Samridha Murali
118551449
ENPM 687- CY01

Final Project - Comprehensive Forensic Investigation

Abstract

In this project, I analyzed an image of a harddrive for a new malware and a final message. This malware was protected by encryption with a special encryption program, which requires a secret key for decryption. To obtain the key, I examined the network traffic of the obiwan2.exe executable file and obtained the secret key as “r2d2”. To obtain the final message, I decrypted the new malware using the obtained secret key and found another executable (final-form.exe), a folder with images and instructions. Further, I analyzed the network traffic of the final-form.exe executable and obtained the final message “We have the blueprints to the Death Star. We will defeat Darth Vader".

Tools

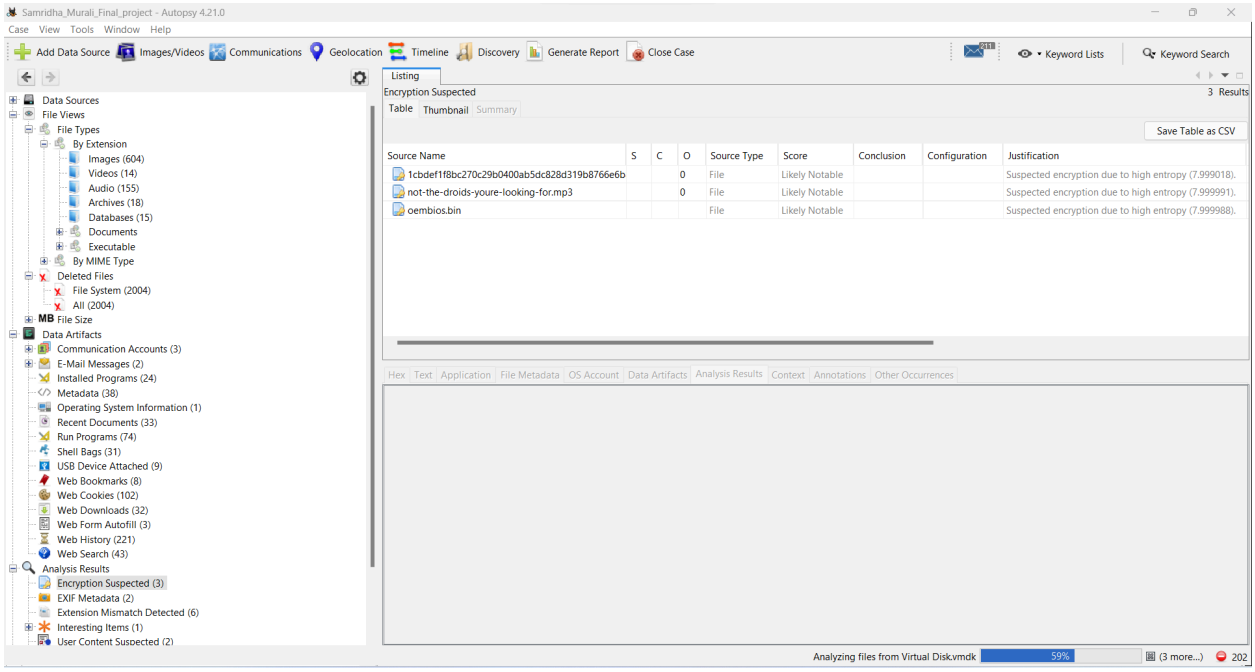
1. Autopsy - Used for digital forensics analysis.
2. Wireshark - Used to capture and analyze Network traffic.
3. Cyberchef - Used to Decode data.

Repository

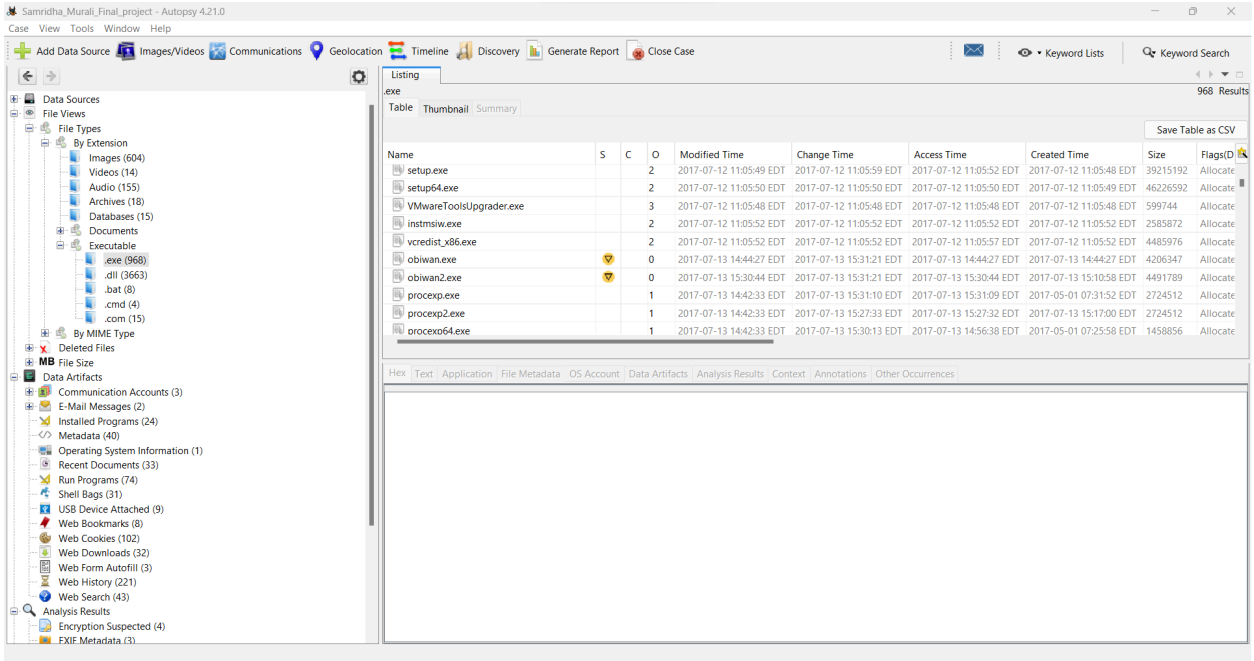
1. We are provided with a Zip file of system image.

Analysis

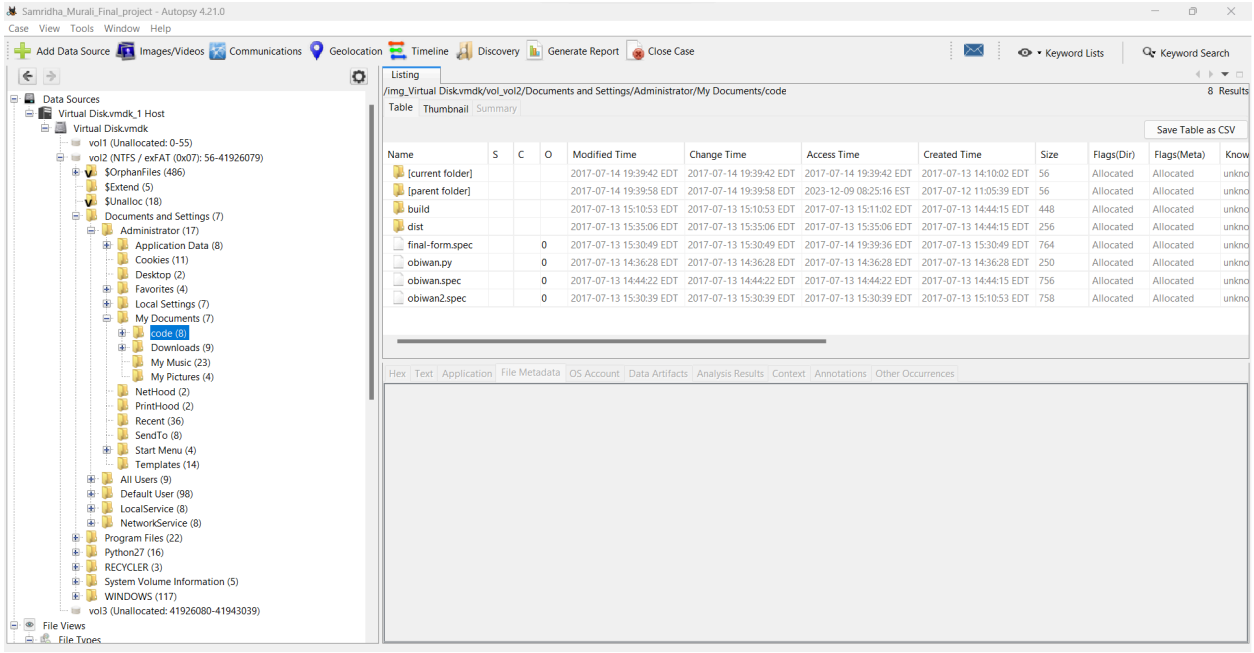
1. I loaded the project in vmware. It was a Windows system with Administrator user account, which required a password for login. I tried some commonly used passwords for administrator accounts like “administrator”, “admin”, “admin123”. I wasn’t successful in my login attempt.
2. I loaded the virtual disk into Autopsy for analysis.



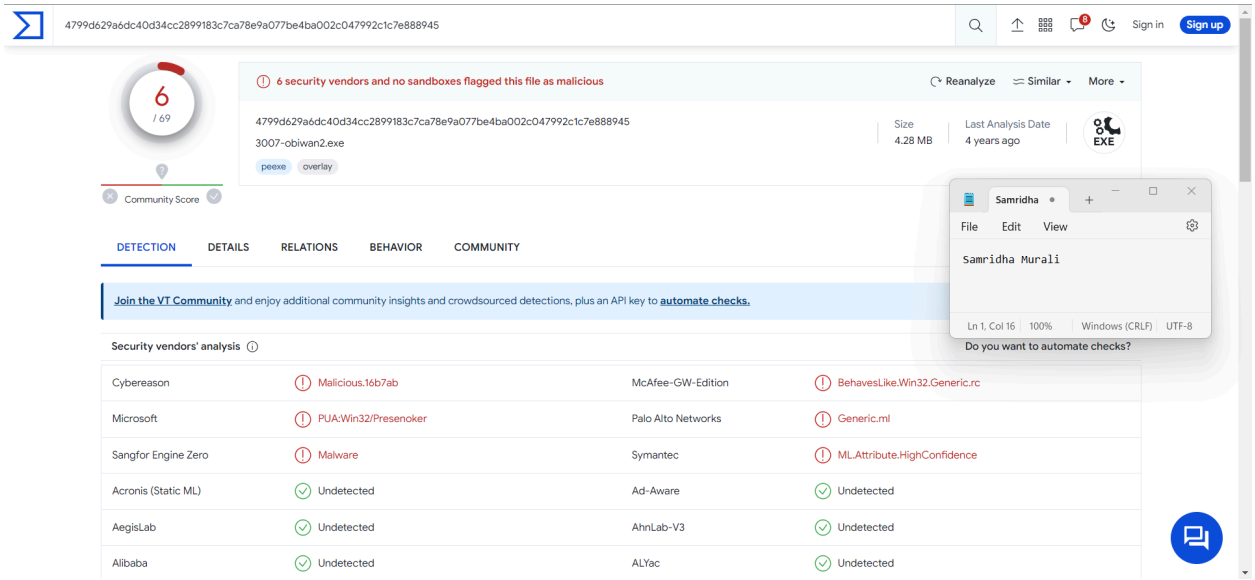
3. Since we are looking for malware I started the analysis by checking all executable files. Found 2 interesting executable files obiwan.exe and obiwan2.exe.



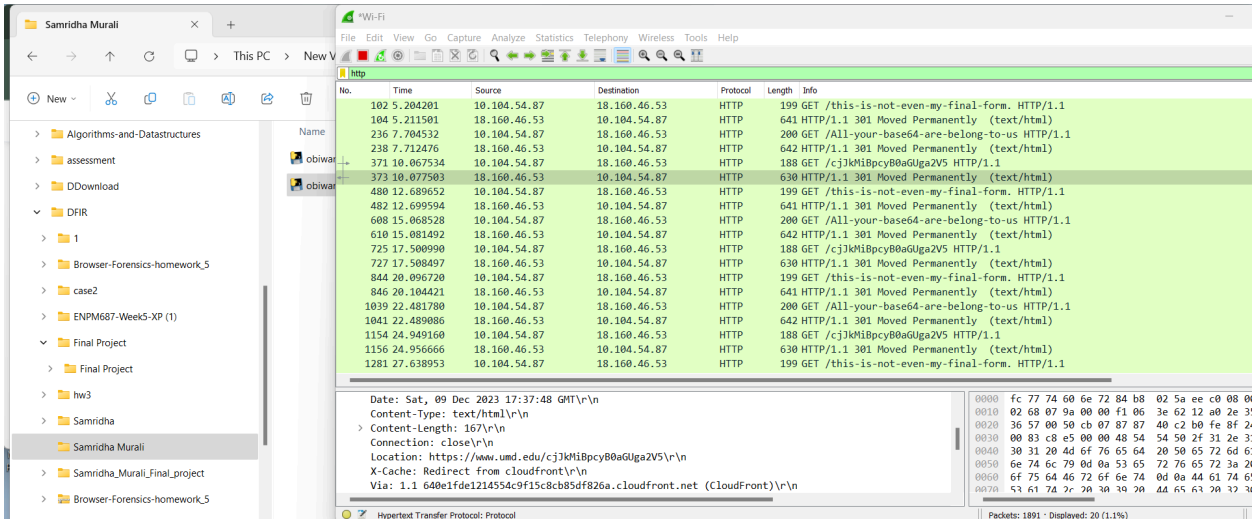
4. On navigating to obiwan.exe location, I found some more interesting files. I extracted them all for further analysis.



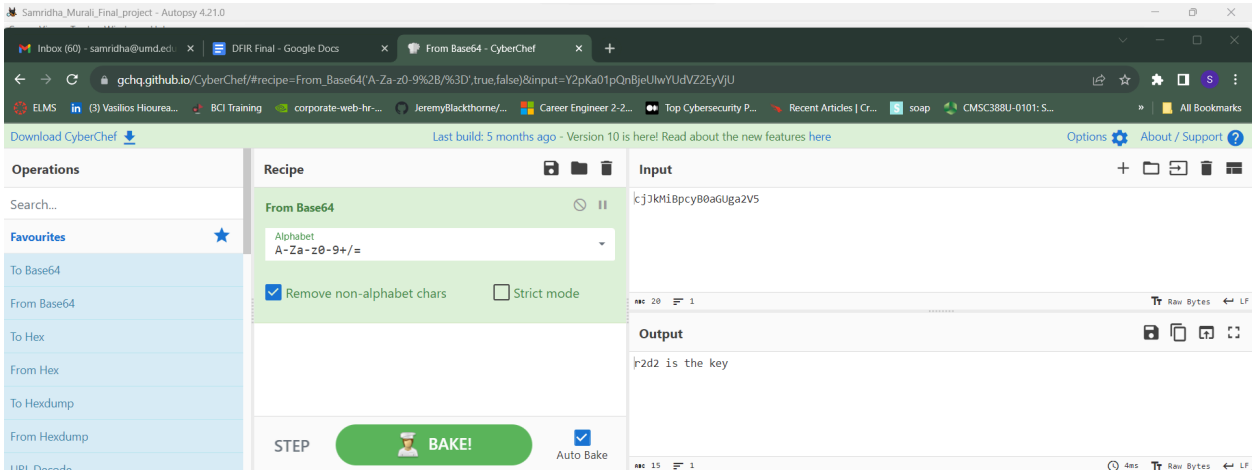
5. Since we are looking for final version of malware, Obiwan2.exe is my primary suspect as this looks like a newer version of our former obiwan, I uploaded it to https://www.virustotal.com/gui/home/upload to check if it is a malware. 6 security vendors have flagged this executable as malware.



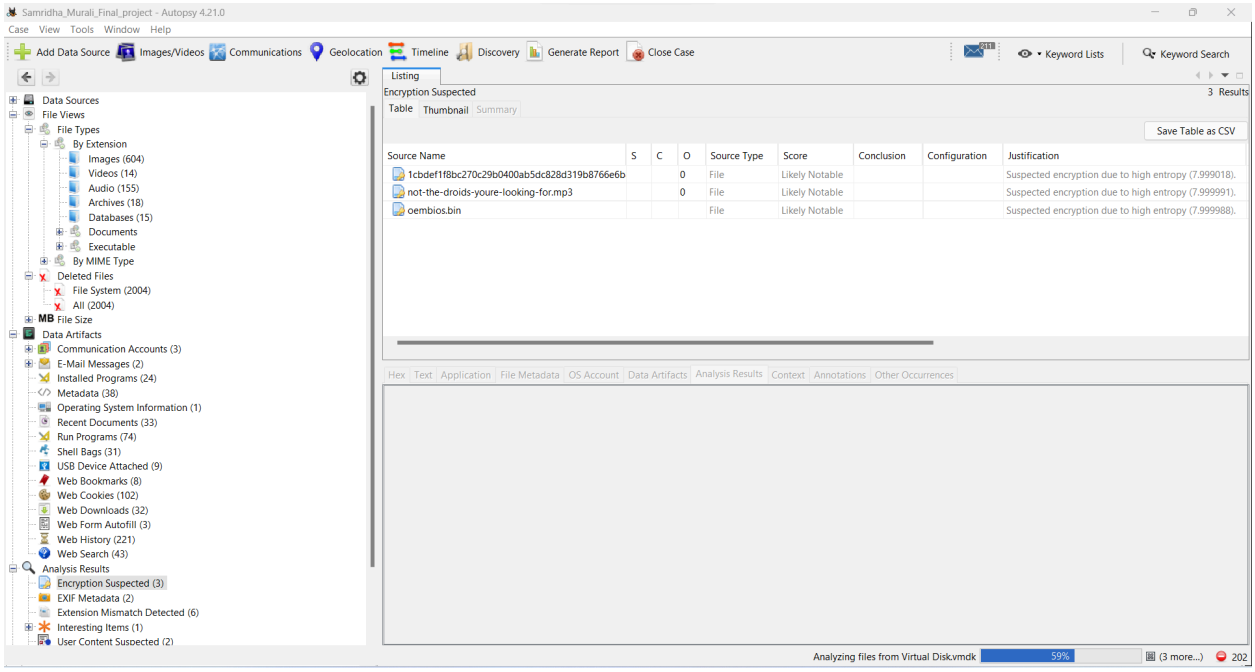
6. To analyze the network behavior of the malware, I started network packet capture in wireshark and executed the malware. A lot of packets were captured, to understand the behavior I filtered only http traffic. There were mainly GET request to https://www.umd.edu/this-is-not-even-my-final-form, https://www.umd.edu/All-your-base64-are-belong-to-us, http://www.umd.edu/cjJkMiBpcyB0aGUga2V5. This made it clear that this is not the final malware I am looking for.



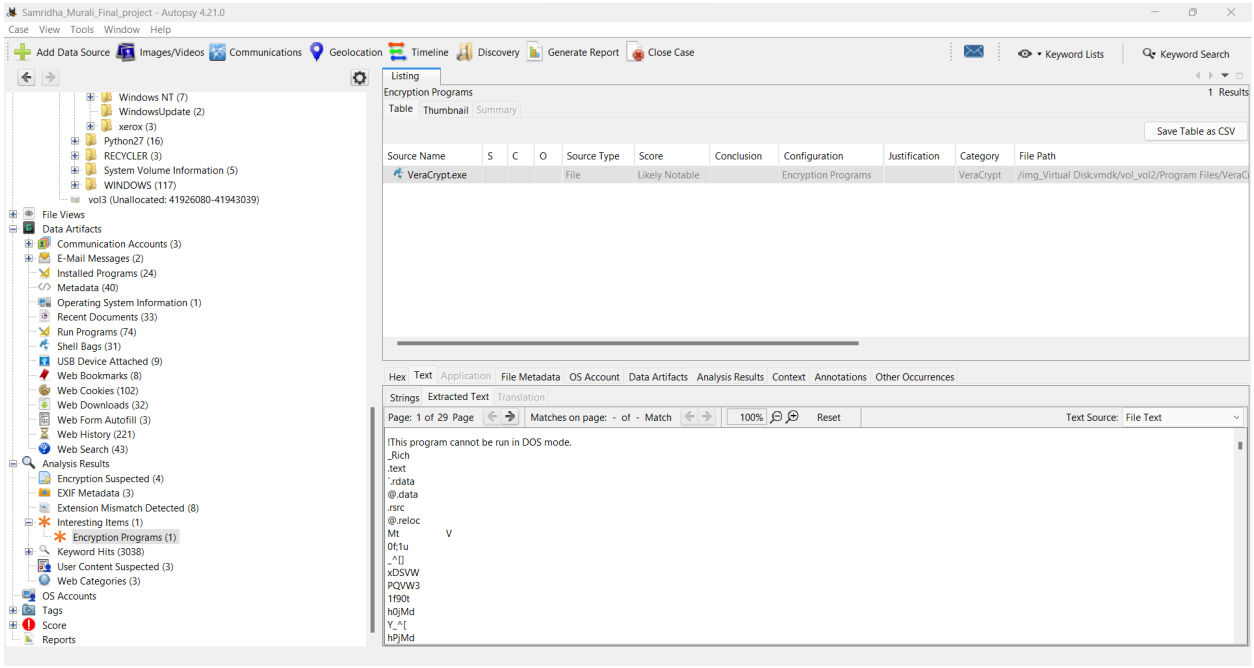
7. Since they are talking about base64 and “cjJkMiBpcyB0aGUga2V5” looking like base64 data, I tried to decode from base64. I used cyberchef for converting from base64. On converting from base64, we get “r2d2 is the key”.



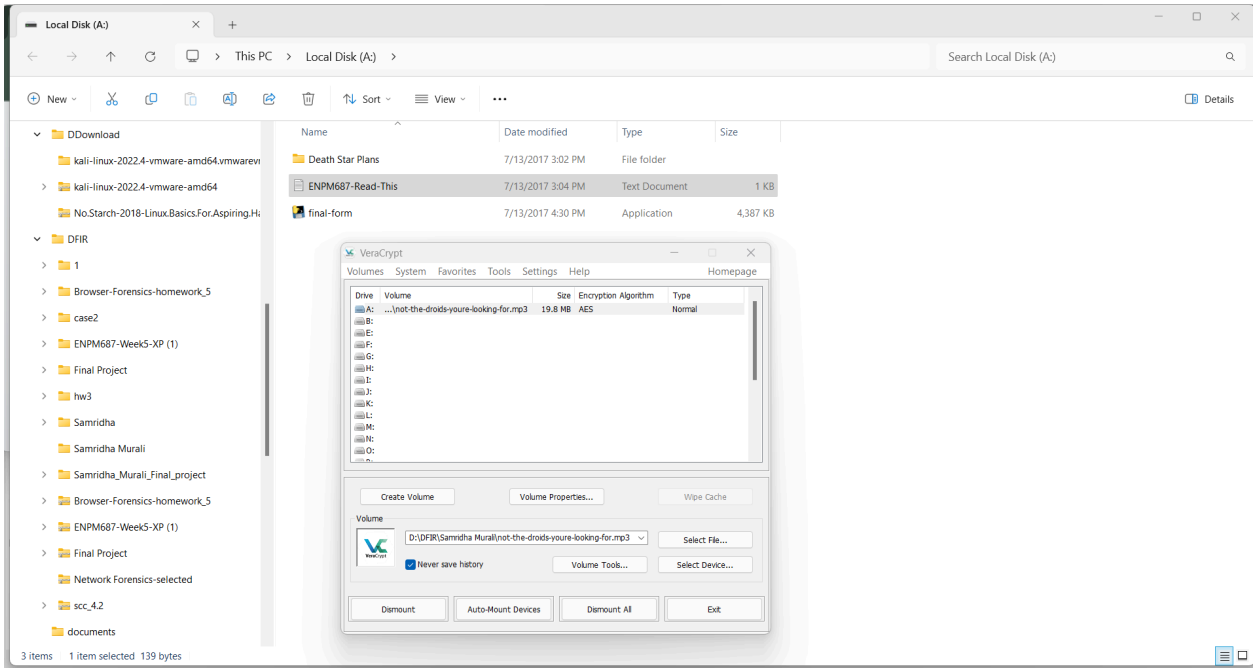
8. After reaching a deadend, I started looking into analysis result in autopsy. I found 4 files with Encryption suspect. One file name looked particularly interesting “not-the-droid-youre-looking-for.mp3.



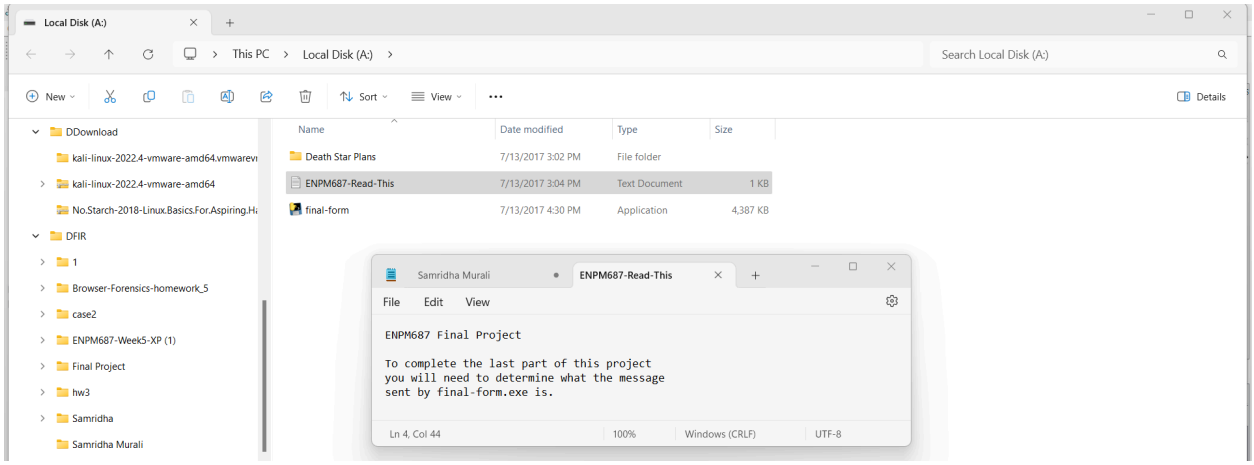
9. In the interesting item section, I found an encryption program VeraCrypt.exe. Now, we have an encryption program, secret key and an encrypted file (since it has been marked as Encryption Suspected in Autopsy).



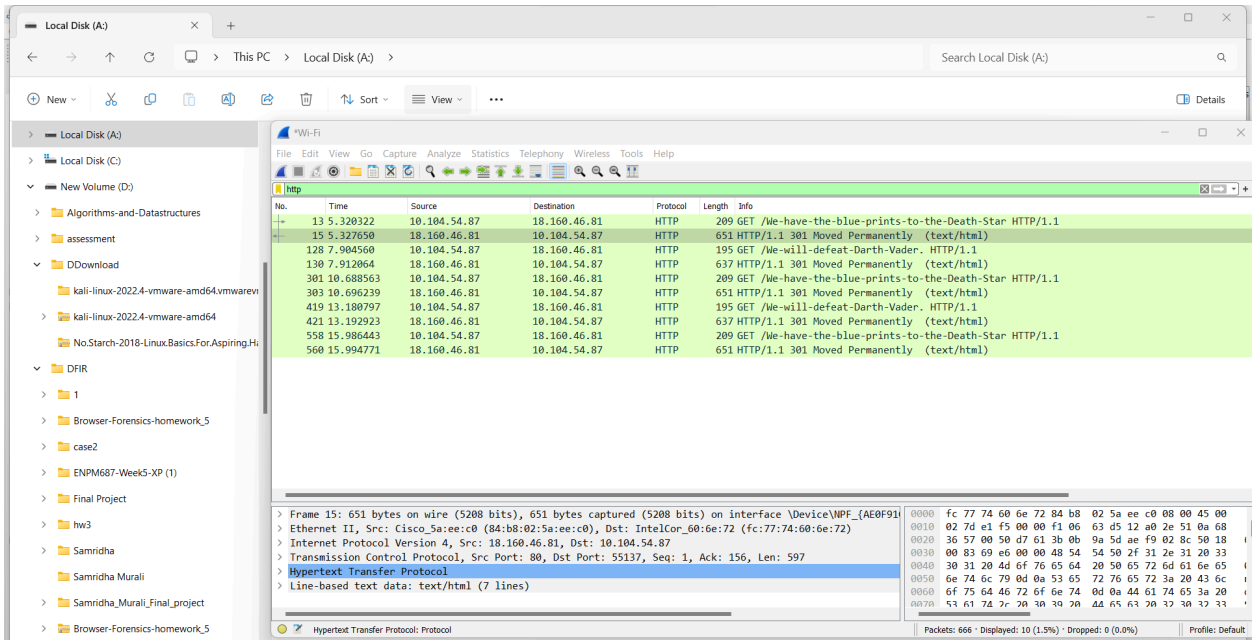
10. I extracted veraCrypt.exe and 2 other necessary .sys files, and installed veraCrypt program. Loaded the not-the-droid-youre-looking-for.mp3 and mounted it to drive A.



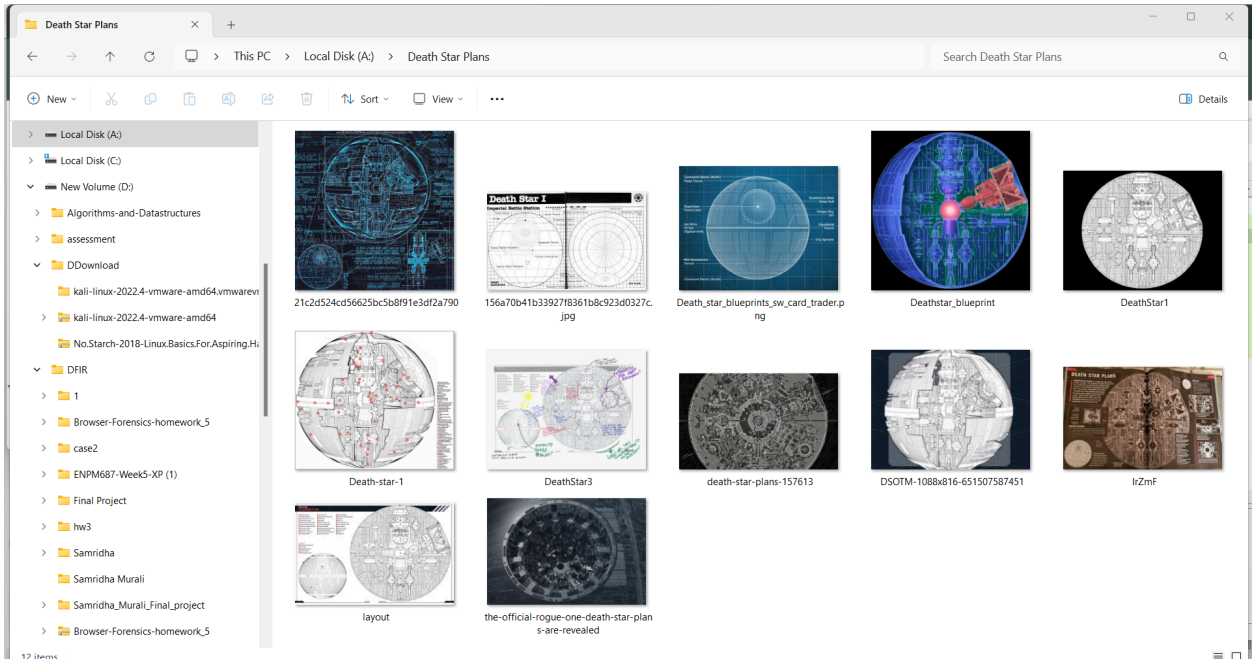
11. On decrypting the not-the-droid-youre-looking-for.mp3 using key “r2d2”. I found the file “ENPM687-Read-This” file and final-form.exe. Final-form.exe is the final version of the malware.



12. I started network packet capture on wireshark and executed the final-form.exe. On filtering only http traffic. We could see the following traffic.



13. Final-form.exe made requests to /We-have-the-blue-prints-to-the-Death-Star and /We-will-defeat-Darth-Vader. So the final message is “We have the blue prints to the Death Star. We will defeat Darth Vader”.
14. In the Death Star Plan folder, we can see the following maps.



Recommendations

- As a next step, all traffic generated by final-form.exe can be analyzed.

- The communication accounts and E-mail messages can be analyzed to get any further information.

Questions and Answers

1. Find the final version of the malware writer's malware
   final-form.exe

2. Determine what the message contained inside of the final malware is
   We-have-the-blue-prints-to-the-Death-Star
   We-Will-Defeat-Darth-Vader

3. Describe two challenges or difficulties you had to overcome to complete the final project.
   a. Initially I had difficulty in capturing traffic in wireshark on executing the obiwan2.exe. This gave me a wrong angle in investigation. Later when I reverted back to obiwan2.exe and after multiple restarts, wireshark captured packets and I was able to proceed.
   b. Upon discovering that "r2d2" is the decryption key, it became clear that there were further layers to discover. Nevertheless, getting to the next phase, specifically locating 'not-the-droid-youre-looking-for.mp3,' was a considerable challenge.