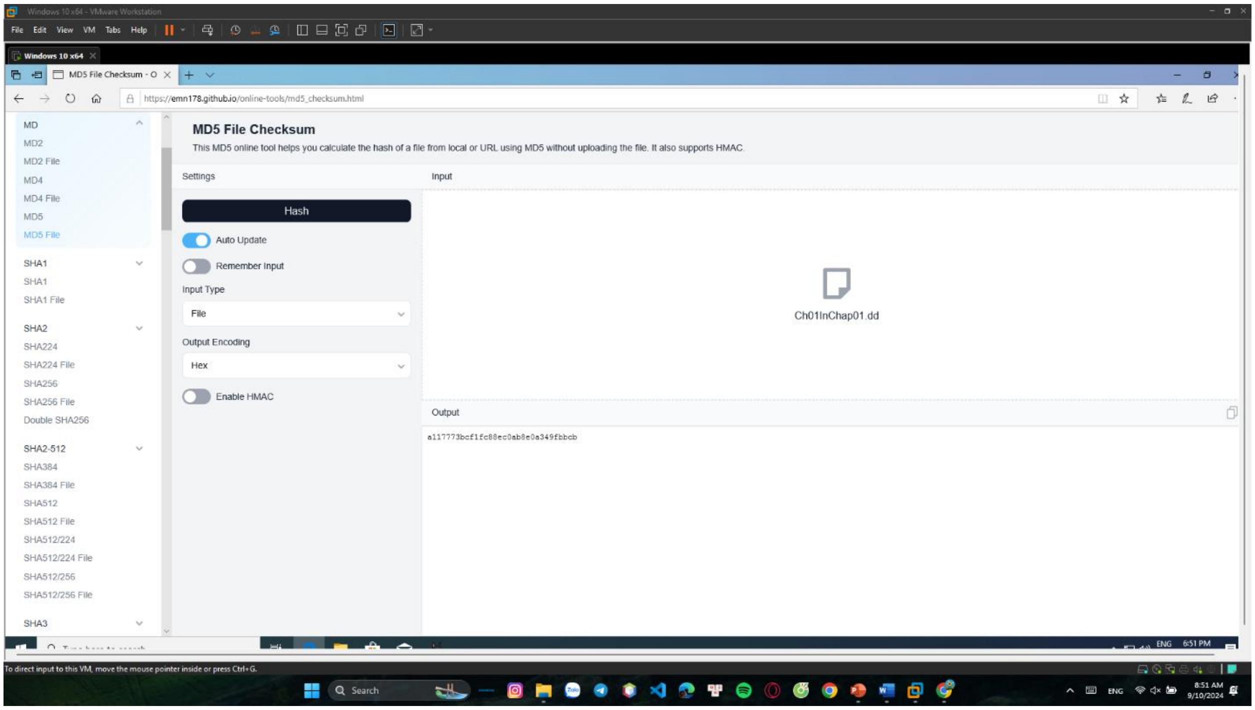
Lab 1: Introduction to Digital Forensics – Autopsy software

Group CyberNOOb :

- Hồ Tài Liên Vy Kha
- Huỳnh Ngọc Quang
- Phạm Thành Long
- Nguyễn Lê Hoàng Thông
- Hoàng Kim Long

Step 1.

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



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.

Settings

- Auto Update: on
- Remember Input: off
- Input Type: File
- Output Encoding: Hex
- Enable HMAC: off

Input: Ch01InChap01.dd

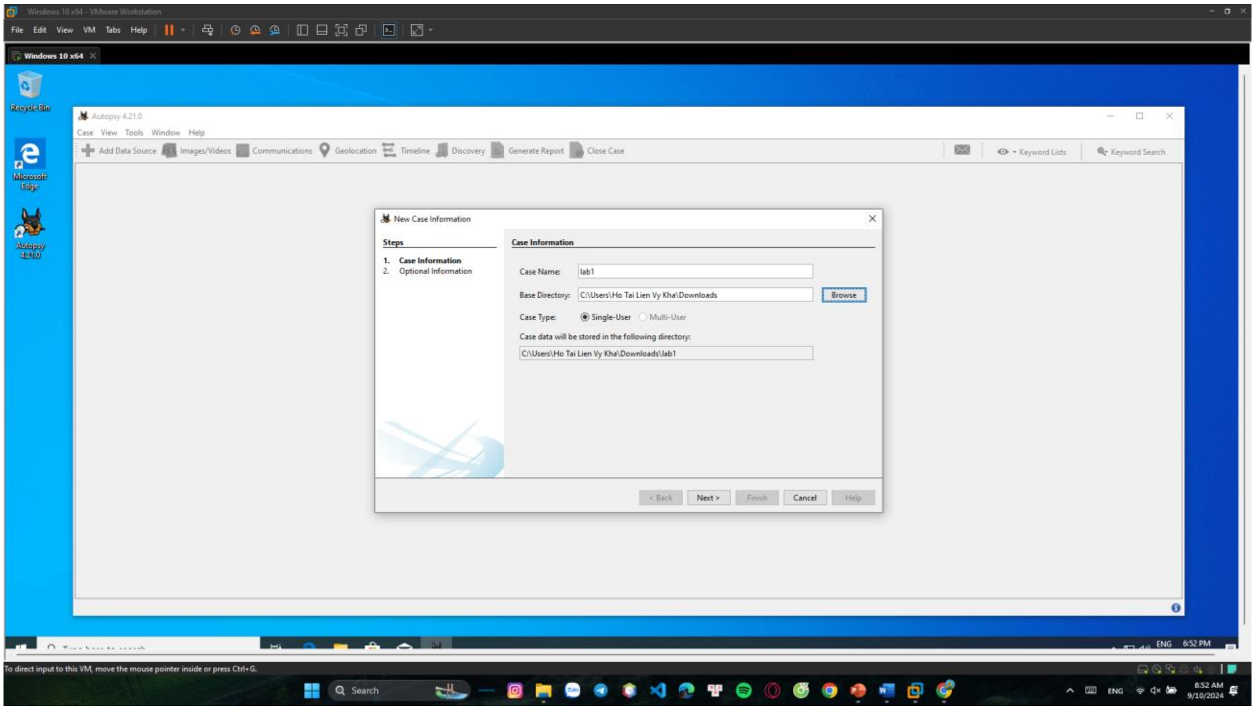
Output

```
a117773bcf1fc88ec0ab8e0a349fbbcb
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 2.

Create a case with name



New Case Information

Case Information

Case Name: lab1

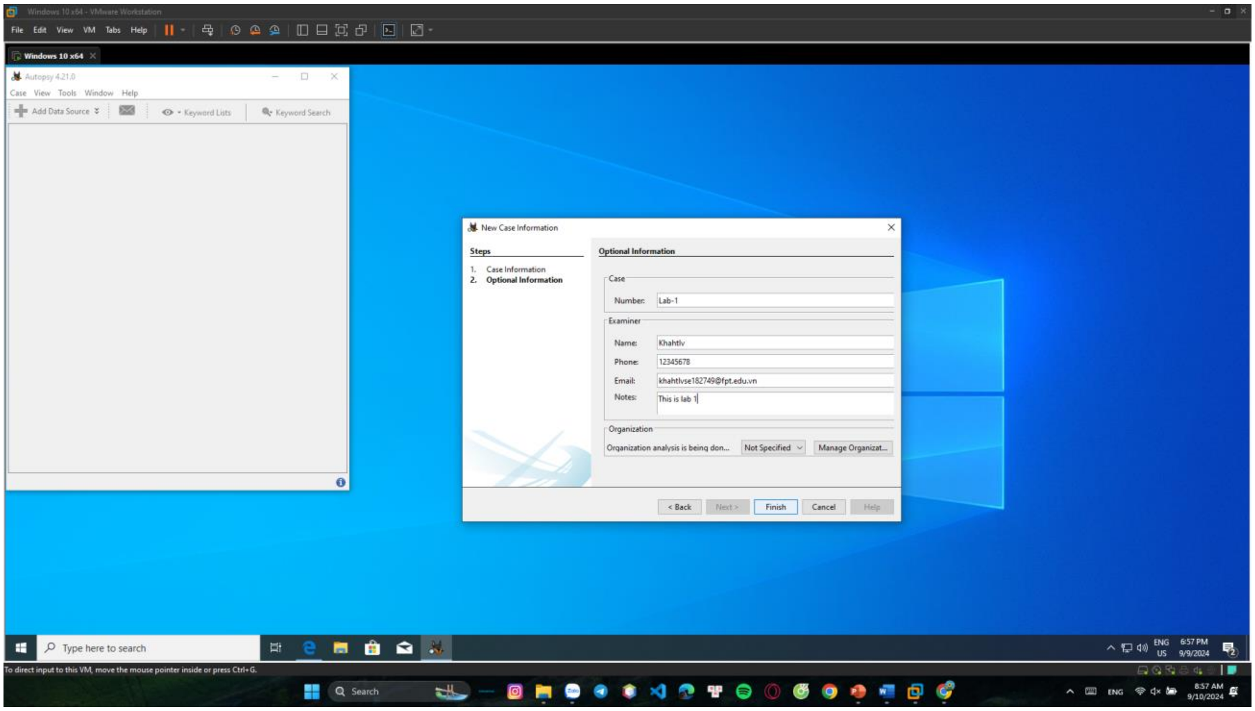
Base Directory: C:\Users\Ho Tai Lien Vy Kha\Downloads

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\Ho Tai Lien Vy Kha\Downloads\lab1

Details of the case



New Case Information

Optional Information

Case

Number: Lab-1

Examiner

Name: Khahtlv

Phone: 12345678

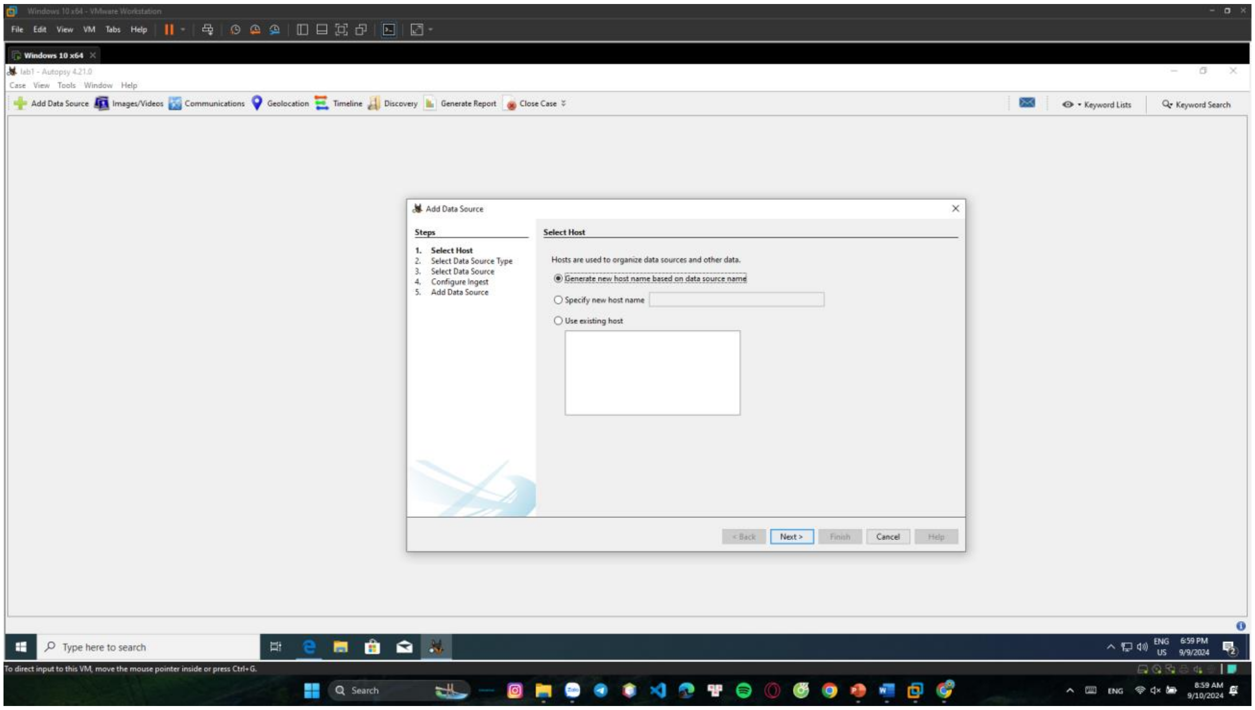
Email: khahtlvse182749@fpt.edu.vn

Notes: This is lab 1

Organization

Organization analysis is being don... Not Specified

Choose Data Format



Steps

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

Select Host

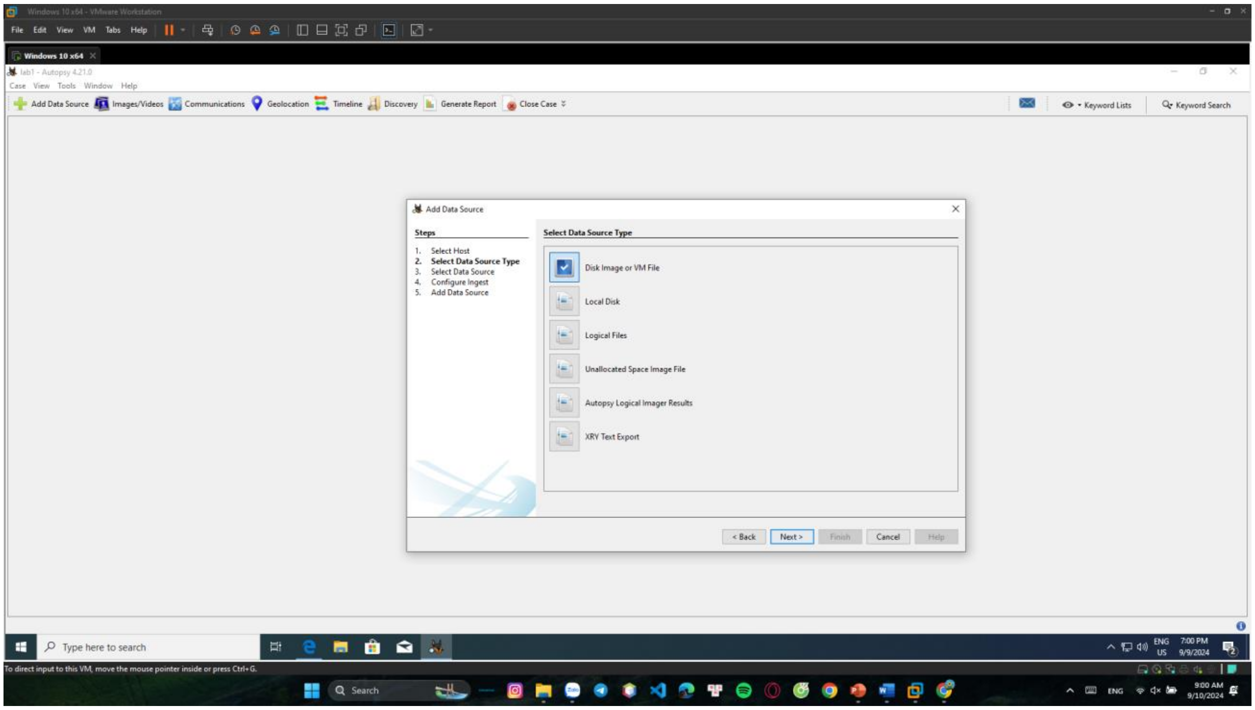
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Click Disk Image or VM File



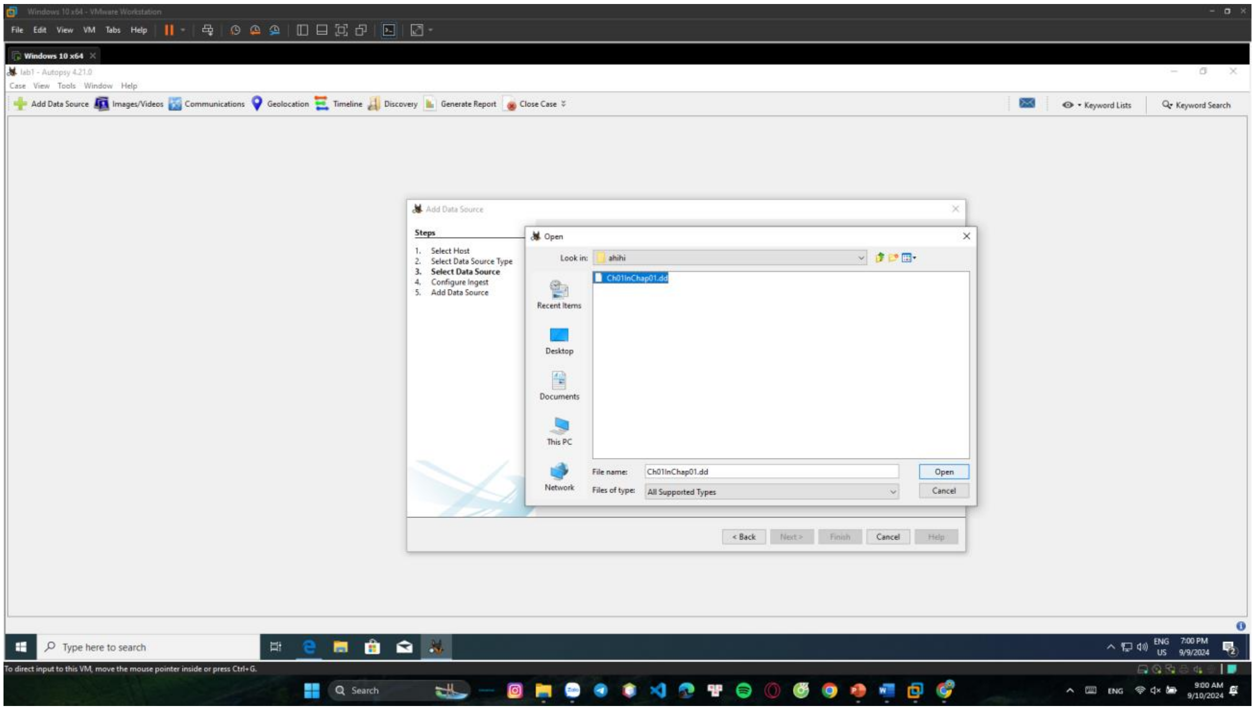
Steps

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

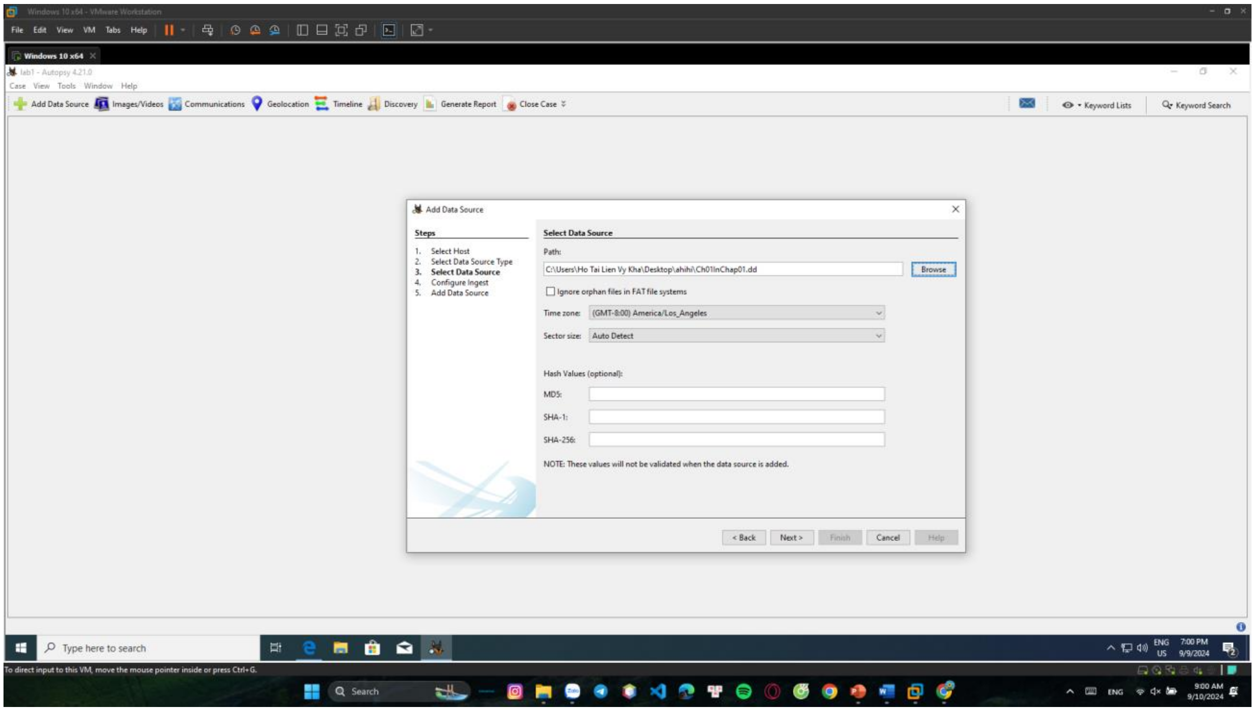


Look in: ahihi

Ch01InChap01.dd

File name: Ch01InChap01.dd

Files of type: All Supported Types



Select Data Source

Path: C:\Users\Ho Tai Lien Vy Kha\Desktop\ahihi\Ch01InChap01.dd

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

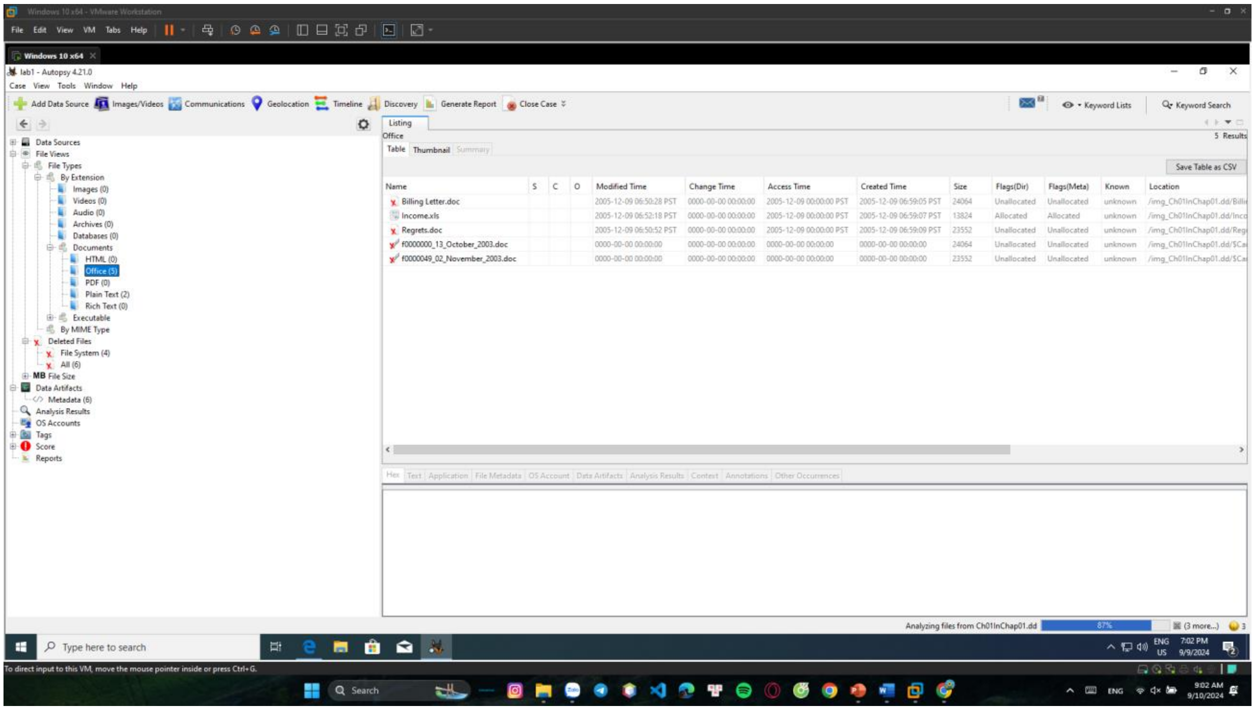
MD5:

SHA-1:

SHA-256:

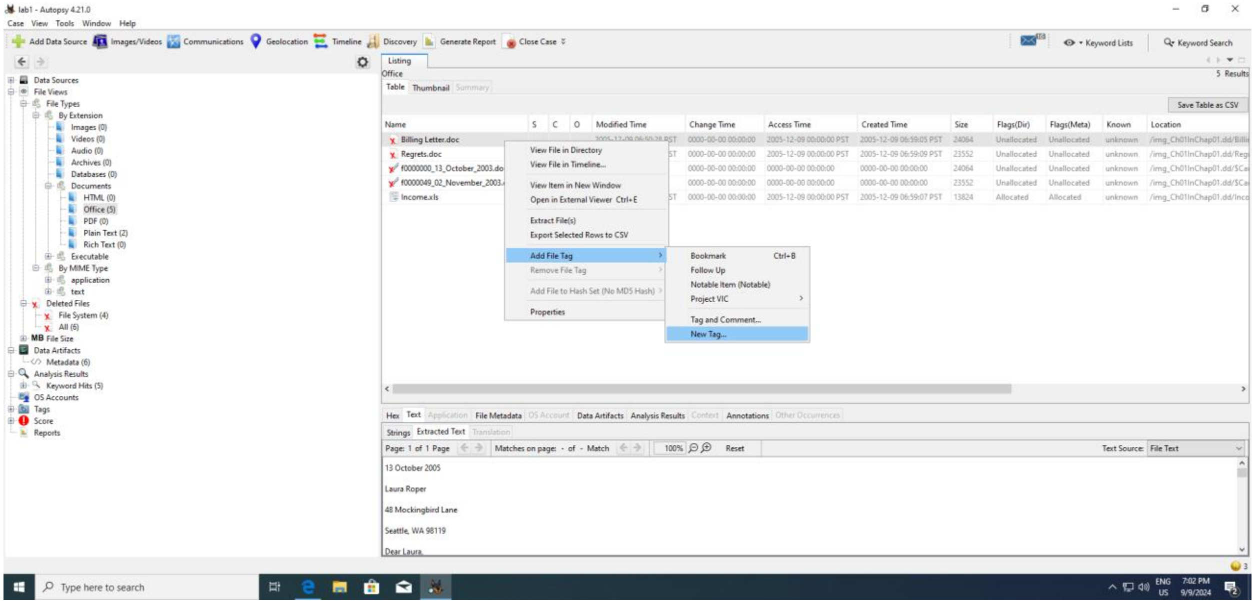
NOTE: These values will not be validated when the data source is added.

Find deleted files :



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 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Billi
Income.xls				2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:07 PST	13824	Allocated	Allocated	unknown	/img_Ch01InChap01.dd/Inco
Regrets.doc				2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Reg
f0000000_13_October_2003.doc				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/$Ca
f0000049_02_November_2003.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/$Ca

Tag the file: right click and click New Tag



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 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Billi
Regrets.doc				ST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Reg
f0000000_13_October_2003.do					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/$Ca
f0000049_02_November_2003.					0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/$Ca
Income.xls				ST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:07 PST	13824	Allocated	Allocated	unknown	/img_Ch01InChap01.dd/Inco

13 October 2005

Laura Roper

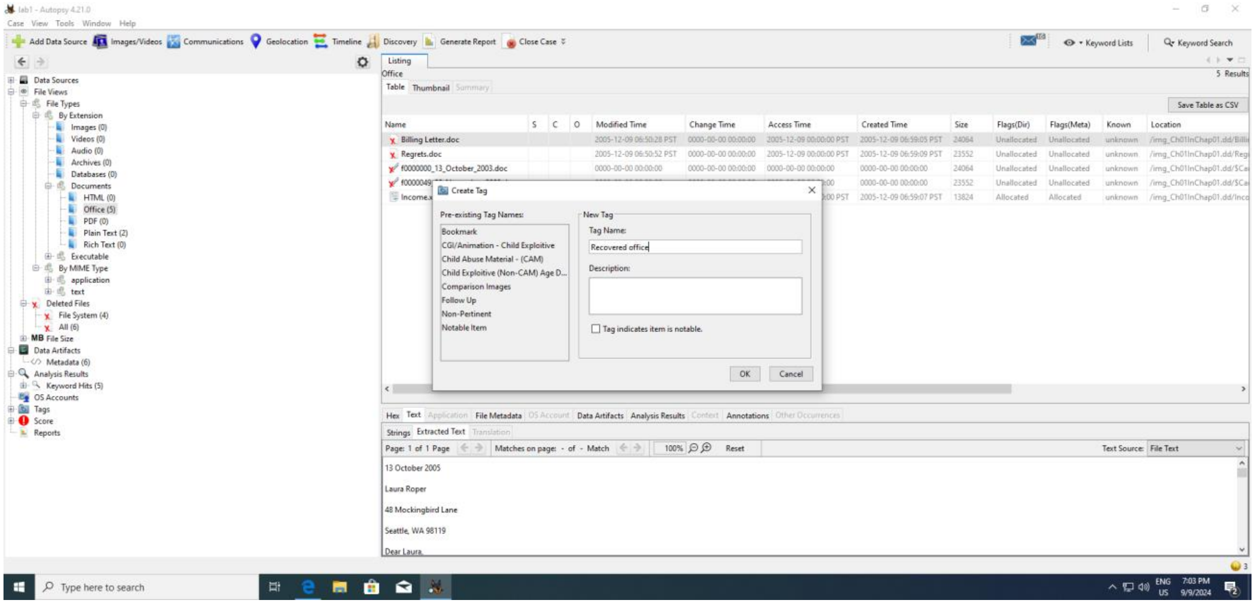
48 Mockingbird Lane

Seattle, WA 98119

Dear Laura,

Step 3.

Create a tag for reporting



Office 5 Results

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 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Billi
Regrets.doc				2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Reg
f0000000_13_October_2003.doc				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/$Ca
f0000049						:00	0000-00-00 00:00:00	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/$Ca
Income.x						:00 PST	2005-12-09 06:59:07 PST	13824	Allocated	Allocated	unknown	/img_Ch01InChap01.dd/Inco

Create Tag

Pre-existing Tag Names:

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

New Tag

Tag Name: Recovered office

Description:

☐ Tag indicates item is notable.

OK Cancel

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

13 October 2005

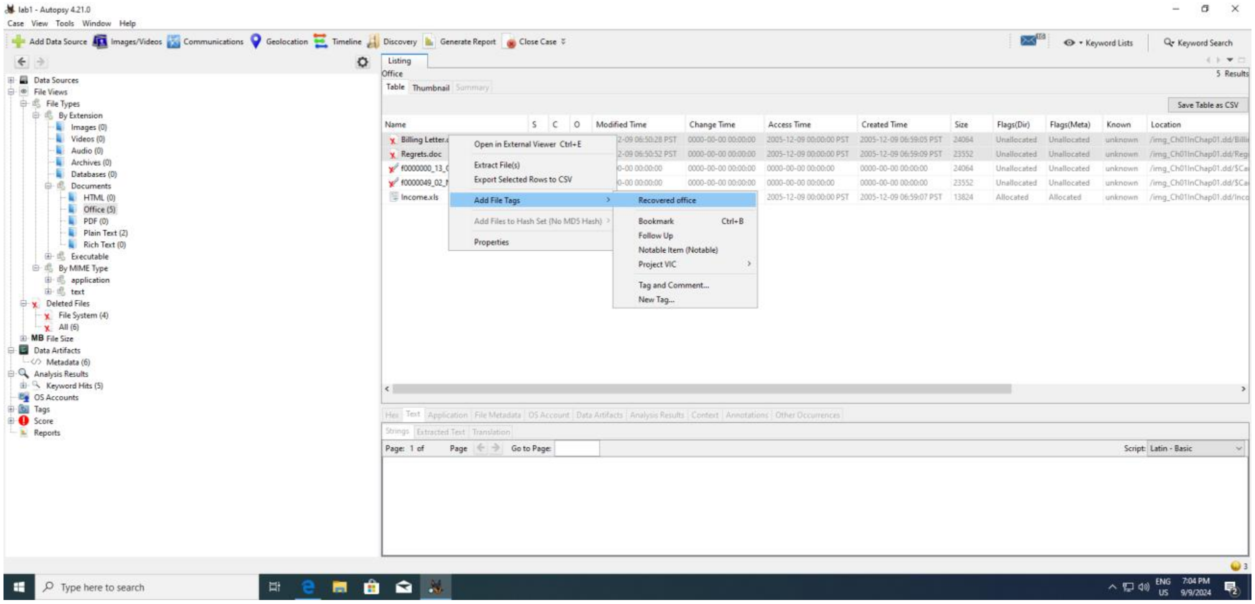
Laura Roper

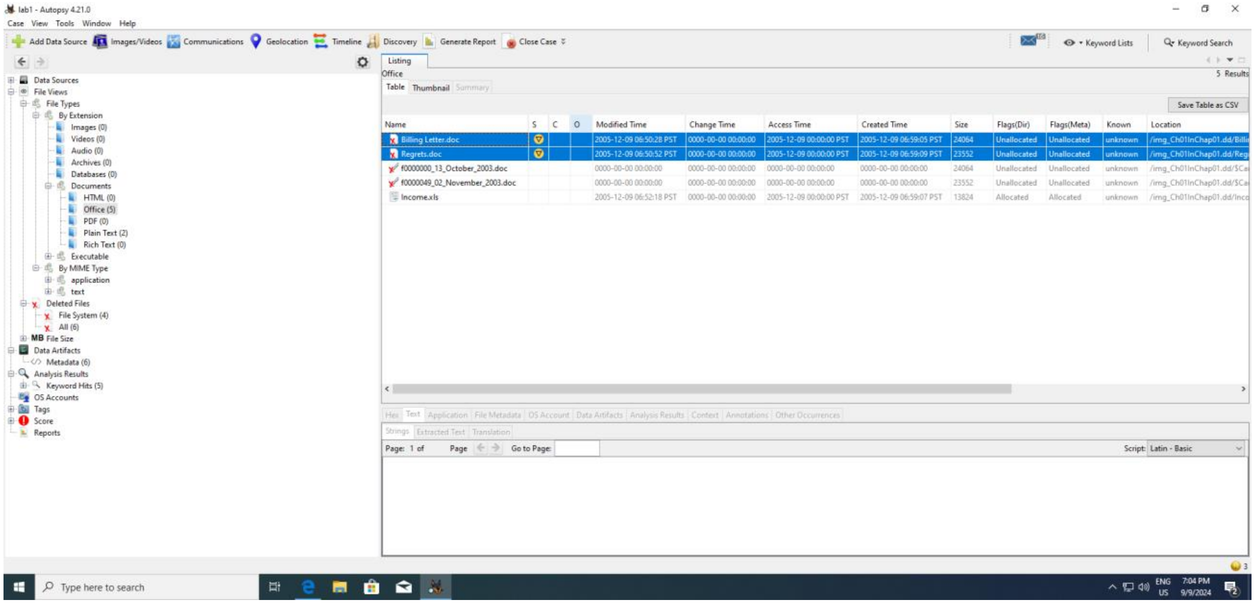
48 Mockingbird Lane

Seattle, WA 98119

Dear Laura,

Tag both deleted files

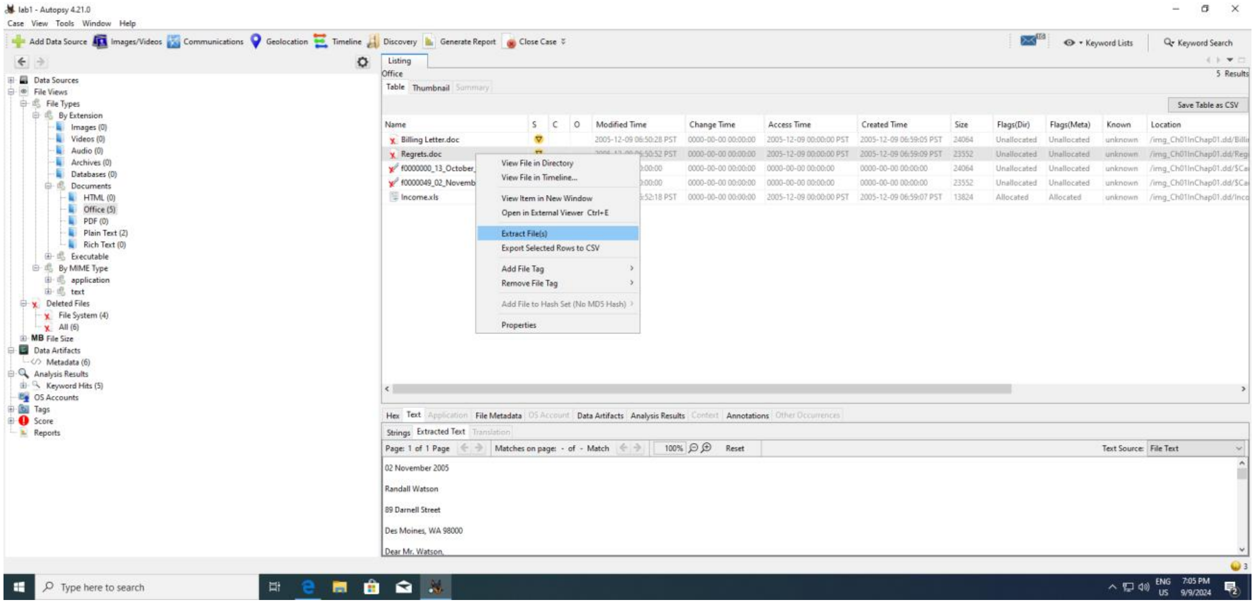




Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Billing Letter.doc	▽			2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Billi
Regrets.doc	▽			2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Reg
f0000000_13_October_2003.doc				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/$Ca
f0000049_02_November_2003.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/$Ca
Income.xls				2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:07 PST	13824	Allocated	Allocated	unknown	/img_Ch01InChap01.dd/Inco

Step 4.

Recover deleted file



Office — 5 Results

Page: 1 of 1 Page · Matches on page: - of - Match · 100% · Text Source: File Text

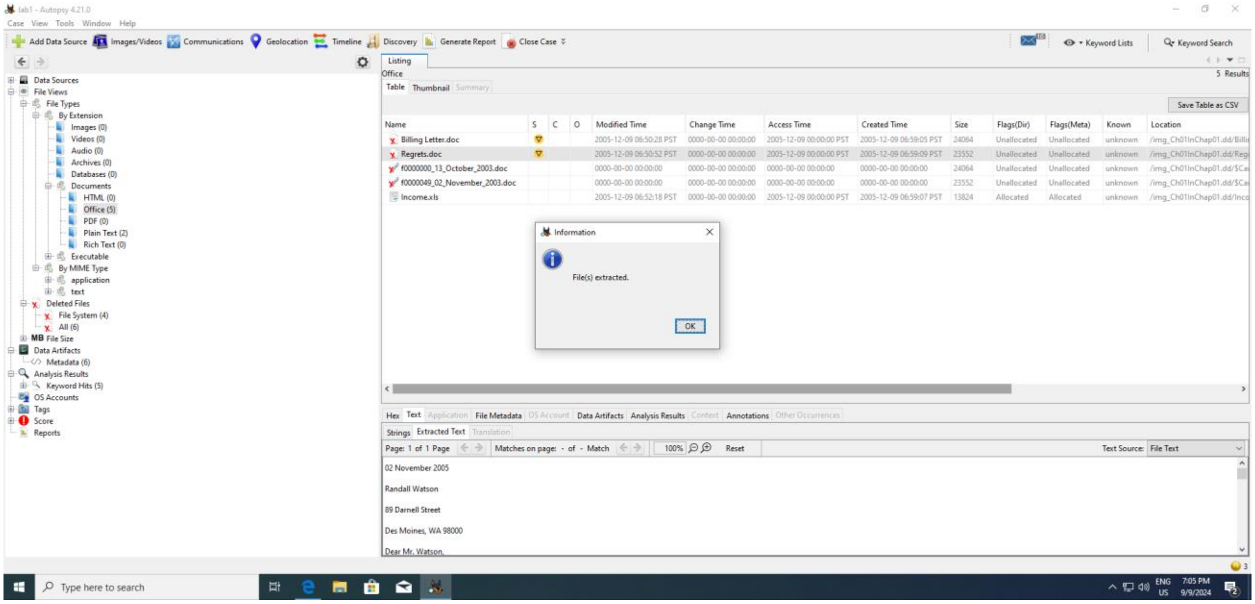
02 November 2005

Randall Watson

89 Darnell Street

Des Moines, WA 98000

Dear Mr. Watson,



Office — 5 Results

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 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Billi
Regrets.doc	▽			2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/Reg
f0000000_13_October_2003.doc				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/$Ca
f0000049_02_November_2003.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552	Unallocated	Unallocated	unknown	/img_Ch01InChap01.dd/$Ca
Income.xls				2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:07 PST	13824	Allocated	Allocated	unknown	/img_Ch01InChap01.dd/Inco

File(s) extracted.

Page: 1 of 1 Page · Matches on page: - of - Match · 100% · Text Source: File Text

02 November 2005

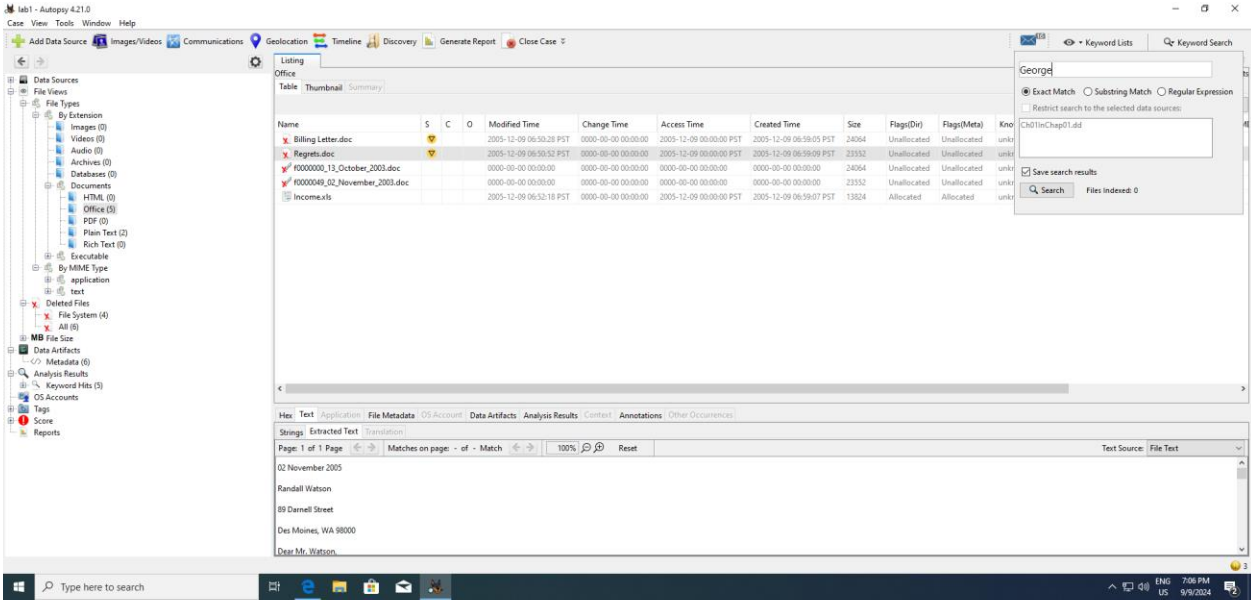
Randall Watson

89 Darnell Street

Des Moines, WA 98000

Dear Mr. Watson,

Search keywords : **“George”**



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

George

● Exact Match ○ Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

Ch01InChap01.dd

☑ Save search results

Search Files Indexed: 0

02 November 2005

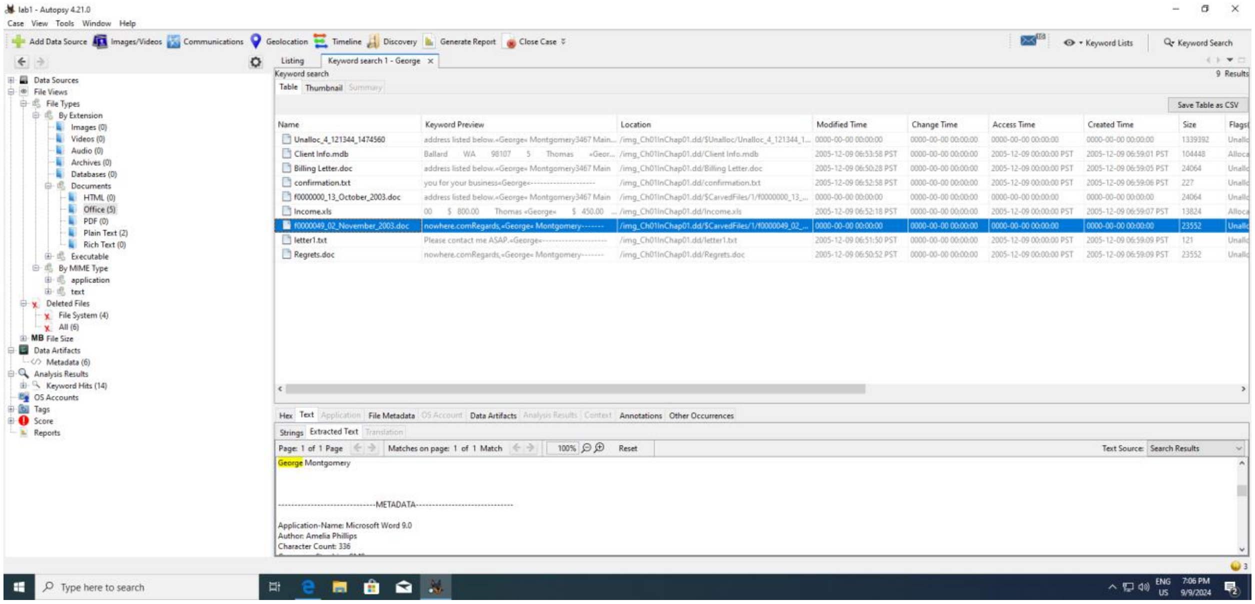
Randall Watson

89 Darnell Street

Des Moines, WA 98000

Dear Mr. Watson,

Search results



Keyword search

Table Thumbnail Summary

9 Results

Save Table as CSV

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(
Unalloc_4_121344_1474560	address listed below.«George« Montgomery3467 Main...	/img_Ch01InChap01.dd/$Unalloc/Unalloc_4_121344_1...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1339392	Unallo
Client Info.mdb	Ballard WA 98107 5 Thomas «Geor...	/img_Ch01InChap01.dd/Client Info.mdb	2005-12-09 06:53:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:01 PST	104448	Alloca
Billing Letter.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	Unallo
confirmation.txt	you for your business«George«--------------------	/img_Ch01InChap01.dd/confirmation.txt	2005-12-09 06:52:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:06 PST	227	Unallo
f0000000_13_October_2003.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000000_13_...	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	Unallo
Income.xls	00 $ 800.00 Thomas «George« $ 450.00 ...	/img_Ch01InChap01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:07 PST	13824	Alloca
f0000049_02_November_2003.doc	nowhere.comRegards,«George« Montgomery-------	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000049_02_...	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	Unallo
letter1.txt	Please contact me ASAP.«George«--------------------	/img_Ch01InChap01.dd/letter1.txt	2005-12-09 06:51:50 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	121	Unallo
Regrets.doc	nowhere.comRegards,«George« Montgomery-------	/img_Ch01InChap01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	Unallo

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

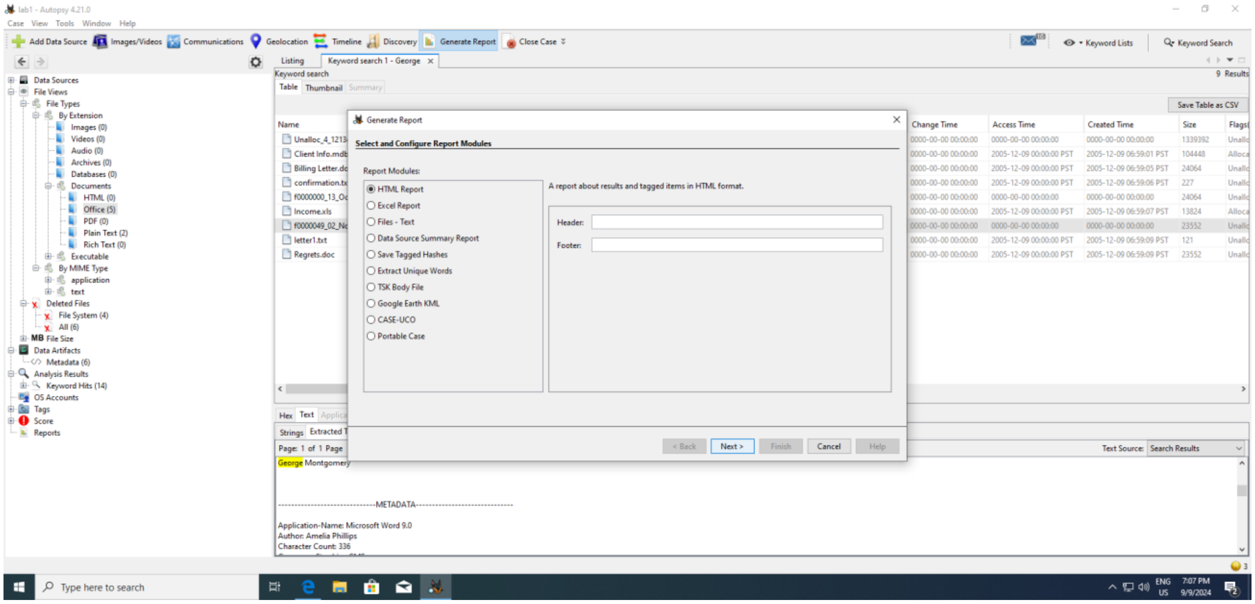
Strings | Extracted Text | Translation

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

```
George Montgomery



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

Application-Name: Microsoft Word 9.0
Author: Amelia Phillips
Character Count: 336
```

Step 5.

Generate reports



Generate Report

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

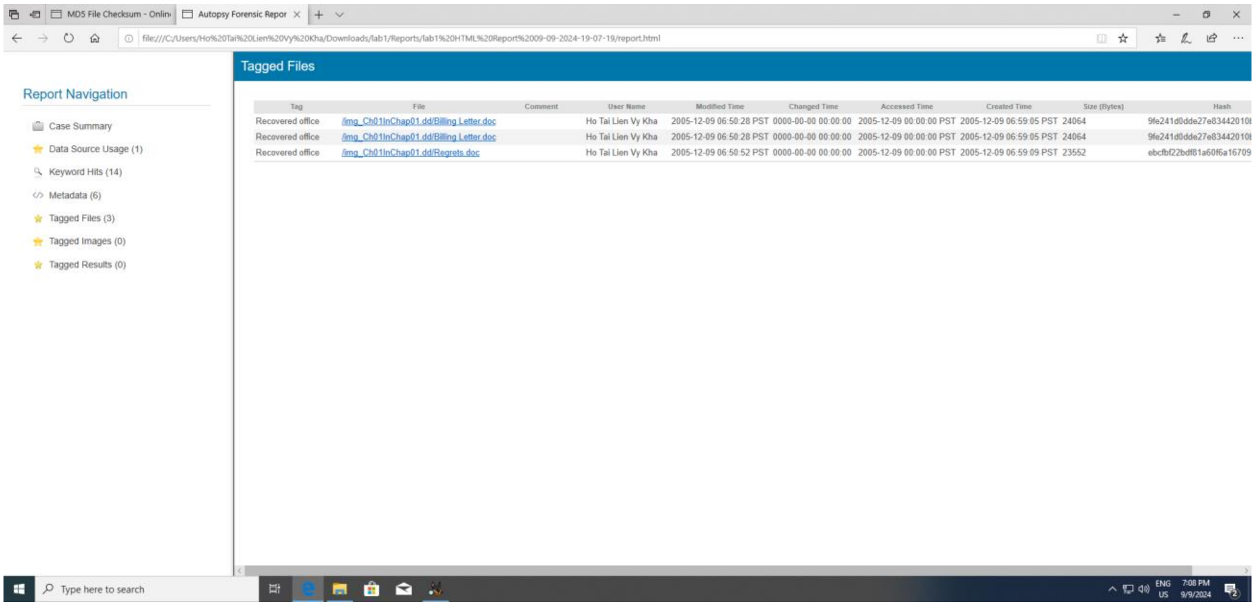
A report about results and tagged items in HTML format.

Header:

Footer:

< Back | Next > | Finish | Cancel | Help

Open or Save as file doc is recovered.



MD5 File Checksum - Onlin
Autopsy Forensic Repor
file:///C:/Users/Ho%20Tai%20Lien%20Vy%20Kha/Downloads/lab1/Reports/lab1%20HTML%20Report%2009-09-2024-19-07-19/report.html
Type here to search
ENG
US
7:08 PM
9/9/2024

Report Navigation

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

Tagged Files

Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Recovered office	/img_Ch01InChap01.dd/Billing Letter.doc		Ho Tai Lien Vy Kha	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	9fe241d0dde27e83442010b
Recovered office	/img_Ch01InChap01.dd/Billing Letter.doc		Ho Tai Lien Vy Kha	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:05 PST	24064	9fe241d0dde27e83442010b
Recovered office	/img_Ch01InChap01.dd/Regrets.doc		Ho Tai Lien Vy Kha	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:59:09 PST	23552	ebcfbf22bdf81a60f6a16709