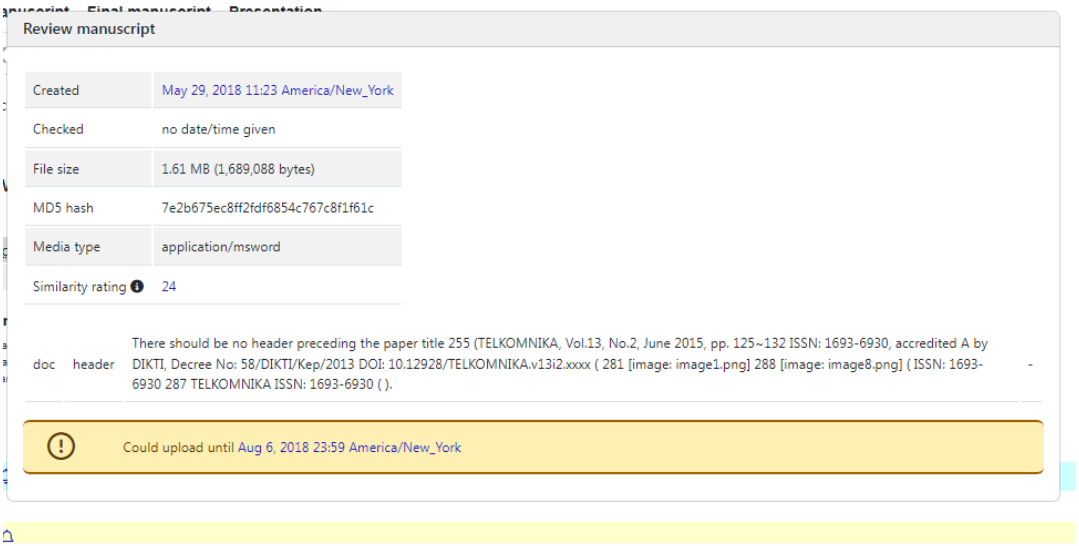
RINGKASAN BUKTI KORESPONDENSI

Judul Artikel : Live forensics of tools on android devices for email forensics
Penulis : Rusydi Umar, Imam riadi, Bashor Fauzan Muthohirin
Jurnal : Telkomnika Vol. 17 No. 4 (2019)
1 Lampiran 1 : Penulis melakukan submission artikel pada 29 May 2018 pada 1st International Conference and Workshop on Telecommunication, Computing, Electronics and Control 2018
2 Lampiran 2 : Pada tanggal 15 Juli 2018, penulis mendapatkan pemberitahuan bahwa penulis diminta untuk merevisi artikel (revisions required)
3 Lampiran 3 : Pada tanggal 04 Agustus 2018, penulis mengirimkan hasil revisi artikel
4 Lampiran 4 : Pada tanggal 4 Agustus 2018, penulis mendapatkan pemberitahuan bahwa artikel diterima (accept submission)
5 Lampiran 5 : Pada bulan Agustus 2019, artikel dinyatakan terbit (published)

1 Lampiran 1



Review manuscript

Created	May 29, 2018 11:23 America/New_York
Checked	no date/time given
File size	1.61 MB (1,689,088 bytes)
MD5 hash	7e2b675ec8ff2fdf6854c767c8f1f61c
Media type	application/msword
Similarity rating	24

doc	header	There should be no header preceding the paper title 255 (TELKOMNIKA, Vol.13, No.2, June 2015, pp. 125~132 ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013 DOI: 10.12928/TELKOMNIKA.v13i2.xxxx (281 [image: image1.png] 288 [image: image8.png] (ISSN: 1693-6930 287 TELKOMNIKA ISSN: 1693-6930 ( ).	-

Could upload until Aug 6, 2018 23:59 America/New_York

TELKOMNIKA, Vol.13, No.2, June 2015, pp. 125~132
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v13i2.xxxx

A Comparison 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, Yogyakarta Indonesia
[2]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta Indonesia
Jln. Prof. Dr. Soepomo, S.H., Janturan, Yogyakarta, 563515 Indonesia
*Corresponding author, e-mail: bashor1707048017@webmail.uad.ac.id

Abstract

The development of information and communication technology are growing rapidly, such as email. Email is one of the communication tools that are used to send and received the information in a matter of minutes and even seconds. Speed in communication causes weaknesses that cybercrime can exploit. Cybercrime is any criminal activity that involves a network, cybercrime must be leaving digital evidence. Digital evidence can be done live forensics using wireshark and networkminer, that are software capable of capturing data packets across the internet network. This study will conduct a comparison of wireshark and networkminer forensic tools, these research subjects focus on e-mail services based android to obtain digital evidence as much as possible on both of these tools. In this process using mobile forensic methods the national institute of standards and technology (NIST). The result of this research is that networkminer get more digital evidence than wireshark.

Keywords*: Email, Networkminer, NIST, Wireshark*

1. Introduction

The development of technology can facilitate human work so that more effective, one of the development of technology is 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 who 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]. The familiar smartphone used by the community is an Android based smartphone.

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].

Received February 23, 2014; Revised May 29, 2014; Accepted June 12, 2014

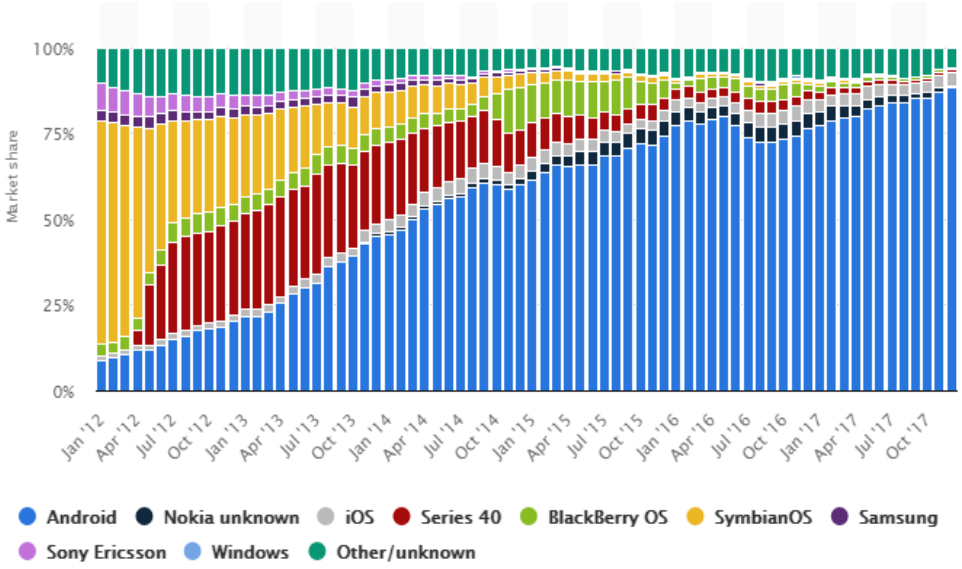


Figure 1. Smartphone User in Indonesia

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 emails it can be detected using several ways, such as viewing email headers [7]–[9], *digital signature*, and reading logs [10]–[13] . Digital forensics is the study of how to deal with crimes involving technology such as computers. 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 [14].

Packages run on the network can be used as digital evidence by way of live forensics [15]–[17], Software that can be used is wireshark and networkminer. Wireshark is a Network Protocol Analyzer software used for packet sniffing and tries to capture network packets and attempts to display all the information in the package as much detail as possible [18]. networkminer is a network analysis software for windows, networkminer has the same functionality as Wireshark is network analyzer protocol [19].

The law on cybercrime crimes is set in the laws on ITE in Indonesia [20]. 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. No criminal cases have escaped evidentiary evidence. Almost all criminal prosecution, always leaning 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 [21].

in [22] Identification and Analysis of Email and Contacts Artefacts on iOS and OSX Kenneth, The tool used for sniffing emails is wireshark. The research is limited to Apple's iOS and OSX Kenneth devices, the results of which are getting artifacts from the Mail and Contacts app.

From the above background, the authors will conduct research on the comparison of forensic tools on the email service based android to get the digital evidance using mobile forensic method based on the guidelines that have been available and prepared by the National Institute of Standards and Technology (NIST) as the process of getting the digital evidence.

2. Research Method

In this study the method used is the mobile forensic method 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 [23].

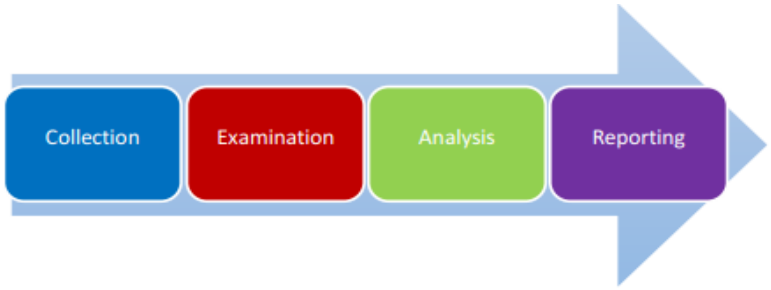


Figure 2. Stages of the NIST Method

1. 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.
2. 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.
3. 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.
4. Re*port*ing
   Report the results of the analysis including the description of the actions performed, what tools are used and the procedures used. After that researchers write the results of the test as well as the results of testing evaluation of Android**.**

3. Results and Analysis

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

3.1. Collection

At this stage of collecting goods on smartphone owners, the smartphone used is google nexus 6 and android version ando 8.0. Smartphone used in this research is smartphone emulator genymotion version 2.12. The following is a collection stage concept.

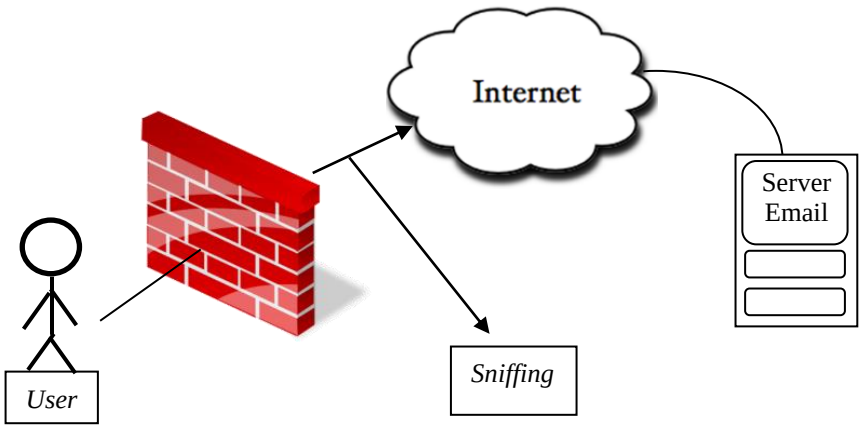


Figure 3. Conceptual Stages in Collection Process.

In 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.

3.2. Examination

At this stage, performing a comparison on wireshark and networkminer forensic tools. In the process of getting the proof of email must be opened through the original browser from smarphone. Smartphone Here is the comparison stage of forensic tools in the process of obtaining digital evidence.

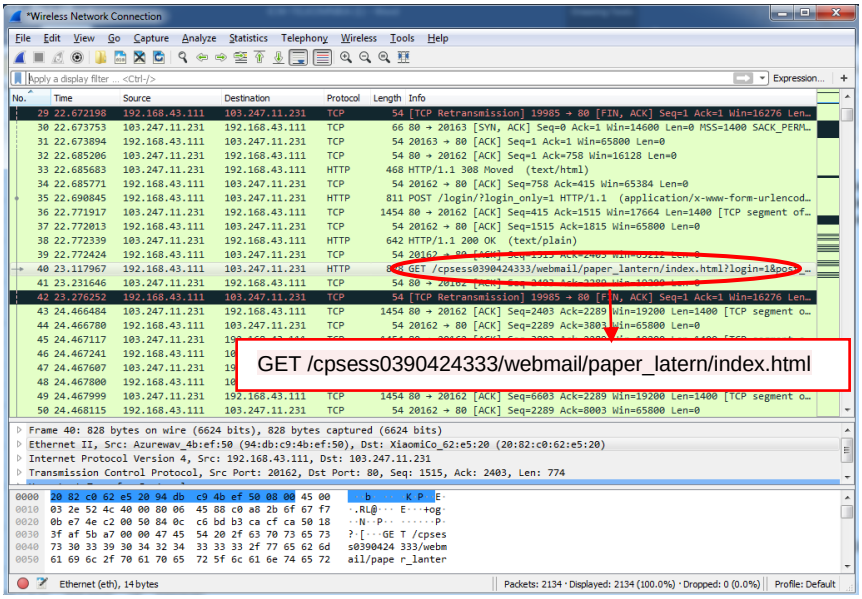


Figure 4. Process examination tools Wireshark

In Figure 4 is a sniffing process using wireshark tools. Tools wireshark successfully do sniffing data packets on email service that opened using android browser, can see there is a red circle in picture 4.

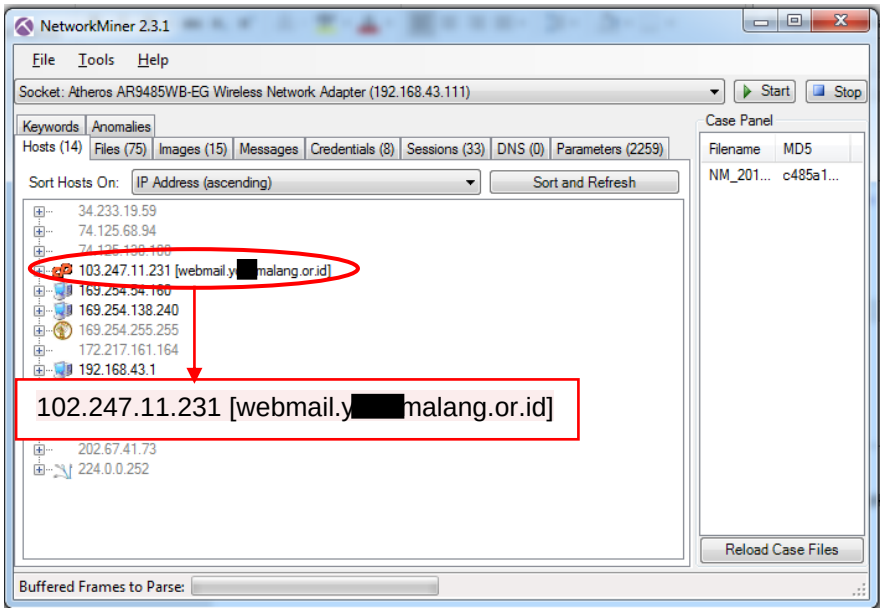


Figure 5. Process examination tools Networkminer

In Figure 5 is a Networkminer sniffing tool. Networkminer succeeded in sniffing and capturing on email packets marked with found IP Address and webmail, can see there is a red circle in figure 5.

3.3. Analysis

At this stage is the result obtained by wireshark and networkminer forensic tools on android-based email is complete. Here are the results obtained.

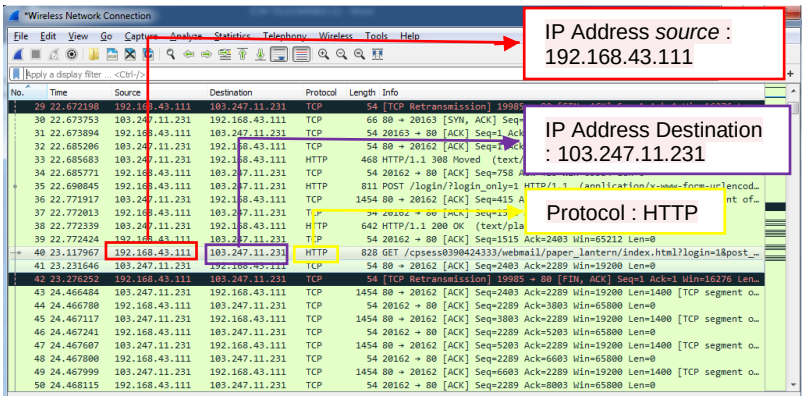


Figure 6. Results of Wireshark Sniffing.

In Figure 6 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.

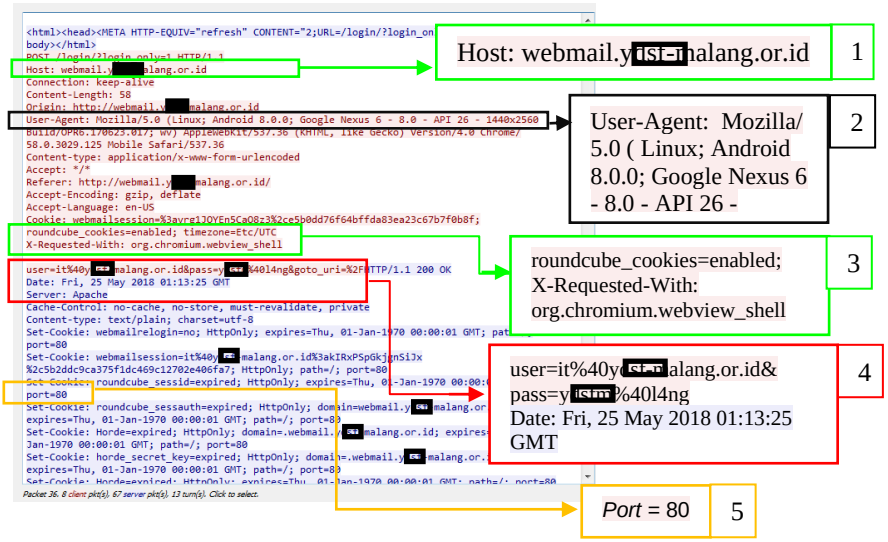


Figure 7. TCP-Stream *Wireshark*.

In Figure 7 is the contents of the TCP stream, in the TCP Stream gives a lot of information. The following information can be found:

- Number 1. Is the webmail host.
- Number 2. Is the smartphone information used.
- Number 3. Is the browser used to open the email.
- Number 4. Is Username and password of the user, timestamp email delivery, and email server.
- Number 5. Is the sending port used.
- Number 6. It is an email recipient timestamp.

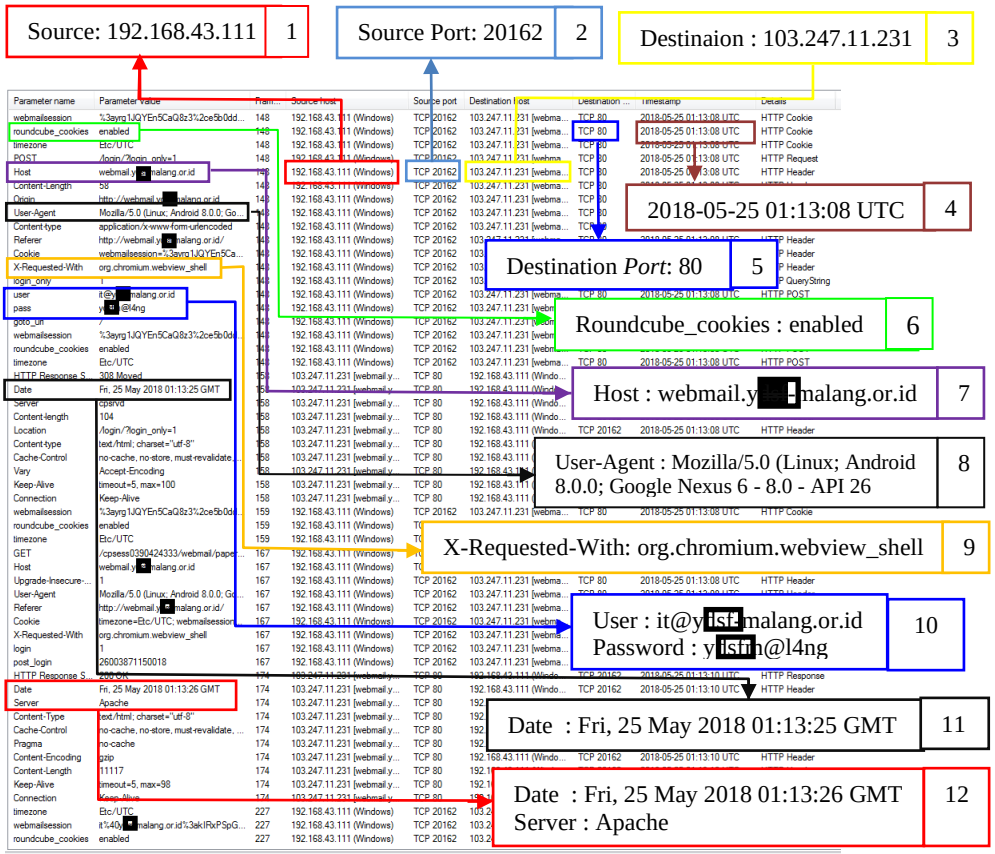


Figure 8. Netwokminer Sniffing Resutl.

In Figure 8 is a result that is captured by networkminer tools. Networkminer can be a lot of information. The following information can be found:

- Number 1. Is the IP Address source.
- Number 2. Is port source.
- Number 3. Is the IP Address destination.
- Number 4. It is the timestamp information on the server.
- Number 5. Is the destination port.
- Number 6. Is the interface used is roudcube.
- Number 7. Is the webmail host used.
- Number 8. Is the browser used to open the email.
- Number 9. Is the user's username and password.
- Number 10. It is an email delivery timestamp.
- Number 11. Represents an email recipient timestamp.

3.4. Re*port*ing

At this stage it is the result of comparison comparison of wireshark and networkminer forensic tools. In Table 1. It is the result found by wireshark and networkminer.

Table 1. Comparison of Forensic Tools

No	Ditemukan	*Wireshark*	*Networkminer*
1.	Host	✓	✓
2.	Username and password	✓	✓
3.	Browser for open email	✓	✓
4.	Server mail	✓	✓

5.	Timestamp email delivery	✓	✓
6.	Timestamp recipient of email	✓	✓
7.	Port delivery	✓	✓
8.	Port recipient	-	✓
9.	IP Address source	✓	✓
10.	IP Address destination	✓	✓
11.	Layout mail	✓	✓
12.	Used smartphone	✓	✓
13.	Interface webmail	✓	✓

Table 1 is sniffing done with wireshark and networkminer forensic tools get different results. The wireshark forensic tool can not find the receiving port, while the networkminer succeeded in sniffing the receiving port. So from the results of the research networkminer get more digital evidence.

4. Conclusion

Based on the results of research that has been done, this study comparing wireshark and networkminer forensic tools to obtain digital evidence on email service based android. The process of comparison of forensic tools to obtain digital evidence using mobile forensic methods is the National Institute of Standards and Technology (NIST). In the early stages of this research is to collect goods on android smartphone. The android smartphone used is android that runs on genymotion emulator. In the second stage of testing, testing is done to compare wireshark and networkminer forensic tools. Forensic tools are running on windows 7 operating system, wireshark and networkminer managed to get evidence such as IP Address pengrim, timestamp, port and others. Networkminer forensic tools successfully get more digital evidence than network minner.

References

[1] W. Jones, H. Bruce, M. J. Bates, N. Belkin, O. Bergman, and C. Marshall, "Personal information management in the present and future perfect: Reports from a special NSF-sponsored workshop," *Proc. Am. Soc. Inf. Sci. Technol.*, vol. 42, no. 1, p. n/a-n/a, 2006.

[2] S. Whittaker, V. Bellotti, and J. Gwizdka, "Email in personal information management," *Commun. ACM*, vol. 49, no. 1, p. 68, 2006.

[3] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.

[4] I. O. Ademu, C. O. Imafidion, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.

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

[6] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android ' s Blackberry Messenger Using NIST Mobile," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. May, pp. 1–7, 2017.

[7] H. Guo, B. Jin, and W. Qian, "Analysis of email header for forensics purpose," *Proc. - 2013 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2013*, pp. 340–344, 2013.

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

[9] D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," *IJCSIS) Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, pp. 326–331, 2017.

[10] I. Riadi, J. Eko Istiyanto, and A. Ashari, "Log Analysis Techniques using Clustering in Network Forensics," *IJCSIS) Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. 7, 2012.

[11] Y. Zulfadhilah, M., Riadi, I., Prayudi, "Log Classification using K-Means Clustering for Identify Internet User Behaviors," *Int. J. Comput. Appl.*, vol. 154, no. 3, pp. 34–39, 2016.

[12] I. Riadi, J. E. Istiyanto, A. Ashari, and S. Subanar, "Internet Forensics Framework Based-on Clustering."

[13] I. Riadi, A. Wirawan Muhammad, and S. Sunardi, "Neural Network-Based DDOS Detection," no.

August, 2017.
[14] M. Agarwal and M. Gupta, "Systematic digital forensic investigation model," *J. Comput.*, no. 5, pp. 118–131, 2011.
[15] M. A. Zulkifli, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," vol. 180, no. 35, pp. 23–30, 2018.
[16] M. I. Mazdadi, I. Riadi, and A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, pp. 406–410, 2017.
[17] M. S. Ahmad, I. Riadi, and Y. Prayudi, "Investigation Live Forensics from User Side to Analyze Man In The Middle Attack based Evil Twin," *ILKOM*, vol. 9, no. April, pp. 1–8, 2017.
[18] S. Raghavan and S. V Raghavan, "A study of forensic & analysis tools," *2013 8th Int. Work. Syst. Approaches to Digit. Forensics Eng.*, pp. 1–5, 2013.
[19] D. Walnycky, I. Baggili, A. Marrington, J. Moore, and F. Breitinger, "Network and device forensic analysis of Android social-messaging applications," *Digit. Investig.*, vol. 14, no. S1, pp. S77–S84, 2015.
[20] R. Indonesia, *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Departemen Komunikasi Dan Informatika, Republik Indonesia*. 2008.
[21] U. Rusydi, A. Yudhana, and M. N. Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, p. 5, 2018.
[22] K. M. Ovens and G. Morison, "Identification and analysis of email and contacts artefacts on iOS and OSX," *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 321–327, 2016.
[23] G. M. Umar, R., Riadi, I., Zamroni, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.

2 Lampiran 2

UNIVERSITAS
AHMAD DAHLAN

BASHOR FAUZAN MUTHOHIRIN <bashor1707048017@webmail.uad.ac.id>

[ICW-TELKOMNIKA 2018] Decision for paper 'A Comparison of Tools on Android Devices for Email Forensics'

2 pesan

lppi@uad.ac.id.edas.info <lppi@uad.ac.id.edas.info> 15 Juli 2018 pukul 10.44
Balas Ke: lppi@uad.ac.id
Kepada: Bashor Fauzan Muthohirin <bashor1707048017@webmail.uad.ac.id>, Rusydi Umar <rusydi_umar@rocketmail.com>, Imam Riadi <imam.riadi@is.uad.ac.id>

Dear Mr. Bashor Muthohirin:

After careful review, the decision for your paper #1570463800 "A Comparison of Tools on Android Devices for Email Forensics" for ICW-TELKOMNIKA 2018 is REVISIONS REQUIRED. You are asked to submit a revised full manuscript for re-review, according to the comment from reviewers. The due date for revision is Aug 1, 2018.

We would like your cooperation with the double check of your REVISED paper:
(1) TEMPLATE for preparing final camera ready paper: http://goo.gl/FiPFbF
(2) Checklist for preparing your paper for publication: http://www.journal.uad.ac.id/index.php/TELKOMNIKA/about/editorialPolicies#custom-1
(3) Please ensure the maximum page of your final paper is 8-page, but still allowed up to 12 pages (required to pay an extra fee).
(4) Most importantly, please ensure the similarity score is less than 30%. If the similarity score of revised version is more than 30%, the paper will be rejected from consideration for ICW-TELKOMNIKA 2018.

The reviews are below or can be found at http://edas.info/showPaper.php?m=1570463800, using your EDAS login name bashor1707048017@webmail.uad.ac.id.

Best Regards,
Assoc. Prof. Dr. Tole Sutikno
General Chair
Editor-in-Chief, TELKOMNIKA Telecommunication, Computing, Electronics and Control
Scopus indexed journal, SJR: 0.265, CiteScore: 0.63, SNIP: 0.580
Q3 on Electrical & Electronics Engineering

--
======= Review 1 =======

> *** Novelty and Contribution: Rate the degree of scientific contribution provided by this paper. Do the authors offer new findings? Do they give proper explanation and detailed analysis?
Average (2)

> *** Paper Presentation: What is your evaluation on the quality of presentation from this paper (e.g. figures, tables, formats, etc.)?
Acceptable (3)

> *** Detailed Comments: Please provide detailed comments that will be helpful to the TPC for assessing the paper. Also provide feedback to the authors.

* The proposed approach could be explained with extra details.
* The challenge and contribution of the paper are not clear.
* The main aim and contribution of the paper are not understandable.

> *** Recommendation: Your overall rating.
Borderline (3)

BASHOR FAUZAN MUTHOHIRIN <bashor1707048017@webmail.uad.ac.id> 26 Juli 2018 pukul 10.22
Kepada: lppi@uad.ac.id

Good morning

sorry, I want to upload a revision, I can upload through what?
i check in edes there is no place upload revision.

thanks
[Kutipan teks disembunyikan]

TELKOMNIKA, Vol.17, No.1, February 2019, pp. 101~10x
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v17i1.xxxx

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, Yogyakarta Indonesia
[2]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta Indonesia
Jln. Prof. Dr. Soepomo, 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 using 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 who 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].

Received September 5, 2017; Revised December 28, 2018; Accepted January 12, 2019

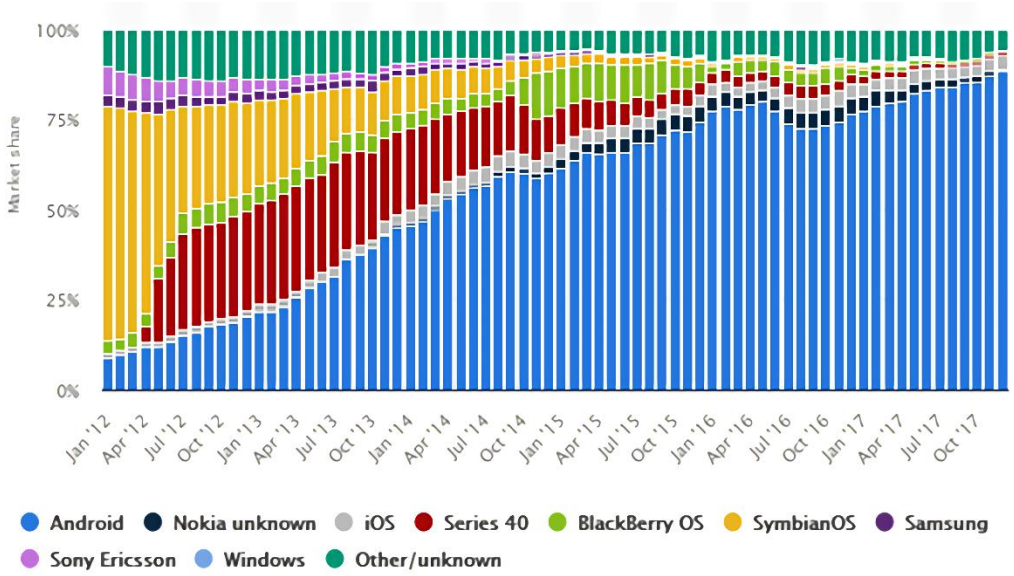


Figure 1. Smartphone User in Indonesia

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 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]. No criminal cases have escaped evidentiary evidence. Almost all criminal prosecution, always leaning 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. 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[15].

In [16] 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 [17] the title of Network and device forensic analysis of Android social-messaging applications. The study focused on detecting the presence of unclear artifacts associated with email accounts, retrieving data from service providers, and representatives email in a well-structured format based on existing standards.

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 [18].

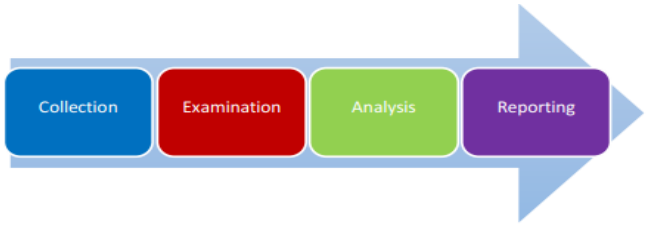


Figure 2. Stages of NIST Method

1. 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.
2. 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.
3. 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.
4. Reporting
   Report the results of the analysis including the description of the actions performed, what tools are used and the procedures used.

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.

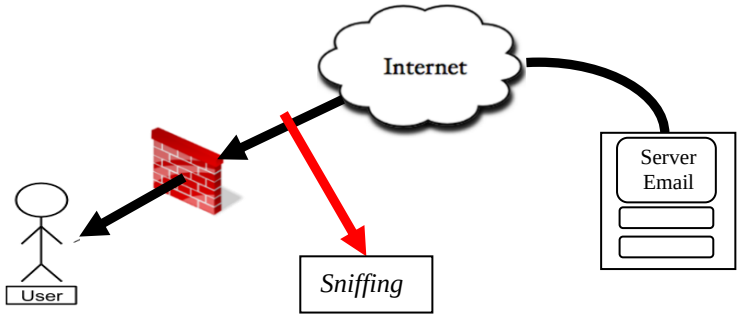


Figure 3. Conceptual Stages in Collection Process

In 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.

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. Android Oreo 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.

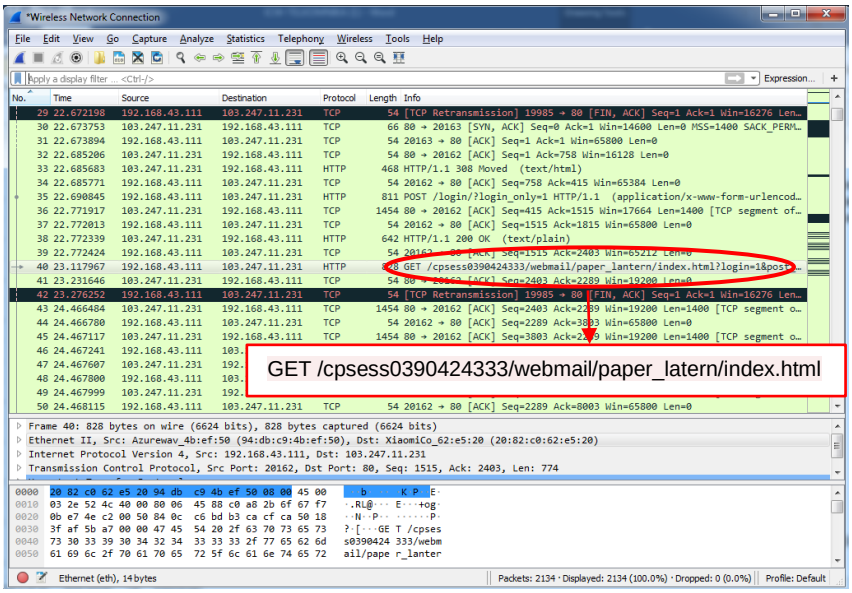


Figure 5. Process Examination Tools Wireshark

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.

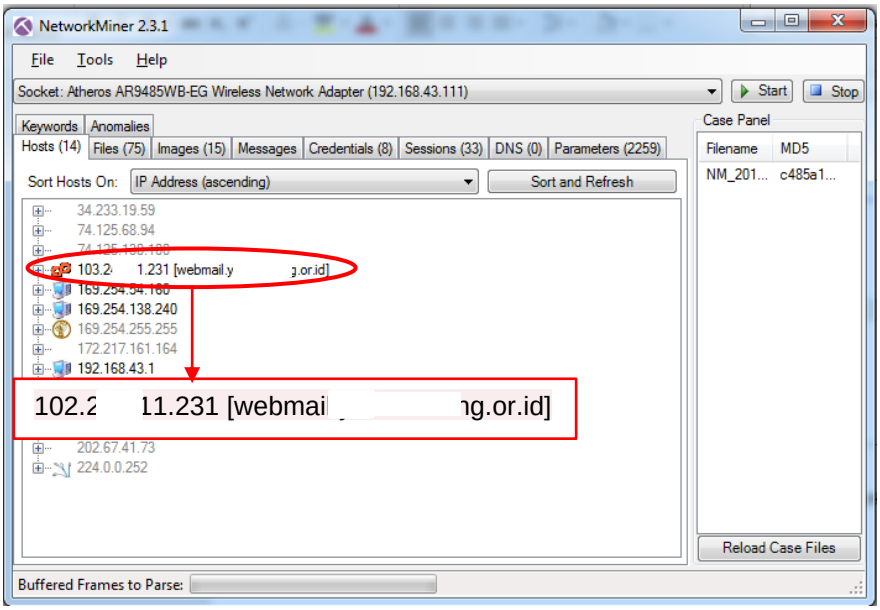


Figure 6. Process Examination Tools Networkminer

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.

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.

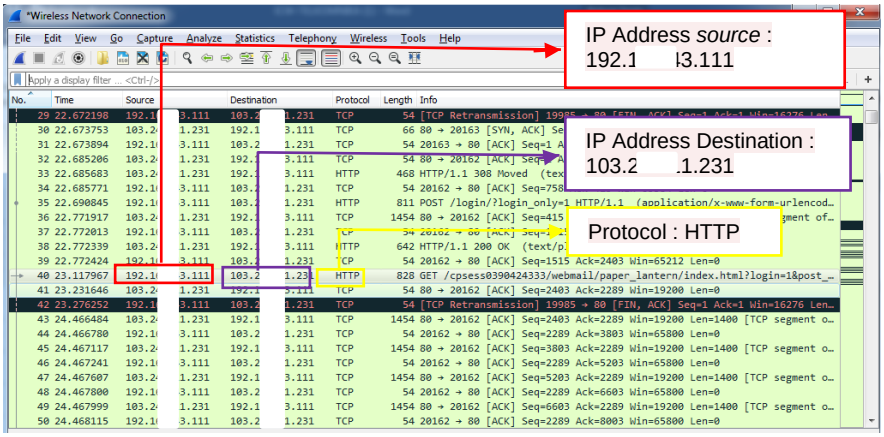


Figure 7. Results of Wireshark Sniffing

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.

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.

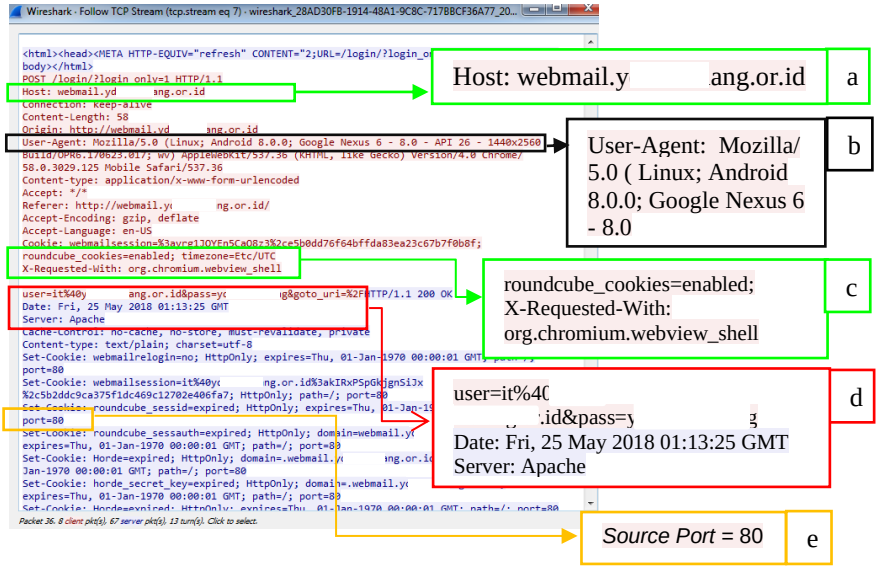


Figure 8. TCP-Stream Wireshark

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.

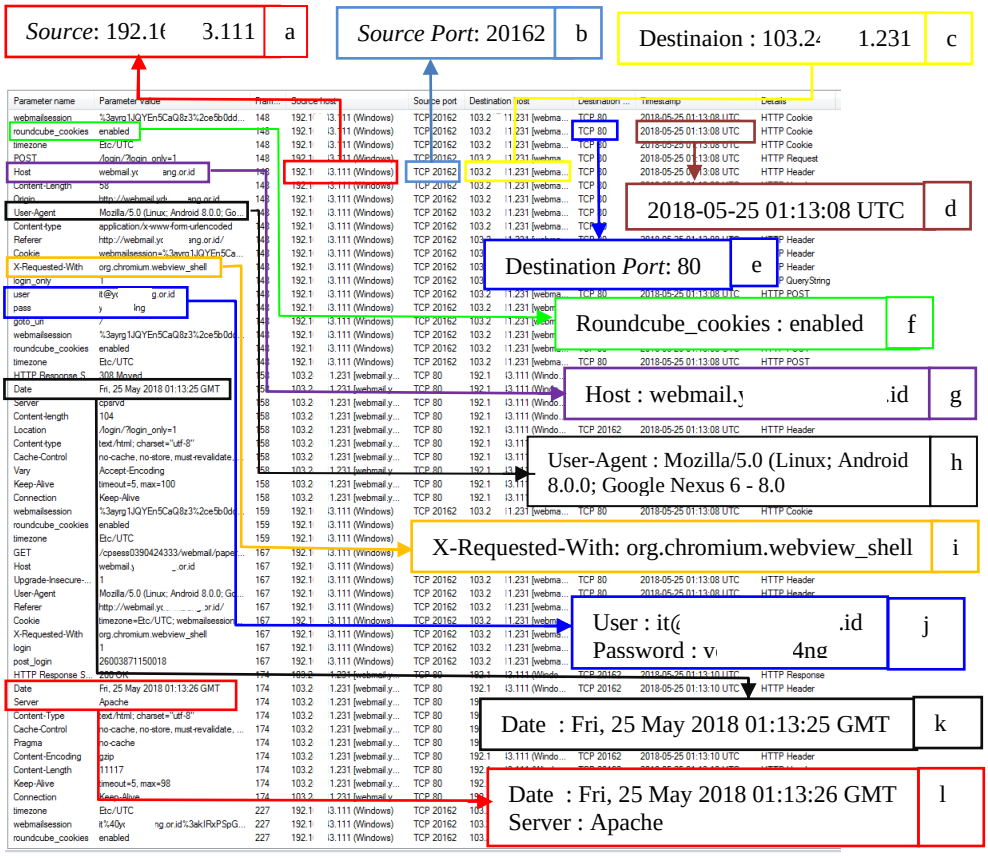


Figure 9. Netwokminer Sniffing Result

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.

3.4. Reporting

Reporting the results of research on a comparison of Wireshark and Networkminer forensic tools. In Table 1, It is the result found.

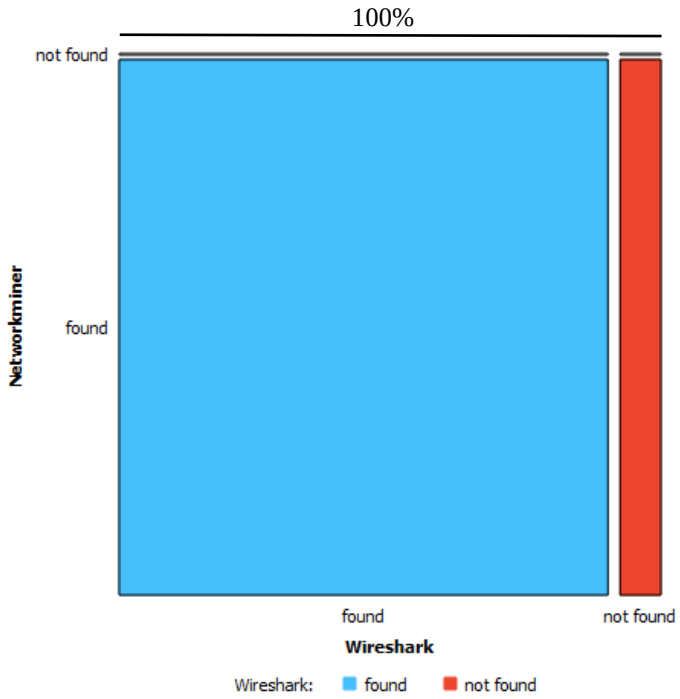


Figure 10. Comparison of Forensics Tools

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.

4. Conclusion

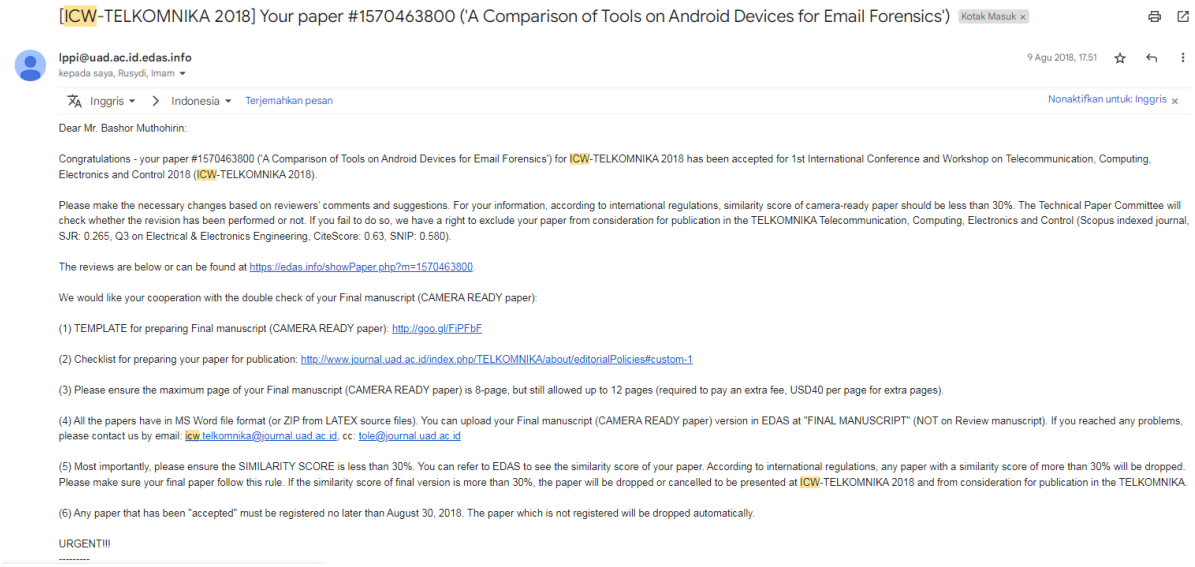
Based on the results of our research we conducted a comparison of Wireshark and Networkminer forensic tools to obtain digital evidence on Android-based live email service in live forensics. In the process of a comparison of forensic tools, the method we use is mobile forensic methods based on the guidelines 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, 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 study, we gave advice to compare more forensic tools in email and on networks that run live forensics.

References

[1] W. Jones, H. Bruce, M. J. Bates, N. Belkin, O. Bergman, and C. Marshall, “Personal information management in the present and future perfect: Reports from a special NSF-sponsored workshop,”

Proc. Am. Soc. Inf. Sci. Technol., vol. 42, no. 1, p. n/a-n/a, 2006.
[2] S. Whittaker, V. Bellotti, and J. Gwizdka, "Email in personal information management," *Commun. ACM*, vol. 49, no. 1, p. 68, 2006.
[3] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.
[4] I. O. Ademu, C. O. Imafidion, and D. S. Preston, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 175–178, 2011.
[5] statCounter Global States, "Mobile Operating System Market Share Indonesia," 2018.
[6] M. S. Zareen, A. Waqar, and B. Aslam, "Digital Forensics : Latest Challenges and Response," pp. 21–29, 2013.
[7] S. Bin Abd Razak and A. F. Bin Mohamad, "Identification of spam email based on information from email header," *Int. Conf. Intell. Syst. Des. Appl. ISDA*, pp. 347–353, 2014.
[8] R. Umar, I. Riadi, and B. fauzan Muthohirin, "Acquisition Of Email Service Based Android," vol. 3, no. 4, 2018.
[9] A. Fadil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensics," *Bull. Electr. Eng. Informatics*, vol. 6, no. 2, pp. 140–148, 2017.
[10] Q. Cao and Y. Qiao, "Machine Learning to Detect Anomalies in Web Log Analysis," pp. 519–523, 2017.
[11] S. Alspaugh, B. Chen, J. Lin, A. Ganapathi, M. A. Hearst, and R. Katz, "Analyzing log analysis: an empirical study of user log mining," pp. 53–68, 2014.
[12] G. Fenu and F. Solinas, "Live digital forensics: Windows XP vs Windows 7," *2013 2nd Int. Conf. Informatics Appl. ICIA 2013*, pp. 1–6, 2013.
[13] Z. Qi, C. Xiang, R. Ma, J. Li, H. Guan, and D. S. L. Wei, "ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 443–456, 2017.
[14] C. S. D. Brown, "Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice," *Int. J. Cyber Criminol.*, vol. 9, no. 1, pp. 55–119, 2015.
[15] M. Kolhe and P. Ahirao, "Live Vs Dead Computer Forensic Image Acquisition," *Int. J. Comput. Sci. Inf. Technol.*, vol. 8, no. 3, pp. 455–457, 2017.
[16] V. K. Devendran, H. Shahriar, and V. Clincy, "A Comparative Study of Email Forensic Tools," *J. Inf. Secur.*, vol. 06, no. 02, pp. 111–117, 2015.
[17] J. Paglierani, M. Mabey, and G.-J. Ahn, "Towards comprehensive and collaborative forensics on email evidence," *Collab. Comput. Networking, Appl. Work. (Collaboratecom), 2013 9th Int. Conf. Conf.*, pp. 11–20, 2013.
[18] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, 2018.

4 Lampiran 4



[ICW-TELKOMNIKA 2018] Your paper #1570463800 ('A Comparison of Tools on Android Devices for Email Forensics') Kotak Masuk ×

lppi@uad.ac.id.edas.info 9 Agu 2018, 17.51
kepada saya, Rusydi, Imam

Inggris > Indonesia Terjemahkan pesan Nonaktifkan untuk: Inggris ×

Dear Mr. Bashor Muthohirin:

Congratulations - your paper #1570463800 ('A Comparison of Tools on Android Devices for Email Forensics') for ICW-TELKOMNIKA 2018 has been accepted for 1st International Conference and Workshop on Telecommunication, Computing, Electronics and Control 2018 (ICW-TELKOMNIKA 2018).

Please make the necessary changes based on reviewers' comments and suggestions. For your information, according to international regulations, similarity score of camera-ready paper should be less than 30%. The Technical Paper Committee will check whether the revision has been performed or not. If you fail to do so, we have a right to exclude your paper from consideration for publication in the TELKOMNIKA Telecommunication, Computing, Electronics and Control (Scopus indexed journal, SJR: 0.265, Q3 on Electrical & Electronics Engineering, CiteScore: 0.63, SNIP: 0.580).

The reviews are below or can be found at https://edas.info/showPaper.php?m=1570463800.

We would like your cooperation with the double check of your Final manuscript (CAMERA READY paper):

(1) TEMPLATE for preparing Final manuscript (CAMERA READY paper): http://goo.gl/FiPFbF

(2) Checklist for preparing your paper for publication: http://www.journal.uad.ac.id/index.php/TELKOMNIKA/about/editorialPolicies#custom-1

(3) Please ensure the maximum page of your Final manuscript (CAMERA READY paper) is 8-page, but still allowed up to 12 pages (required to pay an extra fee, USD40 per page for extra pages).

(4) All the papers have in MS Word file format (or ZIP from LATEX source files). You can upload your Final manuscript (CAMERA READY paper) version in EDAS at "FINAL MANUSCRIPT" (NOT on Review manuscript). If you reached any problems, please contact us by email: icw.telkomnika@journal.uad.ac.id, cc: tole@journal.uad.ac.id

(5) Most importantly, please ensure the SIMILARITY SCORE is less than 30%. You can refer to EDAS to see the similarity score of your paper. According to international regulations, any paper with a similarity score of more than 30% will be dropped. Please make sure your final paper follow this rule. If the similarity score of final version is more than 30%, the paper will be dropped or cancelled to be presented at ICW-TELKOMNIKA 2018 and from consideration for publication in the TELKOMNIKA.

(6) Any paper that has been "accepted" must be registered no later than August 30, 2018. The paper which is not registered will be dropped automatically.

URGENT!!!
---

5 Lampiran 5

UNIVERSITAS
AHMAD DAHLAN

BASHOR FAUZAN MUTHOHIRIN <bashor1707048017@webmail.uad.ac.id>

[ICW-TELKOMNIKA 2018]: Preparing final camera ready paper for publication on the TELKOMNIKA (a Scopus indexed journal, SJR Q3)

1 pesan

Int. Conf. - ICW TELKOMNIKA <icw.telkomnika@journal.uad.ac.id> 27 September 2018 pukul 14.00
Kepada: BASHOR FAUZAN MUTHOHIRIN <bashor1707048017@webmail.uad.ac.id>
Cc: "Assoc. Prof. Dr. Tole Sutikno" <tole@journal.uad.ac.id>

Guideline to extend your paper of the 2018 1st International Conference and Workshop on Telecommunication, Computing, Electrical, Electronics and Control (2018 ICW-TELKOMNIKA) to be published on the TELKOMNIKA, a Scopus indexed journal, SJR Q3

****Please pay attention to the details of this email****

#1570463800 entitled "A Comparison of Tools on Android Devices for Email Forensics"

Dear Prof/Dr/Mr/Mrs Bashor Fauzan Muthohirin

TELKOMNIKA Telecommunication, Computing, Electronics and Control is a Scopus indexed journal, SJR Q3, and ONLY publishes high quality papers. A high quality paper has:
(1) a clear statement of the problem the paper is addressing;
(2) the proposed solution(s); and
(3) results achieved. It describes clearly what has been done before on the problem, and what is new. The goal of your revised paper is to describe novel technical results.

There are four types of technical results:
1. An algorithm;
2. A system construct: such as hardware design, software system, protocol, etc.; The main goal of your revised paper is to ensure that the next person who designs a system like yours doesn't make the same mistakes and takes advantage of some of your best solutions. So make sure that the hard problems (and their solutions) are discussed and the non-obvious mistakes (and how to avoid them) are discussed.
3. A performance evaluation: obtained through analyses, simulation or measurements;
4. A theory: consisting of a collection of theorems.

Your revised paper should focus on:
1. Describing the results in sufficient details to establish their validity;
2. Identifying the novel aspects of the results, i.e., what new knowledge is reported and what makes it non-obvious;
3. Identifying the significance of the results: what improvements and impact do they suggest.

Second, change title of your paper. The title summarizes the main idea or ideas of your study. A good title contains the fewest possible words needed to adequately describe the content and/or purpose of your research paper. Rarely use abbreviations or acronyms unless they are commonly known. Find the below guide, how to update your paper title.

You have **4 weeks, until October 24, 2018** to revised your paper. Please submit your revised paper by reply this email (icw.telkomnika@journal.uad.ac.id), cc: tole@journal.uad.ac.id. Attach:
1. File Response to Mentor(s) Comments
2. File of your revised paper

When your revised paper reached us, it will be re-checked & reviewed by Editor(s) and Mentor(s) based on your response to Mentor & Coach comments and the following criteria: Relevance, Significance,