

# **Guide to Computer Forensics and Investigations Fifth Edition**

## *Chapter 11 E-mail and Social Media Investigations*

# 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
- Explain how to approach investigating social media communications
- Describe some available e-mail forensics tools

# Exploring the Role of E-mail in Investigations

- 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

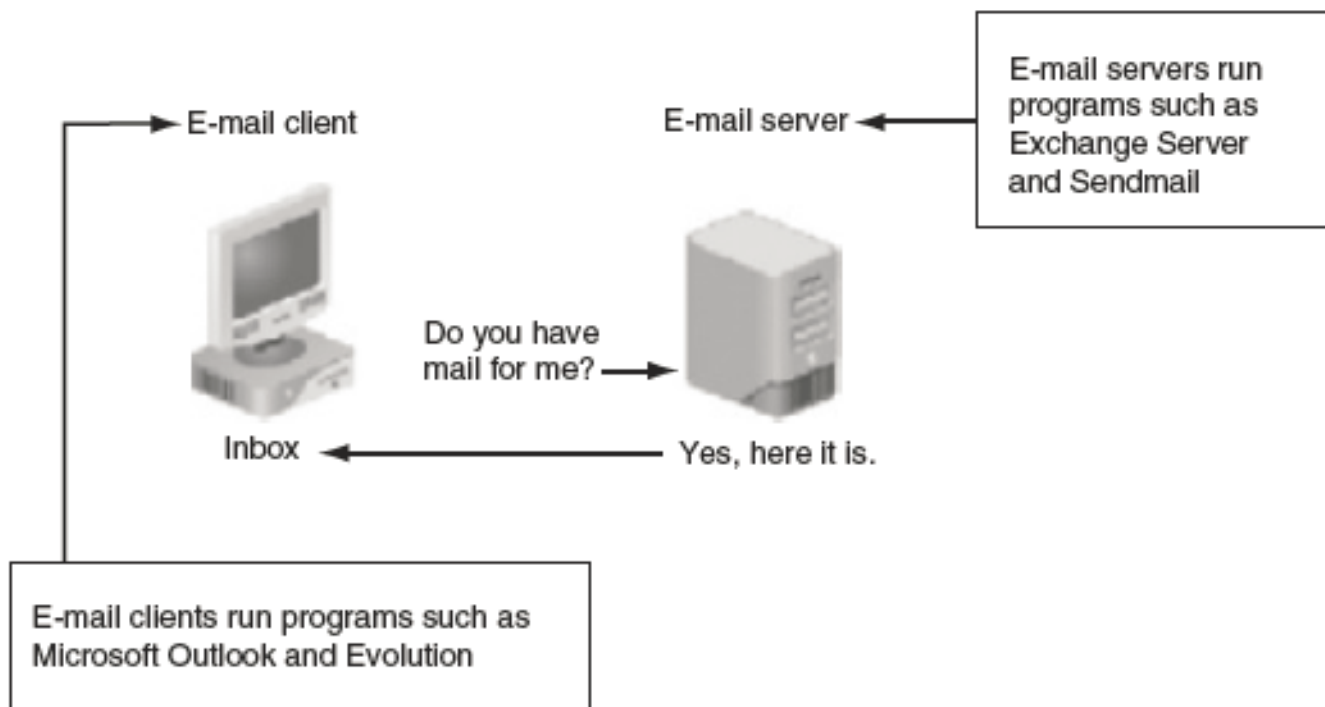
# Exploring the Role of E-mail in Investigations

- **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

- 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



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

© Cengage Learning®

# Exploring the Roles of the Client and Server in E-mail

- 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

- 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



# Investigating E-mail Crimes and Violations

- 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

- Access victim's computer or mobile device to recover the evidence
- Using the victim's e-mail client
  - Find and copy evidence in the e-mail
  - 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

- 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

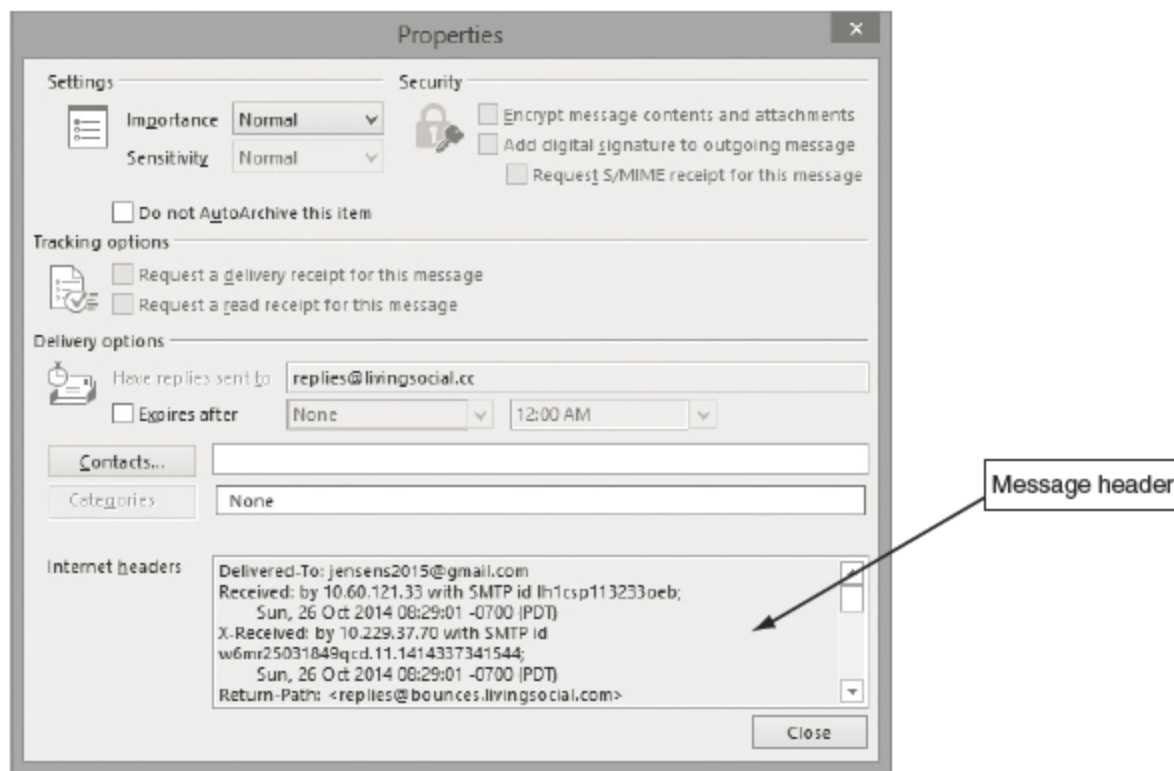
# Viewing E-mail Headers

- 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

- Outlook
  - Double-click the message and then click **File, Properties**
  - Copy headers
  - Paste them to any text editor
  - Save the document as `OutlookHeader.txt` in your work folder

# Viewing E-mail Headers

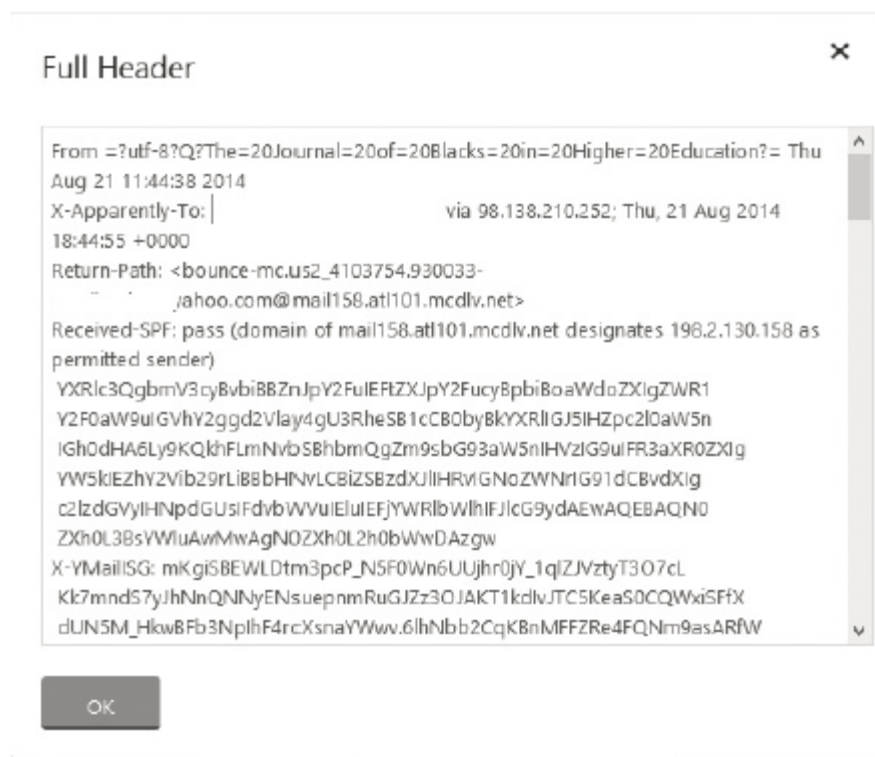


**Figure 11-2** An Outlook e-mail header  
Courtesy of Microsoft Corporation

# Viewing E-mail Headers

- AOL
  - Click the **Options** link, click **E-mail Settings**
  - Click **Always show full headers** check box (Save settings)
  - Click **Back to E-mail**
- Yahoo
  - Click **Inbox** to view a list of messages
  - Above the message window, click **More** and click **View Full Header**
  - Copy and paste headers to a text file

# Viewing E-mail Headers



**Figure 11-3** Viewing headers in Yahoo!

Source: Yahoo! Inc.



# Examining E-mail Headers

- Headers contain useful information
  - The mail 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



```
Outlook Header.txt - Notepad
File Edit Format View Help
1. Received: from SN2PR0801MB0752.namprd08.prod.outlook.com (25.160.57.146) by
   CO2PR0801MB0744.namprd08.prod.outlook.com (25.160.10.142) with Microsoft SMTP
   Server (TLS) id 15.0.1039.15 via Mailbox Transport; Fri, 26 Sep 2014 17:34:08
   +0000
2. Received: from BL2PR08CA0060.namprd08.prod.outlook.com (10.255.170.178) by
   SN2PR0801MB0752.namprd08.prod.outlook.com (25.160.57.146) with Microsoft SMTP
   Server (TLS) id 15.0.1034.13; Fri, 26 Sep 2014 17:34:07 +0000
3. Received: from 0N1AFF011FD000.protection.gbl (2a01:111:f400:7c10::137) by
   BL2PR08CA0060.outlook.office365.com (2a01:111:e400:c4b::50) with Microsoft
   SMTP Server (TLS) id 15.0.1039.15 via Frontend Transport; Fri, 26 Sep 2014
   17:34:06 +0000
4. Received: from online.itwhitpapers.com (66.186.127.67) by
   0N1AFF011FD000.mail.protection.outlook.com (10.58.52.68) with Microsoft SMTP
   Server id 15.0.1029.15 via Frontend Transport; Fri, 26 Sep 2014 17:34:05
   +0000
5. DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; q=dns/txt; l=15361;
   d=online.itwhitpapers.com;s=2008;
   h=from;
   bh=cCk0dA0xetgRz+Ivn6Ms00IdH0ATbWQa7a00hRgkw@s-;
   b=ChreKQ0J2RA0YU7LCiyo4IDym0Ldx2exbV0K0AuZg2gB7NO/czF144fenPnQzV100XIyvm
   +K7nqB6vpRlrome-;
6. DomainKey-Signature: a=rsa-sha1; q=dns; c=noews; s=2008; d=online.itwhitpapers.com;
   h=from;
   b=HajRzpeS96QqkOg715G32eTA/BIgspIh0fMh06GIRQ71C+jpA3qClBo148QgPMIG4e3MPwH 3dcH95Tzotnq4=
7. From: "ITwhitpapers Business Intelligence" <online_resources@online.itwhitpapers.com>
8. To: caphillip@blah.edu
9. Subject: Build a Business Case: Developing Custom Apps
10. Date: Fri, 26 Sep 2014 13:30:00 -0400
11. MIME-Version: 1.0
12. Content-Type: multipart/alternative;
```

**Figure 11-4** An e-mail header with line numbers added  
Courtesy of Microsoft Corporation

# 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

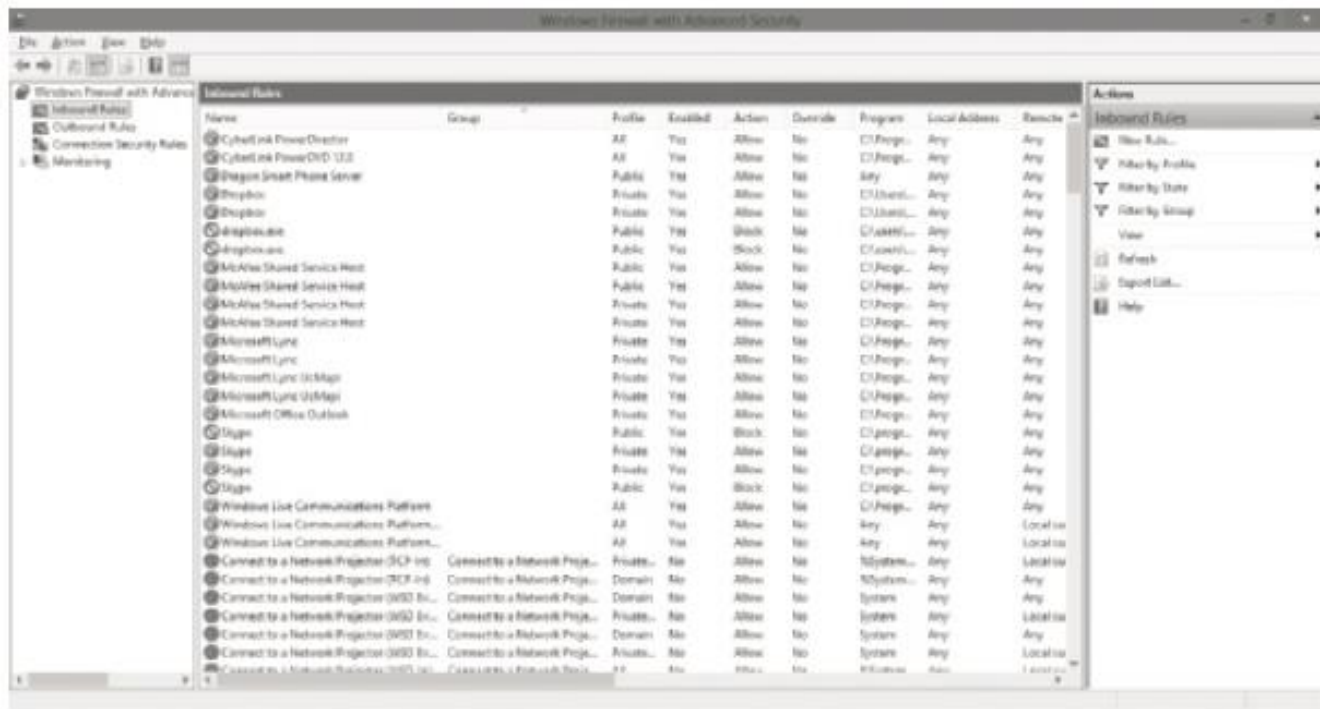
# Tracing an E-mail Message

- 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](http://www.arin.net)
  - [www.internic.com](http://www.internic.com)
  - [www.google.com](http://www.google.com)
- Verify your findings by checking network e-mail logs against e-mail addresses

# Using Network E-mail Logs

- 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



**Figure 11-5** A Windows firewall log

Courtesy of Microsoft Corporation

# Understanding E-mail Servers

- 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

- 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

- 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

- `/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

- 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

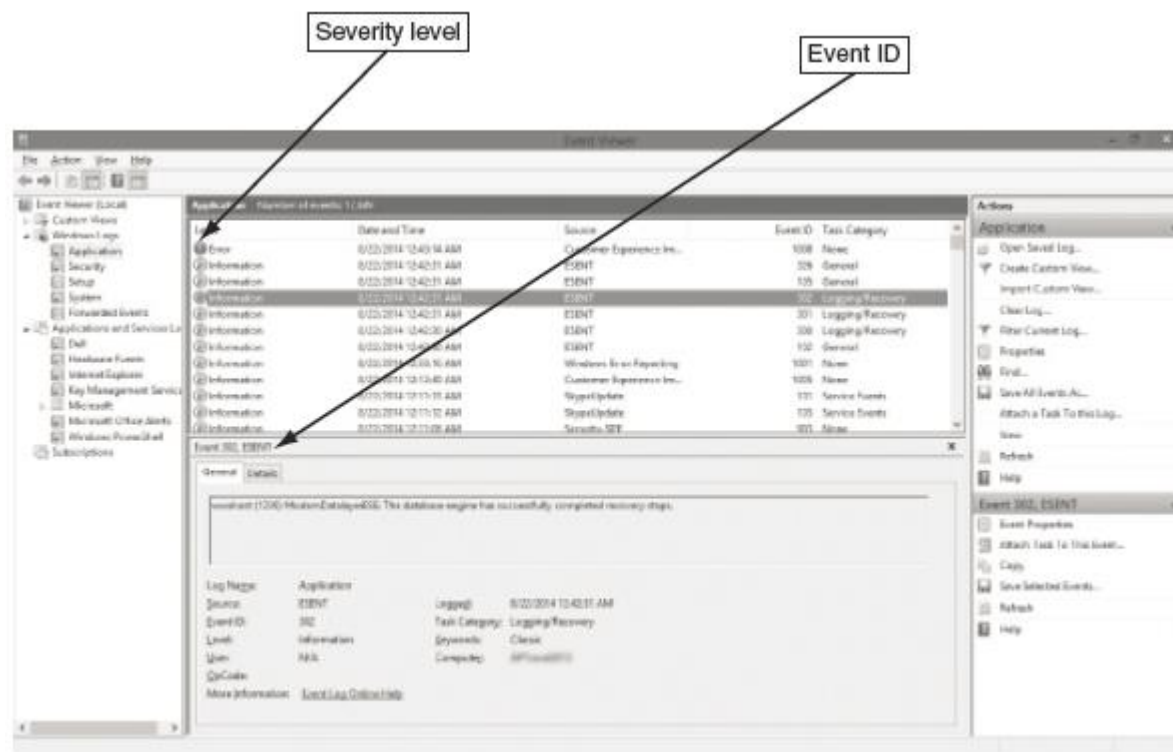
# Examining Microsoft E-mail Server Logs

- 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

- 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



**Figure 11-6** Viewing a log in Event Viewer  
Courtesy of Microsoft Corporation

# Using Specialized E-mail Forensics Tools

- Tools include:
  - DataNumen for Outlook and Outlook Express
  - FINALeMAIL for Outlook Express and Eudora
  - Sawmill for Novell GroupWise
  - DBXtract for Outlook Express
  - 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

- 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



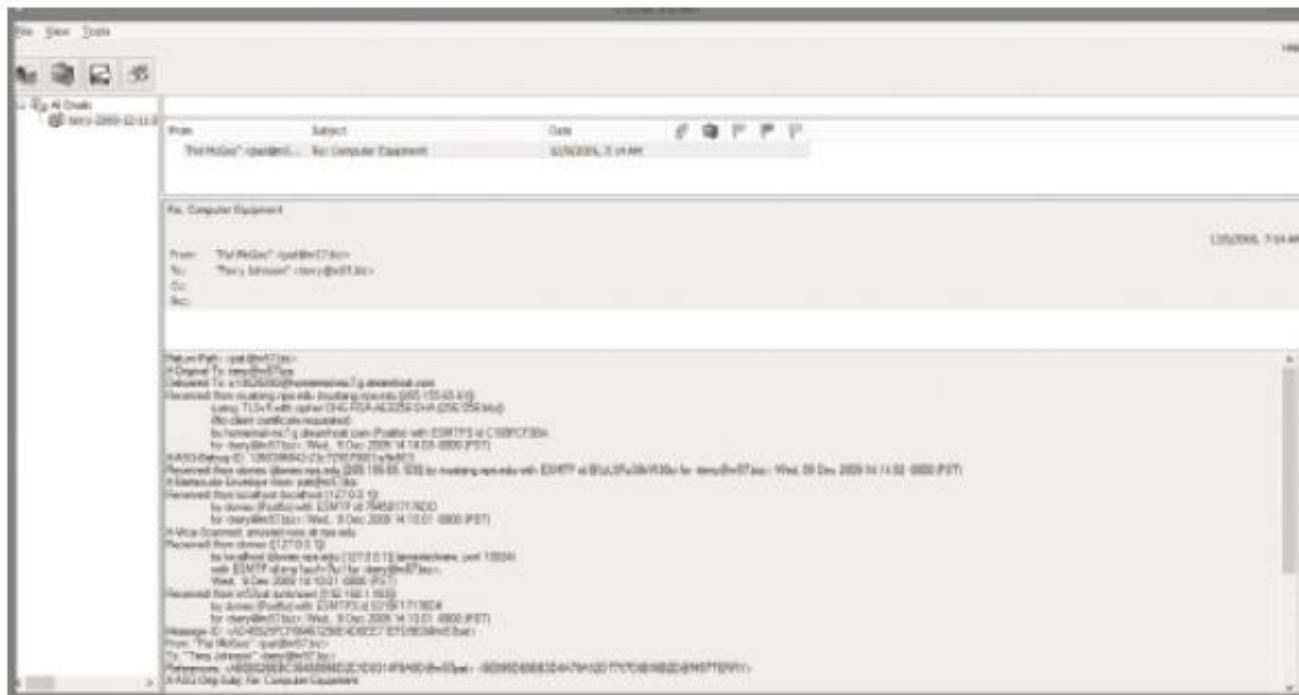
# Using Specialized E-mail Forensics Tools

- 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 OSForensics to Recover E-mail

- OSForensics
  - Indexes data on a disk image or an entire drive for faster data retrieval
  - Filters or finds files specific to e-mail clients and servers
- Follow the steps in the activity on page 439 to learn how to use OSForensics to recover e-mails

# Using OSForensics to Recover E-mail



**Figure 11-7** Viewing e-mail headers in OSForensics

Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)

# Using a Hex Editor to Carve E-mail Messages

- Very 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



**Figure 11-8** WinHex displaying the beginning of the e-mail from Terry Sadler  
Courtesy of X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

# Using a Hex Editor to Carve E-mail Messages



**Figure 11-9** WinHex displaying the ending position of the e-mail from Terry Sadler  
Courtesy of X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

# Using a Hex Editor to Carve E-mail Messages



```
File Edit Format View Help
Martha-emailed-out - Notepad

From: terry.sadler@gooey.com [mailto:terry.sadler@gooey.com]
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.gooey.com ([smtp1.gooey.com [209.126.247.205]]) by smtp-sjt-01.vividround.com
(8.12.11/8.12.11) with ESMTP id 1198Acg0040105 for <martha.dan@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: 0.1718s scanners: attach: 1.1.0 clamav: 0.80.4/m:38/d:1506 spam: 3.1.2X-Spam-Checker-Version:
SpamAssassin 3.1.2 (2006-05-25) on smtp1.gooey.com
X-Spam-Level: X-Spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_TLD, HTML_50_40,HTML_MESSAGE
autolearn=disabled version=3.1.2
Received: from unknown (HELO webserver002) ([192.168.25.102]) (envelope-sender <terry.sadler@gooey.com>) by
smtp1.gooey.com (qmail-lsdp-1.03) with SMTP for <martha.dan@superiorbicycles.biz>; 17 Feb 2007 21:01:53 -
0000gooey; id: 520051From: terry.sadler <terry.sadler@gooey.com>
Reply-To: terry.sadler <terry.sadler@gooey.com>To: martha.dan@superiorbicycles.bizDate: Sat, 17 Feb 2007 21:15:44
(UTC)Message-ID: <2a003158d65c480e95b36d067195294@webserver002>Subject: InvestorsTIME-Version: 1.0X-Mailer: gooey
mail - http://www.gooey.comPriority: NormalX-Priority: 3Content-Type: multipart/alternative; boundary="-----
- BDRP_0000_6acd7458-decb-4ef6-bc8c-d478be09019b"X-Prism-Trap: Default TrapX-Guard-Score: {} 0.6
BIZ_TLD,HTML_50_40,HTML_MESSAGEX-Scanned-By: ePrism email filtering appliance on 199.249.224.252Return-Path:
terry.sadler@gooey.comX-OriginalArrivalTime: 17 Feb 2007 21:15:45.0640 (UTC) FILETIME=[C90F080E-01C75208]X-
Evolution-Source: pop://martha.dan@mail.superiorbicycles.biz/X-Evolution: 0000001a-0010This is a multi-part
message in MIME format.----- BDRP_0000_6acd7458-decb-4ef6-bc8c-d478be09019bContent-Type: text/plain;
charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable=0000Hello, =0000Are you looking for investors for
your company? We specialize in small to medium size companies that have a proven track record for making
quality products and services. Our investor program will provide to you the necessary consultation to achieve
success in the market place along with the needed financing to maintain a competitive edge against your
competitors. =0000If you have interest check out our link here to find out more about this unique and
successful offer. =0000www.sup-eriorbicycles.biz=20----- BDRP_0000_6acd7458-decb-4ef6-bc8c-d478be09019b
Content-Type: text/html; charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable<HTML><HEAD><META http-
equiv=3DContent-Type content=3D"text/html"; charset=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">Hello, </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 program
will provide to you the necessary consultation to achieve success- in the market place along with the needed
```

**Figure 11-10** The Terry Sadler e-mail in Notepad  
Courtesy of Microsoft Corporation

# Recovering Outlook Files

- 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

- 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

- 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

- 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

# 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

- 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
- Access victim's computer to recover evidence
  - Copy and print the e-mail message involved in the crime or policy violation

# Summary

- 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

- 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
- Social media forensics tools are still very new
  - Can be used to find out which people users have been in touch with, when, and how often