

## **Part 1 :- An Introduction to Autopsy**

Autopsy is a graphical user interface (GUI) program that allows easy access to the command-line tools and the C library included in the Sleuth Kit and other digital forensics tools. The tools included in the Sleuth Kit—and other digital forensics tool will allow Autopsy to automate much of the forensics analysis tasks required in most investigations, such as recovering deleted files, analyzing Windows registry, investigating e-mail messages, investigating unallocated disk space, and many more. Autopsy provides additional features that help examiners to be more productive during their analysis work

### Steps:

- Download Autopsy from <https://www.autopsy.com/download/>, and then install it.
- Before beginning this activity, create a directory and **Ch01InChap01.exe** shared along with this manual
- In the following steps, you analyze **George Montgomery's USB drive**. The first task is to configure Autopsy for a new case and analyze the image file of GeorgeMontgomery's USB drive.

1. Double-click the Ch01InChap01.exe file in File Explorer to uncompress it into Ch01InChap01.dd. Start Autopsy for Windows.

2. In Autopsy's main window, click the Create New Case button. In the New Case Information window, enter InChap01 in the Case Name text box (see Figure 1), and click Browse next to the Base Directory text box. Navigate to and click your work folder. Make sure the Single-user option button is selected for Case Type, and then click Next.

**New Case Information**

**Steps**

1. Case Information
2. Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

**Figure 1: The New Case Information window**

3. In the Additional Information window, type “1” in the Case Number text box and your name in the Examiner text box (see Figure 2), and then click Finish to start the Add Data Source Wizard.

**New Case Information**

**Steps**

1. Case Information
2. Optional Information

**Optional Information**

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

Organization analysis is being done for:

< Back Next > **Finish** Cancel Help

**Figure 2: Optional information for the case**

4. In the Select Data Source window (see Figure 3,4,5), click the Select data source type list arrow, and click Disk Image or VM file. Click the Browse button next to the “Browse for an image file” text box, navigate to and click your work folder and the Ch01InChap01.dd file, and then click Open. Click Next.

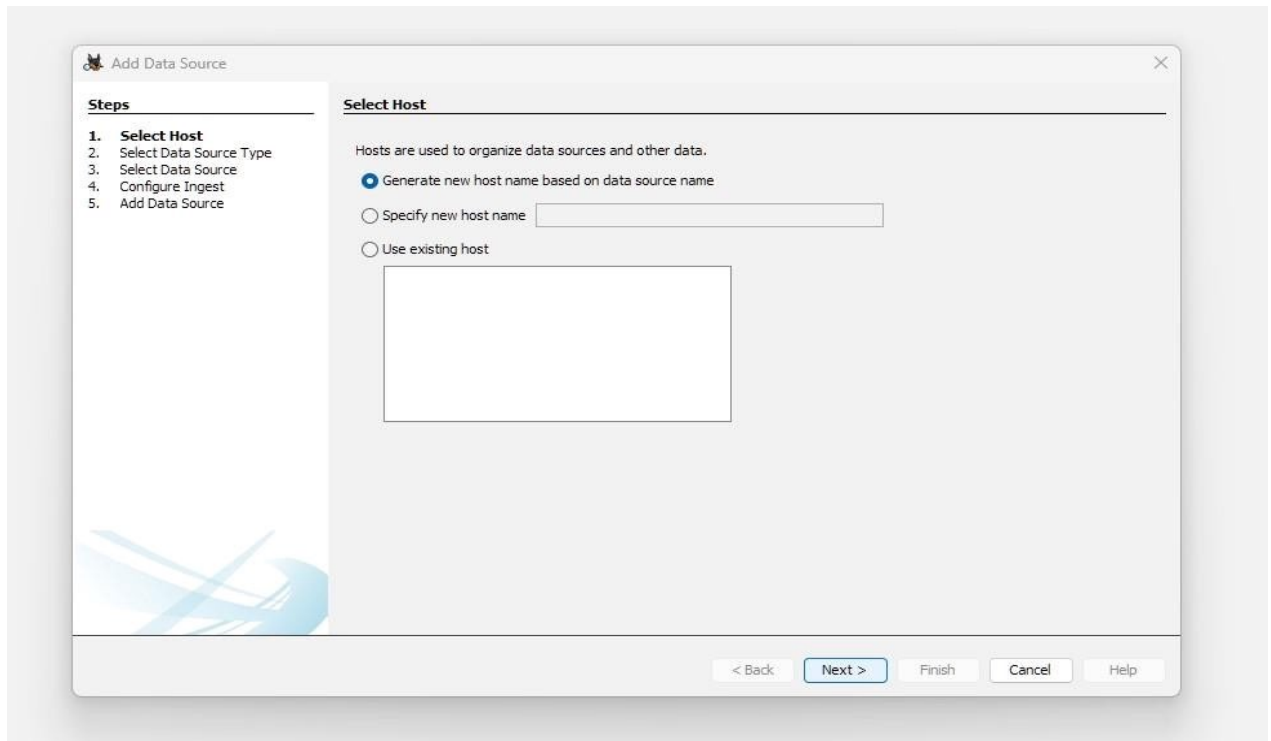


Figure 3

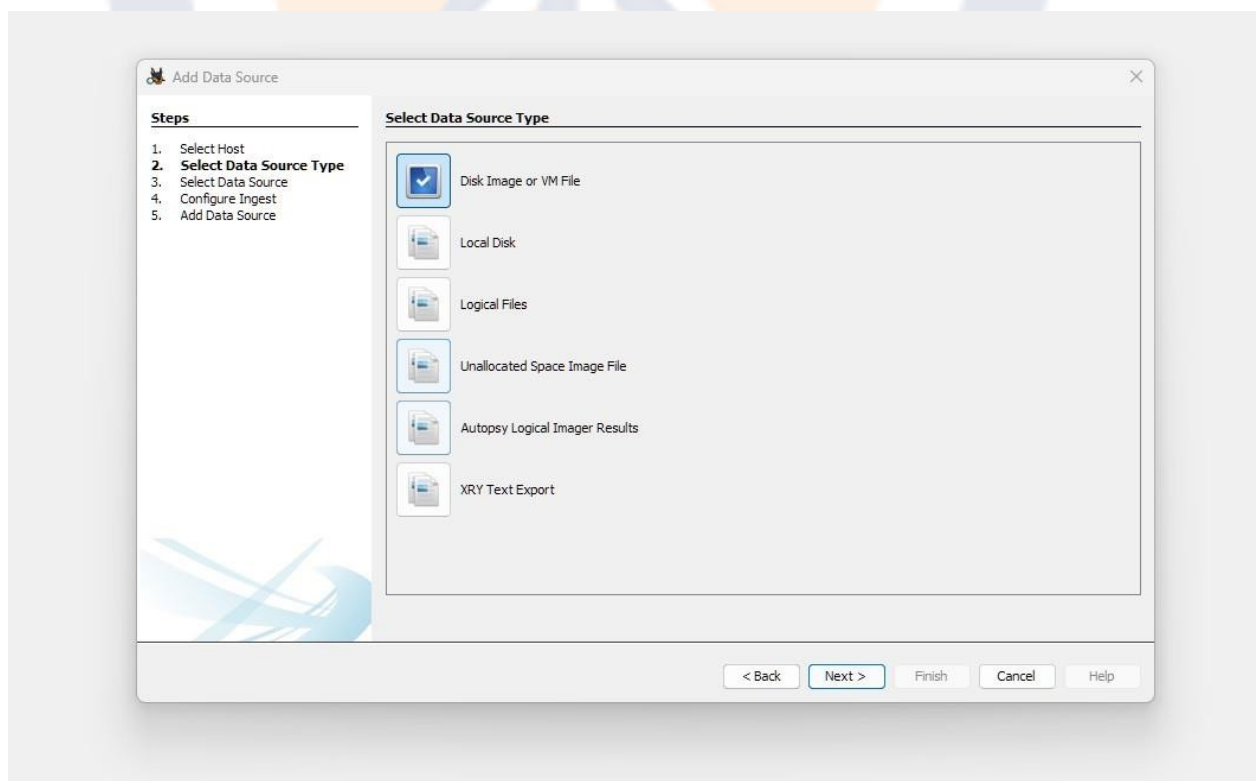
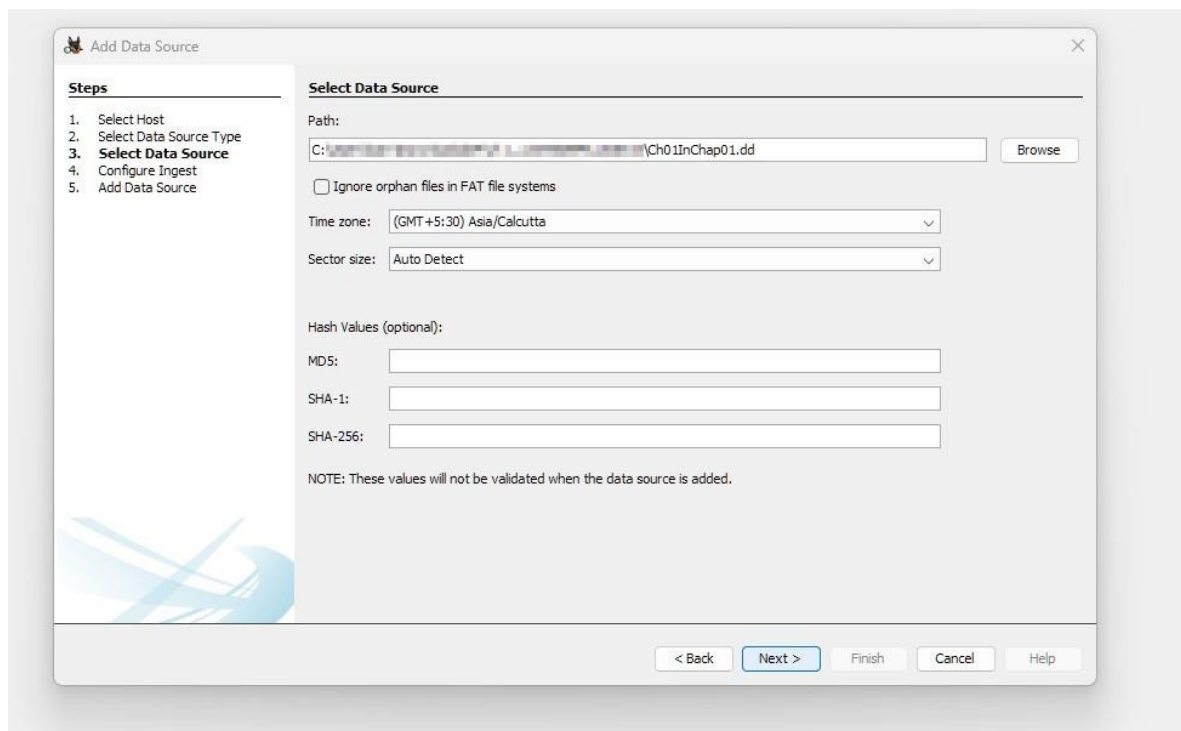


Figure 4



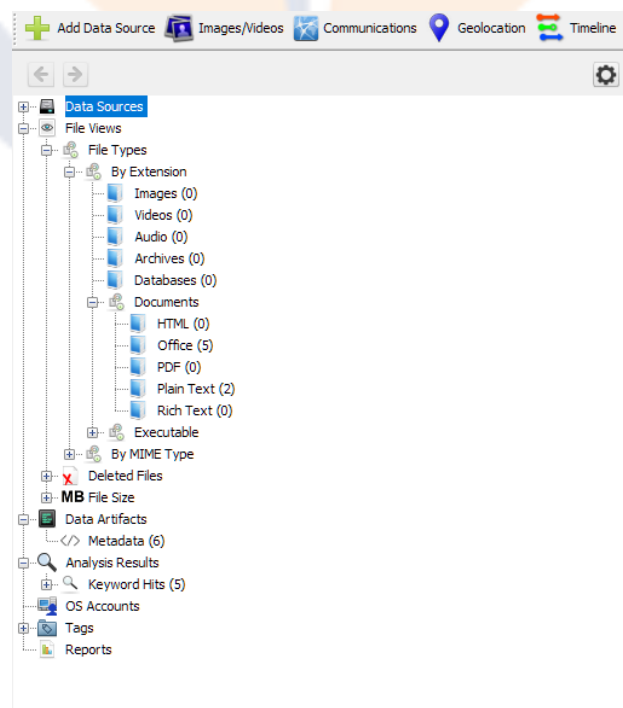
**Figure 5**

5. Keep the default settings in the Configure Ingest Modules window. Click Next and then Finish.

### **View the acquired data**

**Follow these steps to display the contents of the acquired data:**

1. In the Tree Viewer pane on the left, click to expand Views, File Types, By Extension, and Documents (see Figure 6).



**Figure 6: Autopsy's Tree Viewer pane**

2. Under Documents, click Office. In the Result Viewer (upper-right pane), click the first file, Billing Letter.doc, to display its contents in the Content Viewer (lower-right pane).
3. Right-click Billing Letter.doc, point to Tag File, and click Tag and Comment (Figure 7).

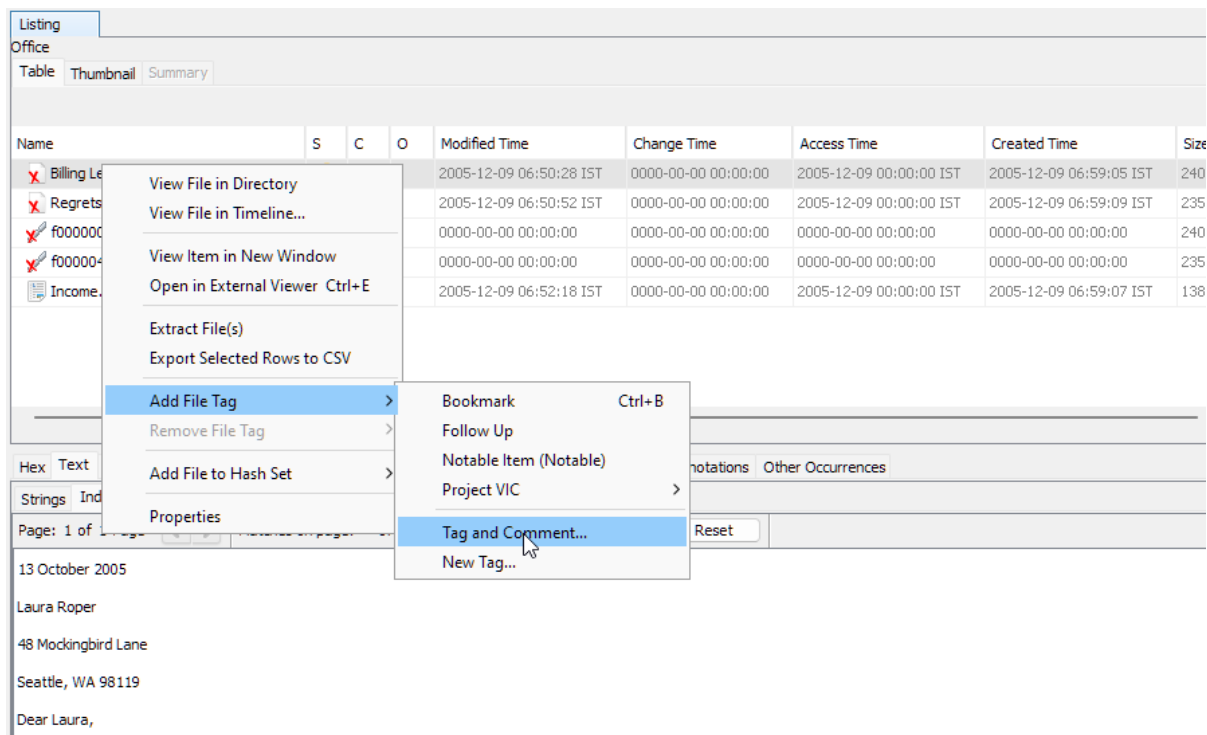


Figure 7

4. In the Create Tag dialog box, click the New Tag Name button shown in Figures 8,9. In the New Tag section, type Recovered Office Documents in the Tag Name text box, click OK, and then click OK again.

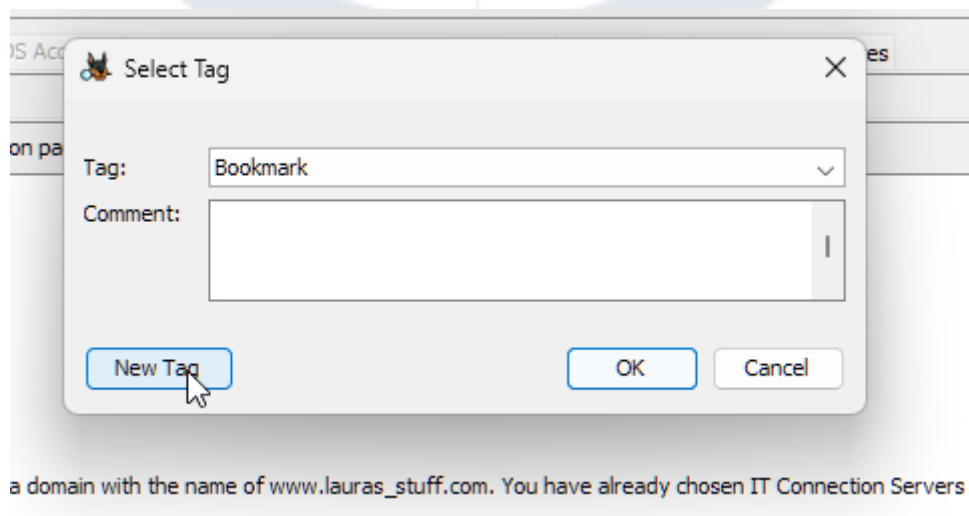
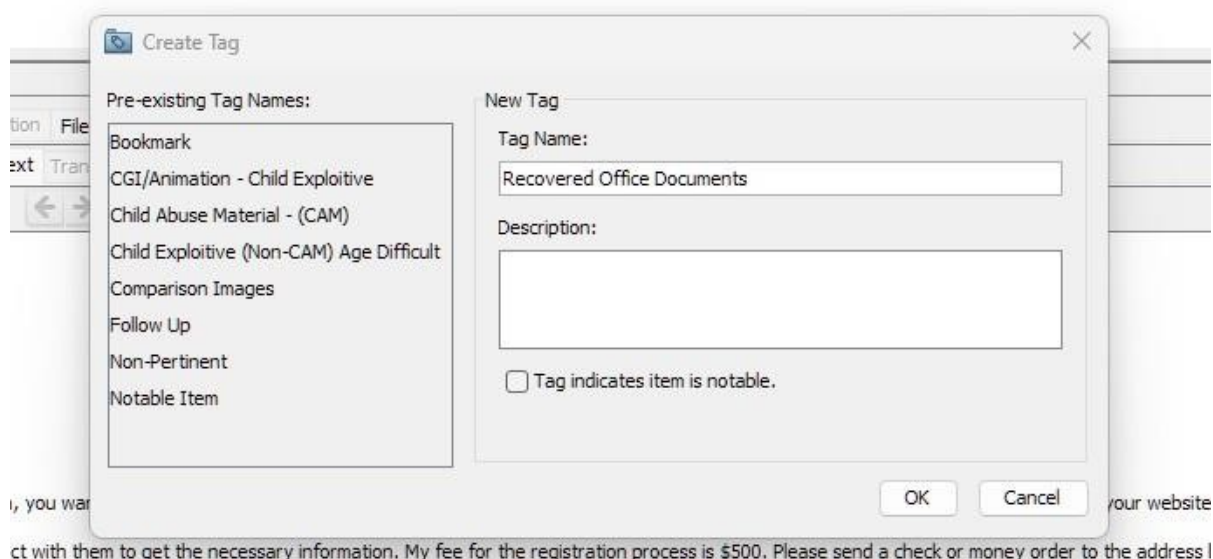


Figure 8: The Create Tag dialog boxes

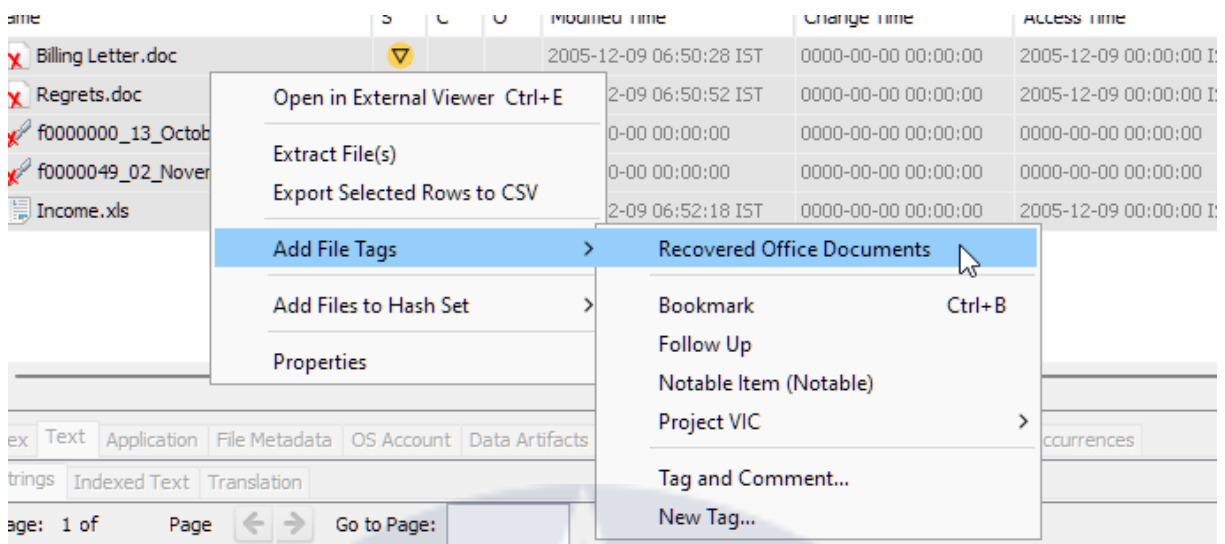


**Figure 9: The Create Tag dialog boxes**

5. In the Result Viewer pane, Ctrl+click Billing Letter.doc, Income.xls, Regrets.doc, f0000000.doc, and f0000049.doc to select these files, and then release the Ctrl key. Right-click the highlighted files shown in Figure 10, point to Tag File and then Quick Tag, and then click Recovered Office Documents.

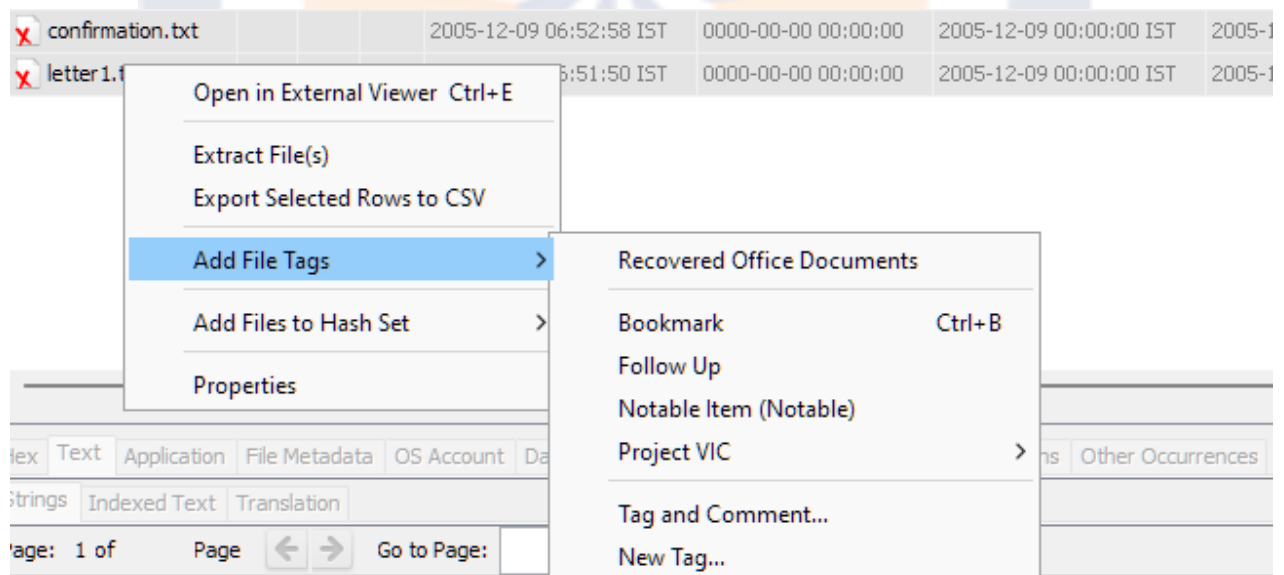
Listing Office												
Table Thumbnail Summary												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Billing Letter.doc				2005-12-09 06:50:28 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:05 IST	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Billing Letter.doc
Regrets.doc				2005-12-09 06:50:52 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:09 IST	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Regrets.doc
f0000000_13_October_2003.doc			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/\$CarvedFiles/1/f0000
f0000049_02_November_2003.doc			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/\$CarvedFiles/1/f0000
Income.xls			0	2005-12-09 06:52:18 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:07 IST	13824	Allocated	Allocated	unknown	/img_Ch01InChap01.dd/Income.xls

**Figure 10**



**Figure 11**

6. Under Documents in the Tree Viewer pane, click Plain Text to display more recovered files.
7. In the Result Viewer pane, select the files listed in Step 5 again, right-click the selection, point to Tag File and then Quick Tag, and then click Follow Up. Leave Autopsy running for the next activity.



**Figure 12**



## Analyzing the data

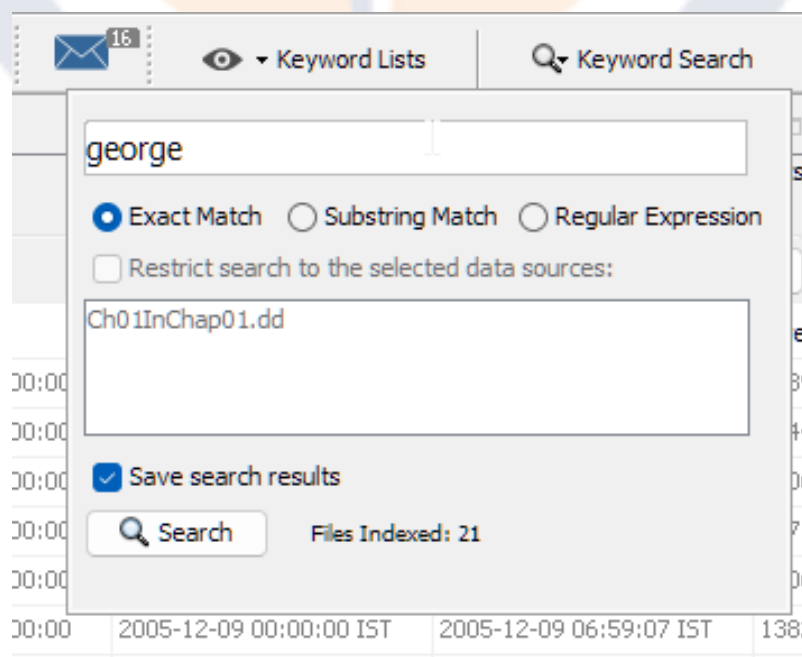
The next step is analyzing the data and searching for information related to the complaint. Data analysis can be the most time-consuming task, even when you know exactly what to look for in the evidence. The method for locating evidentiary artifacts is to search for specific known data values. Data values can be unique words or nonprintable

characters, such as hexadecimal codes. There are also printable character codes that can't be generated from a keyboard, such as the copyright (©) or registered trademark (™) symbols. Many digital forensics programs can search for character strings (letters and numbers)

and hexadecimal values, such as 0xA9 for the copyright symbol or 0xAE for the registered trademark symbol. All these searchable data values are referred to as “keywords.”

With Autopsy, you can search for keywords of interest in the case. For this case, you need to find any files associated with George Montgomery. Follow these steps to search for any reference to the name “George”:

1. Click the Keyword Search button at the far upper right, type George in the text box (see Figure 13), and then click Search.



**Figure 13: Entering a keyword search term**



2. In the Result Viewer pane, a new tab named Keyword search 1 opens. Click each file to view its contents in the Content Viewer (see Figure 15). Look for files containing the name “George.”

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
Unaloc_4_121344_1474560	address listed below.«George» Montgomery3467 Main Street	/img_Ch01InChap01.dd/Unaloc/Unaloc_4_121344_1474...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	133
Client Info.mdb	Ballard WA 98107 5 Thomas «George»...	/img_Ch01InChap01.dd/Client Info.mdb	2005-12-09 06:53:58 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:01 IST	104
Billing Letter.doc	address listed below.«George» Montgomery3467 Main	/img_Ch01InChap01.dd/Billing Letter.doc	2005-12-09 06:50:28 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:05 IST	246
confirmation.txt	you for your business«George»-----	/img_Ch01InChap01.dd/confirmation.txt	2005-12-09 06:52:58 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:06 IST	227
f0000000_13_October_2003.doc	address listed below.«George» Montgomery3467 Main	/img_Ch01InChap01.dd/CarvedFiles/1/f0000000_13_Oct...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	246
Income.xls	00 \$ 800.00 Thomas «George» \$ 450.00	/img_Ch01InChap01.dd/Income.xls	2005-12-09 06:52:18 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:07 IST	138
f0000049_02_November_2003.doc	nowhere.comRegards,«George» Montgomery-----	/img_Ch01InChap01.dd/CarvedFiles/1/f0000049_02_Nov...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	238
letter1.txt	Please contact me ASAP.«George»-----	/img_Ch01InChap01.dd/letter1.txt	2005-12-09 06:51:50 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:09 IST	12
Regrets.doc	nowhere.comRegards,«George» Montgomery-----	/img_Ch01InChap01.dd/Regrets.doc	2005-12-09 06:50:52 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:09 IST	238

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: 1 of 1 Match 100% Reset Text Source: Search Results

letter1.txt Earl,  
We need to meet on the 18th of August to confirm the work I am  
doing for you. Please contact me ASAP.  
  
George  
  
-----METADATA-----

Figure 14: Viewing the results of searching for the keyword “George”

3. Click the Keyword Lists button at the far upper right, click the Email Addresses check box, and then click Search.

16
Keyword Lists

☐ Phone Numbers  
☐ IP Addresses  
☒ Email Addresses  
☐ URLs  
☐ Credit Card Numbers

Name  
Keyword Type  
({?}[a-zA-Z0-9%+\_-]+(\,... Regular Expression

Save

☐ Restrict search to the selected data sources:

Ch01InChap01.dd

☒ Save search results

Search Manage Lists Files Indexed: 21

Figure 15

4. In the Result Viewer pane, a new tab named Keyword search 2 opens. Click each file to view its contents in the Content Viewer pane and examine all e-mail addresses found in the search. Leave Autopsy running so that you can learn about more of its features in the next section.

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Create
Unalloc_4_121344_1474560	hyperlink mailto:«george.montgomery@nowhere.com» geo...	/img_Ch01InChap01.dd/\$UnallocUnalloc_4_121344_1474...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Billing Letter.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01.dd/Billing Letter.doc	2005-12-09 06:50:28 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 00:00:00 IST
f0000000_13_October_2003.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01.dd/\$CarvedFiles/1/f0000000_13_Oct...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000049_02_November_2003.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01.dd/\$CarvedFiles/1/f0000049_02_Nov...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Regrets.doc	1212 or email me at «george.montgomery@nowhere.com»...	/img_Ch01InChap01.dd/Regrets.doc	2005-12-09 06:50:52 IST	0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 00:00:00 IST

Regrets.doc

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: 1 of 10 Match 100% Reset Text Source: Search

HYPERLINK mailto:george.montgomery@nowhere.com

george.montgomery@nowhere.com

Regards,

George Montgomery

www.lauras\_stuff.com

http://www.lauras\_stuff.com/

george.montgomery@nowhere.com

mailto:george.montgomery@nowhere.com

Normal

Heading 1

Default Paragraph Font

Hyperlink

Amelia PhillipsE:\Course Technology\Computer Forensics\Chapter 2 files\Chapter 2 AU2\case files\chapter\Billing Letter.doc

Amelia PhillipsC:\Chap02\case files\chapter\Billing Letter.doc

Unknown

Times New Roman

Symbol

Arial

13 October 2003

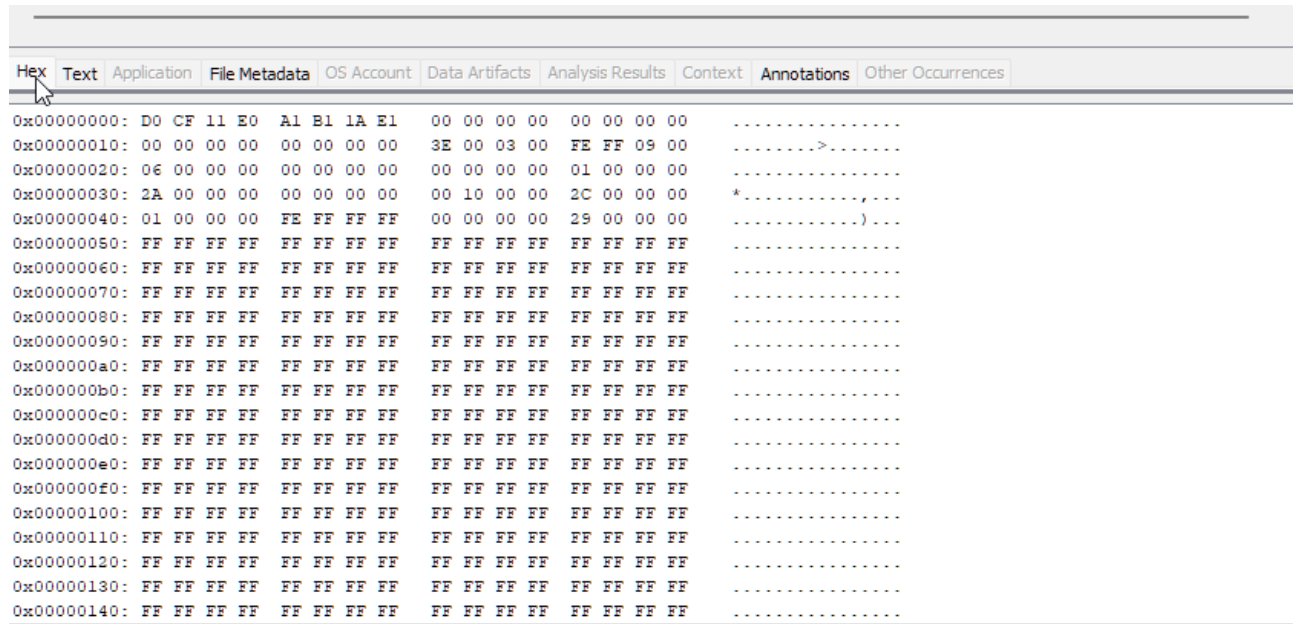
Amelia Phillips

Amelia Phillips

Figure 16

## Some Additional Features of Autopsy

If you find a file of interest that displays binary (nonprintable) data in the Content Viewer, there are six available viewing options in Autopsy: Hex, Strings, File Metadata, Results, Indexed Text, and Media. To view an unallocated sector for its hexadecimal values, click the Hex tab in the Content Viewer, as shown in Figure 17.



Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
0x00000000:	D0 CF 11 E0	A1 B1 1A E1	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....		
0x00000010:	00 00 00 00	00 00 00 00	3E 00 03 00	FE FF 09 00	.....>.....				
0x00000020:	06 00 00 00	00 00 00 00	00 00 00 00	01 00 00 00	.....				
0x00000030:	2A 00 00 00	00 00 00 00	00 10 00 00	2C 00 00 00	*.....,				
0x00000040:	01 00 00 00	FE FF FF FF	00 00 00 00	29 00 00 00	.....)				
0x00000050:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000060:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000070:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000080:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000090:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x000000a0:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x000000b0:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x000000c0:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x000000d0:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x000000e0:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x000000f0:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000100:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000110:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000120:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000130:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				
0x00000140:	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF	.....				

Figure 17

## Autopsy Default Ingest Modules

Module Name	Function
Recent Activity	Extracts recent user activity, such as web browsing and recently opened documents and installed programs. This module supports Windows OS only.
Hash Lookup	Identifies known and notable files using supplied hash sets, such as the NSRL hash set. A premade index of NSRL releases ( <a href="http://www.nist.gov">www.nist.gov</a> ) can be downloaded from <a href="https://sourceforge.net/projects/autopsy/files/NSRL/">https://sourceforge.net/projects/autopsy/files/NSRL/</a> .
File Type Identification	Matches file types based on their signatures (not extension) and reports them based on MIME type.
Embedded File Extractor	Extracts embedded files such as doc, ppt, xls,xlsx, pptx, docx, zip, tar, 7z, gzip, bzip2, arj) and analyzes their contents.
Exif Parser	Extracts EXIF metadata from JPEG files.
Keyword Search	Performs file indexing and uses keywords to search within file's contents.
E-mail Parser	Detects and parses Outlook and Thunderbird e-mails.
Extension Mismatch Detector	Warns about files that have nonstandard extension based on their file type.
E01 Verifier	Validates the integrity of the E01 file type.
Encryption Detection	Detects encrypted files.
Interesting Files Identifier	Searches for a specific file types and directories (e.g., VMware files within a data source) and generates alerts when finding a match.
PhotoRec Carver	Runs PhotoRec tool to retrieve files from unallocated space in the supplied data source and send them for analysis. You can use this tool as a standalone program; detailed instructions on how to use it is available at <a href="http://www.cgsecurity.org/wiki/PhotoRec_Step_By_Step">www.cgsecurity.org/wiki/PhotoRec_Step_By_Step</a> .
Correlation Engine	Saves properties to the central repository for later correlation.
Virtual Machine Extractor	Extracts virtual machine files and adds them to a case as data sources.
Android Analyzer	Extracts and views Android system and other third-party application data.