Digital Forensics Report

Sumanth Vankineni

119351130

Table of Contents

1.Brief Summary of Information

This report presents the findings from the forensic analysis of a hard drive labeled 'ENPM687 Final XP,' which was confiscated from a suspect alleged to be involved in malware creation. The primary tool used for the analysis was Autopsy.

During the investigation, the initial assessment of the hard drive using Autopsy's Data Sources summary indicated its size to be 21 GB with a variety of file types. The hard drive's geolocation was identified as the United Kingdom. A detailed exploration of the 'Recent Files' tab revealed frequent access to the 'My Documents' folder, especially to a subfolder named 'code,' which contained Python-related files and executables. These executables, when executed, showed no immediate output but were found to be making server requests and establishing TCP connections to a remote system. Network traffic captured with Wireshark indicated that these executables were sending encrypted messages, with references to 'Obiwan Kenobi' and phrases like 'you're my only hope.'

Further analysis led to the discovery of significant items in the 'Downloads' folder, including ProcessExplorer, a Python installer, and a VeraCrypt folder. The 'My Music' folder also contained an unusual music file that appeared to be a part of the puzzle, linking back to the Star Wars theme found in other parts of the analysis. Using the key 'r2d2,' deciphered from the encrypted messages, the contents of the mp3 file were decrypted using VeraCrypt, revealing a folder named 'Death Star Plans' and an executable 'final-form.exe,' which transmitted messages suggesting possession of critical information.

This summary encapsulates the key findings from the hard drive analysis, indicating the presence of encrypted communications, potentially malicious software, and references to coded messages and plans. A full analysis is underway to uncover the complete extent and intent of the data found.

2.Tools Used in the Investigation Process

During the forensic investigation of the 'ENPM687 Final XP' hard drive, a variety of specialized tools were utilized, each contributing uniquely to the analysis process. The primary tools employed included Autopsy, Wireshark, and Veracrypt. Here is an overview of each tool, outlining its specific role in the investigation and the assumptions underpinning its usage:

1. Autopsy:

Purpose: Autopsy serves as a digital forensics platform, providing a graphical interface for The Sleuth Kit and other forensic tools. In this case, Autopsy was instrumental in the initial examination of the hard disk image. It was particularly useful for identifying and flagging suspicious files, including the encrypted MP3 file and executable files named 'obiwan.exe' and 'obiwan2.exe'.

Assumptions: The investigation relies on the presumption that Autopsy performs a comprehensive and accurate analysis of the disk image. Key to this reliance is the tool's capability to detect anomalies, potential malware, and encrypted files, forming the foundation for subsequent investigative steps.

2. Wireshark:

Purpose: Wireshark is a network protocol analyzer designed for capturing and inspecting the traffic on computer networks. It was deployed to monitor and analyze the network traffic generated by the executables 'obiwan.exe', 'obiwan2.exe', and 'final-form.exe'. Wireshark aided in identifying the nature of the remote connections these executables established, including the scrutiny of HTTP requests and responses.

Assumptions: The analysis assumes that Wireshark is capable of capturing all pertinent network traffic comprehensively. The accuracy of the findings is contingent on Wireshark's effectiveness in capturing and decoding network packets, which is vital for understanding the network behaviors of the executables.

3. Veracrypt:

Purpose: Veracrypt, an open-source disk encryption software, was employed for encrypting and decrypting files. In this investigation, it decrypted the 'not-the-droids-you-are-looking-for.mp3' file using the key "r2d2," uncovered earlier in the analysis. This decryption was a pivotal component of the investigation, revealing significant data concealed within the encrypted file.

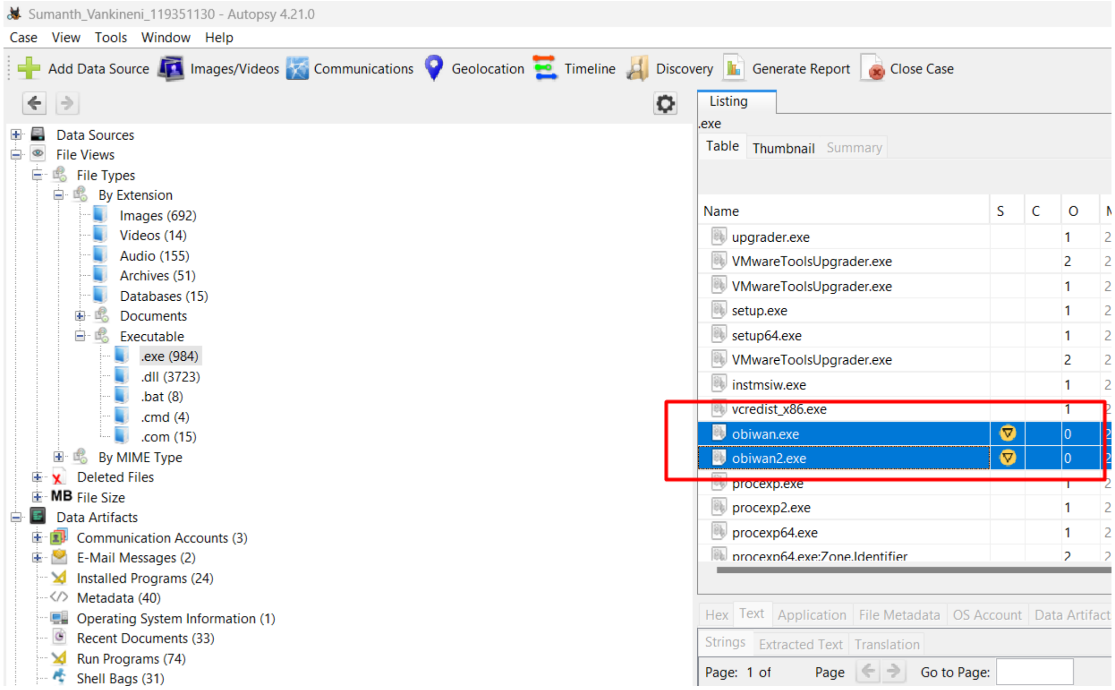
Assumptions: The tool's effectiveness hinges on the assumption that the encryption on the MP3 file is within Veracrypt's decryption capabilities. There is also an underlying assumption that the "r2d2" key is correct and that the file's encryption wasn't multi-layered beyond what Veracrypt can decrypt.

3.Repository #1 Analysis

a.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

The first phase in the comprehensive analysis of the executable files "obiwan.exe" and "obiwan2.exe" involved their extraction from the hard disk image. This step was crucial in obtaining a replicable copy of each executable for thorough examination while upholding the integrity of the original disk image.

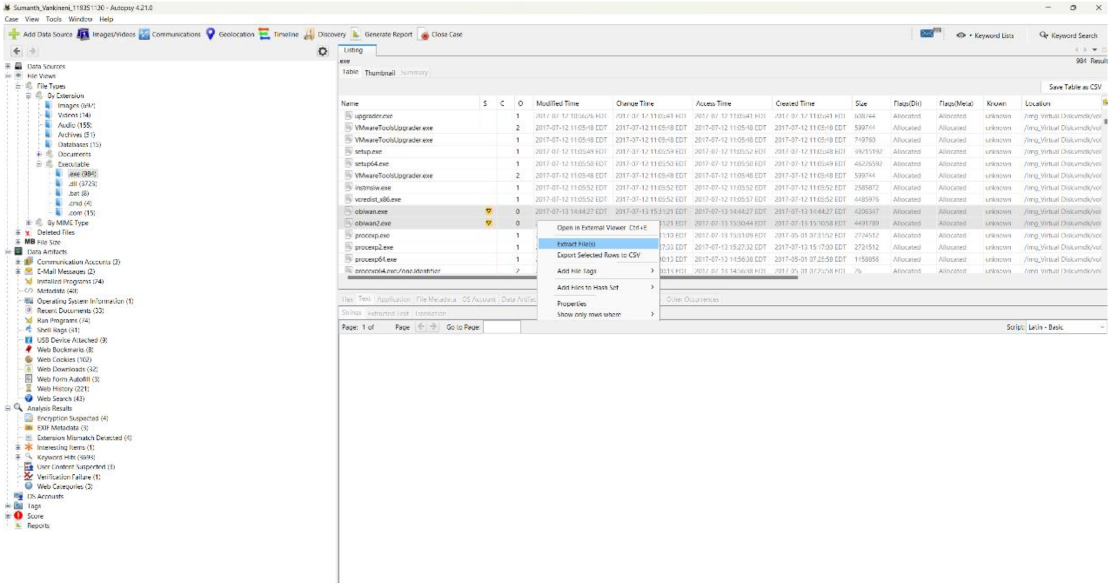


Name	S	C	O	M
upgrader.exe			1	2
VMwareToolsUpgrader.exe			2	2
VMwareToolsUpgrader.exe			1	2
setup.exe			1	2
setup64.exe			1	2
VMwareToolsUpgrader.exe			2	2
instmsiw.exe			1	2
vcredist_x86.exe			1	2
obiwan.exe	▽		0	2
obiwan2.exe	▽		0	2
procexp.exe			1	2
procexp2.exe			1	2
procexp64.exe			1	2
procexp64.exe:Zone.Identifier			2	2

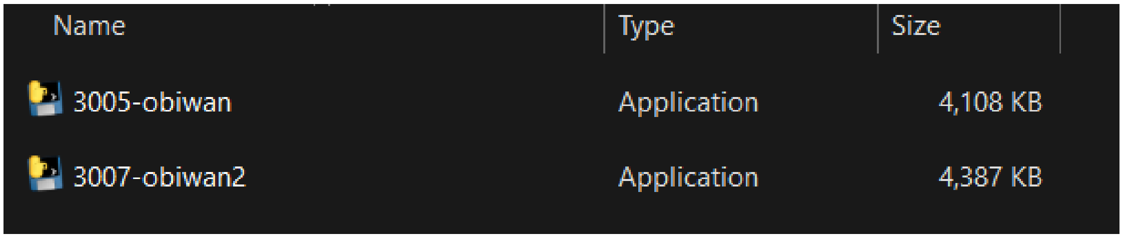
Extraction Process:

Using Autopsy: The executables "obiwan.exe" and "obiwan2.exe" were located within the hard disk image through the Autopsy forensic suite. Autopsy is recognized for its extensive capabilities in digital investigations, particularly in file identification and extraction.

Default Extract Option: For the extraction process, Autopsy's default extraction option was employed. This option is specifically designed to ensure a direct and secure method of file extraction, which is paramount in preserving the forensic validity of the evidence.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
upgrader.exe			1	2017-07-12 10:56:26 EDT	2017-07-12 11:05:41 EDT	2017-07-12 11:05:41 EDT	2017-07-12 11:05:41 EDT	608744	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
VMwareToolsUpgrader.exe			2	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	599744	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
VMwareToolsUpgrader.exe			1	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	749760	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
setup.exe			1	2017-07-12 11:05:49 EDT	2017-07-12 11:05:59 EDT	2017-07-12 11:05:52 EDT	2017-07-12 11:05:48 EDT	39215192	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
setup64.exe			1	2017-07-12 11:05:50 EDT	2017-07-12 11:05:50 EDT	2017-07-12 11:05:50 EDT	2017-07-12 11:05:49 EDT	46226592	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
VMwareToolsUpgrader.exe			2	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	2017-07-12 11:05:48 EDT	599744	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
instmsiw.exe			1	2017-07-12 11:05:52 EDT	2017-07-12 11:05:52 EDT	2017-07-12 11:05:52 EDT	2017-07-12 11:05:52 EDT	2585872	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
vcredist_x86.exe			1	2017-07-12 11:05:52 EDT	2017-07-12 11:05:52 EDT	2017-07-12 11:05:57 EDT	2017-07-12 11:05:52 EDT	4485976	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
obiwan.exe	▽		0	2017-07-13 14:44:27 EDT	2017-07-13 15:31:21 EDT	2017-07-13 14:44:27 EDT	2017-07-13 14:44:27 EDT	4206347	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
obiwan2.exe	▽		0		1:21 EDT	2017-07-13 15:30:44 EDT	2017-07-13 15:10:58 EDT	4491789	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
procexp.exe			1		1:10 EDT	2017-07-13 15:31:09 EDT	2017-05-01 07:31:52 EDT	2724512	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
procexp2.exe			1		7:33 EDT	2017-07-13 15:27:32 EDT	2017-07-13 15:17:00 EDT	2724512	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
procexp64.exe			1		0:13 EDT	2017-07-13 14:56:38 EDT	2017-05-01 07:25:59 EDT	1458856	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol
procexp64.exe:Zone.Identifier			2		0:13 EDT	2017-07-13 14:56:38 EDT	2017-05-01 07:25:58 EDT	26	Allocated	Allocated	unknown	/img_Virtual Disk.vmdk/vol



Name	Type	Size
3005-obiwan	Application	4,108 KB
3007-obiwan2	Application	4,387 KB

i. Analysis of "obiwan.exe"

Detailed Examination of "obiwan.exe" Execution and Network Activity

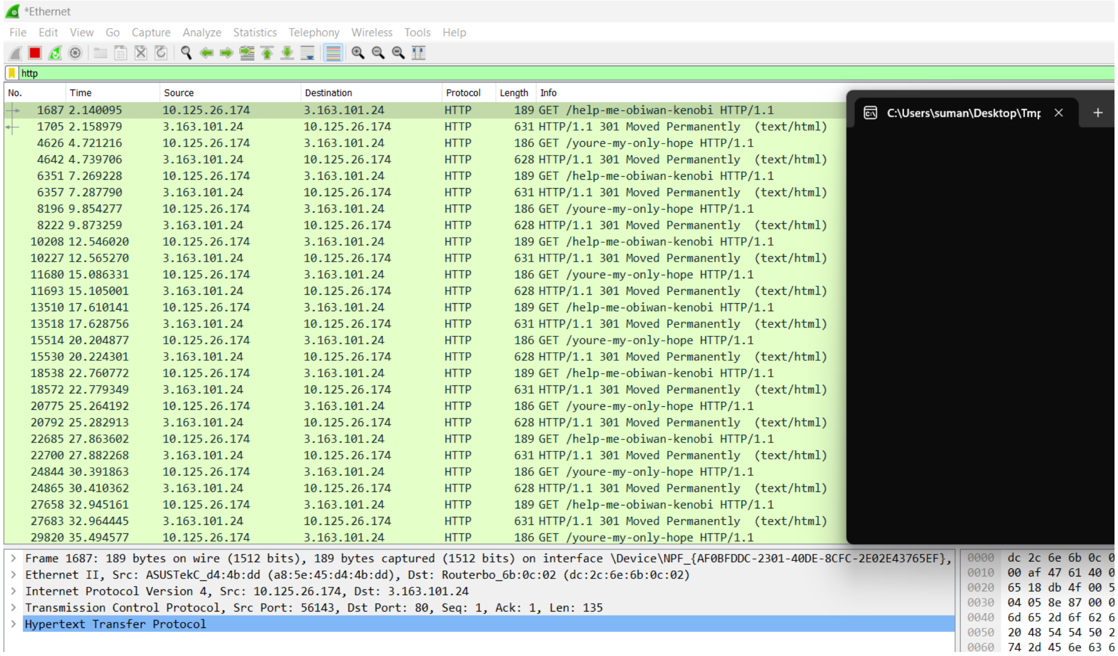
The analysis of "obiwan.exe" encompassed an in-depth review of both its execution behavior and network interactions. This process was bifurcated into two key stages: closely monitoring the execution and behavior of the executable and conducting comprehensive Wireshark analysis to decipher its network interactions.

Execution and Behavior:

Execution Monitoring: "obiwan.exe" was executed within a controlled environment, with vigilant monitoring of its activities. This approach was critical to observing the executable's real-time behavior and system interactions.

Process Explorer Analysis: Utilizing Process Explorer, the running status of "obiwan.exe" was meticulously tracked. This tool revealed that the executable was initiating requests to a remote server over the internet, providing insights into the nature of these requests and the executable's overall process behavior.

TCP Connections Observation: The TCP connections linked to "obiwan.exe" were examined in detail. By tracing the TCP stream, comprehensive information regarding the connections' characteristics and destinations was obtained, elucidating the network behavior of the executable.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
C:\Users\suman\Desktop\Tmp

http

No.	Time	Source	Destination	Protocol	Length	Info
1687	2.140095	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
1705	2.158979	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
4626	4.721216	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
4642	4.739706	3.163.101.24	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
6351	7.269228	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
6357	7.287790	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
8196	9.854277	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
8222	9.873259	3.163.101.24	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
10208	12.546020	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
10227	12.565270	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
11680	15.086331	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
11693	15.105001	3.163.101.24	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
13510	17.610141	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
13518	17.628756	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
15514	20.204877	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
15530	20.224301	3.163.101.24	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
18538	22.760772	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
18572	22.779349	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
20775	25.264192	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
20792	25.282913	3.163.101.24	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
22685	27.863602	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
22700	27.882268	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
24844	30.391863	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1
24865	30.410362	3.163.101.24	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
27658	32.945161	10.125.26.174	3.163.101.24	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
27683	32.964445	3.163.101.24	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
29820	35.494577	10.125.26.174	3.163.101.24	HTTP	186	GET /youre-my-only-hope HTTP/1.1

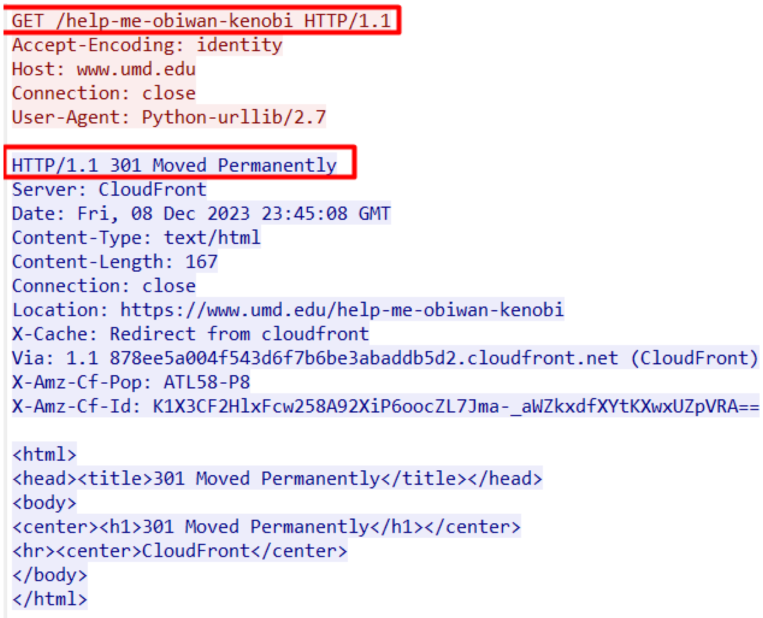
```
> Frame 1687: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF},
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 3.163.101.24
> Transmission Control Protocol, Src Port: 56143, Dst Port: 80, Seq: 1, Ack: 1, Len: 135
> Hypertext Transfer Protocol
```

```
0000  dc 2c 6e 6b 0c 0
0010  00 af 47 61 40 0
0020  65 18 db 4f 00 5
0030  04 05 8e 87 00 0
0040  6d 65 2d 6f 62 6
0050  20 48 54 54 50 2
0060  74 2d 45 6e 63 6
```

Wireshark Analysis:

Packet Capturing: Wireshark was leveraged to capture the network packets generated by "obiwan.exe," crucial for analyzing the data transmitted and received by the executable.

Follow TCP Stream: The TCP stream for the request to "www.umd.edu/help-me-obiwan-kenobi" was analyzed, revealing the full HTTP request and response cycle, including the server's "301 Moved Permanently" status code.

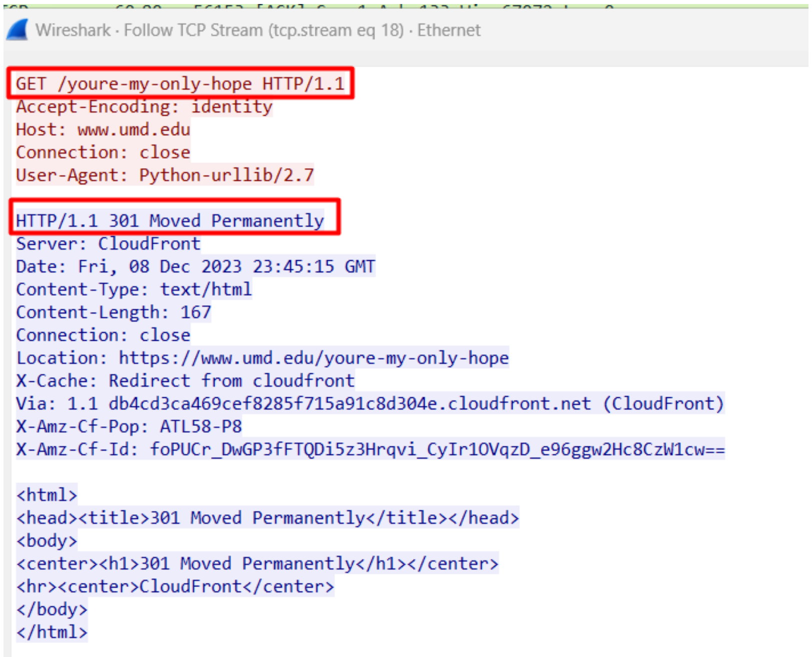


```
GET /help-me-obiwan-kenobi HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Fri, 08 Dec 2023 23:45:08 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 878ee5a004f543d6f7b6be3abaddb5d2.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: K1X3CF2HlxFcw258A92XiP6oocZL7Jma-_aWZkxdfXYtKXwxUZpVRA==

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

Second TCP Stream Analysis: A similar approach was adopted for the request to "www.umd.edu/youre-my-only-hope," providing insights into the nature of this second HTTP request and the server's corresponding response.



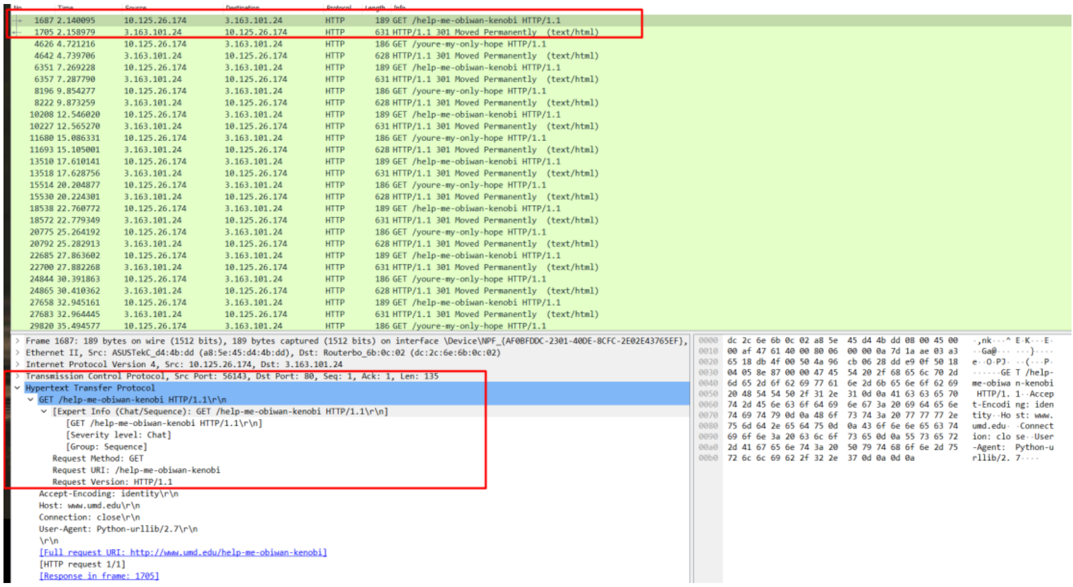
Wireshark · Follow TCP Stream (tcp.stream eq 18) · Ethernet

```
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: Fri, 08 Dec 2023 23:45:15 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 db4cd3ca469cef8285f715a91c8d304e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: foPUCr_DwGP3fFTQDi5z3Hrqvi_CyIr1OVqzD_e96ggw2Hc8CzW1cw==

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

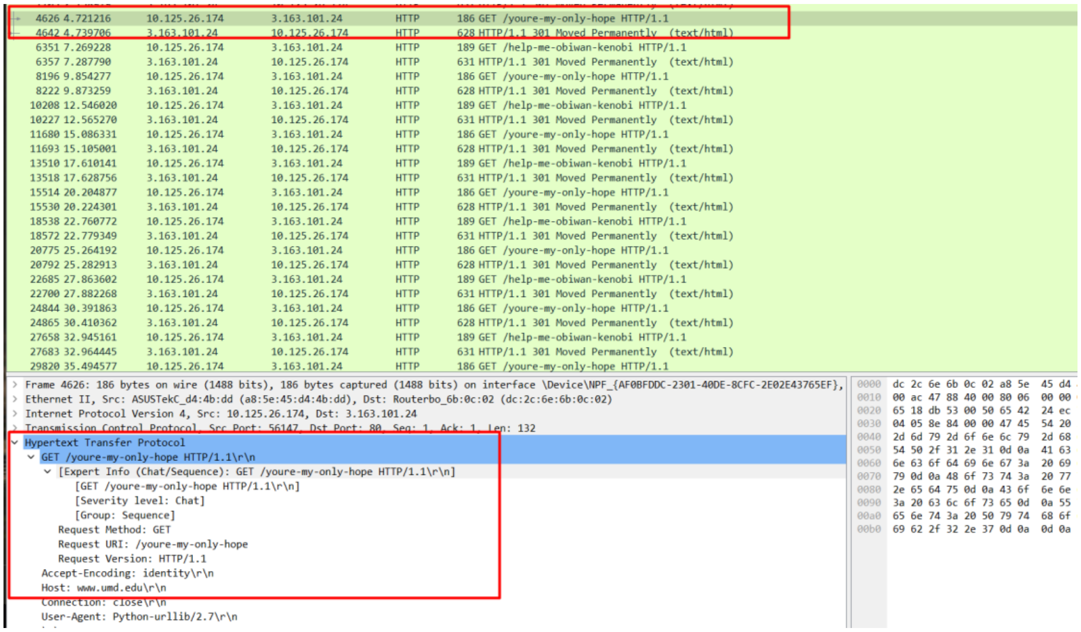
HTTP Requests Examination: The investigation revealed that "obiwan.exe" consistently made specific HTTP requests to URLs on the "www.umd.edu" server, particularly to "www.umd.edu/help-me-obiwan-kenobi" and "www.umd.edu/youre-my-only-hope," indicating a pattern in the executable's network communication.



```
No.   Time       Source         Destination    Protocol Length Info
 1687 2.140095   10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
 1705 2.158979   3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
 4626 4.721216   10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
 4642 4.739706   3.163.101.24   10.125.26.174  HTTP     628 HTTP/1.1 301 Moved Permanently  (text/html)
 6351 7.269228   10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
 6357 7.287790   3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
 8196 9.854277   10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
 8222 9.873259   3.163.101.24   10.125.26.174  HTTP     628 HTTP/1.1 301 Moved Permanently  (text/html)
10208 12.546020  10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
10227 12.565270  3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
11680 15.086331  10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
11693 15.105001  3.163.101.24   10.125.26.174  HTTP     628 HTTP/1.1 301 Moved Permanently  (text/html)
13510 17.610141  10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
13518 17.628756  3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
15514 20.204877  10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
15530 20.224301  3.163.101.24   10.125.26.174  HTTP     628 HTTP/1.1 301 Moved Permanently  (text/html)
18538 22.760772  10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
18572 22.779349  3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
20775 25.264192  10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
20792 25.282913  3.163.101.24   10.125.26.174  HTTP     628 HTTP/1.1 301 Moved Permanently  (text/html)
22685 27.863602  10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
22700 27.882268  3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
24844 30.391863  10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
24865 30.410362  3.163.101.24   10.125.26.174  HTTP     628 HTTP/1.1 301 Moved Permanently  (text/html)
27658 32.945161  10.125.26.174  3.163.101.24   HTTP     189 GET /help-me-obiwan-kenobi HTTP/1.1
27683 32.964445  3.163.101.24   10.125.26.174  HTTP     631 HTTP/1.1 301 Moved Permanently  (text/html)
29820 35.494577  10.125.26.174  3.163.101.24   HTTP     186 GET /youre-my-only-hope HTTP/1.1
```

```
> Frame 1687: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF},
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 3.163.101.24
> Transmission Control Protocol, Src Port: 56143, Dst Port: 80, Seq: 1, Ack: 1, Len: 135
v Hypertext Transfer Protocol
  v GET /help-me-obiwan-kenobi HTTP/1.1\r\n
    v [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
    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/help-me-obiwan-kenobi]
    [HTTP request 1/1]
    [Response in frame: 1705]
```

```
0000  dc 2c 6e 6b 0c 02 a8 5e  45 d4 4b dd 08 00 45 00   ·,nk···^ E·K···E·
0010  00 af 47 61 40 00 80 06  00 00 0a 7d 1a ae 03 a3   ··Ga@··· ···}····
0020  65 18 db 4f 00 50 4a 96  cb 06 28 dd e9 0f 50 18   e··O·PJ· ··(···P·
0030  04 05 8e 87 00 00 47 45  54 20 2f 68 65 6c 70 2d   ······GE T /help-
0040  6d 65 2d 6f 62 69 77 61  6e 2d 6b 65 6e 6f 62 69   me-obiwa n-kenobi
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 41 63 63 65 70    HTTP/1. 1··Accep
0060  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 69 64 65 6e   t-Encodi ng: iden
0070  74 69 74 79 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   tity··Ho st: www.
0080  75 6d 64 2e 65 64 75 0d  0a 43 6f 6e 6e 65 63 74   umd.edu· ·Connect
0090  69 6f 6e 3a 20 63 6c 6f  73 65 0d 0a 55 73 65 72   ion: clo se··User
00a0  2d 41 67 65 6e 74 3a 20  50 79 74 68 6f 6e 2d 75   -Agent:  Python-u
00b0  72 6c 6c 69 62 2f 32 2e  37 0d 0a 0d 0a            rllib/2. 7····
```

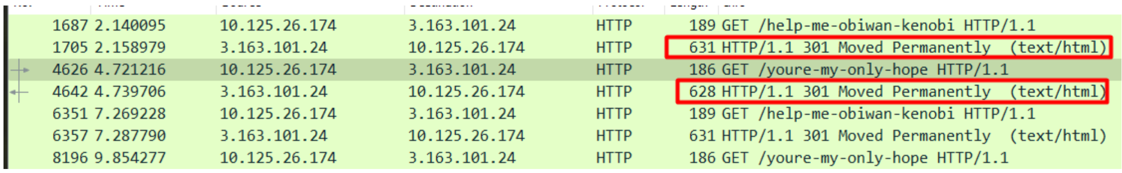


```
 4626 4.721216    10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
 4642 4.739706    3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
 6351 7.269228    10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
 6357 7.287790    3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
 8196 9.854277    10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
 8222 9.873259    3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
10208 12.546020   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
10227 12.565270   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
11680 15.086331   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
11693 15.105001   3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
13510 17.610141   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
13518 17.628756   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
15514 20.204877   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
15530 20.224301   3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
18538 22.760772   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
18572 22.779349   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
20775 25.264192   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
20792 25.282913   3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
22685 27.863602   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
22700 27.882268   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
24844 30.391863   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
24865 30.410362   3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
27658 32.945161   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
27683 32.964445   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
29820 35.494577   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
```

```
> Frame 4626: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF},
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 3.163.101.24
> Transmission Control Protocol, Src Port: 56147, Dst Port: 80, Seq: 1, Ack: 1, Len: 132
v Hypertext Transfer Protocol
  v GET /youre-my-only-hope HTTP/1.1\r\n
    v [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
    Accept-Encoding: identity\r\n
    Host: www.umd.edu\r\n
    Connection: close\r\n
    User-Agent: Python-urllib/2.7\r\n
```

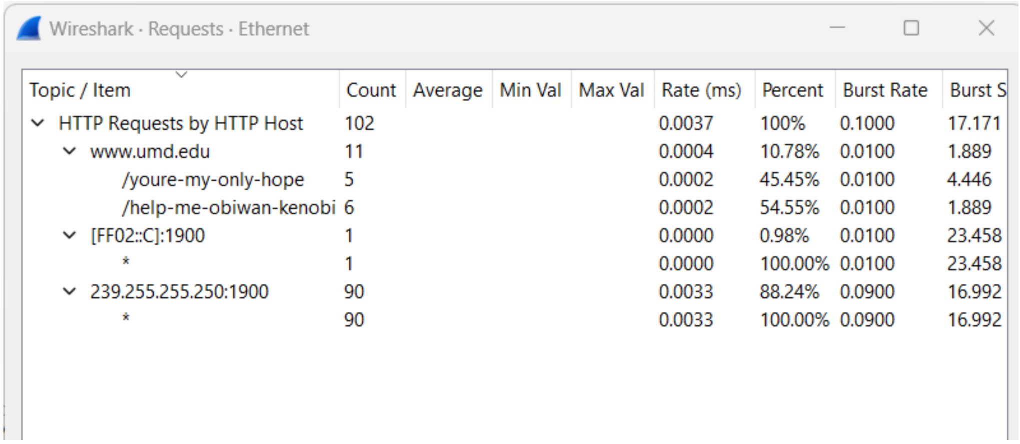
```
0000  dc 2c 6e 6b 0c 02 a8 5e  45 d4
0010  00 ac 47 88 40 00 80 06  00 00
0020  65 18 db 53 00 50 65 42  24 ec
0030  04 05 8e 84 00 00 47 45  54 20
0040  2d 6d 79 2d 6f 6e 6c 79  2d 68
0050  54 50 2f 31 2e 31 0d 0a  41 63
0060  6e 63 6f 64 69 6e 67 3a  20 69
0070  79 0d 0a 48 6f 73 74 3a  20 77
0080  2e 65 64 75 0d 0a 43 6f  6e 6e
0090  3a 20 63 6c 6f 73 65 0d  0a 55
00a0  65 6e 74 3a 20 50 79 74  68 6f
00b0  69 62 2f 32 2e 37 0d 0a  0d 0a
```

Server Responses: The responses from the server consistently included a "301 Moved Permanently" status code, suggesting a redirection technique commonly used in web communication.



```
1687 2.140095   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
1705 2.158979   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
4626 4.721216   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
4642 4.739706   3.163.101.24    10.125.26.174   HTTP   628 HTTP/1.1 301 Moved Permanently  (text/html)
6351 7.269228   10.125.26.174   3.163.101.24    HTTP   189 GET /help-me-obiwan-kenobi HTTP/1.1
6357 7.287790   3.163.101.24    10.125.26.174   HTTP   631 HTTP/1.1 301 Moved Permanently  (text/html)
8196 9.854277   10.125.26.174   3.163.101.24    HTTP   186 GET /youre-my-only-hope HTTP/1.1
```

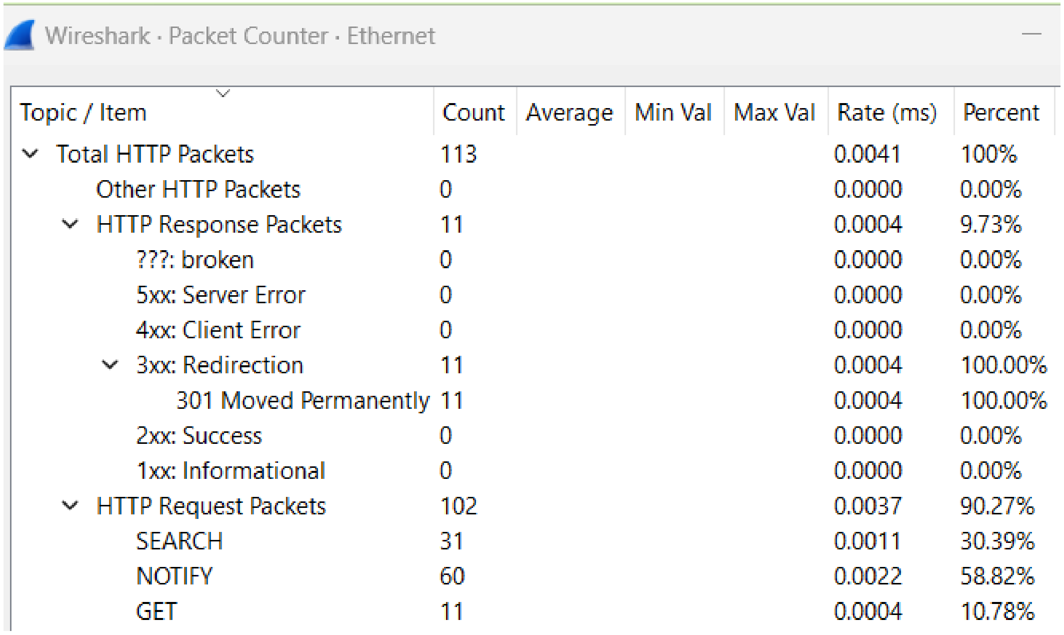
Request Tab Findings: Further scrutiny in the Requests tab indicated a total of 11 requests directed to "www.umd.edu," pointing to a potentially programmed or automated behavior in "obiwan.exe."



Wireshark · Requests · Ethernet

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst S
HTTP Requests by HTTP Host	102				0.0037	100%	0.1000	17.171
www.umd.edu	11				0.0004	10.78%	0.0100	1.889
/youre-my-only-hope	5				0.0002	45.45%	0.0100	4.446
/help-me-obiwan-kenobi	6				0.0002	54.55%	0.0100	1.889
[FF02::C]:1900	1				0.0000	0.98%	0.0100	23.458
*	1				0.0000	100.00%	0.0100	23.458
239.255.255.250:1900	90				0.0033	88.24%	0.0900	16.992
*	90				0.0033	100.00%	0.0900	16.992

Packet Counter Confirmation: The Packet Counter tab in Wireshark corroborated these observations, recording 11 requests and 11 corresponding responses, all marked with the "301 Moved Permanently" status code.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent
Total HTTP Packets	113				0.0041	100%
Other HTTP Packets	0				0.0000	0.00%
HTTP Response Packets	11				0.0004	9.73%
???: broken	0				0.0000	0.00%
5xx: Server Error	0				0.0000	0.00%
4xx: Client Error	0				0.0000	0.00%
3xx: Redirection	11				0.0004	100.00%
301 Moved Permanently	11				0.0004	100.00%
2xx: Success	0				0.0000	0.00%
1xx: Informational	0				0.0000	0.00%
HTTP Request Packets	102				0.0037	90.27%
SEARCH	31				0.0011	30.39%
NOTIFY	60				0.0022	58.82%
GET	11				0.0004	10.78%

Export Attempts: Efforts to export objects from these requests were made for additional examination. However, continuous redirection of the web pages presented challenges in obtaining more detailed information.

ii.Analysis of "obiwan2.exe"

Detailed Examination of "obiwan2.exe" Execution and Network Activity

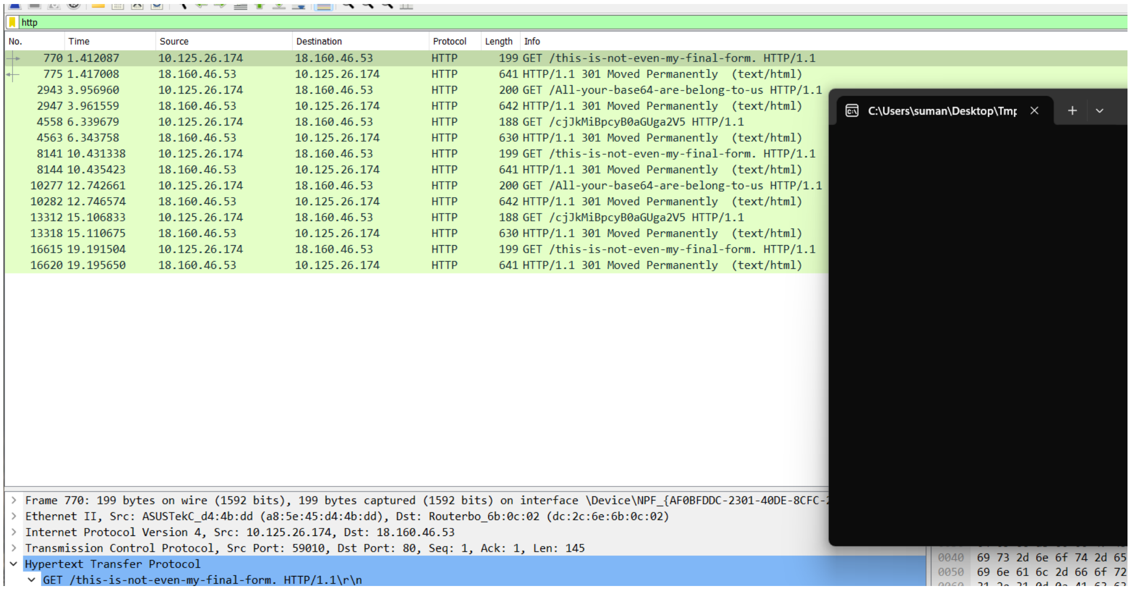
This section covers the analysis of the executable file "obiwan2.exe," focusing on its execution behavior and network interactions, conducted through a similar approach as with "obiwan.exe."

Execution and Behavior:

Execution Monitoring: "obiwan2.exe" was executed within a secure environment, allowing for close observation of its activities and behavior.

Process Explorer Analysis: Process Explorer provided valuable insights into the running status and system interactions of "obiwan2.exe," particularly focusing on its network requests.

TCP Connections Observation: The TCP connections associated with "obiwan2.exe" were carefully monitored to assess the nature and destinations of these connections.



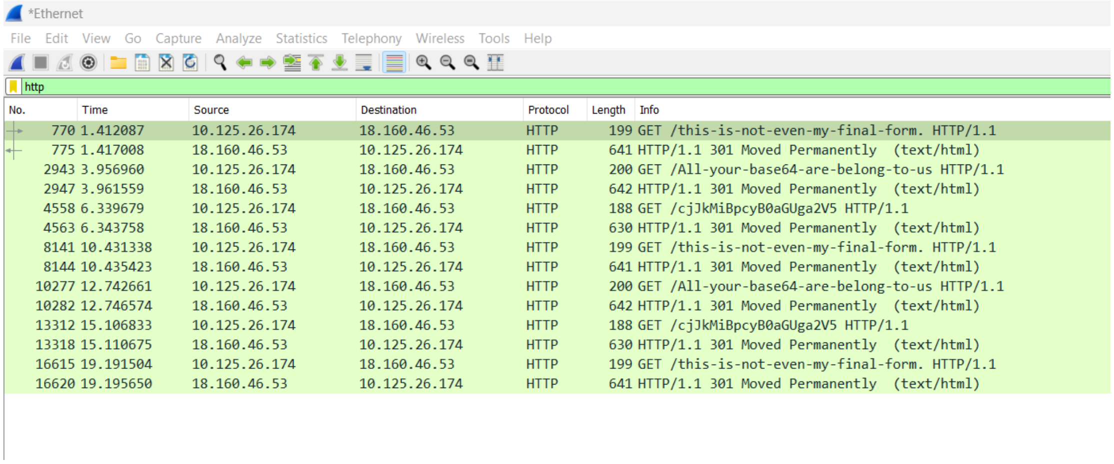
```
No.    Time          Source          Destination     Protocol  Length  Info
  770  1.412087      10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
  775  1.417008      18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
 2943  3.956960      10.125.26.174   18.160.46.53    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 2947  3.961559      18.160.46.53    10.125.26.174   HTTP      642 HTTP/1.1 301 Moved Permanently  (text/html)
 4558  6.339679      10.125.26.174   18.160.46.53    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 4563  6.343758      18.160.46.53    10.125.26.174   HTTP      630 HTTP/1.1 301 Moved Permanently  (text/html)
 8141  10.431338     10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 8144  10.435423     18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
10277  12.742661     10.125.26.174   18.160.46.53    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
10282  12.746574     18.160.46.53    10.125.26.174   HTTP      642 HTTP/1.1 301 Moved Permanently  (text/html)
13312  15.106833     10.125.26.174   18.160.46.53    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
13318  15.110675     18.160.46.53    10.125.26.174   HTTP      630 HTTP/1.1 301 Moved Permanently  (text/html)
16615  19.191504     10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
16620  19.195650     18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)

> Frame 770: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 18.160.46.53
> Transmission Control Protocol, Src Port: 59010, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
v Hypertext Transfer Protocol
  v GET /this-is-not-even-my-final-form. HTTP/1.1\r\n

0040  69 73 2d 6e 6f 74 2d 65
0050  69 6e 61 6c 2d 66 6f 72
```

Wireshark Analysis:

Packet Capturing: Network packets from "obiwan2.exe" were captured using Wireshark.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

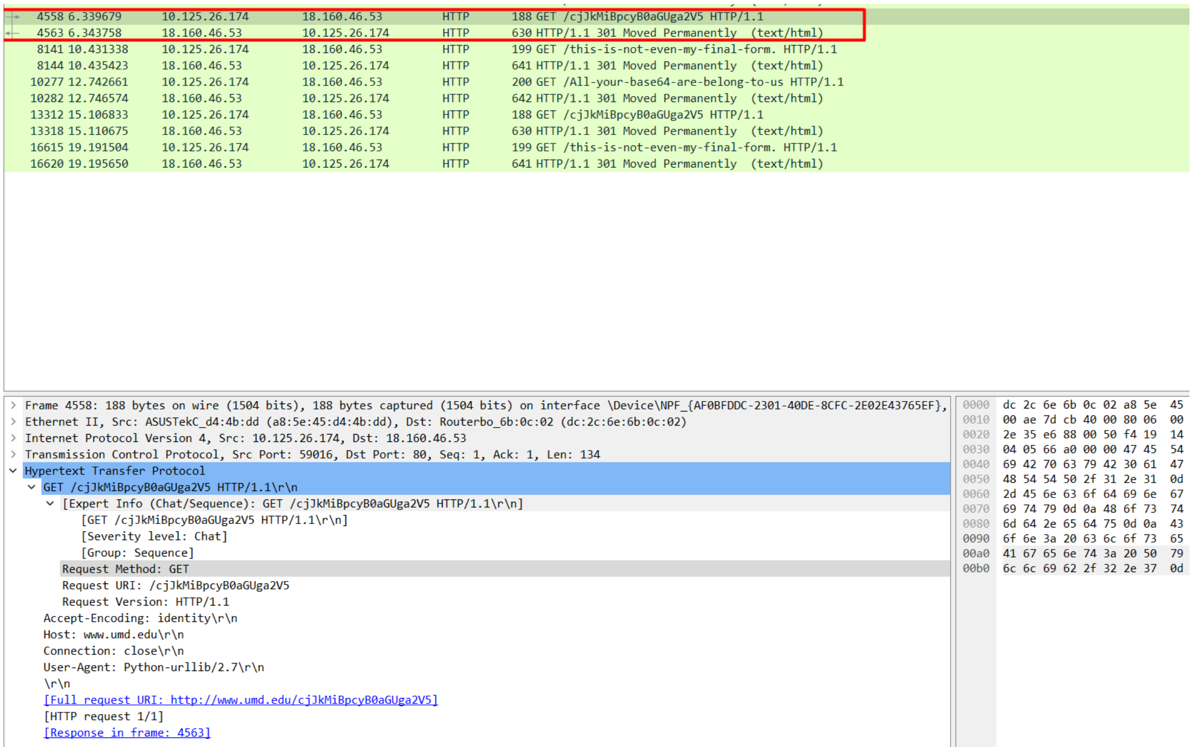
```
No.    Time          Source          Destination     Protocol  Length  Info
  770  1.412087      10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
  775  1.417008      18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
 2943  3.956960      10.125.26.174   18.160.46.53    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 2947  3.961559      18.160.46.53    10.125.26.174   HTTP      642 HTTP/1.1 301 Moved Permanently  (text/html)
 4558  6.339679      10.125.26.174   18.160.46.53    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 4563  6.343758      18.160.46.53    10.125.26.174   HTTP      630 HTTP/1.1 301 Moved Permanently  (text/html)
 8141  10.431338     10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 8144  10.435423     18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
10277  12.742661     10.125.26.174   18.160.46.53    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
10282  12.746574     18.160.46.53    10.125.26.174   HTTP      642 HTTP/1.1 301 Moved Permanently  (text/html)
13312  15.106833     10.125.26.174   18.160.46.53    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
13318  15.110675     18.160.46.53    10.125.26.174   HTTP      630 HTTP/1.1 301 Moved Permanently  (text/html)
16615  19.191504     10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
16620  19.195650     18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
```

HTTP Requests Examination: Wireshark analysis of "obiwan2.exe" revealed three distinct HTTP requests made to the www.umd.edu server. These included:

A request to "http://www.umd.edu/All-your-base64-are-belong-to-us," suggesting a coded message.

A base64 encoded string in the request to "http://www.umd.edu/cjJkMiBpcyB0aGUga2V5," translating to "r2d2 is the key," hinting at the use of an encryption key or passphrase.

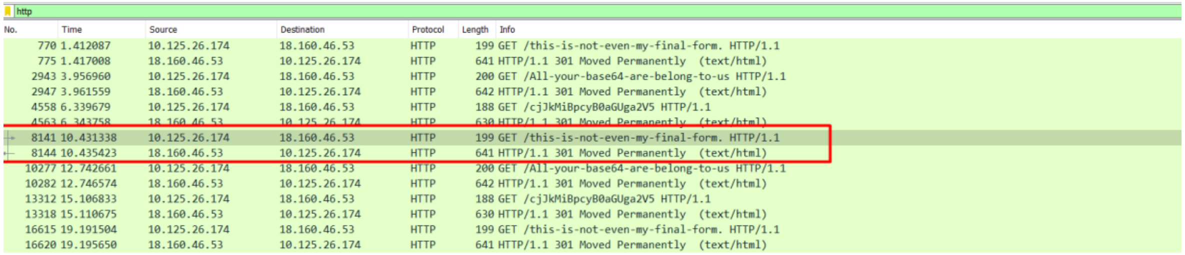
A request to "http://www.umd.edu/this-is-not-even-my-final-form," indicating the possibility of "obiwan2.exe" being part of a more extensive malware operation.



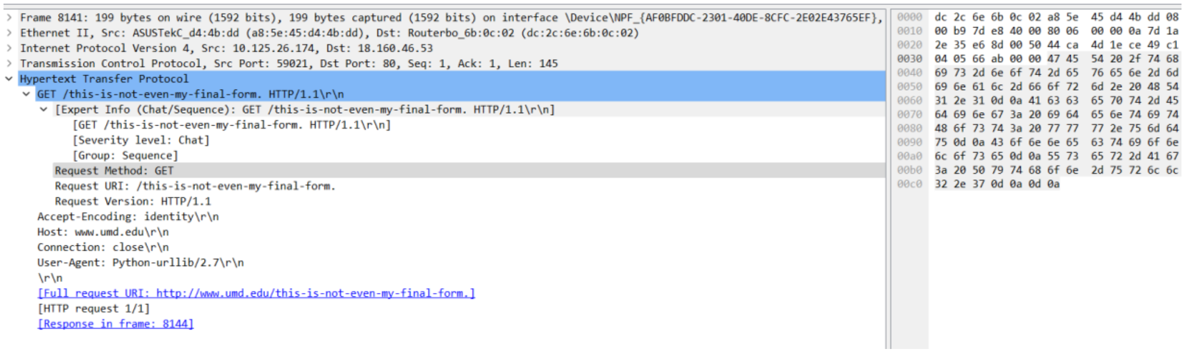
```
  4558 6.339679   10.125.26.174   18.160.46.53    HTTP   188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
  4563 6.343758   18.160.46.53    10.125.26.174   HTTP   630 HTTP/1.1 301 Moved Permanently  (text/html)
  8141 10.431338  10.125.26.174   18.160.46.53    HTTP   199 GET /this-is-not-even-my-final-form. HTTP/1.1
  8144 10.435423  18.160.46.53    10.125.26.174   HTTP   641 HTTP/1.1 301 Moved Permanently  (text/html)
 10277 12.742661  10.125.26.174   18.160.46.53    HTTP   200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 10282 12.746574  18.160.46.53    10.125.26.174   HTTP   642 HTTP/1.1 301 Moved Permanently  (text/html)
 13312 15.106833  10.125.26.174   18.160.46.53    HTTP   188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 13318 15.110675  18.160.46.53    10.125.26.174   HTTP   630 HTTP/1.1 301 Moved Permanently  (text/html)
 16615 19.191504  10.125.26.174   18.160.46.53    HTTP   199 GET /this-is-not-even-my-final-form. HTTP/1.1
 16620 19.195650  18.160.46.53    10.125.26.174   HTTP   641 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
> Frame 4558: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF},
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 18.160.46.53
> Transmission Control Protocol, Src Port: 59016, Dst Port: 80, Seq: 1, Ack: 1, Len: 134
v Hypertext Transfer Protocol
  v GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1\r\n]
        [GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /cjJkMiBpcyB0aGUga2V5
      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/cjJkMiBpcyB0aGUga2V5]
    [HTTP request 1/1]
    [Response in frame: 4563]
```

```
0000  dc 2c 6e 6b 0c 02 a8 5e  45
0010  00 ae 7d cb 40 00 80 06  00
0020  2e 35 e6 88 00 50 f4 19  14
0030  04 05 66 a0 00 00 47 45  54
0040  69 42 70 63 79 42 30 61  47
0050  48 54 54 50 2f 31 2e 31  0d
0060  2d 45 6e 63 6f 64 69 6e  67
0070  69 74 79 0d 0a 48 6f 73  74
0080  6d 64 2e 65 64 75 0d 0a  43
0090  6f 6e 3a 20 63 6c 6f 73  65
00a0  41 67 65 6e 74 3a 20 50  79
00b0  6c 6c 69 62 2f 32 2e 37  0d
```



```
http
No.    Time       Source          Destination     Protocol Length Info
   770 1.412087   10.125.26.174   18.160.46.53    HTTP     199 GET /this-is-not-even-my-final-form. HTTP/1.1
   775 1.417008   18.160.46.53    10.125.26.174   HTTP     641 HTTP/1.1 301 Moved Permanently  (text/html)
  2943 3.956960   10.125.26.174   18.160.46.53    HTTP     200 GET /All-your-base64-are-belong-to-us HTTP/1.1
  2947 3.961559   18.160.46.53    10.125.26.174   HTTP     642 HTTP/1.1 301 Moved Permanently  (text/html)
  4558 6.339679   10.125.26.174   18.160.46.53    HTTP     188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
  4563 6.343758   18.160.46.53    10.125.26.174   HTTP     630 HTTP/1.1 301 Moved Permanently  (text/html)
  8141 10.431338  10.125.26.174   18.160.46.53    HTTP     199 GET /this-is-not-even-my-final-form. HTTP/1.1
  8144 10.435423  18.160.46.53    10.125.26.174   HTTP     641 HTTP/1.1 301 Moved Permanently  (text/html)
 10277 12.742661  10.125.26.174   18.160.46.53    HTTP     200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 10282 12.746574  18.160.46.53    10.125.26.174   HTTP     642 HTTP/1.1 301 Moved Permanently  (text/html)
 13312 15.106833  10.125.26.174   18.160.46.53    HTTP     188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 13318 15.110675  18.160.46.53    10.125.26.174   HTTP     630 HTTP/1.1 301 Moved Permanently  (text/html)
 16615 19.191504  10.125.26.174   18.160.46.53    HTTP     199 GET /this-is-not-even-my-final-form. HTTP/1.1
 16620 19.195650  18.160.46.53    10.125.26.174   HTTP     641 HTTP/1.1 301 Moved Permanently  (text/html)
```

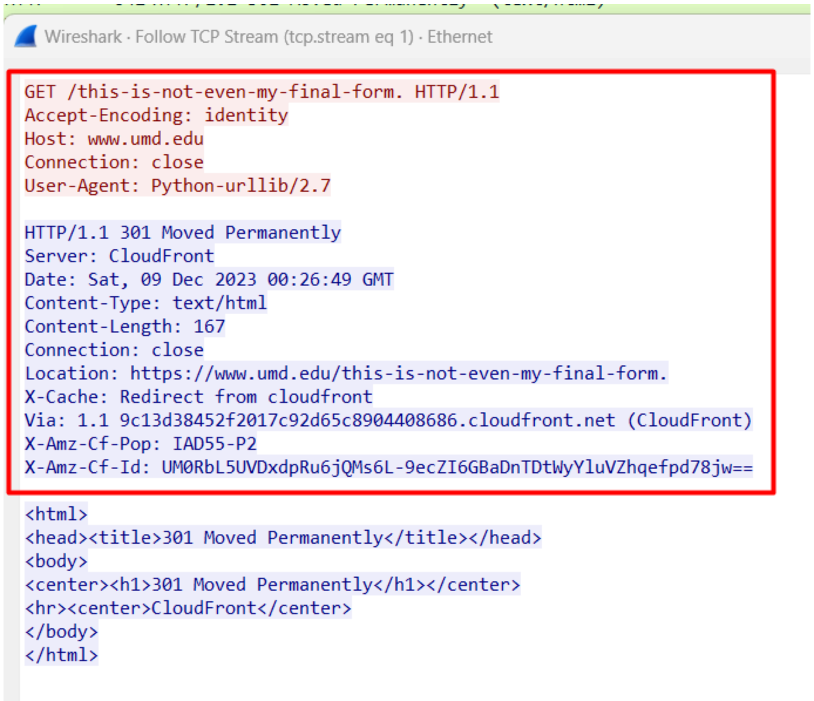


```
> Frame 8141: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF},
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 18.160.46.53
> Transmission Control Protocol, Src Port: 59021, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
v Hypertext Transfer Protocol
  v GET /this-is-not-even-my-final-form. HTTP/1.1\r\n
    v [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: 8144]
```

```
0000  dc 2c 6e 6b 0c 02 a8 5e  45 d4 4b dd 08
0010  00 b9 7d e8 40 00 80 06  00 00 0a 7d 1a
0020  2e 35 e6 8d 00 50 44 ca  4d 1e ce 49 c1
0030  04 05 66 ab 00 00 47 45  54 20 2f 74 68
0040  69 73 2d 6e 6f 74 2d 65  76 65 6e 2d 6d
0050  69 6e 61 6c 2d 66 6f 72  6d 2e 20 48 54
0060  31 2e 31 0d 0a 41 63 63  65 70 74 2d 45
0070  64 69 6e 67 3a 20 69 64  65 6e 74 69 74
0080  48 6f 73 74 3a 20 77 77  77 2e 75 6d 64
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e
00a0  6c 6f 73 65 0d 0a 55 73  65 72 2d 41 67
00b0  3a 20 50 79 74 68 6f 6e  2d 75 72 6c 6c
00c0  32 2e 37 0d 0a 0d 0a
```

Follow TCP Stream Analysis:

For the first request to "http://www.umd.edu/All-your-base64-are-belong-to-us," the TCP stream revealed a "301 Moved Permanently" server response, indicating redirection.

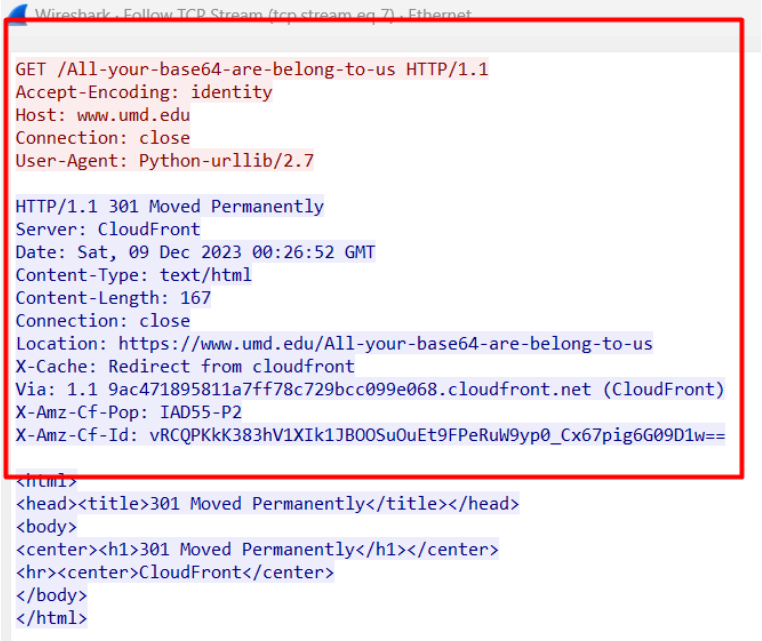


```
GET /this-is-not-even-my-final-form. HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sat, 09 Dec 2023 00:26:49 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 9c13d38452f2017c92d65c8904408686.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: IAD55-P2
X-Amz-Cf-Id: UM0RbL5UVDxdpRu6jQMs6L-9ecZI6GBaDnTDtWyYluVZhqefpd78jw==

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

The second request to "http://www.umd.edu/cjJkMiBpcyB0aGUga2V5" followed a similar pattern with the server responding with a redirection status.

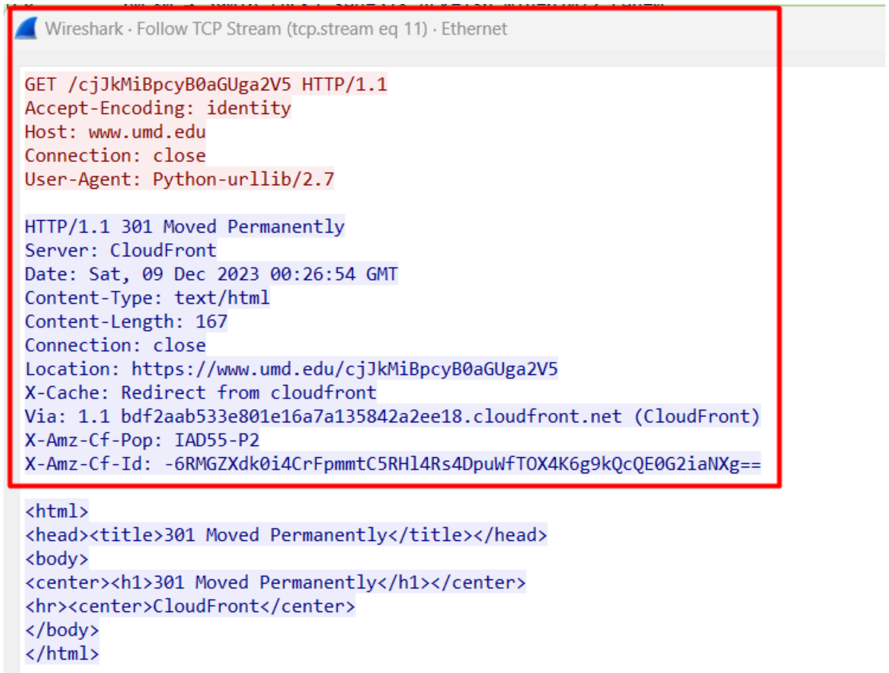


```
GET /All-your-base64-are-belong-to-us HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sat, 09 Dec 2023 00:26:52 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 9ac471895811a7ff78c729bcc099e068.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: IAD55-P2
X-Amz-Cf-Id: vRCQPKkK383hV1XIk1JBOOSuOuEt9FPeRuW9yp0_Cx67pig6G09D1w==

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

The third request to "http://www.umd.edu/this-is-not-even-my-final-form" was also analyzed, confirming the pattern observed in the previous requests.



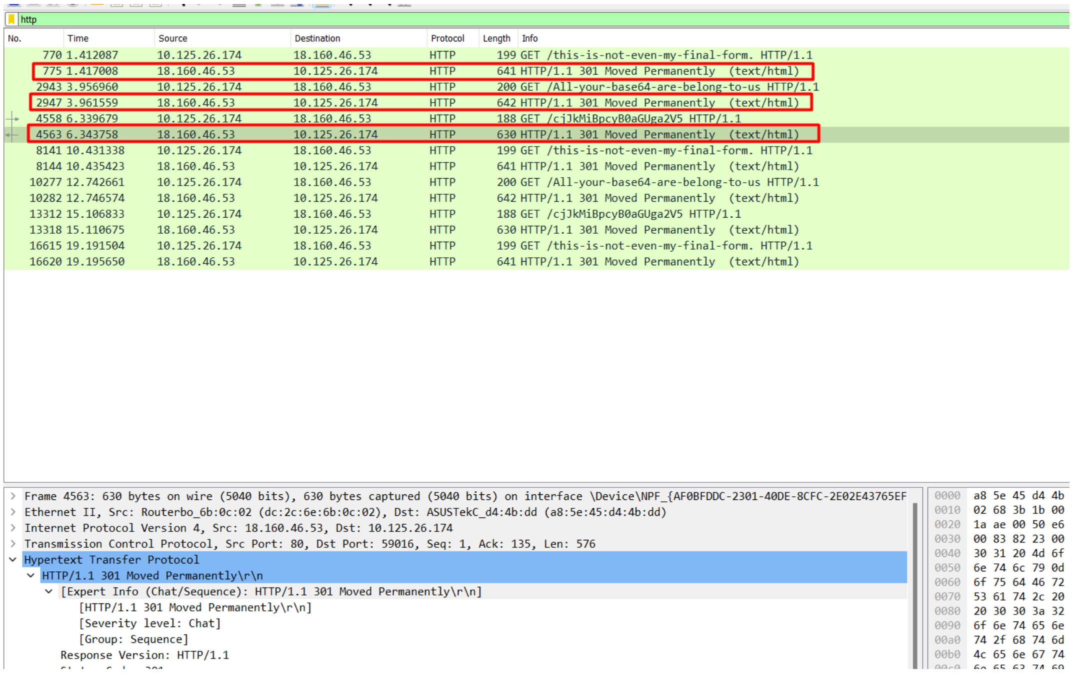
Wireshark · Follow TCP Stream (tcp.stream eq 11) · Ethernet

```
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: Sat, 09 Dec 2023 00:26:54 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/cjJkMiBpcyB0aGUga2V5
X-Cache: Redirect from cloudfront
Via: 1.1 bdf2aab533e801e16a7a135842a2ee18.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: IAD55-P2
X-Amz-Cf-Id: -6RMGZXdk0i4CrFpmmtC5RHl4Rs4DpuWfTOX4K6g9kQcQE0G2iaNXg==

<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 server's responses to these requests consistently included a "301 Moved Permanently" status code, a typical redirection technique in web communication.

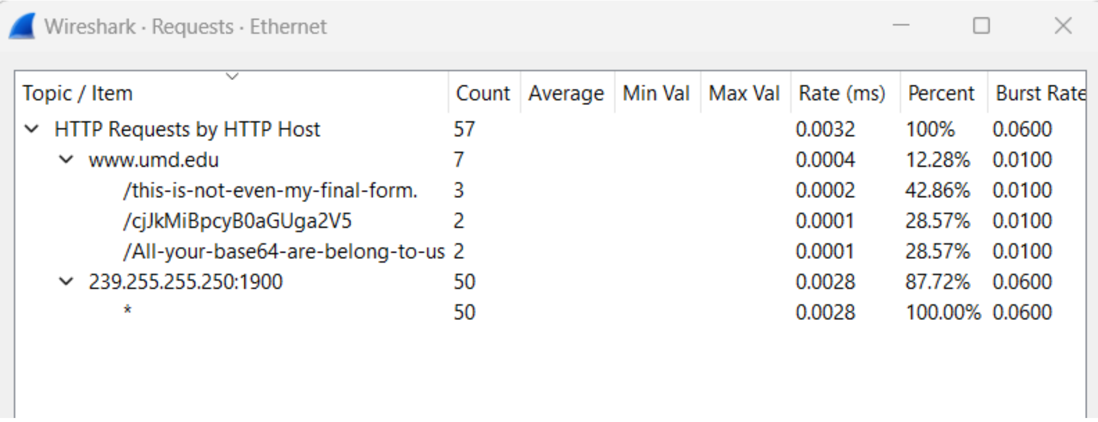


```
No.    Time       Source          Destination     Protocol  Length Info
  770  1.412087   10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
  775  1.417008   18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
 2943  3.956960   10.125.26.174   18.160.46.53    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 2947  3.961559   18.160.46.53    10.125.26.174   HTTP      642 HTTP/1.1 301 Moved Permanently  (text/html)
 4558  6.339679   10.125.26.174   18.160.46.53    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 4563  6.343758   18.160.46.53    10.125.26.174   HTTP      630 HTTP/1.1 301 Moved Permanently  (text/html)
 8141  10.431338  10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 8144  10.435423  18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
10277  12.742661  10.125.26.174   18.160.46.53    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
10282  12.746574  18.160.46.53    10.125.26.174   HTTP      642 HTTP/1.1 301 Moved Permanently  (text/html)
13312  15.106833  10.125.26.174   18.160.46.53    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
13318  15.110675  18.160.46.53    10.125.26.174   HTTP      630 HTTP/1.1 301 Moved Permanently  (text/html)
16615  19.191504  10.125.26.174   18.160.46.53    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
16620  19.195650  18.160.46.53    10.125.26.174   HTTP      641 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
> Frame 4563: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF
> Ethernet II, Src: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02), Dst: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd)
> Internet Protocol Version 4, Src: 18.160.46.53, Dst: 10.125.26.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 59016, Seq: 1, Ack: 135, Len: 576
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        [HTTP/1.1 301 Moved Permanently\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
```

```
0000  a8 5e 45 d4 4b
0010  02 68 3b 1b 00
0020  1a ae 00 50 e6
0030  00 83 82 23 00
0040  30 31 20 4d 6f
0050  6e 74 6c 79 0d
0060  6f 75 64 46 72
0070  53 61 74 2c 20
0080  20 30 30 3a 32
0090  6f 6e 74 65 6e
00a0  74 2f 68 74 6d
00b0  4c 65 6e 67 74
```

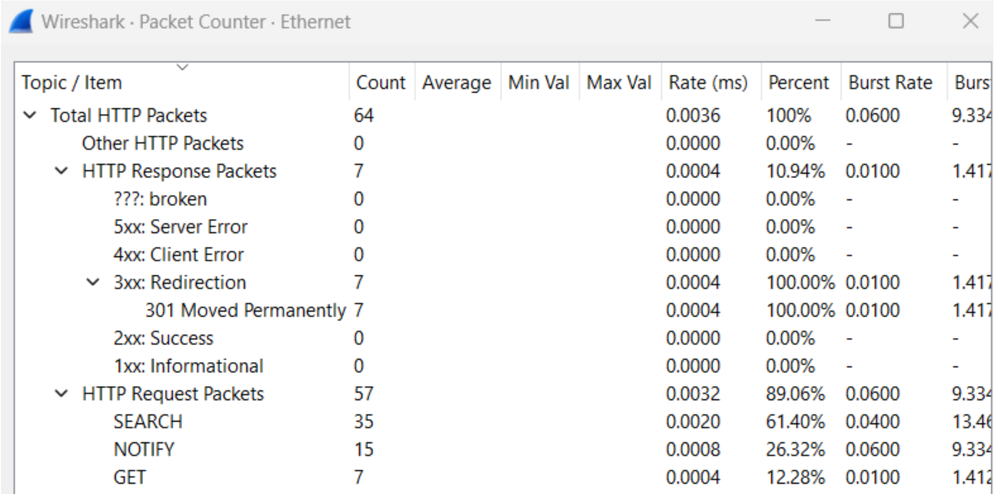
Request Tab Findings: The Requests tab in Wireshark showed a total of 7 HTTP requests made by "obiwan2.exe" to "www.umd.edu." This pattern of repeated communication suggests programmed or automated behavior, with each request targeting different URLs, implying a deliberate sequence of actions or messages.



Wireshark · Requests · Ethernet

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate
HTTP Requests by HTTP Host	57				0.0032	100%	0.0600
www.umd.edu	7				0.0004	12.28%	0.0100
/this-is-not-even-my-final-form.	3				0.0002	42.86%	0.0100
/cjJkMiBpcyB0aGUga2V5	2				0.0001	28.57%	0.0100
/All-your-base64-are-belong-to-us	2				0.0001	28.57%	0.0100
239.255.255.250:1900	50				0.0028	87.72%	0.0600
*	50				0.0028	100.00%	0.0600

Packet Counter Confirmation: The Packet Counter tab in Wireshark recorded 7 requests sent to "www.umd.edu" and an equal number of responses received, all with the "301 Moved Permanently" status code, underscoring the sophisticated and potentially complex nature of "obiwan2.exe."



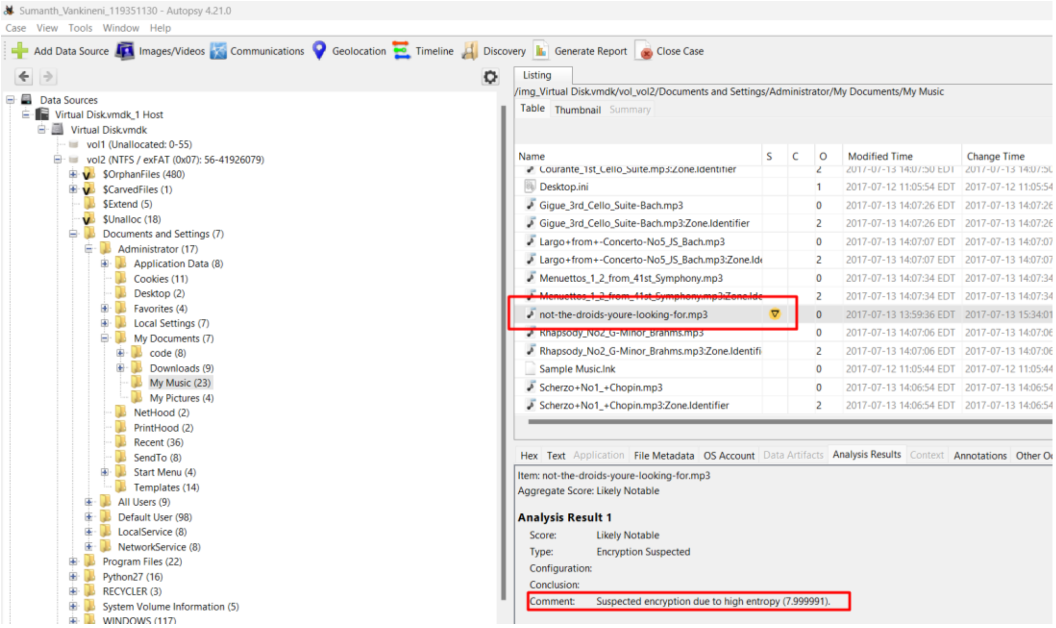
Wireshark · Packet Counter · Ethernet

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burs
Total HTTP Packets	64				0.0036	100%	0.0600	9.334
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	7				0.0004	10.94%	0.0100	1.417
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	7				0.0004	100.00%	0.0100	1.417
301 Moved Permanently	7				0.0004	100.00%	0.0100	1.417
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	57				0.0032	89.06%	0.0600	9.334
SEARCH	35				0.0020	61.40%	0.0400	13.46
NOTIFY	15				0.0008	26.32%	0.0600	9.334
GET	7				0.0004	12.28%	0.0100	1.412

iii.Analysis of "not-the-droids-you-are-looking-for.mp3"

Decrypting and Examining the Encrypted MP3 File

This section details the procedure and findings from the analysis of the encrypted MP3 file "not-the-droids-you-are-looking-for.mp3," which involved crucial decryption using a key derived from the analysis of "obiwan2.exe" and the application of Veracrypt for the decryption process.



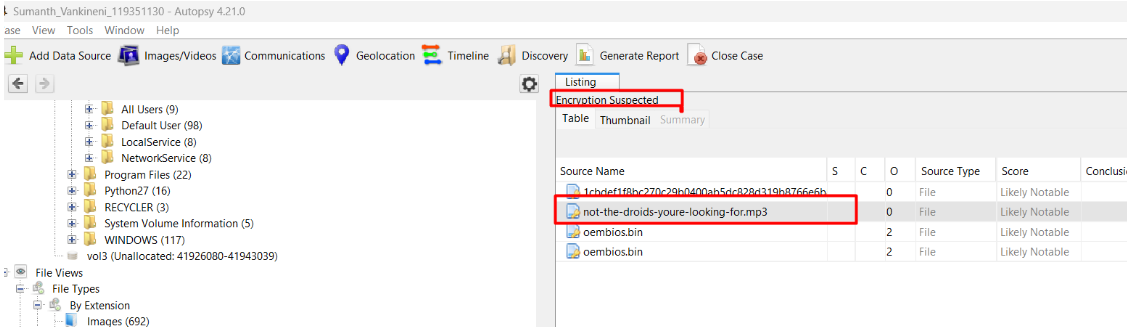
/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/My Music

Name	S	C	O	Modified Time	Change Time
Courante_1st_Cello_Suite.mp3:Zone.Identifier			2	2017-07-13 14:07:50 EDT	2017-07-13 14:07:5
Desktop.ini			1	2017-07-12 11:05:54 EDT	2017-07-12 11:05:54
Gigue_3rd_Cello_Suite-Bach.mp3			0	2017-07-13 14:07:26 EDT	2017-07-13 14:07:26
Gigue_3rd_Cello_Suite-Bach.mp3:Zone.Identifier			2	2017-07-13 14:07:26 EDT	2017-07-13 14:07:26
Largo+from+-Concerto-No5_JS_Bach.mp3			0	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07
Largo+from+-Concerto-No5_JS_Bach.mp3:Zone.Ide			2	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07
Menuettos_1_2_from_41st_Symphony.mp3			0	2017-07-13 14:07:34 EDT	2017-07-13 14:07:34
Menuettos_1_2_from_41st_Symphony.mp3:Zone.Ide			2	2017-07-13 14:07:34 EDT	2017-07-13 14:07:34
not-the-droids-youre-looking-for.mp3	▽		0	2017-07-13 13:59:36 EDT	2017-07-13 15:34:01
Rhapsody_No2_G-Minor_Brahms.mp3			0	2017-07-13 14:07:06 EDT	2017-07-13 14:07:06
Rhapsody_No2_G-Minor_Brahms.mp3:Zone.Identifi			2	2017-07-13 14:07:06 EDT	2017-07-13 14:07:06
Sample Music.lnk			0	2017-07-12 11:05:44 EDT	2017-07-12 11:05:44
Scherzo+No1_+Chopin.mp3			0	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54
Scherzo+No1_+Chopin.mp3:Zone.Identifier			2	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54

Item: not-the-droids-youre-looking-for.mp3
Aggregate Score: Likely Notable

Analysis Result 1

Score: Likely Notable
Type: Encryption Suspected
Configuration:
Conclusion:
Comment: Suspected encryption due to high entropy (7.999991).

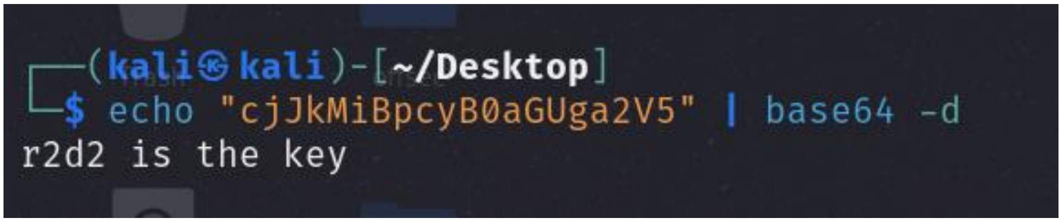


Encryption Suspected

Source Name	S	C	O	Source Type	Score	Conclusi
1cbdef1f8bc270c29b0400ab5dc828d319b8766e6b			0	File	Likely Notable	
not-the-droids-youre-looking-for.mp3			0	File	Likely Notable	
oembios.bin			2	File	Likely Notable	
oembios.bin			2	File	Likely Notable	

Decryption Process:

Base64 Decoded Key: The analysis of "obiwan2.exe" revealed a base64 encoded string. Once decoded, the string read "r2d2 is the key," which was hypothesized to be the decryption passphrase.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "cjJkMiBpcyB0aGUga2V5" | base64 -d
r2d2 is the key
```

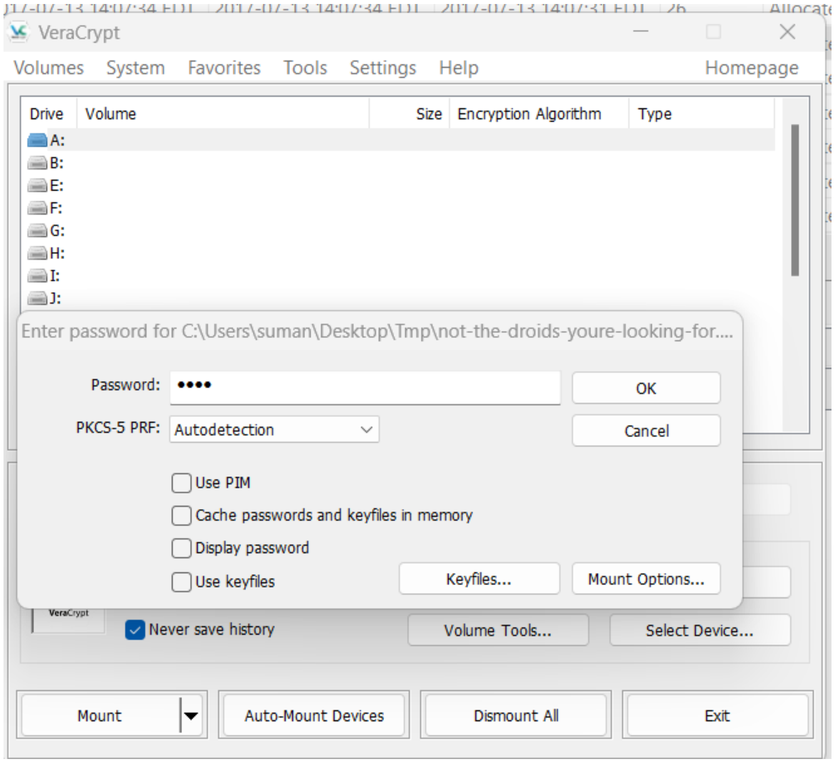
Using Veracrypt: Veracrypt, renowned for its powerful encryption and decryption capabilities, was employed to decrypt the MP3 file.

Decryption Steps:

The MP3 file was loaded into Veracrypt.

"r2d2," derived from the base64 decoded message, was input as the decryption passphrase.

The decryption was initiated, with its successful completion being meticulously monitored.



Enter password for C:\Users\suman\Desktop\Tmp\not-the-droids-youre-looking-for....

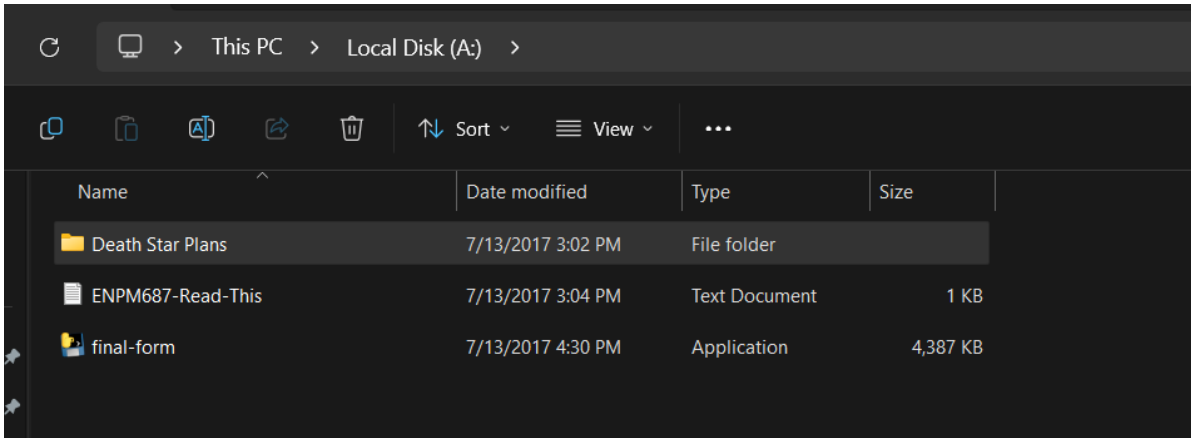
Password: ••••

PKCS-5 PRF: Autodetection

☐ Use PIM
☐ Cache passwords and keyfiles in memory
☐ Display password
☐ Use keyfiles
☑ Never save history

Post-Decryption Examination:

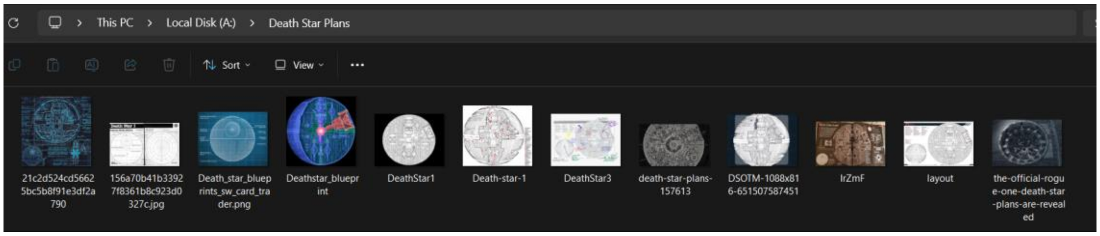
The successful decryption of "not-the-droids-you-are-looking-for.mp3" facilitated an in-depth exploration of its previously encrypted contents.



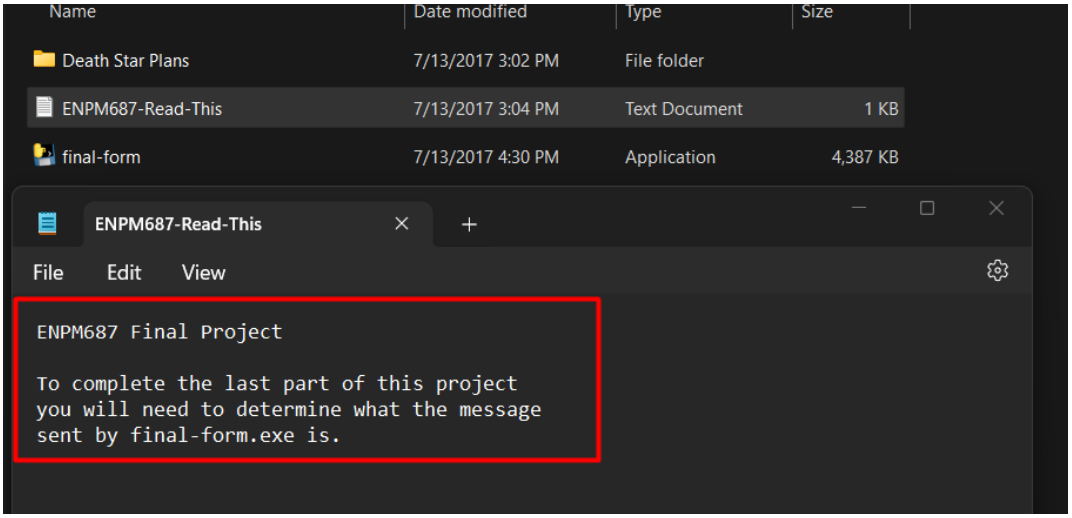
Name	Date modified	Type	Size
Death Star Plans	7/13/2017 3:02 PM	File folder	
ENPM687-Read-This	7/13/2017 3:04 PM	Text Document	1 KB
final-form	7/13/2017 4:30 PM	Application	4,387 KB

Contents of the Decrypted File:

A folder titled “Death Star Plans” was discovered within the decrypted file, containing images and schematics of the Death Star. This finding indicated the file's utilization for covertly storing and transmitting sensitive information.


This PC > Local Disk (A:) > Death Star Plans
Sort
View
21c2d524cd56625bc5b8f91e3df2a790
156a70b41b33927f8361b8c923d0327c.jpg
Death_star_blueprints_sw_card_trader.png
Deathstar_blueprint
DeathStar1
Death-star-1
DeathStar3
death-star-plans-157613
DSOTM-1088x816-651507587451
lrZmF
layout
the-official-rogue-one-death-star-plans-are-revealed

A significant discovery was a text file named “ENPM687-Read-This.txt,” which contained directives to execute 'final-form.exe,' signifying additional steps in the ongoing investigation.

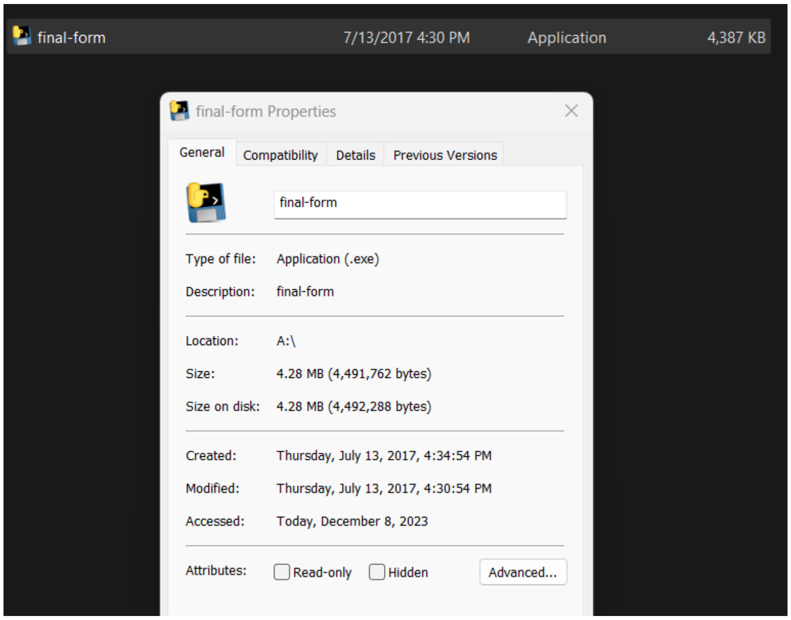


Name	Date modified	Type	Size
Death Star Plans	7/13/2017 3:02 PM	File folder	
ENPM687-Read-This	7/13/2017 3:04 PM	Text Document	1 KB
final-form	7/13/2017 4:30 PM	Application	4,387 KB

```
ENPM687 Final Project

To complete the last part of this project
you will need to determine what the message
sent by final-form.exe is.
```

The presence of an executable named "final-form.exe" within the decrypted file was a notable finding. Its inclusion alongside other contents implied that it could be an integral component in deciphering the broader context and potential objectives of the data concealed within the MP3 file.



final-form	7/13/2017 4:30 PM	Application	4,387 KB

final-form

Type of file: Application (.exe)
Description: final-form

Location: A:\
Size: 4.28 MB (4,491,762 bytes)
Size on disk: 4.28 MB (4,492,288 bytes)

Created: Thursday, July 13, 2017, 4:34:54 PM
Modified: Thursday, July 13, 2017, 4:30:54 PM
Accessed: Today, December 8, 2023

Attributes: □ Read-only □ Hidden

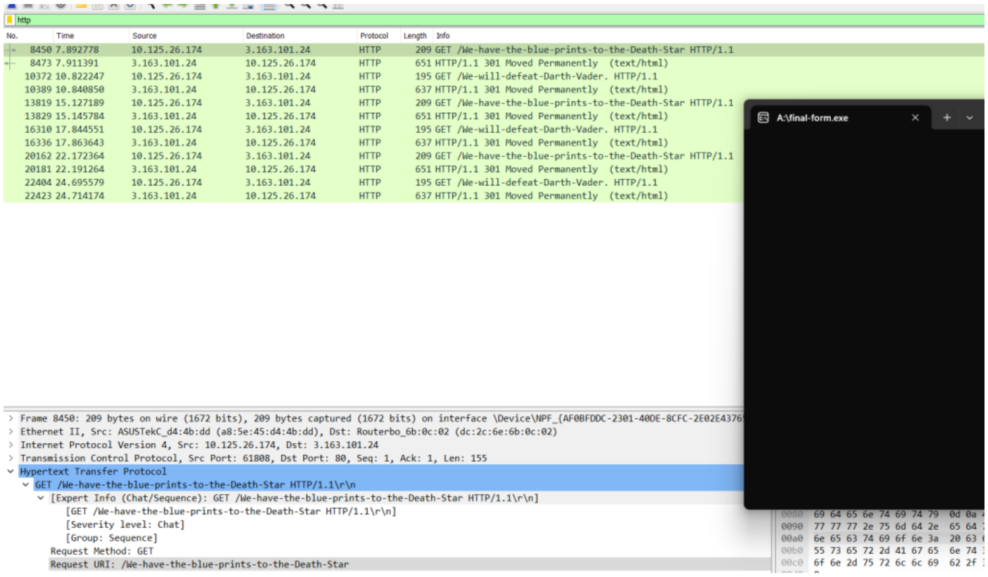
iv.Analysis of "final-form.exe"

Comprehensive Examination of "final-form.exe" Execution and Network Activity

This section outlines the procedure and findings from the analysis of "final-form.exe," focusing on its execution behavior and network interactions. The analysis was segmented into two primary areas: monitoring the execution and behavior of the executable, and conducting an in-depth Wireshark analysis to understand its network interactions.

Execution and Behavior:

Execution Monitoring: "final-form.exe" was executed within a controlled setting, allowing for close observation of its activities. This was essential for understanding the executable's real-time behavior and system and network interactions.



```
No.   Time       Source          Destination     Protocol Length Info
 8450 7.892778   10.125.26.174   3.163.101.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
 8473 7.911391   3.163.101.24    10.125.26.174   HTTP     651 HTTP/1.1 301 Moved Permanently  (text/html)
10372 10.822247  10.125.26.174   3.163.101.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
10389 10.840850  3.163.101.24    10.125.26.174   HTTP     637 HTTP/1.1 301 Moved Permanently  (text/html)
13819 15.127189  10.125.26.174   3.163.101.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
13829 15.145784  3.163.101.24    10.125.26.174   HTTP     651 HTTP/1.1 301 Moved Permanently  (text/html)
16310 17.844551  10.125.26.174   3.163.101.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
16336 17.863643  3.163.101.24    10.125.26.174   HTTP     637 HTTP/1.1 301 Moved Permanently  (text/html)
20162 22.172364  10.125.26.174   3.163.101.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
20181 22.191264  3.163.101.24    10.125.26.174   HTTP     651 HTTP/1.1 301 Moved Permanently  (text/html)
22404 24.695579  10.125.26.174   3.163.101.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
22423 24.714174  3.163.101.24    10.125.26.174   HTTP     637 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
> Frame 8450: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E4376
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 3.163.101.24
> Transmission Control Protocol, Src Port: 61808, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
v Hypertext Transfer Protocol
  v GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
    v [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
```

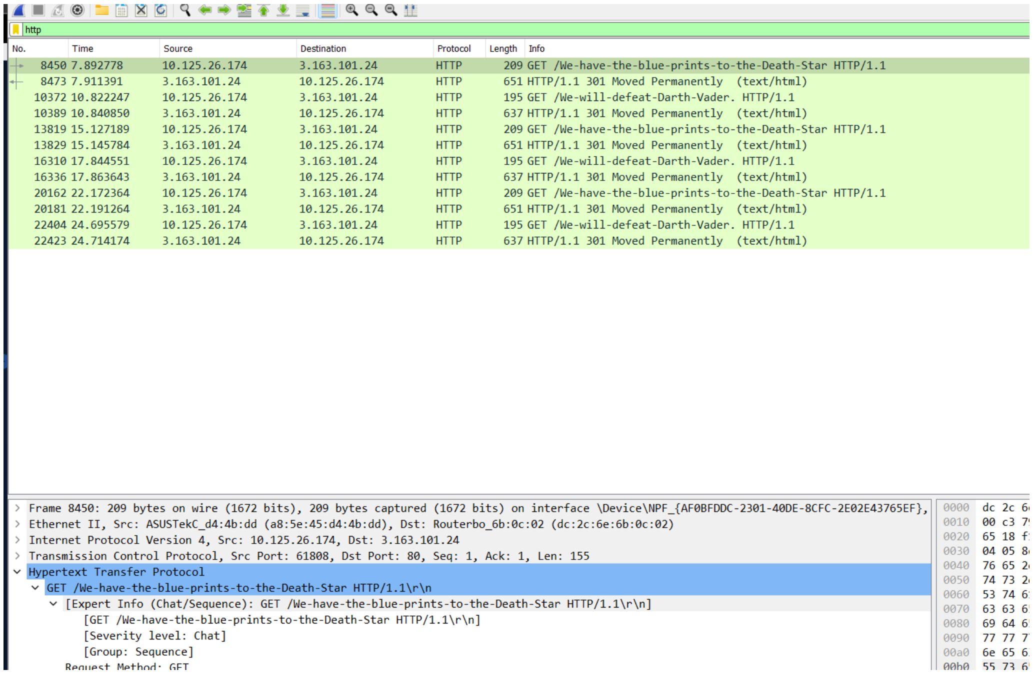
```
0080  69 64 65 6e 74 69 74 79  0d 0a
0090  77 77 77 2e 75 6d 64 2e  65 64
00a0  6e 65 63 74 69 6f 6e 3a  20 63
00b0  55 73 65 72 2d 41 67 65  6e 74
00c0  6f 6e 2d 75 72 6c 6c 69  62 2f
```

Process Explorer Analysis: Process Explorer was used to monitor the running status of "final-form.exe." This tool shed light on the executable's processes, particularly its attempts to establish connections to remote servers over the internet, providing a comprehensive view of its behavior.

TCP Connections Observation: The TCP connections related to "final-form.exe" were meticulously examined. Detailed information regarding the nature and destinations of these connections was gathered through TCP stream monitoring, aiding in deciphering the network behavior of the executable.

Wireshark Analysis:

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



http

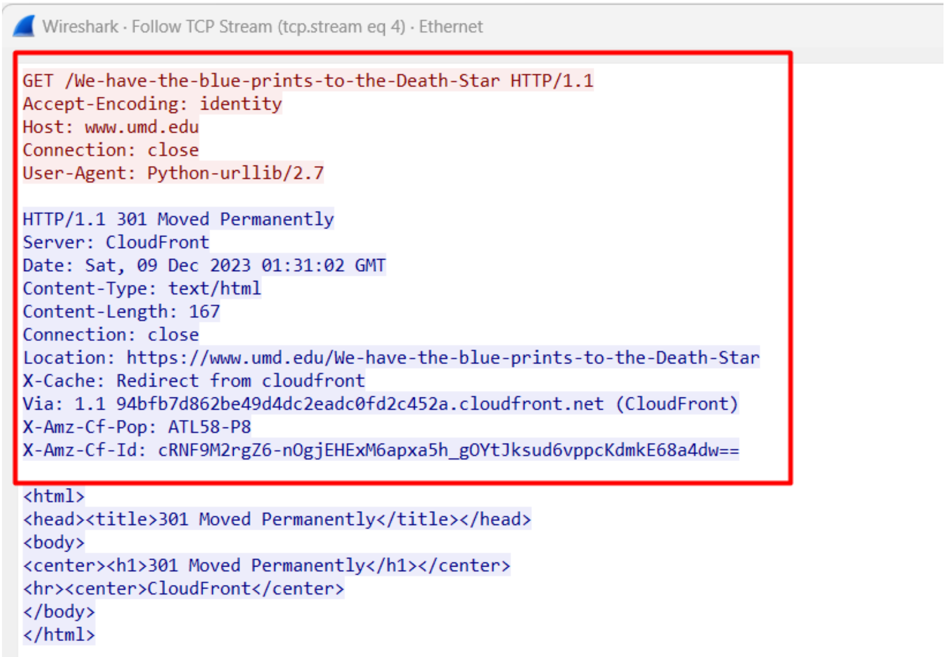
No.	Time	Source	Destination	Protocol	Length	Info
8450	7.892778	10.125.26.174	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
8473	7.911391	3.163.101.24	10.125.26.174	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
10372	10.822247	10.125.26.174	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
10389	10.840850	3.163.101.24	10.125.26.174	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
13819	15.127189	10.125.26.174	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
13829	15.145784	3.163.101.24	10.125.26.174	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
16310	17.844551	10.125.26.174	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
16336	17.863643	3.163.101.24	10.125.26.174	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
20162	22.172364	10.125.26.174	3.163.101.24	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
20181	22.191264	3.163.101.24	10.125.26.174	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
22404	24.695579	10.125.26.174	3.163.101.24	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
22423	24.714174	3.163.101.24	10.125.26.174	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)

```
> Frame 8450: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{AF0BFDDC-2301-40DE-8CFC-2E02E43765EF},
> Ethernet II, Src: ASUSTekC_d4:4b:dd (a8:5e:45:d4:4b:dd), Dst: Routerbo_6b:0c:02 (dc:2c:6e:6b:0c:02)
> Internet Protocol Version 4, Src: 10.125.26.174, Dst: 3.163.101.24
> Transmission Control Protocol, Src Port: 61808, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
v Hypertext Transfer Protocol
  v GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
    v [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
```

```
0000  dc 2c
0010  00 c3
0020  65 18
0030  04 05
0040  76 65
0050  74 73
0060  53 74
0070  63 63
0080  69 64
0090  77 77
00a0  6e 65
00b0  55 73
```

Follow TCP Stream Analysis:

The TCP stream for the first HTTP request to "http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star" was analyzed, revealing the full HTTP request and response cycle, including a "301 Moved Permanently" status code from the server.



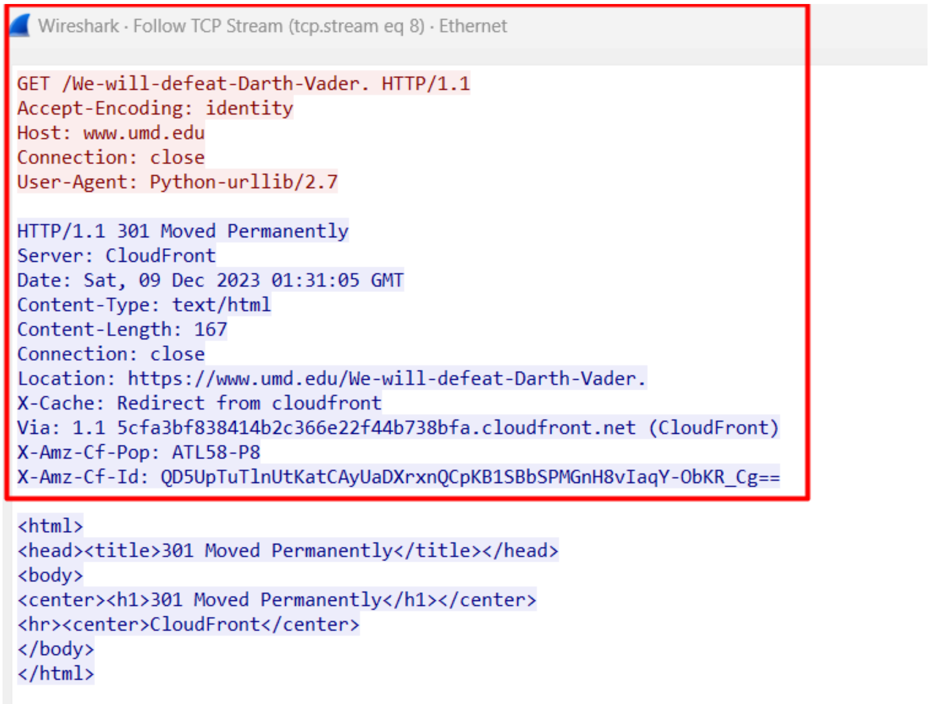
Wireshark · Follow TCP Stream (tcp.stream eq 4) · Ethernet

```
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: Sat, 09 Dec 2023 01:31:02 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 94bfb7d862be49d4dc2eadc0fd2c452a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: cRNF9M2rgZ6-nOgjEHExM6apxa5h_gOYtJksud6vppcKdmkE68a4dw==

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

A similar approach was taken for the second HTTP request to "http://www.umd.edu/We-will-defeat-Darth-Vader," providing insights into the nature of this request and the server's identical response.



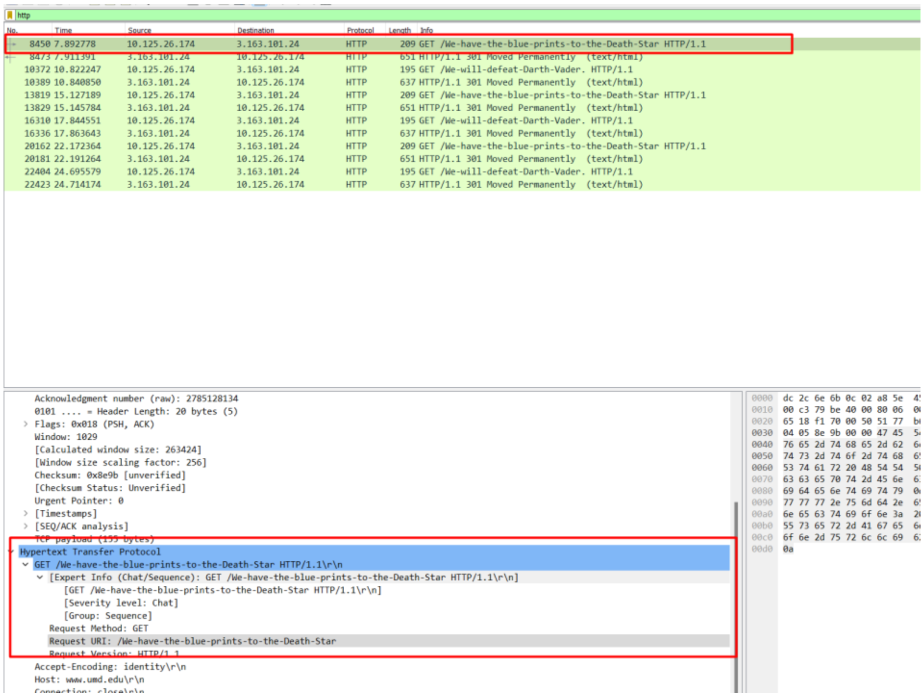
Wireshark · Follow TCP Stream (tcp.stream eq 8) · Ethernet

```
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: Sat, 09 Dec 2023 01:31:05 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 5cfa3bf838414b2c366e22f44b738bfa.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: QD5UpTuTlnUtKatCAyUaDXrxnQCpKB1SBbSPMGnH8vIaqY-ObKR_Cg==

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

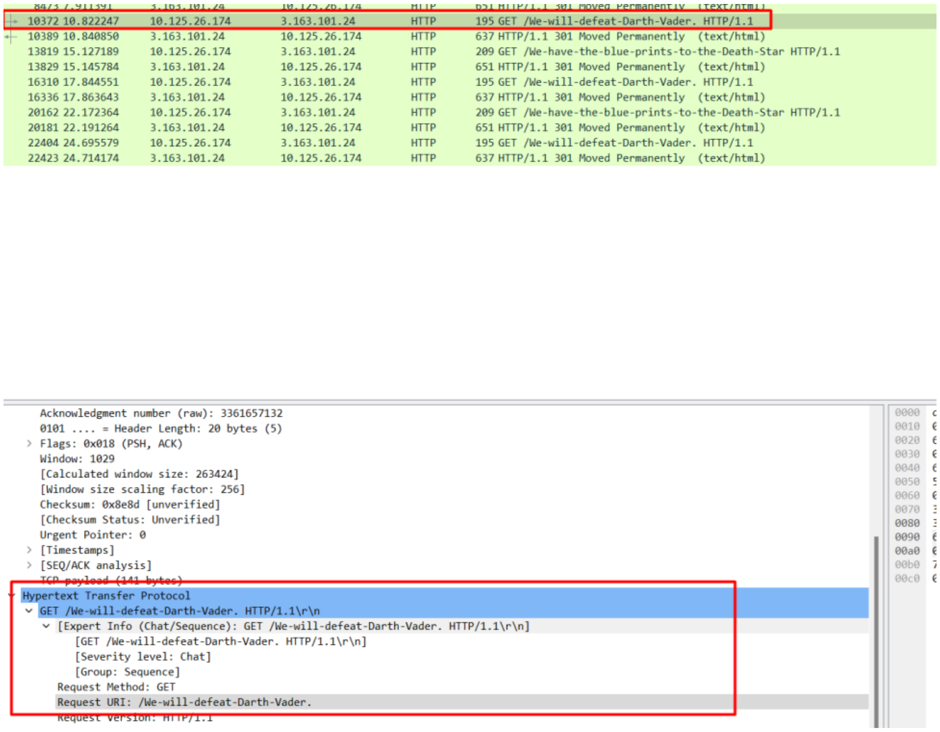
HTTP Requests Examination: Analysis of the HTTP requests indicated that "final-form.exe" specifically targeted URLs on the "www.umd.edu" server, such as "http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star" and "http://www.umd.edu/We-will-defeat-Darth-Vader." This pattern suggested a deliberate communication strategy, potentially revealing the executable's objectives or operational tactics.



```
http
No.    Time       Source         Destination    Protocol Length Info
  8450 7.892778   10.125.26.174  3.163.101.24   HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  8473 7.911391   3.163.101.24   10.125.26.174  HTTP     651 HTTP/1.1 301 Moved Permanently  (text/html)
 10372 10.822247  10.125.26.174  3.163.101.24   HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
 10389 10.840850  3.163.101.24   10.125.26.174  HTTP     637 HTTP/1.1 301 Moved Permanently  (text/html)
 13819 15.127189  10.125.26.174  3.163.101.24   HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
 13829 15.145784  3.163.101.24   10.125.26.174  HTTP     651 HTTP/1.1 301 Moved Permanently  (text/html)
 16310 17.844551  10.125.26.174  3.163.101.24   HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
 16336 17.863643  3.163.101.24   10.125.26.174  HTTP     637 HTTP/1.1 301 Moved Permanently  (text/html)
 20162 22.172364  10.125.26.174  3.163.101.24   HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
 20181 22.191264  3.163.101.24   10.125.26.174  HTTP     651 HTTP/1.1 301 Moved Permanently  (text/html)
 22404 24.695579  10.125.26.174  3.163.101.24   HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
 22423 24.714174  3.163.101.24   10.125.26.174  HTTP     637 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
    Acknowledgment number (raw): 2785128134
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0x8e9b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (155 bytes)
v Hypertext Transfer Protocol
  v GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
    v [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
```

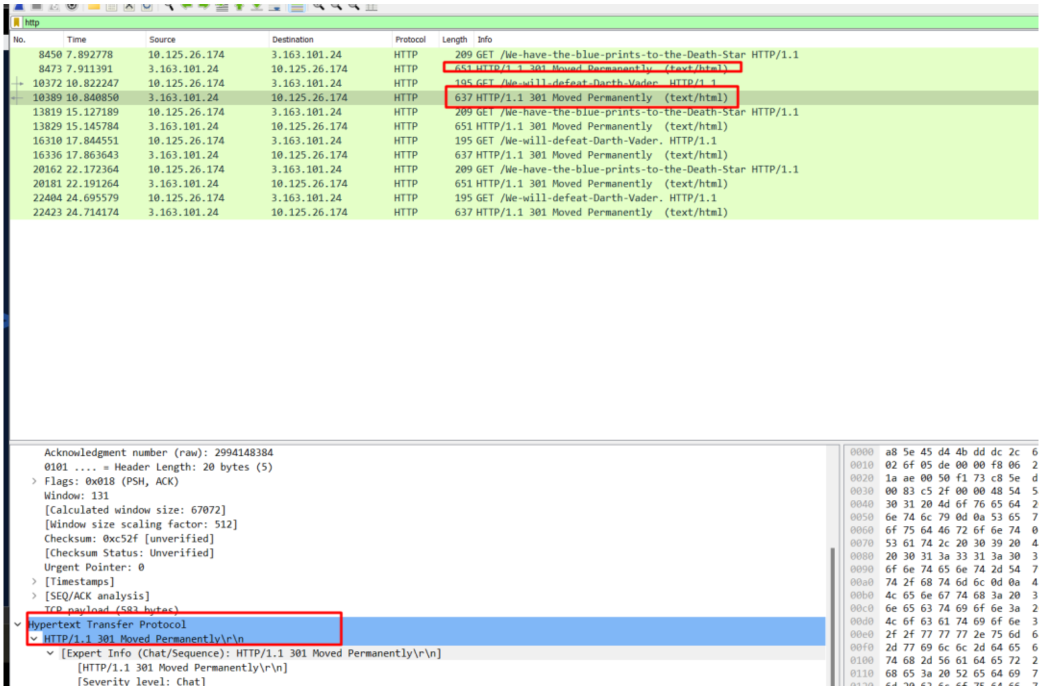
```
0000  dc 2c 6e 6b 0c 02 a8 5e
0010  00 c3 79 be 40 00 80 06
0020  65 18 f1 70 00 50 51 77
0030  04 05 8e 9b 00 00 47 45
0040  76 65 2d 74 68 65 2d 62
0050  74 73 2d 74 6f 2d 74 68
0060  53 74 61 72 20 48 54 54
0070  63 63 65 70 74 2d 45 6e
0080  69 64 65 6e 74 69 74 79
0090  77 77 77 2e 75 6d 64 2e
00a0  6e 65 63 74 69 6f 6e 3a
00b0  55 73 65 72 2d 41 67 65
00c0  6f 6e 2d 75 72 6c 6c 69
00d0  0a
```



```
 8473 7.911391   3.163.101.24    10.125.26.174   HTTP   651 HTTP/1.1 301 Moved Permanently  (text/html)
10372 10.822247  10.125.26.174   3.163.101.24    HTTP   195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
10389 10.840850  3.163.101.24    10.125.26.174   HTTP   637 HTTP/1.1 301 Moved Permanently  (text/html)
13819 15.127189  10.125.26.174   3.163.101.24    HTTP   209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
13829 15.145784  3.163.101.24    10.125.26.174   HTTP   651 HTTP/1.1 301 Moved Permanently  (text/html)
16310 17.844551  10.125.26.174   3.163.101.24    HTTP   195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
16336 17.863643  3.163.101.24    10.125.26.174   HTTP   637 HTTP/1.1 301 Moved Permanently  (text/html)
20162 22.172364  10.125.26.174   3.163.101.24    HTTP   209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
20181 22.191264  3.163.101.24    10.125.26.174   HTTP   651 HTTP/1.1 301 Moved Permanently  (text/html)
22404 24.695579  10.125.26.174   3.163.101.24    HTTP   195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
22423 24.714174  3.163.101.24    10.125.26.174   HTTP   637 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
    Acknowledgment number (raw): 3361657132
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0x8e8d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (141 bytes)
v Hypertext Transfer Protocol
  v GET /We-will-defeat-Darth-Vader. HTTP/1.1\r\n
    v [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
```

Server Responses: The server's responses consistently included a "301 Moved Permanently" status code, suggesting permanent relocation of the requested resources. This redirection technique might indicate an attempt to conceal the true nature of the communication or to redirect to alternate resources.

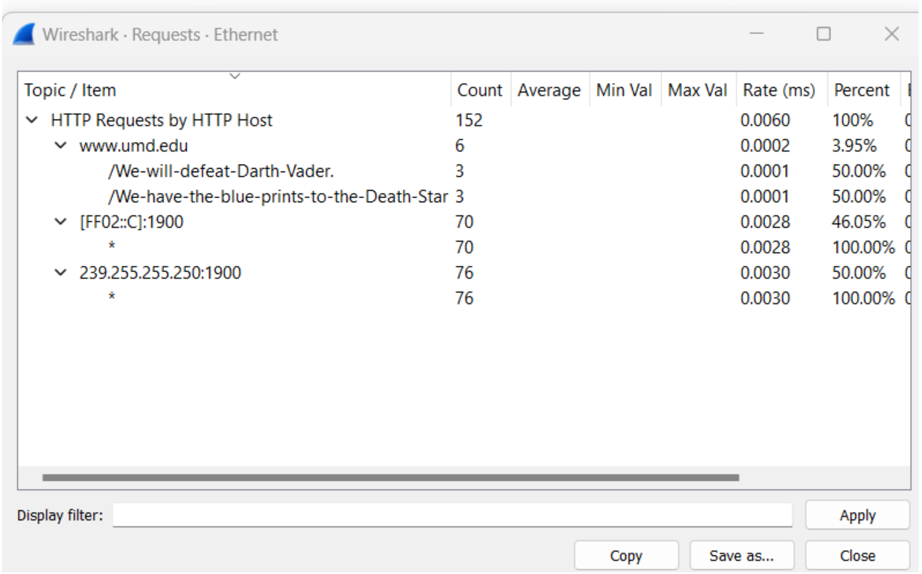


```
http
No.     Time        Source          Destination     Protocol  Length  Info
 8450   7.892778    10.125.26.174   3.163.101.24    HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
 8473   7.911391    3.163.101.24    10.125.26.174   HTTP      651 HTTP/1.1 301 Moved Permanently  (text/html)
10372   10.822247   10.125.26.174   3.163.101.24    HTTP      195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
10389   10.840850   3.163.101.24    10.125.26.174   HTTP      637 HTTP/1.1 301 Moved Permanently  (text/html)
13819   15.127189   10.125.26.174   3.163.101.24    HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
13829   15.145784   3.163.101.24    10.125.26.174   HTTP      651 HTTP/1.1 301 Moved Permanently  (text/html)
16310   17.844551   10.125.26.174   3.163.101.24    HTTP      195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
16336   17.863643   3.163.101.24    10.125.26.174   HTTP      637 HTTP/1.1 301 Moved Permanently  (text/html)
20162   22.172364   10.125.26.174   3.163.101.24    HTTP      209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
20181   22.191264   3.163.101.24    10.125.26.174   HTTP      651 HTTP/1.1 301 Moved Permanently  (text/html)
22404   24.695579   10.125.26.174   3.163.101.24    HTTP      195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
22423   24.714174   3.163.101.24    10.125.26.174   HTTP      637 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
    Acknowledgment number (raw): 2994148384
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 131
    [Calculated window size: 67072]
    [Window size scaling factor: 512]
    Checksum: 0xc52f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (583 bytes)
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        [HTTP/1.1 301 Moved Permanently\r\n]
        [Severity level: Chat]
```

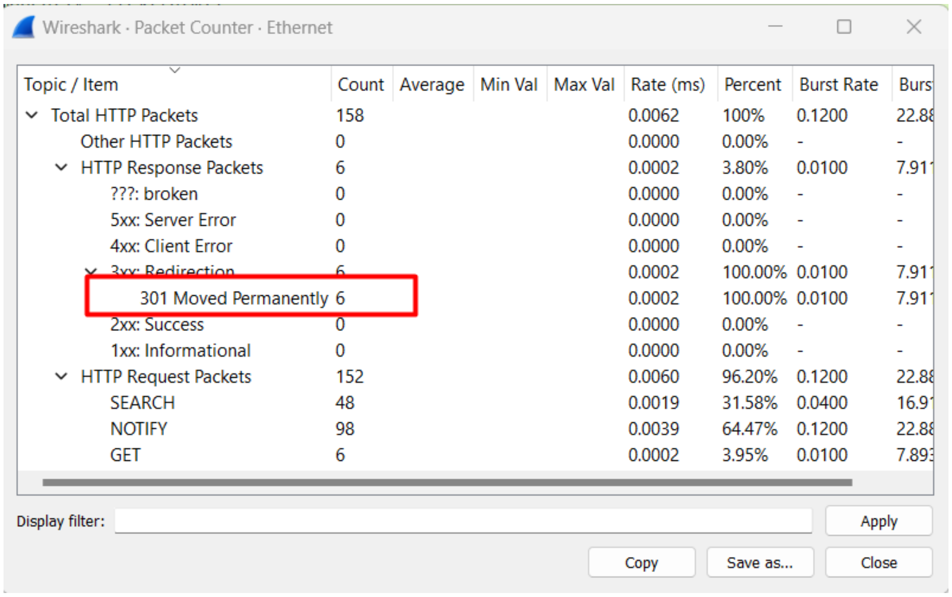
```
0000  a8 5e 45 d4 4b dd dc 2c  6
0010  02 6f 05 de 00 00 f8 06  2
0020  1a ae 00 50 f1 73 c8 5e  d
0030  00 83 c5 2f 00 00 48 54  5
0040  30 31 20 4d 6f 76 65 64  2
0050  6e 74 6c 79 0d 0a 53 65  7
0060  6f 75 64 46 72 6f 6e 74  0
0070  53 61 74 2c 20 30 39 20  4
0080  20 30 31 3a 33 31 3a 30  3
0090  6f 6e 74 65 6e 74 2d 54  7
00a0  74 2f 68 74 6d 6c 0d 0a  4
00b0  4c 65 6e 67 74 68 3a 20  3
00c0  6e 65 63 74 69 6f 6e 3a  2
00d0  4c 6f 63 61 74 69 6f 6e  3
00e0  2f 2f 77 77 77 2e 75 6d  6
00f0  2d 77 69 6c 6c 2d 64 65  6
0100  74 68 2d 56 61 64 65 72  2
0110  68 65 3a 20 52 65 64 69  7
```

Request Tab Findings: The Requests tab in Wireshark showed a total of 6 HTTP requests made by "final-form.exe" to "www.umd.edu." This repetitive communication pattern suggested programmed or automated behavior, possibly designed for specific sequences or triggering certain server actions.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent
HTTP Requests by HTTP Host	152				0.0060	100%
www.umd.edu	6				0.0002	3.95%
/We-will-defeat-Darth-Vader.	3				0.0001	50.00%
/We-have-the-blue-prints-to-the-Death-Star	3				0.0001	50.00%
[FF02::C]:1900	70				0.0028	46.05%
*	70				0.0028	100.00%
239.255.255.250:1900	76				0.0030	50.00%
*	76				0.0030	100.00%

Packet Counter Confirmation: The Packet Counter tab in Wireshark supported these findings, recording 6 requests and 6 corresponding responses, all marked with the "301 Moved Permanently" status code. This consistency reinforces the notion of an automated communication process.



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burs
Total HTTP Packets	158				0.0062	100%	0.1200	22.88
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	6				0.0002	3.80%	0.0100	7.91
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	6				0.0002	100.00%	0.0100	7.91
301 Moved Permanently	6				0.0002	100.00%	0.0100	7.91
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	152				0.0060	96.20%	0.1200	22.88
SEARCH	48				0.0019	31.58%	0.0400	16.91
NOTIFY	98				0.0039	64.47%	0.1200	22.88
GET	6				0.0002	3.95%	0.0100	7.89

Export Attempts: Efforts were made to export objects from these requests for deeper analysis. However, due to continuous redirection, these attempts did not yield significant insights, complicating the retrieval of more detailed information.

4 Strategic Recommendations and Next Steps

Following the in-depth analysis of "obiwan.exe," "obiwan2.exe," "not-the-droids-you-are-looking-for.mp3," and "final-form.exe," we propose a comprehensive strategy for advancing the investigation:

Sophisticated Malware Lifecycle Analysis:

Conduct an in-depth behavioral analysis of the executables to delineate their life cycle, focusing on how they evolve, replicate, and persist within systems. Explore their methods of self-modification and replication to understand their adaptability and resilience.

Source and Distribution Path Exploration:

Investigate the origin of "obiwan.exe" by tracing its distribution channels. Collaborate with ISPs and use advanced forensic tools to track down the initial upload source or distribution networks, potentially uncovering the broader attack infrastructure.

Engagement with Key External Stakeholders:

Initiate a dialogue with the administrators of "www.umd.edu" to assess the server's security status during the periods of executable activity. This engagement could reveal whether there were any security incidents or unusual activities that align with the timeline of the malware's activities.

Intensive Network Traffic and Botnet Investigation:

Perform a comprehensive analysis of network traffic to detect patterns indicative of a larger network of compromised systems or a coordinated cyber attack. Be vigilant for signs of data being siphoned off or lateral movements within the network that could be attributed to the executables.

In-depth Examination of Affected Systems:

Expand the investigation to encompass systems that might have communicated with the compromised device. Analyze their network logs and system files for signs of similar intrusions or malware infections to gauge the extent of the threat.

Cybersecurity Policy Overhaul and Upgrades:

Based on the insights gained from this investigation, thoroughly reassess and upgrade existing cybersecurity policies and incident response frameworks. This could entail refining response strategies, updating configurations of security tools, and enhancing user access control mechanisms.

Key Challenges

Throughout this forensic investigation, I navigated several complex challenges:

Navigating Cryptographic Hurdles:

The process of decrypting the "not-the-droids-you-are-looking-for.mp3" file was a formidable challenge, particularly in accurately determining the decryption key "r2d2" and effectively applying it. This aspect highlighted the critical role of cryptographic expertise in digital forensic investigations.

Addressing Persistent Server Redirection Tactics:

The consistent redirection behavior by "obiwan.exe" and "final-form.exe" complicated the analysis, necessitating advanced network forensic techniques to track and understand the purpose of these redirections and their impact on the investigation.

Recommendation for Controlled Environment Execution:

While the executables have not been run in a controlled environment for this project, it is strongly recommended to do so for any actual investigative purposes. Executing potentially malicious files in a secure, isolated environment is crucial to prevent unintended network spread or activation of harmful payloads. This approach is vital for safely analyzing the behavior and impact of such files, especially in an educational or research setting.

Managing Extensive Data and Complexity:

The sheer volume of data, including diverse file types and extensive network logs, presented significant logistical challenges. This required strategic data management and advanced analytical methodologies to ensure thorough and accurate data interpretation.