Current Digital Forensics Tools

Note: Before starting these labs, create a subfolder of your work folder named Ch06.

Lab 6.1 Using Autopsy 4.7.0 to Search an Image File

Objectives

After completing this lab, you will be able to:

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

Autopsy 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.

Digital forensics tools are constantly improving in capabilities and functions. As a digital forensics examiner, you must learn how to use several tools so that if one tool fails, you can switch to another one. Sometimes tools you've relied on don't always work. In these situations,

check whether any updated versions are available that might correct the problem you've encountered.

In this lab, you examine an image file that has the first sector area altered, making it unreadable with Autopsy version 4.3.0 that you installed in Chapter 1. You need to download and install Autopsy 4.7.0 (or the most current version), and then search for e-mail evidence containing the keyword "Project2400" and explore the timeline features. The image file with the altered first sector is charlie-2009-12-03.E01.

This lab is divided into two sections: The first explains how to download and install Autopsy 4.7.0, and the second shows you how to analyze the evidence.

Materials Required

This lab requires the following:

- Windows
- Internet access
- Autopsy 4.7.0, downloaded in the first section
- The charlie-2009-12-03.E01 file, downloaded in the second section

Estimated completion time: 240–480 minutes

Caution

> Processing the data file used in this lab could take more than 4 hours, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

Lab 6.1 Activity

Installing Autopsy 4.7.0

In this lab, you download and install Autopsy 4.7.0:

1. Open File Explorer, and create a subfolder of your work folder called **Autopsy**. Start a Web browser, and go to https://www.autopsy.com/download/. Download the 32-bit or 64-bit installation file to your *Work/*Autopsy folder.
2. In File Explorer, navigate to your ***Work/*Autopsy** folder. Right-click autopsy-4.7.0-*nn*bit.msi (replacing *nn* with 32 or 64, depending on your computer) and click **Install** to begin the installation. If prompted with the UAC message box, click **Yes** to continue.
3. In the Autopsy Setup Wizard welcome window, click **Next**, and in the Select Installation Folder window, click **Next**. In the Ready to Install window, click **Install**.
4. In the Completing the Autopsy Setup Wizard window, click **Finish**, and then exit Autopsy.

Note : After installing Autopsy 4.7.0, you should have two desktop icons: one for Autopsy 4.3.0 and one for Autopsy 4.7.0. Both programs run separately.

Searching E-mail in Autopsy 4.7.0

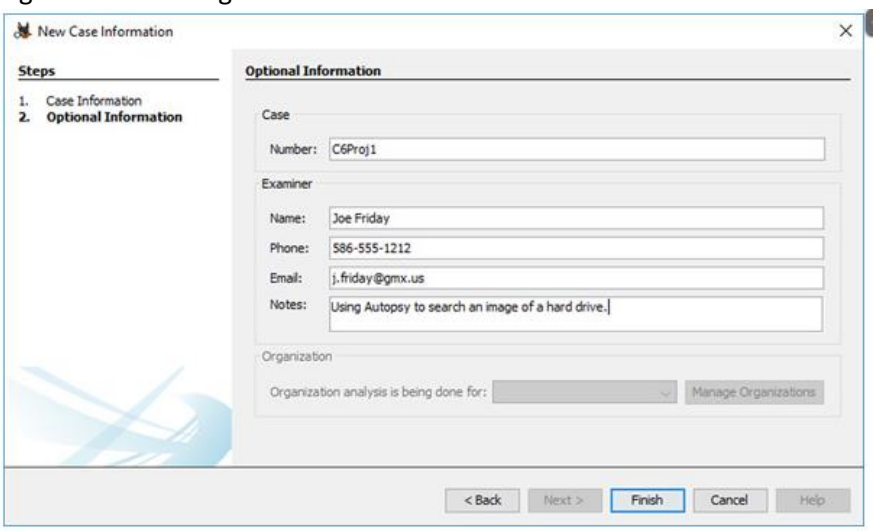
In this lab, you use Autopsy to search an image on a Windows computer:

1. Start a Web browser, if necessary, and go to http://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/. Scroll down, and download **charlie-2009-12-03.E01** file to your work folder.

   http://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/charlie-2009-12-03.E01

2. Start Autopsy 4.7.0, and in the Welcome window, click the **Create New Case** button.
3. In the New Case Information window, type **C6Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Optional Information window, type **C6Proj1** in the Number text box and your name in the Name text box (see Figure 6-1), and then click **Finish**.

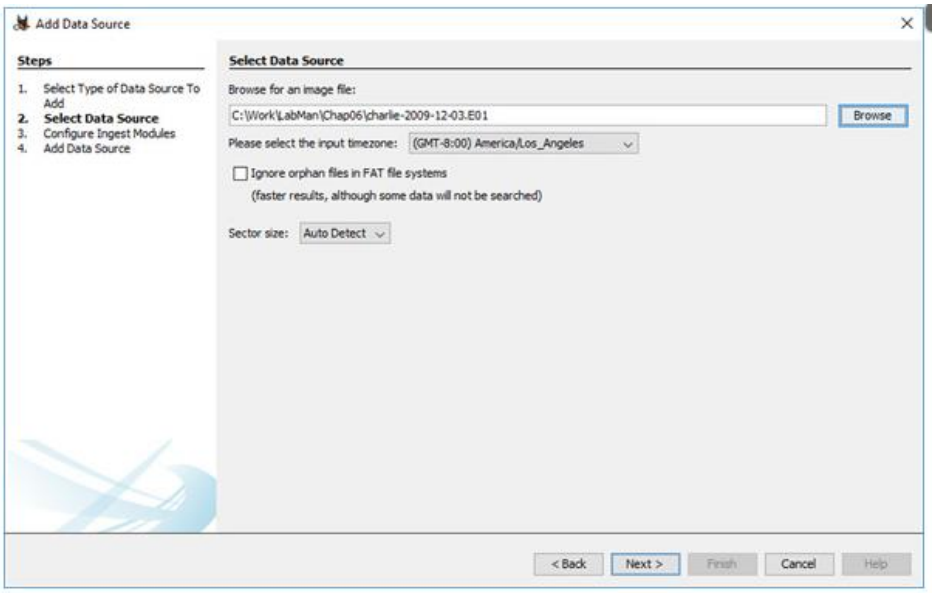
Figure 6-1 Entering case information



Source: www.sleuthkit.org

4. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click **charlie-2009-12-03.E01**, and then click **Open** (see the result in Figure 6-2). Click **Next**.

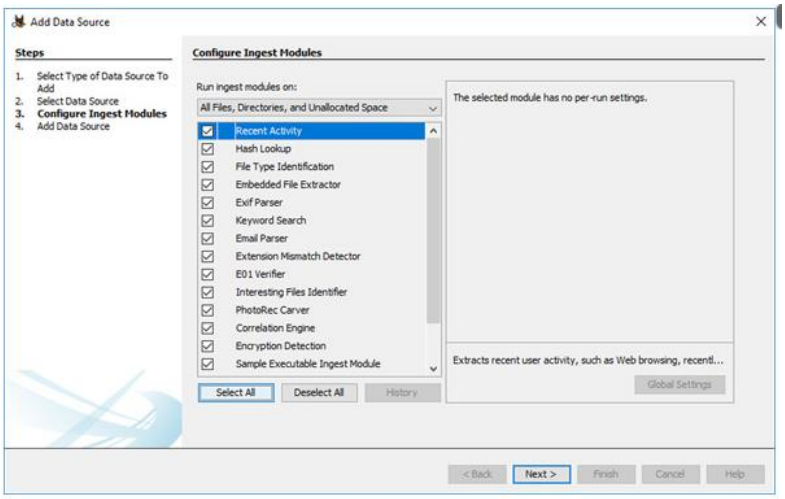
Figure 6-2 Adding an image file



Source: www.sleuthkit.org

5. In the Configure Ingest Modules window, click **Select All** (see Figure 6-3), and then click **Next** and **Finish** to start analyzing the evidence. (See the Caution at the beginning of this lab about the time this process might take.)

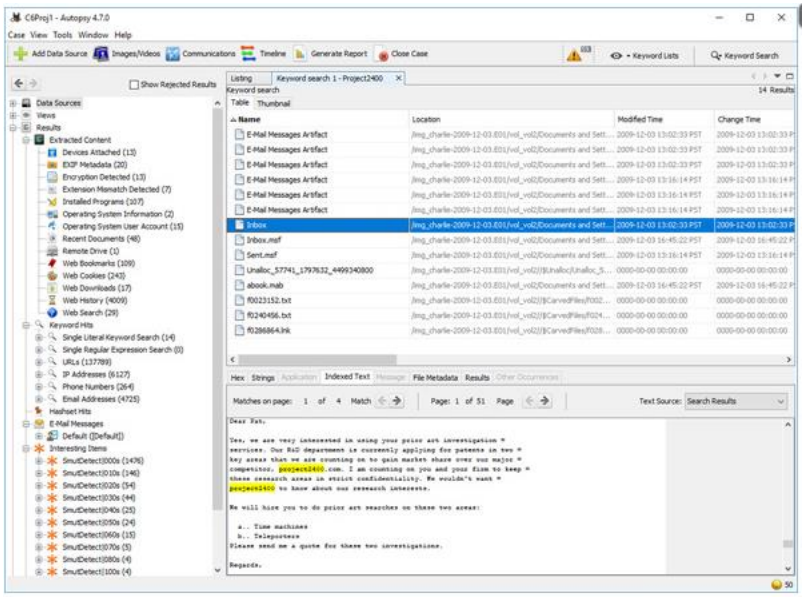
Figure 6-3 Selecting ingest modules



Source: www.sleuthkit.org

6. Click **Keyword Search** at the upper right, type **Project2400** in the text box, and click the **Search** button. The search should return 14 results.
7. Click the **Keyword search 1 - Project2400** tab in the Result Viewer pane, and then click the **Inbox** entry. Notice that the search results for Project2400 are highlighted in yellow in the Content Viewer pane (see Figure 6-4).

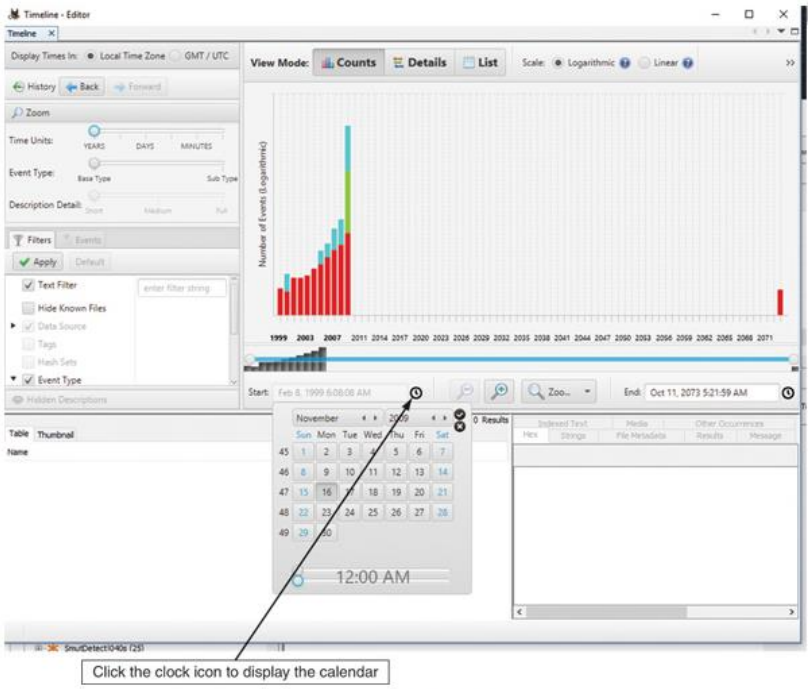
Figure 6-4 Search results displayed in Autopsy



Source: www.sleuthkit.org

8. Click the **Timeline** toolbar button. 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. Expand the Timeline - Editor dialog box to make it easier to read, and then click the **clock** icon at the bottom of the upper-right pane. In the calendar, set the starting date to **November 16, 2009**, use the sliders under the calendar to set the time to **12:00 AM**, and click the **check mark** icon (see Figure 6-5). Use the same procedure to enter the ending date and time: **December 9, 2009** and **11:59 PM**.

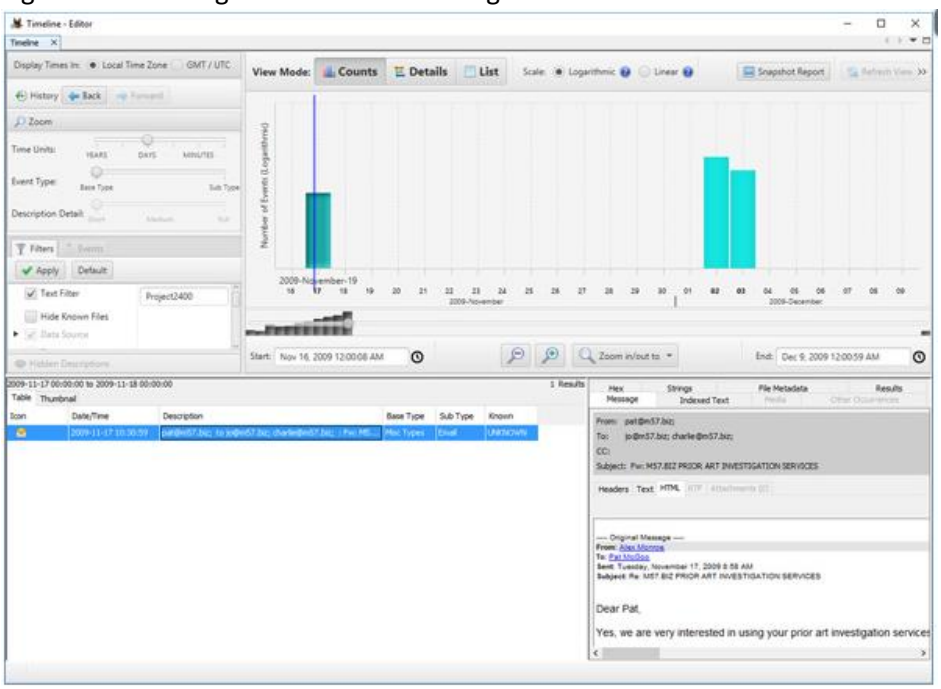
Figure 6-5 Entering timeline settings



Source: www.sleuthkit.org

9. Click the **Filters** tab, if necessary, on the left. Type **Project2400** in the Text Filter text box, click to select the **Text Filter** check box, and then click the **Apply** button. Click the **Counts** button at the top of the upper-right pane, if necessary, and then click the leftmost bar graph. Click the message displayed in the lower-left pane and view its contents in the lower-right pane (see Figure 6-6). The bar graph heights indicate the number of e-mails per day.

Figure 6-6 Viewing the results of entering a filter value



Source: www.sleuthkit.org

10. Click the other two bar graphs, and then click the message displayed in the lower-left pane. View each message's contents in the lower-right pane. When you're finished, close this dialog box.
11. In the left pane, expand **Results** and **Extracted Content**, and then click **Web Search**. In the Result Viewer pane, click the **Text** column header to sort its contents alphabetically, and then scroll down and see what searches Charlie performed.
12. Click **Tools, Generate Report** from the menu. In the Generate Report window, click the **Results - HTML** option button, and then click **Next**. In the Configure Artifact Reports window, click **All Results**, and then click **Finish**.
13. When the report is finished, click the **Results - HTML** pathname in the Report Generation Progress window, 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.

Lab 6.1 Review Questions

1. How many e-mails did Charlie get?
2. How many e-mails did Charlie send?
3. How many Web searches and Web downloads were done on this computer?
4. In the HTML report, what's the name and IP address of a remote drive connected to this computer?
5. In the results of the filter settings you applied, the bar graph heights indicate the number of e-mails per day. True or False?

Lab 6.2 Using OSForensics to Search an Image of a Hard Drive

Objectives

After completing this lab, you will be able to:

- Search image files in OSForensics
- Use the timeline and file search features in OSForensics

OSForensics can perform searches quickly and is capable of sorting date ranges. Investigators can search for exact phrases, documents, graphics, multimedia files, wildcards, and exclusion files. OSForensics also includes a timeline viewer similar to Autopsy's that can reveal recent activity, such as e-mail correspondence, deleted files, MRU storage devices, attached USB devices, and Web browsing history.

> Note: Before beginning this lab, see Chapter 4 of the textbook for download and installation instructions for OSForensics. In this lab, you use OSForensics to identify additional information in the image from Lab 6.1. [Textbook assumes 4.0.1002]
> URL: https://www.osforensics.com/download.html

Materials Required

This lab requires the following: 3

- Windows
- OSForensics
- The charlie-2009-12-03.E01 file from Lab 6.1

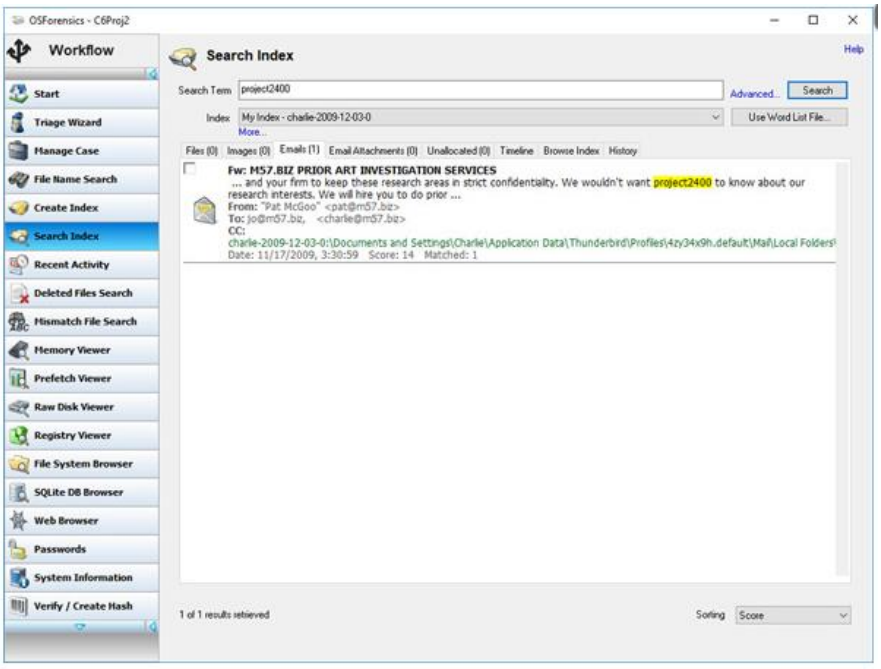
Estimated completion time: 60–120 minutes, depending on your computer's performance

Lab 6.2 Activity

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

1. Start OSForensics. If necessary, click **Continue Using Free Version**. Click **Start** in the left pane, and click **Create Case** in the right pane.
2. In the New Case dialog box, type **C6Proj2** in the Case Name text box and your name in the Investigator text box, and click the **Investigate Disk(s) from Another Machine** option button for the acquisition type. Click **Custom Location** for the case folder. Click the **Browse** button, navigate to and click your work folder, click the **Make New Folder** button, type **C6Proj2**, press **Enter**, and click **OK** twice.
3. Click the **Add Device** button, click the **Image File** option button, and then click the **browse** button. Navigate to and click your work folder, click the **charlie-2009-12-03.E01** file, and click **Open**. Click **Partition 0** in the "Select a partition in the image" dialog box, and then click **OK** twice.
4. Click the **Create Index** button in the left pane. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click the **Uncheck All** button, click the **Emails** and **Images** check boxes, and then click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, verify that the **Whole Drive** option button is selected, click **OK**, and then click **Next**. In the Step 3 of 5 window, click **Start Indexing**. In the OSForensics - Create Index message box, click **OK** to finish indexing.
5. Click the **Search Index** button in the left pane, type **project2400** in the Search Term text box, and click the **Search** button in the right pane. Figure 6-7 shows the results.

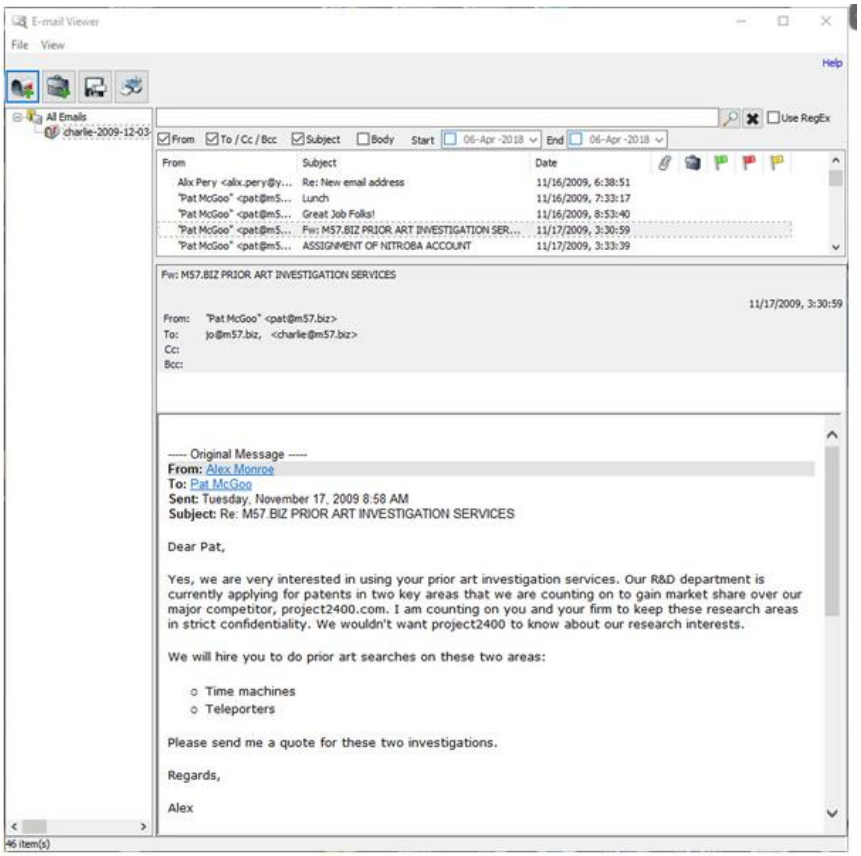
Figure 6-7 Viewing the search results



Source: PassMark Software, www.osforensics.com

6. Right-click the e-mail in the Search Index pane and click **View with E-mail Viewer** to view its contents in the E-mail Viewer window (see Figure 6-8).

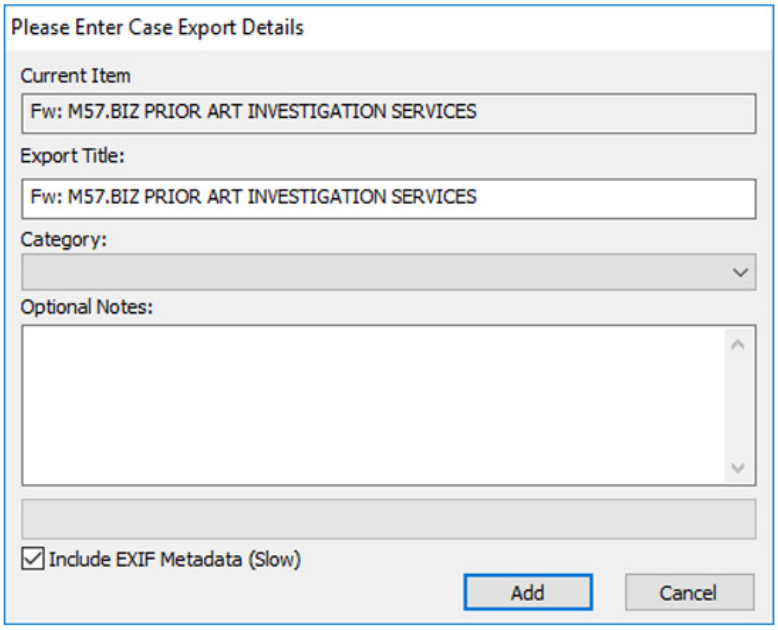
Figure 6-8 Examining the e-mail contents



Source: PassMark Software, www.osforensics.com

7. In the E-mail Viewer window's upper pane, click to highlight the message from Pat McGoo dated 11/17/2009, 3:30:59. Click the **Add E-mail to Case** toolbar icon (the briefcase with a plus sign). In the Please Enter Case Export Details dialog box, click the **Include EXIF Metadata (Slow)** check box (see Figure 6-9), and then click **Add**.

Figure 6-9 Exporting an e-mail



Source: PassMark Software, www.osforensics.com

8. In the E-mail Viewer window's upper pane, right-click the highlighted e-mail, point to **Bookmark**, and click **Red**. Then click **File**, **Close** from the E-mail Viewer menu.
9. Click the **Recent Activity** button in the left pane. In the Recent Activity pane, click the **Scan Drive** option button at the upper left to select the current image, and then click the **Config** button at the upper right to open the Recent Activity Configuration dialog box.
10. Click the **Search date range only** option button. To set the date range, in the From text box, click the current day and type **16**, click the month and type **11** (for November), and then click the year and type **2009** (see Figure 6-10).

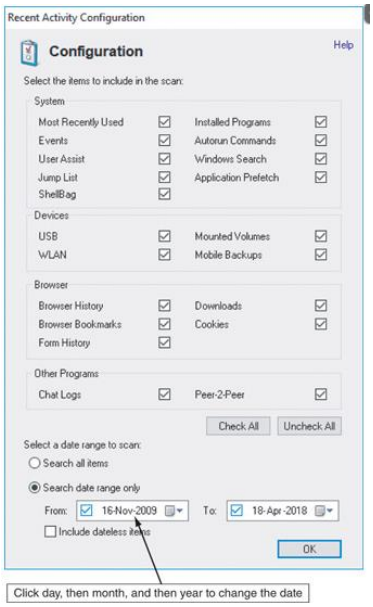
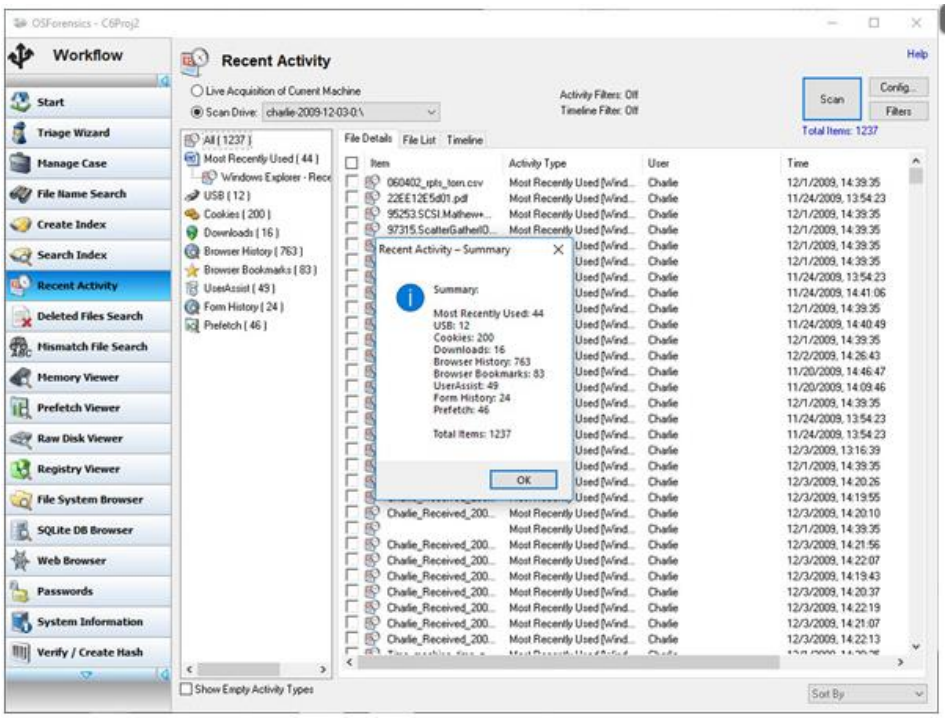


Figure 6-10 Setting the From date

Source: PassMark Software, www.osforensics.com

11. Repeat Step 10 for the To text box to set the date to **December 9, 2009**, and then click **OK** to exit the Recent Activity Configuration dialog box.
12. In the Recent Activity pane, click the **Scan** button at the upper right, and then click **OK** in the Recent Activity - Summary dialog box (see Figure 6-11). Then click the **Timeline** tab to display the timeline of events occurring during the date range you configured. Move your cursor over the different colors in the bar graphs to display the number and types of hits found in this scan. To examine the activities in more detail, click the colored section in each bar graph.

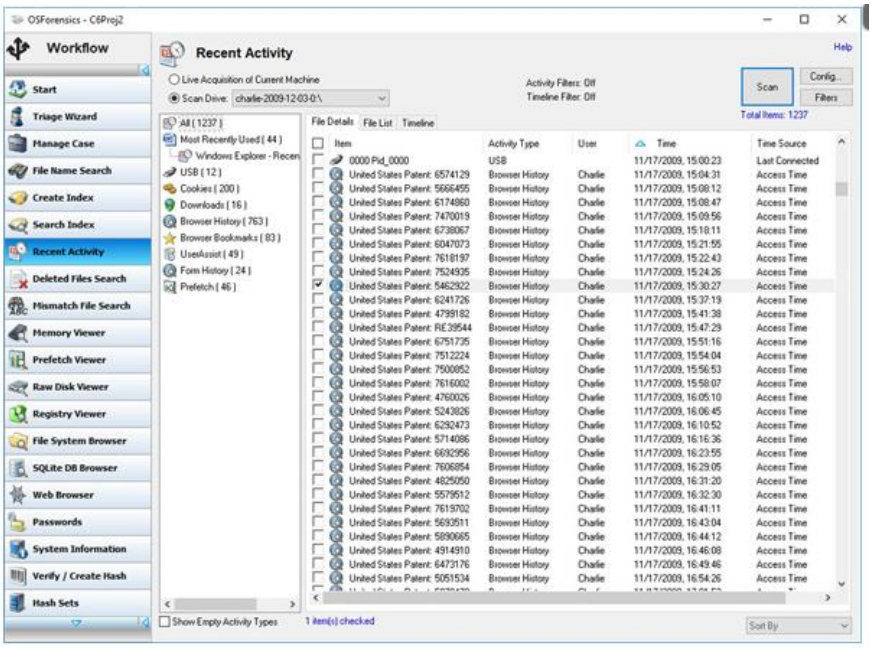
Figure 6-11 Viewing the recent activity summary report



Source: PassMark Software, www.osforensics.com

13. Click the **File Details** tab, if necessary, and click the **Time** column label to sort activities from oldest at the top to most recent at the bottom. Scroll down until you see the activity dated **11/17/2009, 15:30:27** (see Figure 6-12). Right-click it, point to **Open URL**, and click **Open URL with Internet Browser** to identify the Web page contents.

Figure 6-12 Finding recent activity for November 17, 2009, 3:30 p.m.



Source: PassMark Software, www.osforensics.com

14. Click the **File Name Search** button in the left pane. In the File Name Search pane on the right, click the **ellipse** button next to the Start Folder text box, click **charlie-2009-12-03-0**, and click **OK**. If necessary, click the **Presets** list arrow, and click **Images**. Click the **Config** button to open the File Name Search Configuration dialog box. Under the Modify Date Range heading, click the **From** check box, and then set the From date to **November 16, 2009**. Click the **To** check box, and set the To date to **December 9, 2009**, as described in Steps 10 and 11 (see Figure 6-13). Click **OK**.

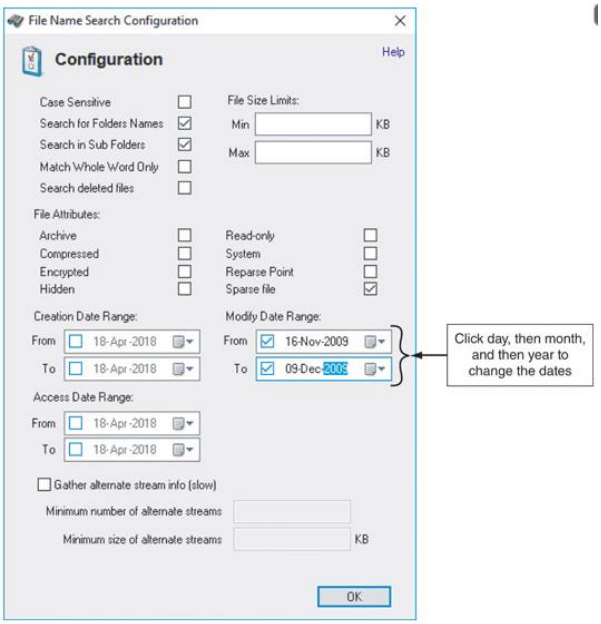
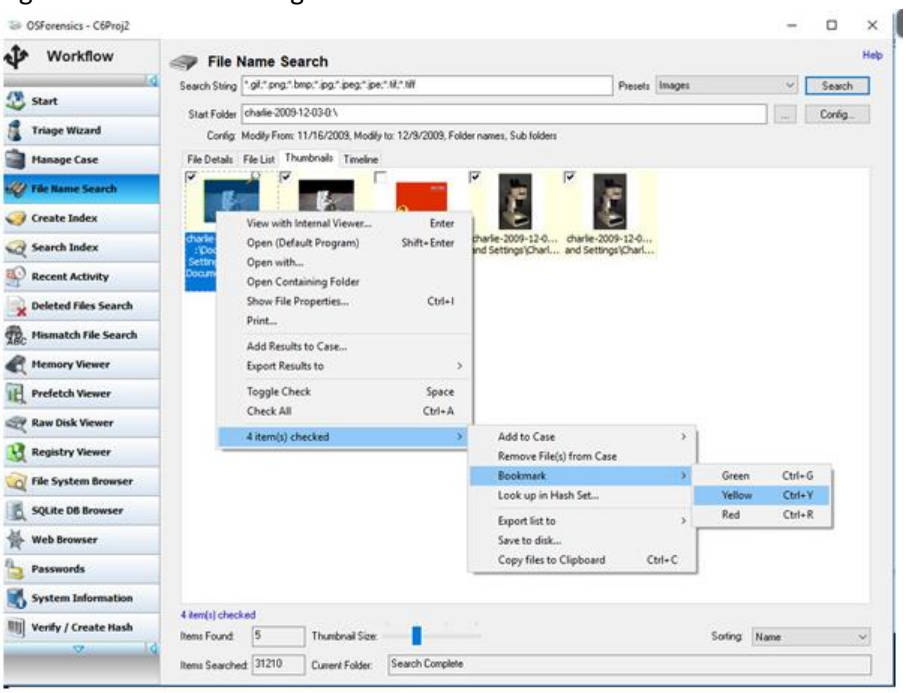


Figure 6-13 Setting the date range

Source: PassMark Software, www.osforensics.com

15. Click the **Search** button at the upper right of the File Name Search pane. Click the **Thumbnails** tab, and then click the check boxes for all .JPG files. Right-click the first highlighted file, point to **4 item(s) checked** and **Bookmark** (see Figure 6-14), and click **Yellow**.

Figure 6-14 Bookmarking .JPG files



Source: PassMark Software, www.osforensics.com

16. Click **Start** in the left pane, and click **Generate Report** in the right pane. In the Export Report dialog box, click the **Copy files to report location** option button, and then click **OK**. If necessary, click **OK** in the error message. If the report doesn't open automatically, start a Web browser, and open the **report.html** file in the C6Proj2\Case Report subfolder of your work folder.
17. Leave OSForensics and the Web browser open as you answer the following review questions. When you're finished, exit OSForensics and the Web browser.

Lab 6.2 Review Questions

1. What was the subject, the sender's name, and the company name in the e-mail sent to Charlie on November 17, 2009, at 3:30 p.m.?
2. How many yellow bookmarks are listed in the HTML report for this case?
3. According to the Recent Activity pane of OSForensics, under the Prefetch heading in the tree view, when was Firefox last run?
4. In the Recent Activity pane of OSForensics, under the Browser History heading in the tree view, what Web page does the item for November 17, 2009, 3:30:27 p.m. open?
5. How many search results did you find for the Project2400 keyword?

Lab 6.3 Examining a Corrupt Image File with FTK Imager Lite, Autopsy, and WinHex

Objectives

After completing this lab, you will be able to:

- Mount an image file as a drive in FTK Imager Lite
- Explain how to identify a corrupt image with WinHex

In Lab 6.1, you learned that the charlie-2009-12-03.E01 image couldn't be loaded in Autopsy 4.3.0. In this lab, you examine this image's boot sector to try to find out why Autopsy couldn't read it. This lab is divided into two sections: testing the image in Autopsy 4.3.0 to see the error message and loading charlie-2009-12-03.E01 in WinHex and comparing it with a known good drive's sector 0.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite, Autopsy 4.3.0, and WinHex
- The charlie-2009-12-03.E01 file from Lab 6.1

Estimated completion time: 60 minutes

Lab 6.3 Activity

Testing an Image File in Autopsy 4.3.0

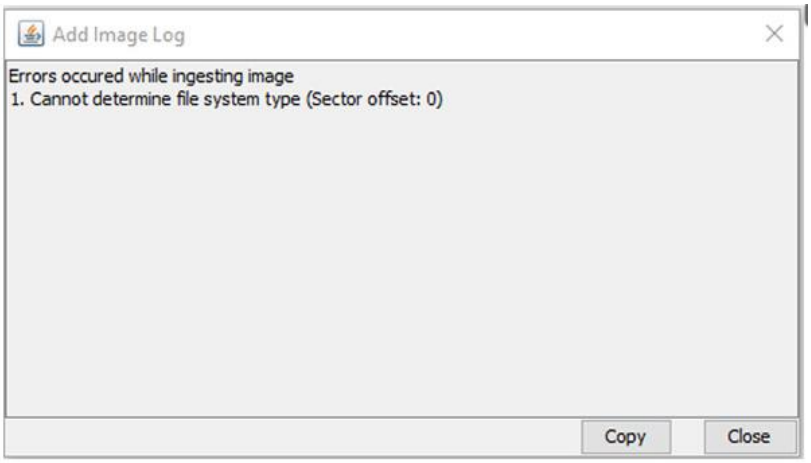
In this section, you see the error message that occurs when attempting to load charlie-2009-12-03.E01 in Autopsy 4.3.0:

1. Start Autopsy 4.3.0, and click the **Create New Case** button. In the New Case Information window, enter **C6Proj3-1** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and click **Select** to enter this path. Make sure the **Single-user** option button is selected for Case Type, and then click **Next**.
2. In the Additional Information window, type **C6Proj3-1** in the Case Number text box and your name in the Examiner text box, and then click **Finish** to start the Add Data Source Wizard.
3. In the Select Data Source window, click **Disk Image or VM file**in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **charlie-2009-12-03.E01** file, and then click **Open**. Click **Next**.

Tip: If you get an error message stating that Autopsy 4.3.0 is missing links, exit the program and reinstall it. In the Autopsy Installation Wizard, click the Repair button to correct this error.

4. Keep the default settings in the Configure Ingest Modules window. Click **Next** and then **Finish**.
5. When the error message box is displayed, click the **View Log** button in the Add Data Source window, and then click the **Copy** and **Close** buttons shown in Figure 6-15. Click **Finish**, and then exit Autopsy.

Figure 6-15 Viewing the log error



Source: www.sleuthkit.org

6. Start a new document in Notepad, and paste the copied error message. Save it as **C6Proj3-1-Autopsy-Error-Msg.txt** in your work folder, and exit Notepad. Proceed to the next section.

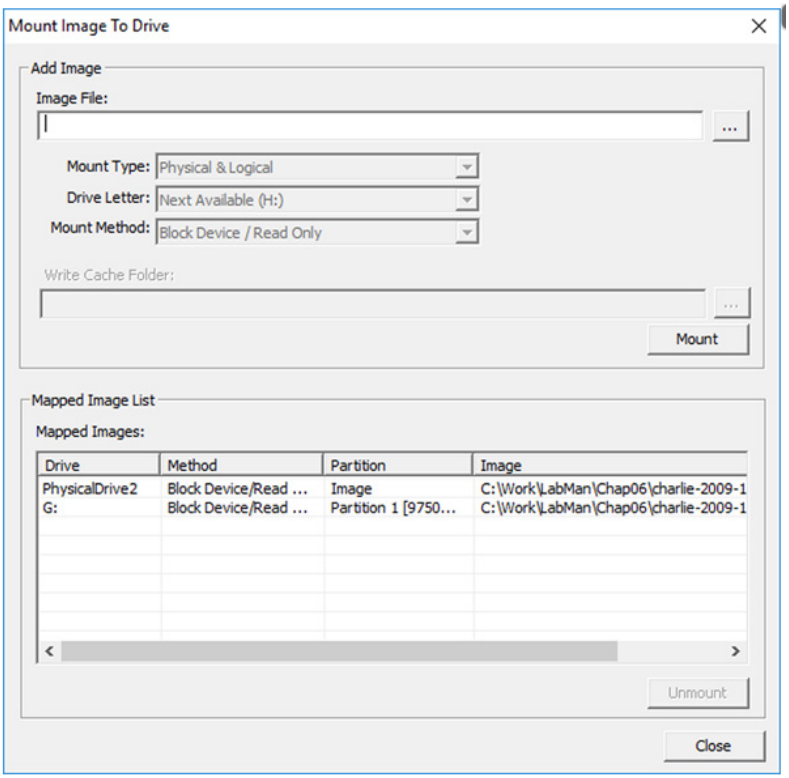
Examining Image Files in WinHex

The error message in Figure 6-15 states that Autopsy 4.3.0 can't determine the file system when it attempts to read sector 0 of charlie-2009-12-03.E01. In this section, you use WinHex to compare sector 0 of the charlie-2009-12-03.E01 image and your computer's C drive to discover any differences that might have caused this error. For more information on what sector 0 of an NTFS disk drive should contain, refer to the following sources:

- NTFS Partition Boot Sector at www.ntfs.com/ntfs-partition-boot-sector.htm
- Master Boot Sector at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc976796(v=technet.10)
- COEN 252 Computer Forensics NTFS at www.cse.scu.edu/~tschwarz/COEN252_09/Lectures/NTFS.html
- Disk Concepts and Troubleshooting at https://technet.microsoft.com/en-us/library/cc977221.aspx

1. Start FTK Imager Lite, and click **File**, **Image Mounting** from the menu. In the Mount Image To Drive dialog box, click the **browse** button next to the Image File text box. Navigate to your ***Work*\C6Proj3-2** folder, double-click **charlie-2009-12-03.E01**, and then click the **Mount** button. In the Mapped Image List section at the bottom, note the PhysicalDrive number and the drive letter created for this image file (see Figure 6-16), and then click **Close**. Leave FTK Imager Lite running in the background.

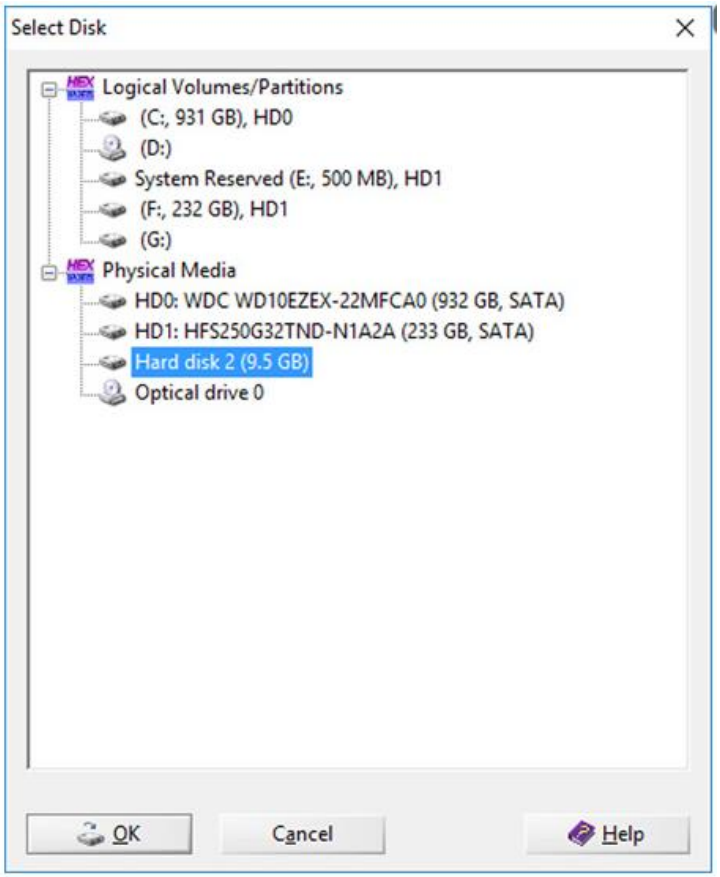
Figure 6-16 Mounting charlie-2009-12-03.E01 in FTK Imager Lite



Source: AccessData Group, Inc., www.accessdata.com

Note: Figure 6-16 shows that FTK Imager Lite defines the mounted image as PhysicalDrive2 for Drive G. Figure 6-17 shows that WinHex defines it as Hard disk 2 (9.5 GB) for Drive G. Your drive number and letter will most likely be different. In the following steps, substitute the drive number and letter you see in Figures 6-16 and 6-17.

Figure 6-17 Selecting disk drives in WinHex

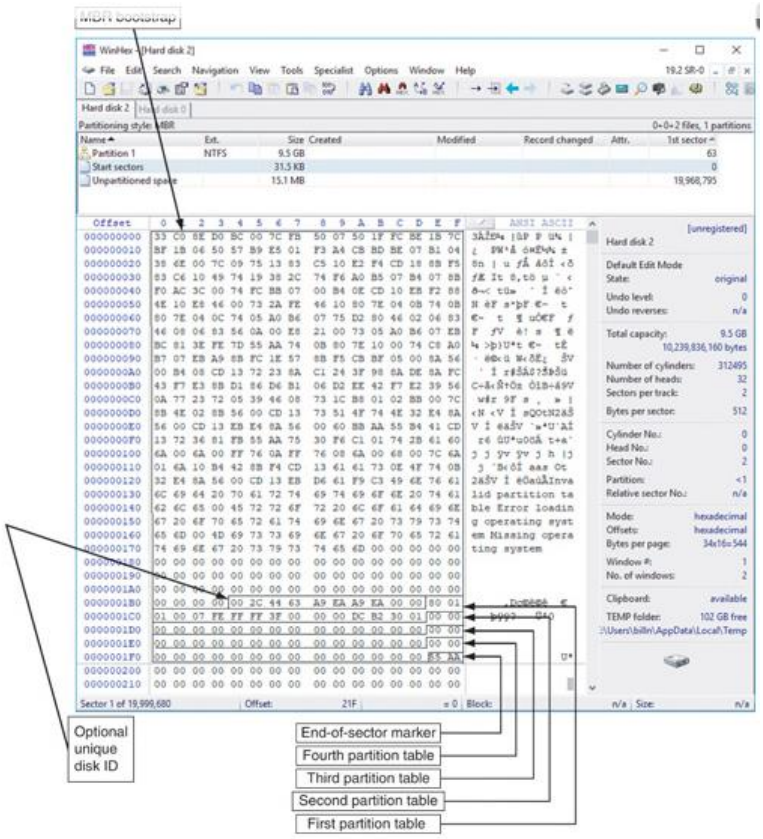


Source: X-Ways AG, www.x-ways.net

2. Start WinHex, and click **OK** in the evaluation warning message. Click **Tools**, **Open Disk** from the menu to open the Select Disk dialog box. Notice that the PhysicalDrive2 entry you saw in FTK Imager Lite is listed as Hard disk 2 in WinHex (refer back to Figure 6-17). Click **Hard disk 2 (9.5 GB)** under the Physical Media heading, and then click **OK**.
3. Click **Tools**, **Open** from the menu again. Under the Physical Media heading, click **HD0:*your-computer-drive's-physical-name*** (which will differ from what's shown in Figure 6-17), and then click **OK**. Click the **Hard disk 2** tab. In the Data Browser pane (upper pane), click **Start sectors**. Then click the **Hard disk 0** tab, and click **Start sectors**.
4. For Windows drives, sector 0 of the MBR is made up of the following fields: the MBR bootstrap starting at offset 000000000; the optional unique disk ID starting at offset 0000001B4; the first partition table starting at offset 0000001BE; the second partition table starting at 0000001CE,

the third partition table starting at offset 0000001DE; the fourth partition table starting at offset 0000001EE; and the end-of-sector marker starting at offset 0000001FE. Examine these fields in Figure 6-18.

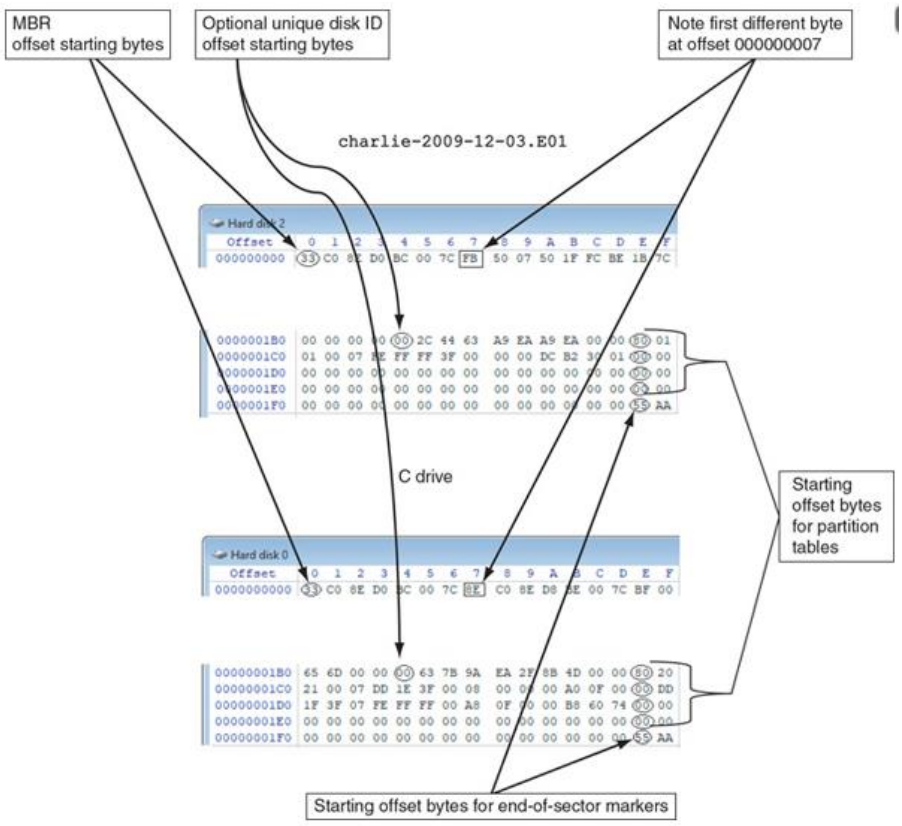
Figure 6-18 Displaying the MBR fields



Source: X-Ways AG, www.x-ways.net

5. At offsets 0000000000 through 0000000006 the hexadecimal values are identical for both the image and drive C. From offset 000000007 through offset 0000001BD, however, the hexadecimal values are different (see Figure 6-19). This difference indicates that the MBR bootstrap code has been altered and might explain why Autopsy 4.3.0 is unable to read sector 0 and identify the file system type. Based on this examination of the MBR, it seems that unlike Autopsy 4.7.0, Autopsy 4.3.0 requires more than the first 7 bytes of the charlie-2009-12-03.E01 file to determine its file system type.

Figure 6-19 Comparing sectors 0 of charlie-2009-12-03.E01 and your C drive



Source: X-Ways AG, www.x-ways.net

6. Leave FTK Imager Lite and WinHex open as you answer the following review questions. When you're finished, exit FTK Imager Lite and WinHex.

Lab 6.3 Review Questions

1. When you attempted to load charlie-2009-12-03.E01 in Autopsy 4.3.0, what error message was displayed?

    a) Failed to add data source (critical errors encountered)
    b) Cannot determine file system type (Sector offset: 0)
    c) Cannot determine file system type (Cluster offset: 2)
    d) Failed to load Configure Ingest Module

2. In what dialog box did Autopsy 4.3.0 fail to load charlie-2009-12-03.E01?

    a) Select Data Source
    b) Configure Ingest Modules
    c) Add Data Source
    d) Reporting

3. What are the hexadecimal values for the optional unique disk ID in the MBR for the charlie-2009-12-03.001 image?

    a) 00 2C 44 63 A9 EA A9 EA 00 00
    b) 33 C0 8E D0 BC 00 7C FB
    c) 80 01 01 00 07 FE FF FF 3F 00 00 00 DC B2 30 01
    d) 33 C0 8E D0 BC 00 7C 8E

4. What's the starting offset for a drive's second partition table?

    a) 0000001B4
    b) 0000001BE
    c) 0000001CE
    d) 0000001FF

5. FTK Imager Lite can mount both the physical and logical drives of a forensic image. True or False?