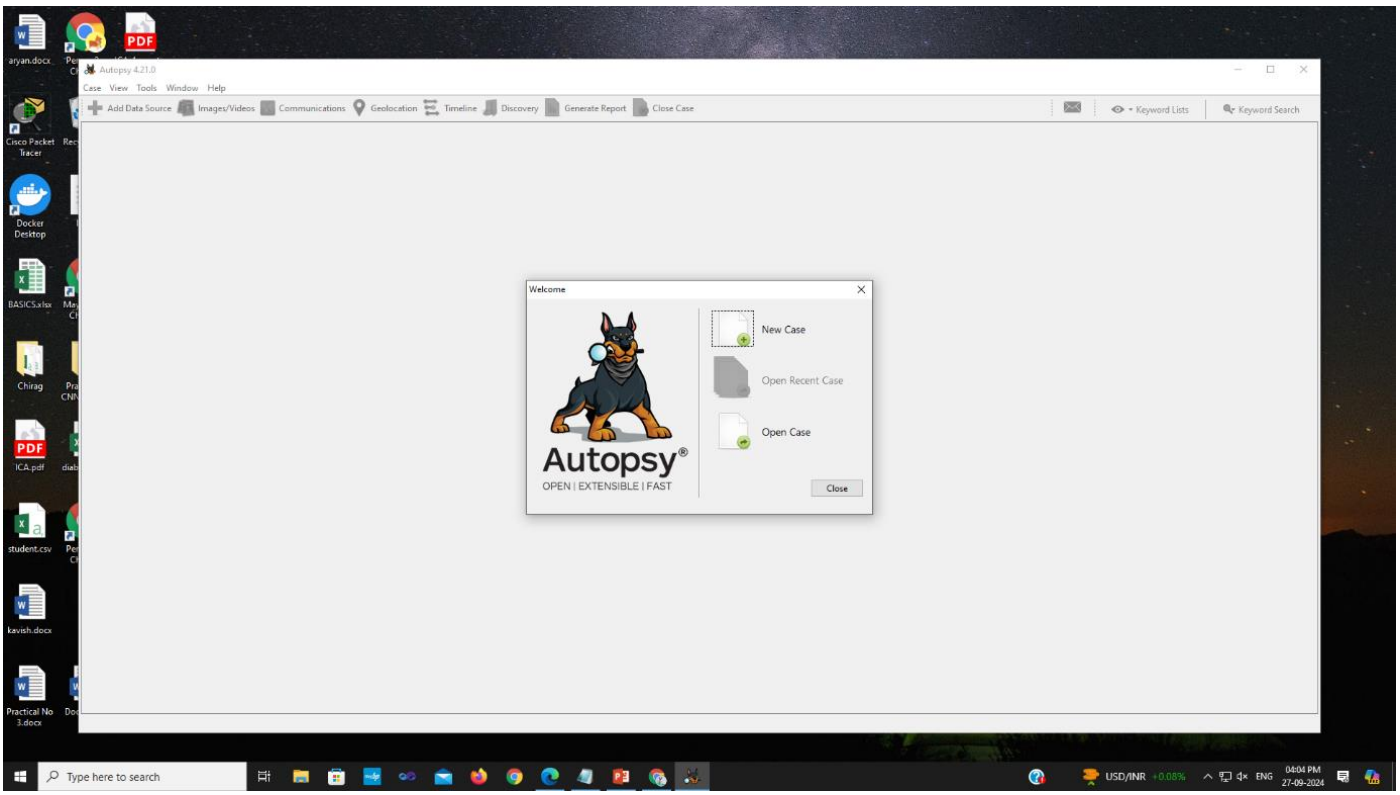
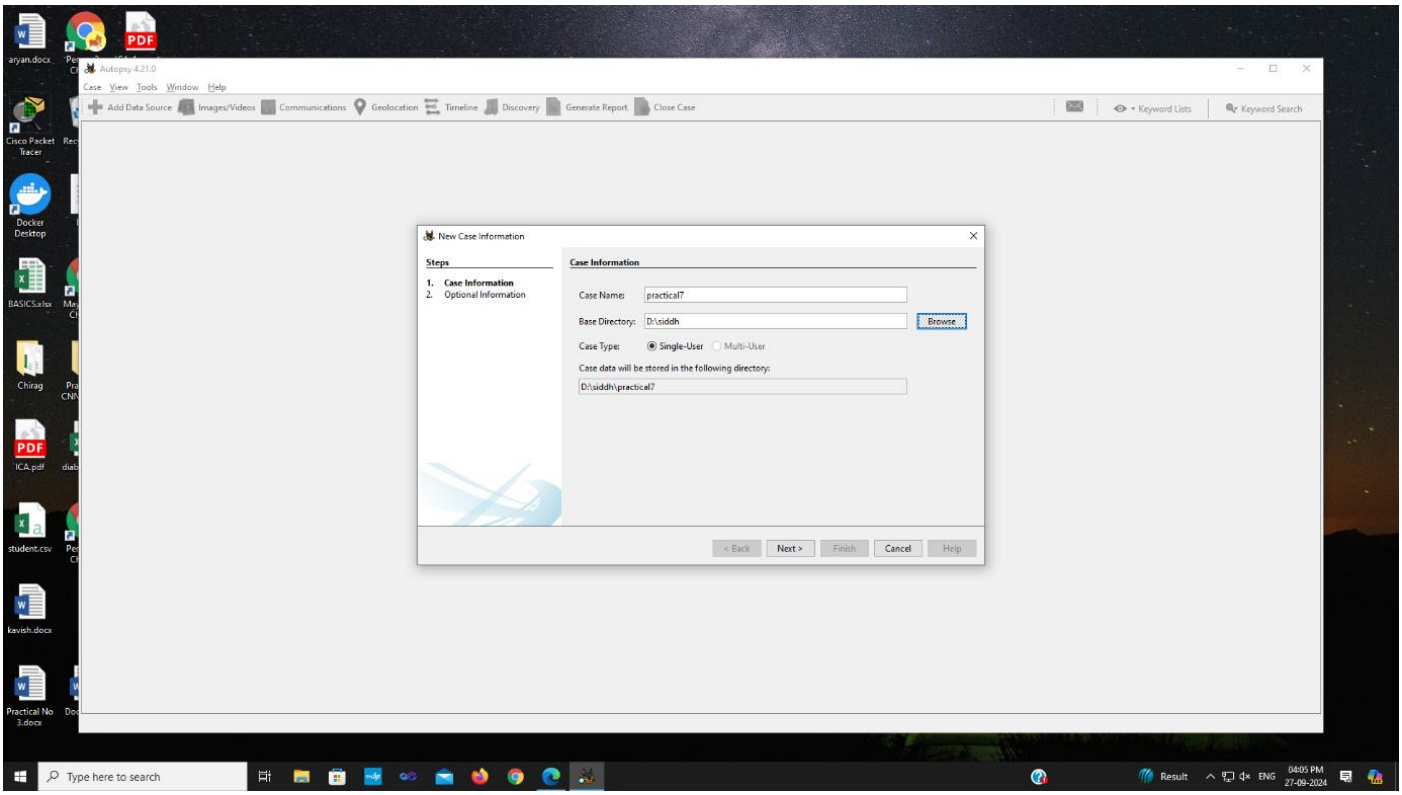
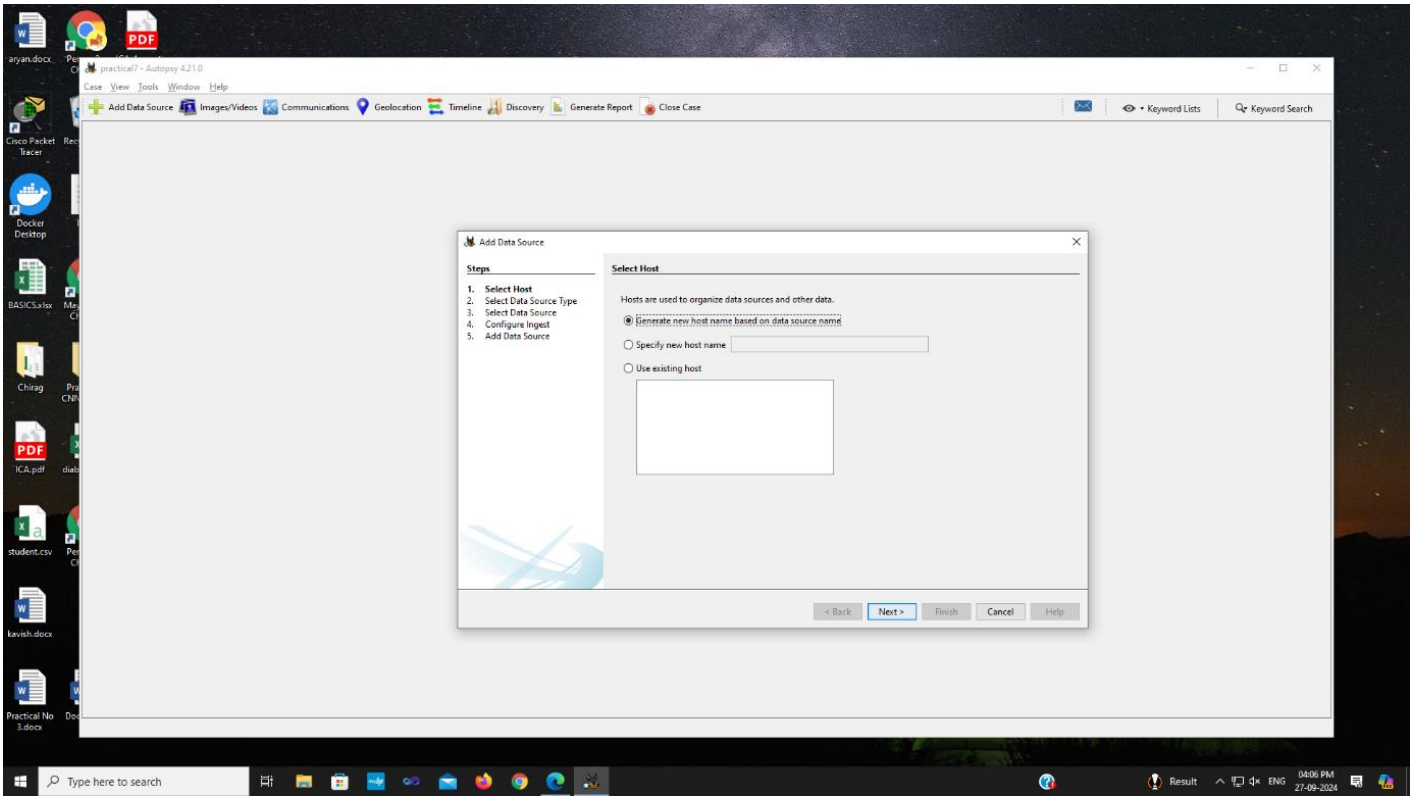
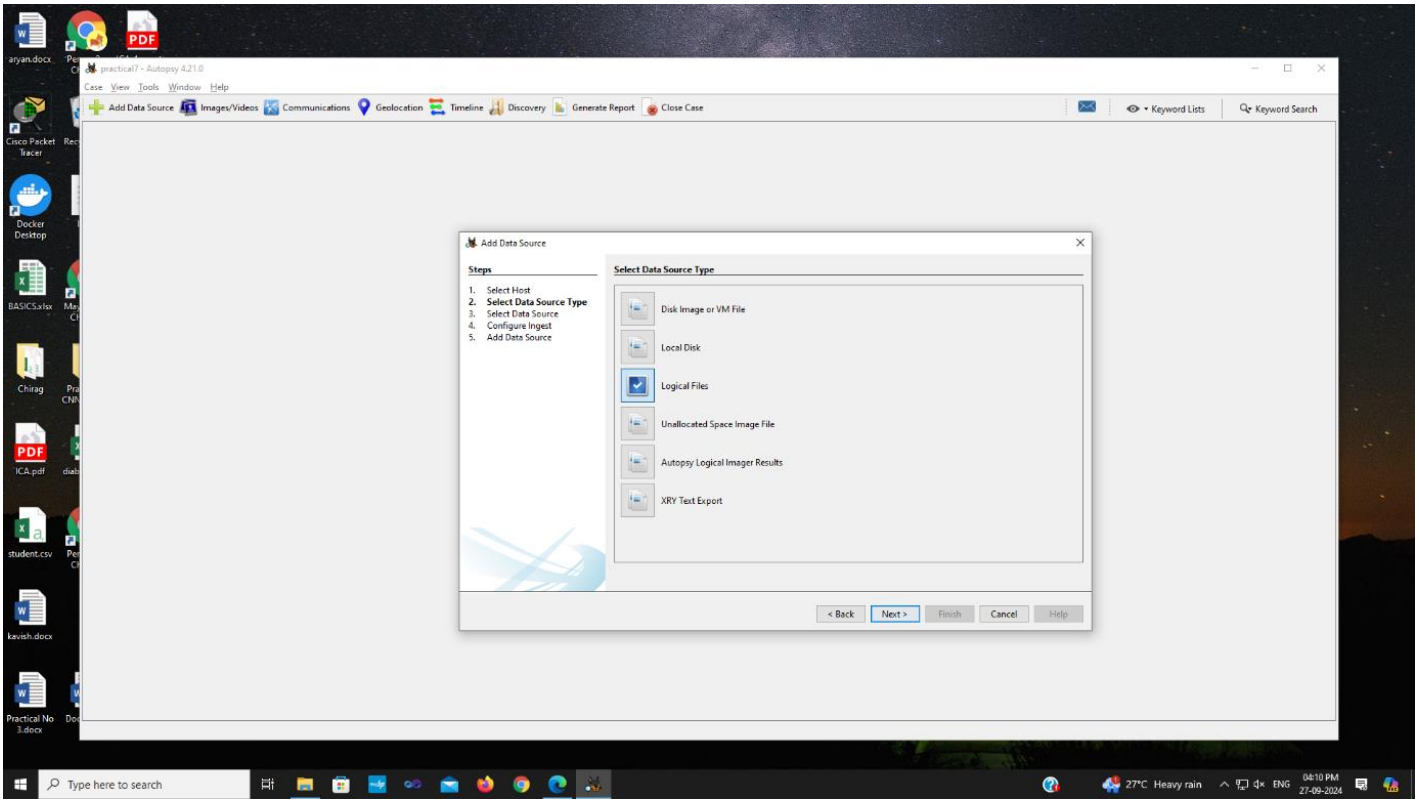
Practical 7

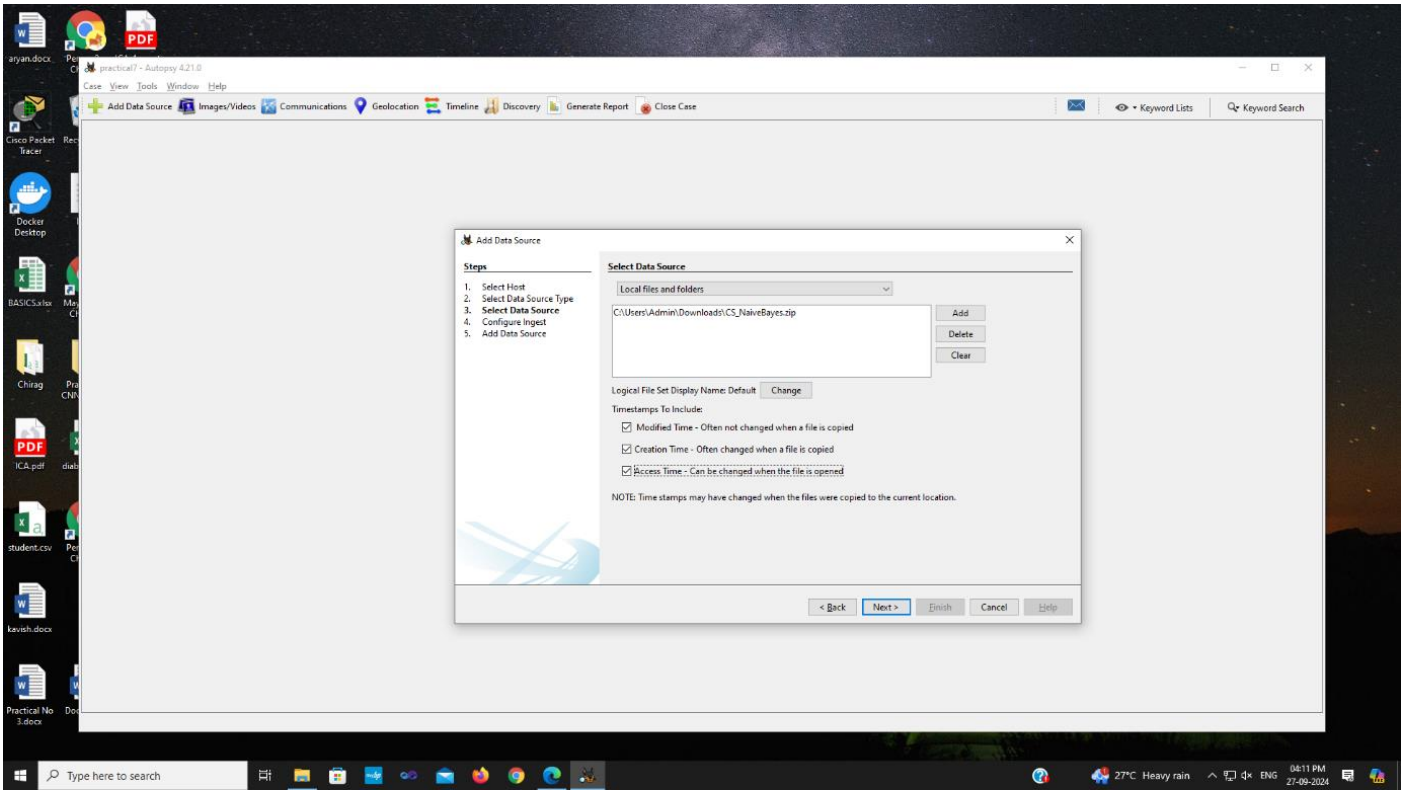
Cyber Security and Digital Forensics – Autopsy

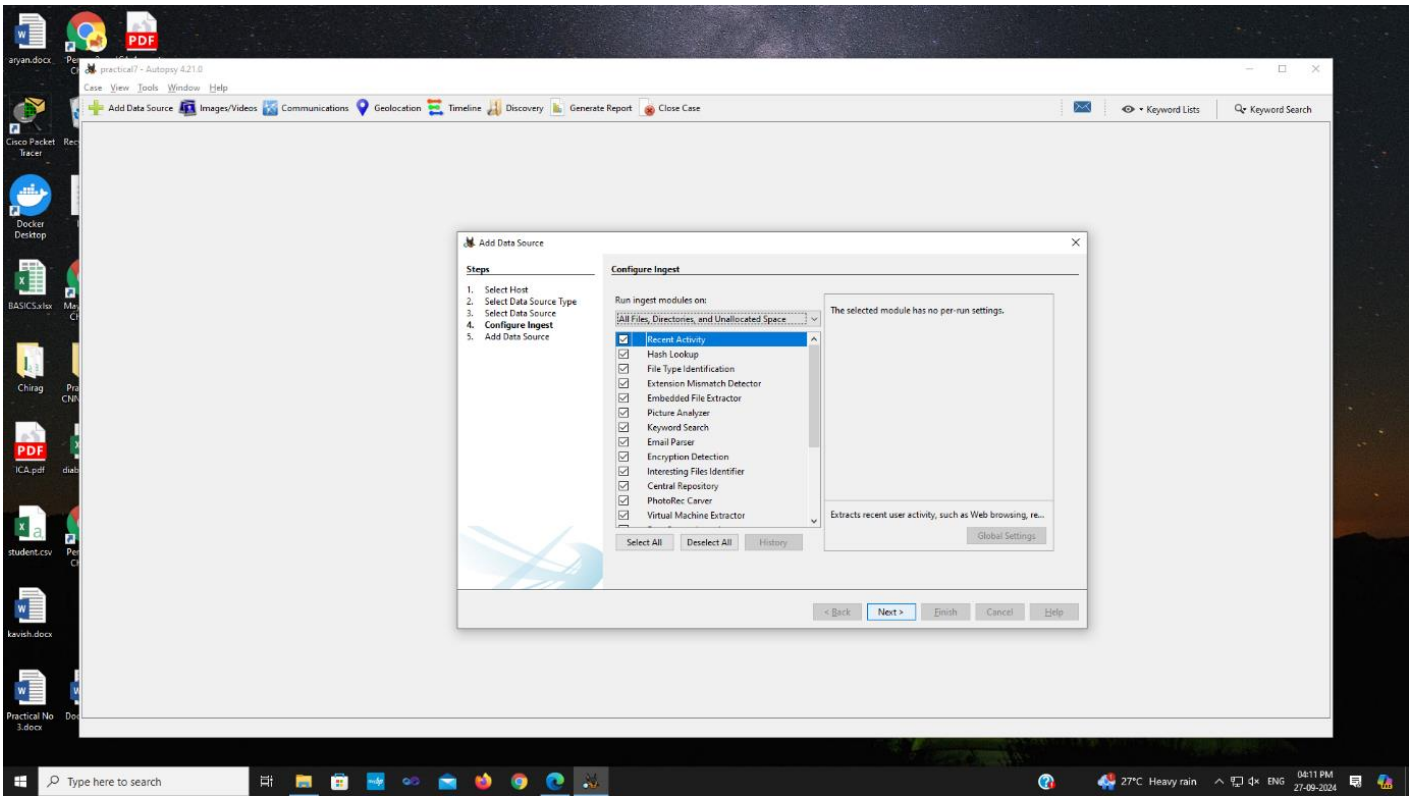


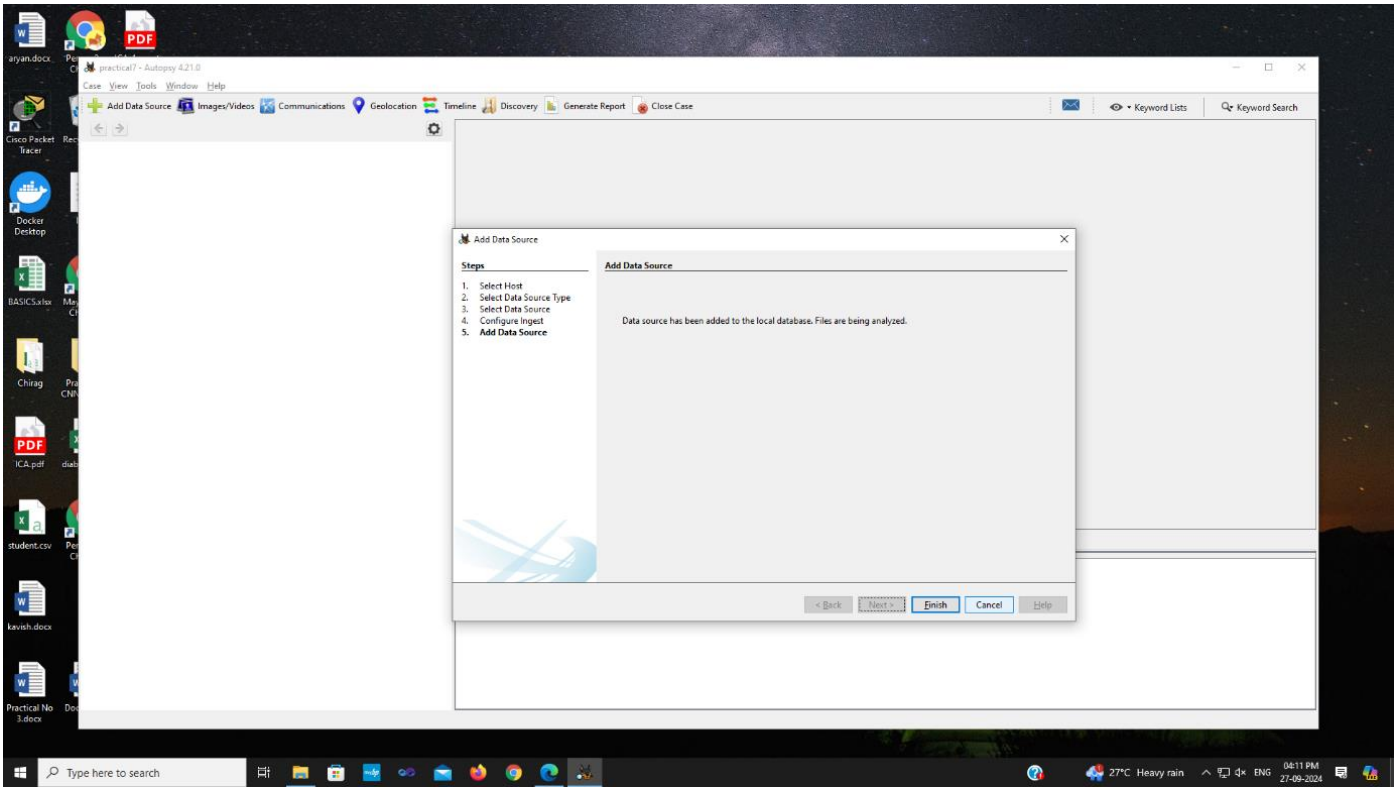


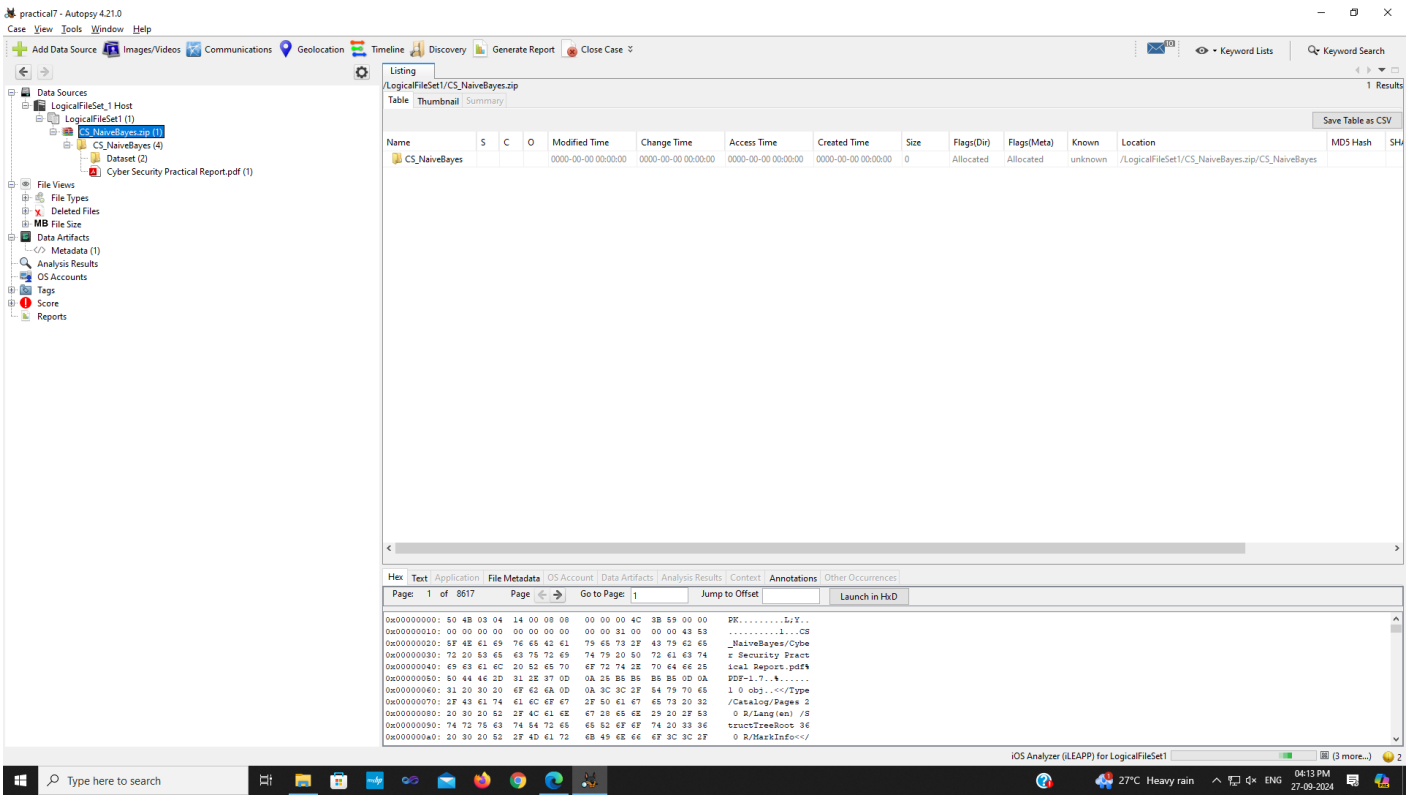

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help


practical7 - Autopsy 4.21.0
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
Select Data Source
Local files and folders
C:\Users\Admin\Downloads\CS_NaiveBayes.zip
Add
Delete
Clear
Logical File Set Display Name: Default
Change
Timestamps To Include:
Modified Time - Often not changed when a file is copied
Creation Time - Often changed when a file is copied
Access Time - Can be changed when the file is opened
NOTE: Time stamps may have changed when the files were copied to the current location.
< Back
Next >
Finish
Cancel
Help
Type here to search
27°C Heavy rain
ENG
04:11 PM
27-09-2024


practical7 - Autopsy 4.21.0
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
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, re...
Global Settings
Select All
Deselect All
History
< Back
Next >
Finish
Cancel
Help
Type here to search
27°C Heavy rain
ENG
04:11 PM
27-09-2024


practical7 - Autopsy 4.21.0
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
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help
Type here to search
27°C Heavy rain
ENG
04:11 PM
27-09-2024


practical7 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
LogicalFileSet_1 Host
LogicalFileSet1 (1)
CS_NaiveBayes.zip (1)
CS_NaiveBayes (4)
Dataset (2)
Cyber Security Practical Report.pdf (1)
File Views
File Types
Deleted Files
File Size
Data Artifacts
Metadata (1)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
/LogicalFileSet1/CS_NaiveBayes.zip
1 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
Location
MD5 Hash
CS_NaiveBayes
0000-00-00 00:00:00
Allocated
Allocated
unknown
/LogicalFileSet1/CS_NaiveBayes.zip/CS_NaiveBayes
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Page: 1 of 8617
Page
Go to Page:
Jump to Offset
Launch in HxD
0x00000000: 50 4B 03 04 14 00 08 08 00 00 00 4C 3B 59 00 00 PK.....L;Y..
0x00000010: 00 00 00 00 00 00 00 00 00 00 31 00 00 00 43 53 ....1...CS
0x00000020: 5F 4E 61 69 76 65 42 61 79 65 73 2F 43 79 62 65 _NaiveBayes/Cybe
0x00000030: 72 20 53 65 63 75 72 69 74 79 20 50 72 61 63 74 r Security Pract
0x00000040: 69 63 61 6C 20 52 65 70 6F 72 74 2E 70 64 66 25 ical Report.pdf%
0x00000050: 50 44 46 2D 31 2E 37 0D 0A 25 B5 B5 B5 0D 0A PDF-1.7..%.....
0x00000060: 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 1 0 obj..<</Type
0x00000070: 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20 32 /Catalog/Pages 2
0x00000080: 20 30 20 52 2F 4C 61 6E 67 28 65 6E 29 20 2F 53 0 R/Lang(en) /S
0x00000090: 74 72 75 63 74 54 72 65 65 52 6F 6F 74 20 33 36 tructTreeRoot 36
0x000000a0: 20 30 20 52 2F 4D 61 72 6B 49 6E 66 6F 3C 3C 2F 0 R/MarkInfo<</
iOS Analyzer (iLEAPP) for LogicalFileSet1
(3 more...)
Type here to search
27°C Heavy rain
ENG
04:13 PM
27-09-2024