BOOK CHAPTER | Messages with "Messages"

Forensic Analysis of Electronic Mail Messages

Eugene Marfo Akoto
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: kwameugn@gmail.com

ABSTRACT

E-mail has revolutionized business, academic, and personal communication. The advantages of e-mail include speedy delivery, ease of communication, cost effectiveness, geographical independence, and the portability of mailboxes. The last two are the biggest advantages over snail mail. However, with e-mail comes the threat of a genuine user being compromised through key loggers, social engineering, shoulder surfing, password guessing and other similar, though less technical, methods. This passive espionage can have a direct impact on the genuine user in terms of denial of information, loss of money, loss of time, mental harassment and an attack of personal privacy. To enable digital forensic analysis of e-mails, we propose behavioral biometric based authentication, which is analogous to a signature in paper documents.

Keyword: E-mail, forensics, threats, digital analysis, security cyber crimes

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Eugeme Marfo Akoto (2022): Forensic Analysis of Electronic Mail Messages
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 147-154
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P24

1. INTRODUCTION

Email is one of the most popular services used over the internet and has become a primary source of communication for organizations and the public. Usage of email services in business activities like banking, messaging and sending file attachments increased at a tremendous rate. This medium for communication has become vulnerable to different kinds of attacks. Hackers can forge the email headers and send the email anonymously for their malicious purposes. Hackers can also exploit open relay servers to carry out massive social engineering. Email is the most common source of phishing attacks. To mitigate these attacks and catch the people responsible, we use email forensics and techniques like performing header analysis, server investigation, sender mailer fingerprints etc. Email forensics is the analysis of source and content of the email message, identification of sender and receiver, date and time of email and the analysis of all the entities involved. Email forensics also reforms to the forensics of client or server systems suspected in an email forgery.

Below is a diagram depicting how e-mail works;

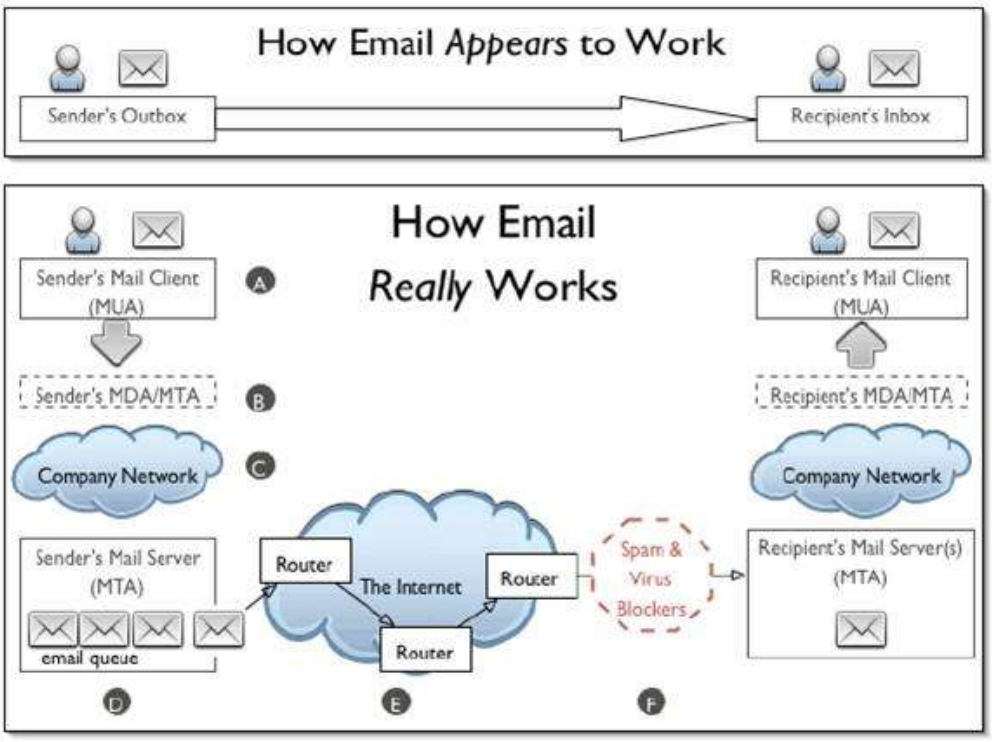

Fig 1.0 How E-mail Systems Works
Source: https://www.startertutorials.com/blog/forensic-analysis-of-e-mail.html

1.1 Background of the Study

Computer Forensics science deals with the preservation, identification, extraction and documentation of computer evidence. The latest statistic showed that 5973 TB of data was processed for FY 2013 which is a 40% increase from FY 2011; as a side note one TB is roughly equivalent to the information in 1,000 encyclopedias. Kara Nance et al have proposed six categories of Digital forensics including Network Forensics also encompassing e-mail forensic analysis. Many studies have been carried out for analyzing tools and techniques used in network forensics and which also include e-mail forensics tools and techniques. E-mail forensic analysis is used to study the source and content of e-mail message as evidence, identifying the actual sender, recipient and timestamp to collect credible evidence to bring criminals to justice.

Additionally, email analysis is challenging due to not only various fields that can be forged by hackers or the wide range email applications in use, but also due to imposed law restrictions in the analysis of email body. Forensic Analysis plays a major role by examining suspected e-mail accounts in an attempt to gather evidence to prosecute criminals in the court of law. Towards this direction, a number of forensics tools, either dedicated to or capable of performing email forensic analysis, have been widely used by the practitioners. However, these tools have been developed in an isolated manner rather than a collaborative approach, while despite the fact that some email forensic analysis tools start as open source and freely accessible solutions, over the years, preferences and options that could help client-side evidence gathering.

The investigation can reveal PST file names, Windows logon username, MAC address, etc. of the client computer used to send e-mail message. Similarly, the received header field and email handling software at the sender side may reveal the software managing emails on the server (due to the different structure in headers). This analysis forms part of a procedure known as sender mailer fingerprints capable of describing applications and their version at the client side; useful as reveals characteristics/vulnerabilities of the bearing host machine. At last, but not least, the less time expensive but also less passive investigation method is known as bait tactics where investigators send an email, to the sender under question, containing an HTTP image source tag hosted on a server of their control.

Once the email is being opened the e-mail client will request through an HTTP call the downloading of the image, revealing its, own or proxy, IP address. It is clear that it is not viable for investigators to perform most of these analyses on a day-to-day basis (with no real evidence in hand) due to their time and resource complexity and also the risk of not being able to gather evidence of real value. Due to this, in this paper we emphasize on email header (tracing) analysis with existing tools in an effort to allow investigators to get to evidence of value in a timely manner.

2. RELATED LITERATURE

There are many tools which may assist in the study of source and content of e-mail message so that an attack or the malicious intent of the intrusions may be investigated. These tools while providing easy to use browser format, automated reports, and other features, help to identify the origin and destination of the message, trace the path traversed by the message; identify spam and phishing networks, etc. This section introduces some of these tools. According to Karkas George, 2016, current forensic tools are designed to help examiners in finding specific pieces of evidence and are not assisting in investigations. Further, these tools were created for solving crimes committed against people where the evidence resides on a computer; they were not created to assist in solving typical crimes committed with computers or and malicious emails. It also displays whether any port is open in any of the HTTP or FTP server in the tracked IP addresses.

Paraben E-Mail Examiner is another proprietary solution capable of processing emails found on a local hard disk and supports comprehensive analysis features, bookmarking as well as advanced searching; including searching within attachments. The tool can examine email headers and bodies, provides information based on the search (including contents from attachments). Paraben E-mail Examiner can recover deleted emails from Exchange (EDB), Lotus Notes (NSF), and Group-Wise email even though they may be deleted from the deleted items folder.

EmailTracer is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier center for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies. This tool traces the originating IP address and other details from e-mail header, generates detailed HTML report of email header analysis, finds the city level details of the sender, plots route traced by the mail and display the originating geographic location of the email. Besides these, it has keyword searching facility on e-mail content including attachment for its classification.

Adcomplain is a command line tool which however does not only take into consideration the header of the message but also the body. It is presented as a tool for reporting inappropriate commercial e-mail and usenet postings, as well as chain letters and "make money fast" postings. It automatically analyses the message, composes an abuse report, and mails the report to the offender's internet service provider by performing a valid header analysis; the report is submitted to U.S. Federal Trade Commission.

MailXaminer by SysTools Software is a digital forensic program built to allow the examination of messages from both web and application-based email clients. MailXaminer loads messages from the chosen email storage source and arranges them hierarchically for the purpose of evidence analysis and extraction. The programming of the application provides carving out of deleted evidence or evidence from damaged sources in cases of evidence spoliation. Post analysis, the software serves output generation in court admissible digital formats.

AbusePipe analyses abuse complaint e-mails and determines which of ESP's customers is sending spam based on the information in e-mailed complaints. It automatically generates reports reporting customers violating ESP's acceptable user policy so that action to shut them down can be taken Messenger toolkit for Microsoft Internet Explorer, Mozilla Firefox, Opera and Apple Safari. The e-mail support includes for Outlook PSTs/OSTs, Outlook Express DBXs, Microsoft Exchange EDB Parser, Lotus Notes, AOL, Yahoo, Hotmail, Netscape Mail and MBOX archives.

FINALeMAIL scans the email database file and locates lost emails that do not have data location information associated with them. FINALeMAIL has the capability of restoring lost emails and restoring them to their original state. Not only can FINALeMAIL recover single email messages it can also recover full email database files. This is an invaluable capability when such files are attacked by viruses or are damaged by accidental formatting. Recover all email messages and attachments emptied from the 'Deleted Items' folder in Outlook Express, Netscape Mail, Eudora, and AL Mail. Sawmill-GroupWise is a GroupWise Post Office Agent log analyzer which can process log files in GroupWise Post Office Agent format, and generate dynamic statistics from them, analyzing and reporting events. It can parse these logs, import them into a MySQL, Microsoft SQL Server, or Oracle database (or its own built-in database), aggregate them, and generate dynamically filtered reports, through a web interface. It supports Window, Linux, FreeBSD, OpenBSD, Mac OS, Solaris, other UNIX, and several other platforms.

Forensics Investigation Toolkit (FIT) is content forensics toolkit to read and analyse the content of the Internet raw data in Packet CAPture (PCAP) format. FIT provides security administrative officers, auditors, fraud and forensics investigator as well as lawful enforcement officers the power to perform content analysis and reconstruction on pre-captured Internet raw data from wired or wireless networks. All protocols and services analyzed and reconstructed are displayed in readable format to the users. The other uniqueness of the FIT is that the imported raw data files can be immediately parsed and reconstructed. It supports case management functions, detailed information including Date-Time, Source IP, Destination IP, Source MAC, etc., WhoIS and Google Map integration functions. Analyzing and reconstruction of various Internet traffic types which includes e-mail (POP3, SMTP, IMAP), Webmail (Read and Sent), IM or Chat, File Transfer (FTP, P2P), Telnet, HTTP (Content, Upload / Download, Video Streaming, Request) and Others (SSL) can be performed using this toolkit.

3. ONLINE SAFETY AND CYBERCRIME PROSECUTION/PREVENTION IN AFRICA

Cybercrime is not only a question of attacks against the confidentiality, integrity and availability of computer data and systems but against the core values and the human development potential of societies increasingly relying on information technology. In the light of this, governments cannot remain passive; they have the obligation to protect society and individuals against crime.

In practice, however, governments face serious challenges:

1. While millions of attacks against computers and data are recorded each day worldwide, only a small fraction of cybercrime2 – that is, offences against and by means of computers is actually prosecuted and adjudicated;
2. Moreover, evidence in relation to any crime is increasingly available in electronic form on computer systems or storage devices and needs to be secured for criminal proceedings. Criminal investigations not relying on electronic evidence seem to become the exception.

An effective criminal justice response is needed. This involves the investigation, prosecution and adjudication of offences against and by means of computer systems and data as well as the securing of electronic evidence in relation to any crime. It also requires efficient international cooperation given the transnational nature of cybercrime and in particular of volatile electronic evidence.

A Legal Framework On Cybercrime And Electronic Evidence: What Is Required?

Governments are not only obliged to take effective measures for the prevention and control of cybercrime and other offences involving electronic evidence, but they must also respect human rights and rule of law requirements when doing so. Criminal law is a means to achieve this. Comprehensive legislation covering both substantive law (conduct to be defined as a criminal offence) and procedural law (investigative powers for law enforcement) is the foundation of a criminal justice response.

Legislation on cybercrime and electronic evidence needs to meet a number of requirements:

1. It must be sufficiently (technology) neutral to cater for the constant evolution of technology and crime as it otherwise risks becoming obsolete already by the time it enters into force.
2. Law enforcement powers must be subject to safeguards to ensure that rule of law and human rights requirements are met.
3. It must be sufficiently harmonized or at least compatible with the laws of other countries to permit international cooperation, for example, to meet the dual criminality condition

African States preparing legislation on cybercrime may draw on a number of documents to seek guidance. These include in particular the African Union Convention on Cyber Security and Personal Data Protection adopted in Malabo in June 2014.4 That treaty reflects a strong commitment by Member States of the African Union to establish a secure and trusted foundation for the information society. It covers a broad range of measures ranging from electronic transactions, to the protection of personal data, cyber security and also cybercrime. Given that this treaty is rather new and is yet to be tested in practice, and given its broad scope, the present report uses the Budapest Convention on Cybercrime5 as reference.

This Convention is more specifically focusing on cybercrime and electronic evidence, including international cooperation, and is increasingly being used in Africa. The Convention on Cybercrime was opened for signature in Budapest, Hungary, in 2001. Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA it is open for accession by any State prepared to implement it and to engage in international cooperation. By April 2016 it had 49 Parties and a further 17 States that had been invited to accede or have signed it.

The Budapest Convention is backed up by the Cybercrime Convention Committee representing the Parties to this treaty and capacity building programmes.
It would seem that the African Union Convention on Cyber Security and Personal Data Protection and the Budapest Convention on Cybercrime complement each other.

5. CONCLUSIONS

Digital forensic analysis is a complex and time-consuming process which involves the analysis of digital evidence. Emails might contain valuable information that could lead investigators to the identity and/or location of the offender. Additionally, email forensic tools through email header analysis may even reveal information related to the host machine used during the composition of the message. In this paper, we have discussed key information related to email forensic analysis as well as important aspects of header tracing. Finally, we listed the available tools that can be utilized for email analysis emphasizing on their key features in an effort to assist investigators in the selection of the appropriate tools

6. RECOMMENDATION FOR POLICY AND PRACTICES

Email forensic investigation can be a complicated task when there are many suspects involved and required analysis of a large number of email mailboxes. Even though the techniques above are quite effective, implementing them accurately can consume a lot of time. That's why professionals use enterprise-grade email forensic tools such as Stellar Email Forensic for fast and accurate analysis. These tools come equipped with features like multiple email views, advanced keyword search filters, deleted email recovery, etc. These programs also generate evidence reports and offer case management tools for easy management of multiple cases

7. DIRECTION FOR FUTURE WORKS

The IM market has seen explosive growth, with millions of users participating in online conversations. However, little has been explored in terms of the research and analysis of the network, messages, user behavior, and data mining of these systems. There are several concerns involving the use of IM systems, including whether the user is really communicating with the intended buddy or friend. The threats include account hijacking, man-in-the-middle attacks, and masquerading. There are various reasons someone would wish to masquerade as someone else including spying, disgruntlement, snooping, and other malicious intentions. This paper presented the use of data mining of IM communications for authorship identification. Classification methods were used to identify IM authors based on various behaviors.

Human behavior presents challenges for analysis. For example, such behavior has an extremely wide "normal" range and can be very unpredictable: abnormal activities are sometimes perfectly normal, and all people change. The results of the experiments here indicate that Naïve Bayes classification is highly accurate (> 99% accuracy) at predicting the author of an IM conversation based on behavior. The experiments also identified the behavior characteristics that are the strongest classifiers. The data showed that users tend to exhibit the same characteristics throughout various conversations. Furthermore, users exhibited different characteristics from each other, much like the uniqueness of biometric data.

Based on these preliminary experiments, future research will involve:

1. Increased numbers of users (classes) in the dataset.
2. Increased numbers of attributes from the set of stylometric features, such as characters, function words, and structural layouts.
3. Varied numbers of characters that are included in an instance, to determine the minimum size necessary for high accuracy and a low false-positive rate.

The author behavior attributes used in these experiments comprise only a subset of the stylometric features that may be used for IM author identification. Other stylometric measures, as shown in Table 1, must also be used to create an accurate, well-rounded user profile. A broad attribute set and larger number of classes should provide a comprehensive analysis of the IM data for highly accurate authorship identification.

REFERENCES

1. AbusePipe - Abuse Email Analysis Solution for ISPs, [available at: http://www.datamystic.com/ abusepipe.html].
2. Adcomplain Home Page, [available at: http://www.rdrop.com/users/billmc/adcomplain.ht ml].
3. Aid4Mail Forensic, [available at: http://www.aid4mail.com/email-forensics].
4. Al-Zarouni, M. (2004). Tracing E-mail Headers. Australian Computer, Network & Information Forensics Conference. 16–30.
5. Arthur, K. K. & Venter, H. S. (2004). An Investigation Into Computer Forensic Tools. ISSA. 1-11.
6. Banday, M. T. (2011). Techniques and Tools for Forensic Investigation of E-mail. International Journal of Network Security & Its Applications. 3, 6.
7. Casey, E. (2004). The need for knowledge sharing and standardization. Digit. Investig. 1, 1, 1–2.
8. Charalambous, E., Bratskas, R., Karkas, G., et al. (2015). An innovative Digital Forensic Tool assisting evidence analysis in Cyprus. 45–54.
9. Crocker, D. (2009). Internet Mail Architecture.
10. Devendran, V. K., Shahriar, H. & Clincy, V. (2015). A Comparative Study of Email Forensic Tools. J. Inf. Secur. 6, 2, 111.