DIGITAL FORENSICS LAB SERIES

Lab 16: Forensic Case Capstone

Objective - Digital Forensics Fundamentals

Document Version: 2014-02-07 (Beta)

Organization: Moraine Valley Community College
Author: Jesse Varsalone

The development of this document is 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 is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

This lab includes the following tasks:

1. Forensic Challenge 1 – Analysis and Reporting in Autopsy
2. Forensic Challenge 2 – Analysis and Reporting in PTK

Performing this lab will provide the student with a hands-on lab experience meeting the Evidence Acquisition, Preparation and Preservation Objective:

The candidate will demonstrate an understanding of forensic examination of user communication applications and methods, including host-based and mobile email applications, Instant Messaging, and other software and Internet-based user communication applications.

In this lab, you will be guided through the image loading process in Autopsy and PTK. After loading the images, you will be searching for artifacts related to “criminal” cases. You will need to bookmark the artifacts you find and generate a report.

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

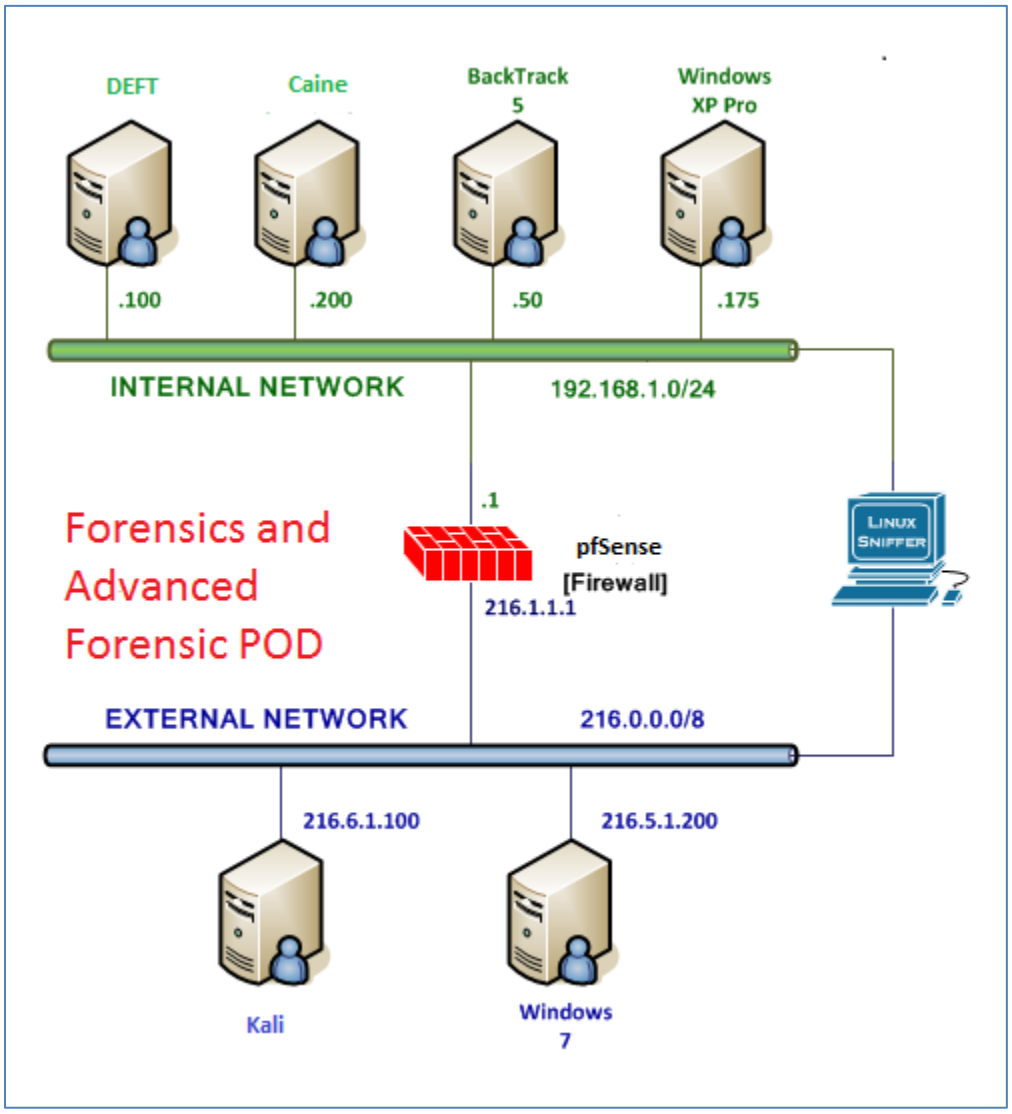
PTK – An open source and commercial forensic suite that will allow you to analyze disk images. DFLabs, based out of Italy, created PTK. The website is www.ptkforensic.com

The Sleuth Kit (TSK) is a collection of command line tools that are utilized by the PTK forensic browser. The Sleuth Kit tools can be utilized without Autopsy.

MD5 – Message Digest 5 is a 128-bit hashing algorithm that aids forensic examiners by “proving” that the copy of the media they are working on is "equivalent" to the original. Other hashes, like SHA-1, which is 160 bits, are more accurate than the 128 bit MD5.

SHA1 – Secure Hash Algorithm is a 160-bit hashing algorithm that aids forensic examiners by “proving” that the copy of the media they are working on is "equivalent" to the original. There are also 256, 384, and 512-bit versions of SHA that are more accurate.

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	216.5.1.200	student	password

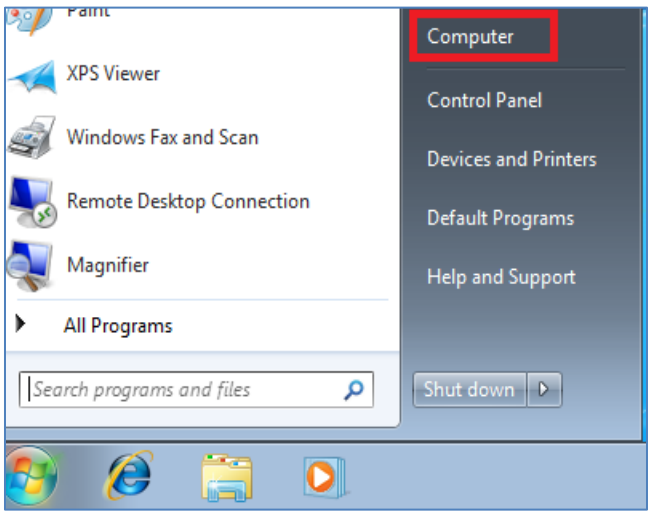
1 Forensic Challenge 1 – Analysis and Reporting Using Autopsy

The high cost of computer forensics software can be cost prohibitive for many companies and organization. Autopsy is one of the few free forensic suite options available. It runs on Linux and Microsoft Windows operating systems. Autopsy, developed by Brian Carrier, utilizes the command line tools of the The Sleuth Kit (TSK), underneath the hood.

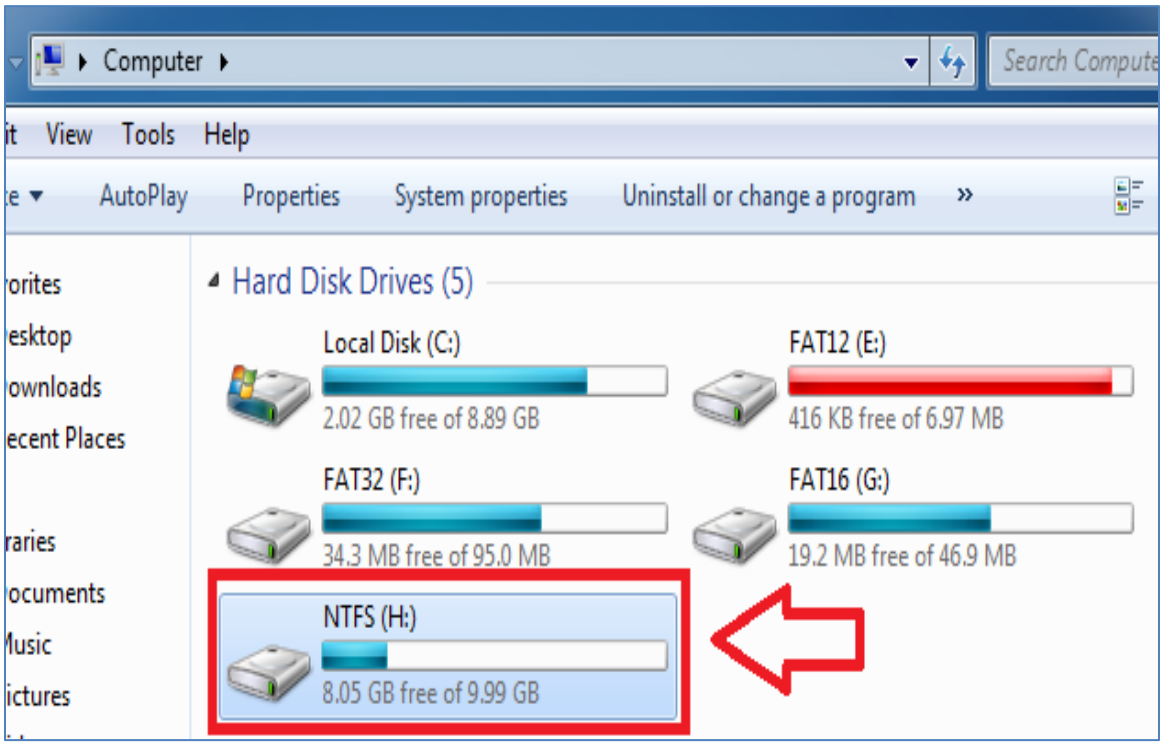
1.1 Installing Autopsy on Windows

1. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password,** and press **Enter** to log in.

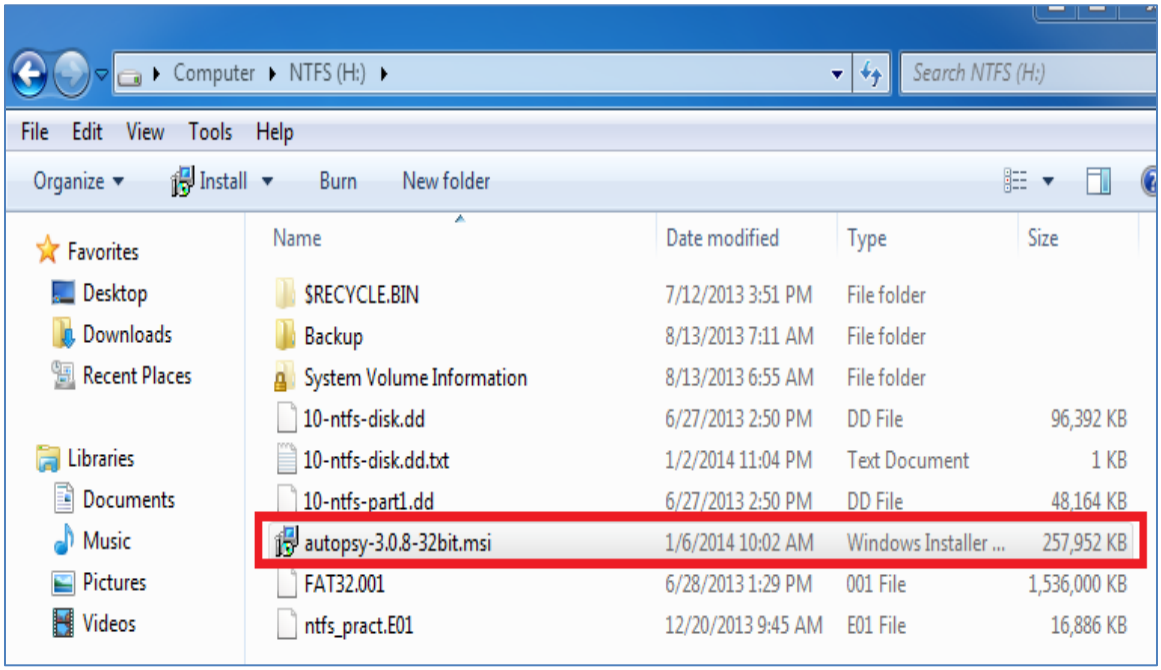
4. Click the Start icon in the lower-left corner and then select **Computer.**



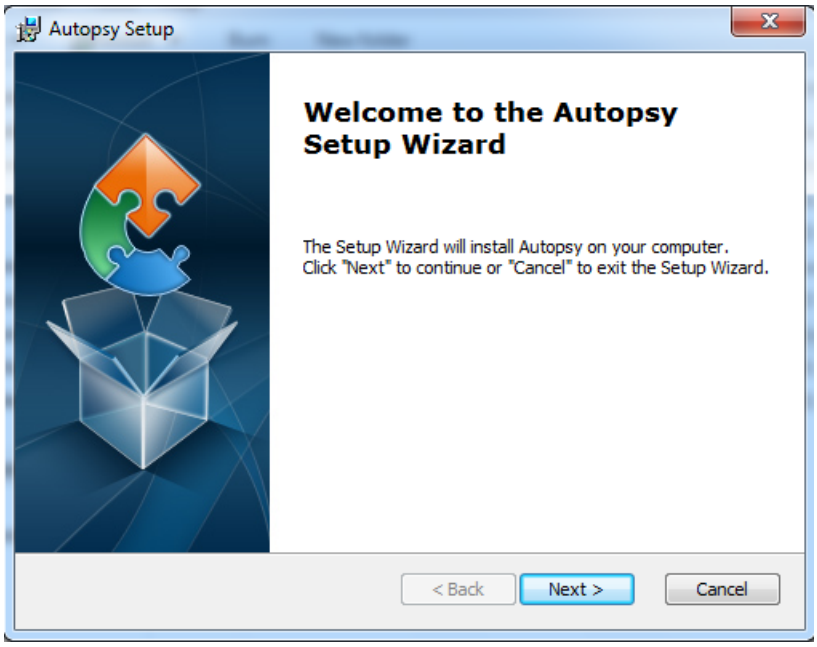
5. Double-click on the **(NTFS) H:** drive within Computer.



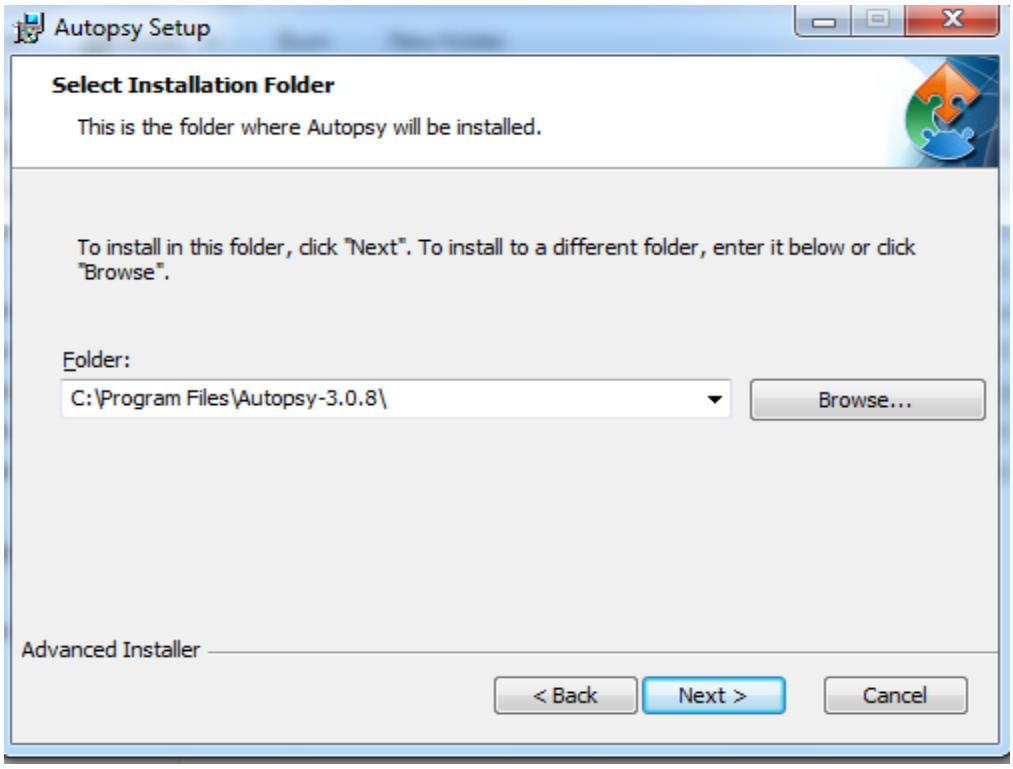
6. Double-click on the **autopsy-3.0.8-32bit.msi** file to install Autopsy.



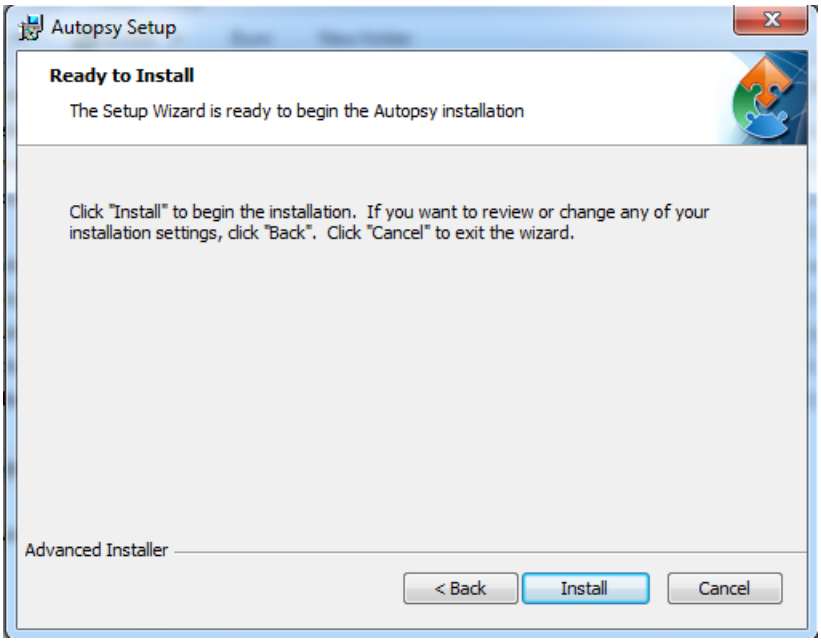
7. Click Next at the Welcome to the Autopsy Setup Wizard.



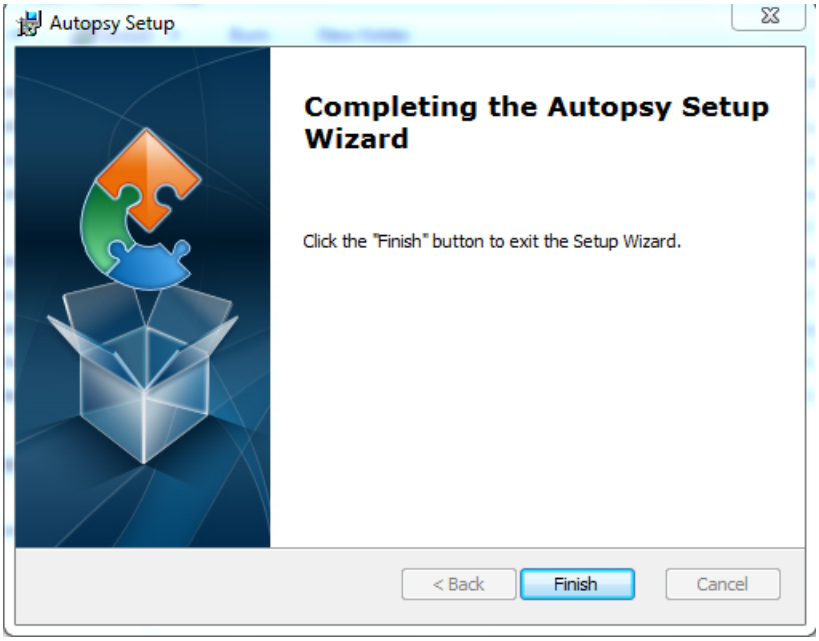
8. Accept the default for the installation directory and click **Next.**



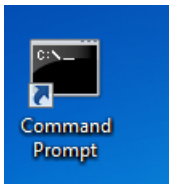
9. At the Ready to Install screen, click **Install**.



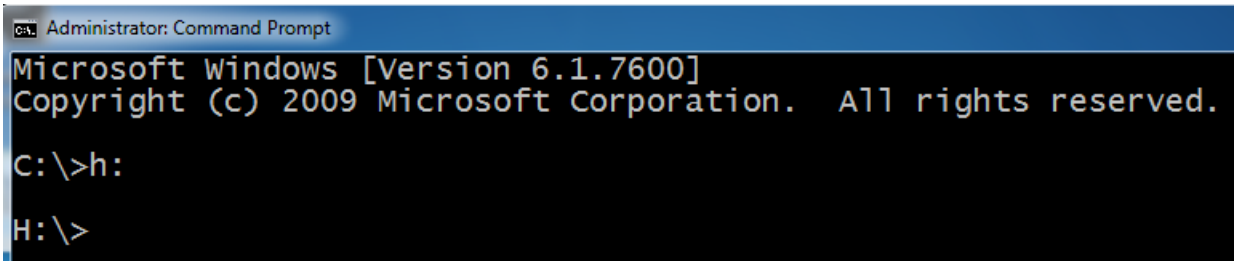
10. Click **Finish** at the Completing the Autopsy Setup Wizard screen.



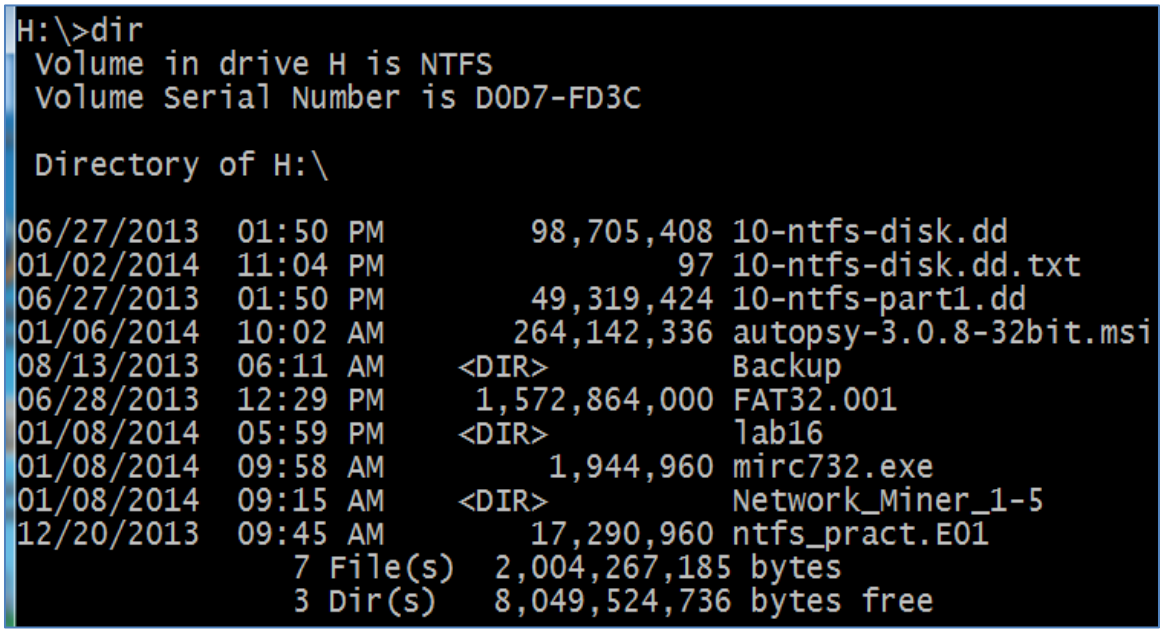
11. Double-click the shortcut to the Command Prompt on the desktop.



12. Type the following command to switch to the H: Drive:
    C:\>**h:**



13. Type the following command to view the directory:
    H:>**dir**



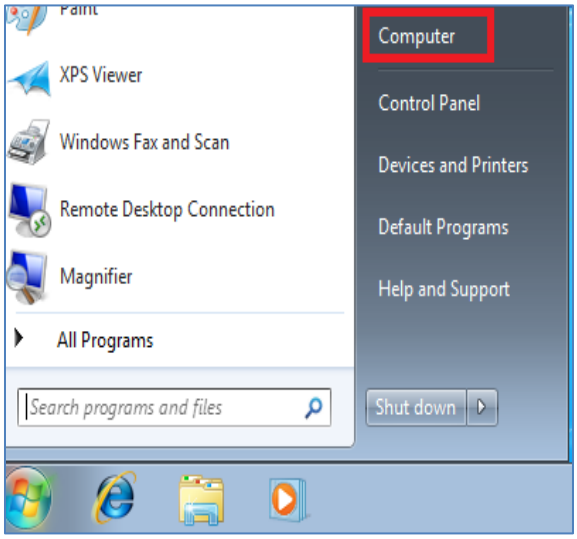
14. Type the following command to delete all of the files (but not the folders) on H:
    H:>**delete *.* /q**

Files are **NOT** sent to the Recycle Bin when deleted from the command line.

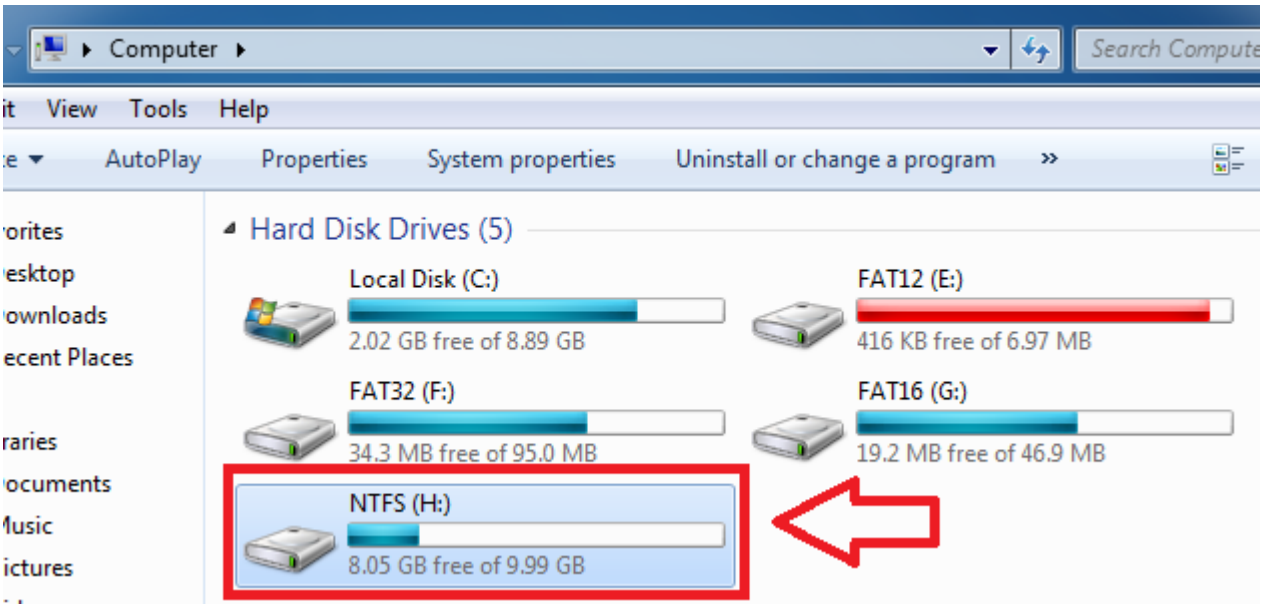
15. Type the following command to view the directory once again (notice the files are gone but the folders are still present):
H:>**dir**

```
H:\>dir
 Volume in drive H is NTFS
 Volume Serial Number is D0D7-FD3C

 Directory of H:\

08/13/2013  06:11 AM    <DIR>          Backup
01/08/2014  05:59 PM    <DIR>          lab16
01/08/2014  09:15 AM    <DIR>          Network_Miner_1-5
               0 File(s)              0 bytes
               3 Dir(s)  10,053,795,840 bytes free
```

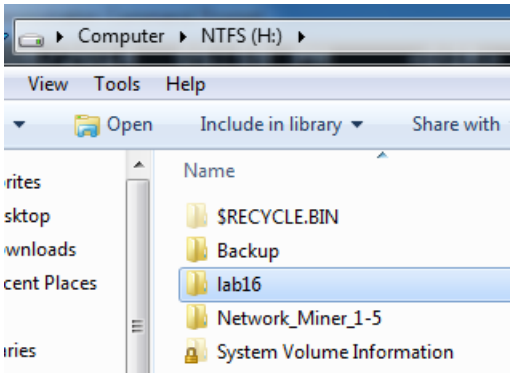
16. Click on the Start button and click on the link for **Computer**.



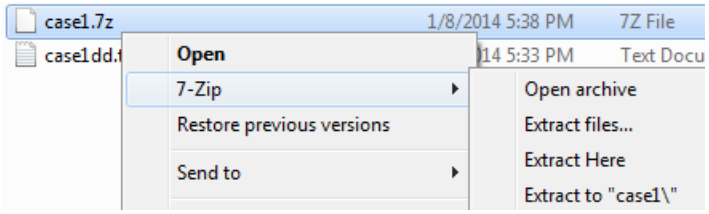
17. Double-click on the (NTFS) H: Drive within Computer.



18. Double-click on the **lab16** folder.

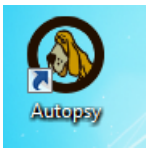


19. Right-click on case1.dd, select 7-zip, and select Extract to "case1\".



STOP: Wait for the file to finish unzipping before you proceed to the next step.

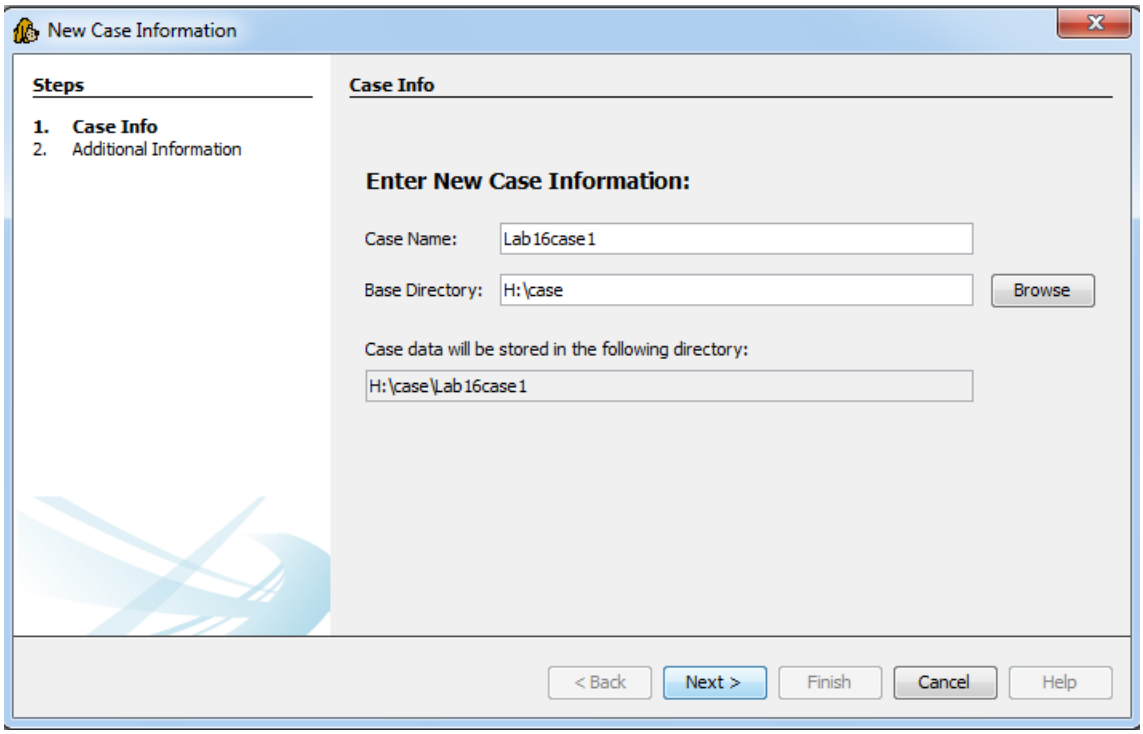
20. Double-click on the shortcut to Autopsy on the desktop.



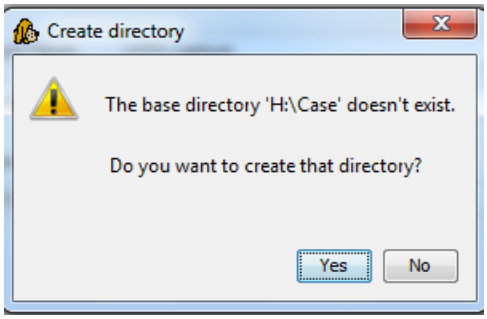
21. A window with a dog should eventually appear that says, *Starting modules.*

22. Click the Autopsy icon on your desktop. Click on **Create New Case**.

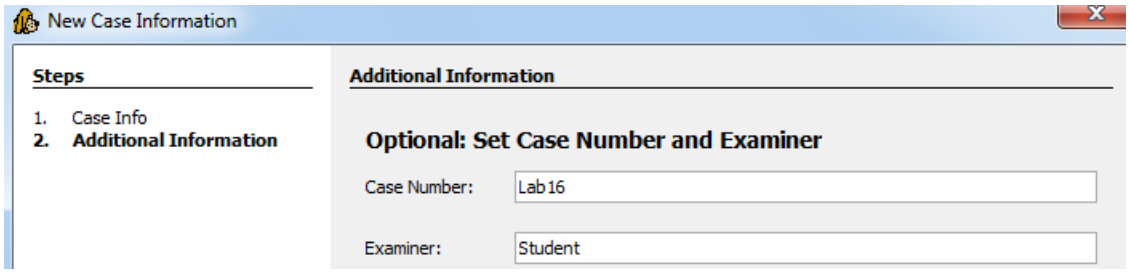
23. Name your case **Lab16case1**. For the Base directory, put H:\Case. Click Next.



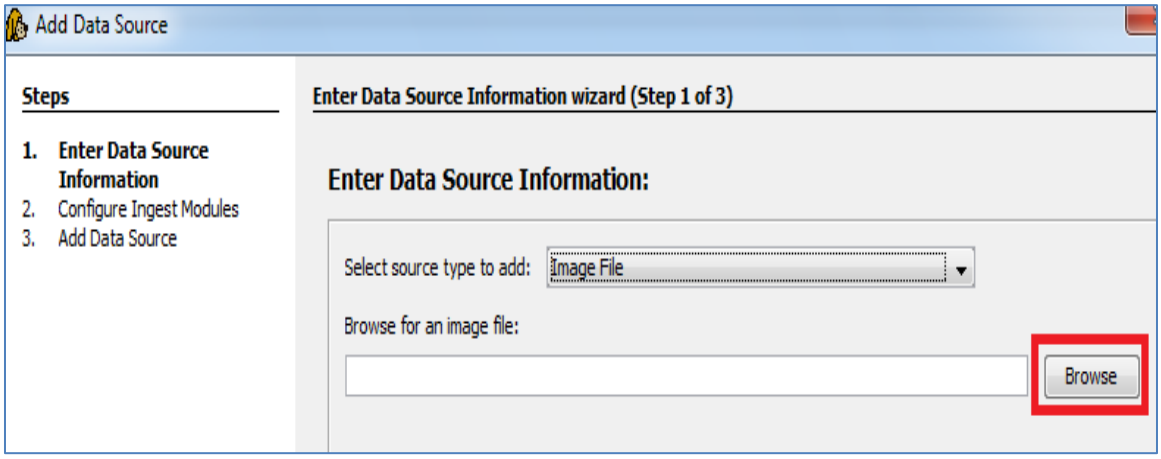
24. Click Yes to create H:\Case directory.



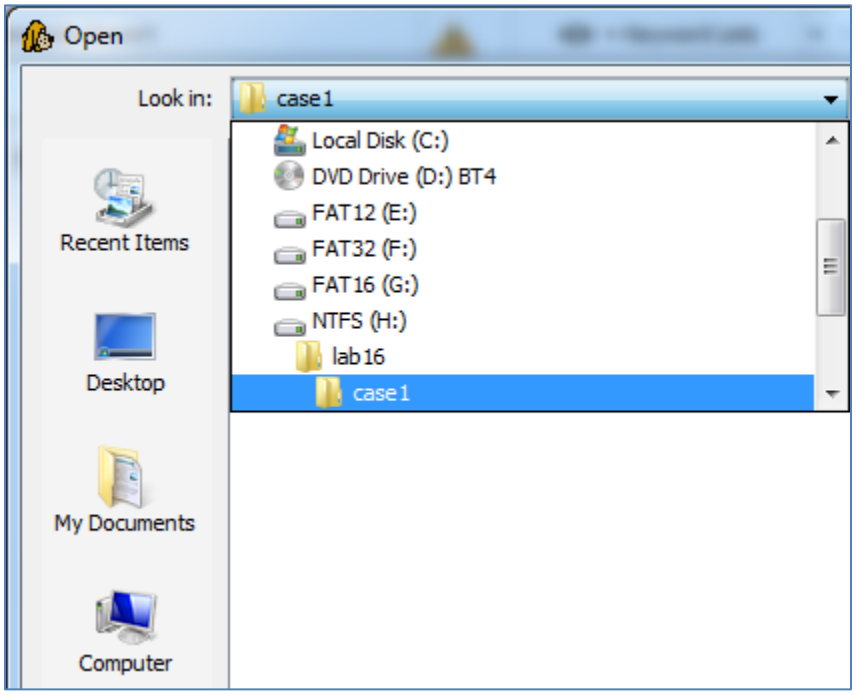
25. The **case number** will be Lab16. Put student in the **Examiner** field. Click **Finish**.



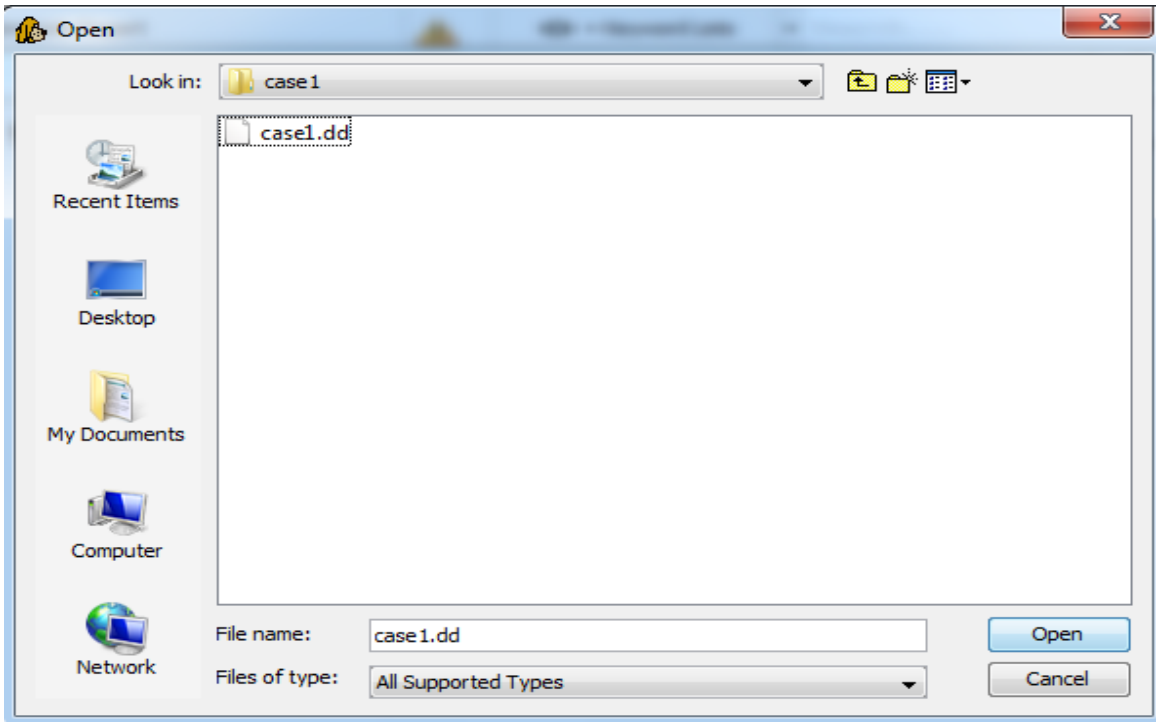
26. In the **Add Image** window, select **Image File** from the **Select Input type to add** dropdown. Click on **Browse.**



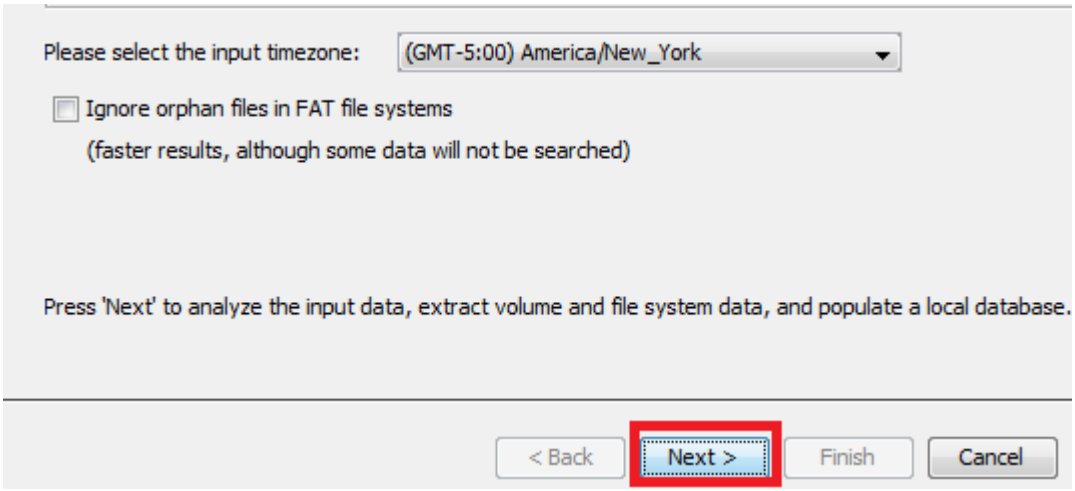
27. Click Computer on the left, then double click on **NTFS H: > lab16 > case1**.



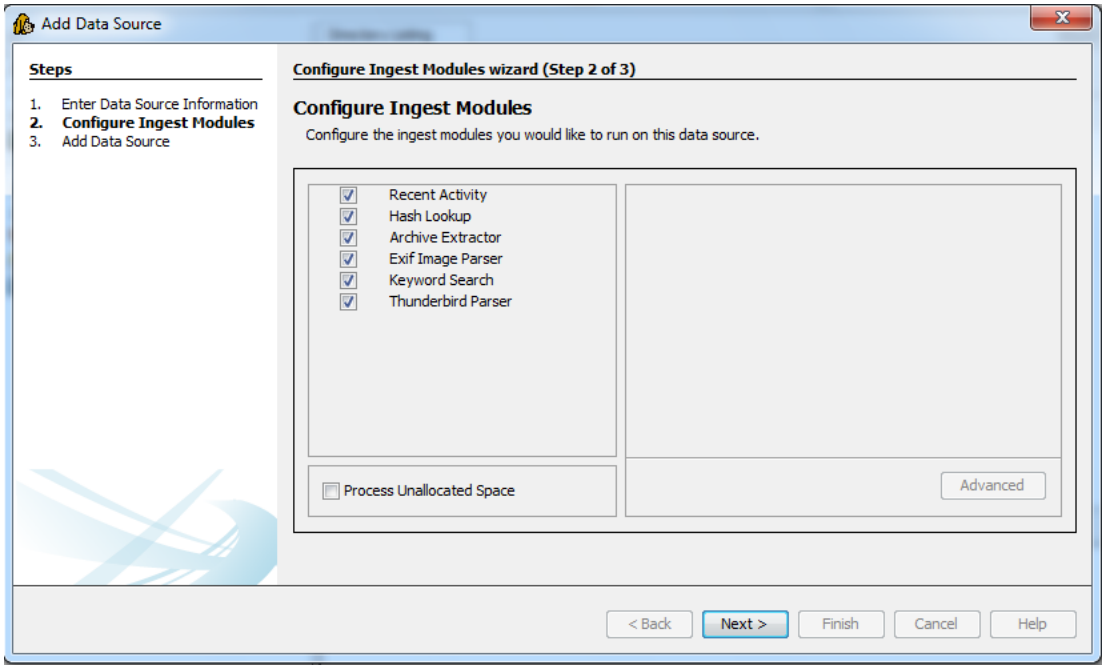
28. Select the case1.dd file and click **Open**.



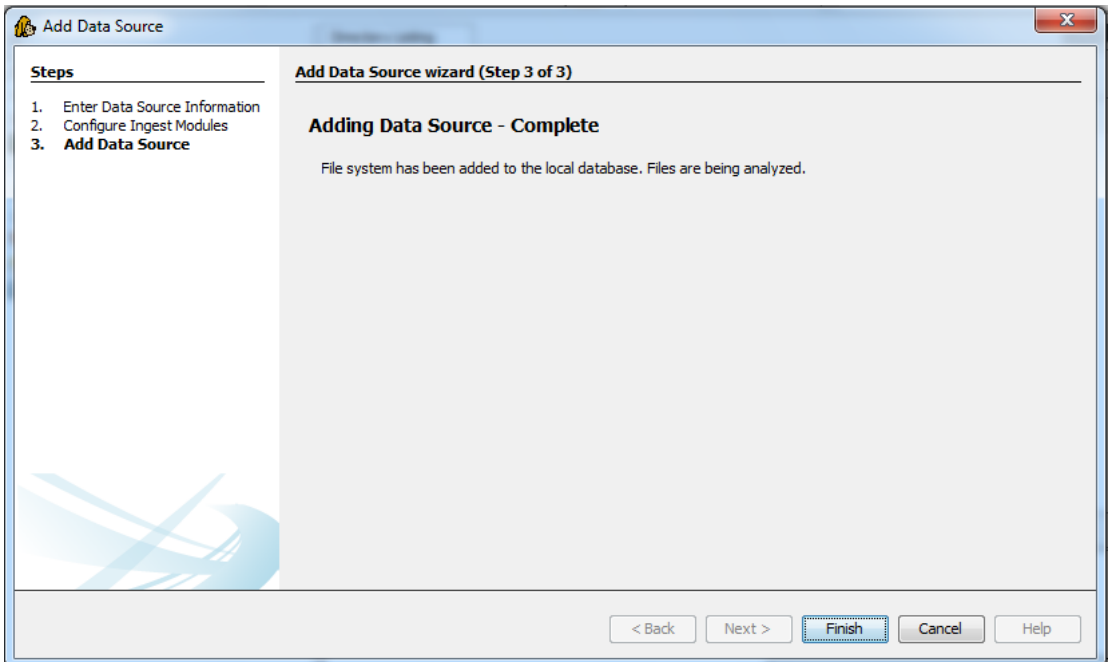
29. Leave the image timezone as (GMT-6:00) America/New York. Click **Next**.



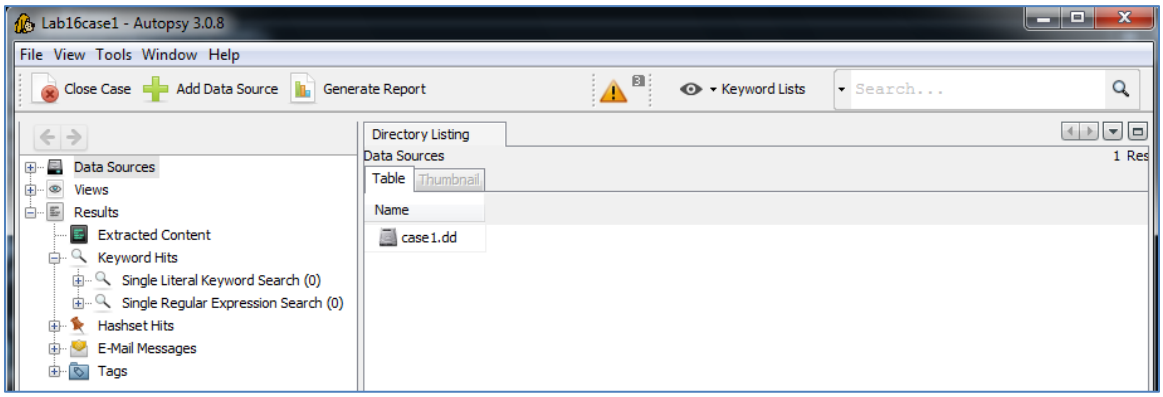
30. Leave all the boxes checked. This will allow different built-in modules in Autopsy to extract files from the image. Click **Next**.



31. The tool will begin processing. Click Finish.



32. Your image should now be loaded and you may begin the forensic challenge.



1.2 Performing Forensic Challenge 1

Forensic Challenge 1 – Analysis and Reporting in Autopsy
Susie Stapleton has gone missing for 3 days. Her husband and kids are worried sick. A police officer has acquired an image of her hard drive. 1. Look through her user profile to find any pictures that might reveal where she is 2. Bookmark any photos you find that you deem to be relevant 3. Generate a forensic report in HTML format

After you have completed the forensic challenge:

1. Close Autopsy.
2. Delete the case1.dd file from the H: drive.
3. Empty the Recycle Bin.

2 Forensic Challenge 2 - Analysis and Reporting Using PTK

PTK, developed by DFLabs in Italy, utilizes the command line tools of The Sleuth Kit. PTK is similar to Autopsy, but has both a free version and a commercial version.

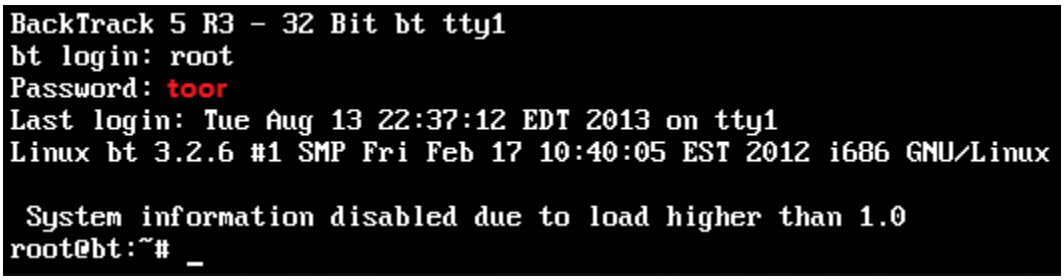
Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

2.1 Loading the NTFS Image into PTK

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

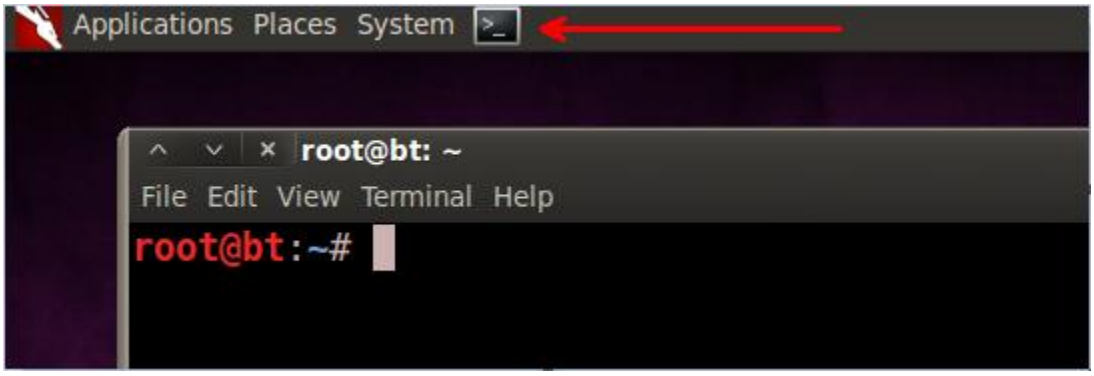
1. Open the **BackTrack 5 R3 Internal Machine**. Type **root** for the login and **toor** *(root spelled backwards)* for the password.

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

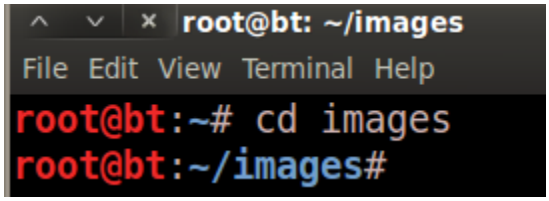


2. Type the following command to start the Graphical User Interface (GUI):
root@bt:~# **startx**

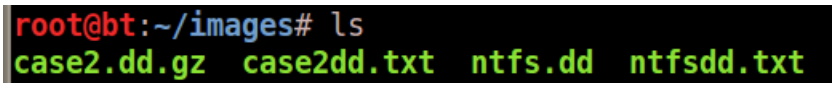
3. Open a terminal by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.



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

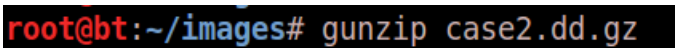


5. Type the following command to view the files in the image folder:
root@bt:~# **ls**



6. Type the following command to remove the large case2.dd image file.
root@bt:~# **rm -rf case2.dd**

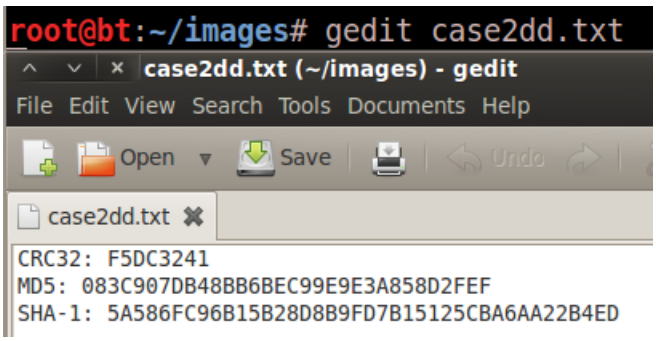
7. Type the following command to remove the large case2.dd image file.
root@bt:~# **gunzip case2.dd.gz**



STOP: Wait for the file to finish unzipping before you proceed to the next step.

8. Type the following command to view the unzipped file
root@bt:~# **ls**

9. Type the following command to view the file from the Graphical User Interface:
root@bt:~/images# **gedit case2dd.txt**



10. Close the file when you are finished viewing it with the gedit application.

11. Type the following command to view the file contents from the terminal:
    root@bt:~/images# **cat case2dd.txt**

```
root@bt:~/images# cat case2dd.txt
CRC32: F5DC3241
MD5: 083C907DB48BB6BEC99E9E3A858D2FEF
SHA-1: 5A586FC96B15B28D8B9FD7B15125CBA6AA22B4ED
```

12. Type the following command to view the MD5 hash:
    root@bt:~/images# **cat case2dd.txt | grep MD5**

```
root@bt:~/images# cat case2dd.txt | grep MD5
MD5: 083C907DB48BB6BEC99E9E3A858D2FEF
```

13. Type the following command to view the file with the hashing information :
    root@bt:~/images# **md5sum case2.dd**

```
root@bt:~/images# md5sum case2.dd
083c907db48bb6bec99e9e3a858d2fef  case2.dd
```

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

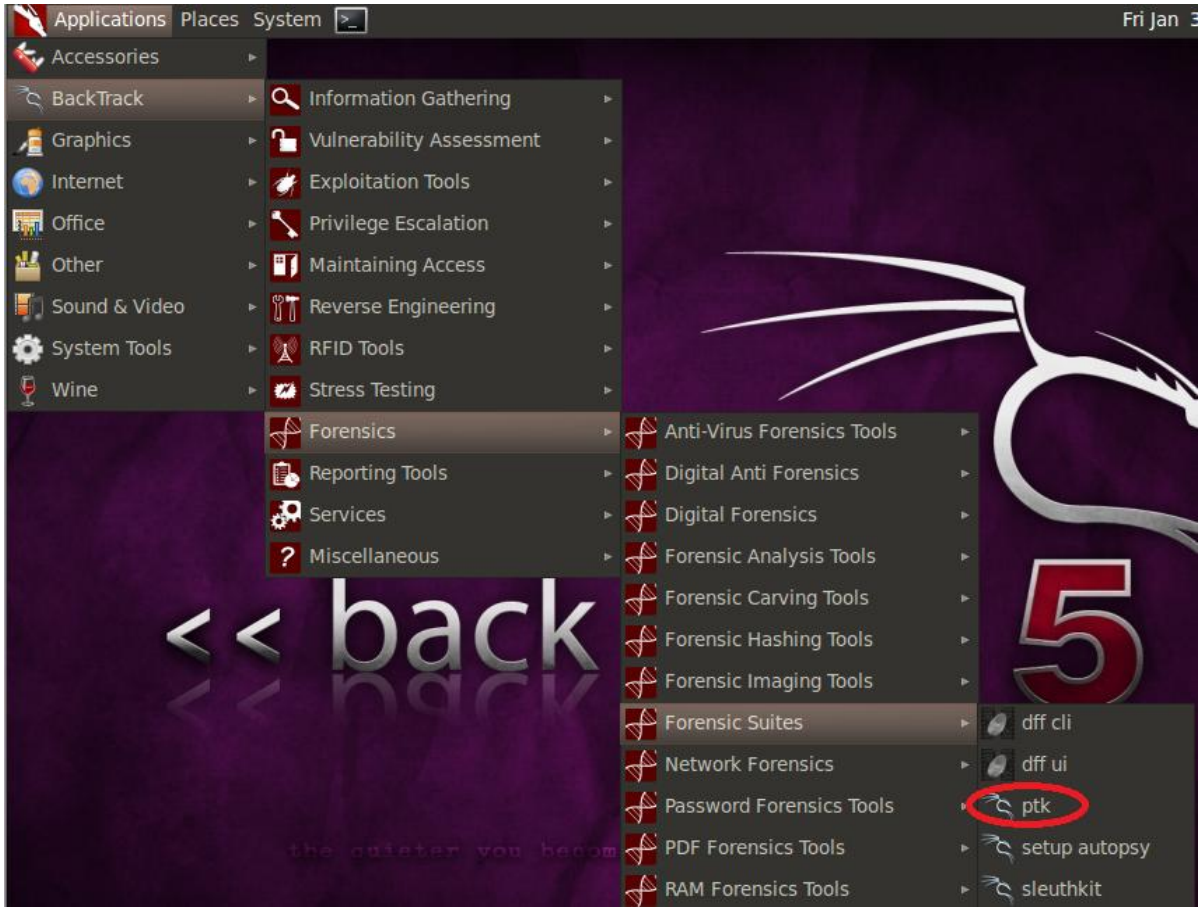
14. Type the following command to view the SHA1 hash:
    root@bt:~/images# **cat case2dd.txt | grep SHA1**

```
root@bt:~/images# cat case2dd.txt | grep SHA-1
SHA-1: 5A586FC96B15B28D8B9FD7B15125CBA6AA22B4ED
```

15. Type the following command to view the file with the hashing information :
    root@bt:~/images# **sha1sum case2.dd**

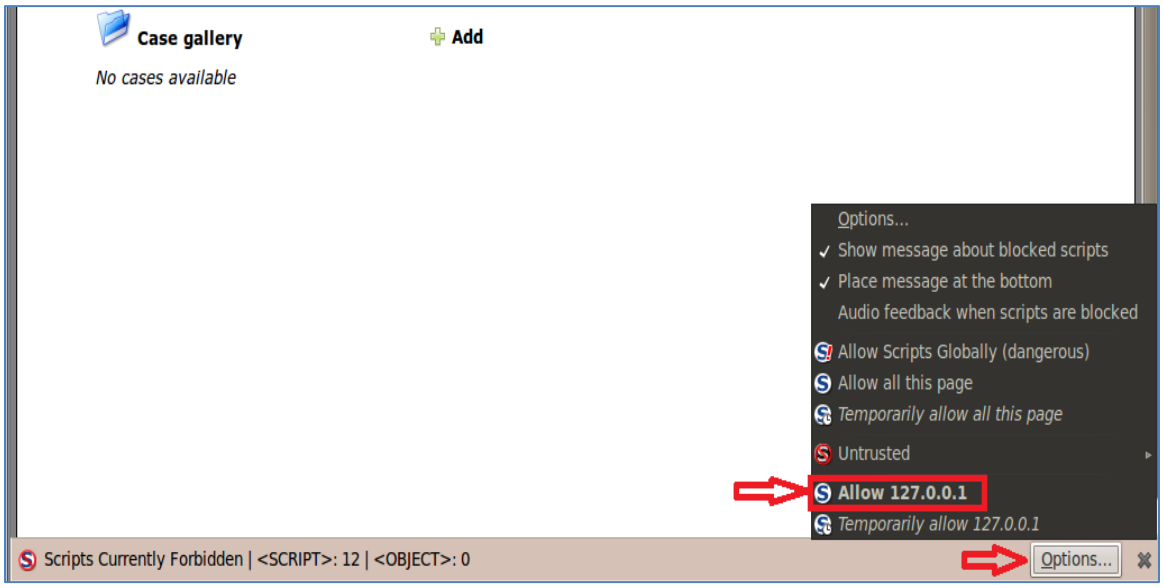
```
root@bt:~/images# sha1sum case2.dd
5a586fc96b15b28d8b9fd7b15125cba6aa22b4ed  case2.dd
```


16. On the BackTrack 5 R3 Internal Machine, click **Applications > BackTrack > Forensics > Forensic Suites > PTK**.

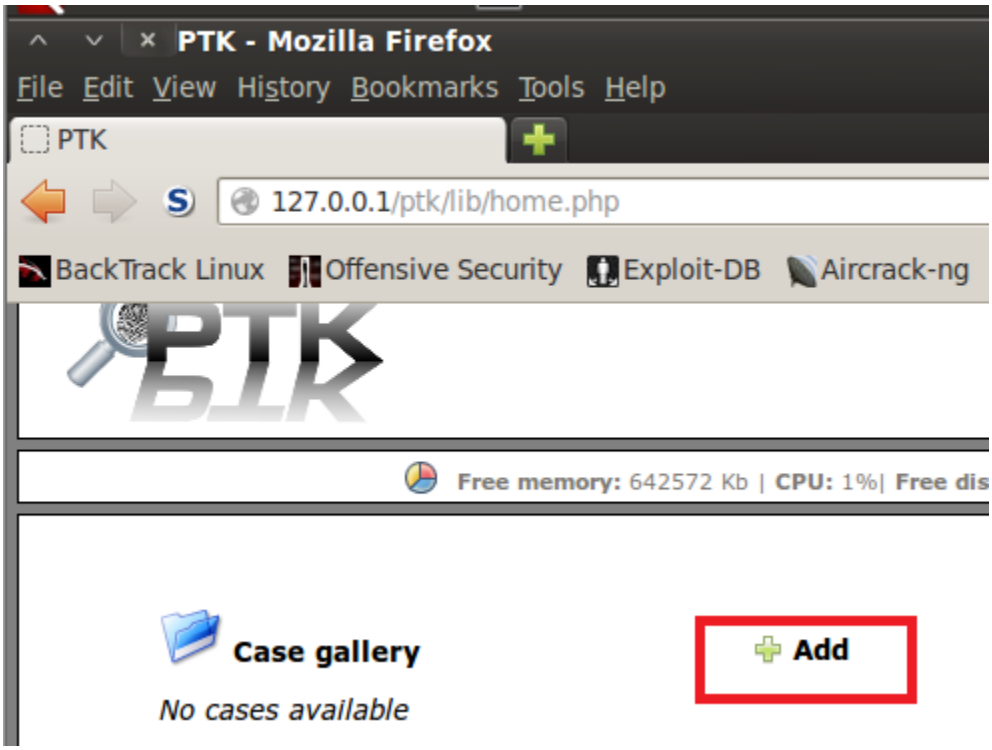


17. For the username, type **admin,** for the password, type **toor.**

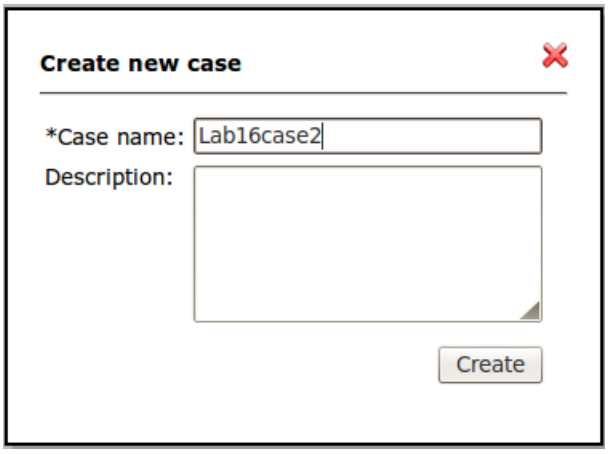
18. In the bottom-right corner of Firefox, click **Allow 127.0.0.1**.



19. Click the **Add** button to start a new case within Autopsy.

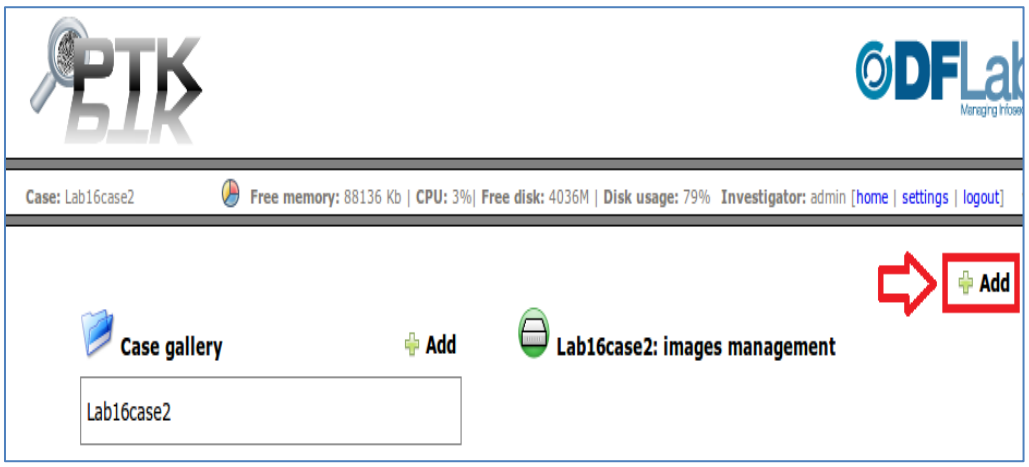


20. Enter **Lab16case2** as the case name and click Create.

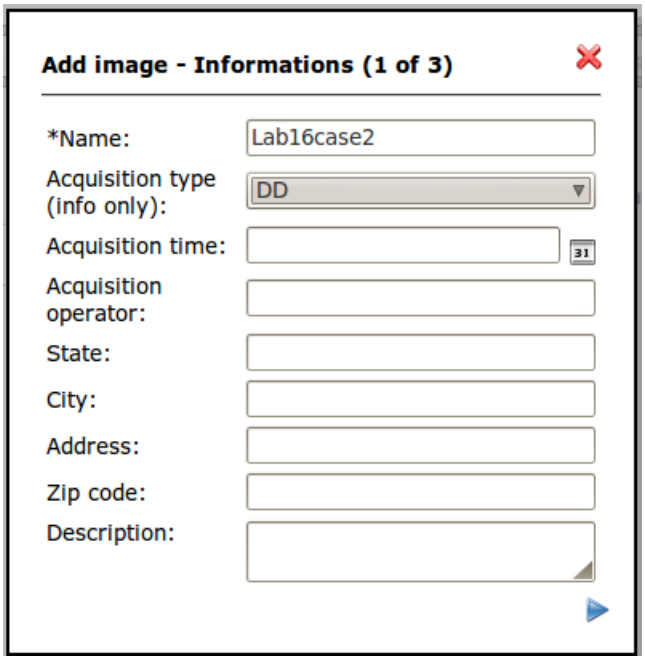


21. Click the Green Drive Icon (manage images) to the right of Lab16case2.

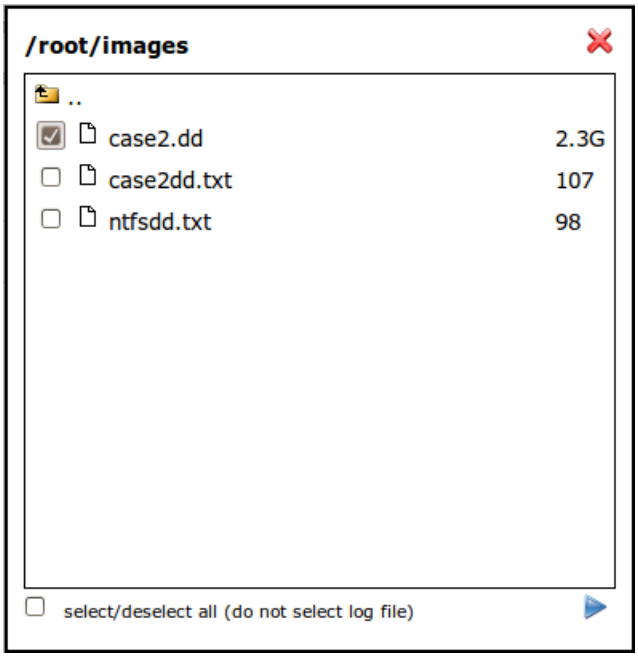
22. Click **Add** to add the Image to the PTK Case.



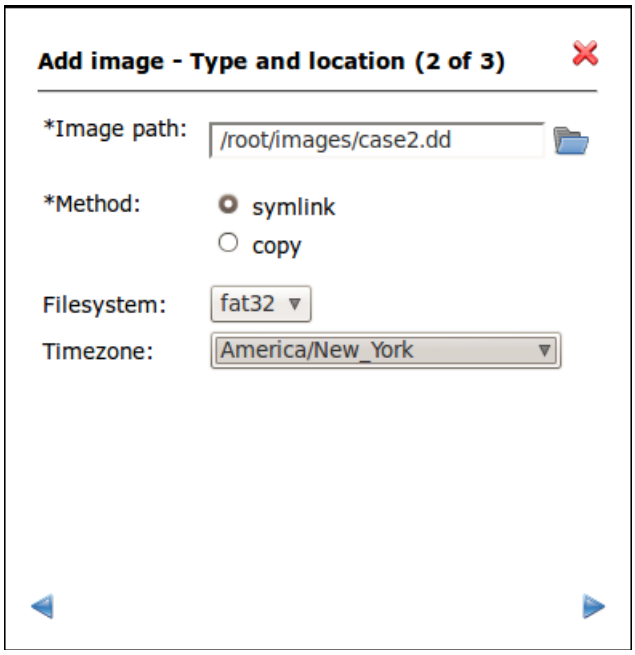
23. Type Lab16case2 for the name and select DD for acquisition type. Click Next.



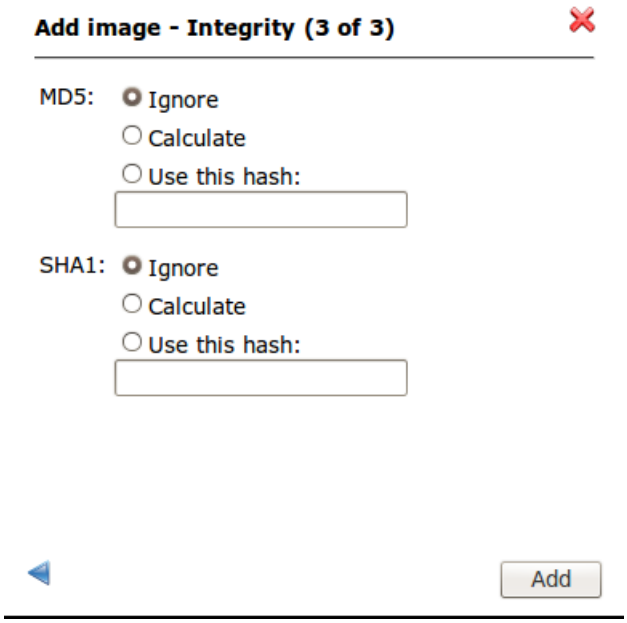
24. Browse to **/root/images**. Check the case2.dd file and click Next.



25. Verify that symlink is checked as the Method and that the Filesystem is recognized as FAT32. Use the dropdown box to change the Timezone to America/New_York. Click Next.

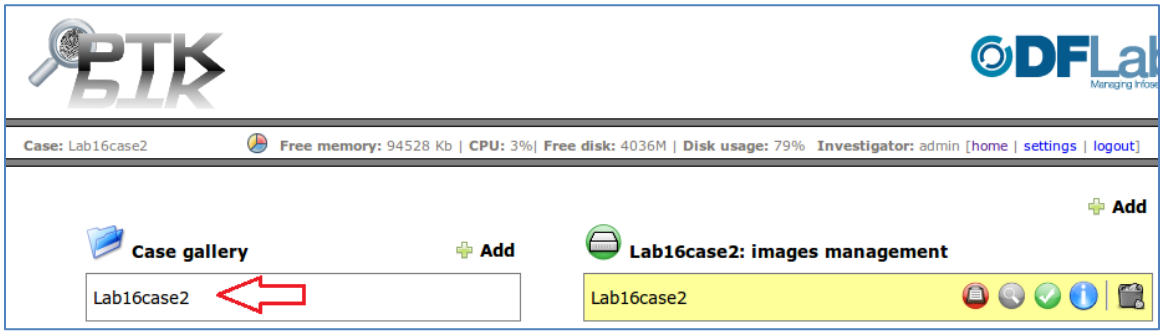


26. Check Ignore for both MD5 and SHA1 and then click Add.

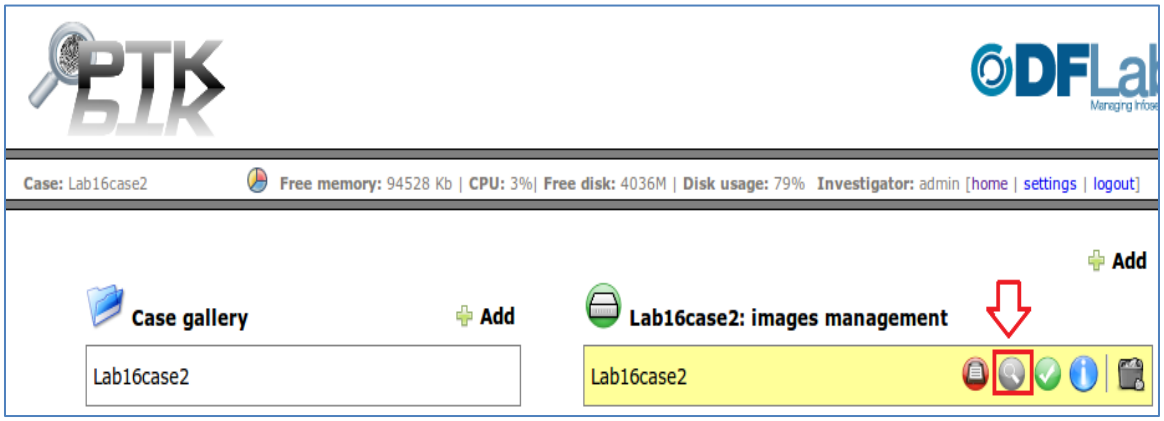


27. Click the **Case: Lab16case2** hyperlink.

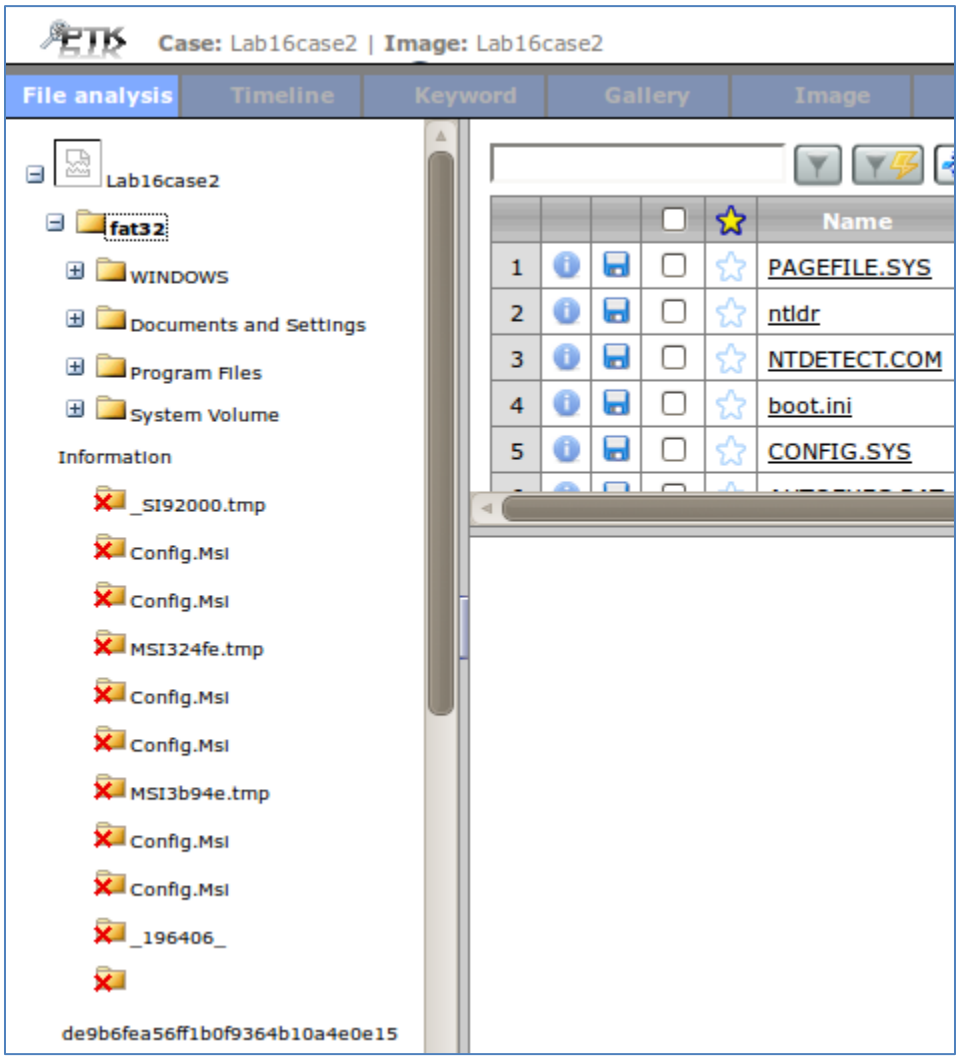
28. Click **Lab16case2** under Case Gallery to view Lab16case2: images management.



29. In the right pane, under lab 16case2: images management, click the gray icon to the right of Lab16case2. This button is used to analyze the NTFS image loaded into the case.



30. Expand Lab16case2, then expand fat32. The file system should load.



2.2 Performing Forensic Challenge 2

Forensic Challenge 2 – Analysis and Reporting in PTK
Jimmy Jamison has been arrested for stealing credit cards. He has used five different credit cards that were not his. A police officer has acquired an image of his hard drive. 1. Look through his user profile to find any documents that Jimmy had 2. Export the documents and view them to determine if credit card info is present 3. Bookmark any documents that you deem to be relevant 4. Generate a forensic report in PDF format

Close PTK, after you have completed the forensic challenge.

References

1. Test Images and Forensic Challenges:
   http://www.forensicfocus.com/images-and-challenges

2. Honeynet Project Challenges:
   http://www.honeynet.org/challenges

3. DFRWS 2014 Forensics Challenge:
   http://www.dfrws.org/2014/challenge/

4. How to Write a Forensic Report:
   http://www.ehow.com/how_5858380_write-forensic-report.html

5. Forensic Reporting:
   http://www.eteraconsulting.com/12/07/forensic-reporting-how-it-works-and-why-it-important

