

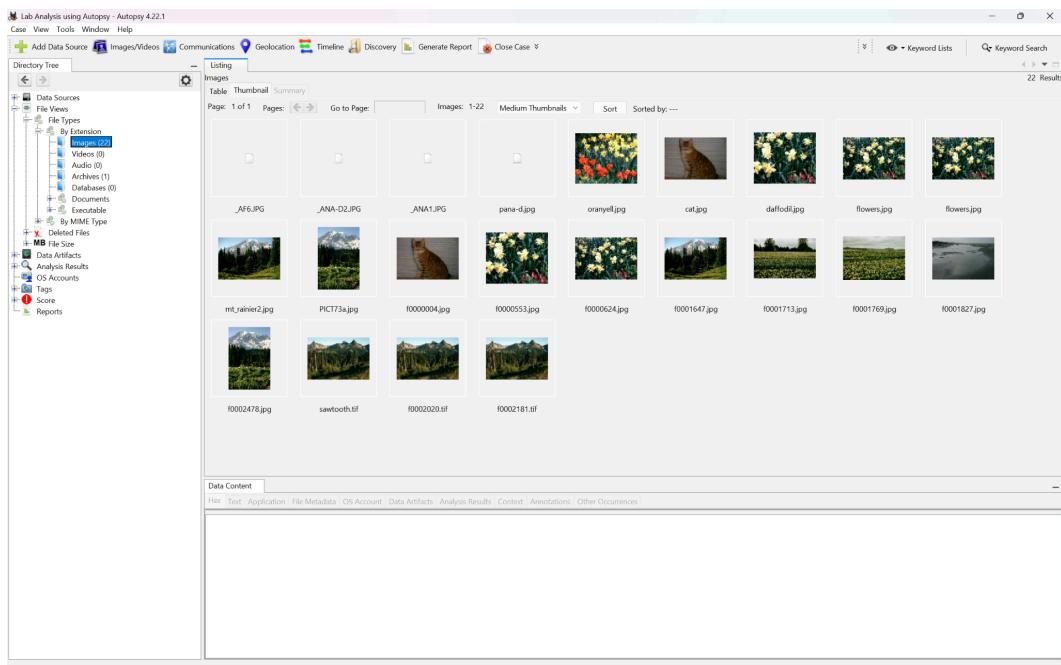
Computer & Network Forensics

Lab 4

Forensics Analysis using Autopsy

Questions

1. How many images are viewable in thumbnail mode?



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

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

Autopsy Analysis Results:

The Autopsy interface shows a list of files under the 'Images' tab. One file, '_AF6.JPG', has a context menu open. The menu includes options like 'View File in Directory', 'View File in Timeline...', 'Open in External Viewer Ctrl+E', 'Extract File(s)', 'Export Selected Rows to CSV', 'Add File Tag', 'Remove File Tag', and 'Properties'. Other files listed include ANA1.JPG, pana-djng, orangell.jpg, cat.jpg, daffodil.jpg, flowers.jpg, flowers.jpg, mnt_rainier, f0000004.jpg, f000053.jpg, f0000624.jpg, f0001647.jpg, f0001713.jpg, f0001769.jpg, f0001827.jpg, f0002478.jpg, sawooth.tif, f0002020.tif, and f0002181.tif.

File Content:

Three FTK Editor windows show the content of the file _AF6.JPG. The first window shows the raw hex dump of the file. The second window shows the extracted text, which contains the following message:

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

The third window shows the file metadata, including the file name, type, size, and creation date.

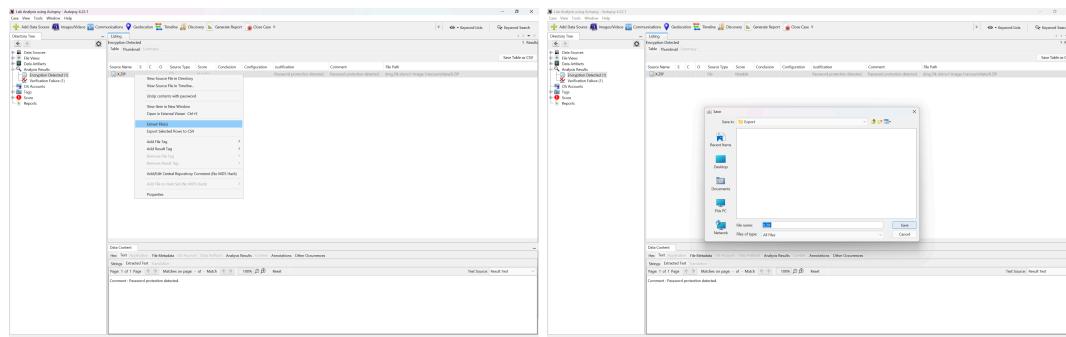
→ Secret message:

“George

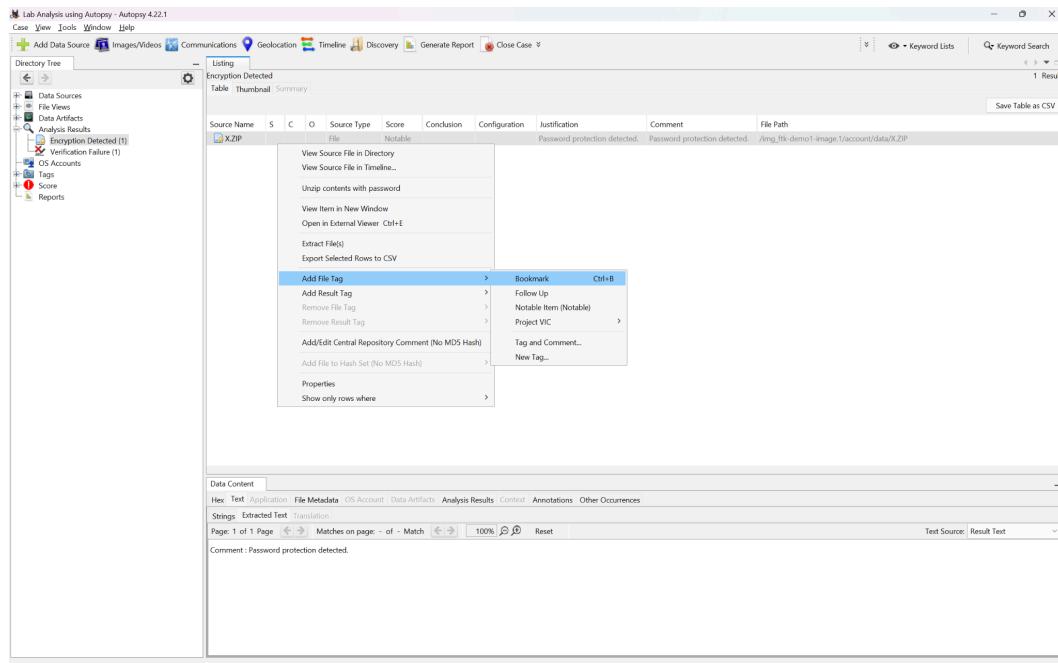
*Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?
Marth”*

(More info included in the report)

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



→ Export File



→ Add Bookmark File Tag

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

→ Keyword Search (“password”)

The screenshot shows the Autopsy interface with a context menu open over a file entry in the left pane. The menu includes options like 'Open Source File in Checker', 'Open Source File in Finder', 'Open in External Viewer', 'Edit', 'Export Selected Files to CSV', 'Add File Tag', 'Remove File Tag', 'Remove from Tag', and 'Additional Context Dependency Generated by this Entry'. Below the menu, a 'Data Content' pane shows file details. At the bottom, a 'Enter Password' dialog box is displayed, asking for the password 'couch'.

→ 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)

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

→ 6 files contain the word “password”

The screenshots show the following findings:

- Encryption Detected Artifacts:** Several files are identified as encrypted, such as `X.ZIP`, `mt_bank_secrecy.htm`, and `SG8.TXT`.
- Comment : Password protection detected.**: A comment is present in multiple files indicating password protection.
- Merriam Webster's Collegiate Dictionary, 10th edition:** The software highlights specific words from the dictionary, such as "couch", which is mentioned in the password for the account.
- Unallocated Space Artifacts:** Files like `Unalloc 4 17920 1474560` and `f0000003.txt` are shown.
- SG8.TXT File Content:** The file contains the text: "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. I hung 2 things. I don't want to spend another longer time - I am necessary in 30'jones. George".
- mt_bank_secrecy.htm File Content:** The file contains the text: "I hung 2 things. I don't want to spend another longer time - I am necessary in 30'jones. George".

- 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.

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
x.msg7.txt				2003-01-15 12:45:44 GMT	2000-05-00 00:00:00	2003-01-15 00:00:00	2003-02-15 15:49:35 GMT	662	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/personal/Messages/msg7.txt
x.msg5.txt				2003-02-15 12:44:16 GMT	2000-05-00 00:00:00	2003-02-15 00:00:00	2003-02-15 15:48:33 GMT	316	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/personal/Messages/msg5.txt
x.msg4.txt				2003-02-15 12:43:30 GMT	2000-05-00 00:00:00	2003-02-15 00:00:00	2003-02-15 15:47:18 GMT	453	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/week/msg4.txt
x>All.S.GIF				2003-02-15 14:35:04 GMT	2000-05-00 00:00:00	2003-02-15 00:00:00	2003-02-15 15:43:42 GMT	487	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/SophareFile/EST/All.S.GIF
✓ 80000001.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	662	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00000001.txt
✓ 80000003.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	506	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00000003.txt
✓ 80000552.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	119	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00000552.txt
✓ 80001487.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	101	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00001487.txt
✓ 80002180.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00002180.txt
✓ 80002722.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	633	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00002722.txt
✓ 80002728.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3660	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00002728.txt
✓ 80002737.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	316	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00002737.txt
✓ 80002738.txt	2	0000-00-00 00:00:00		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	179	Unallocated	Unallocated	unknown	/img_fik_demo1-image/1/ScavelliFiles/1/00002738.txt
SWISS.TXT	1	2003-02-15 10:47:05 GMT		2000-05-00 00:00:00	2000-05-00 00:00:00	2000-05-00 00:00:00	2000-05-00 00:00:00	2429	Allocated	Allocated	unknown	/img_fik_demo1-image/1/account/data/XZIP/SWISS.TXT

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

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
SWISS.CSV				2003-02-15 10:46:40 GMT	2000-05-00 00:00:00	2000-05-00 00:00:00	2000-05-00 00:00:00	2429	Allocated	Allocated	unknown	/MD5 Hash /img_fik_demo1-image/1/account/data/XZIP/SWISS.CSV

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

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

→ There is 3 htm/html files

Bank web files:

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

(More info included in the report)

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

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

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

Left Pane (Raw Text):

```

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

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

George

```

Right Pane (Metadata):

```

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

```

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

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

Message Body (Left Window):

```

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

George

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

```

Message Body (Right Window):

```

George

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

```

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

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

Message Body (Left Window):

```

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

George

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

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

George

```

Message Body (Right Window):

```

George

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

```

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

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

Message Body (Left Window):

```

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

Martha

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

```

Message Body (Right Window):

```

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

```

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

(More info included in the report)

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

The image displays two windows of the Autopsy software. The left window is titled 'Summary' and contains a table with columns for Case Name, File Type, and Size (bytes). The right window is titled 'Tagged Results' and contains a table with columns for Tag, Comment, User Name, Modified Date, and Accessed Time. Both tables show various entries related to the investigation.

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

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

Comparative validation — FTK vs Autopsy

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

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 Findings:** 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

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
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_14745 60 (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

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar displays a tree view of data sources, file types, deleted files, and other artifacts. The main pane shows a grid of images, with the first image, '_AF6.JPG', selected. Below the grid is a hex dump of the file's contents. Three smaller windows are overlaid on the main pane, each showing a different view of the file's content:

- _AF6.JPG - Data Artifacts:** Hex view showing raw file data.
- _AF6.JPG - Editor:** Text view showing the extracted text message: "George...Are yo u sure you know what you are doing. Isn't it dan gerous, won't you get caught?...".
- _AF6.JPG - Editor:** Metadata view showing file details like type (File System), size (238), and SHA-256 (2955f1aa1544baef1fd1fbc432ae1742fe9b04a82head3c7b3d9640f27a4).

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 4.2.2 interface with a keyword search results table. The table lists six files found containing the keyword "password".

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	63
Unalloc_A_17920_1474560	minute. You can find the «password» for the encrypted.	/img_ftk-demo1-image_1/\$Unalloc/Unalloc_A_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
_SG8.TXT	You can find the «password» for the encrypted.	/img_ftk-demo1-image_1/SGphanFiles/_SG8.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	50
_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 15:39:16 GMT	16
f0000003.txt	minute. You can find the «password» for the encrypted.	/img_ftk-demo1-image_1/ScarvedFiles/1/0000003.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	50
mt_bank_secrecy.htm	Jhon M. Jones.The «passwords» for your account is:	/img_ftk-demo1-image_1/account/data/mt_bank_se...	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

Timestamp: 21/10/2025 00:06:07

Files: X.ZIP, Unalloc_A_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 Autopsy 4.22.1 interface with the 'Analysis Results' tab selected. In the left sidebar, under 'Analysis Results', there is a section titled 'Encryption Detected' containing one item. Below it is 'Keyword Search' with six items. The main pane displays a table of files found:

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 13:15:12 GMT	2000-06-00 05:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:52:36 GMT	16
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
_SG8.TXT	You can find the <password> for the encrypted.../img_ftk-demo1-image.1/S0phanFile/_SG8.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/wolv/_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 15:53:16 GMT	1E
00000003.txt	minute. You can find the <password> for the encrypted.../img_ftk-demo1-image.1/\$CarvedFiles/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
mrt_bank_secrecy.htm	htm Mr. Jones.The <password> for your account is: .../img_ftk-demo1-image.1/account/data/mrt_bank_secr...		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	2B

In the bottom right corner of the main pane, there is a note: '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

The image contains four side-by-side screenshots of the Lab Analyst software interface, specifically the 'Keyed Search' feature. Each screenshot shows a list of search results with columns for Name, Report Period, Location, Modified Time, Change Time, and Access Time. The results are for various encrypted files, including 'Unalloc_4_17920_1474560', '_SG8.TXT', '__Y.EXE', and 'f0000003.txt'. Each result includes a link to a detailed view of the file's contents, which is displayed in a separate window below the main list. The detailed views show snippets of text from the Merriam-Webster's Collegiate Dictionary, 10th edition, such as 'Merriam', 'the 10th word in the right column on page 263', and 'It's the 10th word in the right column on page 263.' The software interface includes tabs for 'File', 'Test', 'File Metadata', 'Data Analysis', 'Analysis Results', 'Associations', and 'Other Occurrences'.

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\} n [NL *cotangens*, *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

cote \kōt\ vt [prob. fr. MF *coterer*] (1555) *obs.* : to pass by

co-te-rie \kō-tērē\, \kō-tārē\ n [F, fr. MF, tenants, fr. OF *cotier* cotter, of Gmc origin; akin to OE *ce* hut] (1738) : an intimate and often exclusive group of persons with a unifying common interest or purpose

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

co-thur-nus \kō-thār-nəs\ n, pl -ni, -ne\ [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-i-al \(-kō-tēdēl\} adj (1833) : indicating equality in the tides or a coincidence in the time of high or low tide

co-till-ion \kō-tēl-yōn, kō-\ also **co-till-on** \kō-tēl-yān, kō-, kō-tē(y)o\ 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 \kō-tē-tō-nē-as-tər\, \kō-tē-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-kwēn\ 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 [Cotswoold Hills, England] (ca. 1658) : any of an English breed of large long-wooled 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-tēj\ 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 one-family house 3 : a small detached dwelling

cot-ton-tail \kā-tēn-tāl\ 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 \-,wēd\ n (1562) : any of various weedy plants (as cudweed) with hoary pubescence or cottony seeds

cot-ton-wood \-,wūd\ 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 \kāt-nē, \kā-tē-nē\ adj (1578) : resembling cotton in appearance or character: as a : covered with hairs or pubescence b : SOFT

cot-tony-cush-ion scale \-ku-shān-\ 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 \kā-tē-lē-dōn\ n [NL, fr. Gk *kotylédon* cup-shaped hollow, fr. *kotylé* 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** \-lē-dō-nērē\ adj

cot-y-lo-saur \kā-tē-lō-sōr, kā-tē-lō-sōr\ n [ultim. fr. Gk *kotylē* + *saurus* 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 \kāuch\ 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 \sim 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

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 \kāuch-ānt\ adj [ME, fr. MF, fr. pp. 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

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”)

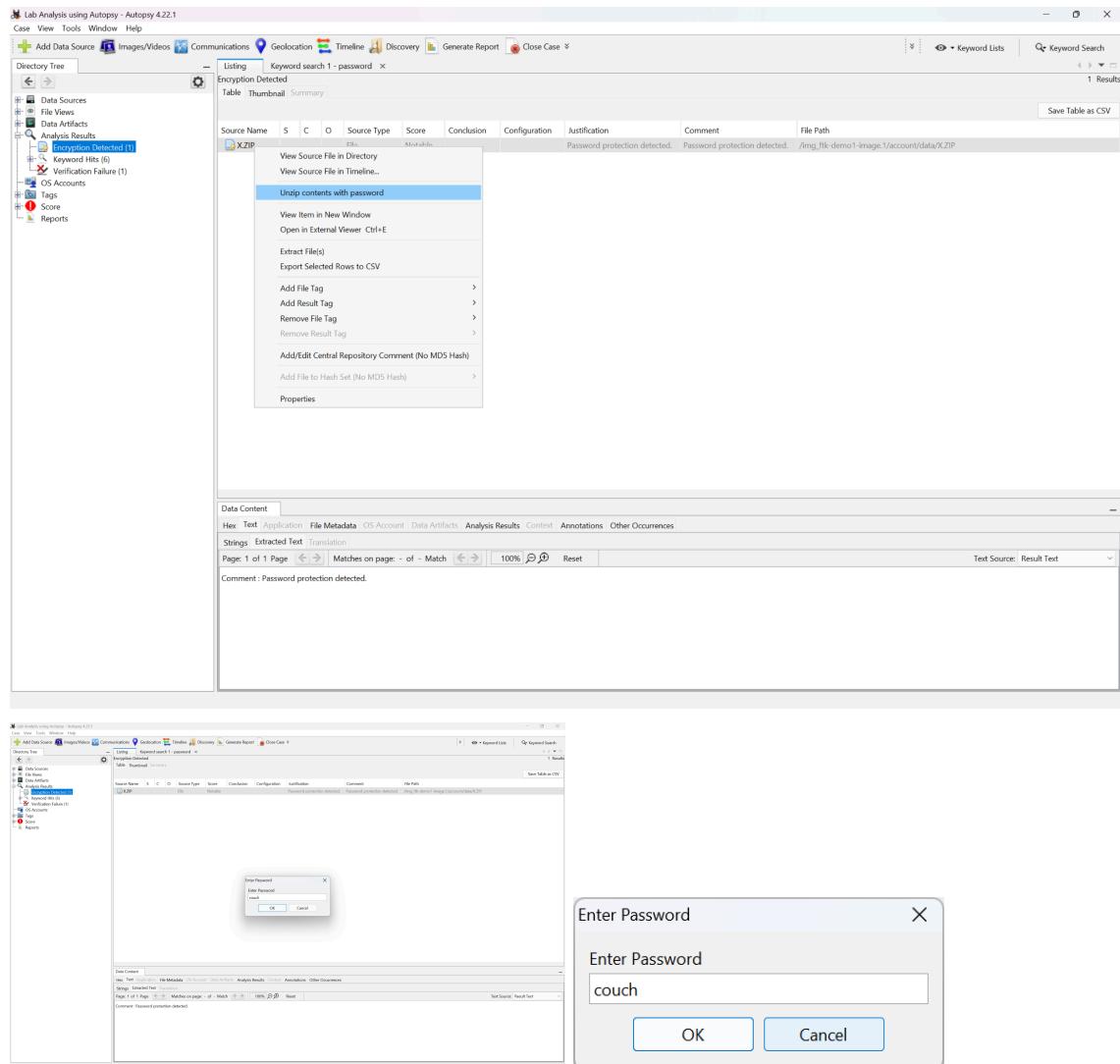
The screenshot shows the Autopsy 4.22.1 interface. The top menu bar includes Case, View, Tools, Window, Help. The main toolbar has icons for Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, and Close Case. The left sidebar shows a Directory Tree with categories like Data Sources, File Views, Data Artifacts, Analysis Results, OS Accounts, Tags, Score, and Reports. A Keyword search tab is active, displaying a table of results. The table columns are Name, Keyword Preview, Location, Modified Time, and Change Time. One result is highlighted: "Encryption Detected Artifact" with the preview "Comment: «Passwords» protection detected. minute. You can find the «password» for the encrypted." and the location "/img_ftk-demo1-image1/account/data/X.ZIP". The modified time is 2003-02-15 13:13:12 GMT and change time is 0000-00-00 00:00:00. The right pane shows search filters for "password", search options (Exact Match, Substring Match, Regular Expression), and a search results summary. Below the search results is a "Data Content" panel with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The "Text" tab is selected, showing page 1 of 1.

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

Export File & Add Bookmark File Tag

The image contains three side-by-side screenshots of the Autopsy interface. The first screenshot shows a context menu open over a file entry in the main pane, with the option "Export File..." highlighted. The second screenshot shows the "Export File" dialog box open, displaying file selection fields and a "Save As" button. The third screenshot shows the "File Tag" dialog box open, where a new tag named "Bank Record" is being created, with the "Add to Case" checkbox checked.

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

Screenshot of Lab Analysis using Autopsy 4.22.1 showing the analysis of the file SWIZZ.XLS.

The interface includes a top navigation bar with tabs like Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, Keyword Lists, and Keyword Search.

The left sidebar shows a Directory Tree with sections like Data Sources, File Views, Data Artifacts, Metadata (5), Analysis Results (Encryption Detected 1, Keyword Hits 6, Verification Failure 1), OS Accounts, Tags, Score, and Reports.

The main content area displays a table with columns: Source Name, S, C, O, Description, Owner, Data Source, Date Created, Date Modified, User ID, Program Name, and Organization. A single row is selected for "SWIZZ.XLS", showing details: 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.

A detailed view of the file's metadata is shown below, including fields like Type, Value, and Source(s) for various properties such as Date Created, Date Modified, User ID, Program Name, Organization, and Source File Path.

Below this is a screenshot of a Microsoft Excel spreadsheet titled "SWIZZ.XLS - Editor". The spreadsheet contains bank statement data with columns for Date, Amount, and Description. The data includes numerous transactions in US dollars, such as deposits from "Swiss Genève Internationale" and "Autres lieux", and withdrawals for "Argent Total Courant". The spreadsheet also shows account numbers like 9882111.0 and 1623.56292, and a balance of 1000.00.

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 'test/plain' view selected. The left sidebar shows various file types and artifacts. The main pane displays a table of 14 plain text files. 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 files such as msg7.txt, msg5.txt, msg4.txt, and AIL5.GIF, along with several unnamed files starting with 'f000'. The location for most files is /img_ftk-demo1-image/1/personal/Messages/.msg7.txt. The 'Known' column indicates that many files are 'Unallocated' or 'Unknown'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
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_ftk-demo1-image/1/personal/Messages/msg7.txt
msg5.txt				2003-02-15 12:44:16 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:48:33 GMT	316	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/personal/Messages/msg5.txt
msg4.txt				2003-02-15 12:43:30 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:47:18 GMT	453	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/work/msg4.txt
AIL5.GIF				2003-02-15 14:35:04 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:43:42 GMT	487	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/OrphanedFile_ESI/AIL5.GIF
f0000001.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_ftk-demo1-image/1/CarvedFiles/1/f0000001.txt
f0000003.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_ftk-demo1-image/1/CarvedFiles/1/f0000003.txt
f000052.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_ftk-demo1-image/1/CarvedFiles/1/f000052.txt
f0001487.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_ftk-demo1-image/1/CarvedFiles/1/f0001487.txt
f0002180.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0002180.txt
f0002722.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_ftk-demo1-image/1/CarvedFiles/1/f0002722.txt
f0002728.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	3660	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0002728.txt
f0002737.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_ftk-demo1-image/1/CarvedFiles/1/f0002737.txt
f0002738.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_ftk-demo1-image/1/CarvedFiles/1/f0002738.txt
SWISS.TXT	1			2003-02-15 10:47:06 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2429	Allocated	Allocated	unknown	/img_ftk-demo1-image/1/account/data/X.ZIP/SWISS...

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 file path and a tab labeled 'Editor'. The left window is for '/img_ftk-demo1-image.1/personal/Messages/msg7.txt' and the right window is for '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0000001.txt'. Both windows have a toolbar at the top with tabs for 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. Below the toolbar is a search bar with 'Text' selected. The main pane displays the extracted text. In the left window, the text reads: '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 .'. In the right window, the text is identical: '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 .' Below the text in both windows is a section labeled 'METADATA'.

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

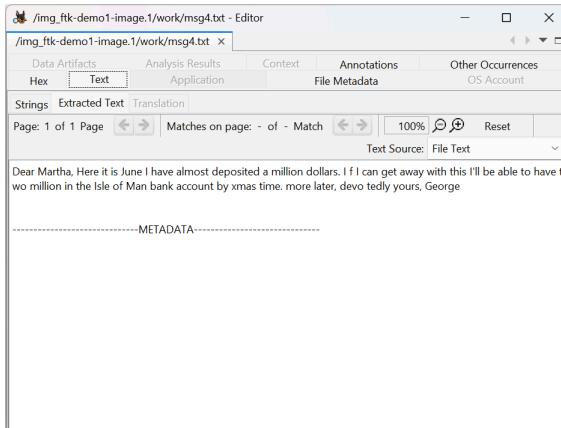
File Name: /img_ftk-demo1-image.1/\$CarvedFiles/1/f0002737.txt

The image shows two side-by-side FTK Editor windows. Both windows have a title bar with the file path and a tab labeled 'Editor'. The left window is for '/img_ftk-demo1-image.1/personal/Messages/msg5.txt' and the right window is for '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002737.txt'. Both windows have a toolbar at the top with tabs for 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. Below the toolbar is a search bar with 'Text' selected. The main pane displays the extracted text. In the left window, the text reads: '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'. In the right window, the text is identical: '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'. Below the text in both windows is a section labeled 'METADATA'.

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



The screenshot shows the FTK Editor interface with the file '/img_ftk-demo1-image.1/work/msg4.txt' open. The 'Text' tab is selected. The content of the file is displayed as follows:

```
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
```

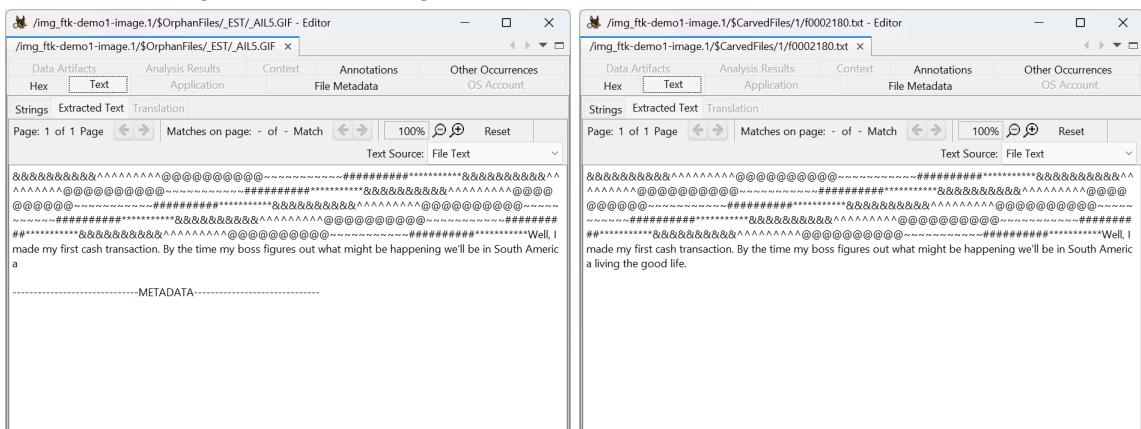
-----METADATA-----

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



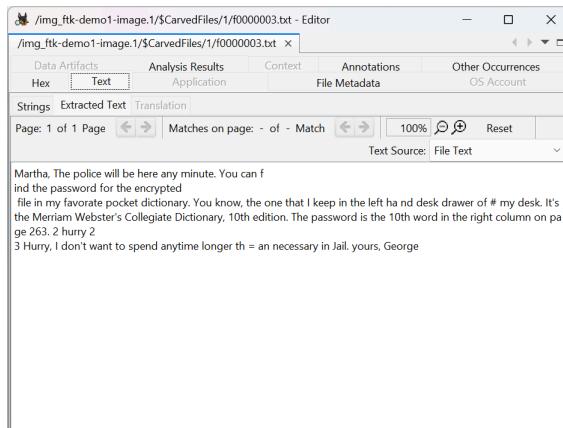
The screenshot shows two side-by-side FTK Editor windows. The left window shows the file '/img_ftk-demo1-image.1/\$OrphanFiles/_EST/_AIL5.GIF' with the 'Text' tab selected. The right window shows the file '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002180.txt' with the 'Text' tab selected. Both windows display a large amount of encoded text (likely ROT13 or similar) followed by the same 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 a living the good life.
```

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



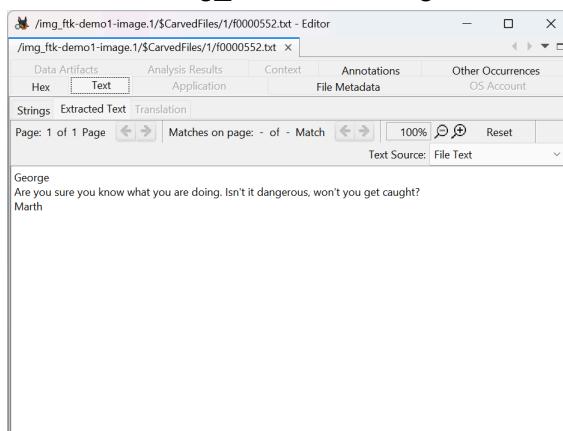
The screenshot shows the FTK Editor interface with the title bar "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0000003.txt - Editor". The "Text" tab is selected. The main pane displays the following text:

```
Martha, The police will be here any minute. You can find the password for the encrypted  
file in my favorite pocket dictionary. You know, the one that I keep in the left hand 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 than 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 hand 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 than 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:

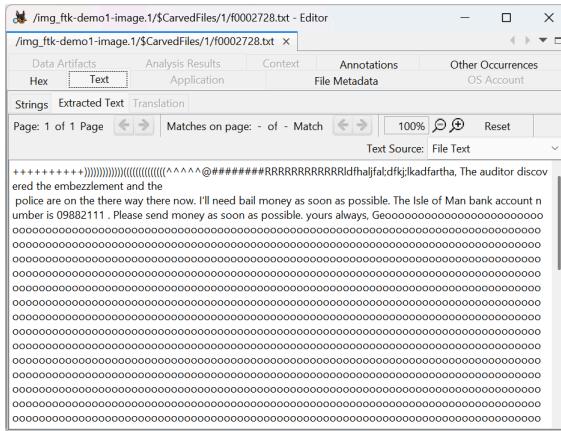
```
George  
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?  
Marth
```

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/f0002728.txt

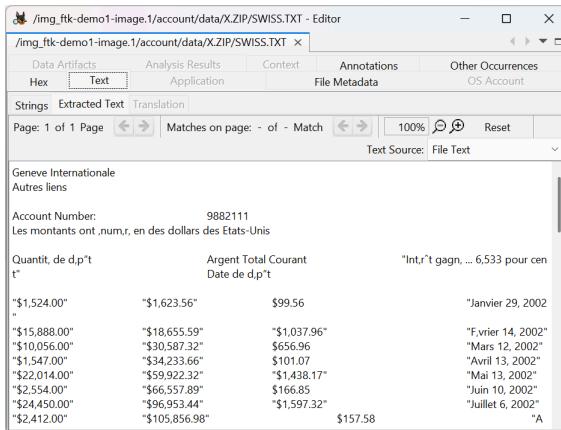


The screenshot shows a window titled "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002728.txt - Editor". The "Text" tab is selected. The text area contains a multi-line message in a mix of binary-like characters and readable text. The readable part starts with "The auditor discovered the embezzlement and 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, Ge...".

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 a window titled "/img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.TXT - Editor". The "Text" tab is selected. The text area contains a bank statement from "Geneve Internationale". It includes sections for "Autres liens", "Account Number: 9882111", and a table of transactions. The table has columns for Date, Amount, and Description.

Date	Amount	Description
"Janvier 29, 2002"	\$1,524.00*	Argent Total Courant
"	"\$1,623.56"	Date de d.p't
"\$15,888.00"	"\$18,655.59"	"\$1,037.96"
"\$10,056.00"	"\$30,587.32"	"\$656.96"
"\$1,547.00"	"\$34,233.66"	"\$10,107"
"\$22,014.00"	"\$59,922.32"	"\$1,438.17"
"\$2,554.00"	"\$66,557.89"	"\$166.85"
"\$24,450.00"	"\$96,953.44"	"\$1,597.32"
"\$2,412.00"	"\$105,856.98"	\$157.58

Excerpt:

*"Geneve Internationale
Autres liens*

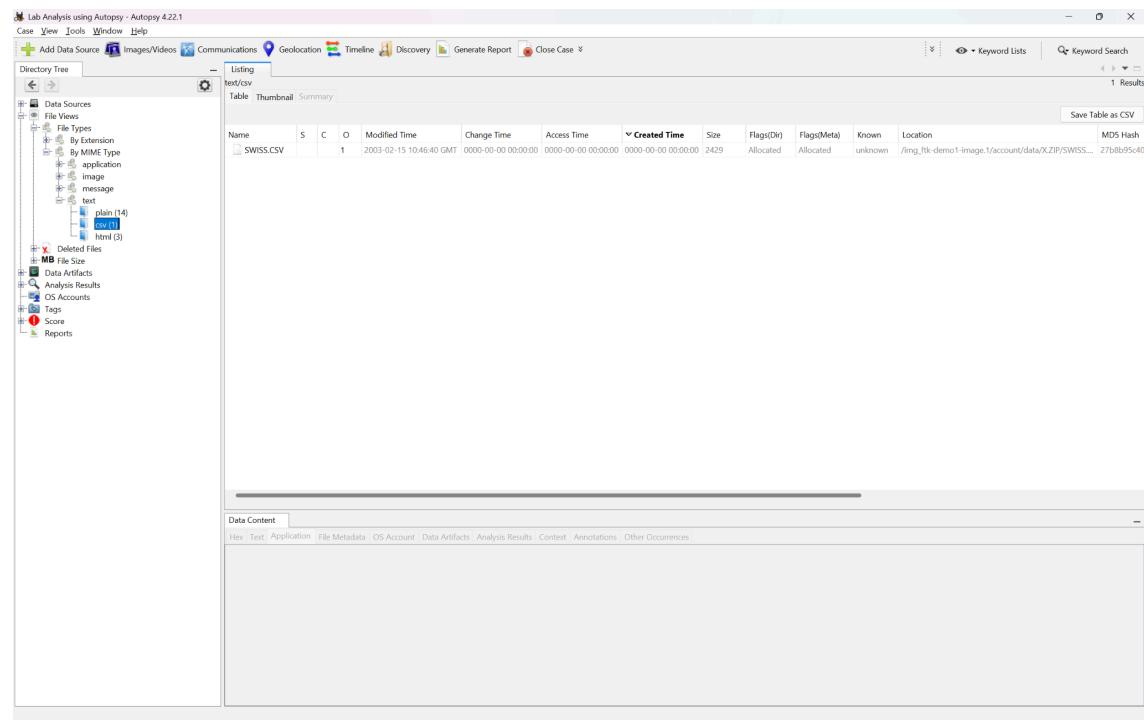
Account Number: 9882111

"

Bank Statements

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

CSV text files



The screenshot shows the Lab Analysis interface of Autopsy 4.22.1. The main window displays a file listing titled "Listing" for "text/csv". There is one result, "SWISS.CSV", shown in a table format. The table columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The file "SWISS.CSV" has a size of 2429 bytes, was modified on 2003-02-15 at 10:46:40 GMT, and was created on 0000-00-00 00:00:00. The location is /img_ftk-demo1-image.1/account/data/XZlP/SWISS... and it has an MD5 hash of 27bb8695c40. The interface includes a "Save Table as CSV" button. On the left, the "Directory Tree" pane shows a hierarchical view of data sources, file types (including plain (14) and csv (1)), deleted files, MB file size, file artifacts, analysis results, OS accounts, tags, score, and reports.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
SWISS.CSV		1		2003-02-15 10:46:40 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2429	Allocated	Allocated	unknown	/img_ftk-demo1-image.1/account/data/XZlP/SWISS...	27bb8695c40

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										
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										
<i>Autres liens</i>										
Account Number:	9882111	Les montants ont été exprimés en dollars des États-Unis	Quantité de dépôt	Argent Total Courant	Intérêt gagné à 6,533 pour cent	Date de dépôt				
\$1,524.00	\$1,621.56	\$99.56				Janvier 29, 2002				
\$15,888.00	\$16,655.59	\$767.96				Février 14, 2002				
\$10,566.00	\$16,587.32	\$630.96				Mars 12, 2002				
\$1,547.00	\$16,233.66	\$101.07				Avril 13, 2002				
\$22,014.00	\$16,922.32	\$1,438.17				Mai 13, 2002				
\$2,000.00	\$16,922.32	\$100.00				Juillet 6, 2002				
\$24,450.00	\$16,951.34	\$1,597.32				Août 23, 2002				
\$2,412.00	\$16,956.56	\$157.58				Septembre 12, 2002				
\$24,186.00	\$16,985.38	\$1,580.07				Octobre 13, 2002				
\$2,541.00	\$17,006.43	\$160.00				Novembre 12, 2002				
\$2,520.00	\$17,057.92	\$477.62				Décembre 2, 2002				
\$24,632.00	\$17,058.79	\$1,609.21				Janvier 24, 2003				
\$212,588.00	\$49,425.84	\$13,888.37				Février 10, 2003				
\$24,553.00	\$49,075.55	\$1,404.05				Mars 12, 2003				
\$2,455.00	\$49,000.43	\$641.74				Avril 4, 2003				
\$7,892.00	\$58,435.93	\$515.58				Mai 22, 2003				
\$2,353.00	\$62,504.46	\$151.72				Juin 15, 2003				
\$221,450.00	\$68,946.82	\$1,446.73				Juillet 2, 2003				
\$2,410.00	\$71,356.38	\$3,032.37				Août 23, 2003				
\$59,311.00	\$91,173.39	\$3,874.79				Septembre 24, 2003				
\$6,548.00	\$97,827.48	\$427.78				Octobre 11, 2003				
\$54,156.00	\$109,999.75	\$1,099,879.55				Novembre 2, 2003				
\$1,178.00	\$110,177.75	\$40.07				Décembre 3, 2003				
\$47,872.00	\$130,716.87	\$5,127.48				Janvier 20, 2004				
\$36,548.00	\$142,693.71	\$2,387.68				Février 13, 2004				
\$231,455.00	\$176,541.24	\$15,120.96				Mars 12, 2004				
\$2,400.00	\$178,941.24	\$111.76				Avril 14, 2004				
\$24,863.00	\$203,922.26	\$1,624.30				Mai 3, 2004				
\$98,765.00	\$270,950.39	\$6,452.32				Juin 12, 2004				
\$17,893.00	\$248,373.53	\$1,168.95				Juillet 4, 2004				
\$3,490.00	\$264,740.03	\$2,116.16				Août 1, 2004				
\$14,492.00	\$289,236.33	\$3,586.09				Septembre 22, 2004				
\$45,789.00	\$310,139.80	\$2,991.40				Octobre 10, 2004				
\$34,447.00	\$340,626.44	\$2,290.42				Novembre 3, 2004				
\$29,833.00	\$359,651.56	\$1,948.99				Décembre 4, 2004				
\$68,945.00	\$389,678.00	\$4,504.18								

METADATA

Content-Encoding: windows-1252
Content-Type: application/x-zip-compressed; charset=windows-1252; delimiter=comma
X-TRKA-detected-By: org.apache.tika.parser.DefaultParser
X-TRKA-detected-Encoding: windows-1252
X-TRKA-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

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar contains a tree view of data sources, including 'File Types' (By Extension, By MIME Type, application, image, message, text), 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main pane displays a table of files under the 'Listing' tab. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. There are three results listed:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
mrt_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
mrt_bank_secrey.htm				2003-02-15 13:38:36 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:54:12 GMT	2828	Allocated	Allocated	unknown	/img_ftk-demo1-image/1/account/data/mt
f0001705_mrt_bankhtml				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/f0

The bottom pane is titled 'Data Content' and includes tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

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

The image shows two side-by-side FTK Editor windows. Both windows have a title bar with the file path and 'Editor' and a toolbar with tabs for 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The left window's toolbar also includes 'Hex', 'Text', 'Application', 'File Metadata', and 'OS Account' buttons, with 'Text' being the active tab. The right window's toolbar includes 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', 'Other Occurrences', 'Hex', 'Text', 'Application', 'File Metadata', and 'OS Account' buttons, with 'Text' being the active tab. Both windows display the same extracted text, which includes the header 'Isle of Mountain Men Banking, Inc.' followed by a list of bank names: Mt. High Private Bank Limited, Rocky Mt. Bank, Mt. Adams Bank, The Brothers Mt. Bank, and Mountain Bank Offshore.

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

The image shows a single FTK Editor window with a title bar 'img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm - Editor' and a toolbar with 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences' tabs. The 'Text' tab is active. The main pane displays a secret message: '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'

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 Lab Analysis using Autopsy 4.22.1 interface. The main window displays a file listing titled 'message/rfc822' with 4 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 results show several Microsoft Outlook message files (msg) from February 2003.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
m-021230.msg	2			2003-02-15 12:03:32 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:57:15 GMT	519	Allocated	Allocated	unknown	/img/rk-demo1-image1/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/rk-demo1-image1/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/rk-demo1-image1/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/rk-demo1-image1/personal/Messages/m-021...

Below the file listing, there is a 'Data Content' section with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The Text tab is selected. It shows a search bar with 'String' and 'Extracted Text' options, and a page navigation area with 'Page: 1 of 1' and 'Go to Page:'. A script selection dropdown shows '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 Editor application. Both windows have the title bar '/img_ftk-demo1-image.1/personal/Messages/g-021218.msg - Editor' and the path '/img_ftk-demo1-image.1/personal/Messages/g-021218.msg' in the address bar.

Left Window (Message Body):

- Toolbars: Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences.
- Text tabs: Hex, Text (selected), Application, File Metadata, OS Account.
- Search: Page: 1 of 1 Page, Matches on page: - of - Match, 100%, Reset.
- Text Source: File Text.
- Content:

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

Right Window (Metadata):

- Toolbars: Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences.
- Text tabs: Hex, Text (selected), Application, File Metadata, OS Account.
- Search: Page: 1 of 1 Page, Matches on page: - of - Match, 100%, Reset.
- Text Source: File Text.
- Content:

George

-----METADATA-----

Content-Type: message/rfc822
Message-From: Jones
Message-To: James
Message-From-Email: georgej@widgets_intl.com]
Message-From-Name: Jones
Message:Raw-Header:Sent: 18 December 2001 18:37
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
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 shows two side-by-side screenshots of the FTK Editor application. Both windows have the title bar "/img_ftk-demo1-image.1/personal/Messages/m-021220.msg - Editor". The left window displays the text content of the email message, which includes two messages from "Martha" and one from "George". The right window displays the metadata extracted from the file, including headers like Content-Type, Message-From, and various X-TIKA-related fields.

Text Content (Left Window):

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

Metadata (Right Window):

```
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 windows of the FTK (Forensic Toolkit) software. 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 quoted section from George, a reference to an original message, and a quoted section from Martha. The right window shows the extracted metadata for the same file. The metadata includes standard headers like Content-Type, Message-From, Message-To, and various X-TIKA-related headers, along with specific fields such as dc:creator, dc:subject, and dc:title.

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

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”*

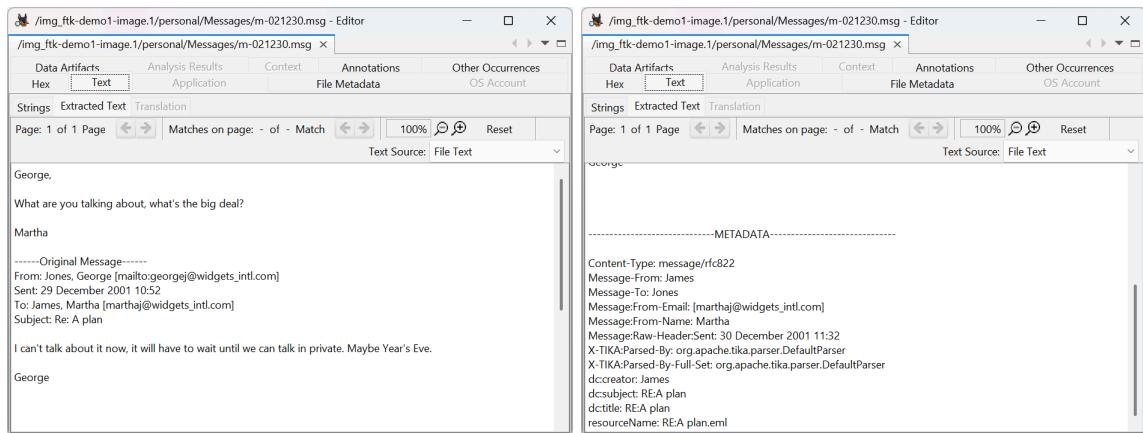
Metadata:

-----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

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?

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 screenshot of a Microsoft Excel spreadsheet titled "Summary". The spreadsheet contains the following data:

	A
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
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	

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.