**NAME** : SATHYAPRAKASH SAHOO **CLASS** : BSC. TY. CS

**ROLL NO :** CS- 4124 **DIV** : 2 **BATCH** : C

**SUBJECT** : CYBER FORENSICS - PRACTICAL

---

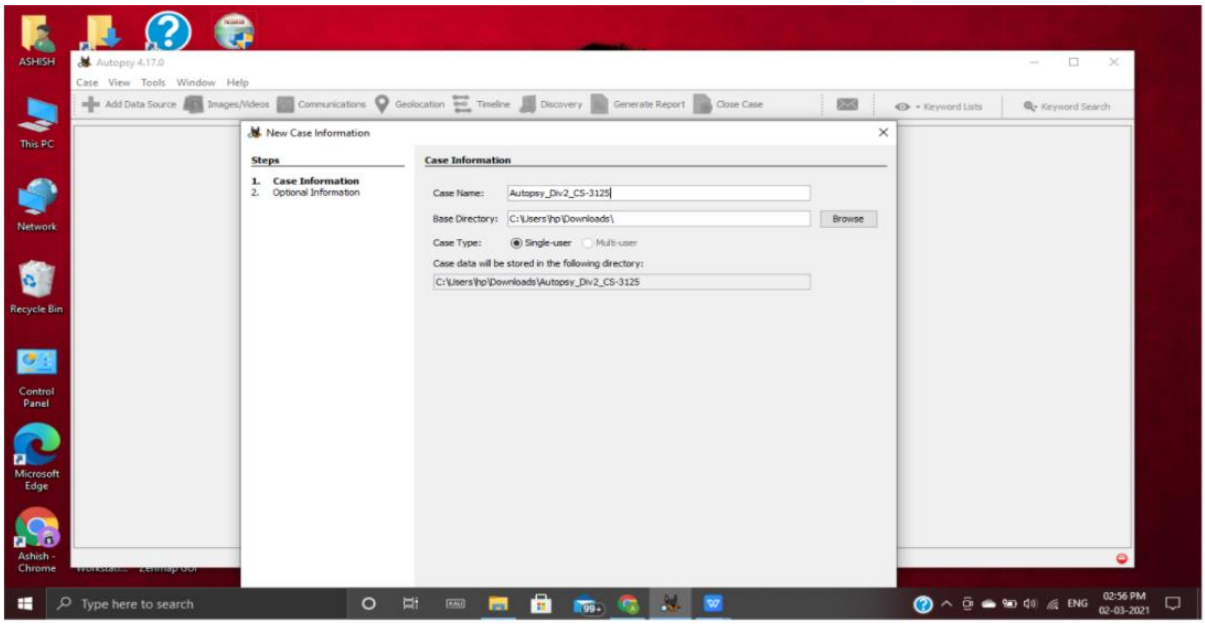
**PRACTICAL NO. 3**

**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 Autospy from https://www.autopsy.com/download/ and install it

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

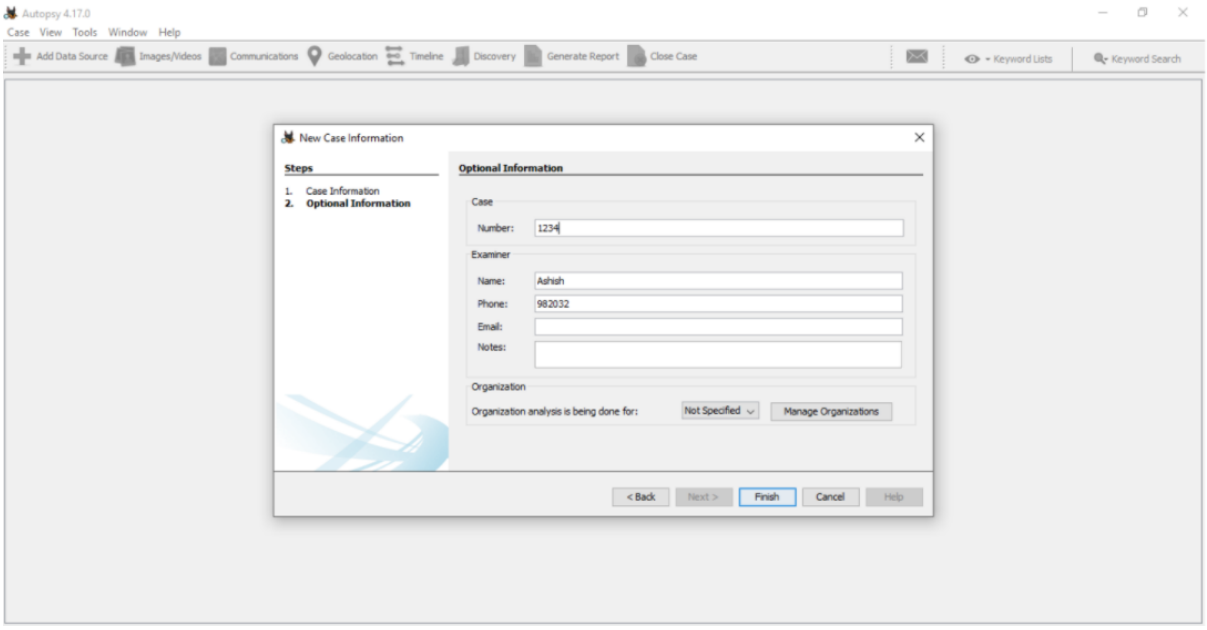



STEP 3: Now enter Optional Information.

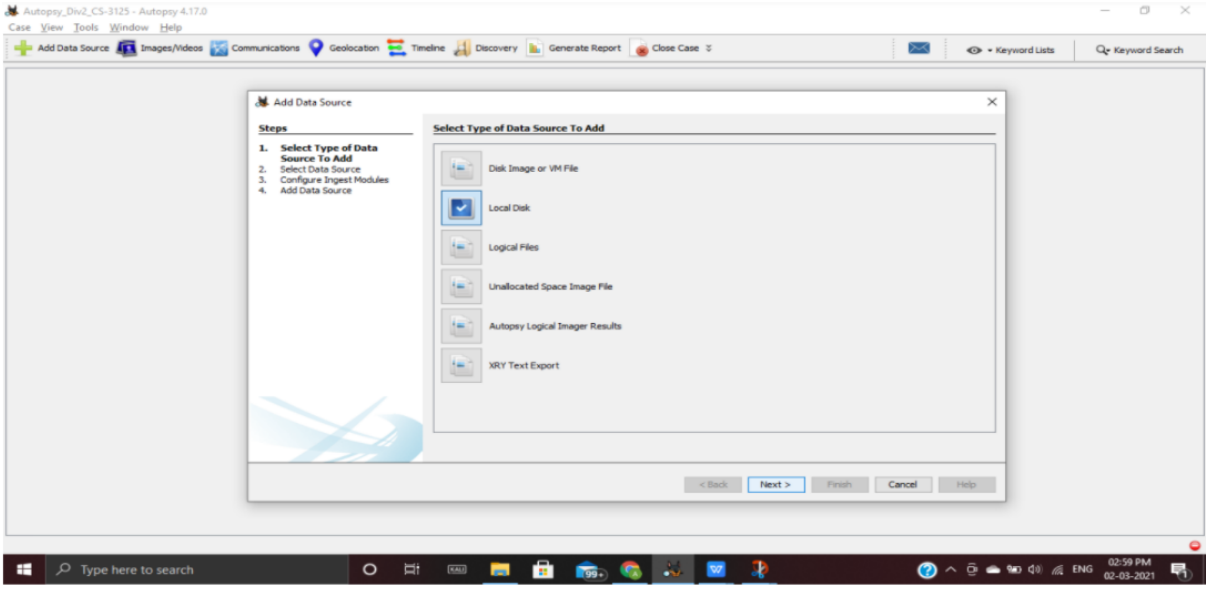
Case number: 1234

Examiner name: Ashish

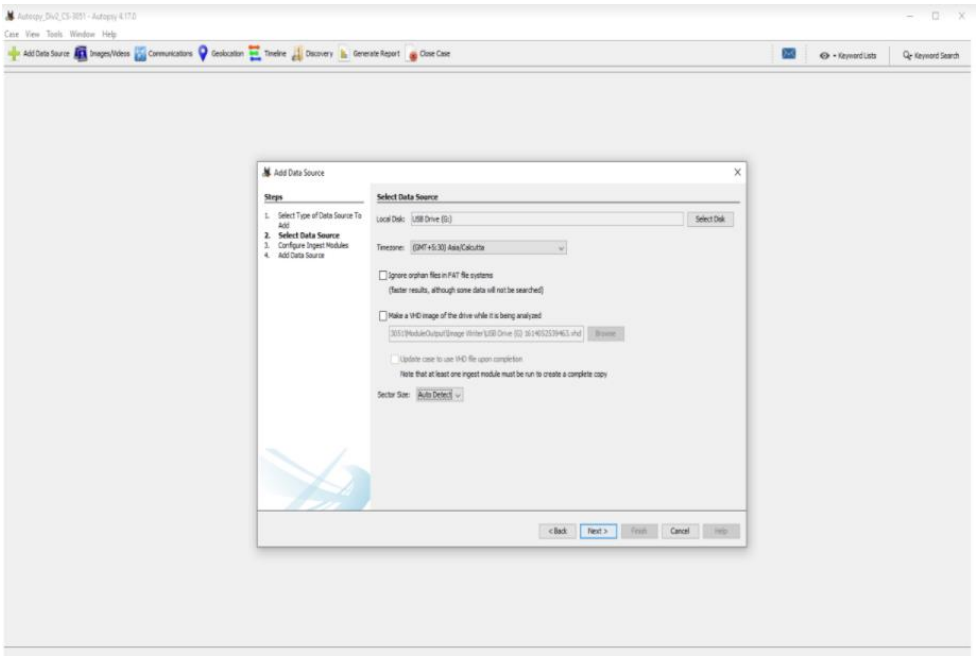
Click on Finish.



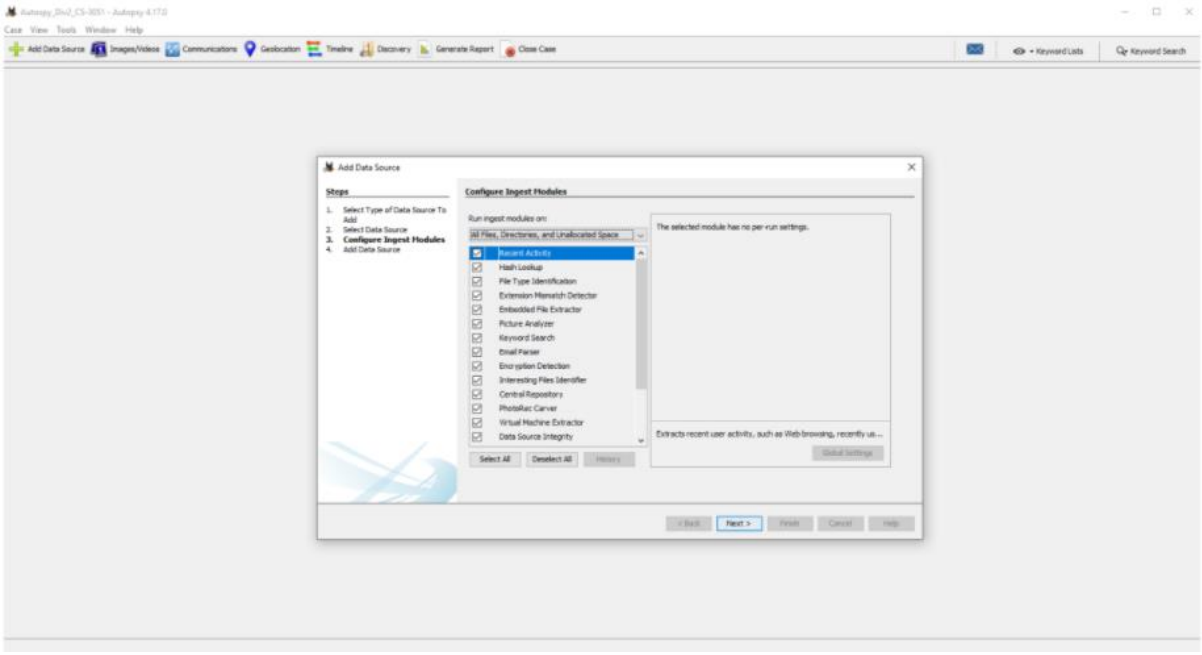

STEP 4: An option will appear as " Select Type of Data Source to Add". Select option " Local Disk" and click on next.



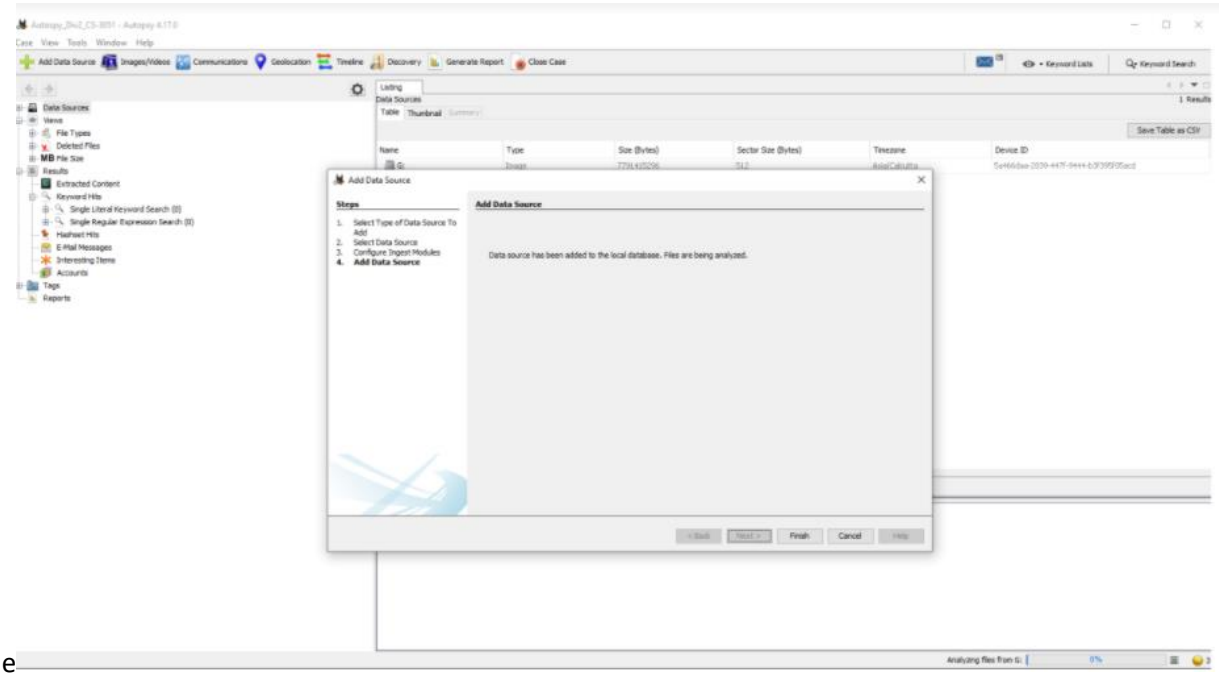

STEP 5: Select local disk USB Drive (G:). Click on Next.



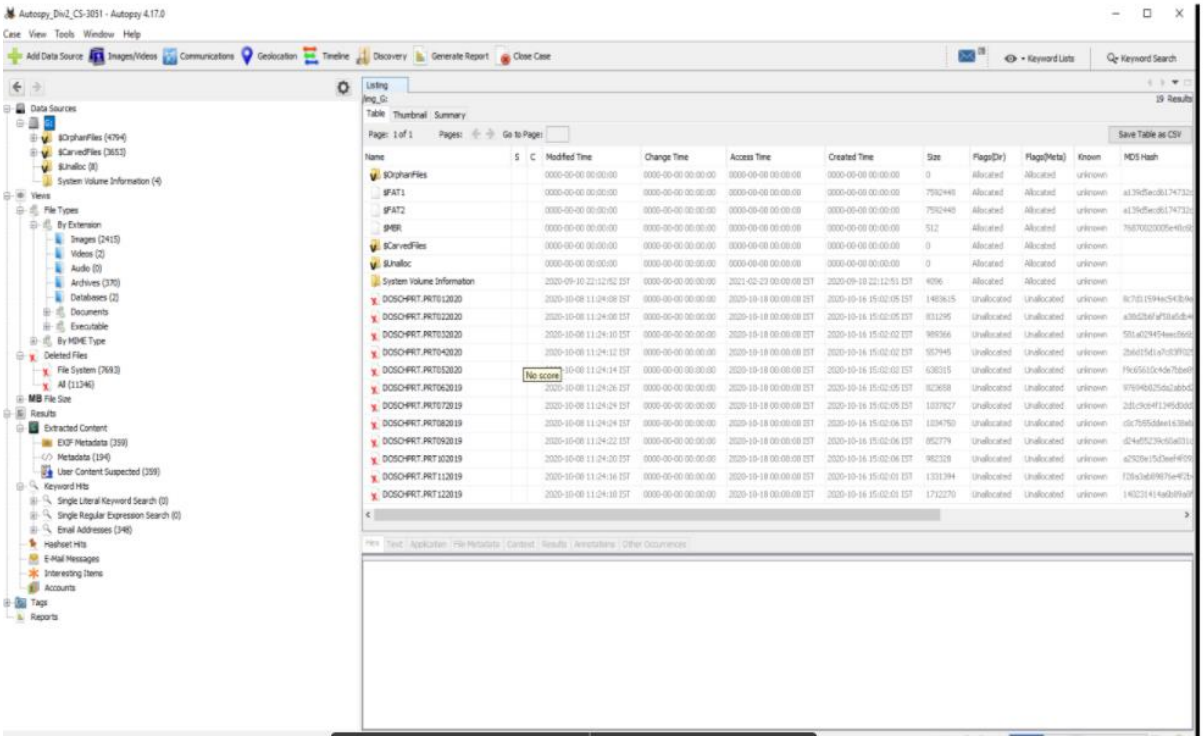

STEP 6: Select all in Configure Ingest Modules and click on next.

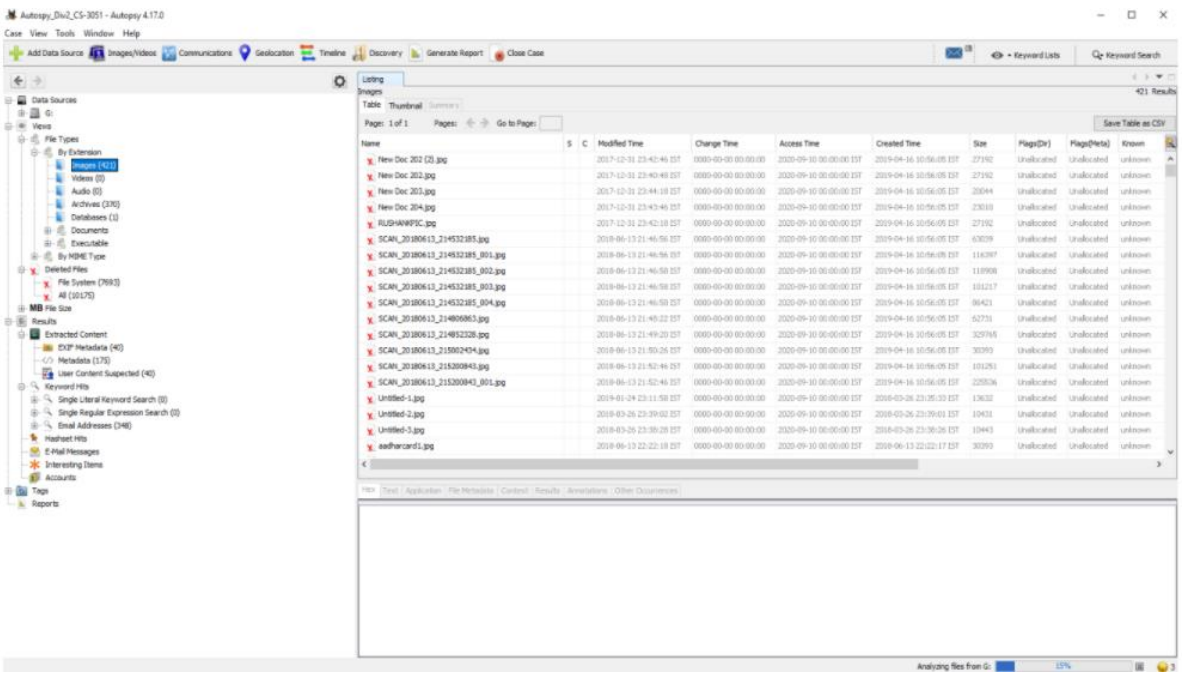


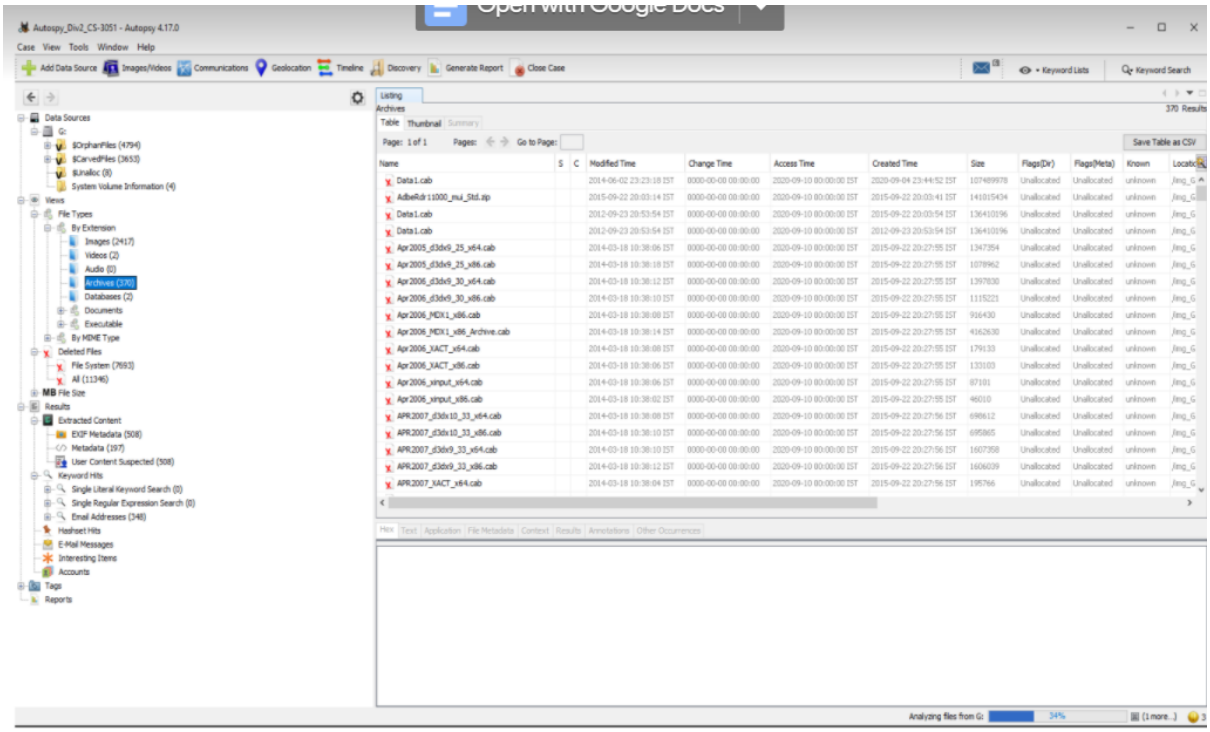

STEP 7: Message box will appear as “Data source has been added to the local databse. Files are being analyzed.”Click on Finish.

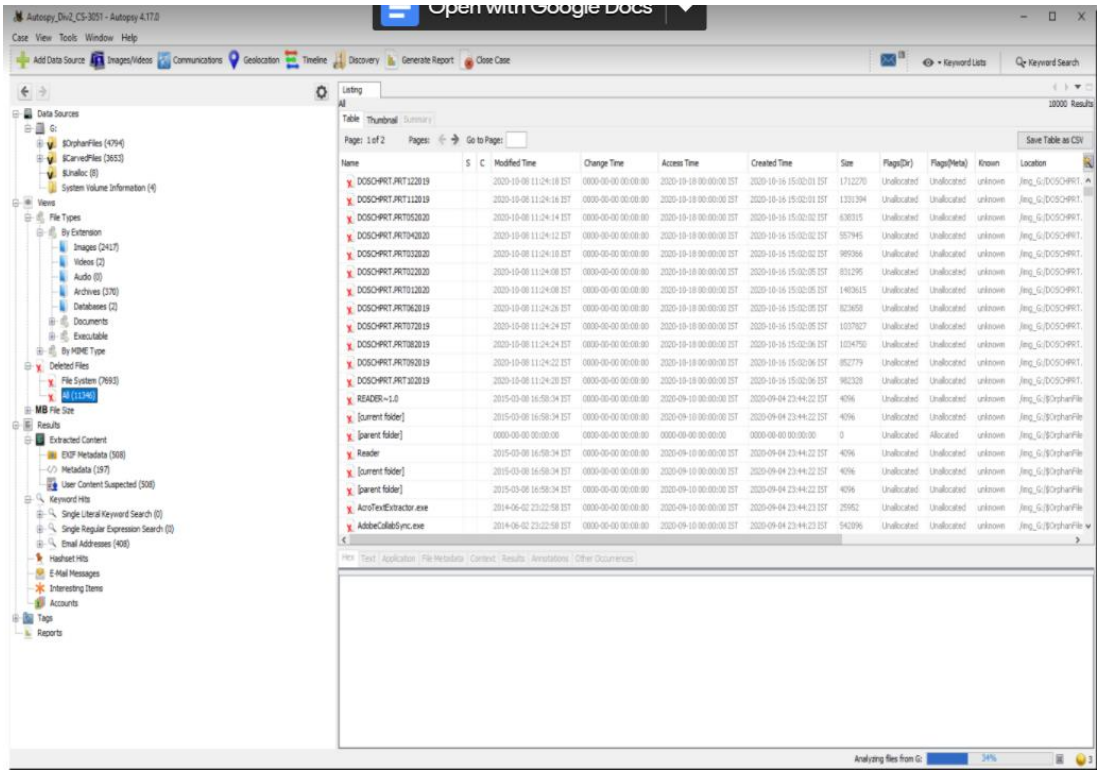

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
Finish
Cancel

e


Autopsy_Div2_CS-3051 - Autopsy 4.17.0
No score


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
Data Sources
Views
File Types
By Extension
Images (421)
Videos (0)
Audio (0)
Archives (370)
Databases (1)
Documents
Executable
By MIME Type
Deleted Files
File System (7693)
All (10175)
File Size
Results
Extracted Content
EXIF Metadata (40)
Metadata (175)
User Content Suspected (40)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (348)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Images
421 Results
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(Dir) Flags(Meta) Known
New Doc 202 (2).jpg
New Doc 202.jpg
New Doc 203.jpg
New Doc 204.jpg
RUSHANIPSC.jpg
SCAN_20180613_214532185.jpg
SCAN_20180613_214532185_001.jpg
SCAN_20180613_214532185_002.jpg
SCAN_20180613_214532185_003.jpg
SCAN_20180613_214532185_004.jpg
SCAN_20180613_214806863.jpg
SCAN_20180613_214852328.jpg
SCAN_20180613_215002434.jpg
SCAN_20180613_215200843.jpg
SCAN_20180613_215200843_001.jpg
Untitled-1.jpg
Untitled-2.jpg
Untitled-3.jpg
eadharcard1.jpg
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Analyzing files from G:


Open with Google Docs
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
Data Sources
G:
$OrphanFiles (4794)
$CarvedFiles (3653)
$Unalloc (9)
System Volume Information (4)
Views
File Types
By Extension
Images (2417)
Videos (2)
Audio (0)
Archives (370)
Databases (2)
Documents
Executable
By MIME Type
Deleted Files
File System (7693)
All (11346)
File Size
Results
Extracted Content
EXIF Metadata (508)
Metadata (197)
User Content Suspected (508)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (348)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
Archives
370 Results
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(Dir) Flags(Meta) Known Locatio
Data1.cab
AdbeRdr11000_mui_Std.zip
Data1.cab
Data1.cab
Apr2005_d3dx9_25_x64.cab
Apr2005_d3dx9_25_x86.cab
Apr2006_d3dx9_30_x64.cab
Apr2006_d3dx9_30_x86.cab
Apr2006_MDX1_x86.cab
Apr2006_MDX1_x86_Archive.cab
Apr2006_XACT_x64.cab
Apr2006_XACT_x86.cab
Apr2006_xinput_x64.cab
Apr2006_xinput_x86.cab
APR2007_d3dx10_33_x64.cab
APR2007_d3dx10_33_x86.cab
APR2007_d3dx9_33_x64.cab
APR2007_d3dx9_33_x86.cab
APR2007_XACT_x64.cab
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Analyzing files from G:
(1 more...)


Open with Google Docs
Autopsy_DivZ_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
Data Sources
G:
$OrphanFiles (4794)
$CarvedFiles (3653)
$Unalloc (8)
System Volume Information (4)
Views
File Types
By Extension
Images (2417)
Videos (2)
Audio (0)
Archives (370)
Databases (2)
Documents
Executable
By MIME Type
Deleted Files
File System (7693)
All (11340)
MB File Size
Results
Extracted Content
EXIF Metadata (308)
Metadata (197)
User Content Suspected (308)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (408)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Reports
Listing
All
10000 Results
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(Dir)
Flags(Meta)
Known
Location
DOSCHPRT.PRT122019
DOSCHPRT.PRT112019
DOSCHPRT.PRT052020
DOSCHPRT.PRT042020
DOSCHPRT.PRT032020
DOSCHPRT.PRT022020
DOSCHPRT.PRT012020
DOSCHPRT.PRT062019
DOSCHPRT.PRT072019
DOSCHPRT.PRT082019
DOSCHPRT.PRT092019
DOSCHPRT.PRT102019
READER~1.0
[current folder]
[parent folder]
Reader
[current folder]
[parent folder]
AcroTextExtractor.exe
AdobeCollabSync.exe
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Analyzing files from G:
34%