# COSC6410 Lab Assignment 2

## Please submit through Blackboard by midnight September 11.

The purpose of this lab is:

1. Working with Windows System (Part 1).
2. Working with Linux and Macintosh file system (Part 2)
    a. Install Autopsy: lab 6.1
    b. Choose one from lab 7.1 or 7.3

**Submission requirement:**
**Submit the answers for all the review questions， and the last screenshot of what your computer display.**

# Part 1

# Lab 5.2 Examining the SAM Hive

## Objectives

The Registry is the central repository of settings and data for the Windows environment as a computer boots. It's divided into five hives in the C:\Windows\System32\Config folder. Each hive contains specific data, such as passwords, desktop settings, hardware and software configurations, and other valuable forensic information. The Registry files most useful to forensics investigators are the Security Accounts Manager (SAM) and SYSTEM hives and the `ntuser.dat` file (which is in the C:\Users*username* folder and is unique for each user). The SAM hive stores information on user accounts and their password hashes as well as group definitions and domain associations by using globally unique IDs (GUIDs). In this lab, you copy Registry files from a Windows image with FTK Imager and view the SAM hive with AccessData Registry Viewer.



After completing this lab, you will be able to:

- Examine the SAM hive containing usernames and password hashes
- View Registry files in Registry Viewer

## Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- AccessData Registry Viewer
- AccessData FTK Imager
- The `InCh05.exe` file on the DVD

Estimated completion time: **15–20 minutes**

## Activity

In this lab, you examine the SAM hive to determine the user accounts on a seized computer:

1. Copy the **`InCh05.exe`** file from the DVD to your **C:\Work\Labs\Evidence** folder. In File Explorer, double-click this file and click **Extract** to extract the Windows image to your evidence folder.
2. Right-click the **AccessData FTK Imager** desktop icon and click **Run as administrator**. If necessary, click **Yes** in the UAC message box.
3. Click **File, Add Evidence Item** from the menu. In the Select Source dialog box, click **Image File**, and then click **Next**. In the Select File dialog box, click **Browse**, navigate to and click **C:\Work\Labs\Evidence\InCh05.img**, and then click **OK** to enter this source path (see Figure 5-4). Click **Finish** to open the image in FTK Imager.
4. In the left pane, click to expand **InCh05.img, 6gb [NTFS], [root]**, and **Users**. Click the **Denise** folder, and then right-click the **`ntuser.dat`** file in the File List pane and click **Export Files**. In the Browse For Folder dialog box, navigate to and click **C:\Work\Labs\Evidence**, click **Make New Folder**, and type **Chap5** for the new name. Click **OK** to copy the file, and click **OK** in the Export Results message box.

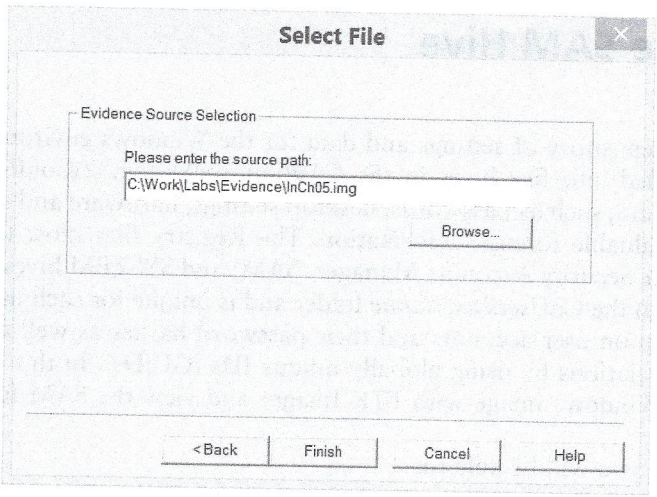



**Figure 5-4** Entering a source path for the image



5. In the left pane, click to expand **Windows** and **System32**, and then click **config**. Ctrl+click **SYSTEM**, **SOFTWARE**, **SECURITY**, **SAM**, and **DEFAULT**. Right-click one of these selected files and click **Export Files**. Navigate to and click **C:\Work\Labs\Evidence\Chap5**, and click **OK** to copy the files. Click **OK** in the Export Results message box, and then exit FTK Imager.
6. Right-click the **AccessData Registry Viewer** desktop icon and click **Run as administrator**. If necessary, click **Yes** in the UAC message box. Click **Yes** in the ERROR dialog box, click **Cancel** in the Security Device Settings dialog box, and click **OK** in the Registry Viewer dialog box to start Registry Viewer in demo mode.
7. Click **File**, **Open** from the menu. Navigate to and click **C:\Work\Labs\Evidence\Chap5\SAM**, and then click **Open**.
8. Click to expand the **SAM**, **Domains**, **Account**, and **Users** folders. Click the **000001F4** folder, and drag to enlarge the Key Properties pane at the lower left. Notice the last logon time and the SID unique identifier field, which indicates the type of account and whether it's created automatically when the OS is installed. Values of 500, 501, and 1000 show default accounts (created automatically). This user account is Administrator, and it has been logged on to three times (see Figure 5-5).
9. Click the **000003E9** folder. The jfriday account has been logged on to seven times, and the SID value 1001 indicates that this account was created.
10. Click the **000003EC** folder. The Denise Robinson account, which was created, has never logged on to the computer.
11. Click to expand the **Names** folder, and then click the **jfriday** folder. The Last Written Time entry indicates that this account was accessed on 2/6/2014 when the password was changed.

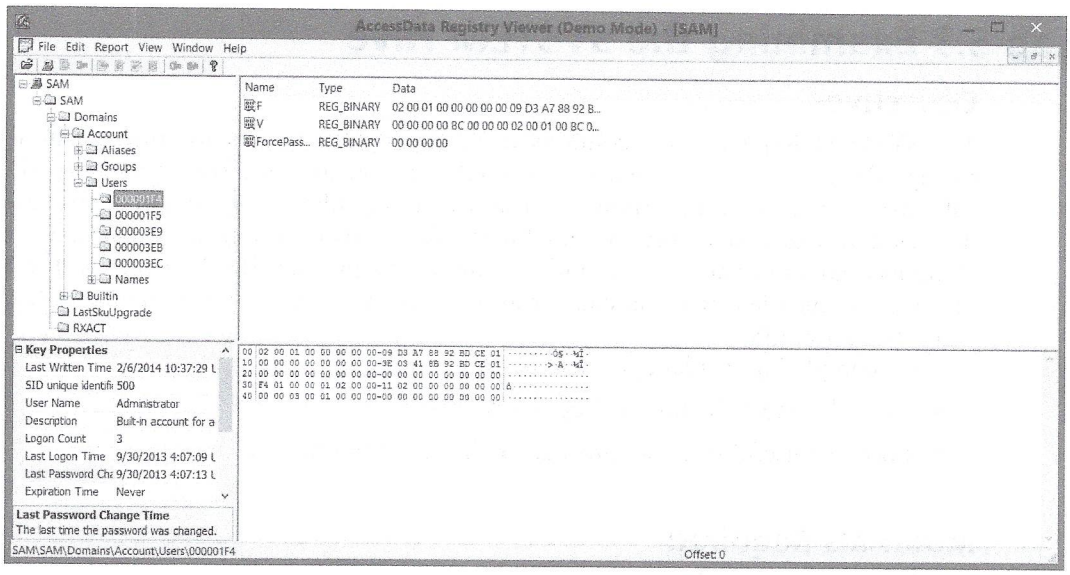



**Figure 5-5** Viewing user account information



12. Leave Registry Viewer open as you answer the following review questions. When you're finished, exit Registry Viewer, and leave your computer running for the next lab.

## Review Questions

1. The Registry contains how many hives?
   a. Three
   b. Two
   c. Five
   d. Six
2. How many user accounts are disabled?
   a. Two
   b. Seven
   c. One
   d. Three
3. The SAM hive uses PIDs to store information on user accounts. True or False?
4. Name two SID values that indicate whether an account was created automatically.
5. The Key Properties pane in Registry Viewer shows when user accounts have changed their passwords. True or False?

# Lab 5.3 Examining the SYSTEM Hive

## Objectives

The SYSTEM Registry hive contains drive letter designations for internal and external storage devices, the system name, and configuration data for the system's hardware and software. This hive is important because it can help identify a computer and any storage devices that might have been mounted in the OS. It also contains information on when the Windows partition was created and activated. The product ID (PID) key in the SYSTEM hive is a unique identifier that can act as an electronic fingerprint to identify a legally activated Windows OS.

After completing this lab, you will be able to:

- View the SYSTEM hive in Registry Viewer
- Look for useful forensic information in the SYSTEM hive

## Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- AccessData Registry Viewer
- The SYSTEM hive copied from the DVD's data files to your C:\Work\Labs\Evidence folder

Estimated completion time: **15 minutes**

## Activity

In this lab, you examine the SYSTEM hive to determine the user accounts on the seized computer:

1. Right-click the **AccessData Registry Viewer** desktop icon and click **Run as administrator**. If necessary, click **Yes** in the UAC message box. Click **Yes** in the ERROR dialog box, click **Cancel** in the Security Device Settings dialog box, and click **OK** in the Registry Viewer dialog box to start Registry Viewer in demo mode.
2. Click **File, Open** from the menu. Navigate to and click **C:\Work\Labs\Evidence\Chap5\SYSTEM**, and then click **Open**.
3. In the left pane of Registry Viewer, click to expand the **ControlSet001** folder, the **Control** folder, and the **ComputerName** folder, and then click the **ComputerName** folder to display the name at the upper right.
4. Scroll down and click the **TimeZoneInformation** folder to display the computer's time zone information. This information is critical because timestamps for files, folders, and logs are based on the time zone (see Figure 5-6).

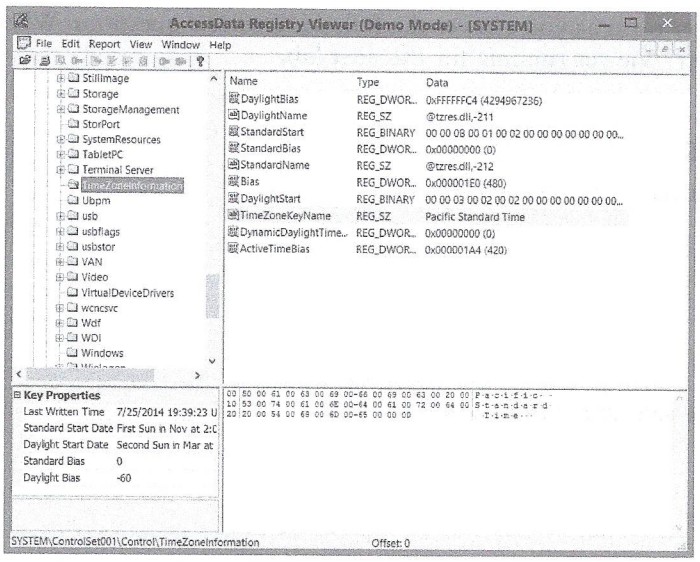



**Figure 5-6** Viewing time zone information



5. Click to expand the **Enum** folder and the **IDE** folder, which contains IDE storage devices, such as the CD/DVD-ROM drive. Click to expand the **USB** folder to see all USB storage devices plugged into the computer. Each storage device has a unique serial number and a Last Written Time entry in the Key Properties pane.
6. Click the **MountedDevices** folder, which lists every storage device that has been mounted in the Windows OS along with its associated drive letter and GUID value (see Figure 5-7). This information can be used to associate hard drives with a Windows computer.

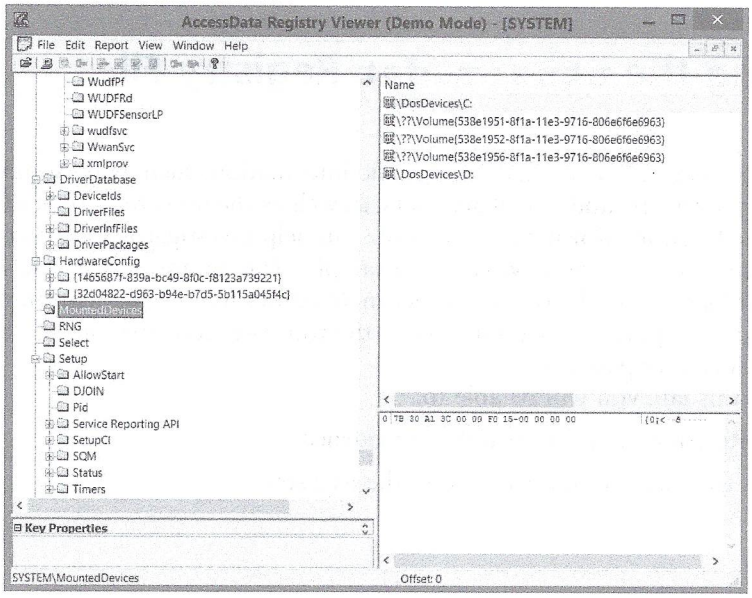



**Figure 5-7** Viewing information on mounted devices

7. Leave Registry Viewer open as you answer the following review questions. When you're finished, leave Registry Viewer running for the next lab.

### Review Questions

1. What's the computer name of this system?
   a. mnmsrv
   b. GCFI5E
   c. HAL
   d. MSDTC
2. What's the time zone setting for this computer?
   a. EST
   b. MST
   c. CST
   d. PST
3. How many mounted devices on this system have assigned drive letters?
4. What information is stored in the Enum folder?
   a. User account information
   b. Password information
   c. File locations
   d. Hardware and software values
5. The SYSTEM hive contains configuration data for passwords. True or False?

## Lab 5.4 Examining the `ntuser.dat` Registry File

### Objectives

The `ntuser.dat` Registry file contains user-specific information, such as personalized settings for the desktop, software, and e-mail accounts, as well as the most recently used (MRU) files and devices. The forensic information in this file can help investigators discover Internet searches and recently used storage devices, for example. The `ntuser.dat` file is in the C:\Users*username* folder, and each account holder in Windows has a separate `ntuser.dat` file. Many password decryption tools require both the `ntuser.dat` file and the SYSTEM Registry hive to retrieve user passwords.

After completing this lab, you will be able to:

- Load a file in Registry Viewer to search for evidence
- Find Windows user account information in the Registry

## Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- AccessData Registry Viewer
- The `ntuser.dat` file extracted in Lab 5.2

Estimated completion time: **15 minutes**

## Activity



In this lab, you examine the `ntuser.dat` file belonging to a suspect's user account for forensics evidence:

1. If necessary, right-click the **AccessData Registry Viewer** desktop icon and click **Run as administrator**. Click **Yes** in the UAC message box. Click **Yes** in the ERROR dialog box, click **Cancel** in the Security Device Settings dialog box, and click **OK** in the Registry Viewer dialog box to start Registry Viewer in demo mode.
2. Click **File, Open** from the menu. Navigate to and click **C:\Work\Labs\Evidence\Chap5\ntuser.dat**, and click **Open**.
3. Click **Edit, Find** from the menu. In the Find dialog box, type **Denise** and press **Enter**. The first Registry key associated with Denise is displayed at the upper right.
4. Press the **F3** key to search for the next Registry key containing any references to Denise. Notice the GUID associated with the username account information. Press **F3** again to locate the next key, and notice the e-mail account for Denise along with her full name (see Figure 5-8).

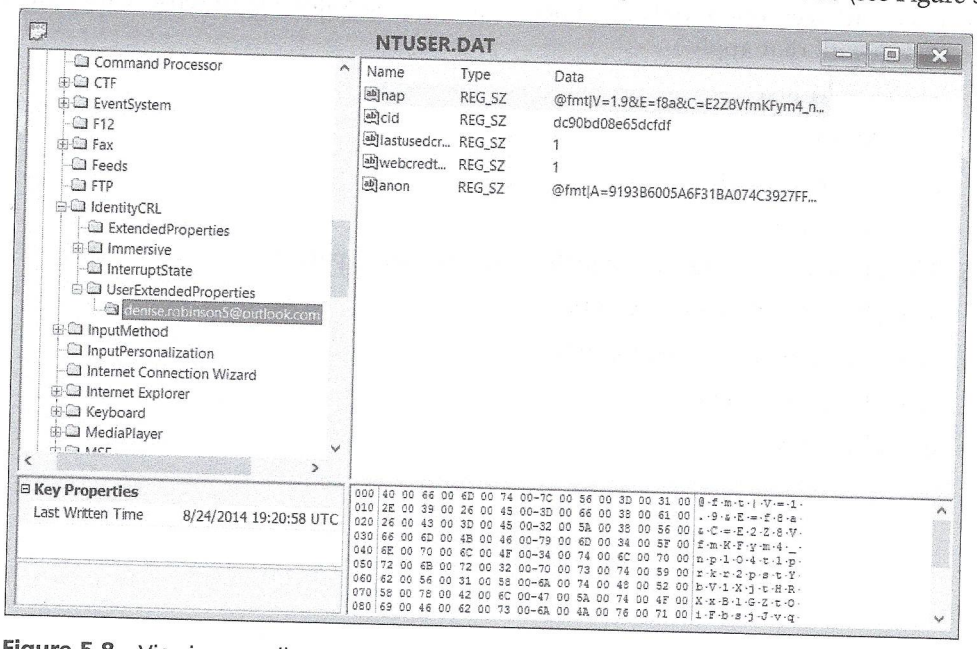



**Figure 5-8** Viewing e-mail account information

5. Click **Edit, Find** from the menu. In the Find dialog box, type **jfriday** and press **Enter** to search for any Registry keys associated with this suspect. A message is displayed stating that Registry Viewer couldn't locate any keys associated with this user. This happened because each `ntuser.dat` file is associated with only one user account.
6. Leave Registry Viewer open as you answer the following review questions. When you're finished, close all open windows and shut down the computer.

## Review Questions

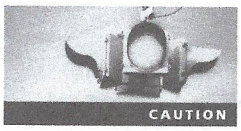
1. The `ntuser.dat` file contains information on multiple account holders. True or False?
2. What's the e-mail account for the Denise user?
   a. Denise.Robertson@.comcast.net
   b. Denise@AOL.com
   c. denise.robinson5@outlook.com
   d. denise.robinson5@comcast.net
3. The `ntuser.dat` file contains information on which of the following? (Choose all that apply.)
   a. Drive letter designations
   b. Personalized desktop settings
   c. PID key
   d. MRU devices
4. Password decryption tools often need which of the following to retrieve user passwords? (Choose all that apply.)
   a. SYSTEM hive
   b. SAM hive
   c. `ntuser.dat` file
   d. Enum folder
5. The `ntuser.dat` file is in which of the following paths?
   a. C:/Windows/System32/Config
   b. C:/Documents and Settings/Users
   c. C:/Users/*username*
   d. C:/SYSTEM

# Part 2

# Lab 6.1 Using Autopsy to Search an Image of a Hard Drive

## Objectives

Autopsy is a free open-source digital forensics tool that serves as a Web-based interface to Sleuth Kit; it's also available in a version for Windows. It offers features for producing reports and includes timeline analysis, hash filtering, keyword searches, and searches for Web artifacts, such as bookmarks, history, and cookies, in Firefox, Chrome, and Internet Explorer. In addition, Autopsy can recover deleted files and extract Exif information from multimedia files. It produces fast results by running background tasks in parallel processes that can take advantage of multicore processors. In this lab, you examine the `charlie-2009-12-03.E01` image file to look for e-mail evidence containing the keyword "Project2400" and explore the timeline features in Autopsy.




Processing the data file used in this chapter can take quite a long time in Autopsy, depending on your computer's performance and the amount of RAM, so you might want to set it up to take place overnight.

After completing this lab, you will be able to:

- Search an image file in Autopsy
- Use the timeline analysis features in Autopsy

## Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- Autopsy 3.1.2 for Windows
- The `charlie-2009-12-03.E01` file

Estimated completion time: **120–240 minutes,** depending on your computer's performance

## Activity

In this lab, you use Autopsy to search an image on a Windows computer:

1. Start a Web browser, and go to **http://sourceforge.net/projects/autopsy/files/autopsy/3.1.2/**. Double-click the **`.msi`** file to download and install Autopsy 3.1.2 for Windows. (*Note*: Choose the 32-bit or 64-bit version, depending on your Windows version.)
2. Next, go to **http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/drives-redacted/**, scroll down, and download the **`charlie-2009-12-03.E01`** file to the **C:\Work\Labs\Evidence** folder on your computer.

3. Double-click the **Autopsy** desktop icon. In the Welcome window, click **Create New Case.**
4. Type **C6Proj1** in the Case Name text box. Click **Browse**, navigate to and click the **C:\Work\Labs\Cases** folder, click **OK** to enter this path in the Base Directory text box (see Figure 6-1), and then click **Next**. Type **C6Proj1** in the Case Number text box and your initials in the Examiner text box, and then click **Finish.**

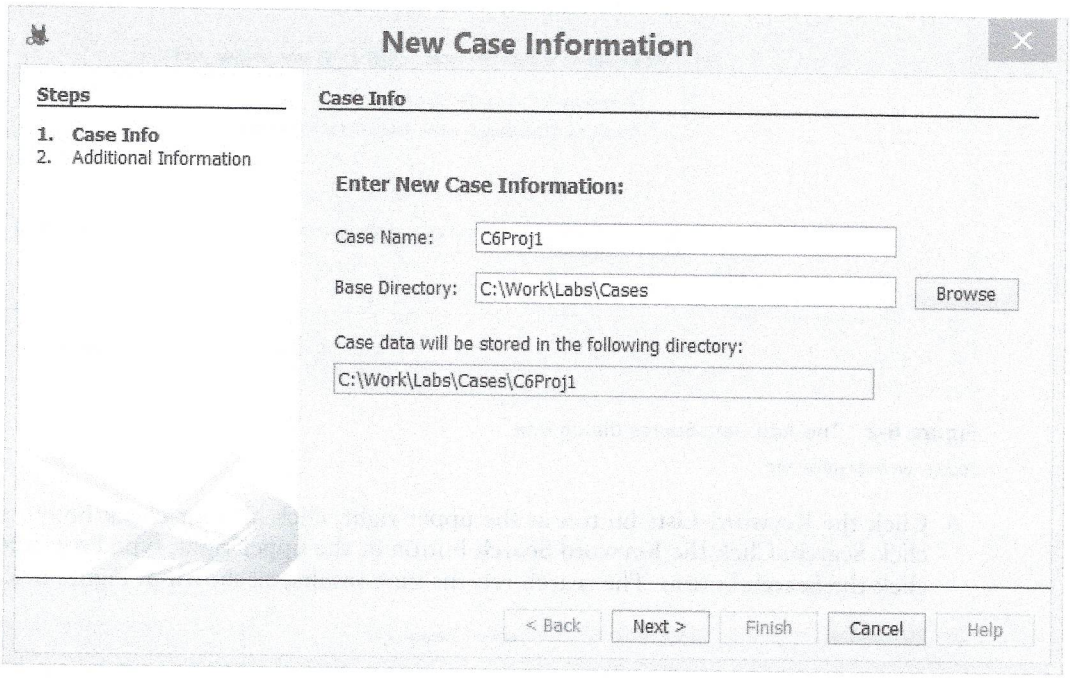



**Figure 6-1** Entering new case information

*Source:* www.sleuthkit.org

5. In the Add Data Source dialog box, click **Browse**, navigate to and click the **charlie-2009-12-03.E01** file you downloaded from the M57 site, click **OK** to enter this path (see Figure 6-2), and then click **Next**. In the Configure Ingest Modules dialog box, click **Next**, and then click **Finish** to start analyzing the evidence. Watch the progress bar in the lower-right corner to determine when the process is finished.

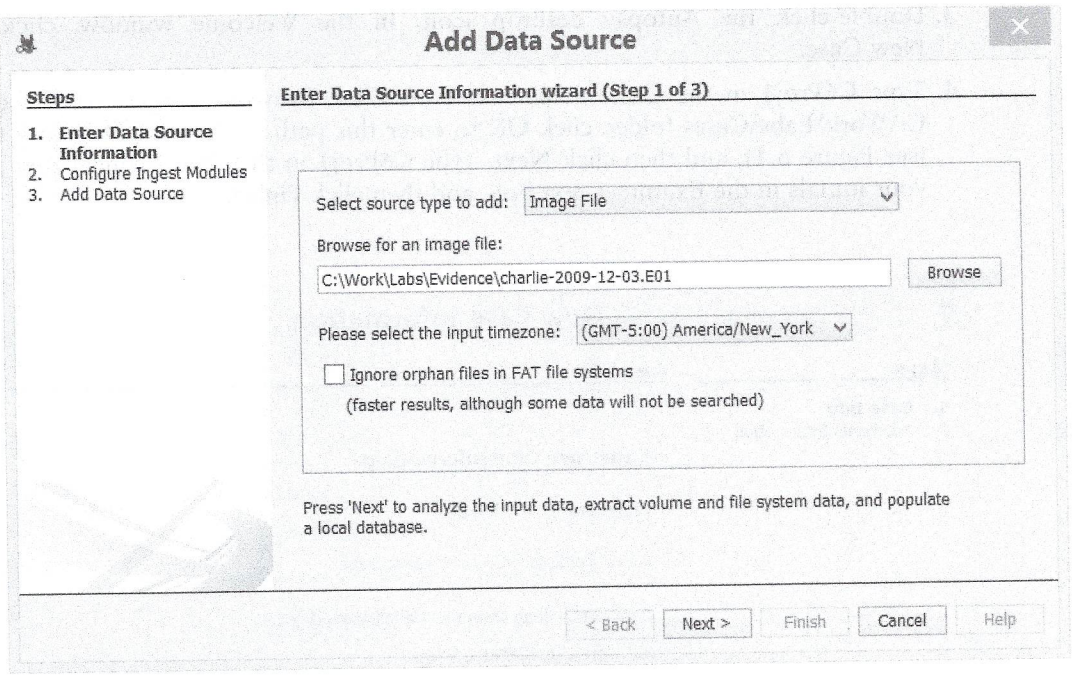



**Figure 6-2** The Add Data Source dialog box

*Source:* www.sleuthkit.org

6. Click the **Keyword Lists** button at the upper right, click all four check boxes, and then click **Search**. Click the **Keyword Search** button at the upper right, type **Project2400**, and click the **Search** button. The search returns nine results, as shown in Figure 6-3.

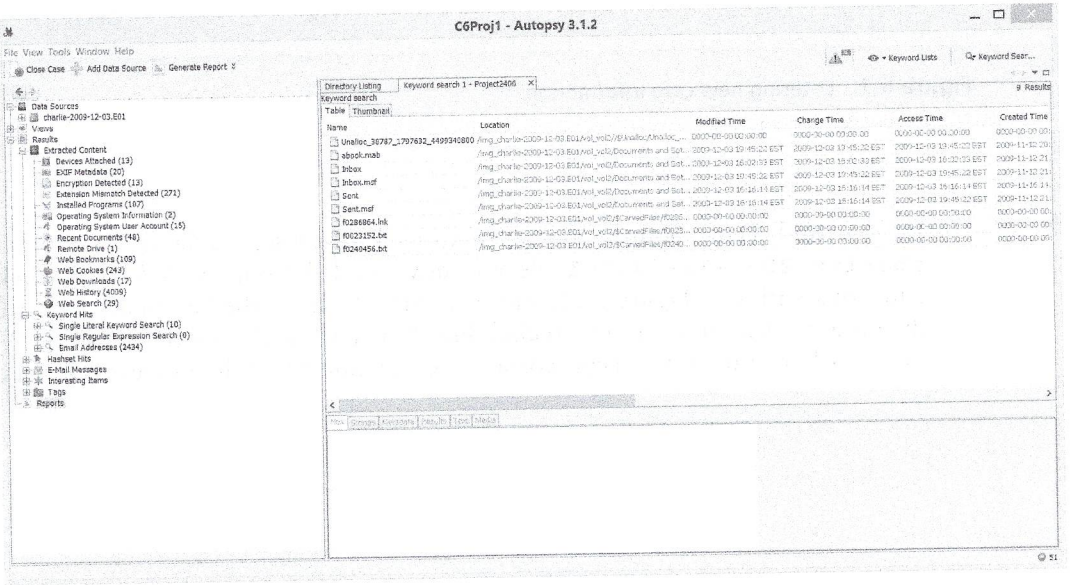



**Figure 6-3** Search results displayed in Autopsy

*Source:* www.sleuthkit.org

7. Click the **Inbox** entry in the right pane, and notice that the Project2400 results are highlighted in yellow. Scroll through the results to find any evidence of Charlie receiving e-mails referencing Project2400. Click the **Sent** entry in the right pane, and look for e-mails sent about Project2400 (see Figure 6-4).

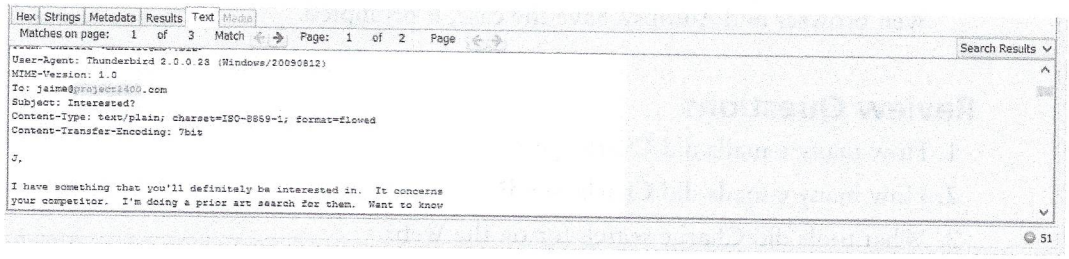



**Figure 6-4** Viewing sent e-mails

*Source:* www.sleuthkit.org



8. Click **Tools, Timeline** from the menu. This process takes a few minutes. By default, the timeline is displayed with a large date range. In this case, you're interested in the period between November 16, 2009, and December 9, 2009. In the Timeline Window - Editor dialog box, click the clock icon in the right pane at the lower left, set the date to **November 16, 2009**, and use the sliders under the calendar to set the time to **12:00 AM** (see Figure 6-5). Use the same procedure to enter the end date and time: **December 9, 2009** at **11:59 PM**. Click the **Filters** tab at the lower left, type **Project2400**, click the **Text Filter** check box, and then click the **Apply** button. Click the **Counts** button to see dates with activity involving project2400. These dates are shown by the columns indicating number of hits. Click the **Details** button to see the e-mails for this filename. You can ignore the Updating Counts Graph indicator during processing. Move your mouse pointer over each event to see details. When you're finished, close this dialog box.

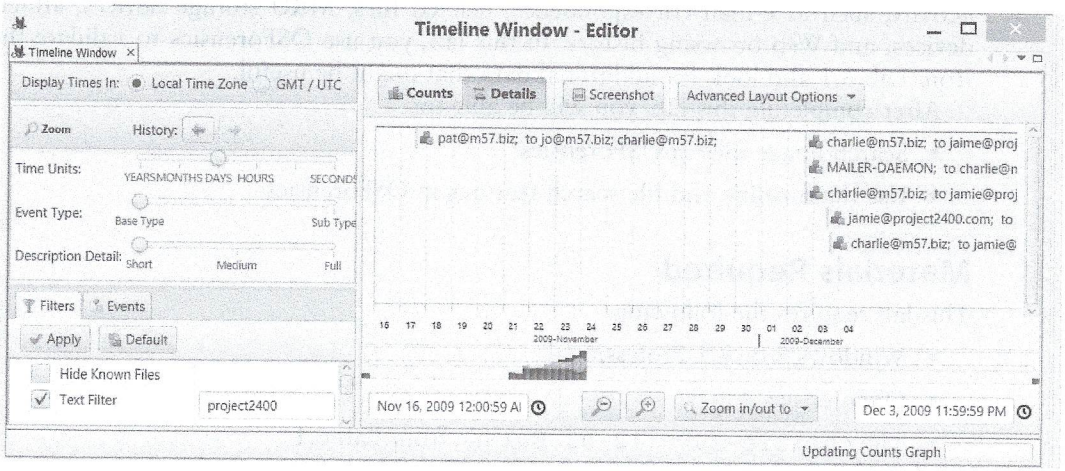



**Figure 6-5** Entering timeline settings

*Source:* www.sleuthkit.org

9. Click **Tools**, **Generate Report** from the menu. In the Generate Report dialog box, click **Results - HTML**, and then click **Next**. Click **All Results**, and then click Finish.
10. When the green check mark is displayed, click the **Results - HTML** link, and leave the report open as you answer the following review questions. When you're finished, exit the Web browser and Autopsy. Save the case, if prompted.

## Review Questions

1. How many e-mails did Charlie get?
2. How many e-mails did Charlie send?
3. What tools did Charlie search for on the Web?
4. Did Charlie install any tools on this computer?
5. How many cameras can be identified by checking the Exif information?
   a. 20
   b. 26
   c. 10
   d. 5

# Lab 7.1 Using Autopsy to Process a Mac OS X Image

## Objectives

The Windows version of Autopsy features the Android Analyzer, which can extract SMS and MMS text messages, call logs, contact information, and GPS data from Google Maps used on Android mobile devices. In Autopsy 3, you can analyze `.E01` and `.dd` images from Linux, UNIX, Mac OS, and Windows file systems. The HFS+ or Mac OS Extended file system was introduced with OS X 10.3 and is used in the current 10.10.2 version, known as Yosemite. This improved version of HFS supports the large disk sizes in current computers. In this lab, you import an OS X image into Autopsy and process it to look for potential evidence.

After completing this lab, you will be able to:

- Import an OS X image into Autopsy
- Use Autopsy to search for evidence in an OS X image

## Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- Autopsy for Windows
- The `GCFI-OSX.zip` file on the DVD


This file might take several hours to process, depending on your computer's performance.

Estimated completion time: **180–240 minutes**

## Activity

In this lab, you import an OS X image into Autopsy to process evidence:

1. Extract the **`GCFI-OSX.zip`** file to your **C:\Work\Labs\Evidence** folder. (This process might take a few minutes.) Start Autopsy for Windows. In the Welcome window, click **Create New Case**. Type **C7Proj1** in the Case Name text box, verify that **C:\Work\Labs\Cases** is displayed in the Base Directory text box, and then click **Next**.
2. In the New Case Information dialog box, type **C7Proj1** in the Case Number text box and your initials in the Examiner text box, and then click **Finish**.
3. In the Add Data Source dialog box, click **Browse**, navigate to the **C:\Work\Labs\Evidence\OSX** folder, click the **`GCFI-OSX.001`** file, and then click **Open**. Click **Next**.
4. Click **Next** to accept the ingest modules, and then click **Finish** to start analyzing the evidence, which could take a while. Figure 7-1 shows the results.

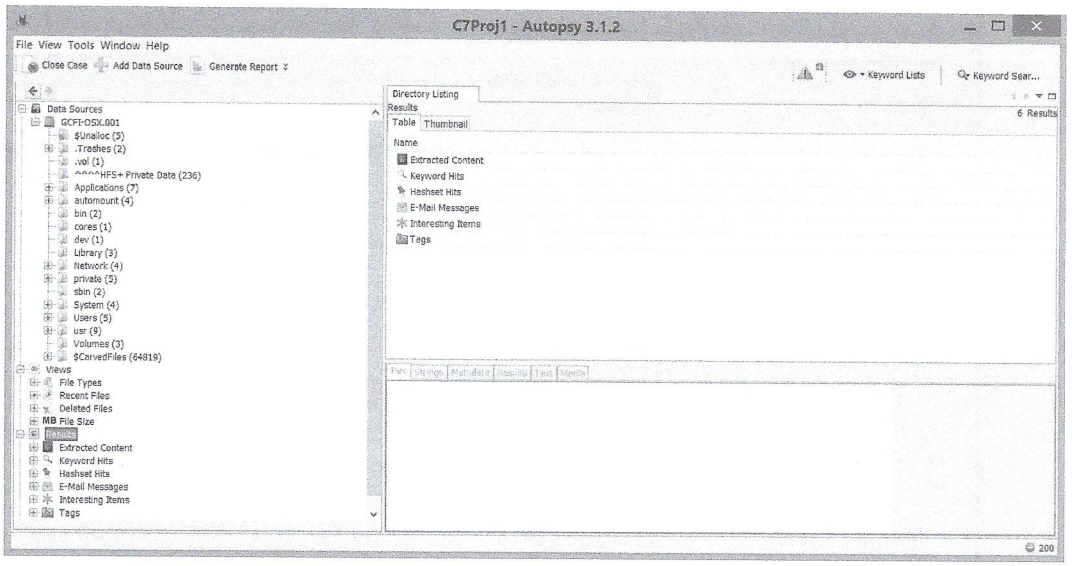



**Figure 7-1** Viewing the results in Autopsy

*Source:* www.sleuthkit.org

5. Click the **Keyword Lists** button at the upper right. Click the **Phone Numbers, IP Addresses, Email Addresses,** and **URLs** check boxes, and then click the **Search** button. Autopsy begins searching the image, which could take some time.
6. Click the **Keyword Search** button, type **Jim Shu** in the text box, and click **Search.** When the search is finished, click the **Keyword search 2** tab, if necessary. The first section of files consists of unallocated and carved files that might have been deleted or cache files. Click the **Table** tab, if necessary, and then click the second unallocated space from the top to display the text associated with search results for Jim Shu.
7. Scroll to the right to display all the file attributes, such as location, timestamps, size, file types, MD5 hash sets, and keyword previews (see Figure 7-2).
8. In the left pane, expand **`GCFI-OSX.001`** to view the file system folders in the image along with the number of files or folders in each folder. Next, expand **Views** and **File Types** and then click **Images** to see all the graphics files (which might take some time). Click the **Thumbnail** tab to see the graphics.
9. In the left pane, expand **Documents** to view the file types and the number of hits. Click **Office** and then click the **Table** tab, if necessary, to see the Word documents. Click a document to view it in the lower-right pane.
10. In the left pane, expand **Keyword Hits,** if necessary, and then expand **Phone Numbers, IP Addresses, Email Addresses,** and **URLs** to see the search results. Expand **E-Mail Messages** to view correspondence with Jim Shu, including sent messages, deleted messages, the inbox, and so forth.
11. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy, but leave your computer running for the next lab.

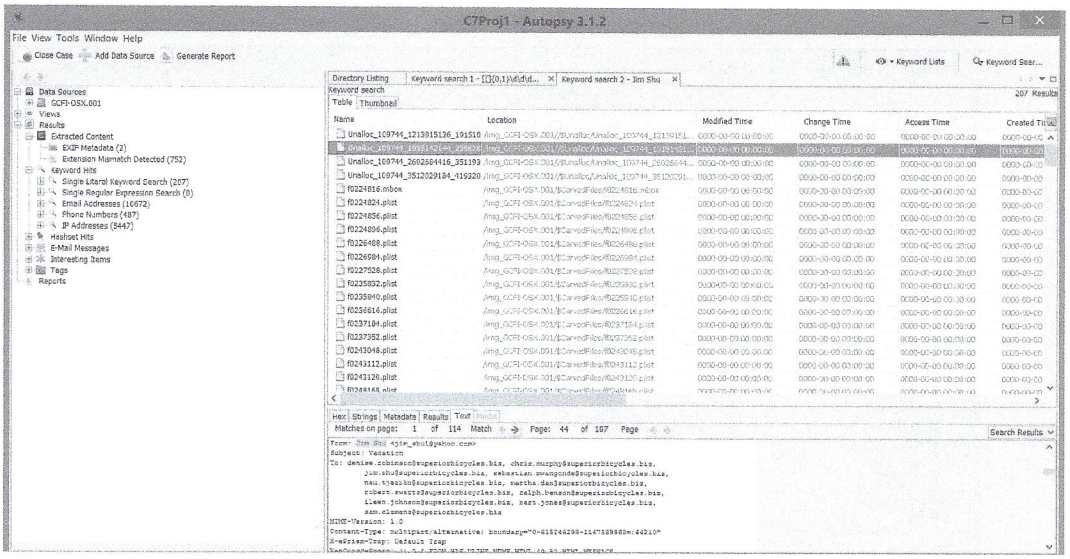



**Figure 7-2** Viewing file attributes

*Source:* www.sleuthkit.org

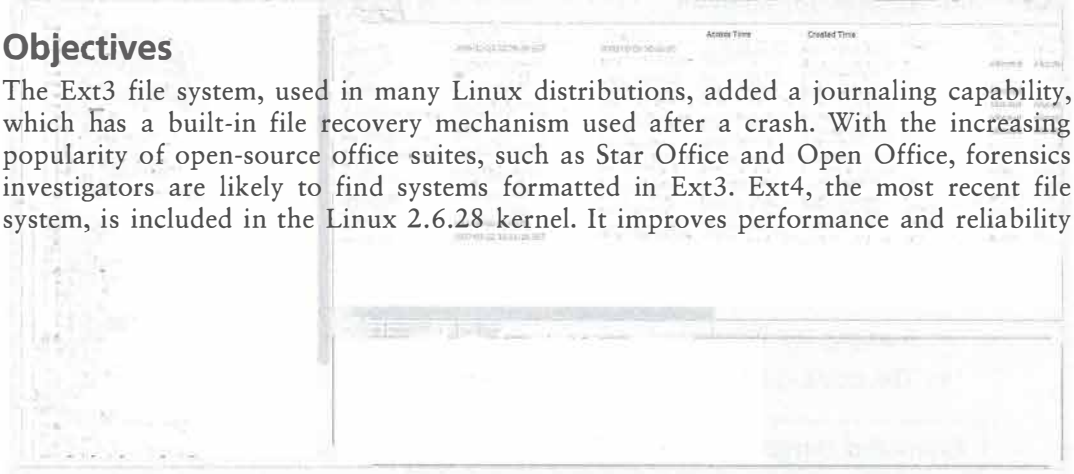
## Review Questions

1. How many Word files are in the image?
2. What or who is the subject of the first message from Jim Shu?
   a. Sebastian
   b. Jim Shu
   c. Superior Bicycles
   d. Free tools
3. What phone number had the most search results?
   a. 602-839-2763
   b. 800-810-0595
   c. 662-656-5045
   d. 859-232-2380
4. The Ext3 file system is used in Mac OS X. True or False?
5. Who sent the last e-mail to Jim Shu?
   a. Martha Dax
   b. Sebastian Mwangonde
   c. Nau Tjeriko
   d. Bart Johnson

# Lab 7.3 Using Autopsy to Process a Linux Image

## Objectives

The Ext3 file system, used in many Linux distributions, added a journaling capability, which has a built-in file recovery mechanism used after a crash. With the increasing popularity of open-source office suites, such as Star Office and Open Office, forensics investigators are likely to find systems formatted in Ext3. Ext4, the most recent file system, is included in the Linux 2.6.28 kernel. It improves performance and reliability



and maintains backward-compatibility with Ext3. Autopsy can be used to search images formatted in this file system, too. In this lab, you extract a Linux image and import it into Autopsy for analysis.

After completing this lab, you will be able to:

- Import a Linux image into Autopsy
- Use Autopsy to search for evidence on a Linux partition

## Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- Autopsy for Windows
- The `GCFI-LX.xxx.exe` file on the DVD

Estimated completion time: **180–240 minutes**

## Activity

In this lab, you import a Linux image into Autopsy to process evidence:

1. Extract the **`GCFI-LX.xxx.exe`** file to your **C:\Work\Labs\Evidence** folder, which might take a few minutes. Start Autopsy for Windows. In the Welcome window, click **Create New Case**. Type **C7Proj3** in the Case Name text box, verify that **C:\Work\Labs\Cases** is displayed in the Base Directory text box, and then click **Next**.
2. In the New Case Information dialog box, type **C7Proj3** in the Case Number text box and your initials in the Examiner text box, and then click **Finish**.
3. In the Add Data Source dialog box, click **Browse**, navigate to the **C:\Work\Labs\Evidence** folder, click the **`GCFI-LX.001`** file, and then click **Open**. Click **Next**.
4. Click **Next** to accept the ingest modules, and then click **Finish** to start analyzing the evidence, which could take a few hours, depending on your computer's performance. The progress bar shows 100% when the processing is finished.
5. In the left pane, expand **`GCFI-LX.001`** to view the folder structure (see Figure 7-5). This structure is common in many Linux distributions. Right-click **GCFI-LX.001** to see these available options: Image Details, Extract Unallocated Space to Single Files, Open File Search by Attributes, and Run Ingest Modules (used to process the image again).

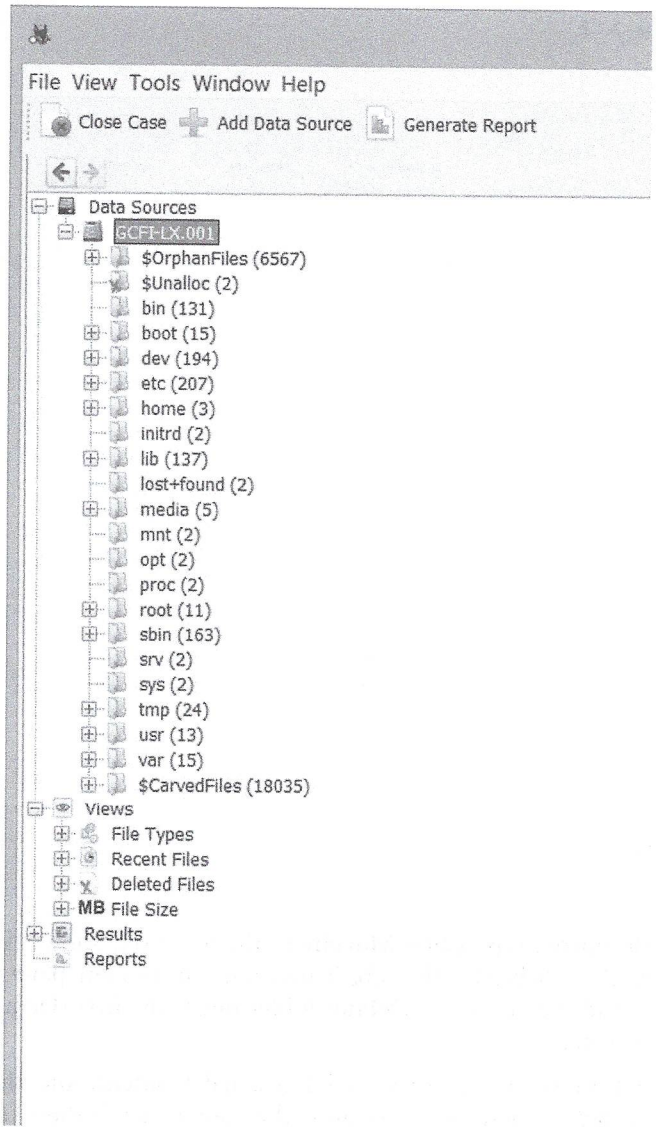



**Figure 7-5** Viewing the folder structure

*Source:* www.sleuthkit.org

6. Click the **Keyword Search** button, type **martha** in the text box, and click **Search.** In the right pane, click the **Keyword search 1 - martha** tab, if necessary, to view all the search results. Click the **Sent** entry to view the e-mail Martha Dax sent to Chris Murphy (see Figure 7-6).

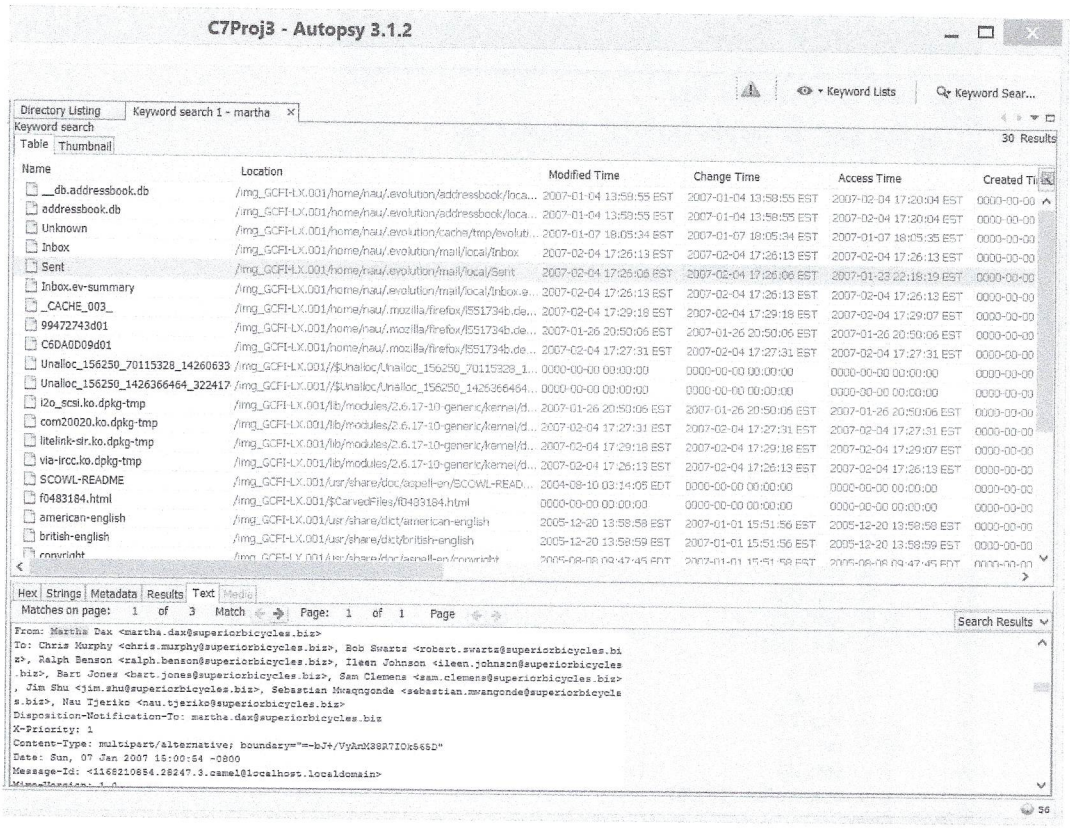



**Figure 7-6** Viewing sent e-mails

*Source:* www.sleuthkit.org

7. Click the **Keyword Search** button, type **Chris Murphy** in the text box, and click **Search**. Click the **Keyword search 2 - Chris Murphy** tab, if necessary. In the left pane, click to expand **E-Mail Messages**, and then click the **Default** folder under the first [Default] icon to see all e-mail correspondence.
8. In the left pane, expand **Results**, if necessary, and **Extracted Content**, and then click **Extension Mismatch Detected** to view file extensions that don't match their file types. This information might reveal files that have been altered to keep them hidden.
9. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy, and shut down your computer.

## Review Questions

1. How many e-mails were recovered from the inbox?
2. How many Word and Excel files were recovered in this image?
3. Martha communicated via e-mail only with Chris Murphy. True or False?
4. What executable file was recovered in this image?
5. How many matches were found for the Martha keyword?