FINAL PROJECT REPORT

Submitted to Professor Kevin Shivers

By Radhika Pai (rpai@umd.edu)

ENPM687-Digital Forensics and Incidence Response |Summer 2017

Problem Description

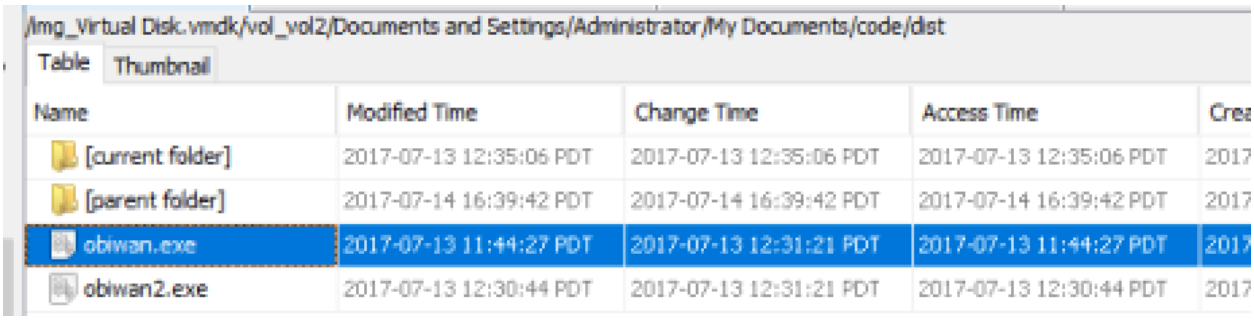
Background
You are the Imperial Forces best forensic analyst. At a great cost the Imperial Army has come into possession of an image of a hard drive for a rebel scum malware writer. Their codes have plagued our computers for the last time, infecting them but also using it to send messages across the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

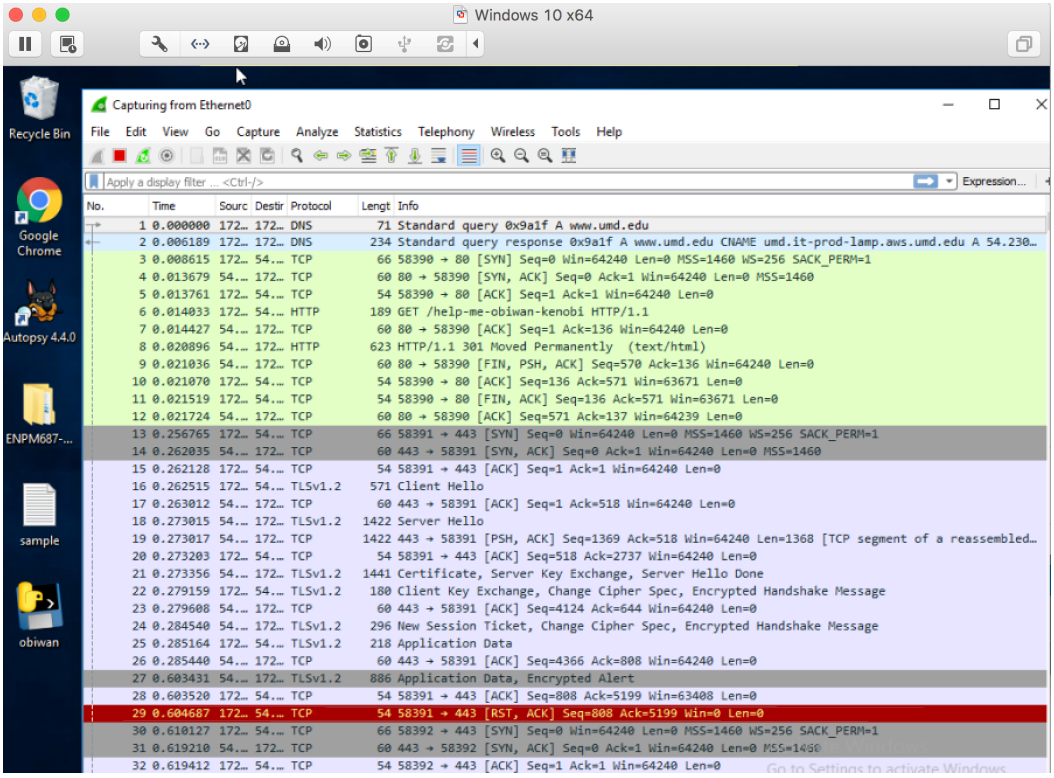
   Location:

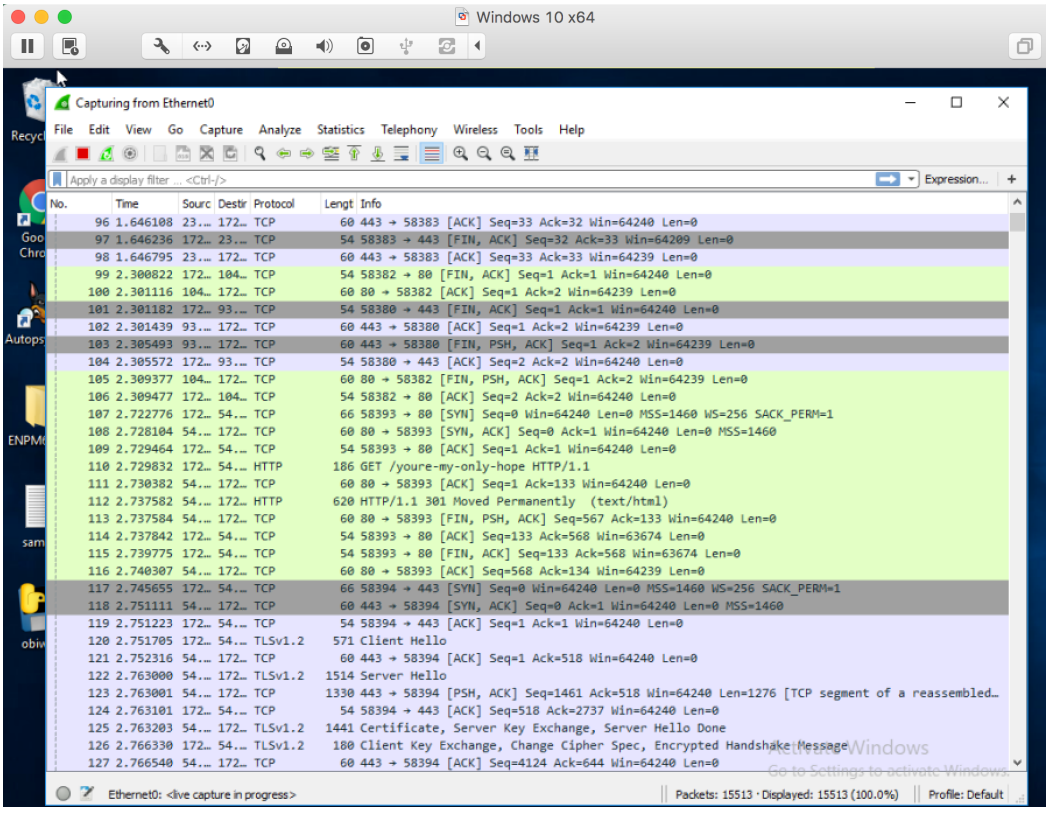


   Description:
   Obiwan.exe tries to make connection to www.umd.edu by making a request to it. This is followed by a 3-way handshake. Next, a GET request is made to https://help-me-obiwan-kenobi, which receives the request and responds with “301 moved permanently” (html/text file). It then acknowledges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

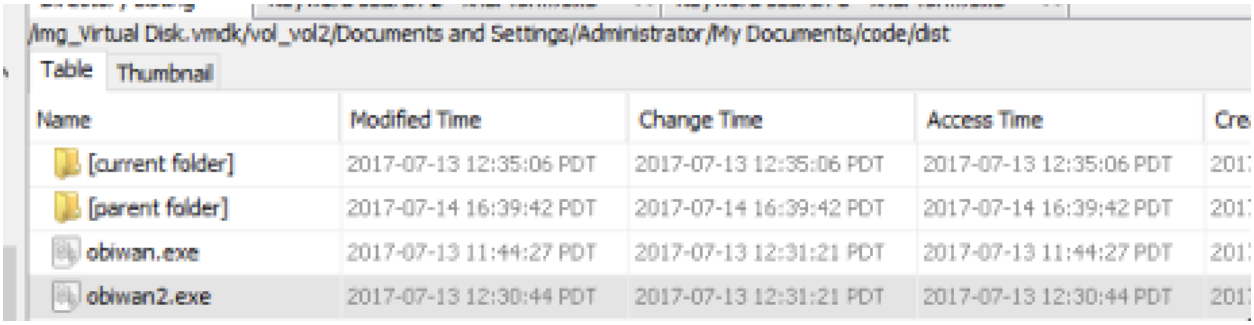
Screenshots:





2. **Obiwan2.exe**

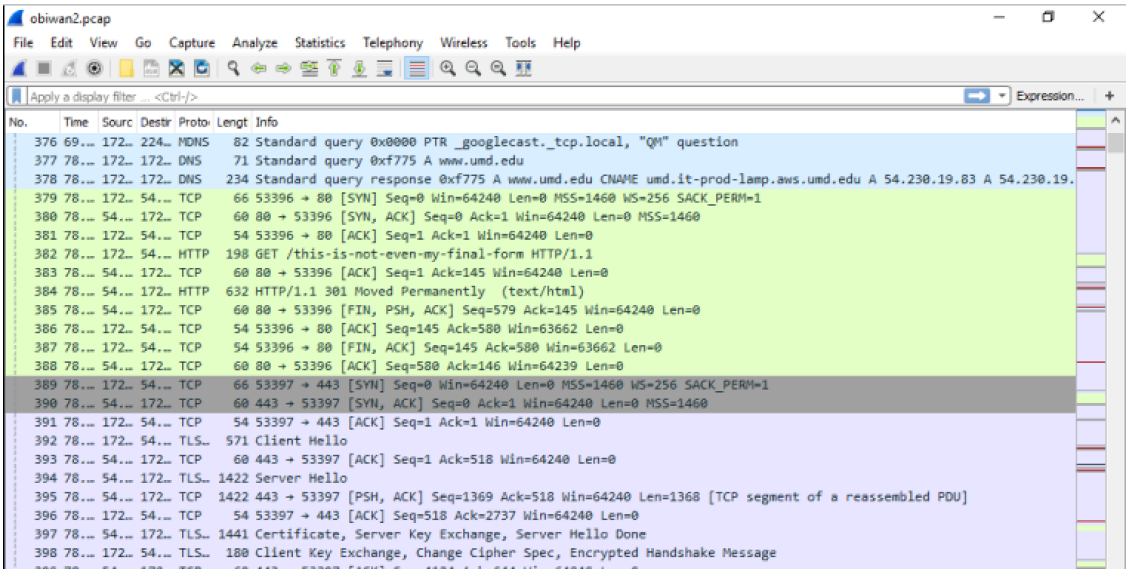
Location:

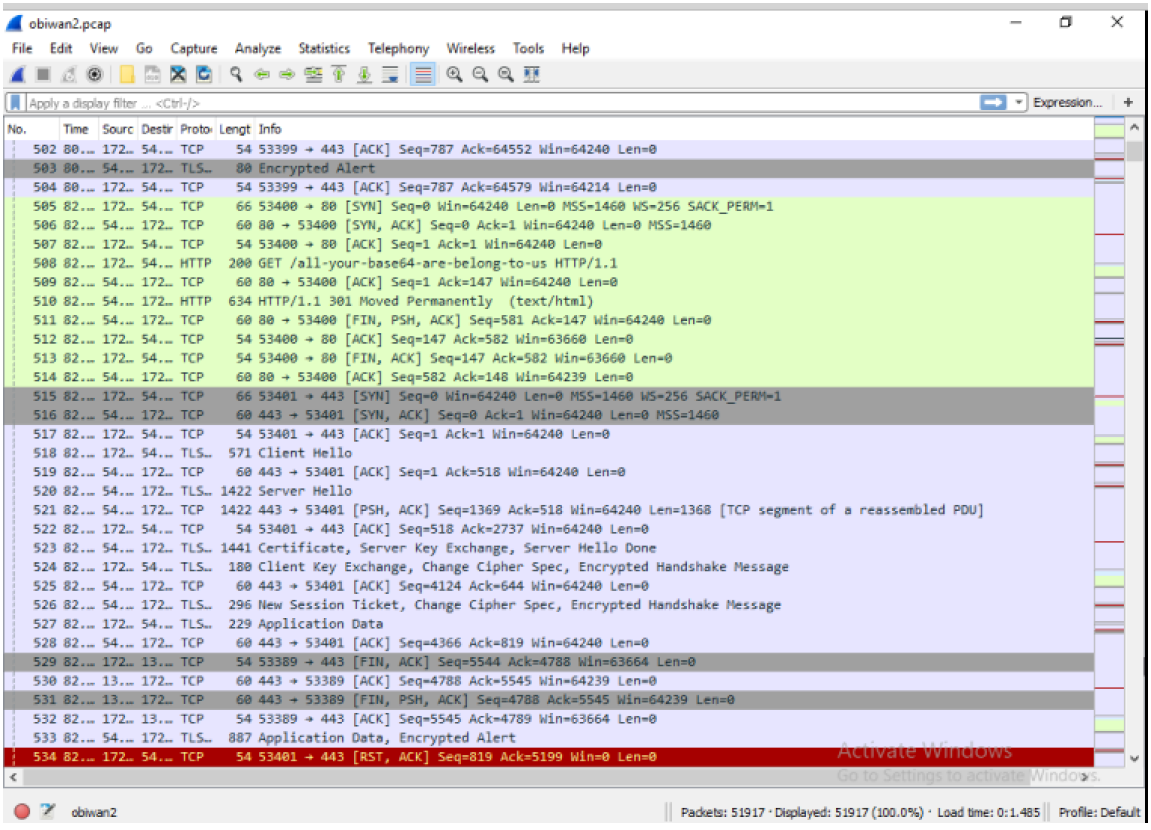


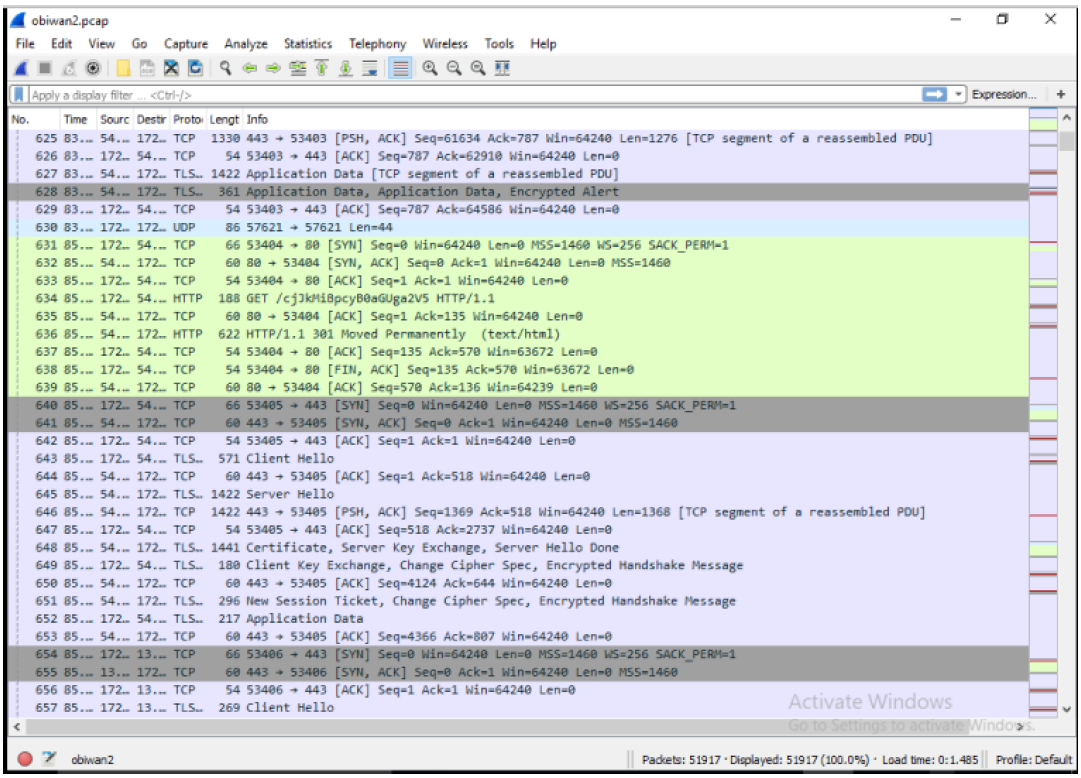
Description:
Obiwan2.exe tries to make connection to www.umd.edu by making a request to it. This is followed by a 3-way handshake. Next, a GET request is made https://www.umd.edu/this-is-not-even-my-final-form , which receives the request and responds with “301 moved permanently” (html/text file). It 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/cjJkMiBpcyB0aGUga2V5 .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 “cjJkMiBpcyB0aGUga2V5” 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
cjJkMiBpcyB0aGUga2V5 -> **r2d2 is the key**

Screenshots:



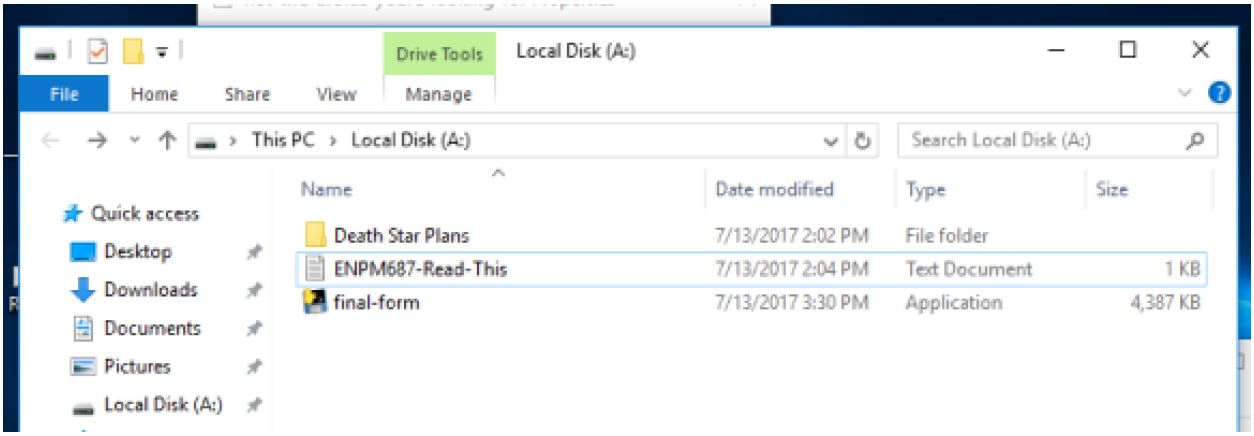




3. Death Star Plans

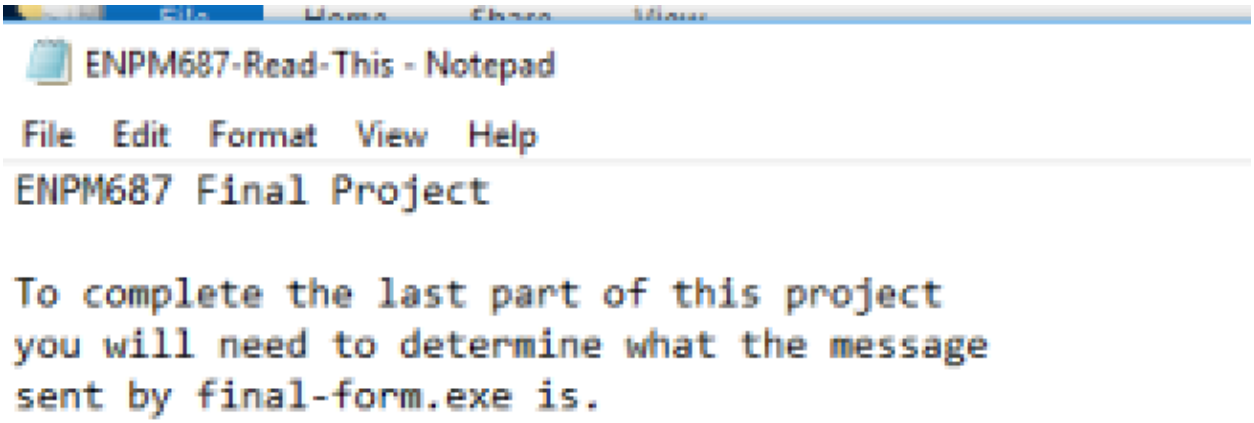
Since the attacker has VeraCrypt installed and is a music fan, used VeraCrypt to decrypt hidden contents of file **not-the-droids-you-are-looking-for.mp3** .

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.



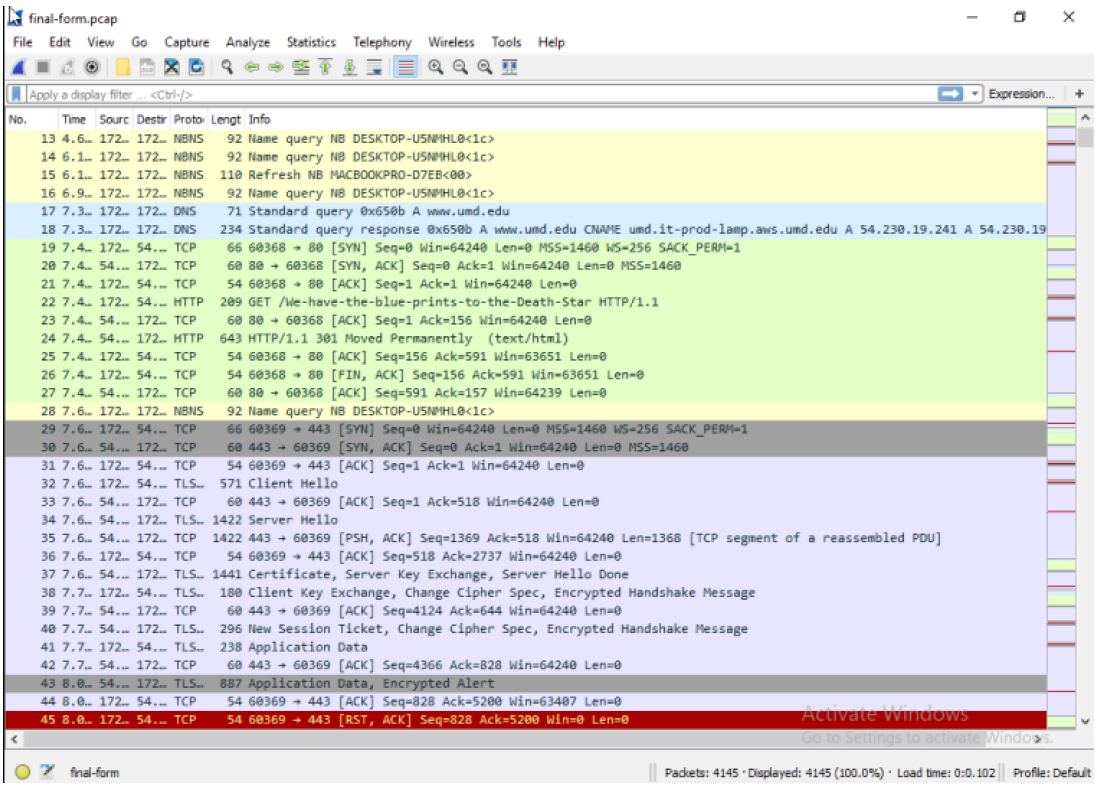
To determine the messages sent by final-form.exe which was also present in the decrypted volume, used WireShark on running the executable to capture the packets sent.

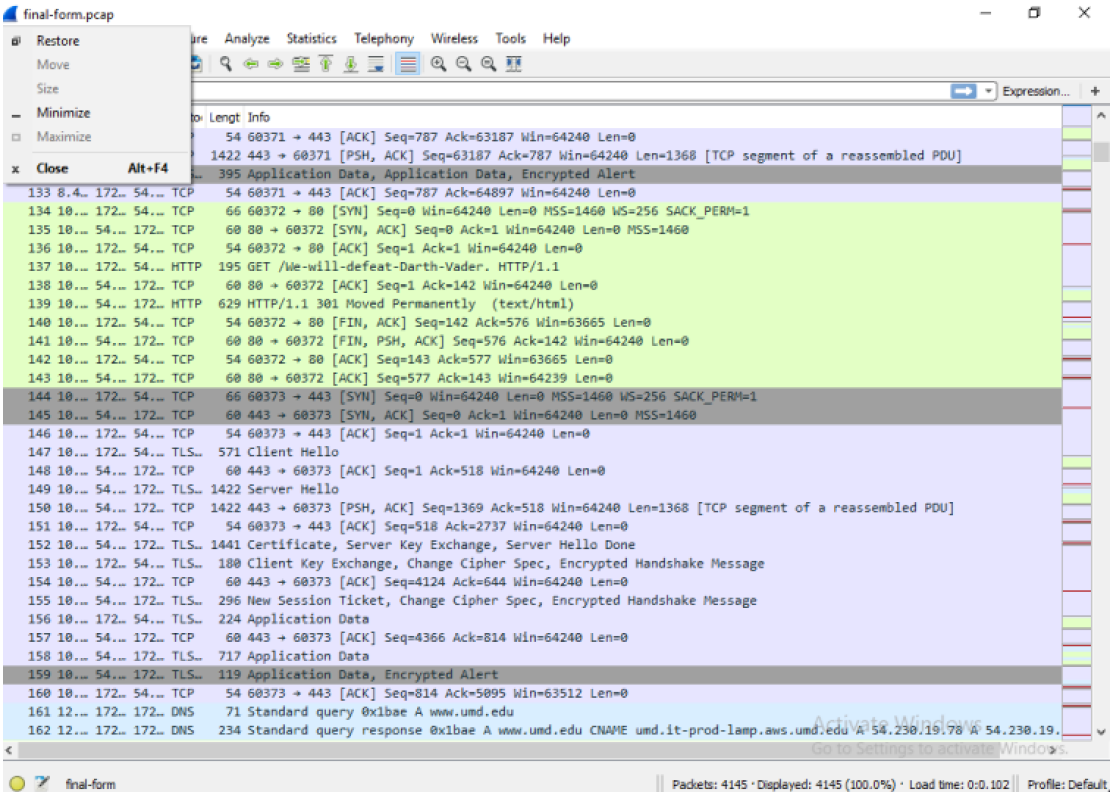
Final-form.exe tries to make connection to www.umd.edu by making a request to it. This is followed by a 3-way handshake. Next, a GET request is made https://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star, which receives the request and responds with “301 moved permanently”. It then acknowledges 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:

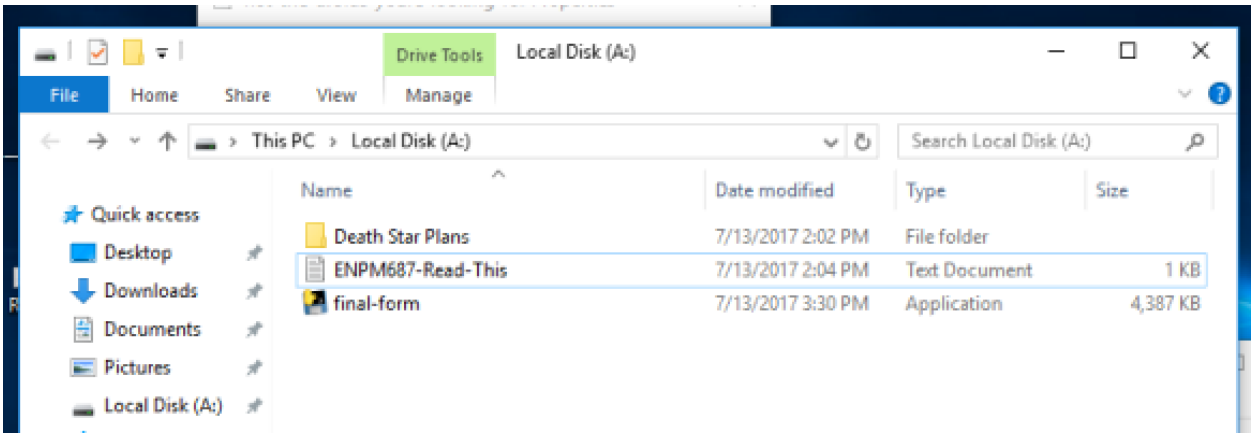


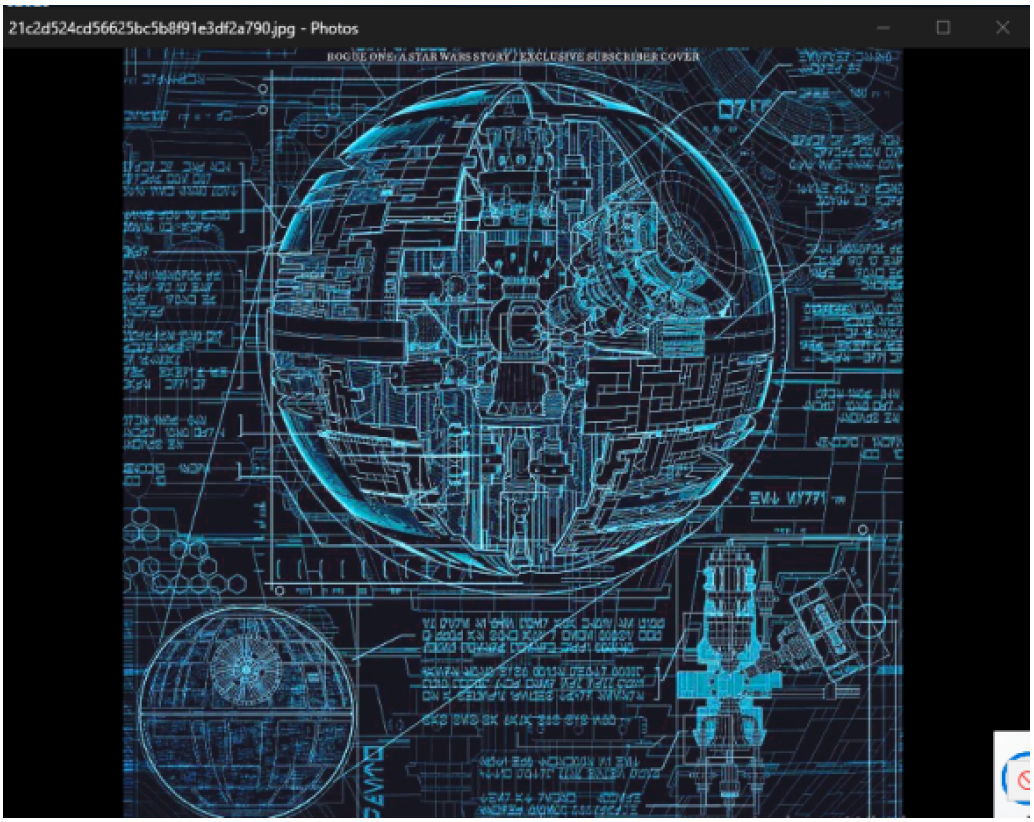


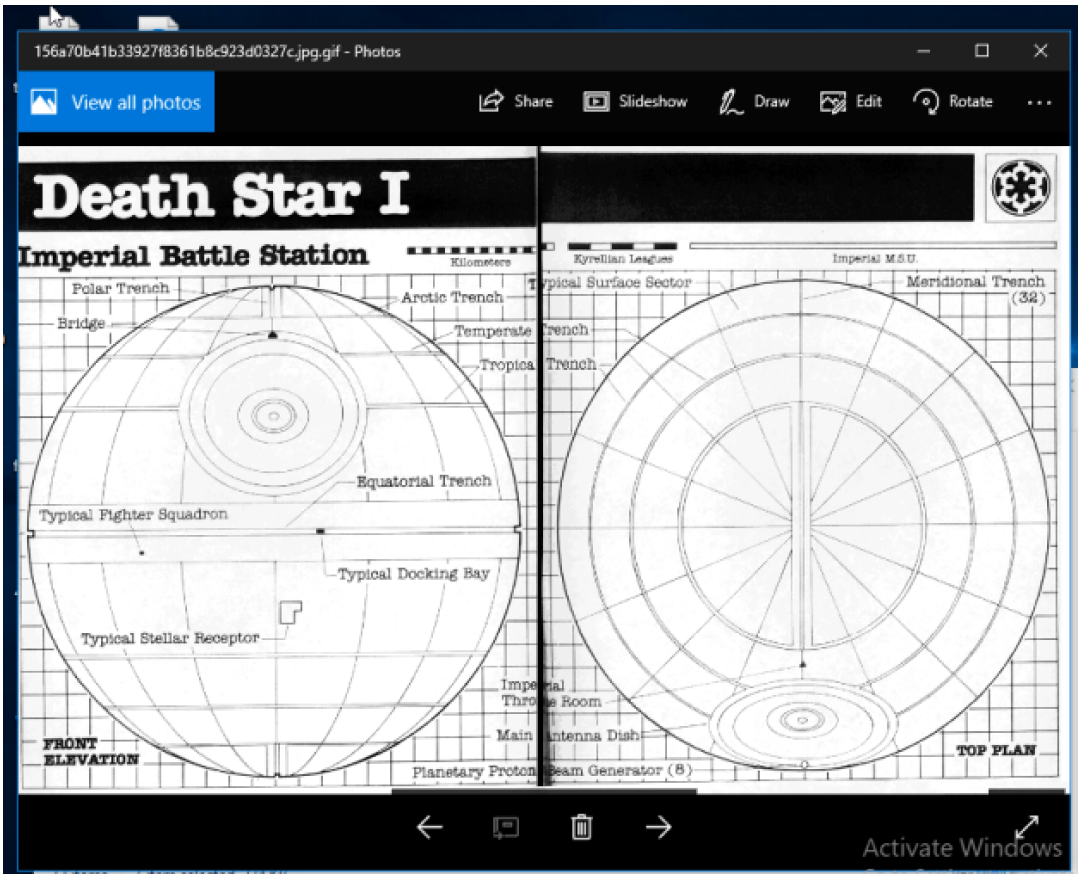
Other Interesting Findings:

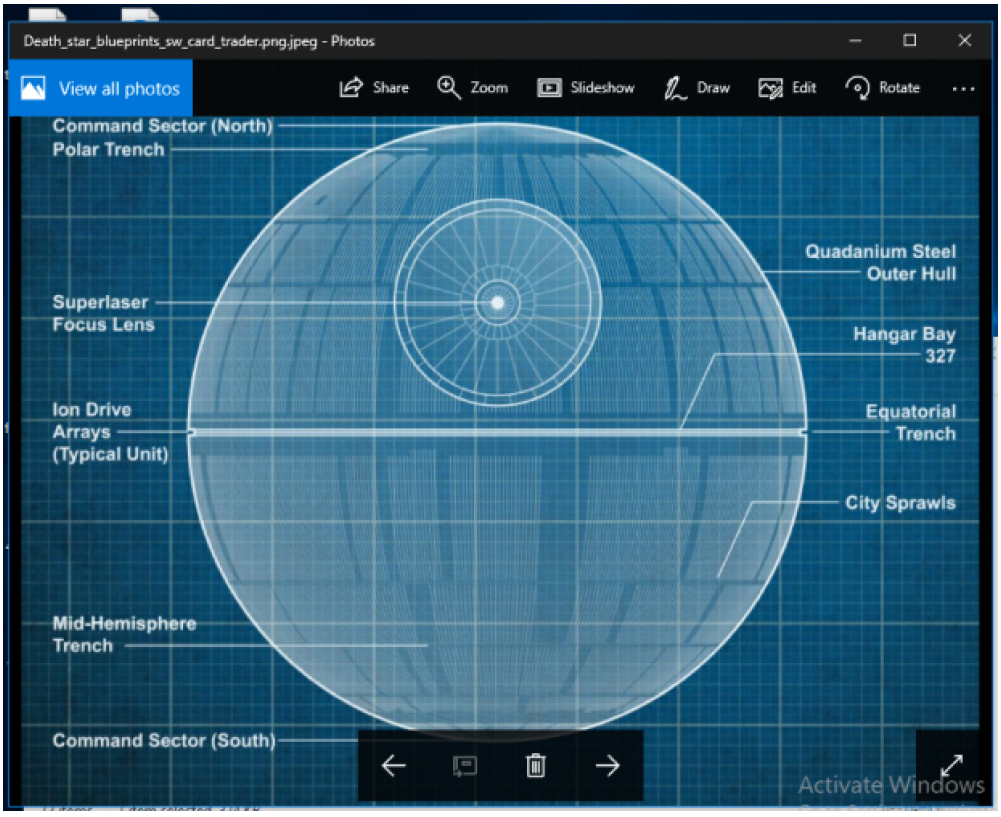
Location: Folder- Death Star Plans within Decrypted Volume

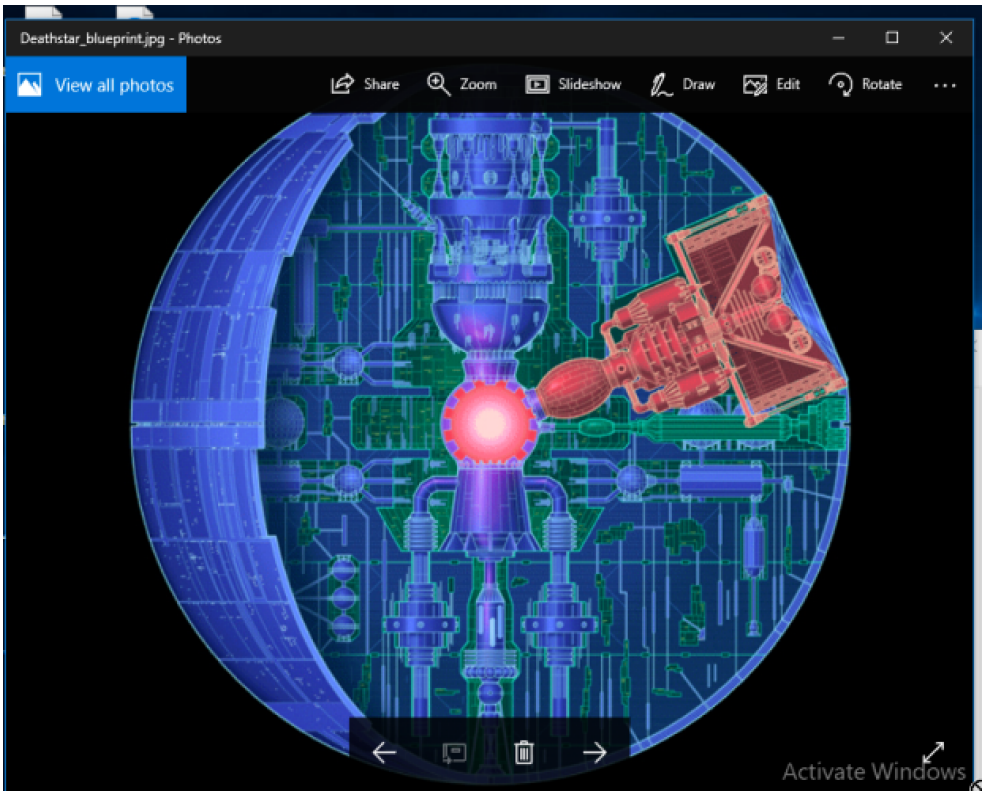
Below are images which include the blueprints of Death Star Plans

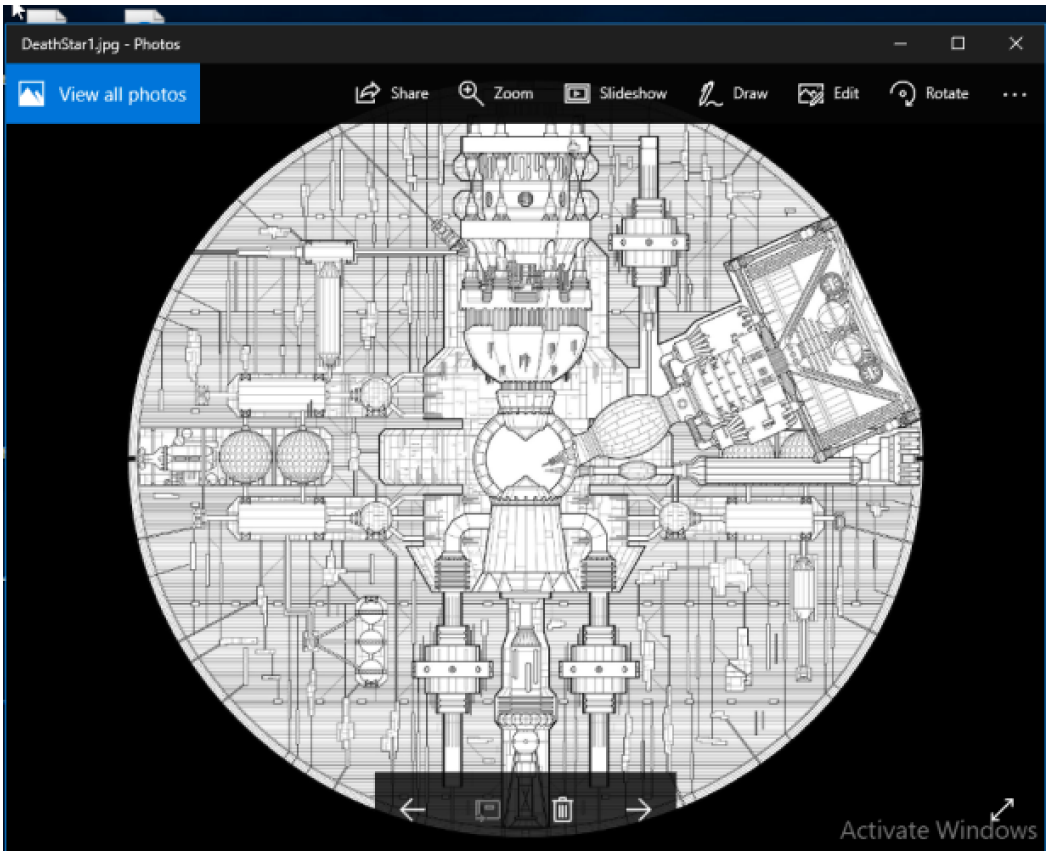


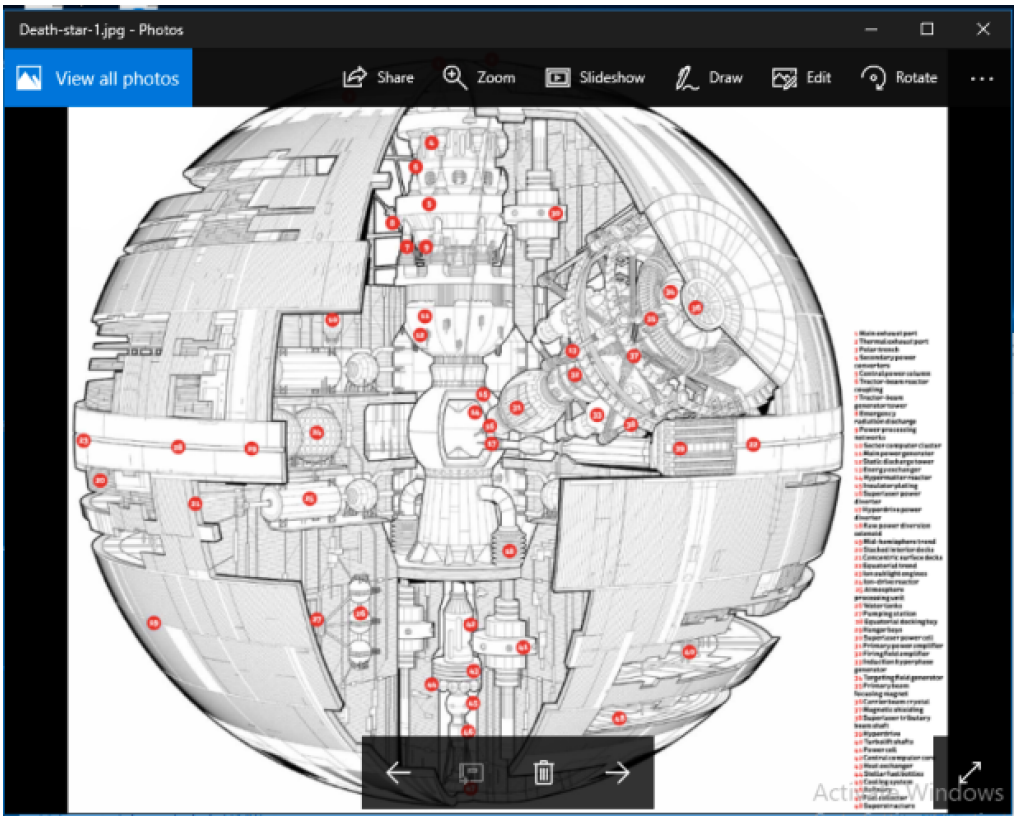


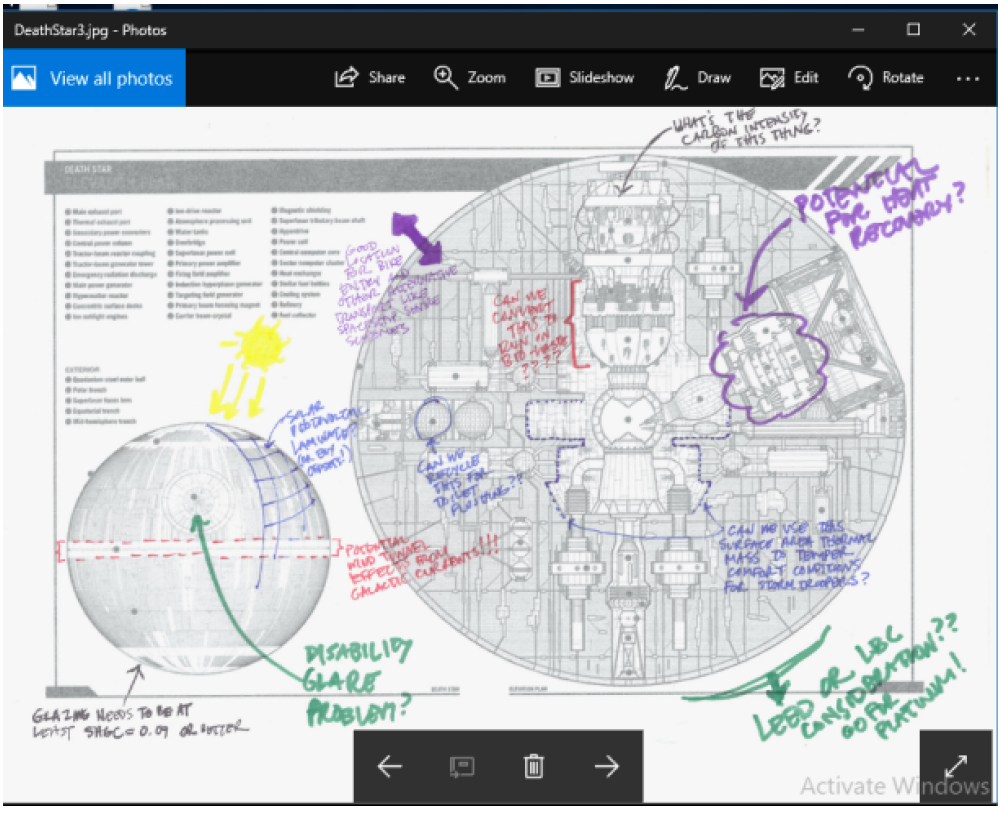

156a70b41b33927f8361b8c923d0327c.jpg.gif - Photos
View all photos
Share
Slideshow
Draw
Edit
Rotate
Death Star I
Imperial Battle Station
Kilometers
Polar Trench
Arctic Trench
Bridge
Temperate
Tropica
Equatorial Trench
Typical Fighter Squadron
Typical Docking Bay
Typical Stellar Receptor
FRONT ELEVATION
Kyrellian Leagues
Imperial M.S.U.
Meridional Trench (32)
TOP PLAN
Activate Windows

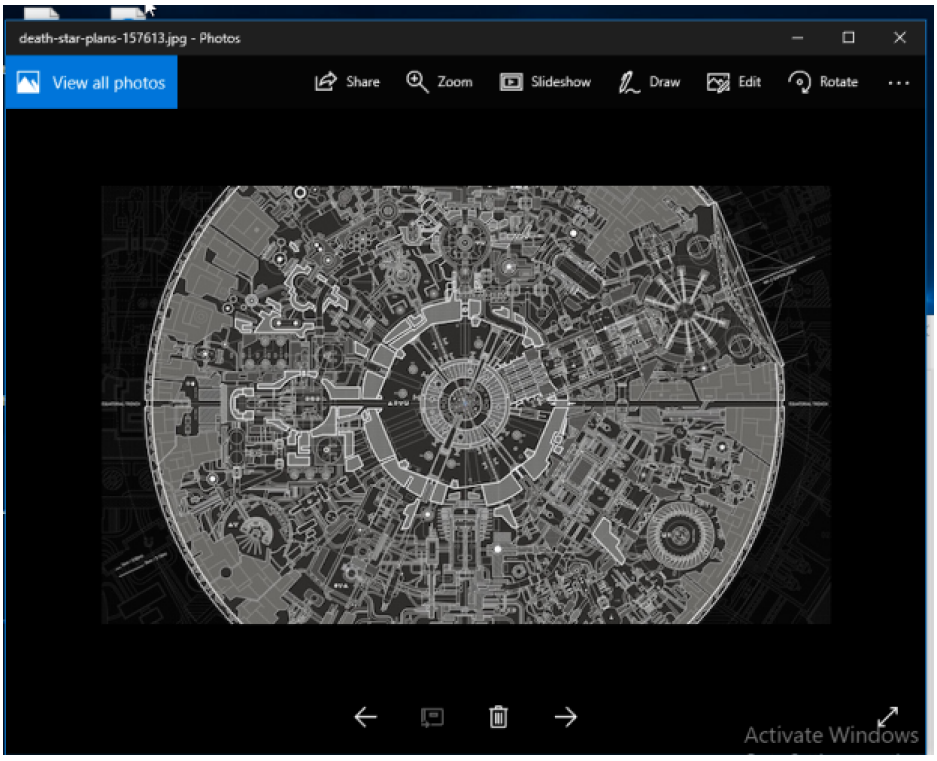

Death_star_blueprints_sw_card_trader.png.jpeg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
Command Sector (North)
Polar Trench
Quadanium Steel
Outer Hull
Superlaser
Focus Lens
Hangar Bay
327
Ion Drive
Arrays
(Typical Unit)
Equatorial
Trench
City Sprawls
Mid-Hemisphere
Trench
Command Sector (South)
Activate Windows

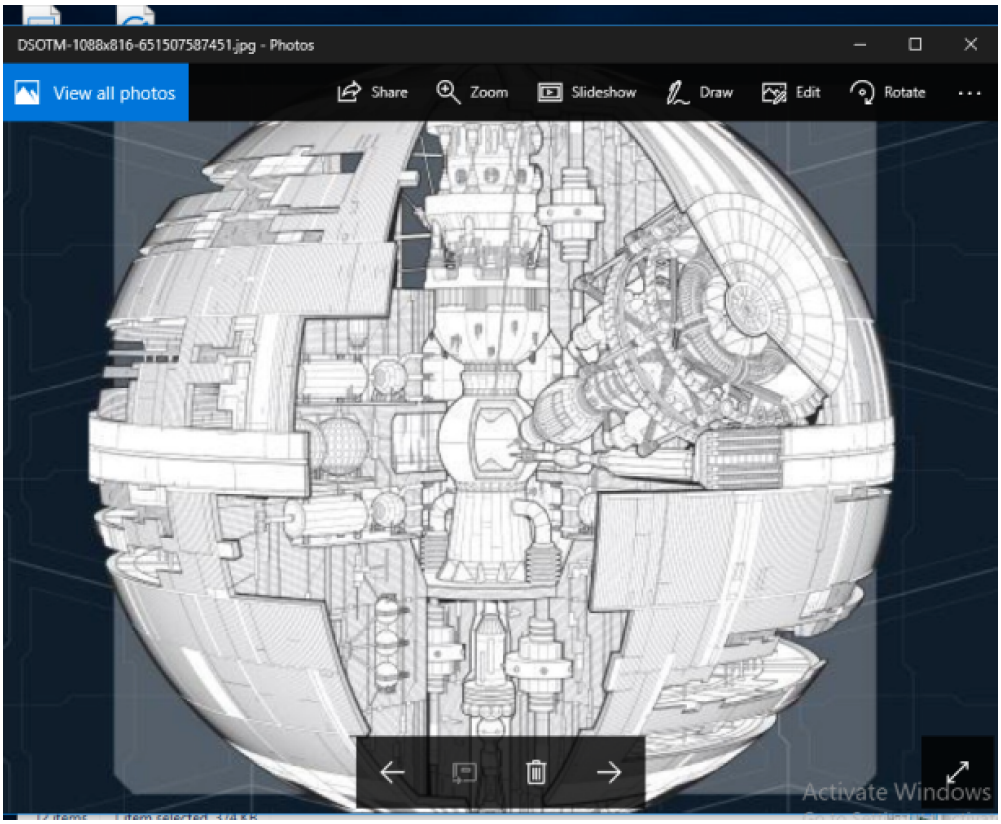

Deathstar_blueprint.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
Activate Windows

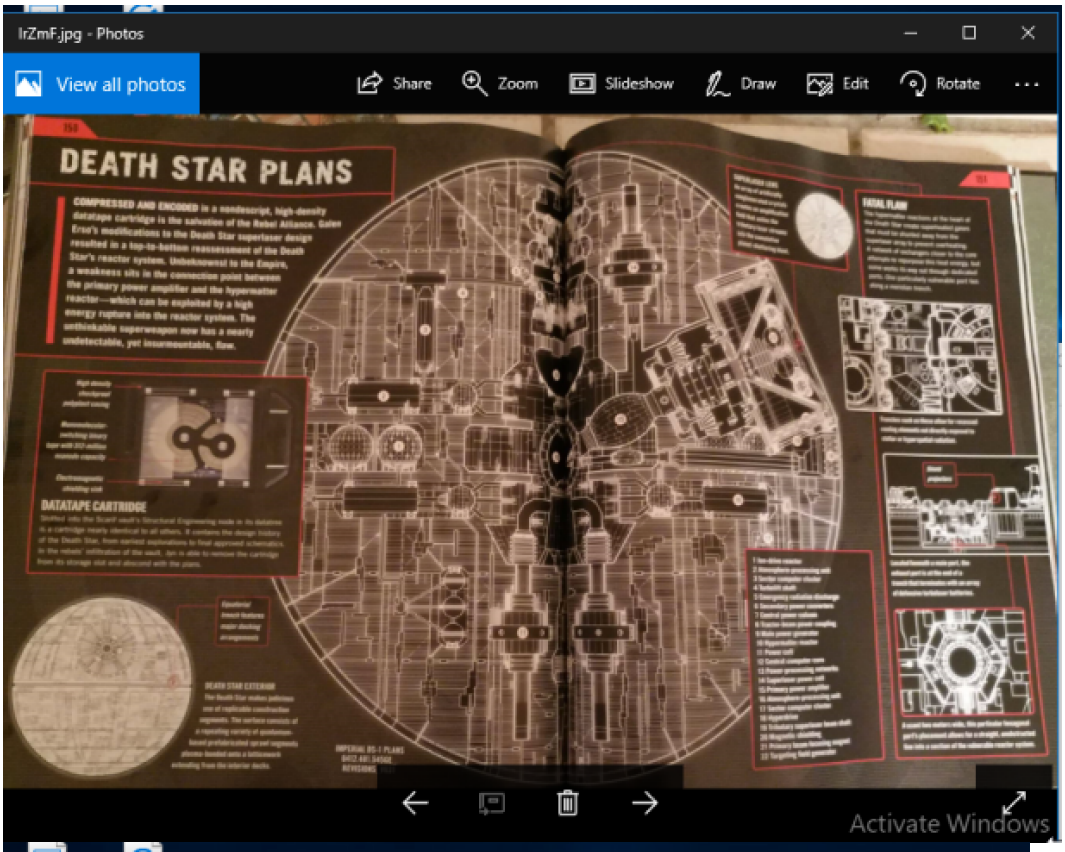

DeathStar1.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
Activate Windows

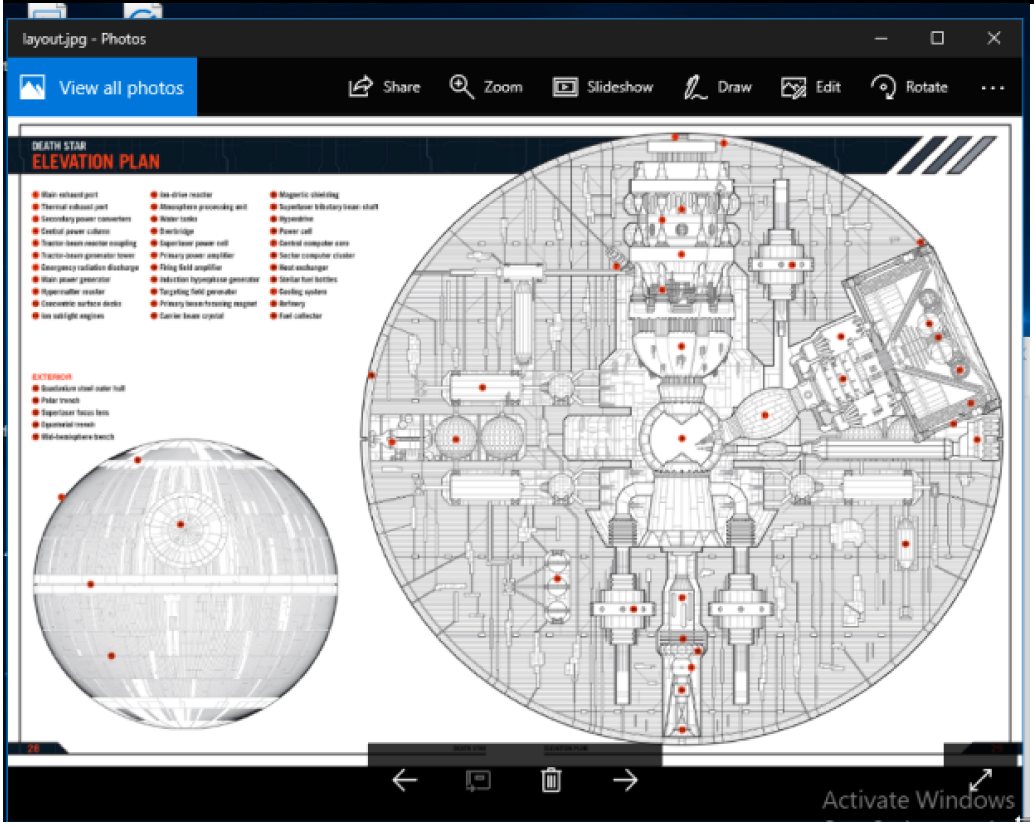

Death-star-1.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
Activate Windows

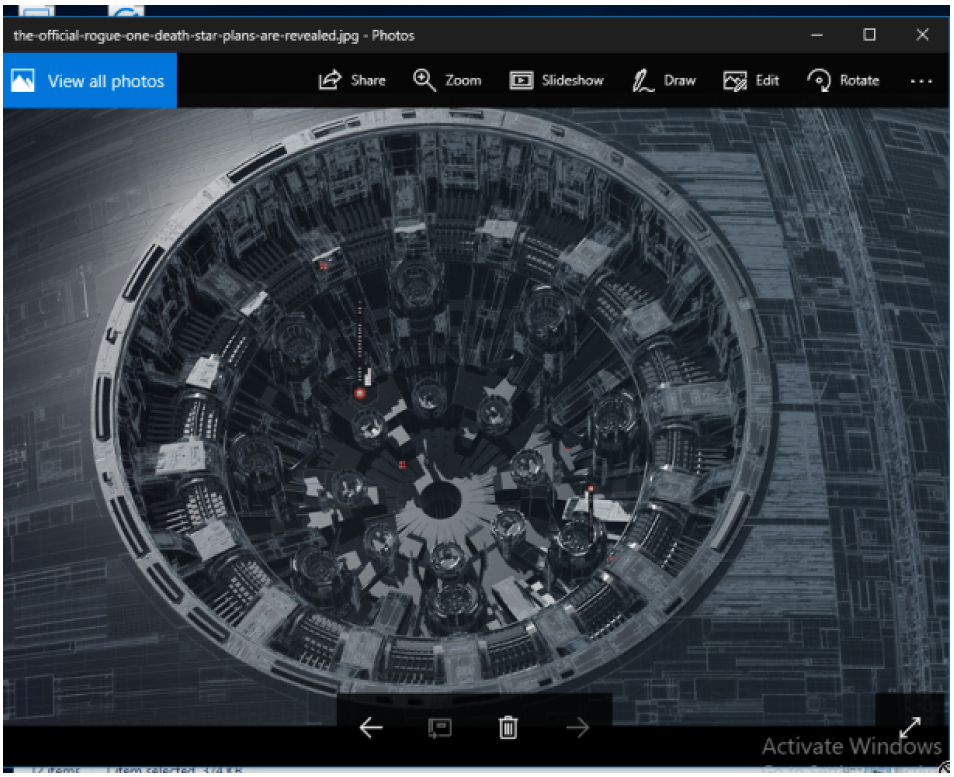

DeathStar3.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
WHAT'S THE CARBON INTENSITY OF THIS THING?
POTENTIAL FOR HEAT RECOVERY?
DISABILITY GLARE PROBLEM?
LEED OR LBC CONSIDERATION?? GO FOR PLATINUM!
Activate Windows


death-star-plans-157613.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
Activate Windows


DSOTM-1088x816-651507587451.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
Activate Windows


IrZmF.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
DEATH STAR PLANS
COMPRESSED AND ENCODED is 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.
DATATAPE CARTRIDGE
DEATH STAR EXTERIOR
IMPERIAL DS-1 PLANS
Activate Windows


layout.jpg - Photos
View all photos
Share
Zoom
Slideshow
Draw
Edit
Rotate
DEATH STAR
ELEVATION PLAN
EXTERIOR
Activate Windows



Tools Used:

Autopsy
WireShark
VeraCrypt
Online Base64 Decoder