FORENSICS
LAB SERIES

Lab 11: Introduction to Autopsy

Document Version: 2016-08-17

Contents

Introduction

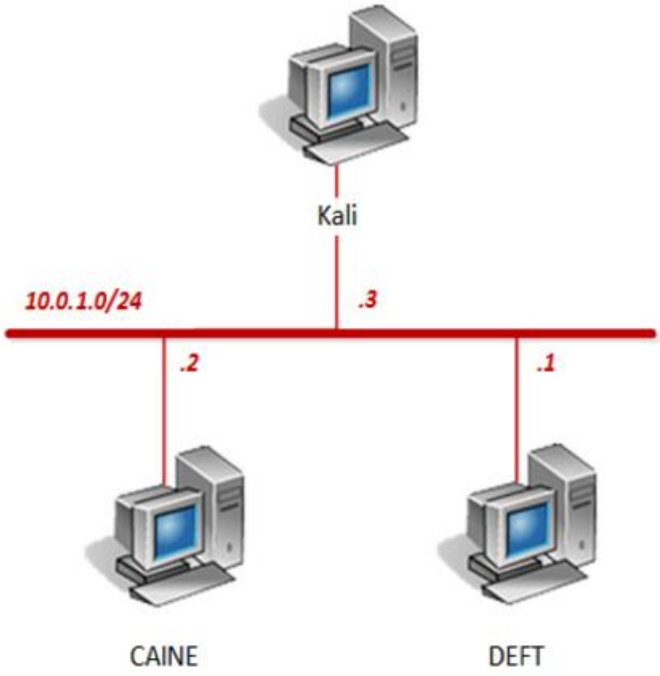
This lab will introduce a tool called Autopsy, which is an open source digital forensics platform and graphical interface to the Sleuth Kit developed by Brian Carrier. The basics of using the tool for performing a forensic investigation will be taught in this lab.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Creating & Adding Images to a Case
2. Analyzing Images with Autopsy

Pod Topology



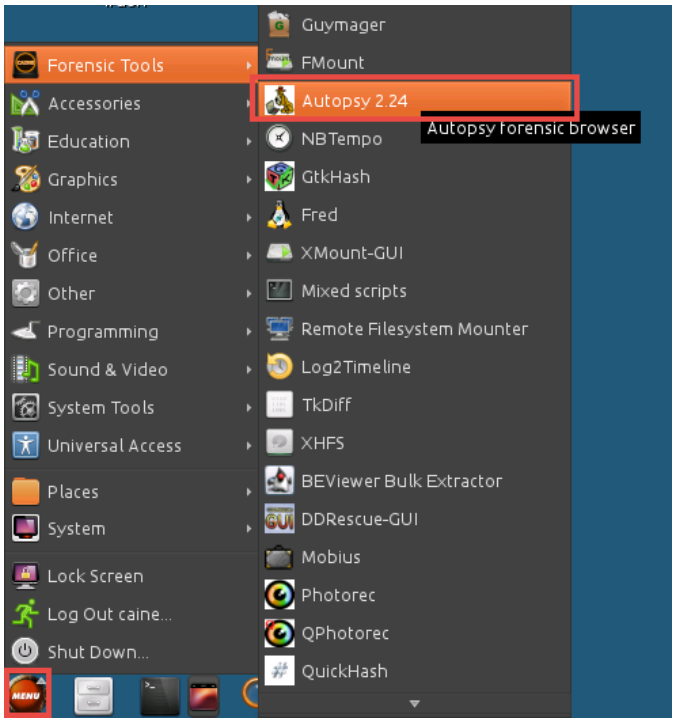
Lab Settings

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.

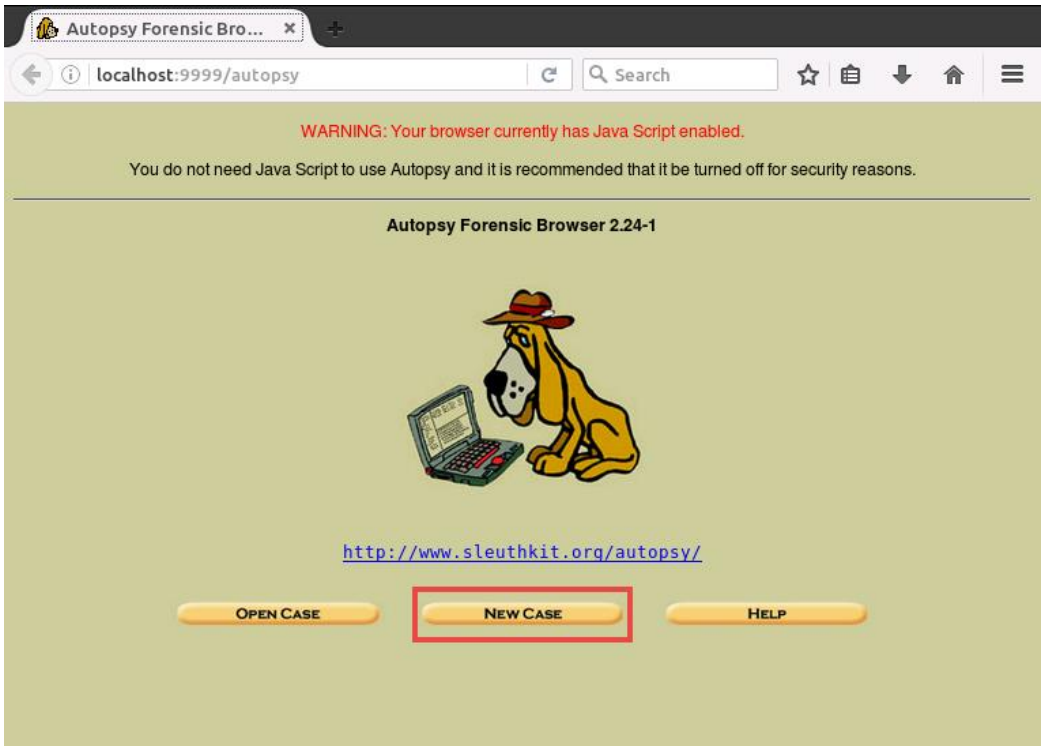
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Creating & Adding Images to a Case

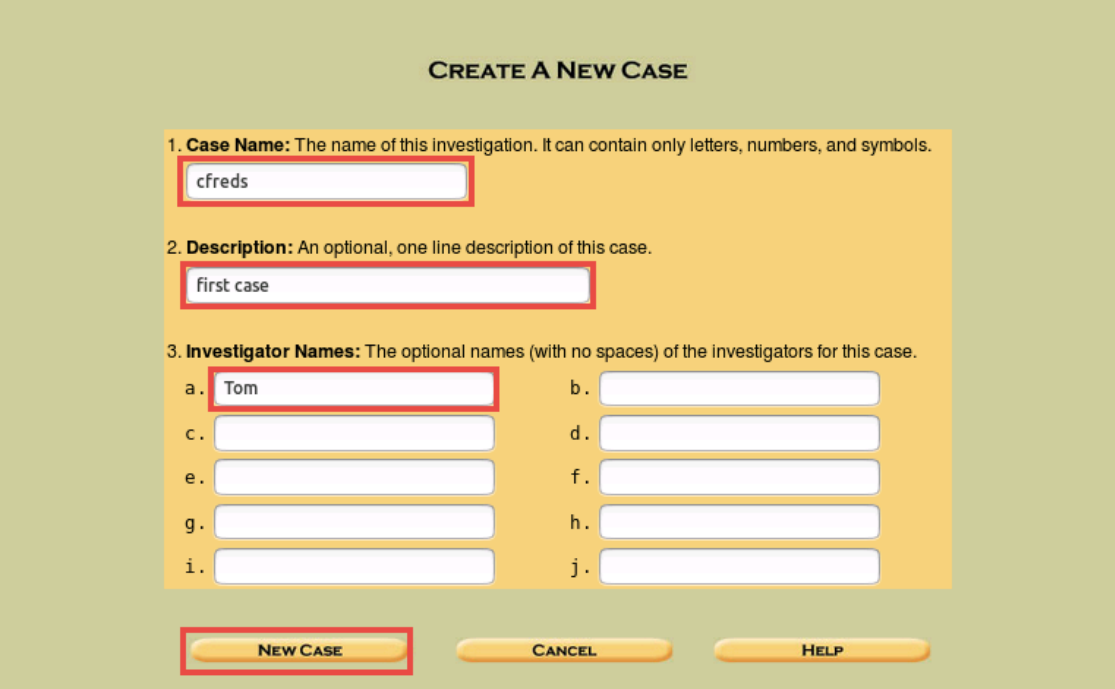
1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open the *Autopsy* application by navigating to **Menu > Forensic Tools > Autopsy 2.24**.



3. In the *Autopsy Forensic Browser* window, click on the **New Case** icon.

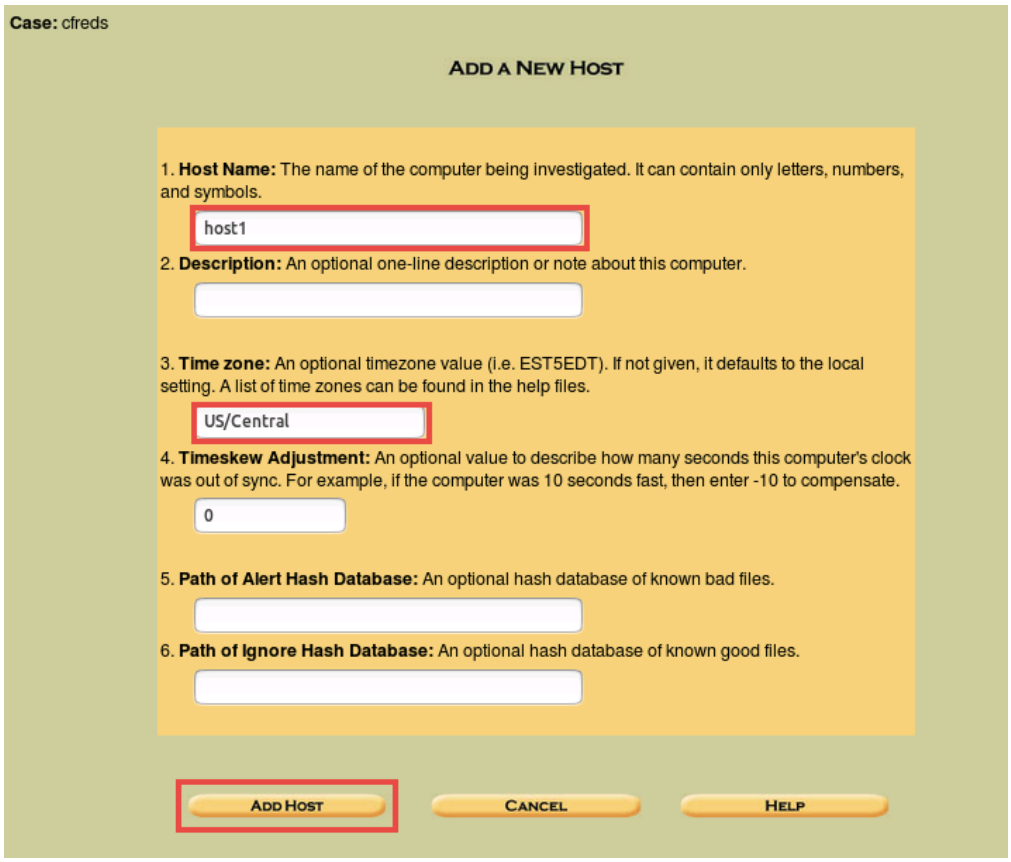


4. On the *Create a New Case* page, enter the following information:
   a. *Case Name*: `cfreds`
   b. *Description*: `first case`
   c. *Investigator Names*: "*Your Name*"

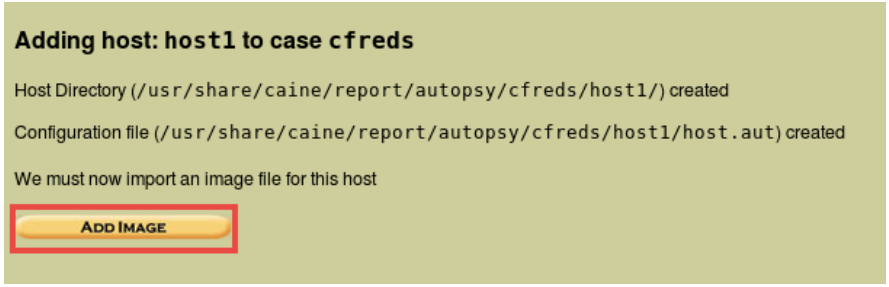


5. Once the information has been filled, click **New Case**.
6. On the *Creating Case* page, confirm that your name is selected and click **Add Host**.

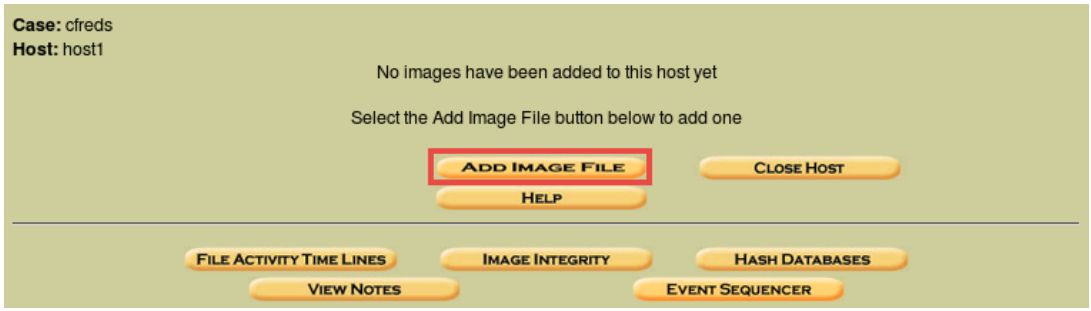
7. On the *Add a New Host* page, enter the following information, leaving the rest with their default values.
    a. *Host Name*: `host1`
    b. *Time Zone*: **US/Central**



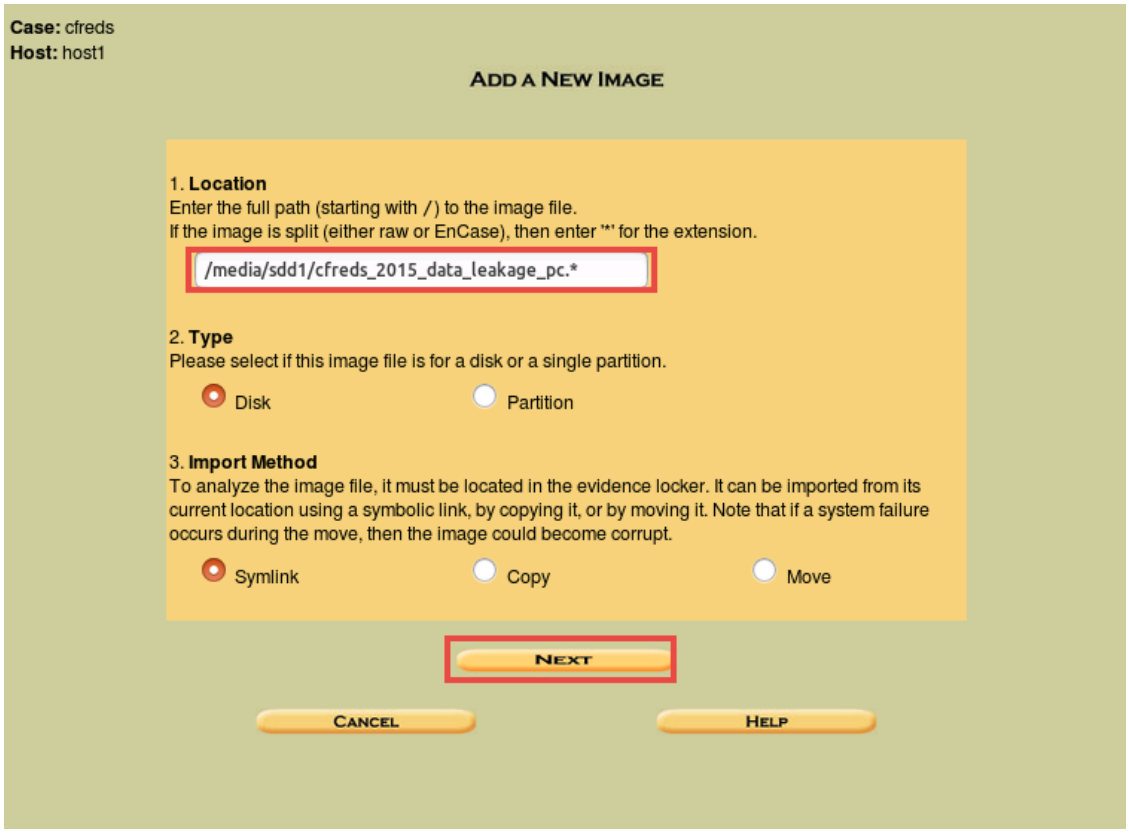
8. Once the information is entered, click **Add Host**.
9. On the *Adding Host* page, click **Add Image**.



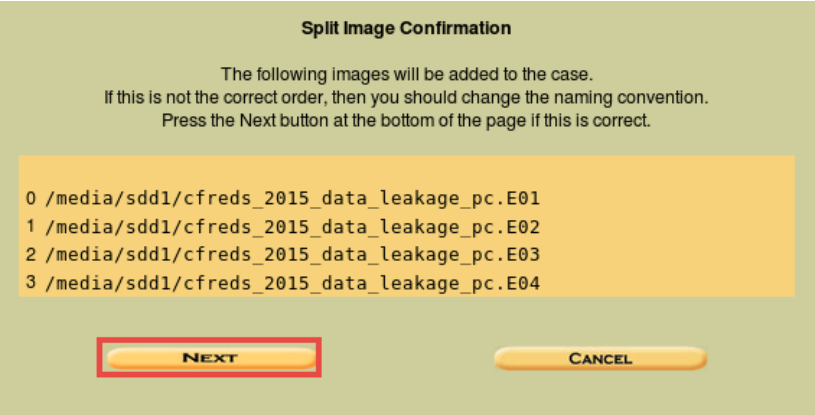
10. Once redirected, click on **Add Image File**.



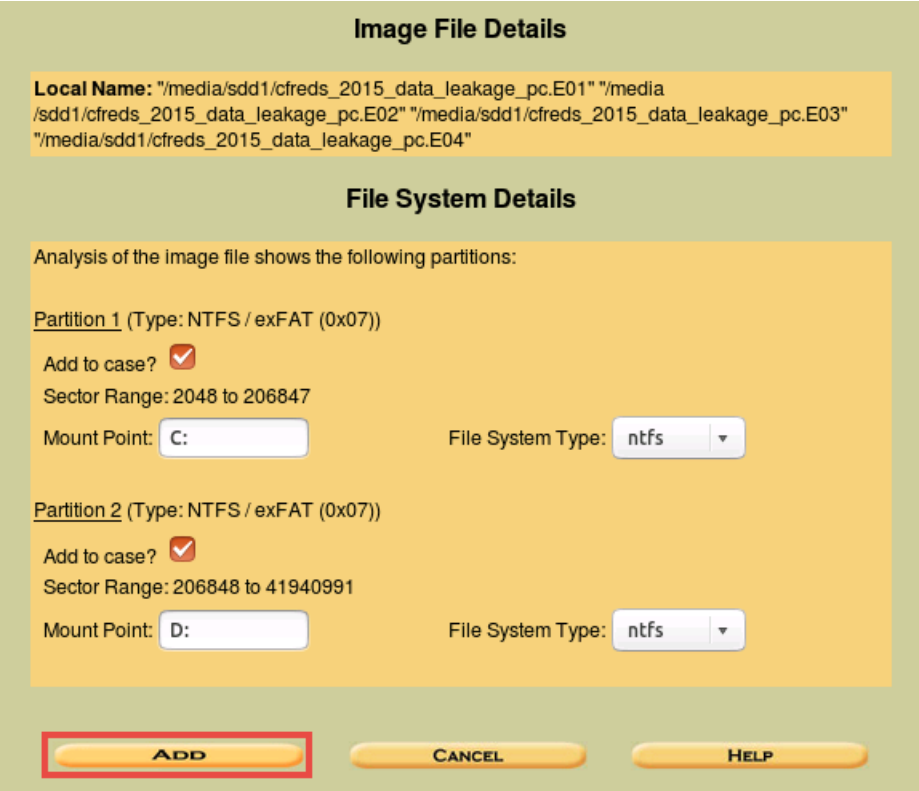
11. Type `/media/sdd1/cfreds_2015_data_leakage_pc.*` in the *Location* text field and click **Next**.



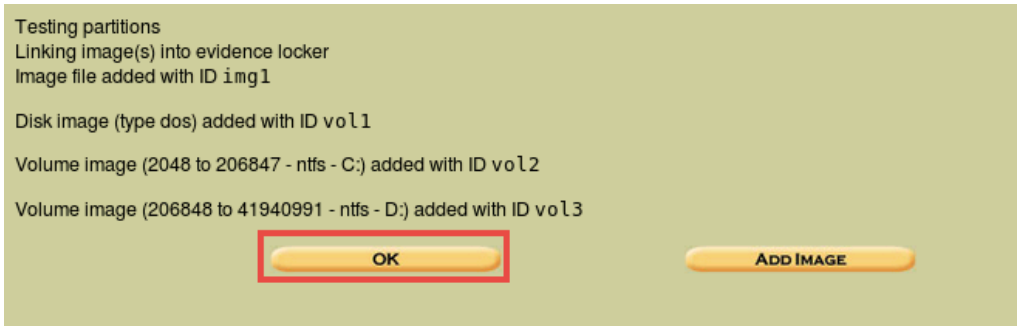
12. On the *Split Image Confirmation* page, notice the images that will be added to the case. Click **Next**.



13. On the *Image File and File System Details* page, leave the defaults and click **Add**.



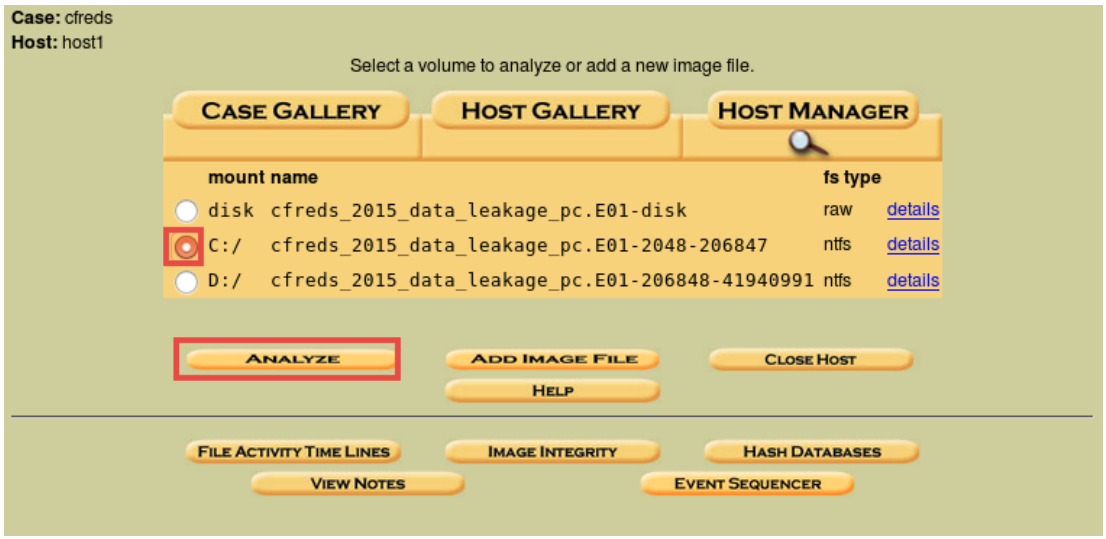
14. Click **OK** to confirm.



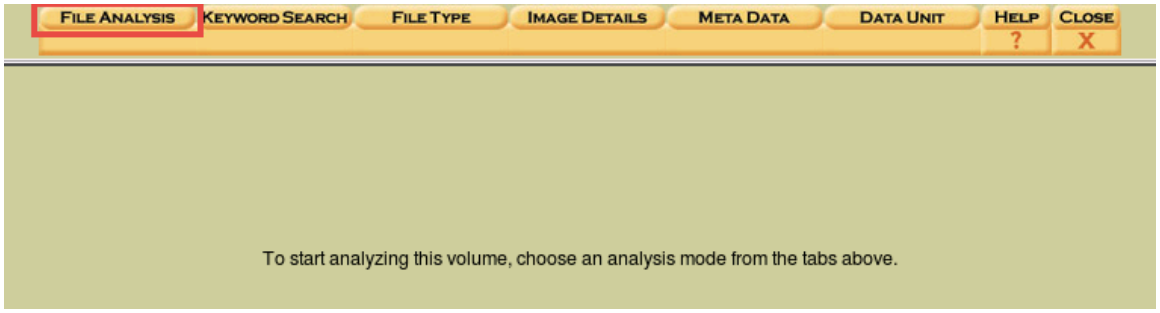
15. Leave the *Autopsy* application open to continue with the next task.

2 Analyzing Images with Autopsy

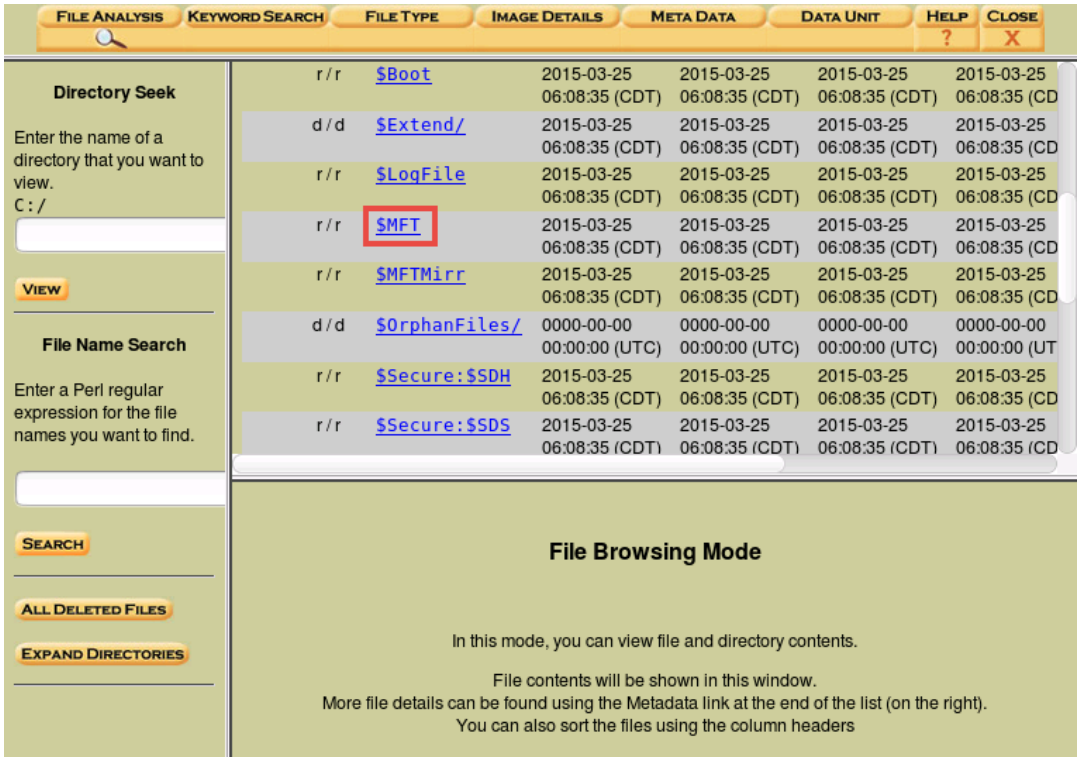
1. On the *Select a Volume* page, choose the **C:/** mount and click **Analyze**.



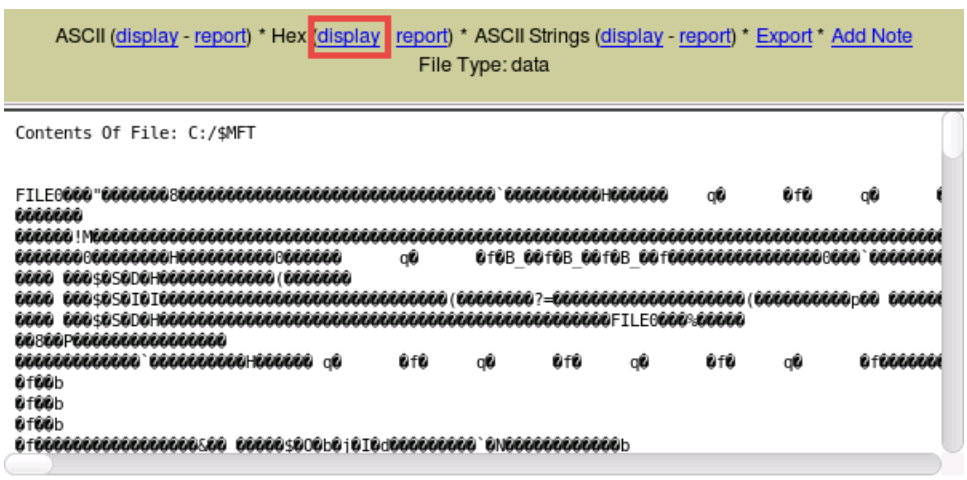
2. Click on **File Analysis** from the tabs in the top pane.



3. Notice the information now available from the boot drive. Any file can now be examined like the *MFT* table. Scroll down the list in the middle pane and click on the **$MFT** file entry.

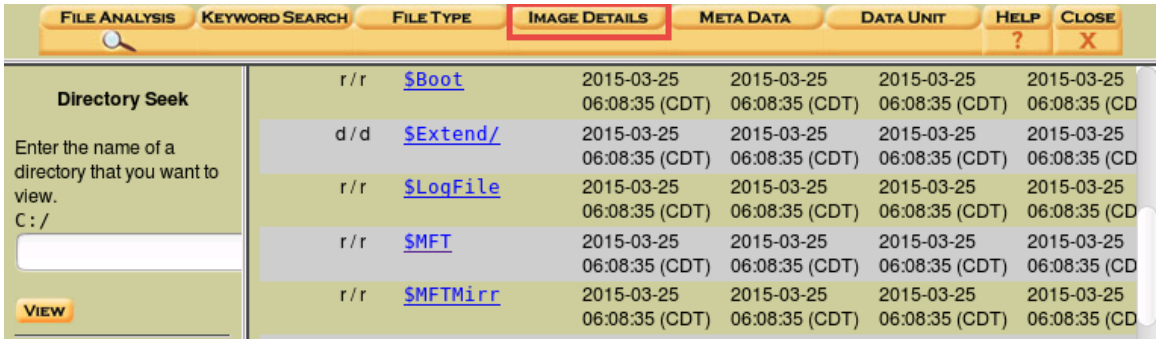


4. Click on the **display** link for *Hex* in the bottom pane.

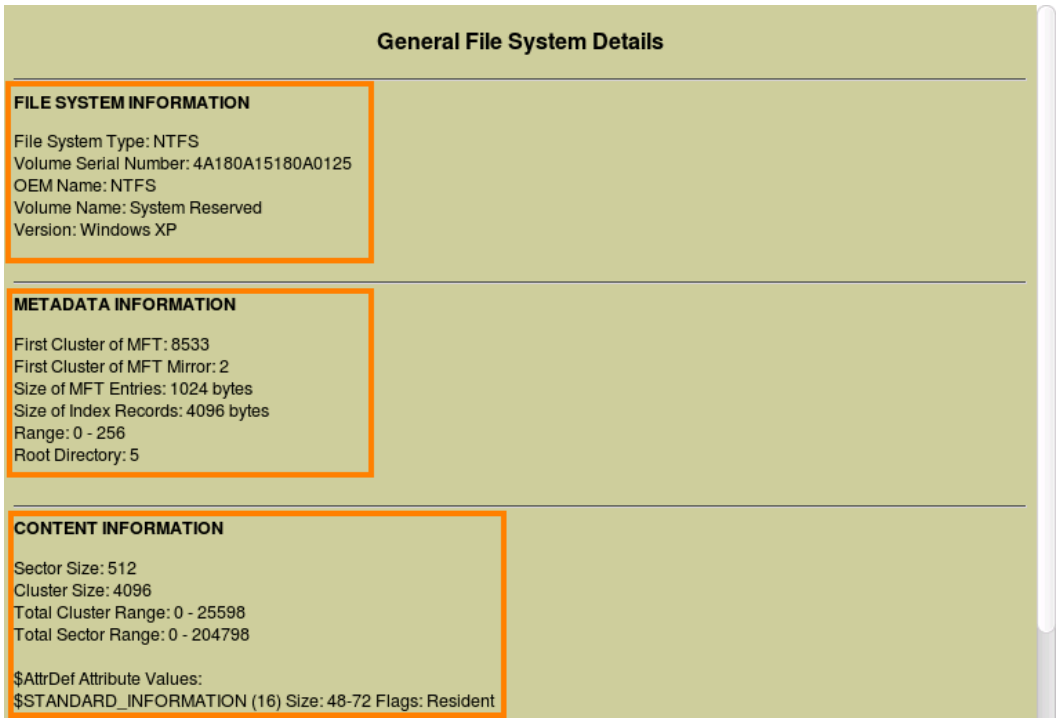


Notice the available Hex information about the *MFT* table.

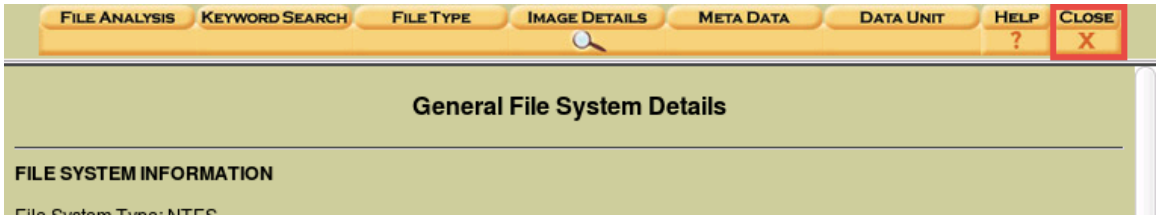
5. Click on **Image Details** from the tabs in the top pane.



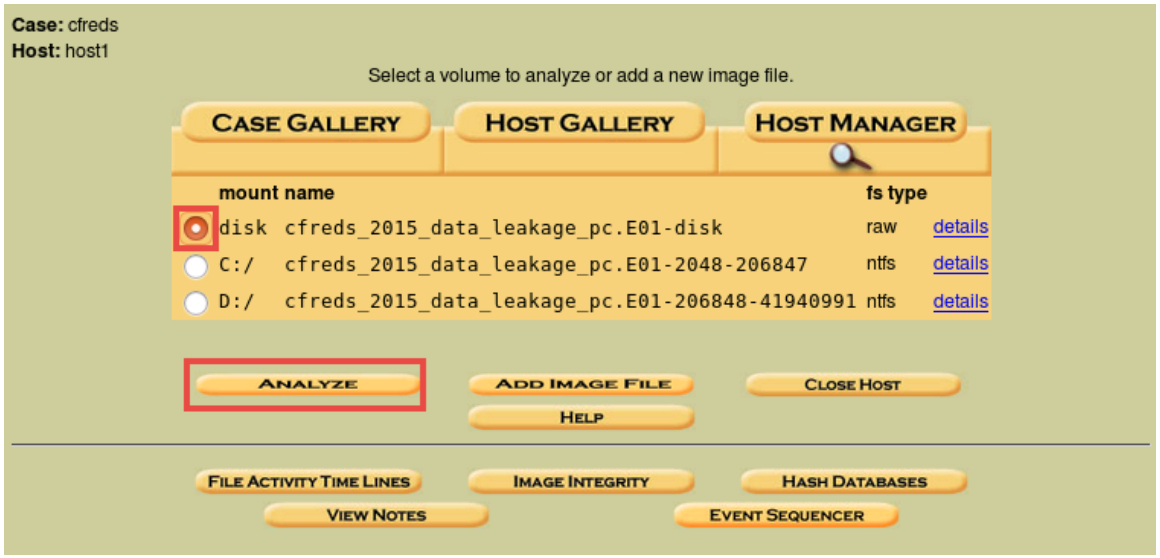
6. Notice the file system, metadata, and content information presented.



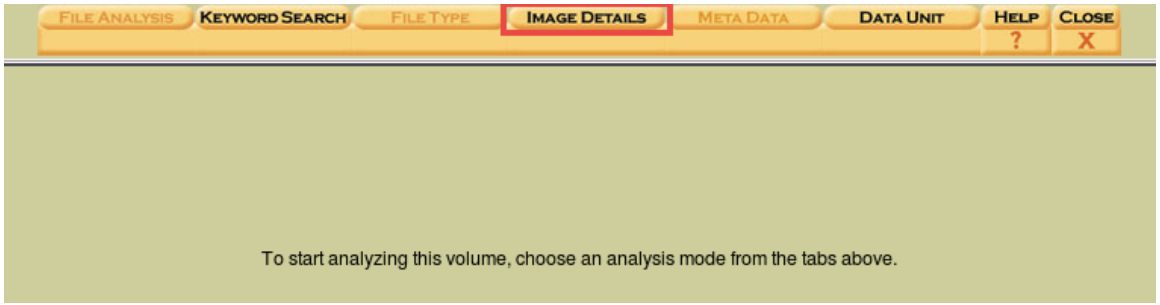
7. Click on **Close** from the tabs in the top pane.



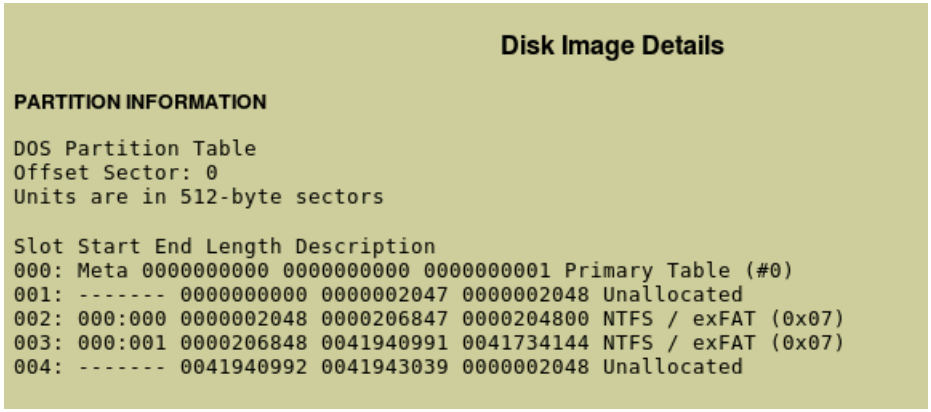
8. On the *Select a Volume* page, choose the **disk** mount and click **Analyze**.



9. Click on **Image Details** from the tabs in the top pane.



10. Notice the information given about the layout of the drive with two partitions listed.



11. Close all **PC Viewers** and end the reservation to complete the lab.

