Digital Forensics to Prove Authenticity and Detect Malware in Email Sent on the Directorate of Innovation and Business Incubator

Rahmat Novrianda Dasmen*[1], Muhammad Dimas Putra[2], Rasmila[3]
Universitas Bina Darma, Jl. Jenderal Ahmad Yani No. 3, 9/10 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30111, Indonesia
*E-mail : rahmat_novrianda@binadarma.ac.id (Orcid-id 0000-0001-7348-5377) *[1], muhammaddimas090704@gmail.com[2], rasmila@binadarma.ac.id (Orcid-id 0000-0003-1789-8171)[3]*
**Corresponding author*
Received 17 September 2025; Revised 23 October 2025; Accepted 4 November 2025

Abstract - The Directorate of Innovation and Business Incubator (DIIB) at Bina Darma University often receives emails from external sources, increasing the risk of phishing, spoofing, and malware threats. This study applies the Digital Forensic Research Workshop (DFRWS) framework comprising Identification, Preservation, Collection, Examination, Analysis, and Presentation to analyze suspicious emails using forensic tools such as MXToolbox, Whois Lookup, Talos Intelligence, Sucuri SiteCheck, and VirusTotal. Ten suspicious emails were examined. Most failed one or more authentication checks (SPF, DKIM, DMARC), indicating weak verification and potential spoofing. Domain and IP analyses showed public domains like Gmail and Yahoo were most exploited, while official domains such as *Upj.ac.id* and *Maranatha.ac.id* had moderate risk. Sucuri classified most domains as medium to high risk, and VirusTotal found no active malware. The study concludes that phishing and spoofing pose greater threats than direct malware, highlighting the importance of forensic email analysis to enhance cybersecurity awareness at DIIB.

Keywords – DIIB, Email, DFRWS, Malware, Tools

1. INTRODUCTION

DIIB has an official email that is used to transfer information both internally, Universitas Bina Darma and external DIIB partners [1] . As part of its operational infrastructure, DIIB relies on email, which is fundamentally based on the Simple Mail Transfer Protocol (SMTP), an internet system that enables organizations to exchange electronic messages efficiently [2]. An email comprises two essential components: the header and the body. For DIIB, the header serves a critical role in providing sender identification, routing information, and timestamps necessary for verifying message authenticity, while the body contains the core information or content to be communicated to recipients [3].

Email has both advantages and disadvantages on the one hand, cybercriminals utilize email as a means to do harm. However, the complex process of sending data provides assurance that the data sent can be checked, although email forgery that harms a particular party can occur. According to the Anti Phishing Working Group (APWG) in April 2024 released data that 963.994 phising attacks occurred, which occurred in the first quarter of 2024 [4].

The increasing number of spam emails in Indonesia, which ranks the country eighth in the world, indicates that spam is now not just an annoying promotional message, but has also evolved into one of the main channels for malware distribution, phishing, and sensitive data harvesting. In this situation, email serves as a critical element in the cybersecurity system and requires special focus in the effort to address digital threats [5]. Anomaly detection in email using machine learning and header information reveals that information from email headers alone is

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

sufficient to effectively detect anomalies such as spam and phishing without the need to analyze the message content. This shows that header-based analysis has advantages in terms of speed, resource efficiency, and reliability [6][7].

This research aims to design a digital forensics approach to identify the identity, authenticity, and possible malware of suspicious emails [8]. The first step is to collect suspicious emails and then analyze them using forensic tools such as MXToolbox, Whois Lookup, Talos Intelligence, Sucuri, and VirusTotal. The main objective of this method is to provide a scalable, systematic solution for email investigation, especially to trace the sender's origin, verify the email's authenticity, and identify threats hidden in the content or attachments. The research findings are expected to produce applicable technical guidelines for academics, cybersecurity practitioners, as well as general users in countering email-based threats such as spoofing, phishing, and malware [9].

Prior research, such as the study by Riadi et al, focused on detecting email spoofing by analyzing header anomalies, while Bachri and Gunawan emphasized the growing threat of spam emails as a medium for malware distribution. Although both studies recognize email as a crucial vector in cybercrime, their approaches are primarily limited to identifying suspicious elements or classifying email threats through surface-level data. In contrast, this study offers a more holistic and forensic-driven investigation by applying the DFRWS methodology. It not only examines email headers, but also validates domain integrity, inspects metadata, and evaluates email attachments using a combination of tools: MXToolbox, Whois Lookup, Talos Intelligence, Sucuri, and VirusTotal. This integrated approach allows for a deeper analysis, even in cases where malware is not directly detected, making it more comprehensive than previous research in identifying hidden threats within email communications.

Email is one of the sources of digital evidence that is often used by criminals, both as a means of communication for the perpetrator, a place to store data, and as a tool for committing fraudulent acts such as phishing and spoofing [7]. Riadi, Sunardi, and Tella, in their study, highlighted a significant problem regarding the increase in digital crimes committed through email media, especially email spoofing techniques. Email spoofing is a method of falsifying information in the email header section, where the perpetrator changes the sender's address to make it look like it comes from a trusted source. The aim is to persuade the recipient to trust the message's content and take potentially harmful actions, such as clicking phishing links or opening malicious attachments. In the study, the authors noted that email headers play a crucial role in determining the authenticity of an email. Data such as the sender's IP address, domain name, Message-ID, and delivery path (Received) can be strong evidence to identify the presence of a non-genuine email [3]. Bachri and Gunawan, in their research, highlighted the phenomenon of the increasing number of spam emails in Indonesia, which has ranked the country eighth in the world in spam delivery. They emphasized that spam is no longer just an annoying promotional message but has become one of the main channels for spreading malware, phishing, and the theft of sensitive information. In this context, email is not only a means of communication, but also one of the crucial cybersecurity hotspots [5].

2. RESEARCH METHOD

This research utilizes the DFRWS (Digital Forensic Research Workshop) investigation model to ensure that each stage of handling digital evidence is conducted in a forensically appropriate and systematic manner [10]. DFRWS is a standardized and consistent forensic framework, making it easy to implement and well understood by users from both technical and non-technical backgrounds [11]. Digital Forensic Research Workshop (DFRWS). This model is designed to offer a structured approach to the digital evidence investigation process, dividing the steps into six main phases: Identification, Preservation, Collection, Examination, Analysis, and Presentation. Each phase is designed to ensure the integrity and validity of the digital data under investigation is maintained, from the digital identification process, evidence collection, to the

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

presentation of the result in the form of a report. In this research, the DFRWS (Digital Forensic Research Workshop) model is applied to investigate email senders, test the authenticity of messages, and analyze potential malware using various forensic tools. Through this method, every investigation activity can be recorded in a structured manner and accounted for both technically and scientifically [12][13]. The DFRWS (Digital Forensic Research Workshop) framework is recognized as one of the leading frameworks in digital forensics as it offers the most comprehensive steps to support the entire investigation process. The DFRWS (Digital Forensic Research Workshop) consists of five main subprocesses within the overall field of digital forensics, making it a complete and significant framework for building a digital crime case construction [14][15].

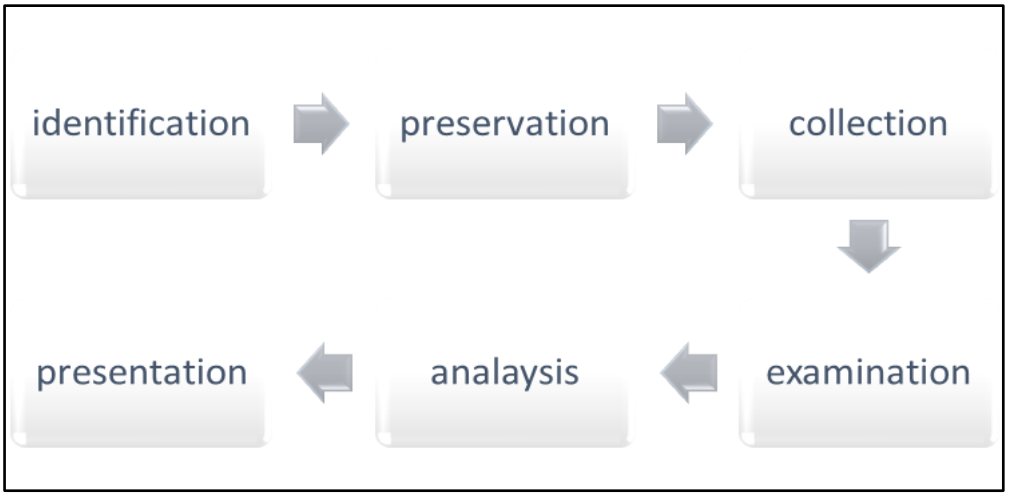

Figure 1. Research Methodology

The following is an explanation of the stages carried out in this test:

a) Identification
Determine the data source or relevant digital evidence, Identify incoming emails that indicate suspicious (phishing, spoofing, malware). Email subjects, sender addresses, attachments, and links that are unusual become the initial focus.

b) Preservation
Maintain data integrity so as not to changed/contaminated, save the original copy of (.eml or .msg) to prevent changes

c) Collection
Retrieve the required data from the source evidence, collecting email headers, sender's IP address, DNS information, attachments, and links contained in the email. Documenting results from tools such as MXToolbox, Talos, Sucuri, and Virustotal.

d) Examination
In the Examination stage, the process is carried out after the digital evidence has been collected. The main goal is to filter data from certain parts of the digital evidence source, at this stage researchers extract information from email headers (IP, SPF / DKIM / DMARC), Using MXToolbox to see the reputation of domains & IP.

e) Analysis
The next stage in the digital forensics process is Analysis. At this stage, the digital evidence that has been obtained and examined is then validated to ensure its authenticity. Researchers compile the results of the examination to find patterns of attacks or violations, and determine whether the email is fake or contains malware.

f) Presentation
Delivering the results of the investigation in a systematic and understandable manner, compiling a report on the results of the examination, suspicious emails complete with

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

screenshots, ip reputation charts, and malware scan results. Provide conclusions on whether the email is safe, dangerous, or comes from an unauthorized source.

2.1. Data Collection

In this research, data collection was conducted using a digital forensic approach based on the Digital Forensic Research Workshop (DFRWS) framework [16]. The main data source came from suspicious incoming emails received by the Direktorat Inovasi dan Inkubator Bisnis (DIIB) of Universitas Bina Darma. The data were collected in a structured manner through observation, documentation, and tool-based technical extraction, ensuring each artifact could be analyzed for authenticity and potential threat indicators [17].

The steps taken in this phase include:

a) email Identification: Collecting emails classified as spam or suspicious by the email system (e.g., Gmail), focusing on characteristics such as unusual subject lines, unknown senders, or external file attachments .
b) Header Extraction: Each selected email was opened through the “Show Original” feature to obtain full header details, including SPF, DKIM, DMARC status, IP address paths, and routing data.
c) Attachment and Link Collection: PDF files or URLs embedded in the email body were extracted for further static and dynamic malware analysis using VirusTotal and Sucuri SiteCheck.
d) Domain and IP Investigation: Sender email domains and source IPs were gathered to be traced through Whois Lookup and Talos Intelligence, aiming to validate ownership and assess sender reputation.

The collected artifacts were organized into structured documentation to ensure the forensic chain of custody and prepare them for further examination stages. This method allows for repeatable and accountable analysis, aligning with forensic best practices

3. RESULTS AND DISCUSSION

The Directorate of Innovation and Business Incubator (DIIB) is an innovation development center that actively receives various email correspondence daily. Among the many emails received, several were suspicious and required further analysis to confirm the sender's identity, the authenticity of the content, and the potential presence of malware.

However, not all of these incoming emails are legitimate. Among the numerous correspondences received, several appeared suspicious and required further investigation. Suspicious indicators may include unusual sender addresses, inconsistencies in message formatting, unexpected attachments, or external domain sources that do not match the sender’s claimed organization. Such characteristics raise concerns regarding the authenticity of the sender, the reliability of the content, and the potential presence of malicious elements such as phishing links or malware attachments. The following are some of the emails received:

a) The first email was sent from Gmail with the title online training on the role and fuction of good university governance

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

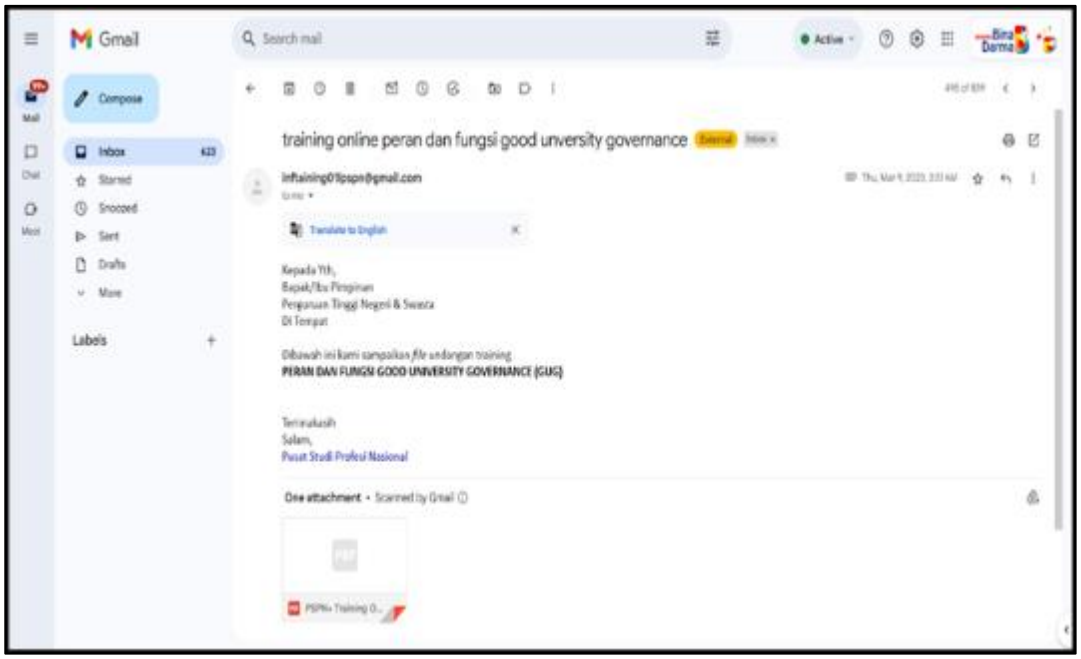

Figure 2. 1st.Email view on DIIB incoming email

b) Second email was sent from Gmail with the title the latest pph tax calculation training related to hpp law

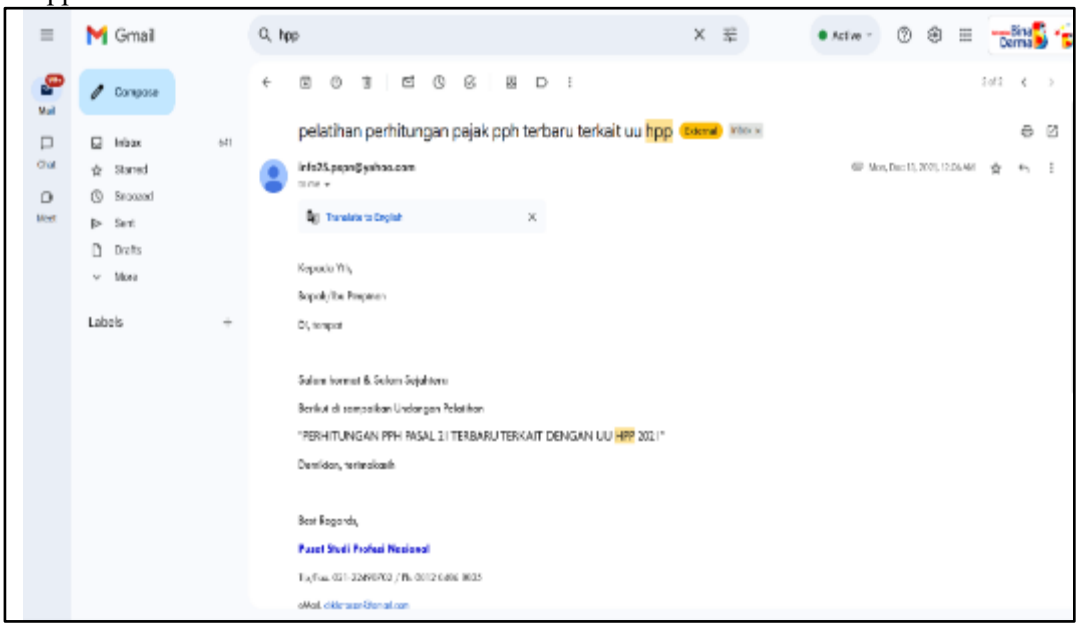

Figure 3. 2nd Email view on DIIB incoming email

c) A third email was sent with the title action required: Critical vulnerability in WooCommerce

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

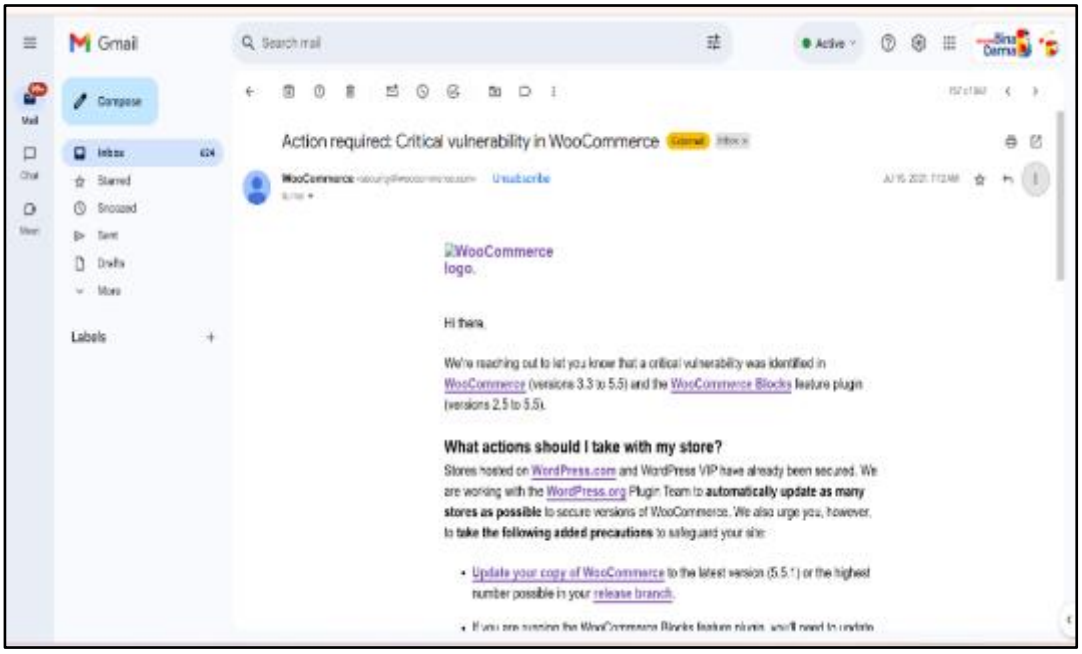

Figure 4. 3rd Email view on DIIB incoming email

d) A fourth email was sent with the title "webinar pelatihan secretary development program."

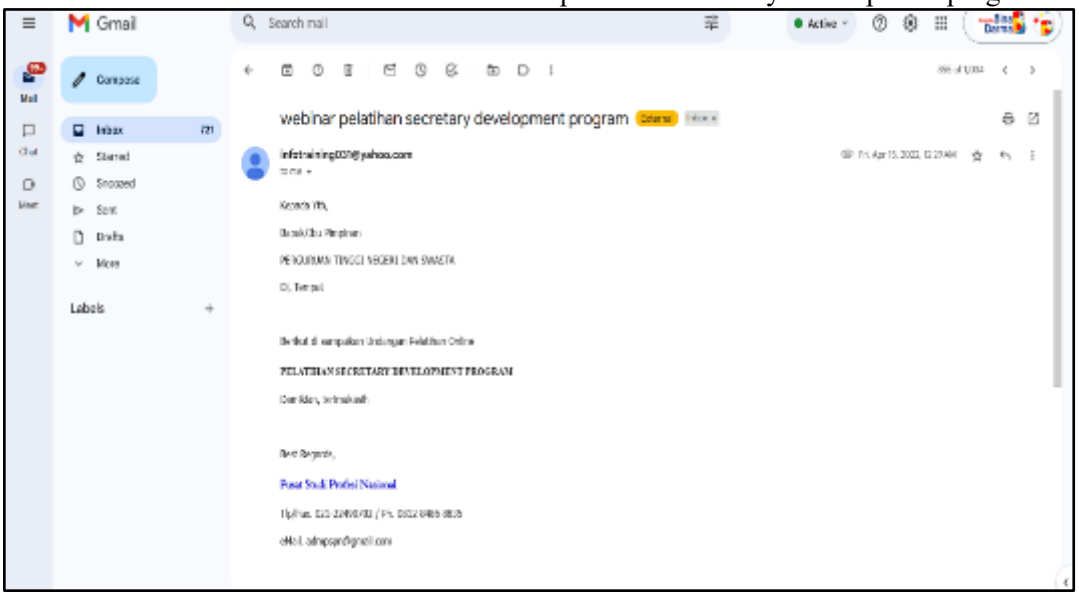

Figure 5. *4th* Email view on DIIB incoming email

e) A fifth email was sent with the title "undangan pelatihan kehumasan perguruan tinggi."

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

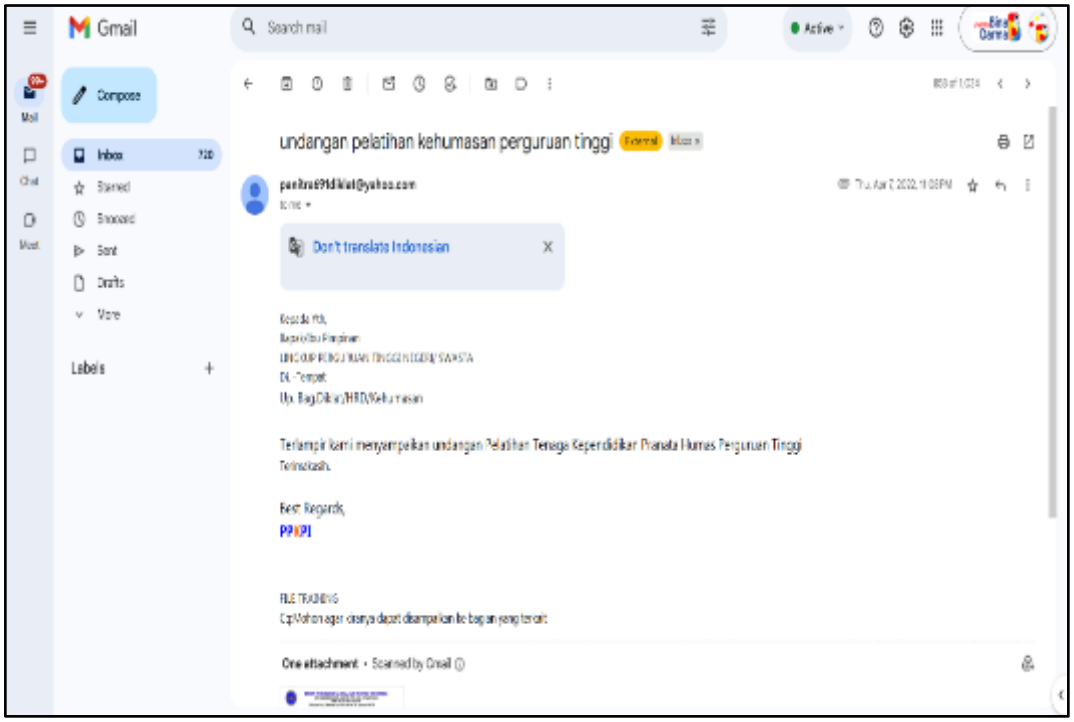

Figure 6. 5th Email view on DIIB incoming email

f) A sixth email was sent with the title "undangan pelatihan kehumasan perguruan tinggi".

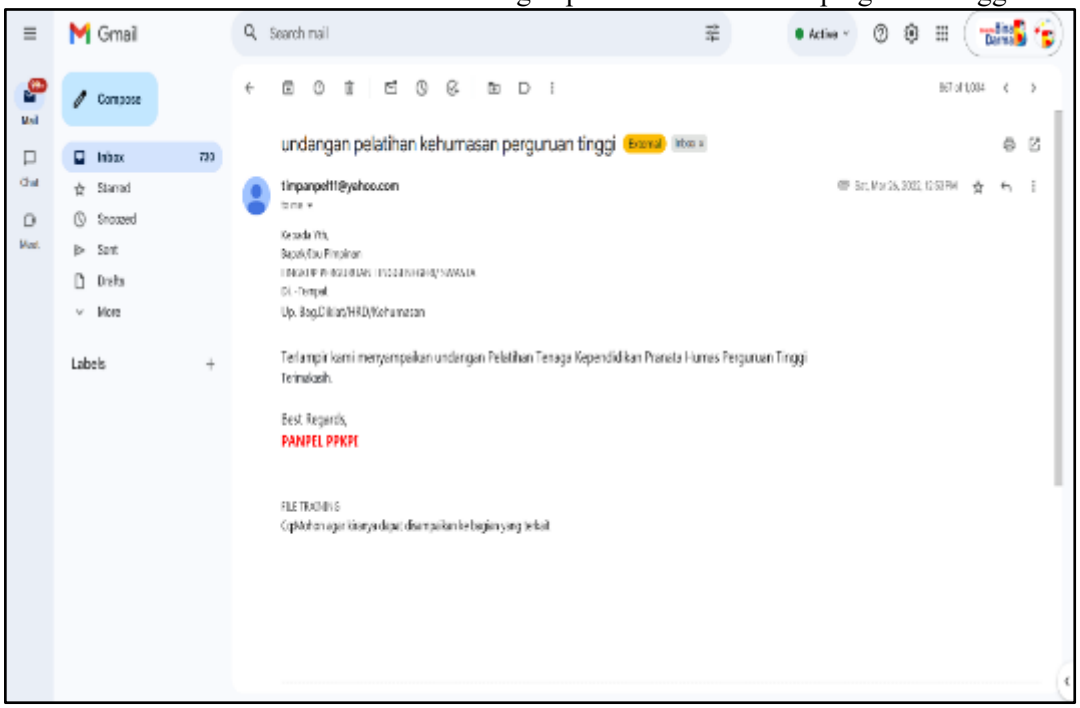

Figure 7. 6th Email view on DIIB incoming email

g) A seventh email was sent with the title "Fwd: Training Sertifikasi Auditor Internal ISO 31001 : 2018 (2021)."

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

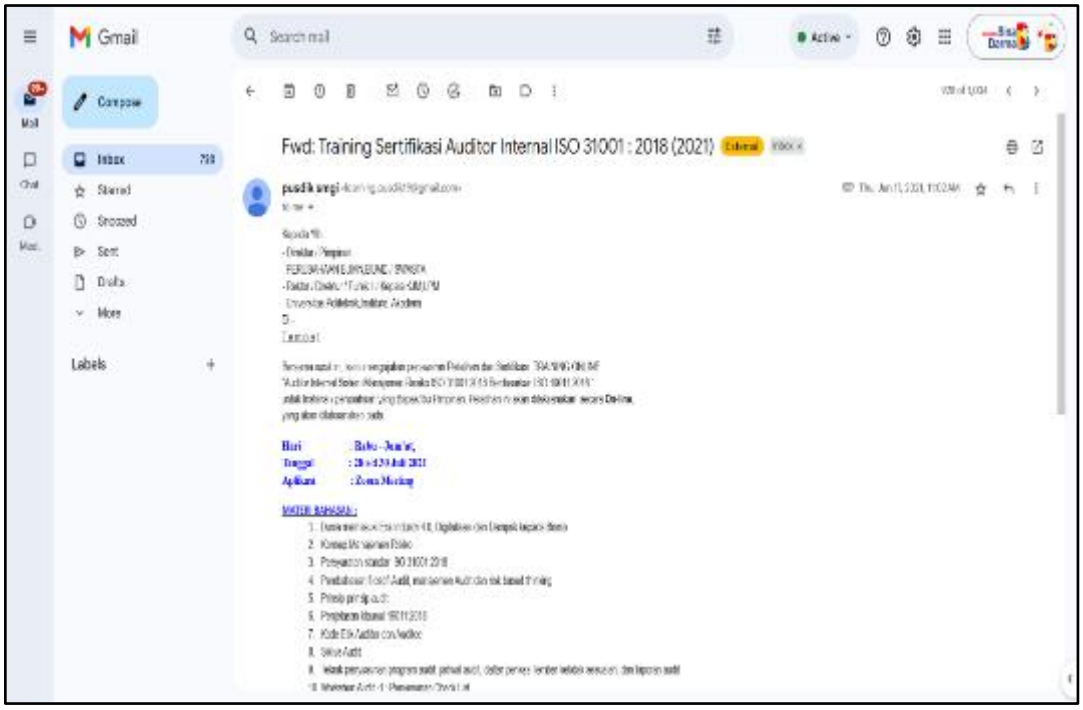

Figure 8. 7th Email view on DIIB incoming email

h) An eighth email was sent with the title "Pelatihan Kompetensi TU Perguruan Tinggi."

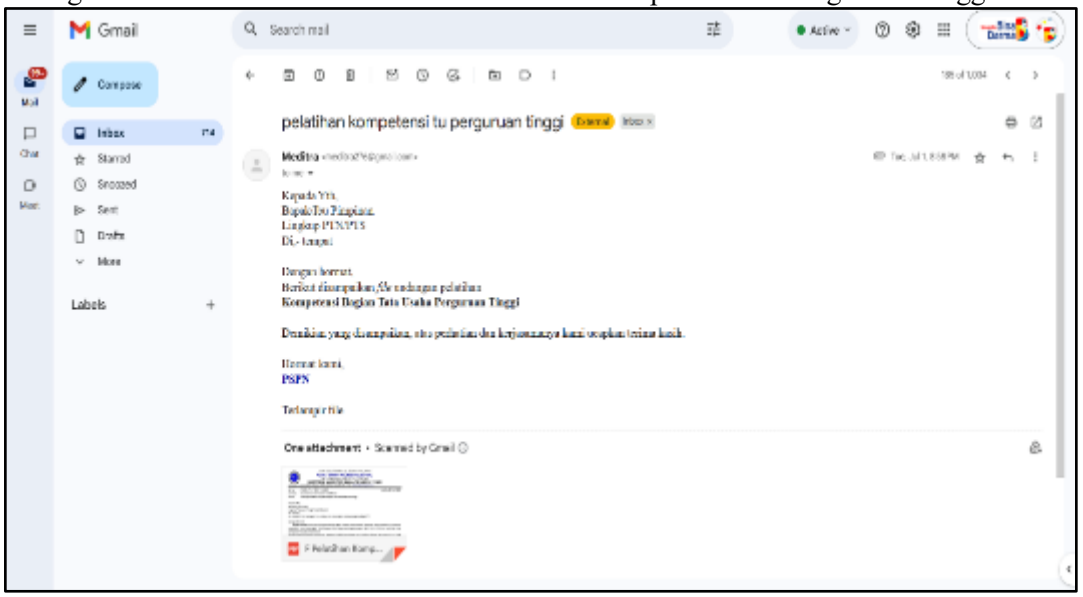

Figure 9. 8th Email view on DIIB incoming email

i) A ninth email was sent with the title "Call for Paper: International Conference on Urban Sustainability, Environment, and Engineering (CUSME 2020)."

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

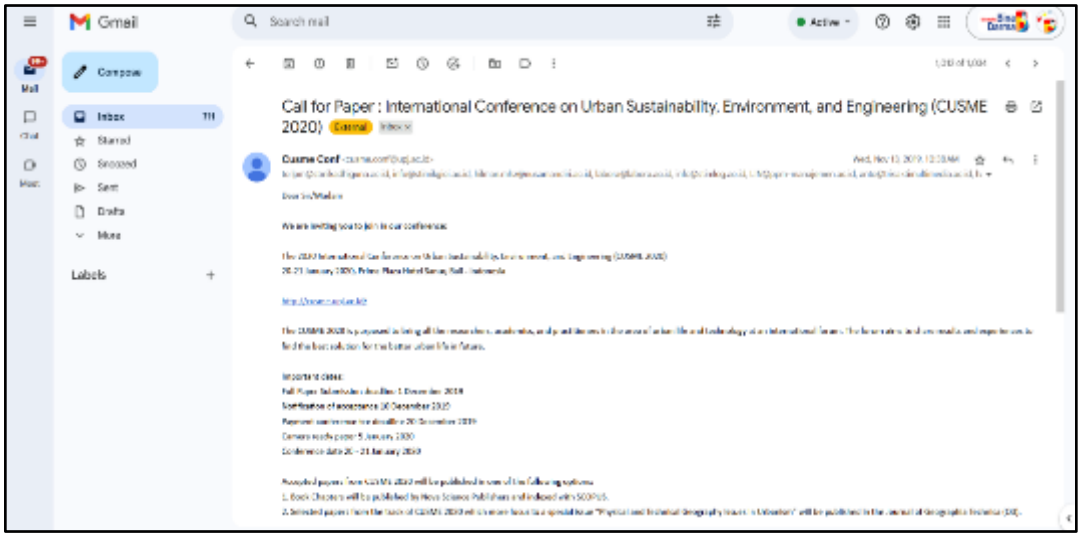

Figure 10. 9th Email view on DIIB incoming email.

j) A tenth email was sent with the title "Undangan Webinar PkM: Pengabdian Masyarakat Sebagai Bagian dari Hilirisasi Riset."

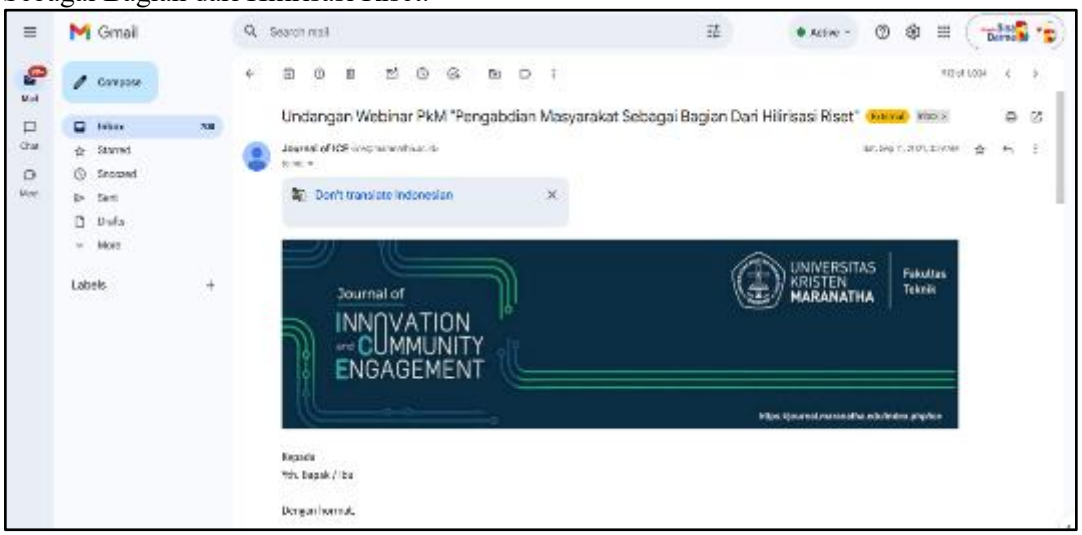

Figure 11. 10th Email view on DIIB incoming email

The ten emails illustrated in Figures 2 through 11 demonstrate several indicators commonly associated with suspicious or potentially malicious correspondence. A number of these messages originated from public email domains such as Gmail and Yahoo, which lack institutional credibility and are frequently exploited in phishing or spoofing attempts. Several emails also failed to include clear information about the sender's organizational affiliation or verifiable institutional identity, raising doubts about their authenticity. Moreover, the overall content, including invitations, training announcements, and academic offers, appeared generic and non-specific, characteristics often found in mass phishing campaigns designed to deceive multiple recipients simultaneously.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

3.1. Flowchart Stages

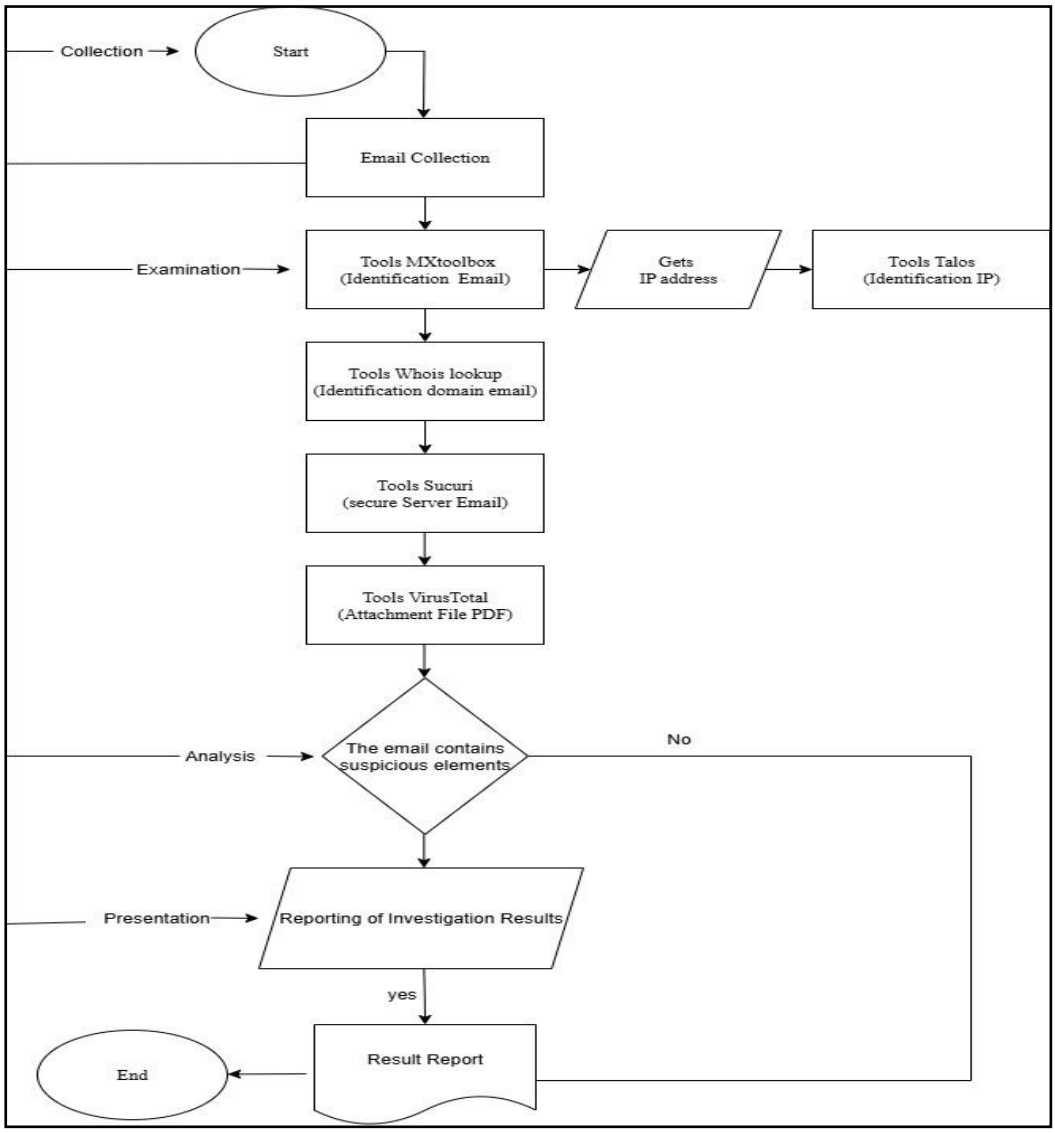

Figure 12. Research stage flow diagram

Figure 12 shows the flow of research stages based on the Digital Forensic Research Workshop (DFRWS) framework. At the Identification stage, researchers identify potentially suspicious incoming emails, both in terms of sender, subject, and message content.

3.2. Header and Authentication Analysis

MXToolbox is a web-based service that provides various features to analyze and monitor email system configurations, especially related to DNS (Domain Name System) records such as MX (Mail Exchange), SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). The following table shows the results of the three emails checked.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

Table 1. Explanation of the results of the second email check with MXToolbox

Parameter	Email 1	Email 2	Email 3
Spf	Pass	Pass	Failed
Dkim	Pass	Pass	Pass
Dmarc	Failed	Pass	Failed
Authentication status	Failed	Failed	Failed

Parameter	Email 4	Email 5	Email 6
Spf	Pass	Pass	Failed
Dkim	Pass	Failed	Pass
Dmarc	Pass	Pass	Failed
Authemtication	failed	Pass	Pass

Parameter	Email 7	Email 8	Email 9
Spf	Pass	Pass	Failed
Dkim	Pass	Failed	Pass
Dmarc	failed	Pass	Failed
Authemtication	Pass	Failed	Failed

Email 10
Failed
Failed
Failed
Failed

Table 1 shows the results of header analysis using MXToolbox on ten suspicious emails received by DIIB. The analysis revealed that several emails had inconsistent authentication statuses. SPF verification was successful in six of the ten emails, DKIM was successful in seven, and DMARC was successful in only four. Some emails exhibited authentication where SPF and DKIM passed but DMARC failed, indicating a possible issue with the email forwarding process or an improperly configured authentication policy. Conversely, several emails exhibited complete authentication failures, indicating potential spoofing or phishing attempts. Specifically, Email 10 failed authentication on all three protocols (SPF, DKIM, and DMARC), thus disproving the sender's identity and indicating a high probability of sender impersonation. These findings emphasize the importance of comprehensive header-based analysis to verify sender authenticity and detect fraudulent or malicious email activity.

3.3. Domain and IP Reputation

Using By using Whois Lookup, the sender's domain is identified as a public domain with no official organizational affiliation, so the sender cannot be verified. While Gmail is a legitimate service, its open nature allows for potential abuse for spoofing. Based on Talos Intelligence, the sender IP has a neutral reputation with no spam activity detected, but its public accessibility still poses a risk of impersonation

Table 2. Domain and IP Reputation Analysis Result

Parameter	Email 1	Email 2	Email 3
Domain Source	Gmail.com	Yahoo.com	Woocommerce.com
Domain Status (whois)	Public, no official affiliation	Public, no official affiliation	Verified official domain

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

IP Source	Google SMTP Server	Yahoo SMTP Server	Official WooCommerce Server
IP Reputation (talos)	209.85.220.65 Status: Neutral	106.10.240.79 Status: Critical	198.2.175.160 Status: Critical
Blacklist Status	Not blacklisted	Not blacklisted	Not blacklisted
Conclusiom	Potential domain misuse	Spam origin, phishing	Email spam

Parameter	Email 4	Email 5	Email 6
Domain Source	Yahoo.com	Yahoo.com	Yahoo.com
Domain Status (whois)	Public, no official affiliation	Public, no official affiliation	Public, no official affiliation
IP Source	Yahoo SMTP Server	Yahoo SMTP Server	Yahoo SMTP Server
IP Reputation (talos)	106.10.242.141 Status: Good	106.10.241.140 Status: Good	106.10.242.37 Status: Neutral
Blacklist Status	Not blacklisted	Not blacklisted	Not blacklisted
Conclusiom	Potential domain misuse	Spam origin, phishing	Email spam

Parameter	Email 7	Email 8	Email 9
Domain Source	Gmail.com	Gmail.com	Upj.ac.id
Domain Status (whois)	Public, no official affiliation	Public, no official affiliation	Verified official domain
IP Source	Google SMTP Server	Google SMTP Server	Official Upj.ac.id Server
IP Reputation (talos)	209.85.220.41 Status: Neutral	209.85.220.41 Status: Neutral	40.107.131.52 Status: Neutral
Blacklist Status	Not blacklisted	Not blacklisted	Not blacklisted
Conclusiom	Potential domain misuse	Spam origin, phishing	Email spam

Email 10
Maranatha.ac.id
Verified official domain
Official Maranatha.ac.id server
209.85.220.65 Status: Critical
Not Blacklisted
Email spam

The results in Table 2 show that most sender domains originated from public services such as Gmail and Yahoo, which have no official organizational affiliation. This condition makes sender identities difficult to verify and increases the risk of misuse for spoofing or phishing activities. Although none of the analyzed domains were listed on major blacklist databases, several IP addresses were flagged with *critical* reputations by Talos Intelligence, particularly those associated with Email 2 and Email 10. This indicates a high likelihood of spam activity or mass email distribution from unverified sources. In contrast, verified domains such as

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

Woocommerce.com, *Upj.ac.id*, and *Maranatha.ac.id* demonstrated better reputation scores; however, improper configuration of authentication mechanisms could still allow potential exploitation. Overall, these findings highlight that domain and IP reputation play a crucial role in assessing the trustworthiness of incoming emails.

3.4. URL and Server Risk Evaluation

The Sucuri SiteCheck tool was used to analyze links embedded in the email or associated with the sender domain. The scan returned a timeout with a medium-level risk assessment, indicating possible vulnerabilities or inactive threat detection mechanisms. Despite not being blacklisted, the domain was categorized as unverified and potentially unsafe. The following table shows the results of the sucuri examination

Table 3. Sucuri SiteCheck Domain Security Results

Parameter	**Email 1**	**Email 2**	**Email 3**
Domain source	Gmail.com	Yahoo.com	Woocommerce.com
Scan result	Time out	Time out	Time out
Risk level	Medium risk	Medium risk	Medium risk
Blacklist status	Not Blacklisted	Not Blacklisted	Not Blacklisted
Security conclusion	Potentiallyunsafe domain	Potential vulnerabilities	potentially contains vulnerabilities
Parameter	**Email 4**	**Email 5**	**Email 6**
Domain source	Yahoo.com	Yahoo.com	Yahoo.com
Scan result	Time out	Time out/ suspicious resources	Time out
Risk level	Low risk	Medium risk	Medium risk
Blacklist status	Not Blacklisted	Not Blacklisted	Not Blacklisted
Security conclusion	No malware detected	Potential vulnerabilities	potentially contains vulnerabilities
Parameter	**Email 7**	**Email 8**	**Email 9**
Domain source	Gmail.com	Gmail.com	Upj.ac.id
Scan result	Time out/ suspicious resources	Time out/ suspicious resources	clean
Risk level	High risk	Medium risk	Medium risk
Blacklist status	Not Blacklisted	Not Blacklisted	Not Blacklisted
Security conclusion	Potentiallyunsafe domain	Potential vulnerabilities	No malware detected

Email 10
Maranatha.ac.id
Time out
Medium risk
Not Blacklisted
Potentiallyunsafe domain

Based on the results in Table 3 obtained from the *Sucuri SiteCheck* analysis, most domains experienced *timeout* responses and were categorized under medium to high risk levels. Such timeouts may indicate potential vulnerabilities on the server side, weak security configurations, or inactive threat detection mechanisms. Some domains, such as those in Email 7 and Email 8, showed *suspicious resources* during scanning, while official domains like *Upj.ac.id* and *Maranatha.ac.id* were still categorized as medium risk due to potential vulnerabilities, even though they were not listed in any blacklist databases. These results suggest that while none of the domains were explicitly identified as malicious, several exhibited conditions that warrant

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

further monitoring. Continuous evaluation of server and URL security remains essential to prevent potential exploitation or phishing-based attacks.

3.5. Malware Detection in Attachment

Emails were scanned using VirusTotal and Sucuri SiteCheck. Emails without PDF attachments were scanned for the attached link, which then scanned the sender's website using tools like Sucuri and VirusTotal. The following table shows the overall virus scan results.

Table 4. Attachment and URL Malware Scan Results Using VirusTotal

Parameter	**Email 1**	**Email 2**	**Email 3**
Attachment type	PDF	PDF	URL
Scan result	Clean – No Malware Detected	Clean – No malware detected	URL Result – No malware detected
Malicious content	None Detected	None Detected	None Detected
Security conclusion	Safe attachment	Safe attachment	Safe attachment

Parameter	**Email 4**	**Email 5**	**Email 6**
Attachment type	PDF	PDF	PDF
Scan result	Clean – No Malware Detected	Clean – No malware detected	URL Result – No malware detected
Malicious content	None Detected	None Detected	Medium Risk
Security conclusion	Safe attachment	Safe attachment	Safe attachment

Parameter	**Email 7**	**Email 8**	**Email 9**
Attachment type	PDF	PDF	URL
Scan result	Clean – No Malware Detected	Clean – No malware detected	URL Result – No malware detected
Malicious content	Low Malware risk	None Detected	None Detected
Security conclusion	Safe attachment	Safe attachment	Safe attachment

Parameter
URL
Scan result
Malicious content
Medium attachment

The malware scanning results presented in Table 4 using *VirusTotal* and *Sucuri* indicate that most email attachments in PDF format were found to be clean with no active malware detected. Similarly, the scanned URLs showed no signs of malicious content or code injection. However, a few emails, particularly Email 6 and Email 9, showed low to medium risk levels in their scanning results, suggesting potential security concerns that warrant further verification. Although no critical malware was identified, the presence of these moderate-risk indicators highlights the importance of cautious handling of attachments from unknown or unverified senders. Overall, these findings reinforce that email threats are not always associated with active malware but can stem from deceptive sender identities, unverified domains, or vulnerable server configurations that facilitate phishing or spam distribution.

3.7. Summary of Findings

The analysis of ten suspicious emails received by DIIB revealed several key findings. Most emails failed one or more authentication protocols (SPF, DKIM, DMARC), indicating weak sender verification and potential spoofing attempts. Email 10 showed complete failure on all three

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

authentication checks (SPF, DKIM, and DMARC), confirming that the sender's identity could not be validated and representing the highest impersonation risk among all samples. Domain and IP reputation results showed that public domains such as Gmail and Yahoo were most frequently used, with several IPs rated *critical* for spam or phishing activity. In contrast, official domains like *Upj.ac.id* and *Maranatha.ac.id* had better reputations but still required validation. URL and server evaluations showed that most domains were categorized as medium to high risk due to *timeout* responses or suspicious resources, even though none were listed on major blacklists. Malware scanning found no active malware, but a few attachments displayed low to medium risk indicators. Overall, the findings indicate that phishing and spoofing were the dominant threats, not direct malware infection. Email 10, in particular, stands out as the most critical case, emphasizing the importance of implementing strict header authentication and continuous domain reputation monitoring to ensure the authenticity of incoming emails.

.

4. CONCLUSION

This study successfully implemented the DFRWS forensic framework to analyze ten suspicious emails received by the Directorate of Innovation and Business Incubator (DIIB). The combination of forensic tools : MXToolbox, Whois Lookup, Talos Intelligence, Sucuri SiteCheck, and VirusTotal enabled a comprehensive examination of email authenticity, domain reputation, and potential malware threats. The results showed that several emails failed one or more authentication protocols (SPF, DKIM, and DMARC), indicating weak verification mechanisms and possible spoofing activity. Email 10 demonstrated a complete authentication failure, confirming a high risk of sender impersonation. Domain and IP reputation analysis revealed that public domains such as Gmail and Yahoo were most frequently misused, while official domains like Upj.ac.id and Maranatha.ac.id had better reputations but still required regular monitoring. URL and server evaluations indicated medium to high vulnerability risks due to timeout and suspicious resource findings, even though none of the domains were blacklisted. Malware scanning confirmed that most attachments were clean; however, some showed low to medium risk indicators related to phishing or malicious intent. Overall, the findings conclude that phishing and spoofing pose greater threats than direct malware infection. Therefore, organizations such as DIIB should strengthen email authentication mechanisms, continuously monitor domain and IP reputation, and conduct periodic forensic assessments to maintain the integrity and security of electronic communications.

REFERENCES

[1] M. Afifah, A. Amaluddin, and R. Soraya, "Pemanfaatan Surat Menyurat Elektronik Dalam Meningkatkan Efektivitas Komunikasi Organisasi," *J. Dialect*, vol. 1, no. 2, pp. 41–49, 2024, doi: 10.46576/dl.v1i2.4630.

[2] T. Ariyadi and M. R. Pohan, "Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators," *J. Penelit. Pendidik. IPA*, vol. 9, no. 12, pp. 10768–10775, 2023, doi: 10.29303/jppipa.v9i12.5551.

[3] I. Riadi, Sunardi, and F. T. Nani, "Analisis Forensik pada Email Menggunakan Metode National Institute of Standards Technology," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 2, pp. 83–90, 2022, doi: 10.14421/jiska.2022.7.2.83-90.

[4] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques," *IEEE Access*, vol. 10, no. June, pp. 65703–65727, 2022, doi: 10.1109/ACCESS.2022.3183083.

[5] C. M. Bachri and W. Gunawan, "JEPIN (Jurnal Edukasi dan Penelitian Informatika) Deteksi Email Spam menggunakan Algoritma Convolutional Neural Network (CNN)," *Edukasi dan Penelit. Inform.*, vol. 10, no. 1, pp. 88–94, 2024.

[6] W. A. Baroto, "Email Analysis in Fraud Investigation: Digital Forensic and Network

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721

Analysis Approach," *Asia Pacific Fraud J.*, vol. 6, no. 2, p. 265, 2022, doi: 10.21532/apfjournal.v6i2.212.

[7] C. Beaman and H. Isah, "Anomaly Detection in Emails using Machine Learning and Header Information," 2022, [Online]. Available: http://arxiv.org/abs/2203.10408

[8] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 68–73, 2024, doi: 10.33884/jif.v12i01.8344.

[9] R. N. Dasmen, A. Triwulanda, R. Rasmila, D. Kurniawan, and J. Julia, "Implementation of Digital Forensics Photorec in Recovering Lost Files on External Storage," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 12, no. 1, pp. 173–178, 2024, doi: 10.33558/piksel.v12i1.9444.

[10] F. Casino *et al.*, "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/ACCESS.2022.3154059.

[11] M. Wibowo, M. R. Firmansyah, and R. S. Efendi, "Analisis Bukti Digital Pada Aplikasi Discord Desktop Dengan Menggunakan Framework Dfrws," *J. Teknol. Inf. Dan Komun.*, vol. 15, no. 1, pp. 98–111, 2024, doi: 10.51903/jtikp.v15i1.826.

[12] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, pp. 43–48, 2022, doi: 10.30591/jpit.v7i1.3639.

[13] R. T. Sibe, "Digital Forensic Investigation of an Unmanned Aerial Vehicle (UAV): A Technical Case Study of a DJI Phantom III Professional Drone," *J. Cybersecurity Inf. Manag.*, vol. 15, no. 1, 2025, doi: 10.54216/jcim.150115.

[14] M. Moreb, S. Salah, and B. Amro, "A Novel Framework for Mobile Forensics Investigation Process," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 125–136, 2024, doi: 10.12785/ijcds/160110.

[15] H. Alazzam, O. Abualghanam, Q. M. Al-Zoubi, A. Alsmady, and E. Alhenawi, "A New Network Digital Forensics Approach for Internet of Things Environment Based on Binary Owl Optimizer," *Cybern. Inf. Technol.*, vol. 22, no. 3, pp. 146–160, 2022, doi: 10.2478/cait-2022-0033.

[16] A. Q. I. Hidayat, E. I. Alwi, and A. W. M. Gaffar, "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS," *J. Minfo Polgan*, vol. 13, no. 1, pp. 1138–1146, 2024, doi: 10.33395/jmp.v13i1.13966.

[17] I. Riadi, H. Herman, and I. A. Rafiq, "Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework," *Int. J. Artif. Intell. Res.*, vol. 6, no. 2, 2022, doi: 10.29099/ijair.v6i2.311.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v24i4.14721