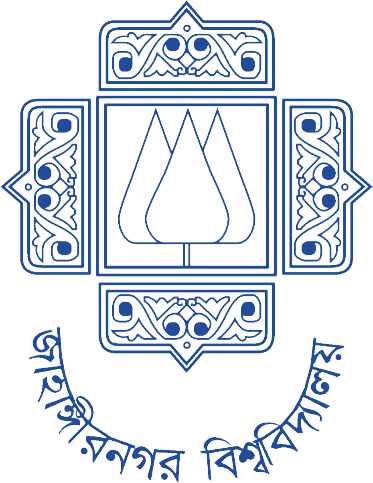
**Institute of Information Technology (IIT)**

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

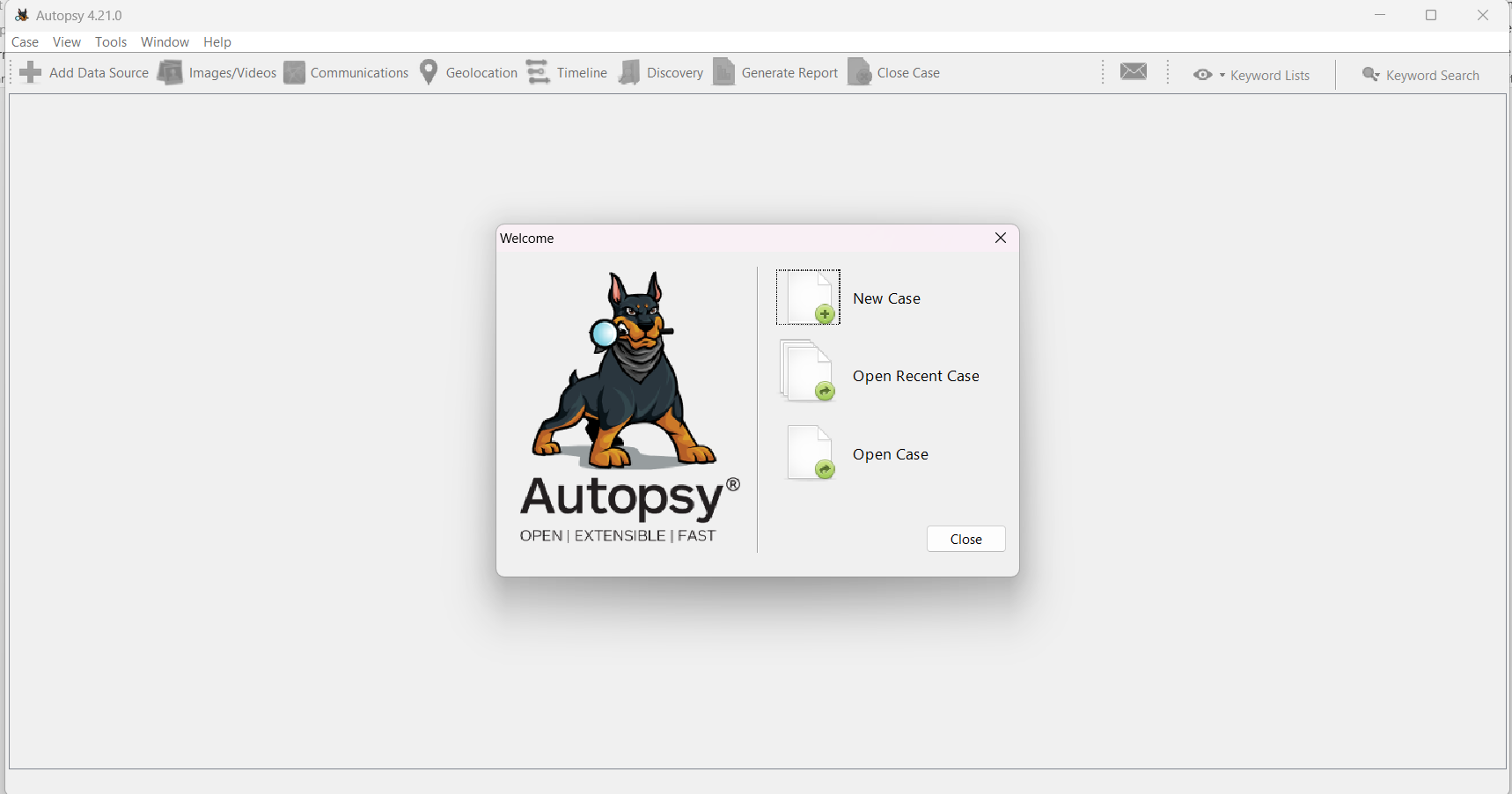
**Submitted To**

  Moinoddeen Quader Al Arabi

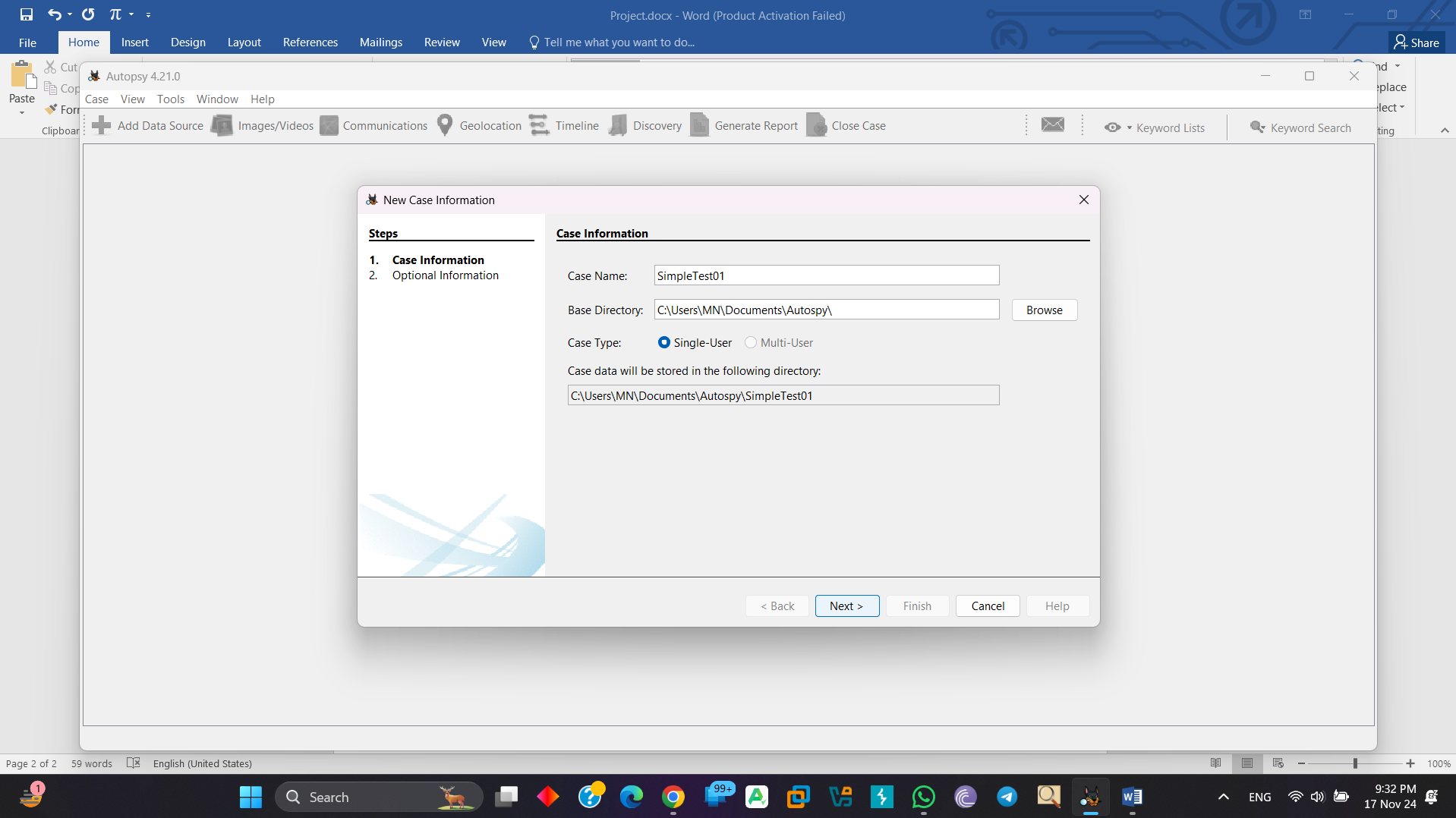
   Ethical Hacker, Forensic Investigator, and VAPT Expert Cyber Security Consultant in Dhaka Division, Bangladesh

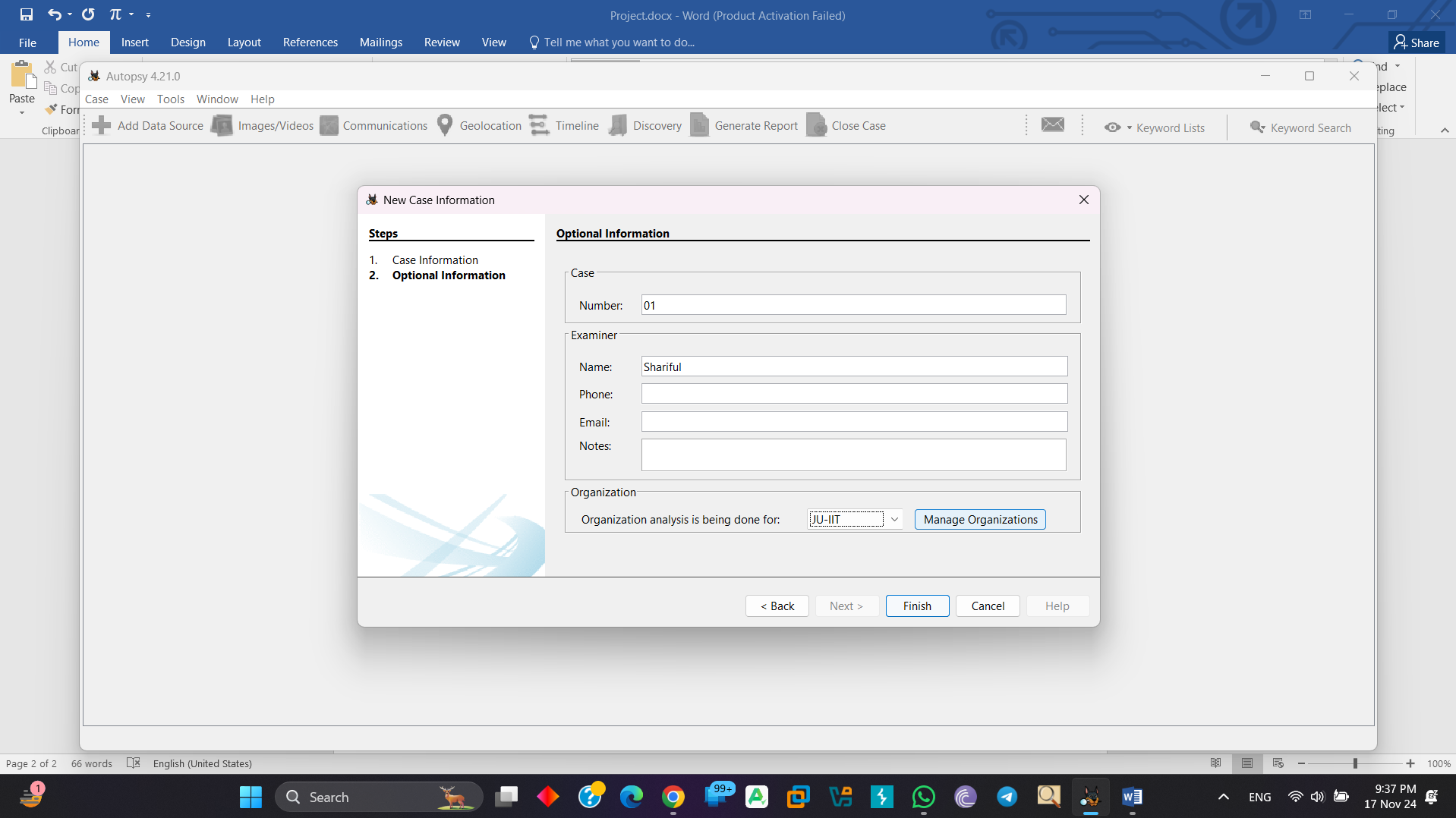
**Disk Forensics with Autopsy**

Create New Case:

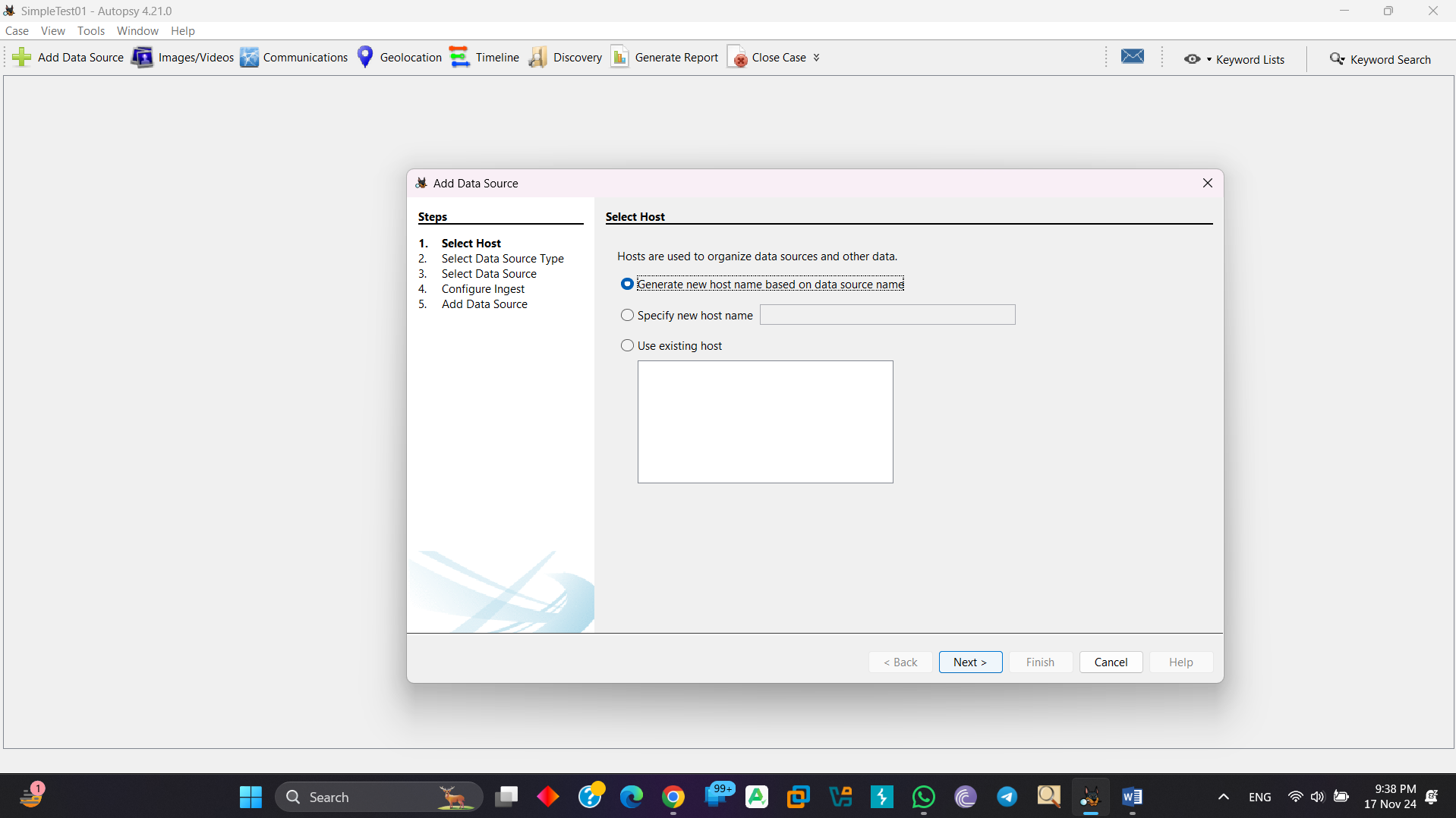


Set a Case Name and Base directory:

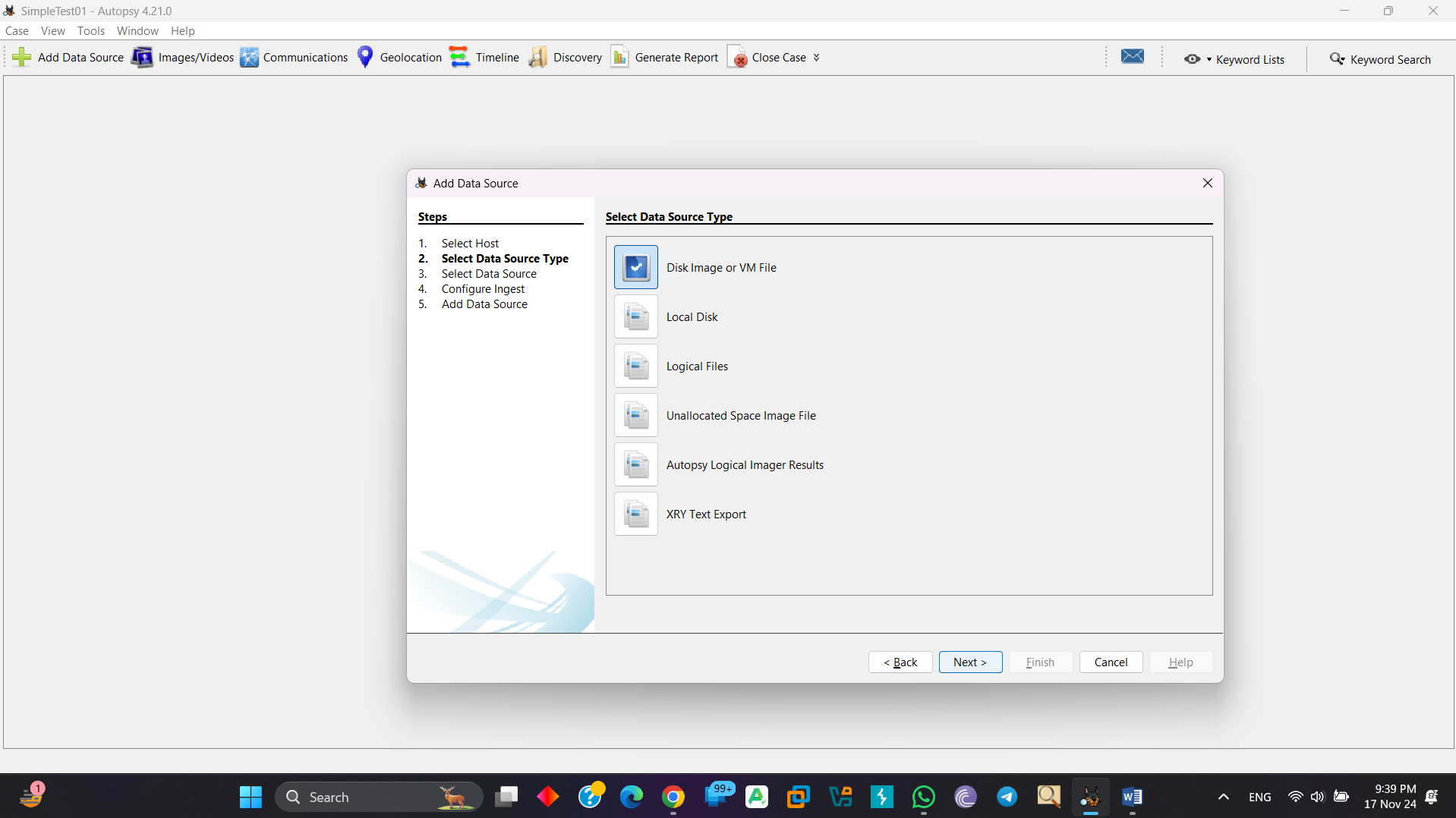




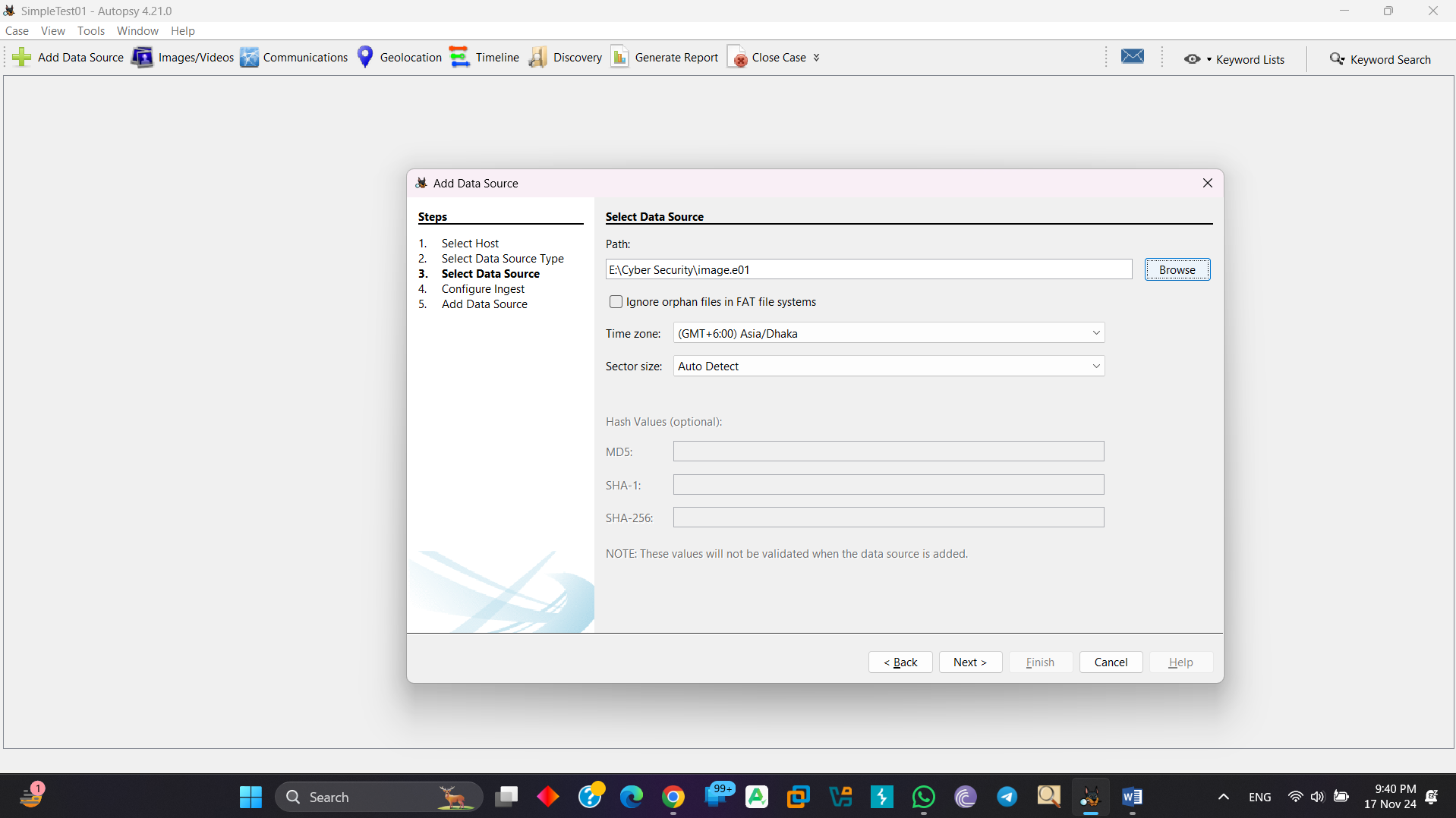
Select a Host (Ex: Generate New Host name based on data source name)



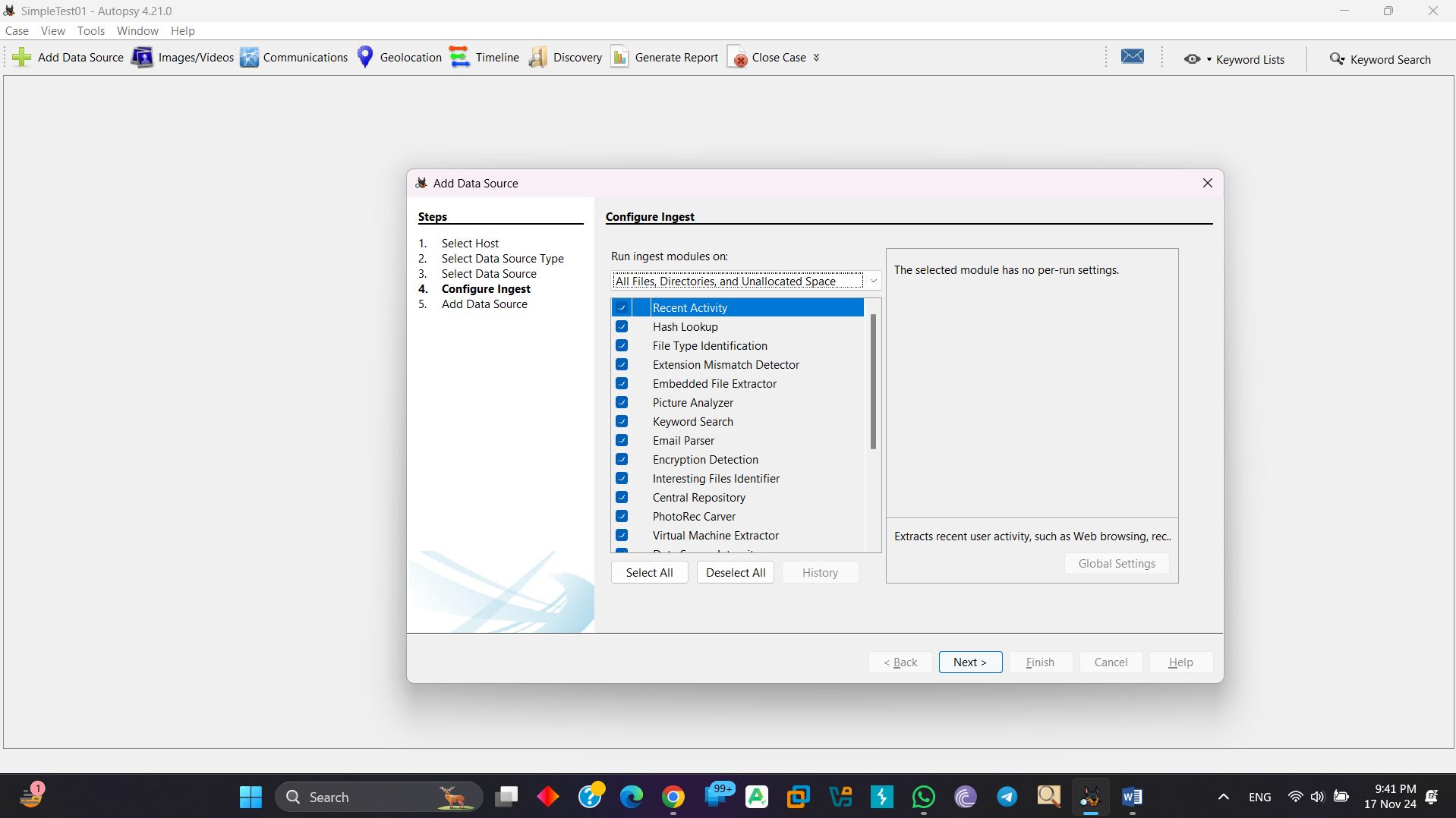
Select any one type of disk:



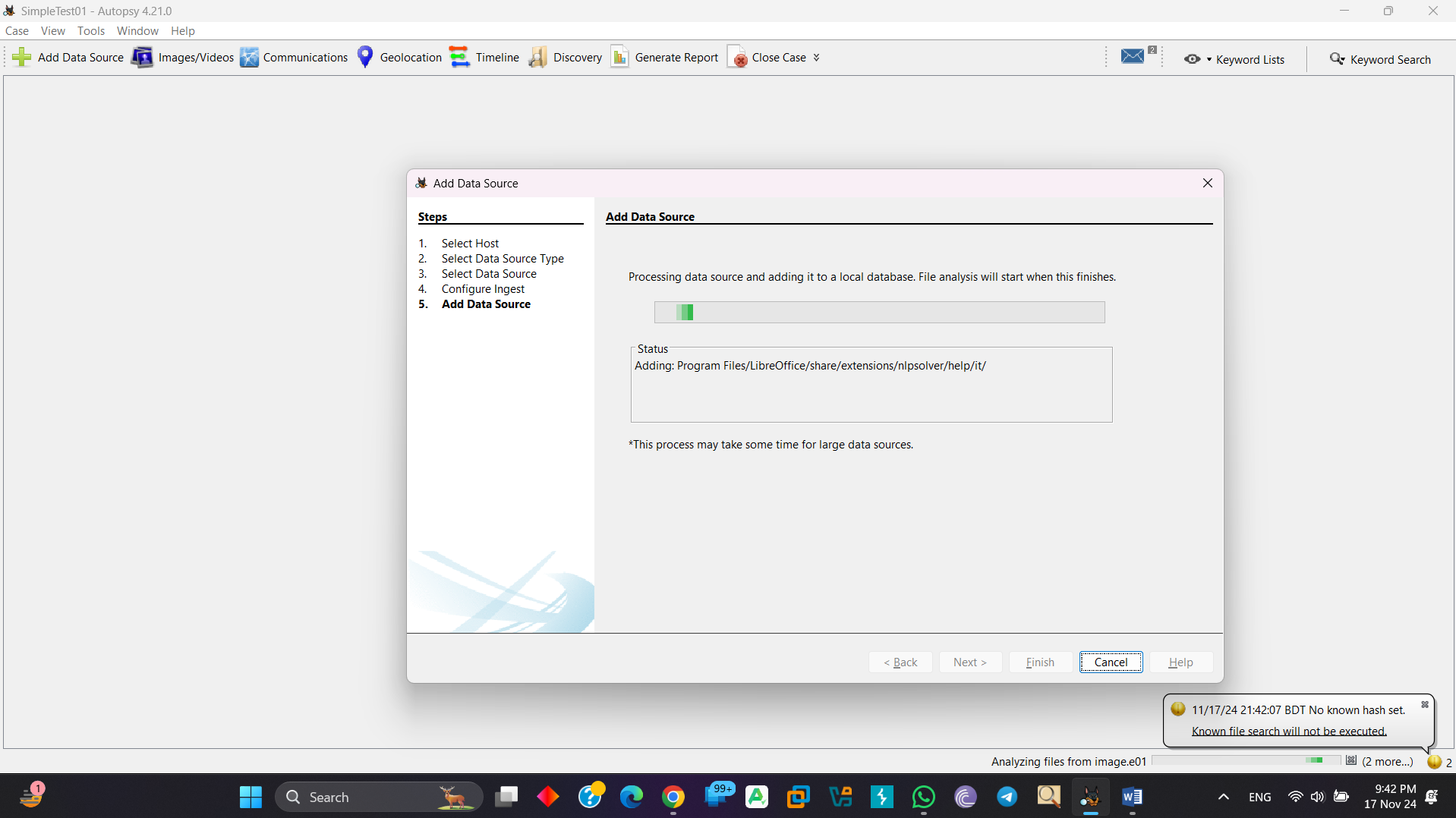
Browse the image:



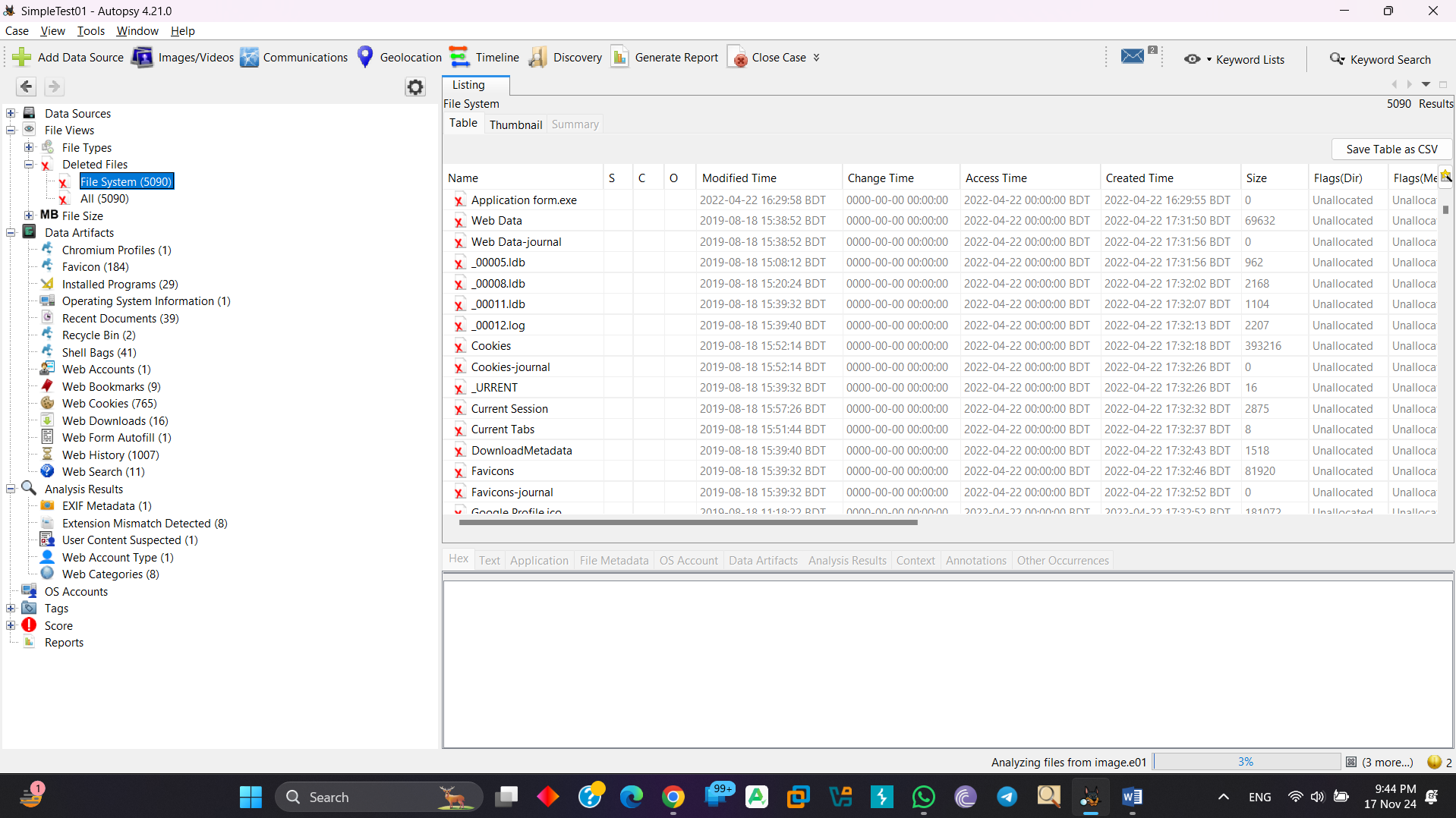
Select needed item and enter next:



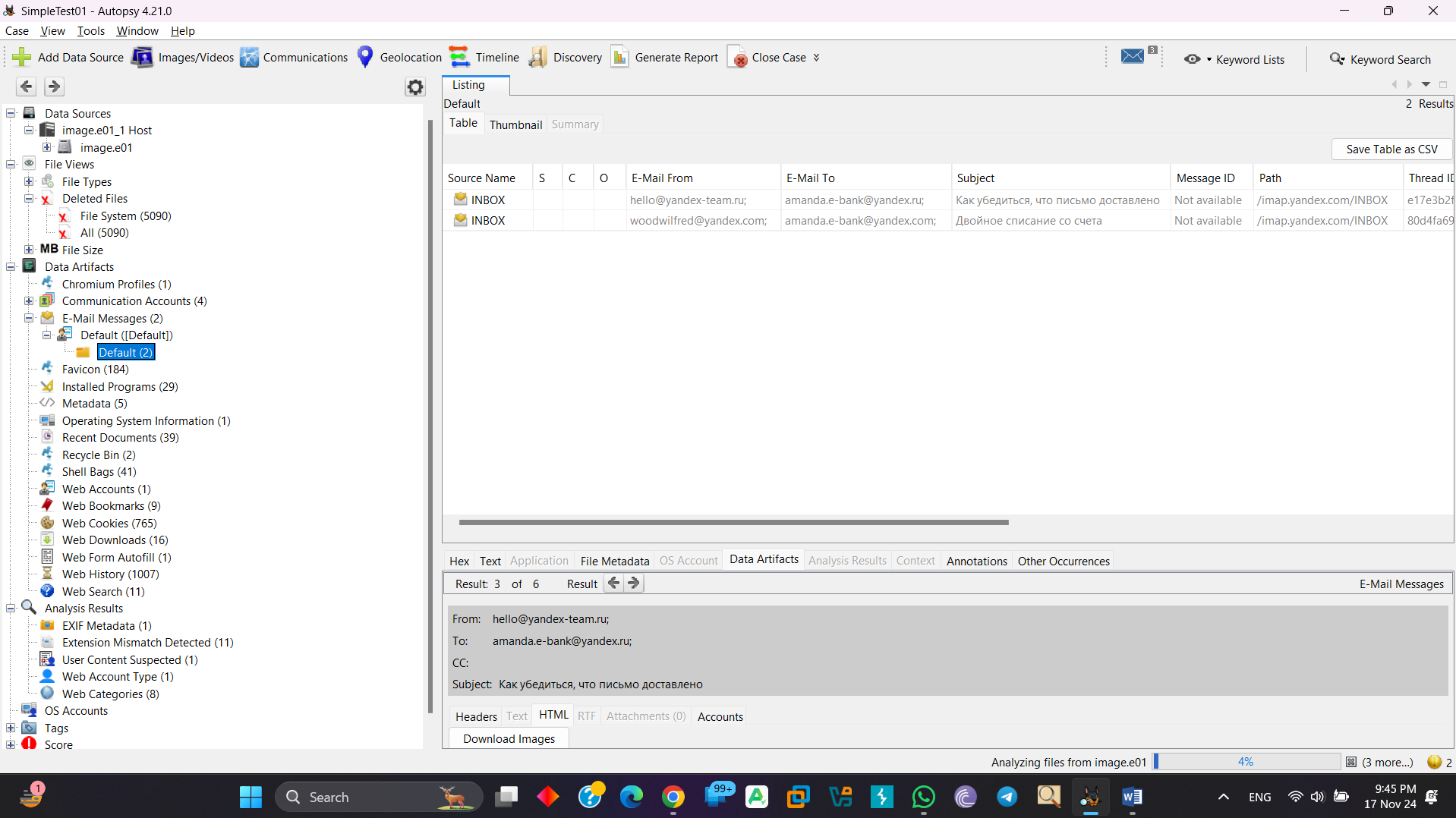
Here add data source:



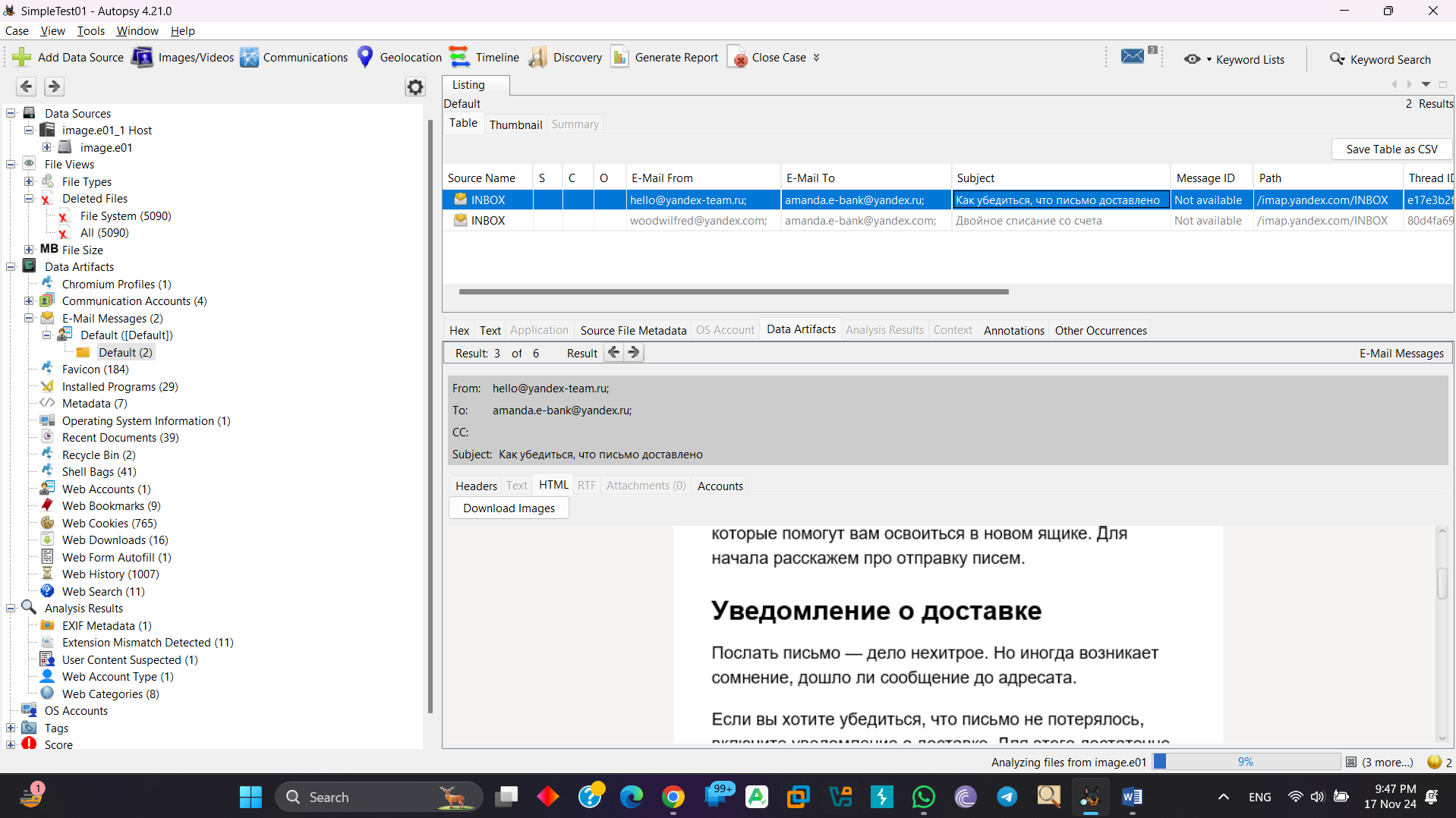
Here is 5090 Delete file:



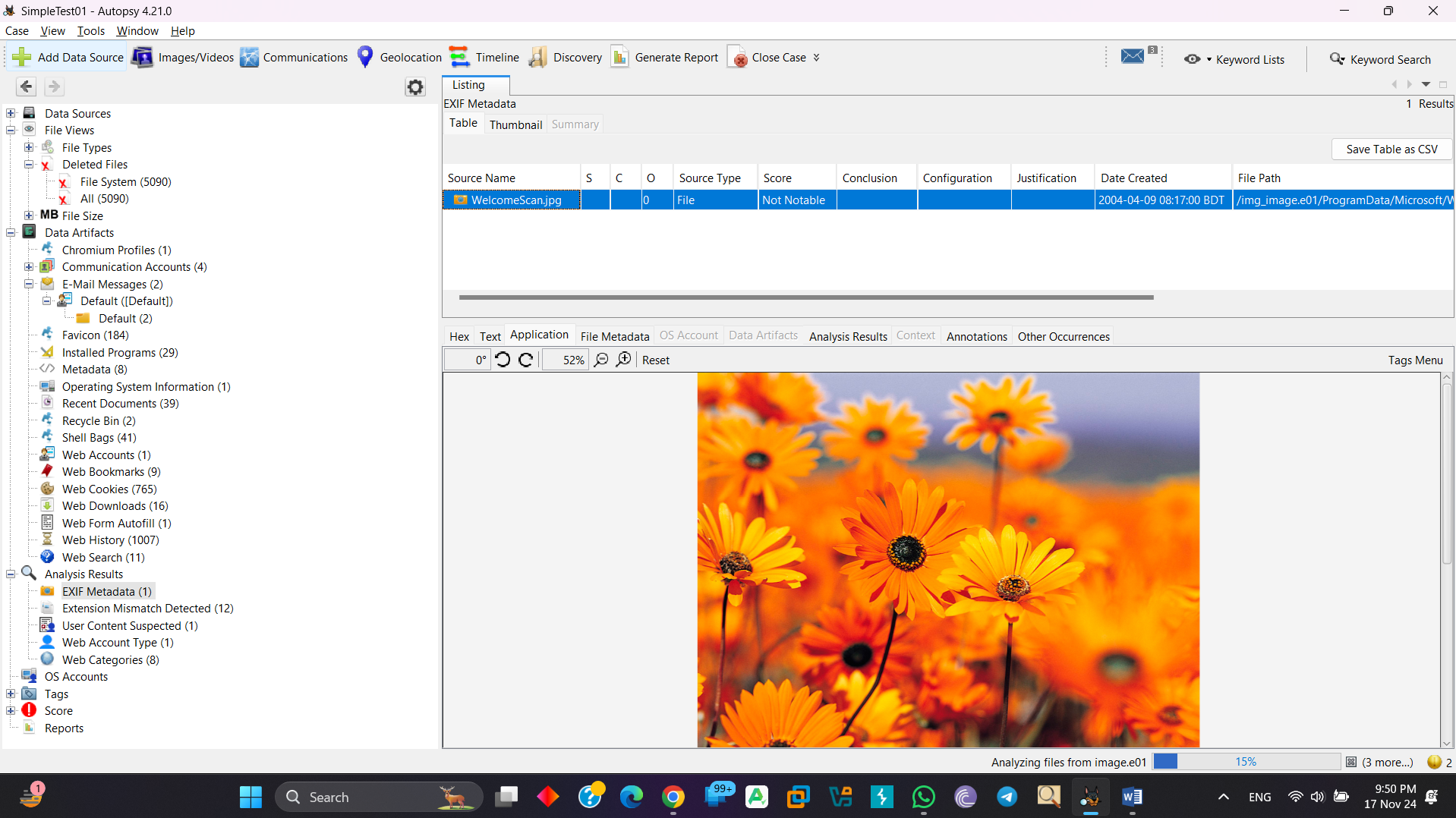
Here are two-email message:



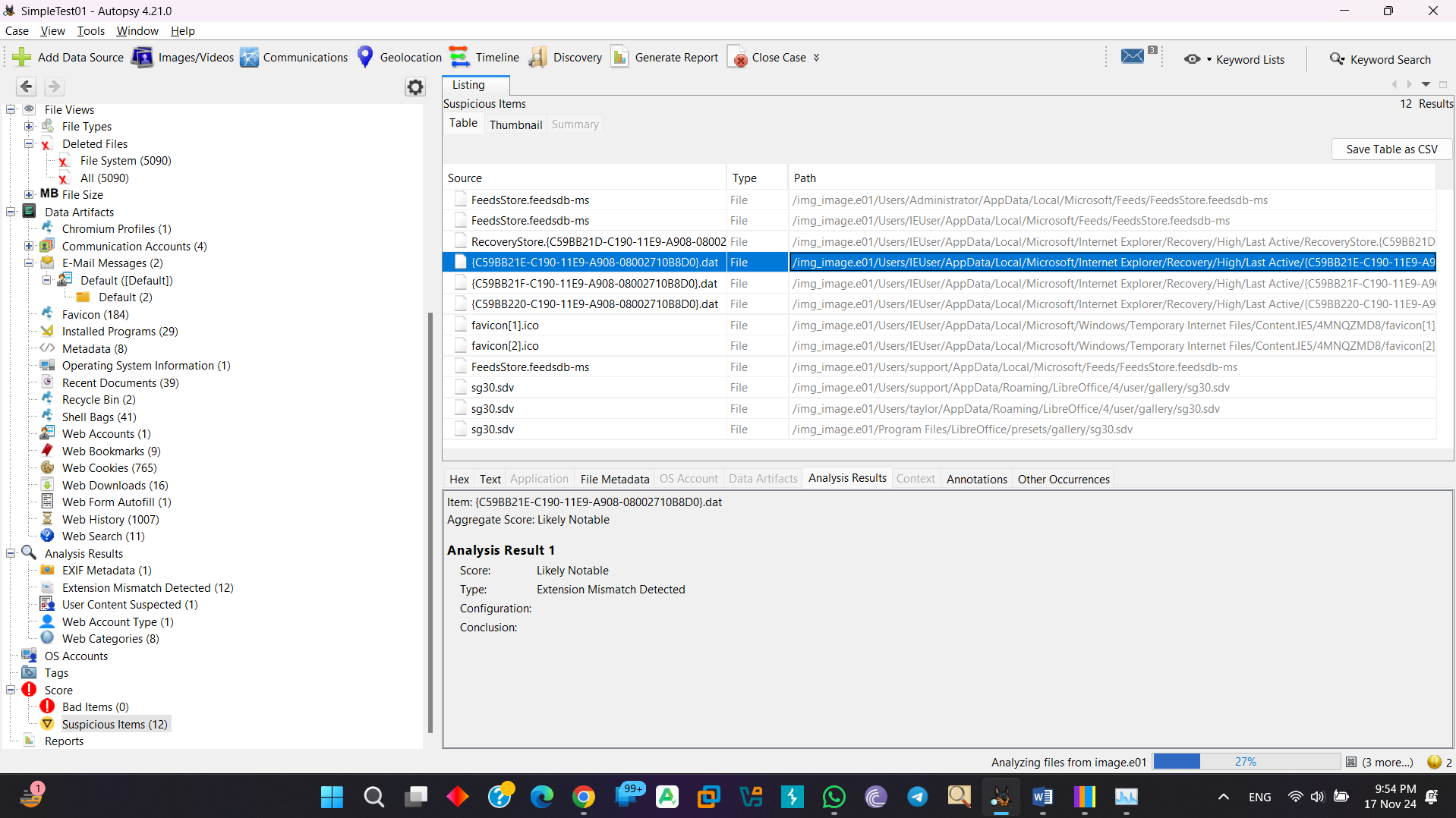
Here is show email from/email to and text of email:



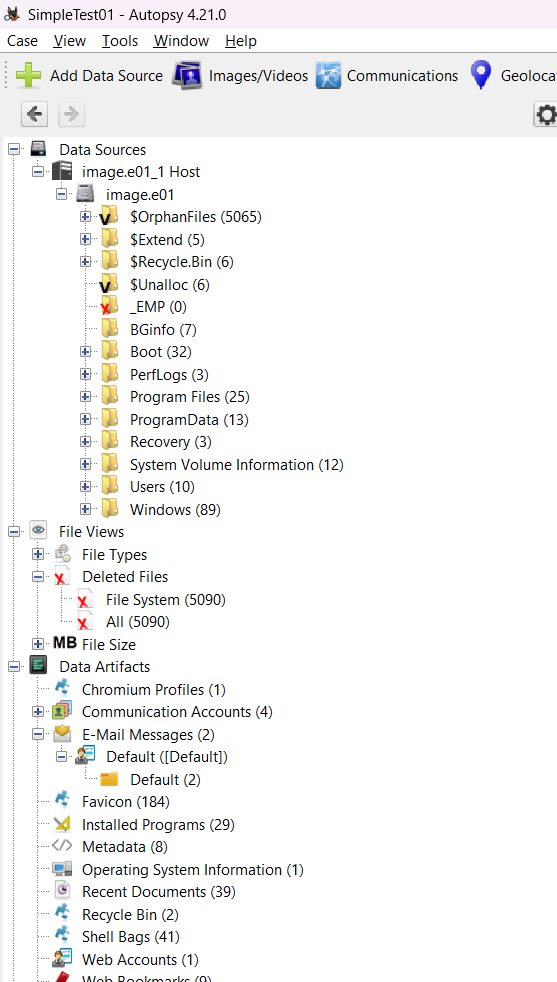
Here is an EXIF Metadata:

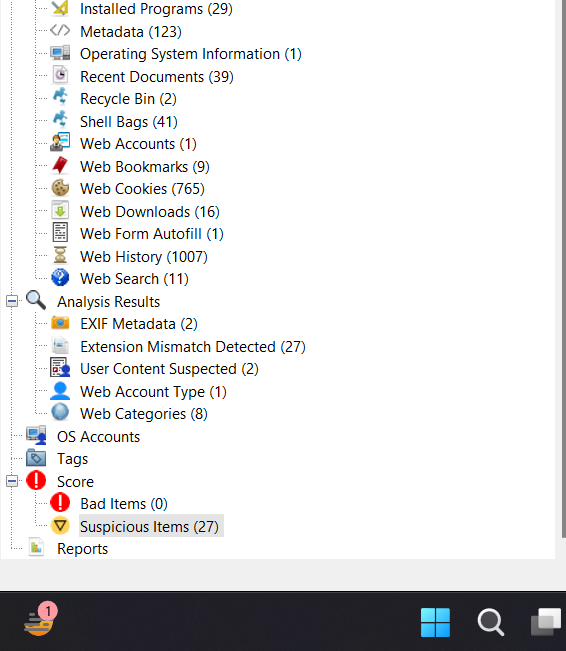


There are 12 suspicious item:



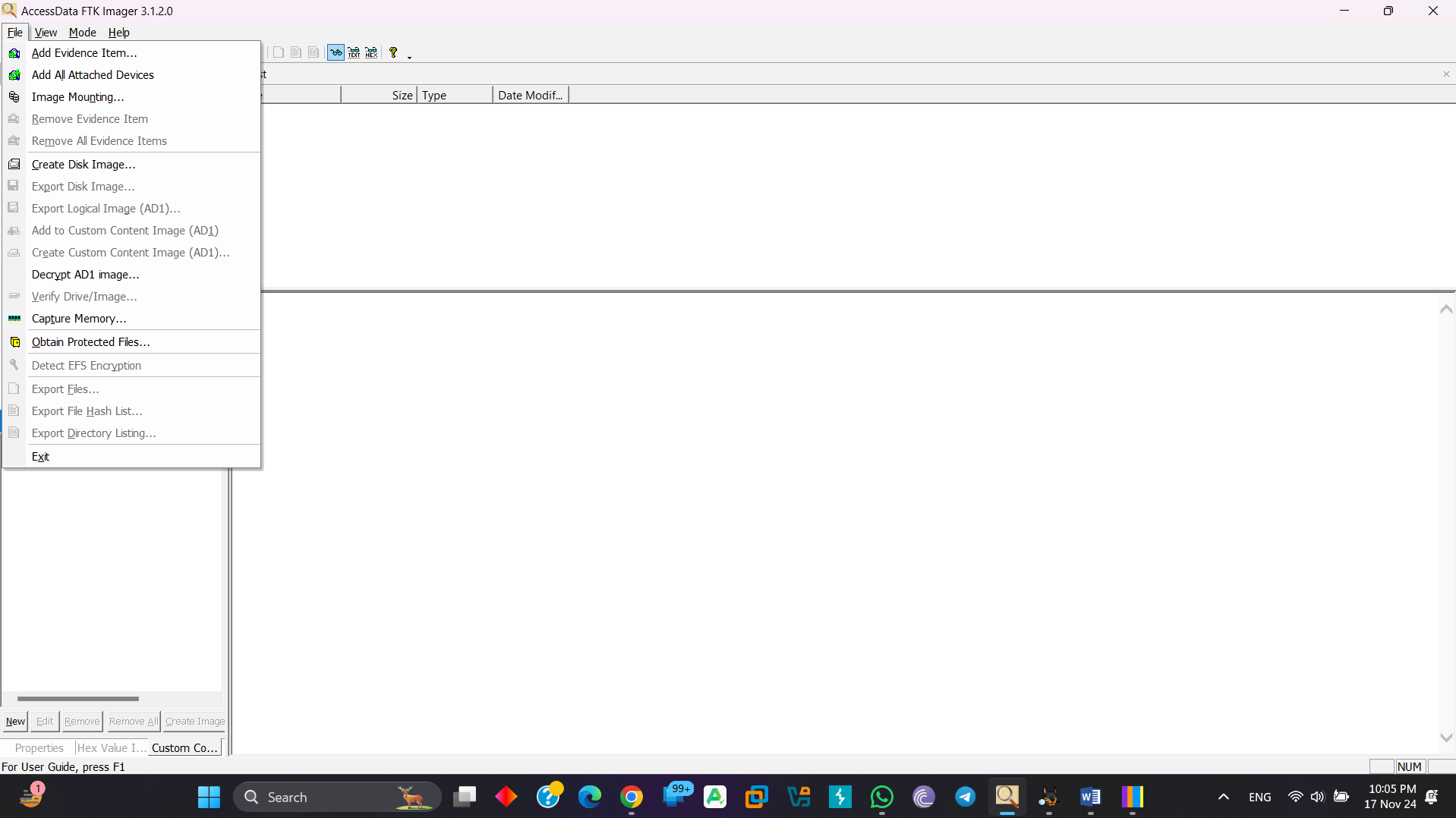
In addition, more other report item:



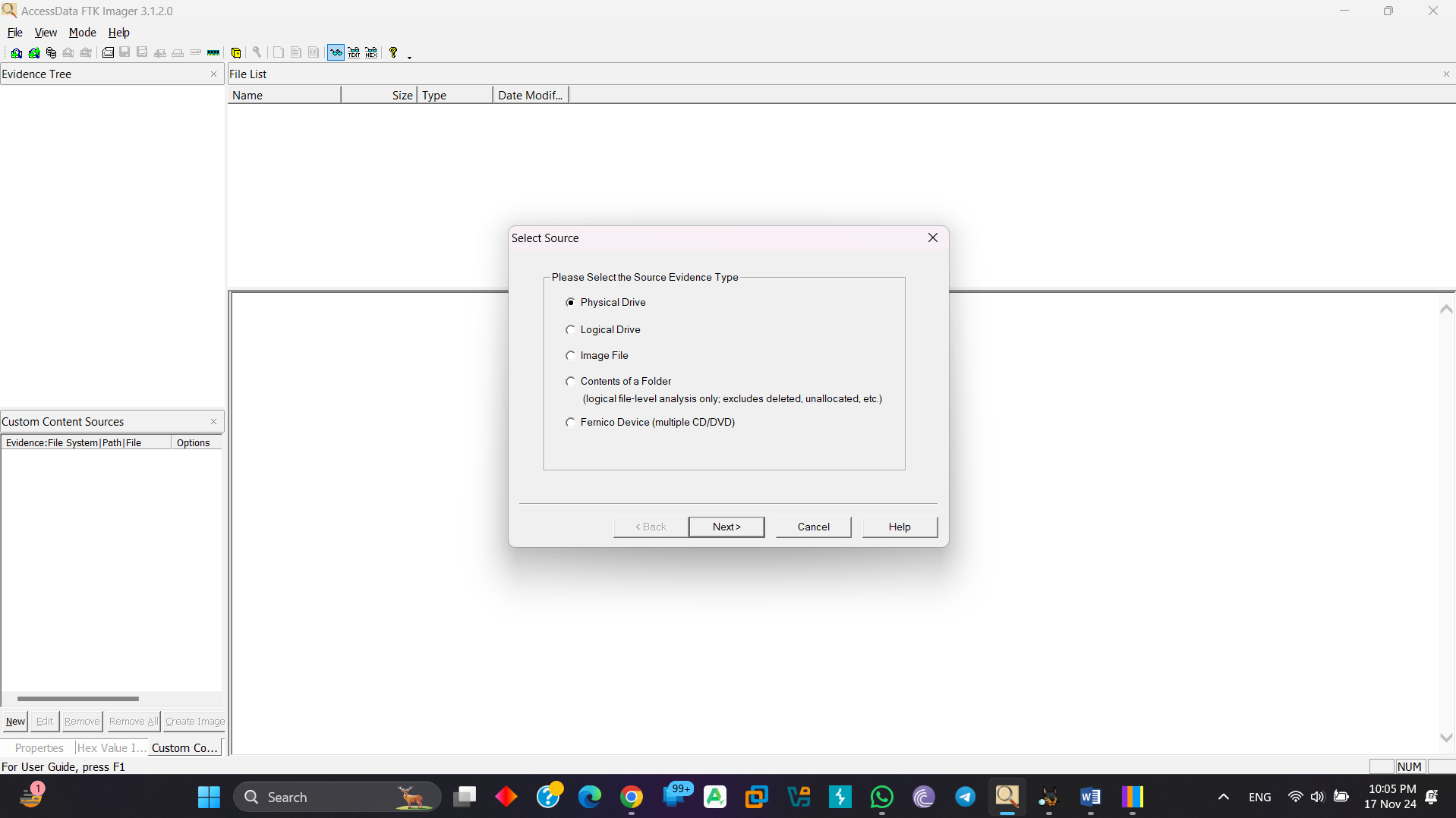


**Disk Forensics with FTK Imager**

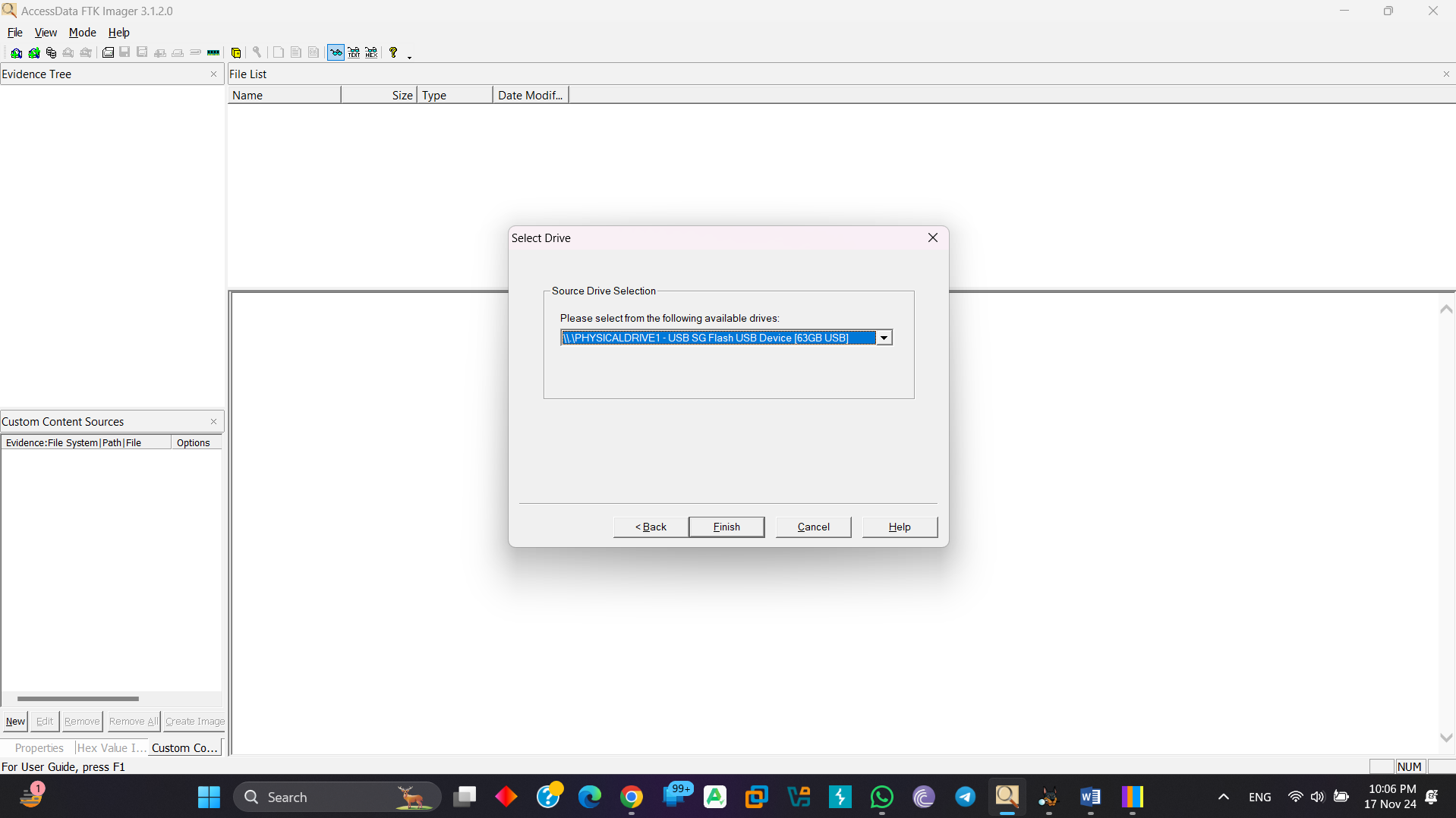
In the beginning go to File🡪Create new disk:



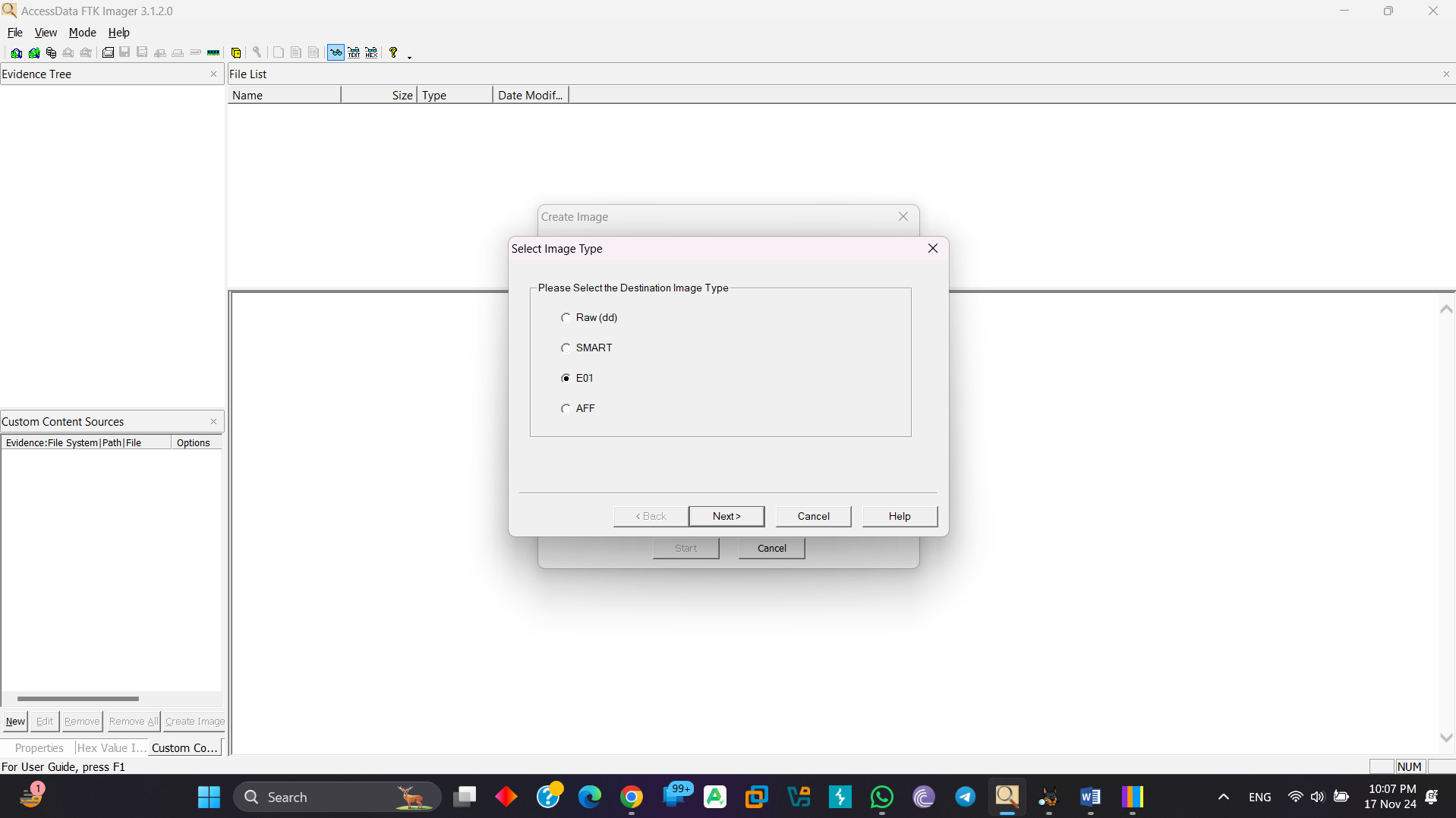
Select any one type:



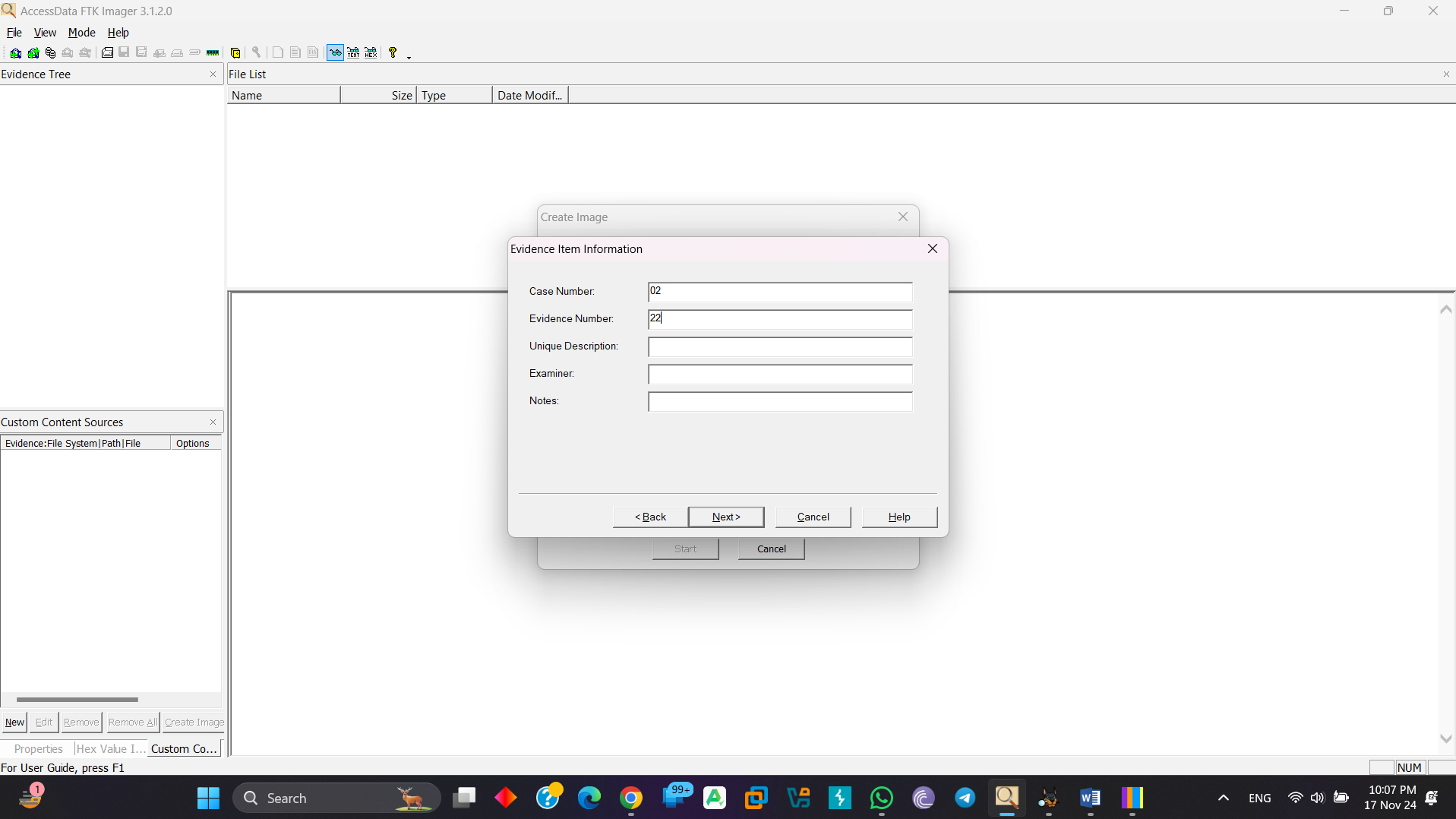
Select the drive:



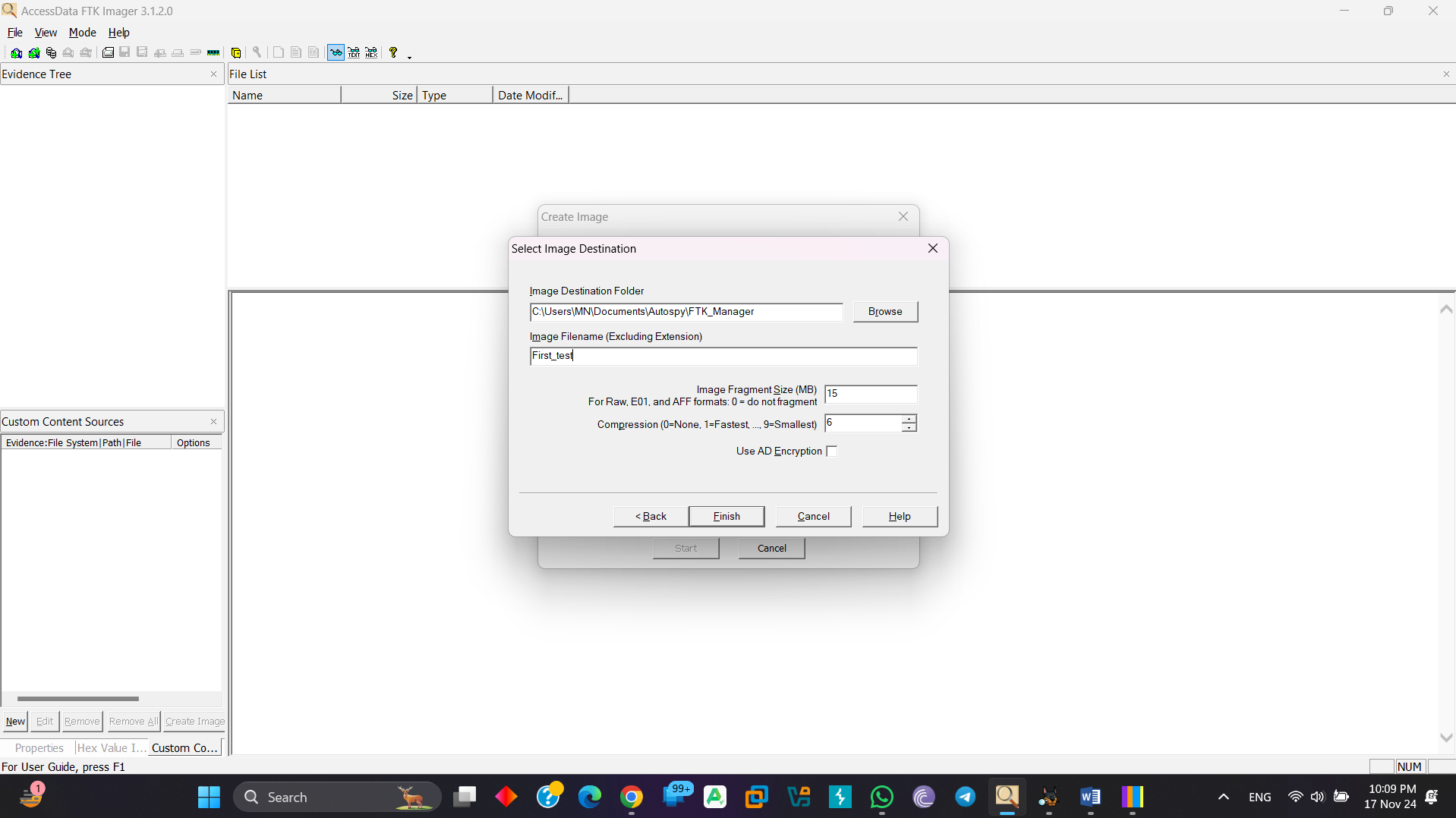
Add image type (any one from them):



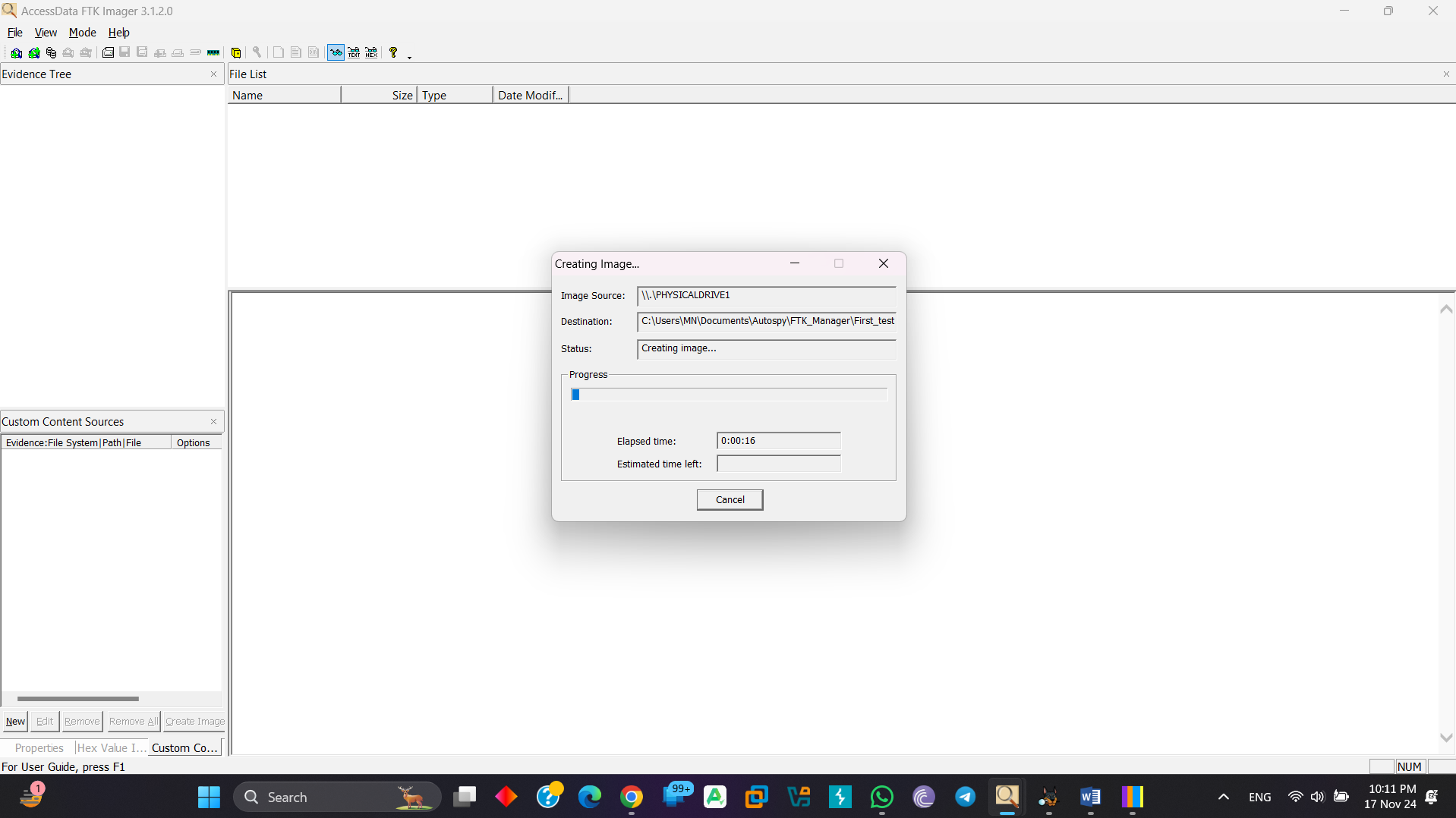
Set Evidence Item Information:



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:

