



## **FORENSICS LAB SERIES**

### **Lab 11: Introduction to Autopsy**

**Document Version: 2016-08-17**

## Contents

Introduction .....	3
Objective .....	3
Pod Topology .....	4
Lab Settings .....	5
1 Creating & Adding Images to a Case .....	6
2 Analyzing Images with Autopsy .....	12

## Introduction

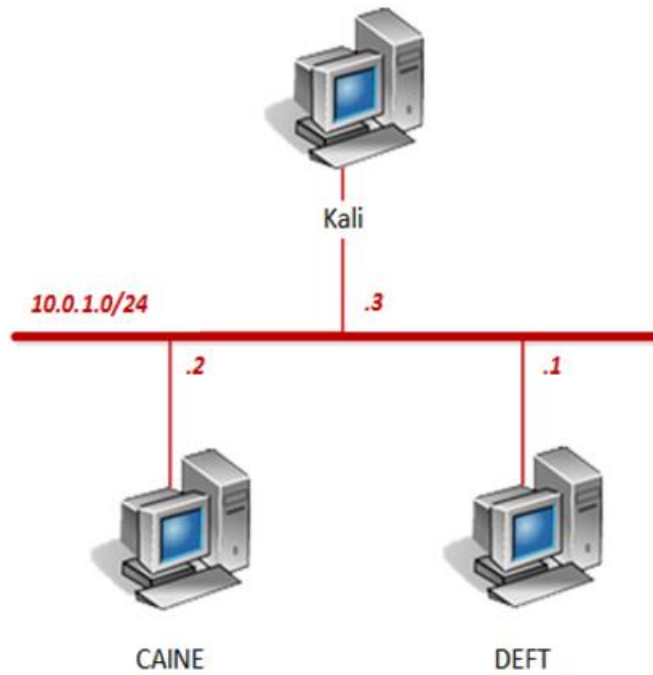
This lab will introduce a tool called Autopsy, which is an open source digital forensics platform and graphical interface to the Sleuth Kit developed by Brian Carrier. The basics of using the tool for performing a forensic investigation will be taught in this lab.

## 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



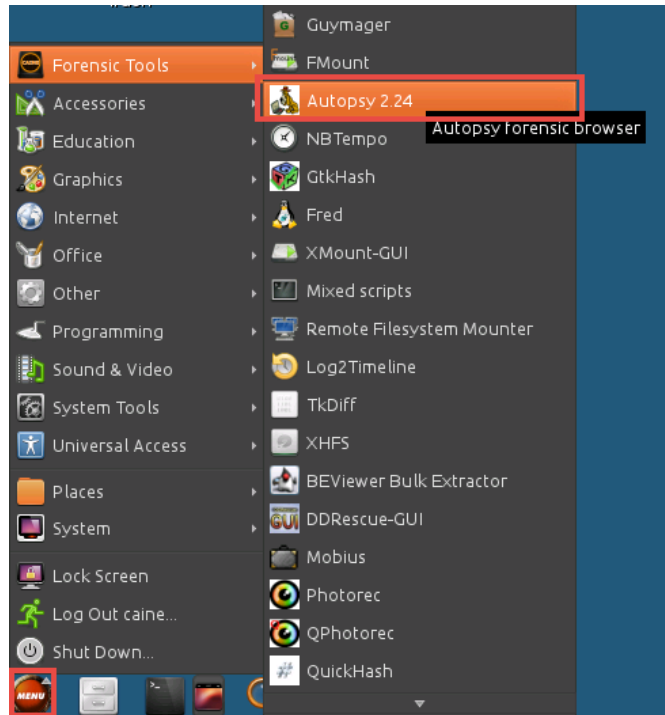
## Lab Settings

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.

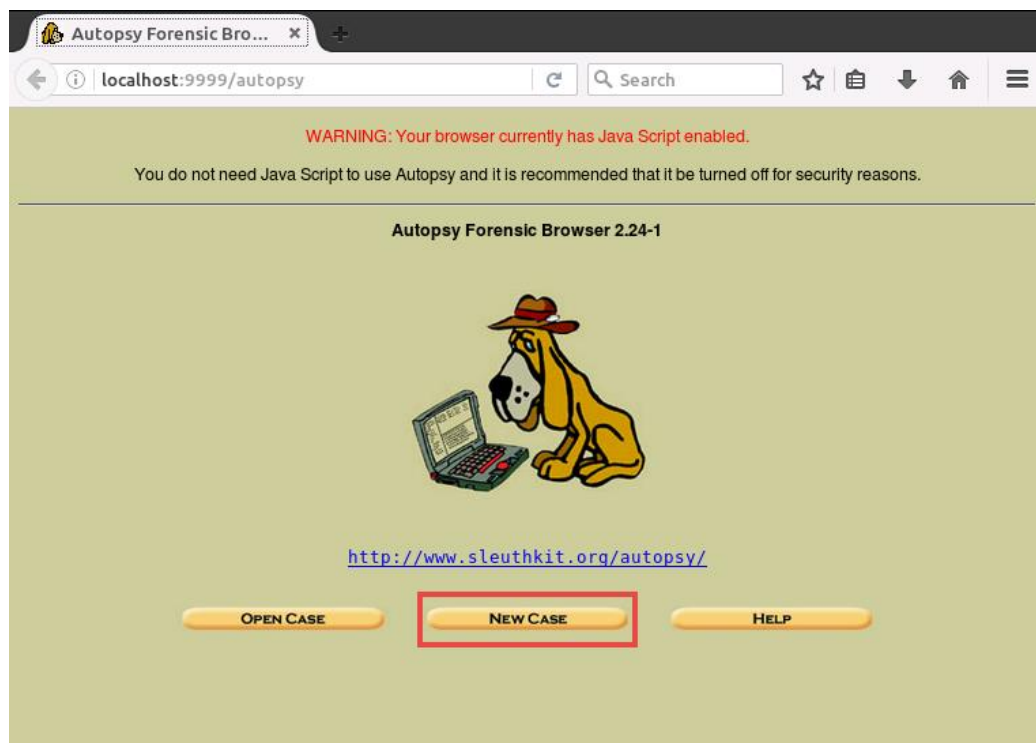
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

## 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"



**CREATE A NEW CASE**

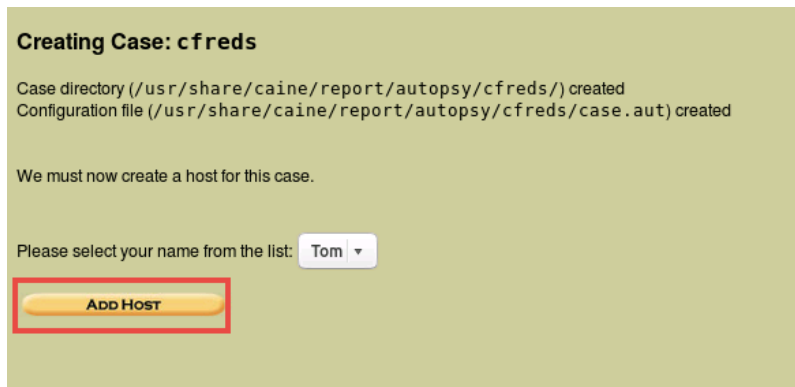
1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. <input type="text" value="Tom"/>	b. <input type="text"/>
c. <input type="text"/>	d. <input type="text"/>
e. <input type="text"/>	f. <input type="text"/>
g. <input type="text"/>	h. <input type="text"/>
i. <input type="text"/>	j. <input type="text"/>

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**.



**Creating Case: cfreds**

Case directory (/usr/share/caine/report/autopsy/cfreds/) created  
 Configuration file (/usr/share/caine/report/autopsy/cfreds/case.aut) created

We must now create a host for this case.

Please select your name from the list:

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**

Case: cfreds

### ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
2. **Description:** An optional one-line description or note about this computer.
3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
5. **Path of Alert Hash Database:** An optional hash database of known bad files.
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

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

### Adding host: host1 to case cfreds

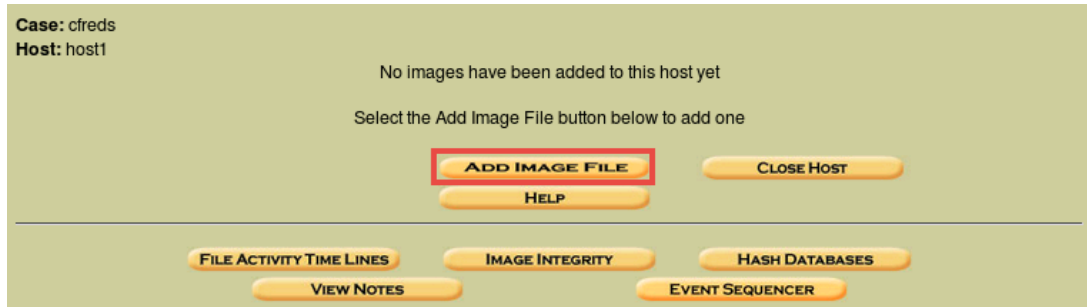
Host Directory (/usr/share/caine/report/autopsy/cfreds/host1/) created

Configuration file (/usr/share/caine/report/autopsy/cfreds/host1/host.aut) created

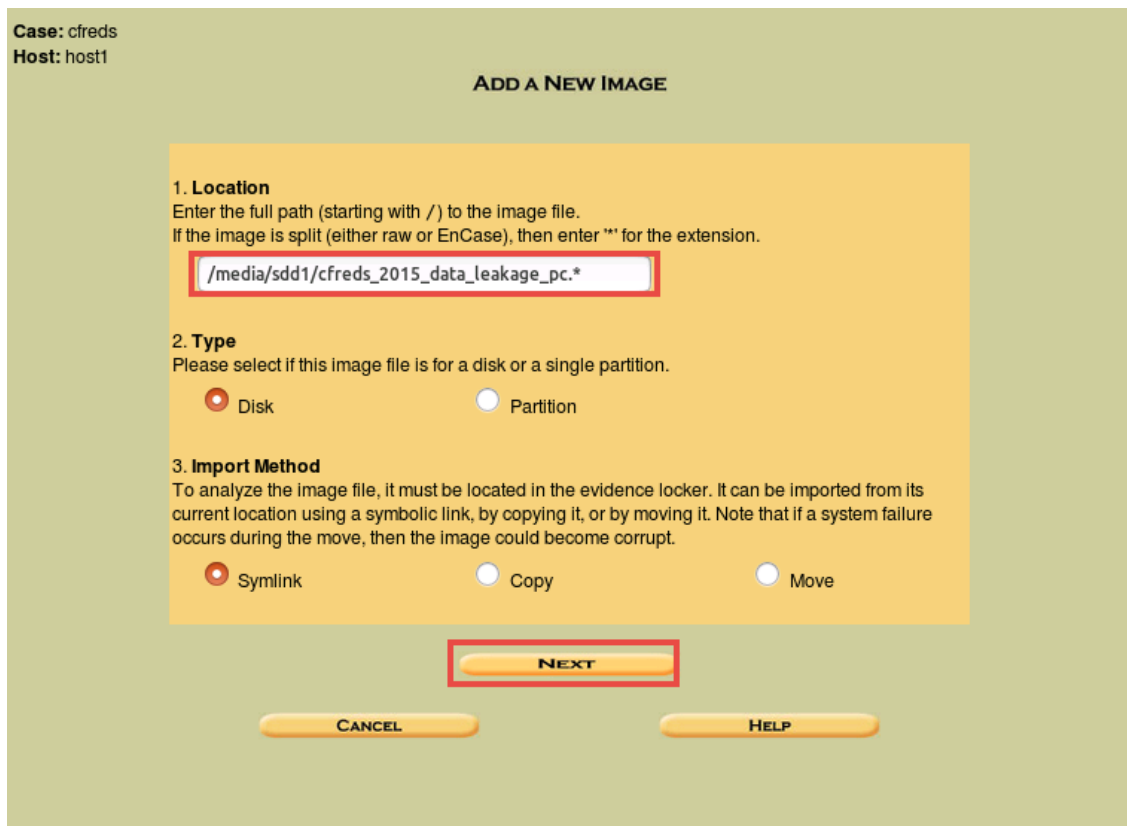
We must now import an image file for this host



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**.

**Split Image Confirmation**

The following images will be added to the case.  
If this is not the correct order, then you should change the naming convention.  
Press the Next button at the bottom of the page if this is correct.

```
0 /media/sdd1/cfreds_2015_data_leakage_pc.E01
1 /media/sdd1/cfreds_2015_data_leakage_pc.E02
2 /media/sdd1/cfreds_2015_data_leakage_pc.E03
3 /media/sdd1/cfreds_2015_data_leakage_pc.E04
```

NEXT
CANCEL

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

**Image File Details**

**Local Name:** "/media/sdd1/cfreds\_2015\_data\_leakage\_pc.E01" "/media/sdd1/cfreds\_2015\_data\_leakage\_pc.E02" "/media/sdd1/cfreds\_2015\_data\_leakage\_pc.E03" "/media/sdd1/cfreds\_2015\_data\_leakage\_pc.E04"

**File System Details**

Analysis of the image file shows the following partitions:

Partition 1 (Type: NTFS / exFAT (0x07))

Add to case? ☒

Sector Range: 2048 to 206847

Mount Point:  File System Type: ntfs

Partition 2 (Type: NTFS / exFAT (0x07))

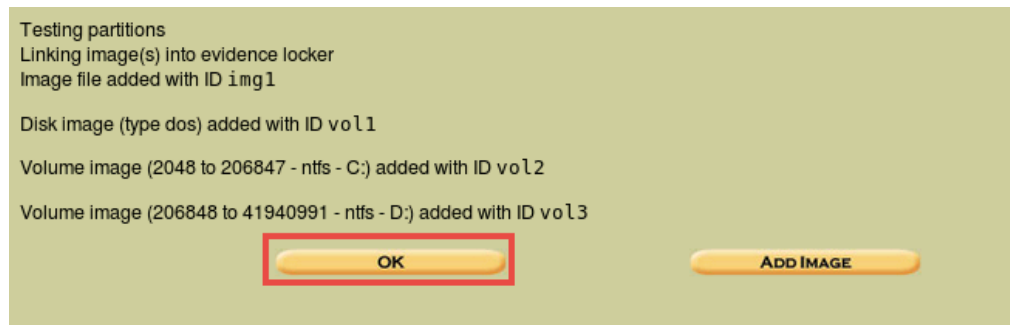
Add to case? ☒

Sector Range: 206848 to 41940991

Mount Point:  File System Type: ntfs

ADD
CANCEL
HELP

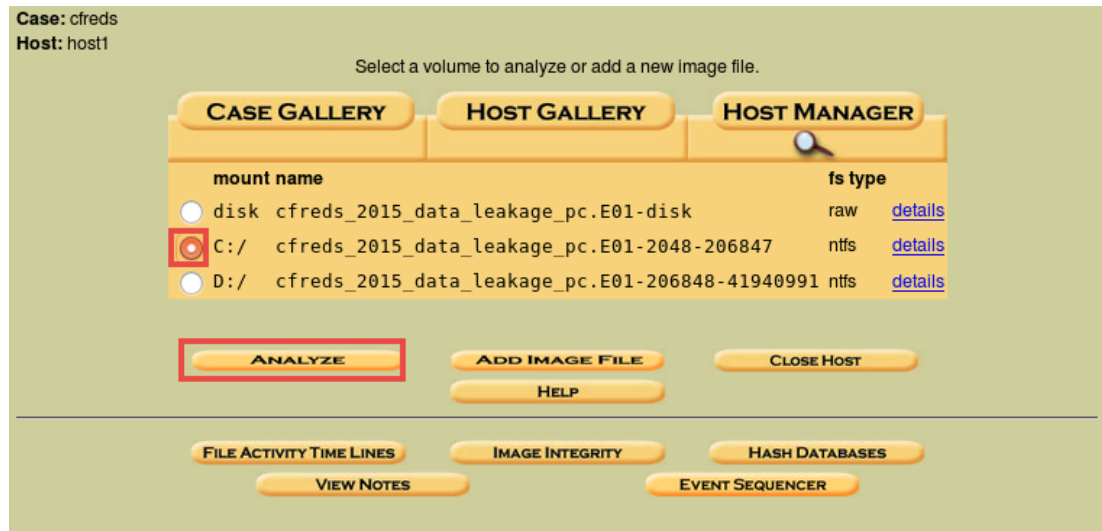
14. Click **OK** to confirm.



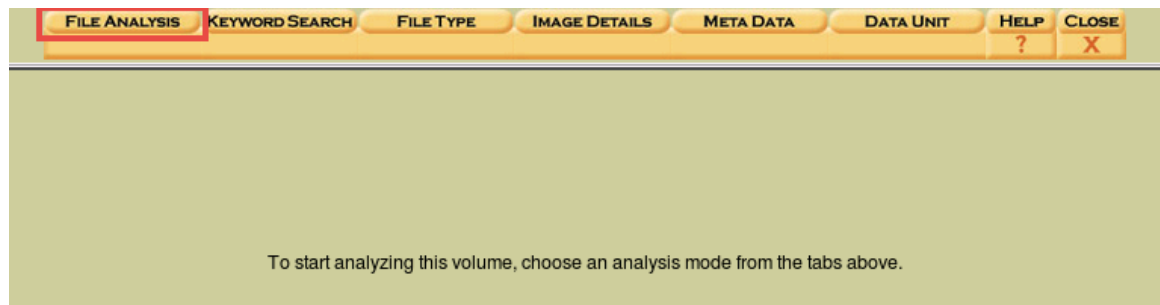
15. Leave the *Autopsy* application open to continue with the next task.

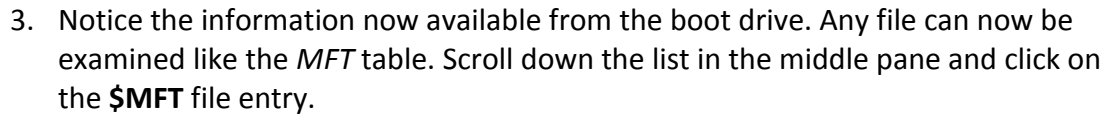
## 2 Analyzing Images with Autopsy

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

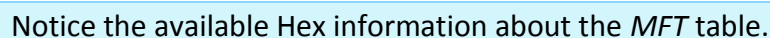


2. Click on **File Analysis** from the tabs in the top pane.





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



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

FILE ANALYSIS	KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP	CLOSE																																								
<div> <div> Directory Seek  Enter the name of a directory that you want to view.  C: /  <input type="text"/>  VIEW </div> <table> <tr> <td>r / r</td><td><a href="#">\$Boot</a></td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td></tr> <tr> <td>d / d</td><td><a href="#">\$Extend/</a></td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td></tr> <tr> <td>r / r</td><td><a href="#">\$LogFile</a></td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td></tr> <tr> <td>r / r</td><td><a href="#">\$MFT</a></td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td></tr> <tr> <td>r / r</td><td><a href="#">\$MFTMirr</a></td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td><td>2015-03-25 06:08:35 (CDT)</td></tr> </table> </div>								r / r	<a href="#">\$Boot</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	d / d	<a href="#">\$Extend/</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	r / r	<a href="#">\$LogFile</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	r / r	<a href="#">\$MFT</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	r / r	<a href="#">\$MFTMirr</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)
r / r	<a href="#">\$Boot</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)																																								
d / d	<a href="#">\$Extend/</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)																																								
r / r	<a href="#">\$LogFile</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)																																								
r / r	<a href="#">\$MFT</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)																																								
r / r	<a href="#">\$MFTMirr</a>	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)	2015-03-25 06:08:35 (CDT)																																								



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

### General File System Details

#### FILE SYSTEM INFORMATION

File System Type: NTFS  
Volume Serial Number: 4A180A15180A0125  
OEM Name: NTFS  
Volume Name: System Reserved  
Version: Windows XP

#### METADATA INFORMATION

First Cluster of MFT: 8533  
First Cluster of MFT Mirror: 2  
Size of MFT Entries: 1024 bytes  
Size of Index Records: 4096 bytes  
Range: 0 - 256  
Root Directory: 5

#### CONTENT INFORMATION

Sector Size: 512  
Cluster Size: 4096  
Total Cluster Range: 0 - 25598  
Total Sector Range: 0 - 204798  
\$AttrDef Attribute Values:  
\$STANDARD\_INFORMATION (16) Size: 48-72 Flags: Resident

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

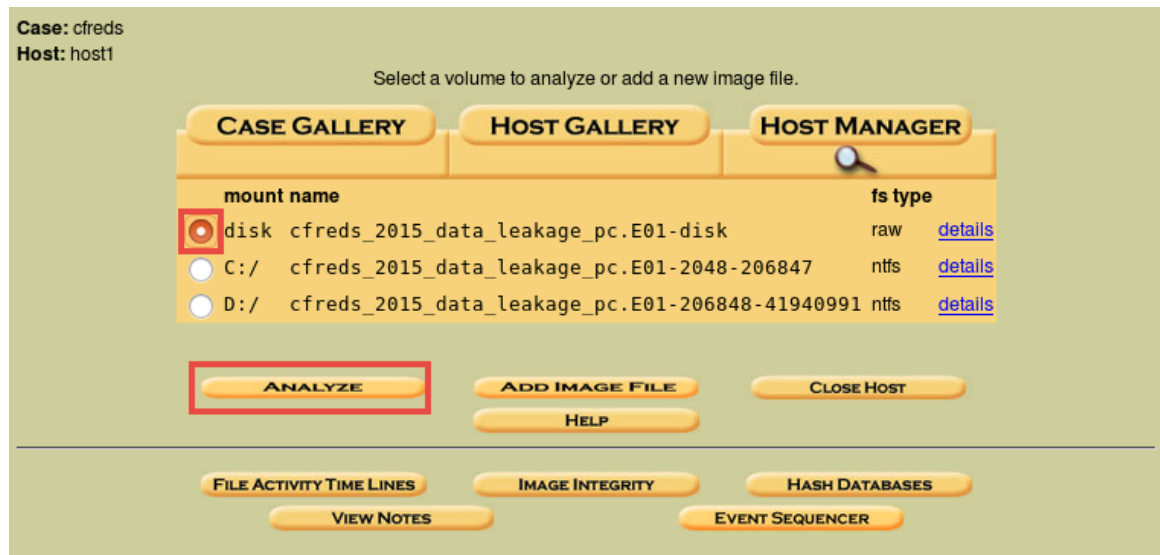
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE

### General File System Details

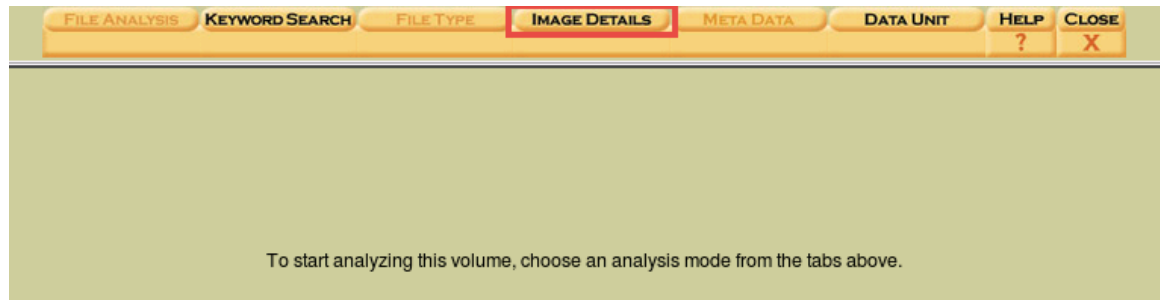
#### FILE SYSTEM INFORMATION

File System Type: NTFS

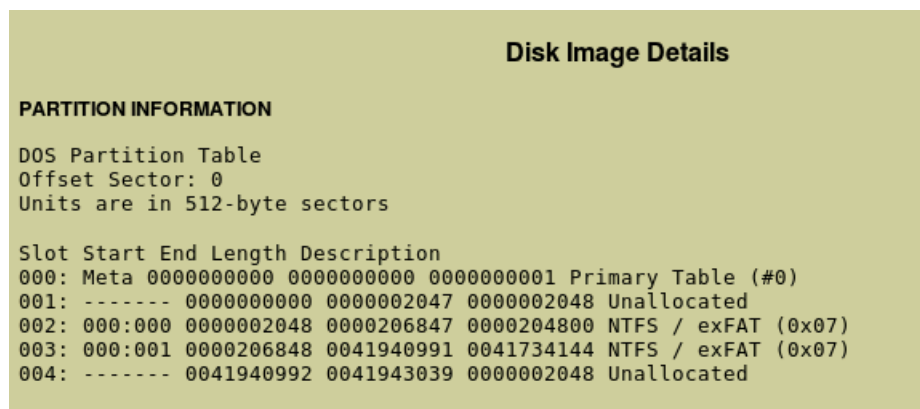
8. On the *Select a Volume* page, choose the **disk** mount and click **Analyze**.



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.