Guide to Computer Forensics and Investigations Sixth Edition

Chapter 11

E-mail and Social Media Investigations

CENGAGE

Objectives

- Explain the role of e-mail in investigations
- Describe client and server roles in e-mail
- Describe tasks in investigating e-mail crimes and violations
- Explain the use of e-mail server logs
- Describe some specialized e-mail forensics tools
- 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

CENGAGE

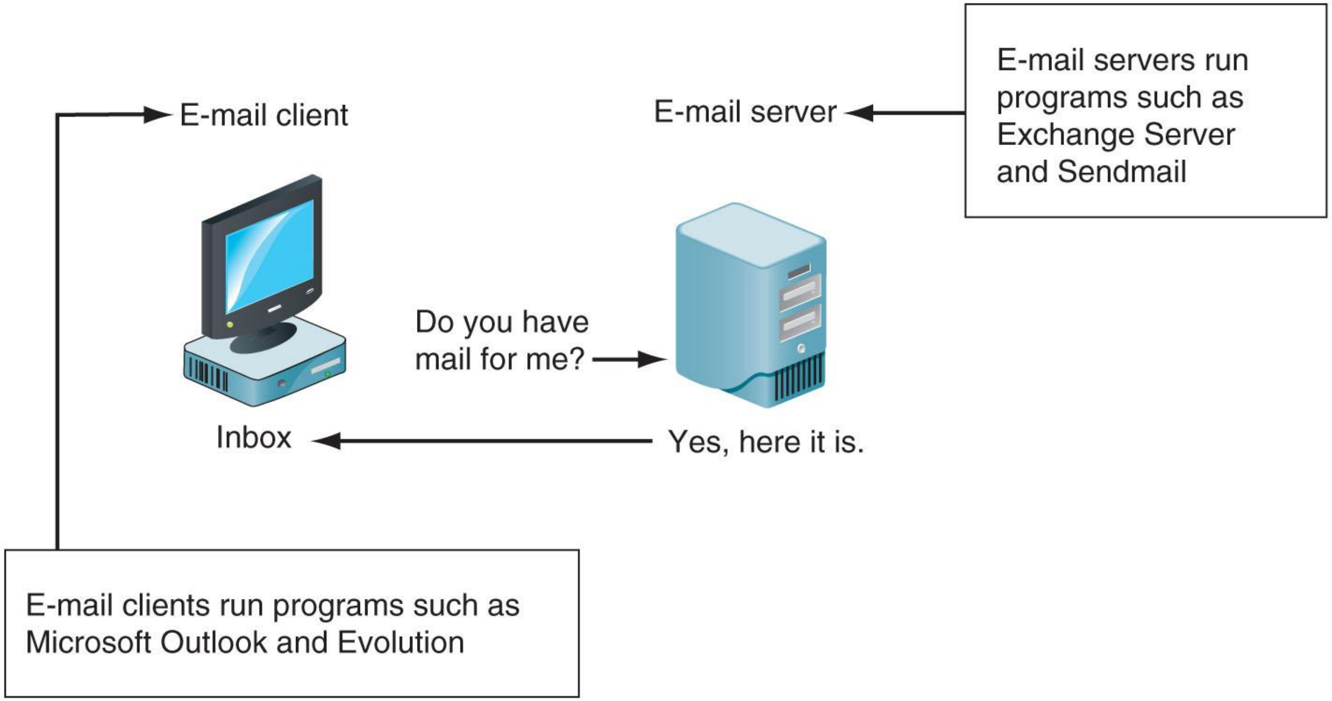
Exploring the Role of E-mail in Investigations (2 of 2)

- **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)



E-mail servers run programs such as Exchange Server and Sendmail

E-mail clients run programs such as Microsoft Outlook and Evolution

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)

- Examples of crimes involving e-mails
  - Narcotics trafficking
  - Extortion
  - Sexual harassment and stalking
  - Fraud
  - Child abductions
  - 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

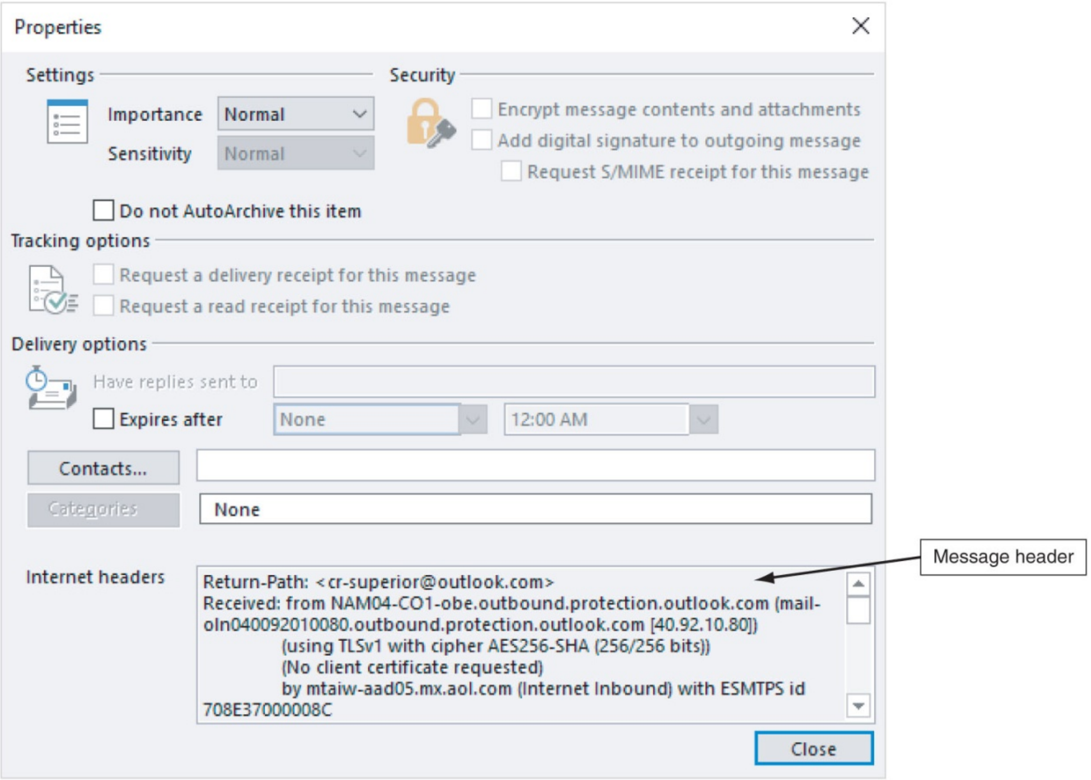
Viewing E-mail Headers (1 of 5)

- 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)



Properties

Settings

Importance: Normal

Sensitivity: Normal

□ Do not AutoArchive this item

Security

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

Tracking options

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

Have replies sent to

□ Expires after: None 12:00 AM

Categories: None

Internet headers

```
Return-Path: <cr-superior@outlook.com>
Received: from NAM04-CO1-obe.outbound.protection.outlook.com (mail-
oln040092010080.outbound.protection.outlook.com [40.92.10.80])
            (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
```

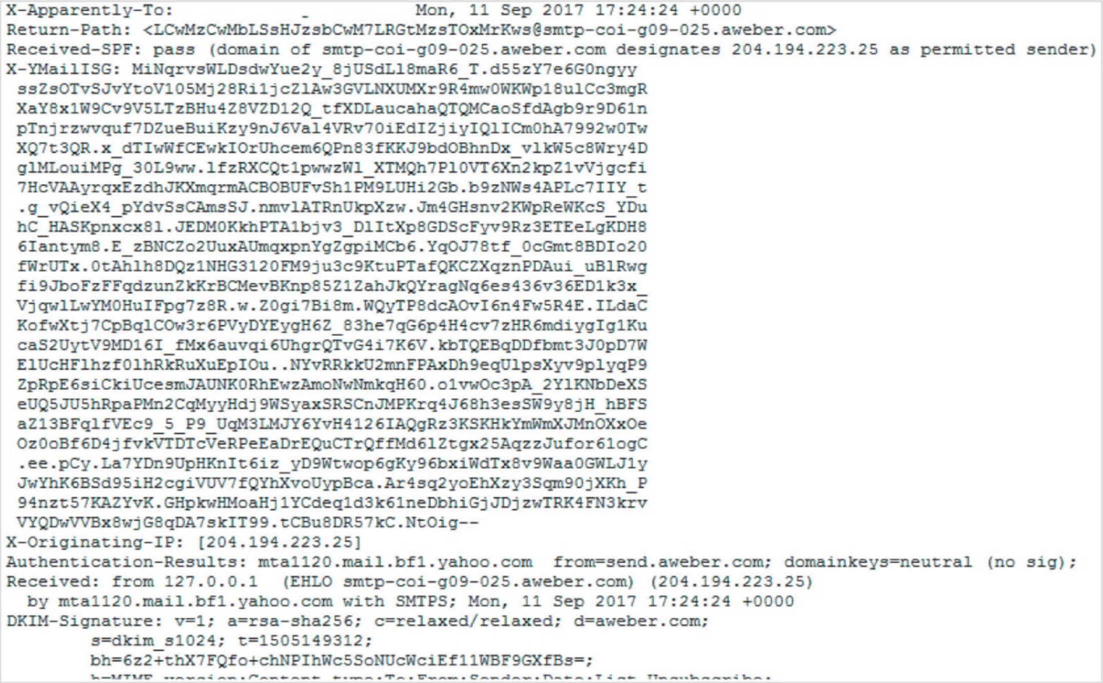
Message header

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
 ssZsOTvSJvYtoV105Mj28Ri1jcZlAw3GVLNXUMXr9R4mw0WKWp18ulCc3mgR
 XaY8x1W9Cv9V5LTzBHu4Z8VZD12Q_tfXDLaucahaQTQMCaoSfdAgb9r9D61n
 pTnjrzwvquf7DZueBuiKzy9nJ6Val4VRv70iEdIZjiyIQlICm0hA7992w0Tw
 XQ7t3QR.x_dTIwWfCEwkIOrUhcem6QPn83fKKJ9bdOBhnDx_vlkW5c8Wry4D
 glMLouiMPg_30L9ww.lfzRXCQt1pwwzWl_XTMQh7Pl0VT6Xn2kpZ1vVjgcfi
 7HcVAAyrqxEzdhJKXmqrmACBOBUFvSh1PM9LUHi2Gb.b9zNWs4APLc7IIY_t
 .g_vQieX4_pYdvSsCAmsSJ.nmvlATRnUkpXzw.Jm4GHsnv2KWpReWKcS_YDu
 hC_HASKpnxcx8l.JEDM0KkhPTA1bjv3_DlItXp8GDScFyv9Rz3ETEeLgKDH8
 6Iantym8.E_zBNCZo2UuxAUmqxpnYgZgpiMCb6.YqOJ78tf_0cGmt8BDIo20
 fWrUTx.0tAhlh8DQz1NHG3120FM9ju3c9KtuPTafQKCZXqznPDAui_uBlRwg
 fi9JboFzFFqdzunZkKrBCMevBKnp85Z1ZahJkQYragNq6es436v36ED1k3x_
 VjqwlLwYM0HuIFpg7z8R.w.Z0gi7Bi8m.WQyTP8dcAOvI6n4Fw5R4E.ILdaC
 KofwXtj7CpBqlCOw3r6PVyDYEygH6Z_83he7qG6p4H4cv7zHR6mdiygIg1Ku
 caS2UytV9MD16I_fMx6auvqi6UhgrQTvG4i7K6V.kbTQEBqDDfbmt3J0pD7W
 ElUcHFlhzf0lhRkRuXuEpIOu..NYvRRkkU2mnFPAxDh9eqUlpsXyv9plyqP9
 ZpRpE6siCkiUcesmJAUNK0RhEwzAmoNwNmkqH60.o1vwOc3pA_2YlKNbDeXS
 eUQ5JU5hRpaPMn2CqMyyHdj9WSyaxSRSCnJMPKrq4J68h3esSW9y8jH_hBFS
 aZ13BFqlfVEc9_5_P9_UqM3LMJY6YvH4126IAQgRz3KSKHkYmWmXJMnOXxOe
 Oz0oBf6D4jfvkVTDTcVeRPeEaDrEQuCTrQffMd6lZtgx25AqzzJufor61ogC
 .ee.pCy.La7YDn9UpHKnIt6iz_yD9Wtwop6gKy96bxiWdTx8v9Waa0GWLJ1y
 JwYhK6BSd95iH2cgiVUV7fQYhXvoUypBca.Ar4sq2yoEhXzy3Sqm90jXKh_P
 94nzt57KAZYvK.GHpkwHMoaHj1YCdeq1d3k61neDbhiGjJDjzwTRK4FN3krv
 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+chNPIhWc5SoNUcWciEf11WBF9GXfBs=;
        h=MIME-version:Content-type:To:From:Sender:Date:List-Unsubscribe:
```

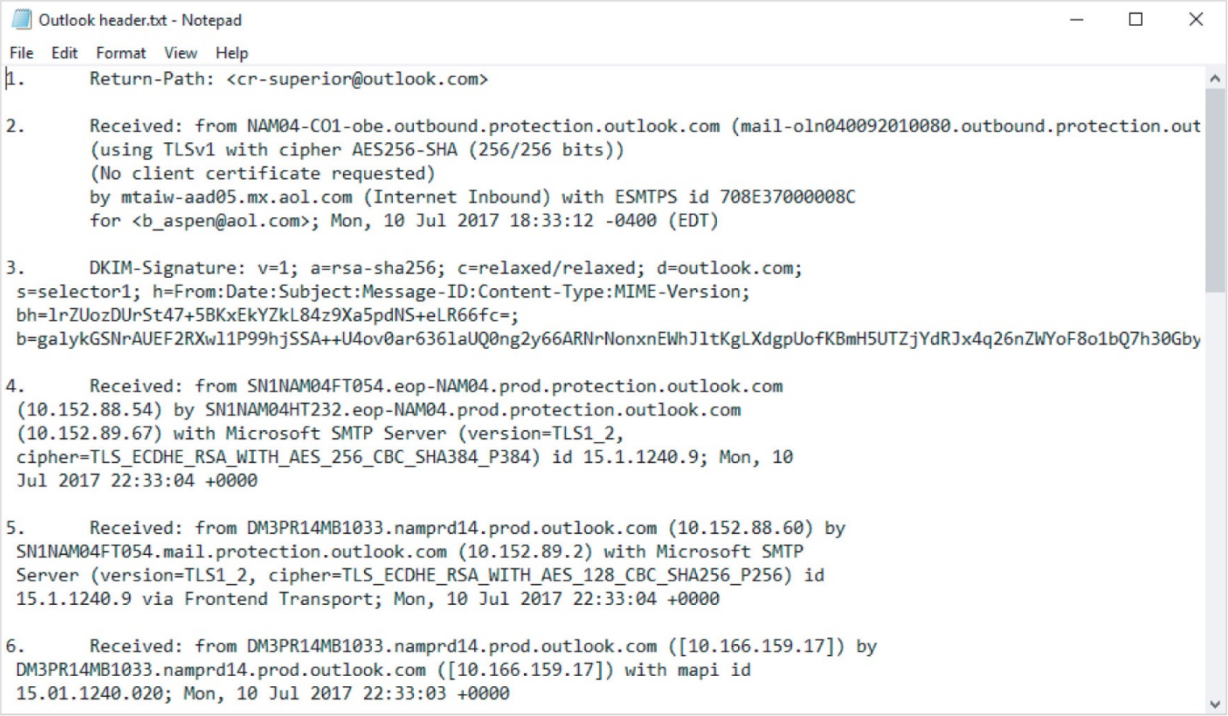
Figure 11-3 Viewing headers in Yahoo!

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

Examining E-mail Headers (1 of 2)

- 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 2)



```
1.      Return-Path: <cr-superior@outlook.com>

2.      Received: from NAM04-CO1-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=lrZUozDUrSt47+5BKxEkYZkL84z9Xa5pdNS+eLR66fc=;
 b=galykGSNrAUEF2RXwl1P99hjSSA++U4ov0ar636laUQ0ng2y66ARNrNonxnEWhJ1tKgLXdgpUofKBmH5UTZjYdRJx4q26nZWYoF8o1bQ7h30Gby

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 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

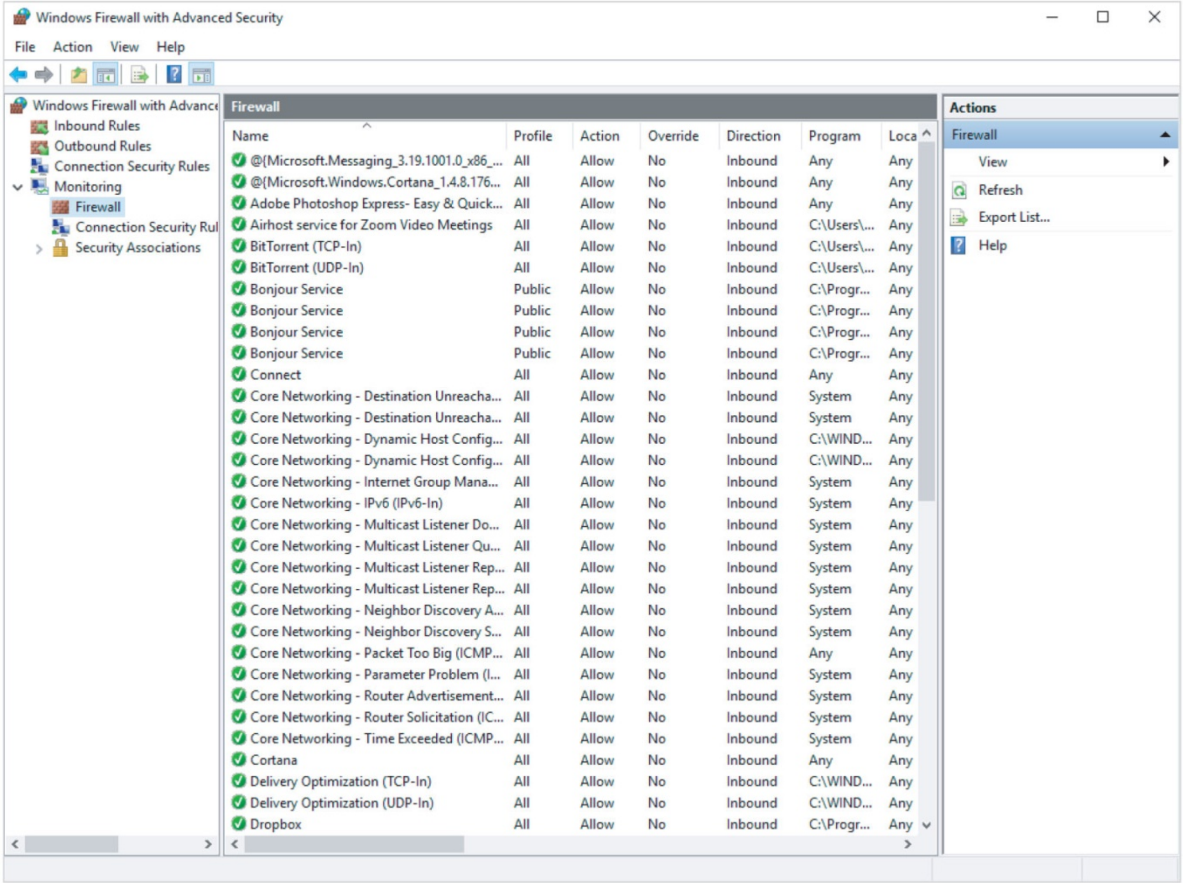
Tracing an E-mail Message

- 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)



Windows Firewall with Advanced Security

Firewall

Name	Profile	Action	Override	Direction	Program	Loca
✓ @{Microsoft.Messaging_3.19.1001.0_x86_...	All	Allow	No	Inbound	Any	Any
✓ @{Microsoft.Windows.Cortana_1.4.8.176...	All	Allow	No	Inbound	Any	Any
✓ Adobe Photoshop Express- Easy & Quick...	All	Allow	No	Inbound	Any	Any
✓ Airhost service for Zoom Video Meetings	All	Allow	No	Inbound	C:\Users\...	Any
✓ BitTorrent (TCP-In)	All	Allow	No	Inbound	C:\Users\...	Any
✓ BitTorrent (UDP-In)	All	Allow	No	Inbound	C:\Users\...	Any
✓ Bonjour Service	Public	Allow	No	Inbound	C:\Progr...	Any
✓ Bonjour Service	Public	Allow	No	Inbound	C:\Progr...	Any
✓ Bonjour Service	Public	Allow	No	Inbound	C:\Progr...	Any
✓ Bonjour Service	Public	Allow	No	Inbound	C:\Progr...	Any
✓ Connect	All	Allow	No	Inbound	Any	Any
✓ Core Networking - Destination Unreacha...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Destination Unreacha...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Dynamic Host Config...	All	Allow	No	Inbound	C:\WIND...	Any
✓ Core Networking - Dynamic Host Config...	All	Allow	No	Inbound	C:\WIND...	Any
✓ Core Networking - Internet Group Mana...	All	Allow	No	Inbound	System	Any
✓ Core Networking - IPv6 (IPv6-In)	All	Allow	No	Inbound	System	Any
✓ Core Networking - Multicast Listener Do...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Multicast Listener Qu...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Multicast Listener Rep...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Multicast Listener Rep...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Neighbor Discovery A...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Neighbor Discovery S...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Packet Too Big (ICMP...	All	Allow	No	Inbound	Any	Any
✓ Core Networking - Parameter Problem (I...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Router Advertisement...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Router Solicitation (IC...	All	Allow	No	Inbound	System	Any
✓ Core Networking - Time Exceeded (ICMP...	All	Allow	No	Inbound	System	Any
✓ Cortana	All	Allow	No	Inbound	Any	Any
✓ Delivery Optimization (TCP-In)	All	Allow	No	Inbound	C:\WIND...	Any
✓ Delivery Optimization (UDP-In)	All	Allow	No	Inbound	C:\WIND...	Any
✓ Dropbox	All	Allow	No	Inbound	C:\Progr...	Any

Figure 11-5 A Windows firewall log

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 have to 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 UNIX E-mail Server Logs (1 of 2)

- Common UNIX e-mail servers: Postfix and Sendmail
- `/etc/sendmail.cf`
  - Configuration file for Sendmail
- `/etc/syslog.conf`
  - Specifies how and which events Sendmail logs
- Postfix has two configuration files
  - `master. cf` and `main.cf` (found in `/etc/postfix`)

Examining UNIX 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 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

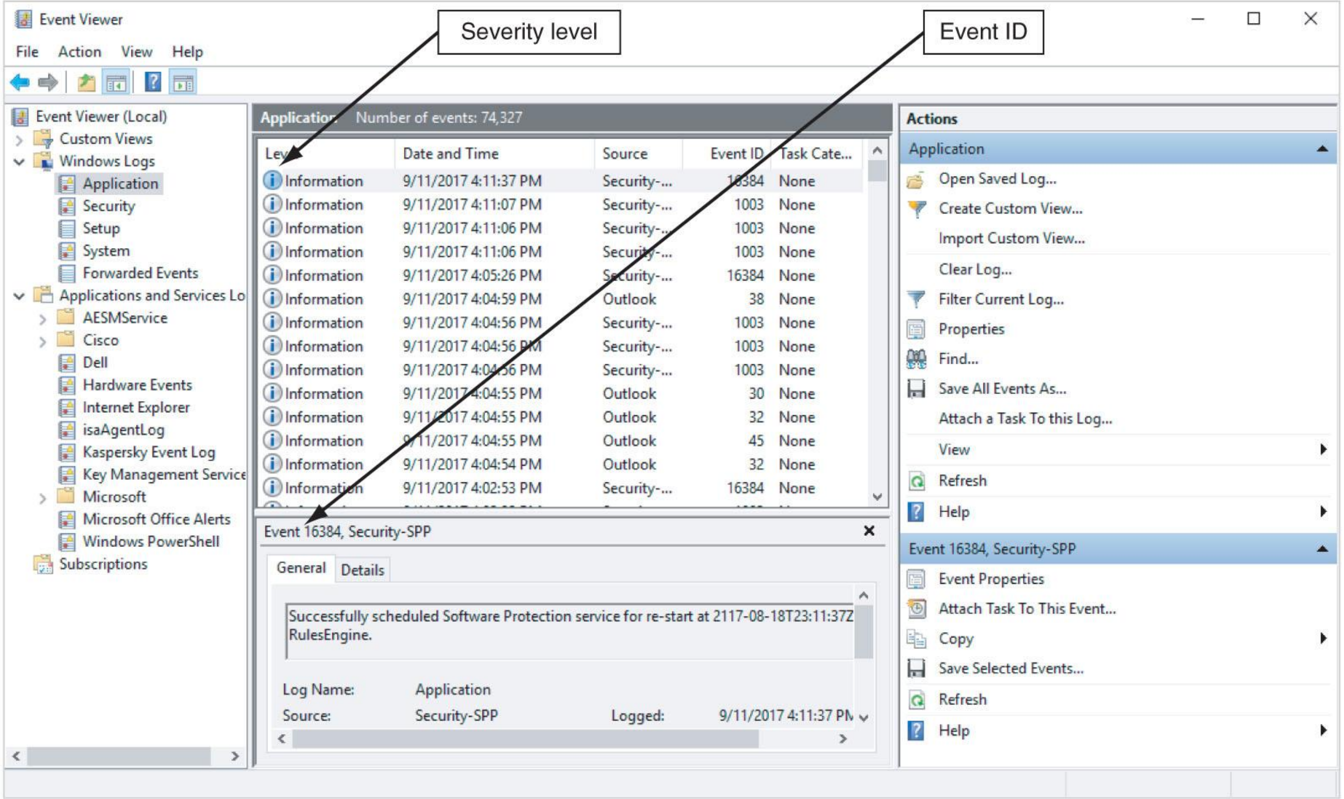
Examining Microsoft E-mail Server Logs (2 of 4)

- 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)



Severity level

Event ID

Application Number of events: 74,327

Lev	Date and Time	Source	Event ID	Task Cate...
Information	9/11/2017 4:11:37 PM	Security-...	16384	None
Information	9/11/2017 4:11:07 PM	Security-...	1003	None
Information	9/11/2017 4:11:06 PM	Security-...	1003	None
Information	9/11/2017 4:11:06 PM	Security-...	1003	None
Information	9/11/2017 4:05:26 PM	Security-...	16384	None
Information	9/11/2017 4:04:59 PM	Outlook	38	None
Information	9/11/2017 4:04:56 PM	Security-...	1003	None
Information	9/11/2017 4:04:56 PM	Security-...	1003	None
Information	9/11/2017 4:04:56 PM	Security-...	1003	None
Information	9/11/2017 4:04:55 PM	Outlook	30	None
Information	9/11/2017 4:04:55 PM	Outlook	32	None
Information	9/11/2017 4:04:55 PM	Outlook	45	None
Information	9/11/2017 4:04:54 PM	Outlook	32	None
Information	9/11/2017 4:02:53 PM	Security-...	16384	None

Event 16384, Security-SPP

General Details

Successfully scheduled Software Protection service for re-start at 2117-08-18T23:11:37Z RulesEngine.

Log Name: Application
Source: Security-SPP Logged: 9/11/2017 4:11:37 PM

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 formatas and large data sets
  - Fookes Aid4Mail and MailBag Assistant
  - Paraben E-Mail Examiner
  - AccessData FTK for Outlook and Outlook Express
  - 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

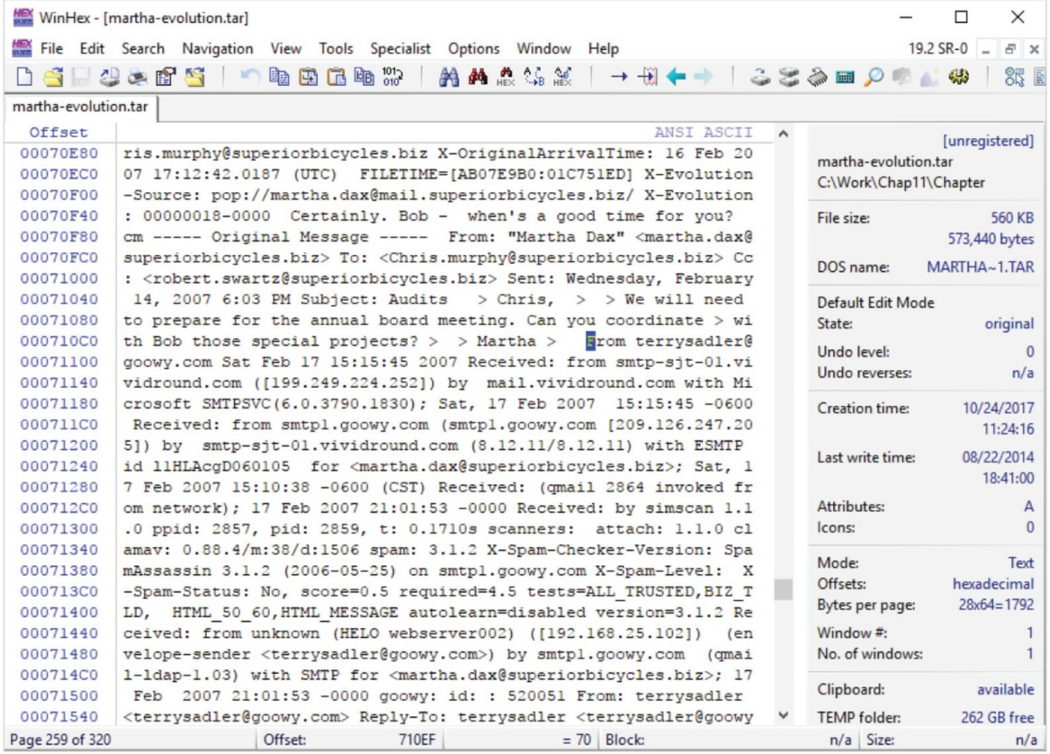
Using Specialized E-mail Forensics Tools (3 of 3)

- 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
    - Magnet AXIOM
    - OSForensics

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

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



```
Offset                                                              ANSI ASCII
00070E80  ris.murphy@superiorbicycles.biz X-OriginalArrivalTime: 16 Feb 20
00070EC0  07 17:12:42.0187 (UTC)  FILETIME=[AB07E9B0:01C751ED] X-Evolution
00070F00  -Source: pop://martha.dax@mail.superiorbicycles.biz/ X-Evolution
00070F40  : 00000018-0000  Certainly. Bob -  when's a good time for you?
00070F80  cm ----- Original Message -----  From: "Martha Dax" <martha.dax@
00070FC0  superiorbicycles.biz> To: <Chris.murphy@superiorbicycles.biz> Cc
00071000  : <robert.swartz@superiorbicycles.biz> Sent: Wednesday, February
00071040   14, 2007 6:03 PM Subject: Audits   > Chris,  >  > We will need
00071080  to prepare for the annual board meeting. Can you coordinate > wi
000710C0  th Bob those special projects? >  > Martha >   From terrysadler@
00071100  goowy.com Sat Feb 17 15:15:45 2007 Received: from smtp-sjt-01.vi
00071140  vidround.com ([199.249.224.252]) by  mail.vividround.com with Mi
00071180  crosoft SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007  15:15:45 -0600
000711C0   Received: from smtpl.goowy.com (smtpl.goowy.com [209.126.247.20
00071200  5]) by  smtp-sjt-01.vividround.com (8.12.11/8.12.11) with ESMTP
00071240  id l1HLAcgD060105  for <martha.dax@superiorbicycles.biz>; Sat, 1
00071280  7 Feb 2007 15:10:38 -0600 (CST) Received: (qmail 2864 invoked fr
000712C0  om network); 17 Feb 2007 21:01:53 -0000 Received: by simscan 1.1
00071300  .0 ppid: 2857, pid: 2859, t: 0.1710s scanners:  attach: 1.1.0 cl
00071340  amav: 0.88.4/m:38/d:1506 spam: 3.1.2 X-Spam-Checker-Version: Spa
00071380  mAssassin 3.1.2 (2006-05-25) on smtpl.goowy.com X-Spam-Level:  X
000713C0  -Spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_T
00071400  LD,  HTML_50_60,HTML_MESSAGE autolearn=disabled version=3.1.2 Re
00071440  ceived: from unknown (HELO webserver002) ([192.168.25.102])  (en
00071480  velope-sender <terrysadler@goowy.com>) by smtpl.goowy.com  (qmai
000714C0  l-ldap-1.03) with SMTP for <martha.dax@superiorbicycles.biz>; 17
00071500   Feb  2007 21:01:53 -0000 goowy: id: : 520051 From: terrysadler
00071540  <terrysadler@goowy.com> Reply-To: terrysadler <terrysadler@goowy
```

[unregistered]
martha-evolution.tar
C:\Work\Chap11\Chapter

File size: 560 KB
573,440 bytes

DOS name: MARTHA~1.TAR

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 10/24/2017 11:24:16

Last write time: 08/22/2014 18:41:00

Attributes: A
Icons: 0

Mode: Text
Offsets: hexadecimal
Bytes per page: 28x64=1792

Window #: 1
No. of windows: 1

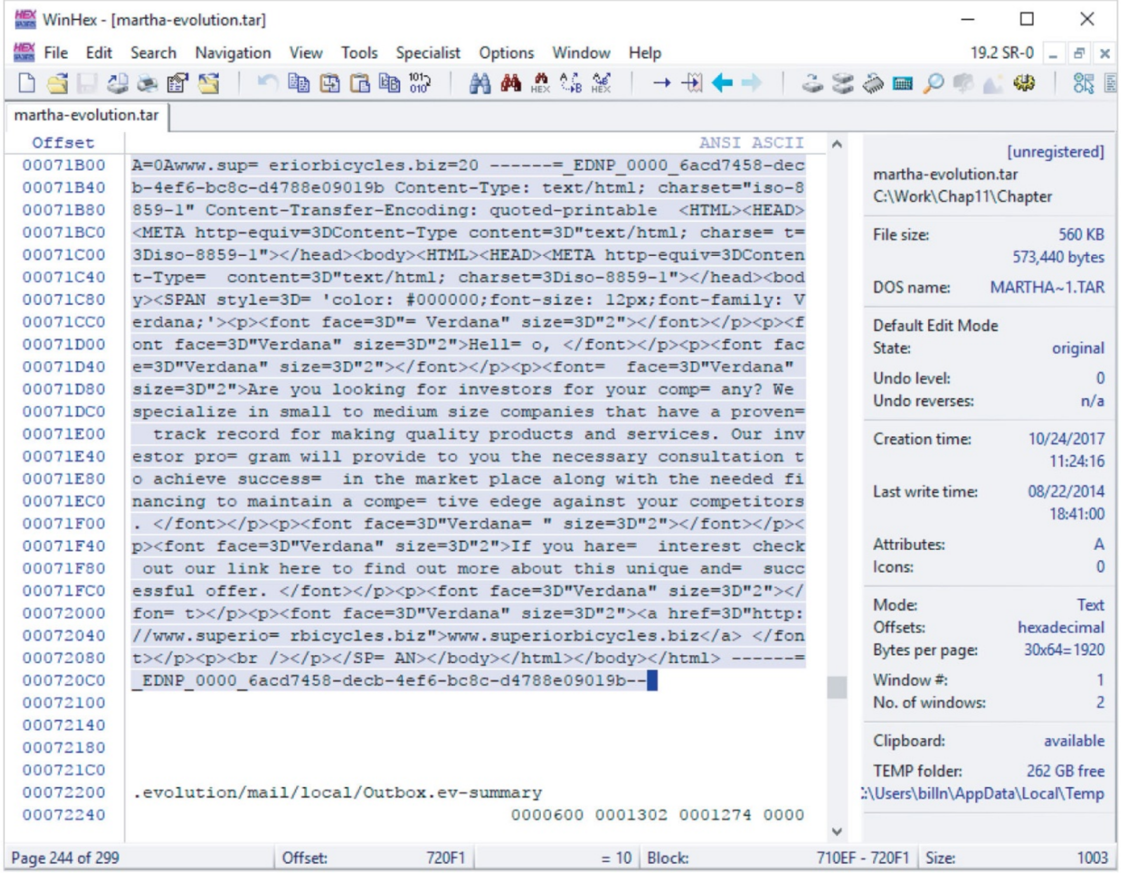
Clipboard: available
TEMP folder: 262 GB free

Page 259 of 320 | Offset: 710EF | = 70 | Block: n/a | Size: n/a

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)



```
Offset                                                                    ANSI ASCII
00071B00   A=0Awww.sup= eriorbicycles.biz=20 ------=_EDNP_0000_6acd7458-dec
00071B40   b-4ef6-bc8c-d4788e09019b Content-Type: text/html; charset="iso-8
00071B80   859-1" Content-Transfer-Encoding: quoted-printable  <HTML><HEAD>
00071BC0   <META http-equiv=3DContent-Type content=3D"text/html; charse= t=
00071C00   3Diso-8859-1"></head><body><HTML><HEAD><META http-equiv=3DConten
00071C40   t-Type=  content=3D"text/html; charset=3Diso-8859-1"></head><bod
00071C80   y><SPAN style=3D= 'color: #000000;font-size: 12px;font-family: V
00071CC0   erdana;'><p><font face=3D"= Verdana" size=3D"2"></font></p><p><f
00071D00   ont face=3D"Verdana" size=3D"2">Hell= o, </font></p><p><font fac
00071D40   e=3D"Verdana" size=3D"2"></font></p><p><font=  face=3D"Verdana"
00071D80   size=3D"2">Are you looking for investors for your comp= any? We
00071DC0   specialize in small to medium size companies that have a proven=
00071E00     track record for making quality products and services. Our inv
00071E40   estor pro= gram will provide to you the necessary consultation t
00071E80   o achieve success=  in the market place along with the needed fi
00071EC0   nancing to maintain a compe= tive edege against your competitors
00071F00   . </font></p><p><font face=3D"Verdana= " size=3D"2"></font></p><
00071F40   p><font face=3D"Verdana" size=3D"2">If you hare=  interest check
00071F80    out our link here to find out more about this unique and=  succ
00071FC0   essful offer. </font></p><p><font face=3D"Verdana" size=3D"2"></
00072000   fon= t></p><p><font face=3D"Verdana" size=3D"2"><a href=3D"http:
00072040   //www.superio= rbicycles.biz">www.superiorbicycles.biz</a> </fon
00072080   t></p><p><br /></p></SP= AN></body></html></body></html> ------=
000720C0   _EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b--
00072100
00072140
00072180
000721C0
00072200   .evolution/mail/local/Outbox.ev-summary
00072240                                      0000600 0001302 0001274 0000
```

[unregistered]
martha-evolution.tar
C:\Work\Chap11\Chapter

File size: 560 KB
573,440 bytes

DOS name: MARTHA~1.TAR

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 10/24/2017
11:24:16

Last write time: 08/22/2014
18:41:00

Attributes: A
Icons: 0

Mode: Text
Offsets: hexadecimal
Bytes per page: 30x64=1920

Window #: 1
No. of windows: 2

Clipboard: available

TEMP folder: 262 GB free
:\Users\billn\AppData\Local\Temp

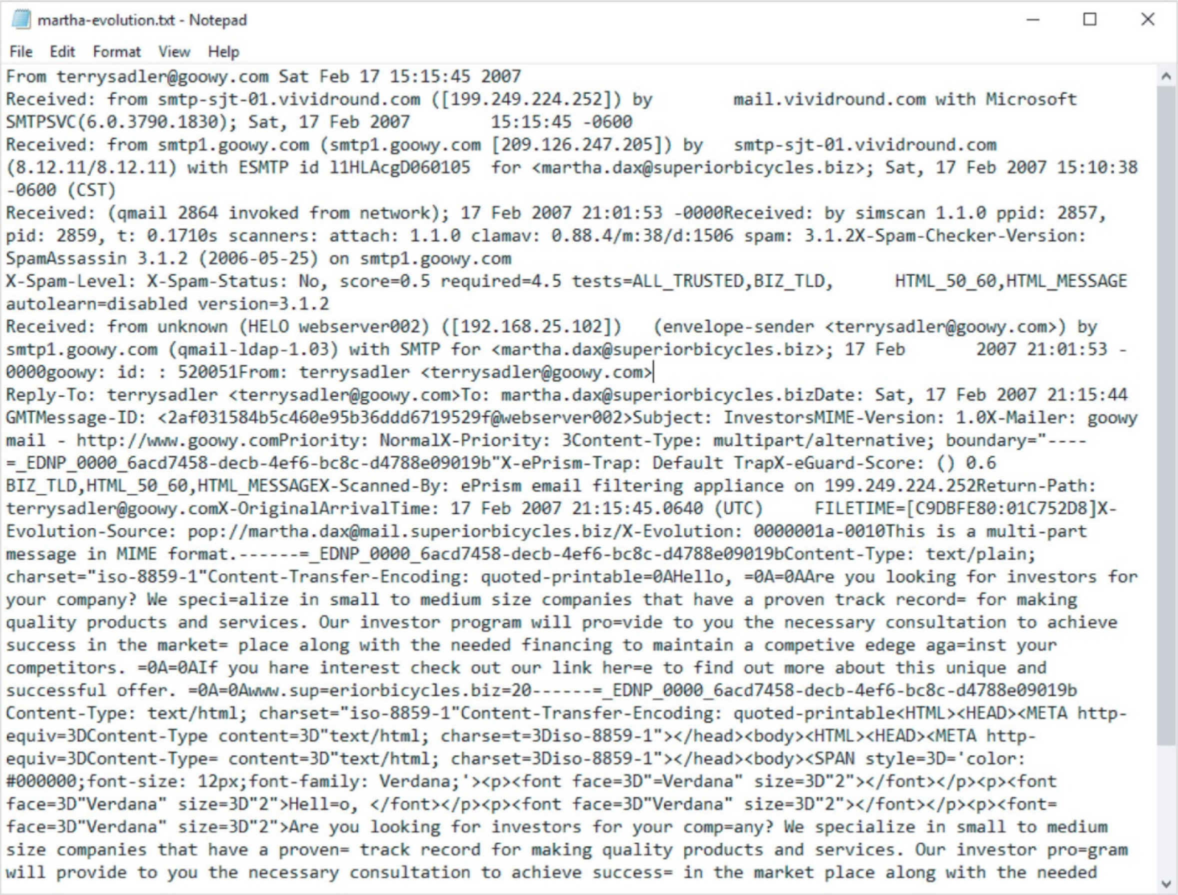
Page 244 of 299 | Offset: 720F1 | = 10 | Block: 710EF - 720F1 | Size: 1003

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

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

CENGAGE

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



```
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 l1HLAcgD060105  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 competive 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=o, </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 recovery files from VMware and Virtual PC

E-mail Case Studies

- In the Enron Case, more than 10,00 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

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