# Unauthorized Data Transfer: A Digital Forensics Case Study

Thomas Knapp | CompTIA A+ | Network+ | Security+

Email: thomasknapp1011@gmail.com | Phone: 631-415-7040

## Case Overview

This case study details the forensic analysis of a digital evidence file labeled 'Smith_Q1.001'. The investigation was conducted using Autopsy 4.19.1 to identify evidence of unauthorized access, deletion, and potential exfiltration of sensitive company data. The report outlines the analysis process, key findings, and conclusions drawn from the recovered digital artifacts.

## Methodology

The investigation began by creating a new case within Autopsy and loading the provided disk image. Default ingest modules were used to parse file metadata, extract deleted content, and analyze user activity. The modules included: File Type Identification, Recent Activity, Hash Lookup, and Keyword Search.

## Evidence Discovery

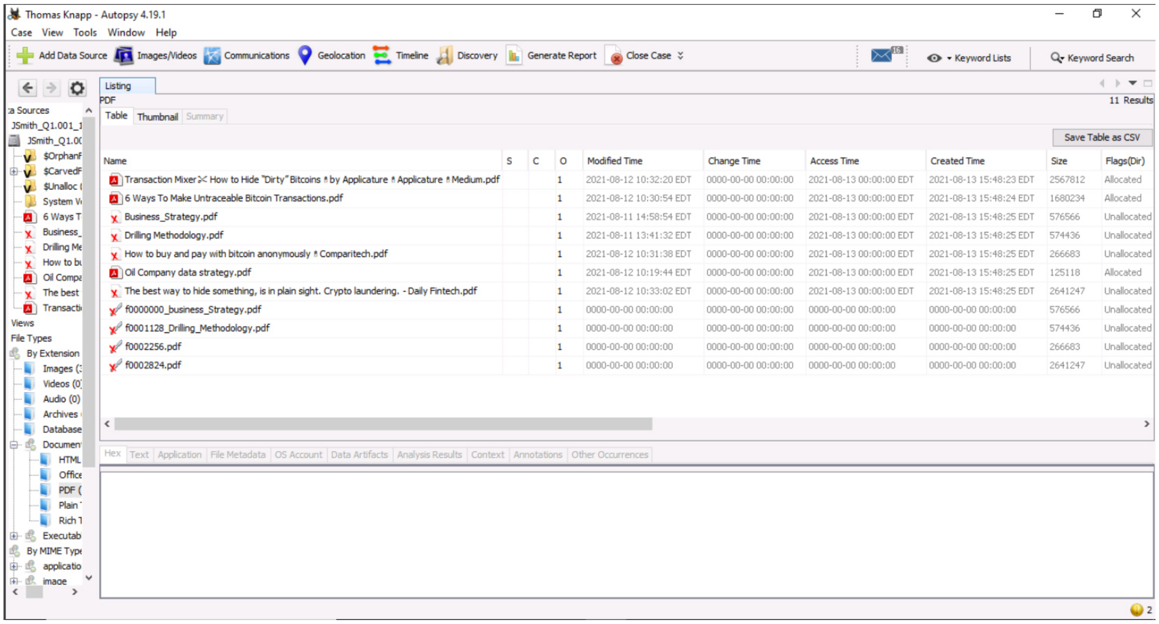
Initial file system analysis revealed several documents indicative of confidential business strategy and technical processes. Among the recovered files were:

- Business_Strategy.pdf

- Drilling_Methodology.pdf

- Oil Company data strategy.pdf

These documents were identified alongside materials relating to cryptocurrency obfuscation methods. Their presence on a corporate asset raises serious concerns regarding user intent and data privacy compliance.



PDF

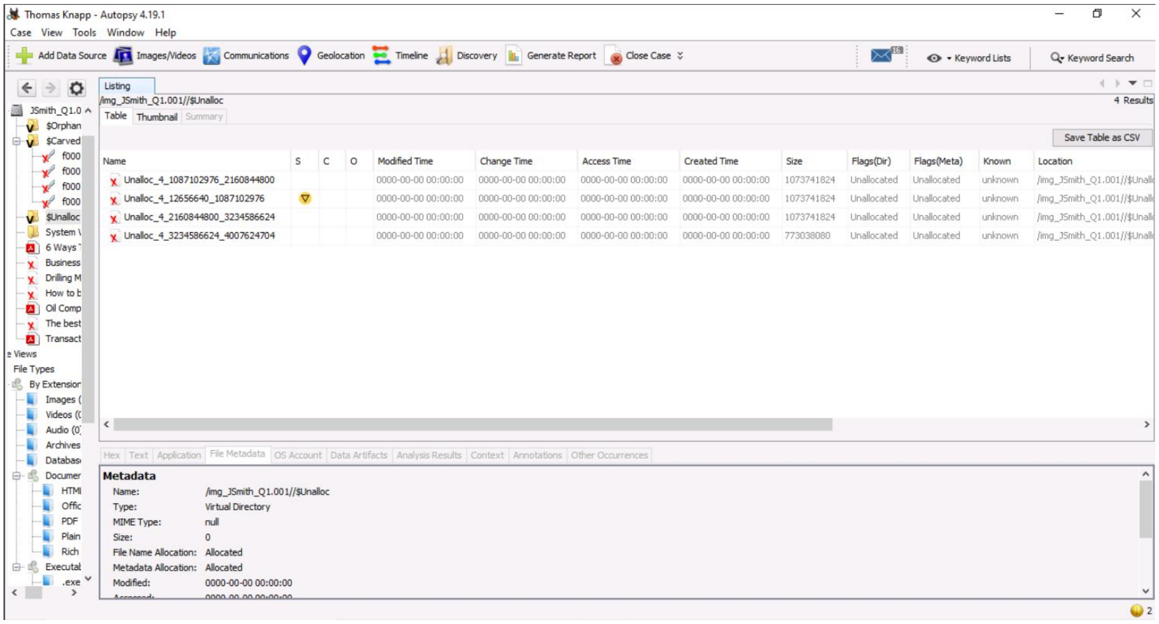
11 Results

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) |
|---|---|---|---|---|---|---|---|---|---|
| Transaction Mixer ✂ How to Hide "Dirty" Bitcoins ∎ by Applicature ∎ Applicature ∎ Medium.pdf | | | 1 | 2021-08-12 10:32:20 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:23 EDT | 2567812 | Allocated |
| 6 Ways To Make Untraceable Bitcoin Transactions.pdf | | | 1 | 2021-08-12 10:30:54 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:24 EDT | 1680234 | Allocated |
| Business_Strategy.pdf | | | 1 | 2021-08-11 14:58:54 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 576566 | Unallocated |
| Drilling Methodology.pdf | | | 1 | 2021-08-11 13:41:32 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 574436 | Unallocated |
| How to buy and pay with bitcoin anonymously ∎ Comparitech.pdf | | | 1 | 2021-08-12 10:31:38 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 266683 | Unallocated |
| Oil Company data strategy.pdf | | | 1 | 2021-08-12 10:19:44 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 125118 | Allocated |
| The best way to hide something, is in plain sight. Crypto laundering. - Daily Fintech.pdf | | | 1 | 2021-08-12 10:33:02 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 2641247 | Unallocated |
| f0000000_business_Strategy.pdf | | | 1 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 576566 | Unallocated |
| f0001128_Drilling_Methodology.pdf | | | 1 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 574436 | Unallocated |
| f0002256.pdf | | | 1 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 266683 | Unallocated |
| f0002824.pdf | | | 1 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 2641247 | Unallocated |

Figure 1: Recovered documents containing proprietary information and cryptocurrency-related guides.

## Deleted and Unallocated File Recovery

Autopsy's file carving functionality recovered several key documents that had been previously deleted. These files were found in unallocated space, confirming that the user attempted to permanently remove traces of their activity. The volume and nature of these deleted files further support the hypothesis of data concealment.



/img_JSmith_Q1.001//$Unalloc

4 Results

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known | Location |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unalloc_4_1087102976_2160844800 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 1073741824 | Unallocated | Unallocated | unknown | /img_JSmith_Q1.001//$Unall |
| Unalloc_4_12656640_1087102976 | ▽ | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 1073741824 | Unallocated | Unallocated | unknown | /img_JSmith_Q1.001//$Unall |
| Unalloc_4_2160844800_3234586624 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 1073741824 | Unallocated | Unallocated | unknown | /img_JSmith_Q1.001//$Unall |
| Unalloc_4_3234586624_4007624704 | | | | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 773038080 | Unallocated | Unallocated | unknown | /img_JSmith_Q1.001//$Unall |

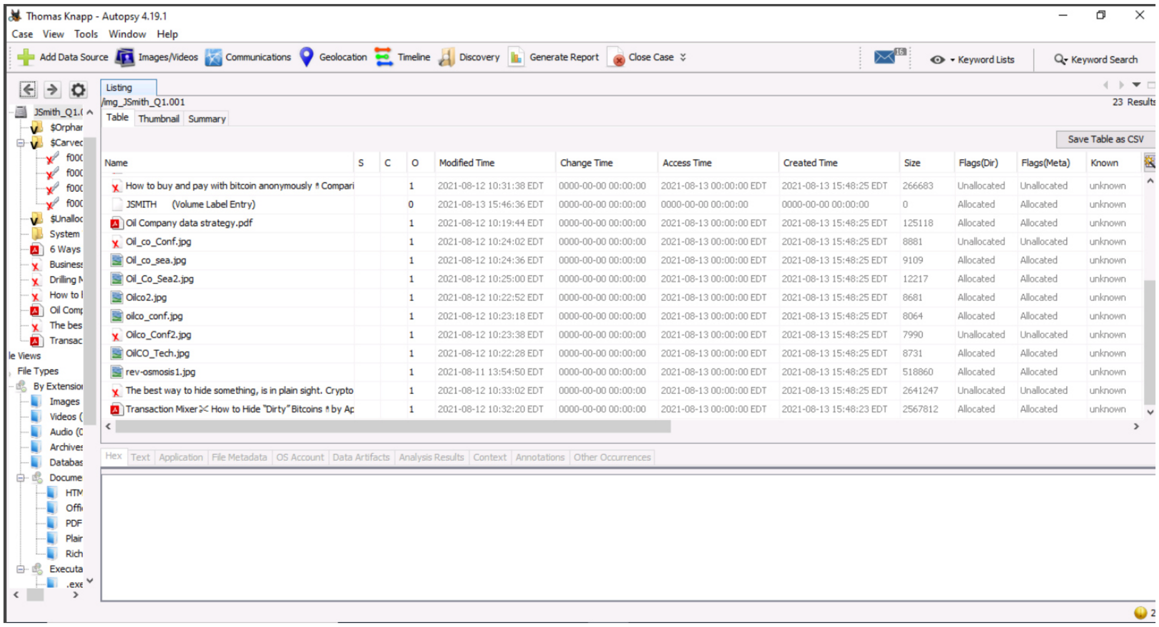
**Metadata**

| | |
|---|---|
| Name: | /img_JSmith_Q1.001//$Unalloc |
| Type: | Virtual Directory |
| MIME Type: | null |
| Size: | 0 |
| File Name Allocation: | Allocated |
| Metadata Allocation: | Allocated |
| Modified: | 0000-00-00 00:00:00 |
| Accessed: | 0000-00-00 00:00:00 |

Figure 2: Deleted and carved files discovered in unallocated space.

## Recovered Image Evidence

Further analysis uncovered several image files with filenames suggesting technical documentation or internal resources. These images, such as 'OilCO_Tech.jpg' and 'Oil_co_Conf.jpg', may contain engineering schematics or process diagrams, further highlighting the sensitivity of the content accessed and potentially exfiltrated.



Thomas Knapp - Autopsy 4.19.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

/img_JSmith_Q1.001

23 Results

| Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size | Flags(Dir) | Flags(Meta) | Known |
|---|---|---|---|---|---|---|---|---|---|---|---|
| How to buy and pay with bitcoin anonymously ⚘ Compari | | | 1 | 2021-08-12 10:31:38 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 266683 | Unallocated | Unallocated | unknown |
| JSMITH (Volume Label Entry) | | | 0 | 2021-08-13 15:46:36 EDT | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0 | Allocated | Allocated | unknown |
| Oil Company data strategy.pdf | | | 1 | 2021-08-12 10:19:44 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 125118 | Allocated | Allocated | unknown |
| Oil_co_Conf.jpg | | | 1 | 2021-08-12 10:24:02 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 8881 | Unallocated | Unallocated | unknown |
| Oil_co_sea.jpg | | | 1 | 2021-08-12 10:24:36 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 9109 | Allocated | Allocated | unknown |
| Oil_Co_Sea2.jpg | | | 1 | 2021-08-12 10:25:00 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 12217 | Allocated | Allocated | unknown |
| Oilco2.jpg | | | 1 | 2021-08-12 10:22:52 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 8681 | Allocated | Allocated | unknown |
| oilco_conf.jpg | | | 1 | 2021-08-12 10:23:18 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 8064 | Allocated | Allocated | unknown |
| Oilco_Conf2.jpg | | | 1 | 2021-08-12 10:23:38 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 7990 | Unallocated | Unallocated | unknown |
| OilCO_Tech.jpg | | | 1 | 2021-08-12 10:22:28 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 8731 | Allocated | Allocated | unknown |
| rev-osmosis1.jpg | | | 1 | 2021-08-11 13:54:50 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 518860 | Allocated | Allocated | unknown |
| The best way to hide something, is in plain sight. Crypto | | | 1 | 2021-08-12 10:33:02 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:25 EDT | 2641247 | Unallocated | Unallocated | unknown |
| Transaction Mixer ✂ How to Hide "Dirty" Bitcoins ⚘ by Ap | | | 1 | 2021-08-12 10:32:20 EDT | 0000-00-00 00:00:00 | 2021-08-13 00:00:00 EDT | 2021-08-13 15:48:23 EDT | 2567812 | Allocated | Allocated | unknown |

Figure 3: Technical images recovered from the suspect's storage device.

## Conclusion

The forensic evidence supports the conclusion that the user accessed, deleted, and attempted to conceal proprietary business data. The presence of anonymization tools and sensitive technical documentation raises the likelihood of an intentional breach of company policies and possibly legal standards. It is recommended that further review include user activity logs, USB device connection history, and network transfer records to correlate evidence of exfiltration.