INTENSIF, Vol.6 No.1 February 2022
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v6i1.16830

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, [2]Sunardi, [3]Fitriyani Tella
[1]Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta
[2]Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
[3]Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta
[1,2,3]Yogyakarta, Indonesia
E-mail: [1]imam.riadi@is.uad.ac.id, [2]sunardi@mti.ac.id,
[3]fitriyani1907048012@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

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v6i1.16830

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.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v6i1.16830

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.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v6i1.16830

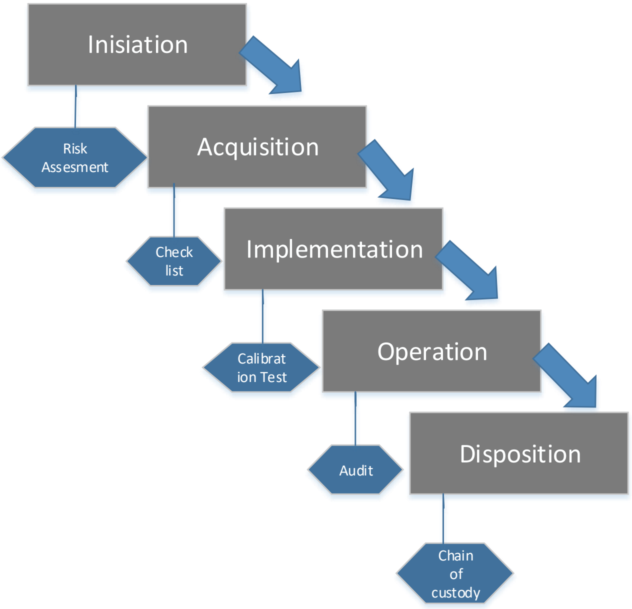


Figure 1. NFDLC METHOD [20]

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.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v6i1.16830

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.

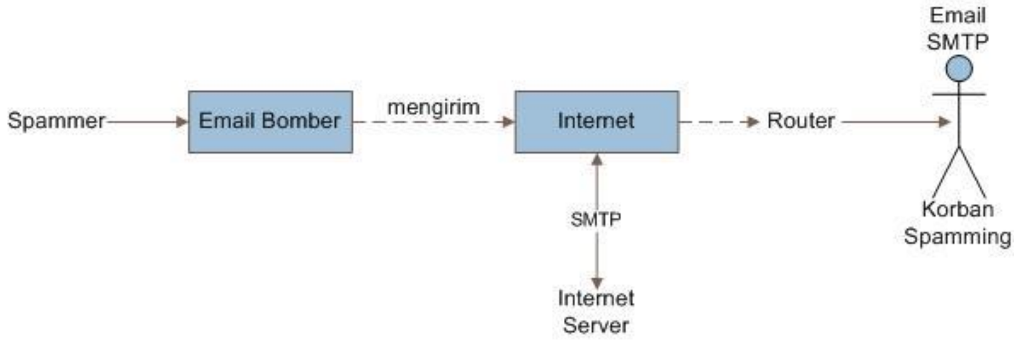
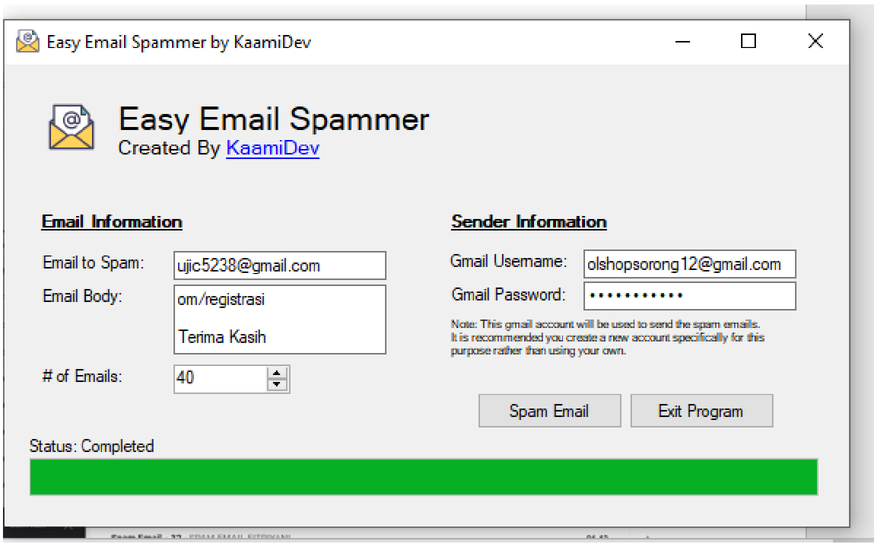


Figure 2. E-MAIL SPAMMING ATTACK SIMULATION FLOW

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 Spammer
Created By KaamiDev

Email Information

Email to Spam: ujic5238@gmail.com
Email Body: om/registrasi
Terima Kasih
# of Emails: 40

Sender Information

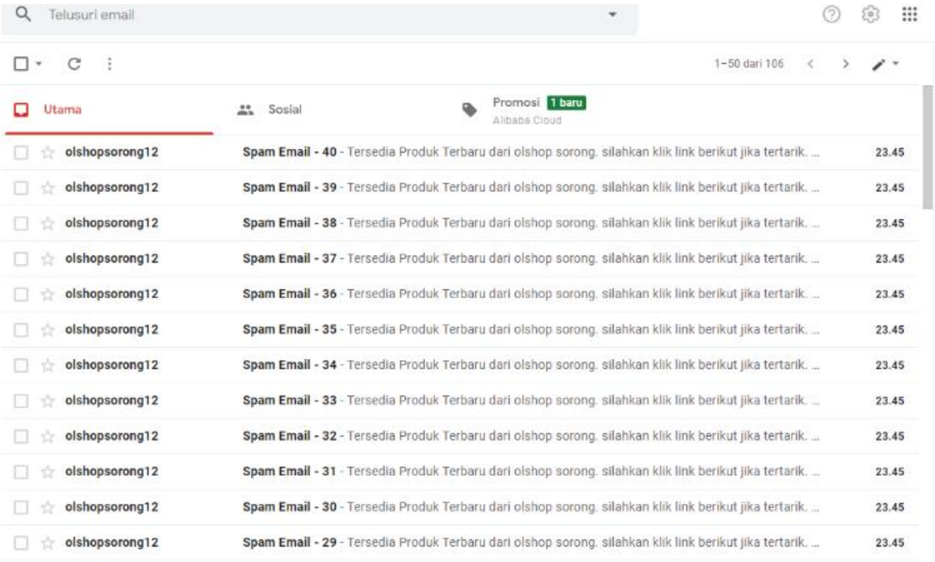
Gmail Username: olshopsorong12@gmail.com
Gmail Password: •••••••••••

Note: This gmail account will be used to send the spam emails. It is recommended you create a new account specifically for this purpose rather than using your own.

Status: Completed

Figure 3. E-MAIL SPAMMING

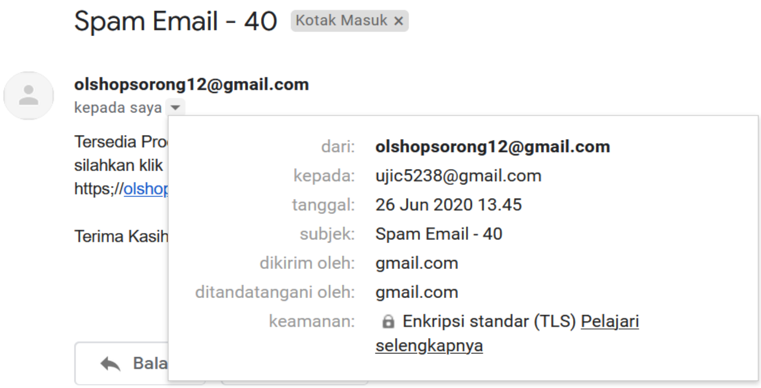
In Figure 4, 40 incoming e-mails were sent by olshopsorong12@gmail.com using the easy e-mail spammer tools. The picture shows that a spammer has sent the evidence in the form of an e-mail.



olshopsorong12	**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
olshopsorong12	**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 4. SPAM E-MAIL RECEIVED BY THE VICTIM

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



Spam Email - 40 Kotak Masuk ×

olshopsorong12@gmail.com
kepada saya

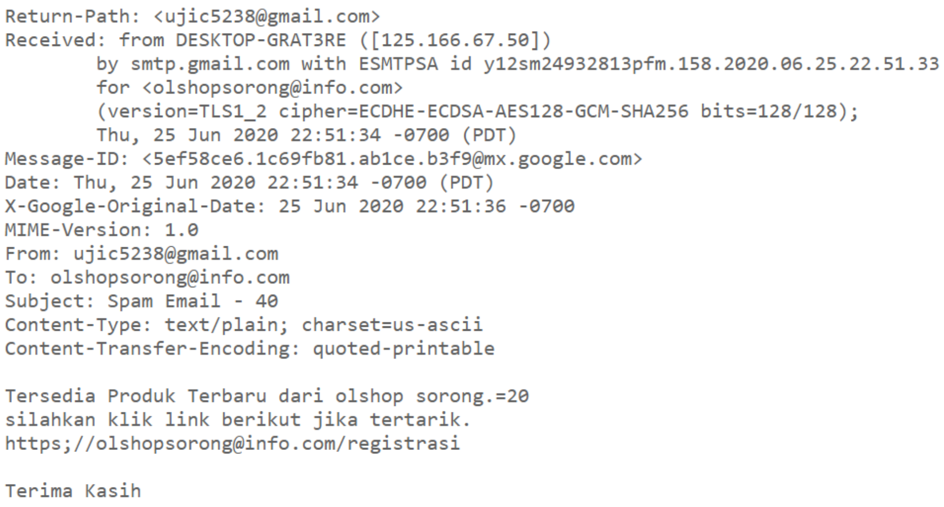
Tersedia Pro
silahkan klik
https;//olshop

Terima Kasih

dari: olshopsorong12@gmail.com
kepada: ujic5238@gmail.com
tanggal: 26 Jun 2020 13.45
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.

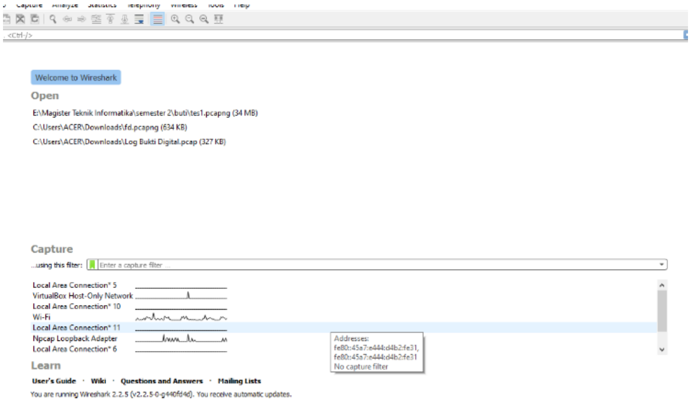


```
Return-Path: <ujic5238@gmail.com>
Received: from DESKTOP-GRAT3RE ([125.166.67.50])
        by smtp.gmail.com with ESMTPSA id y12sm24932813pfm.158.2020.06.25.22.51.33
        for <olshopsorong@info.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Thu, 25 Jun 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.


Capture Analyze Statistics Telephony Wireless Tools Help
<Ctrl-/>
Welcome to Wireshark
Open
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

E:\Magister Teknik Informatika\semester 2\buti\tes1.pcapng (34 MB)
C:\Users\ACER\Downloads\fd.pcapng (634 KB)
C:\Users\ACER\Downloads\Log Bukti Digital.pcap (327 KB)

...using this filter: Enter a capture filter ...

Local Area Connection* 5
VirtualBox Host-Only Network
Local Area Connection* 10
Wi-Fi
Local Area Connection* 11
Npcap Loopback Adapter
Local Area Connection* 6

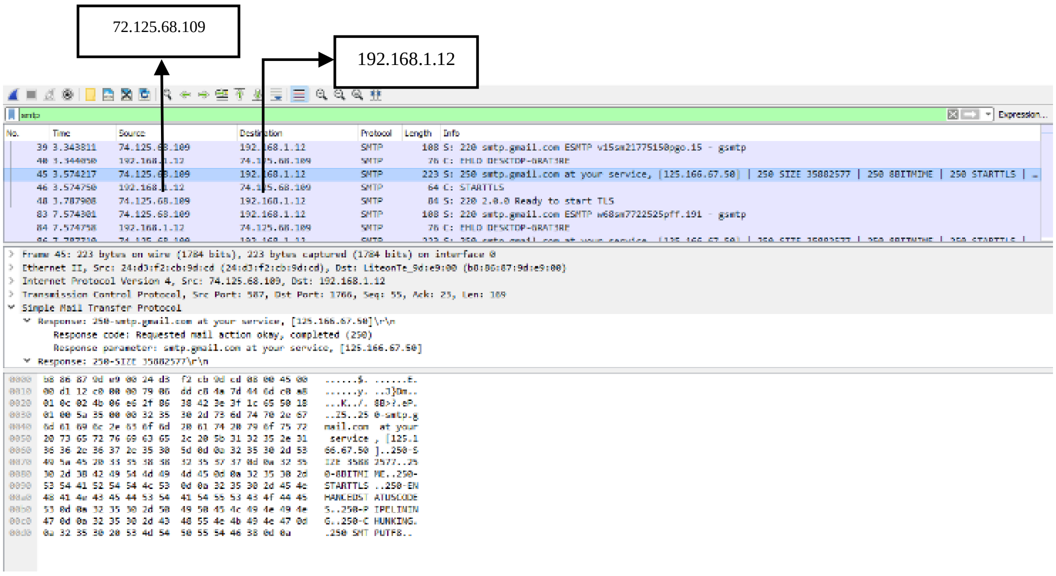
Addresses: fe80::45a7:e444:d4b2:fe31, fe80::45a7:e444:d4b2:fe31
No capture filter

You are running Wireshark 2.2.5 (v2.2.5-0-g440fd4d). You receive automatic updates.

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.



```
No.  Time      Source         Destination    Protocol Length Info
 39 3.343811  74.125.68.109  192.168.1.12   SMTP     108 S: 220 smtp.gmail.com ESMTP v15sm2177515Opgo.15 - gsmtp
 40 3.344050  192.168.1.12   74.125.68.109  SMTP      76 C: EHLO DESKTOP-GRAT3RE
 45 3.574217  74.125.68.109  192.168.1.12   SMTP     223 S: 250 smtp.gmail.com at your service, [125.166.67.50] | 250 SIZE 35882577 | 250 8BITMIME | 250 STARTTLS | …
 46 3.574750  192.168.1.12   74.125.68.109  SMTP      64 C: STARTTLS
 48 3.787908  74.125.68.109  192.168.1.12   SMTP      84 S: 220 2.0.0 Ready to start TLS
 83 7.574381  74.125.68.109  192.168.1.12   SMTP     108 S: 220 smtp.gmail.com ESMTP w68sm7722525pff.191 - gsmtp
 84 7.574758  192.168.1.12   74.125.68.109  SMTP      76 C: EHLO DESKTOP-GRAT3RE
 86 7.787310  74.125.68.109  192.168.1.12   SMTP     223 S: 250 smtp.gmail.com at your service, [125.166.67.50] | 250 SIZE 35882577 | 250 8BITMIME | 250 STARTTLS |
```

```
> Frame 45: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0
> Ethernet II, Src: 24:d3:f2:cb:9d:cd (24:d3:f2:cb:9d:cd), Dst: LiteonTe_9d:e9:00 (b0:86:87:9d:e9:00)
> Internet Protocol Version 4, Src: 74.125.68.109, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 587, Dst Port: 1766, Seq: 55, Ack: 23, Len: 169
v Simple Mail Transfer Protocol
  v Response: 250-smtp.gmail.com at your service, [125.166.67.50]\r\n
      Response code: Requested mail action okay, completed (250)
      Response parameter: smtp.gmail.com at your service, [125.166.67.50]
  v Response: 250-SIZE 35882577\r\n
```

```
0000  b0 86 87 9d e9 00 24 d3  f2 cb 9d cd 08 00 45 00   ......$. ......E.
0010  00 d1 12 c0 00 00 79 06  dd c8 4a 7d 44 6d c0 a8   ......y. ..J}Dm..
0020  01 0c 02 4b 06 e6 2f 86  38 42 3e 3f 1c 65 50 18   ...K../. 8B>?.eP.
0030  01 00 5a 35 00 00 32 35  30 2d 73 6d 74 70 2e 67   ..Z5..25 0-smtp.g
0040  6d 61 69 6c 2e 63 6f 6d  20 61 74 20 79 6f 75 72   mail.com  at your
0050  20 73 65 72 76 69 63 65  2c 20 5b 31 32 35 2e 31    service , [125.1
0060  36 36 2e 36 37 2e 35 30  5d 0d 0a 32 35 30 2d 53   66.67.50 ]..250-S
0070  49 5a 45 20 33 35 38 38  32 35 37 37 0d 0a 32 35   IZE 3588 2577..25
0080  30 2d 38 42 49 54 4d 49  4d 45 0d 0a 32 35 30 2d   0-8BITMI ME..250-
0090  53 54 41 52 54 54 4c 53  0d 0a 32 35 30 2d 45 4e   STARTTLS ..250-EN
00a0  48 41 4e 43 45 44 53 54  41 54 55 53 43 4f 44 45   HANCEDST ATUSCODE
00b0  53 0d 0a 32 35 30 2d 50  49 50 45 4c 49 4e 49 4e   S..250-P IPELININ
00c0  47 0d 0a 32 35 30 2d 43  48 55 4e 4b 49 4e 47 0d   G..250-C HUNKING.
00d0  0a 32 35 30 20 53 4d 54  50 55 54 46 38 0d 0a      .250 SMT PUTF8..
```

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.

Table 1. E-MAIL SPAMMING ANALYSIS RESULTS

No.	Evidence	
	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

[1] 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.