INSTITUTE OF INFORMATION TECHNOLOGY
JAHANGIRNAGAR UNIVERSITY

Number of Project	**: 02**
Name of Project	**: Disk Forensics with Autopsy and FTK Imager**
Course Tittle	**: 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.

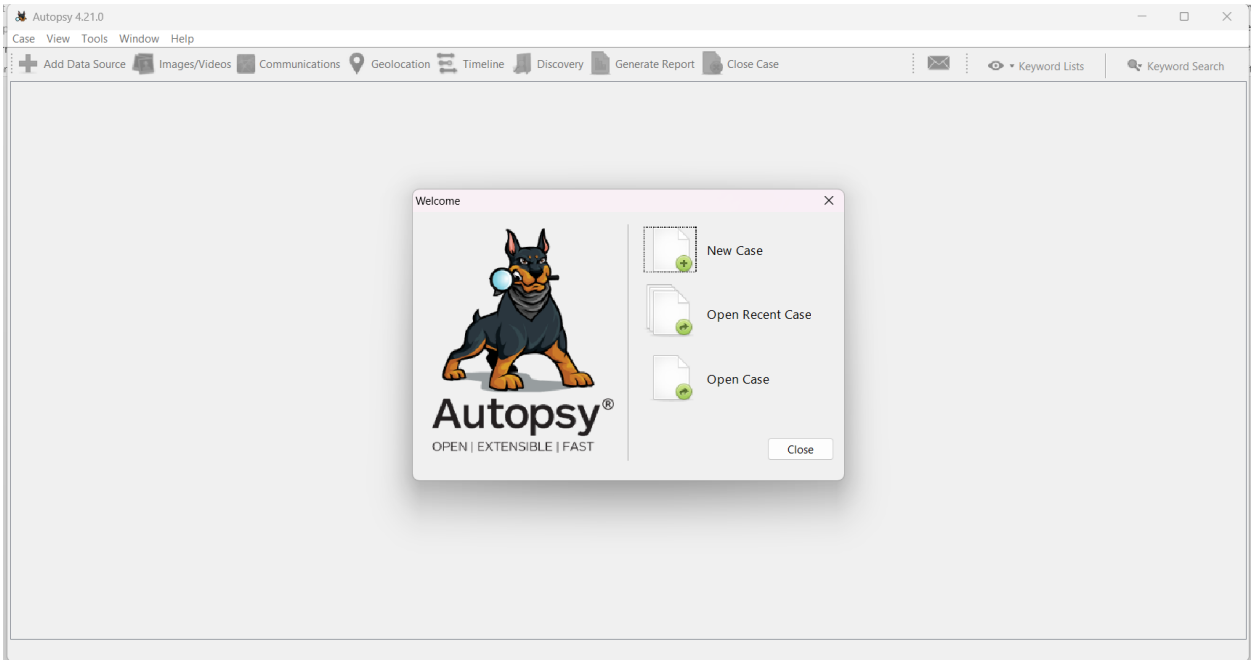
Submitted By

Md. Shakil Hossain

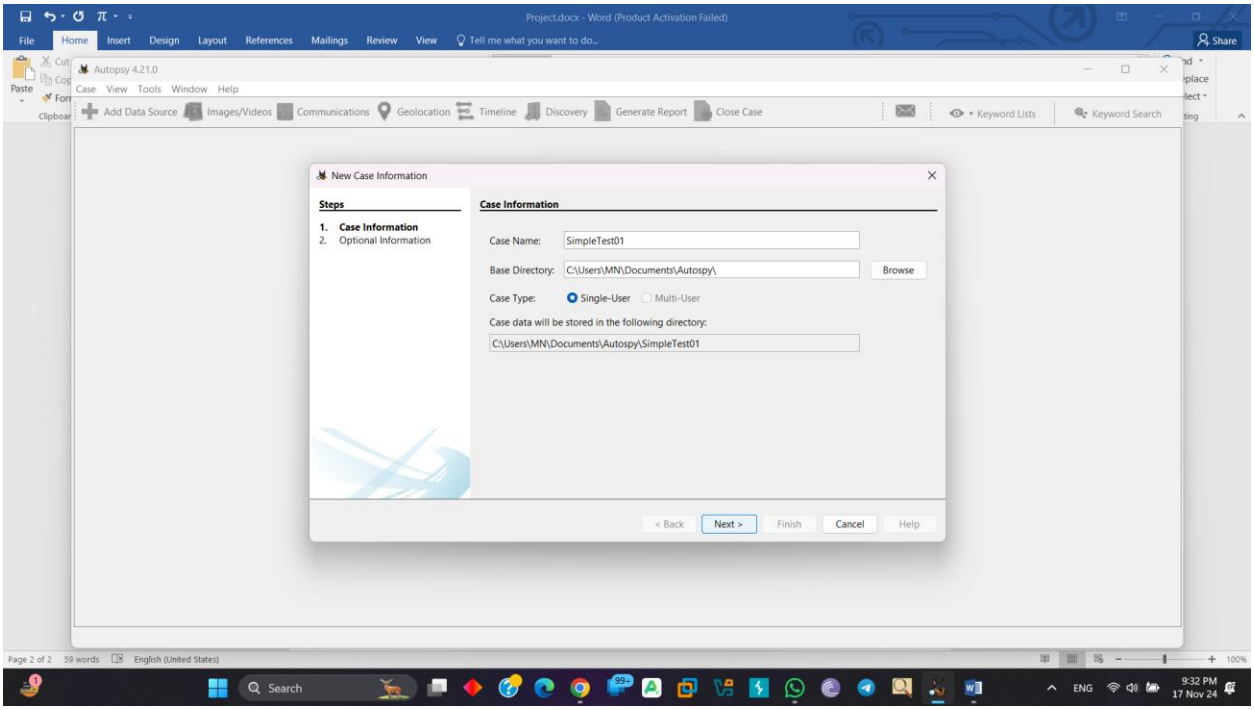
ID: 2111258

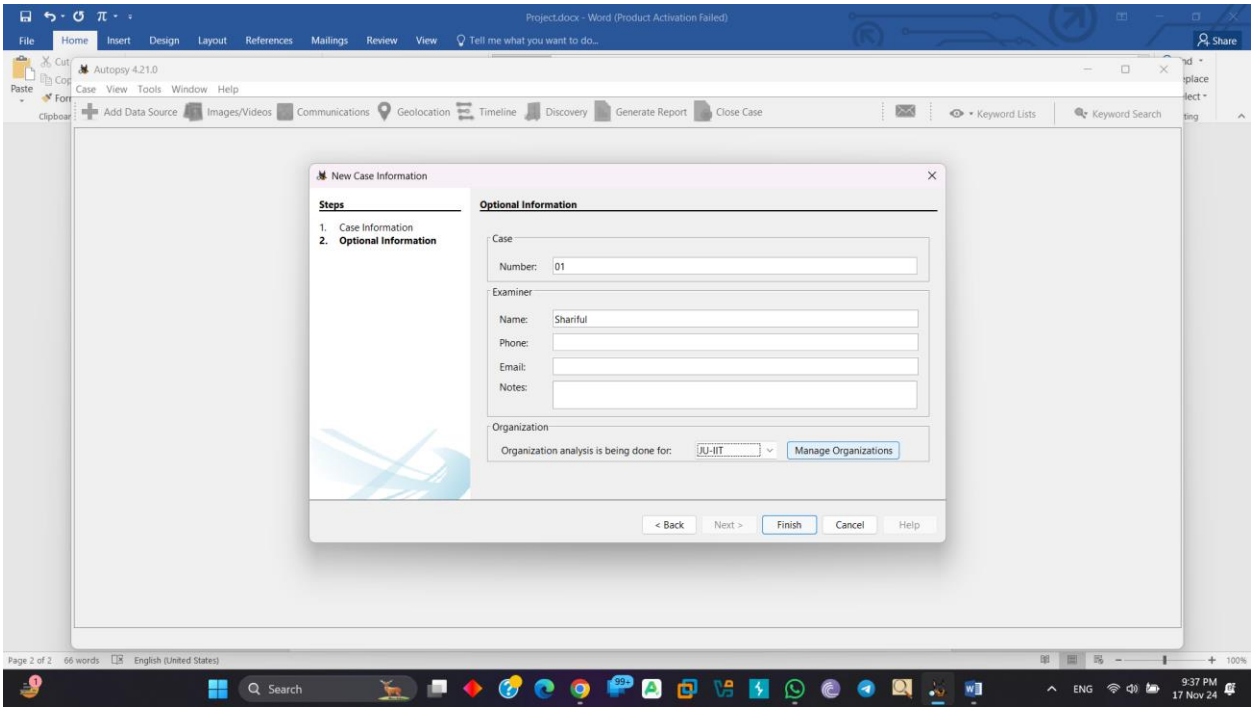
Disk Forensics with Autopsy

Create New Case:

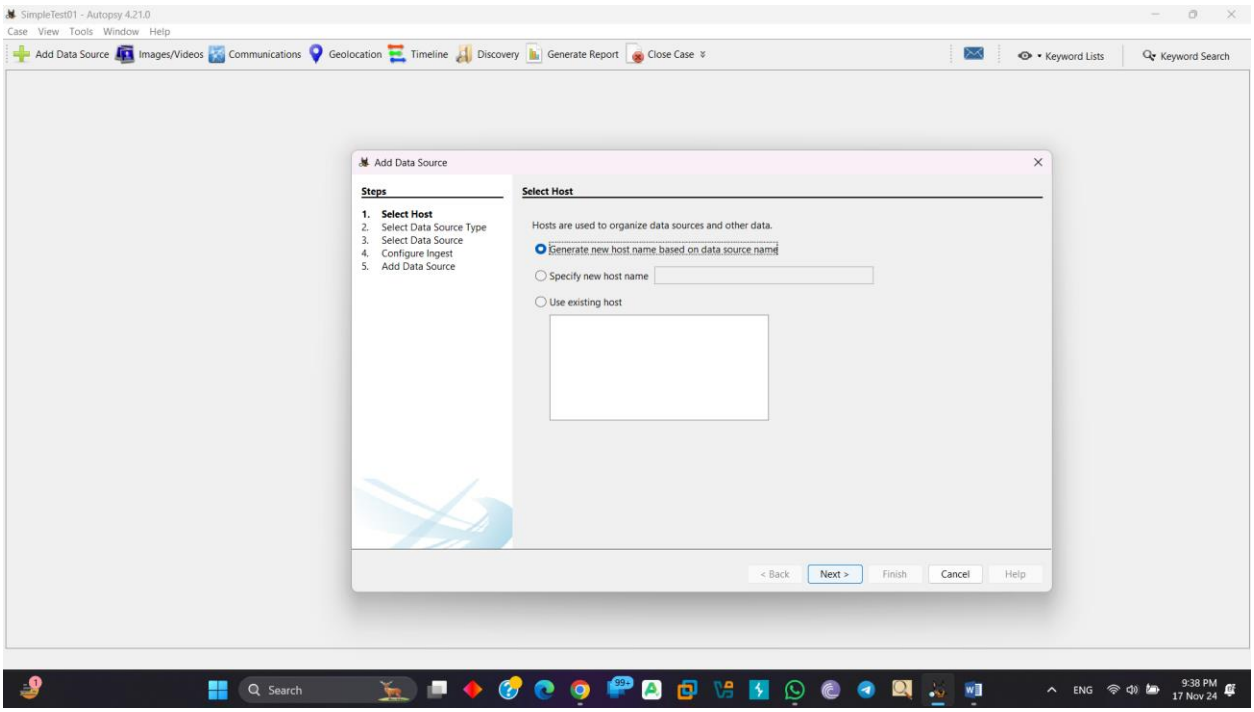


Set a Case Name and Base directory:

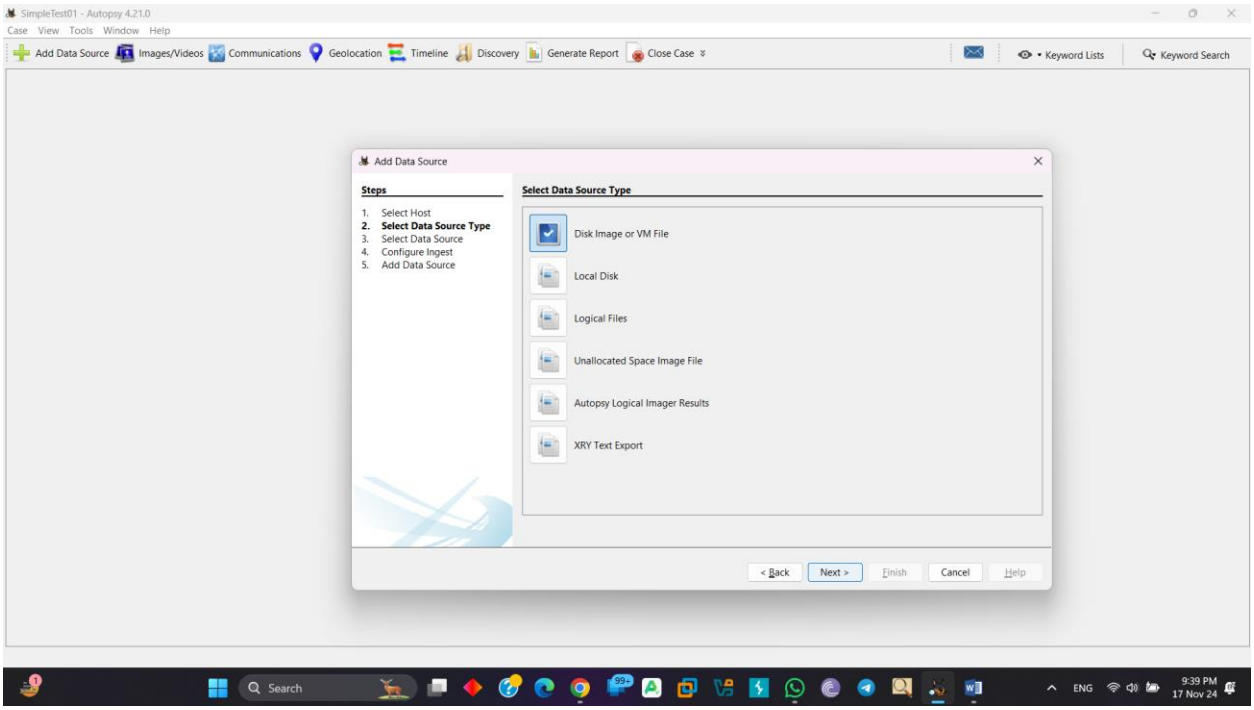




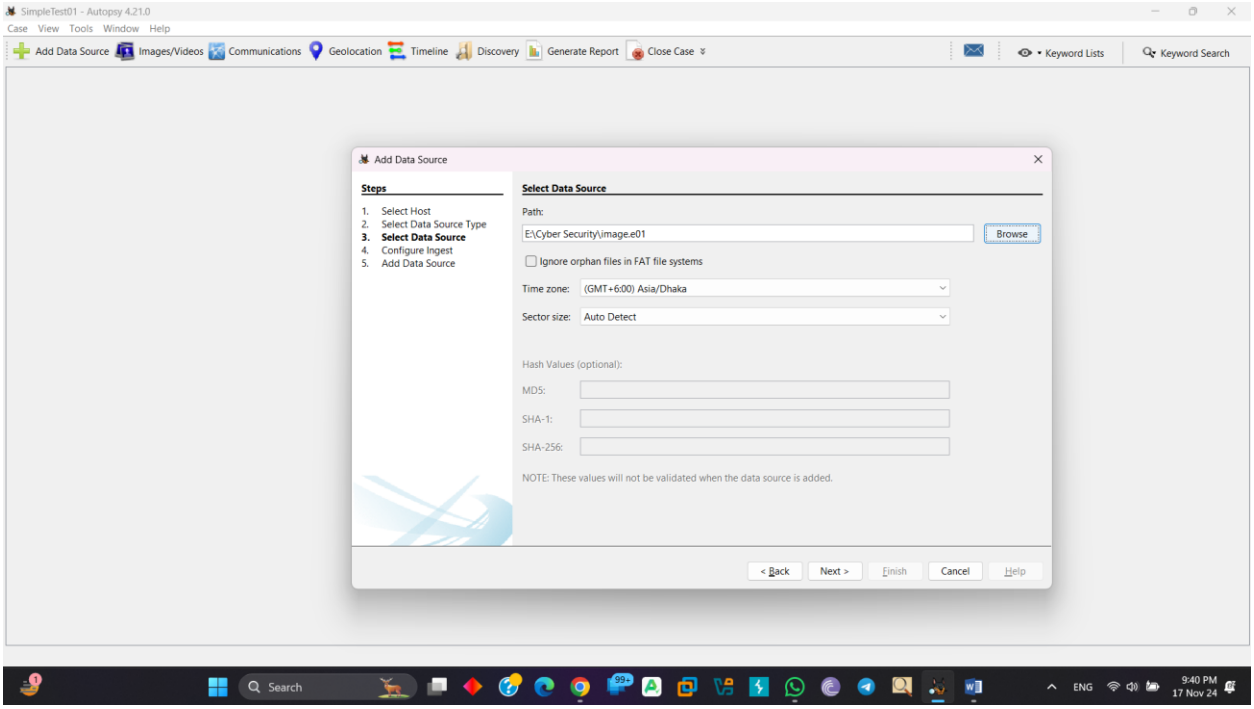
Select a Host (Ex: Generate New Host name based on data source name)



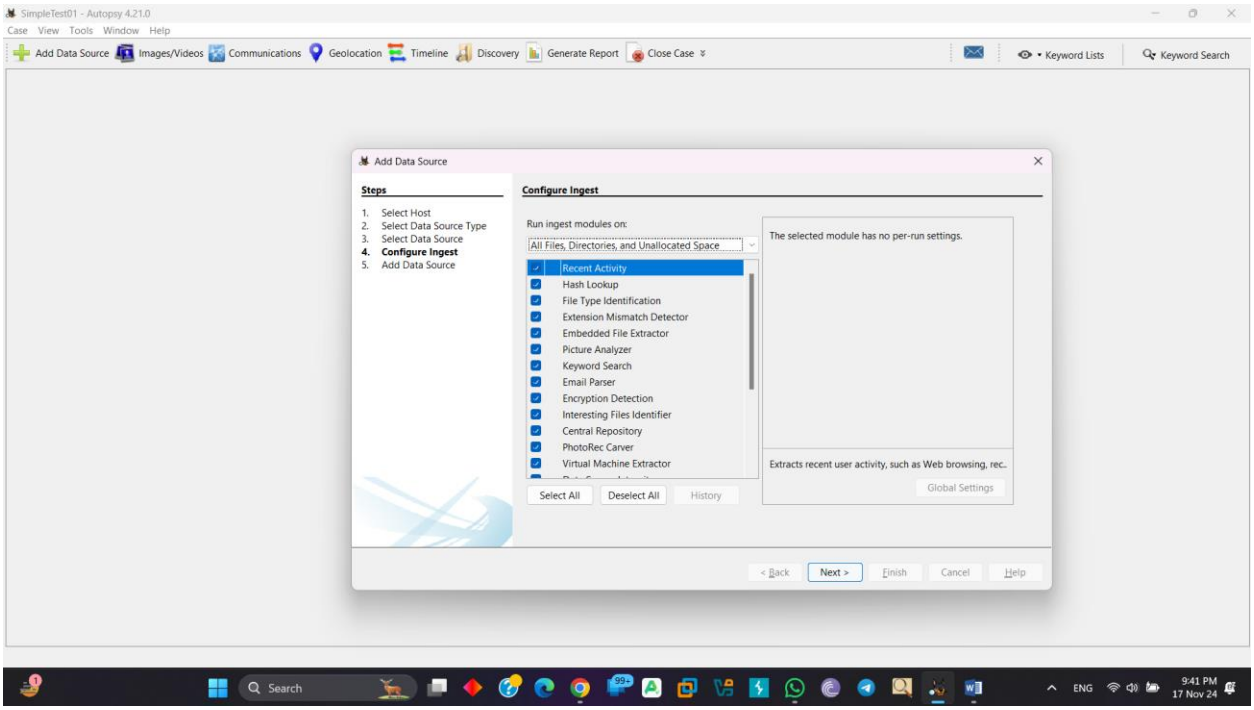
Select any one type of disk:



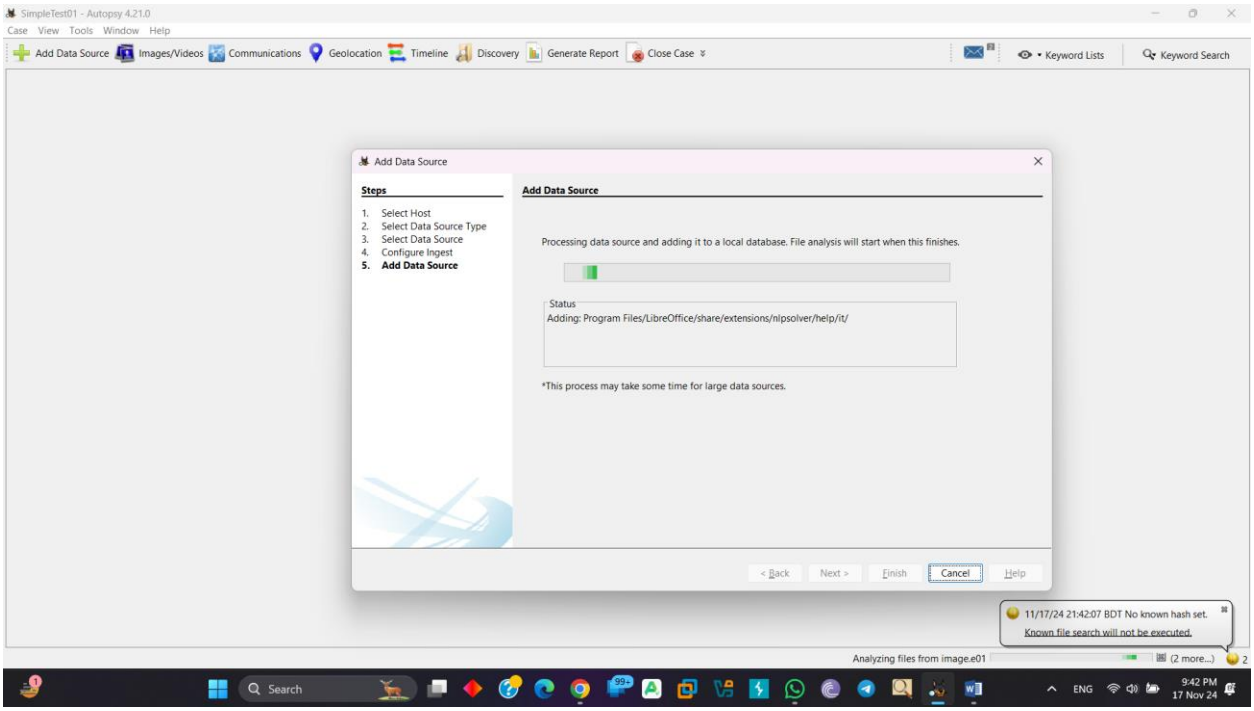
Browse the image:



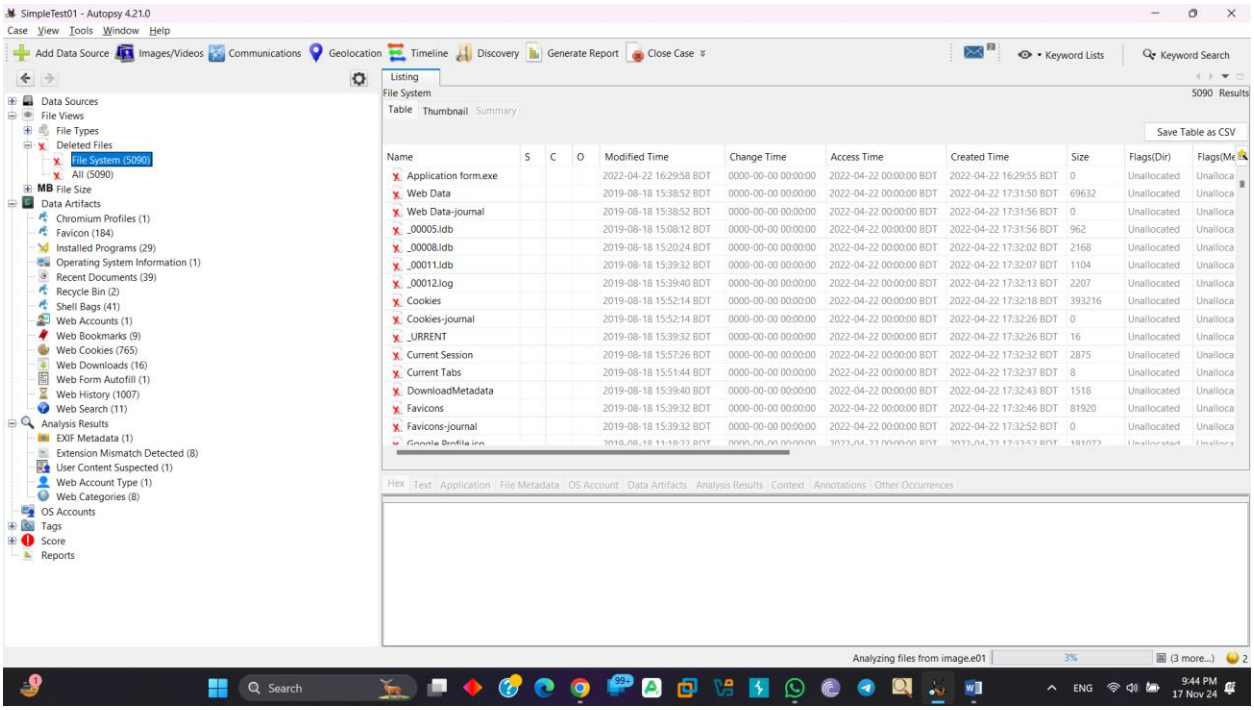
Select needed item and enter next:



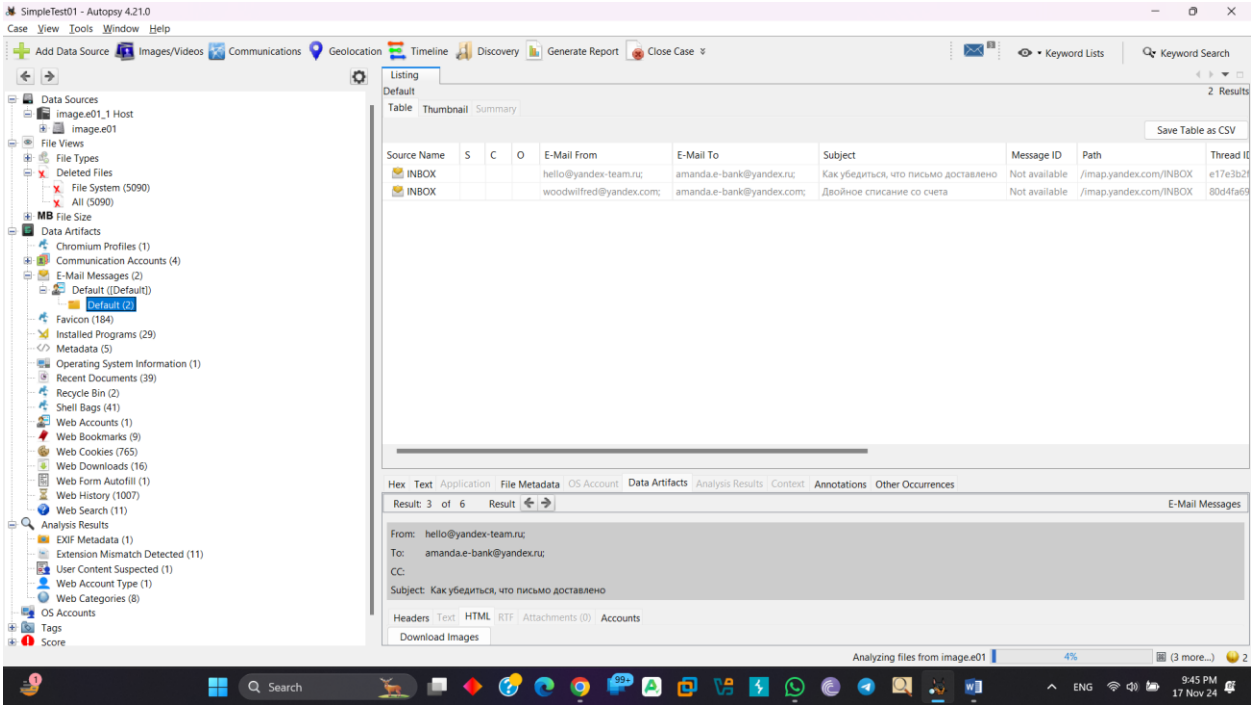
Here add data source:



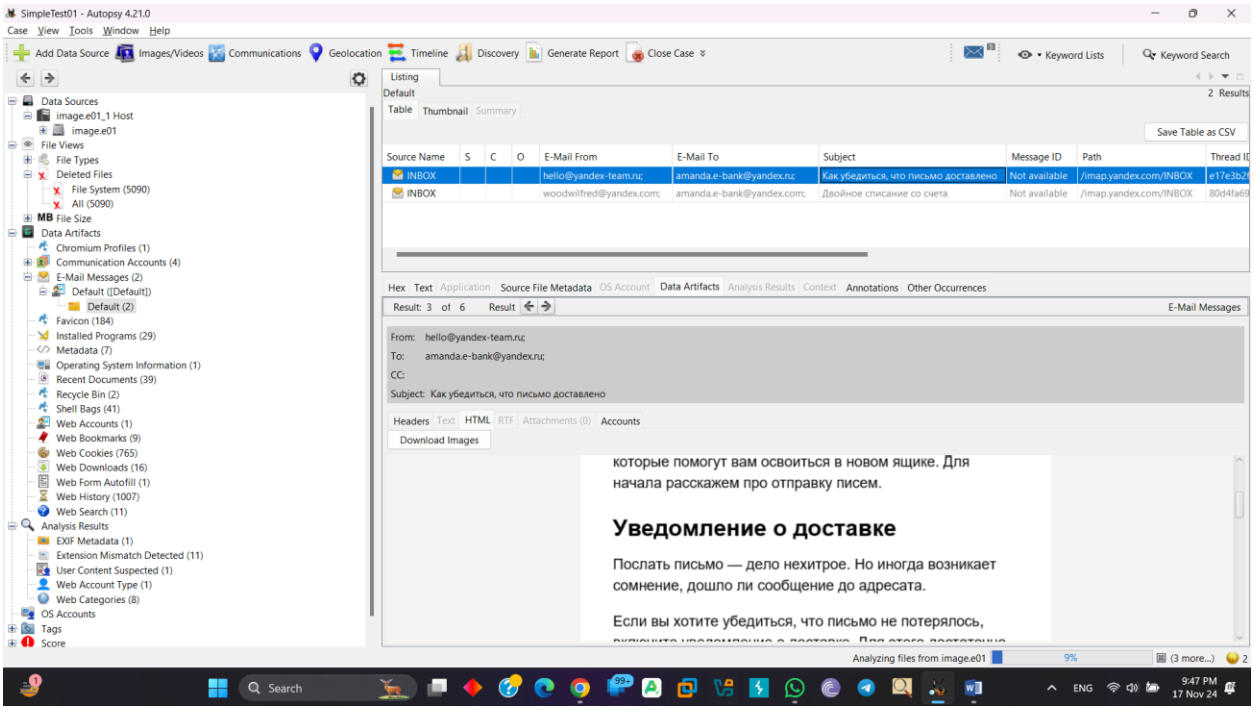
Here is 5090 Delete file:



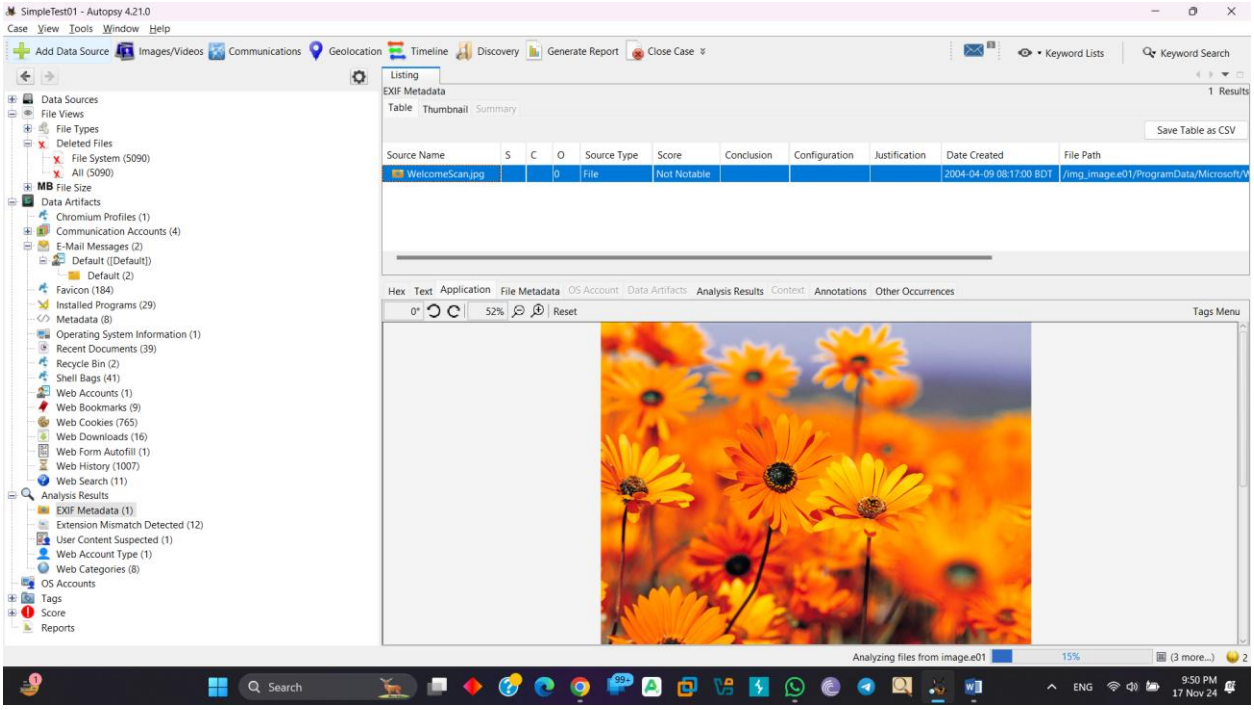
Here are two-email message:



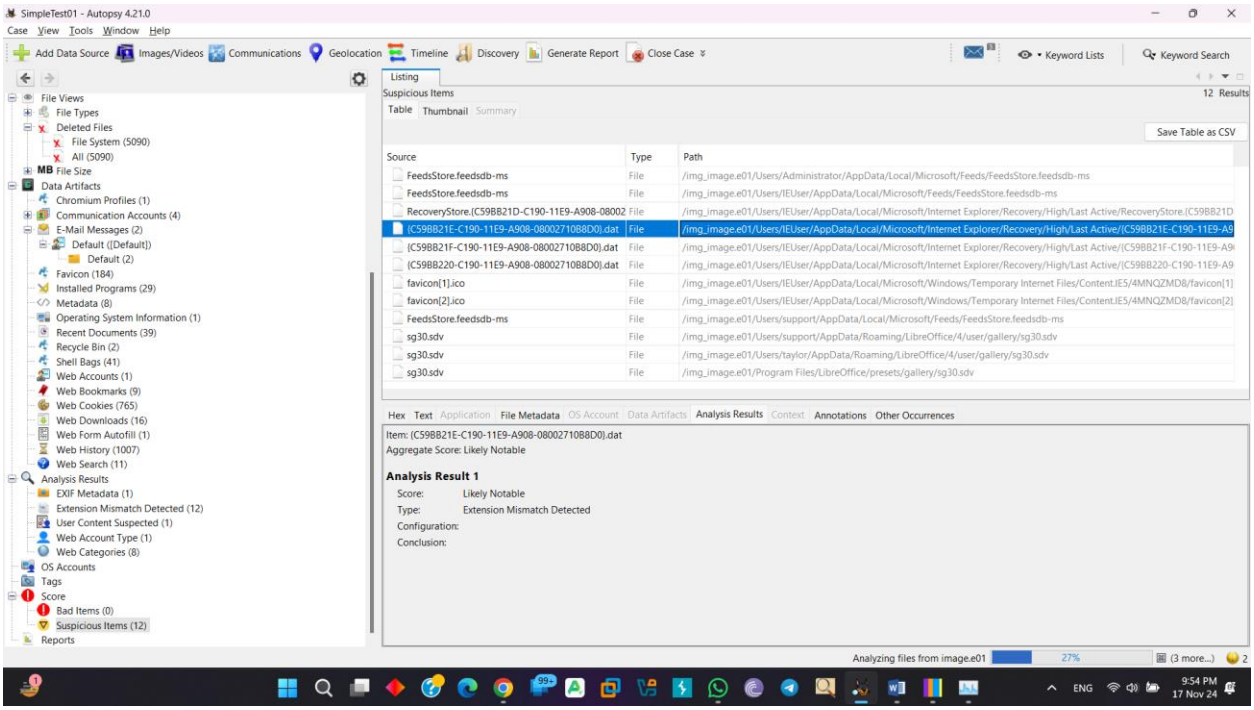
Here is show email from/email to and text of email:



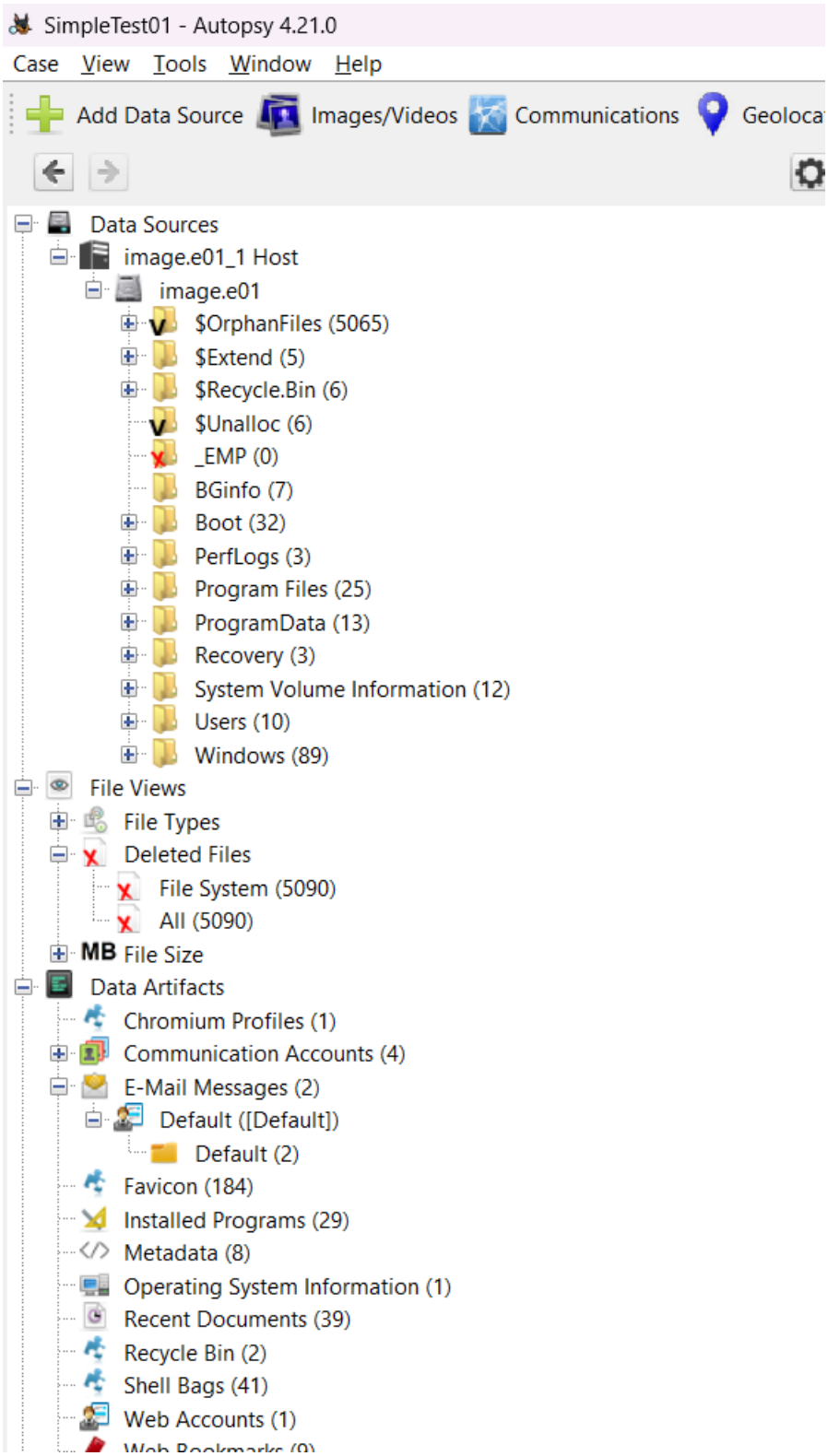
Here is an EXIF Metadata:

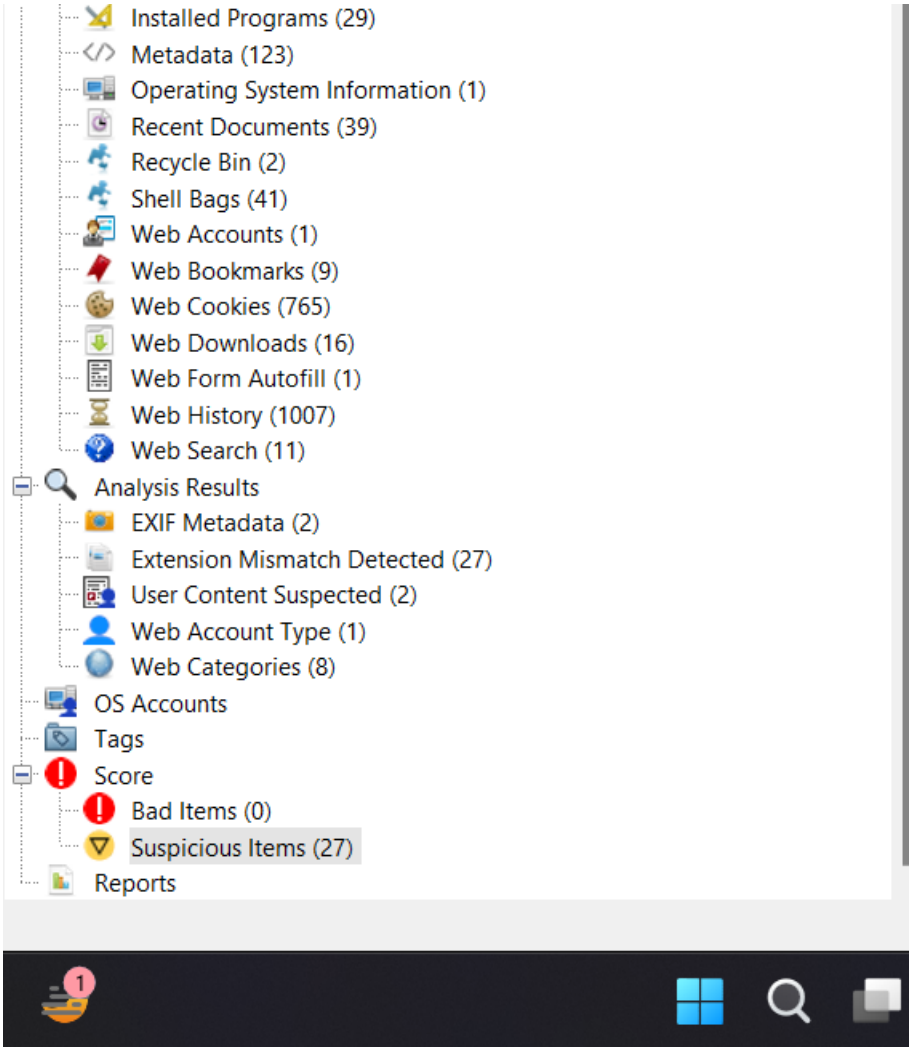


There are 12 suspicious item:



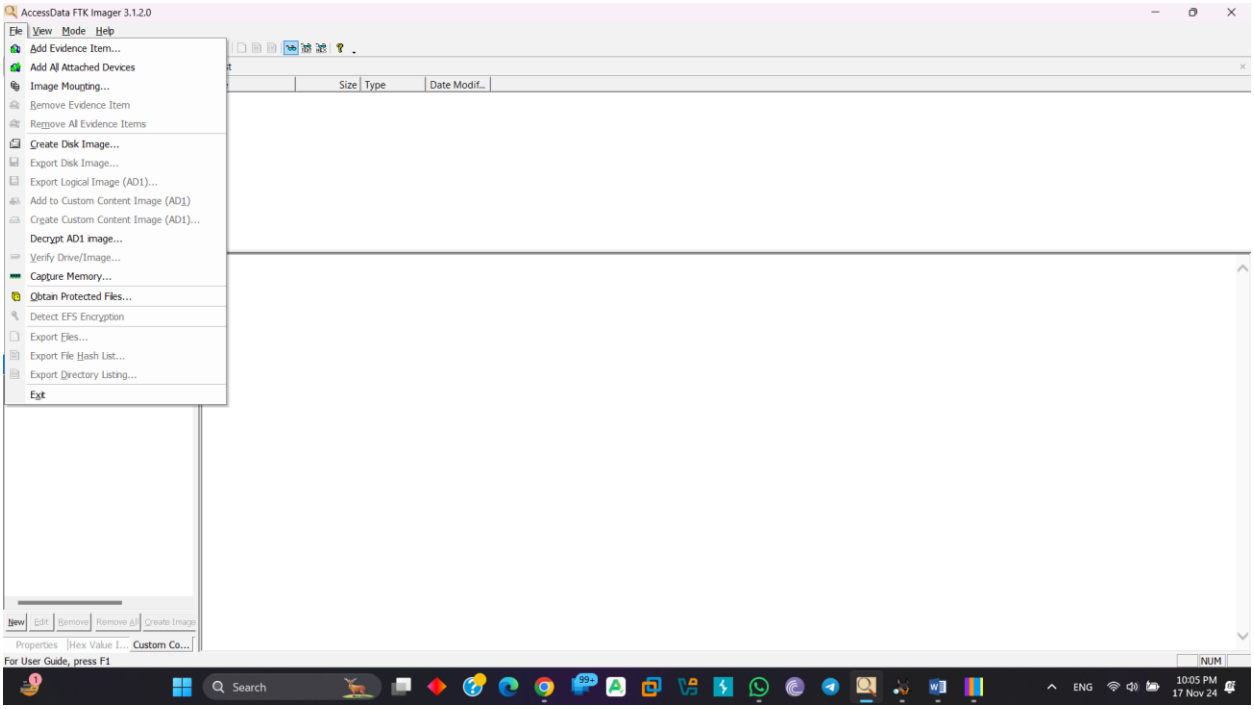
In addition, more other report item:



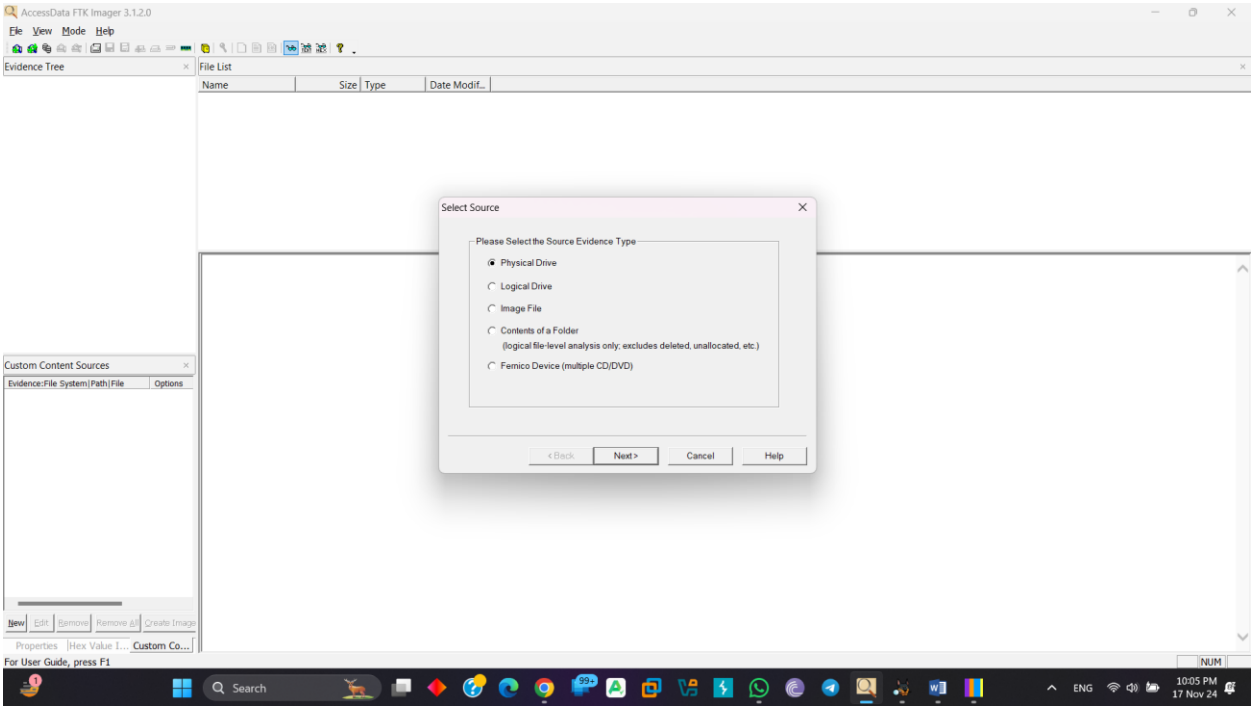

Installed Programs (29)
Metadata (123)
Operating System Information (1)
Recent Documents (39)
Recycle Bin (2)
Shell Bags (41)
Web Accounts (1)
Web Bookmarks (9)
Web Cookies (765)
Web Downloads (16)
Web Form Autofill (1)
Web History (1007)
Web Search (11)
Analysis Results
EXIF Metadata (2)
Extension Mismatch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

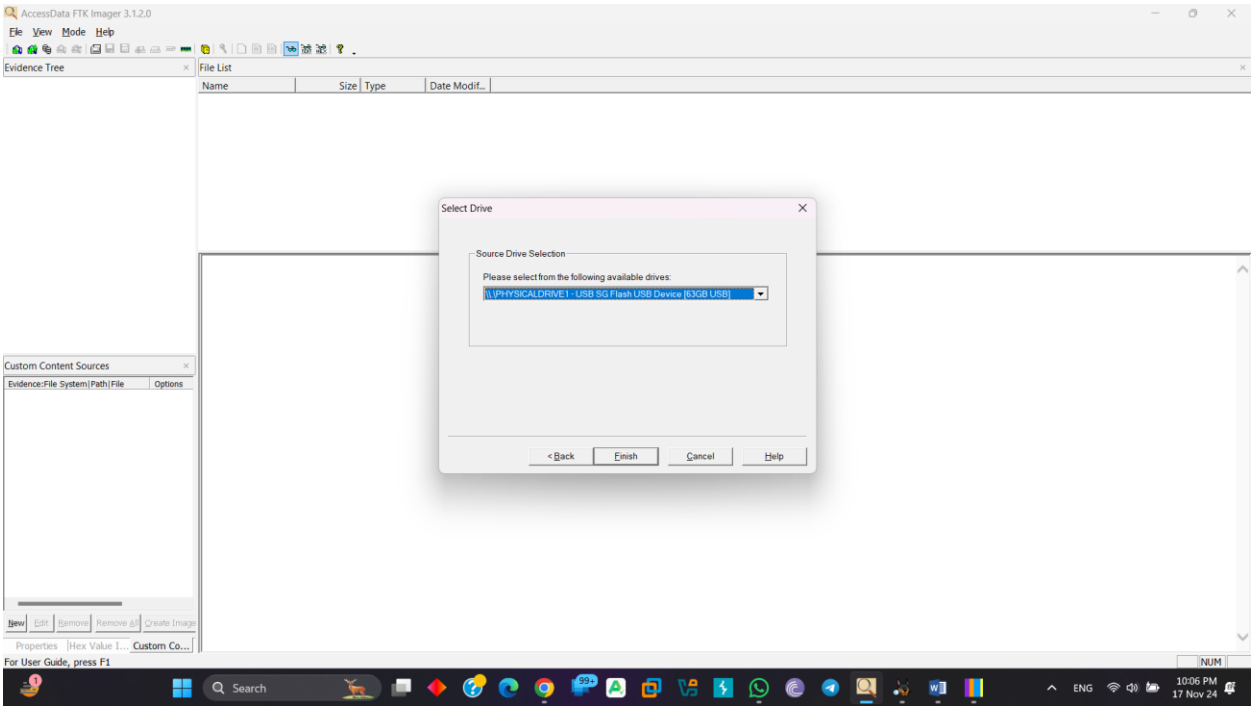
In the beginning go to File→Create new disk:



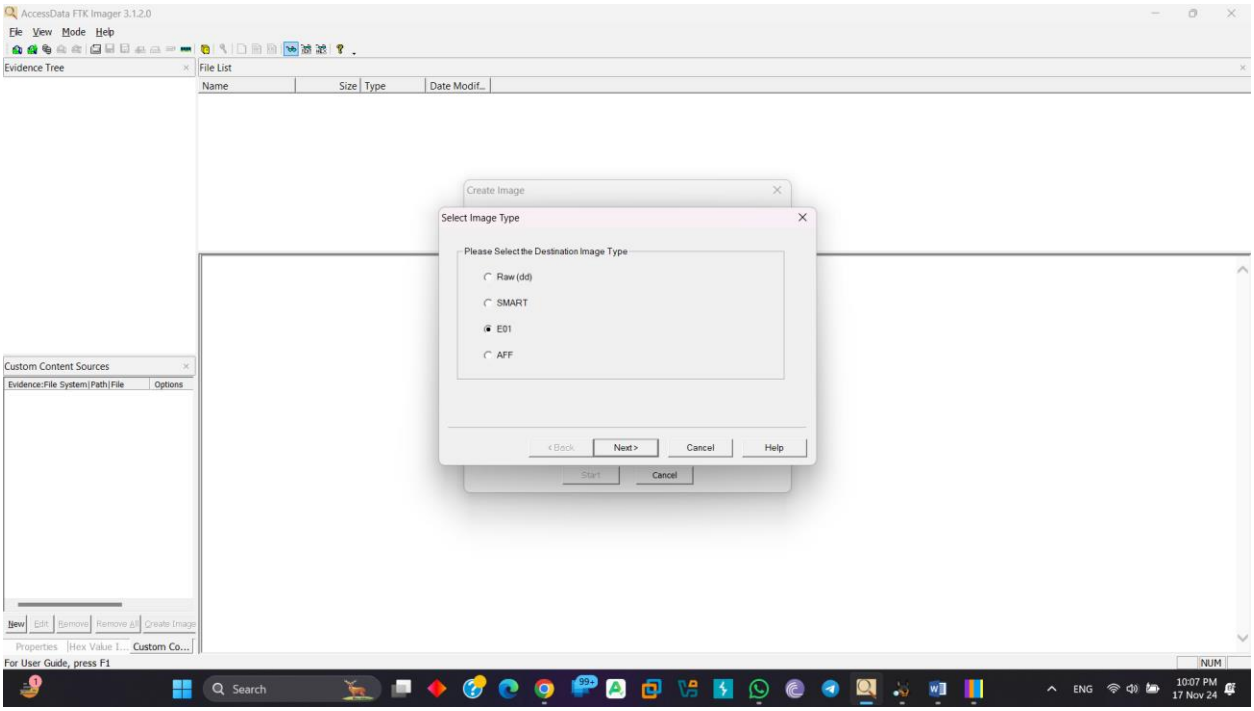
Select any one type:



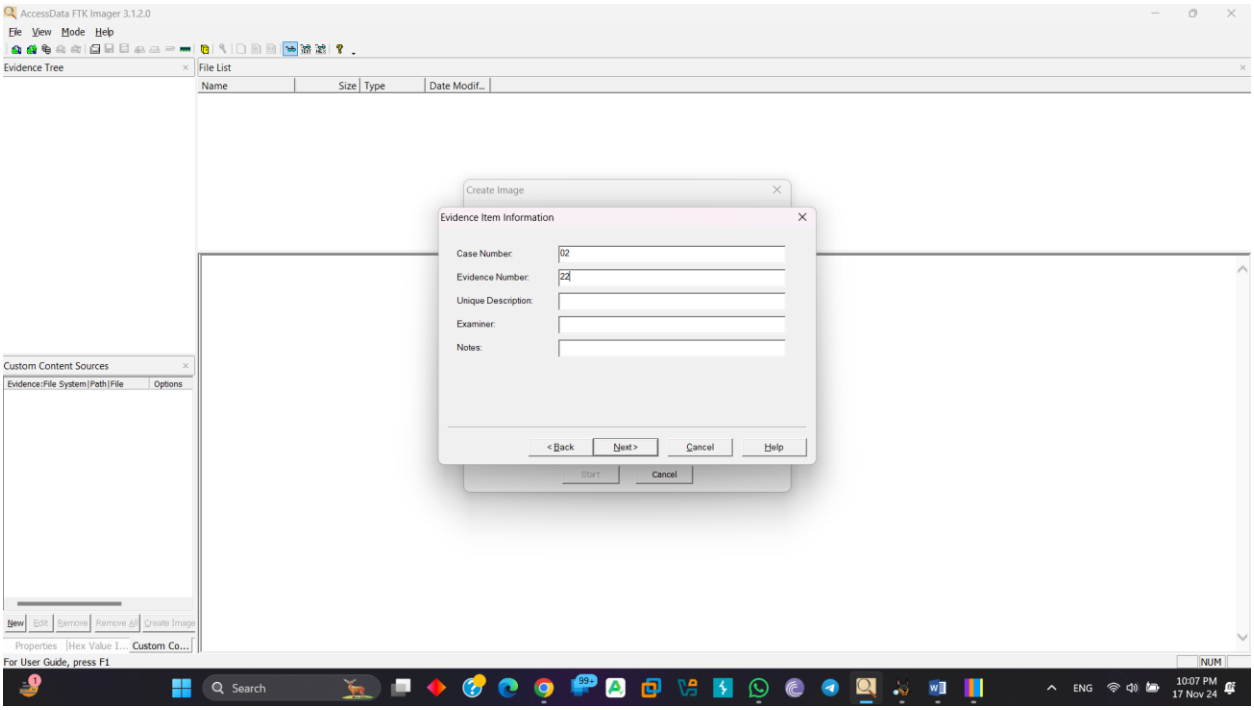
Select the drive:



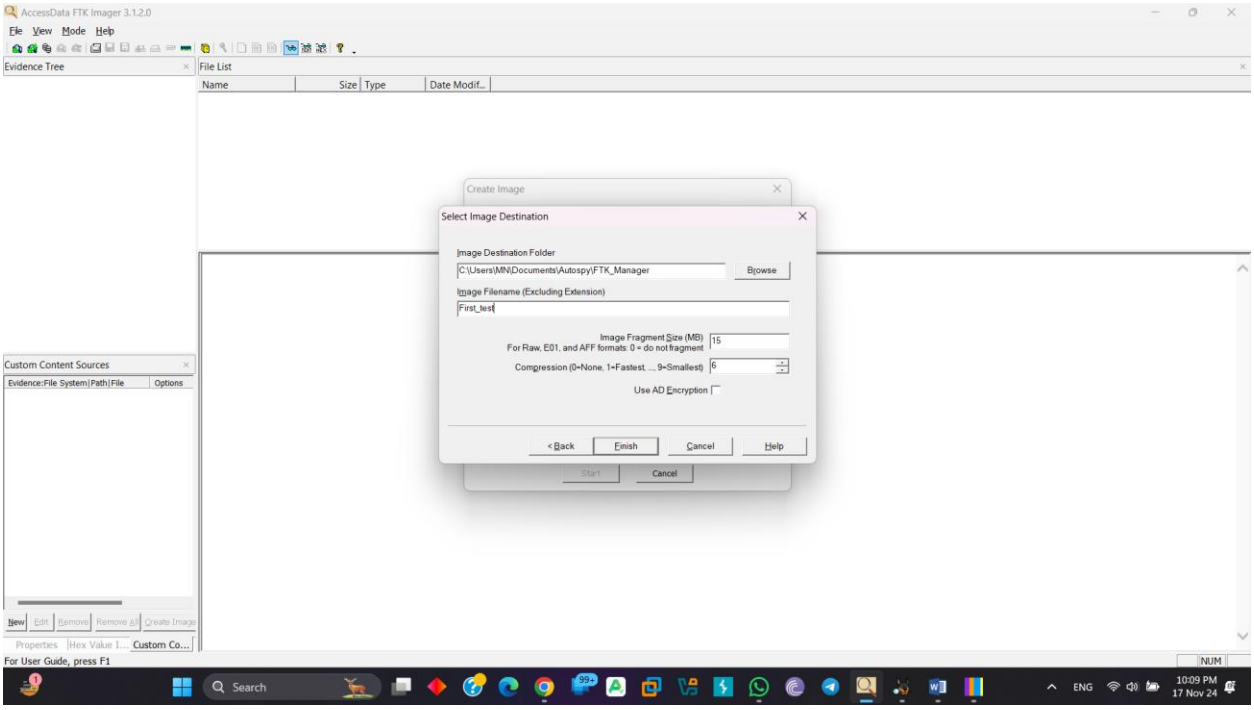
Add image type (any one from them):



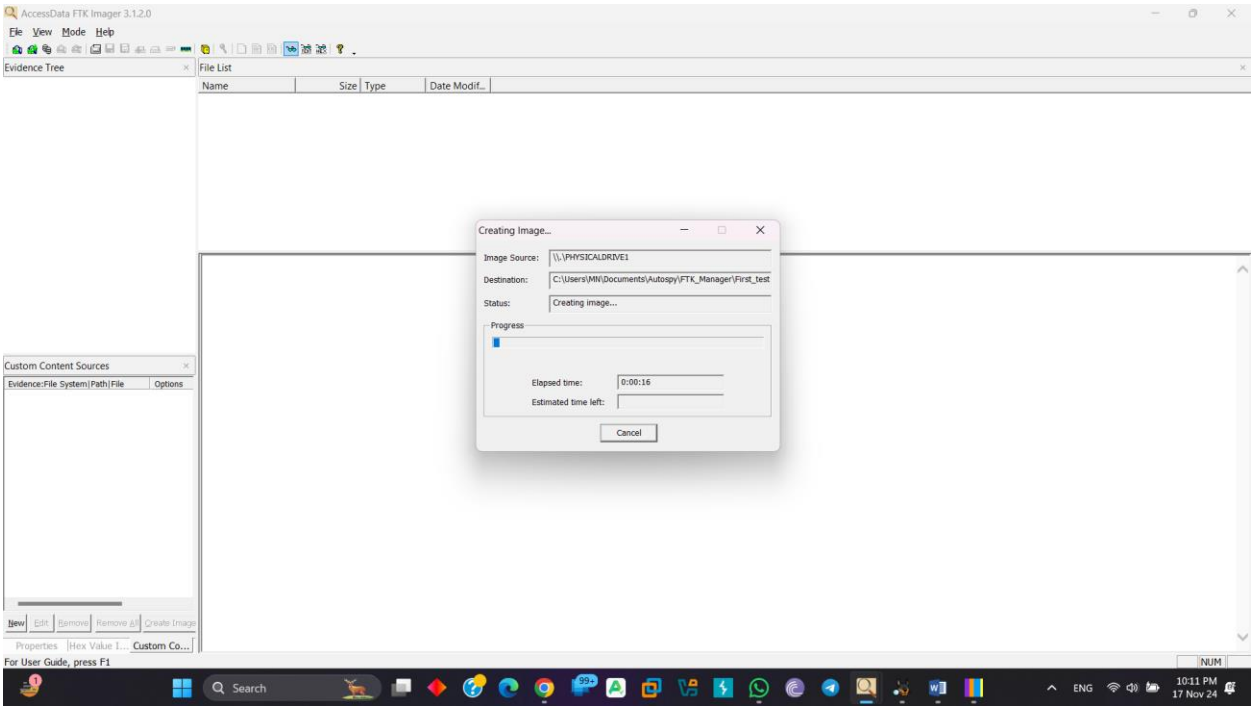
Set Evidence Item Information:



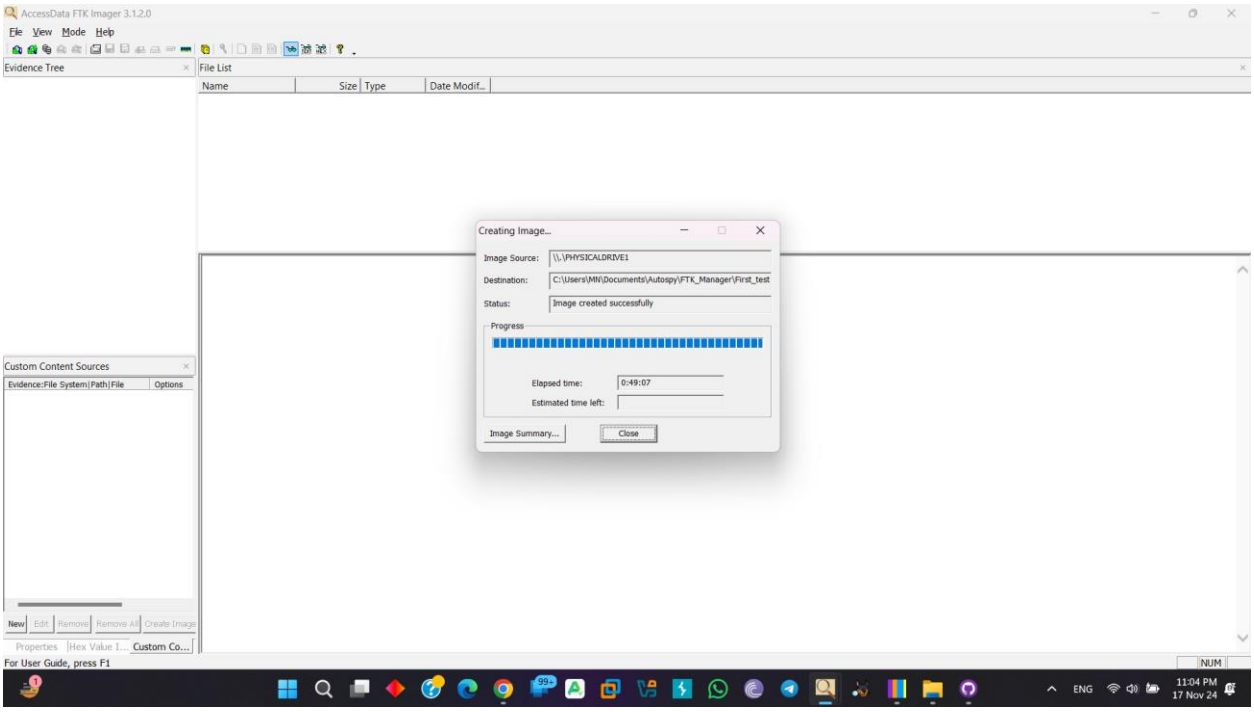
Select Destination folder and set file name and can resize Image Fragment size:



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



It’s take about 49 minutes to execute:



The End