

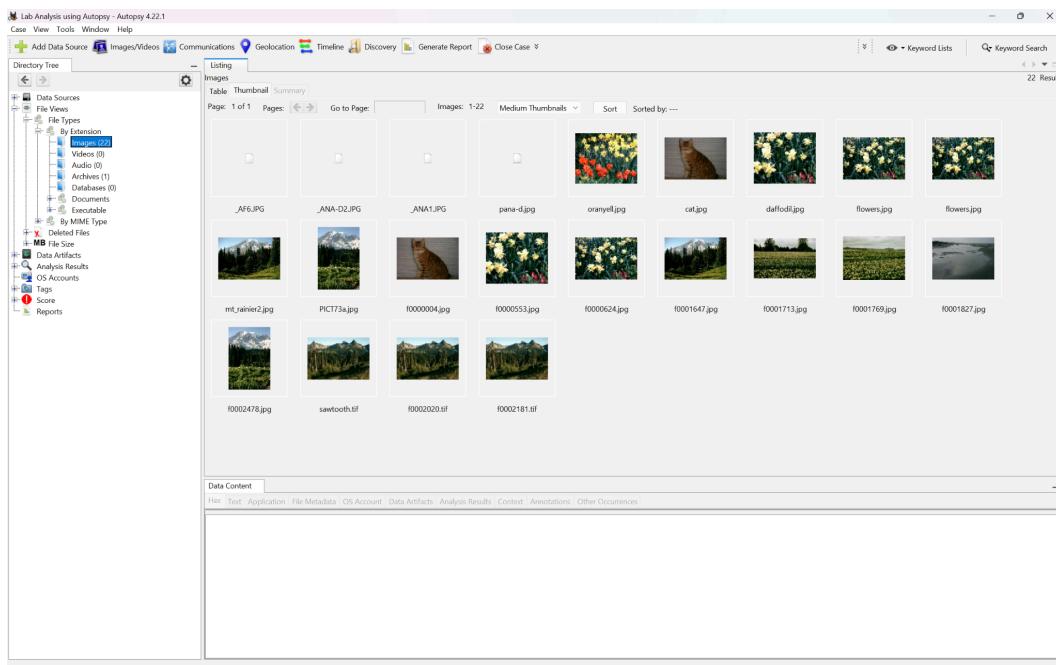
Computer & Network Forensics

Lab 4

Forensics Analysis using Autopsy

Questions

1. How many images are viewable in thumbnail mode?



→ 18 viewable images, and 4 not (total 22)

2. Investigating the image _AF6.JPG using alternative options. What did I find?

Autopsy Analysis Results:

The Autopsy interface shows a list of files under the 'Images' tab. The file '_AF6.JPG' is selected, and its context menu is open, displaying options such as 'View File in Directory', 'View File in Timeline...', 'Open in External Viewer Ctrl+E', 'Extract File(s)', 'Export Selected Rows to CSV', 'Add File Tag', 'Remove File Tag', and 'Properties'. Other files listed include _ANA1.JPG, pana-djng, orangell.jpg, cat.jpg, daffodil.jpg, flowers.jpg, flowers.jpg, f0000004.jpg, f000053.jpg, f0000624.jpg, f0001647.jpg, f0001713.jpg, f0001769.jpg, f0001827.jpg, f0002478.jpg, sawooth.tif, f0002020.tif, and f0002181.tif.

File Content:

Three FTK Editor windows are shown side-by-side, all displaying the same file content:

```

/ /img_ftk-demo1-image.1/work/_AF6.JPG - Editor
/ /img_ftk-demo1-image.1/work/_AF6.JPG - Editor
/ /img_ftk-demo1-image.1/work/_AF6.JPG - Editor

```

The content of the file is as follows:

```

Hex Text Application File Metadata Context Annotations Other Occurrences
Page: 1 of 1 Page Go to Page: 1 Jump to Offset: 1
0x00000000: 0D 0A 47 65 6F 72 67 65 0D 0A 41 72 65 20 79 6F ..George..Are yo
0x00000010: 75 20 73 75 72 65 20 79 6F 75 20 6B 6E 6F 77 20 u sure you know
0x00000020: 77 68 61 74 20 79 67 75 20 61 72 20 64 6E 6F what you are doi
0x00000030: 6E 67 2E 20 74 39 73 6E 27 74 20 69 74 20 64 61 6E ng. Isn't it dan
0x00000040: 67 65 72 60 75 73 2c 20 77 6F 6E 27 74 20 79 6F gerous, won't yo
0x00000050: 72 65 73 60 75 73 2c 20 77 6F 6E 27 74 20 79 6F u get caught?...
0x00000060: 0A 4D 61 72 74 68 09 0A 20 20 20 20 20 20 20 20 .Marth.
0x00000070: 20 20 20 20 20 20 20 00 00 00 00 00 00 00 00 00 ..... .
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0x000000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .

```

File Metadata:

The file metadata is as follows:

Metadata	Value
Name:	/img_ftk-demo1-image.1/work/_AF6.JPG
Type:	File System
MIME type:	application/octet-stream
Size:	238
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2003-02-15 14:36:00 GMT
Accessed:	2003-02-15 00:00:00 GMT
Created:	2003-02-15 15:39:28 GMT
Changed:	0000-00-00 00:00:00
MD5:	537e851201414538c9ff31448f31a848
SHA-256:	c295f5aa1544ebacf6d1bfeec432ae1742fe9b04a82feed3c7b3d964027a4c
Hash Lookup Results:	UNKNOWN
Internal ID:	46

From The Sleuth Kit istat Tool:

Directory Entry: 264

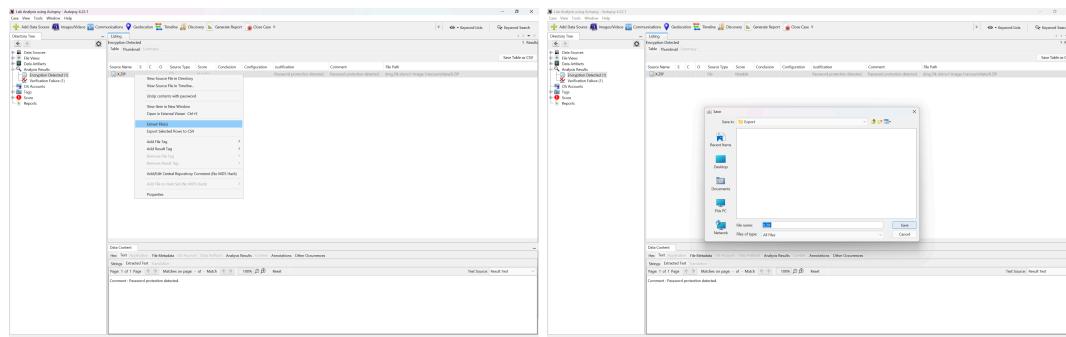
→ Secret message:

“George

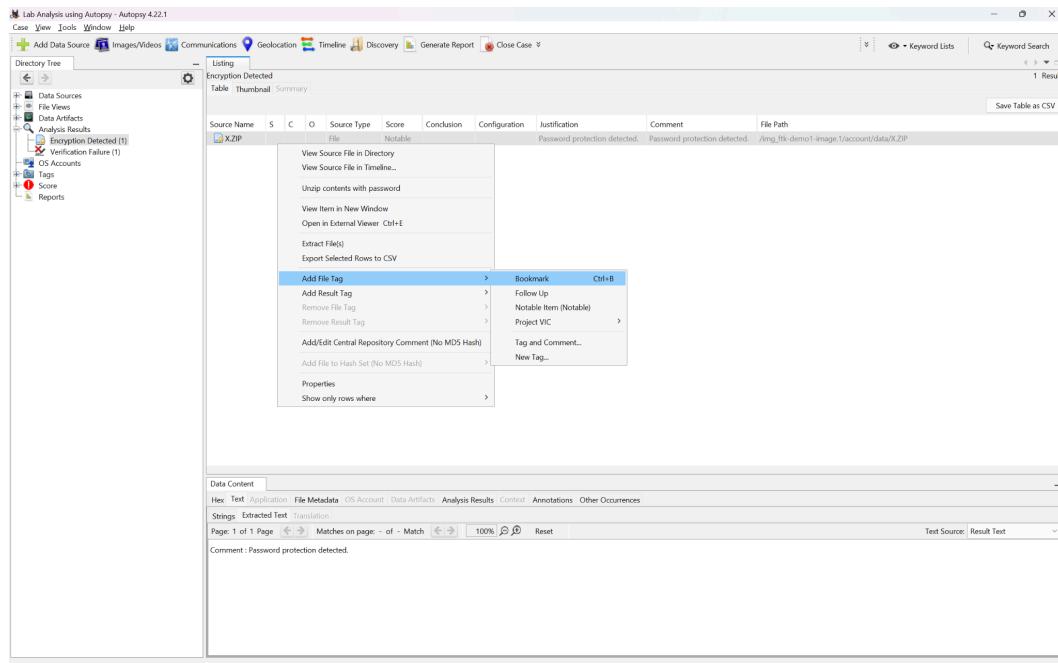
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?
Marth”

(More info included in the report)

3. What happens when I try to unzip the encrypted folder?
 Screen shot and detail the steps I took.



→ Export File



→ Add Bookmark File Tag

Name	Keyword Preview	Location	Modified Time	Change Time
Encryption Detected Artifact	Comment ->password- protection detected.	/Img_ftk-demo1-image/1/account/data/X.ZIP	2003-02-15 13:13:12 GMT	0000-00-00 00:00:00
Unalloc_4_17920_1474560	minute. You can find the <password> for the encrypted.. /Img_ftk-demo1-image/1\$Unalloc_4_17920_..	0000-00-00 00:00:00	0000-00-00 00:00:00	
SG8.TXT	You can find the <password> for the encrypted.. /Img_ftk-demo1-image/1\$0\$pharFile\$SG8.TXT	2003-02-15 12:54:06 GMT	0000-00-00 00:00:00	
_Y_EXE	minute. You can find the <password> for the encrypted.. /Img_ftk-demo1-image/1/work/_Y_EXE	2003-02-15 14:40:34 GMT	0000-00-00 00:00:00	
R0000003.txt	minute. You can find the <password> for the encrypted.. /Img_ftk-demo1-image/1\$carvedFiles/1/R0000003.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	
mt_bank_secrecy.htm	JtM Mr. Jones. The <password> for your account is: /Img_ftk-demo1-image/1/account/data/mt_bank_secre_..	2003-02-15 13:38:36 GMT	0000-00-00 00:00:00	

→ Keyword Search (“password”)

The screenshot shows the Autopsy interface with a context menu open over a file entry in the left pane. The menu options include 'Open Source File in Checker', 'Open Source File in Finder', 'Open in New Window', 'Extract', 'Export Selected Files to CSV', 'Add File Tag', 'Edit File Tag', 'Remove File Tag', and 'Additional Context Dependency Generated by this Entry'. Below the menu, a status bar indicates 'Found 1 password protected artifact'.

The 'Enter Password' dialog is centered in the foreground, containing a text input field with the value 'couch' and two buttons: 'OK' and 'Cancel'.

→ Unzip X.ZIP with password (“couch”)

Lab Analysis using Autopsy - Autopsy 4.22.1

Case View Tools Window Help

Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Save Table as CSV

Source Name S C O Description Owner Data Source Date Created Date Modified User ID Program Name Organization

02/1220.msg RE:A plan James ftk-demo1-image.1
 02/1229.msg Re: A plan Jones ftk-demo1-image.1
 02/1218.msg A plan Jones ftk-demo1-image.1
 02/1230.msg RE:A plan ftk-demo1-image.1

SWISS.XLS Bill Nelson ftk-demo1-image.1 2002-08-16 21:39:27 IST 2002-08-16 22:38:14 IST pc Microsoft Excel The Boeing Company

File Views Metadata

Data Sources Data Artifacts Analysis Results Encrypted Detected (1) Keyword Hits (6) Verification Failure (1) OS Accounts Tags Score Reports

SWISS.XLS

Data Content

New Test Application Source File Metadata OS Account Data Artifacts Analysis Results Content Annotations Other Occurrences

Result: 1 of 1 Result

Type	Value	Source(s)
Date Created	2002-08-16 21:39:27 IST	org.sleuthkit.autopsy.keywordsearch.Key
Date Modified	2002-08-16 22:38:14 IST	org.sleuthkit.autopsy.keywordsearch.Key
User ID	pc	org.sleuthkit.autopsy.keywordsearch.Key
Program Name	Microsoft Excel	org.sleuthkit.autopsy.keywordsearch.Key
Organization	The Boeing Company	org.sleuthkit.autopsy.keywordsearch.Key
Owner	Bill Nelson	org.sleuthkit.autopsy.keywordsearch.Key
Source File Path	/tmp/ftk-demo1-image.1/account/data/X.ZIP/SWISS.XLS	org.sleuthkit.autopsy.keywordsearch.Key
Artifact ID	-922372036854775800	org.sleuthkit.autopsy.keywordsearch.Key

→ The unzipped file (SWIZZ.XLS) is showing in “*Data Artifacts/Metadata*” We can view the content of the unzipped, decrypted files.

(More info included in the report)

4. How many files contain the word "password" and assess their relevance to the case.

The screenshot shows the Autopsy 4.22.1 interface with a keyword search results table. The search term is "password".

Autopsy 4.22.1 - Keyword search 1 - password

Results (6)

Save Table as CSV

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	\$
Encryption Detected Artifact	Comment: «password» protection detected.	/img_nk_demel-1-image/1/account/data/XZP	2003-02-15 13:13:12 GMT	2000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:52:36 GMT	6
Unalloc_4_17920_1474560	minutes. You can find the «password» for the encrypted.	/img_nk_demel-1-image/1/Unalloc/Unalloc_4_17920_-	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	1
Verification Failure (1)	You can find the «password» for the encrypted	/img_nk_demel-1-image/1/OrphanFiles/_SGR.TXT	2003-02-15 12:54:05 GMT	2000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:49:42 GMT	1
OS Accounts	minutes. You can find the «password» for the encrypted.	/img_nk_demel-1-image/1/fwntn_-_TDE	2003-02-15 14:40:34 GMT	2000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:39:16 GMT	1
Tags	minutes. You can find the «password» for the encrypted.	/img_nk_demel-1-image/1/ScarvedFiles/1/00000003.txt	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	1
Score	Jim Mr. Jones. The «password» for your account is:	/img_nk_demel-1-image/1/account/data/mr_bank_sec_	2003-02-15 13:38:36 GMT	2000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:54:12 GMT	2
Reports	mt_bank_secrey.htm						

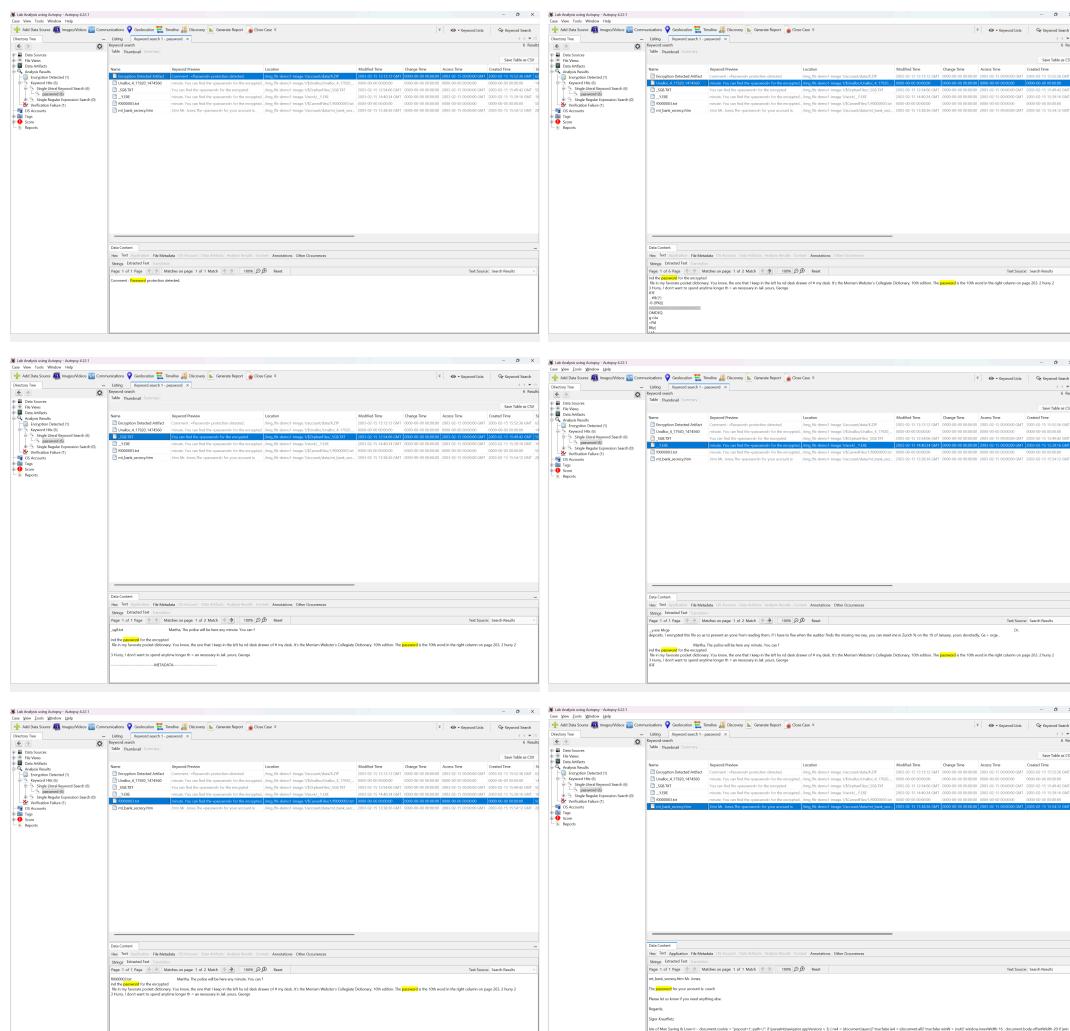
Data Content

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

Strings Extracted Text Translation

Page: 1 of Page ⏪ Go to Page: Script: Latin - Basic

→ 6 files contain the word “password”



→ The first one is the Encryption Detected Artifact (X.ZIP – /img_ftk-demo1-image.1/account/data/X.ZIP), that contains: “*Comment : Password protection detected.*”

→ The next 4 files (Unalloc 4 17920 1474560, SG8.TXT, Y.EXE, f0000003.txt) contain the same information: “*You can find the password for the encrypted file in my favorite pocket dictionary. ... It's the Merriam Webster's Collegiate Dictionary, 10th edition. The password is the 10th word in the right column on page 263.*”

→ The last file (mt_bank_secrecy.htm – /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm), that contains the message from the bank: “*... The password for your account is: couch ...*”

(More info included in the report)

5. Determine how many text files (.txt) can be found throughout the image.

The screenshot shows the Autopsy 4.2.1 interface with a search results table for 'text/plain' files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The results are as follows:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
x.msg7.txt				2003-01-15 12:45:44 GMT	2000-05-00 00:00:00	2003-01-15 00:00:00	2003-02-15 15:49:35 GMT	662	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/personal/Messages/msg7.txt
x.msg5.txt				2003-02-15 12:44:16 GMT	2000-05-00 00:00:00	2003-02-15 00:00:00	2003-02-15 15:48:33 GMT	316	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/personal/Messages/msg5.txt
x.msg4.txt				2003-02-15 12:43:30 GMT	2000-05-00 00:00:00	2003-02-15 00:00:00	2003-02-15 15:47:18 GMT	453	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/week/msg4.txt
x>All.S.GIF				2003-02-15 14:35:04 GMT	2000-05-00 00:00:00	2003-02-15 00:00:00	2003-02-15 15:43:42 GMT	487	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/SophareFile/EST/All.S.GIF
✓ 80000001.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	662	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00000001.txt
✓ 80000003.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	506	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00000003.txt
✓ 80000552.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	119	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00000552.txt
✓ 80001487.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	101	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00001487.txt
✓ 80002180.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00002180.txt
✓ 80002722.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	633	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00002722.txt
✓ 80002728.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3660	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00002728.txt
✓ 80002737.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	316	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00002737.txt
✓ 80002738.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	179	Unallocated	Unallocated	unknown	/img_flik-demo1-image/1/ScavelliFiles/1/00002738.txt
SWISS.TXT	1	2003-02-15 10:47:05 GMT		2000-05-00 00:00:00	2000-05-00 00:00:00	2000-05-00 00:00:00	2000-05-00 00:00:00	2429	Allocated	Allocated	unknown	/img_flik-demo1-image/1/account/data/XZIP/SWISS.TXT

→ There is 13 .txt files and one .gif (contains SWISS.TXT form X.ZIP archive)

The screenshot shows the Autopsy 4.2.1 interface with a search results table for 'text/csv' files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The results are as follows:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
SWISS.CSV				2003-02-15 10:46:40 GMT	2000-05-00 00:00:00	2000-05-00 00:00:00	2000-05-00 00:00:00	2429	Allocated	Allocated	unknown	/MD5 Hash /img_flik-demo1-image/1/account/data/XZIP/SWISS.CSV

→ There is 1 .csv file (SWISS.CSV form X.ZIP archive)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
mt_bank.htm				2003-02-15 13:35:10 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:55:21 GMT	1881	Unallocated	Unallocated	unknown	/img_ftk-demo1-image.1/account/mt_bank
mt_bank_secrecy.htm		2		2003-02-15 13:38:36 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:54:12 GMT	2828	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/account/data/mt
f0001705_mt_bank.html		2		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1879	Unallocated	Unallocated	unknown	/img_ftk-demo1-image.1/\$CarvedFiles/1/0

→ There is 3 htm/html files

Bank web files:

- /img_ftk-demo1-image.1/account/mt_bank.htm
- /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm
- /img_ftk-demo1-image.1/\$CarvedFiles/1/f0001705_mt_bank.html

(More info included in the report)

6. Determine how we know that George has been using Outlook Express to send messages, we can rely on file extensions, which provide important clues about the software used.

Name	S	C	O	Modified Time	Change Time	Access Time	N/Created Time	Size	Flag(Dir)	Flag(Meta)	Known	Location
m-021230.msg	2			2003-02-15 12:03:32 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:57:15 GMT	519	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/personal/Messages/m-021230.msg
g-021218.msg	2			2003-02-15 11:51:20 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:57:12 GMT	256	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/personal/Messages/g-021218.msg
g-021229.msg	2			2003-02-15 11:54:42 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:57:12 GMT	550	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/personal/Messages/g-021229.msg
m-021220.msg	2			2003-02-15 11:53:22 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:57:09 GMT	268	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/personal/Messages/m-021220.msg

→ George used Outlook to communicate with Martha, as evidenced by .msg files

Left Window (Raw Text):

```

George.
What are you talking about, what's the big deal?
Martha
-----Original Message-----
From: Jones, George [mailto:georgej@widgets.intl.com]
Sent: 29 December 2001 10:52
To: James, Martha [marthaj@widgets.intl.com]
Subject: Re: A plan

I can't talk about it now, it will have to wait until we can talk in private. Maybe Year's Eve.

George

```

Right Window (Metadata):

```

Content-Type: message/rfc822
Message-From: James
Message-To: Jones
Message-From-Email: [marthaj@widgets.intl.com]
Message-From-Name: Martha
Message-Raw-Header-Sent: 30 December 2001 11:32
X-TIKA-Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA-Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
ccreator: James
dcsubject: REA plan
dcTitle: REA plan
resourceName: REA plan.eml

```

→ /img_ftk-demo1-image.1/personal/Messages/m-021230.msg

The screenshot shows two side-by-side FTK Editor windows. Both windows have the title bar /img_ftk-demo1-image.1/personal/Messages/g-021218.msg - Editor. The left window displays the message body with two messages from George and one from Martha. The right window shows the same message body with additional metadata at the bottom.

Message Body (Left Window):

```

Martha,
I have a plan to pay for our vacation next Spring. I'll tell you about it later.

George

-----METADATA-----
Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: georgej@widgets.intl.com
Message-From-Name: Jones
Message-Raw-Header-Sent: 18 December 2001 18:37
X-TIKA-Parsed-By: org.apache.tika.parser.DefaultParser

```

Message Body (Right Window):

```

George

-----METADATA-----
Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: georgej@widgets.intl.com
Message-From-Name: Jones
Message-Raw-Header-Sent: 18 December 2001 18:37
X-TIKA-Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA-Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
dcCreator: Jones
dcSubject: A plan
dcTitle: A plan
resourceName: A plan.eml

```

→ /img_ftk-demo1-image.1/personal/Messages/g-021218.msg

The screenshot shows two side-by-side FTK Editor windows. Both windows have the title bar /img_ftk-demo1-image.1/personal/Messages/g-021229.msg - Editor. The left window displays the message body with two messages from George and one from Martha. The right window shows the same message body with additional metadata at the bottom.

Message Body (Left Window):

```

I can't talk about it now, it will have to wait until we can talk in private. Maybe Year's Eve.

George

-----Original Message-----
From: Jones, George [mailto:georgej@widgets.intl.com]
Sent: 26 December 2001 08:02
To: James; Martha [marthaj@widgets.intl.com]
Subject: A plan

Martha,
I have a plan to pay for our vacation next Spring. I'll tell you about it later.

George

```

Message Body (Right Window):

```

George

-----METADATA-----
Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: georgej@widgets.intl.com
Message-From-Name: Jones
Message-Raw-Header-Sent: 29 December 2001 10:52
X-TIKA-Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA-Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
dcCreator: Jones
dcSubject: Re: A plan
dcTitle: Re: A plan
resourceName: Re: A plan.eml

```

→ /img_ftk-demo1-image.1/personal/Messages/g-021229.msg

The screenshot shows two side-by-side FTK Editor windows. Both windows have the title bar /img_ftk-demo1-image.1/personal/Messages/m-021220.msg - Editor. The left window displays the message body with two messages from George and one from Martha. The right window shows the same message body with additional metadata at the bottom.

Message Body (Left Window):

```

George,
What kind of plan do you have to get the money for the mountain vacation you want so badly?

Martha

-----METADATA-----
Content-Type: message/rfc822
Message-From: James
Message-To: Jones
Message-From-Email: [marthaj@widgets.intl.com]
Message-From-Name: Martha
Message-Raw-Header-Sent: 20 December 2001 09:44
X-TIKA-Parsed-By: org.apache.tika.parser.DefaultParser

```

Message Body (Right Window):

```

-----METADATA-----
Content-Type: message/rfc822
Message-From: James
Message-To: Jones
Message-From-Email: [marthaj@widgets.intl.com]
Message-From-Name: Martha
Message-Raw-Header-Sent: 20 December 2001 09:44
X-TIKA-Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA-Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
dcCreator: James
dcSubject: RE:A plan
dcTitle: RE:A plan
resourceName: RE:A plan.eml

```

→ /img_ftk-demo1-image.1/personal/Messages/m-021220.msg

(More info included in the report)

7. Generate a report based on the facts uncovered during my investigation using Autopsy.

The image displays two windows of the Autopsy software's 'Report' feature. The left window is titled 'Summary' and contains a table with the following data:

Case Name	Lab Analysis using Autopsy
Collector	007
Number of data sources in case	1
Timestamp	
A2	
B2	
C2	
D2	
E2	
F2	
G2	
H2	
I2	
J2	
K2	
L2	
M2	
N2	
O2	
P2	
Q2	
R2	
S2	
T2	
U2	
V2	
W2	
X2	
Y2	
Z2	
AA2	
AB2	
AC2	
AD2	
AE2	
AF2	
AG2	
AH2	
AI2	
AJ2	
AK2	
AL2	
AM2	
AN2	
AO2	
AP2	
AQ2	
AR2	
AS2	
AT2	
AU2	
AV2	
AW2	
AX2	
AY2	
AZ2	
BA2	
BB2	
BC2	
BD2	
BE2	
BF2	
BG2	
BH2	
BI2	
BJ2	
BK2	
BL2	
BM2	
BN2	
BO2	
BP2	
BQ2	
BR2	
BS2	
BT2	
BU2	
BV2	
BW2	
BY2	
AZ3	
BA3	
BB3	
BC3	
BD3	
BE3	
BF3	
BG3	
BH3	
BI3	
BJ3	
BK3	
BL3	
BM3	
BN3	
BO3	
BP3	
BQ3	
BR3	
BS3	
BT3	
BU3	
BV3	
BW3	
BY3	
AZ4	
BA4	
BB4	
BC4	
BD4	
BE4	
BF4	
BG4	
BH4	
BI4	
BJ4	
BK4	
BL4	
BM4	
BN4	
BO4	
BP4	
BQ4	
BR4	
BS4	
BT4	
BU4	
BV4	
BW4	
BY4	
AZ5	
BA5	
BB5	
BC5	
BD5	
BE5	
BF5	
BG5	
BH5	
BI5	
BJ5	
BK5	
BL5	
BM5	
BN5	
BO5	
BP5	
BQ5	
BR5	
BS5	
BT5	
BU5	
BV5	
BW5	
BY5	
AZ6	
BA6	
BB6	
BC6	
BD6	
BE6	
BF6	
BG6	
BH6	
BI6	
BJ6	
BK6	
BL6	
BM6	
BN6	
BO6	
BP6	
BQ6	
BR6	
BS6	
BT6	
BU6	
BV6	
BW6	
BY6	
AZ7	
BA7	
BB7	
BC7	
BD7	
BE7	
BF7	
BG7	
BH7	
BI7	
BJ7	
BK7	
BL7	
BM7	
BN7	
BO7	
BP7	
BQ7	
BR7	
BS7	
BT7	
BU7	
BV7	
BW7	
BY7	
AZ8	
BA8	
BB8	
BC8	
BD8	
BE8	
BF8	
BG8	
BH8	
BI8	
BJ8	
BK8	
BL8	
BM8	
BN8	
BO8	
BP8	
BQ8	
BR8	
BS8	
BT8	
BU8	
BV8	
BW8	
BY8	
AZ9	
BA9	
BB9	
BC9	
BD9	
BE9	
BF9	
BG9	
BH9	
BI9	
BJ9	
BK9	
BL9	
BM9	
BN9	
BO9	
BP9	
BQ9	
BR9	
BS9	
BT9	
BU9	
BV9	
BW9	
BY9	
AZ10	
BA10	
BB10	
BC10	
BD10	
BE10	
BF10	
BG10	
BH10	
BI10	
BJ10	
BK10	
BL10	
BM10	
BN10	
BO10	
BP10	
BQ10	
BR10	
BS10	
BT10	
BU10	
BV10	
BW10	
BY10	
AZ11	
BA11	
BB11	
BC11	
BD11	
BE11	
BF11	
BG11	
BH11	
BI11	
BJ11	
BK11	
BL11	
BM11	
BN11	
BO11	
BP11	
BQ11	
BR11	
BS11	
BT11	
BU11	
BV11	
BW11	
BY11	
AZ12	
BA12	
BB12	
BC12	
BD12	
BE12	
BF12	
BG12	
BH12	
BI12	
BJ12	
BK12	
BL12	
BM12	
BN12	
BO12	
BP12	
BQ12	
BR12	
BS12	
BT12	
BU12	
BV12	
BW12	
BY12	
AZ13	
BA13	
BB13	
BC13	
BD13	
BE13	
BF13	
BG13	
BH13	
BI13	
BJ13	
BK13	
BL13	
BM13	
BN13	
BO13	
BP13	
BQ13	
BR13	
BS13	
BT13	
BU13	
BV13	
BW13	
BY13	
AZ14	
BA14	
BB14	
BC14	
BD14	
BE14	
BF14	
BG14	
BH14	
BI14	
BJ14	
BK14	
BL14	
BM14	
BN14	
BO14	
BP14	
BQ14	
BR14	
BS14	
BT14	
BU14	
BV14	
BW14	
BY14	
AZ15	
BA15	
BB15	
BC15	
BD15	
BE15	
BF15	
BG15	
BH15	
BI15	
BJ15	
BK15	
BL15	
BM15	
BN15	
BO15	
BP15	
BQ15	
BR15	
BS15	
BT15	
BU15	
BV15	
BW15	
BY15	
AZ16	
BA16	
BB16	
BC16	
BD16	
BE16	
BF16	
BG16	
BH16	
BI16	
BJ16	
BK16	
BL16	
BM16	
BN16	
BO16	
BP16	
BQ16	
BR16	
BS16	
BT16	
BU16	
BV16	
BW16	
BY16	
AZ17	
BA17	
BB17	
BC17	
BD17	
BE17	
BF17	
BG17	
BH17	
BI17	
BJ17	
BK17	
BL17	
BM17	
BN17	
BO17	
BP17	
BQ17	
BR17	
BS17	
BT17	
BU17	
BV17	
BW17	
BY17	
AZ18	
BA18	
BB18	
BC18	
BD18	
BE18	
BF18	
BG18	
BH18	
BI18	
BJ18	
BK18	
BL18	
BM18	
BN18	
BO18	
BP18	
BQ18	
BR18	
BS18	
BT18	
BU18	
BV18	
BW18	
BY18	
AZ19	
BA19	
BB19	
BC19	
BD19	
BE19	
BF19	
BG19	
BH19	
BI19	
BJ19	
BK19	
BL19	
BM19	
BN19	
BO19	
BP19	
BQ19	
BR19	
BS19	
BT19	
BU19	
BV19	
BW19	
BY19	
AZ20	
BA20	
BB20	
BC20	
BD20	
BE20	
BF20	
BG20	
BH20	
BI20	
BJ20	
BK20	
BL20	
BM20	
BN20	
BO20	
BP20	
BQ20	
BR20	
BS20	
BT20	
BU20	
BV20	
BW20	
BY20	
AZ21	
BA21	
BB21	
BC21	
BD21	
BE21	
BF21	
BG21	
BH21	
BI21	
BJ21	
BK21	
BL21	
BM21	
BN21	
BO21	
BP21	
BQ21	
BR21	
BS21	
BT21	
BU21	
BV21	
BW21	
BY21	
AZ22	
BA22	
BB22	
BC22	
BD22	
BE22	
BF22	
BG22	
BH22	
BI22	
BJ22	
BK22	
BL22	
BM22	
BN22	
BO22	
BP22	
BQ22	
BR22	
BS22	
BT22	
BU22	
BV22	
BW22	
BY22	
AZ23	
BA23	
BB23	
BC23	
BD23	
BE23	
BF23	
BG23	
BH23	
BI23	
BJ23	
BK23	
BL23	
BM23	
BN23	
BO23	
BP23	
BQ23	
BR23	
BS23	
BT23	
BU23	
BV23	
BW23	
BY23	
AZ24	
BA24	
BB24	
BC24	
BD24	
BE24	
BF24	
BG24	
BH24	
BI24	
BJ24	
BK24	
BL24	
BM24	
BN24	
BO24	
BP24	
BQ24	
BR24	
BS24	
BT24	
BU24	
BV24	
BW24	
BY24	
AZ25	
BA25	
BB25	
BC25	
BD25	
BE25	
BF25	
BG25	
BH25	
BI25	
BJ25	
BK25	
BL25	
BM25	
BN25	
BO25	
BP25	
BQ25	
BR25	
BS25	
BT25	
BU25	
BV25	
BW25	
BY25	
AZ26	
BA26	
BB26	
BC26	
BD26	
BE26	
BF26	
BG26	
BH26	
BI26	
BJ26	
BK26	
BL26	
BM26	
BN26	
BO26	
BP26	
BQ	

- shows **__Y.EXE** and carved **f000003.txt** (same content). Both reference the dictionary clue and the password derivation.
 - Password message from the bank: **mt_bank_secrecy.htm** contains “*The password for your account is: couch*” in both reports.
 - Encrypted **X.ZIP** containing **SWISS.XLS/TXT/CSV** and the account number **9882111** — both tools locate the ZIP, both note it is password-protected, and both successfully open it with password: “couch”.
 - Email **.msg** conversation between **George** and **Martha** (dates & excerpts) — present in both reports.
 - Deleted **plain-text messages** admitting deposits / describing invoice rerouting – present in both reports.
 - **Differences / additional findings from Autopsy**
 - **Carved/unallocated artifacts:** Autopsy explicitly documents more carved/unallocated entries (**Unalloc_4_17920_1474560**, / **\$CarvedFiles/1/f000003.txt**, etc.) and shows their extracted text. These carved results reinforce the FTK text evidence and supply copies of the same messages found in FTK. This is complementary rather than contradictory.
 - **File naming differences:** FTK shows **!_Y.EXE** while Autopsy shows **__Y.EXE** (and carved copies). This is likely a difference in how each tool extracted or displayed the filename (*special characters / orphaned/orphan file naming and carving differences*). The content and extracted text match across tools, so it's an artifact of extraction rather than conflicting evidence.
 - **NEW EVIDENCE – Martha farewell message (Autopsy-only):** A newly recovered text fragment in Autopsy reads:
 - “*been really nice knowing you. I'll enjoy the money very much. I hope jail agrees with you. No more yours, Martha*”
 - This fragment was not present in the FTK report. It appears to have been recovered from unallocated space (carved/orphan fragment) by Autopsy. The message is highly significant: it provides direct, self-incriminating evidence of Martha's intent to keep funds and her awareness that George would be jailed. This difference illustrates that Autopsy recovered at least one deleted fragment missed by FTK, strengthening the case and providing additional context for motive and consciousness of guilt.
 - **Workflow differences documented in Autopsy:** Autopsy documents the keyword search step (searching “password”), bookmarking and exporting evidence, and creating an Excel case report. FTK report contains screenshots and notes of analysis but Autopsy's log of the keyword search provides stronger traceability for the “how we found the password” step.
4. Look for consistencies and differences – alignment assessment

- The evidence in Autopsy aligns with FTK: the same incriminating messages, the same password (couch), the same encrypted Swiss bank files and account number, and the same email threads and deleted messages. Differences are limited to additional carved fragments (including the new Martha message) and filename/display variations. The new Autopsy-only fragment does not contradict FTK findings; it complements and strengthens them by adding motive and direct admission from Martha.
5. Does Autopsy corroborate FTK conclusions?
 - **Yes.** Autopsy corroborates the major conclusions from the FTK lab:
 - Existence of incriminating deleted communications and images indicating collusion/awareness between George and Martha.
 - Presence of password-protected financial records (**X.ZIP**) which decrypt with couch.
 - Offshore banking activity (Swiss statements referencing account 9882111).
 - Artifacts pointing to deliberate concealment (dictionary clue, physical note references documented in FTK report). Autopsy recovers the same digital hints and carved text, reinforcing the inference of deliberate concealment.
 6. Document new insights found in Autopsy
 - Autopsy recovered additional carved/unallocated artifacts (including the Martha fragment) that contain the same incriminating messages. Examples: carved **f0000003.txt**, **Unalloc_4_17920_1474560**, and other orphan files that include the dictionary password hint and flight rendezvous text. These show the message existed in multiple forms and was partially deleted/fragmented on disk — strengthens chain-of-evidence that the content was present even if the allocated file was removed.

Comparative validation — FTK vs Autopsy

The findings produced by Autopsy (Lab 4) corroborate the results obtained in the earlier FTK analysis (Lab 3). Both tools recovered the same core set of evidence: the encrypted hint messages referencing the Merriam-Webster dictionary, the bank message indicating the password couch, the password-protected X.ZIP archive (containing SWISS.XLS/TXT/CSV and account 9882111), the email thread between George and Martha, and multiple deleted text messages admitting deposits and describing invoice rerouting. Autopsy additionally recovered carved and unallocated fragments that mirror the FTK-recovered content, and documented a keyword search workflow that led to finding the bank/password artifacts. No substantive contradictions were found between the tool outputs; minor filename/display differences are attributable to extraction/filing differences between tools.