A Review of Forensic Analysis Techniques for Android Phones

[1] Murtaza Ahmed, [2] M.N.A. Khan

[1,2]Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan

[1]murtaza9195@gmail.com
[2]mnak2010@gmail.com

Abstract--Mobile forensics analysis is the sub-domain of digital forensics, which addresses solving the minor technology misuse cases to substantial international digital crime cases. Mobile forensic refers to the acquisition of data and analysis of the artifacts collected from the mobile devices. Mobile phones are used as a means of communication and have evolved to a mini-portable computer having the advanced communication capabilities. New threats and challenges are being faced in the domain of mobile forensics by every passing year. In this paper, we review forensic analysis techniques for android phones and perform a critical analysis of the recent trends and techniques in the field of mobile forensics. We provide a comprehensive overview to the current state-of-the-art in this area. We identify new methodologies, tools and techniques which are successfully being used for forensic investigations of the mobile phones. With the help of this analysis we identify the key challenges and knowledge gaps for potential future research work.

***Keywords*—**Mobile Forensics, Digital Forensics, Android Phone Analysis, Smartphones Analysis, Digital Investigations.

I. INTRODUCTION

Mobile phones can be used as essential part of any digital investigation. From mobile phones, we can obtain some personal information like SMS, contacts, photos call details etc. A number of sub-disciplines have emerged as outshoots from the field of digital forensics such as Network Forensics, Computer Forensics, Multimedia Forensics, Memory Forensics, Mobile/Smart Phone Forensics and Android Forensics etc. Two types of memory forensics can be performed for mobile devices; first one is dynamic analysis and the other is static analysis. Forensic analysis can be generally performed in three major steps. First step is to seize the mobile device as seizure intends to preserve data. Second step in forensic analysis is acquisition of data as it is important for the investigator to acquire data in its original form.

There are different types of data acquisition ways such as, manual, physical, logical and file system. Manual acquisition refers to examining data by means of user interface of the mobile device. In logical acquisition, a bit by bit copy of the logical storage is obtained. In file system acquisition, deleted information can be recovered using the advanced recovery tools. Physical acquisition is similar to examining personal computer as it obtains bit by bit copy of the entire flash memory (physical storage). Third step of forensic analysis relates to examination and analysis of the acquired data. Analysis of data is essential to ensure the integrity of obtained data.

This study is based on identifying, evaluating and interpreting the existing research inputs and contributions relevant to the domain of mobile/smartphone forensics commonly known as Android Forensics. In particular, the study focuses on the following three main aspects:

- Summarize the existing evidence pertaining to the benefits and limitations of Android Forensics.
- Identify gaps in the current research in order to discover potential areas for further investigations.
- Provide a comprehensive research background followed by outlining the expected future research activities in the domain of Android Forensics. In this research study, we partially follow Design Science Research Process.

In this study, we critically analyze recent research papers concurrent with the field of mobile forensics. The purpose of this analysis is to determine the general strengths and limitations related to the field of digital forensics particularly of mobile devices. This study also explores different approaches, tools and techniques currently being used for performing forensic analysis of android mobile devices. The objective of this study is to identify key challenges linked with this domain.

Specifically, the study explores the open source and commercial tools, data acquisition techniques, data preservation techniques, forensic analysis techniques, modes of presenting evidence, legal requirements for ensuring authenticity and genuineness of the forensic analysis. The readers of this paper would be benefitted by knowing the current state of the art in the domain of Android Forensics along with the prominent challenges that this domain faces.

II. LITERATURE REVIEW

Anglano [1] describes how the artifacts left by WhatsApp messenger on android devices can be forensically analyzed. The author analyzes famous instant messaging application WhatsApp from forensic perspective. By correlating different artifacts, it is possible to extract all the information when a specific contact has been added or deleted or when specific message has been send or received. The study results highlight the importance of correlating different artifacts/traces left by WhatsApp messenger to extract useful information of evidentiary value.

Ntantogian *et al*. [2] identify that the compact size of android mobiles makes it vulnerable to theft, stolen or misplaced. The aim of the study was to analyze how to recover authentic credential of users from physical memory of android devices. The study also explores the methods which can be used to discover patterns and expressions which indicate the exact position/location of sensitive data available in the memory dump. Analysis of results reveals that many android applications are vulnerable to security lapse as they are able to recover sensitive data and authentic credential from volatile memory.

Mutawa *et al*. [3] explored the nature of vulnerabilities of social network applications and determined how those applications contributed towards cybercrimes. The aim of study was to determine how the activity performed through social network websites were stored in internal memory of the smartphones. The contribution of the study is that it determined the leftover content on the physical disk and assessed the amount of risk these leftover content pose. Results of this study show that BlackBerry does not store any information of social networking activities in its internal memory while iPhone and Android mobile store significant amount of data which can be recovered easily and can be used for forensic analysis.

Walnycky *et al*. [4] discussed that the instant messaging applications leave the trace of users activities performed through android devices. This study performed forensic analysis of applications and find out how user credential can be obtained during communication. The study aims to forensically investigate how application leave evidentiary trace of users activities. The study acquired digital forensic evidence from data in transit and from mobile memory, and then tried to reconstruct the data vulnerabilities. Cross validation are also performed by network traffic data with data stored on devices.

Son *et al*. [5] describe that maintaining the integrity of data during data acquisition is a big issue. This study evaluates how one can ensure data integrity during data acquisition using Android Recovery Mode. Objective of the study was to evaluate Android Recovery Mode variables and effect of each variable on the integrity of user data during data collection from an android device. The study proposed a tool named Custom Recovery Mode Image (CRMI) for Android recovery mode. The purpose of this tool is to acquire user data efficiently so that integrity of data is ensured. Results of the experiments show that the integrity of user data was successfully preserved using CRMI tool.

Sylve *et al*. [6] studied how the vital information was stored in physical memory of android devices. The study developed a methodology which helped in obtaining almost all information from android device memory. Aim of this study was to obtain maximum information from the internal memory of android device during forensic investigation. The study developed a toolset called Droid Memory Dumper for data acquisition and deep analysis of memory from android mobiles. The experimental results show that it captured 99.46% identical pages as compared to TCP packet, and 99.15% identical pages when compared with the SD card memory.

Anglano *et al*. [7] identify that ChatSecure is a famous mobile application which is used to encrypt instant messages during communication. In addition to many legitimate uses, this application is also used for illicit activities. This study provides forensic analysis of instant message application and obtains data from internal memory of phone. The aim of this study was to forensically analyze ChatSecure application by running it on android devices. The study devises a technique to decrypt instant messages sent or received through ChatSecure application. The accuracy of the proposed techniques was accessed by validating its results against the ones obtained from real android phone.

Yang *et al*. [8] state that most of the existing forensic analysis tools for data acquisition in android devices exploit Android kernel vulnerabilities, but it is becoming difficult to acquire data from android smartphone using existing data acquisition tool as Android OS has been upgraded regularly. The aim of the study was to develop a new data acquisition method based on analyzing firmware update protocols of android mobile devices. The study developed a tool called Android Physical Dump based on analyzing firmware update protocol of android smartphones. The experimental results show that proposed tool preserved integrity of the entire flash memory.

Thing *et al*. [9] discussed that offsite storage of evidence during ongoing criminal activities was not an appropriate approach for investigation. In addition, static media size is constantly increasing so it could take much time for acquiring and processing data. The aim of study was to develop an automated system to perform live analysis of android mobiles. The proposed system supports android phones live memory dynamic analysis of interactive applications. The experimental results show that 100% evidence can be acquired in case of outgoing messages from the memory dump and 97.8% evidence can be acquired from incoming messages.

Guido *et al*. [10] describe that the malicious applications installed on android phones can expose sensitive data exposed to the unauthentic users. The objective of the study was to improve smartphones monitoring by identifying malicious applications. The study presents an approach to remotely audit and monitor android smartphone by using traditional digital forensic techniques. The experimental results show that 71% accuracy was achieved to detect malicious applications from the pool of 31 malicious applications.

Moonsamy *et al*. [11] identified that two types of authorizations are used for android mobiles to detect newly installed applications. The first one is “required permission” which is checked before installation and the other is “used permission” which is needed after the installation of an application. To differentiate between malicious and benign applications, the study focus on the permissions applied from any application for “used permission”. The study proposed a novel pattern mining algorithm for identifying the set of contrast permission that aim to differentiate between malicious and uncontaminated applications.

Elish *et al*. [12] describe that malware applications of android smartphones are threat for confidentiality of personal data. These applications can abuse system resources, damage sensitive data and disrupt normal device usage. For detecting malware applications, the study describes an accurate classification approach. The objective of this paper is to apply rule based classification method for identifying malicious applications on android devices. The study introduced a new android application classification method that uses API or permission features for detecting malware applications.

Glisson *et al*. [13] describe that different Mobile Forensic Toolkit manufacturers have developed several recovery methods for extracting evidence. However, a number of researchers have reported that the reliability of the evidence collected from these Mobile Forensic Toolkit is considerably low and verification of these evidence is difficult. The objective of study was to verify the reliability of the data recovered by the Mobile Forensic Toolkit. The study provides evidentiary results that there is a considerable variation between recovery methods when applied on different devices. The results show that by using all the toolkits, a total of 87.6% artifact were recovered from mobile devices.

Derhab *et al*. [14] identified that some malicious applications used SMS services on android mobile devices for sending messages without the consent and knowledge of the users. The aim of study was to propose a system for providing detection and prevention against unauthorized outgoing malicious SMSs from android smartphones. In order to distinguish between malicious and legitimate SMS applications, the study proposed a model named OnDroid that provides a prevention system for android devices monitoring the SMSs. The core idea of the proposed system was to find inconsistencies (incoherence) between the Android device state and the user behavior. From the experimental results, it can be observed that the system achieved 100% accuracy to detect malicious SMS-sending from android device.

Grover [15] explores that concrete availability of data could aid enterprise level organizations for common security practices like incident response, proactive security monitoring, security auditing and forensic investigation. The study provides a prototype system for automated data collection for monitoring android smartphones. The study focuses on design and implementation of a prototype application named as DroidWatch for automating data acquisition phase in a digital investigation. The study developed a novel design strategy which can be used for monitoring prioritize Android applications. The work serves as a set of guideline for accessing data through the default Android API. Different approaches for finding digital evidence are reported in [16-20].

Roy *et al*. [21] state that there are approximately one billion smart phone users worldwide and the huge number of these small scale digital devices carries tremendous information for forensic analysis. In view of this, there is a pressing need to develop robust forensic analysis techniques specifically aim at analyzing mobile contents. The authors report that there is a scarcity of effective tools and techniques for android forensics.

Hoog [22] provides a comprehensive piece of literature of the subject and have compiled a long list of tools including Debug Bridge, EnCase Neutrino, viaExtract, AccessData MPE+, Cellebrite UFED etc. which can be used to acquire evidence from Android Android smartphones. Most of these smartphone forensic tools support logical data acquisition. On the contrary, physical data acquisition mechanisms do exist for MTD storage, but these solutions are expensive and their data retrieval process is quite slow. Further, there is always a risk of malfunctioning of the mobile device after running such tools.

Vidas *et al*. [23] propose a general process for data collection from Android devices by employing a partitioning schema. Thing *et al*. [24] propose an automated for carrying out live forensic analysis of volatile memory for real-time evidence acquisition. Pooters [25] created a tool to obtain linear bitwise copies of the flash memory of Symbian OS phones. Leppert [26] discuss at length the methods of acquiring Android memory dump and analyzing these acquired from smartphones. Ntantogian *et al*. [27] investigate the methods of obtaining authentic credentials from volatile memory of Android smartphones. The authors create 30 different scenarios for analyzing physical memory.

Simao *et al*. [28] highlight that specific feature of different smartphone platforms needs to be considered while acquiring data from Android smartphones. This issue again serves as a key challenge for smartphone forensics. The diversity of cache formats on the Android based smartphones is another challenge for Android Forensics. Immanuel *et al*. [29] present an Android cache forensic process to extract caches from Android phones and categorize the cache formats followed by analyzing the cache memory content. Kaart and Laraghy [30] emphasize that it is imperative that proper interpretation of traces that are found on Android devices should be made.

III. CRITICAL ANALYSIS

Table 1. Critical Analysis

Reference	**Focused area**	**Smartphones type**	**Tools / Techniques**	**Type of analysis**	**Dimensions of forensic analysis Attributes**	**Phases of forensic analysis addressed**	**System activities**	**Test bed environment/ Attributes used for forensic analysis**	**Validation Criteria**
Angalano [1]	Forensic analysis of WhatsApp messenger on android devices	Android v.4.0.4	You-Wave virtual platform, FTK (Forensic Tool Kit) Imager	Static	Privacy, Security	Data acquisition, Correlation	Add and delete contacts, Exchanging text messages and images	For user contacts: Jid, wa_name, etc. For text messages: Key_remote_jid, key_from_meetc	Cross Validation (with data generated on real smartphone)
Ntantogian et al. [2]	To check how volatile memory of android devices save user credential. To trace remnants of user credentials	Samsung Galaxy S Plus (i9001)	Linux Memory Extractor (LiME)	Static & Dynamic	Privacy, Authenticity	Data acquisition	Login, Logout	Username, passwords	Recovery of user credentials With reboot=0% In idle state = 80% Ensure data integrity
Al Mutawa et al. [3]	Nature of user credentials left on the physical media while using social networking websites	BlackBerry Torch 9800, iPhone 4 and Samsung Galaxy S	BlackBerry Desktop Software (BDS), Apple iTunes application, MyBackup (v2.7.7)	Dynamic	Security, Reliability	Logical image acquire and analysis	Uploading photos, Posting comments, Email within applications	Facebook (Login, Post news feed, Upload photo, etc.), Twitter (Login, follow people, Post tweets, etc.), MySpace (Login, Upload picture, Change status etc.)	Ensure data integrity

Walnycky et al. [4]	To reconstruct message content of instant messaging application running on android device	HTC One M8 (Android 4.4.2), iPad 2 (iOS 7.1.2)	XRY, Helium Backup, Android Backup Extractor, Wire-shark	Static	Privacy, Security	Forensic analysis, Data acquisition	Exchanging text, images, audio, video, locations	Whatsapp (text chat), Viber (Location), Tango (Video), MessageMe (audio), 20 applications were examined.	Cross Validation with static memory image
Son et al. [5]	To ensure data integrity during data acquisition	Galaxy (S2, S3, Note, Note 2, Nexus) Motorola Droid and Pantech Vega LTE.	Indigenously developed tool named CRMI (Custom Recovery Mode Image)	Static	Integrity, Authenticity	Data acquisition	Searching an application within device, changing settings etc.	Android device activities such as changing setting etc.	Ensure data integrity
Sylve et al. [6]	To develop a toolset and methodology for obtaining complete image of volatile memory from Android devices	HTC EVO 4G	Developed DMD (Droid Memory Dumper) tool that matches identical memory pages saved on SD card	Static & Dynamic	Reliability (DMD tool), Authenticity, Accuracy	Data acquisition	Call details, contact, mms	Add Contact, Calling, Multimedia communications	dmd(TCP) = correctly identified 99.46% identical pages dmd (SD Card) = correctly identified 99.15% identical pages
Anglano et al. [7]	Perform forensic analysis of ChatSecure (instant message) application running on android devices	Samsung SM G350, Galaxy Core Plus	Use Android Mobile Device Emulator to create 3 Android Virtual Devices running on android version 4.4, 5.1 and 6.0	Dynamic	Privacy, Security	Data correlation	Exchanging files and messages	Chat Secure (chat management, Point to point communication, Group communication, File transfers)	Validate results with data obtained from smartphones
Yang et al. [8]	Develop a tool based on firmware update protocol for data acquisition in android phone	Samsung Galaxy, LG Optimus, Pantech Vega, Google Nexus 4/5	Developed APD (Android Physical Dump) tools for data acquisition	Dynamic	Integrity, efficiency	Data acquisition	Searching an application within device, changing settings etc.	Android Device Activities such as changing setting etc.	Preserve integrity of entire flash memory
Thing et al. [9]	Develop an automated system to perform live memory analysis of android mobiles	Android v.2.2.3	Memory acquisition tool (memgrab), Memory Dump Analyzer (MDA)	Dynamic	Integrity	Forensic analysis, Data acquisition	Exchange messaging	Android Messaging Application	Accuracy rate for evidence recovery /acquisition (Outgoing message 100% and Incoming message 97.8%)

Guido et al. [10]	To develop an automated system for identifying malicious application on android smartphones	Google Nexus S (Android 2.3.1)	Develop “Tractor Beam” tool for detecting malware applications	Static	Security	Forensic analysis and detection	Installing and deleting applications	Android application installer	71.0% accuracy for detecting malware applications
Moonsamy et al. [11]	A novel contrast permission pattern mining algorithm is presented to distinguish between clean and malicious applications	Android v.4.2 and above	Bi-clustering Algorithm, Contrast permission pattern mining algorithm	Dynamic	Privacy, Security	Forensic analysis	Application installation	Google Play (Android Store)	Normal = 63% Malicious = 25%
Elish et al. [12]	Develop a method for accurately identifying malicious applications for android devices	Android OS	Trigger-based dependence for privileged API calls	Static	Security	Forensic analysis	SMS messages	Google Play, VirusShare	Accuracy of detecting malware = 97.9%
Glisson et al. [13]	Comparison of data recovered by software based methods available in mobile device forensic toolkits	Google Android OS, Apple OS, BlackBerry OS	Cellebrite’s Universal Forensic Extraction Device (CUFED)	Static & Dynamic	Reliability, Verifiability, Completeness	Data acquisition, Forensic analysis	SMS, Images, Call logs, Contacts	Messaging, Calling and Contact Application, Multimedia communications	Artifact recovery = 87.6% (SMS =30.0%, Images= 27.9%, Contacts= 15.6%, Call = 14.0%)
Derhab et al. [14]	Proposed a system model to detect and prevent outgoing malicious SMS from an android device	Android 4.2 (JellyBean), Android 4.4 (KitKat)	Indigenously developed a system model “OnDroid”	Dynamic	Security	Forensic nalysis	Exchanging messages	Android Messaging Application	Prevention accuracy=100%
Grover [15]	To automate data collection process from android devices	Samsung Galaxy S II (Android 2.3.6)	DroidWatch	Dynamic	Security	Data Collection	SMS, Call logs	Android Messaging and Contact Applications	Ensure Data Integrity

IV.KEY CHALLENGES

There are certain key challenges that are faced by the investigators during acquisition or data analysis. Most common challenge identified is mobile security locking mechanism. It is common for users to lock their mobile by password, biometric verification or pattern matching. If anyone tries to open this lock in an unauthentic way, then mobile security mechanism will delete all the files which are saved in its memory. Other important challenges include firmware protocol changing in operating system. Smartphone manufacturers often provide updates for operating system. These updates are essential to introduce new features in their products, but along with these features it also presents a new security mechanism for the devices. Another challenge in acquiring data from mobile devices is rebooting. Many devices delete their recent data including cache memory, recent call logs etc. on rebooting or restarting. But, such type of features put question mark on the integrity of data.

A fact that a large variety of modern day smartphones are available in the market makes this a real challenge for smartphone forensics. A novel challenge for smartphone forensics is the number of operating systems as the number of operating systems available in the smartphone paradigm is more than the operating systems available for desktop computers. Forensic soundness in terms of accurate data extraction is another major challenge. Even data extraction from some varieties of smartphone is unsupported which also pose a great challenge for Android phone forensics. Another issue while performing forensic analysis on smartphones is how to deal with passcode-protected mobile device and decoding the encrypted data. One of the fundamental requirements for performing forensic analysis id to ensure that data extracted from the devices is not altered. This is a key rule that the data acquisition tools do not modify the evidence. But, this issue becomes very vulnerable in smartphone forensics as switching on the mobile change several state variables and certain background processes are constantly running on the mobile devices. Ensuring data integrity in such situation remains a key challenge for forensic analysts.

Presently, there is not a single tool available for smartphone platform that is capable to extract all sorts of data from a smartphone. Because of this, forensic analysts have to use multiple tools to extract different data artifacts from smartphone. This is an added challenge in the smartphone forensics.

V. CONCLUSION

Forensic analysis is an important part of digital investigation. In forensic analysis, evidence is acquired and analyzed to identify sequence of steps taken during any digital crime. In this paper, we explore recent work done in the field of forensic analysis on android mobile devices. The purpose of this study is to identify how mobile applications leave evidentiary trace of user's credential in the internal memory of the mobile phone devices. We also explored different tools and techniques required for extracting data from memory of mobile devices. Considering nature of the digital crime and type of the investigation, different tools are used for logical and physical memory data acquisition. Ensuring data integrity for the sake of reliable forensic analysis is envisaged to be potential future work.

REFERENCES

[1] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digital Investigation*, vol. 11, no. 3, pp: 201-213, 2014.
DOI: 10.1016/j.diin.2014.04.003

[2] C. Ntantogian, D. Apostolopoulos, G. Marinakis and C. Xenakis, "Evaluating the privacy of Android mobile applications under forensic analysis," *Computers & Security*, vol. 42, pp: 66-76, 2014.
DOI: 10.1016/j.cose.2014.01.004

[3] N. Al Mutawa, I. Baggili and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp: S24-S33, 2012.
DOI: 10.1016/j.diin.2012.05.007

[4] D. Walnycky, I. Baggili, A. Marrington, J. Moore and F. Breitinger, "Network and device forensic analysis of Android social-messaging applications," *Digital Investigation*, vol. 14, pp: S77-S84, 2015.
DOI: 10.1016/j.diin.2015.05.009

[5] N. Son, Y. Lee, D. Kim, J. I. James, S. Lee and K. Lee, "A study of user data integrity during acquisition of Android devices". *Digital Investigation*, vol. 10, pp: S3-S11, 2013.
DOI: 10.1016/j.diin.2013.06.001

[6] J. Sylve, A. Case, L. Marziale and G. G. Richard, "Acquisition and analysis of volatile memory from android devices". *Digital Investigation*, vol. 8, no. 3, pp: 175-184, 2012.
DOI: 10.1016/j.diin.2011.10.003

[7] C. Anglano, M. Canonico and M. Guazzone, "Forensic analysis of the ChatSecure instant messaging application on android smartphones," *Digital Investigation*, vol. 19, pp: 44-59, 2016.
DOI: 10.1016/j.diin.2016.10.001

[8] S. J. Yang, J. H. Choi, K. B. Kim and T. Chang, "New acquisition method based on firmware update protocols for Android smartphones". *Digital Investigation*, vol. 14, pp: S68-S76, 2015.
DOI: 10.1016/j.diin.2015.05.008

[9] V. L. L. Thing, K. Y. Ng and E. C. Chang, "Live memory forensics of mobile phones," *Digital Investigation*, vol. 7, pp: S74-S82, 2010.
DOI: 10.1016/j.diin.2010.05.010

[10] M. Guido, J. Ondricek, J. Grover, D. Wilburn, T. Nguyen and A. Hunt, "Automated identification of installed malicious Android applications," *Digital Investigation*, vol. 10, pp: S96-S104, 2013.
DOI: 10.1016/j.diin.2013.06.011

[11] V. Moonsamy, J. Rong and S. Liu, "Mining permission patterns for contrasting clean and malicious android applications," *Future Generation Computer Systems*,

vol. 36, pp: 122-132, 2014.
DOI: 10.1016/j.future.2013.09.014

[12] K. O. Elish, X. Shu, D. D. Yao, B. G. Ryder and X. Jiang, "Profiling user-trigger dependence for Android malware detection," *Computers & Security*, vol. 49, pp: 255-273, 2015.
DOI: 10.1016/j.cose.2014.11.001

[13] W. B. Glisson, T. Storer & J. Buchanan-Wollaston, "An empirical comparison of data recovered from mobile forensic toolkits," *Digital Investigation*, vol. 10, no. 1, pp: 44-55, 2013.
DOI: 10.1016/j.diin.2013.03.004

[14] A. Derhab, K. Saleem, J. Al-Muhtadi and M. A. Orgun, "Leveraging adjusted user behavior in the detection and prevention of outgoing malicious SMSs in Android devices," *Computers in Human Behavior*, vol. 59, pp: 9-17, 2016.
DOI: 10.1016/j.chb.2016.01.023

[15] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," *Digital Investigatio*n, vol. 10, pp: 12-20, 2013.
DOI: 10.1016/j.diin.2013.06.002

[16] M.N.A. Khan, "Finding Digital Evidence in Filesystem Events," *In Proceedings of The 8th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting (PGNet 2007)*, Liverpool, 2007.

[17] M.N.A. Khan, C.R. Chatwin and R.C.D. Young, "A Bayesian Network Approach to Discover Digital Evidence," *In Proceedings of The 2nd conference on Advances in Computer Security and Forensics (ACSF)*, Liverpool, 2007.

[18] M.N.A. Khan and S. W. Ullah, "A log aggregation forensic analysis framework for cloud computing environments," *Computer Fraud & Security*, vol. 7, pp: 11-16, 2017.
DOI: 10.1016/S1361-3723(17)30060-X

[19] M.N.A. Khan, C.R. Chatwin and R.C.D. Young, "A framework for post-event timeline reconstruction using neural networks," *Digital Investigation*, vol. 4, no. 3, pp: 146-157, 2007.
DOI: 10.1016/j.diin.2007.11.001

[20] M.N.A. Khan, "Performance analysis of Bayesian networks and neural networks in classification of file system activities," *Computers & Security*, vol. 31, no. 4, pp: 391-401, 2012.
DOI: 10.1016/j.cose.2012.03.003

[21] N. R. Roy, A. K. Khanna and L. Aneja, "Android phone forensic: Tools and techniques," In *Proceedings of International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp: 605-610.

[22] A. Hoog, "Android forensics: investigation, analysis and mobile security for Google Android," Syngress, Elsevier. 2011.

[23] T. Vidas, C. Zhang and N. Christin, "Toward a general collection methodology for Android devices," *Digital Investigation*, vol. 8, pp: 14-24, 2011.
DOI: 10.1016/j.diin.2011.05.003

[24] V. L. L. Thing, K. Y. Ng and E. C. Chang, "Live memory forensics of mobile phones," *Digital Investigation*, vol. 7, pp: 74-82, 2010.
DOI: 10.1016/j.diin.2010.05.010

[25] I. Pooters, "Full user data acquisition from Symbian smart phones," *Digital Investigation*, vol. 6, no. 3, pp: 125-135, 2010.
DOI: 10.1016/j.diin.2010.01.001

[26] S. Leppert, "Android memory dump analysis," Student Research Paper, Chair of Computer Science, Friedrich-Alexander-University Erlangen-Nuremberg, Germany, 2012.

[27] C. Ntantogian, D. Apostolopoulos, G. Marinakis and C. Xenakis, "Evaluating the privacy of Android mobile applications under forensic analysis," *Computers & Security*, vol. 42, pp: 66-76, 2014.
DOI: 10.1016/j.cose.2014.01.004

[28] A. M. D. L. Simao, F. C. Sicoli, L. P. de Melo, F. E. de Deus and R. T. de Sousa Junior, "Acquisition of digital evidence in android smartphones," In *9th Australian Digital Forensics Conference*, 2011, pp: 116.

[29] F. Immanuel, B. Martini and K. K. R. Choo, "Android cache taxonomy and forensic process," In *Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA*, 2015.
DOI: 10.1109/Trustcom.2015.488

[30] M. Kaart and S. Laraghy, "Android forensics: Interpretation of timestamps," *Digital Investigation*, vol. 11, no. 3, pp: 234-248, 2014.
DOI: 10.1016/j.diin.2014.05.001