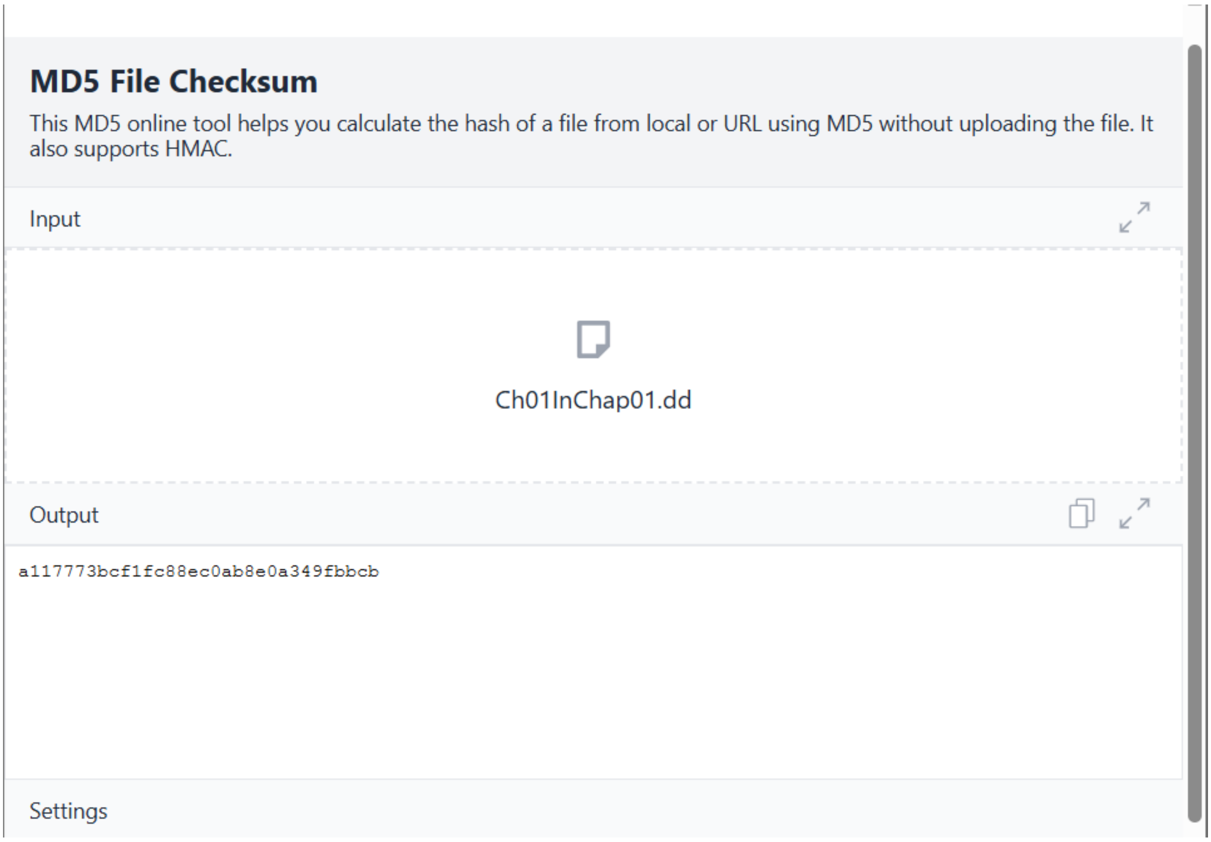
Lab 1: Introduction to Digital Forensics – Autopsy software

What You Need for this lab

- Windows 10
- Investigate a USB drive
    - Owned by George Montgomery
- Assume we have the image file
    - https://www.dropbox.com/s/nw23q14vzsykyup/Ch01InChap01.dd
    - (from book Guide to Computer Forensics and Investigations. Sixth Edition)
- Software
    - Autopsy : https://www.autopsy.com/download/
- Tasks
    - Recover Word files, images
    - Search key words

Step 1.

Check hash code online : https://emn178.github.io/online-tools/md5_checksum.html



MD5 File Checksum

This MD5 online tool helps you calculate the hash of a file from local or URL using MD5 without uploading the file. It also supports HMAC.

Input

Ch01InChap01.dd

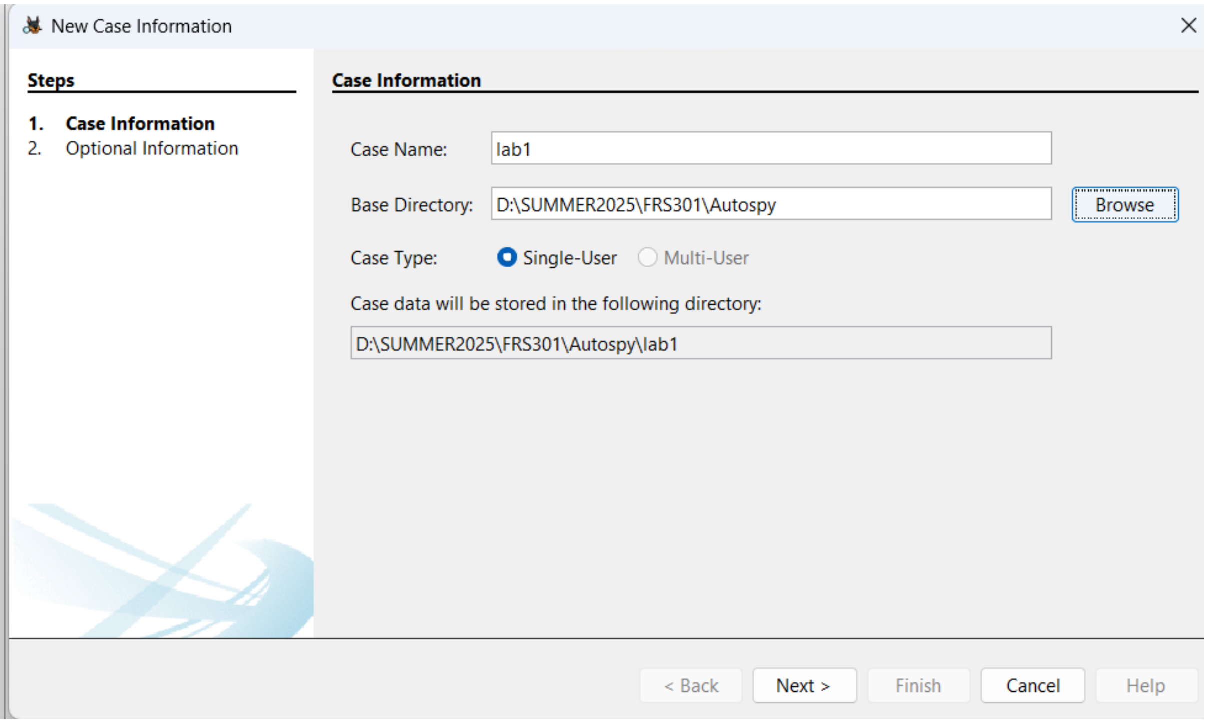
Output

```
a117773bcf1fc88ec0ab8e0a349fbbcb
```

Settings

Step 2.

Create a case with name



Case Information

Case Name: lab1

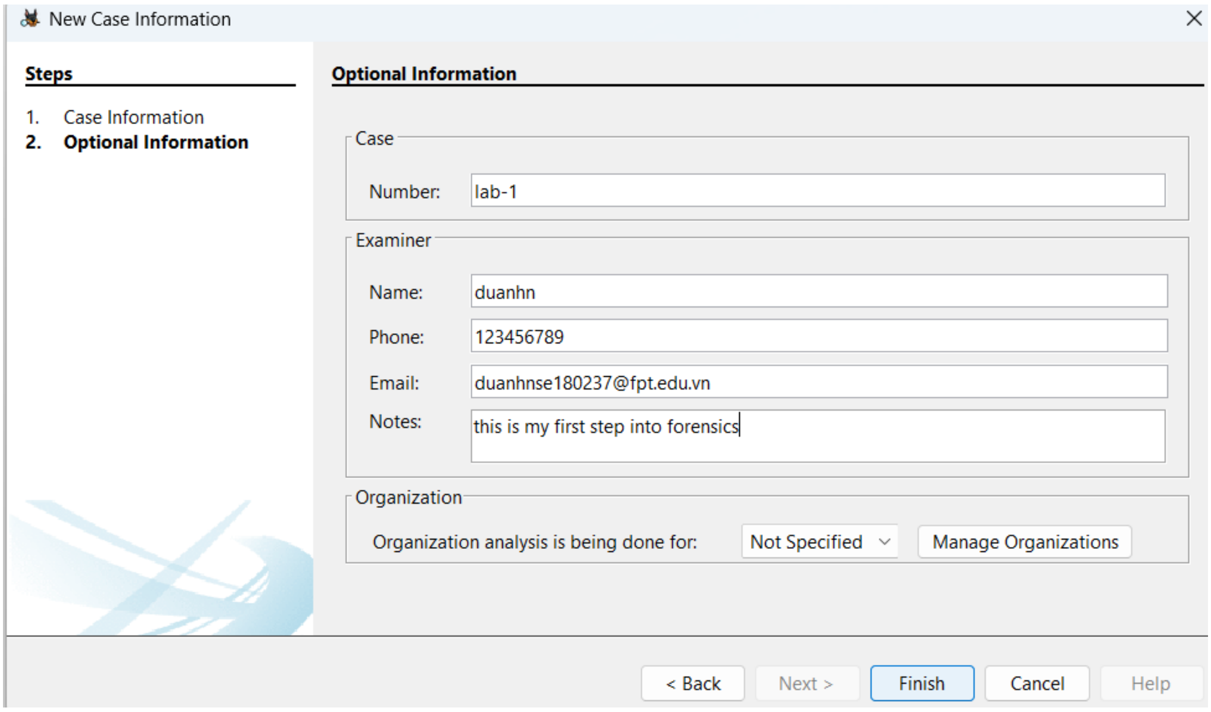
Base Directory: D:\SUMMER2025\FRS301\Autospy

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

D:\SUMMER2025\FRS301\Autospy\lab1

Details of the case



Optional Information

Case

Number: lab-1

Examiner

Name: duanhn

Phone: 123456789

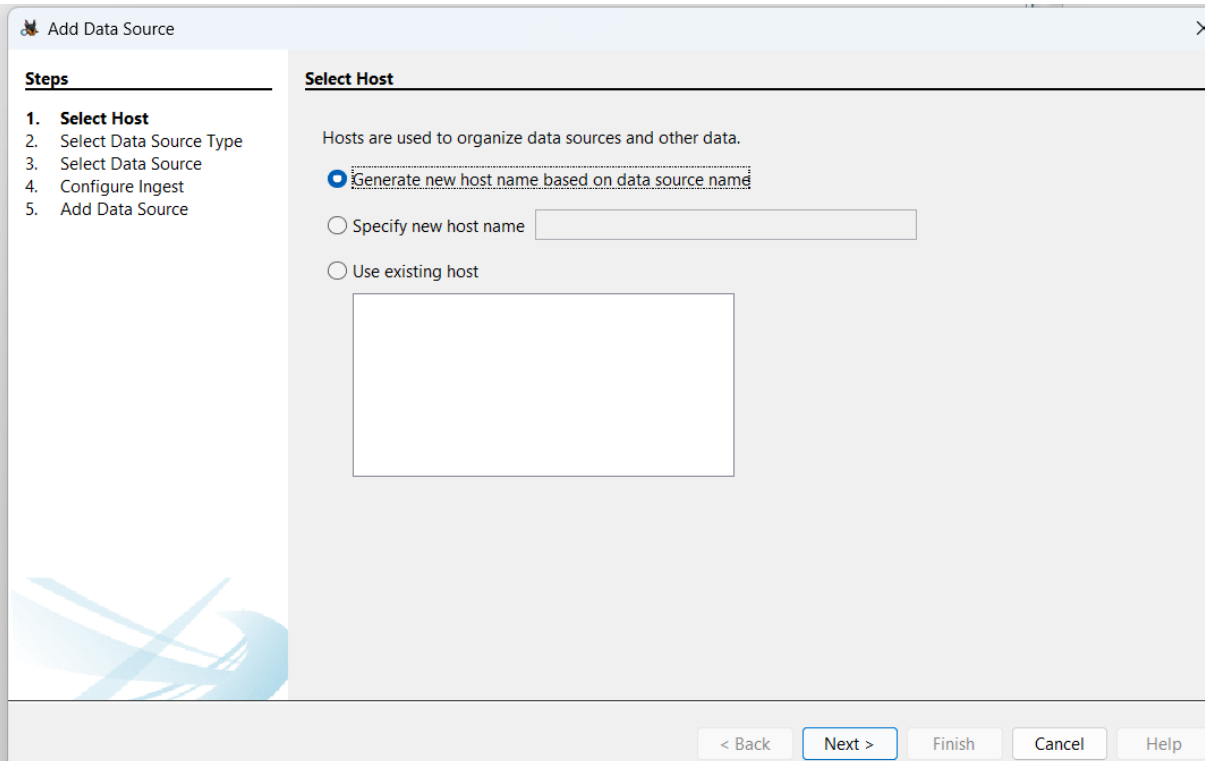
Email: duanhnse180237@fpt.edu.vn

Notes: this is my first step into forensics

Organization

Organization analysis is being done for: Not Specified

Choose Data Format



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

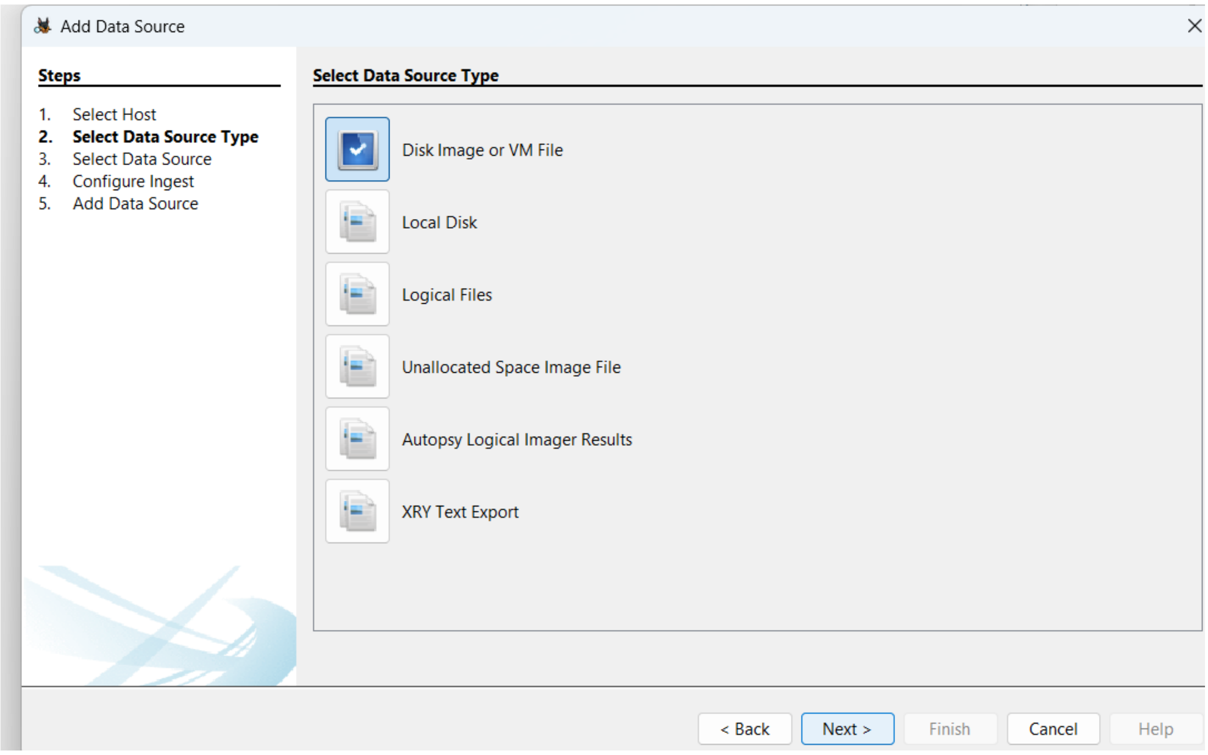
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Click Disk Image or VM File



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

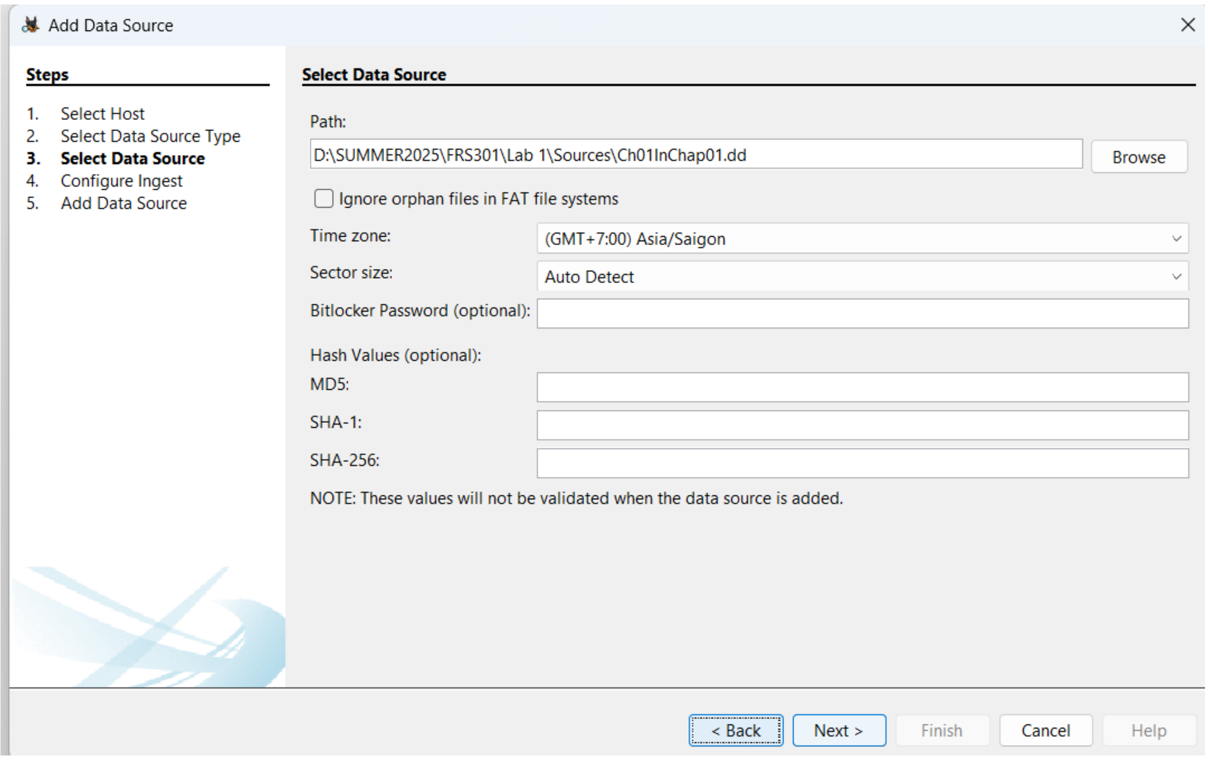
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Choose the image file



Select Data Source

Path: D:\SUMMER2025\FRS301\Lab 1\Sources\Ch01InChap01.dd

□ Ignore orphan files in FAT file systems

Time zone: (GMT+7:00) Asia/Saigon

Sector size: Auto Detect

Bitlocker Password (optional):

Hash Values (optional):

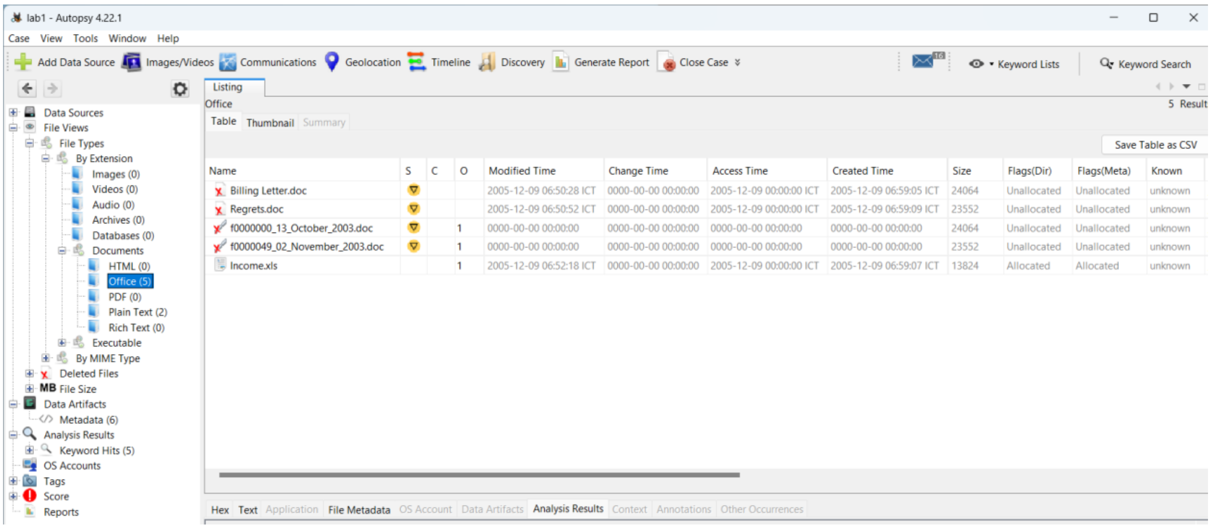
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Find deleted files :

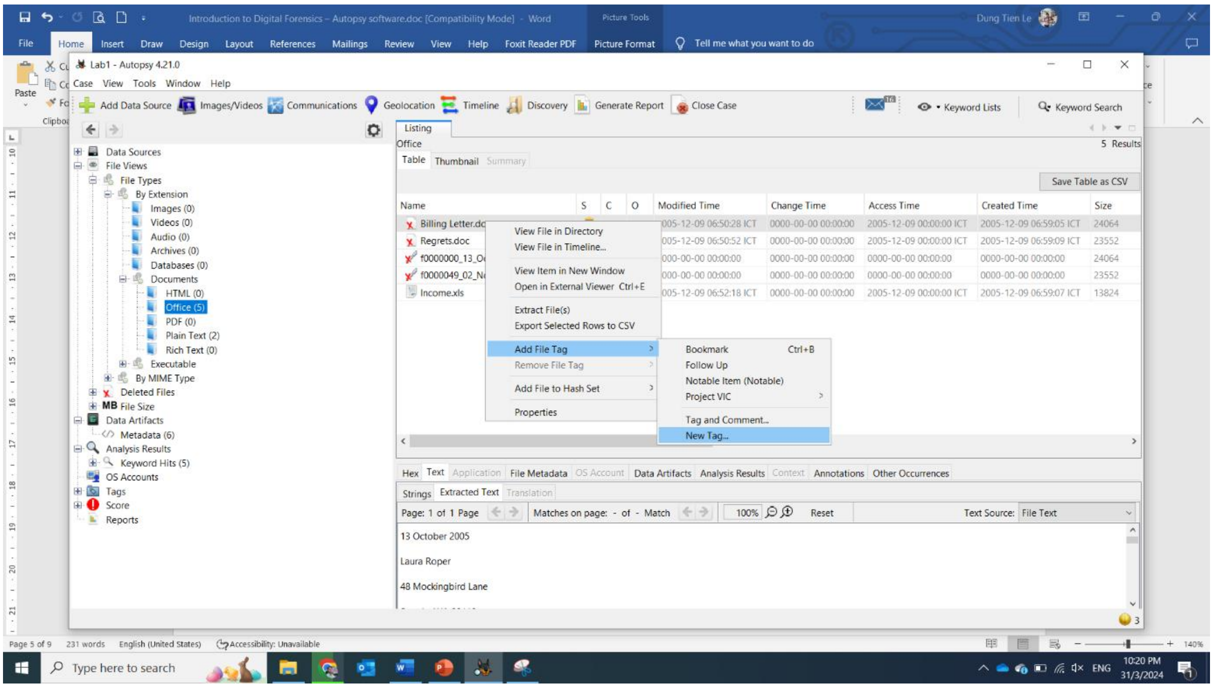


Office

5 Result

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
Billing Letter.doc	▽			2005-12-09 06:50:28 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:05 ICT	24064	Unallocated	Unallocated	unknown
Regrets.doc	▽			2005-12-09 06:50:52 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:09 ICT	23552	Unallocated	Unallocated	unknown
f0000000_13_October_2003.doc	▽		1	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
f0000049_02_November_2003.doc	▽		1	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
Income.xls			1	2005-12-09 06:52:18 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:07 ICT	13824	Allocated	Allocated	unknown

Tag the file: right click and click New Tag



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Billing Letter.dc				005-12-09 06:50:28 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:05 ICT	24064
Regrets.doc				005-12-09 06:50:52 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:09 ICT	23552
f0000000_13_O				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24064
f0000049_02_N				000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552
Income.xls				005-12-09 06:52:18 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:07 ICT	13824

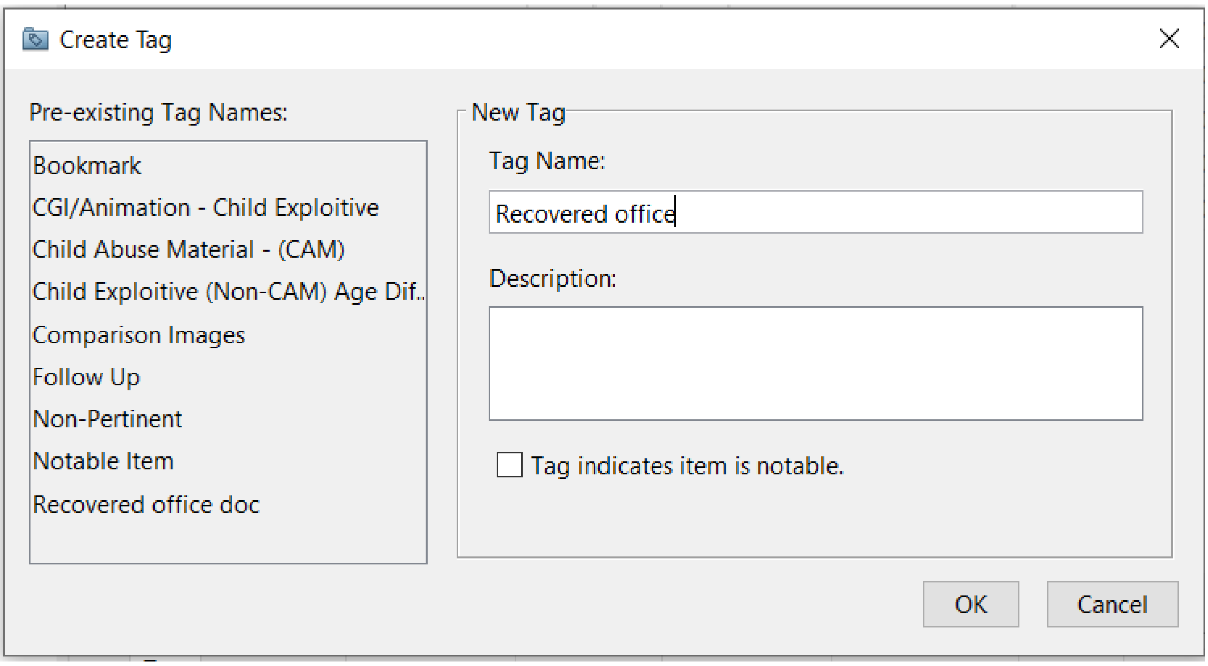
13 October 2005

Laura Roper

48 Mockingbird Lane

Step 3.

Create a tag for reporting



Pre-existing Tag Names:

Bookmark
CGI/Animation - Child Exploitive
Child Abuse Material - (CAM)
Child Exploitive (Non-CAM) Age Dif..
Comparison Images
Follow Up
Non-Pertinent
Notable Item
Recovered office doc

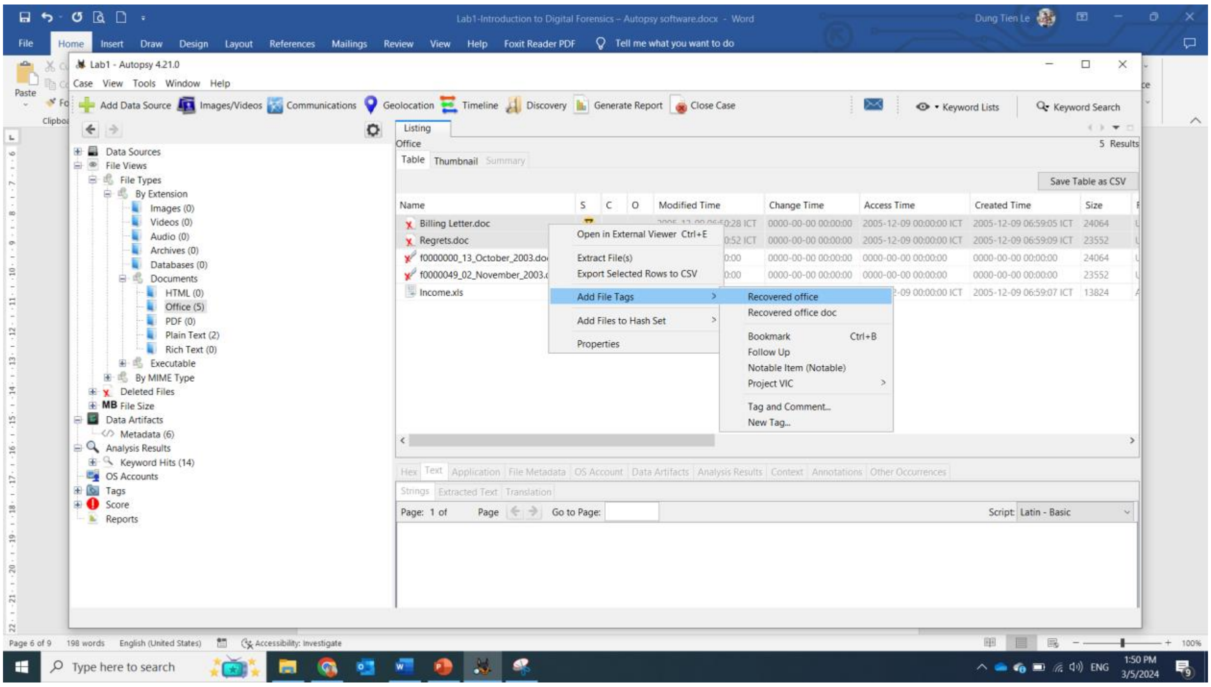
New Tag

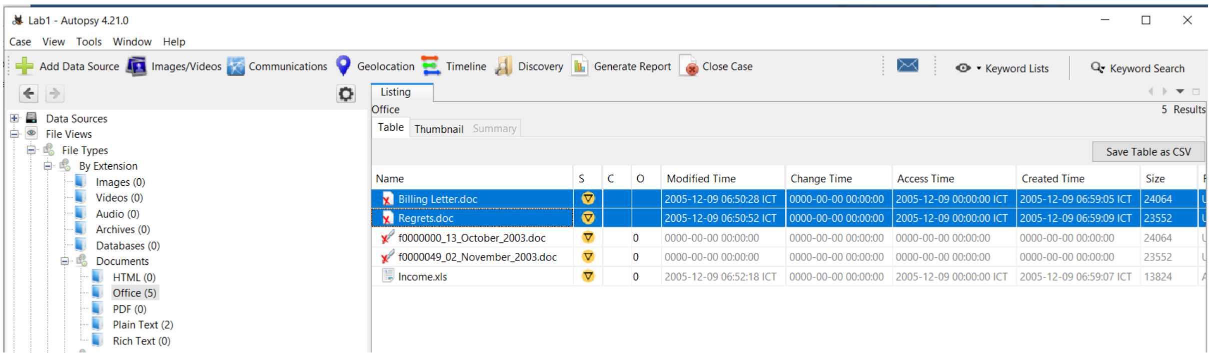
Tag Name: Recovered office

Description:

☐ Tag indicates item is notable.

Tag both deleted files

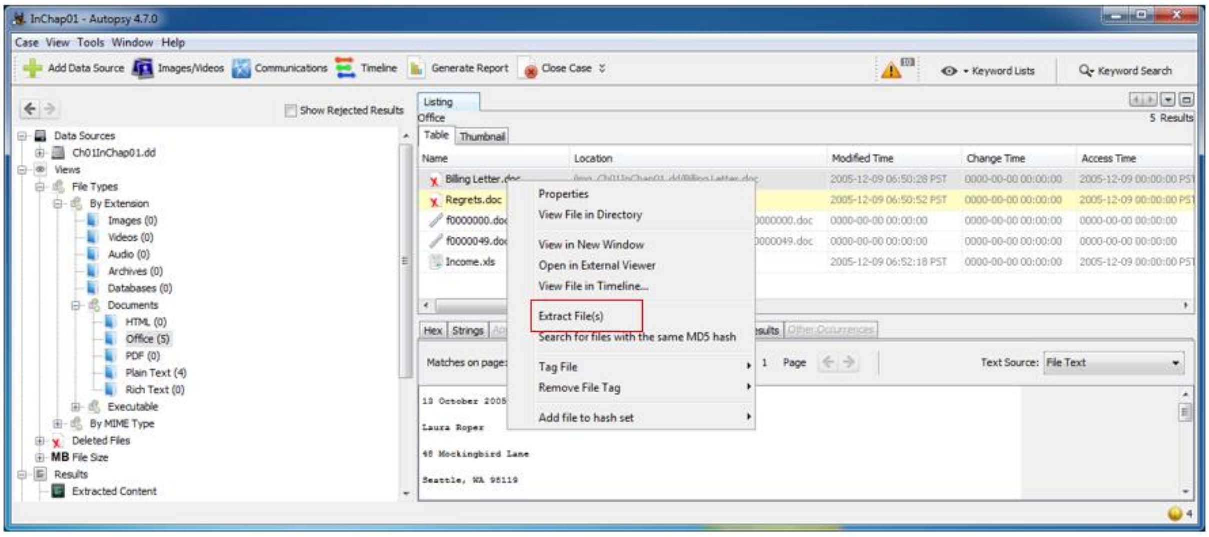




Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Billing Letter.doc				2005-12-09 06:50:28 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:05 ICT	24064
Regrets.doc				2005-12-09 06:50:52 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:09 ICT	23552
f0000000_13_October_2003.doc			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
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
Income.xls			0	2005-12-09 06:52:18 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:07 ICT	13824

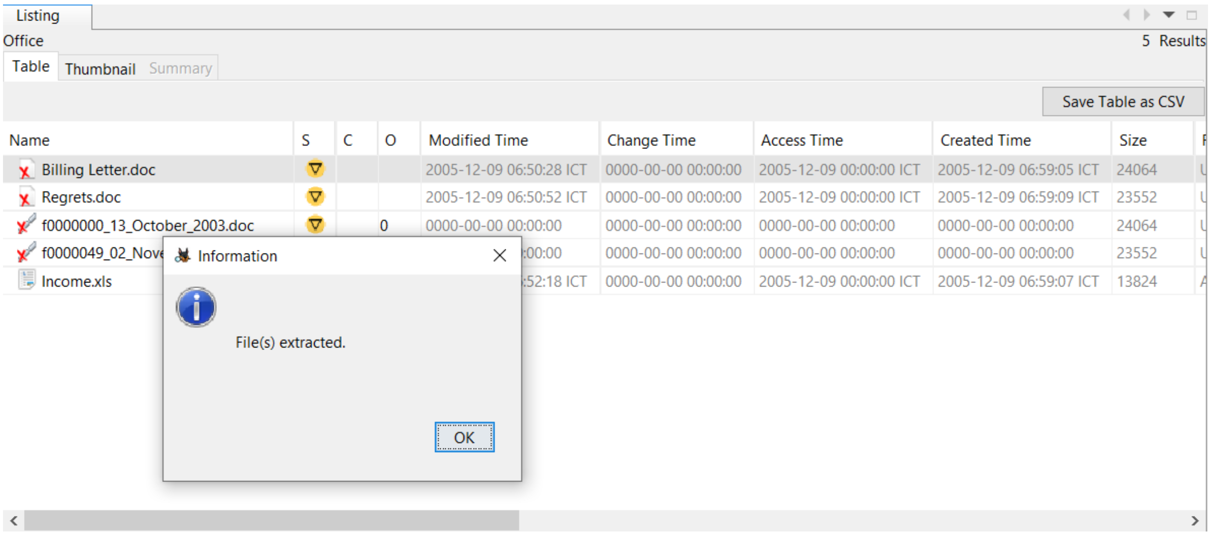
Step 4.

Recover deleted file



Name	Location	Modified Time	Change Time	Access Time
Billing Letter.doc	/img_Ch01InChap01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Regrets.doc		2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
f0000000.doc	0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000049.doc	0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Income.xls		2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST

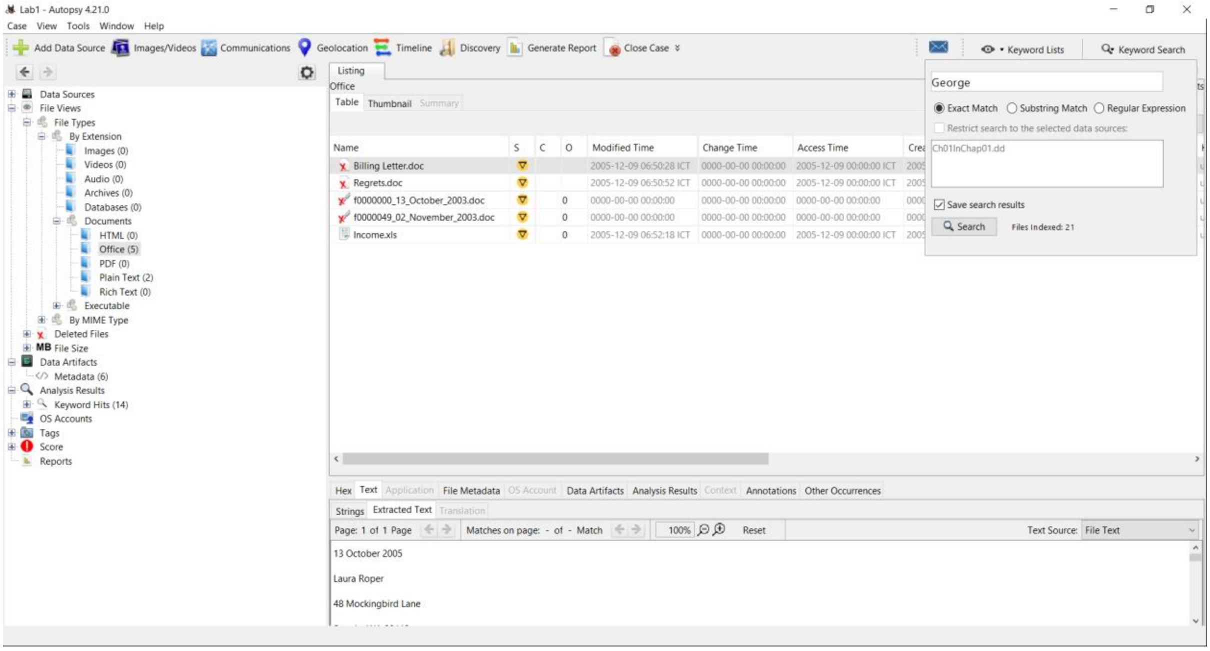
```
13 October 2005
Laura Roper
48 Mockingbird Lane
Seattle, WA 98119
```



File(s) extracted.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Billing Letter.doc	▽			2005-12-09 06:50:28 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:05 ICT	24064
Regrets.doc	▽			2005-12-09 06:50:52 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:09 ICT	23552
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
f0000049_02_Nove				:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552
Income.xls				:52:18 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005-12-09 06:59:07 ICT	13824

Search keywords : **"George"**



George

● Exact Match ○ Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

Ch01InChap01.dd

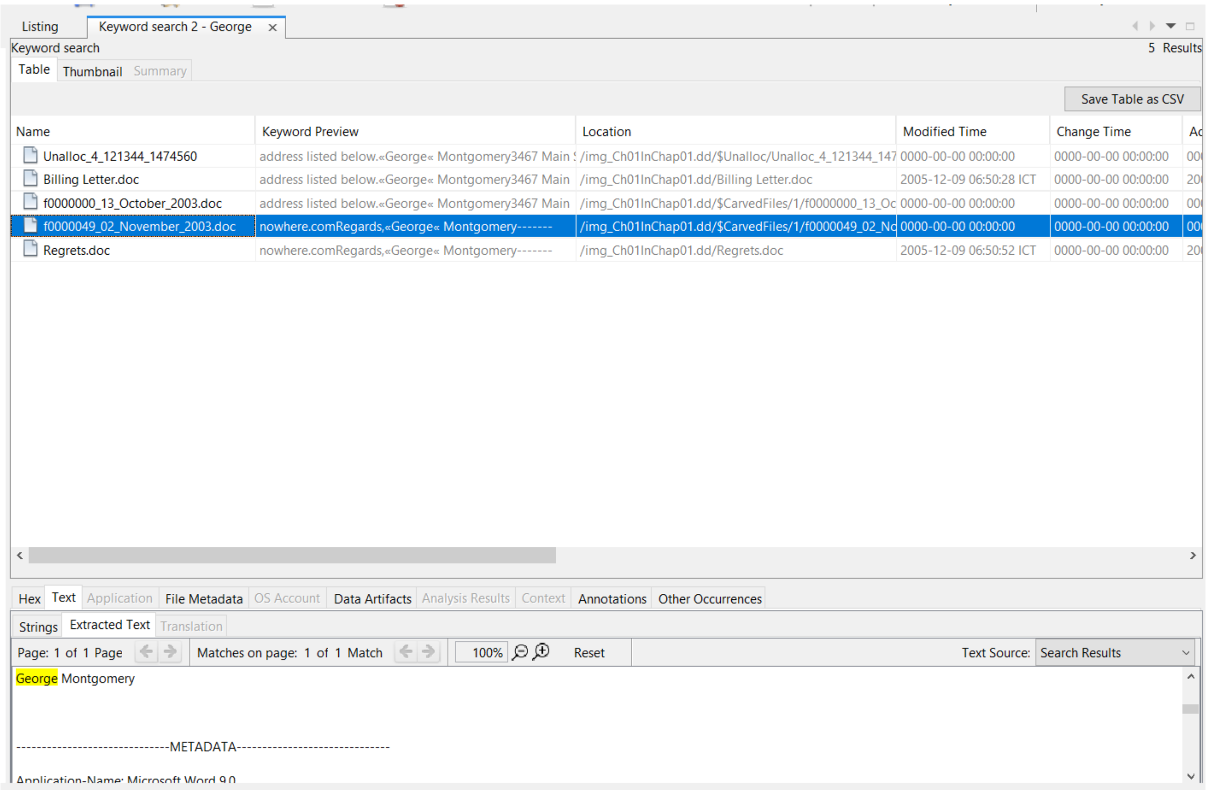
☑ Save search results

Search Files Indexed: 21

Name	S	C	O	Modified Time	Change Time	Access Time	Crea
Billing Letter.doc	▽			2005-12-09 06:50:28 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005
Regrets.doc	▽			2005-12-09 06:50:52 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005
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
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
Income.xls	▽		0	2005-12-09 06:52:18 ICT	0000-00-00 00:00:00	2005-12-09 00:00:00 ICT	2005

```
13 October 2005
Laura Roper
48 Mockingbird Lane
```

Search results



Name	Keyword Preview	Location	Modified Time	Change Time	Ac
Unalloc_4_121344_1474560	address listed below.«George« Montgomery3467 Main !	/img_Ch01InChap01.dd/$Unalloc/Unalloc_4_121344_147	0000-00-00 00:00:00	0000-00-00 00:00:00	00
Billing Letter.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap01.dd/Billing Letter.doc	2005-12-09 06:50:28 ICT	0000-00-00 00:00:00	20
f0000000_13_October_2003.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000000_13_Oc	0000-00-00 00:00:00	0000-00-00 00:00:00	00
f0000049_02_November_2003.doc	nowhere.comRegards,«George« Montgomery-------	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000049_02_Nc	0000-00-00 00:00:00	0000-00-00 00:00:00	00
Regrets.doc	nowhere.comRegards,«George« Montgomery-------	/img_Ch01InChap01.dd/Regrets.doc	2005-12-09 06:50:52 ICT	0000-00-00 00:00:00	20

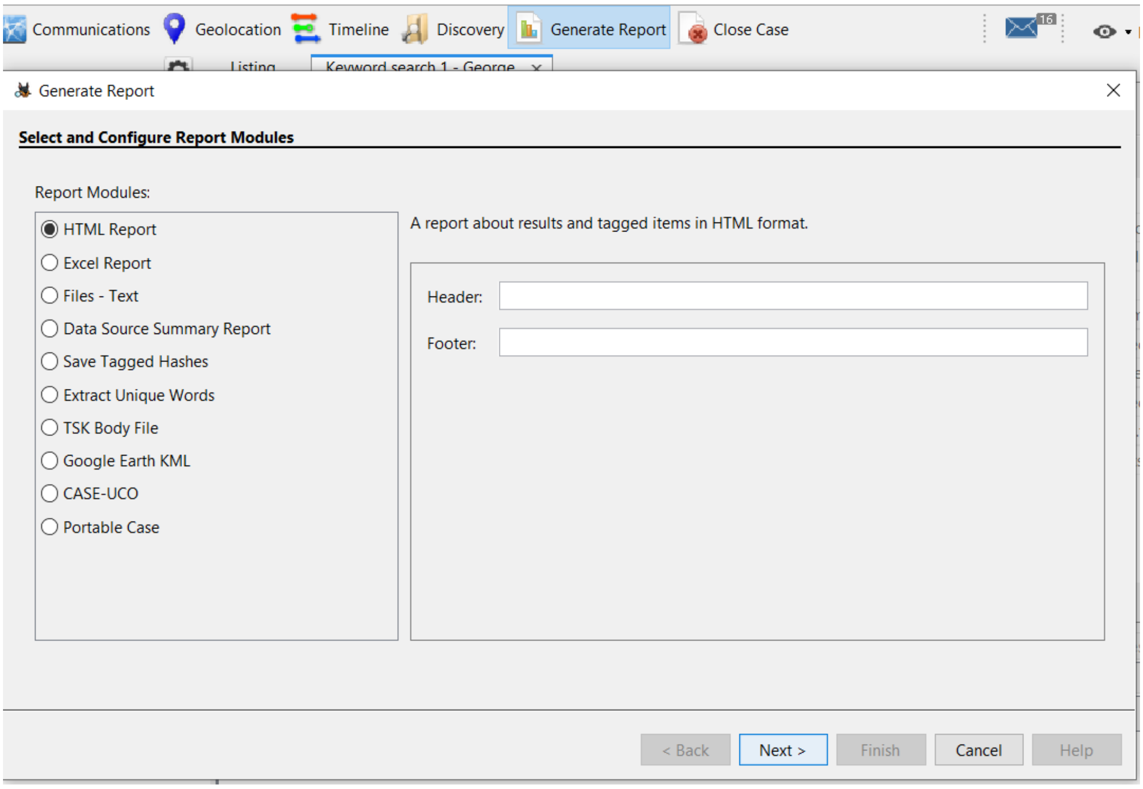
George Montgomery

-----------------------------METADATA-----------------------------

Application-Name: Microsoft Word 9.0

Step 5.

Generate reports



Select and Configure Report Modules

Report Modules:

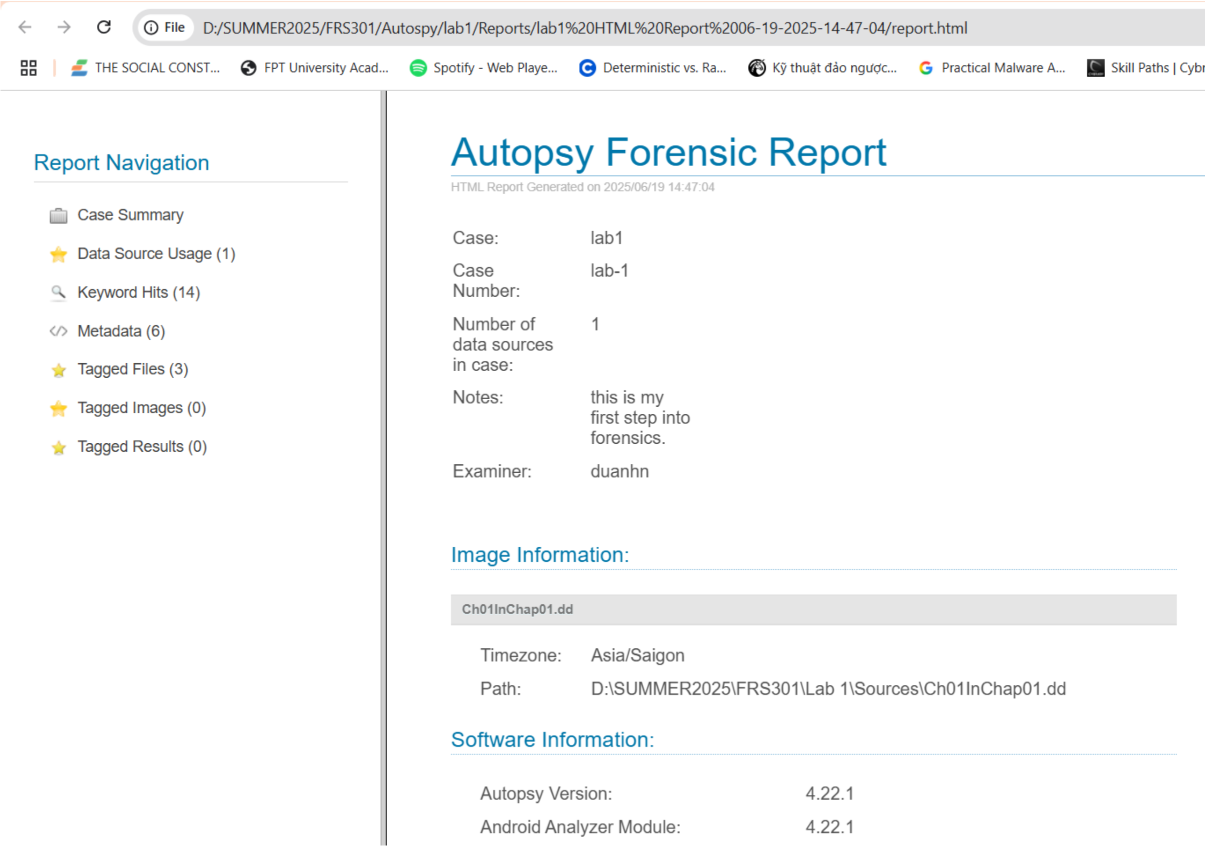
● HTML Report
○ Excel Report
○ Files - Text
○ Data Source Summary Report
○ Save Tagged Hashes
○ Extract Unique Words
○ TSK Body File
○ Google Earth KML
○ CASE-UCO
○ Portable Case

A report about results and tagged items in HTML format.

Header:

Footer:

Open or Save as file doc is recovered.



Report Navigation

- Case Summary
- Data Source Usage (1)
- Keyword Hits (14)
- Metadata (6)
- Tagged Files (3)
- Tagged Images (0)
- Tagged Results (0)

Autopsy Forensic Report

HTML Report Generated on 2025/06/19 14:47:04

Case:	lab1
Case Number:	lab-1
Number of data sources in case:	1
Notes:	this is my first step into forensics.
Examiner:	duanhn

Image Information:

Ch01InChap01.dd

Timezone:	Asia/Saigon
Path:	D:\SUMMER2025\FRS301\Lab 1\Sources\Ch01InChap01.dd

Software Information:

Autopsy Version:	4.22.1
Android Analyzer Module:	4.22.1

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 1.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 1 From YOUR NAME**", replacing "YOUR NAME" with your real name.