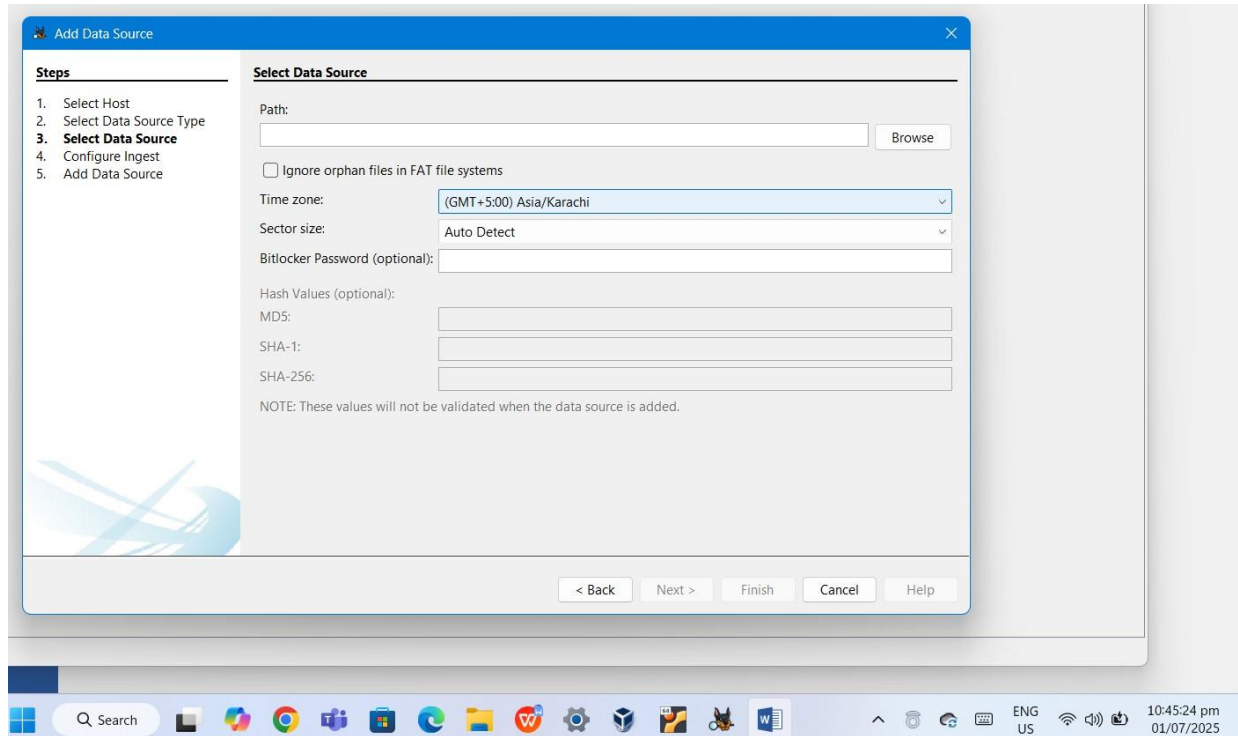
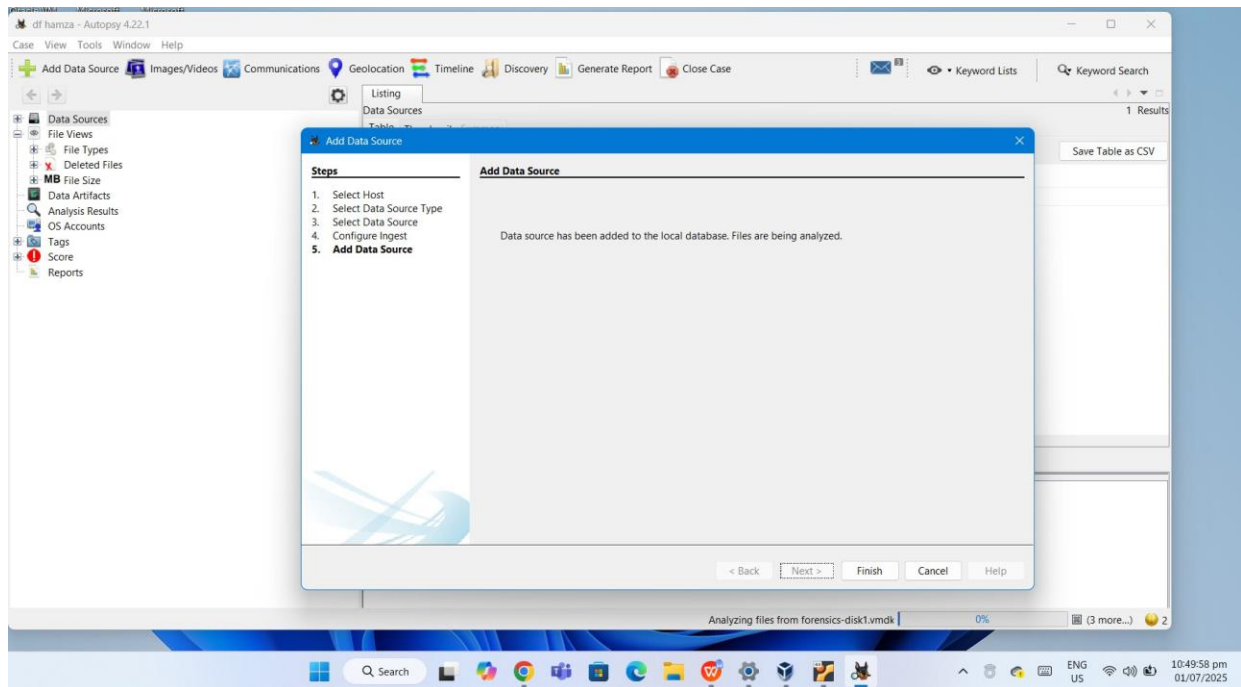


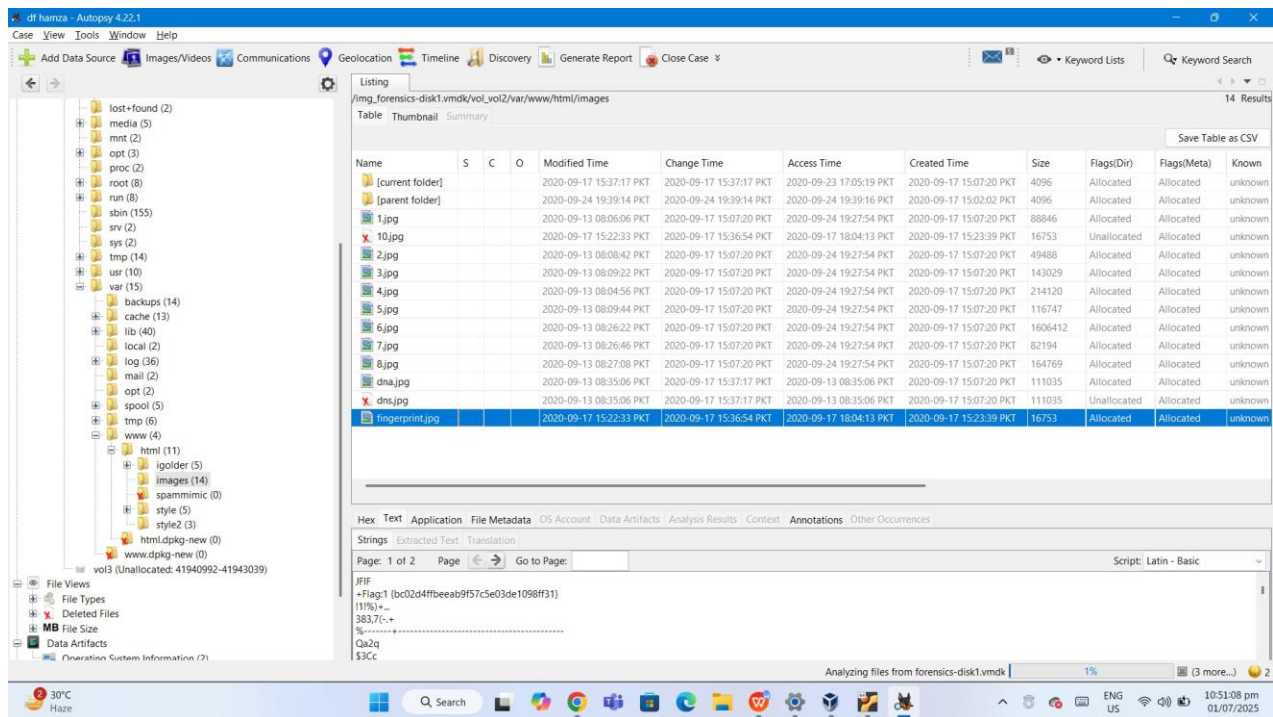
LAB EXAM DIGITAL FORENSICS

First we find flag 1:





Flag 1 Found:



Extract File

df hamza - Autopsy 4.20.1

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/vol2/var/www/html

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]				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				2020-09-13 10:32:28 PKT	2020-09-17 15:07:44 PKT	2020-09-23 17:05:19 PKT	2020-09-17 15:07:20 PKT	4096	Allocated	Allocated	unknown
style2				2020-09-13 08:49:36 PKT	2020-09-25 04:59:39 PKT	2020-09-23 17:05:19 PKT	2020-09-17 15:07:20 PKT	4096	Allocated	Allocated	unknown
index.html.swp				2020-09-25 04:59:39 PKT	2020-09-25 04:59:39 PKT	2020-09-25 04:53:12 PKT	2020-09-25 04:53:12 PKT	8388608	Unallocated	Allocated	unknown
flag.zip				2020-09-24 19:39:14 PKT	2020-09-24 19:39:14 PKT	2020-09-24 19:39:14 PKT	2020-09-24 19:39:14 PKT	18503455	Allocated	Allocated	unknown
index.htm				2020-09-24 19:29:28 PKT	2020-09-24 19:29:31 PKT	2020-09-23 17:05:19 PKT	2020-09-17 15:07:20 PKT	1690	Allocated	Allocated	unknown
tips.txt				2020-09-24 19:30:27 PKT	2020-09-24 19:30:27 PKT	2020-09-24 19:30:27 PKT	2020-09-17 16:43:26 PKT	19	Allocated	Allocated	unknown

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)

Hex Text A Properties

Page: 1

Results Context Annotations Other Occurrences

Jump to Offset Launch in HxD

0x00000000: 50 4B 03 04 14 00 09 00 08 00 39 3B 31 51 5C 2A PK.....9:12~+
0x00000001: 70 92 8D DE 02 00 6C 09 03 00 08 00 1C 00 66 6C P.....f1
0x00000002: 61 67 2E 70 64 66 55 54 09 00 03 BE 47 63 8F 10 ap.pstff.....Gc_+
0x00000003: AF 6C 5F 75 78 0B 00 01 04 00 00 00 00 04 00 00 ..i..K.....
0x00000004: 00 00 2F 02 29 05 D0 4B 0B 80 F4 01 8D BA D6 44/..K.....D
0x00000005: 20 PC 83 22 33 4B 8A 34 CA 29 5A EC AT CE 25 ...*M..4..i..K
0x00000006: E7 54 FA A5 9D 4D 54 CE D8 F2 F5 59 E4 D5 25 82 ..T...Y...K
0x00000007: 83 8C 4B 05 76 66 8B 80 81 07 76 81 10 73 0B 87

Analyzing files from forensics-disk1.vmdk 1% (3 more...) 2

flag

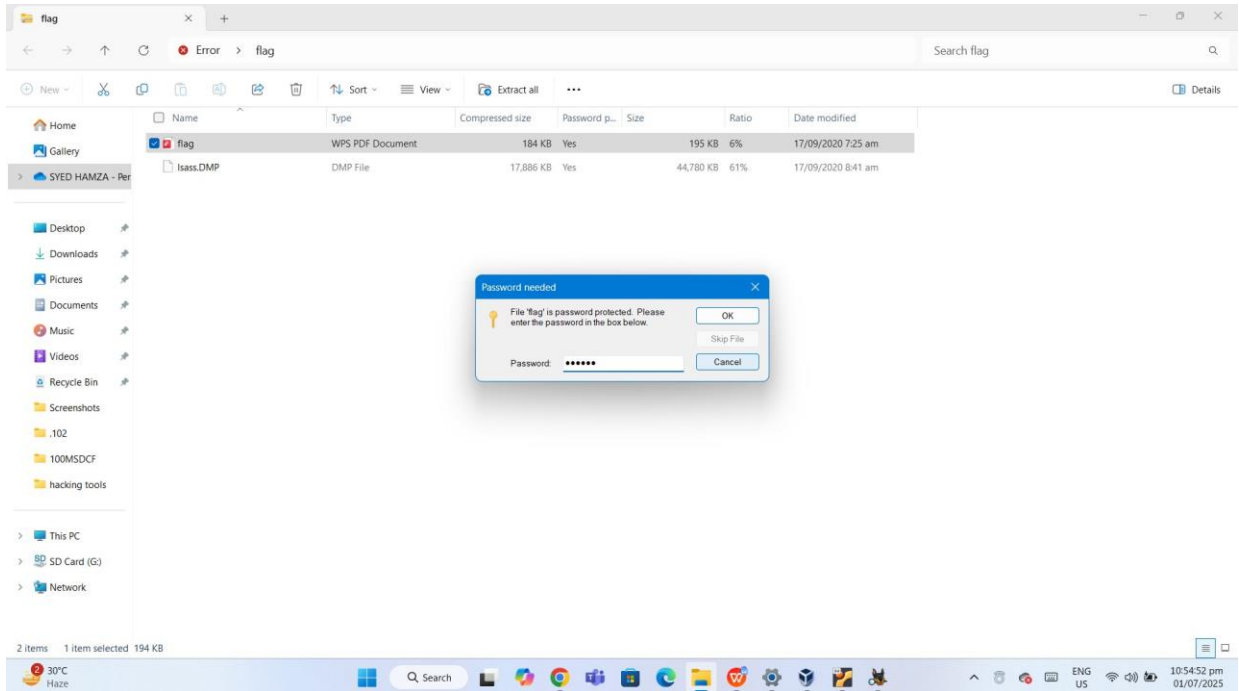
Error > flag

Search flag

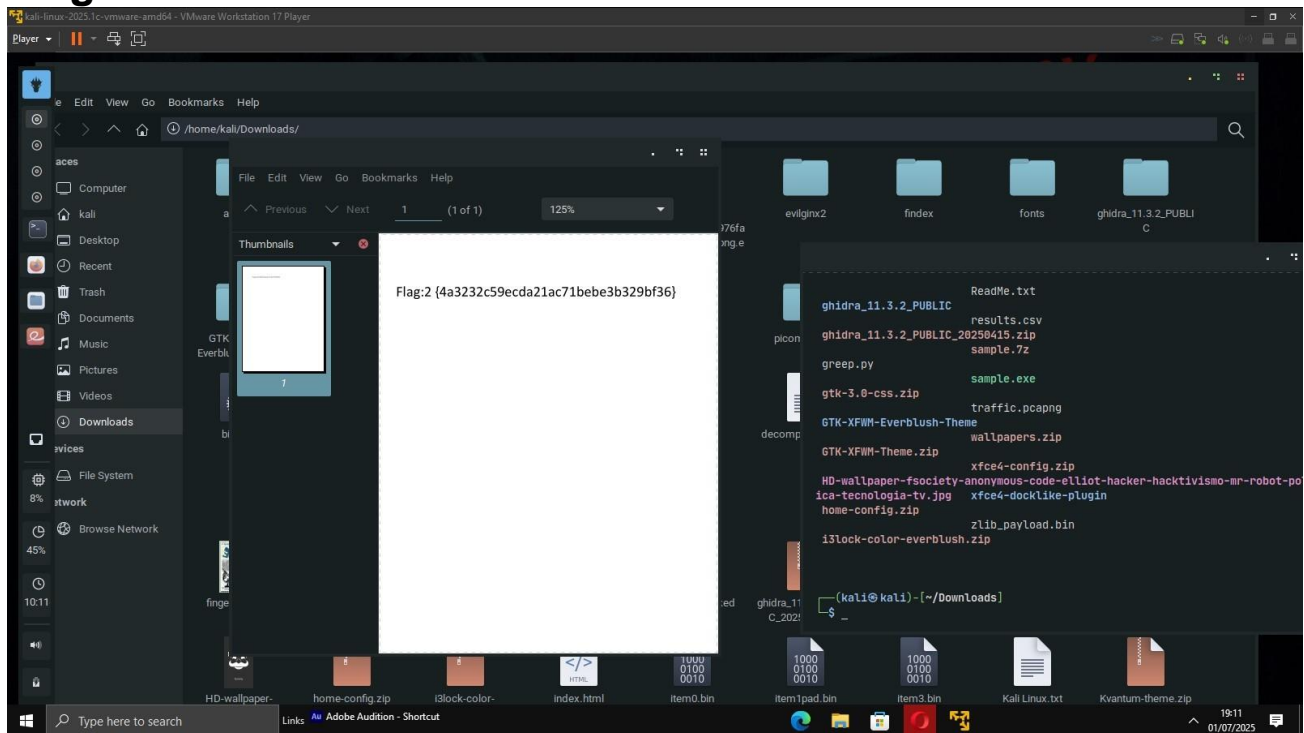
New < > Sort < > View < > Extract all < > Details

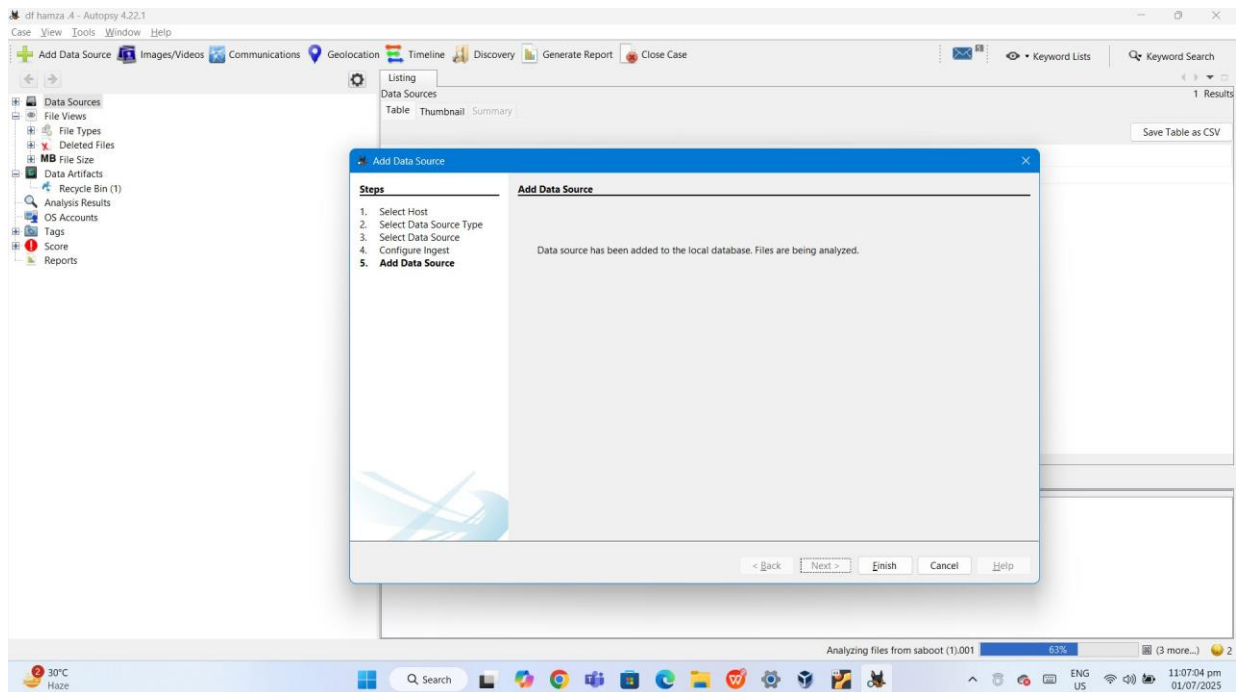
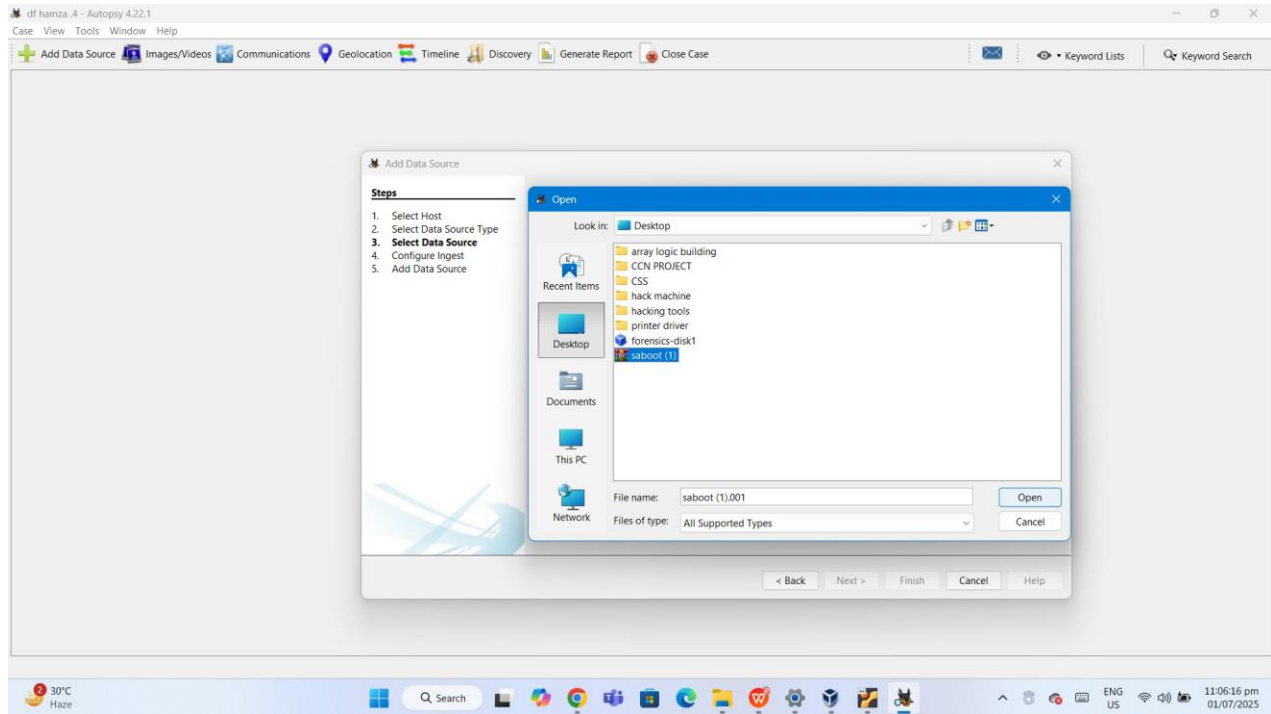
Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
flag	WPS PDF Document	184 KB	Yes	195 KB	6%	17/09/2020 7:25 am
Isass.DMP	DMP File	17,886 KB	Yes	44,780 KB	61%	17/09/2020 8:41 am

2 Items



Flag 2 Found:





Flag 3 found in Flag1.txt

df hamza.A - 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_saboot (1).001

20 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
(SYSTEM.TUNNEL)				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
System Volume Information				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
\$AttrDef				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				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
\$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	6368	Allocated
\$Bitmap	0			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
\$Boot	0			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
\$LogFile	0			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
\$MFT	0			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
\$MFTMirr	0			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
\$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	131072	Allocated
\$UpCase	0			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
\$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	24	Allocated
creds.txt				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	41	Allocated
flag3.txt				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	5	Unallocated
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		

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

Text Source: File Text

Flag3 (8442460f48338fe60a9497b0e0e9022f)

-----METADATA-----

vm 3 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
ubuntu 18.04 LTS ubuntu tty1
ubuntu login: jason
password:
Last login: Thu Sep 24 16:58:41 PDT 2020 on tty1
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-28-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
jason@ubuntu:~$ _
```


Flag 4 Found and Task Completed

