COSC6410 Lab Assignment 1

Please submit through Blackboard by midnight September 4.

The purpose of this lab is:

1. Install and get familiar with some digital forensics tools that we are going to use in later assignments (Part 1).
2. Get familiar with Windows file system and the file conversion and numbering formats (Part 2).

Submission requirement:
Part 1: submit the answers for all the review questions.
Part 2: submit the last screenshot of what your computer display (i.e., Figure 5: Master File Table displayed in the hex editor)

Part 1

Lab 1.1 Installing OSForensics in Windows

Objectives

Investigating digital evidence takes time because of the large storage capacity of modern hard disk drives. In addition, operating systems (OSs) and applications are typically large collections of files and executable programs that work together to form a user interface. OSForensics combines an extensive array of digital forensics tools into a single stand-alone software suite. It enables investigators to analyze storage devices and search for files, folders, e-mails, documents, pictures, and any remaining evidence that might have been deleted and document their findings.

Forensics investigators need to search large volumes of data stored on different types of storage media, such as CDs and DVDs, flash drives, and hard disk drives, for potential digital evidence. In many criminal cases, the suspect might have attempted to delete a file or modify it in some way to prevent other users from seeing it. OSForensics can recover deleted or corrupted files and display the contents, even if they're encrypted with a password. Additional features, such as keyword searching, enable investigators to search for specific words related to the crime or search for number patterns that might reveal telephone or credit card numbers.

OSForensics also creates hash values for every file so that investigators can search for known file types, changed or altered files, malware, and legitimate application and OS files. File hashes are mathematically derived hexadecimal values that uniquely identify both known and unknown files. Hashing is an important feature because it preserves the chain of custody by making sure files haven't been altered or changed and recovered evidence doesn't change over time. OSForensics also supports creating hash sets that allow investigators to import known OS and application hash values into OSForensics to distinguish them from potential file evidence. In this lab, you install OSForensics in Windows to begin investigating digital evidence.

After completing this lab, you will be able to:

- Install OSForensics on a Windows 8 or 8.1 Professional computer
- Explain the OSForensics features that help forensic investigators recover digital evidence

Materials Required

This lab requires the following:

- The `osf.exe` installation file on the DVD
- The `OSFHashSet.zip` file (for your Windows version) on the DVD
- Windows 8 or 8.1 Professional

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

Activity

In this lab, you install OSForensics:

1. Open File Explorer, and copy the **`osf.exe`** file on the DVD to the **Documents** folder on your computer. Right-click this file and click **Run as administrator** to begin the installation. In the User Account Control dialog box, click **Yes** to continue.
2. Click **Next** in the Setup - OSForensics dialog box to continue.

3. In the License Agreement window, click the **I accept the agreement** option button, and then click **Next**.
4. In the Select Destination Location window, shown in Figure 1-1, click **Next** to continue. In the Select Start Menu Folder window, click **Next**.

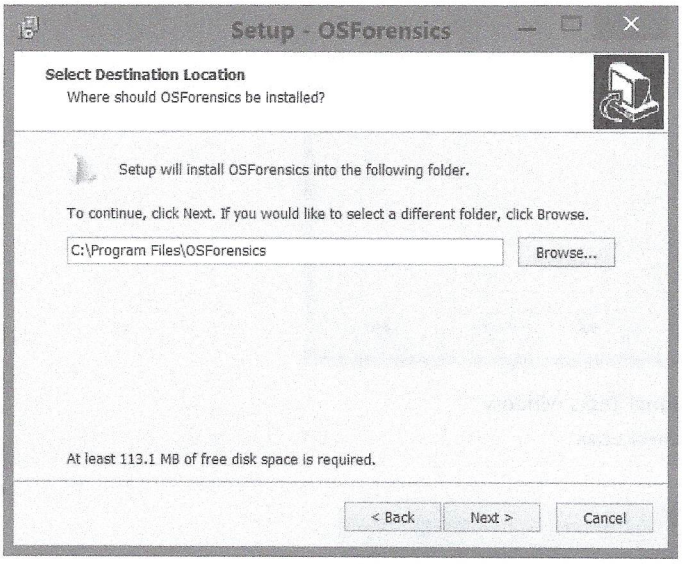

Figure 1-1 The Select Destination Location window

Source: PassMark Software, www.osforensics.com

5. In the Select Additional Tasks window, leave the **Create a desktop icon** check box selected, as shown in Figure 1-2, and click **Next** to continue. Click **Install** in the Ready to Install window to finish the installation.
6. In the Information window, click **Next**. Leave the **Launch OSForensics** check box selected, and click **Finish** to install the program. When the program starts automatically, click the **Continue Using Free Version** button. (You might need to do this each time you run OSForensics.) Exit OSForensics.
7. In File Explorer, browse to the DVD and find the correct `OSFHashSet.zip` file for your version of Windows. Right-click this file and click **Extract All**.
8. In the Select a Destination and Extract Files window that opens, type **C:\ProgramData\PassMark\OSForensics\hashSets** in the "Files will be extracted to this folder" text box, and leave the **Show extracted files when complete** check box selected (see Figure 1-3).
9. Click **Extract**. After Windows extracts the files, you can view them in the C:\ProgramData\PassMark\OSForensics\hashSets folder (see Figure 1-4). Installing hash sets allows you to identify known files, such as OS and program files, during an investigation. Close any open windows, and leave your computer running for the next lab.

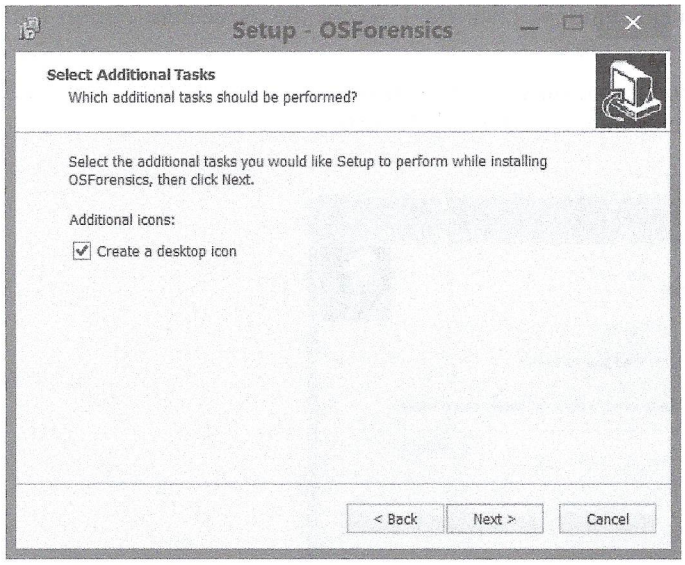

Figure 1-2 The Select Additional Tasks window

Source: PassMark Software, www.osforensics.com

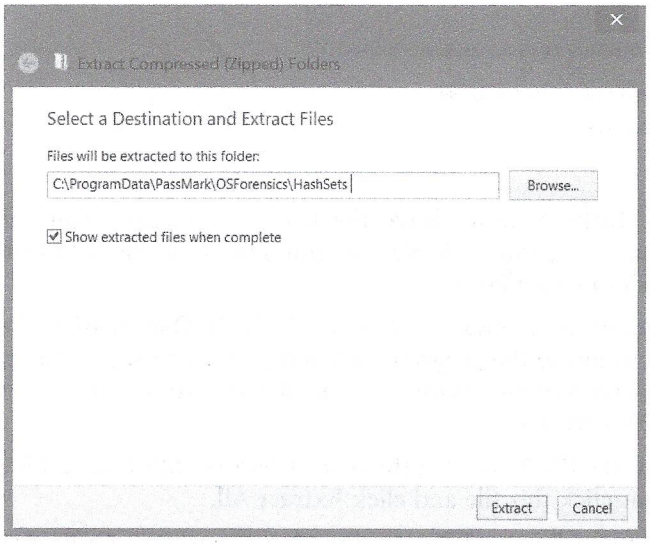

Figure 1-3 Extracting compressed files

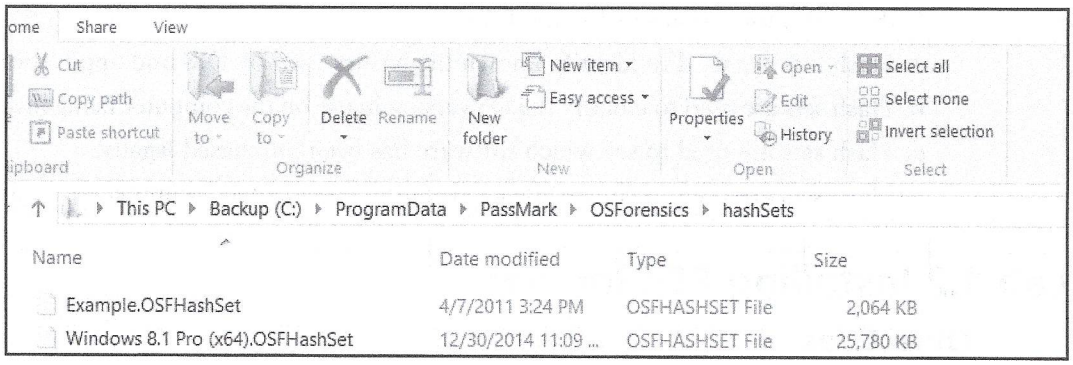

Figure 1-4 Extracted files in the hashSets folder

Review Questions

1. Why is OSForensics an important forensics tool?
   a. It can be used to troubleshoot a computer.
   b. It can be used to test a computer's operability.
   c. It can be used to help digital forensics investigators locate potential evidence.
   d. It can be used to recover human DNA.
2. OSForensics can search for which of the following types of files? (Choose all that apply.)
   a. E-mail
   b. Graphics
   c. Deleted files
   d. Registry files
3. What's a file hash?
   a. A hexadecimal value obtained mathematically from a file
   b. The name of a software program's vendor or manufacturer
   c. The size of the computer's hard disk
   d. The file size of potential evidence
4. Which of the following statements is true?
   a. File hash information can be found in File Explorer.
   b. File hashes can verify that the chain of custody has been maintained.
   c. File hashes can indicate that software has been purchased legally.
   d. File hashing values aren't important to a digital investigator.

5. OSForensics uses hash sets for what purpose?
   a. Hash sets are used to identify known file hashes used by OSs and applications.
   b. Hash sets are used to identify the OS version in use on the computer being investigated.
   c. Hash sets are used to see which software has been purchased legally.
   d. Hash sets are used to copy evidence from the investigated computer to a USB drive.

Lab 1.2 Installing FTK Imager

Objectives

Forensics investigators are required to protect the integrity of digital evidence from the time it's seized until the end of the trial. This protection, known as "maintaining the chain of custody," ensures that the original data hasn't been changed during the investigation. Forensics investigators duplicate digital evidence by using a bit-stream process called "imaging," which preserves the original evidence along with other system files and duplicates the entire storage device with files intact to another lab storage device. Imaging allows examining the duplicated storage device without the risk of damaging potential digital evidence. This bit-stream process makes an exact byte-for-byte copy of the original storage device, which preserves the physical and logical file locations and any unpartitioned space. This process is important because remnants of deleted files still exist on a storage device until they're overwritten during computer operations. The file remnants can be searched and repaired to recover deleted files and make them readable. Imaging also generates file hashes that can be used to identify potential evidence and validate its integrity throughout the investigative process.

FTK Imager can also be used to preview digital files to determine whether evidentiary data exists before starting an extensive investigation. If potential forensic data is located, FTK Imager can then forensically duplicate the storage device to process the data safely. FTK Imager supports the following file systems: Microsoft FAT12, FAT16, FAT32, and NTFS; Linux/UNIX Ext2, Ext3, and Ext4; and Mac HFS and HFS+. It can produce hard disk formats supported by FTK, EnCase, OSForensics, Expert Witness, Linux dd, Symantec Ghost, SMART, and VMware. Although FTK Imager can copy encrypted files, it can't actually decrypt them. In this lab, you install FTK Imager in Windows.

After completing this lab, you will be able to:

- Install FTK Imager in Windows
- Explain the purpose of using an imager tool to copy digital evidence

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional

Estimated completion time: **10 minutes**

Activity

In this lab, you install FTK Imager:

1. Start a Web browser, go to **http://accessdata.com/product-download**, and download FTK Imager 3.3.0. Follow instructions to register the product. Right-click the installation file and click **Run as administrator** to begin the installation.
2. Click **Run** in the Open File Security Warning message box, if necessary, and click **Yes** in the UAC message box.
3. In the welcome window of the AccessData FTK Imager - InstallShield Wizard, click **Next**. In the License Agreement window, click the **I accept the terms in the license agreement** option button, and then click **Next** to continue. In the Destination Folder window, click **Next**.
4. Click **Install** to install the software.
5. When the installation has finished, click to clear the **Launch AccessData FTK Imager** check box, and click **Finish** to complete the installation. Close any open windows, and leave your computer running for the next lab.

Review Questions

1. FTK Imager can be used to search all the following except what?
   a. Deleted files
   b. Documents
   c. Graphics
   d. Encrypted files
2. FTK Imager is used primarily to produce which of the following?
   a. Hard disk images that can be analyzed by forensics software
   b. Forensic evidence
   c. Computer manufacturer information
   d. DNA evidence
3. Why do forensics investigators work with bit-stream images?
   a. Image files are smaller than the actual hard disk files.
   b. Only image files contain forensic evidence.
   c. An image file can be examined without damaging the original evidence.
   d. The original storage device can't be analyzed without the original computer.
4. FTK Imager can detect and view encrypted files. True or False?
5. Bit-stream imaging is the process of _____.
   a. creating hash values from files on a storage device
   b. extracting readable information from encrypted files
   c. duplicating data on storage devices for forensic analysis
   d. determining the forensic nature of digital evidence

Lab 1.3 Installing ProDiscover Basic

Objectives

Forensics investigators often use more than one forensics tool to analyze stored files and search for potential evidence. ProDiscover Basic is a popular forensics tool with many features, such as the capability to produce file hashes, and includes several search tools designed for security. It's used by law enforcement agencies, system administrators, consultants, and forensic accountants to search digital evidence and gather the data needed for civil or criminal litigation. In addition, ProDiscover includes incident response and intrusion detection features for generating reports on intruders attempting to take control of network resources. It also supports searching entire storage disks for existing and deleted files, graphics, Internet history, and Windows Registry keys. It supports searching the FAT12, FAT16, FAT32, NTFS, Sun Solaris UFS, and Ext2 and Ext3 file systems; basic and dynamic disks; and RAID disk drives.

ProDiscover can also extract Exchangeable Image File (Exif) format information, including the camera model, shutter speed, and lens as well as the date and time a photo was taken. This information can be useful in determining which camera took a picture. In addition, it can export Windows disk images to a VMware virtual machine file. Virtualization is the process of running a guest OS inside a host OS, which enables forensics investigators to view an image as a computer running within another computer. In this lab, you install ProDiscover in Windows.

After completing this lab, you will be able to:

- Install ProDiscover Basic in Windows
- Explain the features of ProDiscover Basic

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional
- The ProDiscover Basic installation file on the DVD

Two versions of ProDiscover are included on the DVD. Use `ProDiscoverRelease8202Basicx86.zip` for 32-bit Windows systems and `ProDiscoverRelease8202Basicx64.zip` for 64-bit Windows systems.

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

Activity

In this lab, you install ProDiscover Basic:

1. Open File Explorer, and copy the **`ProDiscoverRelease8202Basicx86.zip`** or **`ProDiscoverRelease8202Basicx64.zip`** file on the DVD to the Documents folder on your computer. Right-click this file and click **Extract All** to extract the contents.
2. When the Select a Destination and Extract Files window opens, click **Browse**. Navigate to and click the **Documents** folder, click **OK**, and then click **Extract** to extract the installation files.

3. In File Explorer, right-click **ProDiscoverRelease8202Basicx86.exe** or **ProDiscoverRelease8202Basicx64.exe** and click **Run as administrator** to begin installing ProDiscover Basic. In the UAC message box, click **Yes**.
4. The Install Wizard starts. This process might take a few minutes. Click **Next** in the Welcome to the InstallShield Wizard for ProDiscover Basic 8.2.0.2 window to continue.
5. In the License Agreement window, click the **I accept the terms in the license agreement** option button, and then click **Next**. In the Readme Information window, click **Next** to continue.
6. In the Customer Information window, type your full name in the User Name text box, and then click **Next**.
7. In the Destination Folder dialog box, accept the default location, and then click **Next** to continue.
8. In the InstallShield Wizard Completed window, click **Finish**. Close any open windows, and leave your computer running for the next lab.

Review Questions

1. ProDiscover can be used to search all the following file systems except _____.
   a. FAT16
   b. HFS+
   c. NTFS
   d. FAT32
2. The Exif format contains information on which of the following? (Choose all that apply.)
   a. Date and time a photo was taken
   b. The shutter speed
   c. When the camera was purchased
   d. The camera model
3. ProDiscover can search digital devices for which of the following? (Choose all that apply.)
   a. Macintosh files
   b. RAID data
   c. Linux files
   d. UNIX files
4. ProDiscover isn't capable of producing file hash values. True or False?
5. Which of the following statements is correct?
   a. ProDiscover can decrypt encrypted Microsoft Word documents.
   b. ProDiscover can decrypt encrypted Microsoft Excel spreadsheets.
   c. ProDiscover can decrypt encrypted e-mail files.
   d. ProDiscover can't decrypt any encrypted files.

Lab 1.4 Installing AccessData Registry Viewer

Objectives

The Windows Registry is the central repository that stores options and settings for hardware, OS software, and user-specific information, such as account usernames and hashed passwords. It's responsible for booting into the Windows environment based on user preferences and contains valuable forensic information. AccessData Registry Viewer enables forensics investigators to view the Registry's contents and search for data such as recently opened files, removable storage devices, user account names, deleted files in the Recycle Bin, and other potential evidence. Although the Registry includes file information, such as timestamps, it doesn't actually store files—only their physical locations. Because of Windows protection systems, you can't view Registry information in the Windows Registry Editor without tools such as Registry Viewer.

The Registry contains five critical system folders (hives) with detailed information on the system state of a Windows computer at any point, including devices that might have been attached and later removed or deleted. Therefore, a forensics analysis of the Registry can yield information that has been deliberately destroyed to hide the details of a crime. The Registry also contains a history of Web sites visited, Internet queries including timestamps, and a list of all programs installed on the computer. In this lab, you install AccessData Registry Viewer in Windows.

After completing this lab, you will be able to:

- Install Registry Viewer in Windows
- Explain the purpose of Registry Viewer

Materials Required

This lab requires the following:

- Windows 8 or 8.1 Professional

Estimated completion time: **10 minutes**

Activity

In this lab, you install Registry Viewer:

1. Start a Web browser, go to **http://accessdata.com/product-download**, and download Registry Viewer 1.8.0.5. Follow instructions to register the product. Right-click the installation file and click **Run as administrator** to start the installation. Click **Yes** in the UAC message box.
2. Click **Next** in the AccessData Registry Viewer - InstallShield Wizard welcome window.
3. In the License Agreement window, click the **I accept the terms in the license agreement** option button, and then click **Next**.

4. In the Destination Folder window, accept the default destination folder **C:\Program Files\AccessData**, and then click **Next**.
5. Click **Install**, and then click **Finish**. Registry Viewer is now installed, and your desktop should include icons for OSForensics, FTK Imager, ProDiscover Basic, and AccessData Registry Viewer. Close any open windows, and shut down your computer.

Review Questions

1. The Windows Registry is responsible for which of the following?
   a. Registering Windows software with Microsoft
   b. Creating the NTFS file system
   c. Booting into the Windows environment
   d. Deleting files and folders
2. The Registry contains valuable forensics information, such as which of the following? (Choose all that apply.)
   a. Account usernames and hashed passwords
   b. Where software was purchased
   c. When files were created or deleted
   d. Duplicate copies of Microsoft Word documents
3. Registry Viewer can recover forensics information, such as _____, that can't be viewed in Windows Registry Editor.
   a. when software was purchased
   b. what software is considered illegal
   c. the version of the HFS+ file system
   d. a history of Web sites visited
4. Which of the following statements is true?
   a. The Registry contains information on the Windows environment.
   b. The Registry contains a list of Linux files.
   c. The Registry doesn't contain useful forensics information.
   d. The Registry doesn't contain hard disk information that has been deleted.
5. The Registry is composed of _____ hives containing system data.
   a. three
   b. seven
   c. five
   d. four

Part 2:

1. Find a personal computer running Microsoft Windows.
2. Go to http://accessdata.com/product-download/digital-forensic/ftk-imagerversion-3.3.0 and download FTK Imager. Once downloaded, **Start** FTK Imager.
3. Click **File** and then, from the displayed menu, click **Add Evidence Item**.
4. In the displayed **Select Source** dialog box, verify that **Physical Drive** is selected and click **Next**.
Clicking the down arrow displays the different physical drives available to be imaged.
5. With **\\.\PHYSICALDRIVE0...** selected, click **Finish**. Compare your screen with Figure 1.
Notice that \\.\PHYSICALDRIVE0 was added to the Evidence Tree.

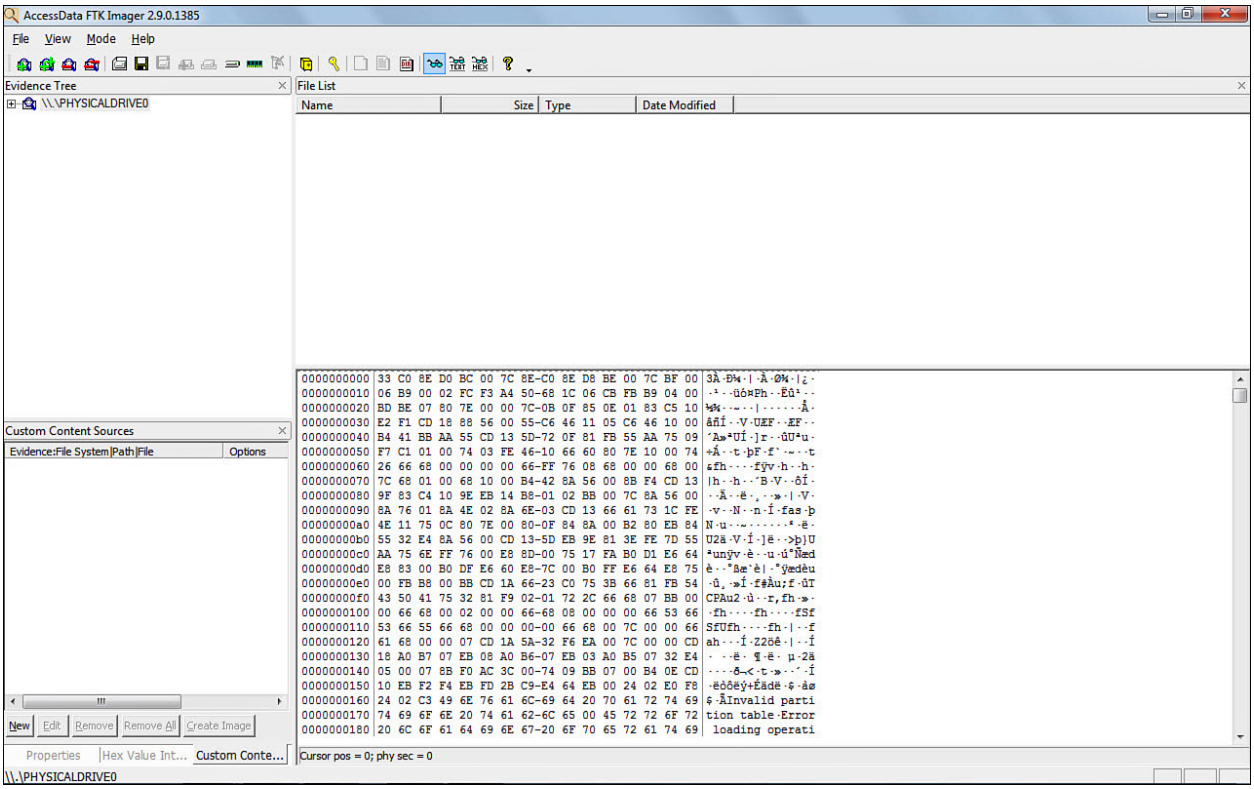

FIGURE 1 Adding the drive to the Evidence Tree

6. Click the \\.\PHYSICALDRIVE0 **Expand button** (see Figure 2.).
Your screen will be slightly different, based on the number of partitions on your system.

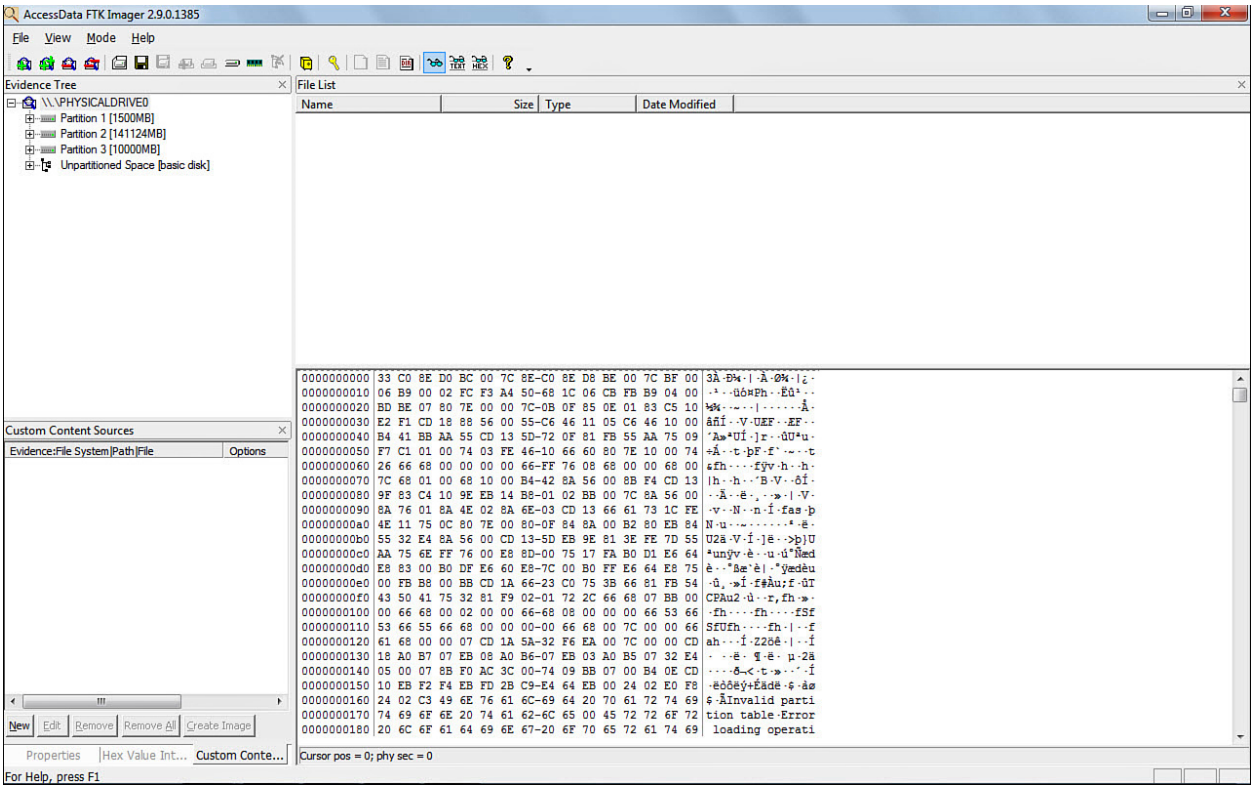

FIGURE 2 Expand button

7. Click **Partition 1** and then compare your screen with Figure 3.
Notice that the name of the file system (NTFS) is displayed in the hex editor.

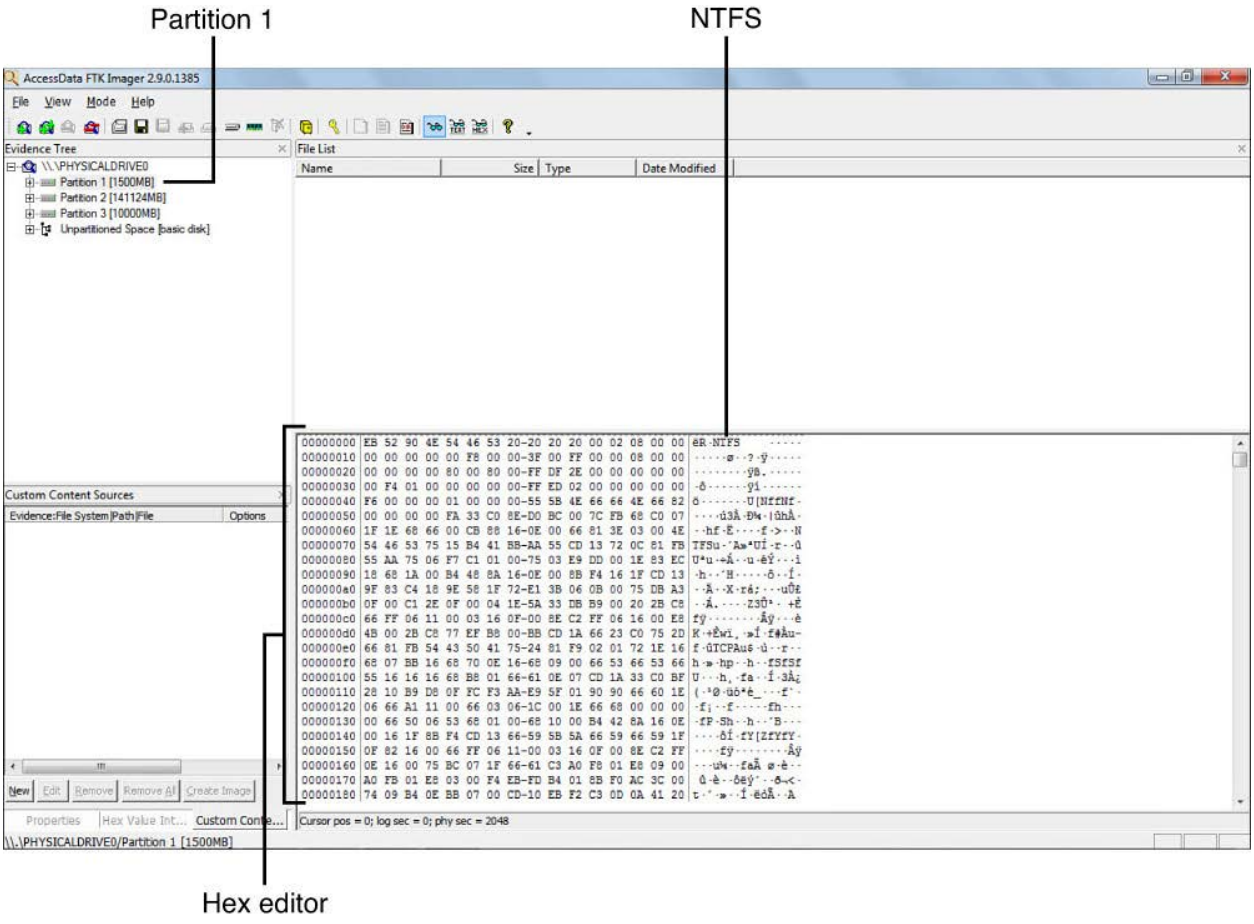

FIGURE 3 Partition 1 selected

8. In the first row of the hex editor, using your mouse, highlight the values **4E 54 46 53**. Compare your screen with Figure 4. Notice that NTFS is highlighted on the right.

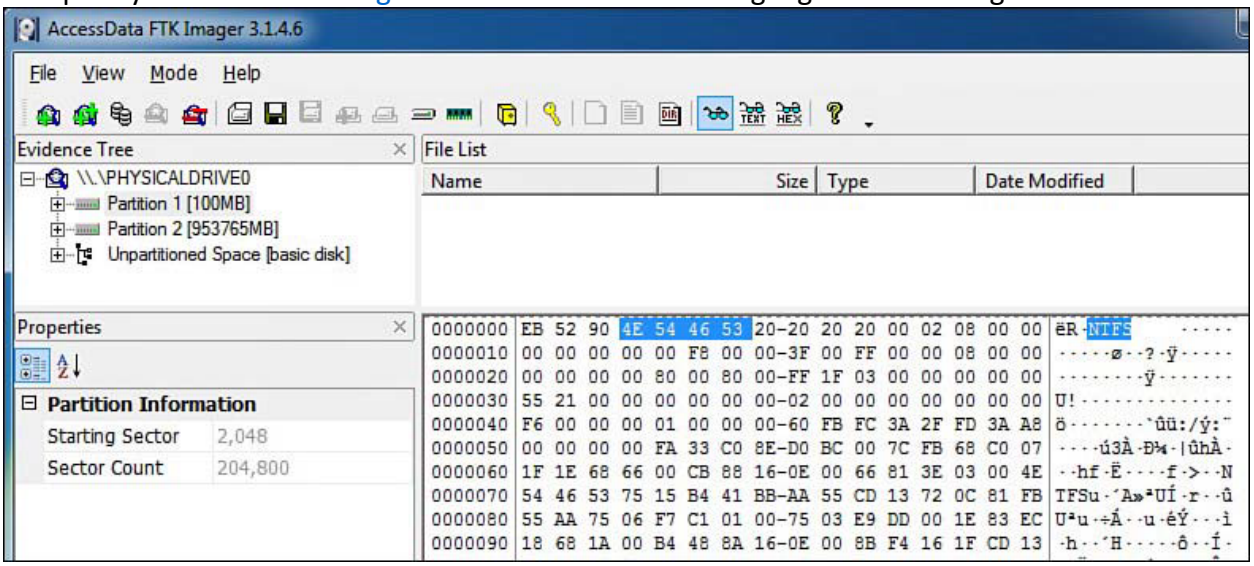

FIGURE 4 NTFS highlighted

9. Click the Partition 1 **Expand button**, and then click the **[root]** directory.

10. In the **File List**, scroll down to see all the files. Click **$MFT**, and then compare your screen with Figure 5. Notice that the hex editor displays the first entry in $MFT as FILE0.

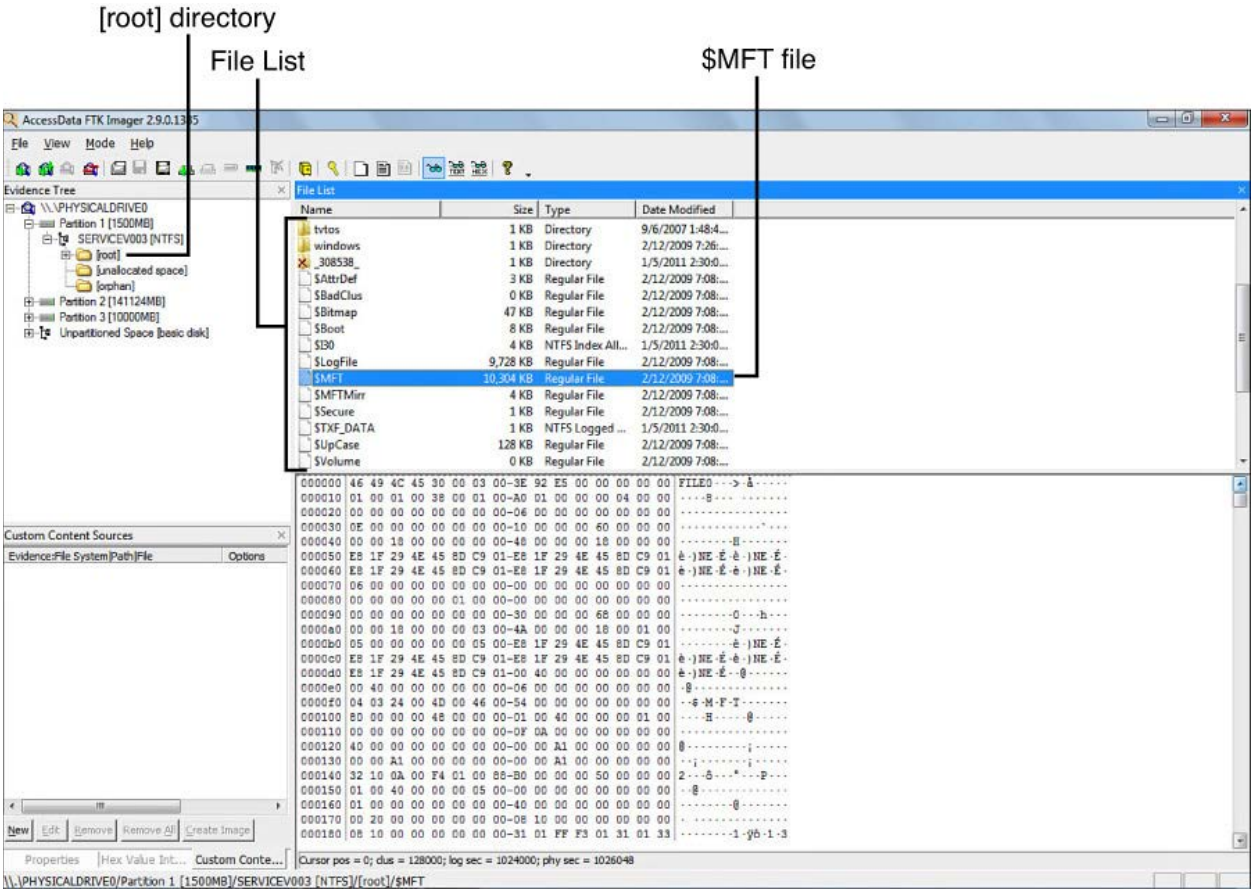

FIGURE 5 Master File Table displayed in the hex editor