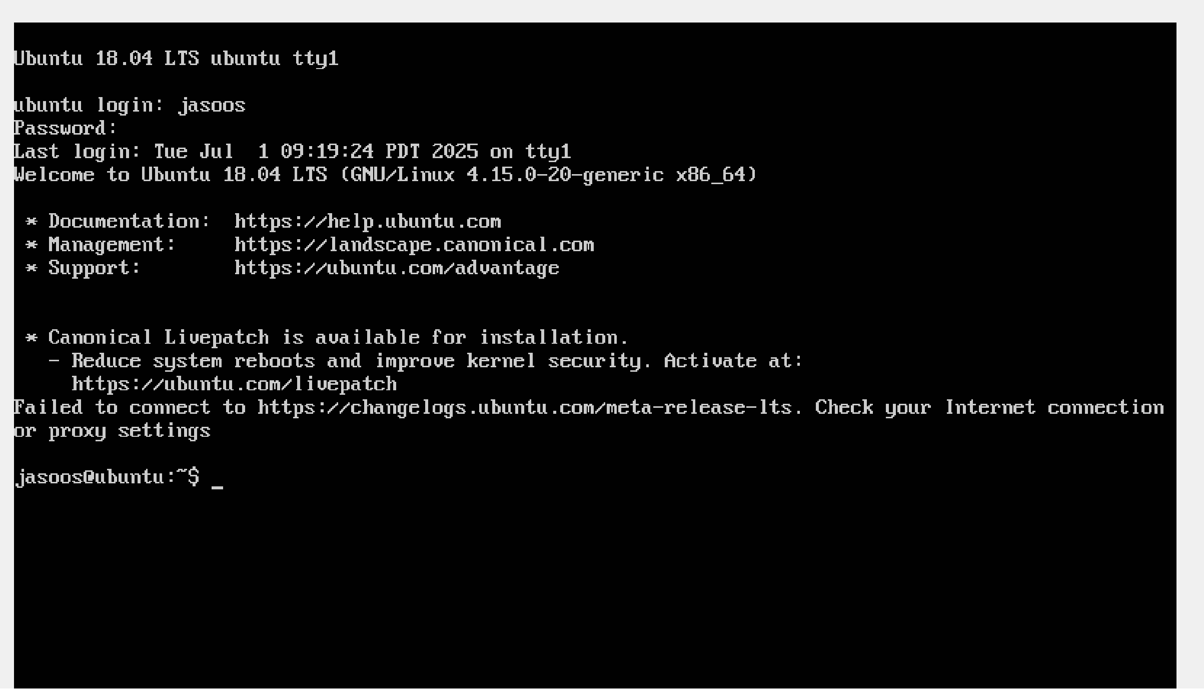
Name :syed taha ali
roll no:bcys-2023s-001

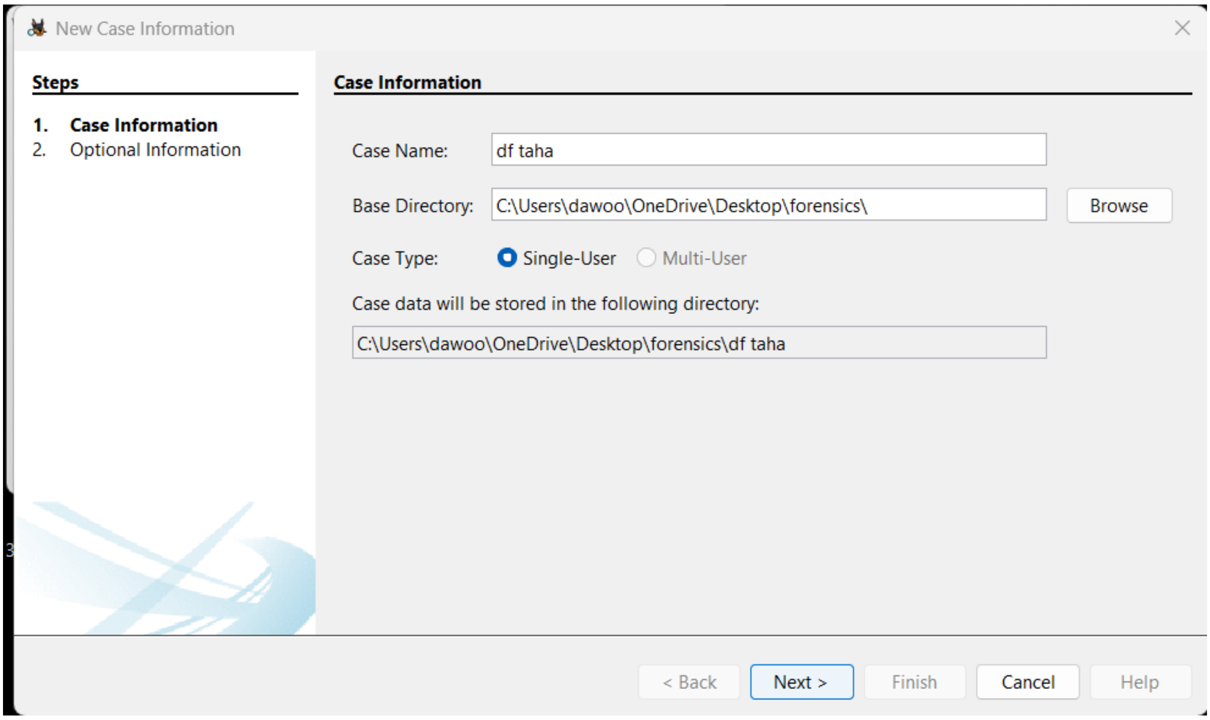
DIGITAL FORENSICS LAB EXAM

Step no 1) log in ubuntu



```
Ubuntu 18.04 LTS ubuntu tty1

ubuntu login: jasoos
Password:
Last login: Tue Jul  1 09:19:24 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:~$ _
```

step2 run in autopsy


New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name: df taha

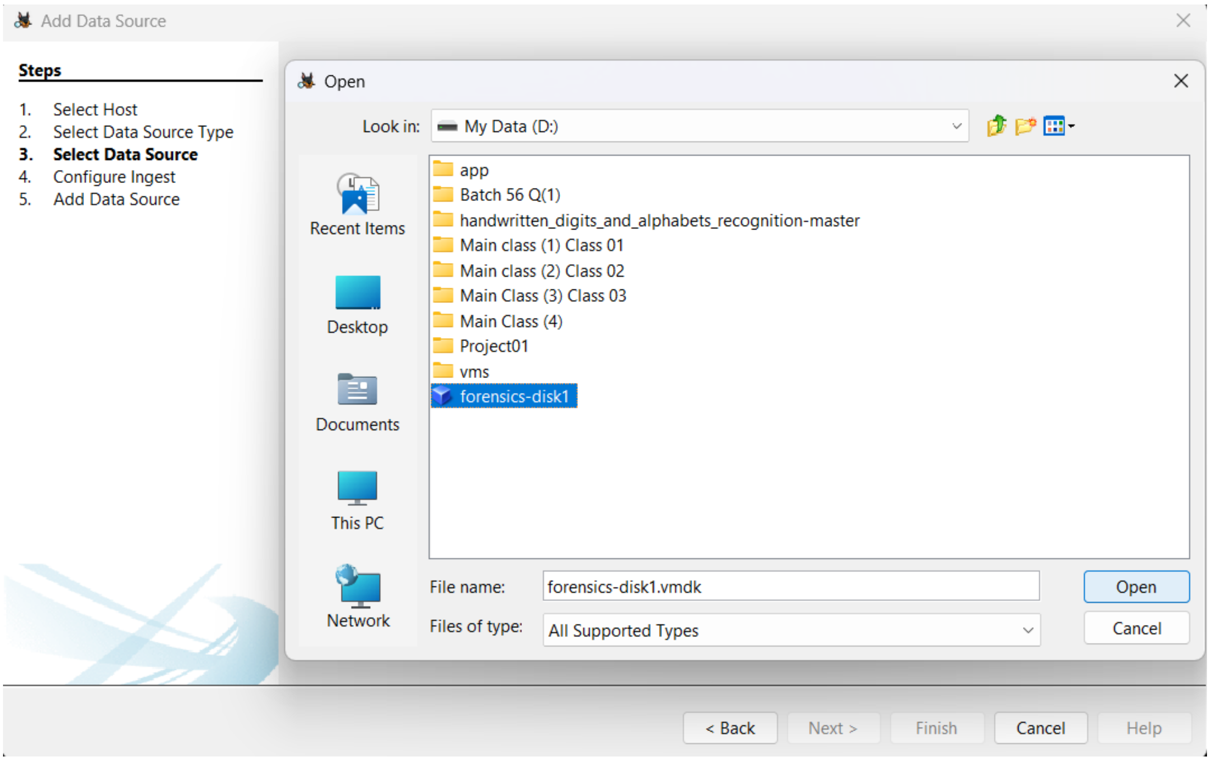
Base Directory: C:\Users\dawoo\OneDrive\Desktop\forensics\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\dawoo\OneDrive\Desktop\forensics\df taha

Check if can find any flag by uploading forensics vm


Add Data Source

Steps

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

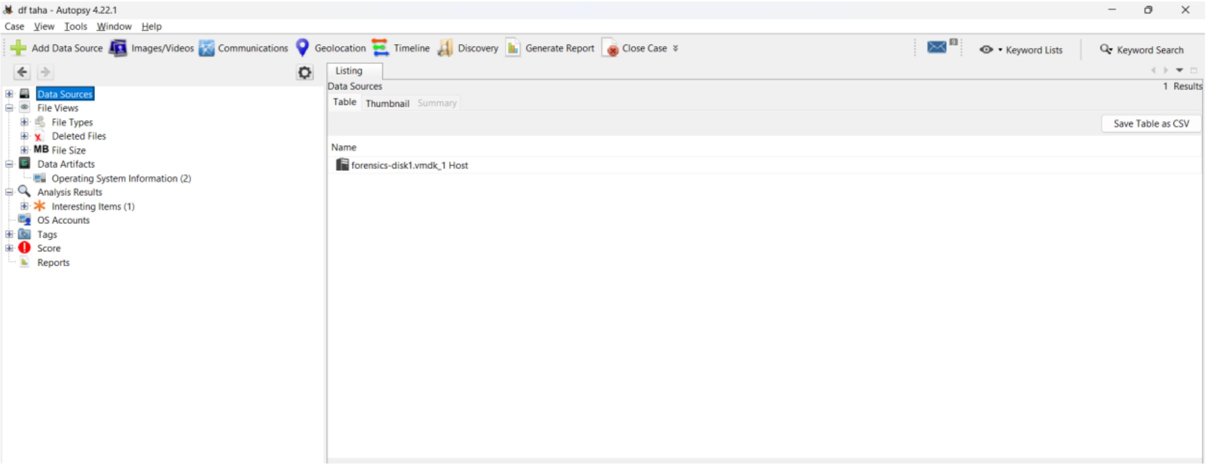
Open

Look in: My Data (D:)

- app
- Batch 56 Q(1)
- handwritten_digits_and_alphabets_recognition-master
- Main class (1) Class 01
- Main class (2) Class 02
- Main Class (3) Class 03
- Main Class (4)
- Project01
- vms
- forensics-disk1

File name: forensics-disk1.vmdk

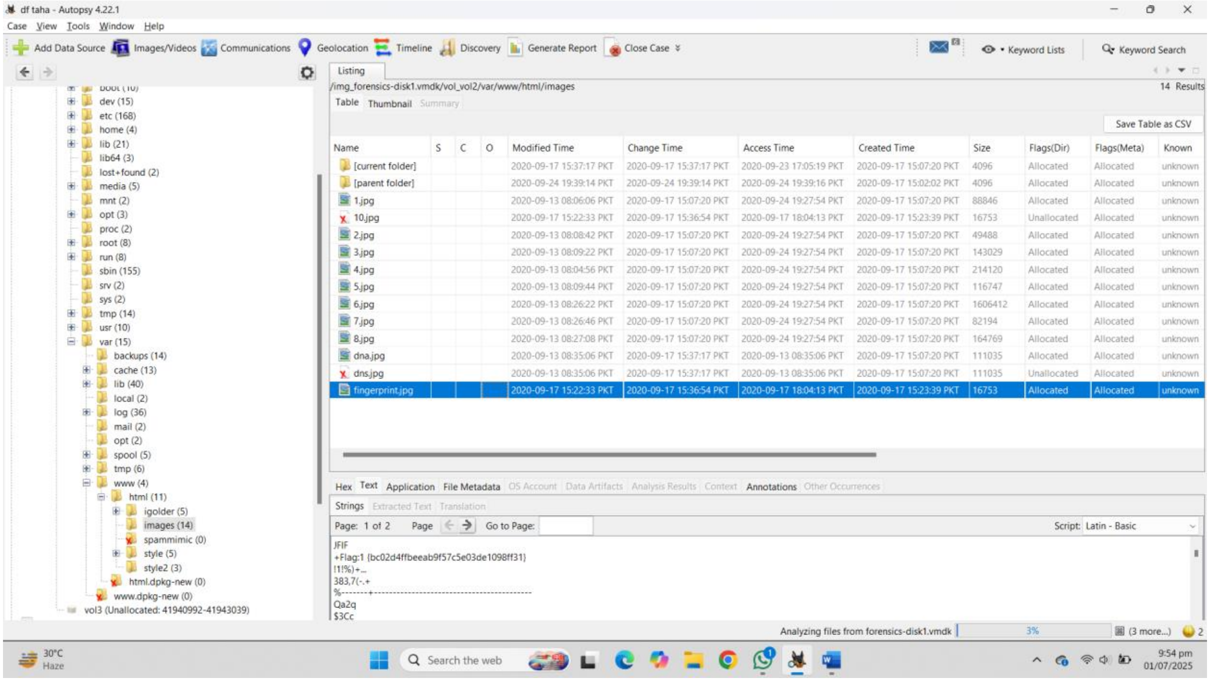
Files of type: All Supported Types



Data Sources 1 Results

Name
forensics-disk1.vmdk_1 Host

I have found flag 1 by using autopsy

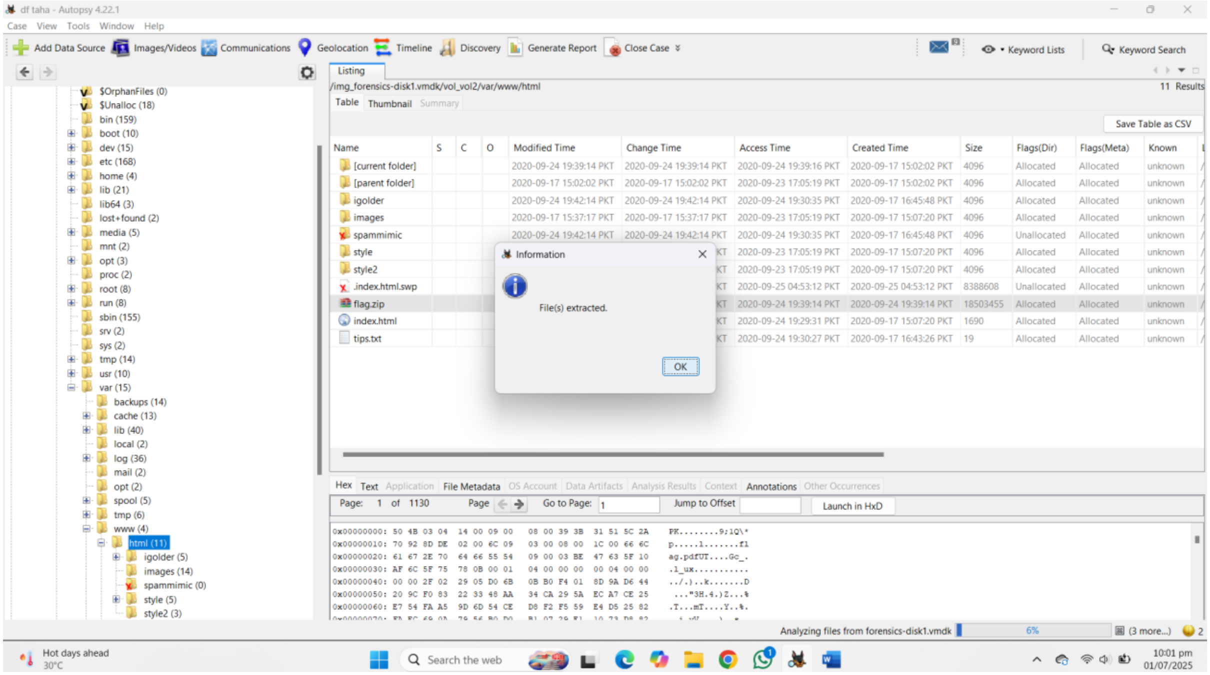


/img_forensics-disk1.vmdk/vol_vol2/var/www/html/images 14 Results

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
dna.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

```
JFIF
+Flag:1 {bc02d4ffbeeab9f57c5e03de1098ff31}
!1!%)+...
383,7(-.+
%-------+-------------------------------------------
Qa2q
$3Cc
```

I have also found flag 2 which was again in autopsy



/img_forensics-disk1.vmdk/vol_vol2/var/www/html

11 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current 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
[parent folder]				2020-09-17 15:02:02 PKT	2020-09-17 15:02:02 PKT	2020-09-23 17:05:19 PKT	2020-09-17 15:02:02 PKT	4096	Allocated	Allocated	unknown
igolder				2020-09-24 19:42:14 PKT	2020-09-24 19:42:14 PKT	2020-09-24 19:30:35 PKT	2020-09-17 16:45:48 PKT	4096	Allocated	Allocated	unknown
images				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
spammimic				2020-09-24 19:42:14 PKT	2020-09-24 19:42:14 PKT	2020-09-24 19:30:35 PKT	2020-09-17 16:45:48 PKT	4096	Unallocated	Allocated	unknown
style					KT	2020-09-23 17:05:19 PKT	2020-09-17 15:07:20 PKT	4096	Allocated	Allocated	unknown
style2					KT	2020-09-23 17:05:19 PKT	2020-09-17 15:07:20 PKT	4096	Allocated	Allocated	unknown
.index.html.swp					KT	2020-09-25 04:53:12 PKT	2020-09-25 04:53:12 PKT	8388608	Unallocated	Allocated	unknown
flag.zip					KT	2020-09-24 19:39:14 PKT	2020-09-24 19:39:14 PKT	18503455	Allocated	Allocated	unknown
index.html					KT	2020-09-24 19:29:31 PKT	2020-09-17 15:07:20 PKT	1690	Allocated	Allocated	unknown
tips.txt					KT	2020-09-24 19:30:27 PKT	2020-09-17 16:43:26 PKT	19	Allocated	Allocated	unknown

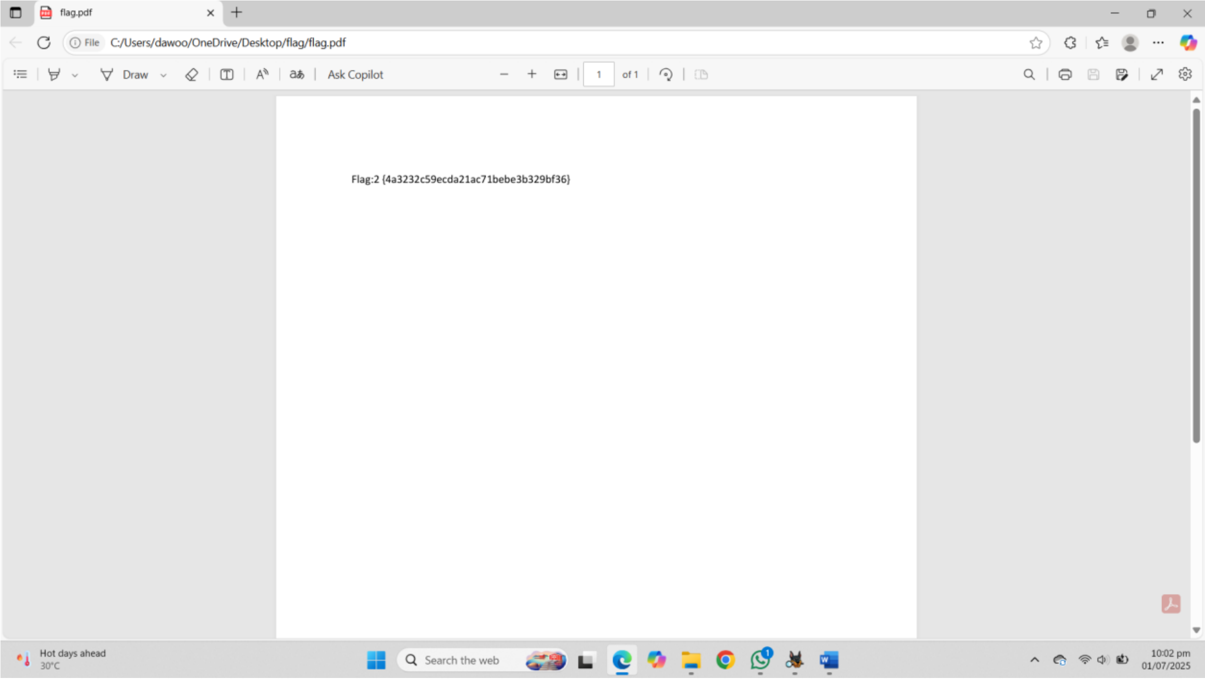
Information

File(s) extracted.

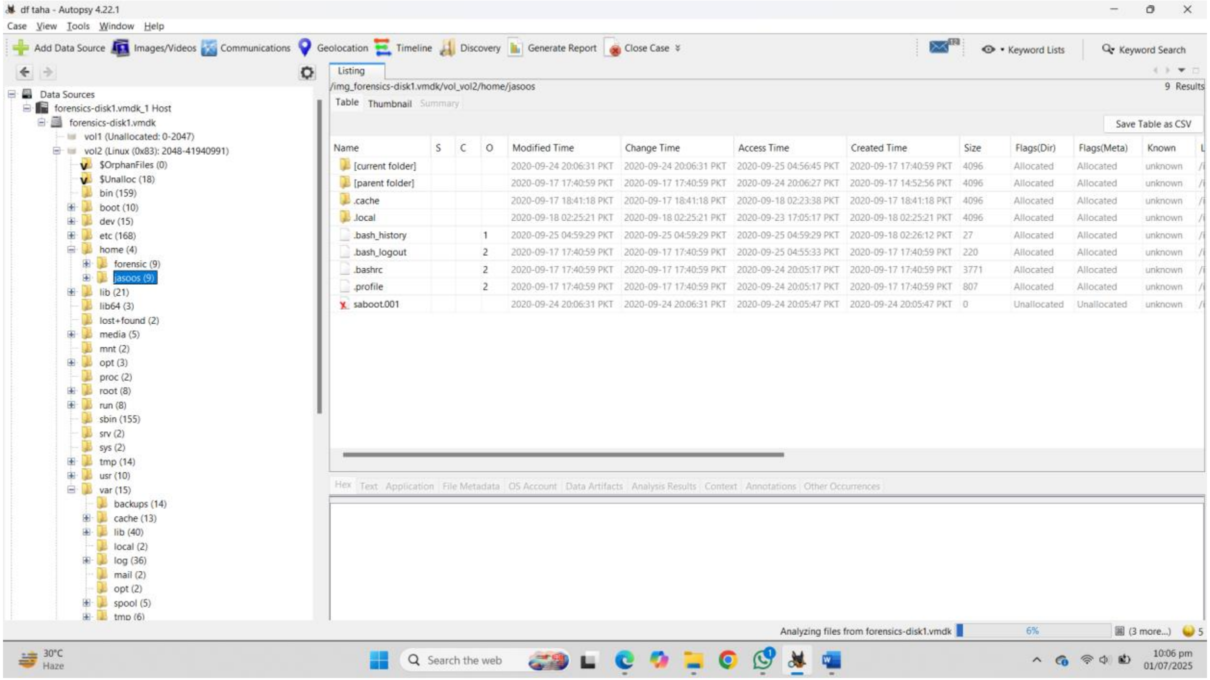
OK

Page: 1 of 1130 Page Go to Page: 1 Jump to Offset

```
0x00000000: 50 4B 03 04  14 00 09 00  08 00 39 3B  31 51 5C 2A   PK........9;1Q\*
0x00000010: 70 92 8D DE  02 00 6C 09  03 00 08 00  1C 00 66 6C   p.....l.......fl
0x00000020: 61 67 2E 70  64 66 55 54  09 00 03 BE  47 63 5F 10   ag.pdfUT....Gc_.
0x00000030: AF 6C 5F 75  78 0B 00 01  04 00 00 00  00 04 00 00   .l_ux...........
0x00000040: 00 00 2F 02  29 05 D0 6B  0B B0 F4 01  8D 9A D6 44   ../.)..k.......D
0x00000050: 20 9C F0 83  22 33 48 AA  34 CA 29 5A  EC A7 CE 25    ..."3H.4.)Z...%
0x00000060: E7 54 FA A5  9D 6D 54 CE  D8 F2 F5 59  E4 D5 25 82   .T...mT....Y..%.
```



Flag:2 {4a3232c59ecda21ac71bebe3b329bf36}



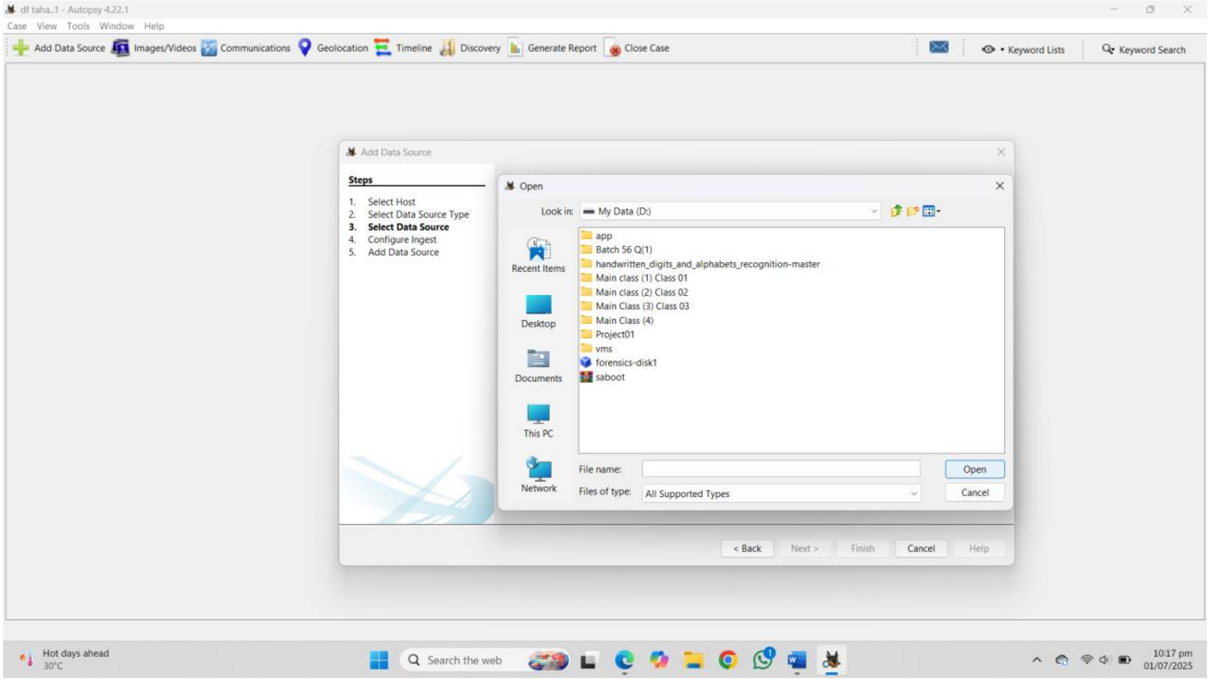
/img_forensics-disk1.vmdk/vol_vol2/home/jasoos

9 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	L
[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			1	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			2	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			2	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			2	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	/

Analyzing files from forensics-disk1.vmdk 6% (3 more...)

10:06 pm 01/07/2025



Steps

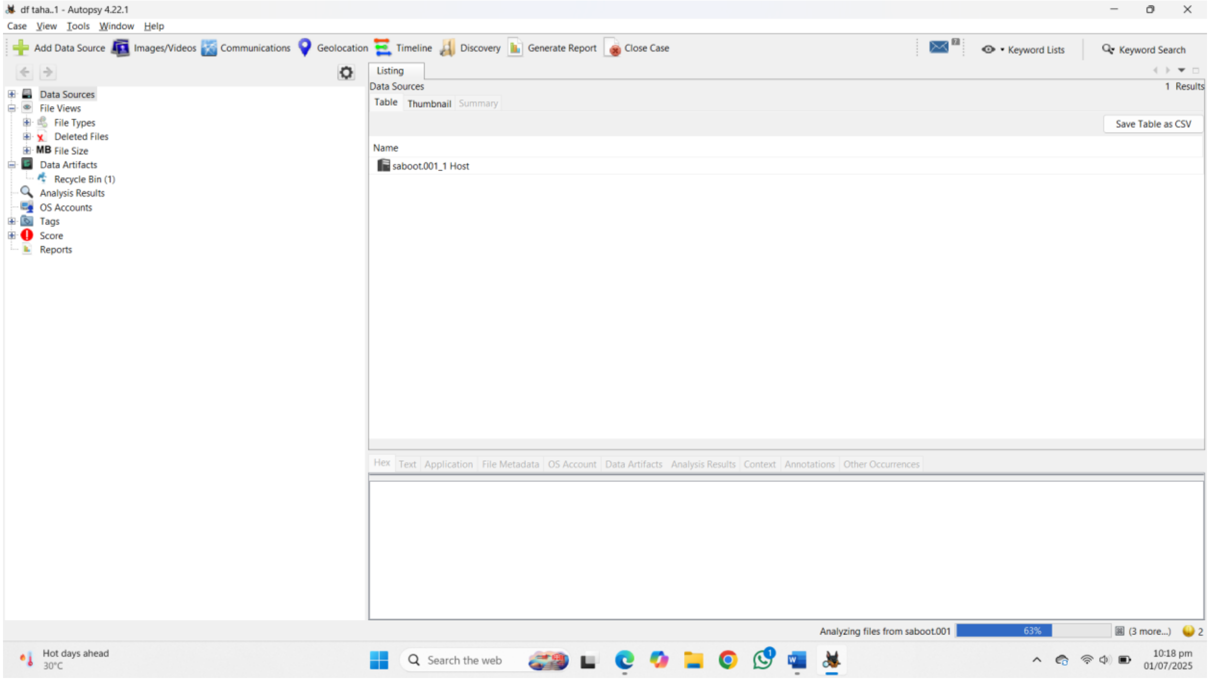
1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Look in: My Data (D:)

File name:

Files of type: All Supported Types

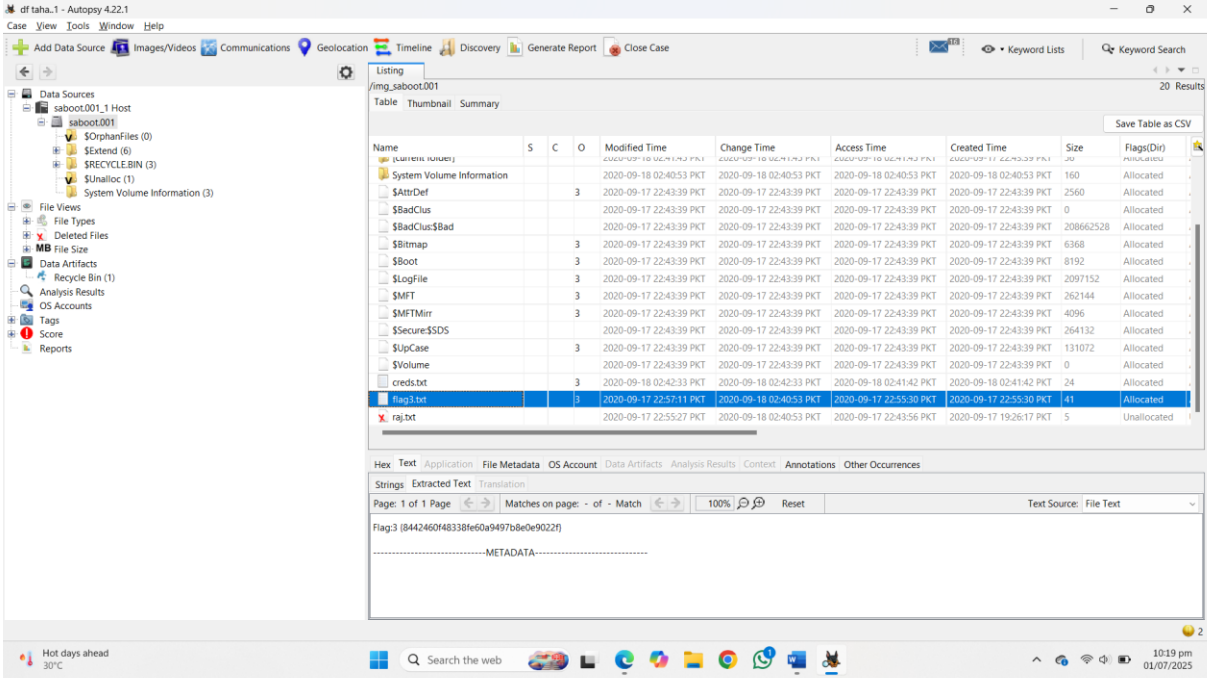
10:17 pm 01/07/2025



Data Sources 1 Results

Name
saboot.001_1 Host

I have found the flag3 in flag1.txt



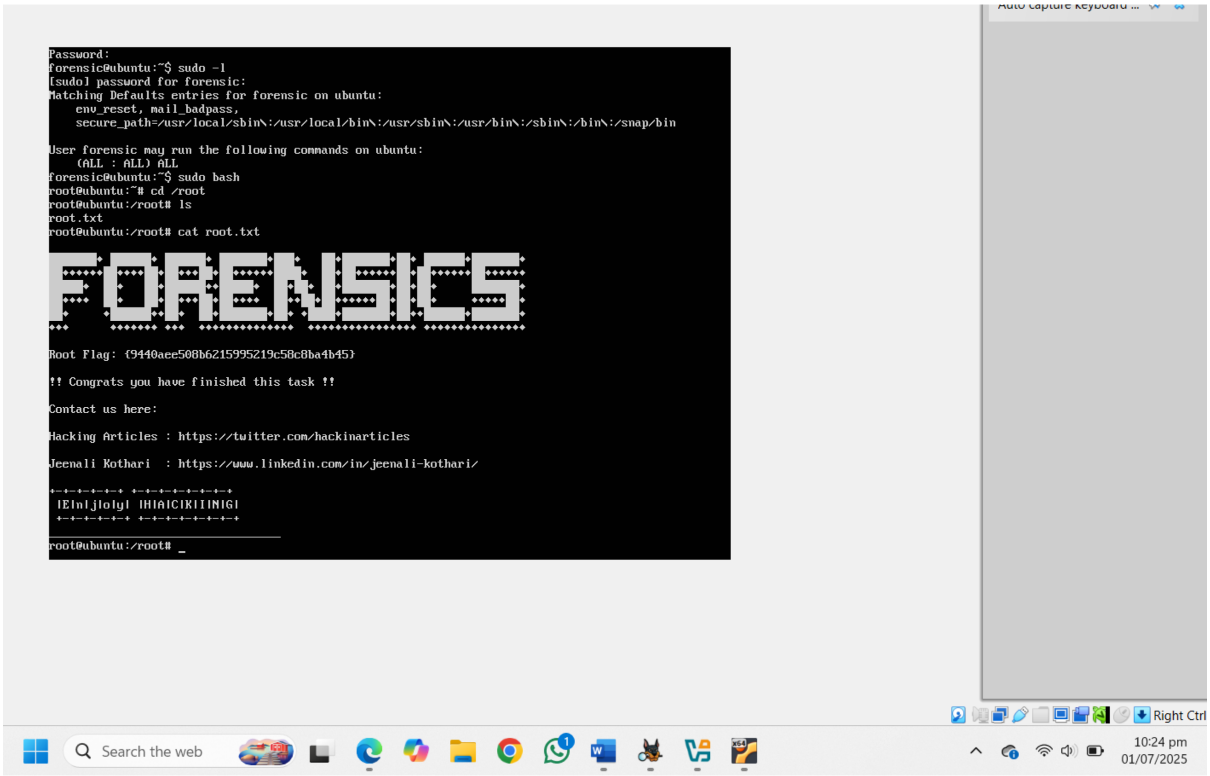
/img_saboot.001 20 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
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
$AttrDef			3	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
$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
$BadClus:$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
$Bitmap			3	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
$Boot			3	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
$LogFile			3	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
$MFT			3	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
$MFTMirr			3	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
$Secure:$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
$UpCase			3	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
$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
creds.txt			3	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
flag3.txt			3	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
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

```
Flag:3 {8442460f48338fe60a9497b8e0e9022f}

------------------------------METADATA------------------------------
```

When I decode the hashes from flag3 in base64 we have found the password which was <u>"jeenaliisagoodgirl"</u>

and when I enter the credentials I have found the flag 4 which is give below



```
Password:
forensic@ubuntu:~$ sudo -l
[sudo] password for forensic:
Matching Defaults entries for forensic on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User forensic may run the following commands on ubuntu:
    (ALL : ALL) ALL
forensic@ubuntu:~$ sudo bash
root@ubuntu:~# cd /root
root@ubuntu:/root# ls
root.txt
root@ubuntu:/root# cat root.txt

FORENSICS

Root Flag: {9440aee508b6215995219c58c8ba4b45}

!! Congrats you have finished this task !!

Contact us here:

Hacking Articles : https://twitter.com/hackinarticles

Jeenali Kothari  : https://www.linkedin.com/in/jeenali-kothari/

+-+-+-+-+-+ +-+-+-+-+-+-+-+
 |E|n|j|o|y| |H|A|C|K|I|N|G|
 +-+-+-+-+-+ +-+-+-+-+-+-+-+
__________________________________
root@ubuntu:/root# _
```

Conclusion

I have solved the ctf by using the autopsy and basically I have done the reverse engineering to find the flags which was give in the scenario