IJFL (International Journal of Forensic Linguistic)

Vol. 4, No. 2, 2025, Page 29-31

P-ISSN: XXXX-XXXX
E-ISSN: XXXX-XXXX

Review Article: Investigation Forensics Email with Such Demonstrations and Tools

Pontianus Cahyono La'ia

Magister of Linguistics – Warmadewa University
pontylaia@gmail.com

Received: DD/MM/YYYY Revised: DD/MM/YYYY Published: DD/MM/YYYY

How to cite (in APA style):

Lai'a, Ponti. (2025). Review Article: Email Forensic Investigation with Various Approaches and Tools. *IJFL (International Journal of Forensic Linguistic)*, *4* (2), 29-31
Doi: http://dx.doi.org/xxxxxxjr.xx.xxx.Page

Abstract- Computer forensics or what is a subfield of forensic science that works with legal evidence obtained on digital storage medium. It is referred to as digital forensics. This branch of science is used to describe facts that will become evidence in the legal process. As opposed to the actual world, cybercrime takes numerous forms. One such form is counterfeiting, sometimes commonly referred to as spam email, which can be a vehicle for the spread of harmful material over a network. The current issue is the wide variety of procedures utilized in each step of digital forensics, each with its own set of benefits and drawbacks. Therefore, literature observation is needed, in this instance, in the form of unique essays that examine email-based crimes, including their methods and flow. According to the review article's findings, every research methodology and tool has pros and cons of its own, allowing users to customize it to suit their needs.

Keywords: email forensics, cybercrime, computer forensics, forensic tools

I. INTRODUCTION

Digital forensics, another name for computer forensics, is a subfield of forensic science that focuses on gathering evidence that can be found on computers and other storage devices for legal purposes, Utdirartatm (2001). Forensics is a scientific process in collecting, analyzing and presenting various evidence in court due to a legal case. This is different from the definition of forensics in general, computer forensics can be defined as the process of collecting and analyzing data from various computer resources which include computer systems, including networks, communication lines and various storage media presented in court, Karsono (2012).

Forensics is an investigative activity and establishing facts related to criminal or legal matters. A branch of forensic science called "digital forensics" deals with the identification and examination of data found on digital devices, Rahardjo (2013). The use of appropriate forensic methods is a very important factor to support a more effective and efficient criminal investigation process in handling a cybercrime case, Umar (2016). An important part of digital forensics is the authenticity of digital evidence, Budiman (2017). Carrying out

an investigation through the stages of the digital forensic examination procedure approach is a valid way to obtain evidence. The discovery of digital evidence obtained by investigators directly leads to the benefit of reconstructing the case at hand, Prayudi (2017). One branch of computer forensics is email forensics, where email or electronic mail is an internet service that is often used in society in the form of text-based electronic mail, but with technological developments, email can not only send files in text form, but also audio. , photos, videos and other extension files, Kurniawan (2005). Since email is the primary means of spreading spam and other harmful content throughout the network, this poses significant risks that follow the convenience that email offers by using this characteristic as a channel for crime in the cyber world. Computer network forensic evidence can be used to design the outcomes of testing and analysis of computer network security solutions. After a computer network security system is created, attackers will not be able to carry out attacks in the future using the same method, Fadlil (2017).

Spamming and spoofing emails is a common crime using electronic communications. Email spoofing is the deliberate sending of emails with the appearance that they came from a legitimate email address, whereas email spamming is the unsolicited and sometimes harmful sending of emails to random recipients, Ojha (2012). As a result, understanding how to prevent frauds in the email industry is crucial.

II. RESEARCH METHODS

The technique is called literature observation, and in this instance, it takes the shape of academic papers that examine email-based crimes, covering their methods and flow.

1) Inclusion Criteria:

- Research articles related to email crime and its analysis methods.

- Research articles in English or Indonesian.

- Research articles containing email crime case simulations.

- Research articles that use tools that can be accessed for free.

2) Exclusion Criteria:

- Research articles that only contain internet crime material, not specific to email crime.

- Research articles that cannot be accessed for free full text.

III. RESULTS AND DISCUSSION

A. Forensic Email Investigation Techniques

Below are several technical approaches to forensic email investigation:

-Sender mail fingerprints
-Style tactics
-Header analysis
-Server investigation
-Software Embedded Identifiers
-Investigation of Network Devices

B. Forensic Email Tools

A portion of the numerous tools available for use in email-based criminal investigations are not available for free download, requiring users to pay for access or ownership. The following list of resources is available without charge:

1) Email Tracker Pro

This tool finds the sender's IP address through analysis of email headers, allowing for message tracking. This tool may predict the city from which the email sender is most likely to have originated, in addition to tracking multiple emails simultaneously. This tool's primary function is the generation of reports that are forwarded straight to the sending ISP, enabling them to take legal action against the message sender.

2) Aid4Mail Forensics

Email searches can be performed in this application using PDF files that can be exported. Emails can be filtered using this program according to text, date, time, keywords, logical operators, regular expressions, header content, and body content. Aside from that, this tool's capabilities include the ability to restore deleted emails and filter duplicate emails.

3) Complain

Spam emails, which are often GLJXQDNDQ-GDODP-SHQLSXDQ-DWDX-FDUD-PHQJKDVLONDQ -valid, can be reported using this program.

4) Email Tracer

This tool gathers information from an email's header, including the sender's IP address, and uses that information to create a thorough HTML report that summarizes the header analysis. The report results include the sender's city information and the originator's geographic location. A keyword search feature for email content, including attachments and their categorization, is another feature of this application.

5) Digital Forensic Framework

Emails saved on the hard drive can be examined by this program. Email content, tags, and time can all be used as search parameters. This tool can also provide the specifics of the email's send date and time.

III. CONCLUSIONS

Email-related crimes, including fraud, theft of private information, and threats, are becoming more frequent. Whoever does this, including in this instance after sending, will remove the email that serves as proof. To examine these harmful emails, email forensics is therefore required. Numerous techniques, including Header Analysis, Email Structure, IP Tracing, Bait Tactics, Email Header Tracing, Server Investigation, and others, can be used for email analysis. In the meanwhile, other tools are employed, each with pros and cons.

REFERENCES

Budiman, R. (2001). Computer Forensics: What and How? Jurnal Fakultas Teknik Elektro dan Informatika, Institut Teknologi Bandung, Jawa Barat.

Fadlil, A., Riadi, I., & Aji, S. (2017). Development of a Computer Network Security System Based on Network Forensic Analysis. Journal of Computer Electrical Engineering and Informatics (JITEKI), 3(1), 11–19.

Karsono, K. (2012). E-mail Forensics. Scientific Forum, 9, 58–75.

Karsono, K. (2012). Forensik E-Mail. Esa Unggul E-Journal.

Kurniawan, H. (2005). Practical Guide to Installing a Free Windows-Based Email Server Using Mail Server. Jakarta: PT Elek Media Komputindo.

Ojha, G., & Tak, G. K. (2012). Novel Approach Against Email Attacks Derived from User Awareness-Based Techniques. International Journal of Information Technology Convergence and Services, 2(4).

Prayudi, Y. (2014). Digital Chain of Custody: Problems and Solutions in the Investigation Process. SENASTI.

Rahardjo, B. (2013). A Glimpse into Digital Forensics. Jurnal Sosioteknologi, FSRD-ITB, 29, 384–387.

Riadi, I., Eko, J., Ashari, A., & Sunardi. (2013). Internet Forensics Framework Based on Clustering. International Journal of Advanced Computer Science and Applications, 4(12), 115–123.

Umar, R., Yudhana, A., & Faiz, M. N. (2016). Performance Analysis of the Live Forensics Method for Investigating Random Access Memory on Proprietary Systems. In Proceedings of the 4th National Conference of the Muhammadiyah Higher Education Postgraduate Program Association (pp. 207–211).

Utdirartatm, F. (2001). Overview of Forensic Analysis and Its Contribution to Computer System Security. Jurnal Fakultas Teknik Elektro dan Informatika, Institut Teknologi Bandung, Jawa Barat.