TELKOMNIKA, Vol.17, No.4, August 2019, pp.1803~1809
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i4.11748

Live forensics of tools on android devices for email forensics

Rusydi Umar[1], Imam Riadi[2], Bashor Fauzan Muthohirin*[3]
[1,3]Department of Informatics Engineering, Universitas Ahmad Dahlan
Prof. Dr. Soepomo St., S.H., Janturan, Yogyakarta, 563515 Indonesia
[2]Department of Information System, Universitas Ahmad Dahlan,
Prof. Dr. Soepomo St, S.H., Janturan, Yogyakarta, 563515 Indonesia
*Corresponding author, e-mail: bashor1707048017@webmail.uad.ac.id

Abstract

Email is one communication technology that can be used to exchange information, data, and etc. The development of email technology not only can be opened using a computer but can be opened using an smartphone. The most widely used smartphone in Indonesian society is Android. Within a row, the development technology of higher cybercrime such as email fraud catching cybercrime offenders need evidence to be submitted to a court, for obtain evidence can use tools like Wireshark and Networkminer to analyzing network traffic on live networks. Opportunity, we will do a comparison of the forensic tools it to acquire digital evidence. The subject of this research focused on Android-based email service to get as much digital evidence as possible on both tools. This process uses National Institute of Standards and Technology method. The results of this research that networkminer managed to get the receiving port, while in Wireshark not found.

Keywords*: android, email, networkminer, NIST, Wireshark*

1. Introduction

The development of technology can facilitate human work so that more effective, one of the developments technology is an electronic mail (email). Email is one of the medium of communication, information dissemination and the number of email provider services makes it all to be concise and easy. Users can send information in minutes and even seconds to the world. Likewise the recipient of the information can easily and quickly reply with the information [1].

The more people connect to the internet, making electronic mail (email) as one form of communication the most rapid and economical. The amount of digital information in email as a result of the development of information technology requires a way of organizing and grouping information in an email inbox for the convenience of its users. This unstructured grouping of information is known by the classification of documents [2].

Smartphones have many applications that can be used to help access email. Smartphones are working phones that use the full potential of operating system software that provides user-friendly connections and powerful hardware. Smartphones have different operating systems, just like with the operating system for desktop computers [3]. Currently smartphone devices have the same functionality as computers. Although the function is the same as the computer, but there are some differences in the process of handling digital forensics between computer devices and smartphones because the smartphone has unique characteristics that cannot be equated with ordinary computer handling [4].

Indonesian society is no stranger to the name of smartphones, Indonesia is one of the market is quite promising for companies makers of smartphones, especially Android. Every year Android users continue to leave because the user interface friendly and open source makes it easy for users to use it and develop it. Based on statistics of mobile operating system market share in Indonesia from January 2012 to December 2017 users Android smartphone continue to increase, can be seen in Figure 1 [5].

In any cybercrime must leave evidence, in the form of digital and electronic evidence [6]. Digital evidence can be seen when the criminal process is direct and can be stored, digital evidence can be handled exclusively by digital forensics science using tools to solve and draw conclusions from criminal cases on digital evidence obtained. In real or fake

Received May 29, 2018; Revised February 23, 2019; Accepted March 18, 2019

emails it can be detected using several ways, such as viewing email headers [7, 8], digital signature, and reading logs [9–11]. Digital forensics is the study of how to deal with crimes involving technology such as computers [12]. There are several techniques in digital forensics, one of which is live forensics that is used to handle digital crimes using approaches to systems operating that are working and connected to the network [13].

The law on cybercrime crimes is set in the laws on ITE in Indonesia. The crimes of ITE can be criminalized by civil or civil law in accordance with the level of the crime committed, the process of arrest of the cybercrime by the authorities based on the evidence of crimes that are stored on the smartphone or on other hardware that can be used as evidence in the law court such as username, ip address and timestamp [14, 15]. No criminal cases have escaped evidentiary evidence. Almost all criminal prosecutions always lean on examination of evidence. At least in addition to proof with other evidence, there is always a need for verification with at least two evidences. Tools that can be used to obtain digital evidence such as Wireshark and Networkminer [16]. Wireshark and Networkminer are open source packet analytical tools that can be used for troubleshooting networks and network analysis. Digital evidence can be found in a way that is by traditional or dead means such as looking for evidence of artifacts, history, and etc. Meanwhile, to obtain the evidence directly or the forensic analysis process when the system is running is called live forensics [17, 18].

In [19] the title of A Comparative Study of Email Forensic Tools. The study conducted a comparison of traditional email forensic tools. Tools used to obtain digital evidence are Mailxaminer, Add4Mail, Digital Forensic Framework, Emailtrackerpro, and Paraben E-Mail Examiner. The study successfully compared between forensic tools. In [20], the title of Network and device forensic analysis of Android social-messaging applications. The research focused on detecting the presence of unclear artifacts associated with email accounts, retrieving data from service providers, and representative email in a well-structured format based on existing standards.

In [21], they discussed the description of email architecture, based on a forensic perspective. on architectures designed to explain the roles and responsibilities of e-mail users and their components, analyze the metadata contained in e-mail headers and then explain the tools used and techniques that can be used by investigators to forensic e-mail. From the results of the metadata presents e-mail messages and various techniques used for e-mail forensics. In [22], they discussed about forensic e-mail which includes analyzing the contents of e-mail, header information, transit lines for e-mail information, senders or recipients and gathering evidence for the culprit and making a safer system. In this case it also discusses e-mail investigative techniques and the tools used in e-mail forensic processes. The email system and internet applications have components such as hardware and software, including services, protocols, servers and agents.

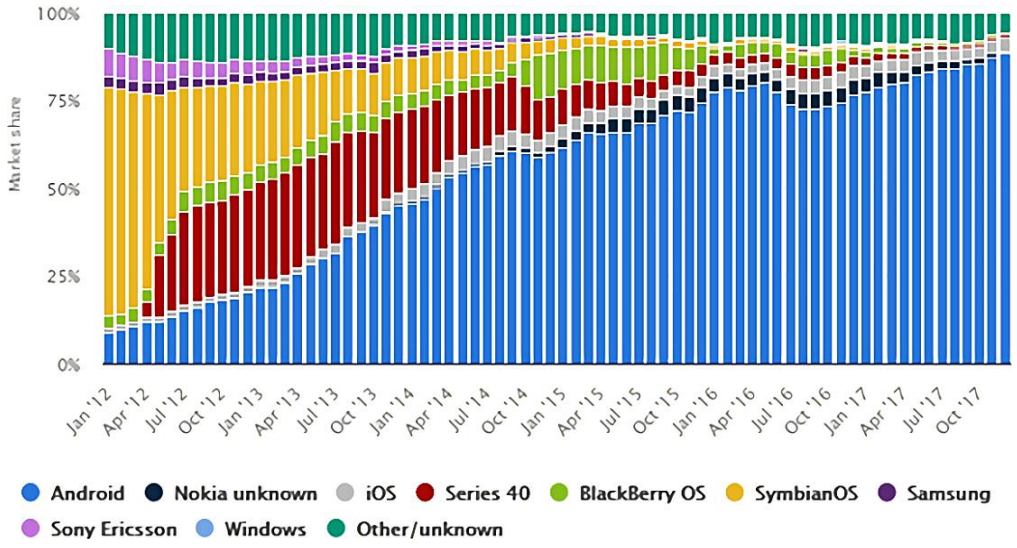

Figure 1. Smartphone user in Indonesia

In [23], they discussed about tools that are open source and can be used to analyze e-mail as digital evidence, and make responsive and interactive graph visualization of e-mail data supported by statistics. The research successfully implemented which can be used for e-mail forensic analysis with a dynamic visualization approach. From the above background then we will conduct research on the comparison of Wireshark and networkminner forensics, forensic tools to get as much digital evidence as possible for use in trials such as IP address, ports, and timestamps. The comparison process, forensic tools use Android-based webmail services. The method used in this study is the National Institute of Standards and Technology (NIST) to obtain digital evidence.

2. Research Method

In this research, we use mobile forensics methods based on the guidelines available and prepared by the National Institute of Standards and Technology (NIST). The NIST method is used to perform analysis of digital evidence in emails and as a stage for obtaining information from digital evidence, consisting of 4 stages such as Figure 2 [24, 25].

a. Collection

Colection is a collection process, identifying, labeling, recording and retrieving evidence in the form of software to be retrieved for use as digital evidence of a digital crime case.

b. Examination

Testing includes an appraisal process and selects appropriate information from all the data collected, as well as bypassing prosses or minimizes various features in the operating system and applications that can eliminate data such as encryption, data compression, access control mechanisms, specify file locations, checks metadata, extract files and more.

c. Analysis

The analysis is done by various method approaches, the task of this analysis includes many activities, such as identifying the users involved indirectly, the location, the occurrence, the device and considering how to get all the components connected to the final conclusion.

d. Reporting

Report the results of the analysis including the description of the actions performed, what tools are used and the procedures used.

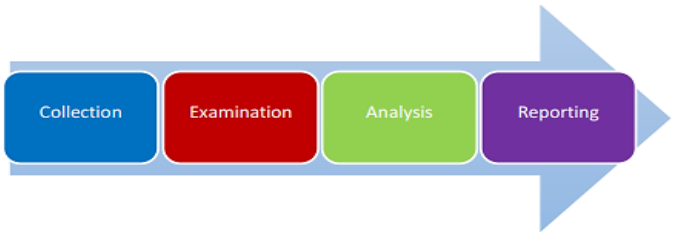

Figure 2. Stages of NIST method

3. Results and Analysis

The results of this research conducted a comparison of forensic tools in finding digital evidence in the email received live forensics. Tools used are Wireshark and Networkminer for sniffing on received email packets. The email used is webmail. Here is a comparison process of forensics tools on Android based email services using the National Institute of Standarts and Technology (NIST) forensics mobile method.

3.1. Collection

At this stage of collecting goods on smartphone owners, the smartphone used is google Nexus 6 and Android version Oreo 8.0. Smartphone used in this research is smartphone emulator genymotion version 2.12. The following is a collection stage concept. Figure 3 is a conceptual stage in the collection process, the user receives an email from someone then opens the email, together the investigator sniffing. This collection process of digital evidence is done live forensics.

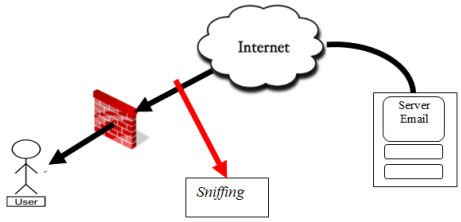

Figure 3. Conceptual stages in collection process

3.2. Examination

In Examination, we performed a comparison on Wireshark and Networkminer forensic tools. The email recipient opens using the Android smartphone browser version of oreo 8.0. The smartphone runs on a 2.12.1 Geanymotion emulator. Here are the comparison stage forensic tools in the process of getting the digital evidence on Android smartphone. Figure 4 is an Android smartphone that is used to open the email received from someone to us. At the same time, Wireshark and Networkminer are running to capture packets of passing data. Here is the process of capturing packages using Wireshark and Networkminer. Figure 5 is a sniffing process using Wireshark tools. Tools Wireshark successfully for sniffing data packets on email service that opened using Android browser can see there is a red circle in Figure 5. Figure 6 is a Networkminer sniffing tool. Networkminer succeeded in sniffing on email packets marked with finding IP Address and webmail, can see there is a red circle in Figure 6.

Figure 4. Android Oreo smartphone

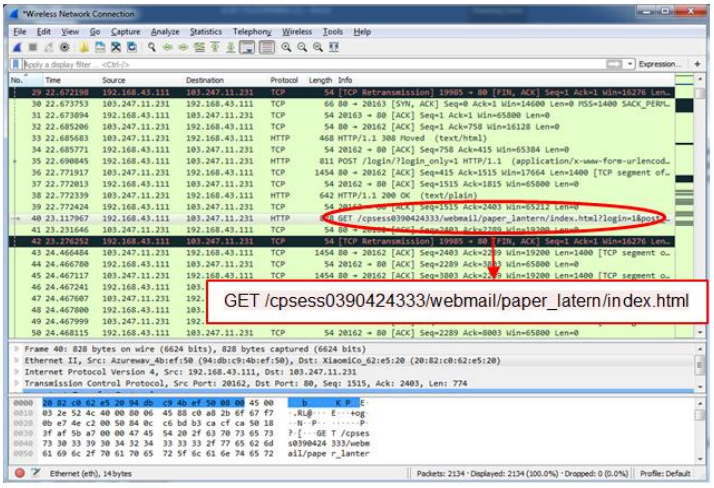

Figure 5. Process examination tools Wireshark

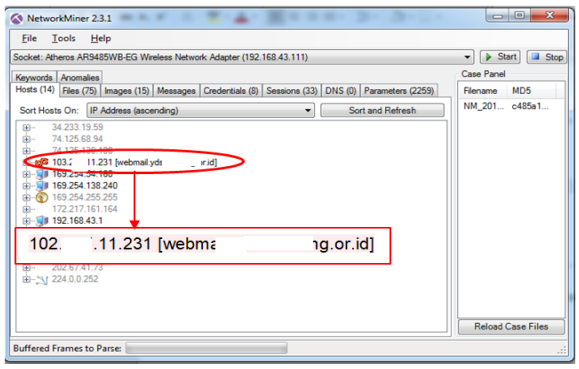

Figure 6. Process examination tools NetworkMiner

3.3. Analysis

At this stage is the result obtained by Wireshark and Networkminer forensics tools on Android-based email is complete. Here are the results obtained. Figure 7 is the result of sniffing on the email service accessed using Android smartphone. Found IP Address source: 192.168.43.111, IP Address destination: 103.247.11.231, and the email protocol: HTTP.

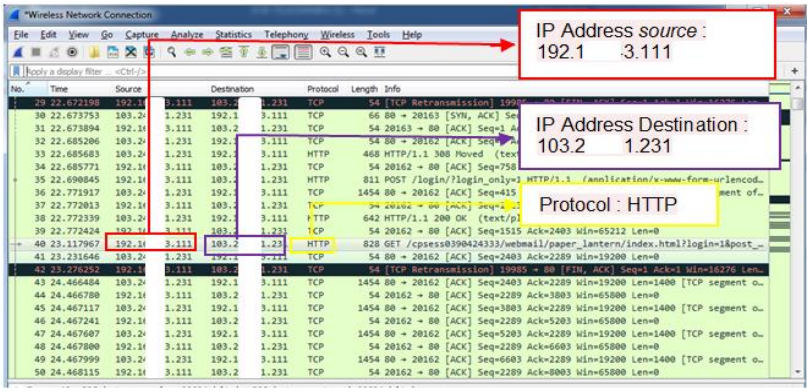

Figure 7. Results of Wireshark sniffing

Packages that are sniffing by Wireshark can be viewed in detail in the Transmission Control Protocol/TCP Stream stream contained in the Wireshark menu. In TCP stream there is complete information about sniffing data. following is the result of capturing Wireshark. Figure 8 is the contents of the TCP stream, in the TCP Stream gives a lot of information. The following information can be found: (a) is the webmail host, (b) is the smartphone information used, (c) is the browser used to open the email and layout webmail, (d) is username and password of the user, timestamp email delivery, and email server, (e) is the sending port used.

Figure 9 is a result that is captured by Networkminer tools. Networkminer can be a lot of information. The following information can be found: (a) is the ip address source, (b) is port source, (c) is the ip address destination, (d) it is the timestamp information on the server, (e) is the destination port, (f) is the interface used is roudcube, (g) is the webmail host used, (h) is a smartphone used to open email, (i) is the browser used to open the email, (j) is the user's username and password, (k) it is an email delivery timestamp, (l) represents an email recipient timestamp.

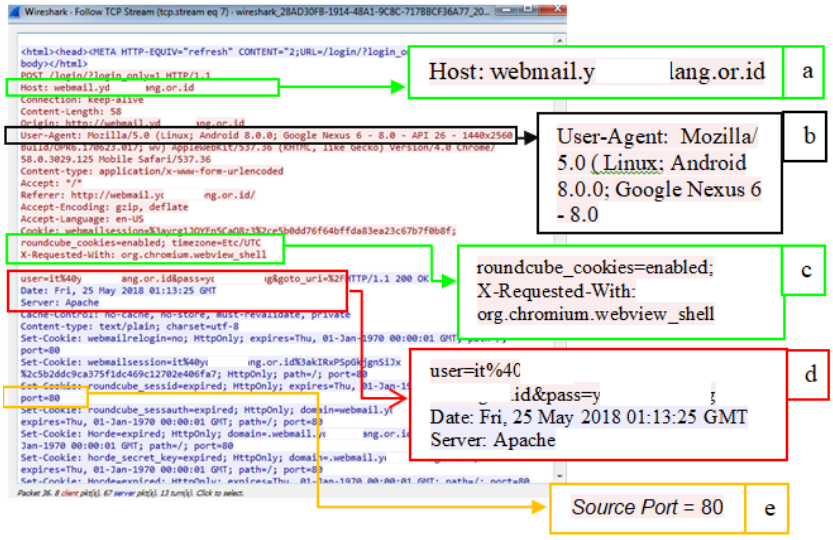

Figure 8. TCP-Stream Wireshark

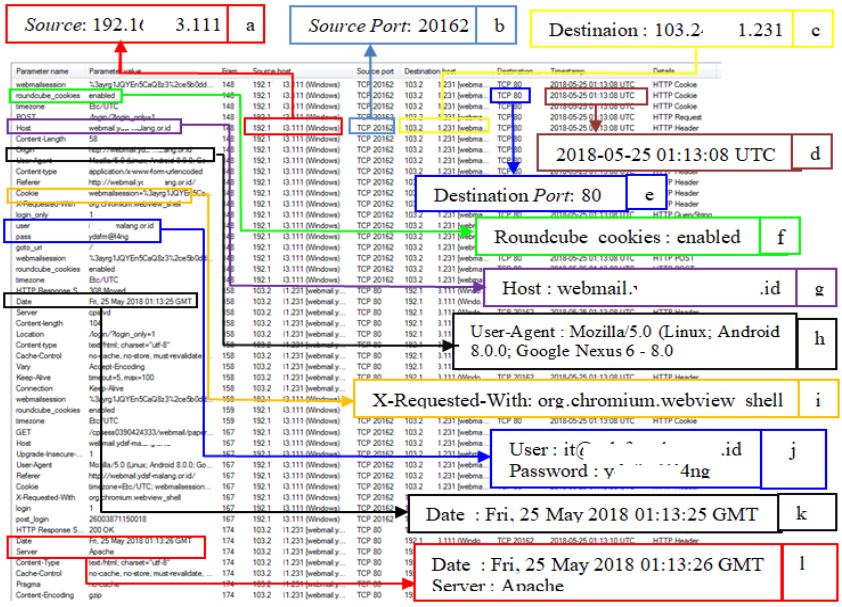

Figure 9. Netwokminer sniffing result

3.4. Reporting

This is a report of the results of research on a comparison of Wireshark and Networkminer forensic tools. In Figure 10, it is the result found. Figure 10 is the result of a comparison of Wireshark and networkminer forensic tools, it is known that 92.3% of the evidence obtained from Wireshark tools and 100% of evidence can be found with the Network Miner tools. Extraction in Figure 10 uses Orange software.

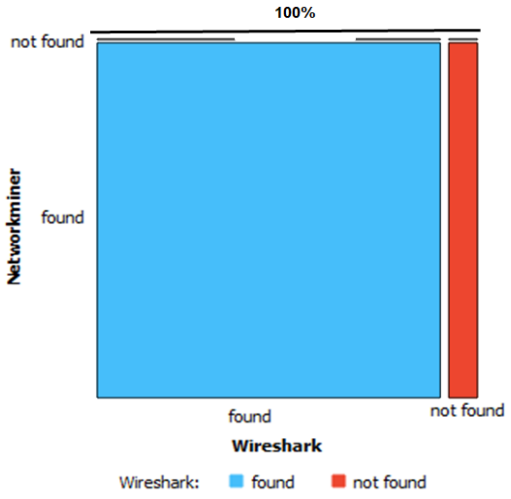

Figure 10. Comparison of forensics tools

4. Conclusion

Based on the results of our research we conducted a comparison of Wireshark and Networkminer forensic tools to obtain digital evidence on Android-based live email service in live forensics. In the process of a comparison of forensic tools, the method we use is mobile forensic methods based on the guidelines available and prepared by the National Institute of Standards and Technology (NIST). The results of comparative analysis of Wireshark and networkminner forensic tools obtained evidence, such as e-mail delivery timestamp, e-mail recipient timestamp,

sender protocol port, recipient protocol port, and source address IP and destination IP address. Networkminer forensic tools have succeeded in getting more digital evidence than Wireshark. Wireshark cannot capture the receiving port and networkminner successfully captures the receiving port. Networkminer has the ability to get digital evidence in emails so that the evidence can be used in court. In the next research, we gave advice to compare more forensic tools in email and on networks that run live forensics.

References

[1] Jones W, Bruce H, Bates MJ, Belkin N, Bergman O, Marshall C. *Personal information management in the present and future perfect: Reports from a special NSF-sponsored workshop*. Proceedings of the American Society for Information Science and Technology. 2005; 42(1).

[2] Whittaker S, Bellotti V, Gwizdka J. Email in personal information management. *Communications of the ACM*. 2006; 49(1): 68-73.

[3] Ayers R, Jansen W, Brothers S. Guidelines on mobile device forensics. *NIST Special Publication 800-101 Revision 1*. 2014; 1(1): 85.

[4] Ademu IO, Imafidon CO, Preston DS. A new approach of digital forensic model for digital forensic investigation. *Int. J. Adv. Comput. Sci. Appl*. 2011; 2(12): 175–178.

[5] statCounter Global States. Mobile Operating System Market Share Indonesia. 2018.

[6] Zareen MS, Waqar A, Aslam B. *Digital forensics: Latest challenges and response*. 2013 2nd National Conference on Information Assurance (NCIA). 2013: 21–29.

[7] Umar R, Riadi I, Muthohirin BF. Acquisition of Email Service Based Android Using NIST. Kinet. Game Technol. *Inf. Syst. Comput. Netw. Comput. Electron. Control*. 2018; 3(3): 263-70.

[8] Bin Abd Razak S, Bin Mohamad AF. *Identification of spam email based on information from email header*. Int. Conf. Intell. Syst. Des. Appl. ISDA. 2014: 347–353.

[9] Fadlil A, Riadi I, Aji S. Review of detection DDOS attack detection using naive bayes classifier for network forensics. *Bulletin of Electrical Engineering and Informatics*. 2017; 6(2): 140-–148.

[10] Cao Q, Qiao Y. *Machine Learning to Detect Anomalies in Web Log Analysis*. 2017 3rd IEEE International Conference on Computer and Communications (ICCC). 2017: 519–523.

[11] Alspaugh S, Chen B, Lin J, Ganapathi A, Hearst M, Katz R. *Analyzing log analysis: An empirical study of user log mining*. 28th Large Installation System Administration Conference (LISA14). 2014: 53–68.

[12] Fenu G, Solinas F. *Live digital forensics: Windows XP vs windows 7*. ICIA 2013 Second International Conference on Informatics and Applications. 2013: 1–6.

[13] Qi Z, Xiang C, Ma R, Li J, Guan H, Wei DS. ForenVisor: A tool for acquiring and preserving reliable data in cloud live forensics. *IEEE Transactions on Cloud Computing*. 2017; 5(3): 443–456.

[14] Harichandran VS, Walnycky D, Baggili I, Breitinger F. Cufa: A more formal definition for digital forensic artifacts. *Digital Investigation*. 2016; 18: S125–S137.

[15] Brown CS. Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*. 2015; 9(1): 55–119.

[16] Ndatinya V, Xiao Z, Manepalli VR, Meng K, Xiao Y. Network forensics analysis using Wireshark. *International Journal of Security and Networks*. 2015; 10(2): 91-106.

[17] Kolhe M, Ahirao P. Live Vs Dead Computer Forensic Image Acquisition. *Int. J. Comput. Sci. Inf. Technol*. 2017; 8(3): 455–457.

[18] Riadi I, Umar R, Nasrulloh IM. Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods. *Lontar Komputer: Jurnal Ilmiah Teknologi Informasi*. 2018: 169–181.

[19] Devendran VK, Shahriar H, Clincy V. A comparative study of email forensic tools. *Journal of Information Security*. 2015; 6(2): 111–117.

[20] Paglierani J, Mabey M, Ahn GJ. *Towards comprehensive and collaborative forensics on email evidence*. 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. 2013: 11–20.

[21] Banday MT. Techniques and Tools for Forensic Investigation of E-mail. *International Journal of Network Security & Its Applications*. 2011; 3(6): 227–241.

[22] Chhabra GS, Bajwa DS. Review of E-mail System, Security Protocols and Email Forensics. *International Journal of Computer Science & Communication Networks*. 2015; 5(3): 201–211.

[23] Stadlinger J, Dewald A. A forensic email analysis tool using dynamic visualization. *Journal of Digital Forensics, Security and Law*. 2017; 12(1): 6.

[24] Umar R, Riadi I, Zamroni GM. Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*. 2018; 8(3): 949-955.

[25] Grance T, Chevalier S, Kent K, Dang H. Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response. National Institute ofStandards and Technology. Report Number: NIST Special Publication 800-86. 2005.