KINETIK, Vol. 3, No. 3, August 2018, Pp. 263-270
ISSN : 2503-2259
E-ISSN : 2503-2267

Acquisition of Email Service Based Android Using NIST

Rusydi Umar*[1], Imam Riadi[2], Bashor Fauzan Muthohirin[3]
[1,3]Universitas Ahmad Dahlan/Informatics Engineering Department
[2]Universitas Ahmad Dahlan/Information System Department
rusydi_umar@rocketmail.com*[1], imam.riadi@is.uad.ac.id[2], fauzan.bashor@gmail.com[3]

Abstract

Email is one of the results of the development of information and communication technology. Email is widely used to exchange information by sending and receiving data, such as document files, images, correspondence and others. With the development of technology and information causing crimes in communicating also growing, the perpetrators of cybercrime commonly referred to as cybercrime. Any crime on email made by cyber crime will surely leave evidence, such as IP Address and others. Evidence of the crime can be used in the trial, so it is necessary forensic on the email. The research will do forensics on emails by way of android-based email acquisition using the method used in this study is a forensic method based on upon the available guidelines prepared by the National Institute of Standards and Technology (NIST). The acquisition process on email using smartphone android xiaomi with android version lollipop, from a series of research using forensic methods NIST got an IP address in the email header. IP addresses that have been found can be used digital evidence.

Keywords: *Email, Evidence, Forensics, IP Address, NIST*

1. Introduction

In recent decades, mobile phone users in Indonesia have been increased from 265 people with 50% penetration is internet users from 50% of internet users that 45% access various sources using mobile [1]. Among the most popular digital services in Indonesia are Gmail, Yahoo Mail and Whatsapp. The growth and development of information and communication technology has led us to exchange information via email and with the help of a web browser inside android. Inside the smartphone android can also be installed web browser like google chrome, mozella Firefox, opera, and others. There are 5 emails frequently used by Indonesian people, like Figure 1 [2].

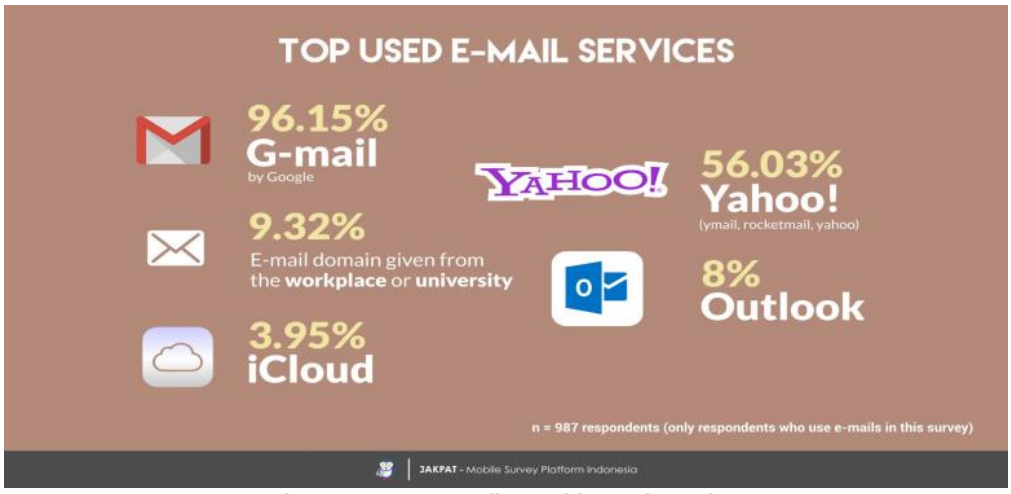

Figure 1. Top Email Used by Indonesian.

There are some emails that are often used by Indonesian people, like Gmail 96.15%, 56.03% yahoo, workplace or university 9:32%, outlook 8% and iCloud 3.95% [2]. As for the reason they use the browser for various reasons such as a faster loading process, easy user interface, safe from viruses, offers many functional features and offers themes for choice [2]. With the increasing number of users cannot be denied anymore if there are impacts in both the positive

Muthohirin, B., Umar, R., & Riadi, I. (2018). Acquisition of Email Service Based Android Using NIST. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 3(3). doi:http://dx.doi.org/10.22219/kinetik.v3i4.637
Receive March 26, 2018; Revise April 21, 2018; Accepted April 21, 2018

and negative impacts. The positive impact is to help complete the activity quickly, and can help a difficult job. Since the negative impact is the abuse of the technology itself is done by people who are not responsible. Email also has a weakness so it can be attacked, one of the crimes in the email there is the theft of username and password [3][4][5]. Crime in cyberspace called cybercrime. Cybercrime is a type of crime associated with utilizing information and communication technologies to gain unauthorized and unlimited access rights, and has a strong characteristic with a technological engineering that relies on a high level of security, from information conveyed and accessed by Internet users [6].

In the crime of cybercrime will leave the evidence, the evidence can be both digital and electronic evidence [7]. Digital evidence can be seen when criminal proceedings take place or when digital evidence has been stored, digital evidence can be handled exclusively by digital forensic science using tools to solve and draw conclusions from criminal cases on digital evidence obtained. In the email is genuine or fake can be detected using a couple of ways to view headers email [8], digital signatures, and read the log [9][10][11]. The handling of crime involving computer technology is still very common for now. Digital forensics is the use of science and methods for discovering, collecting, securing, analyzing, interpreting and presenting digital evidence relating to cases occurring for reconstruction purposes and the validity of the judicial process [12].

The law on cybercrime crimes is set by the laws of ITE [13]. For the crimes of ITE can be criminalized by law or civil just according to the level of crime committed. To arrest the Cybercrime authorities can raise the evil evidence stored in the smartphone as a proof of space. There is no escape from the criminal case of evidence of evidence. Almost all proving criminal cases, always rely on the examination of evidence. At least in addition to proof with other evidences, there is always a need for verification with at least two evidences [13].

In [14], the study compared the security of Google Chrome browser, Mozilla Firefox, and Microsoft Internet Explorer Edge. The methodology used is The U.S. National Institute of Justice (NIJ). The results obtained are Microsoft Edge is the default browser on Windows 10 with a better feature of Internet Explorer, but it turns out for the security aspect is weaker compared to Mozilla Firefox browser, while Google Chrome is stronger in the password.

In [4], live forensics analysis for email security comparison on the proprietary operating system forensics live analysis in the latest operating system is windows 10. This research focuses on the security of any email such as gmail, yahoo and outlook and some browsers in general, such as google chrome, mozilla Firefox, and Microsoft edge.

In [7], the study identifies the Digital Evidence On Blackberry Messenger-based instant messaging android. The results are presented in the form of recording conversations, BBM Personal Identification Number (BBM PIN), the name of the sender and receiver, and the timing of the research timestamp using the National Institute of Standards and Technology (NIST) method.

From the background above, this research will do forensic on email by way of acquisition of android based email to get IP address of sender. The sender's IP address is used as digital evidence. This study uses forensic methods based on guidelines prepared by the National Institute of Standards and Technology (NIST).

2. Research Method

the previous research about email, the study conducted a forensic investigation on email spoofing by examining and comparing the values contained in some email headers defined as email spoofing detection parameters. The parameters used in this study are the headers 'From', 'Message-ID', 'Date' and 'Received'. This research uses header analysis method.

In this research using National Institute of Standards and Technology (NIST) method is one method to analyze digital evidence or to obtain information from digital evidence. Here are the steps of the NIST method[15].

The following explanation in Figure 2:

1. Collection is identify, label, record and retrieve data from relevant data sources, then follow data integrity preservation procedures.
2. Examination is the data has been collected forensic using combinations of scenarios, both manually and automatically, assess and release of data in accordance with the data requirements and maintaining the authenticity of data.

3. Analysis is Perform analysis of the results of investigations by using the correct method both technically and legally to get useful information and answers questions that encourage the collection and examination.
4. Reporting is Report the results of an analysis that includes a description of the action taken, specifies the tool used and the procedure selected, and the required action, then reports the results obtained.

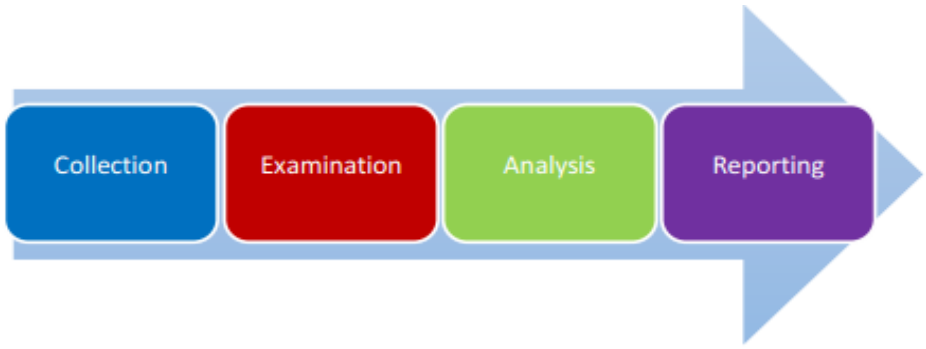

Figure 2. Stage Method of the National Institute of Standards and Technology

3. Results and Discussion

The results of this study conducted the appointment of emails that have been sent by someone to us and then the email is forensic, forensic email is an email from google is google mail or often called Gmail. Here is the process of acquiring on android based emails using the NIST method:

3.1 Collection

At this stage that is collecting goods on smartphone owners, the smartphone used in Xiaomi Mi4i with android version lollipop 5.0.2. In Figure 3 is a conceptual stage in the collection process.

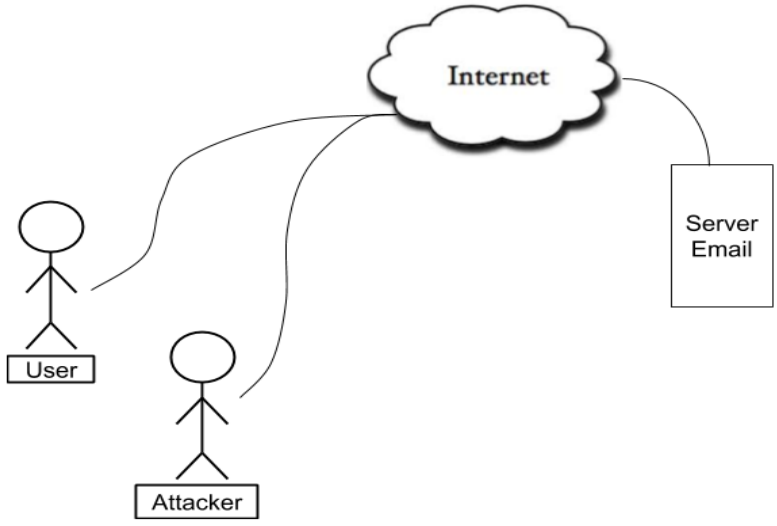

Figure 3. Conceptual Stages of Collection

3.2 Examination

At this stage, how to get digital evidence in email. This study uses the original browser from android system with version 9.4.10. Here is the stage of appointment of digital evidence.

In Figure 4 the initial display when opening the email through the android browser. the acquisition process in the email then must be changed in the desktop display and to change the display to the desktop open the settings menu, see red circle.

In Figure 5 is a display setting on Gmail opened using android browser and then click on the desktop, see the red circle.

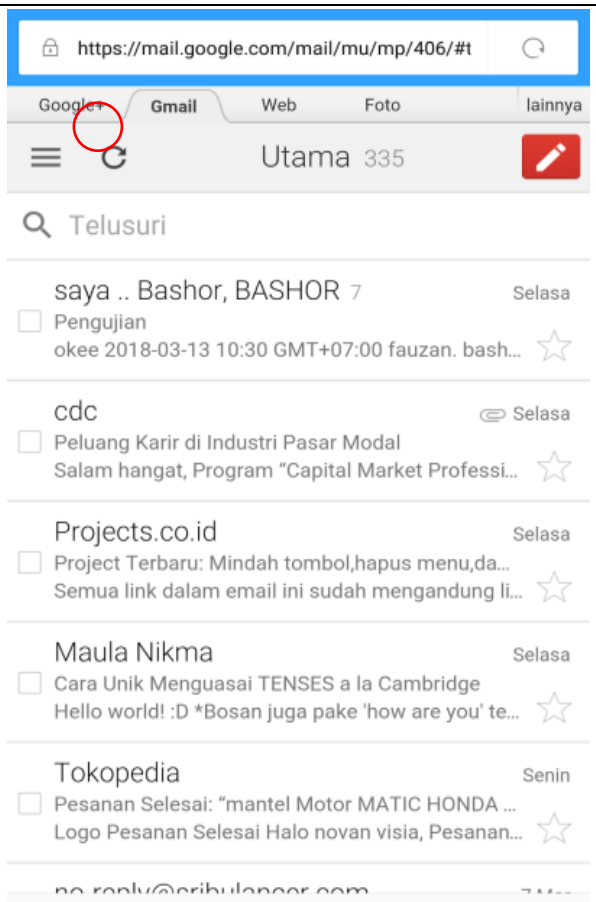

Figure 4. Initial View of Email

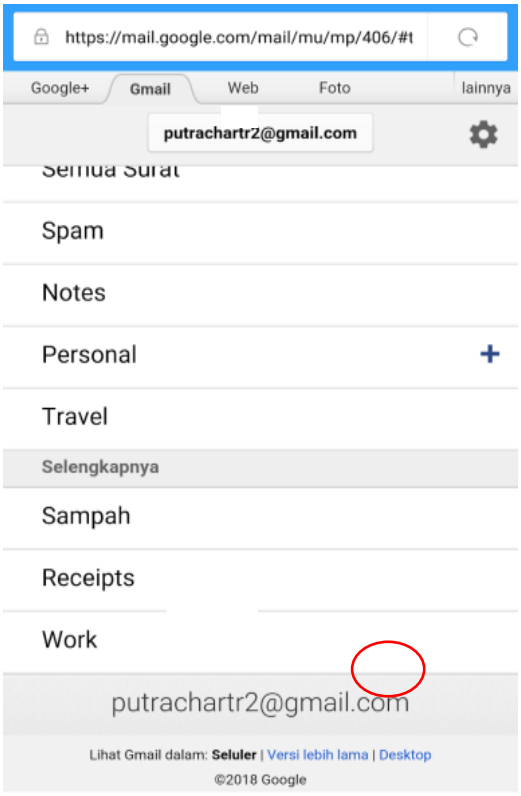

Figure 5. Changing the Display to Desktop

Figure 6. Desktop Display on Smartphone

In Figure 6 is an email appearance of the android browser after the change to the desktop. The next stage is to determine and open the email to be carried out on the android-based email acquisition.

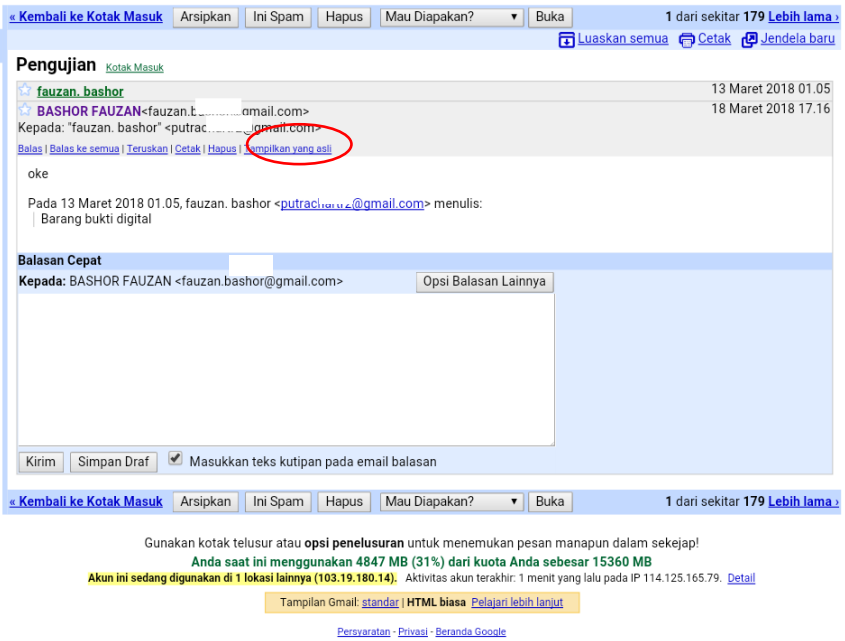

Figure 7. Opening Emails that Will be Forensic

In Figure 7 is the opened email view and to make the acquisition of the email should open the email header by click the original view, See red circle.

Figure 8. Email Header Display

In Figure 8 is an email header display that will be used in the analysis phase to make the acquisition of email.

3.3 Analysis

At this stage, perform an analysis of the acquisition process of the email, which generates the sender's IP address, recipient's IP address, sender's email address, email protocol, sender's email time, email time received, and email encryption obtained from email headers. This research object focuses on acquisition of IP address on the email. The results can be seen in Figure 9.

Figure 9. IP Address Sender Email

3.4 Reporting

At this stage, it is a digital forensic report from the email acquisition process. Email sent from someone via google mail has been found IP address of sender email in the email header, then IP address can be used as digital evidence.

4. Conclusion

From the research that has been done, the growth of information and communication technology is very fast. Email is one of the media used to exchange data information, images and others. As the rapid development of information and communication exchanges, causes cyber crime to flourish. So for the perpetrators of cyber crime or cybercrime required evidence. Crimes committed by cybercrime can be forensic on email. This research will do forensic on emails by way of acquisition of android based emails as digital evidence by using forensic methods of the National Institute of Standards and Technology (NIST). At the collection stage of evidence carried out on the smartphone Android lollipop 5.0.2 type Xiaomi Mi4i, to make an acquisition on Android-based email then the email must be opened using the browser. In this study using the original browser from android. In the testing phase, from a series of processes that have been done in obtaining the IP address of the sender in the email header, other than the sender's IP address is found also the recipient's IP address, sender's email address, email protocol, sender's email time, email time received and email encryption. In the final stages of the acquisition process in email successfully carried out by obtaining an IP address sends email in the header as digital evidence. In the next study can tracker the IP address of the sender of the email.

References

[1] Wearesocial, *"Digital in 2018 : Global Overview,"* 2018.
[2] Jakpat, *"Which And Why: E-Mail Service and Web Browser of Choice,"* 2017.
[3] J. Rose, *"E-Mail Security Risks: Taking Hacks at the Attorney-Client Privilege,"* in Rutgers Computer & Tech. LJ, Vol. 23, 1997, Pp. 179.
[4] M. N. Faiz, R. Umar, and A. Yudhana, *"Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary,"* Jurnal Ilmiah ILKOM., Vol. 8, No. 3, Pp. 242–247, 2016.
[5] D. Mualfah and I. Riadi, *"Network Forensics For Detecting Flooding Attack On Web Server,"* (IJCSIS) International Journal of Computer Science and Information Security, Vl. 15, No. 2, Pp. 326–331, 2017.
[6] Agus Tri P.H, *"Cybercrime Dalam Perspektif Hukum Pidana,"* Universitas Muhammadiyah Surakarta, 2010.
[7] I. Riadi, R. Umar, and A. Firdonsyah, *"Identification Of Digital Evidence On Android ' s Blackberry Messenger Using NIST Mobile," International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 15, No. May, Pp. 1–7, 2017.
[8] Y. Hoiriyah, H., Sugiantoro, B., Prayudi, *"Investigasi Forensik Pada E-Mail Spoofing Menggunakan Metode Header Analysis,"* Jurnal Ilmiah DASI, Vol. 17, No. Desember, Pp. 20–25, 2016.
[9] M. D. R. Wahyudi, *"Deteksi e-mail Palsu dengan mempergunakan,"* Jurnal Teknologi, Vol. 1, Pp. 119–126, 2008.
[10] Y. Zulfadhilah, M., Riadi, I., Prayudi, *"Log Classification using K-Means Clustering for Identify Internet User Behaviors,"* International Journal of Computer Applications (IJCA), Vol. 154, No. 3, Pp. 34–39, 2016.
[11] I. Riadi, J. E. Istiyanto, A. Ashari, and S. Subanar, *"Internet Forensics Framework Based-on Clustering."*
[12] M. Agarwal and M. Gupta, *"Systematic Digital Forensic Investigation Model,"* Journal of Computer, No. 5, Pp. 118–131, 2011.
[13] R. Indonesia, "*Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Departemen Komunikasi dan Informatika, Republik Indonesia*", 2008.
[14] M. N. Faiz, R. Umar, and A. Yudhana, *"Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email,"* JISKa, Vol. 1, No. February, Pp. 108–114, 2017.
[15] G. M. Umar, R., Riadi, I., Zamroni, *"A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements,"* (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 12, Pp. 69–75, 2017.