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

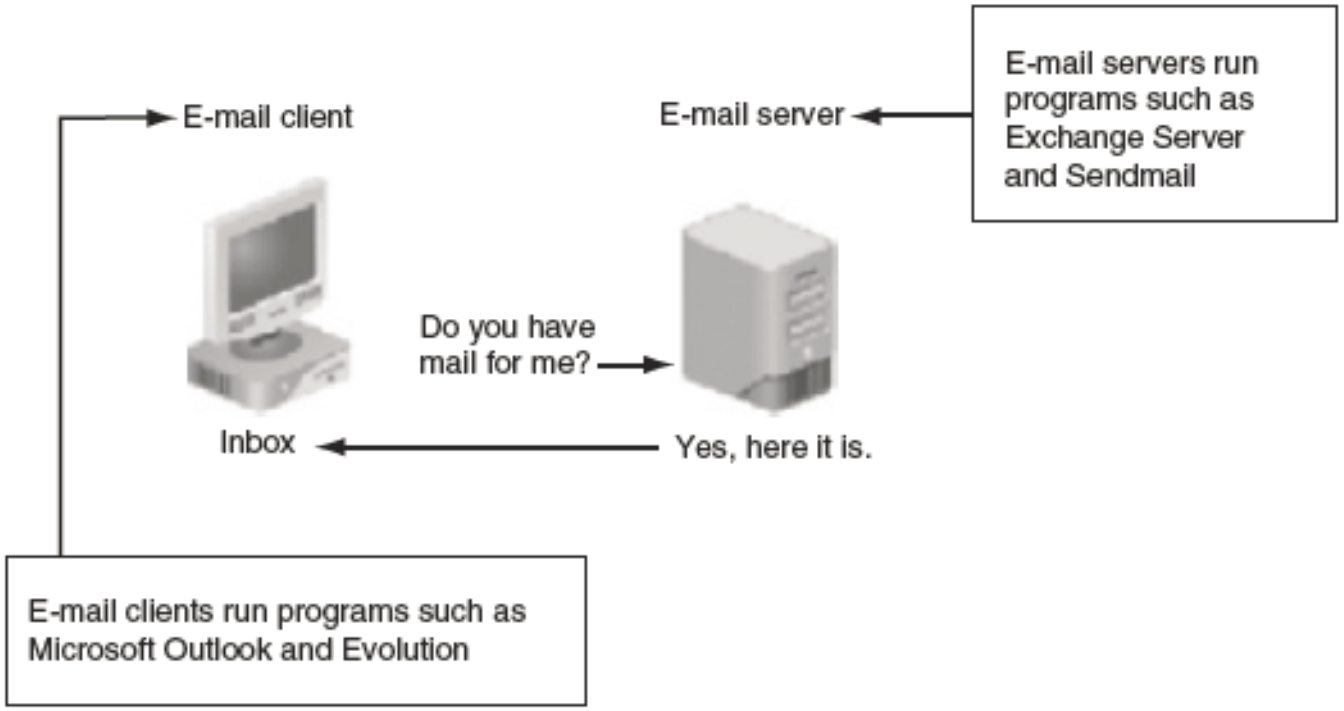

Figure 11-1 E-mail in a client/server architecture

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

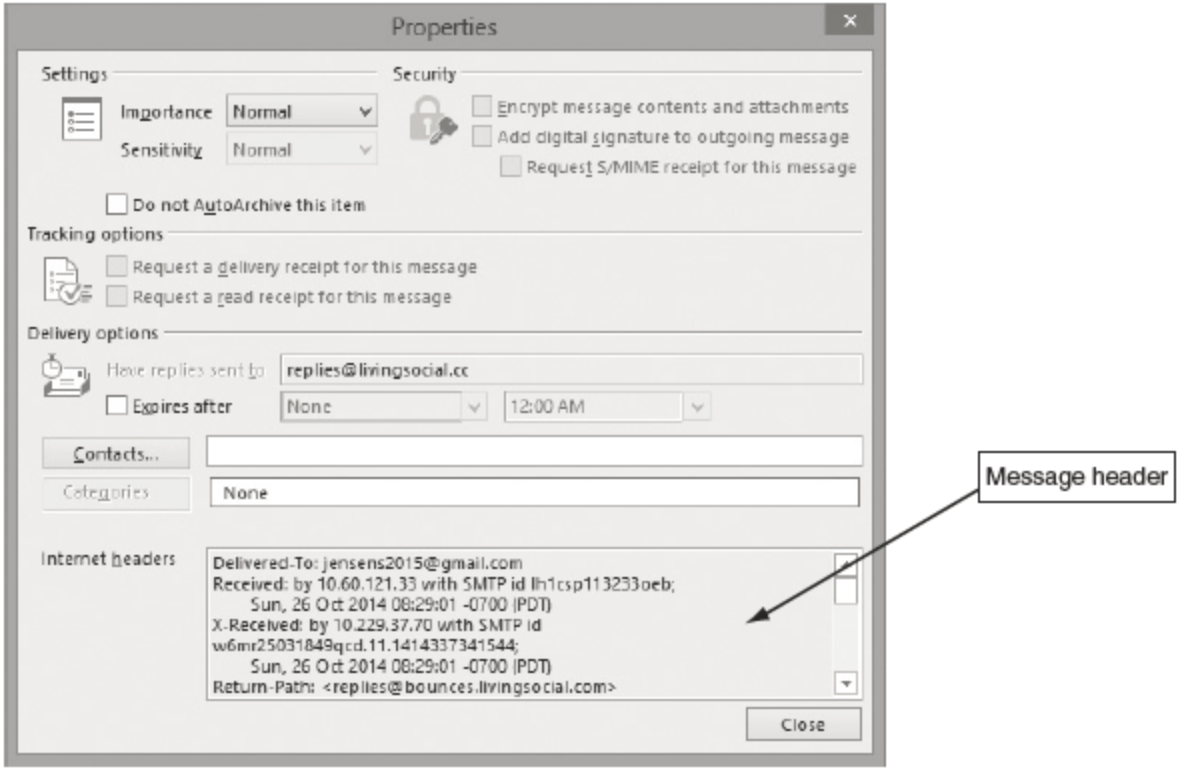

Figure 11-2 An Outlook e-mail header
Courtesy of Microsoft Corporation

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

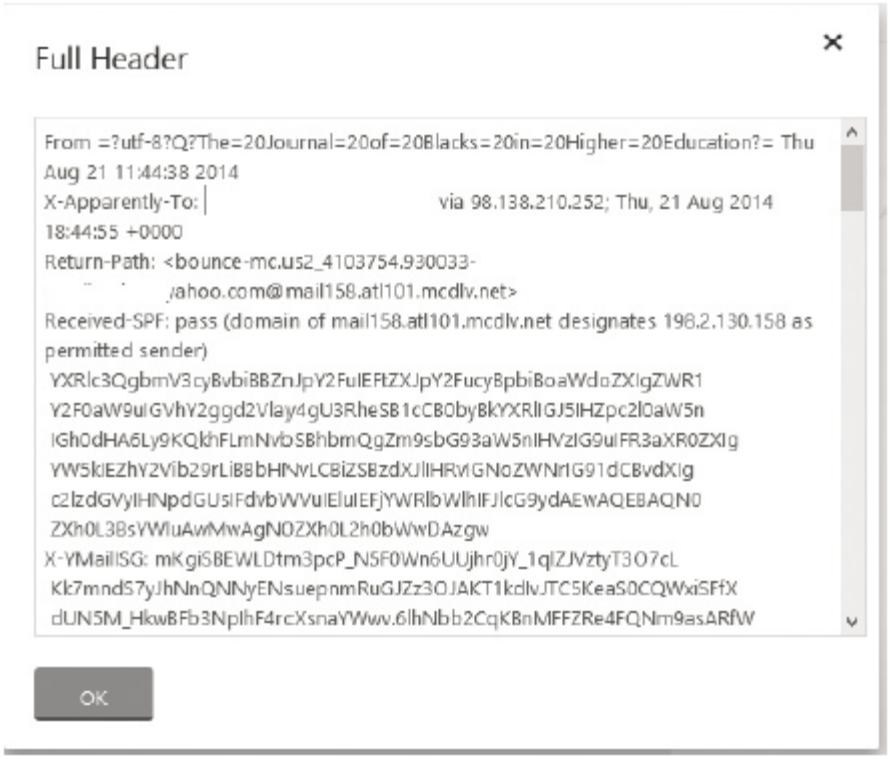

Figure 11-3 Viewing headers in Yahoo!
Source: Yahoo! Inc.

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

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
  - www.internic.com
  - 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

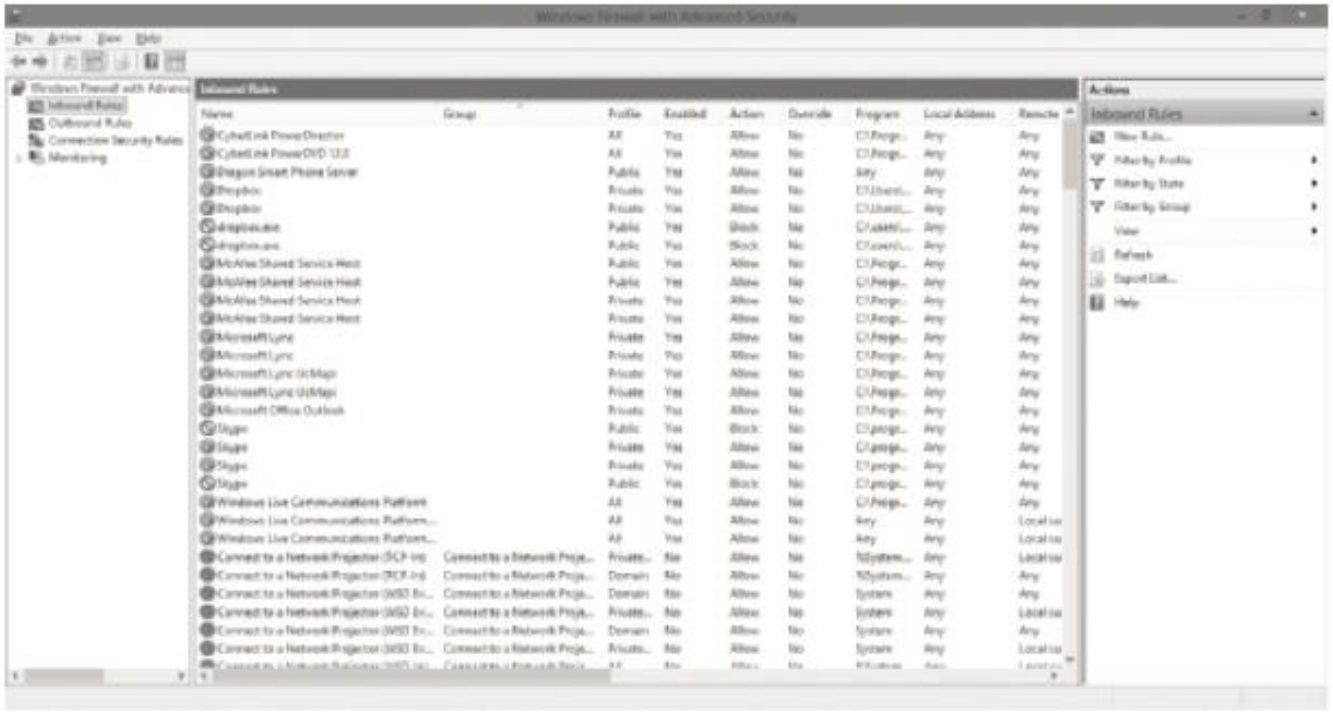

Figure 11-5 A Windows firewall log

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

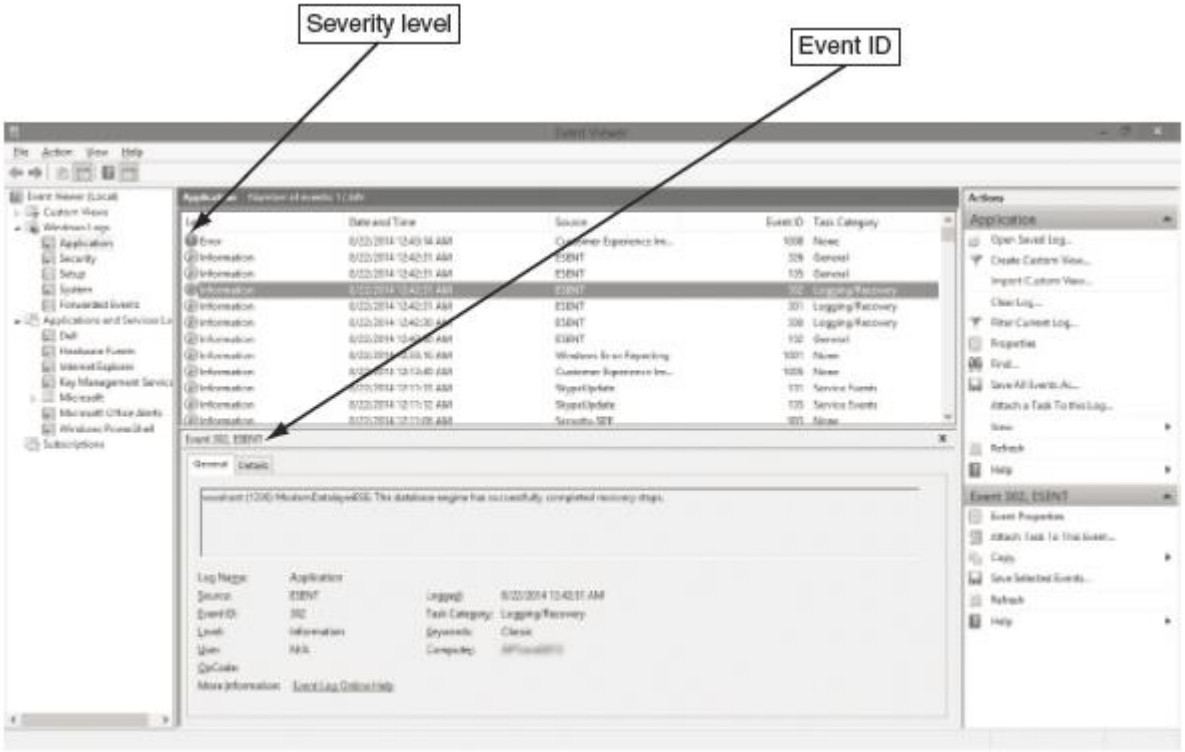

Figure 11-6 Viewing a log in Event Viewer
Courtesy of Microsoft Corporation

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*

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*

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*

Using a Hex Editor to Carve E-mail Messages

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