HASIL CEK_Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method

Submission date: 23-Apr-2022 11:22AM (UTC+0700) Submission ID: 1817908245 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

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

¹*Imam Riadi, ²Sunardi, ³Fitriyani Tella

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



108

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.

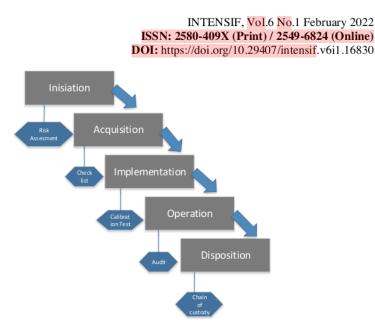


Figure 1. NFDLC METHOD [20]

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.

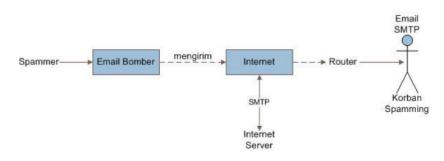


Figure 2. E-MAIL SPAMMING ATTACK SIMULATION FLOW

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 Span	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:	olshop	sorong12@g	gmail.com	
Email Body:	om/registrasi	Gmail Password:	•••••	•••••		
	Terima Kasih	Note: This gmail account It is recommended you or purpose rather than using	eate a new			
# of Emails:	40 ≑					
		Spam Ema	ail	Exit Prog	Iram	
Status: Completed						
Passa Fault	99 - PRARE ERRAIL EXTRINANI		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.

۹	Telusuri email	• 0	8
	C i	1-50 dari 106 <	> 1-
	Utama	Sosial Promosi Ibaru Alibaos Cood	
0	dishopsorong12	Spam Email - 40 - Tersedia Produk Terbaru dari olshop sorong, silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 39 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 38 - Tersedia Produk Terbaru dari olshop sorong, silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 37 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	cishopsorong12	Spam Email - 36 - Tersedia Produk Terbaru dari olshop sorong, silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 35 - Tersedia Produk Terbaru dari olshop sorong, silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 34 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 33 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 32 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 31 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 30 - Tersedia Produk Terbaru dari olshop sorong. silahkan klik link berikut jika tertarik	23.45
	olshopsorong12	Spam Email - 29 - Tersedia Produk Terbaru dari olshop sorong, silahkan klik link 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.

역 ㅎ ㅎ 한 후 호 📱 🧮 역 역 역 표		
Welcome to Wineshark		
Open		
E1/Magister Teknik Informatikal semester 2/buti/tes1.pcaping (34.M8)		
C/Userd/ACER/Dewnloadd/dd.pcaping (634.KB)		
C1(Userd)ACDP(Downloadd)(Log Buildi Digital.pcap (327 KB)		
Capture		
Capture		*
		*)
Local Area Connection" 5		*
Local Area Convection*5 Local Area Convection*5 Local Area Convection*5 Local Area Convection*10		*) X
Lead Area Convector' 5 Lead Area Convector' 5 Lead Area Convector' 1 Lead Area Convector' 1 Lead Area Convector' 1 Lead Area Convector' 1		×
Long the New ()) (rein a context film Lond Leve Connection' 5 Lond Leve Connection' 5 Lond Leve Connection' 10 W-51 Lond Leve Connection' 11 Long Leoplex (Market Leve Leve Leve Leve Leve Leve Leve Le	[Addamases]	
Long the Billin () (citre a report film) Local Area Connection' 5 Virtualities (Not Only Notwork) Local Area Connection' 10 Virtual Local Connection' 11	felth-d5x7-eddd-sidh2/fe11	
Long the New ()) (rein a context film Lond Leve Connection' 5 Lond Leve Connection' 5 Lond Leve Connection' 10 W-Si Lond Leve Connection' 11 Long Leoplex (Markov Long Leoplex (Markov Leoplex (Markov Leop		
Joing No Berry Univer a conduct Her Local Joine Consultant's Visionalitie Velici ON Microsoft	Fe80x45x7xe444x48x2Fe31, Fe80x45x7xe444x84x2Fe31	

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.

(=	2 1 B	200	* * 留下来	. = q.	2, 0, 11		_	
arsto								🛛 🗔 🔹 Doresk
0.	Ting	Deur co	Destinat	tion	Protocol	Longth Dr	fo	
	39 3.343811	74,125,68,10		68.1.12	SHITP			wto.gmail.com ESMTP vi5sm21775150ogo.15 - gsmtp
	48 3, 344058	197.168.1.1		5,68,189	WITP .			DPACTOR-ORATINE
	45 3.574217	74.125.68.10		68.1.12	SHTP	223 5	250 sm	stp.gmail.com at your service, [125.166.67.50] 250 SIIE 35082577 250 68ITHINE 250 STARTLS
	46 3.574758	192.168.1.1		5.68.189	SMTP		START	
	48 3.787966	74.125.68.18		60.1.12	SHITP			.0.0 Ready to start TLS
	83 7.574301	74.125.68.1		68.1.12	SHITP			mtp.gmail.com ESMTP w68sm7722525pff.191 - gsmtp
	84 7.574758	192-168-1-12		5.65.189	SHIP			DESCEPTION OF A AND A AN
Int Tra Sin	connet Protoco Insmission Com ple Mail Tran	ol Version 4, strol Protocol sfer Protocol	:9d:ed (24:d3:f2 Src: 74.125.68.1 , Src Port: 587,	ob:9dicd), 0 09, Dst: 202. Dst Port: 1	.168.1.12 766, Seq: 55,	9d:e9:0	0 (60:00	85:87:9d:e9:00)
Int Tra Sin	Response p Response p Response p	al Version 4, strol Protocol Hostp.gewillo code: Requeste	:9died (24:d3:f2 Src: 74.125.68.1 , Src Port: 587, on at your servic d nail action ok: p.gmail.com at yo	<pre>cb:9d:ed), 0 00, Dst: 102. Dst Port: 10 ee, [125.365. By, completed</pre>	Dst: LiteonTe .168.1.12 766, Seq: 55, .67.58]\r\n d (250)	9d:e9:0	0 (60:00	85:87:9d:e9:00)
Int Tra Sin	Arnet Protoco Inselssion Com ple Hail Tran Response 1 Response 1 Response 1 258 86 87 9d	ol Version 4, http://protocol http://wrtp.gmwil.or tode: Requester http://wrtp.gmwil.or tode: Requester http://wrtp.gmwil.or 1000000000000000000000000000000000000	<pre>:9dicd (24:d3:f2 Src: 74,125.68.1 , Src Port: 587, on at your servic d nail action oks p.gmail.com at yo 7\r\n f2 cb 9d cd 08 00</pre>	<pre>trob:5died), 1 09, Dsti 202. Dst Port: 1: ew, [125.166. sy, completed our service, e 45 00</pre>	Dst: LiteonTe .168.1.12 766, Seq: 55, .67.50]\r\n d (250) [125.166.67.	_9d:e9:0 . Ack: 23 50] E.	0 (60:00	85:87:9d:e9:00)
Into Tra Sim	ornet Protoco nswission Car ple Mail Tran Response : 258 Response : 258 bs 86 87 94 00 di 12 c0	ol Version 4, atrol Protocol aster Protocol E-setp.gemil.o code: Requeste parameter: setp -SIZE 3500257 x9 00 24 d3 00 00 79 05	:9dicd (24:d3:f2 Src: 74,125.68.1 , Src Port: 587, on at your servi d nail action oke p.gmail.com at yo 7\r\m	<pre>trob:5dicd), 1 09, 0st: 292. Dst Port: 1: cw, [125.386. sy, completed our service, d c0 s5 d c0 s5</pre>	Dst: LiteonTe 1.168.1.12 766, Seq: 55, .67.50]\r\n d (250) [125.166.67.	590:e9:0 . Ack: 23 50] E.	0 (60:00	85:87:9d:e9:00)
Int Tra 510 510 510 510 510 510 510 510	ternet Protect insmission Car ple Hail Tran Response : Response : Response : 155 86 87 94 00 41 12 c0 01 0c 02 40 01 0c 02 40 01 06 5a 35	el Version 4, strol Protocol ster Protocol - web, gewillo tode: Requeste arameter: set -5122 3508257 e9 00 24 d3 00 e5 24 05 06 e5 27 05 08 00 32 35	19died (24:d3:f2 Src: 74.125.68.2 , Src Part: 587, on at your servid d neil action okt p.gmail.com at yo 7/rin f2 cb 0d cd 08 0 dd c0 4a 7d 48 6 dd c0 4a 7d 48 (0 dd 2 3 3 f1 c 0) 2 22 7 5 60 74 70	<pre>trob:Sdied), 1 09, Dati 102. Dat Port: 11 ee, [125.186. ay, completed our service, e 45 00 d c0 a5 s5 0 18 s5 0 18 </pre>	Dst: LiteonTe .168.1.12 766, Seq: 55, .67.50%[\r\n d (250) [125.166.67. 	_9d:e9:0 . Ack: 23 50] E. P.	0 (60:00	85:87:9d:e9:00)
Int Tra 510 830 830 830 830 830 830 830 830	const Protoco nsmission Con ple Mail Tran Response 2 10 Response 2 Response 2 Response 2 8 87 9d 00 d1 12 c0 01 06 02 4b 01 00 5a 35 01 00 5a 35	al Version 4, http://protocal hsfer Protocal hsfer Protocal tode: Requeste harvaeter: set h-SIZE 3508237 #9 00 24 d3 00 02 79 05 00 65 27 05 00 06 32 35 24 05 06 dd	<pre>:9d:cd (24:d):f2 Src: 74.125.68.1 , Src Port: 587, </pre>	trob:Sdred), 1 (0), Dstr 102, Dst Pont: 10 ex, [125.188. sy, completed our service, e 45 00 d c0 85 5 50 18 5 50 18 6 22 67 7 27 mmi	Dst: LiteonTe 168.1.12 766, Seq: 55, 167.58[\r\n d (250) [125.166.67. 	- od: e9:0 - Ack: 23 50] E. E. P. 8 - 8	0 (60:00	85:87:9d:e9:00)
Int Tra Sin V 830 830 830 830 830 830 830 830 830 830	cornet Protoco mamission Cor ple Hail Tran Response : 200 Response : 200 Response : 200 00 dl 12 c0 01 dc 02 4b 01 dc 02 4b 01 dc 05 35 0d 61 09 0c	al Version 4, strol Protocol insfer Protocol bode: Requeste protocol:	<pre>:9dicd (24:d):42 Snc: 74.128.68.1 , Snc Part: 587, on at your servin d neil action okt p.gmail.com at yo 7\r\m 72 cb 0d cd 08 96 6d c8 48 7d 48 60 18 42 36 37 1c 60 86 2d 73 6d 74 70 28 61 74 28 78 6 2 28 50 31 32 23</pre>	trob:Sdred), t 40, Dat 102. Dat Port: 1: ex. [135.186. ay, completed our service, 6 45 00 d c0 85 6 22 57 f 75 72 mai	Dst: LiteonTe 1468.1.12 766, Seq: 55, .67.50[\r\n d (250) [125.166.67. 		0 (60:00	85:87:9d:e9:00)
Int Tra 510 010 020 030 040 050 050	connet Protoco musicsion Car pile Hall Tran Response : 210 Response : 20 Response : 20	al Version 4, strol Protocal aster Protocal hostic Protocal code: Requeste arameter: set (-5722 1508272 90 00 24 d3 00 00 79 05 06 60 21 05 20 00 24 05 20 00 25 35 20 01 6 6d 76 09 03 05 78 23 53	<pre>:9d:cd (24:d):f2 Src: 74.125.68.1 , Src Port: 587, </pre>	trob:Sdied), 1 (0), 0st 102, Dst Port: 11 ex, [125.186. Ny, completed our service, 4 d8 a5 5 50 18 6 22 67 f 75 72 mai 5 22 31 st 6 22 53 65.	Dst: LiteonTe 168.1.12 766, Seq: 55, 167.58[\r\n d (250) [125.166.67. 	.9d1e910 . Ack: 23 59] 5. P. P. 	0 (60:00	85:87:9d:e9:00)
2nb Tra 510 020 020 050 050 050 050 050	connet Protoco musicsion Car pile Hall Tran Response : 210 Response : 20 Response : 20	al Version 4, strol Protocol store Protocol store Protocol store Protocol store Protocol store Protocol store 1	Isdiced (24:d3:42 Sec: 74.125.48.1 Sec: 74.125.48.15.15.15.15.15.15.15.15.15.15.15.15.15.	Inconstruct, but 192. Det Port: 192. Det Port: 192. Det Port: 193. Det Port: 192. Det Por	Dst: LiteonTe 1468.1.12 766, Seq: 55, 167.50[\r\n (25.0) [125.166.67. 	59019930 , Acks 23 59] 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5.	0 (60:00	85:87:9d:e9:00)
100 100 100 100 100 100 100 100	conet Protect maximum and pice fail Transformer 2016 Response p Response p Re	al Version 4, http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://protocol http://p	19dicd (24:03:42), scient 74.128:48.1 , Sice Parts: 587, an at your servin d nail action oku p.gwali.com at yo p.gwali.com at yo 72 ch ol cd as 0 d cf 48.74 46.6 10 42 58 37 12.6 10 42 58 37 12.6 10 42 28 38 12.5 10 40 48 22 35 38 2 10 48 32 58 38 2 10 48 38 38 38 38 10 48 38 38 38 10 48 38 38 10 48 38 38 10 48 38 38 10 48 3	tribusdiced), E 40, 0st 1922. Dist Port: 11 0st, [123, 186, my, completed our service, 4 d8 45 5 50 18 	Dat: LiteonTe 1.168.1.12 706, Seq: 55, 1.67.58[\r\n d (250) 1.25.166.67. 	501:09:0 Ack: 25 50] 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5. 5.	0 (60:00	85:87:9d:e9:00)
510 510 510 510 510 510 500 8050 8050 80	ornet Protect maximum and pice fail Tran Response 1 200 Response 1 200 Response 1 200 Response 1 200 00 01 12 c0 00 01 12 c0 00 01 12 c0 00 01 12 c0 01 00 53 35 06 01 10 05 12 07 305 72 35 36 20 30 24 30 44 41 52 35 34 41 52	al Version 4, strol Protocol Franceson Franceson Store Protocol Franceson Store Protocol Franceson Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Store Sto	<pre>19dicd (24:d3:42) sec: 74.125.48.1 , Sec Port: 1007, on at your servin d mail sector okt pegmil.com at y 7/r/n 22 ch 04 d m80 d dd c5 47 d4 6 24 26 a7 12 cd 04 28 42 26 a7 12 cd 28 42 26 a7 12 cd 28 42 36 a7 12 cd 28 43 56 a7 37 malk 45 56 46 a3 22 35 30 2 23 56 45 a4 56 a5 53 48 4 56 56 55 48 3</pre>	tribusdited), E 40, Dati 102. Dat Port: 102. Dat Port: 102. ex, [125.386. ex, [125.386. ex	Det: LiteonTe 1.168.1.12 766, Seq: 55, 1.67.58[\r\n d (250) [125.166.67. , dD7ta 1.5	. 3d1e9:0 . Ack: 23 50] E. , P. 	0 (60:00	85:87:9d:e9:00)
Into Train Sin Sin Sin Sin Sin Sin Sin Sin Sin S	connet Protect maximum and pice fail Trans Response () Response ()	bl Version 4, strol Protocol H-wein, genil (b) strong protocol H-wein, genil (b) strong protocol (c)	19dicd (24:03:42), scient 74.128:48.1 , Sice Parts: 587, an at your servin d nail action oku p.gwali.com at yo p.gwali.com at yo 72 ch ol cd as 0 d cf 48.74 46.6 10 42 58 37 12.6 10 42 58 37 12.6 10 42 28 38 12.5 10 40 48 22 35 38 2 10 48 32 58 38 2 10 48 38 38 38 38 10 48 38 38 38 10 48 38 38 10 48 38 38 10 48 38 38 10 48 3	tribusdiced), E (00, 0st 1002, 0st Port: 11 ce, [123.186, sy, completed our service, 4 d5 00 d c8 a5 5 50 15 6 245 36 6 24 53 65 a 57 5 30 24 0-1 5 30 24 0-1 6 455 455 4 455 465 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	Dat: LiteonTe 1.168.1.12 706, Seq: 55, 1.67.58[\r\n d (250) 1.25.166.67. 	 Sdie9:0 Ack: 25 S0] 50] 50, 50, 50, 51, 51, 52, 53, 54, 54	0 (60:00	86:87:9d:e9:00)

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.

Ne	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)				

Table 1. E-MAIL	SPAMMING ANAL	YSIS RESULTS
-----------------	---------------	--------------

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_Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method

ORIGINALITY REPORT

9%	7%	7%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
MATCH ALL SOURCES (ONL	Y SELECTED SOURCE PRINTED)		

* Submitted to Universitas Kristen Satya Wacana Student Paper

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		