E-Mail Forensics: Techniques And Tools For ForensicInvestigation Of One Court Case

Ljubomir Lazić

Faculty Of Information Technology, Metropolitan University, Belgrade ljubomir.lazic@metropolitan.ac.rs

Case study

DOI: **10.7251/JIT1802064L** UDC: **004.42:004.738.5**

Abstract: E-mail has emerged as the most important application on the Internet for communication of messages, delivery of documents and carrying out transactions and is used not only from computers, but many other electronic gadgets such as mobile phones. This paper is an attempt to illustrate e-mail architecture from forensics perspective. Also, this paper projects the need for e-mail forensic investigation and lists various methods and tools used for its realization. A detailed header analysis of a multiple tactic spoofed e-mail message is carried out in this paper. It also discusses various possibilities for detection of spoofed headers and identification of its originator. Furthermore, difficulties that may be faced by investigators during forensic investigation of an e-mail message have been discussed along with their possible solutions. Our focus is on email header analysis phase offered by the tools. We examine the capability of a particular tools such as EmailTrackerPro and aid4mail in action. The paper describes the court case of cyber crime, the so-called identity theft in Internet communication via electronic mail by two business entities. Identity theft of e-mail addresses and false communications with a foreign company was carried out in order to indicate that a cash transaction of around EUR 100,000 was paid to the account of NN attackers and not to the account in the domestic Serbian bank.

Keywords: E-mail forensic, header analysis, E-mail message as evidence.

Introduction

Modern time communication is impossible without emails. In the field of business communication, emails are considered as its integral part. At the same time, emails are also used by criminals [1,2,4]. In digital forensics, emails are considered as evidence and Email Header Analysis has become important to collect evidence during forensics process [2,3]. Email clients are computer programs that allow users to send and receive emails. Over time, different types of email clients have been invented for the convenience of email users. We will discuss different types of email clients now. Broadly, email clients are divided into two types based on email saving location. These are web-based email clients and desktop-based email clients.

a) Web-based Email Clients: Web-based email clients save all their data to their web server. Some web-based clients are Gmail, Yahoo Mail, Hotmail, etc. The benefit of using web-based email clients is that they can be accessed from anywhere in the world, using Username and Password. One of their disadvantages is the users not knowing where their data is being stored.

b) Desktop-based Email Clients: Desktop-based email clients are the opposite of web-based clients. Outlook, Thunderbird, Mail Bird are some examples of desktop-based email clients. All data of desktop-based web browser is stored in the system of its users. Thus, users do not have to worry about data security. The same point can be considered as a disadvantage in some cases. This is especially the case when it is used in criminal activities, and the evidence cannot be collected from the server [3,5]. E-mail messages include transit handling envelope and trace information in the form of structured fields which are not stripped after messages are delivered, leaving a detailed record of e-mail transactions. A detailed header analysis can be used to map the networks traversed by messages, including the information on the messaging software and patching policies of clients and gateways, etc. Over a period of year's e-mail protocols have been secured through several security extensions and producers, however, cybercriminals continue to misuse it for illegitimate purposes by sending spam, phishing e-mails, distributing child pornography, and hate e-mails besides propagating viruses, worms, hoaxes and Trojan horses. Further, Internet infrastructure misuse through denial of service, waste of storage space and computational resources are costing every Internet user directly or indirectly.

E-mail forensic analysis is used to study the source and content of e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. to collect credible evidence to bring criminals to justice [1-5]. This paper is an attempt to illustrate e-mail architecture from forensics perspective. It describes roles and responsibilities of different e-mail actors and components, itemizes metadata contained in e-mail headers, and lists protocols and ports used in it. It further describes various tools and techniques currently employed to carry out forensic investigation of an e-mail message.

This paper projects the need for e-mail forensic investigation and lists various methods and tools used for its realization. A detailed header analysis of a multiple tactic spoofed e-mail message is carried out in this paper. It also discusses various possibilities for detection of spoofed headers and identification of its originator. Furthermore, difficulties that may be faced by investigators during forensic investigation of an e-mail message have been discussed along with their possible solutions [1,5].

This paper will also discuss tracing e-mail headers and issues associated with it. It will address both HTTP & SMTP initiated e-mails. It will discuss different ways used by e-mail senders to evade tracing and workarounds used by investigators to combat them. It will also discuss advanced measures and techniques used by investigators to track emails [4]. We will discuss particular tools in the paper, such as: *EmailTrackerPro* and *aid4mail* in action.

E-mail Service Architecture

E-mail system comprises of various hardware and software components that include sender's client and server computers and receiver's client and server computers with required software and services installed on each. Besides these, it uses various systems and services of the Internet. The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required [2,3]. E-mail is a highly distributed service that involves several actors which play different roles to accomplish end-to-end e-mail exchange [2]. These actors fall under three groups, namely User Actors, Message Handling Service (MHS) Actors and ADministrative Management Domain (ADMD) Actors. User Actors are Authors, Recipients, Return Handlers and Mediators that represent people, organizations or processes that serve as sources or sinks of messages. They can generate, modify or look at the whole message. Message Handling Service (MHS) Actors are Originators, Relays, Gateways and Receivers which are responsible for end-to-end transfer of messages. These Actors can generate, modify or look at only transfer data in the message. ADministrative Management Domain (ADMD) Actors are Edges, Consumers and Transits which are associated with different organizations and have their own administrative authority, operating policies and trust-based decision making [2].

E-mail system is an integration of several hardware & software components, services and protocols, which provide interoperability between its users and among the components along the path of transfer. The system includes sender's client and server computers and receiver's client and server computers with required software and services installed on each of them. Besides, it uses various systems and services of the Internet [2].

The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required. An e-mail communication, for example, between a sender 'Alice' having e-mail address 'alice@a.com' and recipient 'Bob' having e-mail address 'bob@b.com' is shown in Figure 1.

'Alice' composes an e-mail message on her computer called client for 'Bob' and sends it to her sending server 'smtp.a.org' using SMTP protocol. Sending server performs a lookup for the mail exchange record of receiving server 'b.org' through Domain Name System (DNS) protocol on DNS server [3] 'dns.b.org'. The

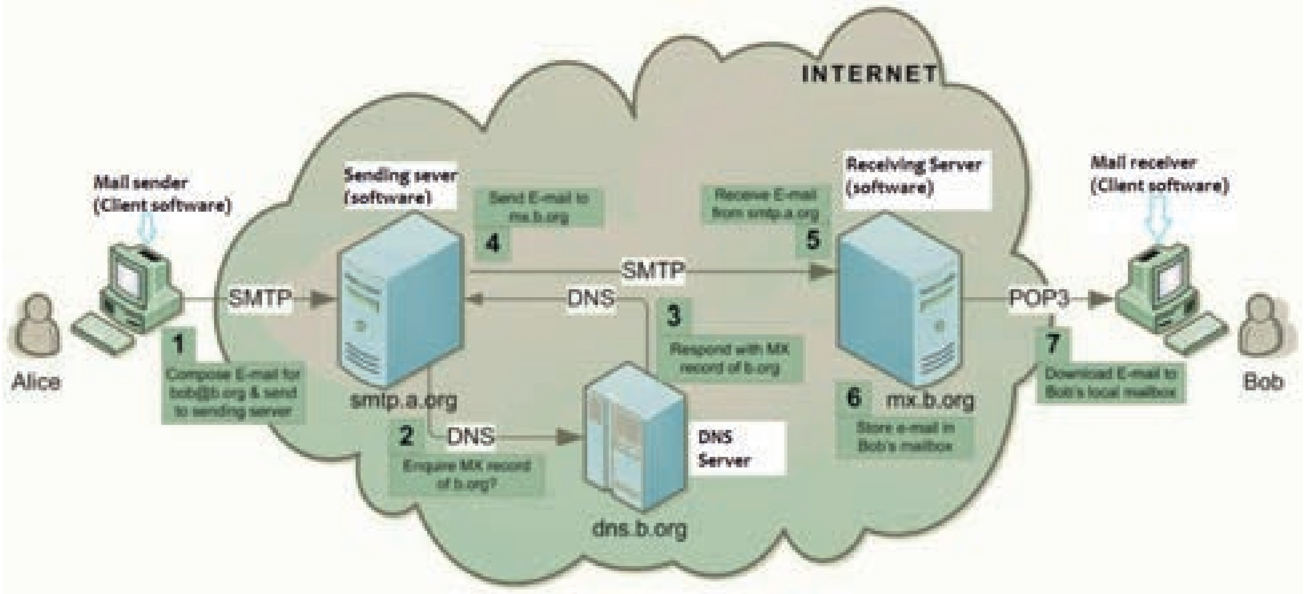

INTERNET
Mail sender
(Client software)
Sending sever
(software)
Send E-mail to mx.b.org
4
SMTP
Receive E-mail from smtp.a.org
5
Receiving Server
(software)
Mail receiver
(Client software)
SMTP
DNS
3
Respond with MX record of b.org
POP3
1
Compose E-mail for bob@b.org & send to sending server
7
Download E-mail to Bob's local mailbox
Alice
smtp.a.org
6
mx.b.org
Bob
2
DNS
Enquire MX record of b.org?
DNS
Server
Store e-mail in Bob's mailbox
dns.b.org

Figure 1. *E-mail communication between a sender 'Alice' and recipient 'Bob' [3]*

DNS server responds with the highest priority mail exchange server 'mx.b.org' for the domain 'b.org'. Sending server establishes SMTP connection with the receiving server and delivers the e-mail message to the mailbox of 'Bob' on the receiving server. 'Bob' downloads the message from his mailbox on receiving server to local mailbox on his client computer using POP3 [3] or IMAP [1] protocols. Optionally, 'Bob' can also read the message stored in his server mailbox without downloading it to the local mailbox by using a Webmail program.

E-mail system is an integration of several hardware and software components, services and protocols which provide interoperability between its users and among the components along the path of transfer. The e-mail architecture shown in Figure 2 below specifies the relationship between its logical components for creation, submission, transmission, delivery and reading processes of an e-mail message. Several communicating entities called e-mail nodes which are essentially software units working on application layer of TCP/IP model are involved in the process of e-mail delivery. Nodes working on lower layers such as routers and bridges which represent options to send e-mail without using SMTP

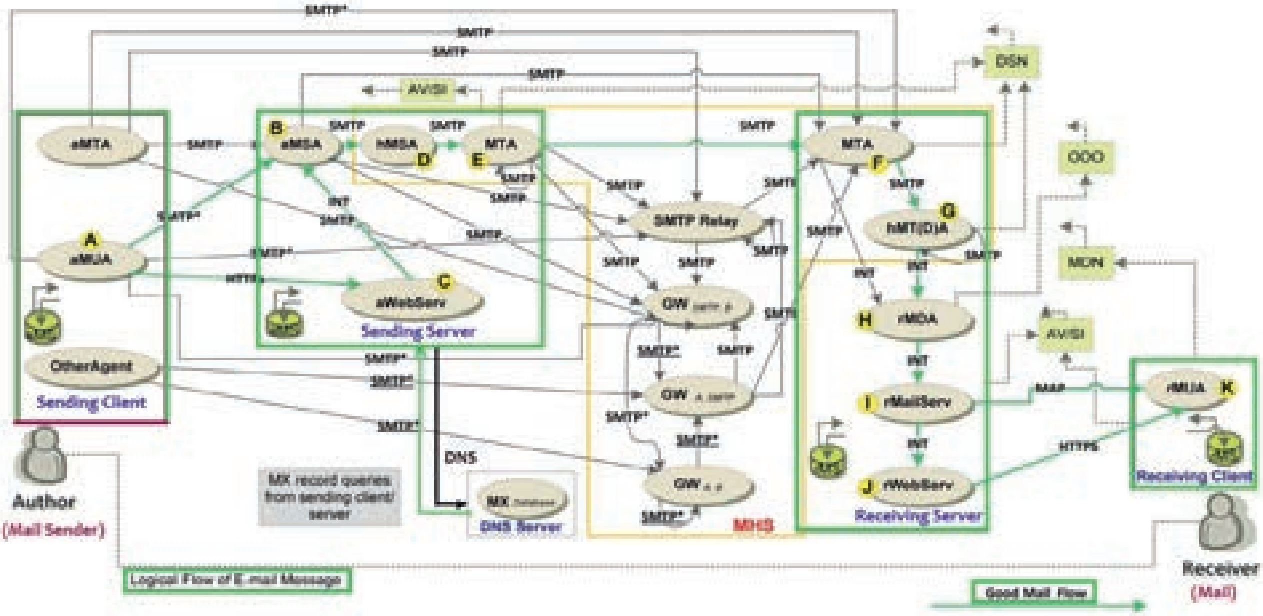


Figure 2. *E-mail Architecture [3]*

are not considered in this architecture because almost all e-mail communication uses SMTP directly or indirectly. Moreover, proprietary nodes used for internal deliveries at sending and receiving servers are also not considered in this architecture.

A mail message from Author to Receiver that traverses through aMUA, aMSA, hMSA, MTA (outbound), MTA (Inbound), hMDA, rMDA, rMailServ and rMUA is considered as good mail by the Sender Policy Forum (SPF). Mails following through other paths are either fully or partially non-SMTP based or uses non-standard transfer modes which are often suspected to contain viruses and spam. Delivery Status Notification (DSN) messages are generated by some components of MHS (MSA, MTA, or MDA) which provide information about transfer errors or successful deliveries and are sent to MailFrom addresses. Message Disposition Notification (MDN) messages are generated by rMUA which provide information about post-delivery processing are sent to Disposition-Notification-To address. Out Of Office (OOO) messages are sent by rMDA to return address [3].

E-mail forensic investigation techniques

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

Various approaches that are used for e-mail forensic are described in [1] and are briefly defined below. E-mail forensic include header analysis, bait tactics, server investigations, and network device investigation. Besides mandatory headers, custom and MIME headers appearing in the body of the message are also analysed for sender mailer fingerprints and software embedded identifiers.

Email Forensics Analysis Steps

A forensic investigation of e-mail can examine both email header and body. This paper will look at header examination.

According to [3] an investigation should have the following:

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

Some other aspects that controls forensics step include the following properties (see Figure 3):

1) Storage format of email: Server side storage format may include maildir (each email is kept separate in a file, for each user), mbox format (all email files are in a single text file). Server-side stores email in SQL Server databases. Reading different types of formats can be done for forensics analysis by using notepad editor and applying regular expression-based searches [5]. At the client-side, an email is stored as mbox format (Thunderbird) [5]. Client side may also store emails as .PST (MSOutlook), and NSF (Lotus Notes) files.

2) Availability of backup copy of email: When checking from the serve side, all copies are transferred to the client. This requires seizing the client computer. For webmail, copies are always saved at the server side [4].

3) Protocol used to transport email: Email can be initiated and transported based on SMTP or HTTP [2] depending on the email server applications.

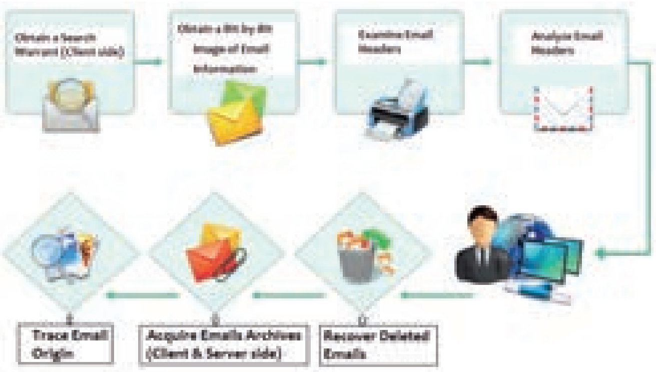

Obtain a Search Warrant (Client side)
Obtain a Bit by Bit Image of Email Information
Examine Email Headers
Analyze Email Headers
Trace Email Origin
Acquire Emails Archives (Client & Server side)
Recover Deleted Emails

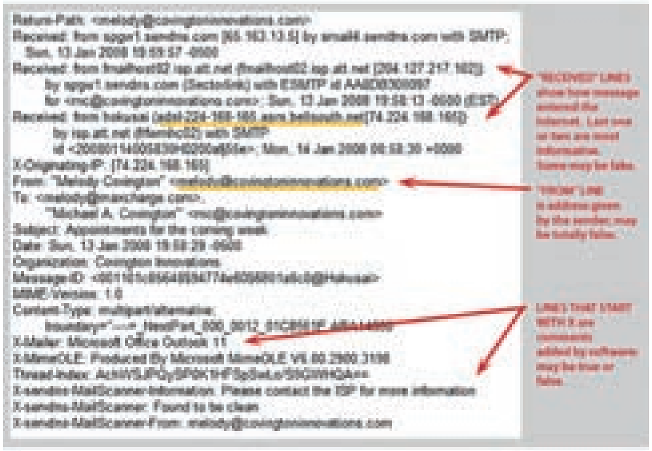
Figure 3. *Broad steps in email forensics for investigator*

Header Analysis

Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis. Besides header analysis, various other approaches that can be used for e-mail forensics include bait tactics, server investigations, and network device investigation. Custom and MIME headers appearing in the body of the message are also analysed for sender mailer fingerprints and software embedded identifiers [2].

Relevance of Headers & Components

Email header forensics basically denotes the examination done on the email message body and the source and path followed by it. This also includes the identification of genuine sender, time, or recipient of the emails. The email header forensic analysis can bring out the candid evidences from various components included in the header part. Let us see Figure 4 which components are helpful for header forensics:



```
Return-Path: <melody@covingtoninnovations.com>
Received: from sgge1.sendns.com [65.163.13.5] by email4.sendns.com with SMTP;
  Sun, 13 Jan 2008 19:59:57 -0500
Received: from fmailhost02.isp.att.net (fmailhost02.isp.att.net [204.127.217.102])
      by sgge1.sendns.com (Sectoolink) with ESMTP id AA8DB30097
      for <mc@covingtoninnovations.com>; Sun, 13 Jan 2008 19:58:13 -0500 (EST)
Received: from hokusai (adsl-224-168-165.asm.bellsouth.net[74.224.168.165])
       by isp.att.net (frfwmhc02) with SMTP
       id <20080114005839H0200a85e>; Mon, 14 Jan 2008 00:58:30 +0000
X-Originating-IP: [74.224.168.165]
From: "Melody Covington" <melody@covingtoninnovations.com>
To: <melody@marchange.com>,
      "Michael A. Covington" <mc@covingtoninnovations.com>
Subject: Appointments for the coming week
Date: Sun, 13 Jan 2008 19:58:29 -0500
Organization: Covington Innovations
Message-ID: <001101c8564a9547[illegible]@Hokusai>
MIME-Version: 1.0
Content-Type: multipart/alternative;
      boundary="----=_NextPart_000_0012_01C8561F.A8A4[illegible]"
X-Mailer: Microsoft Office Outlook 11
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
Thread-Index: AchWSJPQySP0K1HFSp5wLo/S9GWHQA==
X-sendns-MailScanner-Information: Please contact the ISP for more information
X-sendns-MailScanner: Found to be clean
X-sendns-MailScanner-From: melody@covingtoninnovations.com
```

"RECEIVED" LINES show how message entered the Internet. Last one or two are most informative. Some may be false.

"FROM" LINE is address given by the sender; may be totally false.

LINES THAT START WITH X are comments added by software; may be true or false.

Figure 4. *A typical E-mail header*

`X-Apparently-To:` It will reveal recipient's email address while investigating. This can be the validation field for checking email service provider. Generally this field is referred to as "BCC, CC, or To" and is not restricted to "To".

`Delivery To:` This shows the address of the auto-mailer.

`Return-Path:` This field is used for the bounces of email messages. In case the mail server is sending the message and it cannot be delivered.

`Received-SPF:` During email header forensics, this field shows the information of email service used for the sending of mails. It is also having an ID number which is important for log examination for determining the validity of an email. In case of unavailability of the ID, the email must have been spoofed.

`Message ID:` This is a globally used unique identification ID which refers to the genuine time of the emails and version of message. It is highly important to know if investigators want to know whether spoofing is done to the email or not.

`MIME Version:` It stands for Multipurpose Internet Mail Extensions and is an Internet Standard which extends format of message.

`Content-type:` This shows the type of content or format used for the message like; XLML, Text, or HTML.

`X-Mailer:` It displays the email client which is used for sending the message.

`X-Originating-IP&Received:` This is an important field for tracing the IP address used for sending the email. This is the most important message when it comes to the email header forensic analysis as it has to be examined where the mail arrived from.

`DKIM-Signature:` This field stores the signature of an email and all key-fetching information in simple "tag=value" syntax. It is a crucial field to validate the domain name and identity allied to the message via cryptographic authentication.

SECURITY ISSUES IN INTERNET E-MAIL:

A. Secrecy: The content of email is in plain text format. While it is transmitting it never decrypted, so data can be easily revealed if one can get access of your mailbox and one can knows how to tap network and flow.

B. Integrity: Integrity means changes the original data. Email is mainly stored in plain text and also transmitted in plain text. Therefore, anyone can easily hack the way of email transmission and change the original data without being noticed by sender and receiver.

Security Issues In SMTP

Security in information technology is defined as to protect information against unauthorized revelation as well as unauthorized modification. The user needs to take care about possibility of malicious and fraudulent attacks by hackers as well as impact of viruses and denial-of-services attack. Some approaches that are useful for security of your system include:

A. Authentication

The technique can be used to identify and verify if anyone is seeking to access un authorized system.

B. *Access control*

Users can be restricted to ensure they only access data and services for which they have been authorized.

C. Encryption

Techniques that scramble data are used to protect information while data are transmitted over network.

D. Firewall

Firewall is mainly used to differentiate the internal and external information access. Firewall prevents the outsiders to access information within organization.

E. Intrusion detection

Techniques that monitor the system and network to check whether anyone is trying to access network without authentication.

F. Anti-virus software

It can detect viruses and prevent access to infected files.

The Threats to Email Security

A. Viruses

Email security contains multiple issues. Virus is the highest risk issue in network. Virus has capability to destroy complete data at a time. When virus is found in any email it can be bring down the entire mail system, often in a large amount in a single mail.

Many issues can affect the system but virus is stronger than any other. Virus stays long and destroys data immediately. It is not removed by any antivirus product. Virus leaves its impact for a long time and the recovery takes a large amount of money, resources and efforts as well as lost computer information.

B. SPAM

SPAM is another major issue in network security. Viruses and SPAM go hand in hand. Spam is also known as junk email. SPAM mail contains malicious code which affects mail system immediately. SPAM mail contains virus which can bring down the entire system. Users cannot request any mail but them getting number of mails of unintended user which can be a SPAM mail. Mail filtering cannot filter legitimate email from SPAM. Virus and SPAM have negligible difference.

Experiment: Man-in-the-Middle Attack

The main purpose of this experiment is to demonstrate the concept of the man-in-the-middle attack, the attacker being an NN person. This experiment is aimed at capturing data from a suspected user to connect to a WLAN and viewing unauthorized content that certainly happened in this court case. The experiment shows that the unauthorized content accessed by the suspicious user can be collected and can be used for a digital forensic investigation. The reader should take into account that all three actors in this experiment, i.e. router, attacker and legitimate user (see Figure 5), all at the same network address, i.e. 146.64 with the remaining two numbers indicating the address of each host in the network.

Execution of the experiment

In this experiment, a forensic researcher points out that the traffic for this experiment was not encrypted. The D-Link router is configured to be open, which means that no encryption keys such as WEP, WPA2, and WPS are configured.

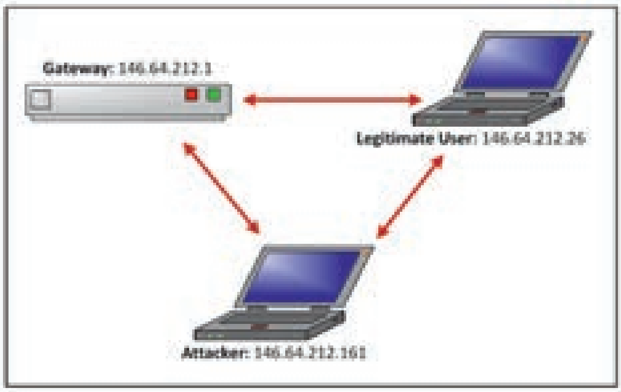


Figure 5. *Participants in an identity theft experiment*

In spite of this, the experiment would continue to be successful, even if encryption is established, although in this case more efforts should be made to crack the passwords first, but it should be emphasized that communication encryption continues to be present as the greatest enemy of forensic scientists.

The main idea of this experiment is that the attacker uses an ARP spoofing mechanism to convince the legitimate user that they are a legitimate participant, device gateway [4]. After the response of a legitimate user, the attacker immediately confirms to the gateway that they are a legitimate user. Both the legitimate user and the gateway will think they have established a relationship with each other, and in fact they have both established a relationship with the attacker. This means that the gateway and legitimate user traffic is directed towards an attacker who can then intercept the communication between the two sides. For the purpose of this experiment, the attacker is only interested in the traffic of a legitimate user suspected of being searched for IMPORTANT online content.

EXAMINING E-MAIL FORENSIC TOOLS: CASE STUDIES

Email analysis, as we already mention, is the task performed in the network forensics. Email analysis is the process which involves analysis of emails sent and received at different ends. In current era, there are very less ways to analyse emails. Most widely accepted method is the Manual Method of Email Analysis [4,5]. Although there have been many attempts into securing e-mail systems, most are still inadequately secured. Installing antiviruses, filters, firewalls and scanners is simply not enough to secure e-mail communication. Some common examples of illegitimate uses of emails are spam, phishing, cyber bullying, botnets, disclosure of confidential information, child pornography and sexual harassment. The anonymity factor of e-mail has made it difficult for digital forensic investigators to identify the authorship of an email, and to aggravate this problem further; there is no standardised procedure to follow.

Therefore, a forensic investigator needs efficient tools and techniques to perform the analysis with a high degree of accuracy and in a timely fashion. It is evident that an email forensic tool may only assist the investigator during a specific stage of analysis [4,5].

While preforming manual method for email analysis, we try to spot spoofed messages which are sent through SMTP (Simple Mail Transfer Protocol). By analysing them we can decode the message being sent. After decoding, all IP addresses are analysed and their location is traced. A timeline of all event is made (in universal standard time) and is checked further for suspicious behaviour. Server logs are checked at the same time to ensure that all the activities are mentioned in the timeline so formed. If any suspicious activity is found, the mails are recovered and can be used as evidence against the sender. Email is extracted from the client server which keeps a copy of sent mails until a specific number.

First case study

First, we will describe a well-known case in court practice i.e. a case study involving the use of Manual Method for Email Analysis [4] using a whaling attack which is a spear-phishing attack directed specifically at high-profile targets like C-level executives, politicians and celebrities:

- An email attached to a $20 million dollar lawsuit purported to be from the CEO of "`tech.com`" to a venture capital broker. The message outlined guaranteed "warrants" on the next round of finding for the broker.
- "`tech.com`" filled counter claim and claimed the email was *forgery*. Their law firm engaged a team to determine the validity of the message.
- The team imaged all of the CEO's computers at his office and his home. Email server backup tapes were recalled from the client servers.
- All hard drivers and email servers were searched for "questioned" message. There were no traces of any such mail on any of the hard drive or mail spool.
- When the time stamps and message id's were compared with the server logs then it was found that the "questioned" message have not gone through either "`tech.com`'s" webmail or mail server at the time indicated by the date/time stamp on the message.
- Based on the analysis the defendants filed motion to image and examine broker's computers.
- Federal judge issued subpoena and the team arrived at the broker's business, he refused to allow his system to image.
- Broker's lawyer went into the state court, on a companion case, and got the judge to issue an order for a new court appointed examiner.
- The examination revealed direct proof of the

alteration of a valid message's header to create a "questioned" email.

The allegedly received email

The header of a problematic e-mail is presented as follows.

```
Return-Path: CEO Good_Guy@tech.com
Received: from mail.tech.com (mail.tech.com
[201.10.20.152])
by hedgefund.fund.com (8.11.0/8.11.0) ESMTP id
e73MfZ331592; Thu, 3 Aug 2000 15:45:31 -0400
Received: from webmail.tech.com (webmail.
tech.com
[10.27.30.190]) by mail.tech.com (Switch-2.0.1/
Switch-2.0.1) ESMTP id e73MfW903843; Thu, 3
Aug 2000 14:41:32 -0500
Received: from tech.com (ostrich.tech.com
[10.27.20.190])
by webmail.tech.com (8.8.8+Sun/8.8.8) with
ESMTP id RAA01318; Thu, 3 Aug 2000 14:41:31
-0500
content-class: urn:content-classes:message
Subject: Warrants on $25 Million Funding
Date: Thu, 3 Aug 2000 14:43:47 -0500
MIME-Version: 1.0
Content-Type: application/ms-tnef;
name="winmail.dat"
Content-Transfer-Encoding: binary
Message-ID: <3989e793.87BDEEE2@tech.com>
X-MS-Has-Attach:
X-MS-TNEF-Correlator: <3989e793.87BDEEE2@
tech.com>
Thread-Topic: Warrants on $25 Million Funding
Thread-Index: AcHatCZUSkaLe0ajEdaelQACpY-
cy8A==
From: "CEO Good_Guy@tech.com" <ceo_good_guy@
tech.com >
To: "Bad_Guy_Broker" <bad_guy@fund.com>
```

Information contained in the header can aid investigators in tracing the sender of the e-mail. A thorough investigation of e-mail headers should include examination of the sender's e-mail address and IP address, examination of the message ID as well as the messaging initiation protocol (HTTP or SMTP). To determine the source of the e-mail, *investigators must first examine the received section at the bottom of the header and work their way up in a bottom to top approach*.

It is also important that e-mail cases examine the logs of all servers in the received chain as soon as possible. Time is very important in e-mail cases as HTTP and SMTP logs are archived frequently; especially by large ISPs. If a log is archived, it could take time and effort to retrieve and decompress the log files needed to trace e-mails. Some e-mails have fake/forged headers in order to deceive investigators, so extreme caution and careful scrutiny should be practiced in investigating every part of the e-mail header.

However, this is quite a bit long and tiring procedure which would involve too many mails to be analysed, which would be excessively time-consuming. Time being the most expensive entity, we need to save the time as much as we can. To save this time certain tools are present which helps to reduce the work burden. So, we need a software tools, such as eMailTrackerPro (http://www.emailtrackerpro.com/) and Aid4Mail Forensic (http://www.aid4mail.com/) that are discussed in the next section.

In this case investigator should look at ESMTP id which is a unique identification assigned by each intermediate relay or gateway server. This id is usually in a hexadecimal string that is reset each day. Resulting in an id that can be resolved to a time window on a particular server. The investigator should also compare the header information against server logs: `webmail@tech.com`. Analysis of the webmail server logs revealed several issues regarding the validity of the suspect message:

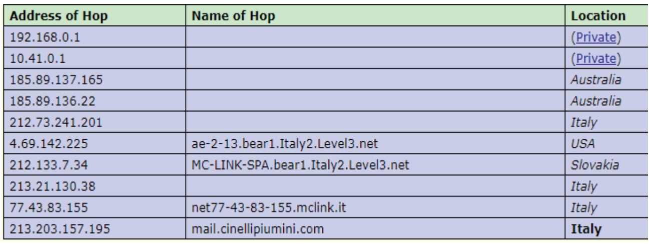
- Matching trace header timestamps and ESMTP ids revealed that RAA01318 was issued at 17:41:31 to the authentic message
- Comparing the 14:41:31 timestamp of the suspect message with the log revealed the server was assigning ESMTP ids beginning with "OAA" not "RRA" as represented in the header.

Analysis of the mail server logs confirmed that the suspect message was not authentic:

- Matching trace header timestamps and ESMTP ids revealed that the authentic Message-ID was logged at 17:41:32 and assigned ESMTP id e73MfW903843 then it was sent to the `hedgefund@fund.com` server and it was assigned a new ESMTP id e73MfZ331592
- Comparing the 14:41:32 timestamp of the suspect message with the log revealed there were no messages for over an hour during that time frame.

Second case study

This section describes the court case of cybercrime so called "identity theft in Internet communication by electronic mail by two business entities". Based on the analysis of the method of communication (e-mails, SMS messages and voice), languages in business correspondence, frequency of transactions, problems in business, ways of solving them in over 100 collected e-mails in communication between two companies during three years of successful cooperation, the author of the work came to indisputable indicators of cybercrime [4]. Identity theft of e-mail addresses and false communication with a foreign company was carried out in order to indicate that a cash transaction of around EUR 100,000 was paid to the account of NN attackers in the London bank, and not to the account in the domestic Serbian bank to which the money was paid up to then in the process of electronic payment of goods and services between the parties to the dispute. The process of examining e-mails is described using the *eMailTrackerPro* tool in the event of identity theft by an NN person (attacker, hacker), an e-mail forensic investigation plan, restrictions, an attacker detection process as the third NN person in an email communication, **Man-in-the-Middle Attack experiment** that served as the basis for forensic analysis of e-mail in the case study. As for this case, it is necessary to see from which address the hacker sent a message, and through which hopes (jumps through the Internet) a message was sent to reach its destination, as can be seen in the following Figure 6 [4].



Address of Hop	Name of Hop	Location
192.168.0.1		(Private)
10.41.0.1		(Private)
185.89.137.165		*Australia*
185.89.136.22		*Australia*
212.73.241.201		*Italy*
4.69.142.225	ae-2-13.bear1.Italy2.Level3.net	*USA*
212.133.7.34	MC-LINK-SPA.bear1.Italy2.Level3.net	*Slovakia*
213.21.130.38		*Italy*
77.43.83.155	net77-43-83-155.mclink.it	*Italy*
213.203.157.195	mail.cinellipiumini.com	**Italy**

Figure 6. *Hopes through which the hacker's mail passed*

As far as the hopes through which the message goes, we can see that it is a little unusual that everything is going from Italy, going to the server in Slovakia, to the US (forged email address of `xxxxx@yahoo.com`), then back to Italy and then to Australia. The following Figure 7 will show the path on the map as the message was traveling.

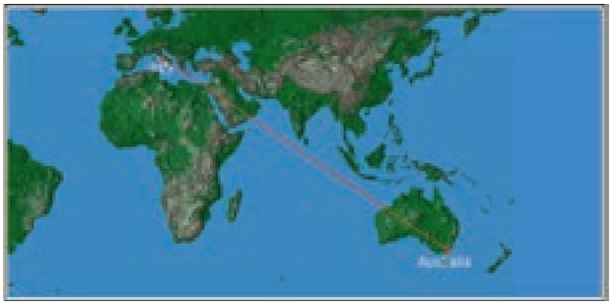


Figure 7. *Path on the map the message travelled*

After this knowledge, it was necessary to analyse other suspicious e-mails, as well as the email server on the victim's side, as we have described earlier. It was found that during the time of the hacker attack, the actual sender did not send any messages. There are many tools which may assist in the study of source and content of e-mail message so that an attack or malicious intent of the intrusions may be investigated. This section introduces some of these tools: eMailTrackerPro and Aid4Mail Forensic.

Software eMailTrackerPro [5] is a proprietary email forensic solution that analyses email files stored in local disk and supports automatic email analysis for the identification of spamming incidents. eMailTrackerPro is capable of recovering the IP address that sends the message along with its associated geographical location (city) to determine the threat level or validity of an e-mail message. It can find the network service provider (ISP) of the sender. A routing table is provided to identify the path between the sender and receiver of an email. It also can check a suspected email against Domain Name Server blacklists to safeguard against spam.

The *disadvantage* associated with this software is that it would be unable to find a spammer which is not blacklisted into its database.

Add4Mail forensic software tool

This is another tool developed for helping in the mail sorting purpose only. This software can find emails which can be searched by any particular keyword. As with *EmailTrackerPro* and on this tool, we need to configure our mail. Let us choose which mail we will use for analysis. In this case, we will use *gmail*. Once we have completed the mail configuration, we are going to the next step that allows us to select the time frame in which we want to search for mail by keywords, and in the window where Vaccky,

VacckY, etc., are located. It is actually a keyword search box as in Figure 8.

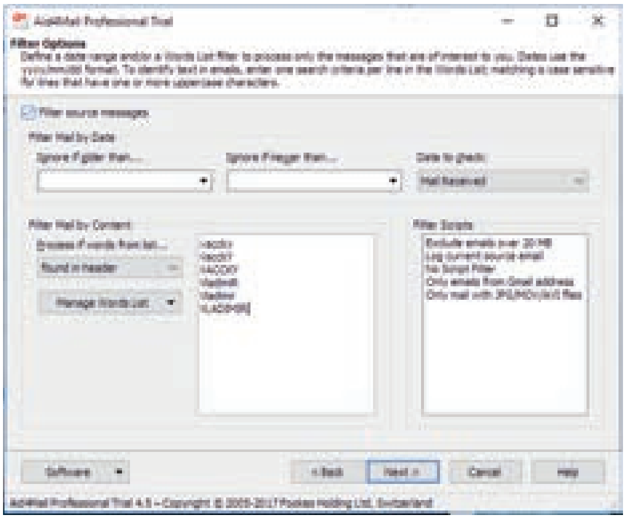


Figure 8. *Example: Search keywords for a mailbox by Add4Mail*

The output provided by this software program is the message written in the email along with the date, time and other information specific to the mail as in Figure 9. This software program can also be used to fetch some deleted mails from their trash folder. Unlike email tracker pro, this tool does not only serve to track the message, but also for detailed forensic mail analysis. This tool can be found at http://www.aid-4mail.com/, but unlike *EmailTrackerPro* it is not an open source, you must actually purchase a license.

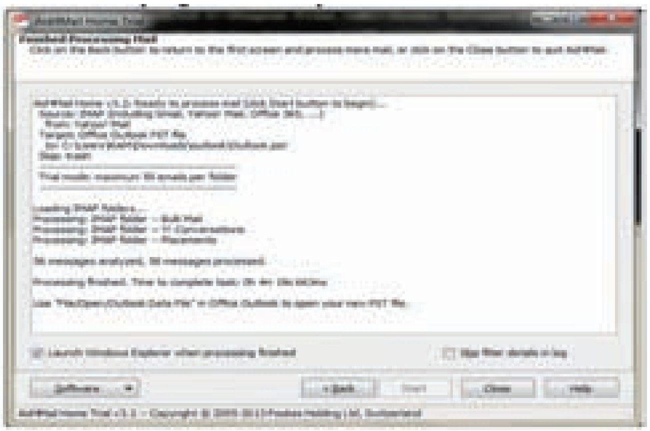


Figure 9. *Example of processing mail by Add4Mail*

The major *disadvantage* of this software is that it can only find keywords that the user searches. It has no artificial intelligence and therefore is a completely manual software program developed to sort and find mails.

Conclusion

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 have demonstrated two forensic tools that can be utilised for email analysis emphasising on their key features in an effort to assist investigators in the selection of the appropriate tools.

High-tech crime, also known as e-crime or cyber-crime, includes a set of offenses that involve the use of the Internet, a computer, or some other electronic device. This paper describes the court case of cyber-crime, the so-called identity theft in Internet communication via electronic mail by two business entities. Based on the analysis of the method of communication (e-mails, SMS messages and voice), languages in business correspondence, frequency of transactions, problems in business, ways of solving them in over 100 collected e-mails in communication between two companies during three years of successful cooperation, the author of the research came to indisputable indicators of cyber-crime. Identity theft of e-mail addresses and false communications with an Italian firm was carried out in order to indicate that a cash transaction of around EUR 100,000 was paid to the account of NN attackers in the London Bank, and not to the account in the domestic Serbian bank to which the money had been paid by then in the process of electronic payment of goods and services between the parties to the dispute.

Acknowledgements

This research was financially supported by the Ministry of Science and Technological Development of the Republic of Serbia, as part of the TR35026 "Software Environment for the optimal management of the quality software development process" project.

References

[1] Al-Zarouni M (2004) Tracing E-mail Headers, Australian Computer, Network & Information Forensics Conference, pp. 16–30.

[2] Banday MT (2011) Analysing E-Mail Headers for Forensic Investigation, Journal of Digital Forensics, Security and Law, Vol. 6(2).

[3] Banday MT (2011) Techniques and Tools for Forensic Investigation of E-mail, International Journal of Network Security & Its Applications, Vol. 3, No. 6.

[4] Lazic Lj (2018) E-Mail Forensics: The Case From The Court Practice Of Theft Of Identity, Conference: ITeO2018, 28. September, Banjaluka, pp. 368- 383.

[5] Mrityunjay UC et al. (2017) Novel Approach for Email Forensics, International Journal of Engineering Research & Technology (IJERT), Special Issue.

Submitted: November 10, 2018
Accepted: November 23, 2018

About the authors

Ljubomir Lazić was born on December 18, 1955. He is software engineering and computer science professor at METROPOLITAN University, Belgrade, Serbia. He received the bechelor degree in electrical engineering from School of Electrical Engineering, Belgrade University in 1979. He was a Post-Doctoral Researcher at The WSEAS (The World Scientific and Engineering Academy and Society) of computer science from 2009 to 2010. He successfully defended PhD thesis: "Integrated and Optimized Software Testing Process" in January, 2007 at University of Belgrade, Faculty of Electrical Engineering.

So far, he have authored over 100 research papers. Courses teach: Software Engineering, Software Project Management, Software Testing, Human Computer Interaction, Component Based Engineering. Current research interests are: Optimal software project management, Software Metrics, Effort Estimation Modeling etc. He continue to serve industry in a variety of roles, including consulting, executive education, and expert testimony.

For citation

Ljubomir Lazić, E-Mail Forensics: Techniques And Tools For ForensicInvestigation Of One Court Case, *JITA – Journal of Information Technology and Applications*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 8(2018) 2:64-74, (UDC: 004.42:004.738.5), (DOI: 10.7251/JIT1802064L), Volume 8, Number 2, Banja Luka, december 2018 (45-96), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004