

# The Metadata That Caught a Lie: Digital Forensics in Action

This report analyses the image of a USB drive found by law enforcement in relation to a suspicious death. The disk image was created on 10/02/2017 using FTK Imager with MD5 and SHA1 hash values verified to ensure data integrity. Autopsy software was used, aiming to assess if there is enough evidence to conclude if John Smith's girlfriend's death was indeed a suicide.



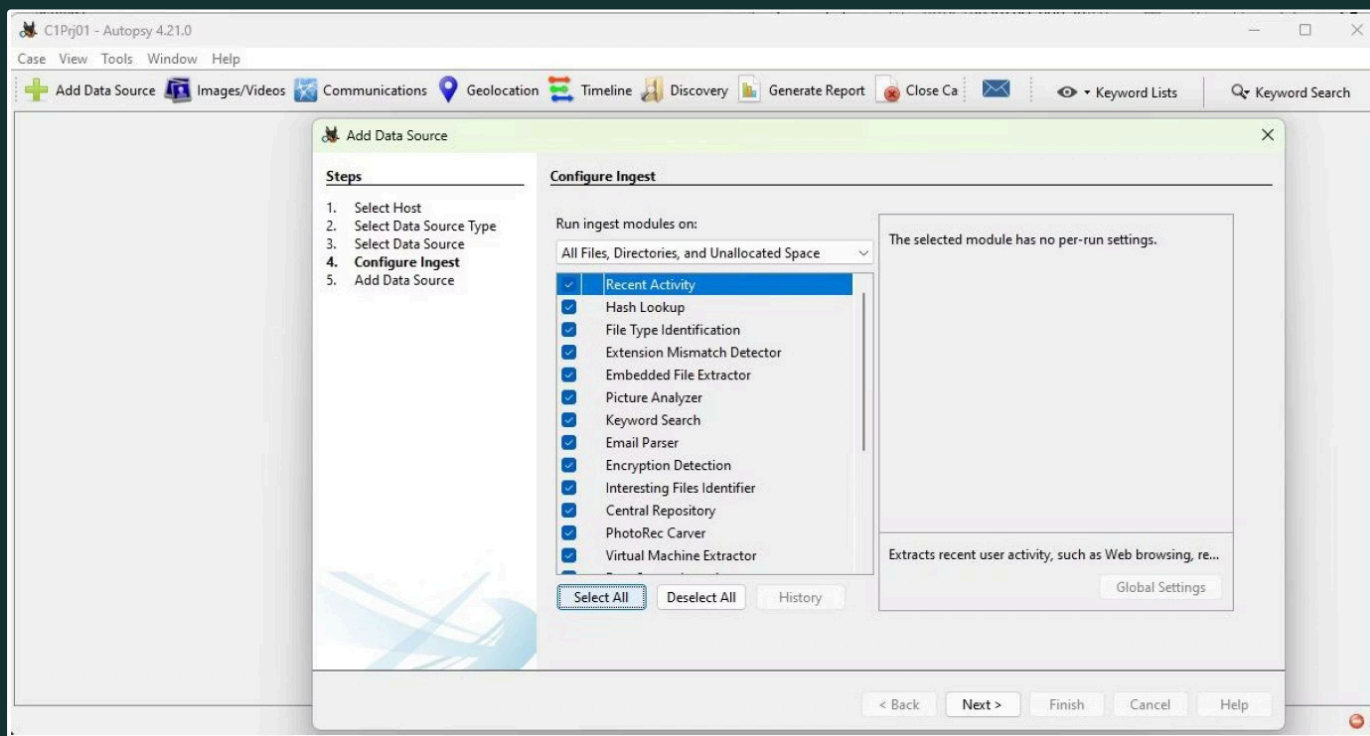
# Examination Process

The disk image in file CaseUSB.E01 was loaded as a new case onto Autopsy with a new case created. Case number CPrj01, examiner Carla Vieira. File CaseUSB.E01 was added as the data source and the Time Zone was set to (GMT-5:00) US/Eastern. Finally, all ingest modules were enabled for comprehensive analysis .

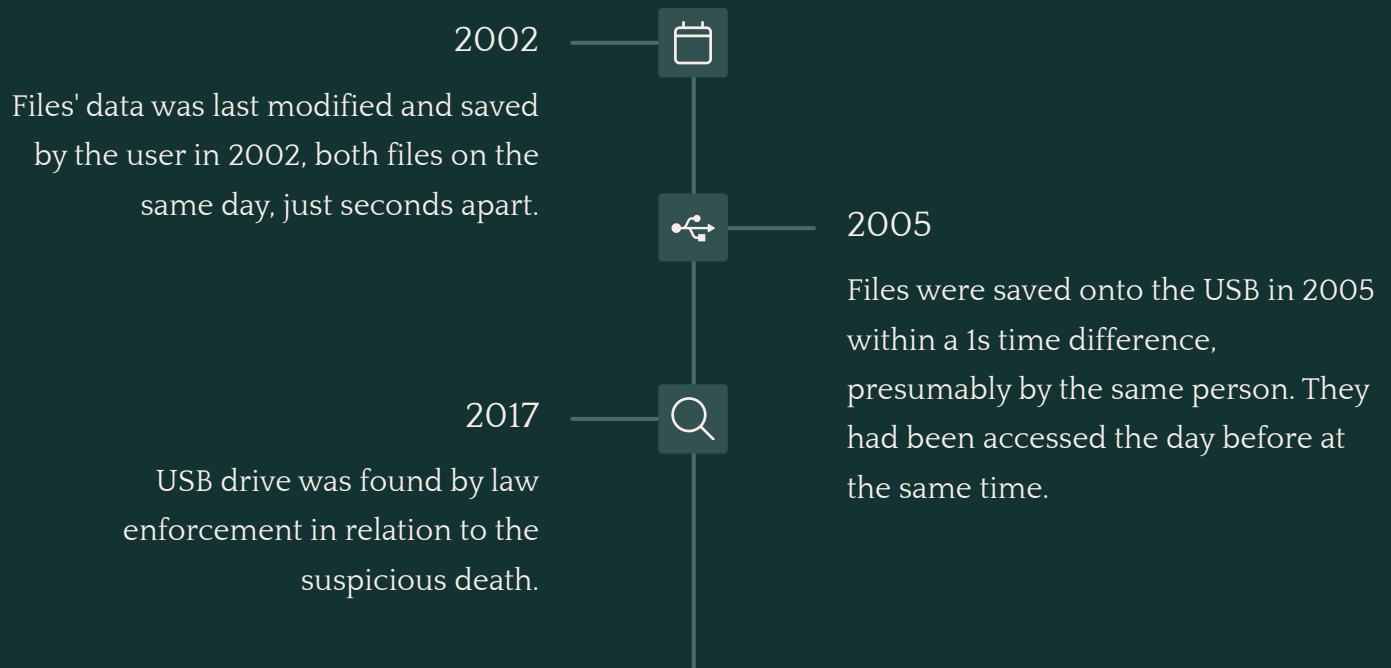


In the Tree Viewer pane, the Documents folder was examined and the two files found were deemed significant ("Donna Assets.xls" and "suic\*\*\*1.txt"). They were both tagged as a Notable Item. They were analysed and exported.

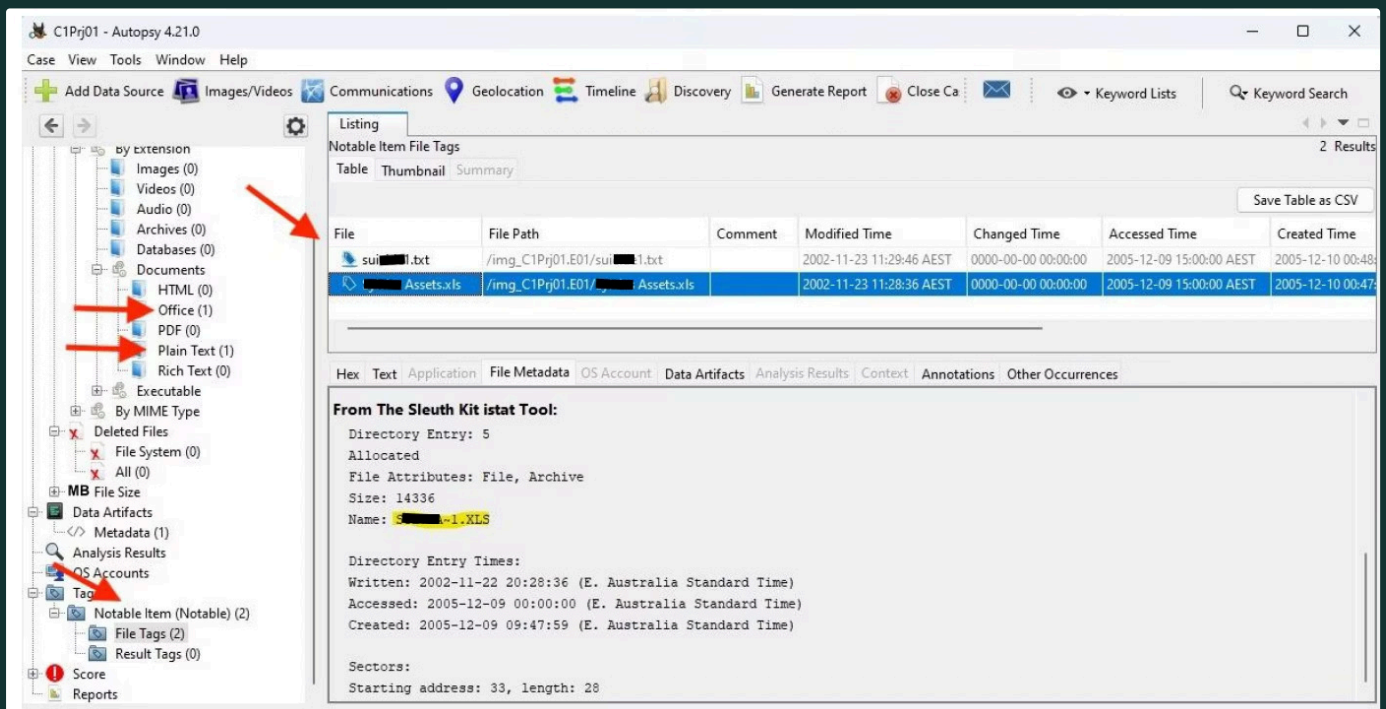
Figure 1. All ingest modules were enabled.



# Key Findings: Timeline Inconsistencies



Autopsy provides timeline information for the files (MACtimes) (Carrier, B., 2025). The metadata associated to both notable items is inconsistent with a suicide. It is unlikely that Donna/Dana wrote a suicide note 15 years before her death.



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a file tree with categories like 'by extension', 'By MIME Type', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Metadata (1)', 'Analysis Results', 'OS Accounts', 'Tag', 'Notable Item (Notable) (2)', 'File Tags (2)', 'Result Tags (0)', 'Score', and 'Reports'. Red arrows point to the 'Tag' and 'Notable Item' sections. The main window shows a 'Listing' of 'Notable Item File Tags' with 2 results. The table below lists the files and their metadata.

File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time
sui-1.txt	/img_C1Prj01.E01/sui-1.txt		2002-11-23 11:29:46 AEST	0000-00-00 00:00:00	2005-12-09 15:00:00 AEST	2005-12-10 00:48:00 AEST
Assets.xls	/img_C1Prj01.E01/Assets.xls		2002-11-23 11:28:36 AEST	0000-00-00 00:00:00	2005-12-09 15:00:00 AEST	2005-12-10 00:47:00 AEST

Below the table, the 'File Metadata' tab is selected, showing details for 'sui-1.txt'.

**From The Sleuth Kit istat Tool:**

Directory Entry: 5  
Allocated  
File Attributes: File, Archive  
Size: 14336  
Name: sui-1.XLS

Directory Entry Times:  
Written: 2002-11-22 20:28:36 (E. Australia Standard Time)  
Accessed: 2005-12-09 00:00:00 (E. Australia Standard Time)  
Created: 2005-12-09 09:47:59 (E. Australia Standard Time)

Sectors:  
Starting address: 33, length: 28

Figure 2. Notable files are tagged.

# Suspicious File Attributes



## Name Discrepancy

"Donnas Assets.xls" has her name written as "Dana". It's unlikely she would misspell her own name.



## Unknown Author

The excel file's author is "Samantha Key".



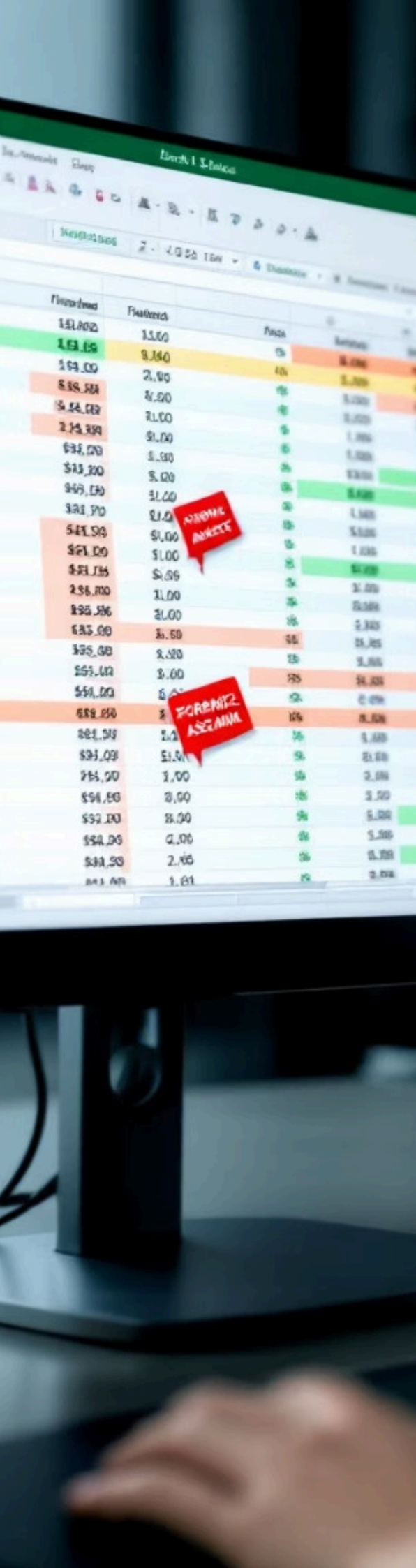
## Legacy File Format

The use of file shortnames ("DANA-1.XLS") suggests that these files may have originated from an older system, which can affect timestamp precision (SANS Institute, 2004; Microsoft, 2025).



## Timing Inconsistency

It would still, however, not explain how files written in 2002, saved onto USB in 2005 were conveniently found in 2017 near the dead body.



# Analysis of Suicide Note

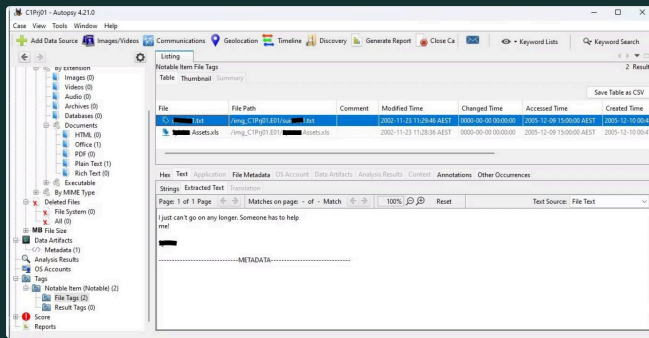


Figure 3. Suspicious suic\*\*\* note.

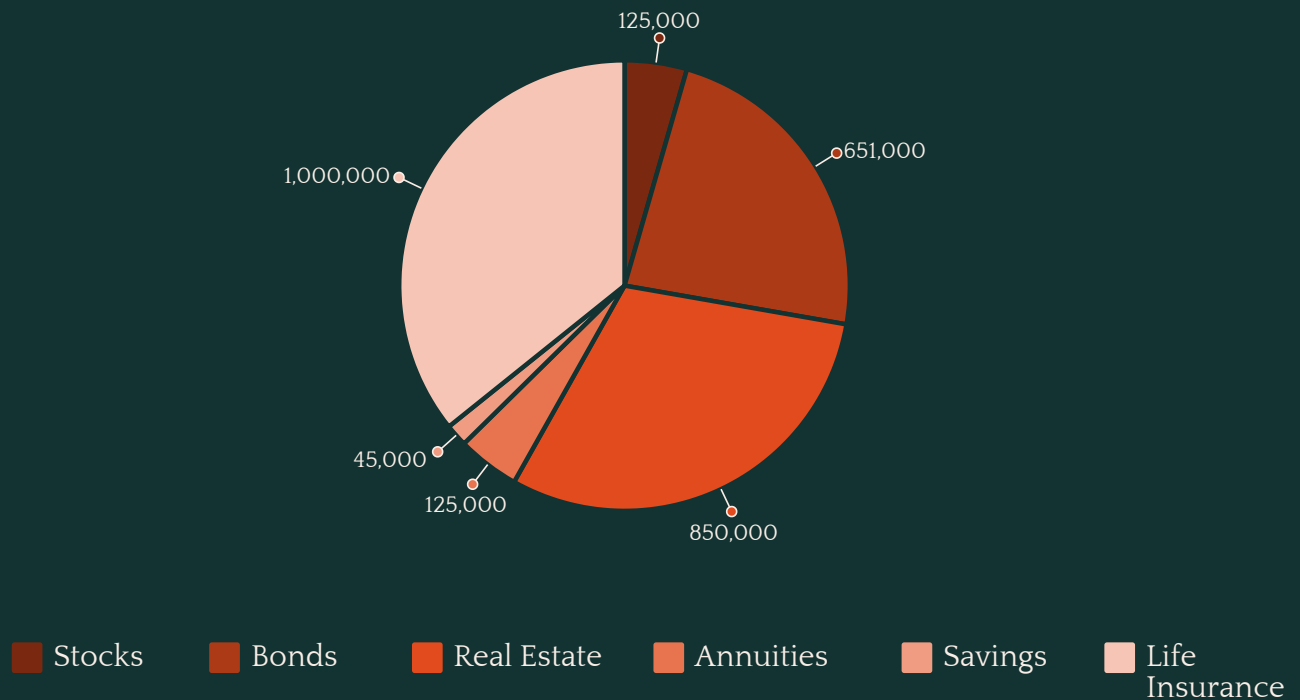
The note (suic\*\*\*1.txt) contains minimal text: "I just can't go on any longer. Someone has to help me! Donna"

## Red Flags in the Suicide Note

- Extremely brief content (only 65 bytes)
- Created in 2002 but found in 2017
- Created within seconds of the assets spreadsheet
- Accessed at the exact same time as the assets file
- Vague content with no specific personal details

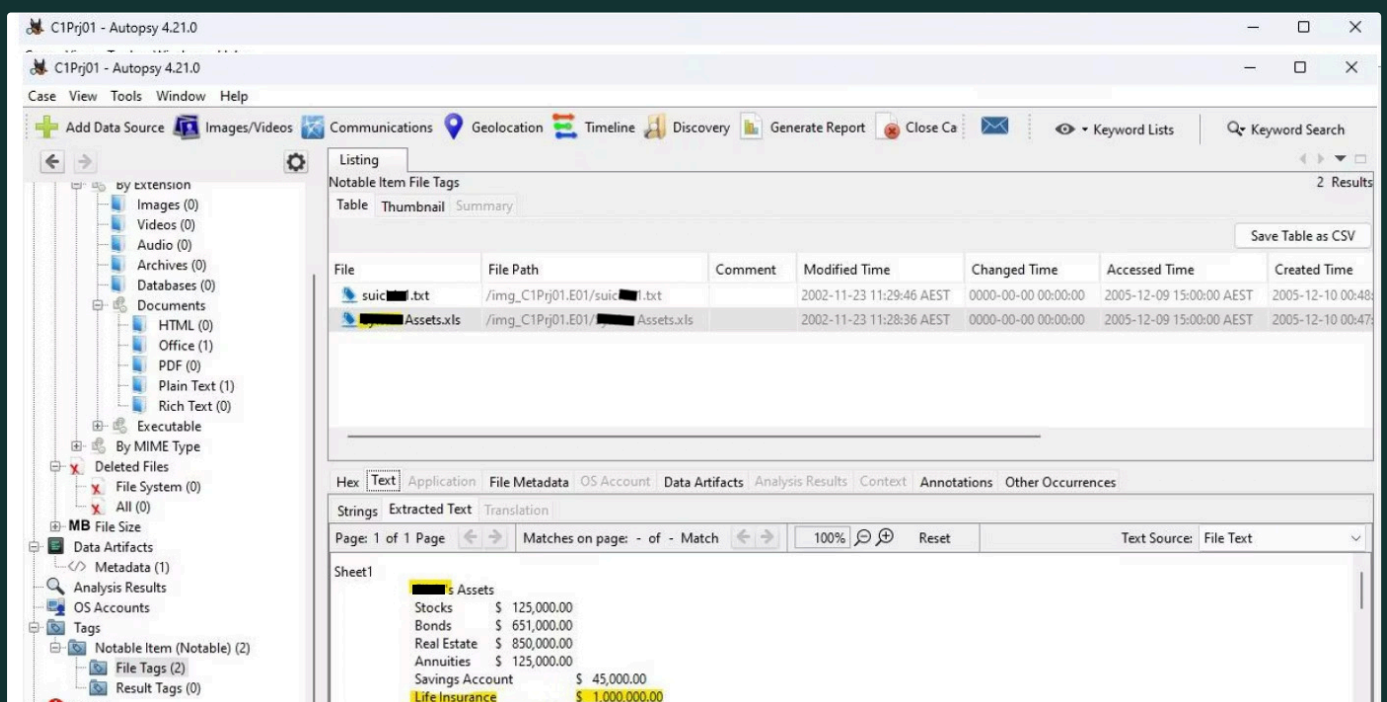


# Financial Motive Analysis



The "Donnas Assets.xls" file shows substantial wealth totaling \$2,796,000.00, with life insurance being the largest single asset at \$1,000,000.00. This raises questions about who would benefit from her death, particularly regarding the life insurance policy. The presence of this detailed financial document alongside a questionable suicide note suggests a potential financial motive for murder.

Figure 4. "Donna's Assets.xls" file recovered.



# Conclusion

## Evidence Inconsistencies

The timeline analysis shows that both files were created in 2002, saved to USB in 2005, and then conveniently found in 2017 near the victim's body - a highly suspicious sequence of events.

## Financial Motive

The detailed asset spreadsheet showing nearly \$2.8 million in assets, including a \$1 million life insurance policy, suggests a clear financial motive for murder rather than suicide.

## Investigative Questions

Who is Samantha Key? Would John Smith financially benefit from her insurance policy pay out? These questions require further investigation to determine the true circumstances of the death.

Overall, the information from the recovered files are more consistent with a murder to potentially benefit the beneficiary of the listed assets.

# Reference Section

Carrier, B. (2025). *Timeline Mode*. Sleuth Kit Website: <https://www.sleuthkit.org/autopsy/help/tl.html>

Microsoft. (2025). *Naming Files, Paths, and Namespaces*. <https://learn.microsoft.com/en-us/windows/win32/fileio/naming-a-file>

SANS Institute. (2004). *Forensic Investigation of USB Flashdrive Image for CC Terminals*. <https://www.giac.org/paper/gcfa/188/forensic-investigation-usb-flashdrive-image-cc-terminals/107219>

IEEE Computer Society. (2021). Research on anti-forensic techniques and timestamp manipulation detection.

International Conference on Availability, Reliability and Security. Research on timeline forgery in digital forensics.

Arizona State University. Anti-forensic technique detection in NTFS file systems.

Data Source Name	Ingest Status	Type	Files
CaseUSB.E01	Completed	Flash Drive	12

Acquisition Details: Examiner Name: Jane Monday, Acquired Date: Fri Feb 10 19:06:37 2017, System Date: Fri Feb 10 19:06:37 2017, Acquirry Operating System: Win 201x, Image Type: E01, Size: 1.47 MB (1474560 bytes), Unallocated Space: 1.44 MB (1442816 bytes), Sector Size: 512 bytes, MD5: c9bfd4d363ce0af8c5b94078737b68d8, SHA1: 85bf2e56439c5261333263477863b399c65ca97b