Institute of Information Technology (IIT)

Jahangirnagar University

EDGE- B11 Cyber Security.

Project No 3:

Disk Forensics with Autopsy and FTK Imager

Submitted By

Name: Shariful Islam

ID No: 2111252

Batch No: B-11

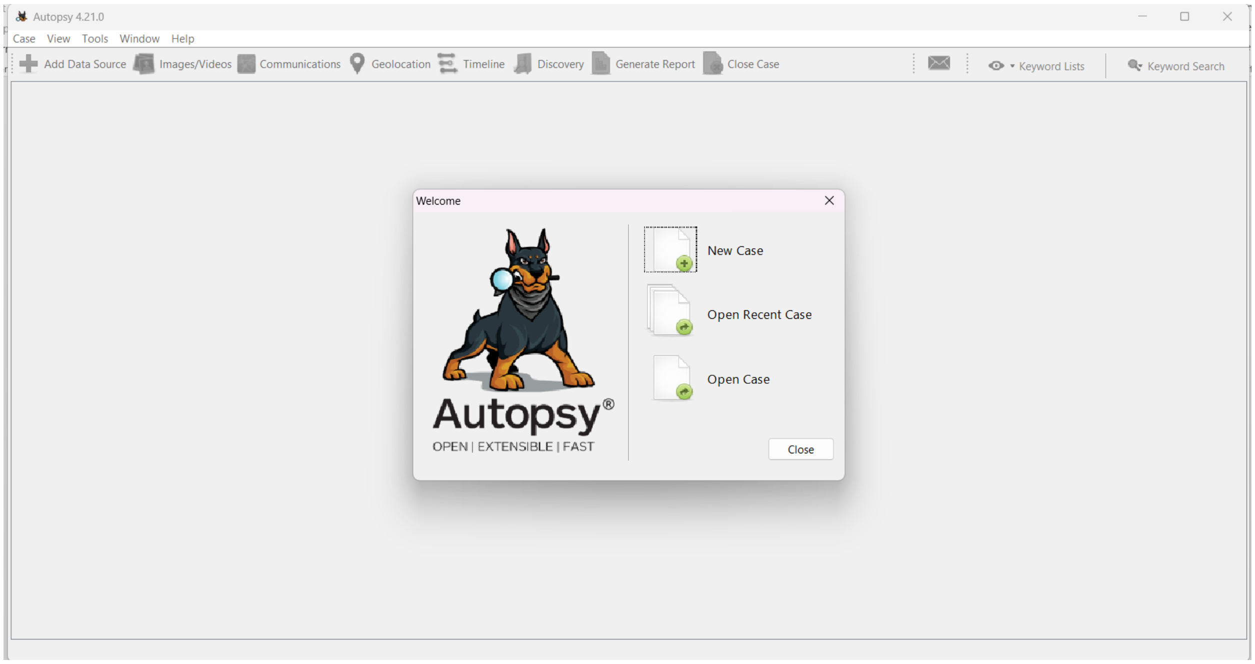
Submitted To

Moinoddeen Quader Al Arabi

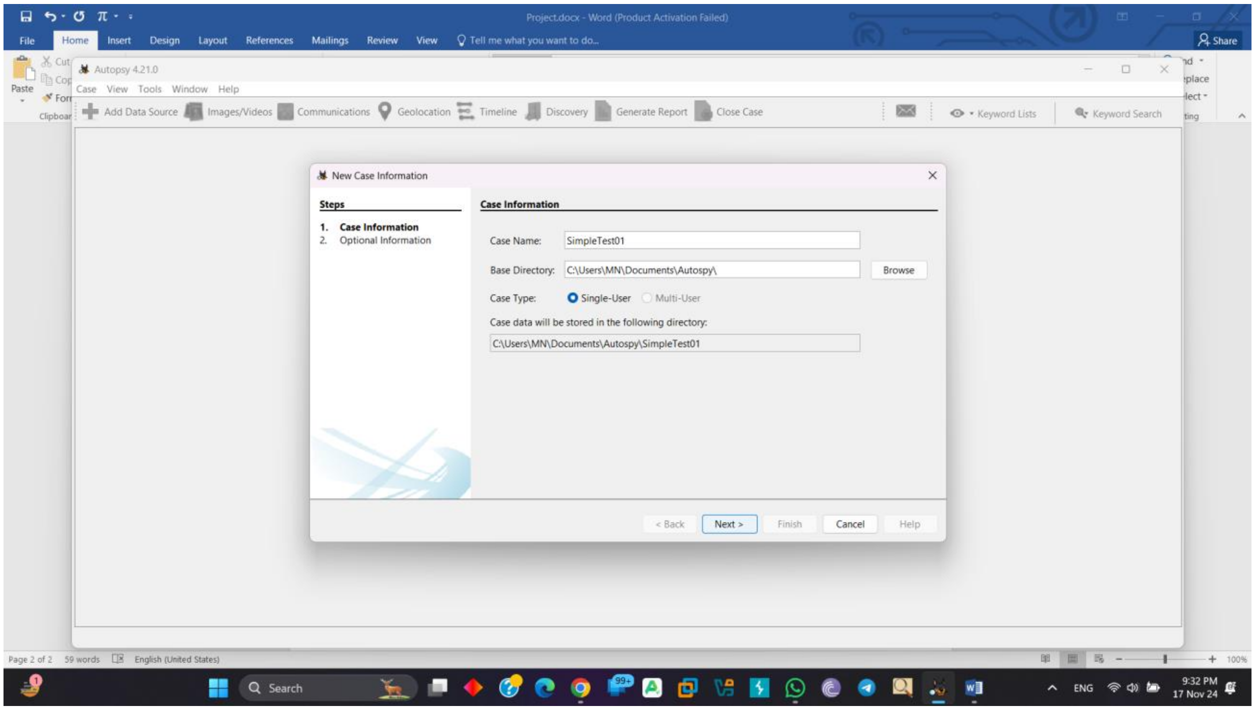
Ethical Hacker, Forensic Investigator, and VAPT Expert Cyber Security Consultant in Dhaka Division, Bangladesh

Disk Forensics with Autopsy

Create New Case:



Set a Case Name and Base directory:



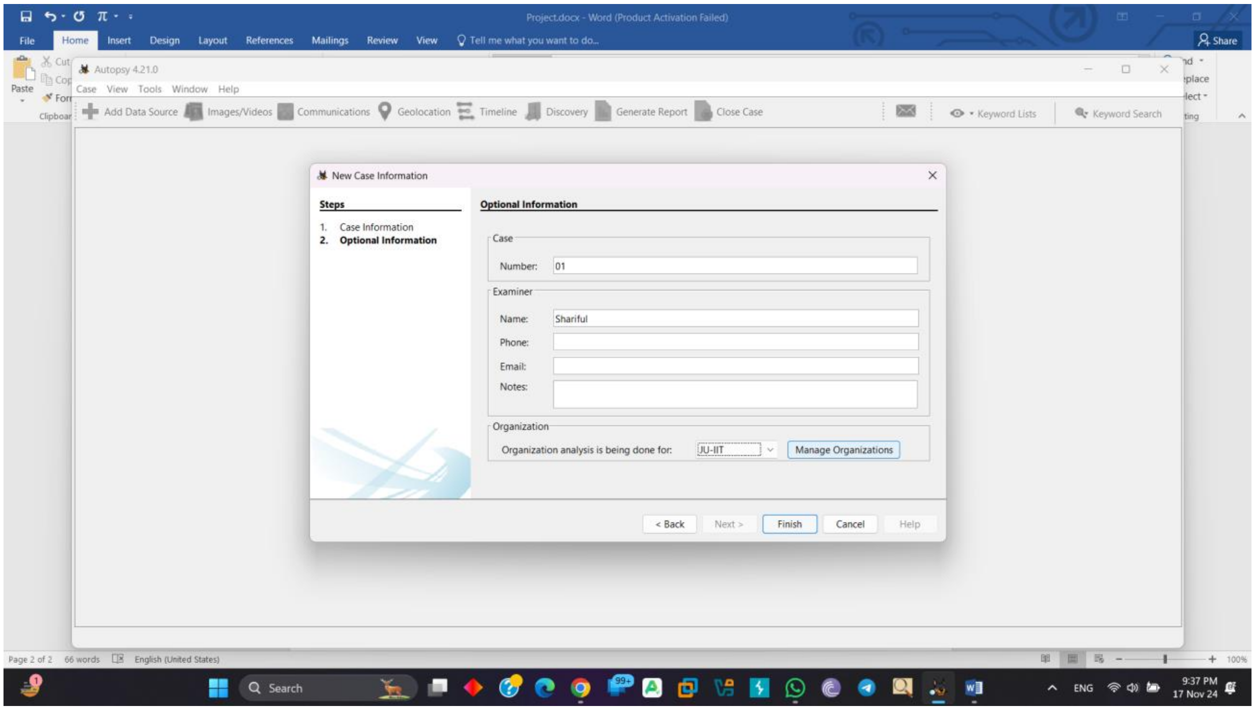
Case Name: SimpleTest01

Base Directory: C:\Users\MN\Documents\Autopsy\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\MN\Documents\Autopsy\SimpleTest01



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 01

Examiner

Name: Shariful

Phone:

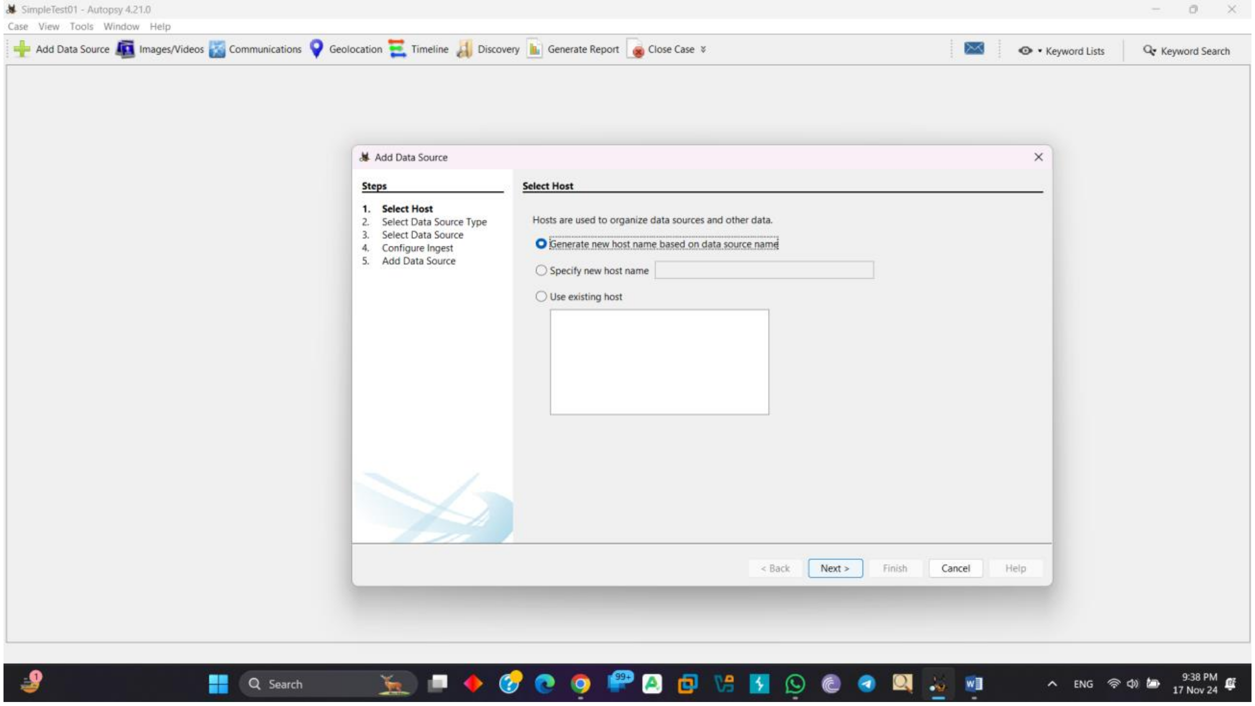
Email:

Notes:

Organization

Organization analysis is being done for: JU-IIT

Select a Host (Ex: Generate New Host name based on data source name)



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

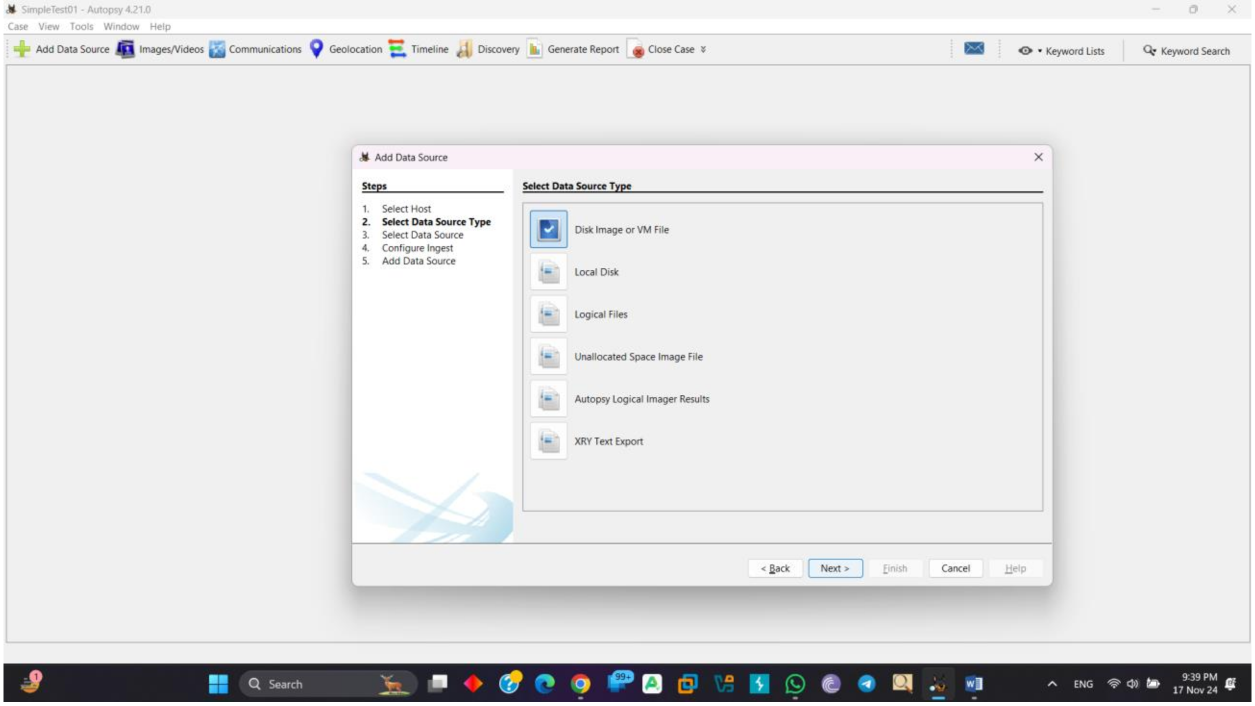
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Select any one type of disk:


SimpleTest01 - 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
< Back Next > Finish Cancel Help
Search
ENG
9:39 PM
17 Nov 24

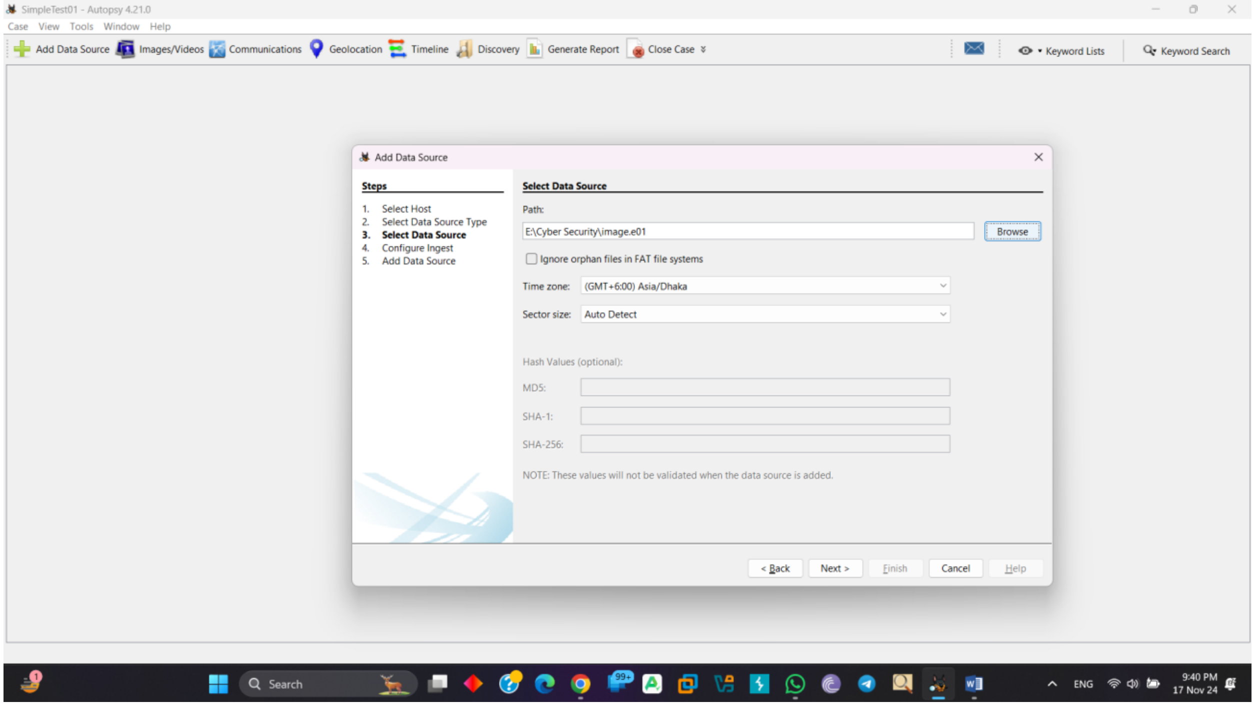
Steps

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

Browse the image:


SimpleTest01 - 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
Browse
< Back Next > Finish Cancel Help
Search
ENG
9:40 PM
17 Nov 24

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: E:\Cyber Security\image.e01

☐ Ignore orphan files in FAT file systems

Time zone: (GMT+6:00) Asia/Dhaka

Sector size: Auto Detect

Hash Values (optional):

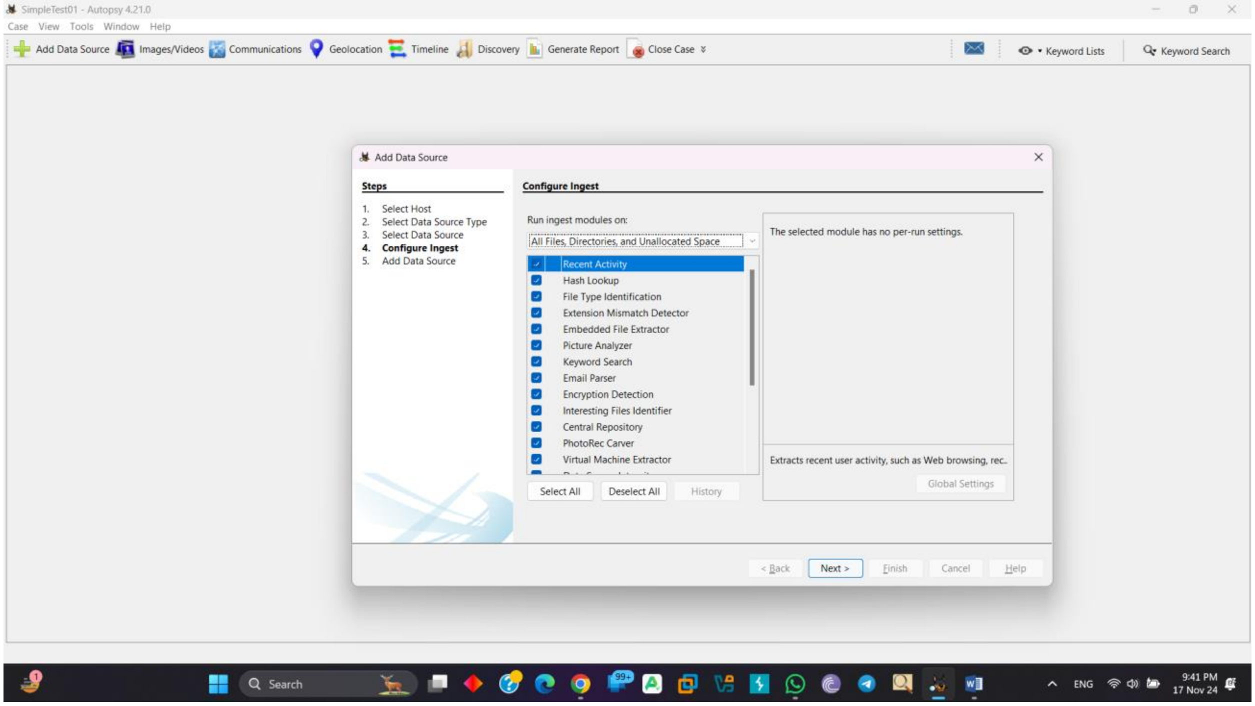
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Select needed item and enter next:



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

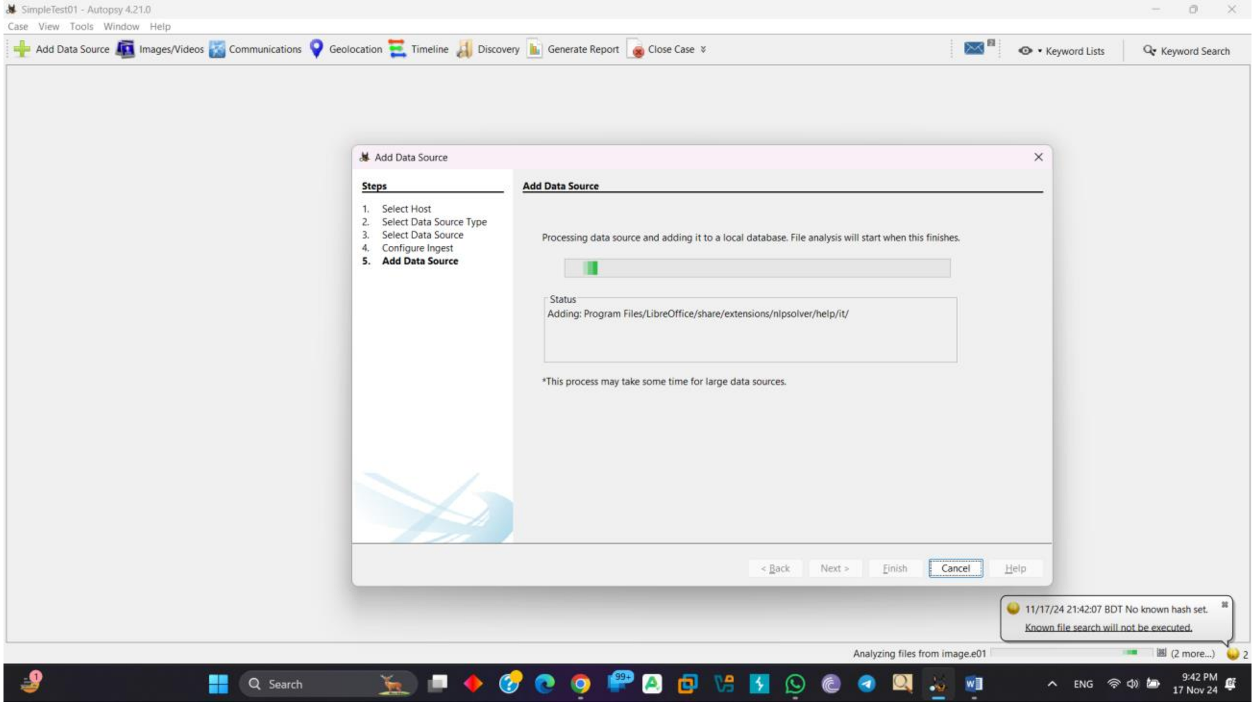
Run ingest modules on:
All Files, Directories, and Unallocated Space

- ☑ 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, rec...

Here add data source:



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

Processing data source and adding it to a local database. File analysis will start when this finishes.

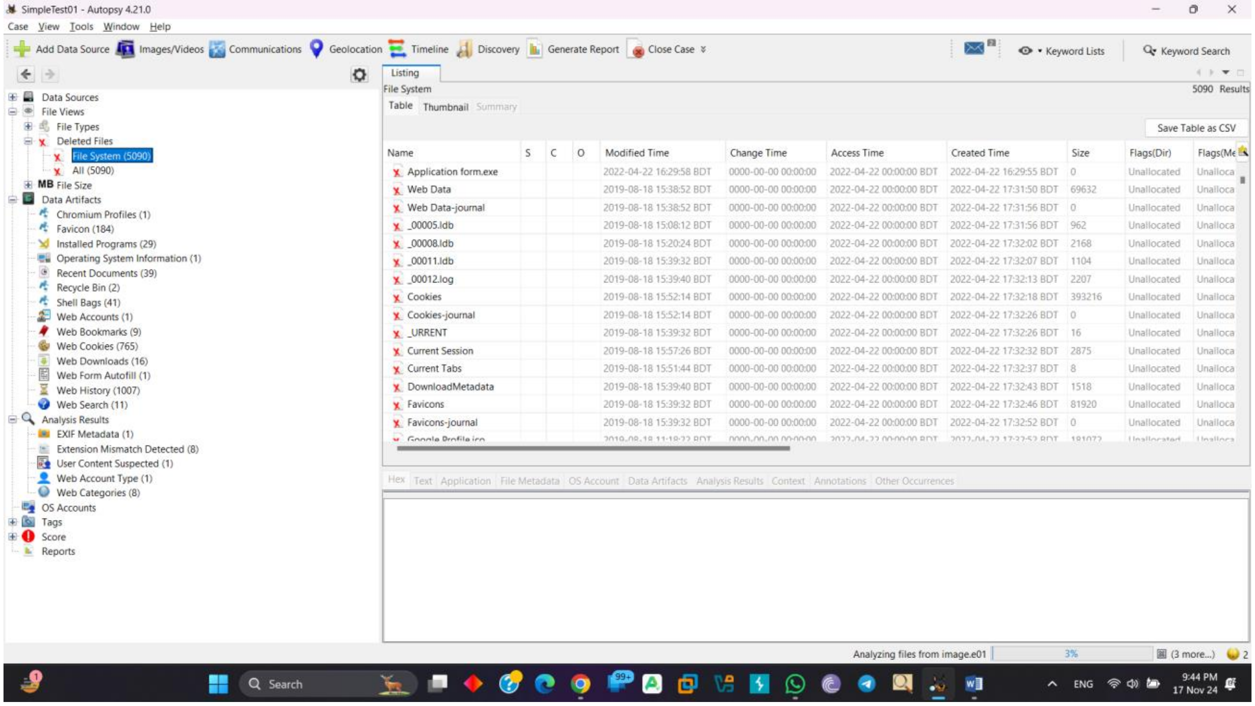
Status
Adding: Program Files/LibreOffice/share/extensions/nlpsolver/help/it/

*This process may take some time for large data sources.

11/17/24 21:42:07 BDT No known hash set.
Known file search will not be executed.

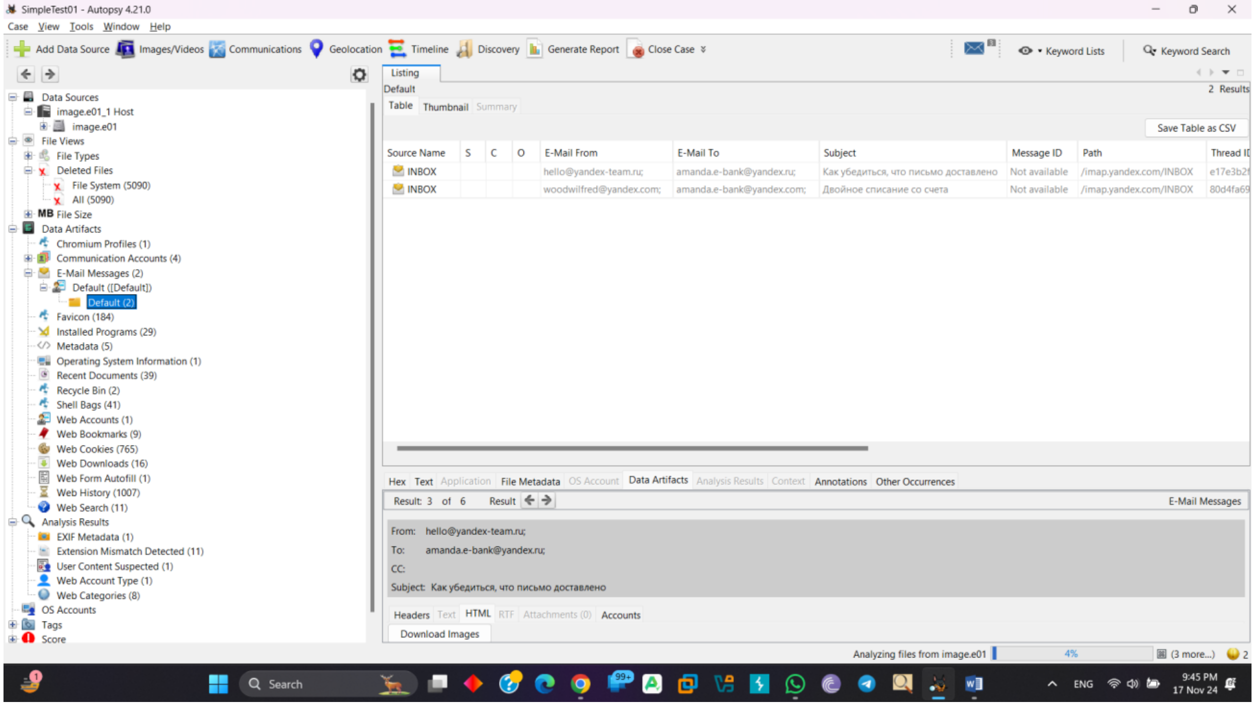
Analyzing files from image.e01

Here is 5090 Delete file:



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
Application form.exe				2022-04-22 16:29:58 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 16:29:55 BDT	0	Unallocated	Unalloca
Web Data				2019-08-18 15:38:52 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:31:50 BDT	69632	Unallocated	Unalloca
Web Data-journal				2019-08-18 15:38:52 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:31:56 BDT	0	Unallocated	Unalloca
_00005.ldb				2019-08-18 15:08:12 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:31:56 BDT	962	Unallocated	Unalloca
_00008.ldb				2019-08-18 15:20:24 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:02 BDT	2168	Unallocated	Unalloca
_00011.ldb				2019-08-18 15:39:32 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:07 BDT	1104	Unallocated	Unalloca
_00012.log				2019-08-18 15:39:40 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:13 BDT	2207	Unallocated	Unalloca
Cookies				2019-08-18 15:52:14 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:18 BDT	393216	Unallocated	Unalloca
Cookies-journal				2019-08-18 15:52:14 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:26 BDT	0	Unallocated	Unalloca
_URRENT				2019-08-18 15:39:32 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:26 BDT	16	Unallocated	Unalloca
Current Session				2019-08-18 15:57:26 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:32 BDT	2875	Unallocated	Unalloca
Current Tabs				2019-08-18 15:51:44 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:37 BDT	8	Unallocated	Unalloca
DownloadMetadata				2019-08-18 15:39:40 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:43 BDT	1518	Unallocated	Unalloca
Favicons				2019-08-18 15:39:32 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:46 BDT	81920	Unallocated	Unalloca
Favicons-journal				2019-08-18 15:39:32 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:52 BDT	0	Unallocated	Unalloca
Google Profile.ico				2019-08-18 11:18:22 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:52 BDT	181072	Unallocated	Unalloca

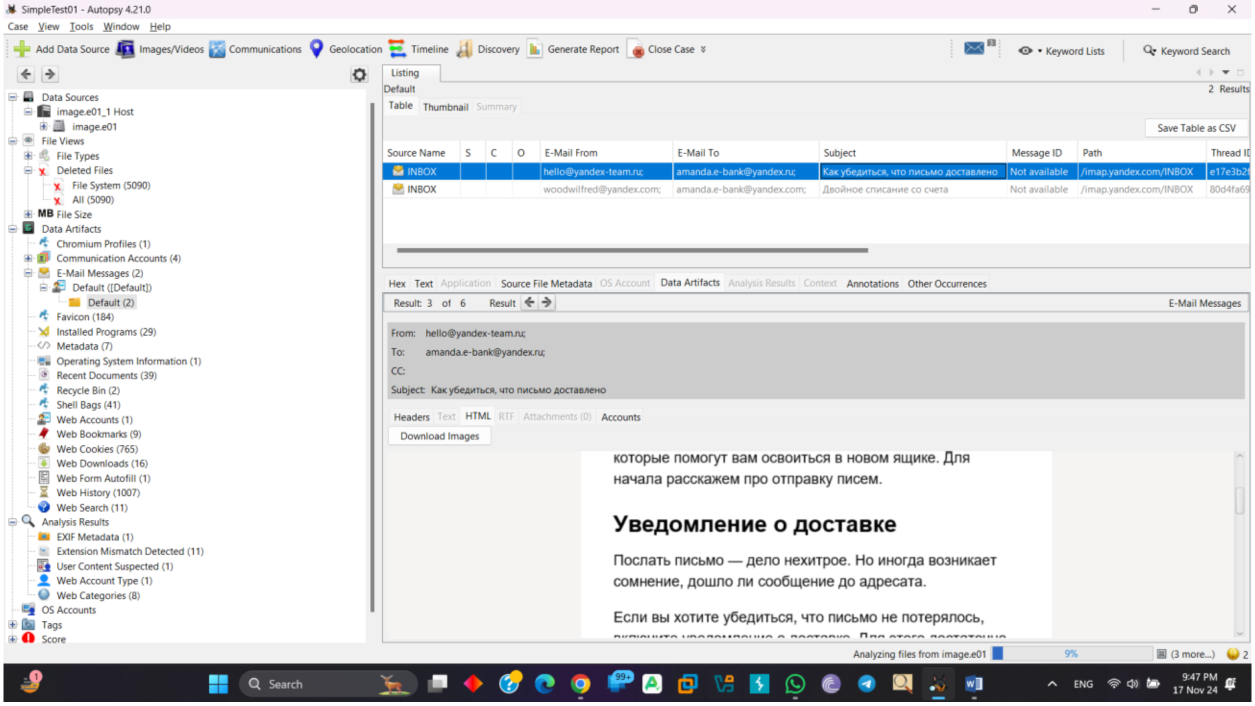
Here are two-email message:



Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Message ID	Path	Thread ID
INBOX				hello@yandex-team.ru;	amanda.e-bank@yandex.ru;	Как убедиться, что письмо доставлено	Not available	/imap.yandex.com/INBOX	e17e3b2f
INBOX				woodwilfred@yandex.com;	amanda.e-bank@yandex.com;	Двойное списание со счета	Not available	/imap.yandex.com/INBOX	80d4fa69

From: hello@yandex-team.ru;
To: amanda.e-bank@yandex.ru;
CC:
Subject: Как убедиться, что письмо доставлено

Here is show email from/email to and text of email:



Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Message ID	Path	Thread ID
INBOX				hello@yandex-team.ru;	amanda.e-bank@yandex.ru;	Как убедиться, что письмо доставлено	Not available	/imap.yandex.com/INBOX	e17e3b2f
INBOX				woodwilfred@yandex.com;	amanda.e-bank@yandex.com;	Двойное списание со счета	Not available	/imap.yandex.com/INBOX	80d4fa69

From: hello@yandex-team.ru;
To: amanda.e-bank@yandex.ru;
CC:
Subject: Как убедиться, что письмо доставлено

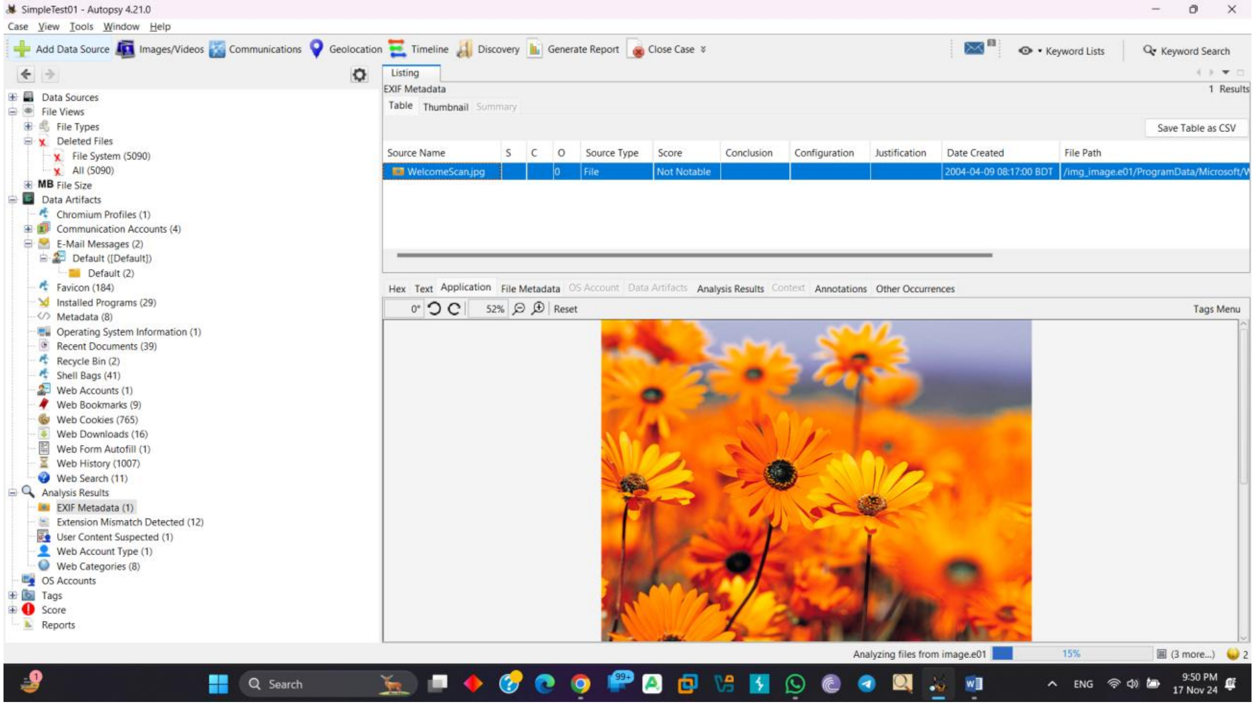
которые помогут вам освоиться в новом ящике. Для начала расскажем про отправку писем.

Уведомление о доставке

Послать письмо — дело нехитрое. Но иногда возникает сомнение, дошло ли сообщение до адресата.

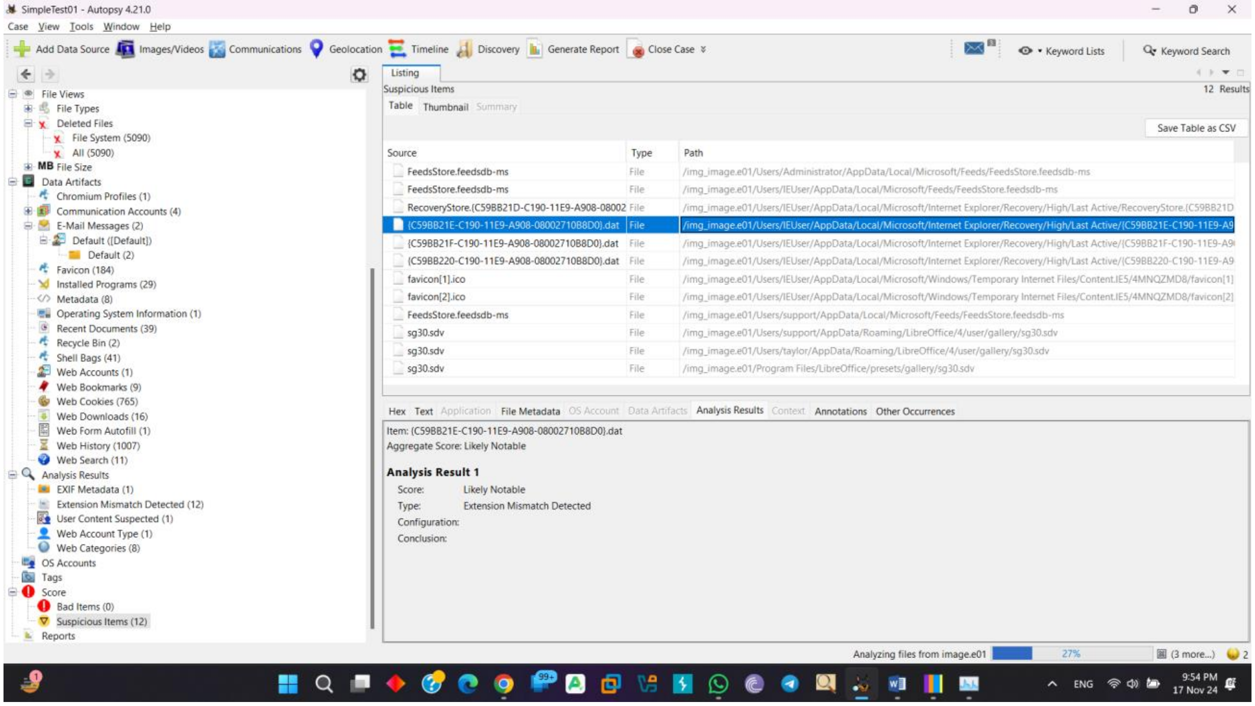
Если вы хотите убедиться, что письмо не потерялось,

Here is an EXIF Metadata:



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Date Created	File Path
WelcomeScan.jpg			0	File	Not Notable				2004-04-09 08:17:00 BDT	/img_image.e01/ProgramData/Microsoft/W

There are 12 suspicious item:



Suspicious Items 12 Results

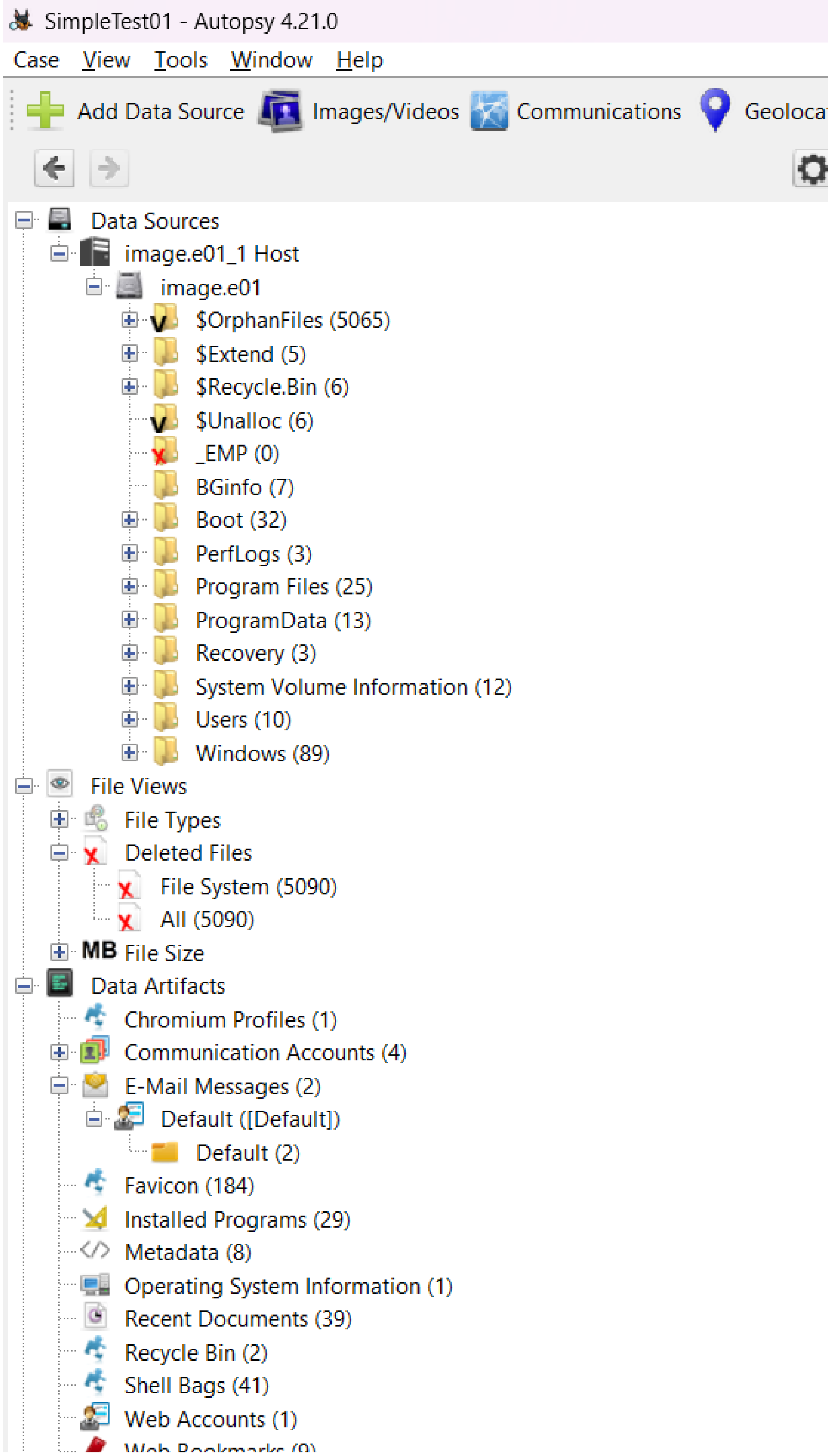
Source	Type	Path
FeedsStore.feedsdb-ms	File	/img_image.e01/Users/Administrator/AppData/Local/Microsoft/Feeds/FeedsStore.feedsdb-ms
FeedsStore.feedsdb-ms	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Feeds/FeedsStore.feedsdb-ms
RecoveryStore.{C59BB21D-C190-11E9-A908-08002	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/RecoveryStore.{C59BB21D
{C59BB21E-C190-11E9-A908-08002710B8D0}.dat	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/{C59BB21E-C190-11E9-A9
{C59BB21F-C190-11E9-A908-08002710B8D0}.dat	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/{C59BB21F-C190-11E9-A9
{C59BB220-C190-11E9-A908-08002710B8D0}.dat	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/{C59BB220-C190-11E9-A9
favicon[1].ico	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/4MNQZMD8/favicon[1]
favicon[2].ico	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/4MNQZMD8/favicon[2]
FeedsStore.feedsdb-ms	File	/img_image.e01/Users/support/AppData/Local/Microsoft/Feeds/FeedsStore.feedsdb-ms
sg30.sdv	File	/img_image.e01/Users/support/AppData/Roaming/LibreOffice/4/user/gallery/sg30.sdv
sg30.sdv	File	/img_image.e01/Users/taylor/AppData/Roaming/LibreOffice/4/user/gallery/sg30.sdv
sg30.sdv	File	/img_image.e01/Program Files/LibreOffice/presets/gallery/sg30.sdv

Item: {C59BB21E-C190-11E9-A908-08002710B8D0}.dat
Aggregate Score: Likely Notable

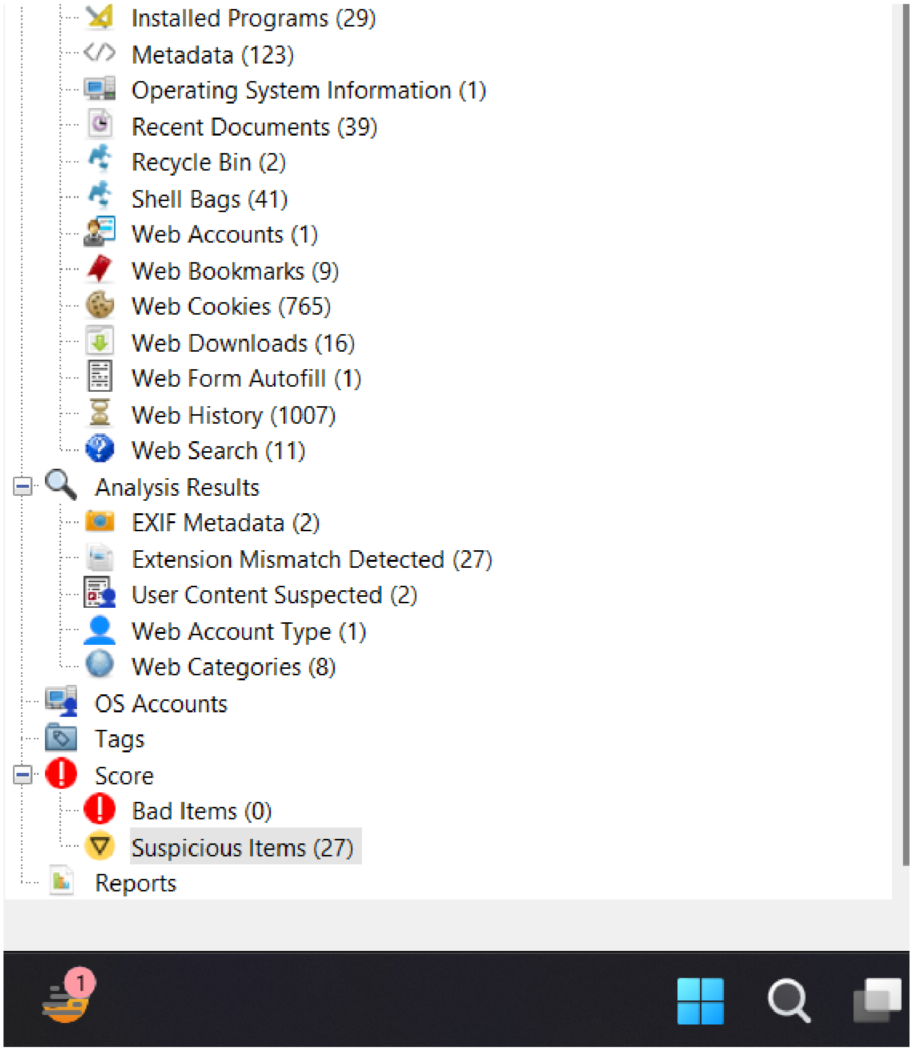
Analysis Result 1

Score: Likely Notable
Type: Extension Mismatch Detected
Configuration:
Conclusion:

In addition, more other report item:



```
Data Sources
  image.e01_1 Host
    image.e01
      $OrphanFiles (5065)
      $Extend (5)
      $Recycle.Bin (6)
      $Unalloc (6)
      _EMP (0)
      BGinfo (7)
      Boot (32)
      PerfLogs (3)
      Program Files (25)
      ProgramData (13)
      Recovery (3)
      System Volume Information (12)
      Users (10)
      Windows (89)
File Views
  File Types
  Deleted Files
    File System (5090)
    All (5090)
  MB File Size
Data Artifacts
  Chromium Profiles (1)
  Communication Accounts (4)
  E-Mail Messages (2)
    Default ([Default])
      Default (2)
  Favicon (184)
  Installed Programs (29)
  Metadata (8)
  Operating System Information (1)
  Recent Documents (39)
  Recycle Bin (2)
  Shell Bags (41)
  Web Accounts (1)
  Web Bookmarks (9)
```



- Installed Programs (29)
- Metadata (123)
- Operating System Information (1)
- Recent Documents (39)
- Recycle Bin (2)
- Shell Bags (41)
- Web Accounts (1)
- Web Bookmarks (9)
- Web Cookies (765)
- Web Downloads (16)
- Web Form Autofill (1)
- Web History (1007)
- Web Search (11)

Analysis Results

- EXIF Metadata (2)
- Extension Mismatch Detected (27)
- User Content Suspected (2)
- Web Account Type (1)
- Web Categories (8)

OS Accounts

Tags

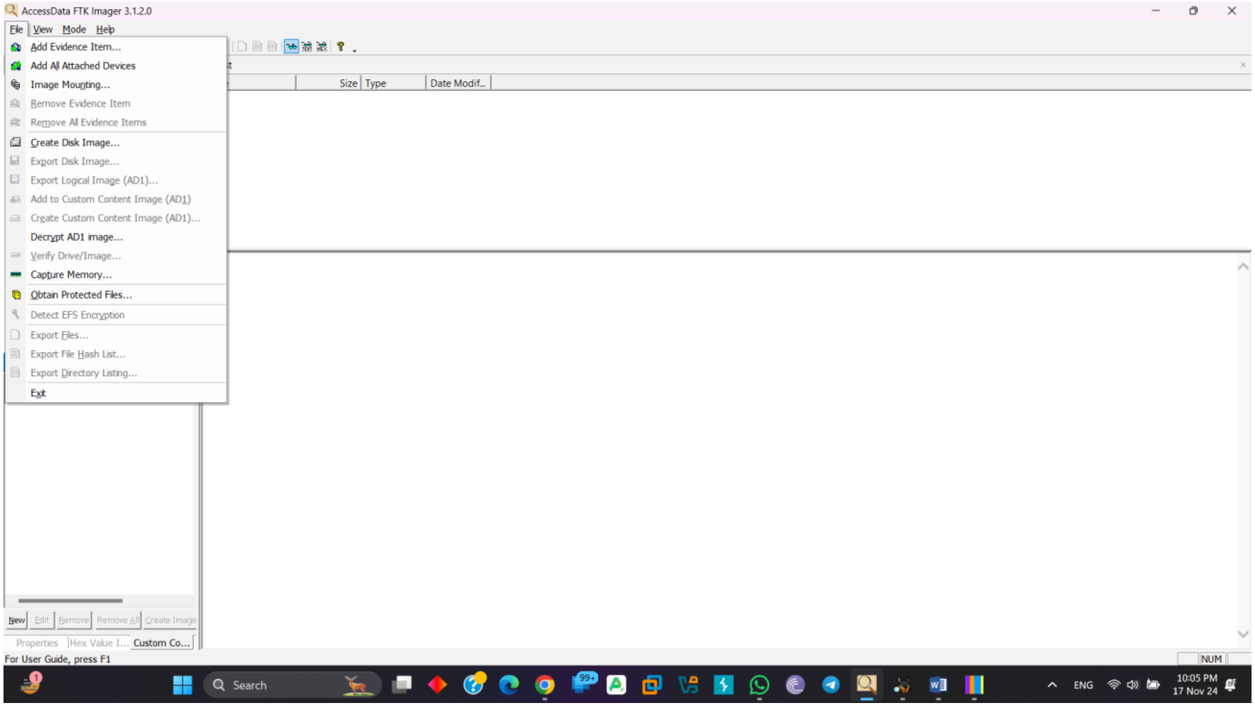
Score

- Bad Items (0)
- Suspicious Items (27)

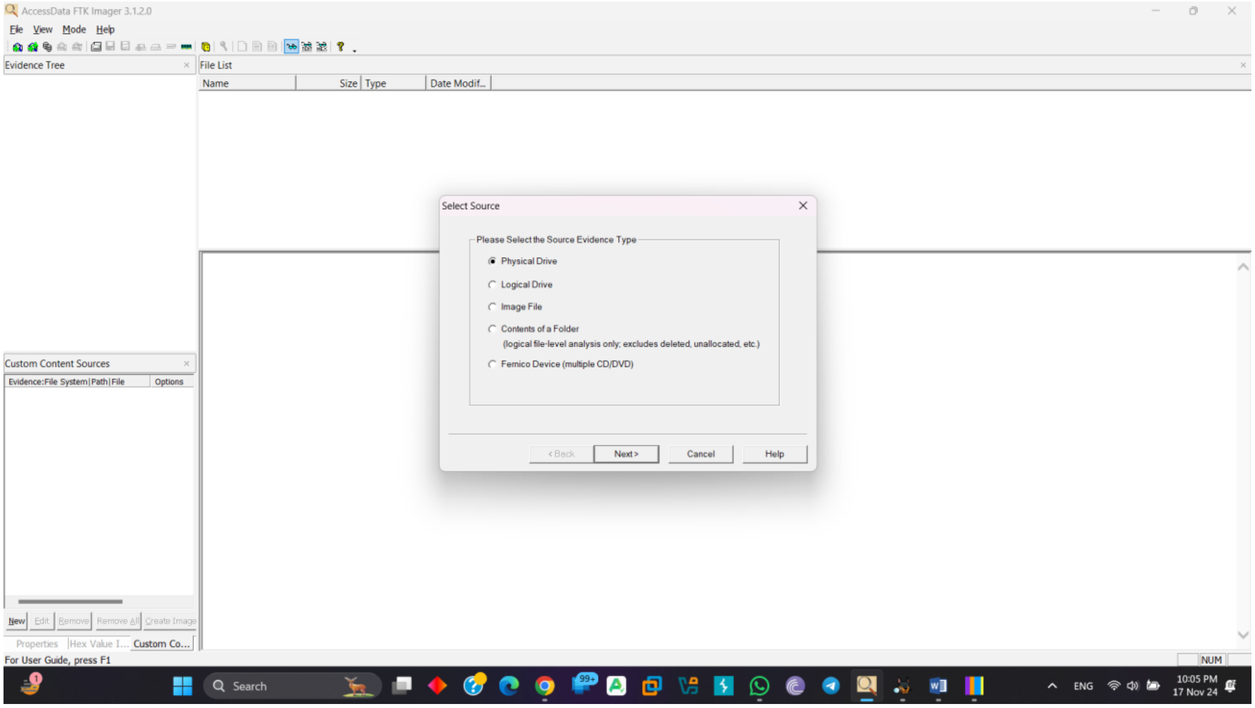
Reports

Disk Forensics with FTK Imager

In the beginning go to File→Create new disk:



Select any one type:



Please Select the Source Evidence Type

● Physical Drive

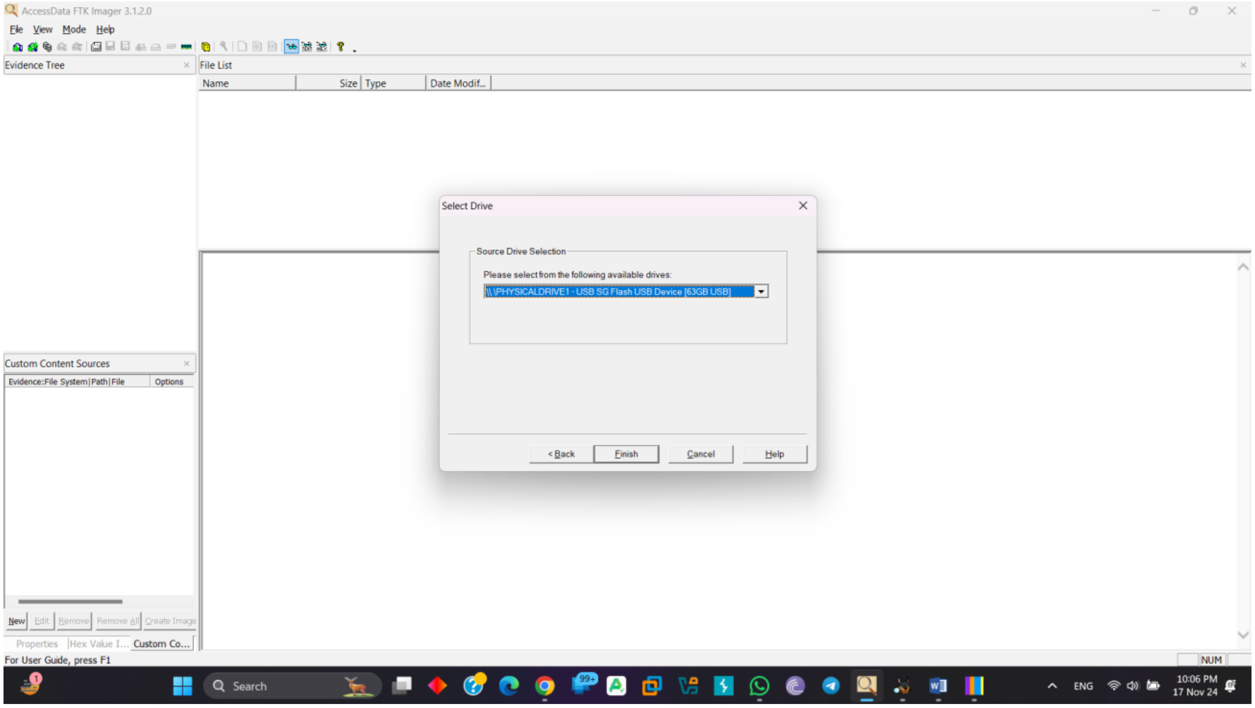
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

Select the drive:



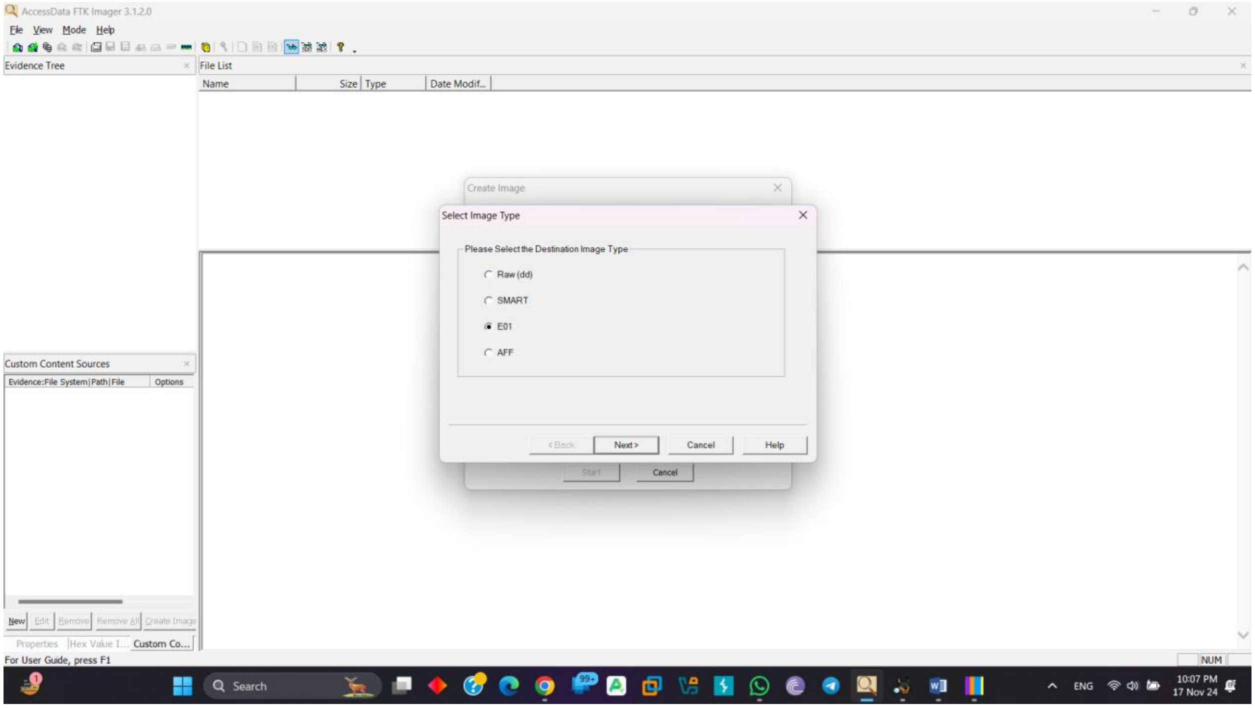
Select Drive

Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - USB SG Flash USB Device [63GB USB]

Add image type (any one from them):



Select Image Type

Please Select the Destination Image Type

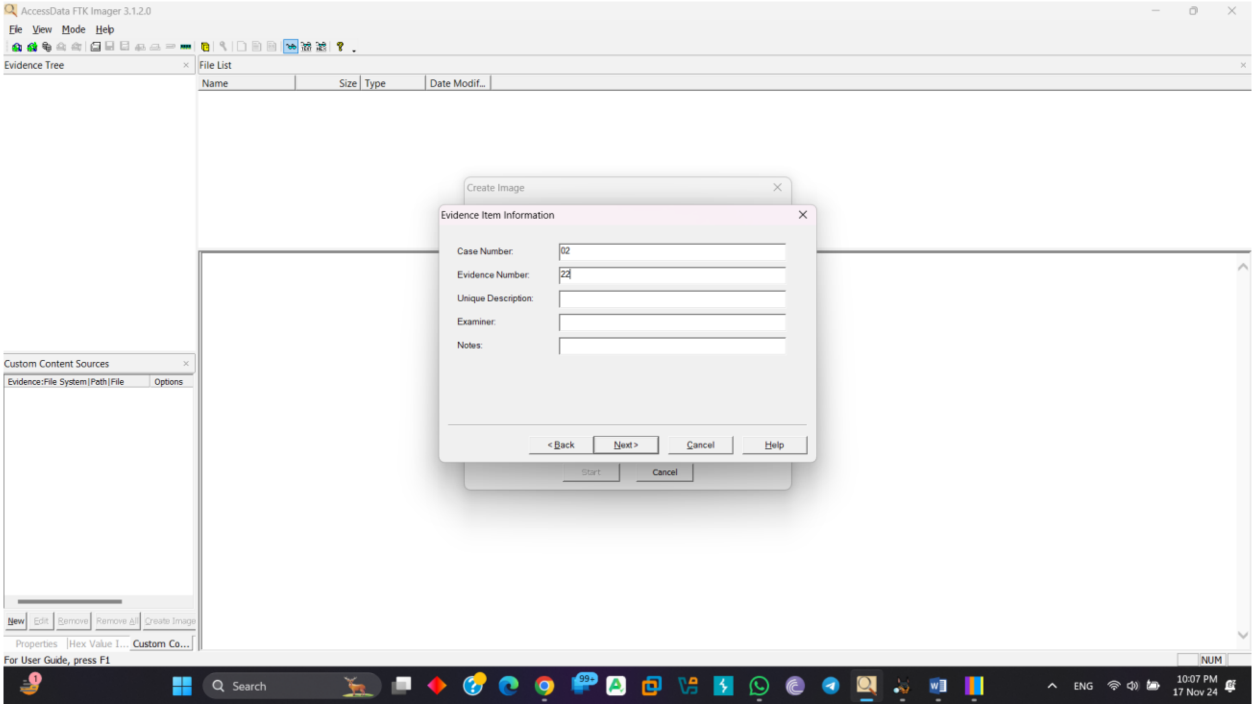
○ Raw (dd)

○ SMART

● E01

○ AFF

Set Evidence Item Information:



Evidence Item Information

Case Number: 02

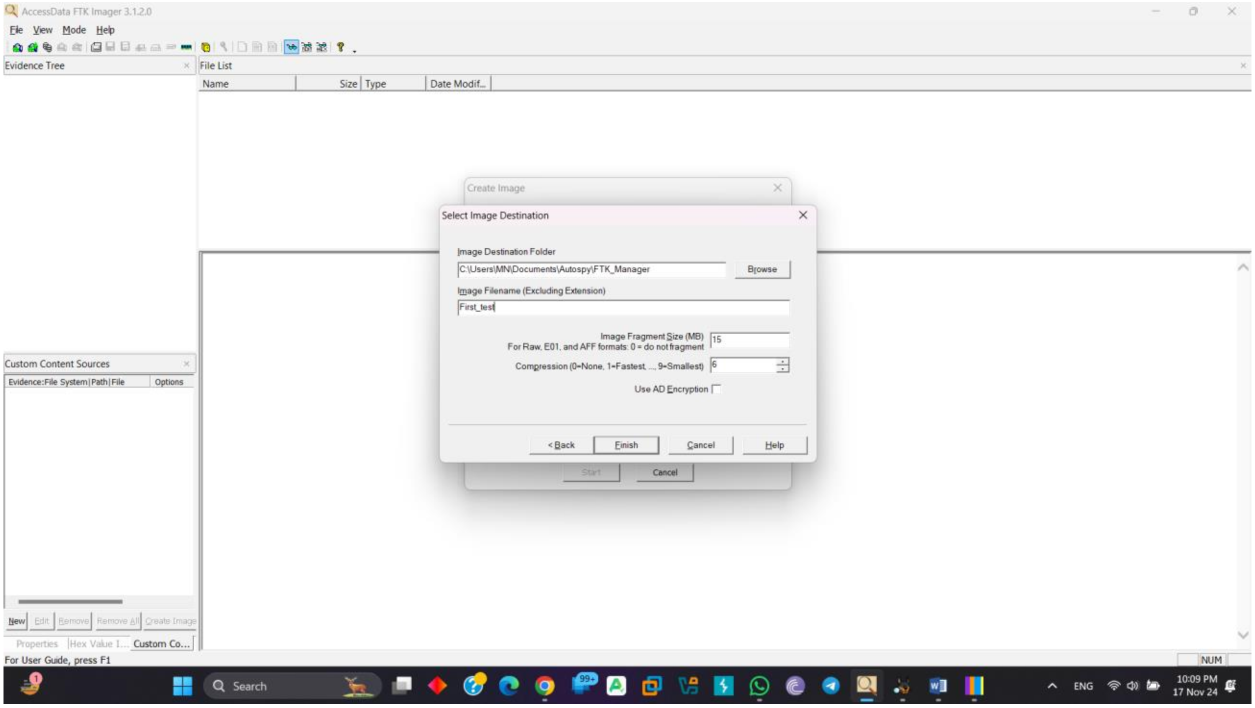
Evidence Number: 22

Unique Description:

Examiner:

Notes:

Select Destination folder and set file name and can resize Image Fragment size:



Select Image Destination

Image Destination Folder: C:\Users\MN\Documents\Autospy\FTK_Manager

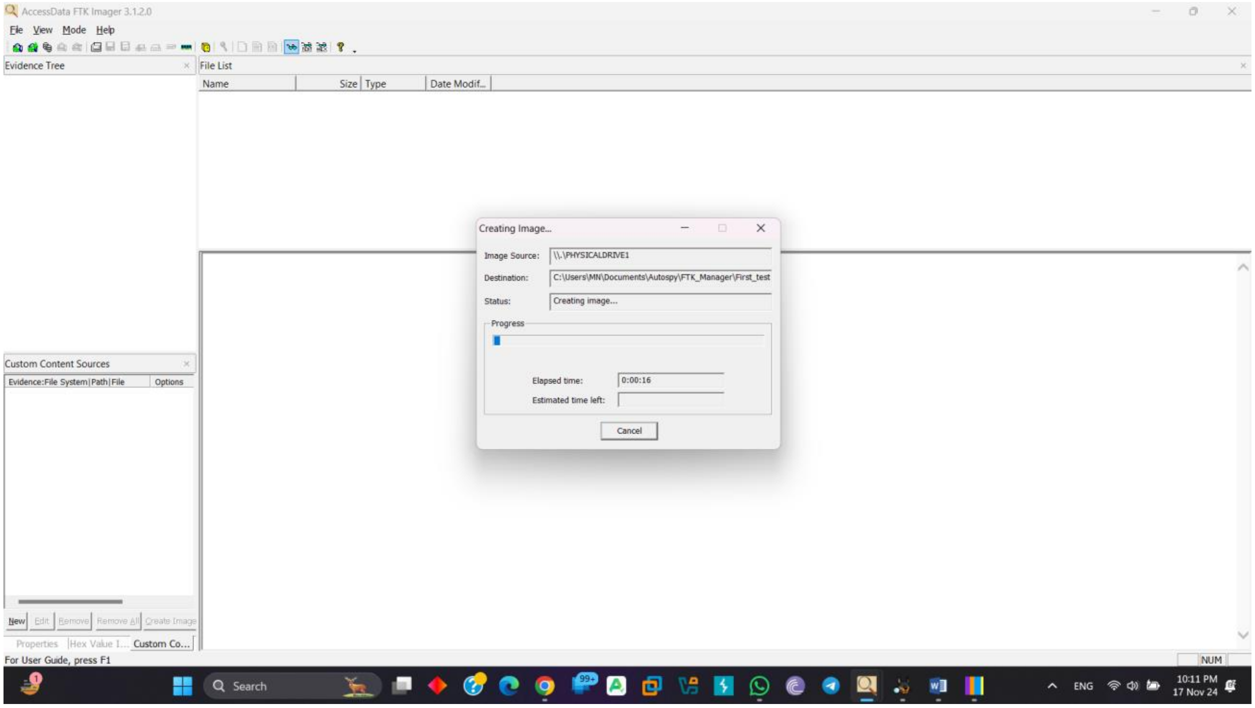
Image Filename (Excluding Extension): First_test

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 15

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption □

Its take huge number of time for Processing depends on processing disk size:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\MN\Documents\Autospy\FTK_Manager\First_test

Status: Creating image...

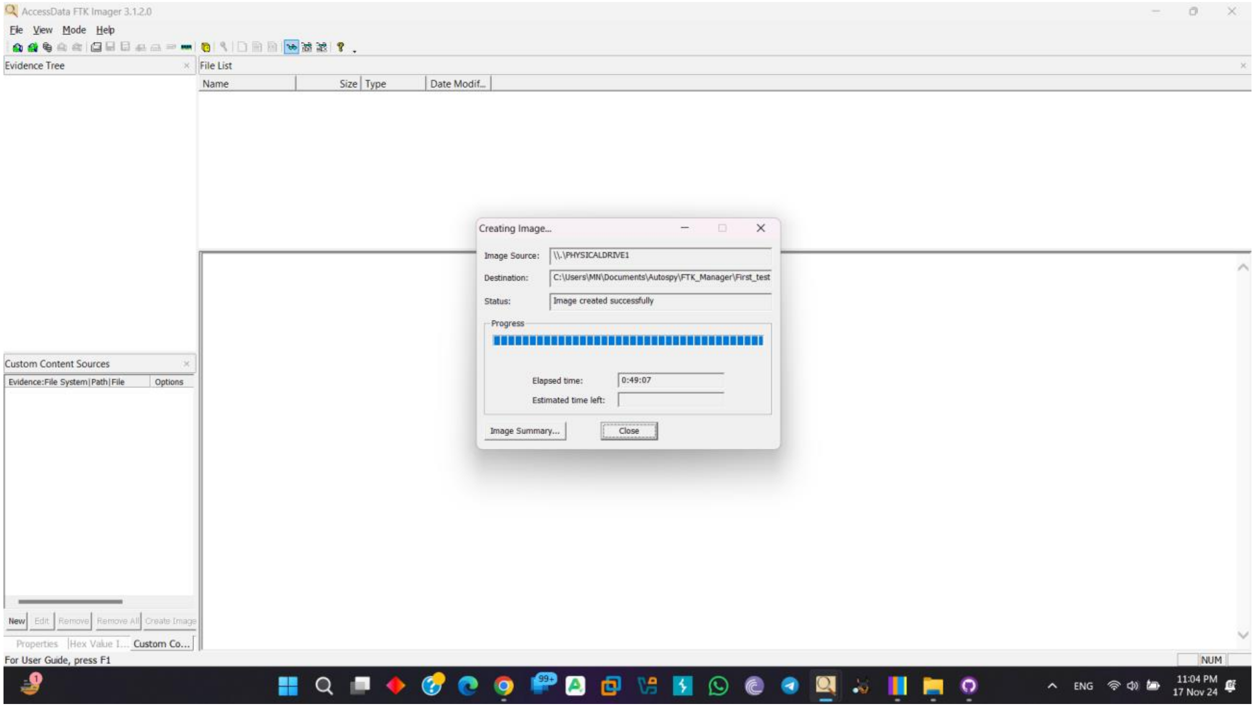
Progress

Elapsed time: 0:00:16

Estimated time left:

Cancel

It’s take about 49 minutes to execute:



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\MN\Documents\Autospy\FTK_Manager\First_test

Status: Image created successfully

Progress

Elapsed time: 0:49:07

Estimated time left:

Image Summary...

Close