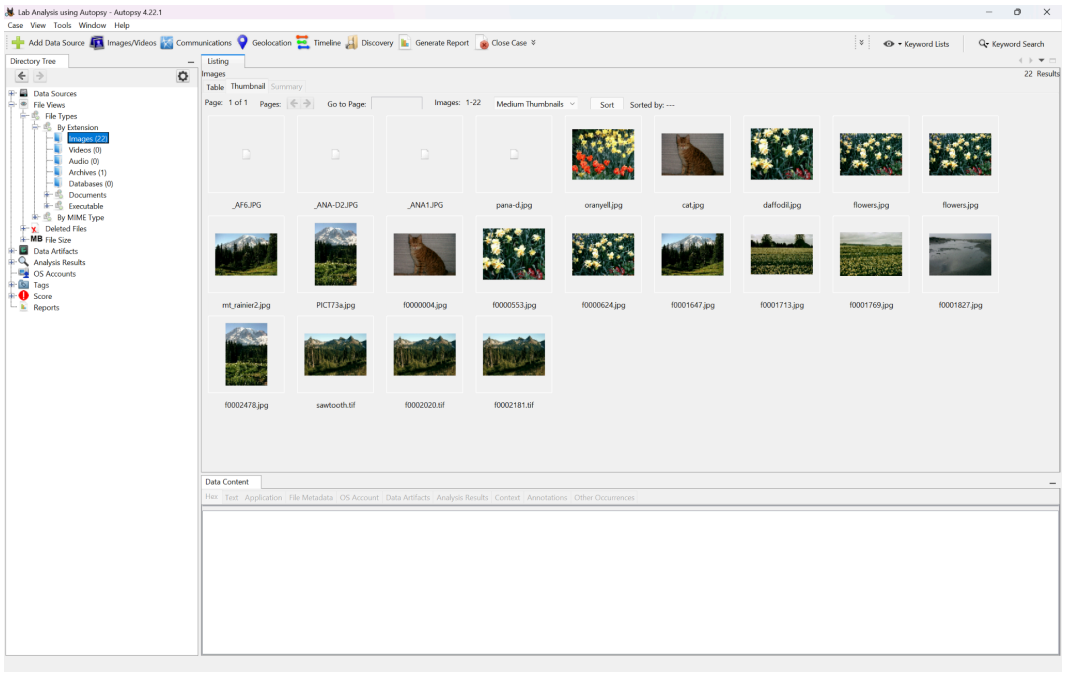
Computer & Network Forensics

Lab 4

Forensics Analysis using Autopsy

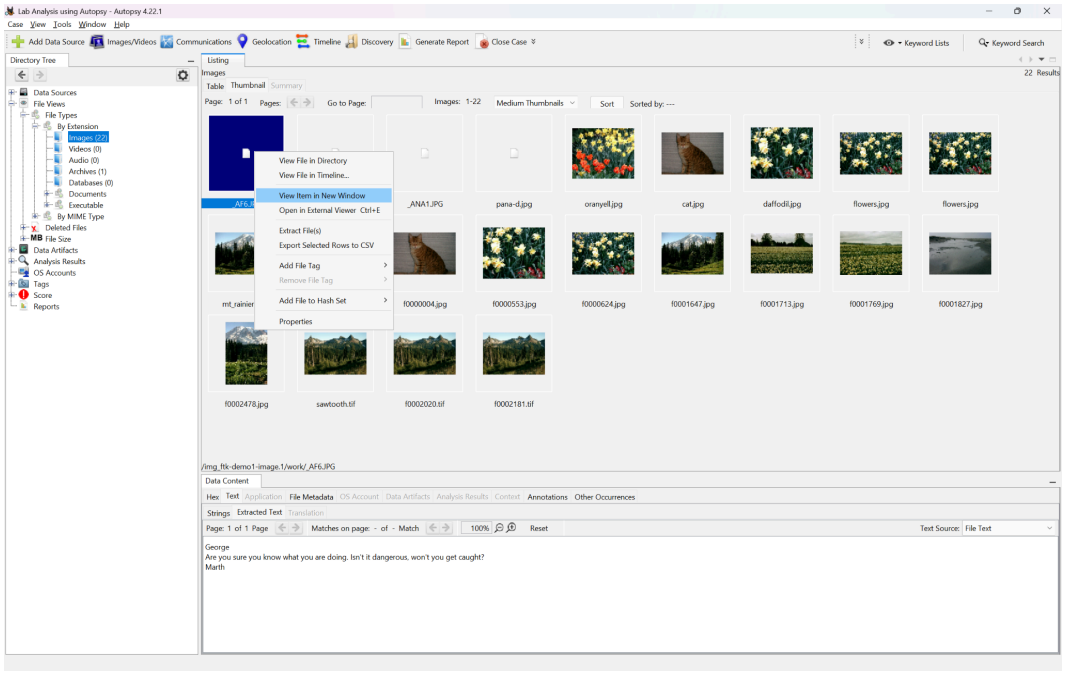
Questions

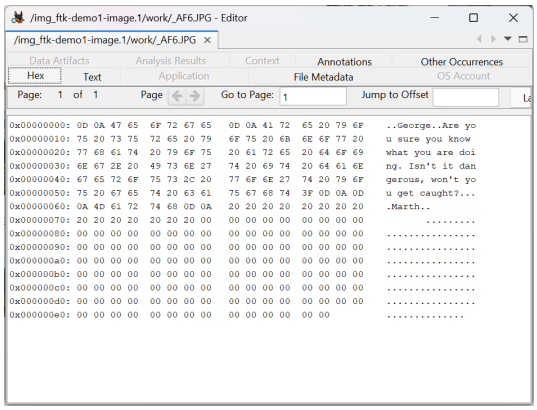
1. How many images are viewable in thumbnail mode?

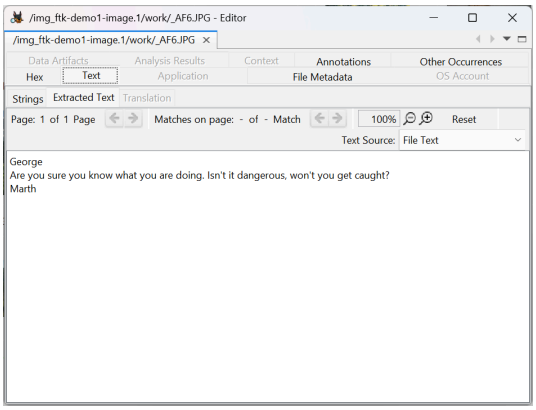


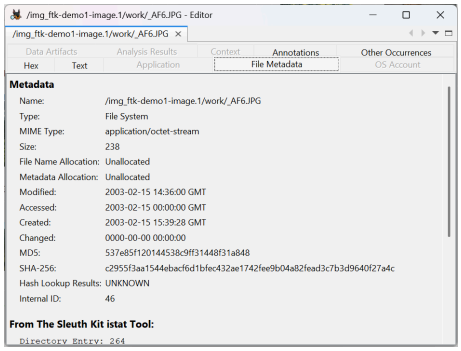
→ 18 viewable images, and 4 not (total 22)

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







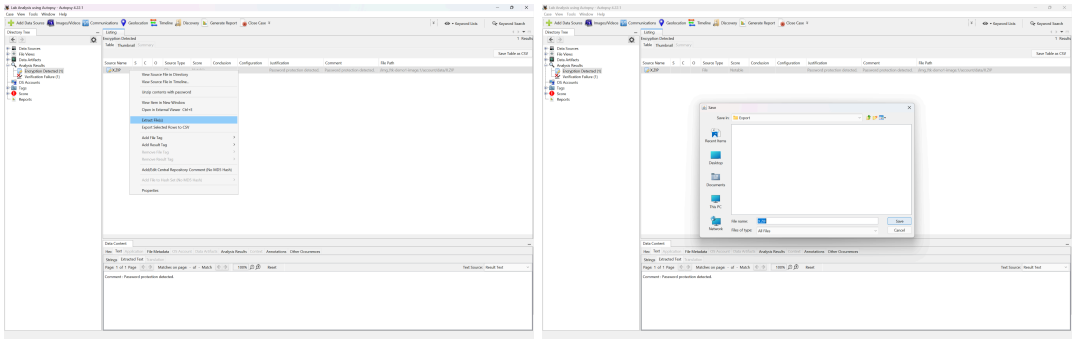


→ **Secret message:**

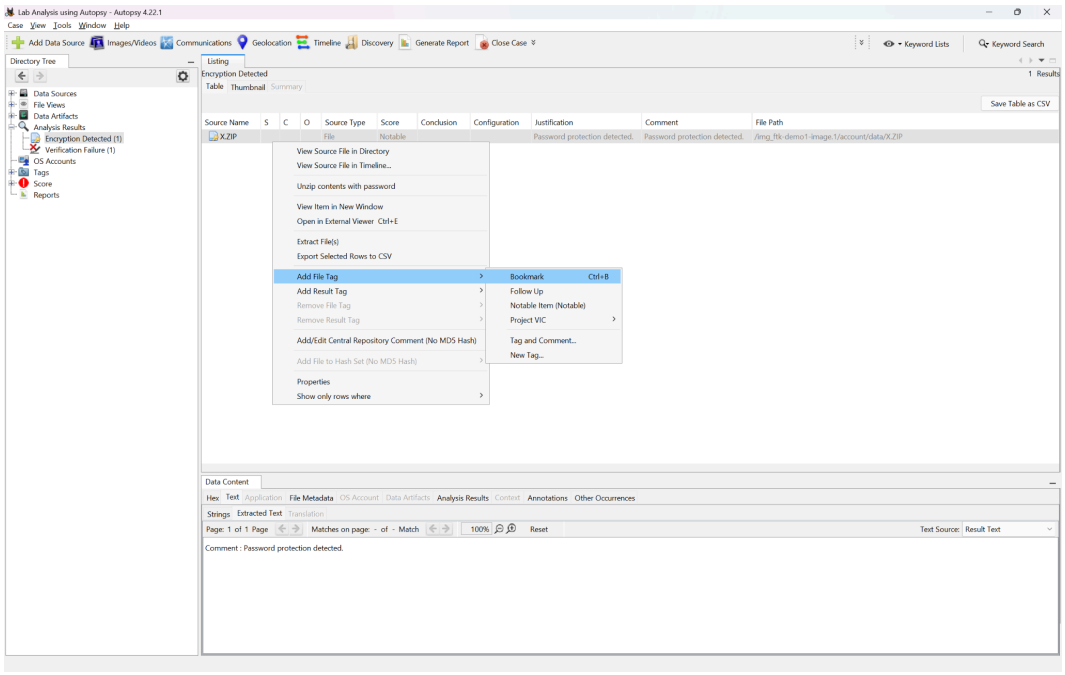
“George
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?
Marth”

(More info included in the report)

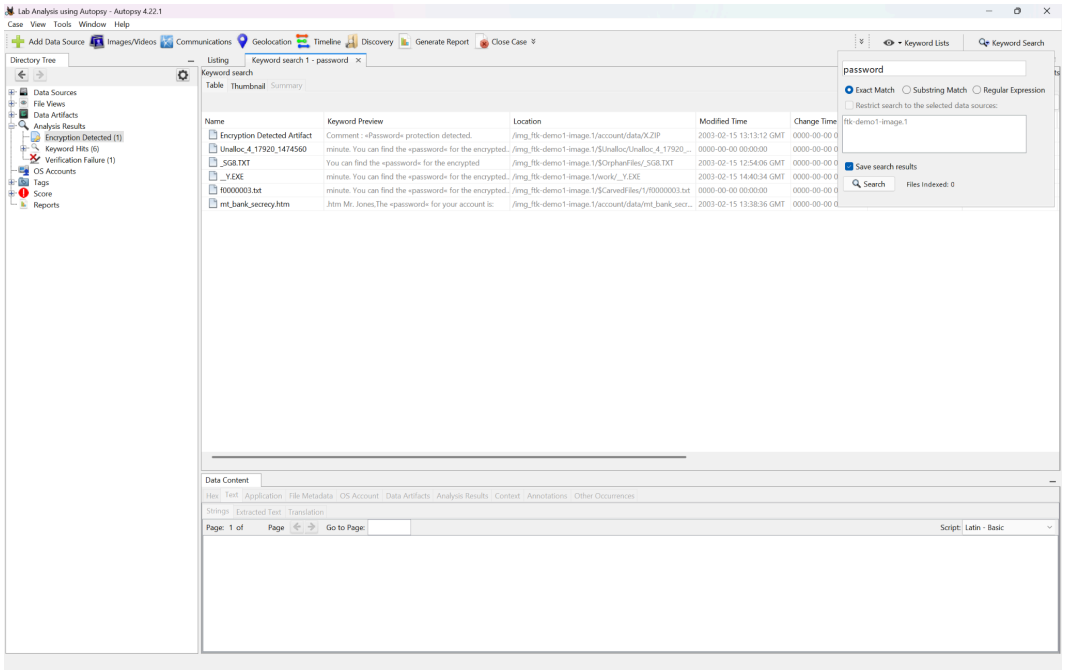
3. What happens when I try to unzip the encrypted folder? Screen shot and detail the steps I took.



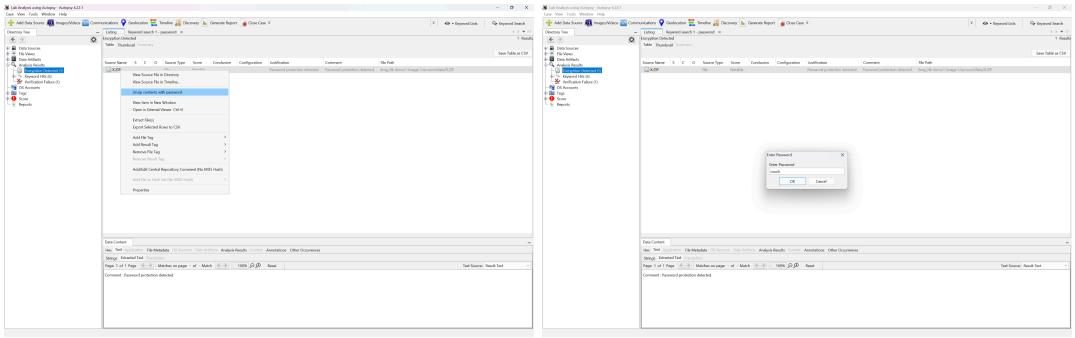
→ **Export File**

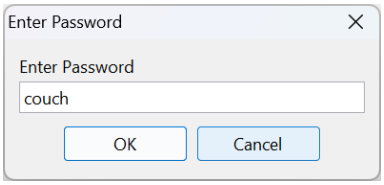


→ **Add Bookmark File Tag**

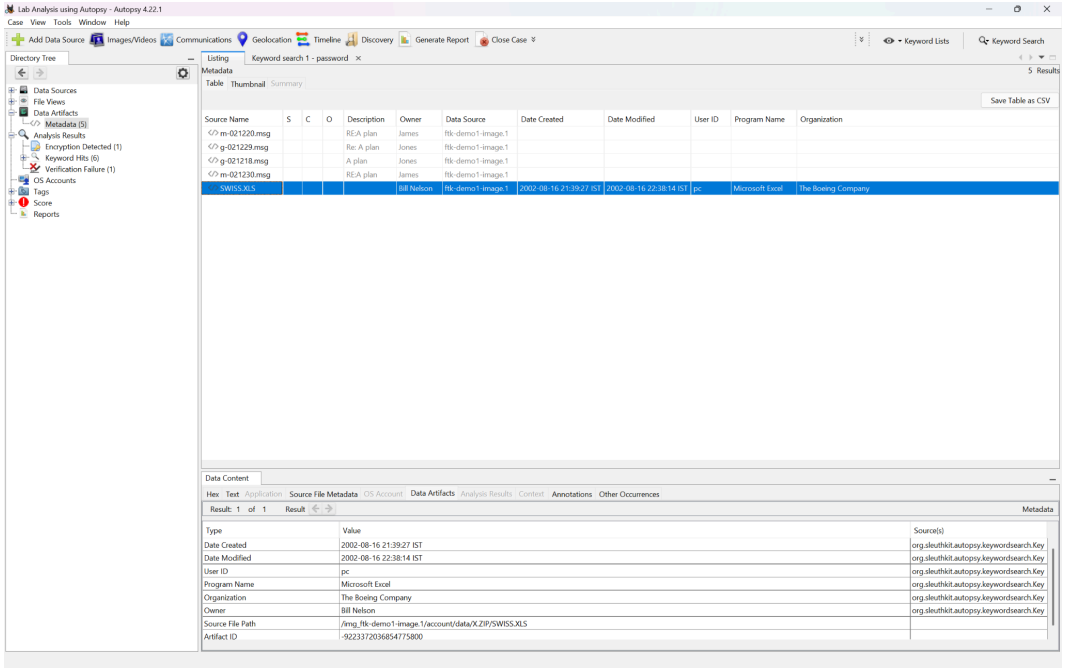


→ **Keyword Search (“password”)**





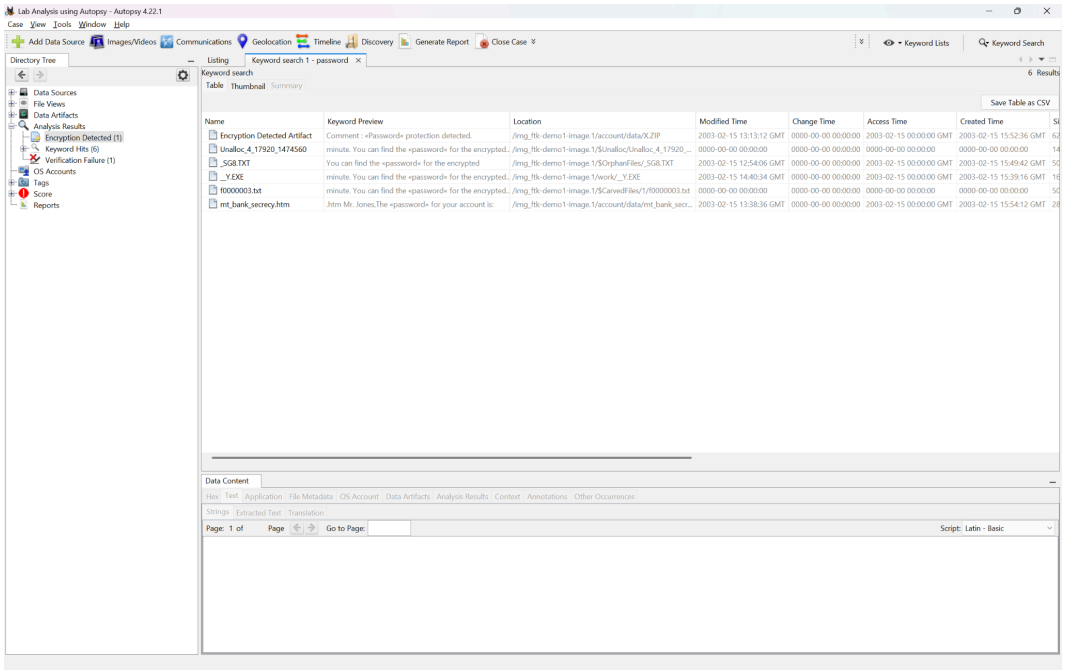
→ **Unzip X.ZIP with password (“couch”)**



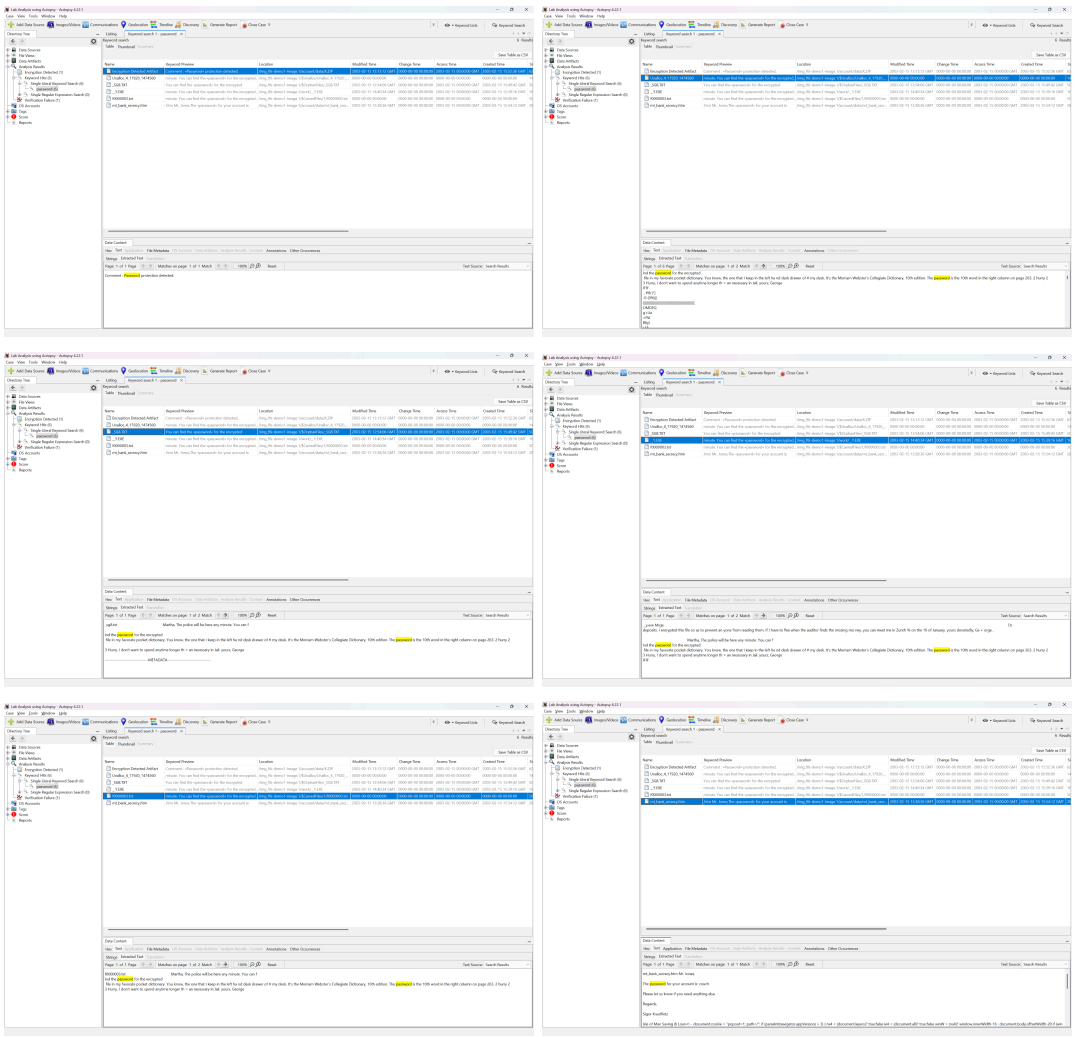
→ **The unzipped file (SWIZZ.XLS) is showing in *“Data Artifacts/Metadata”***
We can view the content of the unzipped, decrypted files.

(More info included in the report)

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



→ **6 files contain the word “password”**



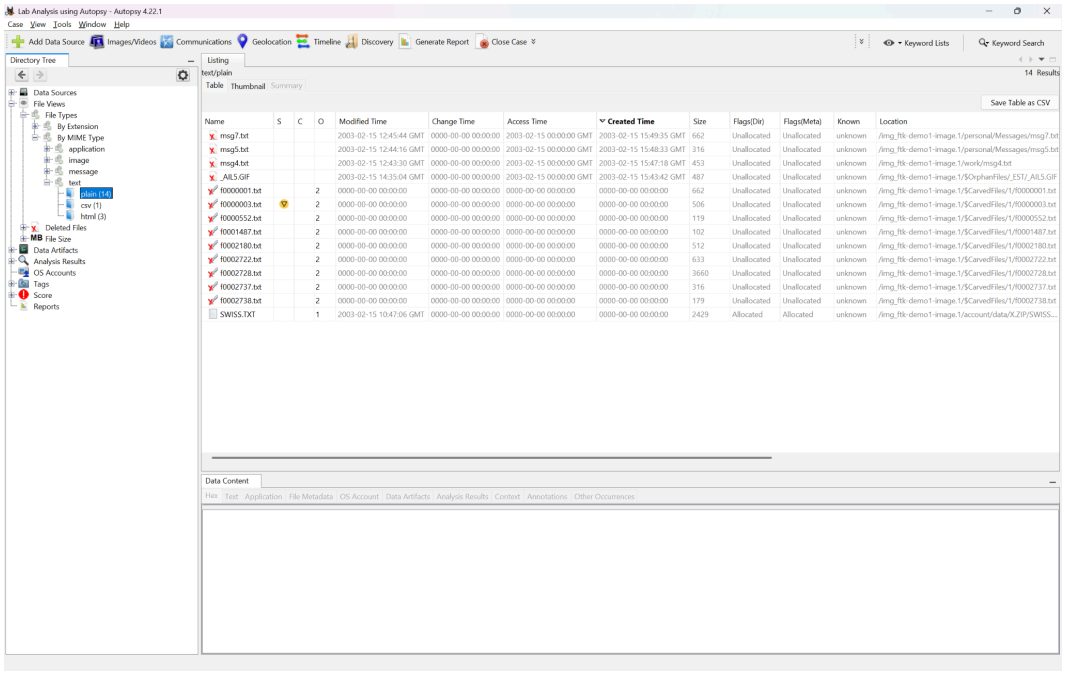
→ The first one is the Encryption Detected Artifact (X.ZIP – /img_ftk-demo1-image.1/account/data/X.ZIP), that contains: *"Comment : Password protection detected."*

→ 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."*

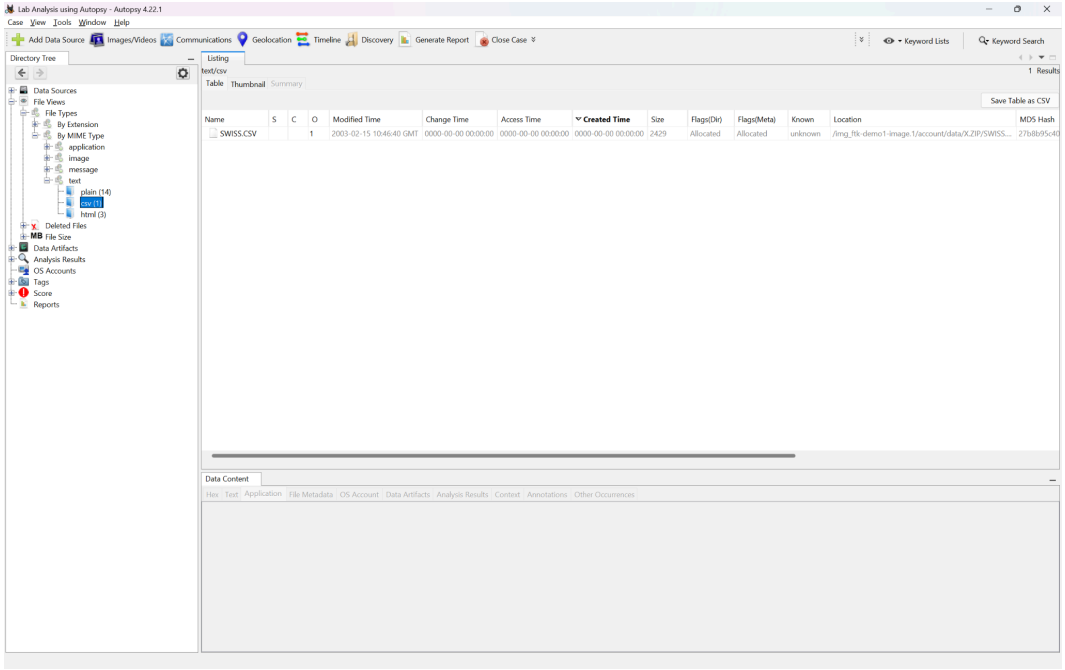
→ The last file (mt_bank_secrecy.htm – /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm), that contains the message form the bank: *"... The password for your account is: couch …"*

(More info included in the report)

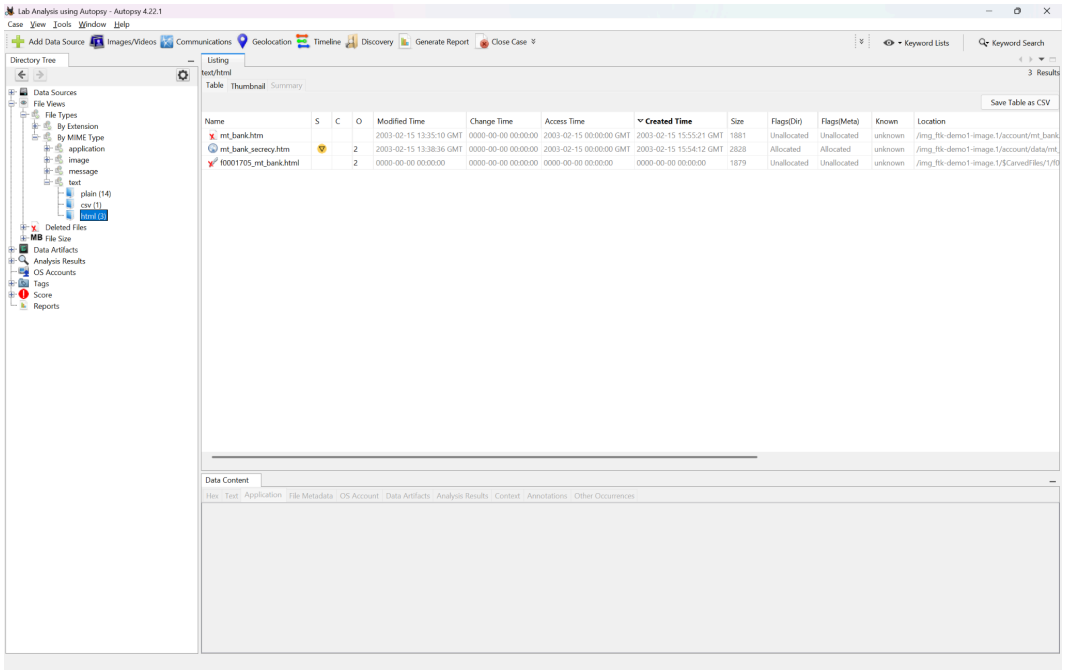
5. Determine how many text files (.txt) can be found throughout the image.



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



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



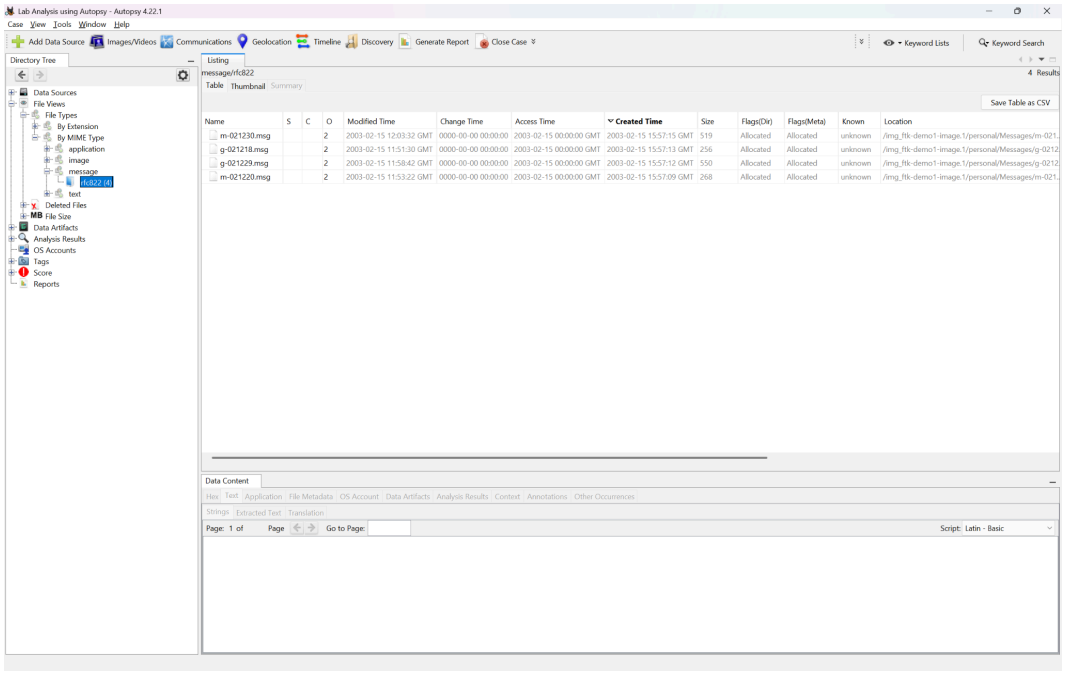
→ **There is 3 htm/html files**

Bank web files:

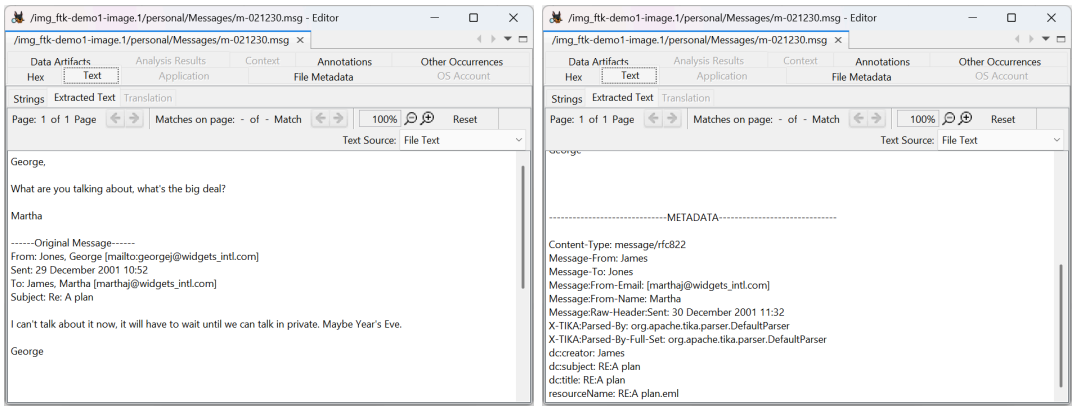
- /img_ftk-demo1-image.1/account/mt_bank.htm
- /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm
- /img_ftk-demo1-image.1/$CarvedFiles/1/f0001705_mt_bank.html

(More info included in the report)

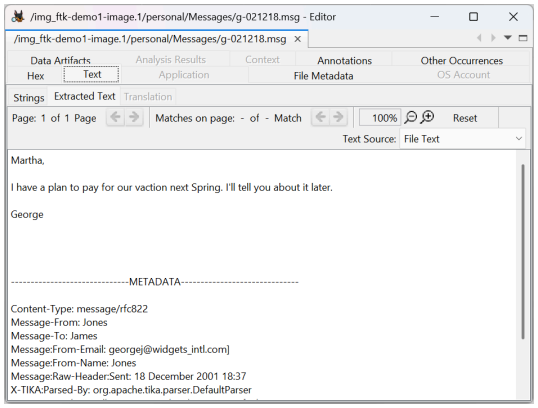
6. Determine how we know that George has been using Outlook Express to send messages, we can rely on file extensions, which provide important clues about the software used.



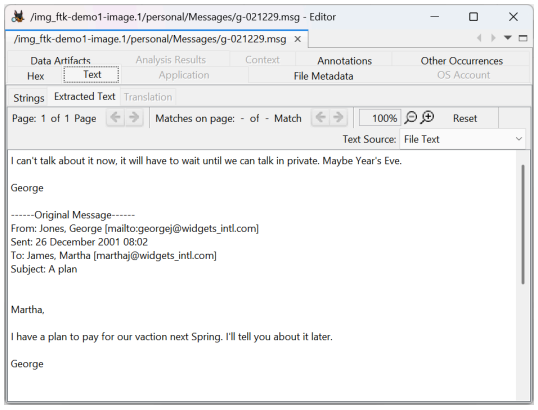
→ George used Outlook to communicate with Martha, as evidenced by .msg files



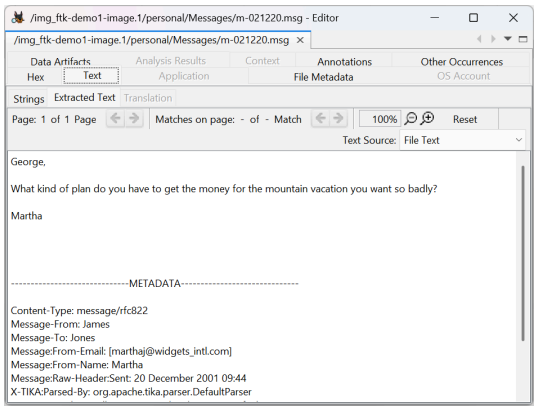
→ /img_ftk-demo1-image.1/personal/Messages/m-021230.msg



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



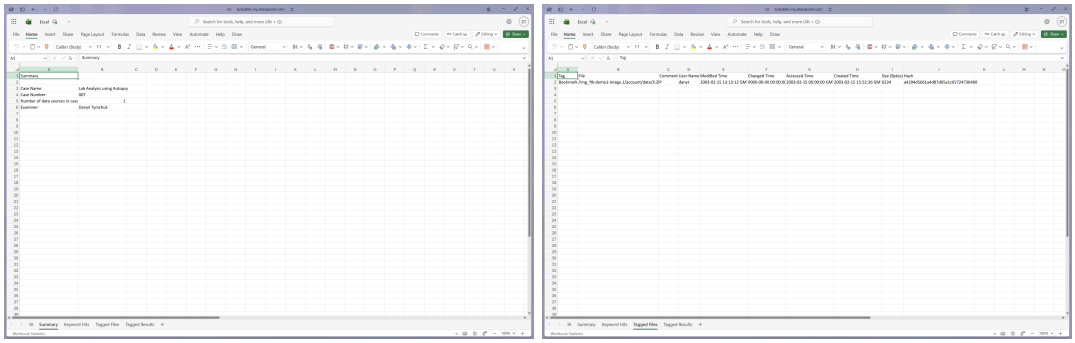
→ **/img_ftk-demo1-image.1/personal/Messages/g-021229.msg**



→ **/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.



→ **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.