis.

2.7.1 Dead/Offline Acquisition

Dead/Offline forensic is conducted on media that is powered off and in the case of hard drives, removed from the potentially compromised system. It creates the snapshot of system information and swap files. In terms of evidence preparation, this method is most comprehensive as it allows for the complete preservation and analysis of a physical volume [21]. There are several methods and tools available, both commercial and free-ware that allow for the proper imaging.

The dead forensic has the slim chance of data modification and small window of opportunity for retrieval of volatile data. However, it will lose the volatile network data, take the gigabytes of data to analyze, lack of standardized procedures, it has practical and legal constraints and evidence can easily render inadmissible [13].

2.7.2 Live Acquisition

Live data forensics is one part of digital forensic science pertaining to legal evidence found in digital devices. The digital forensics deals with the examination of systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Live data forensics follows this aim but is only focused on the digital devices that are powered on. The main purpose is to acquire volatile data that would otherwise get lost if the device is turned off or would be overwritten if the device will stay turned on for a longer period. Volatile Data are digitally stored in a way that the probability is very high for their contents to get deleted, overwritten or altered in a short amount of time by human or automated interaction.

The Random-Access Memory (RAM) use the whole array of quick storage to cache and serve data more quickly the possibility of evidence being stored in this area

is very high. RAM contents are fading very quickly as soon as the investigator cuts the power supply from a device unless they are treated in a special way. In times where more and more data get stored either temporarily in RAM or remotely or the operating system does not store any data on the permanent storage, all these data would get lost without Live Data Forensics techniques [23].

2.8 Mobile Device Forensics

Nowadays, mobile smartphones are leading technology market in Myanmar. They involve confidential and differences of data; from normal to professional life. Most of the Myanmar people use the smartphones for social media and some people use for business or personalities but others use for their profits by illegally. It may bring not only convenience for people but also crimes or security issues. Thus, cyber-crime investigation process on mobile devices is becoming an essential activity in our country. Some researchers and forensic organizations have been searching the different ways and they proposed the guidelines and frameworks for mobile devices forensics. However, some of the developing countries including Myanmar cannot afford to use the commercial tools for android investigation due to the high in price.

Mobile device is a small computing device and portable. Typically, small enough to hold and operate in the hand. Moreover, it has an operating system capable of running mobile applications. There are many types of mobile devices:

- Smartphones
- Laptops
- Tablets
- Bluetooth
- Bring Your Own Device (BYOD)

Smartphone is one of the most popular types of electronic media that endure today. Most people have at least one mobile device, which is usually a smartphone. The smartphone users need to know how to handle their devices, what the data looks like and, more importantly, where the data will be stored. Smartphones have a variety of data storage functions that can include other storage components that need to be addressed during the forensic process. These are:

- Random Access Memory (RAM)
- Read-only Memory (ROM)
- Flash memory

- MicroSD cards for storage expansion
- Subscriber Identity Module (SIM) card
- Central processing unit (CPU)
- Cloud-based storage unit
- Synced computers
- BlackBerry enterprise servers (BES)

Commonly, smartphones have SIM cards and SD cards, which contain unique data that may not be captured during the investigation process. Figure 2.4 shows some aspects of consideration in smartphone components during forensics acquisition of the device.

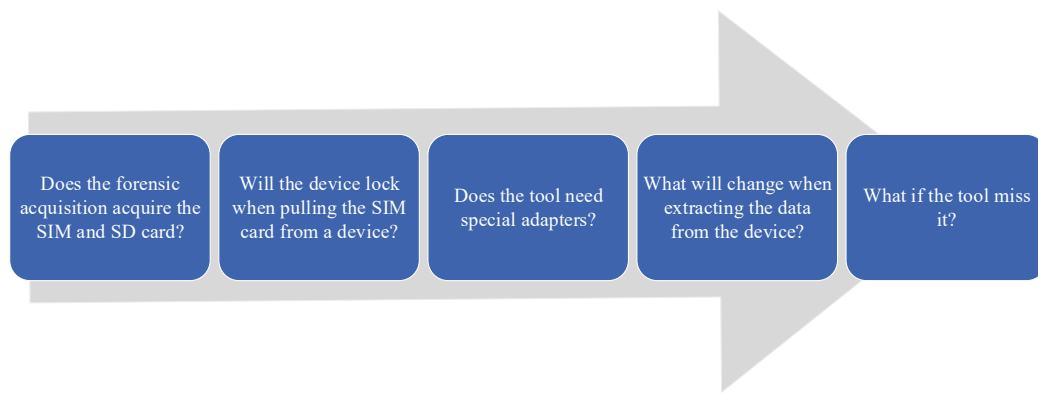


Figure 2.4 Smartphone Component Consideration

Forensic is the application of scientific knowledge to legal problems that are broadly linked to Locard's exchange principle, “every contact leaves a trace” [47][48]. In addition, there are some handling issues with respect to the smartphone devices. These include:

- Many different manufacturers, models, and operating systems
- Mobile devices change constantly when they are switched on
- No write blocking solution for mobile devices
- Collection decisions can affect success
- Removing a SIM card may release the biometric lock
- Looking at it, the biometric lock may be removed
- Faraday solutions do not always work
- Expect the unexpected

There are many operating system platforms that used in smartphones devices such as iOS, Android, Window, BlackBerry and so on. According to the statistics of mobile

device users that mentioned in Chapter 1, Android platform is renowned and widely used in Myanmar.

2.9 Nature of Android Operating System

Android is a mobile operating system developed by Google, based on the modified version of Linux. Linux kernel contains all the low-level device drivers for the various hardware components of an Android device. Android Libraries include all the code that provides the main features of an Android OS. Among these main features, SQLite is a very interesting feature for Android forensics. Android runtime provides a set of core libraries that it includes Dalvik virtual machine or ART Android Runtime depend on Android versions [46]. Their application framework includes the higher-level services and exposes the various capabilities of the Android OS to application developers. It has two types of applications such as built-in system applications and third-party applications. Figure 2.5 illustrates the architecture of Android operating system and Figure 2.6 demonstrates the nature of Android partitions.

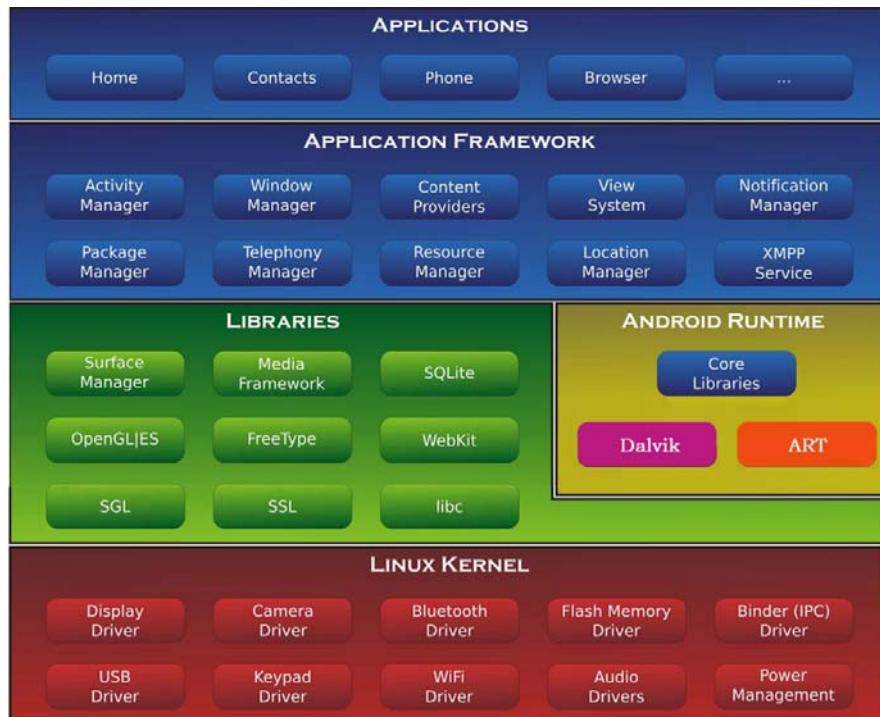


Figure 2.5 Architecture of Android Operating System [44]

Android flash storage is split into several partitions, such as */boot* contains the kernel and the ram disk, */system* for the operating system itself, */recovery* for performing

advanced recovery and maintenance operations on it, */cache* where Android stores frequently accessed data and app components, */Misc* contains miscellaneous system settings in form of on/off switches and */data* for user data and application installations.



Figure 2.6 Android Partitions

2.10 Android Mobile Device Forensic

After studying and analyzing the fundamental of digital forensics process, the emphasis will be on the process of Android forensic in this section. NIST provides basic information on mobile forensics tools and five stages for investigation process. These processes are:

- Preservation
- Acquisition
- Examination
- Analysis
- Reporting

Recently, many researchers have proposed the Android forensic process flow to increase the simplicity and user friendly in different perspectives. However, some of the process flows are complex and some are incomplete as the rapidly growth of technology. Thus, the optimal one is still necessary to implement in the Android forensic process. This research proposed a desirable Android forensic process flow in Myanmar and also proposed a framework which is technically supported the proposed process flow. Moreover, most of the mobile device forensic tools are commercial and expensive to use for developing countries like Myanmar. Therefore, this study also proposed an Android forensic tool for Myanmar based on this proposed framework.

2.11 Commercial Mobile Device Forensic Tools

There are many commercial mobile device forensic tools which are widely used to get the useful evidence from Android smartphones [9][12][42]. They are:

2.11.1 OSAF

The OSAF toolkit is built from Ubuntu 11.10 and pre-compiled with all of the tools needed to rip apart applications for code review and malware analysis. The primary goal with the toolkit is to be able to make application analysis as easy as possible. It also pretends to create a community where security professionals, analysts, developers and new commers can learn, discuss and share methodologies with one another.

2.11.2 Oxygen

Oxygen forensic suite is the only smart phone forensics software that allows analyzing applications in such a deep and structured way. It is very easy to use and it has a user-friendly interface to search, browse, filter and analyze the extracted data. It retrieves numerous application data from a mobile device. In application section, experts view the list of pre-installed and user applications with files created by these programs. Each application can contain valuable user data, like password, logs, history, files and so on.

2.11.3 Autopsy

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Installation is easy and wizards guide you through every step. Autopsy is a convenient tool for analysis of the computers running Windows OS and mobile devices running Android operating system. It has a graphical interface. The tool can be used for investigation of computer-related cases.

2.11.4 XRY

XRY is designed to recover the contents of a device in a forensic manner so that the contents of the data can be relied upon by the user. Typically, it is used in civil and criminal investigations, intelligence operations, data compliance and electronic discovery cases. It is available to law enforcement, military and intelligence agencies. The XRY system allows for both logical examinations (direct communication with the

device operating system) and also physical examinations (bypassing the operating system and dumping available memory).

2.11.5 Andriller

Andriller is a software utility with a collection of forensic tools for smartphones and cross-platform application for Microsoft Windows and Ubuntu Linux. It performs read-only, forensically sound, non-destructive acquisition from Android devices. It has features, such as powerful Lock screen cracking for Pattern, PIN code, or Password. This software also provides the custom decoders for Apps data from Android (some Apple iOS & Windows) databases for decoding communications. Extraction and decoders produce reports in HTML and Excel formats.

2.11.6 UFED

UFED mobile forensic tool provides all-in-one mobile forensic solution by adding flexibility and convenience to investigations process that unrivaled support for Android, iOS, and BlackBerry devices. The UFED extracts mobile device data directly such as decrypt, parse and analyze phonebook contacts, all types of multimedia content, SMS, MMS messages, call log etc. onto an SD card or USB flash drive. This tool aims to use by state and local law enforcement, intelligence agencies, military branches, corporate security and investigation, law firms and private digital forensic examiners.

2.11.7 MOBILedit

MOBILedit Forensic investigates the mobile phones using the classic forensic tool that started it all. It retrieves the data from a phone with a few clicks and generate forensic reports to make ready for the courtroom relied upon by the US Military, FBI, and CIA. This data includes call history, phonebook, text and multimedia messages, files, calendars, notes, reminders, firmware, including SIM details and location area information. MOBILedit Forensic is also able to bypass the passcode, PIN and phone backup encryption.

2.12 The Literature Reviews

This section will briefly explain about the literature reviews of mobile device forensics, Android forensics process flow and frameworks and supporting tool suites.

2.12.1 Mobile Device Forensics

The study carried out by [5] have given the detailed analysis on various data acquisition methods in the mobile forensics. They found that if the data needs to recover for quick analysis, logical or manual acquisition technique is desirable. However, in case of damaged phones and if the detailed analysis is required, physical acquisition technique is more suitable though they are time consuming.

In another research [15] proposed a layered architecture for mobile forensics analysis to help the investigators as easy as possible. It is composed of seven layers including: preparing, detecting the crime scene, seizure and preservation, extracting the data, examining, reporting and documenting. They analyzed to acquire data using different forensic tool suite such as Bulk extractor and MOBILedit.

In [43], the authors introduced a new framework to validate the mobile forensics data to make the investigation process. Their framework was mainly focused upon iOS applications and they performed the data gathering process on iOS devices. Afterwards, these extracted data are transferred into a laptop to make the validation process.

In [13], the examination and analysis of mobile phones is evaluated by obtaining the data from mobile phones through a simple application. In their study, they investigated and analyzed the evidence on Android smartphones using Oxygen Forensic and MOBILedit programs. According to the extracted information; live analysis can damage the evidence and is not recommended for judicial process. They stated that selecting a program that perform on the dump is more important. Also, they suggested that the correctness and diversity of the findings must be revealed by using different programs. Based on their analysis, they observed that the MOBILedit program performed faster and Oxygen Forensics superior to MOBILedit program in terms of dump analysis, social graph, and Wireless Security Protocol.

Authors in [37] analyzed the logical and physical acquisition techniques for investigators and explored a better approach to acquire the important evidence from mobile devices. They carried out the investigation on Samsung Galaxy Grand Duos GT-I9082 smartphone having Android operating system. They extracted the evidence data using AFLogical OSE, Andriller and Wondershare Dr.Fone programs. From the

results obtained, AFlogical OSE is purely based on logical acquisition technique and could recover the undeleted message and call logs from device. Andriller was able to retrieve the undeleted data including the Wi-Fi password, account information and browser history. However, it failed to recover multimedia data. Wondershare Dr.Fone program could extract the deleted and undeleted data with the use of both logical and physical acquisition technique. They concluded that there is no single tool can provide complete evidences from device, thus more than one tool can provide the better insights to help the forensic investigators.

H. Alatawi et al. reviewed the mobile forensics that contains four digital forensics processes such as collection, examination, analysis and reporting. They discussed to extract the evidence data not only from the device itself, but also from other related sources such as platform (personal settings, network information and device IDs), application's data, calls and SMS, audio and image capture, positioning, local and personal networking, mobile telecom, and backup. They presented five data extraction methods with level, advantages, disadvantages and tools. Moreover, they compared the Android malware detection techniques such as N-gram, Decision Tree, Random Forest and so on. [4]

2.12.2 Process Model and Framework for Android Forensics

In [1], R. Ahmed et.al. introduced a well-organized forensics framework for extracting and documenting the evidence from Android platform devices. By using the hashing algorithm, the attempt was brought off the comprehensive and reliable evidences with a high integrity verification. In their framework contained two main processes: extracting the evidence and preparing documentation.

In another study [29], the authors proposed a smartphone investigation scheme focusing on ad hoc acquisition of evidence from device. Their scheme contained six phases: engagement in investigation, choose evidence type, collect the evidence, transmit the evidence, store the evidence and conclude the investigation. It was applicable in inspection of the technological aspects of proactive smartphone forensics.

The author in [41] introduced a common process for acquisition data of Android devices. They suggested that their process was useful in recovering the partition and accompanying recovery mode of Android device for data gathering purposes. The authors in [39] proposed an efficient investigation method for acquiring data and analyzing on Android smartphones. In their method, they considered the issues for-

instance adaptation of the method, structuring for data storage purposes, questioning for what conditions the device is sent to forensic examiners. It contained only two investigation phases: acquisition and examination.

In [32], a common process model was constructed to lead the forensic examiners during conducting a required investigation process on Android device. Their model composed of four main processes: pre-incidence readiness, collecting the evidence, examining and analyzing, and information diffusion. However, their model lacked real application to an actual scenario.

In another project [31], an investigation framework was conducted to apply on Samsung Star 3G smartphone. It has six phases: authorization, first response, device transportation, live acquisition, maintenance, and analysis of the evidence. Their framework was practical and some processes were applicable to other phones and portable devices. They suggested to be used the aluminum foil in the transportation process. Their experimental results showed that the material was completely efficient in the protection of signal.

The authors in [22] proposed an efficient method to collect and analyze the thumbnails from Android devices. Their proposed model consisted of four main processes: identifying, preserving, analyzing, and presenting. They evaluated their proposed model with case study. They identified the thumbnail characteristics to customize the existing file craving tools to recover the thumbnails from the forensic image by decreasing the number of irrelevant files.

In [26], a methodology was constructed to collect evidence data from Android devices. Their proposed method has five stages: identifying the device and preserving the evidence; collecting the evidence; examining and analyzing; and reporting and presentation. Their methodology attempted to make minimum possible changes on suspected device. After identifying the device, they do the preservation techniques. Then, the initial technique is set up the device to bring up a live acquisition from volatile memory of the device.

2.12.3 Tools for Android Forensics

In [34], the forensic analysis in all kinds of memory areas in Android smartphone devices were presented. They also investigated the analysis of call log, messaging, contact information, audio, video and images to provide more evidence data

to analyst in investigation. However, their proposed work could not extract and recover the deleted contacts, messages and data of specific application including volatile data.

One study [38] was proposed to find all the artifacts that produced by private chat, secret chat, hidden chat from social messenger application. According to their investigation of Android forensics and analysis, investigators were able to read, reconstruct and present the chronology of messages. Furthermore, they evaluated on two different smartphone brands and different Android versions to take out the evidence in forensically sound manner.

N. A. Aziz et al. [10] used the Sleuth Kit Autopsy to extract and analyze the data in Android smartphones. They found the valuable information in phone contacts, calendar, messages and images as digital evidence in forensics investigation. Their study pointed out the dd command for imaging and mount in ADB utility. Furthermore, they also explained with case study to know how can be related in different data types.

ADB command utility tool and some open-source tools are presented to express how to forensically recover data from Android devices [18]. Their work demonstrated DB Browser for SQL Lite for database file analysis, Andriller tool for unlock pattern, NowSecure Forensics tool for logical acquisition of data and some tools for other processes.

V. V. Rao et al. [33] surveyed the Android forensics tools and highlight state-of-the-art techniques available in the market. They explained the methods of logical and physical acquisition and analysis. Furthermore, they investigated the comparison of their features such as SAFT, AFLogical, LiME Module, android Backups, OSAF-TK (Open-source Android Forensics Tool Kit), Santoku Linux, WhatsappXtract and Andriller.

In [35], Different tools and techniques that used in Android based smartphones have analyzed. Their survey was focused on the manual acquisition, physical and logical acquisition of data from mobile device. They also examined the characteristics like free or proprietary, number of devices and non-android platforms where these tools can support. In [16], smartphone forensics model for window mobile device has reported. They implemented with twelve stages and compare with other investigation models. However, they only emphasize on the specific information flow of forensics investigation for Windows mobile devices.

ANDROPHSY forensic framework system [2] was suggested. In their work, the first step is to create a case for incident. Every user is assigned as a role such as

administrator, analyst and investigator. Their system also employed the forensics investigation process as NIST. It includes data collection, examination, analysis and reporting. The low-level Linux and Android built-in forensics functionalities like dd and adb command were utilized. The process of digitally investigating on Android smartphones has demonstrated and built up a framework for investigation [3]. There were nine steps of evidence data extraction process in their framework. Moreover, they also recommended the ADB tool for forensics case and Lowmanio Foreman tool for other management case.

In [14], the rooting process with SRS tool on Samsung S3 phone was investigated. They created an image of phone partition with .dd file and extracted the messages for Viber on trial version of UFED Physical analyzer. In [26], the major contribution is an in-depth evidence collection and analysis methodology for forensic practitioners. Their methodology based on four phased of cloud forensic framework. The first phase was Identification and Preservation. Second phase was setup Bootloader and setup for Live OS in memory to collect physical image of device partitions. Third phase was examination and analysis the application files in private and external storage, application databases, account data and analyze application.

In 2014, NIST rendered the necessary information on mobile forensics tools and five stages for investigation process [8]. These were preservation, acquisition, examination, analysis and reporting. Most of the researches based on these NIST guidelines in forensics investigation process for future improvement. In [28], the harmonized digital forensic investigation was introduced for mobile devices including three groups of processes. These were initialization with four stages, acquisition with five stages and investigation with six stages. Also, they encouraged the XRY complete package for forensics process, Faraday bag for packaging, subscriber identity module (SIM) identity-cloner and other requirement materials.

A. Mahajan et al. presented the forensics data analysis in instant messenger applications: Viber and WhatsApp [25]. They investigated in five Android phones with three different versions, named, Froyo, Gingerbread and Ice-Cream Sandwich. They extracted all folders and files from device and analyzed the artifact data using Universal Forensic Extraction Device (UFED). In [7], The social networking applications forensics was enforced on Facebook and WhatsApp applications. In their study, they followed the guideline of NIST process flow for investigation. Furthermore, they utilized the FTK imager to analyze on all types of information for the artifacts data.

They proved that their results provide to reconstruct the list of contacts and chronology of messages that have been exchanged by users.

M. R. Boueiz emphasized the importance of rooting process in Android data acquisition. It tested the Samsung device (v6.0.1) on Microsoft Windows 10 Enterprise Edition and Kali Linux (v2019.4) [11]. The author recommended Dr. Fone Tool for rooting process. Moreover, Autopsy and DB browser SQLite tool is suggested for analysis process.

H. F. Tayeb and C. Varol reviewed the android mobile device forensics that includes five steps of digital forensics (Identification, Preservation, Acquisition, Examination and Analysis, and Presentation), three acquisition methods (File System Acquisition, Memory Acquisition and Environmental Acquisition) and forensics tools (AccessData Forensics Tool Kit - FTK, Joint Test Action Group - JTAG, Cellebrite UFED, AFLogical, etc.) [40]

T. Almeahmadi and O. Batarf presented the effect of android devices rooting on user data integrity in android forensics. They compared three data acquisition methods by using Samsung Galaxy S4 device on Microsoft Windows 10. First method used the ADB backup command for data acquisition. Second method used the Custom Recovery Image and MicroSD for data acquisition. The last one used the KingoRoot tool for rooting process. The Belkasoft tool and dd command utility is applied for data acquisition. They discussed that no data changes occurred during data extraction or during the rooting process [6].

2.13 Comparative Study of Android Forensics Tool Suites

Based on the literature, this section is a comparative study of several Android forensic tool suites that offer both open source and commercial tools. The first example described a test environment and some open-source tools: Now Secure, ADB, Autopsy, SQLite for Android forensics. These tools were then evaluated during the acquisition and analysis process. The NowSecure program can perform both the acquisition and analysis process. However, the free version can only extract data. According to the summary results, ADB, Autopsy and SQLite Browser are superior to NowSecure tools in the data extraction process. Table 2.1 summarizes a comparative study of several open-source tools for Android forensics [27].

Table 2.1 Comparative Study of Some Open-Source Tools for Android Forensics

Testing Environment	Tools and Methodology
Alcatel One Touch 6012x (v4.2.2)	SRDIFM (11 phases)
	adb pull, dd, SQLite and Hexeditor
Intel Pentium 3558U 4GB RAM Windows 7, SP 1 (32 bits)	Andriller tool for decode pattern
	Kingroot for device root access
	Autopsy, AF Logical OSE and Now Secure Forensic tools

Program	Acquisition	Analysis
NowSecure	Yes	Yes
ADB (pull, dd)	Yes	No
Autopsy	No	Yes
SQLite Browser	No	Yes

Moreover, a comparative evaluation of mobile forensic tools was conducted. In [30], the author evaluated several commercial tools on Samsung Galaxy and HTC Desire smartphones. Then, the differences of their abilities were summarized in Tables 2.2 and 2.3. However, the commercial version is a trial version and free mode. In addition, their analysis focused only on data recovery of deleted files.

Table 2.2 Evaluation on Samsung Galaxy (GT-S5300) v2.3.6

Evidence Data	MOBILedit	FTK Imager	Oxygen	Encase
Pictures	No	Yes	No	Yes
Contacts	No	No	No	No
SMS	No	No	No	No
Applications	Yes	No	No	No
Audios	No	Yes	No	Yes
Videos	No	Yes	No	Yes
Web Browser History	Yes	No	No	No
Call logs	No	No	No	No

Table 2.3 Evaluation on HTC Desire 300 v4.1.2

Evidence Data	MOBILedit	FTK Imager	Oxygen	Encase
Pictures	No	Yes	No	Yes
Contacts	No	No	No	No
SMS	No	No	No	No
Applications	No	No	No	No
Audios	No	Yes	No	Yes
Videos	No	Yes	No	Yes
Web Browser History	No	No	No	No
Call logs	No	No	No	No

2.14 Summary

In this chapter, the concept of cyber-attacks and the nature of digital forensics were presented. With the growth of smartphone technology in everyday life, the need for mobile device forensics was highlighted. After studying and analyzing the fundamental of digital forensics, the Android forensics process was emphasized and several commercial mobile device forensics tools such as OSAF, Oxygen, Autopsy, Andriller, UFED etc. were discussed. Although there are many mobile device forensics tools in market, but they are commercial and expensive to use in developing countries like Myanmar. Moreover, the previous related work of process model, framework and tools for Android forensics were reviewed. According to the literature reviews of previous studies on Android forensic, there is no research on Android forensics tool for Myanmar, depending on the desired process flow and framework for the home country. Especially, there is no precise cyber laws and procedures in Myanmar in present time. In addition, a comparative evaluation of mobile forensic tools was conducted. In the next chapter, the proposed methodology of this research will be discussed in detail.

CHAPTER III

THE PROPOSED METHODOLOGY

This chapter has proposed android forensics process flow, analysis framework and android forensics tool (ANDROSICS). According to the description in chapter 2, both the nature of android and forensics that proposed to the android forensics process flow are studied. And then, this study based on the four main acquisition methods for analysis framework as shown in Figure 3.1. They are manual acquisition, volatile acquisition, physical acquisition, and logical acquisition.

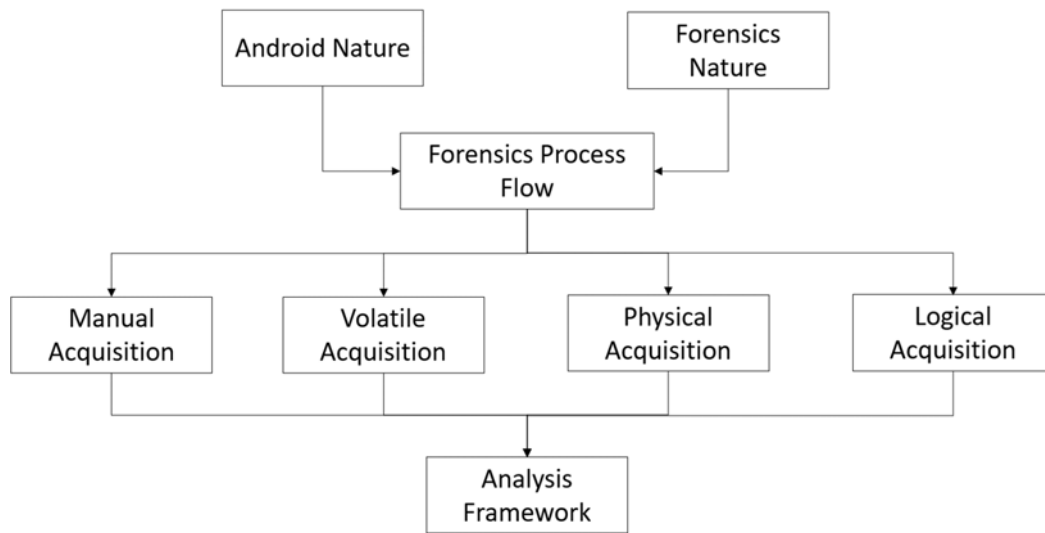


Figure 3.1 The Overview of Proposed Methodology

3.1 Process Flow for Mobile Device Forensics

According to the nature of forensics, this process flow is based on the standard forensics process models established by NIST and their four main stages are Collection, Examination, Analysis and Reporting. However, the proposed process flow has seven stages; they are Preparation, Determine Scope of Crime Scene, Secure Evidence Devices Collection, Documentation and Preservation, Examination and Analysis, Presentation, and Review. It is divided into three locations such as Crime Scene, Forensics Lab, and Court of Law, as shown in Figure 3.2. The investigation process can trace or loop to complete, and it supports update action for the preparation stage. Although this process flow emphasizes the android forensics investigation, it can also be flexible for other digital forensics investigation.

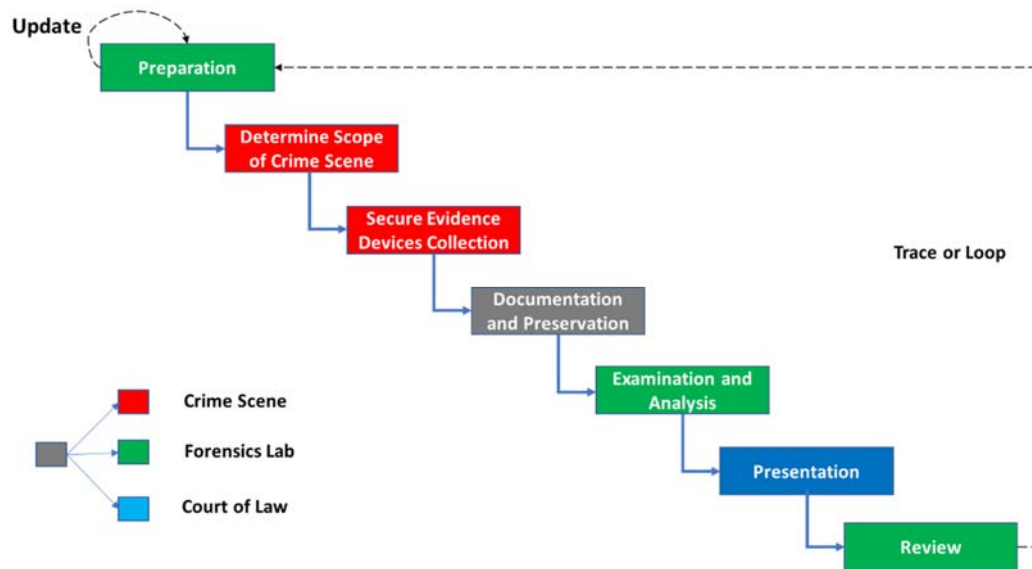


Figure 3.2 Proposed Process Flow for Android Forensics in Cybercrime Investigation

3.1.1 Preparation

The first stage needs to prepare the three main things – (i) Human resource, (ii) Plans and Procedures (iii) Techniques and Tools. Forensics lab always needs to prepare and develop these three important things for improving the forensic investigation process.

- (i) Human resource: It requires to build a forensics team, and all members must have strong knowledge and skills depending on their responsibilities. Knowledge is well understanding the nature of crimes, criminal activities and android technology. They ever need to learn and practice for their skills because android smartphone technology is rapidly growing and changing in every year with various models, accessories, features, firmware version, and so on. Forensics lab can train to their members by using sample scenario based on previous crimes and sharing about the latest technologies and experiences.
- (ii) Plans and Procedures: Forensics lab has to create various plans and procedures depending on the types of crimes. It can help to minimize the loss of evidence data and the risk for the future investigation process.
- (iii) Tools and Techniques: It includes hardware devices, software tools and materials. They can provide to perform the investigation process from beginning to finish the criminal case. The technical expected requirements in preparation are indicated in Table 3.1.

Table 3.1 Technical Expected Requirements in Preparation

Types	Description
Hardware	High Performance Personal Computer or Laptop for investigation process, Android devices for testing, other Forensics tools (Example: Write Blocker)
Software	Operating Systems (Linux, Windows and others), Android Debug Bridge utility, USB drivers, Reliable Root tools and Forensics tools (Example: Androsics)
Material	Power Bank, USB cable, OTG (on the go) devices, Packaging Bags (Example: Faraday) and other accessories

3.1.2 Determine Scope of Crime Scene

Crime scene investigator is an essential person in this second stage. He needs to define the crime scene area to prevent the access of unauthorized person and to collect the suspected things. If it is not restricted, the suspected devices can be destroyed or lost before the analysis process. And mobile devices can be easy to take and hide because they are very portable and smaller than other digital devices. Moreover, everyone knew how to switch off the device power or factory reset. It can be lost the volatile data on memory of mobile devices.

3.1.3 Secure Evidence Devices Collection

The third stage is especially not to lose volatile data when an investigator is collecting the suspected mobile devices. Because the volatile data can be easily lost and difficult to keep. If devices display is active mode, it needs to consider the main four situations – (i) Check the battery status and if the battery percentage is under twenty, it needs to recharge the device immediately. (ii) If the device is connected with the laptop or PC, it needs to check any mobile related process is running on it. The investigator needs to consider to kill the process or wait to finish depending on types of operation. (iii) Criminal can use the anti-forensics applications to control their devices that can run malicious activities (e.g., at least power shutdown or restart the device and wipe data) via SMS messaging, Phone calling, Bluetooth, Data Network and Wireless. Therefore, the investigator needs to consider to prevent any external control to suspected devices with Airplane mode enabled or using a Faraday bag. The suspected

devices need to isolate from any communications. (iv) If the device screen lock is free, the investigator needs to change some settings for control access. They are enabled USB debugging with MTP mode, increase screen timeout, maximum times to lock automatically (under Jelly Bean version is not supported), disabled the lock instantly with power key (above lollipop version), enabled the stay awake feature and set the maximum screen timeout as shown in Figure 3.3.

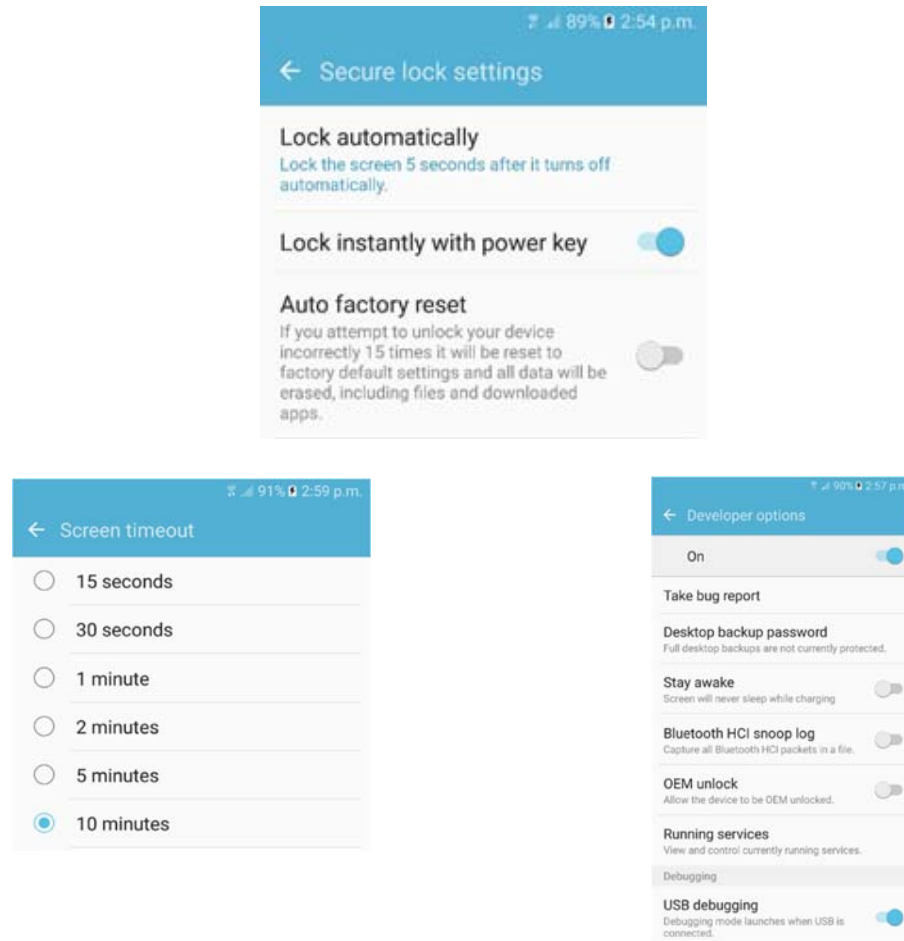


Figure 3.3 Changing Settings for Control Access

3.1.4 Documentation and Preservation

This stage is recording all activities of the investigation process and labelling the suspected devices to provide the second stage. This record contains taking the photos or videos, locations and crime scene mapping, circumstances surrounding the incident, people list, existing states of evidence devices, and so on. Moreover, the

investigator needs to check again that collected devices are ready to transport to the forensic laboratory.

3.1.5 Examination and Analysis

Forensics laboratory plays a significant part in this stage that comprises the data collection process (volatile data and imaging data), brute force process, analysis process, and so on. It can generate various reports based on data types such as case summary, device profiles, applications data, call logs, phone contacts, SMS, and so on.

3.1.6 Presentation

After finishing all of the analysis processes, it needs to build a chain of custody document based on the reports for presenting to the court of law. In this stage, the investigator can use the evidence data and devices that includes photos, videos, documents, logs with timestamp and others.

3.1.7 Review

After completing every presentation stage, it needs to do the review on the entire forensics investigation process whether a trial is finished or not. The reviews will be useful that it can provide to prepare future investigations process and it can help the forensics team to do studying, discussing, training and so on.

3.2 Analysis Framework for Android Forensics Investigation

This framework performs the Examine and Analysis phase in the proposed process flow. With the rapidly growth of technology, the preparation process should be updated over time. The update process in Preparation stage is also supported in proposed framework. According to digital forensics nature, this framework provides Static forensics and Live forensics methods. Firstly, it needs to consider the device's power is on or off when the forensics lab received the suspected devices from a crime scene investigator, as shown in Figure 3.4. If the devices' power is on, it performs the Live forensics process. If the device's power is off, it has to do the Static forensics process.

power key (above lollipop version). Investigator needs to enable all of them for investigator process. After enabled the required accesses, he can extract the current status (last used applications on the screen, notifications), volatile data (dumpsys logs, logcat, etc.) and backup. Also, he needs to check the device is already rooted. If the device is rooted, he can run the imaging process for all partitions of the device (logical or physical). Afterwards, he can examine and analyze all artefacts data from image files for reporting. If the device is not rooted, the investigator needs to run the rooting process. However, if the policy is not allowed, he cannot. Even though the policy is allowed to rooting process on the device, he has to check the compatible root tool depending on the device model and android version. If the root tool is ready, he can continue to root the device, imaging process, examine and analysis process, and reporting process, as shown in Figure 4.3.1. If the root tool is not ready, it cannot do the imaging process, and he continues to examine and analysis process, and the reporting process.

(ii) Device screen lock is active mode

In this situation, the investigator has to check the USB debugging access and RSA key access first. If he had both two accesses, he could run all processes same as the inactive mode. If at least one access is disabled, it needs to consider bypass screen policy that is allowed or not to remove or decode the screen lock (pattern, pin and password). If it is not allowed, it will go to the SD imaging and SIM card information same as the power unavailable situation of Static Forensics. If it is allowed, it needs to check root access. If the device is already rooted, the investigator can bypass the screen lock and enable to all required accesses. And then, he can collect all artefacts data including current status, dump data, backup and imaging files. Then, he can examine and analyze the collected data for reporting. If the device is not rooted, he needs to check two processes that root policy, whether is allowed or not and root tool is available or not. If he can run both of these two processes, he has to root the device and continues to 'enabled require accesses' until the last process. If any process is unavailable, it will do procedures the same as the power unavailable situation of Static Forensics.

3.3 Proposed ANDROSICS Tool Suite

This proposed ANDROSICS tool supports five main categories for android forensics (Live performing process and Dead performing process) in cybercrime investigation process. They are Data Collection, Examination and Analysis, Brute

Forcing, Reporting and Managing. This tool also provides some useful features that is forensically sound conditions for investigation process. Figure 3.5 describes the detail features of proposed ANDROSICS tool suite for Android forensics in cyber-crime investigation.

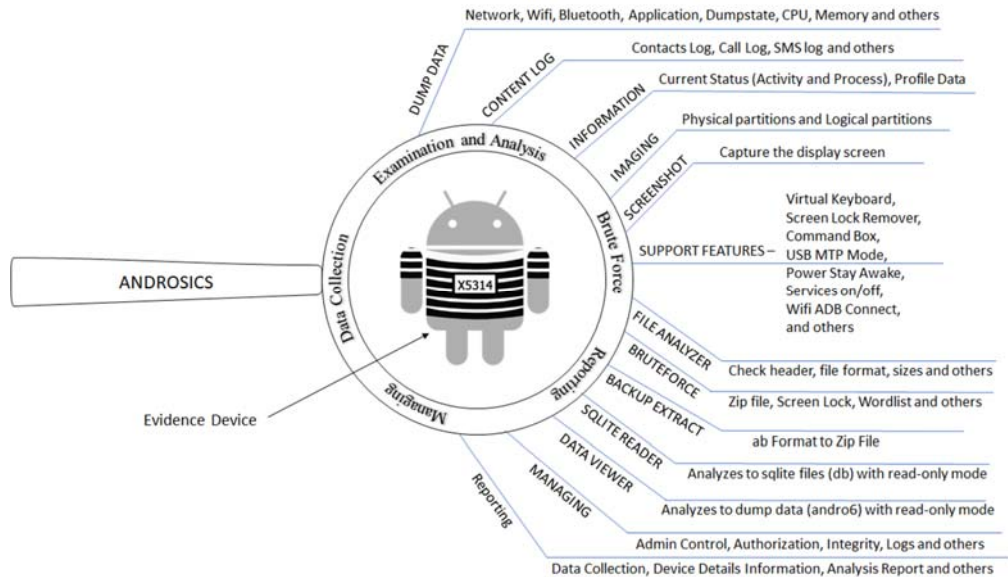


Figure 3.5 Features of Proposed ANDROSICS Tool for Android Forensics in Cybercrime Investigation

They are (1) Data Collection, (2) Examination and Analysis, (3) Brute Forcing, (4) Reporting and (5) Managing. This tool also provides some useful features that are forensically sound conditions for the investigation process.

3.3.1 Data Collection Process

The data collection process will extract various artefact data with four types of file extension, as shown in Table 3.2.

Table 3.2 Four type of file formats from Data Collection Process

File Extension	PNG	AB	ANDRO6	IMG
Data Collection Process	Screenshot	Backup	Dump Data on Memory	Imaging to Logical and Physical partitions

- Screenshot
- Profile Data
- Backup
- Dump system services (E.g., Activity, Network, Wi-Fi, Bluetooth, Memory, and etc.)
- Contact Log
- Call Log
- SMS log
- Recent Uninstall Applications Log
- Logcat
- Dumpstate
- CPU Process
- Property Information
- Imaging Partitions (Logical and Physical)

Screenshot: This feature provides to receive current device display screen information for forensics lab that contains SIM card information, battery percentage, notification bar enabled information and notification messages. Moreover, the investigator can capture any display screen while he is doing data collection.

Profile Data: It means the device profile data such as Manufacturer, Model, Version, Operator, Country, Baseband, IMEI, Device ID, Serial Number and Phone Number.

Backup: It provides the backup of entire logical data from device to an encrypted file including applications (apk), applications data and phone storage data. The extension of the encrypted file is *.ab, and the investigator can provide a password to secure it before starting the backup process. This feature is pretty simple because it does not need the root access.

Dump System Service: This feature uses a dumphsys tool that can extract interesting information about the system services for android forensics. Investigator can get volatile data from this dump system service information. According to the result of testing, it has 251 services on Samsung Galaxy J7 Prime as shown in Figure 3.6. Androsics tool provides to collect all services and interesting services with option such

as Activity, Network, Network dump, Wi-Fi, Wi-Fi History, Bluetooth History, Memory, CPU, Process, Account and Application.

```
DUMP OF SERVICE AAS:
DUMP OF SERVICE AODManagerService:
DUMP OF SERVICE CCM:
DUMP OF SERVICE CustomFrequencyManagerService:
DUMP OF SERVICE DeviceRootKeyService:
DUMP OF SERVICE DirEncryptService:
DUMP OF SERVICE DisplaySolution:
DUMP OF SERVICE DmfManagerService:
DUMP OF SERVICE DockObserver:
DUMP OF SERVICE EngineeringModeService:
DUMP OF SERVICE Exynos.HWCService:
DUMP OF SERVICE FMPlayer:
DUMP OF SERVICE IextSDUFSServiceVold.unionFSStackServiceVold:
Error dumping service info: (Unknown error -2147483646) IextSDUFSServiceVold.unionFSStackServiceVold
DUMP OF SERVICE MultiScreen:
DUMP OF SERVICE OcfKeyService:
DUMP OF SERVICE ReactiveService:
DUMP OF SERVICE SEAMService:
DUMP OF SERVICE SamsungKeyProvisioningManagerService:
DUMP OF SERVICE SatsService:
DUMP OF SERVICE SecExternalDisplayService:
DUMP OF SERVICE SemAuthnrService:
DUMP OF SERVICE SurfaceFlinger:
DUMP OF SERVICE SveService:
Error dumping service info: (Unknown error -1) SveService
DUMP OF SERVICE VaultKeeperService:
DUMP OF SERVICE accessibility:
DUMP OF SERVICE account:
DUMP OF SERVICE activity:
DUMP OF SERVICE alarm:
DUMP OF SERVICE android.security.keystore:
Can't find service: android.service.gatekeeper.IGateKeeperService
DUMP OF SERVICE apn_settings_policy:
DUMP OF SERVICE application_policy:
DUMP OF SERVICE appops:
```

Figure 3.6 Dump System Service List

Contact, Call and SMS log: This feature provides phone contact log, call log and SMS log with detail information. The investigator can extract the contact and call log information without having root access. However, SMS log is needed to be root access that is depending on the device brands or models.

Recent Uninstall Applications log: Sometimes, criminals may delete the application before they arrested. After deleting the application, if the device is still in a live situation, the investigator can check the deleted applications log with this feature. This data helps the investigation process, and it can be evidence data.

Logcat: This feature provides the mechanism to collect and view the system debug output. The logs of various system or third-party applications and portions are collected in the series of circular buffers.

Dumpstate: The dumpstate feature is the detailed log information of memory, virtual memory and uptime/sleep time that dumps state to a file.

CPU process: The CPU process feature is to display the top CPU process providing information about Process ID, CPU Usage, running/sleeping state, and so on.

Property Information: This feature is the property system information of android. This is fascinating data for android forensics.

Imaging Process: This feature does the Bit-by-bit copy from all partitions of android devices and SD card. It replicates all sectors that contain logically bad sectors and blank sectors. Otherwise, it can call the sector-by-sector clone.

3.3.2 Examination and Analysis

In this portion, it has four main features – (i) Data Viewer, (ii) Backup File (.ab) to Zip File Format (iii) File Type Analyzer and (iv) SQLite Reader.

(i) Data Viewer

According to Table 3.2, all dump data are encrypted with the Andro6 file format in the data collection process. With the use of this feature can decrypt and view all Andro6 file format. Additionally, it provides the searching words feature that investigator can search specific terms, and it will help to the analysis process.

(ii) Backup File Extractor

This feature provides to convert from backup file (*.ab) extension to (.tar) file extension. The investigator can extract the tar file for the analyzing process. If the encrypted backup file is locked with the password, he needs the password to decrypt for converting.

(iii) File Type Analyzer

Sometimes criminal can change the file signature for their sensitive data. In this case, the investigator cannot easy to know that the file is corrupted or not. This file type analyzer can provide to analyze this problem, as shown in Table 3.3. In the overview of file type analysis, it generates four statuses based on the file signature and execution process. The investigator can be easy to know file execution process. If he can read the file when he launches it, this is True, and if he cannot read, this is False. But he cannot be easy to know file signature is right or not. In this case, this feature will provide to analyze the file signature. This feature will be explored more detail in Chapter 4.

Table 3.3 The Overview of File Type Analysis

File Signature	Execution	Status
True	True	True Positive
True	False	True Negative
False	True	False Positive
False	False	False Negative

(iv) SQLite Reader

Most android applications used the SQLite database to store their data. In this case, this feature can read SQLite database file with read-only mode and investigator can export the data with pdf file for reporting. If SQLite Reader provides the modify access, the evidence data can be changed.

(v) PNG Manipulation

In photo images, PNG format is one of the best ways to manipulate with files. When the dimension of PNG file is manipulated, Androsics tool provides the feature to recover the correct one. This feature needs to know, where is the width and height of PNG located and is it compatible with the crc checksum to verify the dimension as described in Figure 3.7. Even the crc checksum is also deleted, androsics tool can handle with the Force Generated Files feature. Generally, the investigator has to define the minimum and maximum width/height and generate the output image files. After that, he can look for the suspected PNG files from them. When the investigator wants to get the interesting images quickly, it is recommended to set the minimum height to the maximum height only.

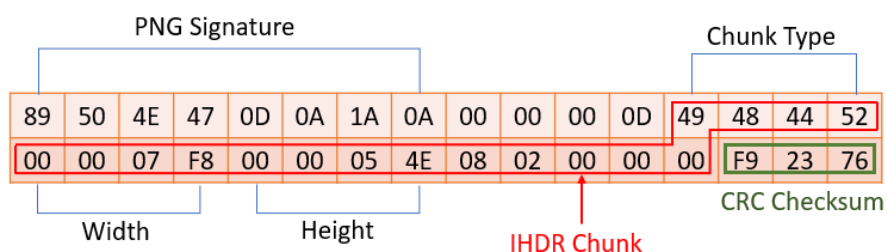


Figure 3.7 PNG Signature and Chunk

3.3.3 Brute Force

Nowadays, brute force process is a challenging task in the forensic investigation. Criminals can be encrypting the file with password for their sensitive data and their device with screen lock (pattern, pin or password). Sometimes, the device owner does not want to give their password to the investigator. In such kind of situation, this feature provides to get access to the files or devices.

3.3.4 Report

Reporting process provides both Live forensics and Static forensics. In Live forensics, it includes extracting the investigation summary, device information, data collection, device property information. In Static forensics, it provides various reporting files from File Analyzer feature and SQLite feature.

3.3.5 Management

The proposed ANDROSICS tool provides not only forensics investigation processes but also management processes. It is based on CIA triad (Confidentiality, Integrity and Availability).

- (i) User Management: Forensics laboratory can separate the admin level and user level for using this tool. Admin level can check all user activities log and can create or remove user accounts. Moreover, it can set the secret keyword to access for all users.
- (ii) Access Control Management: The login process has double-checked that contains *a secret keyword* like as temper protection and *username and password*. A secret keyword is limited to access with three times, and username and password are not limited. If a secret keyword is over three times, forensics camera or CCTV will capture the photo to the user logging in.
- (iii) Crime Case Management: The investigators can create crime cases when they received the suspected devices before the data collection process. In a crime case, it contains the case number, case name, owner name, investigator name, and department. The admin level can check case create list and case analysis list with the timestamp.
- (iv) Logs: It can be divided into two types: case access log and details log. Case access log recorded the information of case creation and analyzing. Details log

kept all user activities including login access, investigation processes and management processes, along with the timestamp.

3.3.6 Other provided features for Android Forensics

In this portion introduces some useful features supported by the ANDROSICS tool suite for Android forensics.

- Virtual keys (swipe lock, airplane mode, power button, etc.)
- Virtual keyboard (alphabetic characters, numbers, symbols, etc.)
- Screen lock remover (pattern, pin and password)
- Command box for ADB utility commands
- USB connected with MTP mode
- Power stays awake (Device screen will never sleep while charging)
- Services On/Off (Data Network, Wi-Fi and Bluetooth)
- Cryptography (encryption, decryption, encode, decode, hashing and hex dump)

3.4 Summary

This chapter discussed a seven-stage- proposed process model and analysis framework based on the standard four-stages forensic process model established by NIST. In addition, the ANDROSICS tool suite which supports five main categories: 1) data collection, 2) examination and analysis, 3) Brute forcing, 4) reporting and 5) management was highlighted. The detailed implementation and experimental setup of proposed ANDROSICS tool suite will demonstrate in the next chapter.

CHAPTER IV

IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed tool suite is based on the open-source tools, freeware tools, trial version of commercial tools, ADB utility tool and nature of the forensic investigation. This tool supports five main categories for android forensics (Live data acquisition process and Static performing process) in cybercrime investigation.

4.1 Testing Environment

Table 4.1 The Detailed Description of Testing Environment

Name	Description	
Host Machine	Intel® Core™ i5-5200U <u>CPU@2.20GHz</u> 12.00GB RAM Windows 10 Enterprise (64-bits)	
Software Tools	Android Debug Bridge Utility (ADB – v 1.0.31)	Android USB Driver (installer.exe) AdbWinApi.dll AdbWinUsbApi.dll Fastboot.exe
	Non-Commercial Tools	FTK imager, LiME, Volatility, and etc.
	ANDROSICS Tool Suite version 2.1.0 (Dark Mode)	Proposed Android Forensics Tool
	Bash on Ubuntu on Windows	Linux Based Terminal (Build-in)
Material	USB Cable OTG (on the go) devices Aluminium foil	
Android Devices	Huawei C8650+ Huawei C8825D Huawei G520-0200 & G510-0100 Honor H30-L02 Samsung Galaxy Tap 4 Samsung Galaxy J7 Prime	Version 2.3.6 (Gingerbread) Version 4.0.4 (Ice-cream sandwich) Version 4.1.1 (Jelly Bean) Version 4.4.2 (KitKat) Version 4.4.2 (KitKat) Version 6.0.1 to 8.1

4.1.1 USB Debugging Mode Preparation

There are many options to switch on the USB debugging mode based on the Android version. In the Gingerbread version, we need to go to Settings > Applications > Development and turn on USB debugging. From Ice-cream Sandwich to the Jelly Bean version, we have to enter Settings > Developer Options and finally turn on USB debugging as shown in Figure 4.1. From KiKat to the latest version, go to Settings > About Device, then go to Build Number by tapping 7 times, then go to Developer Options, and switch on USB Debugging mode as shown in Figure 4.2.

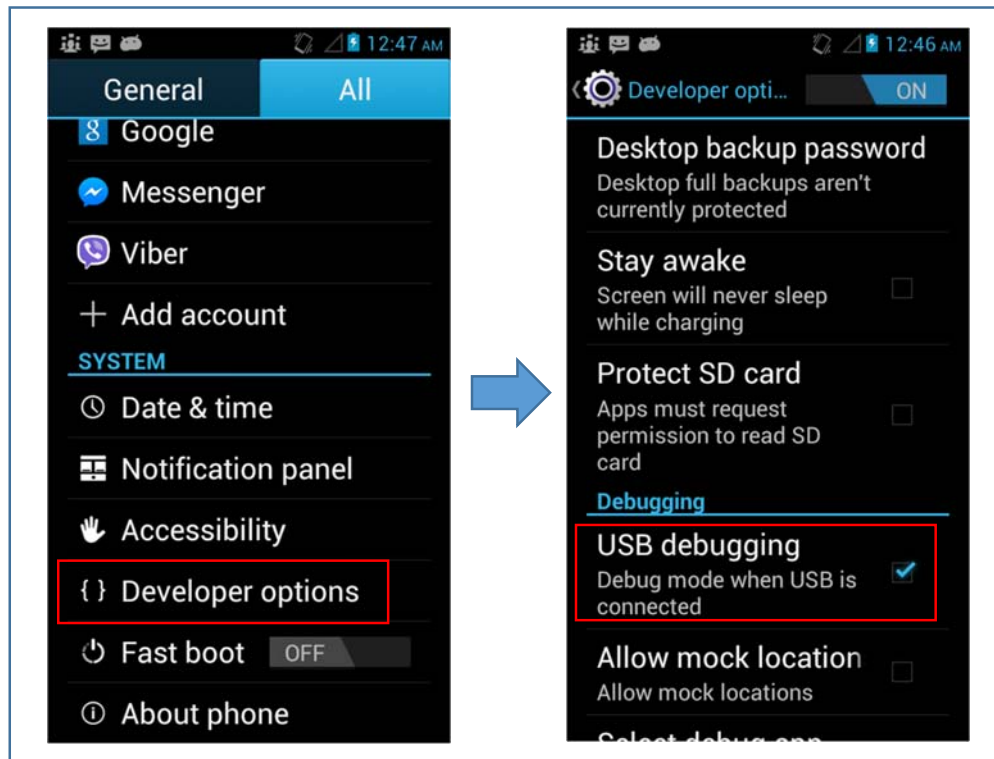


Figure 4.1 USB Debugging Mode Preparation in Jellybean Version

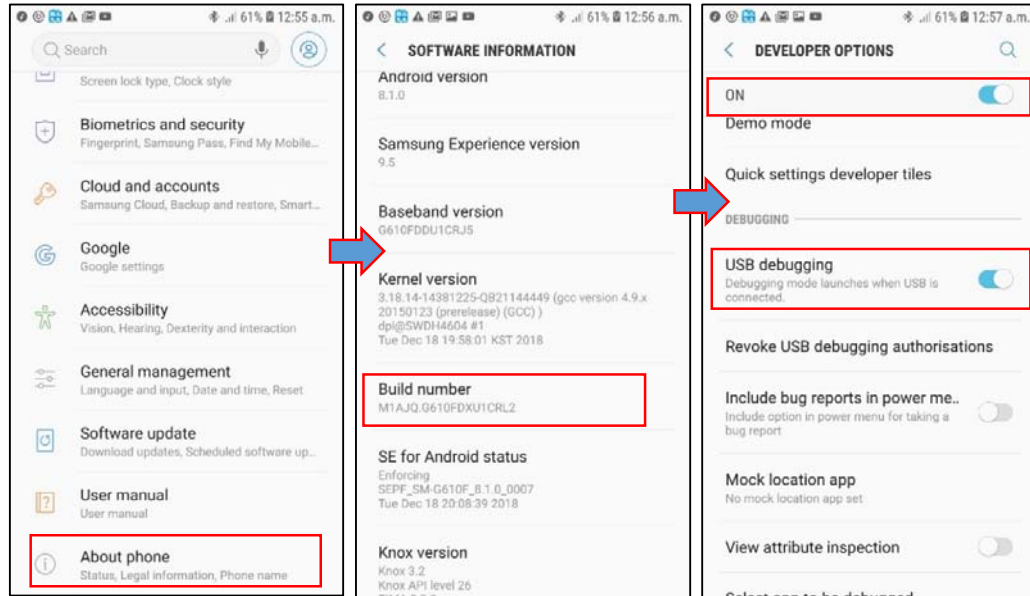


Figure 4.2 USB Debugging Mode Preparation in Oreo Version

4.1.2 Tamper Protection

The proposed ANDROSICS tool suite supports the tamper protection feature to protect the access of unauthorized users. First, when the user runs ANDROSICS tool, the program will display the locked screen and wait for inputting the secret key. If the input secret key is incorrect more than 3 times, the image of current user will be detected. Otherwise, the input secret key is corrected, the tool will verify the user credential via the username and password. If the user credential is matched, the user can start the case ticket process. If the user credential is incorrect, it will claim to the administrator. Figure 4.3 shows the detailed process of tamper protection in ANDROSICS tool.

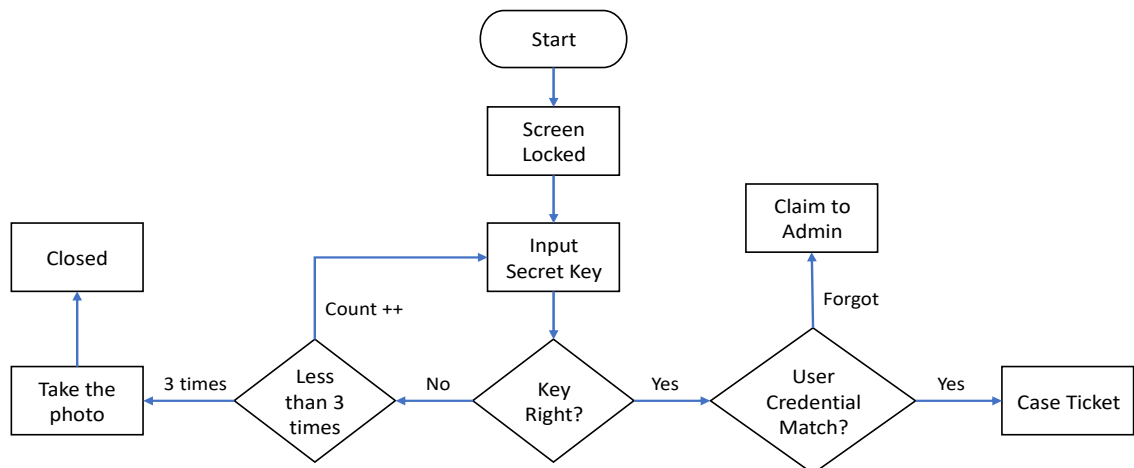


Figure 4.3 Tamper Protection for ANDROSICS Tool

4.1.3 Case Ticket Creation

Before doing the investigation process, the investigator should check to see the case has already been created. If the case is new, he/she will need to create a case ticket and fill out the case form. Then, he/she needs to assure if the device is connected or not. If the device is connected, the investigator can start the data collection process and analyze the data. If the case was previously created, the investigator can select the case and perform the analysis process as instanced in Figure 4.4.

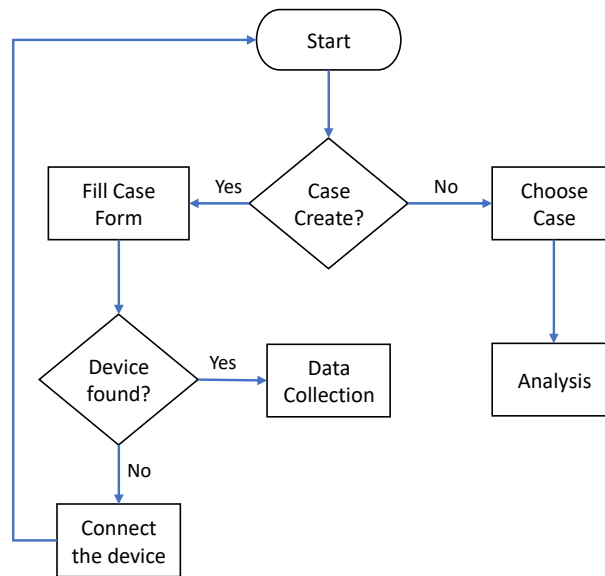


Figure 4.4 Creating and Analyzing a Case Ticket

Moreover, the investigator needs to record the case information including case directory, case number, device owner, investigator name and department before starting the investigation process. Table 4.2 describes the sample case information of a ticket.

Table 4.2 Case information of a ticket

Case Sample	
Case Directory	D:/Crimecase
Case Number	X01
Case Name	66D
Device Owner	Myo Ko Ko San
Investigator	Naing Linn Htun
Department	Cyber Security Research Lab, UCSY

4.2 Data Collection Process

Data Collection process is extracting the artifacts data that includes screenshot image, backup data, device profile, dump data (activity, network, Bluetooth, applications, etc.), device property information, log Data (logcat, call log, contact log, recent uninstall applications log, etc.) and imaging the physical storage or logical storage.

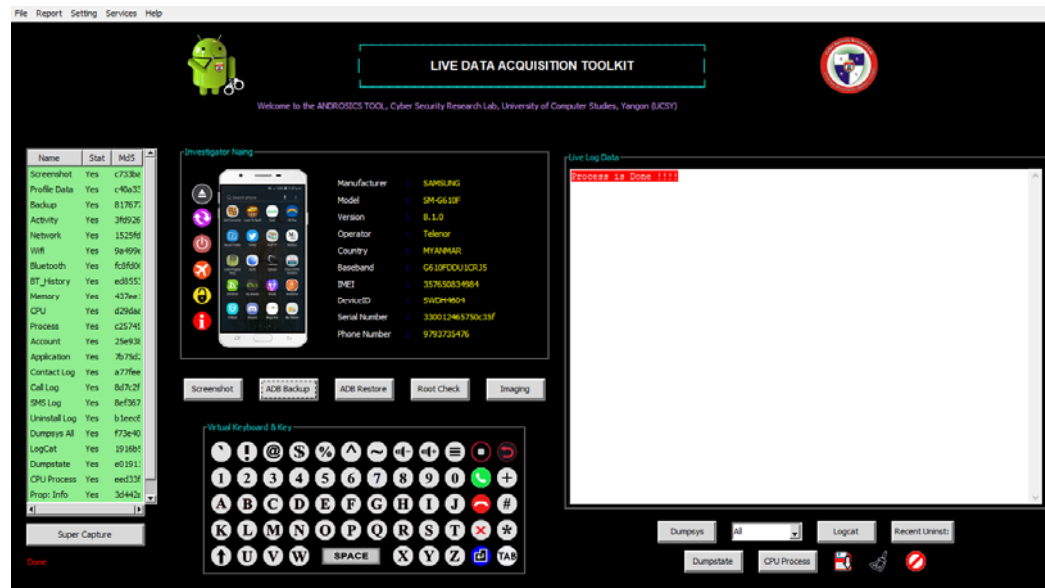


Figure 4.5 Live Data Acquisition on Samsung Device

This Figure 4.5 (Screenshot) is the main page of live data acquisition in ANDROSICS tool. In this page, it emphasizes on data collection process and provides useful features for Android investigation, management process and data collection report. Investigator can get different file types from data collection process. These are screenshot file with PNG format, backup file with AB format, dump data file with ANDRO6 format and storage imaging file with IMG format. Whatever file format is different, it generates the md5 checksum for each file when the investigator collects the data.

Screenshot: It is automatically saved the device display screen by screenshot feature when the device is connected with ANDROSICS tool. If the investigator wants to capture the other display screens, it can use the “Screenshot” button by clicking and saved automatically, as shown in Figure 4.5.

Profile Data: It is also automatically saved and it displays device information on the home page of live data acquisition, as shown in Table 4.3.

Table 4.3 Profile Data of Evidence Device

Profile Data Sample	
Manufacturer	SAMSUNG
Model	SM-G610F
Version	8.1.0
Operator	Telenor
Country	MYANMAR
Baseband	G610FDDU1CRJ5
IMEI	357650834984
Device ID	SWDH4605
Serial Number	330012465750c35f
Phone Number	9793735476

Backup: This feature is one of the valuable things in android forensics because it does not need root access. But it needs the device with active mode (no power sleep, no screen lock) before doing the backup process. For active mode, it will display instruction box with Myanmar language when the investigator pushes the Backup button as shown in Figure 4.6.

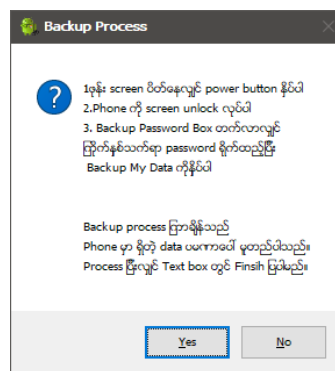


Figure 4.6 Active Mode Instruction Box

If the device with sleep mode situation, he needs to do three steps: 1) push the power button, 2) swipe screen lock and 3) type passwords. In this case, the investigator can use virtual keys on ANDROSICS tool. After doing the device with active mode, he can start the backup process and saved file with a password or not, as shown in Figure 4.7. Otherwise, if the device has any problems during investigation process, the investigator can restore the device with this backup file.

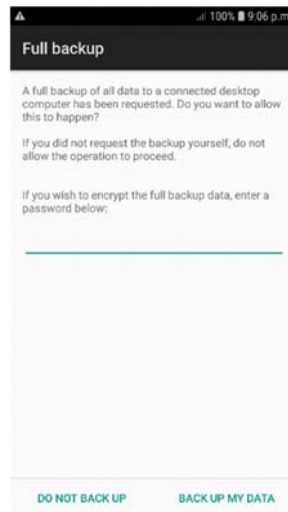


Figure 4.7 Backup Process on Android Device

In backup process, it will collect the data such as applications, applications data, and phone storage. Afterwards, it will compress and save as the “.ab” file as shown in Figure 4.8.

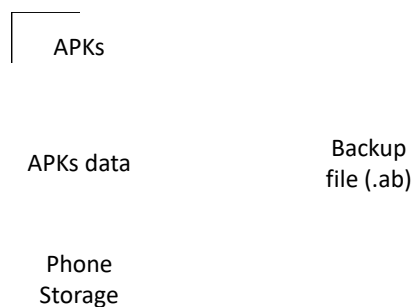


Figure 4.8 Backup Process

Dump Data: In this feature, the investigator can collect a massive amount of dump data that includes activity, network, Wifi, Bluetooth, memory, CPU, current process, and so on. Some dump data keep on volatile memory that can be easy to lose. The investigator can check live-stream data while capturing the dump data, as shown in Figure 4.9.

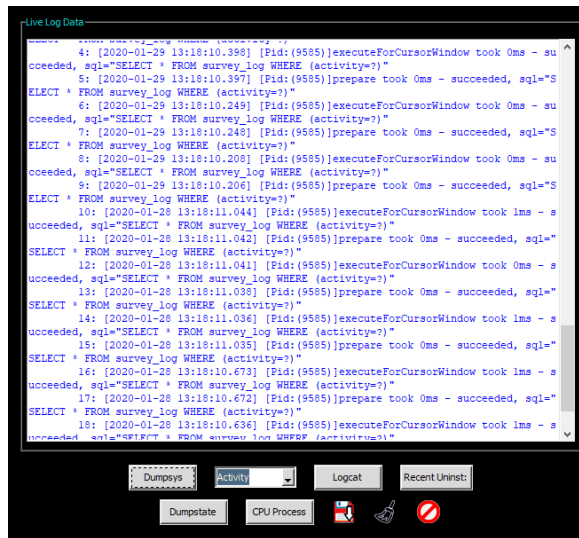


Figure 4.9 Streaming Live Log Data

If the investigator wants to extract all dump data, he can choose the option to All. The capturing process of all dump data, logcat, Dumpstate and CPU process logs takes a long time to finish. After every stream live data is finished or stopped, the investigator needs to save by clicking the “Save” button.

Super Capture: This is the one-click feature to extract some data types. It contains specific dump data (activity, network, Wifi, Bluetooth, BT_History, memory, CPU, process, account, application), contact log, call log, SMS log, uninstall log and device property information. It will display notice box when investigator click this feature as shown in Figure 4.10.

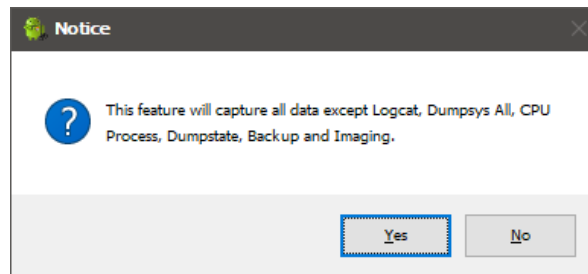


Figure 4.10. Notice of Super Capture Feature

Imaging: This feature is imaging the physical storages and logical partitions, but it needs root access and Media Transfer Protocol (MTP) enabled. If the device is rooted and MTP enabled, the investigator can check detailed partitions list and SD cards list for the imaging process. This process will generate a file with ‘.img’ extension format

and will save in external SD card as shown in Figure 4.11. Moreover, the process of imaging on phone storage partitions is illustrated in Figure 4.12.

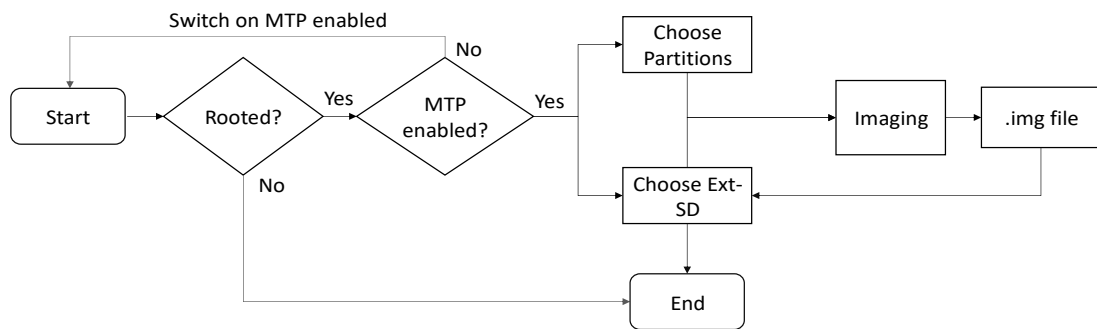


Figure 4.11. Imaging Process Flow

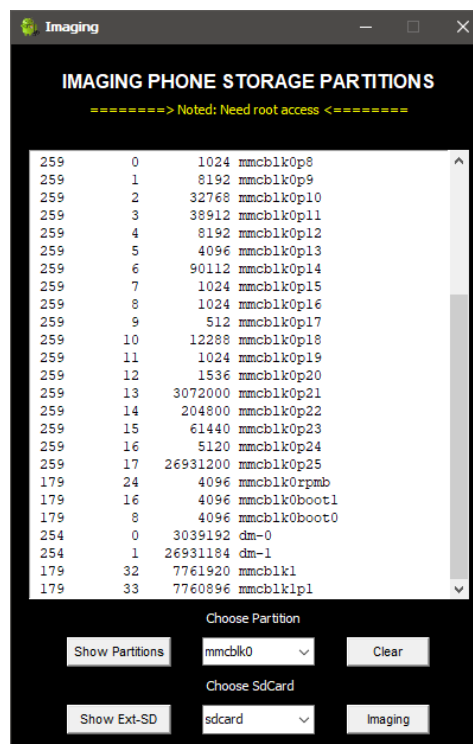
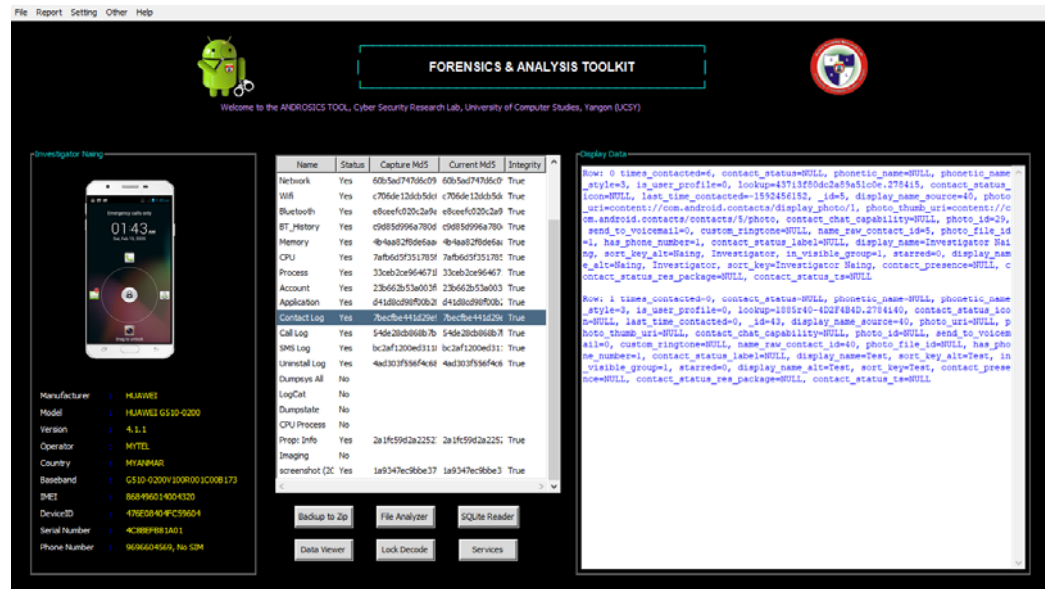


Figure 4.12. Imaging Feature in Androsics Tool

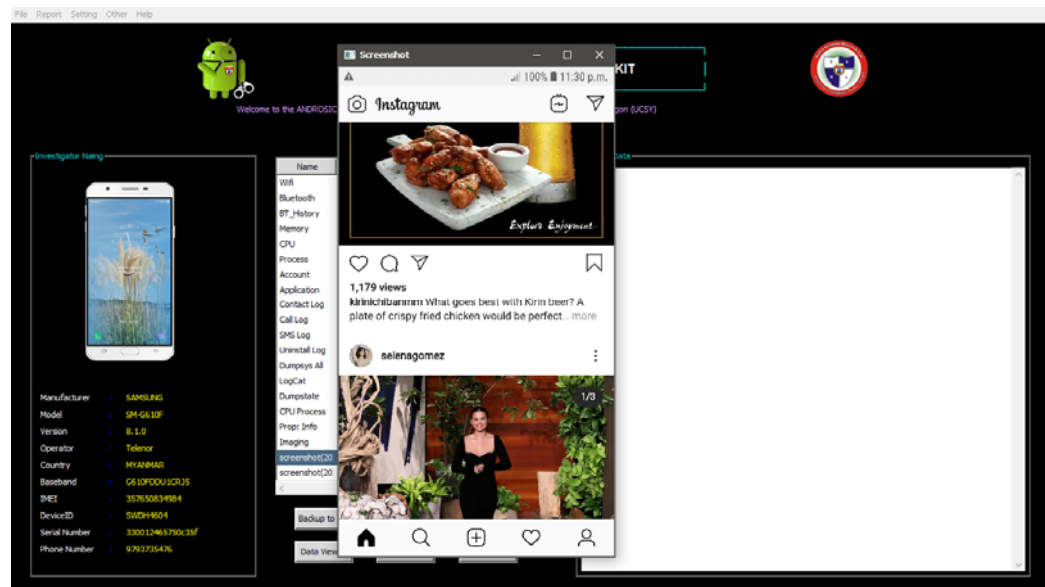
4.3 Examination and Analysis

After the Data Collection process, the investigator needs to do Examination and Analysis process that provides four main features - Data Viewer, Backup Extractor, File Analyzer and SQLite Reader. Firstly, it can check any changes in all collected data files from Live Acquisition Tool (ANDROSICS). It will show details information log

when he selects on each specific data, as shown in Figure 4.13(a). If he selects on screenshot data, it will display a screenshot image, as shown in Figure 4.13(b).



4.13(a) Examination and Analysis Process on Huawei Device Data



4.13(b) Examination and Analysis Process on Samsung Device Data

4.3.1 Data Viewer

Data Viewer analyzes the *.andro6 extension files that contain dump data files, data collection list file, profile data file, property information file, call log file, contact log file, SMS log file and report file. This feature decrypts the all encrypted andro6 files

and display with smart format as shown in Figure 4.14. And it provides keyword searching feature that display total words and check one by one with color. It enables to remove case sensitive while searching the keywords. Additionally, investigator can export each andro6 file with pdf extension format.



Figure 4.14 Data Viewer Feature

4.3.2 Backup File to Zip Format

This feature is decrypted the encrypted backup file (*.ab) and convert to the tar file. Firstly, it can check the status of the backup file process from data collection process list. If the status is No, the investigator does not need to consider running this process. If the investigator runs this feature without backup file, he will see the hint of the invisible text “Didn’t capture any backup file” in backup file directory entry box and save directory entry box is blank as shown in Figure 4.15(a).

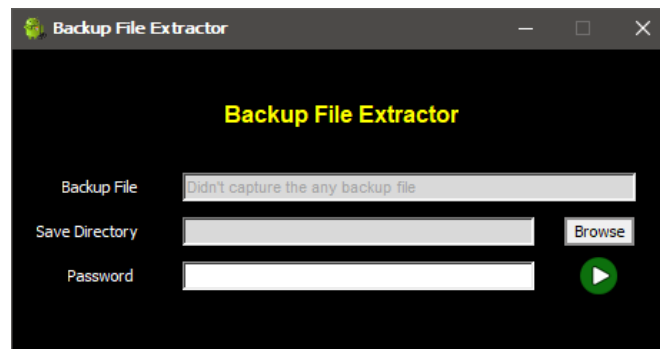


Figure 4.15(a) Backup File Converter without Backup File

If the backup file is already captured, it will display backup file directory and save directory as shown in figure 4.15(b). If the investigator sets the password of the backup file, he needs to input the password before the start. Moreover, he can change the default save directory by clicking the browse button and extract tar file automatically.



Figure 4.15(b) Backup File Converter with Backup File

4.3.3 File Type Analyzer

According to chapter 3.3.2(iii), this feature provides analyzing the file signature (extension and header code) whether the files are corrupted or not. In file analysis process divided into two situations: 1) File with extension and 2) File with no extension. For the 'File with extension' case, it generates four types of status which include False Positive, False Negative, True Positive and True Negative.

Table 4.4 Classified for File Type Analyzer

Extension	Database		Status	Integrity
	Header	Extension		
True	True	True	True Positive	True
	True	False	True Negative	Extension Change
	False	True	False Positive	Header Change
	False	False	False Negative	Analyze
False	True	True	True Positive	True
	True	False	True Negative	Add Extension
	False	False	False Negative	Analyze

However, In the 'File with no extension' case, it generates only three types of status because if the header is False, the extension must be False. Therefore, it does not need to consider the False Positive situation. According to this concept, the integrity types can be classified based on these four types of status. False Positive is header change,

False Negative is needed to analyze, True Positive is no suspicion, and True Negative is extension change or adds the extension as shown in Table 4.4. For this file type analysis process, we collected 527 types of files and stored in the database. Each of them has a file extension, header code and file type description. The header code length is sorted from maximum to a minimum. It provides high accuracy performance because some short header codes may also contain in another header code. Additionally, it can easily check the total number of file formats, filenames, directories and sizes of each file format.

True Positive: In file with the extension (FE), the file type analyzer will check the file header code whether it contains in the database or not. If the header code is contained in the database, we will match the actual file format with the file format of header code in a predefined database. If it is also true, this feature will specify as the True Positive status and Integrity does not have any changes. In the file with no extension (FNE) situation, the analysis process is almost the same as the FE process. However, the extension type must be '*' in the database.

True Negative: Both FE and FNE situations, we found the file header code in the database, but the extension does not match (extension type is '*' for FNE).

False Positive: This analysis process is the opposite of True Negative situation. The extension is included in the database, but the file header code is not found in the database. This situation does not need to consider in FNE because it has no extension.

False Negative: Both file header code and extension are not found in the database.

In summary for this process, to analyze a file, you must first assure that it is with an extension or without an extension. When a file is including an extension, there are probably four statuses as shown in Figure 4.16(a). To identify the status, it must first compare with a database of signatures. If the header is contained in database, then check the extension is correct. If both the header and extension are assured, it is True Positive. If only the header is correct, it will get True Negative. When the header is not in the signature database, the extension is checked. In this situation, if the extension is found, it is False Positive and otherwise it is False Negative.

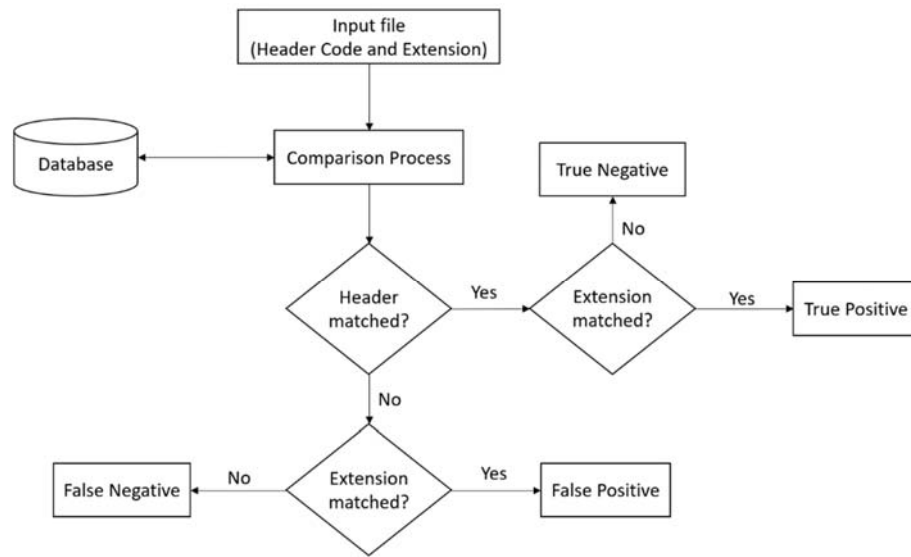


Figure 4.16(a) Four Types of Status for File with Extension

When a file is without an extension, there are probably three statuses as shown in Figure 4.16(b). It also compares with database to identify the status. If the header is found in database, then check the file extension. Before checking the extension, it needs to specify first the file type that has no extension as (*). If the extension is not (*), it is True Negative and if the extension is (*), it is True Positive. Whenever the header is not found in database, it is identified as the False Negative.

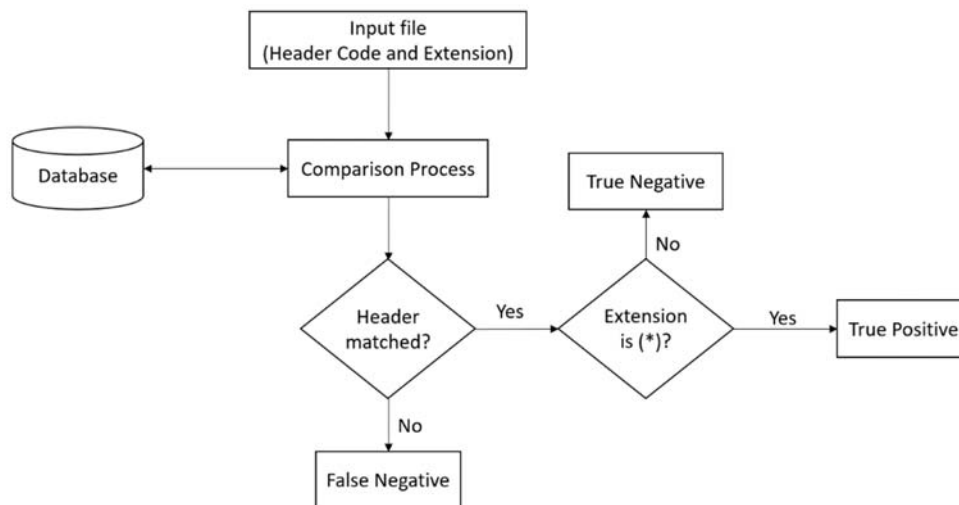


Figure 4.16(b) Three Types of Status for File with no Extension

There are three exceptions in case of file type analyzing process.

Exception – 1: Some Text-based file types that can create their file extensions from notepad have no header code or signature. In such kind of situation, their status may be in False Positive or False Negative as illustrated in Table 4.5.

Table 4.5 Possible Statuses of Some Text-Based File Types

Text-Based file types	Example file	Change known format	Change unknown format	Status
log file	Test.log	Test.zip	-	False Positive
Notepad file	Test.txt	-	Test.blah	False Negative
Python file	Test.py	Test.pdf	-	False Positive

Exception – 2: If a file is changed the header code with others known header code, it is actually False Positive. But it will specify as True Negative because the header code is found in the database first.

Exception – 3: This is called Fake True Positive. Both the extension and file header code are altered, but they are matched and included in the database. In this case, this feature will describe as True Positive, but the file is corrupted and cannot open it.

Solution Methods

True Negative: It needs to change the extension of the header code. If it is still False, it needs to do the brute force on both of the extension and header code.

False Positive: It needs to try to open with Text format(.txt) first. If it has an error, change the header code of the extension. If it is still False, it needs to do the brute force on both of header code and extension.

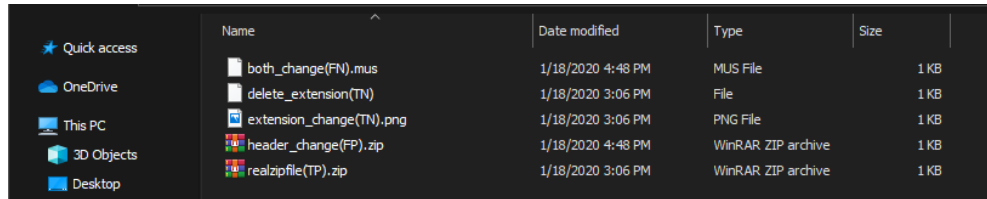
False Negative: It needs to find the right application to open the file first. If it cannot find the correct one, we can open with Text format(.txt). Finally, if it has still a problem, it needs to use the brute force method.

4.3.3.1 Sample Scenario for Evaluation

This section will demonstrate the proposed file type analyzer feature with two cases. The first case is used ZIP file for the file with extension process, and the second one has evaluated the file with no extension originally.

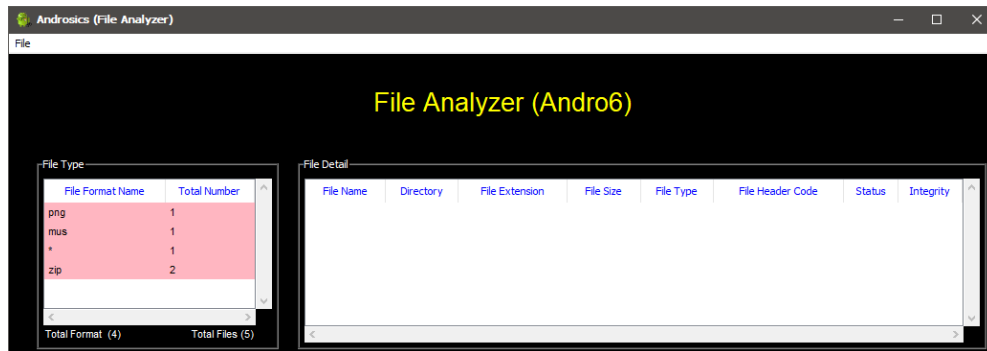
Case 1: File with Extension

Firstly, the proposed file type analyzer is applied on the ZIP file and specified four statuses. It generates four file formats (PNG, ZIP, MUS and Unknown) and the total number of files are five from a ZIP as shown in Figure 4.17(a).



Name	Date modified	Type	Size
both_change(FN).mus	1/18/2020 4:48 PM	MUS File	1 KB
delete_extension(TN)	1/18/2020 3:06 PM	File	1 KB
extension_change(TN).png	1/18/2020 3:06 PM	PNG File	1 KB
header_change(FP).zip	1/18/2020 4:48 PM	WinRAR ZIP archive	1 KB
realzipfile(TP).zip	1/18/2020 3:06 PM	WinRAR ZIP archive	1 KB

Figure 4.17(a) Four File Formats in Five Files based on ZIP File



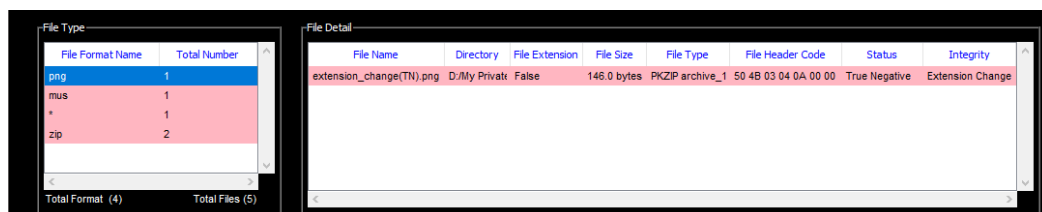
File Format Name	Total Number
png	1
mus	1
*	1
zip	2

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
-----------	-----------	----------------	-----------	-----------	------------------	--------	-----------

Total Format (4) Total Files (5)

Figure 4.17 (b) Using File Analyzer Feature from Androsics for Evaluation

After generating the different files, investigators used the file analyzer tool and browsed the ZIP file directories to analyze all files. He will see the total file formats and the total number of files at the left side of the file analyzer tool, as shown in Figure 4.17(b). Then, he selected the PNG file type to check-in details. This detected file will specify as the True Negative because the file header code is found in the database, and file extension is different. The investigator can easily know that this file is altered the extension from ZIP to PNG, as illustrated in Figure 4.18(a).



File Format Name	Total Number
png	1
mus	1
*	1
zip	2

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
extension_change(TN).png	D:/My Private	False	146.0 bytes	PKZIP archive_1	50 4B 03 04 0A 00 00	True Negative	Extension Change

Total Format (4) Total Files (5)

Figure 4.18(a) True Negative – Extension Changes from ZIP to PNG

This time, we assume to select on MUS file type. This file will generate False Negative status because it cannot find both extension and header code in the database, as shown in Figure 4.18(b). In this situation, the investigator needs to analyze the file whether the file is really corrupted or not. If the device owner makes the corrupted file intentionally, the investigator can get the evidence data from this file.

The screenshot shows two windows. The 'File Type' window on the left has a table with the following data:

File Format Name	Total Number
png	1
mus	1
*	1
zip	2

Below the table, it says 'Total Format (4)' and 'Total Files (5)'. The 'File Detail' window on the right shows a table with the following data:

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
both_change(FN).mus	D:/My Private Tr	False	146.0 bytes	Unknown	False	False Negative	Analyze

Figure 4.18(b) False Negative – both Change Extension and Header Code

If the investigator selected on unknown file type (*), this file describes as False Negative status. Investigator can easily know the file is deleted the extension as shown in Figure 4.18(c).

The screenshot shows two windows. The 'File Type' window on the left is identical to the one in Figure 4.18(b). The 'File Detail' window on the right shows a table with the following data:

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
delete_extension(TN)	D:/My Private Tr	False	146.0 bytes	PKZIP archive_1	50 4B 03 04 0A 00 00	True Negative	Add Extension

Figure 4.18(c) True Negative - Delete Extension of ZIP file

When the ZIP file type is selected, there are two ZIP files in following windows Figure 4.18(d). The investigator can easily check these two files. The first file will show the False Positive status because it is found only extension in the database. The second file will popup True Positive. So, it can be inferred that this file did not change any extension or header code.

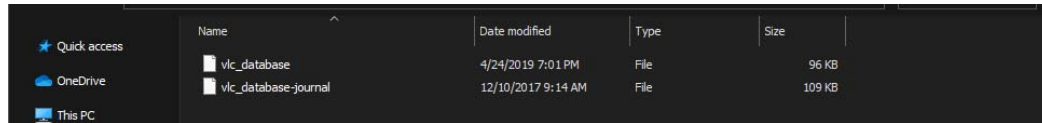
The screenshot shows two windows. The 'File Type' window on the left is identical to the one in Figure 4.18(b). The 'File Detail' window on the right shows a table with the following data:

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
header_change(FP).zip	D:/My Private Tr	ZIP	146.0 bytes	ZLock Pro encry	False	False Positive	Header Change
realzipfile(TP).zip	D:/My Private Tr	ZIP	146.0 bytes	PKZIP archive_1	50 4B 03 04 0A 00 00	True Positive	True

Figure 4.18(d) False Positive and True Positive of ZIP file

Case 2: File with no Extension

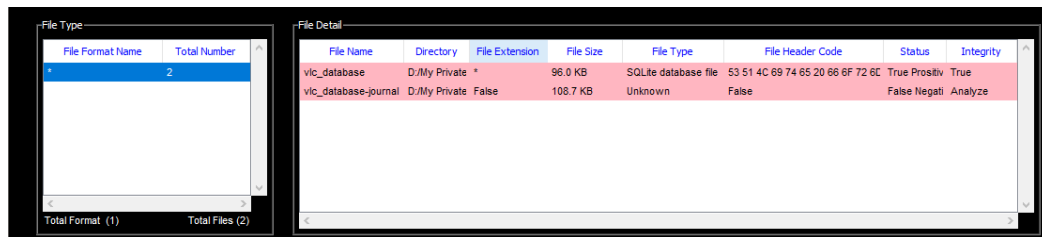
For this experiment, the SQLite file is used with no extension format and unknown file format. Their names are vlc_database and vlc_database-journal, as shown in Figure 4.19(a).



Name	Date modified	Type	Size
vlc_database	4/24/2019 7:01 PM	File	96 KB
vlc_database-journal	12/10/2017 9:14 AM	File	109 KB

Figure 4.19(a) Two Files with no Extension Format

Investigator can easily analyze these two files. The first one is True Positive because the header code is found in the database, and file extension is originally missed. Another file will specify as False Negative status as shown in Figure 4.19(b) because the header code is not found in the database. So, it does not need to consider the extension because it does not have an extension initially.



File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
vlc_database	D:/My Private *	*	96.0 KB	SQLite database file	53 51 4C 69 74 65 20 66 6F 72 6C	True Proativ	True
vlc_database-journal	D:/My Private	False	108.7 KB	Unknown	False	False Negati	Analyze

Figure 4.19(b) True Positive and False Negative in File with no Extension

4.3.3.2 Evaluation of File Analyzer feature using ANDROSICS Tool

This section evaluated the file analyzer features by using ANDROSICS tool suite. The experiment was done on large number of files with various file formats. In this experiment, there are 5,761 files with 123 file formats such as .apk, .jpg, .dat, on and on. Using this file analyzer feature, total 43 APK files can be extracted as shown in Figure 4.20(a). Moreover, it is also evaluated on JPG file format. In this experiment, the tool can extract 843 JPG files as illustrated in Figure 4.20(b).

File Analyzer (Andro6)

File Type	File Format Name	Total Number
DB		1
DB-shm		1
DB-wal		1
PNG		1
_m_u		2
apk		40
apk_block		1
at_block		1
bigram_freq		3
bigram_index_freq		3
bigram_occup		3
bin		1
bs_block		1
c		1
c7419605-6835-4644-BE		1
cache		3
cls		50
dat		6
data		2
db		91
db-journal		82
db-shm		1
db-wal		3
db3		1
dex		1
dh		1
dh-journal		1
c		1
Total Format (123)		Total Files (5761)

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
base.apk	E:\Testing\app\com.br	APK	3.5 MB	Android Package	50 4B 03 04 0A 00 00	True Positive	True
base.apk	E:\Testing\app\com.br	APK	13.0 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.ci	APK	12.1 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.ci	APK	3.7 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.ci	APK	22.4 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.cj	APK	36.3 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.dr	APK	595.3 KB	Android Package	50 4B 03 04 0A 00 00	True Positive	True
base.apk	E:\Testing\app\com.dr	APK	2.6 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.dr	APK	185.4 KB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ec	APK	44.9 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ec	APK	13.4 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.fh	APK	13.8 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.gr	APK	3.8 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	32.1 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	7.5 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	26.7 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	19.3 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	11.6 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	6.6 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	7.5 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.ia	APK	43.2 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.or	APK	3.9 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.Oj	APK	13.3 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.Oj	APK	6.6 MB	Android Package	50 4B 03 04 0A 00 00	True Positive	True
base.apk	E:\Testing\app\com.su	APK	1.3 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.su	APK	13.5 MB	Android Package	50 4B 03 04 00 00 00	True Positive	True
base.apk	E:\Testing\app\com.vr	APK	32.2 MB	Android Package	50 4B 03 04 14 00 00	True Positive	True
base.apk	E:\Testing\app\com.vr	APK	6.0 MB	Android Package	50 4B 03 04 14 03 00	True Positive	True

Figure 4.20(a) Evaluation on APK File Format

File Analyzer (Andro6)

File Type	File Format Name	Total Number
PNG		7
rar		1
txt		2
png		1
JPG		647
jpg		359
Total Format (6)		Total Files (1217)

File Name	Directory	File Extension	File Size	File Type	File Header Code	Status	Integrity
DSC_6276.JPG	E:\Testing\app\com.Ci	JPG	6.1 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6277.JPG	E:\Testing\app\com.Ci	JPG	5.9 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6278.JPG	E:\Testing\app\com.Ci	JPG	5.7 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6279.JPG	E:\Testing\app\com.Ci	JPG	6.1 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6280.JPG	E:\Testing\app\com.Ci	JPG	6.1 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6281.JPG	E:\Testing\app\com.Ci	JPG	6.7 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6282.JPG	E:\Testing\app\com.Ci	JPG	6.4 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6283.JPG	E:\Testing\app\com.Ci	JPG	6.5 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6284.JPG	E:\Testing\app\com.Ci	JPG	6.7 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6285.JPG	E:\Testing\app\com.Ci	JPG	6.5 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6286.JPG	E:\Testing\app\com.Ci	JPG	5.9 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6287.JPG	E:\Testing\app\com.Ci	JPG	6.6 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6288.JPG	E:\Testing\app\com.Ci	JPG	6.5 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6289.JPG	E:\Testing\app\com.Ci	JPG	6.8 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6290.JPG	E:\Testing\app\com.Ci	JPG	6.7 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6291.JPG	E:\Testing\app\com.Ci	JPG	6.8 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6292.JPG	E:\Testing\app\com.Ci	JPG	6.6 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6293.JPG	E:\Testing\app\com.Ci	JPG	6.8 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6294.JPG	E:\Testing\app\com.Ci	JPG	6.2 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6295.JPG	E:\Testing\app\com.Ci	JPG	5.9 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6296.JPG	E:\Testing\app\com.Ci	JPG	6.1 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6297.JPG	E:\Testing\app\com.Ci	JPG	6.3 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6298.JPG	E:\Testing\app\com.Ci	JPG	6.1 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6299.JPG	E:\Testing\app\com.Ci	JPG	5.9 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6300.JPG	E:\Testing\app\com.Ci	JPG	6.1 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6301.JPG	E:\Testing\app\com.Ci	JPG	6.2 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6302.JPG	E:\Testing\app\com.Ci	JPG	6.5 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True
DSC_6303.JPG	E:\Testing\app\com.Ci	JPG	6.7 MB	Digital camera.JPG usn	FF D8 FF E1	True Positive	True

Figure 4.20(b) Evaluation on JPG File Format

4.3.4 SQLite Reader

SQLite Reader provides to view sqlite database files with read-only mode as shown in Figure 4.21. Investigator can check all of database files in android devices and it can analyze detail information of each table. Investigator can get a lot of interesting information from database files that may be useful for investigation processes.

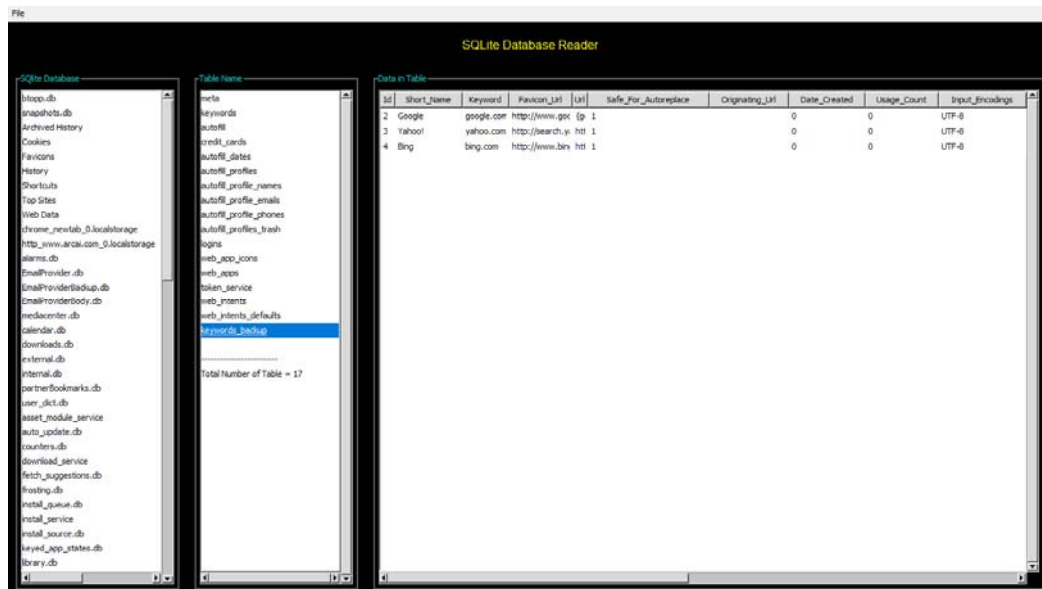


Figure 4.21 SQLite Database Reader

4.4 Brute Force Techniques

Brute Forcing is one of the essential things in the forensics investigation process. Because everybody knew to use the password for securing and they might set pattern lock, pin or password on their smartphone. Moreover, they might set the password to their sensitive files. During the investigation process, if the suspected device is locked and the device owner doesn't want to give their password, or device owner is missing, the investigator needs to crack the password. In this case, ANDROSICS tool provides the Brute Force feature for cracking the password. It includes Wordlist creator, Android Screen Lock Decoder, Zip/Rar password cracker and Microsoft Office file password cracker.

4.4.1 Wordlist Creator

This feature supports to build the powerful dictionary file for cracking the password. It is used permutation algorithms for iterations and contained *Char-Mixer*, *Rules* and *Remove gender titles for Myanmar names* features. The permutation algorithms can generate the reverse and repeat character sets that help in cracking the password, as shown in Table 4.6.

Table 4.6 Permutation and Combination Algorithms for Generating the Passwords

Iterator	Formula	Variable	Password	Output
Permutation with repetitions	n^r	n = length of given password r = length of output password	ABC, $n = 3$ $r = 2$	AA, AB, AC, BA, BB, BC, CA, CB, CC
Permutation without repetitions	$n!$			AB, AC, BA, BC, CA, CB
Combination with repetitions	$\frac{(r + n - 1)!}{r! (n - 1)!}$			AA, AB, AC, BB, BC, CC
Combination without repetitions	$\frac{n!}{r! (n - r)!}$			AB, AC, BC

Char-Mixer is a simple process that includes capital letters, small letters, numbers and punctuation marks as shown in Table 4.7. User can choose any groups (or input any characters) through the checkboxes and mix the characters automatically by using the permutation algorithm with repetitions. Additionally, it can specify the minimum and maximum length of the password.

Table 4.7 Input Characters Groups

Groups	Characters
Small	abcdefghijklmnopqrstuvwxyz
Capital	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Number	0123456789
Punctuation marks	!@#\$%^&*()-_+=~`[]{} :;'\",<,>.,?/

Rules is one of the important factors in Wordlist Creator. It is implemented with five rules: 1) swapping uppercase and special characters, 2) combining possible characters, 3) swapping hacking or l33t characters, 4) switching characters with permutation and 5) included all these rules. Rule 1 and 4 used the permutation algorithm without repetitions as shown in Table 4.8.

List of characters in Rules:

Number List = ['0', '1', '2', '3', '4', '5', '6', '7', '8', '9', '01', '02', '03', '04', '05', '06', '07', '08', '09', '012', '0123', '123', '1234', '12345', '123456', '1234567', '00', '11', '22', '33', '44', '55', '66', '77', '88', '99', '000', '111', '222', '333', '444', '555', '666', '777', '888', '999', '00000',

'11111', '22222', '33333', '44444', '55555', '66666', '77777', '88888', '99999', '0000',
'1111', '2222', '3333', '4444', '5555', '6666', '7777', '8888', '9999', '2019', '2020']

Special Chars List = ['!@', '!@#', '!@#\$', '!@#\$', '!@#%^', '!@#%^&',
'!@#%^&*']

l33t List = {'e': '3', 's': '5', 'a': '4', 'you': 'j00', 'o': '0', 'E': '3', 'S': '5', 'A': '4', 'You': 'j00', 'O':
'0', 't': '7', 'T': '7', 'i': '1', 'I': '1', 'z': '2', 'Z': '2', 'c': '6', 'G': '6', 'q': '9', 'a': '@', 's': '\$', 'i':
'!'}

Table 4.8 Rules of Wordlist Creator

No	Rules	Examples
1	Swapping uppercase and special	abc2019 – Abc2019, aBc2019, abC2019, Abc2o!9, etc.
2	Combining possible chars	abc – abc!, abc@, abc@123, !abc, abc2019, etc.
3	Swapping l33t chars	abc2019 – 4bc2o!9, @bc2O!9, etc.
4	Switching chars with permutation	abcd – acbb, dbac, cdba, cbda, dcba, etc.
5	All	Mixed above four features

Remove gender titles for Myanmar Names is used for creating the wordlist for Myanmar names list because Myanmar gender titles are more complex than others. For examples, Myanmar names include the gender title like U, Ko, Maung, Daw, Ma. It is especially at the first place of the names.

In Wordlist Creator, it needs to enter any characters through typing or from the dictionary file by browsing the file tab or by choosing small letters (a-z), capital letters (A-Z), numbers (0-9) and symbols characters. After finishing the input process, it can limit the password length from minimum to maximum (default is from 6 to 18). Afterwards, we need to choose the output directory to save the wordlist file (default is same current directory). Even though the investigator does not use any specified rules, he can start to generate the possible passwords until the process is finished or stopped and saved as the wordlist file. If he uses the rules that include Swapping uppercase, Extra, L33t, Switch and All as shown in Table 4.6, he can generate the password until finishing the process. Additionally, if he inputs the Myanmar name list, he can select to

remove the gender specified titles such as Mg, Maung, Daw, Ma, U, Ko, and white space.



Figure 4.22 Windows View of Androsics Wordlist Creator

This generated wordlist is useful to brute force the passwords for authorization of file access or login access. It can provide to try many different passwords for brute forcing very quickly. Investigators can generate the most likely passwords according to their knowledge based on what they know about the targets. This proposed wordlist creator will definitely help to investigators because it included pretty rules and special features for Myanmar. The windows view of wordlist creator in Androsics is illustrated in Figure 4.22.

4.4.2 Screen Lock Decoder

This feature provides to decode the screen lock that includes pattern lock, pin code and textual password.

4.4.2.1 Pattern Lock

It is one of the security measures that protect to access devices like smartphones or tablets. Typically, Android users use the pattern lock with default grid (3x3 dots) as shown in Figure 4.23(a). To access the functions and content of a device, users must first draw a pattern in a grid of dots on the screen. If this does not match the pattern set by the device owner, the device cannot be used. If the evidence devices with pattern lock, the investigator needs to know how to set the pattern by the device owner. In this situation, Androsics tool can provide to decode the pattern lock. But it needs three things – USB Debugging is enabled, RSA key and Root access.

In this feature, Androsics defined the pattern numbers from zero to eight (0-8), as shown in Figure 4.23(b).

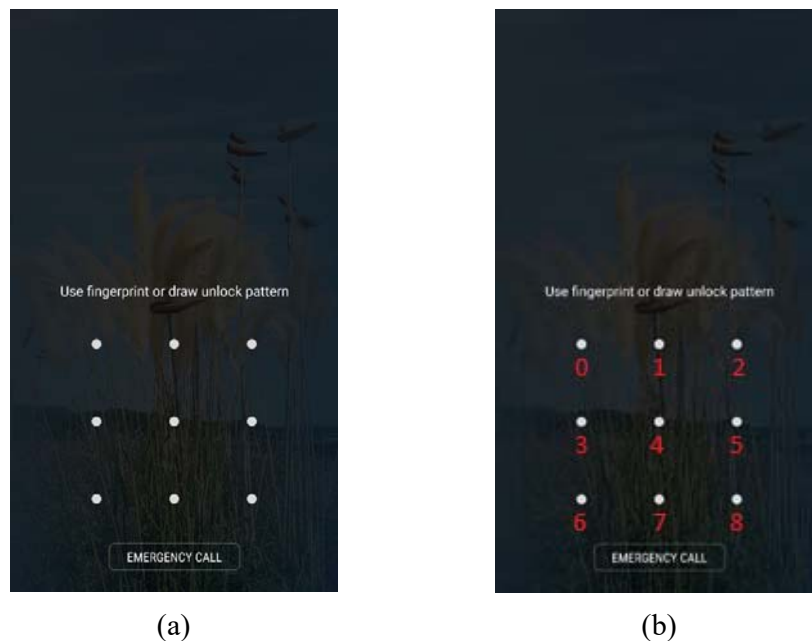


Figure 4.23 Android Phone with Pattern Lock

Step by step calculation of Pattern lock decoding process on Android devices:

- Extract pattern lock file
file directory - /data/system/gesture.key (length-40, SHA-1)
- Convert from each digit (0-8) to two digits
0 1 2 3 4 5 6 7 8 => 00 01 02 03 04 05 06 07 08
- Convert from two digits to byte array with hex type

00 01 02 03 04 05 06 07 08 => ("x00", "x01", "x02", "x03", "x04", "x05",
"x06", "x07", "x08")

- Permutation length from 4 to 9 (based on byte array)
- Convert from each output to SHA-1
- Output matching with gesture.key
- If match, process is done

The computation of possible combination wordlist by using the permutation without repetitions method is described below,

Permutation without repetitions, ${}_nP_r = \frac{n!}{(n-r)!}$

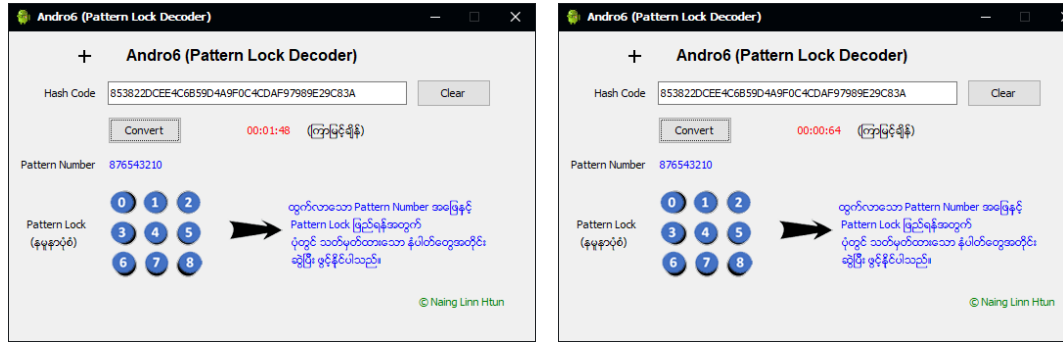
Total number (n) = 9 and length (r) = 4 to 9

$${}_nP_r = \frac{9!}{(9-4)!} + \frac{9!}{(9-5)!} + \frac{9!}{(9-6)!} + \frac{9!}{(9-7)!} + \frac{9!}{(9-8)!} + \frac{9!}{(9-9)!} = 985824$$

It used the permutation method (without repetitions) based on numbers 0-8 for calculating the pattern lock because each number cannot draw twice when the device set the pattern lock. The limitation of pattern length is at least four to nine numbers. This feature tested with Bruteforce and dictionary attacks for decoding the pattern lock. In dictionary attack, it created two wordlist files with possible combinations (985824) such as text file and SQLite database file for testing. It can compare time-consuming based on the maximum length of pattern lock and data integrity, as shown in Table 4.9. The appearance of execution time and sample evaluation results of pattern lock decoding process are instanced in Figure 4.24.

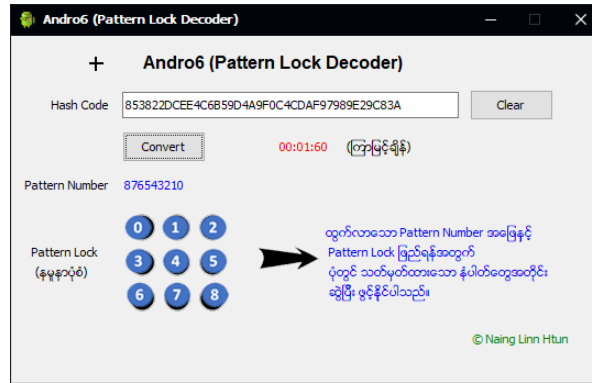
Table 4.9 Execution Time and Integrity on Three Types of Pattern Lock Decoder

Type	Wordlist time	Elapsed time	Integrity
SQLite database (dictionary)	4 kb per 8 seconds	1.48 seconds	Medium
Text file (dictionary)	Maximum 10 seconds	0.64 seconds	Low
Bruteforce Attack	No need	1.60 seconds	High



(a) Dictionary Attack with SQLite Database

(b) Dictionary Attack with Text File



(c) Bruteforce Attack

Figure 4.24 Three Types of Pattern Lock Decoding Process

4.4.2.2 Pin Code (Personal Identification Number)

Pin code is not like that gesture type as pattern lock. However, it is one of the security measures and a numeric code type that prevent unauthorized access to the devices. The users must enter a numeric code to access the content and functions of a device. If the given code does not match the numeric set by the device owner, the device cannot be used. Pin code decoder needs full access of the device that is same as pattern lock decoding process.

In this feature, it used the permutation method (with repetitions) based on zero to nine (0-9) numbers. It does not perform to build wordlist file because pin code length can set at least 4 to 16 numbers and it allowed repeat number in it. Thus, the total number of possible outputs will be massive (1111111111110000) for wordlist. Figure 4.25 shows the appearance of Pin lock screen on Android devices.

Permutation with repetitions, ${}_nP_r = n^r$

Total number (n) = 10 and length (r) = 4 to 16

$${}_nP_r = 10^4 + 10^5 + 10^6 + 10^7 + \dots + 10^{16} = 11111111111110000$$

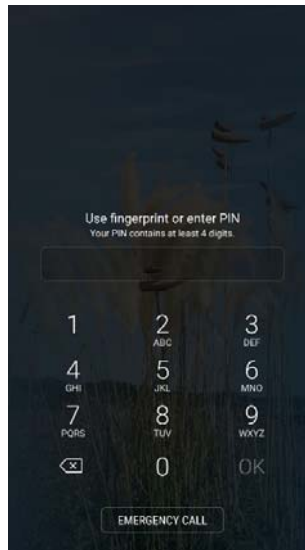


Figure 4.25 The Appearance of Pin Lock on Android Smartphone

Step by step calculation of Pin lock decoding process on Android devices:

- Extract pin lock file and salt number
PIN file directory - /data/system/password.key (length-72, SHA-1+MD5)
- Salt file directory - /data/system/locksettings.db or
/data/data/com.android.providers.settings/databases/settings.db
- Convert from salt number to hex
- Permutation length from 4 to 16
- Encoded (hex salt + each permutation output)
- Convert from encoded to SHA-1 and MD5
- Output SHA-1 + output MD5
- Total output matching with password.key
- If match, process is done

When the investigator uses the Pin lock decoder feature, firstly, he must click the "Browse" button and select the password.key file to decode. The detailed process is shown in Figure 4.26. Afterward, he must input the salt number by copying from settings.db as shown in Figure 4.27. Moreover, the investigator can specify the minimum and maximum password length to do the Bruteforce process. Then, click the "Play" button to start the decoding Pin lock.

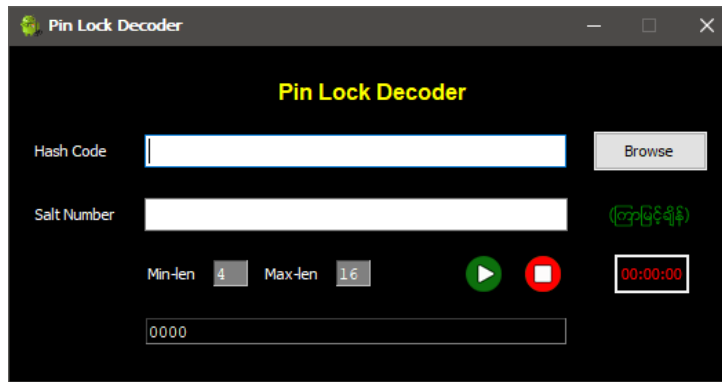


Figure 4.26 Pin Lock Decoder Feature

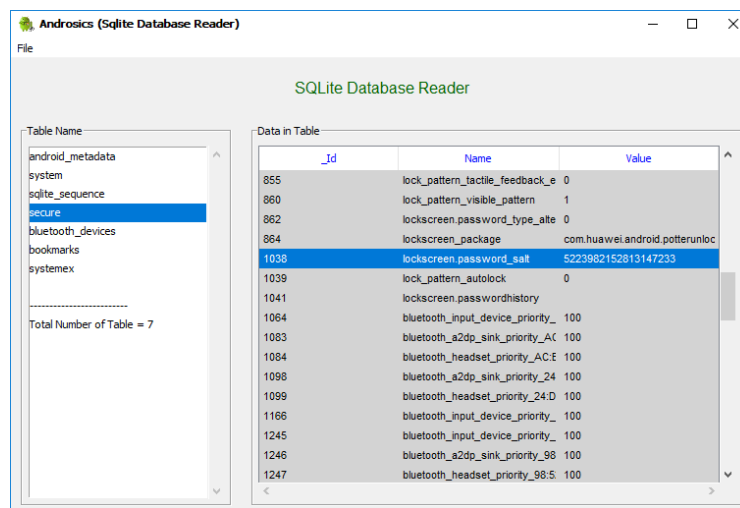


Figure 4.27 Salt Number in settings.db

4.4.2.3 Password Lock

Password is almost the same as the PIN code process; however, it contains not only numbers but also other characters such as small letters, capital letters, and punctuation marks. Therefore, it is the most substantial security measure in android screen lock that can set the password at least 4 to 16 characters length in 94 characters. The password decoder also needs full access for android devices such as USB Debugging, RSA key and Root. The appearance of password lock screen on Android devices is shown in Figure 4.28.

Permutation with repetitions, $nP_r = n^r$

Total number (n) = 94 and length (r) = 4 to 16

$$nP_r = 94^4 + 94^5 + 94^6 + \dots + 94^{16} = 37556971331618802349234821934090$$

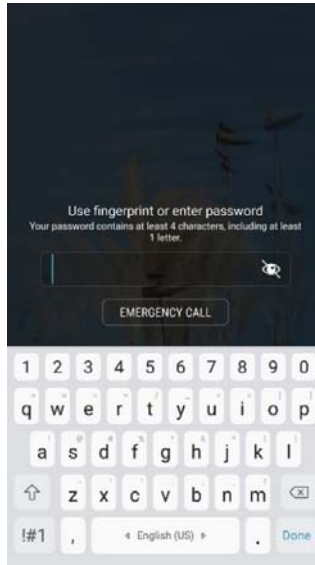


Figure 4.28 Android Phone with Password Lock

Step by step calculation of Password lock decoding process on Android devices:

- Extract pin lock file and salt number
Password file directory - /data/system/password.key (length-72, SHA-1+MD5)
Salt file directory - /data/system/locksettings.db or
/data/data/com.android.providers.settings/databases/settings.db
- Convert from salt number to hex
- Permutation length from 4 to 16
- Encoded (hex salt + each permutation output)
- Convert from encoded to SHA-1 and MD5
- Output SHA-1 + output MD5
- Total output matching with password.key
- If match, process is done

For decoding the android screen lock, device policies file is also an important thing that contains the XML version number, characters encoding and policies. The investigator should check the policies such as length, uppercase, numeric, symbols, and nonletter before trying to decode the android screen lock, as shown in Figure 4.29.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <policies>
  <active-password nonletter="6" symbols="0" numeric="6" letters="0" lowercase="0" uppercase="0"
    length="6" quality="131072"/>
</policies>
```

Figure 4.29 Device Policies File Screenshot

This device policies file provides to investigate the androids' screen lock decoding processes quickly. It helps to narrow the potential password for decoding the Android screen lock. This research investigated on the android version from Gingerbread (2.3.6) to KiKats. When using a password lock decoder, unlike a Pin or Gesture, it needs to have a wordlist as illustrated in Figure 4.30. Because there are many possibilities in calculation, it is more effective to set rules and decode for possible passwords. Without using the wordlist in Brute-force process, it will take much longer.



Figure 4.30 Password Lock Decoder in ANDROSICS tool

4.4.3 Zip/Rar Password Cracker

Compressed 'zip' is popularly used technique because one or more computer documents are packed into a single file or folder to keep less space. It can provide a beneficial way to send and store a large number of soft files. However, the unzip process needs doing to extract and view the contents inside. In some cases, people use a password to encrypt the files to be secure. When the documents are extracted in a zip file, a password is needed to decrypt. Unfortunately, criminal can use this way to hide the evidence information with a negative attitude. The forensics investigators need to crack the given password by using brute-force or dictionary attack to prosecute the criminal. In this study, the proposed Andorsics tool is intended to support the activity of cracking the password to unzip the compressed files.

This feature provides to crack the ZIP file or RAR file (from legacy to AES-256 encryption). In dictionary attack, default wordlist file is 'andro6.txt' and it can change any other custom wordlist files. In brute-force attack, it can adjust the length of

password (from minimum to maximum). Investigator can set mixing characters such as small letters, capital letters, numbers, and punctuation marks for bruteforcing the password. Table 4.10 describes the different types of zip application for evaluation.

Table 4.10 Different Types of Zip Application for Testing

Application	Operating System Environment	Version	Encryption
WinRAR	Windows 10 Enterprise (64-bits)	5.9.1 (64-bits)	- Legacy - AES 256
BreeZip		1.3.18 (Microsoft store)	
ZArchiver	Android v8.1.0	0.9.3.3	- Legacy - AES 128 - AES 192 - AES 256
Zip (built-in)	Kali Linux 2020.2	3.0	Legacy

The feature of zip password cracker is evaluated on ‘ZArchiver’ application that supports from Android operation system. Currently, this application is widely used, and it can set the password to generate zip file. To generate the password, this application can support four types of encryption method such as Legacy mode, AES-128, AES-192, and AES-256. The zip file password cracker feature can be applied from proposed Androsics tool to decrypt all of these zip files that used the above encryption methods, by enforcing the brute force and dictionary attack approaches. Figure 4.31 shows the appearance of ZArchiver application.

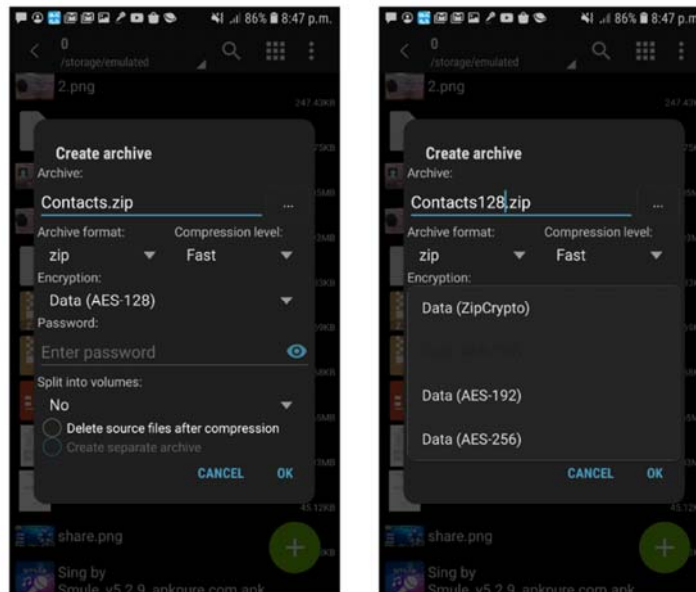


Figure 4.31 Evaluation on ZArchiver Application

Moreover, the experiment on the ‘Breezip’ application is illustrated in Figure 4.32. This application is a popular application that launches on Microsoft store. This is an alternative of ‘Winrar’ application. They only use the AES-256 and there is no encryption option to choose.

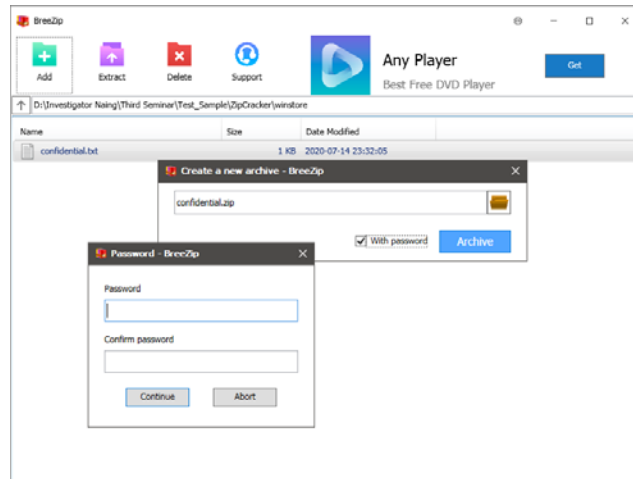


Figure 4.32 Evaluation on BreeZip Application via Microsoft Store

The password cracking process is also studied on ‘Winrar’ application as the mostly used in Windows platform. In this application, the encryption mode like legacy and AES-256 can be chosen as depicted in Figure 4.33.

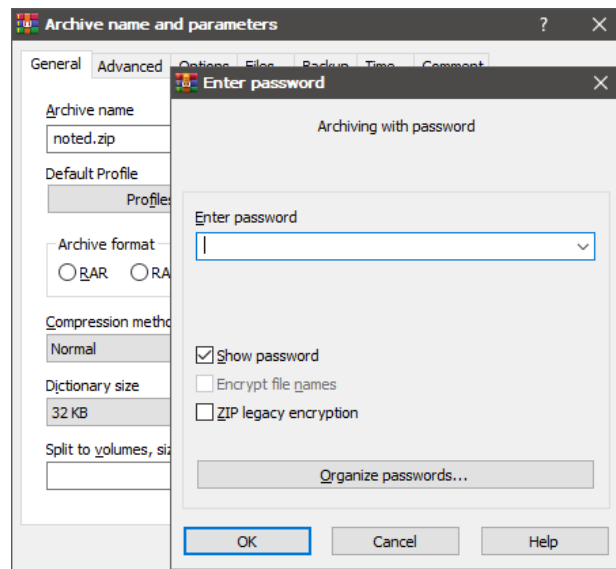


Figure 4.33 Evaluation on WinRAR Application

In Linux platform use the default zip application with legacy mode. Generally, when comparing with other zip file password cracker software, most are commercial

version in Windows application. Even though there are open-source software in Linux platform, they can only use with command line interface. Thus, it is difficult to access for users. In this situation, the proposed Androsics tool intends to support for securing and user friendly with useful and effective features.

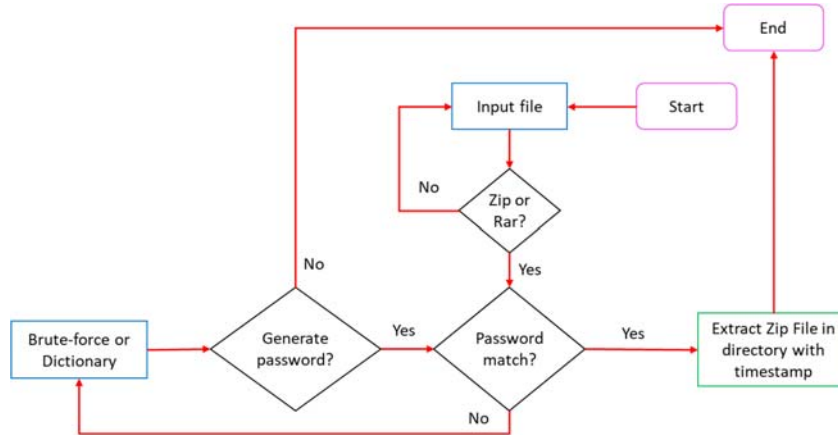


Figure 4.34 The Detailed Process of Zip/Rar Password Cracking Process

The Figure 4.34 shows how the zip/rar password cracking works. First, check if the cracking file type is correct or not. If the file type is correct, choose the Bruteforce or dictionary approach to crack the zip/rar. This cracking process is also the same in Microsoft Office and PDF Password Cracker. The appearance of Zip/Rar cracker feature in Androsics tool is illustrated in Figure 4.35.



Figure 4.35 The Appearance of Zip/Rar Password Cracker in Androsics Tool

4.4.4 Microsoft Office Password Cracker

This section will explain the Microsoft Office file password cracker feature of Androsics tool. Microsoft office files are mostly use in documents process of office affair and education. Additionally, people can use their MS office files with password for confidential or privacy purpose without third-party application. As the growth of technology, this facility may lead to illegally use in crime case. Hence, Androsics tool can support the MS office file password cracker feature for this case. The Microsoft Office file password cracking process is shown in Figure 4.36. The experiment of this feature is done on Microsoft Word, Microsoft PowerPoint, Microsoft Excel of Office 365 (16.0.13001.20266) version.

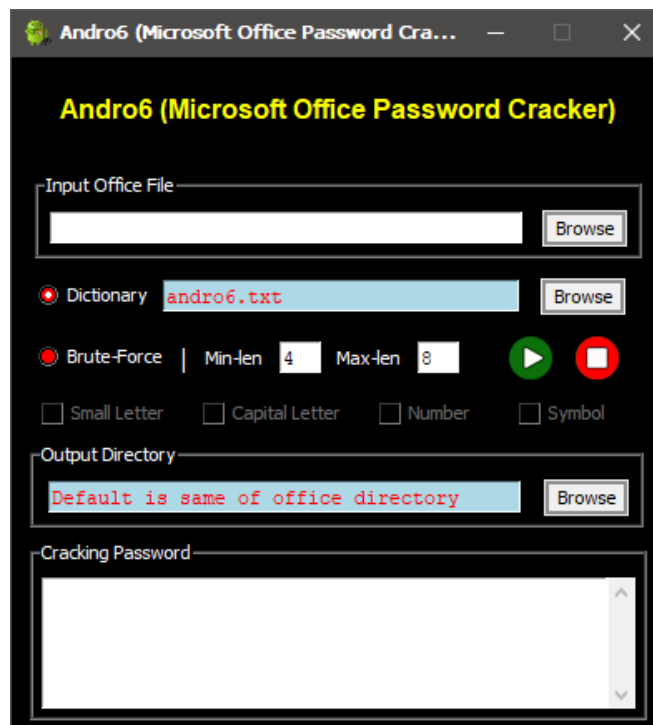


Figure 4.36 Microsoft Office File Password Cracker in Androsics Tool

4.4.5 PDF Password Cracker

This part will briefly discuss the PDF file password cracking process with the help of Brute-Force method. Three different encryption methods RC4, AES 128-bits and AES 256-bit are analyzed on Adobe Acrobat Reader application. They are Acrobat 6.0 And Later (PDF 1.5) with RC4 (128-bits), Acrobat 7.0 And Later (PDF 1.6) with AES (128-bits), and Acrobat X And Later (PDF 1.7) with AES (256-bits). Table 4.11

describes the testing environment for PDF password cracker feature. Figure 4.37 shows the appearance of PDF password cracker feature in Androsics.

Table 4.11 Testing Environment for PDF Password Cracker

PDF Application Name	Operating System	Version	Encryption
Adobe Acrobat Reader	Windows 10 (64-bits)	Acrobat 6.0 And Later (PDF 1.5)	RC4 (128-bits)
		Acrobat 7.0 And Later (PDF 1.6)	AES (128-bits)
		Acrobat X And Later (PDF 1.7)	AES (256-bits)



Figure 4.37 PDF File Password Cracker Feature in Androsics

4.5 Reporting

This part is one of the important things for forensics investigation process. Androsics tool provides reporting feature that generate the report files such as (i) Main Report in Live Forensics Investigation, (ii) Data Viewer Report, (iii) File Analyzer Report, and (iv) SQLite database Report.

4.5.1 Main Report

In Main Report, it contains four subtitle reports – (a) Investigation Summary, (b) Device Information, (c) Data Collection, and (d) Property Information.

(a) Investigation Summary contains the following information.

- Report Creation Time
- Data Collection Tool
- Examiner Name
- Case name
- Case Number
- Case Create Time
- Device Owner
- Department

(b) The Device Information contains the following contents.

- Device ID
- Manufacture
- Model
- Version
- Operator
- Country
- Baseband Version
- IMEI
- Root-Status
- Serial Number
- Bluetooth MAC
- Wifi MAC
- Phone Number
- Up Time
- Time-Zone
- Account
- Applications
- System Applications
- Third-Party Applications

- (c) Data Collection - This report is collecting the data files that includes Data Types, Collect Status, Hash, and Filenames as shown in Table 4.12. It provides easy to check which data is collected or not, and their integrity.
- (d) Property Information – This report contains the detail of device system property information like ac3.decode, af.resampler.quality, audio.decoder_override_check, audio.legacy.postproc, etc.

Table 4.12 Sample of Data Collection Report

01	Screenshot	Yes	5061fb514cef35e150d2ab33b03e84bd	Screenshot (2020-07-27 00-29-59).png
02	Profile Data	Yes	47f4ded664c9e6b105bc21b697299819	data.android6
03	Backup	Yes	b200589a2b04129fc10efb9a46ce49bb	Backup (2020-07-27 00-31-42).ab
04	Activity	No	-	-
05	Network	No	-	-
96	Wi-Fi	Yes	2632af2de7dd11b7ff7fb35b8839b3a6	Wi-Fi (2020-07-27 00-36-06).android6
07	Bluetooth	No	-	-
08	BT_History	No	-	-
09	Memory	Yes	b98aeee4a90a750f643c2ce39f951621	Memory (2020-07-27 00-36-53).android6
10	CPU	No	-	-
11	Process	Yes	ae8e9c8785180480d55918d650c44e66	Process (2020-07-27 00-37-02).android6
12	Account	Yes	26bd6d1b2d1fcd6bf887d4caebace68b	Account (2020-07-27 00-37-08).android6
13	Application	No	-	-
14	Contact Log	No	-	-
15	Call Log	Yes	54de28cb868b7bc7b7e1829d316ab0d5	call_log (2020-07-27 00-37-51).android6
16	SMS log	Yes	bc2af1200ed31188312b38c8986db3e0	sms_log (2020-07-27 00-37-56).android6
17	Uninstall Log	Yes	1f4aea131e71296efd13ecc7496a4662	Uninstall (2020-07-27 00-38-04).android6
18	Dumpsys All	No	-	-
19	LogCat	Yes	b3f3d76f4db616bc3cfdbb6811fad9ba	Logcat (2020-07-27 00-43-16).android6

20	Dumpstate	Yes	3ab68d81473779f51f4d96662ae13297	Dumpstate (2020-07-27 00-42-45).andro6
21	CPU Process	No	-	-
22	Prop: Info	No	-	-
23	Imaging	No	-	-

In Figure 4.38 illustrates the appearance of main report screenshot from Androsics (Andro6) forensics tool suite.

Andro6 (Android Forensics Tool Suite) Report		
<INVESTIGATION SUMMARY>		
01	Report creation time	2020-07-27 01:21:29
02	Data Collection Tool	Andro6 (v2.1)
03	Examiner Name	Investigator Naing
04	Case Name	66D
05	Case Number	x01
06	Case Create time	2020-07-27 00:29:56
07	Device Owner	Myo Ko Ko San
08	Department	CSRL, UCSY
<DEVICE INFORMATION>		
01	Device ID	476E08404FC59604
02	Manufacture	HUAWEI
03	Model	HUAWEI G510-0200
04	Version	4.1.1
05	Operator	MYTEL
06	Country	MYANMAR
07	Baseband Version	G510-0200V100R001C00B173
08	IMEI	868496014004320
09	Root-Status	Rooted
10	Serial Number	4C8BEFB81A01
11	Bluetooth MAC	4C:8B:EF:B8:1A:01
12	Wifi MAC	4C:8B:EF:B8:1A:01
13	Phone Number	9696604569 No SIM

Figure 4.38 Main Report Screenshot

4.5.2 Data Viewer Report

It displays the detailed information of each file from Data Collection Report as shown in Figure 4.39.

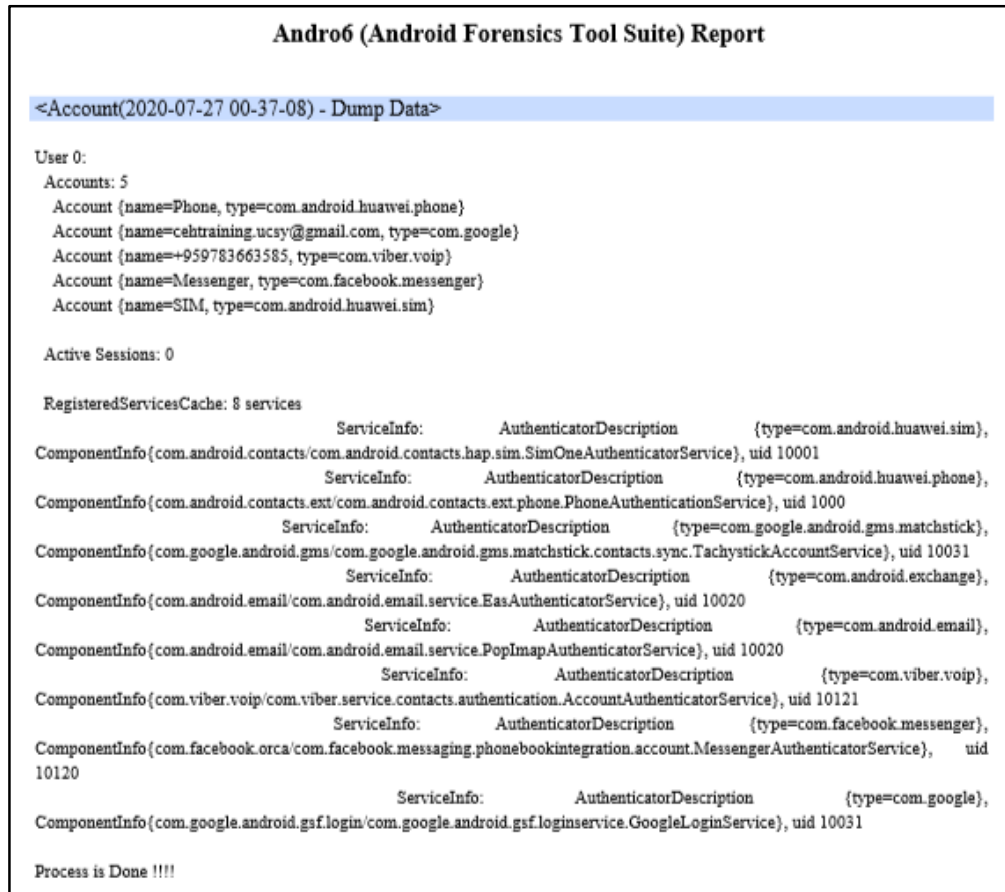


Figure 4.39 Account Information Report (Sample Screenshot)

4.5.3 File Analyzer Report

It provides the two subtitles report - File Summary Report and Specific File Report. In File Summary Report, investigator can check the total number of all file types and specific file type as shown in Figure 4.40. In Specific File Report, investigator can analyze the specific file types such as Filename, Directory, File Size, Recommended File Extension and Type, File Header Code, Status and File Integrity as shown in Figure 4.41.

Andro6 (Android Forensics Tool Suite) Report	
Date: 2020-07-27 01:36:49	
File Summary	
FILE EXTENSION NAME	TOTAL NUMBER
m4a	1
8ec43b0e-ee94-472d-8cf5-4fbc3ddc8fa6	1
0	1
xml	101
sqlite	3
idx	1
properties	1
appid-no-backup	2
json	1
dat	2
meta	25
jpg	52
cls	104
dict	2
db	66
lock	2
ini	2
db-journal	58
nomedia	7
blog	2
zip	5

Figure 4.40 File Summary Report (Sample Screenshot)

ab	
Filename	encrypted(1234).ab
Directory	D:\My Private Tool\File Analyzer\check\
File Size	1.4 GB
File Type	Android adb backup (encrypted)
Header Code	41 4E 44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 41 45 53 2D 32 35 36
Status	True Positive
Integrity	True
Filename	noencrypt.ab
Directory	D:\My Private Tool\File Analyzer\check\
File Size	1.6 GB
File Type	Android adb backup (unencrypted)
Header Code	41 4E 44 52 4F 49 44 20 42 41 43 4B 55 50 0A 35 0A 31 0A 6E 6F 6E 65
Status	True Positive
Integrity	True
png	
Filename	headerchange(FP).png
Directory	D:\My Private Tool\File Analyzer\check\
File Size	11.7 KB
File Type	Relocatable object code
Header Code	80
Status	True Negative
Integrity	Extension Change
Filename	extension_change(TN).png
Directory	D:\My Private Tool\File Analyzer\check\SCENARIO\ZIP\
File Size	146.0 bytes
File Type	Relocatable object code

Figure 4.41 Specific File Report (Sample Screenshot)

4.5.4 SQLite Database Report

In this report, investigator can generate overview report and specific report from SQLite database files. In overview report, it includes all of the database filenames and their directories information as shown in Figure 4.42. In specific report, it describes detailed information of each table from the database file as shown in Figure 4.43.

Andro6(Android Forensics Tool Suite) Report	
Date:	2020-07-28 05:53:04
x04/koko	
Investigator Naing	
SQLite Database Overview Report	
No:	Database_Directory
1	btopp.db D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.bluetooth/db/btopp.db
2	snapshots D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/db/snapshots.db
3	Archived D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Archived History
4	Cookies D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Cookies
5	Favicons D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Favicons
6	History D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/History
7	Shortcuts D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Shortcuts
8	Top Sites D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Top Sites
9	Web Data D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Web Data
10	chrome_n D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Local Storage/chrome_newtab_0.localstorage
11	http_www D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.chrome/r/app_chrome/Default/Local Storage/http_www.arcai.com_0.localstorage
12	alarms.db D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.deskclock/db/alarms.db
13	EmailProv D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.email/db/EmailProvider.db
14	EmailProv D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.email/db/EmailProviderBackup.db
15	EmailProv D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.email/db/EmailProviderBody.db
16	mediacen D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.mediacenter/db/mediacenter.db
17	calendar.c D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.providers.calendar/db/calendar.db
18	download D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.providers.downloads/db/downloads.db
19	external.c D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.providers.media/db/external.db
20	internal.d D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.providers.media/db/internal.db
21	partnerBo D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.providers.partnerbookmarks/db/partnerBookmarks.db
22	user_dict. D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.providers.userdictionary/db/user_dict.db
23	asset_moi D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/asset_module_service
24	auto_upd. D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/auto_update.db
25	counters.c D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/counters.db
26	download D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/download_service
27	fetch_sug D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/fetch_suggestions.db
28	frosting.d D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/frosting.db
29	install_qu D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/install_queue.db
30	install_sei D:/CrimeCase/x04/File_Analysis/Backup/apps/com.android.vending/db/install_service

Figure 4.42 Overview Report of SQLite Database Reader

Andro6(Android Forensics Tool Suite) Report	
Date:	2020-07-28 05:56:00
x04	koko
Investigator	Naing
SQLite Database Report	
Database_Name	: Web Data
Database_Directory	: D:/CrimeCase/x04/File_Analysis\Backup\apps\com.android.chrome\r\app_chrome\Default\Web Data
<Table_List>	
meta	
keywords	
autofill	
credit_cards	
autofill_dates	
autofill_profiles	
autofill_profile_names	
autofill_profile_emails	
autofill_profile_phones	
autofill_profiles_trash	
logins	
web_app_icons	
web_apps	
token_service	
web_intents	
web_intents_defaults	
keywords_backup	
<Table_Name: meta>	
key	value
version	44
last_comp	44
Default Se	2
Default Se	2
Default Se z(Ç`llP▲	
Built-in Ke	38

Figure 4.43 Specific Report of SQLite Database Reader

4.6 Management

In this section, it provides to protect and trace for investigation processes that includes Tamper Protection with Secret Key, User Account Management, and Logs. Tamper Protection with Secret Key, administrator can set a secret key with one character anytime. It can protect unauthorized user to access login feature from tampering. The computer screen is locked, and user will see live black screen with binary number after launching the Androsics tool as shown in Figure 4.44. In this feature, user can attempt to press a secret key with three times. Once user press a correct key, he will see account login feature as shown in Figure 4.45. If user press incorrect key all three times, it will take photo from webcam automatically.



Figure 4.44 Tamper Protection with Secret Key

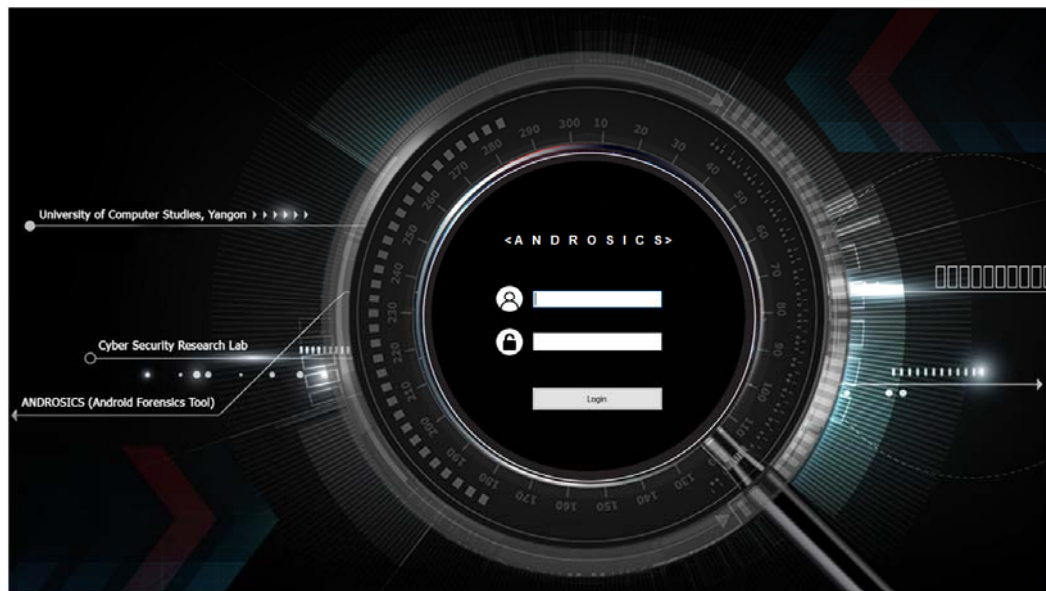


Figure 4.45 User Account Login Feature

In User Account Management feature, administrator can create user accounts for accessing the Androsics tool. He can also check users list and remove any user as shown in Figure 4.46. In Management settings, other users can access only password update feature.

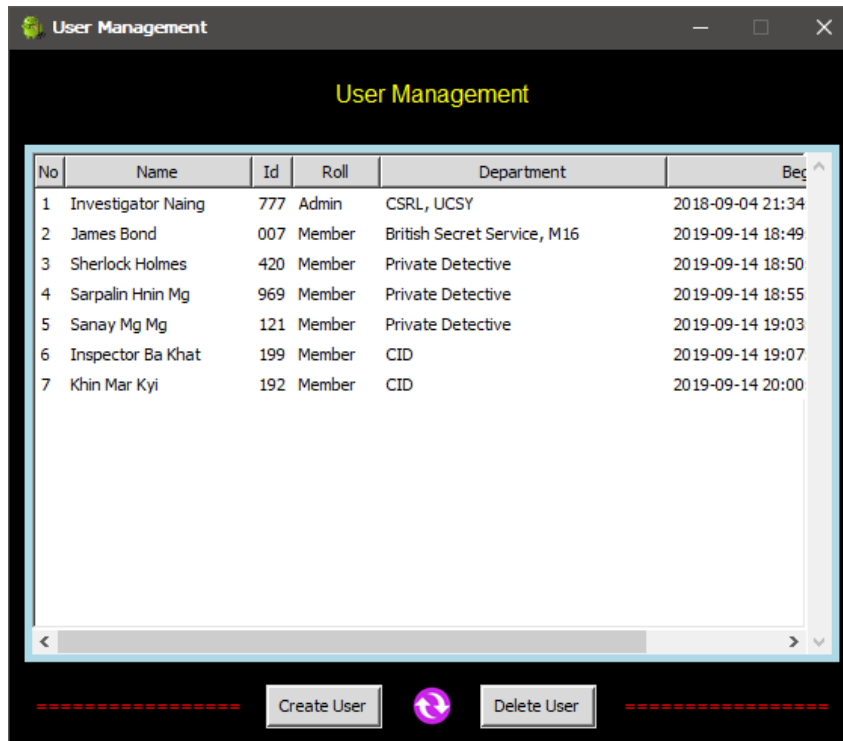
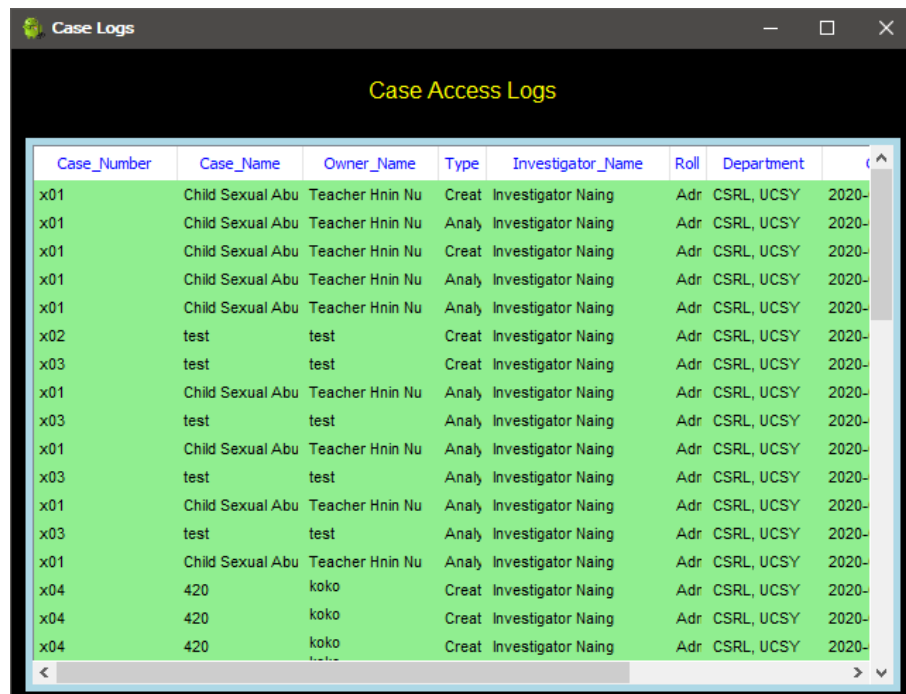


Figure 4.46 User Management Feature

Logs feature includes Case logs and Detail logs. Administrator can check the case information in Case logs that provides Case number, Case name, Device owner name, Case type, Investigator name, Investigator roll, Department, Timestamp and Case directory as shown in Figure 4.47. In Detail logs, it can analyze who is performed any activity and process in Androsics tool. Administrator can be easy to know investigator name and his all activities with timestamp as shown in Figure 4.48.



The screenshot shows a window titled "Case Logs" with a sub-header "Case Access Logs". Below the header is a table with the following columns: Case_Number, Case_Name, Owner_Name, Type, Investigator_Name, Roll, Department, and a date column. The table contains 20 rows of data, with the first 15 rows having Case_Number x01 and the last 5 rows having Case_Number x04.

Case_Number	Case_Name	Owner_Name	Type	Investigator_Name	Roll	Department	
x01	Child Sexual Abu	Teacher Hnin Nu	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x02	test	test	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-
x03	test	test	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x03	test	test	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x03	test	test	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x03	test	test	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x01	Child Sexual Abu	Teacher Hnin Nu	Analy	Investigator Naing	Adr	CSRL, UCSY	2020-
x04	420	koko	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-
x04	420	koko	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-
x04	420	koko	Creat	Investigator Naing	Adr	CSRL, UCSY	2020-

Figure 4.47 Case Access Logs



The screenshot shows a window titled "Detail Logs" with a sub-header "Detail Logs". Below the header is a table with the following columns: Name, Activity, and Timestamp. The table contains 17 rows of data, all for the user "Investigator Naing", showing various activities like "Log in", "Live Forensics", "Power", "Swipe", "Backup", etc., with timestamps from 2020-02-06.

Name	Activity	Timestamp
Investigator Naing	Log in	2020-02-06 17:42:43.587820
	Live Forensics :4C8BEFB81A01	2020-02-06 17:43:09
	Power	2020-02-06 17:43:47
	Swipe	2020-02-06 17:43:51
	Backup	2020-02-06 17:45:46
	New Screenshot	2020-02-06 17:46:36
	Key tab	2020-02-06 17:46:47
	Key tab	2020-02-06 17:46:50
	Key Enter	2020-02-06 17:46:52
	MTP Mode	2020-02-06 17:47:45
	Key home	2020-02-06 17:47:57
	Backup	2020-02-06 17:48:25
	Key back	2020-02-06 17:48:33
	Key Enter	2020-02-06 17:48:40
	Key tab	2020-02-06 17:48:44
	Key Enter	2020-02-06 17:49:05
	Key tab	2020-02-06 17:49:06

Figure 4.48 Detail Logs

4.7 Additional Features

As additional features, this proposed tool provides Android device management and Cryptography. In Android device management, it contains Virtual keys and keyboard, Root checker, Connection mode, Services control, Command Box and Screen lock remover. In Cryptography, it includes Hash calculator, Encode and Decode, Substitution cipher, Modern cipher, Hex Viewer, Steganography and PNG dimension fixer.

4.7.1 Android Device Management

Virtual keys and keyboard: It provide to push the Android button keys (Volume up/down, Airplane mode, Power, Swipe, etc.) and keyboard keys (Characters, numbers and symbols) without touching on device.

Root checker: it can check Android device is rooted or not.

Connection mode: It can use ADB Wi-Fi connection to connect from computer to Android device as shown in Figure 4.49. And it can set MTP (Media Transfer Protocol) mode for imaging process and Power stay awake mode for screen will never sleep while charging.

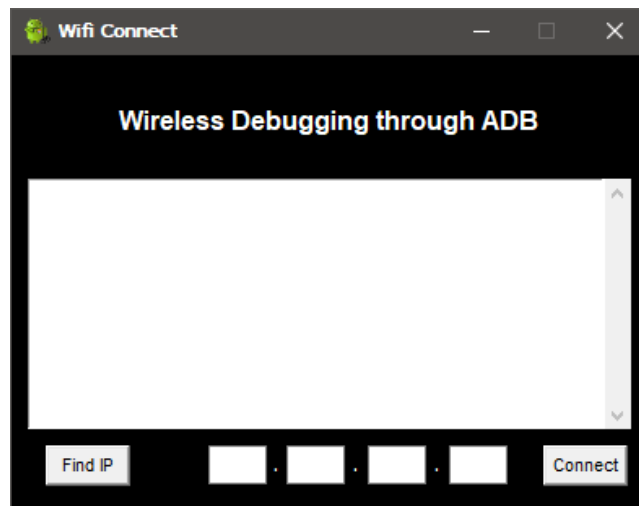
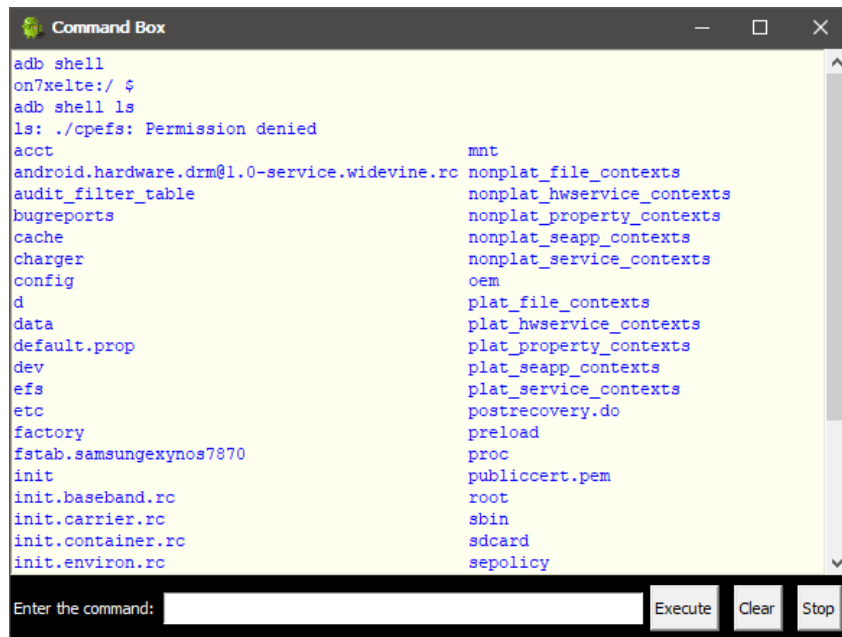


Figure 4.49 Wireless Debugging through ADB

Services Control: it can enable or disable Mobile data, Bluetooth, and Wi-Fi services.

Command Box: it provides to run ADB utility commands for Administrator such as adb devices, adb shell, etc. as shown in Figure 4.50.



The screenshot shows a window titled "Command Box" with a list of files and directories returned by an ADB shell command. The files are listed in two columns. At the bottom, there is an input field labeled "Enter the command:" and three buttons: "Execute", "Clear", and "Stop".

```
adb shell
on7xelte:/ $
adb shell ls
ls: ./cpefs: Permission denied
acct                                mnt
android.hardware.drm@1.0-service.widevine.rc nonplat_file_contexts
audit_filter_table                 nonplat_hwservice_contexts
bugreports                         nonplat_property_contexts
cache                             nonplat_seapp_contexts
charger                           nonplat_service_contexts
config                             oem
d                                 plat_file_contexts
data                              plat_hwservice_contexts
default.prop                       plat_property_contexts
dev                               plat_seapp_contexts
efs                               plat_service_contexts
etc                               postrecovery.do
factory                           preload
fstab.samsungexynos7870           proc
init                              publiccert.pem
init.baseband.rc                  root
init.carrier.rc                   sbin
init.container.rc                 sdcard
init.environ.rc                   sepolicy
```

Figure 4.50 Command Box

Screen lock remover: It can remove the screen lock such as Pattern, Pin, Password on Android.

4.7.2 Cryptography

Hash Calculator: It provides to check data integrity that can generate hash string from three data types (Text String, Hex String and File). It used popular hash algorithms such as MD5 (Message-Digest Algorithm 5), SHA1 (Secure Hash Algorithm 1), SHA224, SHA256, SHA384 and so on as shown in Figure 4.51.

Encode and Decode: It used some encode/decode method such as Base32, Base58, Base64, Base85, Octal, Hexadecimal, Binary and Decimal as shown in Figure 4.52.

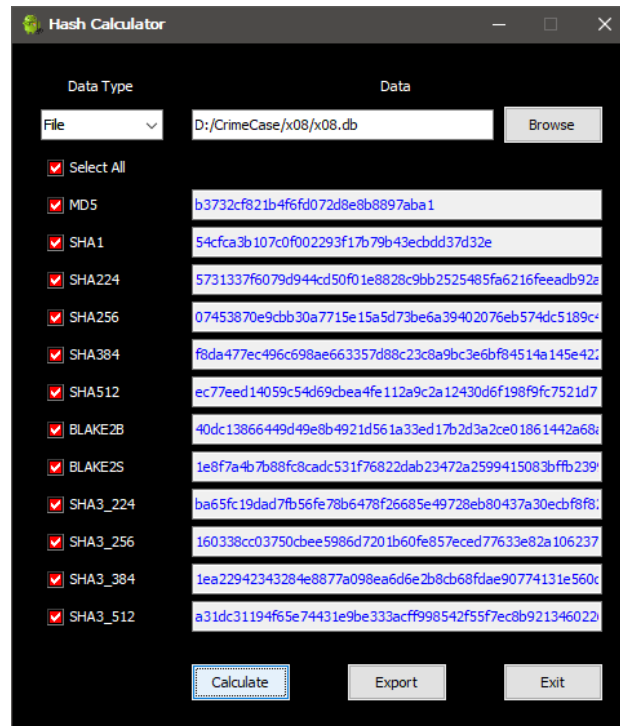


Figure 4.51 Hash Calculator

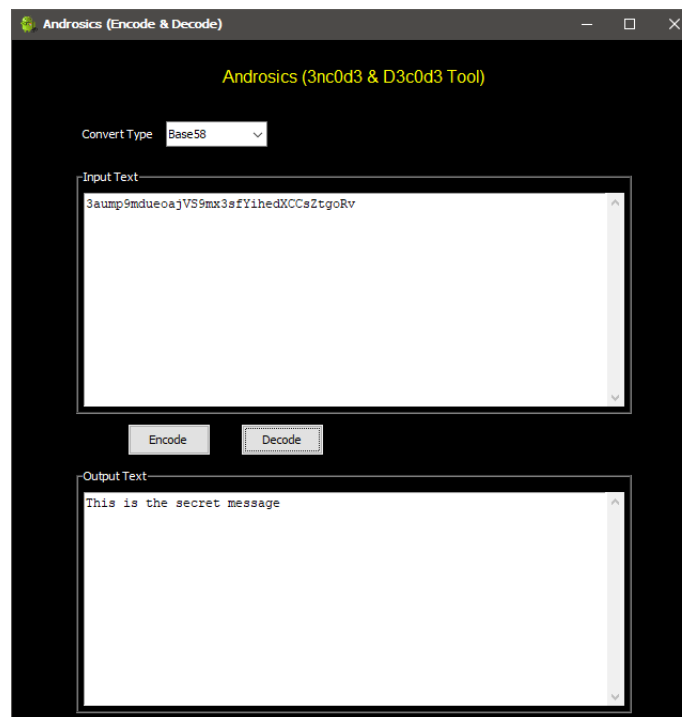


Figure 4.52 Encode and Decode Feature

Substitution Cipher: It provides some substitution ciphers such as Caesar, Vigenere, Rot13, Monoalphabetic and Atbash as shown in Figure 4.53.

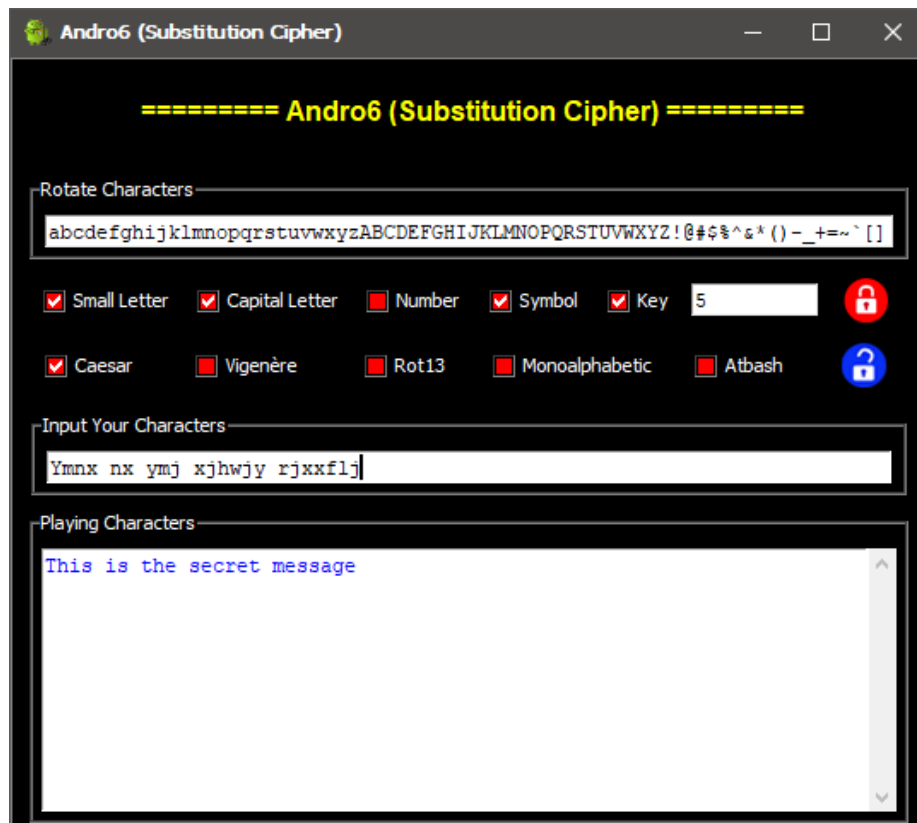


Figure 4.53 Substitution Cipher

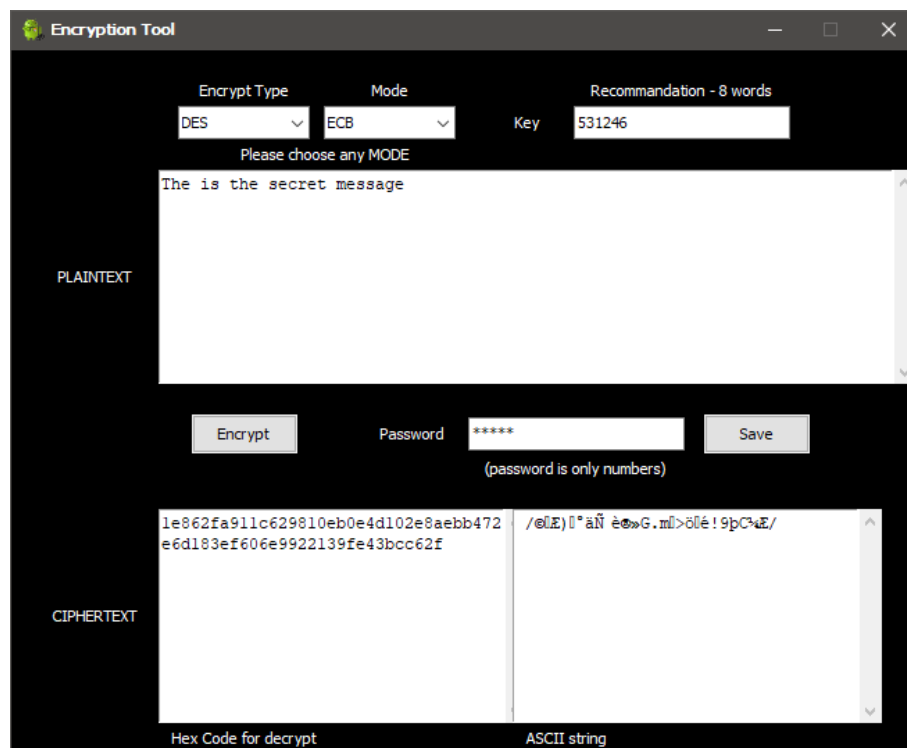


Figure 4.54 Encryption Feature

Modern cipher: Investigator can use this feature to prevent unauthorized users from reading confidential data. It supports DES (Data Encryption Standard), DES3, AES (Advanced Encryption Standard), ARC2 (Rivest Cipher), ARC4, etc. and block modes depend on their encryption algorithms. It used common modes such as electronic codebook (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB) and so on. Figure 4.54 describes the Encryption feature and Figure 4.55 illustrates the Decryption feature that support in Androsics.

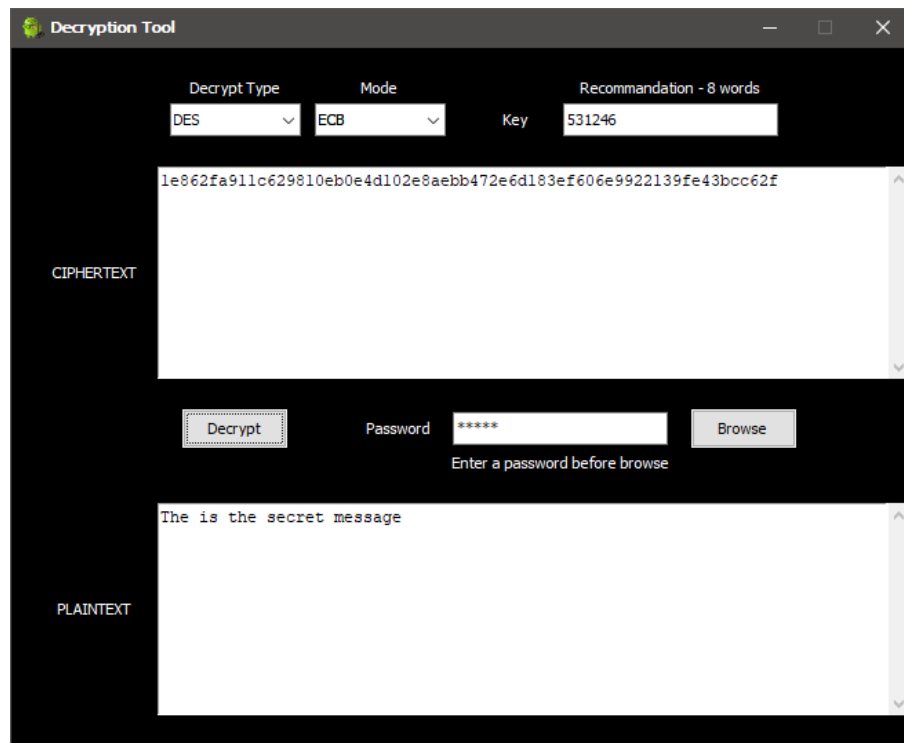


Figure 4.55 Decryption Feature

Hex Viewer: It can check if a file contains more than one signature, and it can fix the signatures as shown in Figure 4.56.

Steganography: It uses Least Significant Bit (LSB) method to extract hidden data from PNG image as shown in Figure 4.57.

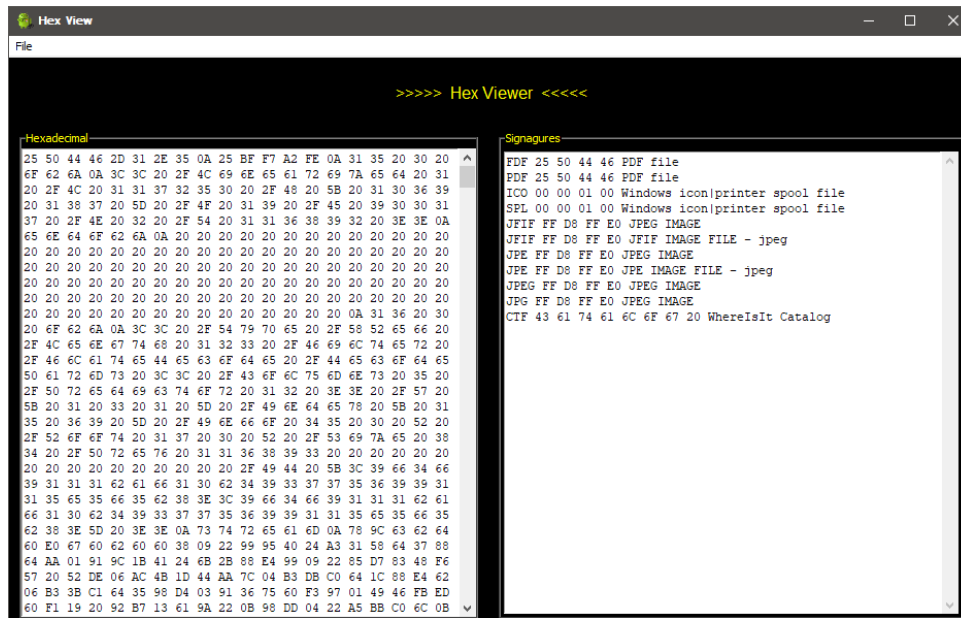


Figure 4.56 Hex Viewer



Figure 4.57 Steganography (LSB)

PNG dimension fixer: It provides to fix the incorrect or missing dimension of image file. There are two methods for fixing the image dimension namely, Dimension Fixer and Force Generate Files. In Dimension Fixer, it used brute force technique for width and height in IHDR chunk that check for matching with CRC checksum. In Force Generate Files, it doesn't need to check CRC checksum that generate the PNG files for each brute force width and height. The detail process of PNG dimension fixer is described in Figure 4.58. The appearance of using image dimension fixer feature in Androsics tool is exemplified in Figure 4.59.

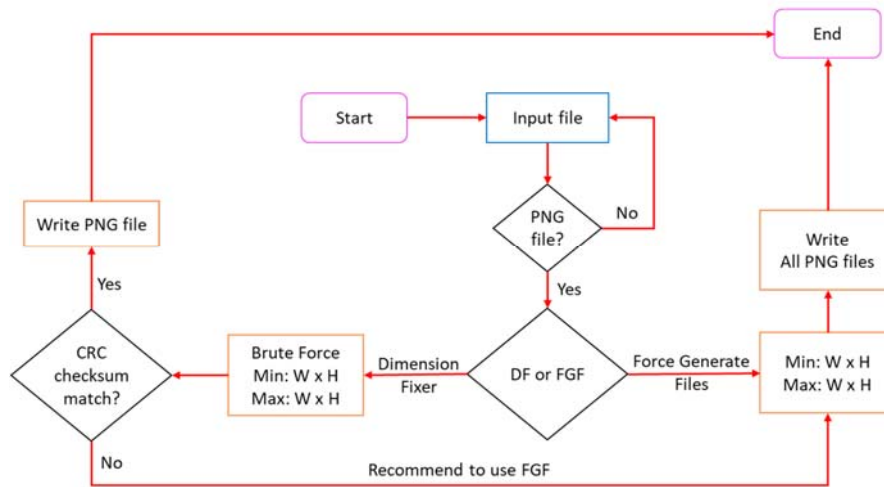


Figure 4.58 The Detailed Process of PNG Dimension Fixer

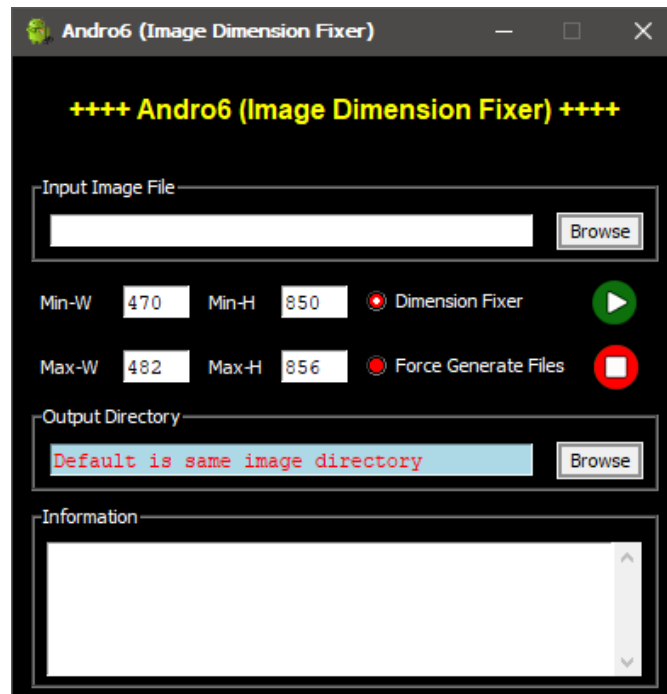


Figure 4.59 The Appearance of Image Dimension Fixer in Androsics Tool

4.8 Comparison

In this section, the comparison of some forensics tools and ANDROSICS tool suite will be described. This comparison is based on a reference review paper and add the features of Androsics to measure the performance. It analyzed on eight main features, namely, open source, user friendly, Bypass screen lock, integrity, partition, export data, support forensics phases and generic. It is set to ‘Yes’, ‘No’, ‘High’ degrees, depending on which feature the tool supports as reported in Table 4.13. This evaluation is rooted on a reference “F. Kausar and T. N. Alyahya, ‘Analysis of Physical Image Acquisition Forensic Tools for Android Smartphones’, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.11, November 2016” [19].

Table 4.13 Comparison of Some Forensics Tools and Proposed ANDROSICS

Forensics Tool	Open Source	Friendly	Bypass Screen Lock	Integrity	Partition	Export Data	Support Forensics Phases	Generic
LiME	Yes	No	No	High	No	TCP/SD	No	No
AMExtractor	Yes	No	No	High	No	TCP	No	No
APD	No	No	Yes	Yes	Yes	No	No	No
Hawkeye	No	No	No	Yes	Yes	No	No	No
ANDROPHSY	Yes	Yes	Yes	Yes	Yes	TCP	Yes	Yes
ADA	Yes	No	No	Yes	No	SD	No	No
UFED	No	Yes	Yes	Yes	No	SD/Flash	Yes	No
Oxygen	No	Yes	Yes	Yes	No	USB/Blu:	Yes	No
MSAB XRY	No	Yes	Yes	Yes	No	USB	Yes	No
DS	No	Yes	Yes	Yes	No	USB	Yes	No
MOBILedit!	No	Yes	No	Yes	No	USB/TCP	Yes	No
ViaExtract	No	Yes	Yes	No	No	No	Yes	No
MPE+	No	Yes	Yes	No	No	Cable/Blu:	Yes	No
ANDROSICS	Yes	Yes	Yes	High	Yes	USB/SD/TCP	High	No

Open-source tool is a tool that can use for free of charge. They are ADA, LiME, ANDROPHSY and AMExtractor. There are many forensics tools that have been developed for commercial use. These commercial tools are too expensive and cannot be used for evaluation in this research. Therefore, the proposed Androsics tool has been compared based on the evaluation of a reference paper. The Androsics tool is also an open-source tool because it is implemented for non-profit purpose.

User Friendly is mainly based on graphical user interface (GUI) and command-based. Mostly, commercial tools have a well-designed interface that is easy to use in multiple languages. The Androsics tool is designed to make the interface simple and

easy to use. Especially, it emphasizes the local requirements in Myanmar, and represents the complicated matter with Myanmar language clearly. Thus, the author believe that the process will be user-friendly.

Android devices usually have a screen lock such as gesture pattern, pin and password. In reference paper, they considered not only the Bypass Screen-Lock, but also the acquisition. Both this Bypass Screen-lock and acquisition (imaging) require USB debugging enabled, rsa key access, and root access. The proposed Androsics tool provides two types of bypass screen lock features, namely, deleting the lock file and decoding it. In this research, the Androsics tool well supports the devices that use the geture.key and password.key for decoding. However, the decoding of Gatekeeper versions will be considered as the future work.

The data collection section uses the hashing algorithm to generate checksum values for better integrity and validates whether the collected data has been modified or manipulated for later analysis. The Androsics tool provides the md5 checksum value that allows to verify all volatile data, screenshots, backups, and imaging files. The partition section mainly focuses on the physical acquisition process. Only the physical acquisition can support the recovery process. Thus, the Androsics tool uses the dd utility to copy bit-by-bit that enables to imaging the logical partitions as well as the physical partitions.

Export data compares whether it can work with USB connection, SD card, Wi-Fi connection for storage. The Androsics tool uses the USB connection or Wi-Fi connection to store dump files, backup and screenshot files on a PC or Laptop. The imaging process will be saved via SD card. The support forensics phase compares whether it provides the data acquisition, analyzing and reporting features in forensics investigation process. The Androsics tool is based on the forensic process flow and analysis framework. Thus, it provides data acquisition, analysis, reporting, as well as management and Brute force. The Genric section compares the availability of different Android devices versions and models. Androsics tool is mainly supported for Samsung and Huawei devices. There may be differences in other versions and models to perform some processes when collecting dump data.

Furthermore, the comparison of other tools has also been done based on the supporting features of Androsics tool. This comparison is based on five key areas, namely, data collection, examination and analysis, Bruteforcing, management and reporting that have been implicated in research. As shown in Table 4.14, the proposed

Androsics tool are evaluated with Autopsy, Andriller, UFED (Demo), AFLogical and FTK Imager free version.

Table 4.14 Comparison of Other Tools based on the Support Features of Androsics

Andro6		Autopsy	Andriller	UFED (Demo)	AFLogical	FTK Imager (free version)
Data Collection	Volatile acquisition	No	No	Yes	No	No (for android)
	Logical acquisition		Yes	Yes	Yes	
	Physical acquisition		No	Yes	No	
Examination and Analysis	File Signature	Yes	No	No	No	No
	PNG Dimension Fixer	No				
Bruteforcing	Wordlist Creator	No	No	Yes (no rules)	No	No
	Screen Lock Decoder		Yes	Yes		
	File Password Cracker		No	No		
Management	Tamper Protection	No	No	No	No	No
	Logs					
Reporting	Live and Static	Yes	Yes	Yes	No	No

In this comparison, the data collection section is based on the volatile acquisition, logical acquisition, and physical acquisition. The volatile acquisition will collect dump service information, screenshots, and current status. The logical acquisition will process full backup and the physical acquisition will do the imaging process. The autopsy (v4.14.0) does not provide any data acquisition. In Andriller (Trail v2.6.1) and AFLogical (v1.5.2), only logical acquisition is possible. The UFED Cellebrite Tool (Demo v7.48-CTF version) provides all three acquisitions. The FTK Imager (free v4.3.0.13) focuses on the computer and performs the acquisition process. In data collection process, the proposed Androsics tool provides all three acquisitions.

In examination and analysis section, it compares based on the file signature and PNG dimension fixer. File signatures use a confusion matrix to determine the file status by matching the file header (signature) with the extension. File formats with extension have four statuses, and file formats without extension have three statuses. The PNG dimension fixer solves the dimension manipulating problem in PNG files using Force Generate File (FGF) and Dimension Fixer (DF) algorithm. Autopsy (v4.14.0) provides only the file signature feature for analysis, but the PNG dimension fixer is not provided. Other tools such as Andriller, UFED, AFLogical, and FTK imager provide other analysis processes, but file signature and PNG dimension fixer are not provided.

In Bruteforcing, comparison is based on the wordlist creator, screen lock decoder and file password cracker (PDF, Microsoft files, Zip and Rar). The Andriller tool can only provide the screen lock decoder. The UFED tool provides a screen lock

decoder; and wordlist can be generated based on user information from the phone, but not by rules. Autopsy, AFLogical and FTK imager tools do not support Bruceforcing.

The management section is based on the Tamper Protection and Logs. The Tamper Protection can detect an unauthorized user with a secret key. It also provides credential access and protection for the unauthorized user. Logs are used to review the user activities and case history. All five comparison tools do not provide this management feature. In the reporting part, the Androsics tool can generate both live and static reports. The Autopsy and Andriller can only report on static sections. The UFED tool provides both live and static reports. However, the AFlogical and FTK Imager did not work in the Report section.

4.9 Sample Scenario

Androsics tool provided the investigation process to analyze and extract the evidence data for stalking crime case in real world. However, it is difficult to describe the confidential information related to the crime that hides it in this dissertation.

Case overview – A forensics service company contact me, and they want me to help their investigation process follow by their status:

“My client is being stalked by her x-husband and she thinks that he loaded malware and was tracking her etc. I am going to be putting together a forensics report for her to submit to the courts. So, your findings I’ll be using for my report. If you have any questions let me know once you accept the job, I’ll send the backups”

The backup process uses the Andriller tool, which collects only application data. Thus, it just needs to analyze the backup file that includes application data. With Androsics tool, it also provides the backup feature which can collect not only application data but also applications and phone storage. The detail crime investigation environment is described in Table 4.15.

Table 4.15 Crime Investigation Environment

Artifact	Description
Collected data	Backup file
Data acquisition tool	Andriller Tool
Analysis tool	Androsics tool and Manual
Device	SAMSUNG-SM-N910A

First, all application data in the verify_apps.db file is checked using Androsics (SQLite Reader), as shown in Figure 4.60. Next, find out which application has tracking capabilities. Within the applications, the Map My Run and Google Maps are suspected to have the tracking functions in this crime scene. Therefore, these two applications are highlighted in this investigation. Table 4.16 shows the main directories for the Map My Run and Google Maps applications on Android.

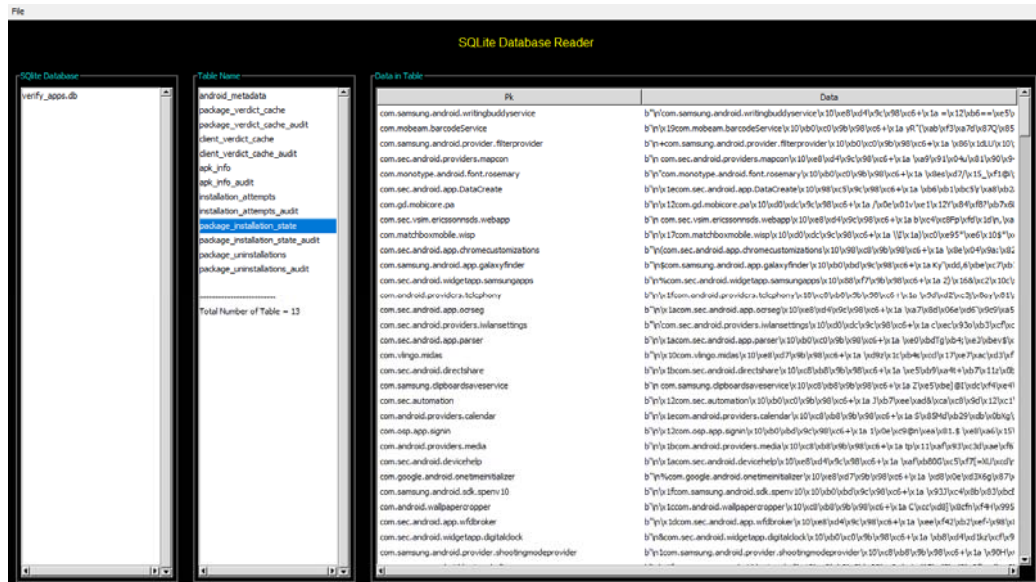


Figure 4.60 View of Application Lists in SQLite Database Reader

Table 4.16 Main Directory of Map My Run and Google Maps Application

Artifact	Main Directory
Application List	com.android.vending
Map My Run	com.mapmyrun.android2
Google Maps	com.google.android.apps.maps

Map My Run – it is an application which is use for fitness purpose. Although it is a legit application, it can be abused to track user's location and movement. The appearance of May My Run application is shown in Figure 4.61. At that time, the investigation found that the account use for the application is not the client or victim email, it is used her x-husband email as shown in Figure 4.62.

Google Maps – It is also a legitimate application used for navigation and location tracking. Same as the application above, the application itself is legal and harmless. However, as shown in Figure 4.63, the application was logged in with the client / victim's x-husband account.

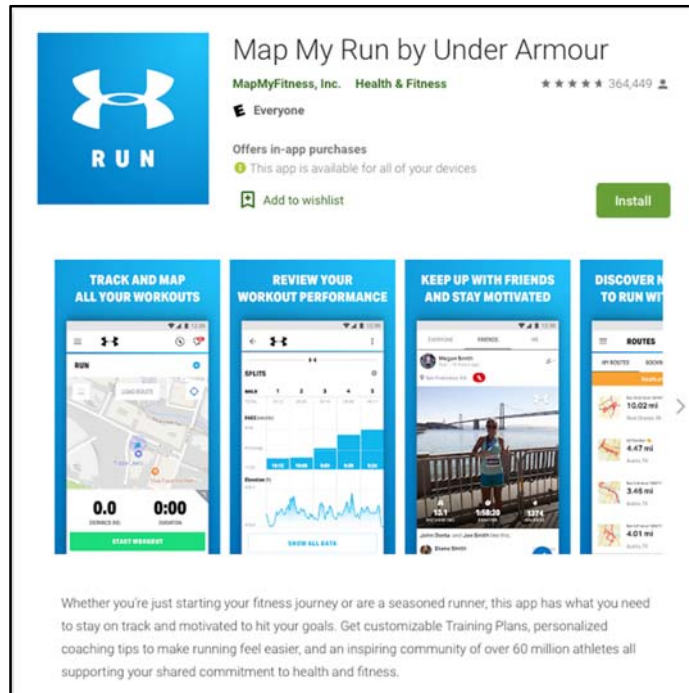


Figure 4.61 The Appearance of Map My Run Application

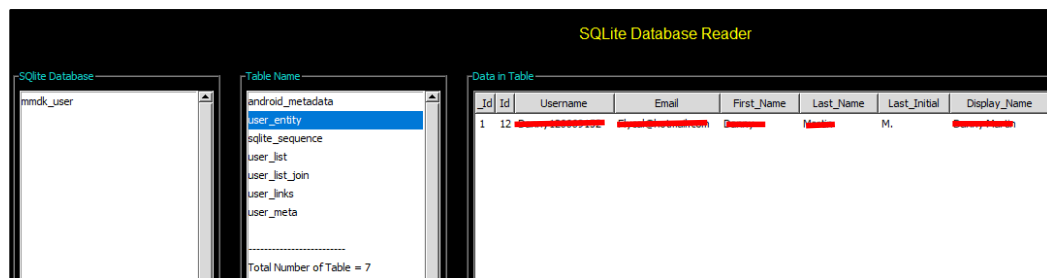


Figure 4.62 Evidence Data in Database File of Map My Run Application

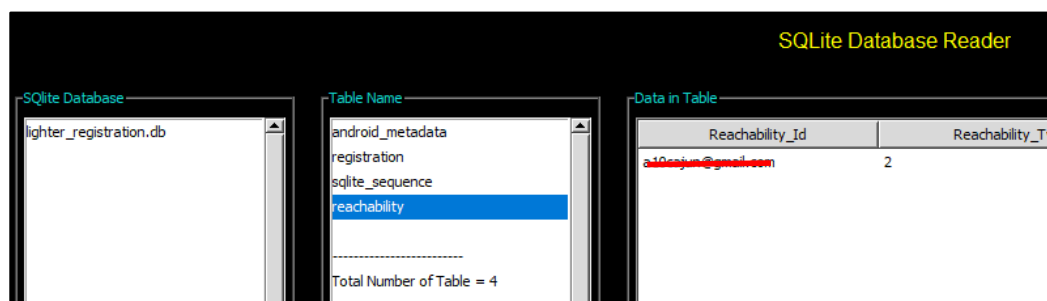


Figure 4.63 Evidence Data in Database File of Google Maps Application

Google Maps application has another feature that allows to track all location history with timeline information. Figure 4.64 described the client's x-husband email account was logged in to Google Maps application and enabled the timeline tracking feature.

```

<boolean name="checked_north_up_preferred" value="true" />
<long name="traffic_hub_add_home_work_promo_first_create_count" value="1" />
<boolean name="timeline_email_opt_out" value="true" />
<int name="offline_initialization_crash_count" value="0" />
<long name="smartspace_commute_notification_last_disabled_timestamp$108610172792089179962" value="1592517053034" />
<boolean name="area_traffic_notification" value="true" />
</map>

```

Figure 4.64 The Configuration of Timeline Tracking Feature

For this scenario, the artifacts from Map My Run and Google Maps mentioned above were sufficient for the Android forensics investigation. The directories of the important files are "apps\com.mapmyrun.android2\db\mmdk_user" in Map My Run. For Google Maps application, the important artifacts are located in "apps\com.google.android.apps.maps\db\lighter_registration.db" and "apps\com.google.android.apps.maps\sp\settings_preference.xml". This scenario was based on the real stalking crime case and the findings using Androsics tool were enough for reporting to court.

4.10 Summary

This chapter delivered the implementation of proposed ANDROSICS tool suite in detail. ANDROSICS tool was based on the open-source tools, freeware tools, trial versions of commercial tools, ADB utility tools, and nature of forensics. First, the test environment was described in this section, such as preparing for USB debugging mode, tamper protection, and creating case tickets. Next, the data collection process to extract the backup data, device profile, dump data, log data, imaging physical or logical storage from suspected mobile device was demonstrated in detail. After the data acquisition process, the examination and analysis process were presented that provides four key functions: Data Viewer, Backup Extractor, File Analyzer, and SQLite Reader. Brute Forcing is one of the essential things in forensics investigation process. Thus, the ANDROSICS tool provides the Brute Force capabilities for cracking the password that includes wordlist creator, Android screen lock decoder, Zip/Rar password cracker and Microsoft Office file password cracker. The tool also supports management, reporting and additional features such as root checker, services control, hash calculator, encode and decode, Steganography, PNG dimension fixer and so on. In reporting, it generates (i) Main Report in Live Forensics Investigation, (ii) Data Viewer Report, (iii) File Analyzer Report, and (iv) SQLite database Report. In addition, the comparison of some forensics tools and proposed ANDROSICS tool suite was demonstrated. The next chapter describes the conclusions of this study, some limitations, and future work.

CHAPTER V

CONCLUSION AND FUTURE WORK

This research has proposed the necessary process flow, analysis framework and tools to do the investigation process successfully for forensics organization. The proposed process flow is based on the standard process flow from NIST and employed more efficient, simple and effective stages. Especially, the implementation of the process flow starting from the crime scene until the reporting process to court has been done for our country, Myanmar, flexibly. It includes seven stages – (1) Preparation, (2) Determine Scope of Crime Scene, (3) Secure Evidence Devices Collection, (4) Documentation and Preservation, (5) Examination and Analysis, (6) Presentation, and (7) Review.

In this process flow, the analysis framework has been proposed to support the examination and analysis stage. Moreover, the detailed step by step process of how to communicate with Android device, how to collect the data and how to do the analysis is performed in this proposed framework. It mentioned two main parts – device screen lock is inactive and active mode for device screen lock conditions. This framework focused on not only the technical view but also the policies and rules for investigation.

For the analysis section, the Androsics tool has also been proposed. In this tool, many valuable and useful features were developed for forensics investigation process. The required process in real-world is mainly solved by evaluating the methods and techniques for these features. It provided five main categories – (1) Data Collection, (2) Examination and analysis, (3) Brute Forcing, (4) Reporting, and (5) Management processes.

In data collection process, ANDROSICS tool extracted screenshots with PNG extension, all dump data (volatile) with andro6 extension, backup file with ab extension and imaging files (included logical and physical) with ‘img’ extension. In examination and analysis process, it provided three main features, namely, Data Viewer, File Analyzer and SQLite Reader. In Data Viewer, it used pattern matching method for keyword searching. In File Analyzer, it used confusion matrix for alerting file statuses that defined tampering signature, manipulating extension, and corrupted or not. The SQLite Reader is used to explore and analyse the database files with read only mode for forensically sound condition. In Brute forcing process, it used the permutation and combination algorithms for generating the passwords depending on

the requirements. In reporting process, it supported live forensics and dead forensics reports that can also generate the specific information for potential artifacts. In management process, this tool provided the user management, access control management, crime case management and Logs. It analysed various data on differences android devices. According to the experiments, it found some interesting directories and artifacts for evidence information as shown in Table 5.1 and Table 5.2.

Table 5.1. Interesting Directories for Evidence Information

Information	Directory
Browser History	data/data/com.android.browser/database/browser2.db
Internet History	data/data/com.android.browser/database/webview.db
Call Log	data/data/com.android.providers.contact/database/contacts2.db
Calendar	/data/com.android.providers.calendar/databases/calendar.db
Wi-Fi Network	/data/misc/wifi/wpa_supplicant.conf
Hotspot	/misc/wifi/softap.conf
Downloads	/data/com.android.providers.downloads/databases/downloads.db
Contacts	/data/com.google.android.gms/databases/icing_contacts.db
SMS/MMS	/data/com.google.android.gms/databases/icing_mmssms.db
Maps	/data/com.google.android.apps.maps/databases/da_destination_history

Table 5.2. Interesting Artifacts Data for Evidence Information

Application Name	Main Folder	Interested Folder	Interested File	Artifacts Data
Viber	com.viber.voip	db	viber_messages	Phone no, Name, ID, Messages, Media info
Internet Browser	com.android.browser	Local storage	0000000000 000001.db	Contacts, Messages, History, Cache, ID

Google Chrome	com.android.chrome	Database and Default	History and https_m.facebook.com_0.db	Account, ID, Bookmark, Chat, Cache
Gmail	com.google.android.gm	databases	mailstore.xxxxxxx@gmail.com	Conversation, ID, Address
Messenger	com.facebook.orca	databases	threads_db2 and tincan_db_100015308449141	Username, ID, User key, messages, event

5.1 Benefits of the Research

There are fundamentally some major reasons why so much research and effort has been made by doing the Android forensic process.

- It is useful for the section of Cybercrime investigation in Myanmar.
- If a countrywide tool in forensic process is available, the investigator does not need to care about the sanction problem.
- It may reduce the cost on account of without buying an expensive license tool.
- It is easy to modify and support flexible.
- It can be user friendly.
- It can provide more convenience and appropriate functions because it is based on the countrywide necessity features.

5.2 Limitations of the Research

Although this research is done to fulfil the requirement as far as possible, there is some limitations and still need to improve. Especially, Since Myanmar is a developing country, too much practical experiments cannot be supported with related materials on this research. There are not many Android devices for testing. Thus, the experiments are only done on a few popular brands for testing devices. As Android technology is rapidly changing in recent days, this present work still needs to develop. It is hoped that this research will be the best even through there were many constraints of time and money.

5.3 Future Work

There are some challenging parts beyond the current proposed work. As the future work, it is necessary to do the part of Steganography more completely. The reason why is steganography is gradually widespread use in the forensics area. Moreover, the investigating process demands the features for supporting OSINT, recovering the deleted files, mounting the image techniques. In addition, the feature of malware analysis, reverse engineering and others will be carried out in the future.

AUTHOR'S PUBLICATIONS

- [P1] Naing Linn Htun, Mie Mie Su Thwin, “Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation”, International Journal of Engineering and Science **(IJES)**, Volume 6, Issue 1, pp. 82-92, 2017.

- [P2] Naing Linn Htun, Mie Mie Su Thwin, “Proposed Applicable Android Forensics Tool Suite (ANDROSICS) for Cybercrime Investigation in Myanmar”, Conference on Science and Technology Development, Defense Services Academy **(DSA 2017)**, Pyin Oo Lwin, Myanmar, November, 2017.

- [P3] Naing Linn Htun and Mie Mie Su Thwin, “Forensics Investigation on Android Social Applications”, In Proceedings of the 16th International Conference on Computer Applications **(ICCA 2018)**, Yangon, Myanmar, pp. 273–279, February 22-23, 2018.

- [P4] Naing Linn Htun, Mie Mie Su Thwin and Cho Cho San, “Evidence Data Collection with ANDROSICS Tool for Android Forensics”, 10th International Conference on Information Technology and Electrical Engineering **(ICITEE 2018)**, Bali, Indonesia, pp. 353-358 July 24-26, 2018.

BIBLIOGRAPHY

- [1] R. Ahmed, D.R.V. Dharaskar, and D.V.M. Thakare, “Digital evidence extraction and documentation from mobile devices”, International Journal of Advanced Research in Computer and Communication Engineering, Vol 2, No. 1, 2013.
- [2] I. U. Akarawita, A. B. Perera, and A. Atukorale, “ANDROPHSY-forensic framework for Android”, In Proceeding of 15th International Conference on Advances in ICT for Emerging Regions (ICTer), pp. 250-258, 2015.
- [3] A. A. M. Alamin and Dr. A. B. A. Mustafa, “Implementing Digital Forensic Framework for Android Smart Phones”, International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 21, Issue 01, Al-Neelain University, Sudan, 2015.
- [4] H. Alatawi, K. Alenazi, S. Alshehri, S. Alshamakhi, M. Mustafa, “Mobile Forensics: A Review”, International Conference on Computing and Information Technology, Vol 02, Issue: ICCIT- 1441, pp. 1 - 6, 2020.
- [5] K. A. Alghafli, A. Jones, and T. A. Martin, “Forensics data acquisition methods for mobile phones”, In proceeding of International Conference for Internet Technology and Secured Transactions, pp. 265-269. IEEE, 2012.
- [6] T. Almeahmadi and O. Batarf, “Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics”, 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019.
- [7] F. A. H. Ambreen and C.N. Kayte, “Forensic Analysis of Social Applications”, IOSR Journal of Computer Engineering, pp. 39-44.
- [8] R. Ayers, S. Brothers, and W. Jansen, “Guidelines on mobile device forensics”, NIST Special Publication 800-101, 2014.
- [9] R. P. Ayers, W. Jansen, A. M. Delaitre, and L. Moenner, “Cell phone forensic tools: An overview and analysis”, update, 2007.
- [10] N. A. Aziz, F. Mokhti and M. N. Nozri, “Mobile Device Forensics: Extracting and Analyzing Data from an Android-Based Smartphone”, In 4th International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), pp. 123-128, 2015.

- [11] M. R. Boueiz, "Importance of rooting in an Android data acquisition", 8th International Symposium on Digital Forensics and Security (ISDFS), 2020.
- [12] P. CedilloA, J. Camacho, K. Campos, A. Bermeo, "Forensics Activity Logger to Extract User Activity from Mobile Devices", 6th International Conference on eDemocracy & eGovernment (ICEDEG), 2019.
- [13] S. Dogan, E. Akbal, "Analysis of mobile phones in digital forensics", In Proceeding of 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1241-1244, IEEE, 2017.
- [14] M. Faheem, N. A. Le-Khac and T. Kechadi, "Smartphone forensic analysis: A case study for obtaining root access of an android Samsung s3 device and analyze the image without an expensive commercial tool", Journal of Information Security, Vol. 5, pp. 83-90, 2014.
- [15] M. Goel, V. Kumar, "Layered framework for mobile forensics analysis", In Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE), 2019.
- [16] A. Goel, A. Tyagi and A. Agarwal, "Smartphone forensic investigation process model", International Journal of Computer Science & Security (IJCSS), Vol. 6, No. 5, pp. 322-341, 2012.
- [17] A. Hadi, "Digital Forensics Professional", Cyber Security Course, INE, 2020.
- [18] M. Isak, "Android forensic using some open-source tools", In Proceeding of 8th International Conference on Business Information Security (BISEC), 2016.
- [19] F. Kausar and T. N. Alyahya, "Analysis of Physical Image Acquisition Forensic Tools for Android Smartphones", International Journal of Computer Science and Network Security (IJCSNS), Vol.16, No.11, 2016.
- [20] M. Khanafseh, M. Qataweh, W. Almobaideen, "A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics", International Journal of Advanced Computer Science and Applications, Vol. 10, No. 8, pp.610-629, 2019.

- [21] M. Kolhe, P. Ahirao, “Live vs dead computer forensic image acquisition”, *International Journal of Computer Science and Information Technologies*, Vol. 8, No. 3, pp. 455-457, 2017.
- [22] M. D. Leom et al., “Forensic collection and analysis of thumbnails in android”, in *IEEE Trustcom/BigDataSE/ISPA.*, IEEE, 2015.
- [23] M. Lessing, and B. V. Solms, “Live forensic acquisition as alternative to traditional forensic processes”, *IMF 2008–IT Incident Management & IT Forensics*, 2008.
- [24] K. D. Lutes and R. P. Mislán, “Challenges in mobile phone forensics”, In *Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA)*, 2008.
- [25] A. Mahajan, M. S. Dahiya and H. P. Sanghvi, “Forensic Analysis of Instant Messenger Applications on Android Devices”, *International Journal of Computer Applications*, Vol.68, No.8, 2013.
- [26] B. Martini, Q. Do, K. K. Choo, “Conceptual evidence collection and analysis methodology for Android devices”, <http://dx.doi.org/10.1016/B978-0-12-801595-7.00014-8>, *Information Assurance Research Group*, (University of South Australia, Syngress, an Imprint of Elsevier), pp. 285-307, 2015.
- [27] I. MRKAÍĆ, “Android Forensic Using Some Open-Source Tools”, *The 8th International Conference on Business Information Security (BISEC)*, 2016.
- [28] E. R. Mumba, H. S. Venter, “Mobile forensics using the harmonised digital forensic investigation process”, *Information Security for South Africa*, pp. 1-10, 2014.
- [29] A. Mylonas et al., “Smartphone forensics: A proactive investigation scheme for evidence acquisition”, in *IFIP International Information Security Conference*, Springer, 2012.
- [30] O. Osho, S. O. Ohida, “Comparative evaluation of mobile forensic tools”, *International Journal of Information Technology and Computer Science*, pp. 74-83, 2016.
- [31] S. Parvez, A. Dehghantanha, and H.G. Broujerdi, “Framework of digital forensics for the Samsung Star Series phone”, in *Proceeding of 3rd*

- International Conference on Electronics Computer Technology, IEEE, 2011.
- [32] K. Paul, “Generic Process Model for Android Smartphones Live Memory Forensics”, The Faculty of Computing and Information Management, KCA University. Nairobi, Kenya, pp. 1-87, 2014.
 - [33] V. V. Rao and A. S. Chakravarthy, “Survey on Android Forensic Tools and Methodologies”, International Journal of Computer Applications, Vol. 154, No.8, pp. 17-21, 2016.
 - [34] V. V. Rao and Dr. A.S.N Chakravarthy, “Forensic Analysis of Android Mobile Devices”, In Proceeding of International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 23-25, 2016.
 - [35] N. R. Roy, A. K. Khanna, L. Aneja, “Android phone forensic: Tools and techniques”, International Conference on Computing, Communication and Automation (ICCCA), pp. 605-610, 2016.
 - [36] D. M. Sai, N. R. G. K. Prasad, and S. Dekka, “The forensic process analysis of mobile device”, International Journal of Computer Science and Information Technologies, Vol. 6 (5), pp. 4847-4856, 2015.
 - [37] S. C. Sathe, N. M. Dongre, “Data acquisition techniques in mobile forensics”, In Proceeding of 2nd International Conference on Inventive Systems and Control (ICISC), pp. 280-286, IEEE, 2018.
 - [38] G. B. Satrya, P. T. Daely, S. Y. Shin, “Android forensics analysis: Private chat on social messenger”, In Proceeding of 8th International Conference on Ubiquitous and Future Networks (ICUFN), pp. 430-435, 2016.
 - [39] A. M. Simão, F. C. Sicoli, L. P. Melo, F. E. Deus, J. RT. Sousa, “Acquisition and analysis of digital evidence in android smartphones”, 2011.
 - [40] H. F. Tayeb and C. Varol, “Android Mobile Device Forensics: A Review”, 7th International Symposium on Digital Forensics and Security (ISDFS), 2019.
 - [41] T. Vidas, C. Zhang, and N. Christin, “Toward a general collection methodology for Android devices. digital investigation”, pp. S14-S24, 2011.

- [42] R. Wilson, H. Chi, “A case study for mobile device forensics tools”, In Proceedings of the South East Conference, pp. 154-157, 2017.
- [43] R. Wilson, H. Chi, “A framework for validating aimed mobile digital forensics evidences”, In Proceedings of the ACMSE Conference, pp. 1–8, 2018.
- [44] Google Inc. (Hrsg.): Android Software Development Kit (SDK). Google Inc., <http://developer.android.com/sdk/index.html> – Android2.2, Release2
- [45] <https://gs.statcounter.com/os-market-share/mobile/myanmar>
- [46] “ART and DALVIK.” [Online]. <https://source.android.com/devices/>
- [47] Prof. Edmond Locard, c. 1910
- [48] Webster’s Dictionary