

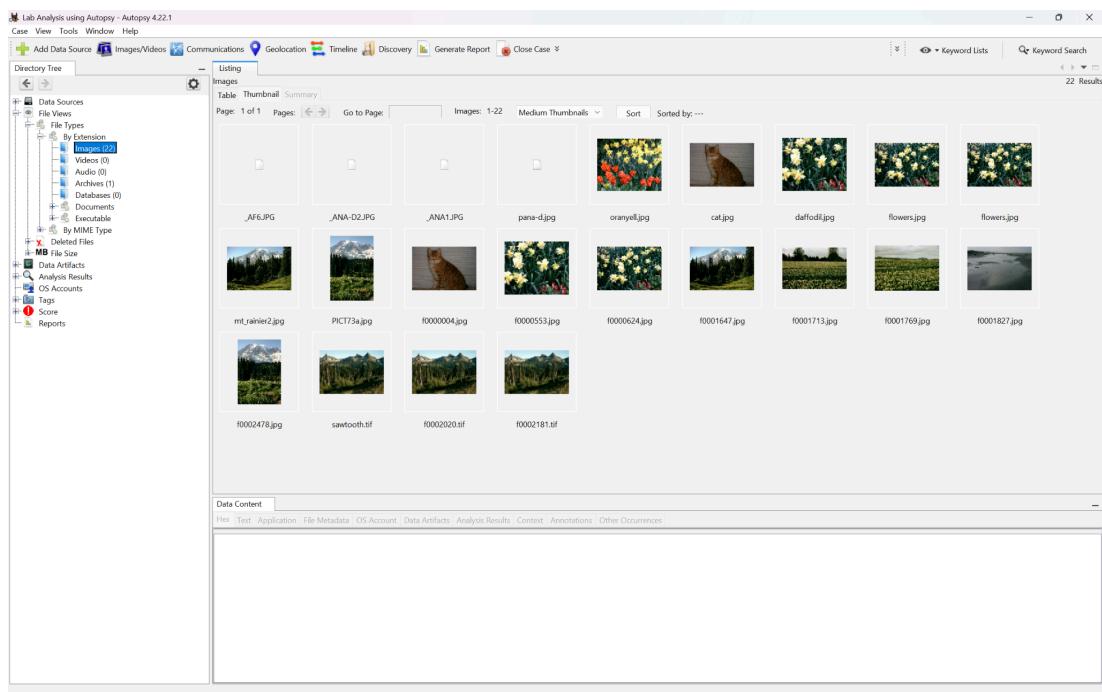
# Computer & Network Forensics

## 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?

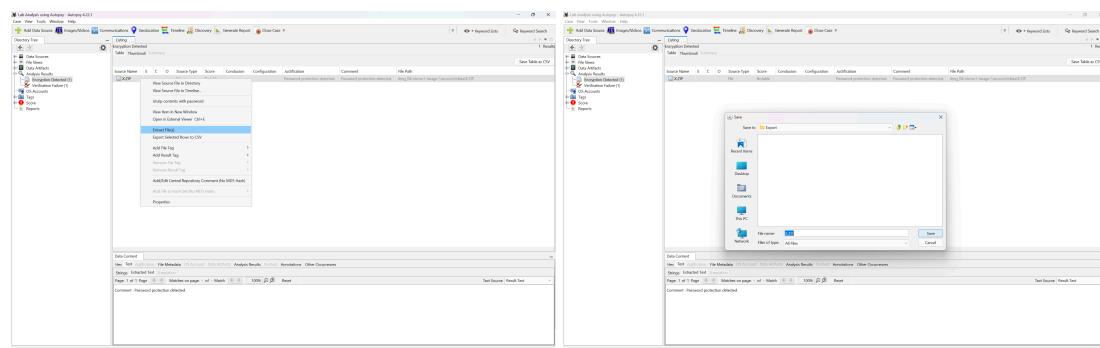
→ **Secret message:**

*"George*

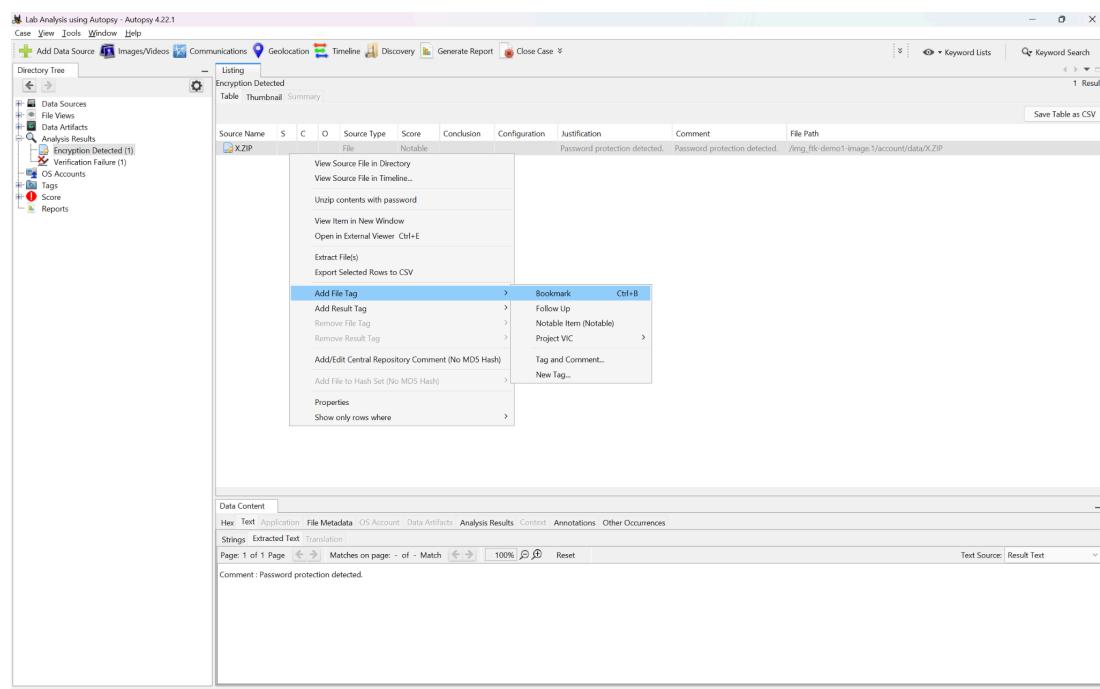
*Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?  
Martha"*

(More info included in the report)

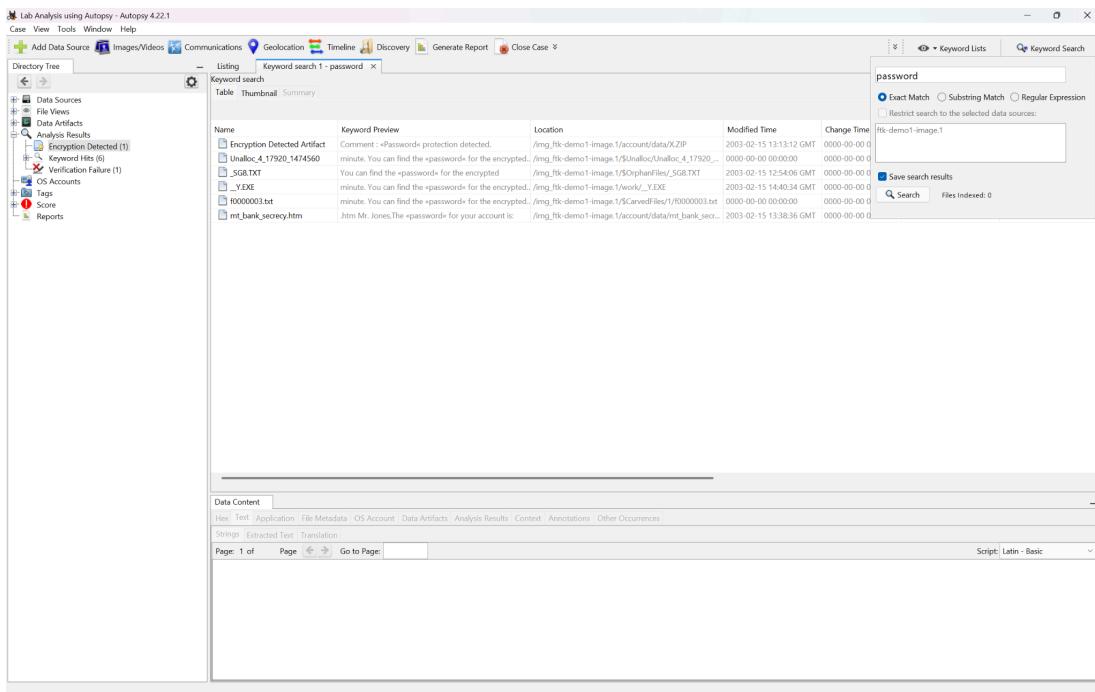
### 3. What happens when I try to unzip the encrypted folder? Screen shot and detail the steps I took.



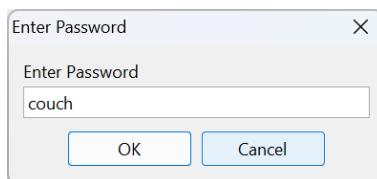
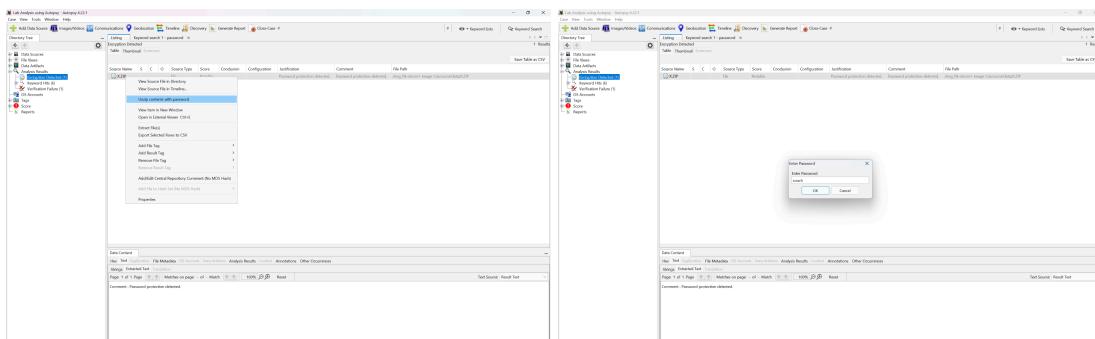
→ Export File



→ Add Bookmark File Tag



→ Keyword Search (“password”)



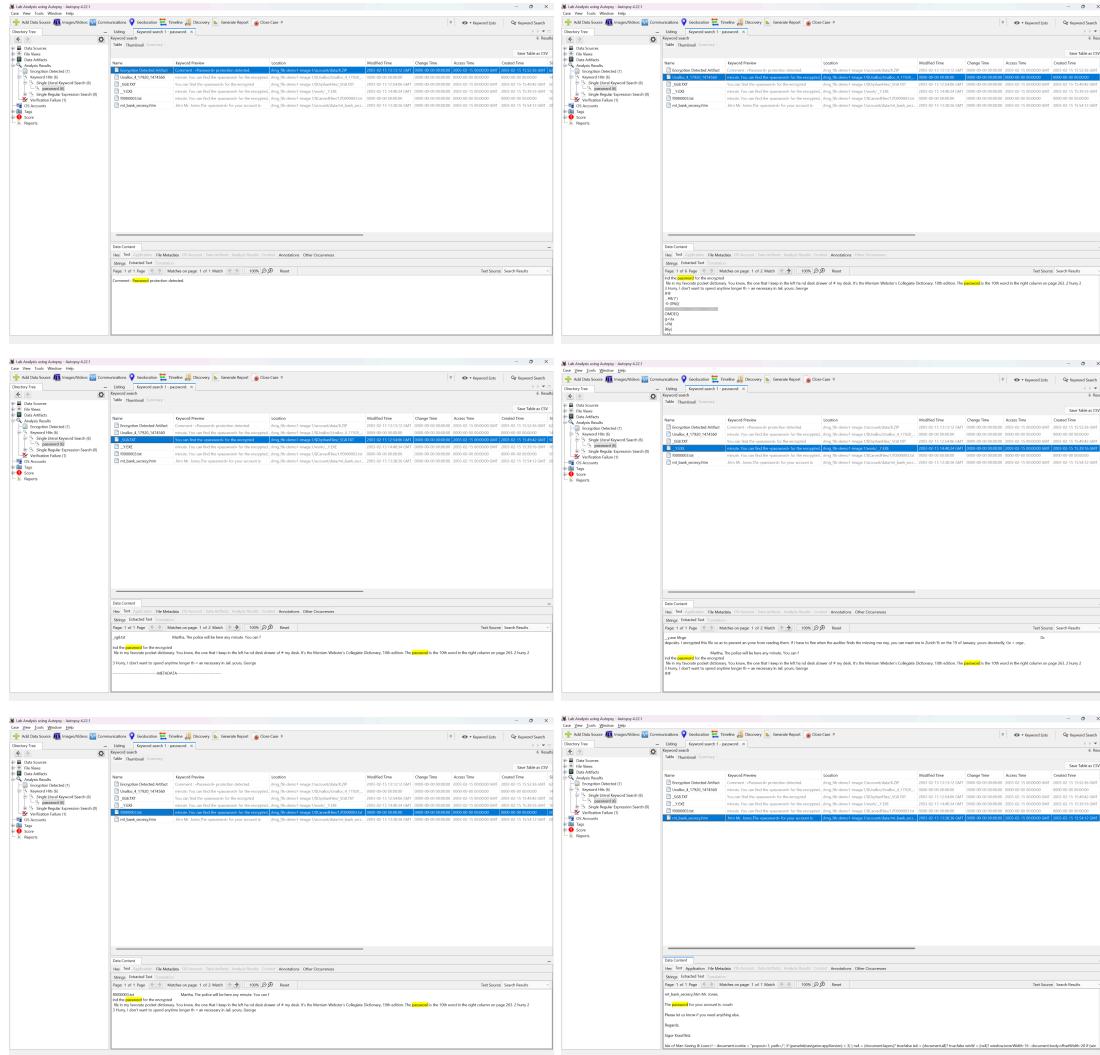
→ Unzip X.ZIP with password (“couch”)

→ 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 form the bank: “... **The password for your account is: couch ...**”

(More info included in the report)



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

Left Window (Content):

```

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
X-TIKA-Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
dcCreator: Jones
dcSubject: A plan
dcTitle: A plan
resourceName: A plan.eml
  
```

Right Window (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
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

Left Window (Content):

```

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
  
```

Right Window (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: 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

Left Window (Content):

```

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
  
```

Right Window (Metadata):

```

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.

# Computer & Network Forensics

## Week 6 (Lab4) – 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 Findings:** Internet Archive ([archive.org](https://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

### **Computer & Network Forensics**

FTK Forensic Analysis Report

    Introduction

    Contents

    Objective

    Evidences from my previous investigation

    Chain of Custody

    Summary of Collected Evidence

    Findings

        Evidence #1 Image Containing Questioning Message

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

        Evidence #3 Encrypted Zip Archive Containing Swiss Bank Records

        Perform Keyword Search ("password")

        Export File & Add Bookmark File Tag

        Evidence #4 Text files

        Evidence #5 Email Correspondence Between George and Martha

        Evidence #6 Martha betrays George?

    Autopsy Excel Case Report (generated)

    Conclusion

## 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
<b>20/10/2025 22:00 – 21/10/2025 01:00</b>	Analysis Period	Danyl Tymchuk
<b>21/10/2025 22:00 – 22/10/2025 01:00</b>	Analysis Period	Danyl Tymchuk
<b>21/10/2025 13:00 – 22/10/2025 16:00</b>	Analysis Period, Case Closure	Danyl Tymchuk

## Summary of Collected Evidence

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

## Findings

### Evidence #1 Image Containing Questioning Message

The screenshot displays the Autopsy 4.22.1 interface. The top navigation bar includes Case, View, Tools, Window, Help, Add Data Source, Communications, Geolocation, Timeline, Discovery, Generate Report, and Close Case. Below the menu is a search bar with Keyword Lists and Keyword Search.

The main area shows a 'Listing' view of files. A sidebar on the left lists various data sources, file types, and artifacts. The 'Images' section shows a grid of thumbnail images, including 'ANA-D2.JPG', 'pana-d.jpg', 'oranye.jpg', 'cat.jpg', 'daffodil.jpg', 'flowers.jpg', 'flowers.jpg', 'f0001827.jpg', 'mt\_rainier2.jpg', 'PICT73a.jpg', 'f000004.jpg', 'f000053.jpg', 'f000062.jpg', 'f0001647.jpg', 'f0001713.jpg', 'f0001769.jpg', 'f0002478.jpg', 'sawtooth.tif', 'f0002020.tif', and 'f0002181.tif'. Below the thumbnails is a detailed hex dump of the file content.

The bottom section contains three windows titled '/img\_ftk-demo1-image.1/work/\_AF6.JPG - Editor'. Each window has tabs for Data Artifacts, Analysis Results, Content, Annotations, and Other Occurrences. The Content tab shows the extracted text: "George...Are yo", "u sure you know", "what are doi", "n't you get caught?", "geous, won't yo", "u get caught?..", "Martha.", and ".....". The bottom right window also shows the file's metadata: Name: /img\_ftk-demo1-image.1/work/\_AF6.JPG, Type: File System, MIME Type: application/octet-stream, Size: 230, and SHA-256: 320551aa1544abacfd1fec432ae1142feef0d4a823ead3c7b3d9649074c.

**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?*

*Martha*

**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"**

The screenshot shows the Autopsy 4.22 interface with a search results table titled 'Keyword search 1 - password'. The table lists six files found in the analysis results. The columns include Name, Keyword Preview, Location, Modified Time, Change Time, Access Time, and Created Time. A 'Save Table as CSV' button is visible at the top right of the table area.

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
Encryption Detected Artifact	Comment : <password> protection detected. /mg_fk-demo1-image.t/account/data/X.ZIP		2003-02-15 13:13:12 GMT	0000-00-00 00:00:00000	2003-02-15 00:00:00000	2003-02-15 15:52:36 GMT	62
Unalloc_4_17920_1474560	minute. You can find the <password> for the encrypted. /mg_fk-demo1-image.t/\$Unalloc/Unalloc_4_17920_...		0000-00-00 00:00:00000	0000-00-00 00:00:00000	0000-00-00 00:00:00000	0000-00-00 00:00:00000	14
_SG8.TXT	You can find the <password> for the encrypted. /mg_fk-demo1-image.t/\$OrphanFiles/_SG8.TXT		2003-02-15 12:54:06 GMT	0000-00-00 00:00:00000	2003-02-15 00:00:00000	2003-02-15 15:49:42 GMT	50
__Y.EXE	minute. You can find the <password> for the encrypted. /mg_fk-demo1-image.t/WorkZ__Y.EXE		2003-02-15 14:40:34 GMT	0000-00-00 00:00:00000	2003-02-15 00:00:00000	2003-02-15 15:38:16 GMT	16
f0000003.txt	minute. You can find the <password> for the encrypted. /mg_fk-demo1-image.t/\$CarvedFiles/1/f0000003.txt		0000-00-00 00:00:00000	0000-00-00 00:00:00000	0000-00-00 00:00:00000	0000-00-00 00:00:00000	50
mt_bank_secrecy.htm	htm Mr. Jones. The <password> for your account is: /mg_fk-demo1-image.t/account/data/mt_bank_secre...		2003-02-15 13:38:36 GMT	0000-00-00 00:00:00000	2003-02-15 00:00:00000	2003-02-15 15:54:12 GMT	28

**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

The screenshot shows the 'Analysis Results' section of the Autopsy tool. The left sidebar lists categories like 'Data Sources', 'File Views', 'Data Artifacts', and 'Analysis Results'. Under 'Analysis Results', there is a single entry: 'Encryption Detected (1)'. This entry has a sub-node 'Single Literal Keyword Search (6)' which further branches into 'password' (6) and 'Single Regular Expression Search (0)'. A red 'X' icon next to 'Verification Failure (1)' indicates an error. The main pane displays a table of results:

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
Encryption Detected Artifact	Comment : <password> protection detected.	/img_ftk-demo1-image.1/account/data/X.ZIP	2003-02-15 13:13:12 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:52:36 GMT	5
Unalloc_4_17920.1474560	minute. You can find the <password> for the encrypted, /img_ftk-demo1-image.1/Unalloc/Unalloc_4_17920...		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14
_SGB.TXT	You can find the <password> for the encrypted, /img_ftk-demo1-image.1/SOphareFiles/_SGB.TXT		2003-02-15 12:54:06 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:49:42 GMT	5C
_Y_EXE	minute. You can find the <password> for the encrypted, /img_ftk-demo1-image.1/Work/_Y_EXE		2003-02-15 14:40:34 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:38:16 GMT	16
00000003.txt	minute. You can find the <password> for the encrypted, /img_ftk-demo1-image.1/Scavved/files/1/00000003.txt		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5C
mt_bank_secrey.htm	Htm Mr. Jones,The <password> for your account is: /img_ftk-demo1-image.1/account/data/mt_bank_sec...		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	28

Below the table, the 'Data Content' tab is selected, showing the following details:

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

Text content:  
Comment : Password protection detected.

**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.”*

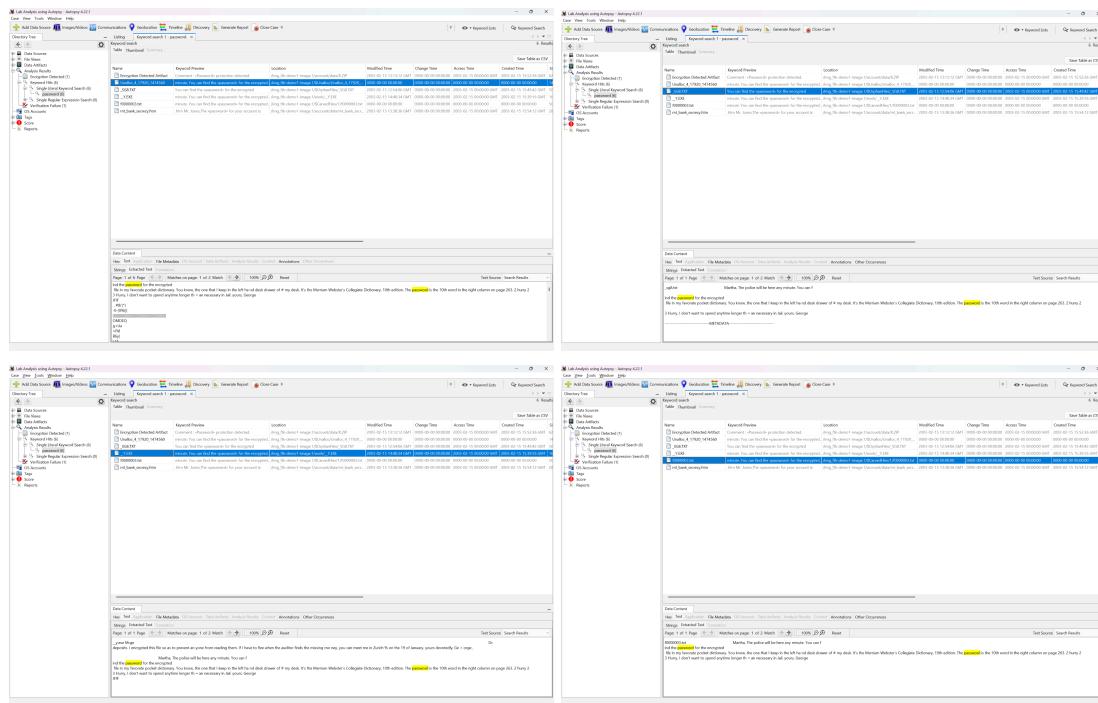
**Description & Analysis:**

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.

**co-tan-gent** \('kō-tān-jənt, 'kō-tān-jənt\} [NL *cotangētus, cotangēns*, fr. co- + *tangētus, tangēns* 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  $\cot \theta$  that is equal to the cosine divided by the sine for all real numbers  $\theta$  for which the sine is not equal to zero and is exactly equal to the cotangent of an angle of measure  $\theta$  in radians **'cote** \('kōt\}, 'kāt\} n [ME, fr. OE] (bef. 12c) **1** *dial Eng* : *'cot* **2** : a shed or coop for small domestic animals and esp. pigeons **'cote** \('kōt\} vt [prob. fr. MF *cotoyer*] (1555) *obs.* : to pass by **cote-rie** \('kō-tē-ri\} n [Fr, 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** \('kō-tēr-mē-nəs\} adj [alter. of *conterminous*] (1799) **1** : having the same or coincident boundaries ( $\sim$  the years of his father —Elizabeth Hardwick) **2** : coextensive in scope or duration (an experience of life  $\sim$  with the years of his father —Elizabeth Hardwick) **co-ter-mi-nously** adv **co-thur-nus** \('kō-thor-nōs\} n, pl -ni \(-nī, -(-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* \('kō-thūrn, kō-\} **2** : the dignified somewhat stilted style of ancient tragedy **co-tid-al** \('kō-tēdāl\} adj (1833) : indicating equality in the tides or a coincidence in the time of high or low tide **co-till-ion** \('kō-tēl-yān, kā-\} also **co-till-on** \('kō-tēl-yān, kā-\} 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** \('kō-tō-nē-as-tər, 'kā-tō-nē-as-tər\} 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** \('kāt-,kwen\} n [*cot* + *quean*] (1547) **1** *archaic* : a coarse masculine woman **2** *archaic* : a man who busies himself with women's work or affairs **Cots-wold** \('kāt-,swōld, -swōld\} n [*Cotswold* Hills, England] (ca. 1658) : any of an English breed of large long-haired sheep **cot-ta** \('kā-tā\} n [ML, of Gmc origin; akin to OHG *kozza* coarse mantle —more at *COAT*] (1848) : a waist-length surplice **cot-tage** \('kā-tij\} n [ME *cottage*, fr. (assumed) AF, fr. ME *cot* — more at *COT*] (14c) **1** : the dwelling of a farm laborer or small farmer **2** : a small frame and family home

**cot-ton-tail** \('kā-tēn-täl\} 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** \('kā-tēnd\} n (1562) : any of various weedy plants (as cudweed) with hoary pubescence or cottony seeds **cot-ton-wood** \('kā-tēdū\} 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** \('kā-tēn-ē\} adj (1578) : resembling cotton in appearance or character: as **a** : covered with hairs or pubescence **b** : soft **cot-tony-cush-ion scale** \('kā-tēn-ē-shūn\} n (1886) : a scale insect (*Iceyra purchasi*) introduced into the U.S. from Australia that infests citrus and other plants **cot-y-lon** *n comb form [cotyledon]*: cotyledon (*hypocotyl*) **cot-y-le-don** \('kā-tē-lē-dōn\} n [NL, fr. Gk *kotylédon* cup-shaped hollow, fr. *kontakte* cup, anything hollow] (1540) **1** : a lobe 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** \('kā-tē-lē-dō-nērē\} adj **co-ty-lo-saur** \('kā-tē-'lō-sōr, kā-'tē-lō-sōr\} 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 **couch** \('kōuch\} vb [ME, fr. MF *coucher*, fr. L *collocare* to set in place — more at COLLOCATE] vt (14c) **1** **a** : 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 specific manner (the memorandum was  $\sim$ ed in strong language —W. L. Shirer) **5** : to treat (a cataract) by displacing the lens of the eye into the vitreous humor  $\sim$  vi **1** : to lie down or recline for sleep or rest **2** : to lie in ambush **couch** 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** \('kōuch-ānt\} adj [ME, fr. MF, fr. prp. of *coucher*] (15c) : lying down esp. with the head up (a heraldic lion  $\sim$ )

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*

The image shows two side-by-side windows of the 'Lab Analysis using Analyst's Notebook' application. Both windows have a title bar 'Lab Analysis using Analyst's Notebook - Summary 6.0.2' and a menu bar with 'File', 'Edit', 'Tools', 'Application', 'File Manager', 'File Browser', 'Analysis Results', 'Annotations', 'Other Occurrences'. The left window displays a 'Discovery Tree' on the left with nodes like 'Data Sources', 'Data Artifacts', 'Data Artifacts (Detected)', 'Data Artifacts (Unverified)', 'Data Artifacts (Unknown)', 'Data Artifacts (Rejected)', 'Data Artifacts (Deleted)', 'Data Artifacts (Archived)', 'Data Artifacts (Pending)', 'Data Artifacts (New)', and 'Reports'. The main pane shows a table titled 'User Table w/ CDF' with columns: Name, Keyword Profile, Location, Modified Time, Change Time, Access Time, Created Time. One row is selected: 'Couch - password protected content' located at 'drag\_be-device-image\Unzipper\Bank.X.ZIP' with modified time '2020-01-11 11:12:12' and access time '2020-01-11 11:12:12'. The right window also has a 'Discovery Tree' and a table titled 'User Table w/ CDF' with similar data for the same file.

Name	Keyword Profile	Location	Modified Time	Change Time	Access Time	Created Time
Couch - password protected content	Couch - password protected content	drag_be-device-image\Unzipper\Bank.X.ZIP	2020-01-11 11:12:12	2020-01-11 11:12:08	2020-01-11 11:12:12	2020-01-11 11:12:12

**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”)

The screenshot shows the Autopsy 4.22.1 interface. In the top navigation bar, the 'Case' tab is selected. Below the menu, there are tabs for 'Add Data Source', 'Images/Videos', 'Communications', 'Geolocation', 'Timeline', 'Discovery', 'Generate Report', and 'Close Case'. The 'Discovery' tab is currently active. A search bar at the top right contains the text 'password' with options for 'Exact Match', 'Substring Match', and 'Regular Expression'. Below the search bar, a checkbox 'Restrict search to the selected data sources.' is checked. The main pane displays a table of 'Keyword Hits (6)'. The table has columns for 'Name', 'Keyword Preview', 'Location', 'Modified Time', and 'Change Time'. One entry in the table is:

Name	Keyword Preview	Location	Modified Time	Change Time
Encryption Detected Artifact	Comment : <Password> protection detected.	/mg_fk-demo1-image/1/account/data/X.ZIP	2003-02-15 11:13:12 GMT	0000-00-00 00:00:00
Unalloc_4_17920_1474560	minute. You can find the <password> for the encrypted., /mg_fk-demo1-image/1/\$halo/Unalloc_4_17920_...	/mg_fk-demo1-image/1/\$halo/Unalloc_4_17920_...	0000-00-00 00:00:00	0000-00-00 00:00:00
_SGB.TXT	You can find the <password> for the encrypted., /mg_fk-demo1-image/1/0/pharFile/_SGB.TXT	/mg_fk-demo1-image/1/0/pharFile/_SGB.TXT	2003-02-15 12:54:06 GMT	0000-00-00 00:00:00
_Y.EXE	minute. You can find the <password> for the encrypted., /mg_fk-demo1-image/1/wolv/_Y.EXE	/mg_fk-demo1-image/1/wolv/_Y.EXE	2003-02-15 14:40:34 GMT	0000-00-00 00:00:00
00000003.txt	minute. You can find the <password> for the encrypted., /mg_fk-demo1-image/1/\$carvedFiles/1/00000003.txt	/mg_fk-demo1-image/1/\$carvedFiles/1/00000003.txt	0000-00-00 00:00:00	0000-00-00 00:00:00
mt_bank_secrey.htm	htm Mr. Jones,The <password> for your account is: /mg_fk-demo1-image/1/account/data/mt_bank_secr...	/mg_fk-demo1-image/1/account/data/mt_bank_secr...	2003-02-15 13:38:36 GMT	0000-00-00 00:00:00

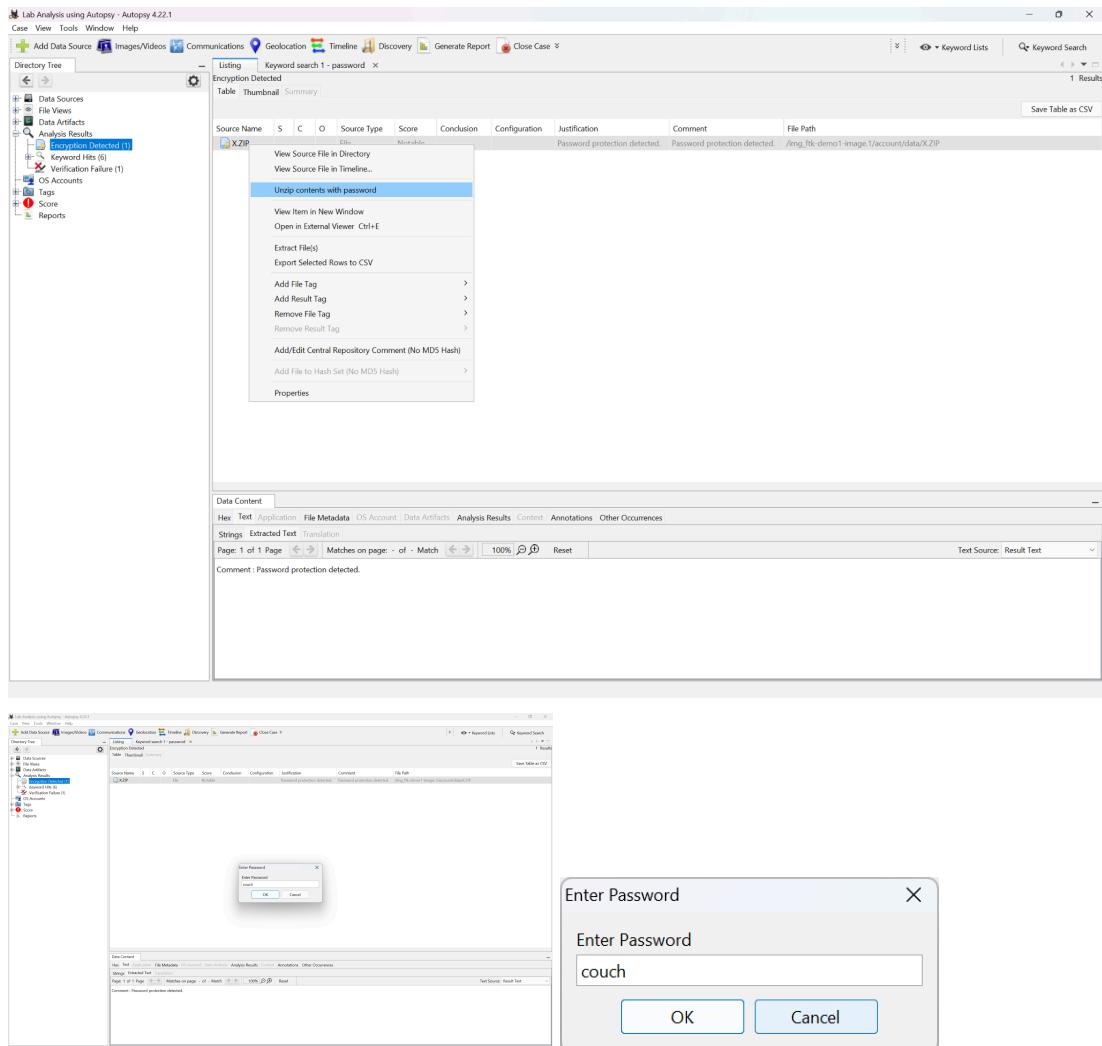
At the bottom of the search results pane, there are buttons for 'Save search results', 'Search' (disabled), and 'Files Indexed: 0'.

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

### Export File & Add Bookmark File Tag

The three screenshots show the Autopsy interface during the process of exporting a file and adding it to a bookmark. The first screenshot shows the 'File Artifacts' tab with a file selected. The second screenshot shows the 'File Artifacts' tab with the file now listed under 'Selected Artifacts'. The third screenshot shows the 'File Artifacts' tab with the file added to a 'Bookmark'.

## 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

The screenshot shows the Autopsy 4.22.1 interface with the following details:

- File Tree:** Shows a directory structure with 'Data Sources', 'File Views', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', and 'Reports'. 'Analysis Results' contains 'Keywords Detected (1)', 'Keyword Hits (0)', 'Verification Failure (1)', and 'OS Accounts'.
- Metadata Table:** Shows the following data for 'SWISS.XLS':

Source Name	S	C	O	Description	Owner	Data Source	Date Created	Date Modified	User ID	Program Name	Organization
OF m-021220.mg				RE-A plan	James	ftk-demo1-image.1					
OF g-021229.mg				Re-A plan	Jones	ftk-demo1-image.1					
OF g-021218.mg				A plan	Jones	ftk-demo1-image.1					
OF m-021230.mg				RE-A plan	James	ftk-demo1-image.1					
SWISS.XLS					Bill Nelson	ftk-demo1-image.1	2002-08-16 21:39:27 IST	2002-08-16 22:38:14 IST	pc	Microsoft Excel	The Boeing Company
- Data Content:** Shows the file's content as a Microsoft Excel spreadsheet. The preview shows bank statements for Swiss Geneva Internationale, account number 98821110, dated February 14, 2002, listing various transactions and a balance of 1524.0.

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

The screenshot shows the Autopsy 4.22.1 interface with the 'Case' tab selected. The main pane displays a table of file analysis results. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and location. The table lists various files such as msg7.txt, msg5.txt, msg3.txt, msg1.txt, AILS.GIF, 10000001.txt, 10000002.txt, 1000052.txt, 10001401.txt, 10002101.txt, 1000222.txt, 1000228.txt, 1000273.txt, and SWISS.TXT. The location column indicates their paths within the image file. The bottom section of the interface shows a 'Data Content' pane with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

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-image1/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 15:48:31 GMT	316	Unallocated	Unallocated	unknown	/img_ft-demo1-image1/personal/Message/msg5.txt
X msg3.txt				2003-02-15 12:43:30 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:47:18 GMT	453	Unallocated	Unallocated	unknown	/img_ft-demo1-image1/work/msg3.txt
X msg1.txt				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-image1/Sophomore_ES7/AIIS.GIF
✓ 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-image1/CarvedFiles/10000001.txt
✓ 10000002.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-image1/CarvedFiles/10000002.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-image1/CarvedFiles/1000052.txt
✓ 10001401.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-image1/CarvedFiles/10001401.txt
✓ 10002101.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-image1/CarvedFiles/10002101.txt
✓ 1000222.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	369	Unallocated	Unallocated	unknown	/img_ft-demo1-image1/CarvedFiles/1000222.txt
✓ 1000228.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-image1/CarvedFiles/1000228.txt
✓ 1000273.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-image1/CarvedFiles/1000273.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	2429	Allocated	Allocated	unknown	/img_ft-demo1-image1/account/data/ZIP/SWISS..
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					

**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

The image shows two side-by-side FTK Editor windows. Both windows have a title bar with the path '/img\_ftk-demo1-image.1/personal/Messages/msg7.txt - Editor' and '/img\_ftk-demo1-image.1/\$CarvedFiles/1/f0000001.txt - Editor'. The left window has tabs for Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences, with 'Text' selected. The right window has similar tabs. Both windows show a 'Strings' tab with search filters like 'Page: 1 of 1 Page', 'Matches on page: - of - Match', and '100%'. Below the tabs is a text area with the following content:

Mrge Dr.  
deposits. I encrypted this file so as to prevent anyone from reading them. If I have to flee when the auditor finds th e missing mo ney, you can meet me in Zurich % on the 19 of January. yours devotedly, Ge + orge ,  
-----METADATA-----

The right window shows the same text with minor differences in line breaks.

Excerpt:

*“...I encrypted this file so as to prevent anyone 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

The image shows two side-by-side FTK Editor windows. Both windows have a title bar with the path '/img\_ftk-demo1-image.1/personal/Messages/msg5.txt - Editor' and '/img\_ftk-demo1-image.1/\$CarvedFiles/1/f0002737.txt - Editor'. The left window has tabs for Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences, with 'Text' selected. The right window has similar tabs. Both windows show a 'Strings' tab with search filters like 'Page: 1 of 1 Page', 'Matches on page: - of - Match', and '100%'. Below the tabs is a text area with the following content:

ear Mart ,  
I've got a plan to get more cash. It involves rerouting invoices here at work to the field offices. It will take six month s to get back here and we can be in Brazil enjoying the fruits of our labo  
-----METADATA-----

The right window shows the same text with minor differences in line breaks.

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

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

Excerpt:

*“Dear Martha, Here it is June I have almost deposited a million dollars. If 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

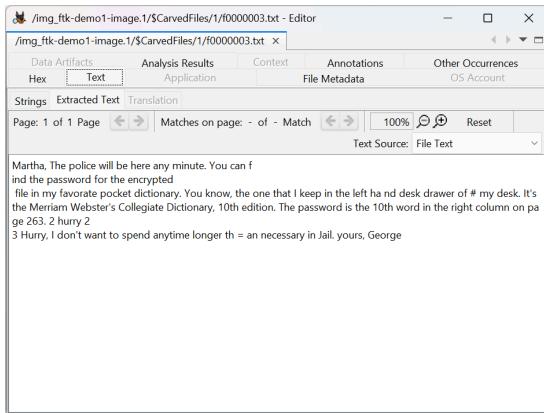
-----  
METADATA-----  
-----

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



The screenshot shows the FTK Editor interface with the title bar "/img\_ftk-demo1-image.1/\$CarvedFiles/1/f0000003.txt - Editor". The "Text" tab is selected. The main pane displays the following text:

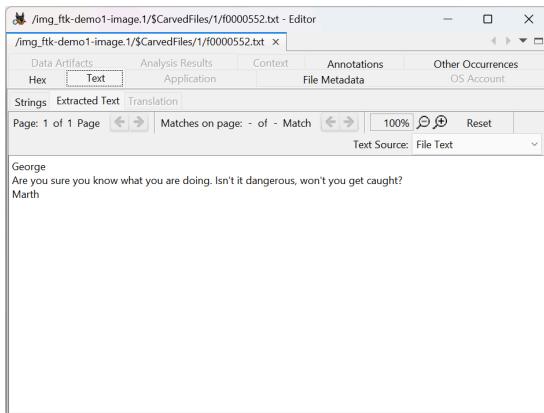
```
Martha. The police will be here any minute. You can find the password for the
ind the password for the encrypted
file in my favorite pocket dictionary. You know, the one that I keep in the left ha nd desk drawer of # my desk. It's the Merriam Webster's Collegiate Dictionary,
10th edition. The password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

Excerpt:

*"Martha, The police will be here any minute. You can find the password for the encrypted file in my favorite 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



The screenshot shows the FTK Editor interface with the title bar "/img\_ftk-demo1-image.1/\$CarvedFiles/1/f0000552.txt - Editor". The "Text" tab is selected. The main pane displays the following text:

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

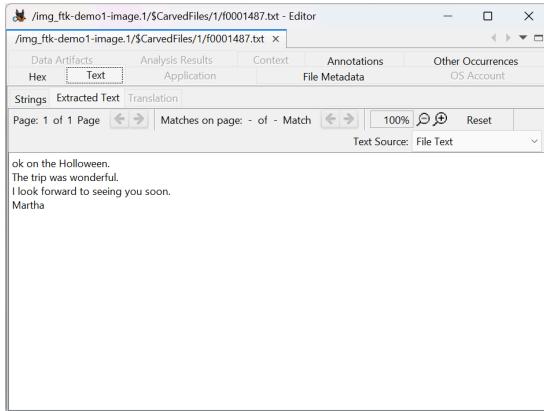
Excerpt:

*"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



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

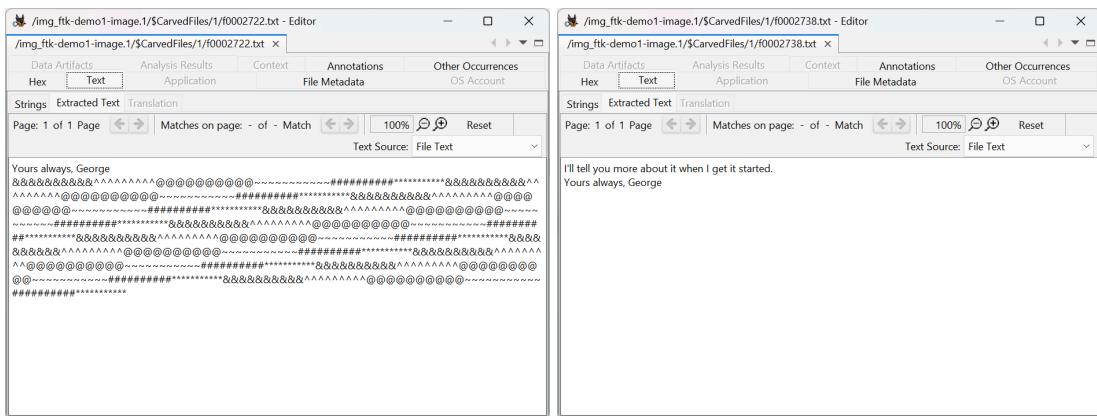
**Excerpt:**

*"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



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

**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

The screenshot shows the FTK Editor interface with the file '/img\_ftk-demo1-image.1/\$CarvedFiles/1/f0002728.txt' open. The 'Text' tab is selected. The extracted text content is as follows:

```
+++++)))))((((((^A^A^A@#####RRRRRRRRRIdhaljaldfkj;ikadfartha. The auditor discovered the embezzlement and the police are on the 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...
```

#### Excerpt:

*“...The auditor discovered the embezzlement and the police are on the 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

The screenshot shows the FTK Editor interface with the file '/img\_ftk-demo1-image.1/account/data/X.ZIP/SWISS.TXT' open. The 'Text' tab is selected. The extracted text content is as follows:

```
Geneve Internationale
Autres liens

Account Number: 9882111
Les montants ont ,num,r, en des dollars des Etats-Unis

Quantit, de d.p*t Argent Total Courant "Int,r,t gagn, ... 6,533 pour cen
t"
Date de d.p*t
"1,524.00" "$1,623.56" $99.56 "Janvier 29, 2002"
"15,888.00" "$18,655.59" "$10,037.96" "Fvrier 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 "A
```

#### Excerpt:

*“Geneve Internationale  
Autres liens*

*Account Number: 9882111*

*”*

*Bank Statements*

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

---

## CSV text files

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar contains a 'Directory Tree' with categories like Data Sources, File Types, File Views, Deleted Files, MB File Size, Data Artifacts, Analysis Results, OS Accounts, Tags, Score, and Reports. Under 'File Types', 'text' is expanded, showing 'plain (14)', 'csv (1)', and 'html (3)'. The main pane displays a table titled 'Listing' for 'text/csv' files. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), Known, and Location. One row is shown: SWISS.CSV, with values: S (1), O (1), Modified Time (2003-02-15 10:46:40 GMT), Change Time (0000-00-00 00:00:00), Access Time (0000-00-00 00:00:00), Created Time (0000-00-00 00:00:00), Size (2429), Flags(Dr) (Allocated), Flags(Meta) (Allocated), Known (unknown), and Location (/img\_fbk-demo1-image.1/account/data/X.ZIP/SWISS...\_27b8b95c40). A 'Save Table as CSV' button is at the top right of the table area. Below the table is a 'Data Content' section with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Content, Annotations, and Other Occurrences.

**Timestamp:** 22/10/2025 00:50:03

**File extension:** CSV – Comma-Separated Values

---



## HTML text files

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar contains a 'File Views' section with 'File Types' expanded, showing categories like 'By Extension', 'By MIME Type', 'application', 'image', 'message', and 'text'. Under 'text', 'plain (14)' is selected. The main pane displays a table of files found in the analysis case:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
mt_bank.htm				2003-02-15 12:35:10 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:53:21 GMT	1881	Unallocated	Unallocated	unknown	/img_hk-demo1-image.1/account/mt_bank
mt_bank_secrey.htm		2		2003-02-15 12:38:36 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_hk-demo1-image.1/account/data/mt
10001705_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_hk-demo1-image.1\$CarvedFiles/1/0

Below the table, a 'Data Content' section is visible with tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Content', 'Annotations', and 'Other Occurrences'. The 'Text' tab is selected.

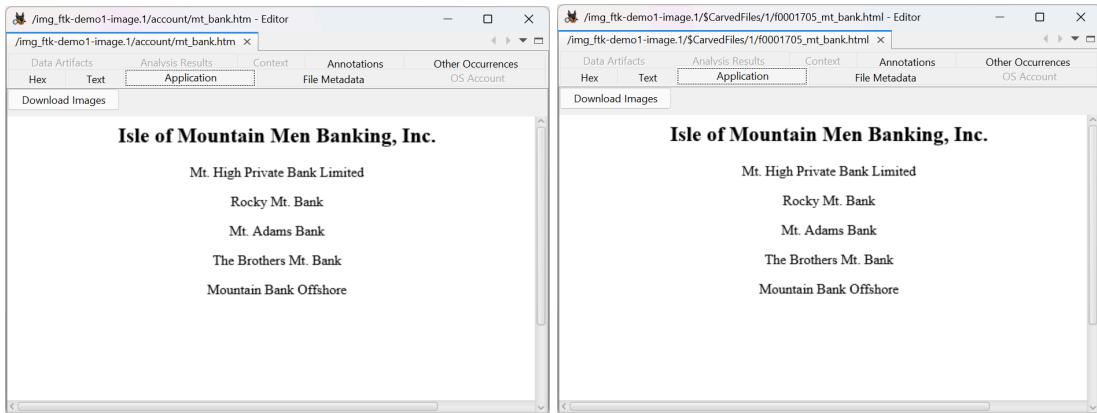
**Timestamp:** 22/10/2025 00:56:19

**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*

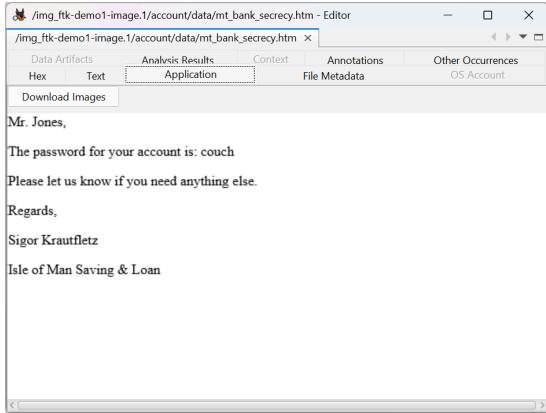
*The Brothers Mt. Bank*

*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

The screenshot shows the Autopsy 4.22.1 interface with the following details:

- Case:** Lab Analysis using Autopsy - Autopsy 4.22.1
- File Views:** Directory Tree, Listing, Table, Thumbnail, Summary (selected)
- Table View:** Shows a list of files found in the directory /rfc822:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
m-021230.msg	z	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/rfk-demo1-image/1/personal/Messages/m-021...
g-021218.msg	z	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/rfk-demo1-image/1/personal/Messages/g-021...
g-021229.msg	z	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/rfk-demo1-image/1/personal/Messages/g-021...
m-021220.msg	z	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/rfk-demo1-image/1/personal/Messages/m-021...
- Data Content:** Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Content, Annotations, Other Occurrences.
- Page:** 1 of [Page] Go to Page: [Input]
- Script:** Latin - Basic

**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

The image displays two side-by-side windows of the FTK (Forensic Toolkit) software interface, both titled "/img\_ftk-demo1-image.1/personal/Messages/g-021218.msg - Editor".  
The left window shows the raw text content of the email message. It contains two messages:  
Martha:  
I have a plan to pay for our vaction next Spring. I'll tell you about it later.  
George:  
-----  
The right window shows the detailed metadata extracted from the file. The metadata includes:  
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

**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*

The image displays two windows of the FTK (Forensic Toolkit) software. Both windows have the title bar '/img\_ftk-demo1-image.1/personal/Messages/m-021220.msg - Editor'.  
The left window shows the raw text content of the email:  
George,  
What kind of plan do you have to get the money for the mountain vacation you want so badly?  
Martha  
-----  
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 shows the extracted metadata fields:  
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

**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*

The image displays two side-by-side windows of the FTK Editor application. Both windows have a title bar: '/img\_ftk-demo1-image.1/personal/Messages/g-021229.msg - Editor'. The left window shows the raw text of an email message. The text includes a greeting from George, a message from Jones, a response from Martha, and a closing from George. The right window shows the extracted metadata for the same file. The metadata includes standard headers like Content-Type, Message-From, and Message-To, along with specific fields such as X-TIKA-Parsed-By, dc:creator, dc:subject, dc:title, and resourceName.

**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](mailto:georgej@widgets_intl.com)]  
Sent: 26 December 2001 08:02  
To: James, Martha [[marthaj@widgets\\_intl.com](mailto:marthaj@widgets_intl.com)]  
Subject: A plan

*"Martha,*

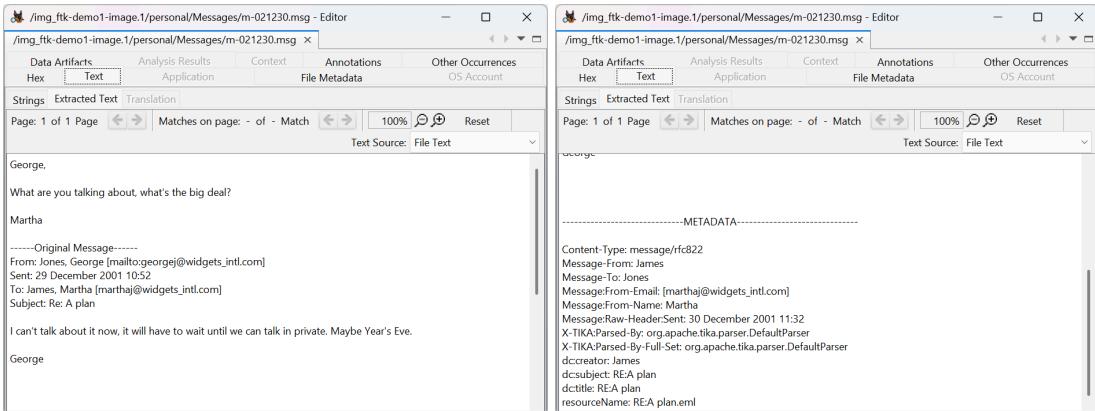
*I have a plan to pay for our vaction next Spring. I'll tell you about it later.  
George"*

### Metadata:

-----METADATA-----  
Content-Type: message/rfc822  
Message-From: Jones  
Message-To: James  
Message:From-Email: [georgej@widgets\\_intl.com](mailto: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

### Excerpt:

“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”

### 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: 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?

The screenshot shows two side-by-side tables from the Lab Analytics tool. Both tables have columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags/CD, Reprofomed, Known, and Location.

**AIL5.GIF Results:**

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags/CD	Reprofomed	Known	Location
AIL5.GIF			2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	700	Unmodified	Unknown	Zeng_Hu_Device_Images\OrphanFiles\AIL5.GIF	
AIL5.GIF			2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	700	Unmodified	Unknown	Zeng_Hu_Device_Images\OrphanFiles\AIL5.GIF	

**SGC.TXT Results:**

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags/CD	Reprofomed	Known	Location
SGC.TXT			2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	1024	Unmodified	Unknown	Zeng_Hu_Device_Images\OrphanFiles\SGC.TXT	
SGC.TXT			2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	2023-01-11 16:18:00.000000000	1024	Unmodified	Unknown	Zeng_Hu_Device_Images\OrphanFiles\SGC.TXT	

**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)

This screenshot shows the 'Summary' sheet of an Excel spreadsheet. The data is as follows:

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

This screenshot shows the 'Tag' sheet of an Excel spreadsheet. The data is as follows:

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