

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)

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	Danyl Tymchuk
21/10/2025 22:00 – 22/10/2025 01:00	Analysis Period	Danyl Tymchuk
21/10/2025 13:00 – 22/10/2025 16:00	Analysis Period, Case Closure	Danyl Tymchuk

Summary of Collected Evidence

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

Findings

Evidence #1 Image Containing Questioning Message

The screenshot shows 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. The main area displays a 'Listing' view of files, with 'Images' selected. A preview pane shows various images, including several flower photos and a cat photo. Below the preview is a detailed hex dump of the file content, showing ASCII text and binary data. Three separate windows show the 'Content' tab of the file analysis for _AF6.JPG, displaying the same textual message from Martha to George.

File Content Hex Dump:

```
0x00000000: 00 0A 47 65 67 72 41 72 65 20 79 6F ..George..Are yo
0x00000010: 75 20 73 75 72 65 20 79 6F 6E 6F 77 20 u sure..you know
0x00000020: 77 65 61 74 20 79 6F 75 6E 6F 77 20 what are doi
0x00000030: 65 62 65 20 64 6F 69 6E 65 62 65 20 64 6F
0x00000040: 65 62 65 20 64 6F 69 6E 65 62 65 20 64 6F
0x00000050: 75 20 67 65 74 20 63 61 75 65 66 74 3F 00 0A 00
0x00000060: 0E 4D 61 72 74 68 00 0A 20 20 20 20 20 20 20 20
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x000000A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x000000B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

File Analysis Content Tab:

Extracted Text:

```
George..Are yo
u sure..you know
what are doi
...geous..won't yo
u get caught?...
.Marth..
```

Text Source: File Text

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

From The Sleuth Kit Isnt Tool:

```
Directory: /img_ftk-demo1-image.1/work/_AF6.JPG
SHA-256: 035553aa1544abacfd1fe432ae1142feef0d4a82f6ad3c7b3d9649074a
Hash Lookup Results: UNKNOWN
Internal ID: 46
```

Timestamp: 20/10/2025 23:42:27

File Name: _AF6.JPG

Full Path: /img_ftk-demo1-image.1/work/_AF6.JPG

File extension: JPG – JPEG image (Images)

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

Description:

The image file _AF6.JPG contains a short textual message from Martha to George.

The visible text reads:

“George

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

Analysis:

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

Relevance:

This evidence establishes:

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

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

The screenshot shows the Autopsy 4.22.1 interface with a search results table titled 'Keyword search 1 - password'. The table lists six results, each with a preview of its contents:

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
Encryption Detected Artifact	Comment : <password> protection detected.	/img/fk-demo1-image/7/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	62
Unalloc_4_17920_1474560	minute. You can find the <password> for the encrypted., /img/fk-demo1-image/7/\$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	0000-00-00 00:00:00	14
_SG8.TXT	You can find the <password> for the encrypted., /img/fk-demo1-image/7/0phanfile/_SG8.TXT	0000-00-00 00:00:00	2003-02-15 12:54:06 GMT	2003-02-15 00:00:00 GMT	2003-02-15 00:00:00 GMT	2003-02-15 15:49:42 GMT	56
__Y.EXE	minute. You can find the <password> for the encrypted., /img/fk-demo1-image/7/worke/_Y.EXE	0000-00-00 00:00:00	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
f0000003.txt	minute. You can find the <password> for the encrypted., /img/fk-demo1-image/7/\$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	0000-00-00 00:00:00	50
mt_bank_secrecy.htm	htm Mr. Jones.The <password> for your account is: /img/fk-demo1-image/7/account/data/mr_bank_secre...	0000-00-00 00:00:00	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_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 string 'Comment : Password protection detected.' under 'Strings'.

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.”

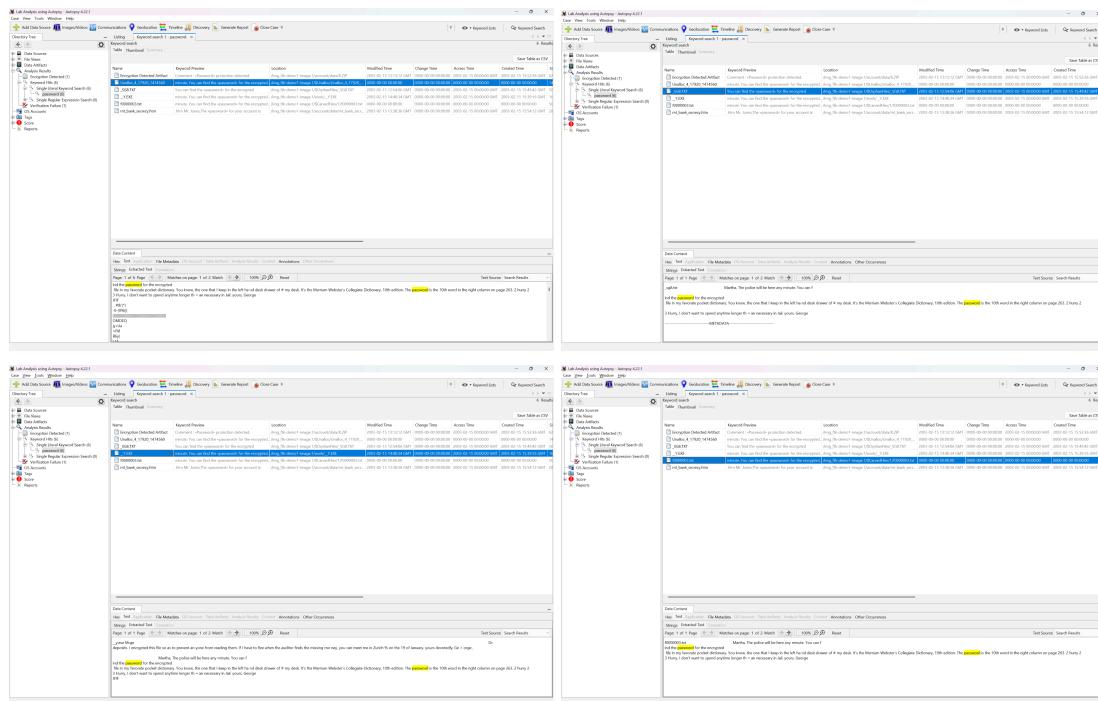
Description & Analysis:

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 *cotangēnt-, cotangēns*, fr. *co-* + *tangēnt-, 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 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\, '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\, 'kō-tē-ri\ n [F, fr. MF, tenants, fr. OF *cotier* cotter, of Gmc origin; akin to OE *cot* hut] (1738) : an intimate and often exclusive group of persons with a unifying common interest or purpose

co-ter-mi-nous \('kō-tēr-mē-nəs\} adj [alter. of *conterminous*] (1799)

1: having the same or coincident boundaries (\sim years) 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-nəs\ n, pl -ni \,-ni, -(ne)s\ [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-thərn, kō-\ 2: the dignified somewhat stilted style of ancient tragedy

co-tid-i-al \('kō-tēdē-əl\} adj (1833) : indicating equality in the tides or a coincidence in the time of high or low tide

co-till-ion \'kō-tēl-yān, kāt-\, kō-tēl-yān\ 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-nē-əs-tər, 'kāt-nē-əs-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-haired sheep

cot-ta \'kā-tə\ 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

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 \',wed\ 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

cot-y-lon n comb form [cotyledon]: cotyledon (*hypocotyl*)

cot-y-le-don \',kā-tē-lē-dōn\ n [NL, fr. Gk *κοτυλέδων* cup-shaped hollow, fr. *κοτύλη* 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-lo-saur \'kā-tē-lō-sōr, kā-tē-lō-sōr\ n [ultim. fr. Gk *κοτύλη* + *saur* 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: 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 *couchē* 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

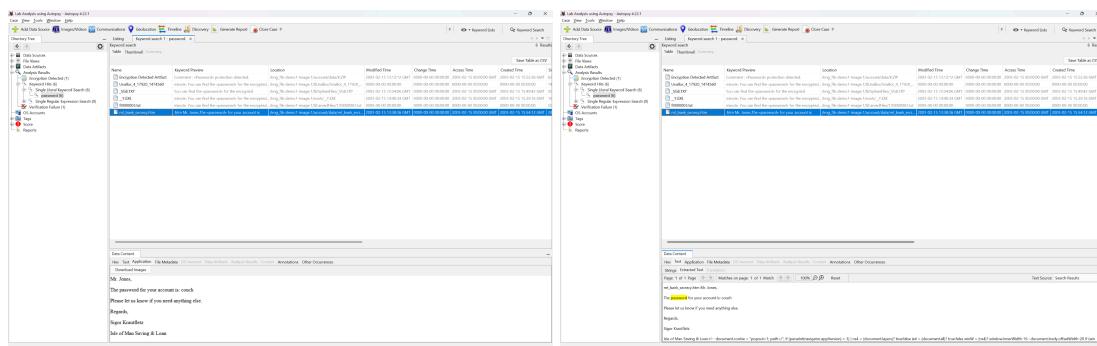
couch-ant \'kōuch-ənt\ adj [ME, fr. MF, fr. prp. of *coucher*] (15c) : lying down esp. with the head up (a heraldic lion \sim)

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 screenshot shows two separate search results from the 'Lab Analytics using Analytics' interface. Both results are for the keyword 'password'. The first result is for 'mt_bank_secrecy.htm' and the second is for 'mt_bank_secrecy.htm'. Both results show a single entry: 'The password for your account is: couch'. The table has columns for Name, Keyword Phrase, Location, Modified Time, Change Time, Access Time, and Created Time.

Name	Keyword Phrase	Location	Modified Time	Change Time	Access Time	Created Time
mt_bank_secrecy.htm	Couch - password protected content	/img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm	2023-01-11 11:12:11 (GMT)	2023-01-10 00:00:00 (GMT)	2023-01-11 11:12:11 (GMT)	2023-01-10 00:00:00 (GMT)
mt_bank_secrecy.htm	password	/img_ftk-demo1-image.1/account/data/mt_bank_secrecy.htm	2023-01-11 11:12:11 (GMT)	2023-01-10 00:00:00 (GMT)	2023-01-11 11:12:11 (GMT)	2023-01-10 00:00:00 (GMT)

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'. A checkbox 'Restrict search to the selected data sources' is unchecked. The main pane displays a table titled 'Keyword search 1 - password' with the following data:

Name	Keyword Preview	Location	Modified Time	Change Time
Encryption Detected Artifact	Comment : <Password> protection detected.	/img_fk-demo1-image.t/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., /img_fk-demo1-image.t/\$halloc/Unalloc_4_17920_...	/img_fk-demo1-image.t/\$halloc/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., /img_fk-demo1-image.t/0\$pharFile/_SGB.TXT	/img_fk-demo1-image.t/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., /img_fk-demo1-image.t/0\$or/_Y.EXE	/img_fk-demo1-image.t/0\$or/_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., /img_fk-demo1-image.t/\$carvedFiles/1/00000003.txt	/img_fk-demo1-image.t/\$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: /img_fk-demo1-image.t/account/data/mt_bank_secr...	/img_fk-demo1-image.t/account/data/mt_bank_secr...	2003-02-15 13:38:36 GMT	0000-00-00 00:00:00

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. At the bottom of the interface, there are buttons for 'Page: 1 of' and 'Go to Page:'.

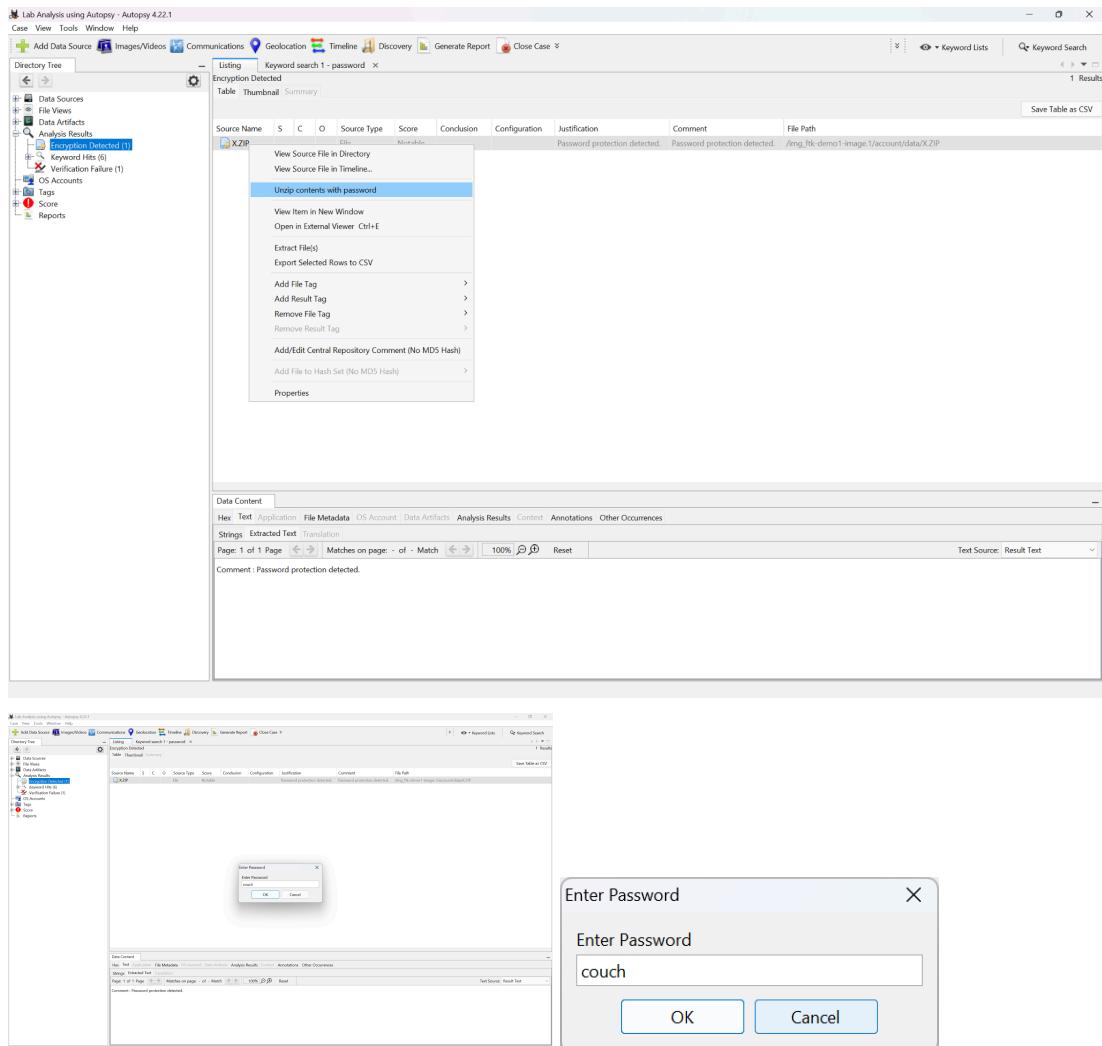
Note: step from the previous evidence, to get the password

Export File & Add Bookmark File Tag

The image consists of three side-by-side screenshots of the Autopsy interface. Each screenshot shows a different step in the process of exporting a file and adding it to a bookmark:

- Screenshot 1:** Shows the 'File Artifacts' panel with a file named 'mt_bank_secrey.htm' selected. A context menu is open over the file, with the 'Export' option highlighted.
- Screenshot 2:** Shows the 'File Artifacts' panel with the same file selected. A context menu is open, and the 'Bookmark' option is highlighted.
- Screenshot 3:** Shows the 'File Artifacts' panel with the file still selected. A context menu is open, and the 'Bookmark' option is highlighted again, indicating the final step in the process.

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 Autopsy 4.22.1 interface showing analysis results for 'SWIZZ.XLS' file.

Autopsy Analysis Results:

- Source Name:** RE-A plan
- Owner:** James
- Data Source:** ftk-demo1-image.1
- Date Created:** 2002-08-16 21:39:27 IST
- Date Modified:** 2002-08-16 22:38:14 IST
- User ID:** pc
- Program Name:** Microsoft Excel
- Organization:** The Boeing Company

Data Content:

Type	Value	Source(s)
Date Created	2002-08-16 21:39:27 IST	org.sleuthkit.autopsy.keywordSearch.Key
Date Modified	2002-08-16 22:38:14 IST	org.sleuthkit.autopsy.keywordSearch.Key
User ID	pc	org.sleuthkit.autopsy.keywordSearch.Key
Program Name	Microsoft Excel	org.sleuthkit.autopsy.keywordSearch.Key
Organization	The Boeing Company	org.sleuthkit.autopsy.keywordSearch.Key
Owner	Bill Nelson	org.sleuthkit.autopsy.keywordSearch.Key
Source File Path	/img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.XLS	org.sleuthkit.autopsy.keywordSearch.Key
Artifact ID	922372036854775800	org.sleuthkit.autopsy.keywordSearch.Key

File Editor View:

Shows a table of bank statements from Swiss Geneva Internationale. The table includes columns for Date, Description, and Amount.

Date	Description	Amount
Janvier 29, 2002	Argent Total Courant	\$15888.0
Janvier 29, 2002	Interet gagné à 6,533 pour cent	\$1037.96304
Février 14, 2002	Date de dépôt	1524.0
1623.56292		
99.56292		
Janvier 29, 2002	Argent Total Courant	\$15888.0
Janvier 29, 2002	Interet gagné à 6,533 pour cent	\$1037.96304
Février 14, 2002	Date de dépôt	1524.0
1623.56292		

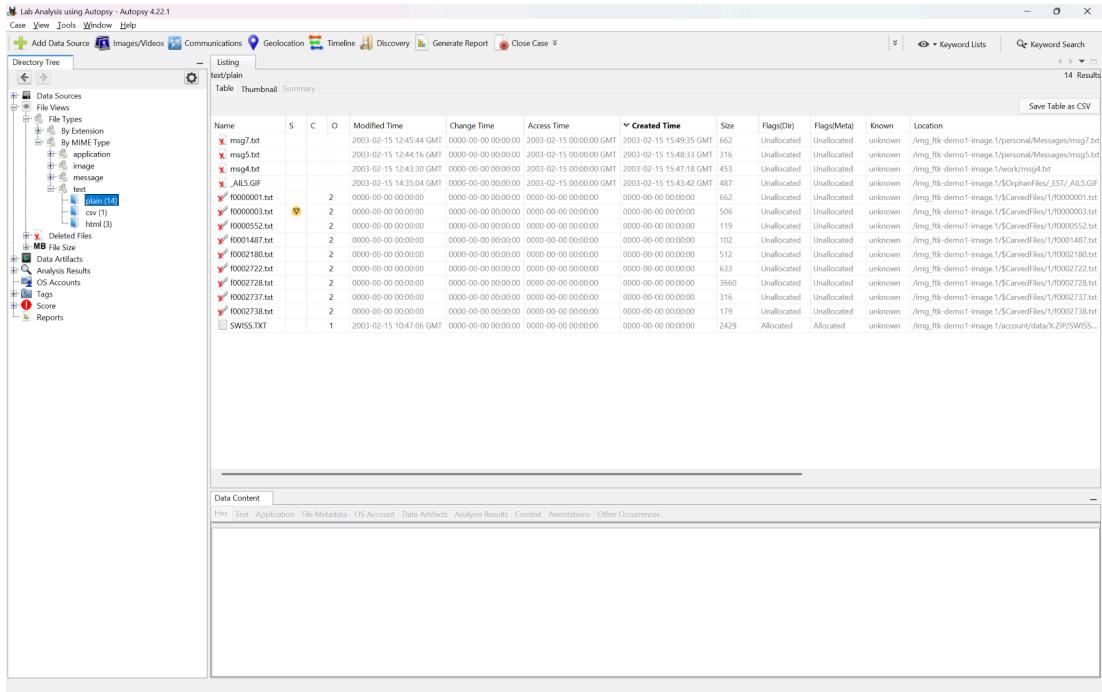
This file contains the bank statements where. Looks like substantial evidence.

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 several files, mostly .txt files, with one .gif file ('A1S.GIF'). The location column shows paths like '/img_ft-demo1-image/1/personal/Messages/msg7.txt' and '/img_ft-demo1-image/1/personal/Message/msg5.txt'. The bottom pane shows 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.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
X msg7.txt				2003-02-15 12:45:44 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:49:35 GMT	662	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/personal/Messages/msg7.txt
X msg5.txt				2003-02-15 12:44:16 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:48:31 GMT	316	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/personal/Message/msg5.txt
X msg4.txt				2003-02-15 12:43:30 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:47:18 GMT	453	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/work/msg4.txt
X msg3.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-image/1/Downloads/_EST/A1S.GIF
A A1S.GIF												
✓ 10000001.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	662	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/10000001.txt
✓ 10000003.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	506	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/10000003.txt
✓ 1000052.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	119	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/1000052.txt
✓ 1000140.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	102	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/1000140.txt
✓ 1000210.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	119	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/1000210.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	633	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/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	3669	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/1000228.txt
✓ 1000237.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	316	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/1000237.txt
✓ 1000278.txt	2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	179	Unallocated	Unallocated	unknown	/img_ft-demo1-image/1/CarvedFiles/1000278.txt
SWISS.TXT	1			2003-02-15 10:47:06 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2429	Allocated	Allocated	unknown	/img_ft-demo1-image/1/account/data/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: '/img_ftk-demo1-image.1/personal/Messages/msg7.txt' and '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0000001.txt'. The left window has tabs for Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences, with 'Text' selected. The right window also has these 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 content.

Excerpt:

“...I encrypted this file so as to prevent anyone from reading them. If I have to flee when the auditor finds the missing money, 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: '/img_ftk-demo1-image.1/personal/Messages/msg5.txt' and '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002737.txt'. The left window has tabs for Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences, with 'Text' selected. The right window also has these 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:

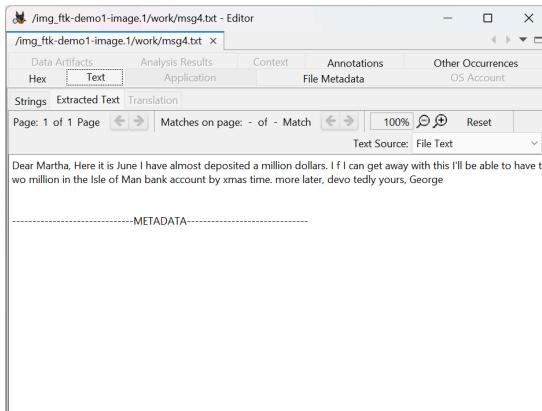
ear Mart ,
I've got a plan to get more cash. It involves rerouting invoices here at work to the field offices. It will take six month s to get back here and we can be in Brazil enjoying the fruits of our labo
-----METADATA-----

The right window shows the same text content.

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



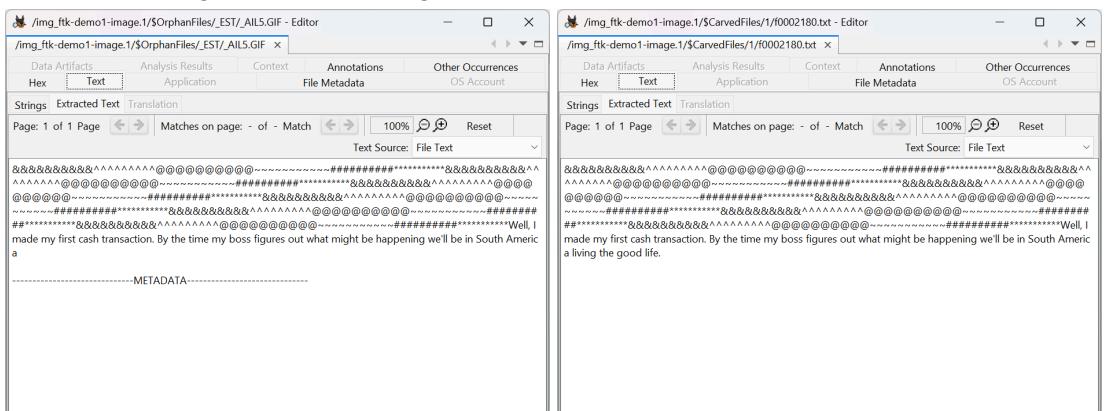
Dear Martha, Here it is June I have almost deposited a million dollars. If I can get away with this I'll be able to have two million in the Isle of Man bank account by xmas time. more later, devo tedly yours, George

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

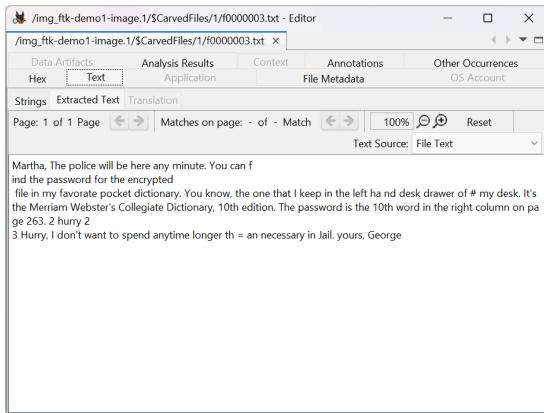


#*****&&&&&&@@@@@@#*****Well, I made my first cash transaction. By the time my boss figures out what might be happening we'll be in South America... Well, I made my first cash transaction. By the time my boss figures out what might be happening we'll be in South America...

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



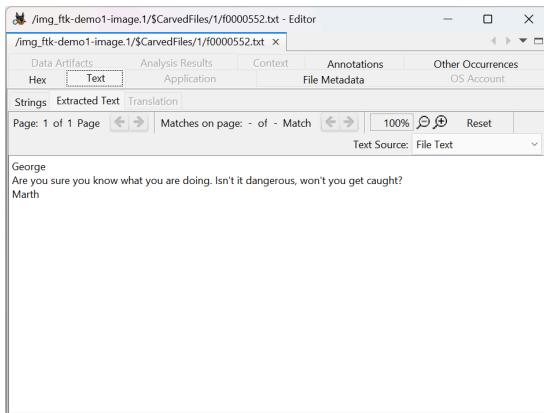
The screenshot shows the FTK Editor interface with the title bar "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0000003.txt - Editor". The "Text" tab is selected. The main pane displays the following text:

```
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

The screenshot shows the FTK Editor interface with the title bar /img_ftk-demo1-image.1/\$CarvedFiles/1/f0001487.txt - Editor. The tabs at the top are Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences, Hex, Text (which is selected), Application, File Metadata, and OS Account. Below the tabs are search and filter controls: Page: 1 of 1 Page, Matches on page: - of - Match, 100%, Text Source: File Text. The main pane displays the following text:
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

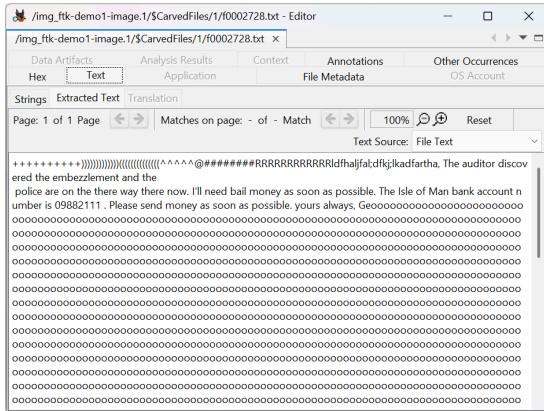
File Name: /img_ftk-demo1-image.1/\$CarvedFiles/1/f0002738.txt

The screenshot shows two side-by-side FTK Editor windows. Both have the title bar /img_ftk-demo1-image.1/\$CarvedFiles/1/f0002722.txt - Editor and /img_ftk-demo1-image.1/\$CarvedFiles/1/f0002738.txt - Editor respectively. The tabs and controls are identical to the first editor. The left pane contains highly encoded text starting with "Yours always, George" followed by a series of symbols including '&', '#', '^', '@', and various punctuation marks. The right pane contains the text "I'll tell you more about it when I get it started." and "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

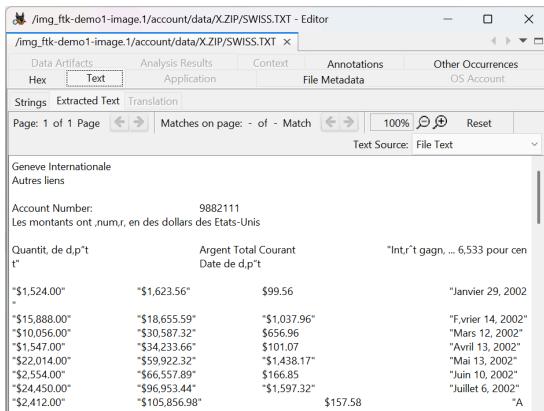


The auditor discovered the embezzlement and the police are on the way there now. I'll need bail money as soon as possible. The Isle of Man bank account number is 09882111. Please send money as soon as possible. yours always.

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



Quantit de d.p*t	Argent Total Courant Date de d.p*t	"Int.r't gagn, ... 6,533 pour cen
"\$1,524.00"	"\$1,623.56"	\$99.56
"		"Janvier 29, 2002"
"\$15,888.00"	"\$18,655.59"	"\$10,037.96"
"\$10,056.00"	"\$30,587.32"	\$656.96
"\$1,547.00"	"\$34,233.66"	\$101.07
"\$22,014.00"	"\$59,922.32"	"\$14,438.17"
"\$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
		"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

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																																																																																																																																																					
Geneve Internationale	Autres liens	100%	Reset																																																																																																																																																						
Text Source: File Text																																																																																																																																																									
<p>Account Number: 9882111</p> <p>Les montants ont été énumérés en dollars des États-Unis.</p> <table><thead><tr><th>Quantité de dépôt</th><th>Argent Total Courant</th><th>Intérêt gagné à 6,533 pour cent</th><th>Date de dépôt</th></tr></thead><tbody><tr><td>\$1,534,00</td><td>\$1,623,56</td><td>\$99,56</td><td>Janvier 29, 2002</td></tr><tr><td>\$15,888,00</td><td>\$16,655,59</td><td>\$1,037,96</td><td>Février 14, 2002</td></tr><tr><td>\$10,056,00</td><td>\$16,587,32</td><td>\$656,96</td><td>Mars 12, 2002</td></tr><tr><td>\$1,547,00</td><td>\$16,233,86</td><td>\$101,07</td><td>Avril 13, 2002</td></tr><tr><td>\$1,545,00</td><td>\$16,233,22</td><td>\$14,03</td><td>Mai 1, 2002</td></tr><tr><td>\$2,554,00</td><td>\$16,655,79</td><td>\$166,83</td><td>Juin 10, 2002</td></tr><tr><td>\$24,450,00</td><td>\$96,953,44</td><td>\$1,597,32</td><td>Juillet 6, 2002</td></tr><tr><td>\$2,412,00</td><td>\$16,854,98</td><td>\$117,58</td><td>Août 23, 2002</td></tr><tr><td>\$1,534,00</td><td>\$16,858,69</td><td>\$115,70</td><td>Septembre 12, 2002</td></tr><tr><td>\$2,541,00</td><td>\$150,296,43</td><td>\$166,00</td><td>Octobre 13, 2002</td></tr><tr><td>\$5,321,00</td><td>\$165,783,92</td><td>\$347,62</td><td>Novembre 12, 2002</td></tr><tr><td>\$3,022,00</td><td>\$165,783,92</td><td>\$19,67</td><td>Décembre 1, 2002</td></tr><tr><td>\$12,588,00</td><td>\$442,584,73</td><td>\$13,888,37</td><td>Janvier 24, 2003</td></tr><tr><td>\$24,533,00</td><td>\$497,655,86</td><td>\$1,604,05</td><td>Février 12, 2003</td></tr><tr><td>\$9,823,00</td><td>\$540,632,43</td><td>\$641,74</td><td>Mars 22, 2003</td></tr><tr><td>\$9,823,00</td><td>\$540,632,43</td><td>\$13,73</td><td>Avril 1, 2003</td></tr><tr><td>\$2,351,00</td><td>\$629,042,46</td><td>\$153,72</td><td>Mai 22, 2003</td></tr><tr><td>\$22,145,00</td><td>\$689,468,22</td><td>\$1,446,73</td><td>Jun 15, 2003</td></tr><tr><td>\$58,200,00</td><td>\$795,513,38</td><td>\$3,802,21</td><td>Juillet 3, 2003</td></tr><tr><td>\$10,000,00</td><td>\$797,513,38</td><td>\$1,000,00</td><td>Août 23, 2003</td></tr><tr><td>\$6,548,00</td><td>\$918,748,4</td><td>\$3,874,79</td><td>Septembre 24, 2003</td></tr><tr><td>\$54,156,00</td><td>\$1,099,879,55</td><td>\$3,538,01</td><td>Octobre 11, 2003</td></tr><tr><td>\$2,144,00</td><td>\$1,174,018,75</td><td>\$140,77</td><td>Novembre 2, 2003</td></tr><tr><td>\$1,534,00</td><td>\$1,174,018,75</td><td>\$3,327,48</td><td>Décembre 1, 2003</td></tr><tr><td>\$36,548,00</td><td>\$1,425,693,71</td><td>\$2,387,68</td><td>Janvier 20, 2004</td></tr><tr><td>\$231,455,00</td><td>\$1,765,410,24</td><td>\$15,120,96</td><td>Février 13, 2004</td></tr><tr><td>\$2,486,00</td><td>\$1,883,392,90</td><td>\$162,41</td><td>Mars 2, 2004</td></tr><tr><td>\$1,534,00</td><td>\$2,020,232,26</td><td>\$16,243,20</td><td>Avril 1, 2004</td></tr><tr><td>\$98,765,00</td><td>\$2,270,950,39</td><td>\$6,452,32</td><td>Mai 3, 2004</td></tr><tr><td>\$17,893,00</td><td>\$2,438,373,53</td><td>\$1,168,95</td><td>Juin 12, 2004</td></tr><tr><td>\$31,950,00</td><td>\$2,634,740,03</td><td>\$2,273,16</td><td>Juillet 4, 2004</td></tr><tr><td>\$14,640,00</td><td>\$2,830,046,33</td><td>\$3,009,29</td><td>Août 21, 2004</td></tr><tr><td>\$45,789,00</td><td>\$3,101,319,80</td><td>\$2,991,40</td><td>Septembre 22, 2004</td></tr><tr><td>\$34,447,00</td><td>\$3,340,626,44</td><td>\$2,250,42</td><td>Octobre 10, 2004</td></tr><tr><td>\$29,833,00</td><td>\$3,590,651,56</td><td>\$1,948,99</td><td>Novembre 3, 2004</td></tr><tr><td>\$68,945,00</td><td>\$3,988,678,00</td><td>\$4,504,18</td><td>Décembre 4, 2004</td></tr></tbody></table>						Quantité de dépôt	Argent Total Courant	Intérêt gagné à 6,533 pour cent	Date de dépôt	\$1,534,00	\$1,623,56	\$99,56	Janvier 29, 2002	\$15,888,00	\$16,655,59	\$1,037,96	Février 14, 2002	\$10,056,00	\$16,587,32	\$656,96	Mars 12, 2002	\$1,547,00	\$16,233,86	\$101,07	Avril 13, 2002	\$1,545,00	\$16,233,22	\$14,03	Mai 1, 2002	\$2,554,00	\$16,655,79	\$166,83	Juin 10, 2002	\$24,450,00	\$96,953,44	\$1,597,32	Juillet 6, 2002	\$2,412,00	\$16,854,98	\$117,58	Août 23, 2002	\$1,534,00	\$16,858,69	\$115,70	Septembre 12, 2002	\$2,541,00	\$150,296,43	\$166,00	Octobre 13, 2002	\$5,321,00	\$165,783,92	\$347,62	Novembre 12, 2002	\$3,022,00	\$165,783,92	\$19,67	Décembre 1, 2002	\$12,588,00	\$442,584,73	\$13,888,37	Janvier 24, 2003	\$24,533,00	\$497,655,86	\$1,604,05	Février 12, 2003	\$9,823,00	\$540,632,43	\$641,74	Mars 22, 2003	\$9,823,00	\$540,632,43	\$13,73	Avril 1, 2003	\$2,351,00	\$629,042,46	\$153,72	Mai 22, 2003	\$22,145,00	\$689,468,22	\$1,446,73	Jun 15, 2003	\$58,200,00	\$795,513,38	\$3,802,21	Juillet 3, 2003	\$10,000,00	\$797,513,38	\$1,000,00	Août 23, 2003	\$6,548,00	\$918,748,4	\$3,874,79	Septembre 24, 2003	\$54,156,00	\$1,099,879,55	\$3,538,01	Octobre 11, 2003	\$2,144,00	\$1,174,018,75	\$140,77	Novembre 2, 2003	\$1,534,00	\$1,174,018,75	\$3,327,48	Décembre 1, 2003	\$36,548,00	\$1,425,693,71	\$2,387,68	Janvier 20, 2004	\$231,455,00	\$1,765,410,24	\$15,120,96	Février 13, 2004	\$2,486,00	\$1,883,392,90	\$162,41	Mars 2, 2004	\$1,534,00	\$2,020,232,26	\$16,243,20	Avril 1, 2004	\$98,765,00	\$2,270,950,39	\$6,452,32	Mai 3, 2004	\$17,893,00	\$2,438,373,53	\$1,168,95	Juin 12, 2004	\$31,950,00	\$2,634,740,03	\$2,273,16	Juillet 4, 2004	\$14,640,00	\$2,830,046,33	\$3,009,29	Août 21, 2004	\$45,789,00	\$3,101,319,80	\$2,991,40	Septembre 22, 2004	\$34,447,00	\$3,340,626,44	\$2,250,42	Octobre 10, 2004	\$29,833,00	\$3,590,651,56	\$1,948,99	Novembre 3, 2004	\$68,945,00	\$3,988,678,00	\$4,504,18	Décembre 4, 2004
Quantité de dépôt	Argent Total Courant	Intérêt gagné à 6,533 pour cent	Date de dépôt																																																																																																																																																						
\$1,534,00	\$1,623,56	\$99,56	Janvier 29, 2002																																																																																																																																																						
\$15,888,00	\$16,655,59	\$1,037,96	Février 14, 2002																																																																																																																																																						
\$10,056,00	\$16,587,32	\$656,96	Mars 12, 2002																																																																																																																																																						
\$1,547,00	\$16,233,86	\$101,07	Avril 13, 2002																																																																																																																																																						
\$1,545,00	\$16,233,22	\$14,03	Mai 1, 2002																																																																																																																																																						
\$2,554,00	\$16,655,79	\$166,83	Juin 10, 2002																																																																																																																																																						
\$24,450,00	\$96,953,44	\$1,597,32	Juillet 6, 2002																																																																																																																																																						
\$2,412,00	\$16,854,98	\$117,58	Août 23, 2002																																																																																																																																																						
\$1,534,00	\$16,858,69	\$115,70	Septembre 12, 2002																																																																																																																																																						
\$2,541,00	\$150,296,43	\$166,00	Octobre 13, 2002																																																																																																																																																						
\$5,321,00	\$165,783,92	\$347,62	Novembre 12, 2002																																																																																																																																																						
\$3,022,00	\$165,783,92	\$19,67	Décembre 1, 2002																																																																																																																																																						
\$12,588,00	\$442,584,73	\$13,888,37	Janvier 24, 2003																																																																																																																																																						
\$24,533,00	\$497,655,86	\$1,604,05	Février 12, 2003																																																																																																																																																						
\$9,823,00	\$540,632,43	\$641,74	Mars 22, 2003																																																																																																																																																						
\$9,823,00	\$540,632,43	\$13,73	Avril 1, 2003																																																																																																																																																						
\$2,351,00	\$629,042,46	\$153,72	Mai 22, 2003																																																																																																																																																						
\$22,145,00	\$689,468,22	\$1,446,73	Jun 15, 2003																																																																																																																																																						
\$58,200,00	\$795,513,38	\$3,802,21	Juillet 3, 2003																																																																																																																																																						
\$10,000,00	\$797,513,38	\$1,000,00	Août 23, 2003																																																																																																																																																						
\$6,548,00	\$918,748,4	\$3,874,79	Septembre 24, 2003																																																																																																																																																						
\$54,156,00	\$1,099,879,55	\$3,538,01	Octobre 11, 2003																																																																																																																																																						
\$2,144,00	\$1,174,018,75	\$140,77	Novembre 2, 2003																																																																																																																																																						
\$1,534,00	\$1,174,018,75	\$3,327,48	Décembre 1, 2003																																																																																																																																																						
\$36,548,00	\$1,425,693,71	\$2,387,68	Janvier 20, 2004																																																																																																																																																						
\$231,455,00	\$1,765,410,24	\$15,120,96	Février 13, 2004																																																																																																																																																						
\$2,486,00	\$1,883,392,90	\$162,41	Mars 2, 2004																																																																																																																																																						
\$1,534,00	\$2,020,232,26	\$16,243,20	Avril 1, 2004																																																																																																																																																						
\$98,765,00	\$2,270,950,39	\$6,452,32	Mai 3, 2004																																																																																																																																																						
\$17,893,00	\$2,438,373,53	\$1,168,95	Juin 12, 2004																																																																																																																																																						
\$31,950,00	\$2,634,740,03	\$2,273,16	Juillet 4, 2004																																																																																																																																																						
\$14,640,00	\$2,830,046,33	\$3,009,29	Août 21, 2004																																																																																																																																																						
\$45,789,00	\$3,101,319,80	\$2,991,40	Septembre 22, 2004																																																																																																																																																						
\$34,447,00	\$3,340,626,44	\$2,250,42	Octobre 10, 2004																																																																																																																																																						
\$29,833,00	\$3,590,651,56	\$1,948,99	Novembre 3, 2004																																																																																																																																																						
\$68,945,00	\$3,988,678,00	\$4,504,18	Décembre 4, 2004																																																																																																																																																						
METADATA																																																																																																																																																									
Content-Encoding: windows-1252																																																																																																																																																									
Content-Type: text/csv; charset=windows-1252; delimiter=comma																																																																																																																																																									
X-ITKA-Parsed-By: org.apache.tika.parser.DefaultParser																																																																																																																																																									
X-ITKA-detectedInEncoding: windows-1252																																																																																																																																																									
X-ITKA-encodingDetector: UniversalEncodingDetector																																																																																																																																																									
csv-delimiter: comma																																																																																																																																																									
csvnum_columns: 6																																																																																																																																																									

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 has a tree view of file types, including 'File Views' which is expanded to show 'File Types' (By Extension, By MIME Type), 'Text' (plain (14)), and 'Deleted Files'. The main area displays a table of files under the 'text/html' 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. Three files are listed:

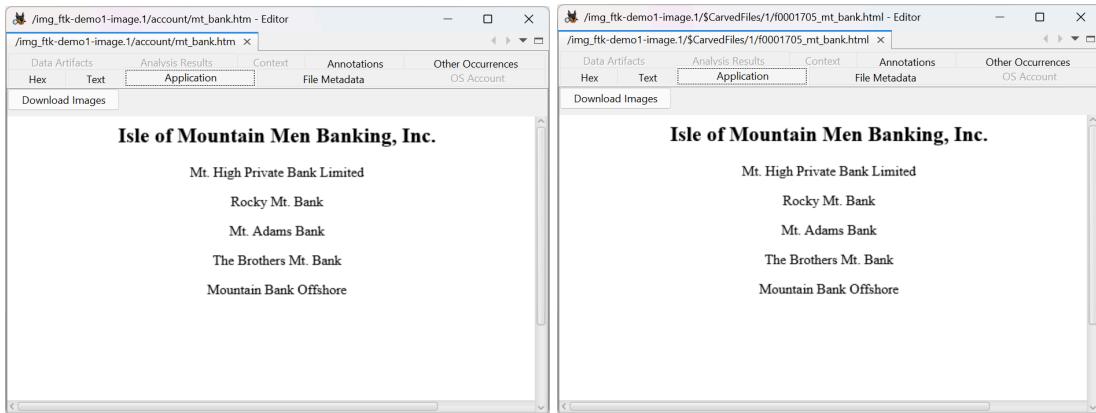
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
mt_bank.htm				2003-02-15 12:35:10 GMT	0000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:55:21 GMT	1881	Unallocated	Unallocated	unknown	/img_hk-demo1-image.1/account/mt_bank
mt_bank_secrey.htm		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

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

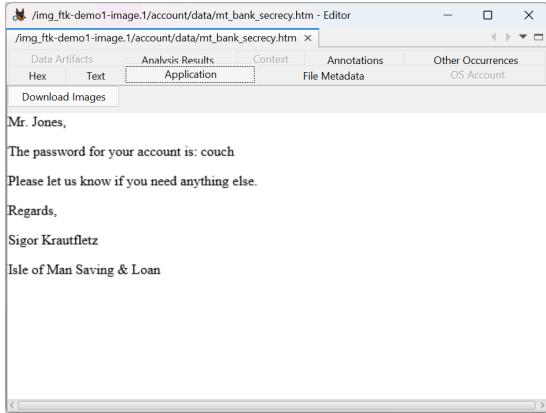
Mt. Adams Bank

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. The left sidebar contains a 'Case' tree with nodes for 'Data Sources', 'File Views', 'File Types' (including 'By Extension', 'By MIME Type', 'application', 'image', 'message', and 'text'), 'MB File Size', 'Data Artifacts', 'Analysis Results', 'OS Accounts', 'Tags', 'Score', and 'Reports'. The main pane displays a 'Listing' view for 'message/rfc822' under 'File Views'. It shows a table with four rows of file metadata:

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/nk-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/nk-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/nk-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/nk-demo1-image/1/personal/Messages/m-021...

Below the table, there is a 'Data Content' section with tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Content', 'Annotations', and 'Other Occurrences'. The 'Text' tab is selected. At the bottom of the main pane, there are buttons for 'Page: 1 of' and 'Page: Go to Page:'. On the right side of the interface, there are buttons for 'Save Table as CSV', 'Keyword Lists', and 'Keyword Search'.

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. Both windows are titled '/img_ftk-demo1-image.1/personal/Messages/g-021218.msg - Editor'.

Left Window (Content View):

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

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

Right Window (Metadata View):

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

George
- Section header: -----METADATA-----
- Content:

```
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

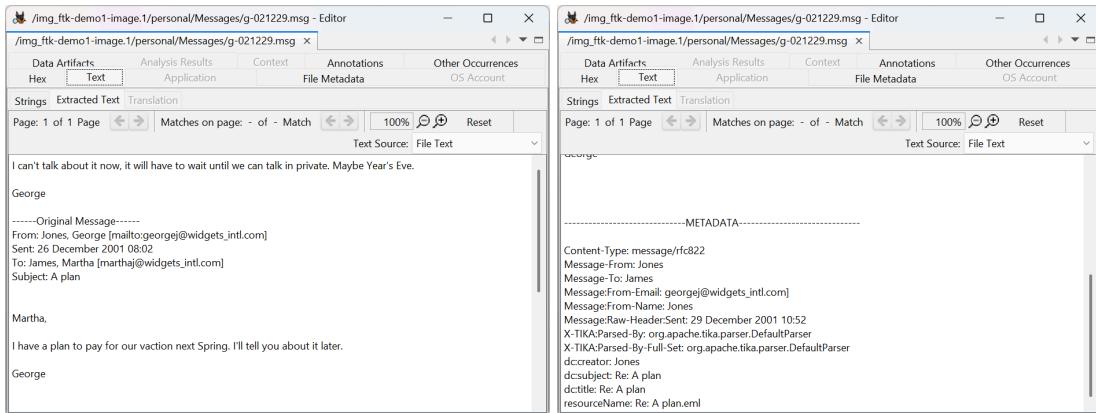
dc:subject: RE:A plan

dc:title: RE:A plan

resourceName: RE:A plan.eml

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

g-021229.msg



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,

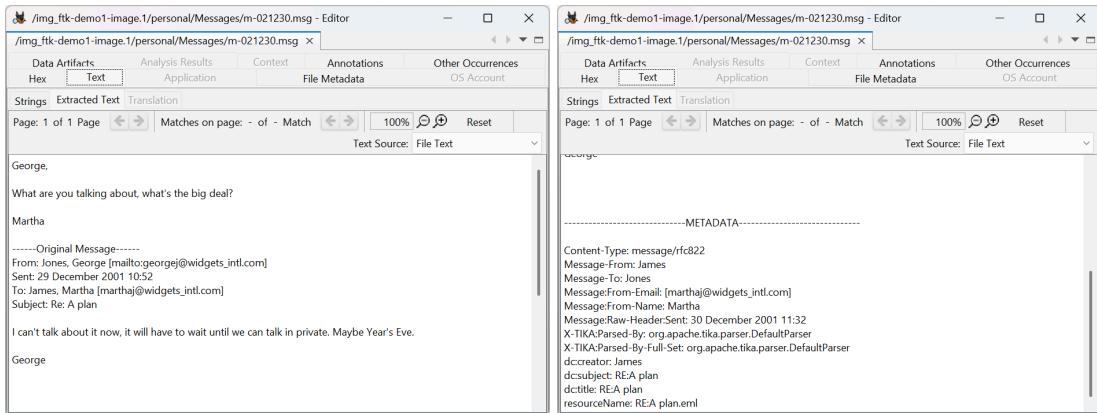
*I have a plan to pay for our vacation next Spring. I'll tell you about it later.
George"*

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:

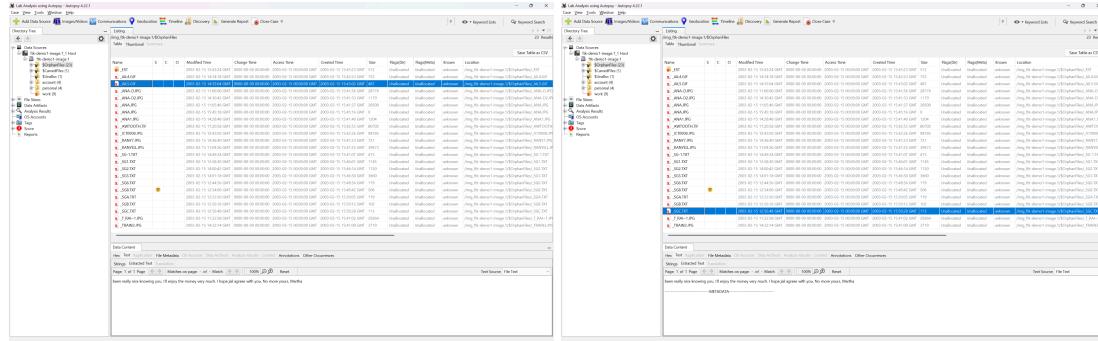
-----METADATA-----

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

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)

The screenshot shows a Microsoft Excel spreadsheet titled "Summary" in the first cell. The data consists of six rows of key information:

	Case Name:	Lab Analysis using Autopsy
4	Case Number:	007
5	Number of data sources in case	1
6	Examiner:	Danyl 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.