

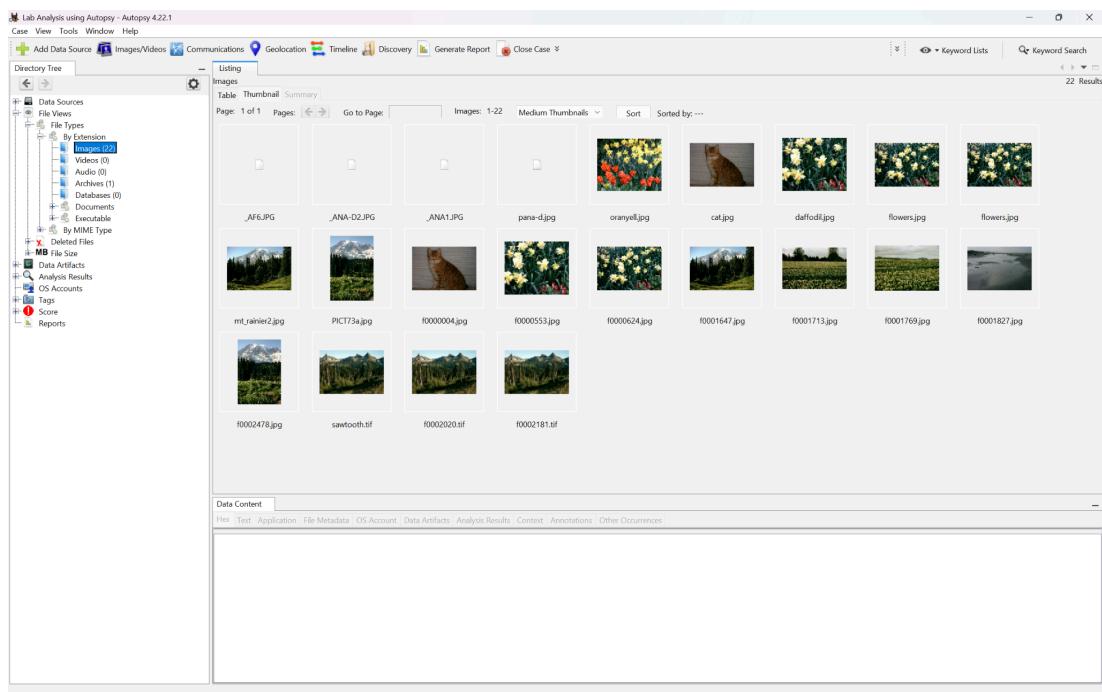
# Computer & Network Forensics

## Week 6 (Lab4)

### 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?

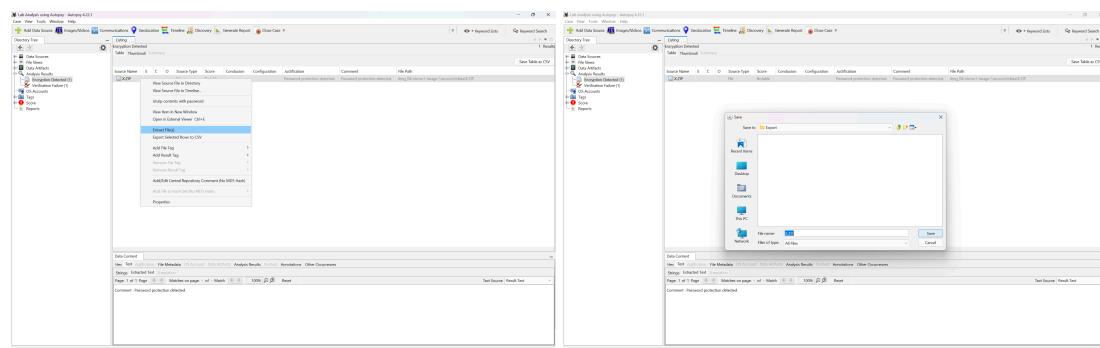
→ **Secret message:**

*"George*

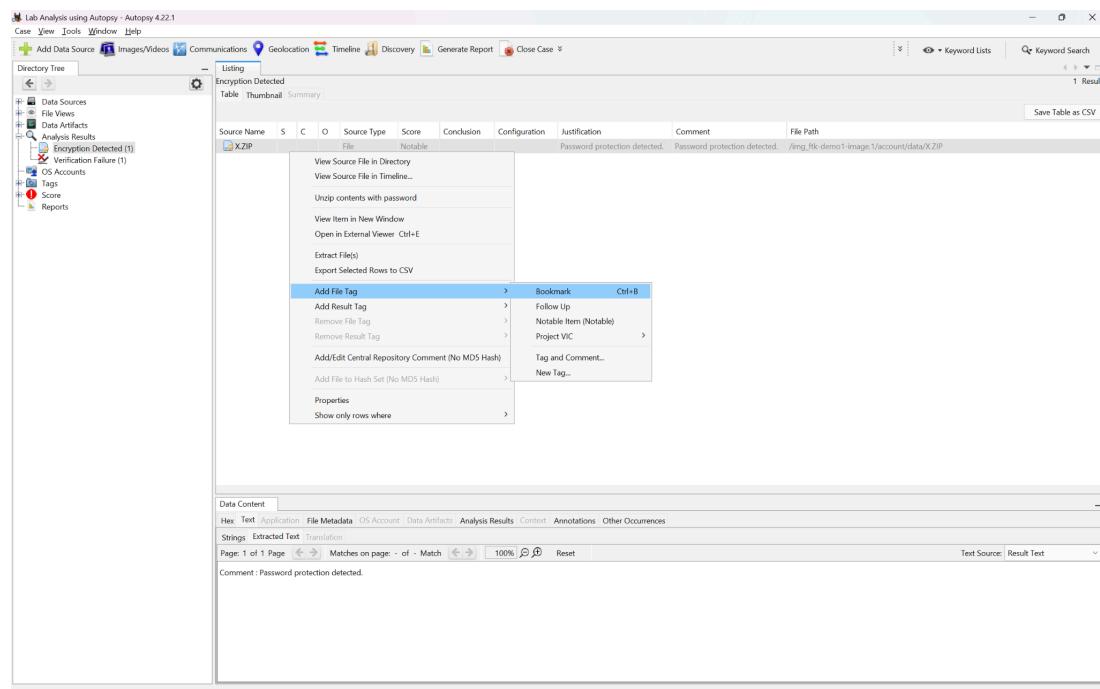
*Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?  
Martha"*

(More info included in the report)

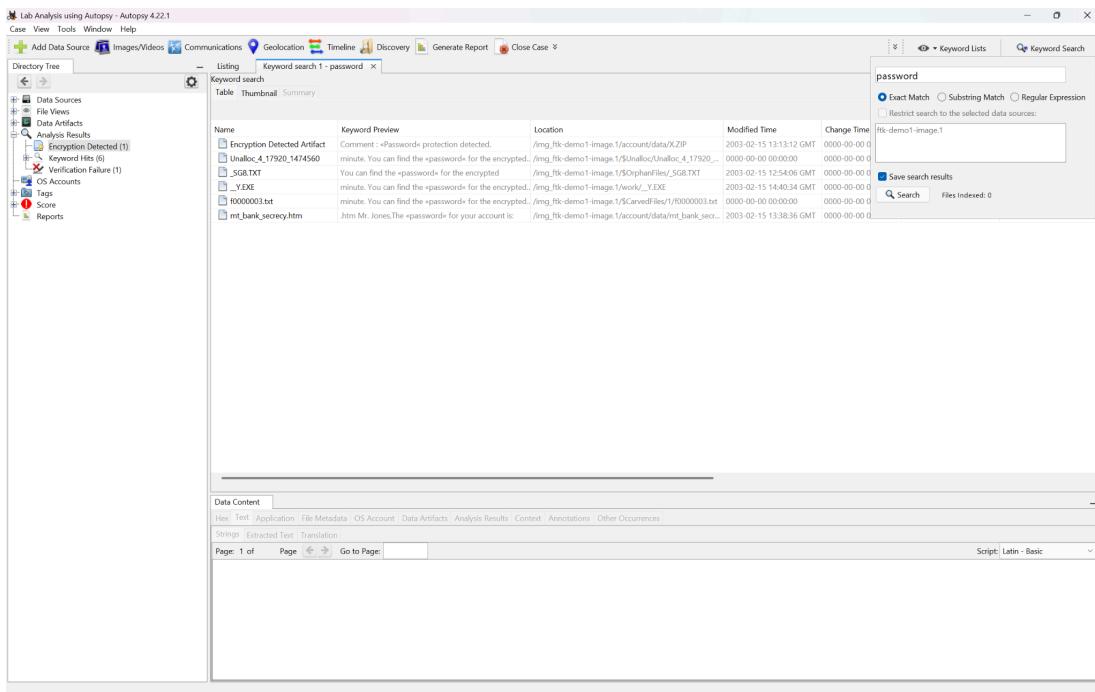
### 3. What happens when I try to unzip the encrypted folder? Screen shot and detail the steps I took.



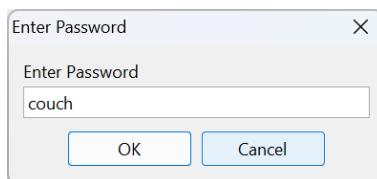
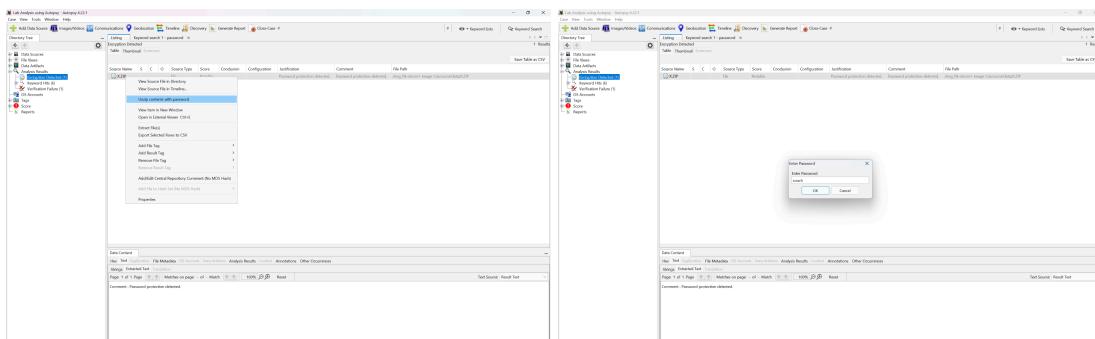
→ Export File



→ Add Bookmark File Tag



→ Keyword Search (“password”)



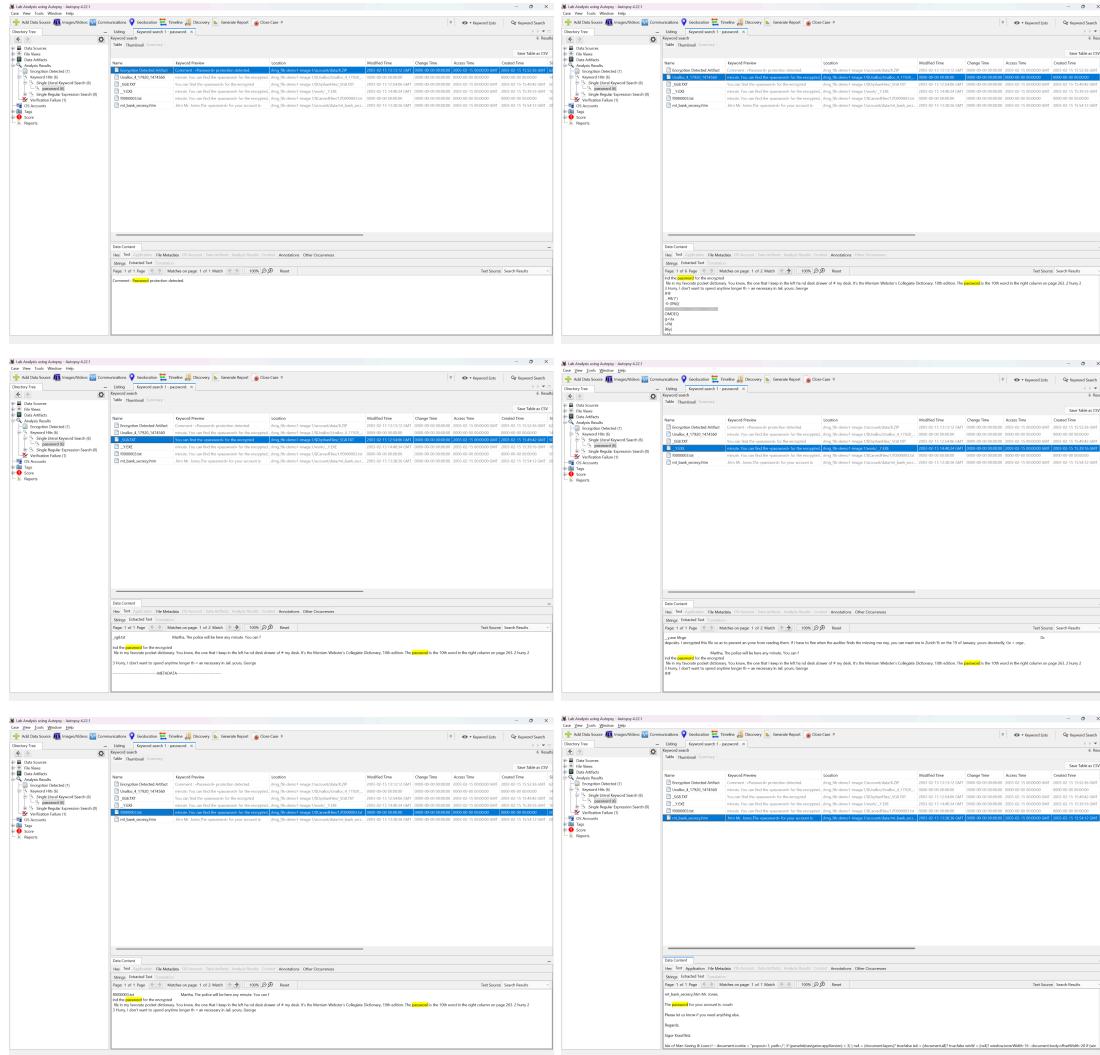
→ Unzip X.ZIP with password (“couch”)

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

(More info included in the report)

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

→ 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 4.22.1 interface with a search result for 'text/plain' files. The results table has the following columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table contains 14 rows, with the last row being 'SWISS.TXT'. The 'Known' column for the .txt files is 'unknown', while for the .gif file it is 'Allocated'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
x msg7.txt				2003-02-15 12:45:44 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:49:35 GMT	662	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/personal/Messages/msg7.txt
x msg5.txt				2003-02-15 12:44:16 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:48:33 GMT	316	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/personal/Messages/msg5.txt
x msg4.txt				2003-02-15 12:43:30 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:47:10 GMT	453	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/work/msg4.txt
x AILS.GIF				2003-02-15 14:35:04 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:43:42 GMT	487	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/SorphanFiles/_EST/AILS.GIF
✓ 10000001.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	662	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10000001.txt
✓ 10000003.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	506	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10000003.txt
✓ 1000052.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	119	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/1000052.txt
✓ 10001407.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	102	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10001407.txt
✓ 10002180.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	512	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10002180.txt
✓ 10002722.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	633	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10002722.txt
✓ 10002728.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	366	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10002728.txt
✓ 10002737.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	316	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10002737.txt
✓ 10002738.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	179	Unallocated	Unallocated	unknown	/img_ft-demo1-image.1/CarvedFiles/10002738.txt
SWISS.TXT	1			2003-02-15 10:47:06 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2429	Allocated	Allocated	unknown	/img_ft-demo1-image.1/account/data/X.ZIP/SWISS...

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

The screenshot shows the Autopsy 4.22.1 interface with a search result for 'text/csv' files. The results table has the following columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and MD5 Hash. The table contains 1 row, with the file 'SWISS.CSV'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash
SWISS.CSV	1			2003-02-15 10:46:40 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2429	Allocated	Allocated	unknown	/img_ft-demo1-image.1/account/data/X.ZIP/SWISS... 27b8b95c40

→ 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	x			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.htm
mt_bank_secrecy.htm	o	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_bank_secrecy.htm
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/f0001705_mt_bank.html

→ 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	Created Time	Size	Flags(D)	Flags(M)	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-021...
g-021218.msg	2			2003-02-15 11:51:30 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:57:13 GMT	256	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/personal/Messages/g-0212...
g-021229.msg	2			2003-02-15 11:58:42 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-0212...
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-021...

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

**Left Window (Raw Text):**

```

-----Original Message-----
From: Jones, George [mailto:george@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
dc_creator: James
dc_subject: REA plan
dc_title: REA plan
resourceName: REA plan.eml

```

→ /img\_ftk-demo1-image.1/personal/Messages/m-021230.msg

The screenshot shows two FTK Editor windows side-by-side. Both windows have the title bar `/img_ftk-demo1-image.1/personal/Messages/g-021218.msg - Editor`. The left window displays the message body:

```

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

-----METADATA-----
Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: george@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

```

The right window also displays the message body and has a larger METADATA section:

```

Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: george@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 FTK Editor windows side-by-side. Both windows have the title bar `/img_ftk-demo1-image.1/personal/Messages/g-021229.msg - Editor`. The left window displays the message body:

```

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:george@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 vaction next Spring. I'll tell you about it later.
George

```

The right window also displays the message body and has a larger METADATA section:

```

Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: george@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 FTK Editor windows side-by-side. Both windows have the title bar `/img_ftk-demo1-image.1/personal/Messages/m-021220.msg - Editor`. The left window displays the message body:

```

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

```

The right window also displays the message body and has a larger METADATA section:

```

Content-Type: message/rfc822
Message-From: Jones
Message-To: James
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: REA plan
dcTitle: REA plan
resourceName: REA 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 left screenshot displays a Microsoft Excel spreadsheet titled "Autopsy Report - Lab Analysis using Autopsy". It contains a single sheet named "Summary" with data in columns A through Z. The first few rows show headers like "Case Number", "File Name", and "Description". The right screenshot shows another Microsoft Excel spreadsheet titled "Autopsy Report - Lab Analysis using Autopsy". It contains a single sheet named "Log" with data in columns A through Z. This sheet includes columns for "Case Number", "File Name", "Comment", "Last Modified Time", "Changed Time", "Accessed Time", and "Creation Time". Both spreadsheets have standard Excel toolbars and menus at the top.

→ Generated Autopsy Excel Report

8. Confirm and validate the findings from FTK in last week's lab using Autopsy.

#### Quick summary

Autopsy confirms and validates the FTK findings. Both tools recovered the same core evidence (the !\_Y.EXE/\_Y.EXE hint, the \_AF6.JPG image, the **deleted text messages**, the **email .msg files**, the mt\_bank\_secrecy.htm message, and the password-protected X.ZIP containing the **SWISS files**). Autopsy additionally shows carved/unallocated artifacts and documents the keyword-search workflow (e.g., files containing the word “password”), providing extra carved fragments that reinforce the FTK findings.

#### Step-by-step confirmation & validation

1. Ensure access to FTK findings/evidence
  - FTK Lab report (Lab 3) enumerates recovered items and analysis (encrypted message !\_Y.EXE, **deleted .txt messages**, mt\_bank\_secrecy.htm, X.ZIP → **SWISS.\***, and **email messages**). Evidence list and findings are in the FTK report.
2. In Autopsy, review current lab findings
  - The Autopsy report (Lab 4) lists the same evidence items and documents the investigation steps in Autopsy: image file paths, keyword search for “password,” detection of X.ZIP password protection, unzipping with password couch, and exported/bookmarked files. Autopsy also lists additional carved/unallocated files (e.g., **Unalloc\_4\_17920\_1474560**, **f0000003.txt**, \_SG8.TXT, \_Y.EXE) recovered by carving and shows the same **.msg email files** and \_AF6.JPG.
3. Compare evidence / findings (Autopsy vs FTK)
  - **Same / corroborated evidence**
    - Encrypted hint message pointing to Merriam-Webster dictionary and password clue. FTK shows !\_Y.EXE and deleted **msg7.txt**; Autopsy shows \_Y.EXE and carved **f0000003.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/f0000003.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.