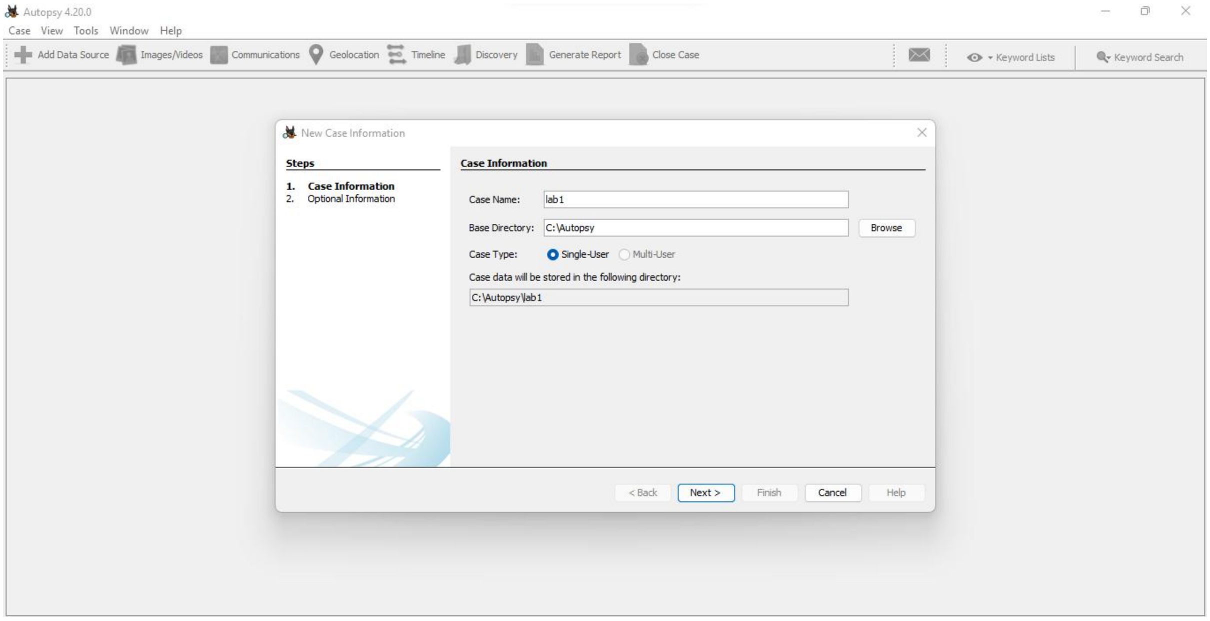
Digital Forensics

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : 'H'

Lab Assignment - 5

A graphical user interface (GUI) programme called Autopsy makes it simple to use the command-linetools, C library, and other digital forensics tools that are part of the Sleuth Kit. The Sleuth Kit's tools,along with other digital forensics tools, will enable Autopsy to automate many of the forensics analysis tasks necessary in the majority of investigations, including recovering deleted files,examining the Windows registry, examining emails, examining unused disc space, and many others. Additional tools provided by autopsy enable examiners to complete their analysis tasks more quickly.

Creating a new case and selecting the base directory.



Case Name: lab1

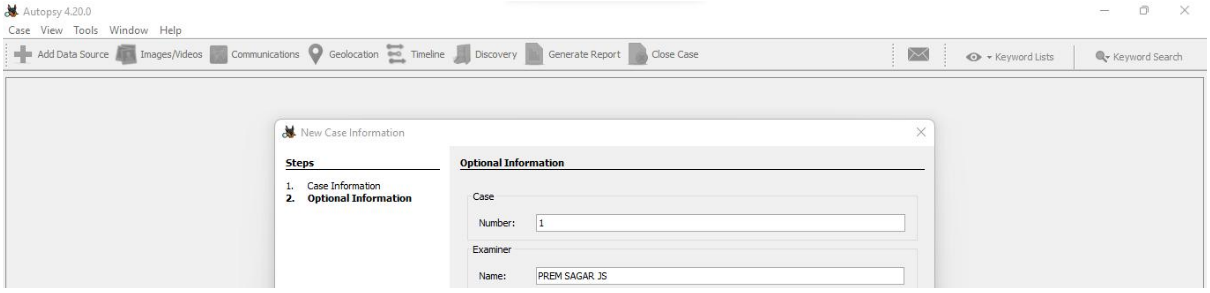
Base Directory: C:\Autopsy

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Autopsy\lab1

Entering the case number and examiner details in the optional information section.

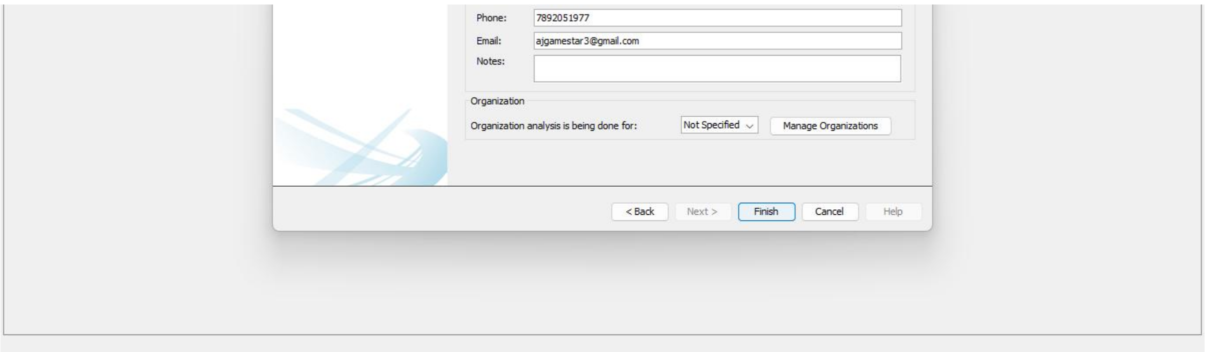


Case

Number: 1

Examiner

Name: PREM SAGAR JS



Phone: 7892051977

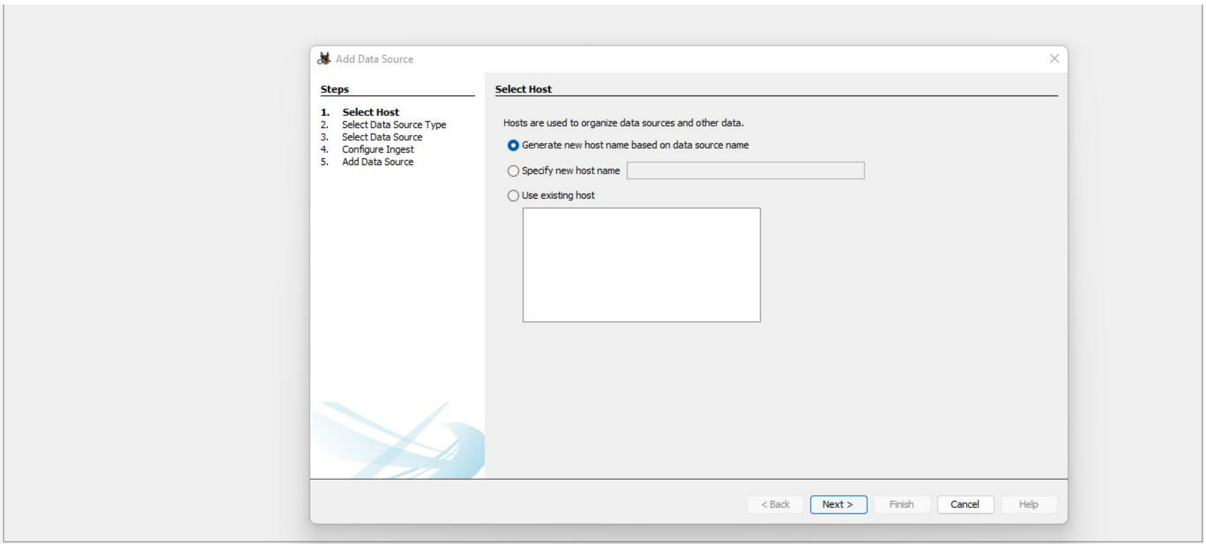
Email: ajgamestar3@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

Keep the default settings as it in in the select host section



Select Host

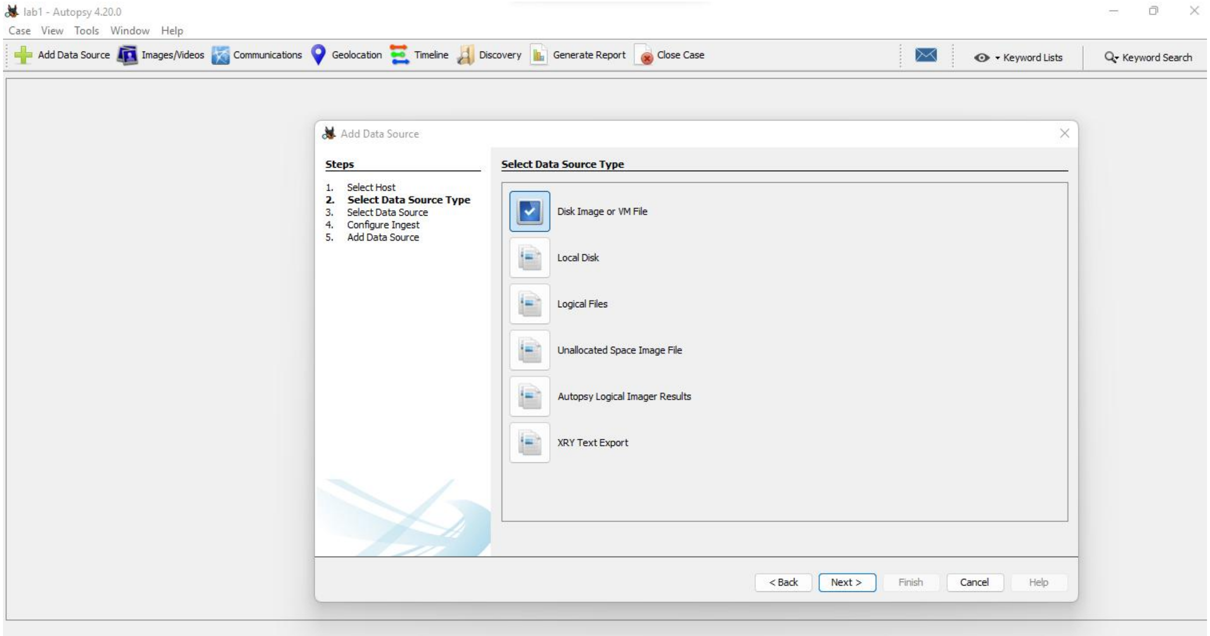
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Selecting the data source type as disk image or VM file.



Select Data Source Type

☑ Disk Image or VM File

Local Disk

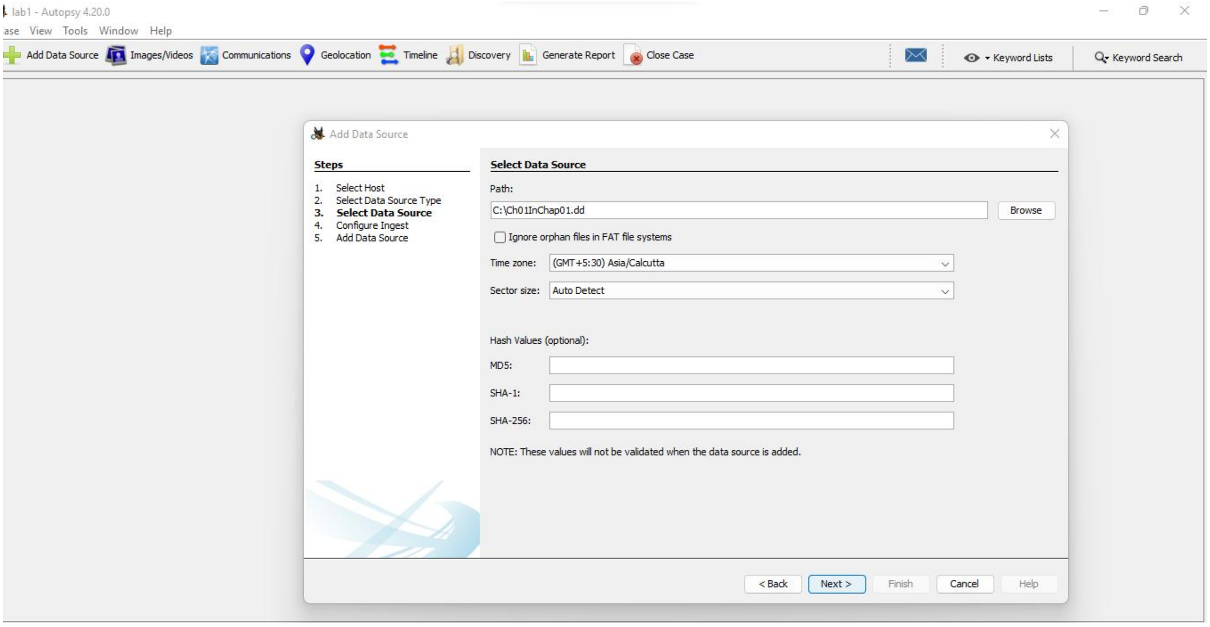
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Selecting the image file “Ch01InChap01.dd” in the select source data section.



Steps

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

Select Data Source

Path: C:\Ch01InChap01.dd

☐ Ignore orphan files in FAT file systems

Time zone: (GMT+5:30) Asia/Calcutta

Sector size: Auto Detect

Hash Values (optional):

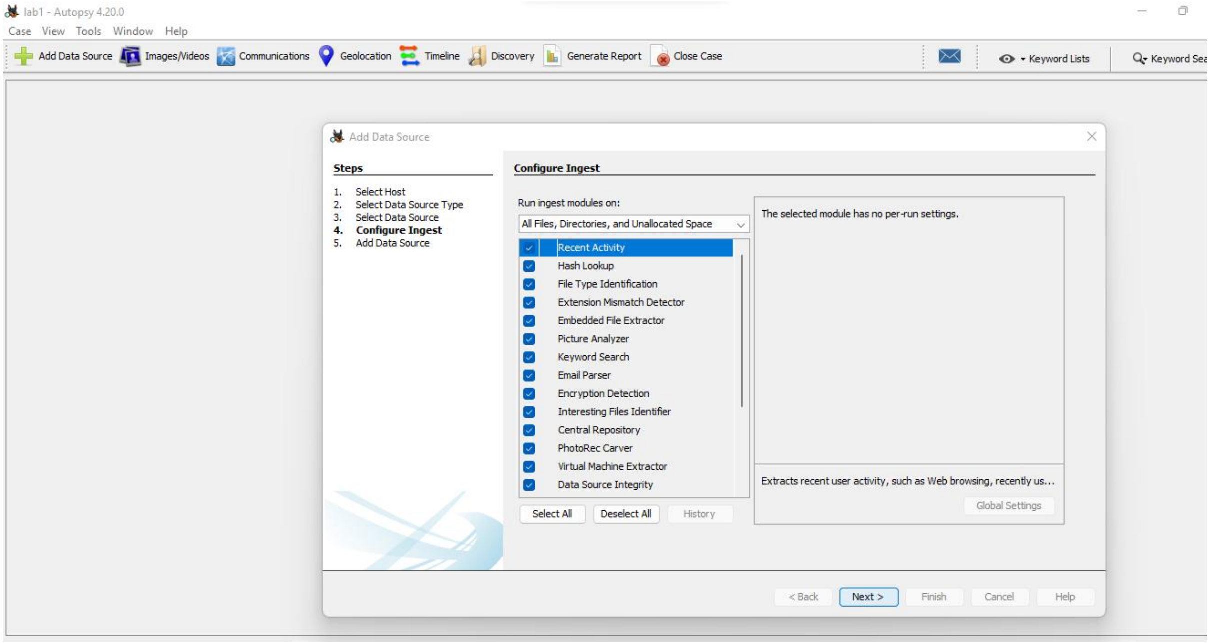
MD5:

SHA-1:

SHA-256:

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

Keep the default setting in configuration Ingest section as it is.



Steps

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

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

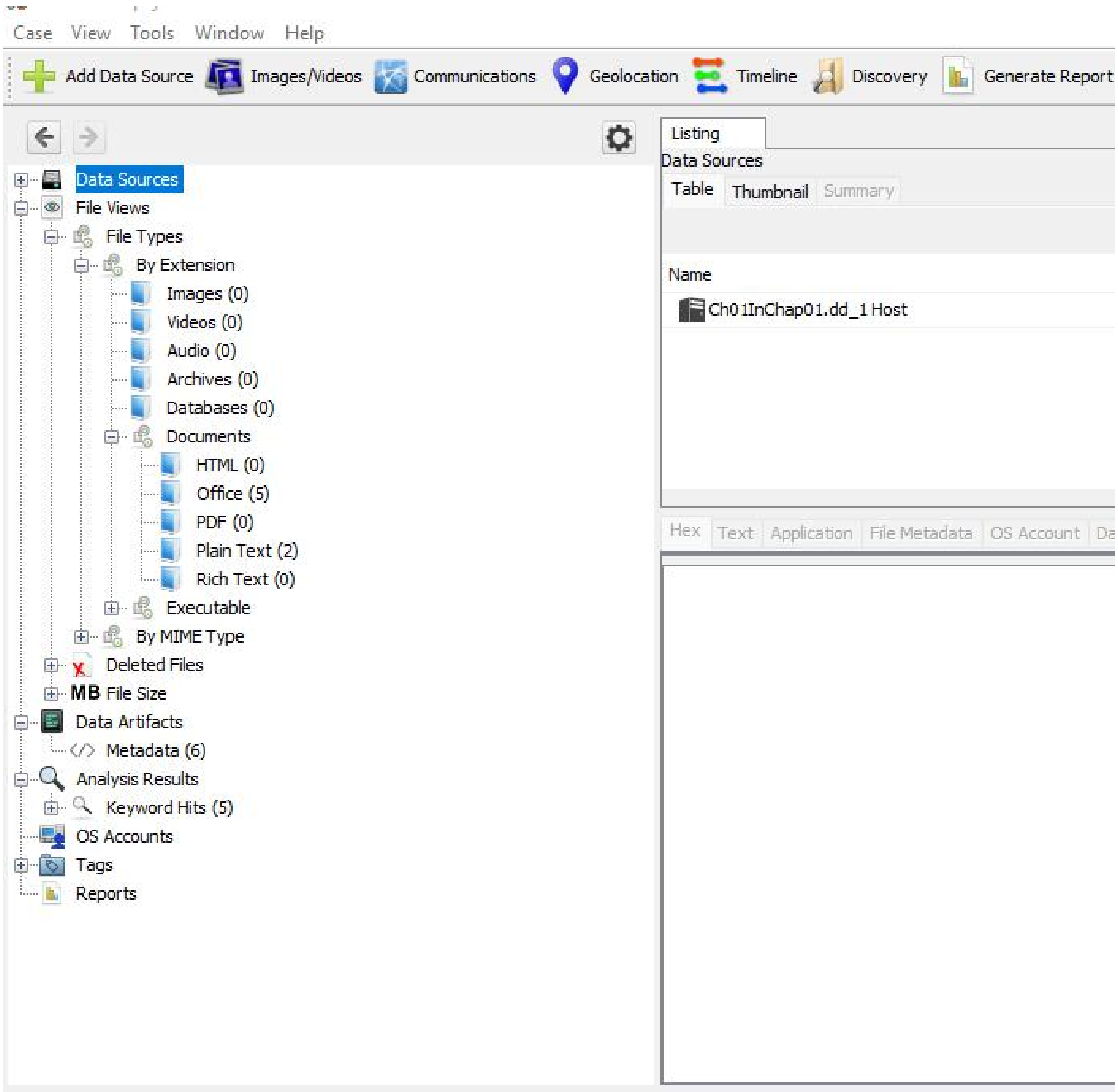
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Picture Analyzer
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Central Repository
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

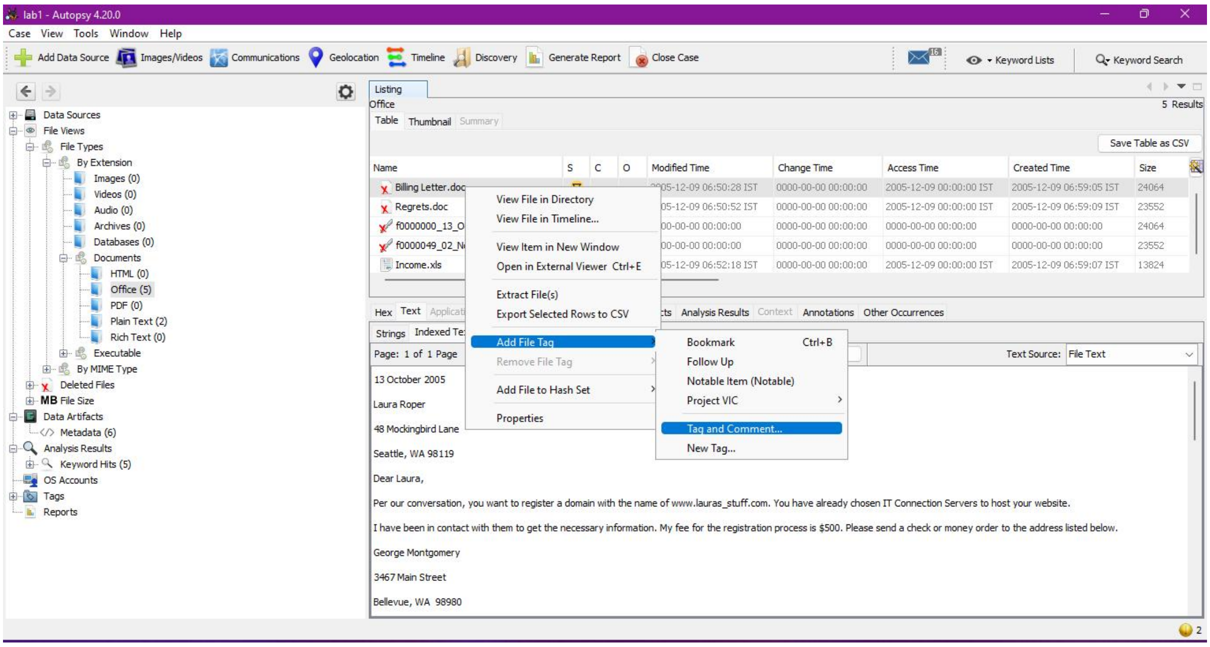
Finished of the initial setup.

Autopsy’s tree viewer panel



Name
Ch01InChap01.dd_1 Host

Adding file tag to billing letter.doc file



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
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
Regrets.doc				05-12-09 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
f0000000_13_O				00-00-00 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				00-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552
Income.xls				05-12-09 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

Text Source: File Text

13 October 2005

Laura Roper

48 Mockingbird Lane

Seattle, WA 98119

Dear Laura,

Per our conversation, you want to register a domain with the name of www.lauras_stuff.com. You have already chosen IT Connection Servers to host your website.

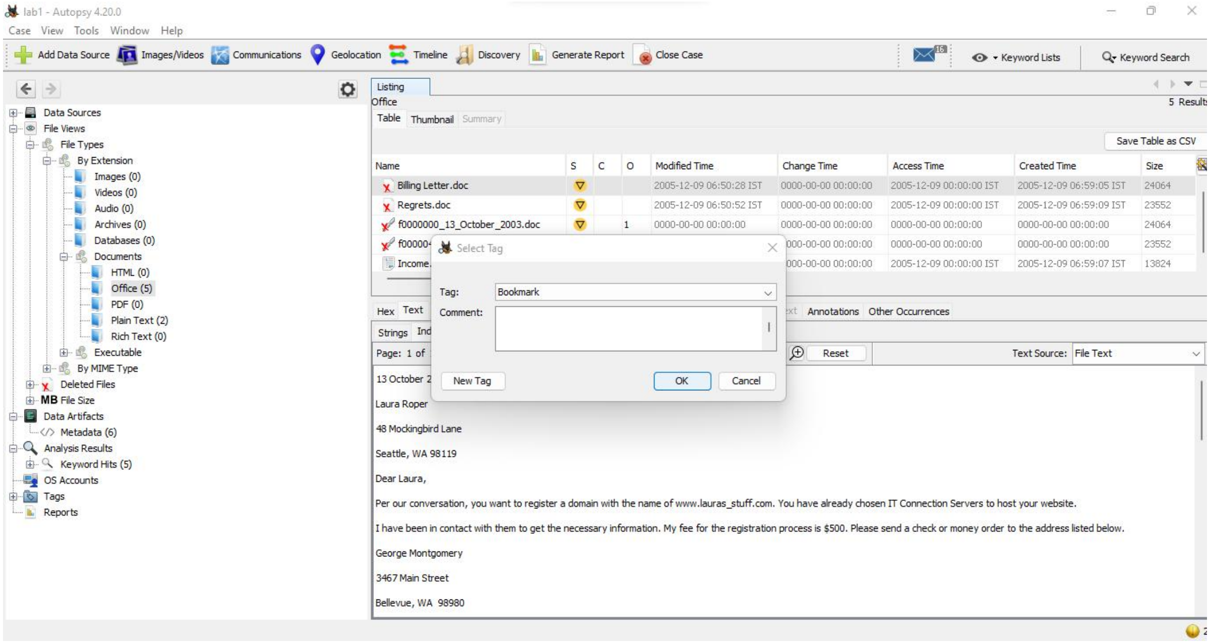
I have been in contact with them to get the necessary information. My fee for the registration process is $500. Please send a check or money order to the address listed below.

George Montgomery

3467 Main Street

Bellevue, WA 98980

Creating a new tag.



Office

5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
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
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
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
f00000					000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	23552
Income.					000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:07 IST	13824

Select Tag

Tag: Bookmark

Comment:

New Tag OK Cancel

Page: 1 of

Text Source: File Text

13 October 2

Laura Roper

48 Mockingbird Lane

Seattle, WA 98119

Dear Laura,

Per our conversation, you want to register a domain with the name of www.lauras_stuff.com. You have already chosen IT Connection Servers to host your website.

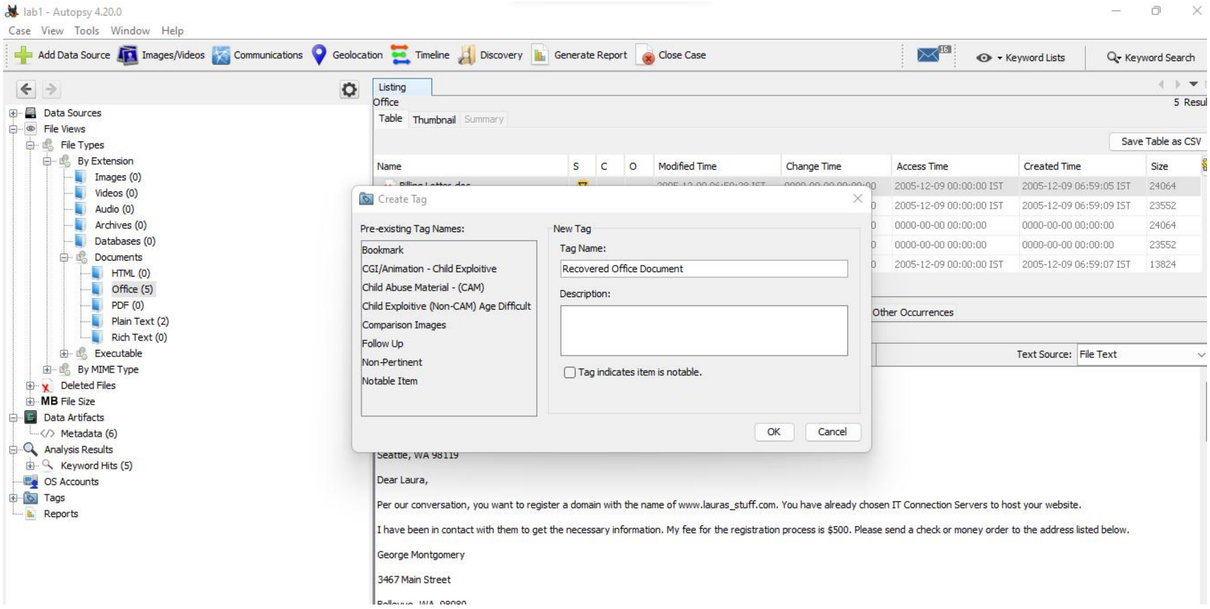
I have been in contact with them to get the necessary information. My fee for the registration process is $500. Please send a check or money order to the address listed below.

George Montgomery

3467 Main Street

Bellevue, WA 98980

Renaming the tag name to recovered office document.



Office

5 Results

Create Tag

Pre-existing Tag Names:

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

New Tag

Tag Name: Recovered Office Document

Description:

☐ Tag indicates item is notable.

OK Cancel

Text Source: File Text

Seattle, WA 98119

Dear Laura,

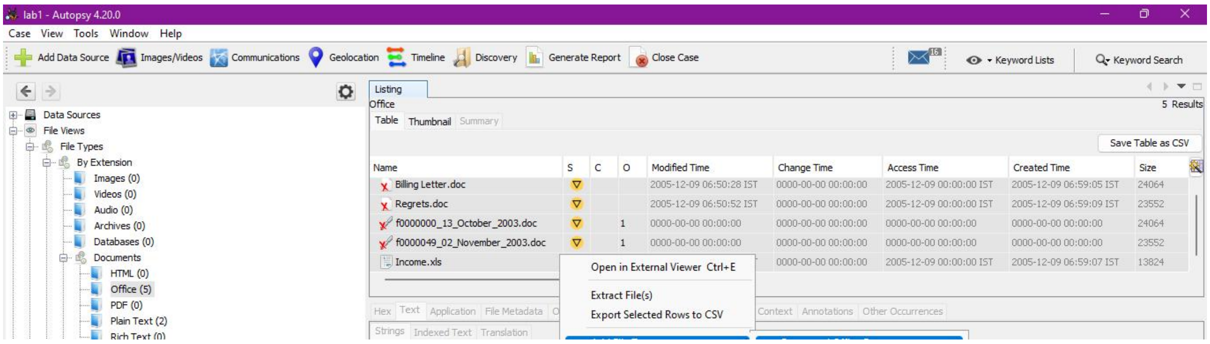
Per our conversation, you want to register a domain with the name of www.lauras_stuff.com. You have already chosen IT Connection Servers to host your website.

I have been in contact with them to get the necessary information. My fee for the registration process is $500. Please send a check or money order to the address listed below.

George Montgomery

3467 Main Street

Now when you click on add file tags recovered office document will be displayed.



Office

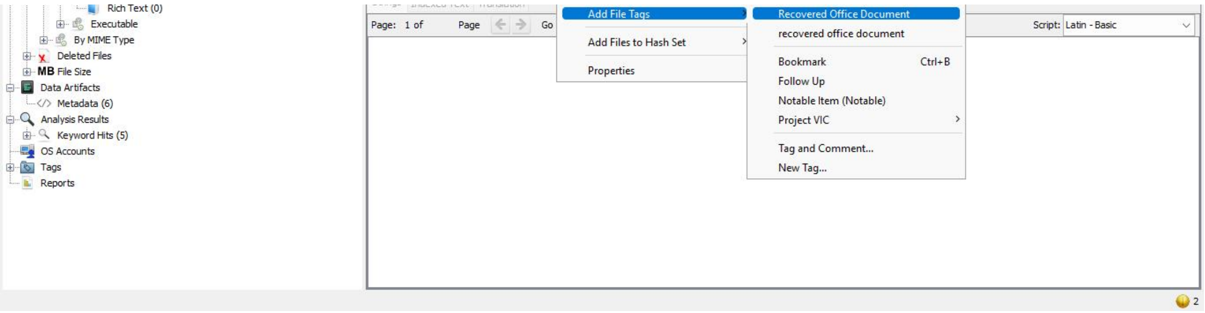
5 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
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
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
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
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
Income.xls					0000-00-00 00:00:00	2005-12-09 00:00:00 IST	2005-12-09 06:59:07 IST	13824

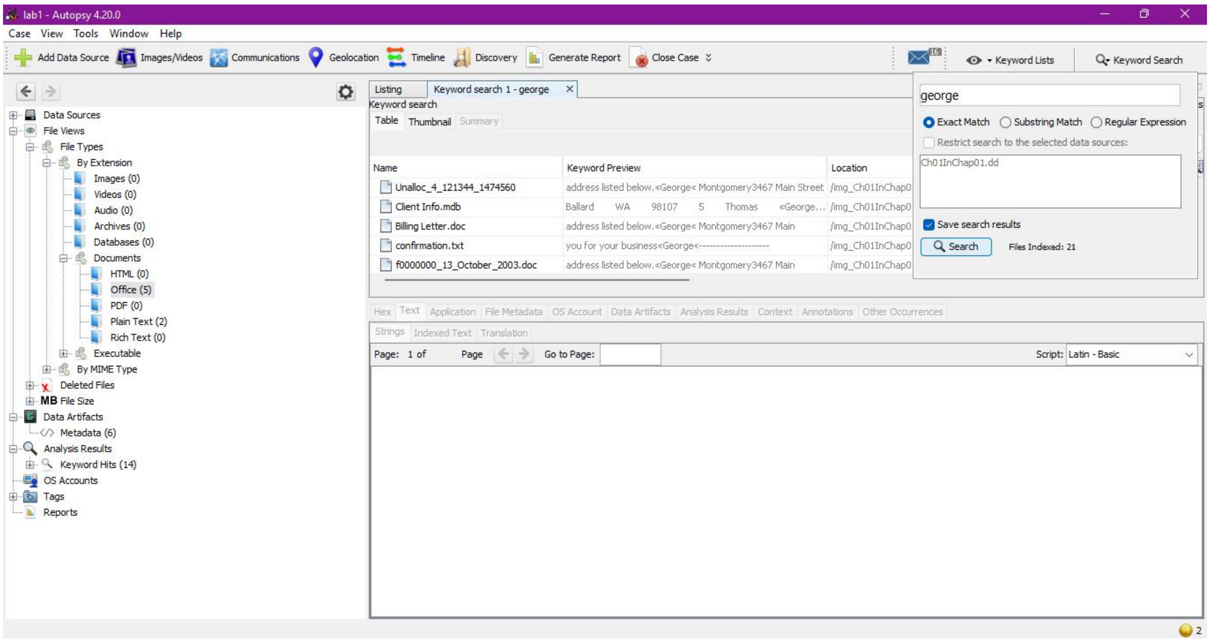
Open in External Viewer Ctrl+E

Extract File(s)

Export Selected Rows to CSV



Keyword search is done for searching if there is any reference to the name “George”. Looking for files containing the name “George.”



george

● Exact Match ○ Substring Match ○ Regular Expression

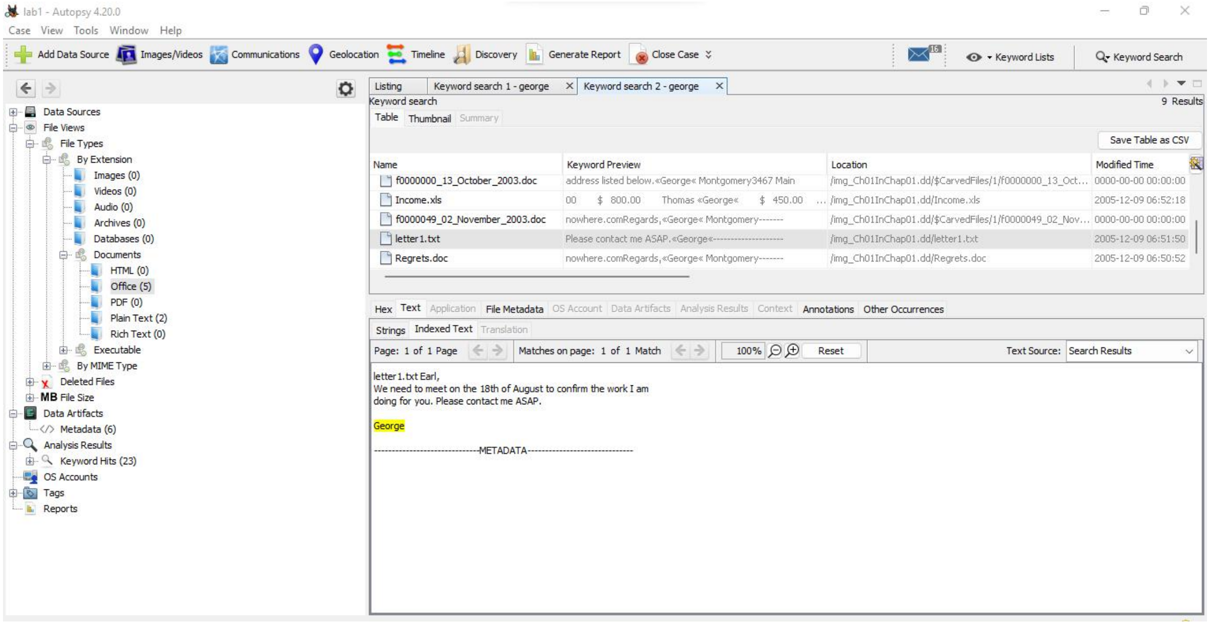
□ Restrict search to the selected data sources:

Ch01InChap01.dd

☑ Save search results

Search   Files Indexed: 21

Name	Keyword Preview	Location
Unalloc_4_121344_1474560	address listed below.«George« Montgomery3467 Main Street	/img_Ch01InChap0
Client Info.mdb	Ballard WA 98107 5 Thomas «George...	/img_Ch01InChap0
Billing Letter.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap0
confirmation.txt	you for your business«George«--------------------	/img_Ch01InChap0
f0000000_13_October_2003.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap0



9 Results

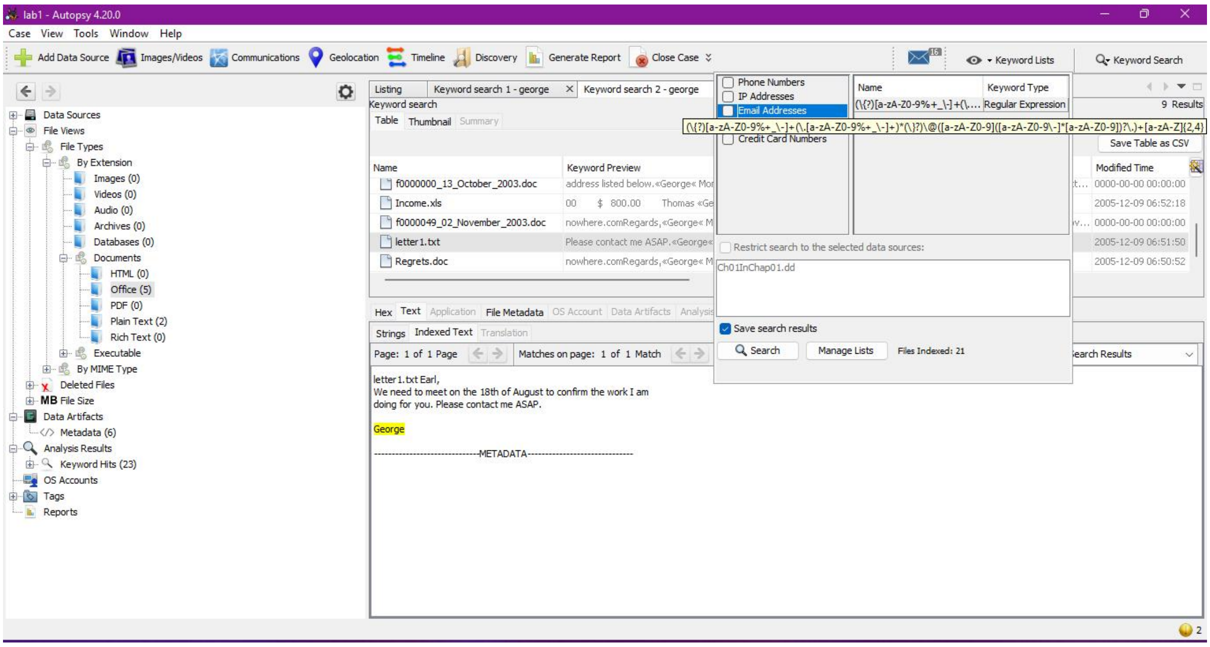
Name	Keyword Preview	Location	Modified Time
f0000000_13_October_2003.doc	address listed below.«George« Montgomery3467 Main	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000000_13_Oct...	0000-00-00 00:00:00
Income.xls	00 $ 800.00 Thomas «George« $ 450.00 ...	/img_Ch01InChap01.dd/Income.xls	2005-12-09 06:52:18
f0000049_02_November_2003.doc	nowhere.comRegards,«George« Montgomery-------	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000049_02_Nov...	0000-00-00 00:00:00
letter1.txt	Please contact me ASAP.«George«--------------------	/img_Ch01InChap01.dd/letter1.txt	2005-12-09 06:51:50
Regrets.doc	nowhere.comRegards,«George« Montgomery-------	/img_Ch01InChap01.dd/Regrets.doc	2005-12-09 06:50:52

```
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-----------------------------
```

Searching for references in email by selecting email in the keyword lists section.



□ Phone Numbers
□ IP Addresses
□ Email Addresses
□ Credit Card Numbers

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

(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}

□ Restrict search to the selected data sources:

Ch01InChap01.dd

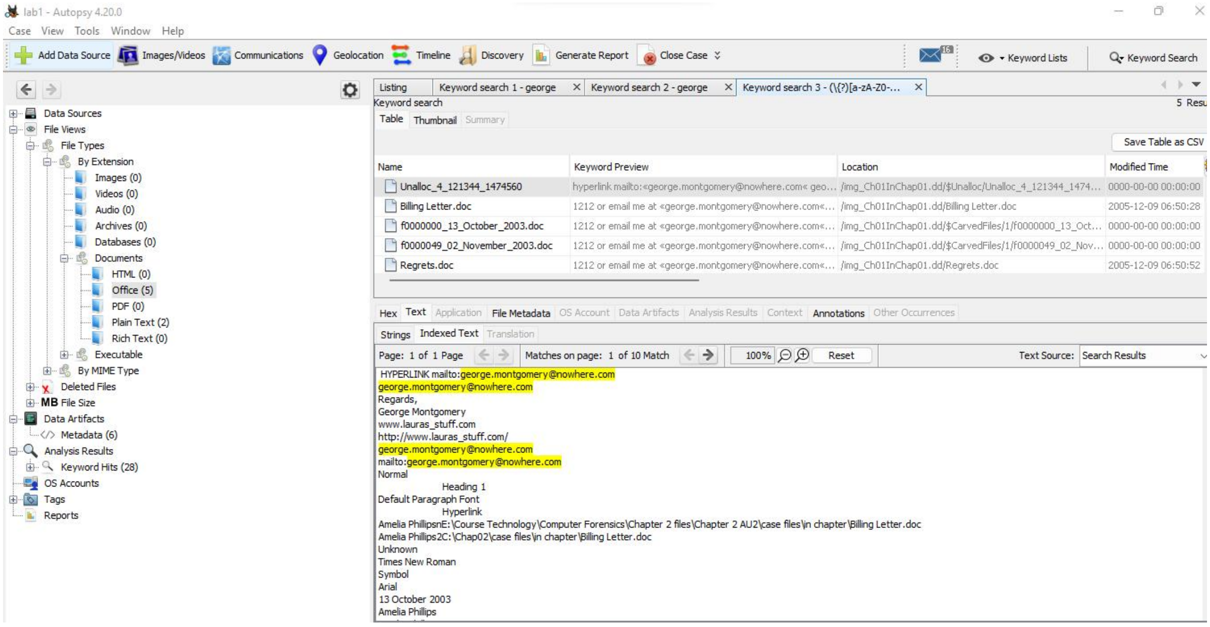
☑ Save search results

Name	Keyword Preview	Modified Time
f0000000_13_October_2003.doc	address listed below.«George« Mor	0000-00-00 00:00:00
Income.xls	00 $ 800.00 Thomas «Ge	2005-12-09 06:52:18
f0000049_02_November_2003.doc	nowhere.comRegards,«George« M	0000-00-00 00:00:00
letter1.txt	Please contact me ASAP.«George«	2005-12-09 06:51:50
Regrets.doc	nowhere.comRegards,«George« M	2005-12-09 06:50:52

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

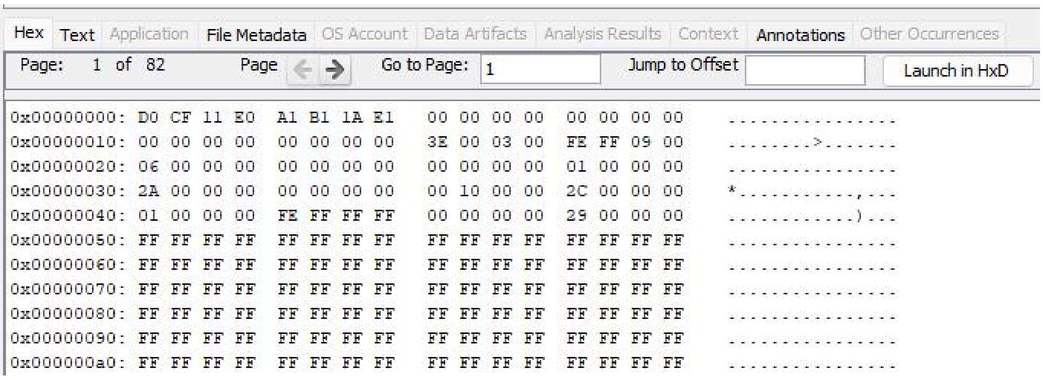
-----------------------------METADATA-----------------------------



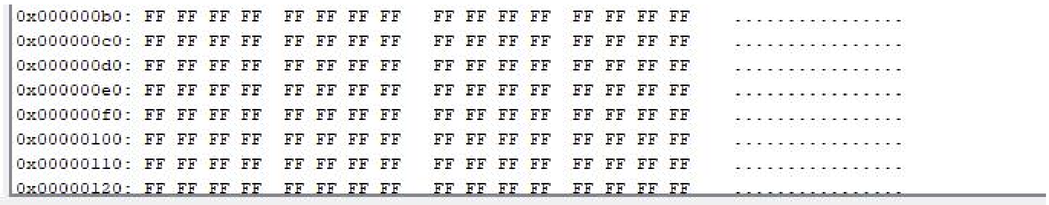
Name	Keyword Preview	Location	Modified Time
Unalloc_4_121344_1474560	hyperlink mailto:«george.montgomery@nowhere.com« geo…	/img_Ch01InChap01.dd/$Unalloc/Unalloc_4_121344_1474…	0000-00-00 00:00:00
Billing Letter.doc	1212 or email me at «george.montgomery@nowhere.com«…	/img_Ch01InChap01.dd/Billing Letter.doc	2005-12-09 06:50:28
f0000000_13_October_2003.doc	1212 or email me at «george.montgomery@nowhere.com«…	/img_Ch01InChap01.dd/$CarvedFiles/1/f0000000_13_Oct…	0000-00-00 00:00:00
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
Regrets.doc	1212 or email me at «george.montgomery@nowhere.com«…	/img_Ch01InChap01.dd/Regrets.doc	2005-12-09 06:50:52

```
 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 PhillipsnE:\Course Technology\Computer Forensics\Chapter 2 files\Chapter 2 AU2\case files\in chapter\Billing Letter.doc
Amelia Phillips2C:\Chap02\case files\in chapter\Billing Letter.doc
Unknown
Times New Roman
Symbol
Arial
13 October 2003
Amelia Phillips
```

Viewing an unallocated sector for its hexadecimal values.



```
0x00000000: D0 CF 11 E0  A1 B1 1A E1   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    ................
```