Aayushi Dubey **UID: - 116934596**

ENPM687

Final Project: - Forensics Examination and Report

Summary.

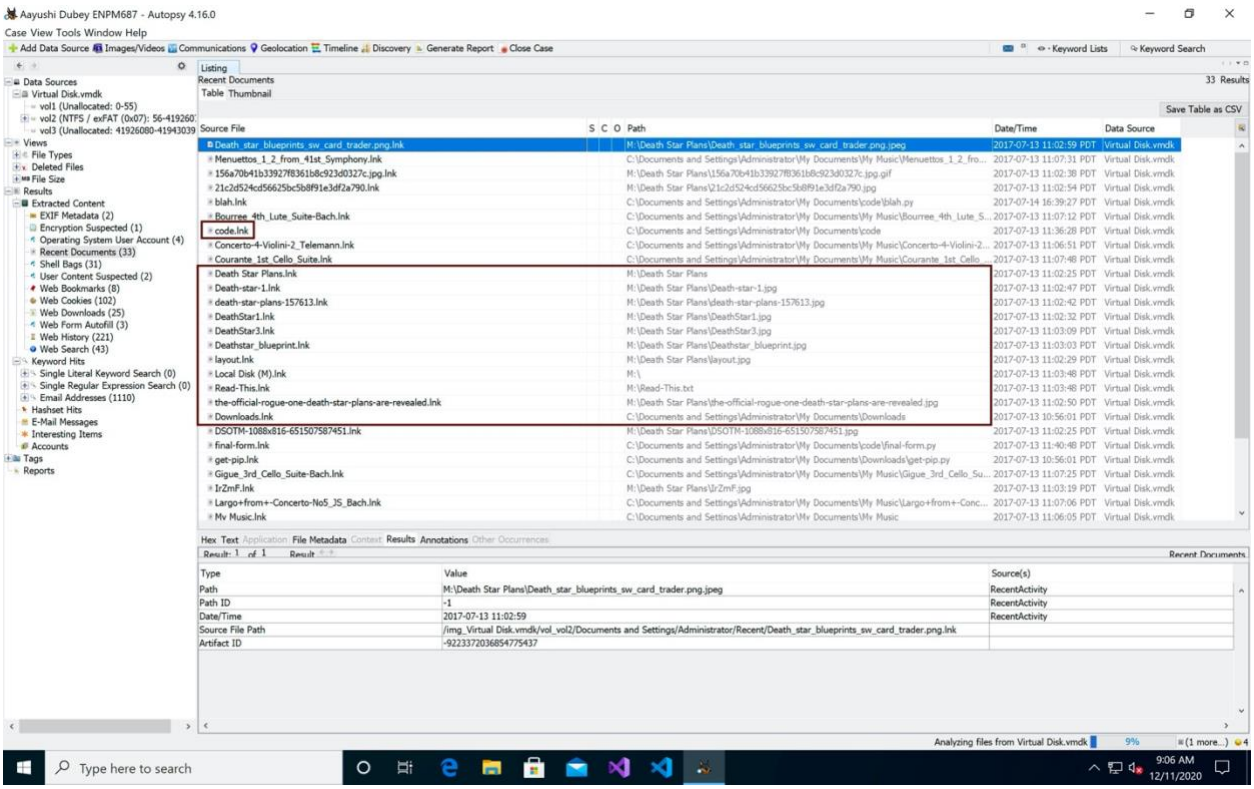
At a great cost the Imperial Army has come into possession of an image of a hard drive for a rebel scum malware writer. Their codes have plagued our computers for the last time, infecting them but also using it to send messages across the galaxy. The mission is to analyze the image of the Rebel malware writer hard drive. Find out what their newest "malware" does, any messages it may send out, and review the image for other useful intelligence. Is it trying to corrupt different files? What kind of messages it is trying to send? Where it is located what is its behavior? By making use of forensics tools and intelligence we have to investigate the scenario.

Tools used in this forensics investigation.

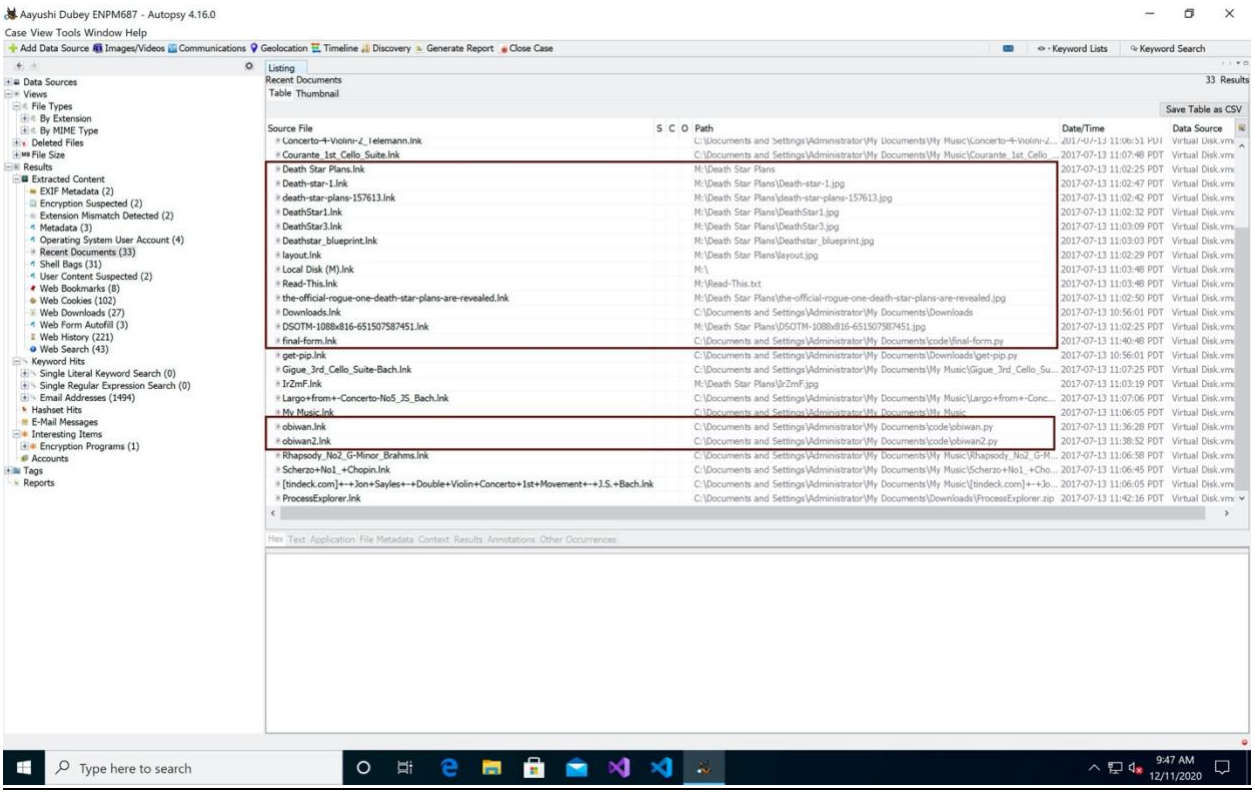
1. Autopsy.
2. Wireshark.
3. VeraCrypt.

Repository.

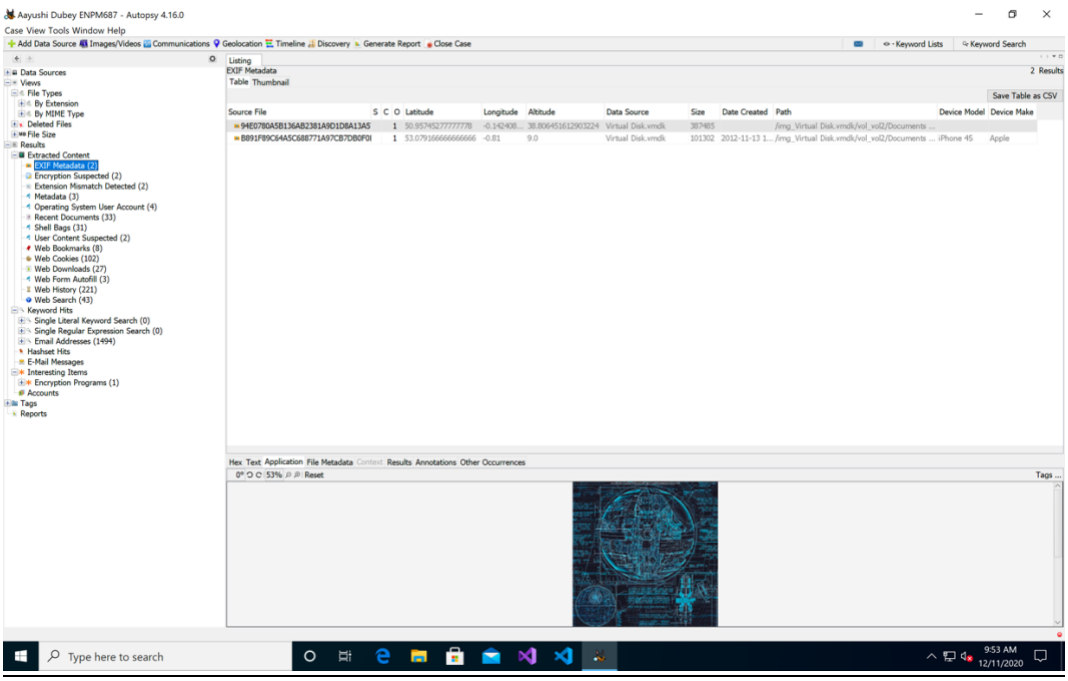
In this scenario I am going to find the final form of the malware that has infected Imperial Force's system and also sending message across the galaxy. I went through the hard drive and found the below evidences which can be really helpful to catch the final form of the malware sent by rebels.

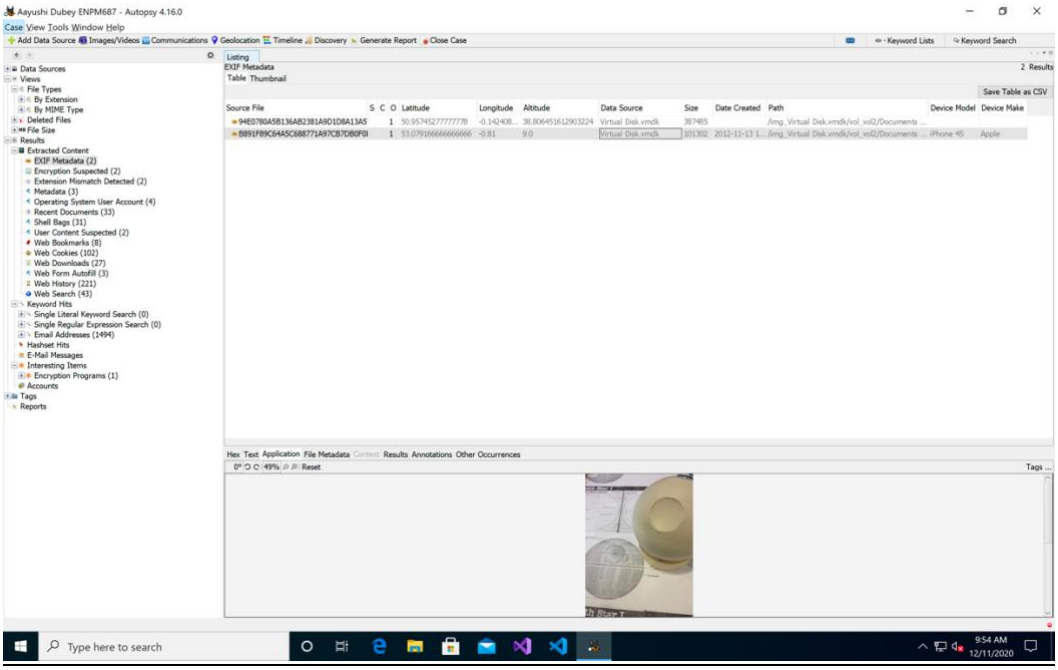


In “Recent Documents” folder I have found some interesting items code.lnk, death star plans, blueprint and many more things related to death star and those were accessed recently. There may be possibility that the death star plans were already leaked to the rebels.

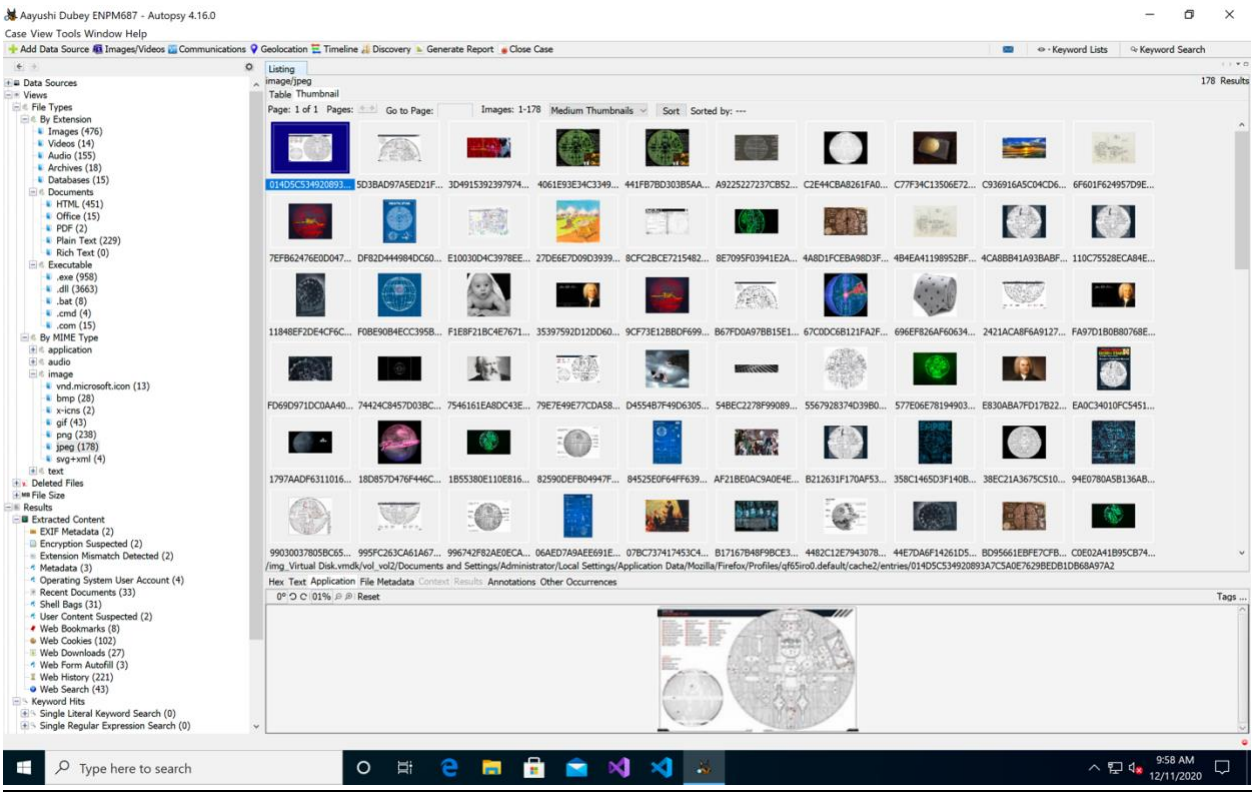


I have also found obiwan.lnk and obiwan2.lnk and final-form.lnk files which are python scripts and located in “My Documents” folder of the Administrator which is highly suspicious. These files may be the malwares. I have investigated further to find these files and other important evidence.

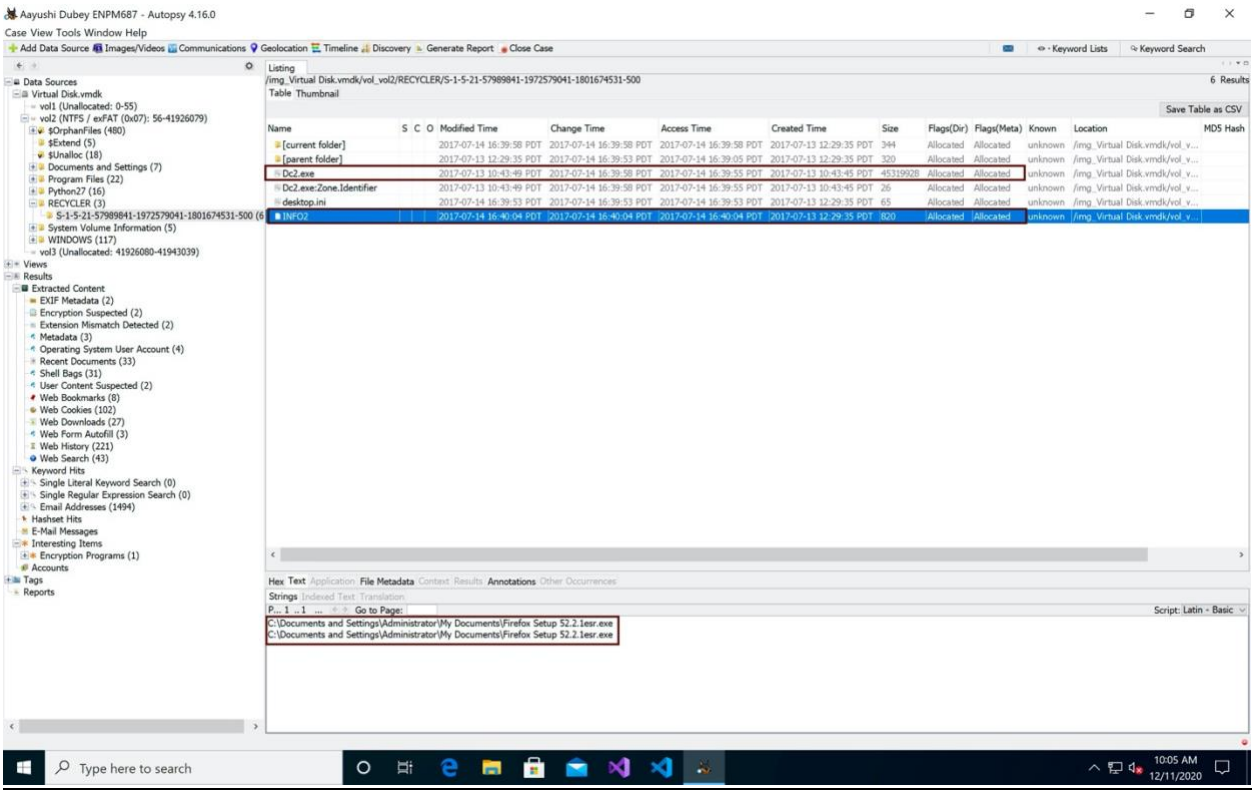




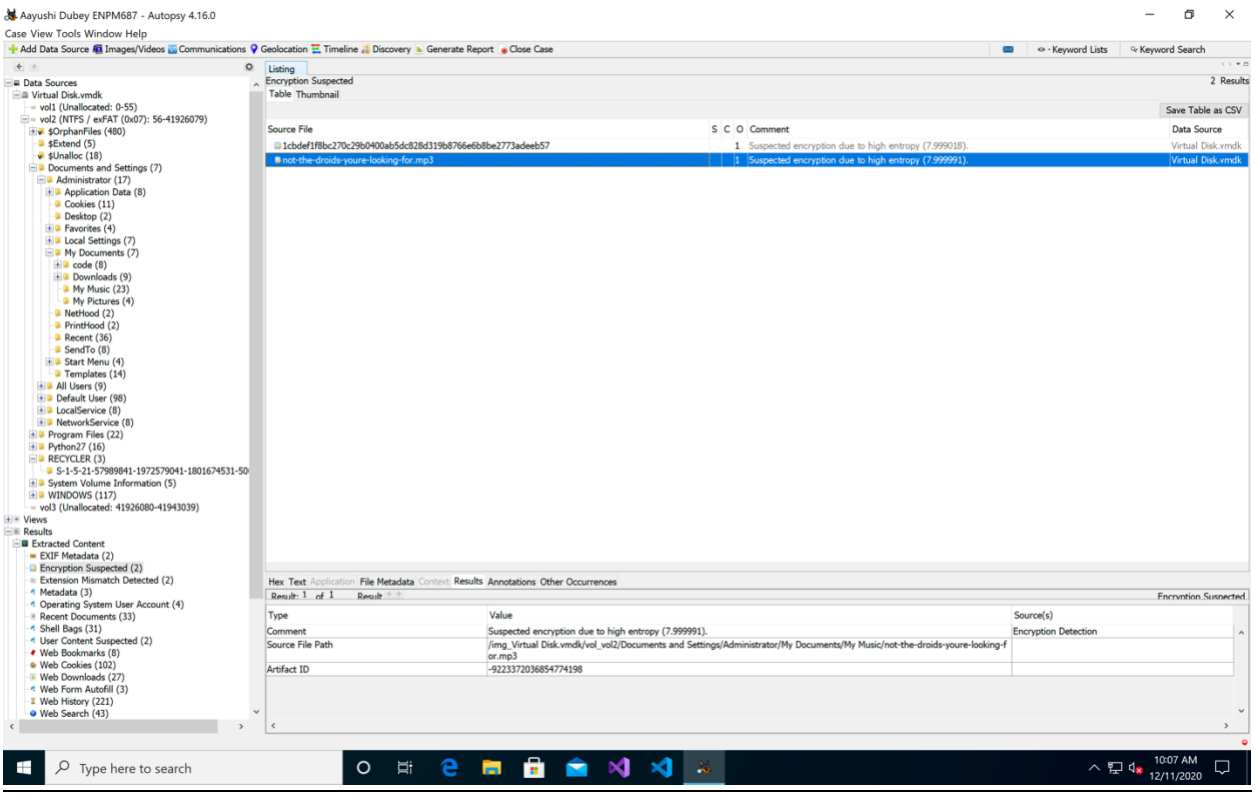
In the EXIF Metadata I found this image in document folder which is the Death star plan. So, I can say that the blueprints/plans of the death star may have been compromised.



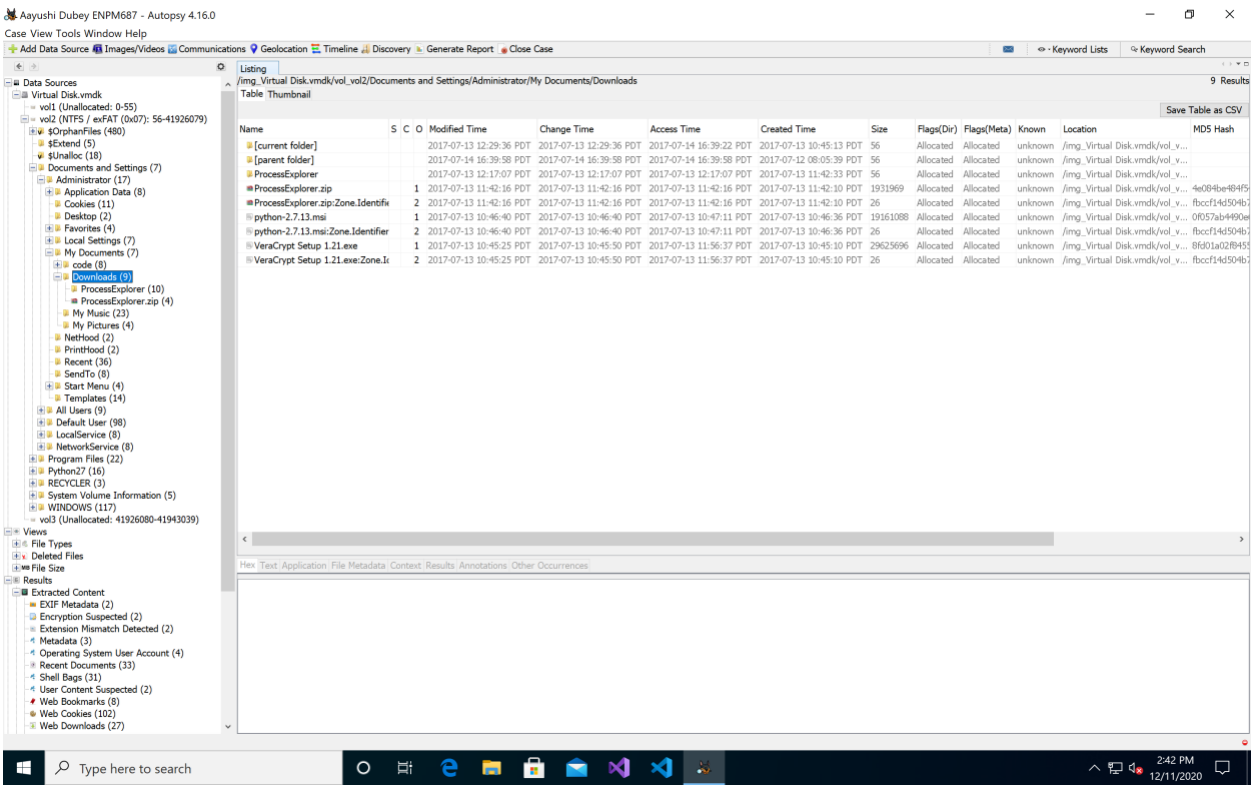
The death star plans are located in the cache section of Firefox.



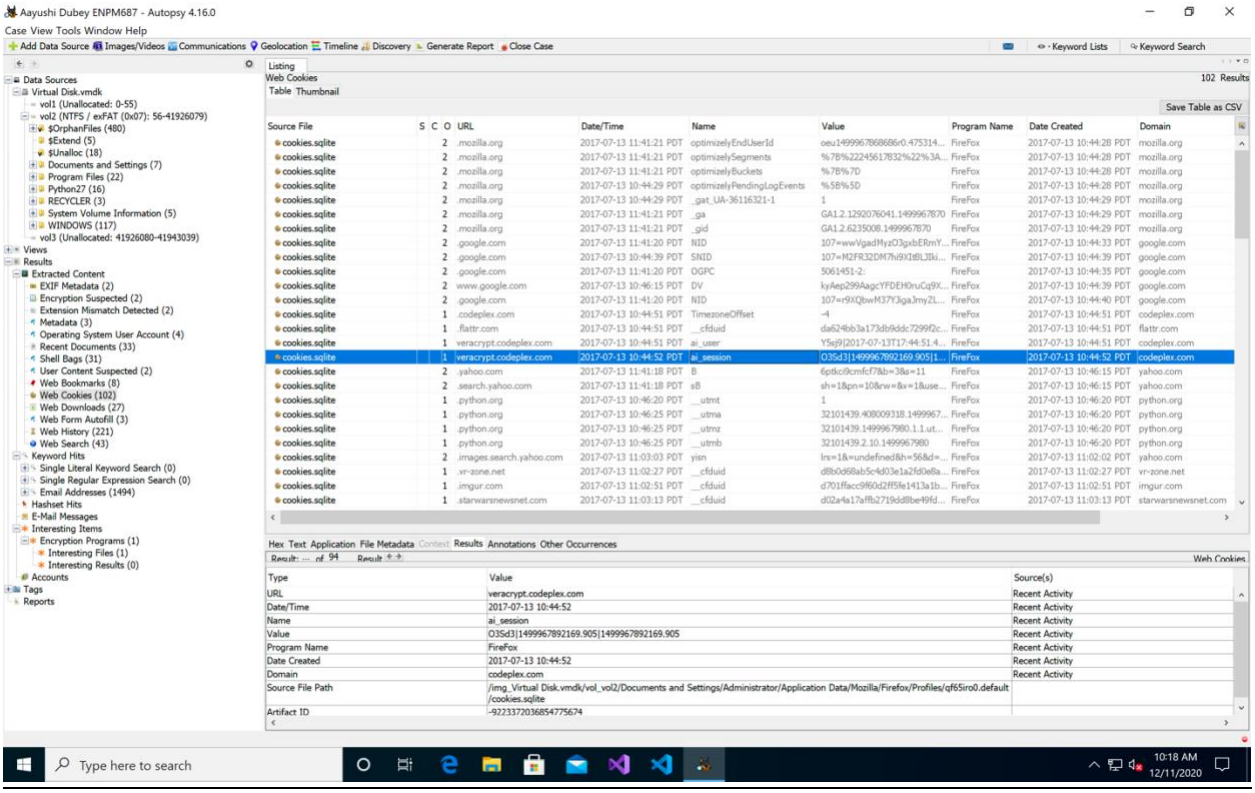
I have also checked the recycler folder if that can give me some useful evidence but found only a deleted installer executable of Firefox. Which was deleted from “My Documents:” folder of Administrator.



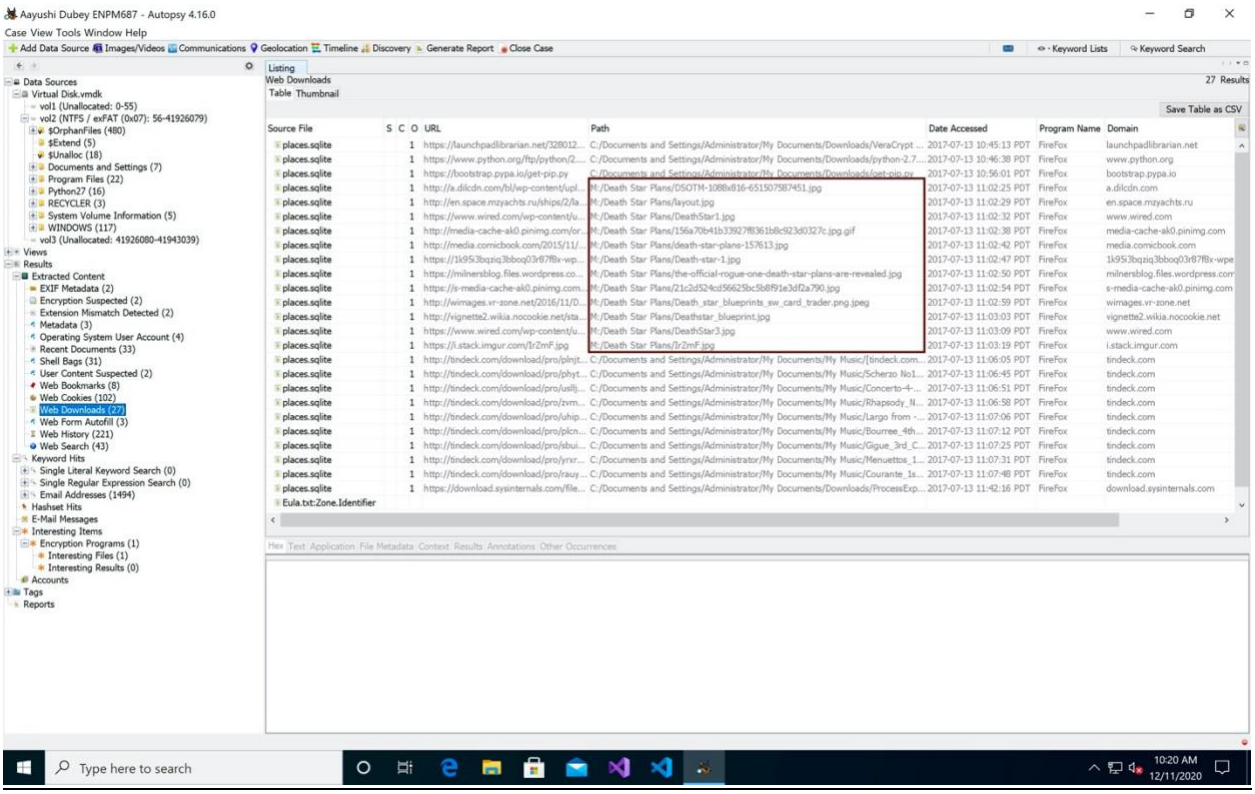
I went through “Encryption suspected” folder which is located under result and found 2 files in which one file named is not-the-droids-you-are-looking-for which is a mp3 file this is encrypted as suspected by autopsy. The other file is system’s file.



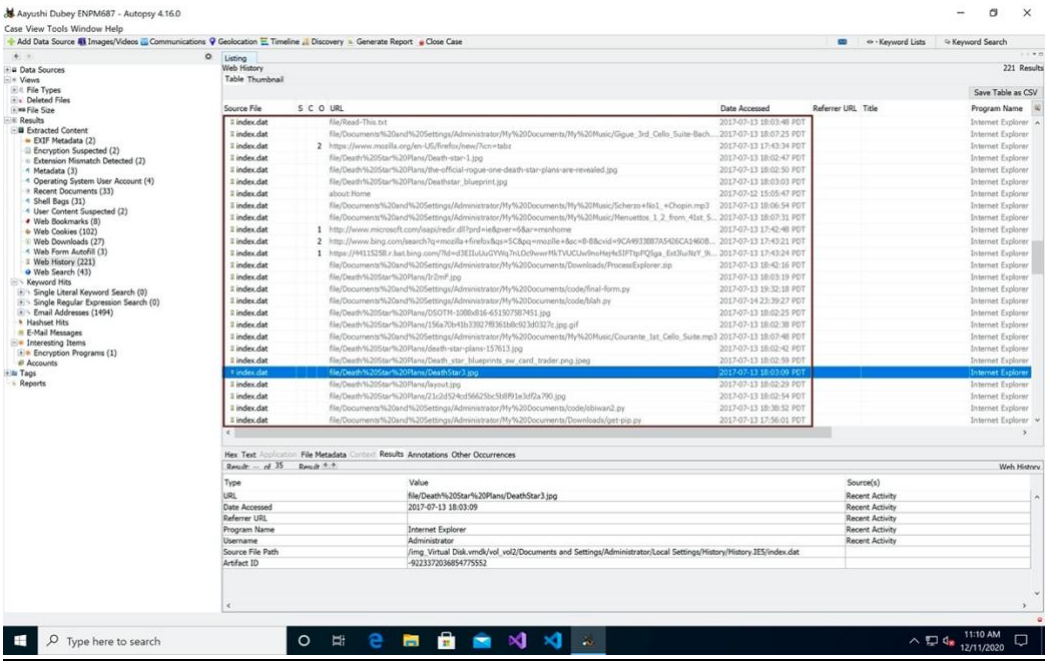
When I checked the Downloads item on the disk and found that VeraCrypt was installed in the system so there may be a possibility that the mp3 file that was found above was encrypted by VeraCrypt.

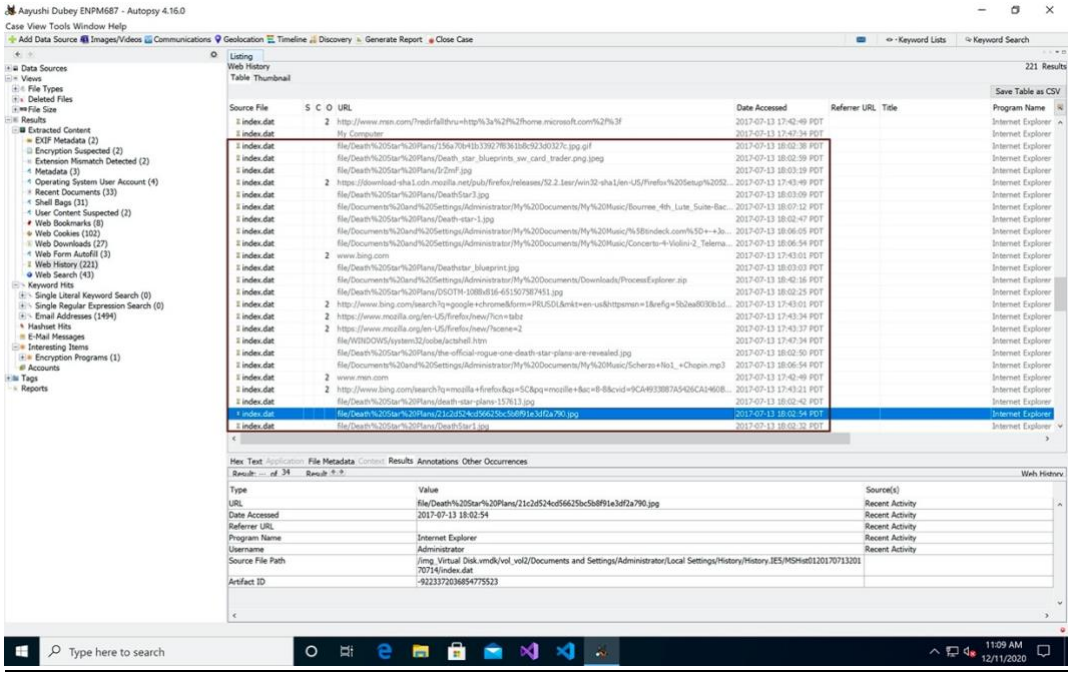


Found VeraCrypt in cookies.

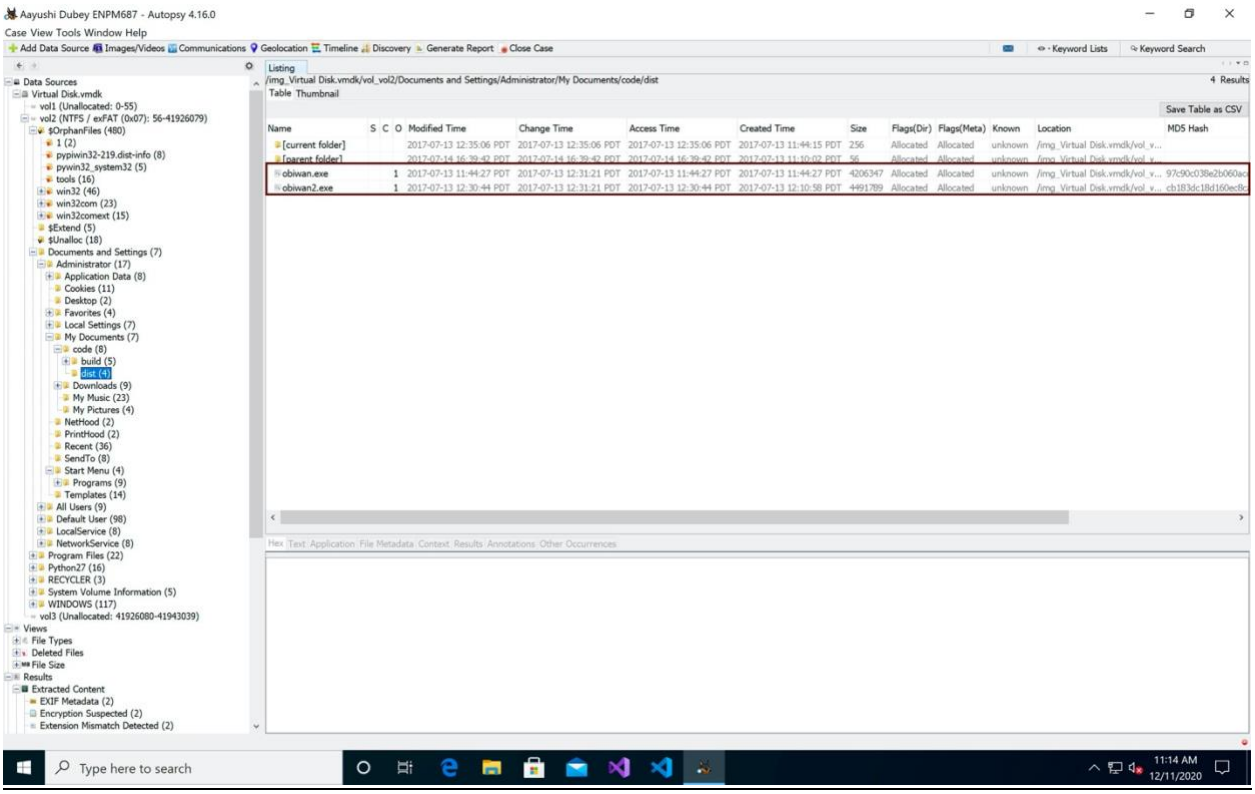


I found some suspicious things under web downloads like the death star plans are located in some M drive.

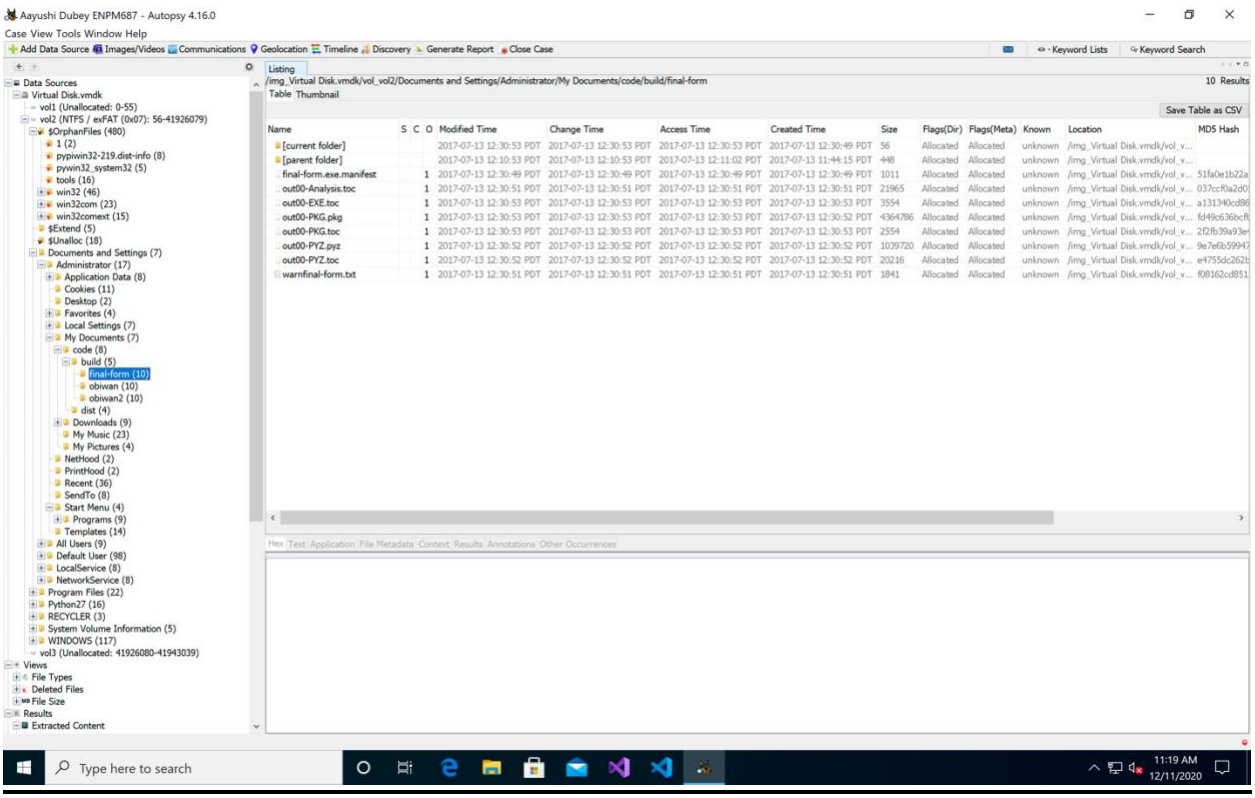




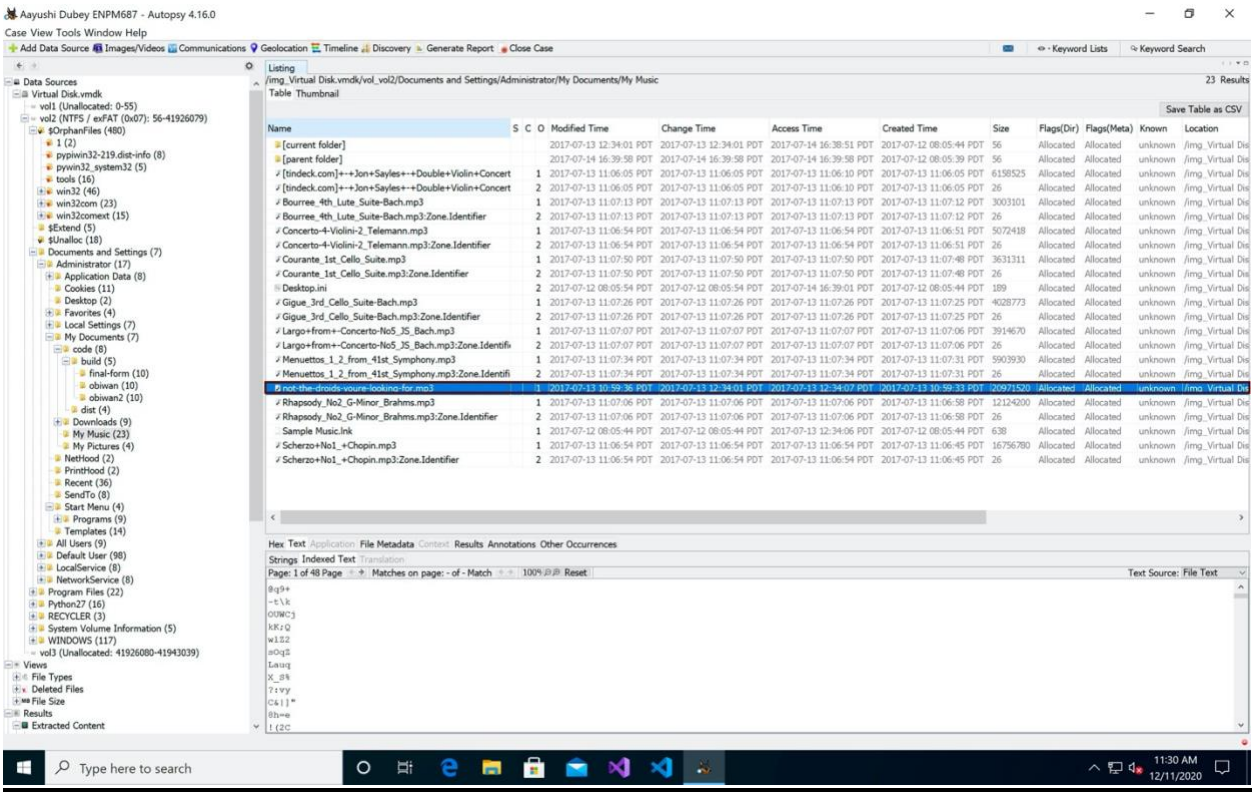
Found some useful files related to the plans of Death Star in the history section of internet explorer.



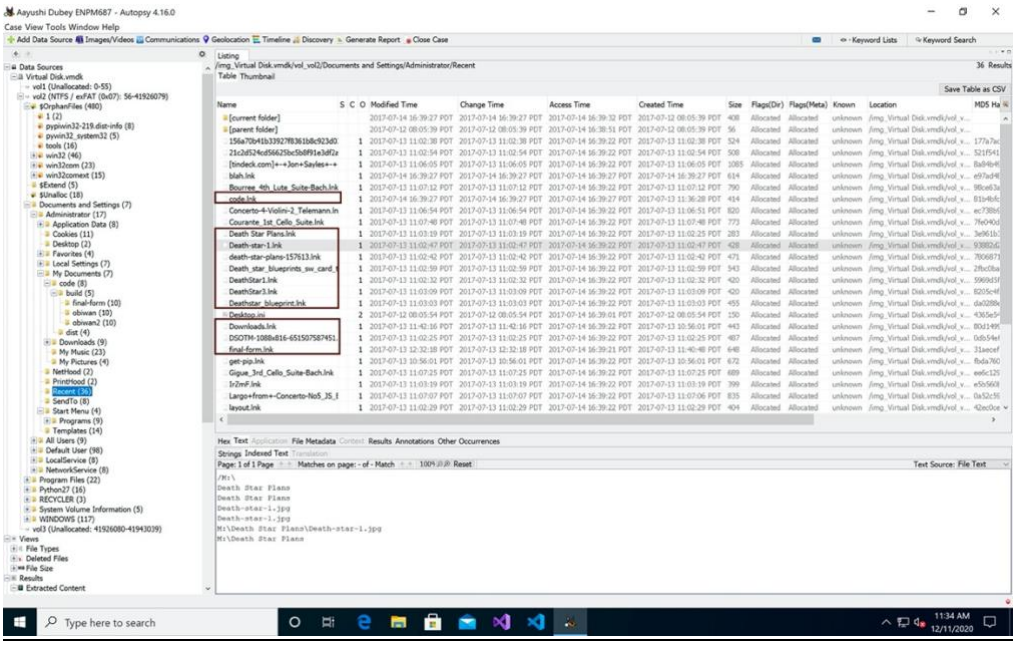
I found some interesting things in Administrator's "My Documents" folder which was obiwan.exe and obiwan2.exe under dist. folder.

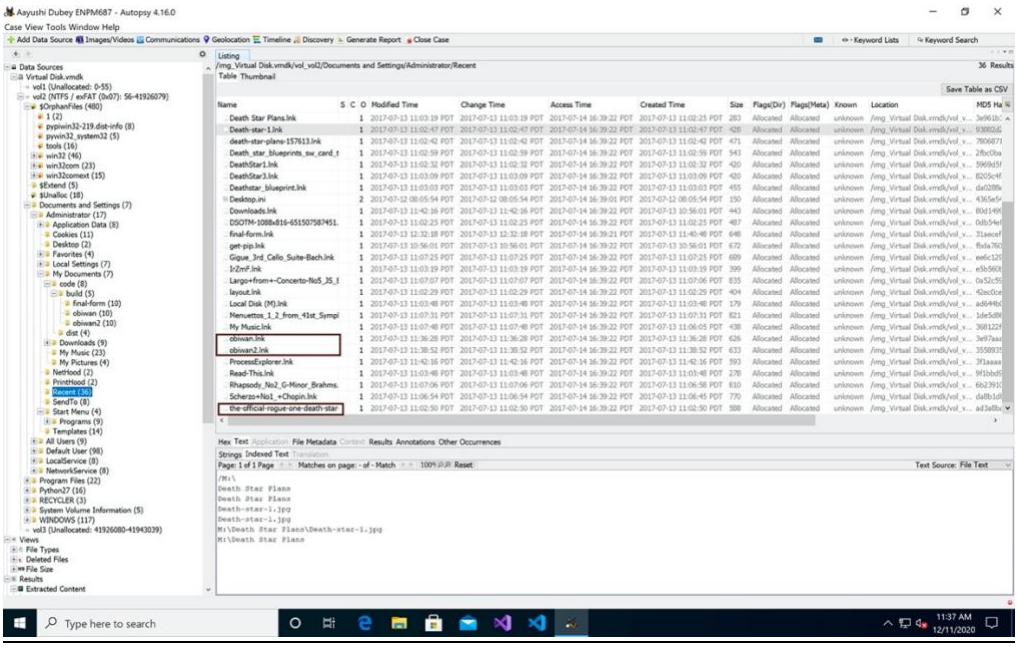


In the same location I have also found 3 folders under the folder named “build” and those 3 folder names are final form, obiwan and obiwan2. They were only the part of code. This is highly likely that obiwan.exe, obiwan2.exe files are malwares also I was only able to find the package of the application named final form which may have used to build the malware.



After analyzing “My Music” folder and extract the mp3 file named not-the-droids-you-are-looking-for. Which was suspected an encrypted file by autopsy. This can be a helpful evidence in future.



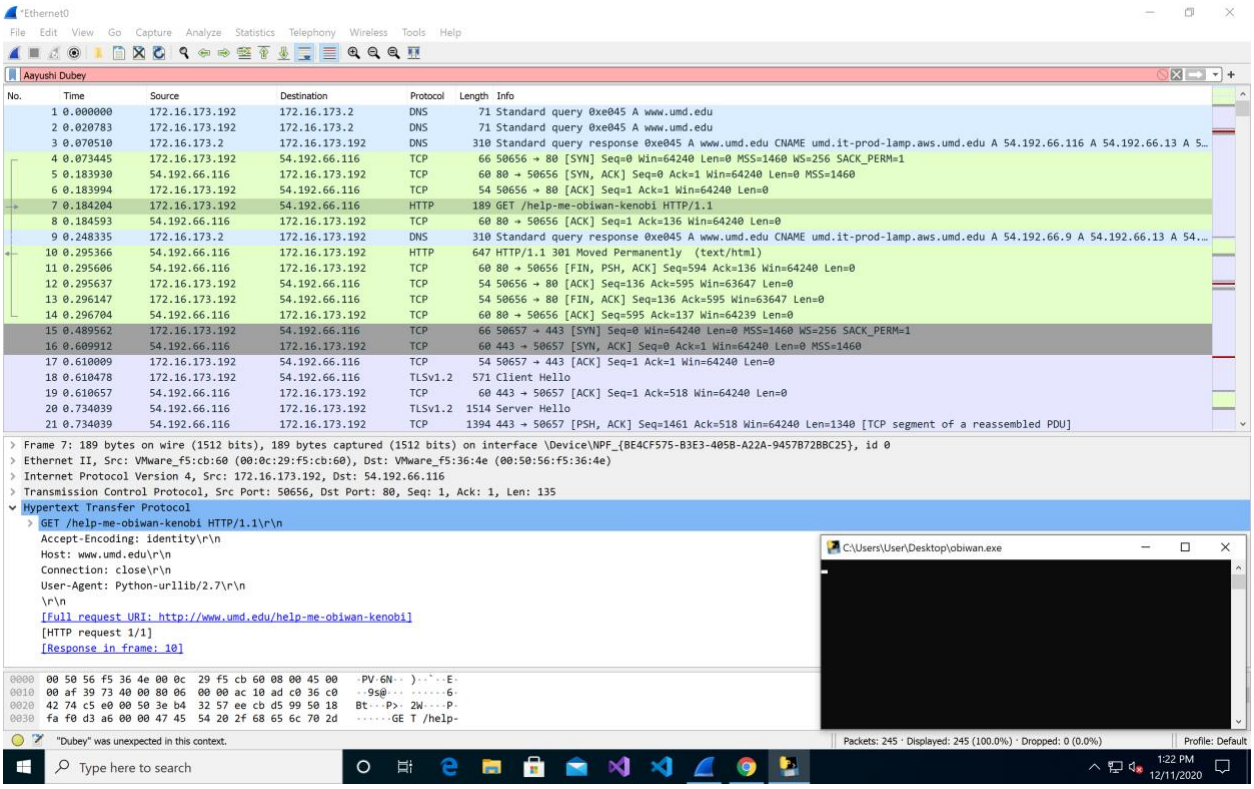


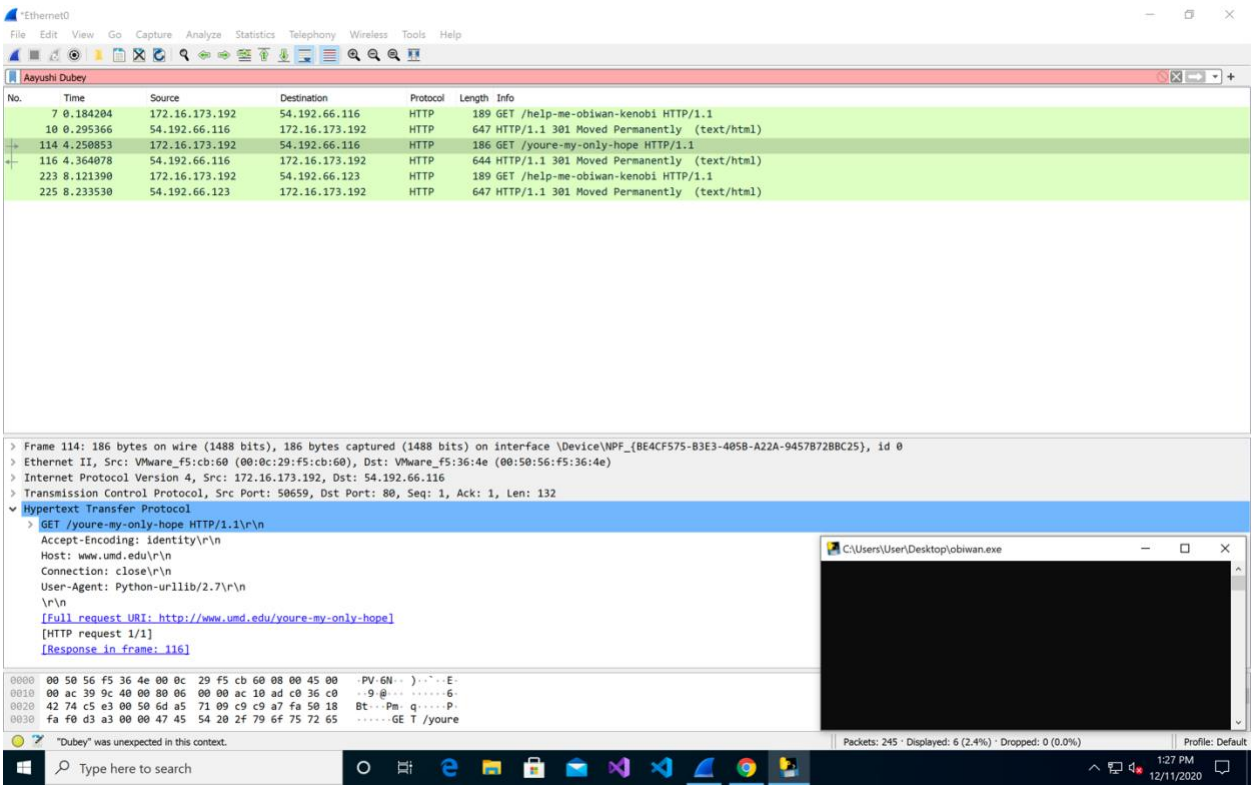
After analyzing recent folder, I found more useful things which may have been access by rebel's malware writer recently and found many useful things like death star plans, code folder, death star blueprints etc. Important/interesting things are highlighted.

Analysis of Evidence found: - Three important files which I have extracted from the rebel's malware writer's disk.

1. Obiwan.exe
2. Obiwan2.exe
3. Not-the-droids-you-are-looking-for.mp3

The first 2 files are executable files which have higher chances that these are the malwares. I analyzed obiwan.exe file and checked the behavior of this file to check if it was sending any messages across the galaxy. I used Wireshark for this analysis.



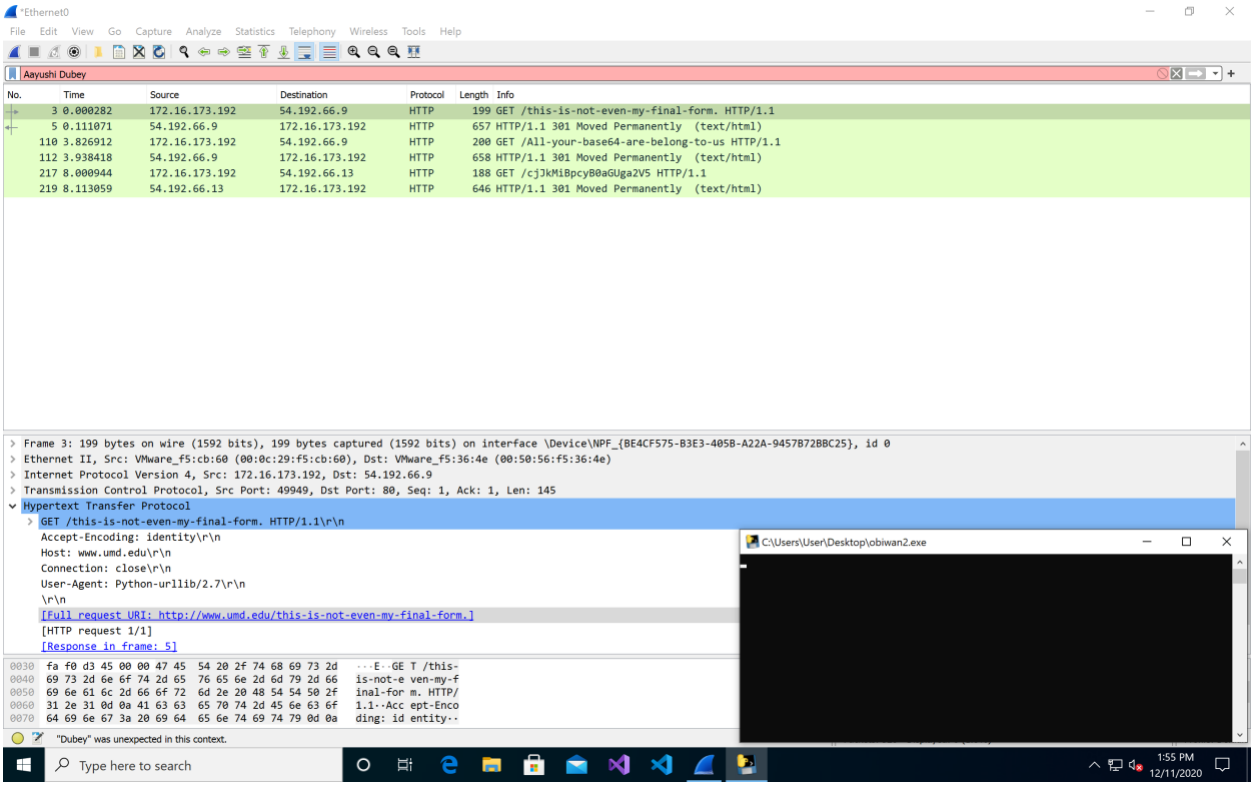


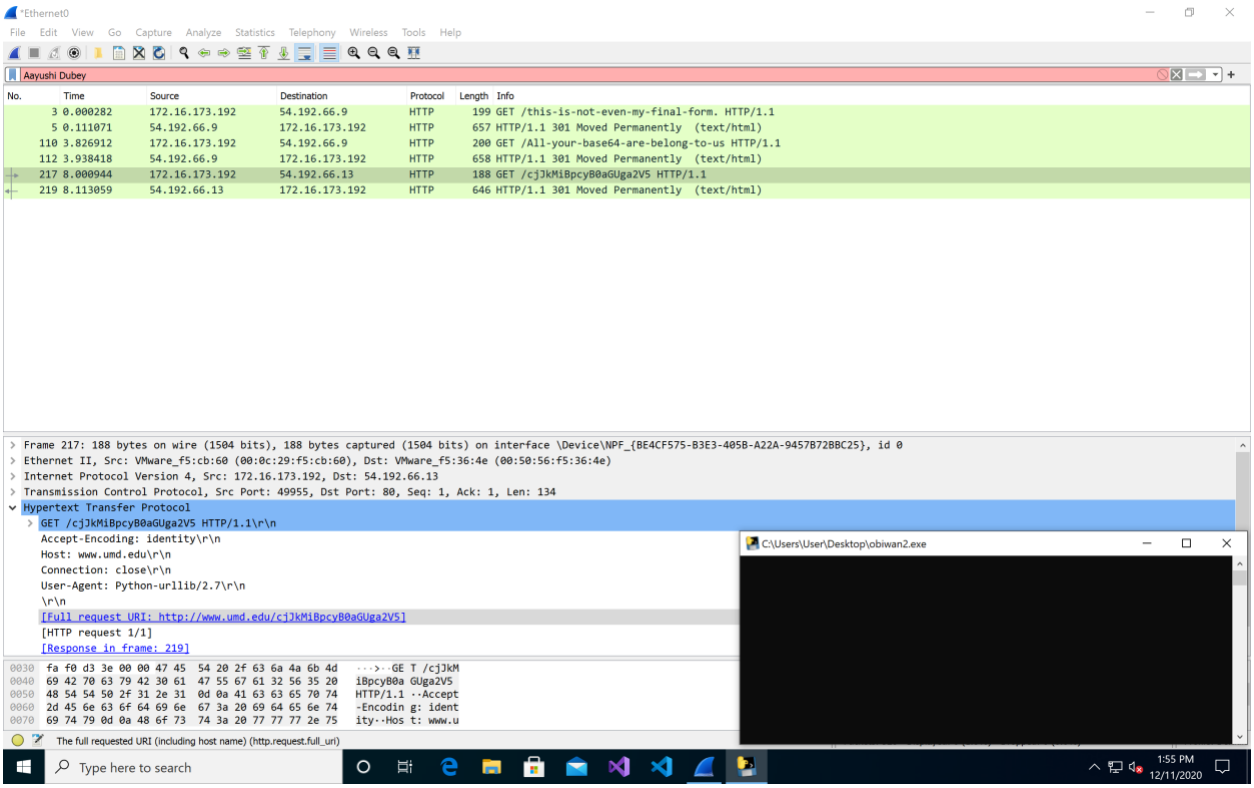
I have found that when this exe file running it is trying to connect to two URL's:

http://www.umd.edu/youre-my-only-hope

http://www.umd.edu/help-me-obiwan-kenobi

These websites are giving http code 301 moved permanently means these websites doesn't host on www.umd.edu server anymore. This message must have sent by Rebels to the Jedi obiwan asking for help.

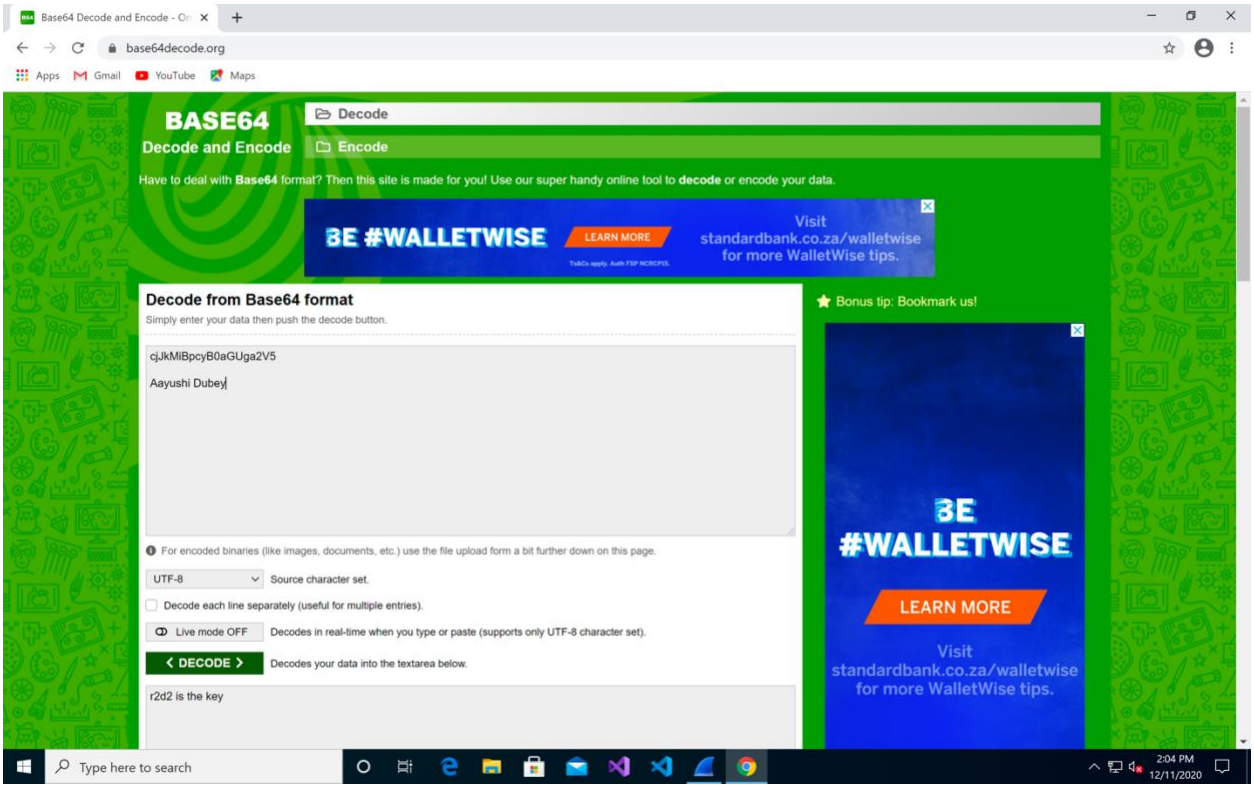

*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Aayushi Dubey
No. Time Source Destination Protocol Length Info
3 0.000282 172.16.173.192 54.192.66.9 HTTP 199 GET /this-is-not-even-my-final-form. HTTP/1.1
5 0.111071 54.192.66.9 172.16.173.192 HTTP 657 HTTP/1.1 301 Moved Permanently (text/html)
110 3.826912 172.16.173.192 54.192.66.9 HTTP 200 GET /All-your-base64-are-belong-to-us HTTP/1.1
112 3.938418 54.192.66.9 172.16.173.192 HTTP 658 HTTP/1.1 301 Moved Permanently (text/html)
217 8.000944 172.16.173.192 54.192.66.13 HTTP 188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
219 8.113059 54.192.66.13 172.16.173.192 HTTP 646 HTTP/1.1 301 Moved Permanently (text/html)
Frame 3: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF_{BE4CF575-B3E3-405B-A22A-9457B72BBC25}, id 0
Ethernet II, Src: VMware_f5:cb:60 (00:0c:29:f5:cb:60), Dst: VMware_f5:36:4e (00:50:56:f5:36:4e)
Internet Protocol Version 4, Src: 172.16.173.192, Dst: 54.192.66.9
Transmission Control Protocol, Src Port: 49949, Dst Port: 80, Seq: 1, Ack: 1, Len: 145
Hypertext Transfer Protocol
GET /this-is-not-even-my-final-form. HTTP/1.1\r\n
Accept-Encoding: identity\r\n
Host: www.umd.edu\r\n
Connection: close\r\n
User-Agent: Python-urllib/2.7\r\n
\r\n
[Full request URI: http://www.umd.edu/this-is-not-even-my-final-form.]
[HTTP request 1/1]
[Response in frame: 5]
0030 fa f0 d3 45 00 00 47 45 54 20 2f 74 68 69 73 2d ···E··GE T /this-
0040 69 73 2d 6e 6f 74 2d 65 76 65 6e 2d 6d 79 2d 66 is-not-e ven-my-f
0050 69 6e 61 6c 2d 66 6f 72 6d 2e 20 48 54 54 50 2f inal-for m. HTTP/
0060 31 2e 31 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 1.1··Acc ept-Enco
0070 64 69 6e 67 3a 20 69 64 65 6e 74 69 74 79 0d 0a ding: id entity··
C:\Users\User\Desktop\obiwan2.exe
"Dubey" was unexpected in this context.
Type here to search
1:55 PM
12/11/2020


*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Aayushi Dubey
No. Time Source Destination Protocol Length Info
3 0.000282 172.16.173.192 54.192.66.9 HTTP 199 GET /this-is-not-even-my-final-form. HTTP/1.1
5 0.111071 54.192.66.9 172.16.173.192 HTTP 657 HTTP/1.1 301 Moved Permanently (text/html)
110 3.826912 172.16.173.192 54.192.66.9 HTTP 200 GET /All-your-base64-are-belong-to-us HTTP/1.1
112 3.938418 54.192.66.9 172.16.173.192 HTTP 658 HTTP/1.1 301 Moved Permanently (text/html)
217 8.000944 172.16.173.192 54.192.66.13 HTTP 188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
219 8.113059 54.192.66.13 172.16.173.192 HTTP 646 HTTP/1.1 301 Moved Permanently (text/html)
Frame 217: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface \Device\NPF_{BE4CF575-B3E3-405B-A22A-9457B72BBC25}, id 0
Ethernet II, Src: VMware_f5:cb:60 (00:0c:29:f5:cb:60), Dst: VMware_f5:36:4e (00:50:56:f5:36:4e)
Internet Protocol Version 4, Src: 172.16.173.192, Dst: 54.192.66.13
Transmission Control Protocol, Src Port: 49955, Dst Port: 80, Seq: 1, Ack: 1, Len: 134
Hypertext Transfer Protocol
GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1\r\n
Accept-Encoding: identity\r\n
Host: www.umd.edu\r\n
Connection: close\r\n
User-Agent: Python-urllib/2.7\r\n
\r\n
[Full request URI: http://www.umd.edu/cjJkMiBpcyB0aGUga2V5]
[HTTP request 1/1]
[Response in frame: 219]
0030 fa f0 d3 3e 00 00 47 45 54 20 2f 63 6a 4a 6b 4d ···>··GE T /cjJkM
0040 69 42 70 63 79 42 30 61 47 55 67 61 32 56 35 20 iBpcyB0a GUga2V5
0050 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 HTTP/1.1 ··Accept
0060 2d 45 6e 63 6f 64 69 6e 67 3a 20 69 64 65 6e 74 -Encodin g: ident
0070 69 74 79 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 75 ity··Hos t: www.u
C:\Users\User\Desktop\obiwan2.exe
The full requested URI (including host name) (http.request.full_uri)
Type here to search
1:55 PM
12/11/2020

From the captured network data analysis sent by obiwan2.exe I have found that this file is trying to connect to 3 websites.

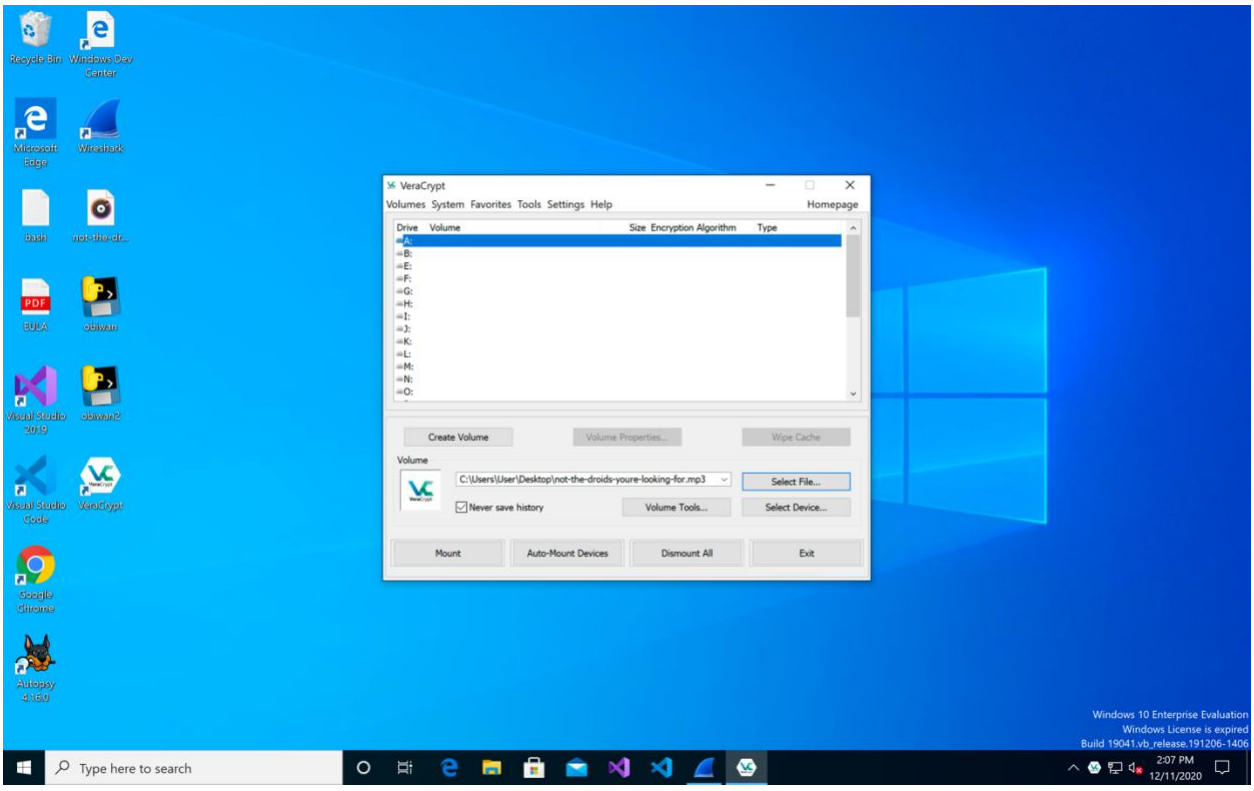
http://www.umd.edu/this-is-not-even-my-final-form.
http://www.umd.edu/All-your-base64-are-belong-to-us
http://www.umd.edu/cjJkMiBpcyB0aGUga2V5

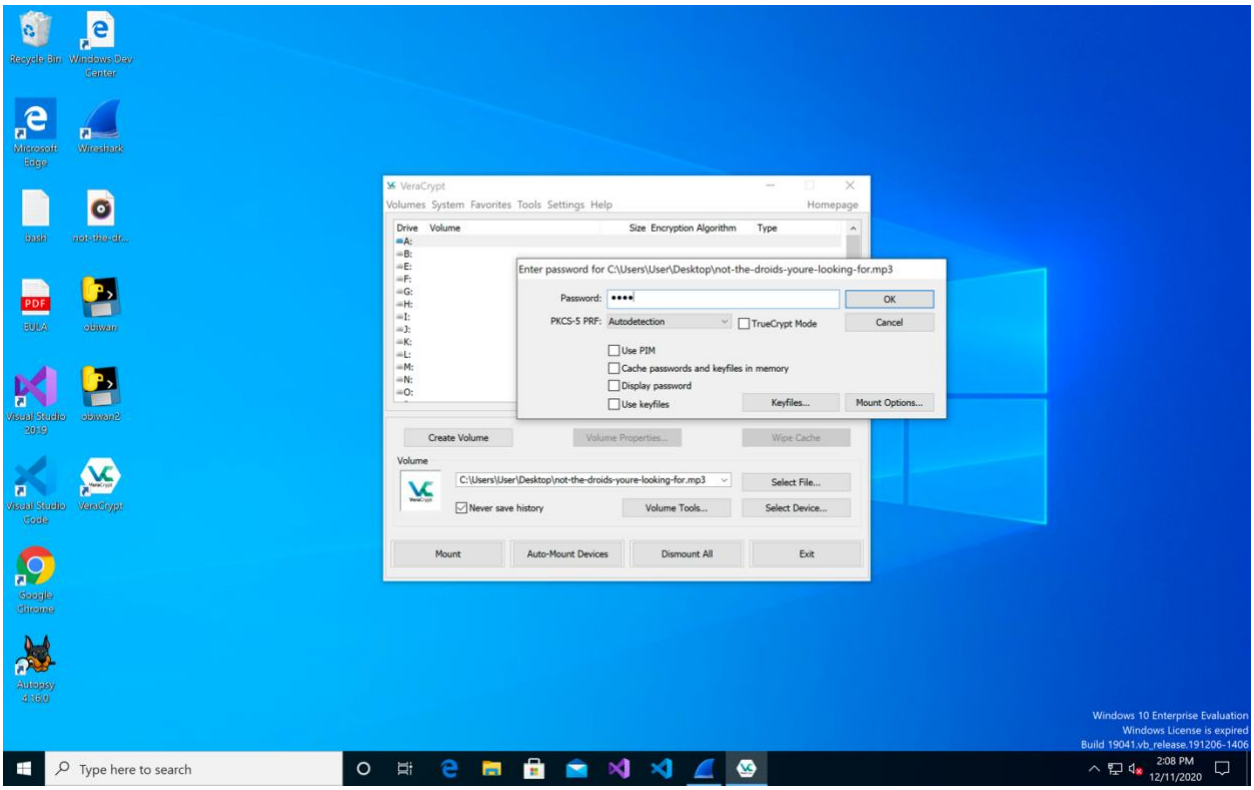
All the 3 websites which are trying to connect are showing http 301 moved permanently message. So, these sites are no longer hosted on umd.edu domain anymore. Also, these can be interpreted as the messages to the imperial army. From these URL's I have concluded that this is not the final form of the virus there may be a malware exist somewhere which is the final form of the malware written by the rebel's malware writer. Also, I have also interpreted as the 3rd no. URL we found is kind of hidden message and may be encoded in base64 as interpreted from the 2nd URL's messaged above.

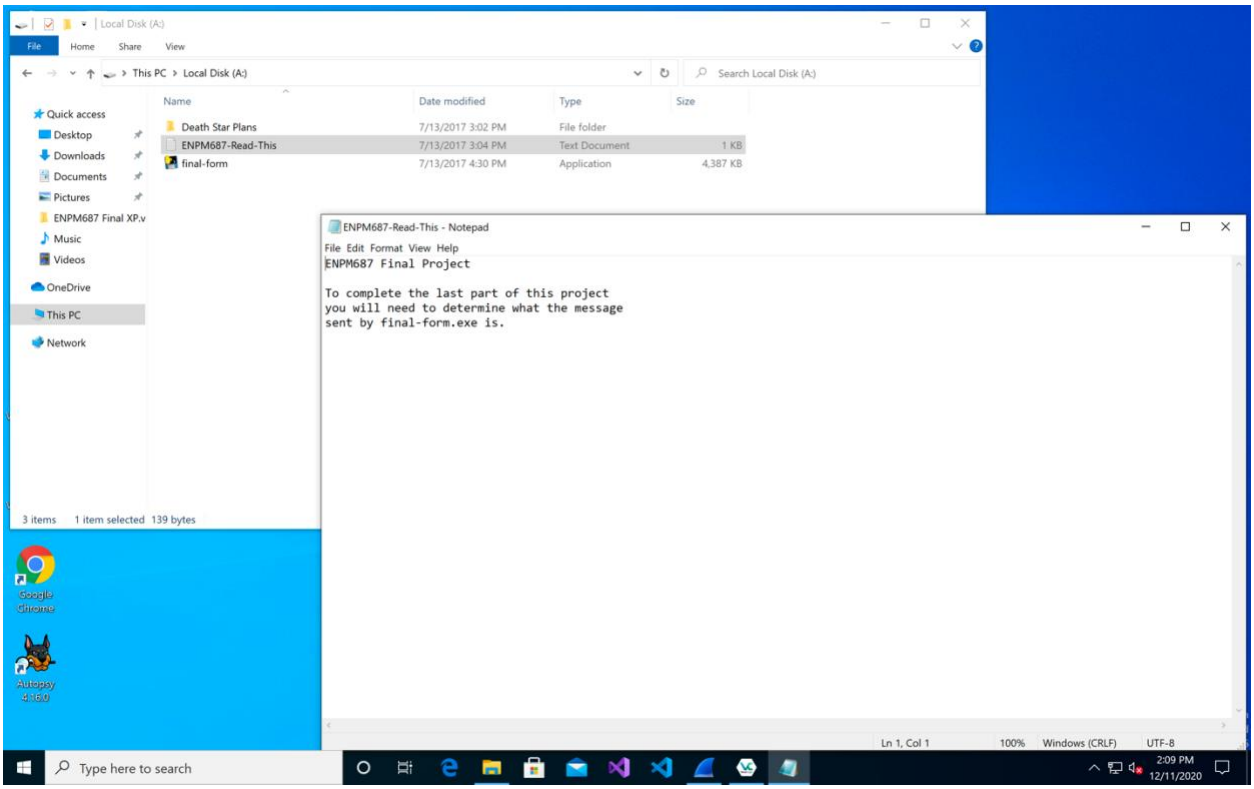


After decoding the hidden message online, the message was r2d2 is the key.

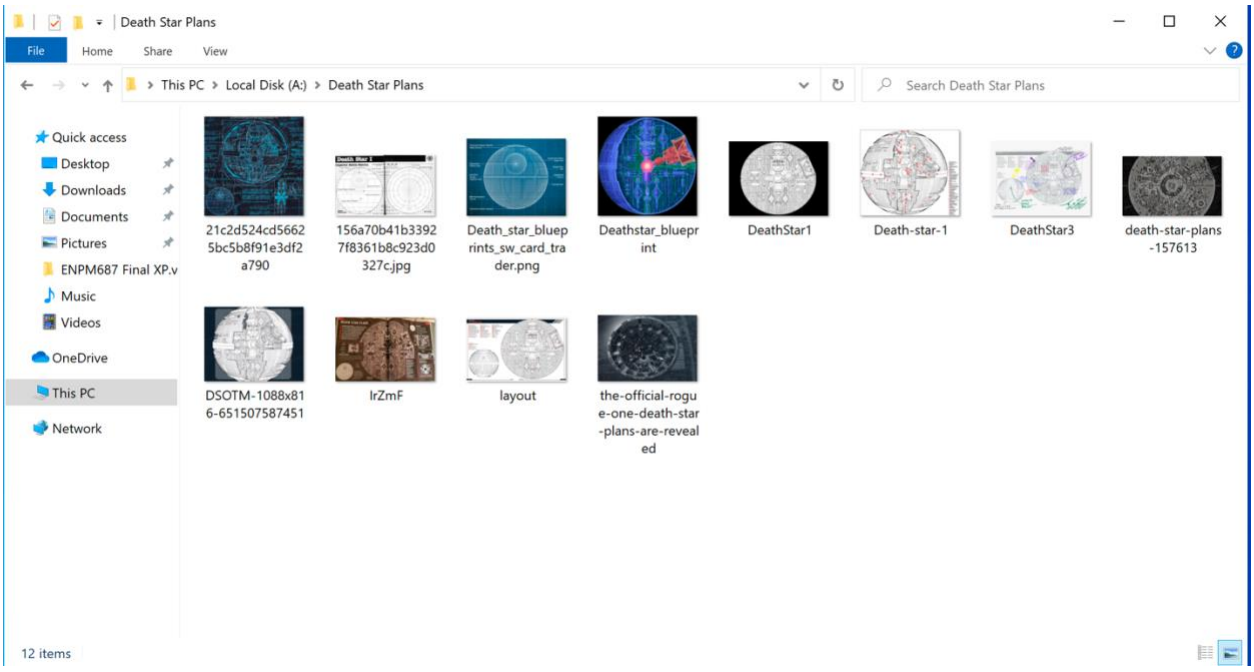
VeraCrypt was installed in the rebel's malware writer's computer also I have found one mp3 file which was suspected by an encrypted file. To unencrypt this mp3 file I need a key and I already got the key. Maybe this mp3 file contains all the secrets and final form of the malware. For that I have analyzed further and used VeraCrypt to mount my mp3 file to my computer's new drive.


Recycle Bin
Windows Dev Center
Microsoft Edge
Wireshark
bash
not-the-dr...
EULA
obiwan
Visual Studio 2019
obiwan2
Visual Studio Code
VeraCrypt
Google Chrome
Autopsy 4.16.0
VeraCrypt
Volumes System Favorites Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\User\Desktop\not-the-droids-youre-looking-for.mp3
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit
Windows 10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406
Type here to search
2:07 PM
12/11/2020

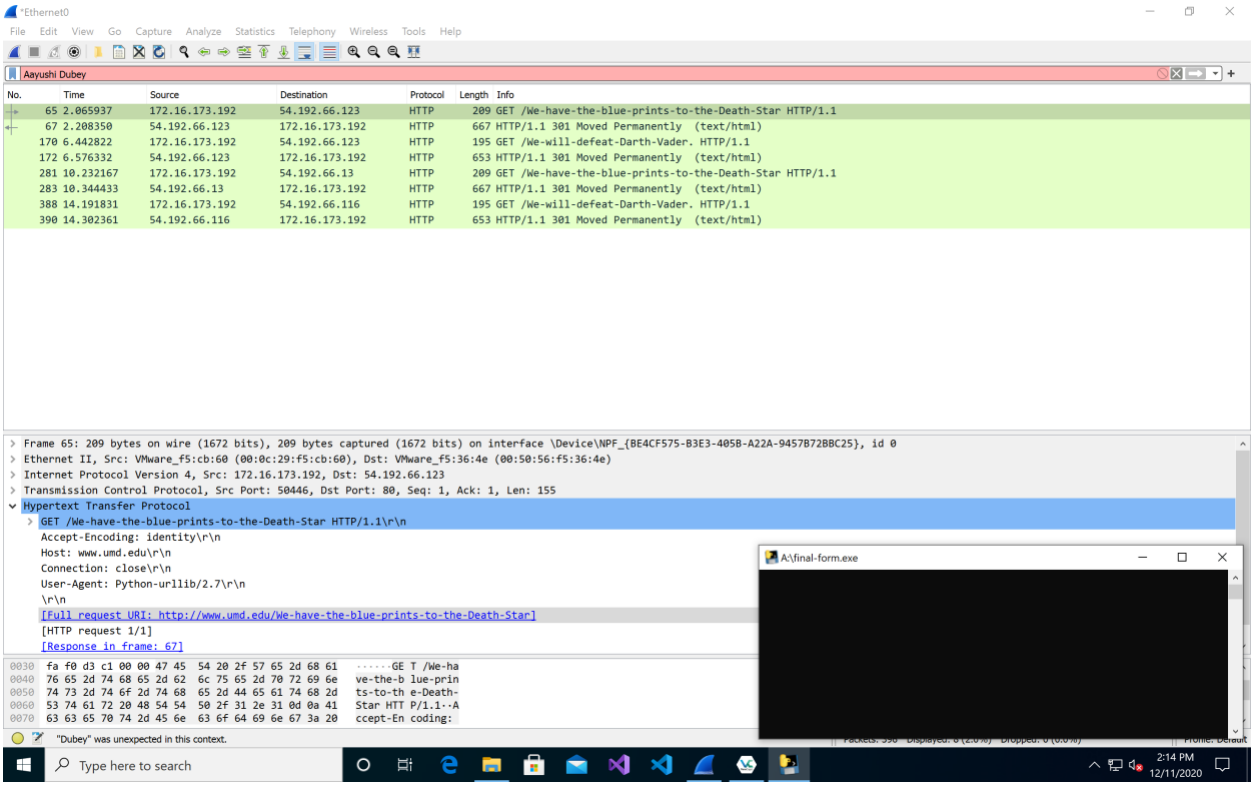

Recycle Bin
Windows Dev Center
Microsoft Edge
Wireshark
bash
not-the-dr...
EULA
obiwan
Visual Studio 2019
obiwan2
Visual Studio Code
VeraCrypt
Google Chrome
Autopsy 4.16.0
VeraCrypt
Volumes System Favorites Tools Settings Help
Homepage
Drive Volume Size Encryption Algorithm Type
Enter password for C:\Users\User\Desktop\not-the-droids-youre-looking-for.mp3
Password:
OK
PKCS-5 PRF: Autodetection
TrueCrypt Mode
Cancel
Use PIM
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\User\Desktop\not-the-droids-youre-looking-for.mp3
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit
Windows 10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406
Type here to search
2:08 PM
12/11/2020

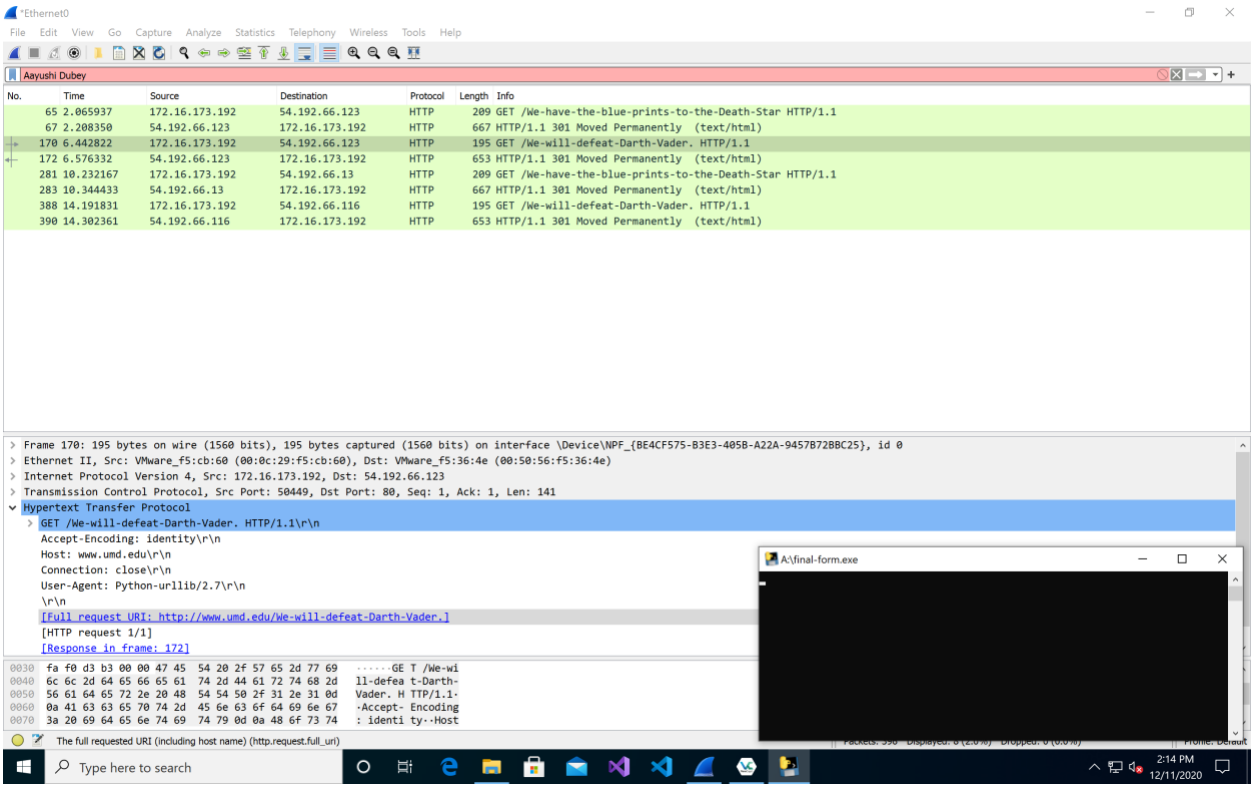


The original content of the mp3 file.



It has the blueprints/design of Death star, a text file and the malware named final-form.exe
This is the final form of the malware written by rebel's malware writer.





After further analyzing what messages does the malware final-form.exe file is sending, and I have found messages/Http connections.

The final-form.exe is trying to connect to the 2 websites.

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

Conclusion: -

From the evidence collected above we can conclude that: -

1. The Blueprints of the Death star are leaked, and they are with the rebels now.
2. Also, final-form.exe is the final form of the malware.

Suggestions to the Imperial Army: -

I would suggest to the imperial army that they should take the hash value of this malware and make an IOC also submit to AV solutions so it can be quarantine from the infected system. Then those systems should be scanned and If needed should be re-imaged and block the websites/domain in the firewall.
Also, I would suggest having good EDR solution and a proper SOC team which can work 24*7. This will be helpful to prevent further breaches and immediately start finding the loopholes in death star if any present to prevent further damage.

Difficulties faced: -

1. I was not able to relate the URL message that was originally in base64. But soon I have realized it and converted it to ASCII.
2. The other difficulty was with VeraCrypt. But after going through anti forensics slide again and doing exercise. I was able to successfully decrypt the content of mp3 file.

Most enjoyed things: -

I learned deeply about Autopsy and Wireshark. These tools are useful and used in everyday life of forensics investigator. I have learned a lot of things and I liked the lectures and the slides which will be really be helpful at the time of interviews. The lectures were in so many details which really helped me in understanding the world of DFIR deeply.