Khushali Dalal 12/9/2017
ENPM 687 : Digital Forensics

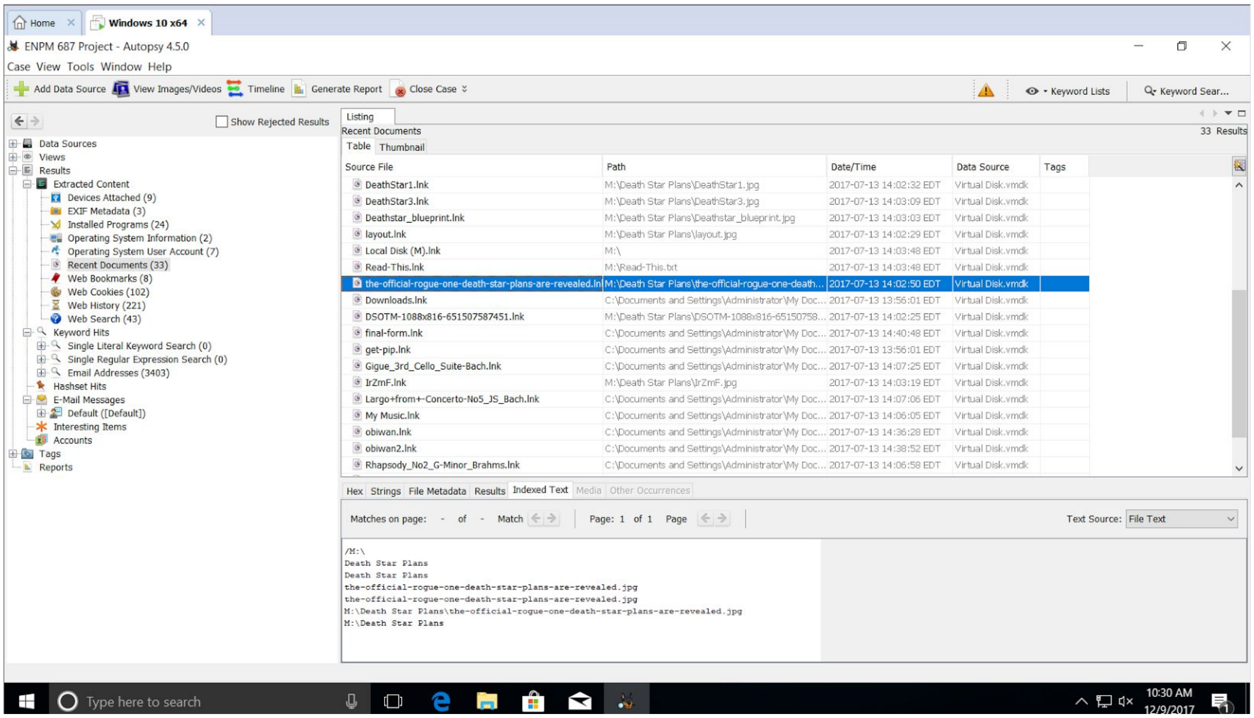
Final Project Report

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.

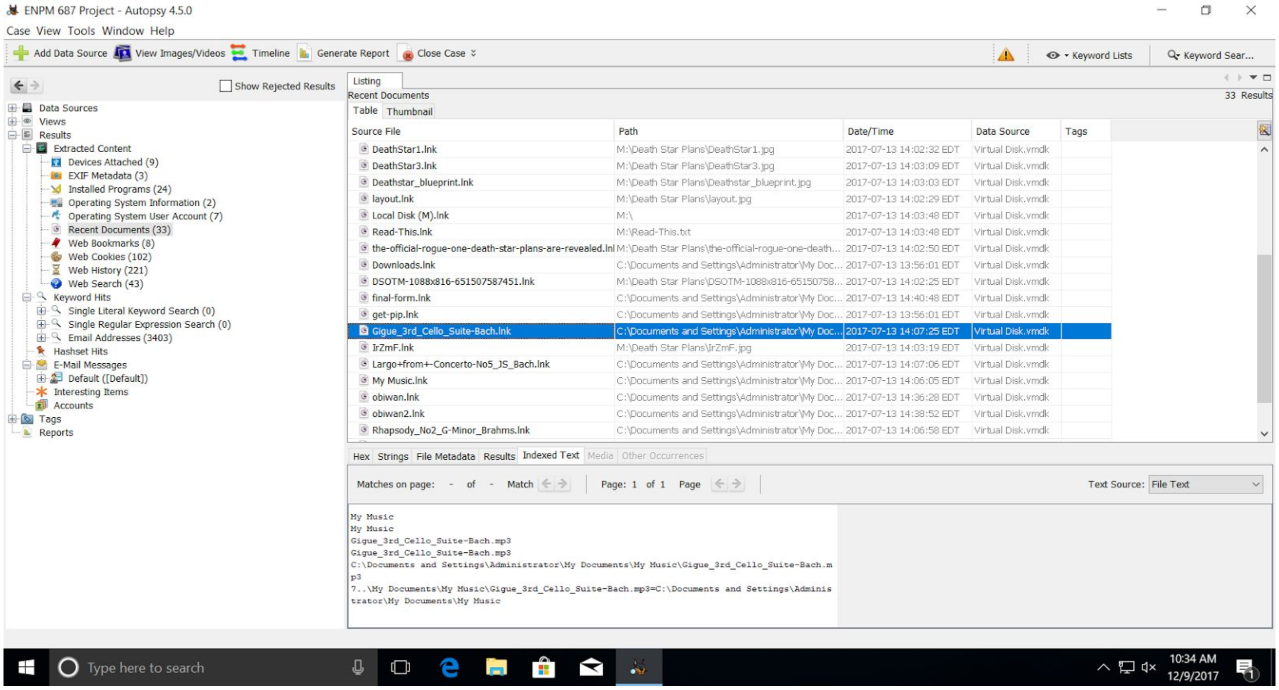
PART 1

First thing that stuck suspicious to me on investigating the image of Rebel malware writer hard drive was the file I found in recent documents. In all, there were 33 files in recent documents folder but, most of them seems to be like .jpg , .mp3 , .py , .ink . Below are the few screenshots of recent documents folder.



Source File	Path	Date/Time	Data Source	Tags
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	
Deathstar_blueprint.lnk	M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 14:03:03 EDT	Virtual Disk.vmdk	
layout.lnk	M:\Death Star Plans\layout.jpg	2017-07-13 14:02:29 EDT	Virtual Disk.vmdk	
Local Disk (M).lnk	M:\	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
Read-This.lnk	M:\Read-This.txt	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
the-official-rogue-one-death-star-plans-are-revealed.ln	M:\Death Star Plans\the-official-rogue-one-death...	2017-07-13 14:02:50 EDT	Virtual Disk.vmdk	
Downloads.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 13:56:01 EDT	Virtual Disk.vmdk	
DSOTM-1088x816-651507587451.lnk	M:\Death Star Plans\DSOTM-1088x816-65150758...	2017-07-13 14:02:25 EDT	Virtual Disk.vmdk	
final-form.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:40:48 EDT	Virtual Disk.vmdk	
get-pip.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 13:56:01 EDT	Virtual Disk.vmdk	
Gigue_3rd_Cello_Suite-Bach.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:07:25 EDT	Virtual Disk.vmdk	
IrZmF.lnk	M:\Death Star Plans\IrZmF.jpg	2017-07-13 14:03:19 EDT	Virtual Disk.vmdk	
Largo+from+-Concerto-No5_JS_Bach.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:07:06 EDT	Virtual Disk.vmdk	
My Music.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:06:05 EDT	Virtual Disk.vmdk	
obiwan.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:36:28 EDT	Virtual Disk.vmdk	
obiwan2.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:38:52 EDT	Virtual Disk.vmdk	
Rhapsody_No2_G-Minor_Brahms.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:06:58 EDT	Virtual Disk.vmdk	

```
/M:\
Death Star Plans
Death Star Plans
the-official-rogue-one-death-star-plans-are-revealed.jpg
the-official-rogue-one-death-star-plans-are-revealed.jpg
M:\Death Star Plans\the-official-rogue-one-death-star-plans-are-revealed.jpg
M:\Death Star Plans
```

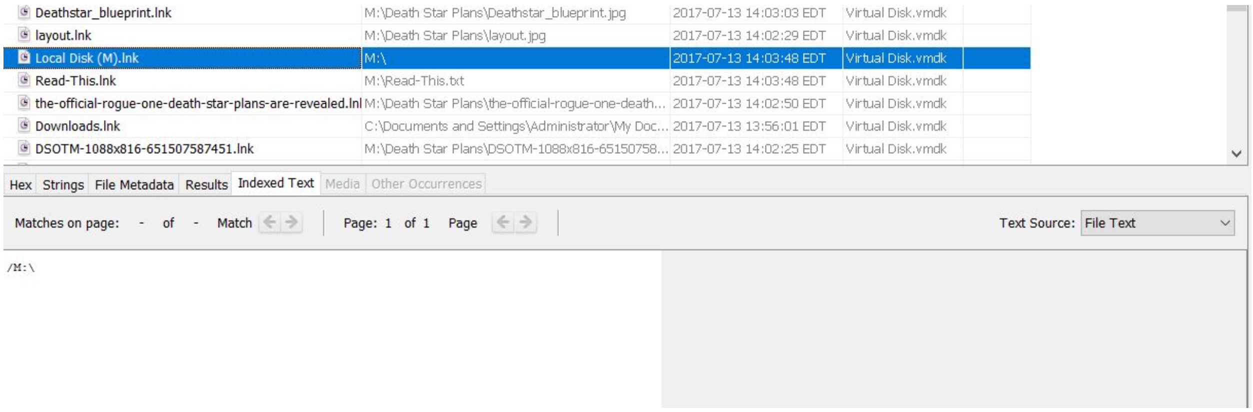


Recent Documents 33 Results

Source File	Path	Date/Time	Data Source	Tags
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	
Deathstar_blueprint.lnk	M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 14:03:03 EDT	Virtual Disk.vmdk	
layout.lnk	M:\Death Star Plans\layout.jpg	2017-07-13 14:02:29 EDT	Virtual Disk.vmdk	
Local Disk (M).lnk	M:\	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
Read-This.lnk	M:\Read-This.txt	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
the-official-rogue-one-death-star-plans-are-revealed.lnl	M:\Death Star Plans\the-official-rogue-one-death...	2017-07-13 14:02:50 EDT	Virtual Disk.vmdk	
Downloads.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 13:56:01 EDT	Virtual Disk.vmdk	
DSOTM-1088x816-651507587451.lnk	M:\Death Star Plans\DSOTM-1088x816-65150758...	2017-07-13 14:02:25 EDT	Virtual Disk.vmdk	
final-form.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:40:48 EDT	Virtual Disk.vmdk	
get-pip.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 13:56:01 EDT	Virtual Disk.vmdk	
Gigue_3rd_Cello_Suite-Bach.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:07:25 EDT	Virtual Disk.vmdk	
IrZmF.lnk	M:\Death Star Plans\IrZmF.jpg	2017-07-13 14:03:19 EDT	Virtual Disk.vmdk	
Largo+from+-Concerto-No5_JS_Bach.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:07:06 EDT	Virtual Disk.vmdk	
My Music.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:06:05 EDT	Virtual Disk.vmdk	
obiwan.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:36:28 EDT	Virtual Disk.vmdk	
obiwan2.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:38:52 EDT	Virtual Disk.vmdk	
Rhapsody_No2_G-Minor_Brahms.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 14:06:58 EDT	Virtual Disk.vmdk	

Matches on page: - of - Match Page: 1 of 1 Page Text Source: File Text

```
My Music
My Music
Gigue_3rd_Cello_Suite-Bach.mp3
Gigue_3rd_Cello_Suite-Bach.mp3
C:\Documents and Settings\Administrator\My Documents\My Music\Gigue_3rd_Cello_Suite-Bach.m
p3
7..\My Documents\My Music\Gigue_3rd_Cello_Suite-Bach.mp3=C:\Documents and Settings\Adminis
trator\My Documents\My Music
```



Source File	Path	Date/Time	Data Source	Tags
Deathstar_blueprint.lnk	M:\Death Star Plans\Deathstar_blueprint.jpg	2017-07-13 14:03:03 EDT	Virtual Disk.vmdk	
layout.lnk	M:\Death Star Plans\layout.jpg	2017-07-13 14:02:29 EDT	Virtual Disk.vmdk	
Local Disk (M).lnk	M:\	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
Read-This.lnk	M:\Read-This.txt	2017-07-13 14:03:48 EDT	Virtual Disk.vmdk	
the-official-rogue-one-death-star-plans-are-revealed.lnl	M:\Death Star Plans\the-official-rogue-one-death...	2017-07-13 14:02:50 EDT	Virtual Disk.vmdk	
Downloads.lnk	C:\Documents and Settings\Administrator\My Doc...	2017-07-13 13:56:01 EDT	Virtual Disk.vmdk	
DSOTM-1088x816-651507587451.lnk	M:\Death Star Plans\DSOTM-1088x816-65150758...	2017-07-13 14:02:25 EDT	Virtual Disk.vmdk	

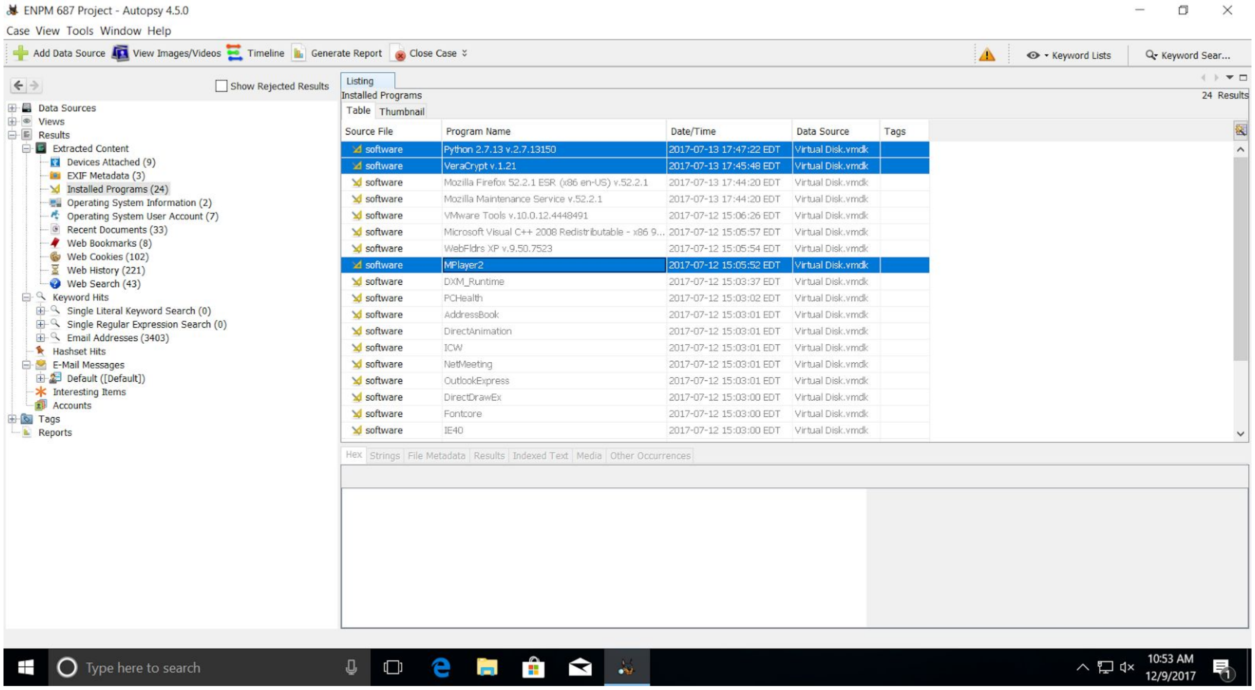
Matches on page: - of - Match Page: 1 of 1 Page Text Source: File Text

```
/M:\
```

Work done on Local Disk (M) drive shows no path, no information of data/files. Three conclusion, it might be empty, deleted or hidden.

PART 2

Now, looking inside installed programs folder some knowledge of software’s installed in the hard drive can be gained. For instance, veracrypt, python, Mplayer2. This reflects that malware writer would have used veracrypt to hide some part of the data on hard drive. But, what and why is still unanswered. Or it might be just to side track.

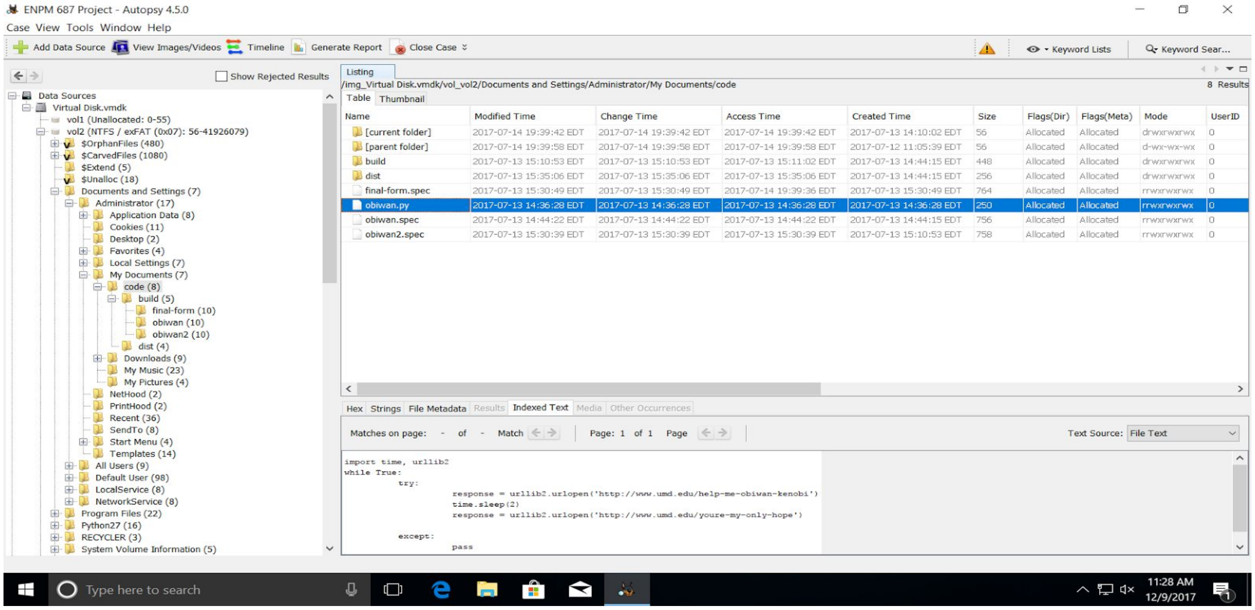


Installed Programs 24 Results

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...	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	
software	DirectDrawEx	2017-07-12 15:03:00 EDT	Virtual Disk.vmdk	
software	Fontcore	2017-07-12 15:03:00 EDT	Virtual Disk.vmdk	
software	IE40	2017-07-12 15:03:00 EDT	Virtual Disk.vmdk	

PART 3

On further analysis I came across, a file named “**code**” in My Documents under Administrator folder. The content of file obiwan.py looks familiar to HW#6. I feel there might be some clue in this folder.



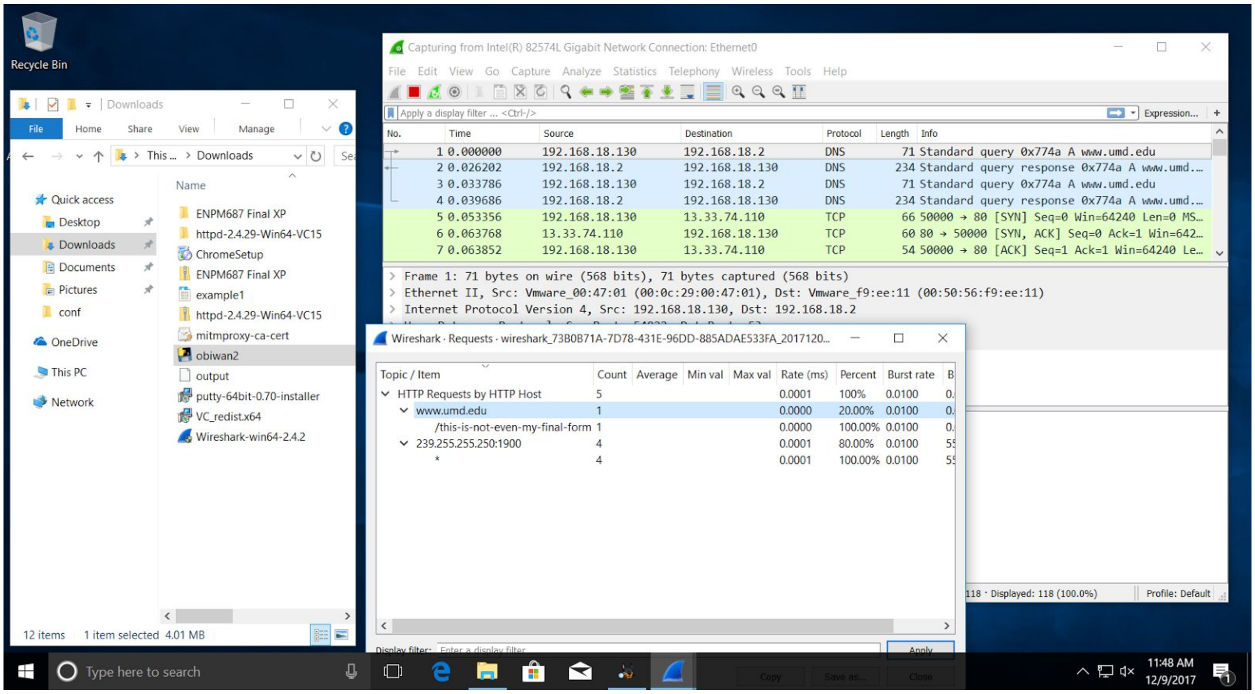
/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/code 8 Results

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID
[current folder]	2017-07-14 19:39:42 EDT	2017-07-14 19:39:42 EDT	2017-07-14 19:39:42 EDT	2017-07-13 14:10:02 EDT	56	Allocated	Allocated	drwxrwxrwx	0
[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	56	Allocated	Allocated	d-wx-wx-wx	0
build	2017-07-13 15:10:53 EDT	2017-07-13 15:10:53 EDT	2017-07-13 15:11:02 EDT	2017-07-13 14:44:15 EDT	448	Allocated	Allocated	drwxrwxrwx	0
dist	2017-07-13 15:35:06 EDT	2017-07-13 15:35:06 EDT	2017-07-13 15:35:06 EDT	2017-07-13 14:44:15 EDT	256	Allocated	Allocated	drwxrwxrwx	0
final-form.spec	2017-07-13 15:30:49 EDT	2017-07-13 15:30:49 EDT	2017-07-14 19:39:36 EDT	2017-07-13 15:30:49 EDT	764	Allocated	Allocated	rrwxrwxrwx	0
obiwan.py	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	250	Allocated	Allocated	rrwxrwxrwx	0
obiwan.spec	2017-07-13 14:44:22 EDT	2017-07-13 14:44:22 EDT	2017-07-13 14:44:22 EDT	2017-07-13 14:44:15 EDT	756	Allocated	Allocated	rrwxrwxrwx	0
obiwan2.spec	2017-07-13 15:30:39 EDT	2017-07-13 15:30:39 EDT	2017-07-13 15:30:39 EDT	2017-07-13 15:10:53 EDT	758	Allocated	Allocated	rrwxrwxrwx	0

```
import time, urllib2
while True:
        try:
                response = urllib2.urlopen('http://www.umd.edu/help-me-obiwan-kenobi')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/youre-my-only-hope')

        except:
                pass
```

It is somewhat impossible to judge what the contents of obiwan.spec, obiwan2.exe.manifest, obiwan2exe, warnobiwan2.txt. So, I think I need to know what’s all this files trying to execute. For that I tried to capture packets in Wireshark let's see if I could find any information from there.

PART 4



Capturing from Intel(R) 82574L Gigabit Network Connection: Ethernet0

```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.18.130  192.168.18.2    DNS        71 Standard query 0x774a A www.umd.edu
   2 0.026202   192.168.18.2    192.168.18.130  DNS       234 Standard query response 0x774a A www.umd....
   3 0.033786   192.168.18.130  192.168.18.2    DNS        71 Standard query 0x774a A www.umd.edu
   4 0.039686   192.168.18.2    192.168.18.130  DNS       234 Standard query response 0x774a A www.umd....
   5 0.053356   192.168.18.130  13.33.74.110    TCP        66 50000 → 80 [SYN] Seq=0 Win=64240 Len=0 MS...
   6 0.063768   13.33.74.110    192.168.18.130  TCP        60 80 → 50000 [SYN, ACK] Seq=0 Ack=1 Win=642...
   7 0.063852   192.168.18.130  13.33.74.110    TCP        54 50000 → 80 [ACK] Seq=1 Ack=1 Win=64240 Le...

> Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
> Ethernet II, Src: Vmware_00:47:01 (00:0c:29:00:47:01), Dst: Vmware_f9:ee:11 (00:50:56:f9:ee:11)
> Internet Protocol Version 4, Src: 192.168.18.130, Dst: 192.168.18.2
```

Wireshark · Requests · wireshark_73B0B71A-7D78-431E-96DD-885ADAE533FA_2017120...

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	B
HTTP Requests by HTTP Host	5				0.0001	100%	0.0100	0.
www.umd.edu	1				0.0000	20.00%	0.0100	0.
/this-is-not-even-my-final-form	1				0.0000	100.00%	0.0100	0.
239.255.255.250:1900	4				0.0001	80.00%	0.0100	55
*	4				0.0001	100.00%	0.0100	55

With the help of obiwan2.exe I tried to capture packets in Wireshark. The very first packet describes www.umd.edu. Looking at the HTTP requests we can see in the above screenshot "**/this-is-not-even-my-final-form**". The easiest way that struck my mind was to do keyword search in Autopsy for "**www.umd.edu**". This was just trial and error methodology. Came across a LogFile. Most important folder in the whole Operating System. All the logs generated would be residing in this folder. Finally found something interesting. Python script tries to throw hint of url's redirecting from www.umd.edu :

1. This-is-not-even-my-final-form

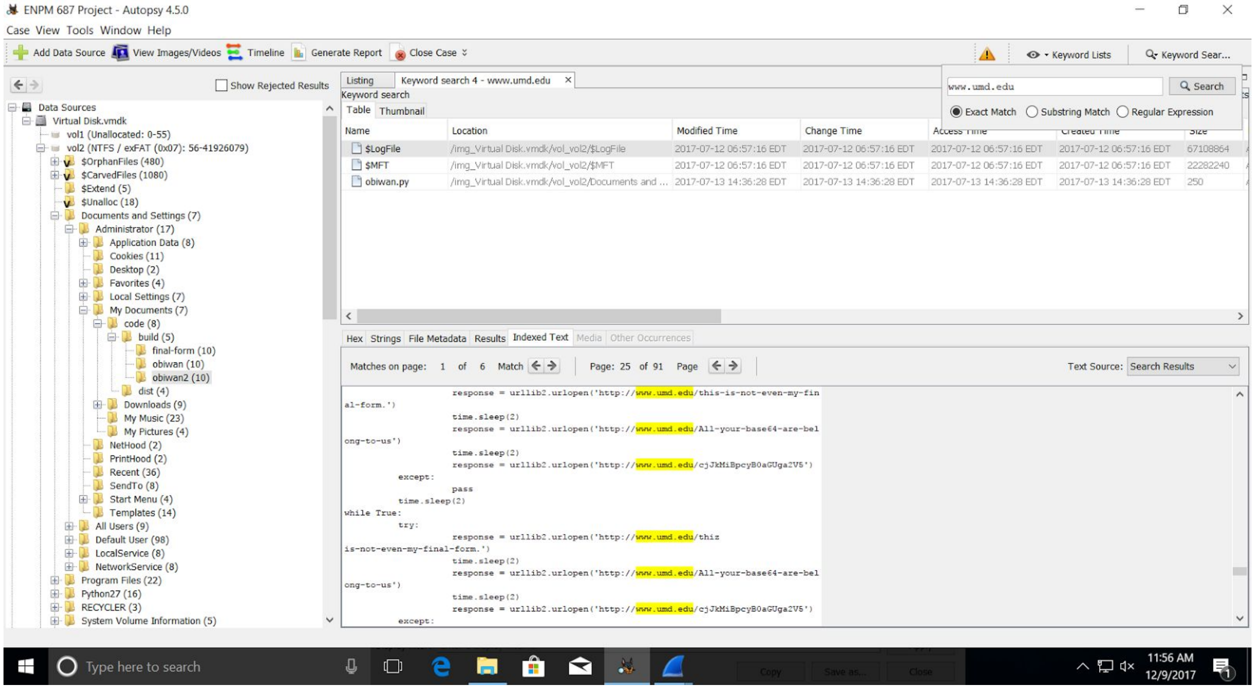
2. All-your-base64-are-belong-to-us

3. cjJkMiBpcyB0aGUga2V5

4. We-have-the-blue-prints-to-the-Death-Star

5. We-will-defeat-Darth-Vader.

The third url looks creepy.



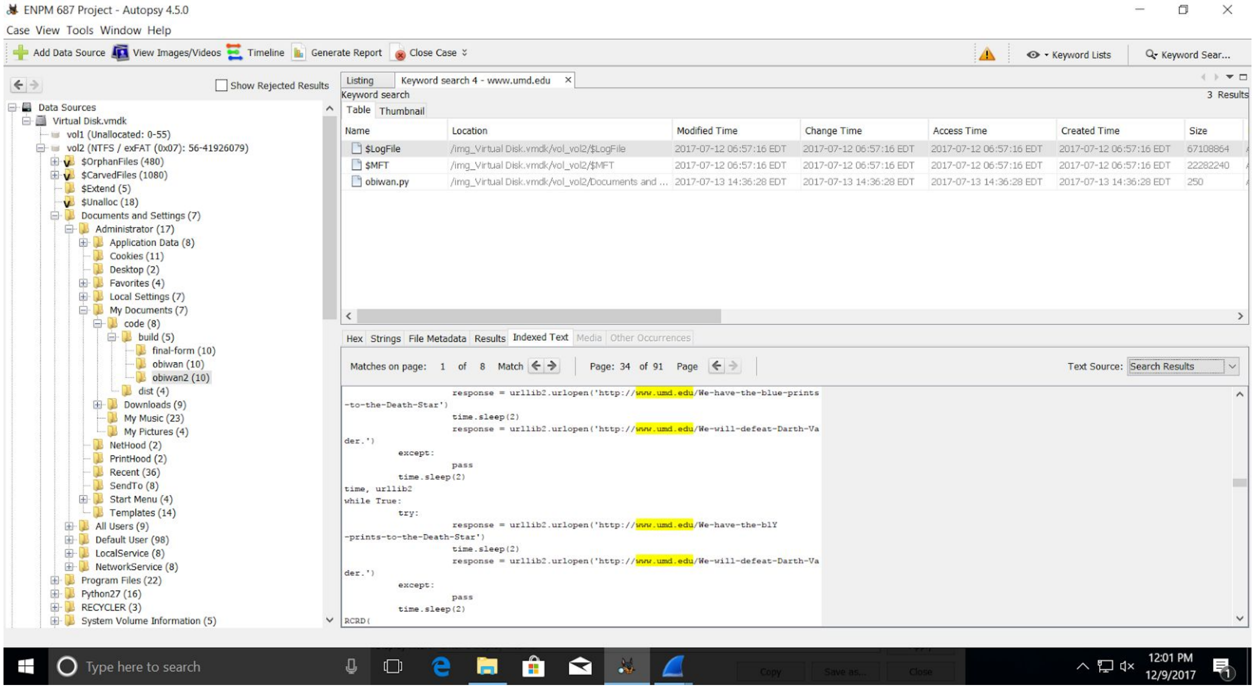
www.umd.edu Search

● Exact Match ○ Substring Match ○ Regular Expression

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size
$LogFile	/img_Virtual Disk.vmdk/vol_vol2/$LogFile	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	67108864
$MFT	/img_Virtual Disk.vmdk/vol_vol2/$MFT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	22282240
obiwan.py	/img_Virtual Disk.vmdk/vol_vol2/Documents and ...	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	250

Matches on page: 1 of 6 Match Page: 25 of 91 Page

```
                response = urllib2.urlopen('http://www.umd.edu/this-is-not-even-my-fin
al-form.')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/All-your-base64-are-bel
ong-to-us')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/cjJkMiBpcyB0aGUga2V5')
        except:
                pass
        time.sleep(2)
while True:
        try:
                response = urllib2.urlopen('http://www.umd.edu/thiz
is-not-even-my-final-form.')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/All-your-base64-are-bel
ong-to-us')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/cjJkMiBpcyB0aGUga2V5')
        except:
```

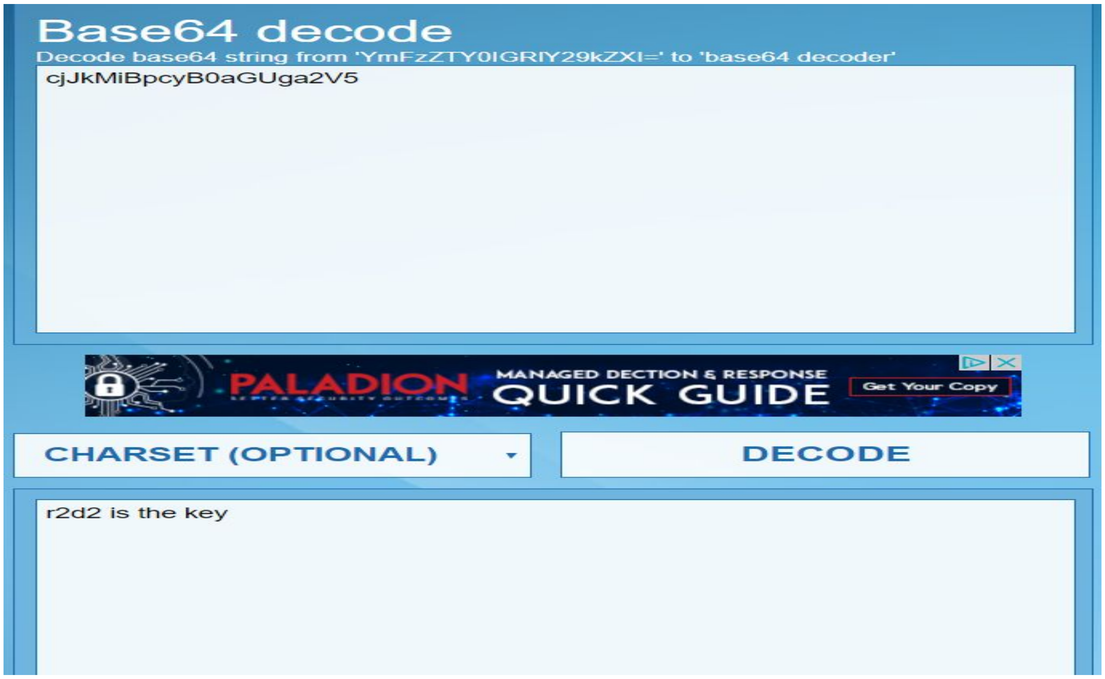


Name	Location	Modified Time	Change Time	Access Time	Created Time	Size
$LogFile	/img_Virtual Disk.vmdk/vol_vol2/$LogFile	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	67108864
$MFT	/img_Virtual Disk.vmdk/vol_vol2/$MFT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	22282240
obiwan.py	/img_Virtual Disk.vmdk/vol_vol2/Documents and ...	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	2017-07-13 14:36:28 EDT	250

Matches on page: 1 of 8 Match Page: 34 of 91 Page

```
                response = urllib2.urlopen('http://www.umd.edu/We-have-the-blue-prints
-to-the-Death-Star')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/We-will-defeat-Darth-Va
der.')
        except:
                pass
        time.sleep(2)
time, urllib2
while True:
        try:
                response = urllib2.urlopen('http://www.umd.edu/We-have-the-blY
-prints-to-the-Death-Star')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/We-will-defeat-Darth-Va
der.')
        except:
                pass
        time.sleep(2)
RCRD(
```

After some serious google search I concluded if I decode the scrambled letters and numbers using base64 decoder I get **r2d2 is the key** .



Base64 decode

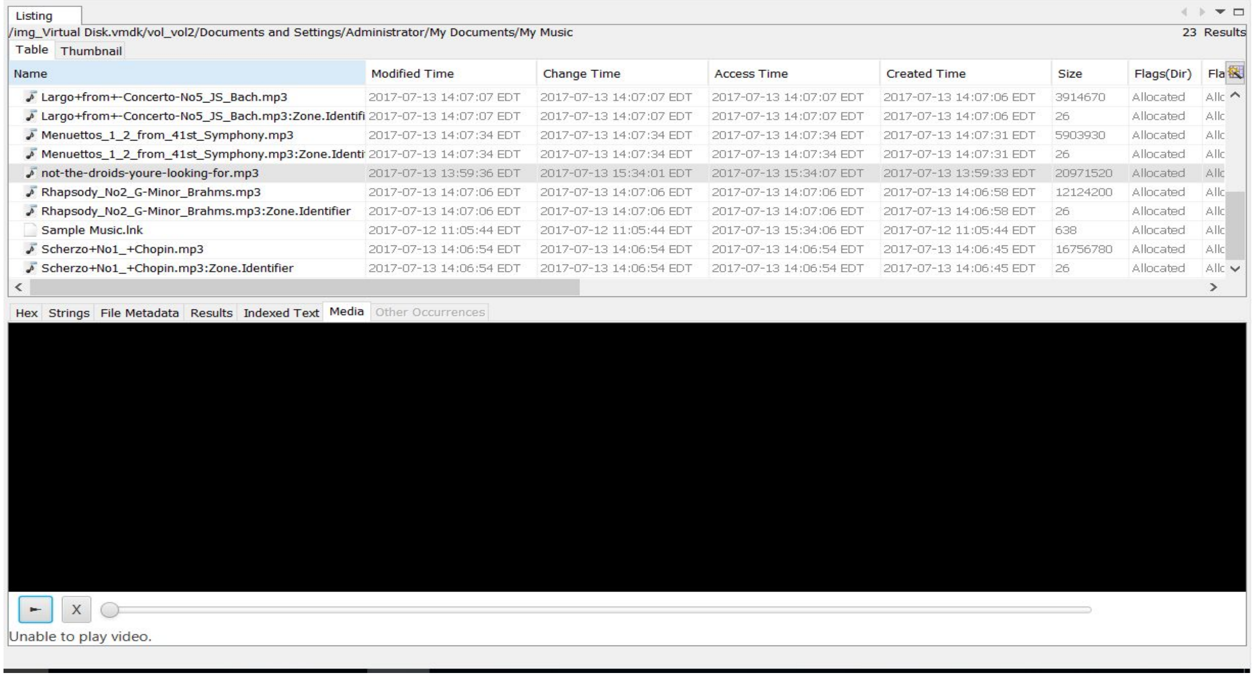
Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'base64 decoder'

```
cjJkMiBpcyB0aGUga2V5
```

```
r2d2 is the key
```

PART 5

Earlier in part 2, I mentioned that Veracrypt was one of the installed program in the hard drive. On top of that the first discovery was that the rebel malware writer was listening to music as there were .mp3 file in the recent documents folder.



Listing

/img_Virtual Disk.vmdk/vol_vol2/Documents and Settings/Administrator/My Documents/My Music 23 Results

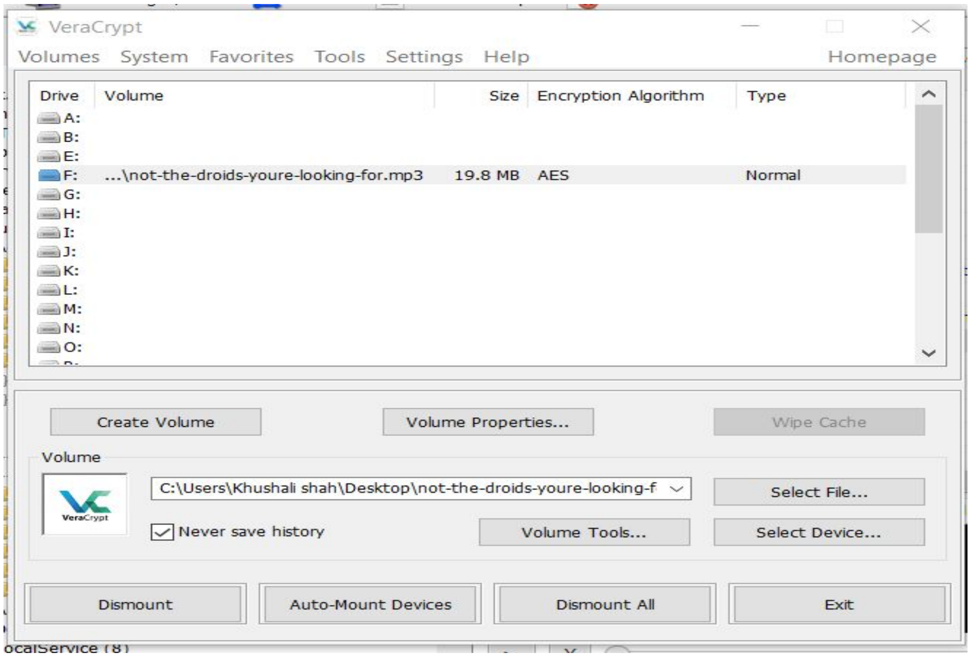
Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Fla
Largo+from+-Concerto-No5_JS_Bach.mp3	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT	2017-07-13 14:07:06 EDT	3914670	Allocated	Allc
Largo+from+-Concerto-No5_JS_Bach.mp3:Zone.Identifi	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT	2017-07-13 14:07:07 EDT	2017-07-13 14:07:06 EDT	26	Allocated	Allc
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	5903930	Allocated	Allc
Menuettos_1_2_from_41st_Symphony.mp3:Zone.Identi	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	26	Allocated	Allc
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	20971520	Allocated	Allc
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	12124200	Allocated	Allc
Rhapsody_No2_G-Minor_Brahms.mp3:Zone.Identifier	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	26	Allocated	Allc
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	638	Allocated	Allc
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	16756780	Allocated	Allc
Scherzo+No1_+Chopin.mp3:Zone.Identifier	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	26	Allocated	Allc

Unable to play video.

So, I went into the My Music folder and observed what kind of music was he/she listening. I came across a music file named “**not-the-droids-you-are-looking-for.mp3**”. The weird part of this music file was it was unable to play. All other music files were executable. That’s where I felt that some pieces are falling in place. I have a file which is not executable. I have a key and lastly I know the malware writer installed Veracrypt.

PART 6

VeraCrypt helped to decrypt the file “**not-the-droids-youre-looking-for.mp3”** using the key r2d2.



Drive	Volume	Size	Encryption Algorithm	Type
A:				
B:				
E:				
F:	...\not-the-droids-youre-looking-for.mp3	19.8 MB	AES	Normal
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				

C:\Users\Khushali shah\Desktop\not-the-droids-youre-looking-f

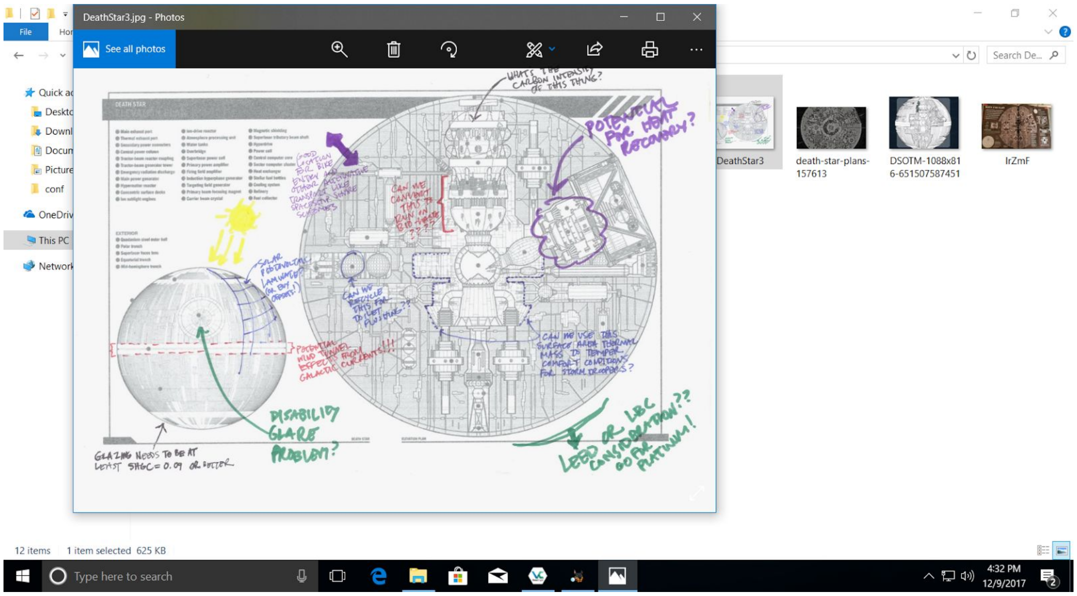
☑ Never save history

The hidden files inside **not-the-droids-youre-looking-for.mp3** are

1. Death Star Plans
2. ENPM687-Read-This
3. Final-form

PART 7

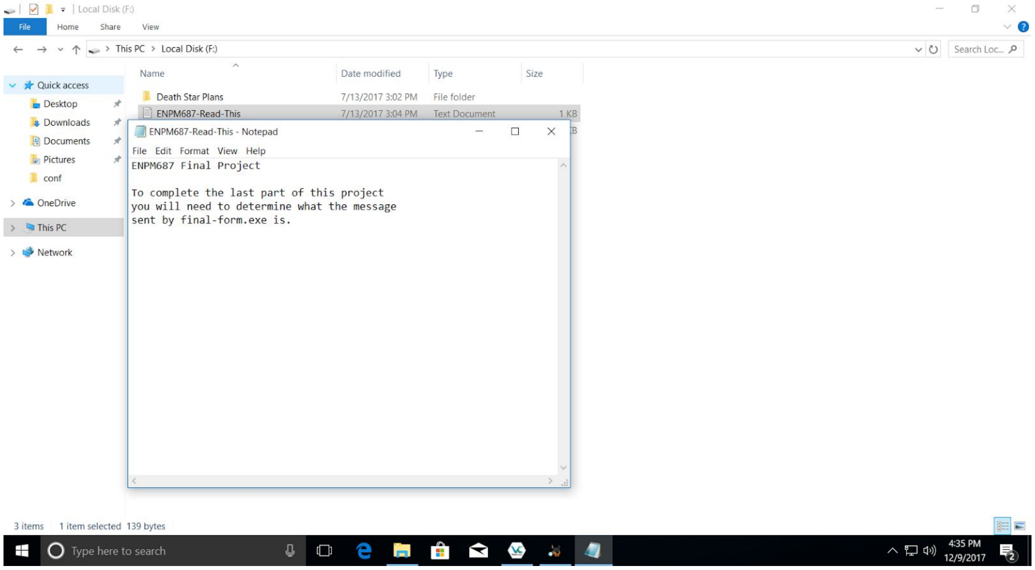
The Death Star Plans folder shows images of some intense planning plotting sketches.


DeathStar3.jpg - Photos
See all photos
DEATH STAR
WHATS THE CARBON INTENSITY OF THIS THING?
POTENTIAL FOR HEAT RECOVERY?
GOOD LOCATION FOR BIKE ENTRY AND OTHER ALTERNATIVE TRANSPORT LIKE SPACESTAR SHARE SCHEMES
CAN WE CONVERT THIS TO RUN ON BIO-WASTE ????
SOLAR PHOTOVOLTAIC LAMINATED (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!
DeathStar3
death-star-plans-157613
DSOTM-1088x816-651507587451
IrZmF
12 items 1 item selected 625 KB
Type here to search
4:32 PM 12/9/2017

The Notepad file "**ENPM687-Read-This**" displays clear cut message.

ENPM687 Final Project

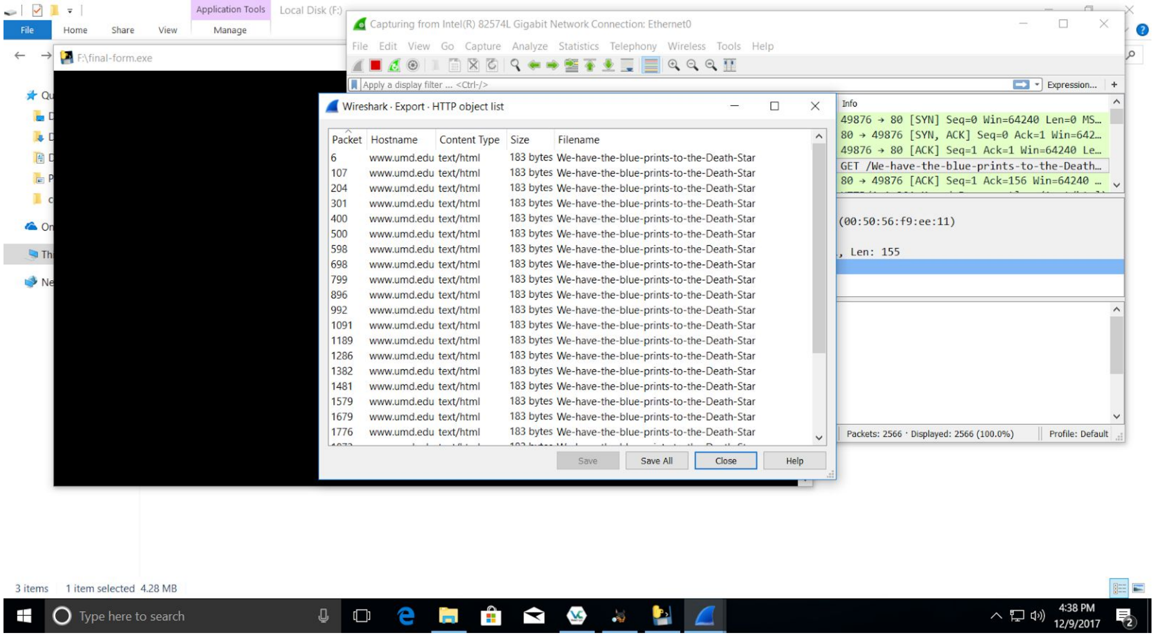
To complete the last part of this project you will need to determine what the message sent by final-form.exe is.



Name	Date modified	Type	Size
Death Star Plans	7/13/2017 3:02 PM	File folder	
ENPM687-Read-This	7/13/2017 3:04 PM	Text Document	1 KB

```
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.
```

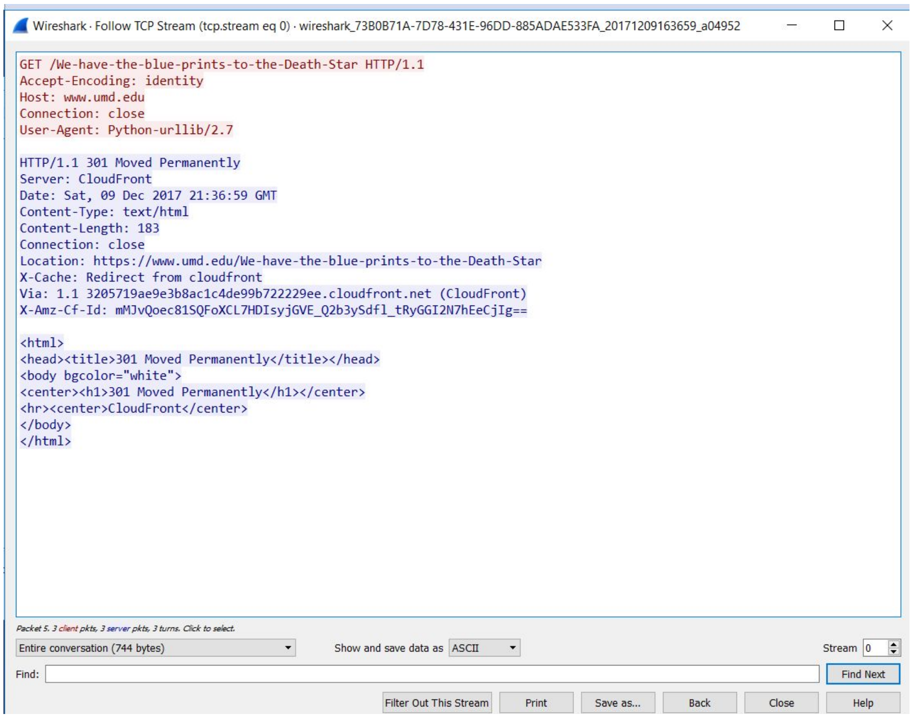
Lastly, the final-form looks like an exe file which can send packets and wireshark can help to capture those packets and make the last part of the project clear.


Capturing from Intel(R) 82574L Gigabit Network Connection: Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Wireshark · Export · HTTP object list
Save
Save All
Close
Help
Packets: 2566 · Displayed: 2566 (100.0%)
Profile: Default
F:\final-form.exe
Application Tools
Local Disk (F:)
File Home Share View Manage
3 items 1 item selected 4.28 MB
Type here to search
4:38 PM
12/9/2017

Packet	Hostname	Content Type	Size	Filename
6	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
107	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
204	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
301	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
400	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
500	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
598	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
698	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
799	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
896	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
992	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1091	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1189	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1286	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1382	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1481	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1579	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1679	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star
1776	www.umd.edu	text/html	183 bytes	We-have-the-blue-prints-to-the-Death-Star

```
Info
49876 → 80 [SYN] Seq=0 Win=64240 Len=0 MS…
80 → 49876 [SYN, ACK] Seq=0 Ack=1 Win=642…
49876 → 80 [ACK] Seq=1 Ack=1 Win=64240 Le…
GET /We-have-the-blue-prints-to-the-Death…
80 → 49876 [ACK] Seq=1 Ack=156 Win=64240 …

(00:50:56:f9:ee:11)

, Len: 155
```

The one suspicious packet visible is the "**We-have-the-blue-prints-to-the-Death-Star**"


Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_73B0B71A-7D78-431E-96DD-885ADAE533FA_20171209163659_a04952
Packet 5. 3 client pkts, 3 server pkts, 3 turns. Click to select.
Entire conversation (744 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

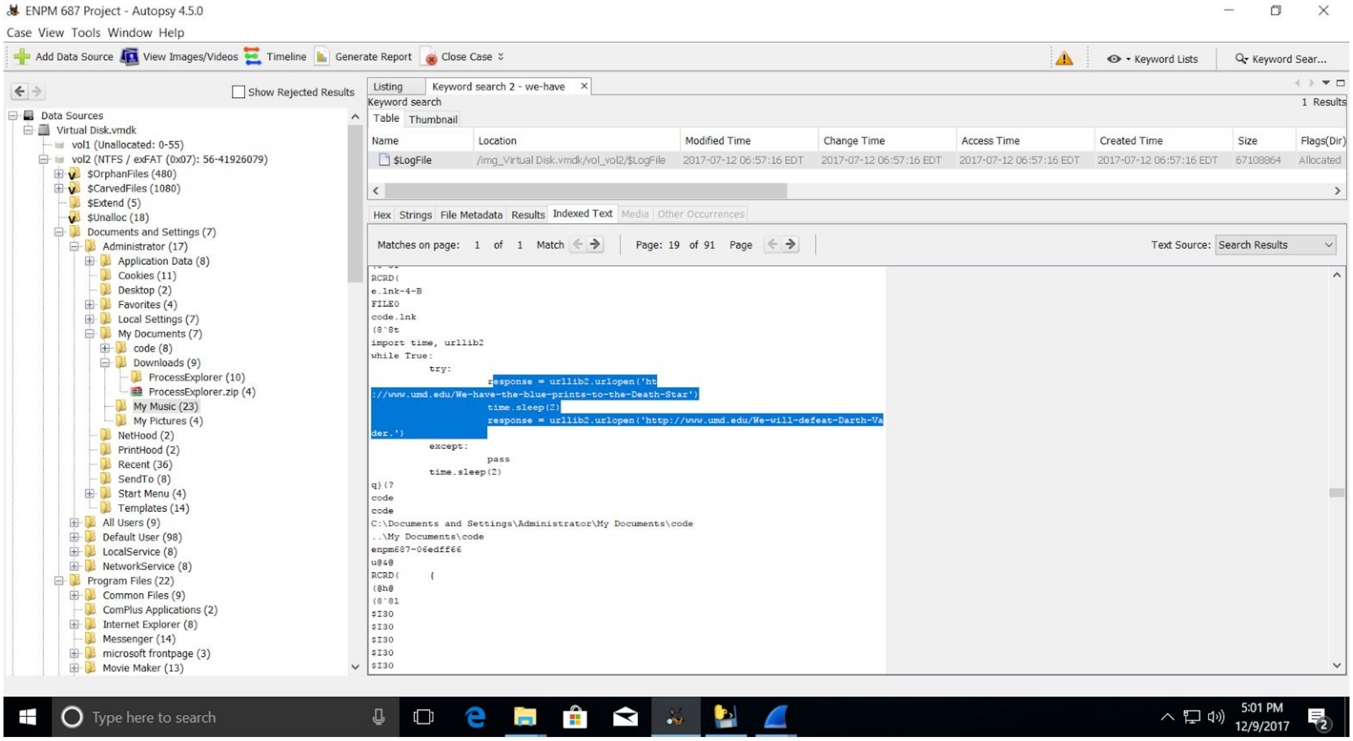
```
GET /We-have-the-blue-prints-to-the-Death-Star HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sat, 09 Dec 2017 21:36:59 GMT
Content-Type: text/html
Content-Length: 183
Connection: close
Location: https://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star
X-Cache: Redirect from cloudfront
Via: 1.1 3205719ae9e3b8ac1c4de99b722229ee.cloudfront.net (CloudFront)
X-Amz-Cf-Id: mMJvQoec81SQFoXCL7HDIsyjGVE_Q2b3ySdfl_tRyGGI2N7hEeCjIg==

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

Khushali Dalal 12/9/2017
ENPM 687 : Digital Forensics

PART 8

I thought this was the end of the project but, there is one more message. That message I discovered when I again explored log file and combining the results got in PART 4. The python scripts displays two messages:

1. We-have-the-blue-prints-to-the-death-star
2. We-will-defeat-Darth-Vader



Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
$LogFile	/img_Virtual Disk.vmdk/vol_vol2/$LogFile	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	2017-07-12 06:57:16 EDT	67108864	Allocated

```
RCRD(
e.lnk-4-B
FILE0
code.lnk
(8`8t
import time, urllib2
while True:
        try:
                response = urllib2.urlopen('ht
://www.umd.edu/We-have-the-blue-prints-to-the-Death-Star')
                time.sleep(2)
                response = urllib2.urlopen('http://www.umd.edu/We-will-defeat-Darth-Va
der.')
        except:
                pass
        time.sleep(2)
q}(?
code
code
C:\Documents and Settings\Administrator\My Documents\code
..\My Documents\code
enpm687-06edff66
u@&@
RCRD(    {
(@h@
(8`81
$I30
$I30
$I30
$I30
$I30
```

I assume these are the two messages send by final-form.exe file.