

CASE NOTES

Case Ref: SM/1/2024

Examiner: Sherlock Holmes

Case name:

Operation Spoiler

Case summary:

investigation into Dr. Taylor Perl Salt's alleged involvement in the unauthorised removal of pages from library books to compile a fabricated manuscript. The suspect's activities were uncovered through analysis of metadata from a forensic disk image and related multimedia evidence including audio, video, and document files.

Other references:

Exhibit DOC1 - OOXML file: "How to write a book from other books"

Witness: Detective Fossil

Contact information:

Woofington BABBAGE, Digital Investigator, BYTE Detective Agency

Detective Fossil, Operation Spoiler, Cyberly Police Department

CASE NOTES

Case Ref: SM/1/2024

Examiner: Sherlock Holmes

Date/time	Notes	Comments
2025-04-25 10:21	Opened forensic disk image SM_2024_04_023_001.dd using HxD Hex Editor.	Start of Task 1 part b: Recovery of JPEG files from unallocated space.
10:23	Performed hex value search for JPEG SOI (Start of Image) header " FF D8 ". Identified valid file header at offset 0x482000.	
10:26	Located JPEG EOI (End of Image) at offset 0x484644 .	
10:28	Selected block from 0x482000 to 0x484644 . Copied the data and made a separate file named orig_image1.jpg .	
10:20	Created duplicate of carved file as image1_copy.jpg . Opened copy using standard image viewer. Image rendered without corruption. The retrieved image is as follows.	Original file remained unopened to preserve forensic integrity.

CASE NOTES

Case Ref: SM/1/2024


Examiner: Sherlock Holmes

Date/time	Notes	Comments
		
10:40	Continued hex search for additional JPEG SOI headers. Identified another valid header at offset 0xC2E5A000 .	
10:43	Located EOI marker " FF D9 " at offset 0xC2F1AF42.	
10:46	Selected block from 0xC2E5A000 to 0xC2F1AF42 , copied, and saved as orig_image2.jpg .	
10:48	Created duplicate of carved file as image2_copy.jpg . Opened copy in image viewer to verify rendering. Image retrieved successfully as shown below.	Again, original remained untouched.

CASE NOTES

Case Ref: SM/1/2024

Examiner: Sherlock Holmes

Date/time	Notes	Comments
		
2025-04-25 11:12	Continued data recovery activity under Task 1 part c. Searched disk image SM_2024_04_023_001.dd in HxD for ZIP file signature 50 4B 03 04 .	Looking for an OOXML (Office Open XML) formatted document.
11:14	Identified valid ZIP file header at offset 0x4EC000 . Confirmed presence of OOXML content via the decoded text field showing [Content_Types].xml .	
11:27	After multiple attempts, located ZIP archive footer via presence of EOCD marker and final ZIP cluster at offset 0xC8B1098 .	

CASE NOTES

Case Ref: SM/1/2024

Examiner: Sherlock Holmes

Date/time	Notes	Comments
11:30	Created a carved file from offsets 0x4EC000 to 0xC8B1098 using "Select Block" function in HxD. Saved original carved file as orig_OOXML.zip .	
11:33	Made a copy of the carved file and renamed it to OOXML_copy.docx inspection.	
11:35	Opened OOXML_copy.docx in Microsoft Word. The file opened without error.	Document contained embedded images located in the word/media directory
11:40	Original file orig_OOXML.zip remains untouched and preserved as digital evidence.	