

Palpatine investigation

Yasmin Hassen

Ferris State University

Information Security and Intelligence

Jasun Hawkins

May 1, 2025

Table of content

Introduction	3
Imaging The hard drive.....	3
FTK Imager	3
Forensics Explore.....	9
Evidence.....	10
Registry File Review.....	29
Conclusion.....	30
Appendix of terms.....	31
References.....	32

Introduction

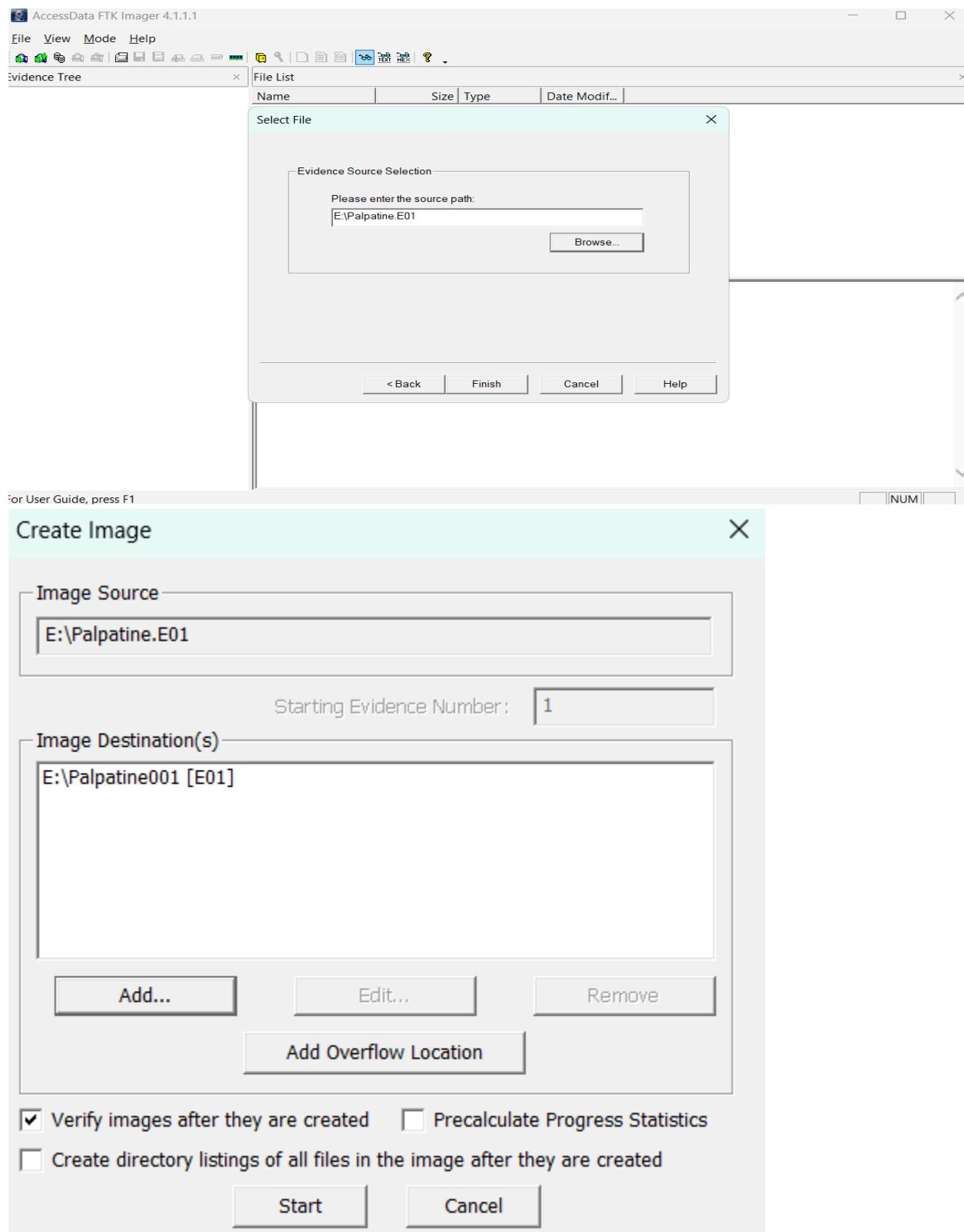
This case was about investigating the hard drive of a fictional suspect, Chancellor Palpatine. He is believed to be secretly working as a Sith Lord and planning dangerous operations like Order 66. My job was to examine his hard drive to look for any signs or proof of criminal activity.

I had permission by the Jedi High Council to perform the investigation. The image was provided for training purposes. I used forensic tools like FTK Imager and Forensic Explorer (FEX) to look through the drive. My goal was to find documents, emails, images, or anything that showed he was planning harm to the Jedi or involved in galactic conspiracies. This project helped me apply everything I've learned about proper forensic procedures, such as imaging, searching, carving, and reporting.

Imaging Information

The first step of the investigation was to create a forensic image of the suspect's hard drive. I used FTK Imager version 4.1.1.1 to do this. The image type was logical, which means it copied files and folders that were visible to the operating system but may have missed hidden or deleted ones in unallocated space.

I filled in the case number, examiner name, and a short description of the case. The imaging was successful. I checked and verified the image using MD5 and SHA1 hash values to make sure the image had not been changed or damaged. Both hashes matched. The image was split into two segments and saved as Palpatine.E01 and Palpatine.E02. The total size was 6.5 GB. It took about 15 minutes to finish imaging and verifying. This created a safe copy that I could now analyze without changing the original evidence.



Drive/Image Verify Results	
Name	Palpatine001.E01
Sector count	13312000
MD5 Hash	
Computed hash	d14337904bf0b9164ecf75ac8d5dc7b1
Stored verification hash	d14337904bf0b9164ecf75ac8d5dc7b1
Report Hash	d14337904bf0b9164ecf75ac8d5dc7b1
Verify result	Match
SHA1 Hash	
Computed hash	4fc3b7dc0e976b23c5589768feef045929
Stored verification hash	4fc3b7dc0e976b23c5589768feef045929
Report Hash	4fc3b7dc0e976b23c5589768feef045929
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image
Close	

Created By AccessData® FTK® Imager 4.1.1.1

Case Information:

Acquired using: ADI4.1.1.1

Case Number: 001

Evidence Number: palpatine

Unique description: palpatine case

Examiner: Yasmin Hassen

Notes: Palpatine

Information for E:\Palpatine001:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Logical

[Verification Hashes]

MD5 verification hash: d14337904bf0b9164ecf75ac8d5dc7b1

SHA1 verification hash: 4fcda3b7dc0e976b23c5589768feef04592900129

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 13,312,000

[Image]

Image Type: E01

Case number: Palpatine

Evidence number: 1

Examiner: Zach Rogers

Notes: Chancellor Palpatine is suspected of being a Sith Lord.

Acquired on OS: Win 201x

Acquired using: ADI4.7.1.2

Acquire date: 12/6/2024 10:28:15 PM

System date: 12/6/2024 10:28:15 PM

Unique description: Image of main drive.

Source data size: 6500 MB

Sector count: 13312000

[Computed Hashes]

MD5 checksum: d14337904bf0b9164ecf75ac8d5dc7b1

SHA1 checksum: 4fca3b7dc0e976b23c5589768feef04592900129

Image Information:

Acquisition started: Thu May 1 19:20:34 2025

Acquisition finished: Thu May 1 19:24:16 2025

Segment list:

E:\Palpatine001.E01

E:\Palpatine001.E02

Image Verification Results:

Verification started: Thu May 1 19:24:16 2025

Verification finished: Thu May 1 19:24:36 2025

MD5 checksum: d14337904bf0b9164ecf75ac8d5dc7b1 : verified

SHA1 checksum: 4fca3b7dc0e976b23c5589768feef04592900129 : verified

Forensic Explorer (FEX)

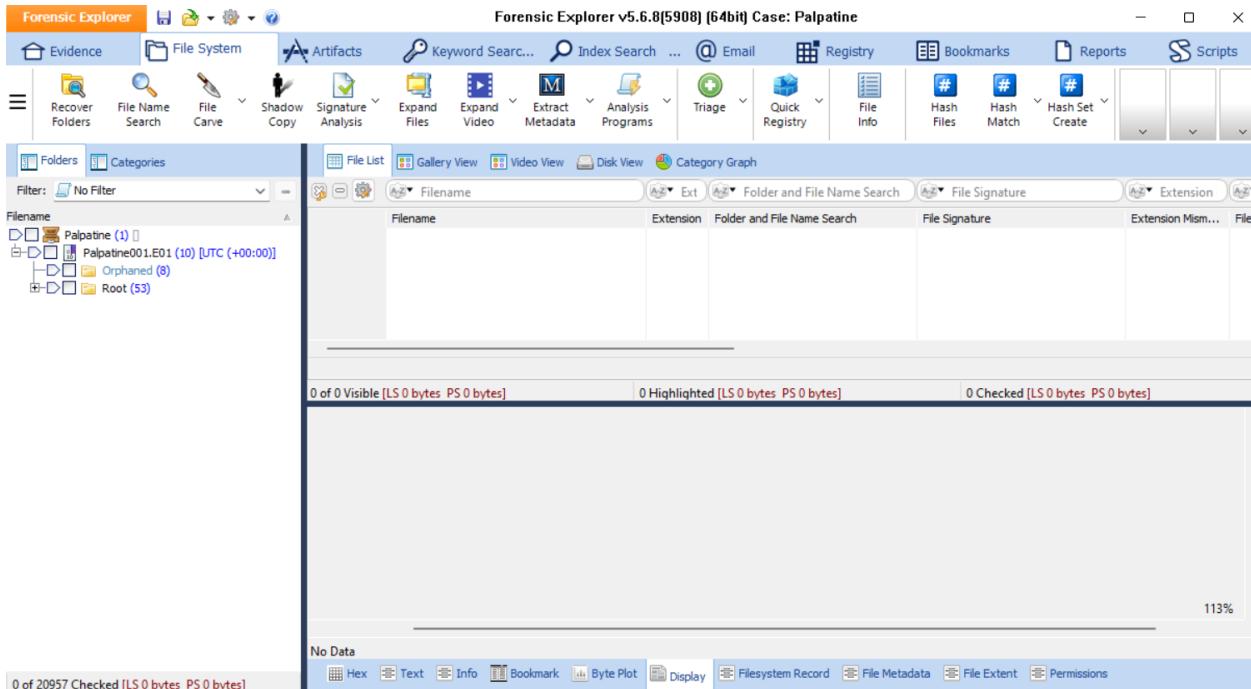
After I finished imaging the hard drive using FTK Imager, I used Forensic Explorer (FEX) to examine the evidence. FEX is a forensic tool that allows you to open and explore the image file without changing anything. It helped me search, sort, and view files inside the hard drive.

I started by creating a new case and adding the evidence image Palpatine001.E01. Once it was loaded, I let the software process and index the data. Then I explored different folders on the drive. I looked through places like Users, Documents, Downloads, and AppData, but most of the personal folders were empty or only had basic Windows files like sample music or pictures.

FEX also helped me do keyword searches. I searched for terms like Jedi, and Death Star. The search found some hits, but none of them were personal documents. Most were just part of system files or random file names.

One of the most helpful parts of FEX was the File Carving feature. I used it to try to recover deleted or hidden files. FEX found over 40,000 carved items, which looked promising. But after checking through different types of files, I realized that most of them were either empty, corrupted, or just random Windows files. I was not able to find anything specific that showed Chancellor Palpatine was doing something illegal.

Even though it was frustrating not finding strong evidence, using FEX helped me understand how to do a full investigation. I learned how to load and examine an image, search for keywords, check the file structure, carve deleted files, and organize results.



File List Gallery View Video View Disk View Category Graph

Filename Extension Folder and File Name Search File Signature Extension Mism... File C

	Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File C
1	Chancellor's Agenda.pdf	pdf		PDF	No	Doc
2	Chancellor's Agenda.pdf~Zone			Text		Tex
3	Contingency Plan.txt	txt		Text		Tex
4	Jedi Order.txt	txt		Text		Tex
5	New Apprentice.txt	txt		Text		Tex
6	Senate Meeting.txt	txt		Text		Tex

Palpatine001.E01\Root\Users\Palpatine\Documents\Chancellor's Agenda.pdf

6 of 6 Visible [LS 47 KB PS 53 KB] 1 Highlighted [LS 45 KB PS 48 KB] 0 Checked [LS 0 bytes PS 0 bytes]

Chancellor's Agenda:

9:00 AM - Begin the day with a visit to the Coruscant Botanical Gardens

11:00 AM - Meeting with Merchant Guilds about new trade agreements

12:30 PM - Meeting with the ambassador of Alderaan

2:00 PM - Lunch outing with Senator Amidala

3:00 PM to 6:00 PM - Senate debate

8:00 PM - Discussion with Jedi Council about the progress of the Clone Wars

Palpatine001.E01\Root\Users\Palpatine\Documents\Chancellor's Agenda.pdf

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

1 Chancellor's Agenda.pdf
 2 Chancellor's Agenda.pdf~Zone
 3 Contingency Plan.txt
 4 Jedi Order.txt
 5 New Apprentice.txt
 6 Senate Meeting.txt

Extension: pdf, txt
Folder and File Name Search:
File Signature: PDF, Text, Text, Text, Text, Text
Extension Mism...: No
File C: Doc, Text, Text, Text, Text, Text

Palpatine001.E01\Root\Users\Palpatine\Documents\Contingency Plan.txt

6 of 6 Visible [LS 47 KB PS 53 KB] 1 Highlighted [LS 142 bytes PS 142 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

Once every piece has been put into place, Order 66 can be executed to turn the Grand Army of the Galactic Republic

Palpatine001.E01\Root\Users\Palpatine\Documents\Contingency Plan.txt

File List Gallery View Video View Disk View Category Graph

1 Chancellor's Agenda.pdf
 2 Chancellor's Agenda.pdf~Zone
 3 Contingency Plan.txt
 4 Jedi Order.txt
 5 New Apprentice.txt
 6 Senate Meeting.txt

Extension: pdf, txt
Folder and File Name Search:
File Signature: PDF, Text, Text, Text, Text, Text
Extension Mism...: No
File C: Do, Te, Te, Te, Te, Te

Palpatine001.E01\Root\Users\Palpatine\Documents\Jedi Order.txt

6 of 6 Visible [LS 47 KB PS 53 KB] 1 Highlighted [LS 212 bytes PS 212 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

There are many enemies I have but none are as revolting as the Jedi.

I hate them all but a few I will make sure to get rid of are:

- Grand Master Yoda
- Mace Windu
- Obi-Wan Kenobi
- Qui-Gon Jin (eliminated)

Palpatine001.E01\Root\Users\Palpatine\Documents\Jedi Order.txt

Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

AZ▼ Filename AZ▼ Ext AZ▼ Folder and File Name Search AZ▼ File Signature AZ▼ Extension

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File
1 Chancellor's Agenda.pdf	pdf		PDF	No	Doc
2 Chancellor's Agenda.pdf~Zone			Text		Tex
3 Contingency Plan.txt	txt		Text		Tex
4 Jedi Order.txt	txt		Text		Tex
5 New Apprentice.txt	txt		Text		Tex
6 Senate Meeting.txt	txt		Text		Tex

Palpatine001.E01\Root\Users\Palpatine\Documents\New Apprentice.txt

6 of 6 Visible [LS 47 KB PS 53 KB] 1 Highlighted [LS 354 bytes PS 354 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

I am in need of a new apprentice, Maul completed his task but was too weak to see the whole picture.

I have found great promise in the former Jedi; Count Dooku. He has the ability to serve my needs.

I will have him raise an alliance of Separatists against the Republic and have him create a secret droid army to :

Palpatine001.E01\Root\Users\Palpatine\Documents\Senate Meeting.txt

File List Gallery View Video View Disk View Category Graph

AZ▼ Filename AZ▼ Ext AZ▼ Folder and File Name Search AZ▼ File Signature AZ▼ Extension

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File
1 Chancellor's Agenda.pdf	pdf		PDF	No	Do
2 Chancellor's Agenda.pdf~Zone			Text		Te
3 Contingency Plan.txt	txt		Text		Te
4 Jedi Order.txt	txt		Text		Te
5 New Apprentice.txt	txt		Text		Te
6 Senate Meeting.txt	txt		Text		Te

Palpatine001.E01\Root\Users\Palpatine\Documents\Senate Meeting.txt

6 of 6 Visible [LS 47 KB PS 53 KB] 1 Highlighted [LS 148 bytes PS 148 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

Notes for next Senate debate:

- Reach out to Senator Breemu about new mining laws.
- Talk about new Separatist threat.
- Settle trade dispute.

Palpatine001.E01\Root\Users\Palpatine\Documents\Senate Meeting.txt

File List Gallery View Video View Disk View Category Graph

AZ▼ Filename AZ▼ Ext AZ▼ Folder and File Name Search AZ▼ File Signature AZ▼ Extension

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File
1 Chancellor's Agenda.pdf	pdf		PDF	No	Do
2 Chancellor's Agenda.pdf~Zone			Text		Te
3 Contingency Plan.txt	txt		Text		Te
4 Jedi Order.txt	txt		Text		Te
5 New Apprentice.txt	txt		Text		Te
6 Senate Meeting.txt	txt		Text		Te

File List Gallery View Video View Disk View Category Graph

Filename Extension Folder and File Name Search File Signature Extension Mism... File C...

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File C...
1 brightfuture.txt	txt		Text		Text
2 Chosen One.txt	txt		Text		Text
3 HoloNetLog.txt	txt		Text		Text
4 Jedi chat log.txt	txt		Text		Text

Palpatine001.E01\Root\Users\Palpatine\Desktop\brightfuture.txt

4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 107 bytes PS 107 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

Becoming Supreme Chancellor of the Galactic Republic was only the beginning.....so much power.....

File List Gallery View Video View Disk View Category Graph

Filename Extension Folder and File Name Search File Signature Extension Mism... File C...

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File C...
1 brightfuture.txt	txt		Text		Text
2 Chosen One.txt	txt		Text		Text
3 HoloNetLog.txt	txt		Text		Text
4 Jedi chat log.txt	txt		Text		Text

Palpatine001.E01\Root\Users\Palpatine\Desktop\Chosen One.txt

4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 353 bytes PS 353 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

[Darth Sidious] - My apprentice, I have discovered a possible threat to my plans. The Jedi have discovered a 'Chosen One'.

[Darth Maul] - Master, what would you have me do?

[Darth Sidious] - Go to Naboo, Jedi Master Qui-Gon Jin is set to train the boy in the ways of the Jedi, kill him.

Palpatine001.E01\Root\Users\Palpatine\Desktop\Chosen One.txt

Hex Text Info Bookmark Byte Plot Display Flesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

Filename Ext Folder and File Name Search File Signature Extension Mism... File C

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File C
1 brightfuture.txt	txt		Text		Text
2 Chosen One.txt	txt		Text		Text
3 HoloNetLog.txt	txt		Text		Text
4 Jedi chat log.txt	txt		Text		Text

Palpatine001.E01\Root\Users\Palpatine\Desktop\HoloNet Log.txt
4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 600 bytes PS 4 KB] 0 Checked [LS 0 bytes PS 0 bytes]

[Darth Tyranus] - Master, I have heard news from Kamino that Jango Fett agreed to the deal and the production of a

[Darth Sidious] - Have the 'modifications' been made?

[Darth Tyranus] - Yes my lord, a biochip will be implanted into each clone to force them to follow any order.

[Darth Sidious] - Splendid!

[Darth Tyranus] - Is there anything further you require of me, master?

[Darth Sidious] - Yes! You will eliminate Jedi Master Sifo-Dyas, he is the only Jedi aware of this army and the or

Palpatine001.E01\Root\Users\Palpatine\Desktop\HoloNet Log.txt

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

Filename Ext Folder and File Name Search File Signature Extension Mism... File C

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...	File C
1 brightfuture.txt	txt		Text		Text
2 Chosen One.txt	txt		Text		Text
3 HoloNetLog.txt	txt		Text		Text
4 Jedi chat log.txt	txt		Text		Text

Palpatine001.E01\Root\Users\Palpatine\Desktop\Jedi chat log.txt
4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 532 bytes PS 532 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

[Chancellor Palpatine] - Greetings Anakin, I wanted to express my condolences for the death of your mother.

[Anakin Skywalker] - Hello Chancellor, I appreciate your concern for my wellbeing, it has been difficult.

[Chancellor Palpatine] - It is gravely unfortunate that tragedies such as these are not preventable. Protecting o

[Anakin Skywalker] - Does such a power exist?

[Chancellor Palpatine] - Come to my office later, I have something to tell you.

Palpatine001.E01\Root\Users\Palpatine\Desktop\Jedi chat log.txt

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
10 Carved_EXE/DLL_56288.exe	exe		EXE/DLL	No
11 Carved_Gif_269920.gif	gif		Gif	No
12 Carved_PDF_52768.pdf	pdf		PDF	No
13 Carved_PNG_206448.png	png		PNG	No
14 Carved_PNG_58504.png	png		PNG	No
15 Carved_Tout Shift TFC 102400.htm	htm		Tout Shift TFC	No

Palpatine.E01\File Carve\Carved_PNG_206448.png

125 of 125 Visible [LS 6.35 GB PS 6.35 GB] 1 Highlighted [LS 8 KB PS 9 KB] 0 Checked [LS 0 bytes PS 0 bytes]



295%

Palpatine.E01\File Carve\Carved_PNG_206448.png

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
200 Carved_EXE/DLL_102400.htm	htm		EXE/DLL	No
201 Carved_PNG_478536.png	png		PNG	No
202 Carved_PNG_482128.png	png		PNG	No
203 Carved_PNG_482256.png	png		PNG	No
204 Carved_PNG_482384.png	png		PNG	No
205 Carved_PNG_482512.png	png		PNG	No

Palpatine.E01\File Carve\Carved_PNG_482128.png

10711 of 10711 Visible [LS 6.38 GB PS 6.38 GB] 1 Highlighted [LS 7 KB PS 7 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

Palpatine.E01\File Carve\Carved_PNG_482128.png

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
6188 Carved_Icon_643656.ico	ico		Icon	No
6189 Carved_Icon_643784.ico	ico		Icon	No
6190 Carved_Icon_643912.ico	ico		Icon	No
6191 Carved_Icon_644040.ico	ico		Icon	No
6192 Carved_Icon_644552.ico	ico		Icon	No
6193 Carved_Icon_644600.ico	---		----	----

Palpatine.E01\File Carve\Carved_Icon_643912.ico

10711 of 10711 Visible [LS 6.38 GB PS 6.38 GB] 1 Highlighted [LS 29 KB PS 29 KB] 0 Checked [LS 0 bytes PS 0 bytes]




100%

Palpatine.E01\File Carve\Carved_Icon_643912.ico

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
1 ouu_over.png	png		png	no
3 add_over.png	png		PNG	No
4 add_up.png	png		PNG	No
5 base-docked.png	png		PNG	No
6 base-undocked-2.png	png		PNG	No
7 base-undocked-3.png	png		PNG	No

Palpatine.E01\Root\Program Files\Windows Sidebar\Gadgets\Currency.Gadget\images\base-undocked-2.png

20 of 20 Visible [LS 212 KB PS 1.0 MB] 1 Highlighted [LS 43 KB PS 64 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

Palpatine.E01\Root\Program Files\Windows Sidebar\Gadgets\Currency.Gadget\images\base-undocked-2.png

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

File List Gallery View Video View Disk View Category Graph

Filename AZ Ext AZ Folder and File Name Search AZ File Signature AZ Extension

	Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
<input type="checkbox"/>	1 brightfuture.txt	txt		Text	
<input type="checkbox"/>	2 Chosen One.txt	txt		Text	
<input type="checkbox"/>	3 HoloNet Log.txt	txt		Text	
<input type="checkbox"/>	4 Jedi chat log.txt	txt		Text	

Palpatine.E01\Root\Users\Palpatine\Desktop\brightfuture.txt
4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 107 bytes PS 107 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

Becoming Supreme Chancellor of the Galactic Republic was only the beginning.....so much power.....

Palpatine.E01\Root\Users\Palpatine\Desktop\brightfuture.txt
Hex Text Info Bookmark Byte Plot Preview Filesystem Record File Metadata File Extent Permissions
File List Gallery View Video View Disk View Category Graph

Filename AZ Ext AZ Folder and File Name Search AZ File Signature AZ Extension

	Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
<input type="checkbox"/>	1 brightfuture.txt	txt		Text	
<input checked="" type="checkbox"/>	2 Chosen One.txt	txt		Text	
<input type="checkbox"/>	3 HoloNet Log.txt	txt		Text	
<input type="checkbox"/>	4 Jedi chat log.txt	txt		Text	

Palpatine.E01\Root\Users\Palpatine\Desktop\Chosen One.txt
4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 353 bytes PS 353 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

[Darth Sidious] - My apprentice, I have discovered a possible threat to my plans. The Jedi have discovered a

[Darth Maul] - Master, what would you have me do?

[Darth Sidious] - Go to Naboo, Jedi Master Qui-Gon Jin is set to train the boy in the ways of the Jedi, kill

Palpatine.E01\Root\Users\Palpatine\Desktop\Chosen One.txt
Hex Text Info Bookmark Byte Plot Preview Filesystem Record File Metadata File Extent Permissions

HoloNet Log.txt

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
1 brightfuture.txt	txt		Text	
2 Chosen One.txt	txt		Text	
3 HoloNet Log.txt	txt		Text	
4 Jedi chat log.txt	txt		Text	

4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 600 bytes PS 4 KB] 0 Checked [LS 0 bytes PS 0 bytes]

```
[Darth Tyranus] - Master, I have heard news from Kamino that Jango Fett agreed to the deal and the producti
[Darth Sidious] - Have the 'modifications' been made?
[Darth Tyranus] - Yes my lord, a biochip will be implanted into each clone to force them to follow any orde
[Darth Sidious] - Splendid!
[Darth Tyranus] - Is there anything further you require of me, master?
```

Jedi chat log.txt

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
1 brightfuture.txt	txt		Text	
2 Chosen One.txt	txt		Text	
3 HoloNet Log.txt	txt		Text	
4 Jedi chat log.txt	txt		Text	

4 of 4 Visible [LS 2 KB PS 5 KB] 1 Highlighted [LS 532 bytes PS 532 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

```
[Chancellor Palpatine] - Greetings Anakin, I wanted to express my condolences for the death of your mother.
[Anakin Skywalker] - Hello Chancellor, I appreciate your concern for my wellbeing, it has been difficult.
[Chancellor Palpatine] - It is gravely unfortunate that tragedies such as these are not preventable. Protecti
[Anakin Skywalker] - Does such a power exist?
[Chancellor Palpatine] - Come to my office later, I have something to tell you.
```

File List Gallery View Video View Disk View Category Graph

Filename Ext Folder and File Name Search File Signature Extension Mism...

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
1 airspeeder.jfif	jfif		JPG	Yes
2 airspeeder.jfif~Zone			Text	
3 Blueprints.webp	webp		WebP	No
4 Blueprints.webp~Zone			Text	
5 chosen one.jfif	jfif		JPG	Yes
6 chosen one.jfif~Zone			Text	
7 city.jfif	jfif		JPG	Yes

Palpatine.E01\Root\Users\Palpatine\Pictures\airspeeder.jfif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 7 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

Palpatine.E01\Root\Users\Palpatine\Pictures\chosen one.jfif

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

Filename Ext Folder and File Name Search File Signature Extension Mism...

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
1 airspeeder.jfif	jfif		JPG	Yes
2 airspeeder.jfif~Zone			Text	
3 Blueprints.webp	webp		WebP	No
4 Blueprints.webp~Zone			Text	
5 chosen one.jfif	jfif		JPG	Yes
6 chosen one.jfif~Zone			Text	
7 city.jfif	jfif		JPG	Yes

Palpatine.E01\Root\Users\Palpatine\Pictures\chosen one.jfif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 7 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



80%

Palpatine.E01\Root\Users\Palpatine\Pictures\chosen one.jfif

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata **File Extent** Permissions

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension Mis...**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mis...
4 Blueprints.webp~Zone	jfff		Text	
5 chosen one.jff	jfff		JPG	Yes
6 chosen one.jfff~Zone			Text	
7 city.jfff	jfff		JPG	Yes
8 city.jfff~Zone			Text	
9 clone war.jfff	jfff		JPG	Yes
10 clone war.jfff~Zone			Text	

Palpatine.E01\Root\Users\Palpatine\Pictures\city.jfff

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 12 KB PS 16 KB] 0 Checked [LS 0 bytes PS 0 bytes]



Palpatine.E01\Root\Users\Palpatine\Pictures\clone war.jfff

Hex Text Info Bookmark Byte Plot Display F filesystem Record File Metadata File Extent Permissions

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension Mis...**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mis...
4 Blueprints.webp~Zone	jfff		Text	
5 chosen one.jff	jfff		JPG	Yes
6 chosen one.jfff~Zone			Text	
7 city.jfff	jfff		JPG	Yes
8 city.jfff~Zone			Text	
9 clone war.jfff	jfff		JPG	Yes
10 clone war.jfff~Zone			Text	

Palpatine.E01\Root\Users\Palpatine\Pictures\clone war.jfff

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 6 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



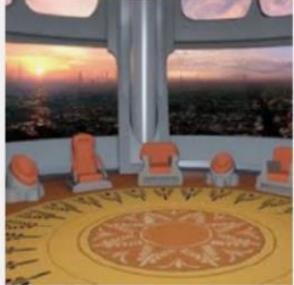
File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism..
7 city.jifif	jifif		JPG	Yes
8 city.jifif~Zone			Text	
9 clone war.jifif	jifif		JPG	Yes
10 clone war.jifif~Zone			Text	
11 holocron.jifif	jifif		JPG	Yes
12 holocron.jifif~Zone			Text	
13 jedi chamber.jifif	jifif		JPG	Yes
14 jedi chamber.jifif~Zone				

Palpatine.E01\Root\Users\Palpatine\Pictures\jedi chamber.jifif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 8 KB PS 12 KB] 0 Checked [LS 0 bytes PS 0 bytes]



89%

Palpatine.E01\Root\Users\Palpatine\Pictures\jedi chamber.jifif

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism..
11 clone war.jifif~Zone	jifif		JPG	Yes
12 holocron.jifif	jifif		Text	
13 jedi chamber.jifif	jifif		JPG	Yes
14 jedi chamber.jifif~Zone			Unknown	
15 me.jifif	jifif		JPG	Yes
16 me.jifif~Zone			Unknown	
17 meeting.jifif	jifif		JPG	Yes

Palpatine.E01\Root\Users\Palpatine\Pictures\me.jifif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 5 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

Palpatine.E01\Root\Users\Palpatine\Pictures\me.jifif

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
11 holocron.jif	jif		JPG	Yes
12 holocron.jif~Zone			Text	
13 jedi chamber.jif	jif		JPG	Yes
14 jedi chamber.jif~Zone			Unknown	
15 me.jif	jif		JPG	Yes
16 me.jif~Zone			Unknown	
17 meeting.jif	jif		JPG	Yes

Palpatine.E01\Root\Users\Palpatine\Pictures\meeting.jif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 7 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

Palpatine.E01\Root\Users\Palpatine\Pictures\meeting.jif

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

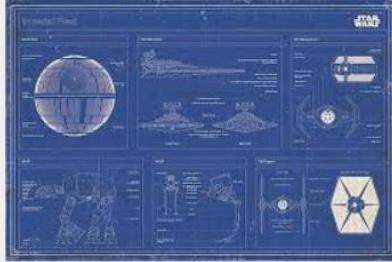
File List **Gallery View** **Video View** **Disk View** **Category Graph**

Filename **Ext** **Folder and File Name Search** **File Signature** **Extension**

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
15 jedi chamber.jif~Zone			UNKNOWN	
16 me.jif	jif		JPG	Yes
17 me.jif~Zone			Unknown	
18 meeting.jif	jif		JPG	Yes
19 moon station.jif	jif		JPG	Yes
20 moon station.jif~Zone			Text	
21 Mustafar.jpg	jpg		JPG	No

Palpatine.E01\Root\Users\Palpatine\Pictures\moon station.jif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 10 KB PS 12 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

Palpatine.E01\Root\Users\Palpatine\Pictures\moon station.jif

Hex **Text** **Info** **Bookmark** **Byte Plot** **Display** **Filesystem Record** **File Metadata** **File Extent** **Permissions**

	Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
15	me.jif	jif		JPG	Yes
16	me.jif~Zone			Unknown	
17	meeting.jif	jif		JPG	Yes
18	meeting.jif~Zone			Text	
19	moon station.jif	jif		JPG	Yes
20	moon station.jif~Zone			Text	
21	Mustafar.jpg	jpg		JPG	No

Palpatine.E01\Root\Users\Palpatine\Pictures\Mustafar.jpg

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 70 KB PS 72 KB] 0 Checked [LS 0 bytes PS 0 bytes]



22%

Palpatine.E01\Root\Users\Palpatine\Pictures\Mustafar.jpg

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

	Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
18	meeting.jif~Zone			Text	
19	moon station.jif	jif		JPG	Yes
20	moon station.jif~Zone			Text	
21	Mustafar.jpg	jpg		JPG	No
22	Mustafar.jpg~Zone			Text	
23	my toy.jif	jif		JPG	Yes
24	my toy.jif~Zone			Unknown	
25	---.jif	jif		---	

Palpatine.E01\Root\Users\Palpatine\Pictures\my toy.jif

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 5 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



90%

Palpatine.E01\Root\Users\Palpatine\Pictures\my toy.jif

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

Filename Ext Folder and File Name Search File Signature Extension

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
20 moon station.jfit~Zone	jpg		Text	
21 Mustafar.jpg	jpg		JPG	No
22 Mustafar.jpg~Zone			Text	
23 my toy.jff	jff		JPG	Yes
24 my toy.jfit~Zone			Unknown	
25 naboo.jff	jff		JPG	Yes
26 naboo.jfit~Zone			Unknown	
27 nbi-wan.jff	jff		JPG	Yes

Palpatine.E01\Root\Users\Palpatine\Pictures\naboo.jff

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 12 KB PS 16 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

File List Gallery View Video View Disk View Category Graph

Filename Ext Folder and File Name Search File Signature Extension

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
22 Mustafar.jpg~Zone			Text	
23 my toy.jff	jff		JPG	Yes
24 my toy.jfit~Zone			Unknown	
25 naboo.jff	jff		JPG	Yes
26 naboo.jfit~Zone			Unknown	
27 obi-wan.jff	jff		JPG	Yes
28 obi-wan.jfit~Zone			Unknown	
29 republik.png	png		PNG	No

Palpatine.E01\Root\Users\Palpatine\Pictures\obi-wan.jff

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 5 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]



100%

File List Gallery View Video View Disk View Category Graph

Filename Ext Folder and File Name Search File Signature Extension

Filename	Extension	Folder and File Name Search	File Signature	Extension Mism...
22 Mustafar.jpg~Zone			Text	
23 my toy.jff	jff		JPG	Yes
24 my toy.jfit~Zone			Unknown	
25 naboo.jff	jff		JPG	Yes
26 naboo.jfit~Zone			Unknown	
27 obi-wan.jff	jff		JPG	Yes
28 obi-wan.jfit~Zone			Unknown	
29 republik.png	png		PNG	No

Palpatine.E01\Root\Users\Palpatine\Pictures\obi-wan.jff

46 of 46 Visible [LS 378 KB PS 430 KB] 1 Highlighted [LS 5 KB PS 8 KB] 0 Checked [LS 0 bytes PS 0 bytes]

File List Gallery View Video View Disk View Category Graph

replic.png robe.jfif Senate buildin... senate chamb... separatist.png ship.jfif speeder.jfif

tatooine.jfif yoda.jfif

Palpatine.E01\Root\Users\Palpatine\Pictures\speeder.jfif

21 /23 of 23 Visible [LS 375 KB PS 428 KB] 1 Highlighted [LS 5 KB PS 8 KB] speeder.jfif



100%

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

replic.png robe.jfif Senate buildin... senate chamb... separatist.png ship.jfif speeder.jfif

tatooine.jfif yoda.jfif

Palpatine.E01\Root\Users\Palpatine\Pictures\Senate building.jfif

17 /23 of 23 Visible [LS 375 KB PS 428 KB] 1 Highlighted [LS 10 KB PS 12 KB] Senate



100%

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

replica.png robe.jifif Senate buildin... senate chamb... separatist.png ship.jifif speeder.jifif

tatooine.jifif yoda.jifif

Palpatine.E01\Root\Users\Palpatine\Pictures\senate chamber.jifif

18/23 of 23 Visible [LS 375 KB PS 428 KB] 1 Highlighted [LS 11 KB PS 12 KB] senate chan



100%

Palpatine.E01\Root\Users\Palpatine\Pictures\senate chamber.jifif

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

A-Z ▾ Filename A-Z ▾ Ext A-Z ▾ Folder and File Name Search A-Z ▾ File Signature A-Z ▾ E

Filename	Extension	Folder and File Name Search	File Signature	Extensi
1	bat_6...		Text	
2	sys_6...		Text	
3	dll_37...		EXE/DLL	Ye:
4	xml_2...		XML	Ye:
5	xml_3...		XML	Ye:
6	xml_0...		XML	Ye:
7	xml_3...		XML	Ye:
-		

Palpatine.E01\Root\Win...x86_microsoft-windows-ntvdm-system32_31bf3856ad364e35_6.1.7601.17514_none_0014e305d0cff0a7_autoexec.bat_6d6f4bc5

38 of 38 Visible [LS 701 KB PS 2.3 MB] 1 Highlighted [LS 24 bytes PS 24 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

REM Dummy file for NTVDM

Palpatine.E01\Root\Windows\winsxs\Backup\x86_microsoft-windows-ntvdm-system32_31bf3856ad364e35_6.1.7601.17514_none_0014e305d0cff0a7_autoe

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

A-Z▼ Filename A-Z▼ Ext A-Z▼ Folder and File Name Search A-Z▼ File Signature

Filename	Extension	Folder and File Name Search	File Signature	Extensi
4	txt		Windows Recycle Bin	Yes
5	txt		Windows Recycle Bin	Yes
6	txt		Text	
7	txt		Text	
8	txt		No size	
9	ini		Unknown	
10	ini		Text	

Palpatine.E01\Root\\$Recycle.Bin\S-1-5-21-346071495-2028852961-265169757-1001\\$R2SVVNE (New Apprentice).txt

10 of 10 Visible [LS 1 KB PS 1 KB] 1 Highlighted [LS 286 bytes PS 286 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

I am in need of a new apprentice, Maul completed his task but was too weak to see the whole picture.

I have found great promise in the former Jedi; Count Dooku. He has the ability to serve my needs.

I will have him raise a secret droid army to incite civil war across the galaxy!!

Palpatine.E01\Root\\$Recycle.Bin\S-1-5-21-346071495-2028852961-265169757-1001\\$R015Q24 (Chosen One).txt

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions

File List Gallery View Video View Disk View Category Graph

A-Z▼ Filename A-Z▼ Ext A-Z▼ Folder and File Name Search A-Z▼ File Signature

Filename	Extension	Folder and File Name Search	File Signature	Extensi
4	txt		Windows Recycle Bin	Yes
5	txt		Windows Recycle Bin	Yes
6	txt		Text	
7	txt		Text	
8	txt		No size	
9	ini		Unknown	
10	ini		Text	

Palpatine.E01\Root\\$Recycle.Bin\S-1-5-21-346071495-2028852961-265169757-1001\\$R015Q24 (Chosen One).txt

10 of 10 Visible [LS 1 KB PS 1 KB] 1 Highlighted [LS 532 bytes PS 532 bytes] 0 Checked [LS 0 bytes PS 0 bytes]

[Chancellor Palpatine] - Greetings Anakin, I wanted to express my condolences for the death of your mother.

[Anakin Skywalker] - Hello Chancellor, I appreciate your concern for my wellbeing, it has been difficult.

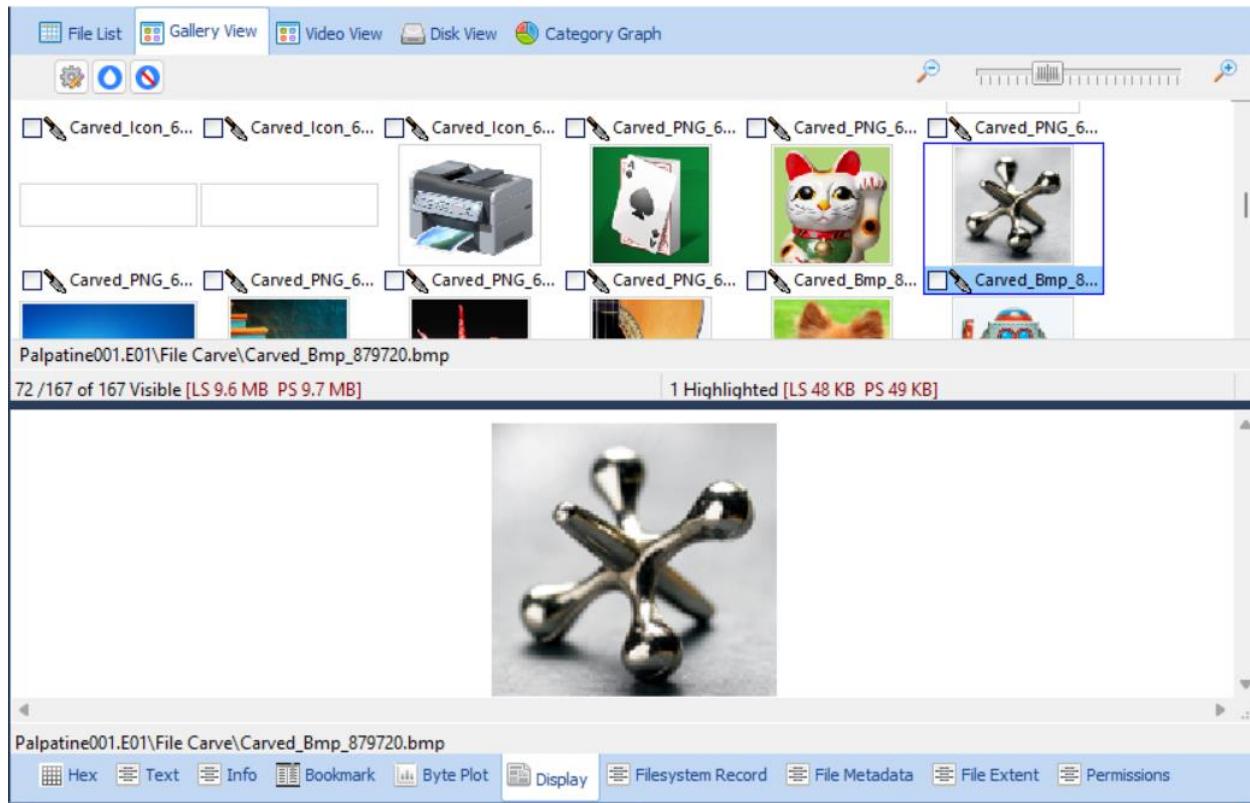
[Chancellor Palpatine] - It is gravely unfortunate that tragedies such as these are not preventable. I understand.

[Anakin Skywalker] - Does such a power exist?

[Chancellor Palpatine] - Come to my office later, I have something to tell you.

Palpatine.E01\Root\\$Recycle.Bin\S-1-5-21-346071495-2028852961-265169757-1001\\$R015Q24 (Chosen One).txt

Hex Text Info Bookmark Byte Plot Display Filesystem Record File Metadata File Extent Permissions



Registry Information

After the file analysis, I checked the Windows registry for more information. Normally, the registry contains data about users, software, computer name, and system activity. These files are usually stored in Windows\System32\config.

Unfortunately, in this case, the registry files like SAM, SYSTEM, and SOFTWARE were not found. I searched manually and also used the keyword search tool, but I couldn't locate the full registry hives. There were a few files that mentioned "SAM," but they were from other system folders and didn't give any useful information.

The reason I couldn't access the registry is most likely because the image was a logical image. Logical images don't always include protected system files, especially the ones needed for registry analysis. Because of that, I couldn't find any usernames, computer names, or system activity logs from the registry.

Conclusion

Doing this forensic project was not easy, but it was a big learning experience for me. I worked hard to follow all the right steps creating the image, verifying the hash values, opening the image in Forensic Explorer, doing keyword searches, exploring folders, and carving files. I spent a lot of time hoping to find strong proof, like a file named “Order66.txt” or something with secret plans. But most folders were empty and many files were unreadable or damaged.

I was also confused when the registry files didn’t show up, but I learned that this happens sometimes with logical images. At first, I thought I did something wrong, but later I realized that the image just didn’t include those files. That was frustrating, but it taught me to stay patient and keep trying different ways to find evidence.

This final exam helped me in using forensic tools, solving problems, and writing clear reports. Even when I was stuck or unsure, I kept going and tried my best. I now understand how careful and detailed forensic work really is.

Appendix of Terms

1. FTK Imager – A tool used to make an exact copy of digital evidence.

2. Forensic Explorer – Software that helps check files, logs, and deleted data.
3. Hash Value – A unique code that confirms a file has not changed.
4. E01 Image File – A file format that stores a full copy of a hard drive.
5. Metadata – Hidden file details like creation date and edits.
6. Registry – A system database that keeps track of settings and user activity.
7. Deleted Files Recovery – A way to bring back removed files.
8. Unallocated Space – Empty-looking space on a hard drive that may still hold deleted files.
9. Encryption – A method to lock data so only certain people can see it.
10. Forensic Imaging – Copying a device for investigation without changing anything.
11. Digital Evidence – Any electronic data that can be used as proof.
12. Confession Document – A file found that may admit wrongdoing.
13. System Logs – Records of computer activity like logins and software use.
14. External Storage Device – A USB or hard drive used to store or move files.
15. Cyber Forensics – Investigating computers and devices for evidence.

References

FTK Imager v4.1.1.1 User Manual

Forensic Explorer Help Documentation

Course Module Week 2: Sample Report