COSC6410 Lab Assignment 3

Please submit through Blackboard by midnight September 18.

The purpose of this lab is: working with data acquisition.

a. Use ProDiscover Basic and FTK Imager for data acquisition.
b. Examine FAT32, NTFS, and HFS+ images.

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

Lab 2.1 Securely Wiping a USB Drive

Objectives

Sometimes data must be deleted from a storage device securely to prevent recovering sensitive or secret files. Simply deleting files isn't enough to remove file data because when a file is deleted from a storage device, only the pointer to the file location is removed. The Master File Table (MFT), which stores the physical location of files in the file system, is updated to reflect the free space. The MFT is a separate structure in the NTFS file system; it's not the Recycle Bin. File information might remain on a computer even if it has been deleted from the Recycle Bin. Therefore, deleted data might still exist on a computer until all remnants have been overwritten by new data.

Deleted files often aren't overwritten immediately, and forensics software can be used to recover file remnants and reconstruct an original file by a process known as "data carving." Unless remnants are overwritten with other data, there's no guarantee that the deleted files can't be retrieved and viewed. Therefore, secure destruction of digital data often requires writing a series of 0 or 1 bits to the storage device to overwrite any file remnants.

The National Institute of Standards and Technology (NIST) 800-88 standard requires seven wiping passes over existing data before the data can be considered unrecoverable on storage devices. ProDiscover includes a disk wipe tool designed to erase storage media completely; it conforms to NIST standards and prevents any forensic recovery. Before digital evidence can be copied to a storage device for forensic analysis, all previous data stored on the device must be erased completely. In this lab, you securely wipe data from a USB drive to prepare it for forensic imaging.

After completing this lab, you will be able to:

- Wipe a storage device securely
- Explain the purpose of wiping a storage device

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- Data files in the C2Proj1 folder on the DVD
- A USB drive with data on it that can be erased
- ProDiscover Basic

Estimated completion time: **60–120 minutes,** depending on the size of your USB drive

Activity

In this lab, you wipe the contents of a USB drive by using ProDiscover Basic:

1. Log on to your computer, and insert a USB drive containing files you don't need.
2. Right-click the **ProDiscover Basic** desktop icon and click **Run as administrator** to start ProDiscover Basic. Click **Yes** in the User Account Control (UAC) message box.

3. In the Launch Dialog dialog box, click the **Don't show this dialog in the future** check box, and then click **Cancel** to close the Open dialog box. Click **Tools, Secure Wipe** from the ProDiscover menu.
4. In the Secure Wipe Disk dialog box, click the **Disk to Wipe** list arrow, and click the drive letter corresponding to the USB drive. Verify that you have selected the correct drive letter to prevent accidentally erasing any other attached storage device. In the Number of Passes list box, type 7, and then click **Start** to begin the process.
5. Click **OK** in the ProDiscover message box to bypass the warning that all data will be securely wiped. The Securely Deleting file message is displayed in the lower-left corner to indicate that disk files are being wiped.
6. When the disk has been wiped seven times, you see the message "The selected disk has been securely wiped." Click **OK**, and exit ProDiscover Basic.
7. Open File Explorer, and then right-click the USB drive and click **Format**.
8. In the Format dialog box, click **NTFS** in the File system list box, and type **EVIDENCE** in the Volume label text box. Click **Start** to format the USB drive. Click **OK** in the Format Removable Disk message box.
9. When the format is finished, click **OK** in the Formatting Removable Disk message box, and close the Format dialog box. Copy the 11 files from the **C2Proj1** folder on the DVD accompanying this book. This folder is your original source of digital evidence. Label the storage device, and don't write any more files to it.
10. Close any open windows, and leave your computer running for the next lab.

Review Questions

1. Which statement about deleted files is true?
   a. Deleted files can be rebuilt from remnants that haven't been overwritten.
   b. After a file has been deleted from the Recycle Bin, it can't be recovered.
   c. After a file pointer has been deleted in the MFT, it can't be recovered.
   d. The MFT isn't updated until all file remnants have been overwritten with new data.
2. When a file is deleted from a storage device, only the pointer to the file location is removed. True or False?
3. According to NIST standards, how many wipes should be done to erase data completely?
   a. Three
   b. One
   c. Two
   d. Seven

4. Which of the following statements about the MFT is true?
   a. The MFT is overwritten each time a file is deleted.
   b. The MFT is updated to indicate free space when files are deleted.
   c. The MFT and the Recycle Bin are the same file structure.
   d. The MFT isn't used in the NTFS file system.
5. Secure destruction of digital data requires doing which of the following?
   a. Overwriting the MFT
   b. Writing 0s and 1s to the storage device to overwrite file remnants
   c. Writing information in the MFT to file remnant locations
   d. Deleting files from the Recycle Bin

Lab 2.2 Using ProDiscover Basic to Image a USB Drive

Objectives

When computers and devices are seized during a forensics investigation, the process of extracting information includes using disk imaging to make a bit-stream copy of the original storage media. Disk imaging builds forensically sound bit-for-bit copies of the evidence data, including the MFT with all physical file locations containing data or remnants and unallocated free space on the hard disk. After the original medium is duplicated, investigators can safely analyze the file structure and recover potential forensics evidence without the danger of destroying it during the process. Additionally, disk imaging maintains the chain of custody by protecting the evidence from any changes that might render it unusable in court.

ProDiscover Basic supports importing several types of image file formats, including `.dd`, `.eve`, `.cmp`, `.pdg`, and `.pds`. In this lab, you simulate seizing digital evidence on the USB drive you prepared in Lab 2.1 and build a ProDiscover Basic `.eve` image to search for existing or deleted files. This process is the same procedure you follow during an actual investigation, except you use a write-blocker in actual investigations to prevent any changes to the original evidence during the acquisition. A write-blocker is a hardware or software component inserted between the original storage device and the computer creating the image to prevent what's on the original storage device from being overwritten, which violates the chain of custody.

After completing this lab, you will be able to:

- Explain the purpose of disk imaging
- Make a bit-stream image of a USB drive or a similar storage device

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- ProDiscover Basic
- The USB drive prepared in Lab 2.1

Estimated completion time: **10–20 minutes**

Activity

In this lab, you image the USB drive you prepared in Lab 2.1:

1. Insert the USB drive containing evidence into your computer.
2. In File Explorer, create a folder called **Work** in your C drive, and then create a subfolder named **Labs** in the Work folder. The Work\Labs folder is used throughout this book for lab files. In C:\Work\Labs, create three subfolders called **Cases**, **Data**, and **Evidence**.
3. Double-click the **ProDiscover Basic** desktop icon. Click **Action**, **Capture Image** from the menu.
4. In the Capture Image dialog box, click the **Source Drive** list arrow, and then click the drive letter for the USB drive.
5. Click the **double arrow** button next to the Destination text box, click **Choose Local Path**, and navigate to and click the **C:\Work\Labs\Evidence** folder. In the Save As dialog box, type **C2Proj2** in the File name text box (see Figure 2-1), and click **Save**.

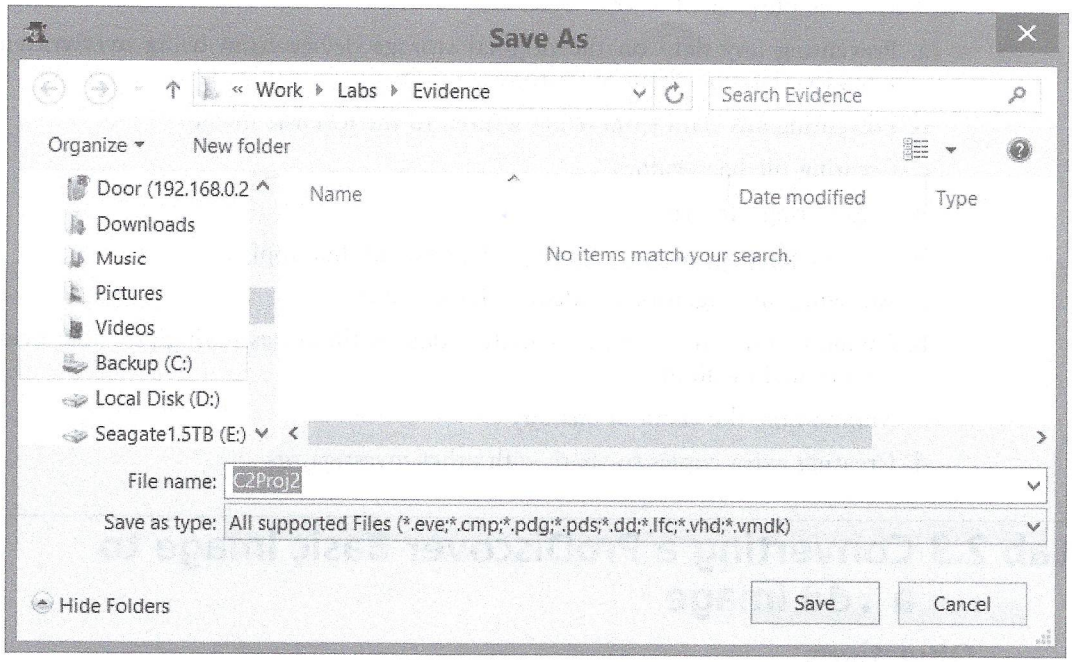

Figure 2-1 Selecting a destination for case files

6. In the Capture Image dialog box, type your full name in the Technician Name text box, and type **C2Proj2** in the Image Number text box. Click **OK** to continue.
7. When the imaging is finished, click **OK**. Navigate to and click the **C:\Work\Labs\Evidence** folder in File Explorer, and confirm that the `C2Proj2.eve` image has been created.
8. Close File Explorer, and leave ProDiscover Basic running for the next lab.

Review Questions

1. ProDiscover Basic supports all the following image formats except _____.
   a. `.dd`
   b. `.eve`
   c. `.pdg`
   d. `.vhd`
2. Disk images don't include the MFT. True or False?
3. Which statement about a ProDiscover Basic image is true?
   a. It doesn't copy the MFT because it isn't needed during analysis.
   b. It copies the MFT and any unallocated free space from the original storage device.
   c. It can't be used during forensic analysis.
   d. It contains only data; it doesn't include unallocated free space.
4. What's the purpose of a write-blocker?
   a. Preventing any data on the original storage device from being overwritten, which would violate the chain of custody
   b. Preventing any data from being written to the forensic image
   c. Creating file hash values
   d. Duplicating the MFT
5. What's the purpose of disk imaging? (Choose all that apply.)
   a. Allowing investigators to calculate hash values
   b. Giving investigators a way to analyze data without destroying potential evidence on the original medium
   c. Maintaining the chain of custody
   d. Creating extra copies to share with other investigators

Lab 2.3 Converting a ProDiscover Basic Image to a `.dd` Image

Objectives

Forensics investigators often use more than one suite of software tools to search for digital evidence because using multiple tools can yield more evidence than using just one tool and is useful for validating results. In addition, they should be able to use different imaging tools in case they need faster duplications in some settings or need tools optimized for specific file systems, such as NTFS or HFS. However, forensics tools typically produce files that aren't compatible with other software tools. For example, ProDiscover Basic produces images in its proprietary `.eve` format that other software might not be able to read. However, ProDiscover Basic can convert `.eve` images to other formats, such as the `.dd` format supported by most forensics software. The `.dd` format produces a bit-by-bit copy of a storage device's contents and can be read by Windows, Linux, UNIX, and Mac OS X.

ProDiscover Basic also supports converting .eve images to ISO, .dd to ISO, and .dd to VMware virtual hard disks. ISO images are files stored in an uncompressed format; they're used to burn a DVD or CD and make it installable or bootable. A VMware virtual hard disk can be viewed as a virtual machine that appears as an OS running in another OS, which enables forensics investigators to run a disk image as though it were connected to the original computer. In this lab, you convert a ProDiscover Basic image to a .dd format that's imported into FTK Imager in Lab 2.4.

After completing this lab, you will be able to:

- Describe ProDiscover Basic's conversion tools
- Convert an .eve image to a .dd image in ProDiscover Basic

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- ProDiscover Basic
- The C2Proj2.eve file created in Lab 2.2

Estimated completion time: **5–10 minutes**

Activity

In this lab, you convert the C2Proj2.eve image to a .dd format:

1. Double-click the **ProDiscover Basic** desktop icon, if necessary. Click **Tools** on the menu, point to **Image Conversion Tools**, and then click **Convert ProDiscover Image to "DD"**, as shown in Figure 2-2.

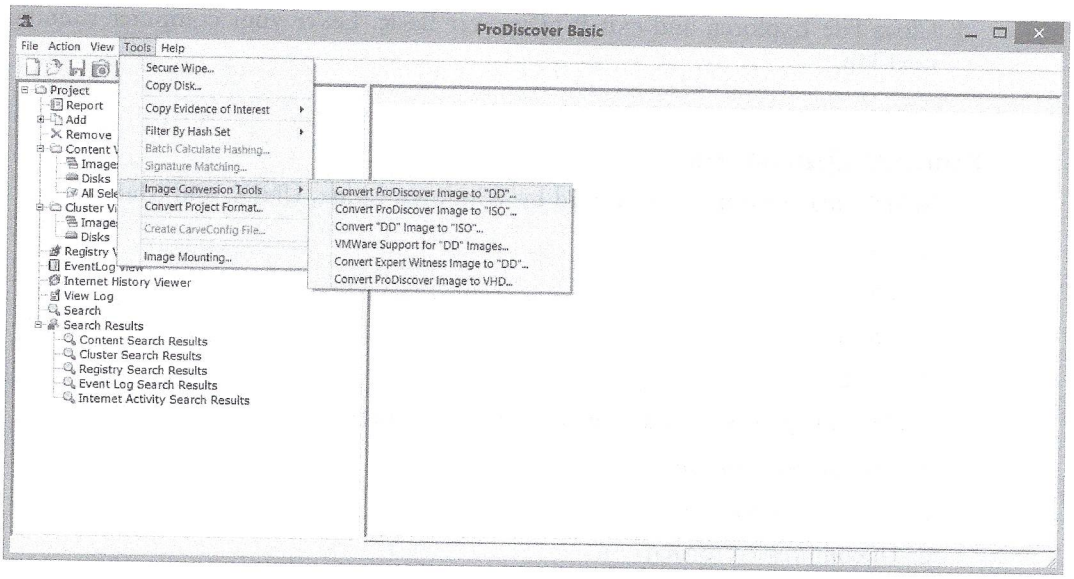

Figure 2-2 Converting a ProDiscover image to the .dd format

2. In the Convert ProDiscover Image to 'DD' Image dialog box, click the **Browse** button, navigate to and click the **C:\Work\Labs\Evidence** folder, and click the **`C2Proj2.eve`** file to enter the path and filename in the Source ProDiscover Image text box (see Figure 2-3).

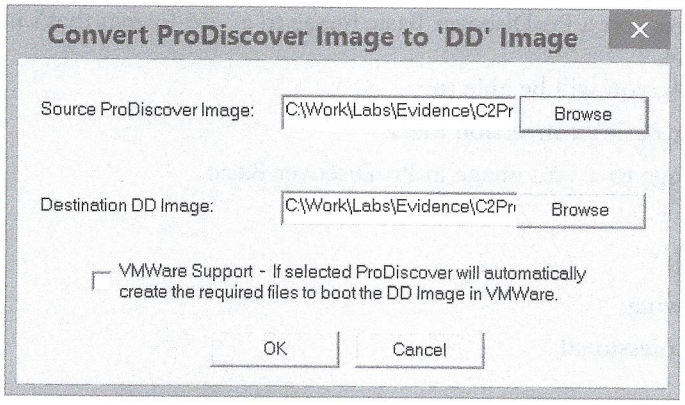

Figure 2-3 Finishing the format conversion

3. Click **OK**. The blue bar in the lower-right corner indicates that the file conversion is in progress.
4. When the conversion is finished, navigate to and click the **C:\Work\Labs\Evidence** folder in File Explorer, and confirm that the `C2Proj2.dd` image has been created. The image's file size should be approximately the size of the storage device, not the data.
5. Close File Explorer, and exit ProDiscover Basic. Leave your computer running for the next lab.

Review Questions

1. Which image format can be read by Windows, Linux, UNIX, and Mac OS X?
   a. `.dd`
   b. `.eve`
   c. `.pdg`
   d. `.mft`
2. An ISO image is stored as which of the following?
   a. Compressed format
   b. Proprietary format
   c. Uncompressed format
   d. Hashed format

3. ProDiscover Basic can perform which of the following image conversions?
   a. ISO to `.dd`
   b. VMware to `.dd`
   c. `.eve` to ISO
   d. `.eve` to `.E01`
4. ProDiscover images are the same size as the total size of all evidence files on the original source. True or False?
5. Forensics investigators should be familiar with more than one forensics analysis tool so that they can maintain the chain of custody. True or False?

Lab 2.4 Imaging Evidence with FTK Imager

Objectives

AccessData FTK Imager creates bit-stream images in raw (`.dd`), Smart (`.s01`), and `.E01` formats and enables investigators to extract Registry files from a Windows computer and import them into Registry-viewing tools, such as AccessData Registry Viewer, for recovering passwords or encrypted files.

Unlike ProDiscover, FTK Imager isn't optimized to search through large volumes of data to find evidence. Instead, it has verification features, such as MD5 and SHA-1 hashing calculations that provide redundant verification to show that files haven't been altered during imaging. FTK Imager does have some basic search features and can be used to look for deleted files or identify encrypted files. It's available in a "lite" version that can be placed on removable media to make it portable; it also makes it possible for investigators to extract files without booting the suspect's computer. In this lab, you identify files that have been deleted on a USB drive.

After completing this lab, you will be able to:

- List the image formats FTK Imager supports
- Use FTK Imager to image a USB drive

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- FTK Imager
- The USB drive prepared in Lab 2.1

Estimated completion time: **30–40 minutes**

Activity

In this lab, you delete two files on the EVIDENCE drive you created in Lab 2.1, and then image the USB drive with FTK Imager to produce an `.E01` image:

1. Open File Explorer, and browse to the USB drive. Delete the **`Qtr 1 Emp.xls`** and **`Online.docx`** files on the USB drive, and then close File Explorer.
2. Double-click the **FTK Imager** desktop icon. Click **Yes** in the UAC message box, if necessary. Click **File, Create Disk Image** from the menu.
3. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**.
4. In the Select Drive dialog box, click the **EVIDENCE [NTFS]** source drive in the drop-down list box, and then click **Finish** to continue.
5. In the Create Image dialog box, click **Add**. In the Select Image Type dialog box, click the **E01** option button, and then click **Next** to continue.
6. In the Evidence Item Information dialog box, type **C2Proj4** in the Case Number and Evidence Number text boxes. Enter your full name in the Examiner text box, and type **USB image with deleted files** in the Notes text box, as shown in Figure 2-4. Click **Next** to continue.

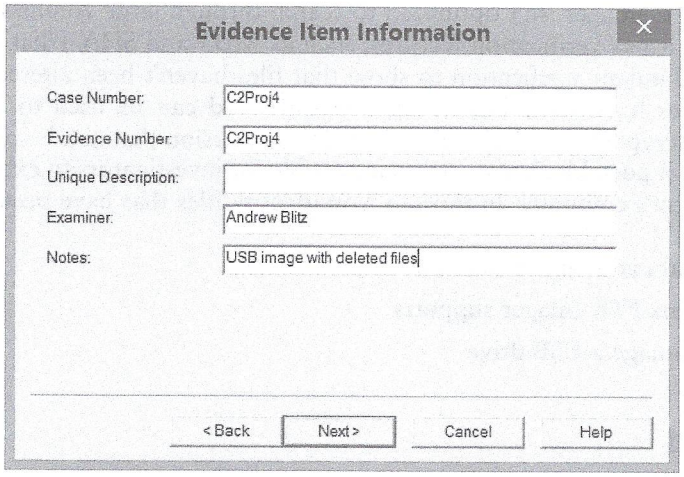

Figure 2-4 Entering evidence item information

7. In the Select Image Destination dialog box, click the **Browse** button, navigate to and click the **C:\Work\Labs\Evidence** folder, click **OK**, and type **C2Proj4** in the Image Filename text box (see Figure 2-5). Click **Finish**.
8. In the Create Image dialog box, click **Start**. When the imaging process is finished, the results are displayed along with the computed MD5 and SHA-1 hashes (see Figure 2-6), which verify the forensic image's integrity. Click **Close** in the Drive/Image Verify Results and Creating Directory Listing dialog boxes. The `C2Proj4.E01` file is used in Lab 2.5. Leave FTK Imager running for the next lab.

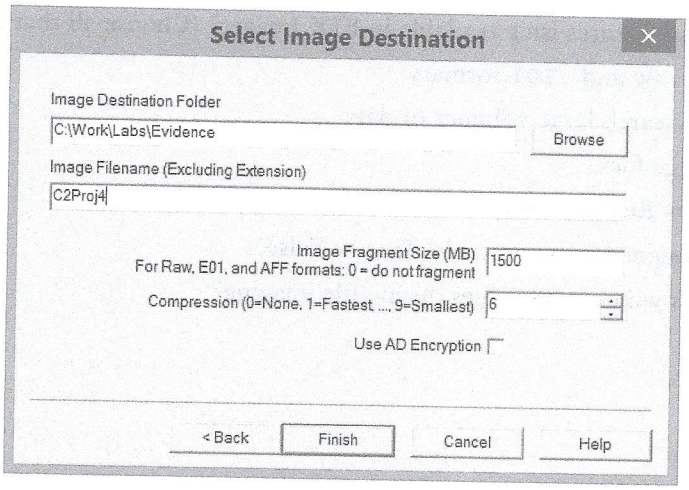

Figure 2-5 Selecting the image destination

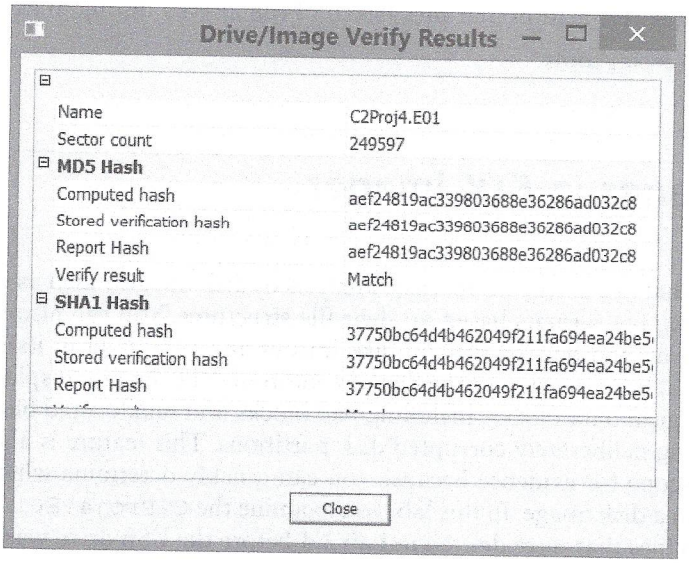

Figure 2-6 Verifying the results

Review Questions

1. FTK Imager can produce all the following image formats except _____.
   a. `.E01`
   b. `.dd`
   c. `.s01`
   d. `.eve`

2. Which of the following features isn't available in FTK Imager? (Choose all that apply.)
   a. Creating images in raw and `.E01` formats
   b. Being optimized to search large volumes of data
   c. Creating `.eve` image files
   d. Extracting Windows Registry files
3. FTK Imager Lite is designed to be portable. True or False?
4. FTK Imager calculates which hash values during file imaging?
   a. MD5
   b. SHA-5
   c. DD5
   d. `.eve`
5. Why does FTK Imager calculate two hash values?
   a. So that they can be read by older versions of Microsoft Office
   b. To provide redundant verification that files haven't been altered during imaging
   c. For use in other forensics tools
   d. None of the above

Lab 2.5 Viewing Images in FTK Imager

Objectives

FTK Imager has features that are useful for forensic analysis of disk images, such as calculating hash values and viewing file formats based on their file structures. You can also use FTK Imager to search for existing and deleted files on disk images and view data in its readable state as well as hexadecimal bytes written to the disk. In addition, FTK Imager displays information on physical and logical data blocks, including bad blocks and unallocated blocks that can be helpful in recovering deliberately corrupted disk partitions. This feature is also useful in narrowing the search scope for evidence because you can quickly determine whether any data has been deleted from a disk image. In this lab, you examine the `C2Proj4.E01` image to locate and export the two files that were deleted in Lab 2.4 before the USB drive was imaged.

After completing this lab, you will be able to:

- View images in FTK Imager for preliminary analysis
- Locate deleted files and export them for further analysis

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- Microsoft Office 2007, 2010, or 2013 (or open-source software capable of reading Office files)

- FTK Imager
- The `C2Proj4.E01` image from Lab 2.4

Estimated completion time: **10–15 minutes**

Activity

In this lab, you add the USB image created in Lab 2.4 and look for two deleted files:

1. Double-click the **FTK Imager** desktop icon, if necessary, and click **File, Add Evidence Item** from the menu.
2. In the Select Source dialog box, click the **Image File** option button, and then click **Next.**
3. In the Select File dialog box, click **Browse,** navigate to and click the **C:\Work\Labs\ Evidence** folder, click the **`C2Proj4.E01`** file, and then click **Open.** Click **Finish.**
4. In the Evidence Tree pane, expand the **C2Proj4.E01, EVIDENCE [NTFS],** and **[root]** folders, and then click the **[root]** folder to view the files on the imaged drive. Notice that the deleted `Qtr 1 Emp.xls` and `Online.docx` files show a red X in the File List pane (see Figure 2-7). FTK Imager was able to recover these deleted files from the USB drive, even though they weren't visible in File Explorer.

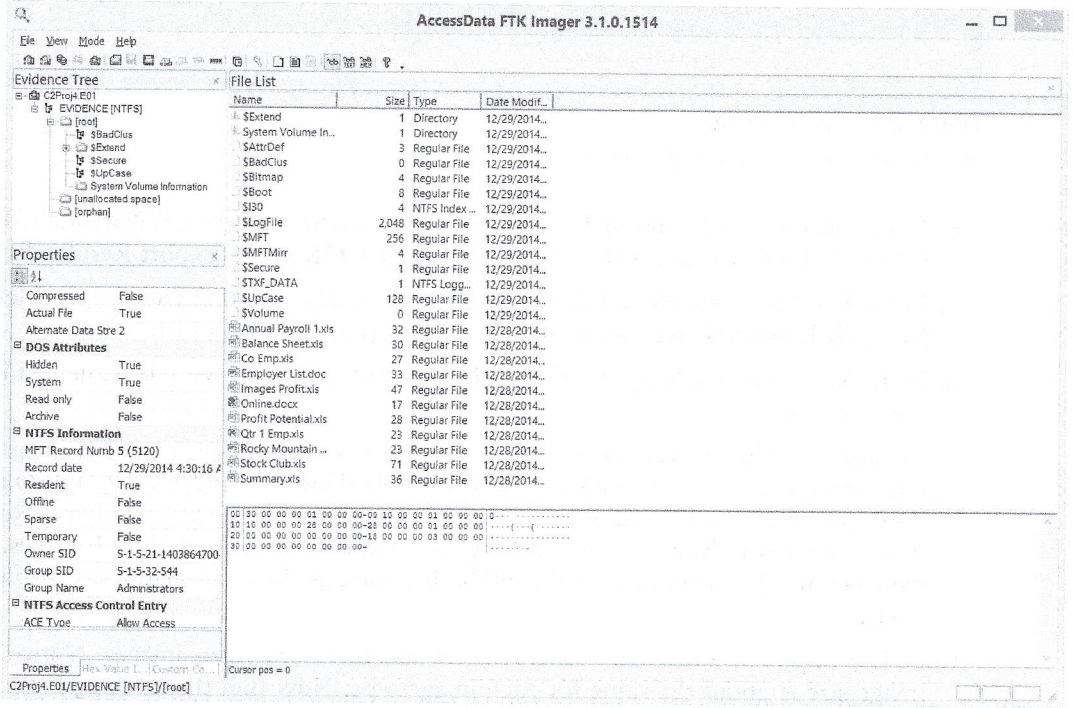

Figure 2-7 Viewing files on an imaged drive

5. In the File List pane, Ctrl+click the **`Qtr 1 Emp.xls`** and **`Online.docx`** deleted files. Right-click the **`Online.docx`** file and click **Export Files**, as shown in Figure 2-8.

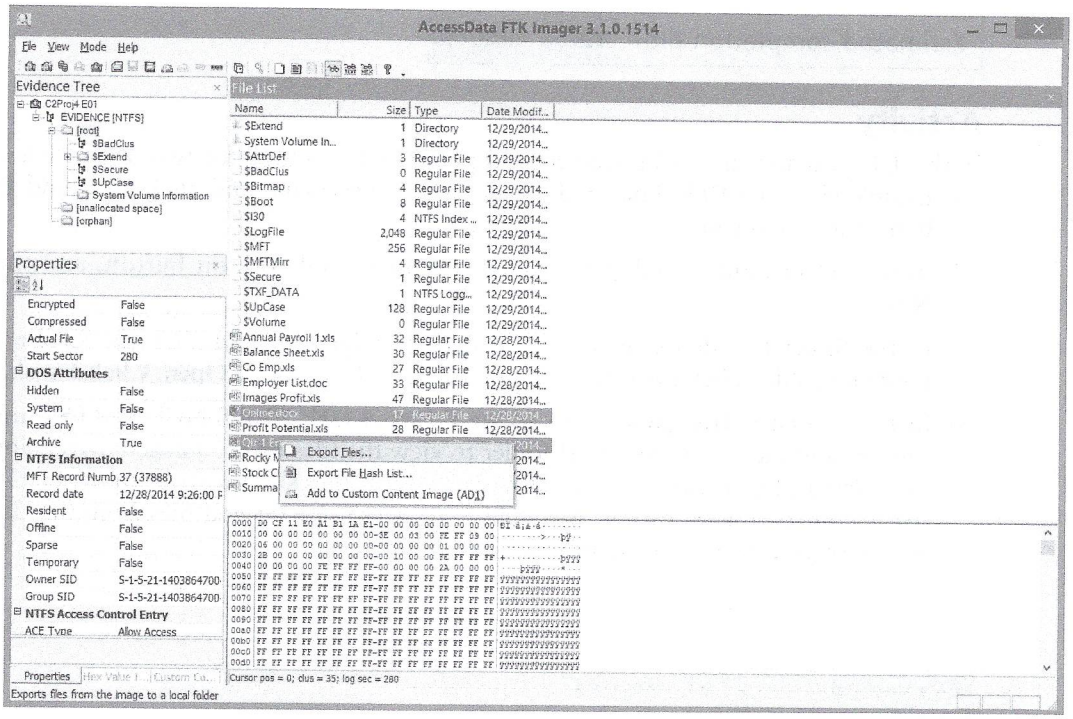

Figure 2-8 Exporting files

6. In the Browse For Folder dialog box, navigate to and click the **C:\Work\Labs\Evidence** folder, click **OK** to export the files, and then click **OK** in the Export Results dialog box.
7. In the File List pane, Ctrl+click the **`Qtr 1 Emp.xls`** and **`Online.docx`** deleted files. Right-click the **`Online.docx`** file and click **Export File Hash List**.
8. In the Save As dialog box, type **C2Proj4 deleted file hashes** in the File name text box, and then click **Save**.
9. Answer the following review questions, and when you're finished, exit FTK Imager. In File Explorer, navigate to and click the **C:\Work\Labs\Evidence** folder. Find and double-click the exported **`C2Proj4 deleted file hashes.csv`** file to open it in Excel. Review the Excel spreadsheet listing the two deleted files and their MD5 and SHA-1 hashes. Expand the columns, if needed, to view the full hash values, as shown in Figure 2-9, and then exit Excel.
10. In File Explorer, locate the `C2Proj2.dd` and `C2Proj2.eve` images. Notice that the image size is about the same for each image type. Now find the `C2Proj4.E01` image, and notice that it's much smaller. FTK Imager creates a compressed image yet preserves all the evidence.
11. Close any open windows.

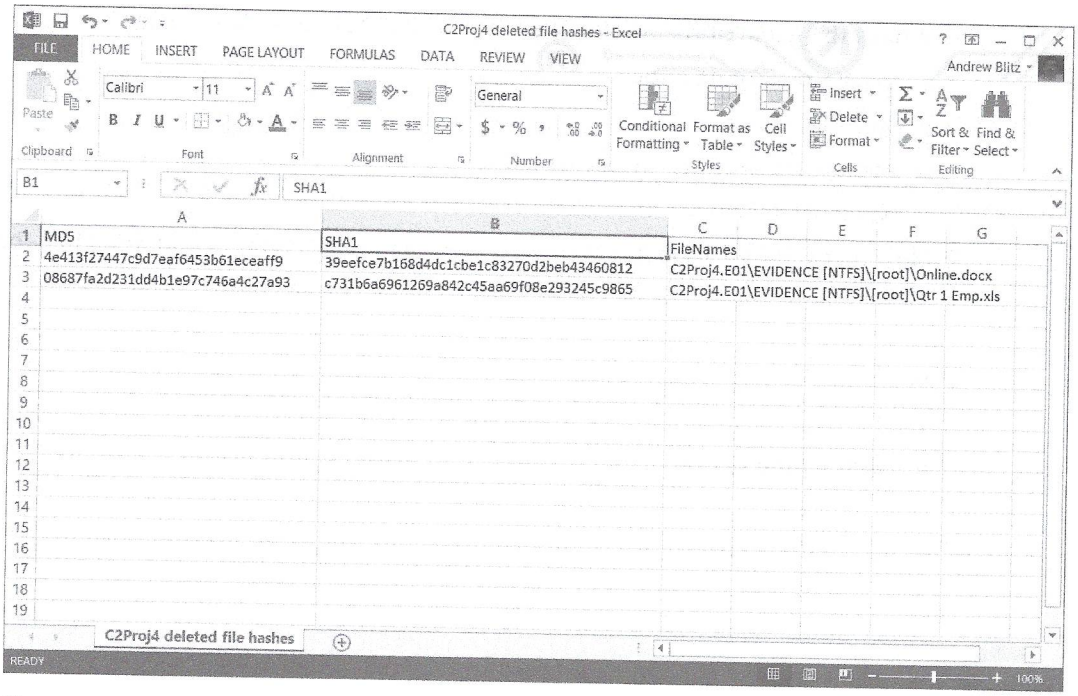

Figure 2-9 Viewing deleted file hashes

Review Questions

1. How many Excel files were recovered in the `C2Proj4.E01` image?
   a. 3
   b. 7
   c. 11
   d. 4
2. How many deleted files were recovered in the `C2Proj4.E01` image?
   a. 2
   b. 7
   c. 11
   d. 4
3. What's the filename of the deleted Excel file in the `C2Proj4.E01` image?
   a. `Annual Payroll 1.xls`
   b. `Profit Potential.xls`
   c. `Qtr 1 Emp.xls`
   d. `Online.xls`

4. What's the name of the deleted Word file in the `C2Proj4.E01` image?
   a. `Employer List.doc`
   b. `Online.docx`
   c. `Rocky Mountain Outline.doc`
   d. None of the above
5. How many SHA-1 hash files were exported to the `C2Proj4 deleted file hashes.csv` file?
   a. 4
   b. 2
   c. 1
   d. None of the above

Lab 3.2 Examining a FAT32 Image

Objectives

FAT32, an improved version of the FAT16 file system, supports disk drives up to 2 terabytes (TB) and filenames up to 255 characters. It's supported by Linux and Mac OS X as well as all versions of Windows except early versions of Windows 95.

After completing this lab, you will be able to:

- Examine a FAT32 dd image in FTK Imager
- Identify a FAT32 file signature

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- FTK Imager
- WordPad or another text editor
- The `C3Proj2.001` file copied from the Chap03 folder on the DVD to your Work\Labs folder

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

Activity

In this lab, you use FTK Imager to examine a FAT32 file structure on a USB device:

1. Double-click the **FTK Imager** desktop icon. If necessary, click **Yes** in the UAC message box.
2. Click **File, Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
3. In the Evidence Source Selection dialog box, click **Browse**, navigate to and click your **Work\Labs** folder, click the **`C3Proj2.001`** file, and click **Open**. Click **Finish** to load the file.
4. The lower-right pane identifies the file system as MSDOS5.0 FAT32. Expand **C3Proj2.001** and **USBDEVICE [FAT32]** in the Evidence Tree pane, and click **C3Proj2.001** to select it. The Properties pane shows the image type as raw (dd) and the original disk geometry as 512 bytes per sector with a total of 249,341 sectors.
5. Click to expand the **[root]** folder. The File List pane shows the files in the `C3Proj2.001` image and their timestamps. The red X next to some files indicates that the user deleted them. Click each file (including the deleted files) to view it.
6. Click the **HEX** toolbar button to display the hexadecimal values for each file. Click the **`Bank Location.doc`** file, view its hex information, and review its details in the Properties pane (see Figure 3-4). The file signature and file size are the same as in FAT16; however, the start cluster and start sector are different than in FAT16.
7. Click the **`interior safe.jpg`** file in the File List pane, and notice the JFIF file signature for a JPEG file. Click the **eyeglasses** toolbar button to see the file in the image viewer.
8. Click to expand the **USBDEVICE [FAT32]** folder, if necessary, and examine the FAT32 file structure and all the files in it. Make a screen capture by pressing **Ctrl+Print Screen**, and then start WordPad. Right-click in the empty document and click **Paste**. Save the file in the **Documents** folder with the filename **`Structures`**, and then exit WordPad.
9. Leave FTK Imager open as you answer the following review questions. When you're finished, exit FTK Imager, and leave your computer running for the next lab.

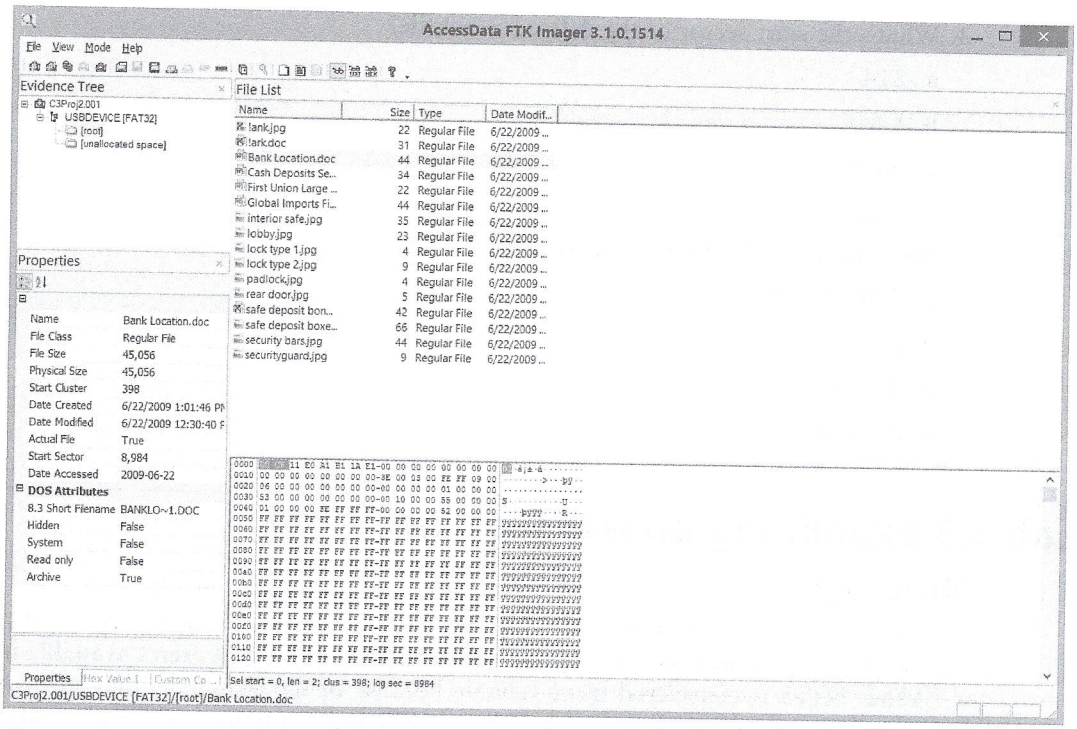

Figure 3-4 Viewing a FAT32 file

Review Questions

1. How many clusters are in the FAT32 image?
   a. 120,229
   b. 120,574
   c. 2048
   d. 8192
2. How many files (existing and deleted) are in the FAT32 image?
   a. 9
   b. 11
   c. 16
   d. 10
3. How many Excel files are in the FAT32 image?
   a. 3
   b. 2
   c. 1
   d. 13

4. What's the start sector of the deleted Excel file?
   a. 214
   b. 8,616
   c. 8,306
   d. 8,262
5. What's the FAT32 drive's volume serial number?
   a. 929E-685C
   b. 2048
   c. 99E-0766
   d. 249,341

Lab 3.3 Examining an NTFS Image

Objectives

NTFS is the default file system in NT 3.51 and later as well as Windows Server OSs because it includes file attributes such as compression and encryption that aren't available in FAT16 or FAT32. NTFS is considered more reliable because of file structures that support redundancy, such as a duplicate Master File Table (MFT) and journaling. NTFS also supports file encryption based on user account information so that multiple users on the same computer can't open each other's encrypted files.

After completing this lab, you will be able to:

- Examine an NTFS `dd` image in FTK Imager
- Identify an NTFS file signature

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- FTK Imager
- WordPad or another text editor
- The `C3Proj3.001` file copied from the Chap03 folder on the DVD to your Work\Labs folder

Estimated completion time: **30–40 minutes**

Activity

In this lab, you examine the NTFS file structure and compare it with the FAT32 file structure on a USB storage device:

1. Double-click the **FTK Imager** desktop icon. If necessary, click **Yes** in the UAC message box.

2. Click **File, Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
3. In the Evidence Source Selection dialog box, click **Browse**, navigate to and click your **Work\Labs** folder, click the **C3Proj3.001** file, and click **Open**. Click **Finish** to load the file.
4. The lower-left pane identifies the file system as NTFS. Expand **C3Proj3.001** and **USBDevice [NTFS]** in the Evidence Tree pane, and click **C3Proj3.001** to select it. The Properties pane shows the image type as raw (dd) and the original disk geometry as 512 bytes per sector with a total of 251,904 sectors.
5. Click the **[root]** folder. The File List pane shows the files in the C3Proj3.001 image and their timestamps. Notice that NTFS has additional hidden folders for bad cluster identification ($BadClus) and two copies of the MFT ($MFT and $MFTMirr), as shown in Figure 3-5.

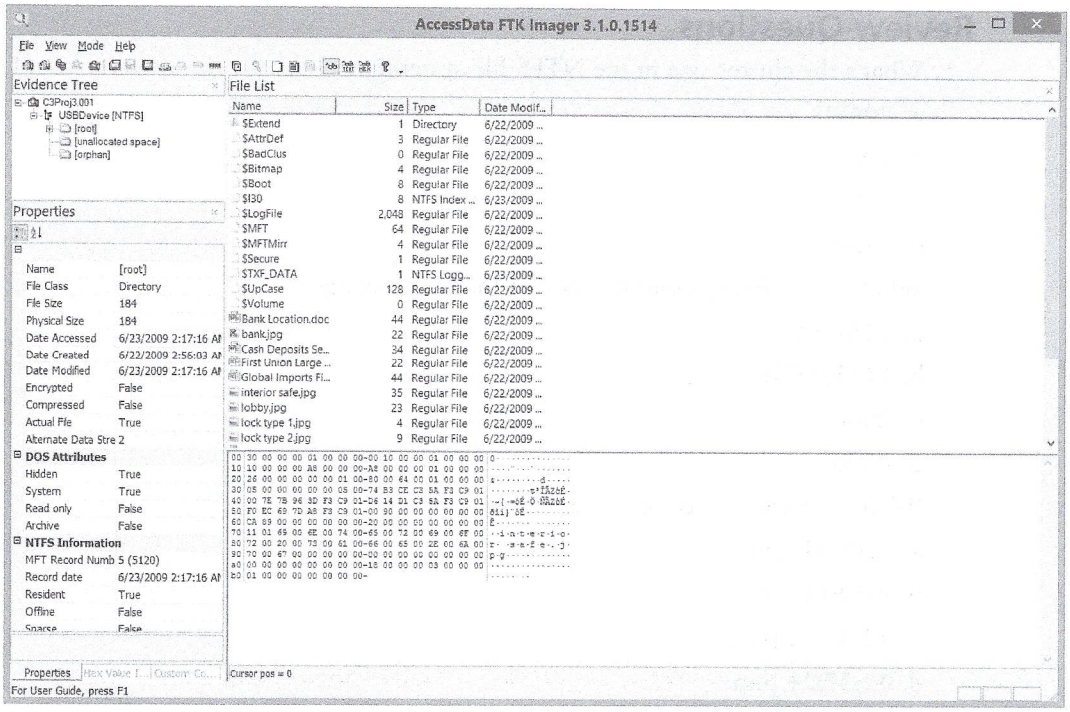

Figure 3-5 Viewing an NTFS image

6. Click each deleted file (with a red X) to view it. Notice that NTFS uses a Date Accessed field in addition to the Date Created and Date Modified fields.
7. Click the **HEX** toolbar button to display the hexadecimal values for each file. Click the **Bank Location.doc** file, view its hex information, and review its details in the Properties pane. The file signature and file size are the same as in FAT16 and FAT32, but the start locations are different.
8. Click the **interior safe.jpg** file in the File List pane, and notice that the JFIF file signature is the same as the FAT16 and FAT32 file signatures for JPEG files. In addition,

NTFS displays Exif file data with information on a digital camera's model and manufacturer as well as its shutter speed, lens aperture, and ISO speed. This information can be useful to forensics investigators.

9. Notice the complex file structure of the [root] folder, compared with other file systems. Expand all subfolders under [root] to see, for example, the $Secure attribute indexes that support NTFS file permissions and the [orphan] folder used to repair files with broken pointers or corrupted indexes.
10. Make a screen capture, and save it in the WordPad **Structures** document. Exit WordPad.
11. Leave FTK Imager open as you answer the following review questions. When you're finished, exit FTK Imager, and leave your computer running for the next lab.

Review Questions

1. What's the cluster size in the NTFS file system?
   a. 2048
   b. 1024
   c. 4096
   d. 31,487
2. What's the volume serial number of the NTFS image?
   a. E16-566
   b. E6FE-1C5F
   c. 2048
   d. 4096
3. What time was the `bank.jpg` file deleted?
   a. 2:15:31 a.m.
   b. 4:59:14 p.m.
   c. 12:37:00 p.m.
   d. 12:37:21 p.m.
4. What's the physical size of the deleted `mark.doc` file?
   a. 31,744
   b. 32,768
   c. 14,808
   d. 118,464
5. What folder in the NTFS image isn't in the FAT32 image?
   a. [unallocated space]
   b. [root]
   c. [orphan]
   d. [encryption]

Lab 3.4 Examining an HFS+ Image

Objectives

HFS+, the file system for Mac OS X 10.4 and later, maintains a journal similar to NTFS to keep track of file changes attempted but not completed because of file errors or hard disk crashes. This journaling feature allows the file system to recover from sudden disk crashes or power losses during a write operation. HFS+ is less susceptible to file corruption caused by broken or missing pointers between blocks of data on a storage device.

After completing this lab, you will be able to:

- Process an HFS+ image in FTK Imager
- Explain the difference between HFS+, FAT32, and NTFS file systems
- Find deleted files

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- FTK Imager
- WordPad or another text editor
- The `C3Proj4.001` image file copied from the Chap03 folder on the DVD to your Work\Labs folder

Estimated completion time: **10–15 minutes**

Activity

In this lab, you examine the HFS+ file structure and compare it with the FAT32 and NTFS file structures on a USB storage device:

1. Double-click the **FTK Imager** desktop icon. If necessary, click **Yes** in the UAC message box.
2. Click **File, Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
3. In the Evidence Source Selection dialog box, click **Browse**, navigate to and click your **Work\Labs** folder, click the **`C3Proj4.001`** image file, and click **Open**. Click **Finish** to load the image file.
4. Expand **C3Proj4.001** and **USBDevice[HFS+]** in the Evidence Tree pane, and click **C3Proj4.001** to select it. The file properties show the image type as raw (dd) and the original disk geometry as 512 bytes per sector with a total of 249,228 sectors.
5. Expand the **USBDevice** folder in the Evidence Tree pane. The File List pane shows the files in the `C3Proj4.001` image and their timestamps (see Figure 3-6). Notice that there's no [root] folder. Examine the hidden folders (.journal and .journal_info_block) used for journaling file transactions. The Properties pane also shows the UNIX permissions for the USBDevice folder: read, write, delete, and modify.

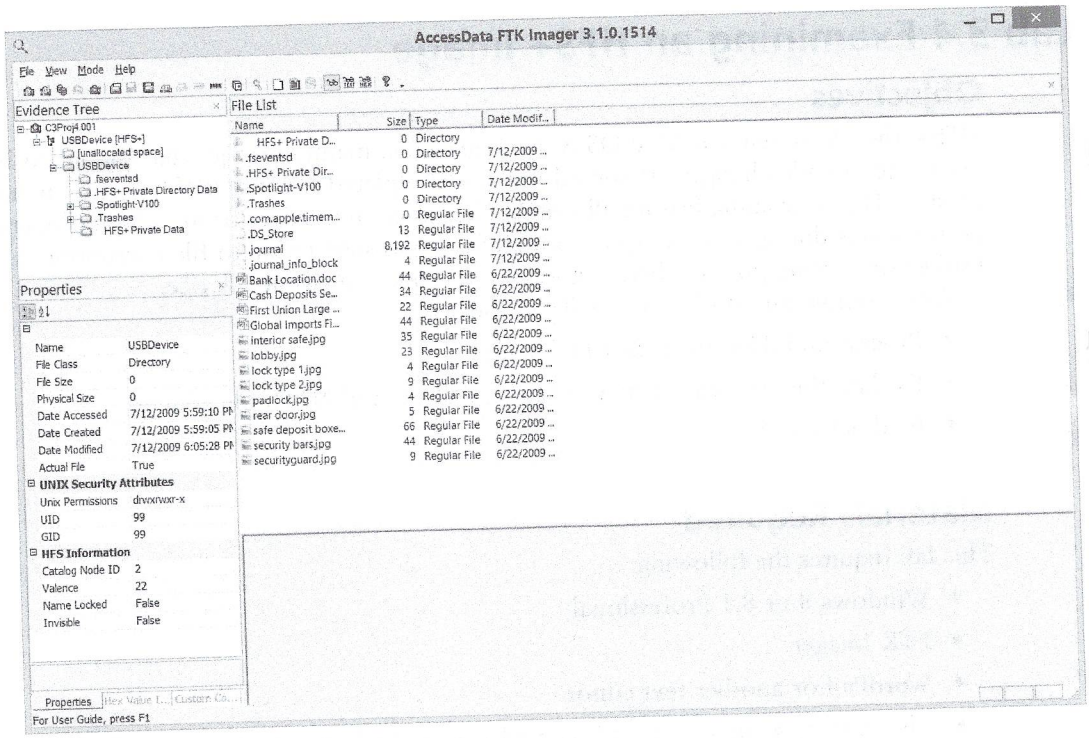

Figure 3-6 Viewing an HFS+ image

6. Expand the **.Trashes** folder and click the **501** folder. You should see the same deleted files you've seen in previous labs, but HFS+ doesn't add a red X to indicate they were deleted.
7. Click each file with an extension to view its properties and security attributes. The Properties pane lists a Date Accessed field in addition to the Date Created and Date Modified fields.
8. Click the **HEX** toolbar button to display the hexadecimal values for each file. Click the **`Bank Location.doc`** file, view its hex information, and review its details in the Properties pane. The file signature is the same as in FAT16, FAT32, and NTFS, but the start locations are different in HFS+.
9. Click the **`interior safe.jpg`** file in the File List pane, and notice that the JFIF file signature is the same as in FAT16 and FAT32. HFS+ also displays Exif file data, as NTFS does.
10. Examine the complex file structure of the USBDevice folder. Make a screen capture, and save it in the WordPad **`Structures`** document. Exit WordPad.
11. Leave FTK Imager open as you answer the following review questions. When you're finished, exit FTK Imager.

Review Questions

1. What's the cluster size in the HFS+ image?
   a. 1024
   b. 2048
   c. 4096
   d. 3077
2. How many clusters are in the HFS+ image?
   a. 31,153
   b. 21,866
   c. 28,099
   d. 249,228
3. What date was the HFS+ partition created?
   a. 6/22/2009
   b. 7/16/2009
   c. 7/12/2009
   d. 7/14/2009
4. What folder doesn't exist in HFS+ but is found in FAT32 and NTFS?
   a. [encryption]
   b. [USB]
   c. [unallocated space]
   d. [root]
5. In what folder are deleted files stored?
   a. .Trashes
   b. 501
   c. [orphan]
   d. [unallocated space]