

**NAME : SATHYAPRAKASH SAHOO**

**CLASS : BSC. TY. CS**

**ROLL NO : CS- 4124**

**DIV : 2 BATCH : C**

**SUBJECT : CYBER FORENSICS - PRACTICAL**

---

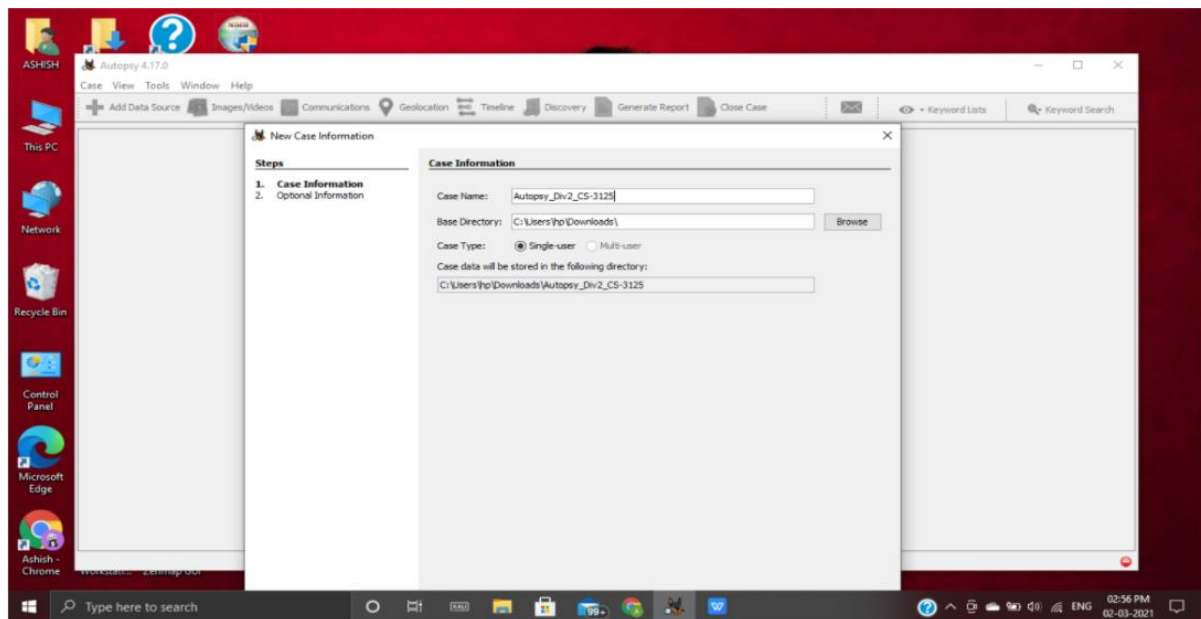
**PRACTICAL NO. 3**

**AIM :** Forensics Case Study:- Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy.

**STEPS :** follow the below steps -

STEP 1: Download Autopsy from <https://www.autopsy.com/download/> and install it

STEP 2: Enter Case information and select base directory as D drive.

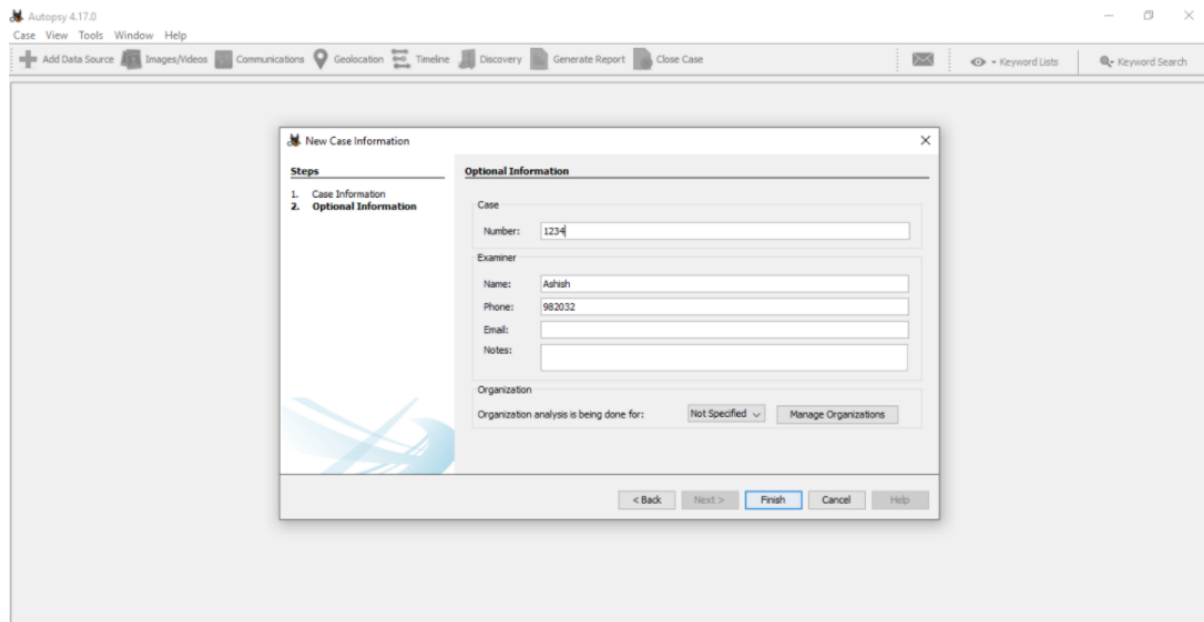


STEP 3: Now enter Optional Information.

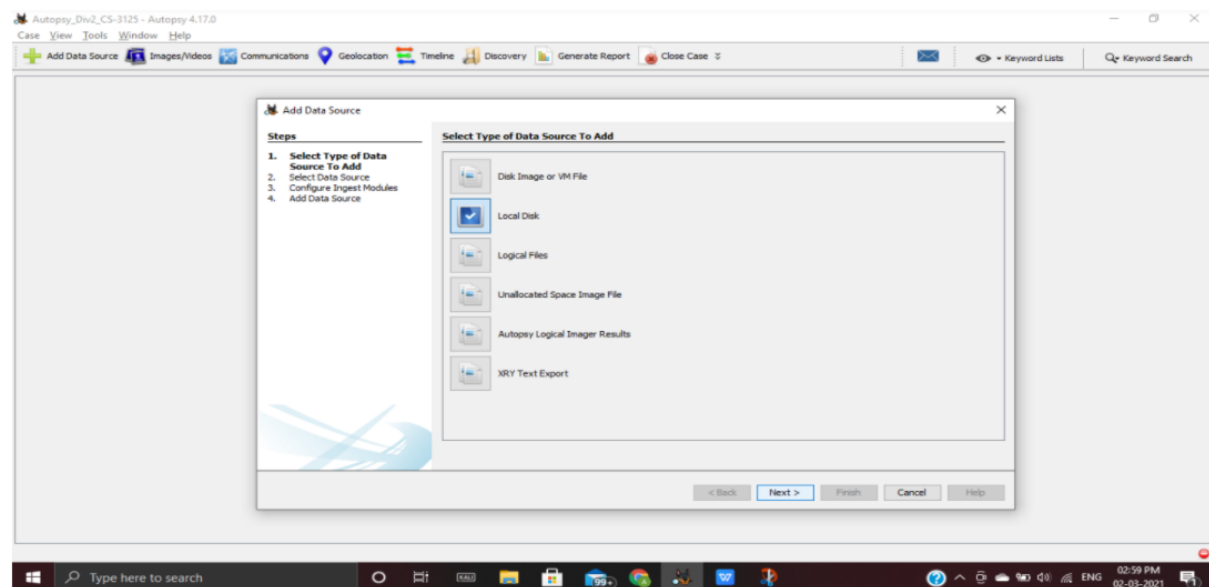
Case number: 1234

Examiner name: Ashish

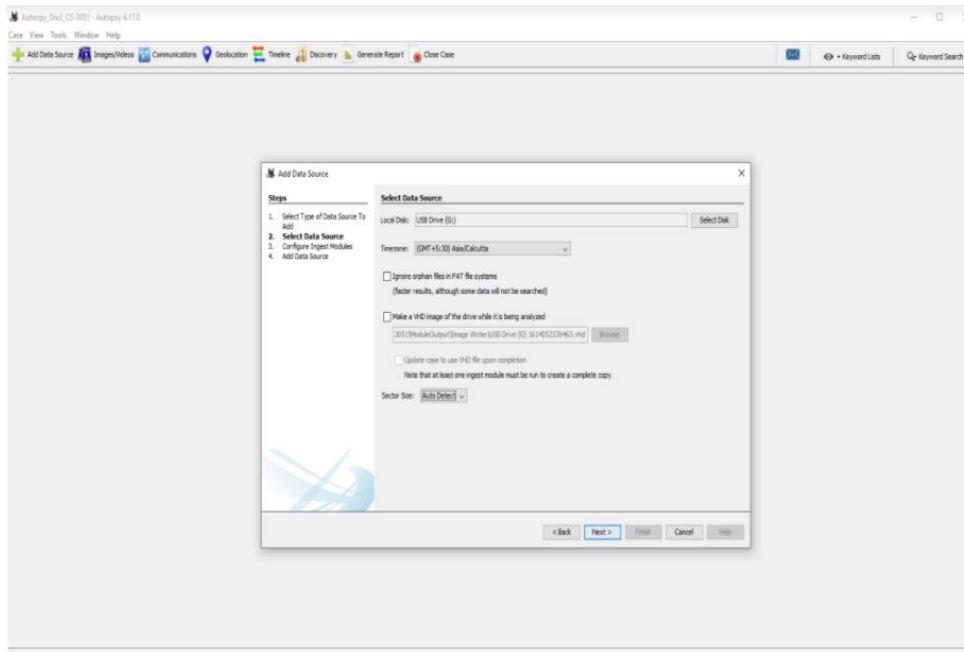
Click on Finish.



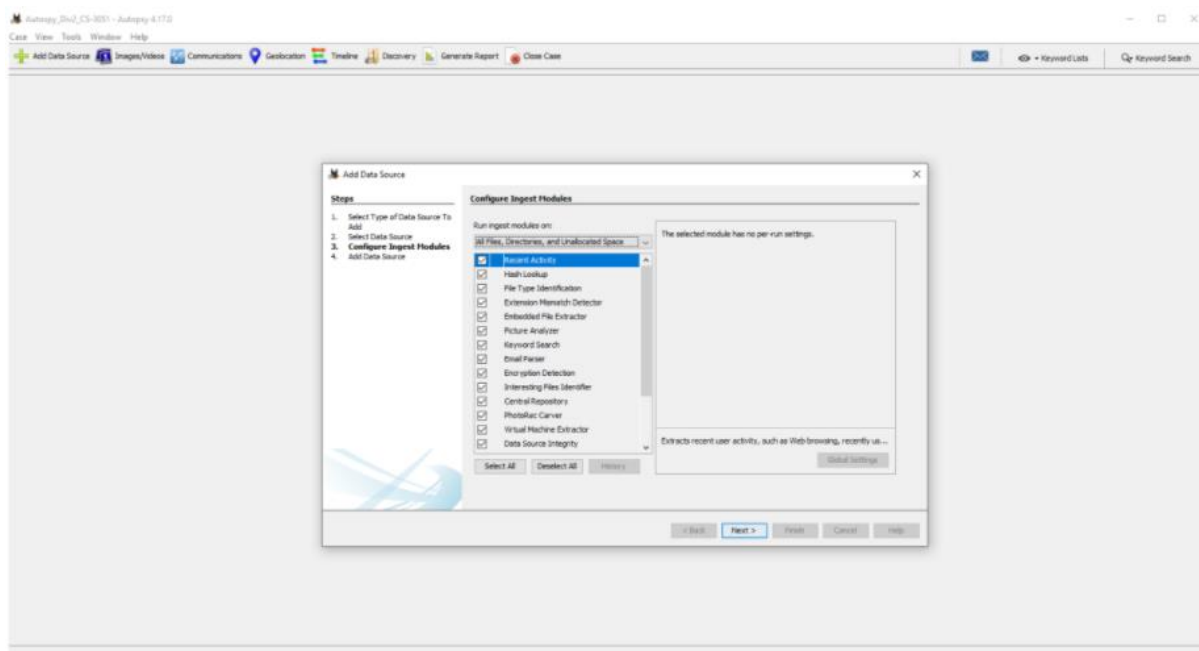
STEP 4: An option will appear as “ Select Type of Data Source to Add”. Select option “ Local Disk” and click on next.



STEP 5: Select local disk USB Drive (G:). Click on Next.



STEP 6: Select all in Configure Ingest Modules and click on next.



STEP 7: Message box will appear as “Data source has been added to the local database. Files are being analyzed.” Click on Finish.



Autopsy\_Dist\_CS-3051 - Autopsy 4.17.0

Case View Tools Window Help

Add Data Source Images/Videos Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Data Sources

- ICSharpFiles (4794)
  - ICSharpFiles (3632)
    - ICSharpFiles (3)
      - System Volume Information (4)

Views

- File Types
  - By Extension
    - Images (2415)
      - Images (2)
      - Audio (2)
      - Archives (205)
      - Databases (2)
    - Documents
    - Executable
    - By MIME Type
  - Deleted Files
    - File System (2683)
      - File System (11246)
  - MB File Size
- Results
  - Extracted Content
    - PDF Metadata (359)
    - Metadata (124)
    - User Content Suspected (359)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (346)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
- Tags
- Reports

Listing

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Hbs)	Known	MD5 Hash
ICSharpFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
IFAT1			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7592440	Allocated	Allocated	unknown	a13955ec817473
IFAT2			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7592440	Allocated	Allocated	unknown	a13955ec817473
IMR			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	unknown	768702005054e8
ICSharpFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
ICSharpFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	
System Volume Information			2020-09-10 22:12:52 EST	0000-00-00 00:00:00	2021-02-23 00:00:00 EST	2020-09-10 22:12:51 EST	4096	Unallocated	Unallocated	unknown	8c7015994e54b4
Y DSCOFRPT.PRT12020			2020-10-08 11:24:09 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:08 EST	1469835	Unallocated	Unallocated	unknown	8c7015994e54b4
Y DSCOFRPT.PRT12020			2020-10-08 11:24:09 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:08 EST	831295	Unallocated	Unallocated	unknown	a30820e6af30a0d
Y DSCOFRPT.PRT12020			2020-10-08 11:24:10 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:02 EST	983966	Unallocated	Unallocated	unknown	55a4c2947ee50d
Y DSCOFRPT.PRT12020			2020-10-08 11:24:12 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:02 EST	927945	Unallocated	Unallocated	unknown	26a15d1a7c5d
Y DSCOFRPT.PRT12020			10-08 11:24:14 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:02 EST	630315	Unallocated	Unallocated	unknown	768702005054e8
Y DSCOFRPT.PRT12020			2020-10-08 11:24:26 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:08 EST	823658	Unallocated	Unallocated	unknown	97094652546ab6
Y DSCOFRPT.PRT12020			2020-10-08 11:24:29 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:08 EST	1234760	Unallocated	Unallocated	unknown	28b3c9a4f124e5d
Y DSCOFRPT.PRT12020			2020-10-08 11:24:22 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:04 EST	852779	Unallocated	Unallocated	unknown	d3c7558d4e1638
Y DSCOFRPT.PRT12020			2020-10-08 11:24:20 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:04 EST	962228	Unallocated	Unallocated	unknown	a67020e320e0f9
Y DSCOFRPT.PRT12020			2020-10-08 11:24:16 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:01 EST	1331394	Unallocated	Unallocated	unknown	733a46d7967e43
Y DSCOFRPT.PRT12020			2020-10-08 11:24:10 EST	0000-00-00 00:00:00	2020-10-18 00:00:00 EST	2020-10-18 15:02:01 EST	1722270	Unallocated	Unallocated	unknown	140220141a4b39

File Metadata | Content | Results | Annotations | Other Occurrences

Autopsy\_Div2\_CS-3051 - Autopsy 4.17.0

Case View Tools Window Help

➕ Add Data Source 📁 Images/Videos 📠 Communications 📍 Geolocation 📅 Timeline 🔍 Discovery 📄 Generate Report 🚫 Close Case

🔍 Keyword Lists 🔍 Keyword Search

🔍 Listing

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Hels)	Known
New Dec 202 (2).jpg			2017-12-21 23:42:46 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	27192	Unallocated	Unallocated	unknown
New Dec 202.jpg			2017-12-21 23:40:40 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	27192	Unallocated	Unallocated	unknown
New Dec 203.jpg			2017-12-21 23:44:18 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	20044	Unallocated	Unallocated	unknown
New Dec 204.jpg			2017-12-21 23:43:40 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	23010	Unallocated	Unallocated	unknown
RUDWANPFC.jpg			2017-12-21 23:42:18 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	27192	Unallocated	Unallocated	unknown
SCAH_20180613_214532385.jpg			2018-06-13 21:46:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	63078	Unallocated	Unallocated	unknown
SCAH_20180613_214532385_R01.jpg			2018-06-13 21:46:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	114387	Unallocated	Unallocated	unknown
SCAH_20180613_214532385_R02.jpg			2018-06-13 21:46:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	119908	Unallocated	Unallocated	unknown
SCAH_20180613_214532385_R03.jpg			2018-06-13 21:46:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	111217	Unallocated	Unallocated	unknown
SCAH_20180613_214532385_R04.jpg			2018-06-13 21:46:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	86421	Unallocated	Unallocated	unknown
SCAH_20180613_214809683.jpg			2018-06-13 21:48:22 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	62731	Unallocated	Unallocated	unknown
SCAH_20180613_214923238.jpg			2018-06-13 21:49:20 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	320765	Unallocated	Unallocated	unknown
SCAH_20180613_215002454.jpg			2018-06-13 21:50:26 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	30393	Unallocated	Unallocated	unknown
SCAH_20180613_215200940.jpg			2018-06-13 21:52:46 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	101261	Unallocated	Unallocated	unknown
SCAH_20180613_215200940_R01.jpg			2018-06-13 21:52:46 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2019-04-14 10:56:05 IST	220306	Unallocated	Unallocated	unknown
Untitled-1.jpg			2019-01-29 23:11:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-03-28 23:35:33 IST	13632	Unallocated	Unallocated	unknown
Untitled-2.jpg			2018-03-26 23:39:02 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-03-26 23:39:01 IST	10431	Unallocated	Unallocated	unknown
Untitled-3.jpg			2018-03-26 23:38:28 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-03-26 23:38:26 IST	10443	Unallocated	Unallocated	unknown
eeefharad1.jpg			2019-06-13 22:22:18 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-06-13 22:22:17 IST	30393	Unallocated	Unallocated	unknown

File | Text | Application | File Metadata | Control | Results | Annotations | Other Occurrences

Analyzing files from G: 15%

Autopsy\_Div2\_CS-3051 - Autopsy 4.17.0

Case View Tools Window Help

➕ Add Data Source 📁 Images/Videos 📠 Communications 📍 Geolocation 📅 Timeline 🔍 Discovery 📄 Generate Report 🚫 Close Case

🔍 Keyword Lists 🔍 Keyword Search

🔍 Listing

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Hels)	Known	Location
Data1.cab			2014-06-02 23:23:18 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:52 IST	10749978	Unallocated	Unallocated	unknown	Img_G
AdWebRd15000_mud_3hd.ap			2015-09-22 20:03:14 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:03:41 IST	141015434	Unallocated	Unallocated	unknown	Img_G
Data1.cab			2012-09-23 20:53:54 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:53:54 IST	136410196	Unallocated	Unallocated	unknown	Img_G
Data1.cab			2012-09-23 20:53:54 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2012-09-23 20:53:54 IST	136410196	Unallocated	Unallocated	unknown	Img_G
Apr 2005_d3d49_25_x64.cab			2014-03-18 10:38:06 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	1347354	Unallocated	Unallocated	unknown	Img_G
Apr 2005_d3d49_25_x86.cab			2014-03-18 10:38:18 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	1078962	Unallocated	Unallocated	unknown	Img_G
Apr 2005_d3d49_30_x64.cab			2014-03-18 10:38:12 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	1297030	Unallocated	Unallocated	unknown	Img_G
Apr 2005_d3d49_30_x86.cab			2014-03-18 10:38:10 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	1115221	Unallocated	Unallocated	unknown	Img_G
Apr 2006_MCX1_x86.cab			2014-03-18 10:38:08 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	916430	Unallocated	Unallocated	unknown	Img_G
Apr 2006_MCX1_x86_archive.cab			2014-03-18 10:38:14 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	4162630	Unallocated	Unallocated	unknown	Img_G
Apr 2006_YACT_x64.cab			2014-03-18 10:38:08 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	179133	Unallocated	Unallocated	unknown	Img_G
Apr 2006_YACT_x86.cab			2014-03-18 10:38:06 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	133103	Unallocated	Unallocated	unknown	Img_G
Apr 2006_xinput_x64.cab			2014-03-18 10:38:06 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	87181	Unallocated	Unallocated	unknown	Img_G
Apr 2006_xinput_x86.cab			2014-03-18 10:38:02 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:55 IST	46010	Unallocated	Unallocated	unknown	Img_G
APR2007_d3d49_10_31_x64.cab			2014-03-18 10:38:08 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:56 IST	698612	Unallocated	Unallocated	unknown	Img_G
APR2007_d3d49_10_31_x86.cab			2014-03-18 10:38:10 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:56 IST	695805	Unallocated	Unallocated	unknown	Img_G
APR2007_d3d49_10_31_x64.cab			2014-03-18 10:38:10 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:56 IST	1607358	Unallocated	Unallocated	unknown	Img_G
APR2007_d3d49_10_31_x86.cab			2014-03-18 10:38:12 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:56 IST	1606039	Unallocated	Unallocated	unknown	Img_G
APR2007_YACT_x64.cab			2014-03-18 10:38:04 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2015-09-22 20:27:56 IST	195766	Unallocated	Unallocated	unknown	Img_G

File | Text | Application | File Metadata | Control | Results | Annotations | Other Occurrences

Analyzing files from G: 34%

Autopsy 4.17.0 - Autopsy 4.17.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing

Table Thumbnail Summary

Page: 1 of 2 Pages: Go to Page: Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dx)	Flags(Meta)	Known	Location
DOSCHPRT.PRT122019			2020-10-08 11:24:18 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:01 IST	1712270	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT112019			2020-10-08 11:24:16 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:01 IST	1331394	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1052020			2020-10-08 11:24:14 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:02 IST	630315	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1042020			2020-10-08 11:24:12 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:02 IST	957945	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1022020			2020-10-08 11:24:10 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:02 IST	905966	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT102020			2020-10-08 11:24:08 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:05 IST	851295	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1012020			2020-10-08 11:24:06 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:05 IST	1403615	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1062019			2020-10-08 11:24:26 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:05 IST	823650	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1072019			2020-10-08 11:24:24 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:05 IST	1017027	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1082019			2020-10-08 11:24:24 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:06 IST	1029750	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT1092019			2020-10-08 11:24:22 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:06 IST	852779	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
DOSCHPRT.PRT102019			2020-10-08 11:24:20 IST	0000-00-00 00:00:00	2020-10-10 00:00:00 IST	2020-10-16 15:02:06 IST	962328	Unallocated	Unallocated	unknown	Jing_S/DOSCHPRT
READER-1.0			2015-03-08 16:58:34 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:22 IST	4096	Unallocated	Unallocated	unknown	Jing_S/80rgharFile
[current folder]			2015-03-08 16:58:34 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:22 IST	4096	Unallocated	Unallocated	unknown	Jing_S/80rgharFile
[parent folder]			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Allocated	unknown	Jing_S/80rgharFile
Reader			2015-03-08 16:58:34 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:22 IST	4096	Unallocated	Unallocated	unknown	Jing_S/80rgharFile
[current folder]			2015-03-08 16:58:34 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:22 IST	4096	Unallocated	Unallocated	unknown	Jing_S/80rgharFile
[parent folder]			2015-03-08 16:58:34 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:22 IST	4096	Unallocated	Unallocated	unknown	Jing_S/80rgharFile
AcroTextExtractor.exe			2014-06-02 23:02:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:23 IST	25962	Unallocated	Unallocated	unknown	Jing_S/80rgharFile
AdobeClib.dll			2014-06-02 23:02:58 IST	0000-00-00 00:00:00	2020-09-10 00:00:00 IST	2020-09-04 23:44:23 IST	943096	Unallocated	Unallocated	unknown	Jing_S/80rgharFile

File Type Application File Metadata Context Results Annotations Other Documents

Analyzing files from G: 34%