Investigating E-Mail Attacks

MODULE 17

Contents

Investigating E-Mail Attacks

17.1 LEARNING OBJECTIVES

After the completion of this unit the learner shall be able to:

- **Define Email Forensics**
- **Identify email information necessary for forensics investigation**
- **Use few email forensic tools.**

17.2 EMAIL FORENSICS

17.2.1 Forensically important email parts

Basically emails information which will be interesting to the investigators are:

a) **Email header**
b) **Body of Emails**
c) **The information hidden in the email packets**
d) **Attachments**

The message header must include at least the following fields:

- ***From*: The email address, and optionally the name of the author(s). In many email clients not changeable except through changing account settings.**
- ***Date*: The local time and date when the message was written. Like the *From:* field, many email clients fill this in automatically when sending. The recipient's client may then display the time in the format and time zone local to him/her.**

The message header should include at least the following fields:

- ***Message-ID*: Also an automatically generated field; used to prevent multiple deliveries and for reference in In-Reply-To: (see below).**
- ***In-Reply-To*: Message-ID of the message that this is a reply to. Used to link related messages together. This field only applies for reply messages.**

RFC 3864 describes registration procedures for message header fields at the IANA; it provides for permanent and provisional message header field names, including also fields

defined for MIME, netnews, and http, and referencing relevant RFCs. Common header fields for email include:

- *To*: The email address(es), and optionally name(s) of the message's recipient(s). Indicates primary recipients (multiple allowed), for secondary recipients see Cc: and Bcc: below.
- *Subject*: A brief summary of the topic of the message. Certain abbreviations are commonly used in the subject, including "RE:" and "FW:".
- *Bcc*: Blind carbon copy; addresses added to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients.
- *Cc*: Carbon copy; Many email clients will mark email in one's inbox differently depending on whether they are in the To: or Cc: list.
- Content-Type: Information about how the message is to be displayed, usually a MIME type.
- *Precedence*: commonly with values "bulk", "junk", or "list"; used to indicate that automated "vacation" or "out of office" responses should not be returned for this mail, e.g. to prevent vacation notices from being sent to all other subscribers of a mailing list. Sendmail uses this header to affect prioritization of queued email, with "Precedence: special-delivery" messages delivered sooner. With modern high-bandwidth networks delivery priority is less of an issue than it once was. Microsoft Exchange respects a fine-grained automatic response suppression mechanism, the X-Auto-Response-Suppress header.
- *References*: Message-ID of the message that this is a reply to, and the message-id of the message the previous reply was a reply to, etc.
- *Reply-To*: Address that should be used to reply to the message.
- *Sender*: Address of the actual sender acting on behalf of the author listed in the From: field (secretary, list manager, etc.).
- *Archived-At*: A direct link to the archived form of an individual email message.

SMTP defines the *trace information* of a message, which is also saved in the header using the following two fields:

- *Received*: when an SMTP server accepts a message it inserts this trace record at the top of the header (last to first).
- *Return-Path*: when the delivery SMTP server makes the *final delivery* of a message, it inserts this field at the top of the header.

Other header fields that are added on top of the header by the receiving server may be called *trace fields*, in a broader sense.

- *Authentication-Results*: when a server carries out authentication checks, it can save the results in this field for consumption by downstream agents.

- ***Received-SPF***: stores results of Sender Policy Framework (SPF) checks in more detail than Authentication-Results.
- ***Auto-Submitted***: is used to mark automatically generated messages.
- ***VBR-Info***: claims VBR whitelisting. Vouch by Reference (VBR) is a protocol for adding third-party certification to email.

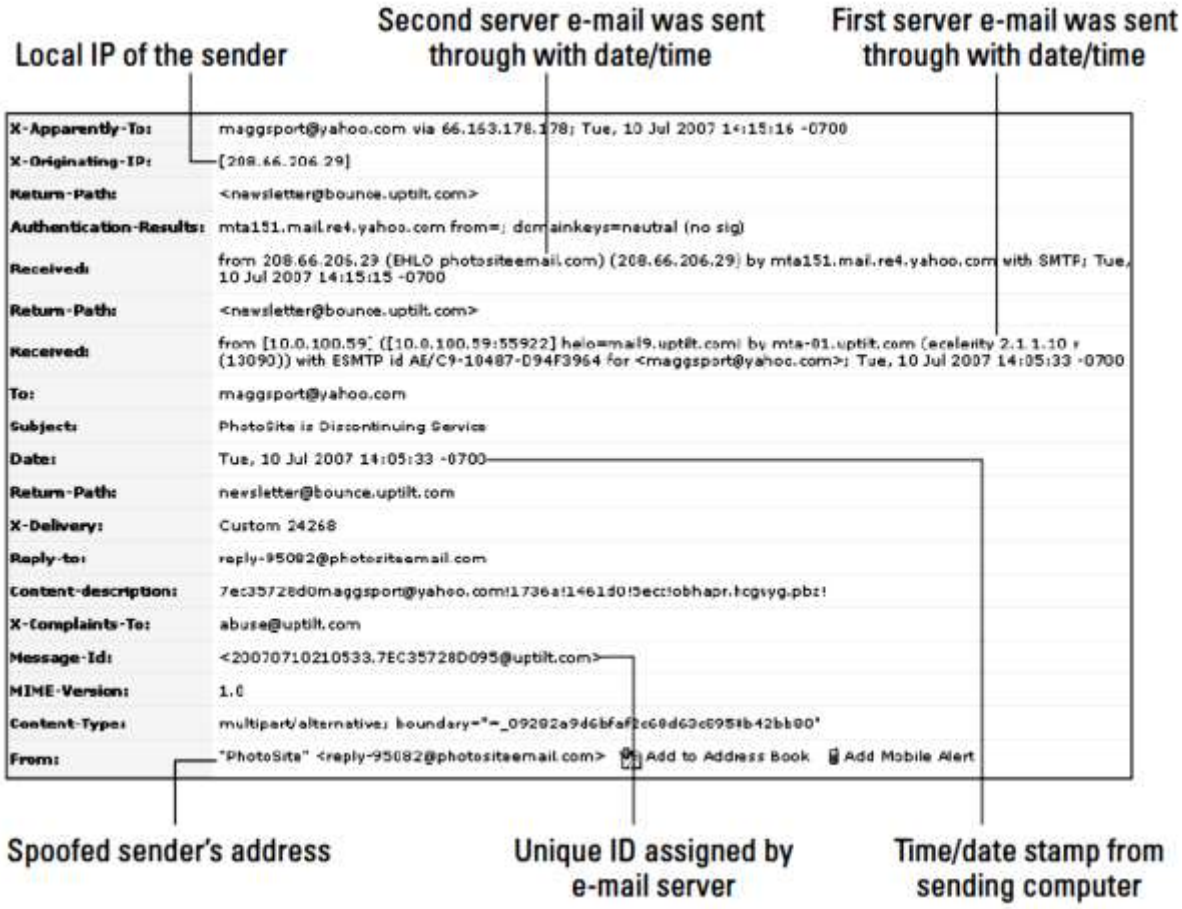

Figure 1: Tracing spoofed sender.

The trace information of an email can provide lots of clues to the investigators.

The email packets can be captured using packet sniffer software. The email packets can be read very easily unless the user is having email encryption. The encrypted emails are read using the password cracking methodologies as discussed in earlier chapters. The trace of an email, headers and even sometimes the body of the email can be used detect a spoof attack as shown in *Figure 1*.

17.2.2 Email forensics investigation

Email forensics involves capturing, securing and analysing and reporting the email evidences. E-mail forensics aims to study the source and contentsof e-mail messages for evidence, this

included identification of the actual sender, recipient, date and time when it wassent, etc. Email Forensic analysis aims at discovering the history ofa message and confirming identity of all involved entities. Apart from message analysis, e-mailforensic also involves investigation of clients or server computers suspectedof being used or misused to carry out e-mail forgery. It might involve inspection of *Internetfavorites*, *Cookies, History, Typed URL's, Temporary Internet Files, Auto-completionEntries, Bookmarks, Contacts, Preferences, Cache*, etc. Several OpenSource software tools are available which helps to perform e-mail header analysisto collect evidence of e-mail fraud.

17.2.3 Analyzing an email

A sample header set of an e-mail message sent by *abc@xyz.com* pretending to be *alice@alice.com* and sent to *bob@bob.com* is shown in figure 3.

1 ***X-Apparently-To:*** *bob@bob.com via a4.b4.c4.d4; Tue, 30 Nov 2010 07:36:34 -0800*
2 ***Return-Path:*** *< alice@alice.com >*
3 ***Received-SPF:*** *none (mta1294.mail.mud.bob.com: domain of alice@alice.com does not designate permitted sender hosts)*
4 ***X-Spam-Ratio:*** *3.2*
5 ***X-Originating-IP:*** *[a2.b2.c2.d2]*
6 ***X-Sieve:*** *CMU Sieve 2.3*
7 ***X-Spam-Charsets:*** *Plain='utf-8' html='utf-8'*
8 ***X-Resolved-To:*** *bob@bob.com*
9 ***X-Delivered-To:*** *bob@bob.com*
10 ***X-Mail-From:*** *alice@alice.com*
11 ***Authentication-Results:*** *mta1294.mail.mud.bob.com from=alice.com; domainkeys=neutral (no sig); from=alice.com; dkim=neutral (no sig)*
12 ***Received:*** *from 127.0.0.1 (EHLO mailbox-us-s-7b.xyz.com) (a2.b2.c2.d2) by mta1294.mail.mud.bob.com with Journal of Digital Forensics, Security and Law, Vol. 6(2)56 SMTP; Tue, 30 Nov 2010 07:36:34 -0800*
13 ***Received:*** *from MTBLAPTOP (unknown [a1.b1.c1.d1]) (Authenticated sender: abc@xyz.com) by mailbox-us-s-7b.xyz.com (Postfix) with ESMTPA id 8F0AE139002E for <bob@bob.com>; Tue, 30 Nov 2010 15:36:23 +0000 (GMT)*
14 ***From:*** *"Allice" <Alice@a.com>*
15 ***Subject:*** *A Sample Mail Message*
16 ***To:*** *"Bob Jones" <bob@bob.com>*
17 ***Content-Type:*** *multipart/alternative; charset="utf-8"; boundary="KnRl8MgwQQWMSCW6Q5=_ HgI2hw Adah5NLY"*
18 ***MIME-Version:*** *1.0*
19 ***Content-Transfer-Encoding:*** *8bit*
20 ***Content-Length:*** *511*
21 ***Reply-To:*** *"Smith" <smith@smith.com>*
22 ***Organization:*** *Alices Organization*
23 ***Date:*** *Tue, 28 Nov 2010 21:06:22 +0530*
24 ***Return-Receipt-To:*** *smith@smith.com*
25 ***Disposition-Notification-To:*** *jones@jones.com*
26 ***Message-Id:*** *<20101130153623. 8F0AE139002E@mailbox-us-s-7b.xyz.com>*

Figure 2: Elaborate email header of a spoofed email. (adapted from: [6])

The Header *X-Apparently-To* shown in Figure 2 is relevant when mail has been sentas a BCC or to recipients of some mailing list. This field in most of the casescontain the address as in

Tofield. But if mail has been sent to a BCC recipient ora mailing list, *X-Apparently-To* is different from *TO* field. Some may show *TO*while others may not show it. Thus *X-Apparently-To* always shows the e-mailaddress of recipient regardless of whether mail has been sent using *TO*, BCC, CCaddresses or by the use of some mailing list.

The *Return-Path* header is the e-mail address of the mailbox specified by thesender in the *MailFrom*command. This address can also be spoofed, if noauthentication mechanism is in place at the sending server it is not possible to determinegenuineness of Return-Path header through header analysis alone.The *Received-SPF* specifies thatthe mail has come from a domain which either does not have a SPF record or isnot yet a designated permitted sender.

If there are some spam filtering software of the receiving serveror MUA the spam score is contained in *X-Spam-Ratio* field. If this value for the e-mail under study ratio exceeds certain pre-defined threshold, emailwill be classified as spam.

X-Originating-IP* specified the IP address of the last MTA of the sending SMTPServer, which has delivered the e-mail to the server of *bob@bob.com*. In thesample e-mail it is *[a2.b2.c2.d2]* as shown in item 5. This address is alsocontained in the *Received* header field.*X-Sieve* header specifies the name and version of message filtering system. Thispertains to the scripting language used to specify conditions for message filteringand handling. In the sample e-mail the name of the message filtering software is*CMU Sieve* and its version is *2.3.X-Spam-Charsets* header specifies the character set used for filtering themessages. The value for this field in sample e-mail at item 7 indicates that 8-bitUnicode Transformation Format (*UTF*) has been used by bob's server. UTF is avariable length character set having a special property of being backwardcompatibleto ASCII.*X-Resolved-To* address is the e-mail address of the mailbox to which the mail hasbeen delivered by MDA of bob's server. In most cases, it is the same as XDelivered-To field. *X-Delivered-To* is the address of the mailbox to which themail has been delivered by MDA of bob's server. In the sample e-mail both *XResolved-To and X-Delivered-To* addresses are *bob@bob.com* as in item 8 and 9.*X-Mail-From* header specifies the e-mail address of the mailbox specified by thesender in the *MailFrom*command which in the sample e-mail is *alice@alice.com*.The *Authentication-Results* header in item 11 indicates that*mta1294.mail.mud.bob.com* received mail from *alice.com* domain which neitherhas DomainKeys signature nor DKIM signature.item 12 is the second *Received* header field containing the trace informationindicating *127.0.0.1* as the IP address of the machine that send the message. Thismachine is actually named *mailbox-us-s-7b.xyz.com* and has IP address*a2.b2.c2.d2*. It has used *EHLO* SMTP command to send the mail. The mail wasreceived by *mta1294.mail.mud.bob.com* using *SMTP*. The message has beenreceived on *Tue, 30 Nov 2010* date at *07:36:34* time. The clock is 8 hrs behindGreenwich Mean Time. Item 13 is the first *Received* header field representing the trace informationindicating *MTBLAPTOP* as the names of the machine that send the message. Thismachine is not known to the receiver but has an IP address *a1.b1.c1.d1* and*abc@xyz.com* is the owner of the mailbox who has sent the message. TheMTA must follow some authentication mechanism to identify its mailbox usersotherwise it is not possible to include authenticated sender's mailbox address withthe *Received* field. The message has been received by *mailbox-us-s-

7b.xyz.com using *ESMTPA* protocol which has been running a program called *Postfix*. Themessage is for *bob@bob.com* and has an ID of *8F0AE139002E*. The message hasbeen received on *Tue, 30 Nov 2010 at 15:36:23*. The clock is set according toGreenwich Mean Time. The *From*, *Subject* and *To*lines respectively are the e-mail address of the author,subject of the message, and the e-mail address of the intended recipient. *Subject*and *To*are specified by the sender, and the *From* address is taken by the systemfrom the current logged in user. However, *From*header can very easily bespoofed as has been dome in this sample e-mail. The items 14, 15 and 16 inthe sample e-mail show the values of these three fields. The *From*address hasbeen spoofed to carry an address *Alice@a.com* with a user friendly name *Alice*.Content-Type, MIME-Version, Content-Transfer-Encoding and Content-length in items 17, 18, 19 and 20 are the MIME headers describing the type of MIMEcontent, transfer encoding, its version and length so that the MUA's can performproper decoding to render the message successfully on client.This is the address, sender of this e-mail wants recipient to use for sending replyin response to this e-mail. Normally, this is used by the senders to send replies.Carefully crafted sender spoofing combined with fake *Reply-To* e-mail addresscan lead to serious information leaks. The *Reply-To* address *"Smith "smith@smith.com* in item 21 is an arbitrary address that may belong to some userwho may not be related to the sender in any way.

Organization header field indicates that the organization of claimed sender is*Alices Organization*. *Organization* header field is an information fieldrepresenting the organization of a sender. It can be misused by the spammer togive a false impression about a sender as has been done in this e-mail.

Date header indicates that the e-mail was composed and submitted for delivery on*Tue, 28 Nov 2010 21:06:22 +0530*, which is not in conformity with the date inthe *Received* field of Para 23.*Return-Receipt-To* field indicates the e-mail address, MSA, MTA and MDA mustuse for sending delivery notifications such as successful or failure notifications.The address mentioned for this field in item 24 is again an arbitrary address thatmay belong to some user who may not be related to the sender in any way.*Disposition-Notification-To* field indicates an e-mail address, MUA must usewhen submitting a message indicating that the message has been displayed. This address specified in item 25 is also an arbitrary address that does belong to someuser who may not be related to the sender in any way.item 26 contains the *Message-Id* of the message which is

20101130153623.8F0AE139002E@mailbox-us-s-7b.xyz.com. Generally, adomain name is appended with a unique number by the sending server to form the*Message-Id*. In the above sample e-mail message, several fields have been spoofed which canbe detected easily because the first *Received* field shows the address ofauthenticated sender which is different from the sender of the message. However,address of authenticated sender may not be always included with theauthentication results (in case no authentication mechanism is adhered to orannomizers strip this line). Further, date is also inconsistent as can be noted fromthe comparison of timestamp in *Received* headers and the date field. Some headerfields with context to authentication and above analysed e-mail message arediscussed further hereby:

SPF mechanisms **can be used to describe the set of hosts which are designatedoutbound mailers for the domain. The test besides success or failure may alsoresult into** ***softfail, neutral, none, permerror*****or** ***temperror*****. For example, asuccessful** ***Received-SPF*** **entry could be as follows:**

Received-SPF**: pass (mta1104.mail.mud.xyz.com: domain of abc@xyz.com designates a2.b2.c2.d2 as permitted sender)Here, the** ***mta1104.mail.mud.xyz.com MTA*** **notifies its recipient through*****Received-SPF*** **that domain of abc@xyz.com i.e.** ***xyz.com*** **which has an** ***IP*****address** ***a2.b2.c2.d2*** **is a permitted sender designated by Sender Policy Framework. In case, the domain** ***alice.com*** **had usedDomainKeys and DKIM complaint andhad passed these tests, it could have been as follows:**

Authentication-Results: **mta1294.mail.mud.bob.com from=alice.com;**
domainkeys=pass (ok); from=a.com; dkim=pass (ok)

In this case, it could have included DKIM-Signature and/orDomainKey-Signature fields as follows:

DKIM-Signature: **v=1; a=rsa-sha1; c=simple; d=alice.com;**
h=from:to:subject:date:message-id:content-type q=dns/txt; s=s512;
bh=XX……=; b=XXX……==;

This is the DKIM Signature signed with SHA1 algorithm. DKIM uses the emailheaders and body to generate a signature. If the headers are rewritten or text is appended to the message body after it has been signed, the DKIM verificationfails. DKIM is backward compatible with the DomainKeys system. When an emailmessage is signed with DKIM, it will include a number of "tags" whosevalues contain authenticating data for the message being sent. In the example email header in figure 3, the tags used are:

v= This tag defines the version of this specification that applies to thesignature record.
a= The algorithm used to generate the signature (plain-text;REQUIRED). It supports "rsa-sha1" and "rsa-sha256", Signersusually signs using "rsa-sha256".
c= It is the canonicalization algorithm 1.e. the method by which theheaders and content are prepared for presentation to the signingalgorithm.
d= It is the domain name of the signing domain.
h= It is a colon-separated list of header field names that identify theheader fields presented to the signing algorithm.
q= It specifies the query method used to retrieve the public key whichby default is dns.
s= It is the selector used in the public key.
bh= The signature data or public key, encoded as a Base64 string.

The example of DomainKeys signature is given below. DomainKeys signaturehas been signed with SHA1 algorithm.

DomainKeys-Signature: **a= rsa-sha1; q=dns; c=simple; s=s512;**
d=alice.com; b=XXX……==;

When an e-mail message is signed with DomainKeys, it will include a number of"tags" whose values contain authenticating data for the message being sent. In theexample above, the tags used are:

a= It is the encryption algorithm used to generate the signature which bydefault is "rsa-sha1".

q= It specifies the query method used to retrieve the public key which bydefault is dns.

c= It is the canonicalization algorithm 1.e. the method by which theheaders and content are prepared for presentation to the signingalgorithm.

s= It is the selector used in the public key.

d= It is the domain name of the signing domain.

b= The signature data or public key, encoded as a Base64 string.

***Date header* represents the date e-mail was composed and submitted for delivery.However, this filed can also be spoofed as has been done in thissample e-mail message. It can be easily noticed by comparing its value in item 23with the dates in the *Received* header fields.**

***Message-Id* is the message Identification attached to the e-mail message. Every e mail has a unique message ID that helps the administrators to locate the e-mail inserver log. Usually every sending server uses its own custom algorithm togenerate this unique number and append domain name to this to make it uniqueon the internet. This ID can also help to identify the domain of the sender but itcan also be forged to confuse the investigators.**

The first *Received* header field representing the trace information contains the IPaddress of the machine used to send the e-mail message. On tracking this IPaddress several cases as explained below are possible:

i. **The IP address in the *Received* header field maps to directconnection having a static IP address. In this case, this address isthe address of the sender's computer. However, if the IP address isdynamic then the logs of the proxy or SMTP server need to beobtained for continuing the e-mail tracking.**
ii. **The IP address contained in the *Received* header corresponds tosome proxy server. In this case, proxy server's log must be obtainedto track the sender. Open proxy server may raise some issues for theinvestigators because they do not maintain a strict log of activities.In case SSL is used to log on to *HTTP* based e-mail server, proxycannot be an issue because IP address of the client shall berecorded. Corporate proxy servers may not be strictly timesynchronized as they may be using Network Time Protocol (*NTP)*and thus may impede the investigation. *ISP* proxy servers usuallymaintain a strict and time synchronized log (using*STIME* protocol)and have a clear devised policy to cooperate with the investigators.**
iii. **The tracked IP address maps to some tunnelling server. In this case,tracking source of e-mail will be difficult because tunnelling maybe done in different ways and some are not logged.**
iv. **The IP address in the *Received* header field maps to SMTP server.In this case, the SMTP server log must be obtained. IP address maymap to SMTP server belonging to**

ISP, or some corporate or anopen relay. In all cases, logs stored must be obtained. If the logs arestrictly time synchronized, then the sender can be tracked easily.ISP and corporate SMTP servers can provide further details aboutthe particular user such as his contact details and credit card number.

v. The IP address contained in the *Received* field resolves to Annomizers or re-mailers. In this case, investigators must obtainlogs and original e-mail message from the anonymous SMTP orHTTP servers. Further, in case the anonymity is a paid service, useraccount details must also be obtained. It is also possible to add one or more false *Received* headers in the data field ofthe message with an intention to freeze the investigation. Investigators must paycareful attention to all fields of the *Received* headers with respect to each otherespecially in terms of delivery methods and date & time. If the delivery methodsvary or the time & date differ considerably, then false headers can be easilyidentified. Otherwise, the investigation shall have to investigate all IP addressesand request logs from all servers. It may be very difficult to track a sender fromthe IP address if the sender has tampered IP address at packet level. Once the source of the e-mail message under investigation has beendetermined or someone is strongly suspected for being the source, his or hercomputer, e-mail client software, web browser, etc. are investigated for traces ofevidence.

17.2.4 Instant Messages

Instant Messages (IM) (as mostly referred as chats) has been becoming very popular among users. Emails are mostly attached to inboxes whereas the IMs are based on text cells or forms. Texting on mobile devices has become very popular nowadays with apps like Whatsapp.

IMs too are very important to forensic examiners because nowadays companies are using this form of communicationfor real-time customer service and internal business communication.On the peopleperspective, IMs are used to chat about everything from recipes to personal attributes or opinions. Chats are relayed by way of a server. Same goes for IMs too. IM software are structurally same as e-mail systems the only difference is that IMs are done in real time.

at real-timesits necessary to logthe data (communication) as it is being typed. Recovering chat sessions is a matter of chance because the caching abilities of the computer is the elementthat is required to re-create the chat sessions. Some IM software logs conversations, but generally people don't activate the logs. IMsare migrating to mobile devices like google hangouts etc., IMs in mobiles are somewhat differentfrom desktop computers. The mobile devices are limited in resources or power of conventional desktopcomputers and they therefore use memory differently. Mobiledevices do not cache data in the same way asdesktops;hence, retrieving chats are much more difficult in mobile devices. If we are recording the IMs we can get all the chats. However, it is very difficult looking at the power and other limitations.Logging the activities on client device might help but finding a complete conversationin memory is almost impossible unless chat logging is enabled.

17.3 EMAIL FORENSIC TOOLS

Various software tools have been developed to assist e-mail forensicinvestigation. These include eMailTrackerPro(http://www.emailtrackerpro.com/), EmailTracer (http://www.cyber forensics. in), Adcomplain(http://www.rdrop.com/users/billmc/adcomplain.html), Aid4Mail Forensic(http://www.aid4mail.com/), AbusePipe(http://www.datamystic.com/ abusepipe.html), AccessData's FTK (www.accessdata.com/), EnCase Forensic (http://www.guidancesoftware.com), FINALeMAIL(http://finaldata2. com), Sawmill-GroupWise (http://www.sawmill.net), Forensics Investigation Toolkit (FIT)(http://www.edecision4u. com/FIT.html), Paraben (Network) E-mail Examiner(http://www.paraben.com/email-examiner.html), etc. These analyse headers of emailmessages to detect the IP address of the originating machine. These toolsoften have abuse reporting features, e-mail classification option, support multipleencryption techniques like Credant, SafeBoot, Utimaco, EFS, PGP, GuardianEdge, Sophos Enterprise and S/MIME. Its current supported e-mail types are:Lotus Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX,Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.),Netscape, AOL and RFC 833. Some of these claim to be vetted by courts asstandard digital investigation platforms.
We will discuss eMailTracker Pro and EmailTracer in little detail.

17.3.1 eMailTrackerPro[1]

Email tracking is a method for monitoring the email delivery to intended recipient. Most tracking technologies use some form of digitally time-stamped record to reveal the exact time and date that an email was received or opened, as well the IP address of the recipient.

Email tracking is useful when the sender wants to know if the intended recipient actually received the email, or if they clicked the links. However, due to the nature of the technology, email tracking cannot be considered an absolutely accurate indicator that a message was opened or read by the recipient.

eMailTrackerPro Standard lets you trace email back to its source, while also scanning each email message to filter out spam and harmful payloads.

Using information contained in the email header, eMailTrackerPro Standard can effectively locate the city or town that an email originated from, including Whois information that you can use to report abuse and shut them down for good. The procedure is as follows:

1. **Trace an email using the header: To make the best use of eMailTrackerPro it's important to trace the email header, and not the email address. An email address, such**

[1] http://www.emailtrackerpro.com

as anyone@hotmail.com will just run a trace on hotmail.com, and every single time you'll get the same result. An email header is a virtual footprint telling the user where an email has travelled. Each step along the way is recorded. Spammers often try and remove/add lines to confuse where it was sent from. eMailTrackerPro can pick up on patterns and inconsistencies and mark the email as suspected spam, this isn't an exact science so anomalies can occur. An example header can be seen on the right, split up into separate lines for understanding purposes.

2. Report Abuse: Abuse reporting is a useful feature for users that want to take a more proactive approach to dealing with spam. EmailTrackerPro provides a platform that auto-generates an abuse report and opens a new email (may not work for all email clients) with the 'to' address filled out to the email spam address detected (as shown on the right). Once the abuse report has been sent to the email provider it is then up to them to take the next steps to shut the account down. Each account that gets shut down is one more step closer to stopping spam in the long run!
3. Spam Filter: The most valuable feature is the ability to trace more than one IP address or domain name at a time. Trace as many IP addresses and domain names as required and either output the results to a new tab or an Excel/HTML file.

17.3.2 Online EMailTracer

Resource Centre for Cyber Forensics (RCCF) is a pioneering institute, pursuing research activities in the area of Cyber Forensics. The centre was dedicated to the nation by the then Honorable union minister in August 2008. EmailTracer developed in RCCF is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.

17.4 SUMMARY

1. An email message consists of two main sections: the header and the body.
2. A typical e-mail header contains the *From*, *To*, *Subject* and *Date*.
3. Email addresses are always made up of a username followed by a @ sign and a domain name. For instance, username@domainname.
4. The body of the message contains the information that the recipients have to read.
5. The basic components of an e-mail system are: User Agent (UA), Message Transfer Agent (MTA), Message Access Agent (MAA), Spool file and Mail Box.
6. The Mail Transfer Agent (MTA) is a server program that is basically responsible for transfer of e-mail message from one system to another.

7. **The delivery of an e-mail message from one MTA to another MTA is done through** Simple Mail Transfer Protocol **(SMTP).**
8. **The Message Access Agent (MAA) is a server program which pulls messages from the message store (say, mailbox) and delivers them to the recipient's user agent.**
9. **The two well known MAA protocols are Post office Protocol, version 3 (POP3) and Internet Mail Access Protocol (IMAP).**
10. **A mailbox is the storage location of e-mail messages which exist on a remote server.**
11. **the e-mail system uses three protocols for message communication, such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol, version 3 (POP3), Internet Mail Access Protocol (IMAP).**
12. **SMTP employs three phases, i.e. connection establishment phase, mail transfer phase and connection termination phase.**
13. **SMTP uses commands and responses to transmit the message between an MTA client and MTA server.**
14. **The POP3 session has three phases:** authorization **phase,** transaction **phase and** update **phase.**
15. **The DNS server translates the domain names to the IP addresses and vice-versa with the help of Mail eXchange (MX) record.**
16. **An email attack may be described as an event in which the email is used to damage or harm an individual or an organization.**
17. **E-mail security is a term for describing different procedures and techniques for protecting sensitive information in email communication, user accounts against unauthorized access, spam filtering, data loss or compromise, e-mail encryption, and so on.**
18. **Laws nowadays give importance to emails and review them with lot of attention.**
19. **Email services can be Web-based email, POP3 email services, The Internet Message Access Protocol (IMAP), MAPI email servers. Most widely used protocol in emailing is simple mail transfer protocol (SMTP).**
20. **Few email attacks or crimes are Flaming, Email spoofing, Email bombing, Email hacking, Spams, Email frauds and Email phishing.**
21. **Email privacy is the broad topic dealing with issues of unauthorized access and inspection of electronic mail.**
22. **Emails information which will be interesting to the investigators are Email header, Body of Emails, The information hidden in the email packets and Attachments.**
23. **Email forensics involves capturing, securing and analysing and reporting the email evidences. E-mail forensics aims to study the source and contents of e-mail messages for evidence.**
24. **Various software tools have been developed to assist e-mail forensic investigation. These include eMailTrackerPro, EmailTracer.**

17.5 CHECK YOUR PROGRESS

1. SMTP is a simple

    a) TCP protocol
    b) UDP protocol
    c) IP protocol
    d) None of the above

2. A simple protocol used for fetching e-mail form a mailbox is

    a) CIMP
    b) POP3
    c) SMTP
    d) None of the above

3. E-mail address is made up of

    a) Single part
    b) Two parts
    c) Three parts
    d) Four parts

4. SMTP stands for

    a) Short Mail Transmission Protocol
    b) Small Mail Transmission Protocol
    c) Server Mail Transfer Protocol
    d) Simple Mail Transfer Protocol

5. E-mail addresses separate the user name from the ISP using the _____ symbol.

    a) &
    b) $
    c) @
    d) %

Answers:

1. (a)
2. (b)
3. (b)
4. (d)

5. (c)

17.6 MODEL QUESTIONS

1. **Desribe briefly about UA, MTA and MAA.**
2. **Why do we need SMTP and IMAP for electronic mail?**
3. **Write the difference between the POP3 and IMAP.**
4. **Describe working of electronic mail.**
5. **Write the advantages and dis-advantages of e-mail.**
6. **What is DNS and its purpose?**
7. **Explain E-mail Architecture with components by using neat diagram.**
8. **Write different types of e-mail attacks.**
9. **Write the some important best practices that organization should follow to ensure secure usage of e-mail.**
10. **Write the some important best practices that individual users (organization employees) should follow to ensure secure usage of e-mail.**
11. **Describe the structure of SMTP messaging with a neat diagram.**
12. **Which headers in SMTP useful in tracing a message sender identity?**
13. **List and describe atleast 4 email attacks.**
14. **How is privacy a big issue in emailing?**
15. **What are the various types of email services?**

17.7 FURTHER READINGS

1. **Debra Littlejohn Shinder, Michael Cross, Scene of the Cybercrime, syngress**
2. **Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.**
3. **Gutiérrez, Carlos A., Web Services Security Development and Architecture: Theoretical and Practical issues, IGI Global, 2010.**

References, Article Source & Contributors

[1] Email - Wikipedia, the free encyclopedia, https://en.m.wikipedia.org/wiki/Mail_headers

[2] Email privacy - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Email_privacy

[3] Email tracking - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Email_tracking

[4] E-mail: Message Format | World4Engineers, world4engineers.com/e-mail-message-format/
[5] EMailTracer, http://www.cyberforensics.in/OnlineEmailTracer/index.aspx
[6] M. Tariq Banday, Techniques and Tools for Forensic Investigation of E-Mail, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011
[7] Phishing - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Phishing

Recommended Youtube Videos

Computer Forensics: Investigating E mail Crimes and Violations by Raja sekhar:
https://youtu.be/F3JNMyUqj9I

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of

CEMCA