

LAB EXAM DF

Description

HA: Forensics is an intermediate level of the lab, which gives you a hand on real-life experience in Cyber Forensic Investigation. This lab is completely dedicated to methods and tools of Cyber Forensic Investigation and there is evidence that can be found with various techniques. As it is a Capture-the-Flag, it is very important to note that it is not a root challenge and comes with a primary motive to find all the flags.

No. of Flags: 4

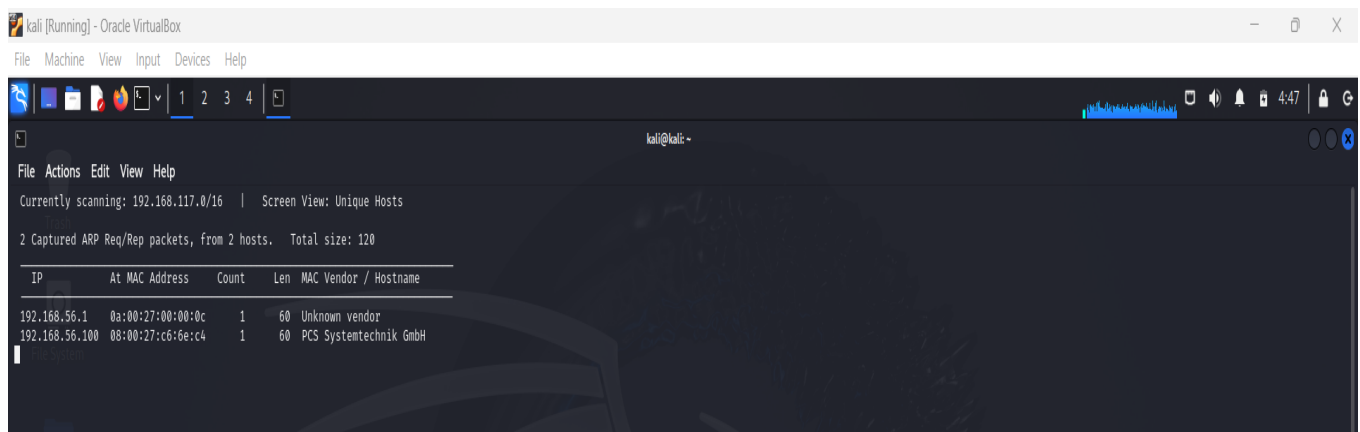
Screen short

```
Ubuntu 18.04 LTS ubuntu tty1
ubuntu login: jasoos
Password:
Last login: Tue Jul 1 03:19:16 PDT 2025 on tty1
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings
jasoos@ubuntu:~$ _
```

Using netdiscover command



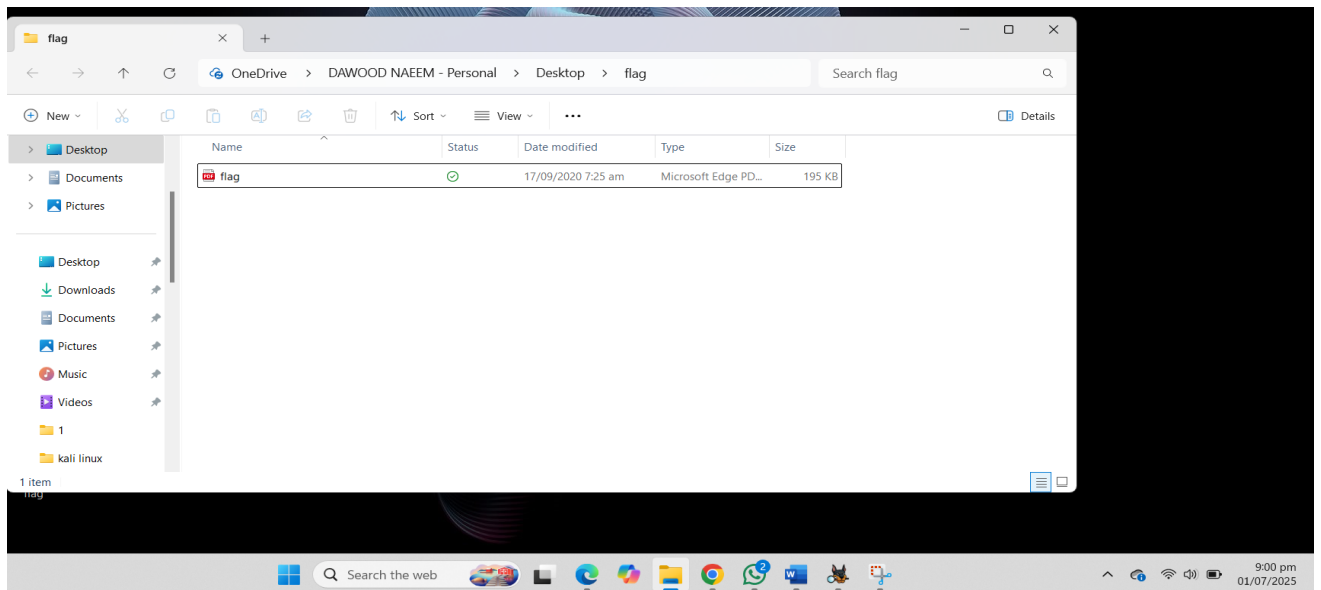
Found Flag 1 In the File Fingerprint.txt

The screenshot shows the Autopsy 4.22.1 interface. On the left, a file tree displays the directory structure of the analyzed disk image. The main pane shows a listing of files in the path `/img_forensics-disk1.vmdk/vol2/var/www/html/images`. The file `fingerprint.jpg` is selected, and its metadata is displayed in the bottom pane.

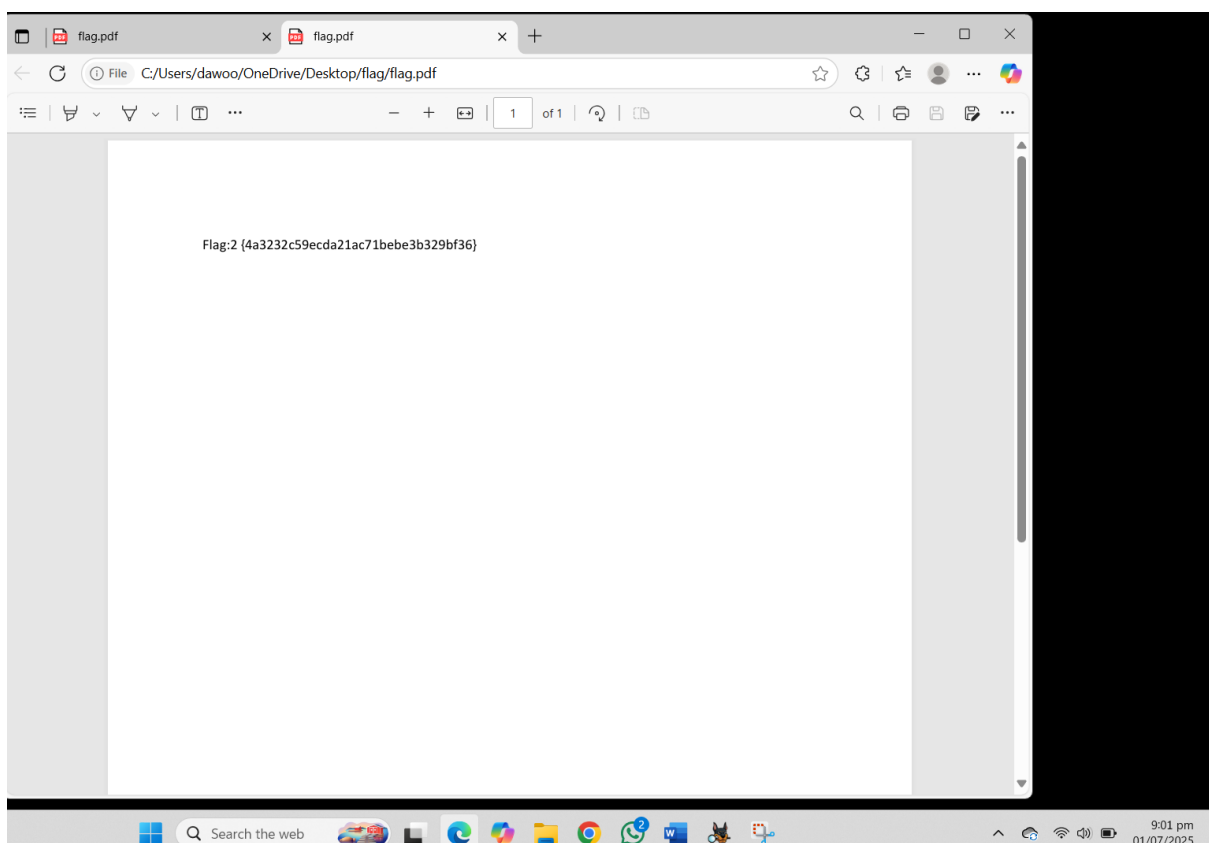
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2020-09-17 15:37:17 PKT	2020-09-17 15:37:17 PKT	2020-09-23 17:05:19 PKT	2020-09-17 15:07:20 PKT	4096	Allocated	Allocated	unknown
[parent folder]				2020-09-24 19:39:14 PKT	2020-09-24 19:39:14 PKT	2020-09-24 19:39:16 PKT	2020-09-17 15:02:02 PKT	4096	Allocated	Allocated	unknown
1.jpg				2020-09-13 08:06:06 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	88846	Allocated	Allocated	unknown
10.jpg				2020-09-17 15:22:33 PKT	2020-09-17 15:36:54 PKT	2020-09-17 18:04:13 PKT	2020-09-17 15:23:39 PKT	16753	Unallocated	Allocated	unknown
2.jpg				2020-09-13 08:08:42 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	49488	Allocated	Allocated	unknown
3.jpg				2020-09-13 08:09:22 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	143029	Allocated	Allocated	unknown
4.jpg				2020-09-13 08:04:56 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	214120	Allocated	Allocated	unknown
5.jpg				2020-09-13 08:09:44 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	116747	Allocated	Allocated	unknown
6.jpg				2020-09-13 08:26:22 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	1606412	Allocated	Allocated	unknown
7.jpg				2020-09-13 08:26:46 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	82194	Allocated	Allocated	unknown
8.jpg				2020-09-13 08:27:08 PKT	2020-09-17 15:07:20 PKT	2020-09-24 19:27:54 PKT	2020-09-17 15:07:20 PKT	164769	Allocated	Allocated	unknown
9.jpg				2020-09-13 08:35:06 PKT	2020-09-17 15:37:17 PKT	2020-09-13 08:35:06 PKT	2020-09-17 15:07:20 PKT	111035	Allocated	Allocated	unknown
dns.jpg				2020-09-13 08:35:06 PKT	2020-09-17 15:37:17 PKT	2020-09-13 08:35:06 PKT	2020-09-17 15:07:20 PKT	111035	Unallocated	Allocated	unknown
fingerprint.jpg				2020-09-17 15:22:33 PKT	2020-09-17 15:36:54 PKT	2020-09-17 18:04:13 PKT	2020-09-17 15:23:39 PKT	16753	Allocated	Allocated	unknown

The bottom pane shows the file's metadata, including its JFIF header and a string containing a flag: `+Flag:1 [bc02d4ffbeeab9f57c5e03de1098ff31]`.

The screenshot shows a file explorer window with a dialog box titled "Password needed". The dialog box contains the message: "File 'flag' is password protected. Please enter the password in the box below." There is a text input field for the password and three buttons: "OK", "Skip File", and "Cancel". The background shows a file explorer window with a progress bar at 0% complete.



Found flag 2 hidden in a pdf file



flags - Autopsy 4.22.1

Case View Tools Window Help

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

Listing

/img_forensics-disk1.vmdk/vol_vol2/home/jasoo

Table Thumbnail Summary

9 Results

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2020-09-24 20:06:31 PKT	2020-09-24 20:06:31 PKT	2020-09-25 04:56:45 PKT	2020-09-17 17:40:59 PKT	4096	Allocated	Allocated	unknown
[parent folder]				2020-09-17 17:40:59 PKT	2020-09-17 17:40:59 PKT	2020-09-24 20:06:27 PKT	2020-09-17 14:52:56 PKT	4096	Allocated	Allocated	unknown
.cache				2020-09-17 18:41:18 PKT	2020-09-17 18:41:18 PKT	2020-09-18 02:23:38 PKT	2020-09-17 18:41:18 PKT	4096	Allocated	Allocated	unknown
.local				2020-09-18 02:25:21 PKT	2020-09-18 02:25:21 PKT	2020-09-23 17:05:17 PKT	2020-09-18 02:25:21 PKT	4096	Allocated	Allocated	unknown
.bash_history		0		2020-09-25 04:59:29 PKT	2020-09-25 04:59:29 PKT	2020-09-25 04:59:29 PKT	2020-09-18 02:26:12 PKT	27	Allocated	Allocated	unknown
.bash_logout		1		2020-09-17 17:40:59 PKT	2020-09-17 17:40:59 PKT	2020-09-25 04:55:33 PKT	2020-09-17 17:40:59 PKT	220	Allocated	Allocated	unknown
.bashrc		1		2020-09-17 17:40:59 PKT	2020-09-17 17:40:59 PKT	2020-09-24 20:05:17 PKT	2020-09-17 17:40:59 PKT	3771	Allocated	Allocated	unknown
.profile		1		2020-09-17 17:40:59 PKT	2020-09-17 17:40:59 PKT	2020-09-24 20:05:17 PKT	2020-09-17 17:40:59 PKT	807	Allocated	Allocated	unknown
saboot.001				2020-09-24 20:06:31 PKT	2020-09-24 20:06:31 PKT	2020-09-24 20:05:47 PKT	2020-09-24 20:05:47 PKT	0	Unallocated	Unallocated	unknown

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: /img_forensics-disk1.vmdk/vol_vol2/home/jasoo/saboot.001

Type: File System

MIME Type: application/octet-stream

Size: 0

File Name Allocation: Unallocated

Metadata Allocation: Unallocated

Modified: 2020-09-24 20:06:31 PKT

Accessed: 2020-09-24 20:05:47 PKT

Analyzing files from forensics-disk1.vmdk 3%

30°C Haze

Search the web

9:02 pm 01/07/2025

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Open

Look in: Desktop

Recent Items

Desktop

Documents

This PC

Network

Gallery

DAWOOD NAEEM - Personal

Desktop

Documents

Pictures

Downloads

Music

Videos

DAWOOD NAEEM KHAN

This PC

Libraries

DVD Drive (E:) Kali Linux amd64

Network

face_recognition_project-main

flag

forensics

saboot

File name: saboot.001

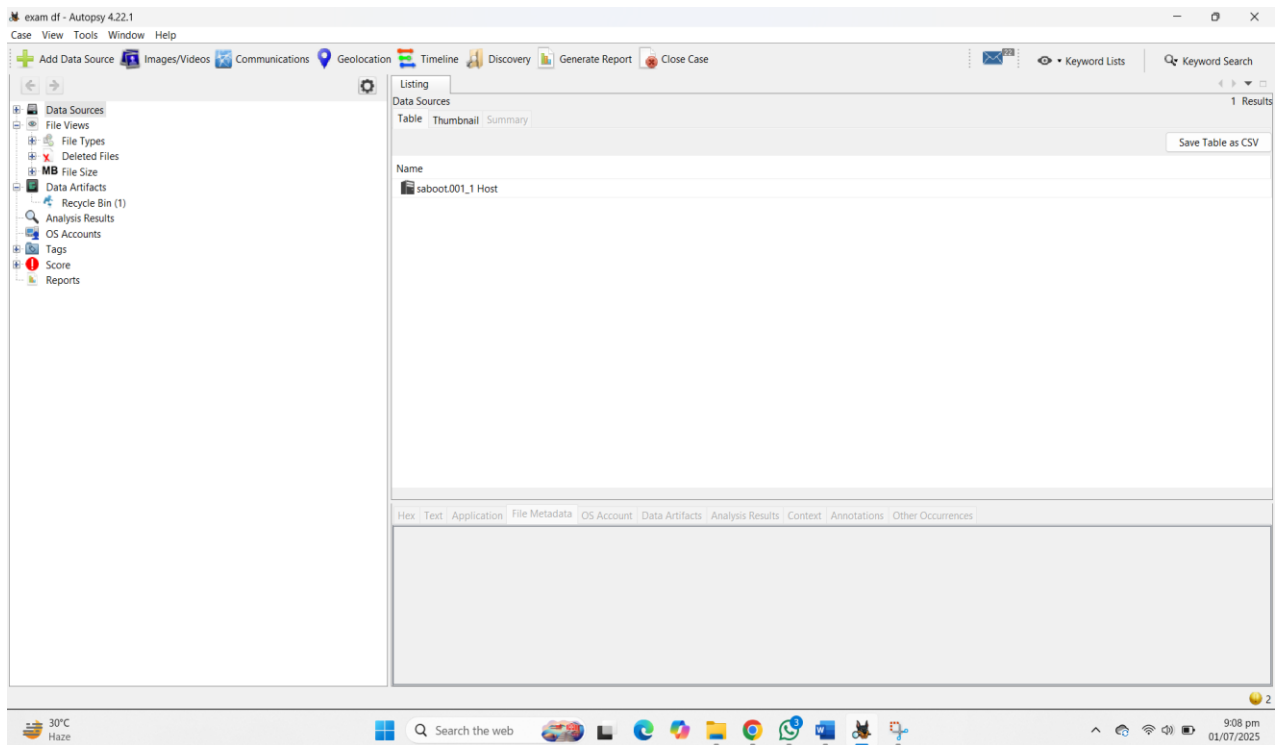
Files of type: All Supported Types

Open

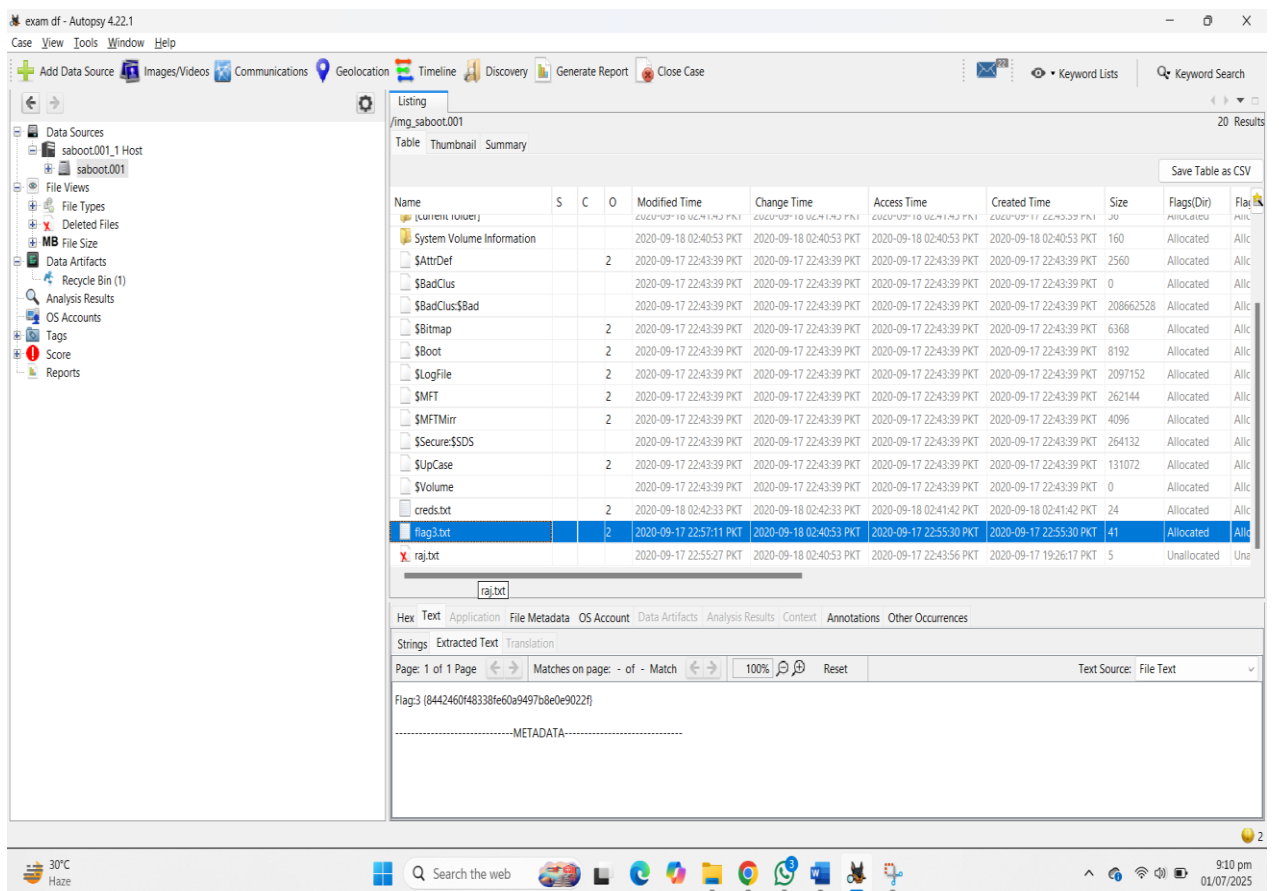
Cancel

< Back Next > Finish Cancel Help

9:06 pm 01/07/2025



Flag 3 was found in saboot.001 -> flag3.txt



For flag 4, we found a creds.txt where we found a base 64 encoded hash. We decoded that hash using chatgpt. Then in the Ubuntu system we followed the walkthrough from medium and found flag 4.

The screenshot shows the Autopsy 4.22.1 interface. The left sidebar displays the file tree for 'saboot001_1 Host' and 'saboot001'. The main window shows a listing of files in the '/img_saboot.001' directory. The 'creds.txt' file is highlighted, showing its metadata and search results.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
System Volume Information				2020-09-18 02:40:53 PKT	2020-09-18 02:40:53 PKT	2020-09-18 02:40:53 PKT	2020-09-18 02:40:53 PKT	160	Allocated	Allc
\$AttrDef			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2560	Allocated	Allc
\$BadClus				2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	0	Allocated	Allc
\$BadClus\$Bad				2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	208662528	Allocated	Allc
\$Bitmap			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	6368	Allocated	Allc
\$Boot			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	8192	Allocated	Allc
\$LogFile			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2097152	Allocated	Allc
\$MFT			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	262144	Allocated	Allc
\$MFTMirr			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	4096	Allocated	Allc
\$Secure\$SDS				2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	264132	Allocated	Allc
\$UpCase			2	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	131072	Allocated	Allc
\$Volume				2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	2020-09-17 22:43:39 PKT	0	Allocated	Allc
creds.txt			2	2020-09-18 02:42:33 PKT	2020-09-18 02:42:33 PKT	2020-09-18 02:41:42 PKT	2020-09-18 02:41:42 PKT	24	Allocated	Allc
flag3.txt			2	2020-09-17 22:57:11 PKT	2020-09-18 02:40:53 PKT	2020-09-17 22:55:30 PKT	2020-09-17 22:55:30 PKT	41	Allocated	Allc
raj.txt				2020-09-17 22:55:27 PKT	2020-09-18 02:40:53 PKT	2020-09-17 22:43:56 PKT	2020-09-17 19:26:17 PKT	5	Unallocated	Una

The screenshot shows the ChatGPT interface. The user has entered the prompt: "What can I help with?". The response is: "amVlbnFsaWlzYWdwb2RnaXJs decode this". The user has also entered the prompt: "amVlbnFsaWlzYWdwb2RnaXJs decode this". The response is: "amVlbnFsaWlzYWdwb2RnaXJs decode this".

