# Guide to Computer Forensics and Investigations Sixth 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

Describe some specialized e-mail forensics tools

Explain how to apply digital forensics methods to investigating social media communications

# Exploring the Role of E-mail in Investigations (3 of 3)

An increase in e-mail scams and fraud attempts with phishing or spoofing

As a digital forensics' investigator, one might be called to investigate a phishing e-mail to see whether it is authentic or not.

Investigators need to know how to examine and interpret the unique content of e-mail messages

One of the Forensics Examiner’s job is also to trace email message

We can also look at resources for spoofed messages, by looking up for email and web addresses.

# Exploring the Role of E-mail in Investigations (2 of 3)

**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

**Spoofing** e-mail can be used to commit fraud

More spoofing examples are on

- www.hoax-slayer.com

To test whether a redirection was done we need to message HTML source code and check if the Internet link is labeled with redirection to a different web site.

# Exploring the Roles of the Client and Server in E-mail (1 of 3)

- E-mail can be sent and received in two environments
  - Internet
  - Intranet (an internal network)
  - In both environment messages are distributed from central server to many connected client computers
- **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 (2 of 3)

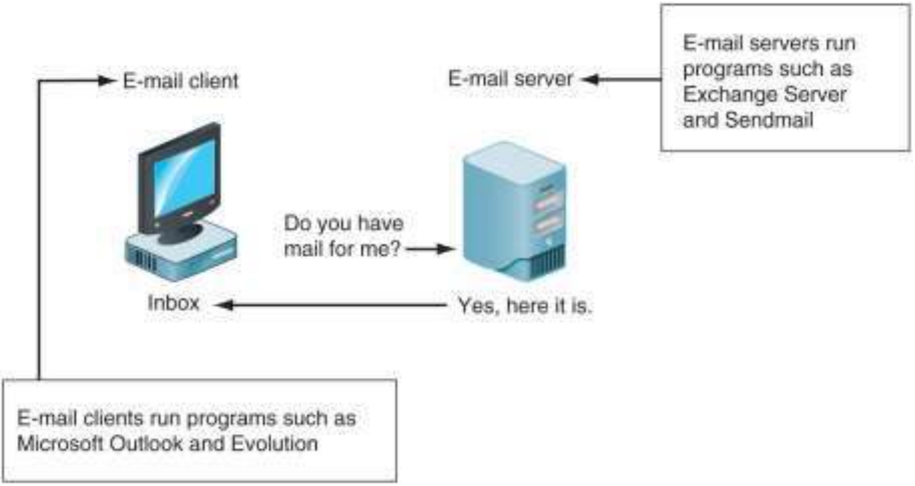

E-mail client
E-mail server
E-mail servers run programs such as Exchange Server and Sendmail
Do you have mail for me?
Inbox
Yes, here it is.
E-mail clients run programs such as Microsoft Outlook and Evolution

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

# Exploring the Roles of the Client and Server in E-mail (3 of 3)

Regardless of the OS or email program users access their email based on permissions the e-mail server administrator grants. These premonitions prevent users from accessing each other’s email.

# Exploring the Roles of the Client and Server in E-mail (3 of 3)

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 (1 of 2)

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 (2 of 2)

## 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 (1 of 2)

Access victim’s computer or mobile device to recover the evidence

Using the victim’s e-mail client

- Find and copy any potential evidence
- 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 (2 of 2)

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 (1 of 5)

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

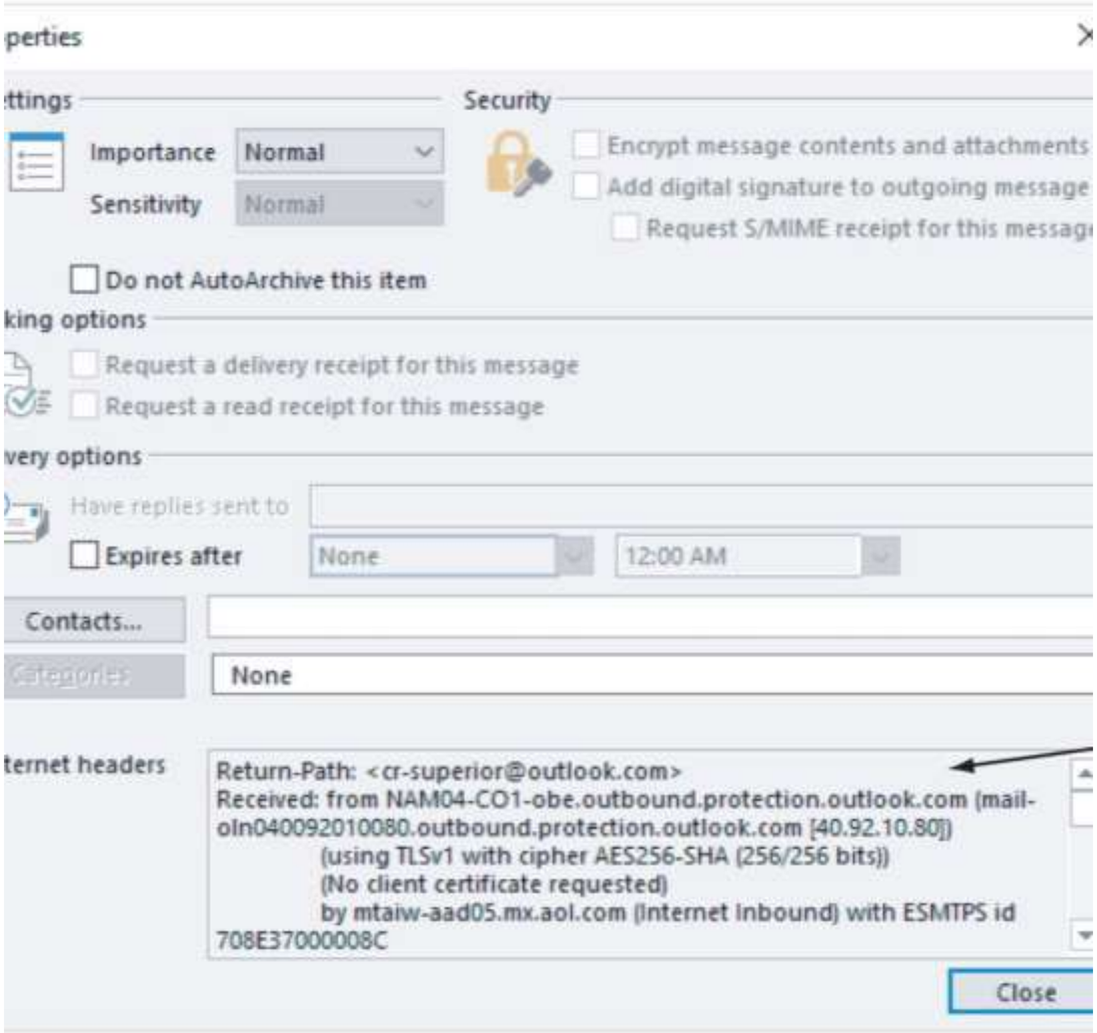
- Often more than one e-mail program is installed

# Viewing E-mail Headers (2 of 5)

Outlook

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

# Viewing E-mail Headers (3 of 5)



perties

ttings

Importance: Normal

Sensitivity: Normal

□ Do not AutoArchive this item

Security

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this messag

king options

□ Request a delivery receipt for this message

□ Request a read receipt for this message

very options

Have replies sent to

□ Expires after: None 12:00 AM

Contacts...

Categories: None

ternet headers

```
Return-Path: <cr-superior@outlook.com>
Received: from NAM04-CO1-obe.outbound.protection.outlook.com (mail-
oln040092010080.outbound.protection.outlook.com [40.92.10.80])
            (using TLSv1 with cipher AES256-SHA (256/256 bits))
            (No client certificate requested)
            by mtaiw-aad05.mx.aol.com (Internet Inbound) with ESMTPS id
708E37000008C
```

ure 11-2 An Outlook e-mail header

# Viewing E-mail Headers (4 of 5)

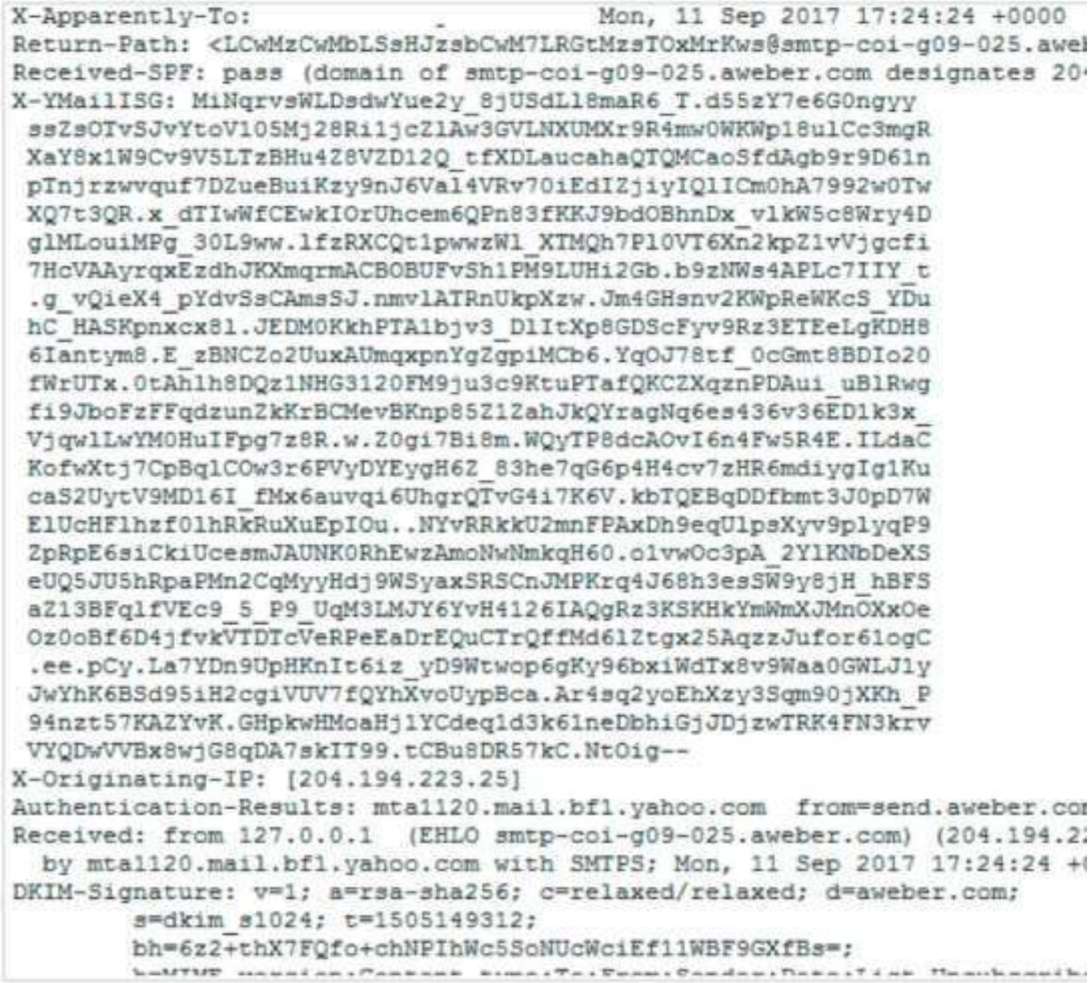
Gmail

- Click the down arrow next to the Reply circular arrow, and click **Show original**
- Click the **Download Original** link to open the “Opening original_msg.txt” dialog box
- Click **Open with Notepad (default)** and click **Okay**
- Save the file in your work folder with the default name

Yahoo

- Click **Inbox** to view a list of messages
- Above the message window, click **More** and click **View Raw Message**
- Copy and paste headers to a text file

# Viewing E-mail Headers (5 of 5)



```
X-Apparently-To:                        Mon, 11 Sep 2017 17:24:24 +0000
Return-Path: <LCwMzCwMbLSsHJzsbCwM7LRGtMzsTOxMrKws@smtp-coi-g09-025.awel
Received-SPF: pass (domain of smtp-coi-g09-025.aweber.com designates 20
X-YMailISG: MiNqrvsWLDsdwYue2y_8jUSdLl8maR6_T.d55zY7e6G0ngyy
 ssZsOTvSJvYtoV105Mj28Ri1jcZ1Aw3GVLNXUMXr9R4mw0WKWp18ulCc3mgR
 XaY8x1W9Cv9V5LTzBHu4Z8VZD12Q_tfXDLaucahaQTQMCaoSfdAgb9r9D61n
 pTnjrzwvquf7DZueBuiKzy9nJ6Val4VRv70iEdIZjiyIQlICm0hA7992w0Tw
 XQ7t3QR.x_dTIwWfCEwkIOrUhcem6QPn83fKKJ9bdOBhnDx_vlkW5c8Wry4D
 glMLouiMPg_30L9ww.lfzRXCQt1pwwzWl_XTMQh7Pl0VT6Xn2kpZ1vVjgcfi
 7HcVAAyrqxEzdhJKXmqrmACBOBUFvSh1PM9LUHi2Gb.b9zNWs4APLc7IIY_t
 .g_vQieX4_pYdvSsCAmsSJ.nmvlATRnUkpXzw.Jm4GHsnv2KWpReWKcS_YDu
 hC_HASKpnxcx81.JEDM0KkhPTA1bjv3_DlItXp8GDScFyv9Rz3ETEeLgKDH8
 6Iantym8.E_zBNCZo2UuxAUmqxpnYgZgpiMCb6.YqOJ78tf_0cGmt8BDIo20
 fWrUTx.0tAhlh8DQz1NHG3120FM9ju3c9KtuPTafQKCZXqznPDAui_uBlRwg
 fi9JboFzFFqdzunZkKrBCMevBKnp85Z1ZahJkQYragNq6es436v36ED1k3x_
 VjqwlLwYM0HuIFpg7z8R.w.Z0gi7Bi8m.WQyTP8dcAOvI6n4Fw5R4E.ILdaC
 KofwXtj7CpBqlCOw3r6PVyDYEygH6Z_83he7qG6p4H4cv7zHR6mdiygIg1Ku
 caS2UytV9MD16I_fMx6auvqi6UhgrQTvG4i7K6V.kbTQEBqDDfbmt3J0pD7W
 ElUcHFlhzf0lhRkRuXuEpIOu..NYvRRkkU2mnFPAxDh9eqUlpsXyv9plyqP9
 ZpRpE6siCkiUcesmJAUNK0RhEwzAmoNwNmkqH60.o1vwOc3pA_2YlKNbDeXS
 eUQ5JU5hRpaPMn2CqMyyHdj9WSyaxSRSCnJMPKrq4J68h3esSW9y8jH_hBFS
 aZ13BFqlfVEc9_5_P9_UqM3LMJY6YvH4126IAQgRz3KSKHkYmWmXJMnOXxOe
 Oz0oBf6D4jfvkVTDTcVeRPeEaDrEQuCTrQffMd61Ztgx25AqzzJufor61ogC
 .ee.pCy.La7YDn9UpHKnIt6iz_yD9Wtwop6gKy96bxiWdTx8v9Waa0GWLJ1y
 JwYhK6BSd95iH2cgiVUV7fQYhXvoUypBca.Ar4sq2yoEhXzy3Sqm90jXKh_P
 94nzt57KAZYvK.GHpkwHMoaHj1YCdeq1d3k61neDbhiGjJDjzwTRK4FN3krv
 VYQDwVVBx8wjG8qDA7skIT99.tCBu8DR57kC.NtOig--
X-Originating-IP: [204.194.223.25]
Authentication-Results: mta1120.mail.bf1.yahoo.com  from=send.aweber.co
Received: from 127.0.0.1  (EHLO smtp-coi-g09-025.aweber.com) (204.194.2
  by mta1120.mail.bf1.yahoo.com with SMTPS; Mon, 11 Sep 2017 17:24:24 +
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=aweber.com;
        s=dkim_s1024; t=1505149312;
        bh=6z2+thX7FQfo+chNPIhWc5SoNUcWciEf11WBF9GXfBs=;
```

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

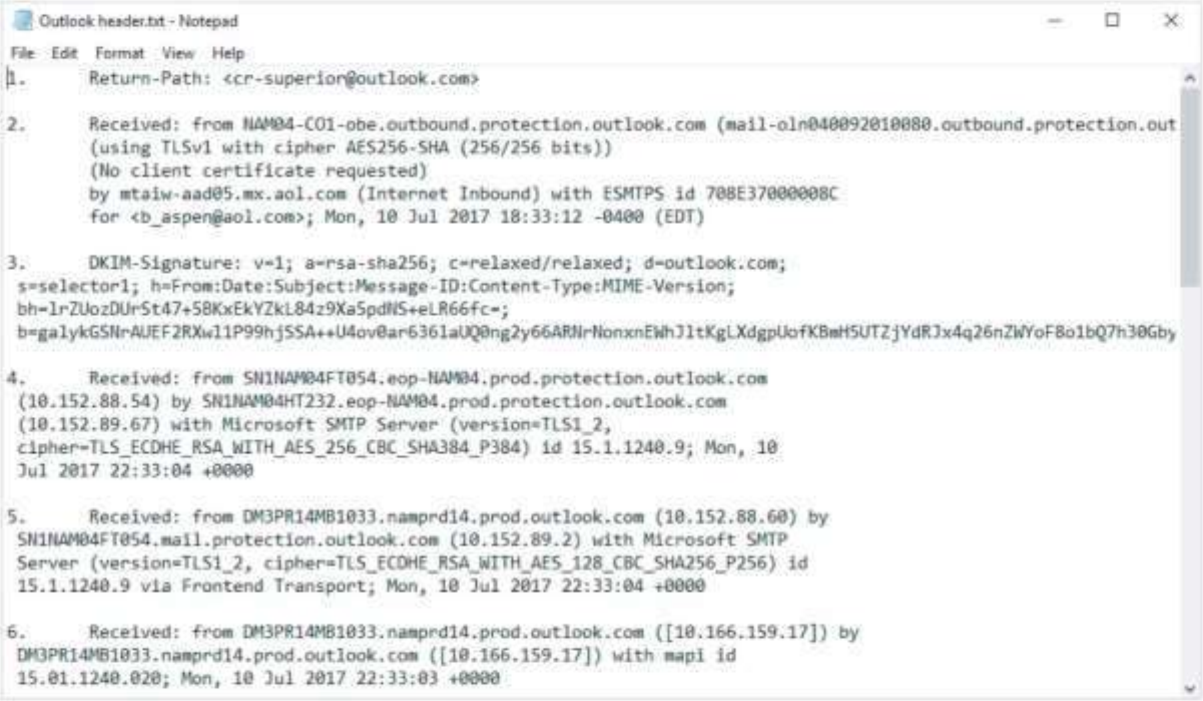
Source: Yahoo! Inc., *www.yahoo.com*

# Examining E-mail Headers (1 of 2)

Headers contain useful information

- The main 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 (2 of 2)



```
1.      Return-Path: <cr-superior@outlook.com>

2.      Received: from NAM04-CO1-obe.outbound.protection.outlook.com (mail-oln040092010080.outbound.protection.out
        (using TLSv1 with cipher AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mtaiw-aad05.mx.aol.com (Internet Inbound) with ESMTPS id 708E37000008C
        for <b_aspen@aol.com>; Mon, 10 Jul 2017 18:33:12 -0400 (EDT)

3.      DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=outlook.com;
 s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
 bh=lrZUozDUrSt47+58KxEkYZkL84z9Xa5pdNS+eLR66fc=;
 b=galykGSNrAUEF2RXwl1P99hjSSA++U4ov0ar6361aUQ0ng2y66ARNrNonxnEWhJ1tKgLXdgpUofKBmH5UTZjYdRJx4q26nZWYoF8o1bQ7h30Gby

4.      Received: from SN1NAM04FT054.eop-NAM04.prod.protection.outlook.com
 (10.152.88.54) by SN1NAM04HT232.eop-NAM04.prod.protection.outlook.com
 (10.152.89.67) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1240.9; Mon, 10
 Jul 2017 22:33:04 +0000

5.      Received: from DM3PR14MB1033.namprd14.prod.outlook.com (10.152.88.60) by
 SN1NAM04FT054.mail.protection.outlook.com (10.152.89.2) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1240.9 via Frontend Transport; Mon, 10 Jul 2017 22:33:04 +0000

6.      Received: from DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) by
 DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) with mapi id
 15.01.1240.020; Mon, 10 Jul 2017 22:33:03 +0000
```

**Figure 11-4** 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, 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

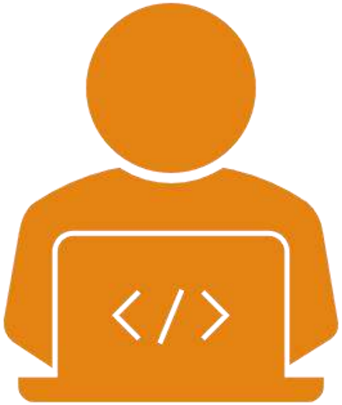
Determining message origin is referred to as "tracing"

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 (1 of 2)

Router logs

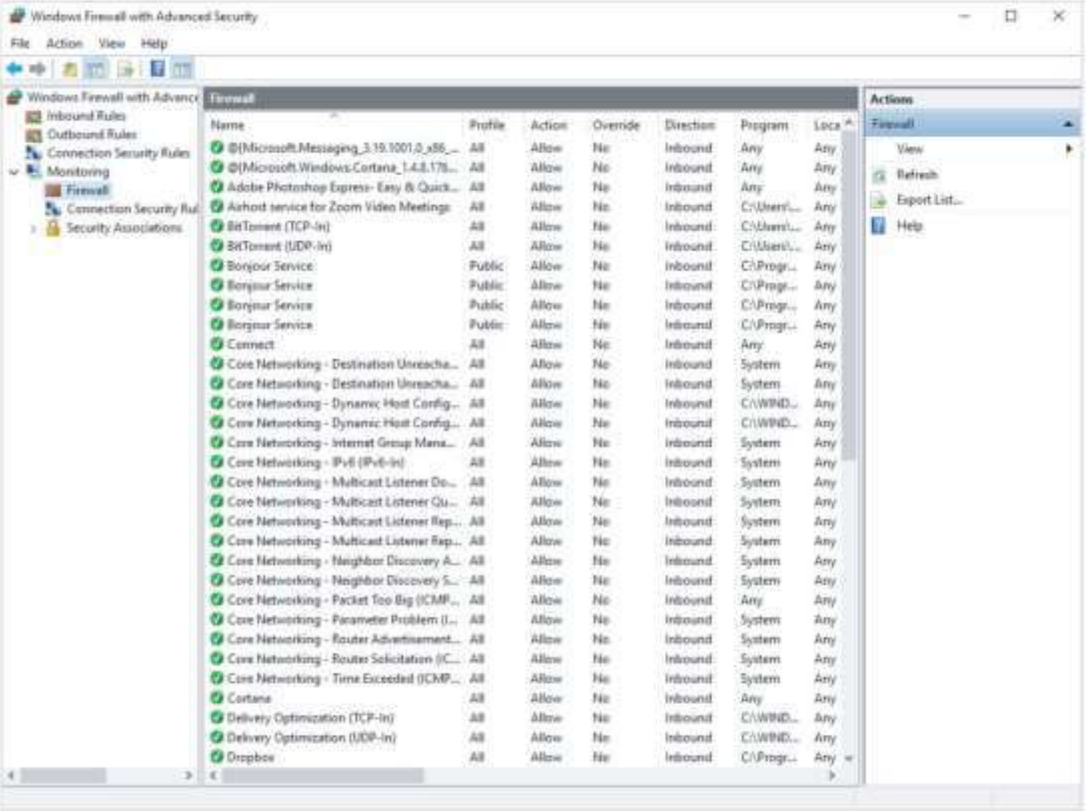
- Record all incoming and outgoing traffic
- Have rules to allow or disallow traffic
- You can resolve the path a transmitted e-mail has taken

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 (2 of 2)



| Name | Profile | Action | Override | Direction | Program | Loca |
|---|---|---|---|---|---|---|
| @{Microsoft.Messaging_3.19.1001.0_x86_... | All | Allow | No | Inbound | Any | Any |
| @{Microsoft.Windows.Cortana_1.4.8.176... | All | Allow | No | Inbound | Any | Any |
| Adobe Photoshop Express- Easy & Quick... | All | Allow | No | Inbound | Any | Any |
| Airhost service for Zoom Video Meetings | All | Allow | No | Inbound | C:\Users\... | Any |
| BitTorrent (TCP-In) | All | Allow | No | Inbound | C:\Users\... | Any |
| BitTorrent (UDP-In) | All | Allow | No | Inbound | C:\Users\... | Any |
| Bonjour Service | Public | Allow | No | Inbound | C:\Progr... | Any |
| Bonjour Service | Public | Allow | No | Inbound | C:\Progr... | Any |
| Bonjour Service | Public | Allow | No | Inbound | C:\Progr... | Any |
| Bonjour Service | Public | Allow | No | Inbound | C:\Progr... | Any |
| Connect | All | Allow | No | Inbound | Any | Any |
| Core Networking - Destination Unreacha... | All | Allow | No | Inbound | System | Any |
| Core Networking - Destination Unreacha... | All | Allow | No | Inbound | System | Any |
| Core Networking - Dynamic Host Config... | All | Allow | No | Inbound | C:\WIND... | Any |
| Core Networking - Dynamic Host Config... | All | Allow | No | Inbound | C:\WIND... | Any |
| Core Networking - Internet Group Mana... | All | Allow | No | Inbound | System | Any |
| Core Networking - IPv6 (IPv6-In) | All | Allow | No | Inbound | System | Any |
| Core Networking - Multicast Listener Do... | All | Allow | No | Inbound | System | Any |
| Core Networking - Multicast Listener Qu... | All | Allow | No | Inbound | System | Any |
| Core Networking - Multicast Listener Rep... | All | Allow | No | Inbound | System | Any |
| Core Networking - Multicast Listener Rep... | All | Allow | No | Inbound | System | Any |
| Core Networking - Neighbor Discovery A... | All | Allow | No | Inbound | System | Any |
| Core Networking - Neighbor Discovery S... | All | Allow | No | Inbound | System | Any |
| Core Networking - Packet Too Big (ICMP... | All | Allow | No | Inbound | Any | Any |
| Core Networking - Parameter Problem (I... | All | Allow | No | Inbound | System | Any |
| Core Networking - Router Advertisement... | All | Allow | No | Inbound | System | Any |
| Core Networking - Router Solicitation (IC... | All | Allow | No | Inbound | System | Any |
| Core Networking - Time Exceeded (ICMP... | All | Allow | No | Inbound | System | Any |
| Cortana | All | Allow | No | Inbound | Any | Any |
| Delivery Optimization (TCP-In) | All | Allow | No | Inbound | C:\WIND... | Any |
| Delivery Optimization (UDP-In) | All | Allow | No | Inbound | C:\WIND... | Any |
| Dropbox | All | Allow | No | Inbound | C:\Progr... | Any |

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

# Understanding E-mail Servers (1 of 2)

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 (2 of 2)

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 Microsoft E-mail Server Logs (1 of 4)

Microsoft Exchange Server (Exchange)

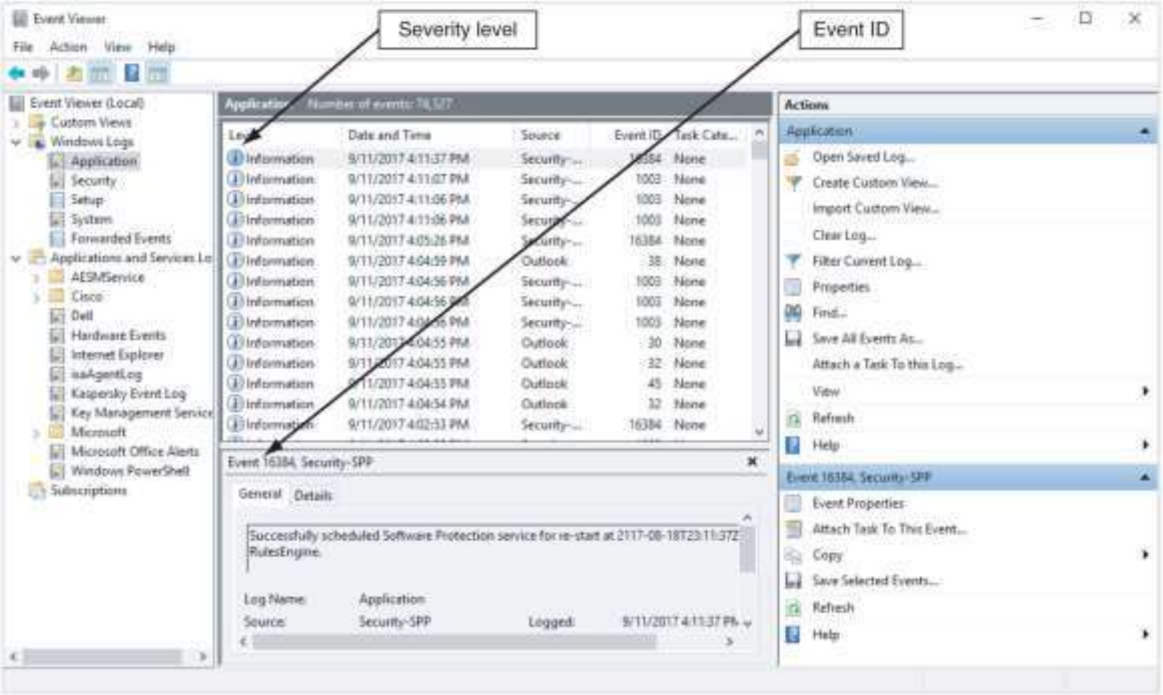
- Uses a database
- Based on Microsoft Extensible Storage Engine (ESE)

Most useful files in an investigation:

- .edb database files, checkpoint files, and temporary files

Information Store files

- Database files *.edb
  - Responsible for **MAPI** information



Severity level

Event ID

Application Number of events: 78,527

| Level | Date and Time | Source | Event ID | Task Cate... |
|---|---|---|---|---|
| Information | 9/11/2017 4:11:37 PM | Security-... | 16384 | None |
| Information | 9/11/2017 4:11:07 PM | Security-... | 1003 | None |
| Information | 9/11/2017 4:11:06 PM | Security-... | 1003 | None |
| Information | 9/11/2017 4:11:06 PM | Security-... | 1003 | None |
| Information | 9/11/2017 4:05:26 PM | Security-... | 16384 | None |
| Information | 9/11/2017 4:04:59 PM | Outlook | 38 | None |
| Information | 9/11/2017 4:04:56 PM | Security-... | 1003 | None |
| Information | 9/11/2017 4:04:56 PM | Security-... | 1003 | None |
| Information | 9/11/2017 4:04:56 PM | Security-... | 1003 | None |
| Information | 9/11/2017 4:04:55 PM | Outlook | 30 | None |
| Information | 9/11/2017 4:04:55 PM | Outlook | 32 | None |
| Information | 9/11/2017 4:04:55 PM | Outlook | 45 | None |
| Information | 9/11/2017 4:04:54 PM | Outlook | 32 | None |
| Information | 9/11/2017 4:02:53 PM | Security-... | 16384 | None |

Event 16384, Security-SPP

General Details

Successfully scheduled Software Protection service for re-start at 2117-08-18T23:11:37Z. RulesEngine.

Log Name: Application
Source: Security-SPP Logged: 9/11/2017 4:11:37 PM

**Figure 11-6** Viewing a log in Event Viewer

# Examining Microsoft E-mail Server Logs (4 of 4)

# Using Specialized E-mail Forensics Tools (2 of 3)

Tools (continued)

- MXToolBox for decoding e-mail headers
- FreeViewer with free tools for various servers

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 (3 of 3)

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

# Recovering Outlook Files (1 of 2)

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

# 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 Communications (1 of 2)

**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 Communications (2 of 2)

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

# Social Media Forensics on Mobile Devices

Mobile devices

- Majority of social network clients

Evidence artifacts vary depending on the social media channel and the device

iPhone and Android devices

- Yielded the most information, and much of the data was stored in SQLite databases

# 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