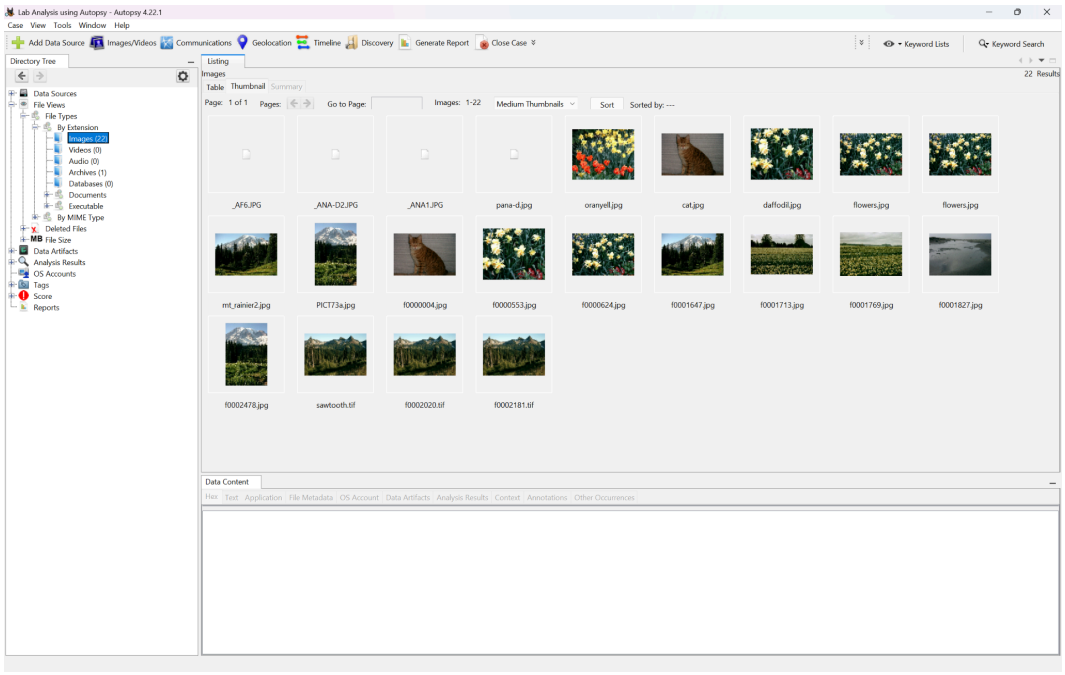
Computer & Network Forensics

Lab 4

Forensics Analysis using Autopsy

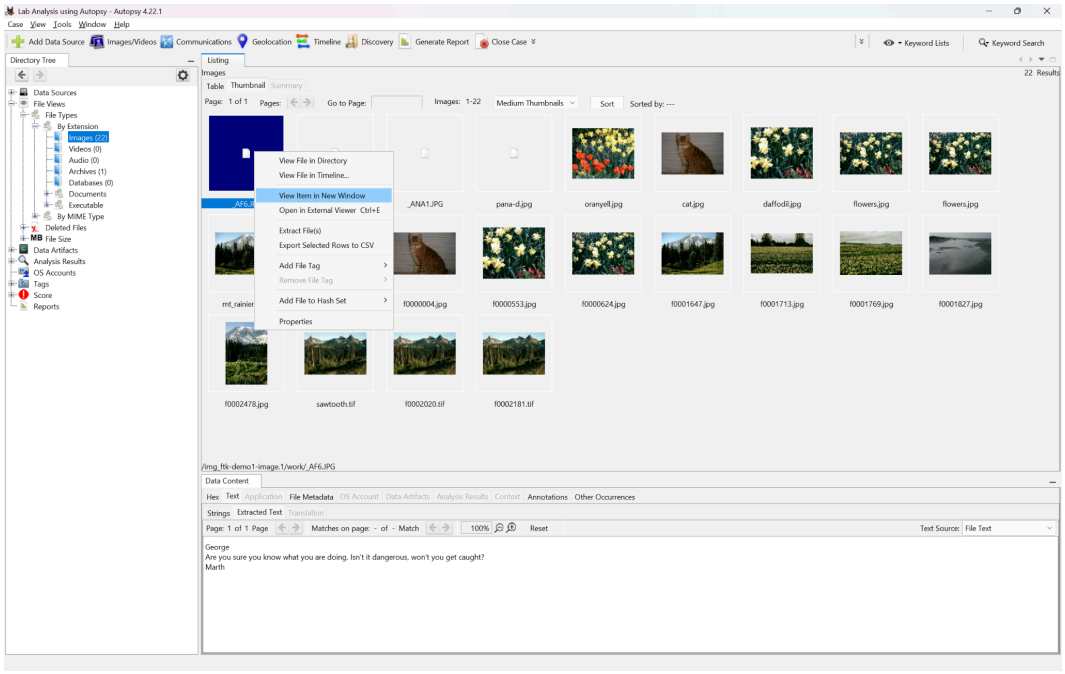
Questions

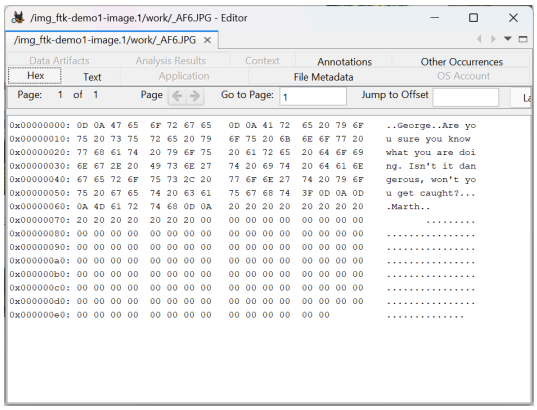
1. How many images are viewable in thumbnail mode?

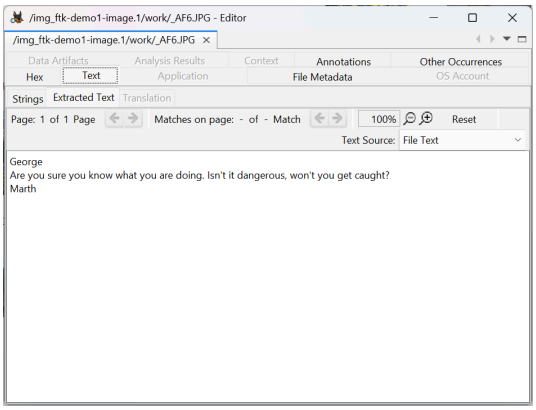


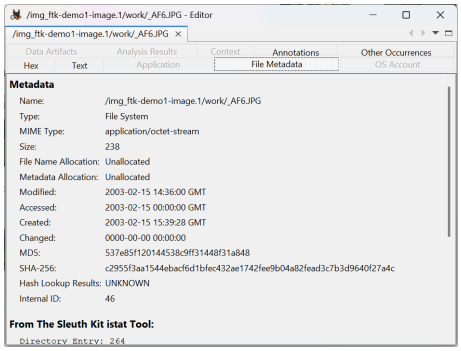
→ 18 viewable images, and 4 not (total 22)

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







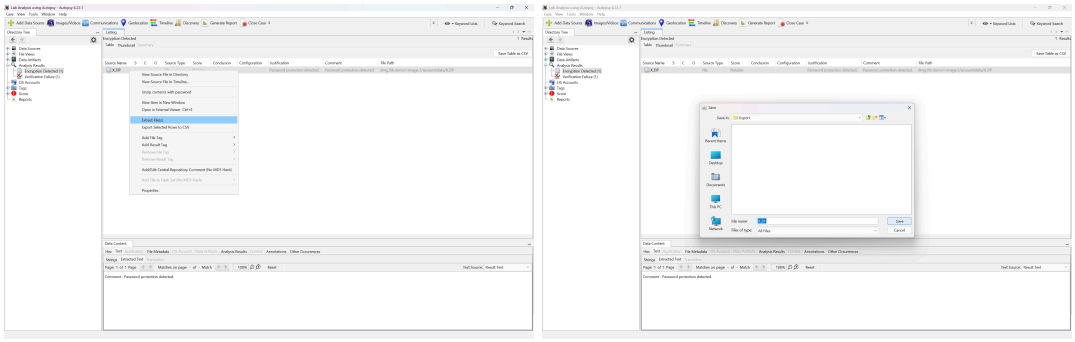


→ **Secret message:**

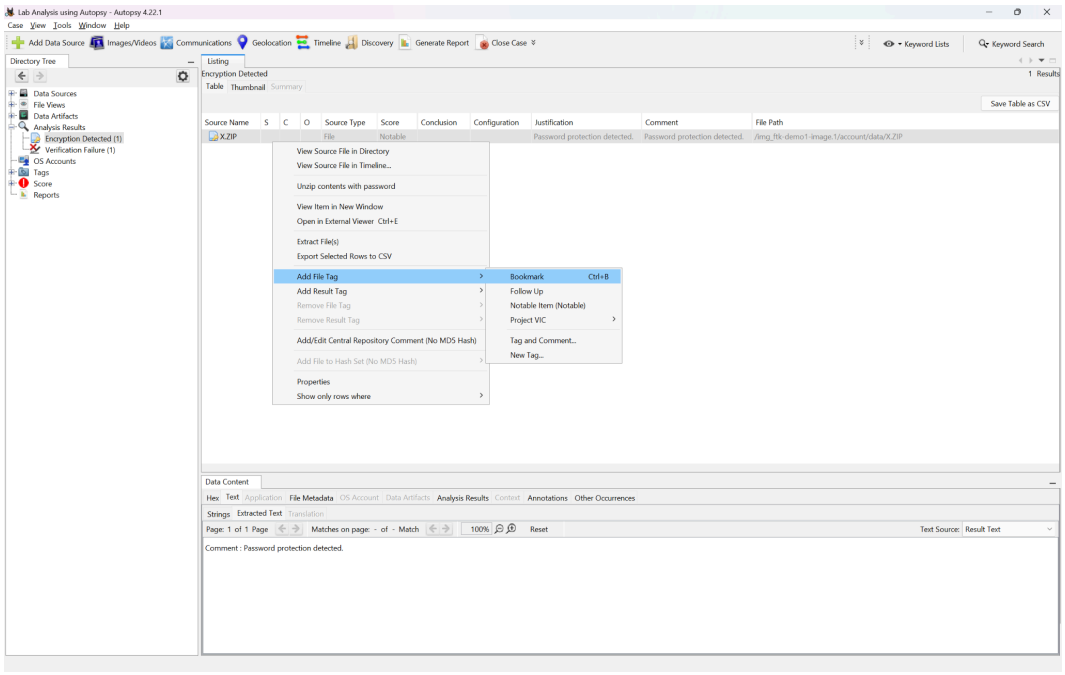
“George
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?
Marth”

(More info included in the report)

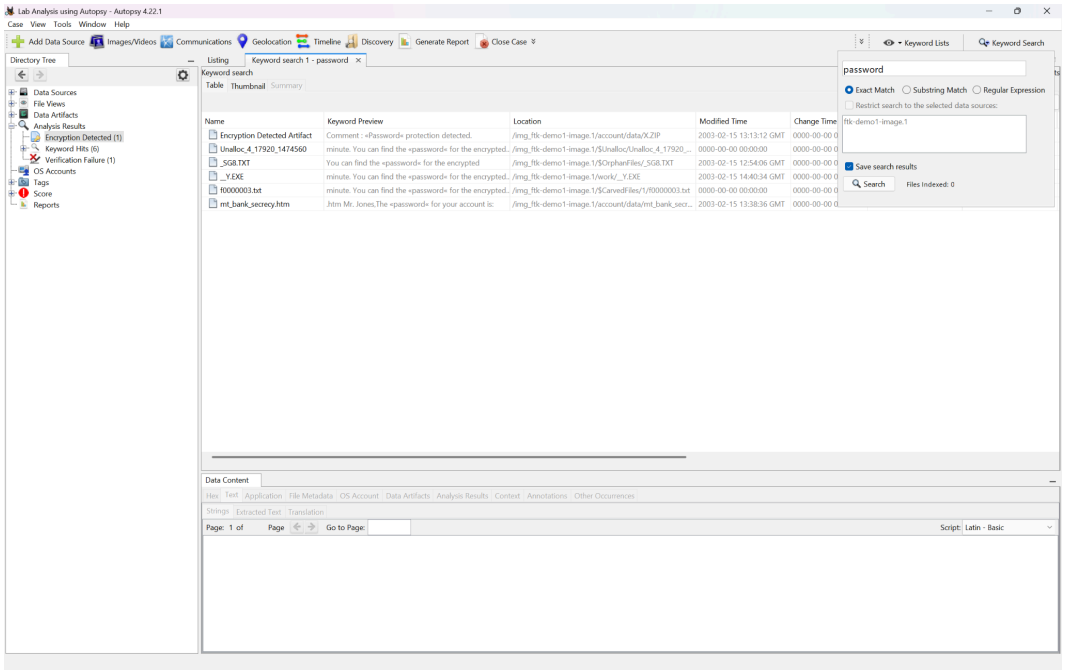
3. What happens when I try to unzip the encrypted folder? Screen shot and detail the steps I took.



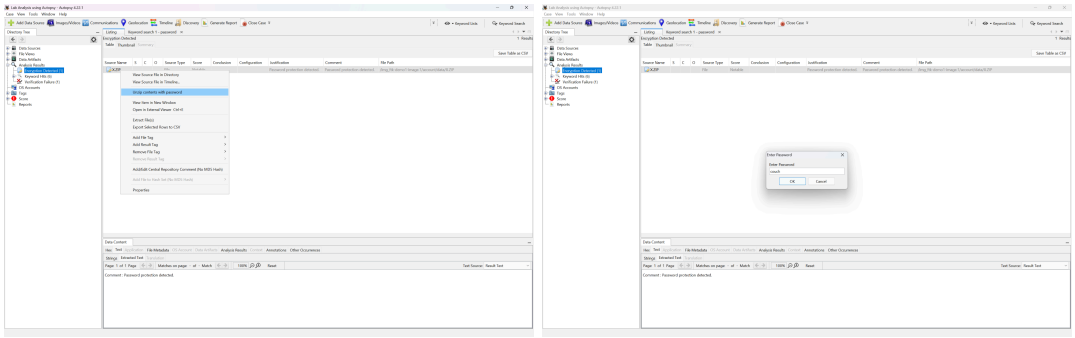
→ **Export File**

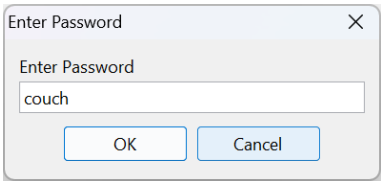


→ **Add Bookmark File Tag**

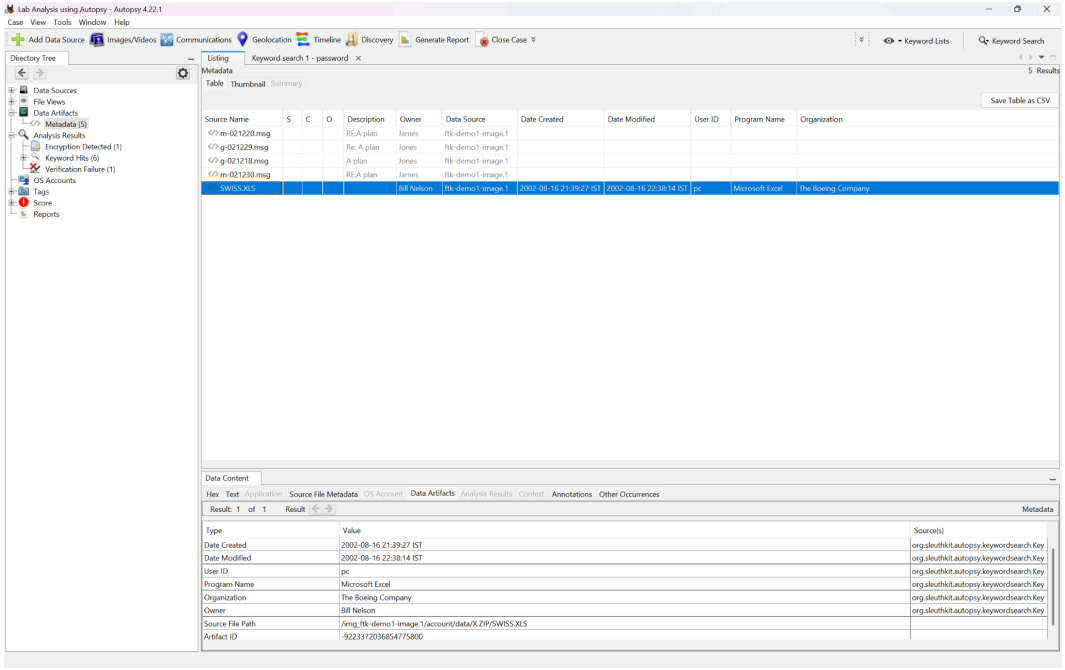


→ **Keyword Search (“password”)**





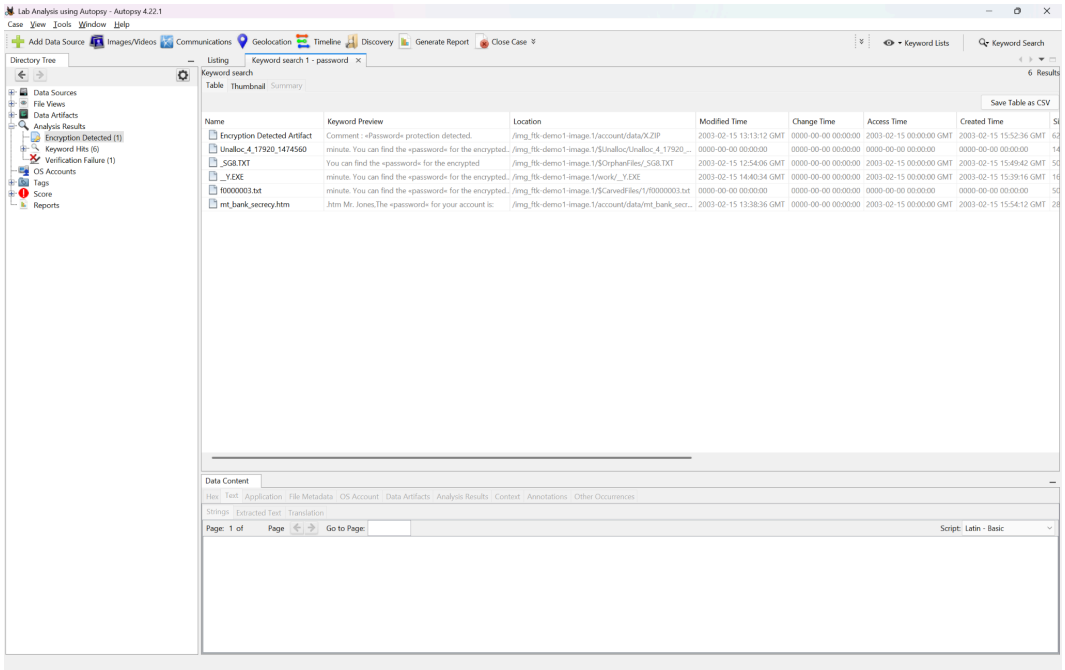
→ **Unzip X.ZIP with password (“couch”)**



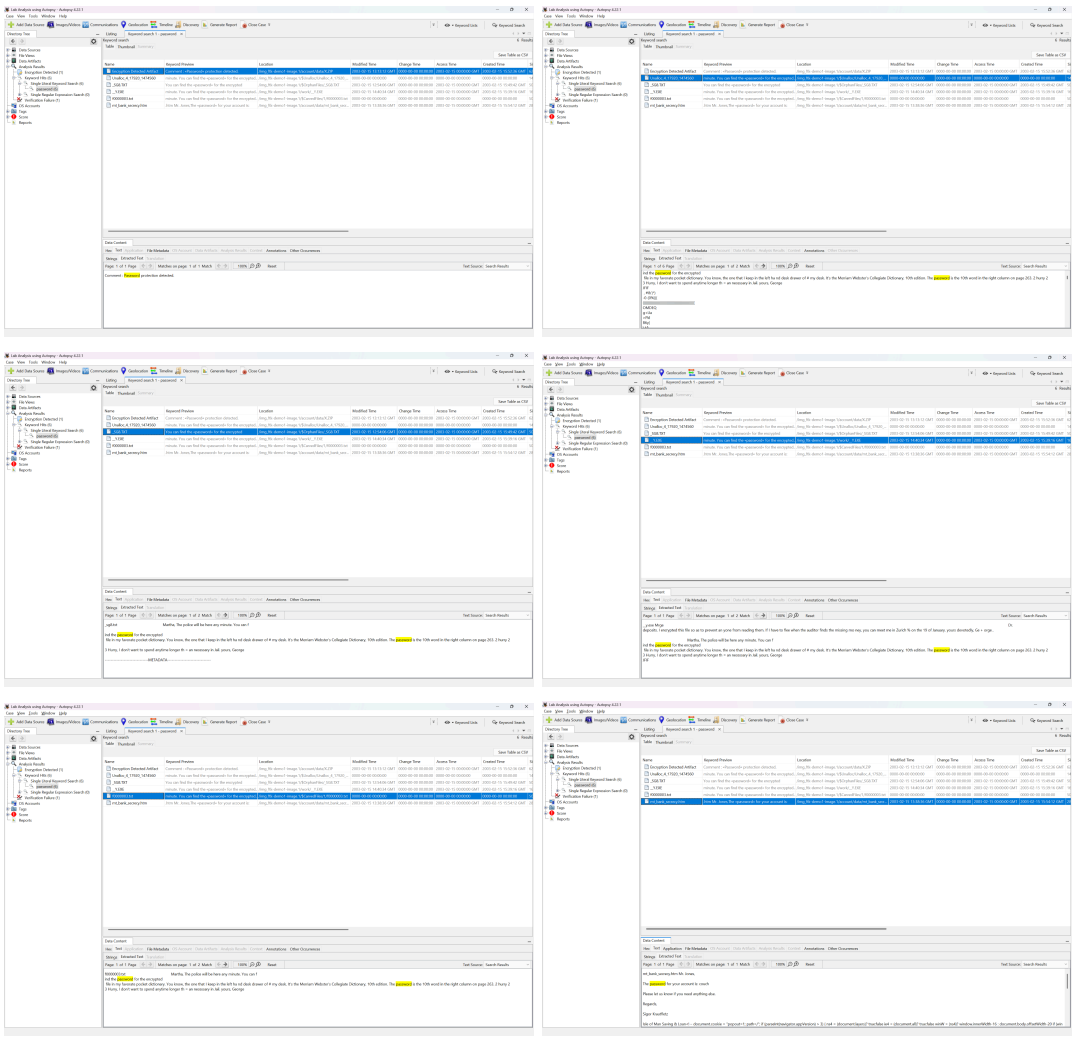
→ **The unzipped file (SWIZZ.XLS) is showing in *“Data Artifacts/Metadata”***
We can view the content of the unzipped, decrypted files.

(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”**



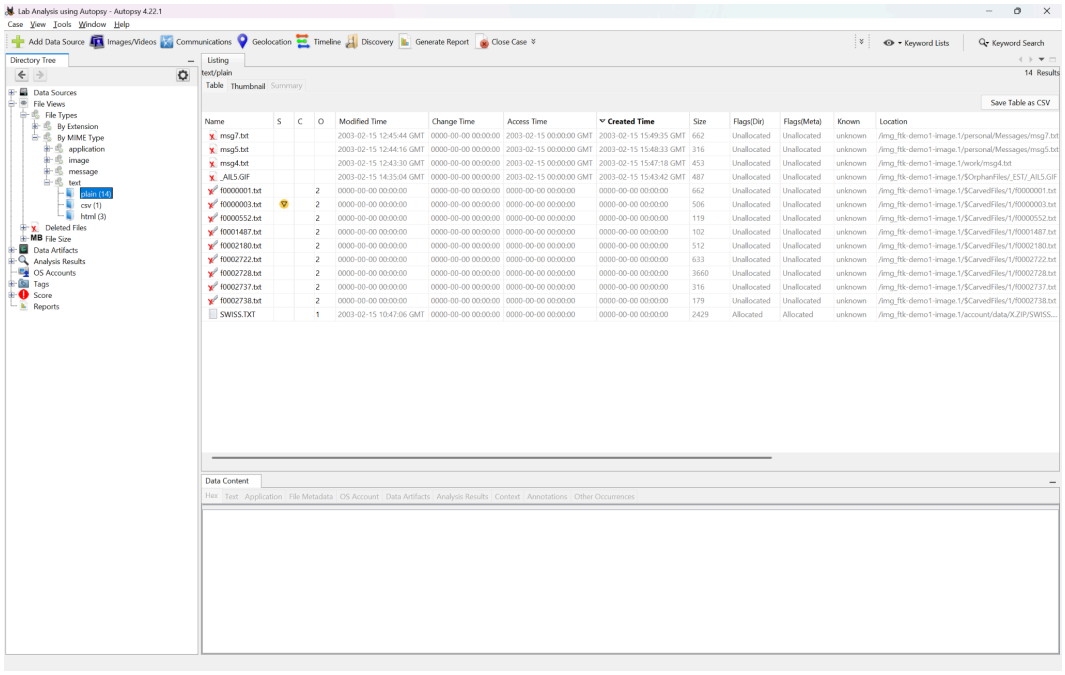
→ The first one is the Encryption Detected Artifact (X.ZIP – /img_ftk-demo1-image.1/account/data/X.ZIP), that contains: *"Comment : Password protection detected."*

→ 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."*

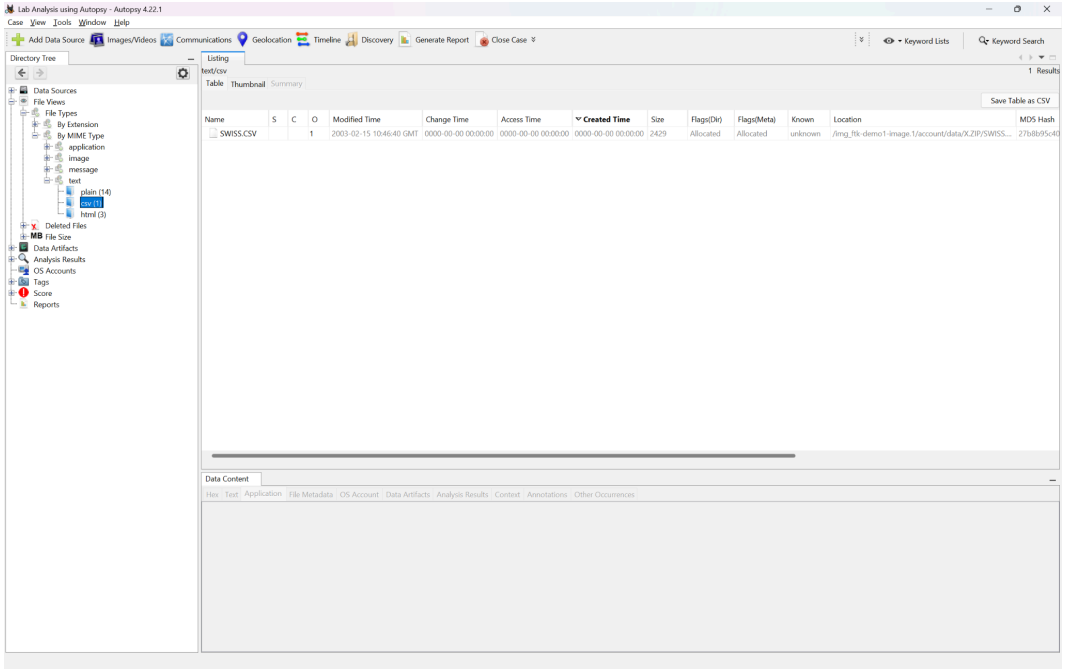
→ The last file (mt_bank_secrecy.htm – /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm), that contains the message form the bank: *"... The password for your account is: couch …"*

(More info included in the report)

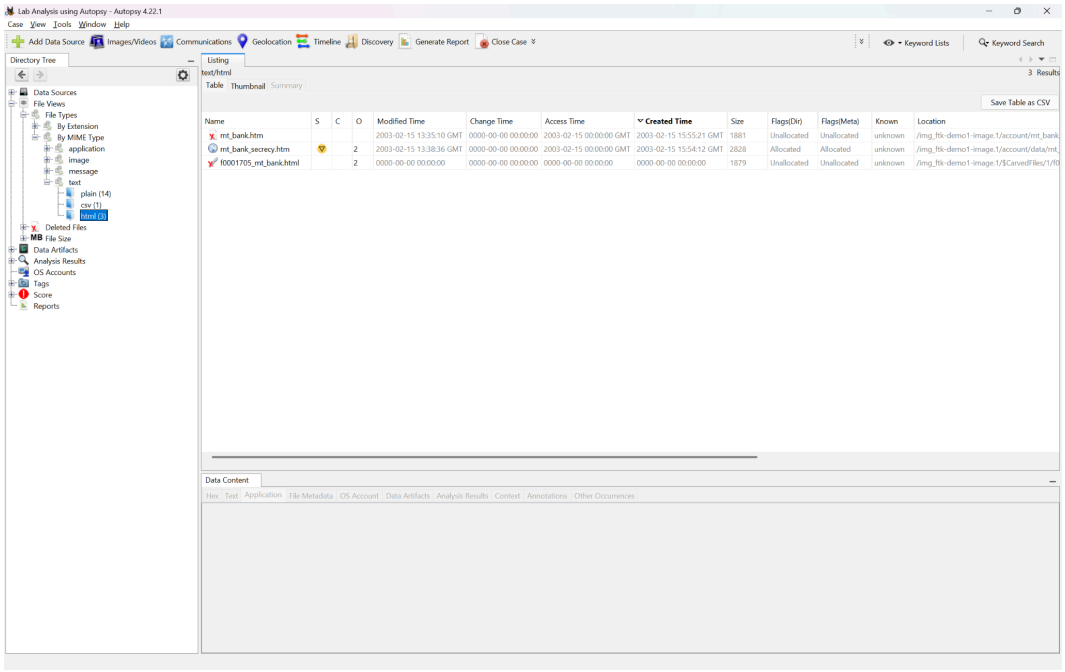
5. Determine how many text files (.txt) can be found throughout the image.



→ 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)



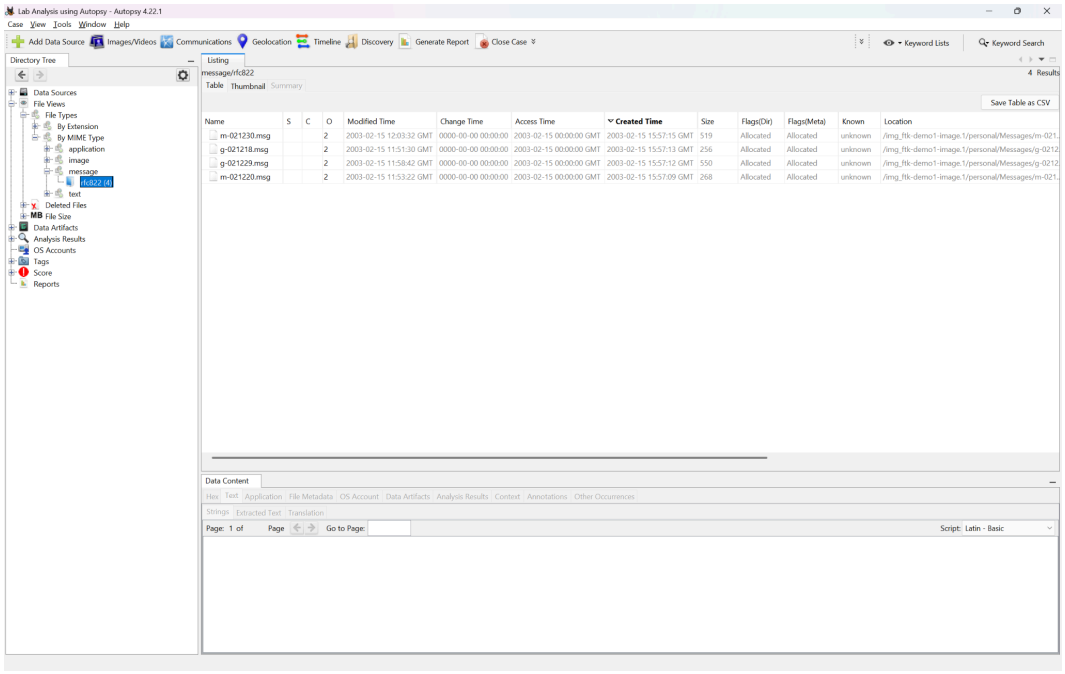
→ **There is 3 htm/html files**

Bank web files:

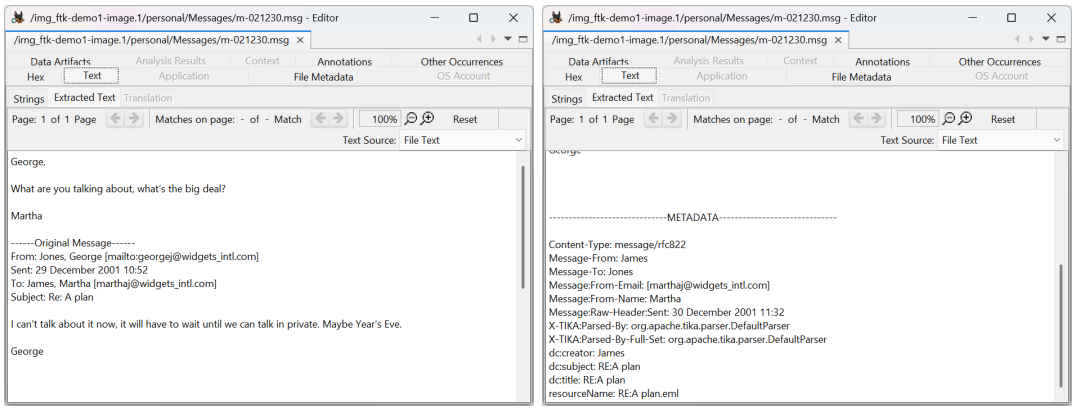
- /img_ftk-demo1-image.1/account/mt_bank.htm
- /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm
- /img_ftk-demo1-image.1/$CarvedFiles/1/f0001705_mt_bank.html

(More info included in the report)

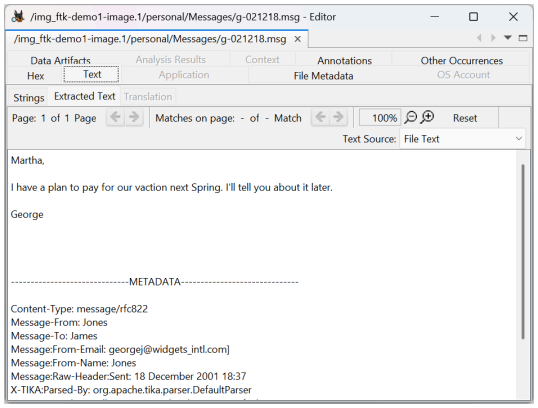
6. Determine how we know that George has been using Outlook Express to send messages, we can rely on file extensions, which provide important clues about the software used.



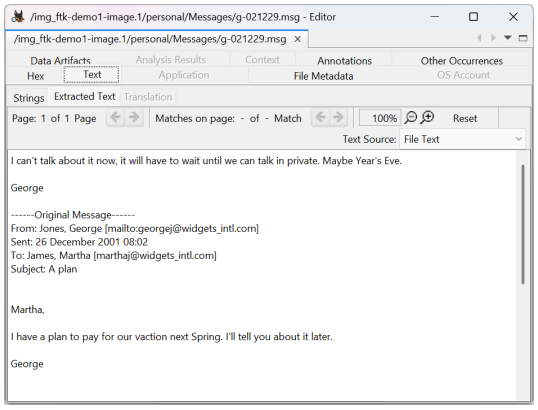
→ George used Outlook to communicate with Martha, as evidenced by .msg files



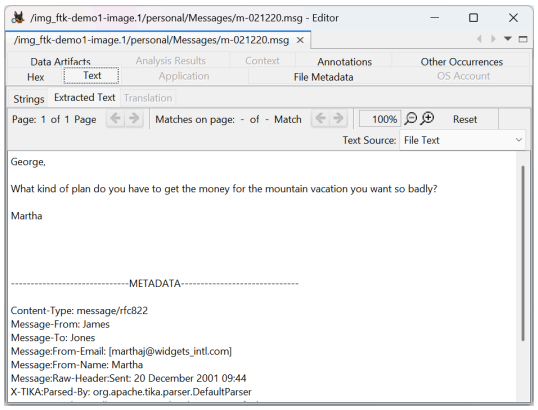
→ /img_ftk-demo1-image.1/personal/Messages/m-021230.msg



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



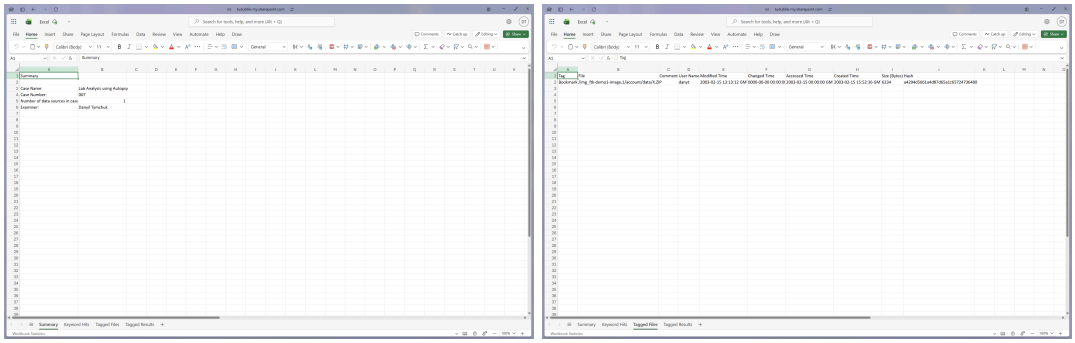
→ **/img_ftk-demo1-image.1/personal/Messages/g-021229.msg**



→ **/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.

Computer & Network Forensics

Lab 4 (Report)

Forensics Analysis using Autopsy

FTK Forensic Analysis Report

Name: Danyil Tymchuk
Date: 20/10/2025
Case Name: Lab Analysis using Autopsy
Tool Used: Autopsy 4.22.1

- **For Investigate Foundings:** Internet Archive (archive.org)

Introduction

This is the second investigation of the same image. First was performed using AccessData Forensic Toolkit (FTK). Now we are using the Autopsy tool to analyze this image, and confirm and try to find new information.
This report documents the digital forensic examination of a sample image file (ftk-demo1-image.1) performed using Autopsy 4.22.1 between 20 October 2025 and 22 October 2025.
The purpose of this analysis was to identify, recover, and interpret digital evidence relating to potential financial misconduct and data concealment by two suspects, George Jones and Martha James, Steve Billings's employees.

All evidence was analyzed in accordance with standard digital forensic procedures, ensuring the preservation of data integrity and maintaining a clear chain of custody.
The analysis focused on uncovering encrypted communications, deleted files, and hidden financial records that could demonstrate intent to defraud or conceal company funds.

What am I doing?

- Locate and recover deleted files from the provided forensic image.
- Analyze email and text communications between involved parties for indications of collusion or fraudulent activity.
- Identify and decrypt password-protected files / archives.
- Correlate digital findings with physical evidence and metadata.
- Document all forensic procedures and maintain evidentiary integrity throughout the analysis.

Contents

Objective

By following these guidelines and documenting my forensic analysis thoroughly, I will create a credible and informative forensic report. This report will not only serve as a record of my investigation but also as a valuable resource for presenting my findings and insights to others involved in the case.

1. Methodical Approach: Begin your investigation with a systematic and methodical approach. Carefully consider the objectives of your analysis and the questions you seek to answer. Remembering 5W-H from lecture-1
2. Document Everything: Maintain detailed records of each step you take during the investigation. Record the tools and software used, the files examined, and the actions performed. Be sure to timestamp your activities to establish a timeline of your investigation.
3. Screenshots: Screenshots are invaluable for documenting your actions and the state of the evidence at various points in the investigation. Capture screenshots to illustrate significant findings, folder structures, and any anomalies you encounter. These visual aids enhance the comprehensibility of your report.
4. File and Folder Organization: Keep your files and folders organized. Create a structured directory where you can store your documentation, screenshots, and any reports you generate during the investigation. This ensures that your findings are easily accessible and well-organized.
5. Analysis and Findings: As you examine files and uncover evidence, document your findings thoroughly. Include relevant information such as file names, timestamps, and any text or data extracted from the evidence. If you encounter any suspicious or noteworthy items, make a note of them.
6. Maintain Chain of Custody: If applicable, ensure the chain of custody for the digital evidence is preserved. Document who had access to the evidence and when, as well as any actions taken by individuals involved in the investigation.
7. Report Compilation: After completing your analysis, compile a forensic report that encapsulates your investigation process, findings, and conclusions. The report should be clear, concise, and organized. Include relevant screenshots and references to evidence.

Evidences from my previous investigation

The following artifacts were recovered and analyzed in the previous lab using AccessData FTK. Each piece of evidence contributed to identifying suspicious communications, encrypted files, and indications of financial fraud involving George and Martha:

1. **!_Y.EXE (deleted executable)**
   - Contained an encrypted text message referencing the Merriam-Webster dictionary, which served as a clue to derive the password used later in the investigation.
2. **!AF6.JPG (deleted)**
   - Image associated with the same email chain, recovered as part of the evidence set linking digital communications to the suspects.
3. **g-021218.msg, g-021220.msg, g-021229.msg, g-021230.msg**
   - Showed coordination between both suspects and further indicated awareness of the concealed financial dealings.
4. **msg4.txt (deleted), msg5.txt (deleted), msg7.txt (deleted)**
   - Contained incriminating communications between George and Martha discussing payments, invoices, and hidden transactions.
5. **mt_bank_secrecy.htm**
   - Email message from a bank containing the line *"The password for your account is: couch"*, directly leading to decryption of the ZIP archive.
6. **X.ZIP (encrypted) → [SWISS.XML, SWISS.TXT, SWISS.CSV] (encrypted)**
   - Encrypted archive unlocked using the password couch. Contained financial files SWISS.TXT, SWISS.XLS, and SWISS.CSV, which referenced Swiss bank account number 9882111.
   - **[SWISS.XML, SWISS.TXT, SWISS.CSV]** – Bank statement files confirming offshore financial activity and the presence of concealed funds.

Chain of Custody

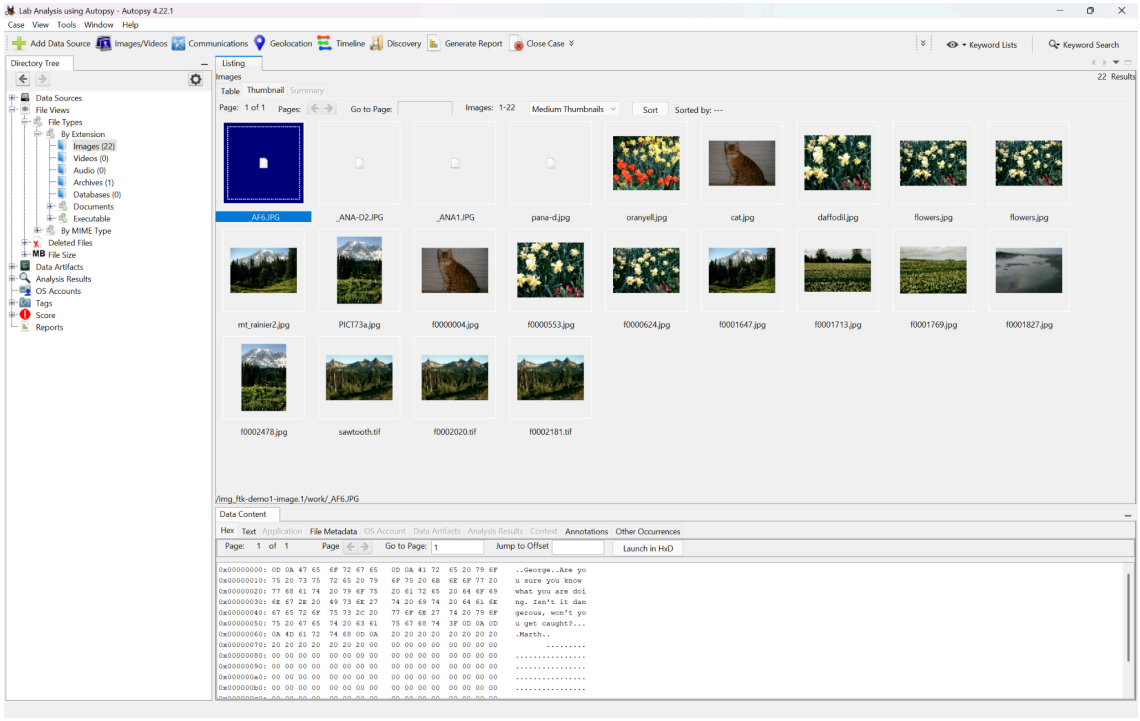
Date / Time	Action	Handled By
20/10/2025 22:00 – 21/10/2025 01:00	Analysis Period	Danyil Tymchuk
21/10/2025 22:00 – 22/10/2025 01:00	Analysis Period	Danyil Tymchuk
21/10/2025 13:00 – 22/10/2025 16:00	Analysis Period, Case Closure	Danyil Tymchuk

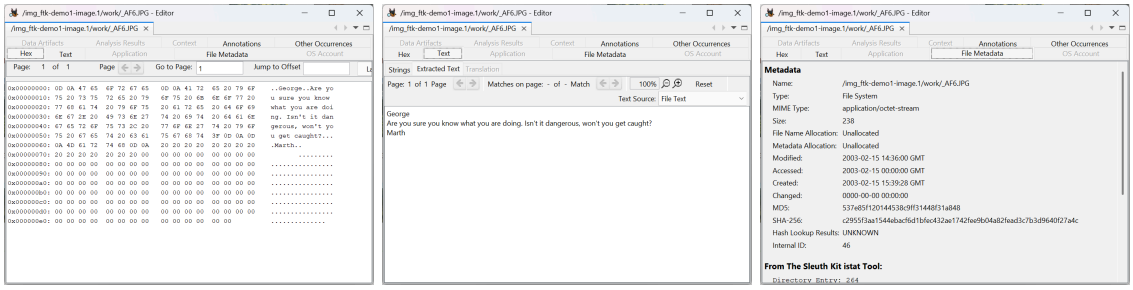
Summary of Collected Evidence

Evidence No.	File Name / Type	Description	Relevance
1	`!AF6.JPG` (deleted)	Image with message from Martha expressing concern.	Confirms awareness and complicity.
2	`X.ZIP` (encrypted), `Unalloc_4_17920_1474560` (deleted), `_SG8.TXT` (deleted), `__Y.EXE` (deleted), `f0000003.txt` (deleted), `mt_bank_secrecy.htm`	Looking for the “password” using the Keyword Search.	To get the password for the encrypted content (X.ZIP).
3	`X.ZIP` (encrypted) `[SWISS.XML, SWISS.TXT, SWISS.CSV]` (encrypted)	Encrypted Zip Archive Containing Swiss Bank Records.	Proof of hidden assets totaling about $3.9M.
4	all text files: `.txt, .csv, .htm/html`	Text files.	Get more evidences.
5	`g-021218.msg`, `g-021220.msg`, `g-021229.msg`, `g-021230.msg`	Email conversation between George and Martha discussing “a plan.”	Indicates coordination and secrecy.
6	`_AIL5.GIF`, `_SGC.TXT`	Martha betrays George?	Martha’s connection to “a plan”

Findings

Evidence #1 Image Containing Questioning Message





Timestamp: 20/10/2025 23:42:27
File Name: _AF6.JPG
Full Path: /img_ftk-demo1-image.1/work/_AF6.JPG
File extension: JPG – JPEG image (Images)

I already discovered and analysed this file in the previous investigation.

Description:

The image file _AF6.JPG contains a short textual message from Martha to George.
The visible text reads:
“George
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?
Marth”

Analysis:

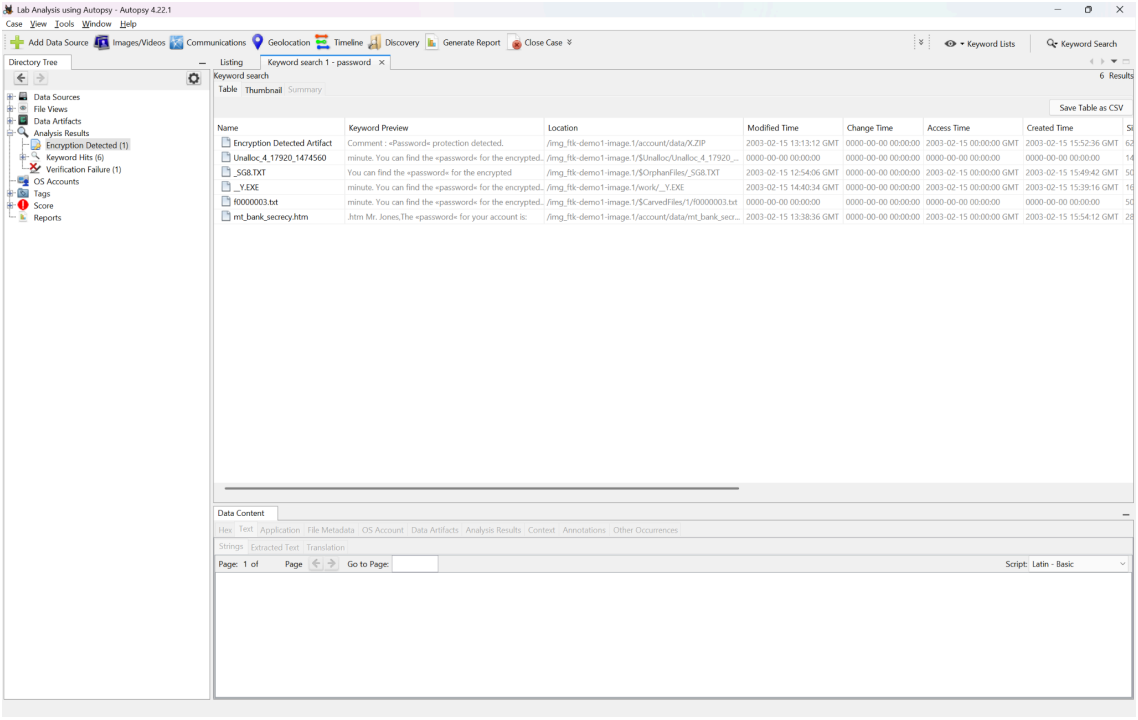
Although brief, this image provides direct evidence of Martha expressing concern about George's actions. The phrasing implies that Martha was aware of potentially risky or illicit behavior and feared detection.

Relevance:

This evidence establishes:

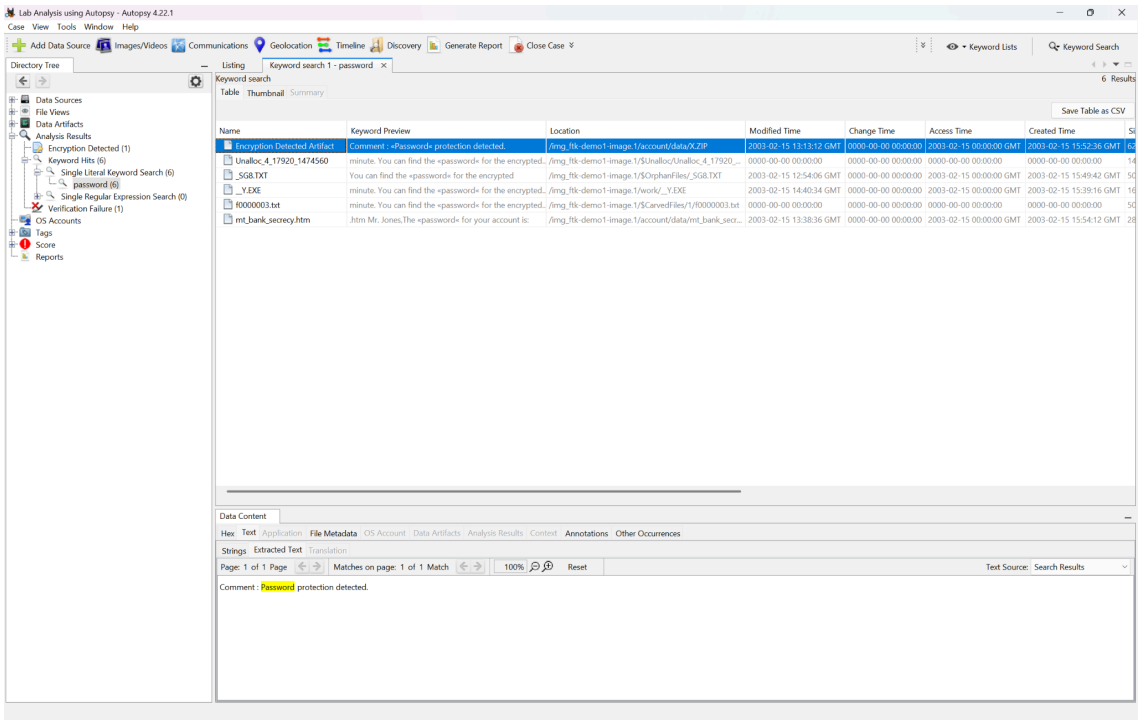
- Corroborates earlier communications showing Martha and George discussing a clandestine plan.
- Demonstrates Martha's awareness and possible complicity, or at least her knowledge of the risky nature of the activities.
- Adds a human/contextual element to the technical evidence.

Evidence #2 Files, that contain the word "password"



Timestamp: 21/10/2025 00:06:07
Files: X.ZIP, Unalloc_4_17920_1474560, _SG8.TXT, __Y.EXE, f0000003.txt, mt_bank_secrecy.htm
– 6 files contain the word "password"

Encryption Detected Artifact (X.ZIP) — excerpt / description



Timestamp: 21/10/2025 00:10:03
File Name: X.ZIP
Full Path: /img_ftk-demo1-image.1/account/data/X.ZIP
File extension: ZIP – Compressed Archive

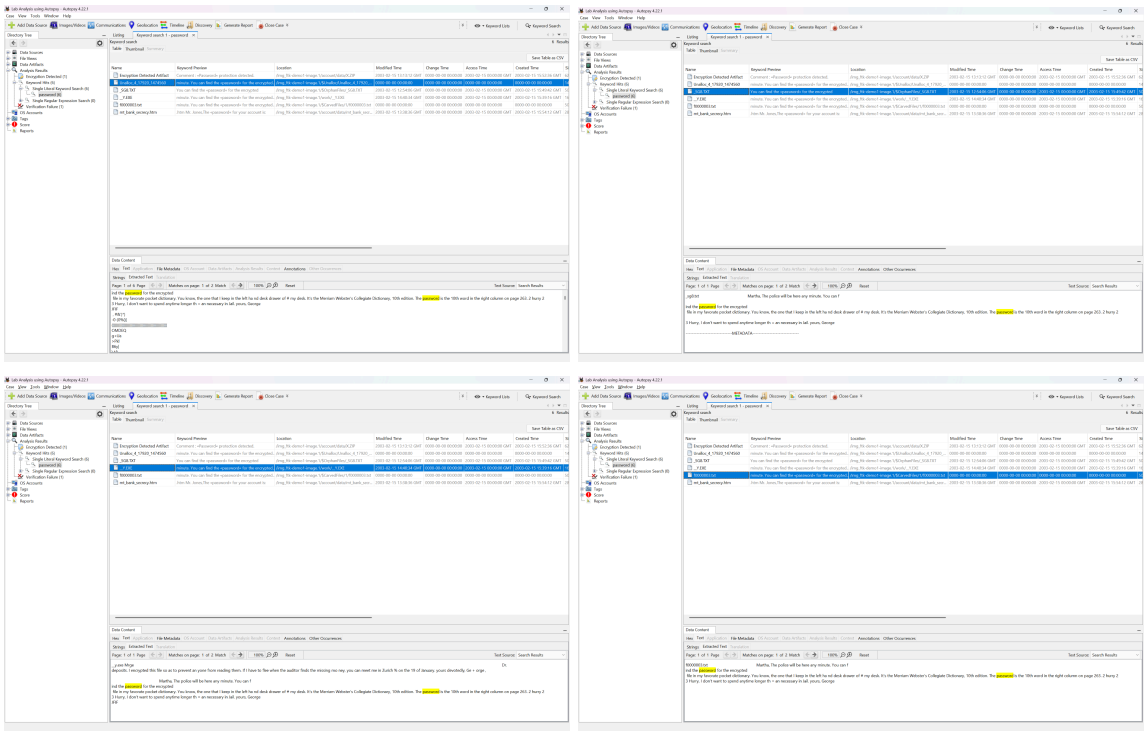
I already discovered and analysed this file in the previous investigation.

Excerpt:
“Comment : Password protection detected.”

Description & Analysis:
This file is password protected.

Relevance:
We are looking for a password for this file.

[Unalloc_4_17920_1474560, _SG8.TXT, __Y.EXE, f0000003.txt] — excerpt / description



Timestamp: 21/10/2025 00:11:30
File Name/Path:

- /img_ftk-demo1-image.1/$Unalloc/Unalloc_4_17920_1474560
- /img_ftk-demo1-image.1/$OrphanFiles/_SG8.TXT
- /img_ftk-demo1-image.1/work/__Y.EXE
- /img_ftk-demo1-image.1/$CarvedFiles/1/f0000003.txt

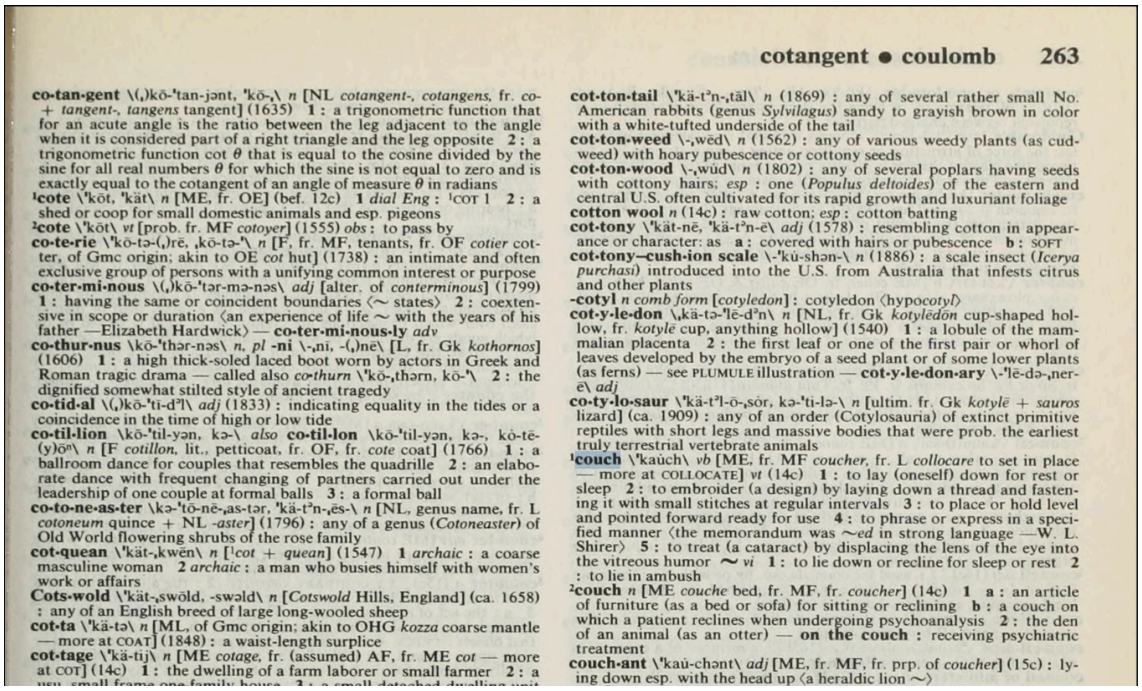
I already discovered and analysed some of these files in the previous investigation.

Excerpt:
All these files 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.”

Description & Analysis:
A hint where to find the password.

Relevance:
Already done this in a previous investigation. Found the hidden password: “couch” in the Merriam Webster's Collegiate Dictionary.

Merriam Webster's Collegiate Dictionary, 10th edition



co·tan·gent \(ˌ)kō-ˈtan-jənt, ˈkō-ˌ\ *n* [NL *cotangent-, cotangens*, fr. *co-* + *tangent-, tangens* tangent] (1635) **1** : a trigonometric function that for an acute angle is the ratio between the leg adjacent to the angle when it is considered part of a right triangle and the leg opposite **2** : a trigonometric function cot θ that is equal to the cosine divided by the sine for all real numbers θ for which the sine is not equal to zero and is exactly equal to the cotangent of an angle of measure θ in radians

¹cote \ˈkōt, ˈkät\ *n* [ME, fr. OE] (bef. 12c) **1** *dial Eng* : ¹COT 1 **2** : a shed or coop for small domestic animals and esp. pigeons

²cote \ˈkōt\ *vt* [prob. fr. MF *cotoyer*] (1555) *obs* : to pass by

co·te·rie \ˈkō-tə-(ˌ)rē, ˌkō-tə-ˈ\ *n* [F, fr. MF, tenants, fr. OF *cotier* cotter, of Gmc origin; akin to OE *cot* hut] (1738) : an intimate and often exclusive group of persons with a unifying common interest or purpose

co·ter·mi·nous \(ˌ)kō-ˈtər-mə-nəs\ *adj* [alter. of *conterminous*] (1799) **1** : having the same or coincident boundaries ⟨~ states⟩ **2** : coextensive in scope or duration ⟨an experience of life ~ with the years of his father —Elizabeth Hardwick⟩ — **co·ter·mi·nous·ly** *adv*

co·thur·nus \kō-ˈthər-nəs\ *n, pl* **-ni** \-ˌnī, -(ˌ)nē\ [L, fr. Gk *kothornos*] (1606) **1** : a high thick-soled laced boot worn by actors in Greek and Roman tragic drama — called also *co·thurn* \ˈkō-ˌthərn, kō-ˈ\ **2** : the dignified somewhat stilted style of ancient tragedy

co·tid·al \(ˌ)kō-ˈtī-dᵊl\ *adj* (1833) : indicating equality in the tides or a coincidence in the time of high or low tide

co·til·lion \kō-ˈtil-yən, kə-\ *also* **co·til·lon** \kō-ˈtil-yən, kə-, kȯ-tē-(y)ōⁿ\ *n* [F *cotillon*, lit., petticoat, fr. OF, fr. *cote* coat] (1766) **1** : a ballroom dance for couples that resembles the quadrille **2** : an elaborate dance with frequent changing of partners carried out under the leadership of one couple at formal balls **3** : a formal ball

co·to·ne·as·ter \kə-ˈtō-nē-ˌas-tər, ˈkä-tᵊn-ˌēs-\ *n* [NL, genus name, fr. L *cotoneum* quince + NL *-aster*] (1796) : any of a genus (*Cotoneaster*) of Old World flowering shrubs of the rose family

cot·quean \ˈkät-ˌkwēn\ *n* [¹*cot* + *quean*] (1547) **1** *archaic* : a coarse masculine woman **2** *archaic* : a man who busies himself with women's work or affairs

Cots·wold \ˈkät-ˌswōld, -swəld\ *n* [*Cotswold* Hills, England] (ca. 1658) : any of an English breed of large long-wooled sheep

cot·ta \ˈkä-tə\ *n* [ML, of Gmc origin; akin to OHG *kozza* coarse mantle — more at COAT] (1848) : a waist-length surplice

cot·tage \ˈkä-tij\ *n* [ME *cotage*, fr. (assumed) AF, fr. ME *cot* — more at COT] (14c) **1** : the dwelling of a farm laborer or small farmer **2** : a [illegible]

cot·ton·tail \ˈkä-tᵊn-ˌtāl\ *n* (1869) : any of several rather small No. American rabbits (genus *Sylvilagus*) sandy to grayish brown in color with a white-tufted underside of the tail

cot·ton·weed \-ˌwēd\ *n* (1562) : any of various weedy plants (as cudweed) with hoary pubescence or cottony seeds

cot·ton·wood \-ˌwüd\ *n* (1802) : any of several poplars having seeds with cottony hairs; *esp* : one (*Populus deltoides*) of the eastern and central U.S. often cultivated for its rapid growth and luxuriant foliage

cotton wool *n* (14c) : raw cotton; *esp* : cotton batting

cot·tony \ˈkät-nē, ˈkä-tᵊn-ē\ *adj* (1578) : resembling cotton in appearance or character: as **a** : covered with hairs or pubescence **b** : SOFT

cot·tony–cush·ion scale \-ˈkù-shən-\ *n* (1886) : a scale insect (*Icerya purchasi*) introduced into the U.S. from Australia that infests citrus and other plants

-cotyl *n comb form* [*cotyledon*] : cotyledon ⟨hypocotyl⟩

cot·y·le·don \ˌkä-tə-ˈlē-dᵊn\ *n* [NL, fr. Gk *kotylēdōn* cup-shaped hollow, fr. *kotylē* cup, anything hollow] (1540) **1** : a lobule of the mammalian placenta **2** : the first leaf or one of the first pair or whorl of leaves developed by the embryo of a seed plant or of some lower plants (as ferns) — see PLUMULE illustration — **cot·y·le·don·ary** \-ˈlē-də-ˌner-ē\ *adj*

co·ty·lo·saur \ˈkä-tᵊl-ō-ˌsȯr, kə-ˈti-lə-\ *n* [ultim. fr. Gk *kotylē* + *sauros* lizard] (ca. 1909) : any of an order (Cotylosauria) of extinct primitive reptiles with short legs and massive bodies that were prob. the earliest truly terrestrial vertebrate animals

¹couch \ˈkau̇ch\ *vb* [ME, fr. MF *coucher*, fr. L *collocare* to set in place — more at COLLOCATE] *vt* (14c) **1** : to lay (oneself) down for rest or sleep **2** : to embroider (a design) by laying down a thread and fastening it with small stitches at regular intervals **3** : to place or hold level and pointed forward ready for use **4** : to phrase or express in a specified manner ⟨the memorandum was ~*ed* in strong language —W. L. Shirer⟩ **5** : to treat (a cataract) by displacing the lens of the eye into the vitreous humor ~ *vi* **1** : to lie down or recline for sleep or rest **2** : to lie in ambush

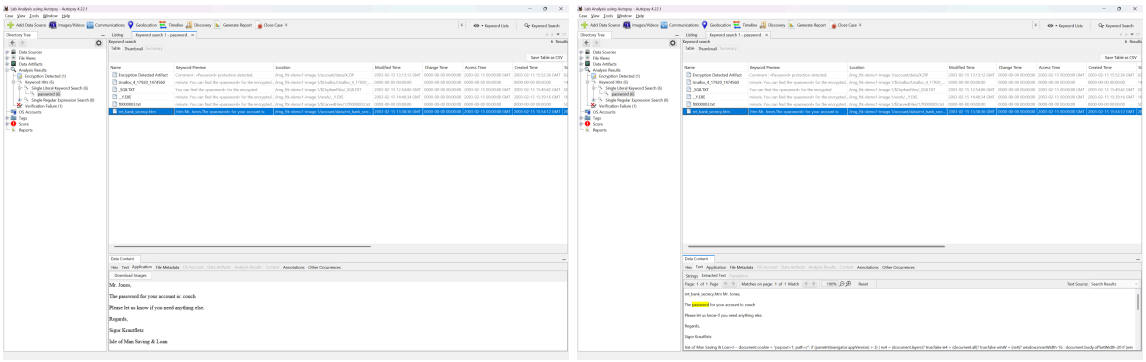
²couch *n* [ME *couche* bed, fr. MF, fr. *coucher*] (14c) **1 a** : an article of furniture (as a bed or sofa) for sitting or reclining **b** : a couch on which a patient reclines when undergoing psychoanalysis **2** : the den of an animal (as an otter) — **on the couch** : receiving psychiatric treatment

couch·ant \ˈkau̇-chənt\ *adj* [ME, fr. MF, fr. prp. of *coucher*] (15c) : lying down esp. with the head up ⟨a heraldic lion ~⟩

Found this book on Internet Archive: https://archive.org/details/merriamwebstersc01merr

When checked, the 10th word in the referenced dictionary page corresponds to **"couch"**, which may serve as the decryption password for the encrypted files found in the same evidence folder.

mt_bank_secrecy.htm — excerpt / description



Timestamp: 21/10/2025 00:11:51
File Name: mt_bank_secrecy.htm
Full Path: /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm
File extension: htm – Hypertext Document

I already discovered and analysed this file in the previous investigation.

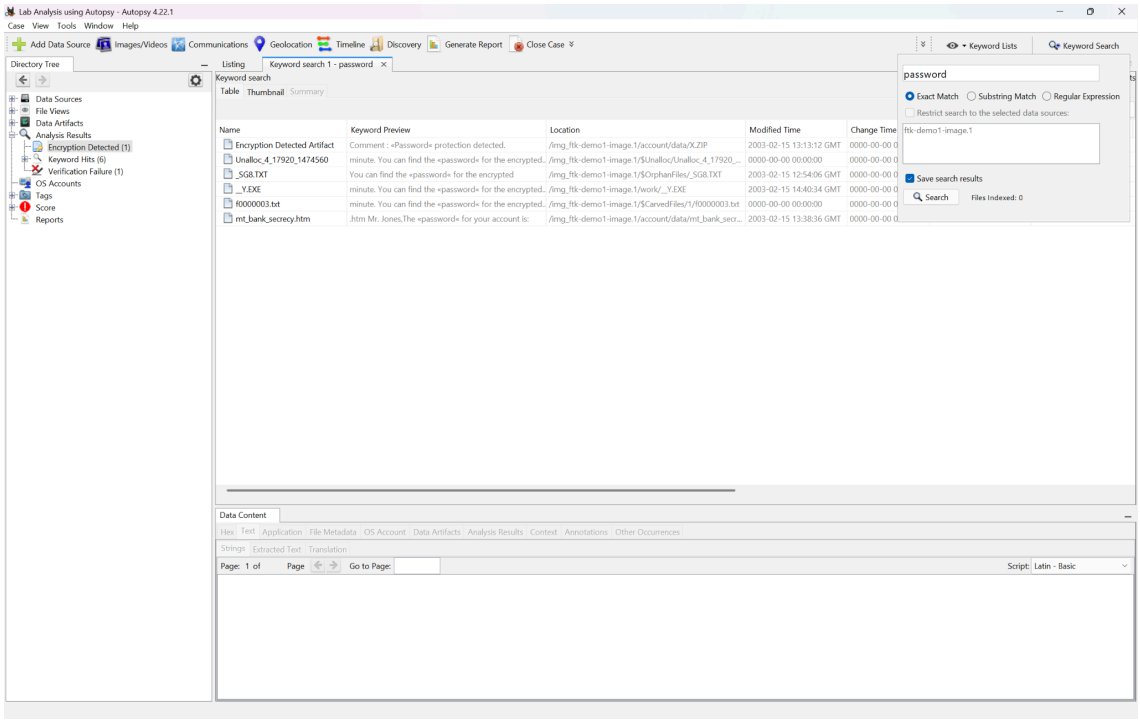
Excerpt:
“…
The password for your account is: couch
…”

Description & Analysis:
Message from the bank, where it says the password is “couch”. This password matches the password we found in the *Merriam Webster's Collegiate Dictionary*, from the previous hint.

Relevance:
Now we know the exact password for the encrypted content (X.ZIP).

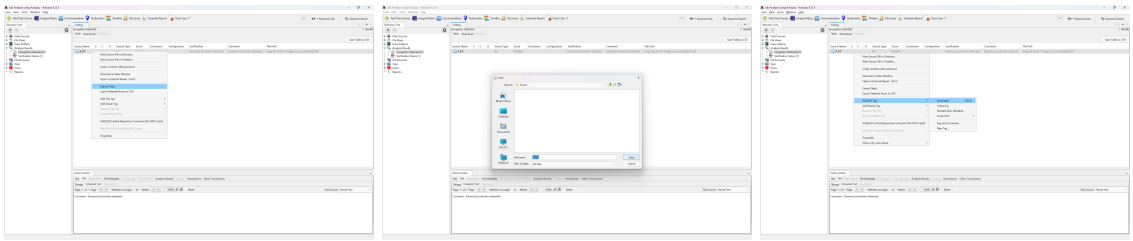
Evidence #3 Encrypted Zip Archive Containing Swiss Bank Records

Perform Keyword Search (“password”)

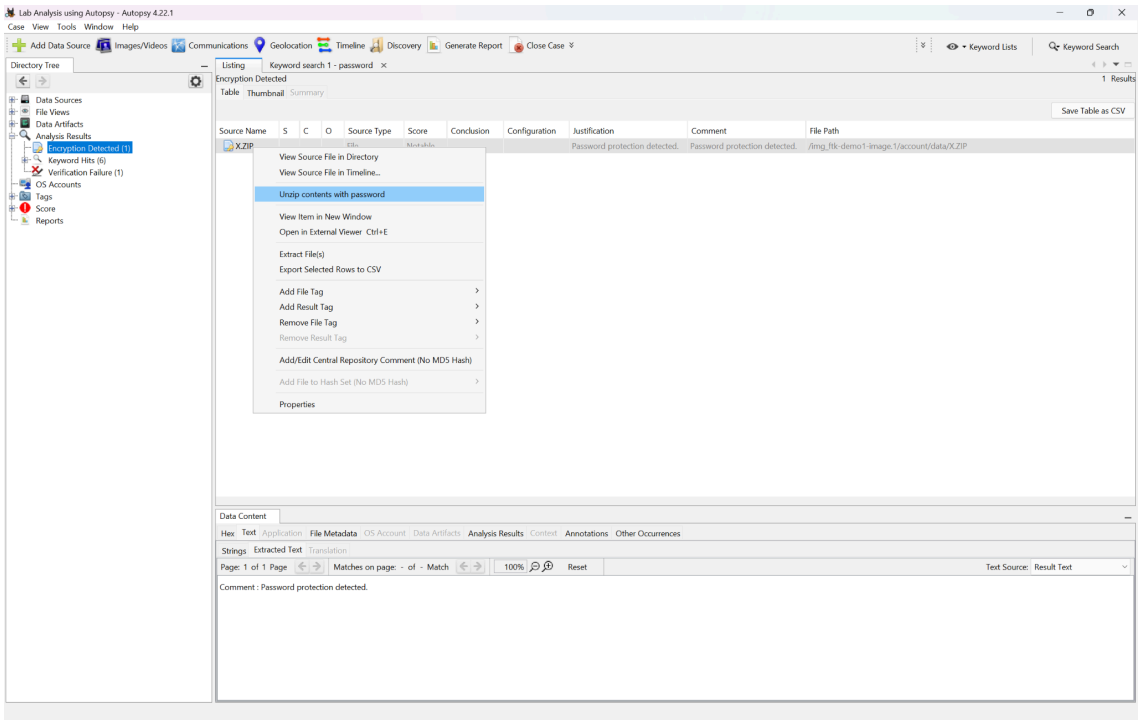


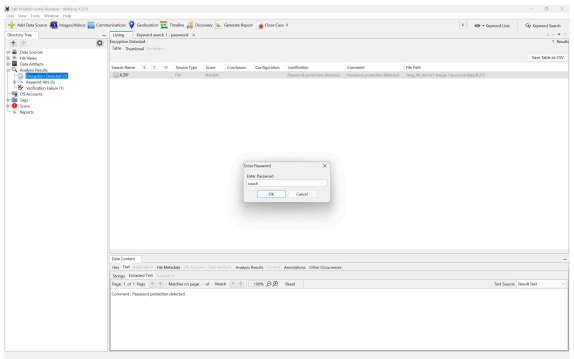
Note: step from the previous evidence, to get the password

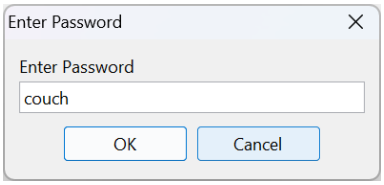
Export File & Add Bookmark File Tag



Unzip X.ZIP with password (“couch”)





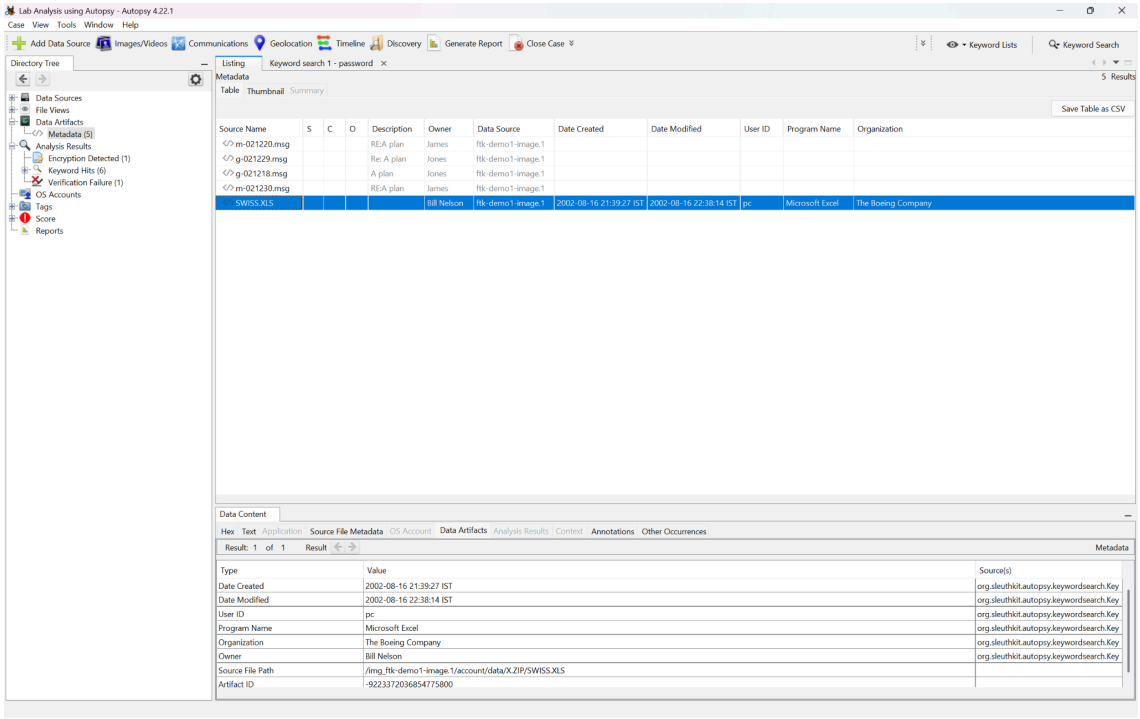


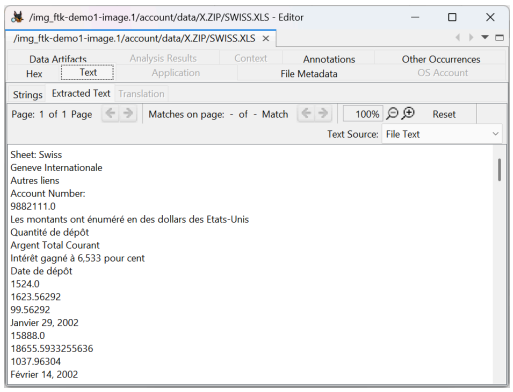
Timestamp: 21/10/2025 00:40:27
File Name: X.ZIP
Full Path: /img_ftk-demo1-image.1/account/data/X.ZIP
File extension: ZIP – Compressed Archive

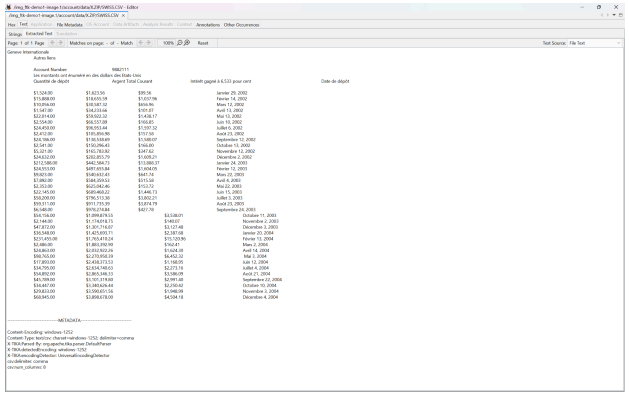
X.ZIP → [SWISS.XLS SWISS.TXT SWISS.CSV]

I already discovered and analysed this file in the previous investigation.

SWIZZ.XLS / SWIZZ.CSV / SWIZZ.TXT







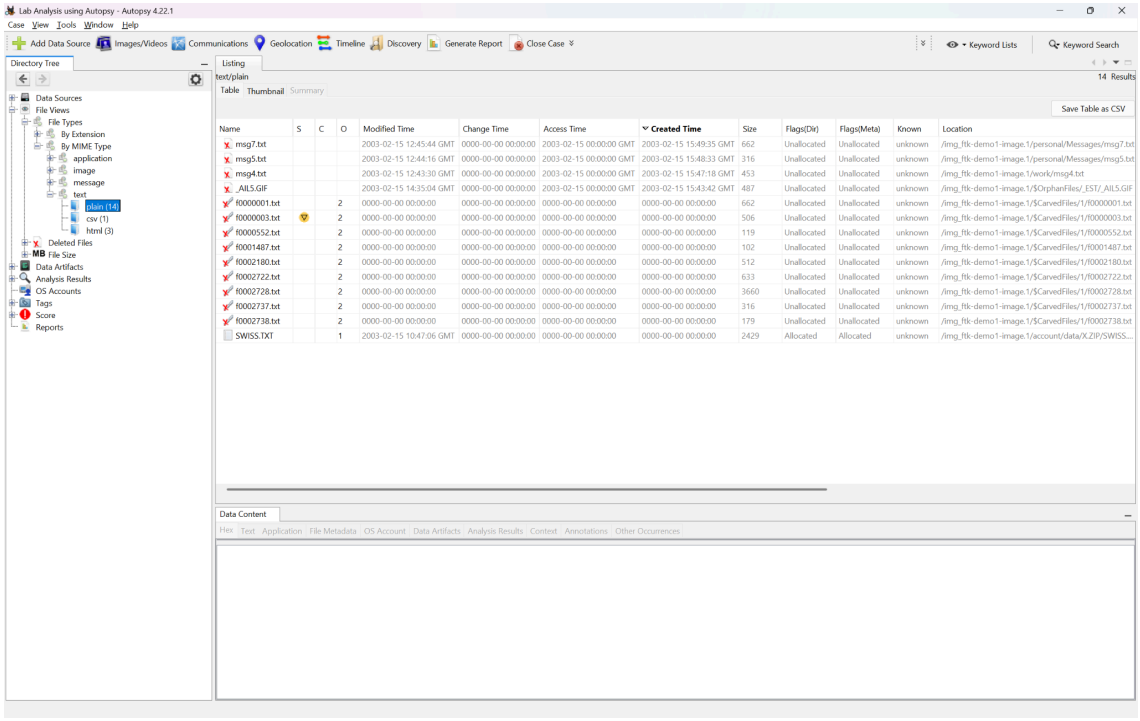
This file contains the bank statements where. **Looks like substantial evidence.**

I already discovered and analysed this file in the previous investigation.

Evidence #4 Text files

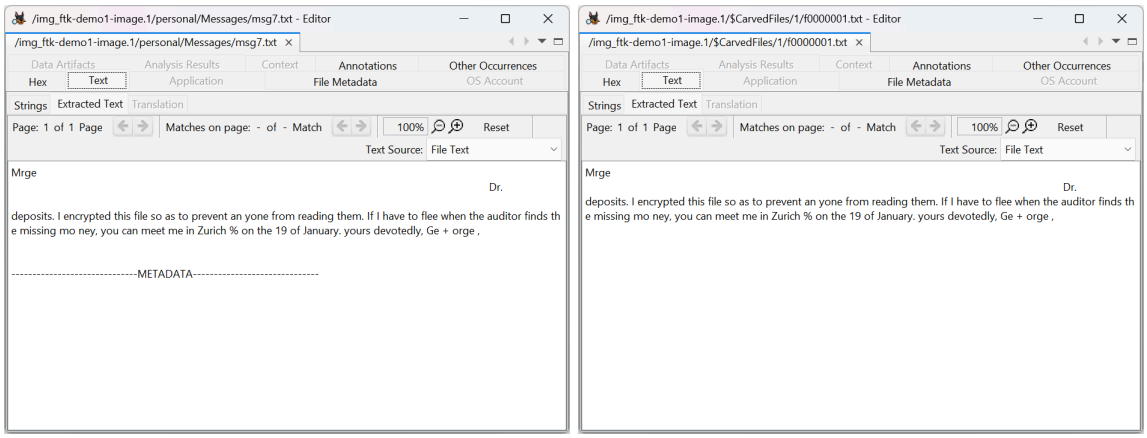
I already discovered and analysed some of these files in the previous investigation.

Plain text files



Timestamp: 22/10/2025 00:00:45
File extension: txt – Plain text (and one .gif)

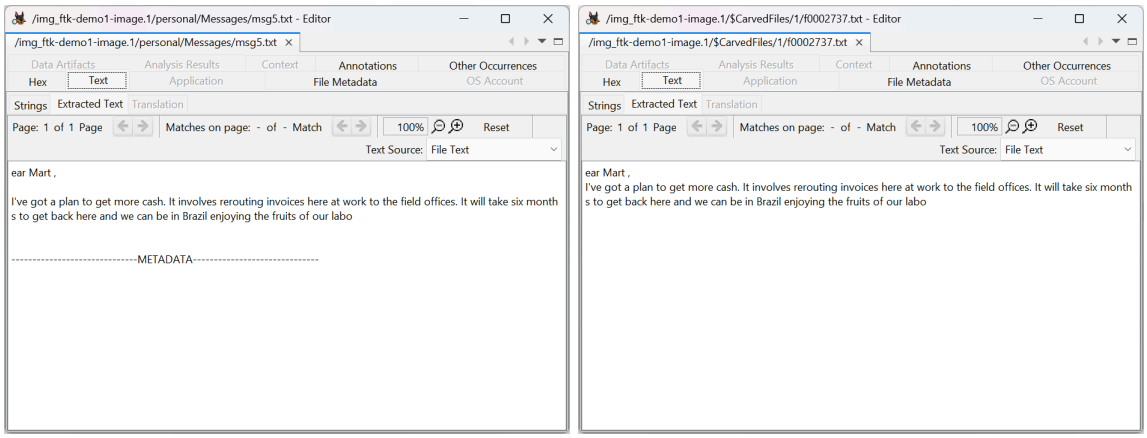
File Name: /img_ftk-demo1-image.1/personal/Messages/msg7.txt
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0000001.txt



Excerpt:

"…I encrypted this file so as to prevent an yone from reading them. If I have to flee when the auditor finds the missing mo ney, you can meet me in Zurich % on the 19 of January. yours devotedly, Ge + orge…"

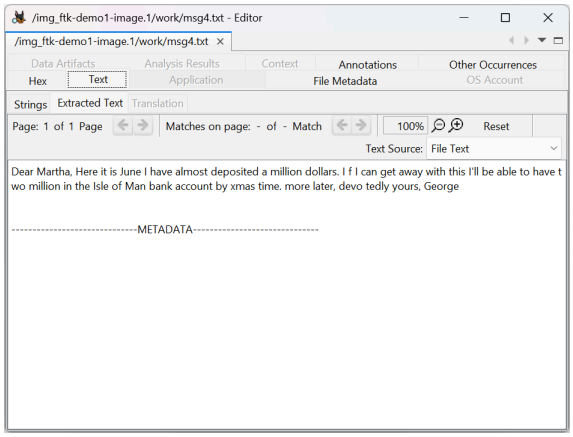
File Name: /img_ftk-demo1-image.1/personal/Messages/msg5.txt
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0002737.txt



Excerpt:

"…I've got a plan to get more cash. It involves rerouting invoices here at work to the field offices. It will take six months to get back here and we can be in Brazil…"

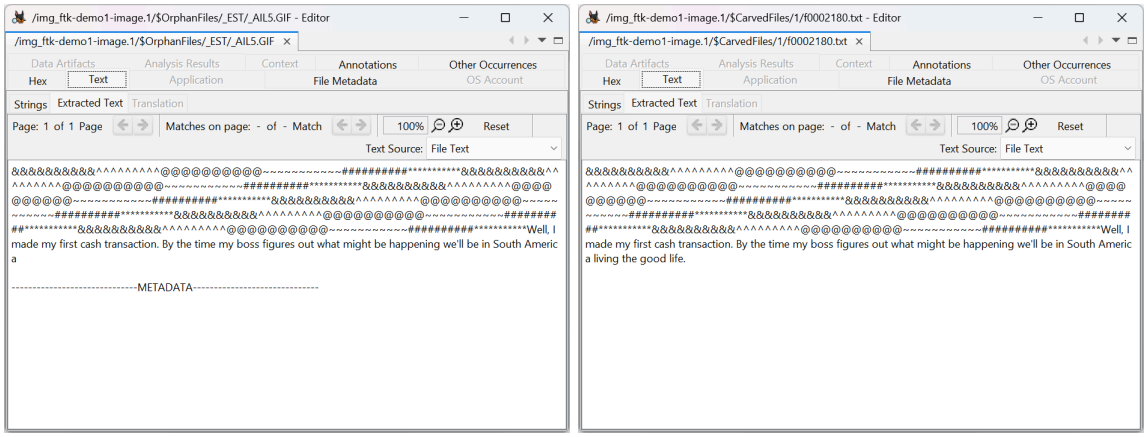
File Name: /img_ftk-demo1-image.1/work/msg4.txt



Excerpt:

“Dear Martha, Here it is June I have almost deposited a million dollars. I f I can get away with this I'll be able to have two million in the Isle of Man bank account by xmas time. more later, devo tedly yours, George”

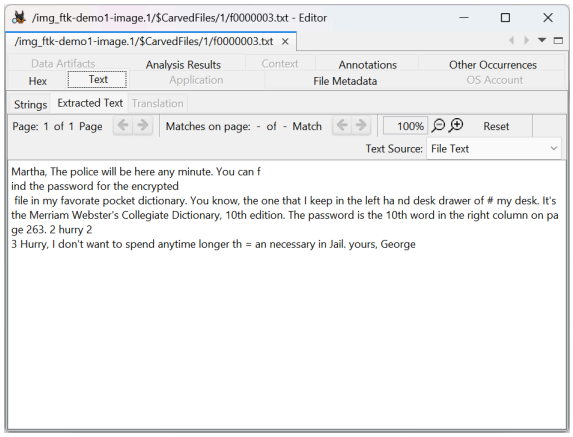
File Name: /img_ftk-demo1-image.1/$OrphanFiles/_EST/_AIL5.GIF
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0002180.txt



Excerpt:

“…Well, I made my first cash transaction. By the time my boss figures out what might be happening we'll be in South America…”

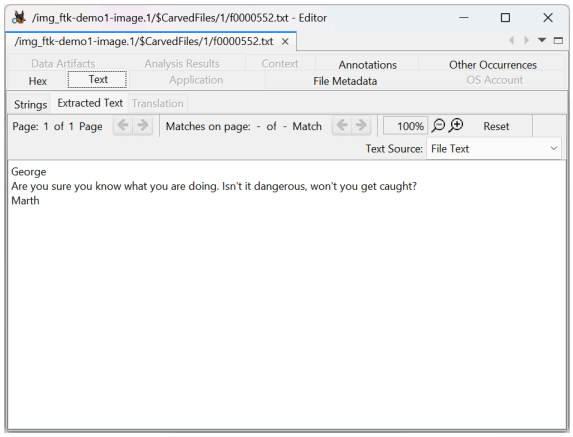
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0000003.txt



Excerpt:

“Martha, The police will be here any minute. You can find the password for the encrypted file in my favorate pocket dictionary. You know, the one that I keep in the left ha nd desk drawer of # my desk. It's the Merriam Webster's Collegiate Dictionary, 10th edition. The password is the 10th word in the right column on page 263. 2 hurry 2 3 Hurry, I don't want to spend anytime longer th = an necessary in Jail. yours, George”

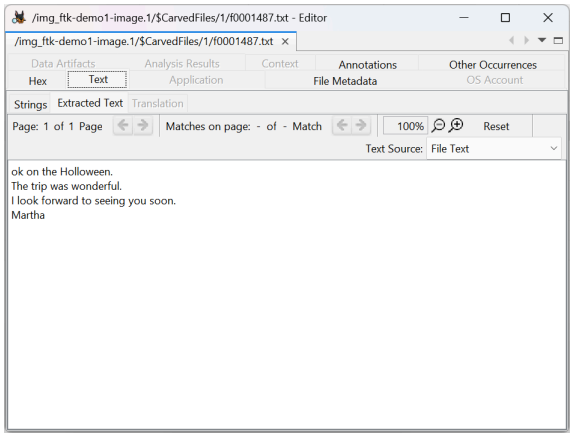
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0000552.txt



Excerpt:

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

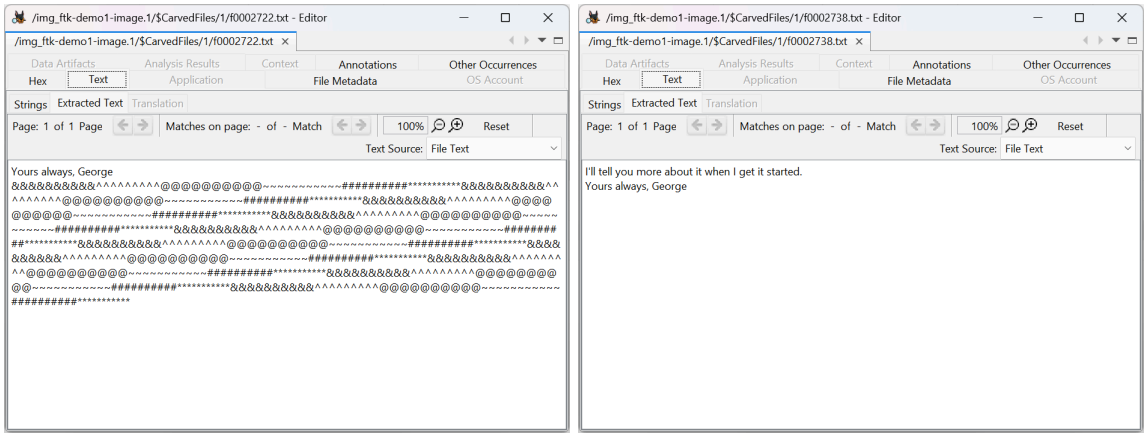
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0001487.txt



Excerpt:

“ok on the Holloween.
The trip was wonderful.
I look forward to seeing you soon.
Martha”

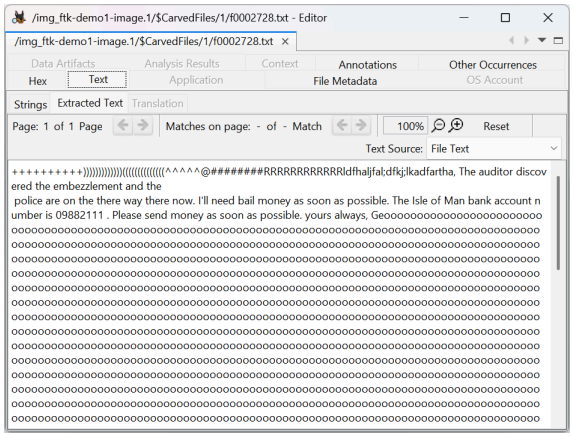
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0002722.txt
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0002738.txt



Excerpt:

“I'll tell you more about it when I get it started.
Yours always, George…”

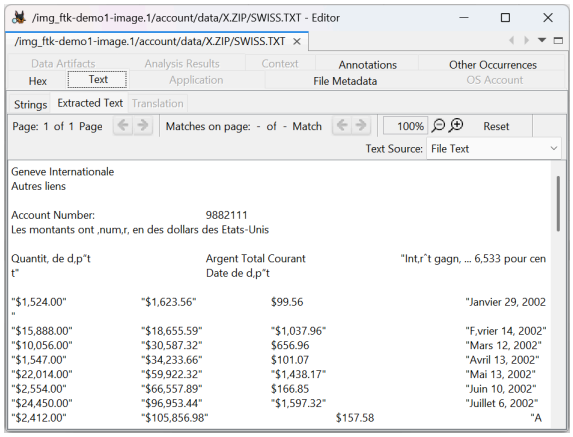
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0002728.txt



Excerpt:

"…The auditor discovered the embezzlement and the police are on the there way there now. I'll need bail money as soon as possible. The Isle of Man bank account number is 09882111 . Please send money as soon as possible. yours always…"

File Name: /img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.TXT



Excerpt:

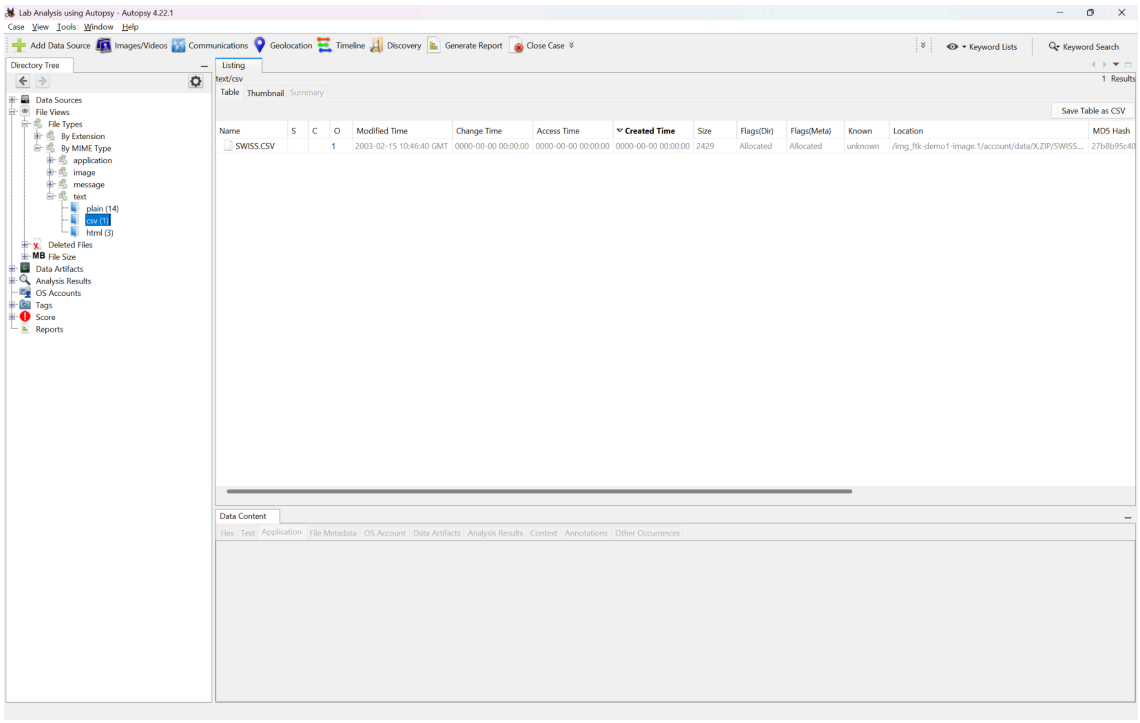
"Geneve Internationale
Autres liens

Account Number: 9882111
…"

Bank Statements

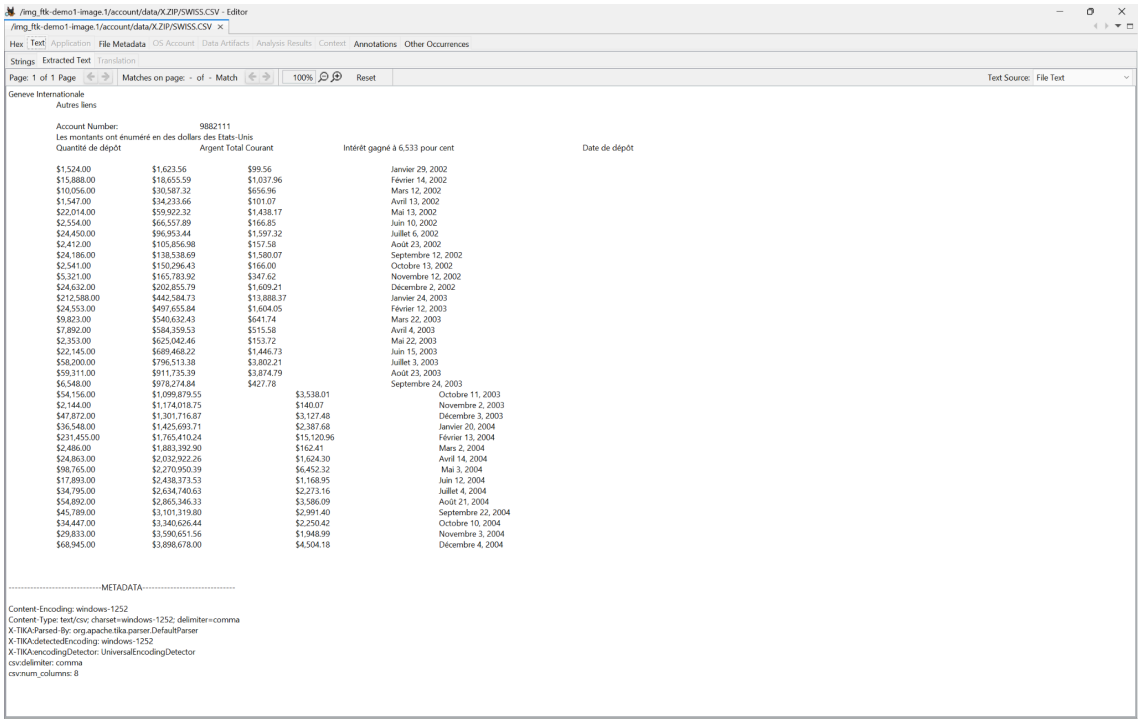
I already discovered and analysed this file in the previous investigation.

CSV text files



Timestamp: 22/10/2025 00:50:03
File extension: CSV – Comma-Separated Values

File Name: /img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.CSV



/img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.CSV - Editor

/img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.CSV

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

Strings | Extracted Text | Translation

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset | Text Source: File Text

Geneve Internationale
Autres liens

Account Number: 9882111
Les montants ont énuméré en des dollars des Etats-Unis

Quantité de dépôt	Argent Total Courant	Intérêt gagné à 6.533 pour cent	Date de dépôt
$1,524.00	$1,623.56	$99.56	Janvier 29, 2002
$15,888.00	$18,655.59	$1,037.96	Février 14, 2002
$10,056.00	$30,587.32	$656.96	Mars 12, 2002
$1,547.00	$34,233.66	$101.07	Avril 13, 2002
$22,014.00	$59,922.32	$1,438.17	Mai 13, 2002
$2,554.00	$66,557.89	$166.85	Juin 10, 2002
$24,450.00	$96,953.44	$1,597.32	Juillet 6, 2002
$2,412.00	$105,856.98	$157.58	Août 23, 2002
$24,186.00	$138,538.69	$1,580.07	Septembre 12, 2002
$2,541.00	$150,296.43	$166.00	Octobre 13, 2002
$5,321.00	$165,783.92	$347.62	Novembre 12, 2002
$24,632.00	$202,855.79	$1,609.21	Décembre 2, 2002
$212,588.00	$442,584.73	$13,888.37	Janvier 24, 2003
$24,553.00	$497,655.84	$1,604.05	Février 12, 2003
$9,823.00	$540,632.43	$641.74	Mars 22, 2003
$7,892.00	$584,359.53	$515.58	Avril 4, 2003
$2,353.00	$625,042.46	$153.72	Mai 22, 2003
$22,145.00	$689,468.22	$1,446.73	Juin 15, 2003
$58,200.00	$796,513.38	$3,802.21	Juillet 3, 2003
$59,311.00	$911,735.39	$3,874.79	Août 23, 2003
$6,548.00	$978,274.84	$427.78	Septembre 24, 2003
$54,156.00	$1,099,879.55	$3,538.01	Octobre 11, 2003
$2,144.00	$1,174,018.75	$140.07	Novembre 2, 2003
$47,872.00	$1,301,716.87	$3,127.48	Décembre 3, 2003
$36,548.00	$1,425,693.71	$2,387.68	Janvier 20, 2004
$231,455.00	$1,765,410.24	$15,120.96	Février 13, 2004
$2,486.00	$1,883,392.90	$162.41	Mars 2, 2004
$24,863.00	$2,032,922.26	$1,624.30	Avril 14, 2004
$98,765.00	$2,270,950.39	$6,452.32	Mai 3, 2004
$17,893.00	$2,438,373.53	$1,168.95	Juin 12, 2004
$34,795.00	$2,634,740.63	$2,273.16	Juillet 4, 2004
$54,892.00	$2,865,346.33	$3,586.09	Août 21, 2004
$45,789.00	$3,101,319.80	$2,991.40	Septembre 22, 2004
$34,447.00	$3,340,626.44	$2,250.42	Octobre 10, 2004
$29,833.00	$3,590,651.56	$1,948.99	Novembre 3, 2004
$68,945.00	$3,898,678.00	$4,504.18	Décembre 4, 2004

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

Content-Encoding: windows-1252
Content-Type: text/csv; charset=windows-1252; delimiter=comma
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:detectedEncoding: windows-1252
X-TIKA:encodingDetector: UniversalEncodingDetector
csv:delimiter: comma
csv:num_columns: 8

Excerpt:

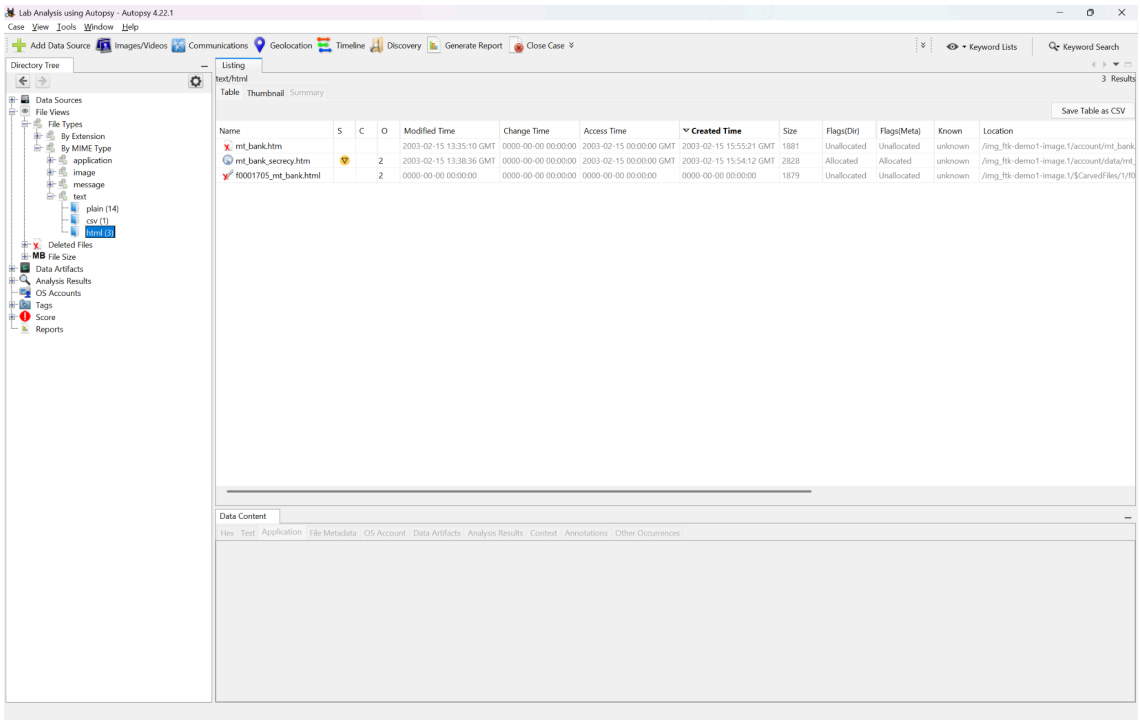
“Geneve Internationale
Autres liens

Account Number: 9882111
…”

Bank Statements

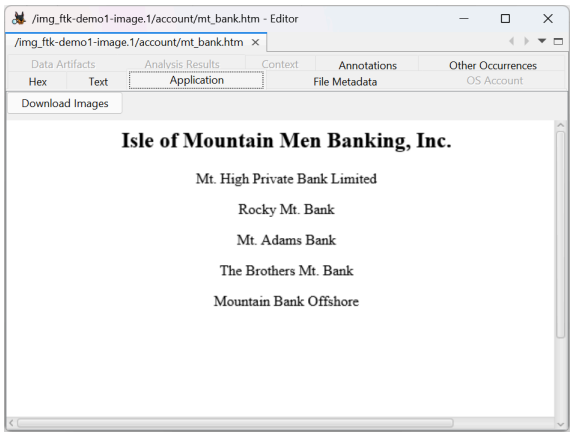
I already discovered and analysed this file in the previous investigation.

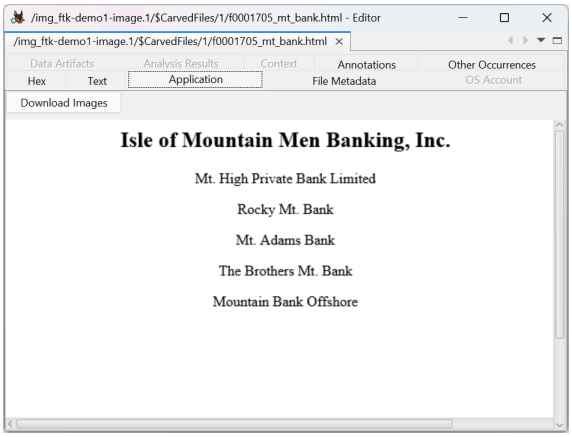
HTML text files



Timestamp: 22/10/2025 00:56:19
File extension: htm/html – Hypertext Document

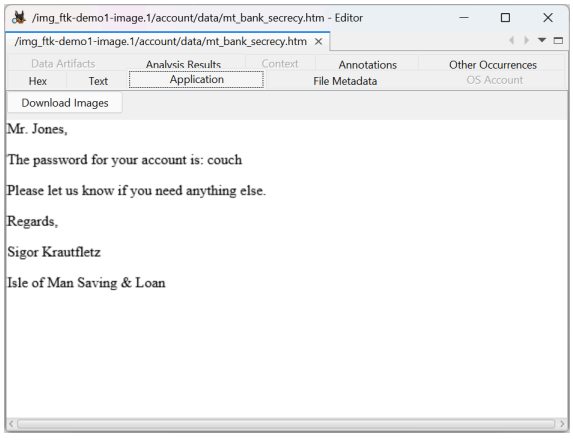
File Name: /img_ftk-demo1-image.1/account/mt_bank.htm
File Name: /img_ftk-demo1-image.1/$CarvedFiles/1/f0001705_mt_bank.html





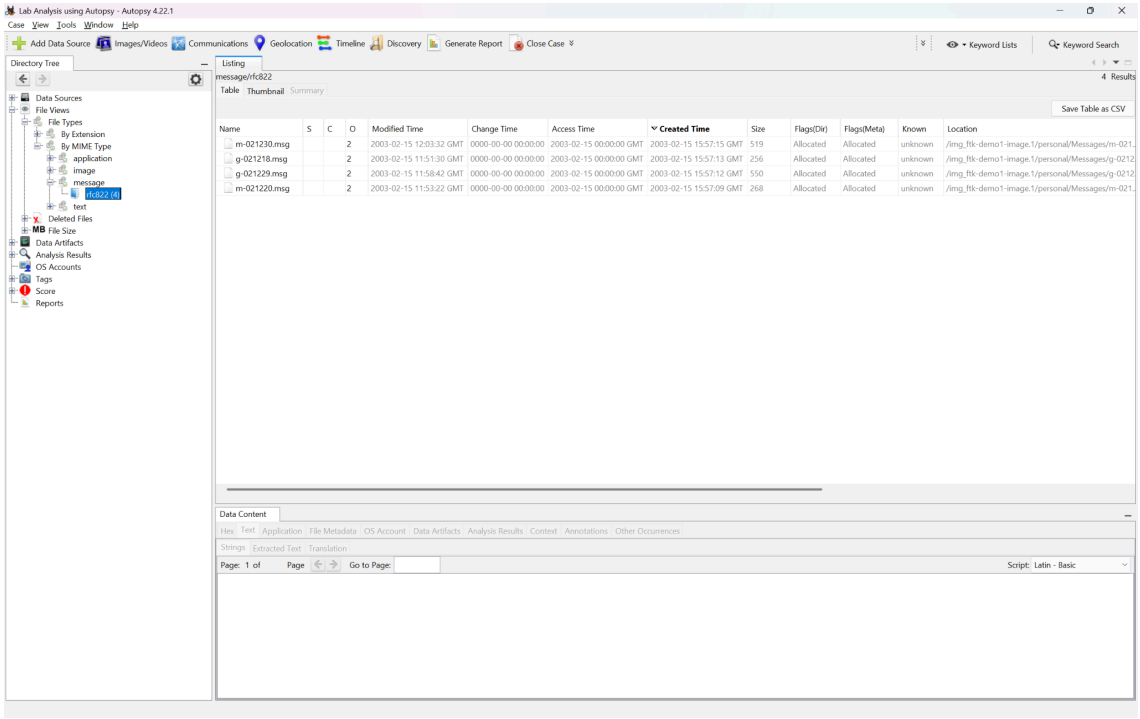
Excerpt:
"Isle of Mountain Men Banking, Inc.
Mt. High Private Bank Limited
Rocky Mt. Bank
Mt. Adams Bank
The Brothers Mt. Bank
Mountain Bank Offshore
Bank Secrecy Requirements"

File Name: /img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm



Excerpt:
"Mr. Jones,
The password for your account is: couch
Please let us know if you need anything else.
Regards,
Sigor Krautfletz
Isle of Man Saving & Loan"

Evidence #5 Email Correspondence Between George and Martha

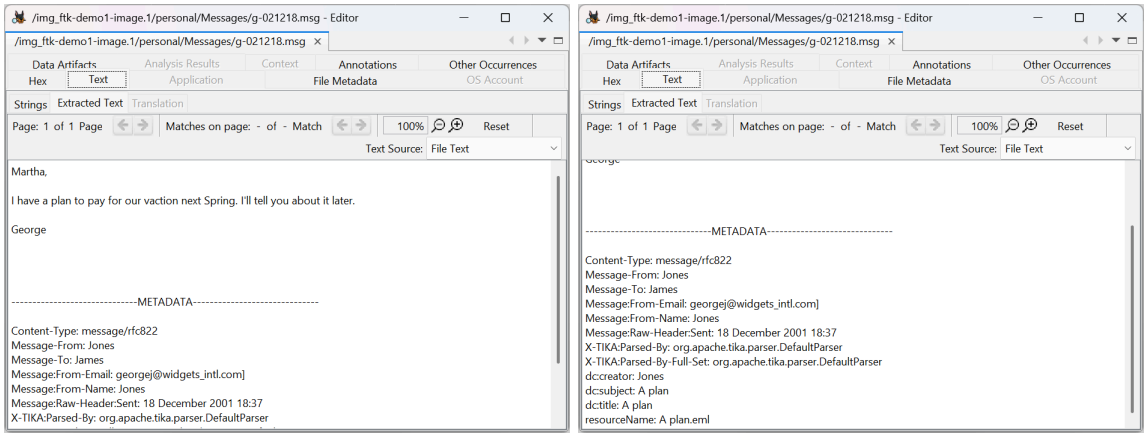


Timestamp: 22/10/2025 13:44:39
File extension: msg – Microsoft Outlook Message Files
Date Range: 18 December 2001 – 30 December 2001

I already discovered and analysed some of these files in the previous investigation.

---

g-021218.msg



File Path: /img_ftk-demo1-image.1/personal/Messages/g-021218.msg

Excerpt:

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

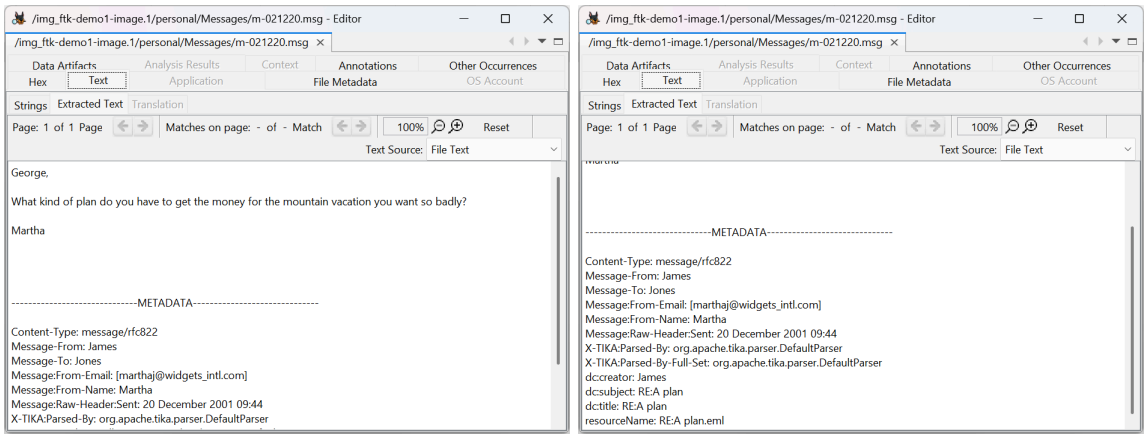
Metadata:

----------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
dc:creator: Jones
dc:subject: A plan
dc:title: A plan
resourceName: A plan.eml

I already discovered and analysed this file in the previous investigation.

---

m-021220.msg



File Path: /img_ftk-demo1-image.1/personal/Messages/m-021220.msg

Excerpt:

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

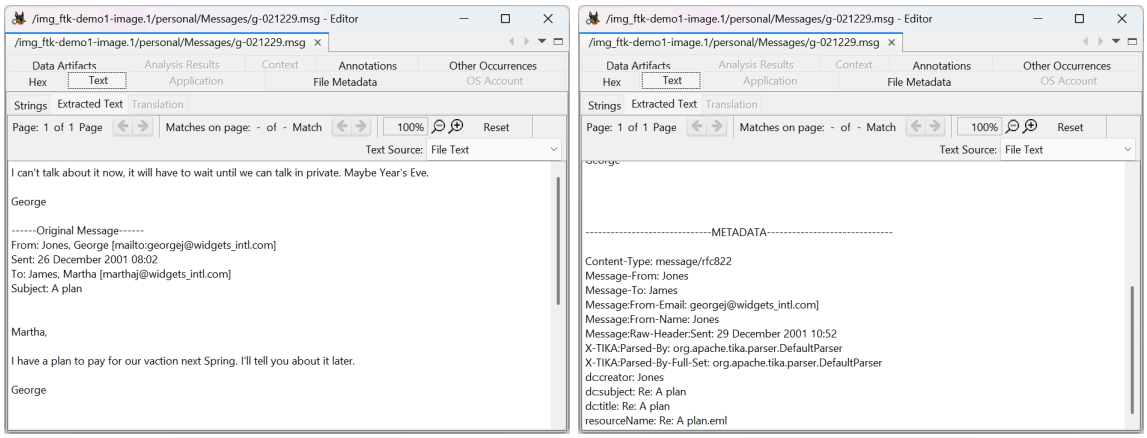
Metadata:

----------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
dc:creator: James
dc:subject: RE:A plan
dc:title: RE:A plan
resourceName: RE:A plan.eml

I already discovered and analysed this file in the previous investigation.

---

g-021229.msg



File Path: /img_ftk-demo1-image.1/personal/Messages/g-021229.msg

Excerpt:

“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 vaction next Spring. I'll tell you about it later.
George”

Metadata:

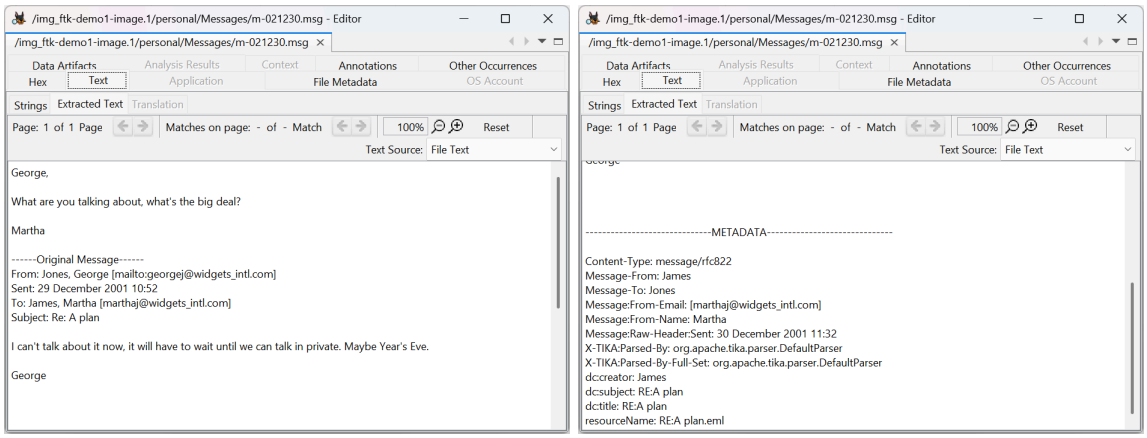
----------METADATA----------
Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message:From-Email: georgej@widgets_intl.com]
Message:From-Name: Jones
Message:Raw-Header:Sent: 29 December 2001 10:52
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
dc:creator: Jones
dc:subject: Re: A plan
dc:title: Re: A plan

resourceName: Re: A plan.eml

I already discovered and analysed this file in the previous investigation.

---

m-021230.msg



File Name: /img_ftk-demo1-image.1/personal/Messages/m-021230.msg

<u>Excerpt:</u>
“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

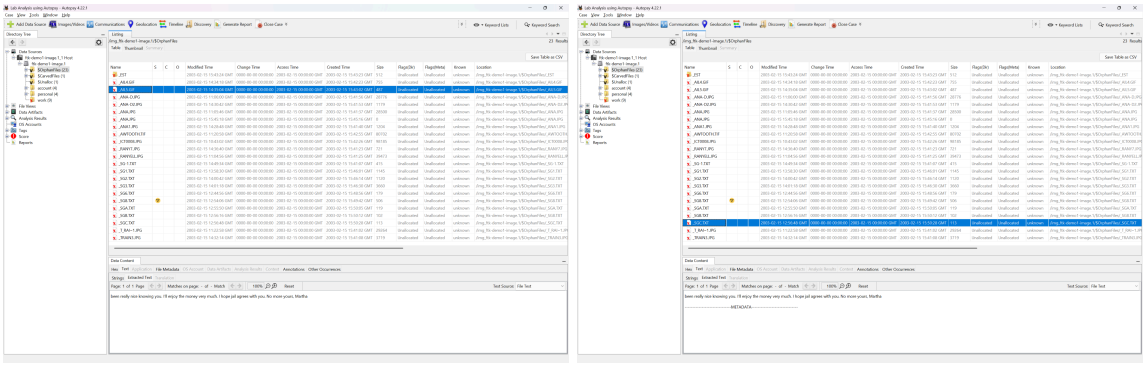
“I can't talk about it now, it will have to wait until we can talk in private. Maybe Year's Eve.
George”

<u>Metadata:</u>
----------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: RE:A plan
dc:title: RE:A plan
resourceName: RE:A plan.eml

I already discovered and analysed this file in the previous investigation.

Evidence #6 Martha betrays George?



Timestamp: 22/10/2025 15:17:11
Full Path:

- /img_ftk-demo1-image.1/$OrphanFiles/_AIL5.GIF
- /img_ftk-demo1-image.1/$OrphanFiles/_SGC.TXT

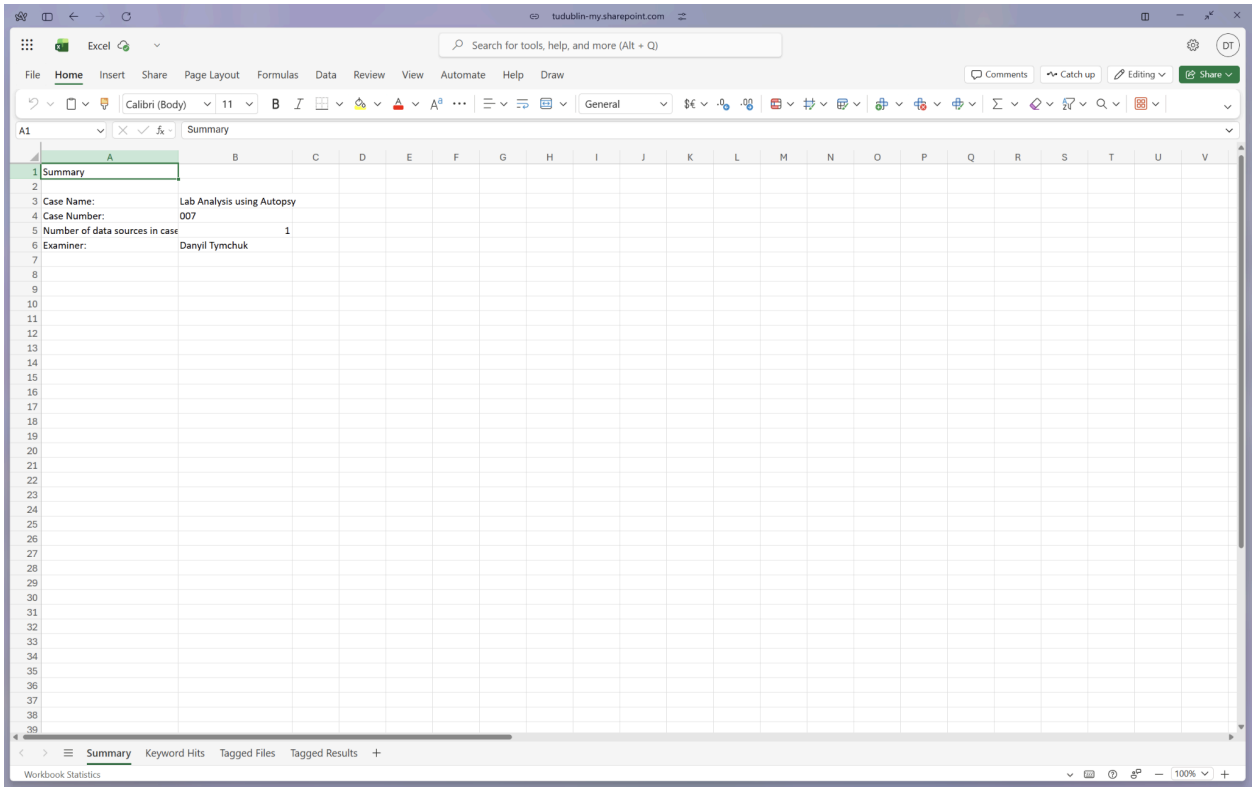
File extension: TXT – Plain Text

Excerpt:
“been really nice knowing you. I'll enjoy the money very much. I hope jail agrees with you. No more yours, Martha”

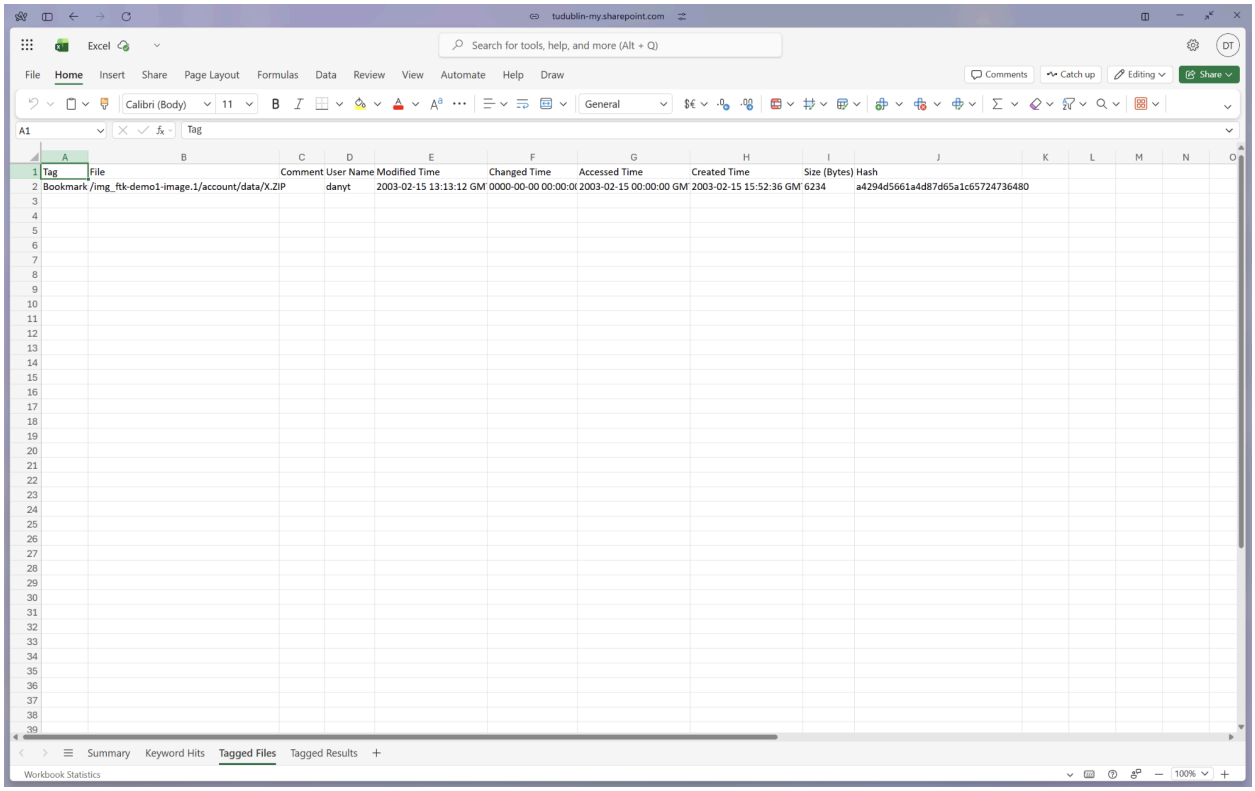
Relevance:
It seems that Martha was with George but betrayed him.

New evidence!

Autopsy Excel Case Report (generated)



	A	B
1	Summary	
2		
3	Case Name:	Lab Analysis using Autopsy
4	Case Number:	007
5	Number of data sources in case	1
6	Examiner:	Danyil Tymchuk



Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Bookmark	/img_ftk-demo1-image.1/account/data/X.ZIP		danyt	2003-02-15 13:13:12 GM	0000-00-00 00:00:0(	2003-02-15 00:00:00 GM	2003-02-15 15:52:36 GM	6234	a4294d5661a4d87d65a1c65724736480

Conclusion

The forensic investigation revealed substantial evidence of financial fraud, encryption concealment, and offshore account management between George Jones and Martha James. Recovered files, deleted communications, and decrypted archives collectively indicate the unauthorized transfer of company funds to Swiss and Isle of Man bank accounts, totaling approximately $3.9 million USD by 2004.

The comparative analysis between FTK and Autopsy confirmed that both forensic tools identified the same core evidence set, establishing consistency and reliability across platforms. Autopsy successfully validated every major artifact discovered in FTK, including the encrypted ZIP archive, the password “couch”, and the Swiss bank files, while also recovering additional carved and unallocated fragments that FTK did not detect.

The new text fragment recovered in Autopsy:
“been really nice knowing you. I'll enjoy the money very much. I hope jail agrees with you. No more yours, Martha”

, provides a significant enhancement to the evidentiary record. This message directly reveals Martha’s intent, confirms her knowledge of the crime, and adds a motive-driven conclusion to the communication trail established in the FTK analysis.

Overall, the results demonstrate that:

- The two tools produce consistent and corroborative findings.
- Autopsy’s carving and unallocated-space recovery capabilities can yield additional evidence missed by FTK.
- The combined use of both tools strengthens the forensic chain of evidence, enhancing the credibility of the investigation and supporting a comprehensive narrative of collusion, concealment, and financial misconduct.

Autopsy’s validation of FTK’s results – along with the discovery of the Martha farewell message – confirms the accuracy of the previous findings and broadens the scope of evidence, delivering a complete and defensible forensic conclusion to the George and Martha case.