Palpatine Investigation

Ferris State University

DFOR 310

Professor Jasun Hawkins

Alexis Cherpes

May 2, 2025

Table of Contents

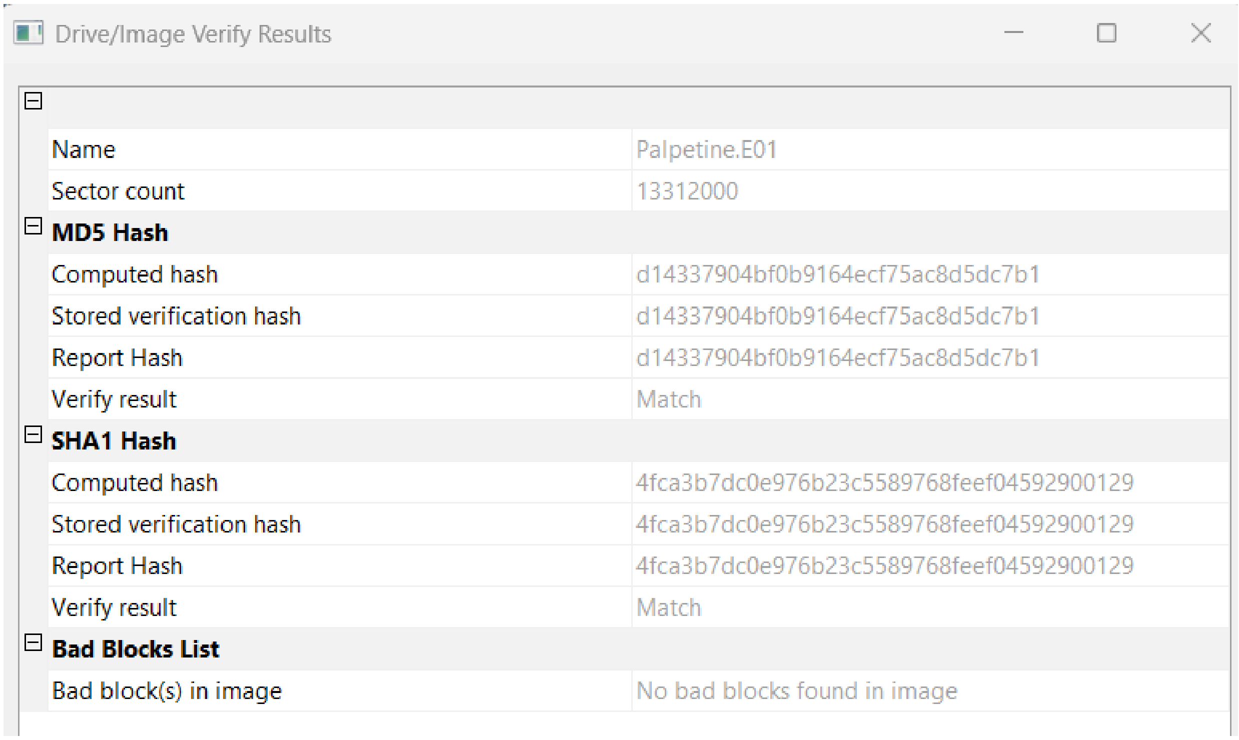
Overview

As the assigned forensic examiner, I was assigned to investigate a device that was seized from the suspected Sith Lord, Chancellor Palpatine. This report summarizes a forensic investigation in connection with allegations that Chancellor Palpatine, was involved in Sith-related activities. Tools such as FTK Imager, Forensic Explorer, and AXIOM are present in this investigation and with help from them a disk image was created and analyzed in a controlled environment.

Imaging the Hard Drive

FTK Imager

After securing the laptop from the suspect and bringing it to a secure lab, I used FTK Imager to capture an image of the file in a controlled setting to preserve the evidence integrity. I have a sterile, verified-clean hard drive that I will use to store the forensic disk image of the suspect's drive. Creating the disk image took about 5 minutes and once it was done, drive verify results, and an image summary is given. It is crucial to create a disk image to preserve the original evidence by making an exact bit-for-bit copy of the suspect's drive. Figure 1.1 shows the hashes provided for the device. Hashes are digital fingerprints of the data used to verify that the contents of a disk image have not been altered during analysis.



Drive/Image Verify Results

Name	Palpetine.E01
Sector count	13312000
MD5 Hash	
Computed hash	d14337904bf0b9164ecf75ac8d5dc7b1
Stored verification hash	d14337904bf0b9164ecf75ac8d5dc7b1
Report Hash	d14337904bf0b9164ecf75ac8d5dc7b1
Verify result	Match
SHA1 Hash	
Computed hash	4fca3b7dc0e976b23c5589768feef04592900129
Stored verification hash	4fca3b7dc0e976b23c5589768feef04592900129
Report Hash	4fca3b7dc0e976b23c5589768feef04592900129
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 1.1

Image Summary

Case Information:

Acquired using: ADI4.7.3.81

Case Number: finalpractical#002

Evidence Number: #002

Unique Description:

Examiner: Alexis Cherpes

Notes:

Information for C:\Users\acher\OneDrive\Desktop\Cases\FinalExam\palpatine:

```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Verification Hashes]
 MD5 verification hash: d14337904bf0b9164ecf75ac8d5dc7b1
 SHA1 verification hash: 4fca3b7dc0e976b23c5589768feef04592900129
[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
```

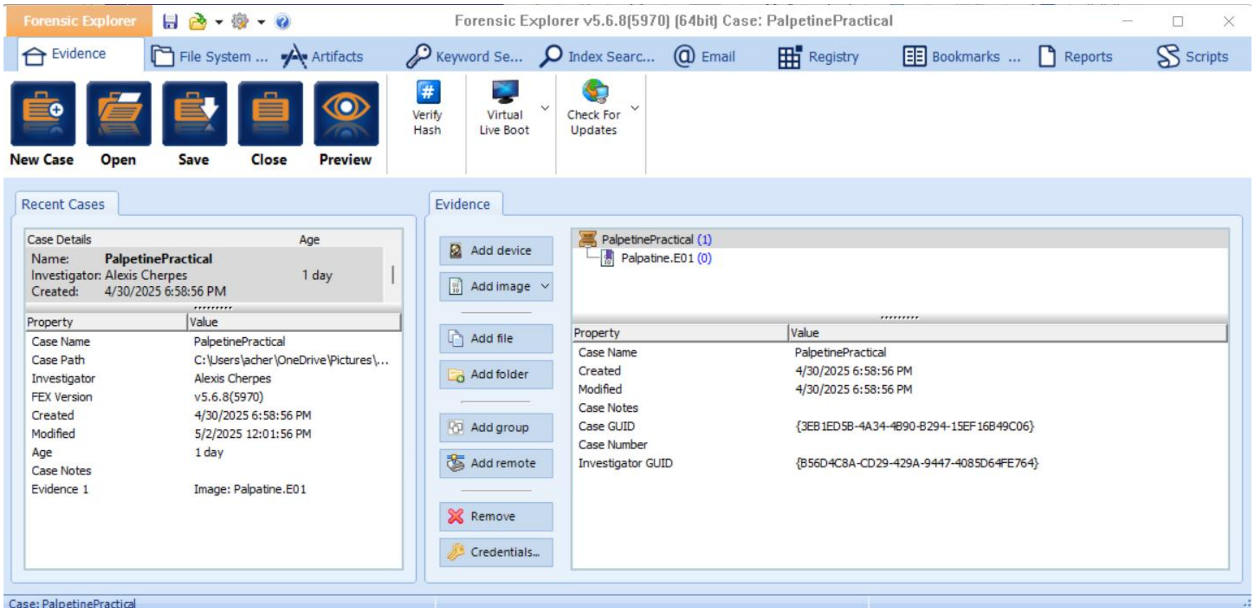
```
Image Information:
 Acquisition started:   Wed Apr 30 22:07:02 2025
 Acquisition finished:  Wed Apr 30 22:07:54 2025
 Segment list:
  C:\Users\acher\OneDrive\Desktop\Cases\FinalExam\palpatine.E01
 COMPUTED HASH :  d14337904bf0b9164ecf75ac8d5dc7b1
 COMPUTED HASH :  4fca3b7dc0e976b23c5589768feef04592900129

Image Verification Results:
 Verification started:  Wed Apr 30 22:07:54 2025
 Verification finished: Wed Apr 30 22:08:32 2025
 MD5 checksum:    d14337904bf0b9164ecf75ac8d5dc7b1 : verified
 SHA1 checksum:   4fca3b7dc0e976b23c5589768feef04592900129 : verified
```

Presentation of Evidence

Forensic Explorer

I used Forensic Explorer to analyze the disk image previously captured from the suspect's drive. This software provides a detailed examination of the items without altering the original data. After launching the program I created a new case called PalpatinePractical shown in Figure 1.2. Once the case is set up, I added the disk image by selecting the "Add Image" option and navigating to the file's location. Figure 1.3 and Figure 1.4 show the criteria I am setting for what I want to look for.



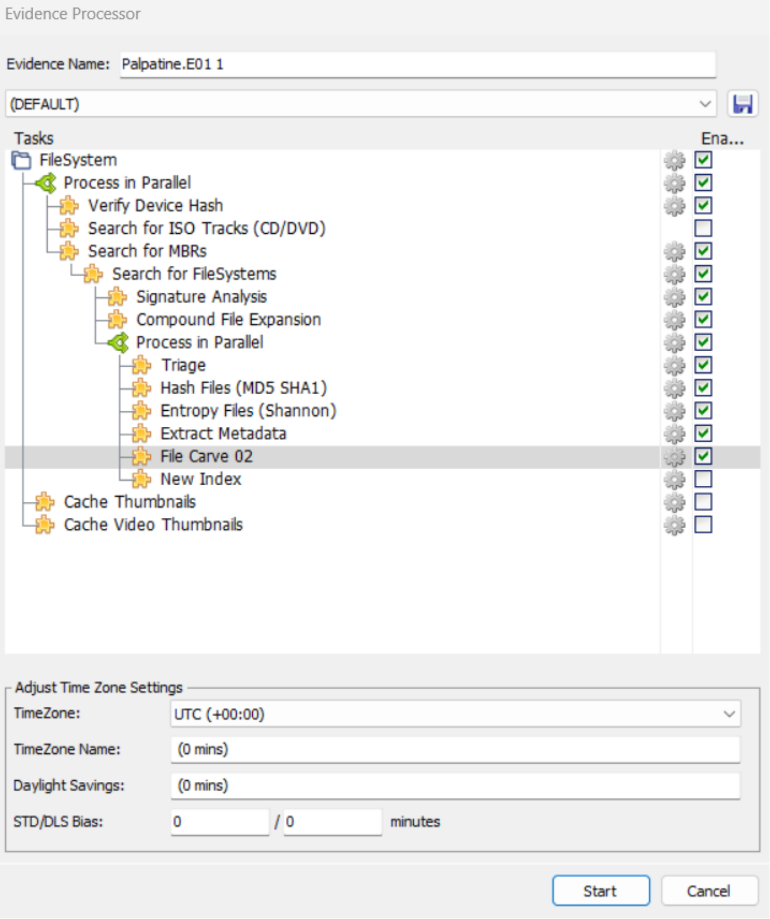
Case Details	Age
Name: **PalpetinePractical** Investigator: Alexis Cherpes Created: 4/30/2025 6:58:56 PM	1 day

Property	Value
Case Name	PalpetinePractical
Case Path	C:\Users\acher\OneDrive\Pictures\...
Investigator	Alexis Cherpes
FEX Version	v5.6.8(5970)
Created	4/30/2025 6:58:56 PM
Modified	5/2/2025 12:01:56 PM
Age	1 day
Case Notes	
Evidence 1	Image: Palpatine.E01

PalpetinePractical (1)
Palpatine.E01 (0)

Property	Value
Case Name	PalpetinePractical
Created	4/30/2025 6:58:56 PM
Modified	4/30/2025 6:58:56 PM
Case Notes	
Case GUID	{3EB1ED5B-4A34-4B90-B294-15EF16B49C06}
Case Number	
Investigator GUID	{B56D4C8A-CD29-429A-9447-4085D64FE764}

Figure 1.2



Evidence Name: Palpatine.E01 1

(DEFAULT)

```
Tasks                                  Ena...
FileSystem                               ☑
  Process in Parallel                    ☑
    Verify Device Hash                   ☑
    Search for ISO Tracks (CD/DVD)       □
    Search for MBRs                      ☑
      Search for FileSystems             ☑
        Signature Analysis               ☑
        Compound File Expansion          ☑
        Process in Parallel              ☑
          Triage                         ☑
          Hash Files (MD5 SHA1)          ☑
          Entropy Files (Shannon)        ☑
          Extract Metadata               ☑
          File Carve 02                  ☑
          New Index                      □
  Cache Thumbnails                       □
  Cache Video Thumbnails                 □
```

Adjust Time Zone Settings

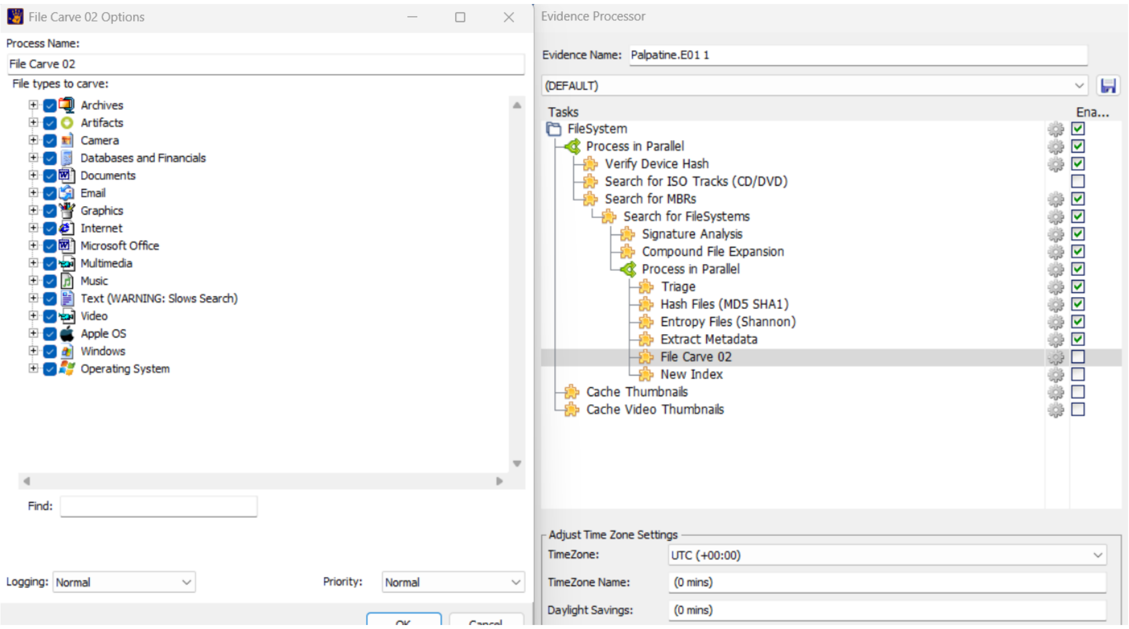
TimeZone: UTC (+00:00)

TimeZone Name: (0 mins)

Daylight Savings: (0 mins)

STD/DLS Bias: 0 / 0 minutes

Figure 1.3


File Carve 02 Options

Process Name: File Carve 02

File types to carve:

- ☑ Archives
- ☑ Artifacts
- ☑ Camera
- ☑ Databases and Financials
- ☑ Documents
- ☑ Email
- ☑ Graphics
- ☑ Internet
- ☑ Microsoft Office
- ☑ Multimedia
- ☑ Music
- ☑ Text (WARNING: Slows Search)
- ☑ Video
- ☑ Apple OS
- ☑ Windows
- ☑ Operating System

Find:

Logging: Normal   Priority: Normal

Evidence Processor

Evidence Name: Palpatine.E01 1

(DEFAULT)

Tasks	Ena...
FileSystem	☑
Process in Parallel	☑
Verify Device Hash	☑
Search for ISO Tracks (CD/DVD)	□
Search for MBRs	☑
Search for FileSystems	☑
Signature Analysis	☑
Compound File Expansion	☑
Process in Parallel	☑
Triage	☑
Hash Files (MD5 SHA1)	☑
Entropy Files (Shannon)	☑
Extract Metadata	☑
File Carve 02	□
New Index	□
Cache Thumbnails	□
Cache Video Thumbnails	□

Adjust Time Zone Settings

TimeZone: UTC (+00:00)

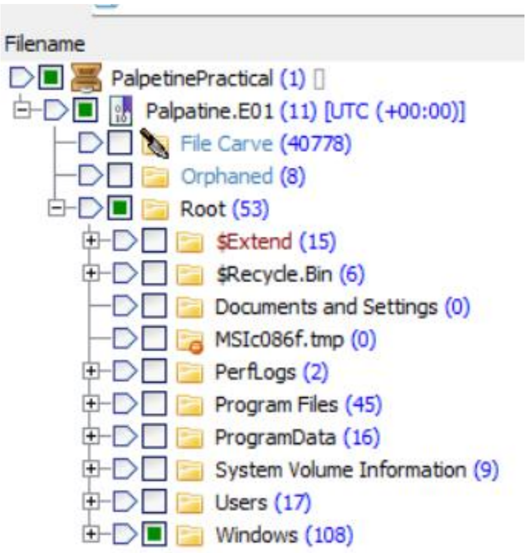
TimeZone Name: (0 mins)

Daylight Savings: (0 mins)

Figure 1.4

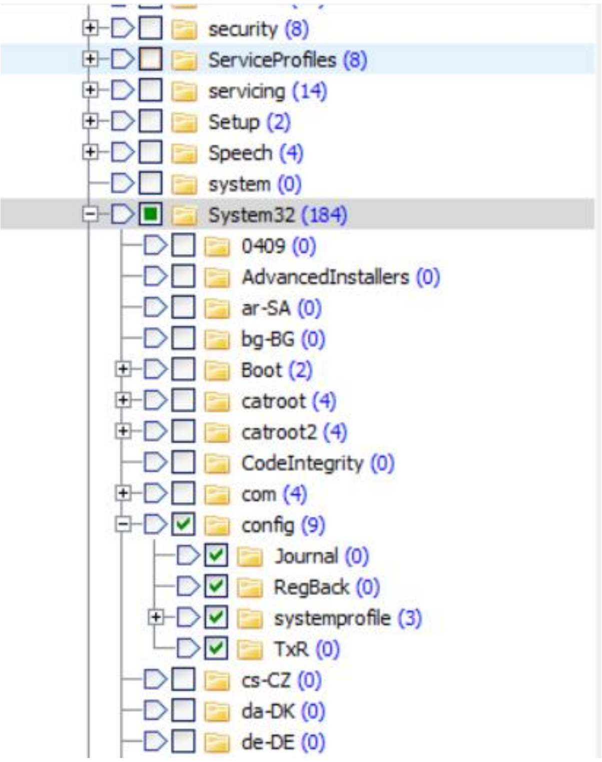
Registry

The windows registry is a critical source of information in forensic investigations and is found exclusively on Windows operating systems. It stores configuration settings, user activity, and system information. The registry hives that I was looking for were SAM, System, Software, and NTuser.dat because these contain data relating to user accounts, system configuration, installed programs, and user-specific activity. *Figure 1.5 and 1.6* show the path to where the registry would be. Going from the image to the Root folder, to the Windows folder, down to Systems32, and then into config. However, in this case, no registry hives were present in the image, meaning either they were deleted, the system was incomplete, or this is not a Windows operating system. The reason we would want to look at the Security Accounts Manager (SAM), is because it contains the user names and the passwords on this machine. The System hive contains detailed configuration data about the operating system such as the computer name. The Software hive provides valuable information about the system including the default user name, the operating systems installation date, and a list of installed applications. The last hive is NTuser.dat and this contains valuable information about user activity.



```
Filename
PalpetinePractical (1)
  Palpatine.E01 (11) [UTC (+00:00)]
    File Carve (40778)
    Orphaned (8)
    Root (53)
      $Extend (15)
      $Recycle.Bin (6)
      Documents and Settings (0)
      MSIc086f.tmp (0)
      PerfLogs (2)
      Program Files (45)
      ProgramData (16)
      System Volume Information (9)
      Users (17)
      Windows (108)
```

Figure 1.5



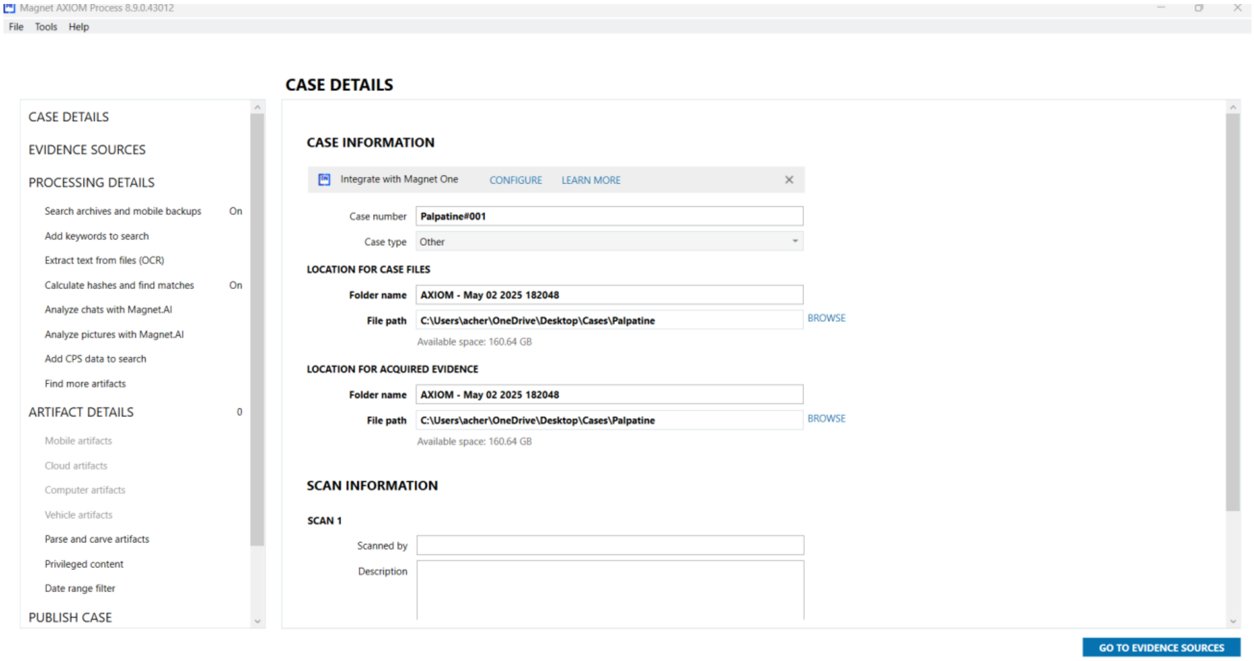
```
security (8)
ServiceProfiles (8)
servicing (14)
Setup (2)
Speech (4)
system (0)
System32 (184)
  0409 (0)
  AdvancedInstallers (0)
  ar-SA (0)
  bg-BG (0)
  Boot (2)
  catroot (4)
  catroot2 (4)
  CodeIntegrity (0)
  com (4)
  config (9)
    Journal (0)
    RegBack (0)
    systemprofile (3)
    TxR (0)
  cs-CZ (0)
  da-DK (0)
  de-DE (0)
```

Figure 1.6

Active File Review

Axiom

The following software I used is AXIOM. Figures 1.7-2.4 show how I went about making a new case for this investigation.



CASE DETAILS

CASE INFORMATION

Case number: Palpatine#001

Case type: Other

LOCATION FOR CASE FILES

Folder name: AXIOM - May 02 2025 182048

File path: C:\Users\acher\OneDrive\Desktop\Cases\Palpatine

Available space: 160.64 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name: AXIOM - May 02 2025 182048

File path: C:\Users\acher\OneDrive\Desktop\Cases\Palpatine

Available space: 160.64 GB

SCAN INFORMATION

SCAN 1

Scanned by

Description

Figure 1.7 – Label the case and create a folder for this case to go into

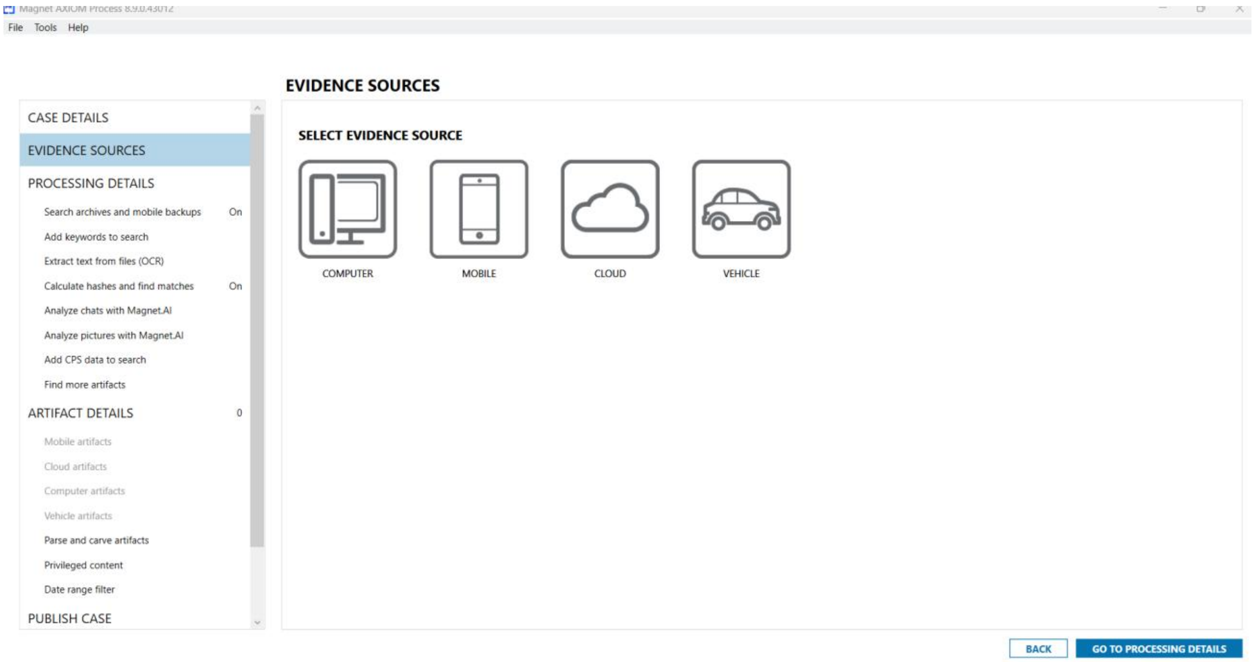


Figure 1.8 – Select "Computer"

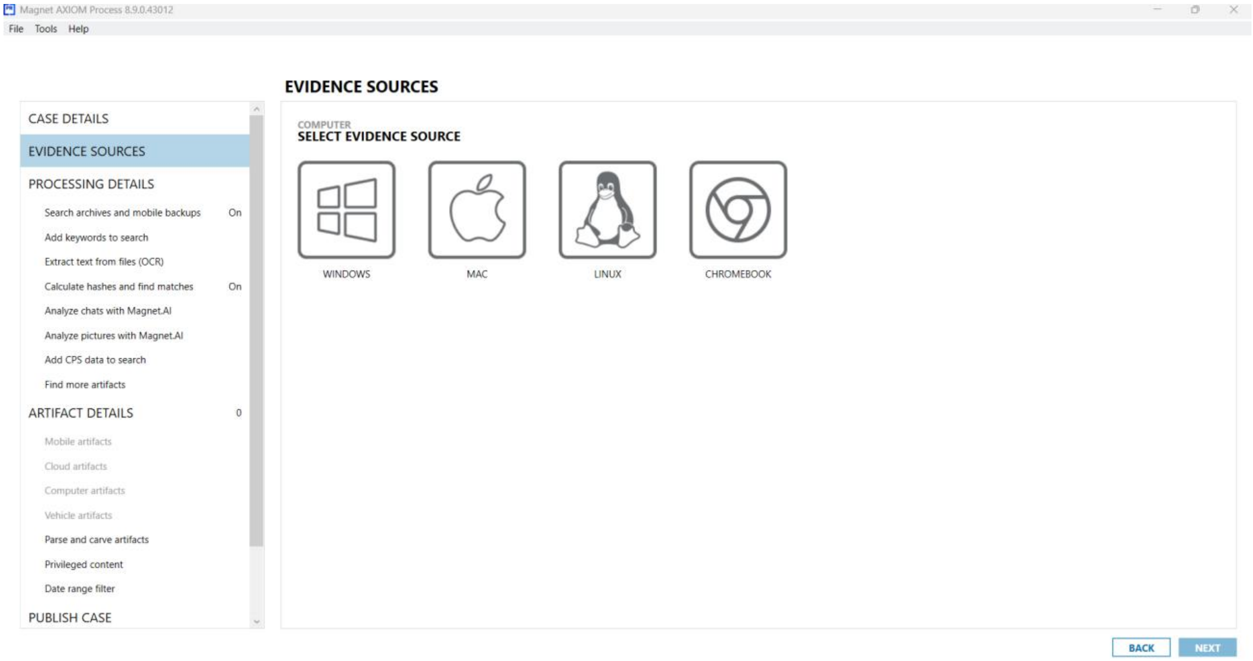


Figure 1.9 – Select "Windows"

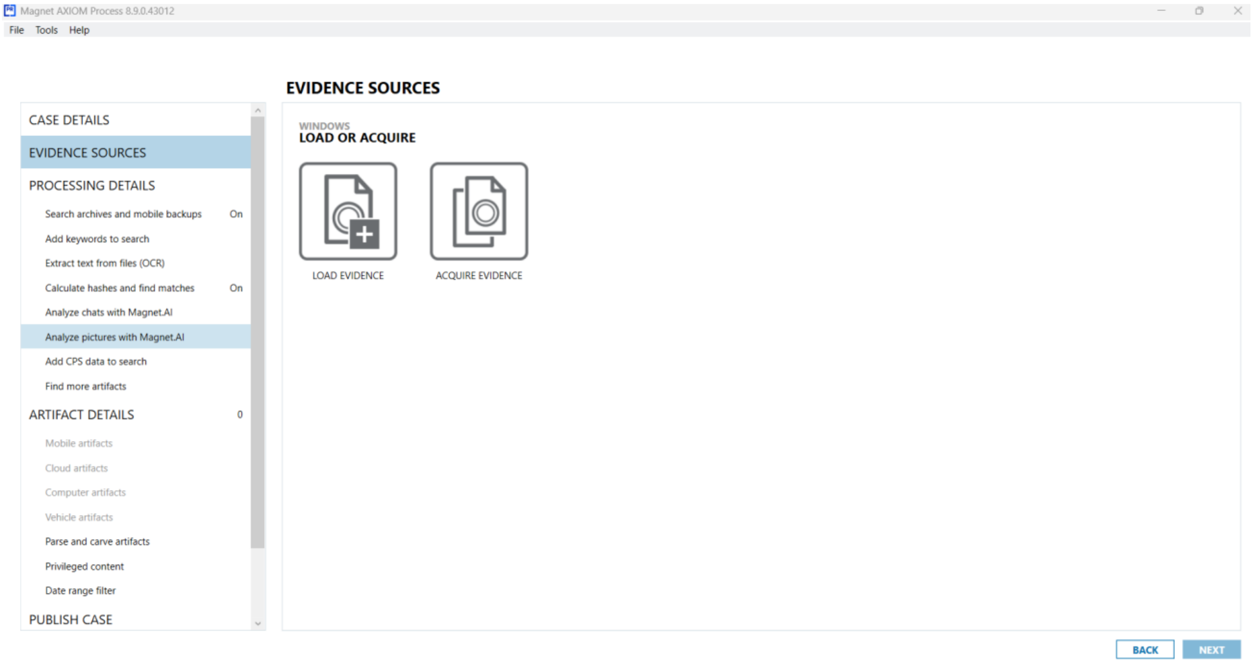
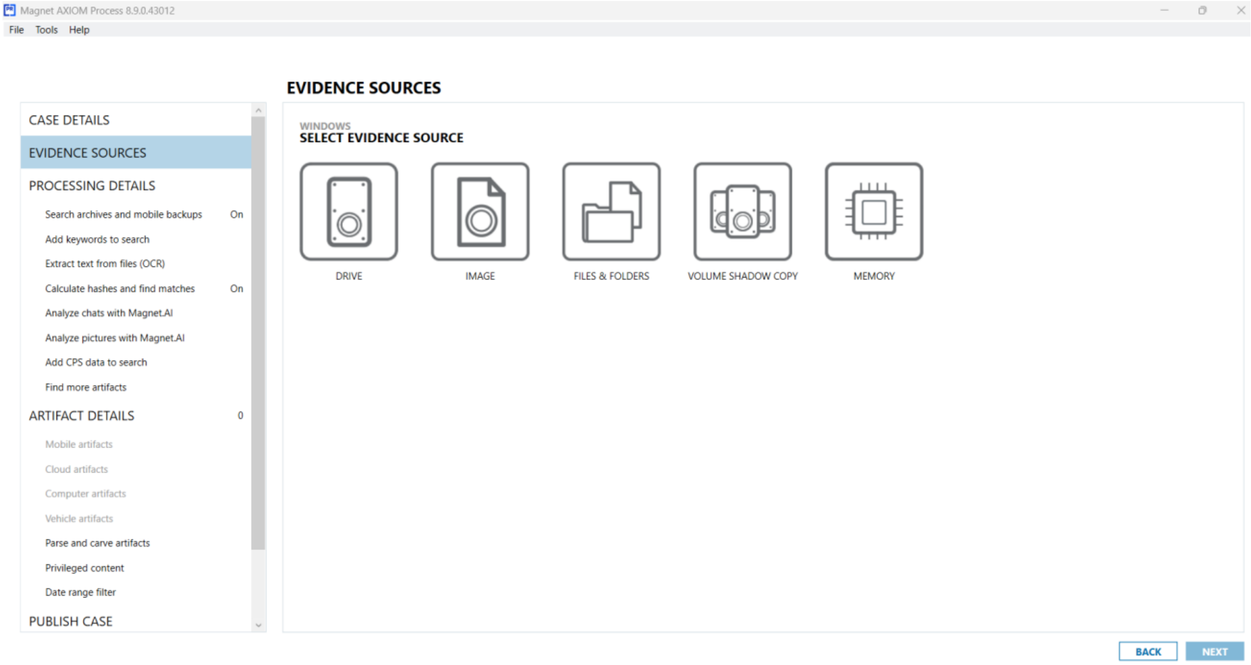


Figure 2.0 – Select "Load Evidence"



EVIDENCE SOURCES

CASE DETAILS

EVIDENCE SOURCES

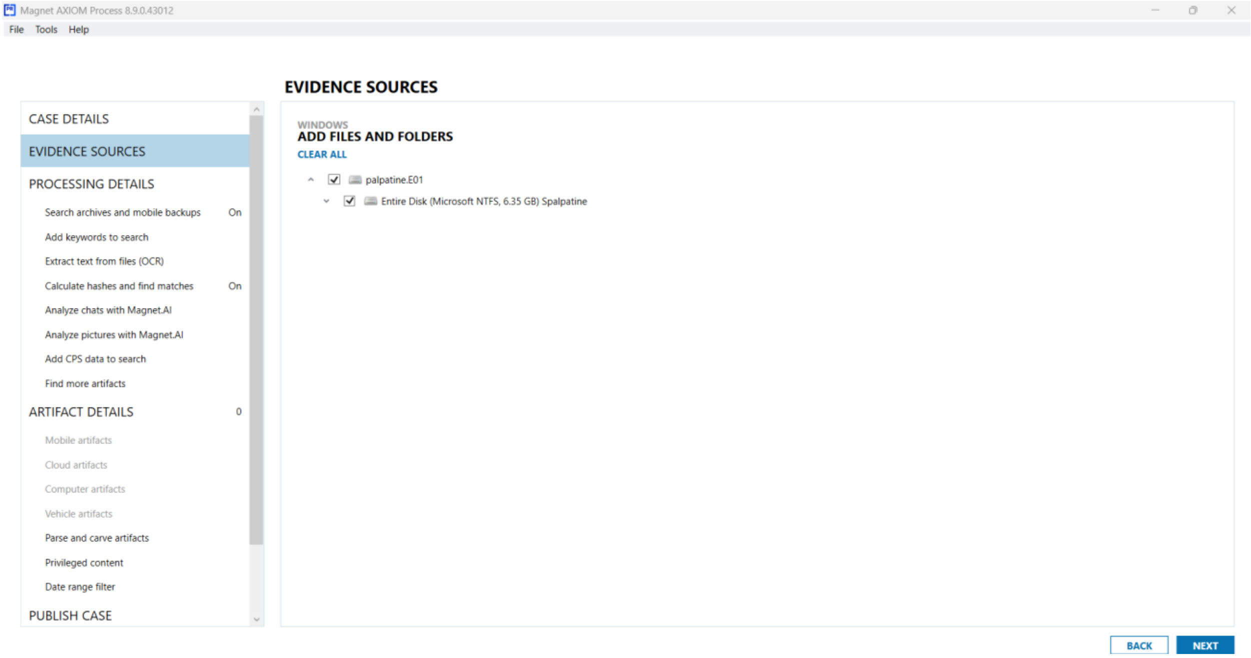
PROCESSING DETAILS

Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hashes and find matches	On
Analyze chats with Magnet.AI	
Analyze pictures with Magnet.AI	
Add CPS data to search	
Find more artifacts	
ARTIFACT DETAILS	0
Mobile artifacts	
Cloud artifacts	
Computer artifacts	
Vehicle artifacts	
Parse and carve artifacts	
Privileged content	
Date range filter	

PUBLISH CASE

WINDOWS
SELECT EVIDENCE SOURCE

Figure 2.1 – Select "Image"



EVIDENCE SOURCES

CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

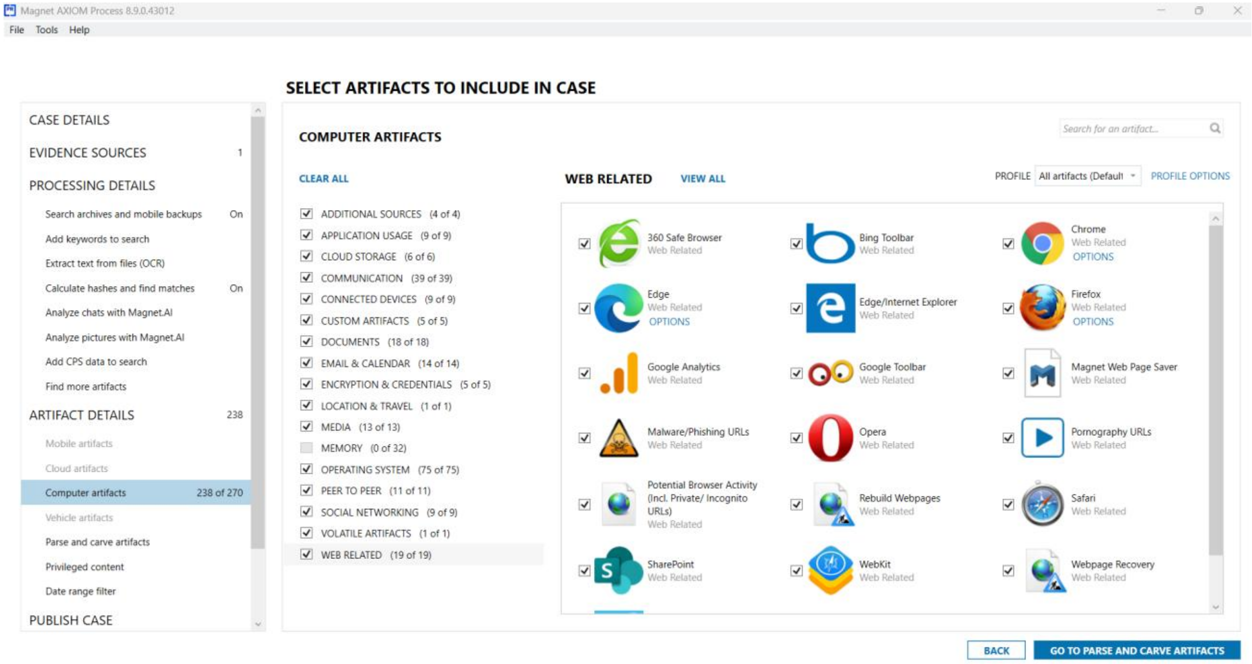
Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hashes and find matches	On
Analyze chats with Magnet.AI	
Analyze pictures with Magnet.AI	
Add CPS data to search	
Find more artifacts	
ARTIFACT DETAILS	0
Mobile artifacts	
Cloud artifacts	
Computer artifacts	
Vehicle artifacts	
Parse and carve artifacts	
Privileged content	
Date range filter	

PUBLISH CASE

WINDOWS
ADD FILES AND FOLDERS

☑ palpatine.E01
☑ Entire Disk (Microsoft NTFS, 6.35 GB) Spalpatine

Figure 2.2 – Select the file



Magnet AXIOM Process 8.9.0.43012

File Tools Help

SELECT ARTIFACTS TO INCLUDE IN CASE

CASE DETAILS	
EVIDENCE SOURCES	1
PROCESSING DETAILS	
Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hashes and find matches	On
Analyze chats with Magnet.AI	
Analyze pictures with Magnet.AI	
Add CPS data to search	
Find more artifacts	
ARTIFACT DETAILS	238
Mobile artifacts	
Cloud artifacts	
Computer artifacts	238 of 270
Vehicle artifacts	
Parse and carve artifacts	
Privileged content	
Date range filter	
PUBLISH CASE	

COMPUTER ARTIFACTS

CLEAR ALL

- ☑ ADDITIONAL SOURCES (4 of 4)
- ☑ APPLICATION USAGE (9 of 9)
- ☑ CLOUD STORAGE (6 of 6)
- ☑ COMMUNICATION (39 of 39)
- ☑ CONNECTED DEVICES (9 of 9)
- ☑ CUSTOM ARTIFACTS (5 of 5)
- ☑ DOCUMENTS (18 of 18)
- ☑ EMAIL & CALENDAR (14 of 14)
- ☑ ENCRYPTION & CREDENTIALS (5 of 5)
- ☑ LOCATION & TRAVEL (1 of 1)
- ☑ MEDIA (13 of 13)
- □ MEMORY (0 of 32)
- ☑ OPERATING SYSTEM (75 of 75)
- ☑ PEER TO PEER (11 of 11)
- ☑ SOCIAL NETWORKING (9 of 9)
- ☑ VOLATILE ARTIFACTS (1 of 1)
- ☑ WEB RELATED (19 of 19)

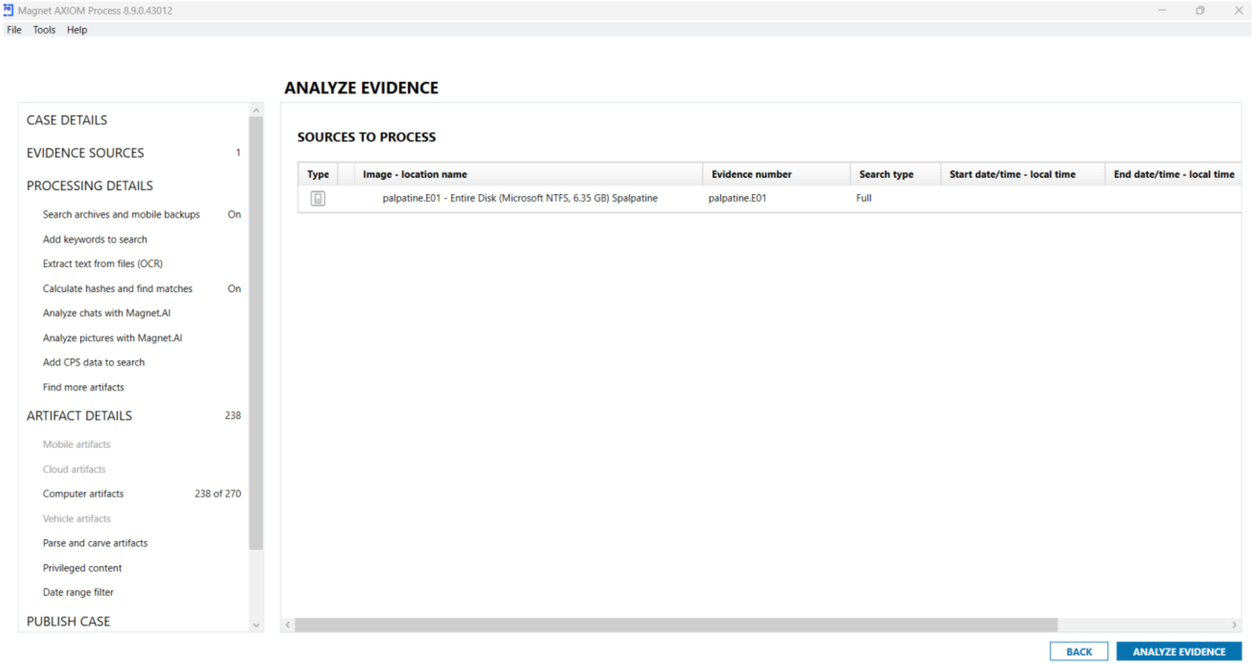
WEB RELATED VIEW ALL

Search for an artifact...

PROFILE All artifacts (Default PROFILE OPTIONS

☑ 360 Safe Browser Web Related	☑ Bing Toolbar Web Related	☑ Chrome Web Related OPTIONS
☑ Edge Web Related OPTIONS	☑ Edge/Internet Explorer Web Related	☑ Firefox Web Related OPTIONS
☑ Google Analytics Web Related	☑ Google Toolbar Web Related	☑ Magnet Web Page Saver Web Related
☑ Malware/Phishing URLs Web Related	☑ Opera Web Related	☑ Pornography URLs Web Related
☑ Potential Browser Activity (Incl. Private/ Incognito URLs) Web Related	☑ Rebuild Webpages Web Related	☑ Safari Web Related
☑ SharePoint Web Related	☑ WebKit Web Related	☑ Webpage Recovery Web Related

Figure 2.3 – Select the defaults up until "Computer Artifacts", then select all the options



Magnet AXIOM Process 8.9.0.43012

File Tools Help

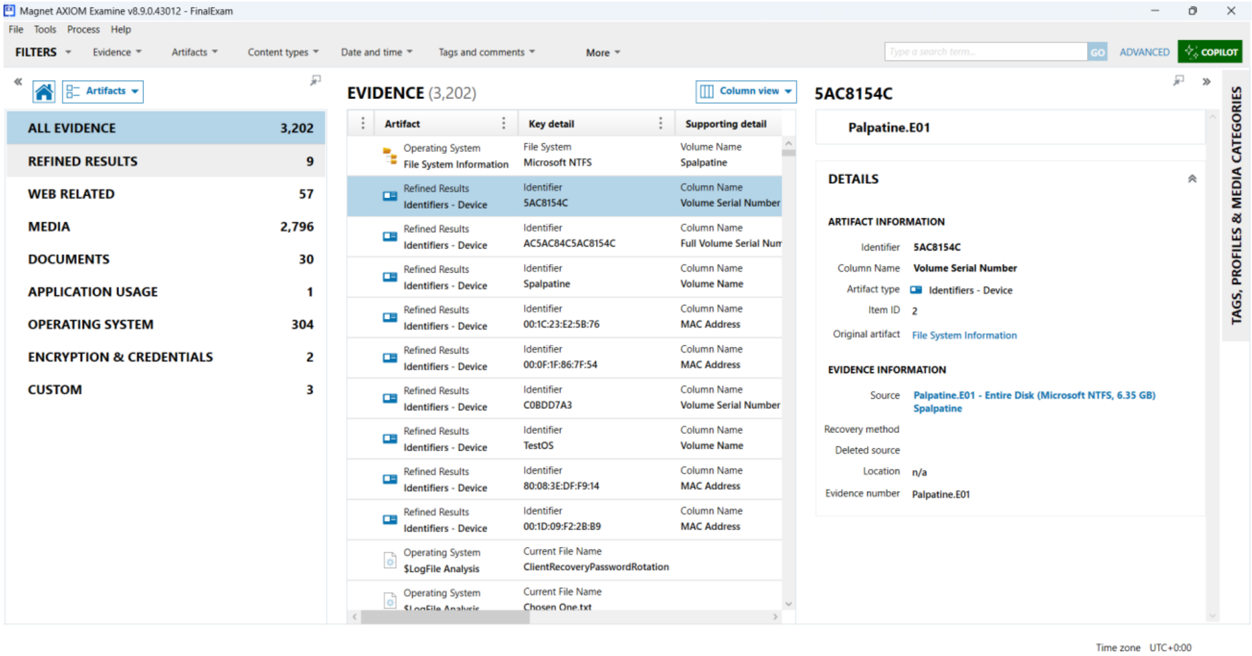
ANALYZE EVIDENCE

CASE DETAILS	
EVIDENCE SOURCES	1
PROCESSING DETAILS	
Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hashes and find matches	On
Analyze chats with Magnet.AI	
Analyze pictures with Magnet.AI	
Add CPS data to search	
Find more artifacts	
ARTIFACT DETAILS	238
Mobile artifacts	
Cloud artifacts	
Computer artifacts	238 of 270
Vehicle artifacts	
Parse and carve artifacts	
Privileged content	
Date range filter	
PUBLISH CASE	

SOURCES TO PROCESS

Type	Image - location name	Evidence number	Search type	Start date/time - local time	End date/time - local time
	palpatine.E01 - Entire Disk (Microsoft NTFS, 6.35 GB) Spalpatine	palpatine.E01	Full		

Figure 2.4 – Select all the defaults until "Analyze Evidence", then analyze the evidence



ALL EVIDENCE	3,202
REFINED RESULTS	9
WEB RELATED	57
MEDIA	2,796
DOCUMENTS	30
APPLICATION USAGE	1
OPERATING SYSTEM	304
ENCRYPTION & CREDENTIALS	2
CUSTOM	3

EVIDENCE (3,202)

Artifact	Key detail	Supporting detail
Operating System File System Information	File System Microsoft NTFS	Volume Name Spalpatine
Refined Results Identifiers - Device	Identifier 5AC8154C	Column Name Volume Serial Number
Refined Results Identifiers - Device	Identifier AC5AC84C5AC8154C	Column Name Full Volume Serial Num
Refined Results Identifiers - Device	Identifier Spalpatine	Column Name Volume Name
Refined Results Identifiers - Device	Identifier 00:1C:23:E2:5B:76	Column Name MAC Address
Refined Results Identifiers - Device	Identifier 00:0F:1F:86:7F:54	Column Name MAC Address
Refined Results Identifiers - Device	Identifier C0BDD7A3	Column Name Volume Serial Number
Refined Results Identifiers - Device	Identifier TestOS	Column Name Volume Name
Refined Results Identifiers - Device	Identifier 80:08:3E:DF:F9:14	Column Name MAC Address
Refined Results Identifiers - Device	Identifier 00:1D:09:F2:2B:B9	Column Name MAC Address
Operating System $LogFile Analysis	Current File Name ClientRecoveryPasswordRotation	
Operating System $LogFile Analysis	Current File Name Chosen One.txt	

5AC8154C

Palpatine.E01

DETAILS

ARTIFACT INFORMATION

Identifier	5AC8154C
Column Name	Volume Serial Number
Artifact type	Identifiers - Device
Item ID	2
Original artifact	File System Information

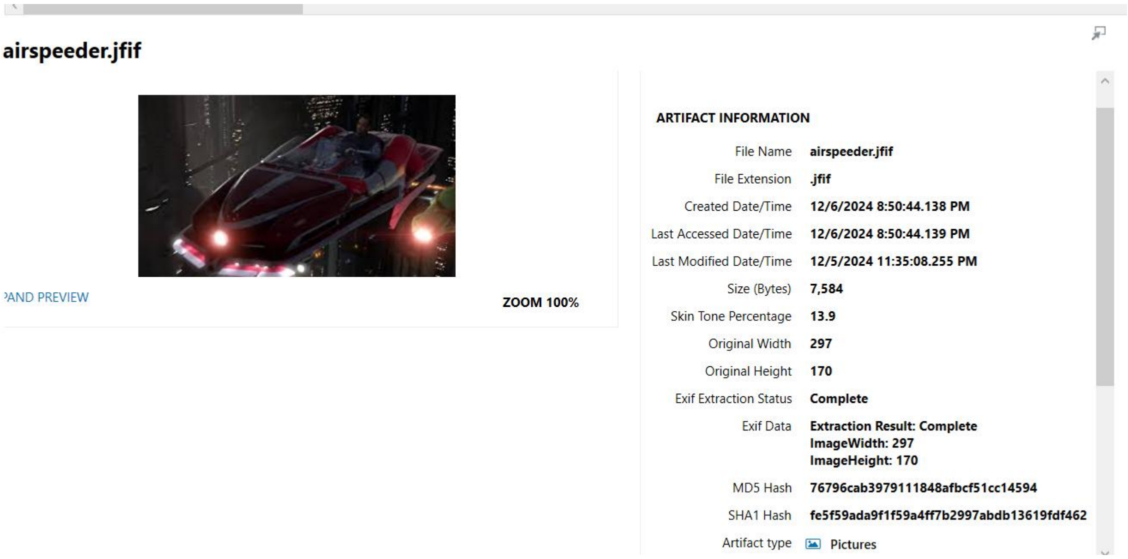
EVIDENCE INFORMATION

Source	Palpatine.E01 - Entire Disk (Microsoft NTFS, 6.35 GB) Spalpatine
Recovery method	
Deleted source	
Location	n/a
Evidence number	Palpatine.E01

Figure 2.5 – Analyzed Evidence

Media

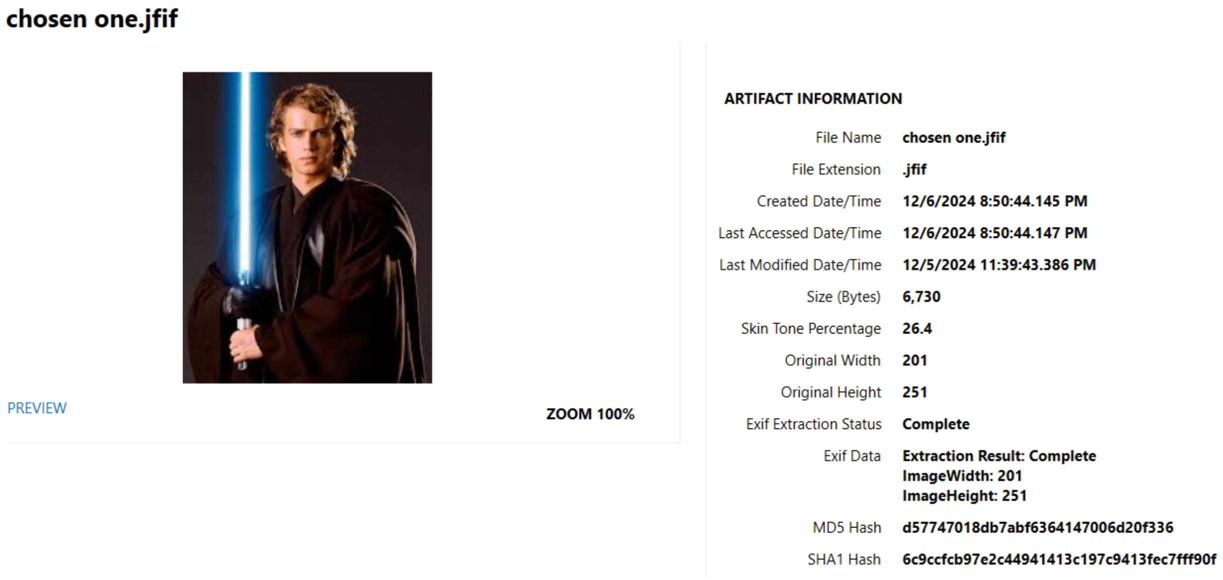
Figures 2.6 - 4.5 are pictures that were found in the media folder relating to Emperor Palpatine's activities, including propaganda materials, visual documentation of known enemies and persons of interest, and imagery referencing strategic plans.



ARTIFACT INFORMATION

File Name	airspeeder.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.138 PM
Last Accessed Date/Time	12/6/2024 8:50:44.139 PM
Last Modified Date/Time	12/5/2024 11:35:08.255 PM
Size (Bytes)	7,584
Skin Tone Percentage	13.9
Original Width	297
Original Height	170
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 297 ImageHeight: 170
MD5 Hash	76796cab3979111848afbcf51cc14594
SHA1 Hash	fe5f59ada9f1f59a4ff7b2997abdb13619fdf462
Artifact type	Pictures

Figure 2.6 – Air speeder

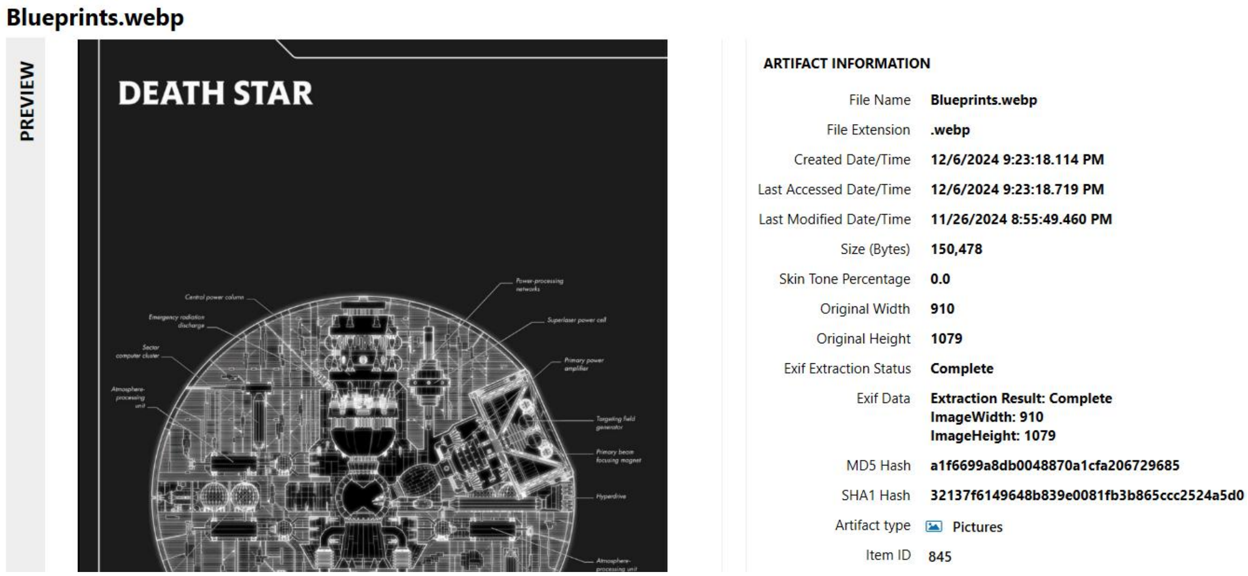


chosen one.jfif

ARTIFACT INFORMATION

File Name	**chosen one.jfif**
File Extension	**.jfif**
Created Date/Time	**12/6/2024 8:50:44.145 PM**
Last Accessed Date/Time	**12/6/2024 8:50:44.147 PM**
Last Modified Date/Time	**12/5/2024 11:39:43.386 PM**
Size (Bytes)	**6,730**
Skin Tone Percentage	**26.4**
Original Width	**201**
Original Height	**251**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 201** **ImageHeight: 251**
MD5 Hash	**d57747018db7abf6364147006d20f336**
SHA1 Hash	**6c9ccfcb97e2c44941413c197c9413fec7fff90f**

Figure 2.7 – Picture of Anakin Skywalker labeled "Chosen One"

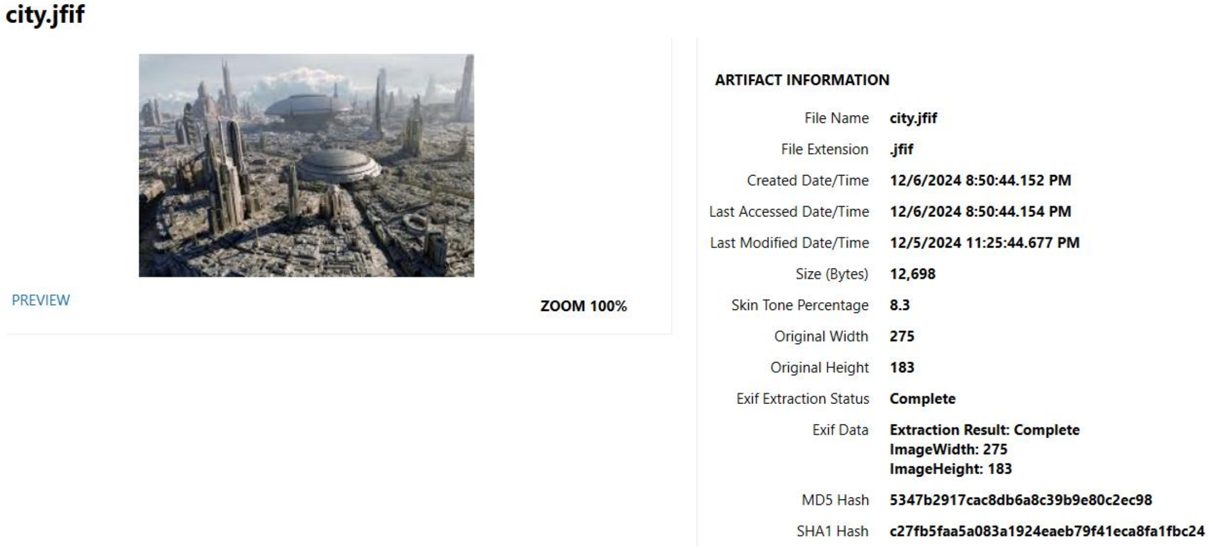

PREVIEW
DEATH STAR
Central power column
Emergency radiation discharge
Sector computer cluster
Atmosphere-processing unit
Power-processing networks
Superlaser power cell
Primary power amplifier
Targeting field generator
Primary beam focusing magnet
Hyperdrive
Atmosphere-processing unit

Blueprints.webp

ARTIFACT INFORMATION

File Name	**Blueprints.webp**
File Extension	**.webp**
Created Date/Time	**12/6/2024 9:23:18.114 PM**
Last Accessed Date/Time	**12/6/2024 9:23:18.719 PM**
Last Modified Date/Time	**11/26/2024 8:55:49.460 PM**
Size (Bytes)	**150,478**
Skin Tone Percentage	**0.0**
Original Width	**910**
Original Height	**1079**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 910** **ImageHeight: 1079**
MD5 Hash	**a1f6699a8db0048870a1cfa206729685**
SHA1 Hash	**32137f6149648b839e0081fb3b865ccc2524a5d0**
Artifact type	Pictures
Item ID	845

Figure 2.8 – Blueprints of the Death Star

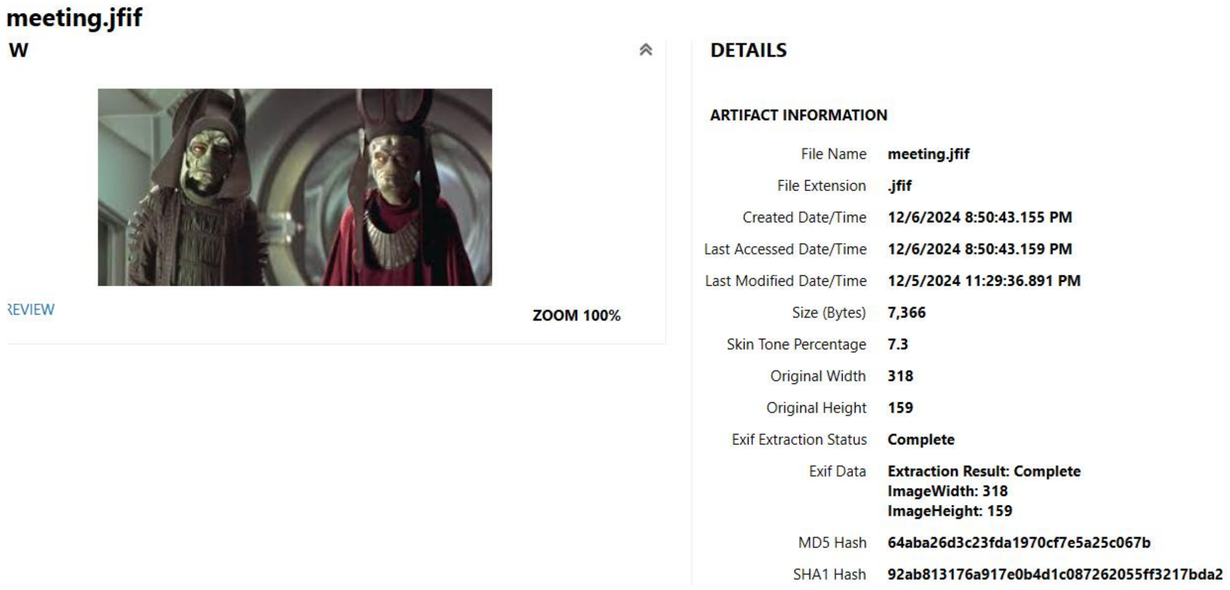


city.jfif

ARTIFACT INFORMATION

File Name	city.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.152 PM
Last Accessed Date/Time	12/6/2024 8:50:44.154 PM
Last Modified Date/Time	12/5/2024 11:25:44.677 PM
Size (Bytes)	12,698
Skin Tone Percentage	8.3
Original Width	275
Original Height	183
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 275 ImageHeight: 183
MD5 Hash	5347b2917cac8db6a8c39b9e80c2ec98
SHA1 Hash	c27fb5faa5a083a1924eaeb79f41eca8fa1fbc24

Figure 2.9 – City



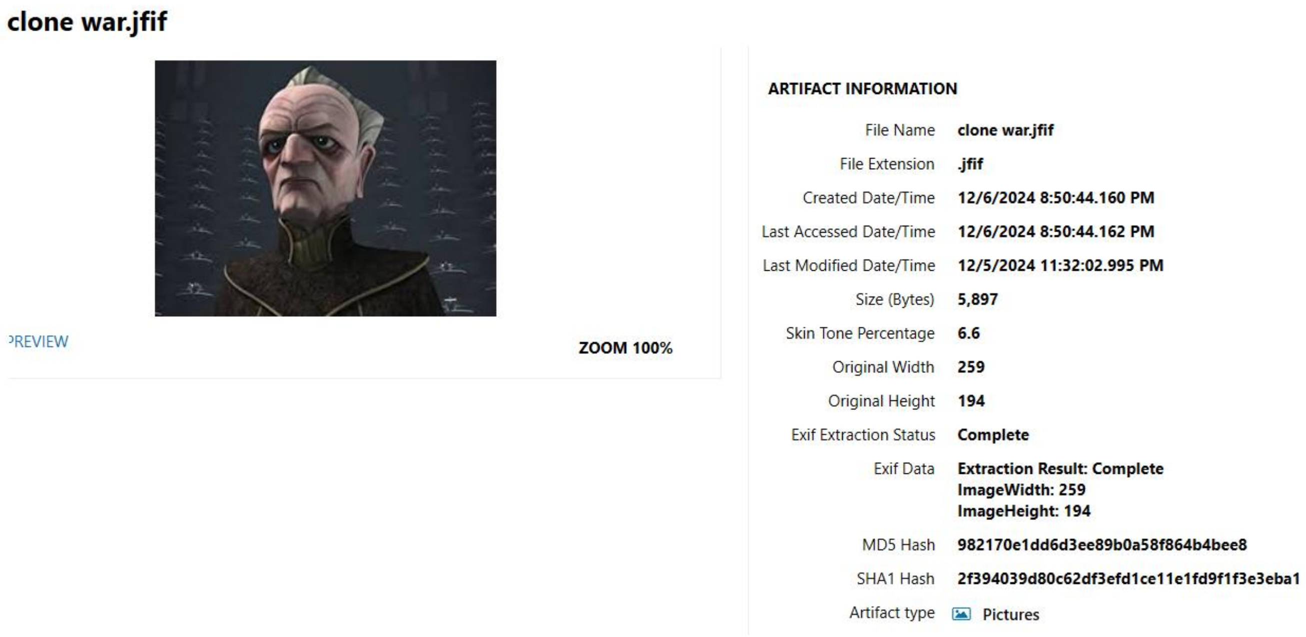
meeting.jfif

DETAILS

ARTIFACT INFORMATION

File Name	meeting.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:43.155 PM
Last Accessed Date/Time	12/6/2024 8:50:43.159 PM
Last Modified Date/Time	12/5/2024 11:29:36.891 PM
Size (Bytes)	7,366
Skin Tone Percentage	7.3
Original Width	318
Original Height	159
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 318 ImageHeight: 159
MD5 Hash	64aba26d3c23fda1970cf7e5a25c067b
SHA1 Hash	92ab813176a917e0b4d1c087262055ff3217bda2

Figure 3.0 – Meeting with Lott Dod

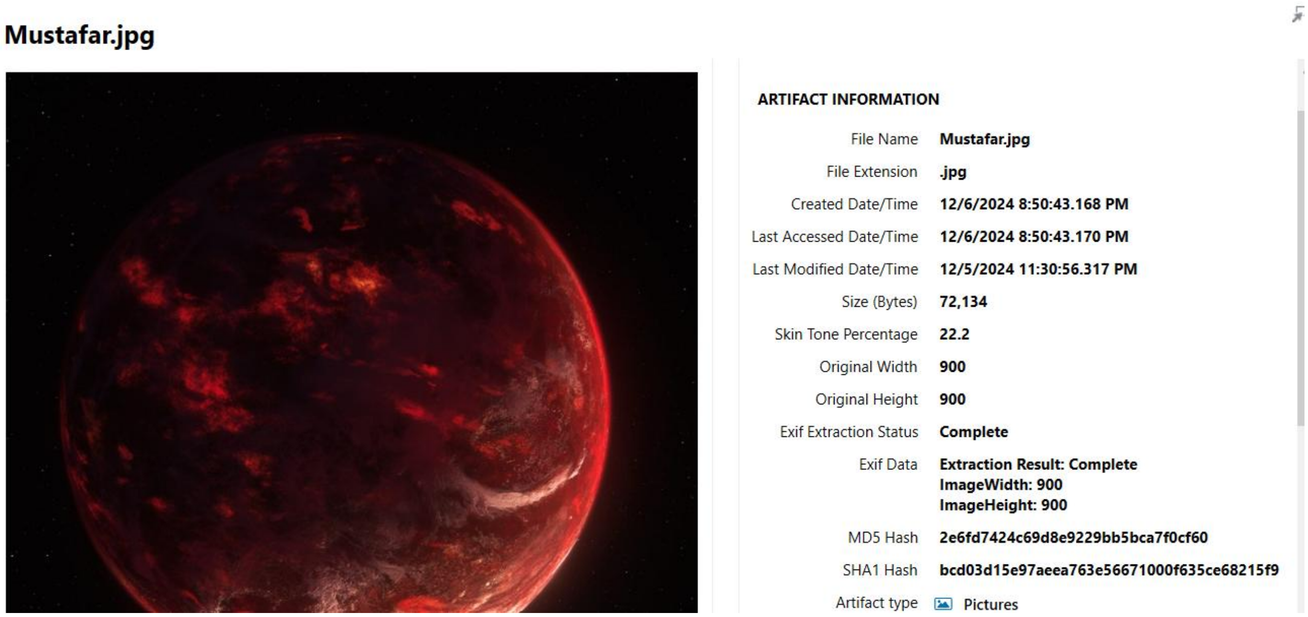


clone war.jfif

ARTIFACT INFORMATION

File Name	clone war.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.160 PM
Last Accessed Date/Time	12/6/2024 8:50:44.162 PM
Last Modified Date/Time	12/5/2024 11:32:02.995 PM
Size (Bytes)	5,897
Skin Tone Percentage	6.6
Original Width	259
Original Height	194
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 259 ImageHeight: 194
MD5 Hash	982170e1dd6d3ee89b0a58f864b4bee8
SHA1 Hash	2f394039d80c62df3efd1ce11e1fd9f1f3e3eba1
Artifact type	Pictures

Figure 3.1 – A picture of the Chancellor labeled "Clone War"

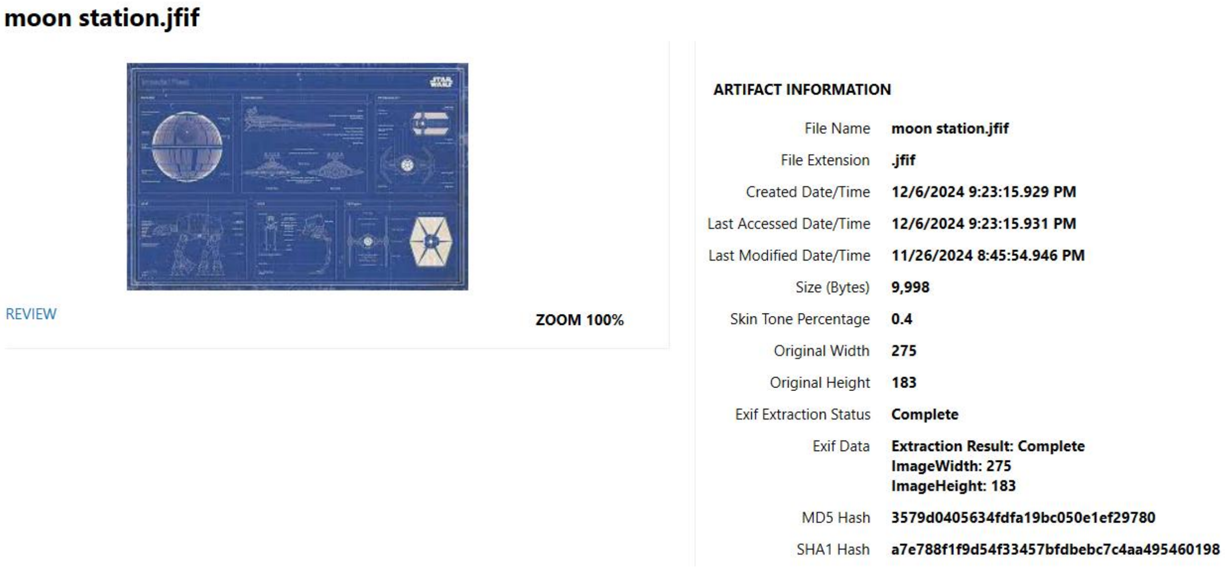


Mustafar.jpg

ARTIFACT INFORMATION

File Name	Mustafar.jpg
File Extension	.jpg
Created Date/Time	12/6/2024 8:50:43.168 PM
Last Accessed Date/Time	12/6/2024 8:50:43.170 PM
Last Modified Date/Time	12/5/2024 11:30:56.317 PM
Size (Bytes)	72,134
Skin Tone Percentage	22.2
Original Width	900
Original Height	900
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 900 ImageHeight: 900
MD5 Hash	2e6fd7424c69d8e9229bb5bca7f0cf60
SHA1 Hash	bcd03d15e97aeea763e56671000f635ce68215f9
Artifact type	Pictures

Figure 3.2 – Planet Mustafar

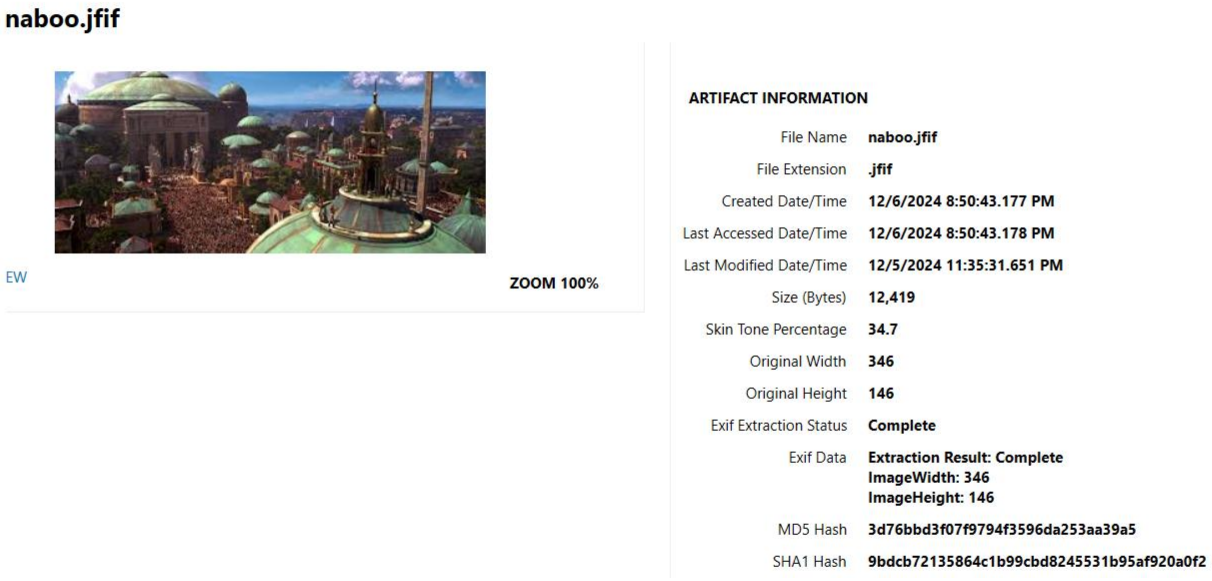


moon station.jfif

ARTIFACT INFORMATION

File Name	moon station.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 9:23:15.929 PM
Last Accessed Date/Time	12/6/2024 9:23:15.931 PM
Last Modified Date/Time	11/26/2024 8:45:54.946 PM
Size (Bytes)	9,998
Skin Tone Percentage	0.4
Original Width	275
Original Height	183
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 275 ImageHeight: 183
MD5 Hash	3579d0405634fdfa19bc050e1ef29780
SHA1 Hash	a7e788f1f9d54f33457bfdbebc7c4aa495460198

Figure 3.3 – Moon station blueprints

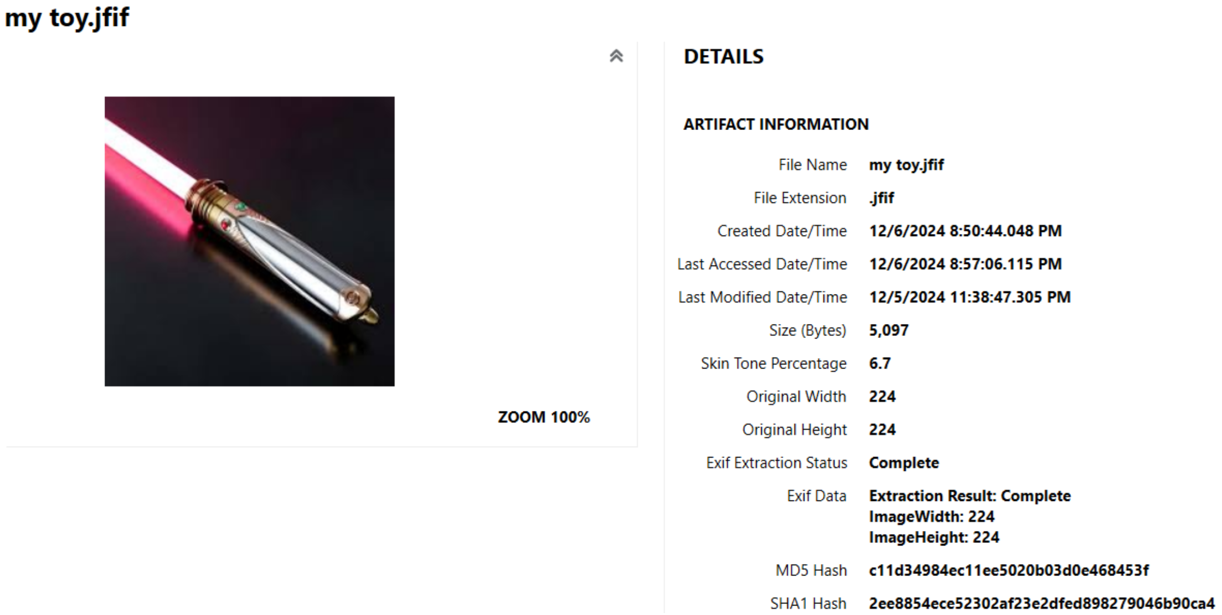


naboo.jfif

ARTIFACT INFORMATION

File Name	naboo.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:43.177 PM
Last Accessed Date/Time	12/6/2024 8:50:43.178 PM
Last Modified Date/Time	12/5/2024 11:35:31.651 PM
Size (Bytes)	12,419
Skin Tone Percentage	34.7
Original Width	346
Original Height	146
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 346 ImageHeight: 146
MD5 Hash	3d76bbd3f07f9794f3596da253aa39a5
SHA1 Hash	9bdcb72135864c1b99cbd8245531b95af920a0f2

Figure 3.4 – Planet Naboo, home to Princess Amidala



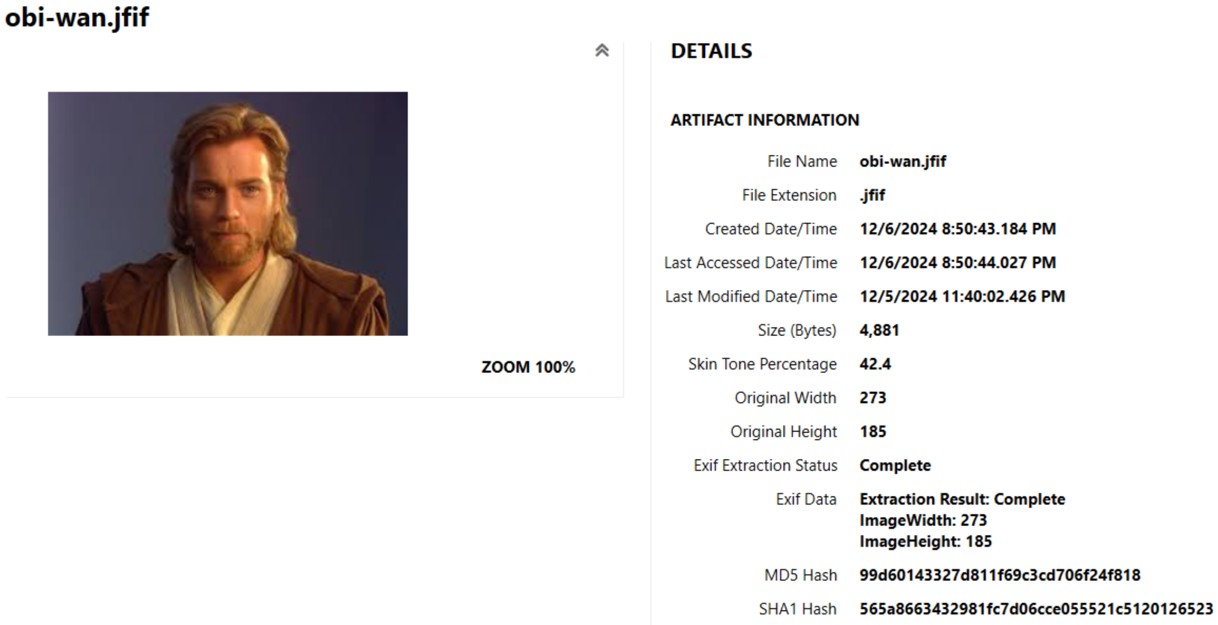
my toy.jfif

DETAILS

ARTIFACT INFORMATION

File Name	**my toy.jfif**
File Extension	**.jfif**
Created Date/Time	**12/6/2024 8:50:44.048 PM**
Last Accessed Date/Time	**12/6/2024 8:57:06.115 PM**
Last Modified Date/Time	**12/5/2024 11:38:47.305 PM**
Size (Bytes)	**5,097**
Skin Tone Percentage	**6.7**
Original Width	**224**
Original Height	**224**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 224** **ImageHeight: 224**
MD5 Hash	**c11d34984ec11ee5020b03d0e468453f**
SHA1 Hash	**2ee8854ece52302af23e2dfed898279046b90ca4**

Figure 3.5 – A picture of a lightsaber labeled "My Toy"



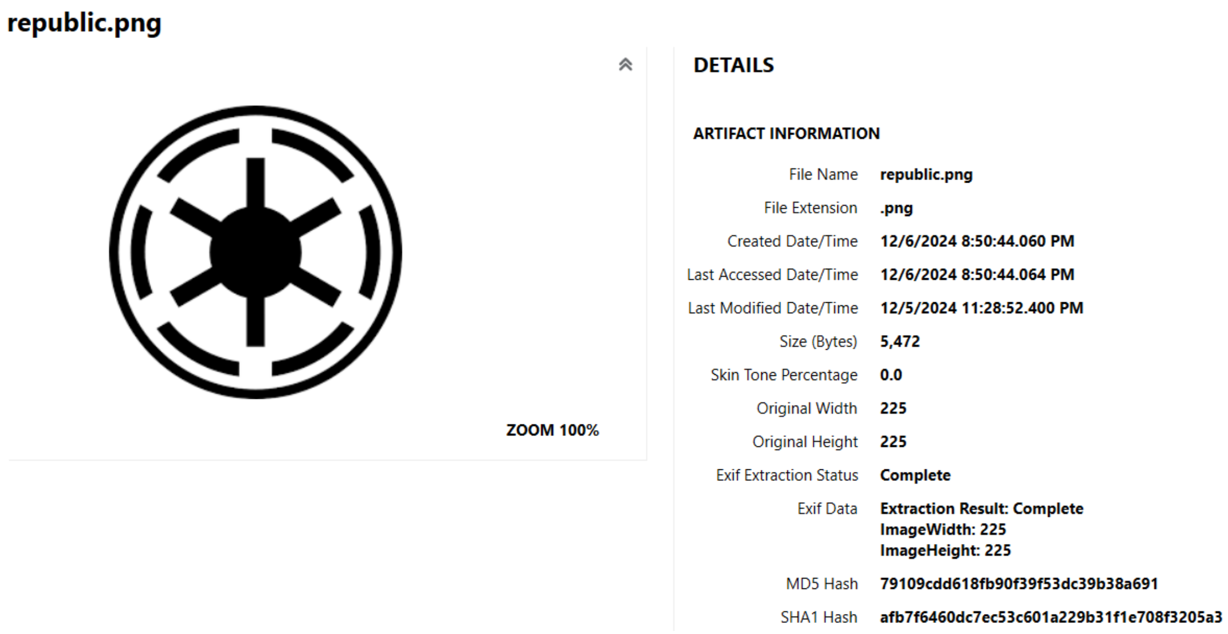
obi-wan.jfif

DETAILS

ARTIFACT INFORMATION

File Name	**obi-wan.jfif**
File Extension	**.jfif**
Created Date/Time	**12/6/2024 8:50:43.184 PM**
Last Accessed Date/Time	**12/6/2024 8:50:44.027 PM**
Last Modified Date/Time	**12/5/2024 11:40:02.426 PM**
Size (Bytes)	**4,881**
Skin Tone Percentage	**42.4**
Original Width	**273**
Original Height	**185**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 273** **ImageHeight: 185**
MD5 Hash	**99d60143327d811f69c3cd706f24f818**
SHA1 Hash	**565a8663432981fc7d06cce055521c5120126523**

Figure 3.6 – Picture of Obi-Wan Kenobi



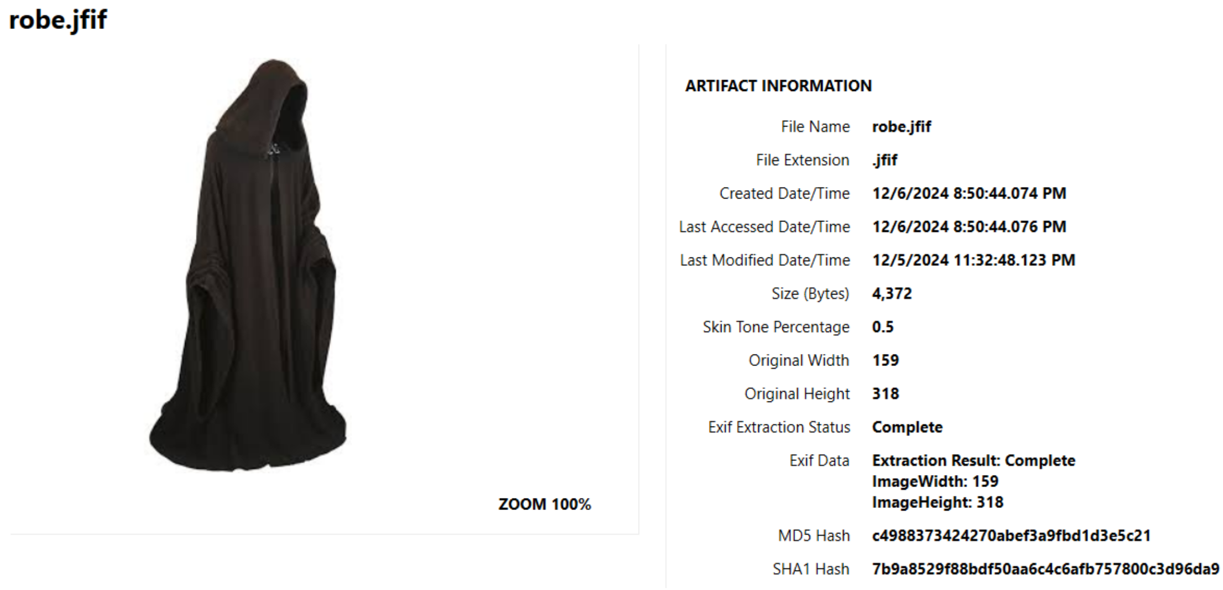
republic.png

DETAILS

ARTIFACT INFORMATION

File Name	republic.png
File Extension	.png
Created Date/Time	12/6/2024 8:50:44.060 PM
Last Accessed Date/Time	12/6/2024 8:50:44.064 PM
Last Modified Date/Time	12/5/2024 11:28:52.400 PM
Size (Bytes)	5,472
Skin Tone Percentage	0.0
Original Width	225
Original Height	225
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 225 ImageHeight: 225
MD5 Hash	79109cdd618fb90f39f53dc39b38a691
SHA1 Hash	afb7f6460dc7ec53c601a229b31f1e708f3205a3

Figure 3.7 – Picture of the republic sign

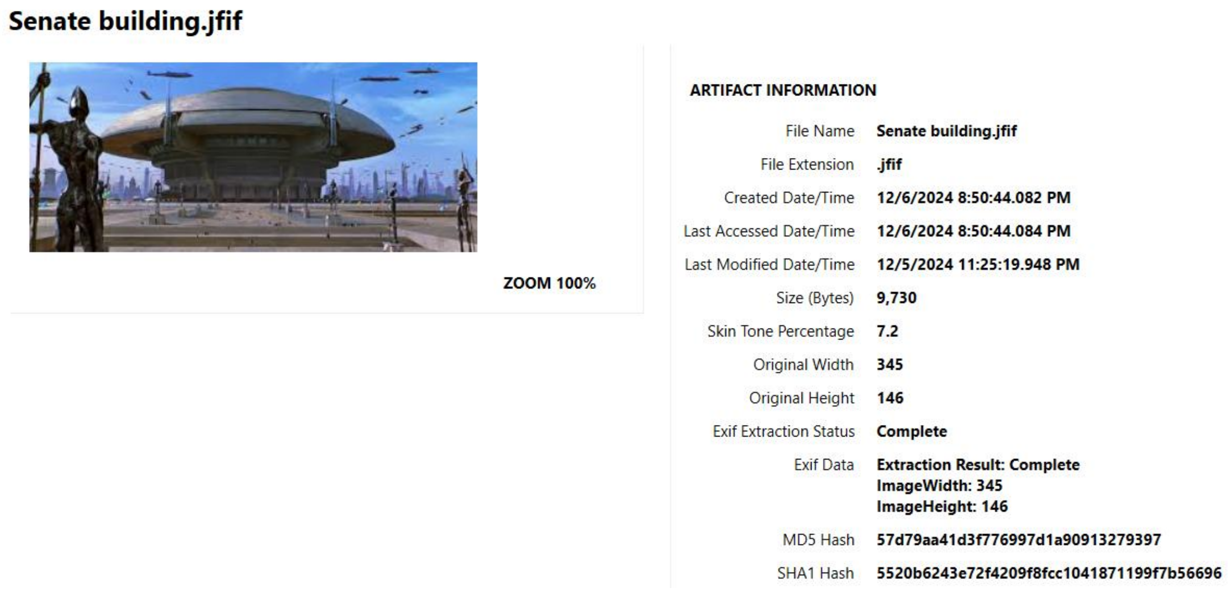


robe.jfif

ARTIFACT INFORMATION

File Name	robe.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.074 PM
Last Accessed Date/Time	12/6/2024 8:50:44.076 PM
Last Modified Date/Time	12/5/2024 11:32:48.123 PM
Size (Bytes)	4,372
Skin Tone Percentage	0.5
Original Width	159
Original Height	318
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 159 ImageHeight: 318
MD5 Hash	c4988373424270abef3a9fbd1d3e5c21
SHA1 Hash	7b9a8529f88bdf50aa6c4c6afb757800c3d96da9

Figure 3.8 – Jedi Robe

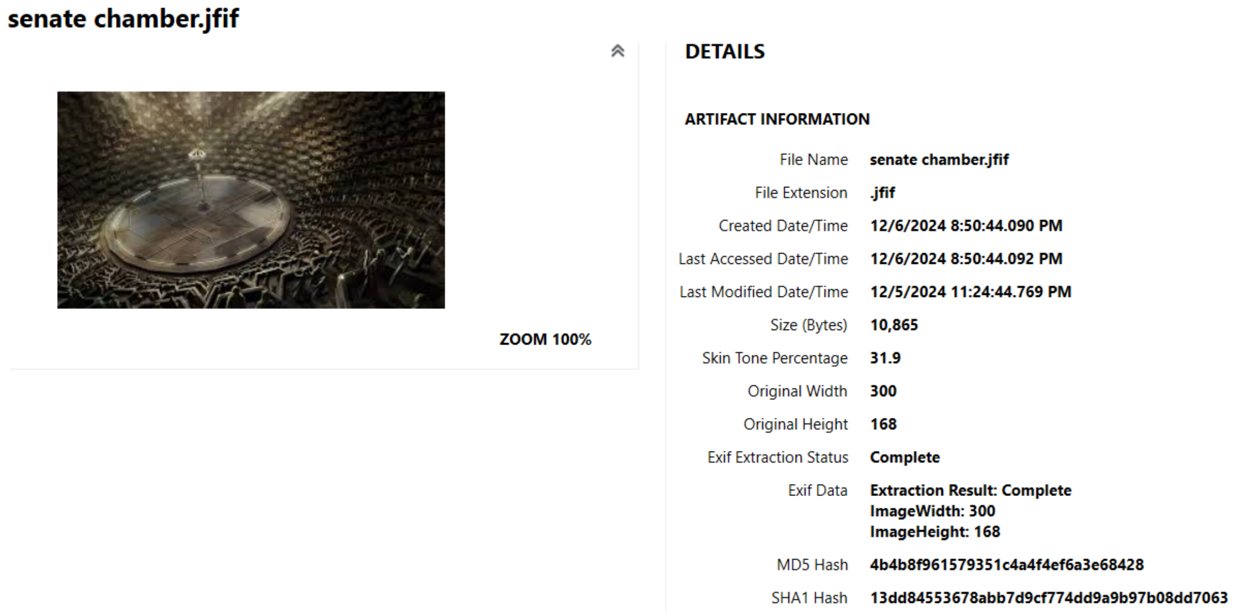


Senate building.jfif

ARTIFACT INFORMATION

File Name	Senate building.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.082 PM
Last Accessed Date/Time	12/6/2024 8:50:44.084 PM
Last Modified Date/Time	12/5/2024 11:25:19.948 PM
Size (Bytes)	9,730
Skin Tone Percentage	7.2
Original Width	345
Original Height	146
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 345 ImageHeight: 146
MD5 Hash	57d79aa41d3f776997d1a90913279397
SHA1 Hash	5520b6243e72f4209f8fcc1041871199f7b56696

Figure 3.9 – Senate Building



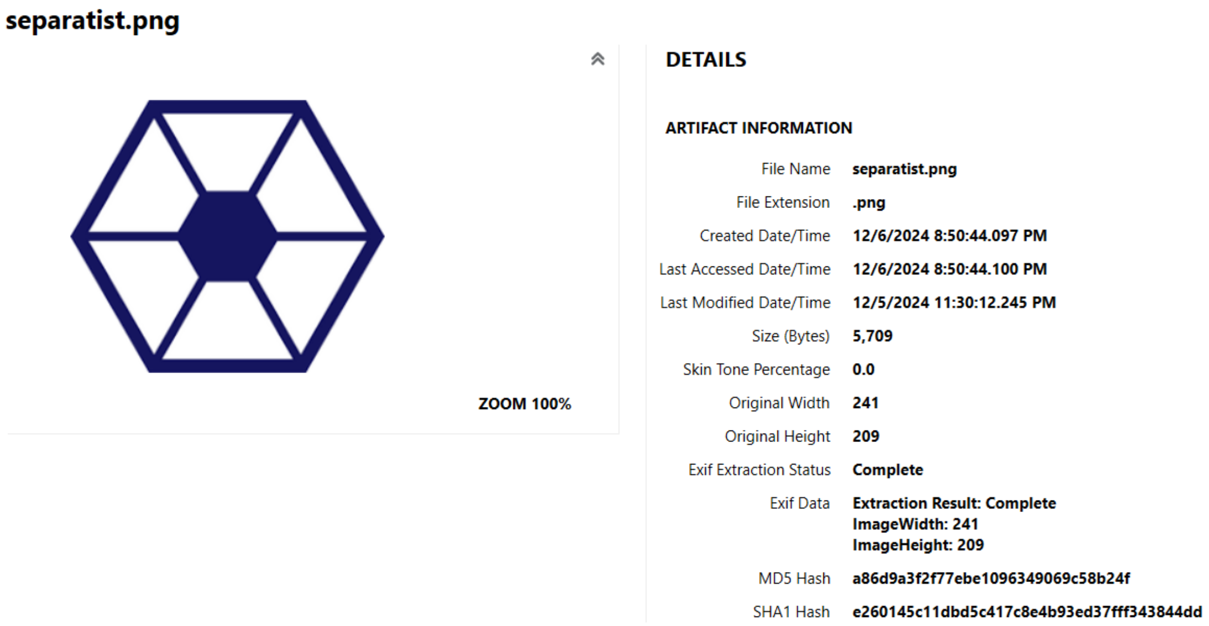
senate chamber.jfif

DETAILS

ARTIFACT INFORMATION

File Name	senate chamber.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.090 PM
Last Accessed Date/Time	12/6/2024 8:50:44.092 PM
Last Modified Date/Time	12/5/2024 11:24:44.769 PM
Size (Bytes)	10,865
Skin Tone Percentage	31.9
Original Width	300
Original Height	168
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 300 ImageHeight: 168
MD5 Hash	4b4b8f961579351c4a4f4ef6a3e68428
SHA1 Hash	13dd84553678abb7d9cf774dd9a9b97b08dd7063

Figure 4.0 – Senate Chamber



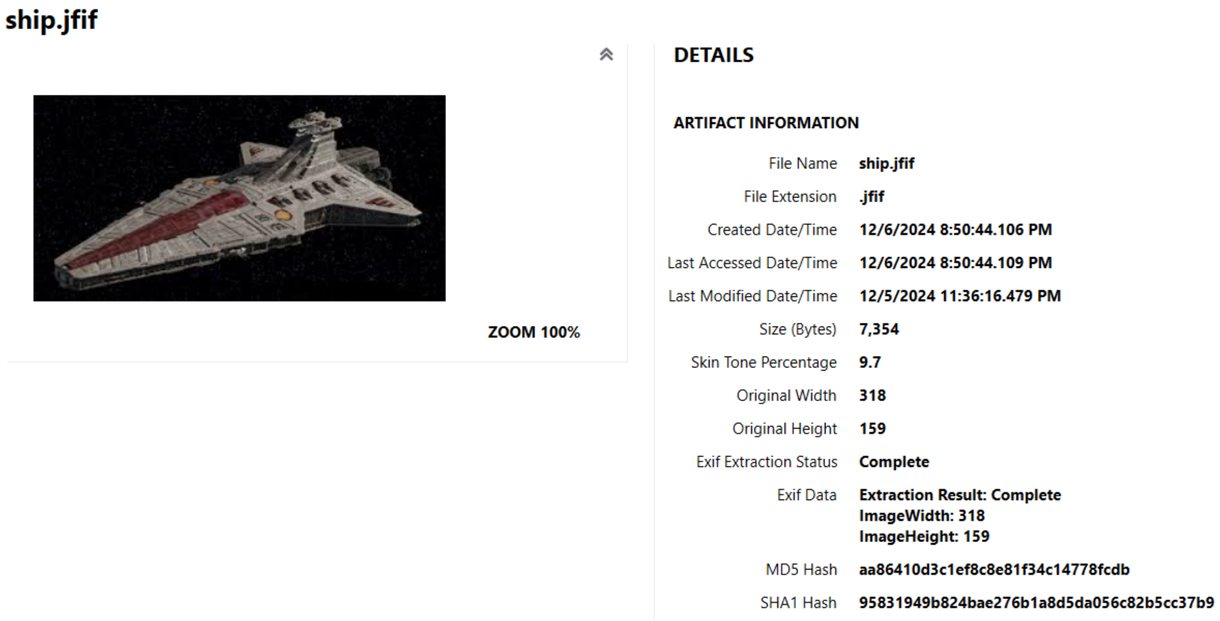
separatist.png

DETAILS

ARTIFACT INFORMATION

File Name	separatist.png
File Extension	.png
Created Date/Time	12/6/2024 8:50:44.097 PM
Last Accessed Date/Time	12/6/2024 8:50:44.100 PM
Last Modified Date/Time	12/5/2024 11:30:12.245 PM
Size (Bytes)	5,709
Skin Tone Percentage	0.0
Original Width	241
Original Height	209
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 241 ImageHeight: 209
MD5 Hash	a86d9a3f2f77ebe1096349069c58b24f
SHA1 Hash	e260145c11dbd5c417c8e4b93ed37fff343844dd

Figure 4.1 – Separatist symbol



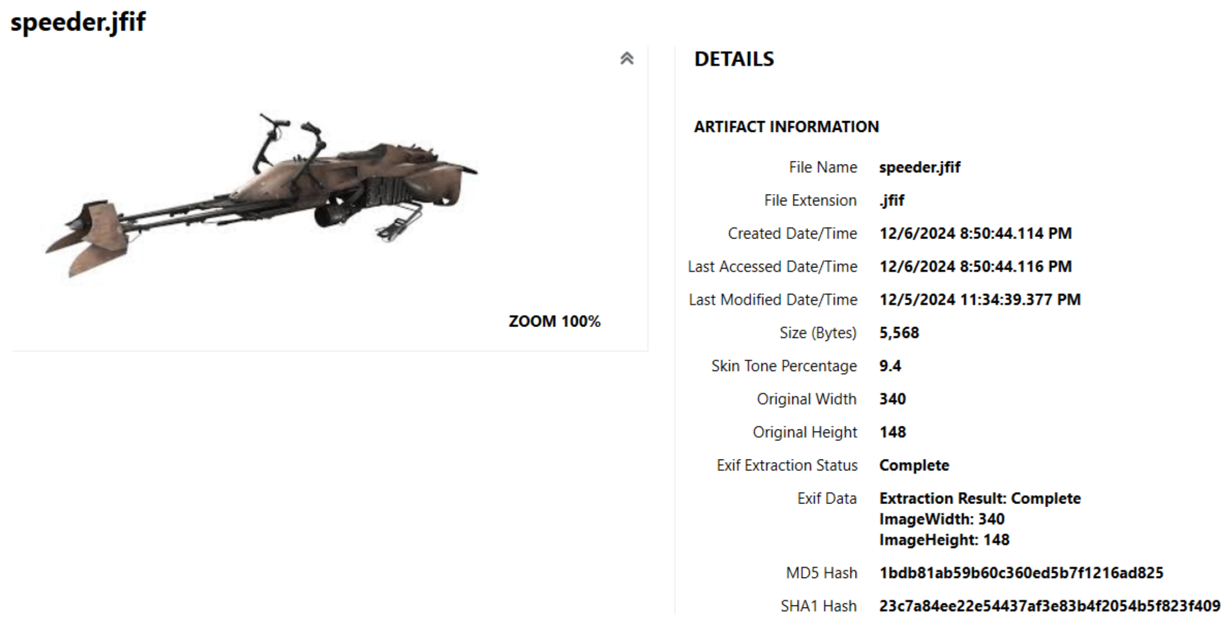
ship.jfif

DETAILS

ARTIFACT INFORMATION

File Name	ship.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.106 PM
Last Accessed Date/Time	12/6/2024 8:50:44.109 PM
Last Modified Date/Time	12/5/2024 11:36:16.479 PM
Size (Bytes)	7,354
Skin Tone Percentage	9.7
Original Width	318
Original Height	159
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 318 ImageHeight: 159
MD5 Hash	aa86410d3c1ef8c8e81f34c14778fcdb
SHA1 Hash	95831949b824bae276b1a8d5da056c82b5cc37b9

Figure 4.2 – Ship



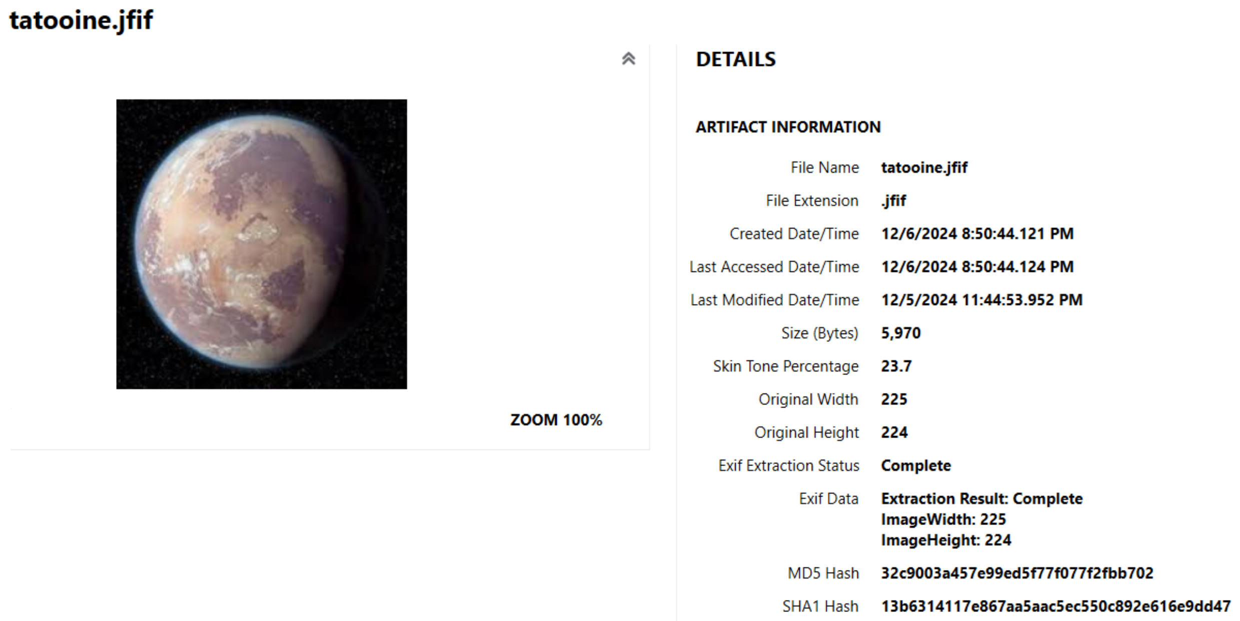
speeder.jfif

DETAILS

ARTIFACT INFORMATION

File Name	**speeder.jfif**
File Extension	**.jfif**
Created Date/Time	**12/6/2024 8:50:44.114 PM**
Last Accessed Date/Time	**12/6/2024 8:50:44.116 PM**
Last Modified Date/Time	**12/5/2024 11:34:39.377 PM**
Size (Bytes)	**5,568**
Skin Tone Percentage	**9.4**
Original Width	**340**
Original Height	**148**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 340** **ImageHeight: 148**
MD5 Hash	**1bdb81ab59b60c360ed5b7f1216ad825**
SHA1 Hash	**23c7a84ee22e54437af3e83b4f2054b5f823f409**

Figure 4.3 – Speeder



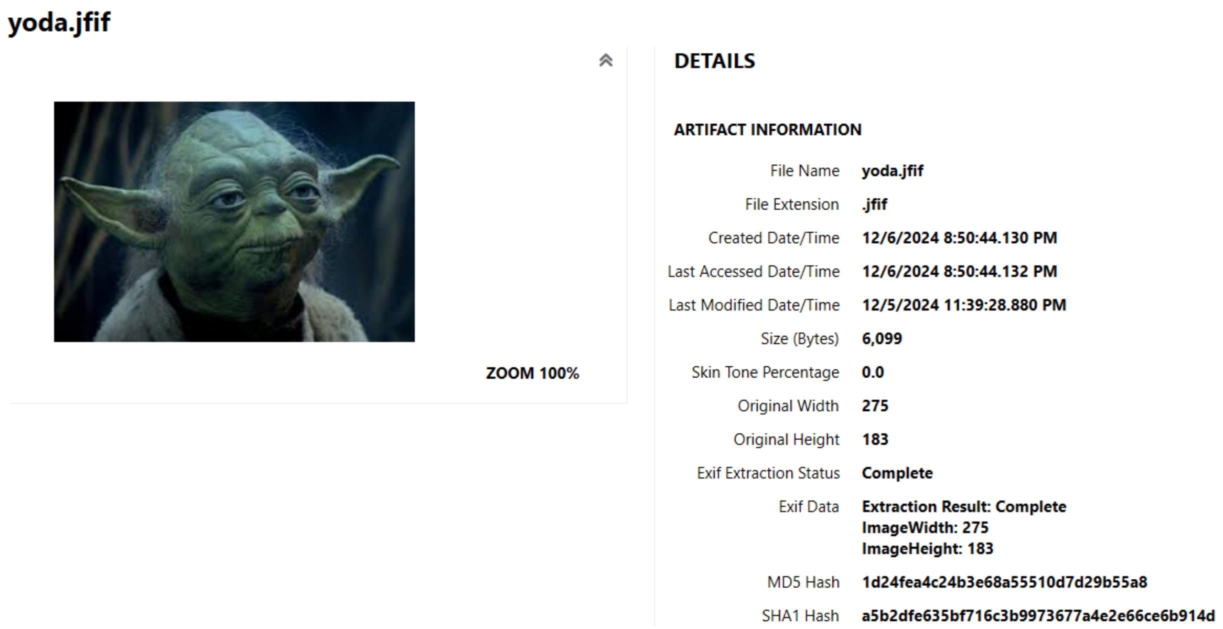
tatooine.jfif

DETAILS

ARTIFACT INFORMATION

File Name	**tatooine.jfif**
File Extension	**.jfif**
Created Date/Time	**12/6/2024 8:50:44.121 PM**
Last Accessed Date/Time	**12/6/2024 8:50:44.124 PM**
Last Modified Date/Time	**12/5/2024 11:44:53.952 PM**
Size (Bytes)	**5,970**
Skin Tone Percentage	**23.7**
Original Width	**225**
Original Height	**224**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 225** **ImageHeight: 224**
MD5 Hash	**32c9003a457e99ed5f77f077f2fbb702**
SHA1 Hash	**13b6314117e867aa5aac5ec550c892e616e9dd47**

Figure 4.4 – Tatooine, home to Anakin Skywalker



yoda.jfif

ZOOM 100%

DETAILS

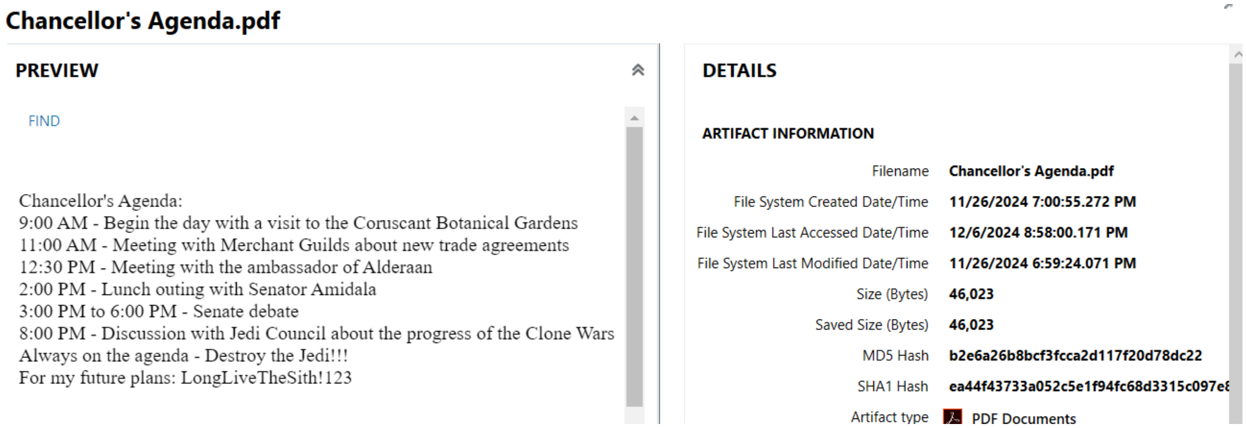
ARTIFACT INFORMATION

File Name	yoda.jfif
File Extension	.jfif
Created Date/Time	12/6/2024 8:50:44.130 PM
Last Accessed Date/Time	12/6/2024 8:50:44.132 PM
Last Modified Date/Time	12/5/2024 11:39:28.880 PM
Size (Bytes)	6,099
Skin Tone Percentage	0.0
Original Width	275
Original Height	183
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 275 ImageHeight: 183
MD5 Hash	1d24fea4c24b3e68a55510d7d29b55a8
SHA1 Hash	a5b2dfe635bf716c3b9973677a4e2e66ce6b914d

Figure 4.5 – Jedi Grand Master Yoda

Documents

During the forensic examination, several documents of interest were recovered from the suspects system. These files provide insight into Emperor Palpatine’s communications, intentions, and affiliations. Some notable recovered documents were an agenda outlining planned activities, a chat log involving members of the Jedi Order, and a conversation discussing the identity of the “Chosen One”. Additional documents referenced the selection of a new apprentice, which suggests that the continuation of the Sith recruitment efforts. These findings may contribute significantly to understanding the scope of the suspects involvement in these operations. Figures 4.6 – 5.4 illustrate the contents, hash values, and creation dates of these documents, supporting their relevance to the ongoing investigation.



Chancellor's Agenda.pdf

PREVIEW

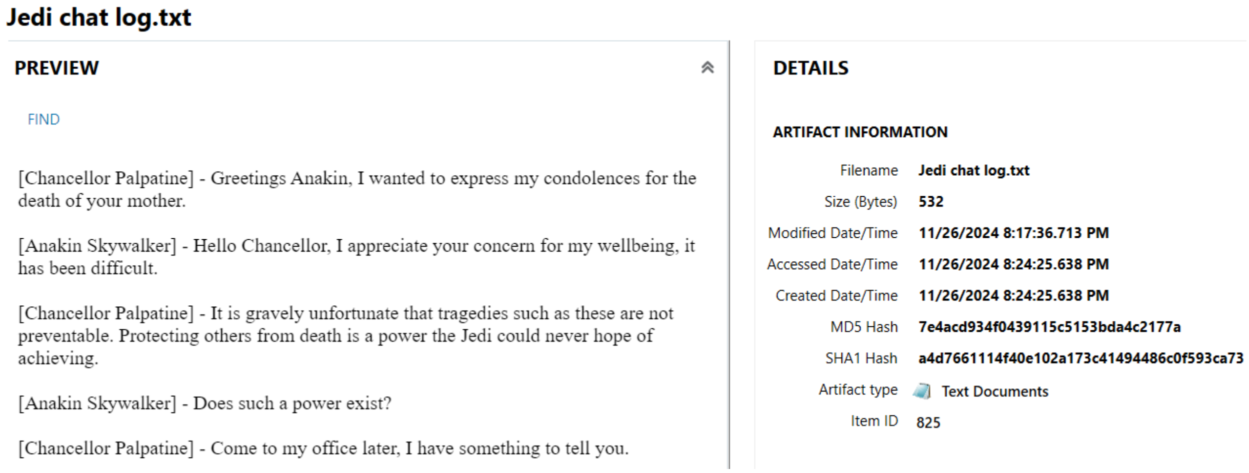
Chancellor's Agenda:
9:00 AM - Begin the day with a visit to the Coruscant Botanical Gardens
11:00 AM - Meeting with Merchant Guilds about new trade agreements
12:30 PM - Meeting with the ambassador of Alderaan
2:00 PM - Lunch outing with Senator Amidala
3:00 PM to 6:00 PM - Senate debate
8:00 PM - Discussion with Jedi Council about the progress of the Clone Wars
Always on the agenda - Destroy the Jedi!!!
For my future plans: LongLiveTheSith!123

DETAILS

ARTIFACT INFORMATION

Filename	**Chancellor's Agenda.pdf**
File System Created Date/Time	**11/26/2024 7:00:55.272 PM**
File System Last Accessed Date/Time	**12/6/2024 8:58:00.171 PM**
File System Last Modified Date/Time	**11/26/2024 6:59:24.071 PM**
Size (Bytes)	**46,023**
Saved Size (Bytes)	**46,023**
MD5 Hash	**b2e6a26b8bcf3fcca2d117f20d78dc22**
SHA1 Hash	**ea44f43733a052c5e1f94fc68d3315c097e8**
Artifact type	PDF Documents

Figure 4.6 -Chancellor's Agenda



Jedi chat log.txt

PREVIEW

[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 others from death is a power the Jedi could never hope of achieving.

[Anakin Skywalker] - Does such a power exist?

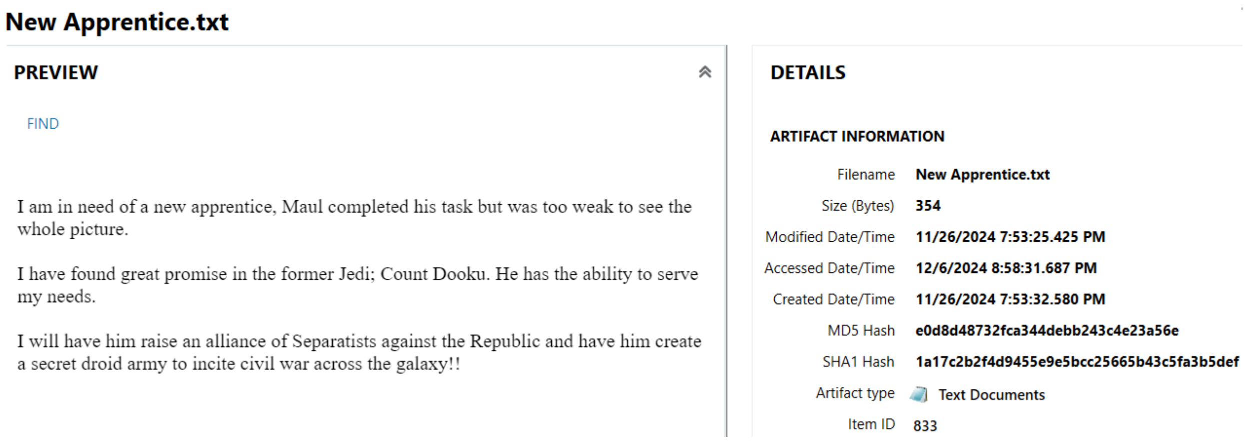
[Chancellor Palpatine] - Come to my office later, I have something to tell you.

DETAILS

ARTIFACT INFORMATION

Filename	**Jedi chat log.txt**
Size (Bytes)	**532**
Modified Date/Time	**11/26/2024 8:17:36.713 PM**
Accessed Date/Time	**11/26/2024 8:24:25.638 PM**
Created Date/Time	**11/26/2024 8:24:25.638 PM**
MD5 Hash	**7e4acd934f0439115c5153bda4c2177a**
SHA1 Hash	**a4d7661114f40e102a173c41494486c0f593ca73**
Artifact type	Text Documents
Item ID	825

Figure 4.7 – "Jedi Chat Log" between Chancellor Palpatine and Anakin Skywalker



New Apprentice.txt

PREVIEW

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.

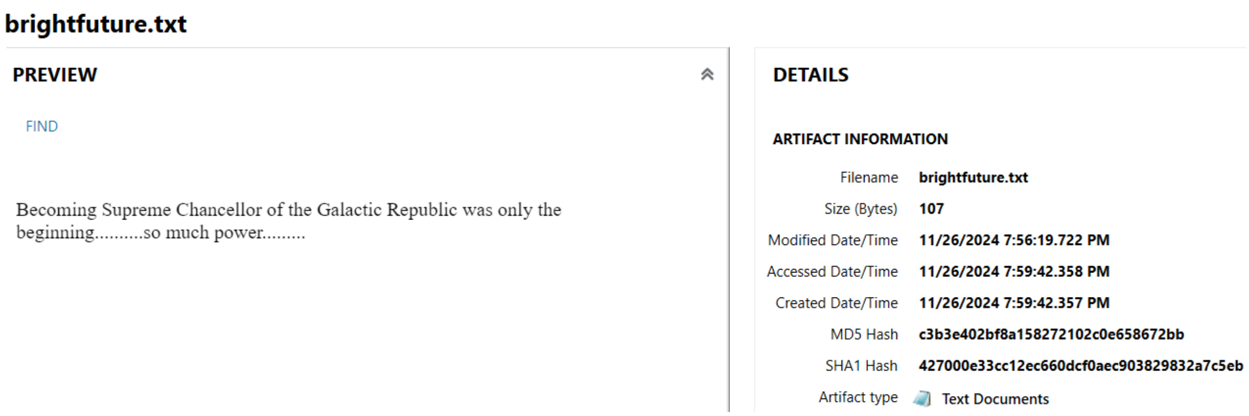
I will have him raise an alliance of Separatists against the Republic and have him create a secret droid army to incite civil war across the galaxy!!

DETAILS

ARTIFACT INFORMATION

Filename	**New Apprentice.txt**
Size (Bytes)	**354**
Modified Date/Time	**11/26/2024 7:53:25.425 PM**
Accessed Date/Time	**12/6/2024 8:58:31.687 PM**
Created Date/Time	**11/26/2024 7:53:32.580 PM**
MD5 Hash	**e0d8d48732fca344debb243c4e23a56e**
SHA1 Hash	**1a17c2b2f4d9455e9e5bcc25665b43c5fa3b5def**
Artifact type	Text Documents
Item ID	833

Figure 4.8 – New Apprentice



brightfuture.txt

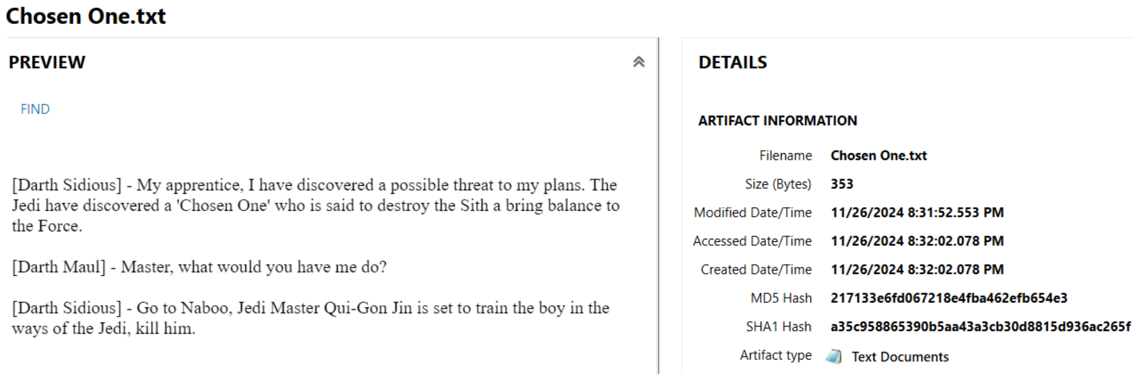
Becoming Supreme Chancellor of the Galactic Republic was only the beginning..........so much power.........

DETAILS

ARTIFACT INFORMATION

Filename	brightfuture.txt
Size (Bytes)	107
Modified Date/Time	11/26/2024 7:56:19.722 PM
Accessed Date/Time	11/26/2024 7:59:42.358 PM
Created Date/Time	11/26/2024 7:59:42.357 PM
MD5 Hash	c3b3e402bf8a158272102c0e658672bb
SHA1 Hash	427000e33cc12ec660dcf0aec903829832a7c5eb
Artifact type	Text Documents

Figure 4.9 – Bright Future



Chosen One.txt

[Darth Sidious] - My apprentice, I have discovered a possible threat to my plans. The Jedi have discovered a 'Chosen One' who is said to destroy the Sith a bring balance to the Force.

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

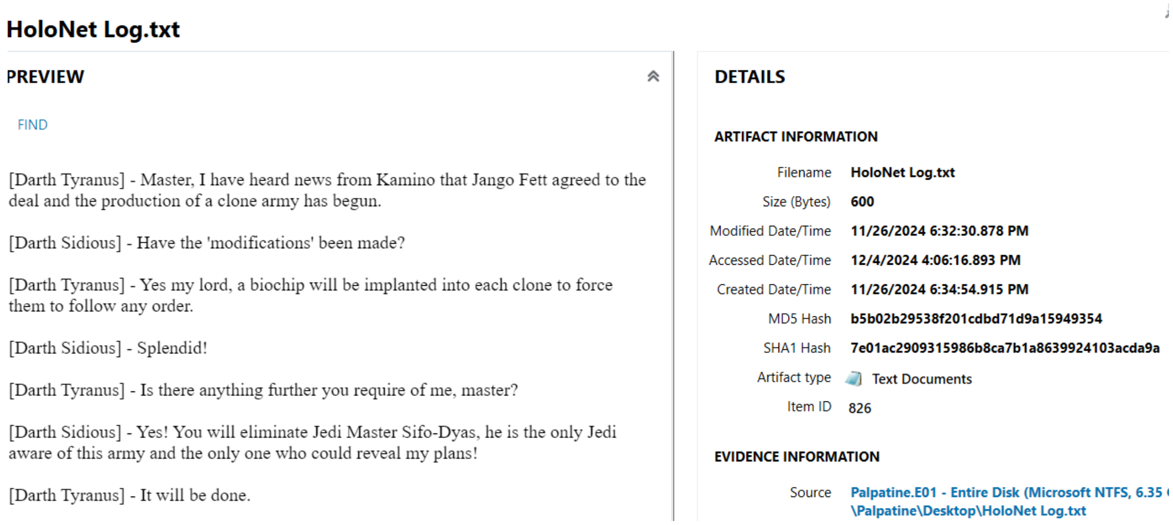
[Darth Sidious] - Go to Naboo, Jedi Master Qui-Gon Jin is set to train the boy in the ways of the Jedi, kill him.

DETAILS

ARTIFACT INFORMATION

Filename	Chosen One.txt
Size (Bytes)	353
Modified Date/Time	11/26/2024 8:31:52.553 PM
Accessed Date/Time	11/26/2024 8:32:02.078 PM
Created Date/Time	11/26/2024 8:32:02.078 PM
MD5 Hash	217133e6fd067218e4fba462efb654e3
SHA1 Hash	a35c958865390b5aa43a3cb30d8815d936ac265f
Artifact type	Text Documents

Figure 5.0 – Chosen One, Darth Sidious's intentions are death upon him



HoloNet Log.txt

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

[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 only one who could reveal my plans!

[Darth Tyranus] - It will be done.

DETAILS

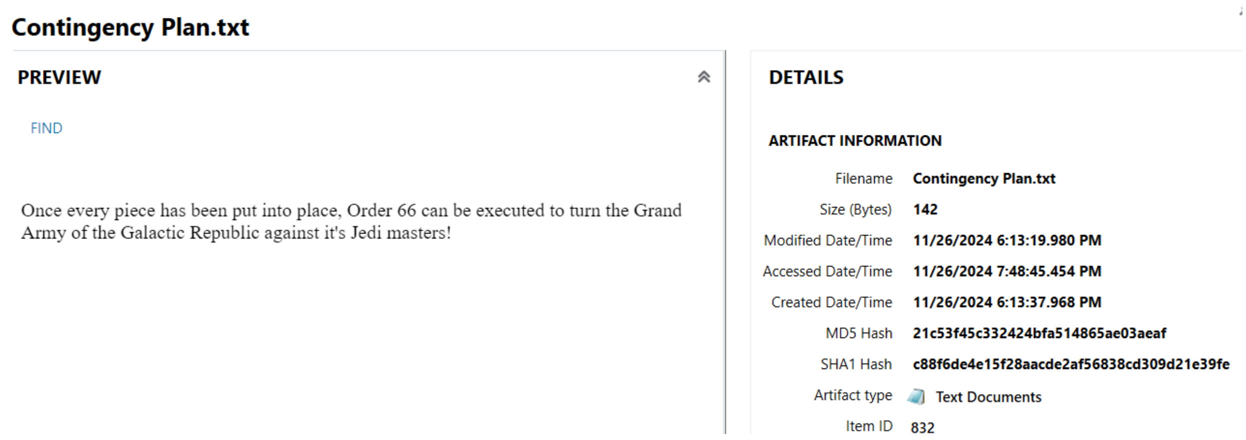
ARTIFACT INFORMATION

Filename	HoloNet Log.txt
Size (Bytes)	600
Modified Date/Time	11/26/2024 6:32:30.878 PM
Accessed Date/Time	12/4/2024 4:06:16.893 PM
Created Date/Time	11/26/2024 6:34:54.915 PM
MD5 Hash	b5b02b29538f201cdbd71d9a15949354
SHA1 Hash	7e01ac2909315986b8ca7b1a8639924103acda9a
Artifact type	Text Documents
Item ID	826

EVIDENCE INFORMATION

Source	Palpatine.E01 - Entire Disk (Microsoft NTFS, 6.35 \Palpatine\Desktop\HoloNet Log.txt

Figure 5.1 – HoloNet Log, Chat between Darth Sidious and Darth Tyranus talking about death upon Jedi Master Sifo-Dyas



Contingency Plan.txt

PREVIEW

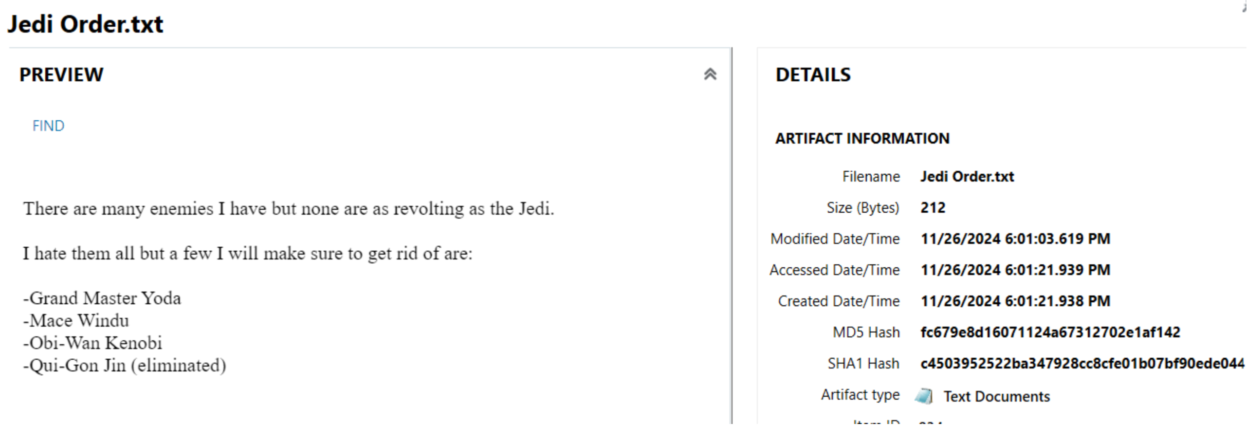
Once every piece has been put into place, Order 66 can be executed to turn the Grand Army of the Galactic Republic against it's Jedi masters!

DETAILS

ARTIFACT INFORMATION

Filename	Contingency Plan.txt
Size (Bytes)	142
Modified Date/Time	11/26/2024 6:13:19.980 PM
Accessed Date/Time	11/26/2024 7:48:45.454 PM
Created Date/Time	11/26/2024 6:13:37.968 PM
MD5 Hash	21c53f45c332424bfa514865ae03aeaf
SHA1 Hash	c88f6de4e15f28aacde2af56838cd309d21e39fe
Artifact type	Text Documents
Item ID	832

Figure 5.2 – Contingency Plan



Jedi Order.txt

PREVIEW

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:

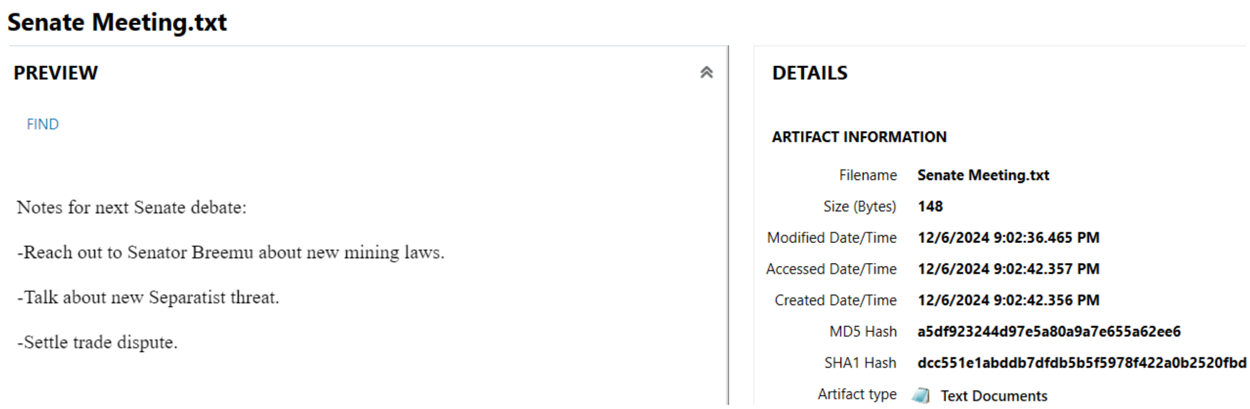
-Grand Master Yoda
-Mace Windu
-Obi-Wan Kenobi
-Qui-Gon Jin (eliminated)

DETAILS

ARTIFACT INFORMATION

Filename	Jedi Order.txt
Size (Bytes)	212
Modified Date/Time	11/26/2024 6:01:03.619 PM
Accessed Date/Time	11/26/2024 6:01:21.939 PM
Created Date/Time	11/26/2024 6:01:21.938 PM
MD5 Hash	fc679e8d16071124a67312702e1af142
SHA1 Hash	c4503952522ba347928cc8cfe01b07bf90ede044
Artifact type	Text Documents

Figure 5.3 – Jedi Order, List of people Chancellor Palpatine plans to execute



Senate Meeting.txt

PREVIEW

Notes for next Senate debate:

-Reach out to Senator Breemu about new mining laws.

-Talk about new Separatist threat.

-Settle trade dispute.

DETAILS

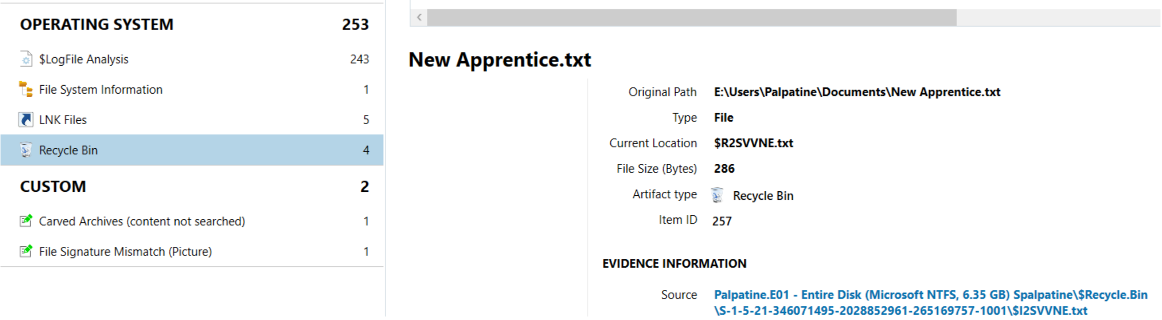
ARTIFACT INFORMATION

Filename	Senate Meeting.txt
Size (Bytes)	148
Modified Date/Time	12/6/2024 9:02:36.465 PM
Accessed Date/Time	12/6/2024 9:02:42.357 PM
Created Date/Time	12/6/2024 9:02:42.356 PM
MD5 Hash	a5df923244d97e5a80a9a7e655a62ee6
SHA1 Hash	dcc551e1abddb7dfdb5b5f5978f422a0b2520fbd
Artifact type	Text Documents

Figure 5.4 – Senate Meeting notes

Recycling Bin

During examination of the Recycle Bin, two notable documents were recovered, “New Apprentice.tx” and “Chosen One.txt”, shown in Figure 5.5 and 5.6. The presence of these files in the Recycle Bin suggests an attempt to delete potentially incriminating information. The New Apprentice.txt document outlines plans for recruiting or training a new Sith apprentice. While the Chosen One.txt contains references to an individual believed to fulfill an ancient prophecy. I believe both documents are highly relevant to the investigation.



OPERATING SYSTEM	253
$LogFile Analysis	243
File System Information	1
LNK Files	5
Recycle Bin	4
CUSTOM	**2**
Carved Archives (content not searched)	1
File Signature Mismatch (Picture)	1

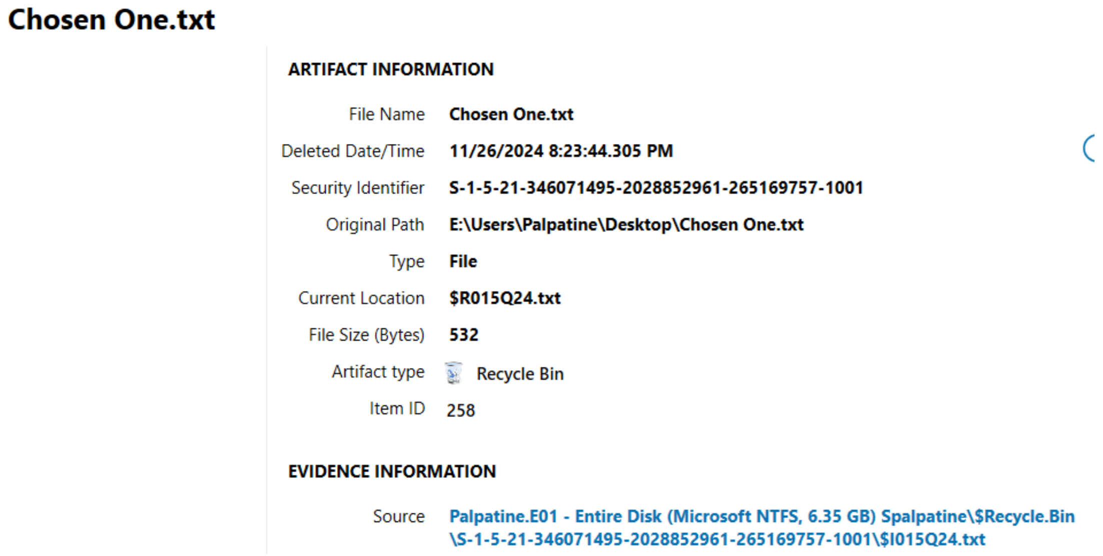
New Apprentice.txt

Original Path **E:\Users\Palpatine\Documents\New Apprentice.txt**
Type **File**
Current Location **$R2SVVNE.txt**
File Size (Bytes) **286**
Artifact type Recycle Bin
Item ID 257

EVIDENCE INFORMATION

Source Palpatine.E01 - Entire Disk (Microsoft NTFS, 6.35 GB) Spalpatine\$Recycle.Bin \S-1-5-21-346071495-2028852961-265169757-1001\$I2SVVNE.txt

Figure 5.5 – New Apprentice.txt in the recycling bin



Chosen One.txt

ARTIFACT INFORMATION

File Name **Chosen One.txt**
Deleted Date/Time **11/26/2024 8:23:44.305 PM**
Security Identifier **S-1-5-21-346071495-2028852961-265169757-1001**
Original Path **E:\Users\Palpatine\Desktop\Chosen One.txt**
Type **File**
Current Location **$R015Q24.txt**
File Size (Bytes) **532**
Artifact type Recycle Bin
Item ID 258

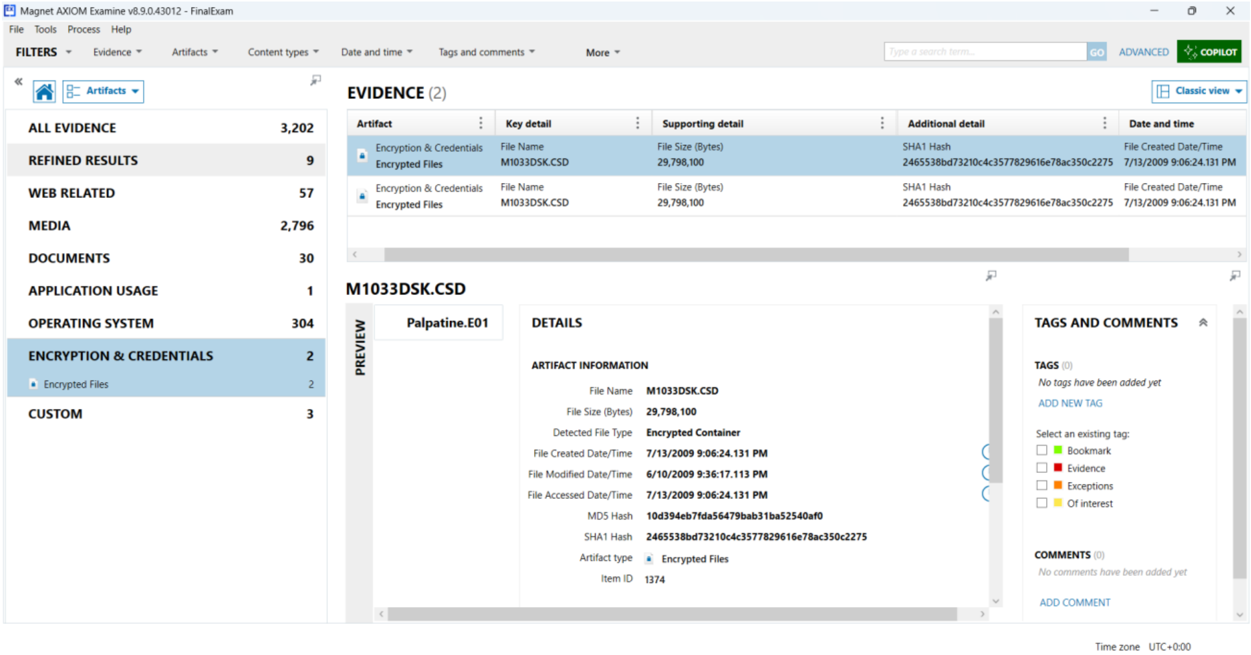
EVIDENCE INFORMATION

Source Palpatine.E01 - Entire Disk (Microsoft NTFS, 6.35 GB) Spalpatine\$Recycle.Bin \S-1-5-21-346071495-2028852961-265169757-1001\$I015Q24.txt

Figure 5.6 – Chosen One.txt in the recycling bin

Encryption & Credentials

In the Encryption and Credentials section of the analysis, one file was identified as being encrypted, but attempts to decrypt it were unsuccessful due to issues with properly downloading the encrypted file. However, during the review, a separate document titled “Chancellors Agenda.pdf” was found to contain the phrase “LongLiveTheSith!123” on the very last line in response to “My Future Plans:”, and it is structured like a password. This information could be relevant to future documents with passwords.



ALL EVIDENCE	3,202
REFINED RESULTS	9
WEB RELATED	57
MEDIA	2,796
DOCUMENTS	30
APPLICATION USAGE	1
OPERATING SYSTEM	304
ENCRYPTION & CREDENTIALS	2
Encrypted Files	2
CUSTOM	3

EVIDENCE (2)

Artifact	Key detail	Supporting detail	Additional detail	Date and time
Encryption & Credentials Encrypted Files	File Name M1033DSK.CSD	File Size (Bytes) 29,798,100	SHA1 Hash 2465538bd73210c4c3577829616e78ac350c2275	File Created Date/Time 7/13/2009 9:06:24.131 PM
Encryption & Credentials Encrypted Files	File Name M1033DSK.CSD	File Size (Bytes) 29,798,100	SHA1 Hash 2465538bd73210c4c3577829616e78ac350c2275	File Created Date/Time 7/13/2009 9:06:24.131 PM

M1033DSK.CSD

DETAILS

ARTIFACT INFORMATION

File Name	M1033DSK.CSD
File Size (Bytes)	29,798,100
Detected File Type	Encrypted Container
File Created Date/Time	7/13/2009 9:06:24.131 PM
File Modified Date/Time	6/10/2009 9:36:17.113 PM
File Accessed Date/Time	7/13/2009 9:06:24.131 PM
MD5 Hash	10d394eb7fda56479bab31ba52540af0
SHA1 Hash	2465538bd73210c4c3577829616e78ac350c2275
Artifact type	Encrypted Files
Item ID	1374

TAGS AND COMMENTS

TAGS (0)

No tags have been added yet

ADD NEW TAG

Select an existing tag:

- □ 🟩 Bookmark
- □ 🟥 Evidence
- □ 🟧 Exceptions
- □ 🟨 Of interest

COMMENTS (0)

No comments have been added yet

ADD COMMENT

Time zone UTC+0:00

Conclusion

This forensic examination was conducted in line with proper digital evidence handling procedures, beginning with the imaging of the suspect, Chancellor Palpatine's, device using FTK Imager. The imaging was performed in a controlled lab environment using a verified-clean hard drive to ensure the preservation of the original evidence. MD5 and SHA1 hash values were recorded and verified. This confirms that the image remained unaltered throughout the investigation process.

Although no Windows registry hives were recovered from the image, a significant amount of user-created content and system artifacts provided insight into Chancellors Palpatine activities. Some of the most incriminating pieces of evidence recovered were documents that directly linked Chancellor Palpatine to Sith related ideology and operations. These documents consist of the "Chancellors Agenda.pdf" document outlining daily schedules and long-term plans. The most revealing line was at the end saying, "My Future Plans: LongLiveTheSith!123". This phrase not only suggests allegiance to the Sith Order but also appears to function as a potential password. The next document was "New Apprentice.txt" document that was recovered from the Recycle Bin making note at who Chancellor Palpatine wants to become his new Sith apprentice. The "Chosen One.txt" was also recovered from the Recycle Bin and this document discusses the individual who is believed to be a prophesied chosen one. This suspect had the intent to sway the Chosen One. As for the Media files, dozens of images showed known Jedi, battle plans, the Death Star blueprints, and other visual content directly related to strategic planning.

The recovered items present Chancellor Palpatine as the central figure behind the Sith plans. These documents show premeditation, coordinated conspiracies, strategic political planning, and efforts to destroy key files.

Appendix of Terms

Active File Review – A process in digital forensics where non-deleted files is examined for relevant content.

AXIOM – A digital forensics software developed by Magnet Forensics used to recover, analyze, and report on digital evidence from devices.

Clone Wars – A fictional galactic conflict within the Star Wars universe.

Credentials – Usernames and passwords used to access secured systems, files, and applications.

Digital Forensics – The practice of collecting, preserving, analyzing, and digital evidence in a legally manner.

Encryption – The process of converting data into a coded form to prevent unauthorized access.

Evidence Image – An exact bit-for-bit copy of a storage device used to ensure the original data is not altered.

Forensic Explorer – Digital forensic examination tool that allows investigators to analyze data from forensic images.

FTK Imager – A tool that is used to create forensic images of digital storage devices.

Hash Value – A unique string generated by applying a hash function to data.

MD5 – A common hash function that produces a 128-bit hash value.

NTuser.dat – A window registry file that stores user-specific configurations.

Registry Hive – Stores system and user configuration data. Examples, SAM, SYSTEM, SOFTWARE, and NTuser.dat.

Security Accounts Manager (SAM) – A registry hive in Windows. Stores user account information.

SHA1 – A hash function that produces a 160-bit hash value.

Strategic Political Planning – Deliberate actions aimed at manipulating political systems.