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

Exploring the Role of E-mail in Investigations

- E-mail evidence has become an important part of many computing 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

Munshani v. Signal Lake Venture Fund

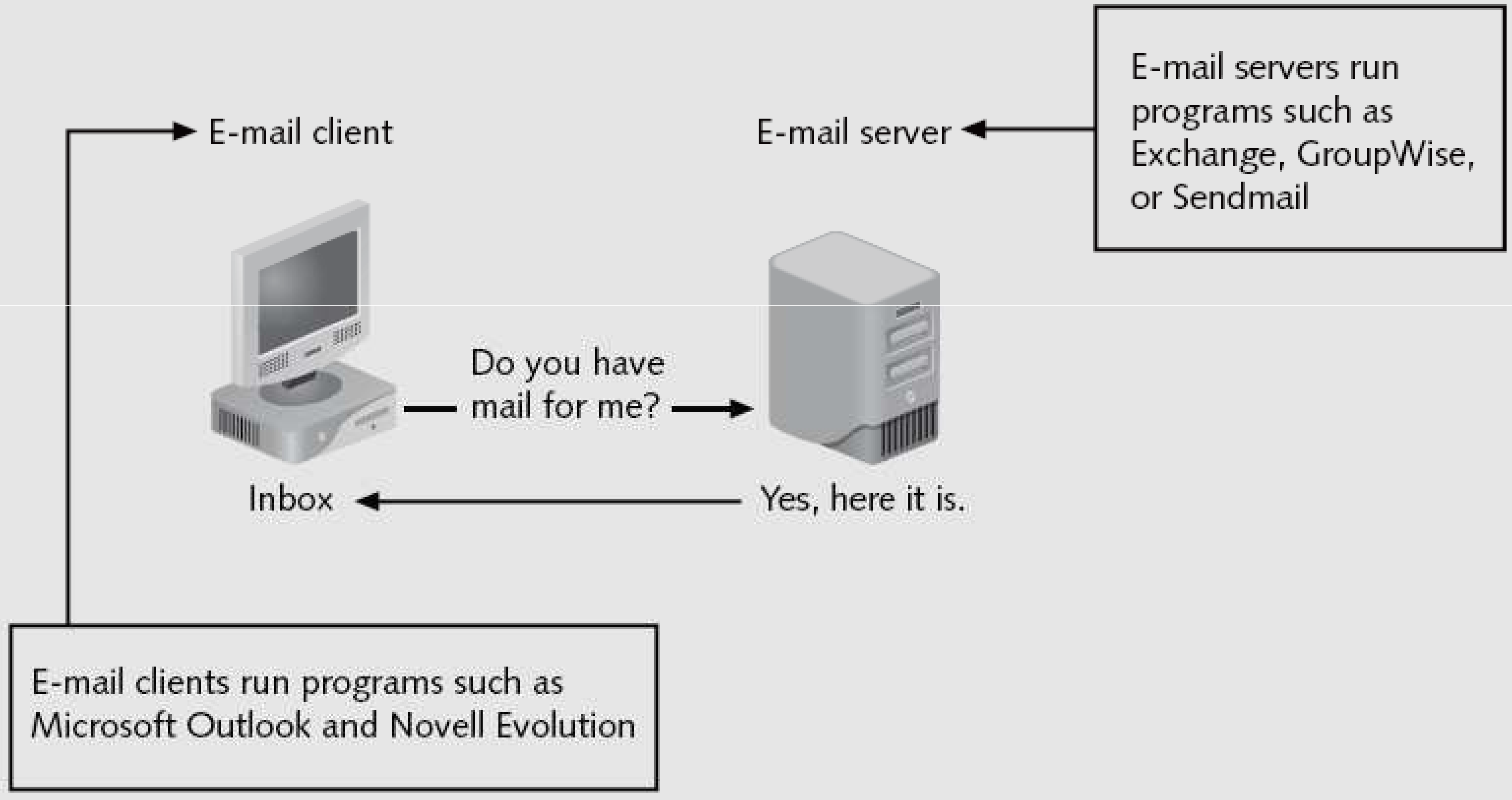
- Munshani received an email and altered it
- But he failed to alter the ESMTP numbers which uniquely identify each message an SMTP server transmits
- Comparing ESMTP numbers from the server and the spoofed email revealed the fraud
  - Link Ch 12a

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

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)



E-mail servers run programs such as Exchange, GroupWise, or Sendmail

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

Figure 12-1 E-mail in a client/server architecture

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

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

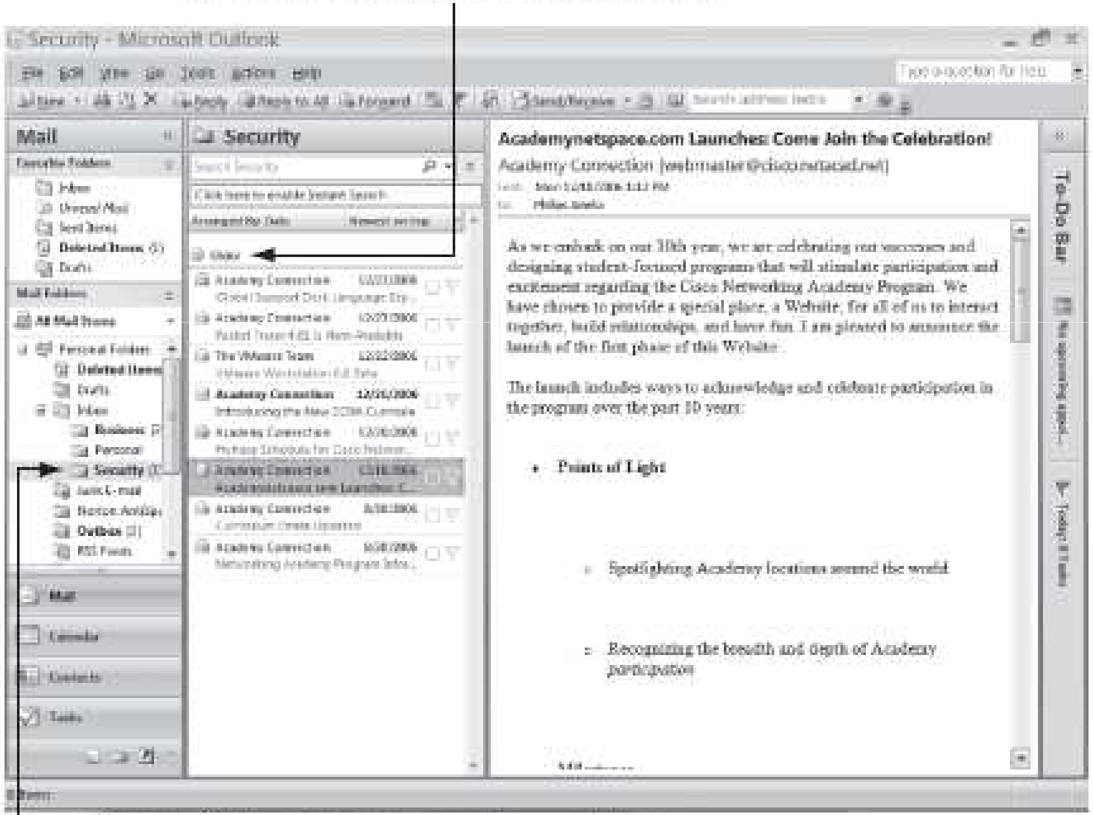
- Access victim’s computer to recover the evidence
- Using the victim’s e-mail client
  - Find and copy evidence in the e-mail
  - Access protected or encrypted material
  - Print e-mails
- Guide victim on the phone
  - Open and copy e-mail including headers
- Sometimes you will deal with deleted e-mails

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



Academynetspace.com Launches: Come Join the Celebration!

Academy Connection [webmaster@cisco.netacad.net]

As we embark on our 10th year, we are celebrating our successes and designing student-focused programs that will stimulate participation and excitement regarding the Cisco Networking Academy Program. We have chosen to provide a special place, a Website, for all of us to interact together, build relationships, and have fun. I am pleased to announce the launch of the first phase of this Website.

The launch includes ways to acknowledge and celebrate participation in the program over the past 10 years:

- Points of Light
  - Spotlighting Academy locations around the world
  - Recognizing the breadth and depth of Academy participation

Select the folder containing the e-mail you want to copy

Figure 12-2 Selecting an e-mail to copy

Viewing E-mail Headers

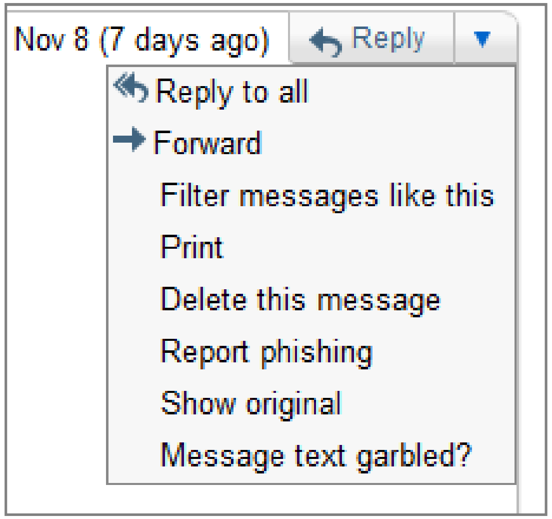
- Learn how to find e-mail headers
  - GUI clients
  - Command-line clients
  - Web-based clients
- After you open e-mail headers, copy and paste them into a text document
  - So that you can read them with a text editor
- Headers contain useful information
  - Unique identifying numbers, IP address of sending server, and sending time

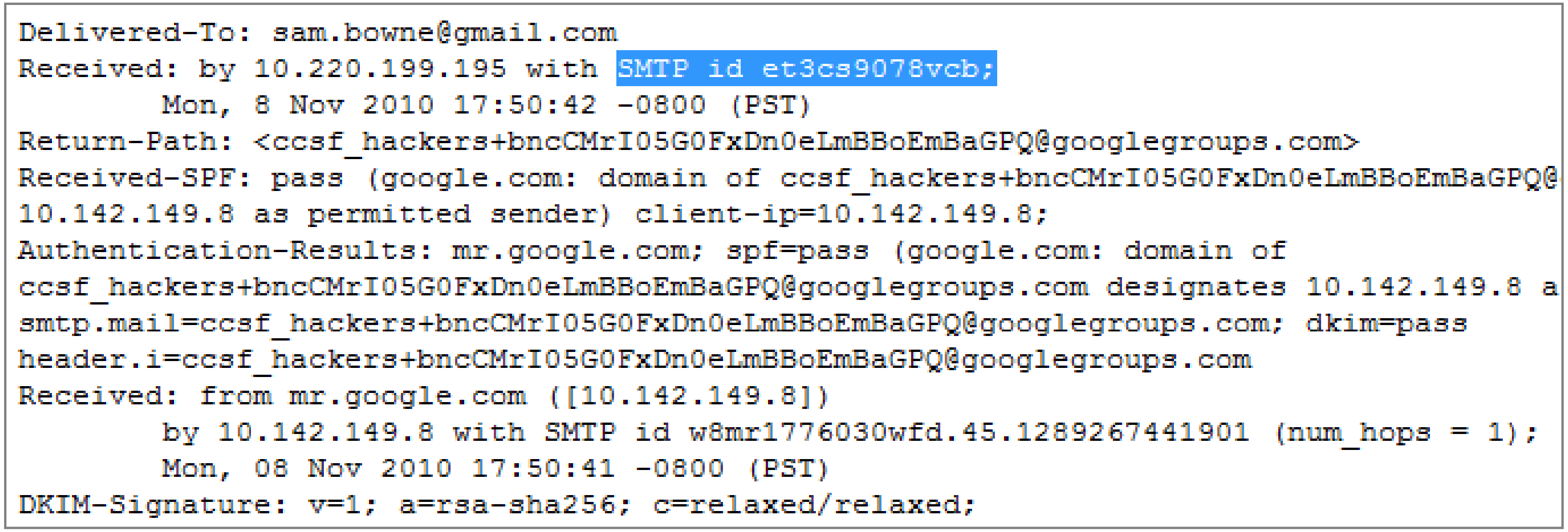
Viewing E-mail Headers (continued)

- 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

Email Headers in Gmail

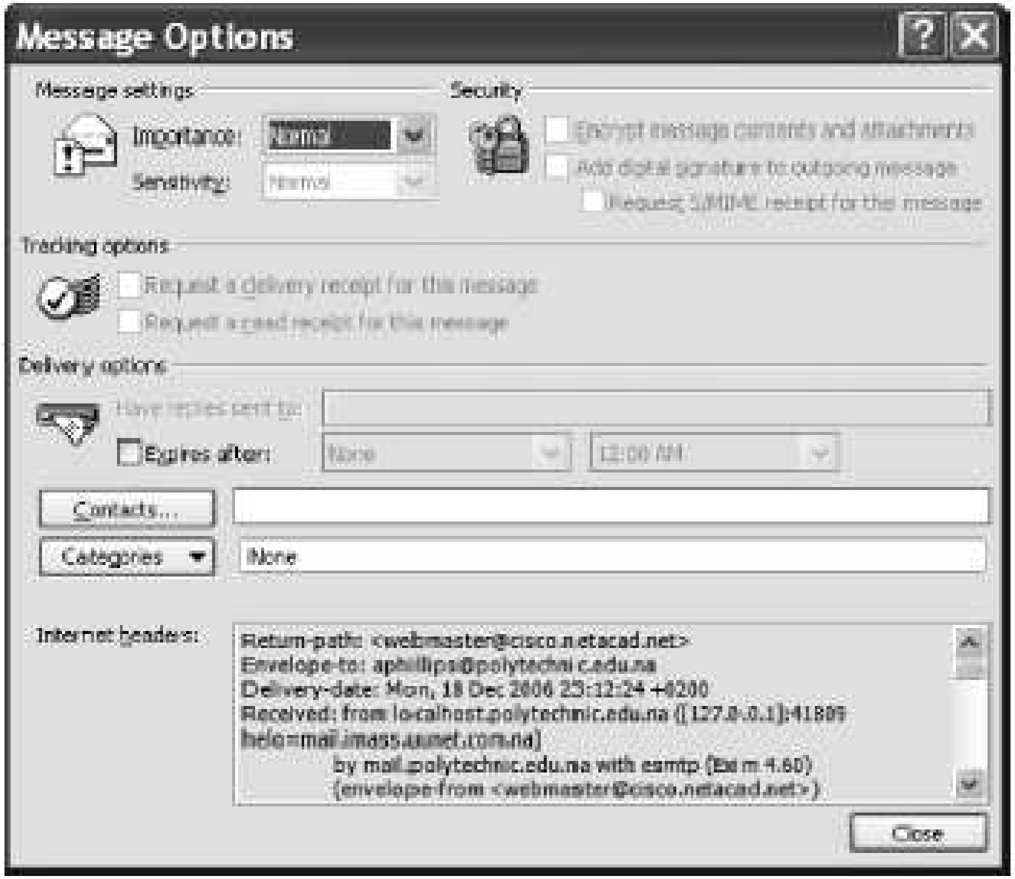
- Click “Reply” drop-down arrow, “Show original”





```
Delivered-To: sam.bowne@gmail.com
Received: by 10.220.199.195 with SMTP id et3cs9078vcb;
        Mon, 8 Nov 2010 17:50:42 -0800 (PST)
Return-Path: <ccsf_hackers+bncCMrI05G0FxDn0eLmBBoEmBaGPQ@googlegroups.com>
Received-SPF: pass (google.com: domain of ccsf_hackers+bncCMrI05G0FxDn0eLmBBoEmBaGPQ@
10.142.149.8 as permitted sender) client-ip=10.142.149.8;
Authentication-Results: mr.google.com; spf=pass (google.com: domain of
ccsf_hackers+bncCMrI05G0FxDn0eLmBBoEmBaGPQ@googlegroups.com designates 10.142.149.8 a
smtp.mail=ccsf_hackers+bncCMrI05G0FxDn0eLmBBoEmBaGPQ@googlegroups.com; dkim=pass
header.i=ccsf_hackers+bncCMrI05G0FxDn0eLmBBoEmBaGPQ@googlegroups.com
Received: from mr.google.com ([10.142.149.8])
        by 10.142.149.8 with SMTP id w8mr1776030wfd.45.1289267441901 (num_hops = 1);
        Mon, 08 Nov 2010 17:50:41 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Viewing E-mail Headers (continued)



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@polytechni c.edu.na
Delivery-date: Mon, 18 Dec 2006 23:12:24 +0200
Received: from lo-calhost.polytechnic.edu.na ([127.0.0.1]:41889
helo=mail.imass.uunet.com.na)
            by mail.polytechnic.edu.na with esmtp (Exim 4.60)
            (envelope-from <webmaster@cisco.netacad.net>)
```

Figure 12-3 An Outlook e-mail header

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
    - See link Ch 12b for an example—tracing the source of spam

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

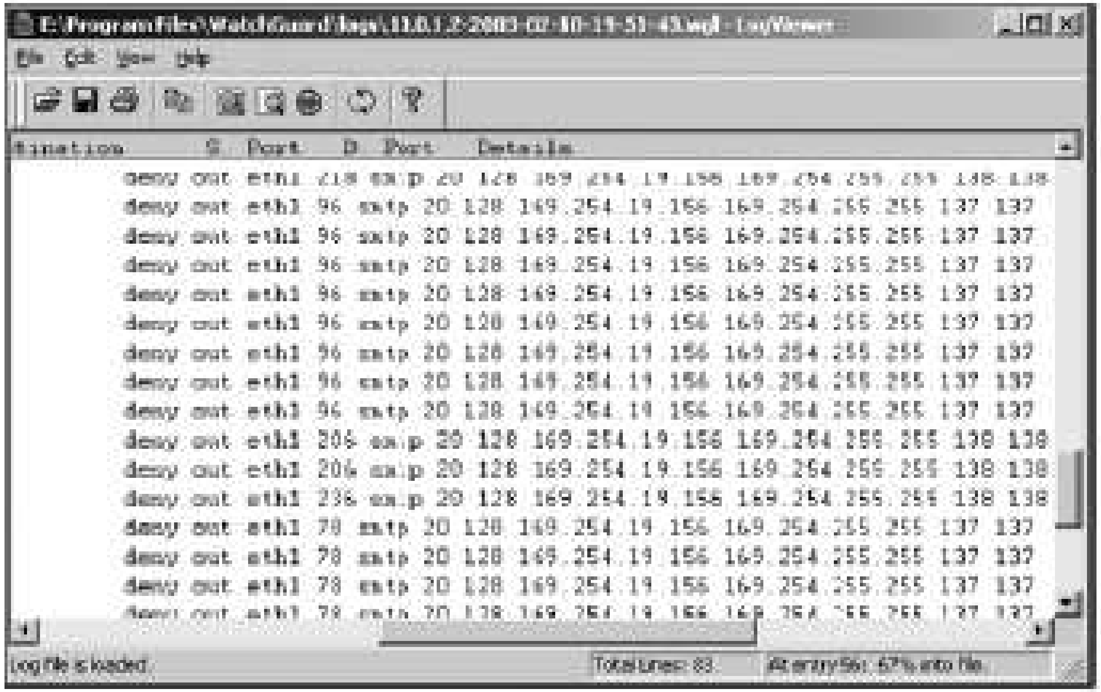
Tracing an E-mail Message

- 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)



E:\Program Files\WatchGuard\logs\11.0.1.2-2003-02-10-19-51-43.wgl - LogViewer
File
Edit
View
Help

```
tination         S. Port   D. Port    Details
         deny out eth1 218 smtp 20 128 169.254.19.156 169.254.255.255 138 138
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 96  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 206 smtp 20 128 169.254.19.156 169.254.255.255 138 138
         deny out eth1 206 smtp 20 128 169.254.19.156 169.254.255.255 138 138
         deny out eth1 236 smtp 20 128 169.254.19.156 169.254.255.255 138 138
         deny out eth1 78  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 78  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 78  smtp 20 128 169.254.19.156 169.254.255.255 137 137
         deny out eth1 78  smtp 20 128 169.254.19.156 169.254.255.255 137 137
```

Log file is loaded. Total lines: 83. At entry 56: 67% into file.

Figure 12-13 A firewall log

Understanding E-mail Servers

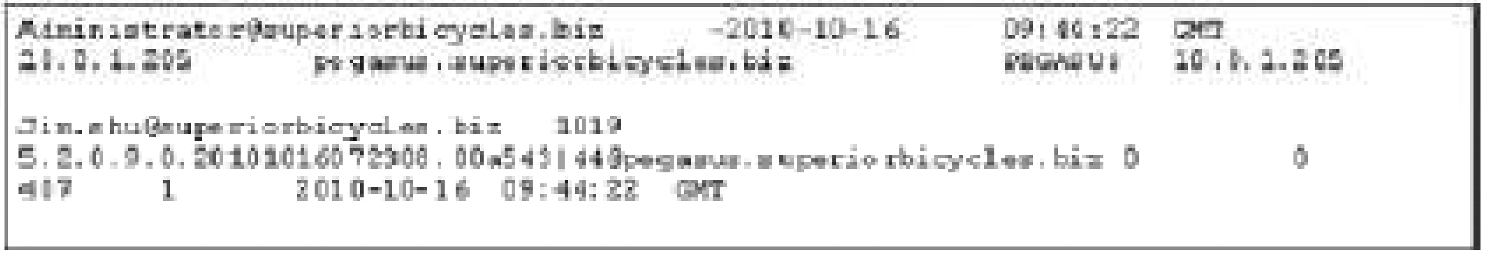
Understanding E-mail Servers

- 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)



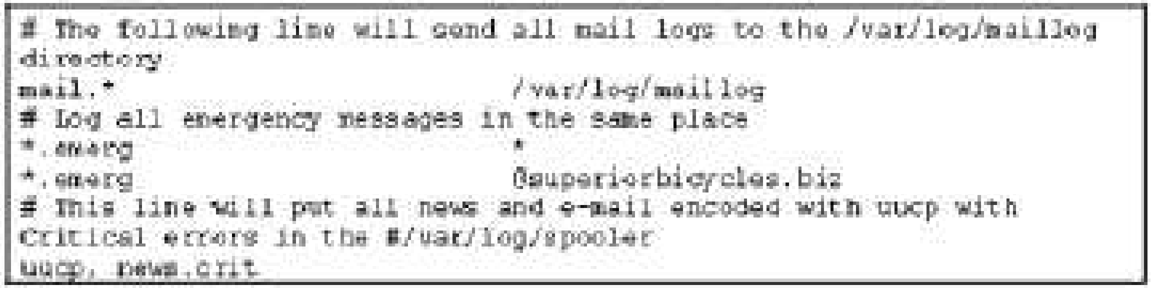
```
Administrator@superiorbicycles.biz      -2010-10-16      09:44:22   GMT
10.0.1.205        pegasus.superiorbicycles.biz           PEGASUS    10.0.1.205

Jim.shu@superiorbicycles.biz    1019
5.2.0.9.0.20101016072308.00a543144@pegasus.superiorbicycles.biz 0          0
417      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

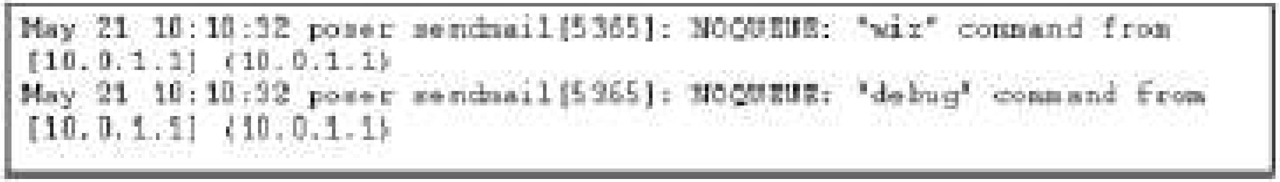
Examining UNIX E-mail Server Logs (continued)



```
# 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 uucp with
Critical errors in the #/var/log/spooler
uucp, news.crit
```

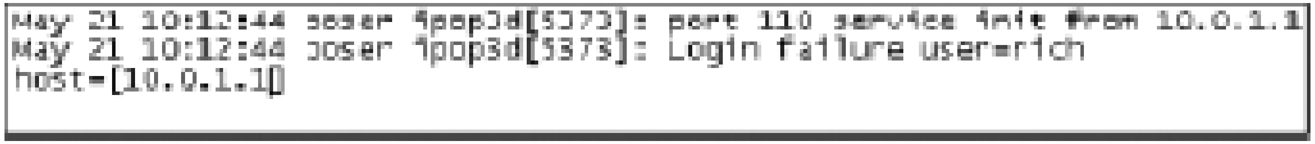
Figure 12-15 A typical syslog.conf file

Examining UNIX E-mail Server Logs (continued)



```
May 21 10:10:32 poser sendmail[5365]: NOQUEUE: "wiz" 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 ipop3d[5373]: port 110 service init from 10.0.1.1
May 21 10:12:44 poser ipop3d[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
- Messaging Application Programming Interface (MAPI)
  - A Microsoft system that enables different e- mail applications to work together

Examining Microsoft E-mail Server Logs

- The “Information Store” is made of tw0 files
  - Database files *.edb
    - Responsible for MAPI information
  - Database files *.stm
    - Responsible for non-MAPI information

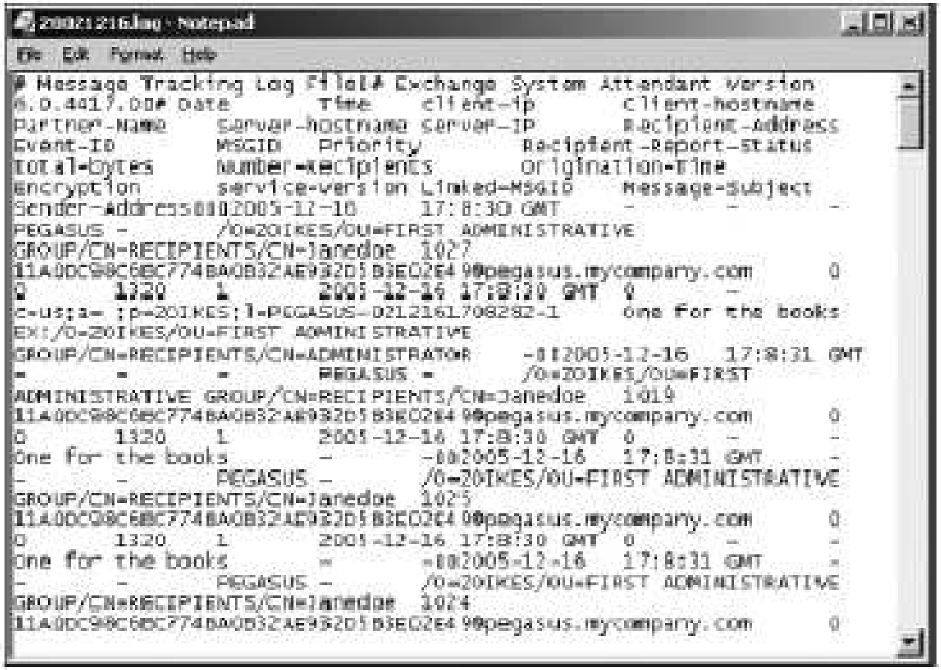
Examining Microsoft E-mail Server Logs (continued)

- Administrators can recover lost or deleted emails from these files:
  - Transaction log
    - Keep track of e-mail databases
  - Checkpoints
    - Marks the place in the transaction log where the last backup was made

Examining Microsoft E-mail Server Logs (continued)

- Other useful files
  - Temporary files
  - E-mail communication logs
    - res#.log
  - Tracking.log
    - Tracks messages

Examining Microsoft E-mail Server Logs (continued)



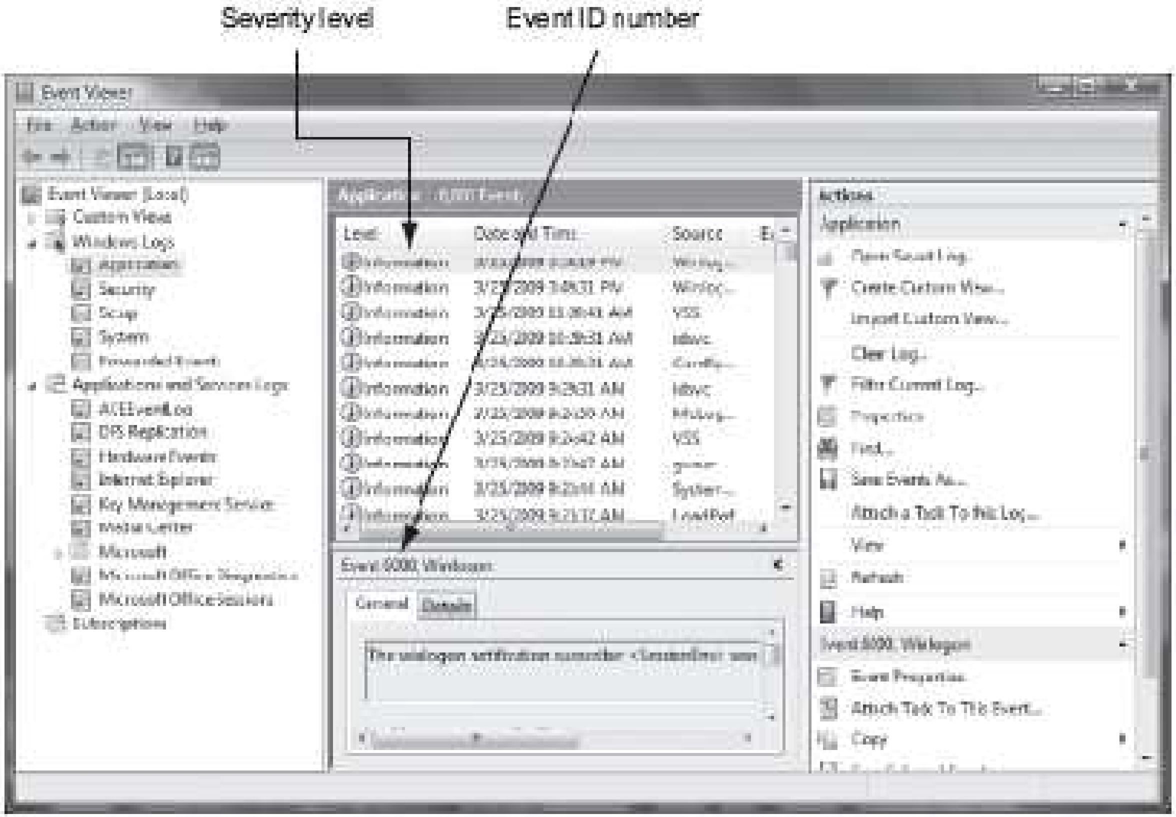
```
# Message Tracking Log File# Exchange System Attendant Version
6.0.4417.0# Date        Time     client-ip        Client-hostname
Partner-Name    Server-hostname server-IP        Recipient-Address
Event-ID        MSGID   Priority         Recipient-Report-Status
total-bytes     Number-Recipients        Origination-Time
Encryption      service-Version Linked-MSGID    Message-Subject
Sender-Address002005-12-16      17:8:30 GMT      -       -       -
PEGASUS -       /O=ZOIKES/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=Janedoe  1027
11A0DC90C60C774BA0B32AE932D5B3E0264 9@pegasus.mycompany.com      0
0       1320    1       2005-12-16 17:8:29 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
11A0DC90C60C774BA0B32AE932D5B3E0264 9@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
11A0DC90C60C774BA0B32AE932D5B3E0264 9@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
11A0DC90C60C774BA0B32AE932D5B3E0264 9@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)



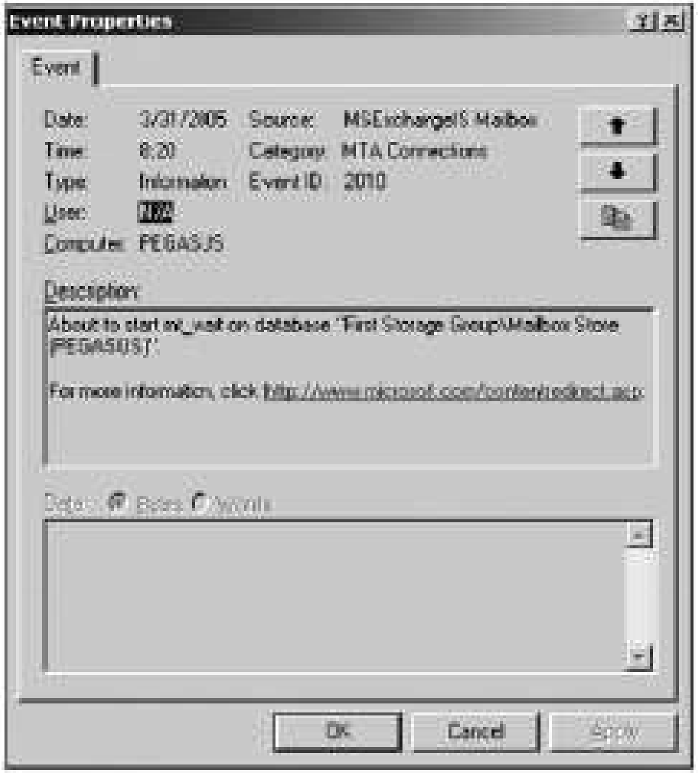
Level	Date and Time	Source	E
Information	3/2[illegible]/2009 [illegible] PM	Winlog...	
Information	3/25/2009 3:49:31 PM	Winlog...	
Information	3/25/2009 11:39:41 AM	VSS	
Information	3/25/2009 10:39:31 AM	ltsvc	
Information	3/25/2009 10:39:31 AM	Config...	
Information	3/25/2009 9:29:31 AM	ltsvc	
Information	3/25/2009 9:24:39 AM	MsiLog...	
Information	3/25/2009 9:24:42 AM	VSS	
Information	3/25/2009 9:[illegible] AM	[illegible]	
Information	3/25/2009 9:23:[illegible] AM	System...	
Information	3/25/2009 9:21:17 AM	LoadPerf	

Event 6000, Winlogon

The winlogon notification subscriber <SessionEnv> was

Figure 12-19 Viewing a log in Event Viewer

Examining Microsoft E-mail Server Logs (continued)



Date: 3/31/2005 Source: MSExchangeIS Mailbox
Time: 8:20 Category: MTA Connections
Type: Information Event ID: 2010
User: N/A
Computer: PEGASUS

Description:
About to start mr_wait on database "First Storage Group\Mailbox Store (PEGASUS)".

For more information, click http://www.microsoft.com/contentredirect.asp.

Data: ● Bytes ○ Words

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

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

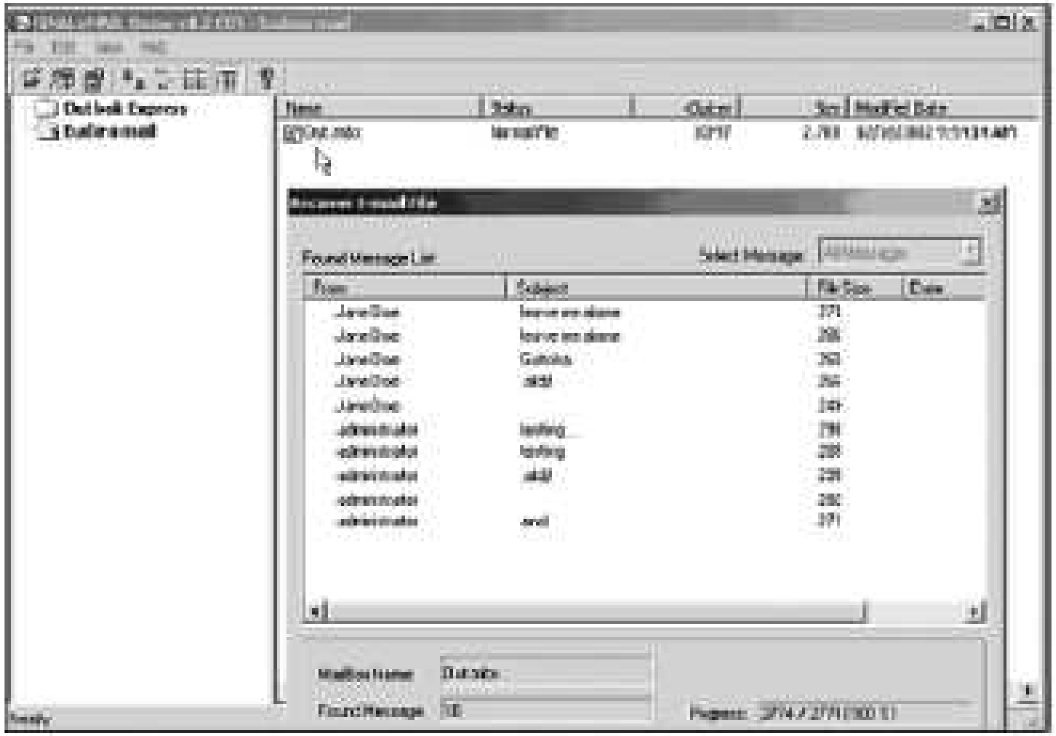
Using Specialized E-mail Forensics Tools (continued)

- 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)



Outlook Express
Outlook email

Name	Status	Cluster	Size	Modified Date
[illegible].mbx	[illegible]	[illegible]	2,[illegible]	[illegible]

Found Message List

Select Message: All Messages

From	Subject	File Size	Date
JaneDoe	leave me alone	271	
JaneDoe	leave me alone	266	
JaneDoe	Gotcha	263	
JaneDoe	[illegible]	256	
JaneDoe		249	
administrator	testing...	298	
administrator	testing	288	
administrator	[illegible]	238	
administrator		282	
administrator	and	271	

MailBox Name: [illegible]

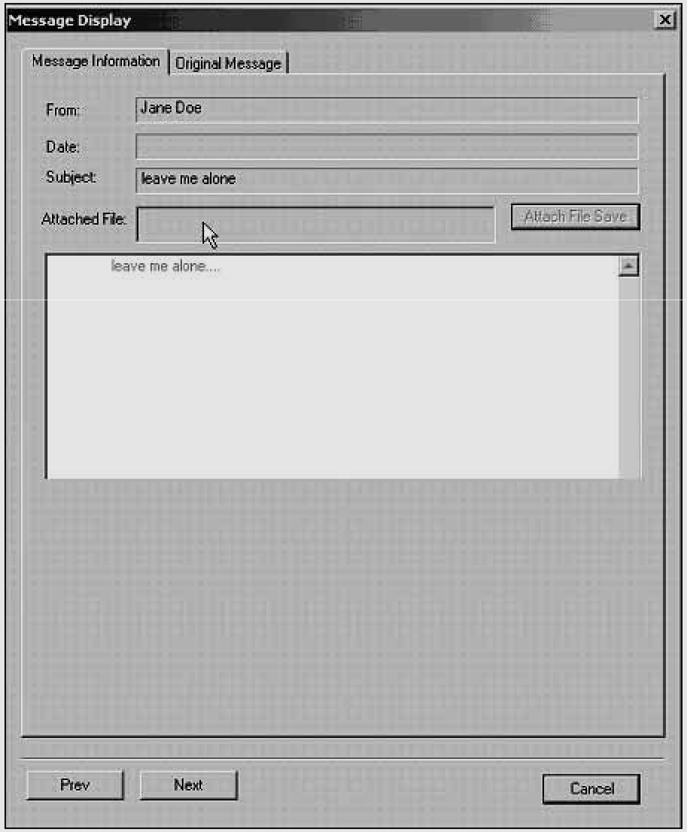
Found Message: 10

Progress: [illegible]

Ready

Figure 12-21 E-mail search results in FINALeMAIL

Using Specialized E-mail Forensics Tools (continued)



From: Jane Doe

Date:

Subject: leave me alone

Attached File:

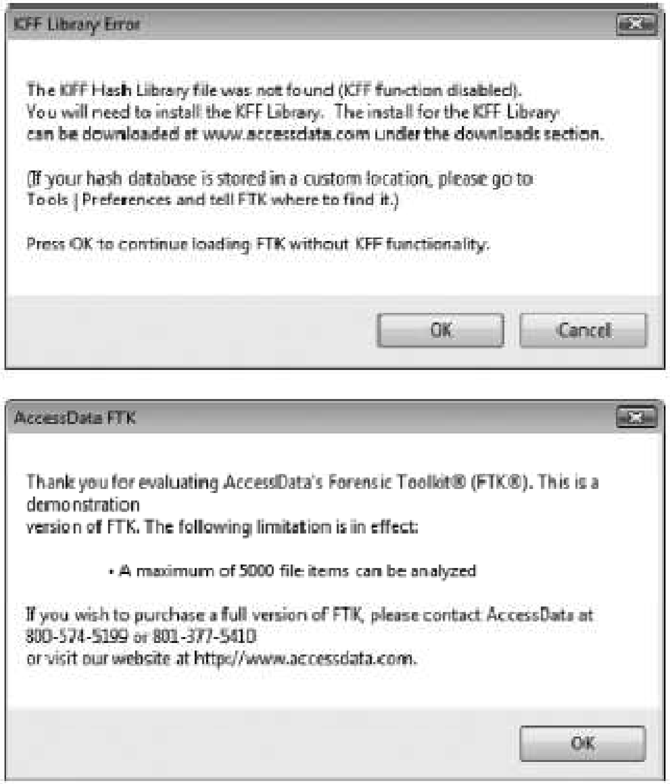
leave me alone....

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)



The KFF Hash Library file was not found (KFF function disabled).
You will need to install the KFF Library. The install for the KFF Library can be downloaded at www.accessdata.com under the downloads section.

(If your hash database is stored in a custom location, please go to Tools | Preferences and tell FTK where to find it.)

Press OK to continue loading FTK without KFF functionality.

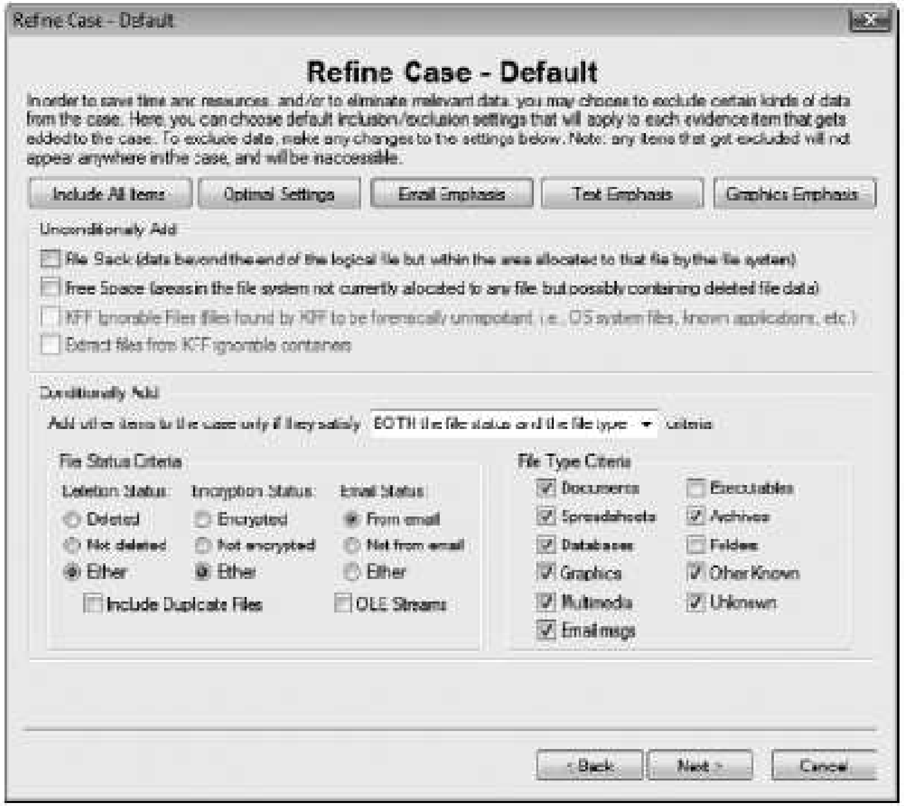
Thank you for evaluating AccessData's Forensic Toolkit® (FTK®). This is a demonstration
version of FTK. The following limitation is in effect:

- A maximum of 5000 file items can be analyzed

If you wish to purchase a full version of FTK, please contact AccessData at 800-574-5199 or 801-377-5410
or visit our website at http://www.accessdata.com.

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

Using AccessData FTK to Recover E-mail (continued)



Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that got excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add

- □ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- □ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- □ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- □ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	● From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	○ Either

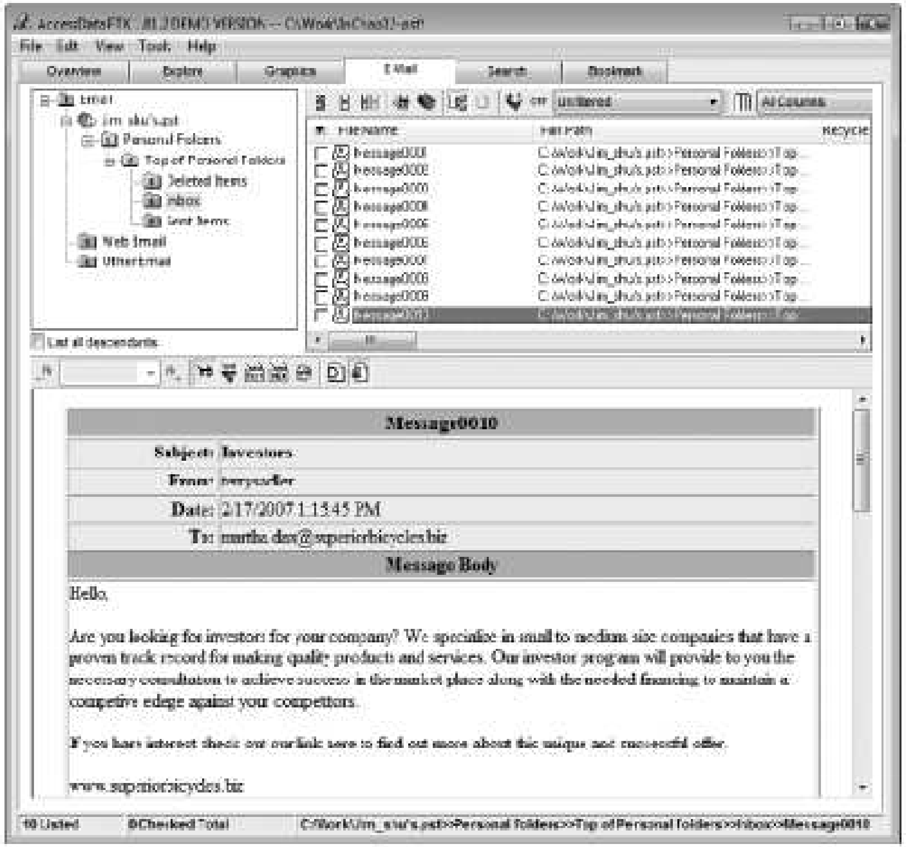
□ Include Duplicate Files □ OLE Streams

File Type Criteria

☑ Documents	□ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	□ Folders
☑ Graphics	☑ Other Known
☑ Multimedia	☑ Unknown
☑ Email msgs	

Figure 12-25 The Refine Case Default dialog box

Using AccessData FTK to Recover E-mail (continued)



File Name	Full Path	Recycle
□ message0001	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0002	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0003	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0004	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0005	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0006	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0007	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0008	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0009	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	
□ message0010	C:\Work\Jim_shu's.pst>>Personal Folders>>Top...	

Message0010

Subject:	Investors
From:	terrysadler
Date:	2/17/2007 1:13:45 PM
To:	martha.dax@superiorbicycles.biz

Message Body

Hello,

Are 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 competive edge against your competitors.

If you have interest check out our link here to find out more about this unique and successful offer.

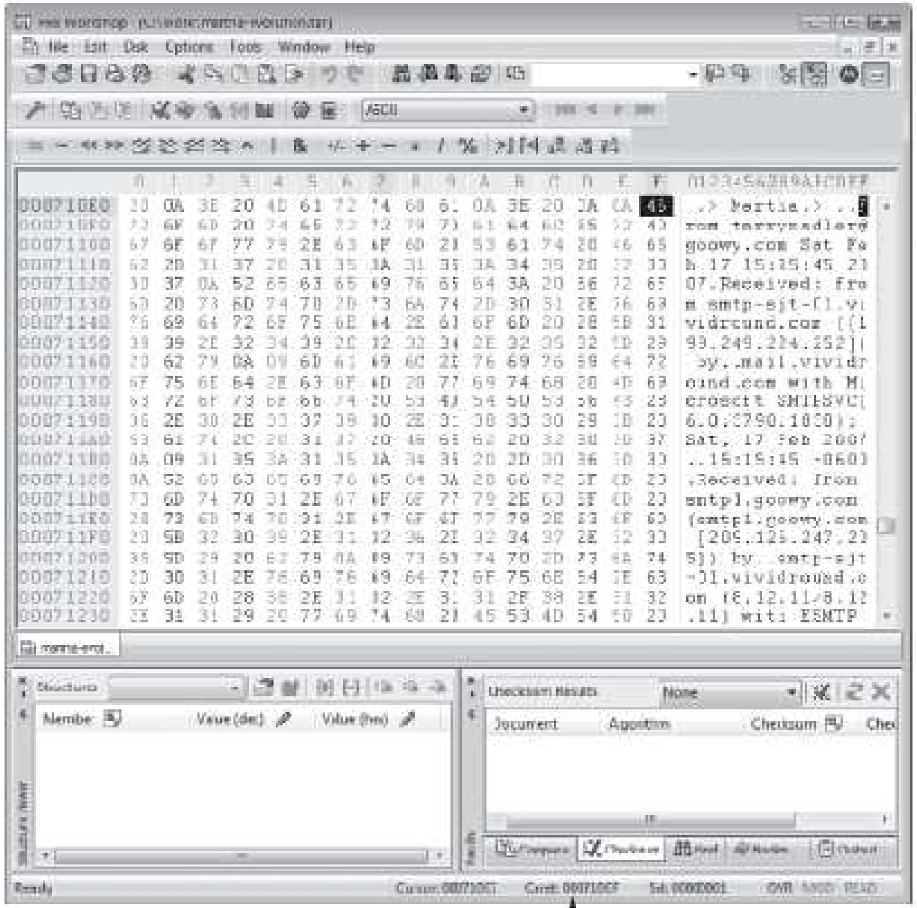
www.superiorbicycles.biz

10 Listed | 0 Checked Total | C:\Work\Jim_shu's.pst>>Personal Folders>>Top of Personal Folders>>Inbox>>Message0010

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

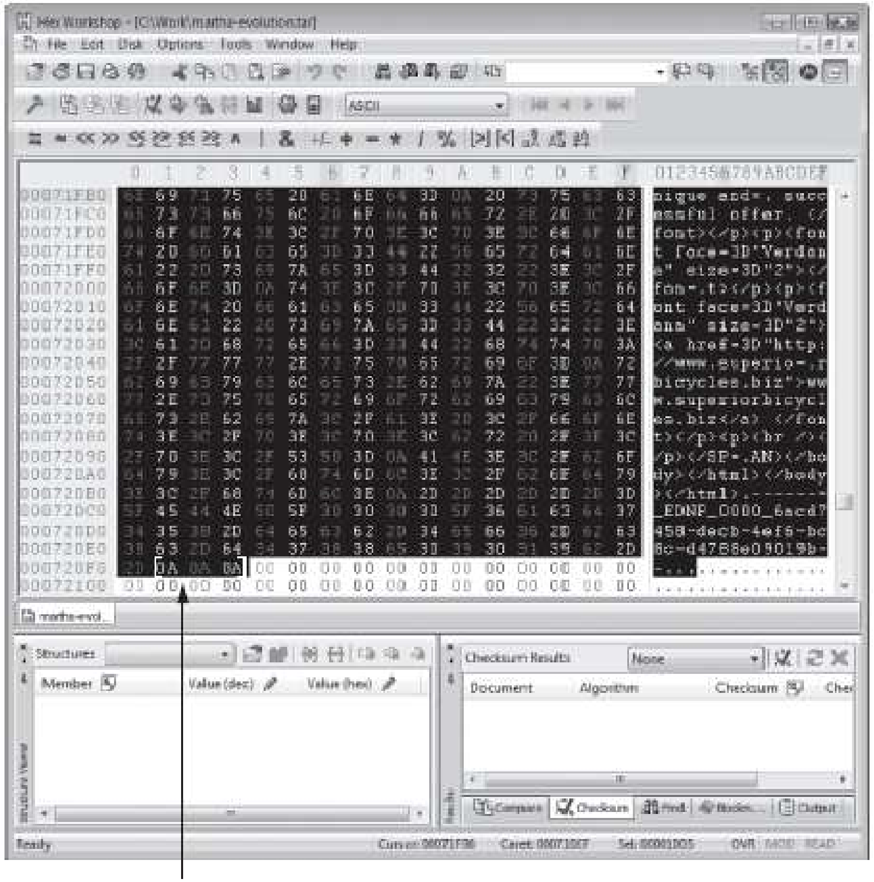


Hex Workshop
File Edit Disk Options Tools Window Help
ASCII
Structures
Member Value (dec) Value (hex)
Checksum Results None
Document Algorithm Checksum Che
Compare Checksum Find Bookmarks Output
Ready Cursor: 000710EF Caret: 000710EF Sel: 00000001 OVR MOD READ

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
000710E0  20 0A 3E 20 4D 61 72 74 68 61 0A 3E 20 0A 0A 46   .> Martha.> ..F
000710F0  72 6F 6D 20 74 65 72 72 79 73 61 64 6C 65 72 40  rom terrysadler@
00071100  67 6F 6F 77 79 2E 63 6F 6D 20 53 61 74 20 46 65  goowy.com Sat Fe
00071110  62 20 31 37 20 31 35 3A 31 35 3A 34 35 20 32 30  b 17 15:15:45 20
00071120  30 37 0A 52 65 63 65 69 76 65 64 3A 20 66 72 6F  07.Received: fro
00071130  6D 20 73 6D 74 70 2D 73 6A 74 2D 30 31 2E 76 69  m smtp-sjt-01.vi
00071140  76 69 64 72 6F 75 6E 64 2E 63 6F 6D 20 28 5B 31  vidround.com ([1
00071150  39 33 2E 32 34 39 2E 32 32 34 2E 32 35 32 5D 29  93.249.224.252])
00071160  20 62 79 0A 09 6D 61 69 6C 2E 76 69 76 69 64 72   by..mail.vividr
00071170  6F 75 6E 64 2E 63 6F 6D 20 77 69 74 68 20 4D 69  ound.com with Mi
00071180  63 72 6F 73 6F 66 74 20 53 4D 54 50 53 56 43 28  crosoft SMTPSVC(
00071190  36 2E 30 2E 33 37 39 30 2E 31 38 33 30 29 3B 20  6.0.3790.1830); 
000711A0  53 61 74 2C 20 31 37 20 46 65 62 20 32 30 30 37  Sat, 17 Feb 2007
000711B0  0A 09 31 35 3A 31 35 3A 34 35 20 2D 30 36 30 30  ..15:15:45 -0600
000711C0  0A 52 65 63 65 69 76 65 64 3A 20 66 72 6F 6D 20  .Received: from 
000711D0  73 6D 74 70 31 2E 67 6F 6F 77 79 2E 63 6F 6D 20  smtp1.goowy.com 
000711E0  28 73 6D 74 70 31 2E 67 6F 6F 77 79 2E 63 6F 6D  (smtp1.goowy.com
000711F0  20 5B 32 30 39 2E 31 32 36 2E 32 34 37 2E 32 33   [209.126.247.23
00071200  35 5D 29 20 62 79 0A 09 73 6D 74 70 2D 73 6A 74  5]) by..smtp-sjt
00071210  2D 30 31 2E 76 69 76 69 64 72 6F 75 6E 64 2E 63  -01.vividround.c
00071220  6F 6D 20 28 38 2E 31 32 2E 31 31 2F 38 2E 31 32  om (8.12.11/8.12
00071230  2E 31 31 29 20 77 69 74 68 20 45 53 4D 54 50 20  .11) with ESMTP 
```

Offset byte count from beginning of file

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

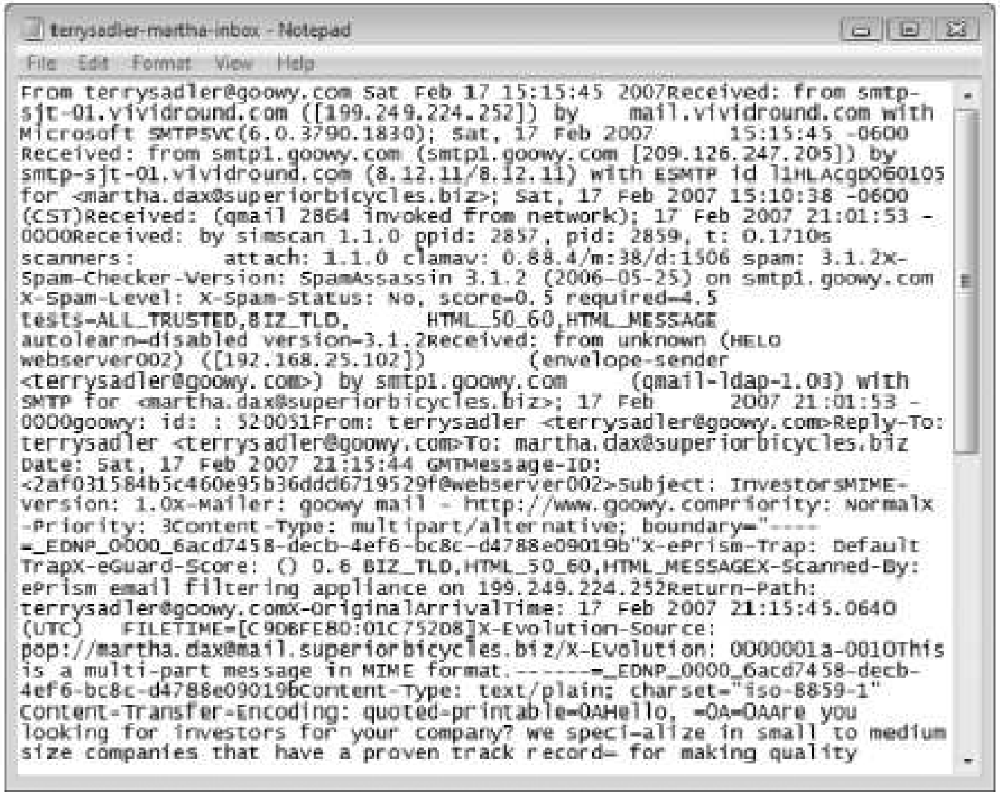


```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00071FB0 6E 69 71 75 65 20 65 6E 64 3D 0A 20 73 75 63 63  nique end=. succ
00071FC0 65 73 73 66 75 6C 20 6F 66 66 65 72 2E 20 3C 2F  essful offer. </
00071FD0 66 6F 6E 74 3E 3C 2F 70 3E 3C 70 3E 3C 66 6F 6E  font></p><p><fon
00071FE0 74 20 66 61 63 65 3D 33 44 22 56 65 72 64 61 6E  t face=3D"Verdan
00071FF0 61 22 20 73 69 7A 65 3D 33 44 22 32 22 3E 3C 2F  a" size=3D"2"></
00072000 66 6F 6E 3D 0A 74 3E 3C 2F 70 3E 3C 70 3E 3C 66  fon=.t></p><p><f
00072010 6F 6E 74 20 66 61 63 65 3D 33 44 22 56 65 72 64  ont face=3D"Verd
00072020 61 6E 61 22 20 73 69 7A 65 3D 33 44 22 32 22 3E  ana" size=3D"2">
00072030 3C 61 20 68 72 65 66 3D 33 44 22 68 74 74 70 3A  <a href=3D"http:
00072040 2F 2F 77 77 77 2E 73 75 70 65 72 69 6F 3D 0A 72  //www.superio=.r
00072050 62 69 63 79 63 6C 65 73 2E 62 69 7A 22 3E 77 77  bicycles.biz">ww
00072060 77 2E 73 75 70 65 72 69 6F 72 62 69 63 79 63 6C  w.superiorbicycl
00072070 65 73 2E 62 69 7A 3C 2F 61 3E 20 3C 2F 66 6F 6E  es.biz</a> </fon
00072080 74 3E 3C 2F 70 3E 3C 70 3E 3C 62 72 20 2F 3E 3C  t></p><p><br /><
00072090 2F 70 3E 3C 2F 53 50 3D 0A 41 4E 3E 3C 2F 62 6F  /p></SP=.AN></bo
000720A0 64 79 3E 3C 2F 68 74 6D 6C 3E 3C 2F 62 6F 64 79  dy></html></body
000720B0 3E 3C 2F 68 74 6D 6C 3E 0A 2D 2D 2D 2D 2D 2D 2D  ></html>.-------
000720C0 5F 45 44 4E 50 5F 30 30 30 30 5F 36 61 63 64 37  _EDNP_0000_6acd7
000720D0 34 35 38 2D 64 65 63 62 2D 34 65 66 36 2D 62 63  458-decb-4ef6-bc
000720E0 38 63 2D 64 34 37 38 38 65 30 39 30 31 39 62 2D  8c-d4788e09019b-
000720F0 2D 0A 0A 0A 00 00 00 00 00 00 00 00 00 00 00 00  -...............
00072100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Ending position for this message

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

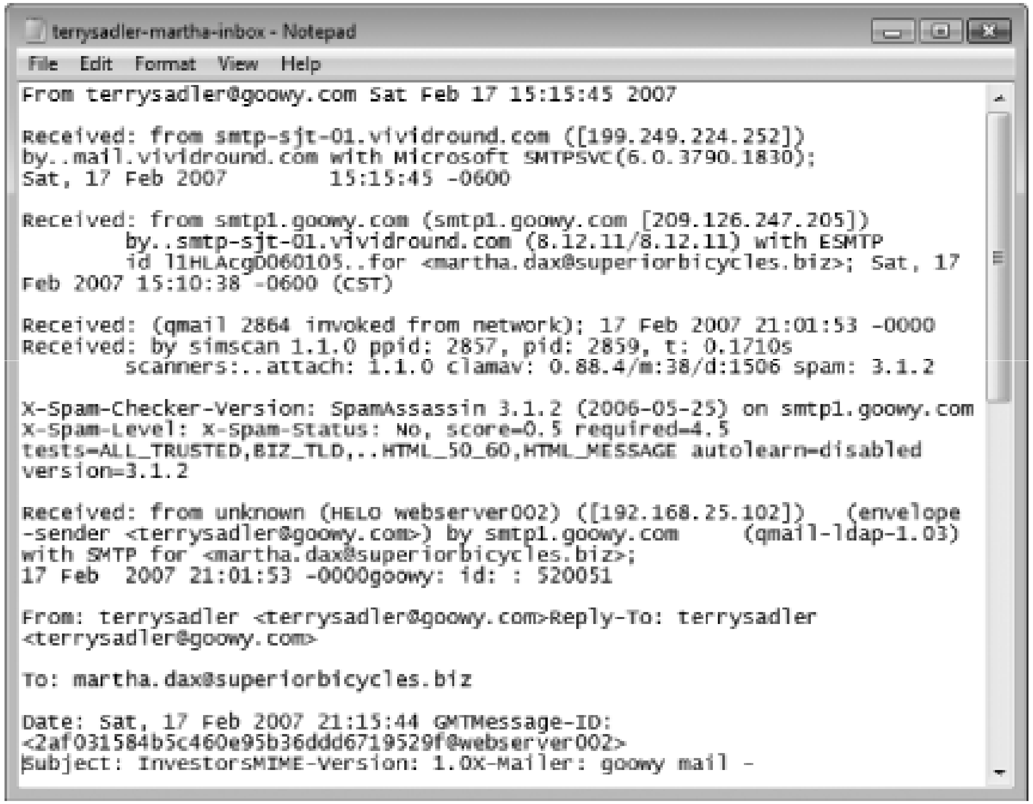
Using a Hexadecimal Editor to Carve E-mail Messages (continued)


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 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=3.1.2Received: 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=[C9D8FE80:01C75208]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)


terrysadler-martha-inbox - Notepad
File Edit Format View Help

```
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 -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 <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: : 520051

From: 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 -
```

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

Recovering Deleted Outlook Files

- Microsoft's Inbox Repair Tool (scanpst)
  - Link Ch 12d
- EnCase
- Advanced Outlook Repair from DataNumen, Inc.
  - Link Ch 12e