UNIT-4

CURRENT FORENSIC TOOLS

Types of Computer Forensics Tools

Computer forensics tools are divided into two major categories: hardware and software. Each category has additional subcategories discussed in more depth later in this chapter. The following sections outline basic features required and expected of most computer forensics tools.

Hardware Forensics Tools Hardware forensics tools range from simple, single purpose components to complete computer systems and servers. Single-purpose components can be devices, such as the ACARD AEC-7720WP Ultra Wide SCSI-to-IDE Bridge, which is designed to write-block an IDE drive connected to a SCSI cable.

Some examples of complete systems are Digital Intelligence F.R.E.D. systems, DIBS Advanced Forensic Workstations, and Forensic Computers ForensicExamination Stations and portable units.

Software Forensics Tools Software forensics tools are grouped into command-line applications and GUI applications. Some tools are specialized to perform one task, such as Safe Back, a command-line disk acquisition tool from New Technologies, Inc. (NTI). Other tools are designed to perform many different tasks. For example, Technology Pathways Pro- Discover, X-Ways Forensics, Guidance Software En Case, and Access Data FTK are GUI tools designed to perform most computer forensics acquisition and analysis functions.

Software forensics tools are commonly used to copy data from a suspect’s drive to an image file. Many GUI acquisition tools can read all structures in an image file as though the image were the original drive. Many analysis tools, such as ProDiscover, En Case, FTK, X-Ways Forensics, ILook, and others, have the capability to analyze image files. In Chapter 4, you learned how some of these tools are used to acquire data from suspects’ drives.

Tasks Performed by Computer Forensics Tools

All computer forensics tools, both hardware and software, perform specific functions. These functions are grouped into five major categories, each with sub functions for further refining data analysis and recovery:

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

In the following sections, you learn how these five functions and associated sub functions apply to computing investigations.

Acquisition, the first task in computer forensics investigations, is making a copy of the original drive. As described in Chapter 4, this procedure preserves the original drive to make sure it doesn’t become corrupt and damage the digital evidence. Sub functions in the acquisition category include the following:

- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote acquisition
- Verification

Some computer forensics software suites, such as Access Data FTK and En Case, provide separate tools for acquiring an image. However, some investigators opt to use hardware devices, such as the Logic be Talon, VOOM Hard Copy 3, or Image MASSter Solo III Forensic unit from Intelligent Computer Solutions, Inc., for acquiring an image. These hardware devices have their own built-in software for data acquisition. No other device or program is needed to make a duplicate drive; however, you still need forensics software to analyze the data.

Validation and Discrimination

Two issues in dealing with computer evidence are critical. First is ensuring the integrity of data being copied—the validation process. Second is the discrimination of data, which involves sorting and searching through all investigation data. The process of validating data is what allows discrimination of data. Many forensics software vendors offer three methods for discriminating data values. These are the sub functions of the validation and discrimination function:

- Hashing
- Filtering
- Analyzing file headers

Validating data is done by obtaining hash values. As a standard feature, most forensics tools and many disk editors have one or more types of data hashing. How data hashing is used depends on the investigation, but using a hashing algorithm on the entire suspect drive and all its files is a good idea. This method produces a unique hexadecimal value for data, used to make sure the original data hasn't changed.

This unique value has other potential uses. For example, in the corporate environment, you could create a known good hash value list of a fresh installation of an OS, all applications, and all known good images and documents (spreadsheets, text files, and so on). With this information, an investigator could ignore all files on this known good list and focus on other files on the disk that aren't on this list. This process is known as filtering. Filtering can also be used to find data for evidence in criminal investigations or to build a case for terminating an employee.

The primary purpose of data discrimination is to remove good data from suspicious data. Good data consists of known files, such as OS files and common programs (Microsoft Word, for example).

Several computer forensics programs can integrate known good file hash sets, such as the ones from the NSRL, and compare them to file hashes from a suspect drive to see whether they match. With this process, you can eliminate large amounts of data quickly so that you can focus your evidence analysis. You can also begin building your own hash sets.

Another feature to consider for hashing functions is hashing and comparing sectors of data. This feature is useful for identifying fragments of data in slack and free disk space that might be partially overwritten.

An additional method of discriminating data is analyzing and verifying header values for known file types. Similar to the hash values of known files, many computer forensics pro- grams include a list of common header values. With this information, you can see whether a file extension is incorre for the file type. Renaming file extensions is a common way to try to hide data, and you could miss pertinent data if you don’t check file headers.

Extraction

The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.

Recovering data is the first step in analyzing an investigation’s data. The following sub functions of extraction are used in investigations:

- Data viewing
- Keyword searching
- Decompressing
- Carving
- Decrypting
- Bookmarking

Many computer forensics tools include a data-viewing mechanism for digital evidence. How data is viewed depends on the tool. Tools such as ProDiscover, X-Ways Forensics, FTK, EnCase, SMART, ILook, and others offer several ways to view data, including logical drive structures, such as folders and files. These tools also display allocated file data and unallocated disk areas with special file and disk viewers. Being able to view this data in its normal form makes analyzing and collecting clues for the investigation easier

Computer Forensics Software Tools

Whether you use a suite of tools or a task-specific tool, you have the option of selecting one that enables you to analyze digital evidence through the command line or in a GUI. The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux.

Command-Line Forensics Tools

Computers used several OSs before MS-DOS dominated the market. During this time, computer forensics wasn’t a major concern. After people started using PCs, however, they figured out how to use them for illegal and destructive purposes and to commit crimes and civil infractions.

Software developers began releasing computer forensics tools to help private- and public-sector investigators examine PCs. The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems.

One of the first MS-DOS tools used for computer investigations was Norton Disk Edit. This tool used manual processes that required investigators to spend considerable time on a typical 500 MB drive. Eventually, programs designed for computer forensics were developed for DOS, Windows, Apple, NetWare, and UNIX systems. Some of these early programs could extract data from slack and free disk space; others were capable only of retrieving deleted files. Current programs are more robust and can search for specific words or characters, import a keyword list to search, calculate hash values, recover deleted items, conduct physical and logical analyses, and more.

One advantage of using command-line tools for an investigation is that they require few sys- tem resources because they're designed to run in minimal configurations. In fact, most tools fit on bootable media (floppy disk, USB drive, CD, or DVD). Conducting an initial inquiry or a complete investigation with bootable media can save time and effort. Most tools also produce a text report small enough to fit on a floppy disk.

Forensic Workstations

Many computer vendors offer a wide range of forensic workstations that you can tailor to meet your investigation needs. The more diverse your investigation environment, the more options you need. In general, forensic workstations can be divided into the following categories:

- *Stationary workstation*—A tower with several bays and many peripheral devices
- *Portable workstation*—A laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation
- *Lightweight workstation*—usually a laptop computer built into a carrying case with a small selection of peripheral options

When considering options to add to a basic workstation, keep in mind that PCs have limitations on how many peripherals they can handle. The more peripherals you add, the more potential problems you might have, especially if you're using an older version of Windows. You must learn to balance what you actually need with what your system can handle.

Validating and Testing Forensics Software

Now that you have selected some tools to use, you need to make sure the evidence you recover and analyze can be admitted in court. To do this, you must test and validate your software. The following sections discuss validation tools available at the time of this writing and how to develop your own validation protocols.

Using National Institute of Standards and Technology (NIST) Tools

The National Institute of Standards and Technology publishes articles, provides tools, and creates procedures for testing and validating computer forensics software. Software should be verified to improve evidence admissibility in judicial proceedings. NIST sponsors the Computer Forensics Tool Testing (CFTT) project to manage research on computer forensics tools.

- Establish categories for computer forensics tools—Group computer forensics software according to categories, such as forensics tools designed to retrieve and tracee-mail.
- Identify computer forensics category requirements—For each category, describe the technical features or functions a forensics tool must have.
- Develop test assertions—Based on the requirements, create tests that prove or diSprove the tool's capability to meet the requirements.
- Identify test cases—Find or create types of cases to investigate with the forensics tool, and identify information to retrieve from a sample drive or other media. For example, use the image of a closed case file created with a trusted forensics tool to test a new tool in the same category and see whether it produces the same results.
- Establish a test method—Considering the tool's purpose and design, specify how to test it.
- Report test results—Describe the test results in a report that complies with ISO 17025, which requires accurate, clear, unambiguous, and objective test reports.

Another standards document, ISO 5725, demands accuracy for all aspects of the testing pro- cess, so results must be repeatable and reproducible. –Repeatable results‖ means that if you work in the same lab on the same machine, you generate the same results. –Reproducible results‖ means that if you're in a different lab working on a different machine, the tool still retrieves the same information.

Exploring the Role of E-mail in Investigations

E-mail evidence has become an important part of many computing investigations, so computer forensics investigators must know how e-mail is processed to collect this essential evidence. In addition, 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.

As a computing investigator, you might be called on to examine a phishing e-mail to see whether it's authentic. Later, in –Tracing an E-mail Message,‖ you learn about resources for looking up e-mail and Web addresses to verify whether they're associated with a spoofed message.

One of the most noteworthy e-mail scams was 419, or the Nigerian Scam, which originated as a chain letter from Nigeria, Africa. Fraudsters now need only access to Internet e-mail to solicit victims, thus saving postage costs of international mail. Unlike newer, more sophisticated phishing e-mail frauds, 419 messages have certain characteristic ploys and a typicalwriting style. For example, the sender asks for access to your bank account so that he can transfer his money to it as a way to prevent corrupt government officials in his homeland from confiscating it. The sender often promises to reward you financially if you make a minor payment or allow access to your bank account. The messages are usually in uppercase letters and use poor grammar

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

You can send and receive e-mail in two environments: via the Internet or an intranet (an internal network). In both e-mail environments, messages are distributed from a central server to many connected client computers, a configuration called client/server architecture. The server runs an e-mail server program, such as Microsoft Exchange Server, Novell GroupWise, or UNIX Send mail, to provide e-mail services. Client computers use e-mail programs (also called e-mail clients), such as Novell Evolution or Microsoft Outlook, to contact the e-mail server and send and retrieve e-mail messages.

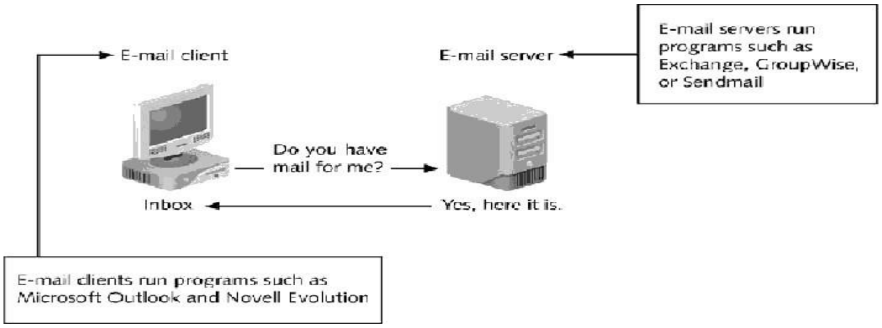

E-mail client
E-mail server
E-mail servers run programs such as Exchange, GroupWise, or Sendmail
Do you have mail for me?
Inbox
Yes, here it is.
E-mail clients run programs such as Microsoft Outlook and Novell Evolution

Fig: Role of client and server in E-mail

Regardless of the OS or e-mail program, users access their e-mail based on permissions the e-mail server administrator grants. These permissions prevent users from accessing each other's e-mail. To retrieve messages from the e-mail server, users identify themselves to the server, as when logging on to the network. Then e-mails are delivered to their computers.

E-mail services on both the Internet and an intranet use a client/server architecture, but they differ in how client accounts are assigned, used, and managed and in how users access their e-mail. Overall, an intranet e-mail system is for the private use of network users, and Internet e-mail systems are for public use. On an intranet, the e-mail server is generally part of the local network, and an administrator manages the server and its services. In most cases, an intranet e-mail system is specific to a company, used only by its employees, and regulated by its business practices, which usually include strict security and acceptable use policies. For example, network users can't create their own e-mail accounts, and usernames tend to follow a naming convention that the e-mail administrator determines.

Investigating E-mail Crimes and Violations

Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes. Your goal is to find out who's behind the crime or policy violation, collect the evidence, and present your findings to build a case for prosecution or arbitration.

E-mail crimes and violations depend on the city, state, and sometimes country in which the e-mail originated. For example, in Washington State, sending unsolicited e-mail is illegal. However, in other states, it isn't considered a crime. Consult with an attorney for your organization to determine what constitutes an e-mail crime.

Committing crimes with e-mail is becoming commonplace, and more investigators are finding communications that link suspects to a crime or policy violation through e-mail. For example, some people use e-mail when committing crimes such as narcotics trafficking, extortion, sexual harassment, stalking, fraud, child abductions, terrorism, child pornography, and so on. Because e-mail has become a major communication medium, any crime or policy violation can involve e-mail.

Examining E-mail Messages

After you have determined that a crime has been committed involving e-mail, first access the victim's computer to recover the evidence. Using the victim's e-mail client, find and copy any potential evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders. If you can't actually sit down at the victim's com- puter, you have to guide the victim on the phone to open and print a copy of an offending message, including the header. The header contains unique identifying numbers, such as the IP address of the server that sent the message. This information helps you trace the e-mail to the suspect.

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, depending on your organization's guidelines.

The following activity shows you how to use Outlook 2007, included with Microsoft Office, to copy an e-mail message to a USB drive. (*Note*: Depending on the Outlook version you use, the steps might vary slightly.) You use a similar procedure to copy messages in other e-mail programs, such as Outlook Express and Evolution. If Outlook or Outlook Express is installed on your computer, follow these steps:

- Insert a USB drive into a USB port.
- Open Windows Explorer or the Computer window, navigate to the USB drive, and leave this window open.
- Start Outlook by clicking Start, pointing to All Programs, pointing to Microsoft Office, and clicking Microsoft Office Outlook 2007.

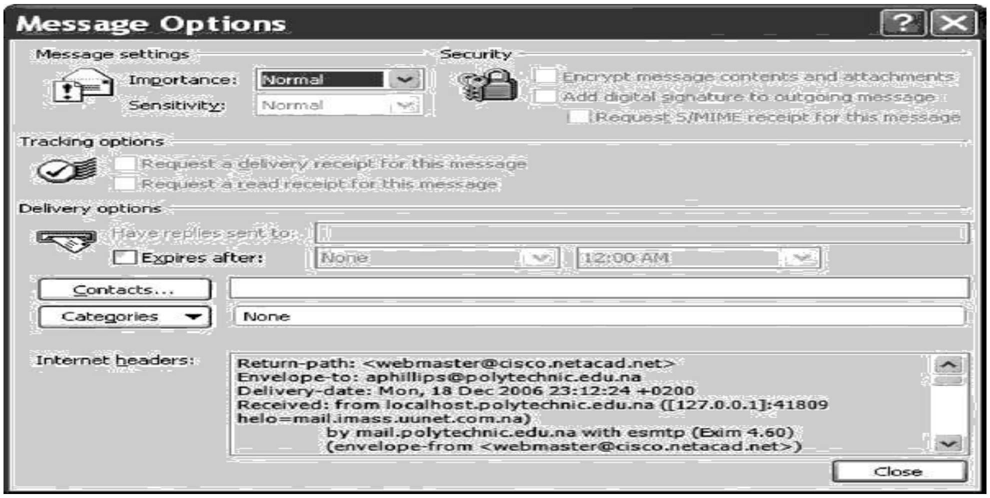
- In the Mail Folders pane (see Figure 12-2), click the folder containing the message you want to copy. For example, click the Inbox folder. A list of messages in that folder is displayed in the pane in the middle. Click the message you want to copy.
- Resize the Outlook window so that you can see the message you want to copy and the USB drive icon in Windows Explorer or the Computer window.
- Drag the message from the Outlook window to the USB drive icon in Windows Explorer or the Computer window.
- Click File, Print from the Outlook menu to open the Print dialog box. After printing the e-mail so that you have a copy to include in your final report, exit Outlook.

Viewing E-mail Headers

After you copy and print a message, use the e-mail program that created it to find the e-mail header. This section includes instructions for viewing e-mail headers in a variety of e-mail programs, including Windows GUI clients, a UNIX command-line e-mail program, and some common Web-based e-mail providers. After you open e-mail headers, copy and paste them into a text document so that you can read them with a text editor, such as Windows.

To retrieve an Outlook e-mail header, follow these steps:

- Start Outlook, and then select the original of the message you copied in the previous section.
- Right-click the message and click Message Options to open the Message Options dia- log box. The Internet headers text box at the bottom contains the message header.



Importance: Normal

Sensitivity: Normal

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Have replies sent to:

□ Expires after: None 12:00 AM

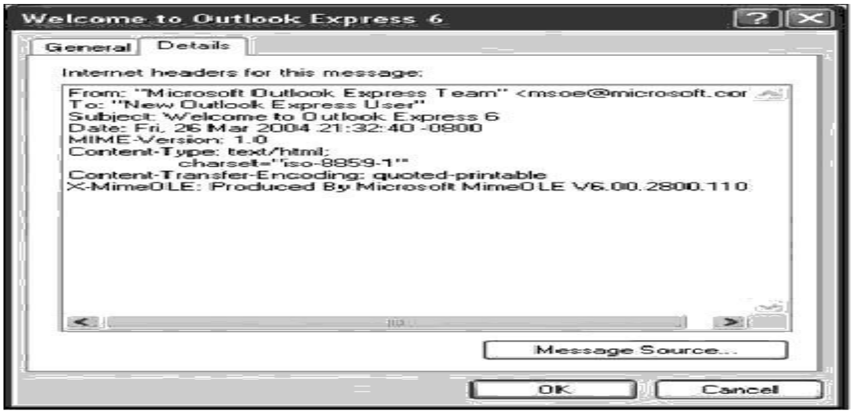
Categories: None

Internet headers:

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

Fig: An Outlook e-mail header

- Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.
- Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Outlook Header.txt in your work folder. Then close the document and exit Outlook. To retrieve an Outlook Express e-mail header, follow these steps:
- Start Outlook Express, and then display the message you want to examine.
- Right-click the message and click Properties to open a dialog box showing general information about the message.

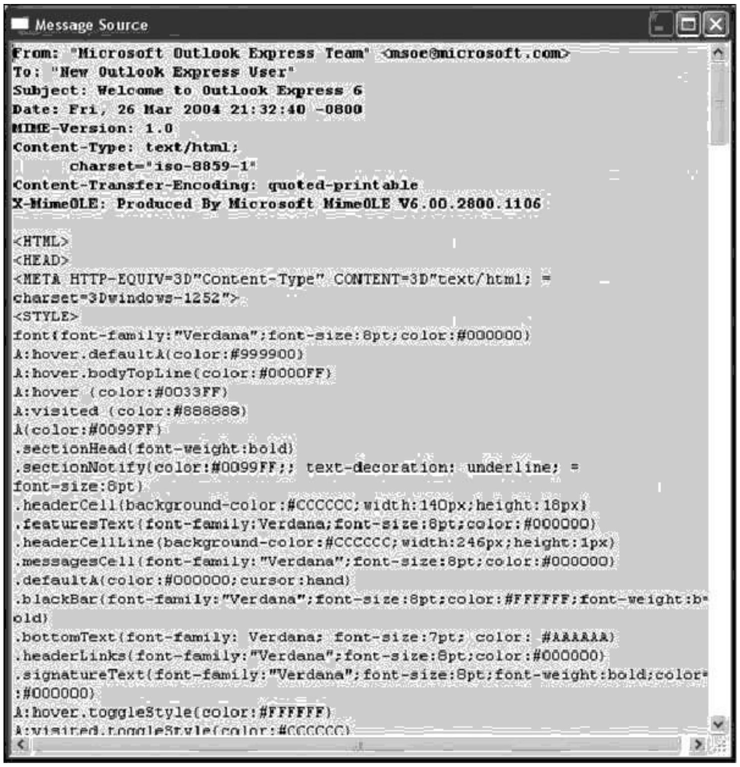


Internet headers for this message:

```
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;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.110
```

Fig: An Outlook Express e-mail header

- Click the Message Source button to view the e-mail's HTML source code ,which can be helpful in examining possible phishing messages.
- Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.
- Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Outlook Express Header.txt in your work folder, and then exit Notepad.
- Close all open windows and dialog boxes, and then exit Outlook Express.



```
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:#CCCCCC;width:140px;height:18px}
.featuresText{font-family:Verdana;font-size:8pt;color:#000000}
.headerCellLine{background-color:#CCCCCC;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:#CCCCCC}
```

Fig: Viewing the message's HTML source code

To retrieve an e-mail header in Novell Evolution, follow these steps:

- Start Evolution, and open the Inbox.
- Double-click the e-mail message to open it.
- Click View, All Message Headers from the menu to display the e-mail header, shown in Figure 12-6.
- Select all the message header text, and then press Ctrl+C to copy it to the Clipboard. Start a text editor, such as KEdit or gedit, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Evolution Header.txt in your work folder, close the file, and then exit the text editor and Evolution.

In the previous activities, you used a GUI program to find the header information. Now you see how to find this same information with a command-line e-mail program. If available, follow these steps to retrieve e-mail headers in UNIX Pine:

- Start Pine by typing pine at the command prompt and pressing Enter. The Pine e-mail screen appears with available options at the bottom.
- Type s to display setup options.

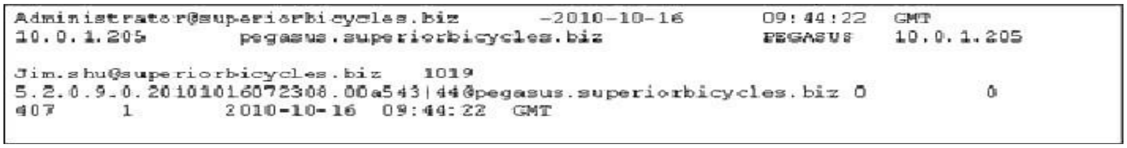
Understanding E-mail Servers

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. As a computer forensics investigator, you can't know everything about e-mail servers. Your focus is not to learn how a particular e-mail server works but how to retrieve information about e-mails for an investigation. Usually, you must work closely with the network administrator or e-mail administrator, who is often willing to help you find the data or files you need and might even suggest new ways to find this information. If you can't work with an administrator, conduct research on the Internet or use the forensics tools discussed later in this chapter to investigate the e-mail server software and OS.

To investigate e-mail abuse, you should know how an e-mail server records and handles the e-mail it receives. Some e-mail servers use databases that store users' e-mails, and others use a flat file system. All e-mail servers can maintain a log of e-mails that are processed. Some e-mail servers are set up to log e-mail transactions by default; others must be configured to do so. Most e-mail administrators log system operations and message traffic to recover e-mails in case of a disaster, to make sure the firewall and e-mail filters are working correctly, and to enforce company policy.

However, the e-mail administrator can disable logging or use circular logging, which over- writes the log file when it reaches a specified size or at the end of a specified time frame. Circular logging saves valuable server space, but you can't recover a log after it's overwritten. For example, on Monday the e-mail server records traffic in the Mon.log file. For the next six days, the e-mail server uses a log for each day, such as Tues.log, Wed.log, and so forth. On Sunday at midnight, the e-mail server starts recording e-mail traffic in Mon.log, overwriting the information logged the previous Monday. The only way to access the log file information is from a backup file, which many e-mail administrators create before a log file is overwritten.

E-mail logs generally identify the e-mail messages an account received, the IP address from which they were sent, the time and date the e-mail server received them, the time and date the client computer accessed the e-mail, the e-mail contents, system-specific information, and any other information the e-mail administrator wants to track. These e-mail logs are usually formatted in plain text and can be read with a basic text editor, such as Notepad or vi.



```
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
5.2.0.9.0.20101016072308.00a543|44@pegasus.superiorbicycles.biz 0          0
407     1       2010-10-16   09:44:22   GMT
```

Fig: An e-mail server log file

Using Specialized E-mail Forensics Tools

For many e-mail investigations, you can rely on e-mail message files, e-mail headers, and e-mail server log files. However, if you can't find an e-mail administrator willing to help with the investigation, or you encounter a highly customized e-mail environment, you can use data recovery tools and forensics tools designed to recover e-mail files.

As technology has progressed in e-mail and other services, so have the tools for recovering information lost or deleted from a hard drive. In previous chapters, you have reviewed many tools for data recovery, such as ProDiscover Basic and Access Data FTK. You can also use these tools to investigate and recover e-mail files. Other tools, such as the ones in the follow- ing list, are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

- Data Numen for Outlook and Outlook Express
- FINAL e MAIL for Outlook Express and Eudora
- Sawmill-GroupWise for log analysis office_agent.html)
- DBX tract for Outlook Express
- Fookes Aid4Mail and Mail Bag Assistant for Outlook, Thunderbird, and Eudora
- Paraben E-Mail Examiner, configured to recover several e-mail formats
- Access Data FTK for Outlook and Outlook Express
- On track Easy Recovery Email Repair for Outlook and Outlook Express
- R-Tools R-Mail for Outlook and Outlook Express.
- Office Recovery's Mail Recovery for Outlook, Outlook Express, Exchange, Exchange Server, and IBM Lotus Notes

When you use a third-party tool to search for a .db file, for example, you can find where the administrator stores .db files for the e-mail server. To find log files, use .log as the search criteria. You're likely to find at least two logs related to e-mail—one listing logged events for messages and the other listing logged events for accounts accessing e-mail.

FTK, En Case, and other forensics tools enable you to find e-mail database files, personal e-mail files, offline storage files, and log files. Some tools allow you to view messages and other files with a special viewer; others require using a text editor to compare information, such as the date and time stamp, username, domain, and message contents, to determine whether it matches what was found on the victim's computer.

One advantage of using data recovery tools is that you don’t need to know how the e-mail server or e-mail client operates to extract data from these computers. Data recovery tools do the work for you and allow you to view evidence on the computer.

After you compare e-mail logs with the messages, you should verify the e-mail account, message ID, IP address, and date and time stamp to determine whether there’s enough evidence for a warrant. If so, you can obtain and serve your warrant for the suspect’s computer equipment.

Understanding Mobile Device Forensics

People store a wealth of information on cell phones, and the thought of losing your cell phone and, therefore, the information stored on it can be a frightening prospect. Despite this concern, not many people think about securing their cell phones, although they routinely lock and secure laptops or desktops. Depending on your phone’s model, the following items might be stored on it:

- Incoming, outgoing, and missed calls
- Text and Short Message Service (SMS) messages
- E-mail
- Instant messaging (IM) logs
- Web pages
- Pictures
- Personal calendars
- Address books
- Music files
- Voice recordings

Many people store more information on their cell phones than they do on their computers and with this variety of information, piecing together the facts of a case is possible. Recent cases, such as the rape allegations at Duke University and the Scott Peterson murder trial, show that cell phone data is used increasingly in court as evidence. In some countries, cell phones are even used to log in to bank accounts and transfer funds from one cell phone to another, which provides even more potential evidence. This handheld device is one of the most versatile pieces of equipment invented yet.

Despite the usefulness of these devices in providing clues for investigations, investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics. No single standard exists for how and where cell phones store messages, although many phones use similar storage schemes. In addition, new phones come out about every six months, and they’re rarely compatible with previous models. Therefore, the cables and accessories you have might become obsolete in a short time. Also, cell phones are often combined with PDAs, which can make forensics investigations more complex.

Mobile Phone Basics

Since the 1970s, when Motorola introduced cell phones, mobile phone technology has advanced rapidly. Gone are the days of two-pound cell phones that only the wealthy could afford. In the past 40 years, mobile phone technology has developed far beyond what the inventors could have imagined.

Up to the end of 2008, there have been three generations of mobile phones: analog, digital personal communications service (PCS), and third-generation (3G). 3G offers increased bandwidth, compared with the other technologies:

- 384 Kbps for pedestrian use
- 128 Kbps in a moving vehicle
- 2 Mbps in fixed locations, such as office building.

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

All mobile devices have volatile memory, so making sure they don’t lose power before you can retrieve RAM data is critical. At the investigation scene, determine whether the device is on or off. If it’s off, leave it off, but find the recharger and attach it as soon as possible. Note this step in your log if you can’t determine whether the device was charged at the time of seizure. If the device is on, check the LCD display for the battery’s current charge level.

Because mobile devices are often designed to synchronize with applications on a user’s PC, any mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately. This precaution helps prevent synchronization that might occur automatically on a preset schedule and overwrite data on the device. In addition, collect the PC and any peripheral devices to determine whether the hard drive contains any information that’s not on the mobile device.

Depending on the warrant or subpoena, the time of seizure might be relevant. In addition, messages might be received on the mobile device after seizure that may or may not be admissible in court. If you determine that the device should be turned off to preserve battery power or a possible attack, note the time and date at which you take this step. The alternative is to isolate the device from incoming signals with one of the following options:

- Place the device in paint can, preferably one that previously contained radio wave– blocking paint.
- Use the Paraben Wireless Strong Hold Bag which conforms to Faraday wire cage standards.
- Use eight layers of antistatic bags (for example, the bags that new hard drives are wrapped in) to block the signal.

The drawback of using these isolating options is that the mobile device is put into roaming mode, which accelerates battery drainage. NIST suggests supplying a portable means of power, such as a battery-powered charger, to prevent this problem. Newer mobile devices shut themselves off or enter a –sleep statel after reaching a certain low battery level.

As mentioned, memory resides in the phone itself and in the SIM card, if the device is equipped with one. The file system for a SIM card is a hierarchical structure. This file structure begins with the root of the system (MF). The next level consists of directory files (DF), and under them are files containing elementary data (EF). EFs under the GSM and DCS1800 DFs contain network data on different frequency bands of operation. The EFs under the Telecom DF contain service-related data.

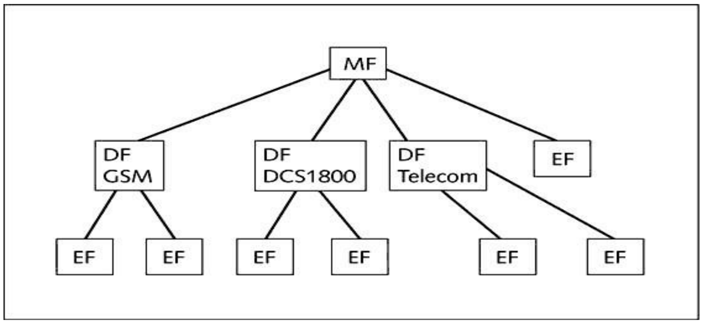


Fig: SIM file structure

You can retrieve quite a bit of data from a SIM card. The information that can be retrieved falls into four categories:

- Service-related data, such as identifiers for the SIM card and subscriber
- Call data, such as numbers dialed
- Message information
- Location information

If power has been lost, you might need PINs or other access codes to view files. Typically, users keep the original PIN assigned to the SIM card, so when you're collecting evidence at he scene, look for users' manuals and other documentation that can help you access the SIM card. With most SIM cards, you have three attempts at entering an access code before the device is locked, which then requires calling the service provider or waiting a certain amount of time before trying again. Common codes to try are 1-1-1-1 or 1-2-3-4.

SIM Card Readers With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/ software device called a SIM card reader. To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you're ready to proceed to this step. The general procedure is as follows:

- Remove the back panel of the device.
- Remove the battery.
- Under the battery, remove the SIM card from its holder.

- Insert the SIM card into the card reader, which you insert into your forensic workstation’s USB port.

A variety of SIM card readers are on the market. Some are forensically sound and some are not; make sure you note this feature of the device in your investigation log. Another problem with SIM card readers is dealing with text and SMS messages that haven’t been read yet. After you view a message, the device shows the message as opened or read. For this reason, documenting messages that haven’t been read is critical. Using a tool that takes pictures of each screen can be valuable in this situation. These screen captures can provide additional documentation.

IPhone Forensics Because the iPhone is so popular, its features are copied in many other mobile devices. The wealth of information that can be stored on this device makes iPhone forensics particularly challenging. At first, many researchers and hackers tried to find a way to –crack‖ the iPhone but were unsuccessful because the device is practically impenetrable. A more fruitful approach was hacking backup files. However, this method does have limitations: You can access only files included in a standard backup, so deleted files, for example, can’t be accessed