DIGITAL FORENSICS LAB SERIES

Lab 10: Analyzing a NTFS Partition with PTK

Objective: File and Program Activity Analysis

Document Version: 2015-09-28

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction

This lab includes the following tasks:

1. Examining the FAT and NTFS File Systems
2. Using a HEX Editor to Explore an NTFS Partition
3. Verifying and Viewing the Image Details
4. Analyzing a NTFS Partition with PTK

Objective: File and Program Activity Analysis

Performing this lab will provide the student with a hands-on lab experience meeting the File and Program Activity Analysis Objective:

The candidate will demonstrate an understanding of how the Windows registry, file metadata, memory, and filesystem artifacts can be used to trace user activities on suspect systems.

Understanding file systems is key to understanding computer forensics investigations. File systems store data using a variety of methods. The NTFS file system is commonly used on Microsoft Windows operating systems. It can also be utilized by Linux and Mac OS X.

NTFS – The New Technology File System (NTFS) was originally introduced with Windows NT. NTFS is a journaling file system, which means it keeps a log of changes being written to the disk. If a computer is shutdown improperly, it will have a better chance of recovery if it has a journaling file system. Files and folder access can be restricted with the security feature of NTFS. Starting with Windows 2000, Microsoft included the Encrypted File System, or EFS, as an NTFS feature. EFS allows users to encrypt files to protect against unauthorized access.

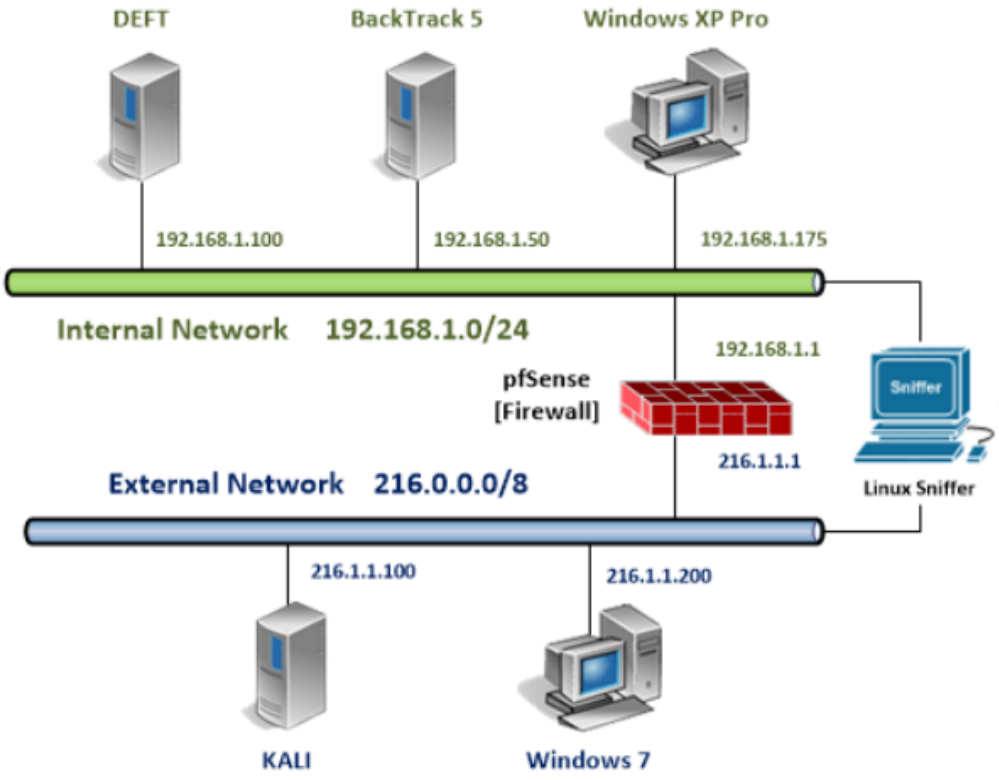
PTK – An open source forensic suite that will allow you to analyze disk images.

ADS – An Alternate Data Stream, or ADS, is a feature of the NTFS file system that allowed compatibility with older versions of the Mac OS. The 'feature can be utilized by an individual who is attempting to hide data on their system with an NTFS volume.

timestomp – The timestomp command allows you to change file Modified, Access, and Created times. The command can only change MAC (Modified Access Created) times on an NTFS volume.

$MFT – The Master File Table is similar to the Table of Contents for an NTFS volume.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
BackTrack 5 R3 Internal Machine	192.168.1.50	root	toor
Windows 7 External Machine	216.1.1.200	student	password

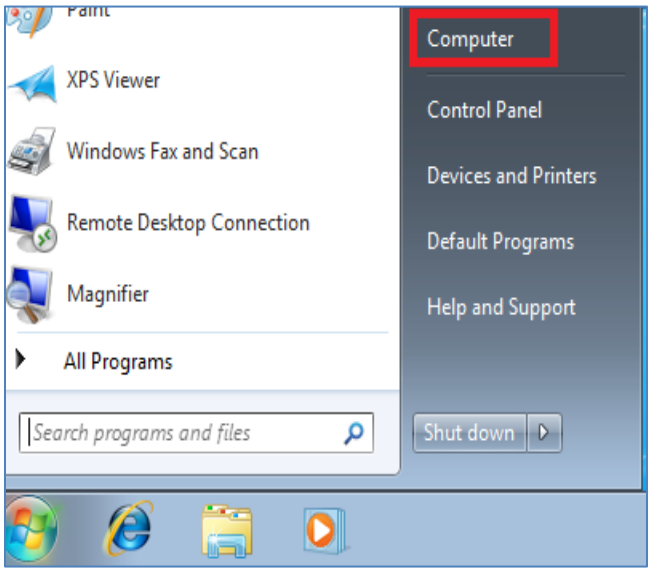
1 Examining the FAT and NTFS File Systems

The most common Windows file systems are FAT and NTFS. There are several versions of NTFS. The older version included on Windows NT did not support the Encrypted File System (EFS). Starting with Windows 2000, NTFS versions support the EFS feature.

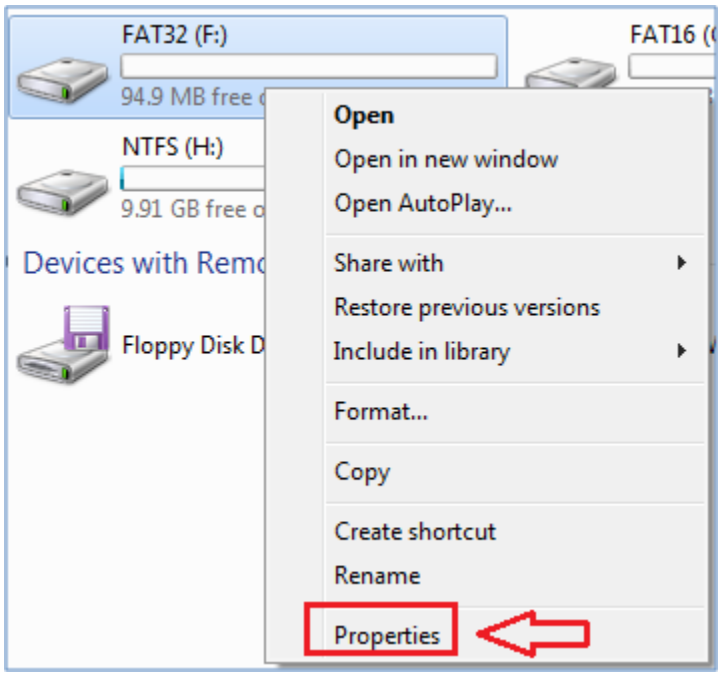
1.1 Viewing File Systems

1. Login into the **Windows 7 Machine on the External Network** by clicking on the **Windows 7** icon on the topology. If prompted, select the **Boot from First Hard Disk** option and press **Enter**.
2. If required, enter the username, **student**.
3. Type in the password, **password,** and press **Enter** to log in.

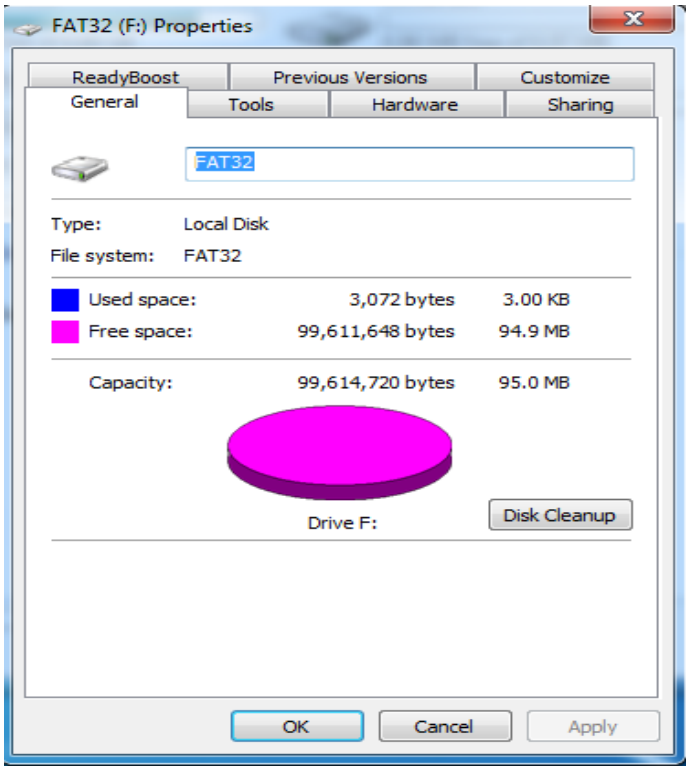
4. Click on the Start button and click on the link to **Computer**.



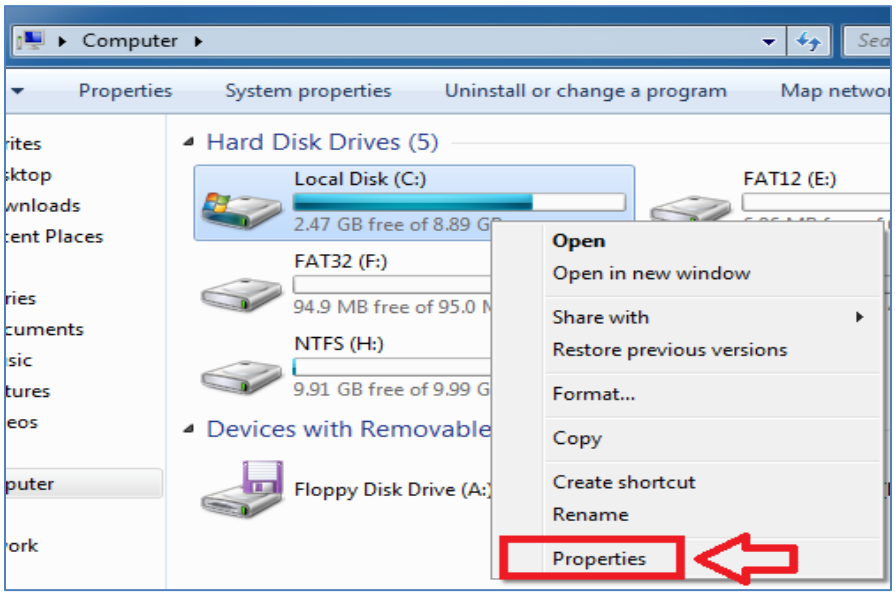
5. Right-click on the FAT 32 Drive (F:) and go to the **Properties** tab.



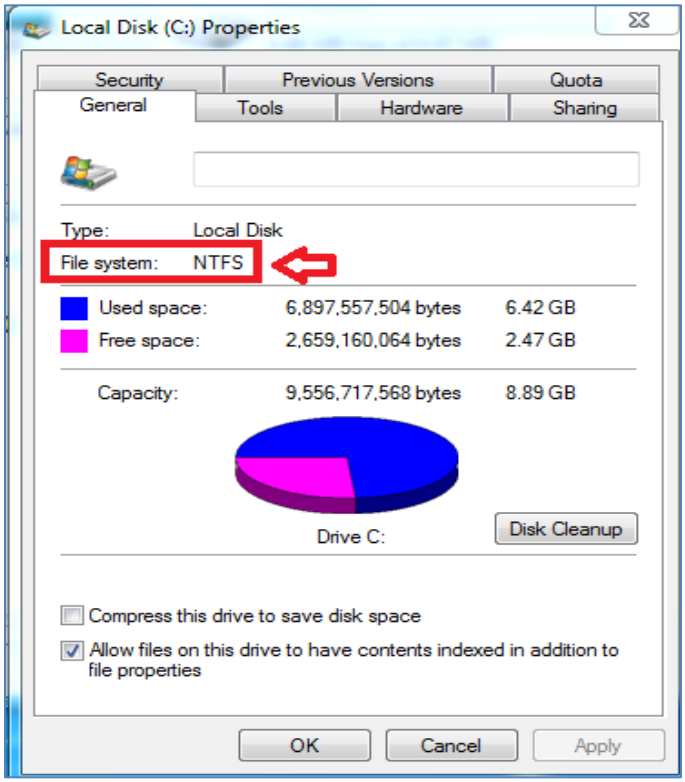
6. Notice that there is no Security or Quota tab on a FAT32 Volume. Close the FAT32 (F:) Properties window.



7. Right-click on Local Disk (C:) and go to the **Properties** tab.

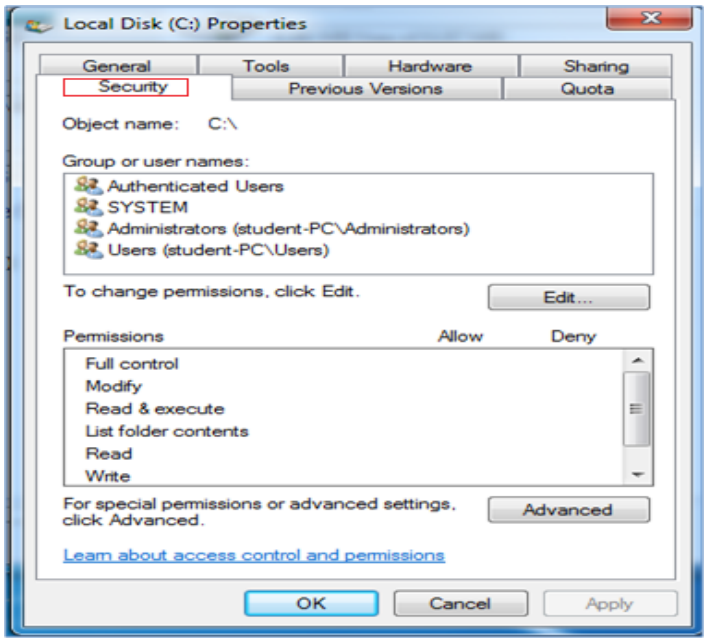


8. View the File system type, which should be listed as **NTFS.**

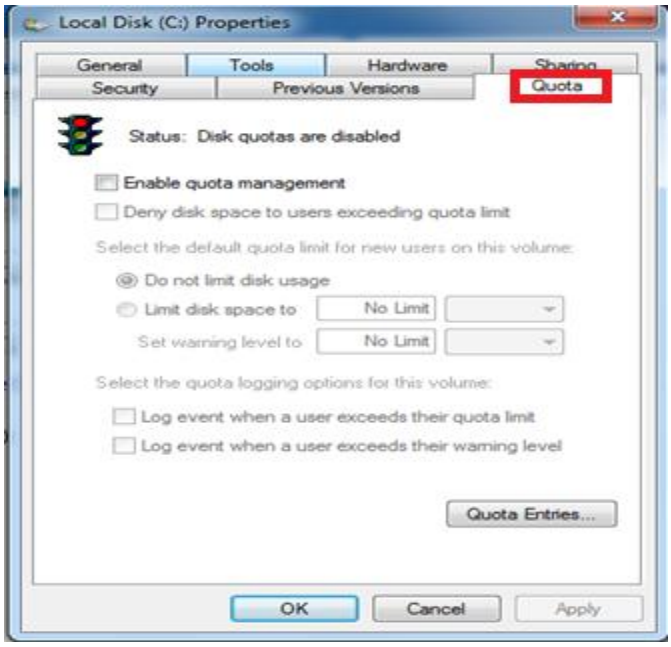


On NTFS volumes, security permissions and quotas can be configured. Security permissions can be configured to restrict access to files or folders. Quotas are used to restrict the amount of storage for each user to prevent a disk from running out of space.

9. Click on the **Security** tab. This is where Access Control Lists can be configured.

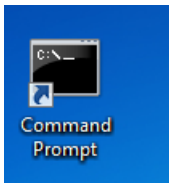


10. Click on the **Quota** tab. This is where disk usage can be restricted for users. Close the Local Disk (C:) Properties and Computer windows.

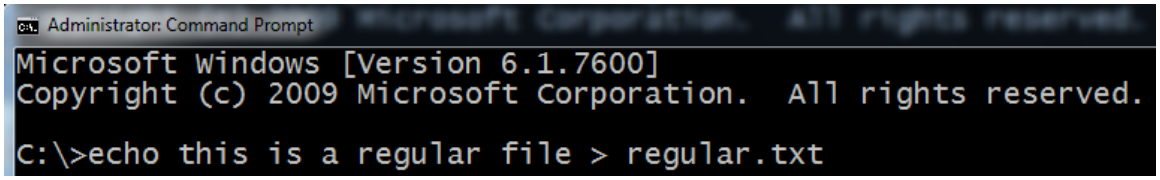


We will now examine some of the features of an NTFS disk, including the Encrypted File System (EFS), Alternate Data Streams (ADS), and timestomping of MAC times (Modified Access Created) times. These features are not available on FAT file system volumes.

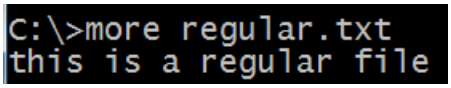
11. Double-click on the shortcut to the Command Prompt on the desktop.



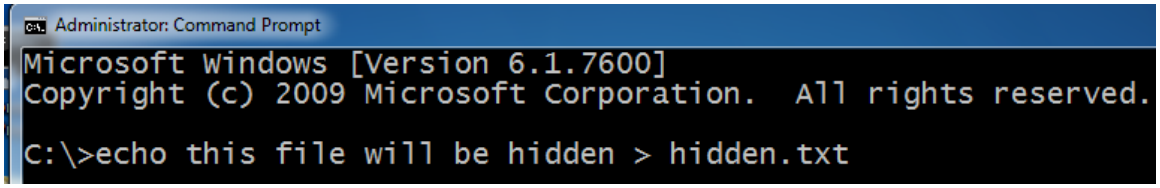
12. Type the following to create a file named regular.txt in the root of C:
    C:\>**echo this is a regular file > regular.txt**



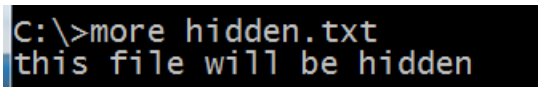
13. Type the following to view the file named regular.txt in the root of C:
    C:\>**more regular.txt**



14. Type the following to make a file named hidden.txt on the root of C:
    C:\>**echo this file will be hidden > hidden.txt**



15. Type the following to view the file named hiddenstuff.txt on the root of C:
    C:\>**more hidden.txt**



Next, we will hide the file named hidden.txt within the file regular.txt using an Alternate Data Stream (ADS). Before doing so, we will examine the file size of regular.txt.

16. Type the following to view the file size of the regular.txt file:
    C:\>**dir regular.txt**

```
C:\>dir regular.txt
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\

01/02/2014  07:50 PM                25 regular.txt
               1 File(s)            25 bytes
               0 Dir(s)   2,180,214,784 bytes free
```

17. To create the ADS, type the following command:
    C:\>**type hidden.txt > regular.txt:hidden.txt**

```
C:\>type hidden.txt > regular.txt:hidden.txt
```

18. And, just to get rid of the evidence, we will delete our file with "hidden info":
    C:\>**del hidden.txt**

```
C:\>del hidden.txt
```

19. Type the following to view the file size of regular.txt. Notice it did not increase.
    C:\>**dir regular.txt**

```
C:\>dir regular.txt
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\

01/02/2014  07:50 PM                25 regular.txt
               1 File(s)            25 bytes
               0 Dir(s)   2,180,214,784 bytes free
```

20. If you type the command to list all files and folders, the ADS will not be present
    C:\>**dir**

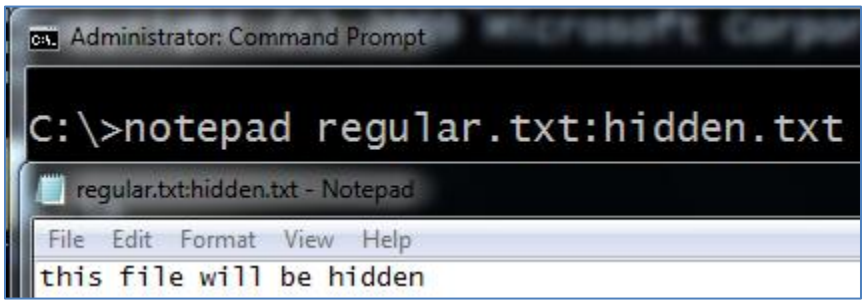
```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\

06/10/2009  04:42 PM                24 autoexec.bat
06/10/2009  04:42 PM                10 config.sys
11/12/2013  11:41 AM                 5 hi.txt
11/12/2013  11:37 AM    <DIR>          inetpub
07/13/2009  09:37 PM    <DIR>          PerfLogs
08/13/2013  07:45 AM    <DIR>          Program Files
01/02/2014  09:01 PM                25 regular.txt
07/08/2013  03:50 PM    <DIR>          Users
11/12/2013  11:38 AM    <DIR>          Windows
               4 File(s)            64 bytes
               5 Dir(s)   2,180,210,688 bytes free
```

21. Type the following command to view all ADS files on the root of C:
    C:\>**dir /r**

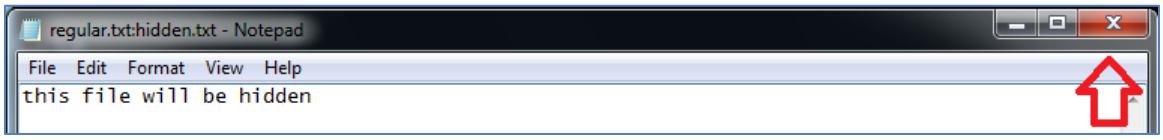
```
C:\>dir /r
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\

06/10/2009  04:42 PM                24 autoexec.bat
06/10/2009  04:42 PM                10 config.sys
11/12/2013  11:41 AM                 5 hi.txt
11/12/2013  11:37 AM    <DIR>          inetpub
07/13/2009  09:37 PM    <DIR>          PerfLogs
08/13/2013  07:45 AM    <DIR>          Program Files
01/02/2014  09:01 PM                25 regular.txt
                                    27 regular.txt:hidden.txt:$DATA
07/08/2013  03:50 PM    <DIR>          Users
11/12/2013  11:38 AM    <DIR>          Windows
               4 File(s)             64 bytes
               5 Dir(s)   2,180,218,880 bytes free
```

The dir /r command is not available in operating systems prior to Windows Vista.

22. Type the following command to view the contents of the ADS file:
    C:\>**notepad regular.txt:hidden.txt**



23. Close the text file when you are finished viewing it, by clicking on the X.



The timestomp.exe utility can be used on an NTFS volume to change MAC (Modified Access Created) times.

24. Type the following command to view the options for the timestomp.exe utility:
    C:\>**timestomp**

```
Administrator: Command Prompt

C:\>timestomp


TimeStomp Usage Information:
-----------------------------------------------------------
If you mix a lot of options, the behavior is unpredictable. All times
should be entered in local time because the utility automatically
converts to UTC time.

TimeStomp <filename> [options]

        <filename>      the name of the file you wish to modify
                        you may need to surround the full path in ""
options:

        -m <date>       M, set the "last written" time of the file
        -a <date>       A, set the "last accessed" time of the file
        -c <date>       C, set the "created" time of the file
        -e <date>       E, set the "mft entry modified" time of the file
        -z <date>       set all four attributes (MACE) of the file

        <date>          "DayofWeek Month\Day\Year HH:MM:SS [AM|PM]"

        -f <src file>   set MACE of <filename> equal to MACE of <src file>
```

25. Type the following command to view the current dates and times of files:
    C:\>**dir**

```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\

06/10/2009  04:42 PM                24 autoexec.bat
06/10/2009  04:42 PM                10 config.sys
11/12/2013  11:41 AM                 5 hi.txt
11/12/2013  11:37 AM    <DIR>          inetpub
07/13/2009  09:37 PM    <DIR>          PerfLogs
08/13/2013  07:45 AM    <DIR>          Program Files
07/08/2013  03:50 PM    <DIR>          Users
01/02/2014  10:10 PM    <DIR>          Windows
               3 File(s)             39 bytes
               5 Dir(s)   2,181,898,240 bytes free
```

26. Type the following command to change the MAC of **hi.txt** to the same MAC as config.sys:
    C:\>**timestomp hi.txt –f config.sys**

```
C:\>timestomp hi.txt -f config.sys
```

27. Type the following command to view the current dates and times of files:
    C:\>**dir**

```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\

06/10/2009  04:42 PM                24 autoexec.bat
06/10/2009  04:42 PM                10 config.sys
06/10/2009  04:42 PM                 5 hi.txt
11/12/2013  11:37 AM    <DIR>          inetpub
07/13/2009  09:37 PM    <DIR>          PerfLogs
08/13/2013  07:45 AM    <DIR>          Program Files
07/08/2013  03:50 PM    <DIR>          Users
01/02/2014  10:10 PM    <DIR>          Windows
               3 File(s)             39 bytes
               5 Dir(s)   2,181,898,240 bytes free
```

28. Type the following command to make a directory called private on the root of C:
    C:\>**mkdir private**

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>mkdir private
```

29. Type the following command to list all files and folders on the root of C:
    C:\>**dir**

```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is E8D7-61E9

 Directory of C:\

07/01/2013  11:13 PM             1,024 .rnd
06/10/2009  05:42 PM                24 autoexec.bat
11/29/2011  08:49 PM    <DIR>          class_tools
06/10/2009  05:42 PM                10 config.sys
03/15/2012  11:27 PM    <DIR>          mame
07/13/2009  10:37 PM    <DIR>          PerfLogs
07/01/2013  11:40 PM    <DIR>          private
05/31/2012  01:23 AM    <DIR>          Program Files
10/17/2011  06:33 PM    <DIR>          Users
05/31/2012  01:50 AM    <DIR>          Windows
               3 File(s)          1,058 bytes
               7 Dir(s)   1,410,277,376 bytes free
```

30. Type the following command to enter the private directory on the root of C:
    C:\>**cd private**

```
C:\>cd private

C:\private>
```

31. Create a file called SSN.txt, which has 123-45-6789 as its contents, by typing the following:
    C:\private>**echo 123-45-6789 > SSN.txt**

```
C:\private>echo 123-45-6789 > SSN.txt
```

32. Type the following to view the files and folders in the private directory:
    C:\>**dir**

```
C:\private>dir
 Volume in drive C has no label.
 Volume Serial Number is E8D7-61E9

 Directory of C:\private

07/02/2013  12:00 AM    <DIR>          .
07/02/2013  12:00 AM    <DIR>          ..
07/02/2013  12:00 AM                14 SSN.txt
               1 File(s)             14 bytes
               2 Dir(s)   1,410,404,352 bytes free
```

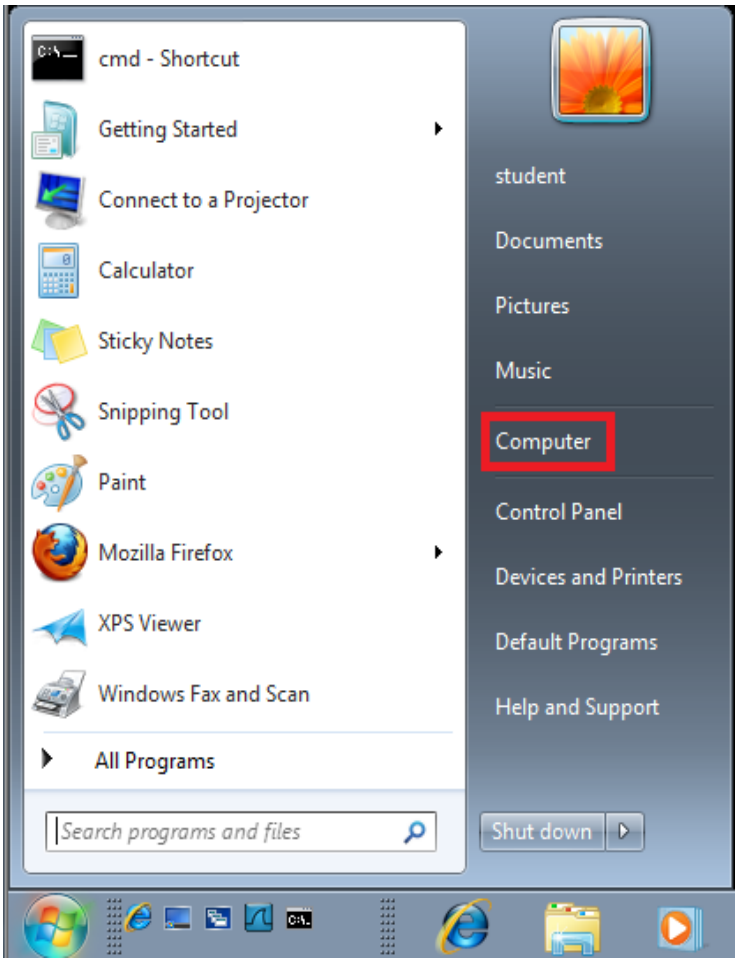
33. Type the following command to view the contents of the SSN.txt file:
    C:\private>**type SSN.txt**

```
C:\private>type SSN.txt
123-45-6789
```

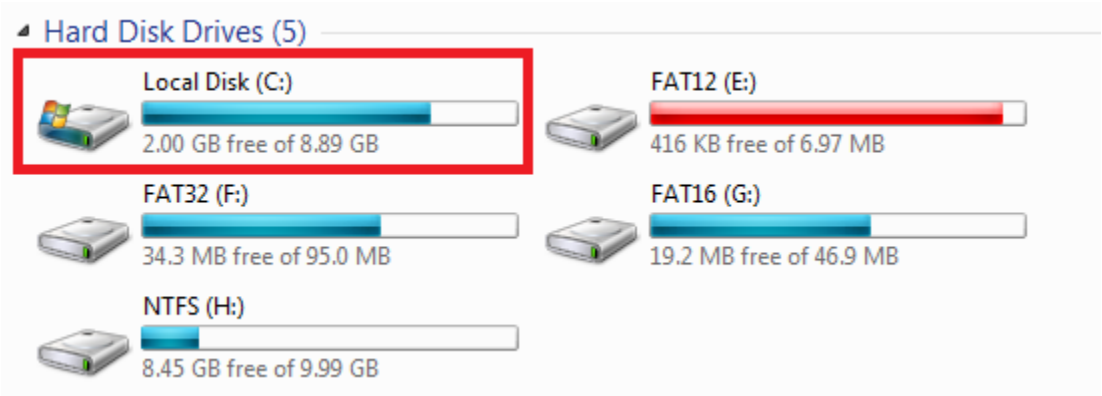
34. Type the following command to leave the command line environment:
    C:\private>**exit**

```
C:\private>exit
```

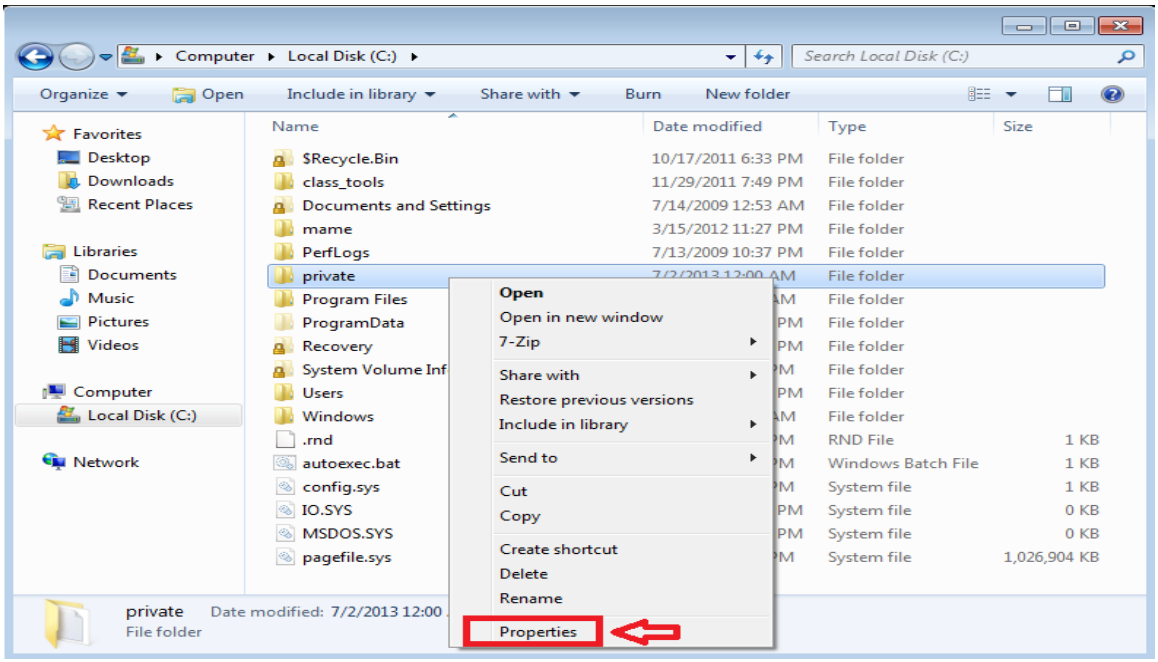
35. Click on the **Start** button and select **Computer** from the Start menu.



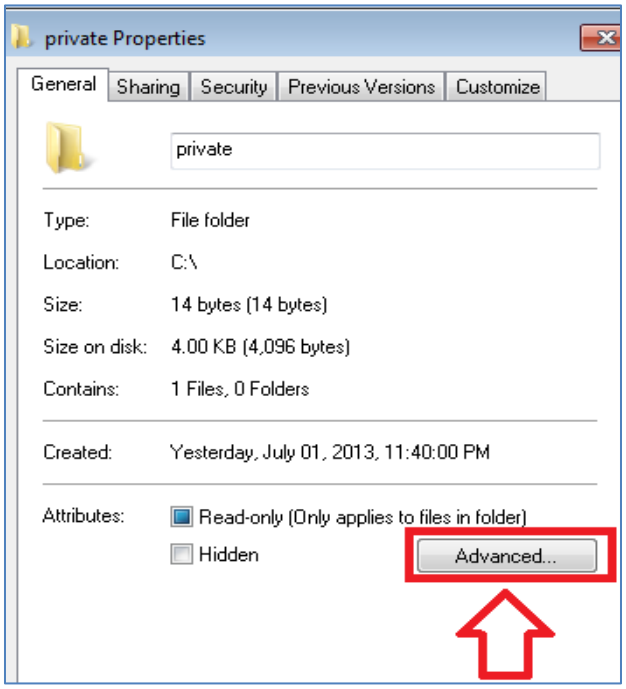
36. Under Hard Disk Drives, double-click on **Local Disk (C :).**



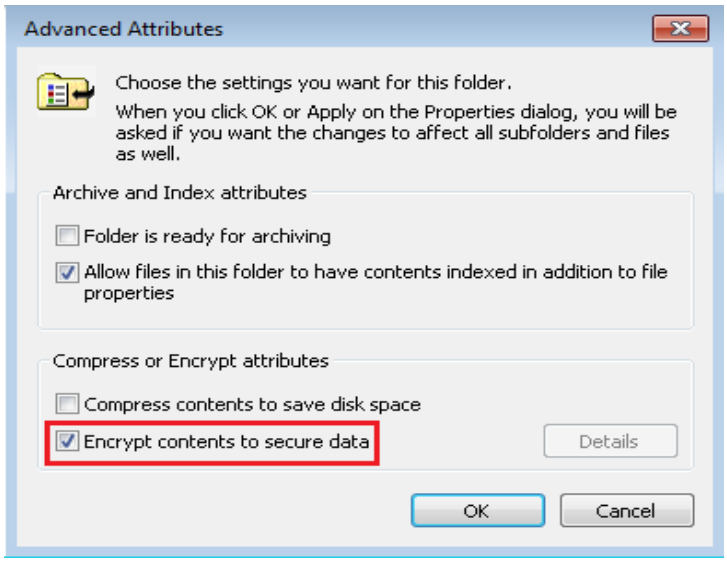
37. Right-click on the **Private** Folder in the list and select **Properties**.



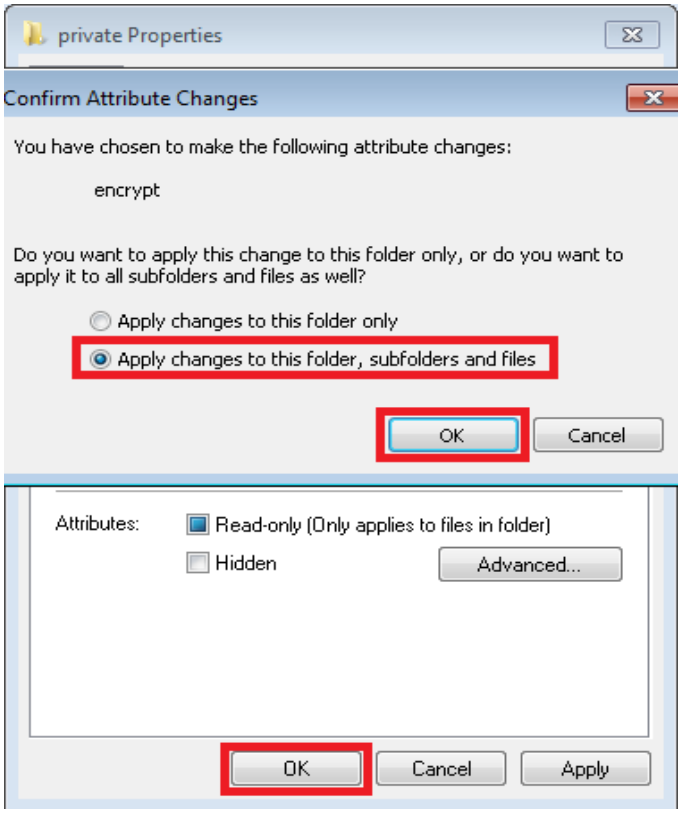
38. On the **General** tab, click the **Advanced** button.



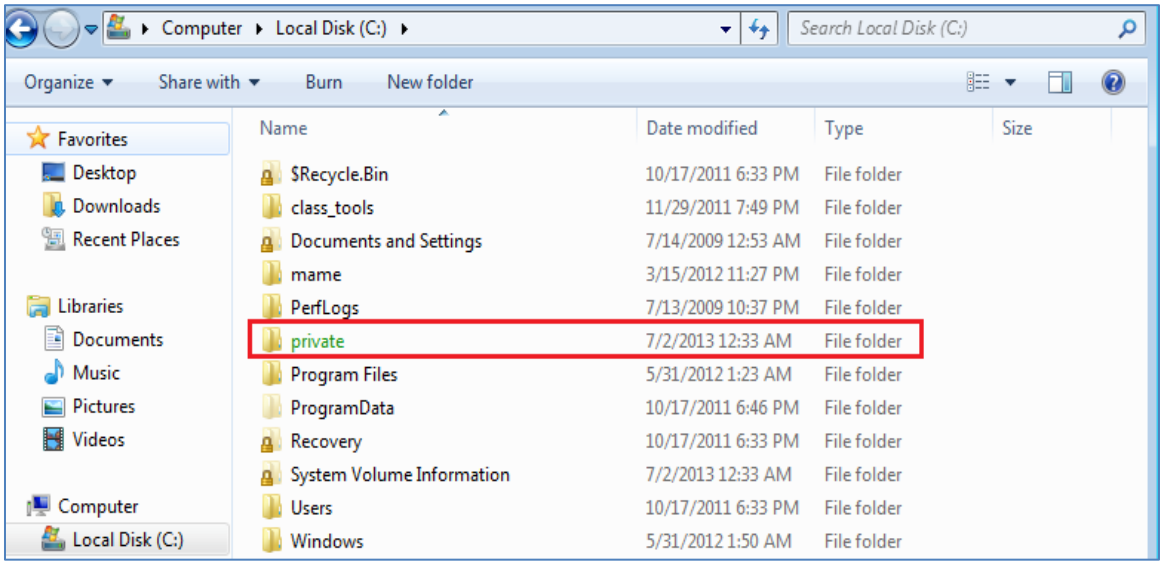
39. Check the box that states, **Encrypt contents to secure data**. Click **OK**.



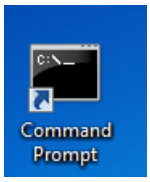
40. Click **OK.** Select **Apply changes to this folder, subfolder and files**. Click **OK**.



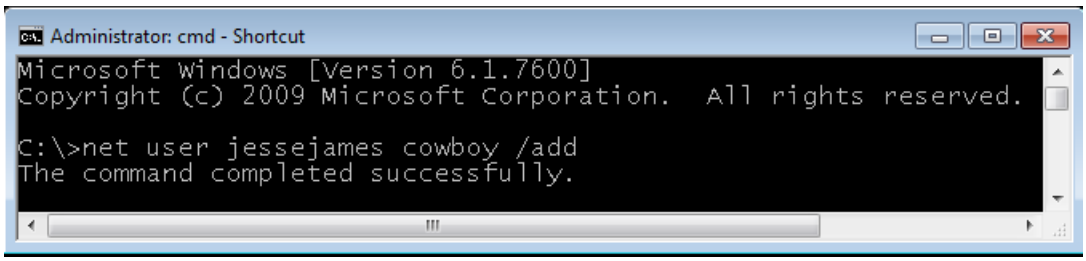
41. View the Private folder on the C: Drive. Notice that the color of the file name changed to green. Close the Computer window.



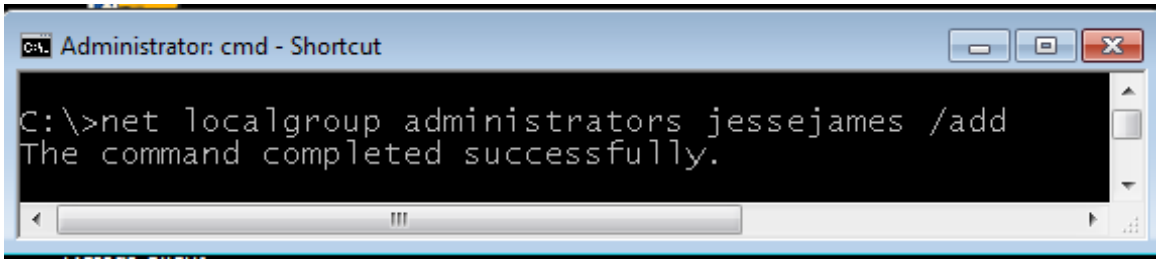
42. Open a Command Prompt by clicking on the shortcut on the desktop.



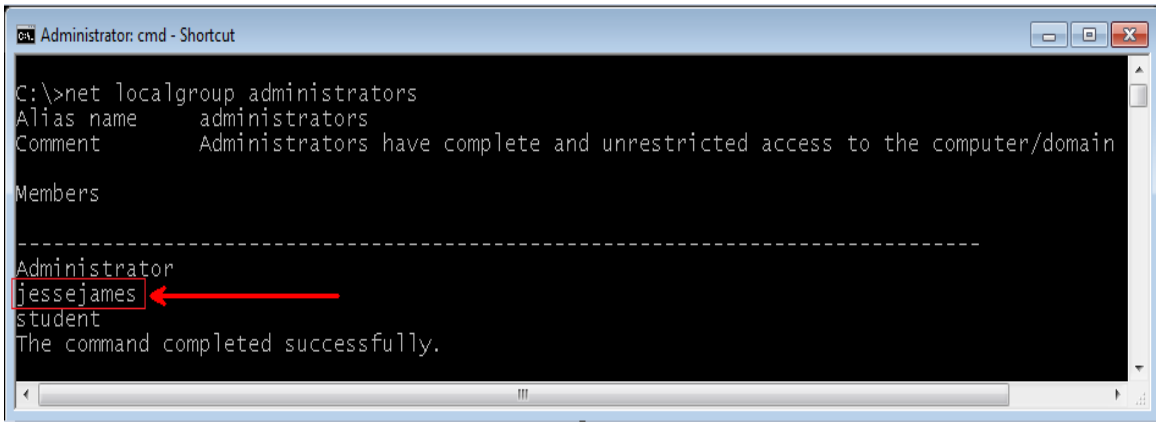
43. Create a user on the Windows 7 External Machine by typing the following command:
C:\>**net user jessejames cowboy /add**



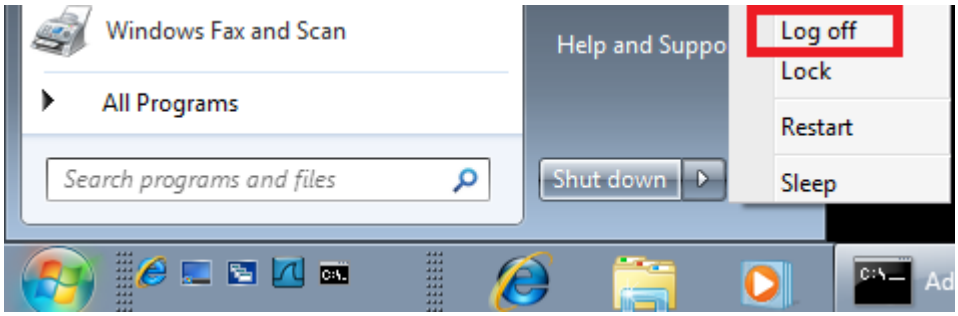
44. Type the following command to add the user to the local administrators group:
    C:\>**net localgroup administrators jessejames /add**



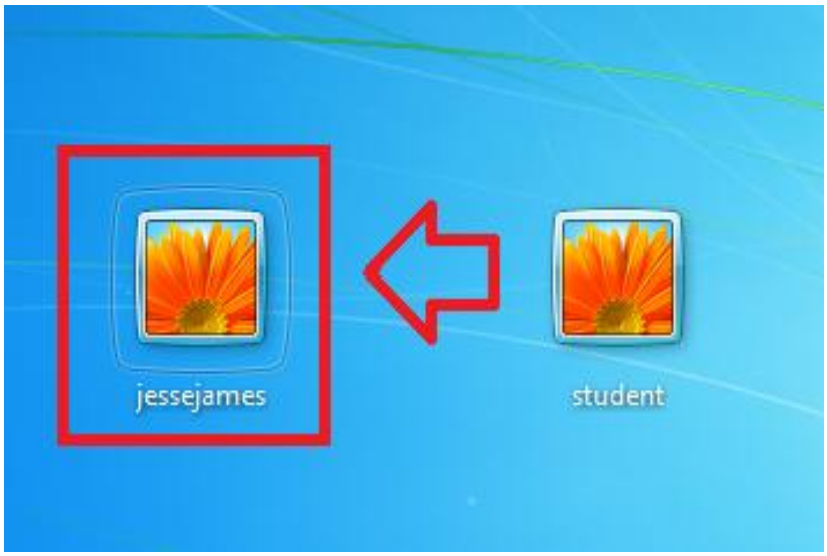
45. Verify that the user has been added to the administrators group by typing:
    C:\>**net localgroup administrators**



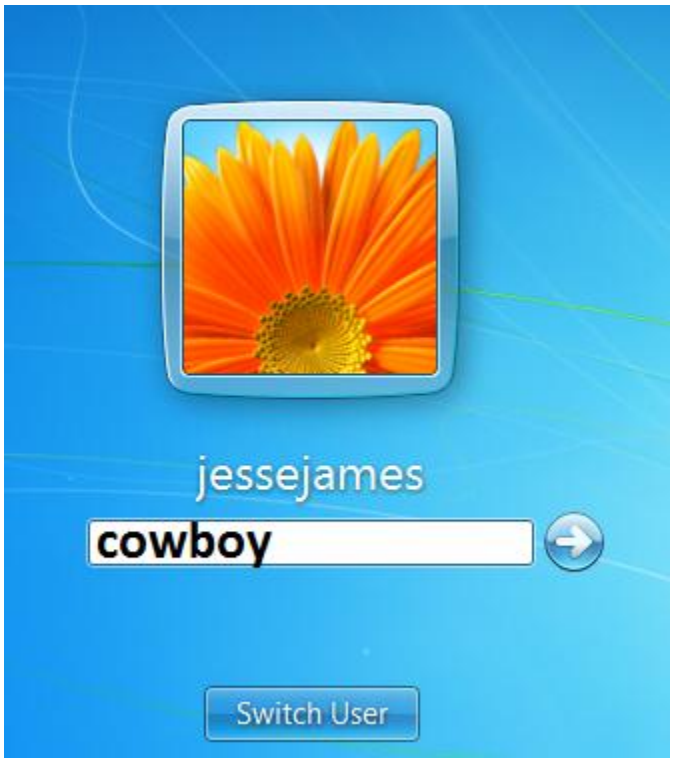
46. Type exit to quit Command Prompt.
47. Click on the **Start** button, click to the right of Shut down, and select **Log off.**



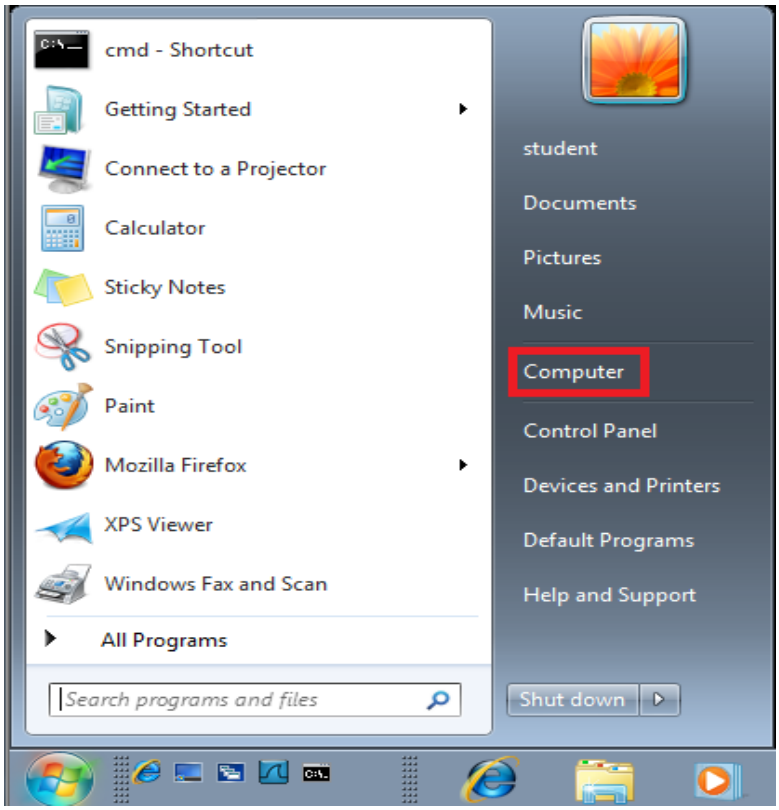
48. Click on the icon with the name **jessejames** at the welcome page.



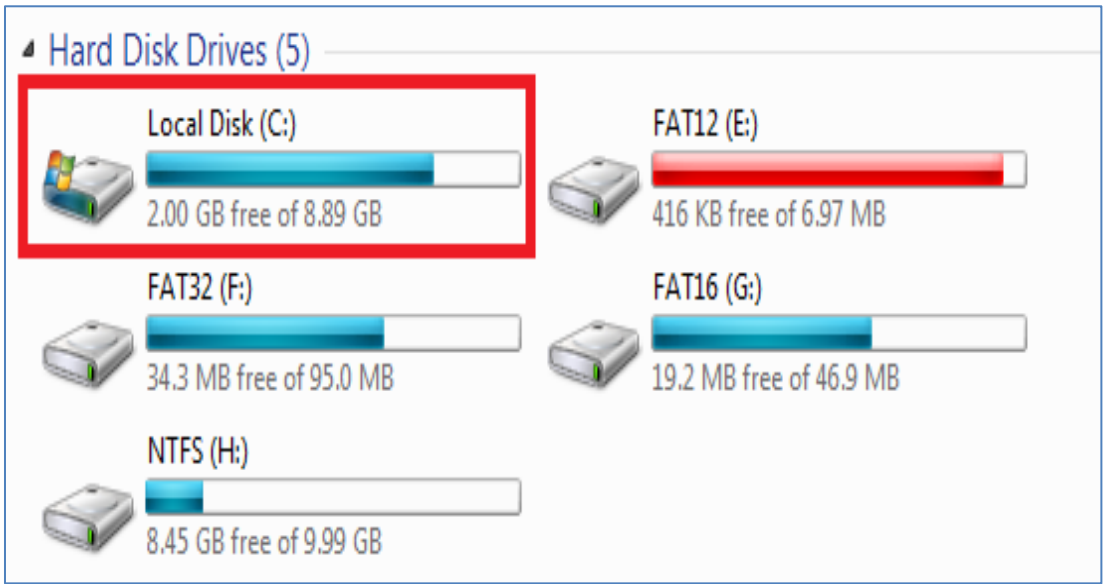
49. Type **cowboy** for the password of the **jessejames** account.



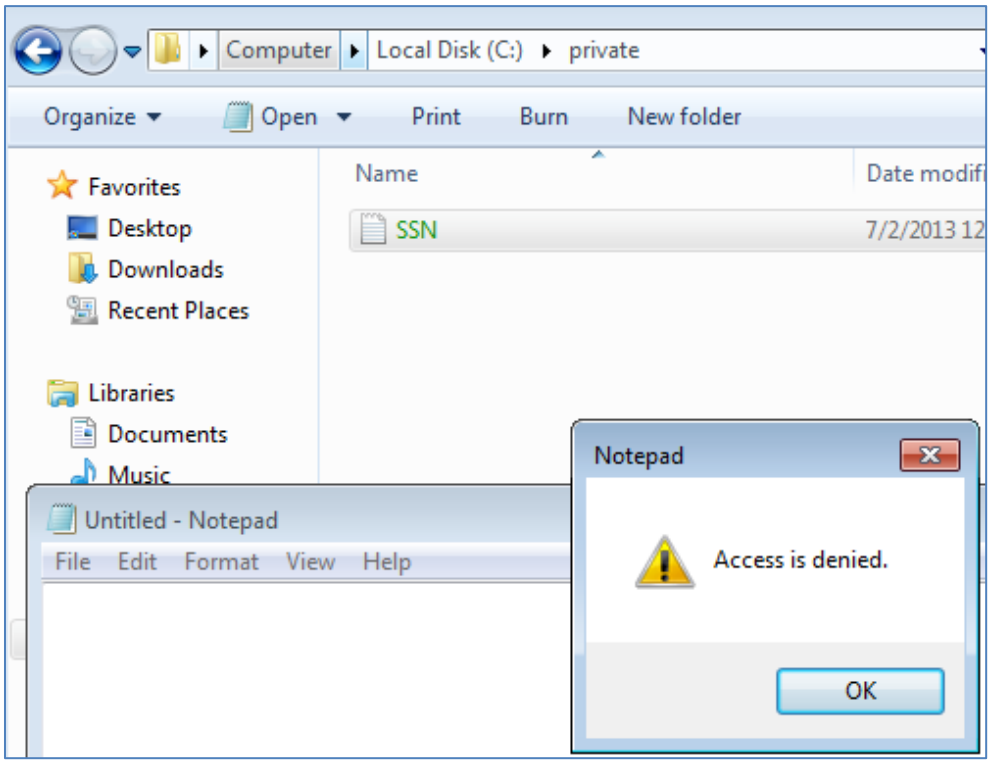
50. Click on the **Start** button and select **Computer** from the Start menu.



51. Under Hard Disk Drives (5), double-click on **Local Disk (C:).**



52. Double-click on the **Private** folder. Try to open **SSN.txt**. Access is denied.



53. Click **OK**, close all windows and **log off** of the Windows 7 Machine.

1.2 Conclusion

There are many variations of file systems used on operating systems. File systems that are common to Microsoft operating systems include File Allocation Table(FAT) and New Technology File System (NTFS). Some of the features included with the NTFS file system include Alternate Data Streams (ADS), and the Encrypted File System (EFS). A hacker can perform timestomping on an NTFS volume.

1.3 Discussion Questions

1. What is an Alternate Data Stream (ADS)?
2. How is timestomping performed?
3. What is the command to display an ADS from the command line?
4. How do you encrypt a file using the EFS feature of NTFS?

2 Using a HEX Editor to Explore a NTFS Partition

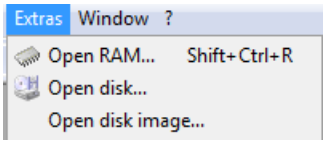
In this section, we will explore the NTFS file system with the hexadecimal (hex) editor HxD. We will be looking at the Master Boot Record (MBR) of an NTFS file system and dissecting it.

2.1 Exploring an NTFS Partition

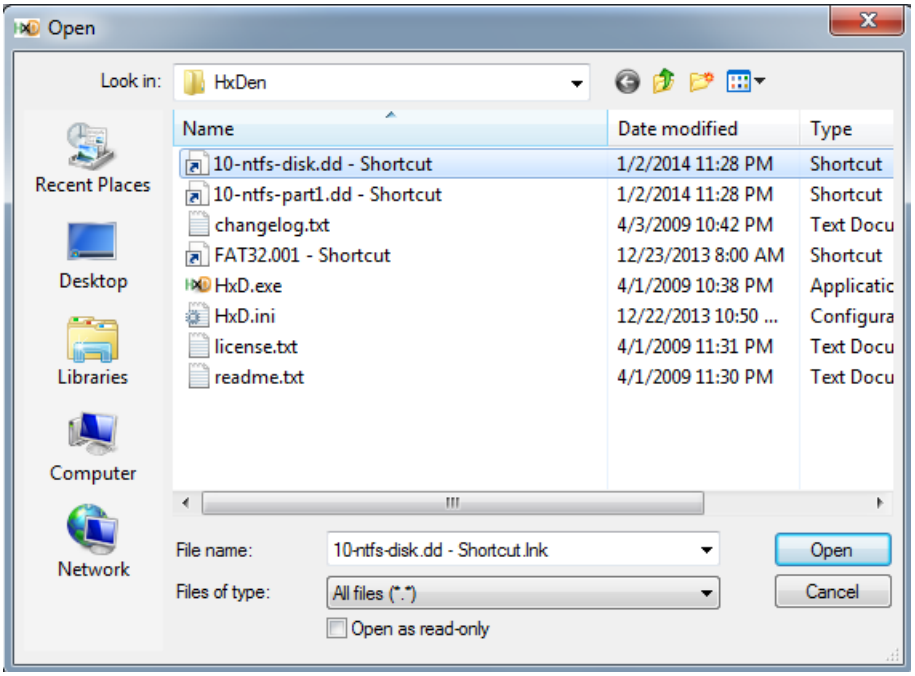
1. On the **Windows 7 Machine**, click on the **student** icon.
2. Type in the password, **password,** and press **Enter** to log in.

3. Double click on the HxD icon on the desktop.

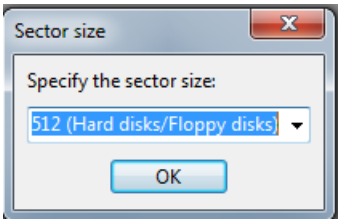
4. From the menu bar, select **Extras > Open disk image**.



5. Click on the **10-ntfs-disk.dd - Shortcut** link and click Open.

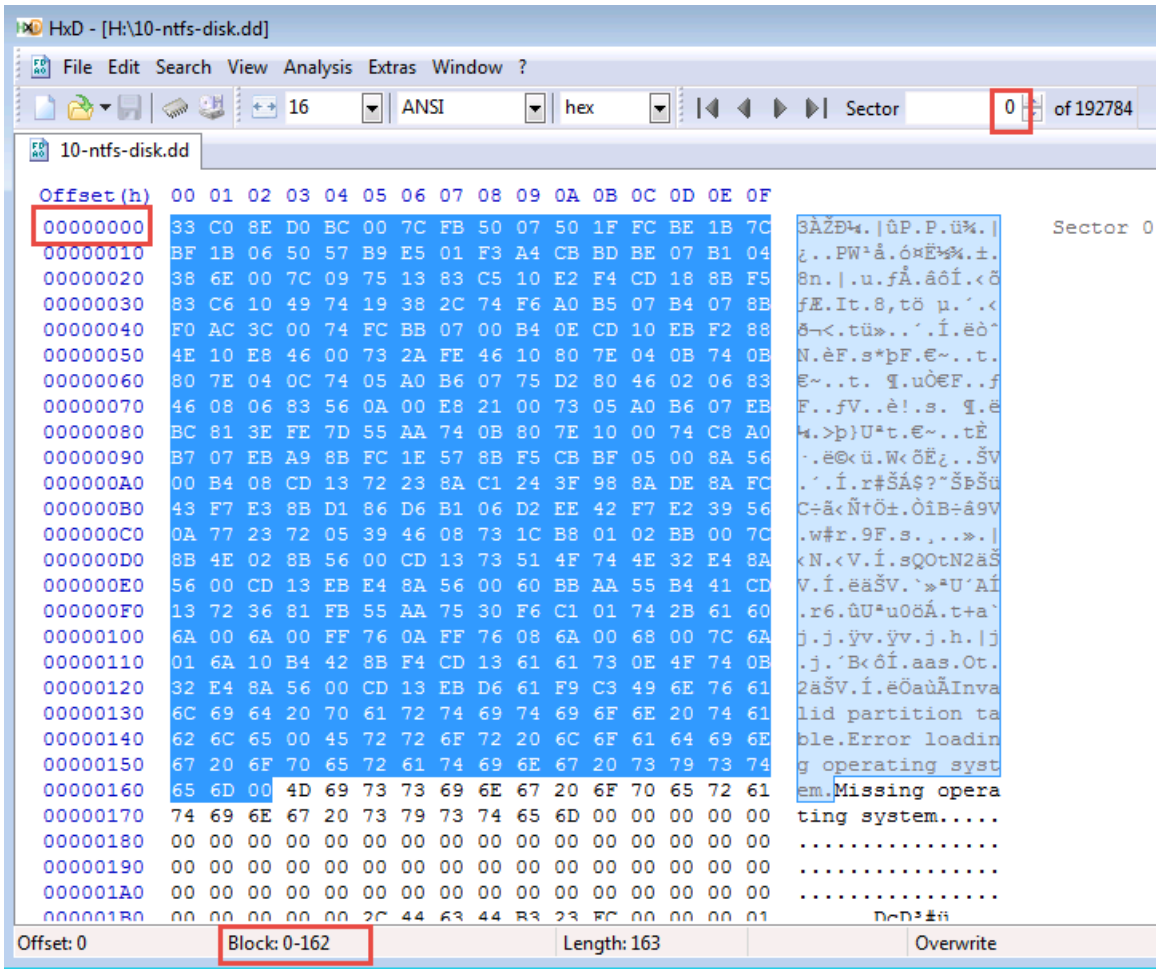


6. Leave the default size as 512 bytes. Click **OK**.

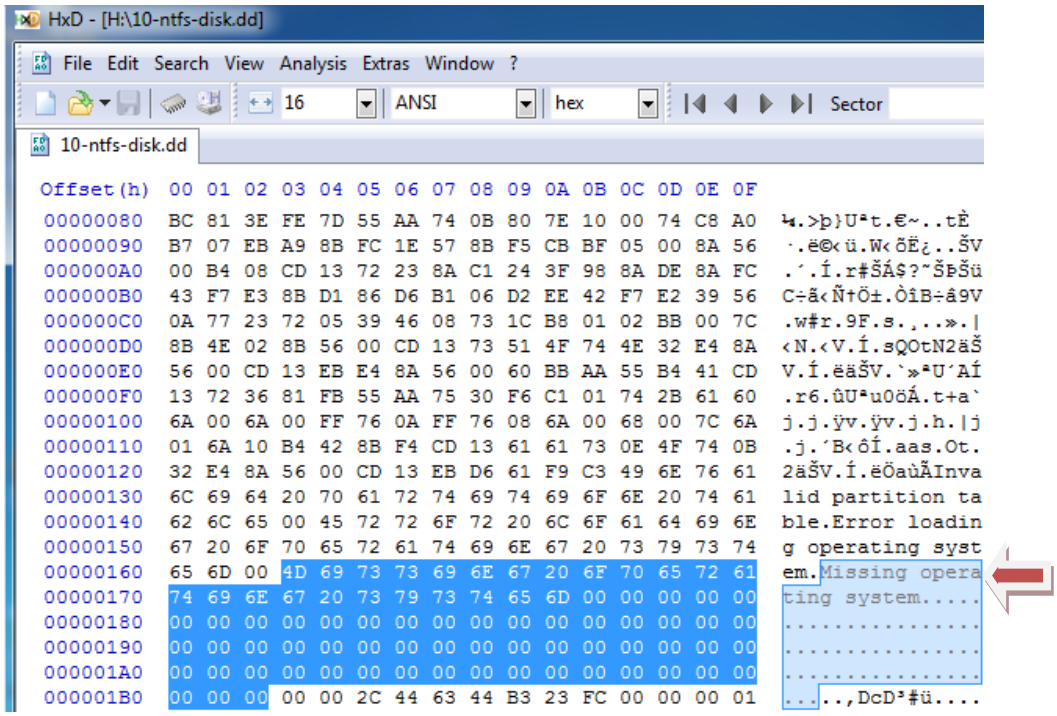


7. Highlight bytes **00000000 to 00000162** by left-clicking and dragging from the beginning bytes down to byte 00000162. If you look at the bottom of the Hex Editor, it counts the hex values for you. This is a piece of the boot code for the drive that allows it to become bootable.

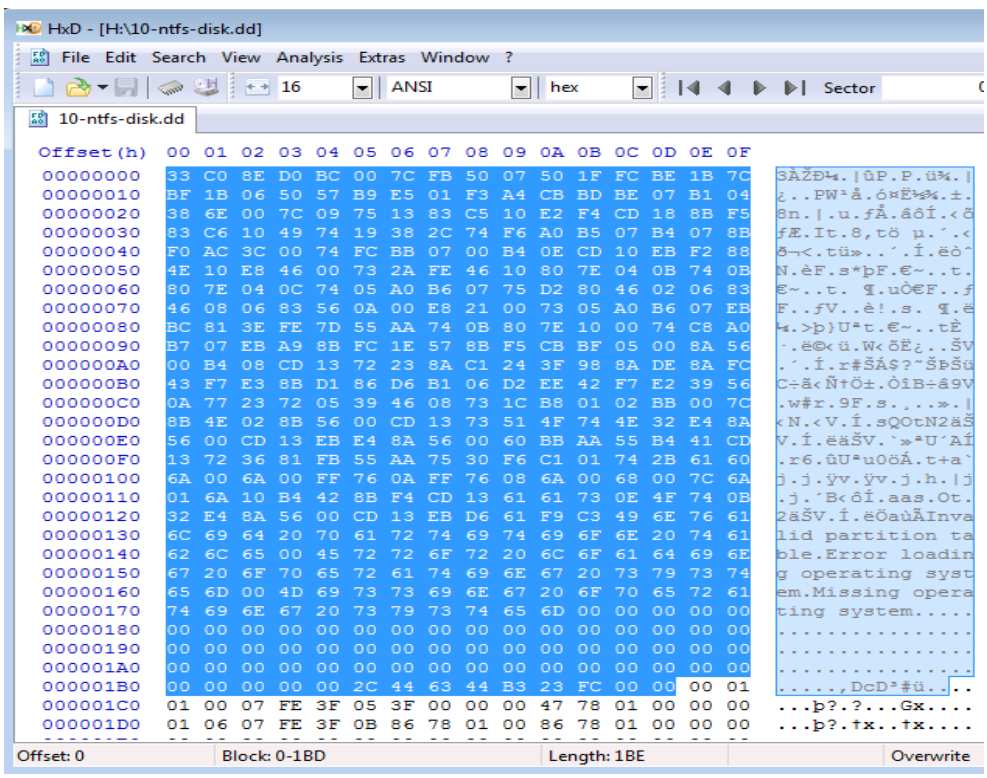
Make sure that you are at **Sector 0**, **Offset 00000000**.



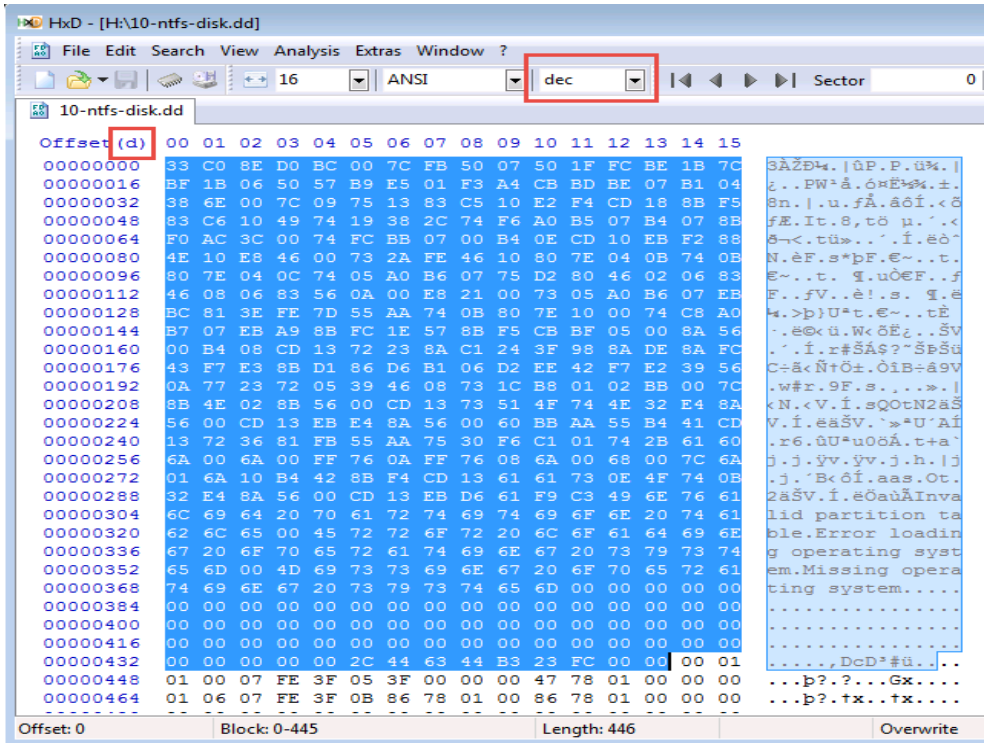
Highlight bytes 00000163 to 000001B2. This area is also part of the boot code and contains any error messages. If you look at the ASCII on the right, you can see the message, **Missing operating system**.



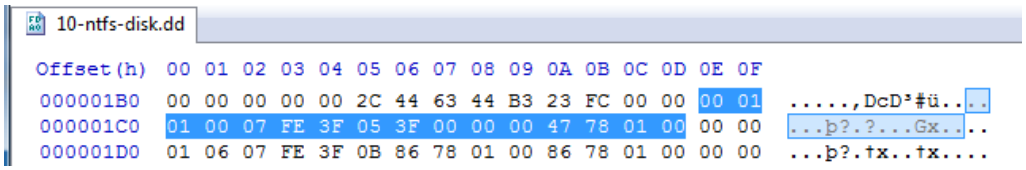
8. Select the entire boot code, which spans from 00000000 to 000001BD or 0-445 in decimal.



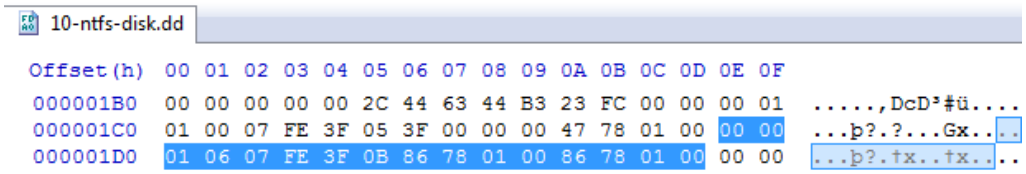
9. Click on **Offset** (in the upper-left corner) to view the decimal values. Offset will change from **h** to **d**.



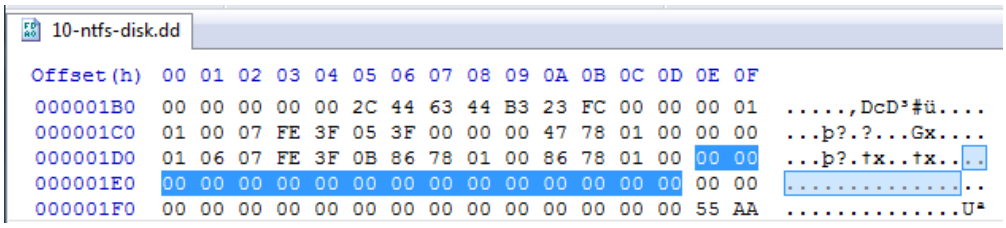
10. Change the offset back to hex. The first partition of the disk begins at location 1BE to 1CD (446-461 in decimal) and is 16 bytes long.



11. You can have up to four primary partitions on a standard DOS based system. There are three more partitions on this image. The second partition goes from 1CE to 1DD (462 to 477 in decimal).



12. The third partition is from 1DE to 1ED (478 to 493 in decimal).



13. The fourth and last partition is 1EE to 1FD (494 to 509 in decimal).

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............Uª
```

14. The entire partition table is 64 bytes in length.

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............Uª
```

15. Look at the first partition again and highlight **1BE to 1CD** (446-461 in decimal).

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

16. The first byte of the partition indicates whether it is a bootable partition or not. Our entry is **00**, which indicates a non-bootable partition. A value of **80** would indicate a bootable partition.

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

17. The next three bytes indicate where the starting Head, Sector and Cylinder (yes, they are out of order) are located, and is commonly called the CHS address for the partition. In our case, CHS is (0,1,1). Note: Data stored by Intel processors is written with LSB (Least Significant Byte) first and MSB (most significant byte) last so the byte order must be reversed.

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

18. The fifth byte is the Partition Type (there are many). In this case, it is **07,** which indicates an NTFS partition.

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

19. The next three bytes indicate the ending CHS address.

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

20. The next four bytes is for Logical Block Addressing (LBA). The Operating System determines the LBA. Possible choices are either CHS or LBA mode (but not both) for the partition.

```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

21. The last 4 bytes indicate the size in sectors of the partition.

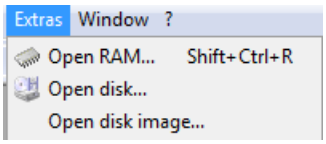
```
10-ntfs-disk.dd
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
000001C0  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
000001D0  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
```

This same analysis applies for each partition.

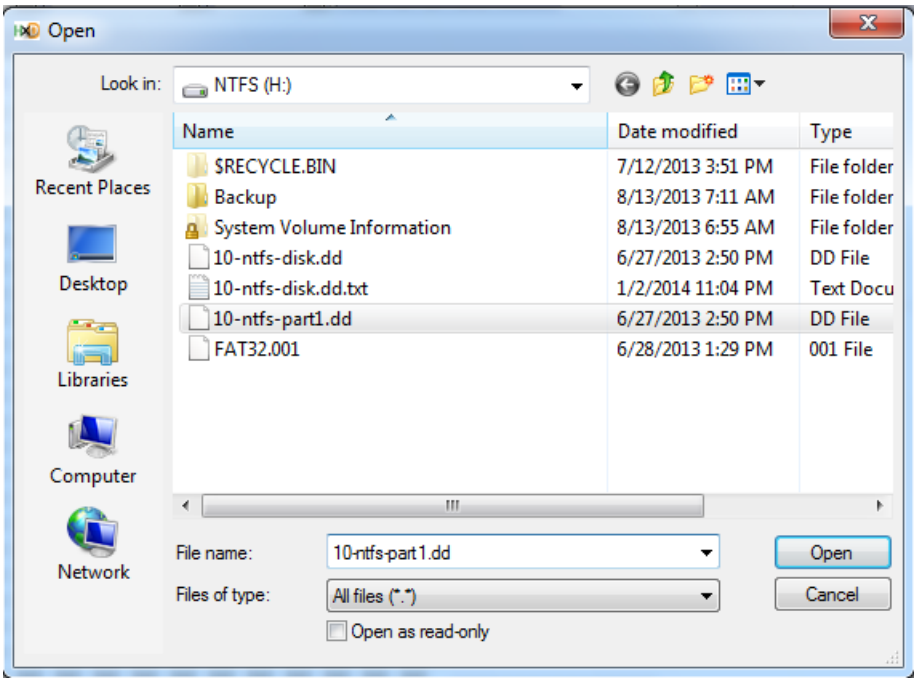
22. Change the offset back to decimal. Finally, the MBR signature is at the end of the Master Root Record as highlighted below: **55 AA.**

```
10-ntfs-disk.dd
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000384  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000416  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000432  00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01  .....,DcD³#ü....
00000448  01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00  ...þ?.?...Gx....
00000464  01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00  ...þ?.†x..†x....
00000480  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000496  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............Uª
```

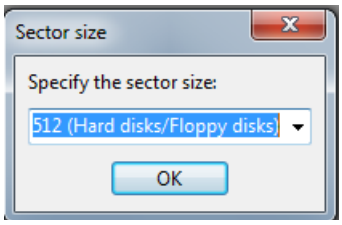
23. From the Menu bar, select **Extras > Open disk image**.



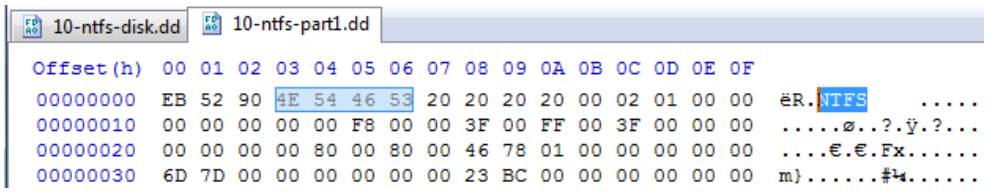
24. Click on the **10-ntfs-part1.dd** file and click Open.



25. Leave the default size as 512 bytes. Click **OK**.



26. Look at the signature for the partition. It is NTFS, as identified in the MBR.



27. Close HxD and the Windows 7 PC Viewer.

2.2 Conclusion

A hexadecimal (hex) editor like HxD will allow you to examine the details of FAT or FAT32 Partitions and disk images.

2.3 Discussion Questions

1. What is the byte range in decimal for the first partition?
2. What number indicates that a partition is bootable?
3. What does LBA stand for and what does it do?
4. The Master Boot Record ends with what signature?

3 Verifying and Viewing the Image Details

An image is a bit-by-bit copy of a disk. In this case, the NTFS file system was used on a volume where the operating system was installed. Starting with Windows Vista, NTFS had to be used on the OS drive. NTFS is also commonly utilized on data drives.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

3.1 Verifying Integrity

1. Open the **BackTrack 5 Machine on the Internal Network**, type **root** for the login and **toor** *(root spelled backwards)* for the password. (You may have to press Enter to see text on screen)

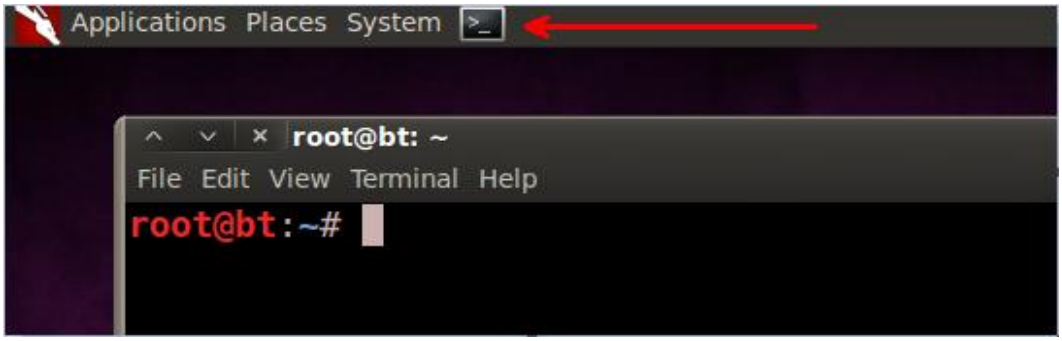
The password will not be displayed when you type it for security purposes.

```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

 System information disabled due to load higher than 1.0
root@bt:~# _
```

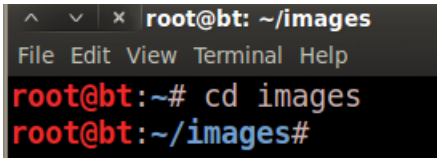
2. Type the following command to start the Graphical User Interface (GUI).
   root@bt:~# **startx**

```
root@bt:~# startx_
```

3. Open a terminal on the Linux system by clicking on the picture to the right of the word **System,** in the task bar in the top of the screen.

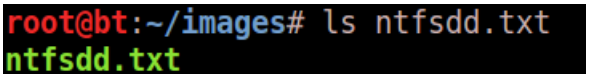


4. Switch to the images directory by typing the following command:
   root@bt:~# **cd images**

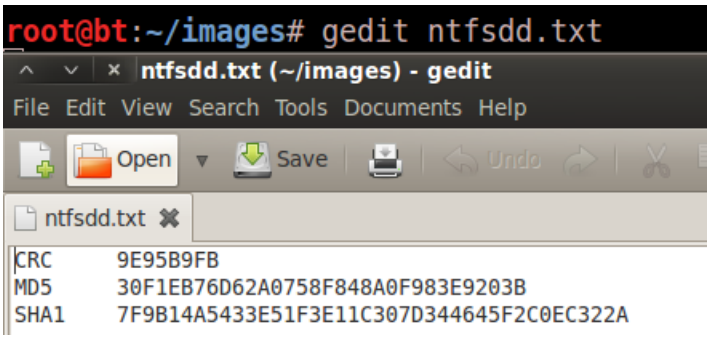


When investigators take an image, they should record the SHA1 and MD5 hashes. The hashes for the disk image are usually put into a text file that accompanies the image file.

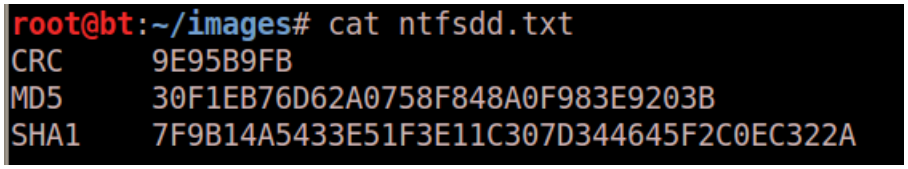
5. Type the following command to view the file with the hashing information :
   root@bt:~/images# **ls ntfsdd.txt**



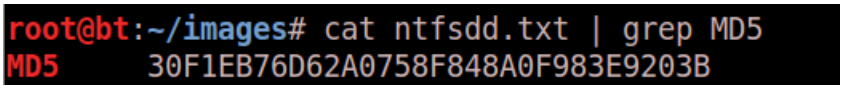
6. Type the following command to view the file from the Graphical User Interface:
   root@bt:~/images# **gedit ntfsdd.txt**



7. Close the file when you are finished viewing it with the gedit application.
8. Type the following command to view the file contents from the terminal :
   root@bt:~/images# **cat ntfsdd.txt**



9. Type the following command to view the MD5 hash:
   root@bt:~/images# **cat ntfsdd.txt | grep MD5**



10. Type the following command to view the file with the hashing information:
    root@bt:~/images# **md5sum ntfs.dd**

```
root@bt:~/images# cat ntfsdd.txt | grep MD5
MD5     30F1EB76D62A0758F848A0F983E9203B
root@bt:~/images# md5sum ntfs.dd
30f1eb76d62a0758f848a0f983e9203b  ntfs.dd
```

Notice that the MD5 sum matches the sum from the acquisition text file.

11. Type the following command to view the SHA1 hash:
    root@bt:~/images# **cat ntfsdd.txt | grep SHA1**

```
root@bt:~/images# cat ntfsdd.txt | grep SHA1
SHA1    7F9B14A5433E51F3E11C307D344645F2C0EC322A
```

12. Type the following command to view the file with the hashing information :
    root@bt:~/forensics# **sha1sum ntfs.dd**

```
root@bt:~/images# cat ntfsdd.txt | grep SHA1
SHA1    7F9B14A5433E51F3E11C307D344645F2C0EC322A
root@bt:~/images# sha1sum ntfs.dd
7f9b14a5433e51f3e11c307d344645f2c0ec322a  ntfs.dd
```

Notice that the SHA1 sum matches the sum from the acquisition text file. Close the Linux terminal.

3.2 Conclusion

When an image is collected, the incident responder should generate a corresponding text file with the image MD5 and SHA1 hash values, as well as other information like the cyclical redundancy check (CRC value). The md5sum and sha1sum utilities can be utilized from the terminal to hash a data set to verify the integrity of the data.

3.3 Discussion Questions

1. What Linux command can be used to parse information out of a txt file?
2. How many bits is the MD5 hashing algorithm?
3. How many bits is the SHA1 hashing algorithm?
4. Which hashing algorithm is more accurate, MD5 or SHA1?

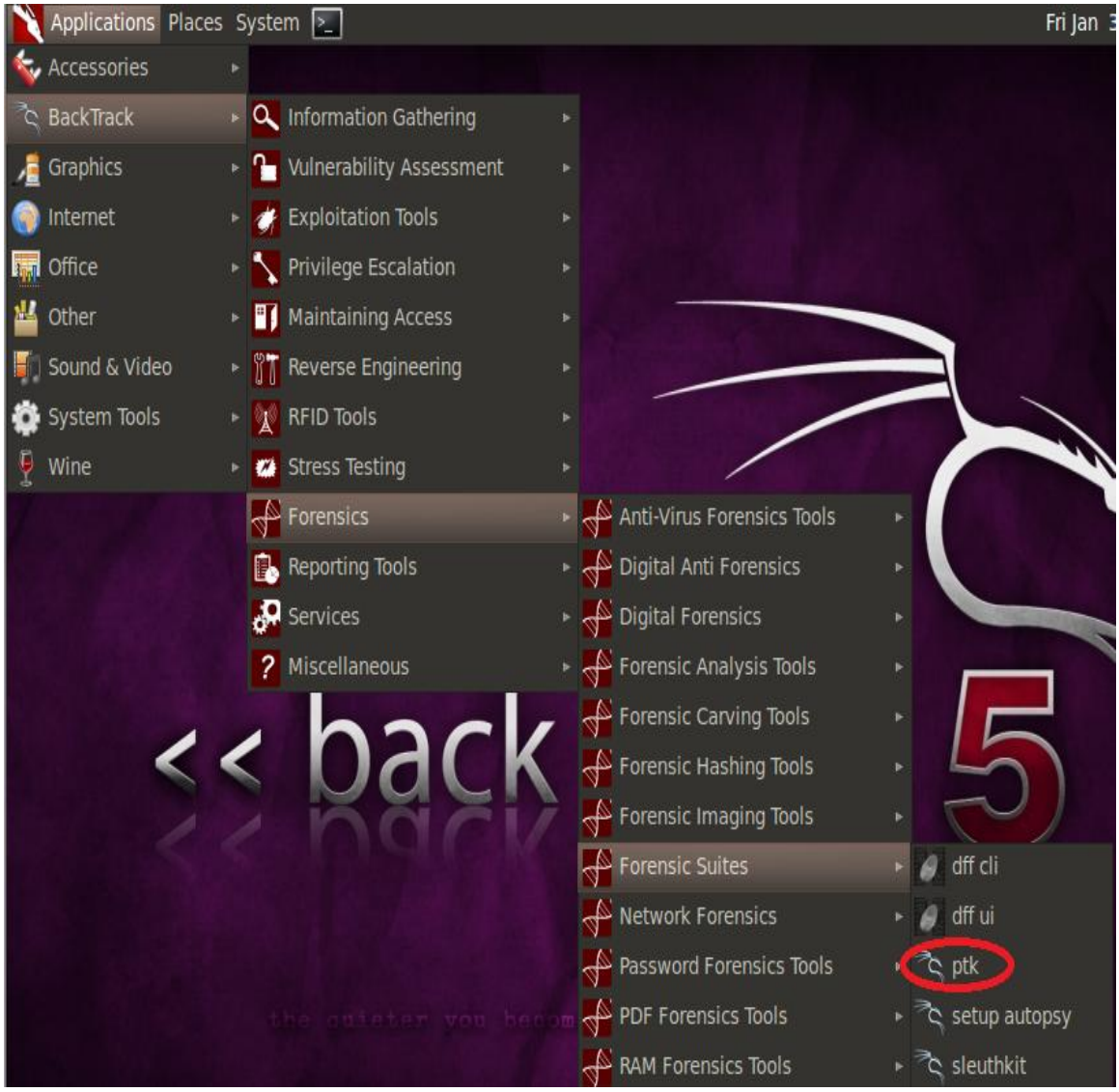
4 Analyzing a NTFS Partition with PTK

Forensic Analysis requires loading an image file into a forensic tool. The most widely used forensic tools are commercial tools such as EnCase and FTK (Forensic Tool Kit). EnCase is made by Guidance software and FTK is made by Access Data. Both tools require hardware dongles, which helps to prevent illegal copying of the software. There are some free tools, such as Autopsy and PTK, which also can be used to perform forensic analysis.

4.1 Loading the NTFS Image into PTK

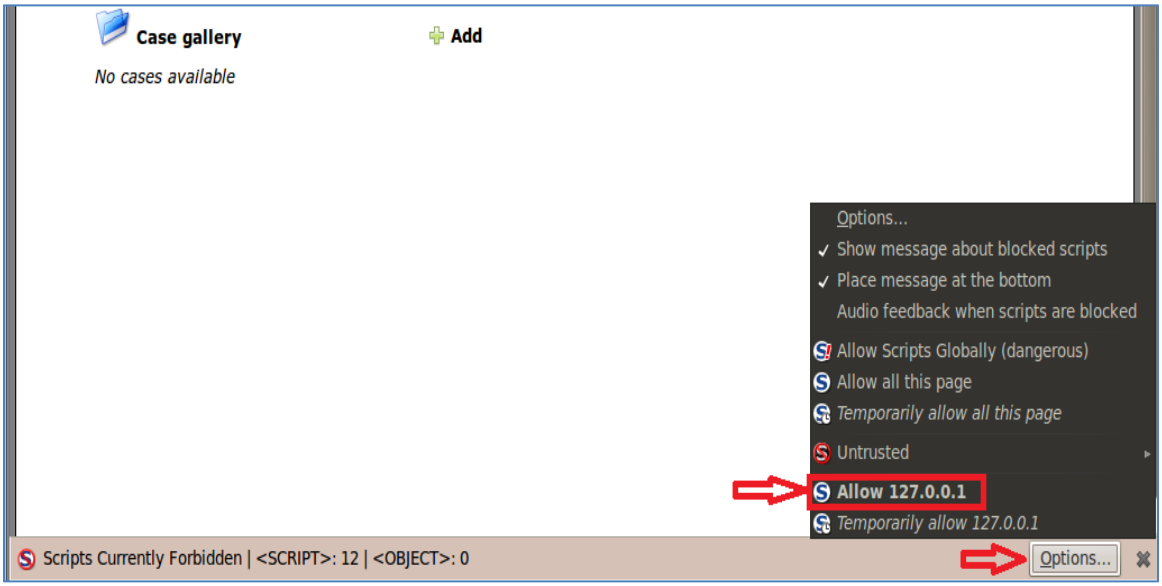
PTK is included with Release 5 of BackTrack. It is not included with the Kali distribution.

1. To use the PTK forensic browser click **Applications > BackTrack > Forensics, Forensic Suites > ptk.**

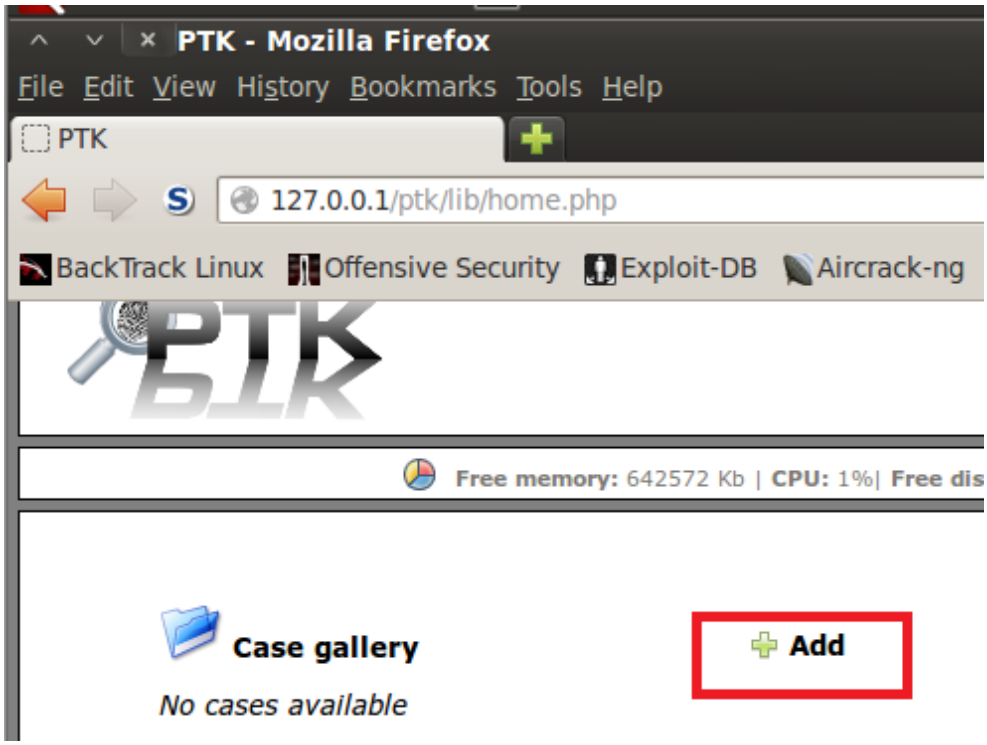


2. For the username, type **admin** and for the password type **toor.**

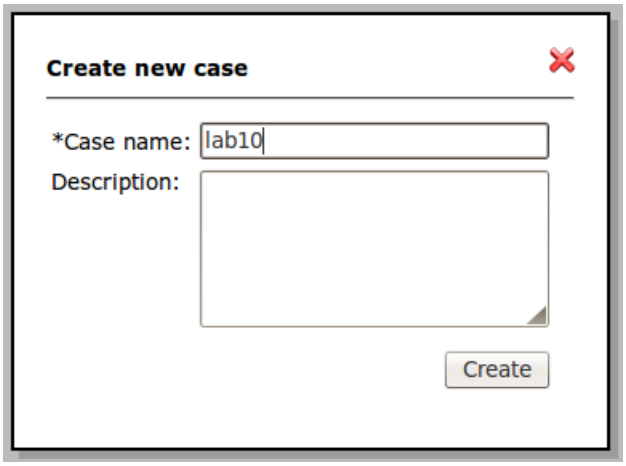
3. In the bottom-right corner of Firefox, click **Options** then click **Allow 127.0.0.1**.



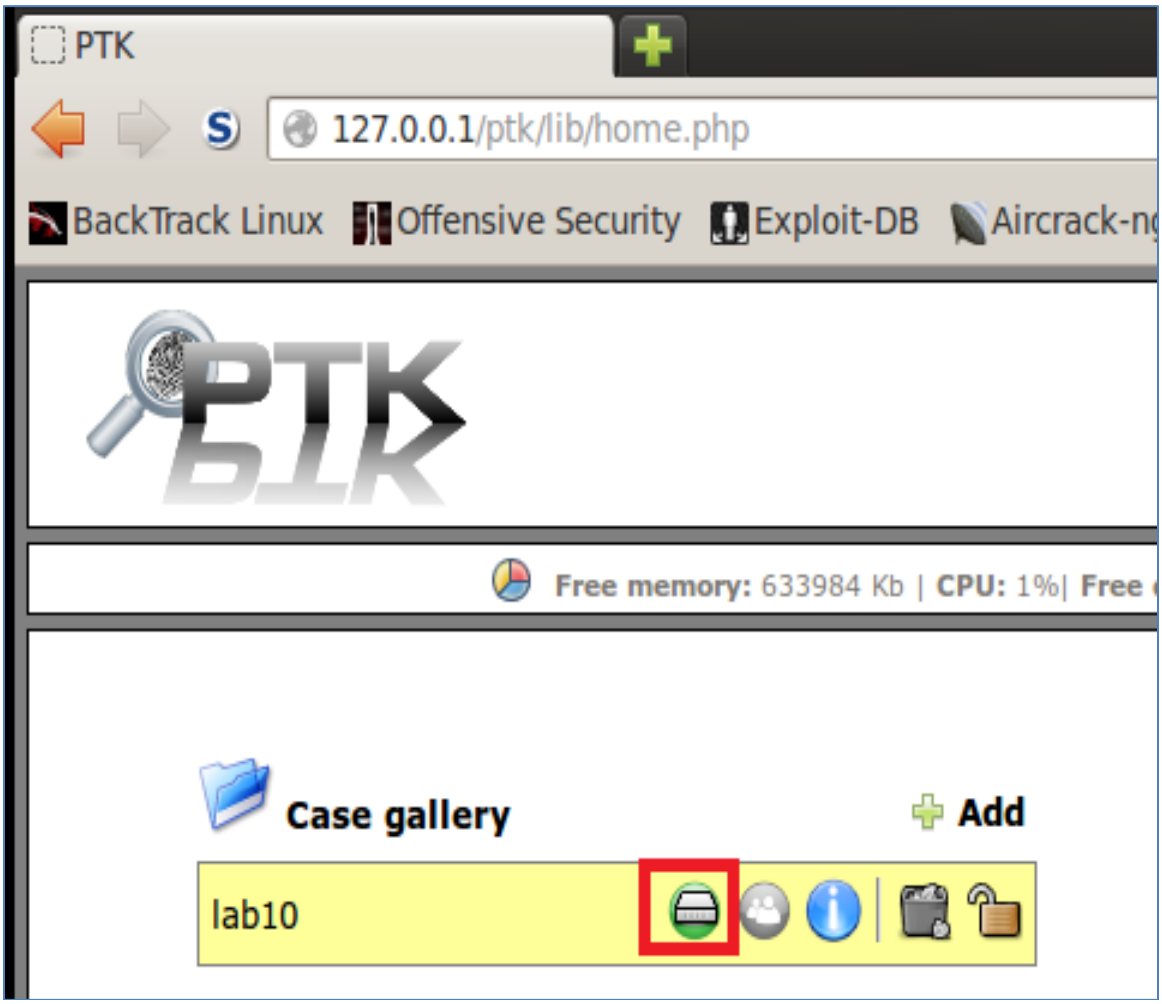
4. Click the **Add** button to start a new case within PTK.



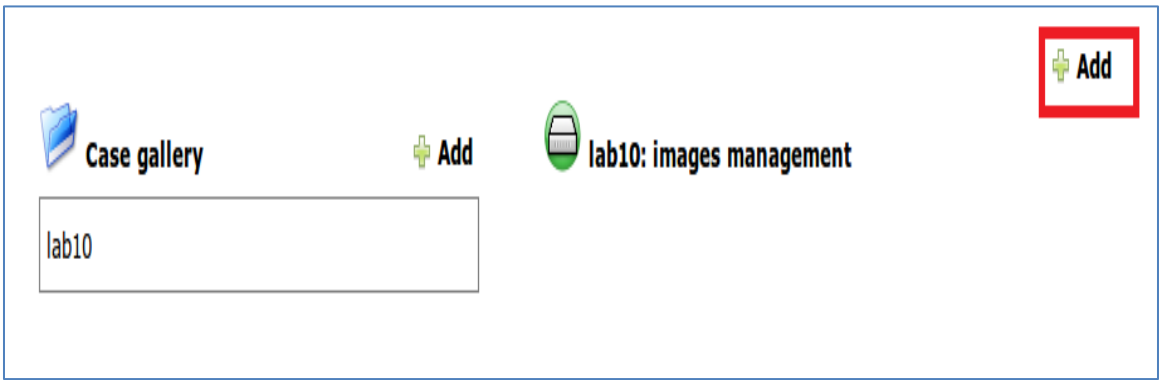
5. Enter **lab10** as the Case name. Click create.



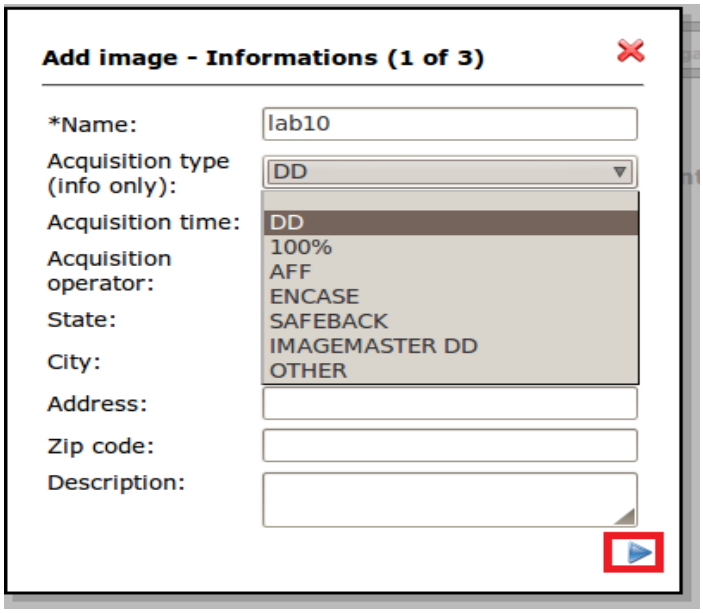
6. Hover to the right of lab10 and click the green drive icon (manage images).



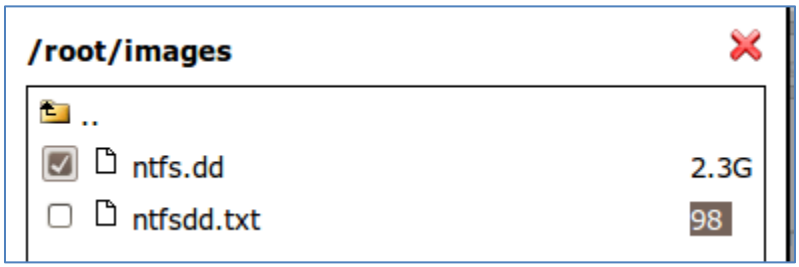
7. Click **Add** in the upper right to add the image to the Case gallery.



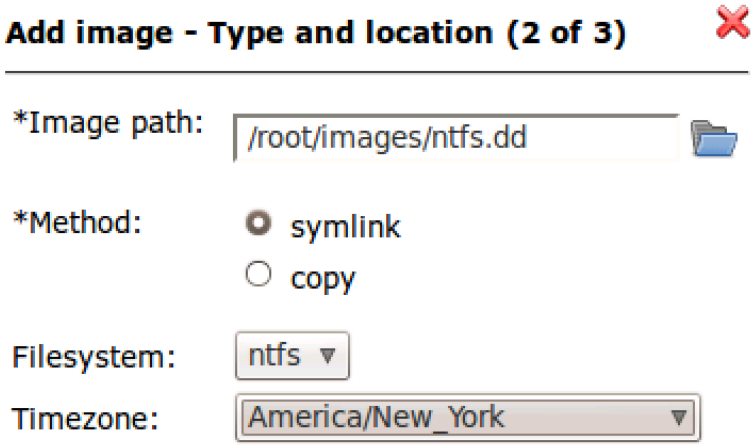
8. Type **lab10** for the name and select **DD** for acquisition type. Click the blue arrow for **Next.**



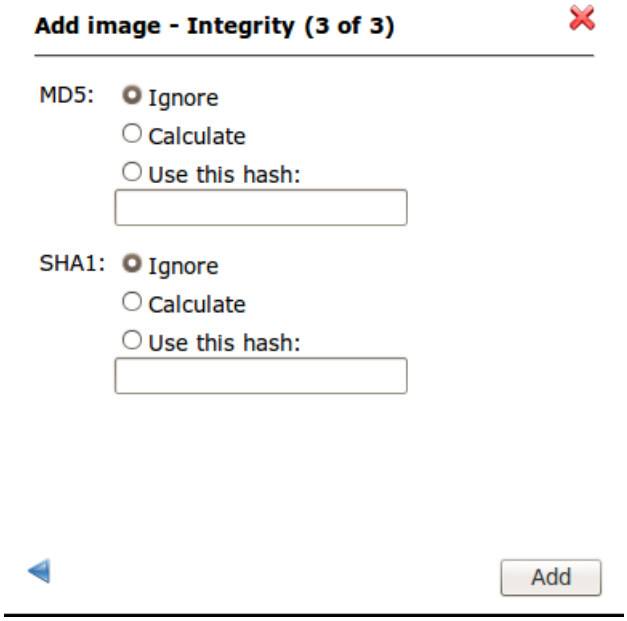
9. Browse to /root/images. Check the ntfs.dd file and click **Next**.



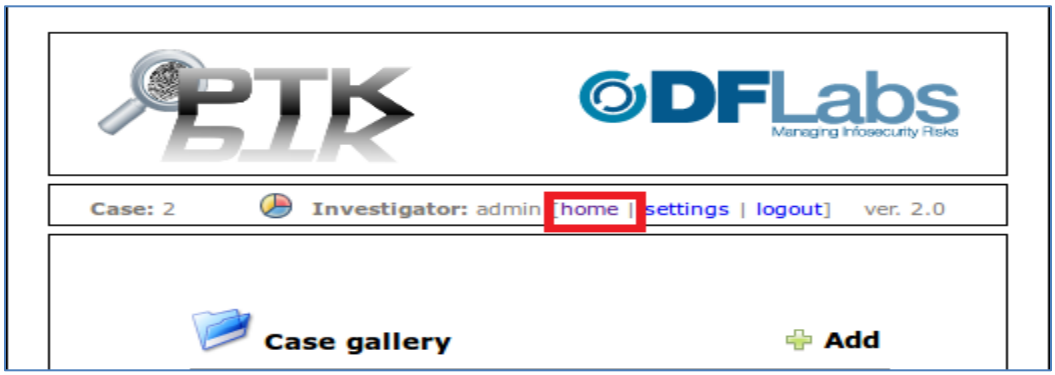
10. Verify that symlink is selected as the Method. Change Timezone to America/New_York and click the Next button. (Blue right arrow)



11. Click ignore for MD5 and SHA1 and select **Add**.

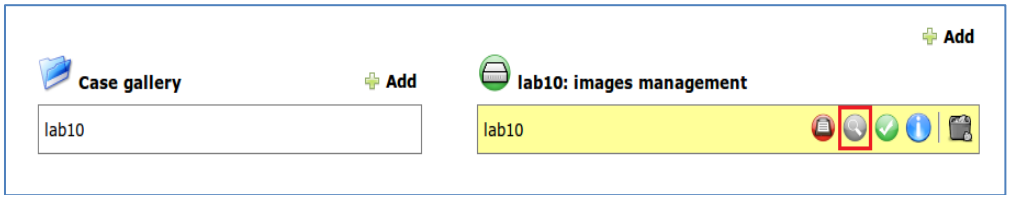


12. Click the **home** link to go back a page.

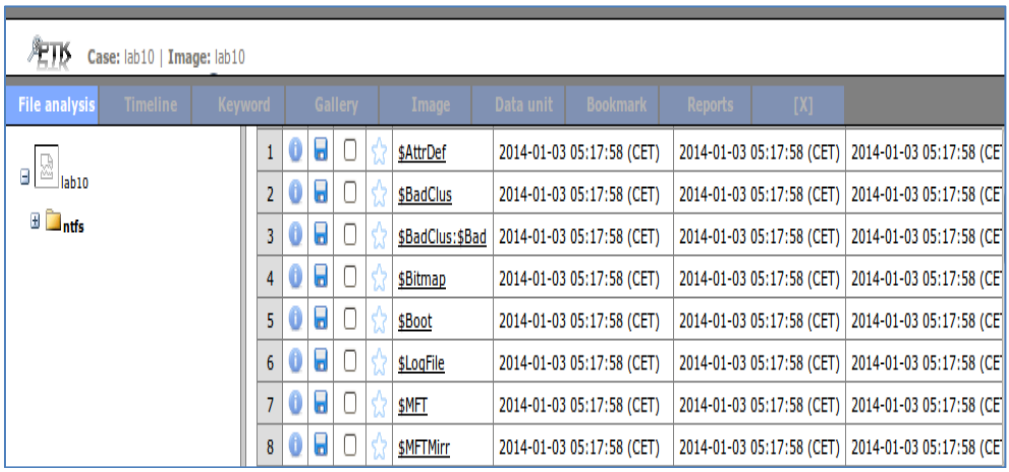


13. Click the green hard disk icon again, under the case gallery pane.

14. In the right pane, under **lab 10:images management**, click the gray magnifying glass icon. This button is used to analyze the NTFS image loaded into the case.



15. Expand Lab10 and then click on NTFS. Notice the NTFS system files including the Master File Table ($MFT).



16. Close the PTK application and the BackTrack 5 PC Viewer.

4.2 Conclusion

PTK is a forensic analysis tool that is free to use. Commercial forensic products, like EnCase and FTK, are more widely used but are not free and require hardware dongles. PTK comes installed on BackTrack, but the end user still needs to do some configuration, including specifying the image location and where evidence will be stored.

4.3 Discussion Questions

1. How do you setup PTK?
2. What link do you need to put in your browser to use PTK?
3. Name three files that should be on every NTFS image.
4. What is the function of the $MFT?

References

1. Comparing NTFS and FAT File Systems: windows.microsoft.com/en-us/windows-vista/comparing-ntfs-and-fat-file-systems

2. Alternate Data Streams: http://www.irongeek.com/i.php?page=security/altds

3. FAT32 vs. NTFS: http://www.pcmag.com/article2/0,2817,2421454,00.asp

4. Encrypted File System: http://en.wikipedia.org/wiki/Encrypting_File_System