Email Forensic from Phishing Attack using Network Forensics Development Life Cycle Method

Zakiyaturrahma
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
Phishing is a technique used by attackers to steal email users' social media accounts by tricking the target into visiting a fake website that has a login form. Due to lack of awareness and insight in internet network education, users are very vulnerable to fall into the trap of attackers. A phishing email attack is a data manipulation activity that is visible in email headers. The purpose of this study is to assist email users in assessing email messages so as not to become victims of phishing attacks. The purpose of this study is to conduct forensics on phishing email attacks. NFDLC method is used to examine cybercrime digital forensic processes and create digital evidence. Wireshark and NetworkMiner programs are used to deduce the IP and IP address of the perpetrator. This research produces an analysis of phishing email attacks against fake login forms. The evidence obtained in the form of a wireshark data packet capture file that managed to capture the victim's IP address, the attacker's IP address, the sender's email, and the phishing website. The experimental results, it is proven that the Network Forensic Development Life Cycle method can analyze phishing email attacks detected on network traffic activity, with the results of data packet analysis carried out header comparison analysis.

Keywords
Forensics, Cybercrime, Email, Phishing, NFDLC.

1. INTRODUCTION
Phishing is a type of fraud in which an individual attempts to steal personal information, such as credit cards and passwords, by impersonating a reputable firm in an official electronic communication, such as an email or instant message[1]. Phishing, or the term 'fishing,' refers to the act of luring people into disclosing financial information and passwords[2].

The phishing criminal case involved the theft of many pieces of information, including account access, email, social media accounts, and even bank accounts[3]. Email is a tool of communicating via the internet[4]. Sending letters via email is a simple and quick process[5]. Emails can be created and sent using electronic devices such as computers or laptops, smartphones, or tablets that are connected to the internet[6].

The NFDLC method is used in the design process of this development system. The NFDLC method is a framework for analyzing phishing attacks[7]. The term cycle is a descriptive term for the development life cycle which includes all activities and stages related to phishing activity analysis[8]. The sender's IP address, specifically the entire email header, can be used to identify phishing email attacks[9].

The purpose of this study is to discuss email phishing attacks utilizing the Network Forensics Development Life Cycle (NFDLC) method, which is a process for investigating and planning illegal data theft strategies[10].

According to some of these study investigations, it is possible to determine phishing attacks on phishing emails by examining the header[11]. As a result, this study focuses on phishing email attacks by analyzing the sender's authenticity via the full email header[12].

2. STUDY LITERATURE
2.1. Email
Electronic Mail, or email, is a very popular and frequently used internet service that is used by many people, both within organizations and companies[13]. In its simplest form, e-mail is a method of sending, receiving, and storing messages via an electronic communication system, specifically the internet[14]. This definition explains that electronic mail is written, sent, and received electronically[15].

2.2. Email Abuse
Email can be a medium for criminals to steal personal data from users (victims).

2.2.1. Fraud Email
Fraud is a deliberate deception perpetrated over email for the perpetrator's personal gain or to cause harm to others[16]. The email's body contains an offer requiring low capital with a high profit margin or a sale of valued things at a discount price[17]. Spoofing and phishing are two types of email fraud.

1) *Email spoofing*, is e-mail falsification that is done by changing the contents of the fields in the e-mail header, so that it appears to come from a completely legitimate source[18].
2) *Email phishing*, is a form of email crime that aims to obtain personal data/information from email recipients. Phishing emails usually contain an inducement to the recipient to fill in personal details with details[19].
3) *Spread of phishing URLs*, phishing sites are fake sites that are almost identical to some social networking sites, email sites or online banking sites that require users to login[20].

2.2.2. Spamming
Spam emails are unsolicited emails sent in bulk and repeatedly to recipients. The majority of these spam emails are commercial in nature, however they can also include chain emails[21].

2.2.3. Bombing
Email bombing is a method of sending a huge volume of emails in an attempt to overflow the inbox or flood

the email server, resulting in a DoS (Denial of Service) attack[22].

2.3. Phishing

Phishing is a type of cybercrime that uses social engineering and technical deception to get the identities and passwords to financial accounts[23]. The social engineering plan is carried out through the use of forged emails claiming to be from legitimate commercial entities and is aimed to direct victims to fake websites, where they are duped into disclosing personal information such as email addresses and passwords[24].

3. METHOD

In email phishing research, the Network Forensics Development Life Cycle (NFDLC) method is one of continuous improvement, where the results of the study are taken into consideration in order to facilitate the collection of evidence during investigations [25]. The following describes the process of obtaining evidence using the NFDLC method, which can be seen in Figure 1.

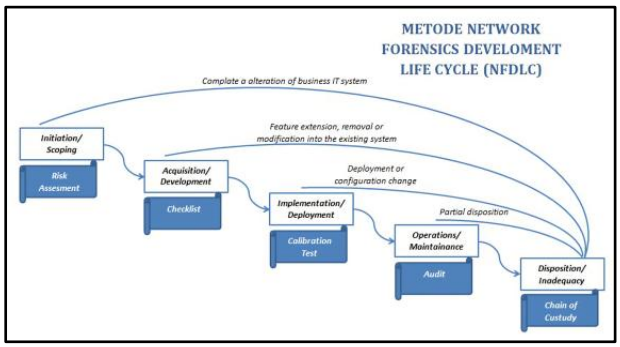

Figure 1 : Network Forensic Development Life Cycle Method

Figure 1 is the stages of the Network Forensics Development Life Cycle (NFDLC) method as follows:

1) *Initiation/Scoping*
   Determine network aspects for Digital Forensic Protection to be analyzed.
2) *Acquisition/Development*
   Contains evidence rules in systems developing, verifying, and calibrating.
3) *Implementation/Deployment*
   Basic testing of the platform by verifying the network mechanism.
4) *Operations/Maintainance*
   Includes verification and measurement of network usage.
5) *Disposition/Inadequacy*
   Perfoming a series of procedures to secure evidence.

3.1. Tahapan penelitian

The research stage is the stage of conducting case simulations for the analysis process on emails against phishing email attacks, which can be seen in Figure 2.

Figure 2 : Research Stages

Figure 2 there are several stages of research, which will be explained as follows:

1) The research problem is the first step taken to obtain and determine the research topic to be studied further. To carry out the analysis of the early stages of research, data collection was carried out. The case that will be carried out in the research is on email against phishing attacks.
2) Research review is the process of finding all information related to the problem to be studied and providing the basis for the direction of the research to be carried out.
3) The case study is the process of applying the Network Forensick Development Life Cycle method, this research analyzes email forensics against phishing email attacks.
4) The conclusion is the result of the research which is analyzed in the form of evidence.

4. RESULT AND DISCUSSION

4.1. Initiation

4.1.1. System Requirements Analysis

The study examined emails that were subjected to phishing email attacks. At the initiation/scoping stage, email analysis of phishing emails is accomplished by needs analysis and system identification; at the needs analysis stage, how to analyze is accomplished using email header analysis and tracking with wireshark and Networkminer. There are two components to system identification: software devices such as operating systems and application software such as wireshark and networkminer, and hardware devices such as desktops or laptops can be seen in Table 1.

Table 1. Software Requirements

Needs	Description
Email	Get email messages
Header Email	Get email details
Email Tracking	Header analysis tool
Wireshark	Network monitoring
Networkminer	Analysis

4.2. Acquisition

4.2.1. Sending phishing emails

The attack carried out is the email object by sending email using Gmail. Perpetrators send phishing emails using Gmail. Perpetrators carry out phishing attacks by attaching the URL address of the website login form. Gmail is used for the purpose of sending emails that are not considered as spam, it can be seen in Figure 3.

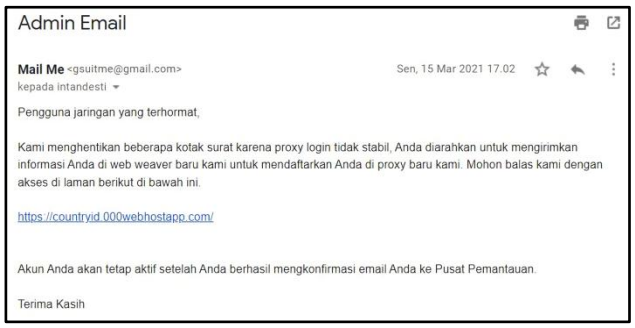

Figure 3 : Contents of Phishing Emails

Figure 3 the creation of an email using Gmail. Perpetrators carry out phishing attacks by attaching the URL address of the website login form. After the message is successfully sent, the perpetrator waits for the victim to enter a phishing trap.

4.2.2. Display the Account Verification Form

Perpetrators carry out phishing attacks by attaching a website URL address in an email. The perpetrator makes a website that

looks the same as the account verification form page in general using the PHP programming language which can be seen in Figure 4.

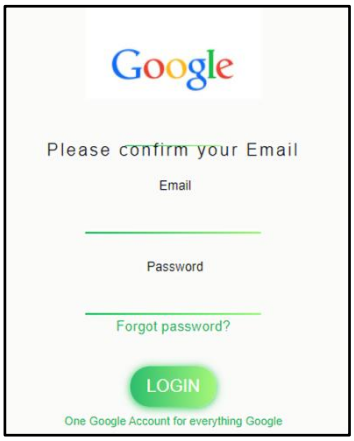

Figure 4 : Verification Page

Figure 4 is a fake login form page created by attackers to lure victims into a phishing trap. on this form page shows that digital evidence involves misuse of emails in the form of phishing URLs.

4.3. Implementation

4.3.1. Phishing Email Investigation Scenario

Email analysis is done by looking at the email header, so to find out the route of the phishing email sender, the first step is to make an email analysis design, which is to make a flowchart of the phishing email investigation scenario, which can be seen in Figure 5.

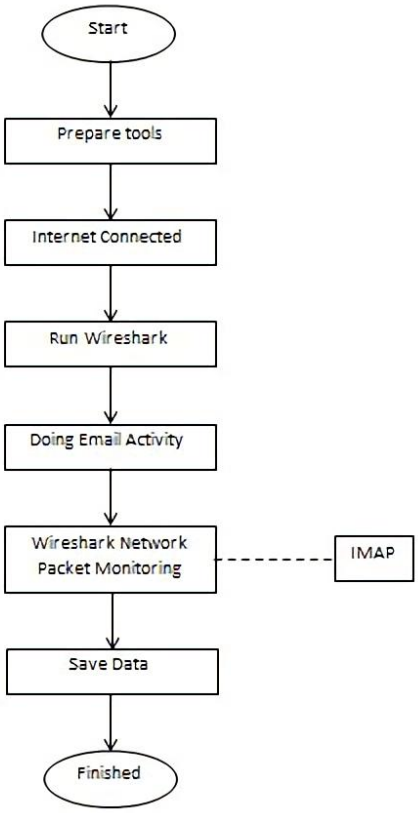

Figure 5 : Flowchart Skenario Investigasi Email Phising

Figure 5 is a scenario of investigating evidence against an email. This scenario explains that the search for evidence is carried out by users by utilizing the internet network to track evidence. Users use the searching application provided by the internet to connect in email. Next, the user performs an analysis using the Wireshark and NetworkMiner applications. In analyzing the received email using the IMAP protocol, then the email will be recorded on Wireshark and will be analyzed on NetworkMiner. Data packets received by email are evidence of the IP address of the sender.

4.3.2. Phishing Email Attack Simulation

Identification of how email phishing works by simulating email phishing attacks using email sending techniques via the internet and creating fake websites using web hosting can be seen in Figure 6.

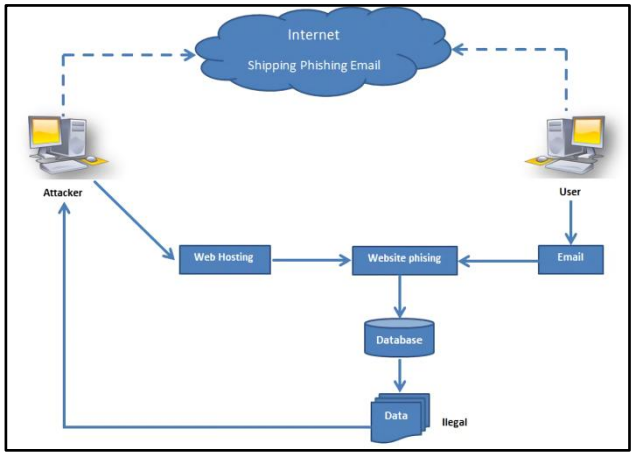

Figure 6 : Phishing Email Attack Simulation

Figure 6 simulation flowchart describes an attack using email phishing techniques, the phishing perpetrator performs a phishing email to verify his email account on the website page created by the perpetrator using hosting then the victim's verification data will be stored in the perpetrator's database.

4.4. Operations

1) Receiving Phishing Emails

Perpetrators carry out phishing emails by tricking the recipient into an official account by using a familiar subject as seen as trustworthy, as can be seen in Figure 7.

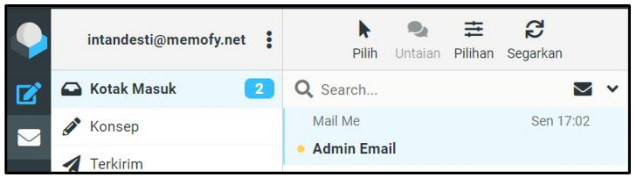

Figure 7 : Email Inbox

Figure 7 is a display in the email inbox that the phishing email was successfully entered and received by the victim, it is clear that the sender came from the user “Mail Me” with the Subject 'Email Admin' with the aim of tricking the recipient into believing that 'Email Admin' is an official account from Gmail.

2) Phishing Emails

Phishing emails that are not considered spam have successfully entered the message inbox, phishing emails ask the recipient to verify their email account at the URL address, phishing emails can be seen in Figure 8.

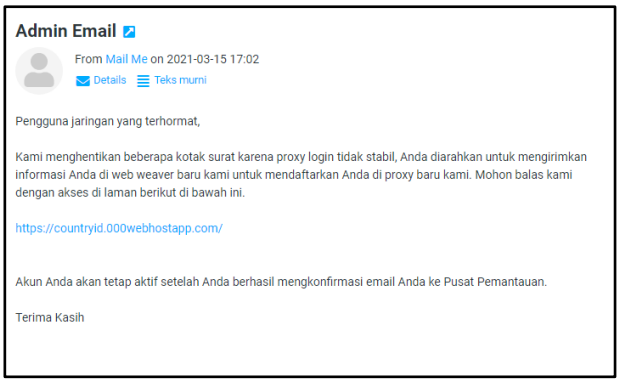

Figure 8 : Contents of Email

Figure 8 contains a fake message with the Subject "Admin Email". The message asks the user to verify the email account by opening the URL address and filling out the form on the prepared website page. The email received is an action that leads to phishing activity.

3) Phishing Email Attack Proof Simulation

Users can track the source of the received email by looking at the header of the email addressed can be seen in Figure 9.

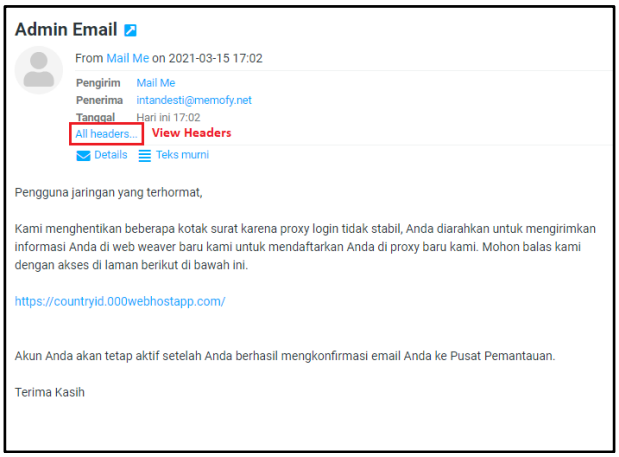

Figure 9 : Viewing Email Header

Figure 9 explains that email headers can be viewed by displaying "All headers" in the inbox. This study analyzes email attacks against phishing emails by analyzing email headers located in the application and email headers can be analyzed using header tracking tools, wireshark and networkminer.

The results obtained from the email header contain received information, namely the email sender and email recipient, the sender's IP address and the time of receiving the email can be seen in Figure 10.

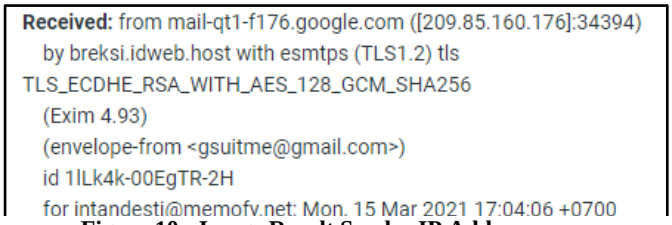

Figure 10 : Image Result Sender IP Address

Figure 10 in the email header contains information that the email comes from the IP address 209.85.160.176, and the sender's address is gsuitme@gmail.com. Email sent via breksi.idweb.host server on Monday, 15 March 2021 17:04.

4) Header Analysis Tool

The header analysis is carried out focusing on the translation of the Received field, so that it answers the questions what, who, when, how shown in Figure 11 and Figure 12.

Figure 11 answers the question what, namely the subject of the email is Admin Email, answers the question when is Mon, 15 Mar 2021 17:02:45, answers the question who is the sender of the email gsuitme@gmail.com and the recipient of intandesti@memofy.net.

Figure 12 answers the question how, namely the process of sending and receiving email, namely hops starting from Hop1: mail-qt-f176.gogle.com, Hop2: breksi.idweb.host, Hop3: breksi.idweb.host.

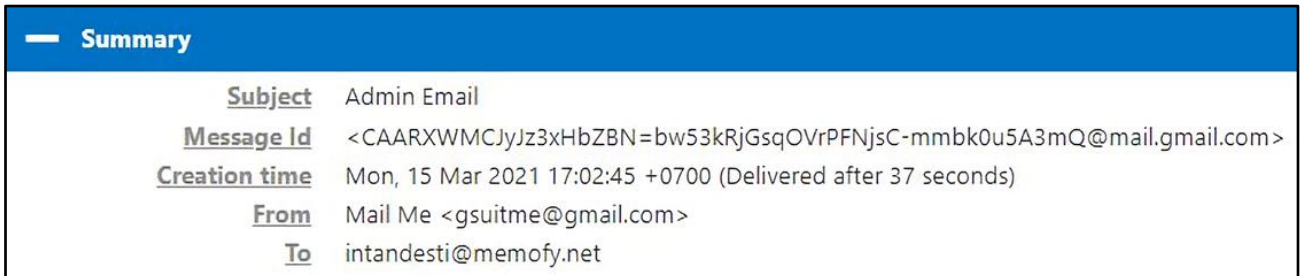

Figure 11 : Email Analysis Tool

Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1		mail-qt1-f176.google.com	3/15/2021 5:03:29 PM		SMTP
2	mail-qt1-f176.google.com ([209.85.160.176]:34394)	breksi.idweb.host	3/15/2021 5:04:06 PM	37 seconds	esmtps (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (Exim 4.93) (envelope-from <gsuitme@gmail.com>)
3	breksi.idweb.host	breksi.idweb.host	3/15/2021 5:04:06 PM	0 seconds	LMTP

Figure 12 : Email Tracking Tool Analysis Result

5) Wireshark

The process of reading the IMAP server email is done to capture email data packets on wireshark. The results of IMAP data packet capture onwireshark are shown in Figure 13.

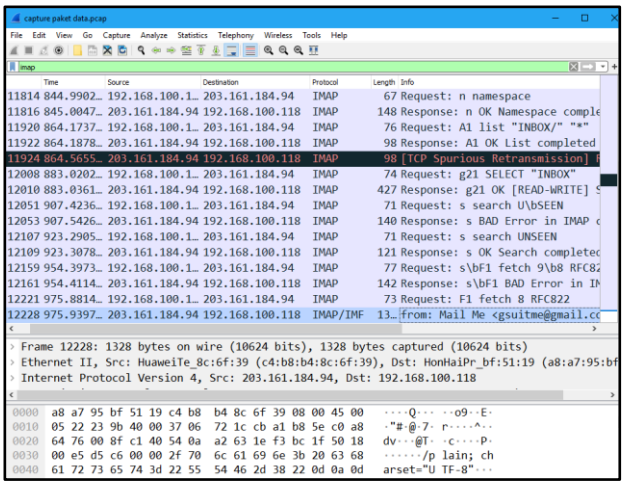

Figure 13 : Wireshark Data Packet Capture

Figure 13 shows the results of data packet retrieval from network traffic captured using wireshark, the results of following TCP Stream can be seen in Figure 14.

Figure 14 shows the results of data packet capture on wireshark which contains information in the form of e-mails received with IP address 203.161.184.94, on Follow TCP Stream result there is information that there is spam software running on the breksi.id.web.host system, then the results of the analysis of the wireshark data packets are analyzed using networkminer.

6) NetworkMiner

Based on the Follow TCP Stream analysis results obtained from the wireshark monitoring results, the PCAP file analysis of wireshark data packets was extracted using NetworkMiner shown in Figure 15.

Figure 15 shows a PCAP file that was successfully extracted on networkminer. The results obtained from monitoring wireshark data packets are analyzed. The email information retrieved by the network displays information from the analysis header, which can be seen in Figure 16.

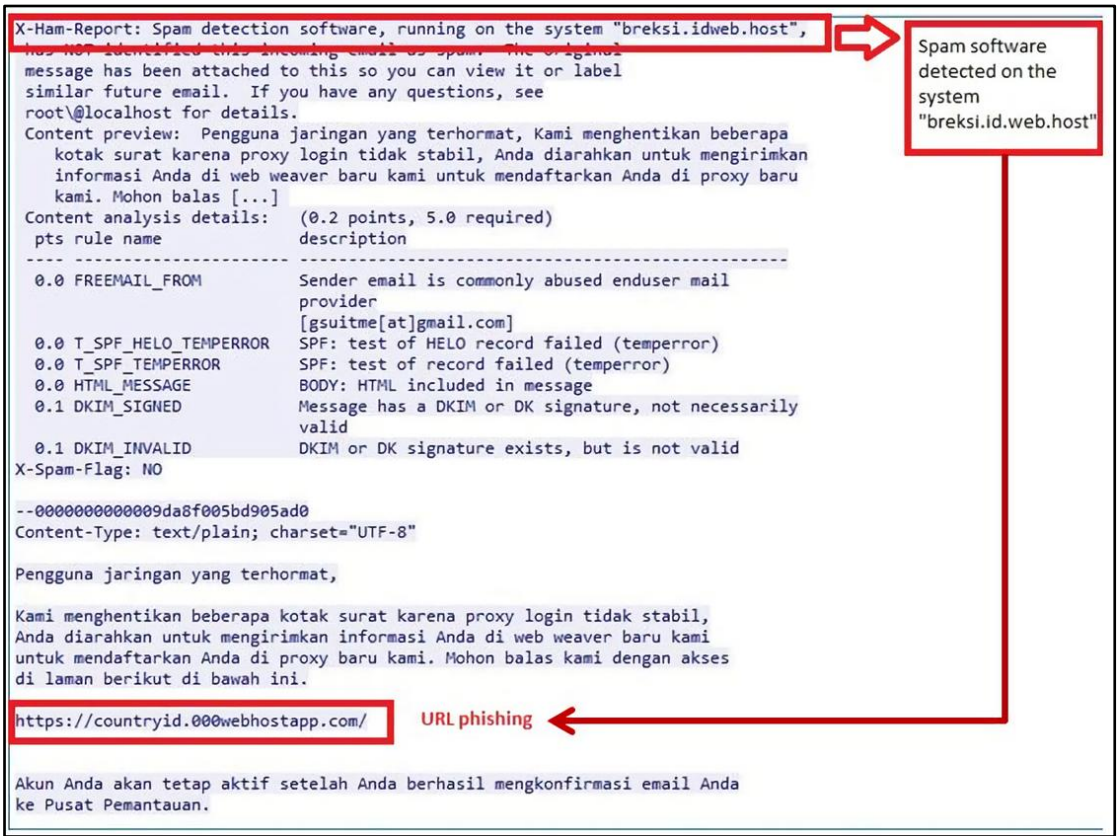

Figure 14 : PCAP File Data Package

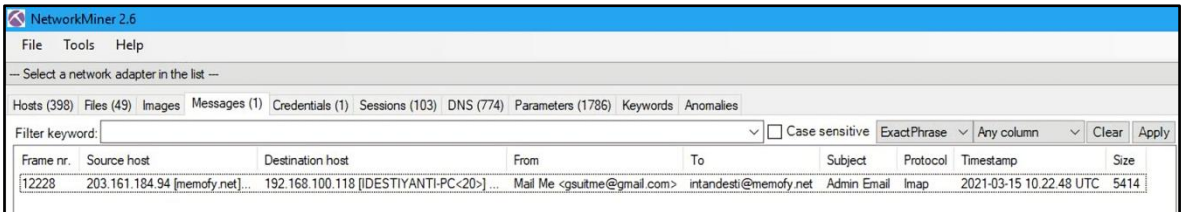

Figure 15 : Extract PCAP with NetworkMiner

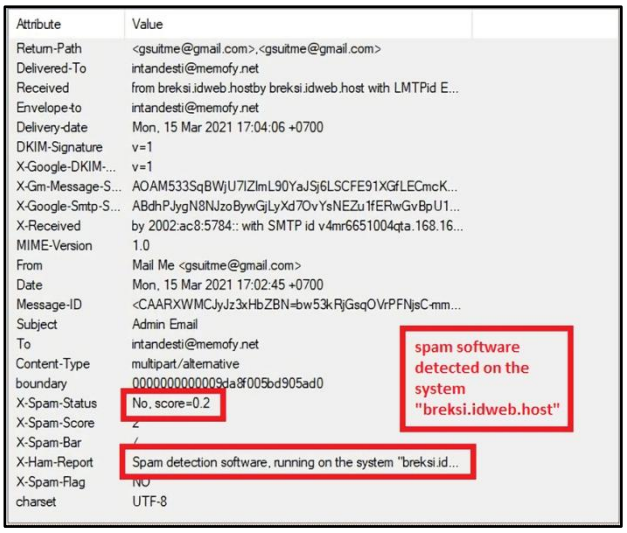

Figure 16 : Extract PCAP with NetworkMiner

Figure 16 shows that the results of the analysis using Networkminer produce detailed email information, the results of Networkminer's analysis based on extracts from the Follow TCP Stream can be seen that there is spam software running on the breksi.id.web.host system.

4.5. Disposition

The results of the discussion in the search, collection, and documentation of digital evidence obtained during the investigation of phishing emails show that by analyzing email headers on header tracking tools and analyzing emails sent over the network using wireshark and networkminer, it is possible to obtain evidence in the form of detailed information on the existence of phishing emails.

Table 2. Header Comparison Analysis Results

Field		Results
Who	Who is the Email Sender?	"Mail Me" <gsuitme@gmail.com>
	Who is the Email Sender?	<intandesti@memofy.net>
What	What is the subject of the email?	Admin Email
	What is the Attachment file on the email?	https://countryid.000webhostapp.com/
When	When is the email sent?	Mon, 15/03/2021 17.02.45 +0700
	When was the email received?	Mon, 15/03/2021 17.04.06 +0700
Where	Where is the Email Sender's server IP Address?	IP Address source : 203. 161.184.94 IP Address Destination : 192.168.100.118
	Where is the location?	Country : Unitad States
How	How is the process of sending Email from sender to recipient?	Hop1 : mail-qt-f176.gogle.com Hop2 : breksi.idweb.host Hop3 : breksi.idweb.host

Table 1 the results of the evidence obtained from email analysis using a header analysis tracking tool and wireshark and networkminer applications can be grouped into a 4W1H concept map.

5. CONCLUSION

Based on the results of email phishing research using the Network Forensics Development Life Cycle method, network forensics applications to obtain evidence against phishing email attacks, namely email tracking tools can obtain evidence by conducting header analysis, wireshark is able to capture network data packets and monitor the process of reading email and networkminer can used to analyze emails based on evidence obtained from wireshark. Phishing emails recorded on the wireshark network are evidence obtained in the form of the victim's IP address, the perpetrator's IP address, the perpetrator's phishing email, the phishing URL and information about spam software. Phishing email attacks are recorded on network traffic, the results of the data packet analysis are carried out by header comparison analysis.

6. REFERENCES

[1] Ahmad, M. S., Riadi, I. and Prayudi, Y. (2017) 'Live Forensic Investigation from the User Side to Analyze Man in The Middle Attack', 9(April), Pp. 1–8.

[2] Efendy, Z., Putra, I. E. and Saputra, R. (2019) 'Asset Rental Information System and Web-Based Facilities at Andalas University', Journal of Applied Information Technology, 2(2), Pp. 47–58. Doi: 10.21460/Jutei.2018.22.103.

[3] Karsono, K. (2012) 'Forensic E-Mail', 9.

[4] Faiz, M. and Cilacap, P. N. (2017) 'Live Forensics Analysis for Comparisonal Email Security', (April). Doi: 10.33096/Ilkom.V8i3.79.242-247.

[5] Mia Haryati Wibowo, N. F. (2017) 'The Threat of Phishing to Social Media Users in Cyber Crime', 1, Pp. 1–5.

[6] Faiz, M. N., Umar, R. and Yudhana, A. (2016) 'Analysis of Live Forensics for Comparison of Email Security in Proprietary Operating Systems', Ilkom Scientific Journal, 8(3), P. 242. Doi:10.33096/Ilkom.V8i3.79.242-247.

[7] Hidayat, M. R. (2021) 'Investigation of Botnet Attacks using Network Forensic Development Life Cycle Method', 183(25), Pp. 30–36.

[8] Hanipah, R. (2020) 'Wireshark', 4(1), Pp. 11–23.

[9] Hadianto, T., Prasetyo, W. and Bahaweres, R. B. (2017) 'Comparative Study of Email Forensic Tools', 10(1), Pp. 53–61.

[10] Ginanjar, A., Widiyasono, N. and Gunawan, R. (2018) 'Analysis of Web Phishing Attacks on E-commerce Services with the Network Forensic Process Method', (2), pp. 147–157. doi: 10.21460/jutei.2018.22.103.

[11] Radiansyah, I. and Priyadi, Y. (2016) 'Analysis of Internal Phishing Threats', 7(1).

[12] Fatimah, M. H. W. and N. (2017) 'The Threat of Phishing to Social Media Users in the World of Cyber Crime', Joeict (Journal of Education and Information Communication Technology), 1, Pp. 1–5. Doi:10.29100/.V1i1.69.

[13] Ardhi, N. H. (2020) Geolocation Tracking in Forensic Email Integrated with Twitter Geo-Social Network.

[14] Andrian Maftuh Nadzifan, F. N. (2018) 'Application to Detect Spoof in Email 268', 7(September), Pp. 268–272.

[15] Purwiantono, F. E. K. A. Et Al. (2017) 'Classification Model for Detection of Phising Sites in Indonesia'.

[16] Mandowen, S. A. (2016) 'Forensic Analysis of Computers on Network Traffic 1', 16, Pp. 14–20.

[17] Hamid (2017) 'Analysis of Security of Android and Gmail Default Email Applications on Wireless Networks', 23, Pp. 125–136.

[18] Kurniawan, A. (2019) 'Application of Owasp Framework and Network Forensics for Analysis, Detection, and Prevention of Injection Attacks on the Host-Based Side', 14(1), Pp. 9–18.

[19] Umar, R., Riadi, I. and Muthohirin, B. F. (2018) 'Acquisition of Email Service Based Android using Nist', 3(3), Pp. 263–270.

[20] Nofiyan, A. (2020) 'Forensic Analysis on Web Phishing using National Institute of Standards and Technology (NIST) Method', 8(2), Pp. 11–23.

[21] Suryana, A. L., Akbar, R. El and Widiyasono, N. (2016) 'Investigation of Email Spoofing with the Digital Forensics Research Workshop (Dfrws) Method', Journal Of Informatics Education and Research (Jepin), 2(2), Pp. 111–117. Doi:10.26418/Jp.V2i2.16821.

[22] Susanto, B. M. Et Al. (2016) 'Identification of Phising Websites with Attribute-Based Selection', 2016(Sentika), Pp. 18–19.

[23] Hoiriyah, Sugiantro, B., Prayudi, P. (2016) 'Forensic Investigation of Email Spofing using the Header Analysis Method', 17.

[24] Sah, A. Et Al. (2018) 'Digital Evidence Detection Online Gambling using Live Abstract', 1(1), Pp. 14–19.

[25] Yudho, O. and Pranolo, A. (2018) 'Email Address Crawler Agent using the Breadth-First Crawling Method', 6(1), Pp. 9–17.