HASIL CEK_Imam Riadi, Sunardi, Fitriyani Tella

by Imam Riadi, Sunardi, Fitriyani Tella Network Forensics Development Life Cycle (nfdlc),

Submission date: 15-Aug-2022 12:15PM (UTC+0700) Submission ID: 1882647959 File name: alysis_Using_Network_Forensics_Development_Life_Cycle_Method.pdf (543.79K) Word count: 3114 Character count: 16894

Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method

¹*Imam Riadi, ²Sunardi, ³Fitriyani Tella

Received: 6 November 2021 Accepted: 28 January 2022 Published: 11 February 2022

¹Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta ²Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta ³Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta ^{1,2,3}Yogyakarta, Indonesia E-mail: ¹imam.riadi@is.uad.ac.id, ²sunardi@mti.ac.id, ³fitriyani1907048012@webmail.uad.ac.id

*Corresponding Author

Abstract— E-mail is electronic mail used to send files, pictures, and others easily and quickly. However, as time goes by, there is a lot of misuse of e-mail, causing inconvenience to the recipient. One of them is spam e-mail sent to many people without prior permission from the intended owner. Hackers can forge e-mail headers anonymously for malicious purposes. The research object is to simulate sending spamming e-mails to 1 victim with a total of 40 spamming e-mails. The research follows the flow of the Network Forensics Development Life Cycle (NFDLC) method with the stages of initiation, acquisition, implementation, operation, and disposition. Simulation of sending e-mail using easy e-mail spammer tools and testing of e-mail using Wireshark tools. The test results show that 40 e-mails were successfully received or entered into the victim's inbox, and the test was successfully carried out by getting results based on predetermined parameters. The parameter is the IP address of the sender or spammer found is 72.125.68.109, the victim's IP address is 192.168.1.12.

Keyword- Network Forensics Development Life Cycle (NFDLC), Email Spamming, Easy Email Spammer, Wireshark



I. INTRODUCTION

Sending letters was a conventional way used by ancient people to communicate [1]. In contrast to today's era, which is easier and faster to communicate even at long distances, one of the things that can be done quickly and efficiently is electronic mail (e-mail). E-mail is a facility for sending digital-based letters that play a crucial role for agencies and companies in communicating [2]. The use of e-mail is no stranger to the whole world using internet technology [3]. Many people can widely use e-mail services to exchange information and collaborate with individuals, companies, and governments [4]. So that in today's era, every individual has an e-mail.

The E-mail itself has a positive side. A widespread negative side is that cybercriminals can also use e-mail as a tool to commit crimes. However, because the data transmission process is quite complicated, the guarantee of the data sent can be questioned. There can even be the possibility of e-mail forgery or attacks by hackers that can harm various parties [5]. It allows parties to misuse e-mail to obtain illegal information [6]. One of the crimes involving e-mail is e-mail spamming using an unknown person sending messages in large numbers so that the server becomes overwhelmed. Spam e-mail usually contains things that are not wanted. Spam e-mail is also traditionally called bulk/junk e-mail [7]. One of the methods commonly used to find digital evidence is to perform network forensics. Network forensics is used to obtain evidence in e-mail addresses and IP addresses of spammers [8].

Previous research used as a reference for this research is to compare e-mail security based on browsers, namely Mozilla Firefox, Google Chrome, and Microsoft Edge. The study results provide recommendations for security purposes so that e-mail providers can add several features for user security [9]. Another study related to e-mail spoofing attacks with the Digital Forensics Research Workshop (DFRWS) method approach has been carried out with the results of being able to distinguish between legitimate e-mails and e-mail spoofing [10]. Research on investigative approaches to tools, each of which has advantages and disadvantages to be adapted to user needs, has also been carried out [11].

This study aims to analyze spamming e-mails detected through network traffic. The research will be conducted simulations to find forensic e-mail spamming, which aims to find forensic evidence. Evidence found based on predetermined parameters. Parameters are the IP address used by the spammer, the IP address used by the victim, the time of sending e-mail, and the type of protocol. Several topics in previous studies were used as the basis for the flow of thought in design and development and their application to adapt to the needs and the latest relevant technological developments.

INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi

109

Digital forensics was an early term used as a synonym for computer forensics but has been expanded to include investigating all devices capable of storing digital data. [12]. In addition to finding direct evidence of a crime, digital forensics can be used to outline or attribute proof to a particular suspect, confirm statements, determine intentions, and identify sources [13]. In general, the components of digital forensics are the same as in other fields [14]. Components include humans, tools, and equipment used, and a series of rules to be managed and empowered to achieve the final goal with all the quality and feasibility [15]. Digital forensics is a science and computer technology to perform analysis and examination of the discovery of electronic evidence and digital evidence in seeing its relation to crime, for example, corruption in e-mail [16]

Network forensics is the activity of capturing, recording, and analyzing events within the network. In theory, capturing information traffic over a network is quite simple, but it is relatively complex in practice [17]. It aims to reveal facts, measure the success of the unauthorized activity, such as damaging, interfering, or infiltrating system components, and provide helpful information in recovering the related system from such harmful activities [18].

E-mail is a method for converting, sending, storing, and receiving messages through electronic communication systems. Other terms of the e-mail include systems based on the Simple Mail Transfer Protocol (SMTP) and Internet systems that allow organizations to send messages to one another [19]. The E-mail consists of two parts, namely header, and body. The title serves to carry the information needed for e-mail routing, subject lines, and timestamps. At the same time, the body is used to write messages or data to be conveyed to the recipient [3].

E-mail spam, according to Paul Graham, is defined as junk e-mail. Spam e-mail is usually intended to advertise products so that it is increasingly becoming rampant. The Cranor and La Macchia survey found that 10% of e-mails received were spam [19].

II. RESEARCH METHOD

The research method used in this research is the Network Forensics Development Life Cycle (NFDLC), as shown in Figure 1 through sequential and structured system work with the stages of Initiation, Acquisition, Implementation, Operation/Maintenance, and Disposition. The analysis on this forensic e-mail will follow the path of this NFDLC method, starting from the simulation used to conducting testing to find forensic evidence that matches the parameters. If one step has not been completed, it cannot be continued to the next step. This method will help develop the framework.

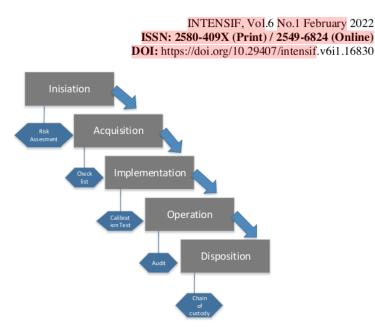


Figure 1. NFDLC METHOD [20]

A. Initiation

In this phase, the main focus is the initial risk assessment, including determining which assets in the network will guarantee digital forensic protection, including the acquisition phase model.

B. Acquisition

The acquisition process is the stage of finding evidence that supports the investigation. Tools are used to support studies and ensure that the device or procedure for collecting forensic data on the system will perform according to standards.

C. Implementation

Traditionally this is the stage where the acquired or deployed tools are used in real-time. Calibration is recommended to verify the performance of the devices used to collect evidence and document the network's performance. Baselines need to be set for network devices and then system software.

D. Operation

The operation or maintenance phase closes the execution during the verification or analysis taken based on the audit. The resulting documentation is maintained as evidence that the network and forensic tools are functioning correctly and recording as required.

E. Disposition

Chain of custody will be put into this phase to preserve the potential evidence value residing in the system.

III. RESULT AND DISCUSSION

A. Initiation

This stage performs scenarios to analyze the detection of e-mail spamming. As in Figure 2, the case scenario aims to find and obtain evidence from incoming e-mails and can validate the truth of spamming e-mails. This case scenario raises a case of online shop fraud sent via e-mail. If the origin of the e-mail is not investigated, many people will be deceived by this scenario. The scenario or design helps know the flow that will be used to analyze evidence in IP addresses and network protocols. Case scenario as in Figure 3.

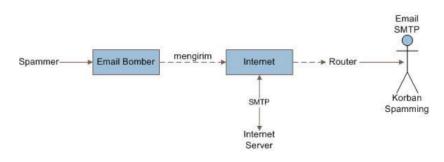


Figure 2. E-MAIL SPAMMING ATTACK SIMULATION FLOW

Figure 2 is a simulation for e-mail spamming. The process of simulating forensic retrieval on e-mail using a laptop that has been connected to the internet network, which is then accessed. The simulation starts by using a laptop as an e-mail spammer with an e-mail account olshopsorong12@gmail.com, then sending 40 spam e-mails to Gmail using the Easy e-mail spammer tool. Then an analysis of the attacked e-mail was carried out using the live forensics method where the device used must be turned on. Retrieve e-mail log data with SMTP (Simple Mail Transfer Protocol) protocol using Wireshark tools. The data is taken by selecting a data package that is recorded using Wireshark.

B. Acquisition

At this stage, an acquisition will be made using an easy e-mail spammer as a tool to simulate the sending of e-mail spamming. Spammers will send 40 spam messages to victims. Victims will receive the e-mail at one time or send it in bulk. The process of sending spam e-mails can be seen in Figure 3, which displays the e-mail spamming process on Gmail using an easy e-mail spammer.

🖄 Easy Email Spar	nmer by KaamiDev			-		×
	sy Email Spammer ed By <u>KaamiDev</u>					
Email Information	<u>20</u>	Sender Informa	tion			
Email to Spam:	ujic5238@gmail.com	Gmail Username:	olshops	sorong12@	gmail.com	
Email Body:	om/registrasi	Gmail Password:	•••••			
	Terima Kasih	Note: This gmail account It is recommended you cr purpose rather than using	eate a new a	to send the span account specifica	n emails. Ily for this	
# of Emails:	40 🜩					
		Spam Ema	ail	Exit Prog	jram	
Status: Completed						
Passe Pass	99. PRASE EXAM. ETTOMAN		A4.45			

Figure 3. E-MAIL SPAMMING

In Figure 4, 40 incoming e-mails were sent by olshopsorong12@gmail.com using the easy email spammer tools. The picture shows that a spammer has sent the evidence in the form of an email.

Q. Telusuri email		*	0	۰ :
□• C :			1-50 dari 106 < >	1.
Utama		Promosi 1 baru Alibaba Cioud		
📄 🚖 olshopsorong12	Spam Email - 40 - Tersedia Produk Terbaru o	dari olshop sorong, silahkan klik l	ink berikut jika tertarik	23.45
olshopsorong12	Spam Email - 39 - Tersedia Produk Terbaru o	dari olshop sorong. silahkan klik l	ink berikut jika tertarik	23.45
alshopsorong12	Spam Email - 38 - Tersedia Produk Terbaru o	dari olshop sorong, silahkan klik l	ink berikut jika tertarik	23.45
🗋 🚖 olshopsorong12	Spam Email - 37 - Tersedia Produk Terbaru o	dari olshop sorong, silahkan klik l	ink berikut jika tertarik	23.45
📄 🚖 olshopsorong12	Spam Email - 36 - Tersedia Produk Terbaru o	dari olshop sorong, silahkan klik l	ink berikut jika tertarik	23.45
olshopsorong12	Spam Email - 35 - Tersedia Produk Terbaru o	dari olshop sorong, silahkan klik l	ink berikut jika tertarik	23.45
🗋 🚖 olshopsorong12	Spam Email - 34 - Tersedia Produk Terbaru o	dari olshop sorong. silahkan klik l	ink berikut jika tertarik	23.45
📄 🚖 olshopsorong12	Spam Email - 33 - Tersedia Produk Terbaru o	dari olshop sorong. silahkan klik l	ink berikut jika tertarik	23.45
🗋 🚖 olshopsorong12	Spam Email - 32 - Tersedia Produk Terbaru o	dari olshop sorong. silahkan klik l	ink berikut jika tertarik	23.45
🗋 🚖 olshopsorong12	Spam Email - 31 - Tersedia Produk Terbaru o	dari olshop sorong. silahkan klik l	ink berikut jika tertarik	23.45
olshopsorong12	Spam Email - 30 - Tersedia Produk Terbaru o	dari olshop sorong, silahkan klik l	ink berikut jika tertarik	23.45
olshopsorong12	Spam Email - 29 - Tersedia Produk Terbaru o	dari olshop sorong. silahkan klik l	ink berikut jika tertarik	23.45



Figure 5 shows an incoming e-mail display, from the sender of the e-mail to the security of the e-mail.

INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi

113

Spam Em	nail - 40 Kotak Ma	suk ×
olshopsorong kepada saya 💌	12@gmail.com	
Tersedia Pro	dari:	olshopsorong12@gmail.com
silahkan klik	kepada:	ujic5238@gmail.com
https;// <u>olsho</u> r	tanggal:	26 Jun 2020 13.45
Terima Kasih	subjek:	Spam Email - 40
	dikirim oleh:	gmail.com
	ditandatangani oleh:	gmail.com
	keamanan:	🖻 Enkripsi standar (TLS) Pelajari
		selengkapnya

Figure 5. RECEIVED E-MAIL FIELD DISPLAY

Figure 6 is the contents of the original header or the full header of the e-mail received by the victim. It explained that the e-mail was sent from the e-mail testc5238@gmail.com. The destination or victim's e-mail is olshopsorong12@gmail.com. E-mail delivery date on June 25, 2020, at around 22:51 WIB. It is also seen that the message ID of the e-mail is 5ef58ce6.1c69fb81.ab1ce.b3f9@mx.google.com, with the e-mail subject being the 40th spam e-mail. Next will be testing using Wireshark.

```
Return-Path: <ujic5238@gmail.com>
Received: from DESKTOP-GRAT3RE ([125.166.67.50])
        by smtp.gmail.com with ESMTPSA id y12sm24932813pfm.158.2020.06.25.22.51.33
         for <olshopsorong@info.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Thu, 25 Jun 2020 22:51:34 -0700 (PDT)
Message-ID: <5ef58ce6.1c69fb81.ab1ce.b3f9@mx.google.com>
Date: Thu, 25 Jun 2020 22:51:34 -0700 (PDT)
X-Google-Original-Date: 25 Jun 2020 22:51:36 -0700
MIME-Version: 1.0
From: ujic5238@gmail.com
To: olshopsorong@info.com
Subject: Spam Email - 40
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
Tersedia Produk Terbaru dari olshop sorong.=20
silahkan klik link berikut jika tertarik
https;//olshopsorong@info.com/registrasi
```

Terima Kasih

Figure 6. HEADER FULL E-MAIL

C. Implementation

The implementation phase will look for IPs that pass through network traffic using the victim's IP address, namely Wireshark, as shown in Figure 7. The protocol used to find the IP address of the spammer is SMTP. All data that passes on the network is recorded and captured based on the filter process in the SMTP protocol. Next, the analysis process is carried out using Wireshark.

Velcome to Wireshark		
pen		
Magister Teknik Informatikal semester 2/butilities1.pcaping (34 MB)		
Userst ACER Downloads/dd.pcaping (634 KB)		
(Juwe)/ICDP(Dewnload/(Log Bukti Digital.pcap (327.KB)		
apture		
apture na finite (<mark>1</mark>) (rem a septor the		*)
ang this filter: 🔣 (reter a copture filter		*
eng the filter: []] [Inter a cepture filter		• •
eng this Riter: [] [Inter a copular Eller		*
eng the Barry () [Inter a coptor libry		*
eng des Reer []] [Stein a ceptor Ber cal Area Connection" 3 cal Area Connection" 3 cal Area Connection" 10 	(Addamana)	*
eng the Reer: () [Forer a copture filer	Addresses (add.sch.org/scheduler)	•

Figure 7. WIRESHARK DISPLAY

D. Operation

Operational stages are carried out regarding the implementation stage. At the operation stage, Wireshark tools are run. Forensic data collection on Gmail affected by e-mail spamming attacks can be seen in Figure 8.

0	= Z 🕸 📴 🖥			▶ 192.1		
	1¢					E Doresk
la.	Ting	Source	Destination	Protocol	/ Longth Diffs	
	39 3.343811	74.125.68.10	9 192.168.1.12	SHITP	108 S: 220 swtp.gmail.com ESMTP v15sm21775150pgp.15 - gsmtp	
	48 3,344058	197.168.1.17	74.175.68.18	SITE	76 C: FHLD DESCEP-GRATINE	
	45 3.574217	74.125.00.10		SHITP	223 5: 250 smtp.gmail.com at your service, (125.166.67.50) 250 SIZE 35082577 250 88ITHINE	250 STARTTLS
	46 3.574758	192.168.1.12			64 C: STARTES	
	48 3.787908	74.125.08.18		SHIP	04 5: 220 2.0.0 Ready to start TL5	
	83 7.574301	74.125.68.18		SHITP	108 5: 220 smtp.gmall.com ESMTP w68sm7722525pff.191 - gsmtp	
	84 7.574758	192-168-1-12		9079	76 C: THEO DESCEPTION AT THE CARACTER (125, 166, 67, 50) 150, 5775, 35693577, 350, 587701045	
In Tr SS	nternet Proteco ransmission Con imple Mail Tran	il Version 4, 5 strol Protocol, sfer Protocol	Snc: 74.125.68.109, Dst , Snc Pont: 587, Dst Po	cd), Dst: Liteon 1 192.168.1.12 rt: 1766, Seq: 5		
14 Tr 51	nternet Proteco ransmission Con imple Mail Tran Response: 250 Response o Response o	<pre>il Version 4, 5 strol Protocol, isfer Protocol -swtp.gmail.co ode: Requested anameter: swtp</pre>	<pre>Src: 74.125.68.100, Dut , Src Port: 587, Dst Po m at your service, [127 f neil action okay, com , gmail.com at your service</pre>	cd), Dst: Liteon 192.168.1.12 rt: 1766, Seq: 5 .188.67.50]\r\n leted (250)	afts[36:e8:00 (MB:08:07:96:e8:00) 55, Adx 25, Less 100 A	
10 Tr 51 V	ntornet Proteco rensmission Con imple Hail Tran Response o Response o Response i 250 to 36 87 9d	<pre>il Version 4, 5 itrol Protocol, isfer Protocol -witp.gmwil.co ode: Requested arameter: setp I=5122 35082577 #9 00 24 d3 f</pre>	Snc: 74.125.68.109, Dat , Snc Part: 587, Dat Pa am at your service, [12] f nail action oksy, comp .gmall.com at your service, r/r/m 72 cb 0d cd 08 00 45 00	<pre>cd), Dst: Liteon 1 102.168.1.12 rt: 1766, Seq: 5 5.168.67.58]\r\n bleted (250) vice, [125.166.615.</pre>	art_Selet00 (80:00:07:06:05:00) 55, A6k: 25, (An: 100 A \$7.30] 	
10 51 51 51 51 51 51 51	nternet Protoco ransmission Con inple Hail Tran 7 Response : 200 Response : 200 7 Response : 200 9 bs 26 87 0d 9 0d 112 c0	<pre>cl Version 4, 5 strol Protocol, ssfer Protocol -wetp.gmail.co cde: Requested arameter: setp -SIZE 35082377 e9 00 24 dS f 80 00 79 05 d</pre>	Src: 74.125.68.109, Dat , Src Port: 587, Dat Po m at your service, [12 f neil action oksy, com , gnall.com at your service,	od), Dst: Liteon 1 202.168.1.12 rt: 1766, Seq: 5 1.188.67.58]\r\n bleted (250) vice, [125.166.67	afts_S41e8100 (MB10801875841e81088) 55, Adx 25, Less 108 A 87.389 	
1/1 Tr 51 51	nternet Protoco renselssion Con imple Mail Tran Response : 250 Response : 250 Response : 250 bit 26 26 87 9d 00 dl 12 c0 01 0c 02 4b 61 06 54 35	<pre>cl Version 4, 5 strol Protocol, ster Protocolsetp.gmail.co code: Requested arameter: setpSIZE 35082577 w9 00 24 d3 f 00 e5 21 05 3 00 c5 21 05 3 00 00 22 35 3</pre>	<pre>inc: 74,125.68,100, Dat</pre>	d), Dst: Liteon 1 202.168.1.12 rt: 1766, Seq: 5 1.188.67.50[\r\n leted (250) vice, [125.166.61 vice, [125.166.61 vice, [125.166.61 vice, [125.166.61 vice, [125.166.61	مالي (16:06:07:06:06:08) 55, Ack: 25, (an: 100 A 57.30) 	
24 Tr 51 51 020 020 030	nternet Protoco rensmission Can imple Hail Tran Response 200 Response	1 Version 4, 5 ttrol Protocal, isfer Protocal, isfer Protocal code: Requested arameter: setp i-SIZE 35882577 a9 00 24 d3 6 00 00 79 05 d 00 00 79 05 d 00 00 23 05 3 20 05 6 d 2	Src: 74,125.68,189, but, Src Part: 587, Dat Po an at your service, [12] real action oksy, comp, spmill.com at your service, spmill.com at your service/ r/n/n 2 cb 0d cd 08 00 45 00 dd cf 45,74 40 0d cm 45 8 42 05 37 16 05 50 10 8 42 05 37 16 05 50 10 10 42 78 60 74 70 20 67 10 61 74 20 76 67 57 20 67	d), Dst: Liteon 1 102.168.1.12 rt: 1766, Seq: 5 1.185.67.50[\r\n bleted (250) vice, [125.166.67 	arts_Seleet-00 (MB100:07:064:05:00) 55, Ackz 25, Less 100 A 47.50 15. 1.05. 1	
1/1 51 51 010 010 010 010 010	ternet Protoco ransmission Can imple Hail Tran Response 1 Response 1 Response 1 Response 1 Response 1 bis 36 87 Md 00 dl 12 c0 01 0c 02 40 01 00 62 40 01 00 62 40 01 00 52 35 0 dl 100 6c 20 73 05 72	el Version 4, 5 strol Protocal, isfer Protocal i-astp.gmill.co ode: Requested orameter: smill.co ode: 24 d3 f 80 00 79 05 d 06 65 21 05 3 90 00 32 35 3 20 55 6 f d3 2 76 59 65 52	Src: 74,128.68,100, Dat , Src Wort: 507, Dat Po an at your service, [12] n sail action oksy, com , gmail.com at your serv ///a /2 cb 0d cd 82 00 45 00 d cd 64 70 46 cd 88 84 42 26 37 12 65 50 18 85 20 73 60 47 40 20 67 85 20 73 60 47 82 20 86 10 42 78 79 75 72 (2 20 50 31 23 35 26 1) (2 20 50 31 23 35 26 1) (2 20 50 31 23 35 26 1)	cd), Dst: Liteon 1 202.168.1.12 rt: 1766, Seq: S 1.185.67.50]\r\n blted (250) vice, [125.166.67 	مالي (16:00:07:06:05:07) 55, Ack: 25, (es: 100 n 47-50 100	
14 Tr 51 51 889 810 820 810 820 810 820 810 820 810 820 810 810 810 810 810 810 810 810 810 81	tornet Proteco ransmission (an imple Mail Tran Response 200 Response 200 Response 200 Response 200 55 26 27 00 01 40 02 40 01 40 02 40 01 40 02 51 01 40 020 51 01 4	<pre>http://working.com/ http://working.com/ string.protocol string.protocol odd: Requested arameter: smtp -5122 35082577 20 08 24 d3 f 00 08 79 06 d 00 08 27 05 3 06 06 27 05 3 26 05 6f 6d 5 7 02 06 365 2 3 26 35 38 5</pre>	Inc: $74, 125, 68, 140$, 05 H , Src Part: 587, 05 H an at your service, [12] mail action only, compared to the service, and the service, and the service, and the service, and the service of the ser	cd), Dst: Liteon 1 202.468.1.12 rt: 1766, Seq: 5 3.386.07.50[Vro lice, [125.166.6] 5. 5. 	HT_SELEND (MILSON7MELEINE) 55, Adda 25, Less 100 A A 55, Adda 25, Less 100 A 55, Adda 25,	
1/1 51 51 000 010 020 050 050 050 050	tornet Proteco renselssion Can Imple Mail Tran * Response p * Response p * Response p * Response p * Response p 01 & 02 40 01 & 02 40 01 & 02 40 01 & 05 25 04 01 49 52 20 73 65 72 36 36 22 36	el Version 4, 5 strol Protocol stron Protocol stron Protocol stron Protocol strong genil.co del Reyested strong 20 06 del 24 d5 f 80 00 52 85 3 20 65 62 10 5 20 65 62 5 20 65 62 5 20 65 65 2 20 7 20 7	Src: 74,128.68,100, Dat , Src Wort: 507, Dat Po an at your service, [12] n sail action oksy, com , gmail.com at your serv ///a /2 cb 0d cd 82 00 45 00 d cd 64 70 46 cd 88 84 42 06 37 12 65 50 18 85 20 73 60 47 40 26 67 85 20 73 60 47 40 26 10 20 50 31 23 35 26 10 20 50 50 13 23 55 26 10 20 50 50 12 20 50 50 10 20 50 50 50 10 20 50 50 10 20 50 50 10 20 50 10 50	cd), Dst: Liteon 1 202.168.1.12 rt: 1766, Seq: S 1.185.67.50]\r\n blted (250) vice, [125.166.67 	art_Steletic0 (MSID:07:061-05100) 55, Adxi 25, Less 109 n 47.50 1	
1/1 51 51 0000 0000 0000 0000 0000	ternet Proteo rensmission Con imple Mail Tran / Response c Response c Respons	cl Version 4, 5 trel Protocol Frances, Benested Frances, Benested Frances, Second Frances, Second Fran	Inc. 74,125,461,409, Dit , Src. Part: 187, Dit Po m at your service, [12] m stil action okky, com , guall.com stypur serv $\Lambda/r/a$ (4 2) at 74 cd cd at (4 2) at 74 cd cd (5 50 15 (4 2) at 74 cd (5 50 15 (4 2) at 74 cd (5 50 15 (5 2) 13 22 cd (5 2) 13 (5 2) 13 22 cd (5	ed), Dati liteor 120.168.112 120.168.112 120.168.112 120.168.112 120.168.112 121.168.112 121.168.112 121.168.112 121.168.112 121.158.1121.158.112 121.	HT_Stele+00 (MIISOIT/MireEixe) 55, Adv 25, Lex: 100 A 55, Adv 255, Lex: 100 A 55, Adv 255, Lex: 100 A 55, Adv 255, Lex: 100 A 55, Adv 255	
1 / 1 /	ternet Preteco renselission Can imple Noil Tran Response D Response D Respons	cl Version 4, 5 throl Protocol. Ster Protocol. Heating genil.co ode: Requested arameter: smtp. -SIZE 35002577 w9 00 24 dB f 00 00 29 00 d 00 00 29 00 d 00 00 29 00 d 00 00 29 00 d 00 00 22 35 3 20 05 0 f 00 d 27 0 f 00 d 57 0 f 00 d 57 0 f 00 d 57 0 d 58 0 d 58 4 4 5 3 54 4	Inc. 74.125.481.140, 051. , Snc. Parts 1307, Dat Pro m at your service, [12] m still action akky, com public com at your serv- Λ_{1} /n (a da 74 dd cd dd dd dd (a da 74 dd 27 dd 72 dd 75 (b dd 20 23 dd 72 dd 74 dd 73 (c dd 72 dd 74 dd 75 dd 75 (c dd 75 dd 73 dd 75 dd 75 (c dd 75 dd 73 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75) (c dd 75 dd 75 dd 75) (c dd 75 dd 7	od), Dsti Liteon 1 202.468.1.12 1 202.468.1.12 1 203.468.1.12 1 126.468.1.12 1 126.468.1 1 125.166.61 1 125.166.61 1 125.126.4 1 125.126.4	art_Stelet00 (80:00:07:04:e5:00) 55, Acki 25, (est: 109 n 67.50] 0	
2 In 7 51 7 51	Internet Protuce resultsion Con imple Holl Tran Response p Response of Response of Respons	cl Version 4, 5 strol Protocol. heatpenet. heatpenet. year Protocol heatpenet. years and seven seven heatpenet. years and seven seven seven heatpenet. years and seven seven seven seven heatpenet. years and seven seve	Inc. 74,125,461,409, Dit , Src. Part: 187, Dit Po m at your service, [12] m stil action okky, com , guall.com stypur serv $\Lambda/r/a$ (4 2) at 74 cd cd at (4 2) at 74 cd cd (5 50 15 (4 2) at 74 cd (5 50 15 (4 2) at 74 cd (5 50 15 (5 2) 13 22 cd (5 2) 13 (5 2) 13 22 cd (5	ed), Dati liteor 120.168.112 120.168.112 120.168.112 120.168.112 120.168.112 121.168.112 121.168.112 121.168.112 121.168.112 121.158.1121.158.112 121.	std_std=0.00 (MDIS01975Md1e5100) 59, Ackz 25, (ANX 100 n 25.00	

Figure 8. CAPTURE WIRESHARK RESULT

Figure 8 The attacker's IP 72.125.68.109, who sends an e-mail in SMTP format, is the address showing the results of recording Wireshark data packets that pass through internet network traffic. Data packets marked with arrows are data packets from IP spammers.

E. Disposition

This stage is based on the results of operations performed using Wireshark. The e-mail sent is spamming using an easy e-mail spammer with olshopsorong12@gmail.com and sent to Ujic5238@gmail.com. Figure 8 is the capture result evidence of e-mail spamming in the form of source IP addresses and destination IP addresses. Table 1 is the result of the research.

No	Evidence				
No.	Data Type	Result			
1.	E-mail spammer address	Olshopsorong12@gmail.com			
2.	Victim's E-mail Address	Ujic5238@gmail.com			
3.	Number of incoming e-mails	40 E-mail			
4.	Protocol Type	SMTP			
5.	IP Address	72.125.68.109 (Spammer) 192.168.1.12 (korban)			

IV. CONCLUSION

E-mail is a system used to send and receive messages in files, images, audio, etc. The NFDLC method was successfully implemented to find evidence. Simulation of sending e-mail using easy e-mail spammer tools and testing of e-mail using Wireshark tools. The test results show that 40 e-mails were successfully received or entered into the victim's inbox, and the test was successfully carried out by getting results based on predetermined parameters. The parameter is the IP address of the sender or spammer found is 72.125.68.109, the victim's IP address is 192.168.1.12.

REFERENCES

- N. A. Q. Muslimin, Sutardi, and L. Tajidun, "Aplikasi Keamanan E-Mail Menggunakan Algoritma AES (Advanced Encryption Standard) Berbasis Android," semanTIK, vol. 2, no. 1, pp. 321–330, 2016, doi: 10.1016/j.nut.2008.10.021.
- [2] M. A. Sutisna and I. Riadi, "Analisa Forensik Pada Email Spoofing," J. Teknol. Terpadu, vol. 4, no. 1, pp. 38–43, 2018.
- [3] N. Nugroho, Z. Azmi, and S. N. Arif, "Aplikasi Keamanan Email Menggunakan Algoritma Rc4," J. SAINTIKOM, vol. 15, no. ISSN: 1978-6603, pp. 81–88, 2016, [Online]. Available: https://lppm.trigunadharma.ac.id/public/fileJurnal/hpO91 Jurnal Nurcahyo.pdf.
- [4] T. Hadianto, W. Prasetyo, and R. B. Bahaweres, "Studi Banding Email Forensic Tools," Stud. Inform. J. Sist. Inf., vol. 10, no. 1, pp. 53–61, 2017, [Online]. Available: http://journal.uinjkt.ac.id/index.php/sisteminformasi/article/view/7751/4303.
- [5] S. Akashi and Y. Tong, "The E-mail Spoofing on the Network Layer Protocols and Countermeasures Besides the Sender Domain Authentication," Int. J. Inf. Electron. Eng., vol. 10, no. 1, pp. 22–27, 2020, doi: 10.18178/ijiee.2020.10.1.715.

- [6] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, "A comprehensive survey for intelligent spam e-mail detection," IEEE Access, vol. 7, pp. 168261–168295, 2019, doi: 10.1109/ACCESS.2019.2954791.
- [7] Hoiriyah, B. Sugiantoro, and Y. Prayudi, "Investigasi Forensik Pada Email Spoofing Menggunakan Metode Header Analysis," J. DASI, vol. 17, no. 4, pp. 20–25, 2016, [Online]. Available: http://ojs.amikom.ac.id/index.php/dasi/article/view/1553/1431.
- [8] A. Ginanjar, N. Widiyasono, and R. Gunawan, "Analisis Serangan Web Pishing Pada Layanan E-commerce dengan Metode Network Forensic Process," J. Terap. Teknol. Inf., vol. 2, no. 2, pp. 47–58, 2018, doi: 10.21460/jutei.2018.22.103.
- [9] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," JISKA (Jurnal Inform. Sunan Kalijaga), vol. 1, no. 3, p. 108, 2017, doi: 10.14421/jiska.2017.13-02.
- [10] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," J. Edukasi dan Penelit. Inform., vol. 2, no. 2, pp. 111–117, 2016, doi: 10.26418/jp.v2i2.16821.
- [11] I. Riadi, R. Umar, and Mustafa, "Review Article: Investigasi Forensik Email dengan Berbagai Pendekatan dan Tools," J. Inform. J. Pengemb. IT, vol. 04, no. 02, pp. 120– 122, 2019, doi: 10.30591/jpit.v4i2.1134.
- [12] I. Zuhriyanto, A. Yudhana, and I. Riadi, "PERANCANGAN DIGITAL FORENSIK PADA APLIKASI TWITTER MENGGUNAKAN METODE LIVE FORENSICS," Semin. Nas. Inform., pp. 86–91, 2018.
- [13] Sunardi, I. Riadi, and A. Sugandi, "Forensic analysis of Docker Swarm cluster using GRR Rapid Response framework," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 2, pp. 459–466, 2019, doi: 10.14569/ijacsa.2019.0100260.
- [14] S. Sunardi, I. Riadi, and I. M. Nasrulloh, "Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response," J. Teknol. Inf. dan Ilmu Komput., vol. 6, no. 5, p. 509, 2019, doi: 10.25126/jtiik.2019651516.
- [15] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.
- [16] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone," J. Edukasi dan Penelit. Inform., vol. 2, no. 1, 2016, doi: 10.26418/jp.v2i1.14369.
- [17] I. W. Ardiyasa, "Aplikasi Analisis Network Forensic Untuk Analisis Serangan Pada Syslog Server," Res. Comput. Inf. Syst. Technol. Manag., vol. 2, no. 02, p. 59, 2019, doi: 10.25273/research.v2i02.5220.
- [18] R. Setiawan, NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT) PROGRAM PASCASARJANA FAKULTAS TEKNOLOGI INDUSTRI. 2019.
- [19] L. O. M. Saidi, Pengembangan Framework untuk Investigasi Email Forensics Menggunakan Metode Systems Development Life Cycle (SDLC), vol. 117. 2017.
- [20] F. Tella et al., "Perbandingan Hasil Forensics Jaringan Terhadap Serangan E-mail Spamming dan Spoofing," vol. XII, no. 2, pp. 121–127, 2020.

INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi

117

HASIL CEK_Imam Riadi, Sunardi, Fitriyani Tella

ORIGINALITY REPORT	11%	10%	10%
	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES Submit Student Pap	<mark>ted to Universit</mark> a er	as Brawijaya	10%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		