

Email and Social Media Investigations

References:

Resources folder on Forensic Linguistics

Nelson, Chapter 11

Introduction

Forensics involving email and social media can play a very important role in investigations

Important sources of information regarding email

Email content itself

Email header

Message ID (useful for tracing email through email server)

Source IP address (where it really came from)

Intermediate IP address (helpful in tracking messages back)

Email server logs

Network logs

Primary goals

Correlation

Tracing

Objectives

- Explain the role of Email Forensics
- Explain the Email software model
- Explain the role of Forensic Linguistics
- Explain the use of e-mail server logs
- Describe some specialized e-mail forensics tools
- Email case study (Enron)
- Explain how to apply digital forensics methods to investigating social media communications

Exploring the Role of E-mail in Investigations (1 of 2)

An increase in e-mail scams and fraud attempts with phishing or spoofing

Investigators need to know how to examine and interpret the unique content of e-mail messages

Phishing e-mails contain links to text on a Web page

Attempts to get personal information from reader

Pharming - DNS poisoning takes user to a fake site

A noteworthy e-mail scam was 419, or the Nigerian Scam

Nigerian 419 Scam

Scammer will contact you out of the blue

Email, letter, text, social media

They may tell an elaborate story about large amounts of their money trapped in banks during events such as civil wars, coups, often in countries in the news

Or they may refer to a large inheritance that is “difficult to access” because of government restrictions

They will then offer you a large sum of money to help them transfer their personal fortune out of the country

Scammers may ask for

Your bank account info to “help them transfer the money” and later steal your funds

You to pay fees, charges, or taxes to “help release or transfer the money out of the country through your bank”

You will never be sent the money that was promised

Known as Nigerian 419 scam because

First wave of these phishing attacks came from Nigeria

419 is reference to Nigeria’s Criminal Code which outlaws the practice

Exploring the Role of E-mail in Investigations (2 of 2)

Spoofing e-mail can be used to commit fraud

Investigators can use the **Enhanced/Extended Simple Mail Transfer Protocol (ESMTP)** number in the message's header to check for legitimacy of email

Exploring the Roles of the Client and Server in E-mail (1 of 3)

E-mail can be sent and received in two environments

Internet

Intranet (an internal network)

Client/server architecture

Server OS and e-mail software differs from those on the client side

Protected accounts

Require usernames and passwords

Exploring the Roles of the Client and Server in E-mail (2 of 3)

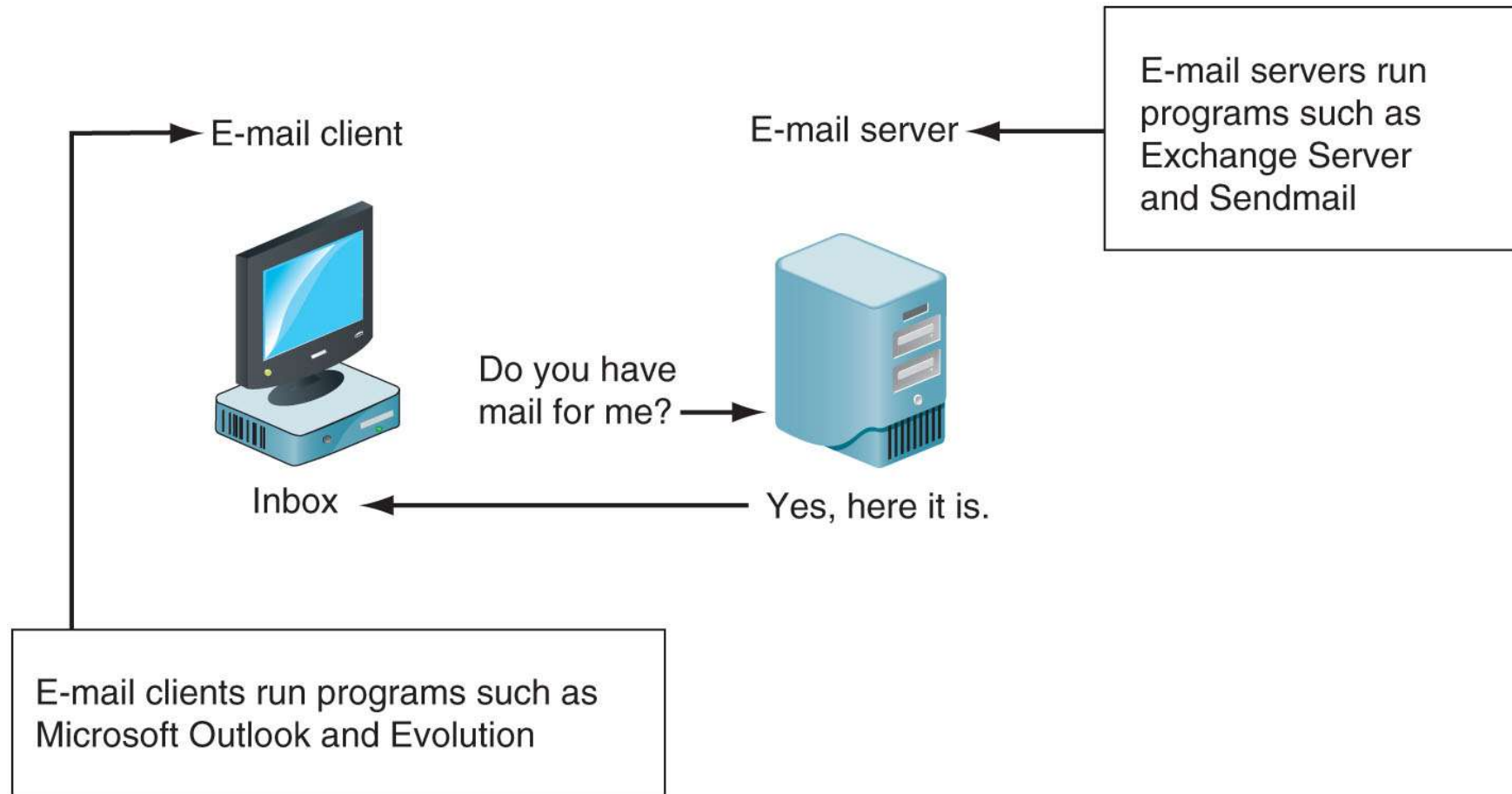


Figure 11-1 E-mail in a client/server architecture

Exploring the Roles of the Client and Server in E-mail (3 of 3)

Name conventions

Corporate: john.smith@somecompany.com

Public: whatever@gmail.com

Everything after @ belongs to the domain name

Tracing corporate e-mails is easier

Because accounts use standard names the administrator establishes

Many companies are migrating their e-mail services to the cloud

Investigating E-mail Crimes and Violations (1 of 2)

Similar to other types of investigations

Goals

Find who is behind the crime

Collect the evidence

Present your findings

Build a case

Know the applicable privacy laws for your jurisdiction

***Electronic Communications Privacy Act (ECPA) and the
Stored Communications Act (SCA) apply to e-mail.***

Investigating E-mail Crimes and Violations (2 of 2)

E-mail crimes depend on the city, state, or country

Example: spam may not be a crime in some states

Always consult with an attorney

Examples of crimes involving e-mails

Narcotics trafficking

Extortion

Sexual harassment and stalking

Fraud

Child abductions and pornography

Terrorism

Examining E-mail Messages (1 of 2)

Access victim's computer or mobile device to recover the evidence

Using the victim's e-mail client

Find and copy any potential evidence

Access protected or encrypted material

Print e-mails

Guide victim on the phone

Open and copy e-mail including headers

You may have to recover deleted e-mails

Examining E-mail Messages (2 of 2)

Copying an e-mail message

Before you start an e-mail investigation

You need to copy and print the e-mail involved in the crime or policy violation

You might also want to forward the message as an attachment to another e-mail address

With many GUI e-mail programs, you can copy an e-mail by dragging it to a storage medium

Or by saving it in a different location

Viewing E-mail Headers (1 of 5)

Investigators should learn how to find e-mail headers

GUI clients

Web-based clients

After you open e-mail headers, copy and paste them into a text document

So that you can read them with a text editor

Become familiar with as many e-mail programs as possible

Often more than one e-mail program is installed

Viewing E-mail Headers (2 of 5)

Outlook

*Double-click the message and then click **File, Properties***

Copy headers

Paste them to any text editor

Save the document as Outlook_header.txt in your work folder

Viewing E-mail Headers (3 of 5)

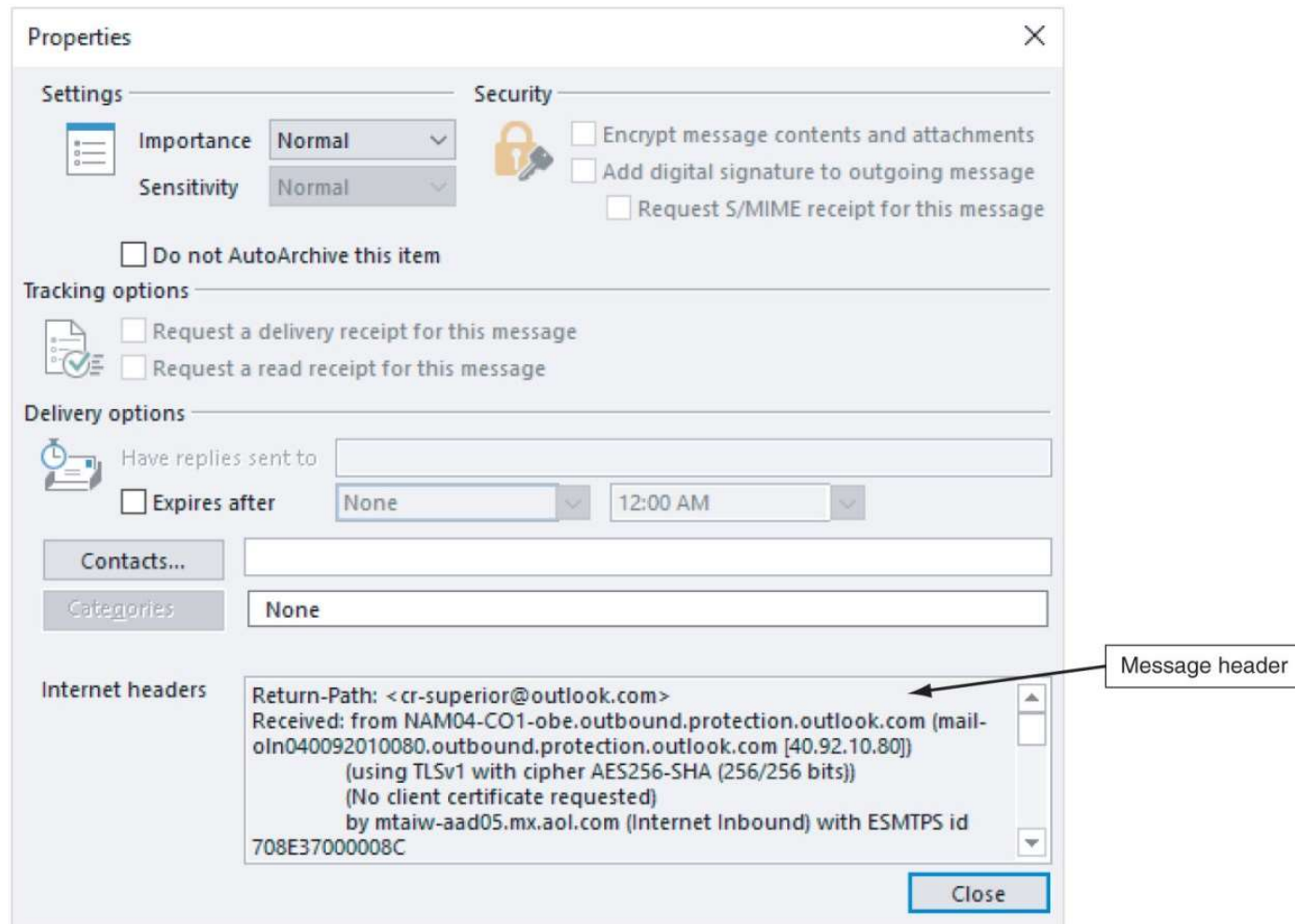


Figure 11-2 An Outlook e-mail header

Viewing E-mail Headers (4 of 5)

Gmail

*Click the down arrow next to the Reply circular arrow, and click **Show original***

*Click the **Download Original** link to open the “Opening original_msg.txt” dialog box*

*Click **Open with Notepad (default)** and click **Okay***

Save the file in your work folder with the default name

Yahoo

*Click **Inbox** to view a list of messages*

*Above the message window, click **More** and click **View Raw Message***

Copy and paste headers to a text file

Viewing E-mail Headers (5 of 5)

```
X-Apparently-To: - Mon, 11 Sep 2017 17:24:24 +0000
Return-Path: <LCwMzCwMbLSsHJzsbCwM7LRGtMzsTOxMrKws@smtp-coi-g09-025.aweber.com>
Received-SPF: pass (domain of smtp-coi-g09-025.aweber.com designates 204.194.223.25 as permitted sender)
X-YMailISG: MiNqrvsWLDsdwYue2y_8jUSdLl8maR6 T.d55zY7e6G0ngyy
ssZsOTvSJvYtoV105Mj28Ri1jcZ1Aw3GVLNXUMXr9R4mw0WKWp18ulCc3mgR
XaY8x1W9Cv9V5LTzBHua4Z8VZD12Q_tfXDLaucahaQTQMcaoSfdAgb9r9D61n
pTnJrzvzwqf7DZueBuiKzy9nJ6Val4VRv70iEdI2jiyIQ1ICm0hA7992w0Tw
XQ7t3QR.x_dTIwWfCEwkIOUhcem6QPn83fKKJ9bdOBhndX_vlkW5c8Wry4D
glMLouiMPg_30L9ww.1fzRXCQt1pwzWl_XTMQh7P10VT6Xn2kpZ1vVjgcfi
7HcVAAyrqxEdzhJKXmqrmACBOBUfVSh1PM9LUHi2Gb.b9zNWs4APLc7IIY_t
.g_vQieX4_pYdvSsCAMSJ.nmv1ATRnUkpXzw.Jm4GHsnv2KWpReWKcS_YDu
hC_HASKpnxcx81.JEDMOKkhPTA1bjv3_DlItXp8GDScfYv9Rz3ETEElgKDH8
6Iantym8.E_zBNCZo2UuxAUmqxpnYgZgpiMCb6.YqOJ78tf_0cGmt8BDIo20
fWUTx.OtAhlh8DQz1NHG3120FM9ju3c9KtuPTafQKCZxqznPDauI_uBlRwg
fi9JboFzFFqdzunZkKrbCMEvBKnp85Z1ZahJkQYragNq6es436v36ED1k3x
VjqwlLwYMOHuIFpg7z8R.w.Z0gi7Bi8m.WQyTP8dcAOvI6n4Fw5R4E.ILdaC
KofwXtj7CpBqlCOW3r6PVyDYEygH6Z_83he7qG6p4H4cv7zHR6mdiygIg1Ku
caS2UytV9MD16I_fmX6auvqi6UhgRQTvG4i7K6V.kbTQEBqDDfbmt3J0pD7W
ElUcHF1hzf01hRkRuXuEpIOu..NYvRRkkU2mnFPAXdh9eqUlpSxyv9plyqP9
ZpRpE6siCkiUcesmJAUNKORhEwzAmoNwNmKqH60.olvwOc3pA_2YlKNbDeXS
eUQ5JU5hRpaPMn2CqMyYHdj9WSYaxSRSCnJMPKrq4J68h3esSW9y8jH_hBFS
aZ13BFqlfVEc9_5_P9_UqM3LMJY6YvH4126IAQgRz3KSKHkYmWmXJmNOXxOe
Oz0oBf6D4jfvkVTDtCvERPeEaDrEQuCTrQffMd61Ztgx25AqzzJufor6logC
.ee.pCy.La7YDn9UpHKnIt6iz_yD9Wtwop6gKy96bxiWdTx8v9Waa0GWLJ1y
JwYhK6BSd95iH2cqiVUV7fQYhXvoUypBca.Ar4sq2yoEhXzy3Sqm90jXKh_P
94nzt57KAZYvK.GHpkwHMOaHj1YCdeqld3k61neDbhiGjJDjzwTRK4FN3krv
VYQDwVVBx8wjG8qDA7skIT99.tCBu8DR57kC.NtOig--
X-Originating-IP: [204.194.223.25]
Authentication-Results: mta1120.mail.bf1.yahoo.com from=send.aweber.com; domainkeys=neutral (no sig);
Received: from 127.0.0.1 (EHLO smtp-coi-g09-025.aweber.com) (204.194.223.25)
by mta1120.mail.bf1.yahoo.com with SMTPS; Mon, 11 Sep 2017 17:24:24 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=aweber.com;
s=dkim_s1024; t=1505149312;
bh=6z2+thX7FQfo+chNPIhWcS5SoNUcWciEf11WBF9GXfBs=;
h=MTIME:version:Content-Type:To:From:Sender:Date:List-Header:Subject:
```

Figure 11-3 Viewing headers in Yahoo!

Source: Yahoo! Inc., www.yahoo.com



Examining E-mail Headers (1 of 3)

Headers contain useful information

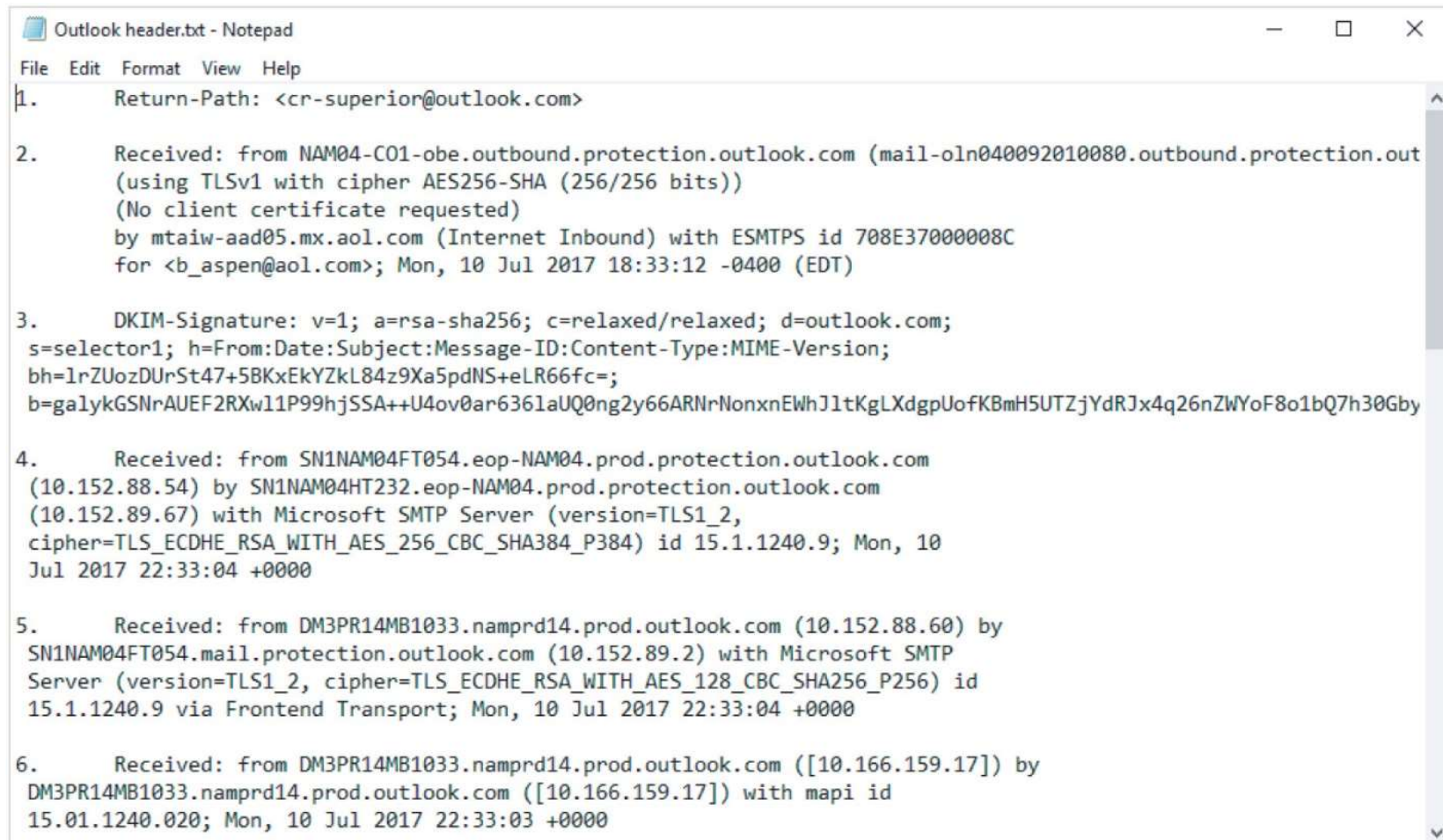
The main piece of information you're looking for is the originating e-mail's IP address

Date and time the message was sent

Filenames of any attachments

Unique message number (if supplied)

Examining E-mail Headers (2 of 3)



```
Outlook header.txt - Notepad
File Edit Format View Help
1. Return-Path: <cr-superior@outlook.com>
2. Received: from NAM04-C01-obe.outbound.protection.outlook.com (mail-oln040092010080.outbound.protection.out
(using TLSv1 with cipher AES256-SHA (256/256 bits))
(No client certificate requested)
by mtaiw-aad05.mx.aol.com (Internet Inbound) with ESMTPS id 708E37000008C
for <b_aspen@aol.com>; Mon, 10 Jul 2017 18:33:12 -0400 (EDT)
3. DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=outlook.com;
s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
bh=1rZUozDUrSt47+5BKxEkYZkL84z9Xa5pdNS+eLR66fc=;
b=galykGSNrAUeF2RXw11P99hjSSA++U4ov0ar6361aUQ0ng2y66ARNrNonxnEWhJ1tKgLXdgpUofKBmH5UTZjYdRJx4q26nZWYoF8o1bQ7h30Gby
4. Received: from SN1NAM04FT054.eop-NAM04.prod.protection.outlook.com
(10.152.88.54) by SN1NAM04HT232.eop-NAM04.prod.protection.outlook.com
(10.152.89.67) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1240.9; Mon, 10
Jul 2017 22:33:04 +0000
5. Received: from DM3PR14MB1033.namprd14.prod.outlook.com (10.152.88.60) by
SN1NAM04FT054.mail.protection.outlook.com (10.152.89.2) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
15.1.1240.9 via Frontend Transport; Mon, 10 Jul 2017 22:33:04 +0000
6. Received: from DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) by
DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) with mapi id
15.01.1240.020; Mon, 10 Jul 2017 22:33:03 +0000
```

Figure 11-4 An e-mail header with line numbers added

Examining E-mail Headers (3 of 3)

Google has an online tool to analyze email headers:

<https://toolbox.googleapps.com/apps/messageheader/>

Other online tools:

<https://mha.azurewebsites.net/>

<https://www.whatismyip.com/email-header-analyzer/>

<https://mxtoolbox.com/EmailHeaders.aspx>

Examining Additional E-mail Files

E-mail messages are saved on the client side or left at the server

Microsoft Outlook uses .pst and .ost files

Most e-mail programs also include an electronic address book, calendar, task list, and memos

In Web-based e-mail

Messages are displayed and saved as Web pages in the browser's cache folders

Many Web-based e-mail providers also offer instant messaging (IM) services

Tracing an E-mail Message

Determining message origin is referred to as “tracing”
Contact the administrator responsible for the sending server

Use a registry site to find point of contact:

www.arin.net

www.internic.com

www.google.com

Verify your findings by checking network e-mail logs against e-mail addresses

Using Network E-mail Logs (1 of 2)

Router logs

Record all incoming and outgoing traffic

Have rules to allow or disallow traffic

You can resolve the path a transmitted e-mail has taken

Firewall logs

Filter e-mail traffic

Verify whether the e-mail passed through

You can use any text editor or specialized tools

Using Network E-mail Logs (2 of 2)

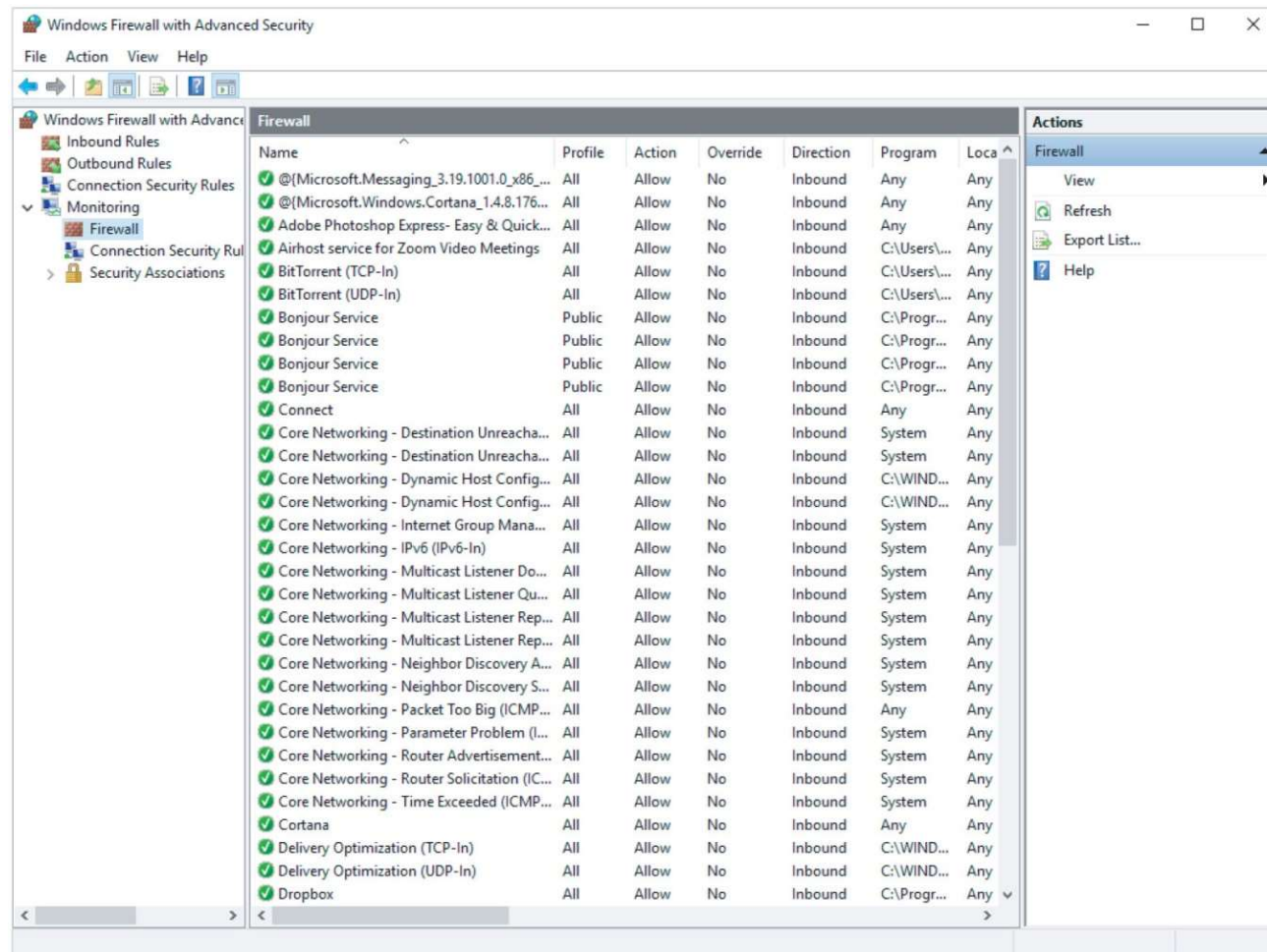


Figure 11-5 A Windows firewall log

Forensic Linguistics

Understanding Forensic Linguistics

Forensic Linguistics

Where language and law intersect

Four categories:

Language and law

Language in the legal process

Language as evidence

This is the area of most interest in Cyber Forensics

Research/teaching

Forensic Linguistic expertise has been utilized in civil cases, criminal cases, cyber-terrorism cases, and other legal proceedings

Forensic Linguistics

Areas of Research and Expertise

Specializations within Forensic Linguistics are:

Voice Identification

Author Identification

Discourse Analysis

Linguistic Proficiency

Dialectology

Linguistic Origin Analysis

Linguistic Veracity Analysis

Forensic Linguistics

Voice Identification

Voice Identification:

Goal: *Determine whether recorded voice was that of defendant or accused*

Also called Forensic Phonetics

Testimony and evidence by qualified Forensic Linguists is widely accepted in courts

Forensic Linguistics

Author Identification

Author Identification:

Goal: *Determine whether written word was that of defendant or accused. Pertains to both:*

Hard copy

Electronic

Also called Forensic Stylistics

Requires several writing samples to draw reliable conclusions

Analysis often hampered by insufficient data

Active area of research: which linguistic features are reliable indicators of authorship

Useful contributions in this area can be made even with relatively small writing sample set

May be able to eliminate someone as author

Can select author from small group of suspects

Forensic Linguistics

Discourse Analysis

Discourse Analysis:

Goal: *Determine whether suspect is agreeing to engage in criminal conspiracy*

Based on written and/or verbal evidence

Typically requires examination of covert recording or communication

Acceptability of evidence is dependent on methodology used and conclusions drawn

E.g., “Yeah” or “uh-huh” in response to a suggestion is not necessarily agreeing with suggestion

Courts have a mixed record of accepting this evidence

Can be useful for case preparation even if not formally accepted as evidence in court

Forensic Linguistics

Linguistic Proficiency

Linguistic Proficiency:

Goal: *Determine whether suspect understood Miranda or police warning*

Involves determining how well a suspect understands the language used

Suspect may try to downplay their language proficiency

Law enforcement may try to overplay the suspect's language proficiency

Related to language origin analysis and dialectology

Evidence widely accepted in courts

Forensic Linguistics

Dialectology

Dialectology:

Goal: *Determine what dialect of a language the person speaks*

Analysis is often needed to show that a defendant has a different dialect from that on an incriminating recording

Can be complicated because dialects are becoming less distinct due to

Influence of mass media

Population mobility

Different than voice identification

Voice identification utilizes acoustics features of speech

Dialectology uses linguistic features

Evidence typically are accepted with the understanding of limitations of this approach

Forensic Linguistics

Linguistic Origin Analysis

Linguistic Origin Analysis:

Goal: *Determine the person's native language*

Typical Purpose: *Granting or denying applications for political asylum*

Analysis can be complicated by fact that

Many languages straddle a border

Many languages are spoken in multiple countries

Evidence typically are accepted with the understanding of limitations of this approach

Forensic Linguistics

Linguistic Veracity Analysis

Linguistic Veracity Analysis:

Goal: *Determine whether speaker or author is being truthful*

Results in this area are unreliable

Few linguists claim that a veracity analysis can be done with any degree of accuracy

Rarely accepted as evidence in courts

Forensic Linguistics

Resources

For more information on Forensic Linguistics

Primary Professional Societies

International Association for Forensic and Legal Linguistics
(IAFL) <http://www.iafl.org>

International Association for Forensic Phonetics and
Acoustics (IAFPA) <http://www.iafpa.net>

Class Blackboard Resource Folder

This topic will be covered on final

Email Forensics

...continued

Understanding E-mail Servers (1 of 2)

An e-mail server is loaded with software that uses e-mail protocols for its services

And maintains logs you can examine and use in your investigation

E-mail storage

Database

Flat file system

Logs

Some servers are set up to log e-mail transactions by default; others must be configured to do so

Understanding E-mail Servers (2 of 2)

E-mail logs generally identify the following:

E-mail messages an account received

Sending IP address

Receiving and reading date and time

E-mail content

System-specific information

Contact suspect's network e-mail administrator as soon as possible

Servers can recover deleted e-mails

Similar to deletion of files on a hard drive

Examining *NIX E-mail Server Logs (1 of 2)

Common UNIX/Linux e-mail servers: Postfix and Sendmail

Postfix has two configuration files

master.cf and main.cf (found in /etc/postfix)

Sendmail has two relevant configuration files

/etc/sendmail.cf

Configuration file for Sendmail

/etc/syslog.conf

Specifies how and which events Sendmail logs

Examining *NIX E-mail Server Logs (2 of 2)

`/var/log/maillog`

Records SMTP, POP3, and IMAP4 communications

Contains an IP address and time stamp that you can compare with the e-mail the victim received

Default location for storing log files:

`/var/log`

An administrator can change the log location

Use the find or locate command to find them

Check Linux/UNIX man pages for more information

Examining Microsoft E-mail Server Logs (1 of 4)

Microsoft Exchange Server (Exchange)

Uses a database

Based on Microsoft Extensible Storage Engine (ESE)

Most useful files in an investigation:

.edb database files, checkpoint files, and temporary files

Information Store files

*Database files *.edb*

Responsible for **MAPI** information

Examining Microsoft E-mail Server Logs (2 of 4)

Transaction logs

Keep track of changes to its data

Checkpoints

Marks the last point at which the database was written to disk

Temporary files

Created to prevent loss when the server is busy converting binary data to readable text

Examining Microsoft E-mail Server Logs (3 of 4)

To retrieve log files created by Exchange

Use the Windows PowerShell cmdlet

GetTransactionLogStats.ps1 -Gather

Tracking.log

An Exchange server log that tracks messages

Another log used for investigating the Exchange environment is the troubleshooting log

Use Windows Event Viewer to read the log

Examining Microsoft E-mail Server Logs (4 of 4)

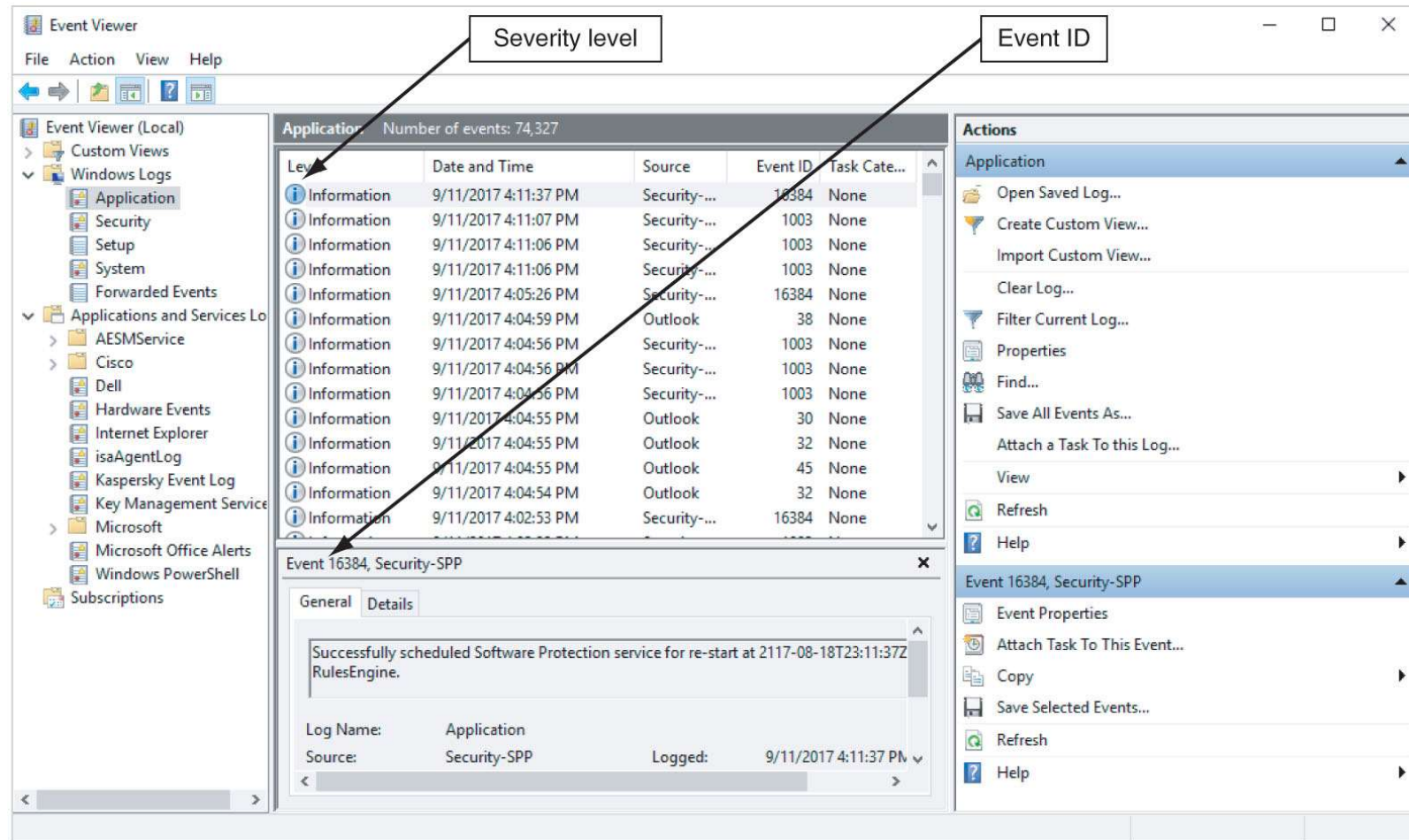


Figure 11-6 Viewing a log in Event Viewer

Using Specialized E-mail Forensics Tools (1 of 3)

Tools include:

DataNumen for Outlook and Outlook Express

FINALeMAIL for Outlook Express and Eudora

Sawmill-Novell GroupWise for log analysis

MailXaminer for multiple e-mail formats and large data sets

Fookes Aid4Mail and MailBag Assistant

Paraben E-Mail Examiner

AccessData Forensic Toolkit

Ontrack Easy Recovery EmailRepair

R-Tools R-Mail

OfficeRecovery's MailRecovery

Using Specialized E-mail Forensics Tools (2 of 3)

Tools (continued)

MXToolBox for decoding e-mail headers

FreeViewer with free tools for various servers

Tools allow you to find:

E-mail database files

Personal e-mail files

Offline storage files

Log files

Advantage of using data recovery tools

You don't need to know how e-mail servers and clients work to extract data from them

Using Specialized E-mail Forensics Tools (3 of 3)

After you compare e-mail logs with messages, you should verify the:

Email account, message ID, IP address, date and time stamp to determine whether there's enough evidence for a warrant

With some tools

You can scan e-mail database files on a suspect's Windows computer, locate any e-mails the suspect has deleted and restore them to their original state

Using Magnet AXIOM to Recover E-mail (1 of 2)

Magnet AXIOM has three modules:

Process

Data acquisition for:

Mobile devices

Computer drives

SIM cards

Cloud-based social media platforms

Magnet.AI

Automated analysis (with AI)

Examine

Investigative analysis

Timeline

Reporting

Using MAGNET Process to Recover E-mail (2 of 2)

Magnet AXIOM Process 1.2.0.6464

File Tools Help

CASE DETAILS

CASE INFORMATION

Case number: InChap11

LOCATION FOR CASE FILES

Folder name: InChapter11

File path: C:\Work\Chapter11\InChapter11 [BROWSE](#)

Available space: 260.31 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name: InChapter11

File path: C:\Work\Chapter11\InChapter11 [BROWSE](#)

Available space: 260.31 GB

SCAN INFORMATION

SCAN 1

Created on: 10/5/2017 2:11:53 AM

Scanned by:

Description:

[GO TO EVIDENCE SOURCES](#)

Figure 11-7 Entering information in the CASE DETAILS window

Source: Magnet Forensics, www.magnetforensics.com

Using a Hex Editor to Carve E-mail Messages (1 of 4)

Few vendors have products for analyzing e-mail in systems other than Microsoft

mbox format

Stores e-mails in flat plaintext files

Multipurpose Internet Mail Extensions (MIME) format

Used by vendor-unique e-mail file systems, such as Microsoft .pst or .ost

Example: carve e-mail messages from Evolution email client

Using a Hex Editor to Carve E-mail Messages (2 of 4)

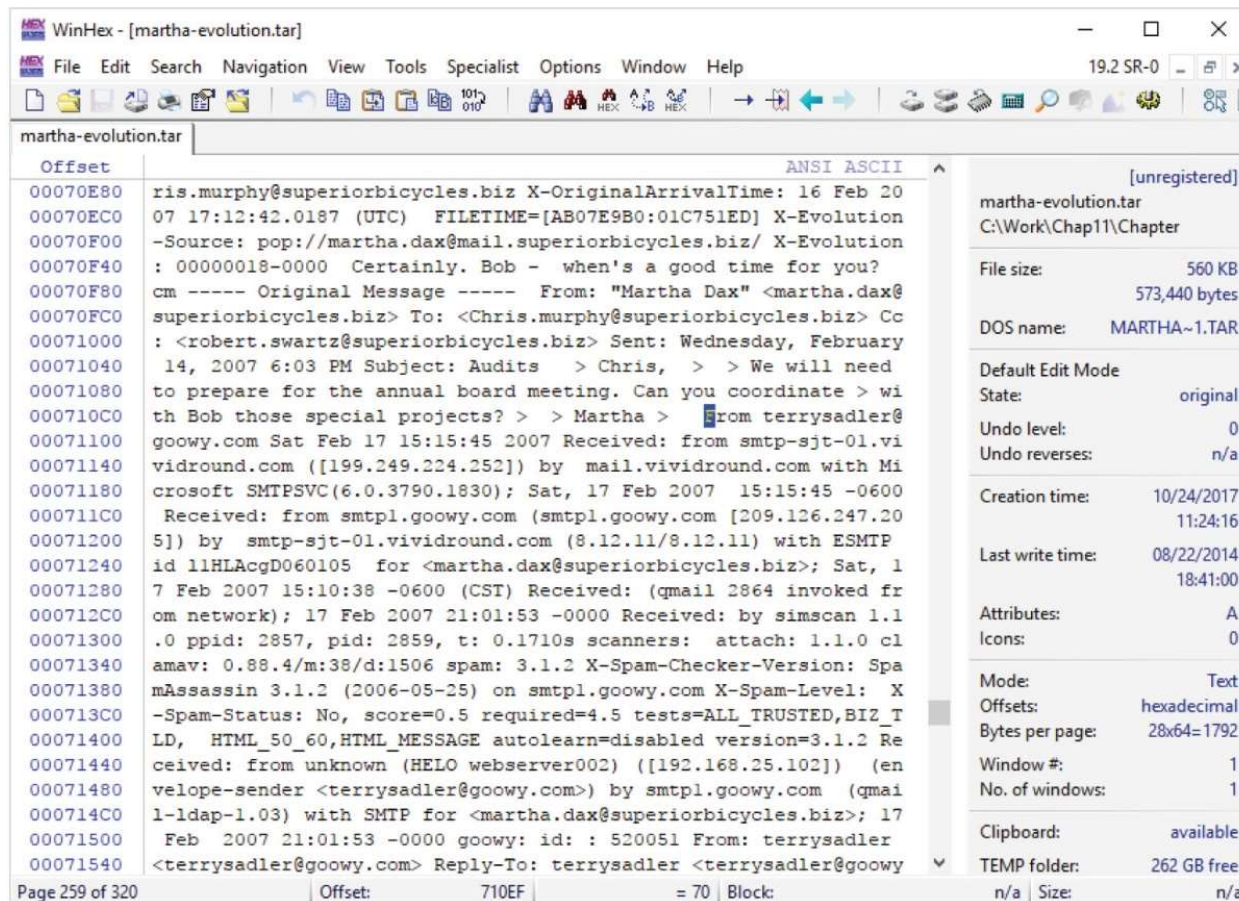


Figure 11-10 WinHex displaying the beginning of the e-mail from Terry Sadler

Source: X-Ways AG, www.x-ways.net

Using a Hex Editor to Carve E-mail Messages (3 of 4)

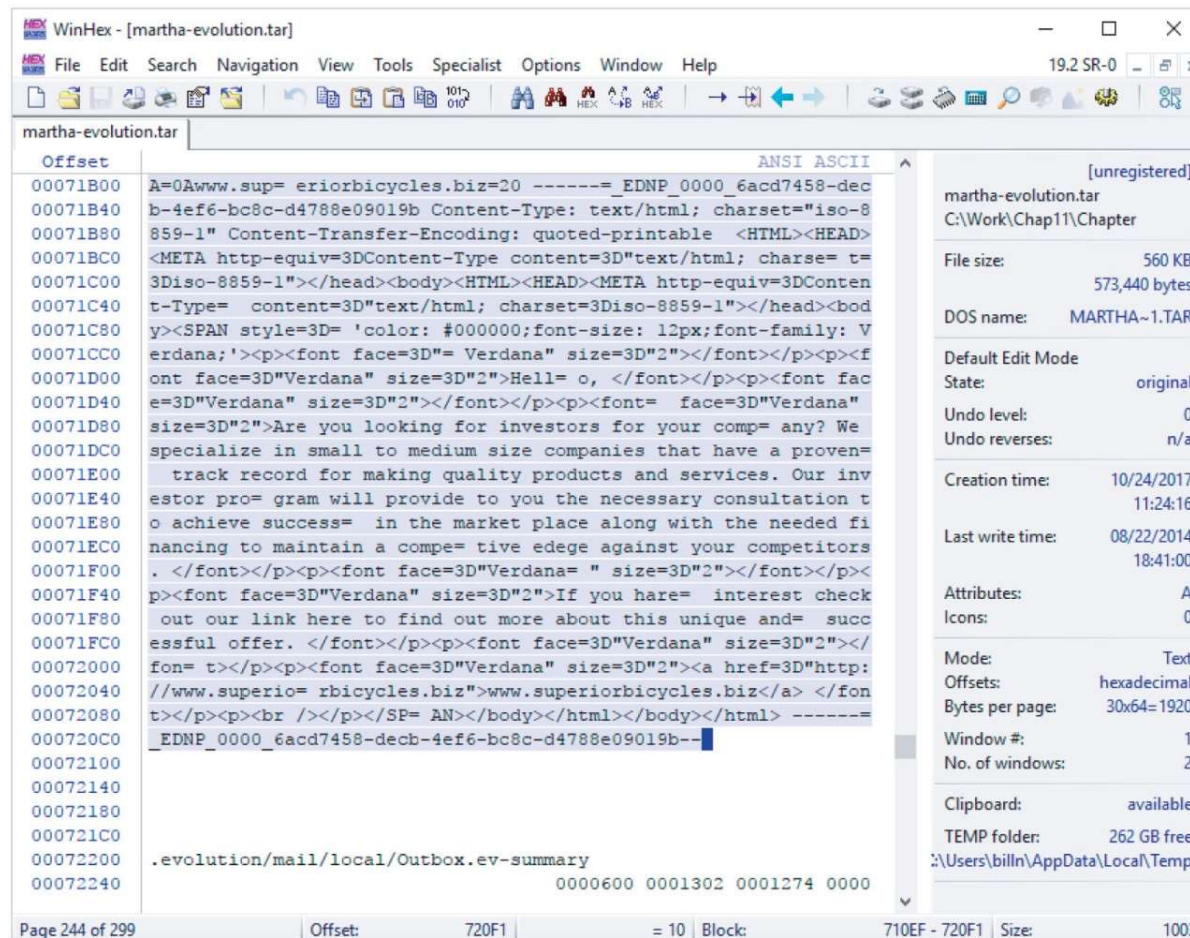
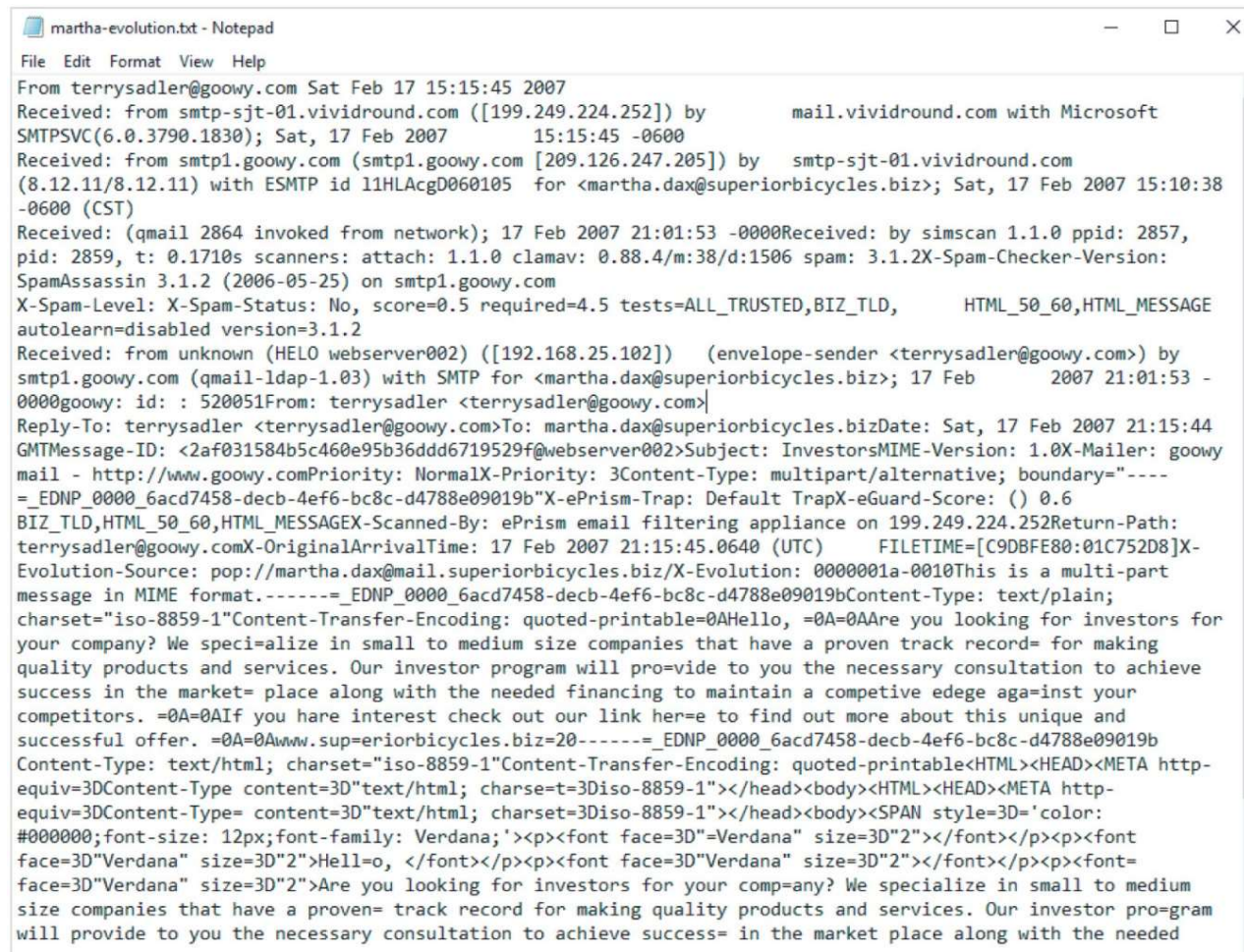


Figure 11-11 WinHex displaying the ending position of the e-mail from Terry Sadler

Source: X-Ways AG, www.x-ways.net

Using a Hex Editor to Carve E-mail Messages (4 of 4)



```
martha-evolution.txt - Notepad
File Edit Format View Help
From terrysadler@goowy.com Sat Feb 17 15:15:45 2007
Received: from smtp-sjt-01.vividround.com ([199.249.224.252]) by mail.vividround.com with Microsoft
SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007 15:15:45 -0600
Received: from smtp1.goowy.com (smtp1.goowy.com [209.126.247.205]) by smtp-sjt-01.vividround.com
(8.12.11/8.12.11) with ESMTP id 11HLAcgD060105 for <martha.dax@superiorbicycles.biz>; Sat, 17 Feb 2007 15:10:38
-0600 (CST)
Received: (qmail 2864 invoked from network); 17 Feb 2007 21:01:53 -0000Received: by simscan 1.1.0 ppid: 2857,
pid: 2859, t: 0.1710s scanners: attach: 1.1.0 clamav: 0.88.4/m:38/d:1506 spam: 3.1.2X-Spam-Checker-Version:
SpamAssassin 3.1.2 (2006-05-25) on smtp1.goowy.com
X-Spam-Level: X-Spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_TLD, HTML_50_60,HTML_MESSAGE
autolearn=disabled version=3.1.2
Received: from unknown (HELO webserver002) ([192.168.25.102]) (envelope-sender <terrysadler@goowy.com>) by
smtp1.goowy.com (qmail-ldap-1.03) with SMTP for <martha.dax@superiorbicycles.biz>; 17 Feb 2007 21:01:53 -
0000goowy: id: : 520051From: terrysadler <terrysadler@goowy.com>
Reply-To: terrysadler <terrysadler@goowy.com>To: martha.dax@superiorbicycles.bizDate: Sat, 17 Feb 2007 21:15:44
GMTMessage-ID: <2af031584b5c460e95b36ddd6719529f@webserver002>Subject: InvestorsMIME-Version: 1.0X-Mailer: goowy
mail - http://www.goowy.comPriority: NormalX-Priority: 3Content-Type: multipart/alternative; boundary="----
=_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b"X-ePrism-Trap: Default TrapX-eGuard-Score: () 0.6
BIZ_TLD,HTML_50_60,HTML_MESSAGEX-Scanned-By: ePrism email filtering appliance on 199.249.224.252Return-Path:
terrysadler@goowy.comX-OriginalArrivalTime: 17 Feb 2007 21:15:45.0640 (UTC) FILETIME=[C9DBFE80:01C752D8]X-
Evolution-Source: pop://martha.dax@mail.superiorbicycles.biz/X-Evolution: 0000001a-0010This is a multi-part
message in MIME format.-----=_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019bContent-Type: text/plain;
charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable=0AHello, =0A=0AAre you looking for investors for
your company? We speci=alize in small to medium size companies that have a proven track record= for making
quality products and services. Our investor program will pro=vide to you the necessary consultation to achieve
success in the market= place along with the needed financing to maintain a competitive edege aga=inst your
competitors. =0A=0AIf you hare interest check out our link her=e to find out more about this unique and
successful offer. =0A=0Awww.sup=eriorbicycles.biz=20-----=_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b
Content-Type: text/html; charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable<HTML><HEAD><META http-
equiv=3DContent-Type content=3D"text/html; charse=t=3Diso-8859-1"></head><body><HTML><HEAD><META http-
equiv=3DContent-Type= content=3D"text/html; charset=3Diso-8859-1"></head><body><SPAN style=3D'color:
#000000;font-size: 12px;font-family: Verdana;'><p><font face=3D"Verdana" size=3D"2"></font></p><p><font
face=3D"Verdana" size=3D"2">Hell=0, </font></p><p><font face=3D"Verdana" size=3D"2"></font></p><p><font=
face=3D"Verdana" size=3D"2">Are you looking for investors for your comp=any? We specialize in small to medium
size companies that have a proven= track record for making quality products and services. Our investor pro=gram
will provide to you the necessary consultation to achieve success= in the market place along with the needed
```

Figure 11-12 The Terry Sadler e-mail in Notepad

Recovering Outlook Files (1 of 2)

A forensics examiner recovering e-mail messages from Outlook

May need to reconstruct .pst files and messages

With many advanced forensics tools

Deleted .pst files can be partially or completely recovered

Scanpst.exe **recovery tool**

Comes with Microsoft Office

Can repair .ost files as well as .pst files

Recovering Outlook Files (2 of 2)

Guidance Software uses the SysTools plug-in

For Outlook e-mail through version 2013

Systools extracts .pst files from EnCase Forensic for analysis

DataNumen Outlook Repair

One of the better e-mail recovery tools

Can recover files from VMware and Virtual PC

E-mail Case Study

Enron

One of the most popular email forensic case studies is the one involving the Enron scandal

Legal investigation into Enron's scandal required collecting and preserving vast amount of data, including email

Enron emails were processed and posted as part of eDiscovery

At the conclusion of the investigation, data was deemed to be in the public domain, to be used for

Historical research

Academic purposes

E-mail Case Study

Enron

The data collected via the Enron scandal investigation is called the ***Enron Corpus***

Reason for Enron Corpus popularity

It's one of the few publicly available mass collections of real email available for study

Most email collection are typically bound by numerous privacy and legal restrictions

Uses

Email forensics tool research and case studies

Test/training data for natural language processing/machine learning

E-mail Case Studies

In the Enron Case, more than 10,000 emails contained the following personal information:

60 containing credit card numbers

572 containing thousands of Social Security or other identity numbers

292 containing birth dates

532 containing information of a highly personal nature

Such as medical or legal matters

The versions publicly available have been sanitized

Email addresses modified

SSNs, etc., have been changed

Redactions

Emails cleaned up

Etc.

Social Media Forensics

Applying Digital Forensics to Social Media Communications (1 of 2)

Online social networks (OSNs) are used to conduct business, brag about criminal activities, raise money, and have class discussions

Social media can contain:

Evidence of cyberbullying and witness tampering

A company's position on an issue

Whether intellectual property rights have been violated

Who posted information and when

Applying Digital Forensics to Social Media Communications (2 of 2)

Social media can often substantiate a party's claims
OSNs involve multiple jurisdictions that might even cross national boundaries

A warrant or subpoena is needed to access social media servers

In cases involving imminent danger, law enforcement can file for emergency requests

Social Media Forensics on Mobile Devices

Mobile devices

Majority of social network clients

Evidence artifacts vary depending on the social media channel and the device

iPhone and Android devices

Yielded the most information, and much of the data was stored in SQLite databases

Forensics Tools for Social Media Investigations

Software for social media forensics is being developed

Not many tools are available now

There are questions about how the information these tools gather can be used in court or in arbitration

Using social media forensics software might also require getting the permission of the people whose information is being examined

Summary (1 of 3)

E-mail fraudsters use phishing, pharming, and spoofing scam techniques

In both Internet and intranet e-mail environments, e-mail messages are distributed from one central server to connected client computers

E-mail investigations are similar to other kinds of investigations

Forensics linguistics is a field where language and the law intersect to determine the author of e-mails, text messages, and other online communications

Access victim's computer to recover evidence

Copy and print the e-mail message involved in the crime or policy violation

Summary (2 of 3)

Use the e-mail program that created the message to find the e-mail header, which provides supporting evidence and can help you track the suspect to the originating location

Investigating e-mail abuse

Be familiar with e-mail servers and clients' operations

For many e-mail investigations you can rely on e-mail message files, headers, and server log files

Summary (3 of 3)

For e-mail applications that use the mbox format, a hexadecimal editor can be used to carve messages manually

Social media, or OSNs can provide evidence in criminal and civil cases

Software for collecting OSN information is being developed

The majority of people engaging in social media communications are mobile users

Social media forensics tools have evolved with the technology, and many forensics suites have built-in social media tools

Aside

Forensic Tool Downloads

Resource

The tool references in your **Nelson** text are fairly recent
However, freely downloadable tools come and go

Forensics organizations will put out free downloads

They serve to gauge and generate interest

*Over time, they are incorporated into their paid products
and pulled from the free download/resources area*

Here is a site that lists free, reputable forensic software

<https://www.secureforensics.com/resources/free-software>

Pretty good reference

However, even this is somewhat out of date