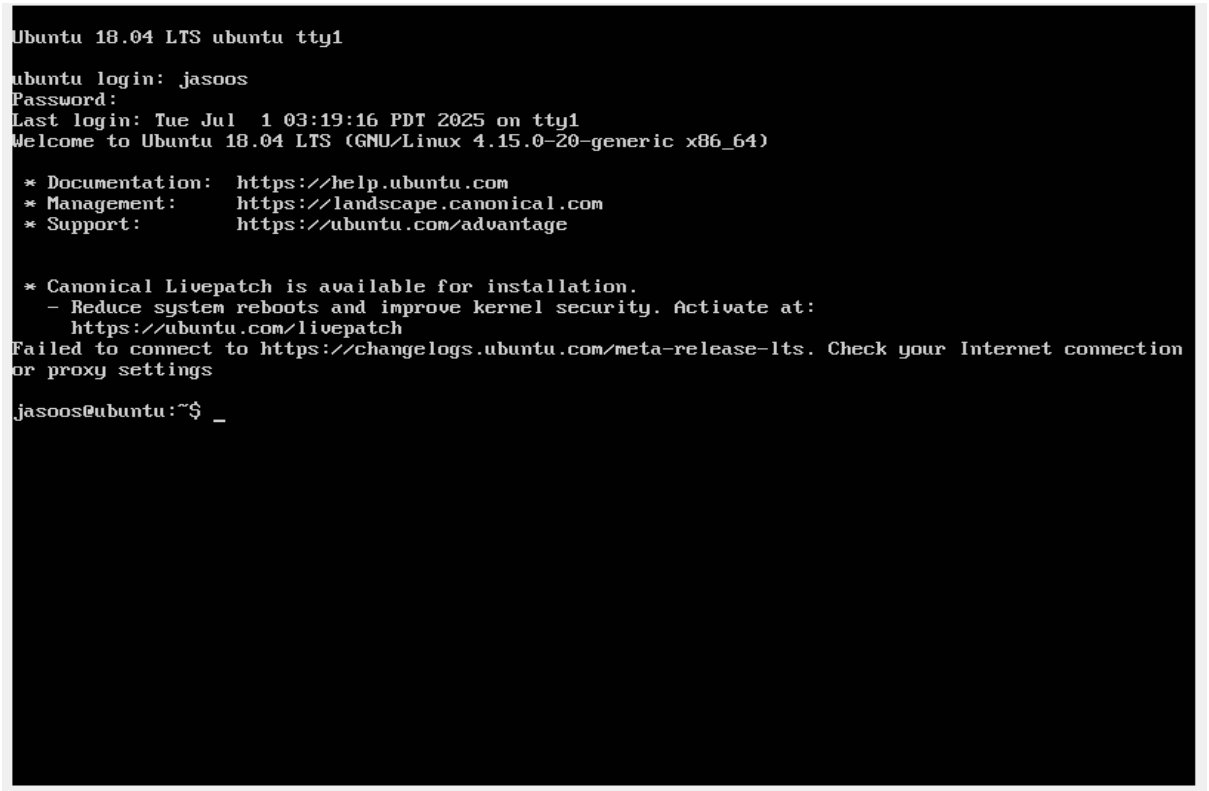
LAB EXAM DF

Description

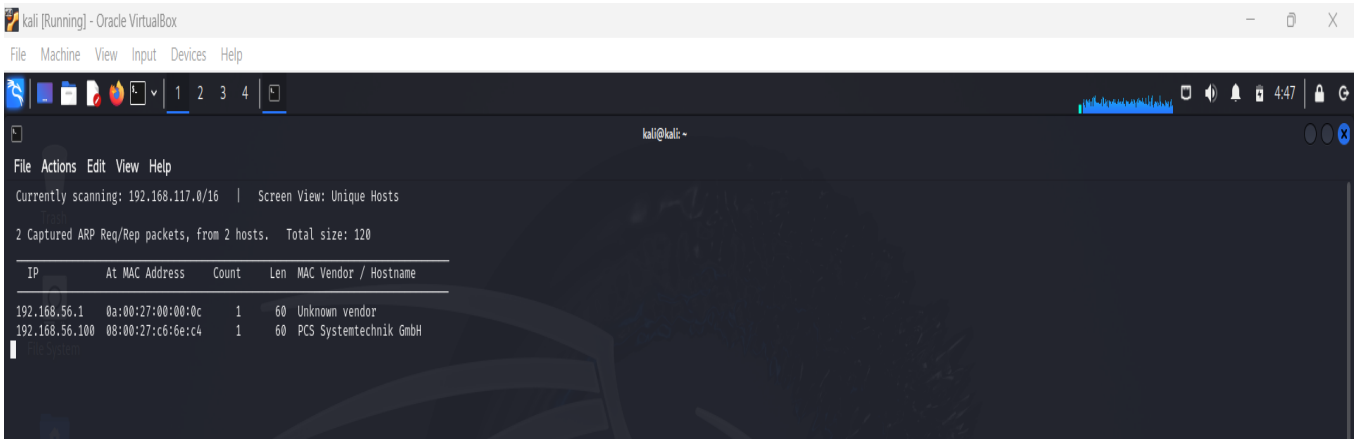
HA: Forensics is an intermediate level of the lab, which gives you a hand on real-life experience in Cyber Forensic Investigation. This lab is completely dedicated to methods and tools of Cyber Forensic Investigation and there is evidence that can be found with various techniques. As it is a Capture-the-Flag, 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

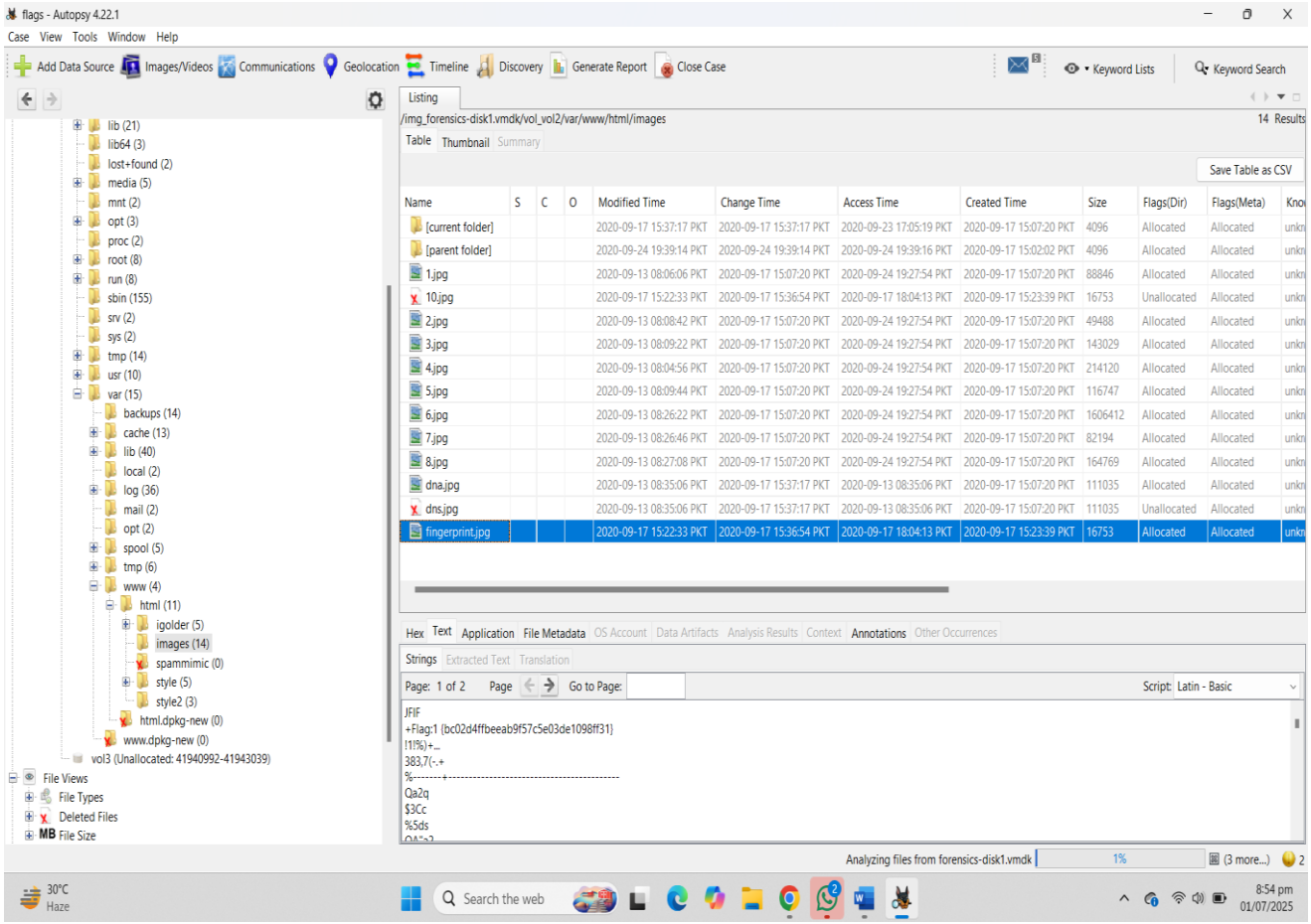
Screen short

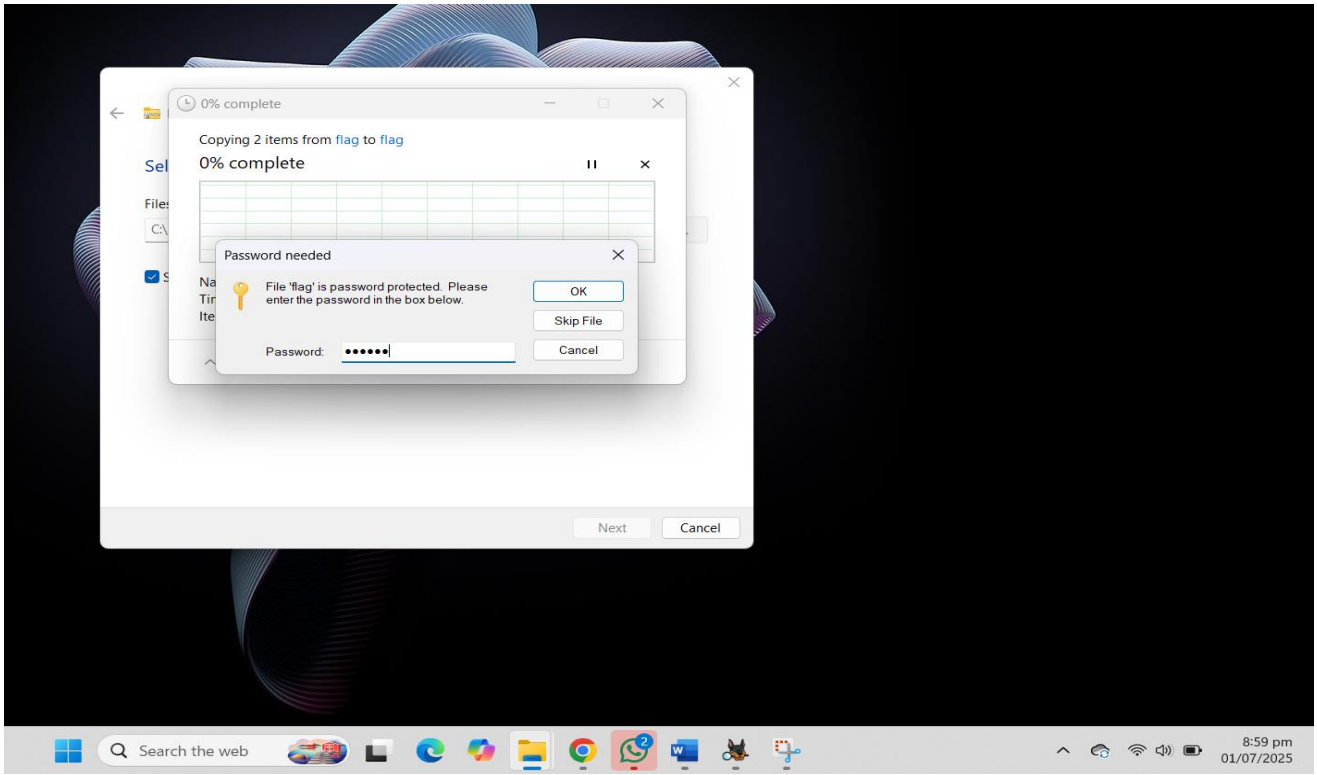


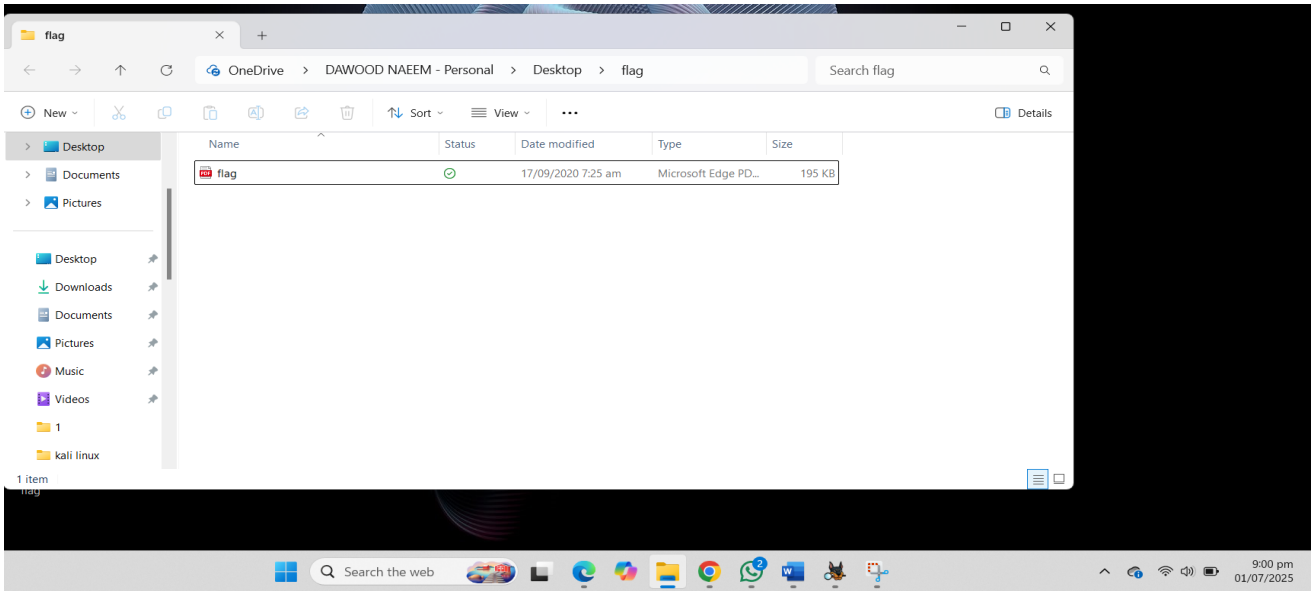
Using netdiscover command



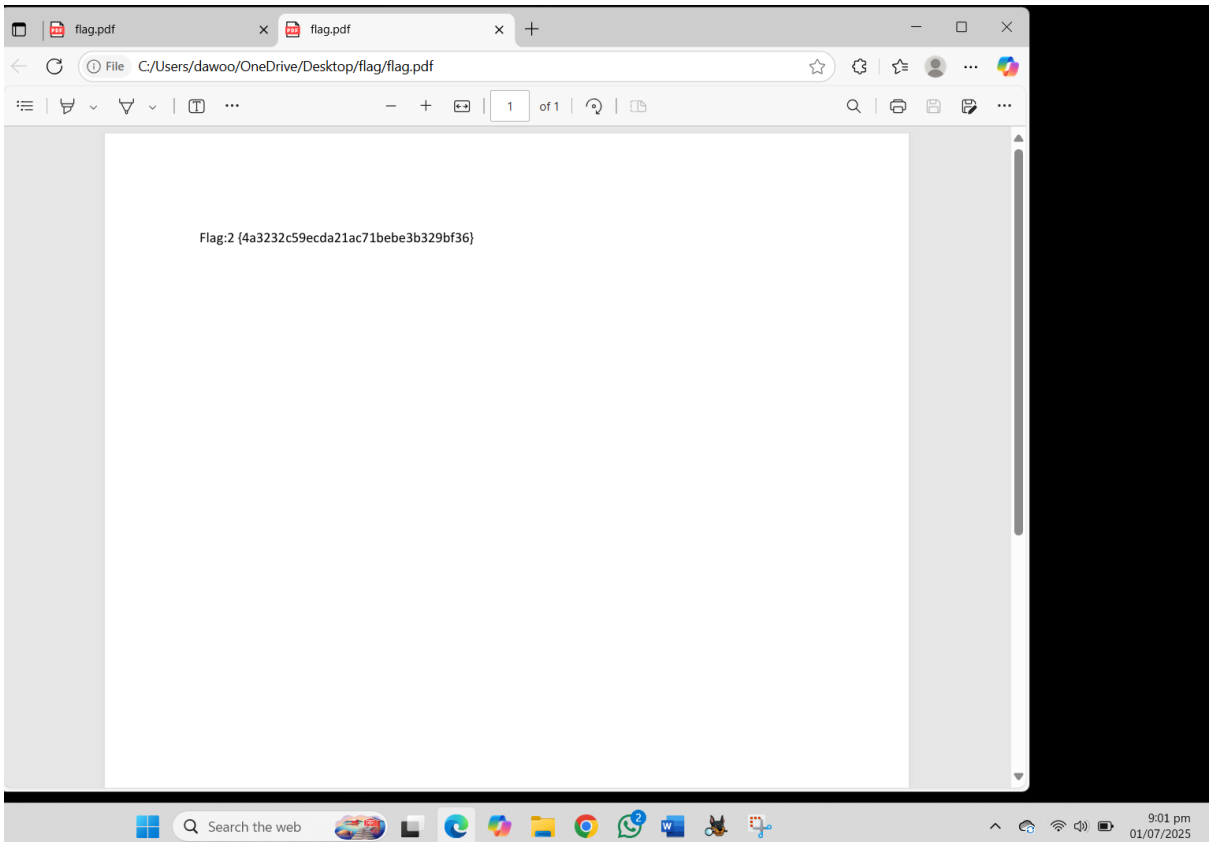
Found Flag 1 In the File Fingerprint.txt

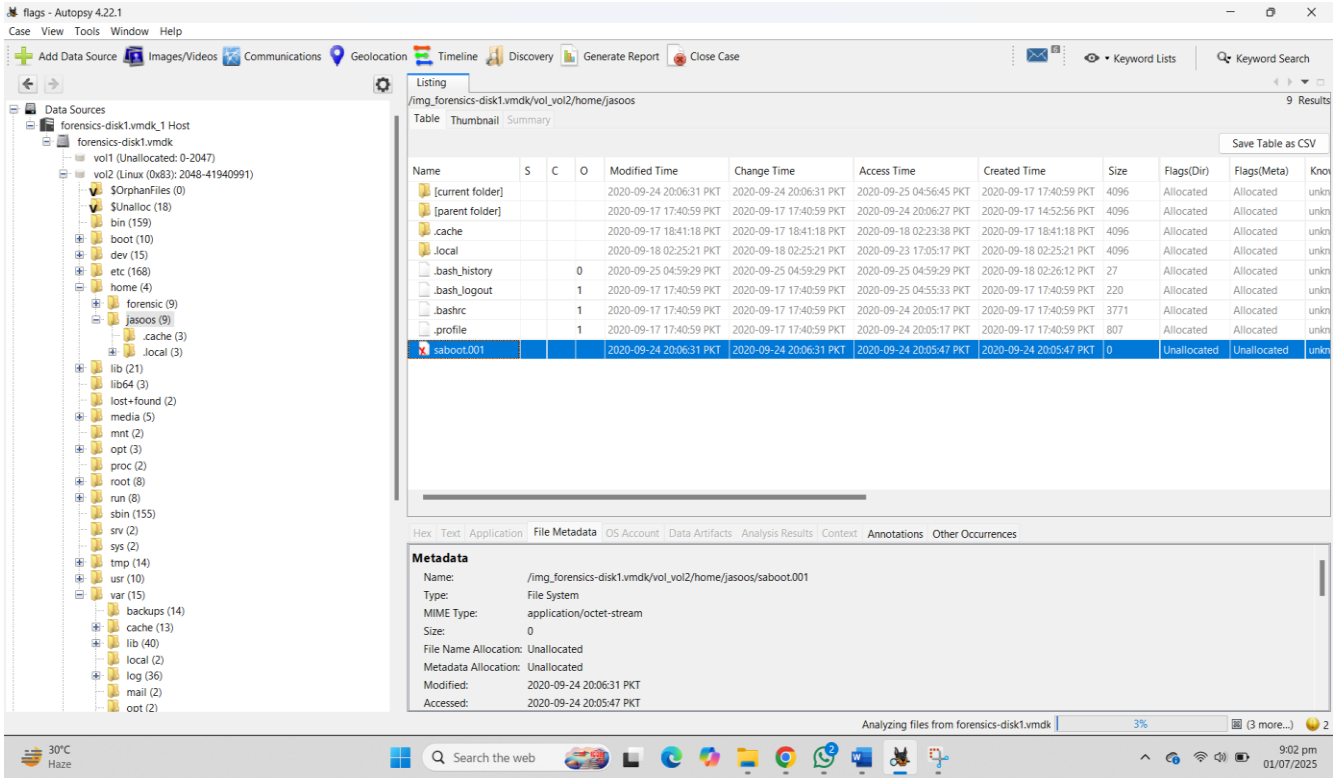


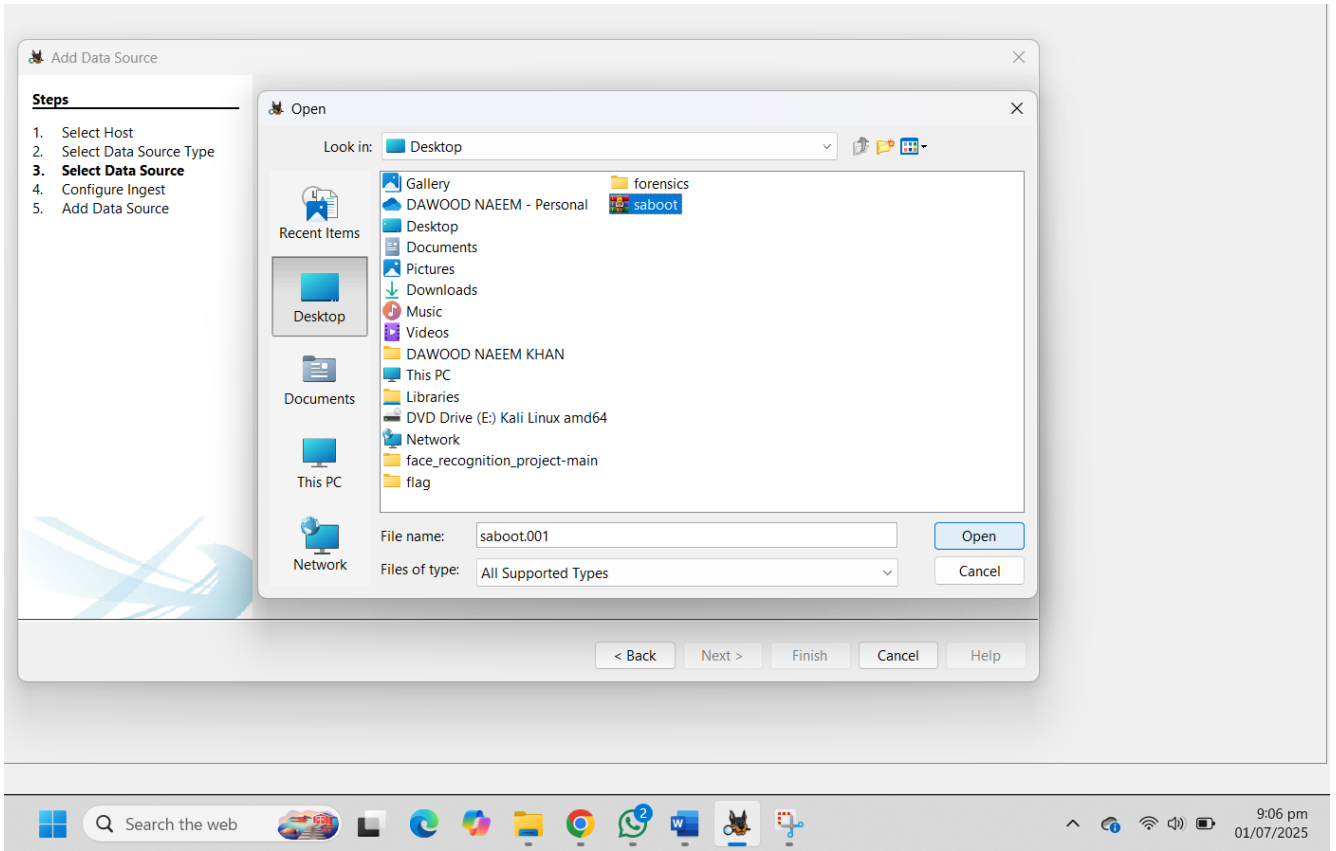


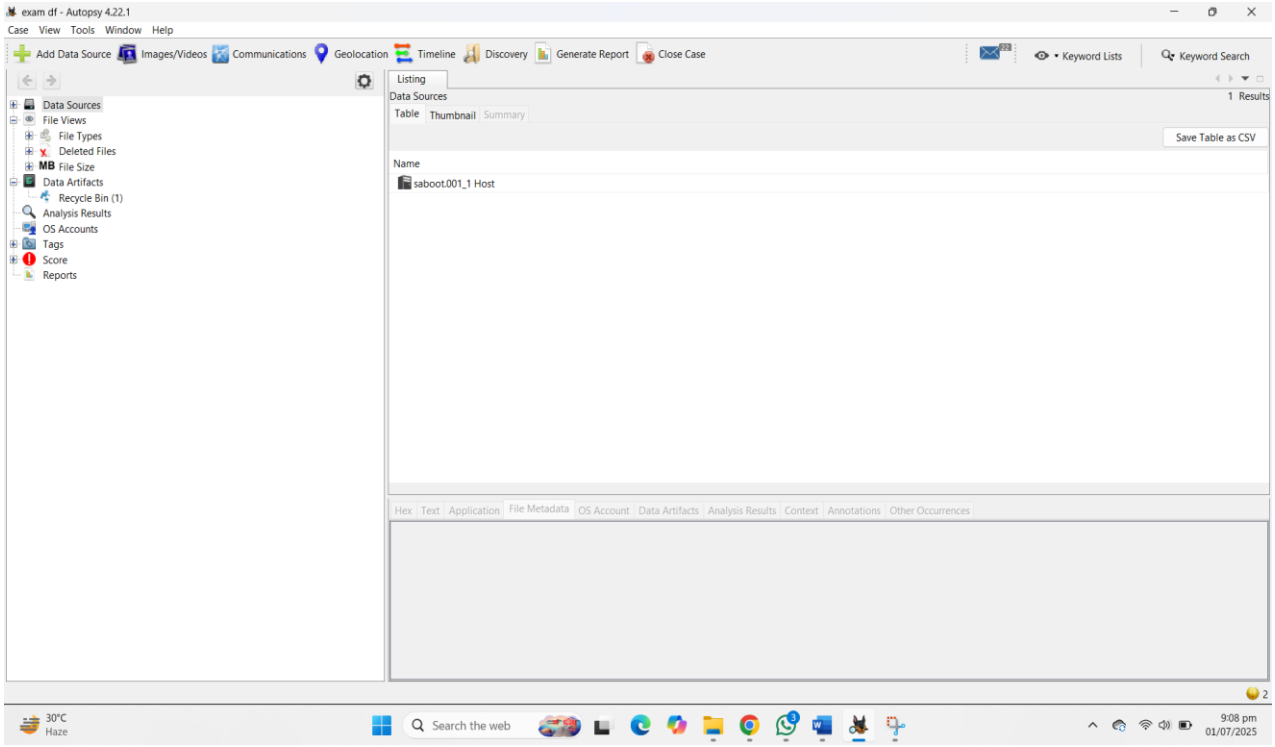


Found flag 2 hidden in a pdf file

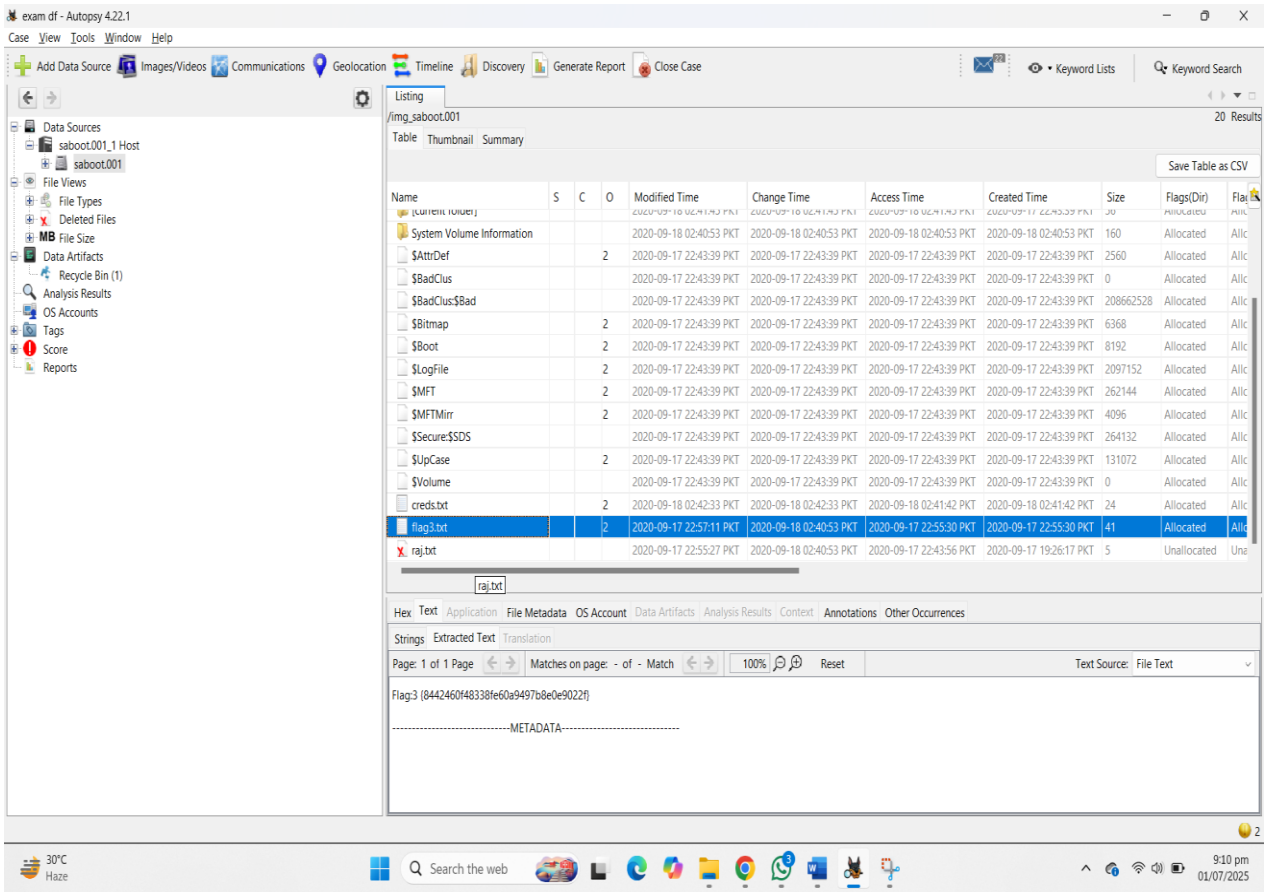



flags - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
forensics-disk1.vmdk_1 Host
forensics-disk1.vmdk
vol1 (Unallocated: 0-2047)
vol2 (Linux (0x83): 2048-41940991)
$OrphanFiles (0)
$Unalloc (18)
bin (159)
boot (10)
dev (15)
etc (168)
home (4)
forensic (9)
jasoos (9)
.cache (3)
.local (3)
lib (21)
lib64 (3)
lost+found (2)
media (5)
mnt (2)
opt (3)
proc (2)
root (8)
run (8)
sbin (155)
srv (2)
sys (2)
tmp (14)
usr (10)
var (15)
backups (14)
cache (13)
lib (40)
local (2)
log (36)
mail (2)
opt (2)
Listing
/img_forensics-disk1.vmdk/vol_vol2/home/jasoos
9 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta)
[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
[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
.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
.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
.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
.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
.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
.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
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
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Metadata
Name: /img_forensics-disk1.vmdk/vol_vol2/home/jasoos/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

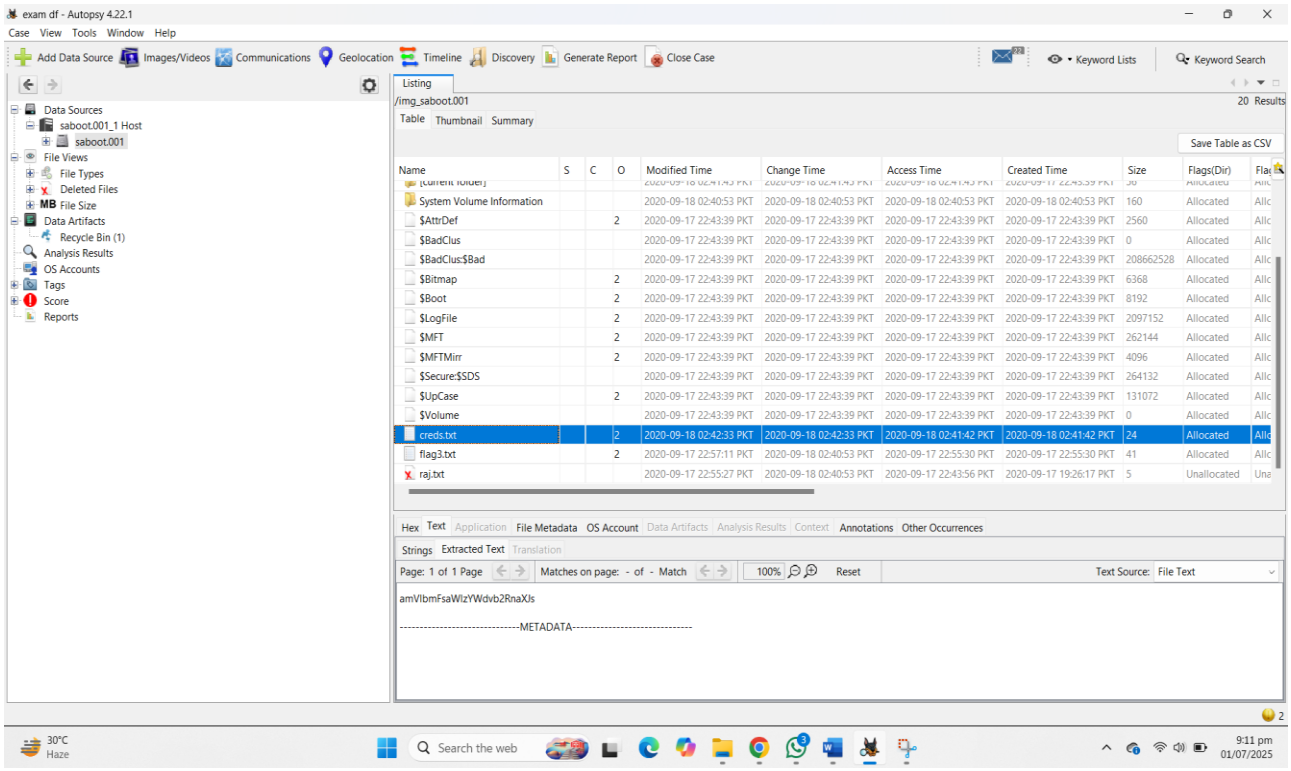

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Open
Look in: Desktop
Recent Items
Desktop
Documents
This PC
Network
Gallery
DAWOOD NAEEM - Personal
Desktop
Documents
Pictures
Downloads
Music
Videos
DAWOOD NAEEM KHAN
This PC
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
Search the web
9:06 pm 01/07/2025

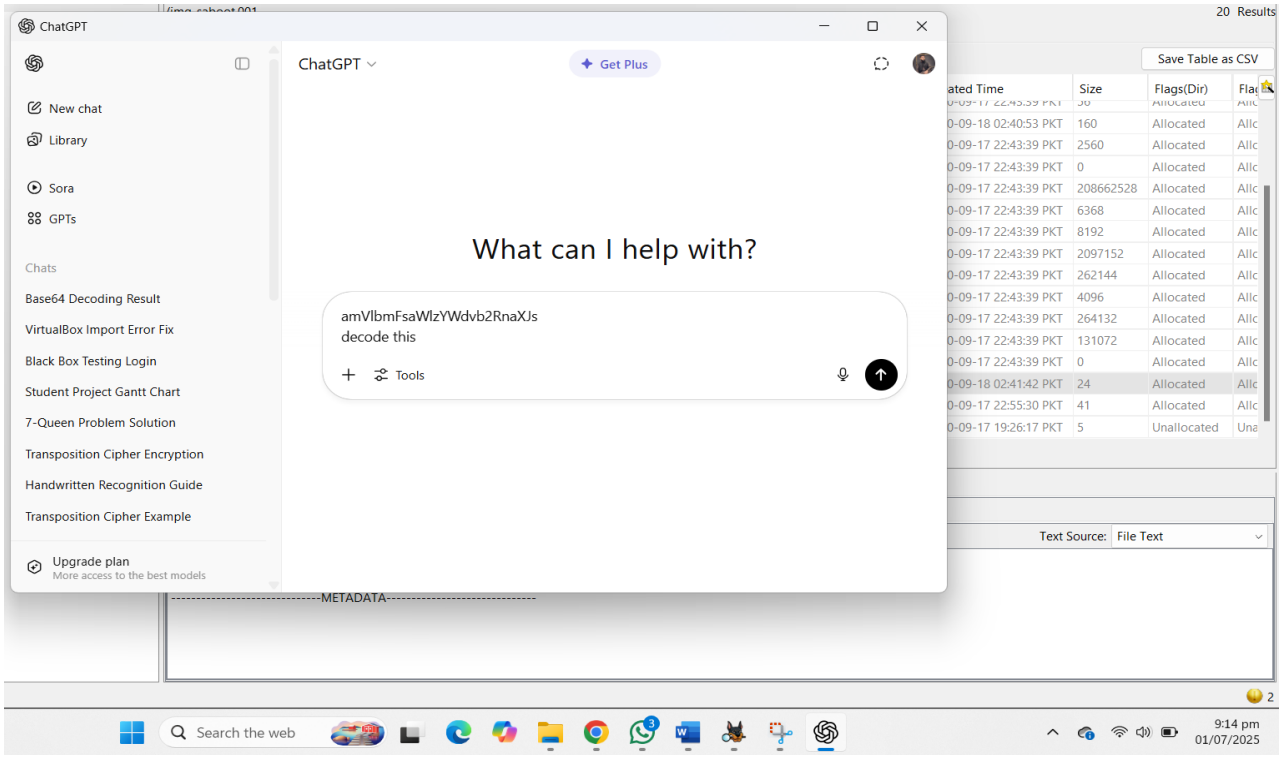


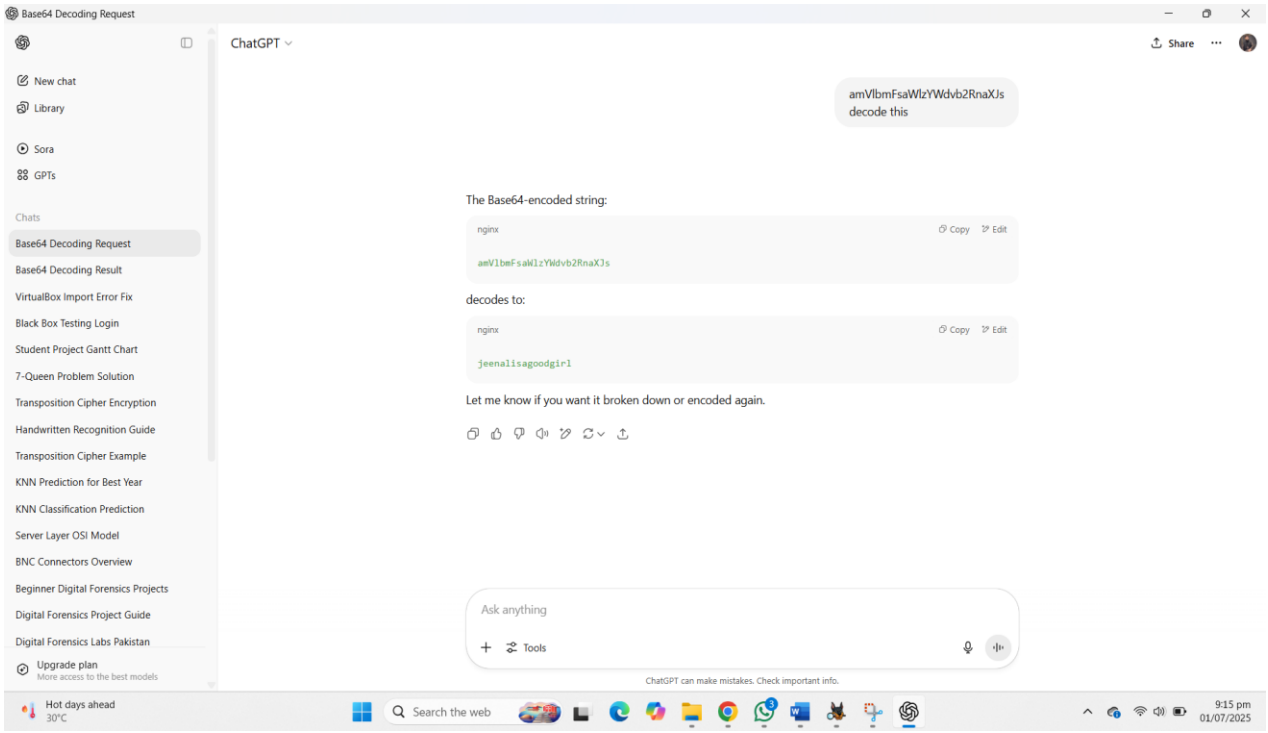
Flag 3 was found in saboot.001 -> flag3.txt

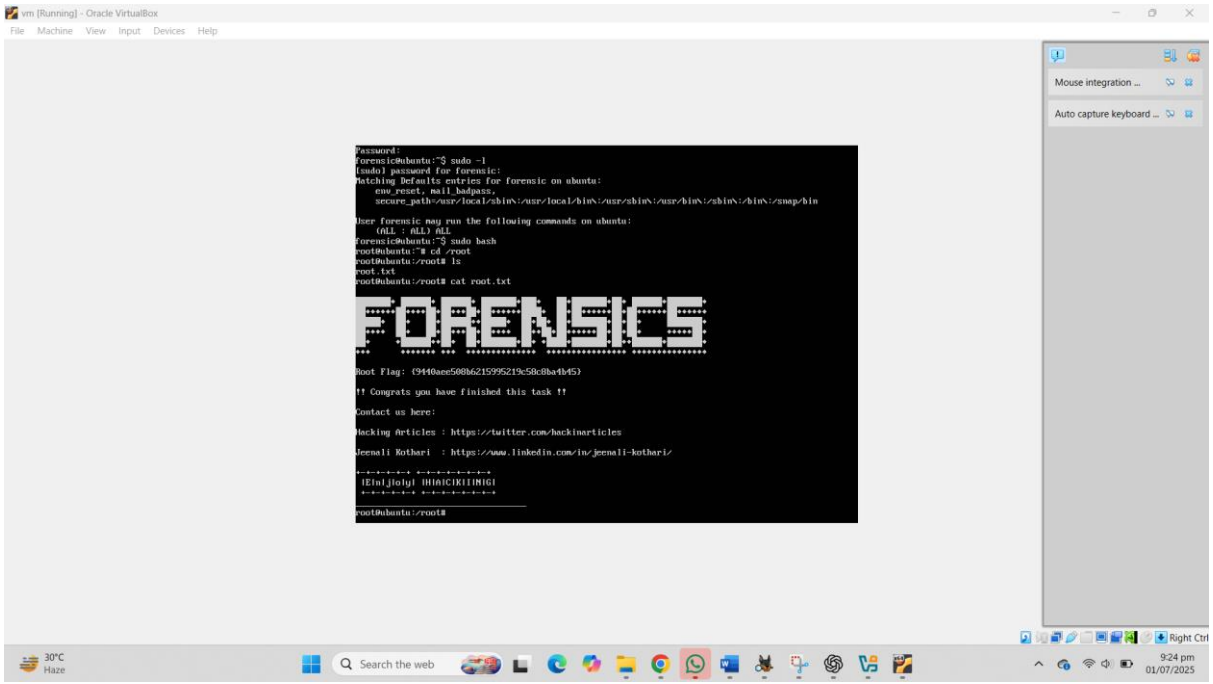


For flag 4, we found a creds.txt where we found a base 64 encoded hash. We decoded that hash using chatgpt. Then in the Ubuntu system we followed the walkthrough from medium and found flag 4.






Base64 Decoding Request
ChatGPT
Share
New chat
Library
Sora
GPTs
Chats
Base64 Decoding Request
Base64 Decoding Result
VirtualBox Import Error Fix
Black Box Testing Login
Student Project Gantt Chart
7-Queen Problem Solution
Transposition Cipher Encryption
Handwritten Recognition Guide
Transposition Cipher Example
KNN Prediction for Best Year
KNN Classification Prediction
Server Layer OSI Model
BNC Connectors Overview
Beginner Digital Forensics Projects
Digital Forensics Project Guide
Digital Forensics Labs Pakistan
Upgrade plan
More access to the best models
amVlbmFsaWlzYWdvb2RnaXJs
decode this
The Base64-encoded string:
nginx
Copy
Edit
amVlbmFsaWlzYWdvb2RnaXJs
decodes to:
nginx
Copy
Edit
jeenalisagoodgirl
Let me know if you want it broken down or encoded again.
Ask anything
Tools
ChatGPT can make mistakes. Check important info.
Hot days ahead
30°C
Search the web
9:15 pm
01/07/2025


vm [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
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/
root@ubuntu:/root#
Right Ctrl
30°C
Haze
Search the web
9:24 pm
01/07/2025