3.5. Email Investigations

Exploring the Role of E-mail in Investigations

- With the 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 are in HTML format
  - Which allows creating links to text on a Web page
- One of the most noteworthy e-mail scams was 419, or the Nigerian Scam
- Spoofing e-mail can be used to commit fraud

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

- Send and receive e-mail in two environments
  - Internet
  - Controlled LAN, MAN, or WAN
- Client/server architecture
  - Server OS and e-mail software differs from those on the client side
- Protected accounts
  - Require usernames and passwords

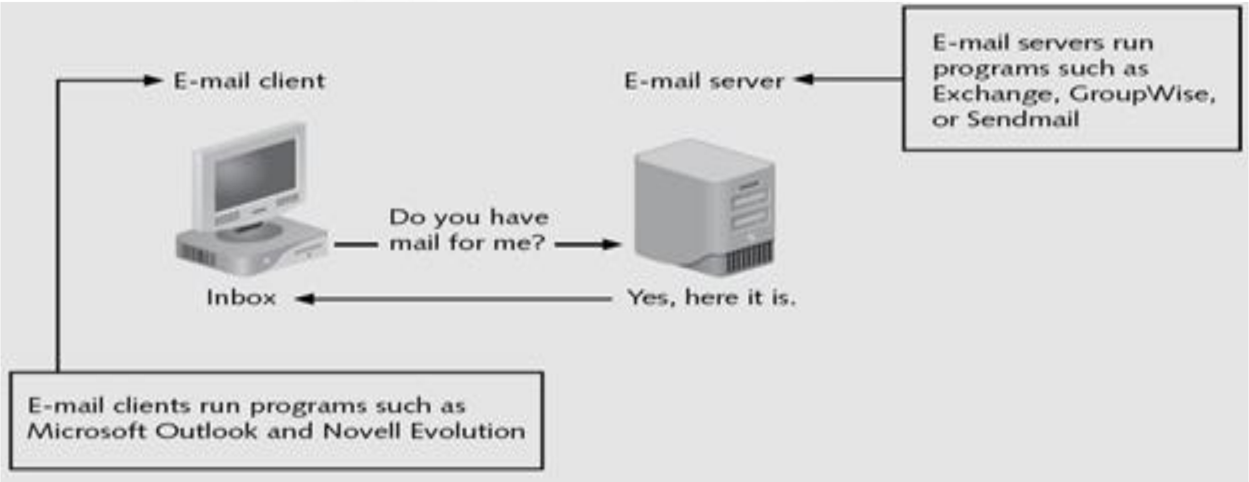

E-mail client
E-mail server
E-mail servers run programs such as Exchange, GroupWise, or Sendmail
Do you have mail for me?
Inbox
Yes, here it is.
E-mail clients run programs such as Microsoft Outlook and Novell Evolution

Fig: E-mail in a client/server architecture

- Name conventions
  - Corporate: john.smith@somecompany.com
  - Public: whatever@hotmail.com
  - Everything after @ belongs to the domain name
- Tracing corporate e-mails is easier
  - Because accounts use standard names the administrator establishes

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
- Depend on the city, state, or country
  - Example: spam
  - Always consult with an attorney
- Becoming commonplace
- Examples of crimes involving e-mails
  - Narcotics trafficking
  - Extortion
  - Sexual harassment
  - Child abductions and pornography

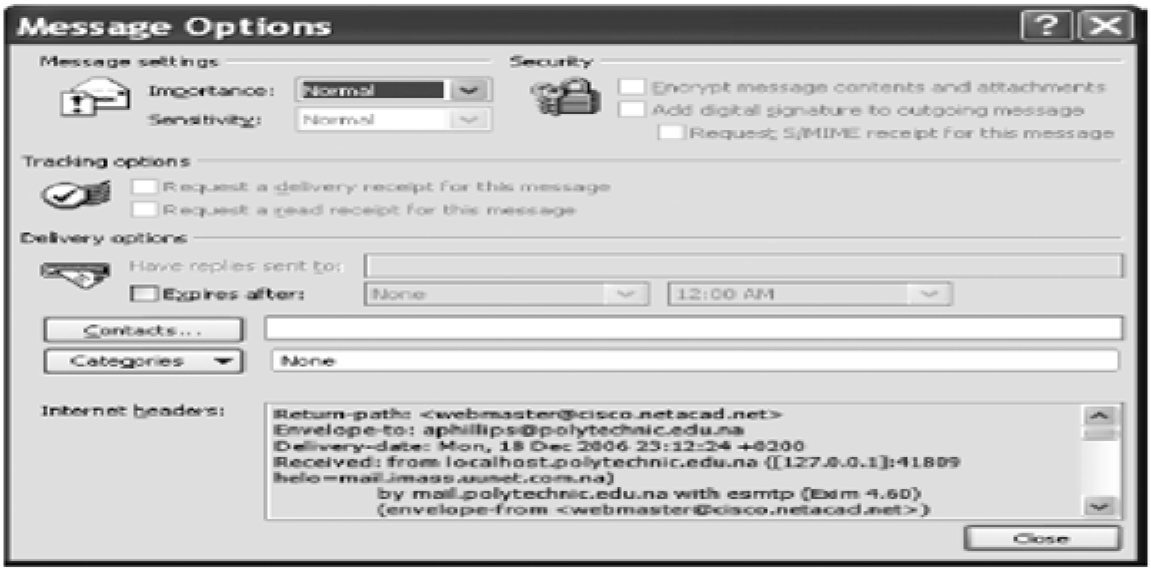
Examining E-mail Messages

- Access victim's computer 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
- Sometimes you will deal with deleted e-mails
- 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

- Learn how to find e-mail headers
  - GUI clients
  - Command-line 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
- Headers contain useful information
  - Unique identifying numbers, IP address of sending server, and sending time
- Outlook
  - Open the Message Options dialog box
  - Copy headers
  - Paste them to any text editor
- Outlook Express
  - Open the message Properties dialog box
  - Select Message Source
  - Copy and paste the headers to any text editor



Importance: Normal

Sensitivity: Normal

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Have replies sent to:

□ Expires after: None 12:00 AM

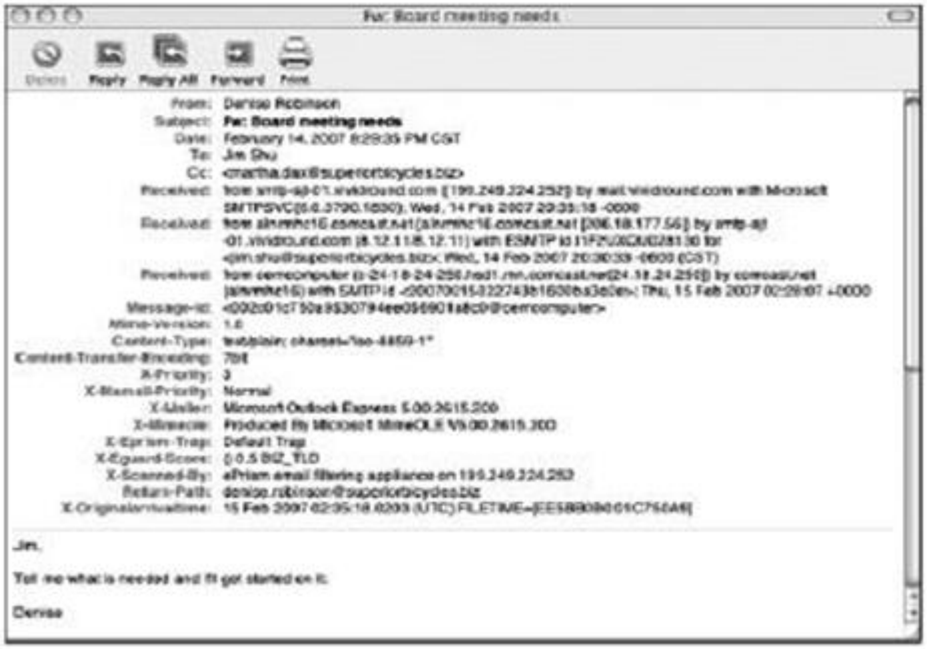
Categories: None

Internet headers:

```
Return-path: <webmaster@cisco.netacad.net>
Envelope-to: aphillips@polytechnic.edu.na
Delivery-date: Mon, 18 Dec 2006 23:12:24 +0200
Received: from localhost.polytechnic.edu.na ([127.0.0.1]:41809
helo=mail.imass.uunet.com.na)
          by mail.polytechnic.edu.na with esmtp (Exim 4.60)
          (envelope-from <webmaster@cisco.netacad.net>)
```

Fig: An Outlook e-mail header

- Novell Evolution
  - Click View, All Message Headers
  - Copy and paste the e-mail header
- Pine and ELM
  - Check enable-full-headers
- AOL headers
  - Click Action, View Message Source
  - Copy and paste headers
- Hotmail
  - Click Options, and then click the Mail Display Settings
  - Click the Advanced option button under Message Headers
  - Copy and paste headers
- Apple Mail
  - Click View from the menu, point to Message, and then click Long Header – Copy and paste headers



```
                 From: Denise Robinson
              Subject: Fw: Board meeting needs
                 Date: February 14, 2007 8:29:35 PM CST
                   To: Jim Shu
                   Cc: <martha.dax@superiorbicycles.biz>
             Received: from smtp-a[l-01.vividround.com ([199.249.224.252]) by mail.vividround.com with Microsoft
                       SMTPSVC(6.0.3790.1830); Wed, 14 Feb 2007 20:35:18 -0000
             Received: from slnmhc16.comcast.net(slnmhc16.comcast.net [206.18.177.56]) by smtp-al
                       -01.vividround.com (8.12.11/8.12.11) with ESMTP id 11F2U0QU028130 for
                       <jim.shu@superiorbicycles.biz>; Wed, 14 Feb 2007 20:30:33 -0600 (CST)
             Received: from cemcomputer (c-24-18-24-256.hsd1.mn.comcast.net[24.18.24.256]) by comcast.net
                       (slnmhc16) with SMTP id <20070215222743b1630a3e0e>; Thu, 15 Feb 2007 02:28:07 +0000
           Message-id: <002d01c750a9530794ee05690 1a6c0@cemcomputer>
         Mime-Version: 1.0
         Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
           X-Priority: 3
    X-Msmail-Priority: Normal
             X-Mailer: Microsoft Outlook Express 5.00.2615.200
          X-Mimeole: Produced By Microsoft MimeOLE V5.00.2615.200
          X-Eprism-Trap: Default Trap
        X-Eguard-Score: () 0.5 BIZ_TLD
         X-Scanned-By: ePrism email filtering appliance on 199.249.224.253
          Return-Path: denise.robinson@superiorbicycles.biz
X-Originalarrivaltime: 15 Feb 2007 02:35:18.0203 (UTC) FILETIME=[EE5B8080:01C750A6]
```

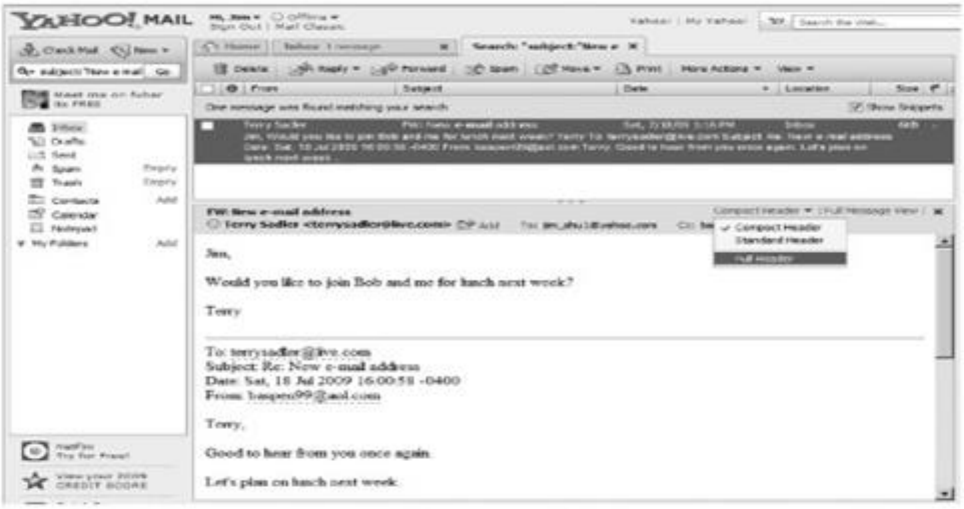
Jim,

Tell me what is needed and I'll get started on it.

Denise

Fig: An Apple mail e-mail header

- Yahoo
  - Click Mail Options
  - Click General Preferences and Show All headers on incoming messages
  - Copy and paste headers



One message was found matching your search

FW: New e-mail address
Terry Sadler <terrysadler@live.com>
To: jim_shu1@yahoo.com

Jim,

Would you like to join Bob and me for lunch next week?

Terry

To: terrysadler@live.com
Subject: Re: New e-mail address
Date: Sat, 18 Jul 2009 16:00:58 -0400
From: baspen99@aol.com

Terry,

Good to hear from you once again.

Let's plan on lunch next week.

Fig: Selecting the option to view headers in Yahoo!

Examining E-mail Headers

- Gather supporting evidence and track suspect
  - Return path
  - Recipient’s e-mail address
  - Type of sending e-mail service
  - IP address of sending server
  - Name of the e-mail server
  - Unique message number
  - Date and time e-mail was sent
  - Attachment files information

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
- 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

- Contact the administrator responsible for the sending server

Finding domain name’s point of contact

- www.arin.net
- www.internic.com
- www.freeality.com
- www.google.com

- Find suspect’s contact information
- 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

Understanding E-mail Servers

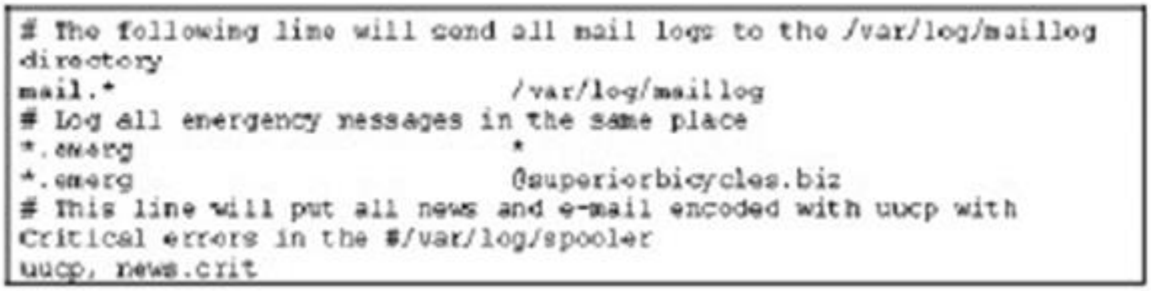
- Computer loaded with software that uses e-mail protocols for its services
  - And maintains logs you can examine and use in your investigation
- E-mail storage
  - Database
  - Flat file
- Logs
  - Default or manual
  - Continuous and circular
- Log information
  - E-mail content
  - Sending IP address
  - Receiving and reading date and time
  - 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

/etc/sendmail.cf

– Configuration information for Sendmail

- /etc/syslog.conf
  - Specifies how and which events Sendmail logs
- /var/log/maillog
  - SMTP and POP3 communications
- IP address and time stamp
- Check UNIX man pages for more information



```
# The following line will send all mail logs to the /var/log/maillog
directory
mail.*                          /var/log/maillog
# Log all emergency messages in the same place
*.emerg                         *
*.emerg                         @superiorbicycles.biz
# This line will put all news and e-mail encoded with uucp with
Critical errors in the #/var/log/spooler
uucp, news.crit
```

Fig: A typical syslog.conf file

Examining Microsoft E-mail Server Logs

- Microsoft Exchange Server (Exchange)
  - Uses a database
  - Based on Microsoft Extensible Storage Engine
- Information Store files
  - Database files *.edb
- Responsible for MAPI information
  - Database files *.stm
- Responsible for non-MAPI information
- Transaction logs

  – Keep track of e-mail databases
- Checkpoints

  - Keep track of transaction logs
- Temporary files
- E-mail communication logs
  - res#.log
- Tracking.log

  --Tracks messages

  Troubleshooting or diagnostic log

  - Logs events
  - Use Windows Event Viewer
  - Open the Event Properties dialog box for more details about an event

Examining Novell GroupWise E-mail Logs

- Up to 25 databases for e-mail users
  - Stored on the Ofuser directory object
  - Referenced by a username, an unique identifier, and .db extension
- Shares resources with e-mail server databases
- Mailboxes organizations
  - Permanent index files
  - QuickFinder
- Folder and file structure can be complex
  - It uses Novell directory structure
- Guardian
  - Directory of every database
  - Tracks changes in the GroupWise environment
  - Considered a single point of failure
- Log files
  - GroupWise generates log files (.log extension) maintained in a standard log format in GroupWise folders

Using Specialized E-mail Forensics Tools

- Tools include:
  - AccessData's Forensic Toolkit (FTK)
  - ProDiscover Basic
  - FINALeMAIL
  - Sawmill-GroupWise
  - DBXtract
  - Fookes Aid4Mail and MailBag Assistant
  - Paraben E-Mail Examiner
  - Ontrack Easy Recovery EmailRepair
  - R-Tools R-Mail
- Tools allow you to find:
  - E-mail database files
  - Personal e-mail files
  - Offline storage files
  - Log files
- Advantage
  - Do not need to know how e-mail servers and clients work
- FINALeMAIL
  - Scans e-mail database files
  - Recovers deleted e-mails
  - Searches computer for other files associated with e-mail using AccessData FTK to Recover E-mail
- FTK
  - Can index data on a disk image or an entire drive for faster data retrieval
  - Filters and finds files specific to e-mail clients and servers
- To recover e-mail from Outlook and Outlook Express – AccessData integrated dtSearch

- dtSearch builds a b-tree index of all text data in a drive, an image file, or a group of files

Using a Hexadecimal 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