

# **ENPM687-CY01 Final**



**Jayraj A. Vakil**

**UID: 119188361**

## Brief Summary of Information

During forensic analysis, two suspicious executables, obiwan.exe and obiwan2.exe, were found. Obiwan2.exe contained a decoded "r2d2" message. Decrypting "not-the-droids-youre-looking-for.mp3" using VeraCrypt revealed Death Star plans. Running "Final-form.exe" displayed messages about Death Star blueprints and defeating Darth Vader, concluding the investigation.

## Tools used in the investigation

**Autopsy:** Autopsy is a widely used open-source digital forensics platform that assists in the analysis of digital media. It provides a graphical interface for examining file systems, recovering data, and uncovering evidence in a forensic investigation.

**Wireshark:** Wireshark is a network packet analyzer that allows for the capture and inspection of network traffic. It is used to monitor and analyze data packets transmitted over a network, making it valuable for understanding network activities during forensic investigations.

**VeraCrypt:** VeraCrypt is an open-source disk encryption software that provides strong data protection by encrypting entire disk volumes. In this investigation, it was used to decrypt an encrypted VeraCrypt volume, revealing its contents.

**Base64 decoder:** It is used to decode base64 text to plain text.

## Repository

### **A. Summary of Evidence**

The forensic analysis of a Windows XP virtual machine revealed two suspicious executable files, "obiwan.exe" and "obiwan2.exe," which made outbound connections to unique URLs. Decoding a base64-encoded string from one of the URLs uncovered the password 'r2d2.' Subsequent investigation in the Autopsy software identified an encrypted VeraCrypt volume and an MP3 file. Using the 'r2d2' password, the VeraCrypt volume was decrypted, revealing a text message, an executable file, and a folder named 'Death Star Plans' containing images and plans. The executable, when run, connected to websites related to defeating 'Darth Vader' and obtaining Death Star blueprints.

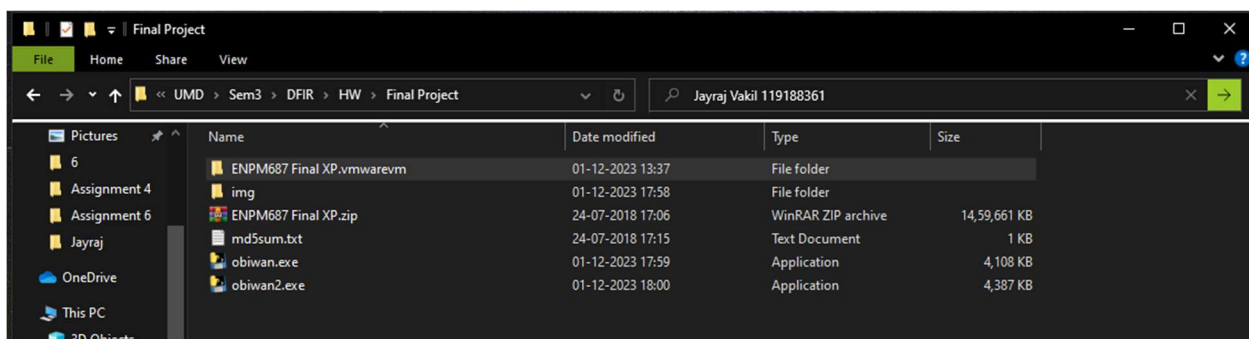
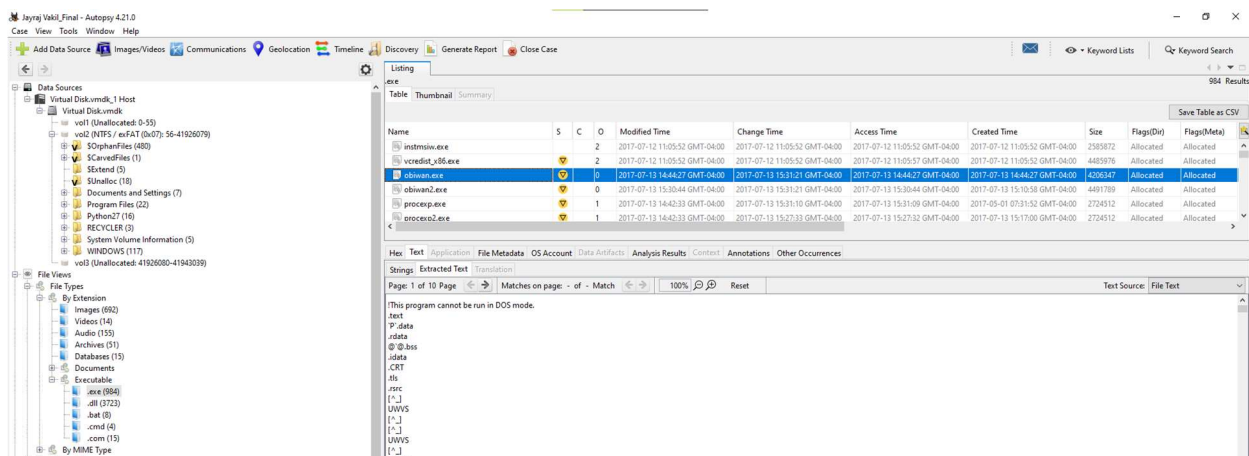
### **B. Analysis**

Upon loading the drive image into the Autopsy software, a comprehensive analysis of the data ensued. Given that the virtual machine in question operated on a Windows

XP platform, the initial suspicion was directed towards the possibility of malicious software manifesting as executable files. In accordance with this hypothesis, a search was conducted for files with the .exe extension, which resulted in the discovery of two distinctive files named "obiwan.exe" and "obiwan2.exe". The obiwan.exe is found at the location /img\_Virtual Disk.vmdk/vol\_vol2/Documents and Settings/Administrator/My Documents/code/dist/obiwan.exe

Obiwan2.exe is found at the location /img\_Virtual Disk.vmdk/vol\_vol2/Documents and Settings/Administrator/My Documents/code/dist/obiwan2.exe

The uniqueness of these file names raised intrigue, prompting their extraction to the local system for further examination.



Subsequently, both executables underwent execution, with a focus on monitoring their network activities through Wireshark. This network traffic assessment revealed that both executables were making outbound connections to specific websites.

"Obiwan.exe" was observed to be reaching out to the following URLs:

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

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

The image shows a Wireshark network traffic capture. The top pane displays a list of network packets. The bottom pane shows the details of a selected packet (Frame 4), which is an HTTP GET request. The packet details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.007666	10.104.73.137	18.160.46.81	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
6	0.017920	18.160.46.81	10.104.73.137	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
130	2.525936	10.104.73.137	18.160.46.81	HTTP	186	GET /youre-my-only-hope HTTP/1.1
132	2.536584	18.160.46.81	10.104.73.137	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
244	4.869780	10.104.73.137	18.160.46.81	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
246	4.878956	18.160.46.81	10.104.73.137	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
356	7.296183	10.104.73.137	18.160.46.81	HTTP	186	GET /youre-my-only-hope HTTP/1.1
358	7.304238	18.160.46.81	10.104.73.137	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
498	9.811929	10.104.73.137	18.160.46.81	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
500	9.822327	18.160.46.81	10.104.73.137	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
617	12.295157	10.104.73.137	18.160.46.81	HTTP	186	GET /youre-my-only-hope HTTP/1.1
619	12.303879	18.160.46.81	10.104.73.137	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
733	14.695499	10.104.73.137	18.160.46.81	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
735	14.703656	18.160.46.81	10.104.73.137	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
846	17.059102	10.104.73.137	18.160.46.81	HTTP	186	GET /youre-my-only-hope HTTP/1.1
848	17.069445	18.160.46.81	10.104.73.137	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
967	19.544885	10.104.73.137	18.160.46.81	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
969	19.554258	18.160.46.81	10.104.73.137	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
1085	21.895251	10.104.73.137	18.160.46.81	HTTP	186	GET /youre-my-only-hope HTTP/1.1
1087	21.905701	18.160.46.81	10.104.73.137	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)

Frame 4: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface \Device\NPF\_{A00538A2-0B83-4000-8000-000000000000} Ethernet II, Src: IntelCor\_77:10:3c (c0:b6:f9:77:10:3c), Dst: All-HSRP-routers\_00 (00:00:0c:07:ac:00) Internet Protocol Version 4, Src: 10.104.73.137, Dst: 18.160.46.81 Transmission Control Protocol, Src Port: 64868, Dst Port: 80, Seq: 1, Ack: 1, Len: 135 Hypertext Transfer Protocol

0000 00 00 0c 07 ac 00 c0 b6 f9 77 10 3c 08 00 45 00 ...  
0010 00 af 8b a0 40 00 80 06 00 00 0a 68 49 89 12 a0 ...  
0020 2e 51 fd 64 00 50 df 76 11 49 7a 93 06 9f 50 18 .Q.  
0030 02 05 95 83 00 00 47 45 54 20 2f 68 65 6c 70 2d ...  
0040 6d 65 2d 6f 62 69 77 61 6e 2d 6b 65 6e 6f 62 69 me-  
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 H1  
0060 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 69 64 65 6e t-t  
0070 74 69 74 79 0d 0a 48 6f 73 74 3a 20 77 77 77 2e tit  
0080 75 6d 64 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 umc  
0090 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 55 73 65 72 lor  
00a0 2d 41 67 65 6e 74 3a 20 50 79 74 68 6f 6e 2d 75 -Ag  
00b0 72 6c 6c 69 62 2f 32 2e 37 0d 0a 0d 0a rll

Meanwhile, "Obiwan2.exe" initiated connections to the following 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>

The peculiar nature of "Obiwan2.exe," particularly its attempt to communicate with a website featuring an encoded string in the URL, raised suspicions. Notably, the second URL contained the term "base64," hinting at the possibility of base64 encoding. Furthermore, the first URL's reference to "not even my final form" suggested that the third URL might provide additional clues.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
126	14.936254	10.104.73.137	18.160.46.99	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
128	14.945312	18.160.46.99	10.104.73.137	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
244	17.406531	10.104.73.137	18.160.46.99	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
246	17.414661	18.160.46.99	10.104.73.137	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
359	19.860707	10.104.73.137	18.160.46.99	HTTP	188	GET /cJkMiBpcyB0aGUga2V5 HTTP/1.1
361	19.869564	18.160.46.99	10.104.73.137	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
477	22.710367	10.104.73.137	18.160.46.99	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
479	22.717681	18.160.46.99	10.104.73.137	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
598	25.144150	10.104.73.137	18.160.46.99	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
600	25.152340	18.160.46.99	10.104.73.137	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
715	27.564650	10.104.73.137	18.160.46.99	HTTP	188	GET /cJkMiBpcyB0aGUga2V5 HTTP/1.1
717	27.572862	18.160.46.99	10.104.73.137	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
832	30.436830	10.104.73.137	18.160.46.99	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
834	30.444645	18.160.46.99	10.104.73.137	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
945	32.815755	10.104.73.137	18.160.46.99	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
947	32.839899	18.160.46.99	10.104.73.137	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
1060	35.291898	10.104.73.137	18.160.46.99	HTTP	188	GET /cJkMiBpcyB0aGUga2V5 HTTP/1.1
1062	35.300390	18.160.46.99	10.104.73.137	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)
1173	38.159813	10.104.73.137	18.160.46.99	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
1175	38.171115	18.160.46.99	10.104.73.137	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
1296	40.509738	10.104.73.137	18.160.46.99	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1
1298	40.519592	18.160.46.99	10.104.73.137	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)
1428	43.003591	10.104.73.137	18.160.46.99	HTTP	188	GET /cJkMiBpcyB0aGUga2V5 HTTP/1.1
1430	43.014598	18.160.46.99	10.104.73.137	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)

Frame 126: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface \Device\NPF\_{A00538A2-0B...}

Ethernet II, Src: IntelCor\_77:10:3c (c0:b6:f9:77:10:3c), Dst: All-HSRP-routers\_00 (00:00:0c:07:ac:00)

Internet Protocol Version 4, Src: 10.104.73.137, Dst: 18.160.46.99

Transmission Control Protocol, Src Port: 65141, Dst Port: 80, Seq: 1, Ack: 1, Len: 145

Hypertext Transfer Protocol

0000 00 00 0c 07 ac 00 c0 b6 f9 77 10 3c 08 00 45 00 .....w-<-E-  
0010 00 b9 cb d2 40 00 80 06 00 00 0a 68 49 89 12 a0 ....@-...-hI...  
0020 2e 63 fe 75 00 50 41 14 6e ce f0 06 7b 34 50 18 .c.u.PA- n-...4P-  
0030 02 05 95 9f 00 00 47 45 54 20 2f 74 68 69 73 2d ....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 6d 0a ding: id entity..  
0080 48 6f 73 74 3a 20 77 77 77 2e 75 6d 64 2e 65 64 Host: ww w.umd.ed  
0090 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 u-Conn ection: c  
00a0 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 lose-U s er-Agent  
00b0 3a 20 50 79 74 68 6f 6e 2d 75 72 6c 6e 69 62 2f : Pvthon -urllib/

Upon decoding the base64-encoded string, the message "r2d2 is the key" was revealed, confirming the encoding method.

## Decode from Base64 format

Simply enter your data then push the decode button.

cJkMiBpcyB0aGUga2V5

Jayraj Vakil  
119188361

For encoded binaries (like images, documents, etc.) use the file upload form a

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports onl

DECODE Decodes your data into the area below.

r2d2 is the key



Within the Autopsy interface, an intriguing section labeled 'Interesting Items' under 'Analysis Results' piqued curiosity. Further exploration yielded a subentry titled 'Encryption Programs,' wherein the program 'VeraCrypt' was identified.

Jayraj Vakil\_Final - Autopsy 4.21.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Encryption Programs

Table Thumbnail Summary

Source Name	S	C	O	Source Type	Score	C
VeraCrypt.exe				File	Likely Notable	

Hex Text Application File Metadata OS Account Data Artifacts Analysis

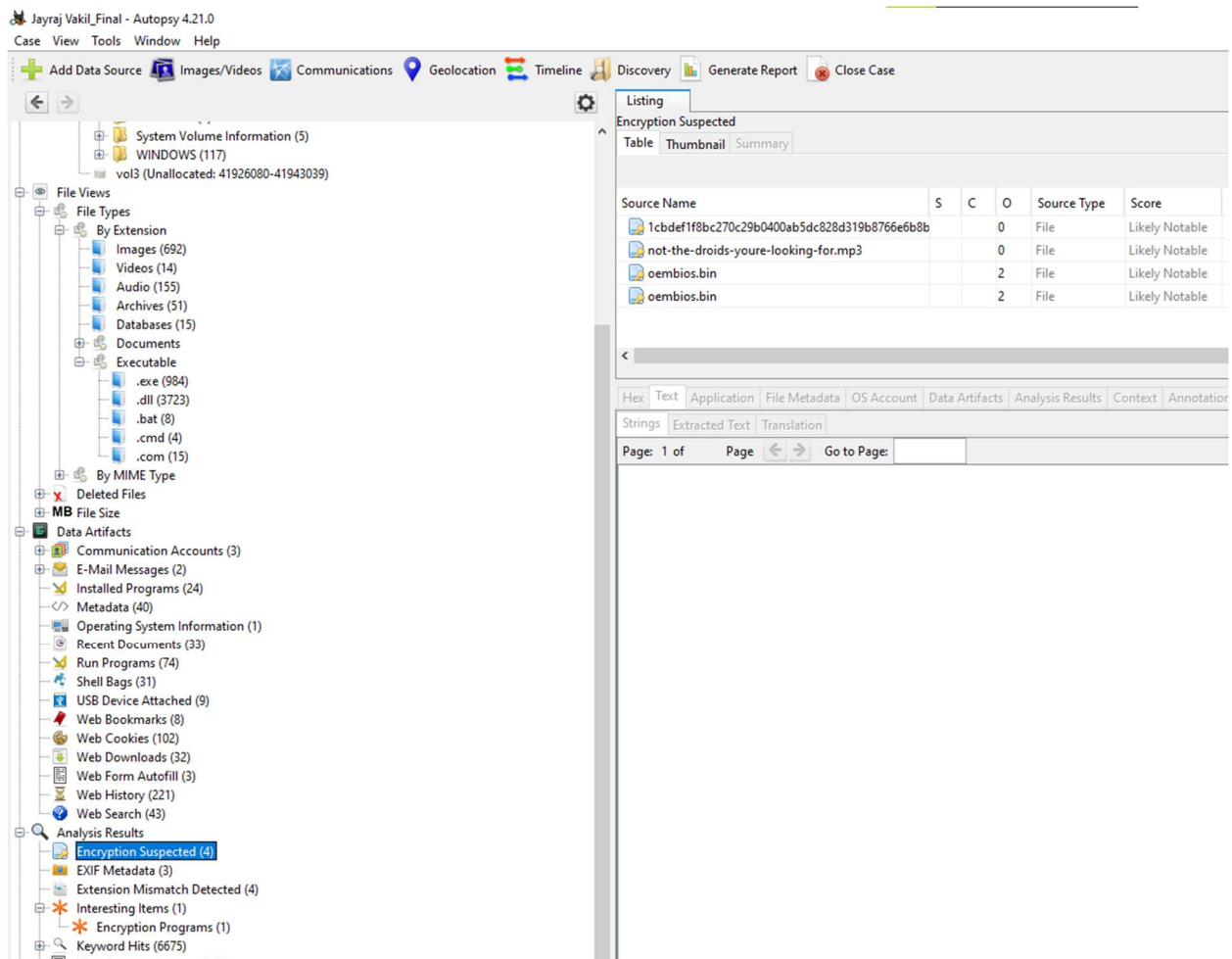
Strings Extracted Text Translation

Page: 1 of Page Go to Page:

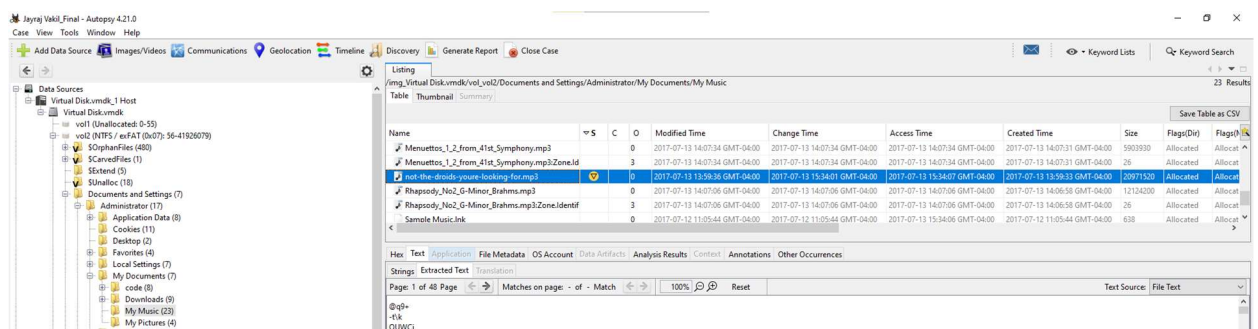
File Views

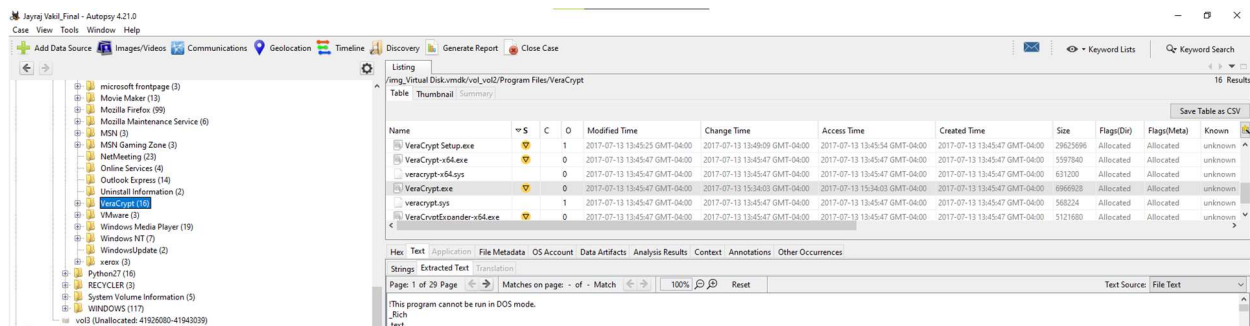
- System Volume Information (5)
- WINDOWS (117)
- vol3 (Unallocated: 41926080-41943039)
- File Types
  - By Extension
    - Images (692)
    - Videos (14)
    - Audio (155)
    - Archives (51)
    - Databases (15)
  - Documents
  - Executable
    - .exe (984)
    - .dll (3723)
    - .bat (8)
    - .cmd (4)
    - .com (15)
  - By MIME Type
- Deleted Files
- MB File Size
- Data Artifacts
  - Communication Accounts (3)
  - E-Mail Messages (2)
  - Installed Programs (24)
  - Metadata (40)
  - Operating System Information (1)
  - Recent Documents (33)
  - Run Programs (74)
  - Shell Bags (31)
  - USB Device Attached (9)
  - Web Bookmarks (8)
  - Web Cookies (102)
  - Web Downloads (32)
  - Web Form Autofill (3)
  - Web History (221)
  - Web Search (43)
- Analysis Results
  - Encryption Suspected (4)
  - EXIF Metadata (3)
  - Extension Mismatch Detected (4)
  - Interesting Items (1)
  - Encryption Programs (1)
  - Keyword Hits (6675)
  - User Content Suspected (3)
  - Web Categories (3)
- OS Accounts
- Tags
- Score
- Reports

Furthermore, the 'Analysis Results' section contained an entry labeled 'Encryption Suspected' with four associated results. One of these results pertained to an MP3 file named 'not-the-droids-youre-looking-for.mp3'.

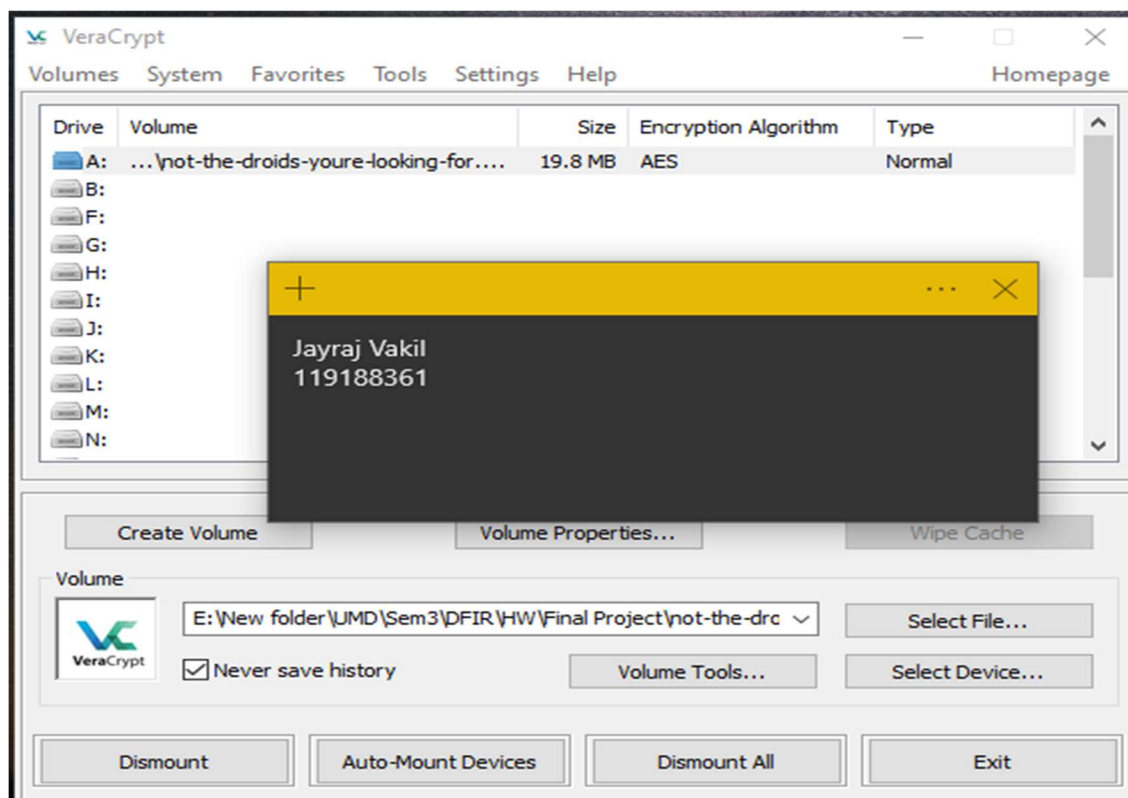


Subsequently, both the MP3 file and the VeraCrypt program were extracted and transferred to the local system for in-depth analysis. The MP3 file's location was identified as '/img\_Virtual Disk.vmdk/vol\_vol2/Documents and Settings/Administrator/My Documents/My Music/not-the-droids-youre-looking-for.mp3', while the VeraCrypt program resided at '/img\_Virtual Disk.vmdk/vol\_vol2/Program Files/VeraCrypt'

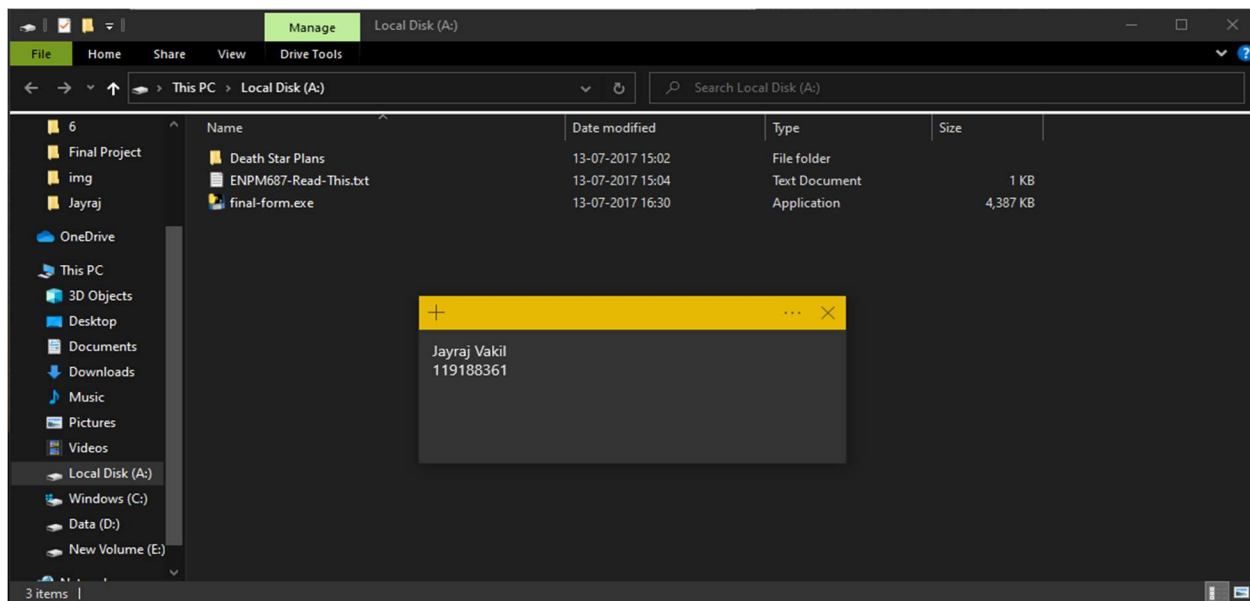




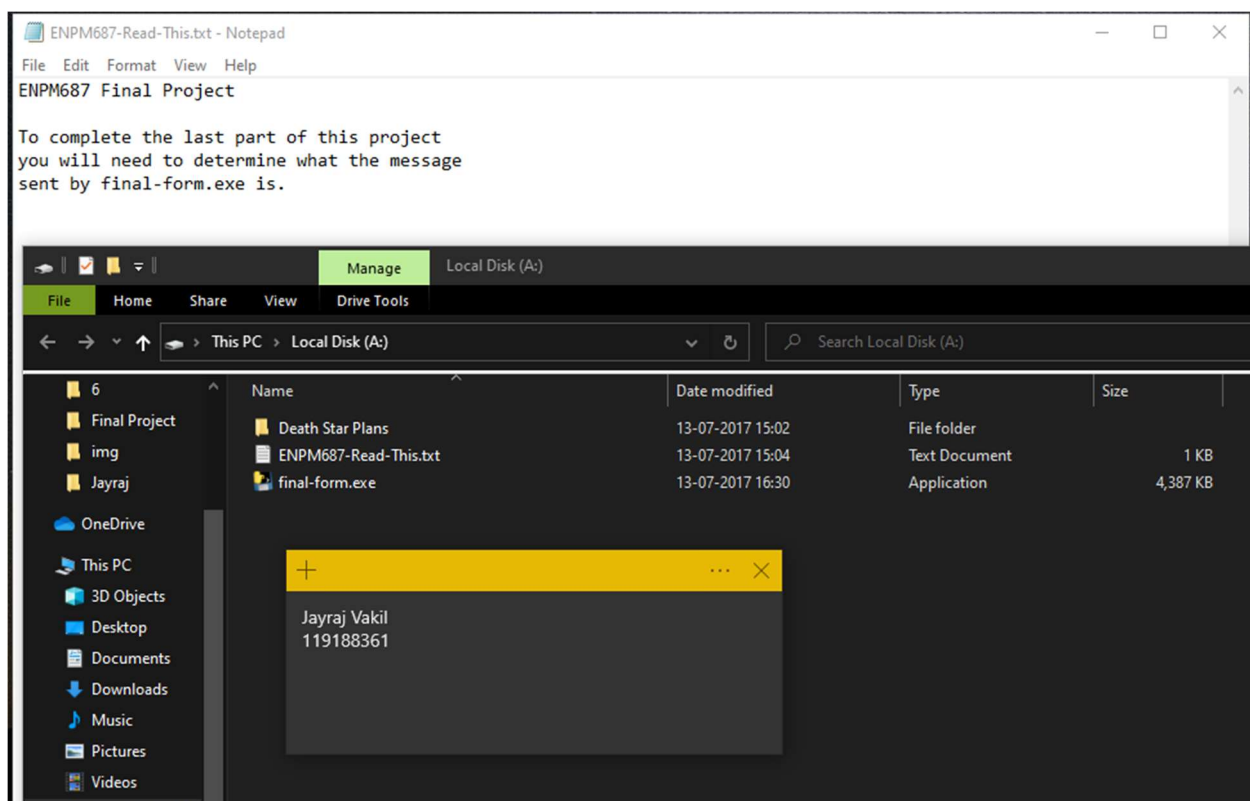
Upon executing the VeraCrypt program and providing the 'r2d2' password obtained from the base64 decoding, the drive was successfully decrypted. Within the decrypted volume, two files (a text file and an executable) and one folder were discovered.







The text file contained a message, the contents of which are provided in the accompanying image.



Upon running the 'Final-form.exe' file, a console window opened with no visible output. Subsequently, a network traffic analysis using Wireshark revealed connections to two webpages: 'We-have-the-blue-prints-to-the-Death-Star' and 'We-will-defeat-Darth-Vader.' This states that the Final-form.exe is the final malware version of the writer.

<http://www.umd.edu/We-will-defeat-Darth-Vader>

<http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star>

The above 2 links are the messages inside the final malware.

The image displays a Wireshark network traffic analysis. The top pane shows a list of HTTP packets. The middle pane shows a packet details view for a selected packet, and the bottom pane shows the packet bytes view.

No.	Time	Source	Destination	Protocol	Length	Info
16	1.089471	10.104.73.137	18.160.46.99	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
19	1.097687	18.160.46.99	10.104.73.137	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
175	3.515818	10.104.73.137	18.160.46.99	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
177	3.525186	18.160.46.99	10.104.73.137	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
350	6.475817	10.104.73.137	18.160.46.53	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
352	6.484922	18.160.46.53	10.104.73.137	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
489	8.898004	10.104.73.137	18.160.46.99	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
492	8.907055	18.160.46.99	10.104.73.137	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
625	11.953261	10.104.73.137	18.160.46.99	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
627	11.965624	18.160.46.99	10.104.73.137	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
793	14.360467	10.104.73.137	18.160.46.81	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
795	14.369930	18.160.46.81	10.104.73.137	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)
928	17.373741	10.104.73.137	18.160.46.53	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
930	17.382528	18.160.46.53	10.104.73.137	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
1046	19.763626	10.104.73.137	18.160.46.53	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
1048	19.776848	18.160.46.53	10.104.73.137	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)

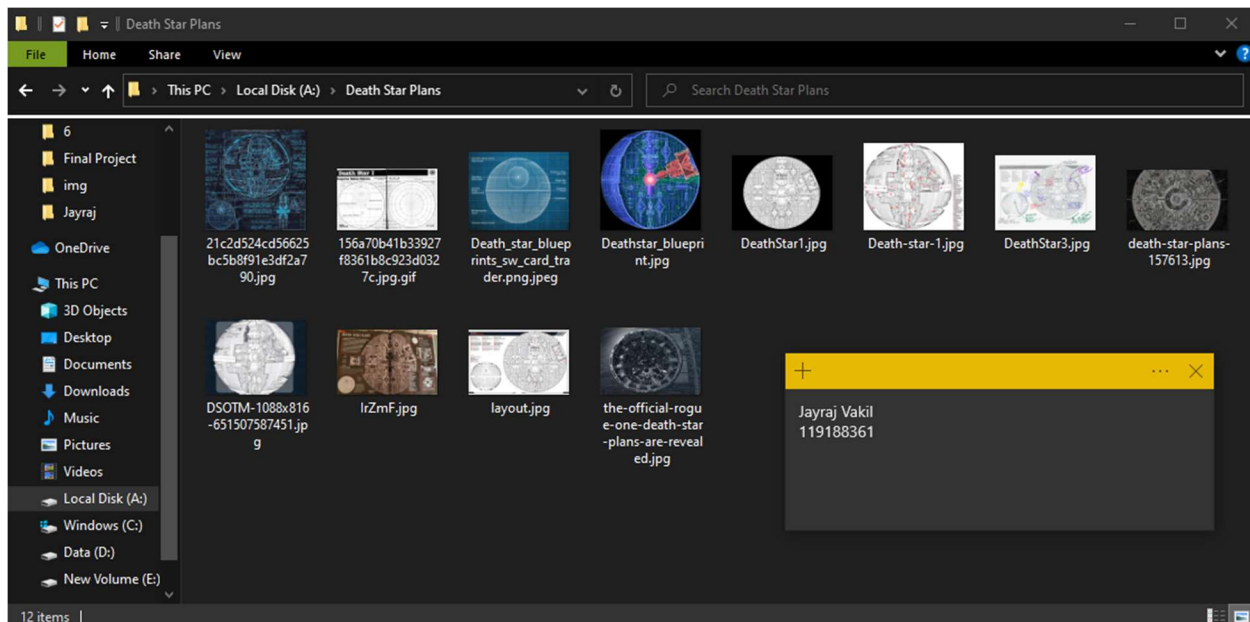
Packet details view for Frame 16:

- Frame 16: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF\_{A00538A2-08B8-4000-8000-000000000000} on interface IntelCor\_77:10:3c (c0:b6:f9:77:10:3c), Dst: All-MSRP-routers\_00 (00:00:0c:07:ac:00)
- Ethernet II, Src: IntelCor\_77:10:3c (c0:b6:f9:77:10:3c), Dst: All-MSRP-routers\_00 (00:00:0c:07:ac:00)
- Internet Protocol Version 4, Src: 10.104.73.137, Dst: 18.160.46.99
- Transmission Control Protocol, Src Port: 52512, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
- Hypertext Transfer Protocol

Packet bytes view for Frame 16:

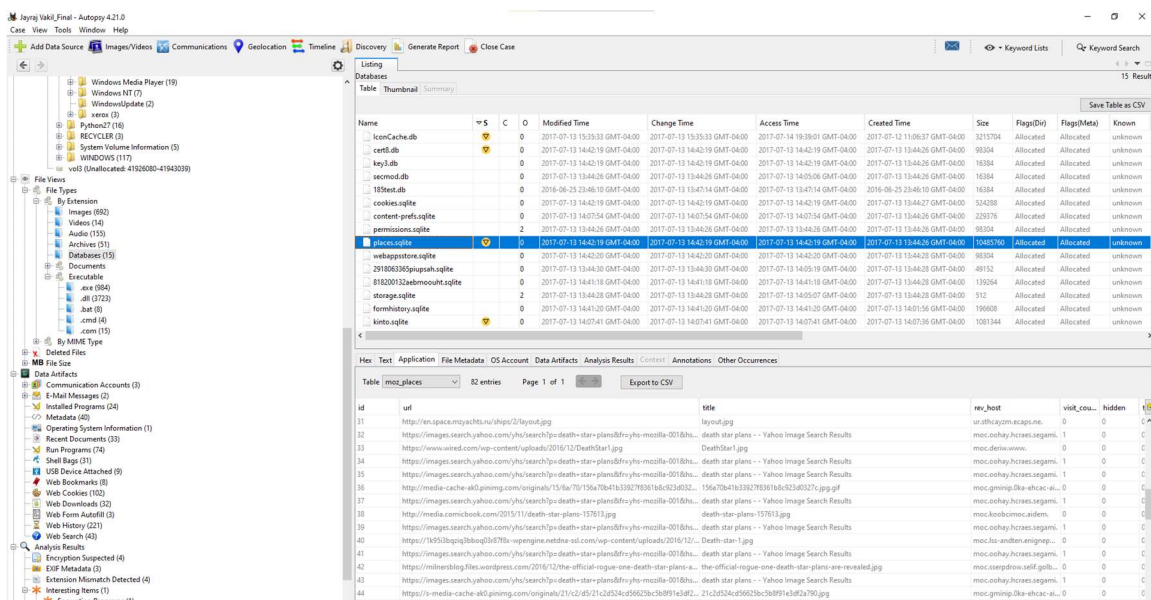
```
0000 00 00 0c 07 ac 00 c0 b6 f9 77 10 3c 08 00 45 00 .....-w-c-E-
0010 00 c3 e0 37 40 00 80 06 00 00 0a 68 49 89 12 a0 ...7@...-hI...
0020 2e 63 cd 20 00 50 cd 20 6f 7e d0 14 d1 11 50 18 ..c..P: o-----P-
0030 02 05 95 a9 00 00 47 45 54 20 2f 57 65 2d 68 61 .....GE T /We-ha
0040 76 65 2d 74 68 65 2d 62 6c 75 65 2d 70 72 69 6e ve-the-b lue-prin
0050 74 73 2d 74 6f 2d 74 68 65 2d 44 65 61 74 68 2d ts-to-th e-Death-
0060 53 74 61 72 20 48 54 54 50 2f 31 2e 31 0d 0a 41 Star HTT P/1.1-A
0070 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 ccept-En coding:
0080 69 64 65 6e 74 69 74 79 0d 0a 48 6f 73 74 3a 20 identity ..Host:
0090 77 77 77 2e 75 6d 64 2e 65 64 75 0d 0a 43 6f 6e www.umd. edu..Con
00a0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a nection: close..
00b0 55 73 65 72 2d 41 67 65 6e 74 3a 20 50 79 74 68 User-Age nt: Pyth
00c0 6f 6e 2d 75 72 6c 6c 69 62 2f 32 2e 37 0d 0a 0d on-urlll b/2.7...
00d0 0a
```

Exploring the folder named 'Death Star Plans,' revealed a collection of images and plans pertaining to the Death Star.



### C. Some interesting finds:

The file “places.sqlite” seems to be of interest because it is referenced in many of the Death Star files and VeraCrypt.



The file “obiwan.py” seems to be what the obiwan.exe does. It calls the 2 websites that obiwan.exe does and sleeps for 2 seconds. This runs for infinite times.

The screenshot shows the Autopsy 4.21.0 interface. The left pane displays the file system tree, and the right pane shows the listing of files in the directory `/img/Virtual Disk/vmdk/vol_v02/Documents and Settings/Administrator/My Documents/code`. The file `obiwan.py` is highlighted in blue.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2017-07-14 19:39:42 GMT-0400	2017-07-14 19:39:42 GMT-0400	2017-07-14 19:39:42 GMT-0400	2017-07-13 14:10:02 GMT-0400	56	Allocated	Allocated	unknown	/img_Virtual
[parent folder]				2017-07-14 19:39:58 GMT-0400	2017-07-14 19:39:58 GMT-0400	2017-07-14 19:39:58 GMT-0400	2017-07-12 11:05:39 GMT-0400	56	Allocated	Allocated	unknown	/img_Virtual
build				2017-07-13 15:10:53 GMT-0400	2017-07-13 15:10:53 GMT-0400	2017-07-13 15:11:02 GMT-0400	2017-07-13 14:44:15 GMT-0400	448	Allocated	Allocated	unknown	/img_Virtual
dist				2017-07-13 15:35:06 GMT-0400	2017-07-13 15:35:06 GMT-0400	2017-07-13 15:35:06 GMT-0400	2017-07-13 14:44:15 GMT-0400	256	Allocated	Allocated	unknown	/img_Virtual
final-form.spc				2017-07-13 15:39:49 GMT-0400	2017-07-13 15:39:49 GMT-0400	2017-07-14 19:39:58 GMT-0400	2017-07-13 15:39:49 GMT-0400	764	Allocated	Allocated	unknown	/img_Virtual
obiwan.py				2017-07-13 14:36:38 GMT-0400	2017-07-13 14:36:38 GMT-0400	2017-07-13 14:36:38 GMT-0400	2017-07-13 14:36:38 GMT-0400	159	Allocated	Allocated	unknown	/img_Virtual
obiwan.spc				2017-07-13 14:44:22 GMT-0400	2017-07-13 14:44:22 GMT-0400	2017-07-13 14:44:22 GMT-0400	2017-07-13 14:44:15 GMT-0400	756	Allocated	Allocated	unknown	/img_Virtual
obiwan2.spc				2017-07-13 15:30:39 GMT-0400	2017-07-13 15:30:39 GMT-0400	2017-07-13 15:30:39 GMT-0400	2017-07-13 15:30:39 GMT-0400	756	Allocated	Allocated	unknown	/img_Virtual

In the “Recents Documents” it is seen that many .lnk files are accessed which are related to Death Star.

The screenshot shows the Autopsy 4.21.0 interface. The left pane displays the file system tree, and the right pane shows the listing of files in the `Recent Documents` directory. The list includes various .lnk files, including `Death Star Plans` and `Death Star Plans-157613.lnk`.

Source Name	S	C	O	Path	Date Accessed	Data Source
Death_star_blueprints_sw_card_trader.png.lnk				M:\Death Star Plans\Death_star_blueprints_sw_card_tr... 2017-07-13 14:02:59 GMT-0400	2017-07-13 14:02:59 GMT-0400	Virtual Disk.vmdk
Menuettos_1_2_from_41st_Symphony.lnk				C:\Documents and Settings\Administrator\My Docum... 2017-07-13 14:01:31 GMT-0400	2017-07-13 14:01:31 GMT-0400	Virtual Disk.vmdk
156c7b41b33877881b6c2d3d37c7c.jpg.lnk				M:\Death Star Plans\156c7b41b33877881b6c2d3d37c7c.jpg... 2017-07-13 14:02:35 GMT-0400	2017-07-13 14:02:35 GMT-0400	Virtual Disk.vmdk
21c2d524cd95623bc3a891e3d72a790.lnk				M:\Death Star Plans\21c2d524cd95623bc3a891e3d72a790... 2017-07-13 14:02:54 GMT-0400	2017-07-13 14:02:54 GMT-0400	Virtual Disk.vmdk
Blah.lnk				C:\Documents and Settings\Administrator\My Docum... 2017-07-14 19:39:27 GMT-0400	2017-07-14 19:39:27 GMT-0400	Virtual Disk.vmdk
Bourree_4th_Suite-Bach.lnk				C:\Documents and Settings\Administrator\My Docum... 2017-07-14 14:07:12 GMT-0400	2017-07-14 14:07:12 GMT-0400	Virtual Disk.vmdk
code.lnk				C:\Documents and Settings\Administrator\My Docum... 2017-07-13 14:36:28 GMT-0400	2017-07-13 14:36:28 GMT-0400	Virtual Disk.vmdk
Concerto-4-Violini-2_Teleman.lnk				C:\Documents and Settings\Administrator\My Docum... 2017-07-13 14:06:51 GMT-0400	2017-07-13 14:06:51 GMT-0400	Virtual Disk.vmdk
Courante_1st_Cello_Suite.lnk				C:\Documents and Settings\Administrator\My Docum... 2017-07-13 14:07:48 GMT-0400	2017-07-13 14:07:48 GMT-0400	Virtual Disk.vmdk
Death Star Plans.lnk				M:\Death Star Plans 2017-07-13 14:02:25 GMT-0400	2017-07-13 14:02:25 GMT-0400	Virtual Disk.vmdk
Death-star-1.lnk				M:\Death Star Plans\Death-star-1.jpg 2017-07-13 14:02:47 GMT-0400	2017-07-13 14:02:47 GMT-0400	Virtual Disk.vmdk
death-star-plans-157613.lnk				M:\Death Star Plans\death-star-plans-157613.jpg 2017-07-13 14:02:42 GMT-0400	2017-07-13 14:02:42 GMT-0400	Virtual Disk.vmdk
DeathStar.lnk				M:\Death Star Plans\DeathStar.l.jpg 2017-07-13 14:02:32 GMT-0400	2017-07-13 14:02:32 GMT-0400	Virtual Disk.vmdk
DeathStar3.lnk				M:\Death Star Plans\DeathStar3.jpg 2017-07-13 14:03:09 GMT-0400	2017-07-13 14:03:09 GMT-0400	Virtual Disk.vmdk
Deathstar_blueprint.lnk				M:\Death Star Plans\Deathstar_blueprint.jpg 2017-07-13 14:03:03 GMT-0400	2017-07-13 14:03:03 GMT-0400	Virtual Disk.vmdk

## Conclusion and Recommendation

### **Conclusion:**

The comprehensive digital forensic analysis of a Windows XP virtual machine using Autopsy software uncovered a complex web of malicious activities. Two executables, "obiwan.exe" and "obiwan2.exe," were found to initiate outbound connections to unique URLs, some containing encoded messages. Decoding these led to the discovery of an encrypted volume using VeraCrypt, which was accessed using a base64-decoded password. Inside, a text file, another executable, and a folder with sensitive contents were found. The second executable, "Final-form.exe," showed further suspicious network activity, pointing to a significant security breach involving critical data related to the Death Star.

### **Recommendations:**

1. Enhanced Monitoring and Network Analysis: Implement continuous monitoring of network traffic to identify and intercept any unauthorized communications, especially those resembling the patterns observed in the executables' activities.
2. Robust Encryption and Access Controls: Strengthen encryption protocols and access control mechanisms to safeguard sensitive data, ensuring that only authorized personnel can access critical information.
3. Regular System Updates and Patch Management: Keep all systems and software updated with the latest security patches to mitigate vulnerabilities that could be exploited by malicious software.
4. Comprehensive Incident Response Plan: Develop and maintain an incident response plan tailored to scenarios like this breach, ensuring swift and effective action in the event of future security incidents. This plan should include steps for containment, eradication, and recovery, along with post-incident analysis to prevent recurrence.

## Challenges Faced

**Challenge 1:** I initially assumed that "obiwan.exe" and "obiwan2.exe" contained similar messages to those in previous assignments, leading me to overlook crucial clues. This oversight delayed the discovery that "obiwan2.exe" held a vital piece of the puzzle - the encryption password hidden in its network traffic.

**Challenge 2:** Deciphering the encoded message from "obiwan2.exe" was challenging, as I was unfamiliar with base64 decryption. Additionally, connecting the "not-the-droids-you-are-looking-for.mp3" file to VeraCrypt encryption proved difficult. I spent significant time searching for hidden data in the wrong places before realizing its true significance.