



INSTITUTE OF INFORMATION TECHNOLOGY JAHANGIRNAGAR UNIVERSITY

Number of Project	: 02
Name of Project	: Disk Forensics with Autopsy and FTK Imager
Course Title	: Cyber Security
Submission Date	: 19/11/2024

Submitted To

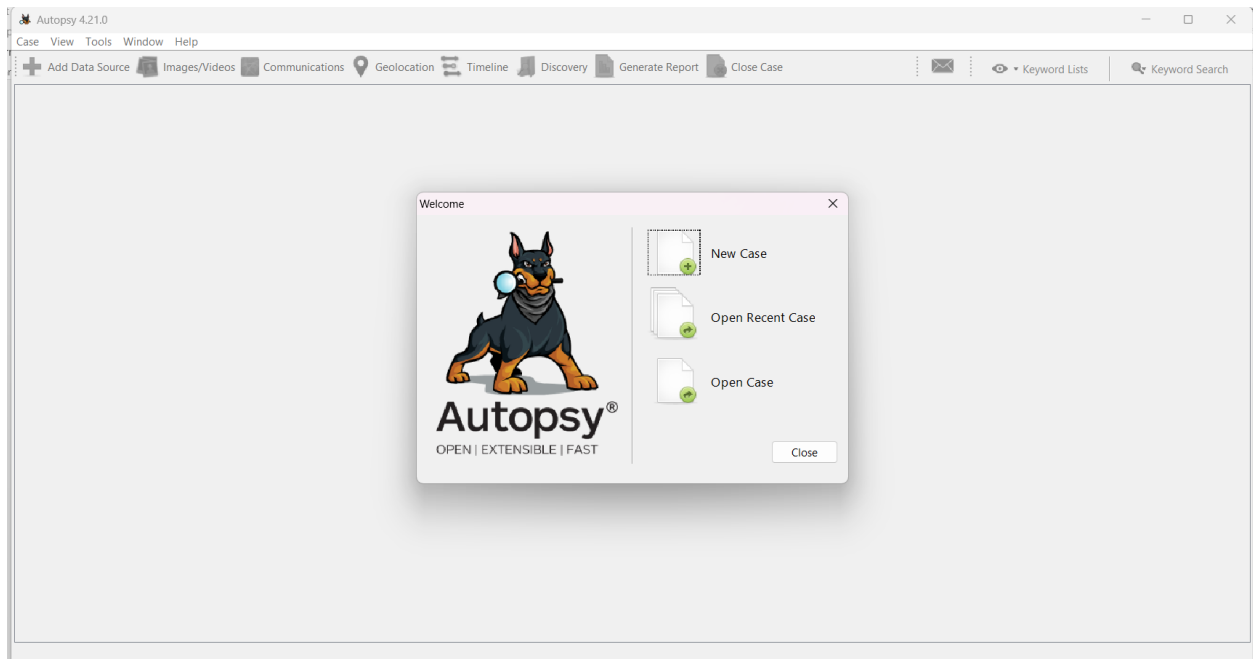
Moinoddeen Quader Al Arabi
Ethical Hacker, Forensic
Investigator, and VAPT Expert
Cyber Security Consultant in
Dhaka Division, Bangladesh.

Submitted By

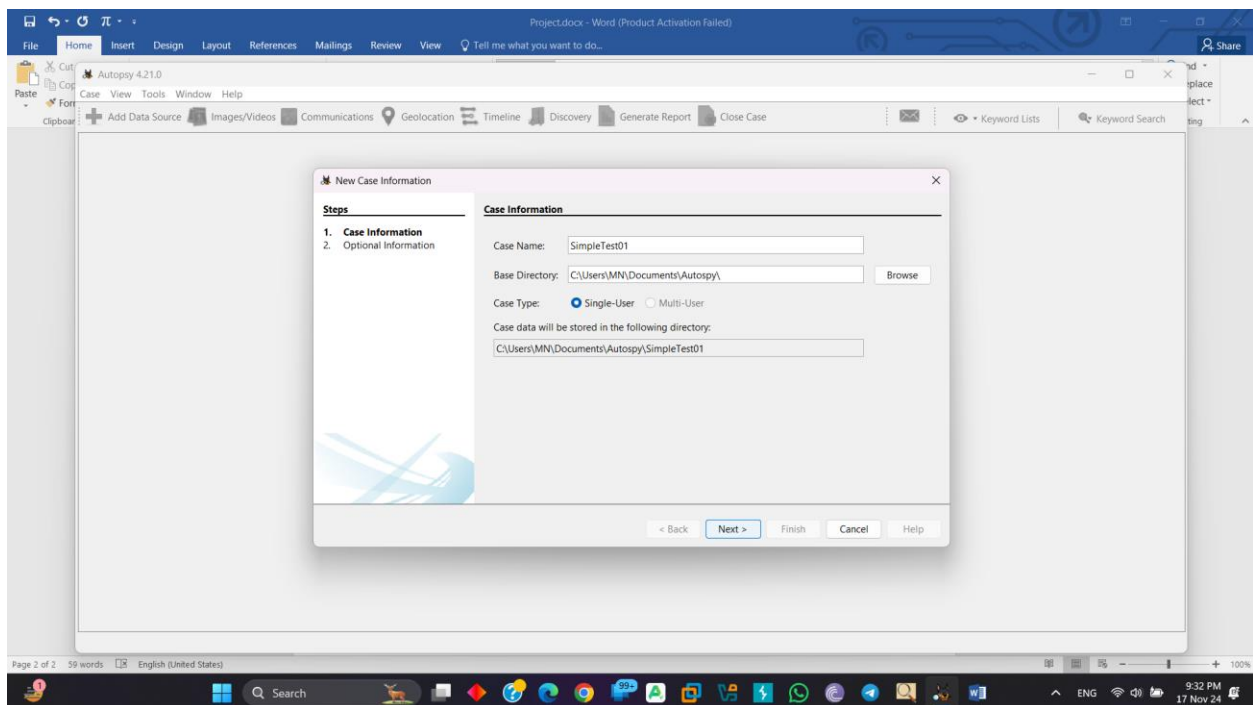
Md. Shakil Hossain
ID: 2111258

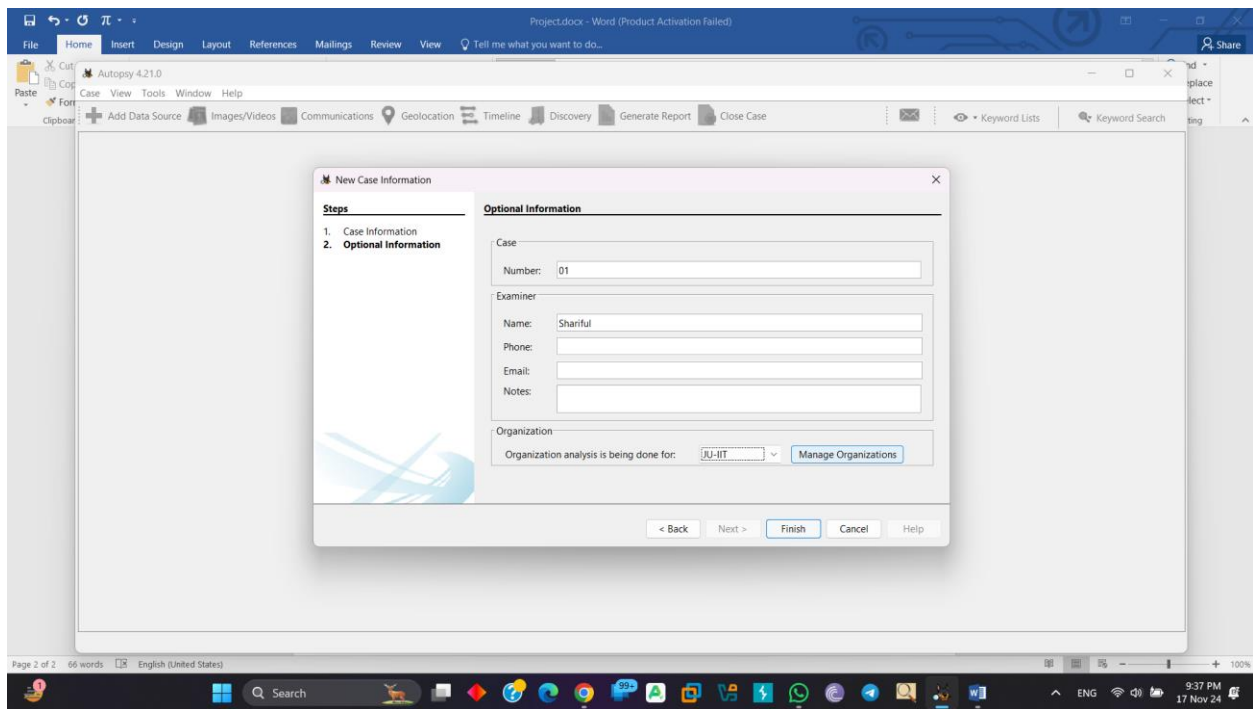
Disk Forensics with Autopsy

Create New Case:

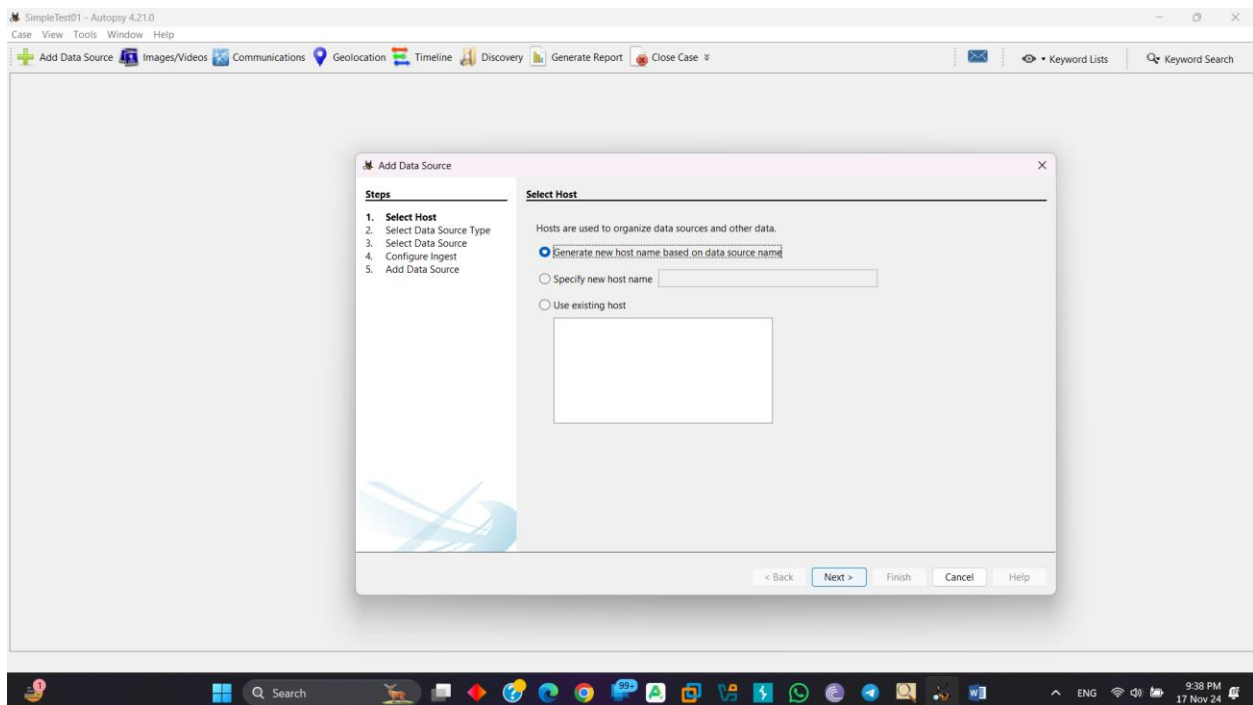


Set a Case Name and Base directory:

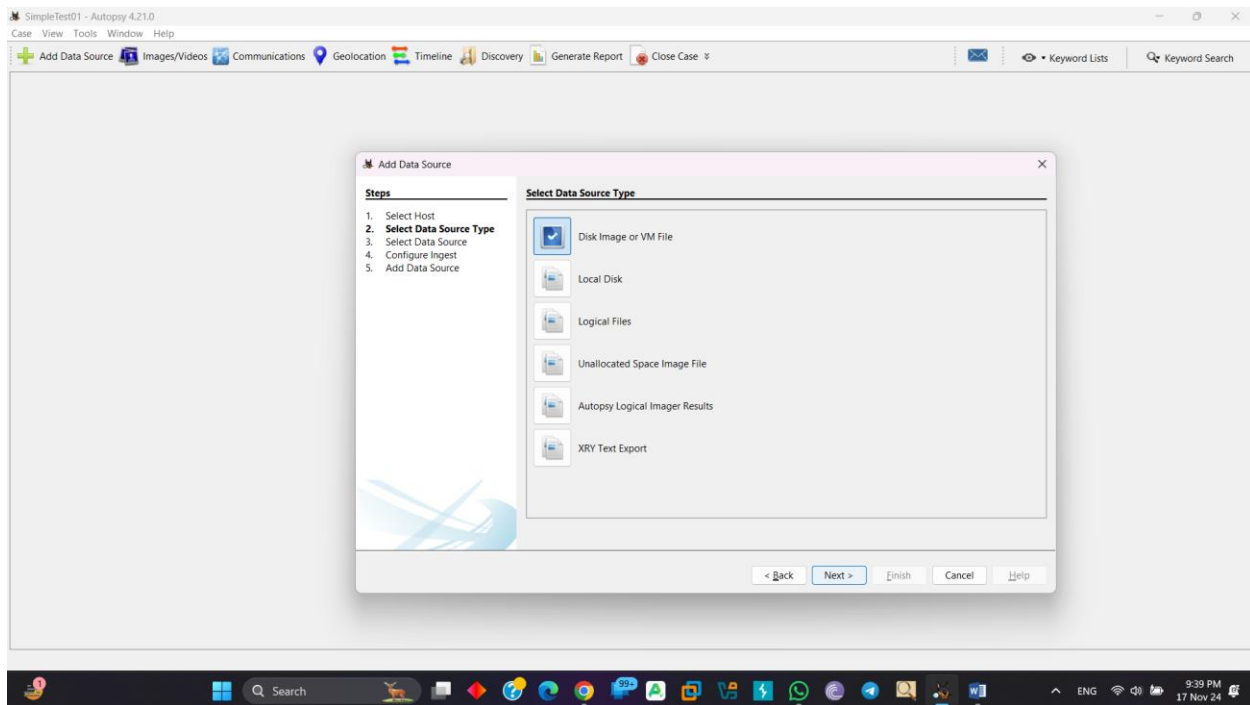




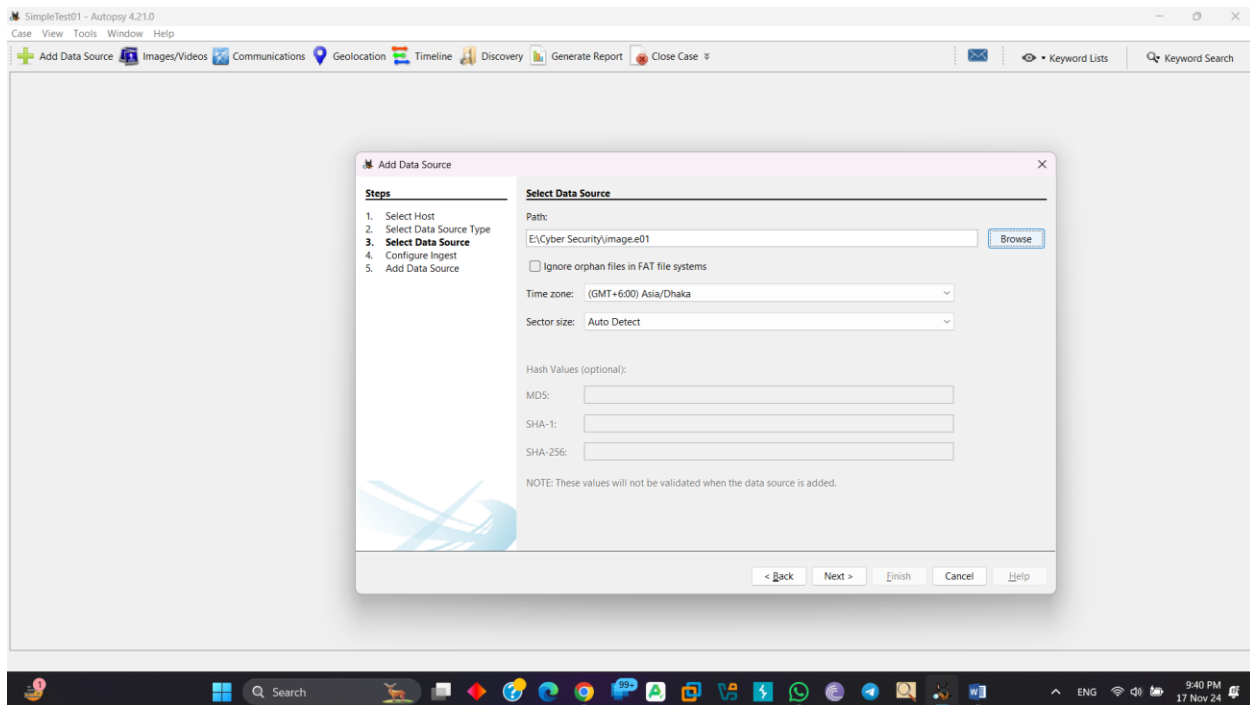
Select a Host (Ex: Generate New Host name based on data source name)



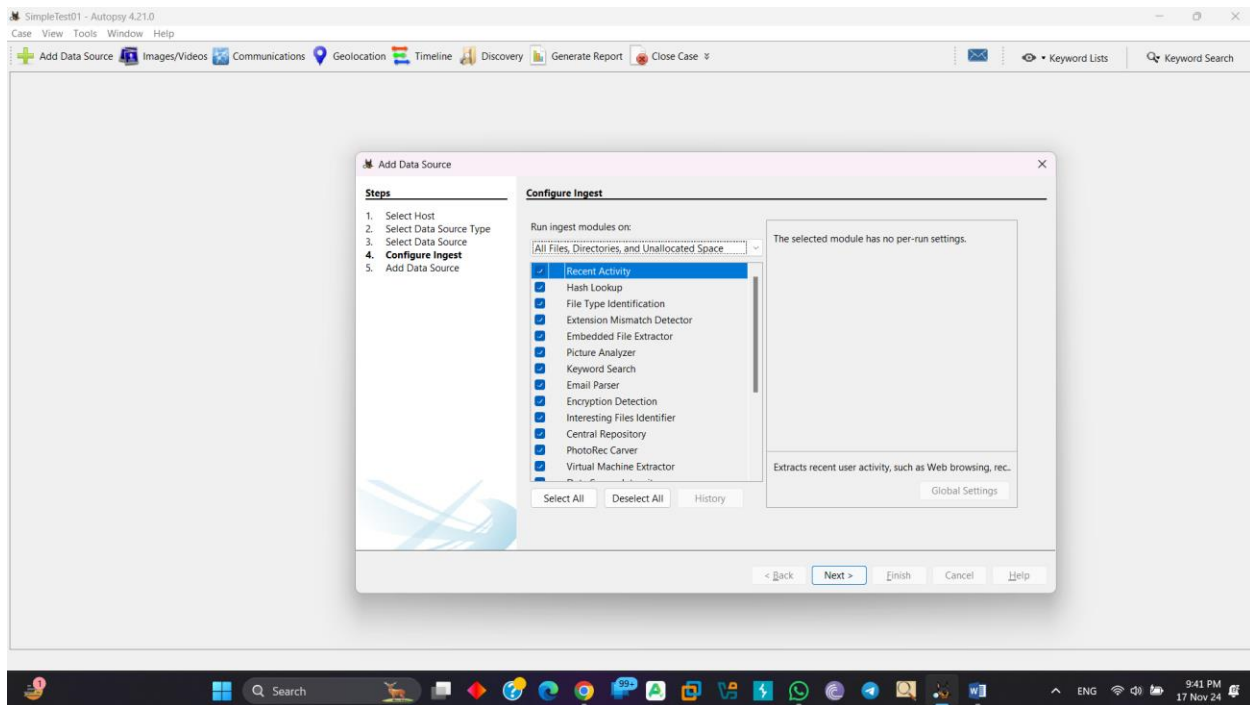
Select any one type of disk:



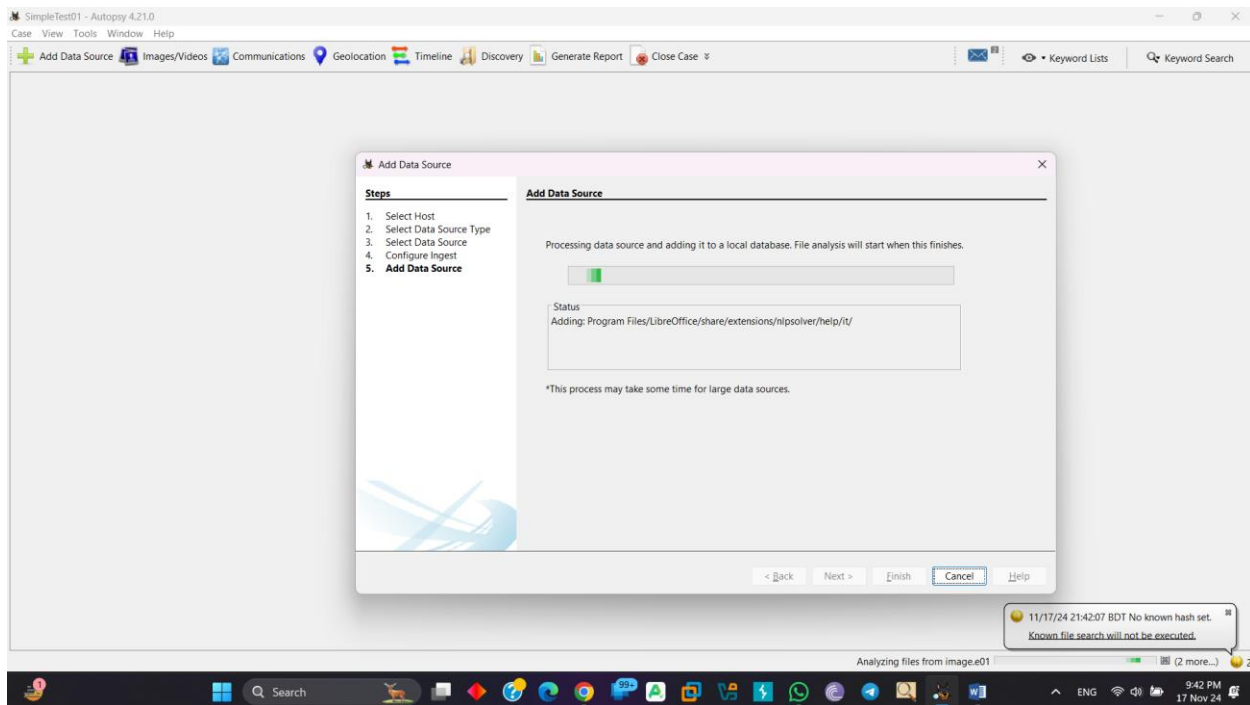
Browse the image:



Select needed item and enter next:



Here add data source:



Here is 5090 Delete file:

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the 'File System' view, highlighting the 'Deleted Files' section. The main pane shows a table of 5090 results, which are files that have been deleted. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Me). The results are sorted by Name, and the first few entries are 'Application form.exe', 'Web Data', 'Web Data-journal', and several '.idb' files. The bottom status bar indicates 'Analyzing files from image.e01' with a progress of 3%.

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
._0008.idb				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
._0008.idb				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
._0011.idb				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
._0012.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
Gonella Dmilia.ion				2019-08-18 11:18:33 BDT	0000-00-00 00:00:00	2022-04-22 00:00:00 BDT	2022-04-22 17:32:53 BDT	181073	Unallocated	Unalloca

Here are two-email message:

The screenshot shows the Autopsy 4.21.0 interface with the 'E-Mail Messages' view selected. The left sidebar shows the 'Data Sources' view, highlighting the 'E-Mail Messages' section. The main pane shows a table of 2 results, which are email messages. The table includes columns for Source Name, S, C, O, E-Mail From, E-Mail To, Subject, Message ID, Path, and Thread ID. The results are sorted by Source Name, and the first two entries are 'INBOX' messages from 'hello@yandex-team.ru' and 'woodwifred@yandex.com' to 'amanda.e-bank@yandex.ru'. The bottom status bar indicates 'Analyzing files from image.e01' with a progress of 4%.

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				woodwifred@yandex.com	amanda.e-bank@yandex.com	Двойное списание со счета	Not available	/imap.yandex.com/INBOX	80d4fa69

Result: 3 of 6 Result

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

Headers Text HTML RTF Attachments (0) Accounts

Download Images

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

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the file tree with 'Data Sources' expanded, showing 'image.e01_1 Host' and 'image.e01'. The 'Data Artifacts' section is expanded, showing 'E-Mail Messages (2)'. The main pane displays the 'Listing' view for 'E-Mail Messages', showing a table with 2 results. The table has columns: Source Name, S, C, O, E-Mail From, E-Mail To, Subject, Message ID, Path, and Thread ID. The first result is from 'hello@yandex-team.ru' to 'amanda.e-bank@yandex.ru' with the subject 'Как убедиться, что письмо доставлено'. The second result is from 'woodwifred@yandex.com' to 'amanda.e-bank@yandex.com' with the subject 'Двойное списание со счета'. Below the table, the 'Text' view of the selected email is shown, displaying the header and body text in Russian. The body text includes a greeting and a notification about email delivery.

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	e17e3b2
INBOX				woodwifred@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:

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the file tree with 'Data Sources' expanded, showing 'image.e01_1 Host' and 'image.e01'. The 'Data Artifacts' section is expanded, showing 'EXIF Metadata (1)'. The main pane displays the 'Listing' view for 'EXIF Metadata', showing a table with 1 result. The table has columns: Source Name, S, C, O, Source Type, Score, Conclusion, Configuration, Justification, Date Created, and File Path. The result is for 'WelcomeScan.jpg' with a score of 0 and a conclusion of 'Not Notable'. Below the table, the 'File Metadata' view is shown, displaying a thumbnail of the image and its EXIF data.

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

0° 52% Reset

Tags Menu

There are 12 suspicious item:

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows a tree view of file types, with 'Suspicious Items (12)' highlighted under the 'Reports' section. The main window is titled 'Listing Suspicious Items' and shows a table of 12 items. The table has columns for Source, Type, and Path. The item 'C598B21E-C190-11E9-A908-0800271088D0.dat' is selected, and its details are shown in the 'Analysis Results' tab. The details include the item name, aggregate score ('Likely Notable'), and an analysis result indicating an 'Extension Mismatch Detected'.

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(C598B21D-C190-11E9-A908-0800271088D0).dat	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/RecoveryStore(C598B21D-C190-11E9-A908-0800271088D0).dat
C598B21E-C190-11E9-A908-0800271088D0.dat	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/C598B21E-C190-11E9-A908-0800271088D0.dat
C598B220-C190-11E9-A908-0800271088D0.dat	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Internet Explorer/Recovery/High/Last Active/C598B220-C190-11E9-A908-0800271088D0.dat
favicon[1].ico	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/4MNQZMD8/favicon[1].ico
favicon[2].ico	File	/img_image.e01/Users/IEUser/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/4MNQZMD8/favicon[2].ico
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

Analysis Result 1

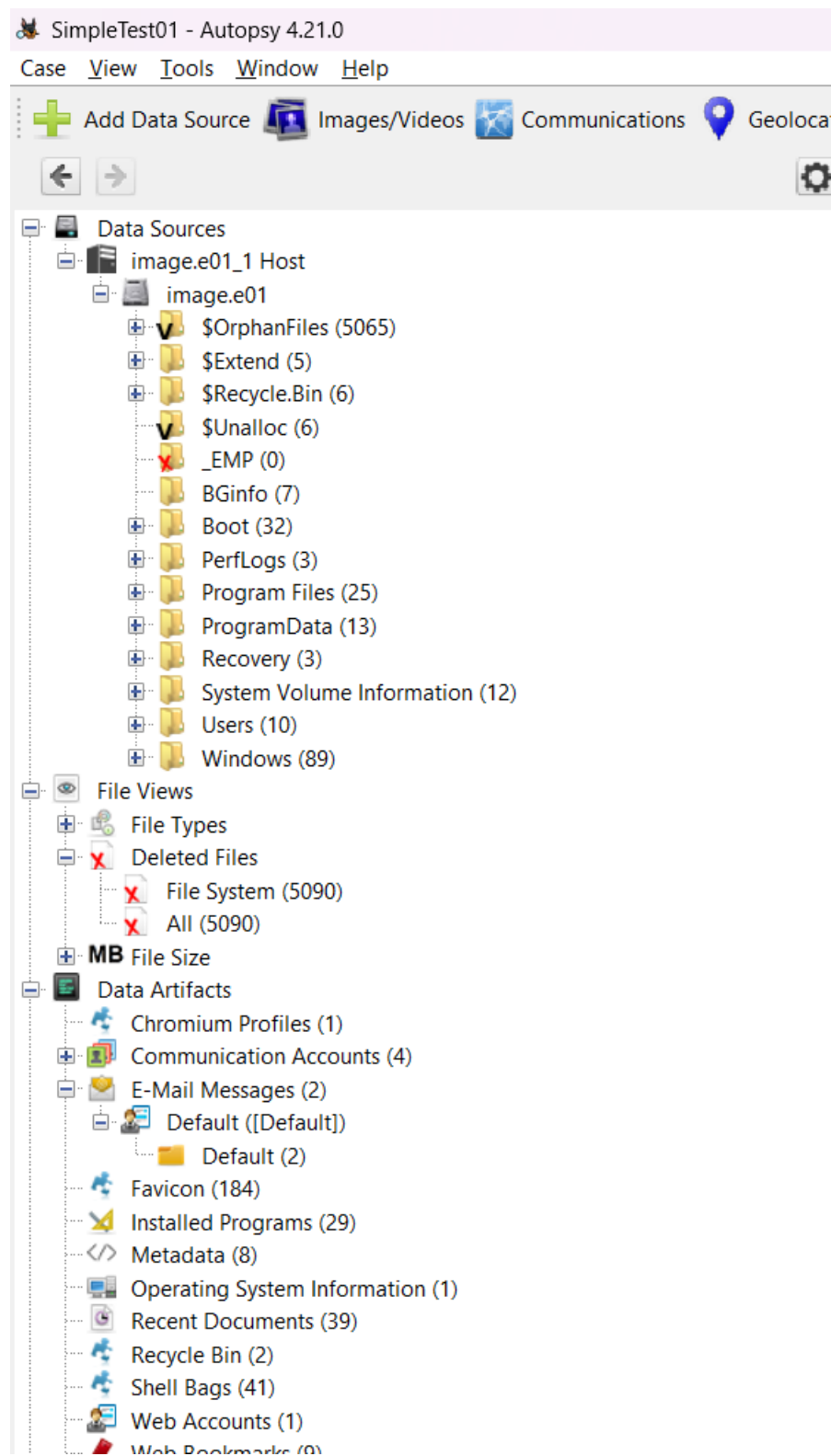
Score: Likely Notable

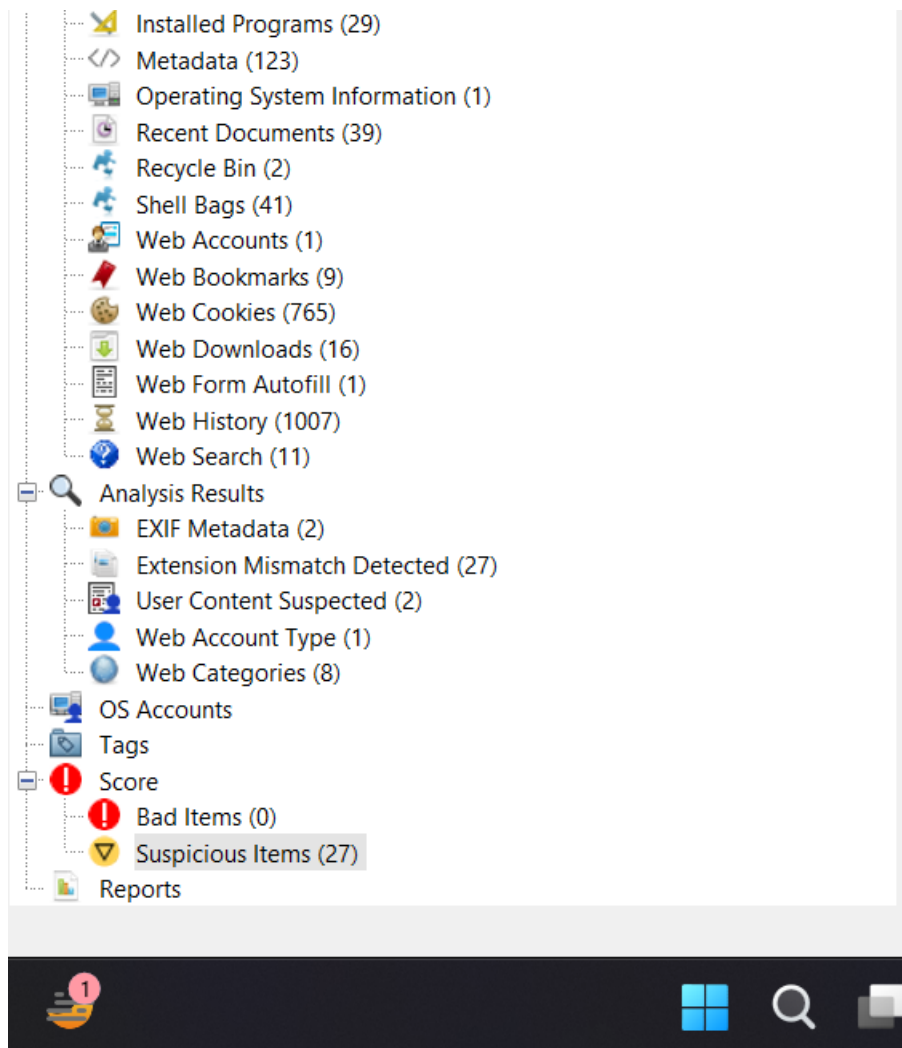
Type: Extension Mismatch Detected

Configuration:

Conclusion:

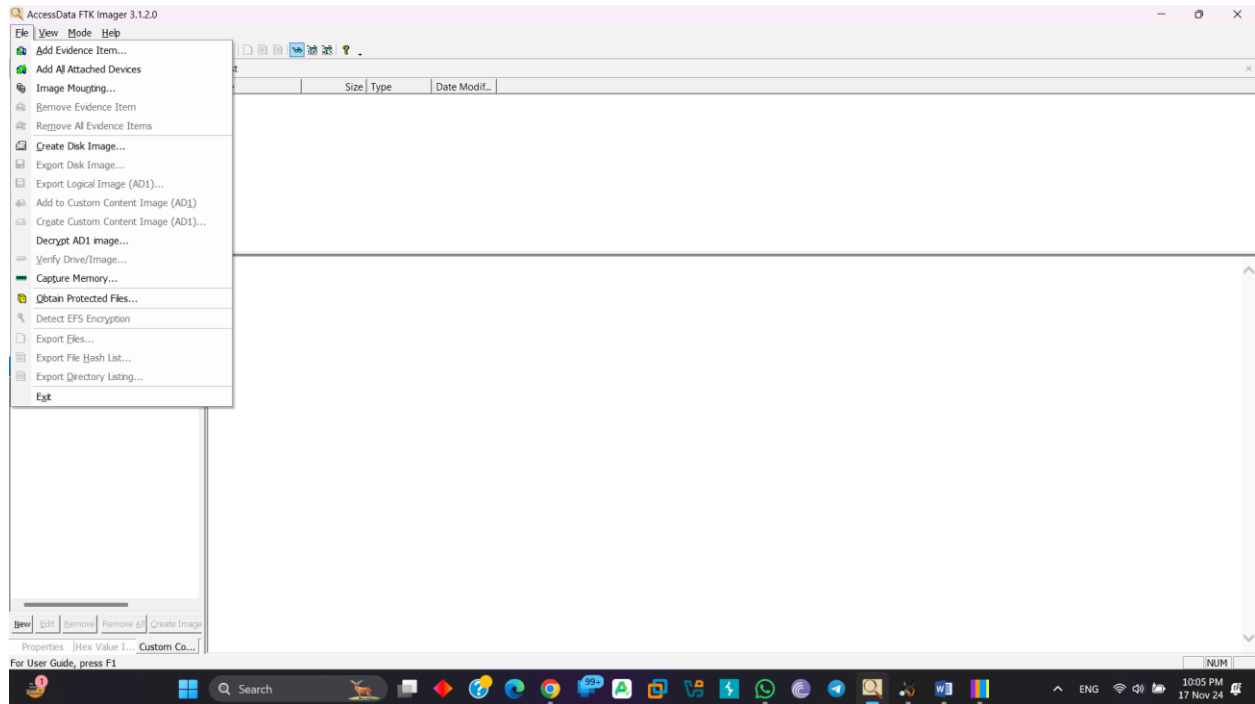
In addition, more other report item:



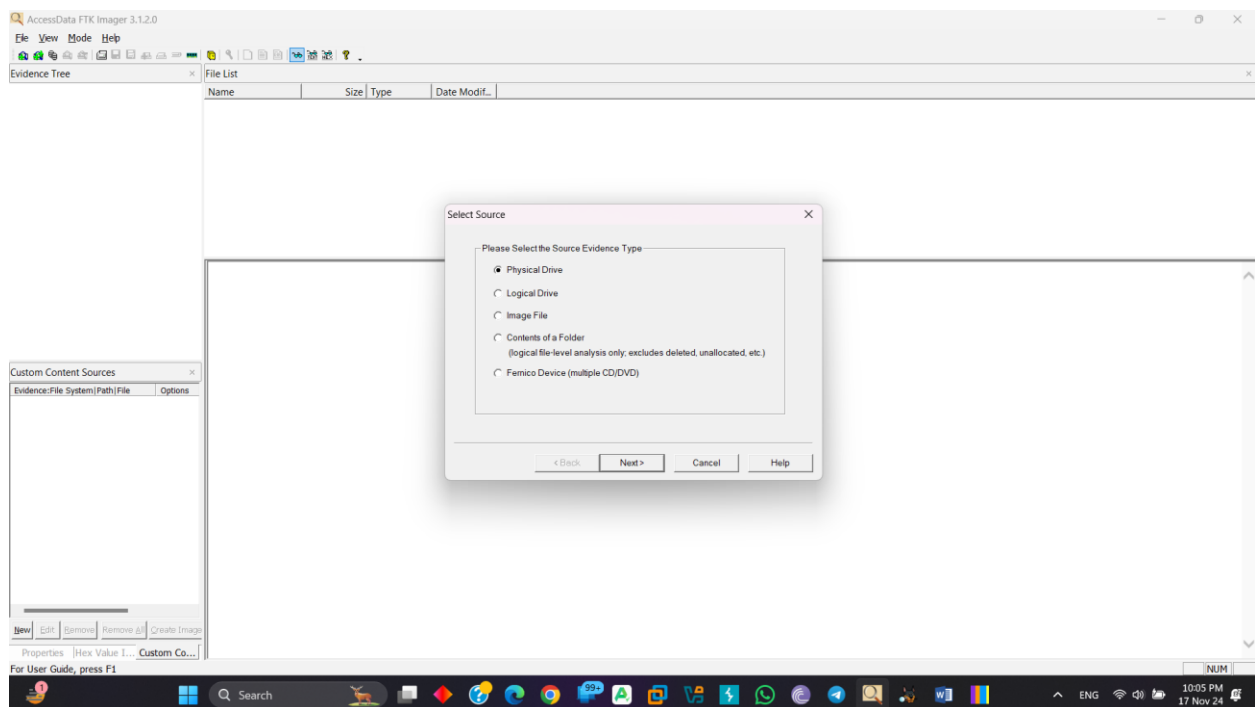


Disk Forensics with FTK Imager

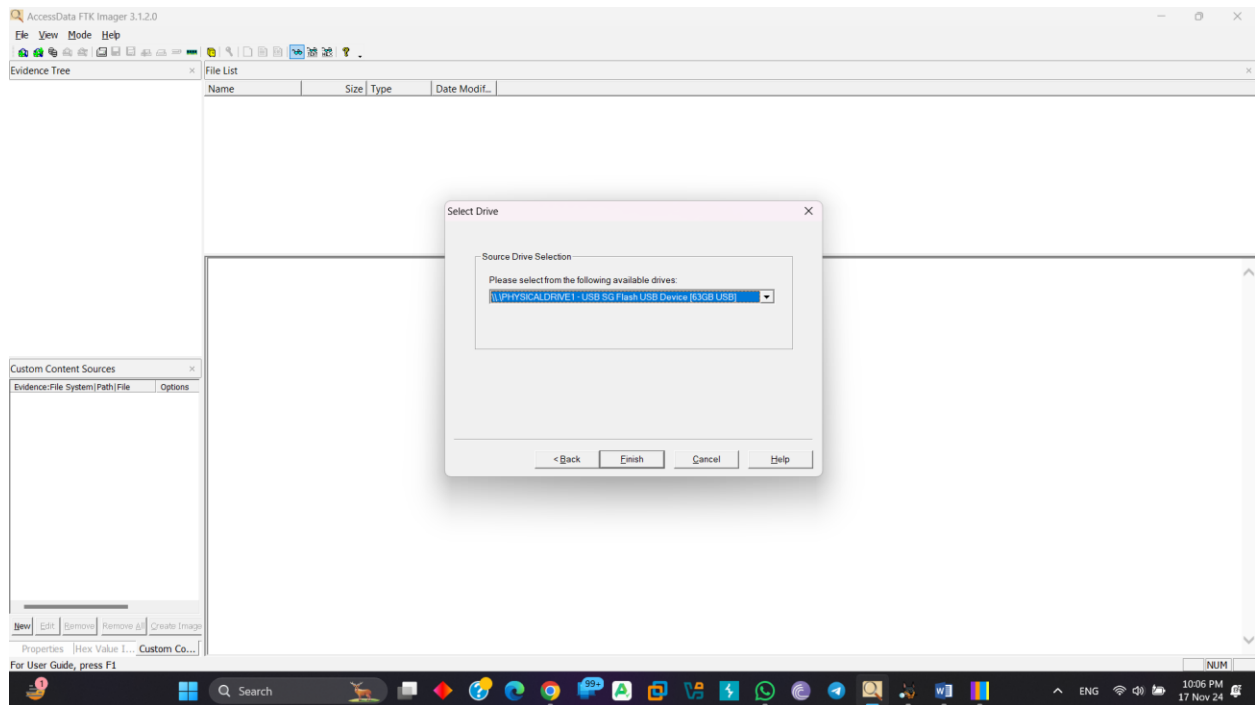
In the beginning go to File→Create new disk:



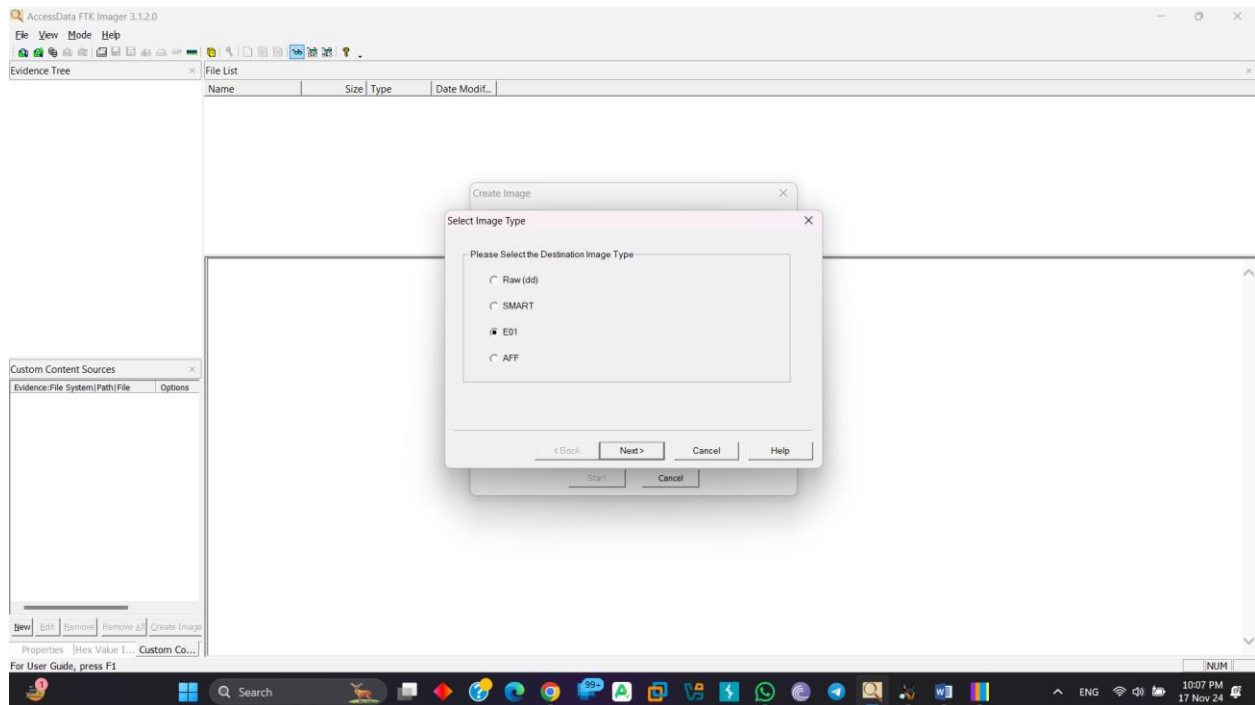
Select any one type:



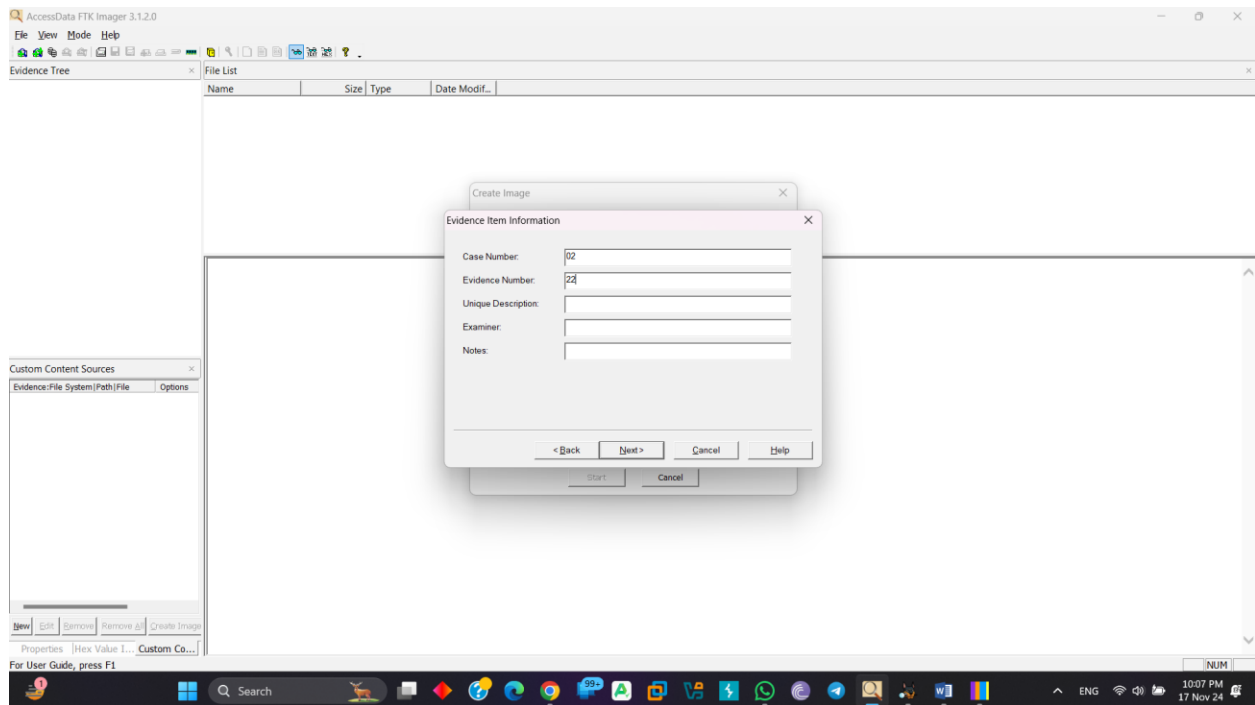
Select the drive:



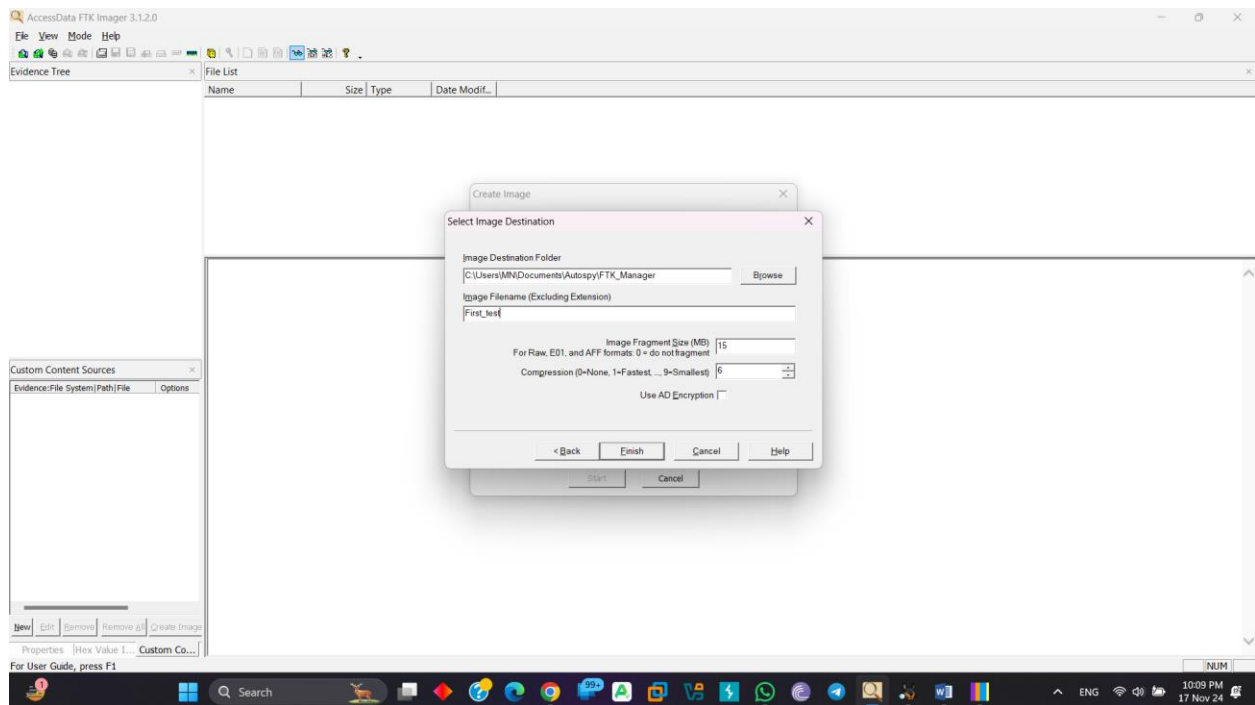
Add image type (any one from them):



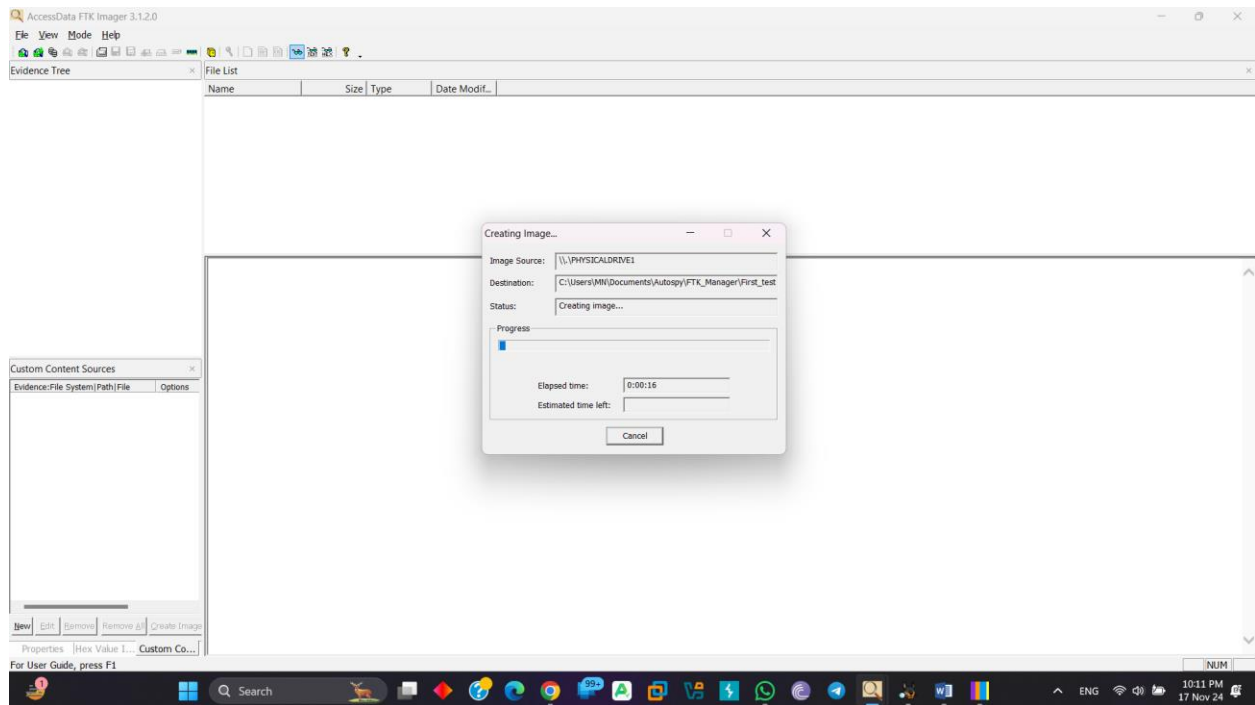
Set Evidence Item Information:



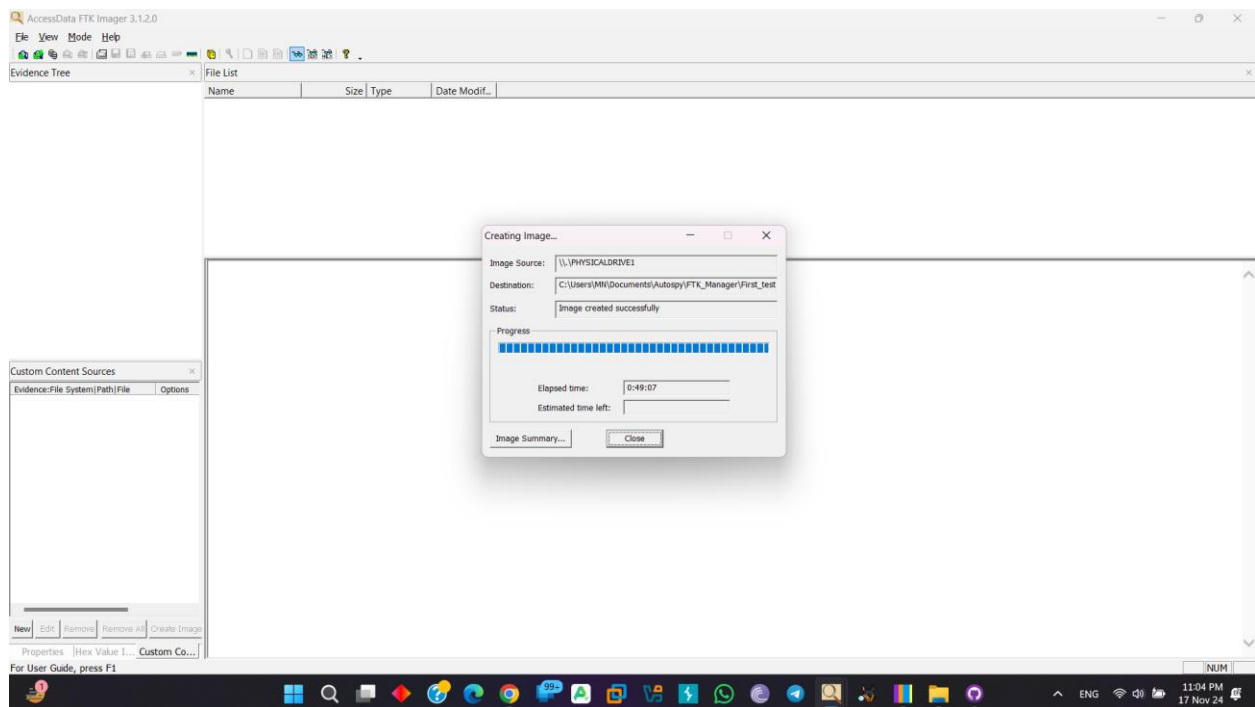
Select Destination folder and set file name and can resize Image Fragment size:



It's take huge number of time for Processing depends on processing disk size:



It's take about 49 minutes to execute:



The End