## RINGKASAN BUKTI KORESPONDENSI

Judul Artikel	Acquisition of Email Service Based Android Using NIST	
Penulis	Rusydi Umar, Imam Riadi, Bashor Fauzan Muthohirin	
Jurnal	(KINETIK) Game Technology, Information System, Computer Ne	twork,
	Computing, Electronics, and Control	

- 1. Lampiran 1 : Penulis melakukan submission artikel pada 26 maret 2018 pada Jurnal Kinetik
- 2. Lampiran 2 : Tanggal 21 April 2018, penulis mendapatkan pemberitahuan bahwa penulis diminta untuk merevisi artikel (revisions required)
- 3. Lampiran 3 : Tanggal 21 April 2018, penulis mengirimkan hasil revisi yang diminta oleh reviewer
- 4. Lampiran 4 : Tanggal 21 April 2018, penulis mendapatkan notifikasi bahwa artikel diterima (accept submission)
- 5. Lampiran 5 : Tanggal 12 November 2020 artikel dinyatakan terbit (*published*)

## 1. Lampiran 1

Kinetik: Game Technology, Information System, Comp	Tasks 0	😧 English 🛛 👁 View Site	💄 bashorfauzan
KINETIK Gurr hetworky, Information Bystem, Computer Network, Computing, Electronics and Control 637 / Umar et al.	/ Acquisition of Email Service Based Android Using NIST		Library
Submissions Kinetik-Management	Publication		
Join As Reviewer Submission	Review Copyediting Production		
Submission	Files	Q Searc	h
► 🕅 12412	4138-1     kinetik, Paper Kinetik ENG.docx     March 2       2018	26, Article Text	
		Download All File	s
			-
Pre-Review	Discussions	Add discussion	n
Name	From Last Re	ply Replies Clo	sed
	No Items		

# Acquisition of Email Service Based Android Using NIST

Rusydi Umar<sup>\*1</sup>, Imam Riadi<sup>2</sup>, Bashor Fauzan Muthohirin<sup>3</sup>

<sup>1,3</sup>Program Studi Teknik Informatika Universitas Ahmad Dahlan <sup>2</sup>Program Studi Sistem Informasi Universitas Ahmad Dahlan e-mail: rusydi\_umar@rocketmail.com<sup>\*1</sup>, imam.riadi@is.uad.ac.id<sup>2</sup>, fauzan.bashor@gmail.com<sup>3</sup>

### 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 xiomi 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

*Citation :* Umar, R; Riadi, I, Fauzan Muthohirin, Bashor. Acquisition of Email Service Based Android Using NIST, [S.I.], v. 1, n. 1, p. 1-8, oct. 2016. doi:http://dx.doi.org/10.22219/kinetik.v1i1.3 Paper submitted on February 26, 2016; Revision on May 1, 2016; Received on June 1, 2016

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].



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

The following explanation in Figure 2:

- a. Collection is identify, label, record and retrieve data from relevant data sources, then follow data integrity preservation procedures.
- b. 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.
- c. 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.
- d. 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.

#### 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 Xiomi 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.

Google+ Gmail	Web	Foto	lainnya
(≡) c	Utam	<b>a</b> 335	1
<b>Q</b> Telusuri			
saya Bashor	, BASHOF	<b>R</b> 7	Selasa
Pengujian okee 2018-03-13 1	10:30 GMT+	07:00 fauzan.	bash 🏠
cdc			© Selasa
Peluang Karir di In Salam hangat, Pro	dustri Pasa ogram "Capi	r Modal al Market Pro	fessi 🏠
Projects.co.id			Selasa
Project Terbaru: N Semua link dalam	lindah tomb email ini su	ol,hapus men dah mengand	u,da ung li 🏠
Maula Nikma			Selasa
Cara Unik Mengua Hello world! :D *Bo	isai TENSES osan juga pa	a la Cambrid ke 'how are yo	ge ou'te 🏠
Tokopedia			Senin
Pesanan Selesai: ' Logo Pesanan Sel	"mantel Mot esai Halo no	or MATIC HOI ovan visia, Pes	NDA sanan 🏠

Figure 4. Initial View of Email

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.

Google+ Gmail	Web	Foto	lainnya
putrac	:@g	mail.com	
semua surat			
Spam			
Notes			
Personal			+
Travel			
Selengkapnya			
Sampah			
Receipts			
Work			
puti	@	gmail.com	

Figure 5. Changing the Display to Desktop

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

1 Gmai		Telusuri Email Telusuri Web Lihat opsi penelusuran Buat filter	
s Email	Arsipkan Ini Spam Hapus	Mau Diapakan? • Buka Segarkan 1 - 100 dari sekitar 179 Lebi	ih lama
ak (a Form)	saya, BASHOR (2)	Pengujian - oke Pada 13 Maret 2018 01.05, fauzan. bashor <putrachartr2@gmail.com></putrachartr2@gmail.com>	18 Ma
uk (15311) vintang 😭	Twitter	People in Genteng shared "PM Australia: Presiden Jokowi Panutan Pemi What's happening	18 Ma
t Terkirim	jobsDB.com	4 new jobs for it staff - Find out more about this job jobsDB.com Hi bashor fauzan muthohirin,	18 Ma
in Frankl	Twitter	SurabayaPunyaCerita Tweeted: Pengecekan kelengkapan Honda C110 oleh AkhireTour,	18 Ma
1 (12)	Maula Nikma	[True Story] Barusan Kejadian di Batu Cave, Kuala Lumpur - Kejadian ini mengingatkan saya	18 Ma
Sampah	Quora Digest	What is it like to study at ETH Zurich? - Answer: I'm an undergraduate in Computer Science, 4th	18 Ma
ak	BLIBLI.COM	Beli LENOVO, Dapat Hadiah JBL! - Klik disini untuk tampilan yang lebih ielas BARU! GoPro	18 Ma
t	The Official Pokémon GO	putrachartr: Three Days Only, Redeem Free Gifts in Pokémon GO Now, - Hello, Pokémon	18 Ma
nal	Projects.co.id	Project Terbaru: Sistem Ekspedisi track resi/awb online - Semua link dalam email ini sudah	18 Ma
nal/Ban	Pinterest	Get inspired with these 18 trending ideas - Here's what's trending on Pinterest Best and worst	18 Ma
	lina@iohstreet.com	Senior Backend Developer (IDR 5.000.000 - 7.000.000) + 11 new jobs - Job Alert from Job	18 Ma
abel	iBlog Market	New Campaign Thread - Halo sobat, Ada campaign baru nib YD - Blog Placement (Maret 2018)	18 Ma
	VouGov	Anda terpilih untuk survei YouGov! - Hai Panelis YouGov, Waktu Anda sangat berharga, iadi	17 Ma
	Pinterest	Hi putrachartr! Apple products   uyury yachts and other topics picked for you - New topics you	17 Ma
	SmartDraw Software	SmartDraw is the New Standard for Diagramming - Welcome to the SmartDraw family. See	17 M
		People in Genterg shared "Mankominfo Ingin Data Center Alihaba Picu	17 M
	iohoDR com	6 new jobe for it staff. Find out more about this job jobeDB com Hi bashor fauzan muthobirin	17 Mc
	JobsDB.com	Toppere Selessikan Transskei VI *PDOMO YTDA COMPO 1002 Kamul - Halo Toppere	17 Mc
		Mata Najwa Tweeted: Kali ini Tamni & Clenn mangunjungi kata kelabira - Human Kata	17 1010
	Takanadia	Incoronany Macile Ade di Cinil. Cale Calerana Sabalum Manyasal. Takanadia. Barana yana	17 Ma
	Tikopedia	Pact Offer This Week Libet tempiles di web browser ands ELICHT TRAIN HOTEL CAD	17 Ma
	DUDU COM	Dekai Kada Vauahas Untuk Detangen De50 0001. Kik disisi untuk tempilan yang labih jalas	17 Ma
	BLIBLI.COM	Pakar Kode Volcher Onder Polongan p30.000: - Kilk disini direk tampian yang tebih jelas	17 Ma
	Joy from JD.id	SSSSTTT Selamat Tahun Baru Saka 1940 view this email in your browser Facebook Twitter	17 Ma
	Booking.com	Prices in Solo dropped again. Act now and save more! - FREE cancellation on most rooms -	17 Ma
	Maula Nikma	Lucu! Ini Kesimpulan Saya Dulu Soal Verb 2 & Verb 3 - Saya yakin, Anda pernah bingung	17 Ma
	Projects.co.id	Project Terbaru: Pembuatan Aplikasi Web Coworking Space - Semua link dalam email ini	17 Ma
	lina@jobstreet.com	Mobile App Developer (IDR 6,000,000 - 10,000,000) + 17 new jobs - Job Alert from JobStr	17 Ma
	Pinterest	We picked some F14 tomcat Pins for you - We found some Pins we think might be right up	16 Ma
	The RedShark Team	Four techniques that are certain to revolutionise cameras - Four techniques that are certain to	16 Ma
	no-reply@sribulancer.com	Ada 2 Job Freelance Baru Yang Sesuai Keahlian Anda - Sribulancer Logo Hi bashor,	16 Ma
	Jason Clark	Thank you for trying SmartDraw Lam here to help - Hello Thank you for signing up for a trial	16 M

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.

Kembali ke Kotak Masuk	Arsipkan	Ini Spam	Hapus	Mau Diapakan?	▼ Bul	ka 1	l dari sekita	r 179 <u>Lebih lama</u>
						Euaskan semua	Cetak	Jendela baru
Pengujian Kotak Masuk								
🗘 <u>fauzan. bashor</u>							13 M	Aaret 2018 01.05
BASHOR FAUZAN <fau "fauzan.="" bashor"<="" kepada:="" td=""><td>za @ <puti !<="" td=""><td>gmail.com&gt; @gmail.com</td><td>&gt;</td><td></td><td></td><td></td><td>18 M</td><td>laret 2018 17.16</td></puti></td></fau>	za @ <puti !<="" td=""><td>gmail.com&gt; @gmail.com</td><td>&gt;</td><td></td><td></td><td></td><td>18 M</td><td>laret 2018 17.16</td></puti>	gmail.com> @gmail.com	>				18 M	laret 2018 17.16
<u>Balas   Balas ke semua   Teruskan</u>	Cetak   Hapus	Tampilkan yang	asli					
oke								
Pada 13 Maret 2018 01. Barang bukti digital	)5, fauzan. ba	ashor < <u>putra</u>	<u>2@g</u>	<u>mail.com</u> > menulis:				
Balasan Cepat								
Kepada: BASHOR FAUZAN	√ <fauzar< td=""><td>@gmail.c</td><td>com&gt;</td><td>Opsi Balas</td><td>an Lainnya</td><td></td><td></td><td></td></fauzar<>	@gmail.c	com>	Opsi Balas	an Lainnya			
Kirim Simpan Draf	🕑 Masukka	n teks kutipa	in pada en	nail balasan				
Kembali ke Kotak Masuk	Arsipkan	Ini Spam	Hapus	Mau Diapakan?	▼ Bul	ka 1	l dari sekita	r 179 <u>Lebih lama</u>
Gun Akun ini sedang	akan kotak te Anda saa digunakan di 1	elusur atau o at ini menggu lokasi lainnya	psi penelu unakan 48 (103.19.180	<b>isuran</b> untuk menem 47 MB (31%) dari ku 0.14). Aktivitas akun te	ukan pesan I <b>ota Anda se</b> rakhir: 1 meni	manapun dalam sek <b>ebesar 15360 MB</b> t yang lalu pada IP 114.1	:ejap! 25.165.79. <u>D</u>	etail
		Tampil	an Gmail: <u>st</u>	andar   HTML biasa Pe	ajari lebih lanj	lut		

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.

Acquisition of Email Service Based Android Using NIST, Rusydi Umar\*1, Imam Riadi<sup>2</sup>, Bashor Fauzan Muthohirin<sup>3</sup>



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 Iollipop 5.0.2 type Xiomi 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 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, p. 179.
- [4] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," *J. Ilm. Ilk.*, vol. 8, no. 3, pp. 242–247, 2016.
- [5] 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.
- [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," *Int. J. Comput. Sci. Inf. Secur.*, 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," *J. Ilm. DASI*, vol. 17, no. DESEMBER, pp. 20–25, 2016.
- [9] M. D. R. Wahyudi, "Deteksi e-mail palsu dengan mempergunakan," *J. Teknol.*, vol. 1, pp. 119–126, 2008.
- [10] 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.
- [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," *J. Comput.*, 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," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.

# 2. Lampiran 2

Kinetik: Game Technology, Information	System, Comp	Tasks 🗕	Q English 💿 View Site 🛔 basho	orfauzan
Submissions				
Kinetik-Management	Workflow	Publication		
Join As Reviewer	Submission	Review Copyediting Production		
	Round 1			
	Reviewe	s Attachments	Q Search	
		No Files		
	Revision		Q Search Upload File	
	► W 124	24177-1 Article Text, Kinetik rev1.docx	April 21, Article Text 2018	
				٦
	Review D	scussions	Add discussion	
	Name	From	Last Reply Replies Closed	
	► <u>Editor D</u>	bashorfau 2018-04-2 AM	Uzan bashorfauzan 1 1 01:38 2018-04-21 07:12 AM	

## **Editor Decision**

## Participants <u>Edit</u>

Mahar Faiqurahman (mfaiqurrahman) Denar Regata Akbi (dakbi) Bashor Fauzan Muthohirin (bashorfauzan)

## Messages

Note	From
The following message is being delivered on behalf of KINETIK.	bashorfauzan 2018-04-21 01:38
Bashor Fauzan Muthohirin:	AM
We have reached a decision regarding your submission to Kinetik, "Acquisition Of Email Service Based Android".	
Our decision is: Revisions Required	
Agus Eko Minarno	
Universitas Muhammadiyah Malang	
Phone 081233084984	
aguseko@umm.ac.id	

# ×

------Reviewer A: Relevancy: Does the article's topic relevance to the scoope of KINETIK journal? (http://kinetik.umm.ac.id/index.php/kinetik/pages/view/Aims) : Yes Relevancy: Is the article supported by relevance journals or proceedings?: Yes Title: Does the title describes overall article's content?: No Abstract: The abstract contains of research problem, method being used, research finding and results, and conclusions: **Below Average** Introduction : The clarity of research problem, comparation with the previous method, and contribution to the literature :

**Below Average** 

Research methodology : Describe clearly the method being used in research (e.g., experimental procedures, algorithms, flow diagrams, analytical tools, ect.) Ċ. **Below Average** Research methodology: Is the method being used can be well understood and possible to implemented? Ċ. Yes Research Result and discussion: The presentation of result, the comformity of methodology being used, the depth of result analysis, and the research findings. • **Below Average** Conclusion : The conclusion contains justification from evidence being presented : **Below Average** References: Does the article cite less than last 10 years publication? : Yes

Detailed Comment for Author: Complete your analysis of result suitable with the method

Reviewer's recommendation: Write the recommendation of overall article's content:: Complete your analysis of result suitable with the method

\_\_\_\_\_

-----

Reviewer B:

Relevancy:

Does the article's topic relevance to the scoope of KINETIK journal? (http://kinetik.umm.ac.id/index.php/kinetik/pages/view/Aims) :

Yes

Relevancy: Is the article supported by relevance journals or proceedings?: Yes

Title: Does the title describes overall article's content?: No

Abstract:

The abstract contains of research problem, method being used, research finding and results, and conclusions: Below Average Introduction : The clarity of research problem, comparation with the previous method, and contribution to the literature : **Below Average** Research methodology : Describe clearly the method being used in research (e.g., experimental procedures, algorithms, flow diagrams, analytical tools, ect.) : Average Research methodology: Is the method being used can be well understood and possible to implemented? : Yes Research Result and discussion: The presentation of result, the comformity of methodology being used, the depth of result analysis, and the research findings. : **Below Average** Conclusion : The conclusion contains justification from evidence being presented

**Below Average** 

References:

Does the article cite less than last 10 years publication?

: Yes

Detailed Comment for Author:

1. Background / Motivation: explain about your most important or interesting point

the research more clearly

2. Aim/objective(s)/problem statement: explain more clearly

3. Conclusion: what the results important from the research?

Reviewer's recommendation:

Write the recommendation of overall article's content::

1. Background / Motivation: explain about your most important or interesting point

the research more clearly

2. Aim/objective(s)/problem statement: explain more clearly

3. Conclusion: what the results important from the research?

based on the above revision, some parts of the article need to be fixed

# 3. Lampiran 3

Kinetik: Game Technology, Information System,	Comp Tasks 👔	English	• View Site	🛓 bashorfauzan
KINETIK Gum Technology Information System, Computer Network, Computing Electronics and Control 637 /	Umar et al. / Acquisition of Email Service Based Android Using NIST			Library
Submissions				
Kinetik-Management	orkflow Publication			
Join As Reviewer	ubmission Review Copyediting Production			
R	ound 1			
	Reviewer's Attachments		Q Search	n
	No Files			
	Revisions	Q Search	Upload File	e
	Image: Market State     Article Text, Kinetik rev1.docx     April 2       2018	, Article T	ext	
	Review Discussions		Add discussion	n
	Name From Last Re	ply	Replies Clo	sed

# Acquisition of Email Service Based Android Using NIST

Rusydi Umar<sup>\*1</sup>, Imam Riadi<sup>2</sup>, Bashor Fauzan Muthohirin<sup>3</sup>

<sup>1,3</sup>Program Studi Teknik Informatika Universitas Ahmad Dahlan <sup>2</sup>Program Studi Sistem Informasi Universitas Ahmad Dahlan e-mail: rusydi\_umar@rocketmail.com<sup>\*1</sup>, imam.riadi@is.uad.ac.id<sup>2</sup>, fauzan.bashor@gmail.com<sup>3</sup>

### 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 xiomi 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

*Citation :* Umar, R; Riadi, I, Fauzan Muthohirin, Bashor. Acquisition of Email Service Based Android Using NIST, [S.I.], v. 1, n. 1, p. 1-8, oct. 2016. doi:http://dx.doi.org/10.22219/kinetik.v1i1.3 Paper submitted on February 26, 2016; Revision on May 1, 2016; Received on June 1, 2016

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].



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

The following explanation in Figure 2:

- a. Collection is identify, label, record and retrieve data from relevant data sources, then follow data integrity preservation procedures.
- b. 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.
- c. 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.
- d. 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.

#### 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 Xiomi 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.

Google+ Gmail	Web	Foto	lainnya
(≡) c	Utam	<b>a</b> 335	1
<b>Q</b> Telusuri			
saya Bashor	, BASHOF	<b>R</b> 7	Selasa
Pengujian okee 2018-03-13 1	10:30 GMT+	07:00 fauzan.	bash 🏠
cdc			© Selasa
Peluang Karir di In Salam hangat, Pro	dustri Pasa ogram "Capi	r Modal al Market Pro	fessi 🏠
Projects.co.id			Selasa
Project Terbaru: N Semua link dalam	lindah tomb email ini su	ol,hapus men dah mengand	u,da ung li 🏠
Maula Nikma			Selasa
Cara Unik Mengua Hello world! :D *Bo	isai TENSES osan juga pa	a la Cambrid ke 'how are yo	ge ou'te 🏠
Tokopedia			Senin
Pesanan Selesai: ' Logo Pesanan Sel	"mantel Mot esai Halo no	or MATIC HOI ovan visia, Pes	NDA sanan 🏠

Figure 4. Initial View of Email

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.

Google+ Gmail	Web	Foto	lainnya
putrac	!@g	mail.com	\$
semua surat			
Spam			
Notes			
Personal			+
Travel			
Selengkapnya			
Sampah			
Receipts			
Work			
putr	.@	gmail.com	

Figure 5. Changing the Display to Desktop

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

1 Gmai		Telusuri Email Telusuri Web Lihat opsi penelusuran Buat filter	
s Email	Arsipkan Ini Spam Hapus	Mau Diapakan? • Buka Segarkan 1 - 100 dari sekitar 179 Lebi	ih lama
ak (a Form)	saya, BASHOR (2)	Pengujian - oke Pada 13 Maret 2018 01.05, fauzan. bashor <putrachartr2@gmail.com></putrachartr2@gmail.com>	18 Ma
uk (15311) vintang 😭	Twitter	People in Genteng shared "PM Australia: Presiden Jokowi Panutan Pemi What's happening	18 Ma
t Terkirim	jobsDB.com	4 new jobs for it staff - Find out more about this job jobsDB.com Hi bashor fauzan muthohirin,	18 Ma
in Frankl	Twitter	SurabayaPunyaCerita Tweeted: Pengecekan kelengkapan Honda C110 oleh AkhireTour,	18 Ma
1 (12)	Maula Nikma	[True Story] Barusan Kejadian di Batu Cave, Kuala Lumpur - Kejadian ini mengingatkan saya	18 Ma
Sampah	Quora Digest	What is it like to study at ETH Zurich? - Answer: I'm an undergraduate in Computer Science, 4th	18 Ma
ak	BLIBLI.COM	Beli LENOVO, Dapat Hadiah JBL! - Klik disini untuk tampilan yang lebih ielas BARU! GoPro	18 Ma
t	The Official Pokémon GO	putrachartr: Three Days Only, Redeem Free Gifts in Pokémon GO Now, - Hello, Pokémon	18 Ma
nal	Projects.co.id	Project Terbaru: Sistem Ekspedisi track resi/awb online - Semua link dalam email ini sudah	18 Ma
nal/Ban	Pinterest	Get inspired with these 18 trending ideas - Here's what's trending on Pinterest Best and worst	18 Ma
	lina@iohstreet.com	Senior Backend Developer (IDR 5.000.000 - 7.000.000) + 11 new jobs - Job Alert from Job	18 Ma
abel	iBlog Market	New Campaign Thread - Halo sobat, Ada campaign baru nib YD - Blog Placement (Maret 2018)	18 Ma
	VouGov	Anda terpilih untuk survei YouGov! - Hai Panelis YouGov, Waktu Anda sangat berharga, iadi	17 Ma
	Pinterest	Hi putrachartr! Apple products   uyury yachts and other topics picked for you - New topics you	17 Ma
	SmartDraw Software	SmartDraw is the New Standard for Diagramming - Welcome to the SmartDraw family. See	17 M
		People in Genterg shared "Mankominfo Ingin Data Center Alihaba Picu	17 M
	iohoDR com	6 new jobe for it staff. Find out more about this job jobeDB com Hi bashor fauzan muthobirin	17 M
	JobsDB.com	Toppere Selessikan Transskei VI *PDOMO YTDA COMPO 1002 Kamul - Halo Toppere	17 Mc
		Mata Najwa Tweeted: Kali ini Tamni & Clenn mangunjungi kata kelabira - Human Kata	17 1010
	Takanadia	Incoronany Macile Ade di Cinil. Cale Calerana Sabalum Manyasal. Takanadia. Barana yana	17 Ma
	Tikopedia	Pact Offer This Week Libet tempiles di web browser ands ELICHT TRAIN HOTEL CAD	17 Ma
	DUDU COM	Deka Kada Vauahas Untuk Detangen De50 0001. Kik disisi untuk tempilan yang labih jalas	17 Ma
	BLIBLI.COM	Pakar Kode Volcher Onder Polongan p30.000: - Kilk disini direk tampilan yang tebih jelas	17 Ma
	Joy from JD.id	SSSSTTT Selamat Tahun Baru Saka 1940 view this email in your browser Facebook Twitter	17 Ma
	Booking.com	Prices in Solo dropped again. Act now and save more! - FREE cancellation on most rooms -	17 Ma
	Maula Nikma	Lucu! Ini Kesimpulan Saya Dulu Soal Verb 2 & Verb 3 - Saya yakin, Anda pernah bingung	17 Ma
	Projects.co.id	Project Terbaru: Pembuatan Aplikasi Web Coworking Space - Semua link dalam email ini	17 Ma
	lina@jobstreet.com	Mobile App Developer (IDR 6,000,000 - 10,000,000) + 17 new jobs - Job Alert from JobStr	17 Ma
	Pinterest	We picked some F14 tomcat Pins for you - We found some Pins we think might be right up	16 Ma
	The RedShark Team	Four techniques that are certain to revolutionise cameras - Four techniques that are certain to	16 Ma
	no-reply@sribulancer.com	Ada 2 Job Freelance Baru Yang Sesuai Keahlian Anda - Sribulancer Logo Hi bashor,	16 Ma
	Jason Clark	Thank you for trying SmartDraw Lam here to help - Hello Thank you for signing up for a trial	16 M

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.

	Arsipkan	Ini Spam	Hapus	Mau Diapakan?	<ul> <li>Buka</li> </ul>	1	dari sekita	r 179 Lebih lama
					6	Luaskan semua	Cetak	Jendela baru
Pengujian Kotak Masuk								
🗘 <u>fauzan. bashor</u>							13 M	Aaret 2018 01.05
BASHOR FAUZAN <fauz Kepada: "fauzan. bashor" &lt;</fauz 	⊻a @g puti :@	mail.com> )gmail.com>					18 M	Maret 2018 17.16
<u>Balas   Balas ke semua   Teruskan</u>	Cetak   Hapus ( T	ampilkan yang a	sli					
oke								
Pada 13 Maret 2018 01.0 Barang bukti digital	15, fauzan. bas	shor < <u>putra</u>	<u>2@gn</u>	<u>nail.com</u> > menulis:				
Balasan Cepat								
Kepada: BASHOR FAUZAN	i <fauzar< td=""><td>@gmail.co</td><td>m&gt;</td><td>Opsi Balasa</td><td>n Lainnya</td><td></td><td></td><td></td></fauzar<>	@gmail.co	m>	Opsi Balasa	n Lainnya			
Kirim Simpan Draf	🗹 Masukkan	teks kutipan	pada em	ail balasan				
Kirim Simpan Draf	Masukkan Arsipkan	teks kutipan Ini Spam	pada em Hapus	ail balasan Mau Diapakan?	▼ Buka	] 1	dari sekita	r 179 <u>Lebih lama</u>
Kirim Simpan Draf Kembali ke Kotak Masuk Gun: Akun ini sedang	Masukkan Arsipkan akan kotak telu Anda saat digunakan di 1 k	teks kutipan Ini Spam usur atau ops ini menggur okasi lainnya (1	pada em Hapus si penelus aakan 484 03.19.180.	ail balasan Mau Diapakan? suran untuk menemu 17 MB (31%) dari kuc 14). Aktivitas akun tera	▼ Buka kan pesan m ta Anda seb akhir: 1 menit ya	anapun dalam sek esar 15360 MB ng lalu pada IP 114.1	dari sekita ejap! 25.165.79. <u>D</u>	r <b>179 <u>Lebih lama</u></b> etail
Kirim Simpan Draf Kembali ke Kotak Masuk Guni Akun ini sedang	Masukkan Arsipkan akan kotak telu Anda saat digunakan di 1 ka	teks kutipan Ini Spam usur atau opa ini menggur okasi lainnya (1 Tampilar	pada em Hapus si penelus akan 484 03.19.180 1 Gmail: <u>sta</u>	ail balasan Mau Diapakan? Kuran untuk menemu 17 MB (31%) dari kuc 14). Aktivitas akun tera ndar   HTML biasa Pela	Buka kan pesan m ta Anda sebu khir: 1 menit ya jari lebih lanjut	1 anapun dalam sek esar 15360 MB ng lalu pada IP 114.1	dari sekita ejap! 25.165.79. <u>D</u>	r <b>179 <u>Lebih lama</u></b> etail

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.

Acquisition of Email Service Based Android Using NIST, Rusydi Umar\*1, Imam Riadi<sup>2</sup>, Bashor Fauzan Muthohirin<sup>3</sup>



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 Iollipop 5.0.2 type Xiomi 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, p. 179.
- [4] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," *J. Ilm. Ilk.*, vol. 8, no. 3, pp. 242–247, 2016.
- [5] 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.
- [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," *Int. J. Comput. Sci. Inf. Secur.*, 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," *J. Ilm. DASI*, vol. 17, no. DESEMBER, pp. 20–25, 2016.
- [9] M. D. R. Wahyudi, "Deteksi e-mail palsu dengan mempergunakan," *J. Teknol.*, vol. 1, pp. 119–126, 2008.
- [10] 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.
- [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," *J. Comput.*, 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," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.

# 4. Lampiran 4

Kinetik: Game Technology, Information Syste	, Comp Tasks  0					G	English	View Site	💄 bashorfauzan
K KINETIK Game Technology, Information System, Computer Network, Computing, Electronics and Control	<b>Umar et al.</b> / Acquisition of Er	mail Service Based	Android Using NIST						Library
Submissions Kinetik-Management	Vorkflow Publication								
Join As Reviewer	Submission Review Coj	pyediting Pro	oduction						
	Copyediting Discussions						P	dd discussio	n
	Name			Fr	om	Last Reply		Replies Clo	osed
	Copyediting				- 020-12-11 05:59 M	-		0	
	Copyedited							Q Searc	:h
	☑         124124179-1         kinetik, 637-1	24124177-1-ED.do	icx			April 21, 2018	Article Tex	t	

#### KINETIK

http://kinetik.umm.ac.id/index.php/kinetik

## • The following message is being delivered on behalf of KINETIK.

Bashor Fauzan Muthohirin:

We have reached a decision regarding your submission to Kinetik, "Acquisition Of Email Service Based Android".

Our decision is to: Accept Submission

Agus Eko Minarno Universitas Muhammadiyah Malang Phone 081233084984 aguseko@umm.ac.id

#### KINETIK

http://kinetik.umm.ac.id/index.php/kinetik

Add Message

bashorfauzan 2018-04-21 07:12 AM

## 5. Lampiran 5

Kinetik: Game Technology, Information S	System, Comp	Tasks 0	😌 English	Over Site	占 bashorfauzan
KINETIK Game Technology, Information System, Computer Network, Computing, Electronics and Control	637 / Umar et al	/ Acquisition of Email Service Based Android Using NIST			Library
Submissions Kinetik-Management	Workflow	Publication			
Join As Reviewer	Submission	Review Copyediting Production			
	Copyediti	g Discussions		Add discussio	n
	Name	From Last Repl	y	Replies Clo	sed
	<u>Copyediting</u>			0	
	Copyedite	d		Q Searc	h
	₩ 124124	kinetik, 637-124124177-1-ED.docx         April 21,           2018         2018	Article Te	ext	

## Acquisition of Email Service Based Android Using NIST

## Rusydi Umar\*<sup>1</sup>, Imam Riadi<sup>2</sup>, Bashor Fauzan Muthohirin<sup>3</sup>

<sup>1,3</sup>Universitas Ahmad Dahlan/Informatics Engineering Department <sup>2</sup>Universitas Ahmad Dahlan/Information System Department rusydi\_umar@rocketmail.com<sup>\*1</sup>, imam.riadi@is.uad.ac.id<sup>2</sup>, fauzan.bashor@gmail.com<sup>3</sup>

#### 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].

TOP USED E-MAIL SE 96.15% G-mail by Google 9.32% E-mail domain given from the workplace or university 3.95%	ERVICES 56.03% Yahoo! (ymail, rocketmail, yahoo) 8% Outlook
n = 987 resp 34kPAT - Mobile Survey Platform Indo	ondents (only respondents who use e-mails in this survey)

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

#### ISSN: 2503-2259; E-ISSN: 2503-2267

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.

264

#### KINETIK

#### ISSN: 2503-2259; E-ISSN: 2503-2267

265

- 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.

	Q
Googles Gmail Web Foto	lainnya
≡ C Utama 335	1
Q Telusuri	
saya Bashor, BASHOR 7 Pengujian okee 2018-03-13 10:30 GMT+07:00 fauzan. b	Selasa ash 🏠
CdC Peluang Karir di Industri Pasar Modal Salam hangat, Program "Capital Market Profe	© Selasa essi 📈
Projects.co.id Project Terbaru: Mindah tombol,hapus menu, Semua link dalam email ini sudah mengandu	Selasa da ng li 🏠
Maula Nikma Cara Unik Menguasai TENSES a la Cambridge Hello world! :D *Bosan juga pake 'how are you	Selasa e u' te 🟠
Tokopedia Pesanan Selesai: "mantel Motor MATIC HON Logo Pesanan Selesai Halo novan visia, Pesa no roply@cribulopcor com Figure 4. Initial View of Fmail	Senin DA inan A
https://mail.google.com/mail/mu/mp/406/#t	0
Google+ Gmail Web Foto	lainnya
putrachartr2@gmail.com	
Semua Surat	\$
Spam	\$
Spam Notes	\$
Semua Surat Spam Notes Personal	\$
Semua Surat Spam Notes Personal Travel	\$
Semua Surat Spam Notes Personal Travel Selengkapnya	\$
Semua Surat Spam Notes Personal Travel Selengkapnya Sampah	\$
Semua Surat Spam Notes Personal Travel Selengkapnya Sampah Receipts	\$
Semua Surat Spam Notes Personal Travel Selengkapnya Sampah Receipts Work	\$
Semua Surat Spam Notes Personal Travel Selengkapnya Sampah Receipts Work putrachartr2@gmail.com	\$

KINETIK Vol. 3, No. 3, August 2018: 263-270

Telusuri Gambar Maps YouTube Berita Gmail Drive Kalender Lainnya »

Tulis Email	Arsipkan Ini Spam Hapus Ma	u Diapakan? • Buka Segarkan 1 - 100 dari sekitar 179 Lebi	h lama :				
Kotak	saya, BASHOR (2)	Pengujian - oke Pada 13 Maret 2018 01.05, fauzan. bashor <putrachartr2@gmail.com></putrachartr2@gmail.com>	18 Mar				
Masuk (15311) Berbintang St	Twitter	ngujian - oke Pada 13 Maret 2018 01.05, fauzan. bashor sputrachart/2@gmail.com> 18 Mar ngujian - oke Pada 13 Maret 2018 01.05, fauzan. bashor sputrachart/2@gmail.com> 18 Mar rew jobs for it staff - Find out more about this job jobsDB.com Hi bashor fauzan muthohirin. 18 Mar rabayaPunyaCerita Tweeted: Pengecekan kelengkapan Honda C110 oleh , AkhireTour, 18 Mar rabayaPunyaCerita Tweeted: Pengecekan kelengkapan Honda C110 oleh , AkhireTour, 18 Mar ue Story] Barusan Kejadian di Batu Cave, Kuala Lumpur - Kejadian ini mengingatkan saya 18 Mar at is it like to study at ETH Zurich? - Answer: I'm an undergraduate in Computer Science, 4th 18 Mar di LENOVO, Dapat Hadiah JBLI - Klik disini untuk tampilan yang lebih jelas BARUI GoPro 18 Mar tracharti: Three Days Only. Redeem Free Gifts in Pokémon GO New Hello, Pokémon oject Terbaru: Sistem Ekspedisi track resi/avb online - Semua link dalam email ini sudah 18 Mar mor Backend Developer (IDR 5,000,000 - 7,000,000) + 11 new jobs - Job Alert from Job 18 Mar w Campaign Thread - Halo sobat, Ada campaign baru nih 70 - Blog Placement (Maret 2018) 18 Mar antati terpilih untuk survei YouGovi - Hai Panelis YouGov, Waktu Anda sangat berharga, jadi 17 Mar anati Davis the New Standard for Diagramming - Welcome to the SmartDraw family. See 17 Mar spile in Genteng shared 'Menkominfo Ingin Data Center Alibaba Picu What's happening 17 Mar ta Najwa Tweeted: Kali ini Tompi & Glenn mengunjungi kota kelahira Humas Kota 17 Mar sta Najwa Tweeted: Kali ini Tompi & Glenn mengunjungi kota kelahira Humas Kota 17 Mar sta Najwa Tweeted: Kali ini Tompi & Glenn mengunjungi kota kelahira Humas Kota 17 Mar sta Najwa Tweeted: Kali ini Tompi & Glenn mengunjungi kota kelahira Humas Kota 17 Mar sta Olfer This Week - Lihat tampilan di web browser anda FLIGHT TRAIN HOTEL CAR 17 Mar					
Surat Terkirim	jobsDB.com	4 new jobs for it staff - Find out more about this job jobsDB.com Hi bashor fauzan muthohirin.					
Draf	Twitter	SurabayaPunyaCerita Tweeted: Pengecekan kelengkapan Honda C110 oleh AkhireTour.					
Spam (12)	Maula Nikma	[True Story] Barusan Kejadian di Batu Cave, Kuala Lumpur - Kejadian ini mengingatkan saya	18 Mar				
Tong Sampah	Quora Digest	What is it like to study at ETH Zurich? - Answer: I'm an undergraduate in Computer Science, 4th	18 Mar				
Kontak	BLIBLI.COM	Beli LENOVO, Dapat Hadiah JBL! - Klik disini untuk tampilan yang lebih jelas BARU! GoPro	<ul> <li>Ih Iama a</li> <li>I8 Mar</li> <li>I7 Mar</li> </ul>				
Label	The Official Pokémon GO .	putrachartr: Three Days Only. Redeem Free Gifts in Pokémon GO Now Hello, Pokémon	18 Mar				
Personal Personal/Ban	Projects.co.id	putrachartr: Three Days Only. Redeem Free Gifts in Pokémon GO Now Hello, Pokémon         18 M           Project Terbaru: Sistem Ekspedisi track resi/awb online - Semua link dalam email ini sudah         18 M           Get inspired with these 18 trending ideas - Here's what's trending on Pinterest Best and worst         18 M           Senior Backend Developer (IDE 5,000,000 - 7,000,000) + 11 new jobs - Job Alert from Job         18 M           New Campaign Thread - Halo sobat, Ada campaign baru nih YD - Blog Placement (Maret 2018)         18 N           Adata terriblit worke sured Young - Halo Bealle YouGovy Wetk and a sanata berbaras laidi         19 N	18 Mar				
Personal/Ban	Pinterest	Get inspired with these 18 trending ideas - Here's what's trending on Pinterest Best and worst	18 Mar				
Travel Work	lina@jobstreet.com	Senior Backend Developer (IDR 5,000,000 - 7,000,000) + 11 new jobs - Job Alert from Job	18 Mar				
Edit label	iBlog Market	New Campaign Thread - Halo sobat, Ada campaign baru nih YD - Blog Placement (Maret 2018)	18 Mar				
	YouGov	Anda terpilih untuk survei YouGov! - Hai Panelis YouGov, Waktu Anda sangat berharga, jadi					
	Pinterest	Hi putrachartr! Apple products, Luxury yachts and other topics picked for you - New topics you					
	SmartDraw Software	SmartDraw is the New Standard for Diagramming - Welcome to the SmartDraw family. See					
	Twitter	People in Genteng shared "Menkominfo Ingin Data Center Alibaba Picu What's happening	17 Mar				
	jobsDB.com	6 new jobs for it staff - Find out more about this job jobsDB.com Hi bashor fauzan muthohirin,	17 Mar				
	Tokopedia	Toppers, Selesaikan Transaksi XL *PROMO XTRA COMBO 10GB Kamu! - Halo Toppers,	17 Mar				
	Twitter	Mata Najwa Tweeted: Kali ini Tompi & Glenn mengunjungi kota kelahira Humas Kota	17 Mar				
	Tokopedia	Incaranmu Masih Ada di Sini! - Cek Sekarang Sebelum Menyesal. Tokopedia. Barang yang	17 Mar				
	Tiket.com	Best Offer This Week - Lihat tampilan di web browser anda FLIGHT TRAIN HOTEL CAR	17 Mar				
	BLIBLI.COM	Pakai Kode Voucher Untuk Potongan Rp50.000! - Klik disini untuk tampilan yang lebih jelas	17 Mar				
	Joy from JD.id	Sssstttt Selamat Tahun Baru Saka 1940 View this email in your browser Facebook Twitter	17 Mar				
	Booking.com	Prices in Solo dropped again. Act now and save more! - FREE cancellation on most rooms -	17 Mar				
	Maula Nikma	Lucu! Ini Kesimpulan Saya Dulu Soal Verb 2 & Verb 3 - Saya yakin, Anda pernah bingung					
	Projects.co.id	Project Terbaru: Pembuatan Aplikasi Web Coworking Space - Semua link dalam email ini	17 Mar				
	lina@jobstreet.com	Mobile App Developer (IDR 6,000,000 - 10,000,000) + 17 new jobs - Job Alert from JobStr	17 Mar				
	Pinterest	We picked some F14 tomcat Pins for you - We found some Pins we think might be right up	16 Mar				
	The RedShark Team	Four techniques that are certain to revolutionise cameras - Four techniques that are certain to	16 Mar				
	no-reply@sribulancer.com	Ada 2 Job Freelance Baru Yang Sesuai Keahlian Anda - Sribulancer Logo Hi bashor,	16 Mar				
	Jason Clark	Thank you for trying SmartDraw. I am here to help Hello, Thank you for signing up for a trial	16 Mar				

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.

Kembali ke Kotak Masuk	Arsipkan	Ini Spam	Hapus	Mau Diapakan?	T	Buka	1	dari sekita	r 179 <u>Lebih lama</u>
						Ŧ	Luaskan semua	Cetak	Jendela baru
Pengujian Kotak Masuk									
😭 <u>fauzan. bashor</u>								13 N	laret 2018 01.05
BASHOR FAUZAN <faux Kepada: "fauzan. bashor"</faux 	ran.b	nmail.com> _igmail.com						18 M	laret 2018 17.16
<u>Balas   Balas ke semua   Teruskan</u>	<u>Cetak</u>   <u>Hapus</u>	impilkan yang	asli						
oke									
Pada 13 Maret 2018 01.0 Barang bukti digital	15, fauzan. ba	shor < <u>putra</u>	charu∠@g	<u>mail.com</u> > menulis:					
Balasan Cepat									
Kepada: BASHOR FAUZAN	<fauzan.bas< td=""><td>hor@gmail.</td><td>com&gt;</td><td>Opsi Balas</td><td>an Lain</td><td>nya</td><td></td><td></td><td></td></fauzan.bas<>	hor@gmail.	com>	Opsi Balas	an Lain	nya			
Kirim Simpan Draf	Masukka	n teks kutipa	n pada em	nail balasan	•	Buka		dari sakita	r 170 l ebih lama
Kembali ke Kotak Masuk	Arsipkan	Ini Spam	Hapus	Mau Diapakan?	•	вика	1	dari sekita	r 179 <u>Lebin Iama</u>
Gun: Akun ini sedang	akan kotak te Anda saa digunakan di 1	lusur atau <b>o</b> t ini menggu lokasi lainnya Tampil	psi penelu unakan 48 (103.19.180 an Gmail: <u>st</u>	<b>suran</b> untuk menem <b>47 MB (31%) dari ku</b> 0.14). Aktivitas akun te andar   HTML biasa Pel	ukan pe ota An rakhir: 1 ajari lebi	esan ma <b>da sebes</b> menit yan <u>h lanjut</u>	napun dalam sek s <b>ar 15360 MB</b> g lalu pada IP 114.1	ejap! 25.165.79. <u>D</u>	etail
			Persvar	atan - Privasi - Beranda Go	onle				

Figure 7. Opening Emails that Will be Forensic

Acquisition of Email Service Based Android Using NIST Bashor Fauzan Muthohirin, Rusydi Umar, Imam Riadi

pu rtr2@gmail.com | Akun Saya | Setelan | Bantuan | Keluar

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

#### KINETIK 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 Iollipop 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, VI. 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.