Forensics CTF 7

Platform: picoCTF 2024

Challenge Name: Dear Diary

Category: Forensics

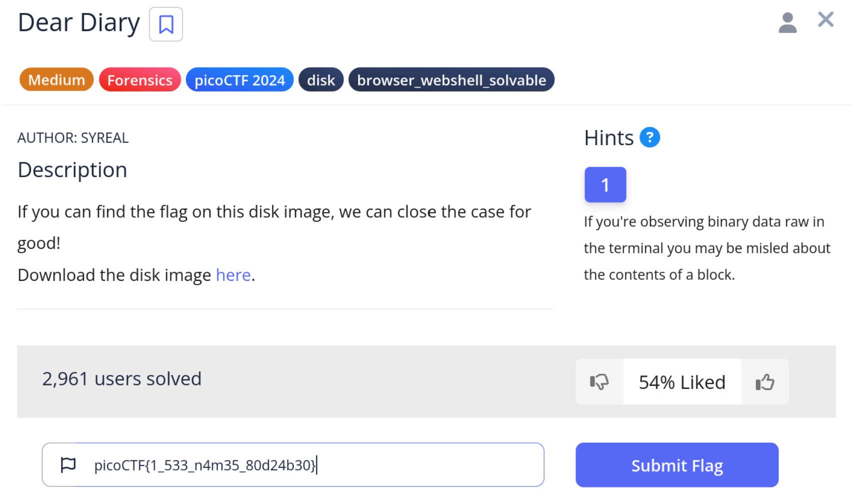
Difficulty: Medium

Submitted By: Gurleen Kaur Brar

Objective

The objective was to investigate a disk image file using forensic techniques and locate an embedded flag, typically hidden in unallocated or slack space. This challenge emphasized disk-level analysis using tools like Autopsy.

Challenge Description



Dear Diary

AUTHOR: SYREAL

Description

If you can find the flag on this disk image, we can close the case for good!

Download the disk image here.

Hints

If you're observing binary data raw in the terminal you may be misled about the contents of a block.

2,961 users solved

picoCTF{1_533_n4m35_80d24b30}

Files and Tools Used

- **File Provided:** `disk.flag.img` (raw disk image)
- **Tools Used:**
    - Kali Linux Terminal

- Autopsy (Forensic Browser)

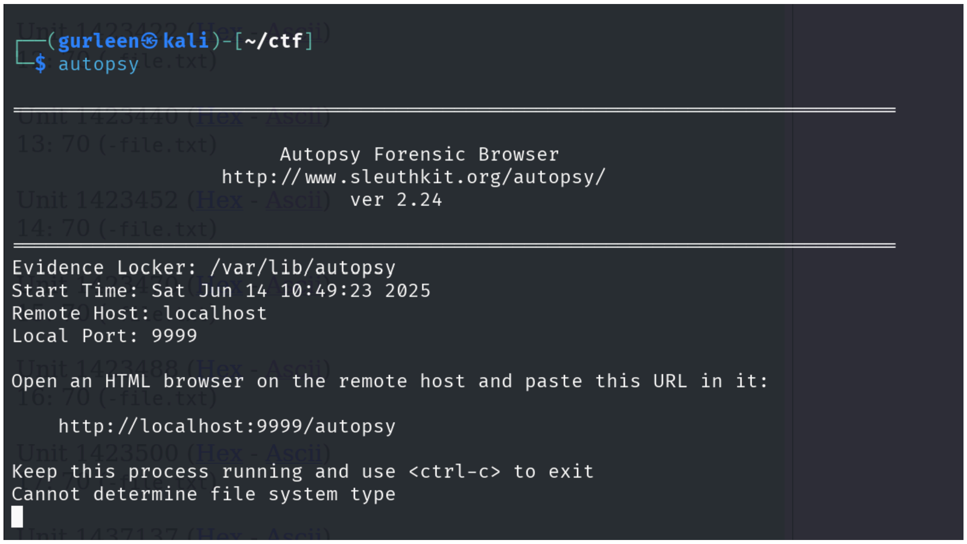
Step-by-Step Process

Step 1: Launch Autopsy

Started the Autopsy forensic browser via terminal.

Accessed it at:

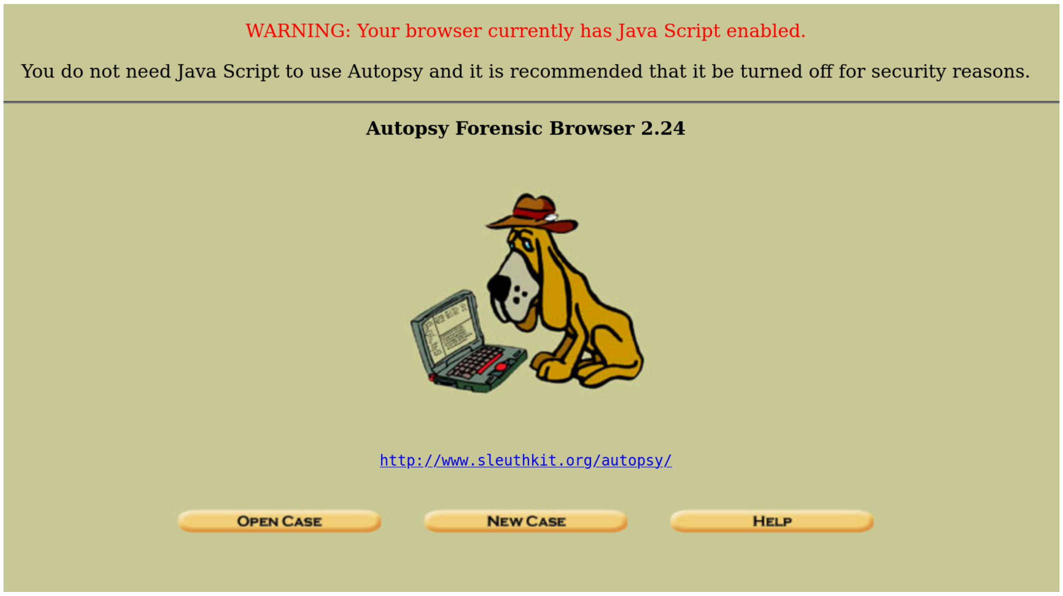
`http://localhost:9999/autopsy`



```
┌──(gurleen㉿kali)-[~/ctf]
└─$ autopsy

============================================================================

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                               ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Sat Jun 14 10:49:23 2025
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
Cannot determine file system type
```

Step 2: Create a New Case

- Case Name: `CTF`
- Investigator: `Gurleen`

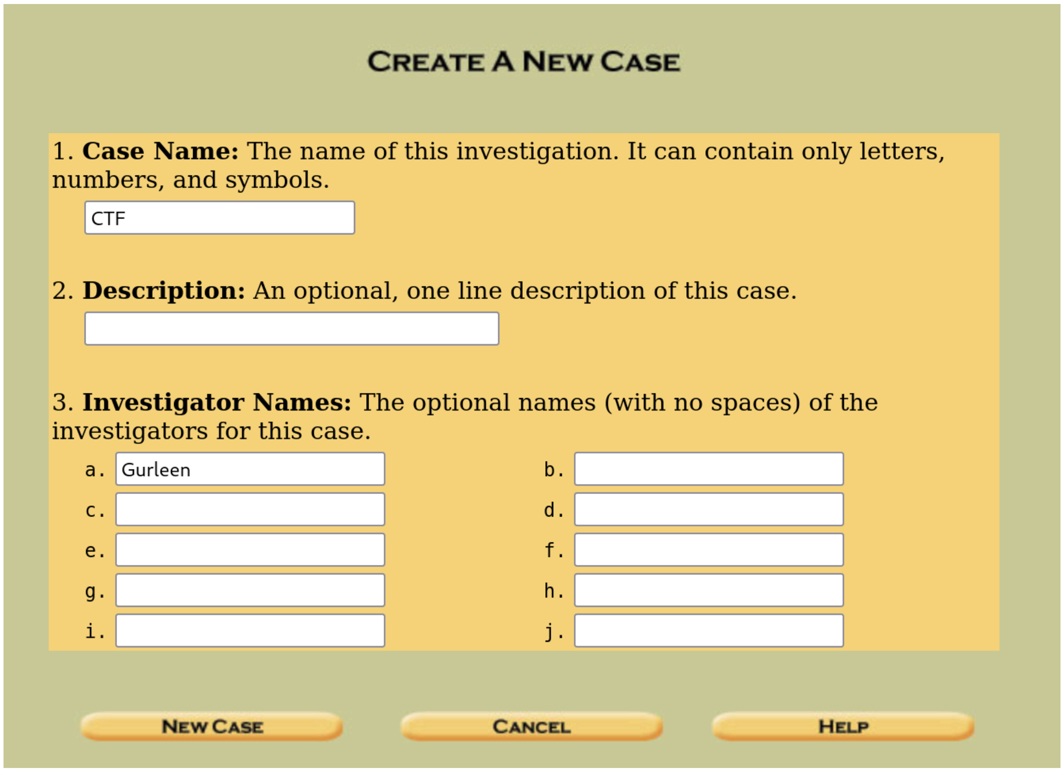


WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

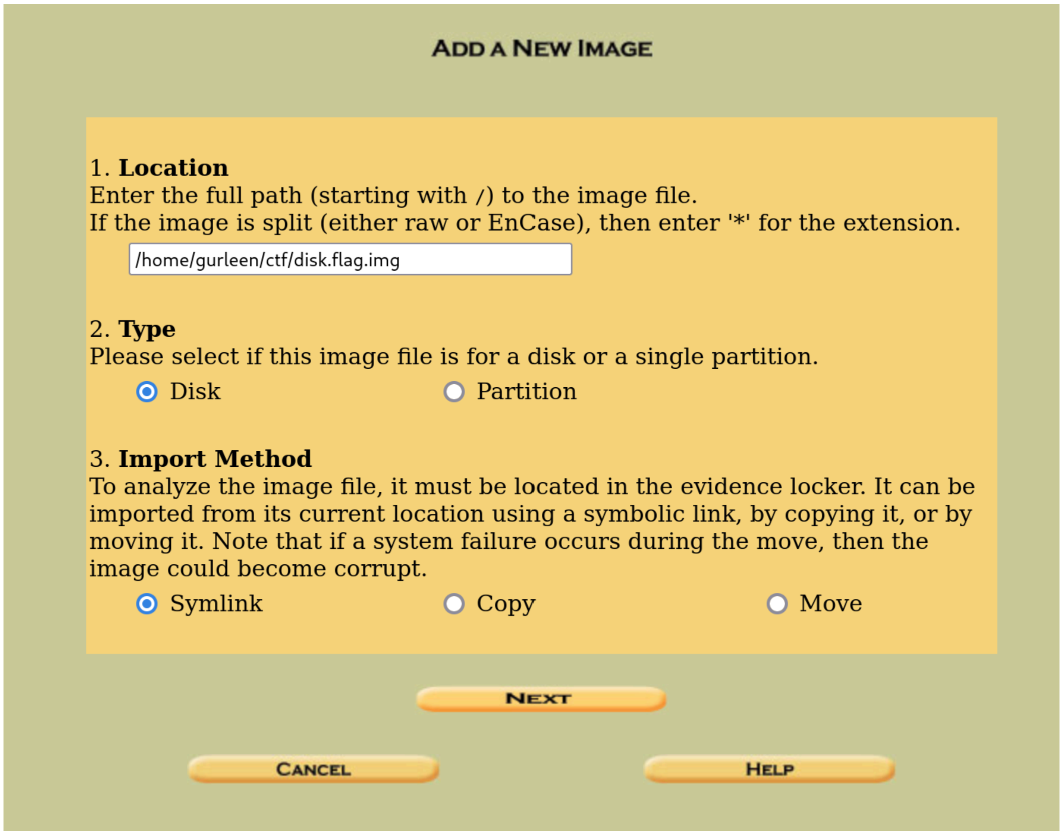
CTF

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Gurleen b.
c. d.
e. f.
g. h.
i. j.

Proceeded to load the `disk.flag.img` file using the “Add New Image” option with the Disk.



1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/gurleen/ctf/disk.flag.img

2. **Type**
Please select if this image file is for a disk or a single partition.

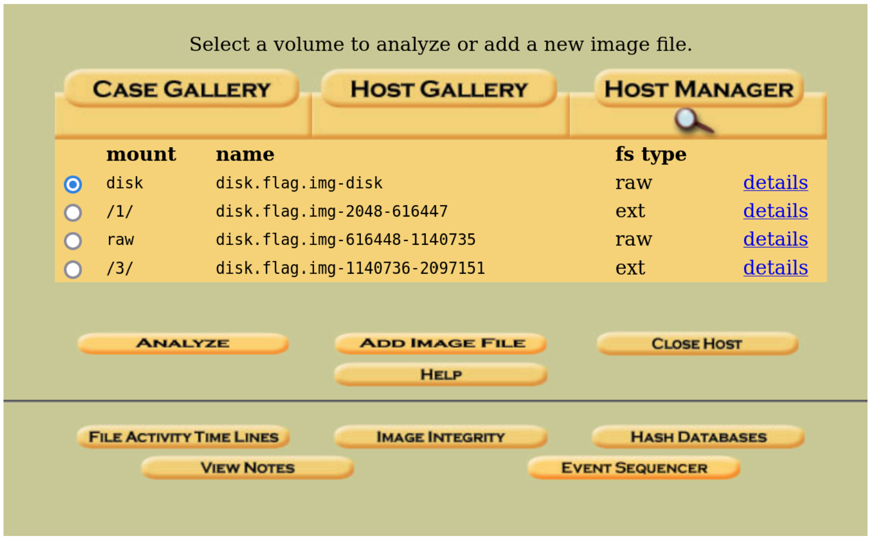
● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

Step 3: Analyze File System Volumes

Mounted and selected available partitions. Multiple ext and raw regions were present. Chose the most promising region to scan.

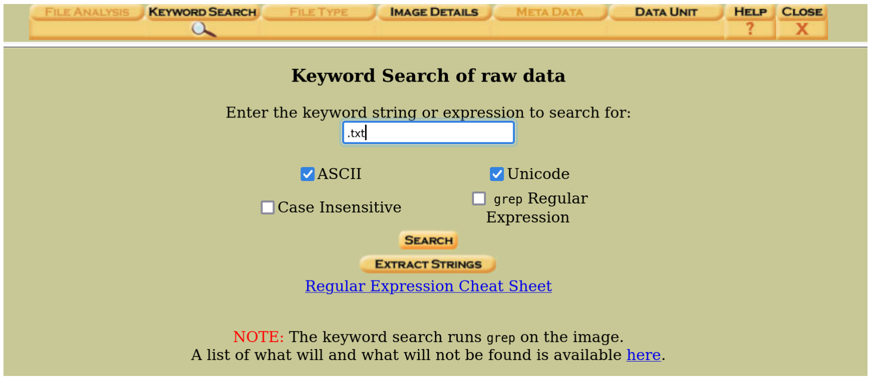


Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	disk	disk.flag.img-disk	raw	details
○	/1/	disk.flag.img-2048-616447	ext	details
○	raw	disk.flag.img-616448-1140735	raw	details
○	/3/	disk.flag.img-1140736-2097151	ext	details

Step 4: Search for Suspicious Text Files

Used **Keyword Search** to look for `txt` files or references.



Keyword Search of raw data

Enter the keyword string or expression to search for: .txt

☑ ASCII ☑ Unicode

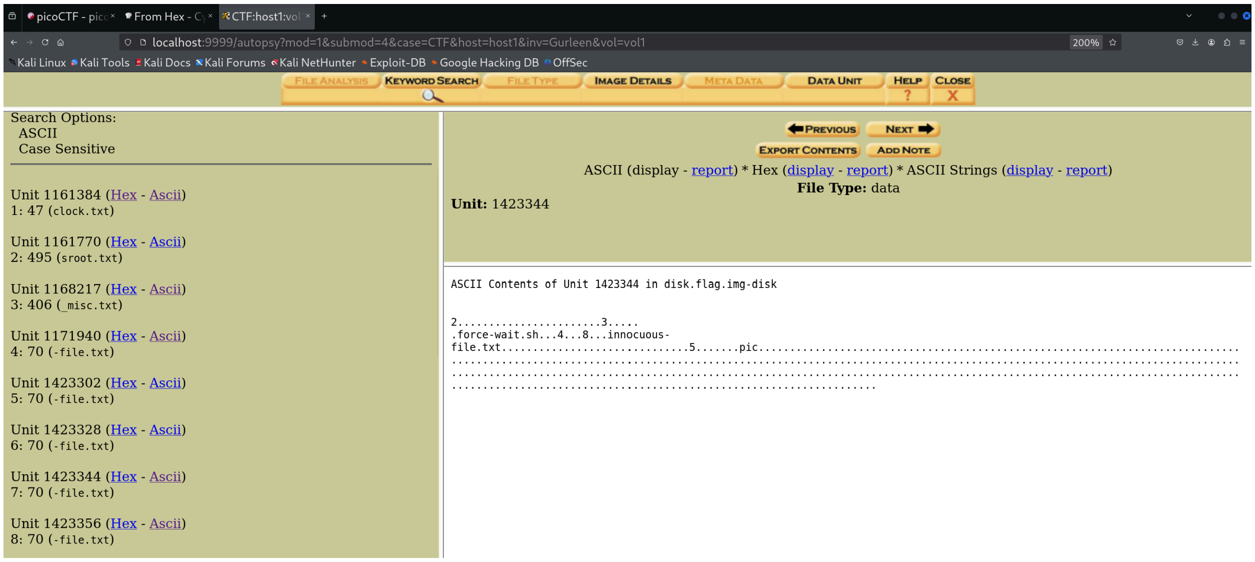
☐ Case Insensitive ☐ `grep` Regular Expression

NOTE: The keyword search runs `grep` on the image.
A list of what will and what will not be found is available here.

Results showed hidden file fragments like:

- `force-wait.sh`
- `innocuous-file.txt`

One of the blocks (Unit 1423356) contained ASCII fragments that revealed a flag structure embedded within.



Search Options:
 ASCII
 Case Sensitive

Unit 1161384 (Hex - Ascii)
1: 47 (`clock.txt`)

Unit 1161770 (Hex - Ascii)
2: 495 (`sroot.txt`)

Unit 1168217 (Hex - Ascii)
3: 406 (`_misc.txt`)

Unit 1171940 (Hex - Ascii)
4: 70 (`-file.txt`)

Unit 1423302 (Hex - Ascii)
5: 70 (`-file.txt`)

Unit 1423328 (Hex - Ascii)
6: 70 (`-file.txt`)

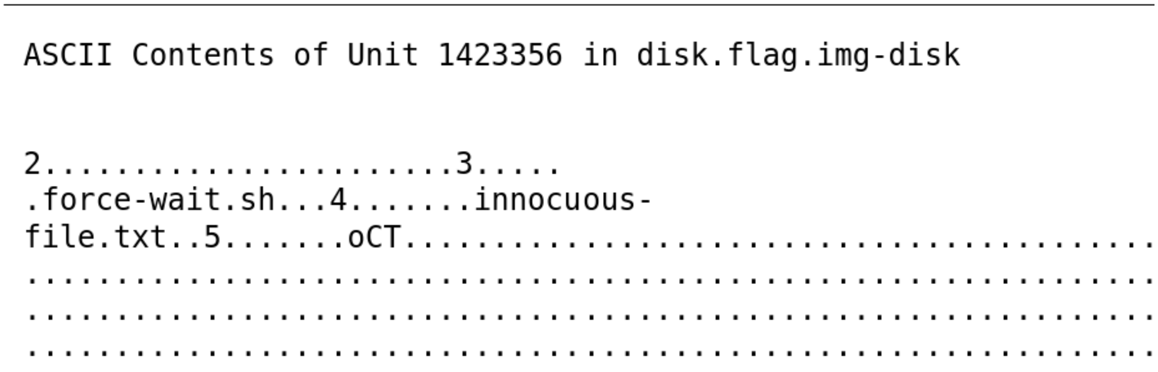
Unit 1423344 (Hex - Ascii)
7: 70 (`-file.txt`)

Unit 1423356 (Hex - Ascii)
8: 70 (`-file.txt`)

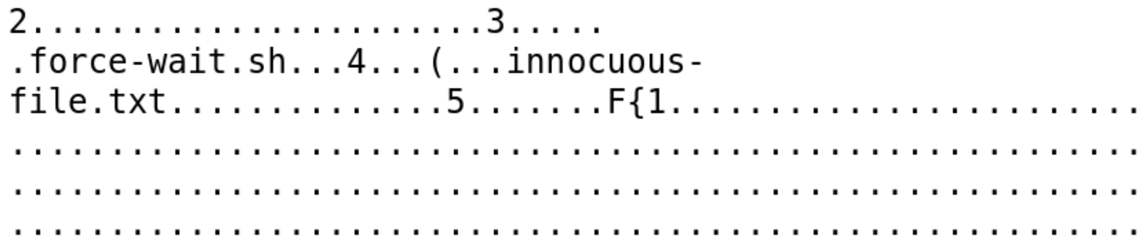
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)
File Type: data

Unit: 1423344

```
ASCII Contents of Unit 1423344 in disk.flag.img-disk


2......................3.....
.force-wait.sh...4...8...innocuous-
file.txt............................5.......pic...............................................................................
.............................................................................................................................
.............................................................................................................................
...................................................................
```

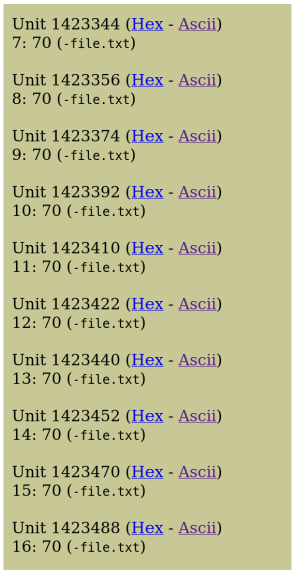


```
ASCII Contents of Unit 1423356 in disk.flag.img-disk


2.......................3.....
.force-wait.sh...4.......innocuous-
file.txt..5.......oCT..........................................
...............................................................
...............................................................
...............................................................
```



```
2.......................3.....
.force-wait.sh...4...(...innocuous-
file.txt..............5.......F{1.........................
..........................................................
..........................................................
..........................................................
```

The flag was within these Units 7-16.



Unit 1423344 (Hex - Ascii)
7: 70 (-file.txt)

Unit 1423356 (Hex - Ascii)
8: 70 (-file.txt)

Unit 1423374 (Hex - Ascii)
9: 70 (-file.txt)

Unit 1423392 (Hex - Ascii)
10: 70 (-file.txt)

Unit 1423410 (Hex - Ascii)
11: 70 (-file.txt)

Unit 1423422 (Hex - Ascii)
12: 70 (-file.txt)

Unit 1423440 (Hex - Ascii)
13: 70 (-file.txt)

Unit 1423452 (Hex - Ascii)
14: 70 (-file.txt)

Unit 1423470 (Hex - Ascii)
15: 70 (-file.txt)

Unit 1423488 (Hex - Ascii)
16: 70 (-file.txt)

Flag Submitted

```
picoCTF{1_533_n4m35_80d24b30}
```

The flag was successfully recovered and accepted.