

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 Foundations:** 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 show detailed analysis of the file: one for file artifacts, one for application data, and one for file metadata. The file metadata window shows the file is a JPEG image (application/octet-stream) with a size of 238 bytes, unallocated allocation, and was modified on 2003-02-15 14:36:00 GMT.

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 4.2.2 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/ScavvedFiles/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

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
Encryption Detected	Comment : «Passwords» 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/\$OphashFiles/_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

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 Acme 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 interface includes tabs for 'File', 'Text', 'File Metadata', 'Data Objects', '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-tij\ n [ME *cottage*, fr. (assumed) AF, fr. ME *cot* — more at *COT*] (14c) 1 : the dwelling of a farm laborer or small farmer 2 : a small frame 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 with a keyword search results window open. The search term 'password' has been entered in the search bar. The results table lists several files found in the search:

Name	Keyword Preview	Location	Modified Time	Change Time
Encryption Detected Artifact	Comment : «Passwords» protection detected.	/img_ftk-demo1-image1/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-image1/JSUnalloc/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-image1/SOphianFile/_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-image1/work/_Y_EXE	2003-02-15 14:40:34 GMT	0000-00-00 00:00:00
F0000003.tct	minute. You can find the «password» for the encrypted.	/img_ftk-demo1-image1/ScarvedFiles/1/F0000003.tct	0000-00-00 00:00:00	0000-00-00 00:00:00
mrt_bank_secrey.htm	Jttn Mr. Jones,The «password» for your account is:	/img_ftk-demo1-image1/account/data/mrt_bank_secr...	2003-02-15 13:38:36 GMT	0000-00-00 00:00:00

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

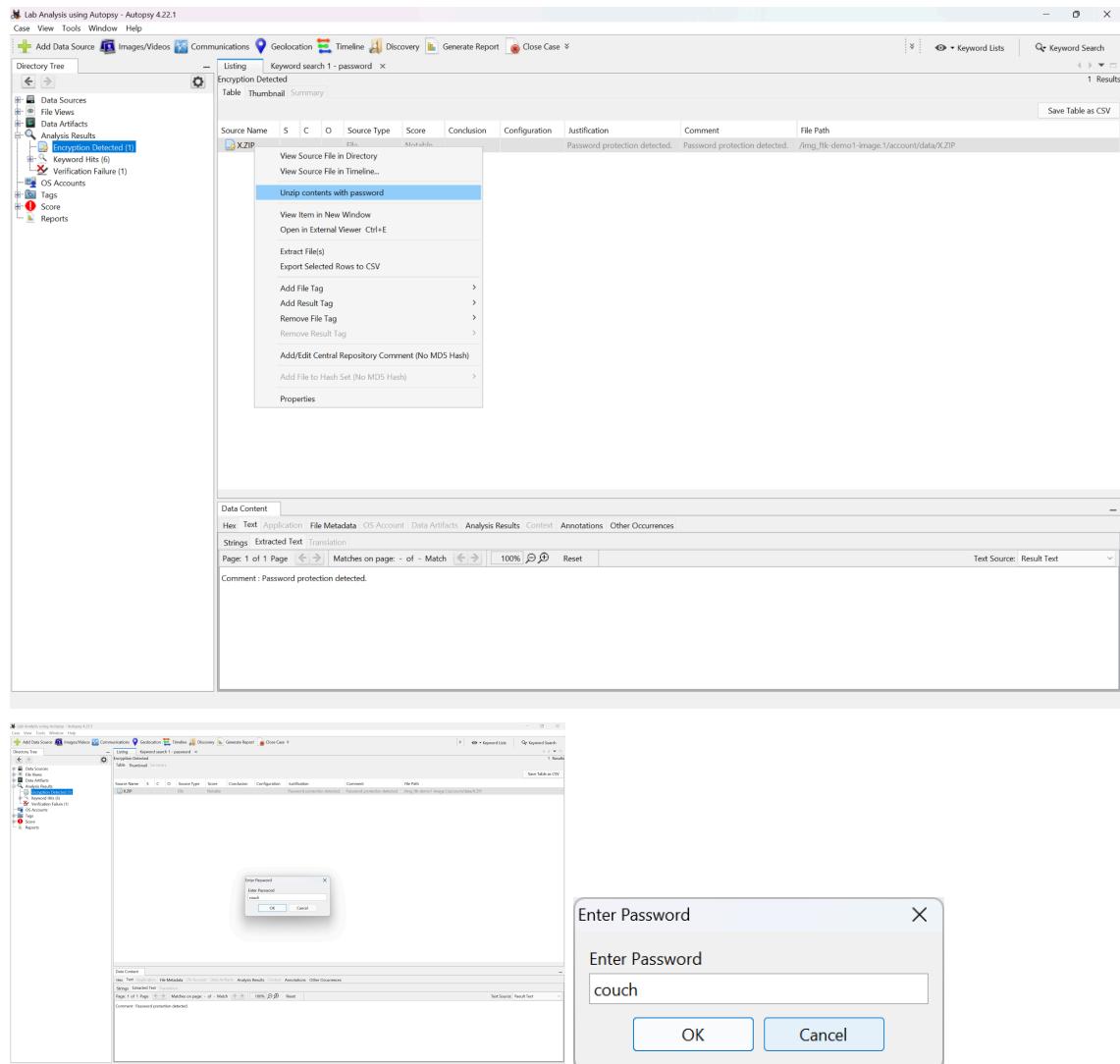
Note: step from the previous evidence, to get the password

Export File & Add Bookmark File Tag

The three screenshots show the steps involved in exporting a file and adding a bookmark tag:

- The first screenshot shows the 'File Artifacts' pane with a file selected for export.
- The second screenshot shows the 'File Artifacts' pane after the file has been successfully exported.
- The third screenshot shows the 'File Artifacts' pane with a 'Bookmark' tag added to the file.

Unzip X.ZIP with password (“couch”)



Timestamp: 21/10/2025 00:40:27

File Name: X.ZIP

Full Path: /img_ftk-demo1-image.1/account/data/X.ZIP

File extension: ZIP – Compressed Archive

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

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

SWIZZ.XLS / SWIZZ.CSV / SWIZZ.TXT

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

- Directory Tree:** Shows a hierarchy of data sources, artifacts, and analysis results. Key items include "Analysis Results" (Encryption Detected 1, Keyword Hits 6, Verification Failure 1), "OS Accounts" (OS Accounts), and "Reports".
- Listing:** A table showing file metadata for "SWIZZ.XLS". Columns include Source Name, S, C, O, Description, Owner, Data Source, Date Created, Date Modified, User ID, Program Name, and Organization.
- Metadata:** A detailed view of the file's metadata, including fields like Type, Value, and Source(s). Key entries include:
 - Type: Date Created - 2002-08-16 21:39:27 IST
 - Type: Date Modified - 2002-08-16 22:38:14 IST
 - Type: User ID - pc
 - Type: Program Name - Microsoft Excel
 - Type: Organization - The Boeing Company
 - Type: Owner - Bill Nelson
 - Type: Source File Path - /img_ftk-demo1-image1/account/data/X.ZIP/SWIZZ.XLS
 - Type: Artifact ID - -9223372036854775800
- Text Editor:** A separate window titled "/img_ftk-demo1-image1/account/data/X.ZIP/SWIZZ.XLS - Editor" displays the contents of the XLS file. The content is a bank statement from "Swiss Genève Internationale" dated February 14, 2002, showing transactions and a balance of \$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 'test/plain' view selected. The left sidebar shows various file types and artifacts. The main pane displays a table of 14 plain text files with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table includes files like msg7.txt, msg5.txt, msg4.txt, and AIL5.GIF, along with several unnamed files starting with 'f000'. The 'Known' column indicates they are unlocated, and the 'Location' column shows paths such as /img_ftk-demo1-image/1/personal/Messages/msg7.txt and /img_ftk-demo1-image/1/work/msg4.txt.

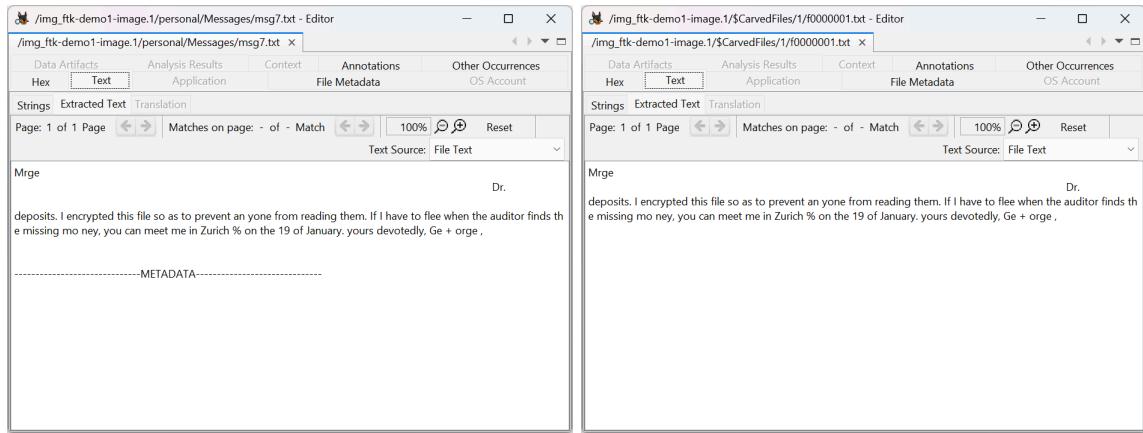
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
msg7.txt				2003-02-15 12:45:44 GMT	2000-00-00 00:00:00	2003-02-15 00:00:00 GMT	2003-02-15 15:49:35 GMT	662	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/personal/Messages/msg7.txt
msg5.txt				2003-02-15 12:44:16 GMT	2000-00-00 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	2000-00-00 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	2000-00-00 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/OrphanFile/_EST/_AIL5.GIF
f0000001.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	662	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0000001.txt
f0000003.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	506	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0000003.txt
f000052.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	119	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f000052.txt
f0001487.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	102	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0001487.txt
f0002180.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	512	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0002180.txt
f0002722.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	633	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0002722.txt
f0002728.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	3660	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0002728.txt
f0002737.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	316	Unallocated	Unallocated	unknown	/img_ftk-demo1-image/1/CarvedFiles/1/f0002737.txt
f0002738.txt	2			2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 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	2000-00-00 00:00:00	2000-00-00 00:00:00	2000-00-00 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



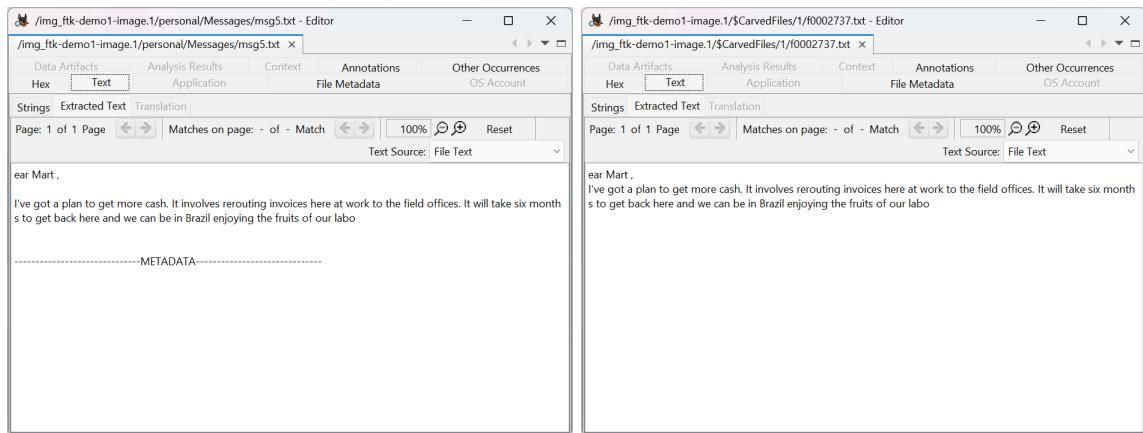
The image shows two side-by-side FTK Editor windows. Both windows have a title bar with the path '/img_ftk-demo1-image.1/personal/Messages/msg7.txt - Editor' and '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0000001.txt - Editor'. The left window displays the original file content, which includes a message from 'Mrge' to 'Dr.' about encrypting files to prevent reading by auditors. The right window shows the same message, but with some text redacted or removed, indicating the difference between the original file and the carved file.

Excerpt:

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

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

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

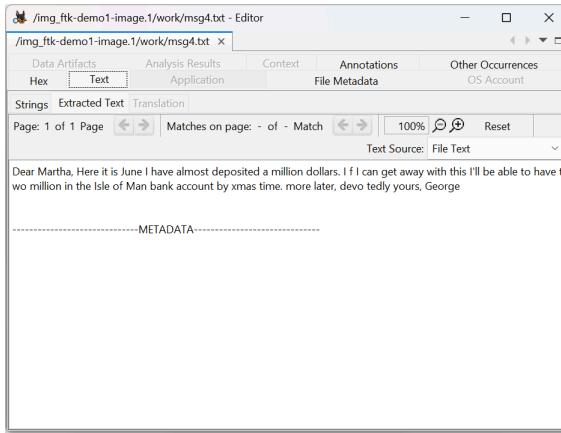


The image shows two side-by-side FTK Editor windows. Both windows have a title bar with the path '/img_ftk-demo1-image.1/personal/Messages/msg5.txt - Editor' and '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002737.txt - Editor'. The left window displays a message from 'ear Mart.' to someone about a plan to get more cash by rerouting invoices to Brazil. The right window shows the same message, but with some text redacted or removed, indicating the difference between the original file and the carved file.

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 enjoying the fruits of our labo

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

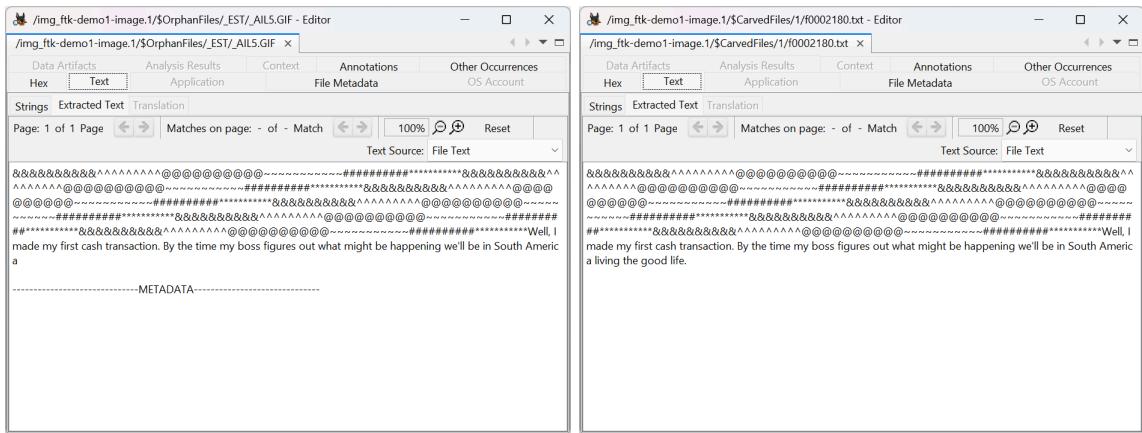
-----METADATA-----

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

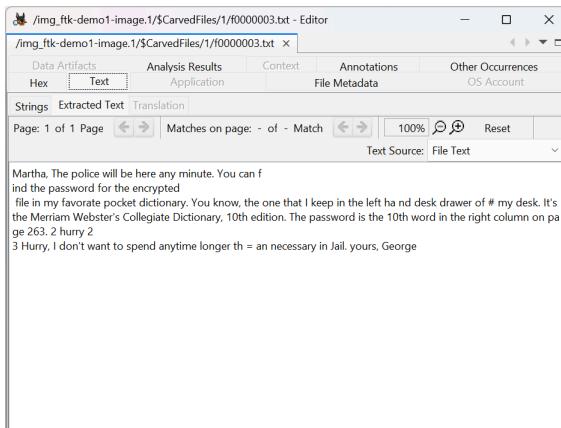


Well, I made my first cash transaction. By the time my boss figures out what might be happening we'll be in South America a living the good life.

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



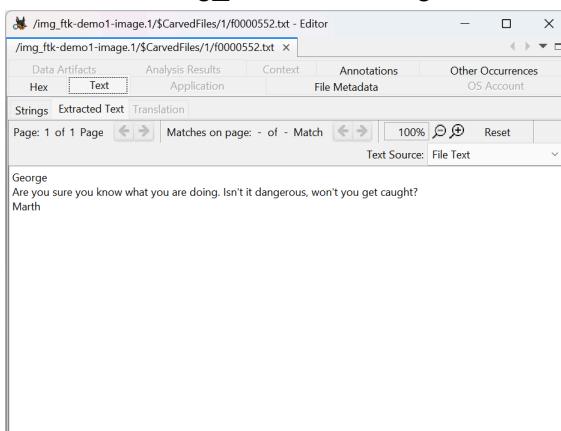
The screenshot shows the FTK Editor interface with the title bar "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0000003.txt - Editor". The "Text" tab is selected. The main pane displays the following text:

```
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:

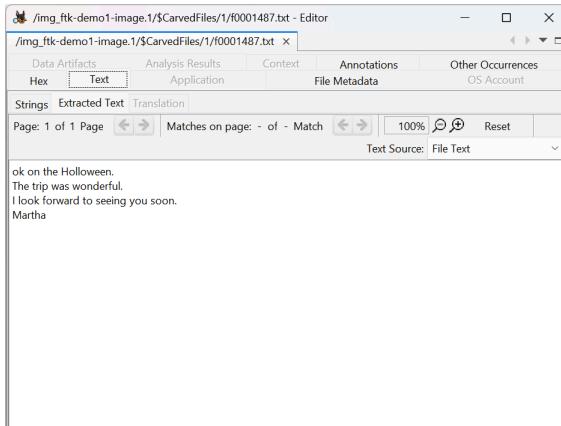
```
George  
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?  
Marth
```

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/f0001487.txt



The screenshot shows the FTK Editor interface with the title bar "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0001487.txt - Editor". The "Text" tab is selected. The main pane displays the following text:

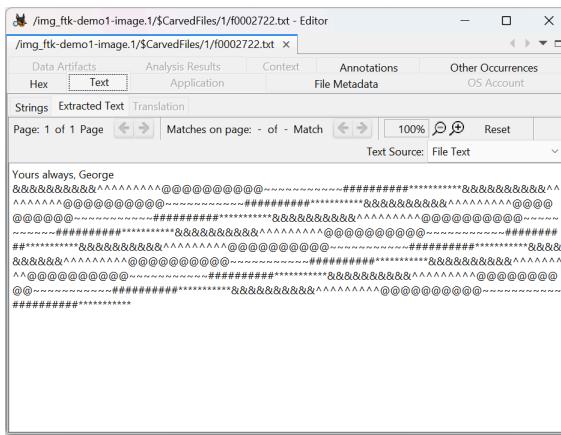
```
ok on the Holloween.  
The trip was wonderful.  
I look forward to seeing you soon.  
Martha
```

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. The left window has the title bar "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002722.txt - Editor" and the right window has the title bar "/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002738.txt - Editor". Both windows have the "Text" tab selected. The left window contains a large amount of encoded text starting with "Yours always, George" followed by a long string of characters like '&&&&&&&'. The right window contains the text "I'll tell you more about it when I get it started." followed by "Yours always, George".

Excerpt:

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

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

The screenshot shows the FTK Editor interface with the file path '/img_ftk-demo1-image.1/\$CarvedFiles/1/f0002728.txt' in the title bar. The main pane displays a large amount of text that has been heavily redacted, appearing as a grid of question marks.

Excerpt:

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

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

The screenshot shows the FTK Editor interface with the file path '/img_ftk-demo1-image.1/account/data/X.ZIP/SWISS.TXT'. The main pane displays a table of bank statement data. The columns are labeled 'Quantit de d.p't', 'Argent Total Courant', and 'Int,r't gagn, ... 6,533 pour cen t''. The table includes rows for account numbers, transaction details, and dates.

Quantit de d.p't	Argent Total Courant	Int,r't gagn, ... 6,533 pour cen t'
\$1,524.00"	\$1,623.56"	\$99.56
"		"Janvier 29, 2002"
\$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
		"A

Excerpt:

“Geneve Internationale

Autres liens

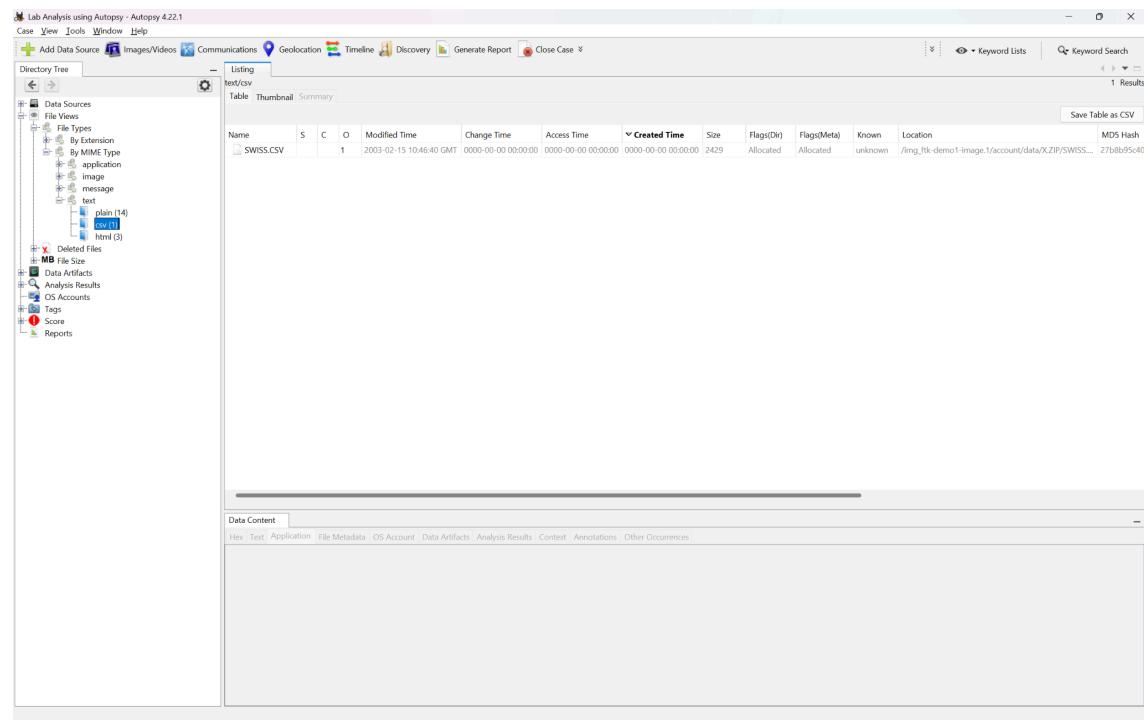
Account Number: 9882111

”

Bank Statements

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

CSV text files



The screenshot shows the Lab Analysis interface of Autopsy 4.22.1. The main window displays a file listing titled "Listing" for "text/csv". A single file, "SWISS.CSV", is listed in the table view. The table has columns for 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 sidebar with "Data Sources" and "File Types" sections, and a bottom panel titled "Data Content" with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	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																																																																														
<p>Geneve Internationale</p> <p>Autres liens</p> <p>Account Number: 9882111</p> <p>Les montants ont été énumérés en dollars des États-Unis</p> <p>Quantité de dépôt Argent Total Courant Intérêt gagné à 6,533 pour cent Date de dépôt</p> <table><thead><tr><th>Montant</th><th>Date</th></tr></thead><tbody><tr><td>\$1,524.00</td><td>Janvier 29, 2002</td></tr><tr><td>\$15,888.00</td><td>Février 14, 2002</td></tr><tr><td>\$10,566.00</td><td>Mars 12, 2002</td></tr><tr><td>\$1,547.00</td><td>Avril 13, 2002</td></tr><tr><td>\$22,014.00</td><td>Mai 13, 2002</td></tr><tr><td>\$2,035.00</td><td>Juin 10, 2002</td></tr><tr><td>\$24,450.00</td><td>Juillet 6, 2002</td></tr><tr><td>\$2,412.00</td><td>Août 23, 2002</td></tr><tr><td>\$24,186.00</td><td>Septembre 12, 2002</td></tr><tr><td>\$2,541.00</td><td>Octobre 13, 2002</td></tr><tr><td>\$2,520.00</td><td>Novembre 12, 2002</td></tr><tr><td>\$24,632.00</td><td>Décembre 2, 2002</td></tr><tr><td>\$212,588.00</td><td>Janvier 24, 2003</td></tr><tr><td>\$24,553.00</td><td>Février 10, 2003</td></tr><tr><td>\$2,455.00</td><td>Mars 7, 2003</td></tr><tr><td>\$2,892.00</td><td>Avril 4, 2003</td></tr><tr><td>\$2,353.00</td><td>Mai 22, 2003</td></tr><tr><td>\$221,450.00</td><td>Juin 15, 2003</td></tr><tr><td>\$2,380.00</td><td>Juillet 12, 2003</td></tr><tr><td>\$59,311.00</td><td>Août 23, 2003</td></tr><tr><td>\$6,548.00</td><td>Septembre 24, 2003</td></tr><tr><td>\$54,156.00</td><td>Octobre 11, 2003</td></tr><tr><td>\$1,178.00</td><td>Novembre 2, 2003</td></tr><tr><td>\$47,872.00</td><td>Décembre 3, 2003</td></tr><tr><td>\$36,548.00</td><td>Janvier 20, 2004</td></tr><tr><td>\$231,455.00</td><td>Février 13, 2004</td></tr><tr><td>\$2,080.00</td><td>Mars 10, 2004</td></tr><tr><td>\$24,863.00</td><td>Avril 14, 2004</td></tr><tr><td>\$98,765.00</td><td>Mai 3, 2004</td></tr><tr><td>\$17,893.00</td><td>Juin 12, 2004</td></tr><tr><td>\$31,400.00</td><td>Juillet 4, 2004</td></tr><tr><td>\$14,492.00</td><td>Août 1, 2004</td></tr><tr><td>\$45,789.00</td><td>Septembre 22, 2004</td></tr><tr><td>\$34,447.00</td><td>Octobre 10, 2004</td></tr><tr><td>\$29,833.00</td><td>Novembre 3, 2004</td></tr><tr><td>\$68,845.00</td><td>Décembre 4, 2004</td></tr></tbody></table> <p>-----</p> <p>METADATA</p> <p>Content-Encoding: windows-1252 Content-Type: application/x-msexcel; charset=windows-1252; delimiter=comma X-Tika-detected-By: org.apache.tika.parser.DefaultParser X-Tika-detected-encoding: windows-1252 X-Tika-encodingDetector: UniversalEncodingDetector csv.delimiter: comma csv.num_columns: 5</p>	Montant	Date			\$1,524.00	Janvier 29, 2002	\$15,888.00	Février 14, 2002	\$10,566.00	Mars 12, 2002	\$1,547.00	Avril 13, 2002	\$22,014.00	Mai 13, 2002	\$2,035.00	Juin 10, 2002	\$24,450.00	Juillet 6, 2002	\$2,412.00	Août 23, 2002	\$24,186.00	Septembre 12, 2002	\$2,541.00	Octobre 13, 2002	\$2,520.00	Novembre 12, 2002	\$24,632.00	Décembre 2, 2002	\$212,588.00	Janvier 24, 2003	\$24,553.00	Février 10, 2003	\$2,455.00	Mars 7, 2003	\$2,892.00	Avril 4, 2003	\$2,353.00	Mai 22, 2003	\$221,450.00	Juin 15, 2003	\$2,380.00	Juillet 12, 2003	\$59,311.00	Août 23, 2003	\$6,548.00	Septembre 24, 2003	\$54,156.00	Octobre 11, 2003	\$1,178.00	Novembre 2, 2003	\$47,872.00	Décembre 3, 2003	\$36,548.00	Janvier 20, 2004	\$231,455.00	Février 13, 2004	\$2,080.00	Mars 10, 2004	\$24,863.00	Avril 14, 2004	\$98,765.00	Mai 3, 2004	\$17,893.00	Juin 12, 2004	\$31,400.00	Juillet 4, 2004	\$14,492.00	Août 1, 2004	\$45,789.00	Septembre 22, 2004	\$34,447.00	Octobre 10, 2004	\$29,833.00	Novembre 3, 2004	\$68,845.00	Décembre 4, 2004		
Montant	Date																																																																													
\$1,524.00	Janvier 29, 2002																																																																													
\$15,888.00	Février 14, 2002																																																																													
\$10,566.00	Mars 12, 2002																																																																													
\$1,547.00	Avril 13, 2002																																																																													
\$22,014.00	Mai 13, 2002																																																																													
\$2,035.00	Juin 10, 2002																																																																													
\$24,450.00	Juillet 6, 2002																																																																													
\$2,412.00	Août 23, 2002																																																																													
\$24,186.00	Septembre 12, 2002																																																																													
\$2,541.00	Octobre 13, 2002																																																																													
\$2,520.00	Novembre 12, 2002																																																																													
\$24,632.00	Décembre 2, 2002																																																																													
\$212,588.00	Janvier 24, 2003																																																																													
\$24,553.00	Février 10, 2003																																																																													
\$2,455.00	Mars 7, 2003																																																																													
\$2,892.00	Avril 4, 2003																																																																													
\$2,353.00	Mai 22, 2003																																																																													
\$221,450.00	Juin 15, 2003																																																																													
\$2,380.00	Juillet 12, 2003																																																																													
\$59,311.00	Août 23, 2003																																																																													
\$6,548.00	Septembre 24, 2003																																																																													
\$54,156.00	Octobre 11, 2003																																																																													
\$1,178.00	Novembre 2, 2003																																																																													
\$47,872.00	Décembre 3, 2003																																																																													
\$36,548.00	Janvier 20, 2004																																																																													
\$231,455.00	Février 13, 2004																																																																													
\$2,080.00	Mars 10, 2004																																																																													
\$24,863.00	Avril 14, 2004																																																																													
\$98,765.00	Mai 3, 2004																																																																													
\$17,893.00	Juin 12, 2004																																																																													
\$31,400.00	Juillet 4, 2004																																																																													
\$14,492.00	Août 1, 2004																																																																													
\$45,789.00	Septembre 22, 2004																																																																													
\$34,447.00	Octobre 10, 2004																																																																													
\$29,833.00	Novembre 3, 2004																																																																													
\$68,845.00	Décembre 4, 2004																																																																													

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 an 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 window displays an email 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 MSG files (m-021230.msg, g-021218.msg, g-021229.msg, m-021220.msg) with various metadata. Below the listing 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 a blank page area.

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...

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 address bar '/img_ftk-demo1-image.1/personal/Messages/g-021218.msg'.
The left window's content pane shows two messages:

- A message from 'Martha' containing the text: 'I have a plan to pay for our vaction next Spring. I'll tell you about it later.'
- A message from 'George'.

The right window's content pane shows the message body:

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 shows two side-by-side windows of the FTK (Forensic Toolkit) software. Both windows are titled '/img_ftk-demo1-image.1/personal/Messages/g-021229.msg - Editor'.

Left Window (Content View):

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

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

Right Window (Metadata View):

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

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
dc:creator: Jones
dc:subject: 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

The image displays two side-by-side windows of the FTK (Forensic Toolkit) software interface, both titled "/img_ftk-demo1-image.1/personal/Messages/m-021230.msg - Editor".
The left window is focused on the "Text" tab of the "Data Artifacts" panel. It shows the message body with the following content:
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
The right window is also focused on the "Text" tab of the "Data Artifacts" panel. It shows the message body with the same content as the left window, followed by a "METADATA" section:
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
dcreator: James
dcsubject: REA plan
dctitle: REA plan
resourceName: REA plan.eml

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.