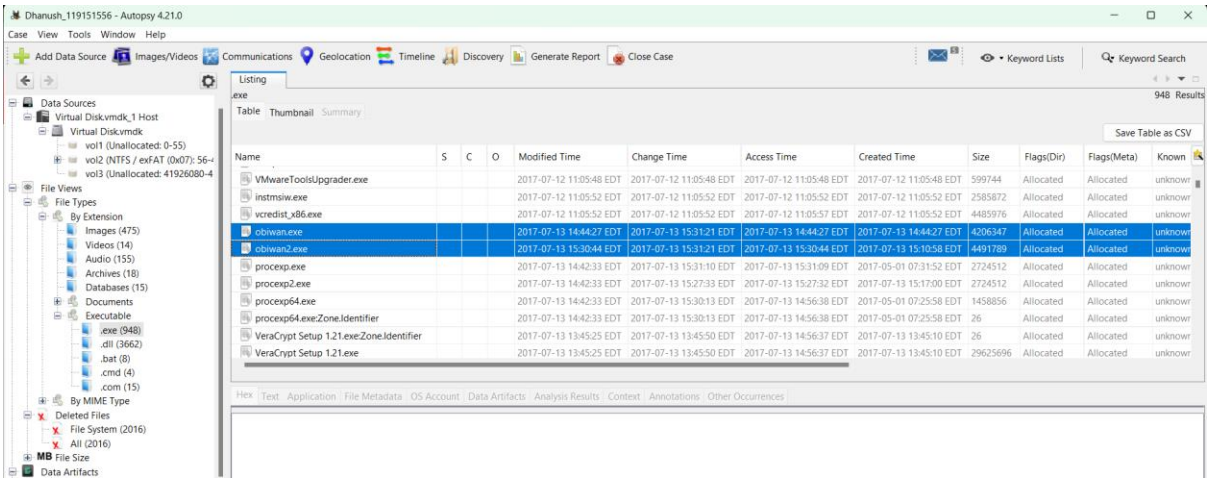
FINAL

Analysis of the obiwan2.exe

Extracting the **obiwan2.exe** file from autopsy.

>Prior to conducting an in-depth examination of "obiwan2.exe," this file was extracted from the hard disk image using Autopsy's default extraction feature. This crucial initial process ensured that we obtained a copy of the executable file for analysis while maintaining the original disk image's integrity. It was fundamental in facilitating a thorough investigation without compromising the integrity of the source data.

>



>There is also another suspicious file,which is obiwan.exe file ,which we will take a look after.

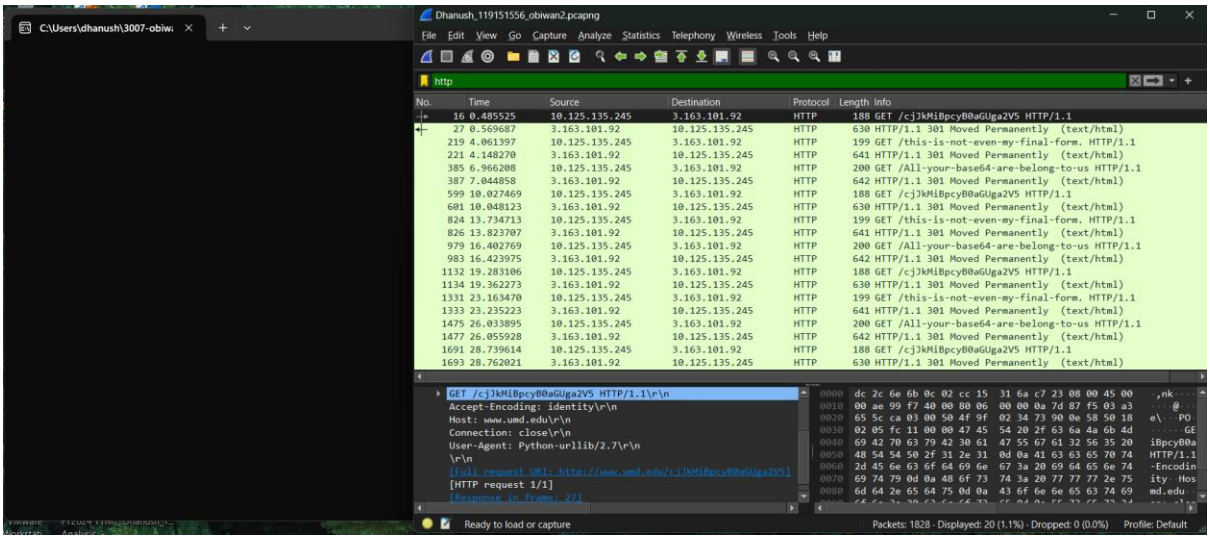
The next step would be to extract the obiwan2.exe file and we run it in a safe environment or a virtual machine,since it might be a malicious executable.

• Observing Execution: The file underwent execution within a secure environment, allowing us to closely monitor its activities and behavior.

• Analyzing with Process Explorer: Utilizing Process Explorer, we gained detailed insights into the operational aspects of "obiwan2.exe," specifically its system interactions and network requests.

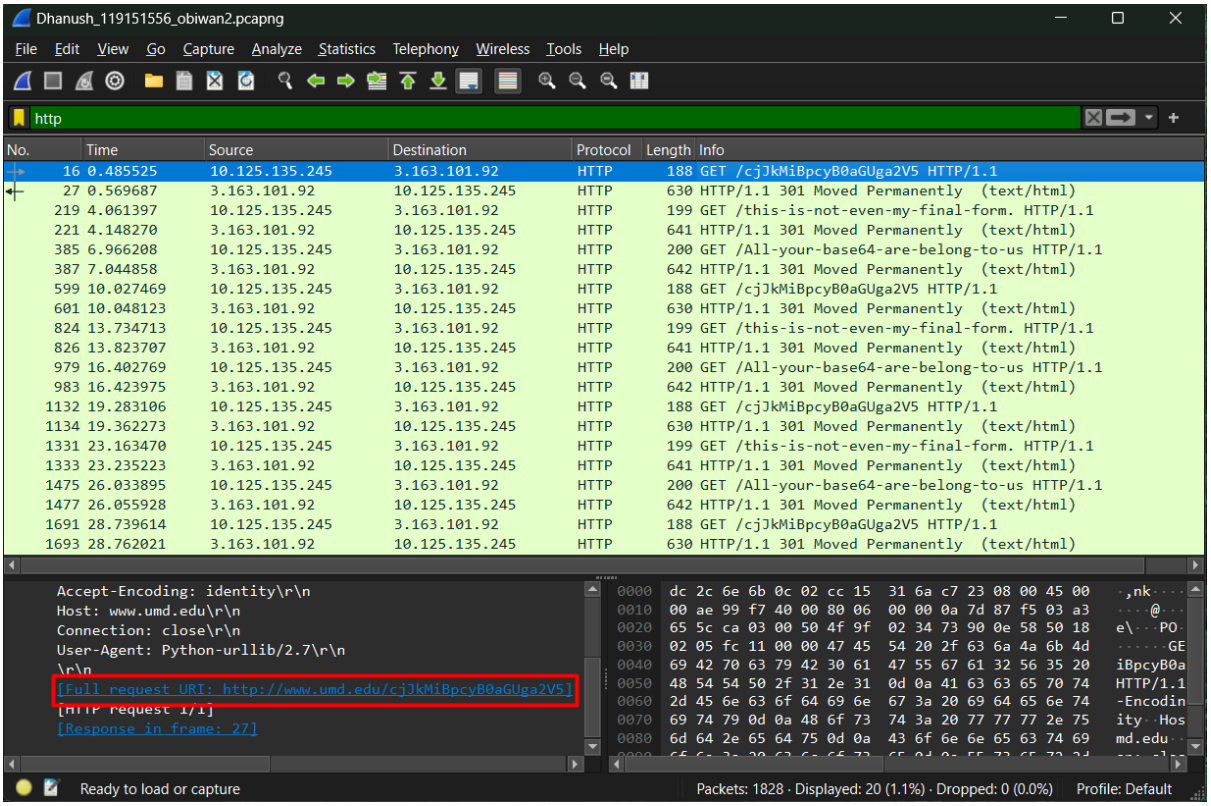
• Tracking TCP Connections: We meticulously observed the TCP connections associated with "obiwan2.exe," scrutinizing their characteristics and endpoint destinations.

ANALYSING USING WIRESHARK.



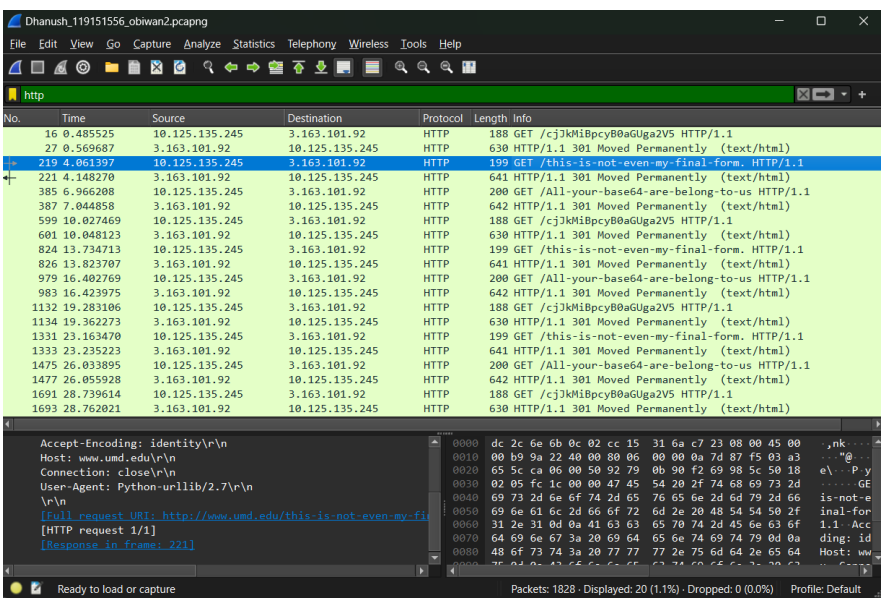
>The http request tab shows how the executable made requests to various url's to get certain data. Wireshark unveiled three distinct HTTP requests sent by the executable to the www.umd.edu server. Each request carried a unique and potentially significant payload. The initial request was addressed to http://www.umd.edu/All-your-base64-are-belong-to-us, referencing what could be a concealed or encoded message. The second request targeted http://www.umd.edu/cjJkMiBpcyB0aGUga2V5, housing a base64 encoded string that, when decoded, translates to "r2d2 is the key," indicating the potential use of an encryption key or passphrase. The final request was made to http://www.umd.edu/this-is-not-even-my-final-form, hinting at the possibility that "obiwan2.exe" might be part of a more expansive, intricate malware operation or signaling the existence of additional, yet undiscovered, components within the malware system.

>



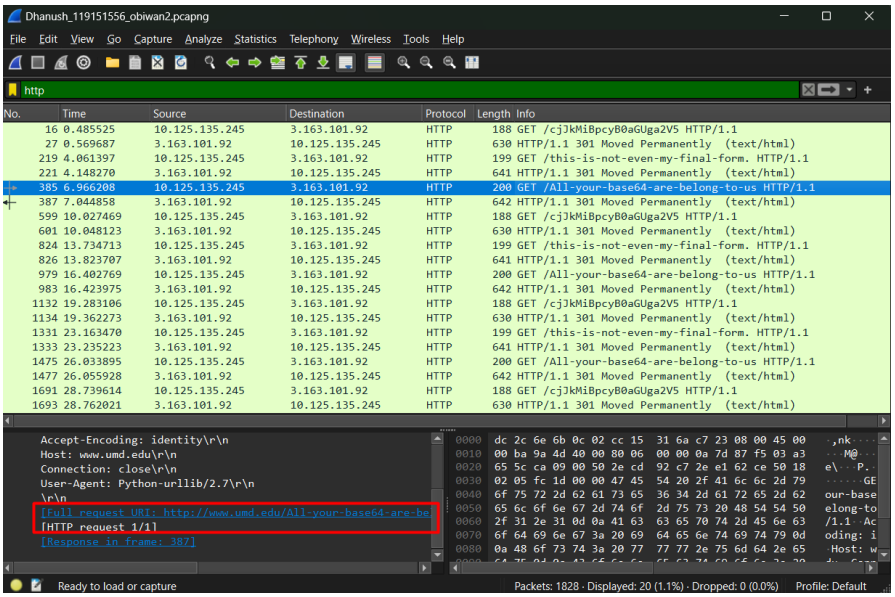
>The second url.

>



>the third url.

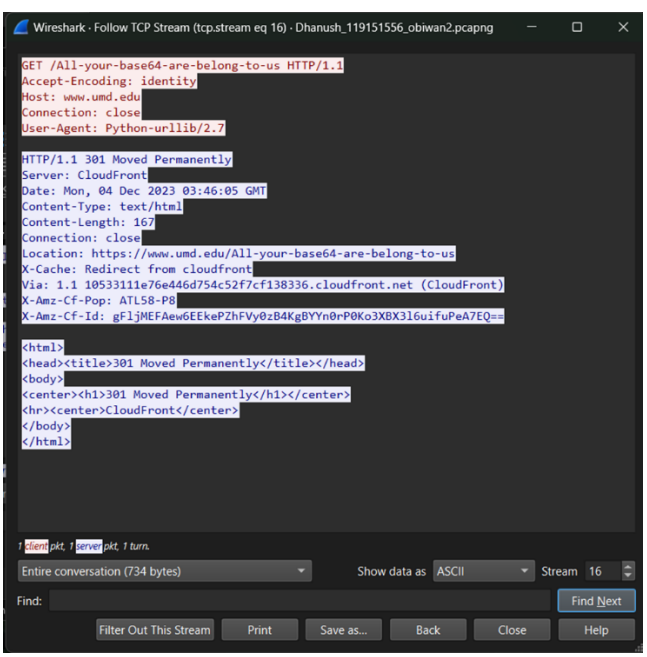
>



>The tcp stream of the requests were followed

- Examining the TCP stream related to the HTTP request made to "http://www.umd.edu/All-your-base64-are-belong-to-us" provided a comprehensive analysis. This thorough review uncovered the entire HTTP request along with the server's response, notably featuring a "301 Moved Permanently" status code, signaling a redirection.

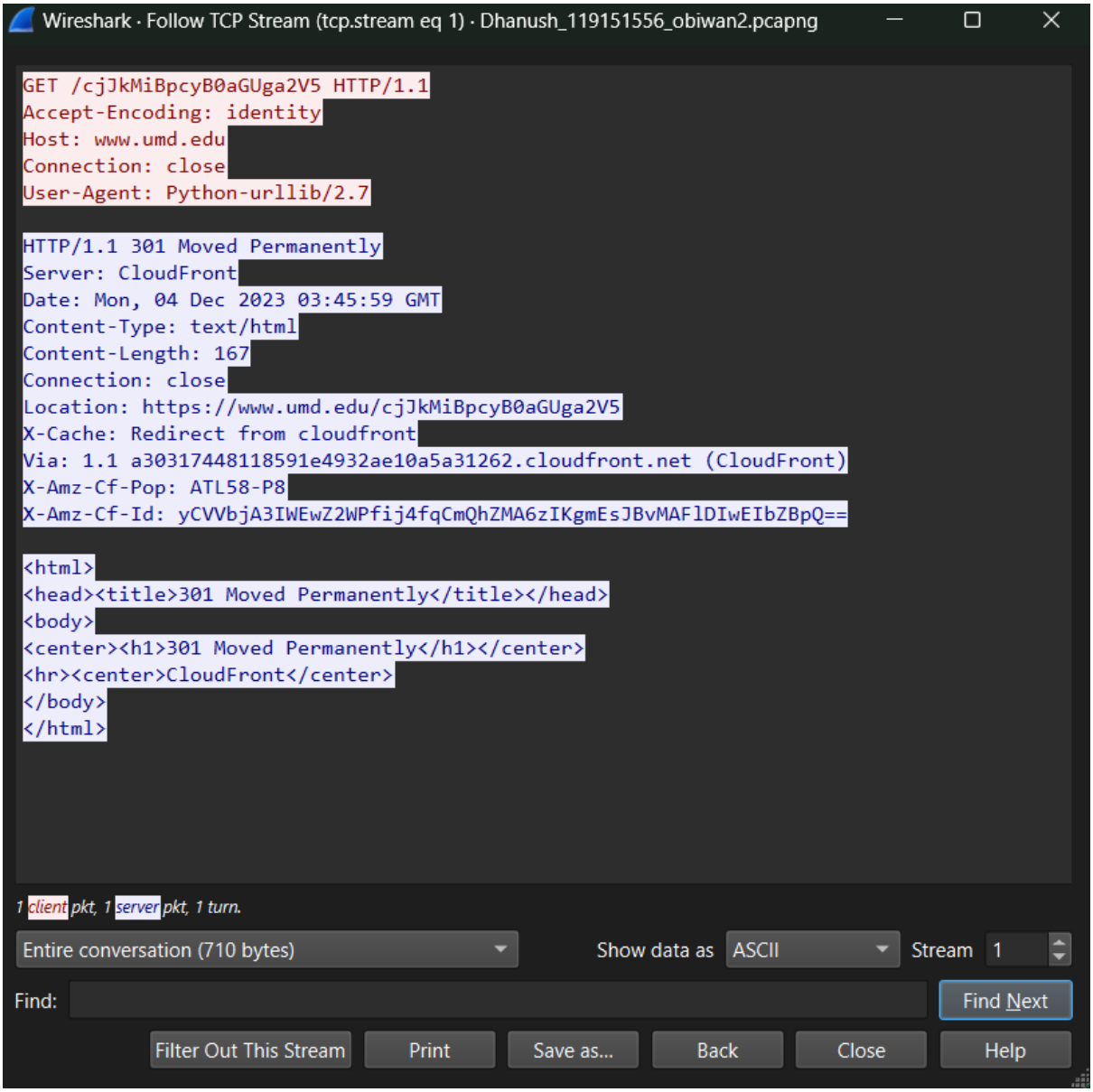
>



>The TCP stream of the second request was followed:-

- Analogous scrutiny was applied to the TCP stream linked to the request made to "http://www.umd.edu/cjJkMiBpcyB0aGUga2V5." This examination yielded crucial understandings regarding the characteristics of the second HTTP request and mirrored the server's response of redirection.

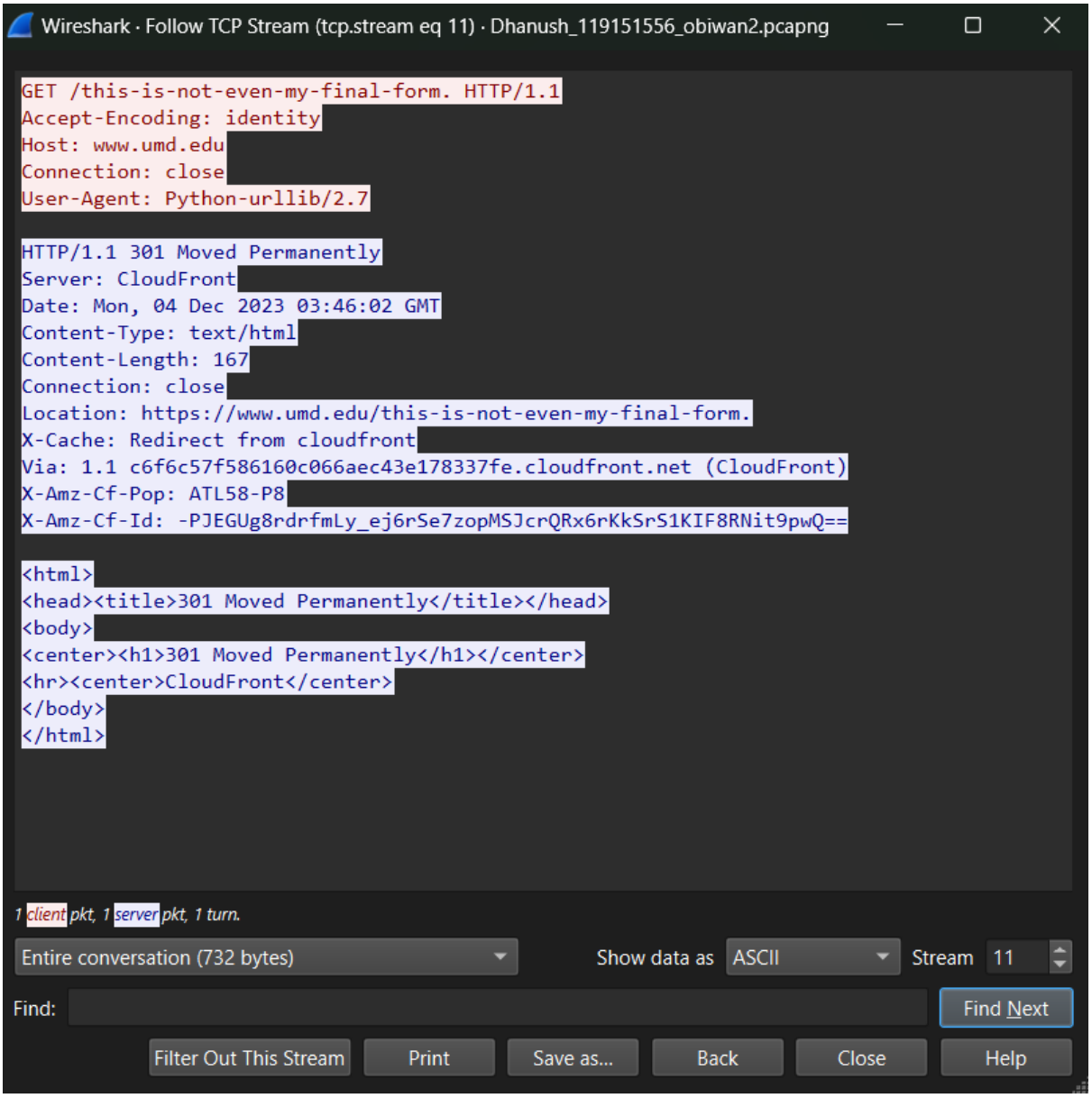
>



>The TCP stream of the third request was followed:-

- This was also similar to the last two request,it gave a 301 response after the request was sent to the particular url.

>



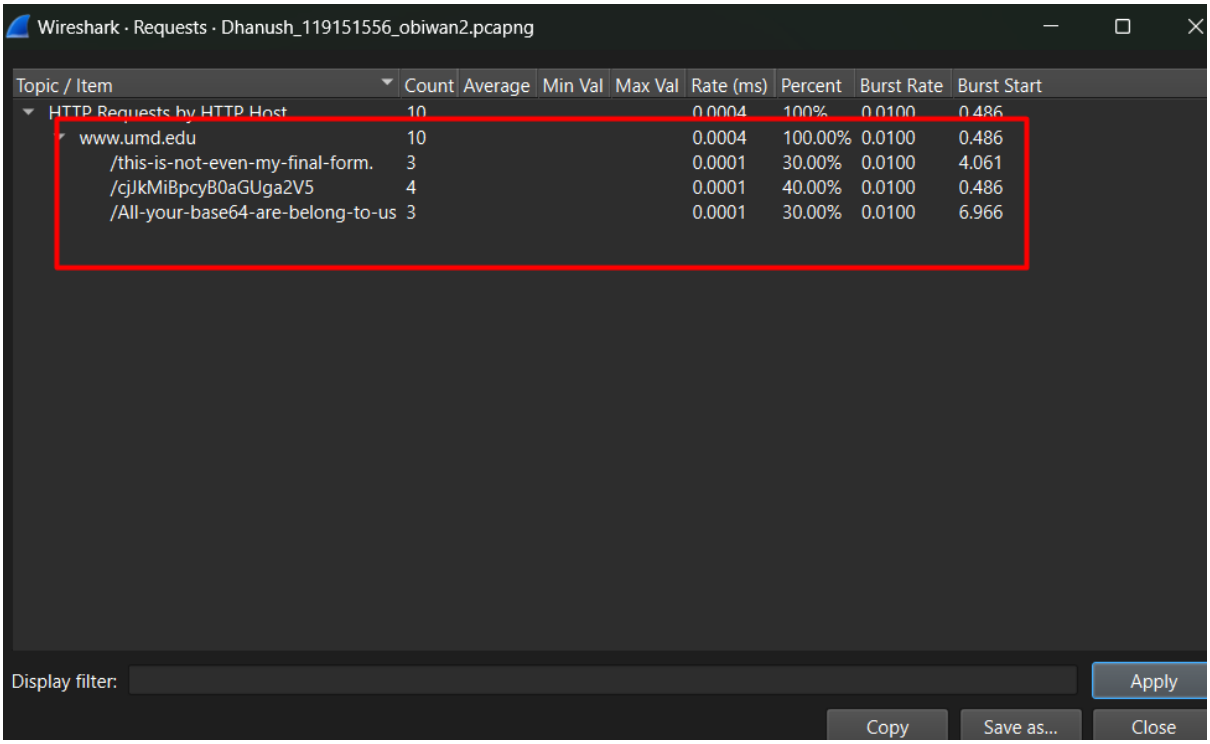
FINDINGS

> A thorough analysis of the Requests tab within Wireshark while examining "obiwan2.exe" uncovered a series of 17 HTTP requests sent to "www.umd.edu." This recurrent communication pattern implies a programmed or automated behavior inherent in "obiwan2.exe." Despite each request being directed at the same domain, they targeted distinct URLs, suggesting a deliberate

sequence of actions or message transmissions. The consistent quantity of requests and their precise targeting align with the characteristics of an executable designed for systematic communication, potentially as part of a larger coordinated operation or to execute sequential

tasks contingent on server responses. This repetitive and structured network activity highlights the sophistication and potential complexity inherent in "obiwan2.exe."

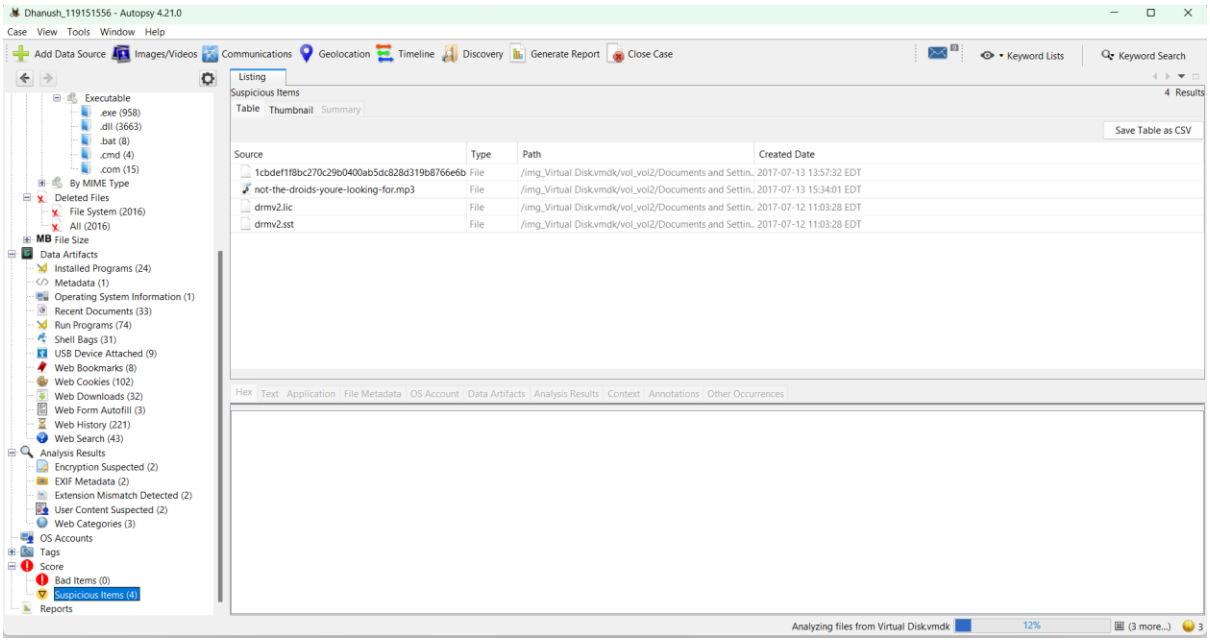
>



>While analyzing "obiwan2.exe" in Wireshark, a consistent trend emerged upon examining the Packet Counter tab. It documented a total of 9 requests dispatched to "www.umd.edu," mirrored by an equivalent count of responses received, each marked with the "301 Moved Permanently" status code.

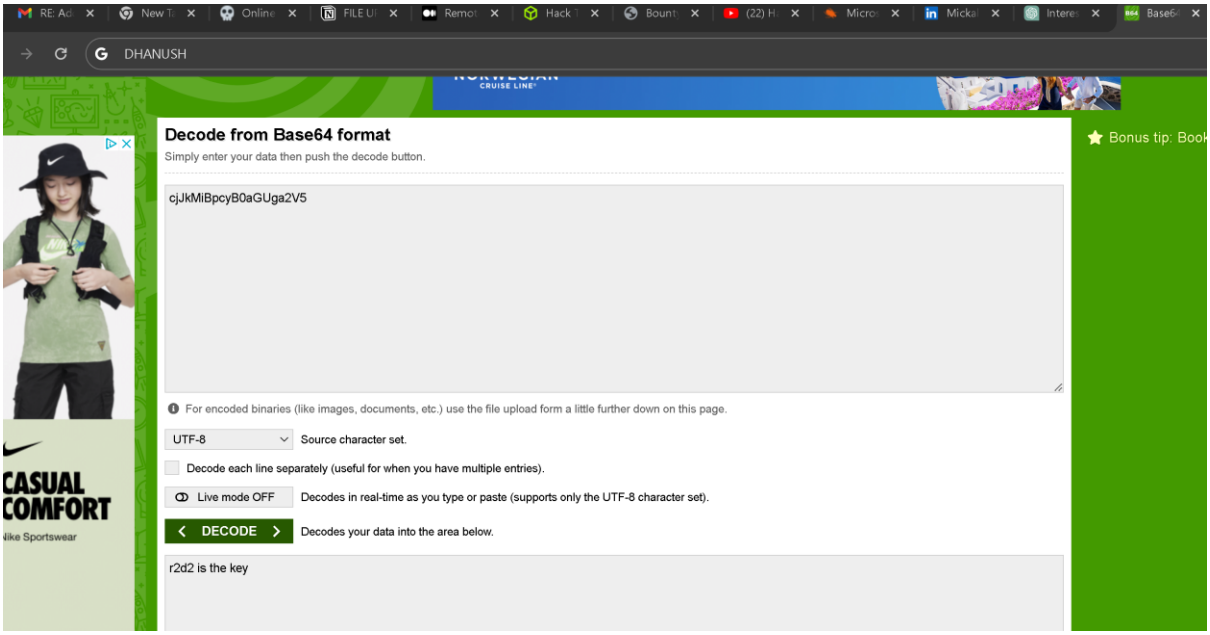
<u>Analysis of “not-the-droids-you-are-looking-for.mp3”</u>

>



> The decryption process for the encrypted MP3 file, "not-the-droids-you-are-looking-for.mp3," was pivotal. It included a critical step of decoding a base64-encoded URL path, revealing the key necessary for unlocking one of the encrypted files. After decrypting it, we obtained the phrase "r2d2 is the key." This key, derived from the analysis of "obiwan2.exe," played a vital role in decrypting the data, leveraging Veracrypt for this crucial decryption process.

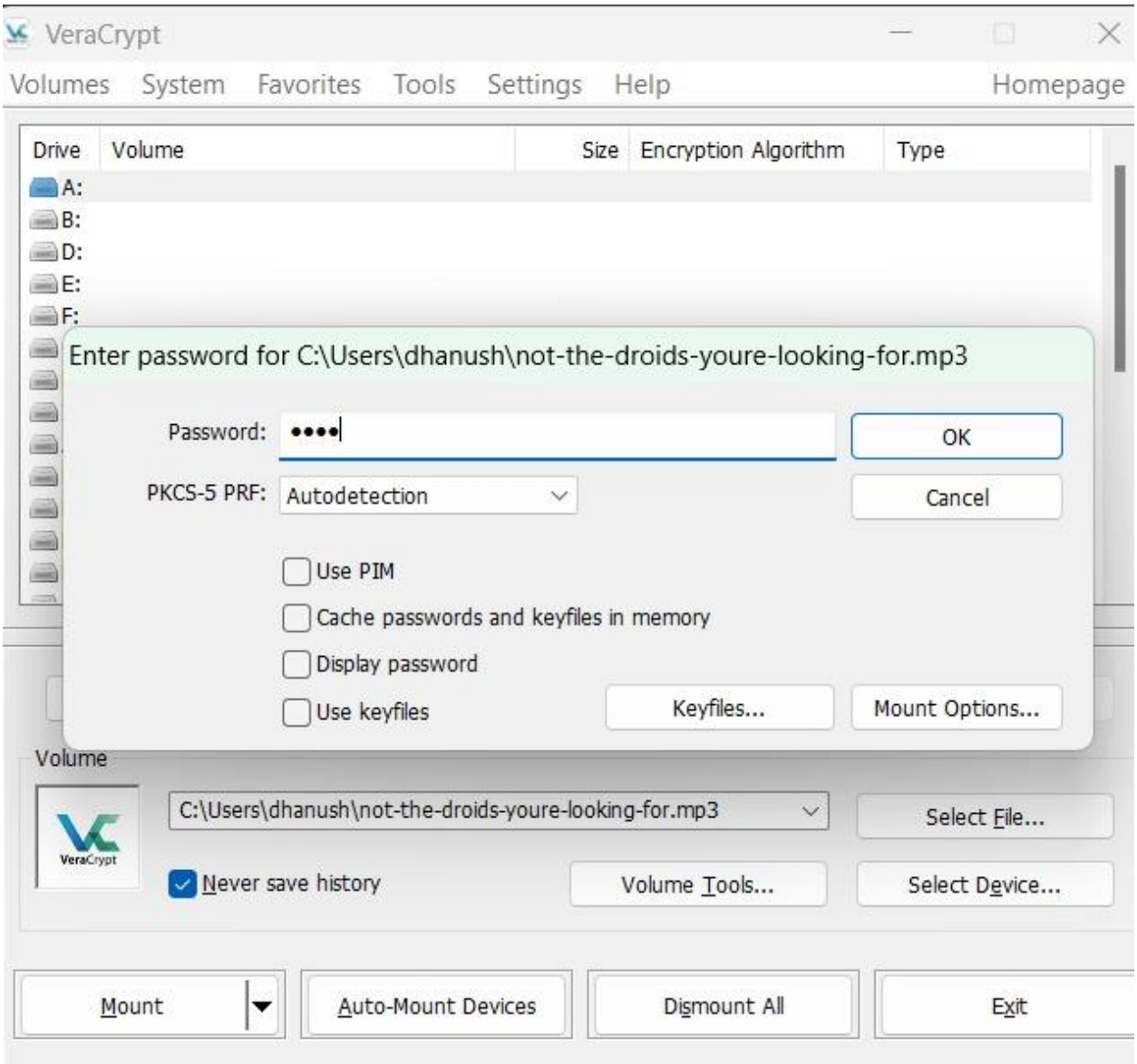
>



STEPS IN VERACRYPT

- Veracrypt Launch: The Veracrypt application was opened to initiate the decryption process.
- Selection of Encrypted Container: A specific Veracrypt volume containing the encrypted files, including "not-the-droids-you-are-looking-for.mp3," was selected.
- Mounting the Volume: The chosen Veracrypt volume was mounted, allocating a designated drive letter for access.
- Passphrase Entry: The passphrase "r2d2 is the key" was provided upon prompt by Veracrypt for decryption.
- Access to Decrypted Files: Upon successful mounting, the assigned drive letter was accessed, allowing navigation to the decrypted files within the Veracrypt volume.

>



Analysis of the MP3 File:

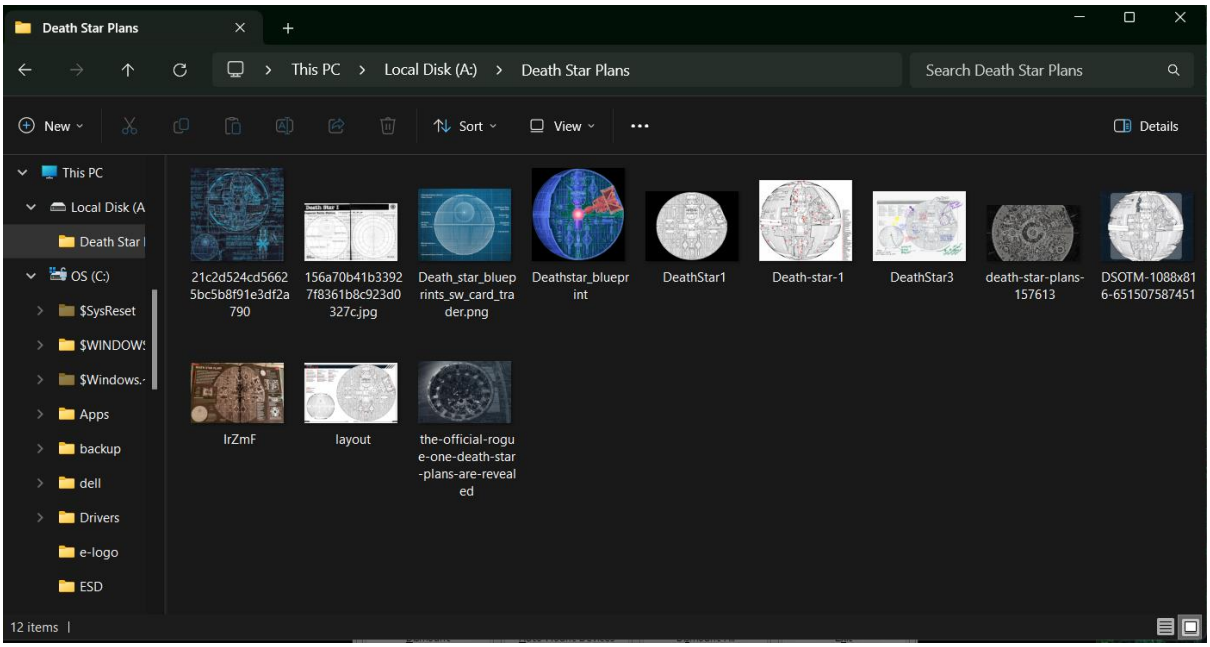
• After unlocking "not-the-droids-you-are-looking-for.mp3," an extensive review of its previously encrypted contents became feasible.

• Decrypted File Contents:

Inside the decrypted data, an enclosed directory labeled "Death Star Plans" was uncovered. It housed images and blueprints of the Death Star, hinting at the file's purpose for clandestine storage and transmission of sensitive data.

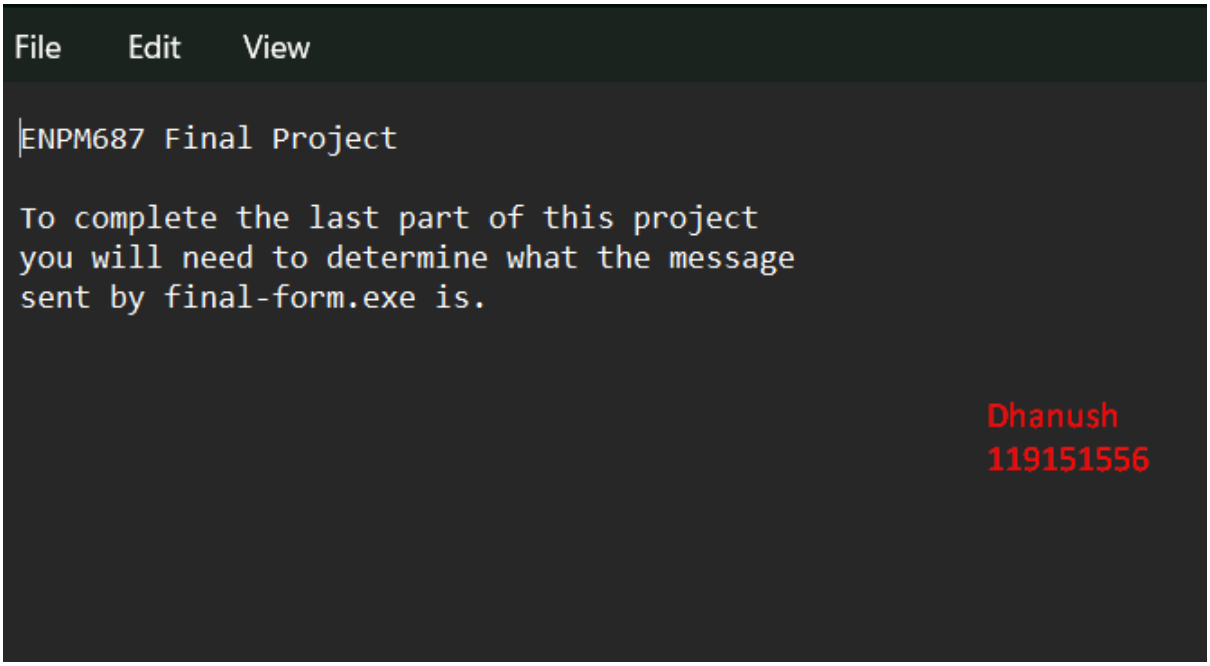
• Key Discovery: Notably, a significant finding emerged—an accompanying text document labeled “ENPM687-Read-This.txt.” This file contained explicit instructions to execute 'final-form.exe,' implying subsequent investigative steps in the ongoing examination.

>



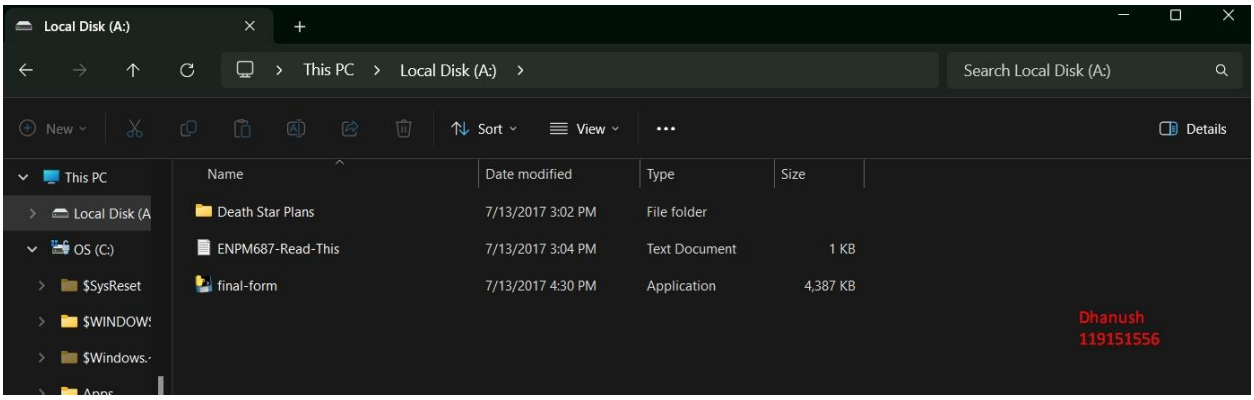
>This was the message.

>



>the final .exe file can also be found when we extract the data from the .mp3 file from veracrypt.

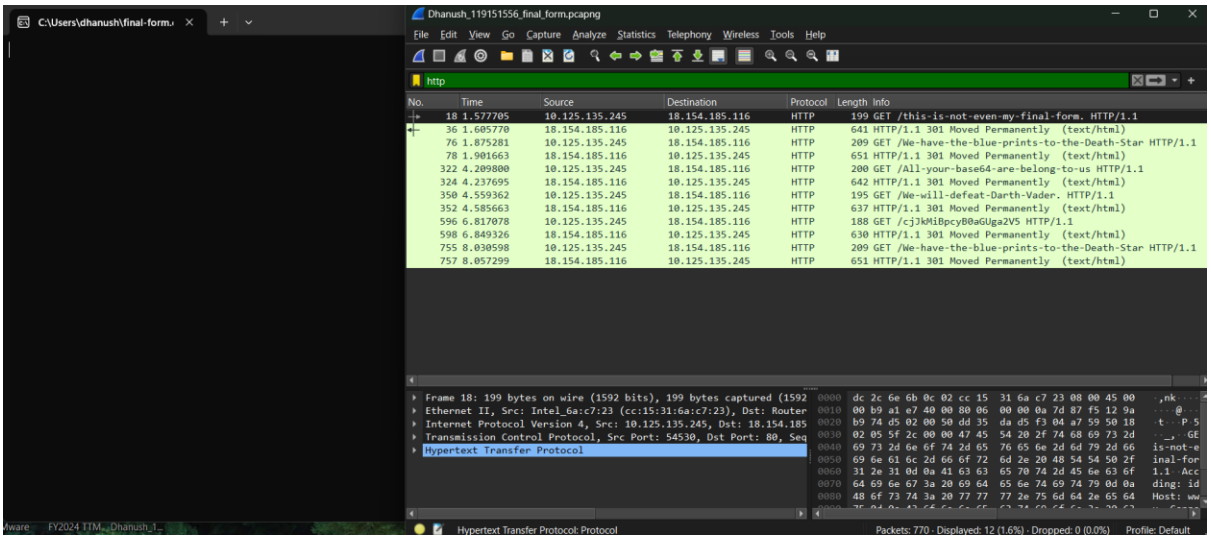
>



FINAL STEP

>we had to run the final-form.exe file on the system and check the behaviour using wireshark

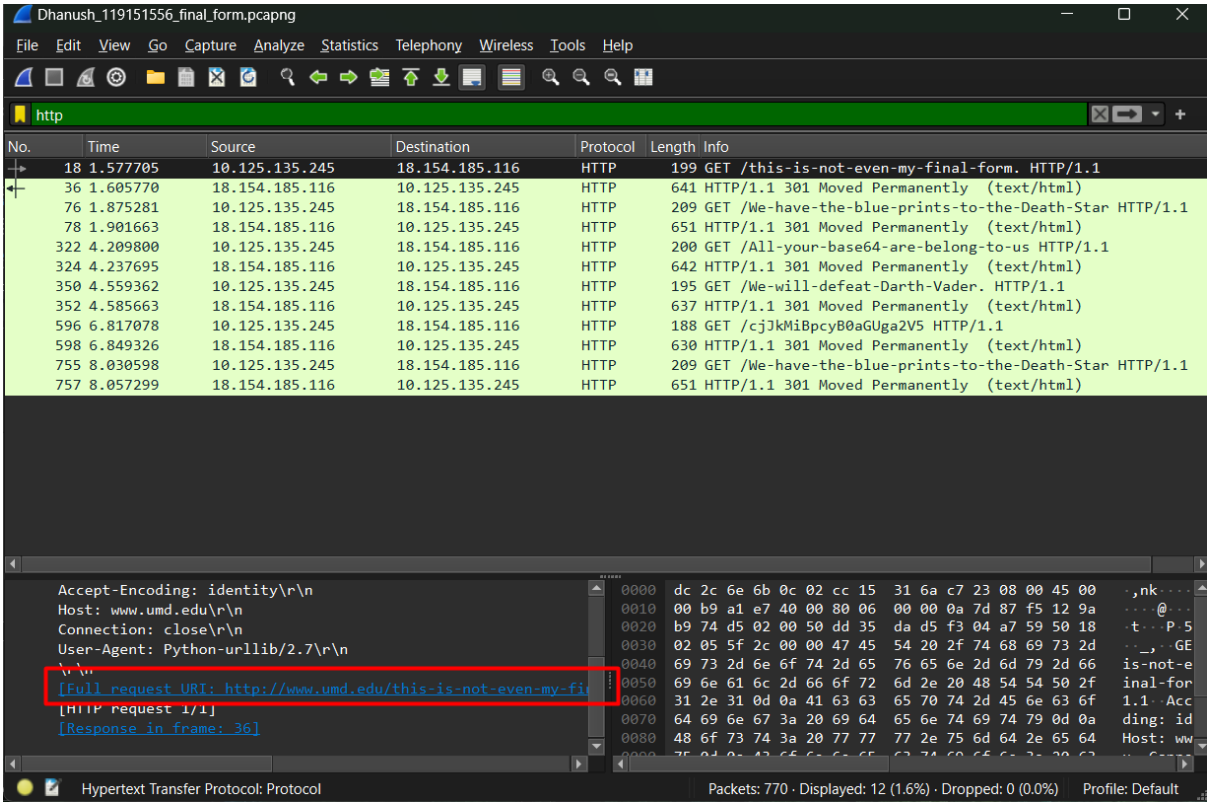
>



>• Network Packet Capture: Wireshark served to capture the network packets generated by "final-form.exe," a pivotal step in scrutinizing the transmitted and received data by the executable.

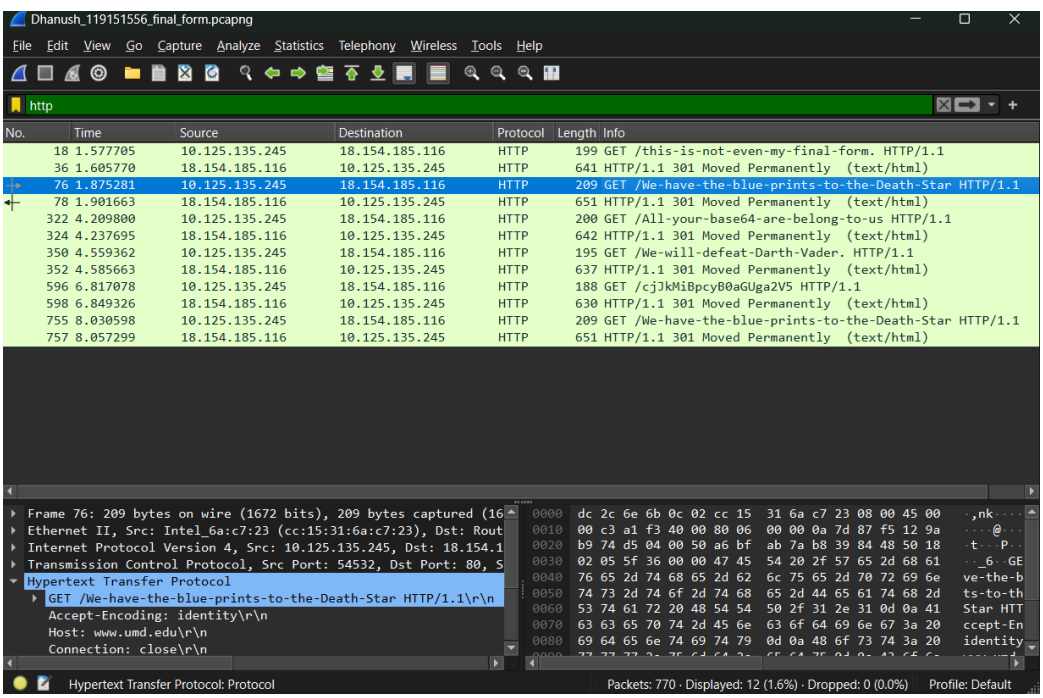
• TCP Stream Analysis - First Request: An examination of the TCP stream focused on the initial HTTP request launched by "final-form.exe" directed at the URL "http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star." This comprehensive analysis unveiled the entire HTTP request and response cycle, including the server's "301 Moved Permanently" status code.

• TCP Stream Analysis - Second Request: Similarly, scrutiny of the TCP stream was applied to the second HTTP request to "http://www.umd.edu/We-will-defeat-Darth-Vader." This investigation provided insights into the nature of the second HTTP request and mirrored the server's identical response.



>the second request

>



• The scrutiny of HTTP requests revealed the targeted URLs by "final-form.exe" on the "www.umd.edu" server, specifically "http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star" and "http://www.umd.edu/We-will-defeat-Darth-Vader." This discernible pattern in the executable's network communication potentially signifies its objectives or operational strategies.

RESPONSE

Notably, the server's consistent response to these requests comprised the "301 Moved Permanently" status code, indicating the permanent relocation of requested resources. This redirection technique in web communications might signify an attempt to obfuscate the communication's true nature or redirect to alternative resources.

Efforts were undertaken to extract objects from these requests to delve deeper into their examination. Regrettably, this endeavor didn't produce substantial findings owing to persistent redirection, causing complications in retrieving more detailed information about the requests.

NEXT STEPS

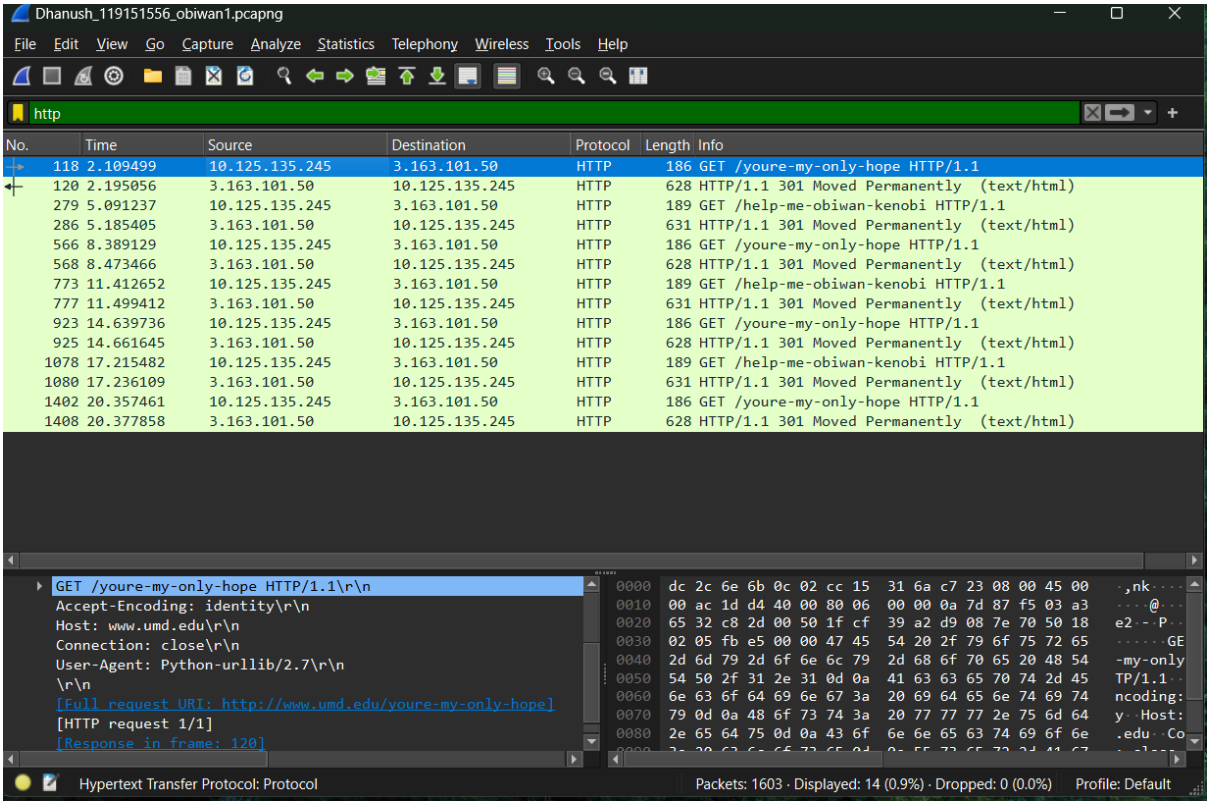
Proposed Steps for Further Investigation

- Use advanced tools (like disassemblers and debuggers) to fully understand the capabilities of "obiwan.exe" and "obiwan2.exe," uncovering any hidden functions.Analyze "final-form.exe" similarly to understand its broader role and potential impact.
- Investigate the "www.umd.edu" server to understand the resources accessed by the executables. Determine if these are controlled or external servers.Collaborate with server admins or authorities for additional request logs and information.
- Scrutinize the contents in the “Death Star Plans” folder and the "ENPM687-Read-This.txt" file for hidden messages or clues.
- Strengthen network security by updating firewalls, intrusion detection systems, and adopting advanced threat protection solutions.

OTHER FINDINGS

>We also find the **obiwan.exe** with the obiwan2.exe file as you can see in the first screenshot on top.We run the .exe file and see the behaviour of the executable using wireshark.

>



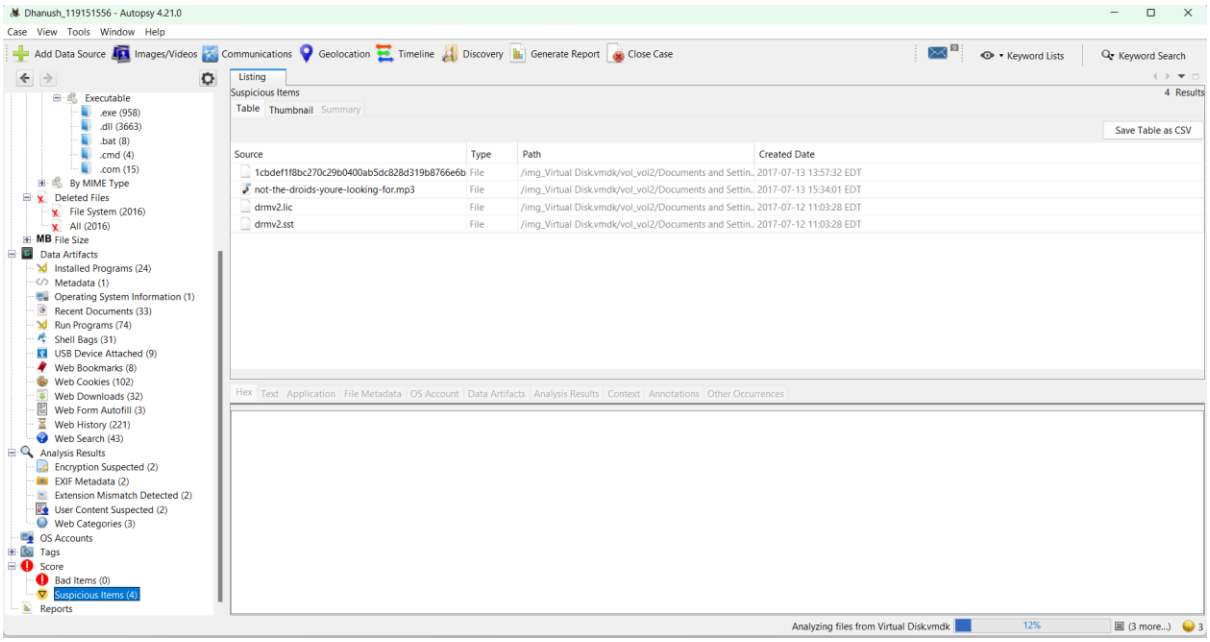
>There are two URL's it visits

- /youre-my-only-hope
- /Help-me-obiwan-kenobi

>They both give out a 301 response(moved permentaly).There were a totoal of 9 request made after running the executable.The request was made to www.umd.edu. With the ablove paths mentioned.

I also found other suspicious files using autopsy

>

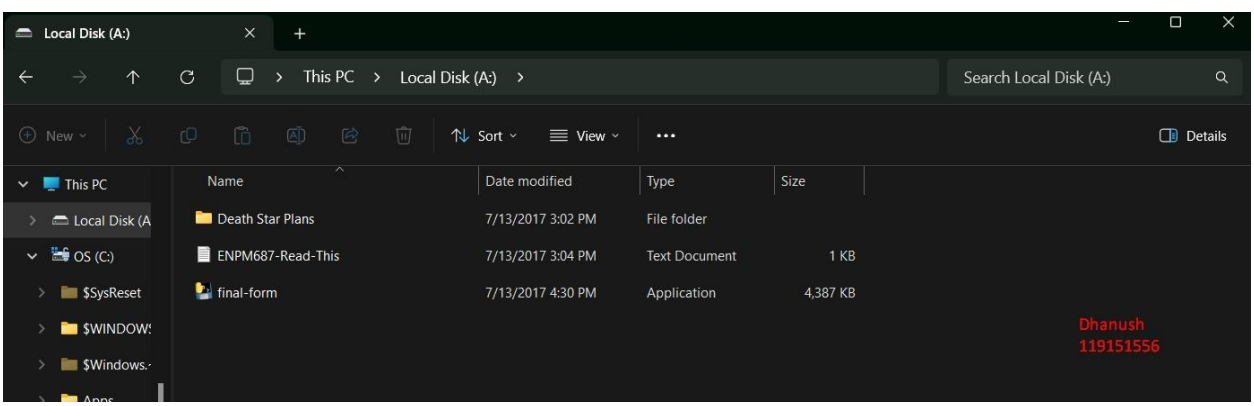


- drmv2.lic
- drmv2.sst

1 - Find the final version of the malware writer's malware

Ans:-the final version of the writers malware is

>

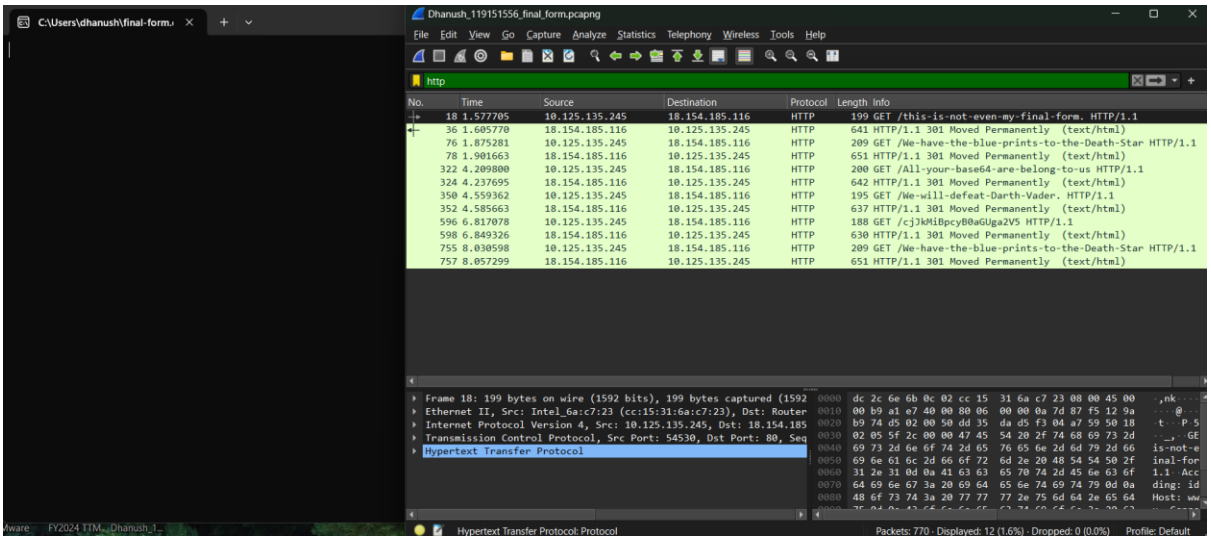


>final-form.exe

2 - Determine what the message contained inside of the final malware is

Ans:-the final message is

>



>we-have-the-blue-prints-to-the-death-star

>we-will-defeat-darth-vedar

3 - Find some other interesting items/artifacts/clues that are definitely **'relevant'** to the investigation that will aide the Imperial Forces. Include these in your report in order to get full credit.

>Other relavent findings are mentioned in the report.

4. - Describe two challenges or difficulties you had to overcome to complete the final project.

Ans:-the two challenges were

>Figuring out one of the path in the GET request sent when we executed obiwan2.exe was a base64 encoded password for the encrypted .mp3 disk.

>Also figuring out in such large amount of files present in the disk.Which files are the ones that stand out as suspicious.There might have been a possibility of false positives as well.