

FINAL PROJECT REPORT

Submitted to Professor Kevin Shivers

By Radhika Pai (rpai@umd.edu)

ENPM687-Digital Forensics and Incidence Response | Summer 2017

Problem Description

Background

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 sent out, and review the image for other useful intelligence.

Your deliverable is a report of your findings.

You should find the final version of the malware writer’s malware, be able to determine what the message contained inside of it is, and find some other interesting items as well.

My Findings

1. Obiwan.exe

Location:

/Img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code/dist					
Name	Modified Time	Change Time	Access Time	Create Time	Last Write Time
📁 [current folder]	2017-07-13 12:35:06 PDT	2017-07-13 12:35:06 PDT	2017-07-13 12:35:06 PDT	2017	2017
📁 [parent folder]	2017-07-14 16:39:42 PDT	2017-07-14 16:39:42 PDT	2017-07-14 16:39:42 PDT	2017	2017
exe obiwan.exe	2017-07-13 11:44:27 PDT	2017-07-13 12:31:21 PDT	2017-07-13 11:44:27 PDT	2017	2017
exe obiwan2.exe	2017-07-13 12:30:44 PDT	2017-07-13 12:31:21 PDT	2017-07-13 12:30:44 PDT	2017	2017

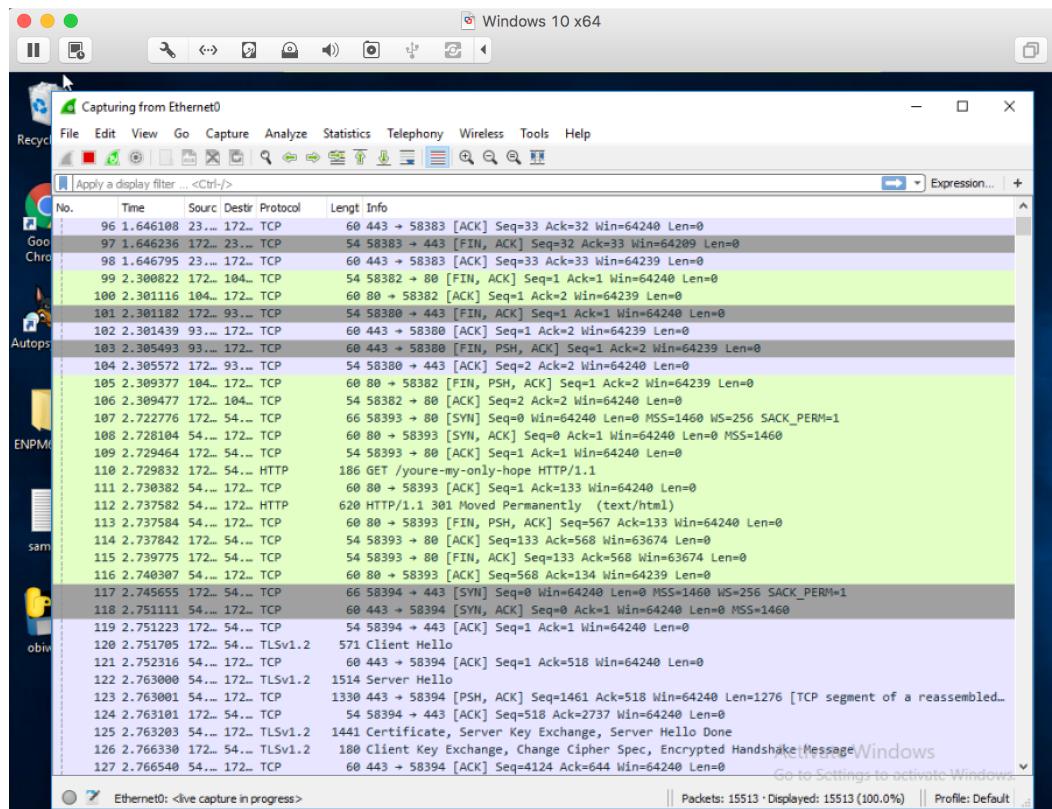
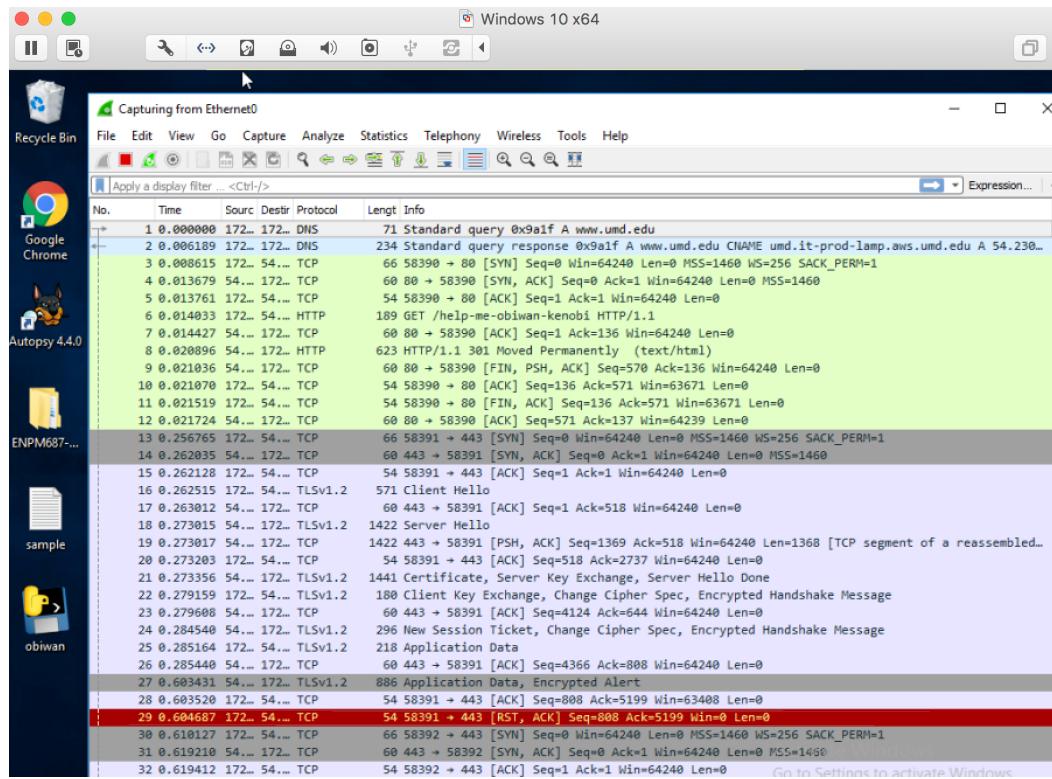
Description:

Obiwan.exe tries to make connection to www.umd.edu by making a request to it. This is followed by a 3-way handshake. Next, a GET request is made to https://help-me-obiwan-kenobi, which receives the request and responds with “301 moved permanently” (html/text file). It then acknowledges and closes the connection. Next another get request is made to https://www.umd.edu/youre-my-only-hope which receives the request and again responds with “301 moved permanently” (html/text file). These steps are then repeated.

Messages Sent:

Help me obiwan kenobi
Youre my only hope

Screenshots:



2. Obiwan2.exe

Location:

/Img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code/dist					
Name	Modified Time	Change Time	Access Time	Create Time	Last Write Time
[current folder]	2017-07-13 12:35:06 PDT				
[parent folder]	2017-07-14 16:39:42 PDT				
obiwan.exe	2017-07-13 11:44:27 PDT	2017-07-13 12:31:21 PDT	2017-07-13 11:44:27 PDT	2017-07-13 11:44:27 PDT	2017-07-13 11:44:27 PDT
obiwan2.exe	2017-07-13 12:30:44 PDT	2017-07-13 12:31:21 PDT	2017-07-13 12:30:44 PDT	2017-07-13 12:30:44 PDT	2017-07-13 12:30:44 PDT

Description:

Obiwan2.exe tries to make connection to www.umd.edu by making a request to it. This is followed by a 3-way handshake. Next, a GET request is made <https://www.umd.edu/this-is-not-even-my-final-form>, which receives the request and responds with “301 moved permanently” (html/text file). It then acknowledges and closes the connection. Next another get request is made to <https://www.umd.edu/all-your-base64-are-belong-to-us> which receives the request and again responds with “301 moved permanently” (html/text file) and lastly a GET request is made to <https://www.umd.edu/cJkMiBpcyB0aGUga2V5>. These steps are then repeated.

From this I can decode the messages as “this is not even my final form”, “all your base64 are belong to us” thus the “cJkMiBpcyB0aGUga2V5” when decoded using Base64 gives “**r2d2 is the key**”.

Messages Sent:

this is not even my final form

all your base64 are belong to us

cJkMiBpcyB0aGUga2V5 -> **r2d2 is the key**

Screenshots:

obiwlan2.pcap

No.	Time	Source	Dest	Proto	Length	Info
376	69...	172...	224...	MNDS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
377	78...	172...	172...	DNS	71	Standard query 0xf775 A www.umd.edu CNAME umd.it-prod-lamp.aws.umd.edu A 54.230.19.83 A 54.230.19.
378	78...	172...	172...	DNS	234	Standard query response 0xf775 A www.umd.edu CNAME umd.it-prod-lamp.aws.umd.edu A 54.230.19.83 A 54.230.19.
379	78...	172...	54...	TCP	66	53396 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
380	78...	54...	172...	TCP	60	80 + 53396 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
381	78...	172...	54...	TCP	54	53396 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
382	78...	172...	54...	HTTP	198	GET /this-is-not-even-my-final-form HTTP/1.1
383	78...	54...	172...	TCP	60	80 + 53396 [ACK] Seq=1 Ack=145 Win=64240 Len=0
384	78...	54...	172...	HTTP	632	HTTP/1.1 301 Moved Permanently (text/html)
385	78...	54...	172...	TCP	60	80 + 53396 [FIN, PSH, ACK] Seq=579 Ack=145 Win=64240 Len=0
386	78...	172...	54...	TCP	54	53396 → 80 [ACK] Seq=145 Ack=588 Win=63662 Len=0
387	78...	172...	54...	TCP	54	53396 → 80 [FIN, ACK] Seq=145 Ack=588 Win=63662 Len=0
388	78...	54...	172...	TCP	60	80 + 53396 [ACK] Seq=588 Ack=146 Win=64239 Len=0
389	78...	172...	54...	TCP	66	53397 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
390	78...	172...	54...	TCP	60	443 + 53397 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
391	78...	172...	54...	TCP	54	53397 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
392	78...	172...	54...	TLS...	571	Client Hello
393	78...	54...	172...	TCP	60	443 + 53397 [ACK] Seq=1 Ack=518 Win=64240 Len=0
394	78...	54...	172...	TLS...	1422	Server Hello
395	78...	54...	172...	TCP	1422	443 + 53397 [PSH, ACK] Seq=1369 Ack=518 Win=64240 Len=1368 [TCP segment of a reassembled PDU]
396	78...	172...	54...	TCP	54	53397 → 443 [ACK] Seq=518 Ack=2737 Win=64240 Len=0
397	78...	54...	172...	TLS...	1441	Certificate, Server Key Exchange, Server Hello Done
398	78...	172...	54...	TLS...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

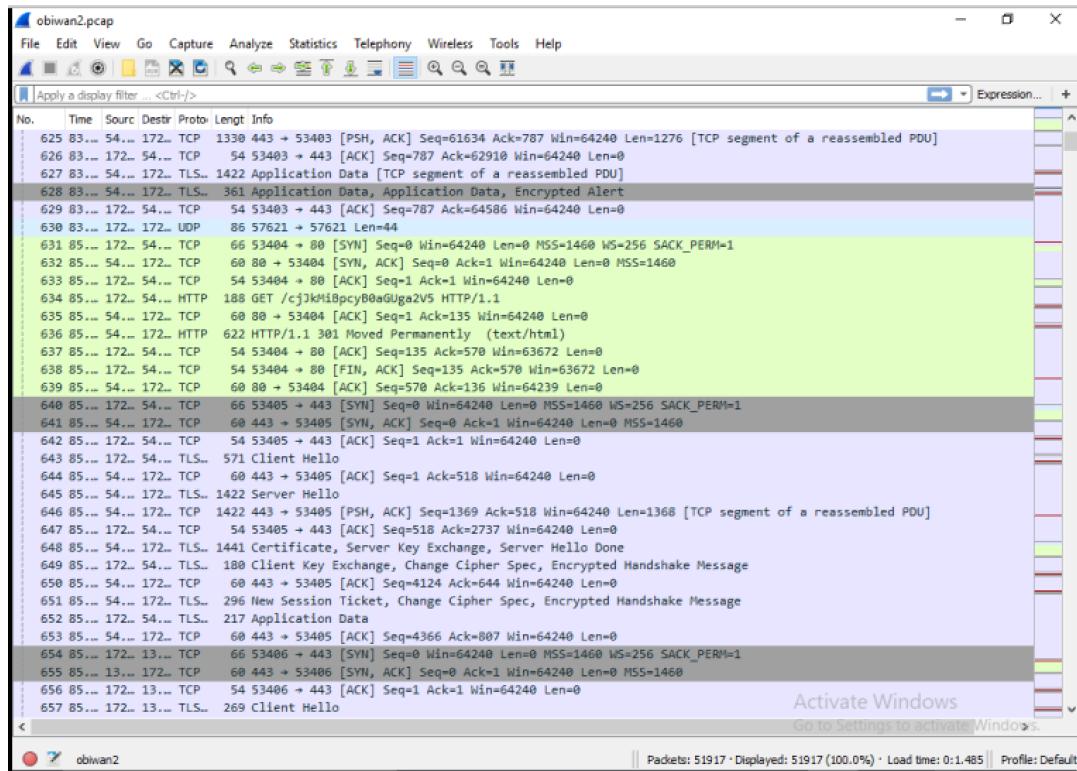
obiwlan2.pcap

No.	Time	Source	Dest	Proto	Length	Info
502	80...	172...	54...	TCP	54	53399 → 443 [ACK] Seq=787 Ack=64552 Win=64240 Len=0
503	80...	54...	172...	TLS...	80	Encrypted Alert
504	80...	172...	54...	TCP	54	53399 → 443 [ACK] Seq=787 Ack=64579 Win=64214 Len=0
505	82...	172...	54...	TCP	66	53400 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
506	82...	54...	172...	TCP	60	80 + 53400 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
507	82...	172...	54...	TCP	54	53400 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
508	82...	172...	54...	HTTP	200	GET /all-your-base64-are-belong-to-us HTTP/1.1
509	82...	54...	172...	TCP	60	80 + 53400 [ACK] Seq=1 Ack=147 Win=64240 Len=0
510	82...	54...	172...	HTTP	634	HTTP/1.1 301 Moved Permanently (text/html)
511	82...	54...	172...	TCP	60	80 + 53400 [FIN, PSH, ACK] Seq=581 Ack=147 Win=64240 Len=0
512	82...	172...	54...	TCP	54	53400 → 80 [ACK] Seq=147 Ack=582 Win=63668 Len=0
513	82...	172...	54...	TCP	54	53400 → 80 [FIN, ACK] Seq=147 Ack=582 Win=63668 Len=0
514	82...	172...	54...	TCP	60	80 + 53400 [ACK] Seq=582 Ack=148 Win=64239 Len=0
515	82...	172...	54...	TCP	66	53400 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
516	82...	172...	54...	TCP	60	443 + 53401 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
517	82...	172...	54...	TCP	54	53401 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
518	82...	172...	54...	TLS...	571	Client Hello
519	82...	54...	172...	TCP	60	443 + 53401 [ACK] Seq=1 Ack=518 Win=64240 Len=0
520	82...	172...	54...	TLS...	1422	Server Hello
521	82...	54...	172...	TCP	1422	443 + 53401 [PSH, ACK] Seq=1369 Ack=518 Win=64240 Len=1368 [TCP segment of a reassembled PDU]
522	82...	172...	54...	TCP	54	53401 → 443 [ACK] Seq=518 Ack=2737 Win=64240 Len=0
523	82...	54...	172...	TLS...	1441	Certificate, Server Key Exchange, Server Hello Done
524	82...	172...	54...	TLS...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
525	82...	172...	54...	TCP	60	443 + 53401 [ACK] Seq=4124 Ack=644 Win=64240 Len=0
526	82...	54...	172...	TLS...	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
527	82...	172...	54...	TLS...	229	Application Data
528	82...	172...	54...	TCP	60	443 + 53401 [ACK] Seq=4366 Ack=819 Win=64240 Len=0
529	82...	172...	13...	TCP	54	53389 → 443 [FIN, ACK] Seq=5544 Ack=4788 Win=63664 Len=0
530	82...	13...	172...	TCP	60	443 + 53389 [ACK] Seq=4788 Ack=5545 Win=64239 Len=0
531	82...	13...	172...	TCP	60	443 + 53389 [FIN, PSH, ACK] Seq=4788 Ack=5545 Win=64239 Len=0
532	82...	172...	13...	TCP	54	53389 → 443 [ACK] Seq=5545 Ack=4789 Win=63664 Len=0
533	82...	54...	172...	TLS...	887	Application Data, Encrypted Alert
534	82...	172...	54...	TCP	54	53401 → 443 [RST, ACK] Seq=819 Ack=5199 Win=0 Len=0

Activate Windows
Go to Settings to activate Windows.

obiwlan2

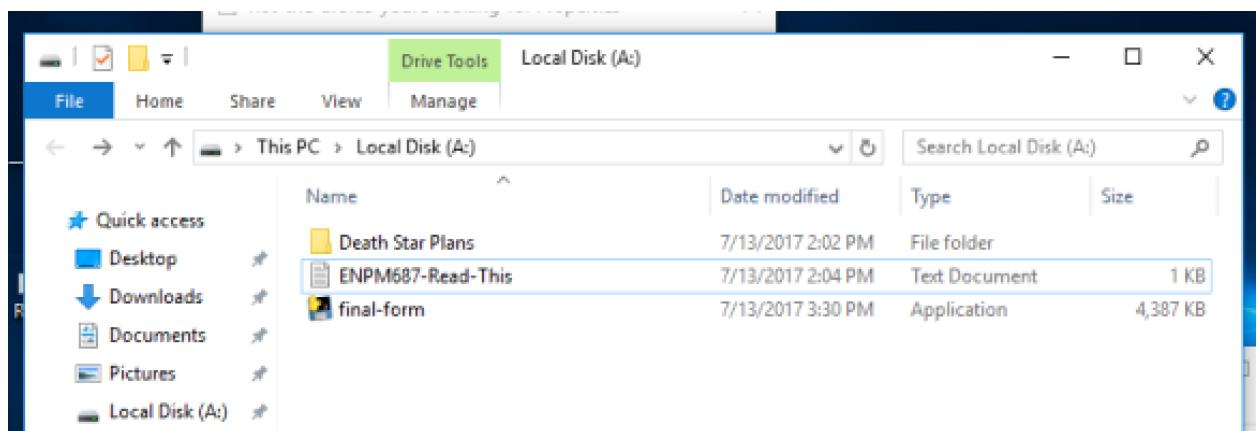
Packets: 51917 · Displayed: 51917 (100.0%) · Load time: 0:1.485 · Profile: Default



3. Death Star Plans

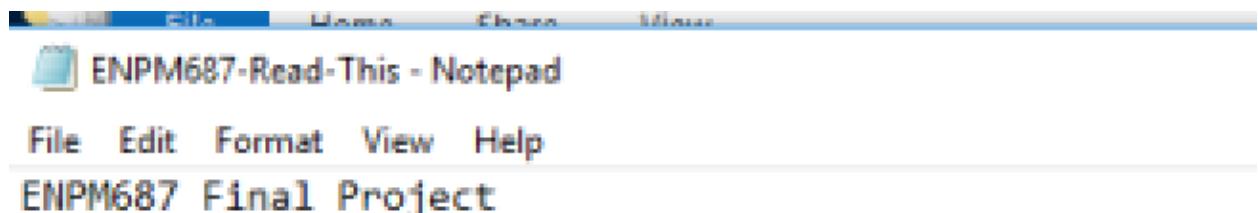
Since the attacker has VeraCrypt installed and is a music fan, used VeraCrypt to decrypt hidden contents of file **not-the-droids-you-are-looking-for.mp3**.

Contents of the decrypted volume included a folder “Death Star Plans” which had images of useful intelligence that could be sent out. The images are added under the section - other interesting findings.



4. Final-form.exe

Contents of the decrypted file also included a text file “ENPM687-Read-This” as shown below.



To complete the last part of this project you will need to determine what the message sent by final-form.exe is.

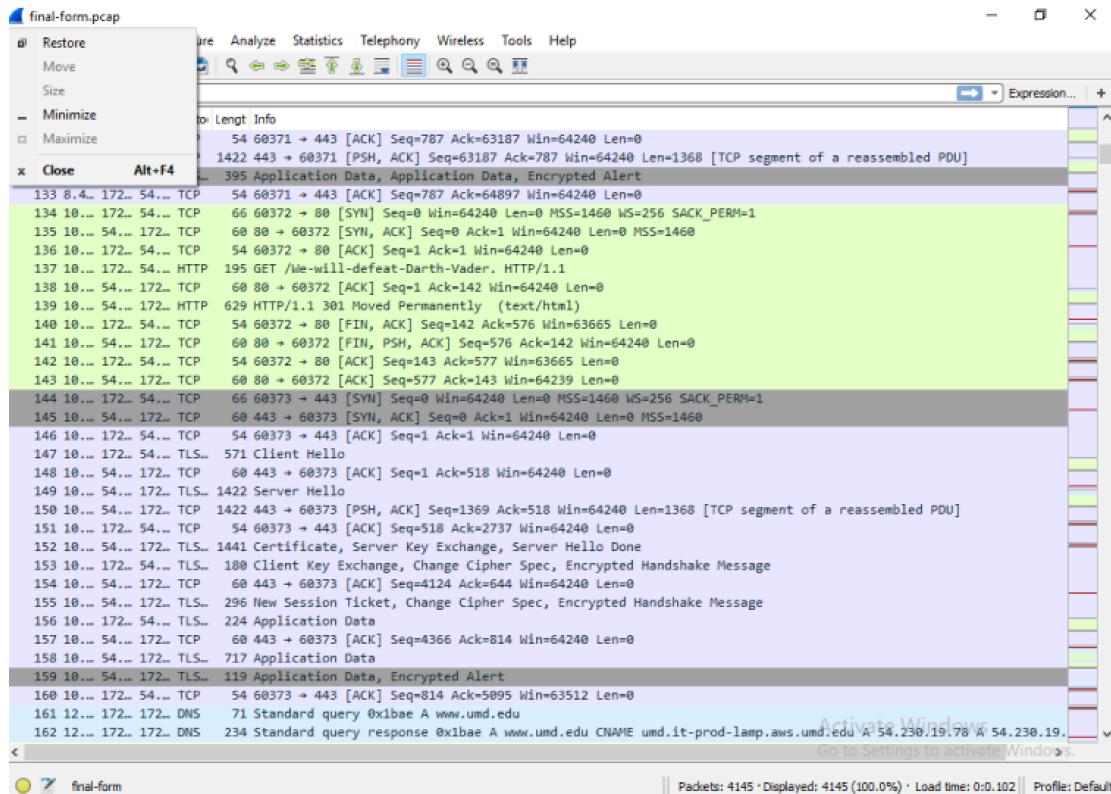
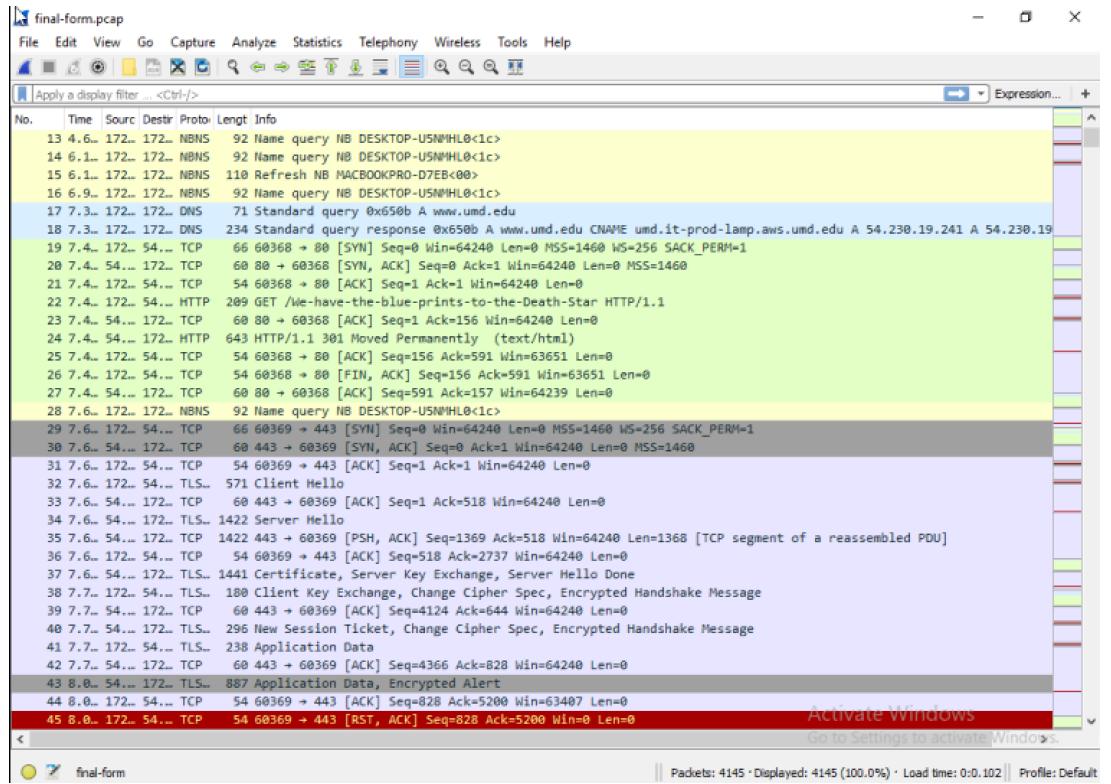
To determine the messages sent by final-form.exe which was also present in the decrypted volume, used Wireshark on running the executable to capture the packets sent.

Final-form.exe tries to make connection to www.umd.edu by making a request to it. This is followed by a 3-way handshake. Next, a GET request is made <https://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star>, which receives the request and responds with “301 moved permanently”. It then acknowledges and closes the connection. Next another GET request is made to <https://www.umd.edu/We-will-defeat-Darth-Vader> which receives the request and again responds with “301 moved permanently”. These steps are then repeated.

Messages Sent:

We have the blue prints to the Death Star
We will defeat the Darth Vader

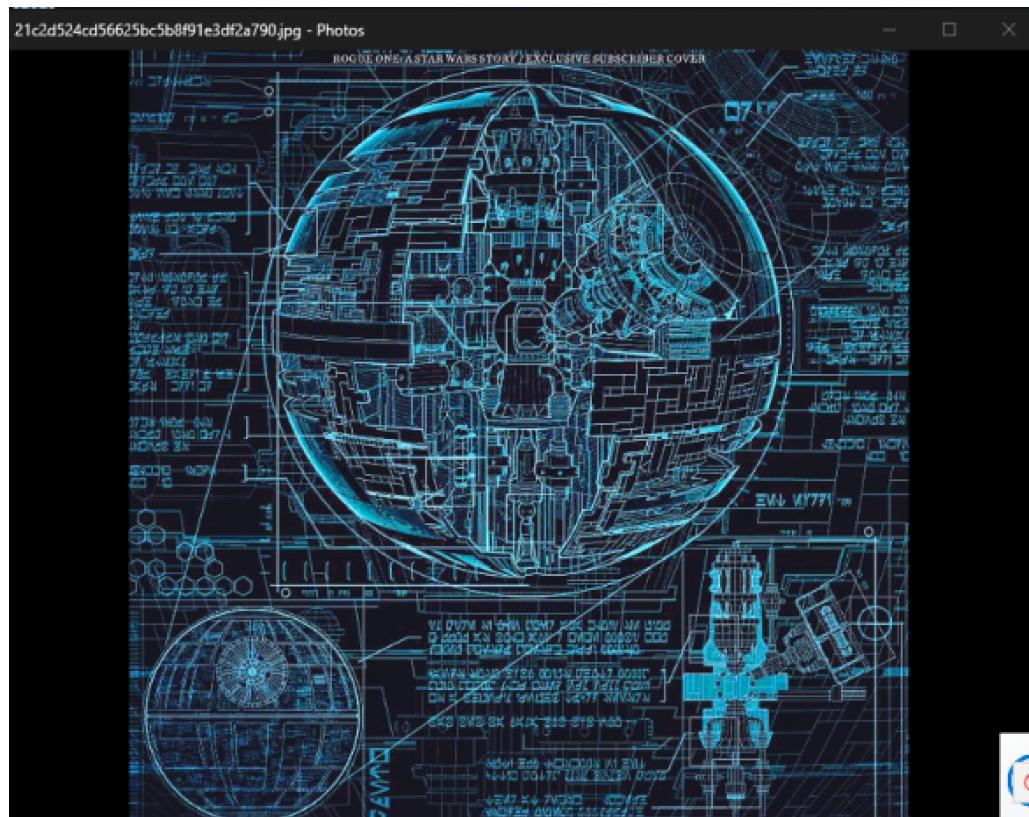
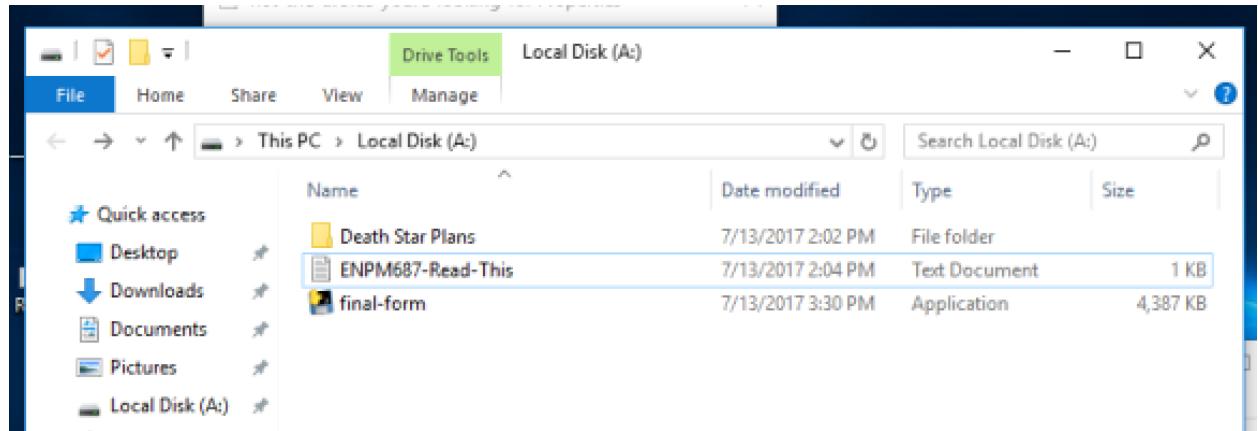
Screenshots:

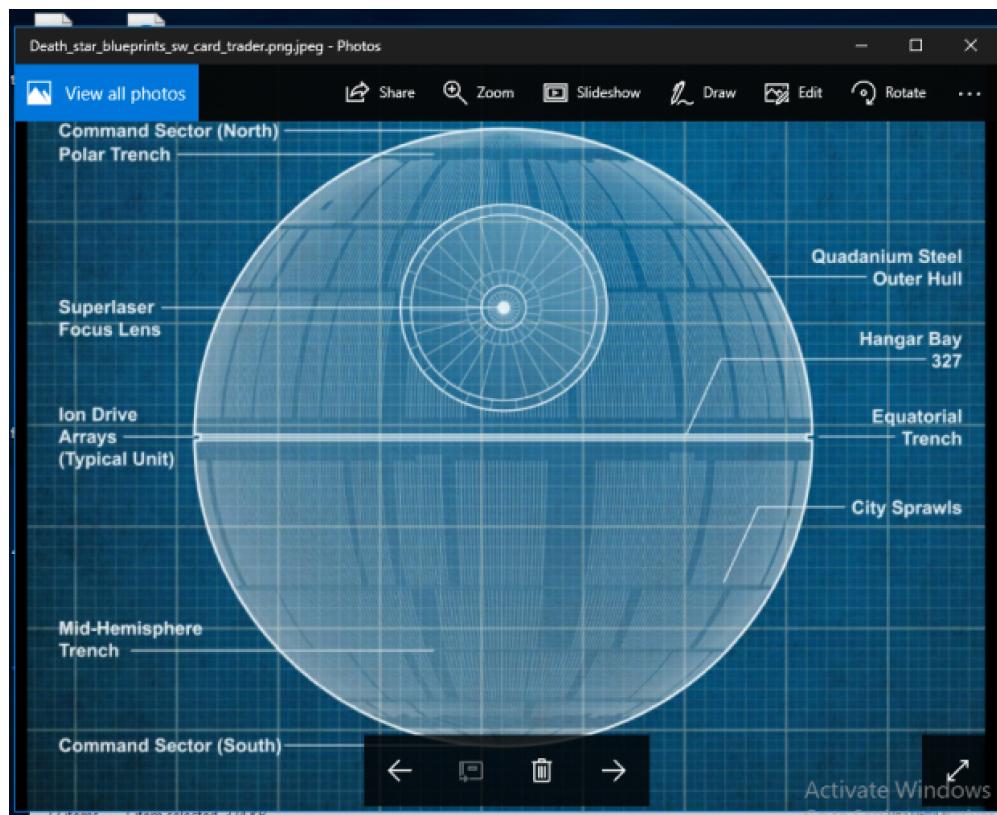
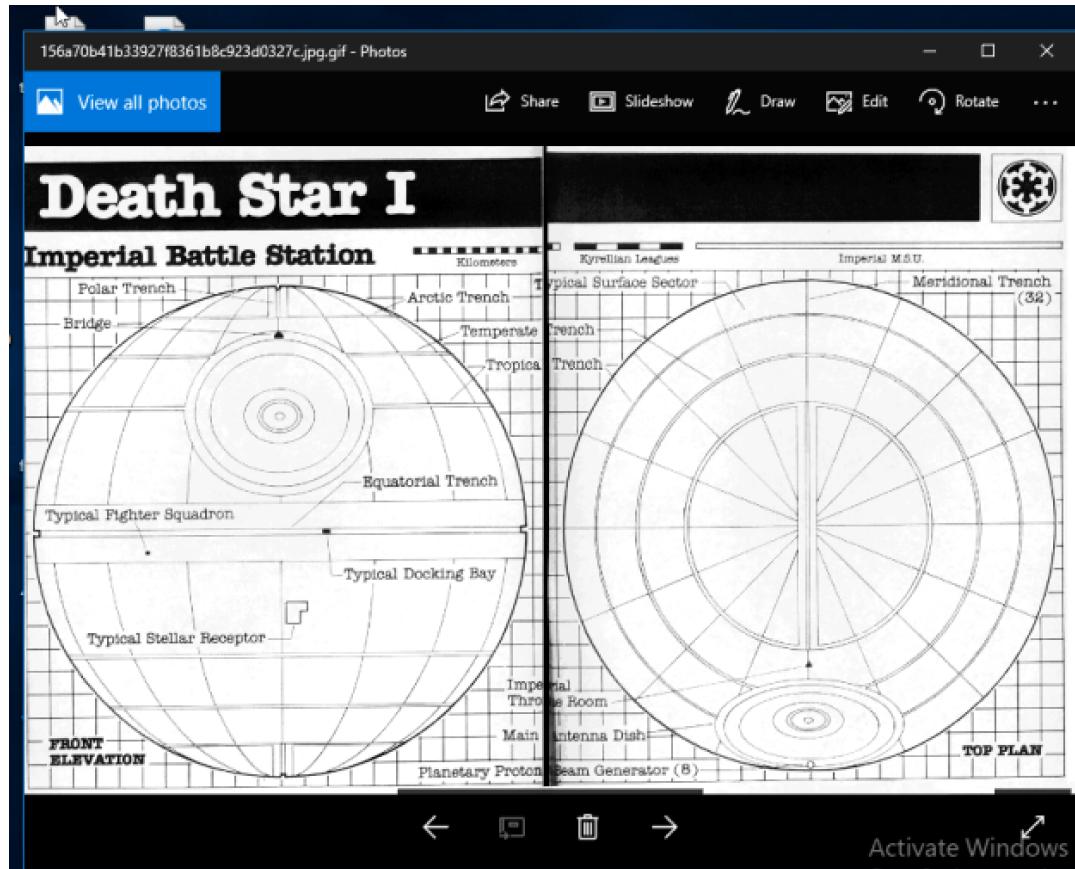


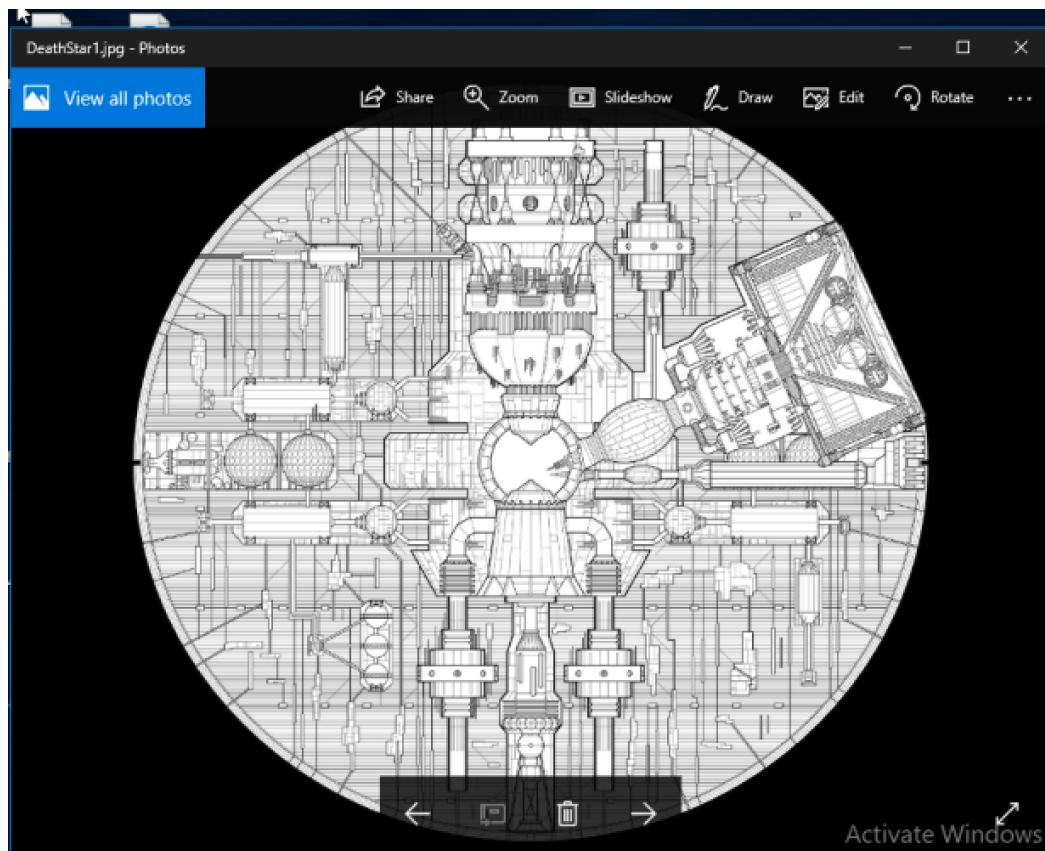
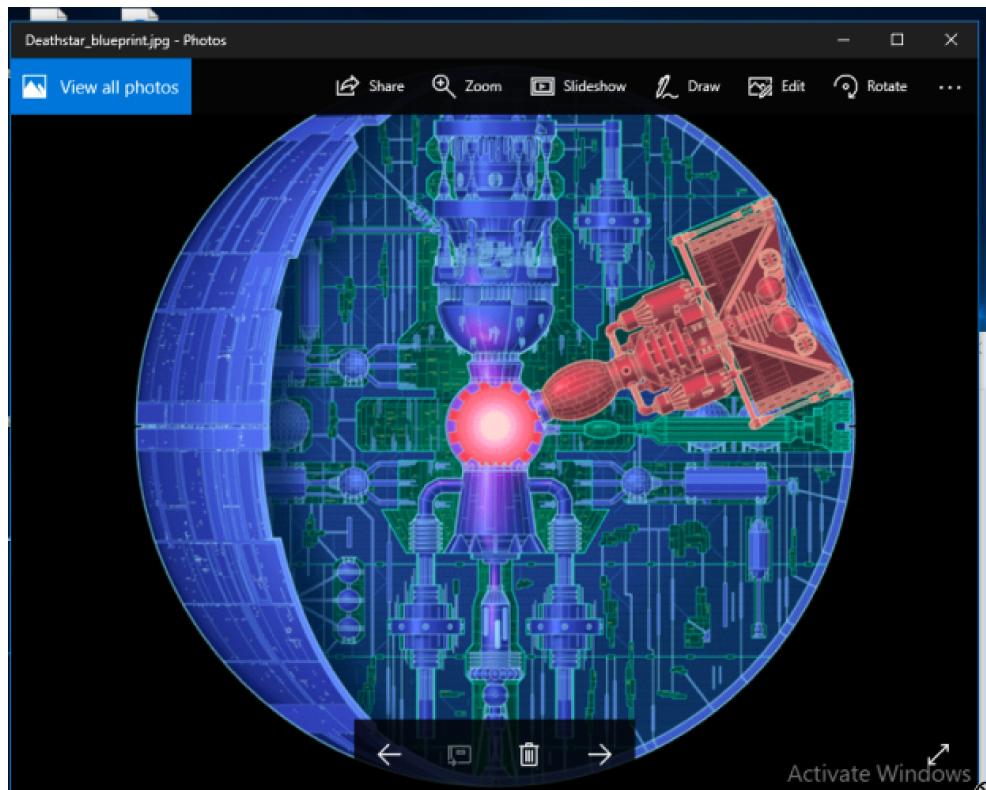
Other Interesting Findings:

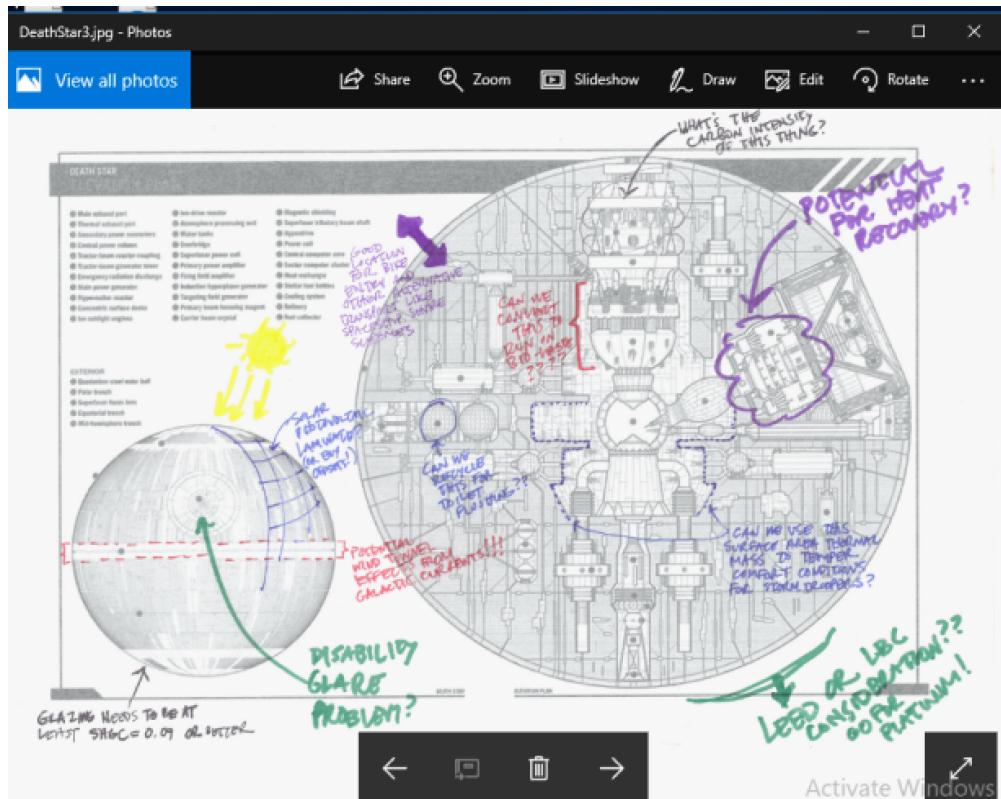
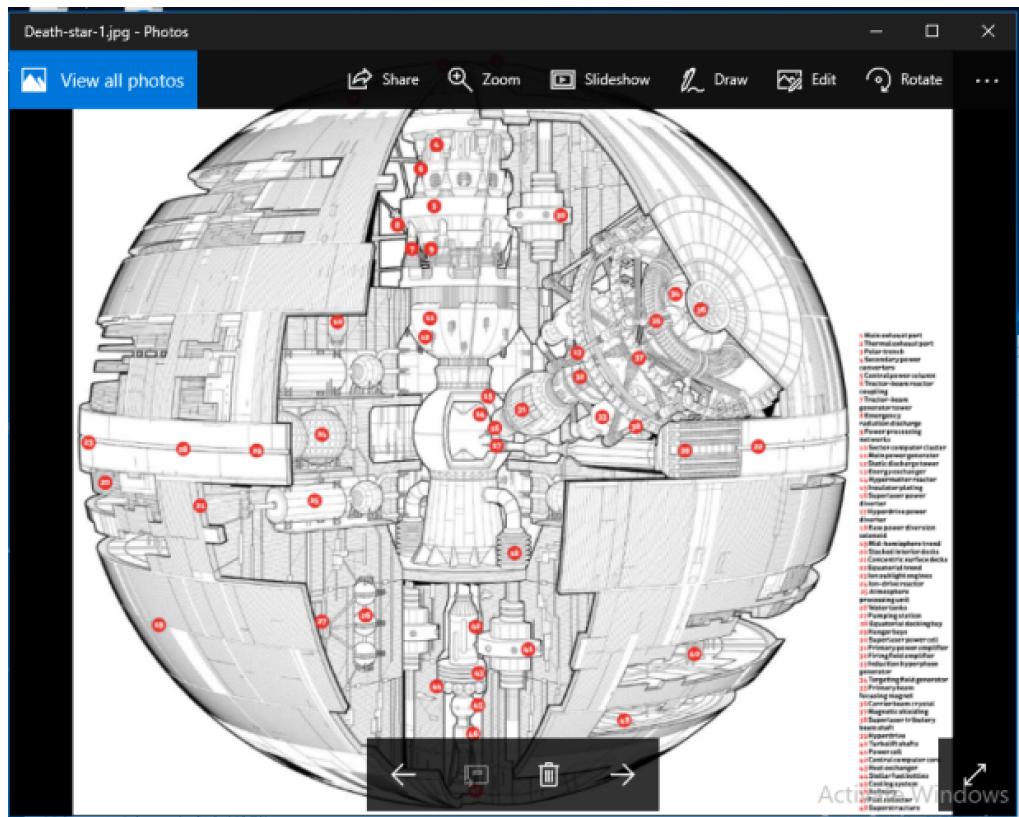
Location: Folder- Death Star Plans within Decrypted Volume

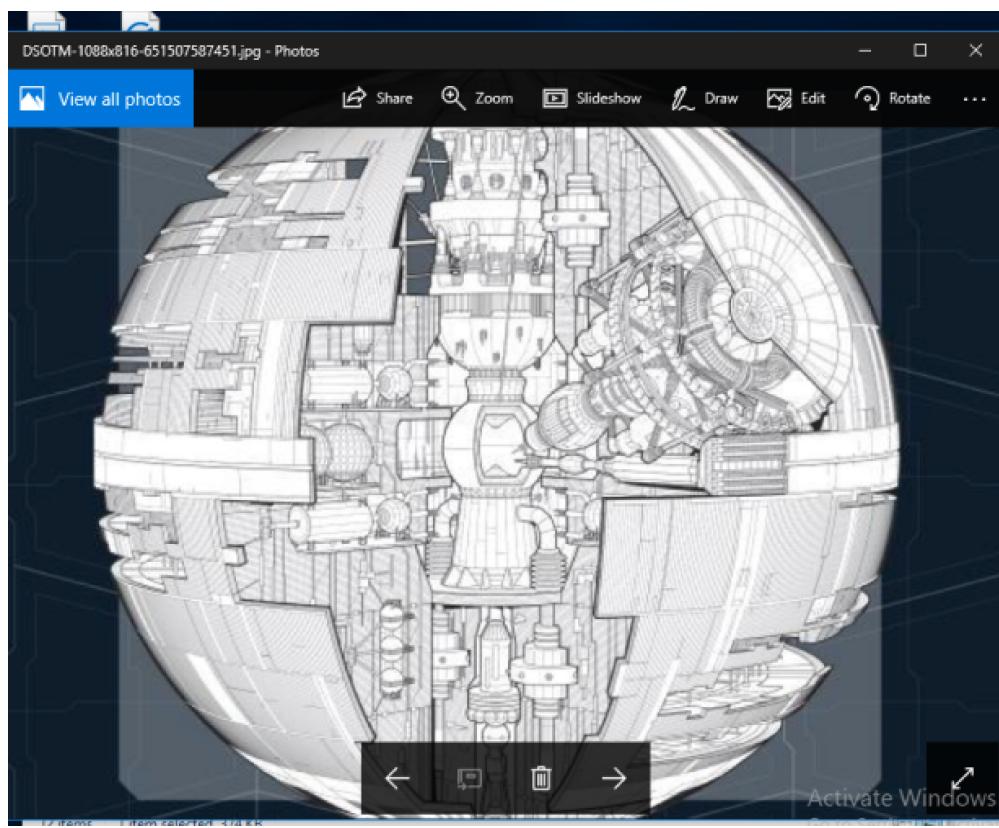
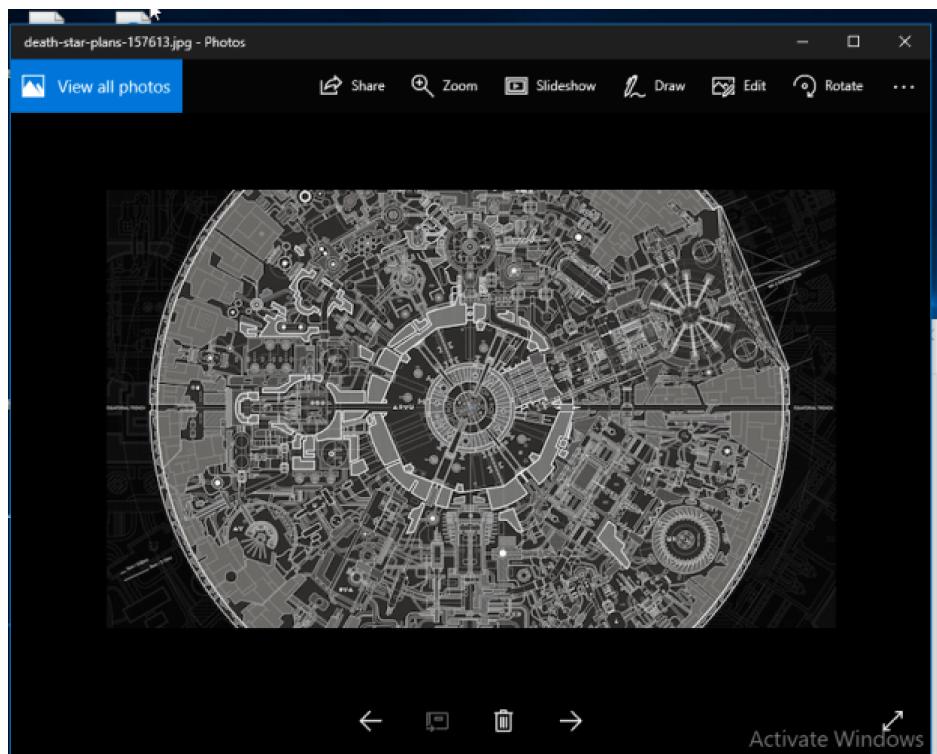
Below are images which include the blueprints of Death Star Plans

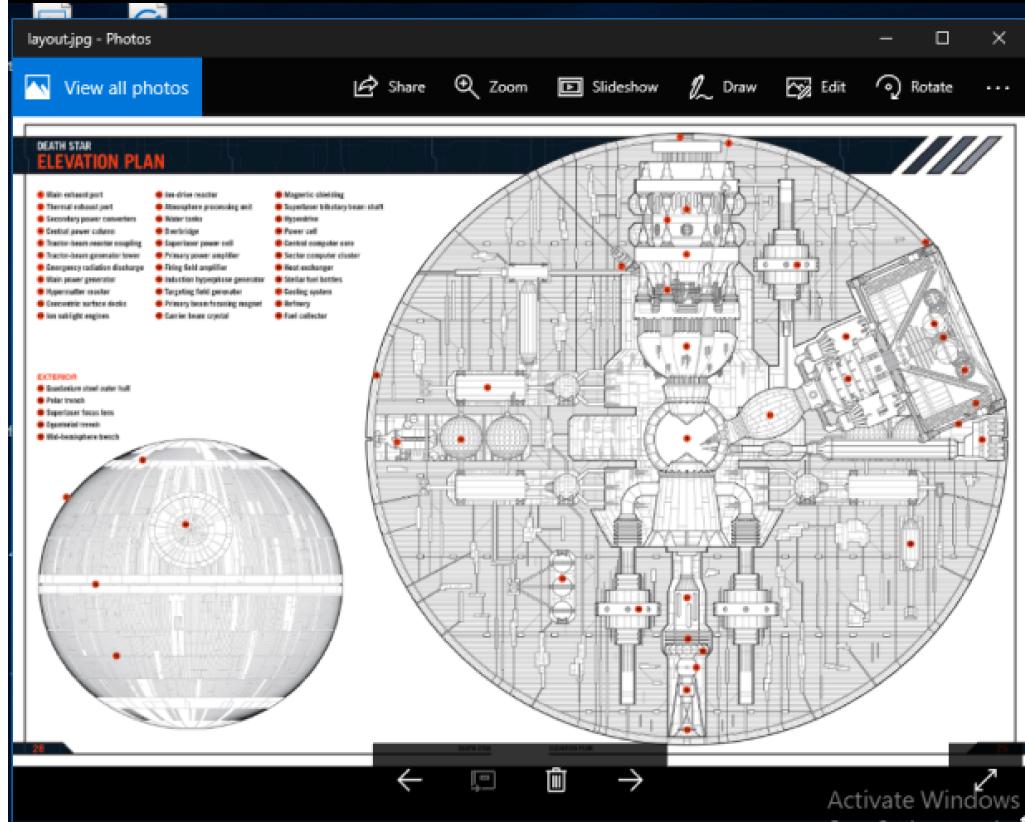
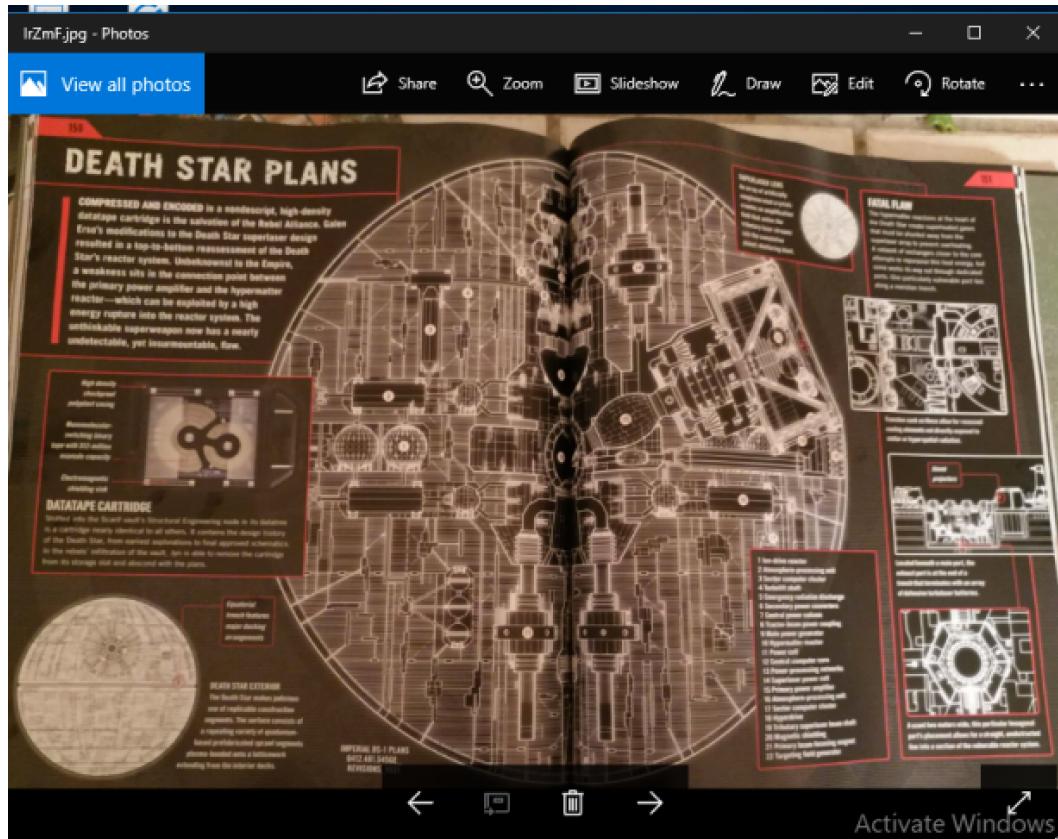


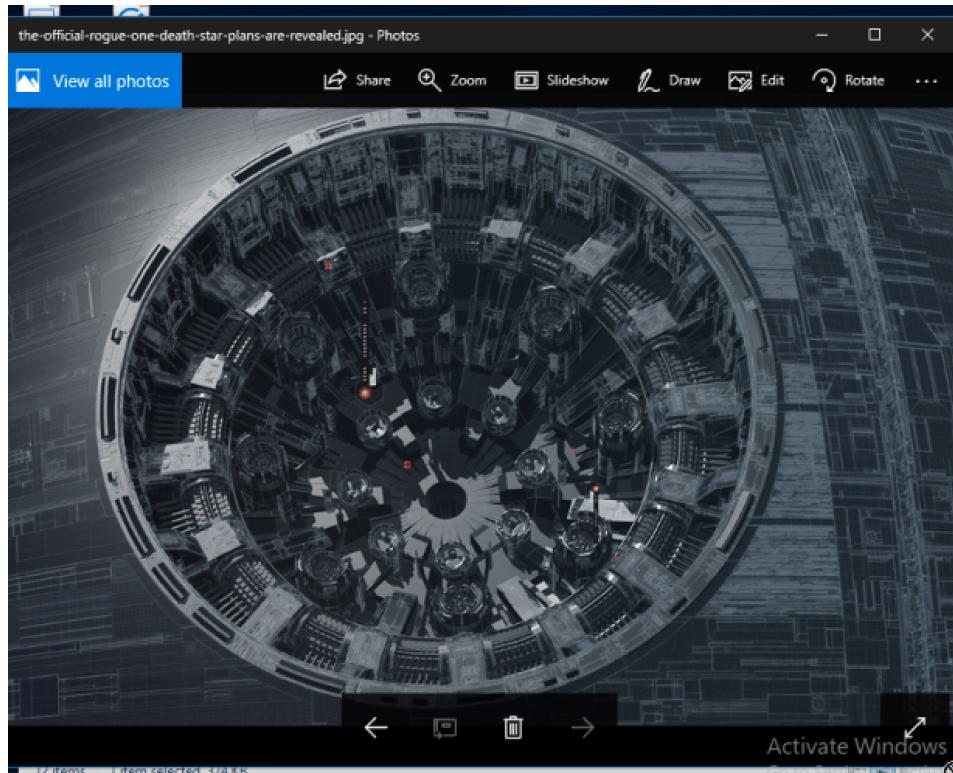












Tools Used:

Autopsy
WireShark
VeraCrypt
Online Base64 Decoder