ENPM687-CY01 Final

Jayraj A. Vakil

UID: 119188361

Brief Summary of Information

During forensic analysis, two suspicious executables, obiwan.exe and obiwan2.exe, were found. Obiwan2.exe contained a decoded "r2d2" message. Decrypting "not-the-droids-youre-looking-for.mp3" using VeraCrypt revealed Death Star plans. Running "Final-form.exe" displayed messages about Death Star blueprints and defeating Darth Vader, concluding the investigation.

Tools used in the investigation

Autopsy: Autopsy is a widely used open-source digital forensics platform that assists in the analysis of digital media. It provides a graphical interface for examining file systems, recovering data, and uncovering evidence in a forensic investigation.

Wireshark: Wireshark is a network packet analyzer that allows for the capture and inspection of network traffic. It is used to monitor and analyze data packets transmitted over a network, making it valuable for understanding network activities during forensic investigations.

VeraCrypt: VeraCrypt is an open-source disk encryption software that provides strong data protection by encrypting entire disk volumes. In this investigation, it was used to decrypt an encrypted VeraCrypt volume, revealing its contents.

Base64 decoder: It is used to decode base64 text to plain text.

Repository

A. Summary of Evidence

The forensic analysis of a Windows XP virtual machine revealed two suspicious executable files, "obiwan.exe" and "obiwan2.exe," which made outbound connections to unique URLs. Decoding a base64-encoded string from one of the URLs uncovered the password 'r2d2.' Subsequent investigation in the Autopsy software identified an encrypted VeraCrypt volume and an MP3 file. Using the 'r2d2' password, the VeraCrypt volume was decrypted, revealing a text message, an executable file, and a folder named 'Death Star Plans' containing images and plans. The executable, when run, connected to websites related to defeating 'Darth Vader' and obtaining Death Star blueprints.

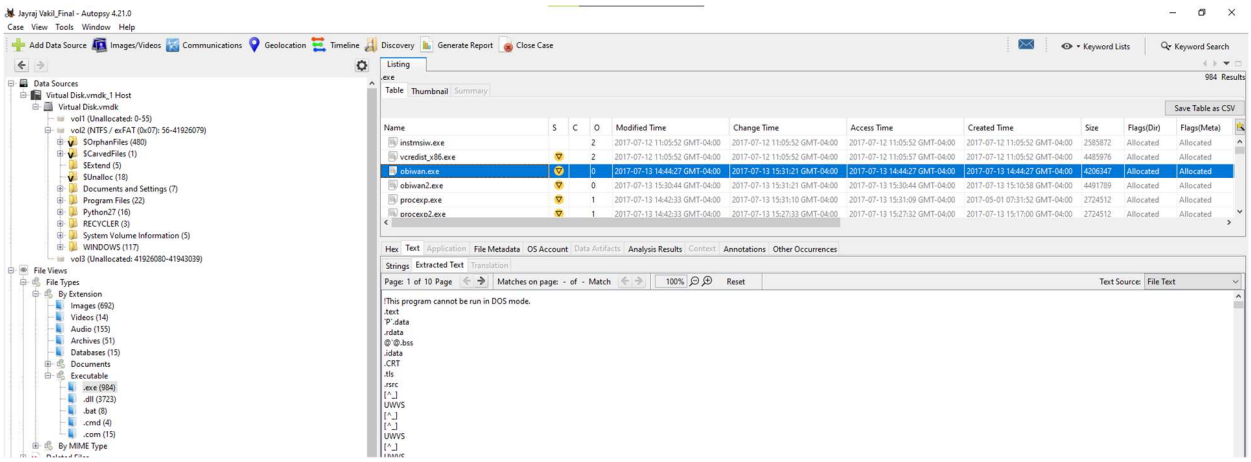
B. Analysis

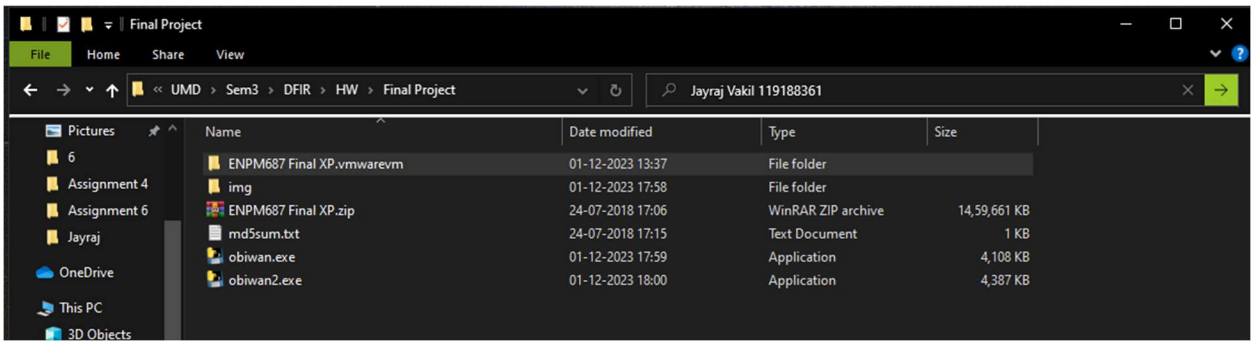
Upon loading the drive image into the Autopsy software, a comprehensive analysis of the data ensued. Given that the virtual machine in question operated on a Windows

XP platform, the initial suspicion was directed towards the possibility of malicious software manifesting as executable files. In accordance with this hypothesis, a search was conducted for files with the .exe extension, which resulted in the discovery of two distinctive files named "obiwan.exe" and "obiwan2.exe". The obiwan.exe is found at the location /img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code/dist/obiwan.exe

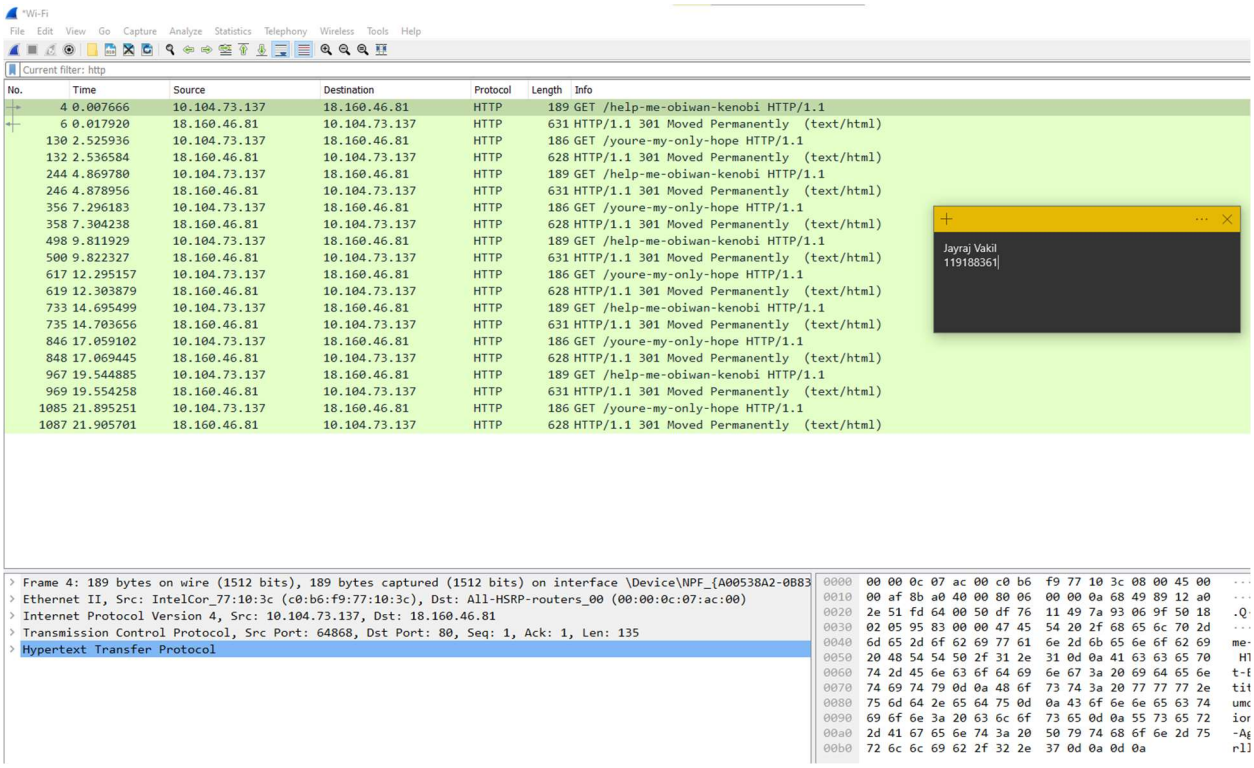
Obiwan2.exe is found at the location /img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code/dist/obiwan2.exe

The uniqueness of these file names raised intrigue, prompting their extraction to the local system for further examination.



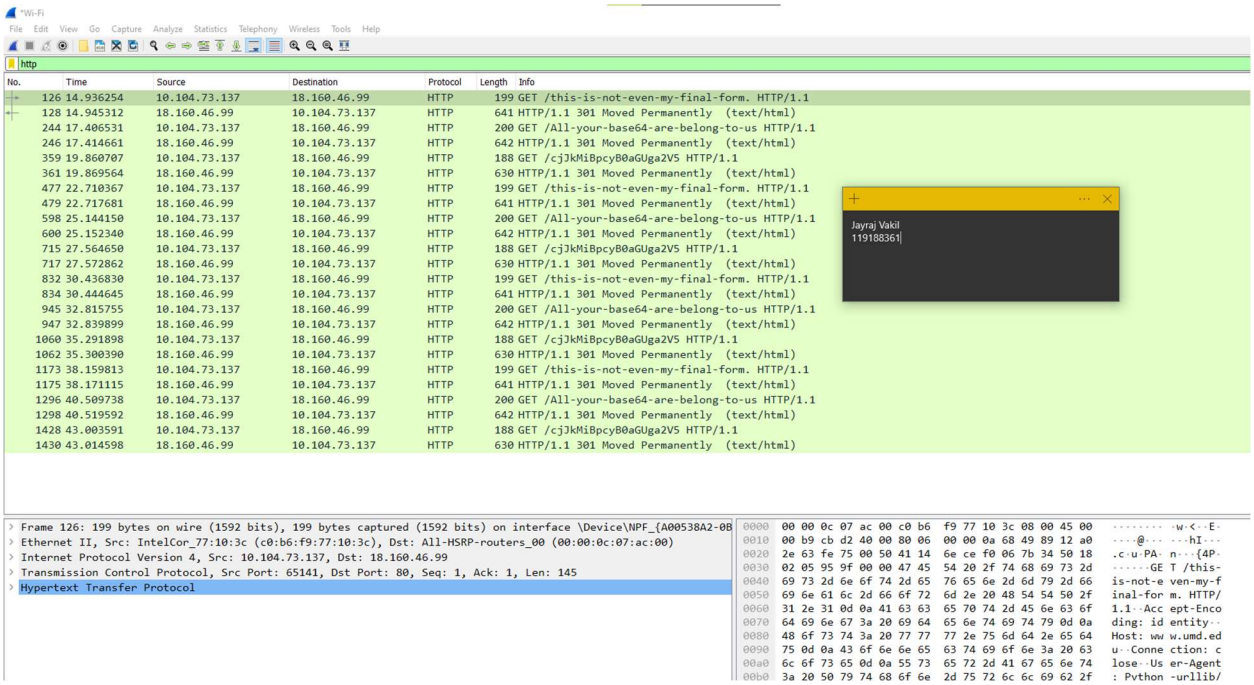


Subsequently, both executables underwent execution, with a focus on monitoring their network activities through Wireshark. This network traffic assessment revealed that both executables were making outbound connections to specific websites. "Obiwan.exe" was observed to be reaching out to the following URLs:
http://www.umd.edu/help-me-obiwan-kenobi
http://www.umd.edu/youre-my-only-hope

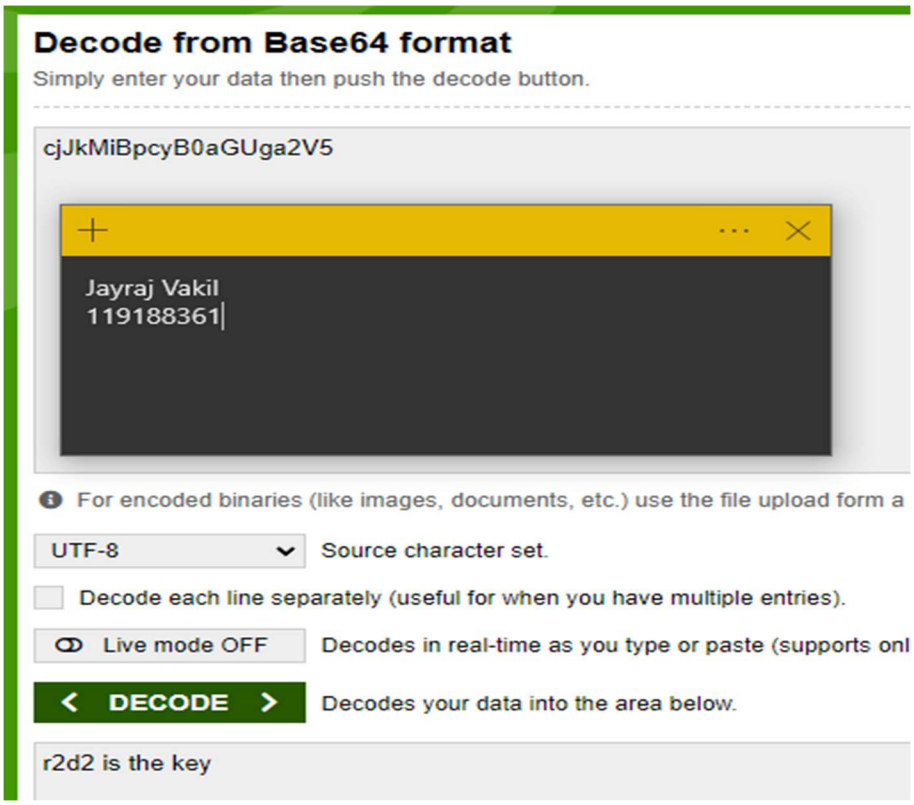


Meanwhile, "Obiwan2.exe" initiated connections to the following websites:
http://www.umd.edu/this-is-not-even-my-final-form
http://www.umd.edu/All-your-base64-are-belong-to-us
http://www.umd.edu/cjJkMiBpcyB0aGUga2V5

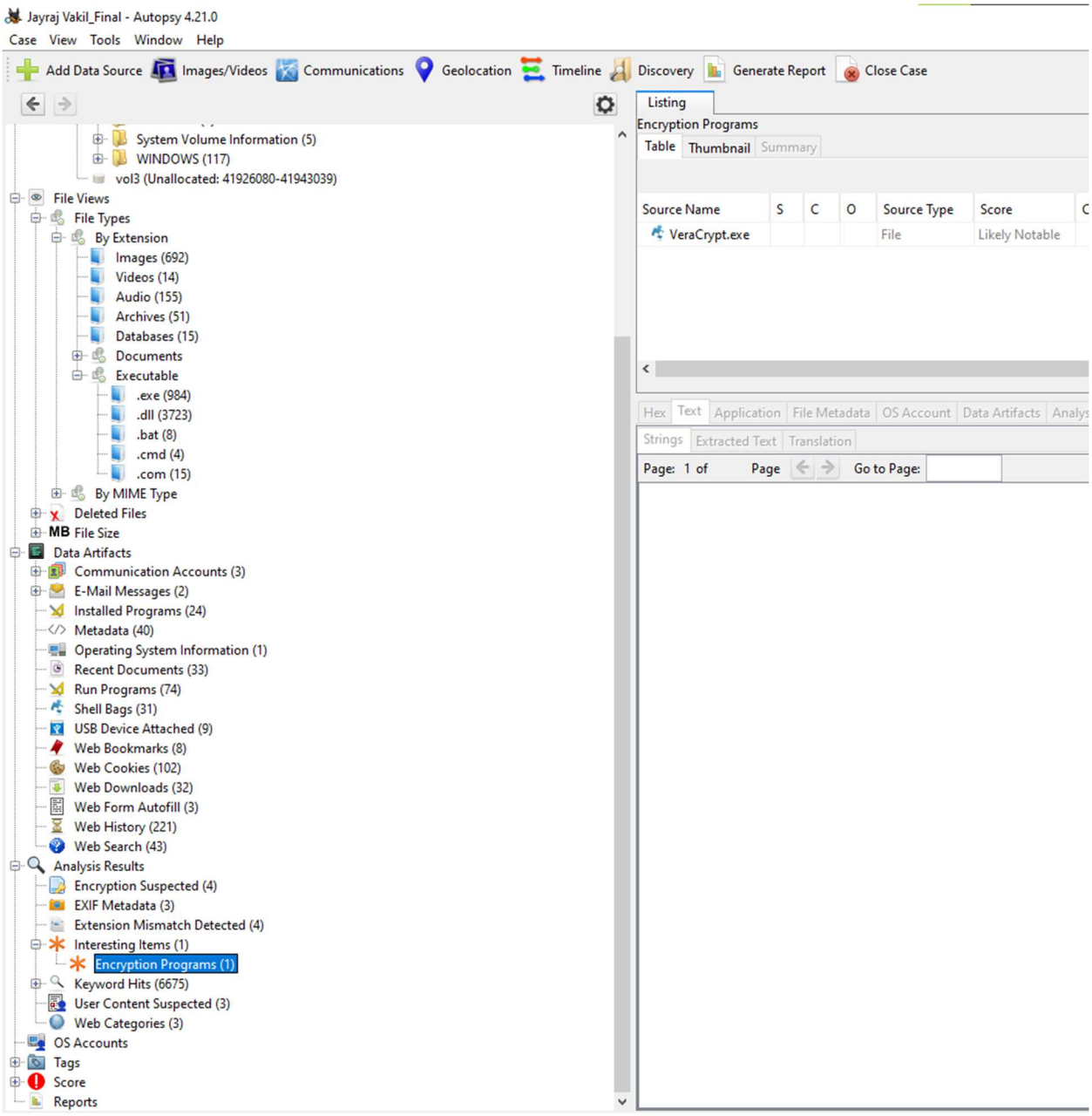
The peculiar nature of "Obiwan2.exe," particularly its attempt to communicate with a website featuring an encoded string in the URL, raised suspicions. Notably, the second URL contained the term "base64," hinting at the possibility of base64 encoding. Furthermore, the first URL's reference to "not even my final form" suggested that the third URL might provide additional clues.



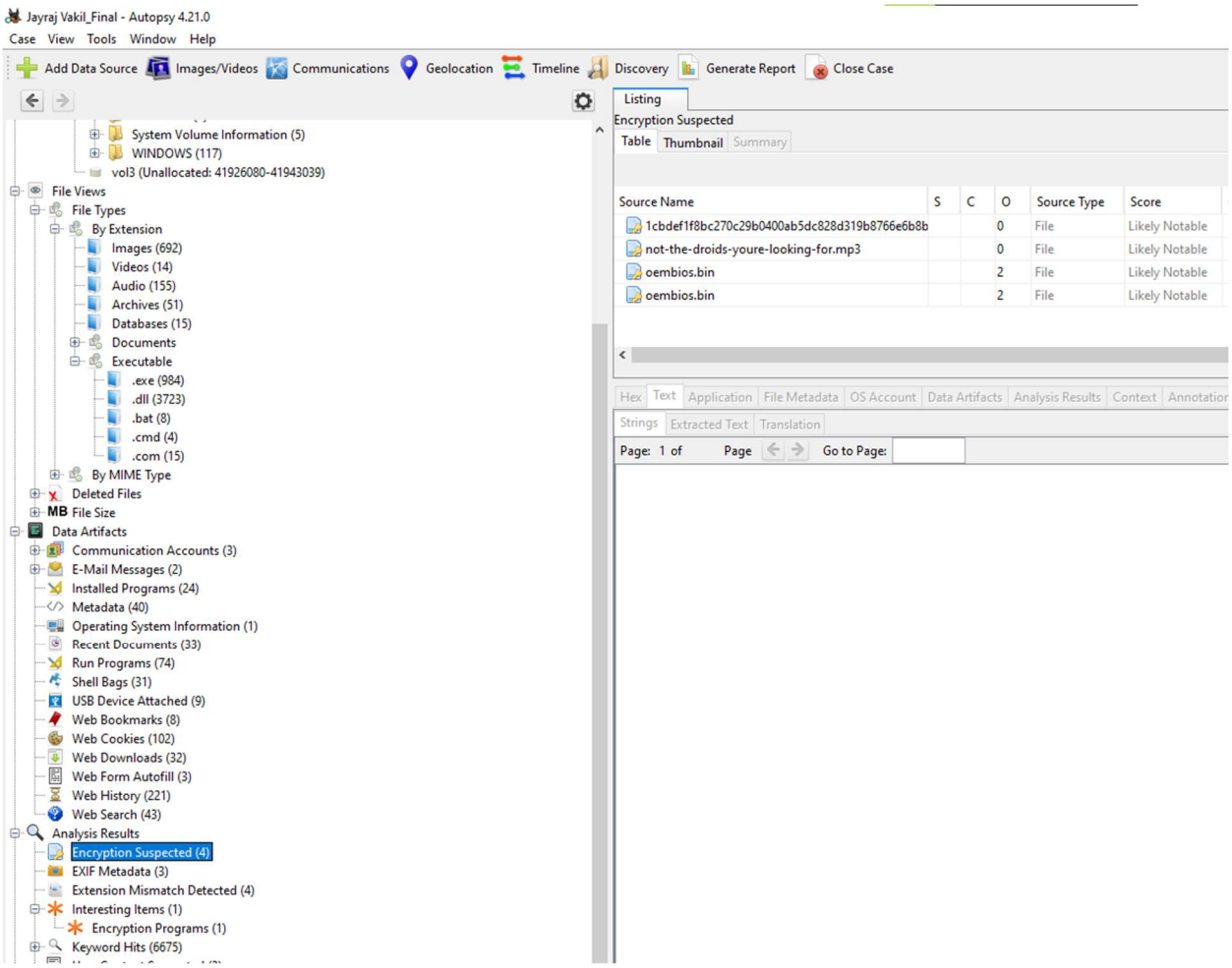
Upon decoding the base64-encoded string, the message "r2d2 is the key" was revealed, confirming the encoding method.



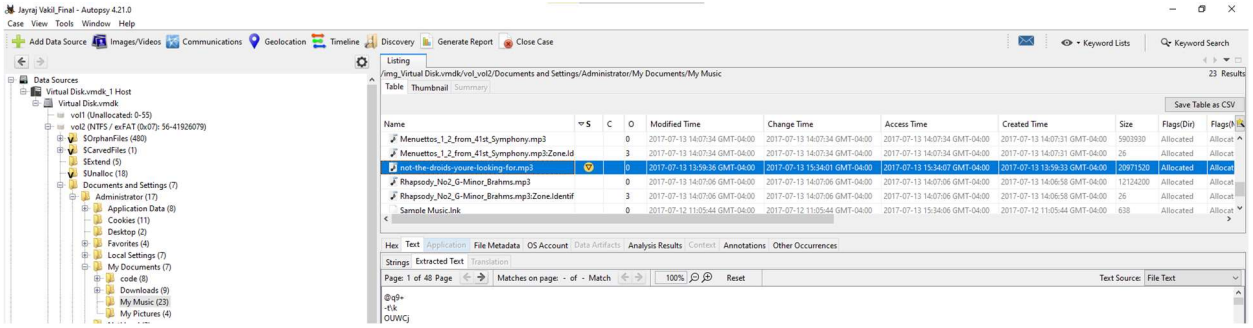
Within the Autopsy interface, an intriguing section labeled 'Interesting Items' under 'Analysis Results' piqued curiosity. Further exploration yielded a subentry titled 'Encryption Programs,' wherein the program 'VeraCrypt' was identified.

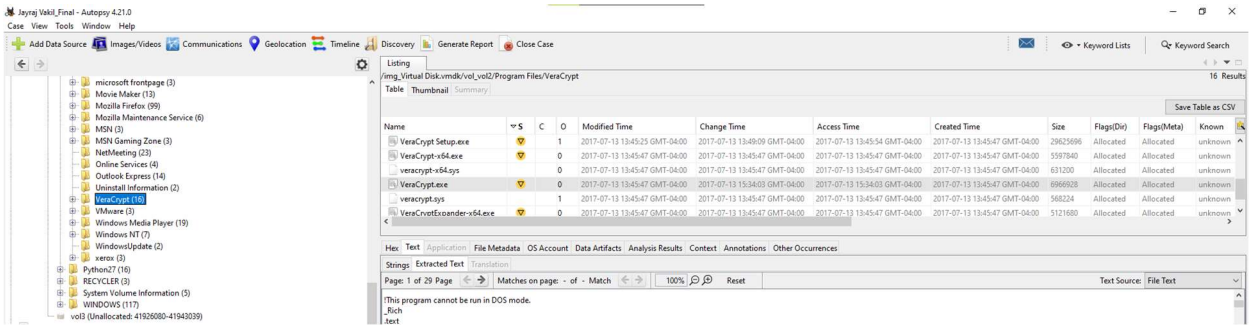


Furthermore, the 'Analysis Results' section contained an entry labeled 'Encryption Suspected' with four associated results. One of these results pertained to an MP3 file named 'not-the-droids-youre-looking-for.mp3'.

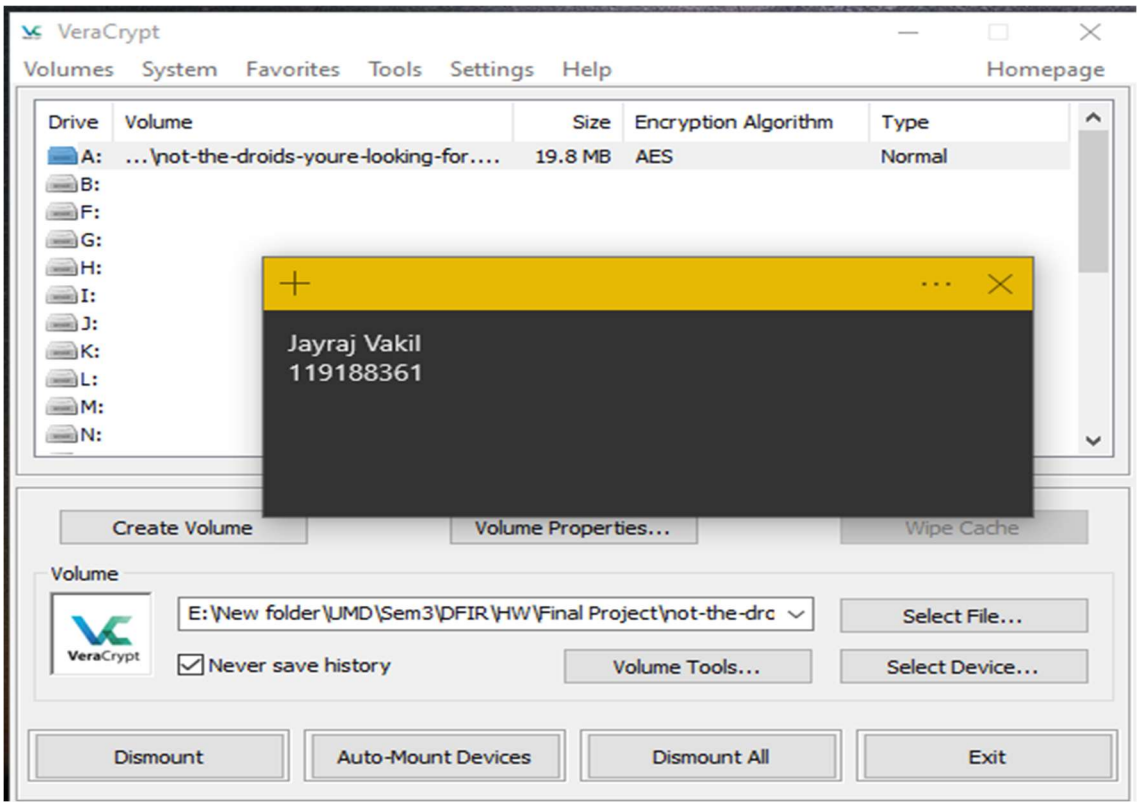


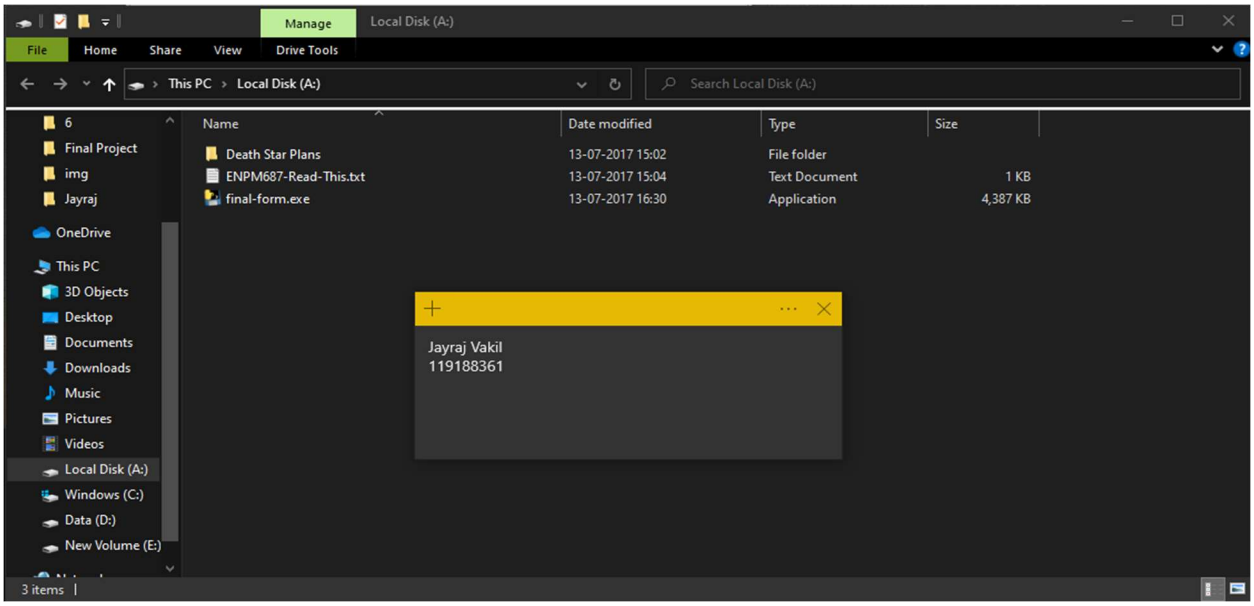
Subsequently, both the MP3 file and the VeraCrypt program were extracted and transferred to the local system for in-depth analysis. The MP3 file's location was identified as '/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/My Music/not-the-droids-youre-looking-for.mp3', while the VeraCrypt program resided at '/img_Virtual Disk.vmdk/vol_vol2/Program Files/VeraCrypt'



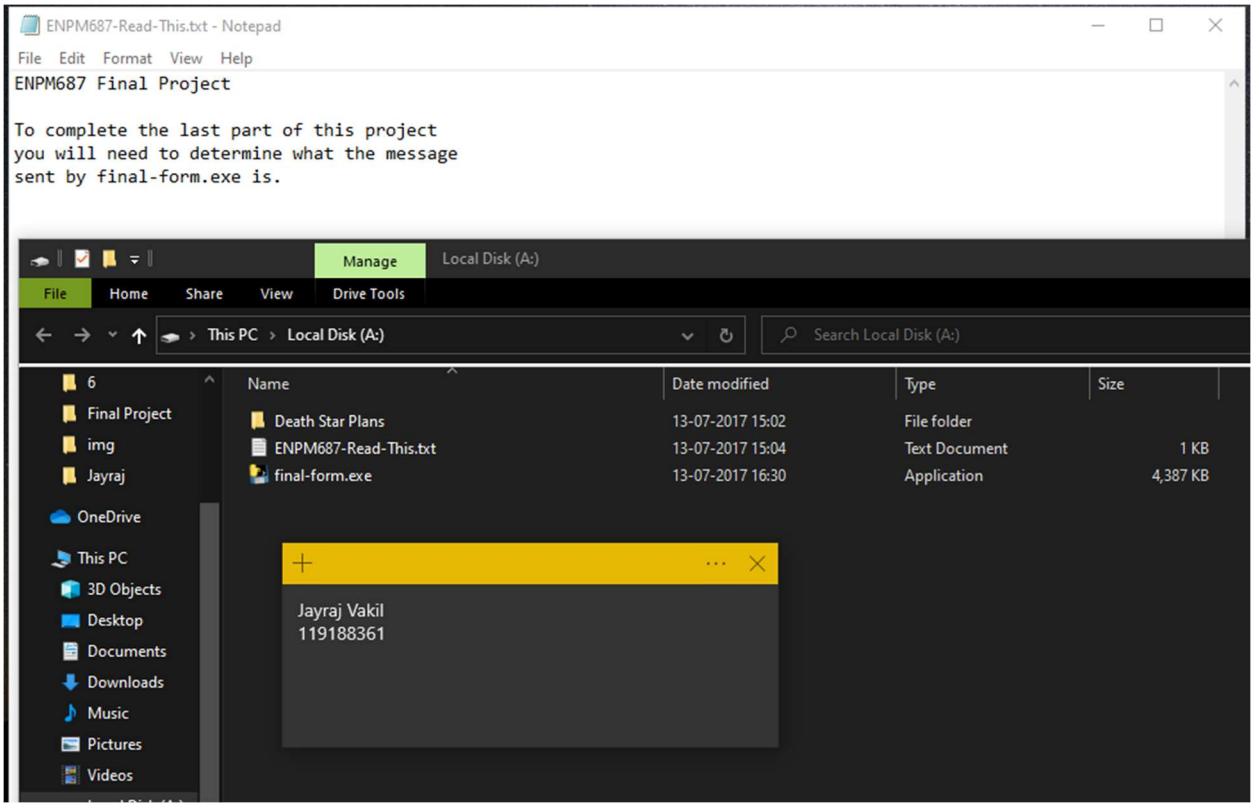


Upon executing the VeraCrypt program and providing the 'r2d2' password obtained from the base64 decoding, the drive was successfully decrypted. Within the decrypted volume, two files (a text file and an executable) and one folder were discovered.





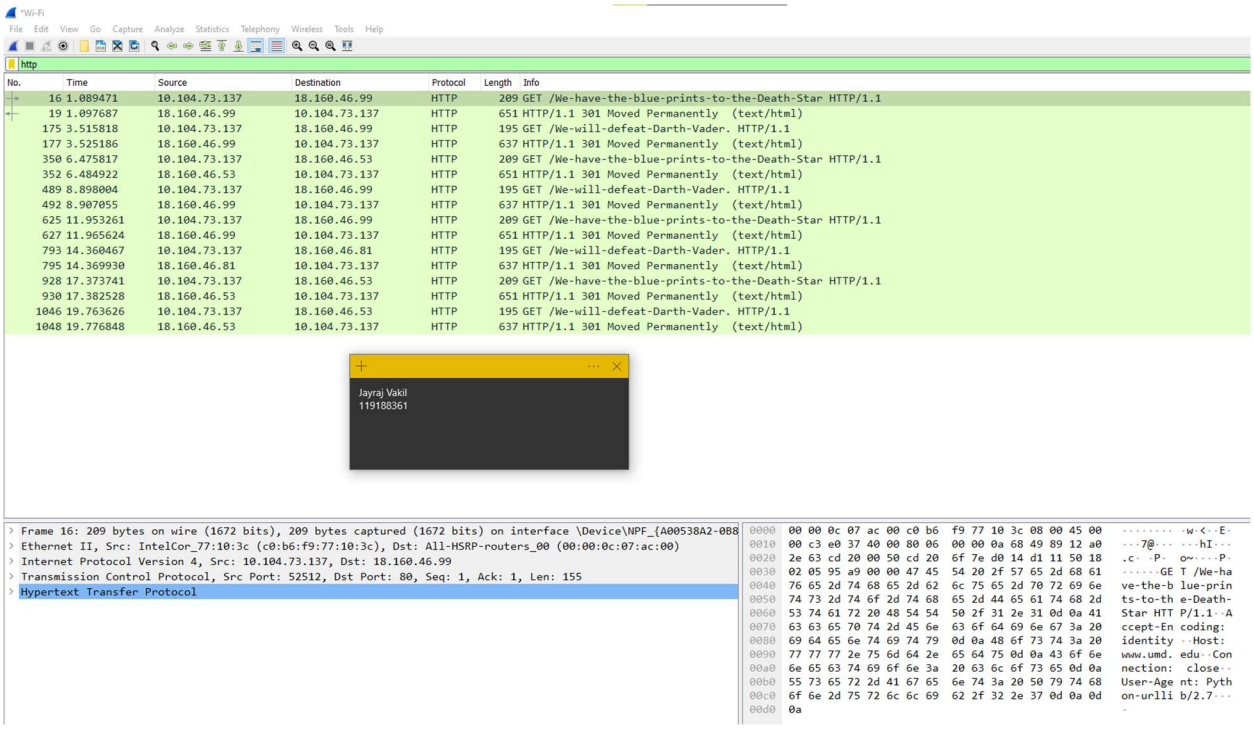
The text file contained a message, the contents of which are provided in the accompanying image.



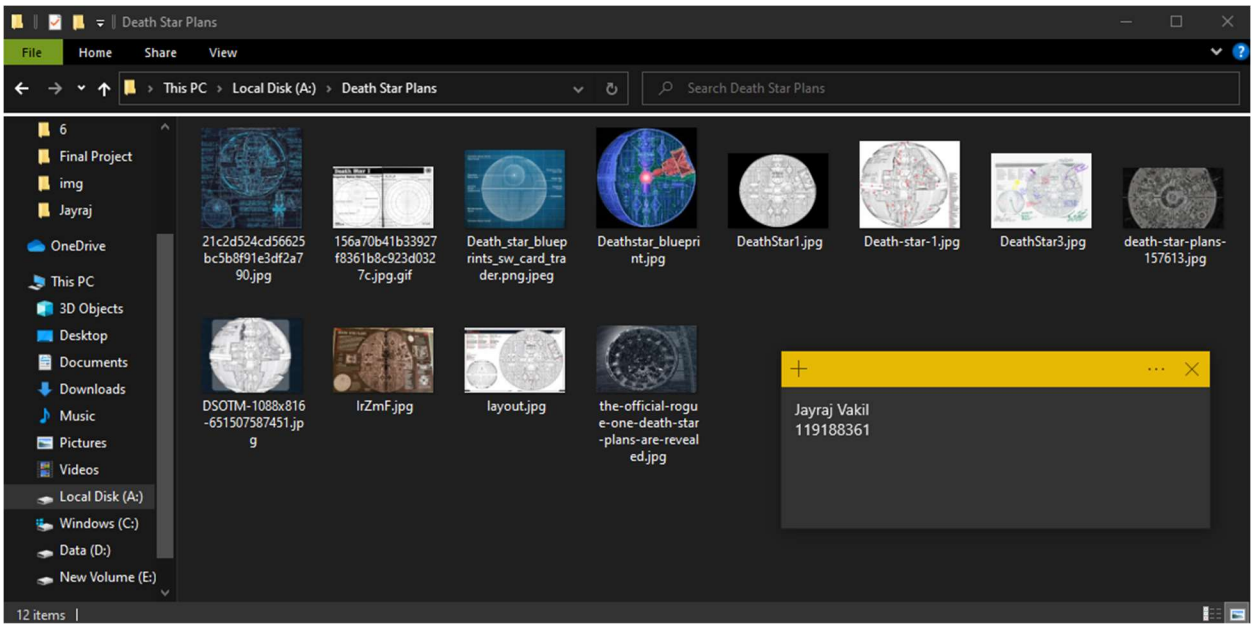
Upon running the 'Final-form.exe' file, a console window opened with no visible output. Subsequently, a network traffic analysis using Wireshark revealed connections to two webpages: 'We-have-the-blue-prints-to-the-Death-Star' and 'We-will-defeat-Darth-Vader.' This states that the Final-form.exe is the final malware version of the writer.

http://www.umd.edu/We-will-defeat-Darth-Vader
http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star

The above 2 links are the messages inside the final malware.

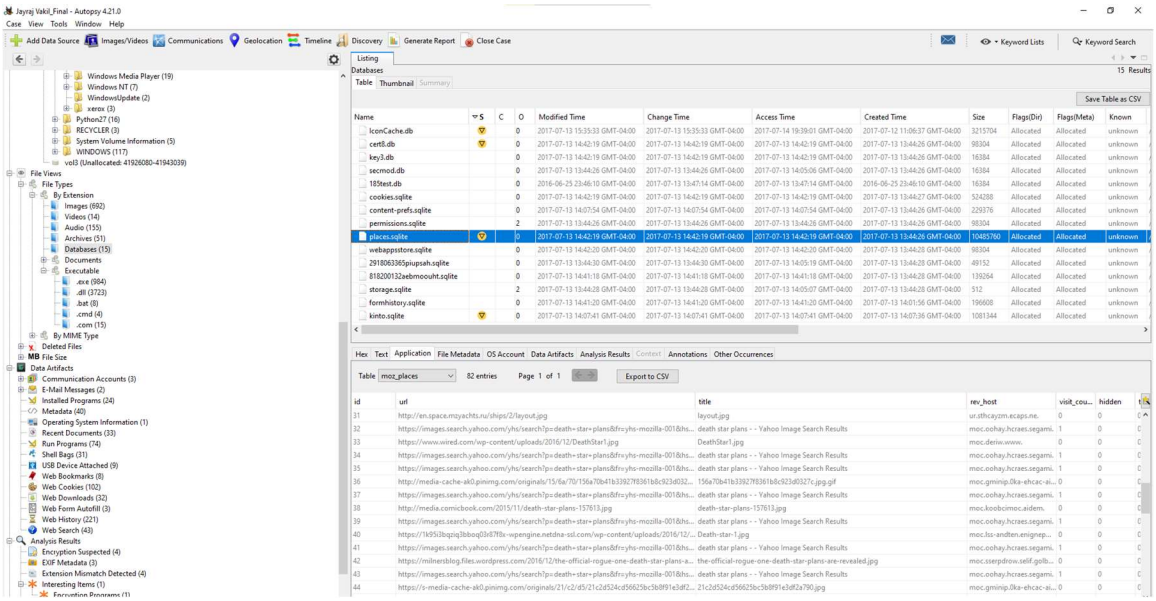


Exploring the folder named 'Death Star Plans,' revealed a collection of images and plans pertaining to the Death Star.

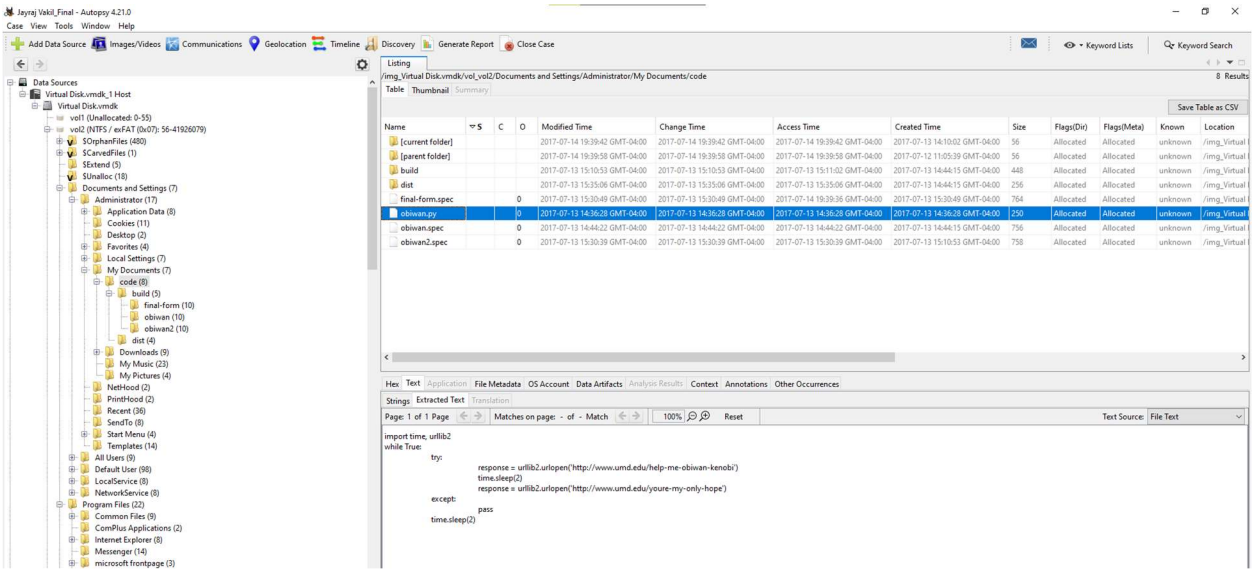


C. Some interesting finds:

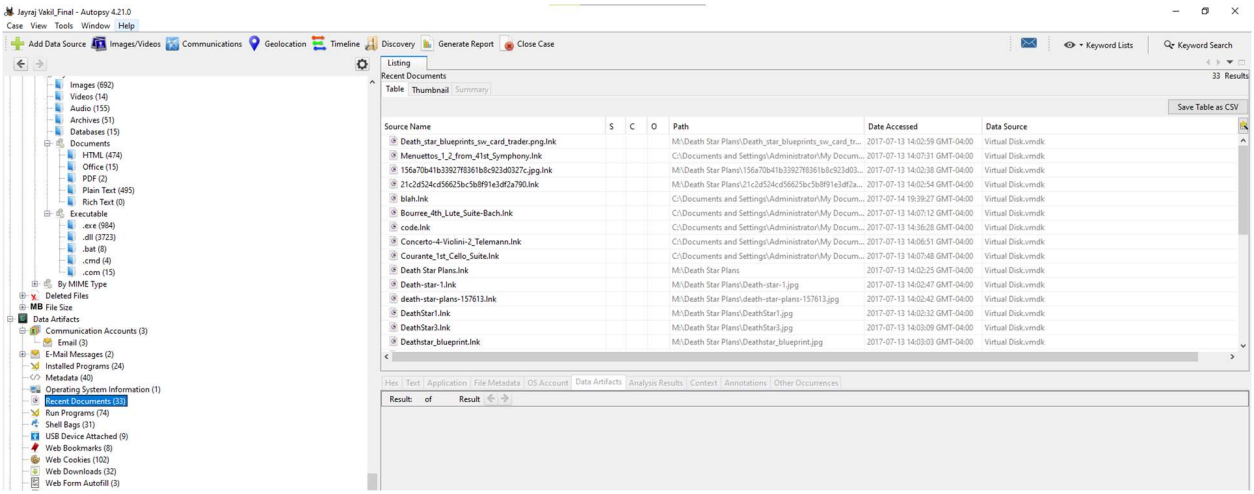
The file “places.sqlite” seems to be of interest because it is referenced in many of the Death Star files and VeraCrypt.



The file “obiwan.py” seems to be what the obiwan.exe does. It calls the 2 websites that obiwan.exe does and sleeps for 2 seconds. This runs for infinite times.



In the “Recents Documents” it is seen that many .lnk files are accessed which are related to Death Star.



Conclusion and Recommendation

Conclusion:

The comprehensive digital forensic analysis of a Windows XP virtual machine using Autopsy software uncovered a complex web of malicious activities. Two executables, "obiwan.exe" and "obiwan2.exe," were found to initiate outbound connections to unique URLs, some containing encoded messages. Decoding these led to the discovery of an encrypted volume using VeraCrypt, which was accessed using a base64-decoded password. Inside, a text file, another executable, and a folder with sensitive contents were found. The second executable, "Final-form.exe," showed further suspicious network activity, pointing to a significant security breach involving critical data related to the Death Star.

Recommendations:

1. Enhanced Monitoring and Network Analysis: Implement continuous monitoring of network traffic to identify and intercept any unauthorized communications, especially those resembling the patterns observed in the executables' activities.
2. Robust Encryption and Access Controls: Strengthen encryption protocols and access control mechanisms to safeguard sensitive data, ensuring that only authorized personnel can access critical information.
3. Regular System Updates and Patch Management: Keep all systems and software updated with the latest security patches to mitigate vulnerabilities that could be exploited by malicious software.
4. Comprehensive Incident Response Plan: Develop and maintain an incident response plan tailored to scenarios like this breach, ensuring swift and effective action in the event of future security incidents. This plan should include steps for containment, eradication, and recovery, along with post-incident analysis to prevent recurrence.

Challenges Faced

Challenge 1: I initially assumed that "obiwan.exe" and "obiwan2.exe" contained similar messages to those in previous assignments, leading me to overlook crucial clues. This oversight delayed the discovery that "obiwan2.exe" held a vital piece of the puzzle - the encryption password hidden in its network traffic.

Challenge 2: Deciphering the encoded message from "obiwan2.exe" was challenging, as I was unfamiliar with base64 decryption. Additionally, connecting the "not-the-droids-you-are-looking-for.mp3" file to VeraCrypt encryption proved difficult. I spent significant time searching for hidden data in the wrong places before realizing its true significance.