Windows Machine Incident Digital Forensics Investigation

By: Bhavik Shah

Problem Statement

You are the Imperial Forces best forensic analyst. At a great cost the Imperial Army has come into possession of an image of a hard drive for a rebel scum malware writer. Their codes have plagued our computers for the last time, infecting them but also using it to send messages across the galaxy.

Your mission is to analyze the image of the Rebel malware writer hard drive. Find out what their newest “malware” does, any messages it may send out, and review the image for other useful intelligence.

Final Report

Brief Summary of Information

The assigned case was a case of intrigue, being a machine captured from the rebel forces. The evidence captured was an instance of a virtual machine with a Windows operating system. The objective was to investigate the machine and find the malware hidden by the rebel forces on the machine. There were several suspicious artifacts recovered during the investigation which revealed the plans stolen by the rebel forces and a few applications which sent out secret messages on the network. After following a methodological approach, I was able to uncover the final form of the malware encrypted inside an audio file and the messages being sent out using the malware.

Tools Used in the Investigation

This investigation required several tools to achieve the final goal. Firstly, I used Autopsy to mount and investigate the virtual machine. Autopsy is a premier end-to-end open-source digital forensics platform. It is a fast and efficient hard drive investigation solution that evolves with the user’s needs. Autopsy enables to look at the files present on the hard drive and allows us to extract a particular file if it requires a deeper investigation.

Through the investigation, I uncovered several executables which on being ran did not show any activity but when looked through task manager, I could observe that they were showing some network activity. Treating those files as a network traffic investigation, the best tool to analyse network packets is Wireshark. Wireshark is a network packet analyser. A network packet analyser presents captured packet data in as much detail as possible. We can think of it as a measuring device for examining what is happening inside a network cable. It lets us see what is happening on the network at a microscopic level and is the de facto standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

Apart from that, the system in question had VeraCrypt installed on it. VeraCrypt is an open-source utility for file encryption. The software can create a virtual encrypted disk that works just a regular disk but within a file, which can be of any nature. It can also encrypt a partition or the entire storage device.

Repository #1: Captured Virtual System (ENPM687 Final XP)

A. Summary of Evidence

"ENPM687 Final XP" is the captured virtual system in question. After uploading it to Autopsy, I found that it had one NTFS drive with all the data in it. A major breakthrough was immediately achieved through the "Analysis Results" section which pointed to 4 files which were encrypted, out of which 1 had a suspicious name. I got the final name of the malware in question through the "Recent documents" section. And a search through "Installed Programs" section pointed out to the applications installed on the system which led to a breakthrough in the investigation. After a detailed investigation, I was finally able to uncover the final malware created by the rebels, "Final-Form.exe." The detailed steps on investigation are described below.

B. Analysis / Investigation Steps

Firstly, I mounted the virtual hard drive onto Autopsy. I took the "Analysis Results" view as my starting point.

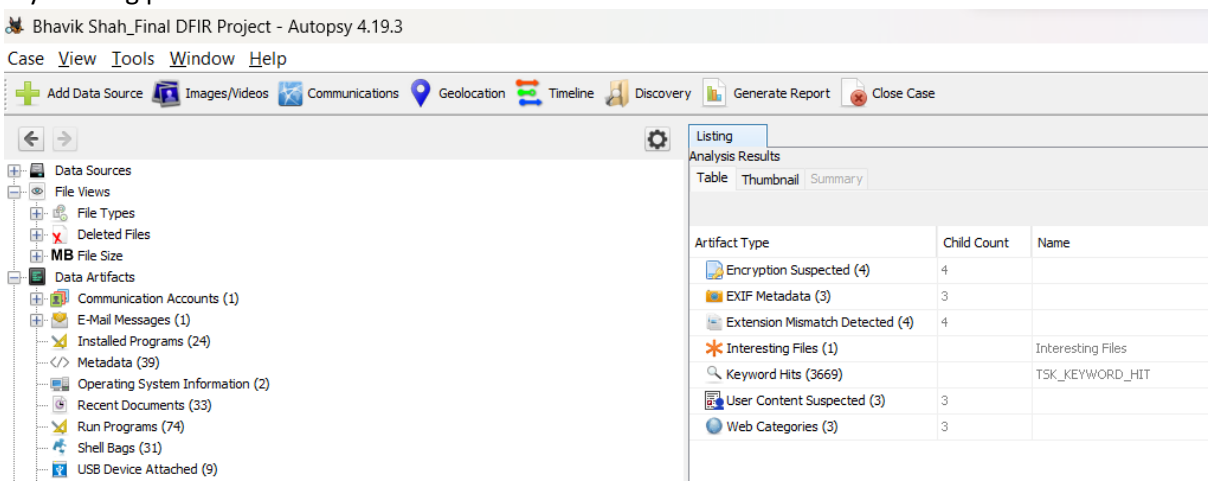

Figure 1 - Analysis Results View

I went each folder, out of which 2 of the artifact types had suspicious artifacts. Under "Encryption suspected" type, we observed 4 files out which 1 was related to the rebel forces. And under "Interesting files" type, we could see that there was an encryption software installed on the system.

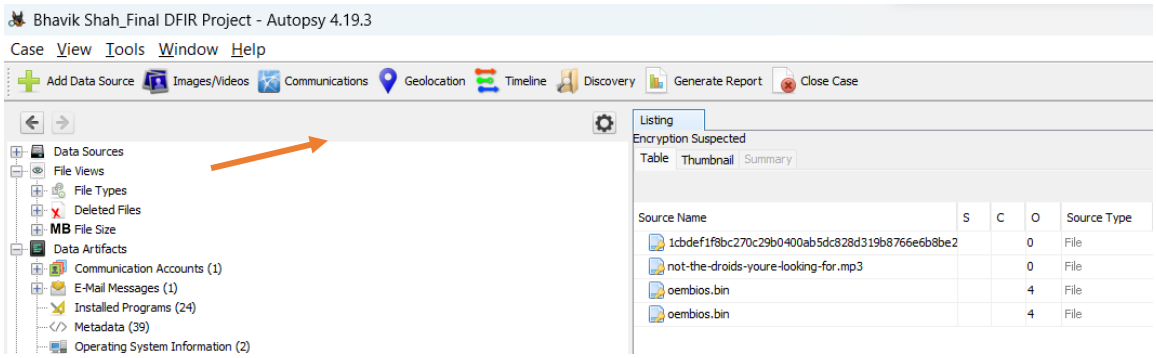

Figure 2 - Encryption Suspected Files List

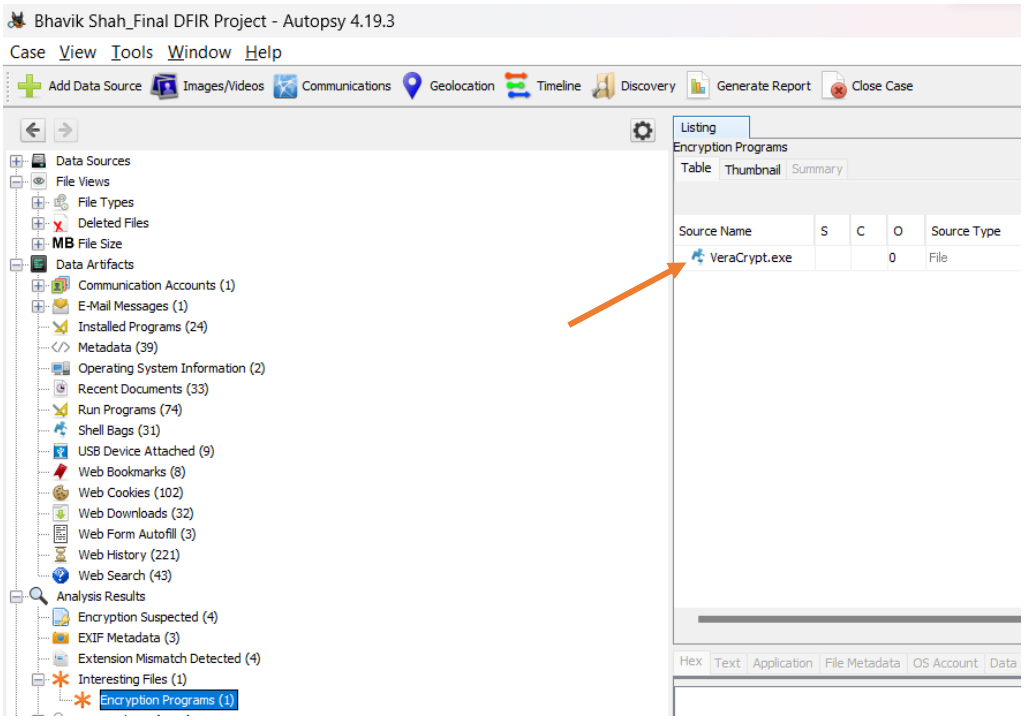

Figure 3 - Interesting Files View

The encryption software installed was VeraCrypt. This gave me 2 clues: (1) Out of the first 2 "encryption suspected" files, one must be encrypted. (2) If they are encrypted, then might have been encrypted using VeraCrypt.

Next, I went to "Recent Documents" artifact type under "Data Artifacts" view to see the files which the user might have accessed. Initially, the user was accessing Death Star plans files on a drive named "M." And in the recent logs, he accessed 3 python files in "code" folder under "Administrator" user's "My Documents."

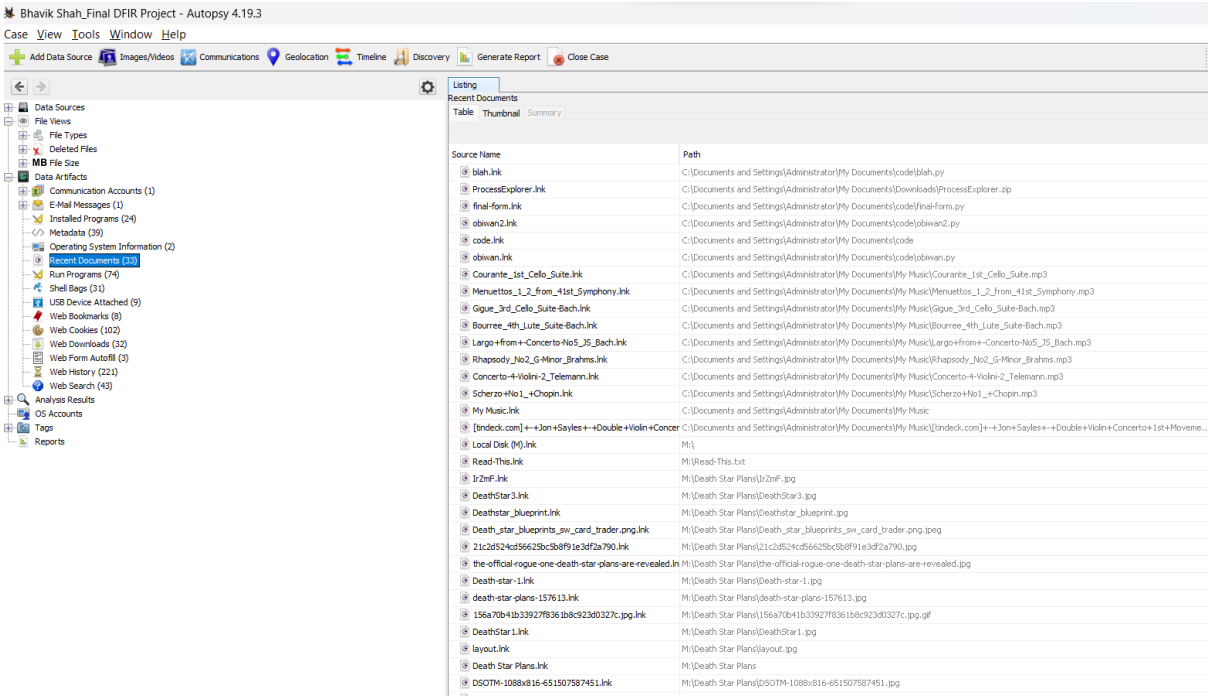

Figure 4 - Recent Documents View

Next, I expanded the “Data Sources” section to see how many drives were present. But in this case, there was only a single drive loaded onto the system and the folders indicated that it was the main C drive. This confirmed the suspicion that a drive has been encrypted on top of a file present on the system.

Then, I accessed the “code” folder to see if I could find the python files. As per python standards, I can assume that the dist folder would contain the compiled and built versions of the python files. But there were only 2 python executables – obiwan.exe and obiwan2.exe.

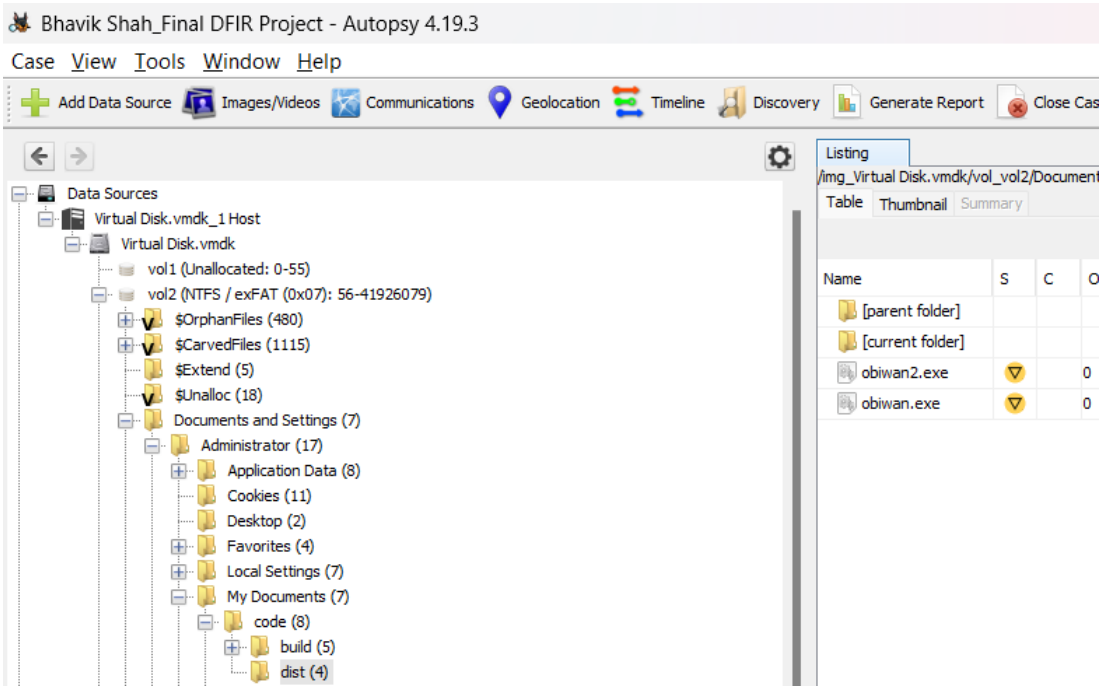

Figure 5 - Finding obiwan and obiwan2 (Dist folder)

I extracted both the files using the “Extract files” utility of Autopsy. I took turns of running both the files separately and when I did not see any output on the screen, I opened Wireshark and ran a traffic capture.

Repository #2: Obiwan.exe and Obiwan2.exe

A. Summary of Evidence

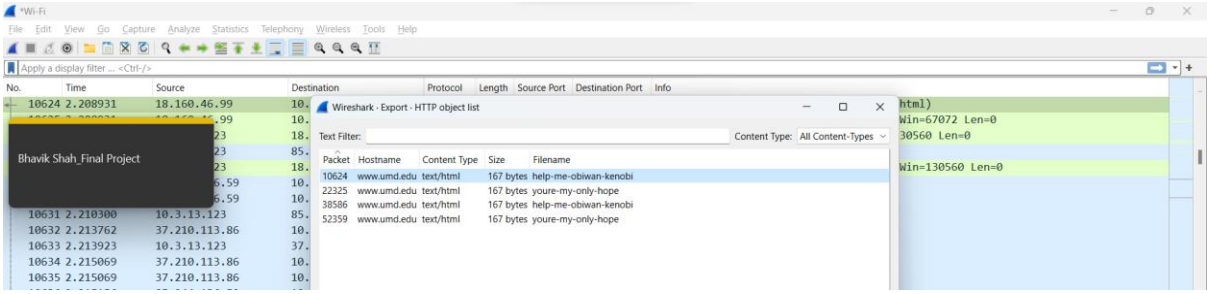

Figure 6 - Message being sent from obiwan.exe

On running capture for obiwan.exe, I observed a message being sent out on loop – "**help me obiwan Kenobi” and “you’re my only hope**.”

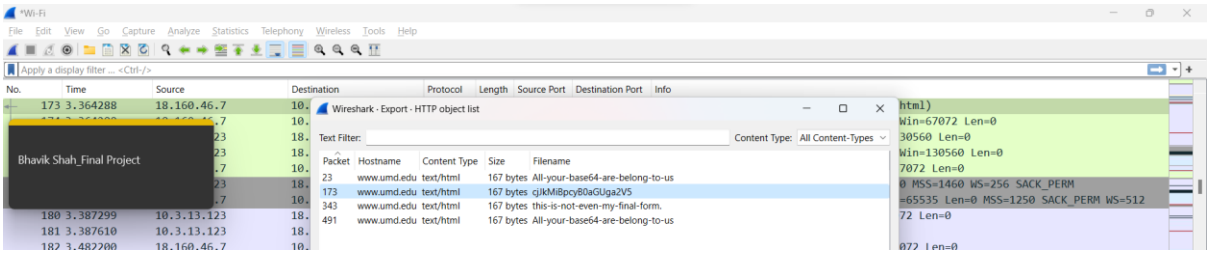

Figure 7 - Message being sent from obiwan2.exe

For obiwan2.exe, I got a series of messages, out of which 1 indicated that this is not the final form of malware. The other message looked gibberish, with random characters typed but the next message indicated a clue that the message might be encoded in base64. So, I went to a website and inputted the string and got a meaningful output from the gibberish: "**r2d2 is the key**." This could be a clue that the string "r2d2" might be a password being used somewhere.

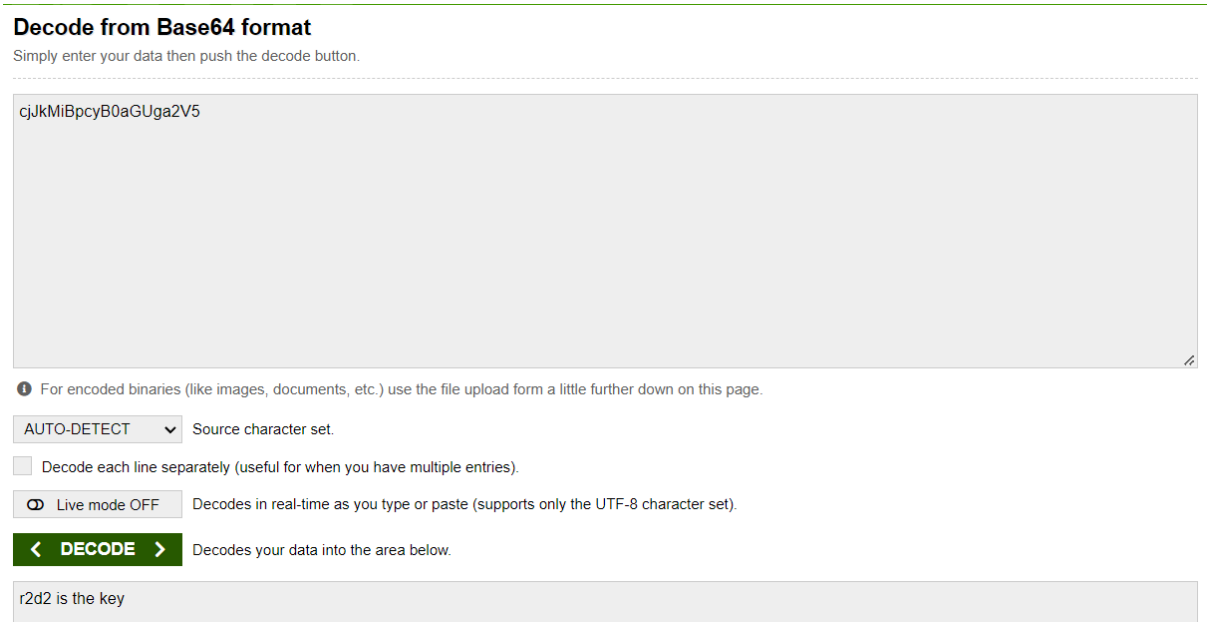

Figure 8 - Decoding Base64 message captured from obiwan2

Repository #3: Not-the-droids-you-are-looking-for.mp3

A. Summary of Evidence

Next, I went to "My Documents/My Music" folder because that's where lied the majority number of files recently accessed in the system as well as one of the encryption suspected file. I extracted all the mp3 files using the "Extract files" utility of Autopsy. Every file opened successfully and played the respective track except "not-the-droids-you-are-looking-for.mp3."

My first suspicion was that the file had some data enabled into it using steganography and the password to extract the binary data would be r2d2. But no steganography tools detected hidden data inside it. At that point, I realised that a drive can be encrypted using VeraCrypt and be renamed or stored as a random file. To confirm my suspicions, I mounted the mp3 file on VeraCrypt. The file asked for a password and for this we had already got the answer from obiwan2.exe, the key was "r2d2."

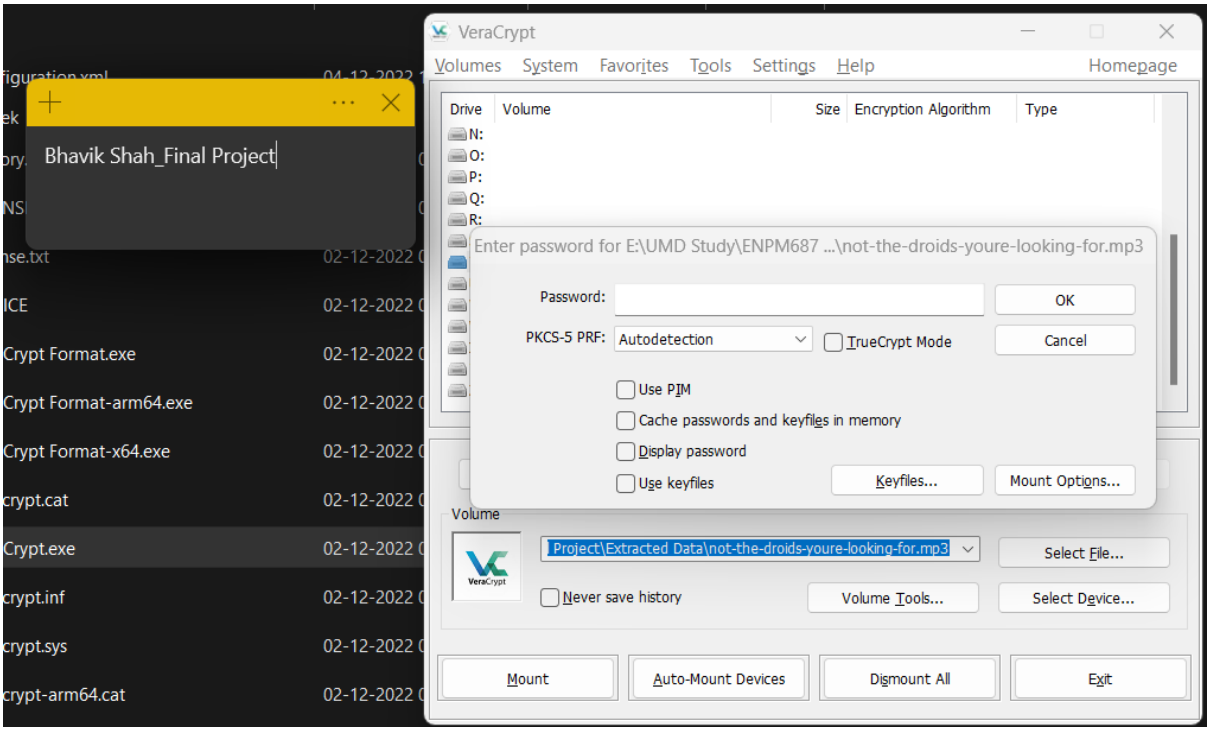

Figure 9 - Mounting not-the-droids-you-are-looking-for.mp3 using VeraCrypt

And we successfully found the final form of malware hidden on the drive with all the death star plans.

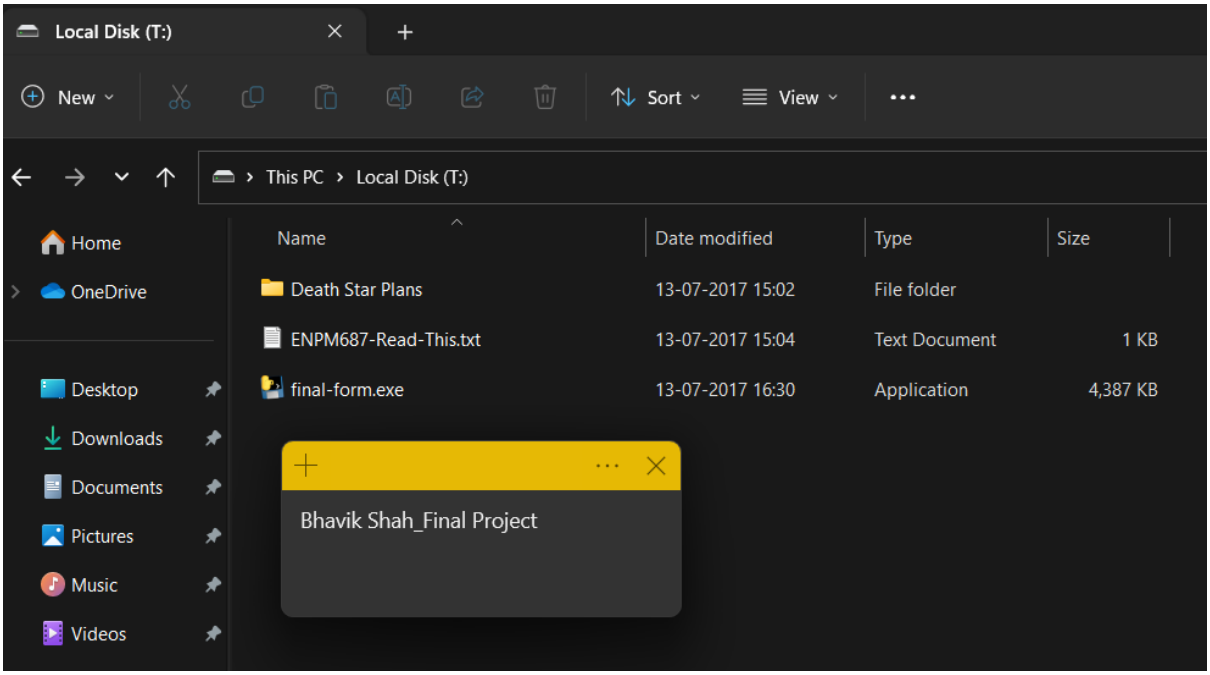

Figure 10 - Successfully Accessing Encrypted Drive and Getting access to final form of malware

I executed final-form.exe malware and ran a Wireshark traffic capture to analyse the messages being sent by it.

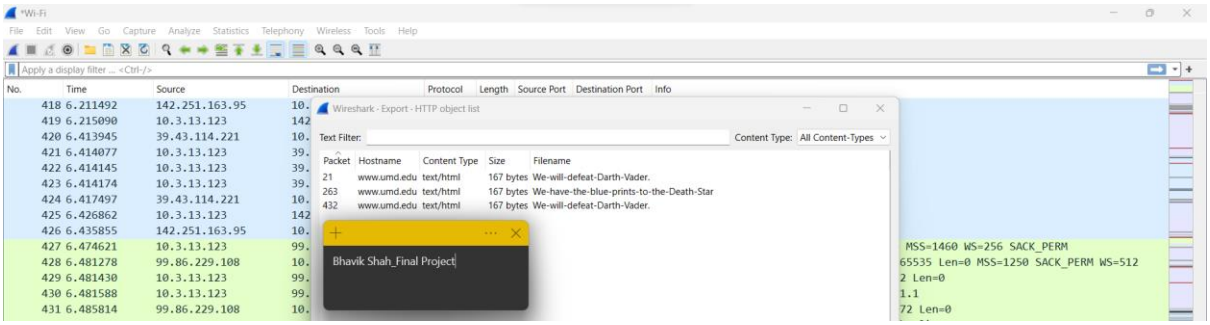

Figure 11 - Final Message from Final Form of Malware

And I got the final messages: “We will defeat Darth Vader” and “We have the blue prints to the Death Star,” being repeated on a loop. And the folder had all the plans acquired by the rebel forces.

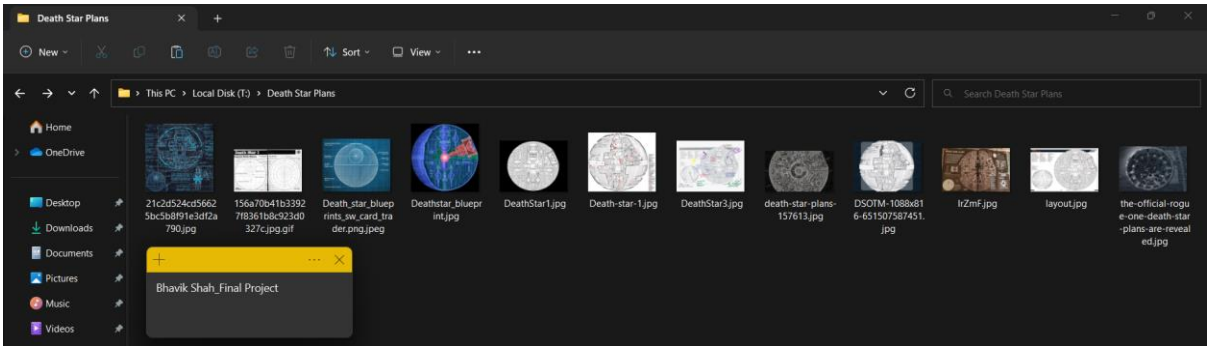

Figure 12 - Evidence of Death Star Plans in Rebel Forces hands

Recommendation / Next Steps

From the evidence analysed, we can conclude that the program could have been a danger, if it contained malicious code. As obiwan.exe, obiwan2.exe and final-form.exe were able to connect to the network and request for webpages, it could have been used to open a network backdoor or used to fetch a malware like a worm or virus into the system. And with the death star plans captured on the system, Imperial Forces should make changes in the Death Star so that rebel forces are not able to use this information in any way possible. With this conclusion, we can close the investigation.