

UNIT-IV

Current Forensic Tools

In this, we are going to explore many software and hardware tools used during digital forensics investigations. No specific tools are recommended; instead, the goal is to explain how to select tools for digital investigations based on specific criteria.

Forensics tools are constantly being developed, updated, patched, revised, and discontinued. Therefore, checking vendors' Web sites routinely to look for new features and improvements is important. These improvements might address a difficult problem you're having in an investigation.

Evaluating computer forensic tool need:

As we know, we need to develop a business plan to justify the acquisition of digital forensics hardware and software. When researching options, consider open-source tools, which sometimes include technical support. The goal is to find the best value for as many features as possible.

Some questions to ask when evaluating tools include the following:

- On which OS does the forensics tool run? Does the tool run on multiple OSs?
- Is the tool versatile? For example, does it work in both Windows and Linux?
- Can the tool analyze more than one file system, such as FAT, NTFS, and Ext4?
- Can a scripting language be used with the tool to automate repetitive functions and tasks?
- Does the tool have any automated features that can help reduce the time needed to analyze data?
- What is the vendor's reputation for providing product support? For open-source tools, how good are the support forums?

As you learn more about digital investigations, you'll have more questions about tools for conducting these investigations. When you search for tools, keep in mind what OSs and file types you'll be analyzing. For example, if you need to analyze Microsoft Access or SQL Server databases, look for a product designed to read these files. If you're analyzing e-mail messages, look for a forensics tool that specializes in reading e-mail content.

When you're selecting tools for your lab, keep an open mind, and compare platforms and applications for different tasks. Although many investigators are most comfortable using Windows tools, check into other options, such as Linux and Macintosh platforms.

Types of Digital Forensics Tools

Digital forensics tools are divided into two major categories: hardware and software.

Hardware Forensics Tools

Hardware forensics tools range from simple, single-purpose components to complete computer systems and servers. For example, the Tableau T35es-R2 SATA/IDE eSATA bridge is a single-purpose component that makes it possible to access a SATA or an IDE drive with one device. Some examples of complete systems are Digital Intelligence F.R.E.D. systems (www.digitalintelligence.com/forensichardware.php), DIBS Advanced Forensic Workstations (www.dibsforensics.com/index.html), Forensic Computers' Forensic Examination Stations and portable units (www.forensic-computers.com), and Ace Laboratory systems (www.ancelaboratory.com/catalog/), designed for data recovery of failed drives, a feature that comes in handy in many situations.

Software Forensics Tools

Software forensics tools are grouped into command-line applications and GUI applications. Some tools are specialized to perform one task. For example, SafeBack, from New Technologies, Inc. (NTI), was designed as a command-line disk acquisition tool. It's no longer supported, but you can still find it distributed online. However, it's used more as a reliable fallback when all else fails than a primary tool. Other tools are designed to perform many different tasks. For example, PassMark Software OSForensics, X-Ways Forensics, Guidance Software EnCase, Magnet Forensics AXIOM, and AccessData FTK are GUI tools designed to perform most 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 and have the capability to analyze image files.

Tasks Performed by Digital Forensics Tools

All digital forensics tools, both hardware and software, perform specific functions. When you're testing new tools, you might find it helpful to follow guidelines set up by NIST's Computer Forensics Tool Testing (CFTT) program, ASTM International's (formerly the American Society of Testing and Materials) E2678 standard, and the International Organization on Computer Evidence (IOCE). In addition, ISO standard 27037 states that Digital Evidence First Responders (DEFRRs) should use validated tools.

The following categories of functions are meant as guidelines for evaluating digital forensics tools, with sub functions for refining data analysis and recovery and ensuring data quality:

- Acquisition
- Validation and verification
- Extraction
- Reconstruction
- Reporting

NIST's CFTT and other groups include additional functions, such as data acquisition, data extraction from mobile devices, file reconstruction, and string searching, that aren't included in these guidelines ("Verification of Digital Forensics Tools", Jim Lyle, May 2010, Montana Supreme Court Spring Training Conference). In the following sections, you learn how these functions and sub functions apply to digital investigations.

Acquisition The first task in digital forensics investigations is making a copy of the original drive.

Validation is a way to confirm that a tool is functioning as intended, and **verification** proves that two sets of data are identical by calculating hash values or using another similar method. Another related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data.

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

Reconstruction The purpose of having a reconstruction function in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident. Another reason for duplicating a suspect drive is to create a copy for other digital investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence. Reconstruction is also done if a drive has been compromised by malware or a suspect's actions.

Reporting To perform a forensics disk analysis and examination, you need to create a report. Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually. The investigator then copied the evidence to a separate program, such as a word processor, to create a report.

Digital 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 are some options for command-line and GUI tools in both Windows and Linux.

Computers used several OSs before Windows and MS-DOS dominated the market. During this time, digital 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 with them. Software developers began releasing 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 digital investigations was *Norton DiskEdit*. This tool used manual processes that required investigators to spend considerable time on a typical 500 MB drive. Eventually, programs designed for digital forensics were developed for DOS, Windows, Apple, NetWare, and UNIX systems.

Some command-line forensics tools are created specifically for Windows command-line interface (CLI) platforms; others are created for Macintosh and UNIX/Linux. Because there are many different versions of UNIX and Linux, these OSs are often referred to as "Linux platforms."

The following are several Linux tools for forensics analysis,

Those are

- SMART,
- Helix3
- Kali Linux
- Autopsy with Sleuth Kit.

SMART: SMART is designed to be installed on numerous Linux versions, including Gentoo, Fedora, SUSE, Debian, Knoppix, Ubuntu, Slackware, and more. You can analyze a variety of file systems with SMART; for a list of file systems or to download an evaluation ISO image for SMART and SMART Linux, go to www.asrdata.com/forensic-software/software-download/.

SMART includes several plug-in utilities. This modular approach makes it possible to upgrade SMART components easily and quickly. SMART can also take advantage of multithreading capabilities in OSs and hardware, a feature lacking in other forensics utilities. This tool is one of the few that can mount different file systems, such as journaling file systems, in a read-only format.

Helix 3: One of the easiest suites to use is Helix because of its user interface. Although Helix is no longer a free package, you can go to www.e-fense.com/products.php to learn more about it. What's unique about Helix is that you can load it on a live Windows system, and it loads as a bootable Linux OS from a cold boot. Its Windows component is used for live acquisitions. Be aware, however, that some international courts haven't accepted live acquisitions as a valid forensics practice.

Kali Linux: Kali Linux, formerly known as BackTrack, is another Linux Live CD used by many security professionals and forensics investigators. It includes a variety of tools and has an easy-to-use KDE interface. You can download the ISO image from www.kali.org. Kali includes several tools, such as Autopsy and Sleuth Kit, ophcrack, dcfldd, MemFetch, and MBoxGrep.

Autopsy and Sleuth Kit: Sleuth Kit is a Linux forensics tool, and Autopsy is the GUI browser interface for accessing Sleuth Kit's tools. For example, shut down your Windows computer with the Kali disc in the CD/DVD drive, making sure your system is set to boot from the CD/DVD drive before the hard drive. Then do a hard boot to the computer.

In the options that are displayed, select Expert Mode. (Note that this mode is forensically sound.) If you're booting from a laptop, you might have display issues. You can click "scan" to have Kali find the correct settings. (If Kali fails to find these settings, experiment until you finds a setting that works.) After the correct display setting is applied, a GUI is displayed. If prompted, specify whether to load SCSI modules or additional modules from a floppy disk.

Digital Forensics Hardware Tools:

Technology changes rapidly, and hardware manufacturers have designed most computer components to last about 18 months between failures. Hardware is hardware; whether it's a rack-mounted server or a forensic workstation, eventually it fails. For this reason, you should schedule equipment replacements periodically ideally, every 18 months if you use the hardware fulltime. Most digital forensics operations use a workstation 24 hours a day for a week or longer between complete shutdowns.

You should plan your hardware needs carefully, especially if you have budget limitations. Include the amount of time you expect the forensic workstation to be running, how often you expect hardware failures, consultant and vendor fees to support the hardware, and how often to anticipate replacing forensic workstations. The longer you expect the forensic workstation to be running, the more you need to anticipate physical equipment failure and the expense of replacement equipment.

Forensic Workstations

Many hardware 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 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.

Building Your Own Workstation

To decide whether you want to build your own workstation, first ask “How much do I have to spend?” Building a forensic workstation isn’t as difficult as it sounds but can quickly become expensive if you aren’t careful. If you have the time and skill to build your own forensic workstation, you can customize it to your needs and save money, although you might have trouble finding support for problems that develop. For example, peripheral devices might conflict with one another, or components might fail. If you build your own forensic workstation, you should be able to support the hardware.

Using a Write-Blocker

The first item you should consider for a forensic workstation is a write-blocker. Write-blockers protect evidence disks by preventing data from being written to them. Software and hardware write-blockers perform the same function but in a different fashion.

Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode (such as a Windows CLI). PDBlock changes interrupt 13 of a workstation’s BIOS to prevent writing to the specified drive. If you attempt to write data to the blocked drive, an alarm sounds, advising that no writes have occurred. PDBlock can run only in a true DOS mode, however, not in a Windows CLI.

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 Tools

The National Institute of Standards and Technology (NIST) publish articles, provide tools, and create procedures for testing and validating computer forensics software. Software should be verified to improve evidence admissibility in judicial proceedings. NIST sponsors the CFTT project to manage research on forensics tools. For additional information on this testing project, visit www.cfft.nist.gov. The Computer Forensic Reference Data Sets (CFReDS; www.cfreds.nist.gov) has been created recently to provide data sets for tools, training, and hardware testing.

E-Mail Investigations

Exploring the Role of E-mail in Investigations:

E-mail evidence is an important part of any computing investigation, so digital 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 are associated with a spoofed message.

The Internet links in a phishing e-mail often appear to be correct, such as the U.S. Internal Revenue Service's Web page, www.irs.gov. Typically, phishing e-mails contain links to text on a Web page. By using this technique, a phishing message attempts to get personal information by luring readers with false promises.

When pharming is used, readers might go to the correct Web site address, but DNS poisoning takes them to a fake site. To determine whether redirection has been used, you need to view the message's HTML source code and check whether an Internet link is a label with a redirect to a different Web address.

One of the most noteworthy e-mail scams was 419, or the Nigerian Scam, which originated as chain letters from Nigeria, Africa. Fraudsters need only access to Internet e-mail to solicit victims, thus saving the costs of international mail and phone calls. Unlike newer, more sophisticated phishing e-mail frauds, 419 messages have certain characteristic ploys and a typical writing style.

For example, 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. Another common scam is a sender stating you have won a lottery and asking you to send money to claim the prize.

Example:

One noteworthy example of a lawsuit involving spoofing e-mail occurred in February 2001 in the Superior Court of Massachusetts: *Suni Munshani v. Signal Lake Venture Fund II, LP et al.*

Suni Munshani claimed he received an e-mail from the CEO of Signal Lake Venture Fund instructing him to purchase options (financial warrants) for a total of \$25 million.

Signal Lake Venture Fund investigated its e-mail servers and didn't find the e-mail Munshani claimed he received.

In preparation for the trial, Signal Lake Venture Fund conducted a discovery demand for all of Munshani's e-mail. Because of the sensitive information Munshani had on his e-mail server, the court appointed an impartial discovery firm to examine the e-mail. The discovery firm found that Munshani had used a text editor to alter an e-mail the CEO of Signal Lake Venture Fund had sent.

The clue to the e-mail being a fake was the Enhanced/Extended Simple Mail Transfer Protocol (ESMTP) number in the message's header, which is unique to each message an e-mail server transmits. The e-mail Munshani claimed was a legitimate message instructing him to purchase options had the same ESMTP value as the other message the CEO sent. This level of examination revealed that Munshani committed fraud.

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 a client/server architecture.

The server runs an e-mail server program, such as Microsoft Exchange Server, to provide e-mail services. Client computers use e-mail programs (also called e-mail clients), such as Microsoft Outlook, to contact the e-mail server and send and retrieve e-mail messages.

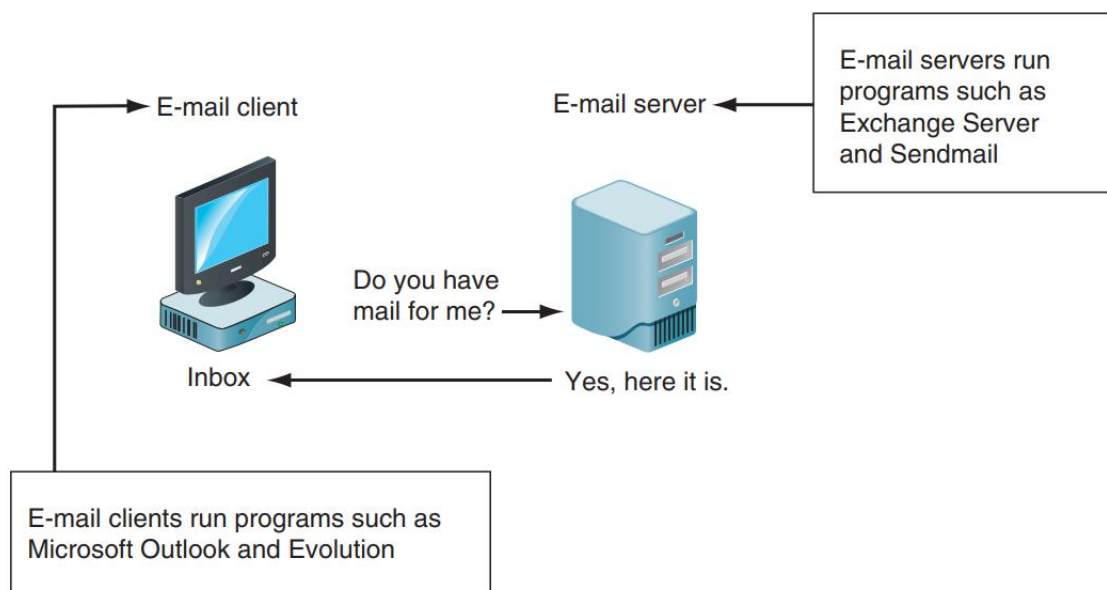


Figure: E-mail in a client/server architecture

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, for example, for John Smith at Some Company, *jsmith* is the username, and it is followed by the company's domain name, *somecompany.com*, to create the e-mail address *jsmith@somecompany.com*.

In contrast, a company that provides public e-mail services, such as Google, Hotmail, or Yahoo!, owns the e-mail server and accepts everyone who signs up for the service by providing a username and password. E-mail companies also provide their own servers and administrators.

After users sign up, they can access their e-mail from any computer connected to the Internet. In most cases, Internet e-mail users aren't required to follow a standardized naming convention for usernames. They can choose their own usernames (but not the domain name), as long as they aren't already in use.

For digital investigators, tracking intranet e-mail is easier because accounts use standard names the administrator establishes. For example, *jane.smith@mycompany.com* is easily recognized as the e-mail address for an employee named Jane Smith.

Tracking Internet e-mail users is more difficult because these accounts don't always use standard naming schemes, and e-mail administrators aren't familiar with all the user accounts on their servers. Identifying the owner of an e-mail account with an address such as *itty_bitty@gmail.com*, for example, is not easy.

With the expansion of cloud service providers, many companies are migrating their e-mail services to the cloud. This setup is convenient because employees can easily access their e-mail from anywhere in the world, but it adds a layer of complexity for investigations, depending on the service level agreement with the cloud provider.

Investigating E-mail Crimes and Violations:

Investigating crimes or policy violations involving e-mail is like investigating other types of computer abuse and crimes. Your goal is to find out who is behind the crime or policy violation, collect the evidence, and present your findings in the court of law.

E-mail crimes and violations depend on the city, state, and 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 common, 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, access the victim's computer or mobile device to recover the evidence on it. 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.

With a corporate investigation, be sure policies are in place for this action. For a criminal investigation, you need warrants to access or get copies of files on a server. When dealing with a stalker, if you can't actually sit down at the victim's computer, you might 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, 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.

If Outlook or Outlook Express is installed on your computer, follow these steps:

1. Insert a USB drive into a USB port.
2. Open File Explorer, navigate to the USB drive, and leave this window open.
3. Start Outlook by going to the Start screen, typing Outlook, and pressing Enter.
4. In the Mail Folders pane, 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.

5. Resize the Outlook window so that you can see the message you want to copy and the USB drive icon in File Explorer.
6. Drag the message from the Outlook window to the USB drive icon in File Explorer.
7. Click the File tab, and then click Print to open the Print pane. After printing the e-mail so that you have a copy to include in your final report, exit Outlook.

Tip: Instead of dragging, you can click a message in the Inbox, click the File tab, and click Save As. In the Save As dialog box, navigate to where you want to copy the message, making sure you select Outlook Message Format if you want to make a copy. If you select the Text Only format, you get only the message contents. Finally, click the Save button.

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. In this, we are going to learn viewing e-mail headers in a variety of e-mail programs, including Windows GUI clients 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 Notepad, Linux vim, Nano (used with UNIX), or Apple TextEdit.

Outlook e-mail header:

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

1. Start Outlook, and then select the message you copied in the previous section.
2. Double-click the message, and then click File, Properties. The “Internet headers” textbox at the bottom contains the message header, shown in Figure.

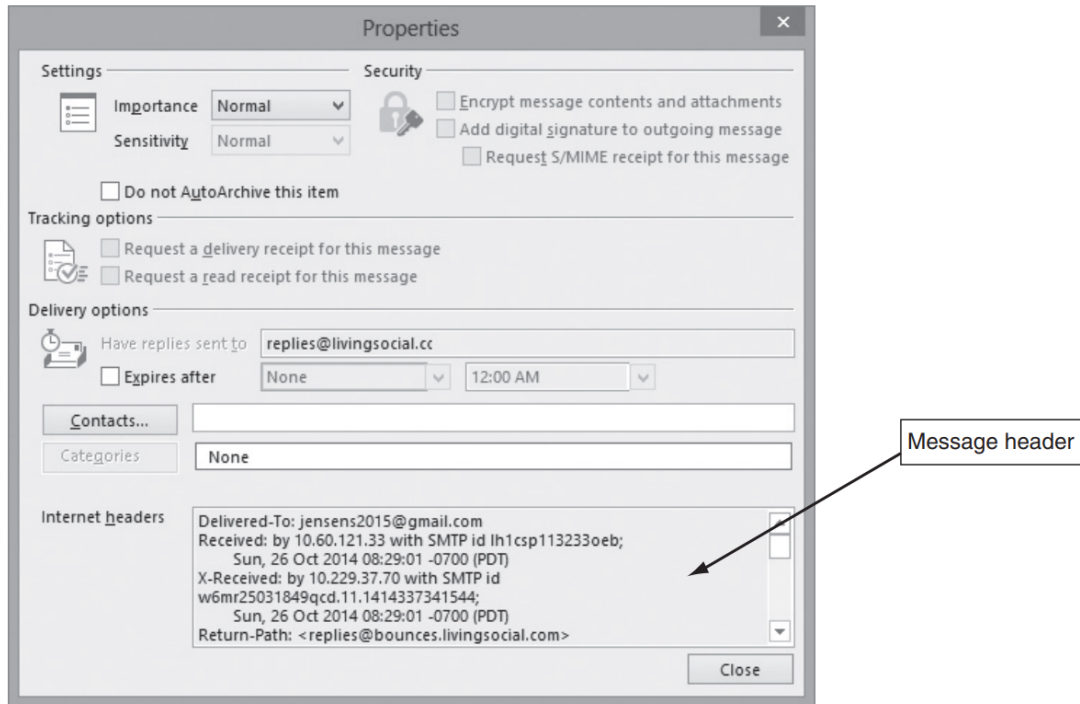


Figure: An Outlook e-mail header

3. Select the message header text, and then press Ctrl+C to copy it to the Clipboard.
4. Start Notepad, and then press Ctrl+V in a new document window to paste the messageheader text.
5. Save the document as Outlook Header.txt in your work folder. Then close thedocument and exit Outlook.

e-mail headers in Yahoo!:

Follow these steps to view e-mail headers in Yahoo!:

1. Log on to your Yahoo! mail account, and click Inbox to view a list of messages.
2. Above the message window, click the More list arrow, and click View Full Header(see Figure)
3. In the Full Header window, select all the text, press Ctrl+C to copy it, and then clickOK.
4. Start Notepad, and then press Ctrl+V in a new document window to paste the messageheader text. Save the document as **Yahoo_Header.txt** in your work folder. Log offYahoo!, and exit your Web browser.



```
1. Received: from SM2PR0801MB0752.namprd08.prod.outlook.com (25.160.57.146) by
2. CO2PR0801MB0744.namprd08.prod.outlook.com (25.160.10.142) with Microsoft SMTP
3. Server (TLS) id 15.0.1039.15 via Mailbox Transport; Fri, 26 Sep 2014 17:34:08
4. +0000
5. Received: from BL2PR08CA0060.namprd08.prod.outlook.com (10.255.170.178) by
6. SM2PR0801MB0752.namprd08.prod.outlook.com (25.160.57.146) with Microsoft SMTP
7. Server (TLS) id 15.0.1034.13; Fri, 26 Sep 2014 17:34:07 +0000
8. Received: from BN1AFF011FD008.protection.gbl (2a01:111:f400:7c10::137) by
9. BL2PR08CA0060.outlook.office365.com (2a01:111:e400:c4b::50) with Microsoft
10. SMTP Server (TLS) id 15.0.1039.15 via Frontend Transport; Fri, 26 Sep 2014
11. 17:34:06 +0000
12. Received: from online.itwhitpapers.com (66.186.127.67) by
13. BN1AFF011FD008.mail.protection.outlook.com (10.58.52.68) with Microsoft SMTP
14. Server id 15.0.1029.15 via Frontend Transport; Fri, 26 Sep 2014 17:34:05
15. +0000
16. DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; q=dns/txt; l=15361;
17. d=online.itwhitpapers.com;s=2008;
18. h=from;
19. bh=cChkNADxtgRz+Ivn6Ms88idH0ATbNQa7a08hRgIowS-;
20. b=ChreKQD3JRAOYU7LCIyRo4IDymWlIdX2exbvK0kAuZg2gB7NO/czFT44fmPnQzV100Xlyvm
21. +k7nq86vpInrom=-;
22. DomainKey-Signature: a=rsa-sha1; q=dns; c=noews; s=2008; d=online.itwhitpapers.com;
23. h=from;
24. b=NajRzpeS96Qk0g7i5G32eTA/BTgspIw0FMW6GIXQ71C+JpA3qC18oi48QgUMIG4m3MPwH 3dcCH95TzotnqA==
25. From: "ITwhitpapers Business Intelligence" <online_resources@online.itwhitpapers.com>
26. To: <aphillip@blah.edu>
27. Subject: Build a Business Case: Developing Custom Apps
28. Date: Fri, 26 Sep 2014 13:30:00 -0400
29. MIME-Version: 1.0
30. Content-Type: multipart/alternative;
```

Figure: An e-mail header with line numbers added

The e-mail header in the above figure supplies useful information. Lines 1 through 4 shows the servers the message passed through. Lines 3 and 4 include “via Frontend Transport,” which is a stateless proxy for inbound traffic on Microsoft Exchange Server.

Line 5 shows “DKIM Signature,” which stands for DomainKeys Identified Mail (www.dkim.org). It is a way to verify the names of domains a message is flowing through and was developed to help cut down on spam. Line 6 is the verification from DKIM.

Lines 7 through 10 are simply the From, To, Subject, and Date fields in the e-mail. Lines 11 and 12 show the MIME-Version and Content Type information.

Tracing an E-mail Message:

As part of the investigation, you need to determine an e-mail’s origin by further examining the header with one of many free Internet tools. Determining message origin is referred to as “tracing.” In this, you learn about some Internet lookup tools that can be used to trace where an e-mail originated.

For example, if a company is listed in an e-mail address, you can visit the company’s site to find out who administers the domain. If the point of contact is not listed on the Web site or the domain does not have a Web site, you need to use a registry site, such as those in the following list, to determine the point of contact:

www.arin.net—Use the American Registry for Internet Numbers (ARIN) to map an IP address to a domain name and find the domain's point of contact.

www.internic.com—Like *www.arin.net*, you use this site to find a domain's IP address and point of contact.

www.google.com—Use this search engine and others to look for more information and additional postings on discussion boards.

Using one of these Web sites, you can find the suspect's full e-mail address, such as *jim.shu@superiorbicycles.biz*, and contact information.

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 digital forensics investigator, you cannot 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.

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.

Most e-mail administrators log system operations and message traffic for the following reasons:

- Recover e-mails in case of a disaster.
- Make sure the firewall and e-mail filters are working correctly.
- Enforce company policy.

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 vim.

Examining UNIX E-mail Server Logs

More than a dozen UNIX e-mail server programs are available. Most produce log files similar to the ones. Postfix and Sendmail are two common UNIX e-mail servers.

Sendmail is the default for FreeBSD systems, such as CentOS.

Log files and configuration files can provide helpful information. The configuration file for Sendmail is `/etc/mail/sendmail.cf`, which can help you determine where log files are stored. Sendmail refers to the `sendmail.cf` file to find out what to do with an e-mail after it's received. For example, if the server receives an e-mail from an unsolicited site, a line in the `sendmail.cf` file can tell the Sendmail server to discard it.

Postfix is another common UNIX e-mail server. Similar to Sendmail, it has configuration files, `master.cf` and `main.cf`, in the `/etc/postfix` directory, and e-mails are stored in `/var/spool/postfix`.

Because a UNIX system has a variety of e-mail servers available, the `syslog.conf` file simply specifies where to save different types of e-mail log files. The first log file it configures is `/var/log/maillog`, which usually contains a record of Simple Mail Transfer Protocol (SMTP) communication between servers.

Examining Microsoft E-mail Server Logs

Exchange Server, generally called Exchange, is the Microsoft e-mail server software. Exchange uses an Exchange database and is based on the Microsoft Extensible Storage Engine (ESE), which uses several files in different combinations to provide e-mail service. The files most useful to an investigation are .edb database files, checkpoint files, and temporary files.

Exchange servers can also maintain a log called `Tracking.log` that tracks messages. If the Message Tracking feature has been enabled and the e-mail administrator selects verbose (detailed) logging, you can see the timestamp, IP address of the sending computer, and the e-mail's contents or body. Except for special forensics tools, the message-tracking log in verbose mode provides the most information about messages sent and received in Exchange.

Another log used for troubleshooting and investigating the Exchange environment is the troubleshooting log. You can read this log, also known as a "diagnostic log," by using Windows Event Viewer, shown in the following figure, which is available in Administrative Tools. Each event logged has an ID number and a severity level.

To examine the details of an e-mail event, double-click the event to open its Event Properties dialog box. This dialog box shows date and time information that might be useful if, for example, you suspect the e-mail server has been tampered with to alter its contents.

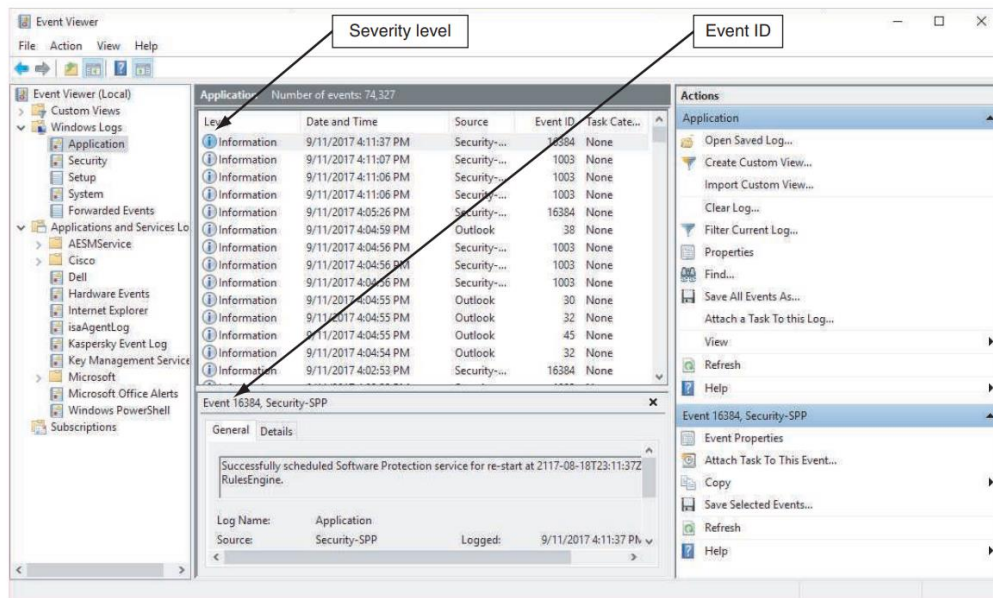


Figure: Viewing a log in Event Viewer

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. We have many tools for data recovery, such as Magnet AXIOM, Autopsy, and OSForensics.

You can also use these tools to investigate and recover e-mail files. Other tools, such as the ones in the following list, are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

- **DataNumen** for Outlook and Outlook Express (www.datanumen.com/products.htm)
- **FINALEMAIL** for Outlook Express and Eudora (<http://finalemail-1-2.en.softonic.com>)
- **MailXaminer** for multiple e-mail formats and large data sets (www.mailxaminer.com/)
- **Fookes Aid4Mail** and **MailBag Assistant** for Outlook, Thunderbird, and Eudora (www.fookes.com)
- **Paraben E-Mail Examiner**, configured to recover several e-mail formats (www.paraben.com/products/e3-emx)
- **AccessData FTK** for Outlook and Outlook Express (www.accessdata.com)

- **OntrackEasyRecoveryEmailRepair** for Outlook and Outlook Express (www.ontrackdatarecovery.ie/data-recovery/email-recovery/)
- **R-Tools R-Mail** for Outlook and Outlook Express (www.r-tt.com/outlook_mail_recovery/)
- **MXToolBox** for decoding e-mail headers (<https://mxtoolbox.com/EmailHeaders.aspx>)
- **FreeViewer** with free tools for Outlook, Windows Live Mail, Thunderbird, and other servers (www.freeviewer.org/email-forensics/free-tools.html).

Using OSForensics to Recover E-mail

OSForensics isn't task or file specific, as other tools are. However, it indexes data on a disk image or an entire drive for faster data retrieval. It can also filter or find files specific to e-mail clients and servers. You can configure these filters when you enter search parameters.

In this activity, you learn how to use OSForensics to recover e-mails:

1. Start OSForensics and start a new case. In the New Case dialog box, enter your name. For the case name, type InChap11. Fill in the contact details and the organization, and then click OK. Create a subfolder of your work folder called Chap11, and then create a subfolder called Terry.
2. Click the Add Device button. Navigate to the folder where you stored the M57 case files, click the hard drive file terry-2009-12-11-002.e01, and click OK.
3. Click the Create Index button in the left pane to start the Create Index Wizard. In the Step 1 of 5 window, click the Use Pre-defined File Types option button, if necessary. Click the Emails and Attachments check boxes, and then click Next. In the Step 2 of 5 window, click the Add button. In the Add Start Location dialog box, click the Whole Drive option button, if necessary. Click the list arrow, click terry-2009-12-11-002.e01, and then click OK. Click Next. In the Step 3 of 5 window, click Start Indexing. When the indexing has finished, click OK in the message box informing you that errors reading some files might have occurred in the indexing process, if necessary.
4. Click Search Index in the left pane. In the Enter Search Words text box, type money, and then click Search.
5. Click the Emails tab, if necessary. The search should have returned 10 e-mails. Right-click the first e-mail with the subject line "Computer Equipment" and click Open.
6. To see more details, click View, Headers from the menu. The following figure shows the results.
7. When you're finished examining the e-mail, close the Email Viewer window, and exit OSForensics.