

Guide to Computer Forensics and Investigations Fourth Edition

Chapter 12 E-mail 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
- Describe some available e-mail computer forensics tools

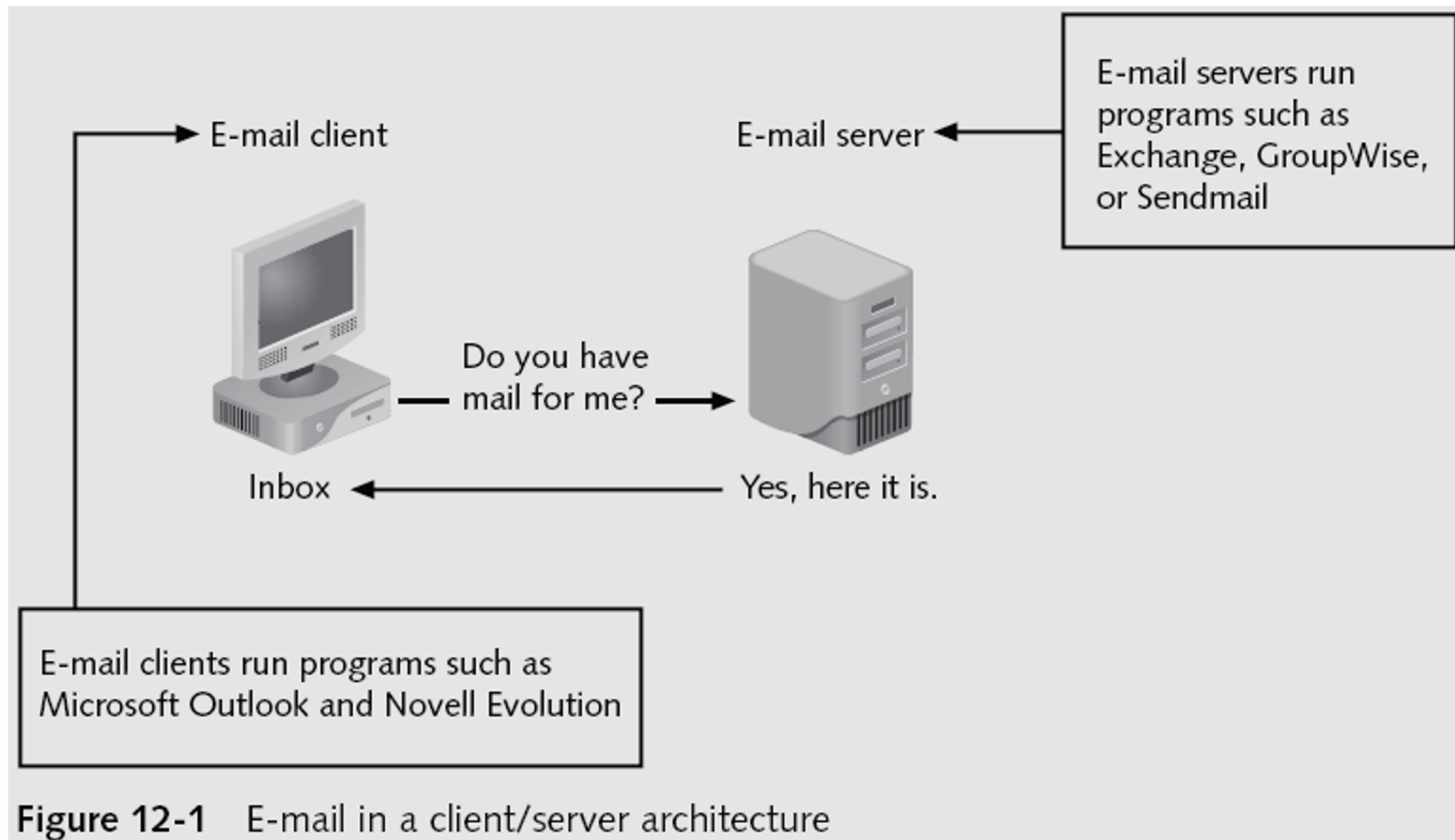
Exploring the Role of E-mail in Investigations

- 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

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



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

- 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

Investigating E-mail Crimes and Violations (continued)

- 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

Examining E-mail Messages (continued)

- 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

Examining E-mail Messages (continued)

Messages in the selected folder are displayed here

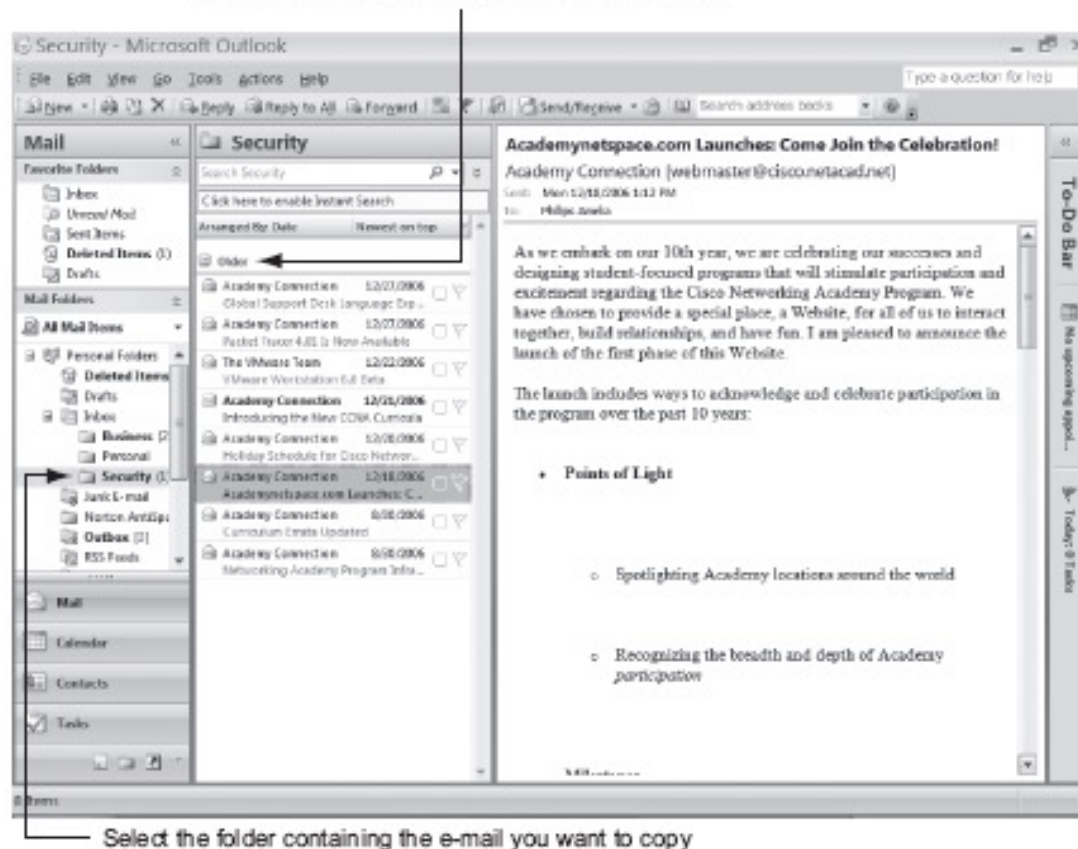


Figure 12-2 Selecting an e-mail to copy

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

Viewing E-mail Headers (continued)

- 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

Viewing E-mail Headers (continued)

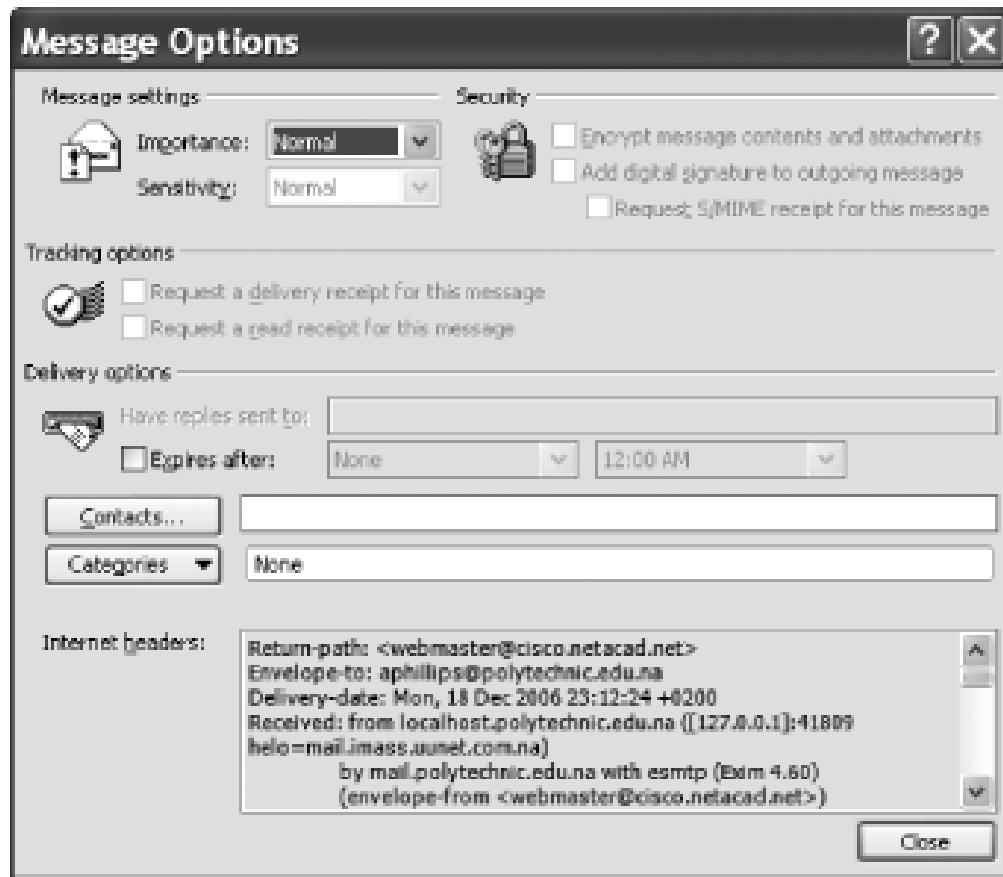


Figure 12-3 An Outlook e-mail header

Viewing E-mail Headers (continued)

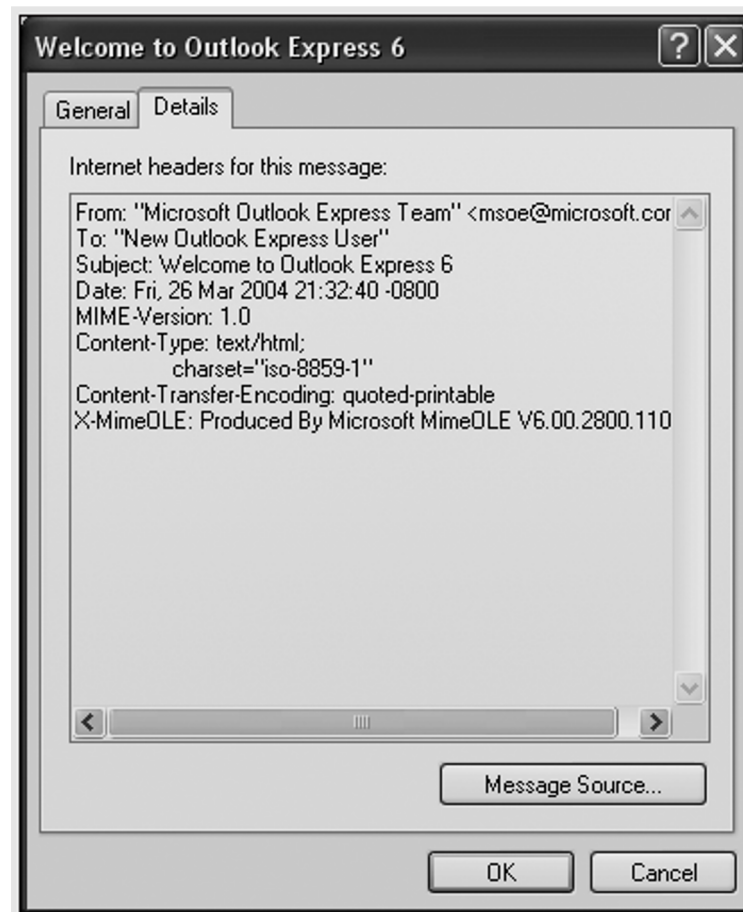


Figure 12-4 An Outlook Express e-mail header



```
Message Source

From: "Microsoft Outlook Express Team" <msoe@microsoft.com>
To: "New Outlook Express User"
Subject: Welcome to Outlook Express 6
Date: Fri, 26 Mar 2004 21:32:40 -0800
MIME-Version: 1.0
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106

<HTML>
<HEAD>
<META HTTP-EQUIV=3D"Content-Type" CONTENT=3D"text/html; =
charset=3Dwindows-1252">
<STYLE>
font{font-family:"Verdana";font-size:8pt;color:#000000}
A:hover.defaultA(color:#999900)
A:hover.bodyTopLine(color:#0000FF)
A:hover (color:#0033FF)
A:visited {color:#888888}
A(color:#0099FF)
.sectionHead(font-weight:bold)
.sectionNotify(color:#0099FF;; text-decoration: underline; -
font-size:8pt)
.headerCell(background-color:#CCCCC; width:140px; height:18px)
.featuresText(font-family:Verdana;font-size:8pt;color:#000000)
.headerCellLine(background-color:#CCCCC; width:246px; height:1px)
.messagesCell(font-family:"Verdana";font-size:8pt;color:#000000)
.defaultA(color:#000000; cursor:hand)
.blackBar(font-family:"Verdana";font-size:8pt;color:#FFFFFF;font-weight:b=
old)
.bottomText(font-family: Verdana; font-size:7pt; color: #AAAAAA)
.headerLinks(font-family:"Verdana";font-size:8pt;color:#000000)
.signatureText(font-family:"Verdana";font-size:8pt;font-weight:bold;color=
:#000000)
A:hover.toggleStyle(color:#FFFFFF)
A:visited.toggleStyle(color:#CCCCC)
```

Figure 12-5 Viewing the message's HTML source code

Viewing E-mail Headers (continued)

- 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

Viewing E-mail Headers (continued)

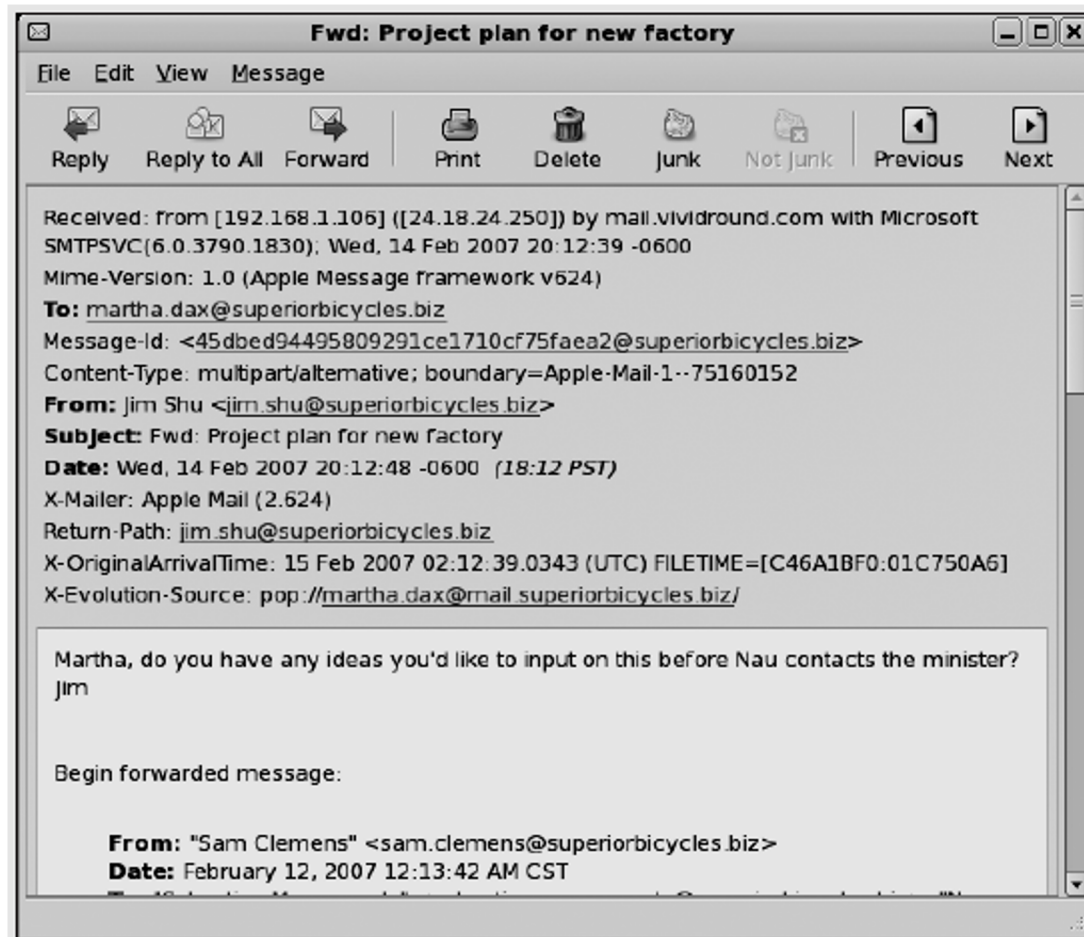
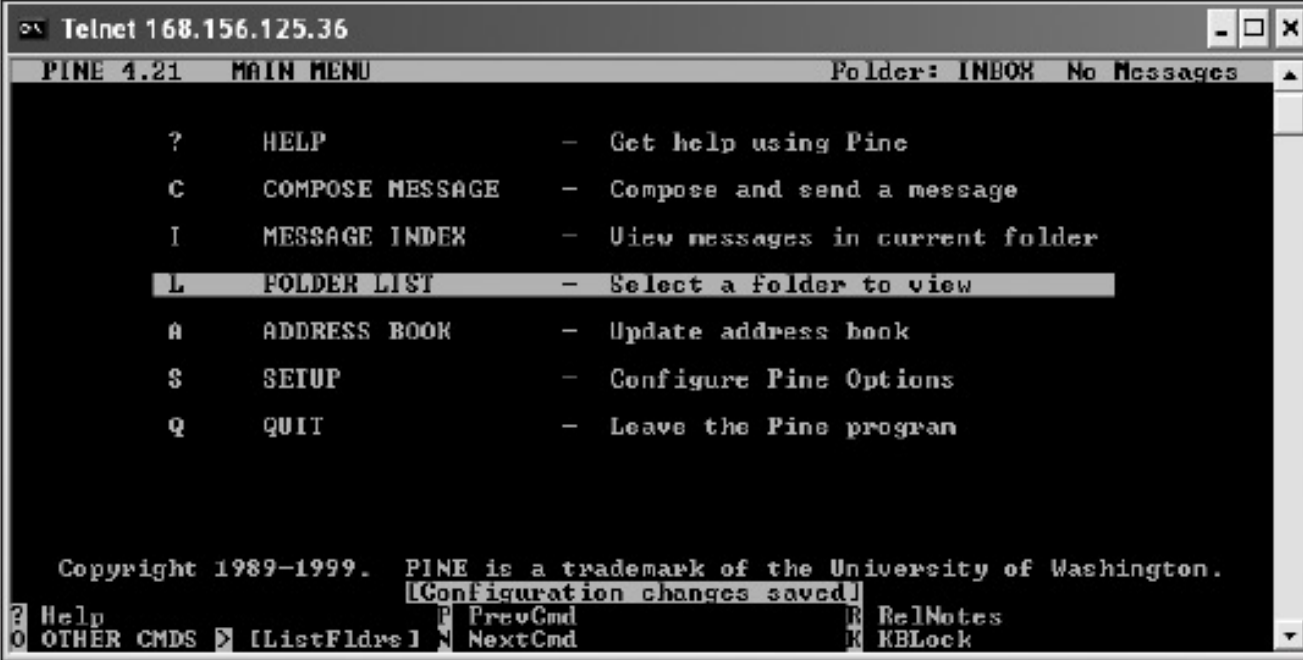


Figure 12-6 An Evolution e-mail header

Viewing E-mail Headers (continued)



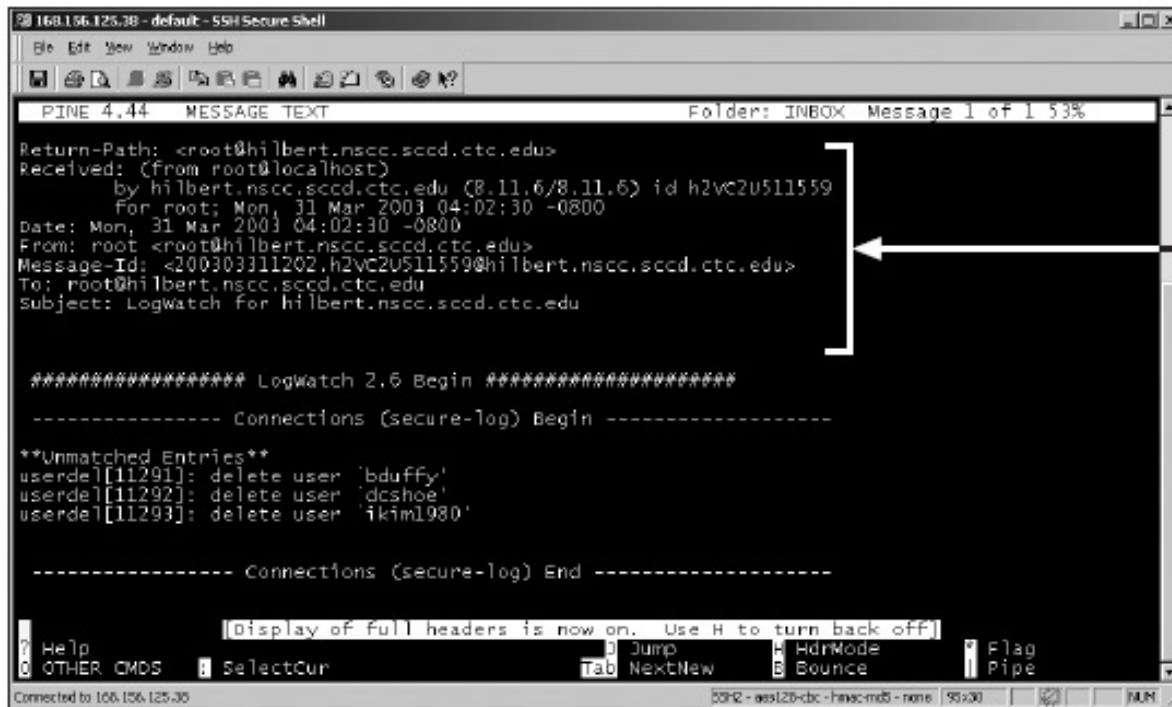
The screenshot shows a Telnet window titled "Telnet 168.156.125.36". Inside the window, the Pine 4.21 main menu is displayed. The menu is titled "PINE 4.21 MAIN MENU" and "Folder: INBOX No Messages". The menu items are listed as follows:

- ? HELP - Get help using Pine
- C COMPOSE MESSAGE - Compose and send a message
- I MESSAGE INDEX - View messages in current folder
- L FOLDER LIST - Select a folder to view**
- A ADDRESS BOOK - Update address book
- S SETUP - Configure Pine Options
- Q QUIT - Leave the Pine program

At the bottom of the menu, there is a copyright notice: "Copyright 1989-1999. PINE is a trademark of the University of Washington." Below this, there is a status bar with the following text: "[Configuration changes saved]". At the very bottom, there is a row of keyboard shortcuts: "? Help", "O OTHER CMDS", "P PrevCmd", "N NextCmd", "R RelNotes", and "K KBlock".

Figure 12-7 E-mail options in Pine

Viewing E-mail Headers (continued)



```
PINE 4.44 MESSAGE TEXT Folder: INBOX Message 1 of 1 53%

Return-Path: <root@hilbert.nscd.ctc.edu>
Received: (from root@localhost)
  by hilbert.nscd.ctc.edu (8.11.6/8.11.6) id h2vc2v511559
  For root; Mon, 31 Mar 2003 04:02:30 -0800
Date: Mon, 31 Mar 2003 04:02:30 -0800
From: root <root@hilbert.nscd.ctc.edu>
Message-Id: <200303311202.h2vc2v511559@hilbert.nscd.ctc.edu>
To: root@hilbert.nscd.ctc.edu
Subject: Logwatch for hilbert.nscd.ctc.edu

***** Logwatch 2.6 Begin *****

----- Connections (secure-log) Begin -----

**Unmatched Entries**
userdel[11291]: delete user 'bduffy'
userdel[11292]: delete user 'dcshoe'
userdel[11293]: delete user 'ikim1980'

----- Connections (secure-log) End -----

[Display of full headers is now on. Use H to turn back off.]

Help      Jump      HdrMode   Flag
OTHER CMDS SelectCur Tab NextNew B Bounce   Pipe

Connected to 168.156.125.38      SSH2 - aes128-ctc - hmac-md5 - none | 90x30 | RUN
```

Message header

Figure 12-8 An e-mail header in Pine

Viewing E-mail Headers (continued)

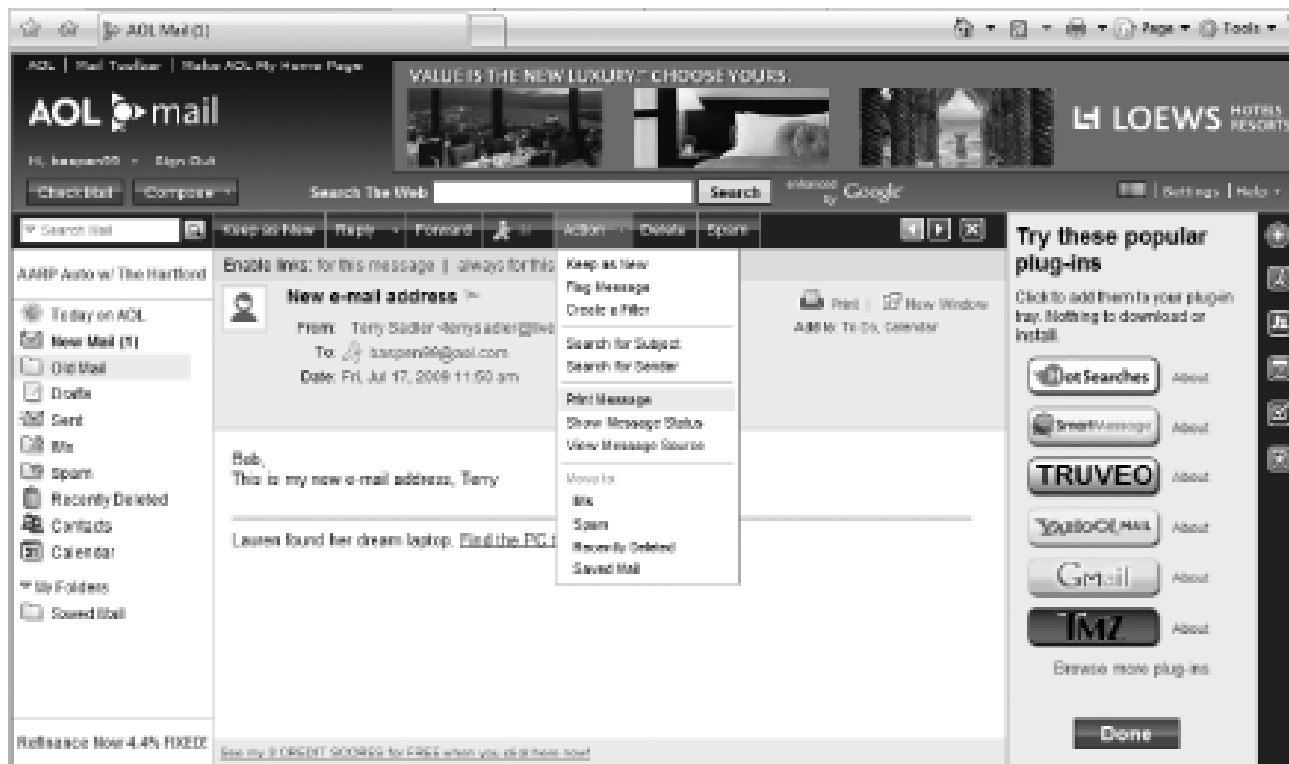


Figure 12-9 Printing an e-mail in AOL

Viewing E-mail Headers (continued)

- 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

Viewing E-mail Headers (continued)

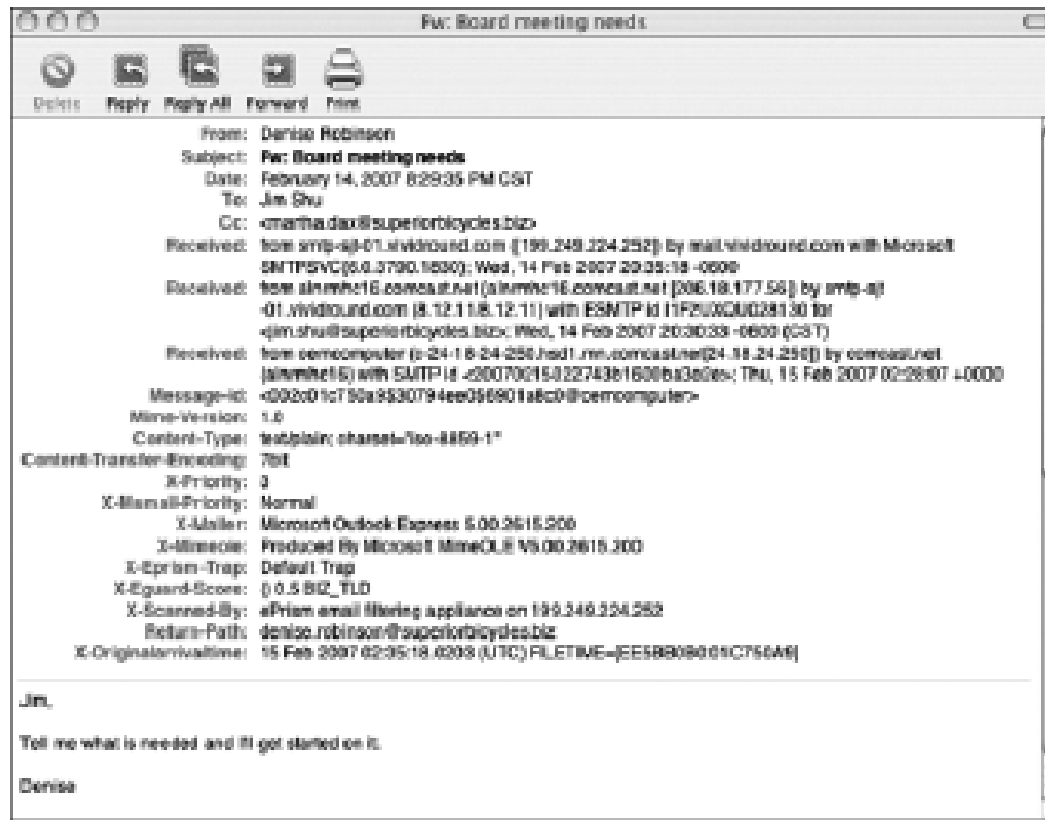


Figure 12-10 An Apple Mail e-mail header

Viewing E-mail Headers (continued)

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

Viewing E-mail Headers (continued)

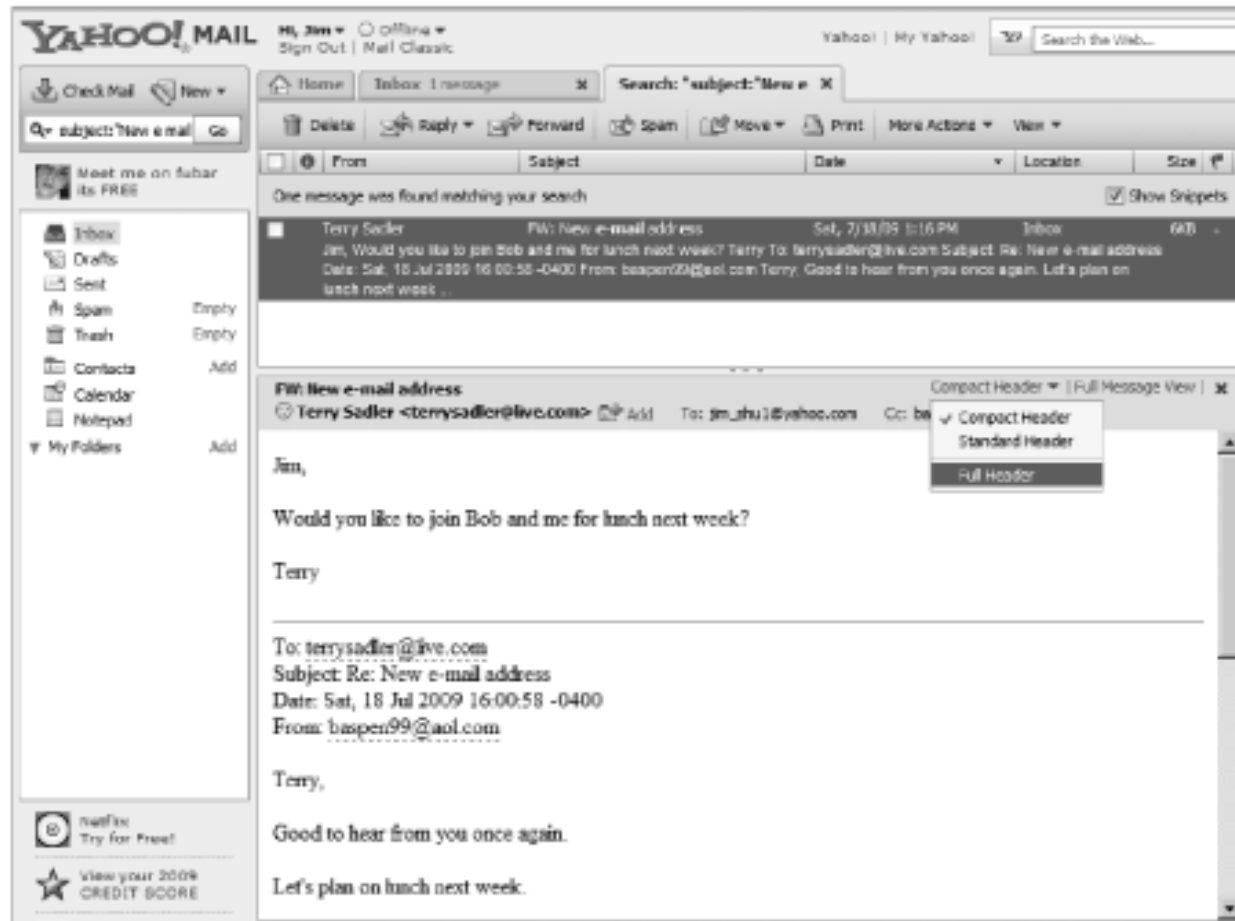


Figure 12-11 Selecting the option to view headers in Yahoo!

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 E-mail Headers (continued)

```
1. Return-Path: <Samspede@myway.com>
2. Delivered To: jim.shu@superiorbicycles.biz
3. Received (qmail 12780 invoked by uid 0): 12 Dec 2010 08:23:37 -
   0000
4. Received from unknown (HELO smtp.superiorbicycles.biz)
   (192.152.64.20) by mail.superiorbicycles.biz with SMTP; 12 Dec
   2010 08:23:37 -0000
5. Received: from Web4009 mail0.myway.com
   (Web4009.mail0.myway.com[192.218.78.27])
   by smtp.superiorbicycles.biz (16.12.6/16.12.6) with SMTP id
   q8C8ILAJ005229
   for <jim.shu@superiorbicycles.biz>; Sun 12 Dec 2010
   00:18:21 -0800
6. Message-ID: <20101212082330.40429.qmail@web4009.mail0.myway.com>
7. Received: from [10.187.241.199] by Web4009.mail0.myway.com via
   HTTP; Sun 12 Dec 2010 00:23:30 PST

Date: Sun 12 Dec 2010 00:23:30 PST |
XIME-Version: 1.0
```

Figure 12-12 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
- 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

Using Network E-mail Logs (continued)

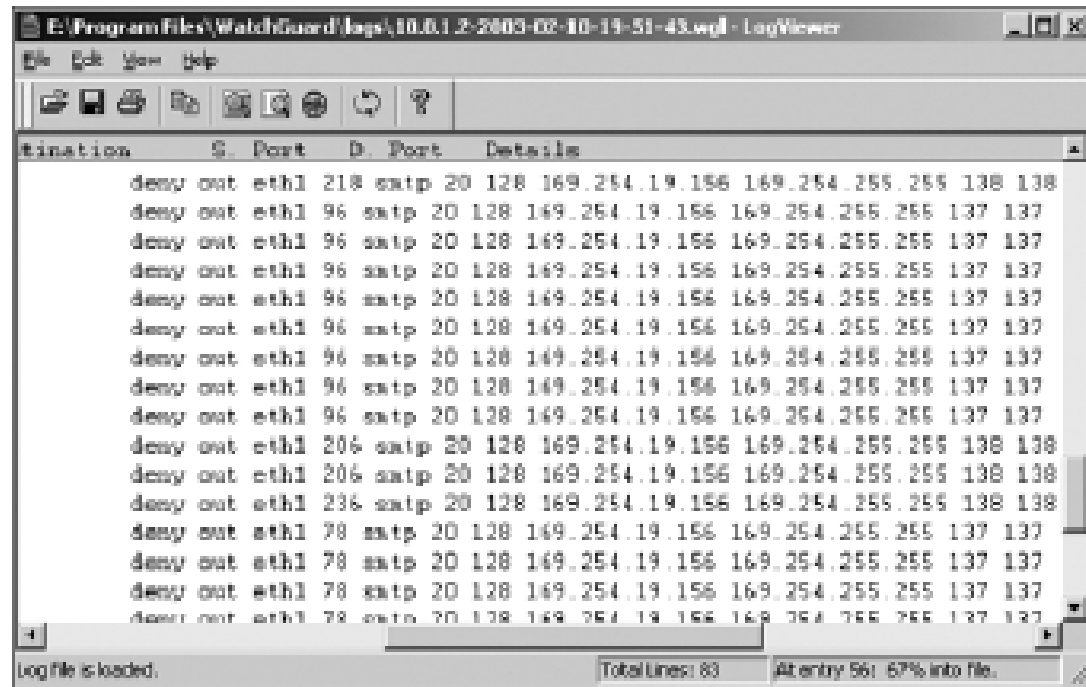


Figure 12-13 A firewall log

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

Understanding E-mail Servers (continued)

- 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

Understanding E-mail Servers (continued)

```
Administrator@superiorbicycles.biz -2010-10-16 09:44:22 GMT
10.0.1.205 pegasus.superiorbicycles.biz PEGASUS 10.0.1.205

Jim.s.hu@superiorbicycles.biz 1019
5.2.0.9.0.20101016072308.00w543|44@pegasus.superiorbicycles.biz 0 0
407 1 2010-10-16 09:44:22 GMT
```

Figure 12-14 An e-mail server log file

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

Examining UNIX E-mail Server Logs (continued)

```
# 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 uuwp with
critical errors in the #/var/log/spooler
uuwp, news.crit
```

Figure 12-15 A typical syslog.conf file

Examining UNIX E-mail Server Logs (continued)

```
May 21 10:10:32 poser sendmail[5365]: NOQUEUE: "wir" command from  
[10.0.1.1] (10.0.1.1)  
May 21 10:10:32 poser sendmail[5365]: NOQUEUE: "debug" command from  
[10.0.1.1] (10.0.1.1)
```

Figure 12-16 A maillog file with SMTP information

```
May 21 10:12:44 poser `pop3d[5373]: port 110 service init from 10.0.1.1  
May 21 10:12:44 poser `pop3d[5373]: Login failure user=rich  
host=[10.0.1.1]
```

Figure 12-17 A maillog file with POP3 information

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

Examining Microsoft E-mail Server Logs (continued)

- 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

Examining Microsoft E-mail Server Logs (continued)



The screenshot shows a Notepad window titled "20021216.log - Notepad". The menu bar includes "File", "Edit", "Format", and "Help". The text content is a message tracking log file with the following fields: # Message Tracking Log File, # Exchange System Attendant Version, # Date, Time, Client-IP, Client-hostname, Partner-Name, Server-hostname, Server-IP, Recipient-Address, Event-ID, MSGID, Priority, Recipient-Report-Status, Total-bytes, Number-recipients, Origination-time, Encryption, Service-version, Linked-MSGID, Message-Subject, Sender-Address, and a series of dashes. The log entries include details for a message sent from PEGASUS to a recipient at mycompany.com, with a subject line "One for the books".

```
# Message Tracking Log File# Exchange System Attendant Version
# 6.0.4417.00# Date      Time      Client-IP      Client-hostname
Partner-Name      Server-hostname  Server-IP      Recipient-Address
Event-ID          MSGID          Priority      Recipient-Report-Status
Total-bytes      Number-recipients  Origination-time
Encryption      Service-version  Linked-MSGID      Message-Subject
Sender-Address0002005-12-16 17:8:30 GMT - - -
PEGASUS - /O=ZOIKES/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=Janedoe 1027
11A0DC98C6BC774BA0B32AE932D5B3E02E49@pegasus.mycompany.com 0
0 1320 1 2005-12-16 17:8:30 GMT 0 -
c-us;a= ;p=ZOIKES;l=PEGASUS-0212161708282-1 one for the books
EX:/O=ZOIKES/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=ADMINISTRATOR -002005-12-16 17:8:31 GMT
- - - PEGASUS - /O=ZOIKES/OU=FIRST
ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=Janedoe 1019
11A0DC98C6BC774BA0B32AE932D5B3E02E49@pegasus.mycompany.com 0
0 1320 1 2005-12-16 17:8:30 GMT 0 -
One for the books - -002005-12-16 17:8:31 GMT -
- - PEGASUS - /O=ZOIKES/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=Janedoe 1025
11A0DC98C6BC774BA0B32AE932D5B3E02E49@pegasus.mycompany.com 0
0 1320 1 2005-12-16 17:8:30 GMT 0 -
One for the books - -002005-12-16 17:8:31 GMT -
- - PEGASUS - /O=ZOIKES/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=Janedoe 1024
11A0DC98C6BC774BA0B32AE932D5B3E02E49@pegasus.mycompany.com 0
```

Figure 12-18 A message tracking log in verbose mode

Examining Microsoft E-mail Server Logs (continued)

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

Examining Microsoft E-mail Server Logs (continued)

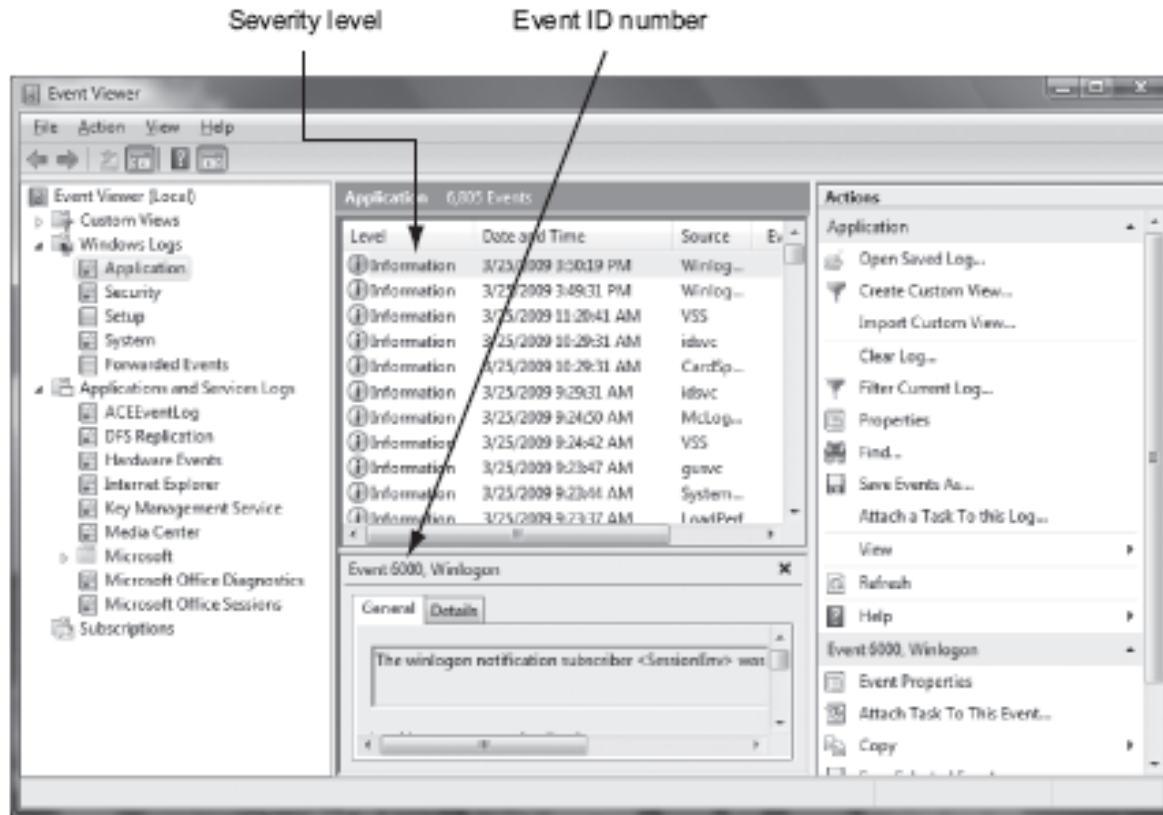


Figure 12-19 Viewing a log in Event Viewer

Examining Microsoft E-mail Server Logs (continued)

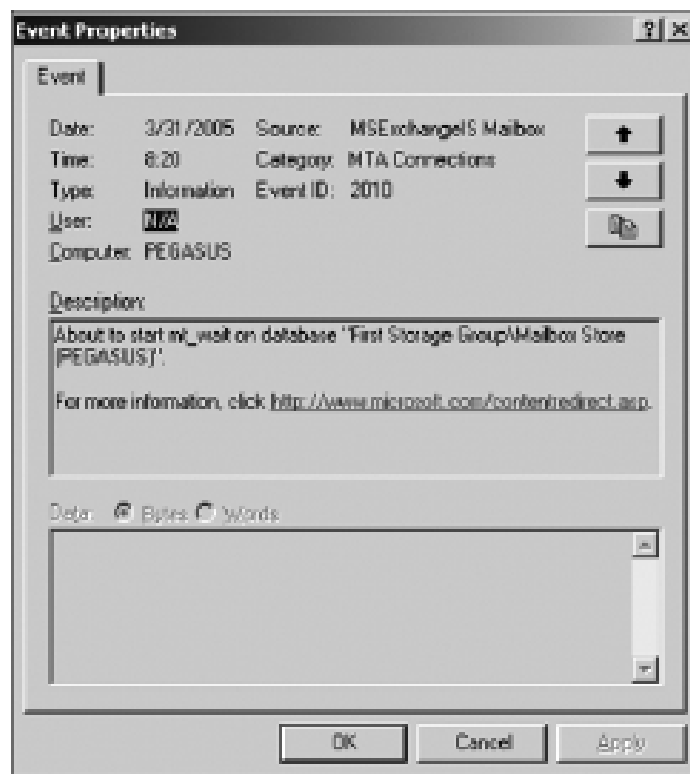


Figure 12-20 The Event Properties dialog box

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

Examining Novell GroupWise E-mail Logs (continued)

- 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

Using Specialized E-mail Forensics Tools (continued)

- 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

Using Specialized E-mail Forensics Tools (continued)

- FINALeMAIL
 - Scans e-mail database files
 - Recovers deleted e-mails
 - Searches computer for other files associated with e-mail

Using Specialized E-mail Forensics Tools (continued)

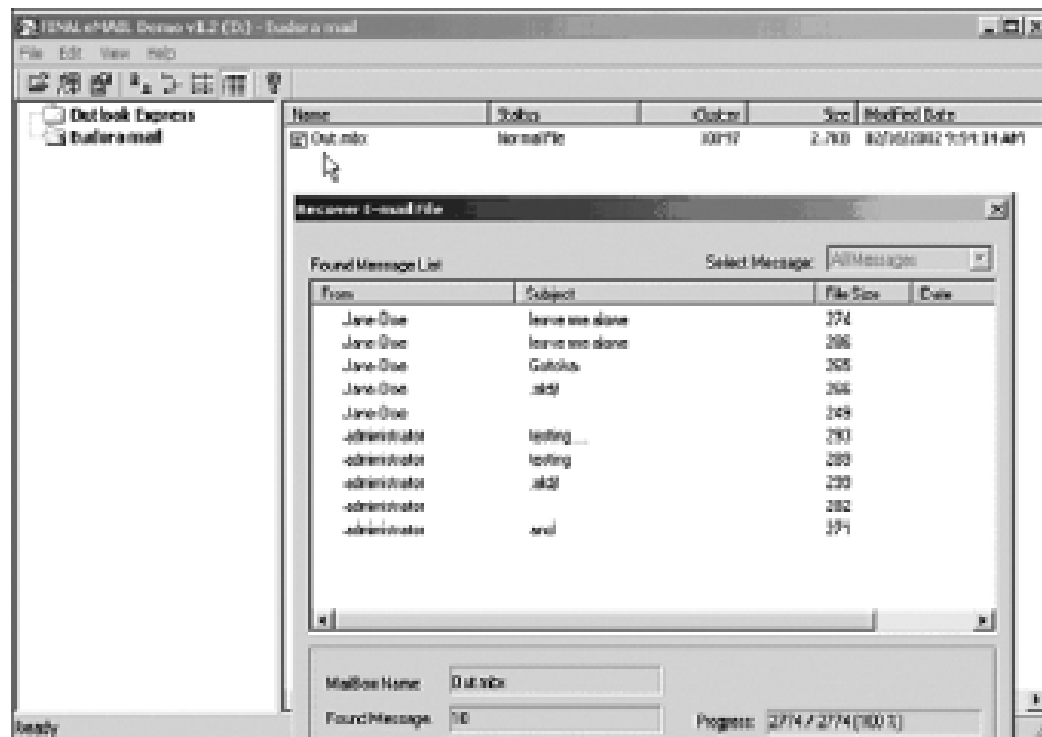


Figure 12-21 E-mail search results in FINALEMAIL

Using Specialized E-mail Forensics Tools (continued)

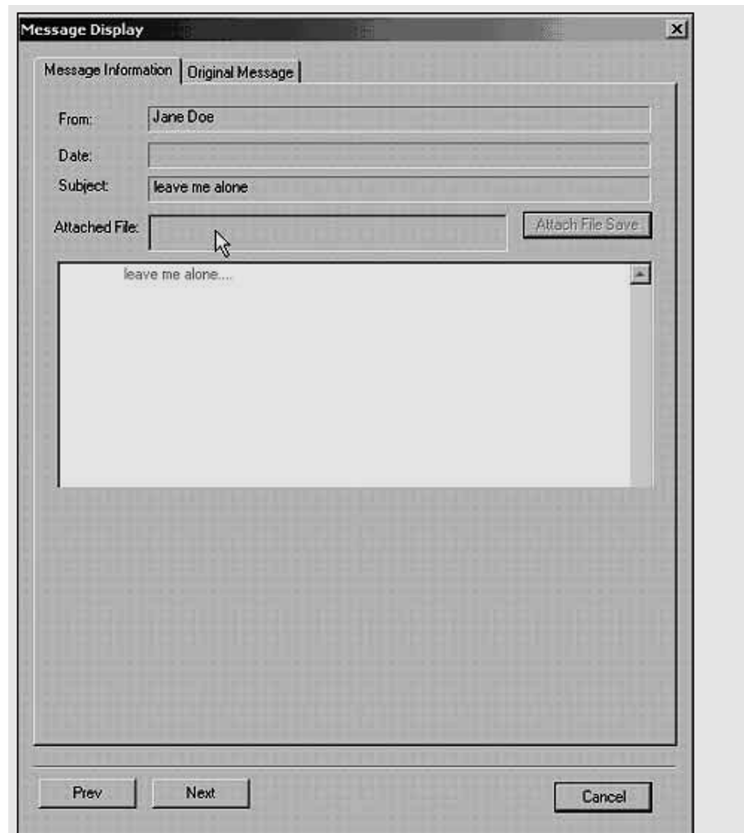


Figure 12-23 Viewing message contents in FINALEMAIL

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 AccessData FTK to Recover E-mail (continued)

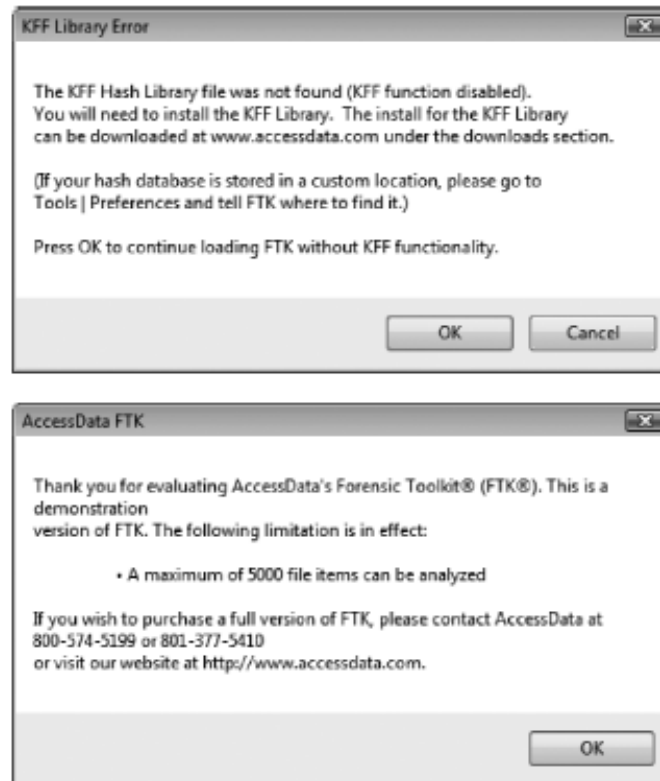


Figure 12-24 KFF warning and AccessData's evaluation notice

Using AccessData FTK to Recover E-mail (continued)

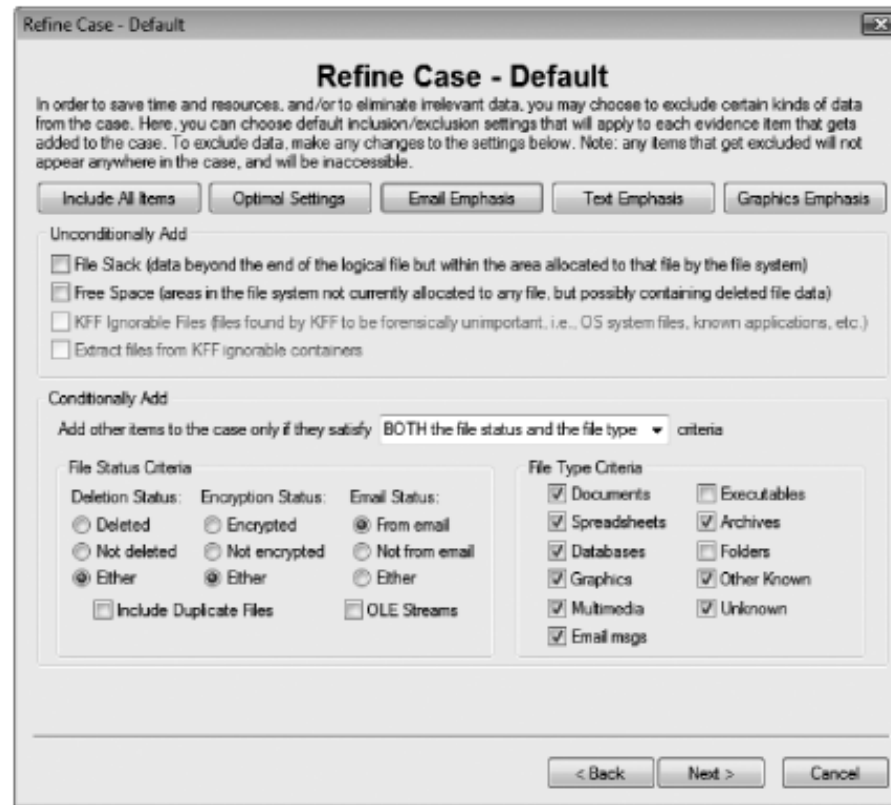


Figure 12-25 The Refine Case - Default dialog box

Using AccessData FTK to Recover E-mail (continued)

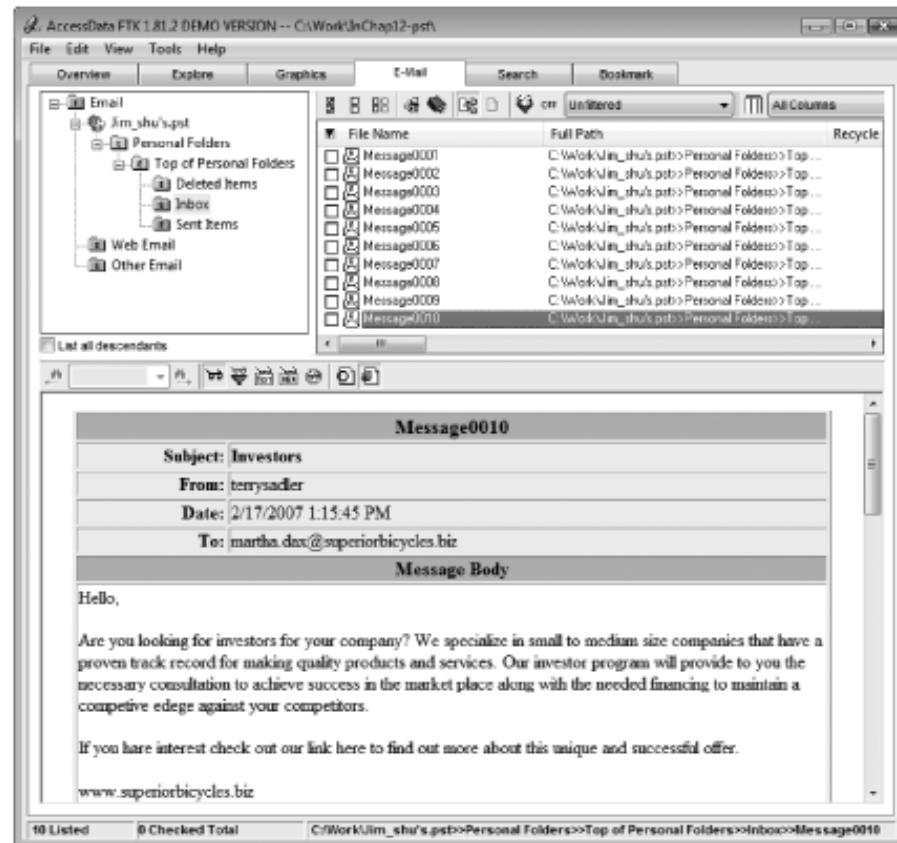
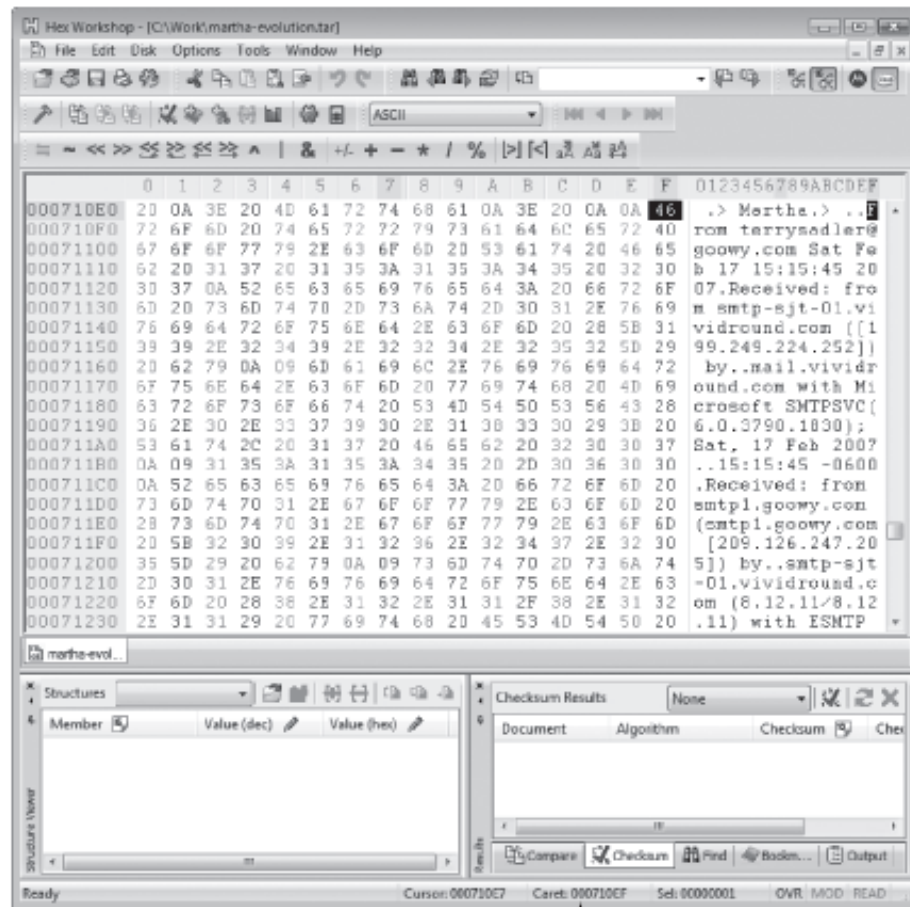


Figure 12-28 The E-Mail tab showing all messages

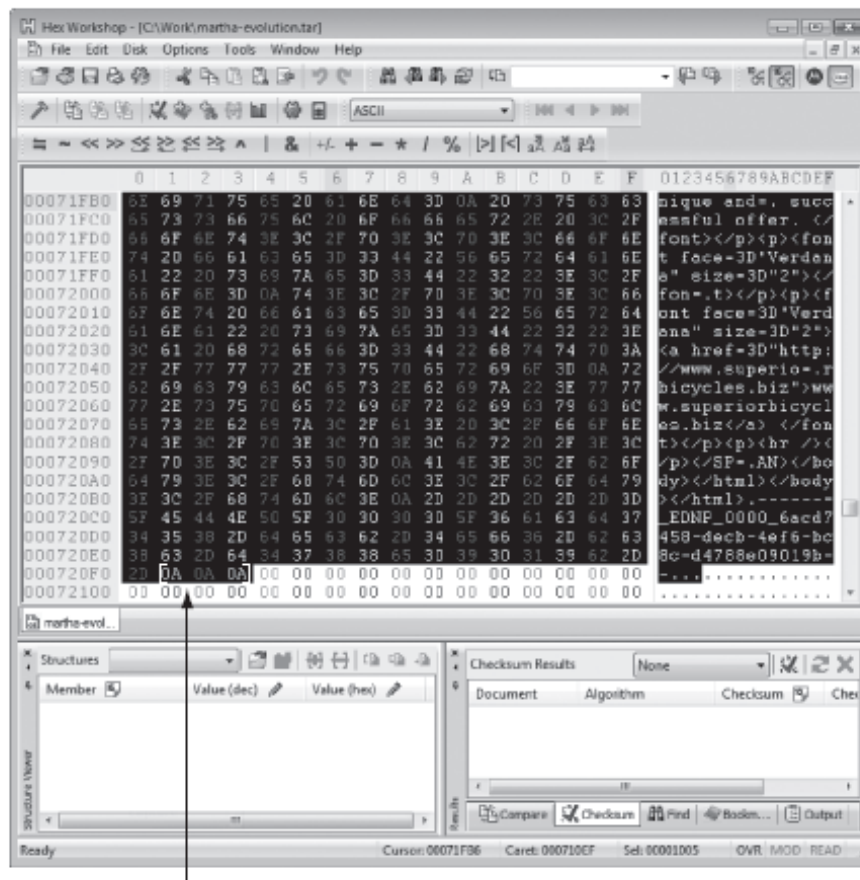
Using a Hexadecimal Editor to Carve E-mail Messages

- 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



Offset byte count from beginning of file

Figure 12-29 Hex Workshop displaying the beginning of the e-mail from Terry Sadler



Ending position for this message

Figure 12-30 Hex Workshop displaying the ending position of the e-mail from Terry Sadler

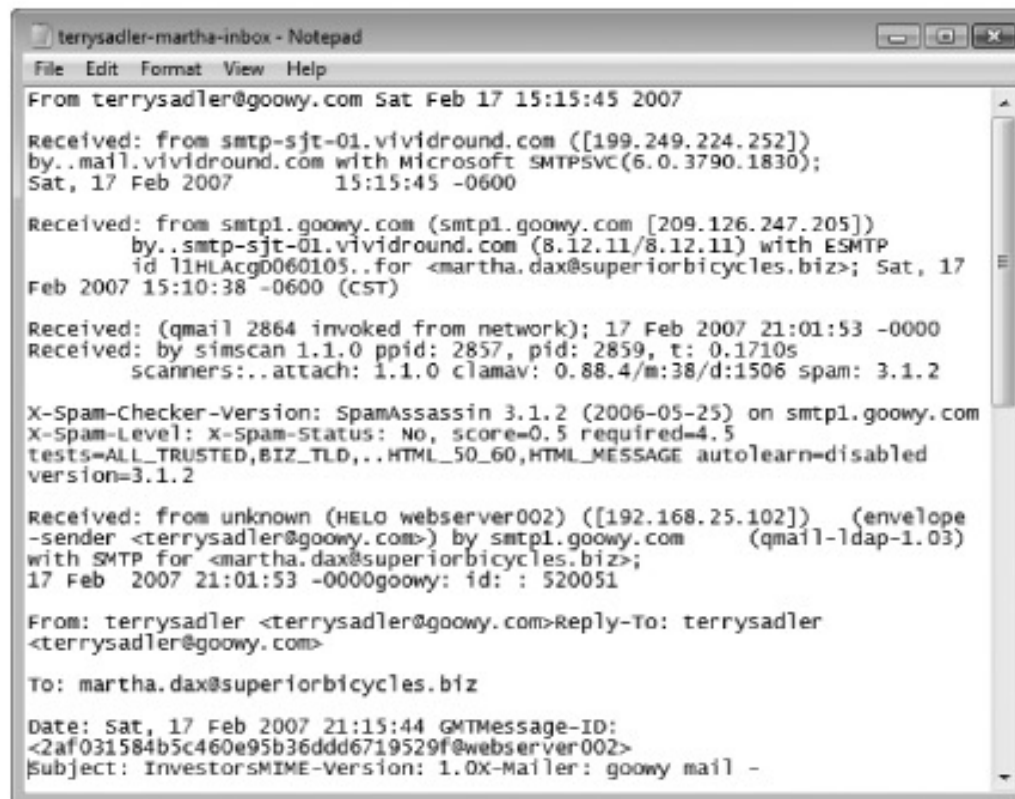
Using a Hexadecimal Editor to Carve E-mail Messages (continued)



```
terrysadler-martha-inbox - Notepad
File Edit Format View Help
From terrysadler@goowy.com Sat Feb 17 15:15:45 2007Received: 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 ESMTD 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=3.1.2Received: 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.biz
Date: 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
```

Figure 12-31 Carved e-mail message in Notepad

Using a Hexadecimal Editor to Carve E-mail Messages (continued)



The screenshot shows a Notepad window titled "terradsler-martha-inbox - Notepad". The text inside is a formatted email message. The header includes the sender "terradsler@goowy.com" and the date "Sat Feb 17 15:15:45 2007". The body contains several "Received:" lines detailing the message's path through various mail servers (smtp-sjt-01.vividround.com, smtp1.goowy.com) and the use of Microsoft SMTPSVC and ESMT. It also includes spam filtering information from X-Spam-Checker-Version: SpamAssassin 3.1.2. The "From:" line is "terradsler <terradsler@goowy.com>". The "To:" line is "martha.dax@superiorbicycles.biz". The "Date:" is "Sat, 17 Feb 2007 21:15:44 GMT". The "Subject:" is "InvestorsMIME-Version: 1.0".

```
terradsler-martha-inbox - Notepad
File Edit Format View Help
From terradsler@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 ESMT
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 -0000
Received: 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: 3.1.2
X-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 <terradsler@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: : 520051
From: terradsler <terradsler@goowy.com>Reply-To: terradsler
<terradsler@goowy.com>
To: martha.dax@superiorbicycles.biz
Date: Sat, 17 Feb 2007 21:15:44 GMTMessage-ID:
<2af031584b5c460e95b36ddd6719529f@webserver002>
Subject: InvestorsMIME-Version: 1.0X-Mailer: goowy mail -
```

Figure 12-32 After formatting the e-mail message in Notepad

Summary

- E-mail fraudsters use phishing and spoofing scam techniques
- Send and receive e-mail via Internet or a LAN
 - Both environments use client/server architecture
- 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
- Find e-mail headers

Summary (continued)

- Investigating e-mail abuse
 - Be familiar with e-mail servers and clients' operations
- Check
 - E-mail message files, headers, and server log files
- Currently, only a few forensics tools can recover deleted Outlook and Outlook Express messages
- For e-mail applications that use the mbox format, a hexadecimal editor can be used to carve messages manually

Summary (continued)

- Advanced tools are available for recovering deleted Outlook files