International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Forensic Technical Process by E-Mail

Sudhanshu Gupta, Anand. R, Anil G.N

Abstract: ***Forensic mail network were based more on the e-mail message structure, whereas email content was rarely used. In different security extension schemes, cyber criminals tend to make use of email protocols by multiple producers over the course of a year for illegal purposes, for example send emails have become the most important digital platform for communication, file transfer and transactions and use not only laptops but also many other electronic gadgets including mobile phones.In this context, a number of forensics open source resources were frequently used by professionals. Furthermore, the misuse of Internet infrastructure by denial of service, storage waste and computer resources costs every internet user directly or indirectly. E-mail forensic is used to the origin and the content of e-mail as evidence, to determine the actual sender, the recipient, and when and how it was sent, etc. These instruments were nevertheless developed in isolation rather than in cooperation. Since forensic email users have to know the utility of a method for forensics research in their own situations. This paper is intended to illustrate the email system architecture from a forensic perspective. It describes the email partners ' roles and responsibilities, the metadata in the email headers***

Keywords: ***E-mail Forensics; E-mail Headers; Header; Architecture of E-mail***

I. INTRODUCTION

A. IMFORMATION

E-mail systems have already covered all aspects of life, making interaction between people easier. It nevertheless offers criminals a new way of crime. Some criminals use email to organize and plan a number of activities, including the smuggling of goods. Email crimes have a serious adverse effect on the security of human property[1].As an important industry in digital forensics, research and discussion have focused on the problem of the technology application of email forensics.

Past situation:

The earth. E-mail and chats were mostly unknown to people. Earlier emails were used in good faith for communication without harming others, but now this scenario has been changed.

Present situation:

The e-mail was based primarily on the network structure and the e-mail content. The network structure-based focused on the email network culture[1,2].And content-based included mainly the spam filtering[3], identification of the author[4], mining of e-mail users ' behavior patterns, authenticity and header , retrieval, etc. These research could play an important role of digital forensics.The e-mail system comprises a number of hardware and software components including client, server and receiver computers and required software and services[5]. In addition, it uses different Internet systems and services.The capabilities of a number of popular forensic email tools, such as Main Xaminer, Add4Mail, Digital Forensic Framework (DFFF)[6]. Our work complements the previous research efforts aimed at understanding the potential of other kinds of forensic devices, such as forensics networkand forensic tools for disc / memory[7].

Network Forensics:

Network forensics for the compilation, legal proof or intrusion detection of data is a sub-sector of digital forensics for monitoring and of software net traffic. Network research deals with volatile and complex data, unlike other areas of digital forensics. Transmission of network traffic and then failure, so forensic networks are often pro-active [8]. In this situation may include reassembling transferred data, searching for keywords and r human communication, e-mails or talk sessions.

II. EMAIL ROLES AND RESPONSIBILITIES

By using the Internet Email offers the exchange of stored emails. The web-based and client-server-based standards can also be used for sending e-mails in two standard methods. Email communication, messages in ASCII format can be attached and transmitted to the binary streams of the non-text files, such as sound and images[10].Examining sender's e-mail address

- Examining message initiation protocol (HTTP, SMTP)
- Examining Message ID
- Examining sender's IP address

Application protocols developed for email include: IMAP, Post Office Protocol (POP), UNIX-to-UNIX copy protocol (UUCP), Simple mail transfer protocol (SMTP) and the MTP[5]. However in the late 1980's these protocols were developed and some were taken into account.At present, SMTP, POP and IMAP[8] are the most frequent protocols used in the sending and receipt of emails.

Manuscript published on January 30, 2020.
* Correspondence Author
Mr.Sudhanshu gupta*, BMS institute of technology and management, bengalurur,india :sudhanshu085@gmail.com
Mr. Anand.R, Assistant Professor BMS institute of technology and management**,** india : anandor@bmsit.in
Dr. Anil G. N, Working as HOD and professor in computer science and engineering department BMS Institute of technology and management,bengaluru,Karnataka,india, : anilgn@bmsit.in

Below are popular email access protocols currently in use.The SMTP, POP and IMAP are included. Although SMTP is used for sending client e-mails to the server, the two other protocols are used to recover server to client e-mails[9]. These email only took into account the network's logical structure without taking into account specific email features. In addition to common social network structural characteristics, the email network has numerous typical features like time, relation, the subject matter and the contents, etc. These characteristics are important in network for email communication. However, these properties were not fully utilized by existing . In order to find out which destination mail-server (referred to in "Mail exchanger," or MX) to deliver the message, the sender's mail-server(technically known as "Mail Transfer Agent" or MTA) is searching "@domain.com" portion of the email address in an address server called Domain Name System(DNS).

III. METHODOLOGY

E-mail system integrates a number of hardware, software, services and protocols that allow for interoperability between its users and between the components along the transmission path[11].In the impact of e-mail delivery there are several communicators called E-mail nodes, which are basically software units that work on the TCP / IP model application layer.Network protocol is a set of conventions defining accurate network syntax and sequencing. In order to implement client / server mail on the Internet, two main protocols have developed: SMTP and POP3[11]. These basic protocols have been further refined. The encrypted attachments support PEM and S/MIME,and the encrypted server-to-server transmission is provided by S / SMTP.Every website has one Message Store and one MTA. There may be a number of User Agents connected to MTA — some may be software-enabled by mail. Every user agent is used by one person and every user agent is connected to an MTA.

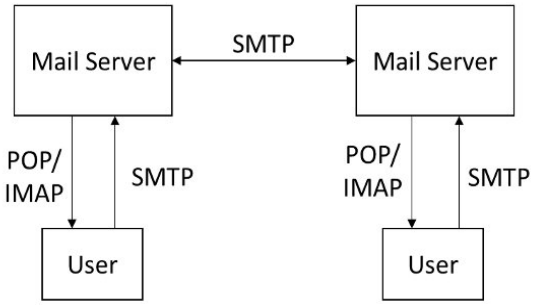

Fig 1. Relationship between components

- **Message / Mail User Agent (MUA):**

Works as your representative within the email service for user players and applications. The Author MUA (aMUA) is the author who works for the Author, and the recipient MUA is the recipient (rMUA)[12]. Initial submission via Mail Submission Agent is created and performed by aMUA.

- **Message mail store(MSS):**

This is a long-term MUA message store that can be placed on a remote server, or on a MUA-operated machine. Messages in different ways can be organized by MS. A local mechanism or POP or IMAP is used for accessing the MS.

- **Relay:**

SMTP-Relaxation is the nodes which transmit e-mail. Recovery of a SMTP e-mail node is the message of receiving and transmitting the message to another. They are like packet switches or IP routers and perform routing to move the communication closer to the recipients. They also add trace data and all MTA roles.

- **Gateway:**

The e-mail messages from one application layer to the next are converted by gateway nodes. Gateway nodes named GWSMTP, B accept SMTP protocol based e-mails and transfer them with protocols other that SMTP and GWA, SMTP performs the inverse incoming and outgoing interfaces[13].A default port assignment list is provided in Table 1.

Table 1: Usually used Email Communication ports

Port No	Protocol Services	Description
25	SMTP SMTP e-mail server	Simple Mail Transfer Protocol - core Internet protocol used to transfer from client to server (MUA to MTA) and server to server (MTA to MTA)
110	POP3 POP e-mail server	Post Office Protocol allows clients (MUA's) to retrieve stored e-mail
80	HTTP	Webmail
443	HTTPS	Secure Webmails
143	IMAP IMAP(4) e-mail server	Internet Message Access Protocol provides a means of e-mail messages on a remote server and retrieve stored e-mail

IV. FORENSICS E-MAIL TECH

E-mail forensics refers to the of e-mail source and content as evidence of a sender and receiver's actual message, data / date of sending, detailed e-mail transmission record, sender intent, etc[14].This research comprises metadata research, search for keywords, port scan, etc.

- **Header Source**

Meta information containing information on the sender / path along which the message passed in the form of control information, i.e. envelope and headers including headers within the messages body.

- **Network Device Source**

In this type the archives of messages are used for the purposes of the origins of a email message generated by network devices such as routers, firewalls and switches[15].

- **Software Embedded Identifiers**

The e-mail could disclose some vital information on the priorities and choices of the senders to collect customer side data[15]. The work will show the user machine PST file names, windows logon name, MAC address, etc.

- **Sender Mailer Fingerprints**

Software e-mail identification on the server can be revealed from the received header field and the identification of the client's software e-mail can be determined by using different headers such as "X-mailers" or equivalent.

- **Server Headers**

In this system, the origins of an e-mail message were by copying e-mails sent and database logs. E-mails are purged byclient(s) whose recovery is impossible, as most e-mails save a copy of all e-mails after their delivery may be requested from the servers (Proxy or ISP)[16].

V. E-MAIL FORENSIC TOOLS

- **Email Tracker**

Pro e-mail headers to identify the IP address of the computer that sent the email and trace the recipient.

- **Abuse Pipe**

manipulation of complaint e-mails and defines which ESP consumers e-mail complaint-based spam. AbusePipe can be programmed to respond people reporting abuse. Automatically.

- **EnCase Forensic**

It is a computer forensic program that enables to picture and preserve a drive using EnCase evidence file format in forensic style[17]. This provides a complete set of research, bookmarking and monitoring. The Web and email work was sponsored. Outlook PSTs / OSTs, the Outlook Express DBXs, the Lotus Notes, AOL, Yahoo, Hotmail, Netscape Mail, the MBOX archives, are enabled via phone.

- **Final e-mail**

Can access an email archive document and find missing emails that are not connected to the position of the records[16].
FINALeMAIL will restore lost e-mails, recover complete e-mail data base files even if such files were virus attacked or destroyed by incidents**.**

- **Forensics Toolkit (FIT)**

It is a technical software toolkit for the reading of the material in the CAPture Packet (PCAP) format of the Internet raw data[17]. FIT provides the power to perform content and recovery on precautioned wired or wi-fi Web raw data for safety administrative staff, scammers, prosecutors, and legal enforcement officers.

VI. RESULTS OF ANALYSIS

With the JavaMail library we have developed the Backscatter Email Analysis Tool (BEAT). It can process the messages of backscatter as they come. When new messages arrive in the spam inbox, the analyzer first checks that the email is an e-mail backscatter and then scans the fake or final' Received' header on the RFC822 headers MIME tag. This collects an IP address of the server, the spam message, and it tests whether it's in any of the four DNSBLs if it finds helpful header of spam that lead the backscatter. The knowledge collected from a spam backpack is processed system

1. Outlook allows users to show email headers with the attachments in rich text format and also.
2. You can evaluate the email header by navigating to the email properties that provide the following information.

E-mail identifiers are internationally special, comprising of email, domain name, address identity and ENVID. Mail boxes are assigned e-mail for accepting mail bodies. E-mail address has grown into a common Internet identification identifier. A user name and a domain name divided by @sign e.g. sud@a.com consists of an e-mail address. Next, Ray Tomlinson started using @ sign as a username separator from domain name. An Internet site domain name, like a server, network or device maps to an IP address(es), is a regional connection in Table II.

Table II. Analysis Data

Field Name	Set By	Field Description
Layer: *Message Header Fields (Identification Fields)*		
Messag e- ID:	Originator	String of identity of the globally unique message produced when sent.
In-Repl y-To:	Originator	Contains the initial user message ID to which the response reply is sent.
Referen ces:	Originator	Identifies other records, such as other e-mail messages relevant to this corresponde nce.

Field Name	Set By	Field Description
Layer: Fields Email Headers (Address Fields Destination)		
Messag TO :	Originator	Enter a sample of the message recipient's emails. Such addresses can range from RcptTo SMTP commands in general to To Field.
In-Repl To:	Originator	Such addresses are special. Usually determines the primary recipient to whom acts and CC addresses are intended.

The X-Apparently-To header shown in the first article is important when mail was sent as a BCC or to a mailing list receiver. In most instances, this area includes the address in To. Nonetheless, X-Apparently-To varies from a TO area when mail was sent to an BCC receiver or a mailing list. Many people may display TO while others may not. Therefore X-Apparently-To always displays the recipient's e-mail address when mail is sent via TO, BCC, CC or a mailing list.

VII. CONCLUSION

Increasing numbers were issued threatening emails, confidential information can also be stealed via phone. Upon reading or using important content, anyone can erase e-mail since forensics is required for e-mail.

Different criteria such as email Header , address monitoring, IP tracking, lure strategies are shown and emails removed from garbage can be seen from the detailed .

Removed mail can be retrieved from Yahoo, Rediff, Gmail and other emails from trash / recycling bin if accidentally or intentionally removed, but the possibility of retrieving them if mails are deleted from trash / recycling bin is very small. And therefore it can be seen that fewer email tasks have been performed permanently

REFERENCES

1. The Polish Society for Privacy and Reliability Summers Seminars, Volume 7 novermber ,2016: Charalambous Elizavet, Bratskas Romeos, Koudras Nikolaos, Karkas George, Anastasiades Andreas, "A Roadmap to Email Header Research Event."
2. Hossain Shahriar, "Compartmental of Email Forensic Methods," 2015, 6, 111-117, Vamshee Krishna Devendran, Hossain Shahriar, Victor Clincy.
3. Matt Bishop, Kara Nance, Brian Hay. (2009). (2009). The 42nd Hawaiian International Conference in Computer Sciences 2009, Electronic Forensics: Setting the work agenda.
4. Sumanth Reddy Allam and Loretta A. Moore, Natarajan Meghanathan. (2009). (2009). Forensic Network Tools and Techniques, International Network Security & its Applications Journal, Vol.1, No. 1, April 2009.
5. Stephen V. Flowerda, Himal Lalla. (2010). (2010). In the interests of a structured electronic forensic : forensics e-mail, data security protocols for South Africa in 2010 (ISSA 2010).
6. Matt Bishop, Kara Nance, Brian Hay. 1995]. Visual Forensics: Defining Program for the 42nd International System Sciences Conference of Hawaii – 2009.
7. A. And S, Jayan. IEEE International Conference on computational intelligence and computer science (ICCIC), Dija, Spoofed Mail Detection, Madurai, India, Dec. 2015.
8. F. R. Staden and H. Van Staden S. Venter, Info Safety for South Africa, Johannesburg, South Africa, S.1-5, Sep. 2011, Bringing automated security capability to electronic communication using the Security Monitoring System.
9. M. Eloff, M. D. Kohn, and J. H. Eloff, Computers & Security, ' Integrated Digital Forensic Model, ' vol. 38, p. 103-115, 2013.
10. [S. R. Selamat, R. Yúsef, S. Sahib, International Journal of Computer Science and network security, vol.: "Mapping of the Digital Forensic Research Framework." 8, 163-169, 2008.
11. A. Agarwal, M. Gupta, S. Gupta, and S. Gupta, "Systematic digital forensic model," International Journal of Computer Science and Security (IJCSS), vol. 5, pp. 118-131, 2011.
12. Haibo Wang, Ning Zheng, Ming Xu, Yanhua Guo.Detecting Community Structure in Weighted Email Network[C]. proceedings of 1st International Symposium on Computer Network and Multimedia Technology, Wuhan, CHINA 2009.
13. Eric D. Kolaczyk, Marc Barthélemy, David B. Chu. Betweenness and co-betweenness of groups: interconnected concepts of central coalition. 31 (2009) 190–203 Social Networks.
14. Brandes Ulrik. A simpler method for the centrality of media. Maths Sociology Journal,2001,25(2): 163-177.
15. Ali Tizghadam, University of Toronto, and Alberto Leon-Garcia. Centrality of wear and tear and opposition to communications networks. 2010,6(24): 10-16, IEEE Network, 2010.
16. Mourad Debbabi, Rachid Hajidj, Hakim Lounis, Farkhund Iqbal, Adam Szporer, Jamel Benredjem. To a robust email system for forensic [J]. Digital Science, 2009,5(3-4), 124-137.
17. Alexander J. Karran, Alexander J. Lamb.[15] John Haggerty. A forensic platform for unstructured email interaction information. Mobile Crime and Forensics Global 2011,3(3), 1-18.

AUTHORS PROFILE

Sudhanshu Gupta, obtained my Bachelor of Technology degree in Information Technology From Dehradun Institute Of Technology university Dehradun, Uttrakhand in 2014-2018. I am Persuing my Master's degree From BMS Institute Of Technology and Management,bengaluru karnatakka which will complete in 2020 with the specialization of Computer Science and Engineering. MY research interest include Programming skills and I have done one reaserch paper on Hadoop database system and mobile application development.

Mr.Anand. R, currently working as Assistant Professor in the Department of computer science & Engineering . BMS Institute of Technology and Management, Bangalore, Karnataka, India. He is also a research scholar in the prestigious VTU University & simultaneously doing his research work & progressing towards his Ph.D. in the computer science and Engineering. He has also published a number of research papers in various national & international conferences. He has conducted a number of seminars, workshops, conferences, summer courses in various fields of computer science & engineering. His research interests are Data Mining and Computer Network.

Dr. Anil G. N, Working as HOD and professor in computer science and engineering department BMS Institute of technology and management. His research area are computer network, Mobile adhoc network and sensors network. He published and presented papers in reputed international journal and conference. He Has conducted many conference, workshops, and seminars in various field of computer sciencescience and engineering. His research intrest in computer network and sensor network.