

Final Project - Forensic Investigation

Name: Bhavin Panchal

UID: 120278907

1. Brief Summary of information

This Forensic analysis involves identifying, collecting, analyzing, and interpreting digital evidence to investigate malware, and support legal or investigative processes. Key artifacts include system recent files, file metadata, network analysis for given application, and browser history, analyzed using tools like Autopsy, VeraCrypt, and Wireshark. It supports further investigation of the system to find final messages resides inside.

The analysis of the provided disk image ENPM687FinalXP.vmwarevm uncovered crucial evidence through a detailed forensic investigation. Key findings included the decryption of an mp3 file obtained by analyzing the executables obiwan.exe and obiwan2.exe. This led to discovering an encrypted drive containing the final form executable, which provided the final clues. Images and messages collected during the investigation revealed that the rebels possess the blueprints of the Death Star and are planning a mission to destroy it and defeat Darth Vader. The investigation successfully achieved its objectives by uncovering critical evidence supporting these conclusions.

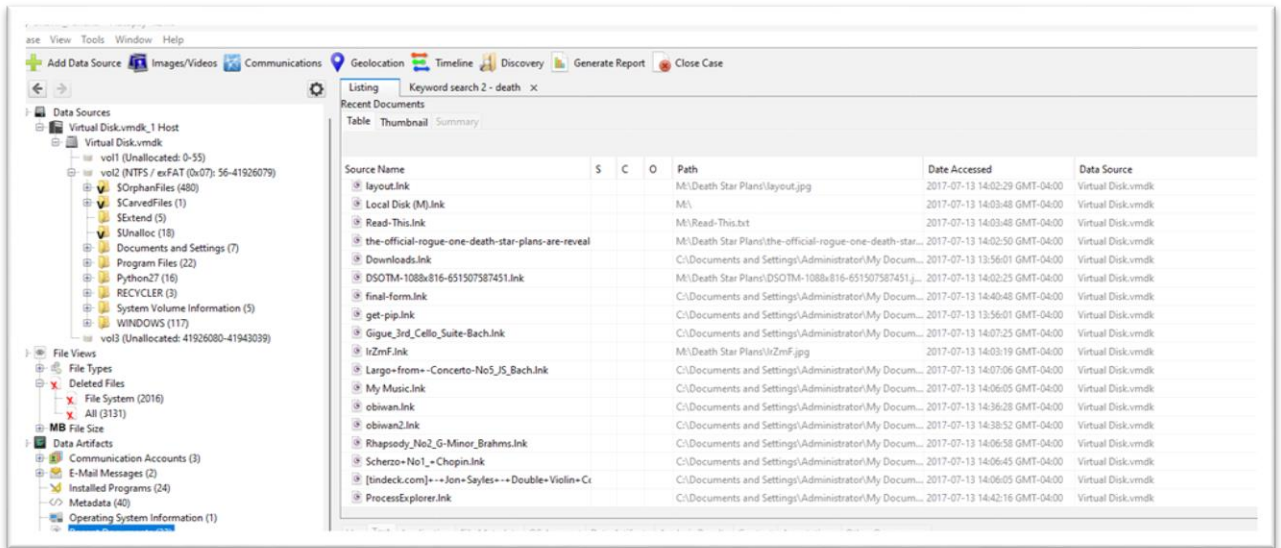
2. Tools used in investigation process

- (i) VeraCrypt: A disk encryption tool used to decrypt sensitive data by creating volumes, ensuring data extraction during forensic investigations for preserving integrity of file.
- (ii) Wireshark: A network protocol analyzer used to capture and analyze network traffic, helping identify suspicious application activity for the investigation.
- (iii) Autopsy: A digital forensics tool that helps in examining file systems, analyzing application files and disk images for evidence in investigations.

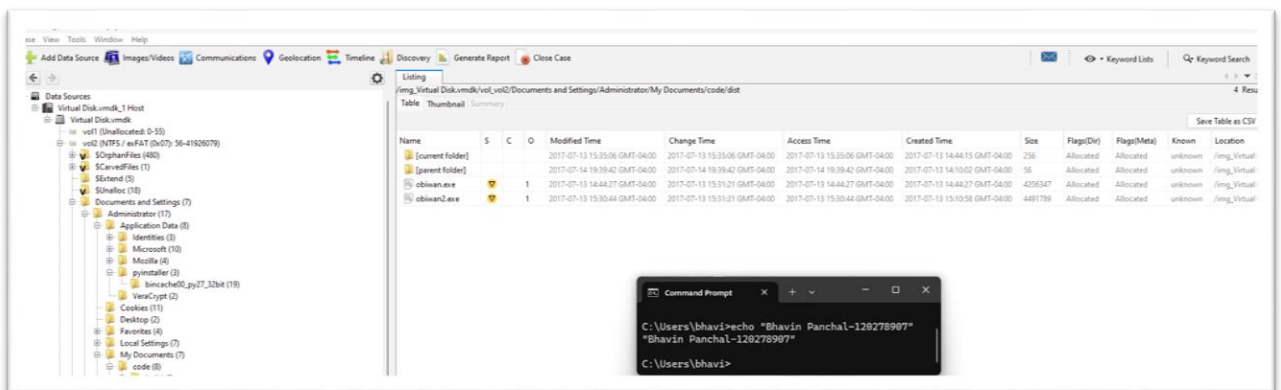
3. Repository #1 – ENPM687FinalXP.Vmwarevm

a. Summary of Evidence:

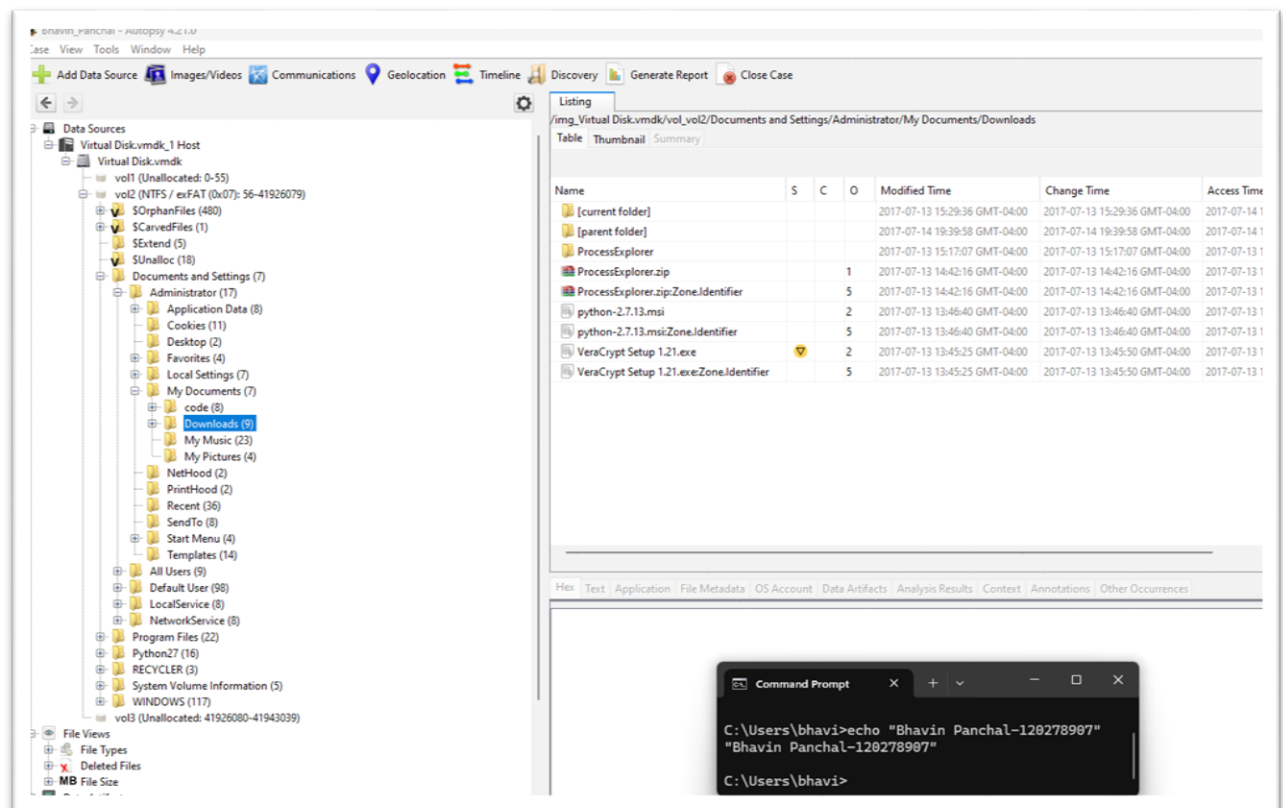
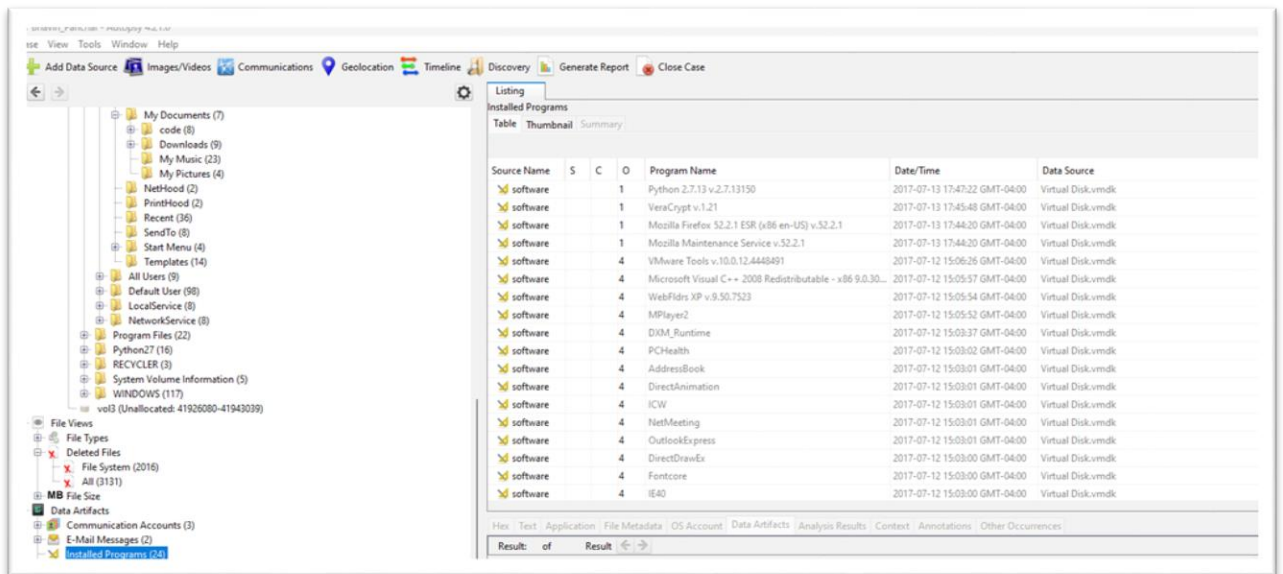
The given disk image needs to be analyzed with autopsy to find overall investigation clues and anomalies present in the disk image. To start investigating checked important folders and directories. Also check the recent documents folder in which I have found **obiwan** named unusual file type. With that keep in mind, explore downloaded and installed programs on the system to find clues.



By exploring these things, I have moved towards the original location of obiwan file which is present in Path C:\Documents and Settings\Administrator\My Documents\code. It looks like an application, must analyze further it.



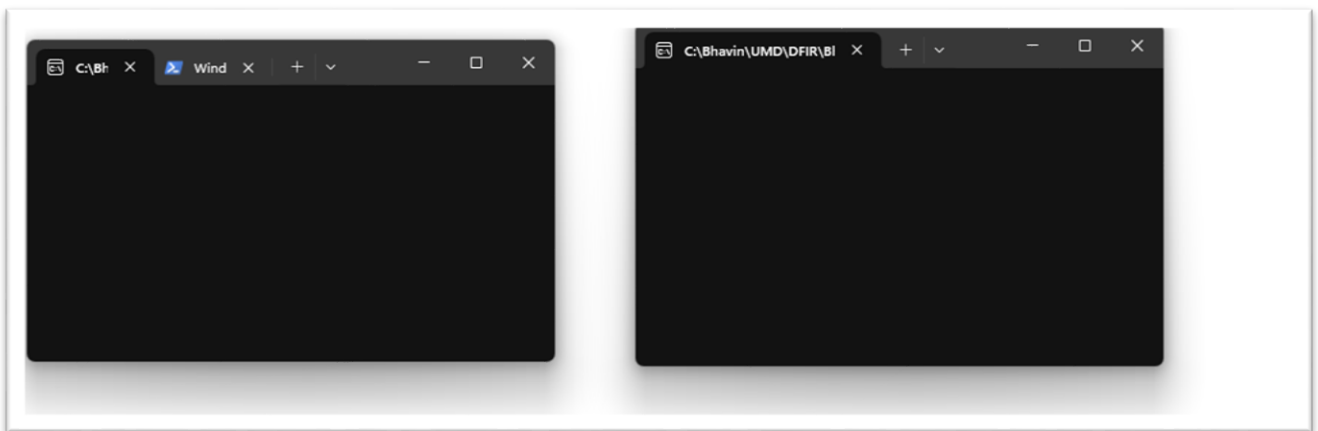
One more thing noticed is that the system has VeraCrypt installed, which means there could be some files encrypted using it



b. Analysis of Applications:

For the above two obiwans named files, I extracted it and ran it in my local machine. There was a command line opened but there was not anything noticeable inside it.

<div> <div> <div>↑</div> <div>↺</div> <div>📁</div> <div>></div> <div>This PC</div> <div>></div> <div>OS (C:)</div> <div>></div> <div>Bhavin</div> <div>></div> <div>UMD</div> <div>></div> <div>DFIR</div> <div>></div> <div>Bhavinkumar Panchal (120278907)</div> </div> <div> <div>✂</div> <div>📄</div> <div>📁</div> <div>🔍</div> <div>🗑</div> <div>↕ Sort</div> <div>☰ View</div> <div>⋮</div> </div> </div>					
	Name	Date modified	Type	Size	
Personal	Cache	04-09-2024 20:33	File folder		
	Export	04-09-2024 20:33	File folder		
	Log	13-09-2024 23:33	File folder		
	ModuleOutput	04-09-2024 20:33	File folder		
	Reports	04-09-2024 20:33	File folder		
nts	3005-obiwan	02-12-2024 11:54	Application	4,108 KB	
ads	3007-obiwan2	02-12-2024 11:54	Application	4,387 KB	
ip	autopsy	04-09-2024 20:33	Data Base File	464 KB	
Roll	Bhavinkumar Panchal (120278907).aut	04-09-2024 20:33	AUT File	1 KB	
	dcs_tpm_owner_02	02-12-2024 13:39	Adobe Acrobat D...	132 KB	
	disk_encryption_v1_2	02-12-2024 13:38	Adobe Acrobat D...	132 KB	
umar Panchal	final-form	13-07-2017 11:30	Application	4,387 KB	
	not-the-droids-youre-looking-for	02-12-2024 12:57	MP3 File	20,480 KB	
Cloud File:	SolrCore	13-09-2024 23:01	Properties Source ...	1 KB	



Now I have analyzed two applications using Wireshark network tool. I have started network listing on my local machine with corresponding interface and again run both programs. There is some suspicious http traffic by using different filtering protocols.

http						
No.	Time	Source	Destination	Protocol	Length	Info
49	2024-12-02 17:00:56.310443	192.168.1.189	3.167.56.56	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
51	2024-12-02 17:00:56.329968	3.167.56.56	192.168.1.189	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
399	2024-12-02 17:00:59.017902	192.168.1.189	3.167.56.116	HTTP	186	GET /youre-my-only-hope HTTP/1.1
401	2024-12-02 17:00:59.038769	3.167.56.116	192.168.1.189	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
627	2024-12-02 17:01:01.557849	192.168.1.189	3.167.56.116	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
629	2024-12-02 17:01:01.578160	3.167.56.116	192.168.1.189	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
869	2024-12-02 17:01:02.325601	192.168.1.189	3.167.56.116	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
871	2024-12-02 17:01:02.345995	3.167.56.116	192.168.1.189	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
1020	2024-12-02 17:01:04.081154	192.168.1.189	3.167.56.116	HTTP	186	GET /youre-my-only-hope HTTP/1.1
1022	2024-12-02 17:01:04.102183	3.167.56.116	192.168.1.189	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)

```

NMAP
[Request in frame: 49]
[Time since request: 0.019525000 seconds]
[Request URI: /help-me-obiwan-kenobi]
[Full request URI: http://www.umd.edu/help-me-obiwan-kenobi]
File Data: 167 bytes

```


There are some moved permanently website URL under the protocol hierarchy. I have tried to open that redirected URL but taken me to UMD official website. Also notice in info section there are get endpoints with some cryptic messages.



However, all the redirected URL link pointed to UMD official site.

No.	Time	Source	Destination	Protocol	Length	Info
49	2024-12-02 17:00:56.310443	192.168.1.189	3.167.56.56	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
51	2024-12-02 17:00:56.329968	3.167.56.56	192.168.1.189	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
399	2024-12-02 17:00:59.017902	192.168.1.189	3.167.56.116	HTTP	186	GET /youre-my-only-hope HTTP/1.1
401	2024-12-02 17:00:59.038769	3.167.56.116	192.168.1.189	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
627	2024-12-02 17:01:01.557849	192.168.1.189	3.167.56.116	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
629	2024-12-02 17:01:01.578160	3.167.56.116	192.168.1.189	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
869	2024-12-02 17:01:02.325601	192.168.1.189	3.167.56.116	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1
871	2024-12-02 17:01:02.345995	3.167.56.116	192.168.1.189	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
1020	2024-12-02 17:01:04.081154	192.168.1.189	3.167.56.116	HTTP	186	GET /youre-my-only-hope HTTP/1.1
1022	2024-12-02 17:01:04.102183	3.167.56.116	192.168.1.189	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 399: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{278744DD-E69B-4C9D-8BEE-FA0FF3CD4B53}, id 0

> Ethernet II, Src: f6:6d:4c:e7:bc:9c (f6:6d:4c:e7:bc:9c), Dst: Arcadyan_f2:02:be (04:a2:22:f2:02:be)

> Internet Protocol Version 4, Src: 192.168.1.189, Dst: 3.167.56.116

> Transmission Control Protocol, Src Port: 49893, Dst Port: 80, Seq: 1, Ack: 1, Len: 132

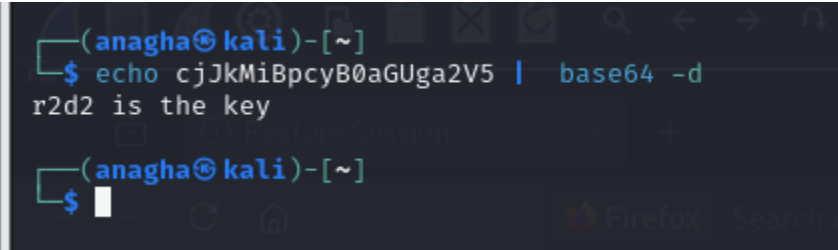
> Hypertext Transfer Protocol

> GET /youre-my-only-hope HTTP/1.1\r\nAccept-Encoding: identity\r\nHost: www.umd.edu\r\nConnection: close\r\nUser-Agent: Python-urllib/2.7\r\n\r\n

Here, I got nothing but tried to capture again with only http traffic for both programs. And I have seen something with some more endpoints. One of them was All-your base64 belong to us. So decided to investigate it and with one base64 code cjJkMiBpcyB0aGUga2V5 was below there.

Current filter: http							
No.	Time	Source	Destination	Protocol	Length	Info	
6	2024-12-02 17:23:17.895850	192.168.1.189	3.167.56.116	HTTP	200	GET /All-your-base64-are-belong-to-us HTTP/1.1	
9	2024-12-02 17:23:17.913859	3.167.56.116	192.168.1.189	HTTP	642	HTTP/1.1 301 Moved Permanently (text/html)	
229	2024-12-02 17:23:19.940132	192.168.1.189	3.167.56.116	HTTP	186	GET /youre-my-only-hope HTTP/1.1	
231	2024-12-02 17:23:19.958866	3.167.56.116	192.168.1.189	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)	
281	2024-12-02 17:23:20.406318	192.168.1.189	3.167.56.116	HTTP	188	GET /cjJkMiBpcyB0aGUga2V5 HTTP/1.1	
286	2024-12-02 17:23:20.425196	3.167.56.116	192.168.1.189	HTTP	630	HTTP/1.1 301 Moved Permanently (text/html)	
501	2024-12-02 17:23:22.511479	192.168.1.189	3.167.56.116	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1	
503	2024-12-02 17:23:22.531421	3.167.56.116	192.168.1.189	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)	
2513	2024-12-02 17:23:23.895183	192.168.1.189	3.167.56.116	HTTP	199	GET /this-is-not-even-my-final-form. HTTP/1.1	

By decoding that code got a message r2d2 is the key. By this message, it enlighten me towards VeraCrypt password because it is installed and used for encrypt files.



Again, I investigated an autopsy for VeraCrypt for further clues. While that process, I have come around VeraCrypt details with some of file’s location which are encrypted on the system. There were some documents and windows configs files encrypted though there was one prominent file was in MY Music folder with name not-the-droids-youre-looking-for.mp3.

VERACRYPT FORMAT.EXE-2f283235.pf	VERACRYPT FORMAT.EXE	/PROGRAM FILES/VERACRYPT	2017-07-13 13:58:18 GMT-04:00	1	Prefetch File	Virtual Disk.vmx
VERACRYPT SETUP 1.21.EXE-157BCBf4.pf	VERACRYPT SETUP 1.21.EXE	/DOCUMENTS AND SETTINGS/ADMINISTRATOR/MY D...	2017-07-13 13:45:39 GMT-04:00	1	Prefetch File	Virtual Disk.vmx
VERACRYPT.EXE-03f62152.pf	VERACRYPT.EXE	/PROGRAM FILES/VERACRYPT	2017-07-13 15:34:03 GMT-04:00	4	Prefetch File	Virtual Disk.vmx
VERCLSID.EXE-3667BD09.pf	VERCLSID.EXE	/WINDOWS/SYSTEM32	2017-07-13 15:29:23 GMT-04:00	19	Prefetch File	Virtual Disk.vmx
VGAUTHSERVICE.EXE-28845F58.pf	VGAUTHSERVICE.EXE	/PROGRAM FILES/VMWARE/VMWARE TOOLS/VMWA...	2017-07-12 11:06:16 GMT-04:00	1	Prefetch File	Virtual Disk.vmx
VMACTHLP.EXE-0790714A.pf	VMACTHLP.EXE	/PROGRAM FILES/VMWARE/VMWARE TOOLS	2017-07-12 11:06:16 GMT-04:00	1	Prefetch File	Virtual Disk.vmx
VMTOOLS.DX-2376BC03.pf	VMTOOLS.DX	/PROGRAM FILES/VMWARE/VMWARE TOOLS	2017-07-12 13:38:43 GMT-04:00	3	Prefetch File	Virtual Disk.vmx

VERACRYPT.EXE-03f62152.pf	VERACRYPT.EXE	/PROGRAM FILES/VERACRYPT	2017-07-13 15:34:03 GMT-04:00	4	Prefetch File	Virtual Disk.vmdk
VERCLSID.EXE-3667BD09.pf	VERCLSID.EXE	/WINDOWS/SYSTEM32	2017-07-13 15:29:23 GMT-04:00	19	Prefetch File	Virtual Disk.vmdk
VGAUTHSERVICE.EXE-28845F58.pf	VGAUTHSERVICE.EXE	/PROGRAM FILES/VMWARE/VMWARE TOOLS/VMWA...	2017-07-12 11:06:16 GMT-04:00	1	Prefetch File	Virtual Disk.vmdk
VMACTHLP.EXE-0790714A.pf	VMACTHLP.EXE	/PROGRAM FILES/VMWARE/VMWARE TOOLS	2017-07-12 11:06:16 GMT-04:00	1	Prefetch File	Virtual Disk.vmdk
VMTOOLS.DX-2376BC03.pf	VMTOOLS.DX	/PROGRAM FILES/VMWARE/VMWARE TOOLS	2017-07-12 13:38:43 GMT-04:00	3	Prefetch File	Virtual Disk.vmdk
WINLOGON.EXE-32C57D49.pf	WINLOGON.EXE	/WINDOWS/SYSTEM32	2017-07-12 11:05:38 GMT-04:00	1	Prefetch File	Virtual Disk.vmdk

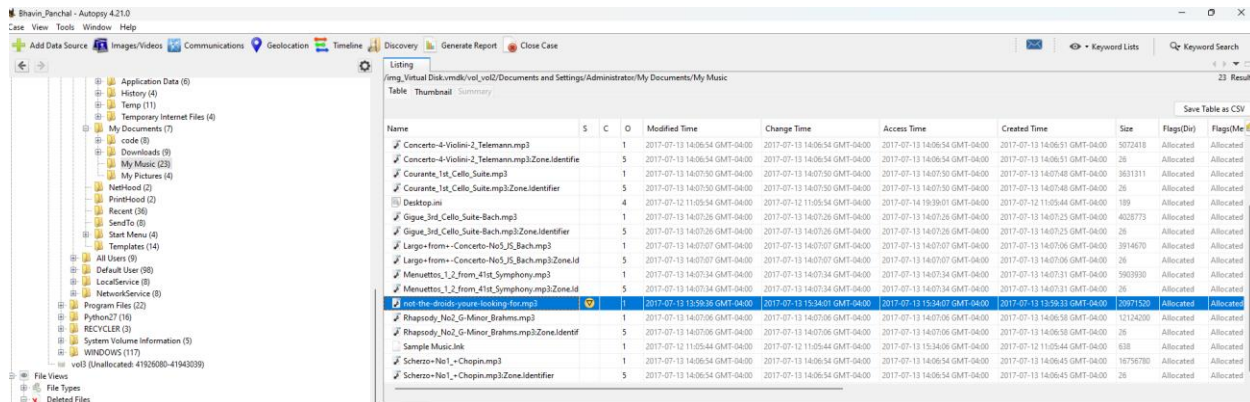
HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsExtracted TextTranslation

Page: 1 of 1 PageMatches on page: - of - Match100%ResetText SourceFile Text

\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WINMM.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\AVIFIL32.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MSACM32.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WMVCORE.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DRMCLIE.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MSDMO.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\URLMON.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WMASF.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WMIDX.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\W32K32.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WS2_32.DLL
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WS2HELP.DLL
\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ADMINISTRATOR\MY DOCUMENTS\MY MUSIC\not-the-droids-youre-looking-for.mp3
\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MI...D.DLL

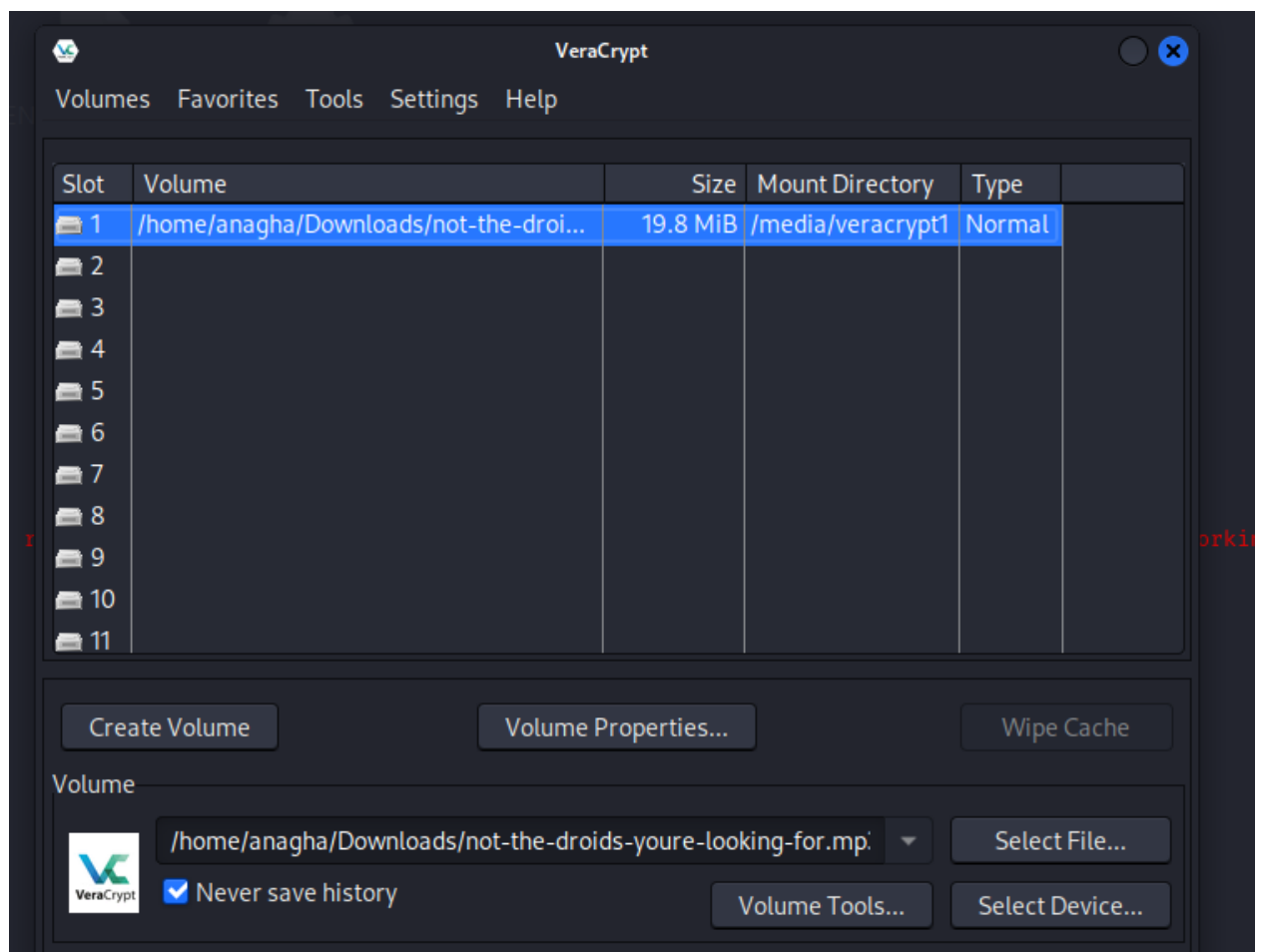
Then I moved towards the original file location and extracted files from the autopsy to my local machine. It was not opening for some reason. I suspected it and put it into my kali machine.



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a file tree with categories like Application Data, History, Temp, and My Documents. The main window shows a file listing table for the path `/img_Virtual Disk.vmdk/vol_v02/Documents and Settings/Administrator/My Documents/My Music`. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Me). The file `not-the-droids-youre-looking-for.mp3` is highlighted in blue.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me)
✓ Concerto-4-Violini-2-Telemann.mp3	1			2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:51 GMT-04:00	5072418	Allocated	Allocated
✓ Concerto-4-Violini-2-Telemann.mp3.Zone.Identifier	5			2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:51 GMT-04:00	28	Allocated	Allocated
✓ Courante_1st_Cello_Suite.mp3	1			2017-07-13 14:07:50 GMT-04:00	2017-07-13 14:07:50 GMT-04:00	2017-07-13 14:07:50 GMT-04:00	2017-07-13 14:07:48 GMT-04:00	3631311	Allocated	Allocated
✓ Courante_1st_Cello_Suite.mp3.Zone.Identifier	5			2017-07-13 14:07:50 GMT-04:00	2017-07-13 14:07:50 GMT-04:00	2017-07-13 14:07:50 GMT-04:00	2017-07-13 14:07:48 GMT-04:00	28	Allocated	Allocated
Desktop.m	4			2017-07-12 11:05:54 GMT-04:00	2017-07-12 11:05:54 GMT-04:00	2017-07-12 11:05:54 GMT-04:00	2017-07-12 11:05:44 GMT-04:00	189	Allocated	Allocated
✓ Dighe_1st_Cello_Suite-Back.mp3	1			2017-07-13 14:07:36 GMT-04:00	2017-07-13 14:07:36 GMT-04:00	2017-07-13 14:07:36 GMT-04:00	2017-07-13 14:07:25 GMT-04:00	4028773	Allocated	Allocated
✓ Dighe_1st_Cello_Suite-Back.mp3.Zone.Identifier	5			2017-07-13 14:07:36 GMT-04:00	2017-07-13 14:07:36 GMT-04:00	2017-07-13 14:07:36 GMT-04:00	2017-07-13 14:07:25 GMT-04:00	28	Allocated	Allocated
✓ Largo+from+Concerto-No.5_Bach.mp3	1			2017-07-13 14:07:07 GMT-04:00	2017-07-13 14:07:07 GMT-04:00	2017-07-13 14:07:07 GMT-04:00	2017-07-13 14:07:06 GMT-04:00	3914670	Allocated	Allocated
✓ Largo+from+Concerto-No.5_Bach.mp3.Zone.Identifier	5			2017-07-13 14:07:07 GMT-04:00	2017-07-13 14:07:07 GMT-04:00	2017-07-13 14:07:07 GMT-04:00	2017-07-13 14:07:06 GMT-04:00	28	Allocated	Allocated
✓ Menuettes_1_2_from_41st_Symphony.mp3	1			2017-07-13 14:07:34 GMT-04:00	2017-07-13 14:07:34 GMT-04:00	2017-07-13 14:07:34 GMT-04:00	2017-07-13 14:07:31 GMT-04:00	5903930	Allocated	Allocated
✓ Menuettes_1_2_from_41st_Symphony.mp3.Zone.Identifier	5			2017-07-13 14:07:34 GMT-04:00	2017-07-13 14:07:34 GMT-04:00	2017-07-13 14:07:34 GMT-04:00	2017-07-13 14:07:31 GMT-04:00	28	Allocated	Allocated
not-the-droids-youre-looking-for.mp3	1			2017-07-13 13:56:36 GMT-04:00	2017-07-13 13:54:01 GMT-04:00	2017-07-13 13:54:07 GMT-04:00	2017-07-13 13:56:33 GMT-04:00	20971520	Allocated	Allocated
✓ Rhapsody_No.2_G-Minor_Brahms.mp3	1			2017-07-13 14:07:06 GMT-04:00	2017-07-13 14:07:06 GMT-04:00	2017-07-13 14:07:06 GMT-04:00	2017-07-13 14:06:58 GMT-04:00	12124200	Allocated	Allocated
✓ Rhapsody_No.2_G-Minor_Brahms.mp3.Zone.Identifier	5			2017-07-13 14:07:06 GMT-04:00	2017-07-13 14:07:06 GMT-04:00	2017-07-13 14:07:06 GMT-04:00	2017-07-13 14:06:58 GMT-04:00	28	Allocated	Allocated
Sample Music.mk	1			2017-07-12 11:05:44 GMT-04:00	2017-07-12 11:05:44 GMT-04:00	2017-07-12 11:05:44 GMT-04:00	2017-07-12 11:05:44 GMT-04:00	638	Allocated	Allocated
✓ Scherzo-No.1_+Chopin.mp3	1			2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:45 GMT-04:00	16756780	Allocated	Allocated
✓ Scherzo-No.1_+Chopin.mp3.Zone.Identifier	5			2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:54 GMT-04:00	2017-07-13 14:06:45 GMT-04:00	28	Allocated	Allocated

This file has been encrypted. Let's try to decrypt it using the key that we got with VeraCrypt tool.



After mounting and decrypting the file, I got some files and read the text file which was under the same folder. It is also suggested to investigate the final form.exe file.

```

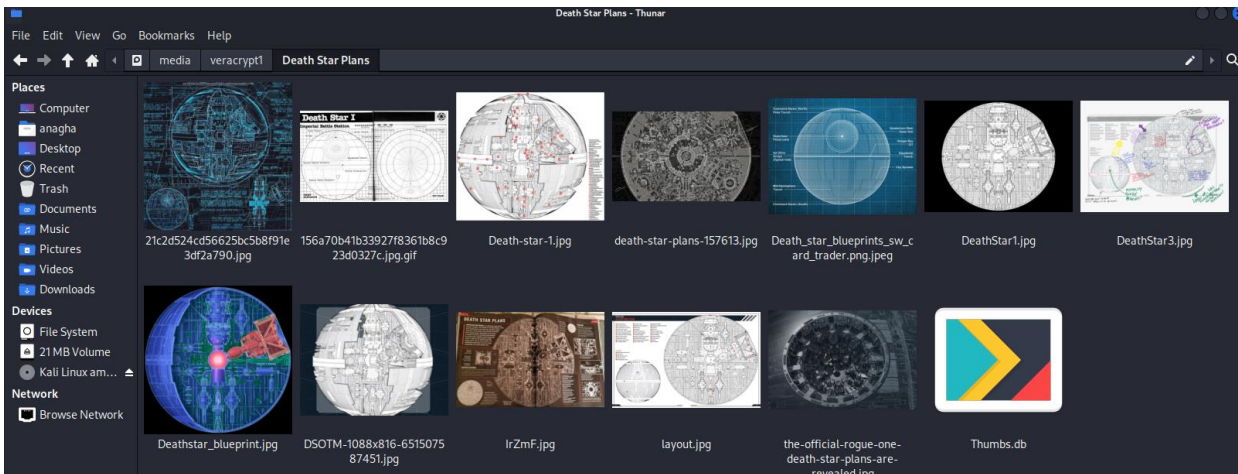
(anagha@kali)-[/media/veracrypt1]
$ ls
'Death Star Plans'  ENPM687-Read-This.txt  'System Volume Information'  final-form.exe

(anagha@kali)-[/media/veracrypt1]
$ cat ENPM687-Read-This.txt
ENPM687 Final Project

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

```

Another folder was death star plans which consists of a images and blue prints of the spheres with different data.



After extracting that mp3 file and putting finalform.exe into my local machine again I ran it and used wire shark for capturing traffic. I used http traffic for simplicity. I have seen some info of get endpoints with messages.

There are two messages that have caught my attention.

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

http

No.	Time	Source	Destination	Protocol	Length	Info
52	2024-12-02 18:21:25.301614	192.168.1.189	3.167.56.56	HTTP	209	GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
54	2024-12-02 18:21:25.322313	3.167.56.56	192.168.1.189	HTTP	651	HTTP/1.1 301 Moved Permanently (text/html)
183	2024-12-02 18:21:28.088691	192.168.1.189	3.167.56.56	HTTP	195	GET /We-will-defeat-Darth-Vader. HTTP/1.1
185	2024-12-02 18:21:28.112726	3.167.56.56	192.168.1.189	HTTP	637	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 52: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{278744DD-E69B-4C9D-BBEE-FA0FF3CD4B53}, id 0
> Ethernet II, Src: f6:6d:4c:e7:bc:9c (f6:6d:4c:e7:bc:9c), Dst: Arcadyan_f2:02:be (04:a2:22:f2:02:be)
> Internet Protocol Version 4, Src: 192.168.1.189, Dst: 3.167.56.56
> Transmission Control Protocol, Src Port: 56706, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
✓ Hypertext Transfer Protocol
 ✓ GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1\r\n
 Request Method: GET
 Request URI: /We-have-the-blue-prints-to-the-Death-Star
 Request Version: HTTP/1.1
 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
 [Response in frame: 54]
 [Full request URI: http://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star]
 [Community ID: 1:MroPF/G5XhoMGfpcRhqIpDBu7Wc=]

Command Prompt

```
C:\Users\bhavi>echo "Bhavin Panchal-120278907"  
"Bhavin Panchal-120278907"  
  
C:\Users\bhavi>
```

c. Other evidence to support findings:

I have a search that keyword inside autopsy and it gave me several evidence that leads to believe me that attacker trying to attack on some kind of name Death star related.

Also, there are some images with blueprints are preparations to gathering target information corroborate attack on Death -star.

Bhavin_Panchal - Autopsy 4.21.0

Case View Tools Window Help

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

Listing Keyword search 2 - death

Keyword search

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
Web Search Artifact	yahoo.com:st-death-star-plansprogram	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:42:19 GMT-0400	2017-07-13 14:42:19 GMT-0400	2017-07-13 14:42:19 GMT-0400
Recent Documents Artifact	path: m:\death-star-planspath id	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:03:19 GMT-0400	2017-07-13 14:03:19 GMT-0400	2017-07-14 19:39:22 GMT-0400
NTFSERDART	folders you select-death-star-plans	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-14 19:40:08 GMT-0400	2017-07-14 19:40:08 GMT-0400	2017-07-14 19:40:08 GMT-0400
Recent Documents Artifact	path: m:\death-star-plansdeath-st	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:47 GMT-0400	2017-07-13 14:02:47 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-plansdeath-st	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:42 GMT-0400	2017-07-13 14:02:42 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-plansdeathstota	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:03:02 GMT-0400	2017-07-13 14:03:02 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-plansdeathstota	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:03:09 GMT-0400	2017-07-13 14:03:09 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-plansdeathstota	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:03:03 GMT-0400	2017-07-13 14:03:03 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-planslayout.j	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:29 GMT-0400	2017-07-13 14:02:29 GMT-0400	2017-07-14 19:39:22 GMT-0400
2DA317186AEA125F164821BC08052546A85274F	["death at"] "death star".	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:01:57 GMT-0400	2017-07-13 14:01:57 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-plans-the-offi	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:50 GMT-0400	2017-07-13 14:02:50 GMT-0400	2017-07-14 19:39:22 GMT-0400
0	its page "the-death-star-plans are now	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Death_star_blueprints_sw_card_trader.png.link	death_star_blueprints_sw_	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:59 GMT-0400	2017-07-13 14:02:59 GMT-0400	2017-07-14 19:39:22 GMT-0400
Death_star_blueprints_sw_card_trader.png.link-stack	death_star_blueprints_sw_	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:59 GMT-0400	2017-07-13 14:02:59 GMT-0400	2017-07-14 19:39:22 GMT-0400
Recent Documents Artifact	path: m:\death-star-plans\doom-10	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:25 GMT-0400	2017-07-13 14:02:25 GMT-0400	2017-07-14 19:39:22 GMT-0400
79E7E49E7CDA389E090294AD39EC2F02B35285	BbimBimBimBimBim-death_star_manual_null	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:29 GMT-0400	2017-07-13 14:02:29 GMT-0400	2017-07-13 14:02:29 GMT-0400
156a70b41b339278361b0c9230327c.jpg.link	/m:\death-star-plansdeath st	/img_Virtual Disk.vmdk/vol_vo2/Documents and Sett...	2017-07-13 14:02:38 GMT-0400	2017-07-13 14:02:38 GMT-0400	2017-07-14 19:39:22 GMT-0400

Strings: Extracted Text Translation

Page: 1 of 1 Page 100% Matches on page: 1 of 8 Match Reset Text Source Search

death_star_blueprints_sw_card_trader.png.link @<1C

Death Star Plans

Death Star Plans

Death_star_blueprints_sw_card_trader.png.jpeg

Death_star_blueprints_sw_card_trader.png.jpeg

M:\Death Star Plans\Death_star_blueprints_sw_card_trader.png.jpeg

M:\Death Star Plans

Bhavini_Panchal - Autopsy 4.21.0

Case View Tools Window Help

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

Listing Keyword search 2 - death x

Recent Documents

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-04:00	Virtual Disk.vmdk
Menuettes_1_2_from_41st_Symphony.lnk				C:\Documents and Settings\Administrator\My Docum...	2017-07-13 14:07:31 GMT-04:00	Virtual Disk.vmdk
156a70b41b33927f8361b8c923d03.jpg.lnk				M:\Death Star Plans\156a70b41b33927f8361b8c923d03...	2017-07-13 14:02:38 GMT-04:00	Virtual Disk.vmdk
21c2d524cd56625bc5b8f91e3df2a790.lnk				M:\Death Star Plans\21c2d524cd56625bc5b8f91e3df2a...	2017-07-13 14:02:54 GMT-04:00	Virtual Disk.vmdk
blah.lnk				C:\Documents and Settings\Administrator\My Docum...	2017-07-14 19:39:27 GMT-04:00	Virtual Disk.vmdk
Bourree_4th_Lute_Suite-Bach.lnk				C:\Documents and Settings\Administrator\My Docum...	2017-07-13 14:07:12 GMT-04:00	Virtual Disk.vmdk
code.lnk				C:\Documents and Settings\Administrator\My Docum...	2017-07-13 14:36:28 GMT-04:00	Virtual Disk.vmdk
Concerto-4-Violini-2_Teleman.lnk				C:\Documents and Settings\Administrator\My Docum...	2017-07-13 14:06:51 GMT-04:00	Virtual Disk.vmdk
Courante_1st_Cello_Suite.lnk				C:\Documents and Settings\Administrator\My Docum...	2017-07-13 14:07:48 GMT-04:00	Virtual Disk.vmdk
Death Star Plans.lnk				M:\Death Star Plans	2017-07-13 14:02:25 GMT-04:00	Virtual Disk.vmdk
Death-star-1.lnk				M:\Death Star Plans\Death-star-1.jpg	2017-07-13 14:02:47 GMT-04:00	Virtual Disk.vmdk
death-star-plans-157613.lnk				M:\Death Star Plans\death-star-plans-157613.jpg	2017-07-13 14:02:42 GMT-04:00	Virtual Disk.vmdk
DeathStar1.lnk				M:\Death Star Plans\DeathStar1.jpg	2017-07-13 14:02:32 GMT-04:00	Virtual Disk.vmdk
DeathStar3.lnk				M:\Death Star Plans\DeathStar3.jpg	2017-07-13 14:03:09 GMT-04:00	Virtual Disk.vmdk
Deathstar_blueprint.lnk				M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 14:03:03 GMT-04:00	Virtual Disk.vmdk
layout.lnk				M:\Death Star Plans\layout.jpg	2017-07-13 14:02:29 GMT-04:00	Virtual Disk.vmdk
Local Disk (M).lnk				M:\	2017-07-13 14:03:48 GMT-04:00	Virtual Disk.vmdk
Read-This.lnk				M:\Read-This.txt	2017-07-13 14:03:48 GMT-04:00	Virtual Disk.vmdk

File Views

- File Types
- Deleted Files
- File System (2016)
- All (3131)
- MB File Size
- Data Artifacts
 - Communication Accounts (3)
 - E-Mail Messages (2)
 - Installed Programs (24)
 - Metadata (40)
 - Operating System Information (1)
 - Process Documents (1)

File Metadata : OS Account : Data Artifacts : Analysis Results : Context : Annotations : Other Occurrences

Furthermore, there are some web searches regarding to death star plans and images downloaded in the system by user which are those that we have seen blueprints inside mp3 file, are concrete evidence suggesting the attacker goal and mindset.

places.sqlite		google.com	veracrypt	FireFox Analyzer	2017-07-13 13:44:39 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	python windows	FireFox Analyzer	2017-07-13 13:46:15 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	pyinstaller	FireFox Analyzer	2017-07-13 13:46:44 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:01:59 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:02 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:03 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:26 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:29 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:33 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:34 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:39 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:43 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:47 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:51 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:55 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:56 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:02:59 GMT-04:00	Virtual Disk.vmdk
places.sqlite		yahoo.com	death star plans	FireFox Analyzer	2017-07-13 14:03:03 GMT-04:00	Virtual Disk.vmdk

places.sqlite	1	http://a.dilcdn.com/wp-content/uploads/sites/6/2...	M:\Death Star Plans\DSOTM-1088x816-651507587451.j...	2017-07-13 14:02:25 GMT-04:00	FireFox Analyzer	dilcdn.com
places.sqlite	1	http://en.space.mzyachts.ru/ships/2/layout.jpg	M:\Death Star Plans\layout.jpg	2017-07-13 14:02:29 GMT-04:00	FireFox Analyzer	mzyachts.ru
places.sqlite	1	https://www.wired.com/wp-content/uploads/2016/12...	M:\Death Star Plans\DeathStar1.jpg	2017-07-13 14:02:32 GMT-04:00	FireFox Analyzer	wired.com
places.sqlite	1	http://media-cache-ak0.pinimg.com/originals/15/6a/...	M:\Death Star Plans\156a70b41b33927f8361b8c923d03...	2017-07-13 14:02:38 GMT-04:00	FireFox Analyzer	pinimg.com
places.sqlite	1	http://media.comicbook.com/2015/11/death-star-pla...	M:\Death Star Plans\death-star-plans-157613.jpg	2017-07-13 14:02:42 GMT-04:00	FireFox Analyzer	comicbook.cor
places.sqlite	1	https://1k95i3bqic3bboq03r87f8x-wpengine.netdna-s...	M:\Death Star Plans\Death-star-1.jpg	2017-07-13 14:02:47 GMT-04:00	FireFox Analyzer	netdna-ssl.com
places.sqlite	1	https://milnersblog.files.wordpress.com/2016/12/the...	M:\Death Star Plans\the-official-rogue-one-death-star...	2017-07-13 14:02:50 GMT-04:00	FireFox Analyzer	wordpress.com
places.sqlite	1	https://s-media-cache-ak0.pinimg.com/originals/21/...	M:\Death Star Plans\21c2d524cd56625bc5b8f91e3df2a...	2017-07-13 14:02:54 GMT-04:00	FireFox Analyzer	pinimg.com
places.sqlite	2	http://wimages.vr-zone.net/2016/11/Death_star_bluep...	M:\Death Star Plans\Death_star_blueprints_sw_card_tr...	2017-07-13 14:02:59 GMT-04:00	FireFox Analyzer	vr-zone.net
places.sqlite	1	http://vignette2.wikia.nocookie.net/starwars/images/...	M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 14:03:03 GMT-04:00	FireFox Analyzer	nocookie.net
places.sqlite	1	https://www.wired.com/wp-content/uploads/2016/12...	M:\Death Star Plans\DeathStar3.jpg	2017-07-13 14:03:09 GMT-04:00	FireFox Analyzer	wired.com
places.sqlite	2	https://i.stack.imgur.com/lrZmf.jpg	M:\Death Star Plans\lrZmf.jpg	2017-07-13 14:03:19 GMT-04:00	FireFox Analyzer	imgur.com

4. Recommendation and Next Steps

Based on the findings and analysis of the provided image ENPM687 Final XP.vmwarevm, the investigation has successfully uncovered critical evidence, including the decrypted mp3 file, the encrypted drive containing the final form executable, and associated images and messages. These findings conclusively point to the rebels possessing the blueprints of the Death Star and planning a mission to destroy it and defeat Darth Vader.

Recommendation:

Given the insights into the investigation and the significance of the evidence obtained, it is recommended to cease the investigation as the primary objectives have been met. The findings are robust and provide a clear narrative supported by technical evidence.

Next Steps:

Evidence Documentation: Compile all evidence, including decrypted files, messages, and the analysis report, into a formal documentation package for further reference or legal proceedings.
Stakeholder Communication: Share the findings with relevant stakeholders to enable decision-making based on the intelligence gathered.

Post-Incident Actions:

Assess vulnerabilities in the Death Star's security based on the findings to prevent exploitation.
Enhance monitoring systems to detect and mitigate further threats from the attackers. Also need to implement encryption and access controls to protect critical assets in future missions