

Forensic Report – Disk Image Analysis

Tanishq Javvaji
119070185

Contents

Brief Summary of Information	1
Tools Used in the Investigation Process	2
Repository #1 Analysis of "obiwan.exe," "obiwan2.exe," "not-the-droids-you-are-looking-for.mp3," and "final-form.exe"	3
1. Analysis of "obiwan.exe"	4
2. Analysis of "obiwan2.exe"	8
3. Analysis of "not-the-droids-you-are-looking-for.mp3" using Base64 Decoded Key and Veracrypt	15
4. Analysis of "final-form.exe"	19
Recommendations and Next Steps	25
Challenges Faced	26

Brief Summary of Information

An image of a hard drive labeled 'ENPM687 Final XP' was seized from a suspected malware creator. A thorough investigation using diverse forensic methodologies is essential. Autopsy is the primary tool suited for analyzing this hard drive image.

During my analysis with Autopsy, I first examined the Data Sources summary to gauge the overall content of the hard drive and assess the time needed for a complete review. The image was found to be 21 GB, containing a variety of file types.

I then pinpointed the hard drive's geolocation as being in the United Kingdom.

My next step was to explore the 'Recent Files' tab to identify which files and folders the suspect might have accessed. This revealed numerous frequently visited files and folders. A notable area of interest was the 'My Documents' folder, which had been accessed multiple times. Therefore, I began my detailed investigation there.

In the 'My Documents' folder, particularly in the 'code' folder, I found two subfolders named 'build' and 'dist,' along with three spec files related to PyInstaller and a file named 'obiwan.py.' Delving into the 'build' folder, I discovered two folders with significant analysis scores, raising suspicions of potential malicious software. The 'dist' folder contained two executables, 'obiwan.exe' and 'obiwan.exe,' which warranted further examination due to their unusual scores. After exporting these files for deeper analysis, I attempted disassembly but soon realized they were Python executables. Running these executables individually revealed no immediate output, but Process Explorer showed them actively making server requests. Further investigation with TCPView confirmed they were establishing TCP connections to a remote system. Capturing the network traffic with Wireshark, I found 'obiwan.exe' sending messages to a contact named 'Obiwan Kenobi,' including phrases like 'you're my only hope' and seeking assistance. The other executable, 'obiwan.exe,' transmitted three messages, including cryptic ones like 'all your base64 are belong to us' and 'this is not even my final form.' A third message, encoded or encrypted, hinted at a connection to base64 encoding. Decoding this message using a base64 algorithm revealed the phrase 'r2d2 is the key,' suggesting a cryptic key to an unknown lock.

My attention then shifted to the 'Downloads' folder, previously flagged in the analysis. It contained three downloaded files: ProcessExplorer, a Python installer, and a VeraCrypt folder. The Python installer, likely used for building the earlier Python executables, and VeraCrypt, a disk encryption utility, were notable findings.

I also explored the 'My Music' folder, flagged for recent activity and significant analysis results. A peculiarly named music file, 'not-the-droids-youre-looking-for.mp3,' seemed out of place. Research revealed references to the Star Wars franchise, tying back to earlier findings involving characters like Obiwan and R2-D2. The 'Death Star Plans' mentioned earlier and missing from the hard drive were blueprints for the Death Star, aligning with the story of Leah sending them to Obiwan Kenobi through R2-D2. This indicated the mp3 file might conceal hidden data.

Using the previously discovered 'r2d2' key, I used VeraCrypt to decrypt the contents of the mp3 file. Selecting 'A' as the volume letter, based on its presence on the hard drive, I mounted the mp3 file as a drive. The successful mounting of the A-drive, measuring 19.8 MB, revealed a folder named 'Death Star Plans' with around 12 images of Death Star blueprints, a text file 'ENPM687-Read-This.txt' instructing to decipher a message sent by the 'final-form.exe' file, and the executable itself. Analyzing 'final-form.exe'

using Wireshark captured two messages: 'We have the blueprints to the Death Star' and 'We will defeat Darth Vader.

Tools Used in the Investigation Process

The investigation employed several specialized tools, each serving a distinct purpose in the forensic analysis. The key tools used were Autopsy, Wireshark, and Veracrypt. Below is a detailed overview of each tool, its purpose in this investigation, and any underlying assumptions associated with its use:

1. Autopsy:

- **Purpose:** Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. In this investigation, it was primarily used for the initial analysis of the hard disk image. Autopsy facilitated the identification and flagging of suspicious files on the disk, including the encrypted MP3 file and the executable files ('obiwan.exe' and 'obiwan2.exe').
- **Assumptions:** It is assumed that Autopsy accurately and comprehensively analyzes the disk image. The tool's effectiveness depends on its ability to detect anomalies, potential malware, and encrypted files, which forms the basis of further investigation.

2. Wireshark:

- **Purpose:** Wireshark is a network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It was utilized to capture and analyze the network traffic generated by 'obiwan.exe', 'obiwan2.exe', and 'final-form.exe'. Wireshark helped in identifying the nature of the remote connections established by these executables, including the analysis of HTTP requests and responses.
- **Assumptions:** The investigation assumes that Wireshark captures all relevant network traffic without omission. The accuracy of the analysis is dependent on Wireshark's ability to effectively capture and interpret network packets, which is crucial for understanding the executables' network behavior.

3. Veracrypt:

- **Purpose:** Veracrypt is an open-source disk encryption software used to encrypt and decrypt files. In this case, it was used to decrypt the 'not-the-droids-you-are-looking-for.mp3' file, using the key "r2d2" which was discovered during the analysis. This decryption was a critical part of the investigation, revealing important data hidden within the encrypted file.
- **Assumptions:** The tool's efficacy relies on the assumption that the encryption used on the MP3 file is compatible with Veracrypt's decryption capabilities. There is also an implicit assumption that the discovered key, "r2d2", is correct and that the file's encryption was not multi-layered beyond the scope of Veracrypt's decryption abilities.

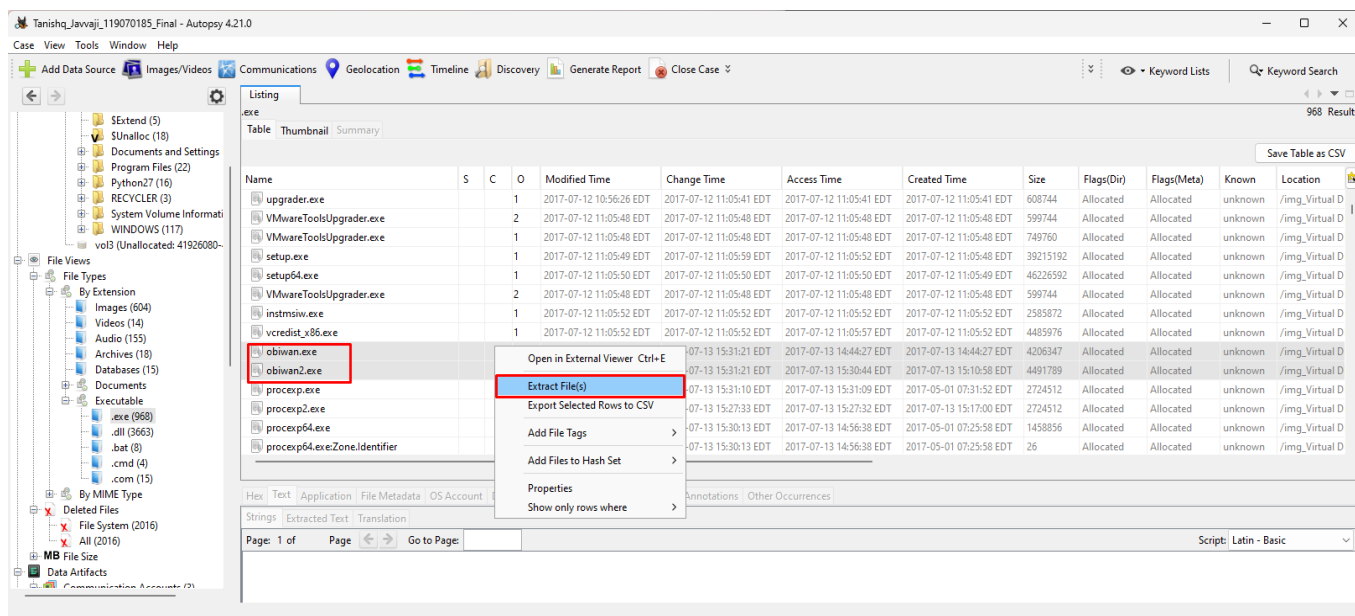
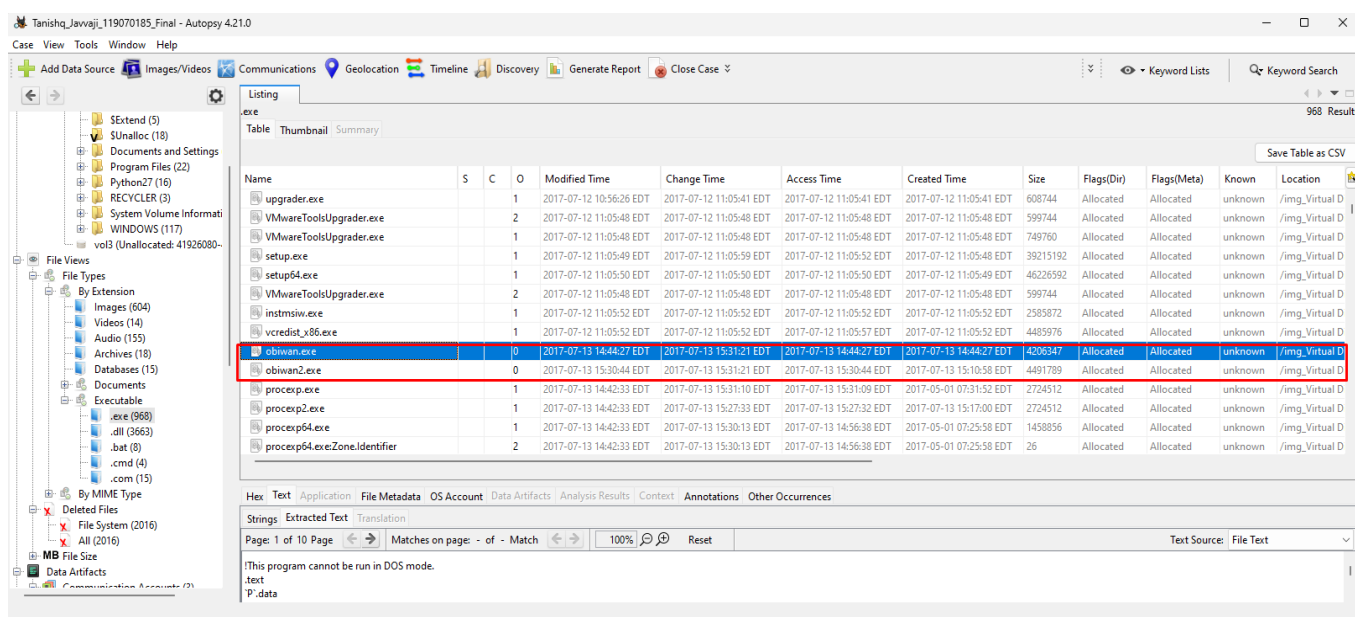
Repository #1 Analysis of "obiwan.exe," "obiwan2.exe," "not-the-droids-you-are-looking-for.mp3," and "final-form.exe"

Extraction of "obiwan.exe" and "obiwan2.exe" from Autopsy

Before delving into the detailed analysis of "obiwan.exe" and "obiwan2.exe," the files were extracted from the hard disk image using Autopsy's default extraction option. This initial step was essential for securing a copy of the executable for analysis while preserving the integrity of the original disk image.

Extraction Process:

- **Using Autopsy:** The file "obiwan.exe" and "obiwan2.exe" was located within the hard disk image using the Autopsy forensic suite. Autopsy provides a comprehensive platform for digital investigations, offering tools for file identification and extraction.
- **Default Extract Option:** The default extraction option in Autopsy was utilized. This option ensures a straightforward and secure method of extracting files, crucial for maintaining the forensic integrity of the evidence.

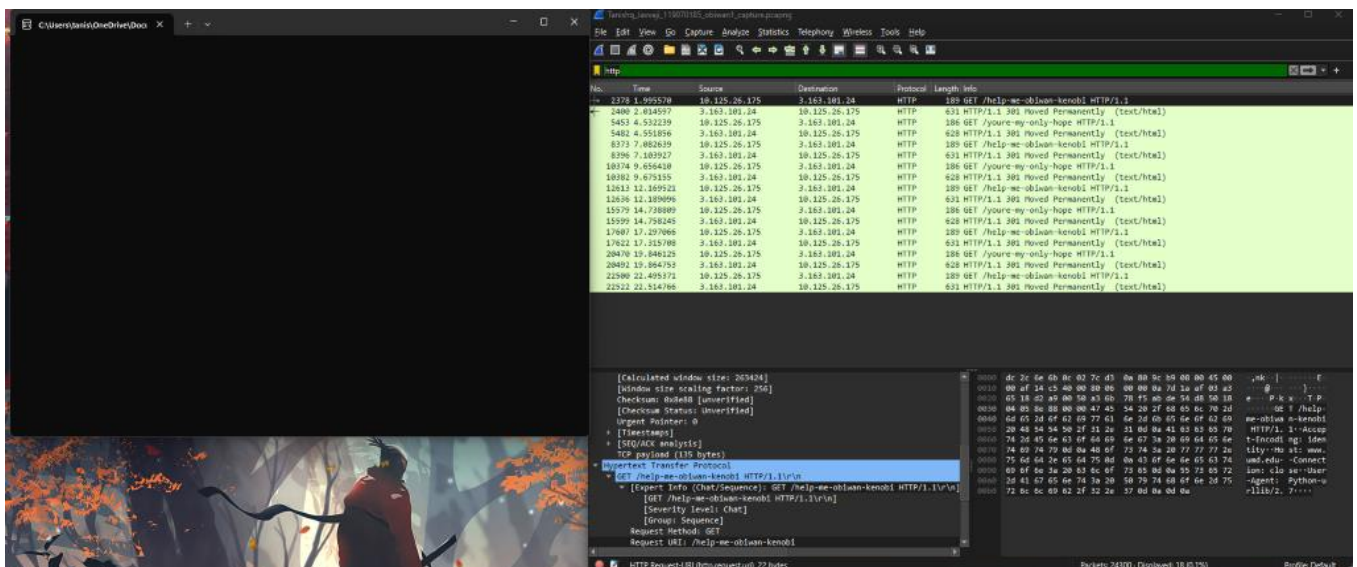


1. Analysis of "obiwan.exe"

The analysis of "obiwan.exe" involved a detailed examination of its execution behavior and network activity. This process was segmented into two main parts: monitoring the execution and behavior of the executable and conducting a thorough Wireshark analysis to understand its network interactions.

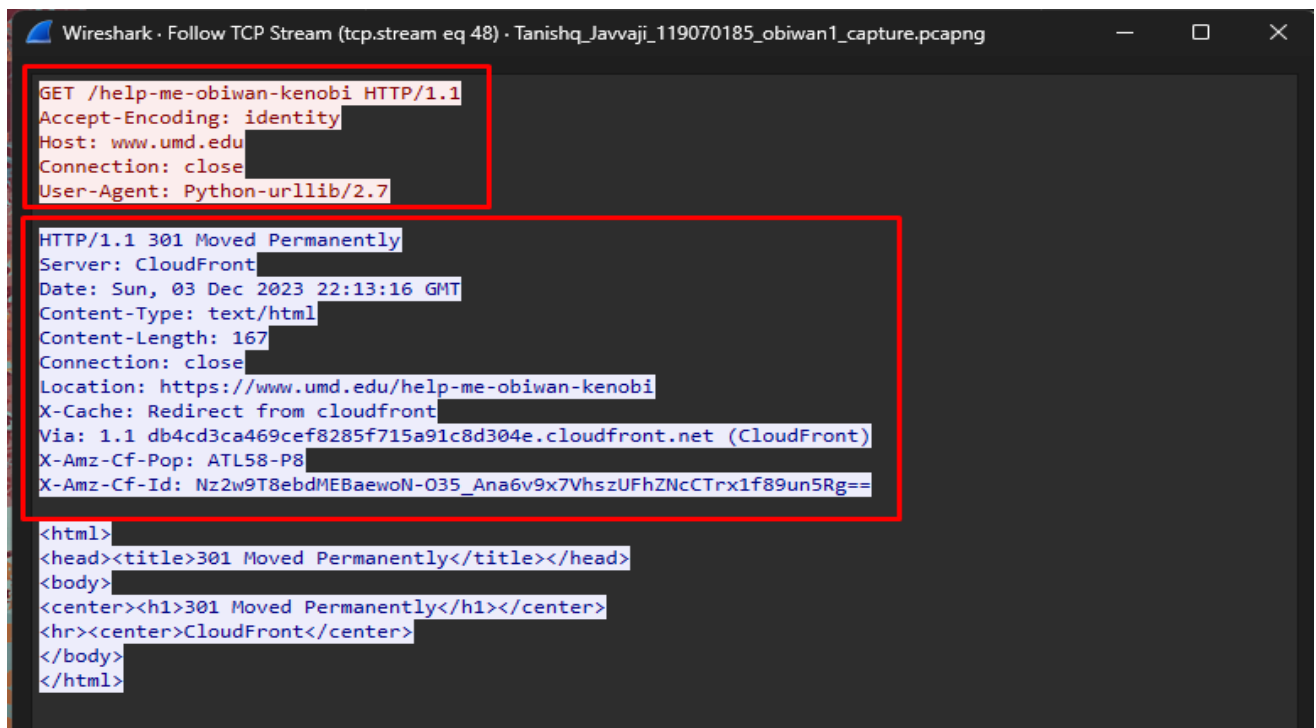
Execution and Behavior:

- **Execution Monitoring:** "obiwan.exe" was executed in a controlled environment, and its activities were closely monitored. This step was crucial to observe the executable's real-time behavior and interactions.
- **Process Explorer Analysis:** Process Explorer was used to track the running status of "obiwan.exe." This tool revealed that the executable was making requests to a remote server over the internet. It provided insights into the state of these requests and the overall behavior of the process.
- **TCP Connections Observation:** The TCP connections associated with "obiwan.exe" were scrutinized. By following the TCP stream, detailed information about the nature and destination of these connections was gathered, offering a clearer picture of the executable's network behavior.



Wireshark Analysis:

- **Packet Capturing:** Wireshark was employed to capture the network packets generated by "obiwan.exe." This was essential to analyze the data being transmitted and received by the executable.
- **Follow TCP Stream for First Request:** Analyzed the TCP stream for the request to "www.umd.edu/help-me-obiwan-kenobi." This revealed the complete HTTP request and response cycle, including the server's "301 Moved Permanently" status code.



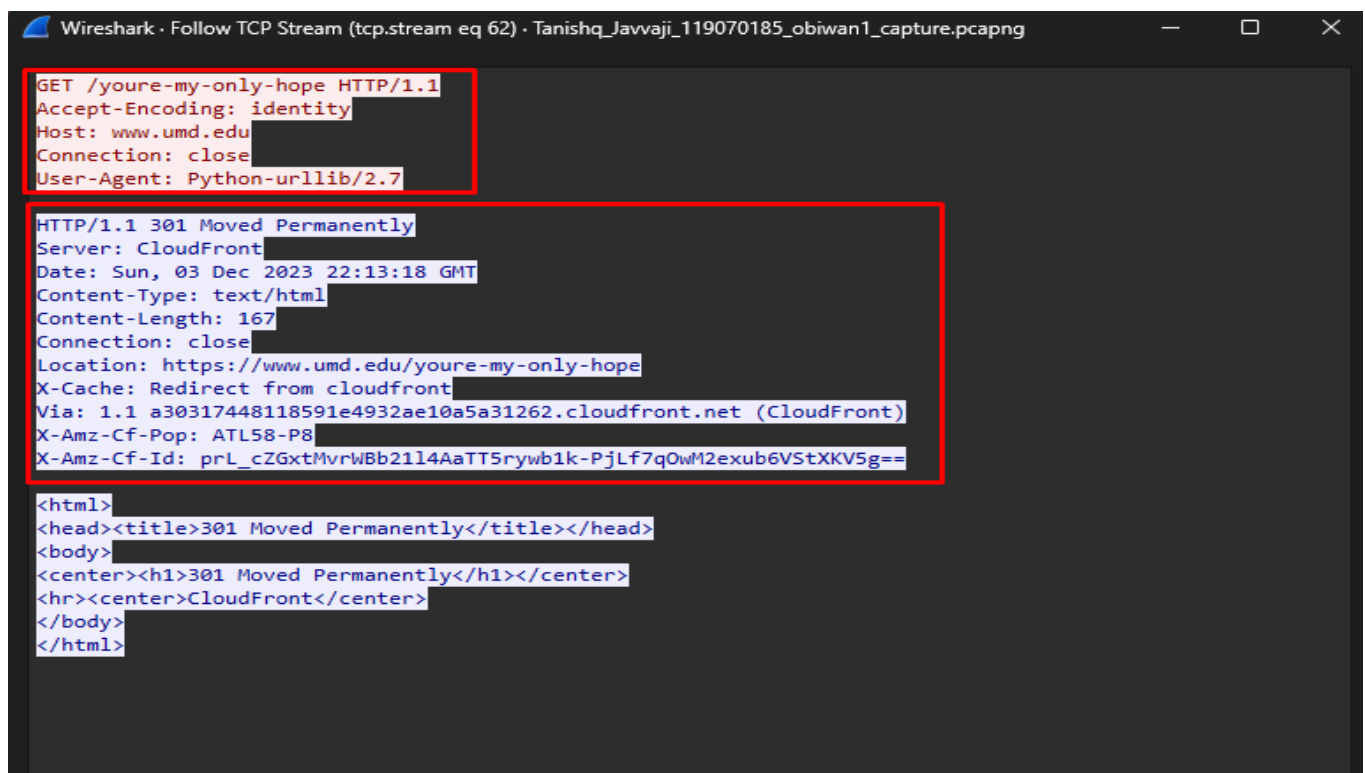
Wireshark · Follow TCP Stream (tcp.stream eq 48) · Tanishq_Javvaji_119070185_obiwan1_capture.pcapng

```
GET /help-me-obiwan-kenobi HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 03 Dec 2023 22:13:16 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/help-me-obiwan-kenobi
X-Cache: Redirect from cloudfront
Via: 1.1 db4cd3ca469cef8285f715a91c8d304e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: Nz2w9T8ebdMEBaewoN-035_Ana6v9x7VhszUFhZNcCTrx1f89un5Rg==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

- **Follow TCP Stream for Second Request:** Similarly, followed the TCP stream for the request to "www.umd.edu/youre-my-only-hope." This provided insights into the nature of the second HTTP request and the server's identical response.



Wireshark · Follow TCP Stream (tcp.stream eq 62) · Tanishq_Javvaji_119070185_obiwan1_capture.pcapng

```
GET /youre-my-only-hope HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 03 Dec 2023 22:13:18 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/youre-my-only-hope
X-Cache: Redirect from cloudfront
Via: 1.1 a30317448118591e4932ae10a5a31262.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: prL_cZGxtMvrWBb2114AaTT5rywb1k-PjLf7qOwM2exub6VStXKV5g==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

- **HTTP Requests Examination:** These conversations revealed that "obiwan.exe" made specific HTTP requests to URLs on the "www.umd.edu" server, notably "www.umd.edu/help-me-obiwan-kenobi" and "www.umd.edu/youre-my-only-hope." This indicated a pattern in the executable's network communication.

Tanishq_Javaji_119070185_obiwan1_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2378	1.995570	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
2400	2.014597	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
5453	4.532239	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
5482	4.551856	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
8373	7.082639	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
8396	7.103927	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
10374	9.656410	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
10382	9.675155	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
12613	12.169521	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
12636	12.189096	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
15579	14.738809	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
15599	14.758245	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
17607	17.297066	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
17622	17.315708	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
20470	19.846125	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
20492	19.864753	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
22500	22.495371	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
22522	22.514766	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)

[Window size scaling factor: 256]
Checksum: 0x8e88 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (135 bytes)
Hypertext Transfer Protocol
GET /help-me-obiwan-kenobi HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /help-me-obiwan-kenobi HTTP/1.1\r\n]
[GET /help-me-obiwan-kenobi HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /help-me-obiwan-kenobi
Request Version: HTTP/1.1

HTTP Request-URI (http.request.uri), 22 bytes

Packets: 24300 · Displayed: 18 (0.1%)

Profile: Default

Tanishq_Javaji_119070185_obiwan1_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2378	1.995570	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
2400	2.014597	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
5453	4.532239	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
5482	4.551856	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
8373	7.082639	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
8396	7.103927	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
10374	9.656410	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
10382	9.675155	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
12613	12.169521	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
12636	12.189096	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
15579	14.738809	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
15599	14.758245	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
17607	17.297066	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
17622	17.315708	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
20470	19.846125	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
20492	19.864753	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
22500	22.495371	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
22522	22.514766	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)

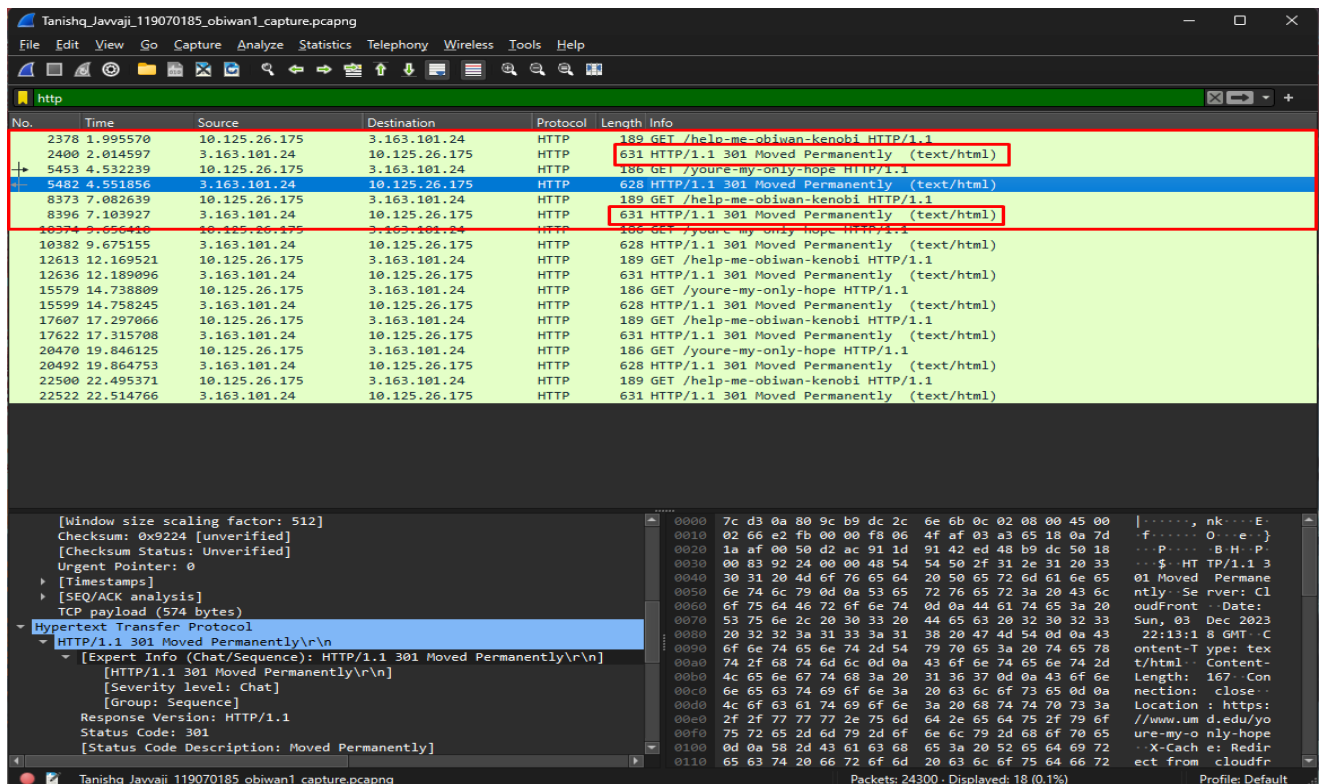
[Window size scaling factor: 256]
Checksum: 0x8e85 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (132 bytes)
Hypertext Transfer Protocol
GET /youre-my-only-hope HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /youre-my-only-hope HTTP/1.1\r\n]
[GET /youre-my-only-hope HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /youre-my-only-hope
Request Version: HTTP/1.1

HTTP Request-URI (http.request.uri), 19 bytes

Packets: 24300 · Displayed: 18 (0.1%)

Profile: Default

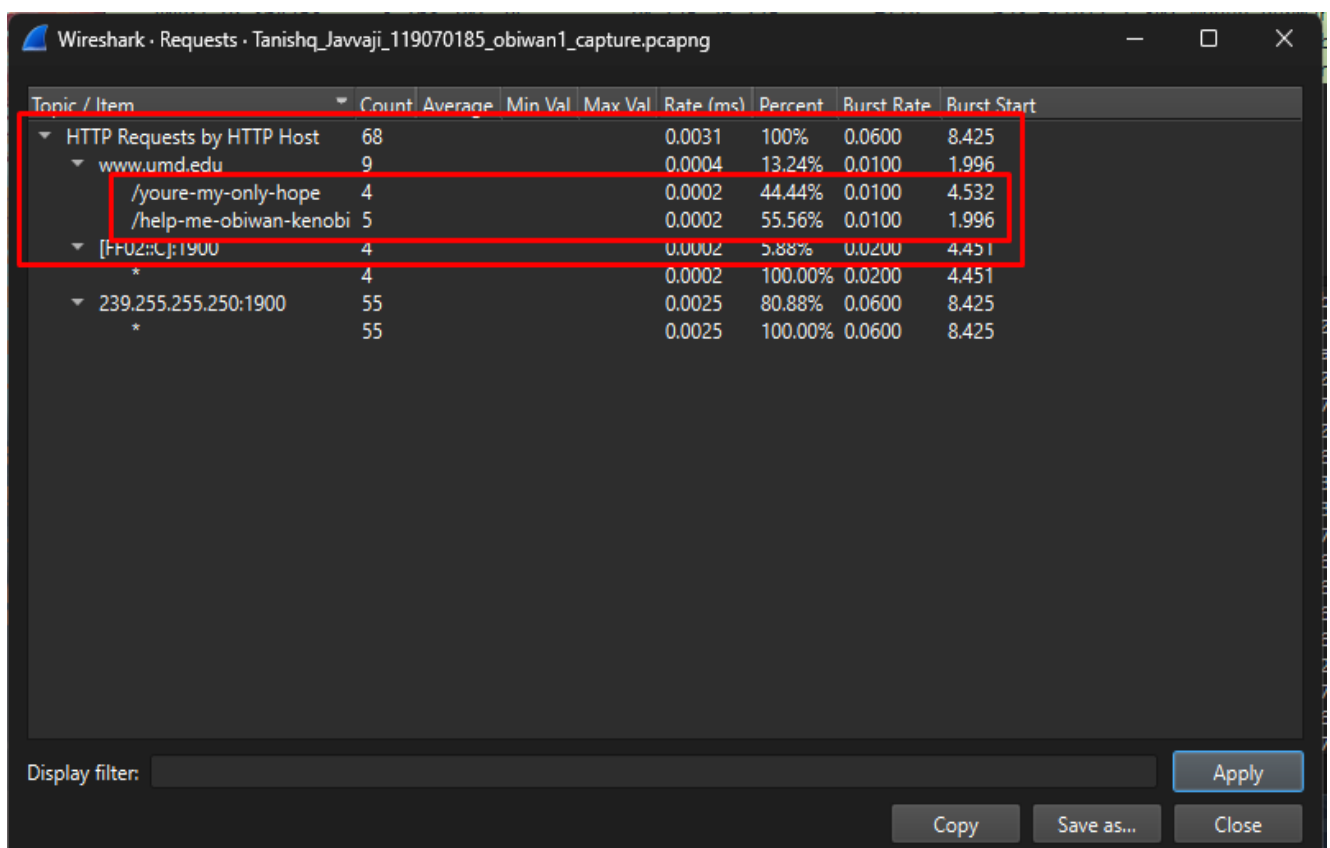
- **Server Responses:** The responses from the server to these requests consistently included a "301 Moved Permanently" status code, suggesting that the requested resources had been permanently relocated, a common technique for redirection in web communication.



The image shows a Wireshark packet capture of an HTTP session. The top pane displays a list of packets, with several highlighted in red. The bottom pane shows the details of a selected packet (No. 631), which is an HTTP 301 Moved Permanently response. The details pane shows the response structure, including the status code and the 'Location' header pointing to 'https://www.umd.edu/youre-my-only-hope'.

No.	Time	Source	Destination	Protocol	Length	Info
2378	1.995570	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
2400	2.014597	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
5453	4.532239	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
5482	4.551856	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
8373	7.082639	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
8396	7.103927	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
8394	6.066446	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
10382	9.675155	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
12613	12.169521	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
12636	12.189096	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
15579	14.738809	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
15599	14.758245	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
17607	17.297066	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
17622	17.315708	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
20470	19.846125	10.125.26.175	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
20492	19.864753	3.163.101.24	10.125.26.175	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
22500	22.495371	10.125.26.175	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
22522	22.514766	3.163.101.24	10.125.26.175	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)

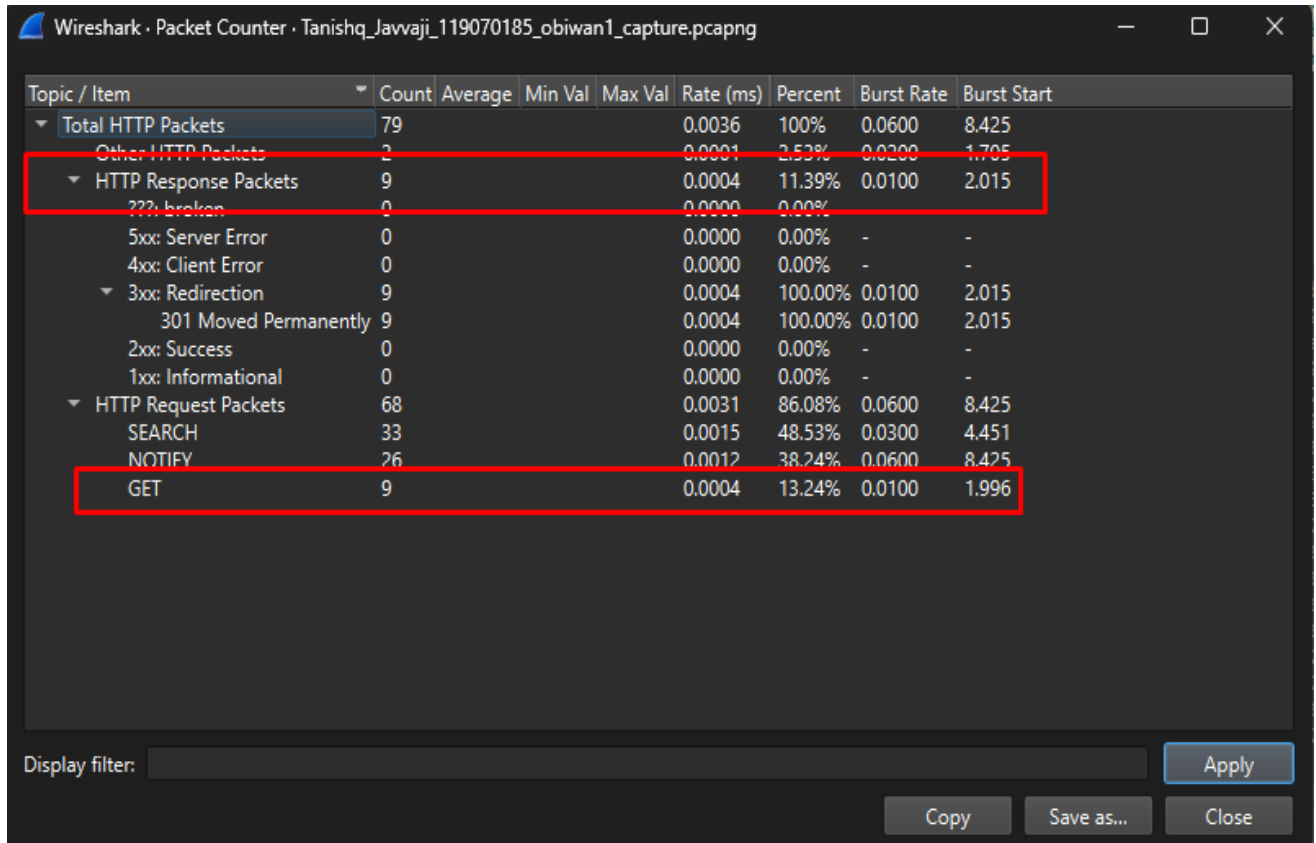
- **Request Tab Findings:** Further analysis in the Requests tab showed a total of 9 requests made to "www.umd.edu." This repetitive nature of communication suggested a programmed or automated behavior in "obiwan.exe."



The image shows the 'Requests' tab in Wireshark, displaying a summary of HTTP requests. The table lists the topic, count, average, min/max values, rate, percent, burst rate, and burst start. The requests are categorized by HTTP host, with a total of 68 requests to 'www.umd.edu'.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	68				0.0031	100%	0.0600	8.425
www.umd.edu	9				0.0004	13.24%	0.0100	1.996
/youre-my-only-hope	4				0.0002	44.44%	0.0100	4.532
/help-me-obiwan-kenobi	5				0.0002	55.56%	0.0100	1.996
[FF02::C]:1900	4				0.0002	5.88%	0.0200	4.451
*	4				0.0002	100.00%	0.0200	4.451
239.255.255.250:1900	55				0.0025	80.88%	0.0600	8.425
*	55				0.0025	100.00%	0.0600	8.425

- **Packet Counter Confirmation:** The Packet Counter tab in Wireshark confirmed these findings, recording 9 requests and 9 corresponding responses, all with the "301 Moved Permanently" status code.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	79				0.0036	100%	0.0600	8.425
Other HTTP Packets	2				0.0001	2.53%	0.0200	1.705
HTTP Response Packets	9				0.0004	11.39%	0.0100	2.015
???: broken	0				0.0000	0.00%		
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	9				0.0004	100.00%	0.0100	2.015
301 Moved Permanently	9				0.0004	100.00%	0.0100	2.015
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	68				0.0031	86.08%	0.0600	8.425
SEARCH	33				0.0015	48.53%	0.0300	4.451
NOTIFY	26				0.0012	38.24%	0.0600	8.425
GET	9				0.0004	13.24%	0.0100	1.996

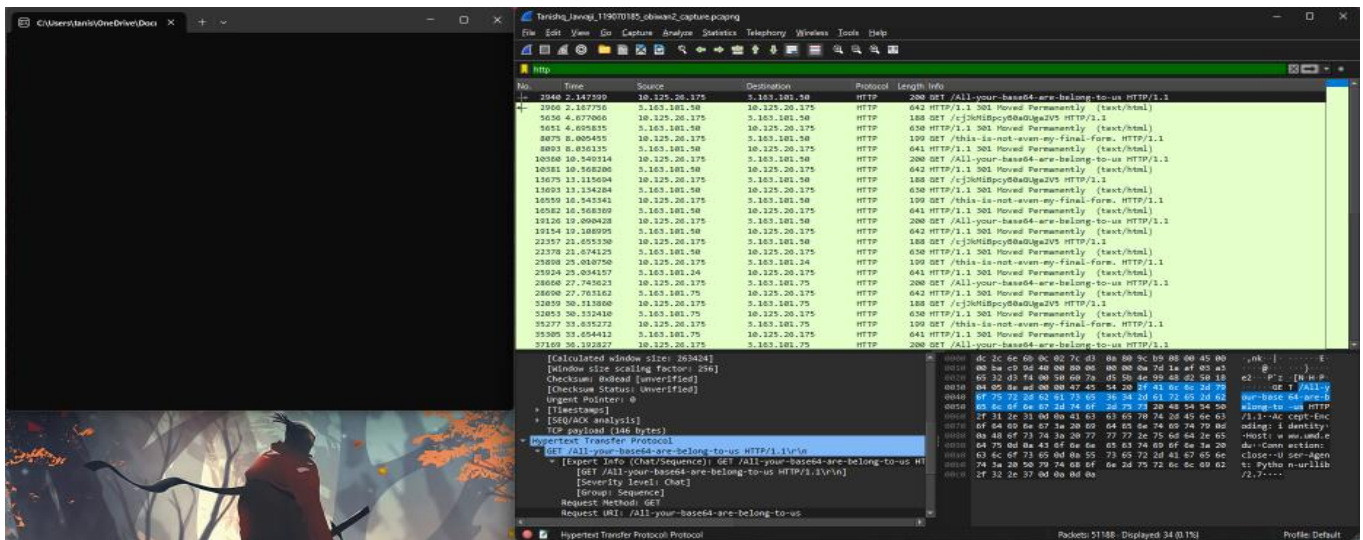
Display filter: Apply Copy Save as... Close

- **Export Attempts:** An attempt was made to export objects from these requests for further examination. However, this did not yield significant findings, as the web pages appeared to be continuously redirected, hindering the retrieval of more detailed information.

2. Analysis of "obiwan2.exe"

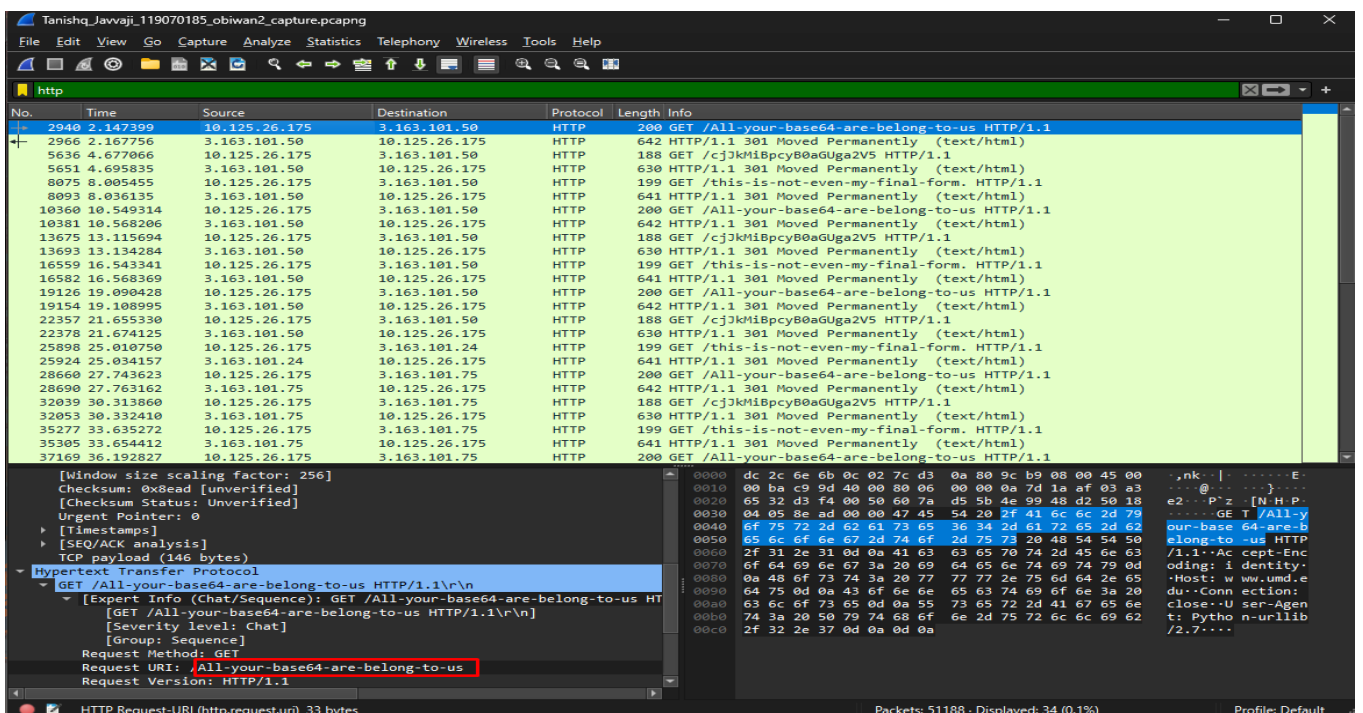
Execution and Behavior:

- **Execution Monitoring:** The file was executed in a secure environment, with its activities and behavior under close observation.
- **Process Explorer Analysis:** Process Explorer provided insights into the running status of "obiwan2.exe," focusing on its system interactions and network requests.
- **TCP Connections Observation:** The TCP connections related to "obiwan2.exe" were meticulously monitored, examining the nature and endpoints of these connections.



Wireshark Analysis:

- **Packet Capturing:** Wireshark was used to capture the network packets from "obiwan2.exe."



- **HTTP Requests Examination:** In the HTTP analysis of "obiwan2.exe," Wireshark revealed three distinct HTTP requests made by the executable to the www.umd.edu, each carrying a unique and potentially significant payload. The first request was directed to <http://www.umd.edu/All-your-base64-are-belong-to-us> a reference that might indicate a coded or disguised message. The second request targeted <http://www.umd.edu/cjJkMiBpcyB0aGUga2V5> a base64 encoded string that, when decoded, translates to "r2d2 is the key," suggesting the possible use of an encryption key or passphrase. The final request was to <http://www.umd.edu/this-is-not-even-my-final-form> hinting at the possibility that "obiwan2.exe" could be part of a larger, more complex malware operation or signalling the existence of additional, yet undiscovered, components of the malware system.

Tanishq_Javvaji_119070185_obiwan2_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2940	2.147399	10.125.26.175	3.163.101.50	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
2966	2.167756	3.163.101.50	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
5636	4.677066	10.125.26.175	3.163.101.50	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
5651	4.695835	3.163.101.50	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
8075	8.005455	10.125.26.175	3.163.101.50	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
8093	8.036135	3.163.101.50	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
10360	10.549314	10.125.26.175	3.163.101.50	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
10381	10.568206	3.163.101.50	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
13675	13.115694	10.125.26.175	3.163.101.50	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
13693	13.134284	3.163.101.50	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
16559	16.543341	10.125.26.175	3.163.101.50	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
16582	16.568369	3.163.101.50	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
19126	19.090428	10.125.26.175	3.163.101.50	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
19154	19.108995	3.163.101.50	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
22357	21.655330	10.125.26.175	3.163.101.50	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
22378	21.674125	3.163.101.50	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
25898	25.010750	10.125.26.175	3.163.101.24	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
25924	25.034157	3.163.101.24	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
28660	27.743623	10.125.26.175	3.163.101.75	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
28690	27.763162	3.163.101.75	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
32039	30.313860	10.125.26.175	3.163.101.75	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
32053	30.332410	3.163.101.75	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
35277	33.635272	10.125.26.175	3.163.101.75	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
35305	33.654412	3.163.101.75	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
37169	36.192827	10.125.26.175	3.163.101.75	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1

[Expert Info (Chat/Sequence): GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1\r\n]
 [GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /cjJkMi8PcyB0aGUga2V5
 Request Version: HTTP/1.1
 Accept-Encoding: identity\r\n
 Host: www.umd.edu\r\n
 Connection: close\r\n
 User-Agent: Python-urllib/2.7\r\n
 \r\n
 [Full request URI: http://www.umd.edu/cjJkMi8PcyB0aGUga2V5]
 [HTTP request 1/1]
 [Response in frame: 5651]

HTTP Request-URI (http.request.uri), 21 bytes

Packets: 51188 - Displayed: 34 (0.1%)

Profile: Default

Tanishq_Javvaji_119070185_obiwan2_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2940	2.147399	10.125.26.175	3.163.101.50	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
2966	2.167756	3.163.101.50	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
5636	4.677066	10.125.26.175	3.163.101.50	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
5651	4.695835	3.163.101.50	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
8075	8.005455	10.125.26.175	3.163.101.50	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
8093	8.036135	3.163.101.50	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
10360	10.549314	10.125.26.175	3.163.101.50	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
10381	10.568206	3.163.101.50	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
13675	13.115694	10.125.26.175	3.163.101.50	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
13693	13.134284	3.163.101.50	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
16559	16.543341	10.125.26.175	3.163.101.50	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
16582	16.568369	3.163.101.50	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
19126	19.090428	10.125.26.175	3.163.101.50	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
19154	19.108995	3.163.101.50	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
22357	21.655330	10.125.26.175	3.163.101.50	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
22378	21.674125	3.163.101.50	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
25898	25.010750	10.125.26.175	3.163.101.24	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
25924	25.034157	3.163.101.24	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
28660	27.743623	10.125.26.175	3.163.101.75	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
28690	27.763162	3.163.101.75	10.125.26.175	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
32039	30.313860	10.125.26.175	3.163.101.75	HTTP	188	GET /cjJkMi8PcyB0aGUga2V5 HTTP/1.1
32053	30.332410	3.163.101.75	10.125.26.175	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
35277	33.635272	10.125.26.175	3.163.101.75	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
35305	33.654412	3.163.101.75	10.125.26.175	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
37169	36.192827	10.125.26.175	3.163.101.75	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1

[Expert Info (Chat/Sequence): GET /this-is-not-even-my-final-form. HTTP/1.1\r\n]
 [GET /this-is-not-even-my-final-form. HTTP/1.1\r\n]
 [Severity level: Chat]
 [Group: Sequence]
 Request Method: GET
 Request URI: /this-is-not-even-my-final-form.
 Request Version: HTTP/1.1
 Accept-Encoding: identity\r\n
 Host: www.umd.edu\r\n
 Connection: close\r\n
 User-Agent: Python-urllib/2.7\r\n
 \r\n
 [Full request URI: http://www.umd.edu/this-is-not-even-my-final-form.]
 [HTTP request 1/1]
 [Response in frame: 8093]

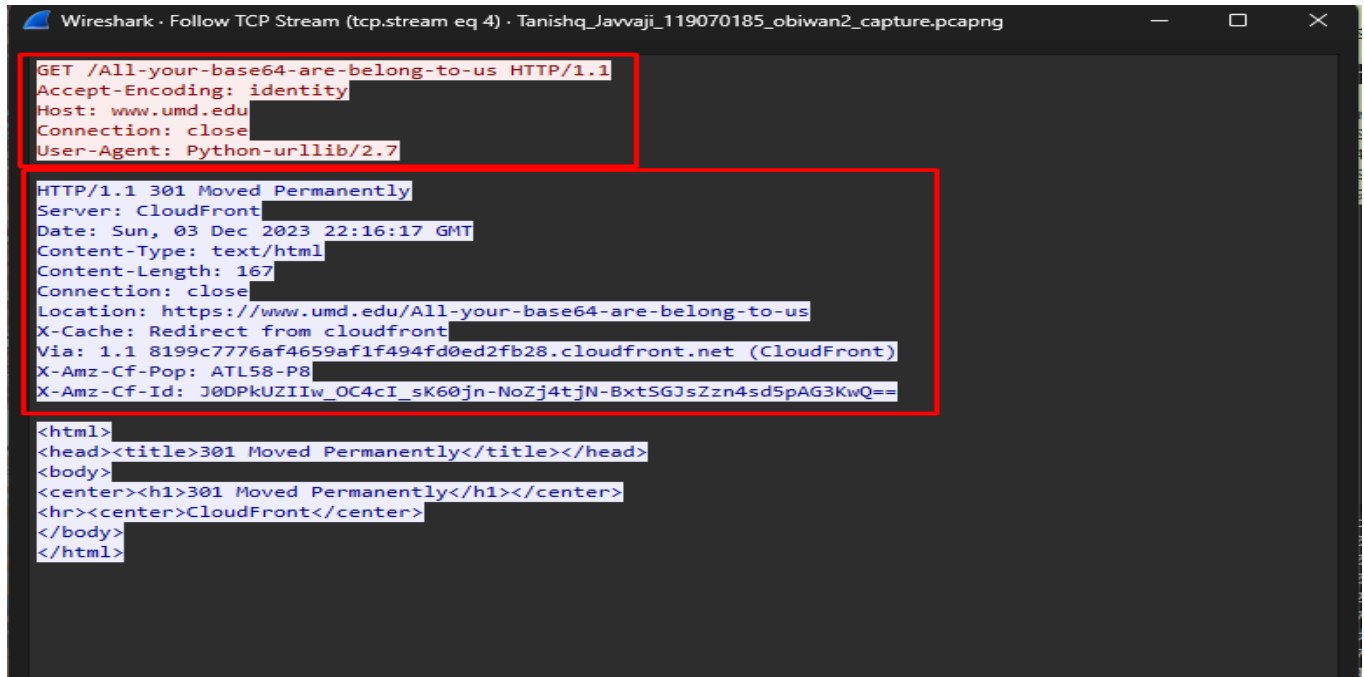
HTTP Request-URI (http.request.uri), 32 bytes

Packets: 51188 - Displayed: 34 (0.1%)

Profile: Default

- Follow TCP Stream for First Request:

- The TCP stream for the HTTP request to "<http://www.umd.edu/All-your-base64-are-belong-to-us>" was analysed. This detailed investigation revealed the complete HTTP request and the server's response, which included a "301 Moved Permanently" status code, indicating a redirection.



```
Wireshark · Follow TCP Stream (tcp.stream eq 4) · Tanishq_Javvaji_119070185_obiwan2_capture.pcapng

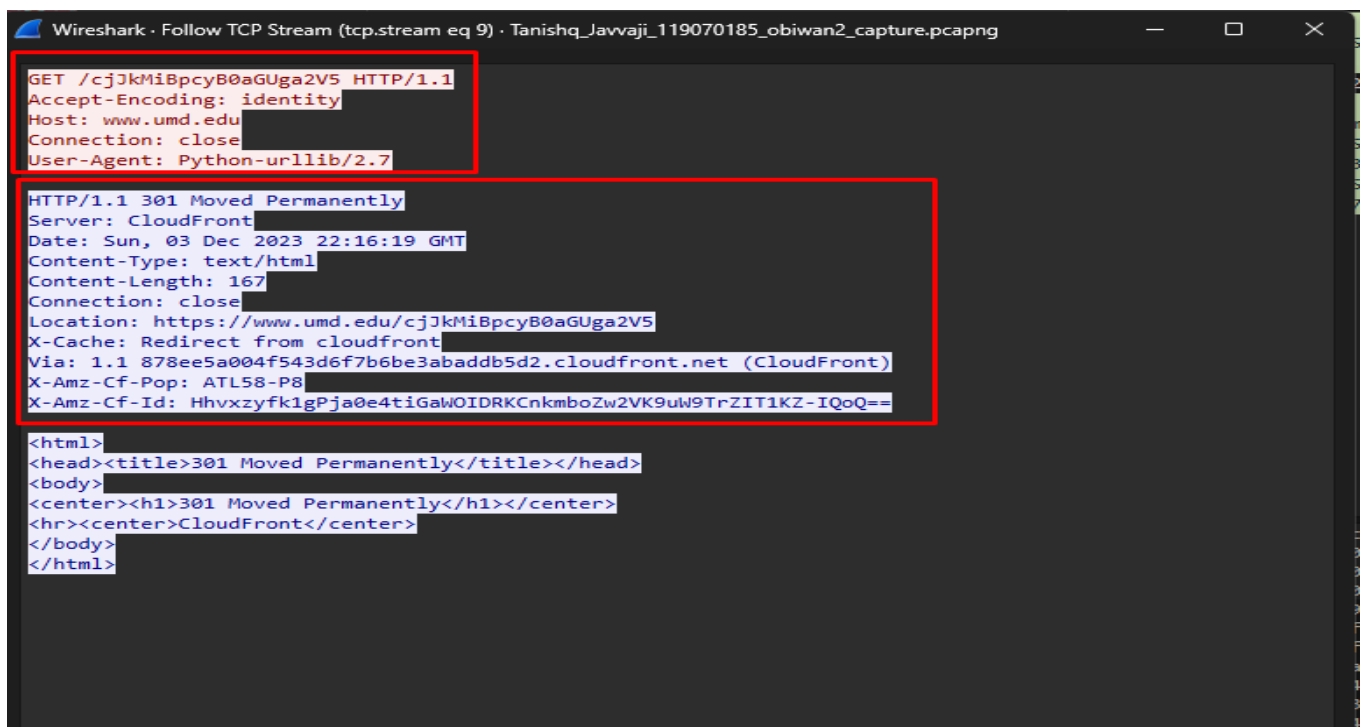
GET /All-your-base64-are-belong-to-us HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 03 Dec 2023 22:16:17 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/All-your-base64-are-belong-to-us
X-Cache: Redirect from cloudfront
Via: 1.1 8199c7776af4659af1f494fd0ed2fb28.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: J0DPkUZIIw_OC4cI_sK60jn-NoZj4tjN-Bxt5GJsZzn4sd5pAG3KwQ==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

- Follow TCP Stream for Second Request:

- A similar analysis was conducted for the TCP stream of the request to "<http://www.umd.edu/cjJkMiBpcyB0aGUga2V5>." This provided valuable insights into the second HTTP request's nature and the server's identical redirection response.



```
Wireshark · Follow TCP Stream (tcp.stream eq 9) · Tanishq_Javvaji_119070185_obiwan2_capture.pcapng

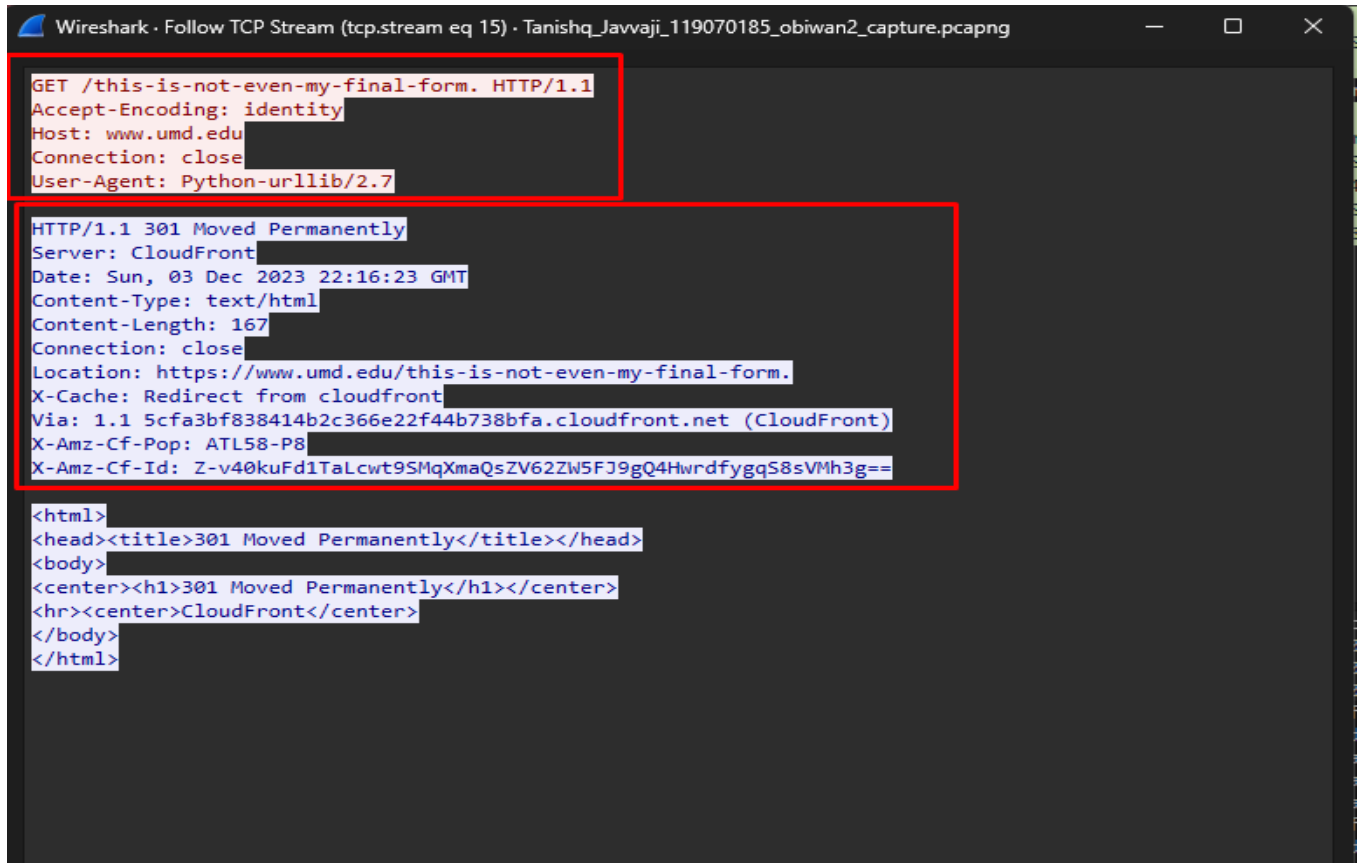
GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 03 Dec 2023 22:16:19 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/cjJkMiBpcyB0aGUga2V5
X-Cache: Redirect from cloudfront
Via: 1.1 878ee5a004f543d6f7b6be3abaddb5d2.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: Hhvxzyfk1gPja0e4tiGawOIDRKcnkmb0Zw2VK9uW9TrZIT1KZ-IQoQ==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

- **Follow TCP Stream for Third Request:**

- The stream for the request to "<http://www.umd.edu/this-is-not-even-my-final-form>" was also followed. This gave an understanding of the communication pattern and response for the third request, which was consistent with the earlier findings.



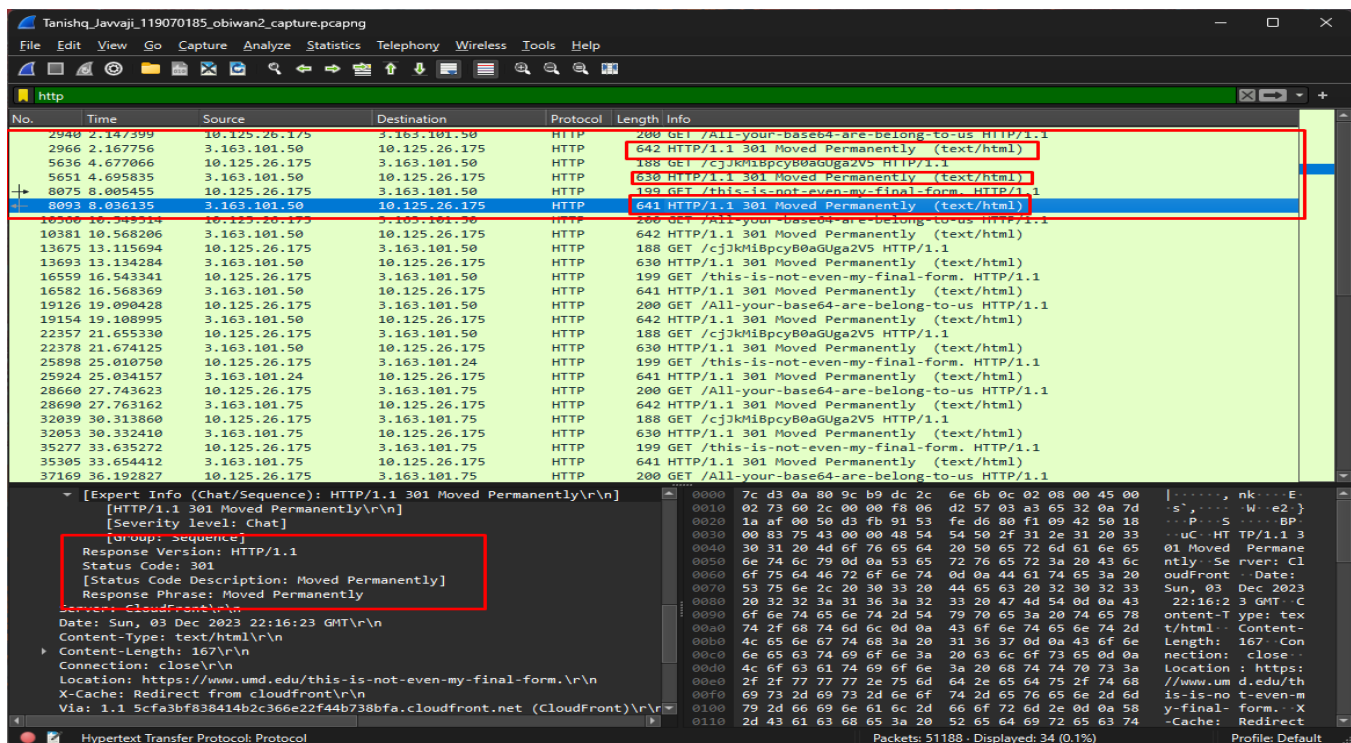
```
Wireshark · Follow TCP Stream (tcp.stream eq 15) · Tanishq_Javvaji_119070185_obiwan2_capture.pcapng

GET /this-is-not-even-my-final-form. HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 03 Dec 2023 22:16:23 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/this-is-not-even-my-final-form.
X-Cache: Redirect from cloudfront
Via: 1.1 5cfa3bf838414b2c366e22f44b738bfa.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: Z-v40kuFd1TaLcwt9SMqXmaQsZV62ZW5FJ9gQ4HwrdfygqS8sVMh3g==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

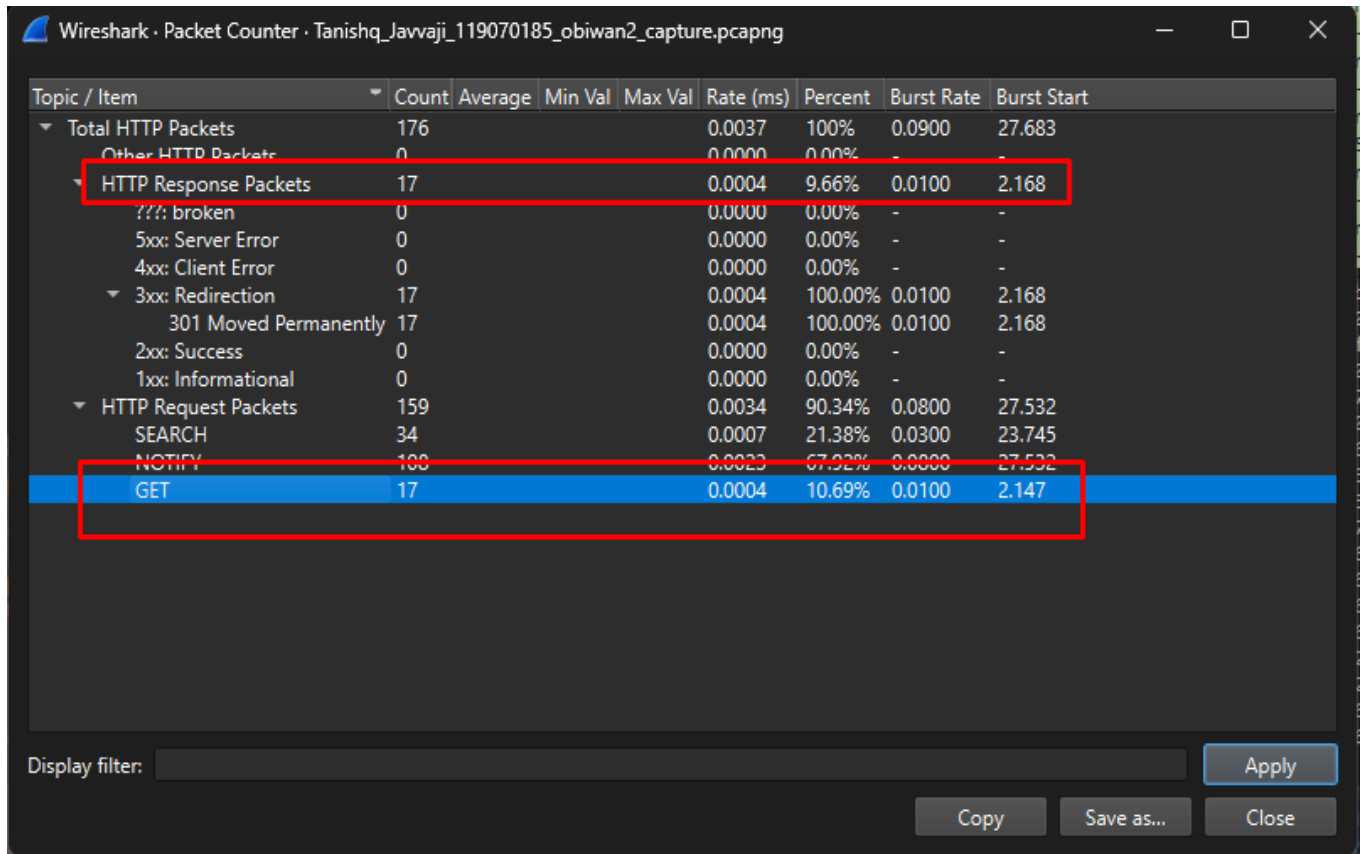
- **Server Responses:** The responses from the server to these requests consistently included a "301 Moved Permanently" status code, suggesting that the requested resources had been permanently relocated, a common technique for redirection in web communication.



- Request Tab Findings:** A detailed examination of the Requests tab in Wireshark during the analysis of "obiwan2.exe" revealed a total of 17 HTTP requests made to "www.umd.edu." This pattern of repeated communication indicates a programmed or automated behavior within "obiwan2.exe." Each request, while directed to the same domain, targeted different URLs, suggesting a deliberate sequence of actions or messages being transmitted. The consistent number of requests and their specific targeting align with the characteristics of an executable programmed for systematic communication, possibly as part of a larger coordinated operation or to execute a sequence of tasks based on server responses. This repetitive and structured nature of the network activity underscores the sophistication and potential complexity embedded within "obiwan2.exe."

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	159				0.0034	100%	0.0800	27.532
www.umd.edu	17				0.0004	10.69%	0.0100	2.147
/this-is-not-even-my-final-form.	5				0.0001	29.41%	0.0100	8.005
/cjJkMiBpcyB0aGUga2V5	6				0.0001	35.29%	0.0100	4.677
/All-your-base64-are-belong-to-us	6				0.0001	35.29%	0.0100	2.147
[FF02::C]:1900	43				0.0009	27.04%	0.0300	33.297
239.255.255.250:1900	99				0.0021	62.26%	0.0600	7.549

- **Packet Counter Confirmation:** Upon reviewing the Packet Counter tab in Wireshark during the analysis of "obiwan2.exe," a consistent pattern was observed. The Packet Counter recorded a total of 17 requests sent to "www.umd.edu" and an equal number of responses received, all bearing the "301 Moved Permanently" status code.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Total HTTP Packets	176				0.0037	100%	0.0900	27.683
Other HTTP Packets	0				0.0000	0.00%	-	-
▼ HTTP Response Packets	17				0.0004	9.66%	0.0100	2.168
??? broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
▼ 3xx: Redirection	17				0.0004	100.00%	0.0100	2.168
301 Moved Permanently	17				0.0004	100.00%	0.0100	2.168
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
▼ HTTP Request Packets	159				0.0034	90.34%	0.0800	27.532
SEARCH	34				0.0007	21.38%	0.0300	23.745
NOTIFY	100				0.0023	67.92%	0.0000	27.532
GET	17				0.0004	10.69%	0.0100	2.147

Display filter: Apply

Copy Save as... Close

3. Analysis of "not-the-droids-you-are-looking-for.mp3" using Base64 Decoded Key and Veracrypt

The analysis of the encrypted MP3 file, "not-the-droids-you-are-looking-for.mp3," involved a critical decryption step using a key obtained from the analysis of "obiwan2.exe" and employing Veracrypt for the decryption process.

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a file tree with 'My Music (23)' selected. The main pane shows a listing of files in the directory '/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/My Music'. The file 'not-the-droids-you-are-looking-for.mp3' is highlighted in red. A red box around the file name and its score (0) contains the text 'Has an Likely Notable analysis result score'.

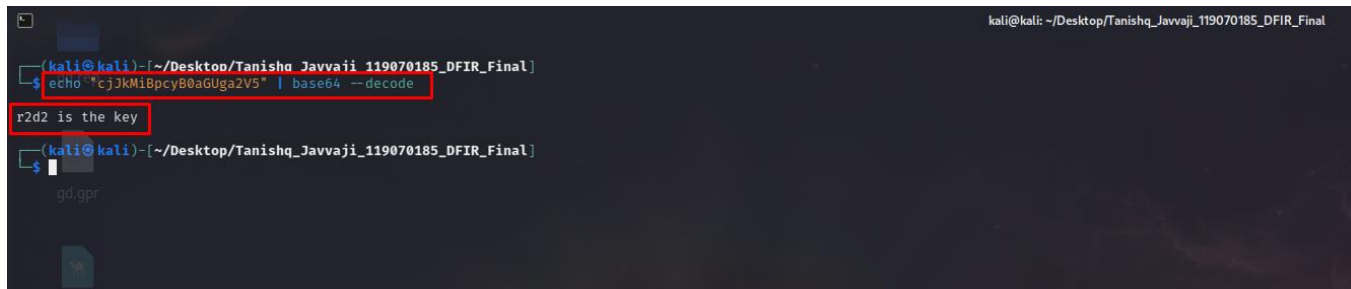
Name	S	C	O	Modified Time	Change Time
Concerto-4-Violini-2_1eleimann.mp3:Zone.Identifier			2	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54 EDT
Courante_1st_Cello_Suite.mp3			0	2017-07-13 14:07:50 EDT	2017-07-13 14:07:50 EDT
Courante_1st_Cello_Suite.mp3:Zone.Identifier			2	2017-07-13 14:07:50 EDT	2017-07-13 14:07:50 EDT
Desktop.ini			1	2017-07-12 11:05:54 EDT	2017-07-12 11:05:54 EDT
Gigue_3rd_Cello_Suite-Bach.mp3			0	2017-07-13 14:07:26 EDT	2017-07-13 14:07:26 EDT
Gigue_3rd_Cello_Suite-Bach.mp3:Zone.Identifier			2	2017-07-13 14:07:26 EDT	2017-07-13 14:07:26 EDT
Largo+from+-Concerto-No5_JS_Bach.mp3			0	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT
Largo+from+-Concerto-No5_JS_Bach.mp3:Zone.Id			2	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT
Menuettos_1_2_from_41st_Symphony.mp3			0	2017-07-13 14:07:34 EDT	2017-07-13 14:07:34 EDT
Menuettos_1_2_from_41st_Symphony.mp3:Zone.Id			2	2017-07-13 14:07:34 EDT	2017-07-13 14:07:34 EDT
not-the-droids-you-are-looking-for.mp3			0	2017-07-13 13:59:36 EDT	2017-07-13 15:34:01 EDT
Rhapsody_No2_G-Minor_Brahms.mp3					2017-07-13 14:07:06 EDT

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a file tree with 'Analysis Results' selected, and 'Encryption Suspected (3)' is highlighted in red. The main pane shows a listing of files under the heading 'Encryption Suspected'. The file 'not-the-droids-you-are-looking-for.mp3' is highlighted in red. A red box around the file name and its score (0) contains the text 'Likely Notable'.

Source Name	S	C	O	Source Type	Score	Conclusion
1cbdef1f8bc270c29b0400ab5dc828d319b8766e6b8b			0	File	Likely Notable	
not-the-droids-you-are-looking-for.mp3			0	File	Likely Notable	
oembios.bin			1	File	Likely Notable	

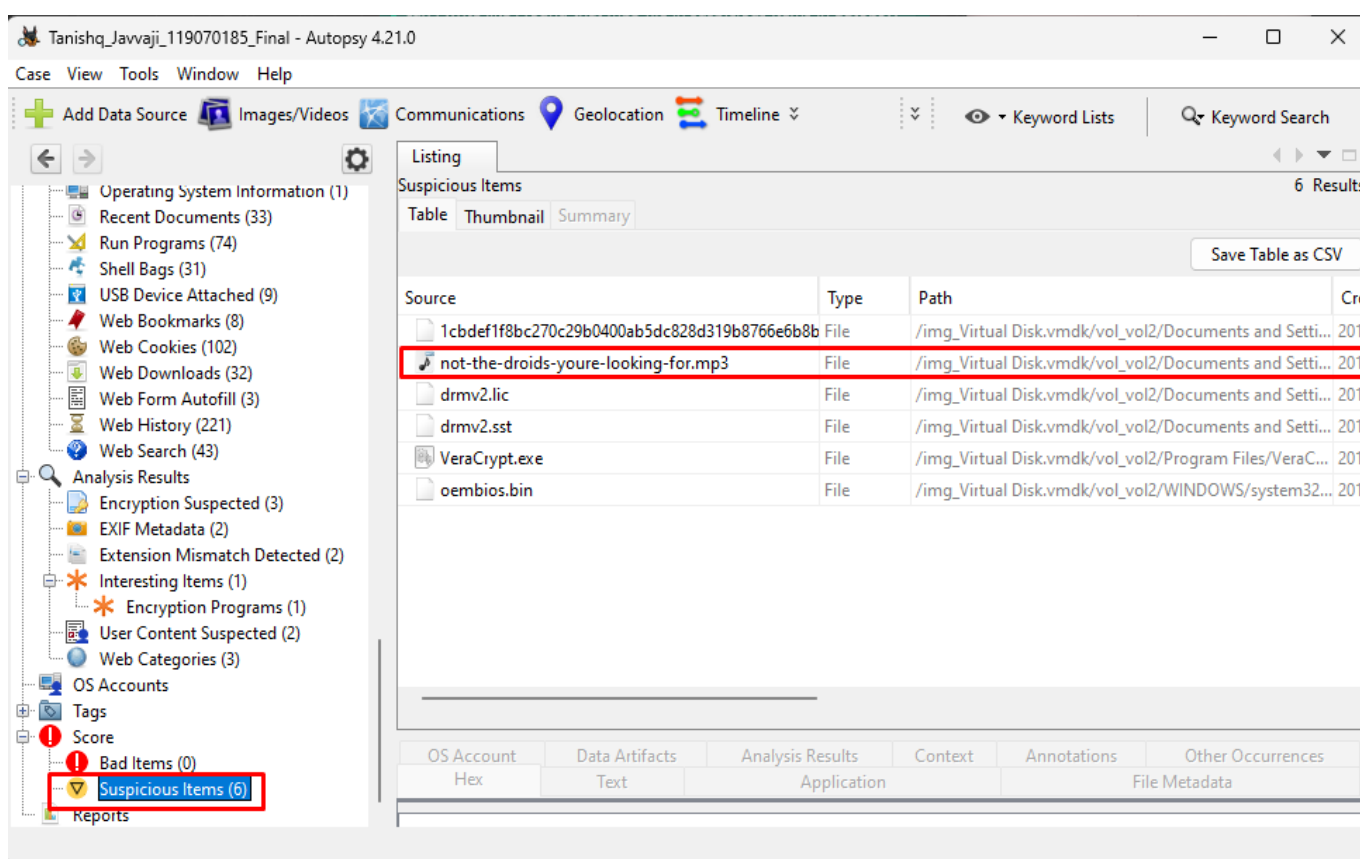
Decryption Process:

- **Base64 Decoded Key:** The analysis of "obiwan2.exe" yielded a base64 encoded string, which when decoded read "r2d2 is the key." This phrase was presumed to be the decryption key.



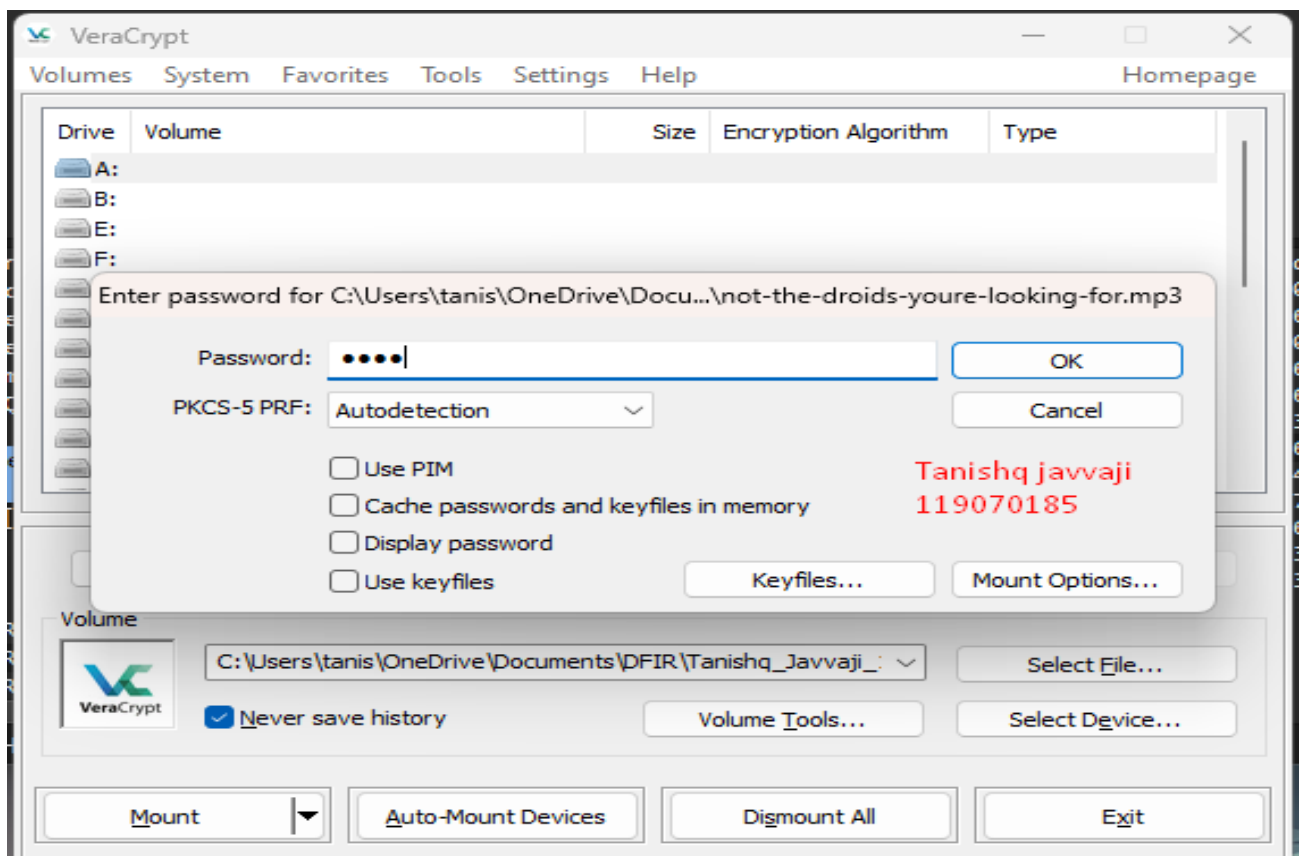
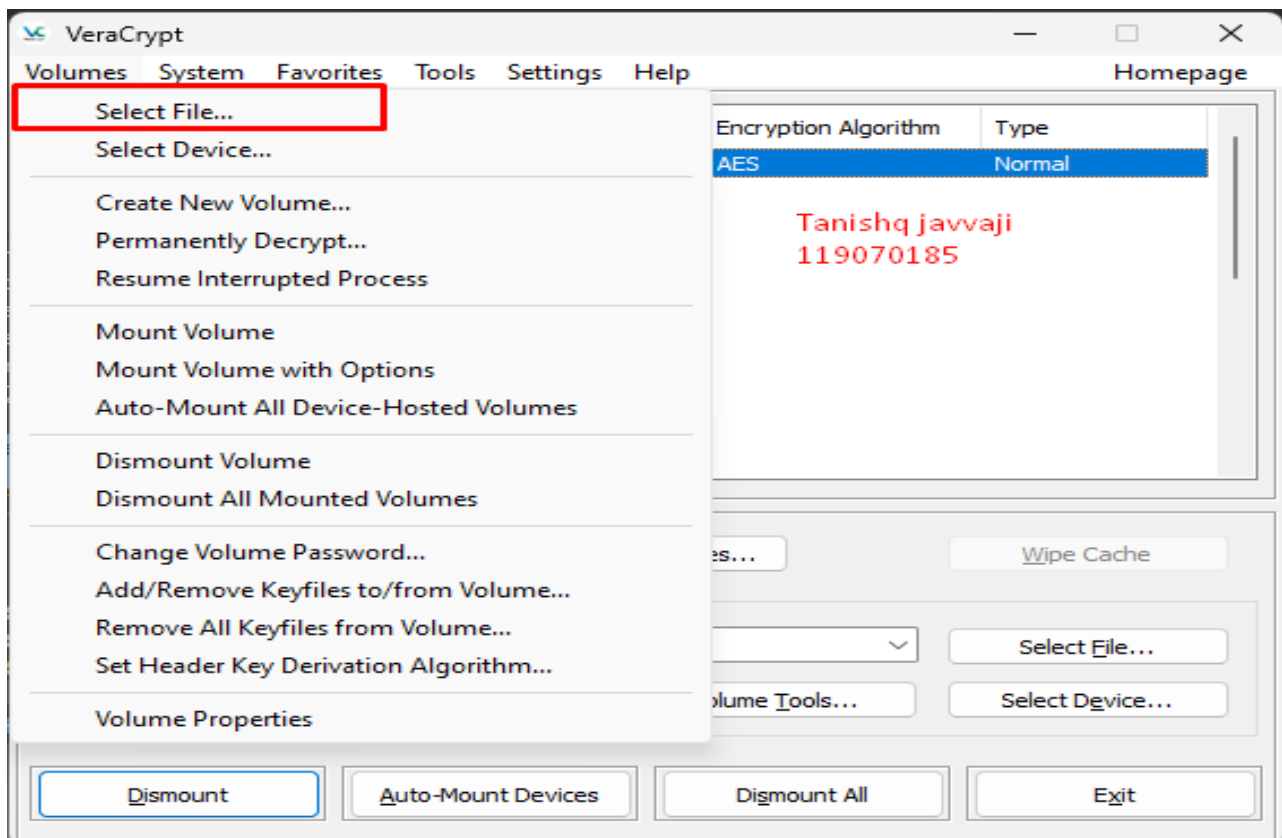
```
(kali@kali)~[/Desktop/Tanishq_Javvaji_119070185_DFIR_Final]
$ echo "cjJkMiBpcyB0aGUa2V5" | base64 --decode
r2d2 is the key
(kali@kali)~[/Desktop/Tanishq_Javvaji_119070185_DFIR_Final]
$
```

- **Using Veracrypt:** Veracrypt, known for its robust encryption and decryption capabilities, was used for decrypting the MP3 file.



Decryption Steps:

- The encrypted MP3 file was loaded into Veracrypt.
- "r2d2" was entered as the decryption passphrase, derived from the base64 decoded message.
- The decryption process was initiated, with successful completion being closely monitored.

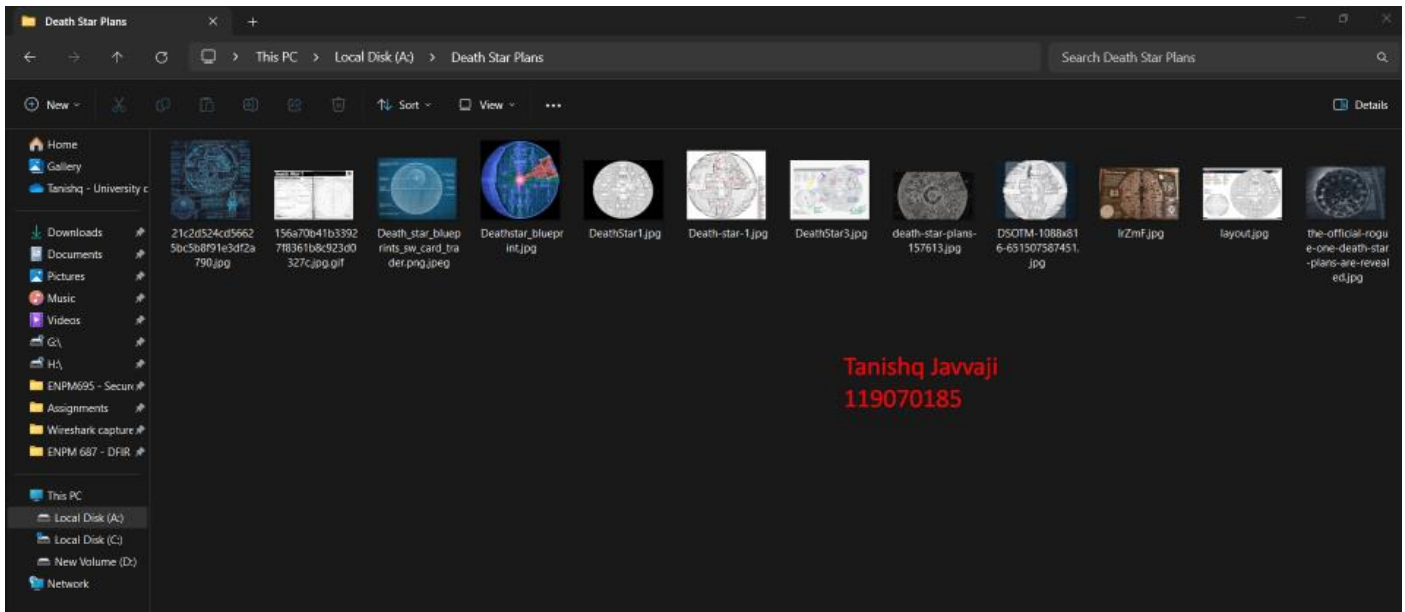


Post-Decryption Examination:

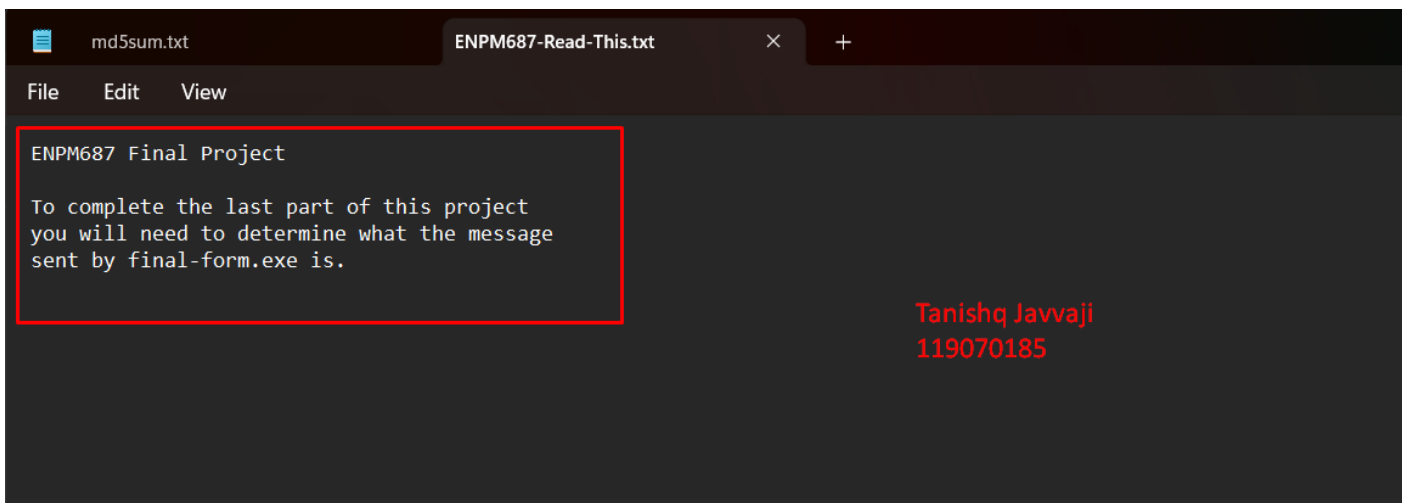
- The successful decryption of "not-the-droids-you-are-looking-for.mp3" allowed for a detailed examination of its previously encrypted contents.

- **Contents of the Decrypted File:**

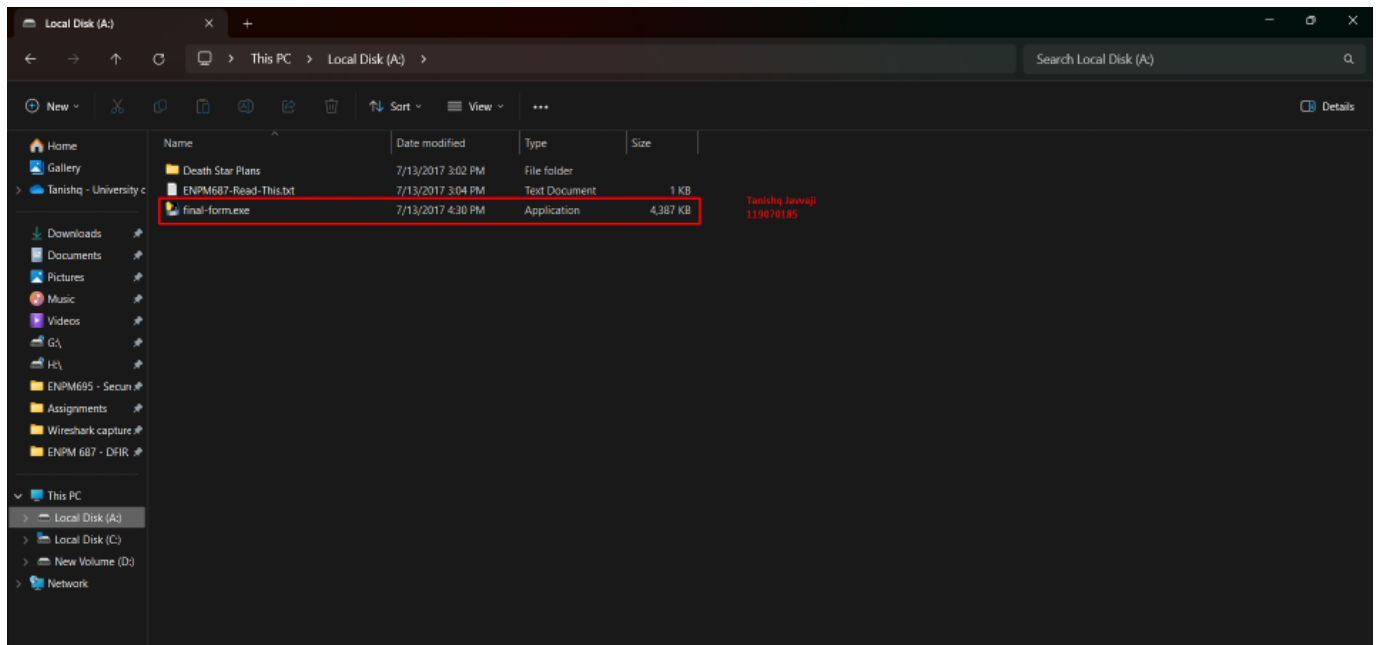
- Inside the decrypted file, a folder named “Death Star Plans” was found, containing images and schematics of the Death Star, suggesting the file's use for covert storage and transmission of sensitive information.



- A crucial discovery was a text file named “ENPM687-Read-This.txt,” which contained instructions to run 'final-form.exe', indicating further steps in the unfolding investigation.



- Importantly, the decrypted file also included an executable named "final-form.exe." This file's presence alongside the other contents suggested it could be a critical piece in understanding the broader context and potential intent of the data hidden within the MP3 file.

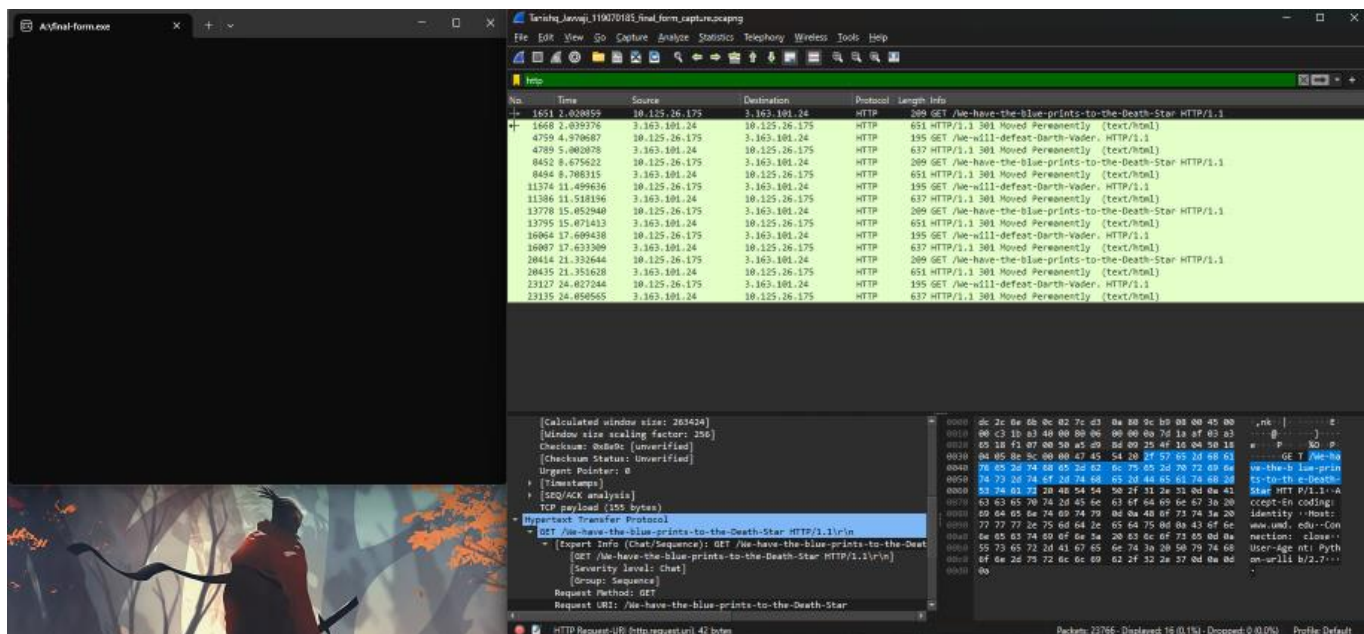


4. Analysis of "final-form.exe"

The analysis of "final-form.exe" involved a comprehensive examination of its execution behavior and network activity. This analysis was divided into two primary components: monitoring the execution and behavior of the executable, and conducting a detailed Wireshark analysis to understand its network interactions.

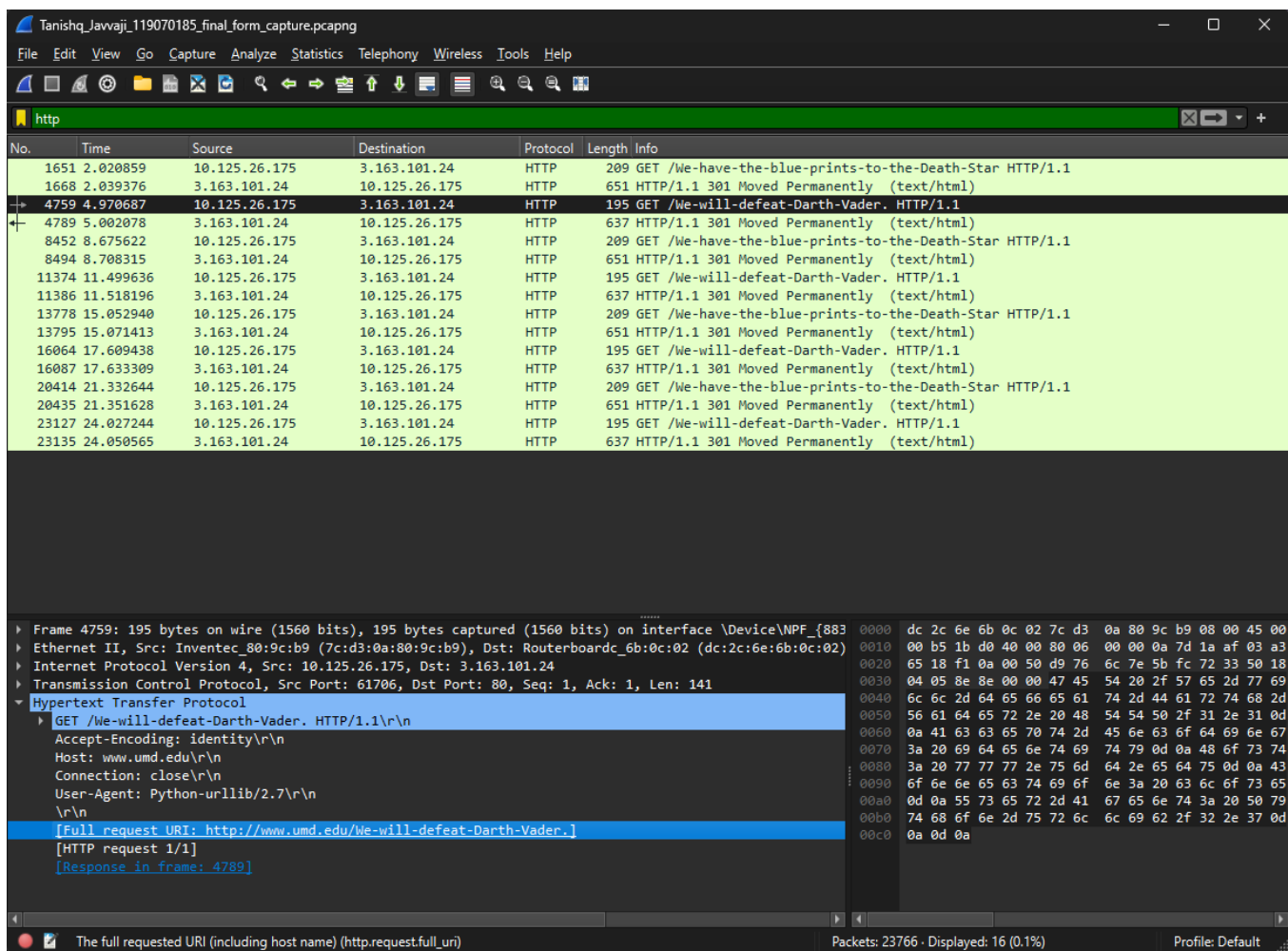
Execution and Behavior:

- **Execution Monitoring:** "final-form.exe" was executed in a controlled environment to closely monitor its activities. This was crucial for observing the executable's real-time behavior and interactions with the system and network.
- **Process Explorer Analysis:** Process Explorer was utilized to observe the running status of "final-form.exe." This tool provided insights into the executable's processes, revealing its attempts to establish connections to remote servers over the internet and offering a detailed view of its overall behavior.
- **TCP Connections Observation:** The TCP connections associated with "final-form.exe" were carefully examined. Detailed information about the nature and destination of these connections was gathered by monitoring the TCP stream, which helped in understanding the executable's network behavior.



Wireshark Analysis:

- **Packet Capturing:** Wireshark was employed to capture the network packets generated by "final-form.exe," a critical step in analyzing the data being transmitted and received by the executable.



- **Follow TCP Stream for First Request:** The TCP stream was analyzed for the first HTTP request made by "final-form.exe" to the URL "<http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star>."

This revealed the complete HTTP request and response cycle, including the server's "301 Moved Permanently" status code.



```
Wireshark · Follow TCP Stream (tcp.stream eq 1) · Tanishq_Javvaji_119070185_final_form_capture.pcapng

GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Mon, 04 Dec 2023 00:27:04 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star
X-Cache: Redirect from cloudfront
Via: 1.1 5cbb59a113897ae54ff954b3b38272e4.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: 4qhCgdF0iLF65rVad6mwEletP6vzj-bjOn3gNipA6HrUd9Bdzag1Ig==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

- **Follow TCP Stream for Second Request:** Similarly, the TCP stream for the second HTTP request to "<http://www.umd.edu/We-will-defeat-Darth-Vader>" was followed. This provided insights into the nature of the second HTTP request and the server's identical response.



```
Wireshark · Follow TCP Stream (tcp.stream eq 7) · Tanishq_Javvaji_119070185_final_form_capture.pcapng

GET /We-will-defeat-Darth-Vader. HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Mon, 04 Dec 2023 00:27:07 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/We-will-defeat-Darth-Vader.
X-Cache: Redirect from cloudfront
Via: 1.1 fc14e875a60ccec1a95a0b8b7d32822e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: 9t0oMb6sptLv6ox2XEDQSTAiKc2lJAXuHp00z389At-vCrr8BB4faA==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

- **HTTP Requests Examination:** The analysis of the HTTP requests showed that "final-form.exe" specifically targeted URLs on the "www.umd.edu" server, namely "<http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star>" and "<http://www.umd.edu/We-will-defeat-Darth-Vader>." This indicated a pattern in the executable's network communication, potentially revealing its objectives or operational tactics.

The screenshot shows a Wireshark packet capture of an HTTP request. The packet list on the left shows a GET request to `/We-have-the-blue-prints-to-the-Death-Star` from 10.125.26.175 to 3.163.101.24. The packet details pane on the right shows the request structure, including the request URI and version. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1651	2.020859	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
1668	2.039376	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
4759	4.970687	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
4789	5.002078	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
8452	8.675622	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
8494	8.708315	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
11374	11.499636	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
11386	11.518196	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
13778	15.052940	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
13795	15.071413	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
16064	17.609438	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
16087	17.633309	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
20414	21.332644	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
20435	21.351628	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
23127	24.027244	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
23135	24.050565	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)

Packet details for the selected packet (No. 1651):

- [SEQ/ACK analysis]
- TCP payload (155 bytes)
- Hypertext Transfer Protocol
 - GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n]
 - [GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /We-have-the-blue-prints-to-the-Death-Star
 - Request Version: HTTP/1.1
 - Accept-Encoding: identity\r\n
 - Host: www.umd.edu\r\n
 - Connection: close\r\n
 - User-Agent: Python-urllib/2.7\r\n
 - \r\n

HTTP Request-URI (http.request.uri), 42 bytes

The screenshot shows a Wireshark packet capture of an HTTP request. The packet list on the left shows a GET request to `/We-will-defeat-Darth-Vader.` from 10.125.26.175 to 3.163.101.24. The packet details pane on the right shows the request structure, including the request URI and version. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

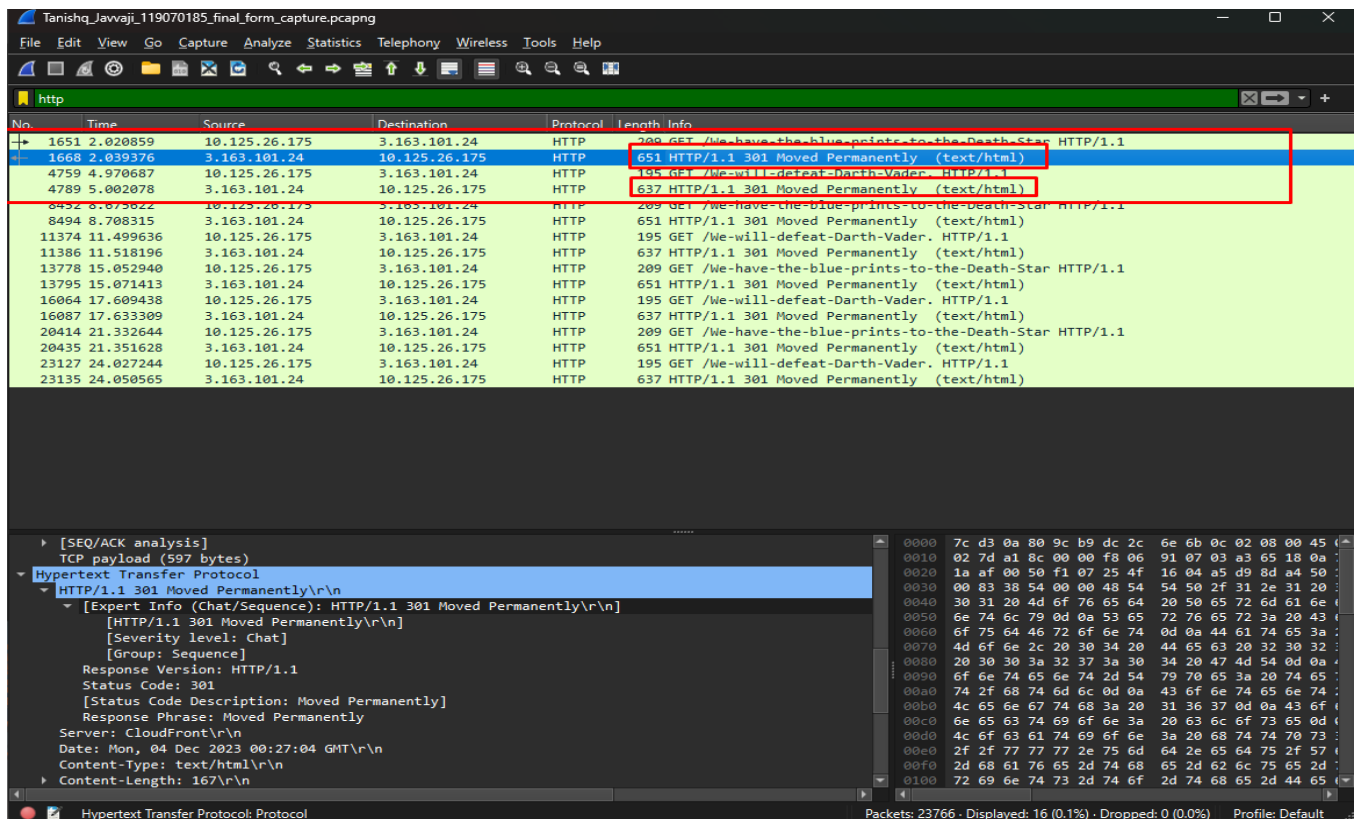
No.	Time	Source	Destination	Protocol	Length	Info
1651	2.020859	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
1668	2.039376	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
4759	4.970687	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
4789	5.002078	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
8452	8.675622	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
8494	8.708315	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
11374	11.499636	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
11386	11.518196	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
13778	15.052940	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
13795	15.071413	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
16064	17.609438	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
16087	17.633309	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
20414	21.332644	10.125.26.175	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
20435	21.351628	3.163.101.24	10.125.26.175	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
23127	24.027244	10.125.26.175	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
23135	24.050565	3.163.101.24	10.125.26.175	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)

Packet details for the selected packet (No. 4759):

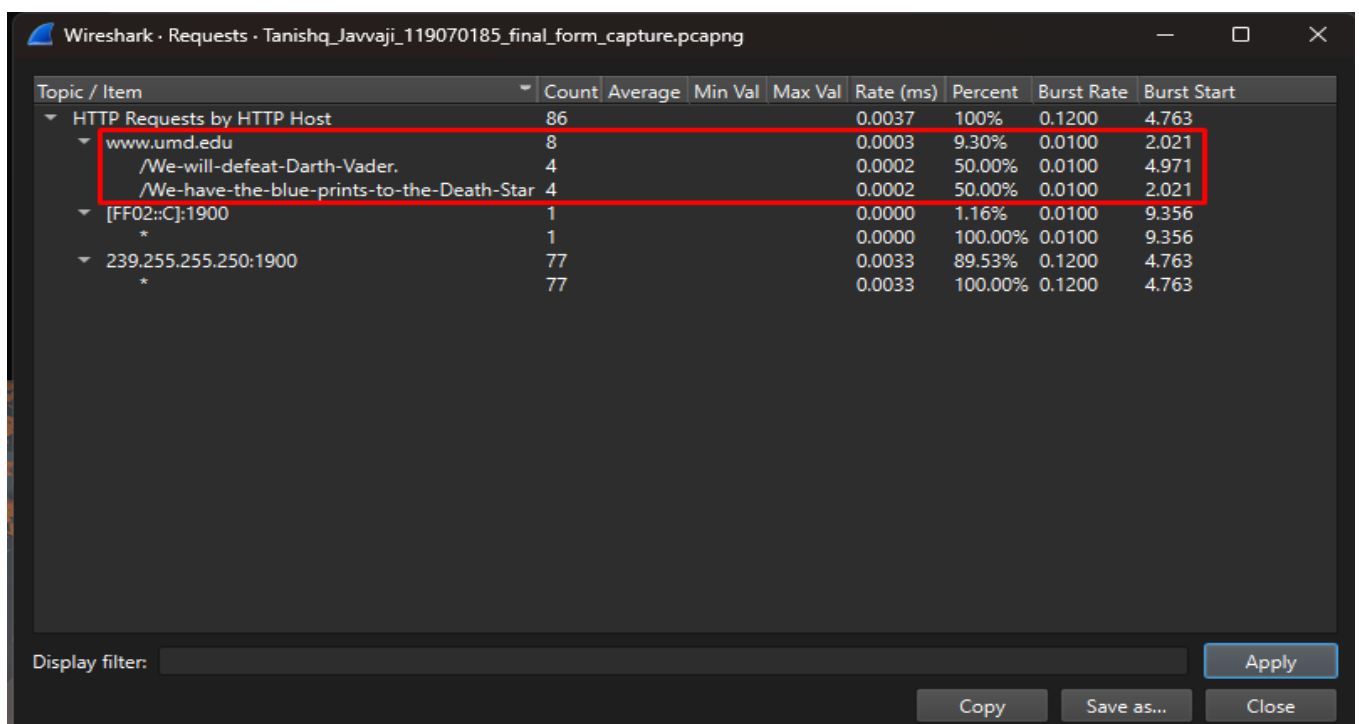
- [SEQ/ACK analysis]
- TCP payload (141 bytes)
- Hypertext Transfer Protocol
 - GET /We-will-defeat-Darth-Vader. HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /We-will-defeat-Darth-Vader. HTTP/1.1\r\n]
 - [GET /We-will-defeat-Darth-Vader. HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /We-will-defeat-Darth-Vader.
 - Request Version: HTTP/1.1
 - Accept-Encoding: identity\r\n
 - Host: www.umd.edu\r\n
 - Connection: close\r\n
 - User-Agent: Python-urllib/2.7\r\n
 - \r\n

HTTP Request-URI (http.request.uri), 28 bytes

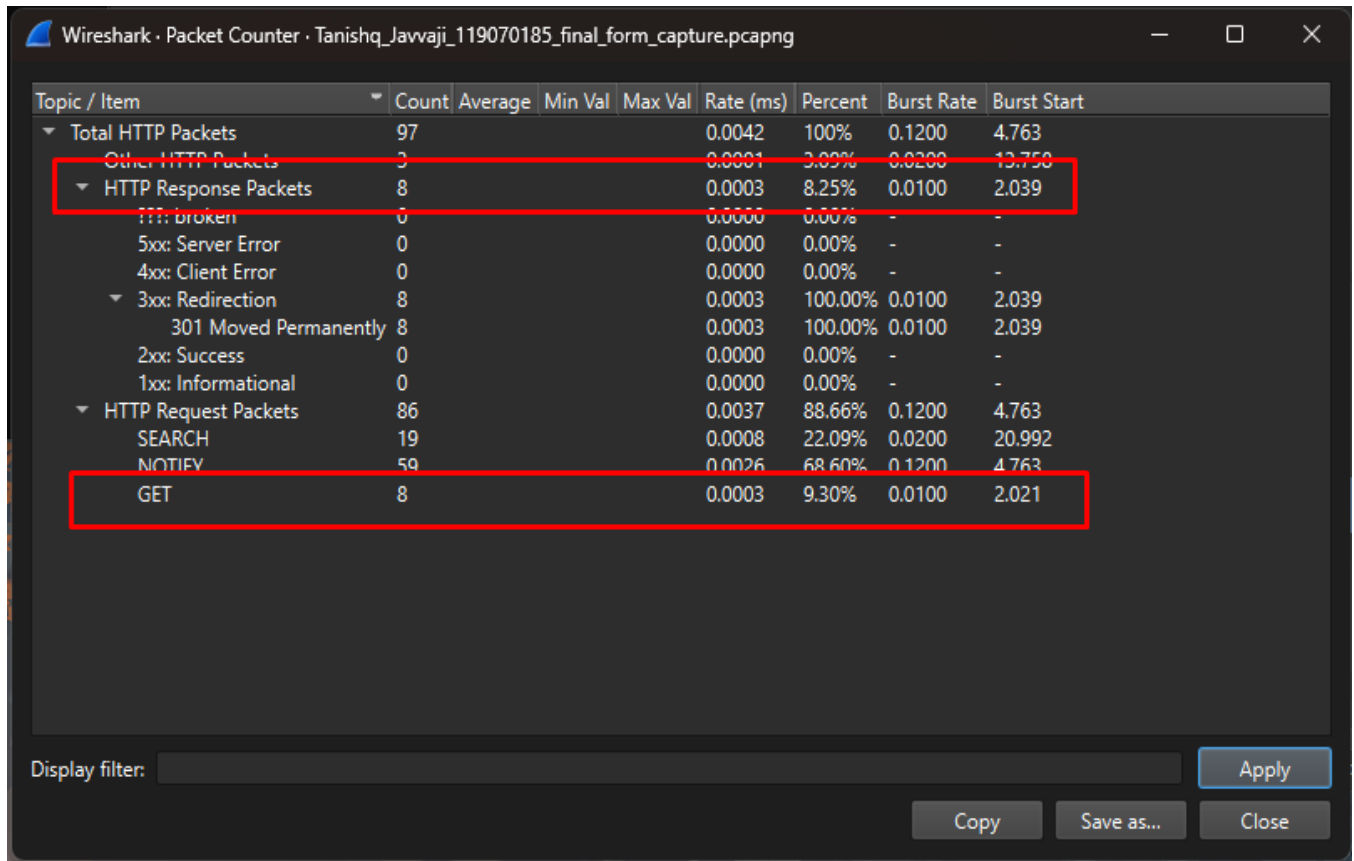
- **Server Responses:** The server responses to these requests consistently included a "301 Moved Permanently" status code, suggesting that the requested resources had been permanently relocated. This pattern is a common technique for redirection in web communications and might indicate an attempt to obfuscate the true nature of the communication or redirect to other resources.



- **Request Tab Findings:** Further examination in the Requests tab of Wireshark revealed a total of 8 requests made by "final-form.exe" to "www.umd.edu." This repetitive nature of communication suggested a programmed or automated behavior, possibly designed for specific communication sequences or triggering certain actions on the server.



- **Packet Counter Confirmation:** The Packet Counter tab in Wireshark corroborated these findings, recording 8 requests and 8 corresponding responses, all with the "301 Moved Permanently" status code. This consistency further supports the notion of an automated communication process.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Total HTTP Packets	97				0.0042	100%	0.1200	4.763
Other HTTP Packets	3				0.0001	3.09%	0.0200	13.750
▼ HTTP Response Packets	8				0.0003	8.25%	0.0100	2.039
1xx: Informational	0				0.0000	0.00%	-	-
2xx: Success	0				0.0000	0.00%	-	-
3xx: Redirection	8				0.0003	100.00%	0.0100	2.039
301 Moved Permanently	8				0.0003	100.00%	0.0100	2.039
4xx: Client Error	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
??? : broken	0				0.0000	0.00%	-	-
▼ HTTP Request Packets	86				0.0037	88.66%	0.1200	4.763
NOTIFY	59				0.0026	68.60%	0.1200	4.763
SEARCH	19				0.0008	22.09%	0.0200	20.992
GET	8				0.0003	9.30%	0.0100	2.021

Display filter: Apply Copy Save as... Close

- **Export Attempts:** Attempts were made to export objects from these requests for further examination. However, this effort did not yield significant findings due to continuous redirection, which complicated the retrieval of more detailed information about the requests.

Recommendations and Next Steps

Based on the findings from the analyses of "obiwan.exe," "obiwan2.exe," "not-the-droids-you-are-looking-for.mp3," and "final-form.exe," the following recommendations and next steps are proposed to continue the investigation effectively:

1. Further Malware Analysis:

- Conduct an in-depth code analysis of both "obiwan.exe" and "obiwan2.exe" using advanced malware analysis tools (such as disassemblers and debuggers) to understand their full capabilities and uncover any hidden functionalities.
- Analyze "final-form.exe" in a similar manner to ascertain its role in the broader context and its potential impact.

2. Server Interaction Investigation:

- Investigate the "www.umd.edu" server to understand the nature of the resources that the executables were trying to access. Determine if these resources are part of a controlled environment or a legitimate external server.
- If possible, collaborate with the server administrators or relevant authorities to gather logs and additional information about the requests coming from the executables.

3. Network Traffic Analysis:

- Further analyze the network traffic to trace the origin of the TCP connections established by the executables. This may provide insights into potential command and control (C&C) servers.
- Investigate any other network activities initiated by the executables that were not captured in the initial analysis.

4. Decrypted Content Scrutiny:

- Perform a detailed examination of the contents found in the "Death Star Plans" folder and the "ENPM687-Read-This.txt" file for any hidden messages or clues.
- Conduct a security analysis of "final-form.exe" to determine its purpose, especially in relation to the text file's instructions.

5. Security Measures:

- Strengthen network security to prevent similar malware infections in the future. This includes updating firewalls, intrusion detection systems, and implementing advanced threat protection solutions.
- Educate employees about the dangers of malware and the importance of following security best practices.

Challenges Faced

Throughout the course of this forensic investigation, several challenges were encountered that posed hurdles to the analysis process. These challenges, though demanding, were ultimately instrumental in refining the investigative techniques and enhancing the overall understanding of the case. Three notable challenges include:

1. Cryptographic Complexity

The presence of robust encryption in the "not-the-droids-you-are-looking-for.mp3" file added an intricate layer to the investigation. The identification of the decryption key, "r2d2," through the analysis of "obiwan2.exe" was a breakthrough; however, validating the key's accuracy and successfully decrypting the file proved to be a complex task. Decrypting files in a forensic context can be time-consuming and contingent on obtaining the precise decryption key. This challenge underscores the importance of cryptographic analysis in modern digital forensics.

2. Continuous Server Redirection

The executables, particularly "obiwan.exe" and "final-form.exe," displayed a persistent pattern of server redirection when communicating with "www.umd.edu." This behavior posed a substantial challenge as it impeded the capture and analysis of specific content from the server. Dealing with continuous redirection in network analysis can be cumbersome and may obscure critical information. Mitigating this challenge required innovative approaches to ensure a comprehensive understanding of the communication.

3. Overcoming Data Volume and Complexity

The vast volume of digital data involved in this investigation, including disk images, network captures, and executable files, presented a formidable challenge. Managing, processing, and correlating this extensive dataset required meticulous organization and a considerable amount of time. Additionally, different data sources often had varying levels of complexity, making the task of ensuring data integrity and relevance a substantial challenge.