Final Forensics Report

Digital Forensics and Incidence Response

Dheepshika Raghunathan

Contents

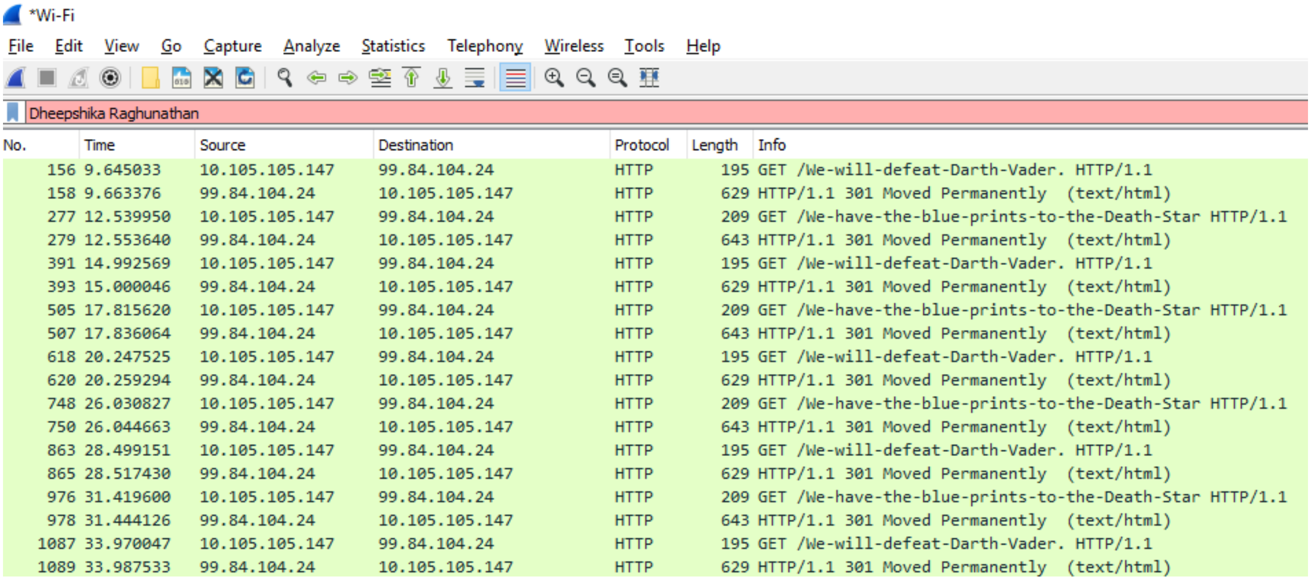
1. Summary of Results

1.1. Find the final version of the malware writer’s malware

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

1.2. 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.

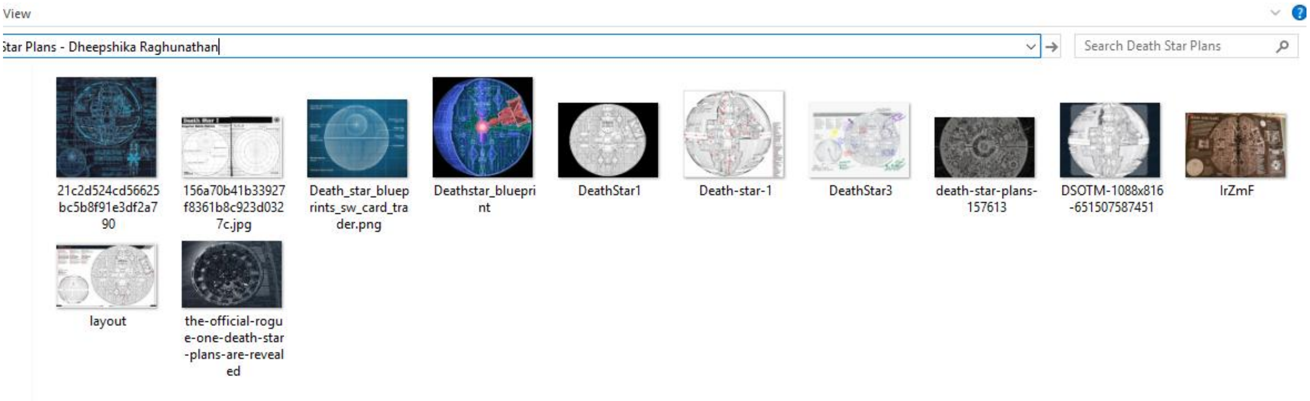

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

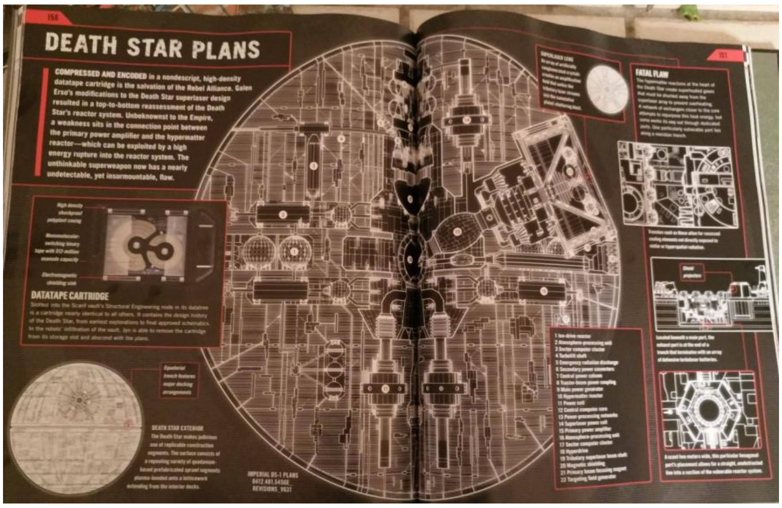
```
Dheepshika Raghunathan
No.   Time       Source          Destination     Protocol Length Info
  156 9.645033   10.105.105.147  99.84.104.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  158 9.663376   99.84.104.24    10.105.105.147  HTTP     629 HTTP/1.1 301 Moved Permanently  (text/html)
  277 12.539950  10.105.105.147  99.84.104.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  279 12.553640  99.84.104.24    10.105.105.147  HTTP     643 HTTP/1.1 301 Moved Permanently  (text/html)
  391 14.992569  10.105.105.147  99.84.104.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  393 15.000046  99.84.104.24    10.105.105.147  HTTP     629 HTTP/1.1 301 Moved Permanently  (text/html)
  505 17.815620  10.105.105.147  99.84.104.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  507 17.836064  99.84.104.24    10.105.105.147  HTTP     643 HTTP/1.1 301 Moved Permanently  (text/html)
  618 20.247525  10.105.105.147  99.84.104.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  620 20.259294  99.84.104.24    10.105.105.147  HTTP     629 HTTP/1.1 301 Moved Permanently  (text/html)
  748 26.030827  10.105.105.147  99.84.104.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  750 26.044663  99.84.104.24    10.105.105.147  HTTP     643 HTTP/1.1 301 Moved Permanently  (text/html)
  863 28.499151  10.105.105.147  99.84.104.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  865 28.517430  99.84.104.24    10.105.105.147  HTTP     629 HTTP/1.1 301 Moved Permanently  (text/html)
  976 31.419600  10.105.105.147  99.84.104.24    HTTP     209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  978 31.444126  99.84.104.24    10.105.105.147  HTTP     643 HTTP/1.1 301 Moved Permanently  (text/html)
 1087 33.970047  10.105.105.147  99.84.104.24    HTTP     195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
 1089 33.987533  99.84.104.24    10.105.105.147  HTTP     629 HTTP/1.1 301 Moved Permanently  (text/html)
```

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.

1.3. 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.


View
Star Plans - Dheepshika Raghunathan
Search Death Star Plans
21c2d524cd56625bc5b8f91e3df2a790
156a70b41b33927f8361b8c923d0327c.jpg
Death_star_blueprints_sw_card_trader.png
Deathstar_blueprint
DeathStar1
Death-star-1
DeathStar3
death-star-plans-157613
DSOTM-1088x816-651507587451
IrZmF
layout
the-official-rogue-one-death-star-plans-are-revealed



150

DEATH STAR PLANS

COMPRESSED AND ENCODED in a nondescript, high-density datatape cartridge is the salvation of the Rebel Alliance. Galen Erso's modifications to the Death Star superlaser design resulted in a top-to-bottom reassessment of the Death Star's reactor system. Unbeknownst to the Empire, a weakness sits in the connection point between the primary power amplifier and the hypermatter reactor—which can be exploited by a high energy rupture into the reactor system. The unthinkable superweapon now has a nearly undetectable, yet insurmountable, flaw.

High density shockproof polyplast casing
Monomolecular-switching binary tape with 512-million exanode capacity
Electromagnetic shielding sink

DATATAPE CARTRIDGE

Slotted into the Scarif vault's Structural Engineering node in its datatree is a cartridge nearly identical to all others. It contains the design history of the Death Star, from earliest explorations to final approved schematics. In the rebels' infiltration of the vault, Jyn is able to remove the cartridge from its storage slot and abscond with the plans.

DEATH STAR EXTERIOR

The Death Star makes judicious use of replicable construction segments. The surface consists of a repeating variety of quadanium-based prefabricated sprawl segments plasma-bonded onto a latticework extending from the interior decks.

IMPERIAL DS-1 PLANS
0412.481.5456E
REVISIONS_V631

SUPERLASER LENS

An array of artificially [illegible] crystals creates an amplification field that unites the tributary laser streams into the cumulative planet-shattering blast.

FATAL FLAW

The hypermatter reactions at the heart of the Death Star create superheated gases that must be shunted away from the superlaser array to prevent overheating. A network of exchangers closer to the core attempts to repurpose this heat energy, but some works its way out through dedicated ports. One particularly vulnerable port lies along a meridian trench.

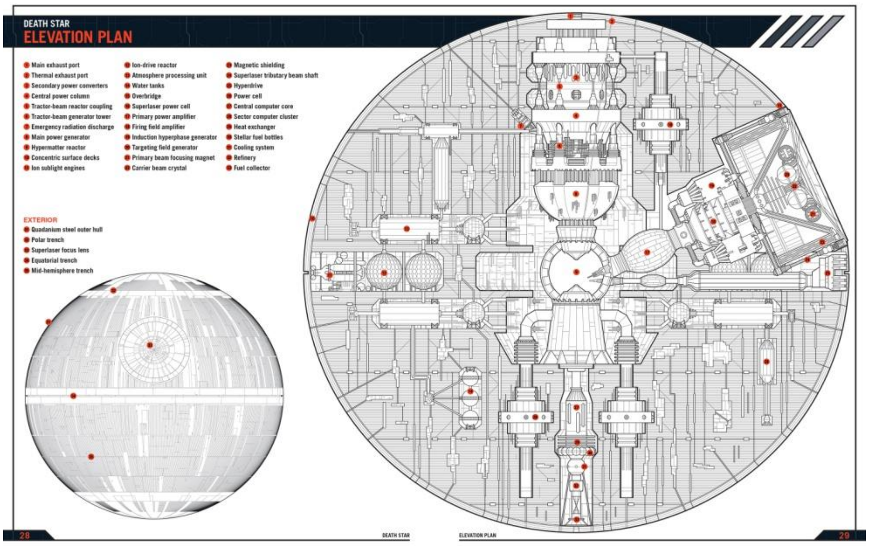
Trenches such as these allow for recessed cooling elements not directly exposed to stellar or hyperspatial radiation.

Located beneath a main port, the exhaust port is at the end of a trench that terminates with an array of defensive turbolaser batteries.

A scant two meters wide, this particular hexagonal port's placement allows for a straight, unobstructed line into a section of the vulnerable reactor system.

1 Ion-drive reactor
2 Atmosphere-processing unit
3 Sector computer cluster
4 Turbolift shaft
5 Emergency radiation discharge
6 Secondary power converters
7 Central power column
8 Tractor-beam power coupling
9 Main power generator
10 Hypermatter reactor
11 Power cell
12 Central computer core
13 Power-processing networks
14 Superlaser power cell
15 Primary power amplifier
16 Atmosphere-processing unit
17 Sector computer cluster
18 Hyperdrive
19 Tributary superlaser beam shaft
20 Magnetic shielding
21 Primary beam focusing magnet
22 Targeting field generator

151



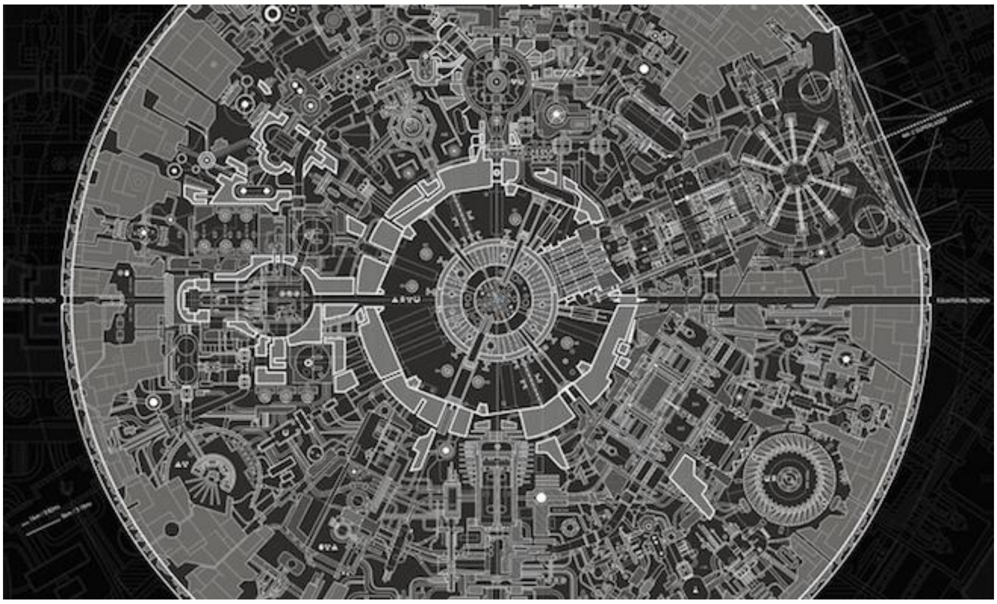
DEATH STAR
ELEVATION PLAN

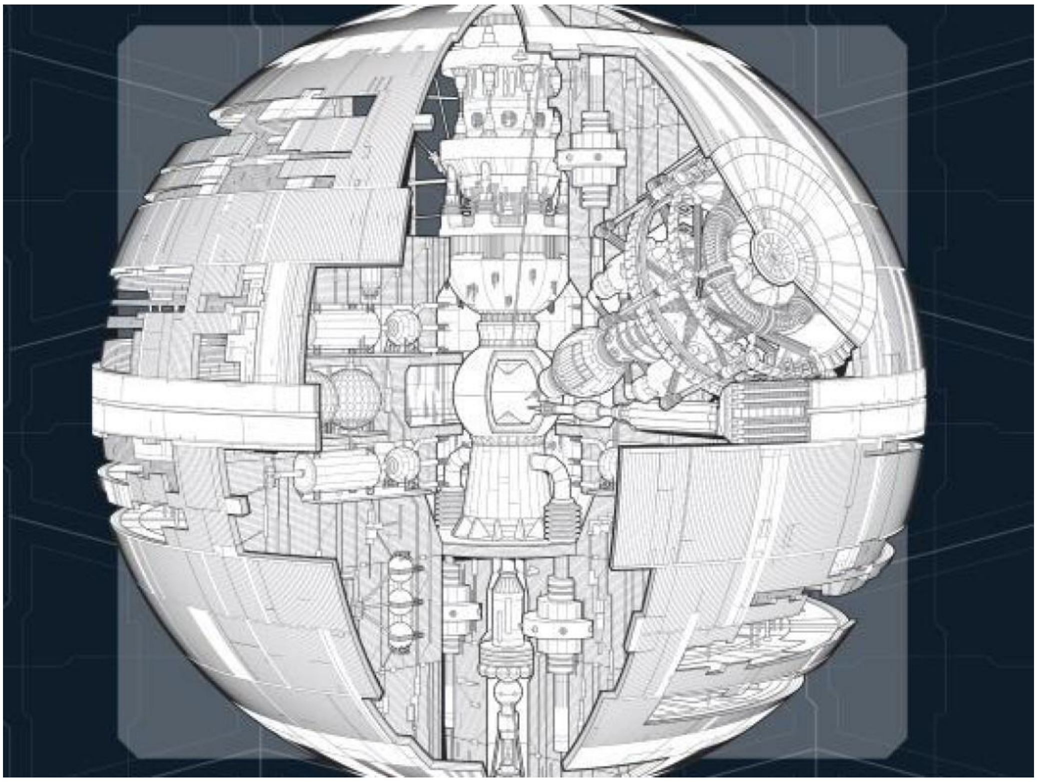
- Main exhaust port
- Thermal exhaust port
- Secondary power converters
- Central power column
- Tractor-beam reactor coupling
- Tractor-beam generator tower
- Emergency radiation discharge
- Main power generator
- Hypermatter reactor
- Concentric surface decks
- Ion sublight engines
- Ion-drive reactor
- Atmosphere processing unit
- Water tanks
- Overbridge
- Superlaser power cell
- Primary power amplifier
- Firing field amplifier
- Induction hyperphase generator
- Targeting field generator
- Primary beam focusing magnet
- Carrier beam crystal
- Magnetic shielding
- Superlaser tributary beam shaft
- Hyperdrive
- Power cell
- Central computer core
- Sector computer cluster
- Heat exchanger
- Stellar fuel bottles
- Cooling system
- Refinery
- Fuel collector

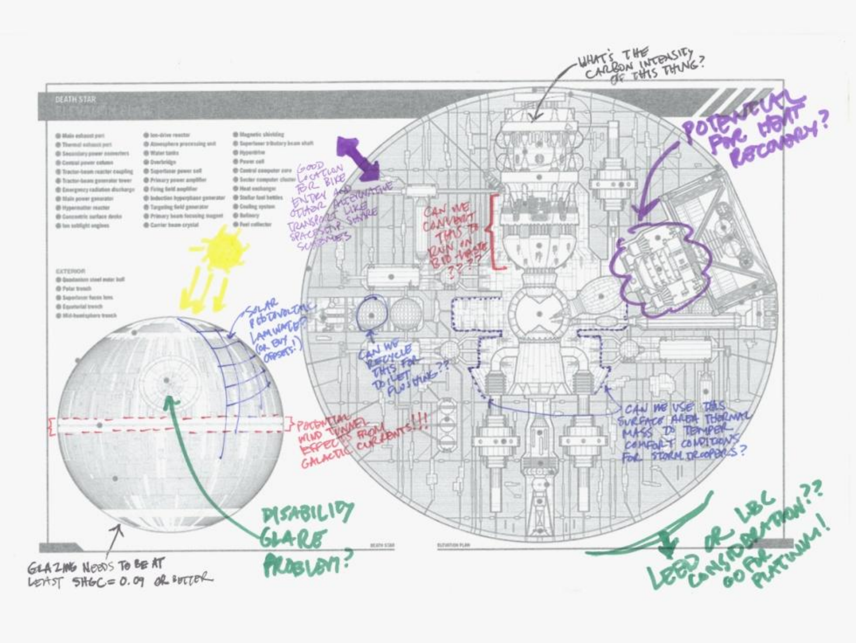
EXTERIOR
- Quadanium steel outer hull
- Polar trench
- Superlaser focus lens
- Equatorial trench
- Mid-hemisphere trench

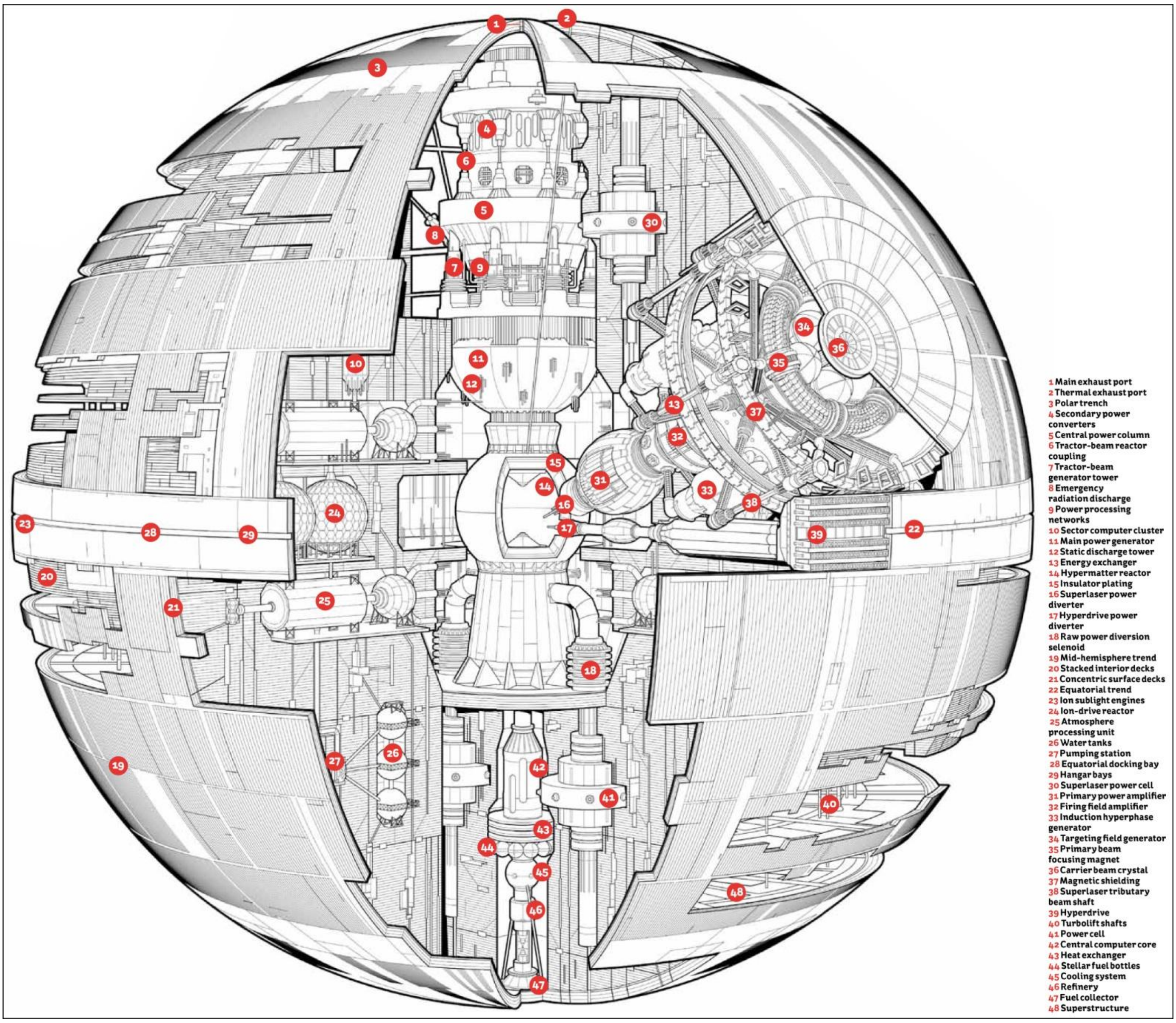
28 DEATH STAR

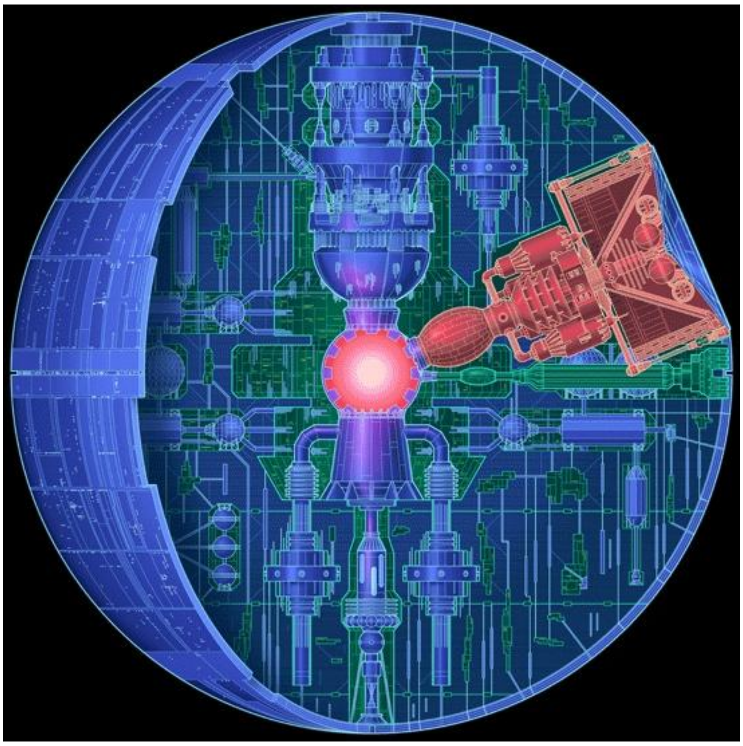
ELEVATION PLAN 29

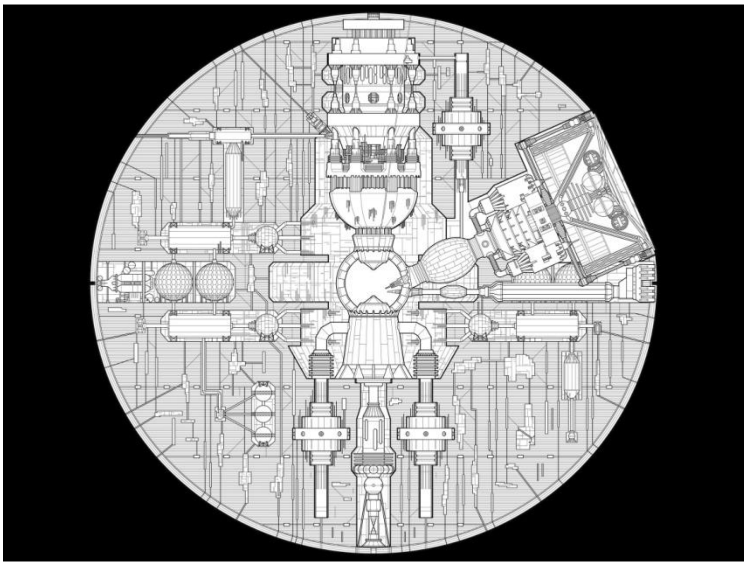

EQUATORIAL TRENCH
EQUATORIAL TRENCH

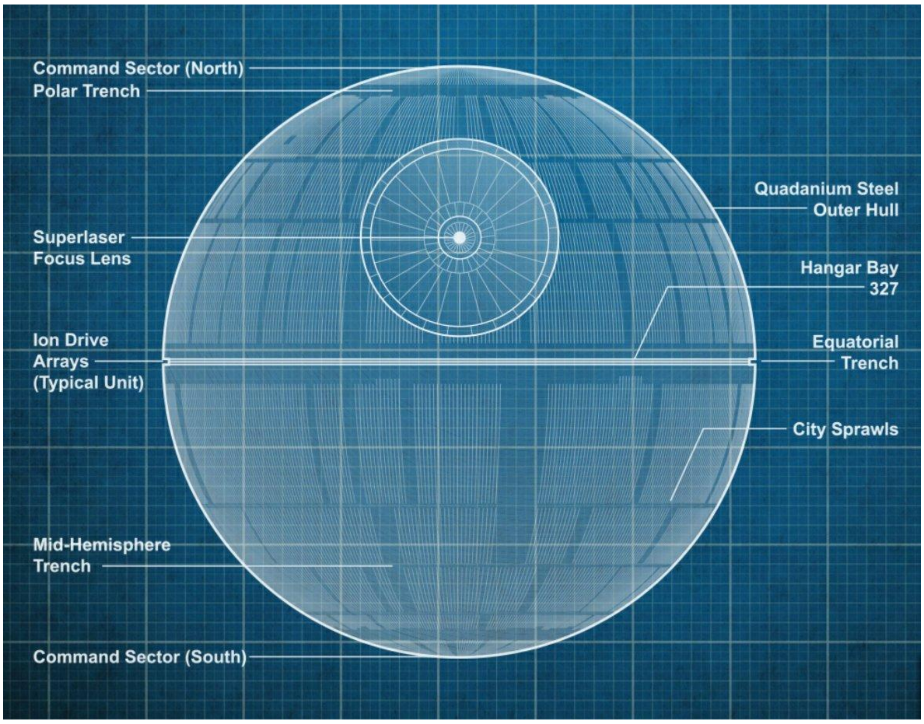


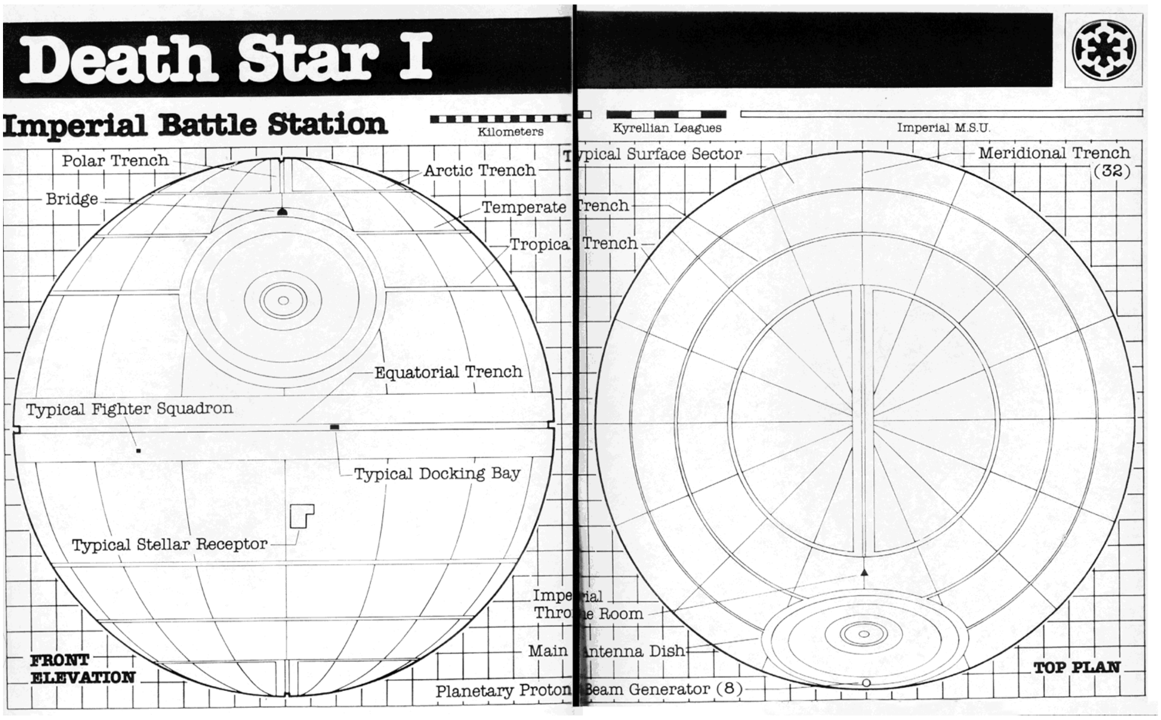

DEATH STAR
Main exhaust port
Thermal exhaust port
Secondary power converters
Central power column
Tractor-beam reactor coupling
Tractor-beam generator tower
Emergency radiation discharge
Main power generator
Hypermatter reactor
Concentric surface decks
Ion sublight engines
Ion-drive reactor
Atmosphere processing unit
Water tanks
Overbridge
Superlaser power cell
Primary power amplifier
Firing field amplifier
Induction hyperphase generator
Targeting field generator
Primary beam focusing magnet
Carrier beam crystal
Magnetic shielding
Superlaser tributary beam shaft
Hyperdrive
Power cell
Central computer core
Sector computer cluster
Heat exchanger
Stellar fuel bottles
Cooling system
Refinery
Fuel collector
EXTERIOR
Quadanium steel outer hull
Polar trench
Superlaser focus lens
Equatorial trench
Mid-hemisphere trench
WHAT'S THE CARBON INTENSITY OF THIS THING?
POTENTIAL FOR HEAT RECOVERY?
GOOD LOCATION FOR BIKE ENTRY AND OTHER ALTERNATIVE TRANSPORT LIKE SPACESHIP SHARE SCHEMES
CAN WE CONVERT THIS TO RUN ON BIO WASTE ???
SOLAR PHOTOVOLTAIC LAMINATE? (OR BUY OFFSETS!)
CAN WE RECYCLE THIS FOR TOILET FLUSHING??
POTENTIAL WIND TUNNEL EFFECTS FROM GALACTIC CURRENTS!!!
CAN WE USE THIS SURFACE AREA THERMAL MASS TO TEMPER COMFORT CONDITIONS FOR STORM TROOPERS?
DISABILITY GLARE PROBLEM?
GLAZING NEEDS TO BE AT LEAST SHGC= 0.09 OR BETTER
LEED OR LBC CONSIDERATION?? GO FOR PLATINUM!
DEATH STAR
ELEVATION PLAN

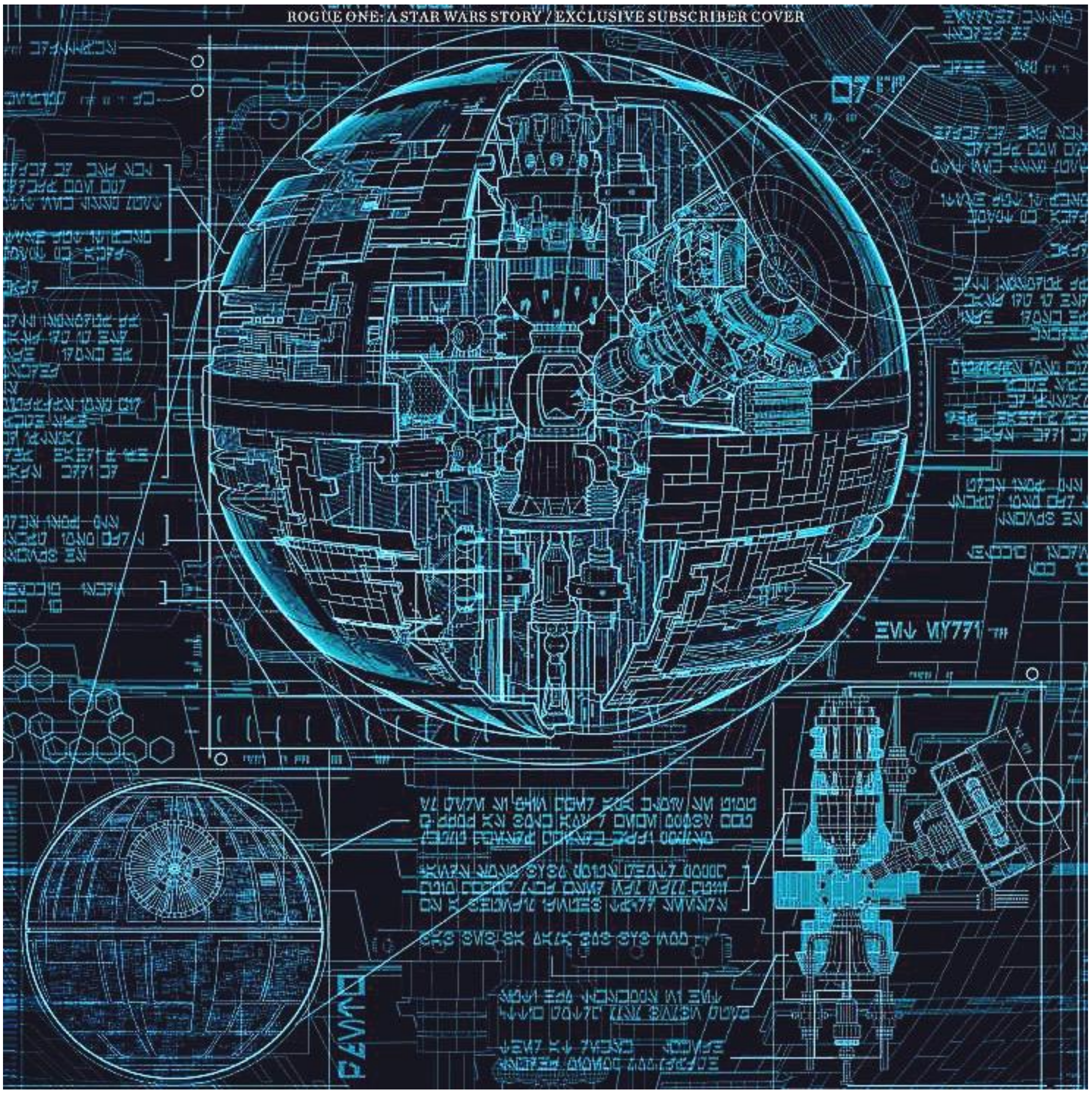

1 Main exhaust port
2 Thermal exhaust port
3 Polar trench
4 Secondary power converters
5 Central power column
6 Tractor-beam reactor coupling
7 Tractor-beam generator tower
8 Emergency radiation discharge
9 Power processing networks
10 Sector computer cluster
11 Main power generator
12 Static discharge tower
13 Energy exchanger
14 Hypermatter reactor
15 Insulator plating
16 Superlaser power diverter
17 Hyperdrive power diverter
18 Raw power diversion selenoid
19 Mid-hemisphere trend
20 Stacked interior decks
21 Concentric surface decks
22 Equatorial trend
23 Ion sublight engines
24 Ion-drive reactor
25 Atmosphere processing unit
26 Water tanks
27 Pumping station
28 Equatorial docking bay
29 Hangar bays
30 Superlaser power cell
31 Primary power amplifier
32 Firing field amplifier
33 Induction hyperphase generator
34 Targeting field generator
35 Primary beam focusing magnet
36 Carrier beam crystal
37 Magnetic shielding
38 Superlaser tributary beam shaft
39 Hyperdrive
40 Turbolift shafts
41 Power cell
42 Central computer core
43 Heat exchanger
44 Stellar fuel bottles
45 Cooling system
46 Refinery
47 Fuel collector
48 Superstructure






Command Sector (North)
Polar Trench
Superlaser Focus Lens
Ion Drive Arrays (Typical Unit)
Mid-Hemisphere Trench
Command Sector (South)
Quadanium Steel Outer Hull
Hangar Bay 327
Equatorial Trench
City Sprawls


Death Star I
Imperial Battle Station
Kilometers
Kyrellian Leagues
Imperial M.S.U.
Polar Trench
Bridge
Arctic Trench
Temperate Trench
Tropical Trench
Typical Surface Sector
Meridional Trench (32)
Equatorial Trench
Typical Fighter Squadron
Typical Docking Bay
Typical Stellar Receptor
Imperial Throne Room
Main Antenna Dish
Planetary Proton Beam Generator (8)
FRONT ELEVATION
TOP PLAN


ROGUE ONE: A STAR WARS STORY / EXCLUSIVE SUBSCRIBER COVER

2. Tools Used

2.1. Wireshark

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

2.2. Autopsy

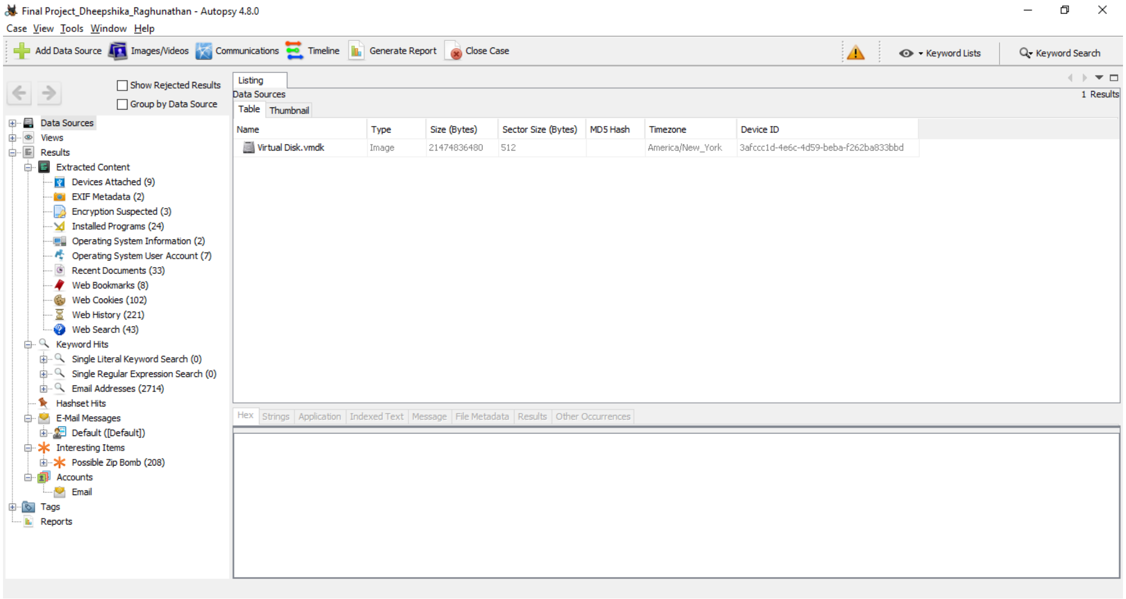
Autopsy is forensics software that has a graphical interface. Autopsy was used to analyse and extract the contents of the given drive.

2.3. 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.

3. 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.

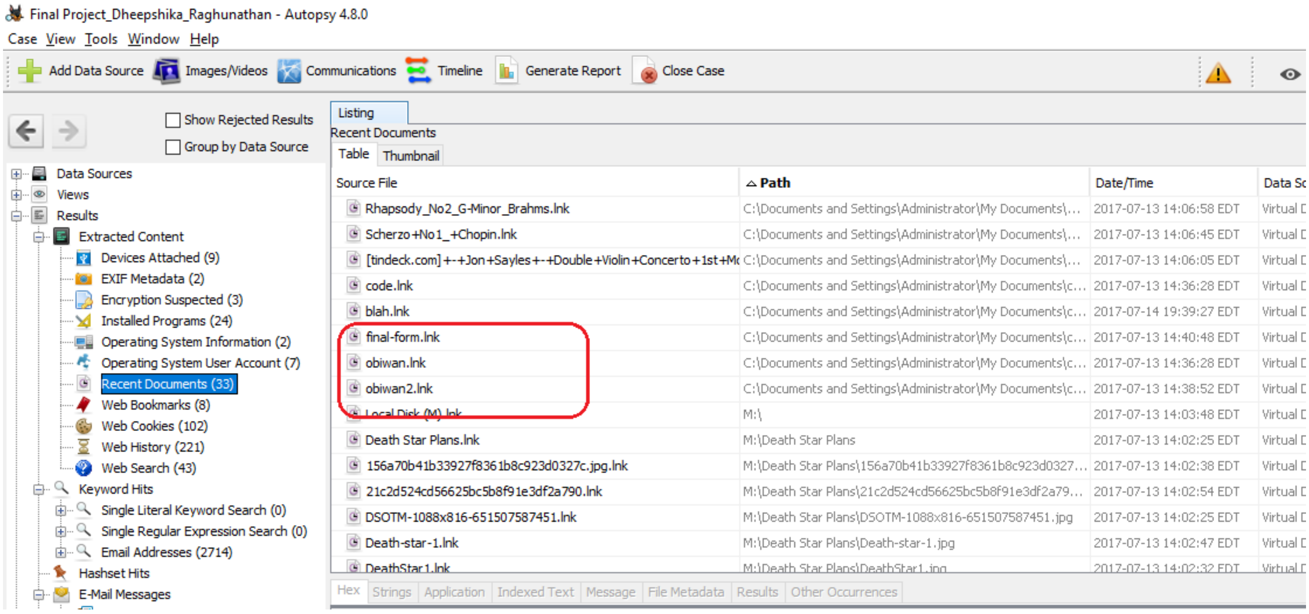


Name	Type	Size (Bytes)	Sector Size (Bytes)	MD5 Hash	Timezone	Device ID
Virtual Disk.vmdk	Image	21474836480	512		America/New_York	3afccc1d-4e6c-4d59-beba-f262ba833bbd

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.

3.1 Obiwan2.exe

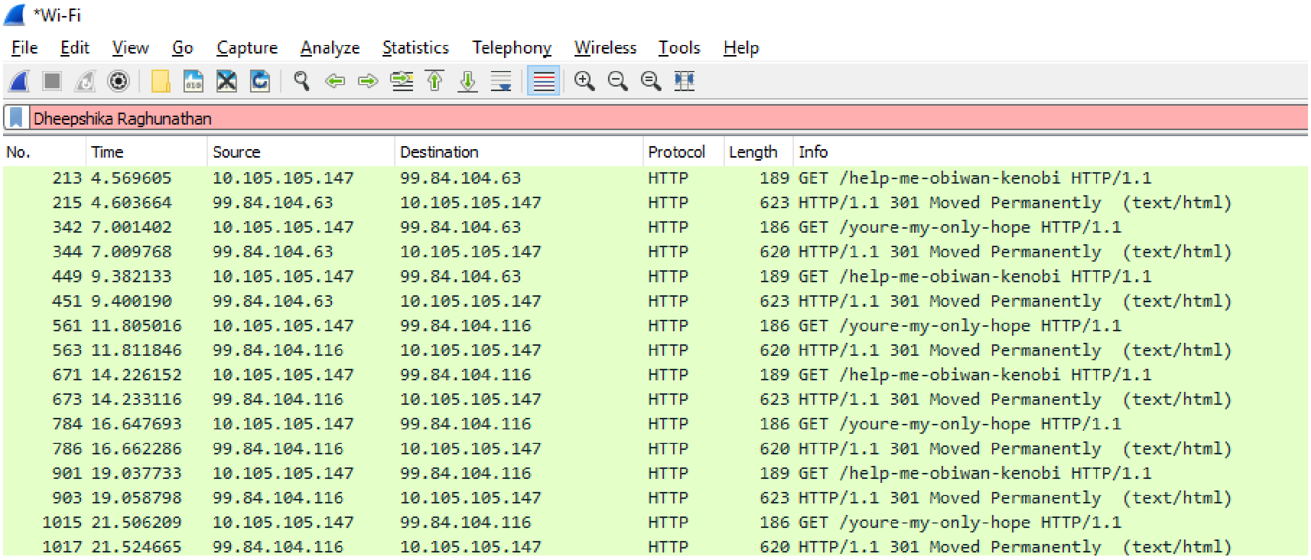
While going through the Recent Documents in the Extracted Content, links to python files named obiwan.py, obiwan2.py and final-form.py were found.



Source File	Path	Date/Time	Data Sc
Rhapsody_No2_G-Minor_Brahms.lnk	C:\Documents and Settings\Administrator\My Documents\...	2017-07-13 14:06:58 EDT	Virtual D
Scherzo+No1_+Chopin.lnk	C:\Documents and Settings\Administrator\My Documents\...	2017-07-13 14:06:45 EDT	Virtual D
[tindeck.com]+-+Jon+Sayles+-+Double+Violin+Concerto+1st+Mc	C:\Documents and Settings\Administrator\My Documents\...	2017-07-13 14:06:05 EDT	Virtual D
code.lnk	C:\Documents and Settings\Administrator\My Documents\c...	2017-07-13 14:36:28 EDT	Virtual D
blah.lnk	C:\Documents and Settings\Administrator\My Documents\c...	2017-07-14 19:39:27 EDT	Virtual D
final-form.lnk	C:\Documents and Settings\Administrator\My Documents\c...	2017-07-13 14:40:48 EDT	Virtual D
obiwan.lnk	C:\Documents and Settings\Administrator\My Documents\c...	2017-07-13 14:36:28 EDT	Virtual D
obiwan2.lnk	C:\Documents and Settings\Administrator\My Documents\c...	2017-07-13 14:38:52 EDT	Virtual D
Local Disk (M).lnk	M:\	2017-07-13 14:03:48 EDT	Virtual D
Death Star Plans.lnk	M:\Death Star Plans	2017-07-13 14:02:25 EDT	Virtual D
156a70b41b33927f8361b8c923d0327c.jpg.lnk	M:\Death Star Plans\156a70b41b33927f8361b8c923d0327...	2017-07-13 14:02:38 EDT	Virtual D
21c2d524cd56625bc5b8f91e3df2a790.lnk	M:\Death Star Plans\21c2d524cd56625bc5b8f91e3df2a79...	2017-07-13 14:02:54 EDT	Virtual D
DSOTM-1088x816-651507587451.lnk	M:\Death Star Plans\DSOTM-1088x816-651507587451.jpg	2017-07-13 14:02:25 EDT	Virtual D
Death-star-1.lnk	M:\Death Star Plans\Death-star-1.jpg	2017-07-13 14:02:47 EDT	Virtual D
DeathStar1.lnk	M:\Death Star Plans\DeathStar1.jpg	2017-07-13 14:02:32 EDT	Virtual D

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.



Dheepshika Raghunathan

```
No.   Time       Source          Destination     Protocol Length Info
  213 4.569605   10.105.105.147  99.84.104.63    HTTP      189 GET /help-me-obiwan-kenobi HTTP/1.1
  215 4.603664   99.84.104.63    10.105.105.147  HTTP      623 HTTP/1.1 301 Moved Permanently  (text/html)
  342 7.001402   10.105.105.147  99.84.104.63    HTTP      186 GET /youre-my-only-hope HTTP/1.1
  344 7.009768   99.84.104.63    10.105.105.147  HTTP      620 HTTP/1.1 301 Moved Permanently  (text/html)
  449 9.382133   10.105.105.147  99.84.104.63    HTTP      189 GET /help-me-obiwan-kenobi HTTP/1.1
  451 9.400190   99.84.104.63    10.105.105.147  HTTP      623 HTTP/1.1 301 Moved Permanently  (text/html)
  561 11.805016  10.105.105.147  99.84.104.116   HTTP      186 GET /youre-my-only-hope HTTP/1.1
  563 11.811846  99.84.104.116   10.105.105.147  HTTP      620 HTTP/1.1 301 Moved Permanently  (text/html)
  671 14.226152  10.105.105.147  99.84.104.116   HTTP      189 GET /help-me-obiwan-kenobi HTTP/1.1
  673 14.233116  99.84.104.116   10.105.105.147  HTTP      623 HTTP/1.1 301 Moved Permanently  (text/html)
  784 16.647693  10.105.105.147  99.84.104.116   HTTP      186 GET /youre-my-only-hope HTTP/1.1
  786 16.662286  99.84.104.116   10.105.105.147  HTTP      620 HTTP/1.1 301 Moved Permanently  (text/html)
  901 19.037733  10.105.105.147  99.84.104.116   HTTP      189 GET /help-me-obiwan-kenobi HTTP/1.1
  903 19.058798  99.84.104.116   10.105.105.147  HTTP      623 HTTP/1.1 301 Moved Permanently  (text/html)
 1015 21.506209  10.105.105.147  99.84.104.116   HTTP      186 GET /youre-my-only-hope HTTP/1.1
 1017 21.524665  99.84.104.116   10.105.105.147  HTTP      620 HTTP/1.1 301 Moved Permanently  (text/html)
```

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.

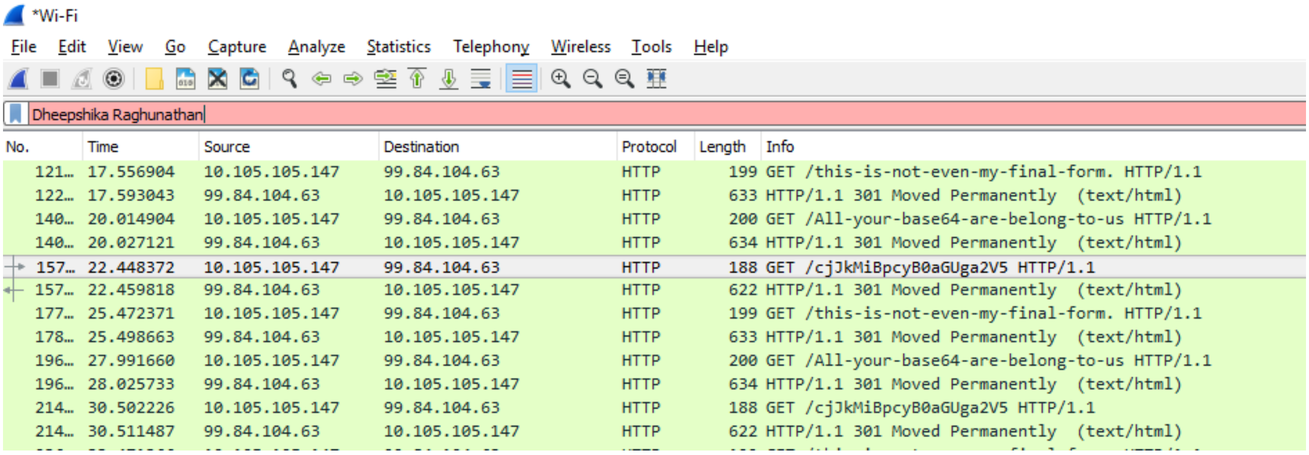
After 3 seconds, it sends its next message as below,

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

After 2 seconds, it sends the final message,

cjJkMiBpcyB0aGUga2V5

This process repeats every 3 seconds,



Dheepshika Raghunathan

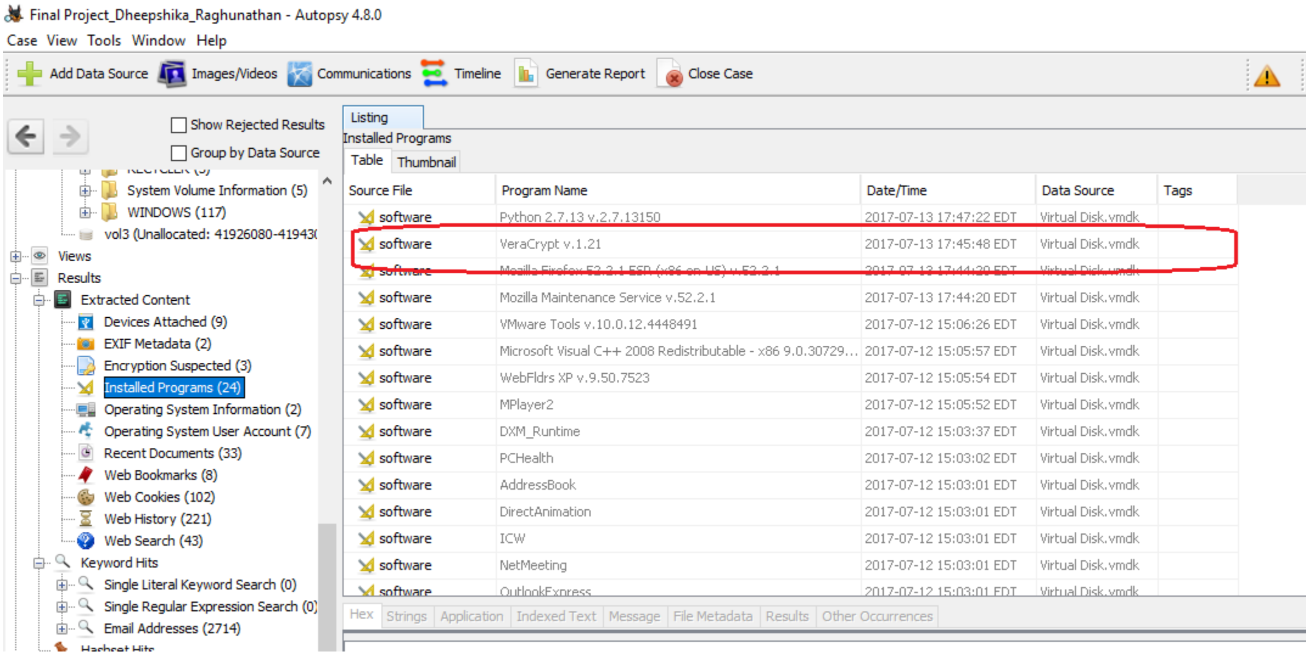
```
No.   Time       Source          Destination     Protocol Length Info
 121… 17.556904  10.105.105.147  99.84.104.63    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 122… 17.593043  99.84.104.63    10.105.105.147  HTTP      633 HTTP/1.1 301 Moved Permanently  (text/html)
 140… 20.014904  10.105.105.147  99.84.104.63    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 140… 20.027121  99.84.104.63    10.105.105.147  HTTP      634 HTTP/1.1 301 Moved Permanently  (text/html)
 157… 22.448372  10.105.105.147  99.84.104.63    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 157… 22.459818  99.84.104.63    10.105.105.147  HTTP      622 HTTP/1.1 301 Moved Permanently  (text/html)
 177… 25.472371  10.105.105.147  99.84.104.63    HTTP      199 GET /this-is-not-even-my-final-form. HTTP/1.1
 178… 25.498663  99.84.104.63    10.105.105.147  HTTP      633 HTTP/1.1 301 Moved Permanently  (text/html)
 196… 27.991660  10.105.105.147  99.84.104.63    HTTP      200 GET /All-your-base64-are-belong-to-us HTTP/1.1
 196… 28.025733  99.84.104.63    10.105.105.147  HTTP      634 HTTP/1.1 301 Moved Permanently  (text/html)
 214… 30.502226  10.105.105.147  99.84.104.63    HTTP      188 GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1
 214… 30.511487  99.84.104.63    10.105.105.147  HTTP      622 HTTP/1.1 301 Moved Permanently  (text/html)
```

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.

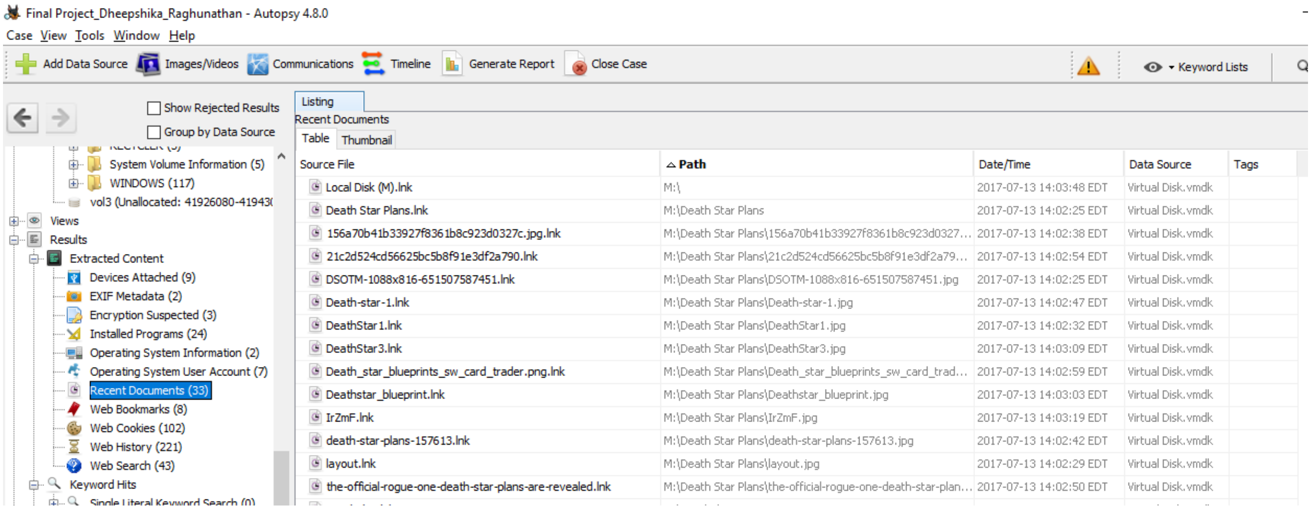
3.2 Veracrypt mounted volume

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



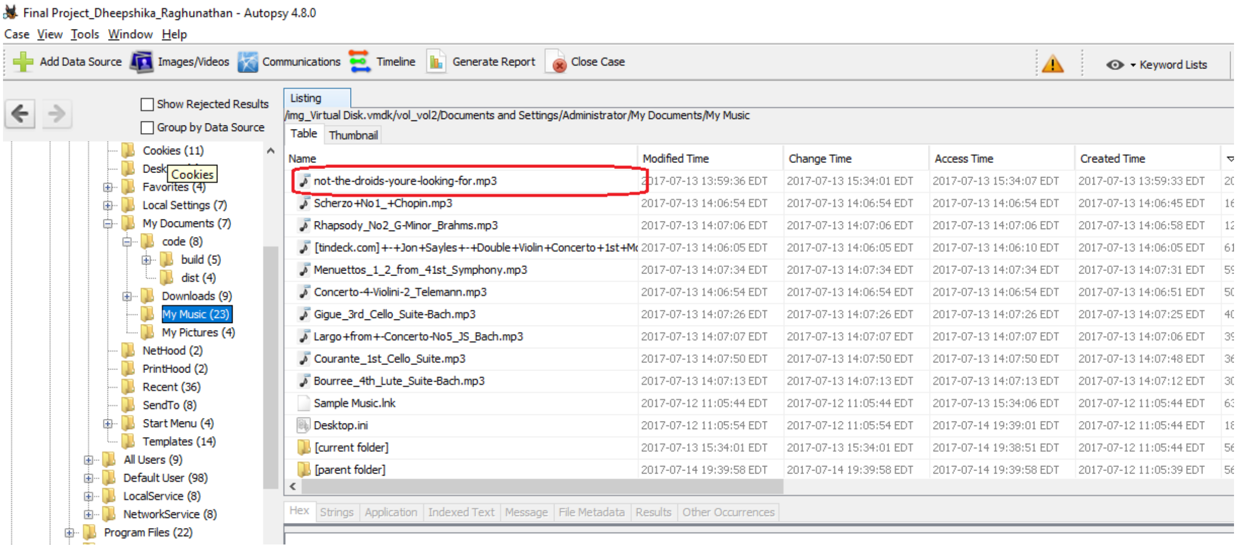
Source File	Program Name	Date/Time	Data Source	Tags
software	Python 2.7.13 v.2.7.13150	2017-07-13 17:47:22 EDT	Virtual Disk.vmdk	
software	VeraCrypt v.1.21	2017-07-13 17:45:48 EDT	Virtual Disk.vmdk	
software	Mozilla Firefox 52.2.1 ESR (x86 en-US) v.52.2.1	2017-07-13 17:44:20 EDT	Virtual Disk.vmdk	
software	Mozilla Maintenance Service v.52.2.1	2017-07-13 17:44:20 EDT	Virtual Disk.vmdk	
software	VMware Tools v.10.0.12.4448491	2017-07-12 15:06:26 EDT	Virtual Disk.vmdk	
software	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729…	2017-07-12 15:05:57 EDT	Virtual Disk.vmdk	
software	WebFldrs XP v.9.50.7523	2017-07-12 15:05:54 EDT	Virtual Disk.vmdk	
software	MPlayer2	2017-07-12 15:05:52 EDT	Virtual Disk.vmdk	
software	DXM_Runtime	2017-07-12 15:03:37 EDT	Virtual Disk.vmdk	
software	PCHealth	2017-07-12 15:03:02 EDT	Virtual Disk.vmdk	
software	AddressBook	2017-07-12 15:03:01 EDT	Virtual Disk.vmdk	
software	DirectAnimation	2017-07-12 15:03:01 EDT	Virtual Disk.vmdk	
software	ICW	2017-07-12 15:03:01 EDT	Virtual Disk.vmdk	
software	NetMeeting	2017-07-12 15:03:01 EDT	Virtual Disk.vmdk	
software	OutlookExpress	2017-07-12 15:03:01 EDT	Virtual Disk.vmdk	

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.



Source File	Path	Date/Time	Data Source	Tags
Local Disk (M).lnk	M:\	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
Death Star Plans.lnk	M:\Death Star Plans	2017-07-13 14:02:25 EDT	Virtual Disk.vmdk	
156a70b41b33927f8361b8c923d0327c.jpg.lnk	M:\Death Star Plans\156a70b41b33927f8361b8c923d0327…	2017-07-13 14:02:38 EDT	Virtual Disk.vmdk	
21c2d524cd56625bc5b8f91e3df2a790.lnk	M:\Death Star Plans\21c2d524cd56625bc5b8f91e3df2a79…	2017-07-13 14:02:54 EDT	Virtual Disk.vmdk	
DSOTM-1088x816-651507587451.lnk	M:\Death Star Plans\DSOTM-1088x816-651507587451.jpg	2017-07-13 14:02:25 EDT	Virtual Disk.vmdk	
Death-star-1.lnk	M:\Death Star Plans\Death-star-1.jpg	2017-07-13 14:02:47 EDT	Virtual Disk.vmdk	
DeathStar1.lnk	M:\Death Star Plans\DeathStar1.jpg	2017-07-13 14:02:32 EDT	Virtual Disk.vmdk	
DeathStar3.lnk	M:\Death Star Plans\DeathStar3.jpg	2017-07-13 14:03:09 EDT	Virtual Disk.vmdk	
Death_star_blueprints_sw_card_trader.png.lnk	M:\Death Star Plans\Death_star_blueprints_sw_card_trad…	2017-07-13 14:02:59 EDT	Virtual Disk.vmdk	
Deathstar_blueprint.lnk	M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 14:03:03 EDT	Virtual Disk.vmdk	
IrZmF.lnk	M:\Death Star Plans\IrZmF.jpg	2017-07-13 14:03:19 EDT	Virtual Disk.vmdk	
death-star-plans-157613.lnk	M:\Death Star Plans\death-star-plans-157613.jpg	2017-07-13 14:02:42 EDT	Virtual Disk.vmdk	
layout.lnk	M:\Death Star Plans\layout.jpg	2017-07-13 14:02:29 EDT	Virtual Disk.vmdk	
the-official-rogue-one-death-star-plans-are-revealed.lnk	M:\Death Star Plans\the-official-rogue-one-death-star-plan…	2017-07-13 14:02:50 EDT	Virtual Disk.vmdk	

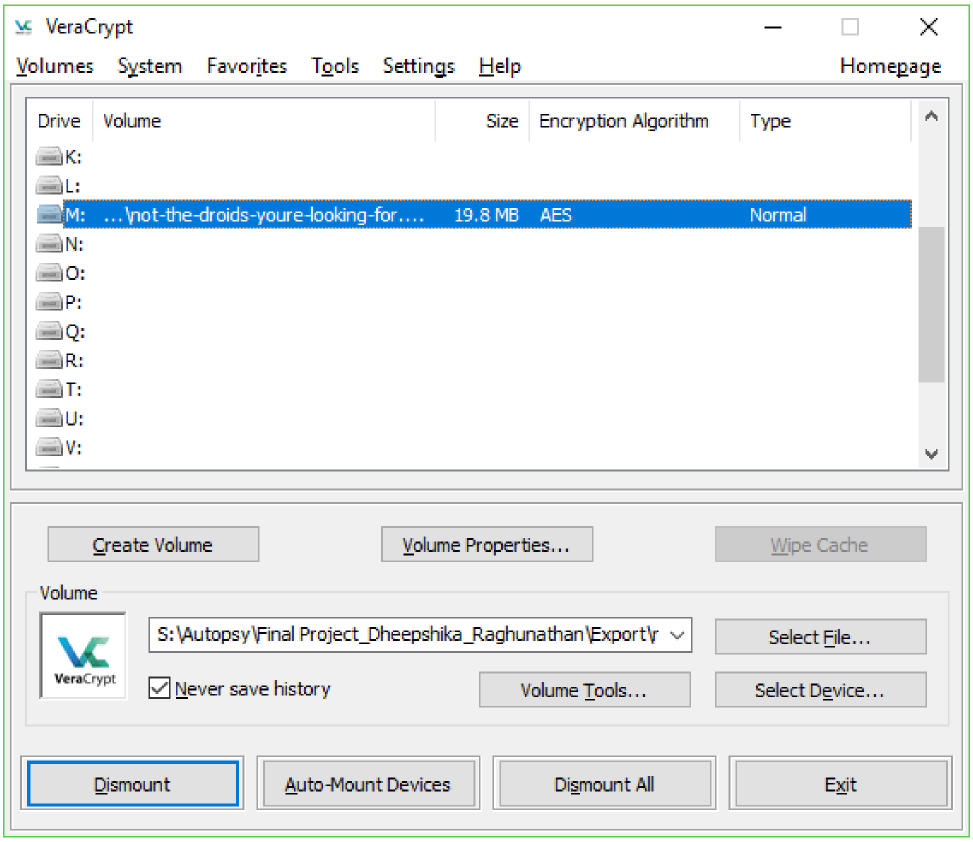
This means that there must be a volume in the disk that has been encrypted using Veracrypt. While searching for such a volume, it was found that the “My Music” contained a lot of the user’s music. A few of these files were of size in GBs. So when these files were played, there was one file which could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



/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/My Music

Name	Modified Time	Change Time	Access Time	Created Time
not-the-droids-youre-looking-for.mp3	2017-07-13 13:59:36 EDT	2017-07-13 15:34:01 EDT	2017-07-13 15:34:07 EDT	2017-07-13 13:59:33 EDT
Scherzo+No1_+Chopin.mp3	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54 EDT	2017-07-13 14:06:45 EDT
Rhapsody_No2_G-Minor_Brahms.mp3	2017-07-13 14:07:06 EDT	2017-07-13 14:07:06 EDT	2017-07-13 14:07:06 EDT	2017-07-13 14:06:58 EDT
[tindeck.com]+-+Jon+Sayles+-+Double+Violin+Concerto+1st+Mc	2017-07-13 14:06:05 EDT	2017-07-13 14:06:05 EDT	2017-07-13 14:06:10 EDT	2017-07-13 14:06:05 EDT
Menuettos_1_2_from_41st_Symphony.mp3	2017-07-13 14:07:34 EDT	2017-07-13 14:07:34 EDT	2017-07-13 14:07:34 EDT	2017-07-13 14:07:31 EDT
Concerto-4-Violini-2_Telemann.mp3	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54 EDT	2017-07-13 14:06:54 EDT	2017-07-13 14:06:51 EDT
Gigue_3rd_Cello_Suite-Bach.mp3	2017-07-13 14:07:26 EDT	2017-07-13 14:07:26 EDT	2017-07-13 14:07:26 EDT	2017-07-13 14:07:25 EDT
Largo+from+-Concerto-No5_JS_Bach.mp3	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT	2017-07-13 14:07:06 EDT
Courante_1st_Cello_Suite.mp3	2017-07-13 14:07:50 EDT	2017-07-13 14:07:50 EDT	2017-07-13 14:07:50 EDT	2017-07-13 14:07:48 EDT
Bourree_4th_Lute_Suite-Bach.mp3	2017-07-13 14:07:13 EDT	2017-07-13 14:07:13 EDT	2017-07-13 14:07:13 EDT	2017-07-13 14:07:12 EDT
Sample Music.lnk	2017-07-12 11:05:44 EDT	2017-07-12 11:05:44 EDT	2017-07-13 15:34:06 EDT	2017-07-12 11:05:44 EDT
Desktop.ini	2017-07-12 11:05:54 EDT	2017-07-12 11:05:54 EDT	2017-07-14 19:39:01 EDT	2017-07-12 11:05:44 EDT
[current folder]	2017-07-13 15:34:01 EDT	2017-07-13 15:34:01 EDT	2017-07-14 19:38:51 EDT	2017-07-12 11:05:44 EDT
[parent folder]	2017-07-14 19:39:58 EDT	2017-07-14 19:39:58 EDT	2017-07-14 19:39:58 EDT	2017-07-12 11:05:39 EDT

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.

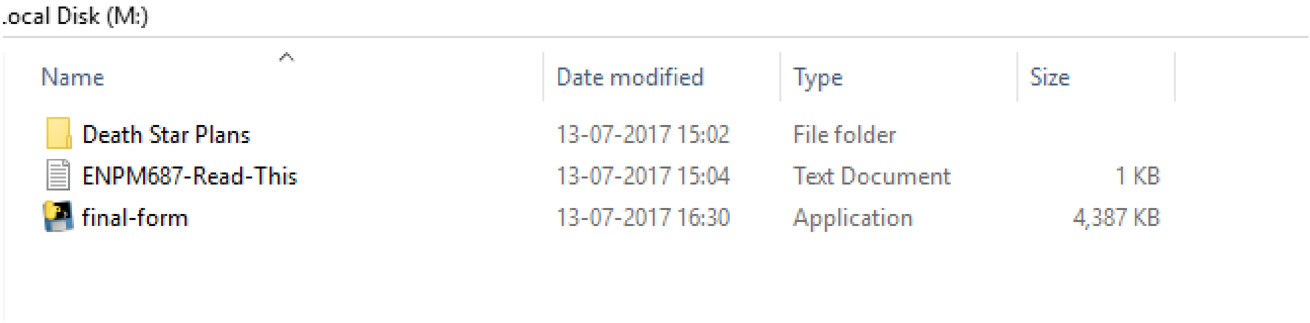


Drive	Volume	Size	Encryption Algorithm	Type
K:				
L:				
M:	...\not-the-droids-youre-looking-for....	19.8 MB	AES	Normal
N:				
O:				
P:				
Q:				
R:				
T:				
U:				
V:				

Volume: S:\Autopsy\Final Project_Dheepshika_Raghunathan\Export\r

☑ Never save history

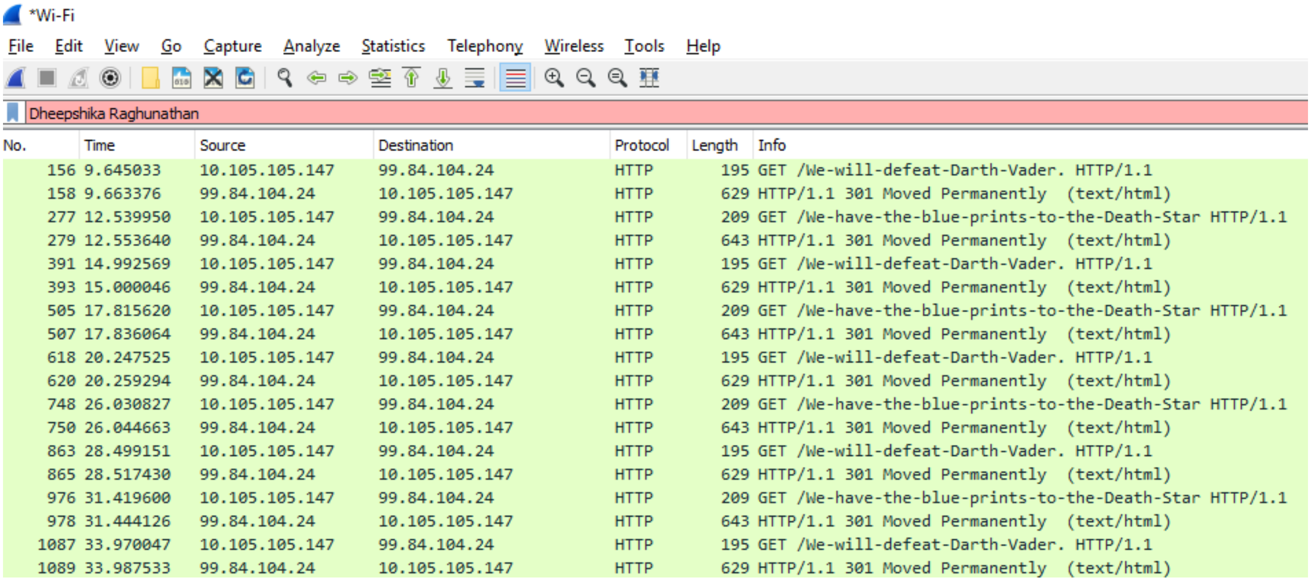
When this drive was opened, many files were found.



.ocal Disk (M:)

Name	Date modified	Type	Size
Death Star Plans	13-07-2017 15:02	File folder	
ENPM687-Read-This	13-07-2017 15:04	Text Document	1 KB
final-form	13-07-2017 16:30	Application	4,387 KB

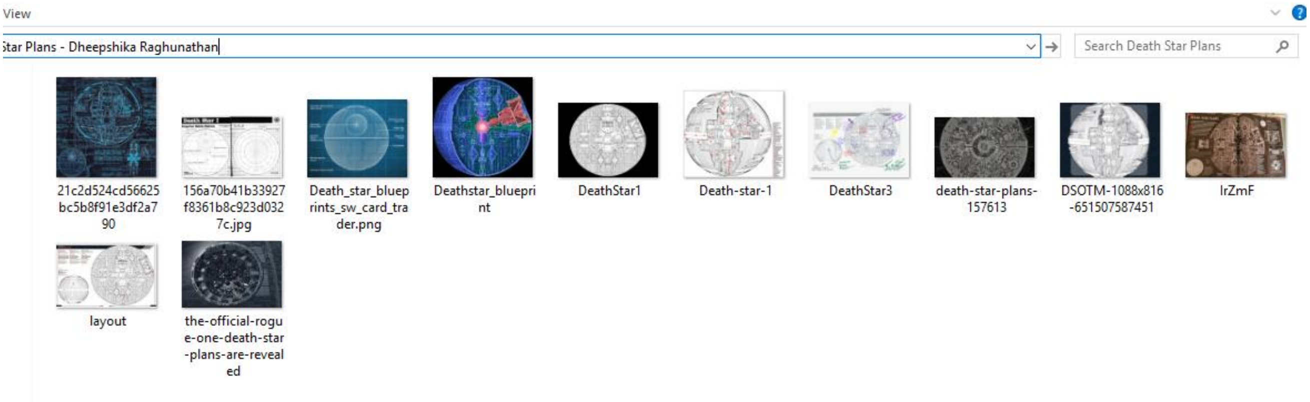
This drive contained a malware application called “final-form.exe”. On running this application while capturing the packets on Wireshark, it was found that this malware was communicating with umd.edu at IP address 99.84.104.24.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Dheepshika Raghunathan

```
No.    Time        Source            Destination       Protocol  Length  Info
  156 9.645033    10.105.105.147    99.84.104.24      HTTP       195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  158 9.663376    99.84.104.24      10.105.105.147    HTTP       629 HTTP/1.1 301 Moved Permanently  (text/html)
  277 12.539950   10.105.105.147    99.84.104.24      HTTP       209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  279 12.553640   99.84.104.24      10.105.105.147    HTTP       643 HTTP/1.1 301 Moved Permanently  (text/html)
  391 14.992569   10.105.105.147    99.84.104.24      HTTP       195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  393 15.000046   99.84.104.24      10.105.105.147    HTTP       629 HTTP/1.1 301 Moved Permanently  (text/html)
  505 17.815620   10.105.105.147    99.84.104.24      HTTP       209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  507 17.836064   99.84.104.24      10.105.105.147    HTTP       643 HTTP/1.1 301 Moved Permanently  (text/html)
  618 20.247525   10.105.105.147    99.84.104.24      HTTP       195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  620 20.259294   99.84.104.24      10.105.105.147    HTTP       629 HTTP/1.1 301 Moved Permanently  (text/html)
  748 26.030827   10.105.105.147    99.84.104.24      HTTP       209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  750 26.044663   99.84.104.24      10.105.105.147    HTTP       643 HTTP/1.1 301 Moved Permanently  (text/html)
  863 28.499151   10.105.105.147    99.84.104.24      HTTP       195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
  865 28.517430   99.84.104.24      10.105.105.147    HTTP       629 HTTP/1.1 301 Moved Permanently  (text/html)
  976 31.419600   10.105.105.147    99.84.104.24      HTTP       209 GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
  978 31.444126   99.84.104.24      10.105.105.147    HTTP       643 HTTP/1.1 301 Moved Permanently  (text/html)
 1087 33.970047   10.105.105.147    99.84.104.24      HTTP       195 GET /We-will-defeat-Darth-Vader. HTTP/1.1
 1089 33.987533   99.84.104.24      10.105.105.147    HTTP       629 HTTP/1.1 301 Moved Permanently  (text/html)
```

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.



View
Star Plans - Dheepshika Raghunathan
Search Death Star Plans
21c2d524cd56625bc5b8f91e3df2a790
156a70b41b33927f8361b8c923d0327c.jpg
Death_star_blueprints_sw_card_trader.png
Deathstar_blueprint
DeathStar1
Death-star-1
DeathStar3
death-star-plans-157613
DSOTM-1088x816-651507587451
IrZmF
layout
the-official-rogue-one-death-star-plans-are-revealed