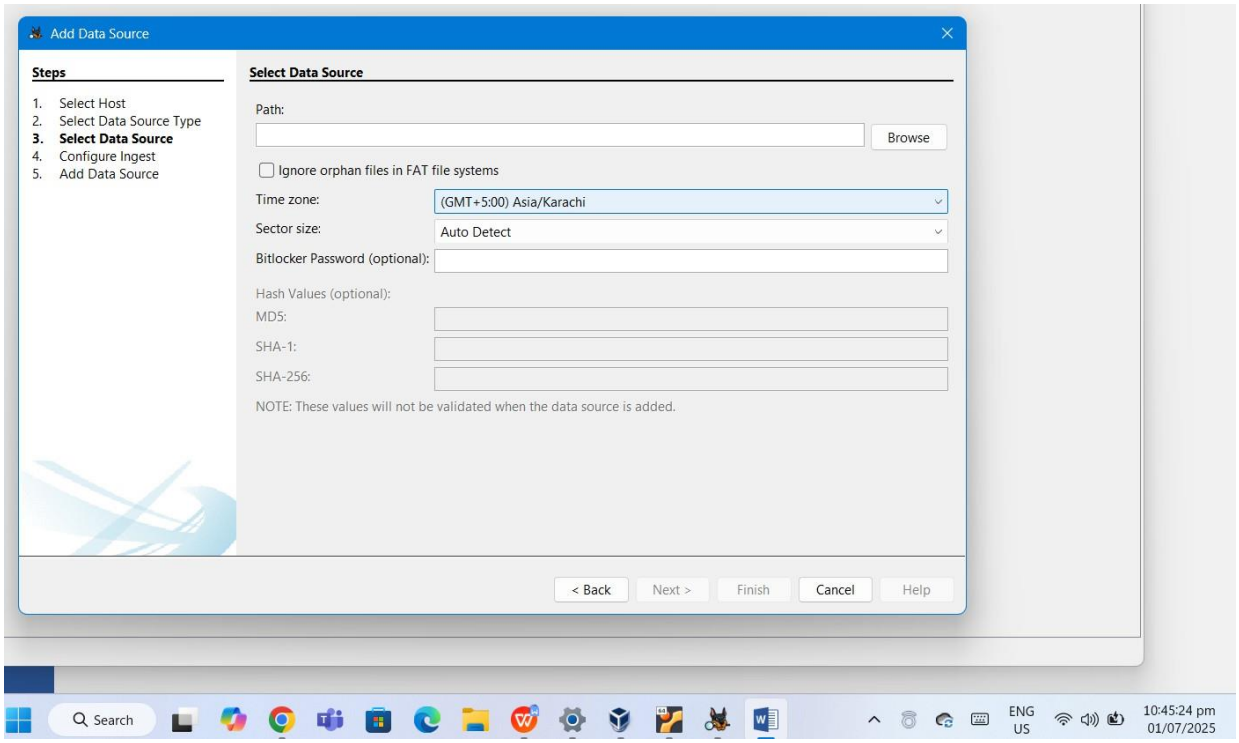
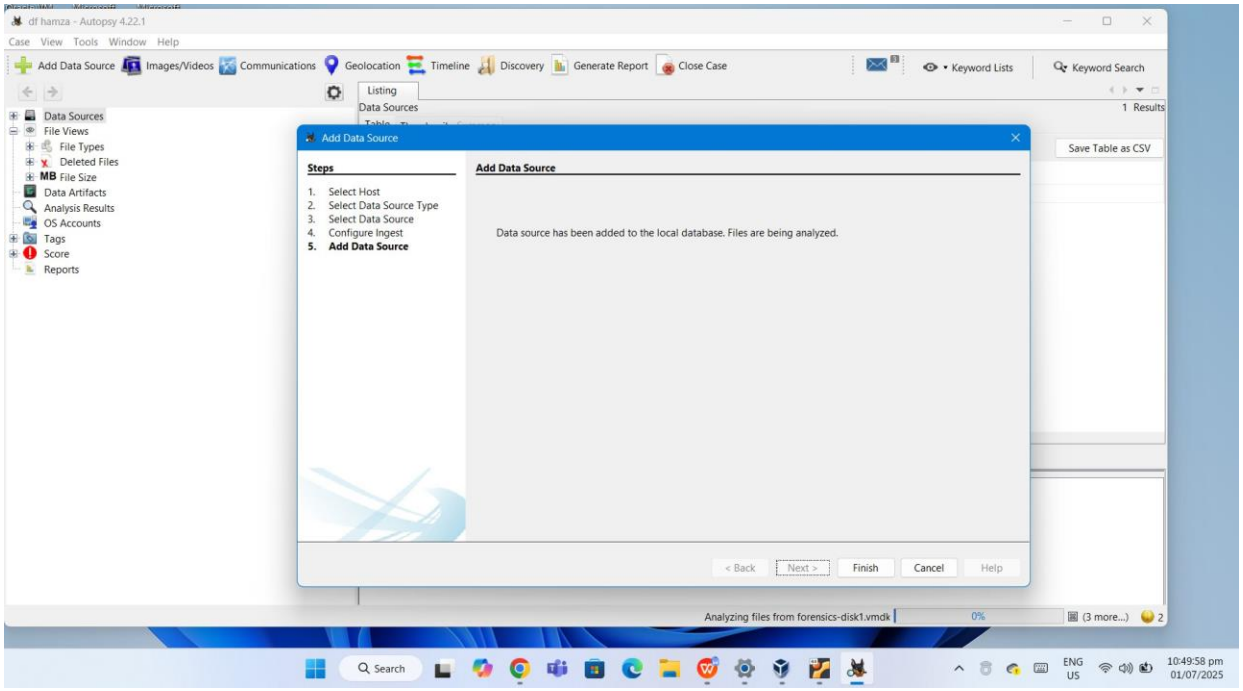
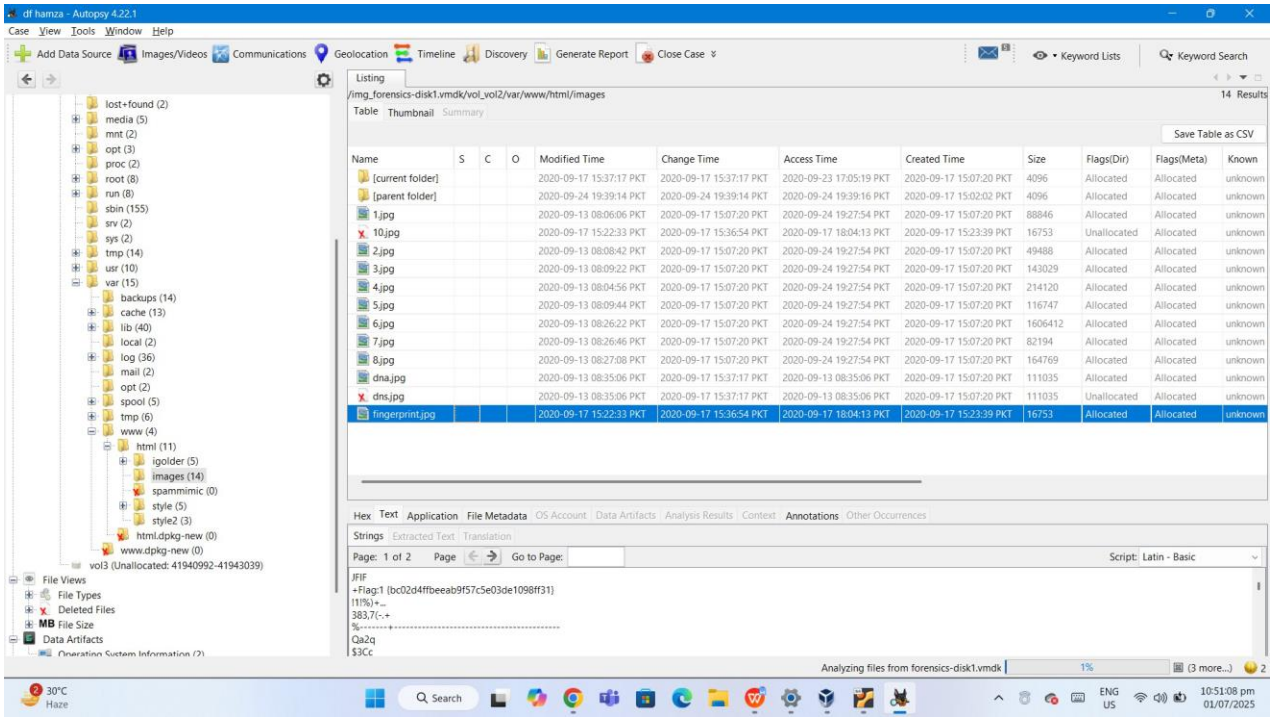
LAB EXAM DIGITAL FORENSICS

First we find flag 1:

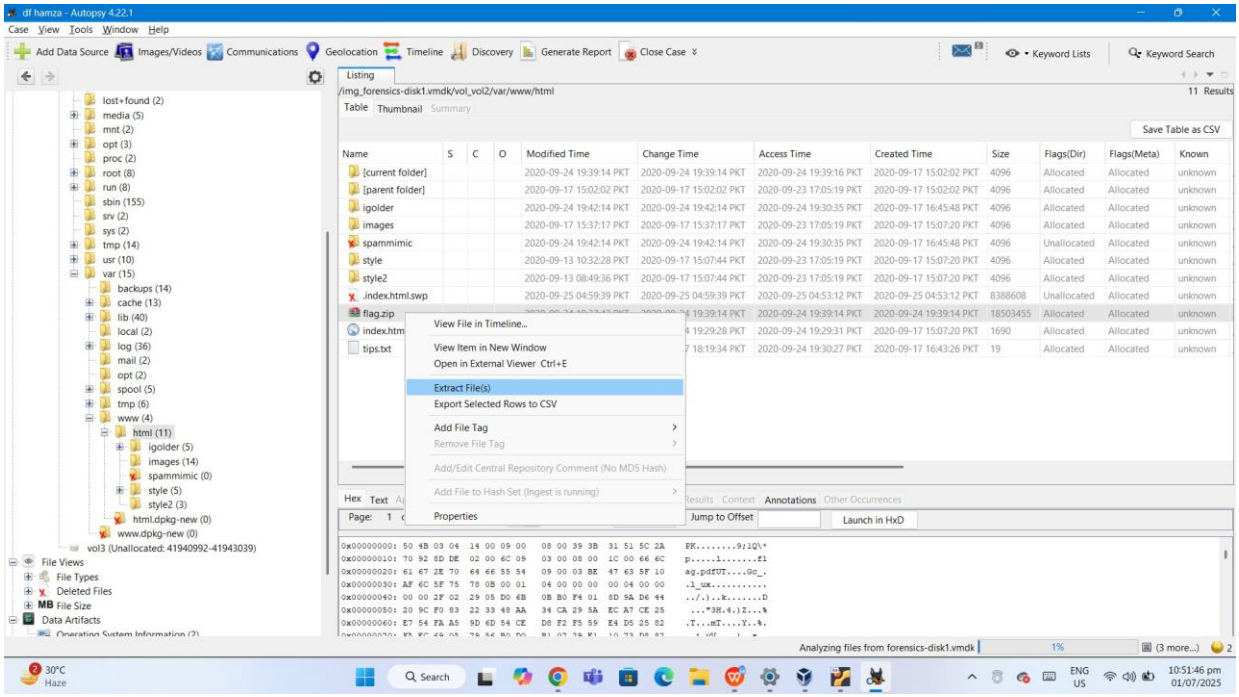


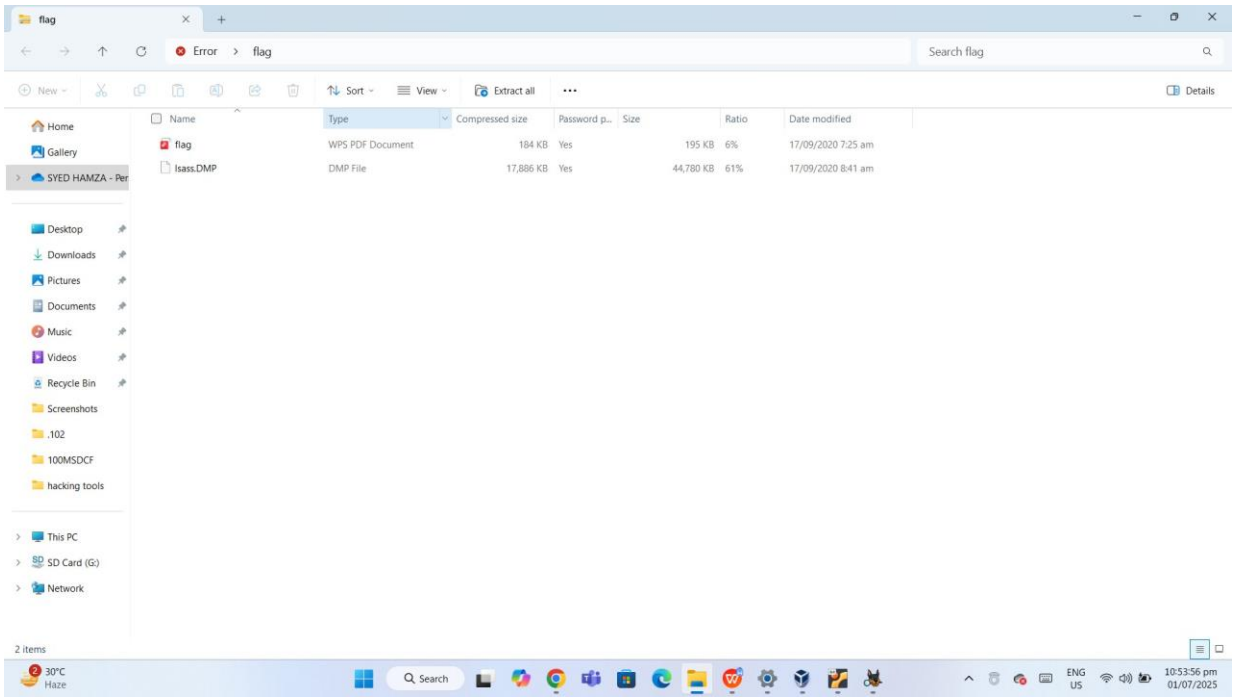


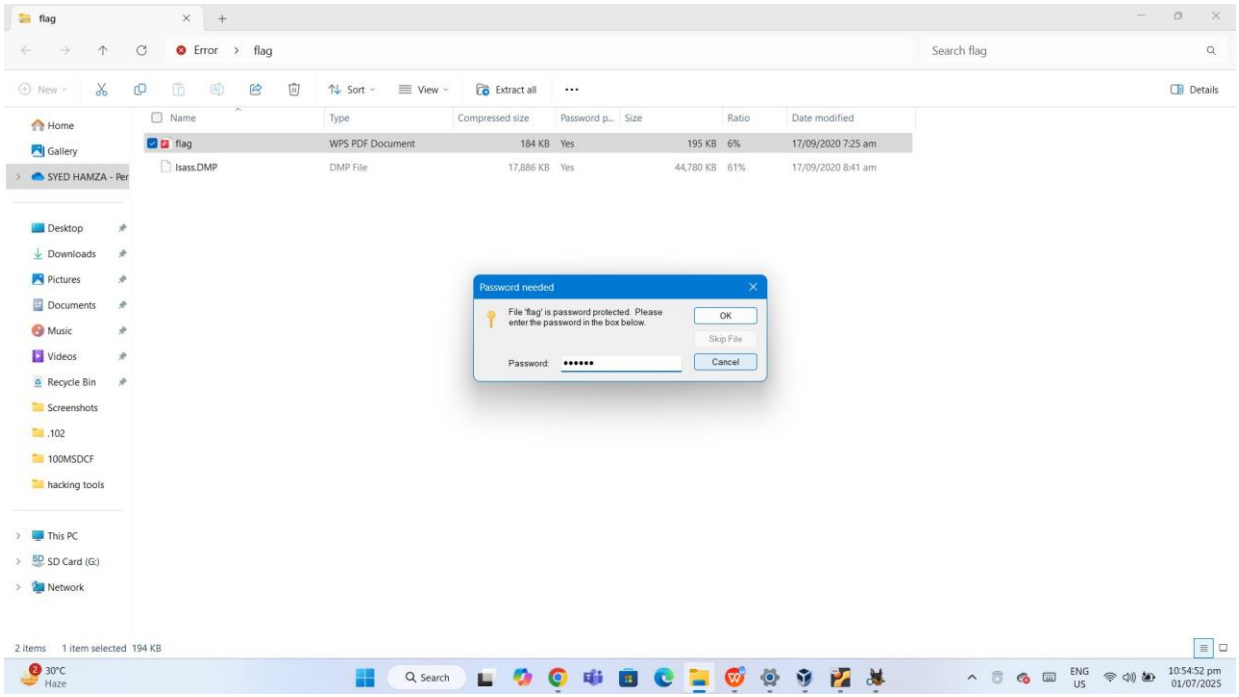
Flag 1 Found:



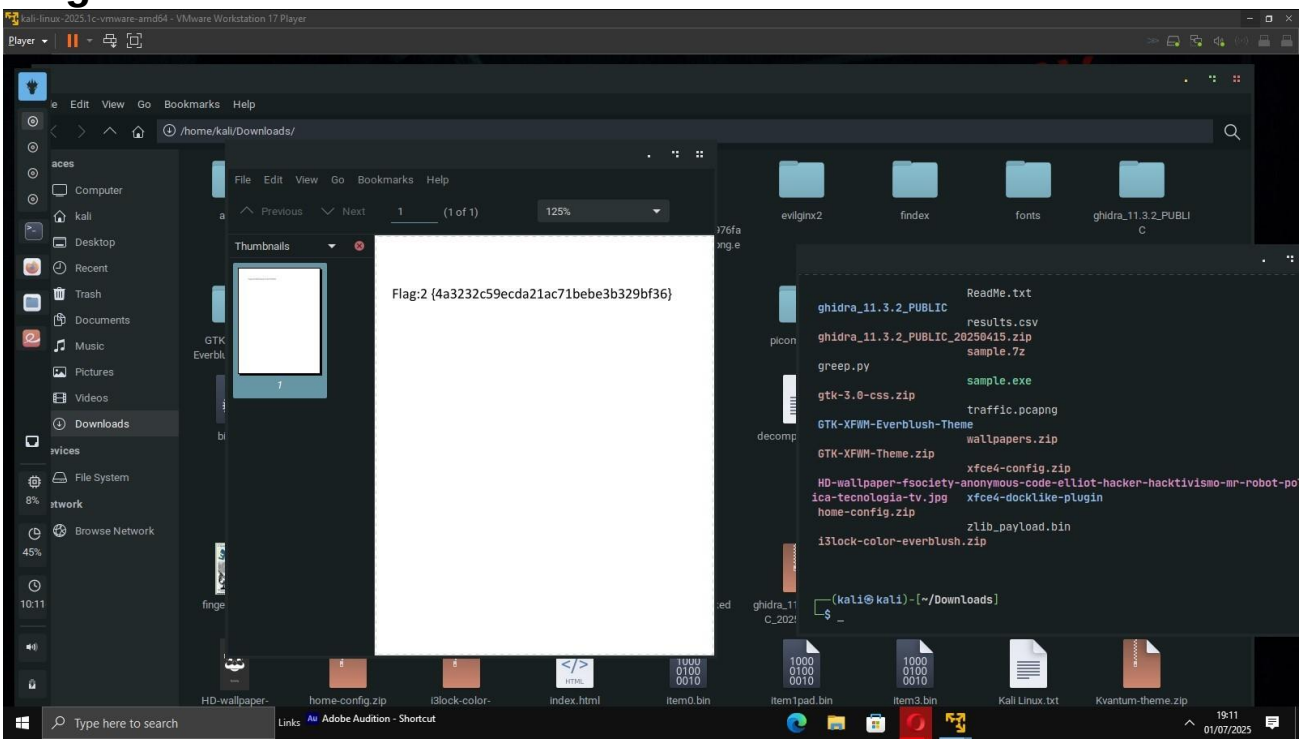
Extract File

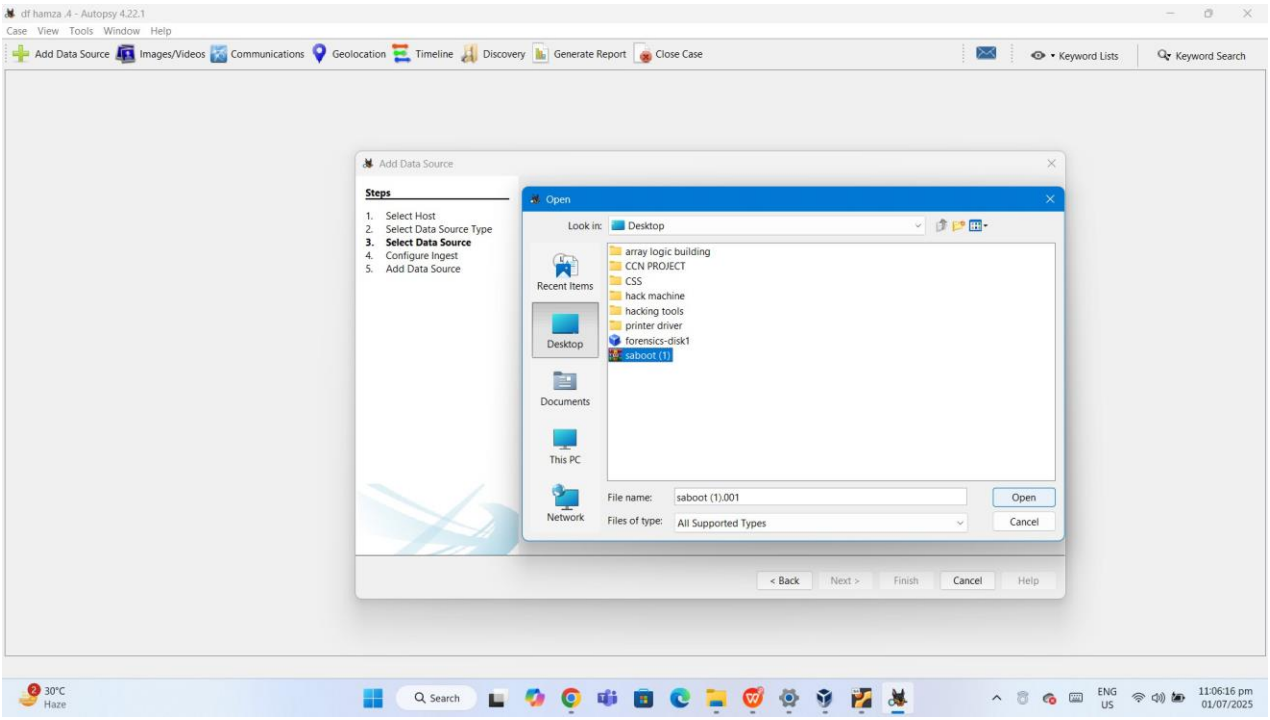

df hamza - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
/img_forensics-disk1.vmdk/vol_vol2/var/www/html
11 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
Known
[current folder]
[parent folder]
igolder
images
spammimic
style
style2
.index.html.swp
flag.zip
index.htm
tips.txt
View File in Timeline...
View Item in New Window
Open in External Viewer Ctrl+E
Extract File(s)
Export Selected Rows to CSV
Add File Tag
Remove File Tag
Add/Edit Central Repository Comment (No MD5 Hash)
Add File to Hash Set (Ingest is running)
Properties
Hex
Text
Annotations
Other Occurrences
Page:
Jump to Offset
Launch in HxD
Analyzing files from forensics-disk1.vmdk
1%
30°C
Haze
Search
ENG
US
10:51:46 pm
01/07/2025

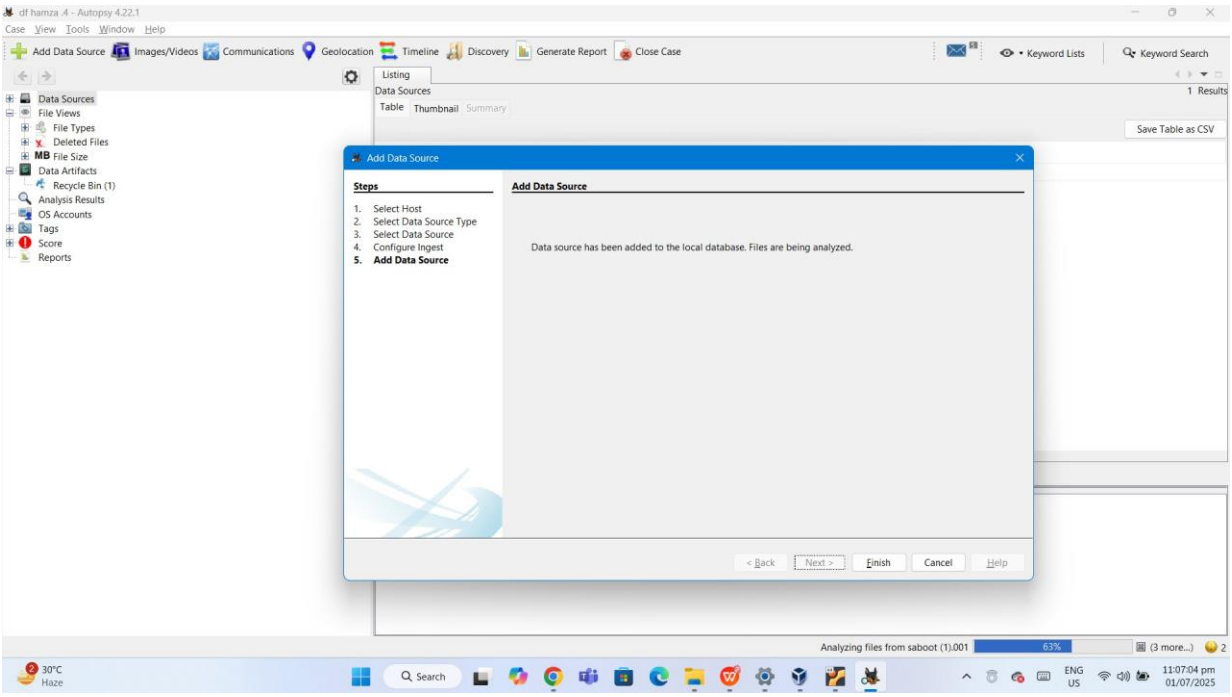

flag
Error
flag
Search flag
New
Sort
View
Extract all
Details
Home
Gallery
SYED HAMZA - Per
Desktop
Downloads
Pictures
Documents
Music
Videos
Recycle Bin
Screenshots
.102
100MSDCF
hacking tools
This PC
SD Card (G:)
Network
Name
Type
Compressed size
Password p...
Size
Ratio
Date modified
flag
WPS PDF Document
184 KB
Yes
195 KB
6%
17/09/2020 7:25 am
lsass.DMP
DMP File
17,886 KB
Yes
44,780 KB
61%
17/09/2020 8:41 am
2 items
30°C
Haze
Search
ENG
US
10:53:56 pm
01/07/2025


flag
Error › flag
Search flag
Name
Type
Compressed size
Password p...
Size
Ratio
Date modified
flag
WPS PDF Document
184 KB
Yes
195 KB
6%
17/09/2020 7:25 am
lsass.DMP
DMP File
17,886 KB
Yes
44,780 KB
61%
17/09/2020 8:41 am
Password needed
File 'flag' is password protected. Please enter the password in the box below.
OK
Skip File
Password:
Cancel
2 items
1 item selected 194 KB

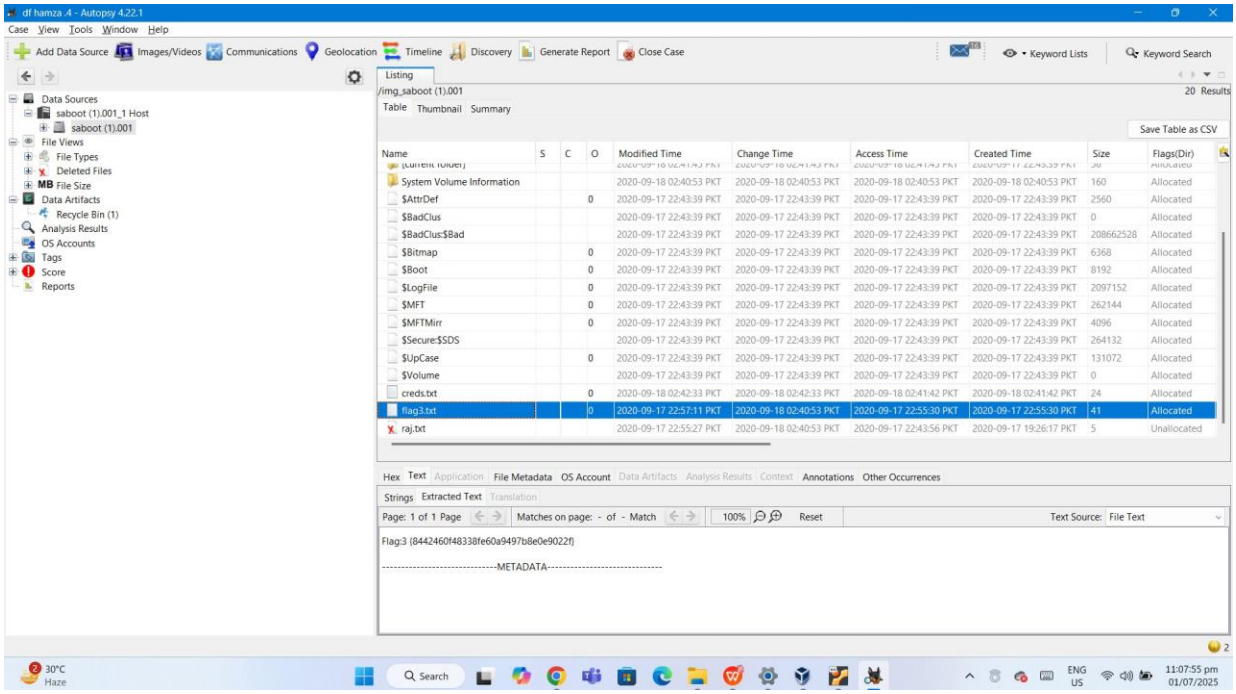
Flag 2 Found:

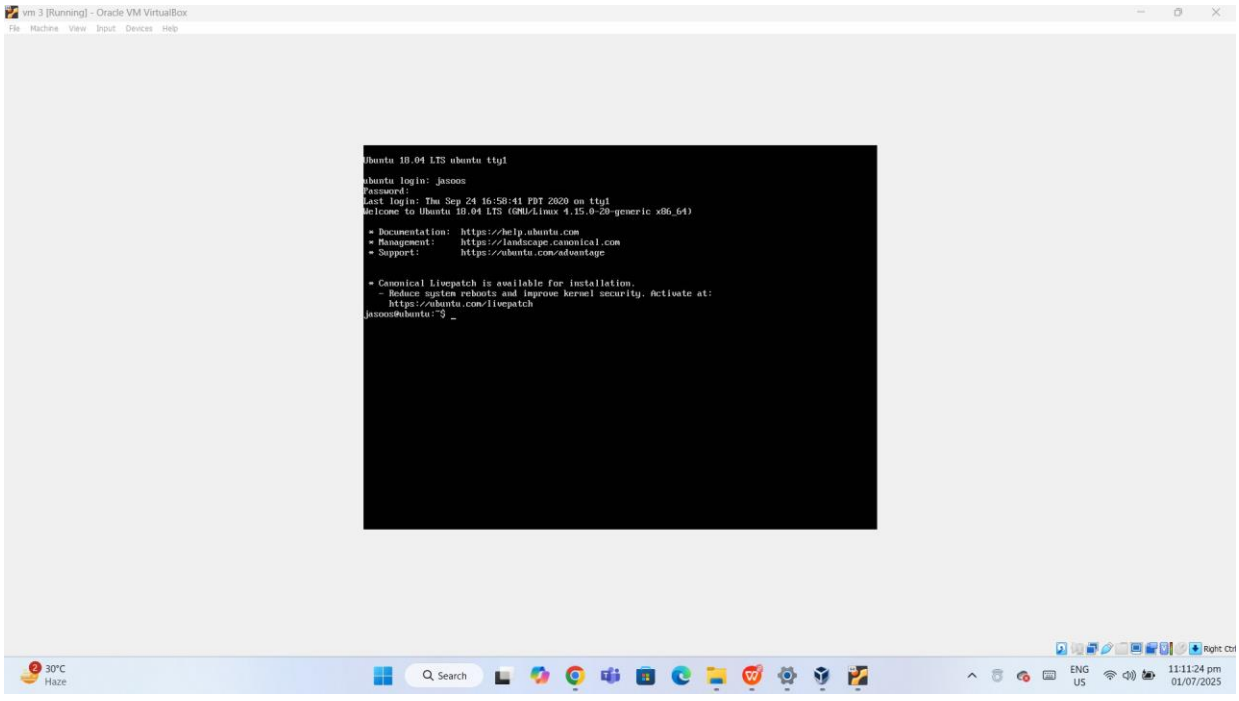

Flag:2 {4a3232c59ecda21ac71bebe3b329bf36}
ReadMe.txt
ghidra_11.3.2_PUBLIC
results.csv
ghidra_11.3.2_PUBLIC_20250415.zip
sample.7z
greep.py
sample.exe
gtk-3.0-css.zip
traffic.pcapng
GTK-XFWM-Everblush-Theme
wallpapers.zip
GTK-XFWM-Theme.zip
xfce4-config.zip
HD-wallpaper-fsociety-anonymous-code-elliot-hacker-hacktivismo-mr-robot-po
ica-tecnologia-tv.jpg
xfce4-docklike-plugin
home-config.zip
zlib_payload.bin
i3lock-color-everblush.zip
(kali㉿kali)-[~/Downloads]
$ _


df hamza .4 - 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
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
array logic building
CCN PROJECT
CSS
hack machine
hacking tools
printer driver
forensics-disk1
saboot (1)
File name: saboot (1).001
Files of type: All Supported Types
Open
Cancel
< Back
Next >
Finish
Cancel
Help
30°C
Haze
Search
ENG
US
11:06:16 pm
01/07/2025


df hamza .4 - 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
Listing
Data Sources
1 Results
Table
Thumbnail
Summary
Save Table as CSV
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Recycle Bin (1)
Analysis Results
OS Accounts
Tags
Score
Reports
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help
Analyzing files from saboot (1).001
63%
(3 more...)
30°C
Haze
Search
ENG
US
11:07:04 pm
01/07/2025

Flag 3 found in Flag1.txt





Flag 4 Found and Task Completed