Network Forensics

E-mail Tracing & Investigations

Prof. Zaheed Shaikh Department of Computer Engineering

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 email by dragging it to a storage medium
 - Or by saving it in a different location

Examining E-mail Messages (continued)

- 1⁰ X Security - Microsoft Outlook ype a question for he is Elle Edit View Go Icols Actions Help Silvere - 🖓 😳 🗙 Galleply, Gilleply to All, Gallepoyard, 🖽 R Send/Receive - B III Search address bodys - @ -Mail Security Academynetspace.com Launches: Come Join the Celebration! -52 **Eavorite** Folders Academy Connection (webmaster@cisco.netacad.net) p ್ Sent: Men \$245,2906 1:12 PM Ci Islee lick here to enable instant Search Philos Anela D Unread Mol ģ Arsanged By Dalle Newest on top. E3 Settlers Bar Deleted Items (1) As we embark on our 10th year, we are celebrating our successes and 🖻 Older 🔫 13 Date designing student-focused programs that will stimulate participation and Academy Connection 52/27/2806 excitement segarding the Cisco Networking Academy Program. We Mail Folders Global Support Derk Language Drp., have chosen to provide a special place, a Website, for all of us to interact Academy Connection 12/07/2906 A Mai Items together, build relationships, and have fun. I am pleased to announce the Packet Traxer 4.81 is Now Anailable 🗃 🐯 Personal Folders 🖷 launch of the first phase of this Website. Sit The VMvisre Team 12/22/2806 Deleted Items WMware Workstation 6JE Deta The launch includes ways to acknowledge and celebrate participation in CB Drafts Academy Connection 12/35/3806 the program over the past 10 years: in [2] Mass Introducing the New COVA Curricals Basiness (2) Academy Connection 52/28/2006 Personal Holiday Schedule For Clasp Network Points of Light Security (1). Arademy Connection 12/18/2006 Junk E-mail Academyneta pase xom Launcher: C. Noton Antilips Azadewy Connection 8,95,2906 Curriculum Emails Updated 🔯 Outbax 🔯 Academy Connection 8:58:0906 (i) ESS Feeds Networking Academy Program Infra... Spotlighting Academy locations around the world TM-R Calendar Recognizing the breadth and depth of Academy participation Contacts / Talo . Ca 21 . N.F.B.

Messages in the selected folder are displayed here

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

- 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

Message Opti	ons ?X
Message settings	Security
Importance	: Normal
Sensitivit <u>v</u> :	Normal V Add digtal ggnature to outgoing message Request S/MIME receipt for this message
Tracking options	
Request a	delivery receipt for this message
Delivery options	gead receipt for this message
- Have realize a	and for
	en in
Expires an	ter: None V 12:00 AM V
⊆ontacts	
Categories 🔻	None
·	
Internet headers:	Return-path: <webmaster@cisco.netacad.net></webmaster@cisco.netacad.net>
	Envelope-to: aphilipsippolytechnic.edu.na Delivery-date: Mon, 18 Dec 2006 23:12:24 +0200
	Received: from localhost.polytechnic.edu.na ([127.0.0.1]:41809
	by mail.polytechnic.edu.na with esmtp (Exim 4.60)
	(envelope-from <webmaster@cisco.netacad.net>)</webmaster@cisco.netacad.net>
	Close

Figure 12-3 An Outlook e-mail header

Welcome to Outlook Express 6
General Details
Internet headers for this message:
From: "Microsoft Outlook Express Team" <msoe@microsoft.cor 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:</msoe@microsoft.cor
charset="iso-8859-1" Content-Transfer-Encoding: guoted-printable
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.110
Message Source
OK Cancel



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="1so-8859-1" Content-Transfer-Encoding: guoted-printable X-MimeOLE: Produced By Nicrosoft NimeOLE V6.00.2800.1106 <HTML> <HEAD> <META HTTP-EQUIV=3D"Content-Type" CONTENT=3D"text/html; =</pre> charset=3Dwindows-1252"> <STYLE> font{font-femily:"Verdana";font-size:Spt;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:#CCCCCC;width:140px;height:18px} .featuresText{font-family:Verdana;font-size;Bot;color;#000000} .headerCellLine(background-color:#CCCCCC;width:246px;height:1px) .messagesCell{font-family:"Verdana";font-size:Spt;color:#000000) .defaultA{color:#000000;cursor:hand} .blackBar{font-family:"Verdana";font-size:Bpt;color:#FFFFFF;font-weight:b= 01d} .bottomText{font-family: Verdana; font-size:7pt; color: #AAAAAA} .headerLinks{font-family:"Verdana";font-size:Bpt;color:#000000} .signatureText{font-family:"Verdana":font-size:Spt;font-weight:bold;color= :#000000} A:hover.toggleStyle(color:#FFFFFF) A:visited.toggleStyle{color:#CCCCCC}

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

- 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

		Fwd: Pr	oject pla	an for new	w factory	/		
Eile Edit	⊻iew <u>M</u> e	ssage						
Reply	Reply to All	Forward	🖨 Print) Delete) Junk	Not Junk	■ Previous	Next
Received SMTPSVC Mime-Ve To: <u>mart</u> Message	d: from [192 2(6.0.3790.1 ersion: 1.0 (A tha.dax@sup e-Id: <45dbe	.168.1.106] ([830); Wed, 14 pple Message periorbicycles d9449580929	24.18.24. Feb 200 framewo <u>biz</u> 1ce17100	250]) by m 7 20:12:39 ork v624) cf75faea2@	all.vividro -0600 Superiori	ound.com wi	th Microsoft	4
Content- From: Ji Subject	Type: multip im Shu < <u>jim.</u> :: Fwd: Projec	art/alternative shu@superior ct plan for nev	; bounda bicycles v factory	ry=Apple-M <u>biz</u> >	lail-1753	60152		
Date: W X-Mailer: Return-P	/ed, 14 Feb 2 : Apple Mail (ath: iim.shu(2007 20:12:48 2.624) @superiorbicy	ر) 0600 cles.biz	18:12 PST)				
X-Origin X-Evoluti	X-Evolution-Source: pop://martha.dax@mail.superiorbicycles.biz/							6]
Martha, Jim	do you hav	e any ideas yo	ou'd like t	o input on t	his before	Nau contac	ts the minist	ter?
Begin fo	orwarded me	essage:						
Fr Da	om: "Sam (ate: Februar	Clemens" <sar y 12, 2007 12</sar 	n.clemer :13:42 Al	ns@superio M CST	rbicycles	biz>		

Figure 12-6 An Evolution e-mail header

🔤 Telnet 168.	156.125.36	- 🗆 ×
PINE 4.21	MAIN MENU	Folder: INBOX No Messages 🔺
?	HELP	- Get help using Pine
с	COMPOSE MESSAGE	 Compose and send a message
I	MESSAGE INDEX	- View messages in current folder
L	FOLDER LIST	 Select a folder to view
Ĥ	ADDRESS BOOK	- Update address book
S	SEIUP	 Configure Pine Options
Q	QUIT	- Leave the Pine program
Copyright	1989-1999. PINE 14	a trademark of the University of Washington.
2 Help O OTHER CMDS	E Pro ListFldrs] New	vGnd R RelNotes ctCnd K KBLock

Figure 12-7 E-mail options in Pine



Figure 12-8 An e-mail header in Pine



Figure 12-9 Printing an e-mail in AOL

• 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

0.0.0	1		Fw: Roard meeting needs	0
0 Deitte	Rafy Party All	-	ê	
Content	From Subject Date To Cc Received Received Received Missage-ID Missage-ID Missage-ID Missage-ID Missage-ID	Denise Per Bo Februs Jim Shi, criatthi tom sin samms from all off.vini qimshi hom ce jaliwith 4002c0 1.0 textplai 7bit	Robinson and meeting needs ty 14. 2007 8:29:35 PM CST adaxiii superiorbicycle s.biz> rp-siP-01. invidround.com (; 199. 249. 324. 252) by mail. Vividround.com with Microsoft VC(56. 3:700. 1630); Wed, 14 Piels 2007 20:05:18 -0000 withc16.comcaut.net(().invitine16.comcaut.net(206.18.177.56)) by umb-sit dound.com (8.12.1.1.8.12.11) with ESN/TP id 11F2/02000/028130 for withc16.comcaut.net(().invitine16.comcaut.net(206.18.177.56)) by umb-sit dound.com (8.12.1.1.8.12.11) with ESN/TP id 11F2/02000/028130 for without (). 24-18-24.250.261.rm.comcaut.net(24.18.24.256)) by comcast.net e(5) with SM/TP id -2007/021532274361600/ba3e0/av; Thu, 15 Feb 2007 02:28107.+0000 1cT 10a8530794ee056901a8c0/il/cemcomputer> in; chanset=fiso-8859-1*	
×o	X-Priority X-Ban all-Priority X-Brian com X-Eprism Trap X-Equard-Score X-Econnod-By Relam-Path riginalorrivaltime	3 Normal Microso Produc Default 0.5 B aPrian denise. 15 Feb	A Outlook Express 5.00.2615.200 et By Microsoft MimeOLE V5.00.2615.300 Trap 2, TLD email Mining appliance on 199.349.204.252 pbinson/Esuperiorbicydes.bjz 2007 02:05:18.0203 (UTC) FILETIME=[EE588080011C756446]	
Jin, Tol ne wit Denisa	at is needed and !	li got star	ed en it.	1.1

Figure 12-10 An Apple Mail e-mail header

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



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: <Samspade@myway.com>
Delivered To: jim.shu8superiorbicycles.bit

    Received (amail 12780 invoked by uid 0); 12 Dec 2010 08:23:37 -

   0000

    Received from unknown (HELO suppriorbicycles.biz)

   (192.152.64.20) by mail.superiorbicycles.biz with SMTP; 12 Dec
   2010 08:23:37 -0000
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 SHTP id
         dBC81LJJ005229
         for <jim.shu@superiorbicycles.biz>; Sun 12 Dec 2010
         00:18:21 -0800

    Message-ID: <20101212082330.40429.gmail@web4009.mail0.myway.comb</li>

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 |
   MIME-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)

🖹 E:\Program Files'\WatchGu	rd'ilags 10.0.1.2-2103-02-10-19-51-43.wgl - LogViewer	1 <u>×</u> 1
Elle Edit Yom Help		
	8 0 8	
tination S. Port	D. Port Details	
deny out eth1	218 extp 20 128 169.254.19.156 169.254.255.255 138 13	8
deny out eth1	96 extp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	96 amtp 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 ethi	96 matp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	96 matp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	96 matp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	96 satp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	96 extp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	206 omtp 20 128 169.254.19.156 169.254.255.255 138 13	8
deny out eth1	206 amtp 20 128 169.254.19.156 169.254.255.255 138 13	8
deny out eth1	236 gatp 20 128 169.254.19.156 169.254.255.255 138 13	8
deny out eth1	78 matp 20 128 169.254.19.156 169.254.255.255 137 137	_
deny out eth1	78 satp 20 128 169.254.19.156 169.254.255.255 137 137	
deny out eth1	78 shtp 20 128 169.254.19.156 169.254.255.255 137 137	
deer out ath1	78 outo 20 128 169 264 19 166 169 264 265 266 187 187	التر.
Log file is loaded.	Total Lines: 83 At entry 56: 67% into file.	B

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	CMT
10.0.1.205 pegasus.superiorbicycl	.es.biz	PEGAEUS	10.0.1.205
Jim.shu@superiorbicycles.bix 1019 5.2.0.9.0.20101016072308.00x543 449peg 407 1 2010-10-16 09:44:22 4	sus.superiorbicyc MT	les.biz Ö	ō

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 energency 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: "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

- 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

- 2	00212	216.lag ·	Notepad											×I
Ele .	Edit	Format	Help											
P 14	essa	ge Tra	ackting	Log F1	lei≉ ⊑	echang	le SAs.	tem A	.tt en	dant	Vens	:tan	l l	-
6.0	. 441	7.0D#	Date"	Г Т	ine	clief	it−1p		C11	ent -	hostr	hante	- 1	1
Pari	ther	-Name	ser	ver –ho	stname	serve	er−1Þ		Rec	1p1e	nt - Ac	idness		
EVB	nt-I	D	MSG	ID P	riorit	y .	R.e	cipie	nt – R	epor:	t-sta	tus		ш,
LOT.	al-b	ytes	NUT	ber-Re	cip1er	its –	Of	igina	tion	-T în	e			
Enc	rypt	lon	ser	v1ce-v	eris 1 on	i ∟1nke	rd-MSG	IŐ	Mes	sage	-Subj	ect		
Sen	der-	Addre	55000,2D	05-12-	16	17:8:	30 GM	Г	-		-	-		
PEG	ASUS	-	/0=	ZOIKES	/OU=FI	RST_A0	MINIS	TRATI	VE					
GRO	UP/C	N-REC	IPIENTS	/CN-Ja	nedoe	1027								
11A	0009	@C6BC	774 BAOB	32AE93	2D5B3E	02E496	Ppega si	us.my	'comp	any.	com	0		
P		1320	1	2	005-12	-16 17	18:30	GMT	0	_	-			
c-u	s;a-	;p=20	DIKES;]	-PEGAS	US-021	216170	8282-	1	one	for	the	books		
EX1,	/0=z	OIKES/	/OU-FIR	ST ADM	INISTR	ATIVE								
GRO	UP/C	N=REC	EPIENTS	/CN=ADI	MINIST	RATOR	- 0	2005	-12-3	16	17:3	8:31 G	MT	
I		-	-	P	EGASUS	-	/0	=ZOIK	ES/O	U=FI	RST			
ADM	INIS	TRATI	VE GROU	P/CN=R	ECIPIE	INTS/CK	l=Jane	doe	101	9				
11A	0009	8C68C	774 BAOB	32AE93	2D5B3E	028496	*pega si	us.my	comp	any.	com	0		
0	~	1320	. 1	2	005-12	-16 17	:8:30	GMT	0		-	-		
One	tor	the	books	-		-0020	05-12	-16	17:	B:31	GMT	-		
L		-	PEG	ASUS -		Z0	MKES/	OU=FI	RST .	ADPII	NISTR	ATIVE (ATIVE		
GRO	UP/C	N=REC	IPIENTS	/CN=Ja	nedbe	1025								
114	0009	8C68C	774 BAOB	32AE93	2D 5 B 3E	026498	*pegas	us.my	comp	any.	com	0		
<u>р</u>	-	1320	1	2	005-12	-16 17	18:30	QMT	0		-	-		
one	TOP	the i	books	-		-0020	05-12	-16	17:	8:31	GMT			
-		-	PEG	ASUS -		20=20	NIKES/	0U=FI	RST .	ad e i I	NISTR	OUTIVE (NTINE		
GRO	UP/C	N=REC	IPIENTS	/CN=Ja	nedbe	1074								
114	0003	9C68C	774 BAOB	32AE93	205836	02E4.96	*pega s	us.ny	comp	any.	COM	0		
L														•

Figure 12-18 A message tracking log in verbose mode

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



Figure 12-19 Viewing a log in Event Viewer

ivent Prope	rties			? ×
Event				
Date: Time: Type: User: Compute:	3/31/2005 8:20 Information 2022 PEGASUS	Source: Category Event ID:	MSExchangelS Maibox MTA Connections 2010	+ + 100
About to a PEGASU	n Hart m/_waik o S]'.	n database	'First Storage Group/Mailbo	a Store
For more i	nformation, el	ick <u>http://w</u>	ww.microsoft.com/contentre	direct.acp.
Dete P	Balla C W	ads		
				-
		1	K Cancel	Apply .

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)

Outlook Express	Nene IEI Out mice	3.sho	Oute	See Mal	ed Bate	11.45
300000	4			Comp. Helen	and the second	11.00
	Recover t-modifie	-	1 martine		-	<u>×</u>
	Found Message Lief		Select Message	Allvering	n 1	3
	han	Subject		File Sale	E un	
	Jave Dive	leave are alone		274		- 11
	Jare Date	Intructive dane		296		
	Jave-God	Galicita		355		
	Jane Doe	:1620		256		
	Jave Oos			249		
	admentiale	texting		290		
	-odiminational	(Child		200		
	-edimentator			220		
	-conversion and	-		104		
		0.00		(2.5)		1
	at .					

Figure 12-21 E-mail search results in FINALeMAIL

Using Specialized E-mail Forensics Tools (continued)

From:	Jane Doe		
Date:		an that the	
Subject:	leave me alone	وتقندا المتقاد	
Attached Fil		Attach File Say	e.
k	save me alone		-
			22
I			
			TIE
Prev	Next	Cancel	5

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)

KFF Library Error
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.
OK Cancel

AccessData FTK	X
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.	
ОК	

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

Using AccessData FTK to Recover E-mail (continued)

phics Empha
000200000000000000000000000000000000000
ystem)
file data)
plications, etc
tables
es
Known
wn



Using AccessData FTK to Recover E-mail (continued)





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

E	9	5	9	ę	3	3		4	; C	h	CB.	83	1	6	20		89.4	n n	2	4B		_	_	_	• fi
1	۱ ę	1	Q	6	泊	1	¥,	4	9	8	0	hi		@ I		ASC	1) (i N	1.4	1	н	
=	~	• •	<<	×	> :	\$\$	ž	2.4	2	>3	. ^			8	+/-	+ -	• *	1	%	[>] [·	<] _2	Ag .	4		
-	_	-	-	-		0		1	2	2	3	Γ	4	5	6	7	8	9	A	В	C	D	Ε	F	0123456789ABCDEF
10	07	11	JΕ	0	2	20	0	A	33	Е	20	4	Ð	61	72	74	68	61	0A	3E	20	0A	0A	46	.> Mørtha.>
	07	11)F	Û	-7	2	б	F	61	D.	20	- 7	4	б5	72	72	7.9	73	61	- 64	-6C	65	72	40	rom terrysadler@
	07	11	10	0	ŧ	17	6	F	61	P.	77	- 7	19	2E	63	-6F	6D	20	53	61	-74	20	46	65	goowy.com Sat Fe
10	07	11	11	0	5	2	2	D	З	1	37	ā	20	31	35	ЗA	31	35	ЗA	34	35	20	32	30	b 17 15:15:45 20
10	07	11	12	0	3	0	З	7	02	Α.	52	6	5	63	65	69	76	65	64	- 3A	20	66	72	6 F	07.Received: fro
	07	11	13	0	8	Ð	2	0	7	3	6D	-7	4	70	2 D	73	68	74	2D	30	31	2E	76	69	m smtp-sjt-01.vi
0	07	11	14	0	-7	6	6	9	6	ŧ.	72	Ē	F	75	6 E	64	2E	63	6F	6D	20	28	5B	31	vidround.com ([1
0	07	11	15	Ö	1	9	3	19	21	Ε	32	1	14	39	2E	32	32	34	2E	32	35	32	SD	29	99.249.224.252])
	07	11	16	0	1	0	6	2	71	9	ΟÀ	. (9	бD	61	69	-6C	28	76	69	76	69	64	72	bymail.vividr
10	07	11	17	0	6	Ŧ	7	5	63	Ε	64	2	E.	63	6 F	6D	20	77	69	74	68	20	4D	69	ound.com with Mi
0	07	11	18	0	8	Ε (7	2	63	F	73	6	F	66	-74	20	53	4D	54	50	53	56	43	28	crosoft SMTPSVC(
0	07	11	19	0	1	6	2	Е	31	0	2E	2	E (37	39	30	-2E	31	38	33	30	29	ЗB	20	6.0.3790.1830);
D	07	11	ιà	Ö	5	E	6	1	7	4	2C	- 2	20	31	37	20	4.6	65	62	20	32	30	30	37	Sat, 17 Feb 2007
	07	11	18	Ö	1	۱Å,	Ū	9	3	1	35	1	à.	31	35	ЗÀ	34	35	20	2D	30	36	30	30	15:15:45 -0600
10	07	11	1C	0	1	IA.	5	Ζ	6	5	63	6	5	69	76	65	64	ЗA	20	66	72	6F	6D	2 O	.Received: from
0	07	11	1D	0	7	Έ.	6	D	7	4	70	- 2	11	2E	67	6F	-6F	77	79	2E	63	6F	6 D	20	smtpl.goowy.con
	07	11	1E	0	12	38	7	3	61	D	74	- 7	10	31	2E	67	6F	6F	77	79	2E	63	6F	6 D	(emtp1.goowy.com
10	07	11	1F	0	-2	20	5	в	33	2	30	1	9	2E	31	32	36	2E	32	- 34	37	2E	32	30	[209.126.247.20
	07	17	20	0	3	35	5	D	2	9	20	E	Z	79	0.A	09	73	61	74	70	ZD	73	6A	74	5]) bysmtp-sjt
	07	17	21	0	2	D	З	0	3.	1	2E	-7	6	69	76	69	64	72	6F	75	6E	64	2E	63	-D1.vividround.c
	07	17	22	0	1	Ŧ	6	D	21	0	28	13	88	2E	31	32	2E	31	31	2F	38	2E	31	32	om (8.12.11/8.12
10	07	12	23	0	2	Ξ	3	1	3.	1	29	2	20	77	69	74	68	20	45	53	4D	54	50	20	.11) with ESMTP
à	Tart	18-	evi	sl																					
1	itruc	tu	ies								-	2	1	F I B	0 🗄	t@	-	-B	* c	heck	sum Re	sults		N	one - 🕺 🗶 🖉 🕽
ſ	Mer	mb	er	5)				Va	lue	(de	c)	P		/alue	(hec)	1		9	Docu	ment		Algo	rithm	Checksum 🗐 Cl
ľ																									
l																		- 11							
l																		- 11							
																		- 11	4	£	_	1.44		.00	AA
ł	4							_	_			_	_		_	_	_	P	la l	120	ompara	K	Check	sun	The Find I Bookm (E) Output

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

3 File Eant 3 중 급 은	93 1	opti	(Pa	1008	63. G	(h000	20	i j	84	n n	2	¢Β					- (P Q	88	30	2
》 18 18 (18 N	Z 🕸	3	()		6		ASCI				٣	E H	-	P 1	IH				
≒ ~ ≪ ≫	25	23	<u>×</u> ×	A		8	+/- •	+ -	• *	1	%	>] [<	l all	AN R	4					
	0	1	2	3	4	5	6	7	8	- 9	A	В	C	D	Ε	F	012345	6789A	BCDE	
0071FB0	6E	69	71	75	65	20	61	6E	64	3D	0A	20	73	75	63	63	nique	ands.	succ	1
0071FC0	65	73		56		- 6C		6F		66		72		20		2F	essful fortivi	offe:	r. (/	
0071FE0	74	20		61		30		10		30		35		64		5E 5E	tont/<	- 30 ° V.	2510B Ardan	
0071FE0	61	22		73		78		3D		44		32		9년 기반		215	e race a" siz	e=30";	989400 28577	
0072000	6.6	6F		3D		74		30		70		30		ЗE		66	font	>	(p) (f	
0072010	67	6E		20		61		65		33		22		65		64	ont fa	ce=3D	Verd	
0072020	61	6E		22		73		7λ		ЗD		-44		32		3E	ana" s	ize-31	D"2")	
0072030	3C	61		68		65		ЗD		-44		68		74		ЗA	<a hre<="" td=""><td>£=30"1</td><td>http:</td><td></td>	£=30"1	http:	
0072040	ZF	ZF		77		ZE		75		65		69		зр		72	//www.	super	ior	
0072050	62	69		79	63	6C	65	73		62	69	7A		3E	77	77	bicycl	es.bi:	Z">WW	
0072060	77	2E		25		05		69		72		69		79		6C	w.supe	riorb:	1cycl	
0072070	74	38		20		28		20		36		30		25		30	e≘.D12 ±\//n\	syaa Antoh	(/:ON w /\/	
0072090	27	70		30		53		30		41	41	38		28		6E	200228	$P = -2N^{2}$	S C / ho	
00720A0	64	79		зč		68		6D		ЗĒ		2F		6F	64	79	dv > Ch	$tnD \oplus$	body	
0072080	3E	ač.		68		61		3E		21		2D		20		3D	> <td>1></td> <td></td> <td></td>	1>		
0072DC0	5F	45		4E		SF		30		30		36		63		37	_EDNP_	0000_(6acd7	ł
00720D0	34	35		ZD		65		62		34		66		ZD		63	458-de	cb-4e;	f6-bc	
00720E0	38	63		64	34	37	38	38	65	30	39	30	31	39	62	ZD	8c-d <u>47</u>	88e09	019b-	
00720F0	20	0A	<u>A0</u>	DA	00	00	00	00	00	00	0.0	00	00	00	00	00	- · · · ·			
0072100	UU	00	00	00	UU	υu	00	00	00	0.0	00	00	UU	UU	00	00				÷
a martha-evol										_										
Structures				• 6	31	e e	0 ()	t@	4	-ā	î, c	hecks	um Re	sults		N	one	•	X 2	>
Member 🖄			Valu	e (dec) 1	1	/alue	(hec)	1		9	Docum	ient		Algo	ithm		Checksum	15	Ch
										-										
										- 11						-		_		
											4	Bin	maxe	197	Charle		thew i the	Barken	(E) netw	
*	-		-		-	-	-	-	-	P	2	-0-0	- designed and	- 75			and the second second		Constp	1

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)

Iterrysadler-martha-inbox - Notepad		3
File Edit Format View Help		
File Edit Format View Help From terrysadler@goowy.com Sat Feb 17 15:15:45 2007Received: from sit-01.vividround.com ([199.249.224.252]) by mail.vividround.c Microsoft SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007 15:15:45 Received: from smtpl.goowy.com (smtpl.goowy.com [209.126.247.205] smtp-sjt-01.vividround.com (8.12.11/8.12.11) with ESMTP id l1HLAG for <martha.dax@superiorbicycles.biz>; Sat, 17 Feb 2007 15:10:38 (CST)Received: (qmail 2864 invoked from network); 17 Feb 2007 21: 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. Spam-Checker-Version: SpamAssassin 3.1.2 (2006-05-25) on smtpl.go 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 smtpl.goowy.com (qmail=1dap=1.03) SMTP for <martha.dax@superiorbicycles.biz; 17="" 2007="" 21:<br="" feb="">0000goowy: id: : 520051From: terrysadler <terrysadler@goowy.com>7 terrysadler <terrysadler@goowy.com>To: martha.dax@superiorbicycle Date: Sat, 17 Feb 2007 21:15:44 GMTMessage=1D: <2af031584b5c460e95b36ddd6719529f@webserver002>subject: Investors version: 1.0x-Mailer: goowy mail = http://www.goowy.comPriority: =Priority: 3Content=Type: multipart/alternative; boundary=" =_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e0019b"x-ePrism=Trap: I TrapX-eGuard=Score: () 0.6 BIZ_TLD,HTML_50_60,HTML_MESSAGEX-Scann ePrism email filtering appliance on 199.249.224.252Return-Path: terrysadler@goowy.comX-originalArrivalTime: 17 Feb 2007 21:15:45. (UTC) FILETIME=[C90BFE80:01C75208]X-Evolution=Source: pop://martha.dax@mil.superiorbicycles.biz/x=evolution: 000001a- is_a multi-part message in MIME format=EDNP_0000_6acd7459</terrysadler@goowy.com></terrysadler@goowy.com></martha.dax@superiorbicycles.biz;></terrysadler@goowy.com></martha.dax@superiorbicycles.biz>	n smtp- com with -0600)) by cgD060105 -0600 :01:53 - .1.2X- powy.com) with 01:53 - Reply-To: es.biz sMIME- Normalx Default ned-By: .0640 -0010This 8-decb-	
4ef6-bc8c-d4788e09019bContent-Type: text/plain; charset="iso-8855 Content-Transfer-Encoding: quoted-printable-OAHello, -OA-OAAre y	9-1" ou	
size companies that have a proven track record= for making qualit	ty	

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]) bymail.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]) bysmtp-sjt-01.vividround.com (8.12.11/8.12.11) with ESMT id l1HLAcgD060105for <martha.dax@superiorbicycles.biz>; Feb 2007 15:10:38 -0600 (CST)</martha.dax@superiorbicycles.biz>	P Sat, 17 ^E
Received: (qmail 2864 invoked from network); 17 Feb 2007 21:01:53 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:	-0000
X-Spam-Checker-Version: SpamAssassin 3.1.2 (2006-05-25) on smtpl.g X-spam-Level: X-spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_TLD,HTML_50_60,HTML_MESSAGE autolearn=disa version=3.1.2	oowy.com bled
Received: from unknown (HELO webserver002) ([192.168.25.102]) (e -sender <terrysadler@goowy.com>) by smtpl.goowy.com (qmail-lda with SMTP for <martha.dax@superiorbicycles.biz>; 17 Feb 2007 21:01:53 -0000goowy: id: : 520051</martha.dax@superiorbicycles.biz></terrysadler@goowy.com>	nvelope p-1.03)
From: terrysadler <terrysadler@goowy.com>Reply-To: terrysadler <terrysadler@goowy.com></terrysadler@goowy.com></terrysadler@goowy.com>	
To: martha.dax@superiorbicycles.biz	
Date: Sat, 17 Feb 2007 21:15:44 GMTMessage-ID: <2af031584b5c460e95b36ddd6719529f@webserver002> Bubject: InvestorsMIME-Version: 1.0X-Mailer: goowy mail -	-





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