Final Forensics Report

Digital Forensics and Incidence Response

Dheepshika Raghunathan

Contents

[1. Summary of Results 3](#_Toc532676547)

[1.1. Find the final version of the malware writer’s malware 3](#_Toc532676548)

[1.2. Determine what the message contained inside of the final malware is 3](#_Toc532676549)

[1.3. Find some other interesting items/artifacts/clues that are definitely 'relevant' to the investigation. 3](#_Toc532676550)

[2. Tools Used 11](#_Toc532676551)

[2.1. Wireshark 11](#_Toc532676552)

[2.2. Autopsy 11](#_Toc532676553)

[2.3. Veracrypt 11](#_Toc532676554)

[3. Analysis of Rebel Malware Writer’s Hard Disk 12](#_Toc532676555)

[3.1 Obiwan2.exe 12](#_Toc532676556)

[3.2 Veracrypt mounted volume 14](#_Toc532676557)

# Summary of Results

## Find the final version of the malware writer’s malware

The final version of the malware writer’s malware was called “final-form.exe”.



## Determine what the message contained inside of the final malware is

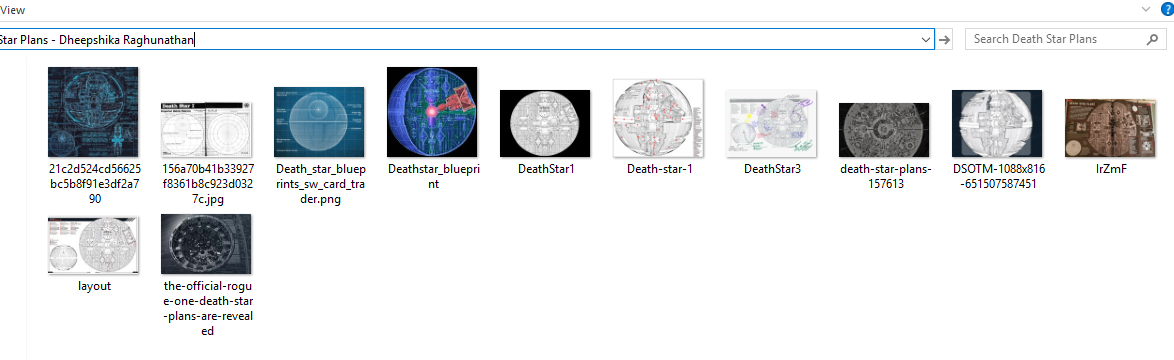
The above malware communicates with theumd.edu at IP address 99.84.104.24.



The malware sent the message “We-will-defeat-Darth-Vader.” and after 3 seconds it sends the message “We-have-the-blue-prints-to-the-Death-Star”. This process repeats periodically.

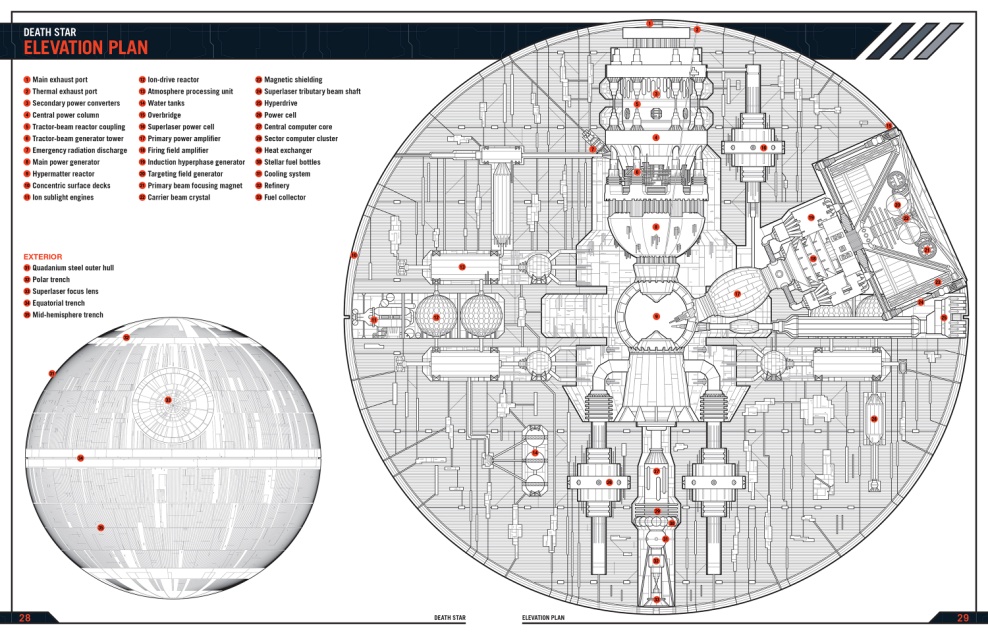
## Find some other interesting items/artifacts/clues that are definitely 'relevant' to the investigation.

The plans to the Death Star were found inside the VeraCrypt encrypted drive.

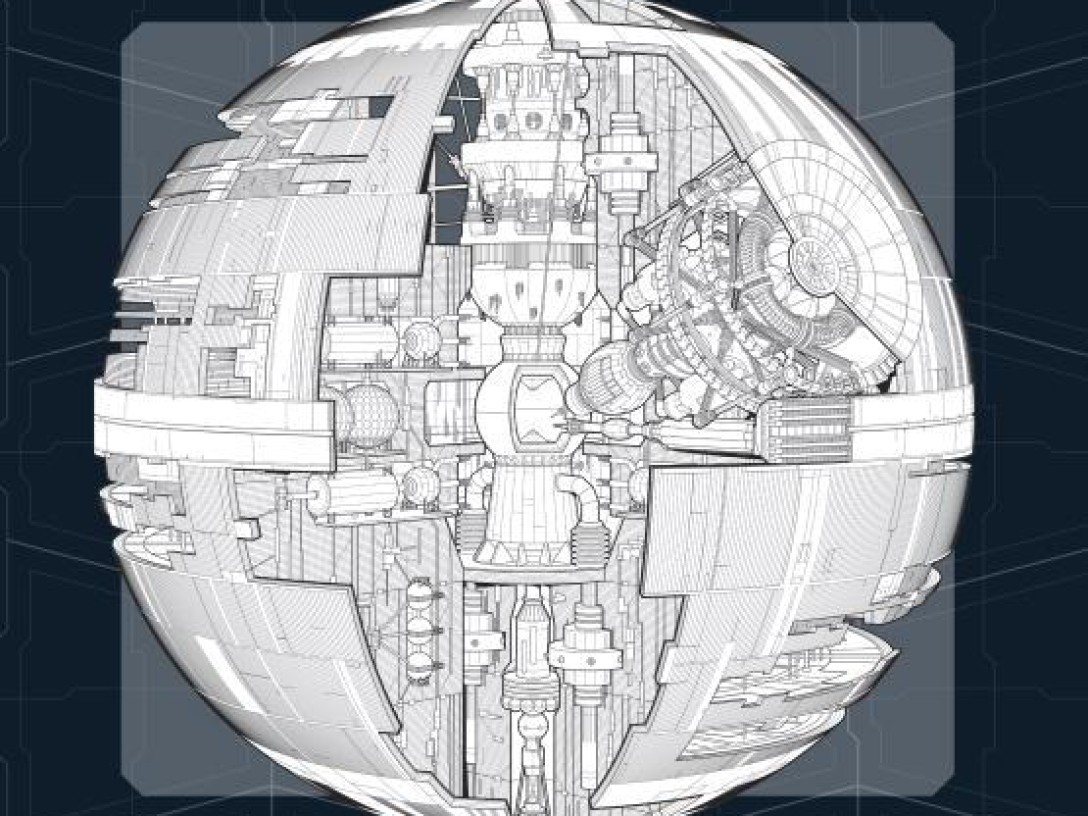


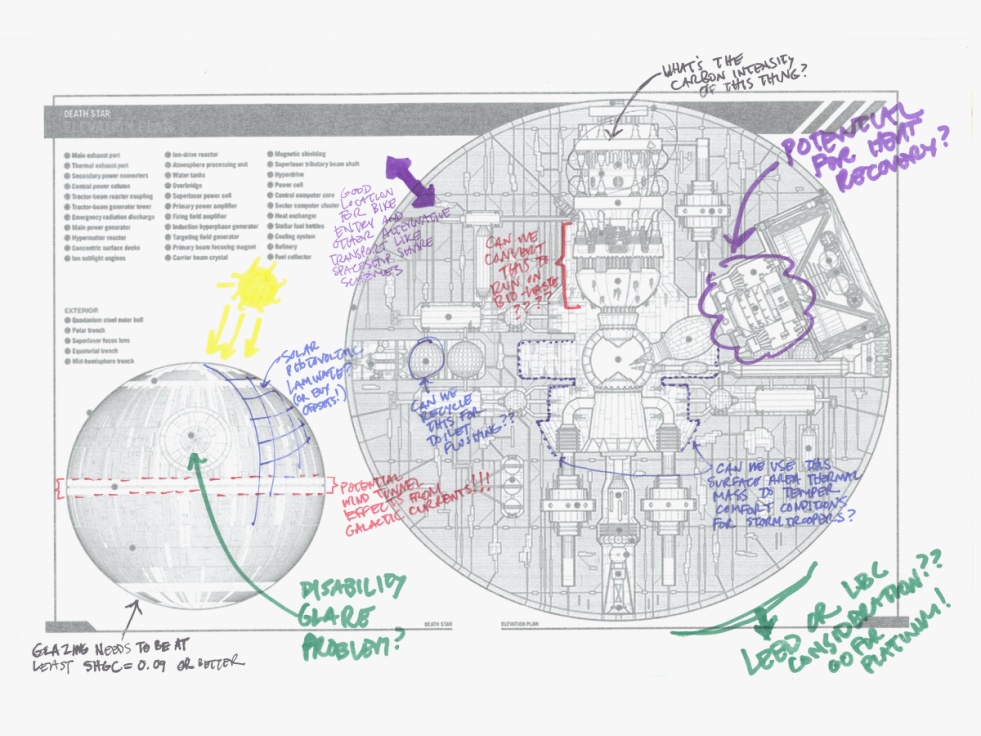






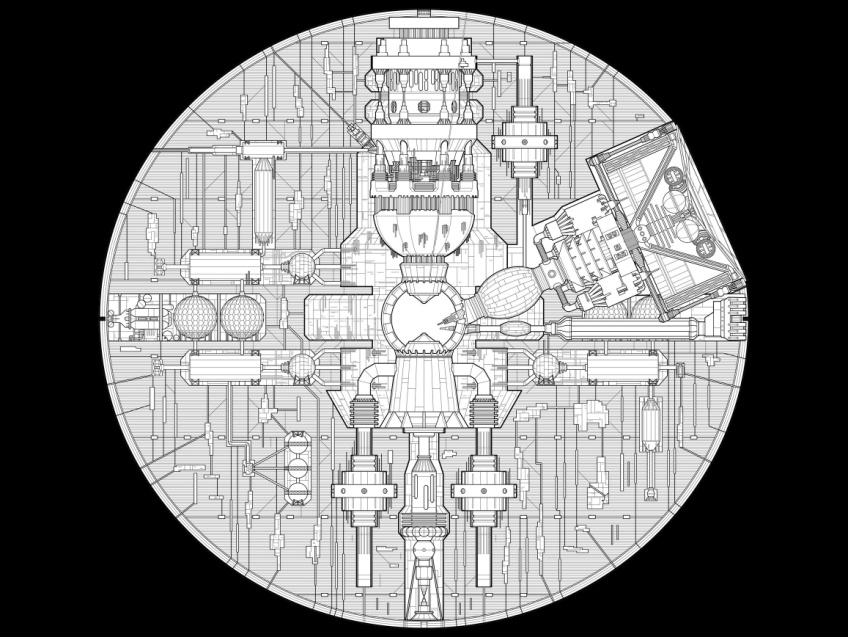


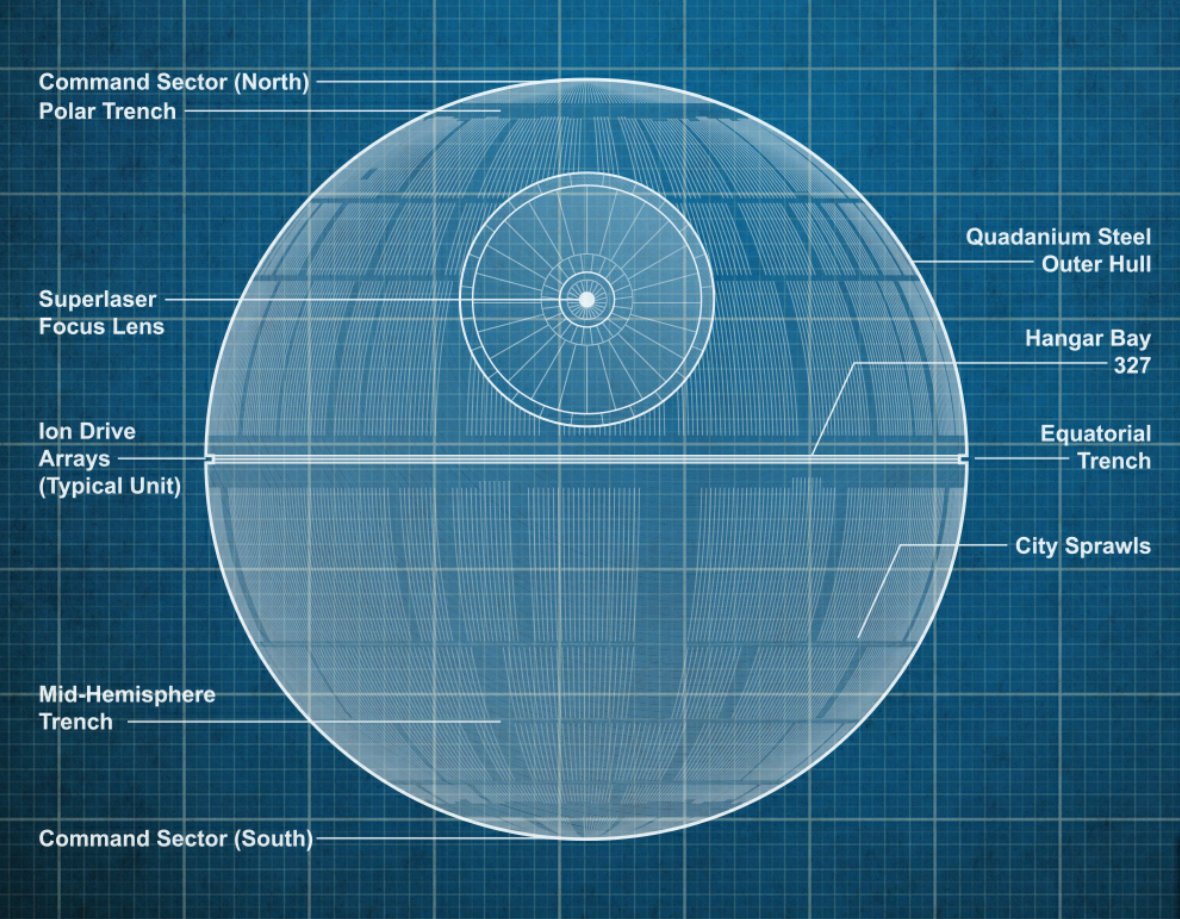


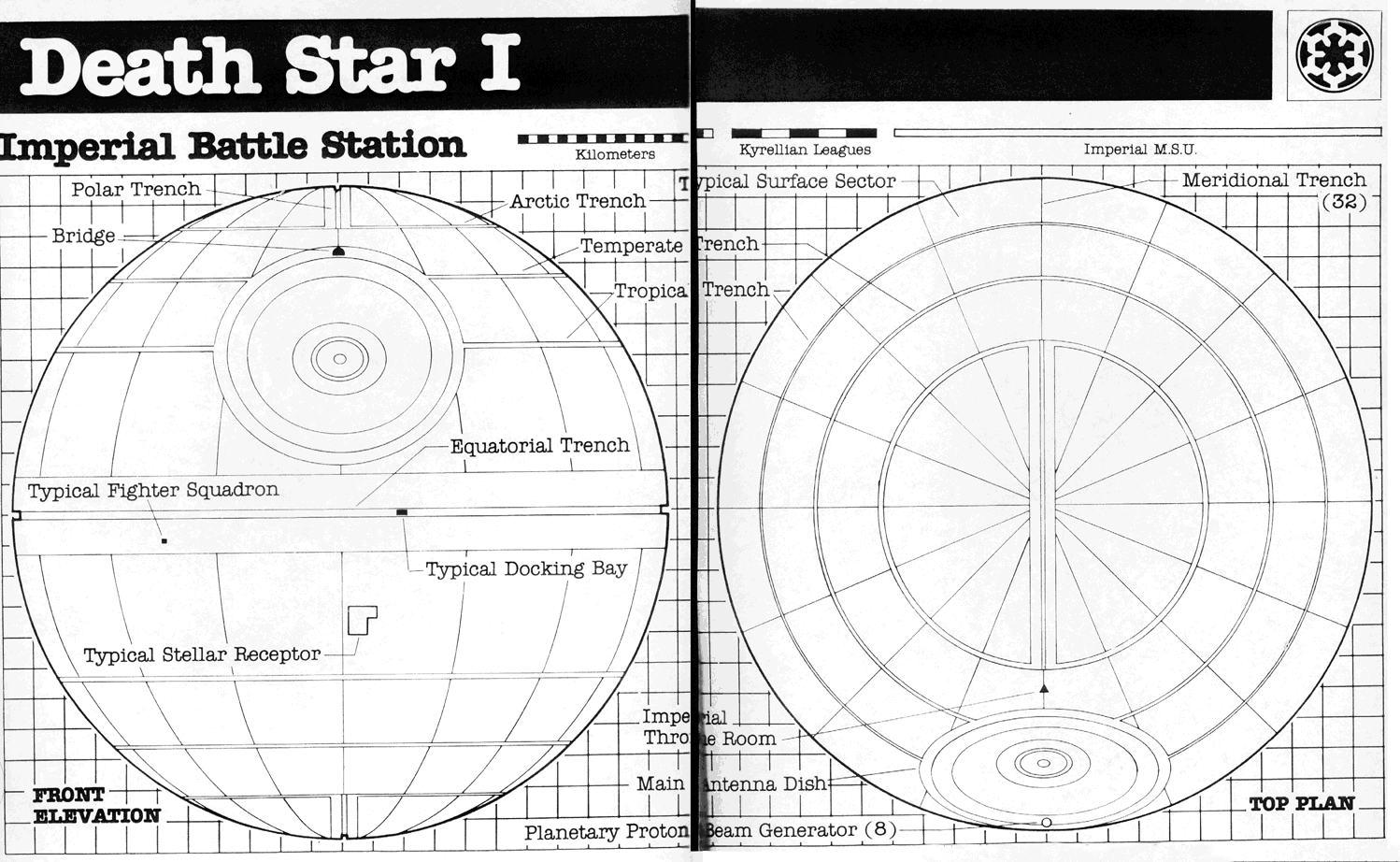


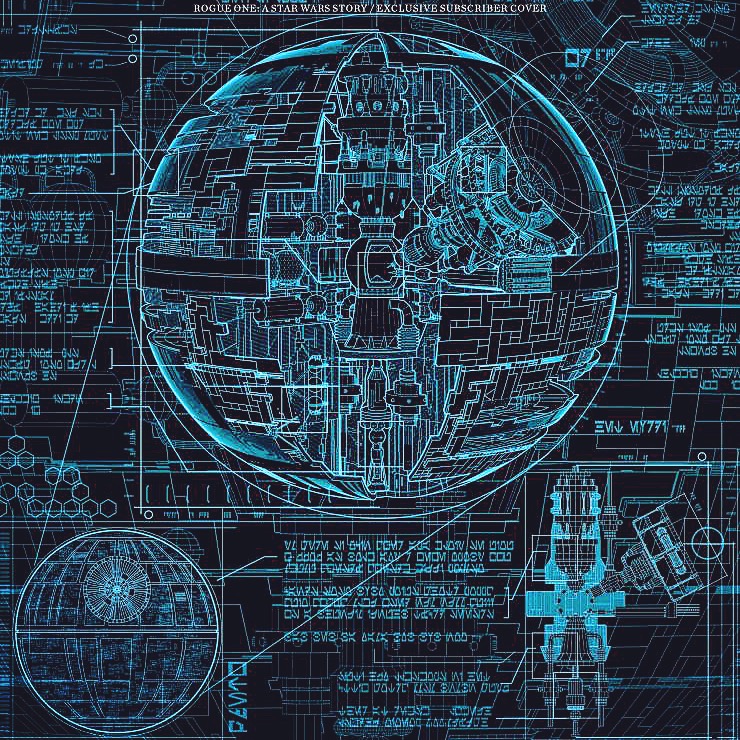












# Tools Used

## Wireshark

Wireshark is a very popular network analyzer. Wireshark was used to analyze the communication that the various malware found in the disk performed.

## Autopsy

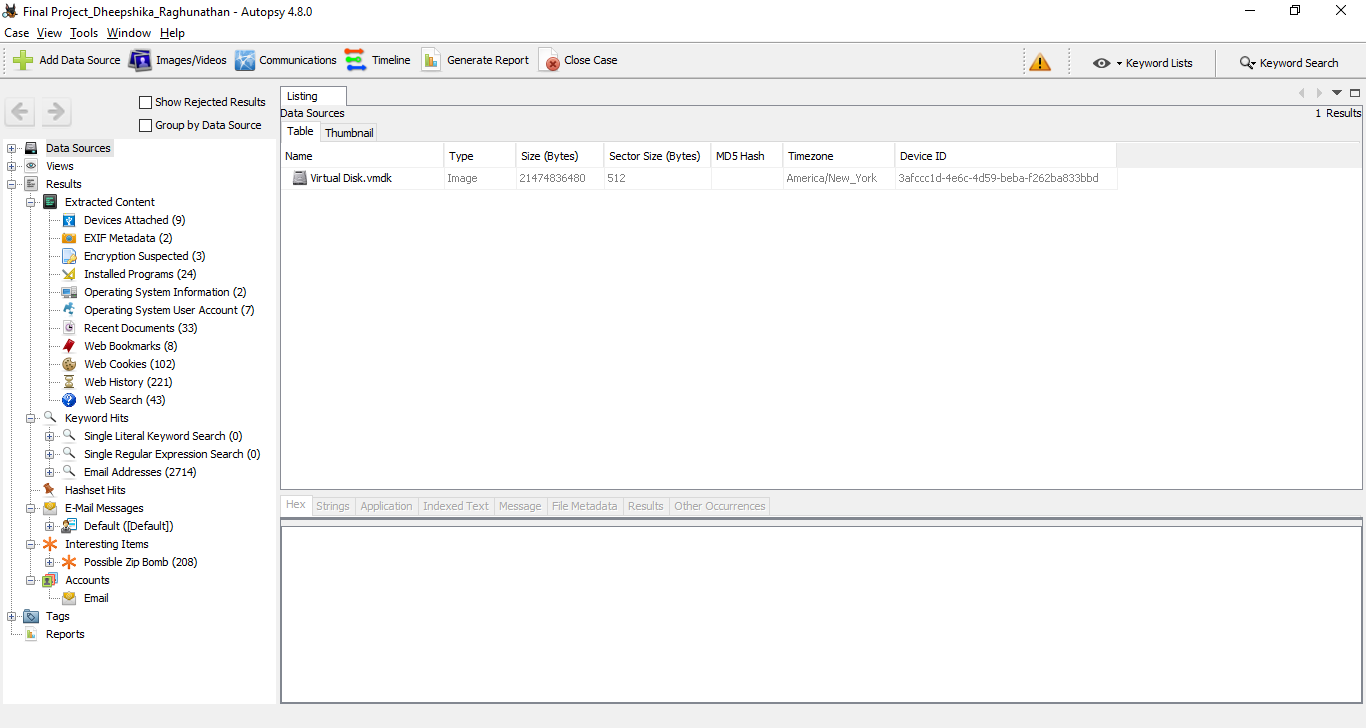
Autopsy is forensics software that has a graphical interface. Autopsy was used to analyse and extract the contents of the given drive.

## Veracrypt

During analysis it was found that the disk contained a volume which was encrypted using Veracrypt. Veracrypt is an open source encryption software that could be used to encrypt certain volumes in a disk.

# Analysis of Rebel Malware Writer’s Hard Disk

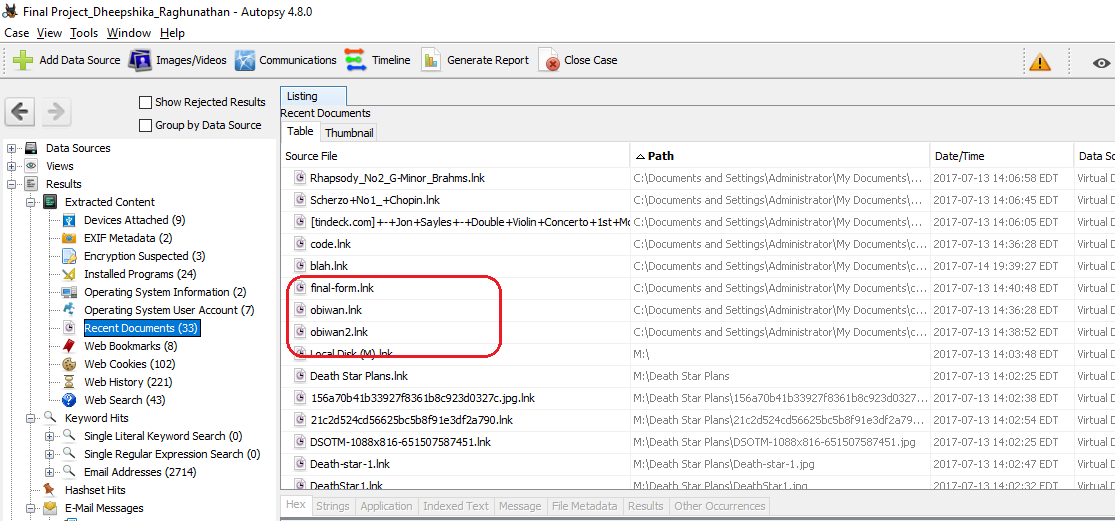
Initially the hard disk was opened using Autopsy and the contents in the hard disk were analysed.



While going through the Extracted Content, it was found that many of the files that were recently accessed were in the C:\ drive. It was also found that many of these files were in the M:\ drive, which could not be found on the disk initially.

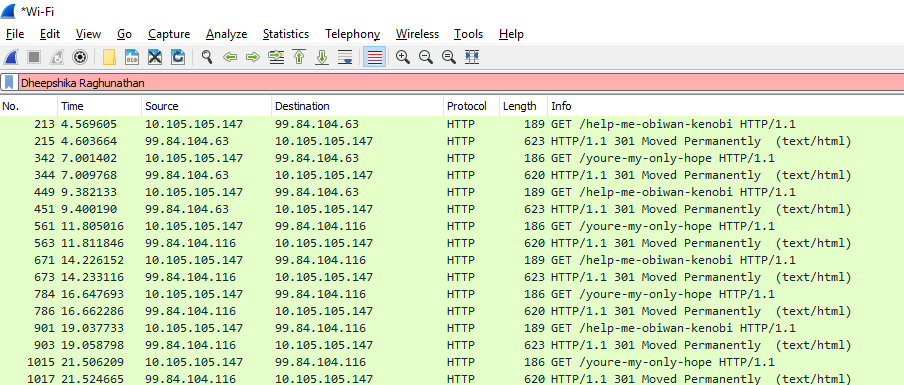
## Obiwan2.exe

While going through the Recent Documents in the Extracted Content, links to python files named obiwan.py, obiwan2.py and final-form.py were found.



In the corresponding drive location, there was another folder named **dist**, which contained 2 executables named obiwan.exe and obiwan2.exe.

On running obiwan.exe it was found that this malware sent the message “help-me-obiwan-kenobi” and “youre-my-only-hope” after 3 seconds. This was repeated every 2 seconds.



On running obiwan2.exe and capturing the packets using Wireshark, it was found that this malware was trying to communicate with a umd.edu host with IP address 99.84.104.63. It first sends the message,

This-is-not-even-my-final-form.

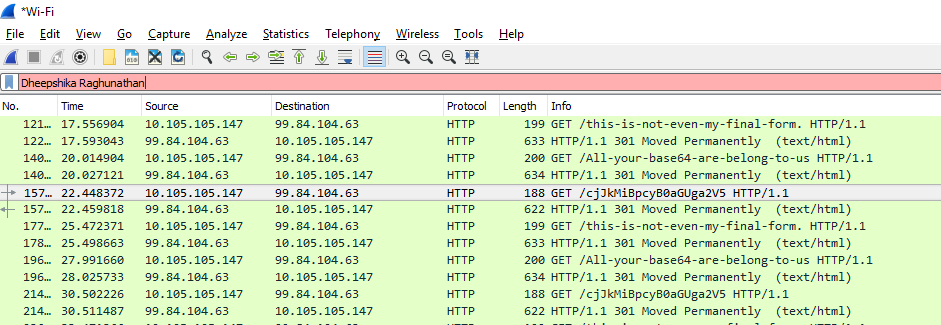
After 3 seconds, it sends its next message as below,

All-your-base64-are-belong-to-us

After 2 seconds, it sends the final message,

cjJkMiBpcyB0aGUga2V5

This process repeats every 3 seconds,

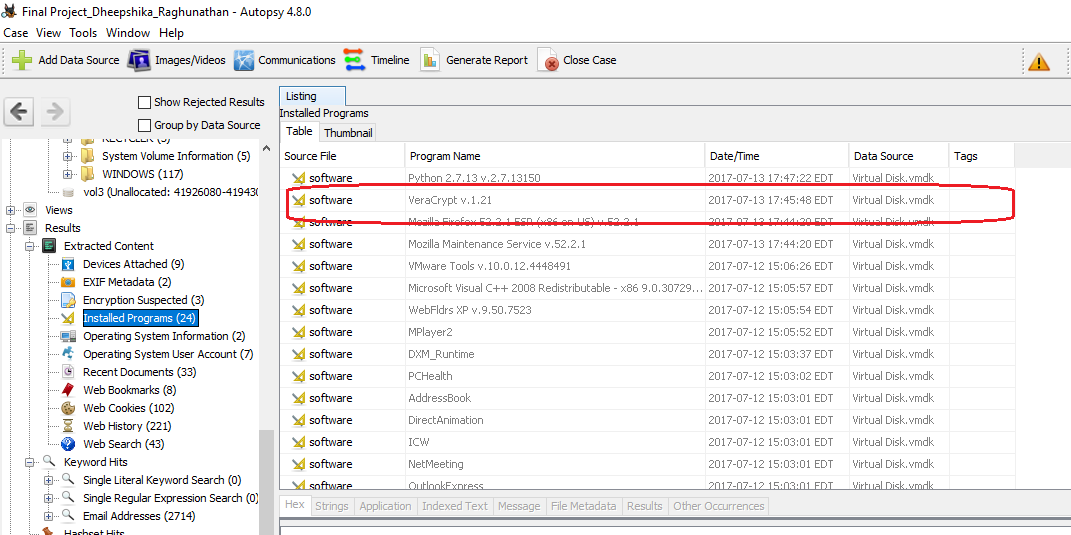


When a Base64 decoding of this message “cjJkMiBpcyB0aGUga2V5” is performed, it was decoded to “r2d2 is the key”.

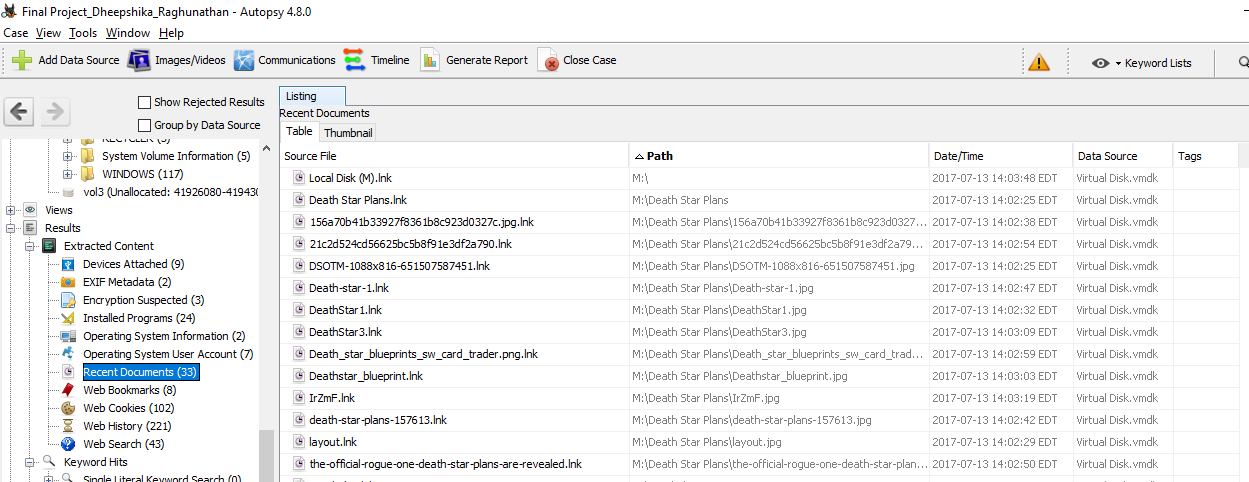
This could mean that “r2d2” is a key for some artefact in this disk.

## Veracrypt mounted volume

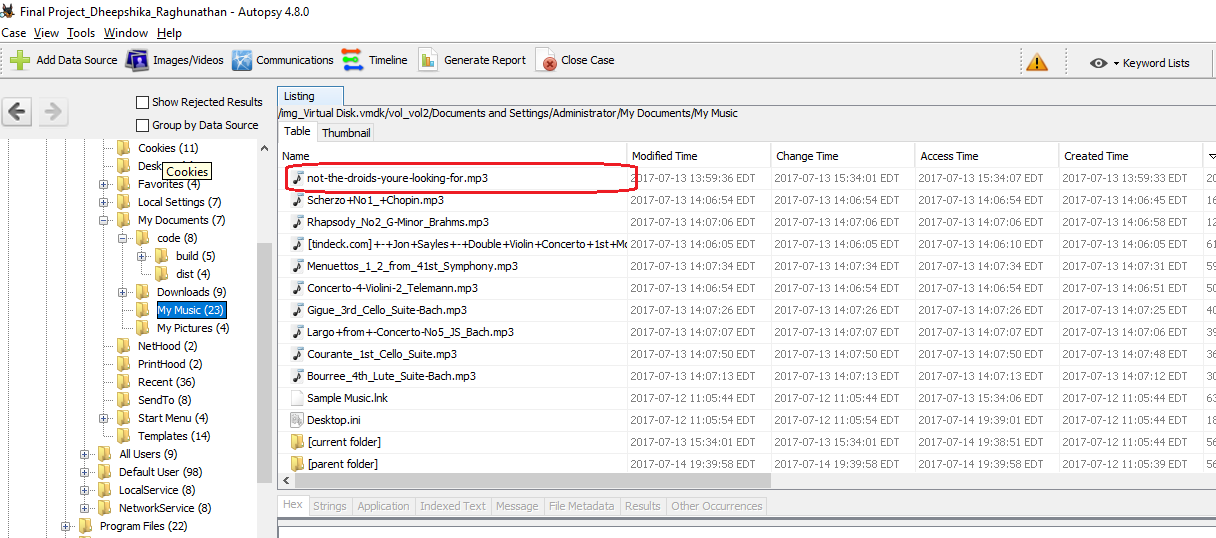
While going through the installed programs it was found that veracrypt was installed in this machine.



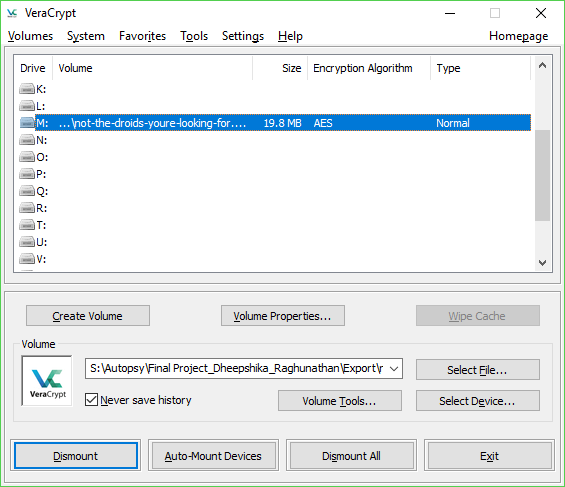
It was also found in the Recent Documents that many files from the M:\ drive was accessed. But this drive was not found in the drive.



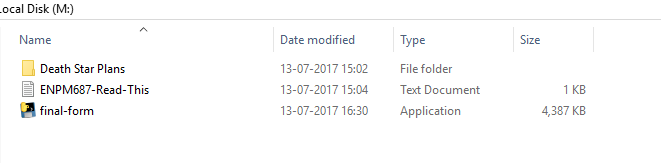
This means that there must be a volume in the disk that has been encrypted using Veracrypt. While searching for such a volume, it was found that the “My Music” contained a lot of the user’s music. A few of these files were of size in GBs. So when these files were played, there was one file which could not be played by the music player.



It turns out that this was also the biggest file in the folder. So this was extracted and decrypted using Veracrypt. From the above step, “r2d2” was used as the decryption password.



When this drive was opened, many files were found.



This drive contained a malware application called “final-form.exe”. On running this application while capturing the packets on Wireshark, it was found that this malware was communicating with umd.edu at IP address 99.84.104.24.



The malware sent the message “We-will-defeat-Darth-Vader.” and after 3 seconds it sends the message “We-have-the-blue-prints-to-the-Death-Star”. This process repeats periodically.

