CIS-387: Digital Forensics (4 credits)

With Dr. Jinhua Guo

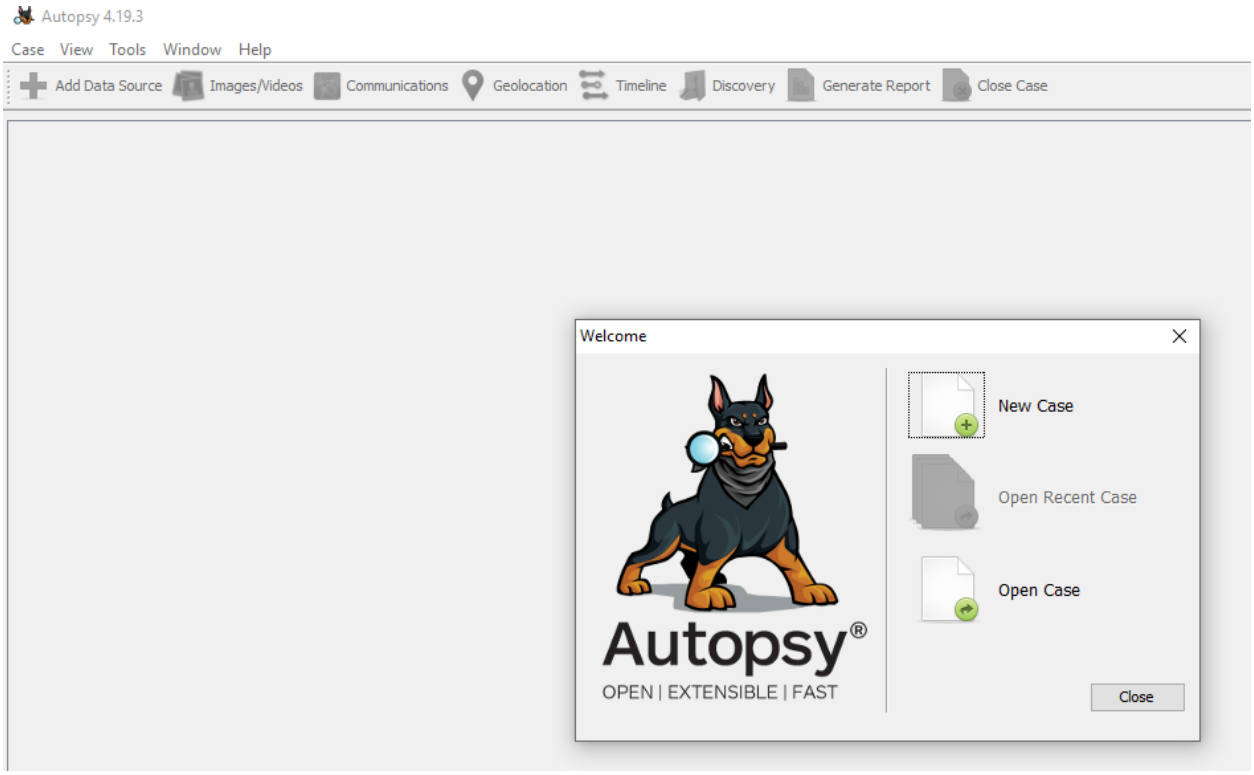
Lab 5

Demetrius Johnson

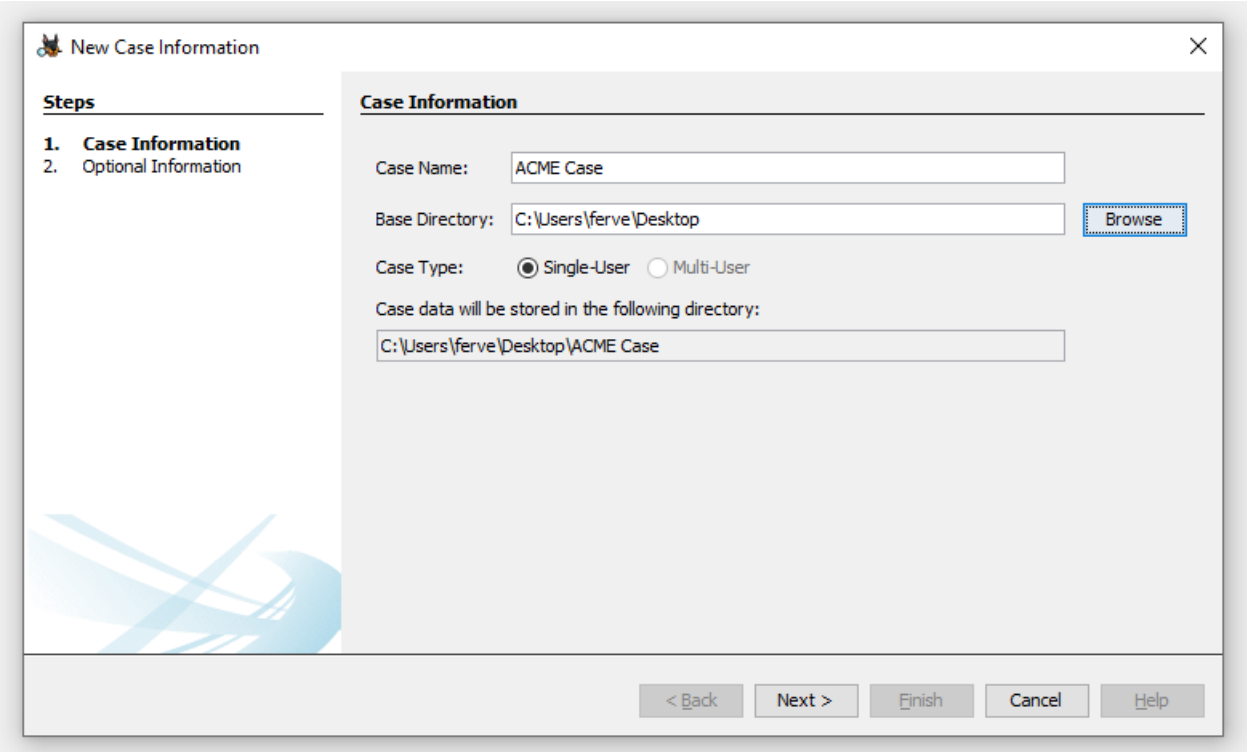
October 26, 2022

ACTIVITY: Disk Image Analysis with ACME Autopsy Tool (GUI version of Sleuthkit)

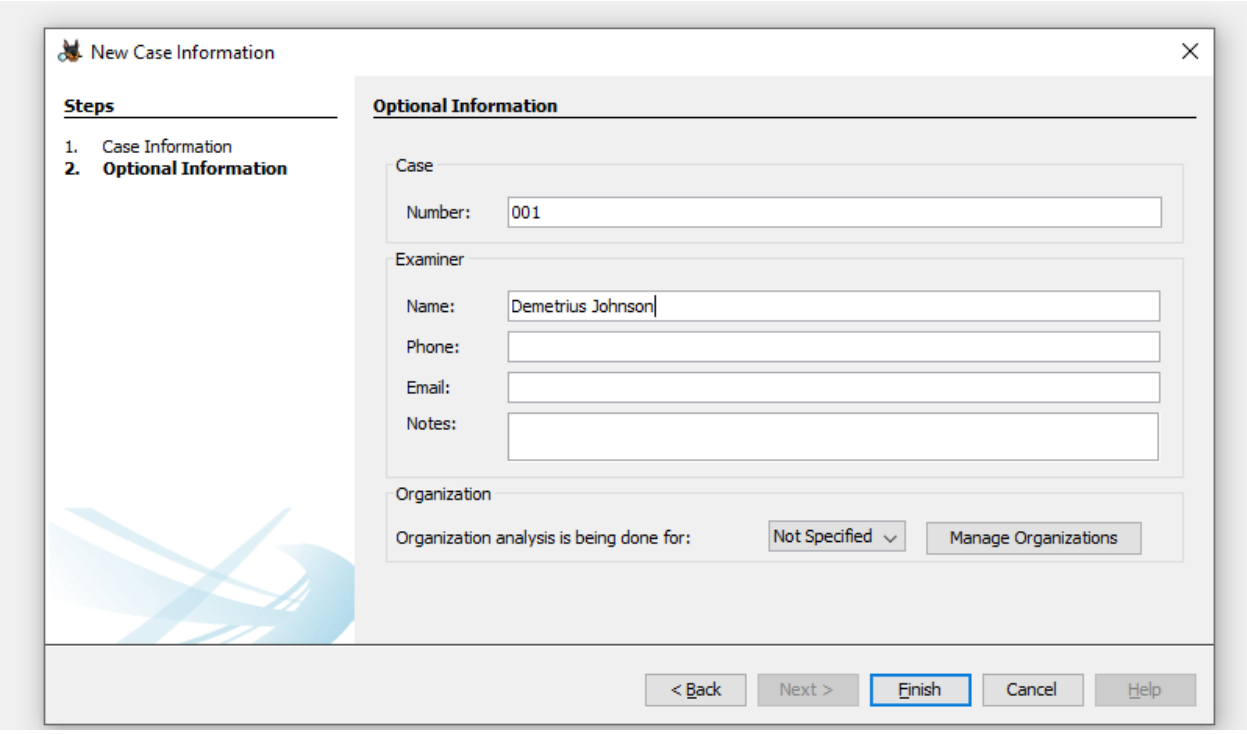
1. Launch Autopsy from the Toolbox folder on the desktop and follow the instruction below to create a case and add the given image into the case.



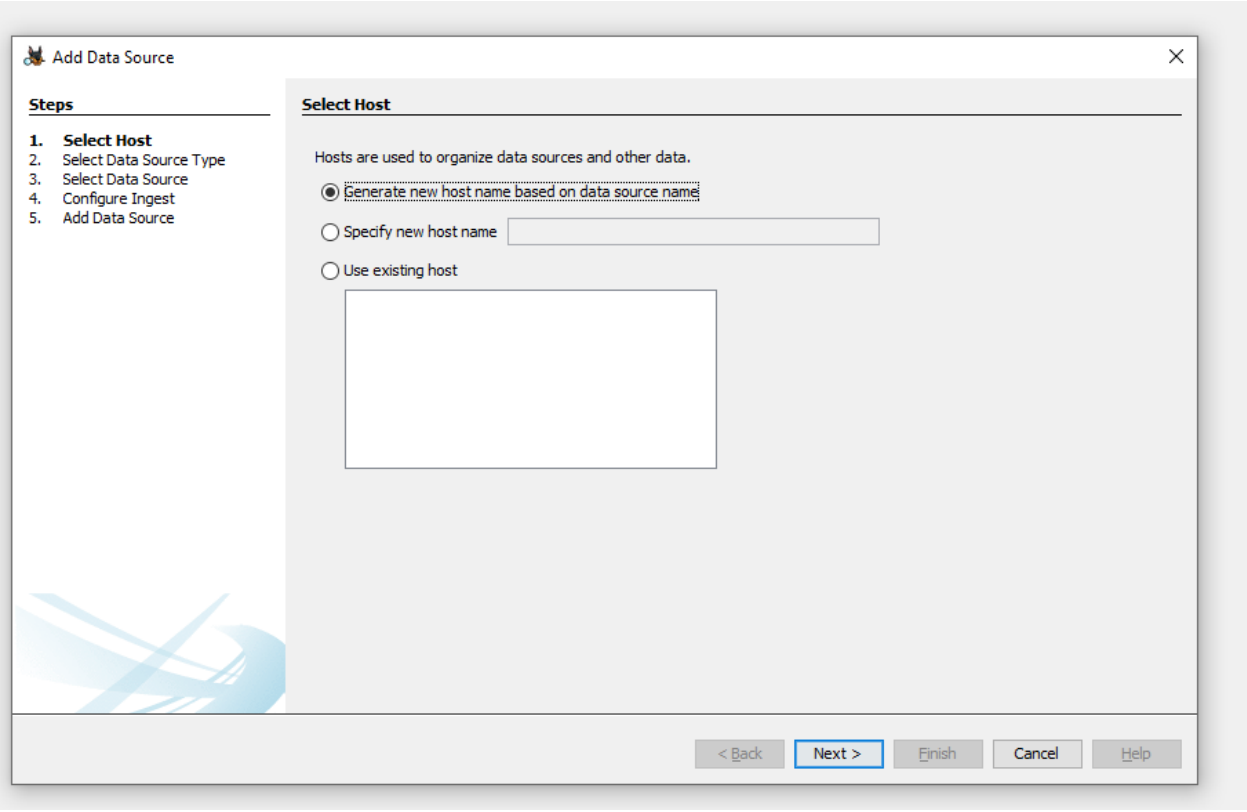
2. Select > Create New Case
3. Name the case as “ACME Case”.
4. Use the default Base Directory (Desktop) to store the case data in Desktop\ACME Case\.



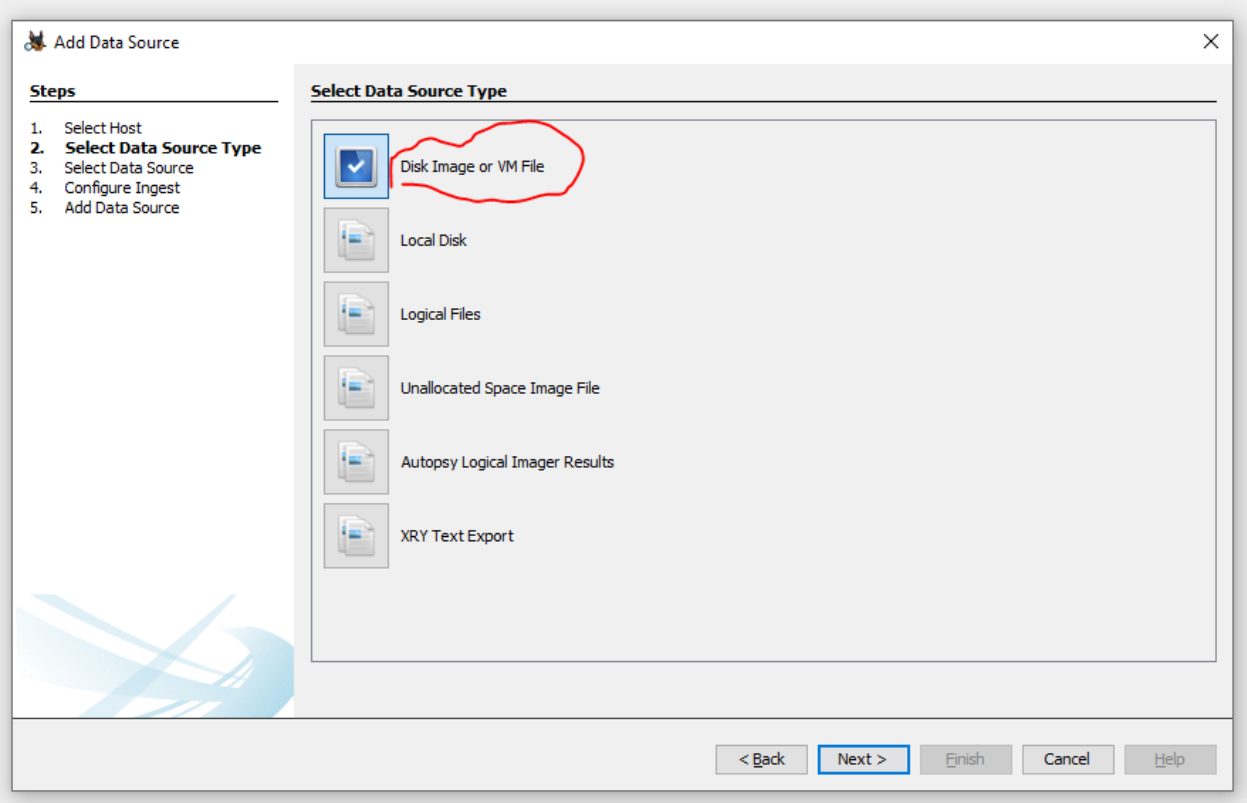
5. Enter the Case Number as “001” and enter your name as “Examiner.”



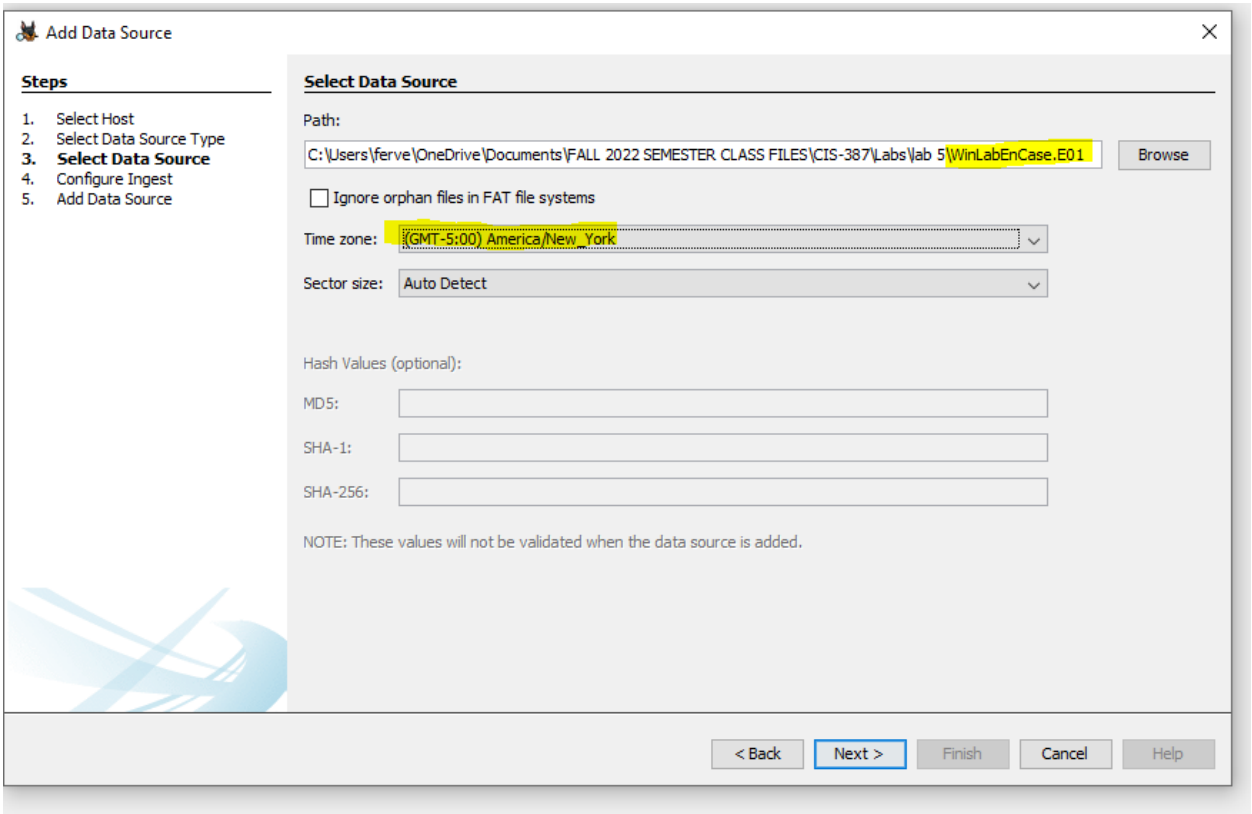
6. Click Finish. You will see the "Add Data Source" window.



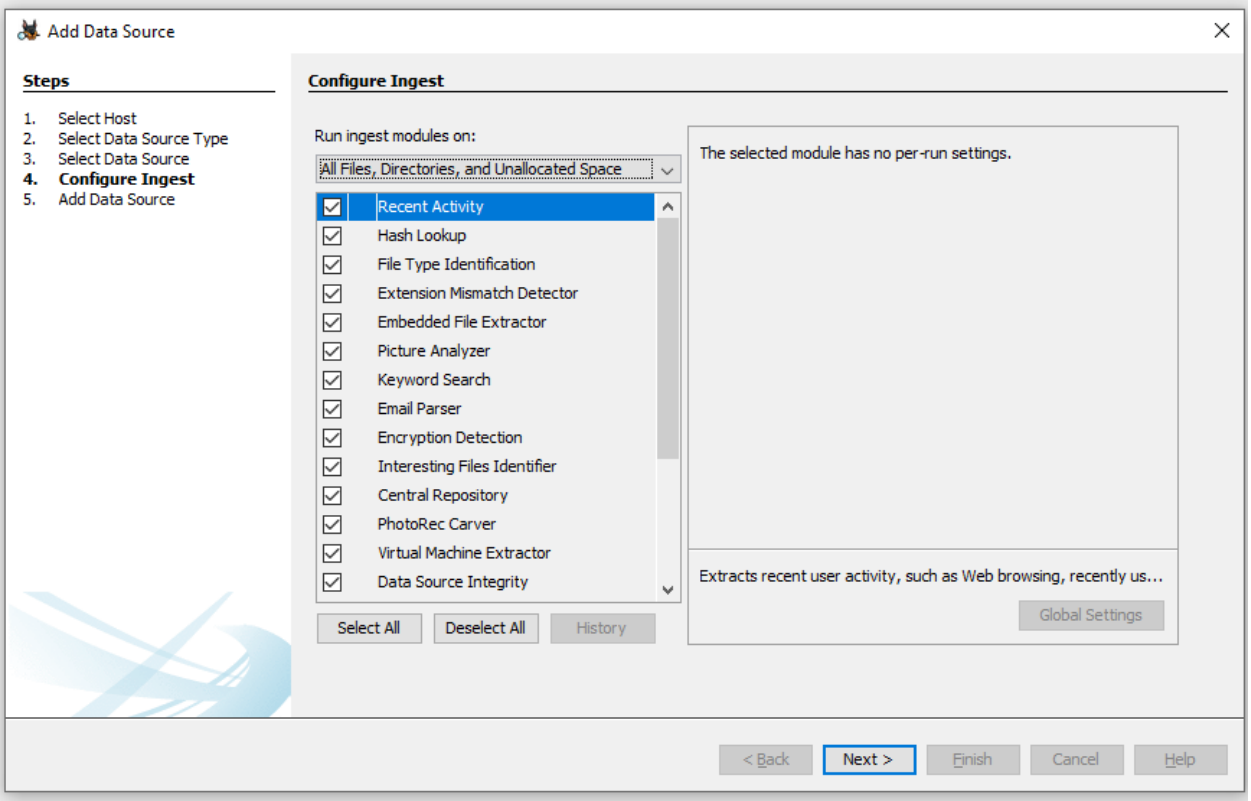
7. Select data source type: choose Disk Image or VM File; browse and select the path to "WinLabEnCase.E01".



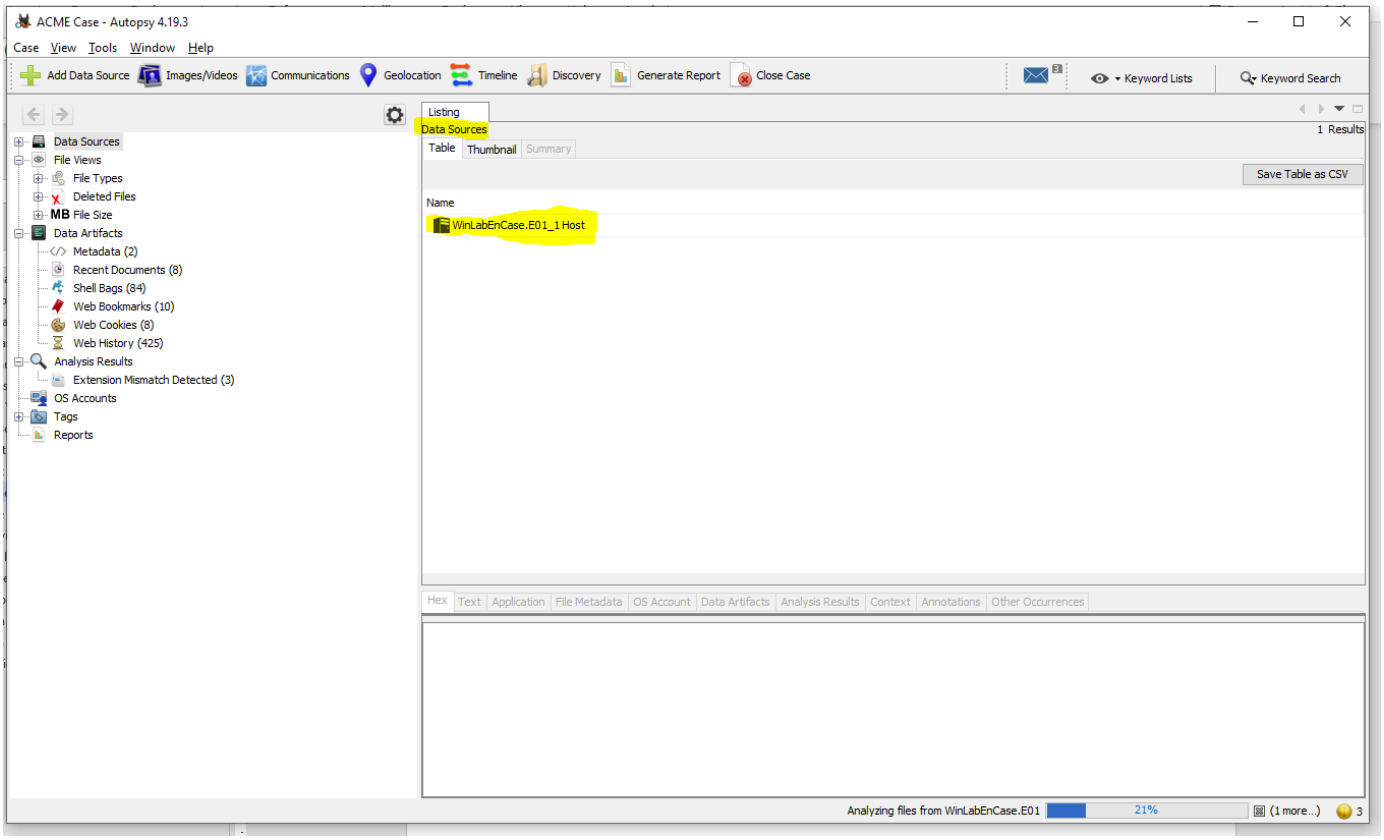
8. In our case, the computer image's time zone is North American Eastern Time Zone. Select the time zone accordingly and click Next.



9. In the Ingest (processing) modules window, leave all modules checked; click Next and then click Finish.

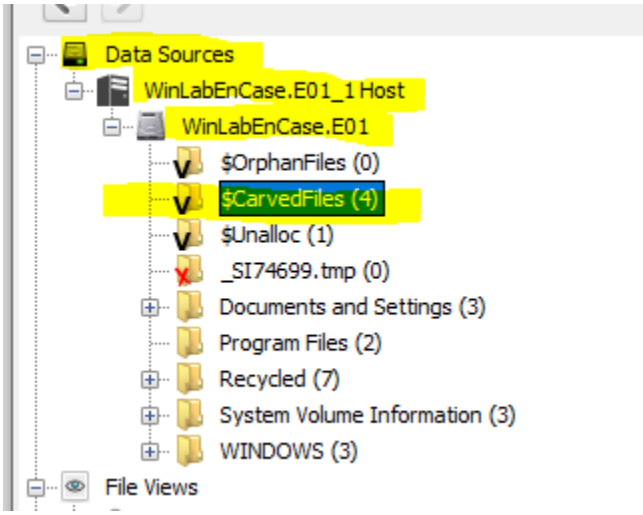


10. Examine the files in Data Sources > WinLabEnCase.E01 and categorized data under Views and Results to identify pertinent evidence.



11. Explore the image contents and results, and answer the following questions.

a) Data carving is the process of extracting files and objects that have been deleted or are embedded in other files. Check under Data Sources > WinLabEnCase.E01> $CarvedFiles. How many embedded files did Autopsy extract by performing the data carving process? List all the files.



Notice 4 files have been extracted by the data carving process:

Listing

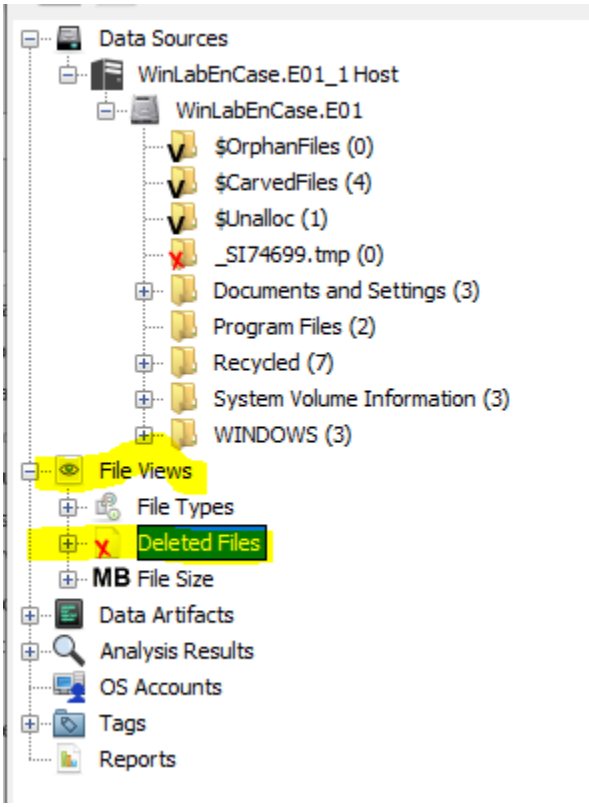
/img_WinLabEnCase.E01//$CarvedFiles — 4 Results

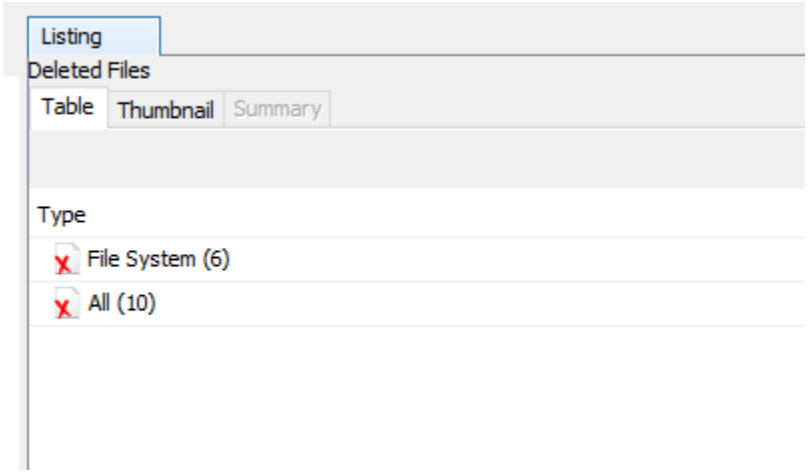
Table | Thumbnail | Summary

Save Table as CSV

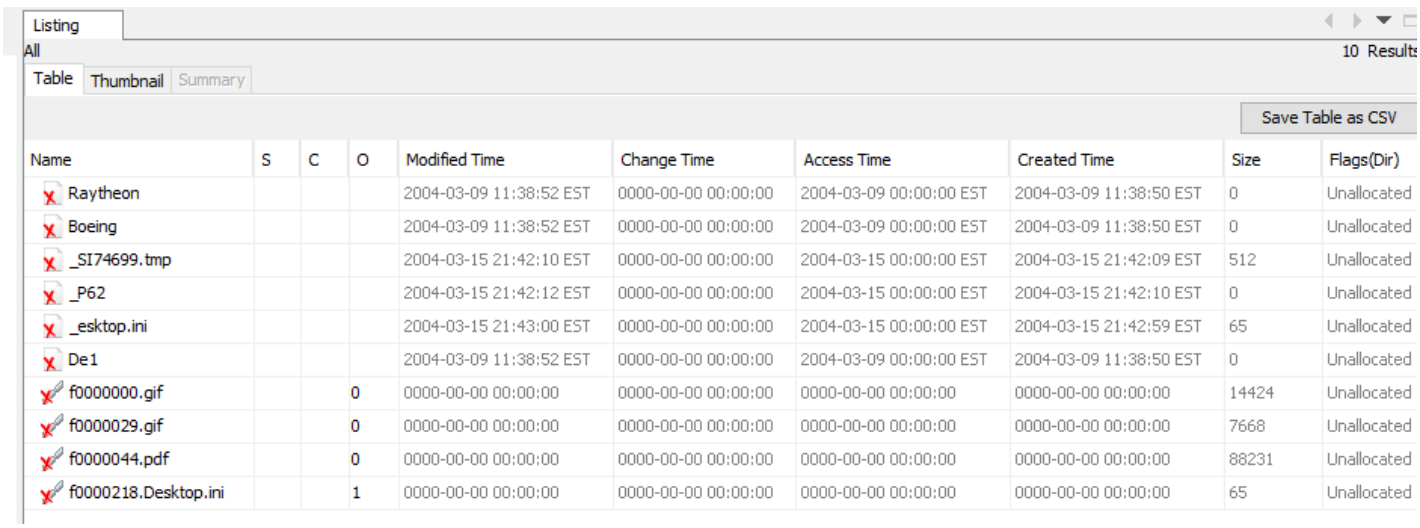
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(
f0000000.gif			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14424	Unallocated	Unallo
f0000029.gif			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7668	Unallocated	Unallo
f0000044.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88231	Unallocated	Unallo
f0000218.Desktop.ini			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	65	Unallocated	Unallo

b) Autopsy lists all deleted files in Views > Deleted Files. What have you found by examining these deleted files?



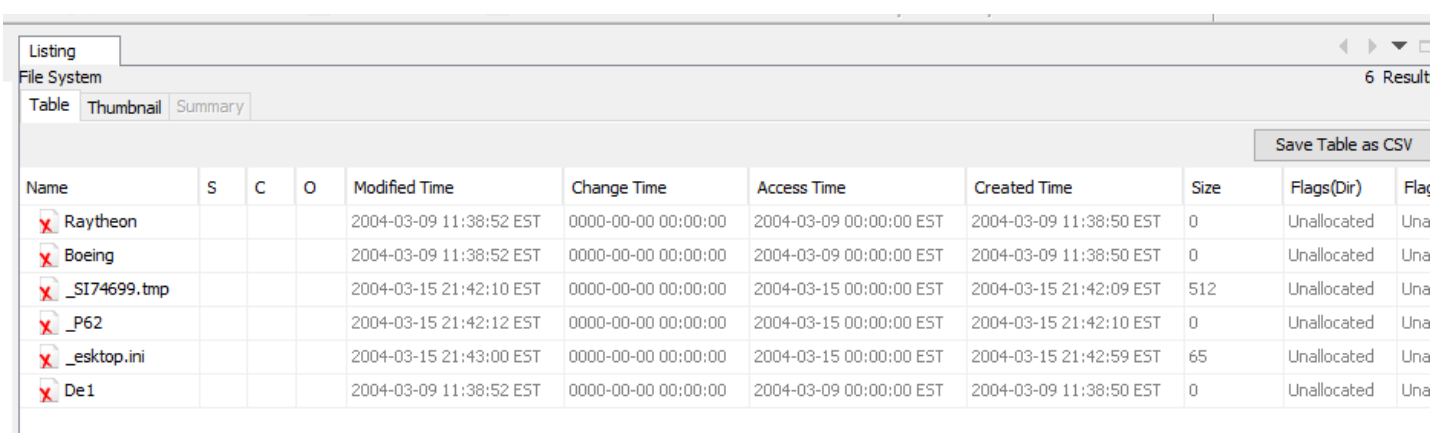


Here are all the deleted files:



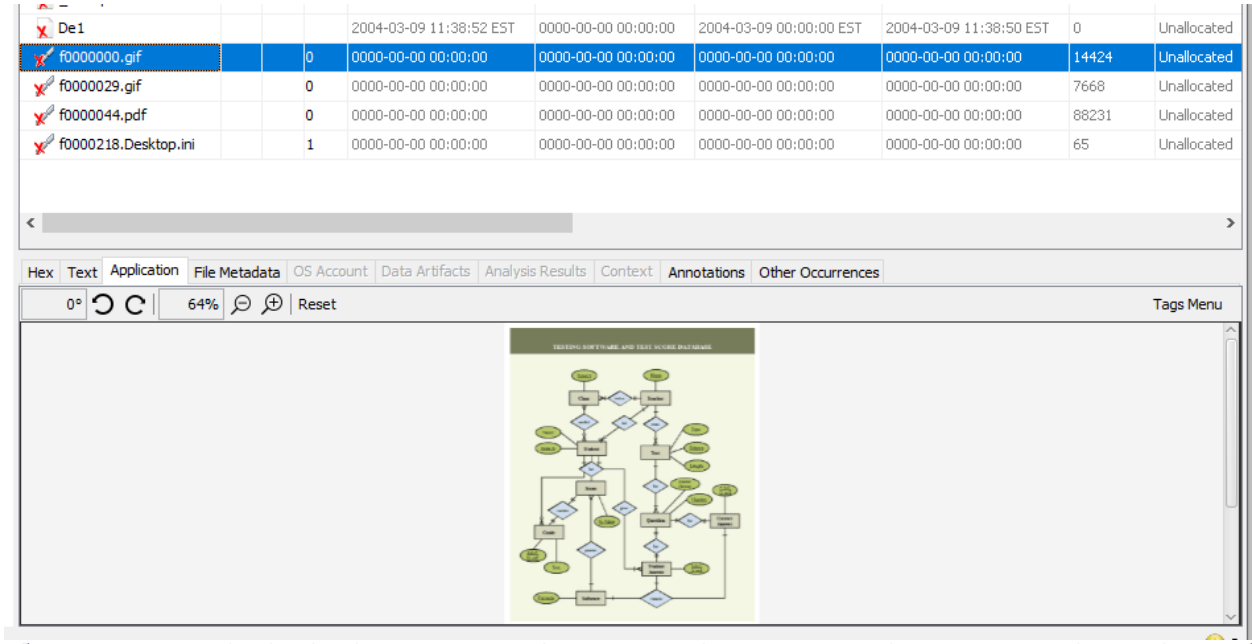
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Raytheon				2004-03-09 11:38:52 EST	0000-00-00 00:00:00	2004-03-09 00:00:00 EST	2004-03-09 11:38:50 EST	0	Unallocated
Boeing				2004-03-09 11:38:52 EST	0000-00-00 00:00:00	2004-03-09 00:00:00 EST	2004-03-09 11:38:50 EST	0	Unallocated
_SI74699.tmp				2004-03-15 21:42:10 EST	0000-00-00 00:00:00	2004-03-15 00:00:00 EST	2004-03-15 21:42:09 EST	512	Unallocated
_P62				2004-03-15 21:42:12 EST	0000-00-00 00:00:00	2004-03-15 00:00:00 EST	2004-03-15 21:42:10 EST	0	Unallocated
_esktop.ini				2004-03-15 21:43:00 EST	0000-00-00 00:00:00	2004-03-15 00:00:00 EST	2004-03-15 21:42:59 EST	65	Unallocated
De1				2004-03-09 11:38:52 EST	0000-00-00 00:00:00	2004-03-09 00:00:00 EST	2004-03-09 11:38:50 EST	0	Unallocated
f0000000.gif			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	14424	Unallocated
f0000029.gif			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	7668	Unallocated
f0000044.pdf			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	88231	Unallocated
f0000218.Desktop.ini			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	65	Unallocated

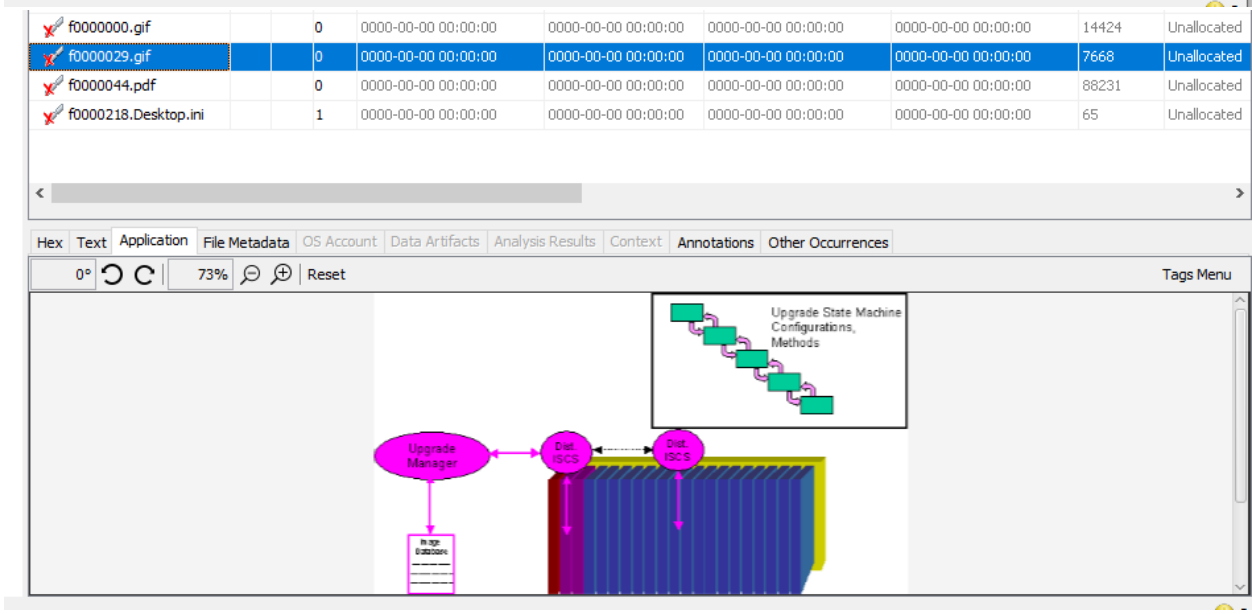
Here are the deleted system files, a subset of all deleted files:

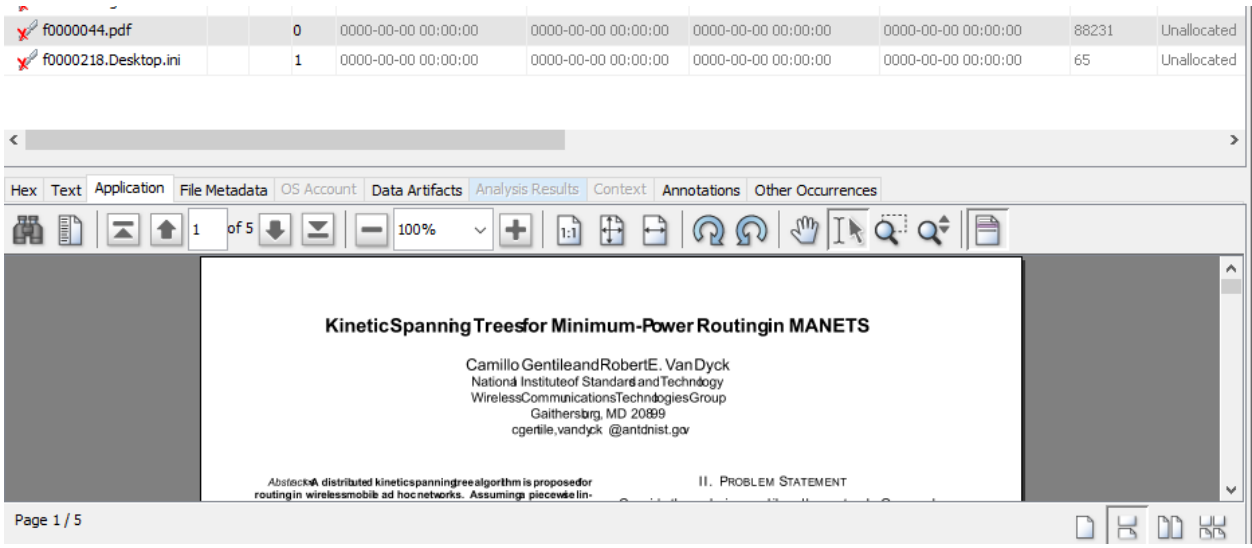


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
Raytheon				2004-03-09 11:38:52 EST	0000-00-00 00:00:00	2004-03-09 00:00:00 EST	2004-03-09 11:38:50 EST	0	Unallocated	Una
Boeing				2004-03-09 11:38:52 EST	0000-00-00 00:00:00	2004-03-09 00:00:00 EST	2004-03-09 11:38:50 EST	0	Unallocated	Una
_SI74699.tmp				2004-03-15 21:42:10 EST	0000-00-00 00:00:00	2004-03-15 00:00:00 EST	2004-03-15 21:42:09 EST	512	Unallocated	Una
_P62				2004-03-15 21:42:12 EST	0000-00-00 00:00:00	2004-03-15 00:00:00 EST	2004-03-15 21:42:10 EST	0	Unallocated	Una
_esktop.ini				2004-03-15 21:43:00 EST	0000-00-00 00:00:00	2004-03-15 00:00:00 EST	2004-03-15 21:42:59 EST	65	Unallocated	Una
De1				2004-03-09 11:38:52 EST	0000-00-00 00:00:00	2004-03-09 00:00:00 EST	2004-03-09 11:38:50 EST	0	Unallocated	Una

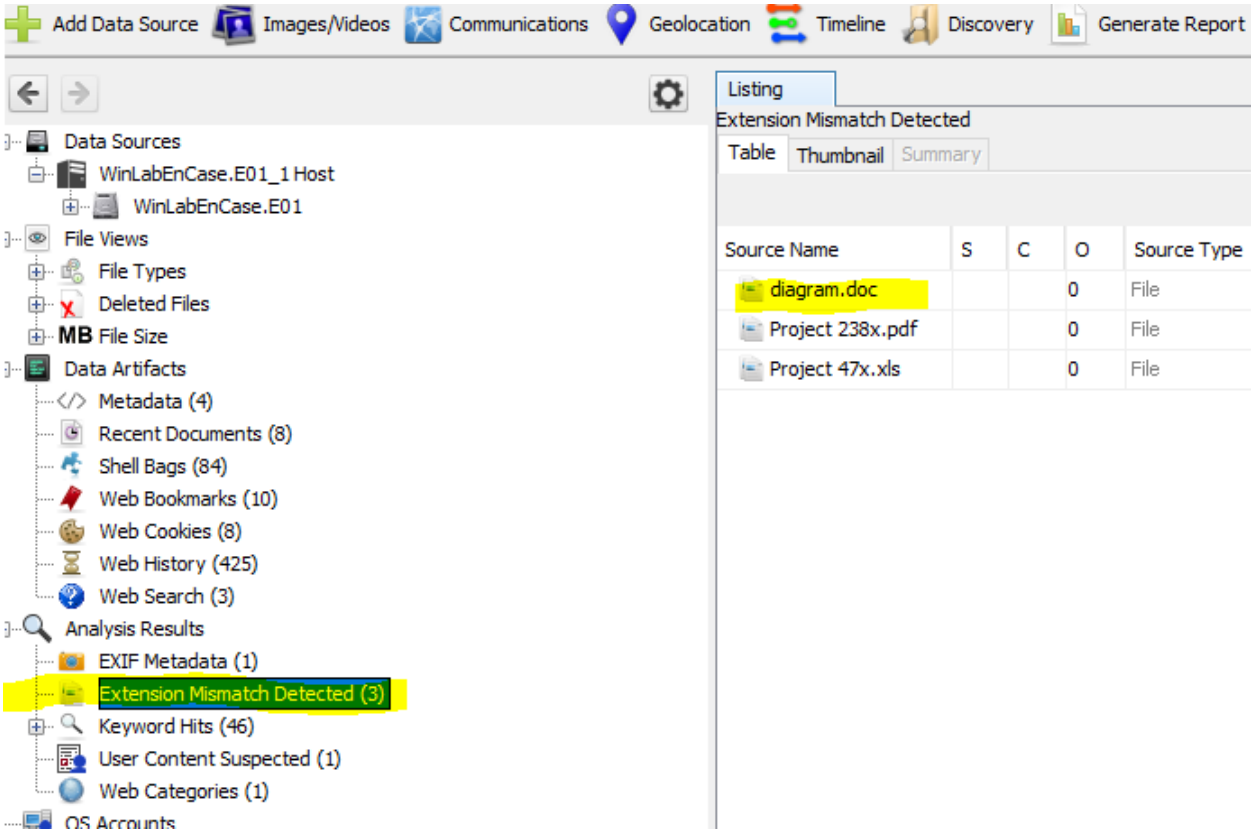
- Raytheon, Boeing, and _P62 were all directories which were small enough that their file data was able to be stored as attributes in the MFT table.

- There were also two .gif files with diagrams and a .pdf file which contained a research paper or abstract.
  - 

  - 

- 

c) A file type can be determined by a header that precedes the data in the file. If a file's extension has been deliberately changed, the extension will not match with the file header. File Signature Analysis detects such mismatches by comparing the file extension with its header. Autopsy performs file signature analysis and lists these files in Results > Extracted Content > Extension Mismatch Detected. In this case, diagram.doc has a mismatched extension. What is the real file type of diagram.doc?

- 

  - Above, I am showing diagram.doc file that is found to have extension mismatch.

- Here is the detected actual file type:

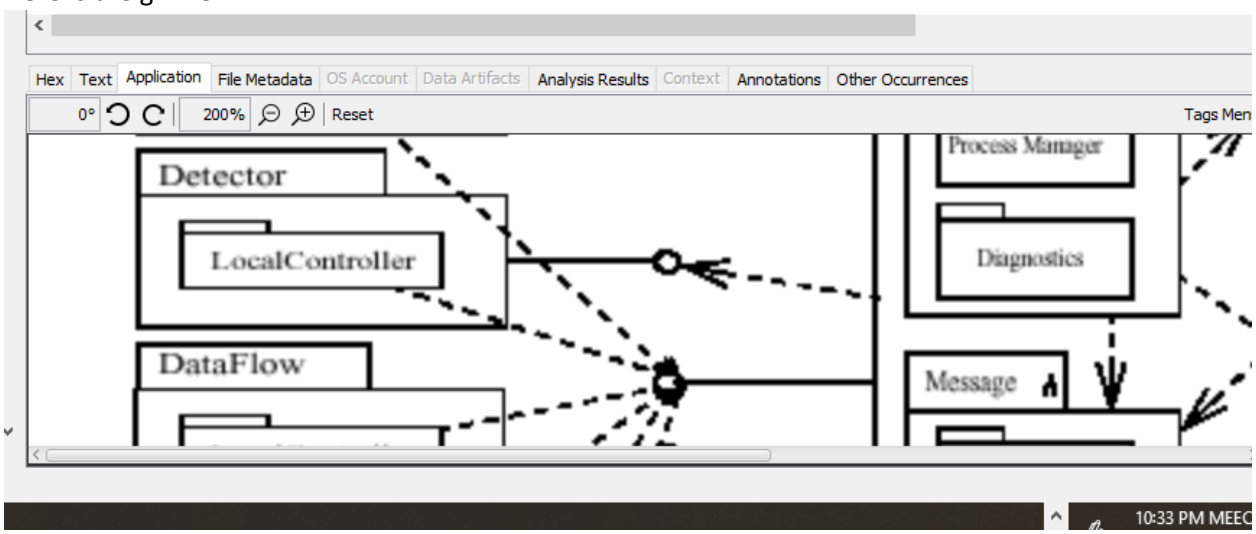
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occ

Metadata

Name:	/img_WinLabEnCase.E01/Documents and Settings/psmith/My Documents/Confidential/diagram.doc
Type:	File System
MIME Type:	image/gif
Size:	15480
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2004-01-24 21:27:46 EST
Accessed:	2004-03-09 00:00:00 EST
Created:	2004-03-09 11:38:50 EST
Changed:	0000-00-00 00:00:00
MD5:	81ec4f559263f56862b0552b3377c88e
SHA-256:	25df9af4b67746b26b72430c3bb9f6cf4495afe21f144acaa60d51a09a5ee4e3
Hash Lookup Results:	UNKNOWN

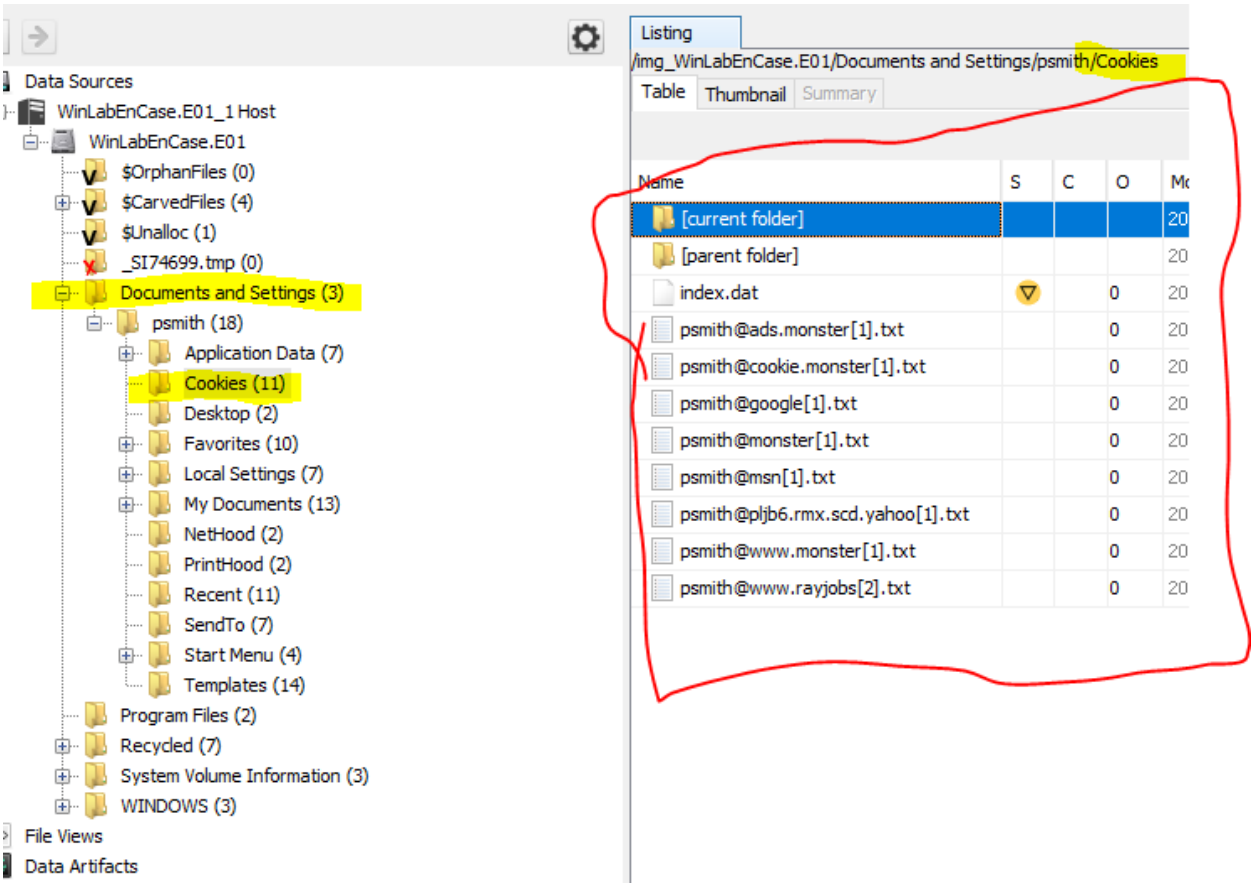
It is really a image/.gif file type.

- Here is the gif file:



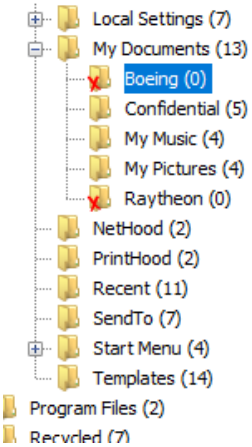
-
- Notice it is a schematic of some sort.
- This is potential evidence that he is hiding data inside of this file and sending it somewhere or downloading it.
-

d) Check cookies from \Documents and Settings\psmith\Cookies and identify the sites that stored cookies on psmith's machine during his visits.



Above are listed the websites that the user has visited and logged in to according to the cookies stored on their drive. I noticed he visited and logged into a site called **rayjobs.com**; thus, this is some evidence that Pat Smith is searching for a job.

Also as a side note, I notice two deleted folders named **Boeing** and **Raytheon** were found on the disk under his profile:



Here is what google search for rayjobs brings up:

rayjobs

All Shopping News Images Videos More Tools

About 167,000 results (0.46 seconds)

https://careers.rtx.com

Raytheon jobs: Careers at Raytheon

Doers, makers, creators: This is your moment. Find jobs at Raytheon in Digital Technology, Finance, Marketing and more. Join us and let's rise to the ...

Search results | Available job ...

Your search results for the jobs at Raytheon. Find the available ...

More results from rtx.com »

https://jobs.rayjobs.com › TGWebHost › searchresults

Raytheon Company - Search results

Browse and apply for our job opportunities. Search for current openings across the world.

https://www.indeed.com › q-X-Ray-I-Michigan-jobs

X Ray Jobs, Employment in Michigan | Indeed.com

350 X **Ray jobs** available in Michigan on Indeed.com. Apply to X-ray Technician, Technician, Technology Assistant and more!

Notice **rayjobs.com** is the name for their career application site. His machine stored login cookies for that site, so there is good reason to believe that Pat created a profile and logged into the site to apply for a job.

e) Files with the extension of .lnk are shortcuts or link files. Examine \Documents and Settings\psmith\Recent\Confidential.lnk. What is the file name and path that Confidential.lnk points to? (Hint: read its content by looking at the "result" and "File Metadata")

[parent folder]			2004-03-09 11:38:50 EST	0000-00-00 00:00:00	2004
cleanup.log.lnk		0	2004-01-24 20:35:26 EST	0000-00-00 00:00:00	2004
Confidential.lnk		0	2004-03-09 08:30:40 EST	0000-00-00 00:00:00	2004
Desktop.ini		0	2004-01-23 11:57:56 EST	0000-00-00 00:00:00	2004
diagram.gif.lnk		0	2004-03-09 08:30:40 EST	0000-00-00 00:00:00	2004
Outlook Express.lnk		0	2004-01-24 20:35:26 EST	0000-00-00 00:00:00	2004
Project 238x.rtf.lnk		0	2004-03-09 08:30:32 EST	0000-00-00 00:00:00	2004
Project 47x.doc.lnk		0	2004-03-09 08:30:14 EST	0000-00-00 00:00:00	2004
test.eml.lnk		0	2004-01-24 20:43:12 EST	0000-00-00 00:00:00	2004
You Won't Believe this Awesome Offer.eml.lnk		0	2004-01-24 20:54:14 EST	0000-00-00 00:00:00	2004

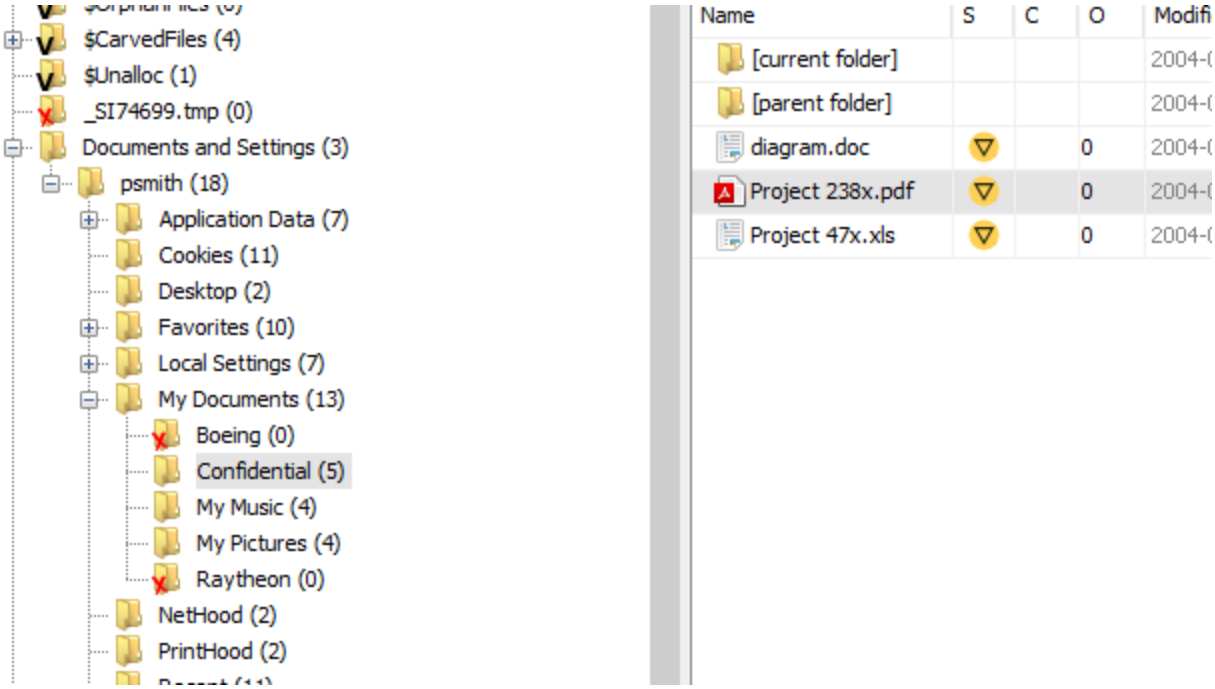
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 1 of 1 Result

Type	Value
Path	C:\Documents and Settings\psmith\My Documents\Confidential
Path ID	167
Date Accessed	2004-03-09 11:38:49 EST
Source File Path	/img_WinLabEnCase.E01/Documents and Settings/psmith/Recent/Confidential.lnk
Artifact ID	-9223372036854775805

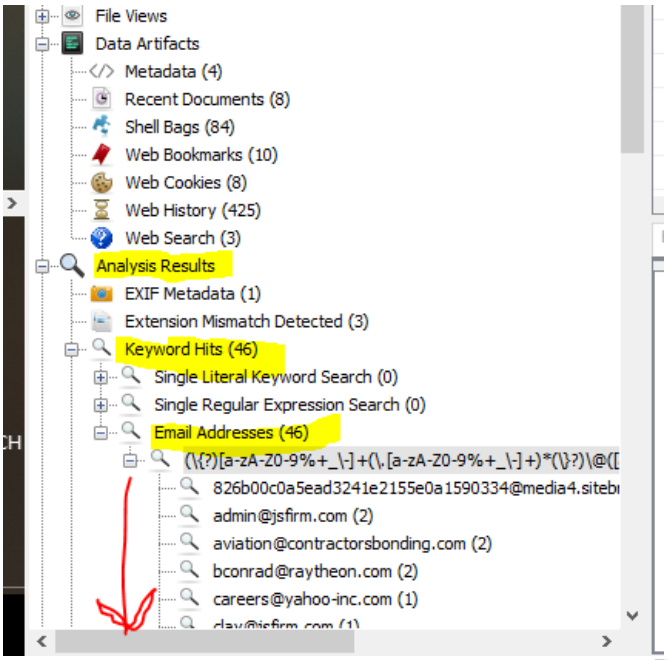
The shortcut file contains a data segment showing that the file stores a pointer to the path as highlighted → documents and settings\psmith\my documents\Confidential.

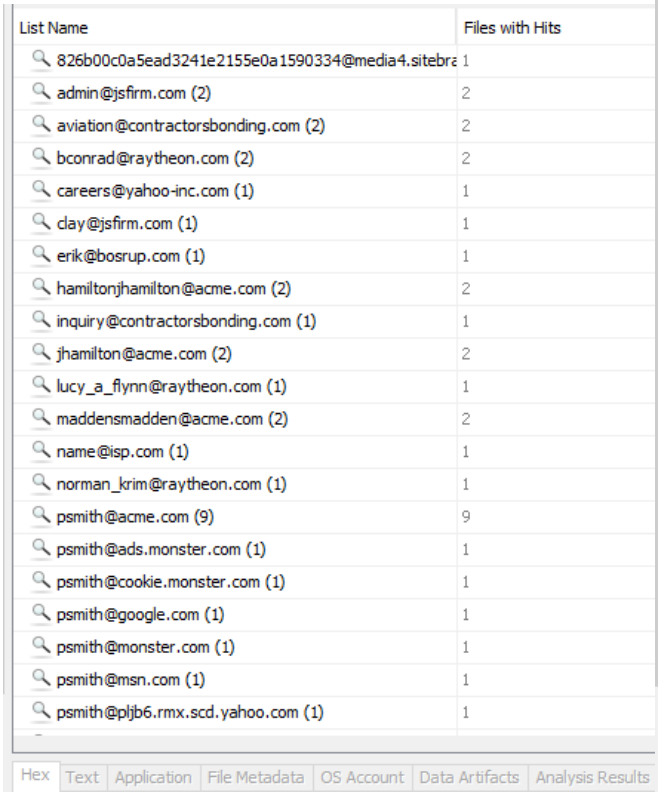
Here are the contents under that directory:



Notice that diagram.doc is under this directory and has the mismatch extension. Also, the project238x and 47x is property of ACME industries and is confidential. This is not yet incriminating however because he is only doing this within the company and has not been proven at this point in this investigatory document to have sent this information to anyone not authorized to receive it.

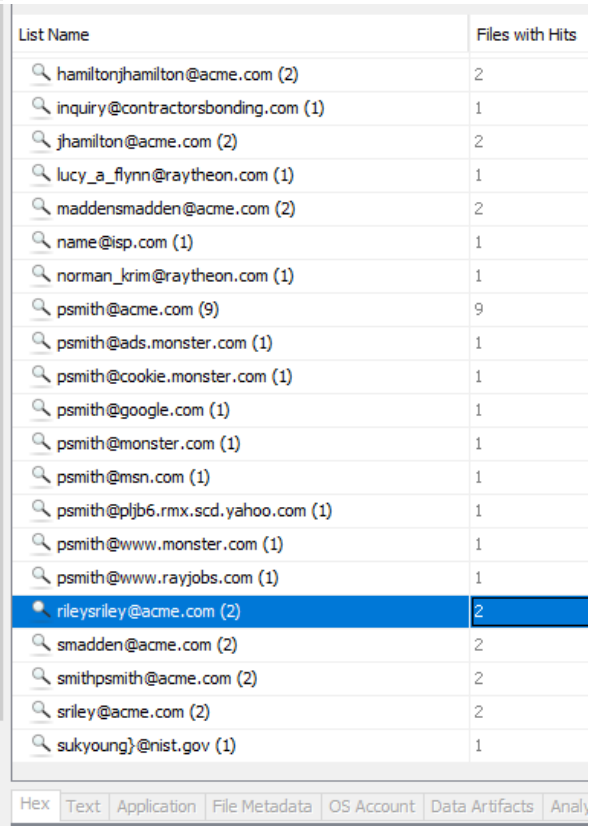
12. Perform a keyword search on email address: Click the Keyword Lists (on the top left corner) and Check the Email check box, then click Search, Check Results > Keyword Hits > Email Addresses. Did you find any pertinent evidence (e.g. job offers, attempt to leak company information)? Include those evidence in your report.





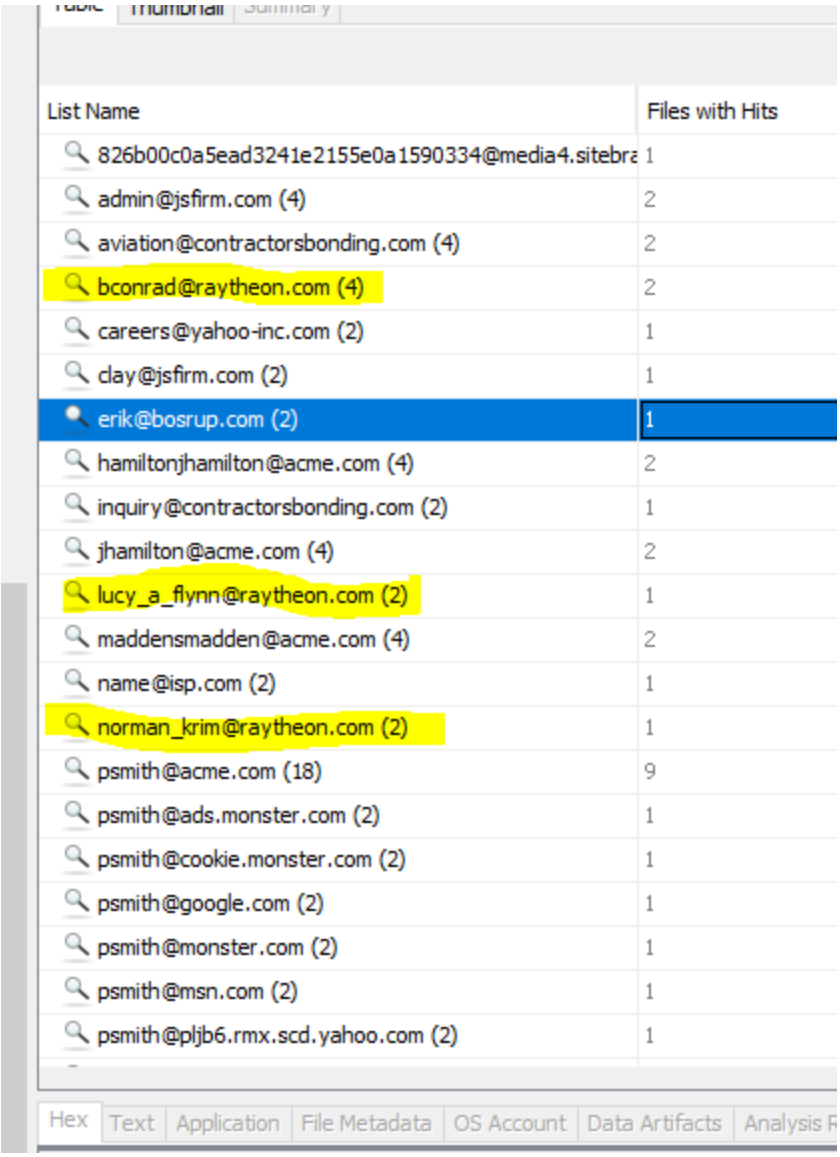
List Name	Files with Hits
826b00c0a5ead3241e2155e0a1590334@media4.sitebra	1
admin@jsfirm.com (2)	2
aviation@contractorsbonding.com (2)	2
bconrad@raytheon.com (2)	2
careers@yahoo-inc.com (1)	1
clay@jsfirm.com (1)	1
erik@bosrup.com (1)	1
hamiltonjhamilton@acme.com (2)	2
inquiry@contractorsbonding.com (1)	1
jhamilton@acme.com (2)	2
lucy_a_flynn@raytheon.com (1)	1
maddensmadden@acme.com (2)	2
name@isp.com (1)	1
norman_krim@raytheon.com (1)	1
psmith@acme.com (9)	9
psmith@ads.monster.com (1)	1
psmith@cookie.monster.com (1)	1
psmith@google.com (1)	1
psmith@monster.com (1)	1
psmith@msn.com (1)	1
psmith@pljb6.rmx.scd.yahoo.com (1)	1

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results



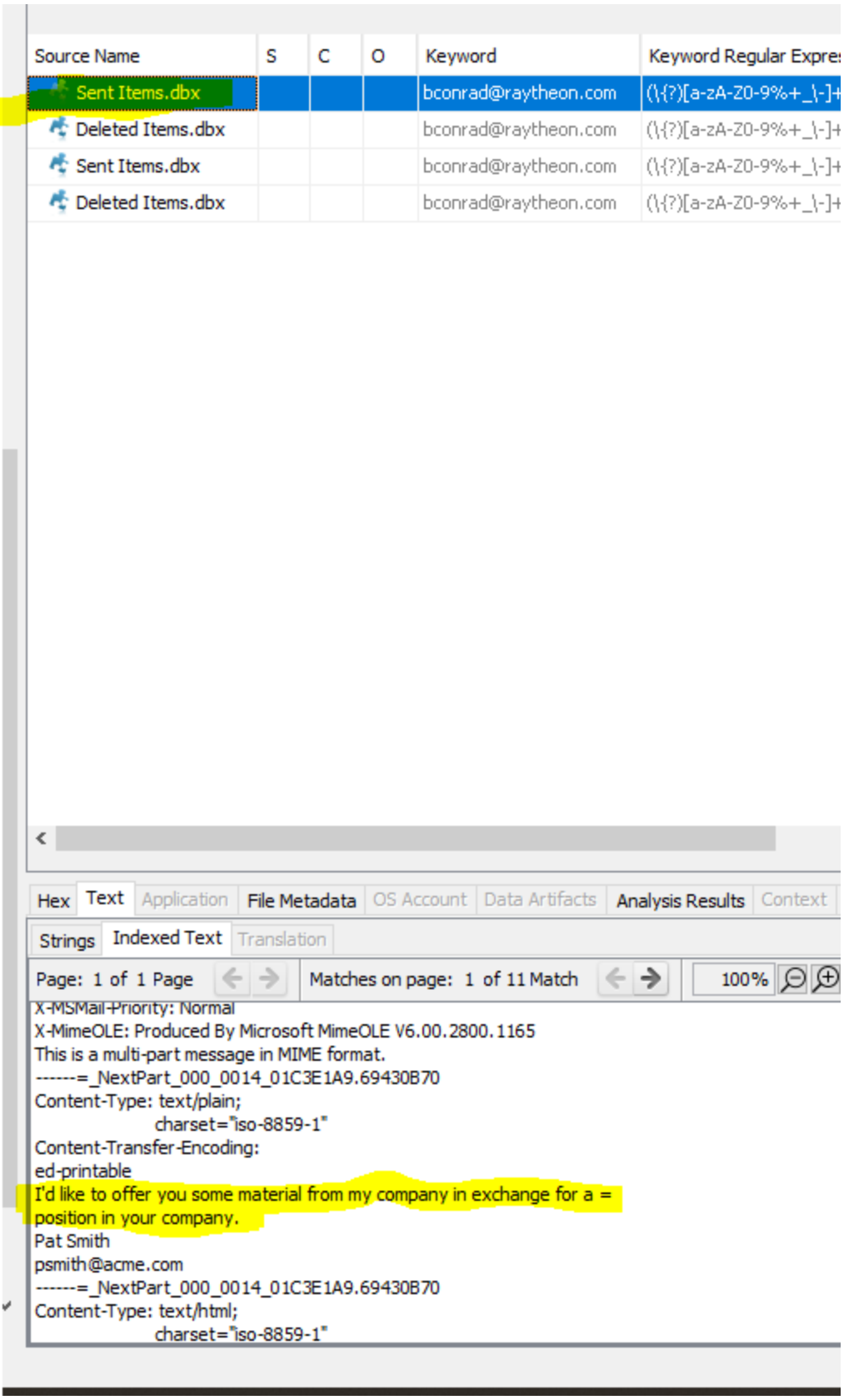
List Name	Files with Hits
hamiltonjhamilton@acme.com (2)	2
inquiry@contractorsbonding.com (1)	1
jhamilton@acme.com (2)	2
lucy_a_flynn@raytheon.com (1)	1
maddensmadden@acme.com (2)	2
name@isp.com (1)	1
norman_krim@raytheon.com (1)	1
psmith@acme.com (9)	9
psmith@ads.monster.com (1)	1
psmith@cookie.monster.com (1)	1
psmith@google.com (1)	1
psmith@monster.com (1)	1
psmith@msn.com (1)	1
psmith@pljb6.rmx.scd.yahoo.com (1)	1
psmith@www.monster.com (1)	1
psmith@www.rayjobs.com (1)	1
rileysriley@acme.com (2)	2
smadden@acme.com (2)	2
smithpsmith@acme.com (2)	2
sriley@acme.com (2)	2
sukyoung}@nist.gov (1)	1

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analy

- 

List Name	Files with Hits
826b00c0a5ead3241e2155e0a1590334@media4.sitebra	1
admin@jsfirm.com (4)	2
aviation@contractorsbonding.com (4)	2
bconrad@raytheon.com (4)	2
careers@yahoo-inc.com (2)	1
clay@jsfirm.com (2)	1
erik@bosrup.com (2)	1
hamiltonjhamilton@acme.com (4)	2
inquiry@contractorsbonding.com (2)	1
jhamilton@acme.com (4)	2
lucy_a_flynn@raytheon.com (2)	1
maddensmadden@acme.com (4)	2
name@isp.com (2)	1
norman_krim@raytheon.com (2)	1
psmith@acme.com (18)	9
psmith@ads.monster.com (2)	1
psmith@cookie.monster.com (2)	1
psmith@google.com (2)	1
psmith@monster.com (2)	1
psmith@msn.com (2)	1
psmith@pljb6.rmx.scd.yahoo.com (2)	1

  - Notice he sent and received mail from Raytheon.com to email users Lucy Flynn, B Conrad, and Norman Krim
  - Here is one of the email exchanges where Pat sent a request to Ben from RAYTHEON asking for a position in the company in exchange for information from ACME company:


Source Name
S
C
O
Keyword
Keyword Regular Expres
Sent Items.dbx
bconrad@raytheon.com
(\{?)[a-zA-Z0-9%+_\-]+
Deleted Items.dbx
bconrad@raytheon.com
(\{?)[a-zA-Z0-9%+_\-]+
Sent Items.dbx
bconrad@raytheon.com
(\{?)[a-zA-Z0-9%+_\-]+
Deleted Items.dbx
bconrad@raytheon.com
(\{?)[a-zA-Z0-9%+_\-]+
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Strings
Indexed Text
Translation
Page: 1 of 1 Page
Matches on page: 1 of 11 Match
100%
X-MSMail-Priority: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
This is a multi-part message in MIME format.
------=_NextPart_000_0014_01C3E1A9.69430B70
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding:
ed-printable
I'd like to offer you some material from my company in exchange for a =
position in your company.
Pat Smith
psmith@acme.com
------=_NextPart_000_0014_01C3E1A9.69430B70
Content-Type: text/html;
charset="iso-8859-1"

-
-

Summary/Reflection

Include a brief reflection on what you learned (one or two paragraphs).

I learned that the ACME graphical user interface tool is very powerful for analyzing the contents of a disk. It automatically finds deleted files and directories that have not yet been overwritten with contents from a new file, it analyzes the meta data of the file system and all files and allows you to get the true file types. The auto-analysis feature is probably the most powerful feature because it allows you to quickly and effectively (although not as complete) audit a drive to find important or key information. According to my investigation, it is clear that there is good evidence Pat is trying to get a job at Raytheon, and there is even evidence that he sent an email offering company information in exchange for a job.