



## DIGITAL FORENSICS LAB SERIES

### Lab 7: Introduction to the Autopsy Forensic Browser

**Objective: Evidence Acquisition, Preparation and Preservation**

**Document Version: 2015-09-28**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

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.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

## Contents

Introduction .....	3
Objective: Evidence Acquisition, Preparation and Preservation .....	3
Lab Topology .....	4
Lab Settings .....	5
1 Installing the Autopsy Forensic Browser .....	6
1.1 Installing Autopsy on Windows.....	6
1.2 Conclusion .....	10
1.3 Discussion Questions.....	10
2 Creating a Case in Autopsy Forensic Browser .....	11
2.1 Starting a Case within Autopsy .....	11
2.2 Conclusion .....	15
2.3 Discussion Questions.....	15
3 Examining an Image with Autopsy.....	16
3.1 Navigation within Autopsy .....	16
3.2 Conclusion .....	23
3.3 Discussion Questions.....	23
4 Report Generation .....	24
4.1 Using the Autopsy Report Generator.....	24
4.2 Conclusion .....	29
4.3 Discussion Questions.....	29
References .....	30



## Introduction

This lab includes the following tasks:

1. Installing the Autopsy Forensic Browser
2. Creating a case in Autopsy Forensic Browser
3. Examining an Image with Autopsy
4. Generating a Report

## Objective: Evidence Acquisition, Preparation and Preservation

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 understanding of evidence chain-of-custody and integrity, E-discovery concepts, evidence acquisition and preservation, and the tools and techniques used by computer forensic examiners.*

This lab introduces the basic functionality of the Autopsy Forensic Browser, a graphical interface to The Sleuth Kit and other open source tools. Investigators use this tool to examine disk images. The investigator creates a case, examines the files in the case, and then generates a report of the items found.

**Autopsy** - The open source digital investigation tool (digital forensic tool), Autopsy, runs on Windows, Linux, OS X, and other UNIX systems. Autopsy can be used to analyze disk images and perform in-depth analysis of file systems, such as NTFS and FAT.

**Bookmark** – Within a case, relevant items can be designated important or bookmarked

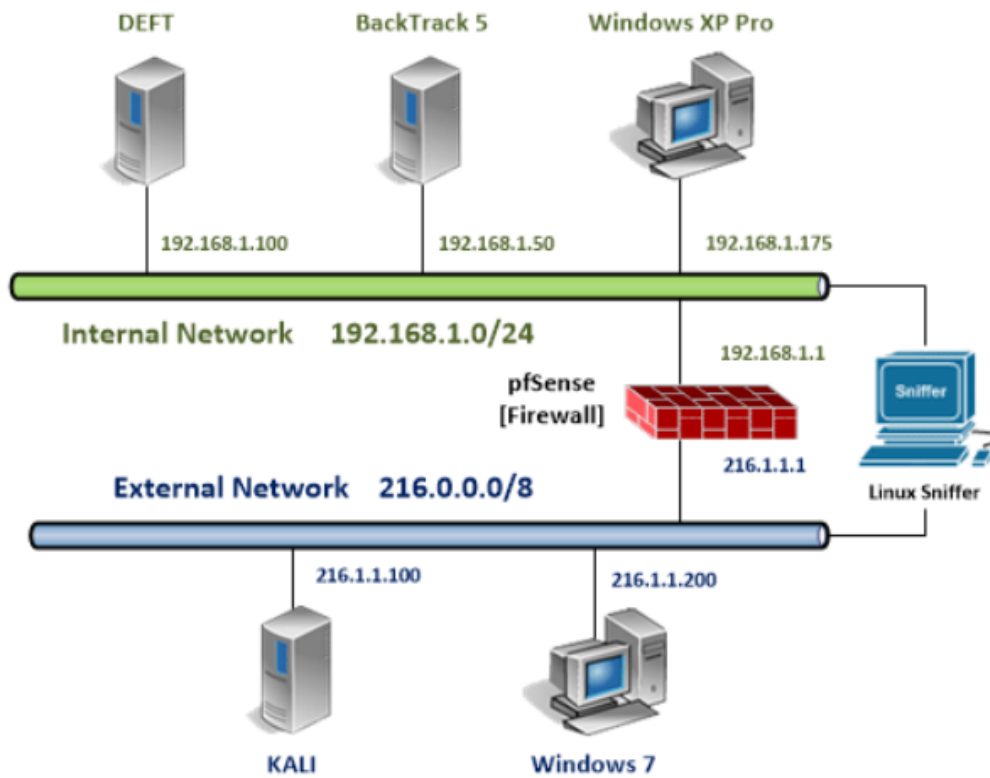
**Forensic Report** – Forensic software such as FTK, EnCase, and Autopsy allow examiners to generate forensic reports, which contain relevant bookmarks of important artifacts.

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

**E01 File**– A proprietary imaging format developed by Guidance Software (the makers of EnCase). This image format is supported by other tools, such as FTK, PTK, and Autopsy.



## 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)
Windows 7 External Machine	216.1.1.200	student	password



## 1 Installing the Autopsy Forensic Browser

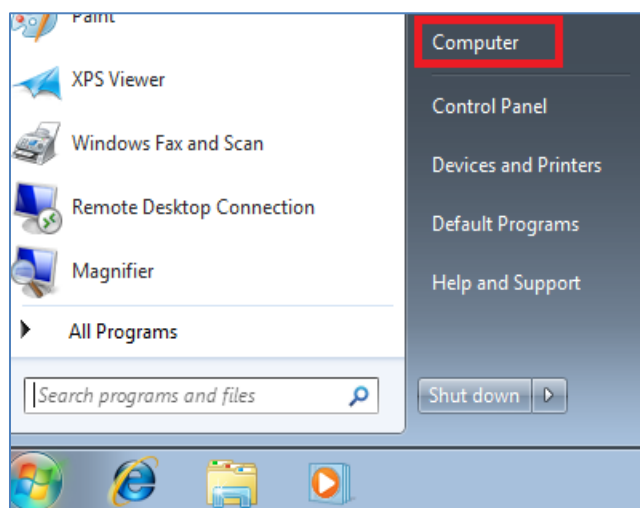
Computer forensic software can be very costly for a company or organization. There are not a lot of options for free forensic suites, but Autopsy is one of them. It runs on Linux and Microsoft Windows operating systems. Autopsy was developed by Brian Carrier, and utilizes the command line tools of The Sleuth Kit (TSK) underneath the hood.

### 1.1 Installing Autopsy on Windows

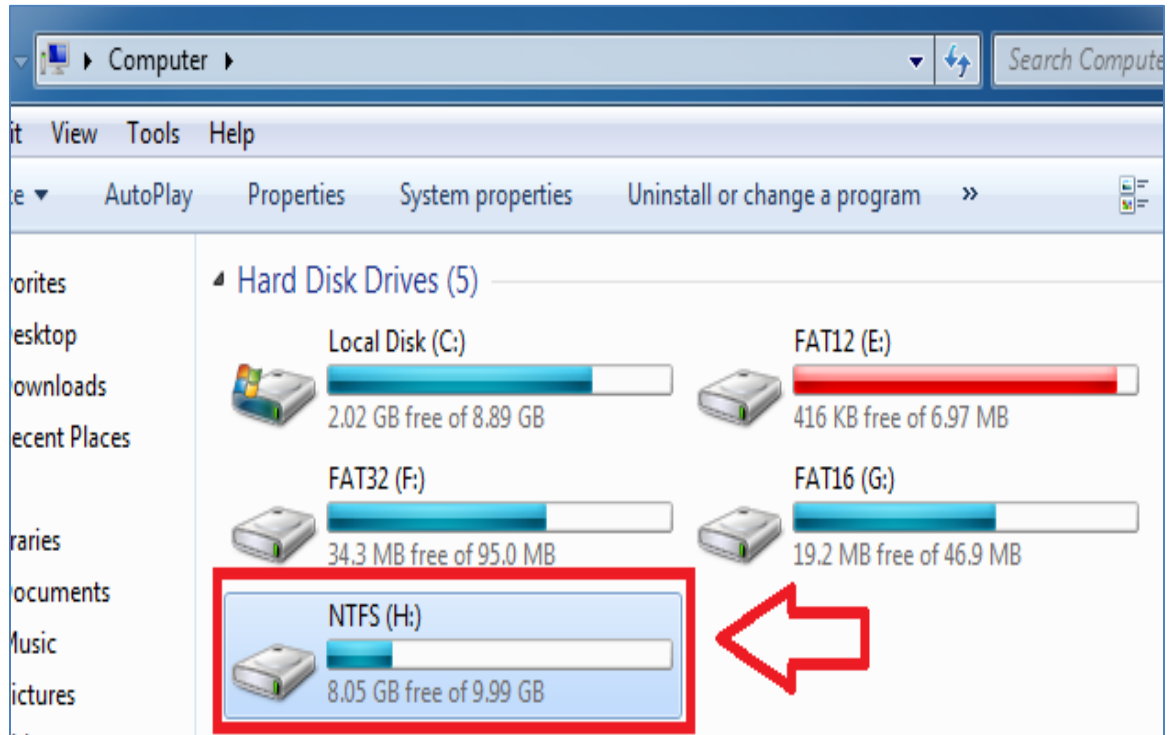
1. Log on to the **Windows 7 Machine** on the External Network by clicking on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password**, and press **enter** to log in.



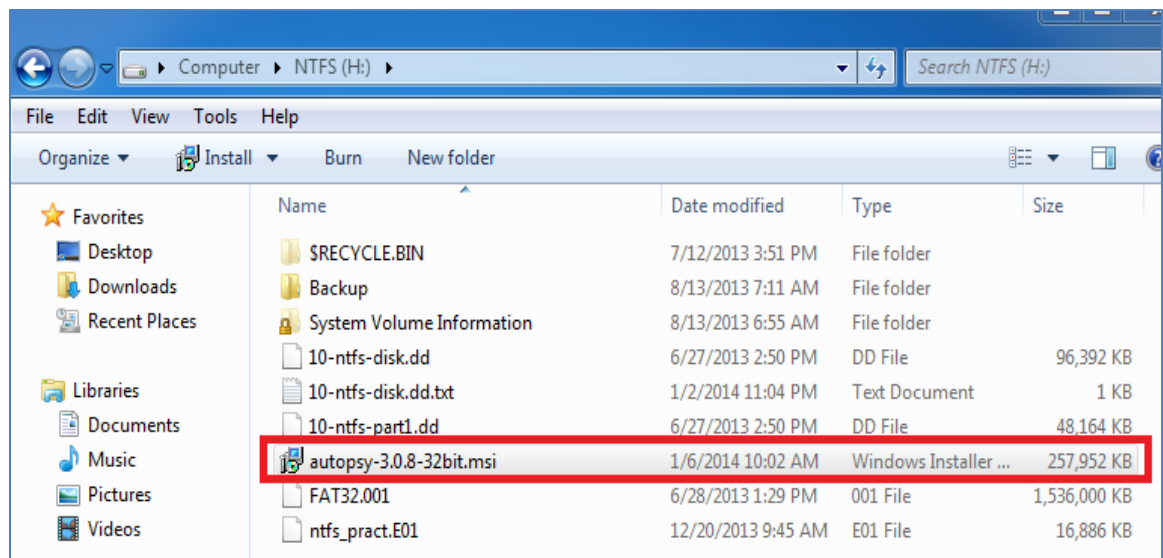
4. Click the Start icon in the lower-left corner and then select **Computer**.



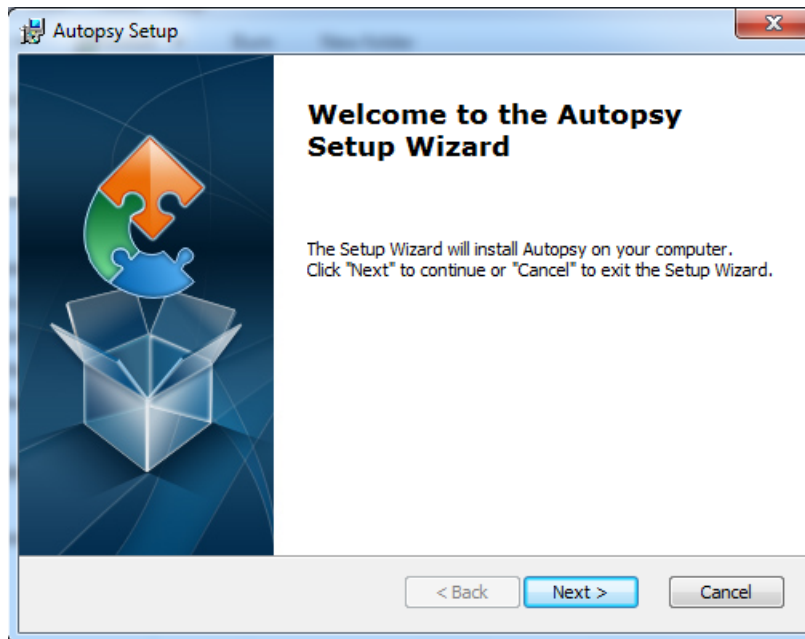
- Double-click on the **(NTFS) H:** drive within Computer.



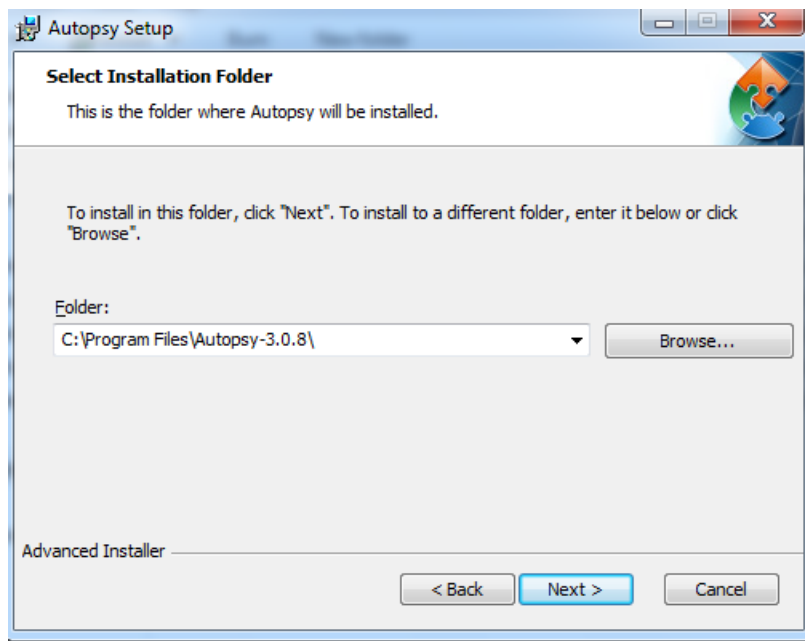
- Double-click on the **autopsy-3.0.8-32bit.msi** file to install Autopsy.



- Click **Next** at the Welcome to the Autopsy Setup Wizard.

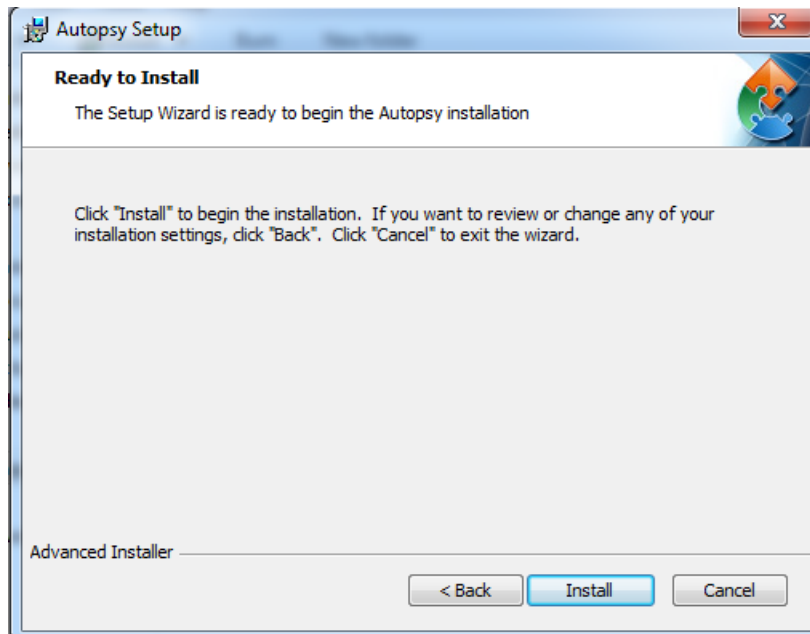


- Accept the default for the installation directory and click **Next**.

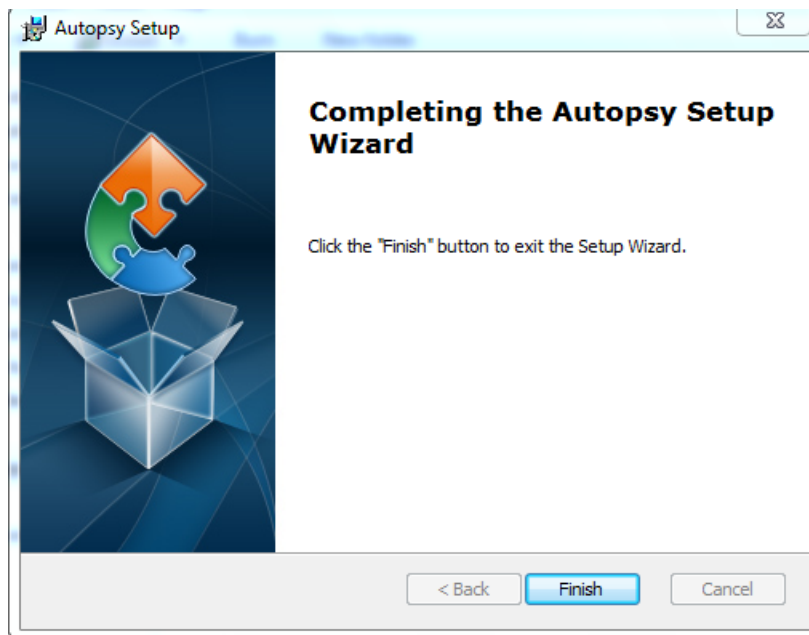




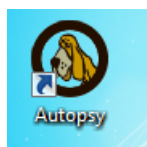
9. At the Ready to Install screen, click **Install**.



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



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



12. A window with a dog should eventually appear with the message, *Starting modules.*



## 1.2 Conclusion

The Autopsy forensic browser is a free forensic analysis platform that runs on Linux and Windows operating systems. The software utilizes The Sleuth Kit, and was developed by Brian Carrier.

## 1.3 Discussion Questions

1. What operating systems will Autopsy run on?
2. Name the command line tools that Autopsy utilizes.
3. What makes the Autopsy forensic browser a good choice for analysis?
4. Who developed the Autopsy forensic browser?

## 2 Creating a Case in Autopsy Forensic Browser

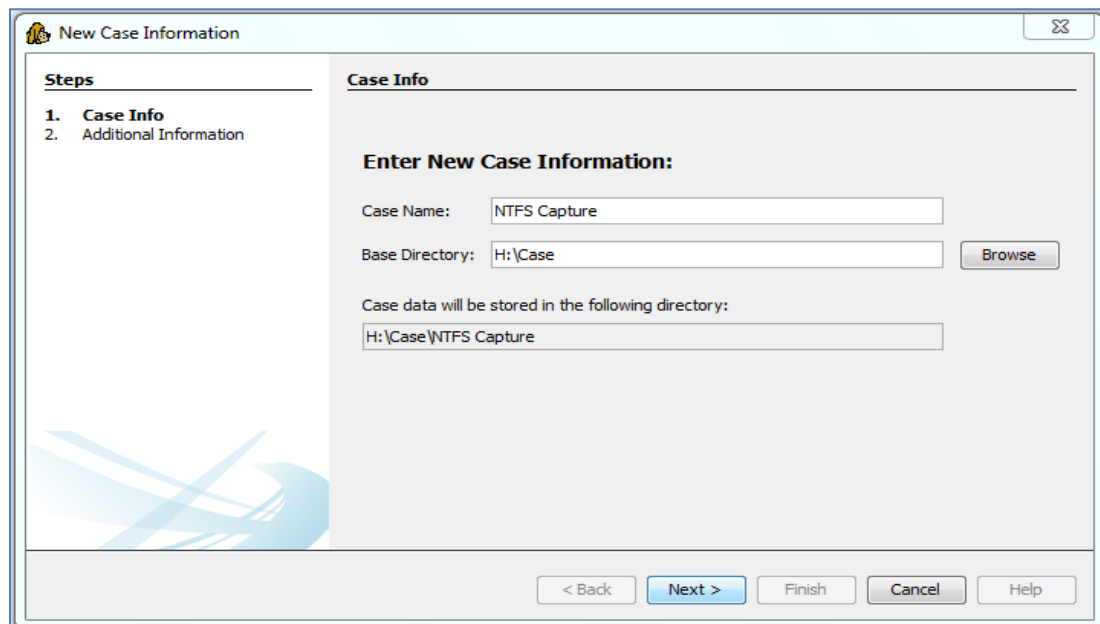
The first step, when using most computer forensic software, is to start a new case. The case will include information about the investigator as well as items like DD or E01 images.

### 2.1 Starting a Case within Autopsy

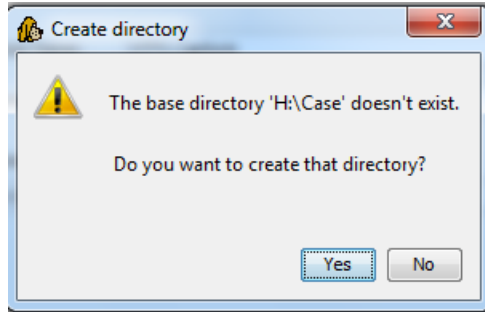
1. Click the Autopsy icon on your desktop. Click on **Create New Case**.



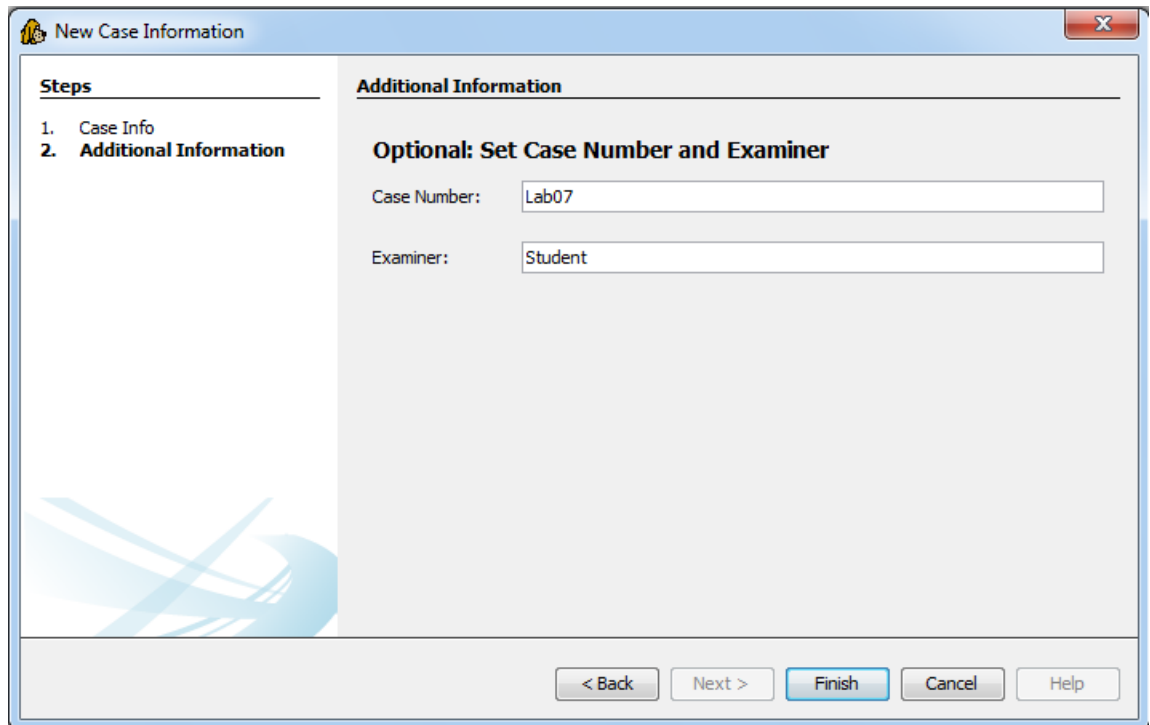
2. Name your case **NTFS Capture**. For the Base Directory, type **H:\Case**. Click **Next**.



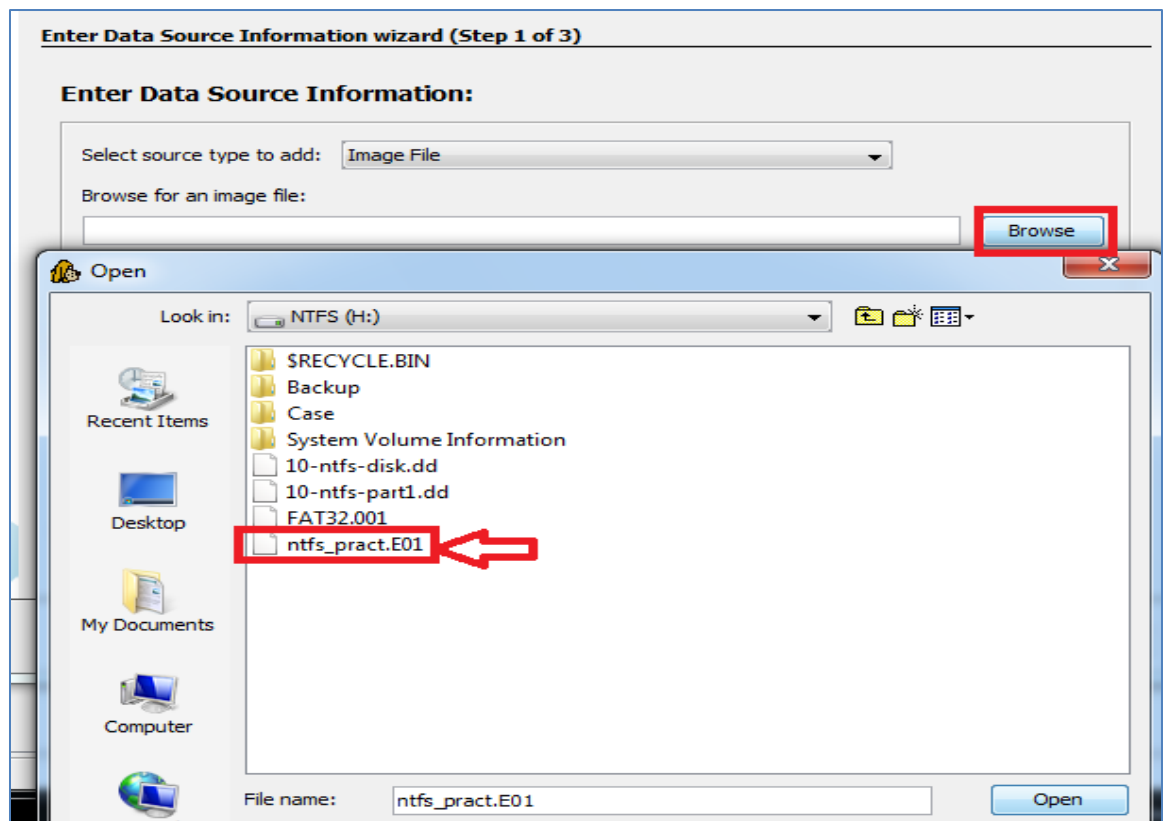
3. Click **Yes** to creating the directory H:\Case.



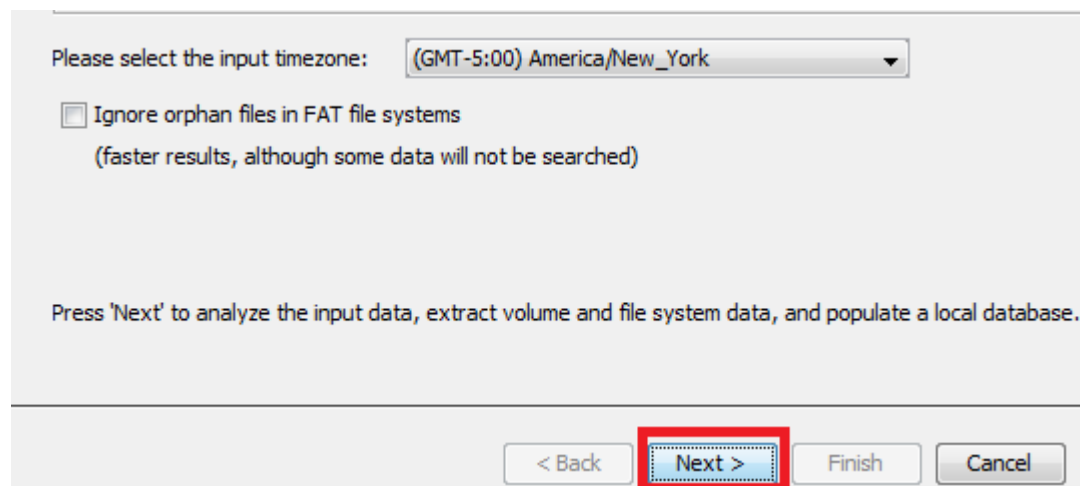
4. Enter **Lab07** as the Case Number and **Student** in the Examiner field. Click **Finish**.



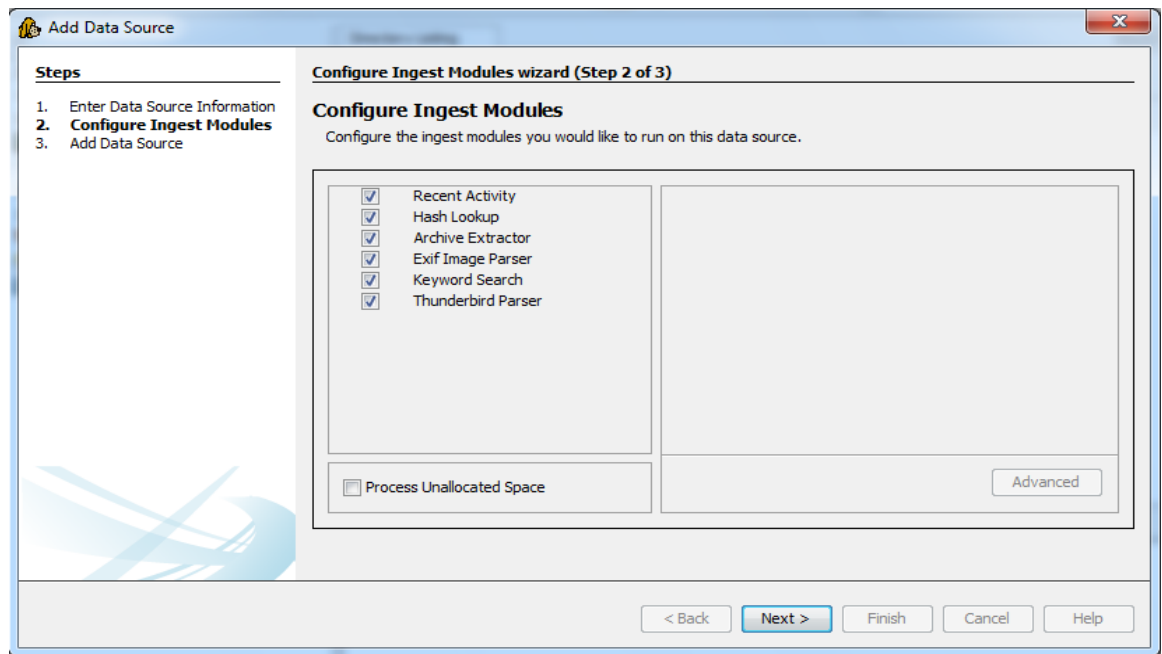
5. In the **Add Data Source** window, select **Image File** from the **Select Input type to add** drop-down. Click on **Browse** to find the image file on H: called **ntfs\_pract.E01** and click Open. This file is a hard disk image in the Encase Forensic Image format.



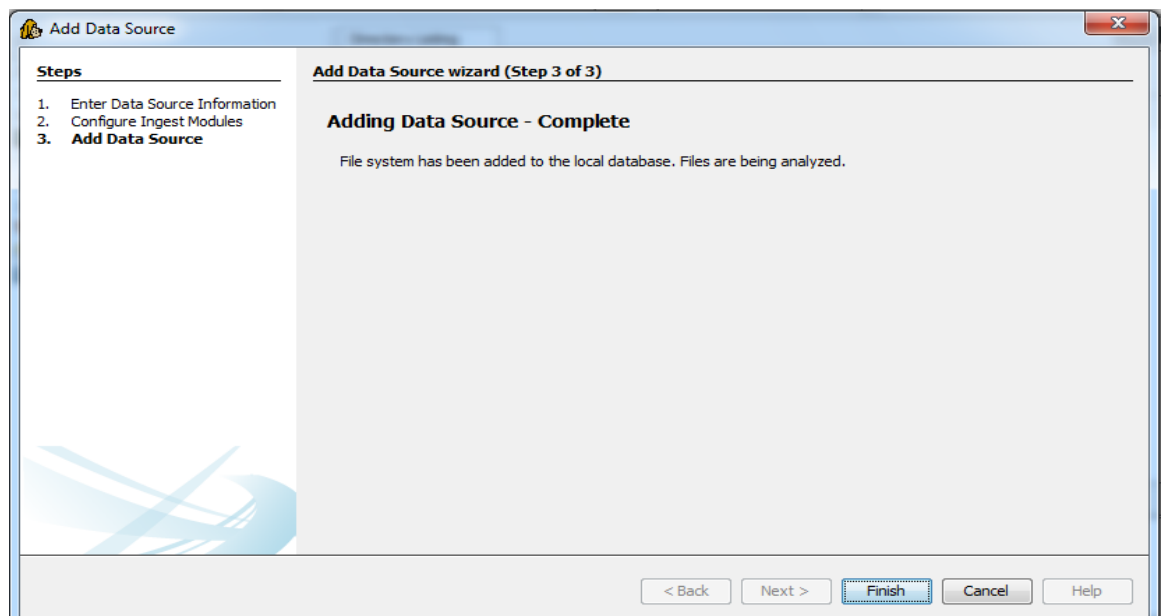
6. Leave the image timezone as (GMT-5:00) America/New York. Click **Next**.



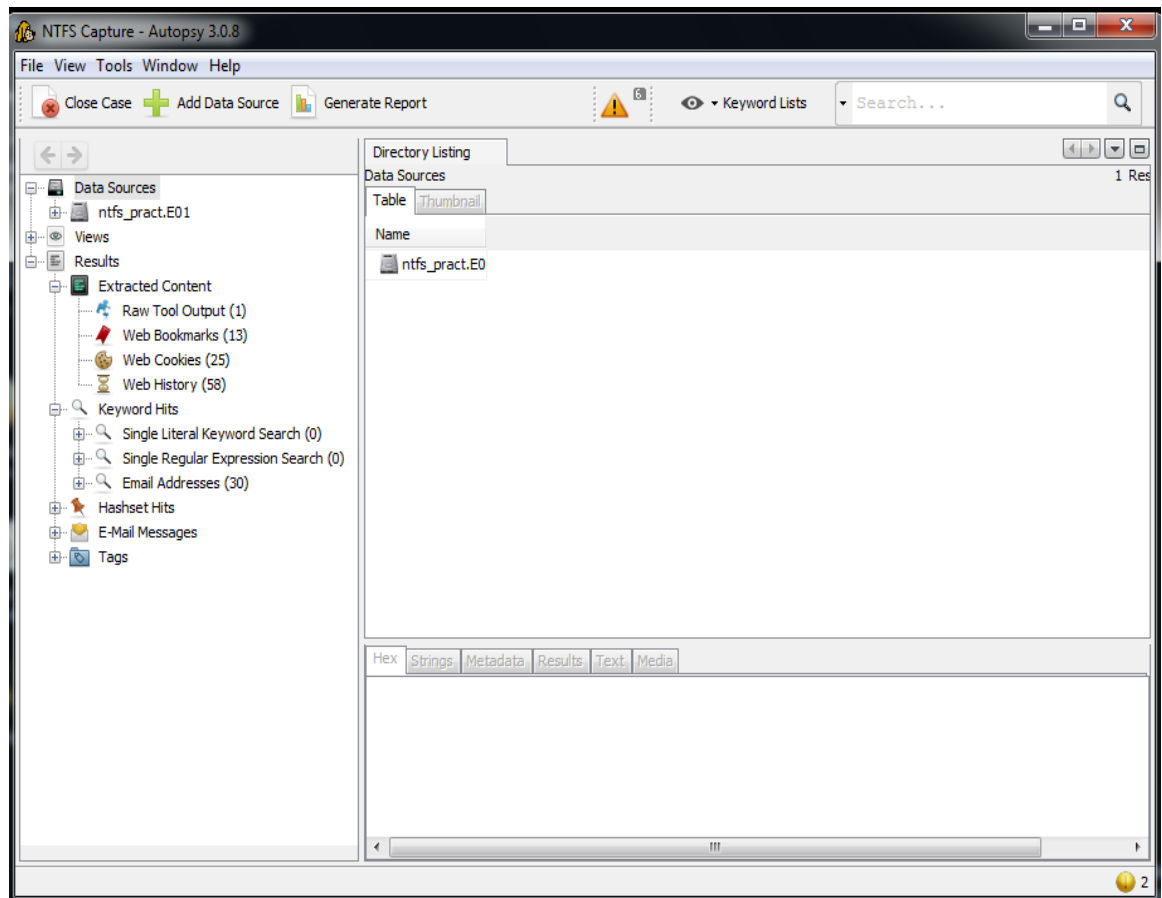
7. Leave all the boxes checked. This will allow different built-in modules in Autopsy to extract files from the image. Click **Next**.



8. The tool will begin processing. Click **Finish**.



9. You have created your first case. Keep the window open, you will continue to use it in the next task.



## 2.2 Conclusion

Starting a new case is typically the first step when using computer forensic software. A case will have information about the investigator as well as items like DD or E01 images. An E01 file is an image in the Encase Forensic Image format. This image can be loaded into a variety of forensic tools including FTK, PTK, and the Autopsy Forensic Browser.

## 2.3 Discussion Questions

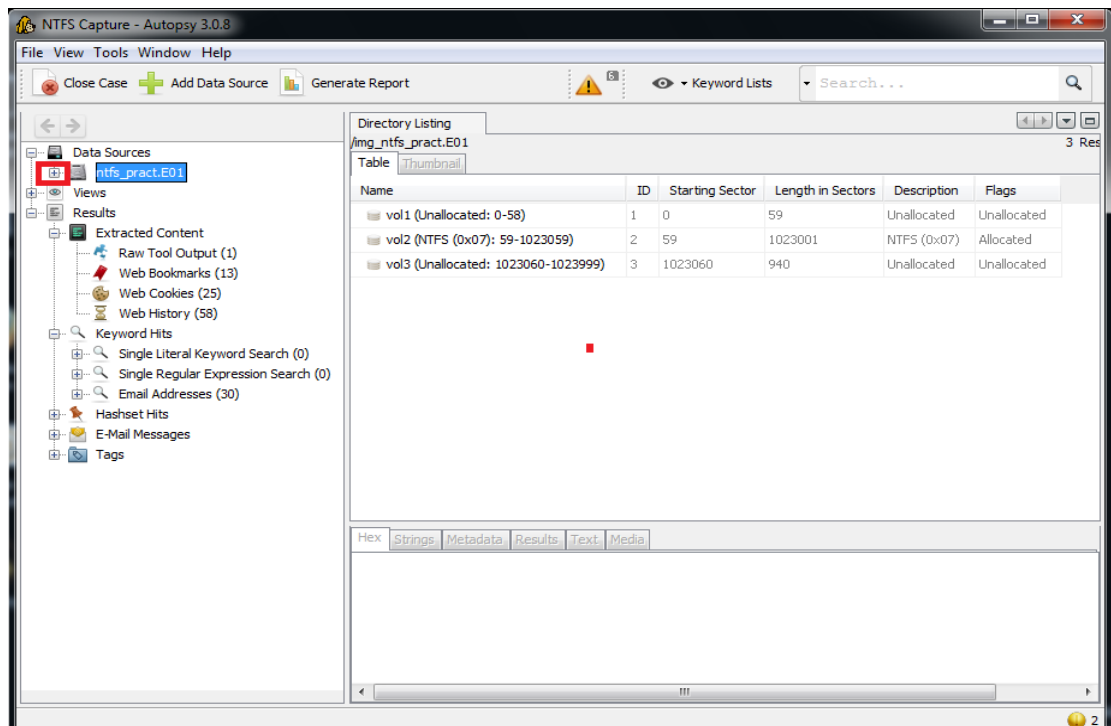
1. What tasks are typically completed when a forensic case is created?
2. What is an E01 file?
3. Can an E01 file be loaded into forensic analysis tools other than EnCase?
4. What is an image file? (explain in detail)

### 3 Examining an Image with Autopsy

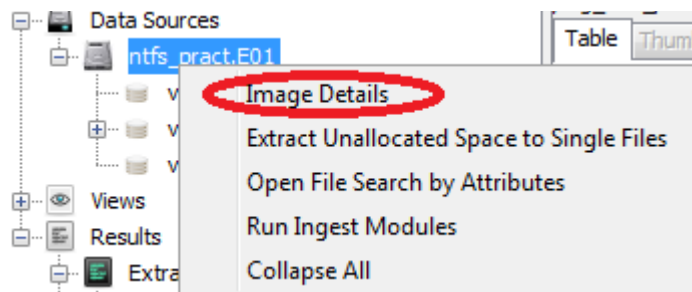
Navigation in Autopsy is similar to that in Windows Explorer. The left pane contains a directory tree for your image. It provides a listing of all the extracted data and categorizes the data by type.

#### 3.1 Navigation within Autopsy

1. Expand a listing by clicking the + sign next to the item.

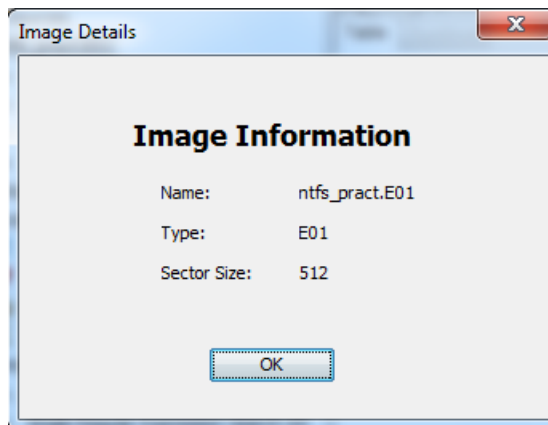


2. Look at the properties of the image we used. Right-click on **ntfs\_pract.E01** and select **Image details** from the right-click menu.

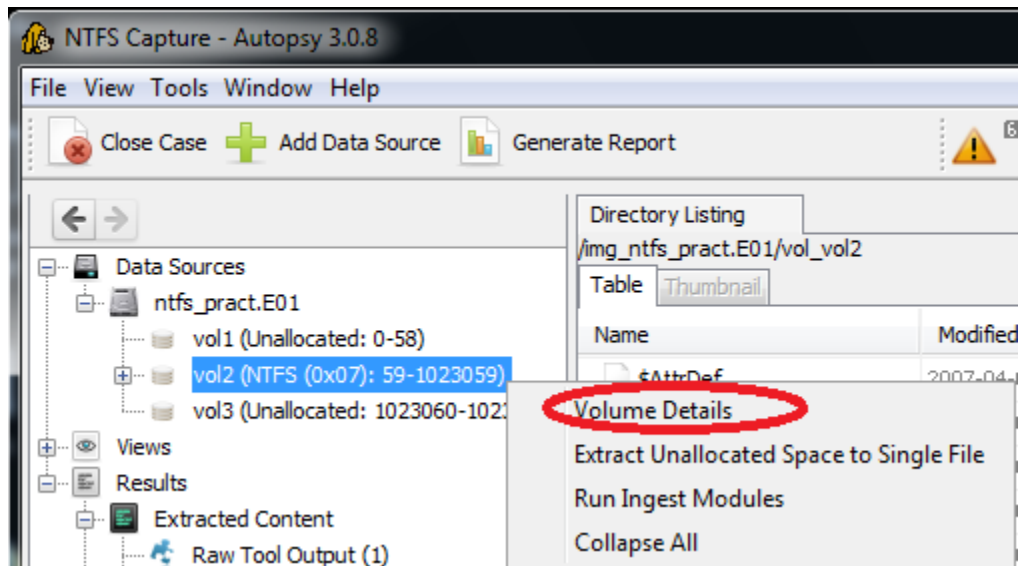




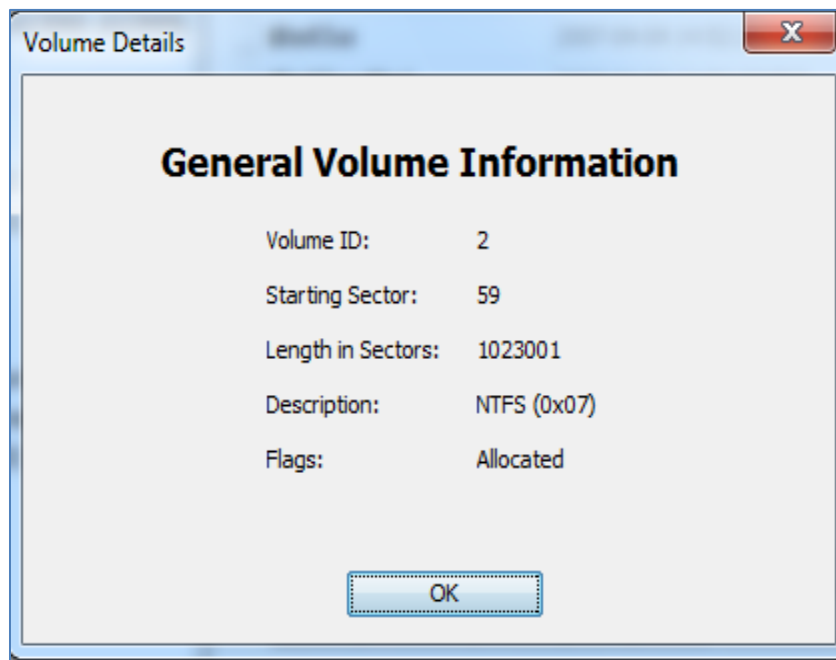
3. The image was saved in Expert Witness Format (which is the format used by Encase) and has a sector size of 512K. Click **Ok**.



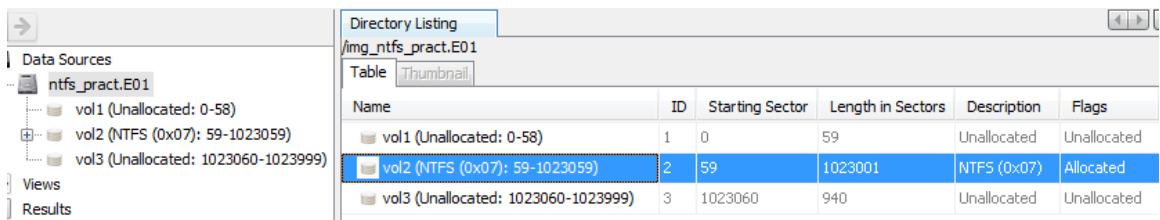
4. Expand the + sign for the **ntfs\_pract.E01** image file and right-click on vol2/NTFS. Select **Volume Details** from the right-click menu.



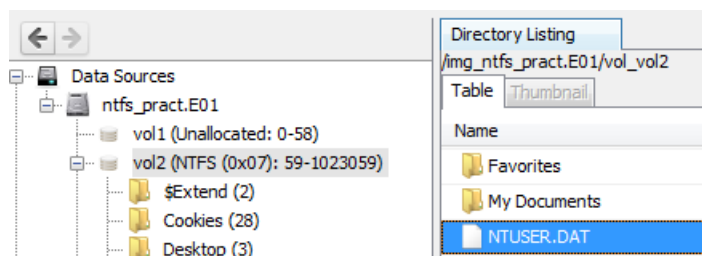
- The volume for this image starts at sector 59 and the length is 1023001 sectors. Notice vol1 and vol3 are unallocated or unused. Click **OK**.



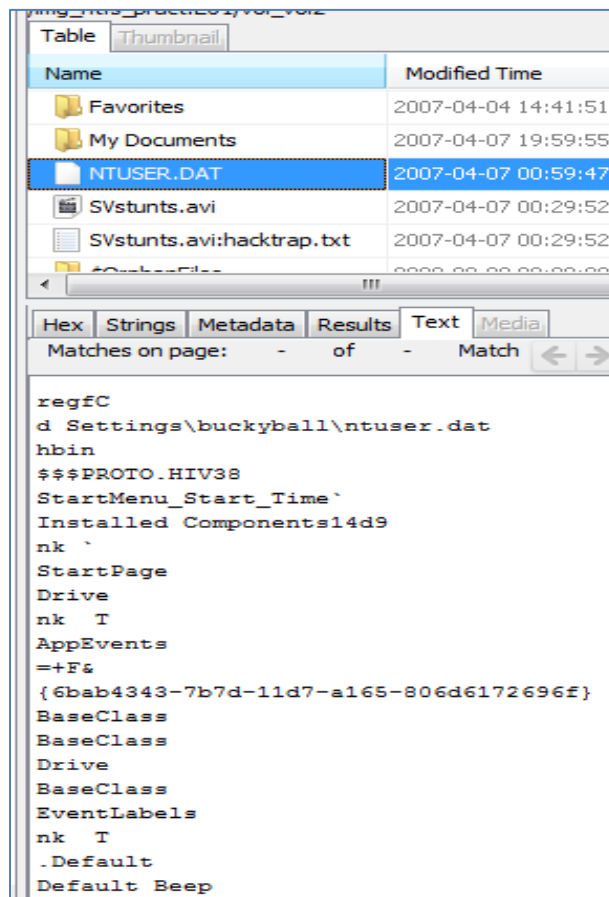
- Click on the **ntfs\_pract.E01** in the left pane and highlight **vol2 (NTFS)** in the right pane. Notice the details, including starting sector 59 and the length of 1023001 in sectors.



- Double-click on **vol2 (NTFS)** in the right pane. Scroll down and click once on the **NTUser.dat** file, in the right pane under Table.



8. Below the Table View, there are several views available for a given file. The **Text View** displays the extracted text from the file.



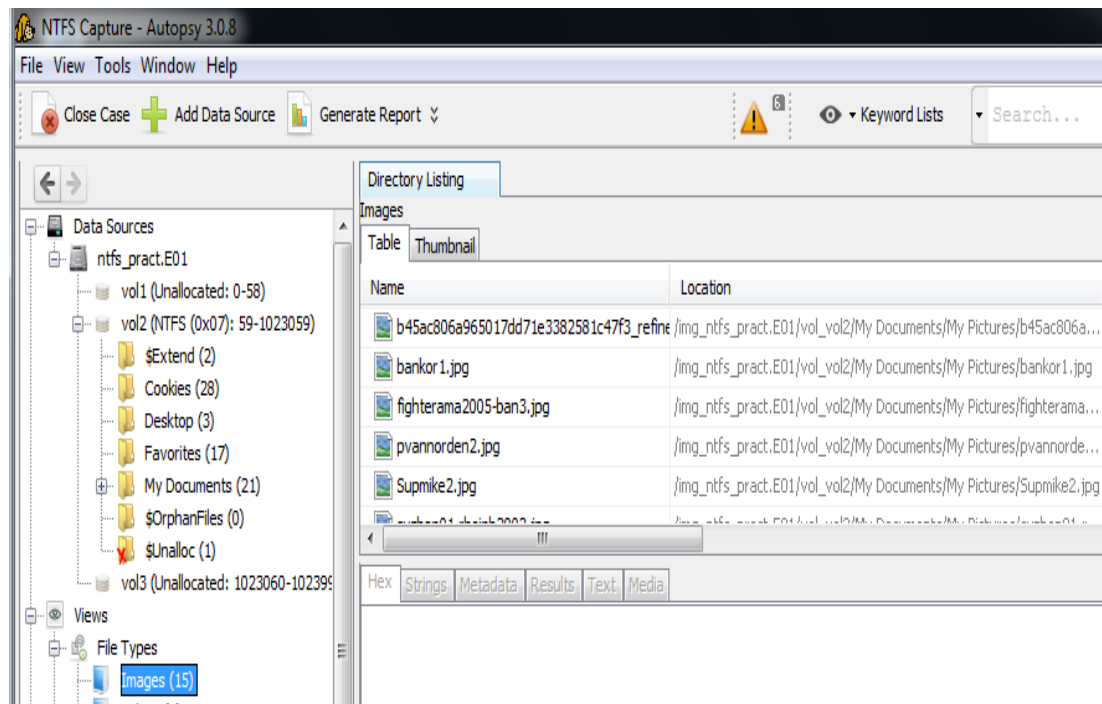
9. Select the **Hex View** tab to see the hexadecimal view of the same file.

NTUSER.DAT	2007-04-07 00:59:47 EDT	2007-04-07 00:59:47 EDT	2007-04-07 00:59:47 EDT	2007-04-07 00:59:47 EDT
SVstunts.avi	2007-04-07 00:29:52 EDT	2007-04-07 00:57:22 EDT	2007-04-07 00:57:22 EDT	2007-04-07 00:57:22 EDT
SVstunts.avi:hacktrap.txt	2007-04-07 00:29:52 EDT	2007-04-07 00:57:22 EDT	2007-04-07 00:57:22 EDT	2007-04-07 00:57:22 EDT
AutopsyFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

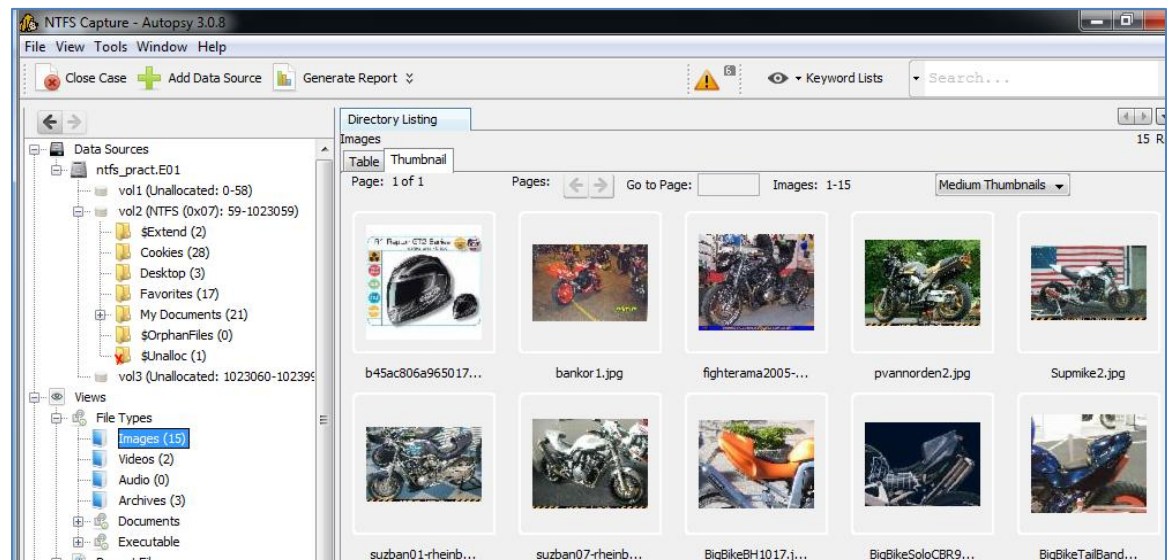
  

Hex	Strings	Metadata	Results	Text	Media
Page: 1	of 96	Page: 1	of 96	Go to Page:	
0x000000: 72 65 67 66 43 07 00 00	43 07 00 00	E0 5C C7 F1	regfC...C....\..		
0x000010: 5F 78 C7 01 01 00 00 00	03 00 00 00	00 00 00 00	_x.....		
0x000020: 01 00 00 00 20 00 00 00	00 60 15 00	01 00 00 00	.....`.....		
0x000030: 64 00 20 00 53 00 65 00	74 00 74 00	69 00 6E 00	d. .S.e.t.t.i.n.		
0x000040: 67 00 73 00 5C 00 62 00	75 00 63 00	6B 00 79 00	g.s.\.b.u.c.k.y.		
0x000050: 62 00 61 00 6C 00 6C 00	5C 00 6E 00	74 00 75 00	b.a.l.l.\.n.t.u.		
0x000060: 73 00 65 00 72 00 2E 00	64 00 61 00	74 00 00 00	s.e.r...d.a.t...		

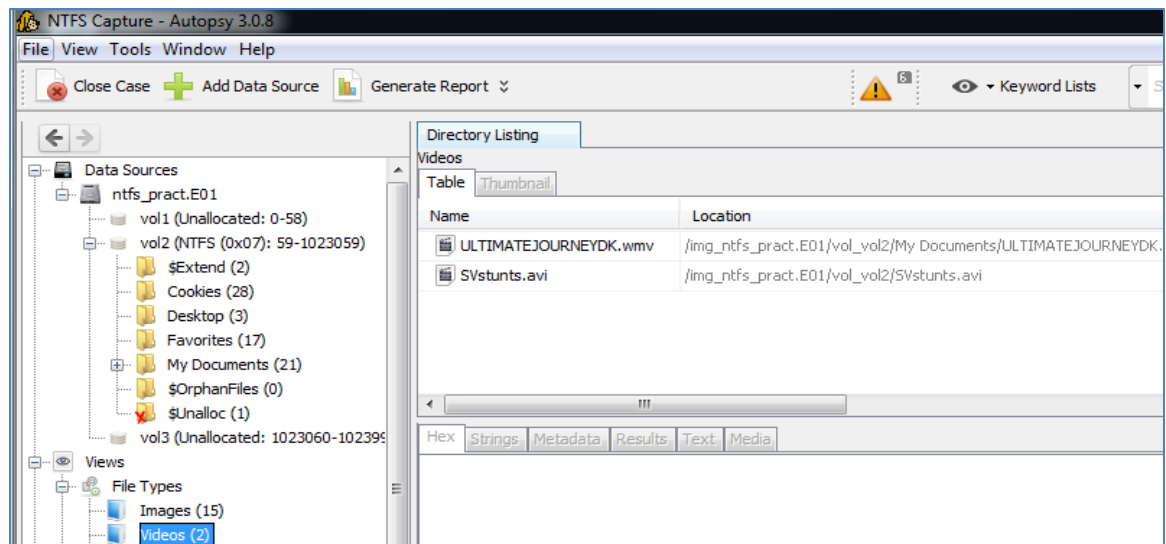
10. In the directory tree view, click the + sign to expand **Views**, then expand **File Types** and click **Images**.



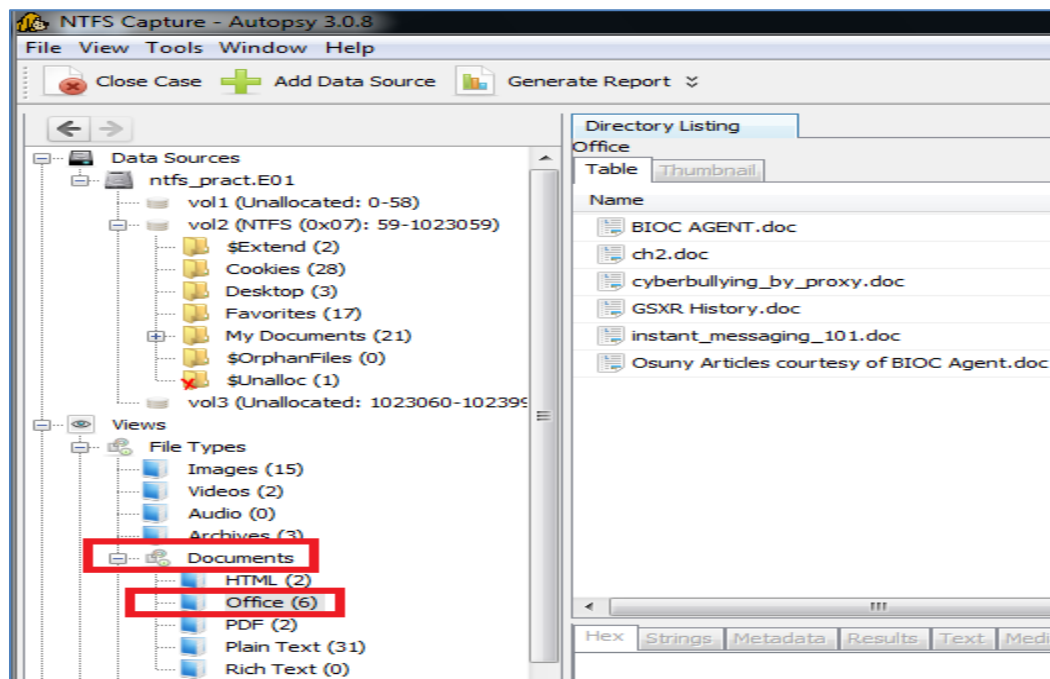
11. Files that match the selection appear in the Table View. You can view image files as well as play video and audio files in the viewer. Click the **Thumbnail** tab in the viewer on the right. All of the extracted images appear.



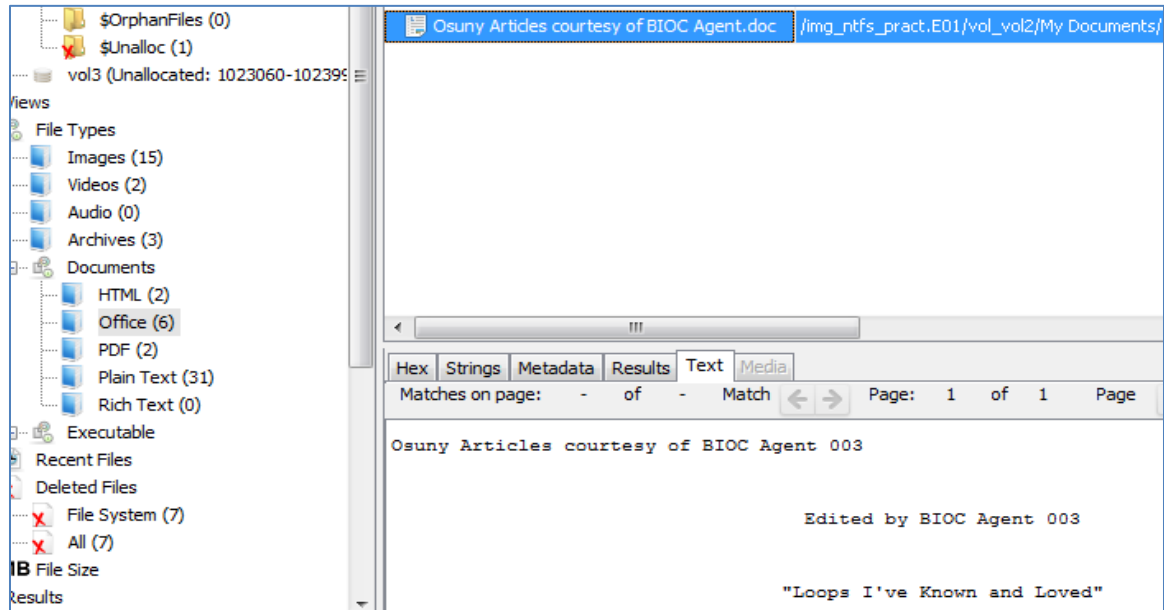
12. Click on **Videos** in the directory tree. You can play the two videos that are listed from the Table View. Click on a video in the Table View and the video appears in the **Media View** window.



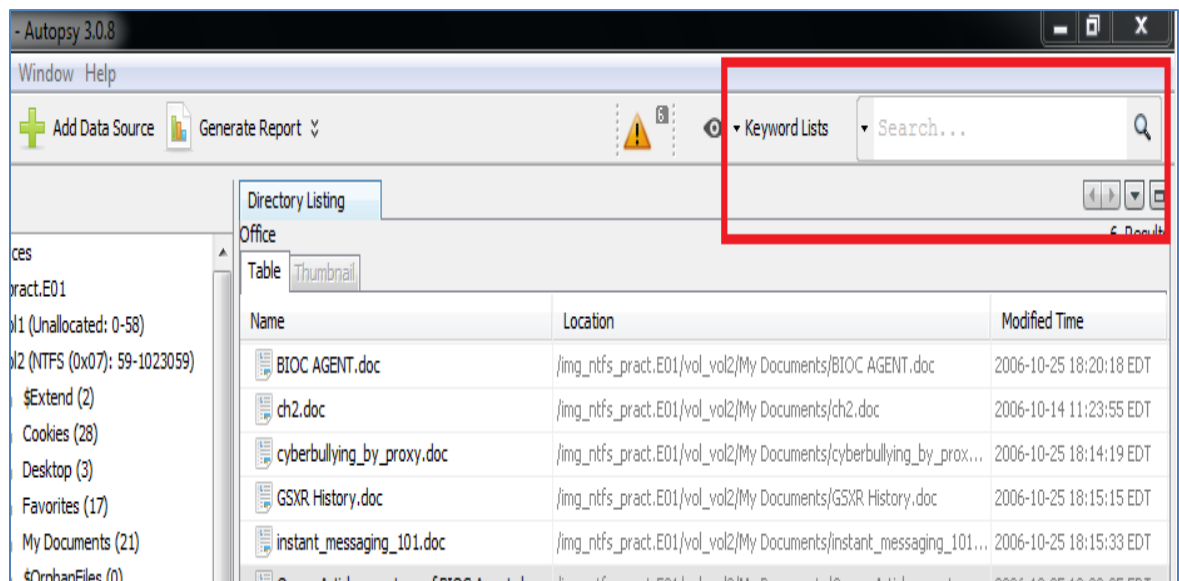
13. Expand the + next to **Documents**. Choose **Office** to display a list of documents from the image file. Deleted documents have a red X designation.



14. Highlight the last document and you can view its contents in the **Text View**.



15. The **Keyword Lists** feature on the bar allows you to pattern match certain values that may be stored in the image.



16. There are four preconfigured searches that you may try or you can write your own. All searches use **Regular Expressions**. Use the box next to the Keyword Lists to perform a text search. All search results display in the directory tree.

## 3.2 Conclusion

Autopsy is a powerful forensic program that will give you information about a disk image or a volume loaded into the case. Autopsy will parse out items, such as images, video files, and documents. The text reader will allow you to view document contents.

## 3.3 Discussion Questions

1. Where do you navigate to within Autopsy to recover documents?
2. Where do you navigate to within Autopsy to recover video files?
3. Where do you navigate to within Autopsy to recover image files?
4. What are two ways to obtain information about a volume without Autopsy?



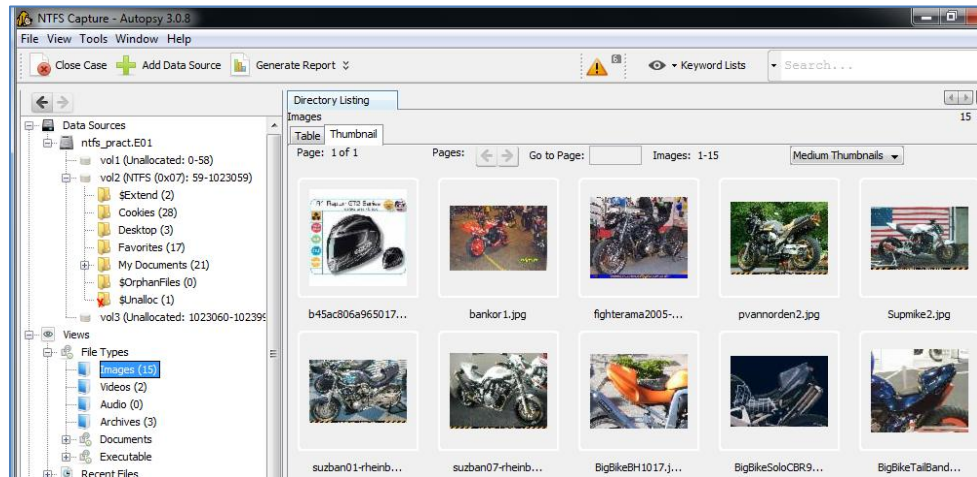


## 4 Report Generation

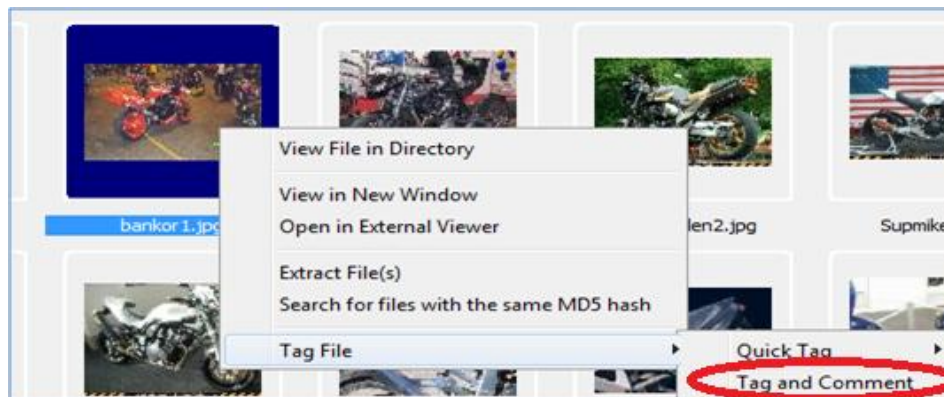
One of the most important tasks an investigator performs is to produce a report of his/her findings. A built-in report generator in Autopsy reports on any tagged items.

### 4.1 Using the Autopsy Report Generator

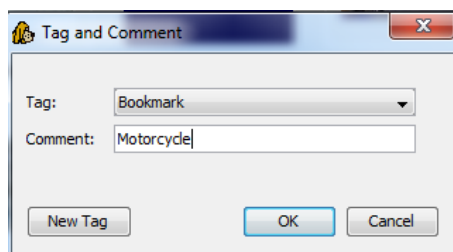
1. We will tag a few items to be included in the report. Go to **Images** in the directory tree under **File Types**. Choose the **Thumbnail View** on the right.



2. Right-click on an image. Choose **Tag File > Tag and Comment**.

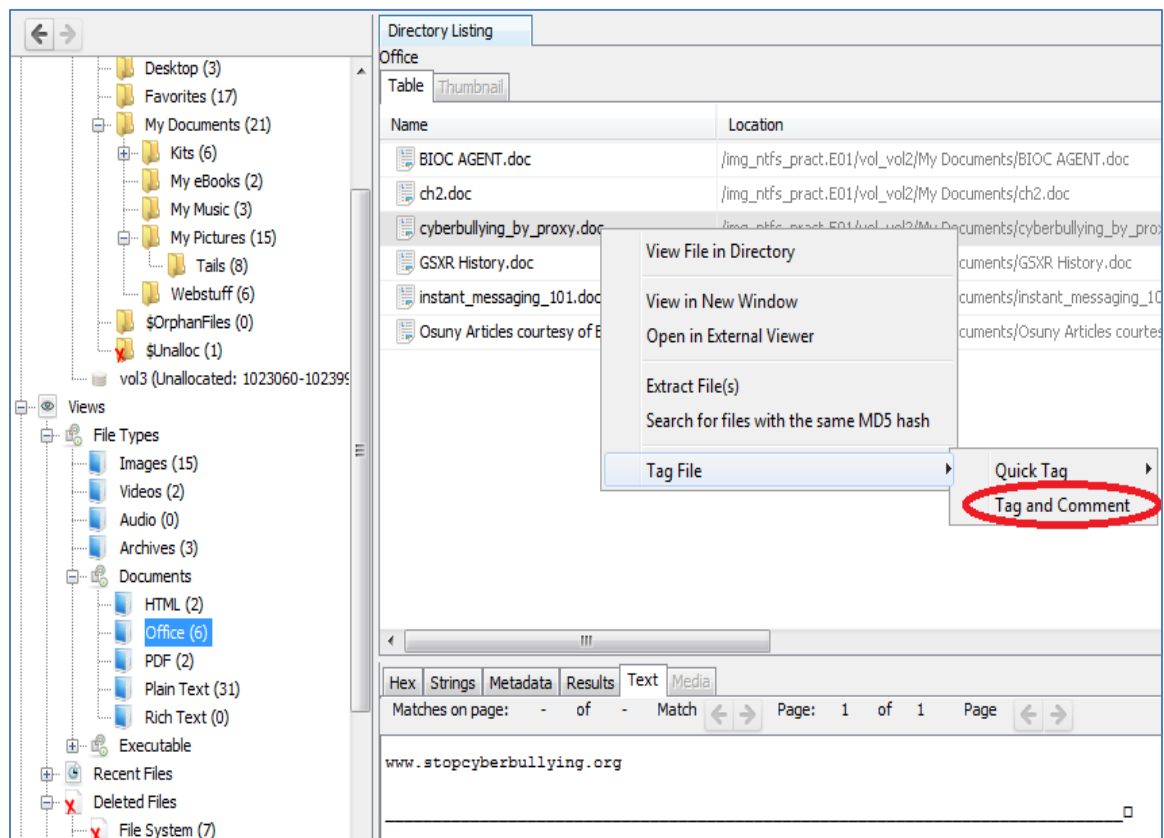


3. Leave **Bookmark** as the tag. Write a description in the Comment field. Click **OK**.

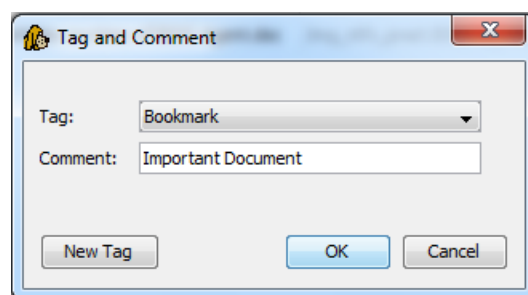




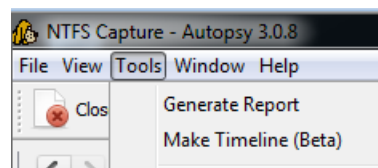
4. In the left pane, expand **Documents > Office**. Right-click on a few documents in the right pane and choose **Tag File > Tag and Comment** to bookmark.



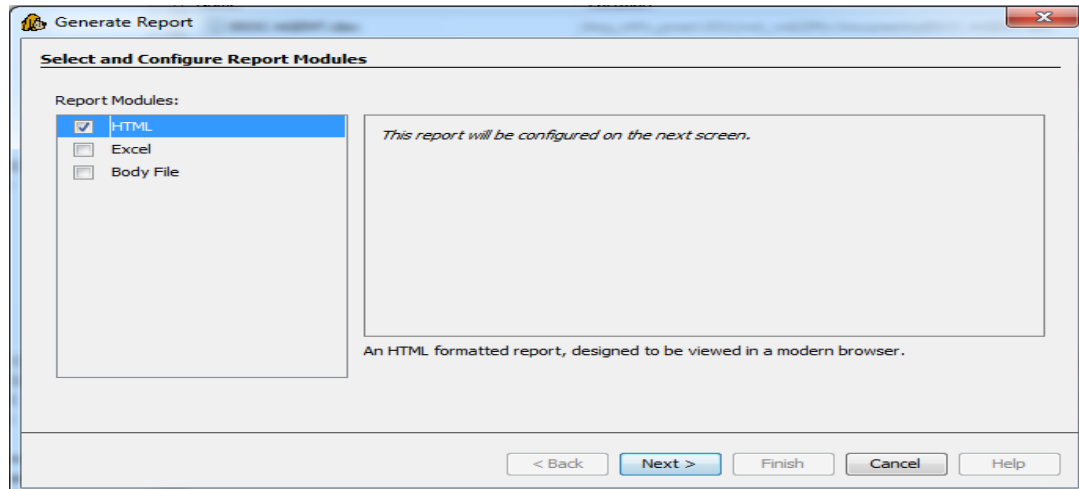
5. Leave Bookmark for the tag. Write a description in the comment field. Click **OK**.



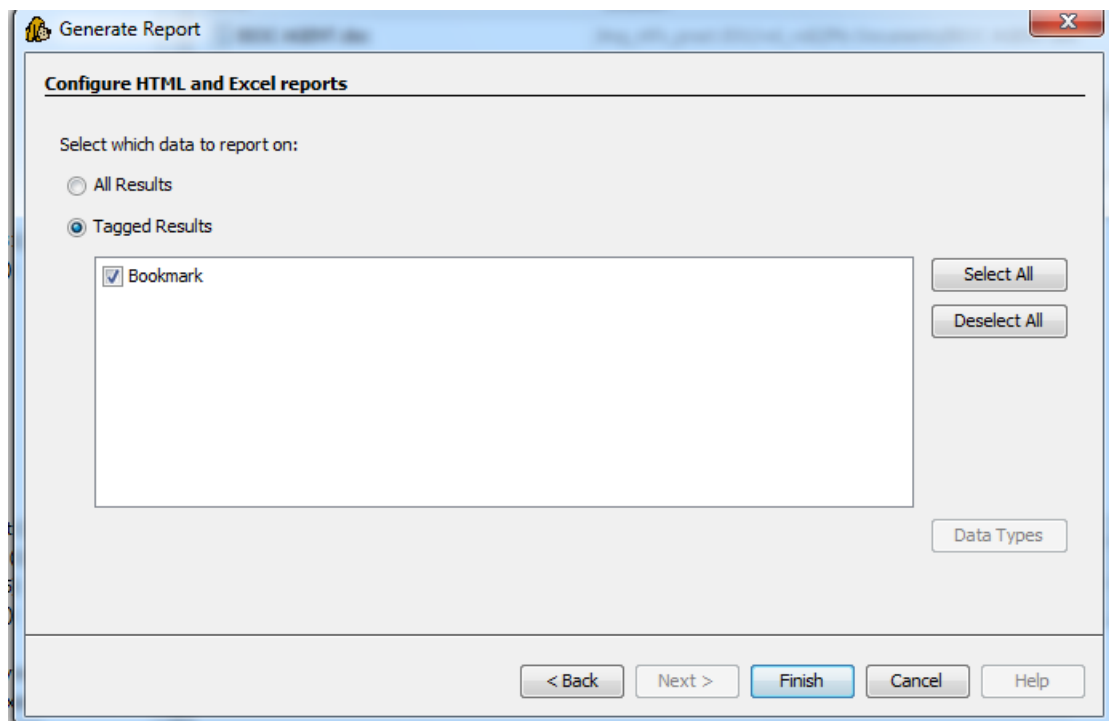
6. To generate a report, click on **Tools** in the menu bar and select **Generate Report**.



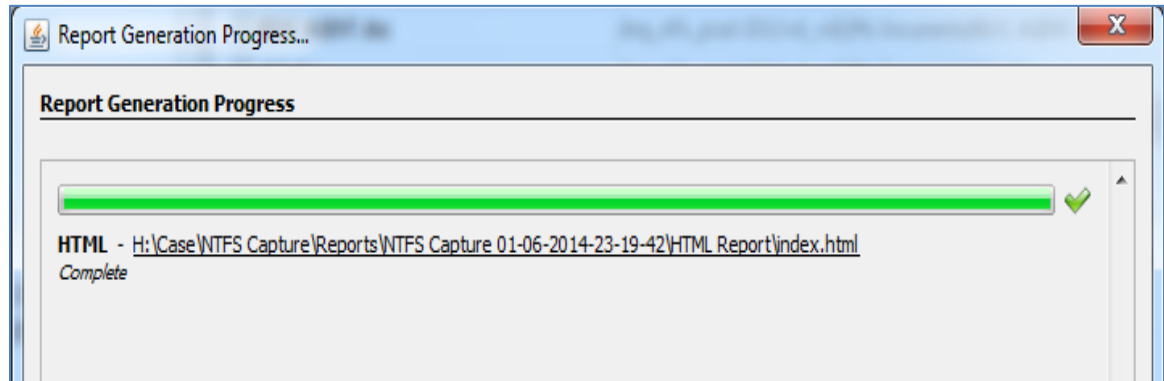
7. You can choose from three report formats: HTML, Excel, or Body File. Select **HTML** and click **Next**.



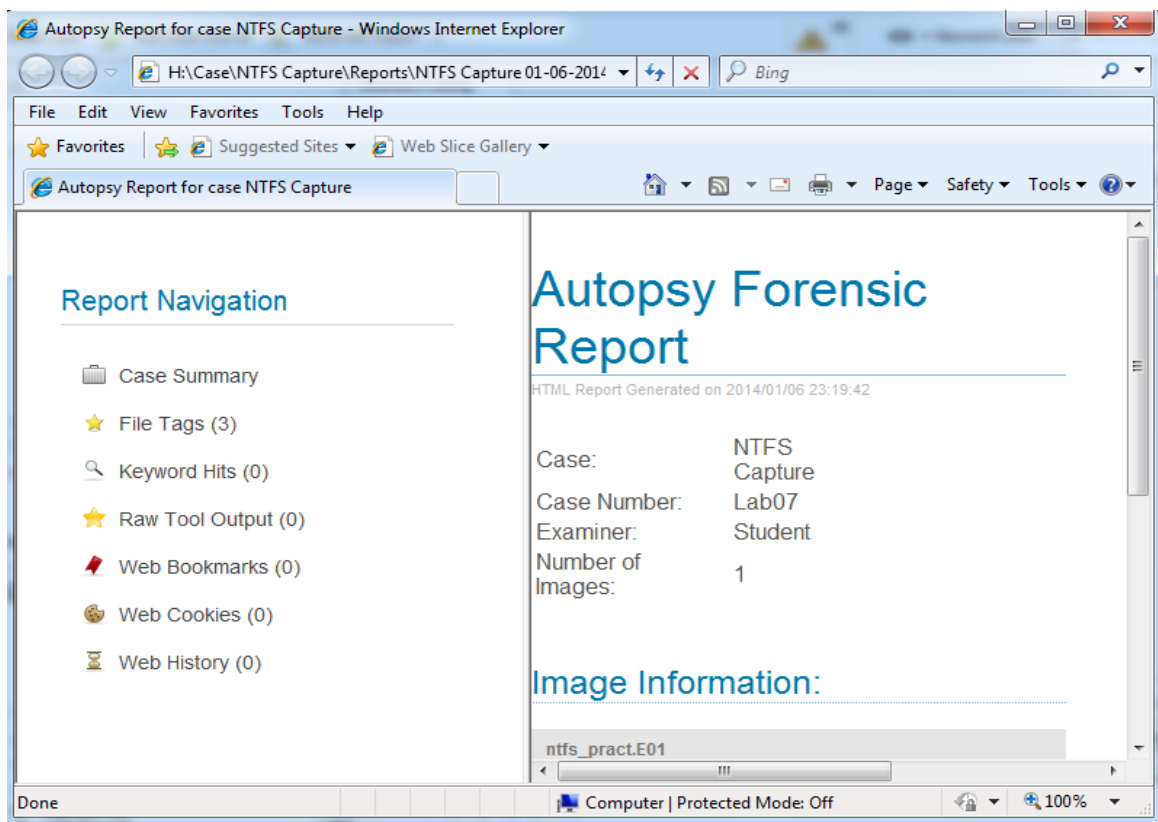
8. Choose **Tagged Results** and check **Bookmark**. Click **Finish**.



- Click on the URL that the tool has created. Your browser will open with a report.



- The report will open in an Internet Explorer browser.



## 11. Select **File Tags**.

### Report Navigation

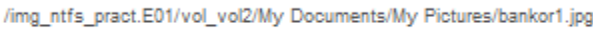
- Case Summary
- File Tags (3)**
- Keyword Hits (0)
- Raw Tool Output
- Web Bookmarks (0)
- Web Cookies (0)
- Web History (0)

### File Tags

This report only includes files and artifacts tagged with: Bookmark


File	Tag	Comment	
/img_ntfs_pract.E01/vol_vol2/My Documents/My Pictures/bankor1.jpg	Bookmark		<a href="#">View File</a>
/img_ntfs_pract.E01/vol_vol2/My Documents/cyberbullying_by_proxy.doc	Bookmark	Important Document	<a href="#">View File</a>
/img_ntfs_pract.E01/vol_vol2/My Documents/My Pictures/bankor1.jpg	Bookmark	Motorcycle	<a href="#">View File</a>

## 12. Click on the link to view the file that is contained within the report.


Bookmark
Motorcycle
**View File**

### Report Navigation

- Case Summary
- File Tags (3)**
- Keyword Hits (0)
- Raw Tool Output
- Web Bookmarks (0)
- Web Cookies (0)
- Web History (0)



## 13. Close all open windows and the Windows7 PC Viewer.

## 4.2 Conclusion

Autopsy has a reporting feature that will allow an investigator to bookmark items within a case. The report can be generated in three different formats: HTML, Excel, or Body File. Once the report is opened, items that were bookmarked can be viewed in the report.

## 4.3 Discussion Questions

1. In what three formats can a report be generated in Autopsy?
2. Where do you navigate to within Autopsy to generate a report?
3. How do you bookmark an item?
4. Where do you go within the report to view the bookmarked items?



## References

1. Autopsy Forensic Browser Download:  
<http://www.sleuthkit.org/autopsy/download.php>
2. The Sleuth Kit:  
<http://www.sleuthkit.org/>
3. E01 File Format:  
<http://pcsupport.about.com/od/fileextensions/f/e01file.htm>
4. How to Write a Forensic Report:  
[http://www.ehow.com/how\\_5858380\\_write-forensic-report.html](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>

