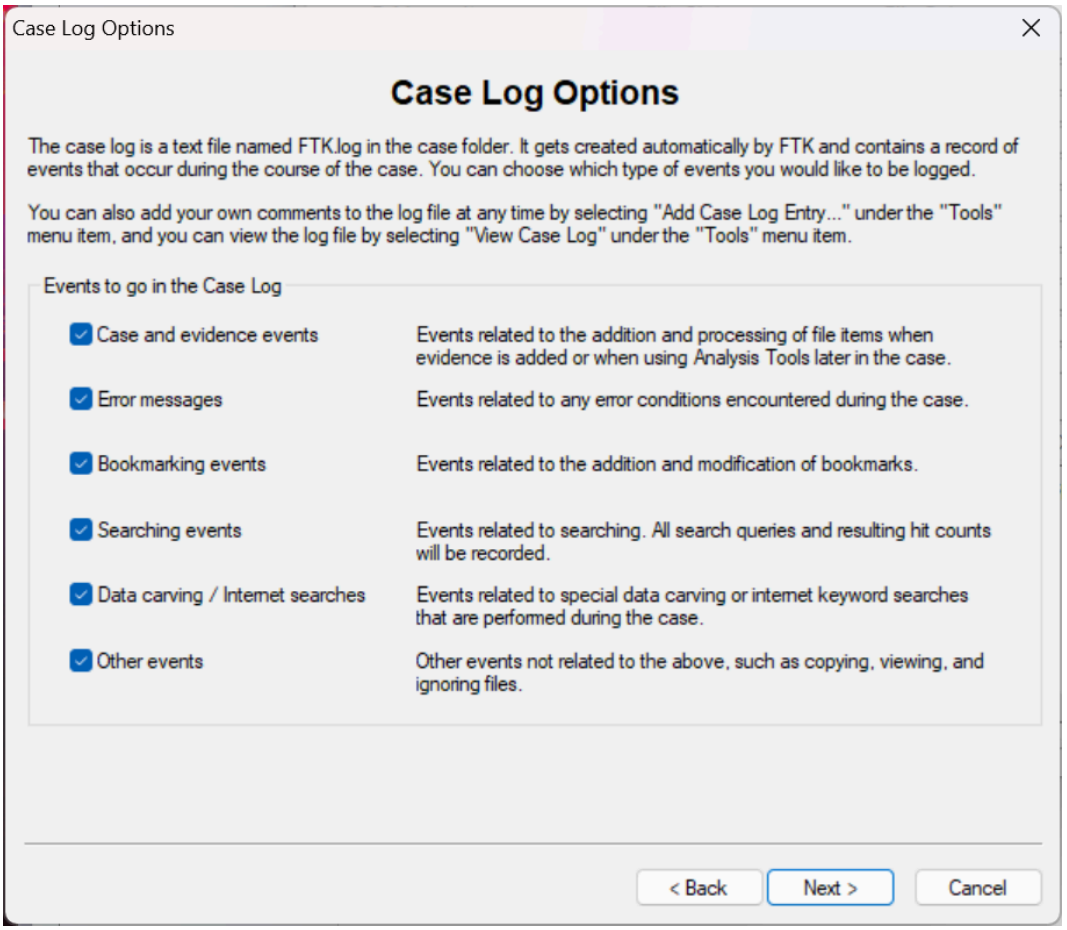
Computer & Network Forensics

Week 5 (Lab3)

Introduction to Forensics Analysis using FTK

Questions

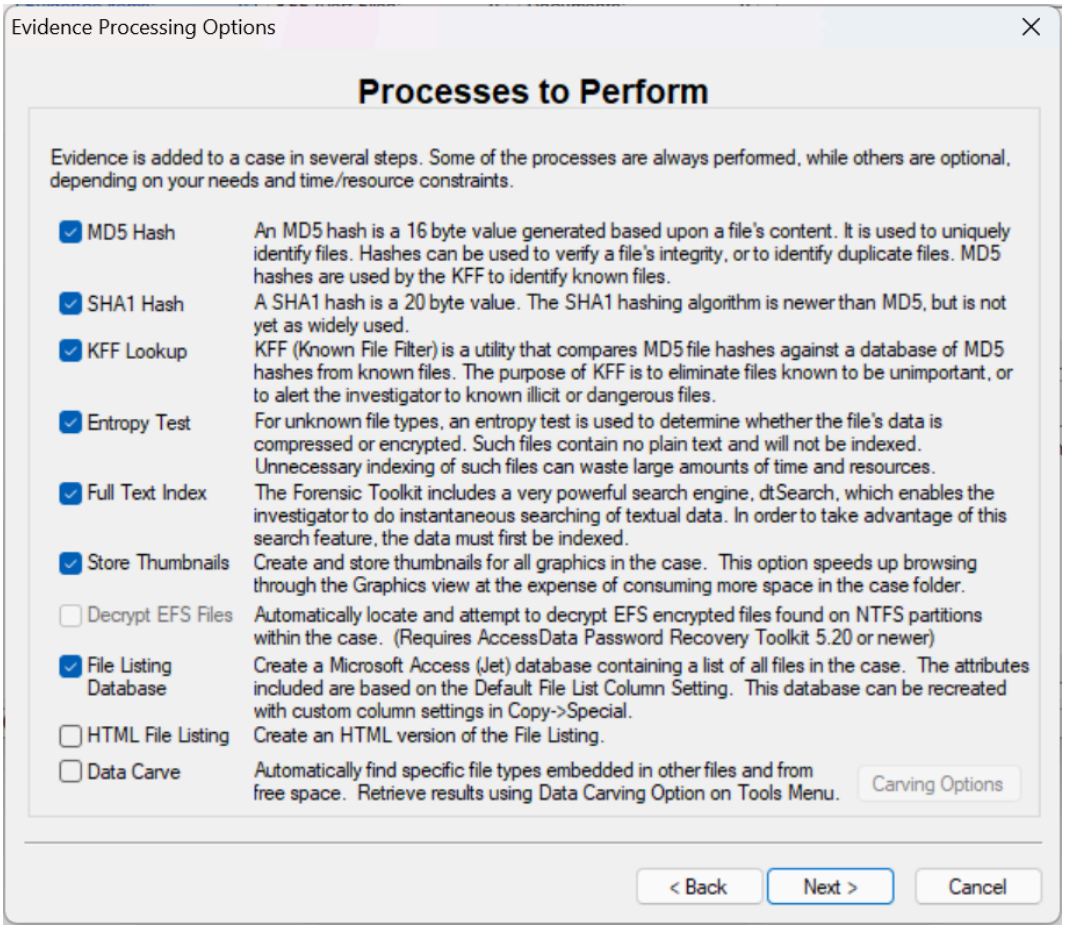
1. Case Log Options



1. **What is the format of the FTK.log file?**
   The FTK.log file is a text file created automatically by FTK in the case folder. It is stored in plain text (.log) format and can be opened and viewed with any text editor.

2. **What is a log file used for?**
   A log file is used to record a detailed history of events and actions that occur during a forensic case. It provides an audit trail showing what was done, when, and by whom – useful for documentation, verification, and accountability.
3. **What kind of events can be recorded in a log file?**
   - Case and evidence events (when evidence is added or processed)
   - Error messages
   - Bookmarking events
   - Searching events (all search queries and hit counts)
   - Data carving / Internet search events
   - Other events (e.g., copying, viewing, or ignoring files)
4. **How can you add comments to a log file?**
   Comments can be added by selecting “Add Case Log Entry…” under the Tools menu in FTK.
5. **List 3 events that can go in a Case Log.**
   - Adding or processing evidence files
   - Recording search queries and results
   - Logging error messages or warnings

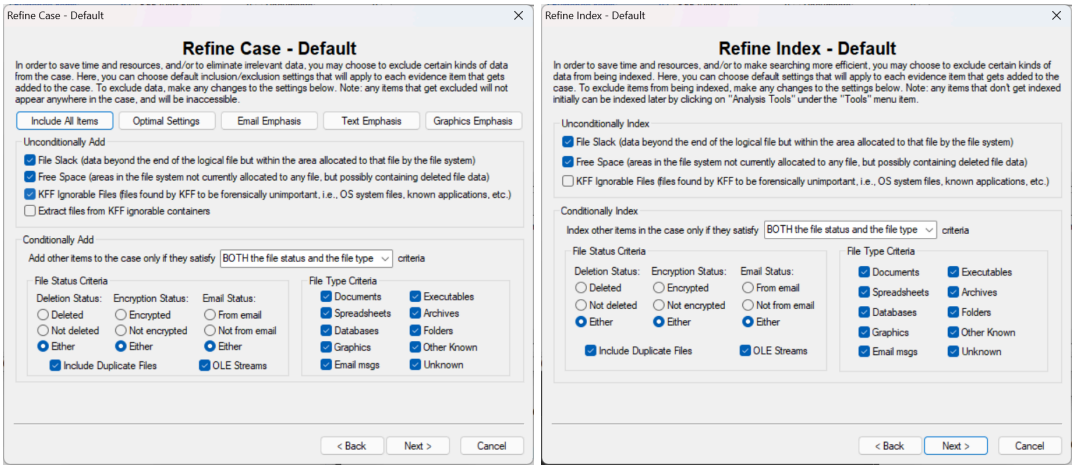
2. Process to Perform



1. **How many bits in a MD5 and SHA1 key? List 3 other Hash Algorithms**
    - MD5: 128 bits (16 bytes)
    - SHA-1: 160 bits (20 bytes)
    - Other hash algorithms: SHA-256, SHA-512, CRC32
2. **What is the function of the KFF utility?**
   The KFF (Known File Filter) utility compares MD5 file hashes against a database of known file hashes.
   Its main purpose is to:
    - Eliminate files known to be unimportant (like standard system files).
    - Identify known illicit or dangerous files by matching their hashes to known bad entries.
3. **What is an Entropy Test?**
   An entropy test is used to measure the randomness of data in a file.
    - It helps determine whether a file's data is compressed or encrypted.
    - Files with high entropy likely contain encrypted or compressed data and therefore contain no plain text, meaning they will not be indexed by FTK.
4. **How can we check if a file is compressed?**
    - Running an entropy test — high entropy indicates compression or encryption.
    - Checking the file header or extension (e.g., .zip, .rar, .gz).
    - Looking at FTK's file details or properties (FTK identifies compressed files during analysis).
5. **Why does data need to be indexed?**
   Data is indexed to enable fast and efficient keyword searching.
   FTK uses its built-in search engine (dtSearch) to quickly locate text or data across all files.
   Without indexing, searches would be very slow because FTK would need to scan each file individually.
6. **What does HTML File Listing function do?**
   The HTML File Listing function creates an HTML version of the file listing – a browsable webpage that shows all files and their metadata.
   This allows examiners or reviewers to view the case contents in a browser without using FTK.
7. **What is a thumbnail?**
   A thumbnail is a small preview image automatically generated for each picture file in the case.
   It allows the examiner to quickly view and identify images without opening each one individually.
   FTK stores these thumbnails to speed up browsing in the Graphics view.
8. **What other types of databases can be used to store lists of files?**
   FTK uses a Microsoft Access (Jet) database for file listings, but other databases can also be used, such as: MySQL, PostgreSQL, SQLite

9. **What is data carving? “Research further”**
   Data carving is the forensic process of recovering files from unallocated or free space on a disk by searching for known file signatures (headers and footers).
   It does not rely on file system metadata – instead, it reconstructs files based on their binary patterns.
   This technique is especially useful for recovering deleted, damaged, or partially overwritten files.

3. Refine Case - Default



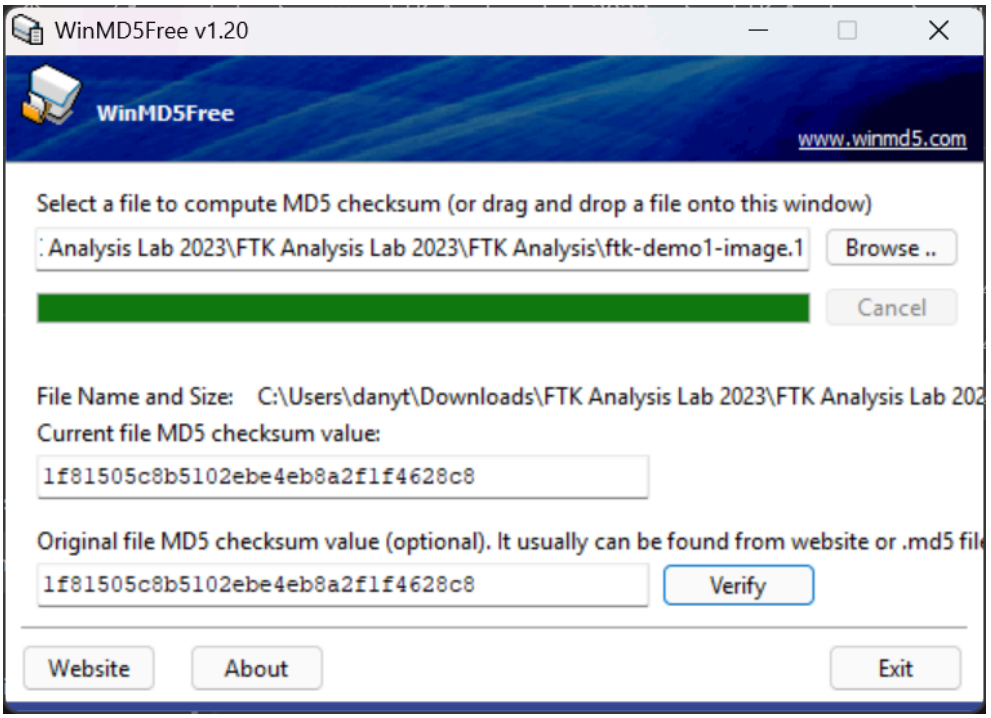
1. **What are the options for excluding certain kinds of data?**
   - File Slack: Data beyond the end of a logical file but still within the allocated cluster.
   - Free Space: Unallocated areas of the file system that may still contain deleted data.
   - KFF Ignorable Files: Files identified by the Known File Filter as forensically unimportant (e.g., system or common application files).
   - Conditional filters:
     - File Status (deleted, encrypted, email-related).
     - File Type (documents, graphics, executables, archives, etc.).
     - Duplicate files (optionally include or exclude duplicates).

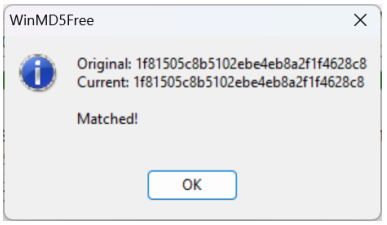
2. **What is the difference Slack Space and Free Space? Expand your answer with additional research.**
   Slack space exists within allocated clusters of existing files, while free space consists of unallocated clusters that can still hold recoverable deleted data.

Aspect	**Slack Space**	**Free Space**
Definition	The unused area within an allocated cluster after the end of a file's actual data	Disk space not currently assigned to any file or folder
Location	Inside the last cluster of an existing file	Outside of allocated files – part of unallocated disk area
Created When	A file does not completely fill its last cluster (e.g., file size = 6 KB, cluster size = 8 KB → 2 KB slack)	Files are deleted, partitions formatted, or space never used
Contents	May contain fragments of old data from previously stored files	May contain full deleted files or remnants of earlier data
Forensic Value	Useful for finding hidden data fragments inside active files	Useful for data carving and recovering entire deleted files

3. **What utility compares file hashes against a reference database to eliminate known files?**
   It matches the hash values of files in the case against a database of known good or known bad hashes to:
   - Automatically exclude common system files (known good).
   - Identify known illegal or malicious files (known bad).
4. **What is difference between File Status and File Type?**
   - File Status – Describes the current state or condition of a file within the file system. *(tells how the file exists)*
     - Deleted, Encrypted, From Email, etc.
   - File Type – Describes the kind or format of the file, determined by its content or extension. *(tells what the file is)*
     - Documents (.docx, .pdf), Executables (.exe), Archives (.zip), Graphics (.jpg)

4. Verify Data Integrity





Computer & Network Forensics

Week 5 (Lab3) – Report

Introduction to Forensics Analysis using FTK

FTK Forensic Analysis Report

Name: Danyil Tymchuk
Date: 13/10/2025
Case Name: FTK Lab
Tool Used: AccessData Forensic Toolkit (FTK)

- **For Investigate Foundings:** Internet Archive (archive.org), Microsoft Excel and Windows Notepad

Introduction

This report documents the digital forensic examination of a sample image file (ftk-demo1-image.1) performed using AccessData Forensic Toolkit (FTK) between 13 October 2025 and 17 October 2025.
The purpose of this analysis was to identify, recover, and interpret digital evidence relating to potential financial misconduct and data concealment by two suspects, George Jones and Martha James, Steve Billings's employees.

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

What am I doing?

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

Contents

Objective

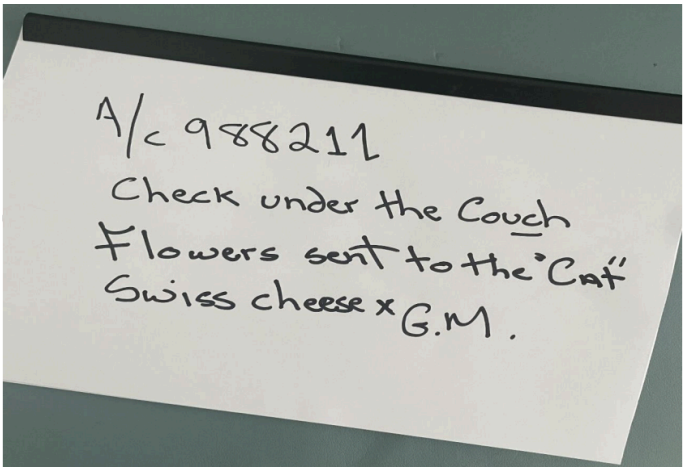
By following these guidelines and documenting my forensic analysis thoroughly, I will create a credible and informative forensic report. This report will not only serve as a record of my investigation but also as a valuable resource for presenting my findings and insights to others involved in the case.

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

Discovery of Evidence

In the case of George Montgomery, Steve found:

- Three unused vape devices.
- Links to online gaming websites.
- Tik-Tok search for “hard drive wipe”.
- Google Search for “Cat Adoption Dublin”.
- Microsoft Bing Search “florist in Blanchardstown”.
- Google Translate with text translated from French.
- Access to a website regarding Geneva.
- Handwritten documents (one displayed below) relating to a supplier based in Switzerland with whom Steve himself had previous dealings.



Steve had his IT person access the PC used by George and they discovered all data on the C/Drive and Cloud had been deleted by George. Additionally, a Memory Stick labelled with the former supplier's name and a 4-digit code (2398) was discovered taped under the desk used by George.

Chain of Custody

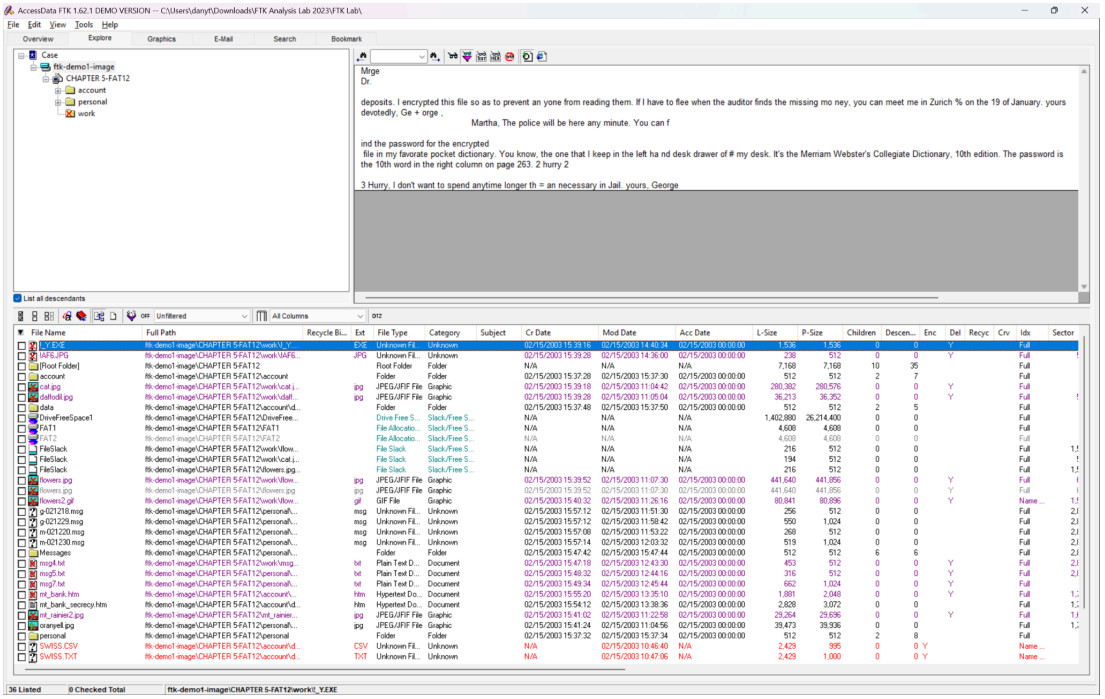
Date / Time	Action	Handled By
13/10/2025 – 15/10/2025	Analysis Period	Danyil Tymchuk
17/10/2025 09:00 – 12:00	Case Closure	Danyil Tymchuk

Summary of Collected Evidence

Evidence No.	File Name / Type	Description	Relevance
1	`!_Y.EXE` (deleted)	Deleted message referencing missing funds and Zurich meeting; password clue.	Establishes intent and encryption method.
2	`!AF6.JPG` (deleted)	Image with message from Martha expressing concern.	Confirms awareness and complicity.
3	`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.
4	`msg4.txt` (deleted), `msg5.txt` (deleted), `msg7.txt` (deleted)	Deleted text messages about embezzlement and offshore transfers.	Confirms fraud, intent to conceal.
5	`mt_bank_secrecy.htm`	Message confirming password “couch” and Isle of Man bank link.	Links to offshore account and encryption.
6	`X.ZIP` (encrypted) `[SWISS.XML, SWISS.TXT, SWISS.CSV]` (encrypted)	Encrypted ZIP with Swiss financial statements (Account No. 9882111).	Proof of hidden assets totaling about $3.9M.

Findings

Evidence #1 Encrypted Message File



Timestamp: 13/10/2025 23:54:52
File Name: !_Y.EXE
Full Path: ftk-demo1-image\CHAPTER 5-FAT12\work\!_Y.EXE
File extension: EXE – Executable File (contains embedded text message)
MAC: (Cr) 02/15/2003 15:39:16 (Mod) 02/15/2003 14:40:34 (Acc) 02/15/2003 00:00:00

Description:

Upon examination of the file `!_Y.EXE`, FTK revealed a hidden or embedded text message between Martha and George. The message indicates an attempt to conceal financial information by encrypting data and planning to flee the country.

<u>The decrypted content (visible in FTK's text view) reads in part:</u>
"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 19th of January… The password is the 10th word in the right column on page 263 of the Merriam Webster's Collegiate Dictionary, 10th edition."

Analysis:

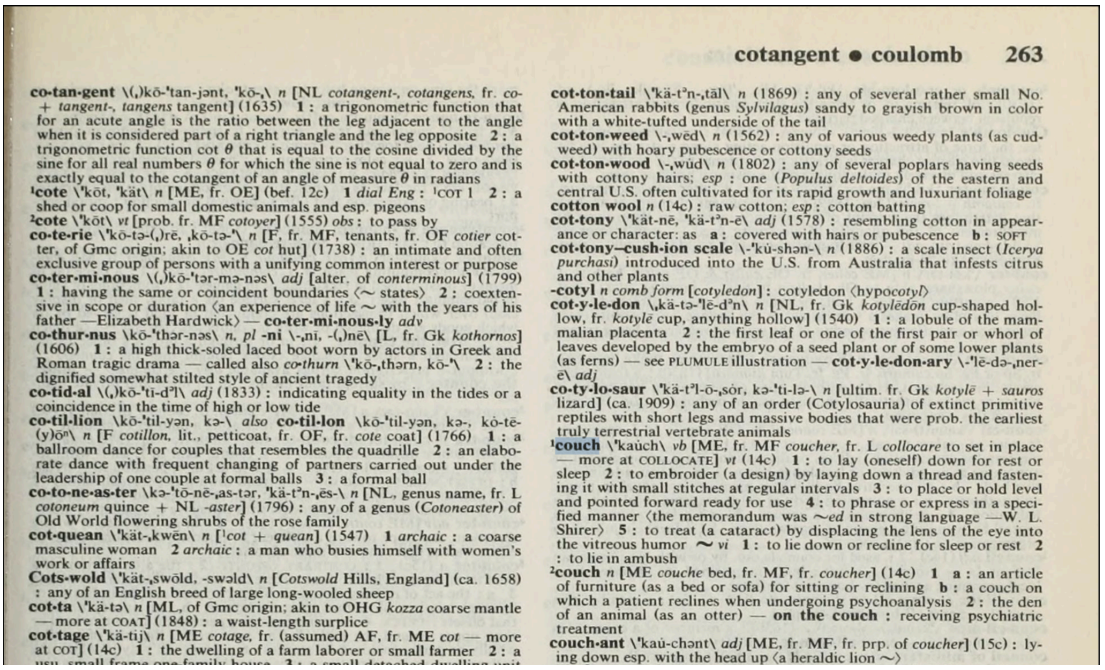
The message suggests deliberate concealment of data and coordination between Martha and George to avoid detection. The reference to an encryption password hidden in a physical dictionary implies premeditation and an effort to hide information outside the digital domain.

Relevance:

This file is a critical piece of evidence, as it directly references:

- The missing money is under investigation.
- A planned escape to Zurich, suggesting intent to flee.
- An encryption scheme used to hide incriminating data.
- A potential password (“couch”) for decrypting other evidence files.

Merriam Webster’s Collegiate Dictionary, 10th edition



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

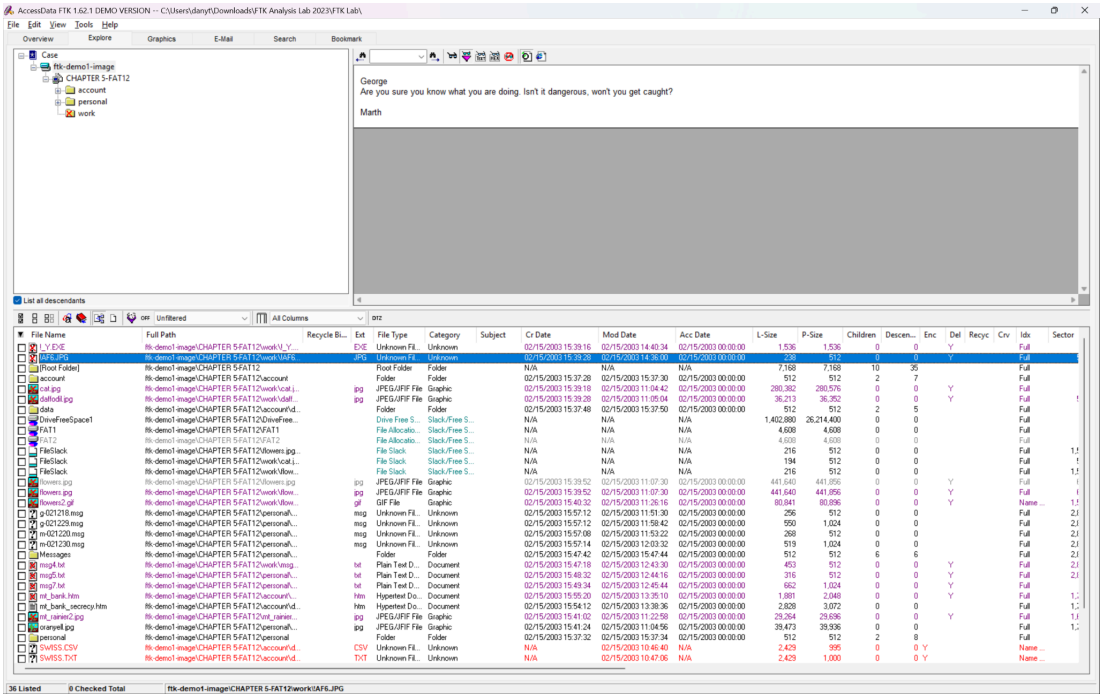
²couch *n* [ME *couche* bed, fr. MF, fr. *coucher*] (14c) **1 a** : an article of furniture (as a bed or sofa) for sitting or reclining **b** : a couch on which a patient reclines when undergoing psychoanalysis **2** : the den of an animal (as an otter) — **on the couch** : receiving psychiatric treatment

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

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

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

Evidence #2 Image Containing Questioning Message



Timestamp: 14/10/2025 00:05:07
File Name: !AF6.JPG
Full Path: ftk-demo1-image\CHAPTER 5-FAT12\work\!AF6.JPG
File extension: JPG – JPEG image (Graphics)

Description:

The image file !AF6.JPG contains a short textual message from Martha to George.
<u>The visible text reads:</u>
“George
Are you sure you know what you are doing. Isn't it dangerous, won't you get caught?
Marth”

Analysis:

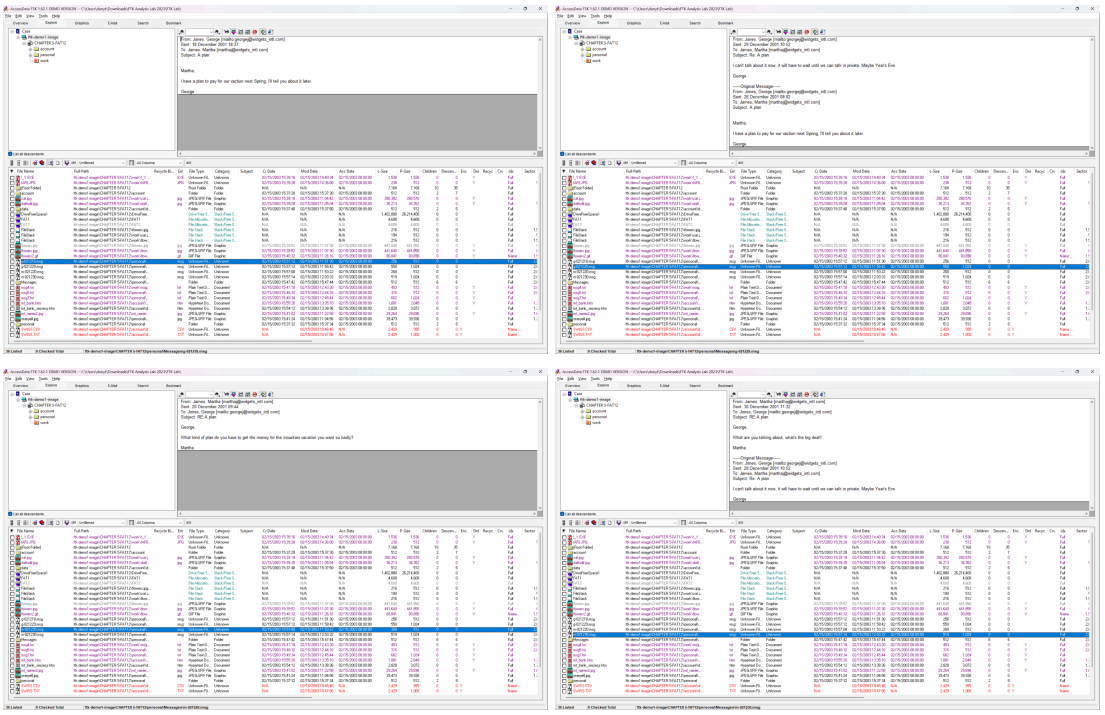
Although brief, this image provides direct evidence of Martha expressing concern about George’s actions. The phrasing implies that Martha was aware of potentially risky or illicit behavior and feared detection.

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 #3 Email Correspondence Between George and Martha



Timestamp: 14/10/2025 00:06:52
Full Path:

- ftk-demo1-image\CHAPTER 5-FAT12\personal\Messages\g-021218.msg
- ftk-demo1-image\CHAPTER 5-FAT12\personal\Messages\g-021220.msg
- ftk-demo1-image\CHAPTER 5-FAT12\personal\Messages\g-021229.msg
- ftk-demo1-image\CHAPTER 5-FAT12\personal\Messages\g-021230.msg

File extension: msg – Microsoft Outlook Message Files
Date Range: 18 December 2001 – 30 December 2001

Description:

A series of internal email messages were recovered between George Jones (georgej@widgets_intl.com) and Martha James (marthaj@widgets_intl.com) discussing what George refers to as *“a plan”*.

- 18 & 26 Dec 2001: George writes, *“I have a plan to pay for our vaction next Spring. I'll tell you about it later.”*
- 20 Dec 2001: Martha replies, *“What kind of plan do you have to get the money for the mountain vacation you want so badly?”*
- 29 Dec 2001: George responds, “I can't talk about it now, it will have to wait until we can talk in private. Maybe Year's Eve.”
- 30 Dec 2001: Martha follows up, “What are you talking about, what's the big deal?”

Analysis:

These emails demonstrate an ongoing private conversation between the two employees regarding a financial plan that George was unwilling to discuss electronically.

The phrase *“plan to pay for our vacation”* and the insistence on discussing it *“in private”* suggest that the plan may have been illicit or confidential, likely connected to the missing funds mentioned in other evidence.

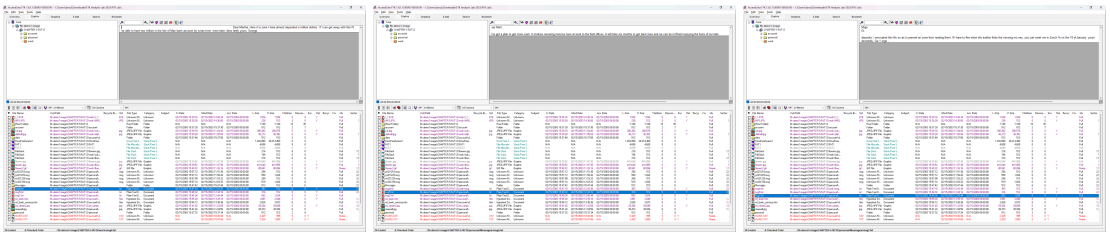
The timing of the emails – late December 2001 – aligns closely with the period leading up to the Zurich meeting mentioned in the encrypted note, reinforcing their involvement in coordinated activity.

Relevance:

This evidence establishes:

- A personal and confidential relationship between Martha and George.
- Early discussion of financial matters prior to the disappearance of funds.
- Evidence that both parties were aware and involved in a possible scheme.

Evidence #4 Deleted Text Messages



Timestamp: 14/10/2025 00:08:38
Full Path:

- ftk-demo1-image\CHAPTER 5-FAT12\work\msg4.txt (Deleted)
- ftk-demo1-image\CHAPTER 5-FAT12\personal\Messages\msg5.tx (Deleted)
- ftk-demo1-image\CHAPTER 5-FAT12\personal\Messages\msg7.txt (Deleted)

File extension: txt – Plain text

msg4.txt — excerpt / description

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

Description & Analysis:
This deleted file is a direct admission of large-scale embezzlement or misappropriation. The author (George) states he has deposited approximately one million dollars and plans to move funds to an Isle of Man bank account, indicating concealment of assets offshore. This is corroborative of the encrypted note and the email correspondence that mentioned a private *“plan”*.

Relevance:
Strongly indicates illegal diversion of funds and intent to conceal proceeds overseas. Highly probative for the investigation.

msg5.txt — excerpt / description

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...”

Description & Analysis:
This deleted message contains an operational description of how George intended to divert company funds – specifically, rerouting invoices to field offices to siphon money over time. The mention of a six-month timeframe and escape to Brazil indicates planning and premeditation.

Relevance:
Provides a likely method of the fraud (invoice rerouting) and timeline for the scheme; useful for correlating with accounting records, invoice logs, and network/access timestamps.

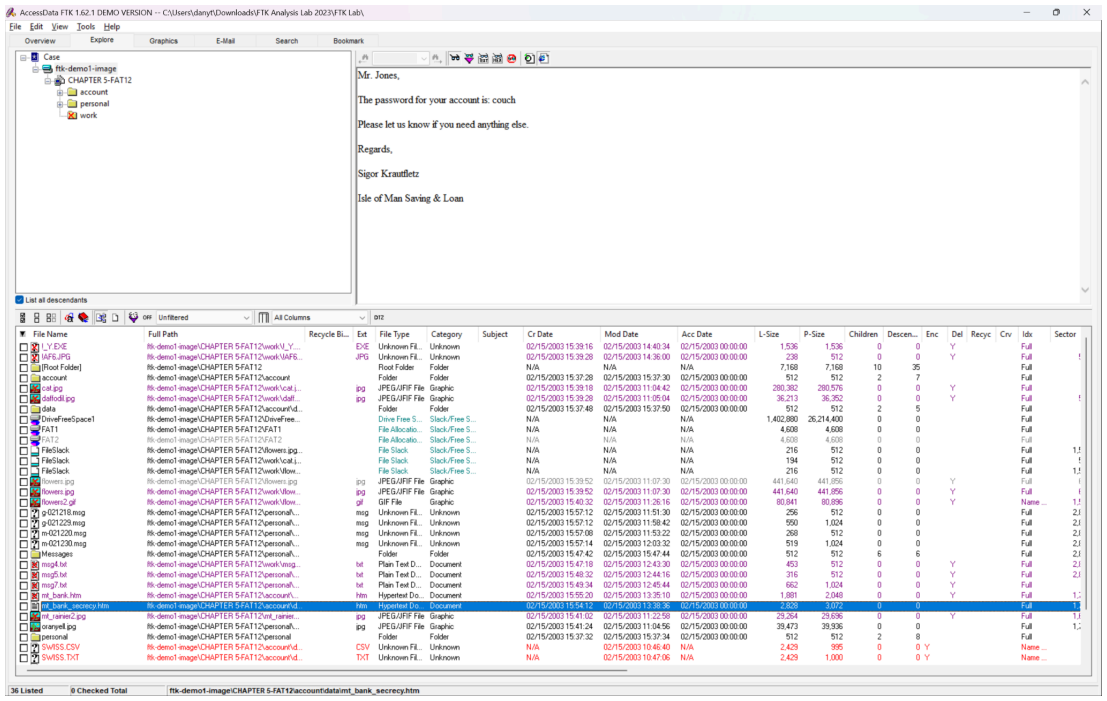
msg7.txt — excerpt / description

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

Description & Analysis:
This deleted file is essentially the same content as the previously noted *!_Y.EXE* message and reaffirms: (1) encrypted deposits exist, (2) a contingency plan to flee, and (3) a rendezvous in Zurich on 19 January. This file confirms coordination and contingency planning between George and the co-conspirator (Martha).

Relevance:
Corroborates earlier evidence (*!_Y.EXE* message and email thread) and strengthens the inference that encryption and planned flight were part of the scheme.

Evidence #5 Message From Bank



Timestamp: 14/10/2025 00:14:36
File Name: mt_bank_secrecy.htm
Full Path: ftk-demo1-image\CHAPTER 5-FAT12\account\data\mt_bank_secrecy.htm
File extension: htm – Hypertext Document

Description:

This file is an email-style message addressed to Mr. Jones (George Jones).

The text reads:
“Mr. Jones,
The password for your account is: couch
Please let us know if you need anything else.
Regards,
Sigor Krautfeltz
Isle of Man Saving & Loan”

Analysis:

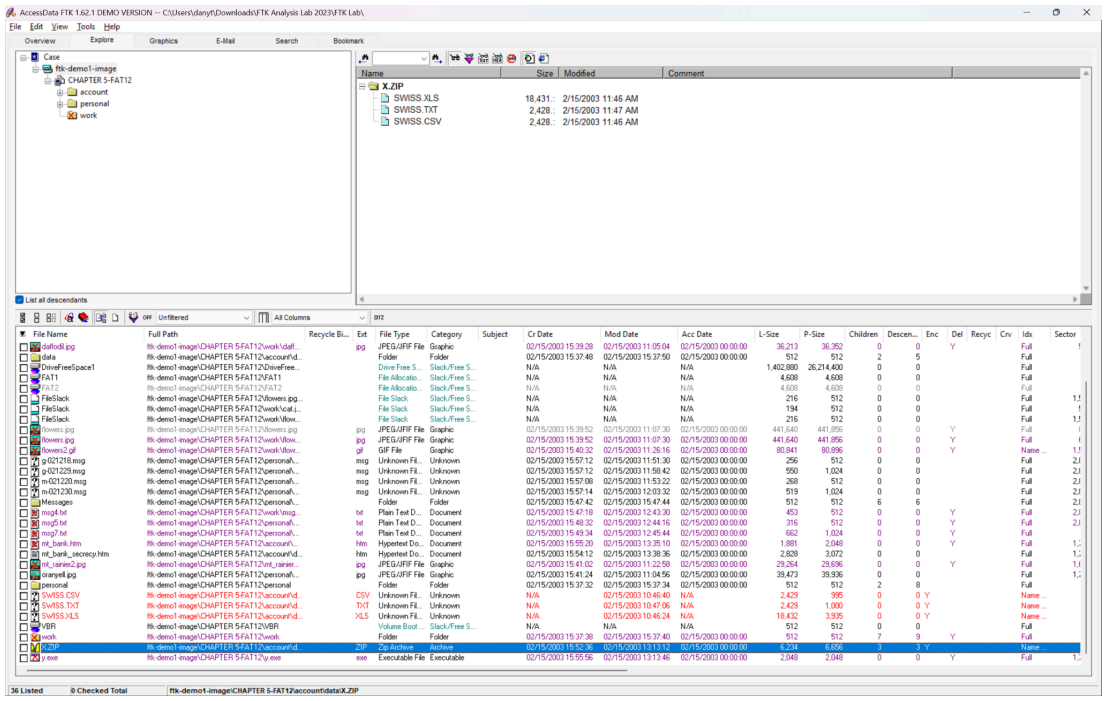
This message confirms that the account password is “couch”, matching the dictionary clue found in the encrypted *!_Y.EXE* file. The sender, Sigor Krautfeltz, appears to represent the Isle of Man Saving & Loan, which aligns with the previously recovered deleted message (*msg4.txt*) referencing the transfer of over one million dollars to an Isle of Man bank account.

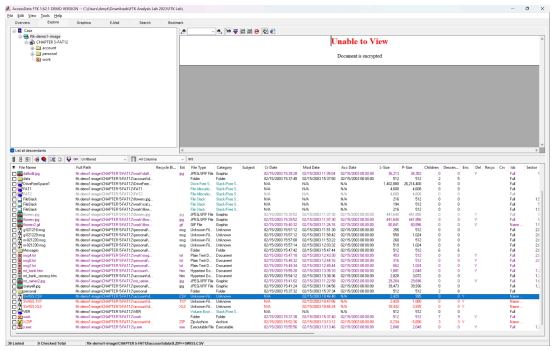
This demonstrates a direct link between George Jones and an offshore bank, and verifies that “couch” was the legitimate password used for his account. It also provides clear evidence that the parties were attempting to hide funds overseas, confirming the suspicions raised by other evidence (emails, deleted notes, and encrypted files).

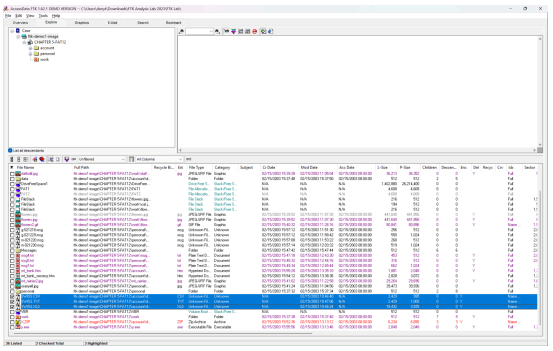
Relevance:

- Confirms “couch” as the password to the offshore account.
- Connects George Jones directly to the Isle of Man Savings & Loan institution.
- Corroborates statements in earlier deleted files (*msg4.txt* and *!_Y.EXE*).
- Provides strong evidence of financial concealment and fraudulent intent.

Evidence #6 Encrypted Zip Archive Containing Swiss Bank Records







Timestamp: 14/10/2025 00:18:28
File Name: X.ZIP
Full Path: ftk-demo1-image\CHAPTER 5-FAT12\account\data\X.ZIP
File extension: ZIP– Compressed Archive
Contained Files:

- SWISS.XML
- SWISS.TXT
- SWISS.CSV

Encryption: Password-protected; successfully opened using password “couch” derived from prior evidence (*bank_secrecy.htm* and *!_Y.EXE*).

Description:

The archive *X.ZIP* contains three files — SWISS.CSV, SWISS.TXT, and SWISS.XLS — all detailing financial transactions in a Swiss bank account identified as:

- **Account Number:** 9882111
- **Institution:** Geneve Internationale (Geneva International)
- **Currency:** USD (United States Dollars)

Each record lists deposits, interest accrued, and running totals between January 2002 and December 2004, entirely in French. The columns include:

Deposit Amount (USD)	Total Balance (USD)	Interest Earned	Deposit Date
$1,524.00	$1,623.56	$99.56	29 Jan 2002
$15,888.00	$18,655.59	$1,037.96	14 Feb 2002
…	…	…	…
$68,945.00	$3,898,678.00	$4,504.18	4 Dec 2004

Over time, the deposits and interest show a steady increase in balance, reaching approximately $3.9 million USD by late 2004.

Analysis:

This encrypted archive directly corroborates statements found in earlier deleted files (*msg4.txt* and *msg5.txt*), where George Jones described secretly depositing money and transferring funds to a bank account in the Isle of Man and Switzerland.

The reuse of the password “couch” across multiple files demonstrates a consistent security practice and links the same user to both the offshore communication and these financial transaction records.

The French-language data and Geneva references suggest the use of an international intermediary, possibly to disguise the funds’ origin.

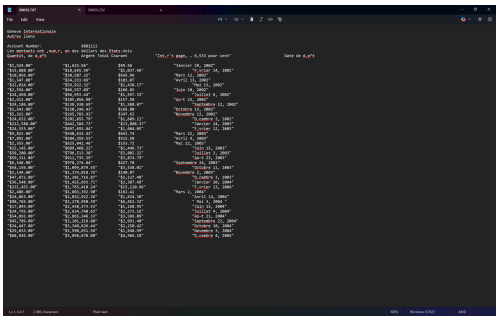
The account number 9882111 appears multiple times and is likely tied to the fraudulent deposits discussed in prior messages.

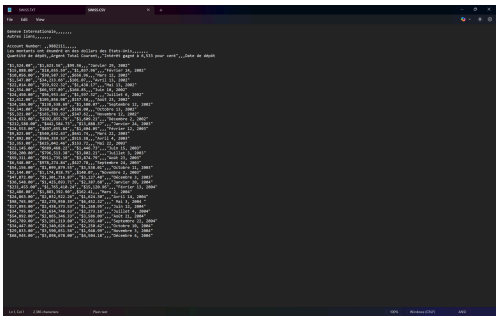
Relevance:

- Confirms the existence of offshore accounts used to hide embezzled funds.
- Matches amounts and timeline mentioned in deleted communications.
- Connects George Jones to Swiss and Isle of Man banking activity.
- Provides concrete numerical evidence of financial misconduct and money laundering.

SWISS.XLS SWISS.TXT SWISS.CSV (X.ZIP)

	A	B	C	D	E	F	G	H	I
1									
2	Geneve Internationale								
3	Autres liens								
4									
5	Account Number:		9882111						
6	Les montants ont énuméré en des dollars des Etats-Unis								
7	Quantité de dépôt		Argent Total Courant		Intérêt gagné à 6,533 pour cent			Date de dépôt	
8									
9	$1,524.00		$1,623.56		$99.56			Janvier 29, 2002	
10	$15,888.00		$18,655.59		$1,037.96			Février 14, 2002	
11	$10,056.00		$30,587.32		$656.96			Mars 12, 2002	
12	$1,547.00		$34,233.66		$101.07			Avril 13, 2002	
13	$22,014.00		$59,922.32		$1,438.17			Mai 13, 2002	
14	$2,554.00		$66,557.89		$166.85			Juin 10, 2002	
15	$24,450.00		$96,953.44		$1,597.32			Juillet 6, 2002	
16	$2,412.00		$105,856.98		$157.58			Août 23, 2002	
17	$24,186.00		$138,538.69		$1,580.07			Septembre 12, 2002	
18	$2,541.00		$150,296.43		$166.00			Octobre 13, 2002	
19	$5,321.00		$165,783.92		$347.62			Novembre 12, 2002	
20	$24,632.00		$202,855.79		$1,609.21			Décembre 2, 2002	
21	$212,588.00		$442,584.73		$13,888.37			Janvier 24, 2003	
22	$24,553.00		$497,655.84		$1,604.05			Février 12, 2003	
23	$9,823.00		$540,632.43		$641.74			Mars 22, 2003	
24	$7,892.00		$584,359.53		$515.58			Avril 4, 2003	
25	$2,353.00		$625,042.46		$153.72			Mai 22, 2003	
26	$22,145.00		$689,468.22		$1,446.73			Juin 15, 2003	
27	$58,200.00		$796,513.38		$3,802.21			Juillet 3, 2003	
28	$59,311.00		$911,735.39		$3,874.79			Août 23, 2003	
29	$6,548.00		$978,274.84		$427.78			Septembre 24, 2003	
30	$54,156.00		$1,099,879.55		$3,538.01			Octobre 11, 2003	
31	$2,144.00		$1,174,018.75		$140.07			Novembre 2, 2003	
32	$47,872.00		$1,301,716.87		$3,127.48			Décembre 3, 2003	
33	$36,548.00		$1,425,693.71		$2,387.68			Janvier 20, 2004	
34	$231,455.00		$1,765,410.24		$15,120.96			Février 13, 2004	
35	$2,486.00		$1,883,392.90		$162.41			Mars 2, 2004	
36	$24,863.00		$2,032,922.26		$1,624.30			Avril 14, 2004	
37	$98,765.00		$2,270,950.39		$6,452.32			Mai 3, 2004	
38	$17,893.00		$2,438,373.53		$1,168.95			Juin 12, 2004	
39	$34,795.00		$2,634,740.63		$2,273.16			Juillet 4, 2004	
40	$54,892.00		$2,865,346.33		$3,586.09			Août 21, 2004	
41	$45,789.00		$3,101,319.80		$2,991.40			Septembre 22, 2004	
42	$34,447.00		$3,340,626.44		$2,250.42			Octobre 10, 2004	
43	$29,833.00		$3,590,651.56		$1,948.99			Novembre 3, 2004	
44	$68,945.00		$3,898,678.00		$4,504.18			Décembre 4, 2004	





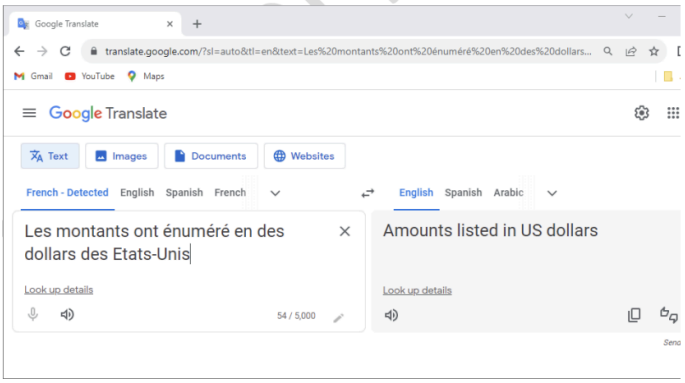
X.ZIP → [SWISS.XLS SWISS.TXT SWISS.CSV]

After unzipping an encrypted X.ZIP file with “couch” password, I opened contained files (SWISS.XLS, SWISS.TXT, SWISS.CSV) using Microsoft Excel and Windows Notepad.

It seems like all these three files contain the same data, but in different formats. (Bank Statements)

Google Translate Activity

Google Translate

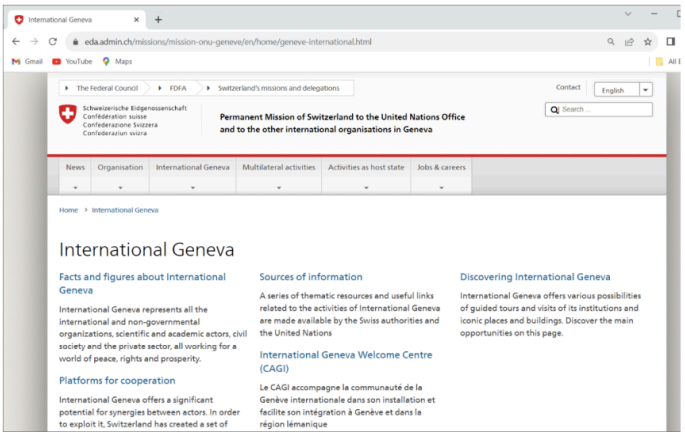


Browser activity shows use of Google Translate to convert French text to English. One translation recorded is:
"Les montants ont énuméré en des dollars des États-Unis" →
"Amounts listed in US dollars"

This phrase exactly matches a line appearing in the decrypted SWISS.XLS (TXT/CSV) file found inside X.ZIP.
The translation activity demonstrates that the user (likely Martha or George) was attempting to understand the French-language Swiss financial documents, confirming awareness of the contents and intentional access to the hidden bank data.

Webpage Related to Geneva

Website regarding Geneva

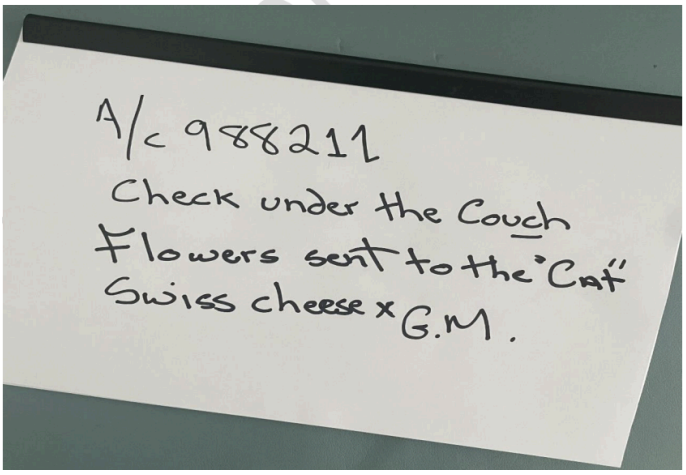


A visited webpage referencing "Geneva" and "Switzerland" was identified, consistent with the bank title "Geneve Internationale" found in SWISS.XLS (TXT/CSV).

This suggests research or interaction with the Swiss financial institution hosting the illicit account.
Combined with translation activity, it shows the suspects were actively verifying and managing offshore financial information from their work environment.

Handwritten Note (Physical Evidence)

Handwritten note



Recovered Text:
"A/c 988211
Check under the couch
Flowers sent to the "Cat"
Swiss cheese × G.M."

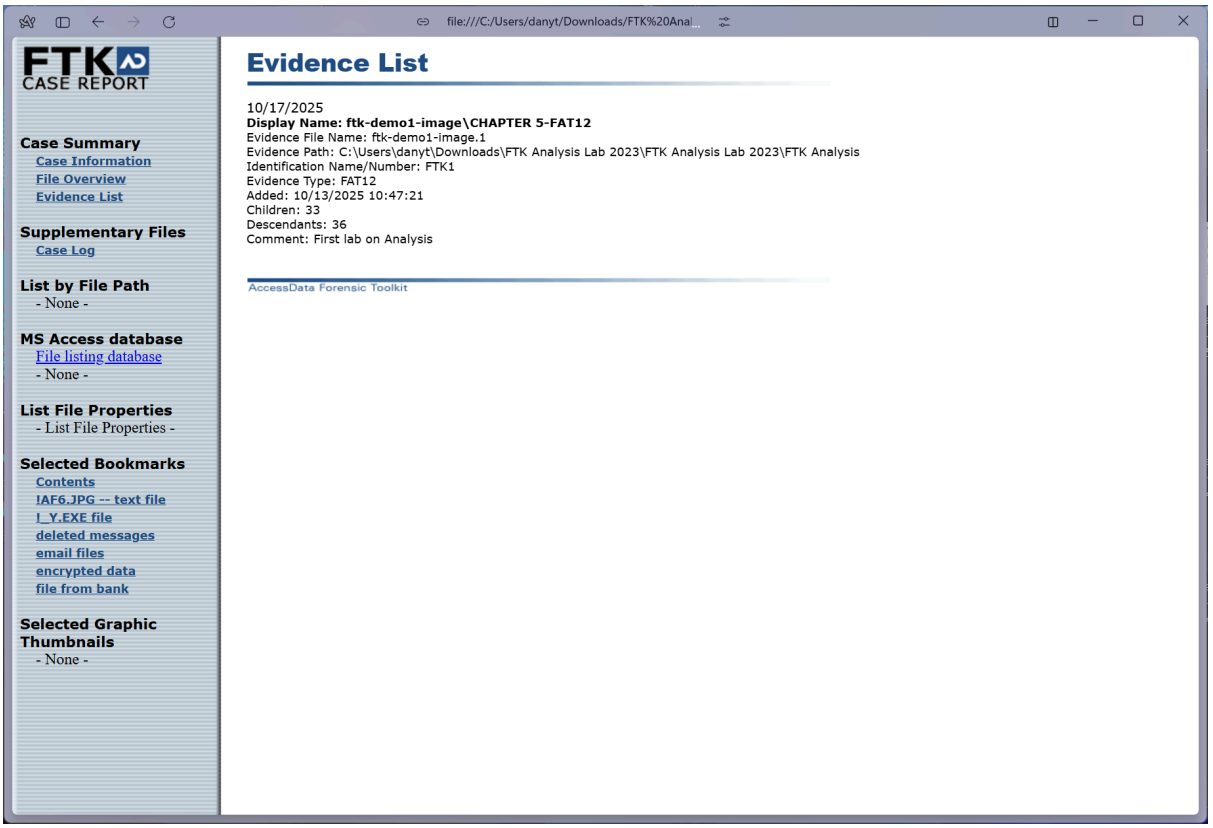
This physical note directly correlates to multiple digital findings:

- **"A/c 988211"** → Matches the Swiss bank account number in SWISS.CSV.
- **"Check under the couch"** → References the password "couch", used to decrypt X.ZIP.
- **"Swiss cheese × G.M."** → "G.M." likely refers to George Montgomery/Jones, confirming authorship or intended recipient.
- The mention of "Cat" and "Flowers" may correspond to browser searches for "Cat Adoption Dublin" and florist pages, indicating possible use of personal communications as code or cover phrases.

The handwritten note acts as physical corroboration for the digital evidence.
It establishes:

- The same account number and password.
- A clear link between offline planning and digital concealment of funds.
- Awareness and coordination between George and Martha.

FTK Case Report (generated)



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database
- None -

List File Properties
- List File Properties -

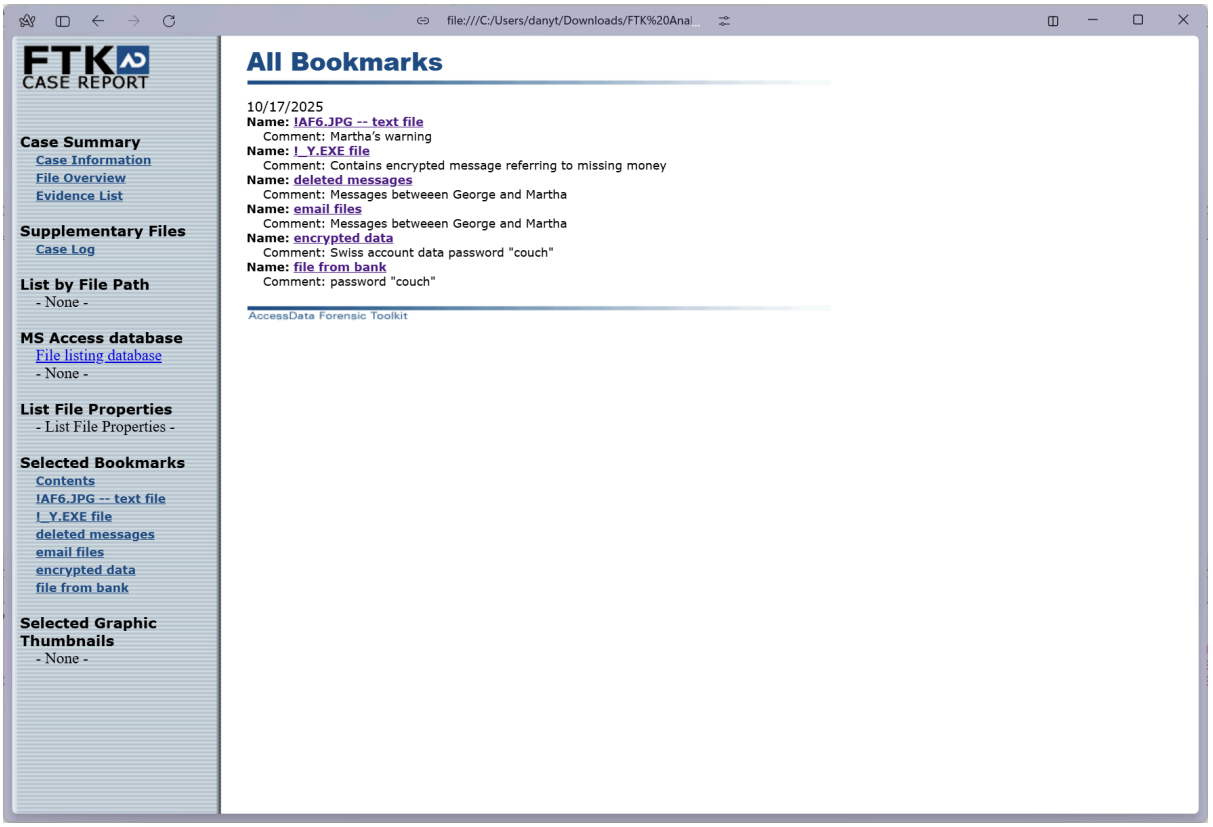
Selected Bookmarks
Contents
!AF6.JPG -- text file
!_Y.EXE file
deleted messages
email files
encrypted data
file from bank

Selected Graphic Thumbnails
- None -

Evidence List

10/17/2025
Display Name: ftk-demo1-image\CHAPTER 5-FAT12
Evidence File Name: ftk-demo1-image.1
Evidence Path: C:\Users\danyt\Downloads\FTK Analysis Lab 2023\FTK Analysis Lab 2023\FTK Analysis
Identification Name/Number: FTK1
Evidence Type: FAT12
Added: 10/13/2025 10:47:21
Children: 33
Descendants: 36
Comment: First lab on Analysis

AccessData Forensic Toolkit



FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
Case Log

List by File Path
- None -

MS Access database
File listing database
- None -

List File Properties
- List File Properties -

Selected Bookmarks
Contents
!AF6.JPG -- text file
!_Y.EXE file
deleted messages
email files
encrypted data
file from bank

Selected Graphic Thumbnails
- None -

All Bookmarks

10/17/2025
Name: !AF6.JPG -- text file
Comment: Martha's warning
Name: !_Y.EXE file
Comment: Contains encrypted message referring to missing money
Name: deleted messages
Comment: Messages betweeen George and Martha
Name: email files
Comment: Messages betweeen George and Martha
Name: encrypted data
Comment: Swiss account data password "couch"
Name: file from bank
Comment: password "couch"

AccessData Forensic Toolkit

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.