Program 8. Perform email analysis using the Autopsy tool.

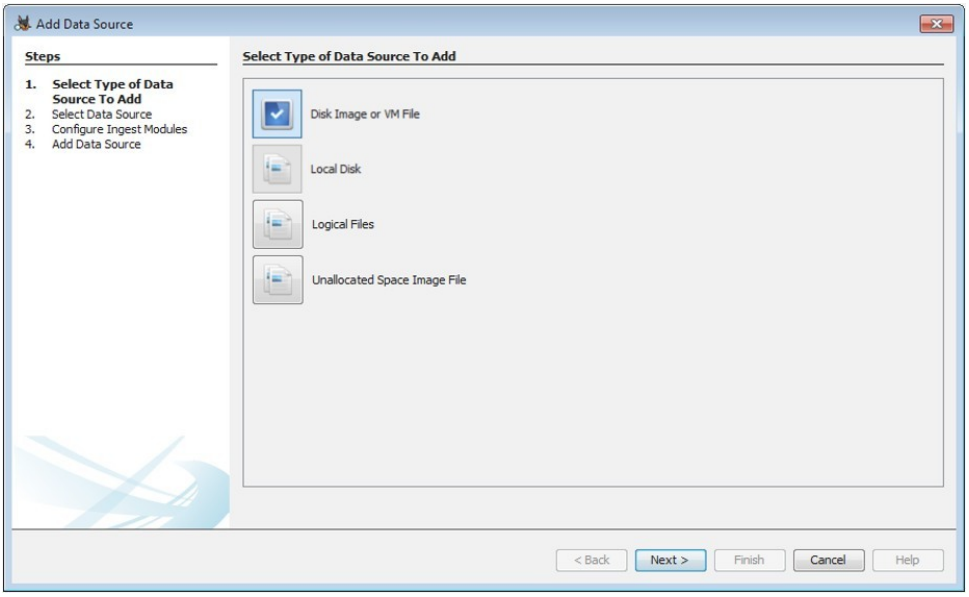
1. Getting Started

Open Autopsy and create a new case.

Click on **Finish** after completing both the steps.

2. Add a data source.

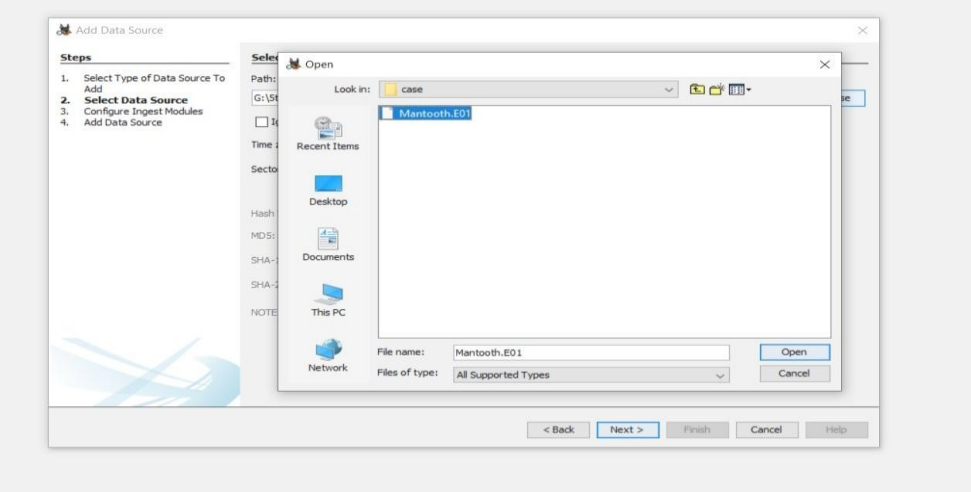
Select the appropriate data source type.



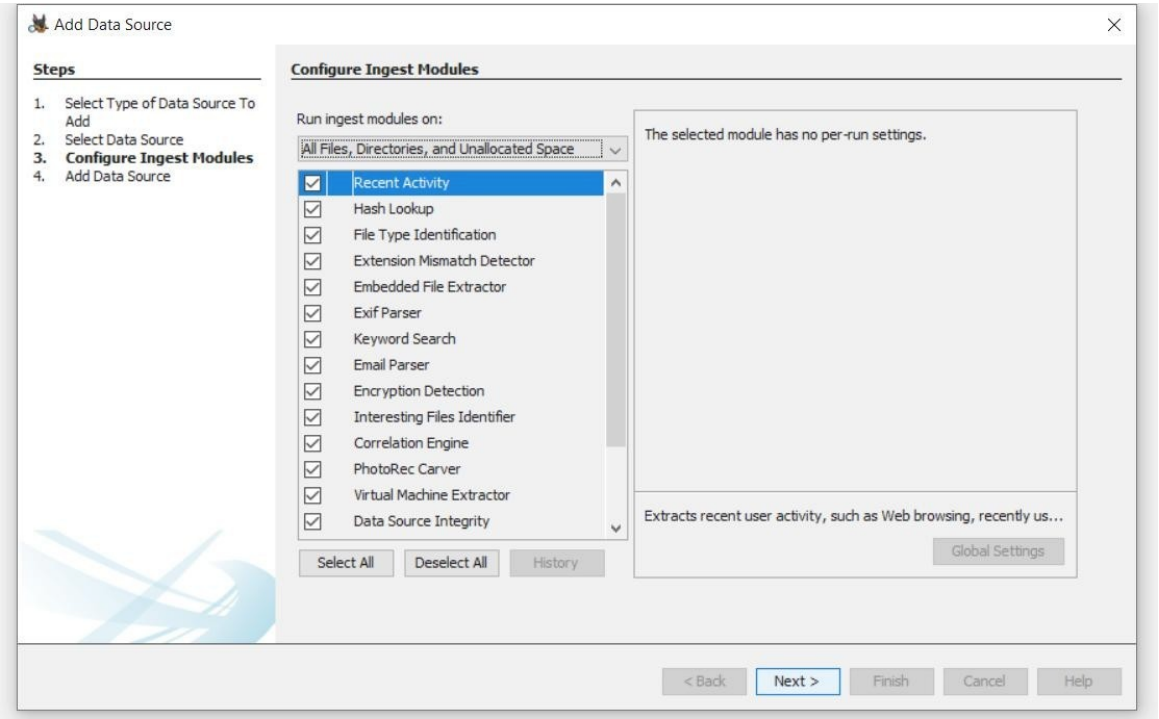
- **Disk Image or VM file:** Includes images that are an exact copy of a hard drive or media card, or a virtual machine image.
- **Local Disk:** Includes Hard disk, Pen drive, memory card, etc.
- **Logical Files.** : Includes local folders or files.

- **Unallocated Space Image File**: Includes files that do not contain a file system but need to run through ingest.

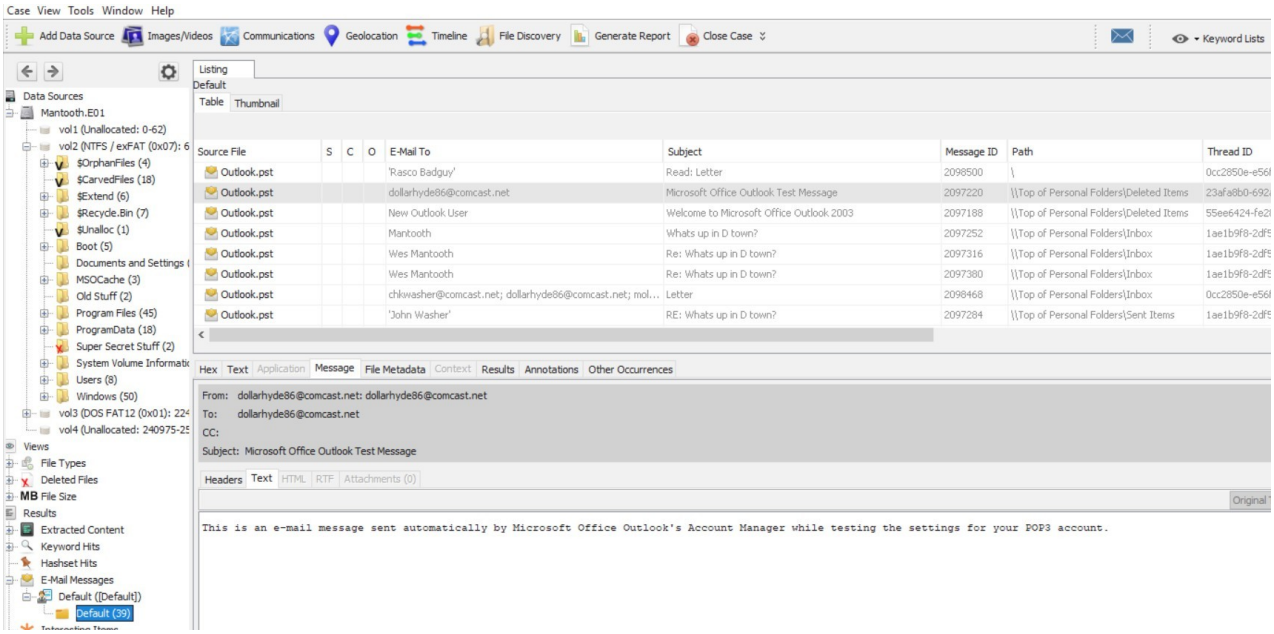
The data source used here is a disk image. Add the data source destination.



Configure ingest modules.



- **E-mail Messages:** Here all the outlook.pst files can be explored.


Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
File Discovery
Generate Report
Close Case
Keyword Lists
Data Sources
Mantooth.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 6
$OrphanFiles (4)
$CarvedFiles (18)
$Extend (6)
$Recycle.Bin (7)
$Unalloc (1)
Boot (5)
Documents and Settings (
MSOCache (3)
Old Stuff (2)
Program Files (45)
ProgramData (18)
Super Secret Stuff (2)
System Volume Informati
Users (8)
Windows (50)
vol3 (DOS FAT12 (0x01): 224
vol4 (Unallocated: 240975-25
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
Keyword Hits
Hashset Hits
E-Mail Messages
Default ([Default])
Default (39)
Listing
Default
Table
Thumbnail
Source File
S
C
O
E-Mail To
Subject
Message ID
Path
Thread ID
Outlook.pst
'Rasco Badguy'
Read: Letter
2098500
\
0cc2850e-e56
Outlook.pst
dollarhyde86@comcast.net
Microsoft Office Outlook Test Message
2097220
\\Top of Personal Folders\Deleted Items
23afa8b0-692
Outlook.pst
New Outlook User
Welcome to Microsoft Office Outlook 2003
2097188
\\Top of Personal Folders\Deleted Items
55ee6424-fe2
Outlook.pst
Mantooth
Whats up in D town?
2097252
\\Top of Personal Folders\Inbox
1ae1b9f8-2df
Outlook.pst
Wes Mantooth
Re: Whats up in D town?
2097316
\\Top of Personal Folders\Inbox
1ae1b9f8-2df
Outlook.pst
Wes Mantooth
Re: Whats up in D town?
2097380
\\Top of Personal Folders\Inbox
1ae1b9f8-2df
Outlook.pst
chkwasher@comcast.net; dollarhyde86@comcast.net; mol...
Letter
2098468
\\Top of Personal Folders\Inbox
0cc2850e-e56
Outlook.pst
'John Washer'
RE: Whats up in D town?
2097284
\\Top of Personal Folders\Sent Items
1ae1b9f8-2df
Hex
Text
Application
Message
File Metadata
Context
Results
Annotations
Other Occurrences
From: dollarhyde86@comcast.net: dollarhyde86@comcast.net
To: dollarhyde86@comcast.net
CC:
Subject: Microsoft Office Outlook Test Message
Headers
Text
HTML
RTF
Attachments (0)
Original
This is an e-mail message sent automatically by Microsoft Office Outlook's Account Manager while testing the settings for your POP3 account.

Program 9. Perform Registry analysis and get boot time logging using process monitor tool

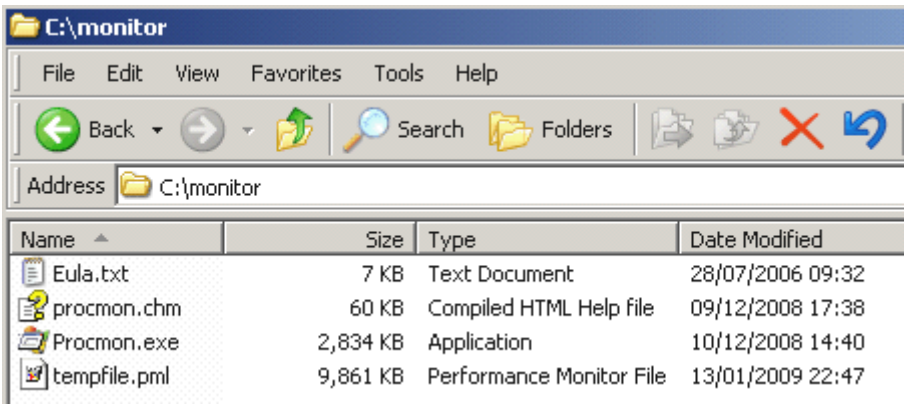
Prepare —Process Monitor‖ for logging

1. Login using an account with administrative privilege (for example “Administrator”)

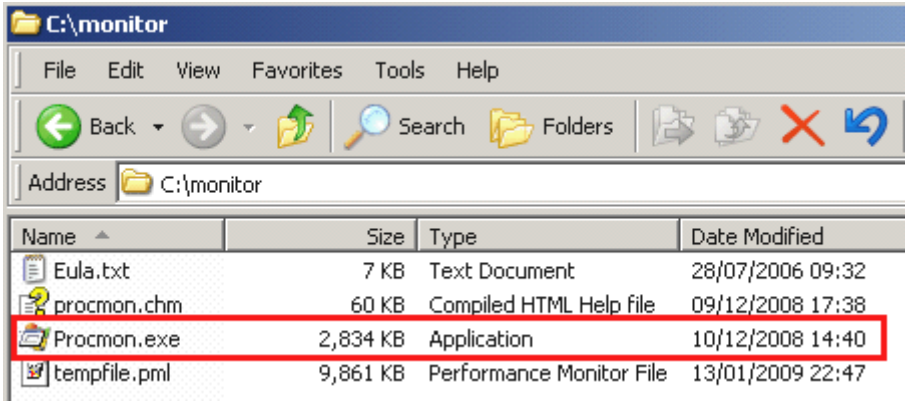
2. Create a folder in system drive (default C:\ ) named “monitor”

3. Download the software using the following link: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

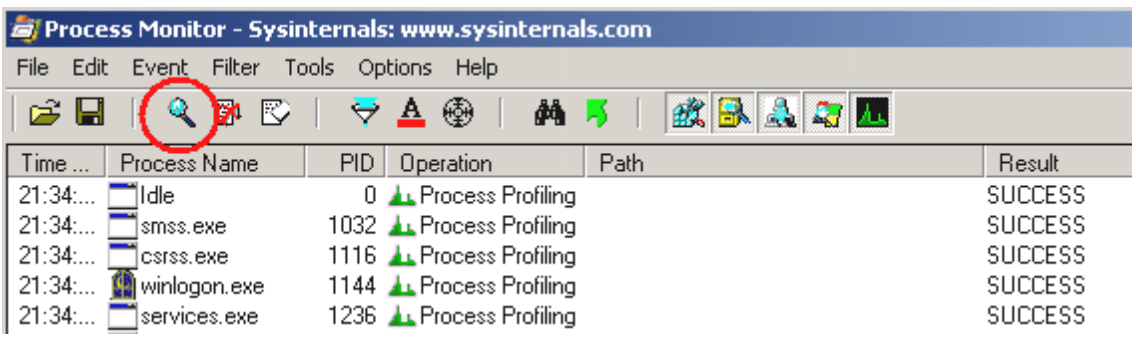
4. Extract the archive to the folder C:\monitor created in step 2.



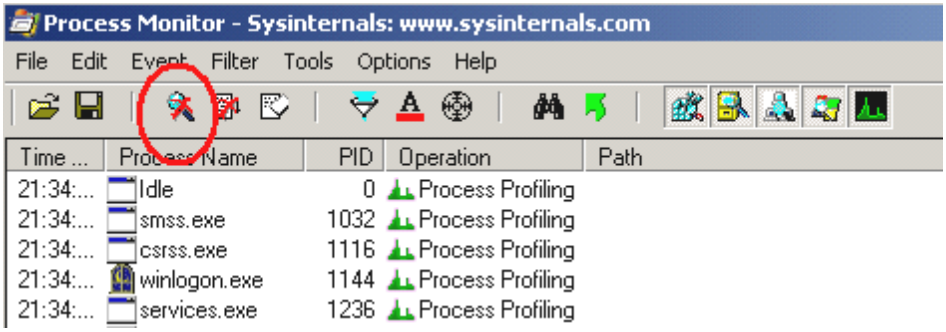
5. Double Click on the file “Procmon.exe”



6. Click on the “Capture” icon to stop the capture process.

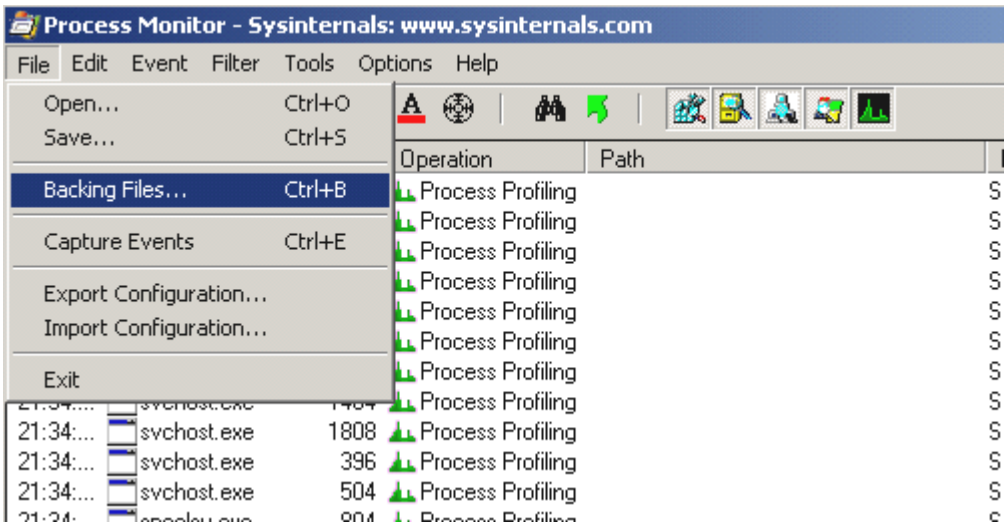


7. The Capture icon will now have a red X over it, meaning that the program is no longer capturing events.

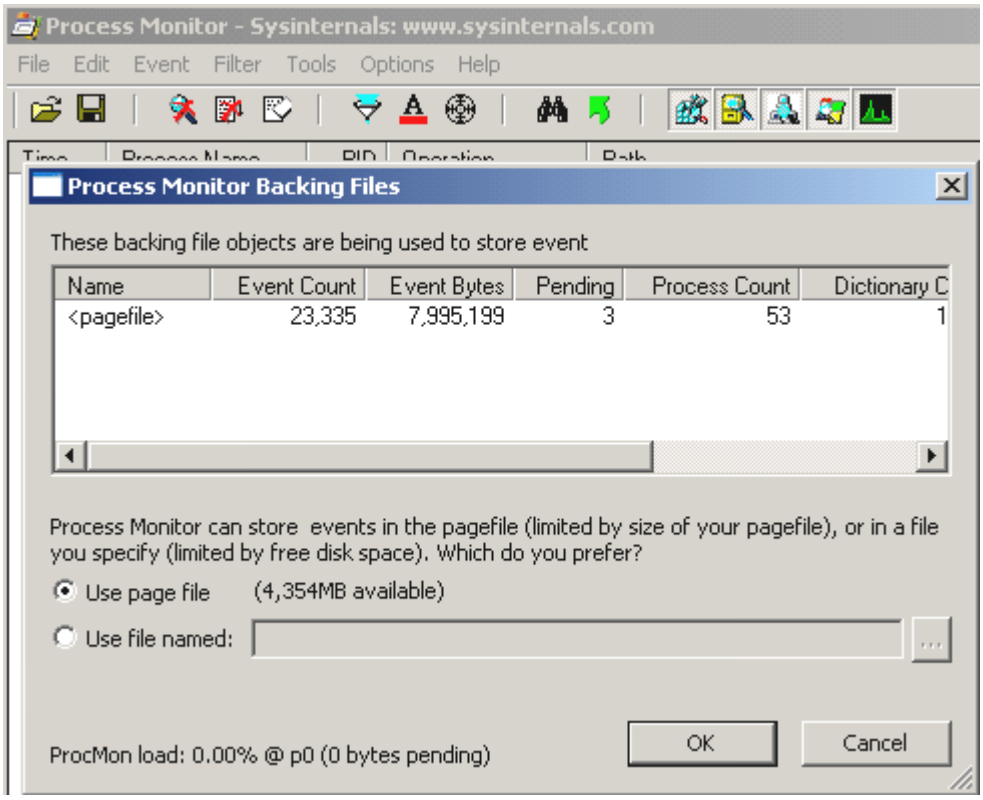


8. Now go into the “File” menu (first from left in the program window)

9. Select “Backing Files” (Shortcut CTRL-B) scrolling down on the menu and click with the left mouse button, or if you use a keyboard scroll down with arrows and press enter

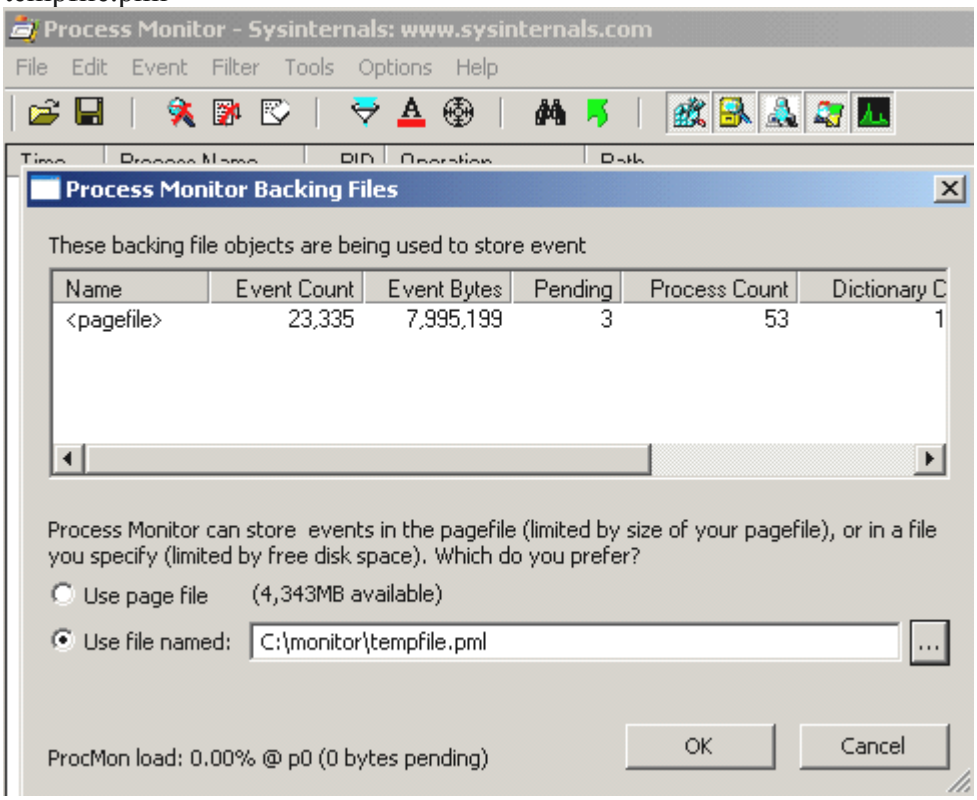


10.This will open the “Process Monitor Backing Files” windo

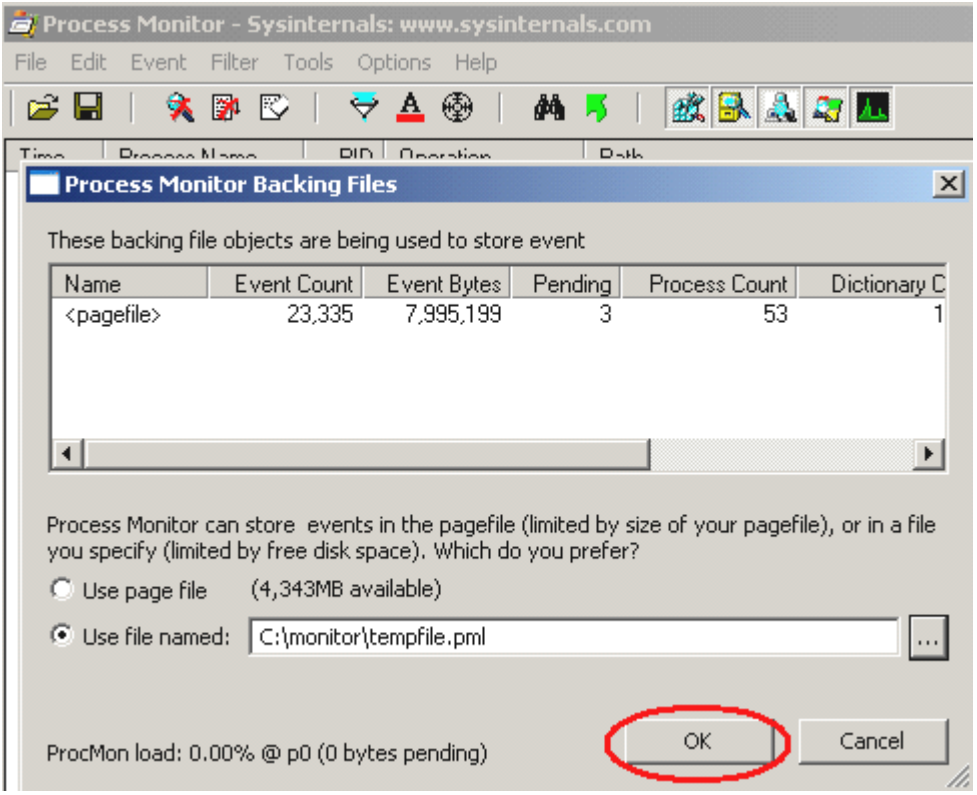


11. Now click on the radial button near “Use file named:” to enable the named field

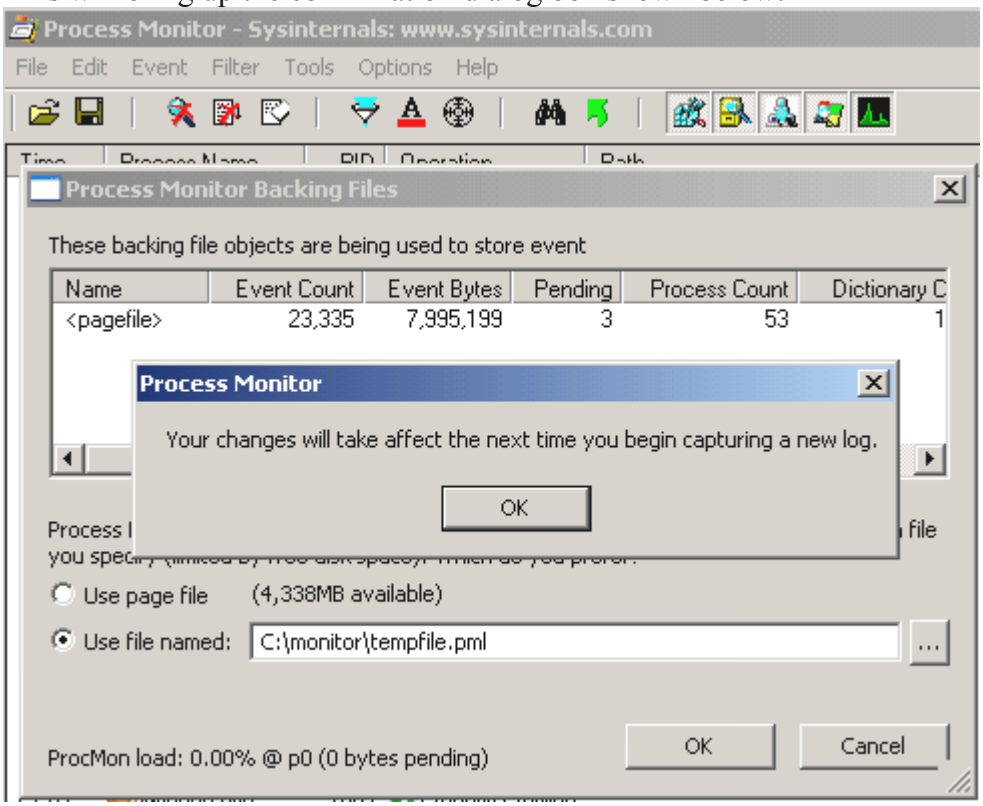
12. Insert in the name field the desired destination folder (here we will use the folder "C:\monitor" that we initially extracted the ProcessMonitor.zip to) and target file name e.g. “C:\monitor\ tempfile.pml”



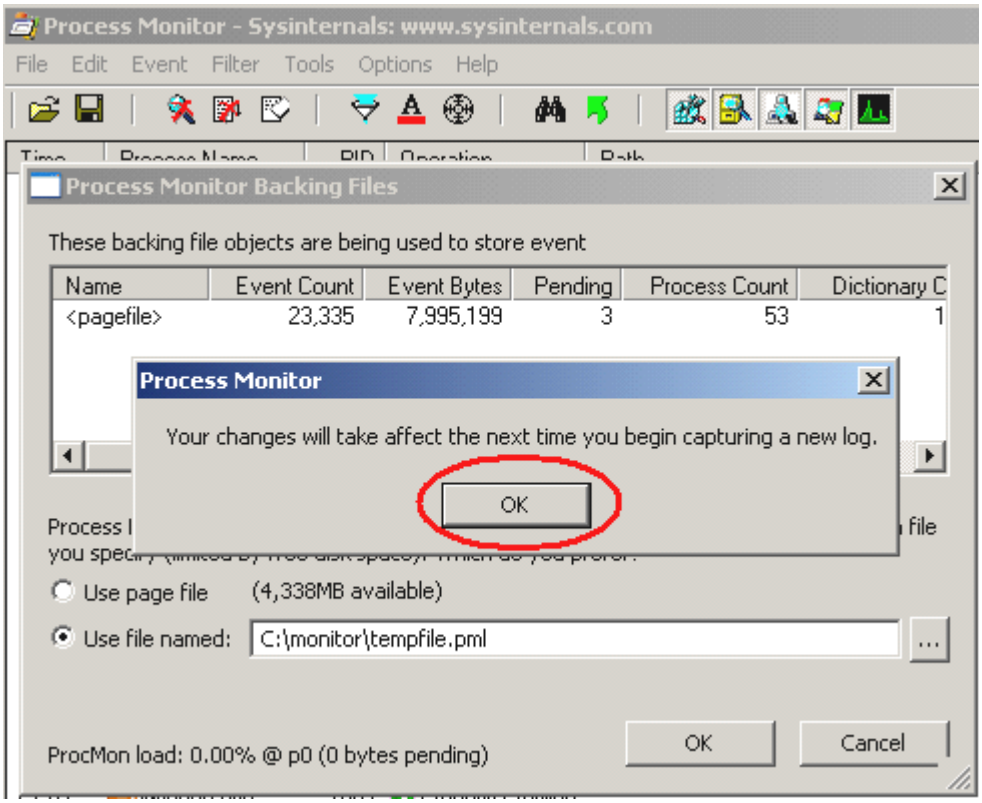
13. Now click on the OK button to confirm



14. This will bring up the confirmation dialog box shown below:



15. Select the “OK” button to continue.

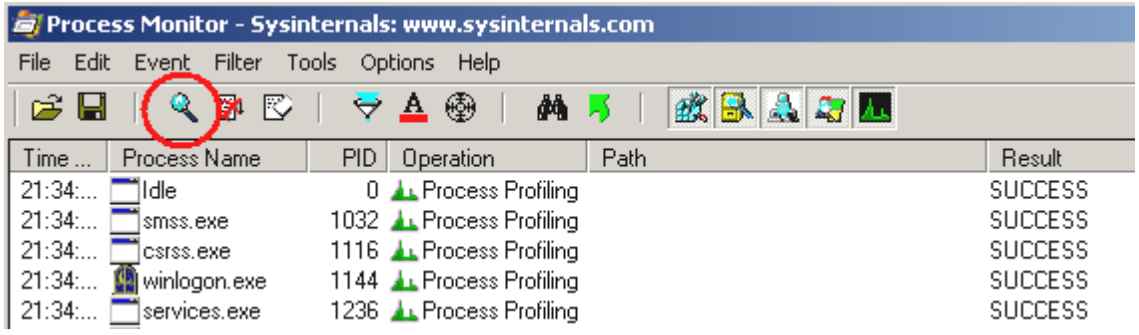


16. As soon as “OK” is selected you will be returned to the main window.

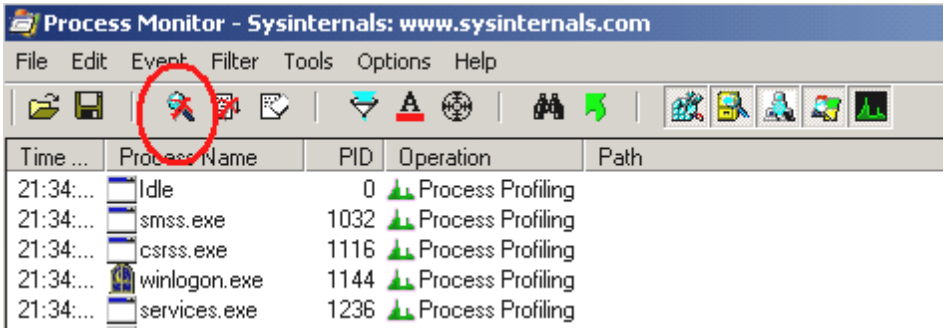
17.Close the program.

18.Double Click on the file “Procmon.exe”.

19.Click on the “Capture” icon to stop the capture process.

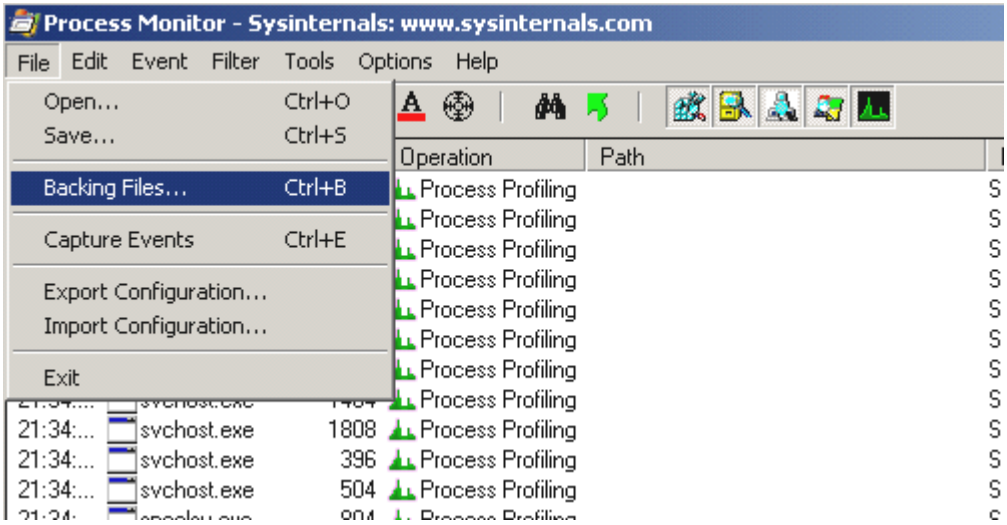


20. The Capture icon will now have a red X over it, meaning that the program is no longer capturing events.



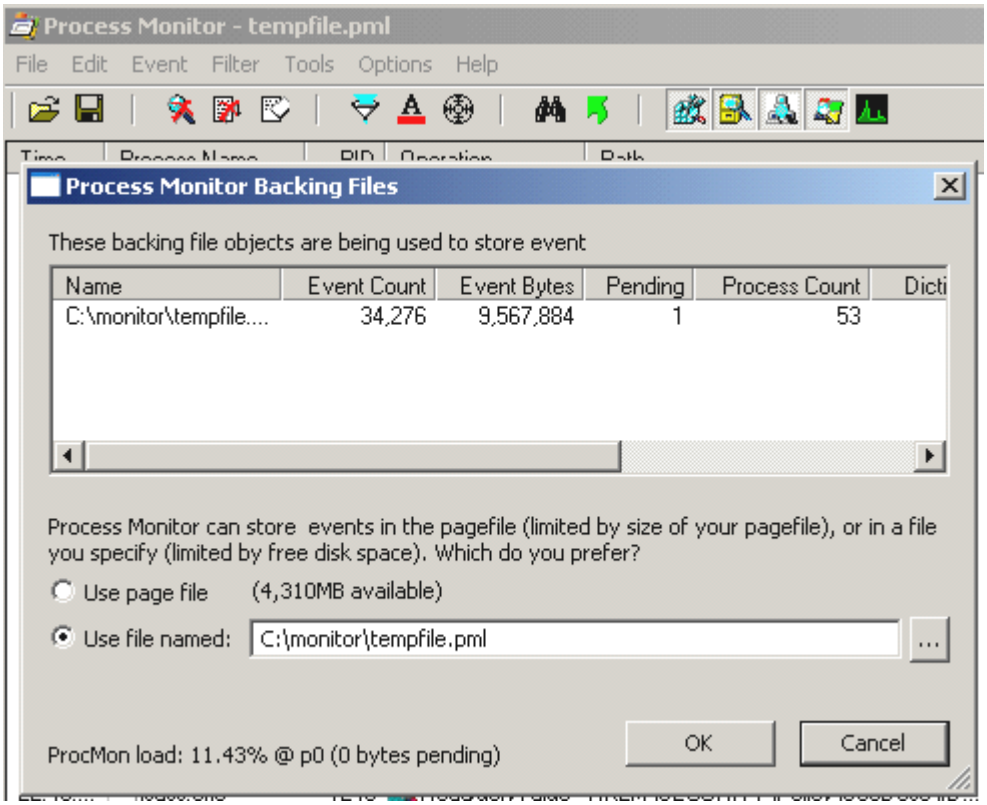
21. Now go into the "File" menu (first from left in the program window)

22. Select "Backing Files" (Shortcut CTRL-B) scrolling down on the menu and click with left mouse button, or if you use a keyboard scroll down with arrows and press enter

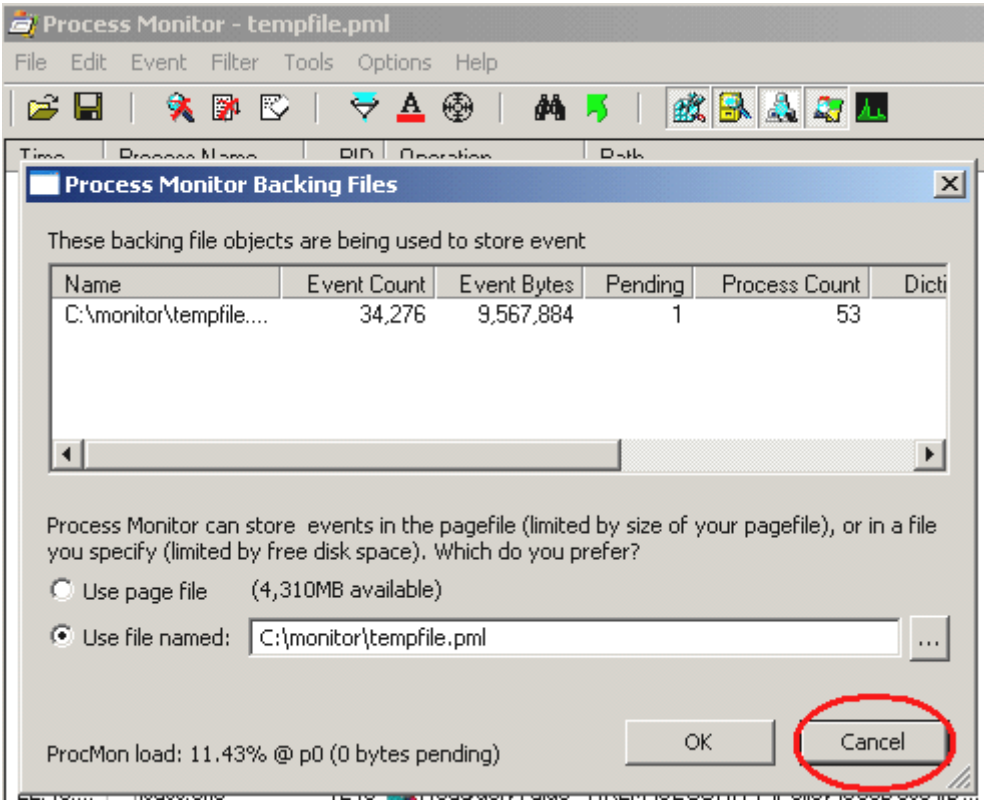


23. Now appears a new windows with title "Process Monitor Backing Files"

24. Verify that ProcMon is using the previously configured named file.



25. Select the “Cancel” button to close the window.



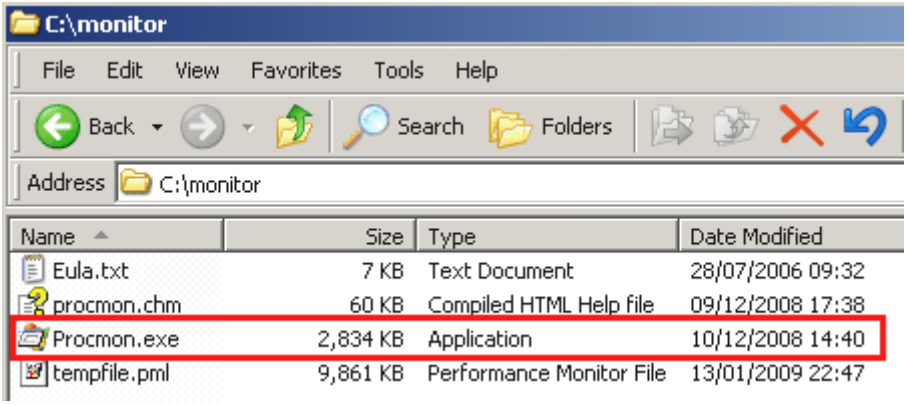
26. Now the program is ready for analysis.

Use —Process Monitor‖ for —Boot Logging‖

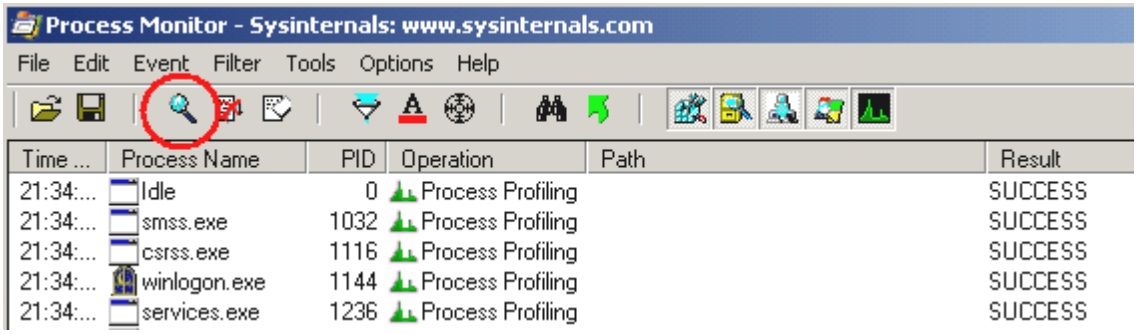
1. Login using an account with administrative privilege (Administrator is recommended)

2. Navigate to the folder that ProcessMonitor.zip was extracted to (e.g. C:\monitor)

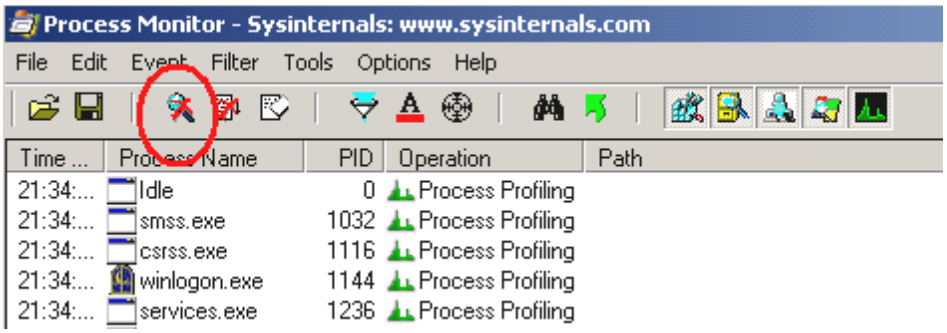
3. Double Click on the file “Procmon.exe”



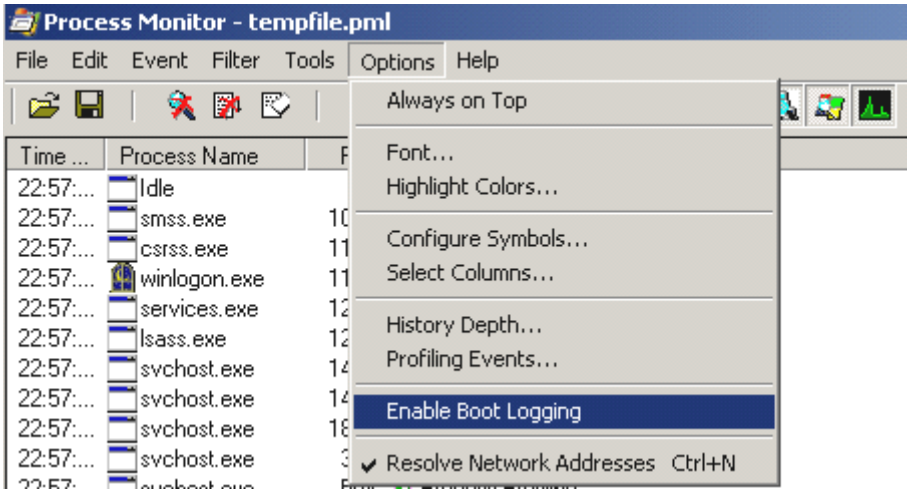
4. Click on the “Capture” icon to stop the capture process.



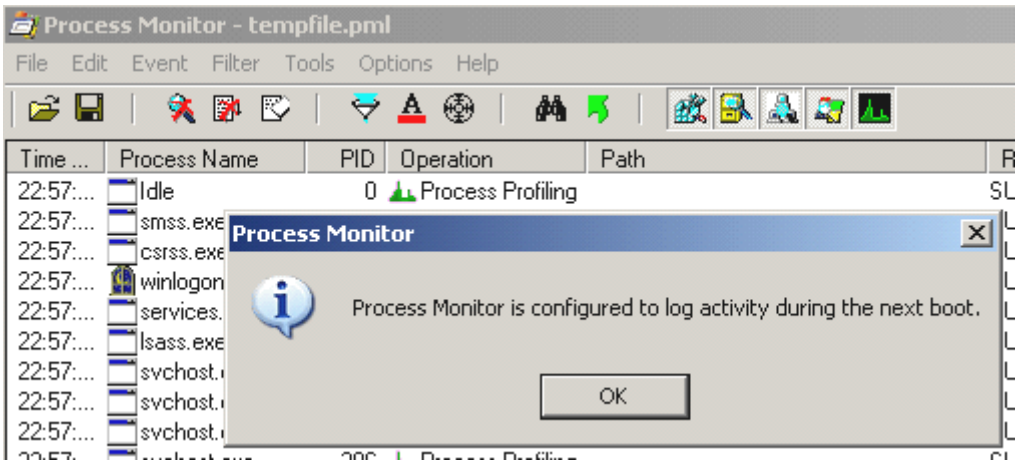
5. The Capture icon will now have a red X over it, meaning that the program is no longer capturing events.



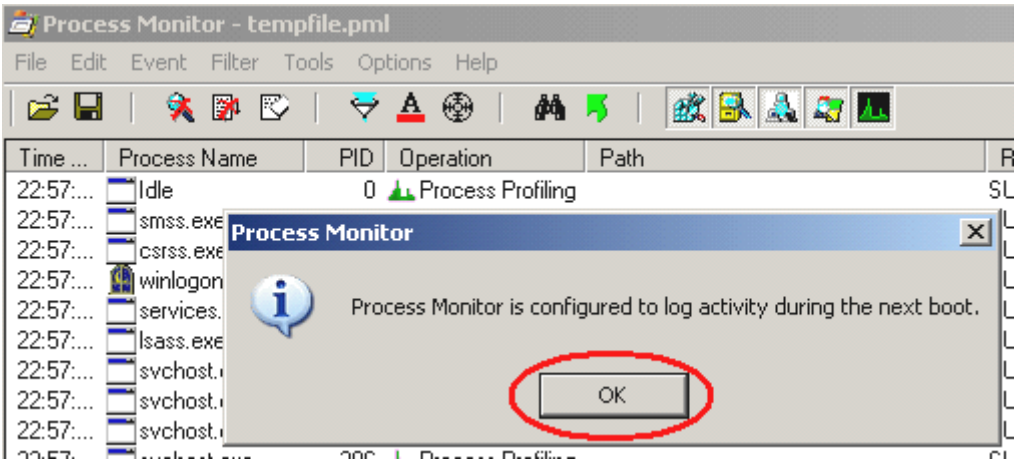
6. Now go into the "Options" menu and select "Enable Boot Logging"



7. The following dialog box will open.



8. “Process monitor” is configured to log activity during the next boot. Select the “OK” button to close the program.



Program 10. Perform File type detection using Autopsy tool

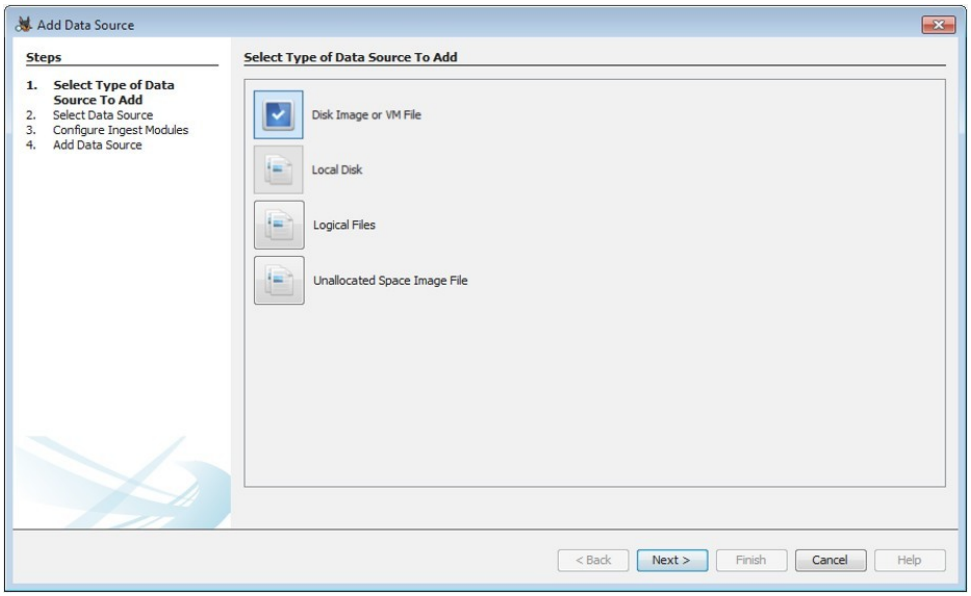
1. Getting Started

Open Autopsy and create a new case.

Click on **Finish** after completing both the steps.

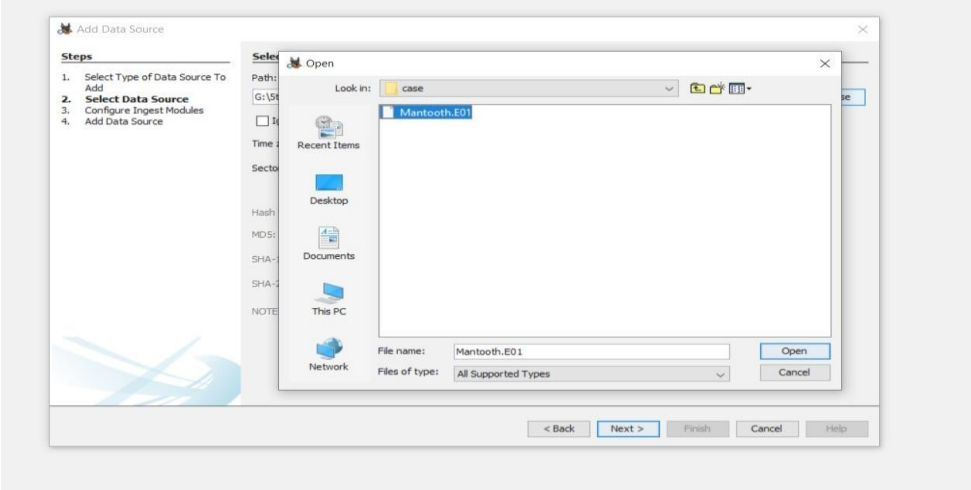
2. Add a data source.

Select the appropriate data source type.

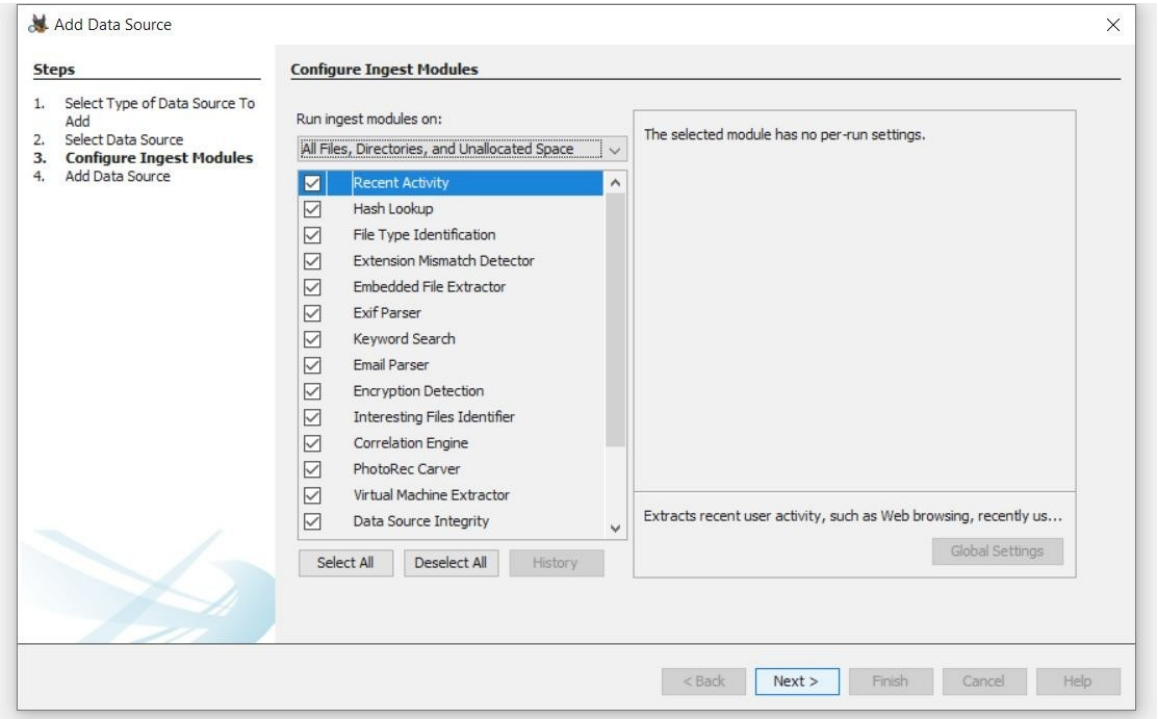


- **Disk Image or VM file:** Includes images that are an exact copy of a hard drive or media card, or a virtual machine image.
- **Local Disk:** Includes Hard disk, Pen drive, memory card, etc.
- **Logical Files.** : Includes local folders or files.
- **Unallocated Space Image File**: Includes files that do not contain a file system but need to run through ingest.

The data source used here is a disk image. Add the data source destination.



Configure ingest modules.

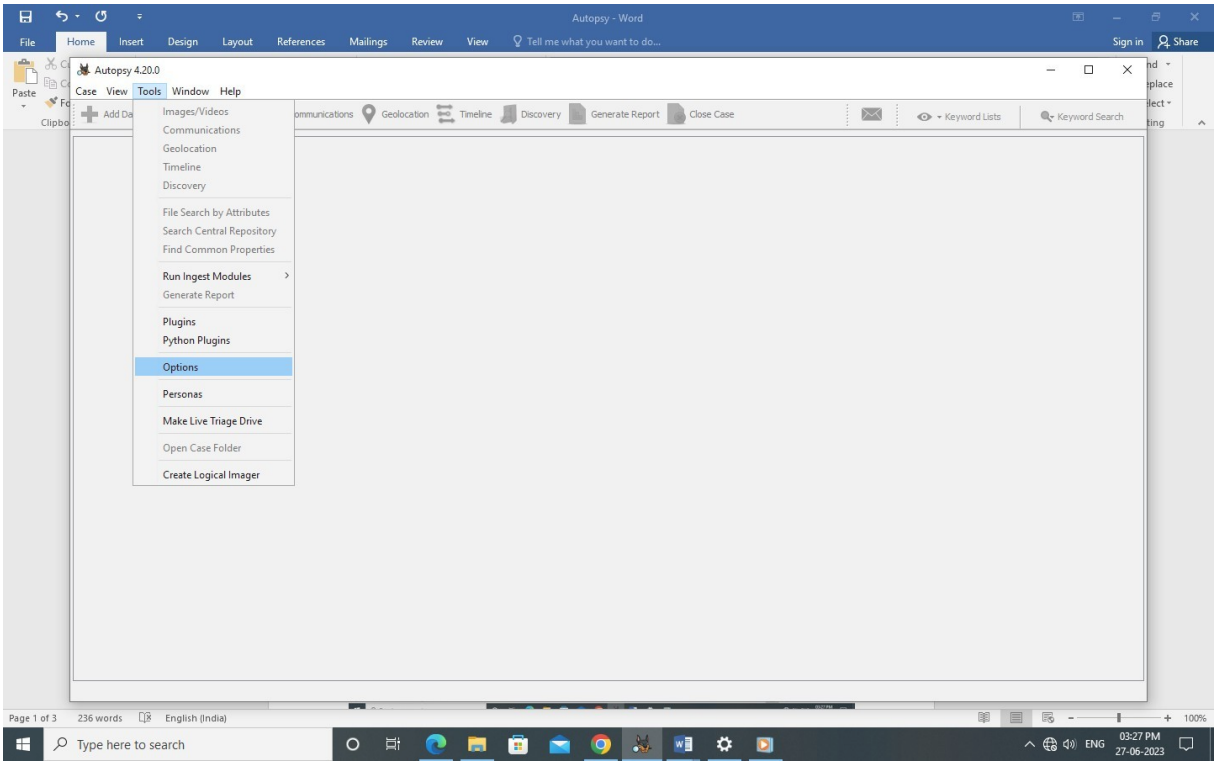


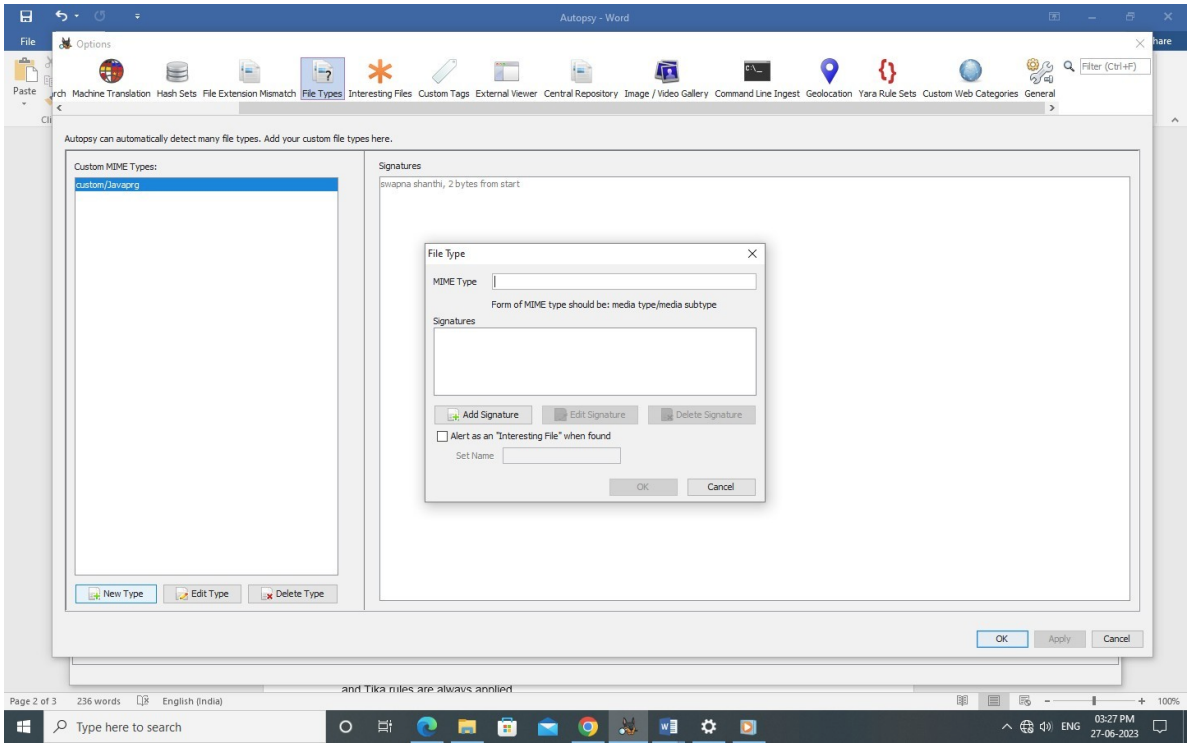
Configuration

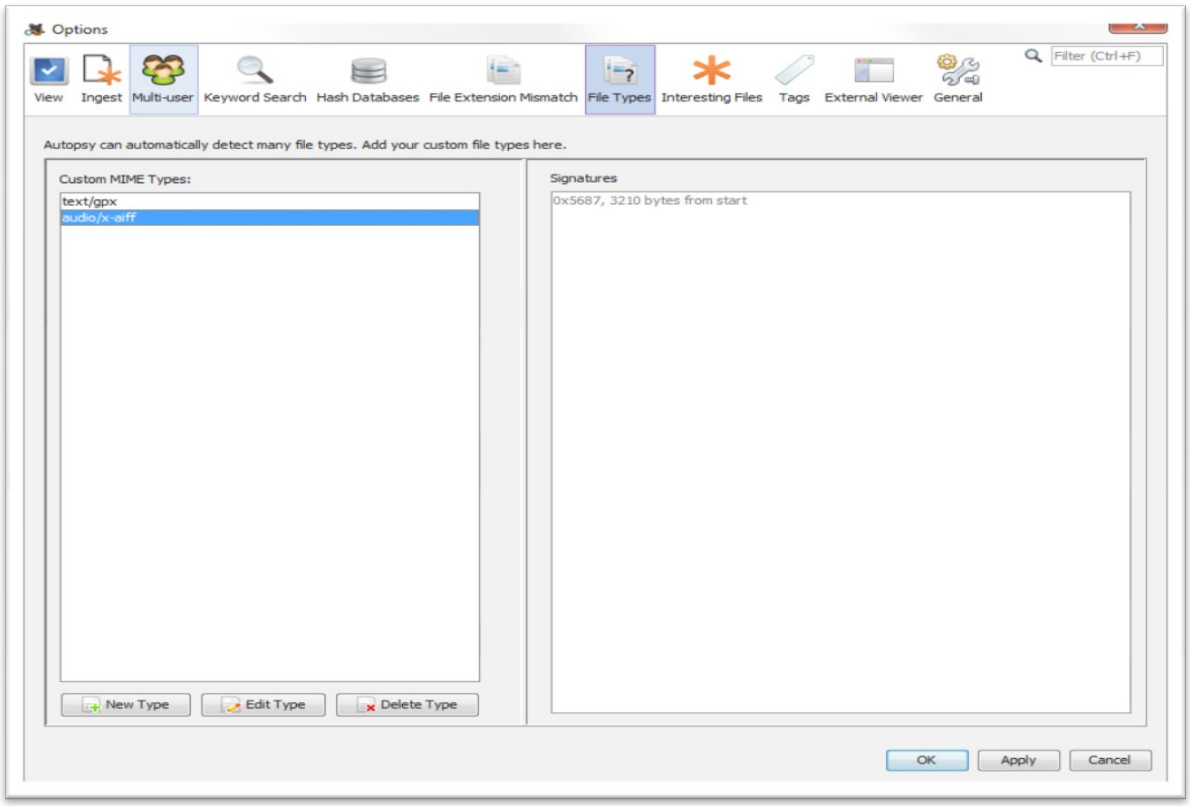
You do not need to configure anything with this module unless you want to define your own types.

To define your own types, go to "Tools", "Options", "File Type Id" panel.

From there, you can define rules based on the offset of the signature and if the signature is a byte sequence of an ASCII string.


Autopsy - Word
Autopsy 4.20.0
Case View Tools Window Help
Images/Videos
Communications
Geolocation
Timeline
Discovery
File Search by Attributes
Search Central Repository
Find Common Properties
Run Ingest Modules
Generate Report
Plugins
Python Plugins
Options
Personas
Make Live Triage Drive
Open Case Folder
Create Logical Imager
Type here to search


Autopsy - Word
Options
Machine Translation
Hash Sets
File Extension Mismatch
File Types
Interesting Files
Custom Tags
External Viewer
Central Repository
Image / Video Gallery
Command Line Ingest
Geolocation
Yara Rule Sets
Custom Web Categories
General
Autopsy can automatically detect many file types. Add your custom file types here.
Custom MIME Types:
custom/Javaprg
Signatures
swapna shanthi, 2 bytes from start
File Type
MIME Type
Form of MIME type should be: media type/media subtype
Signatures
Add Signature
Edit Signature
Delete Signature
Alert as an "Interesting File" when found
Set Name
OK
Cancel
New Type
Edit Type
Delete Type
OK
Apply
Cancel
Type here to search



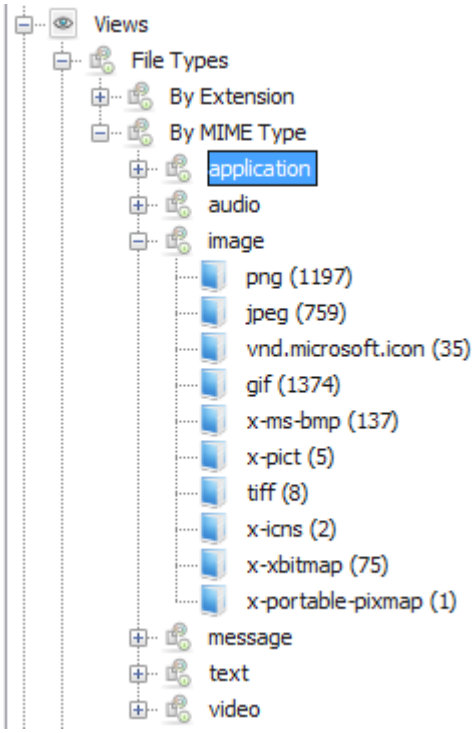
Using the Module

Ingest Settings

There are no run-time settings for this module when you run it on a data source. All user-defined and Tika rules are always applied.

Seeing Results

The results can be seen in the views area of the tree, under Views->File Types->By MIME Type.



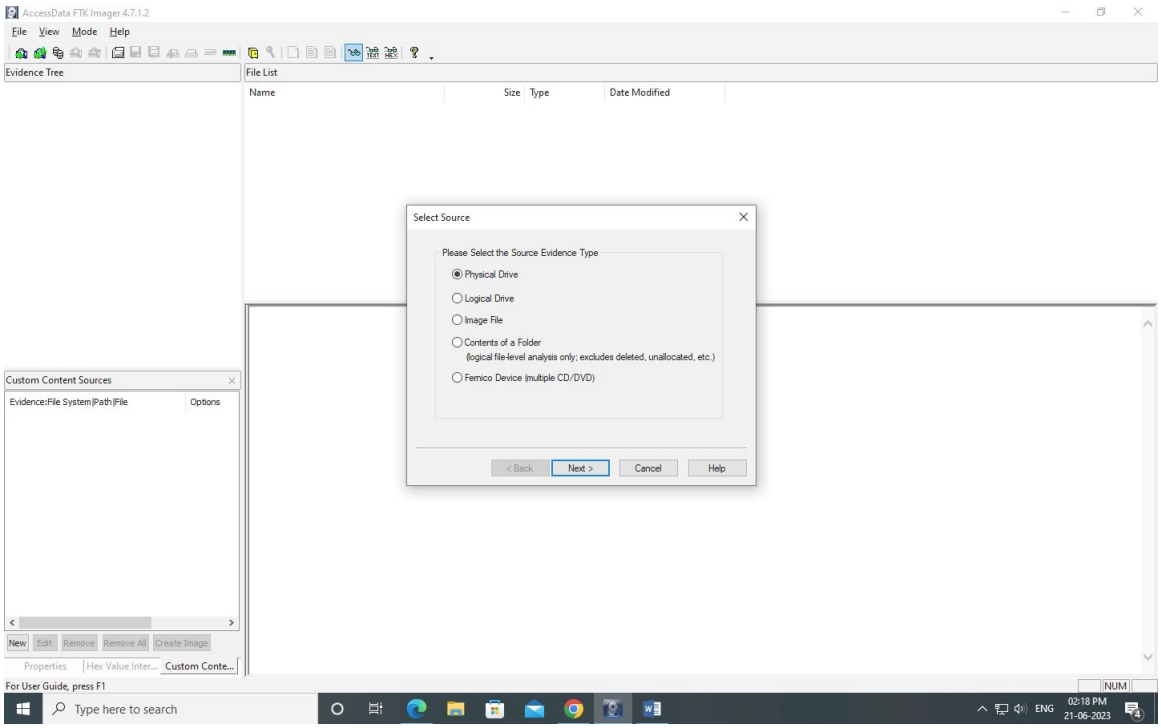
Note that only user-defined MIME types of the form (media type) / (media subtype) will be displayed in the tree.

To see the file type of an individual file, view the "Results" tab in the lower right when you navigate to the file. You should see a page in there that mentions the file type.

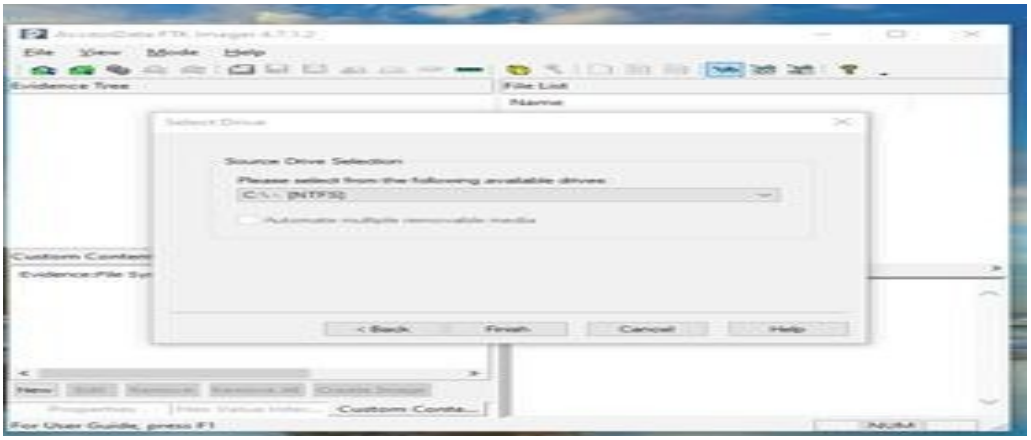
Program 11. Perform Memory capture and analysis using FTK imager tool

- FTK Forensic Toolkit) Imager allows you to perform memory capture or registry capture on a live device, to recover passwords or other data stored in memory on the active device.
- This tool saves an image of a hard disk in one file or in segments that may be later on reconstructed.
- It calculates MD5 and SHA1 hash values and can verify the integrity of the data imaged is consistent with the created forensic image
- The forensic image can be saved in several formats, including DD/raw, E01, and AD1

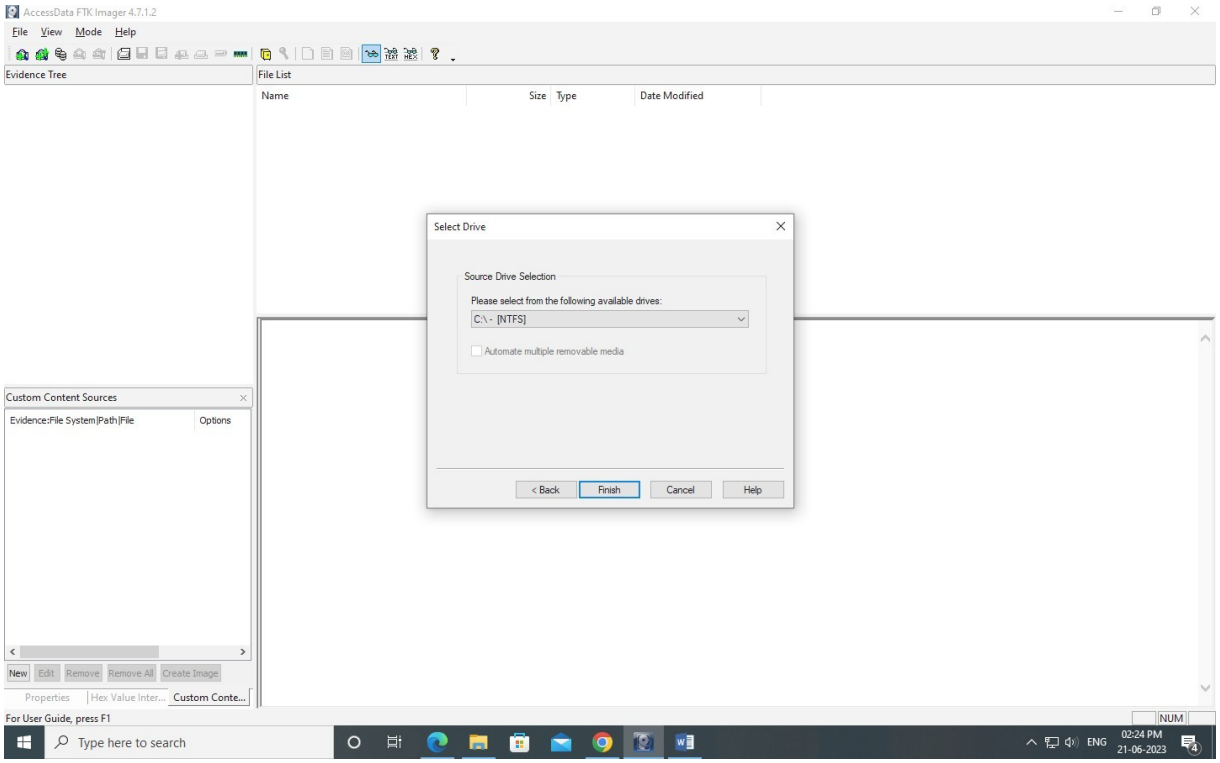
Step 1: Download FTK imager
Step 2: Open file and select create disk



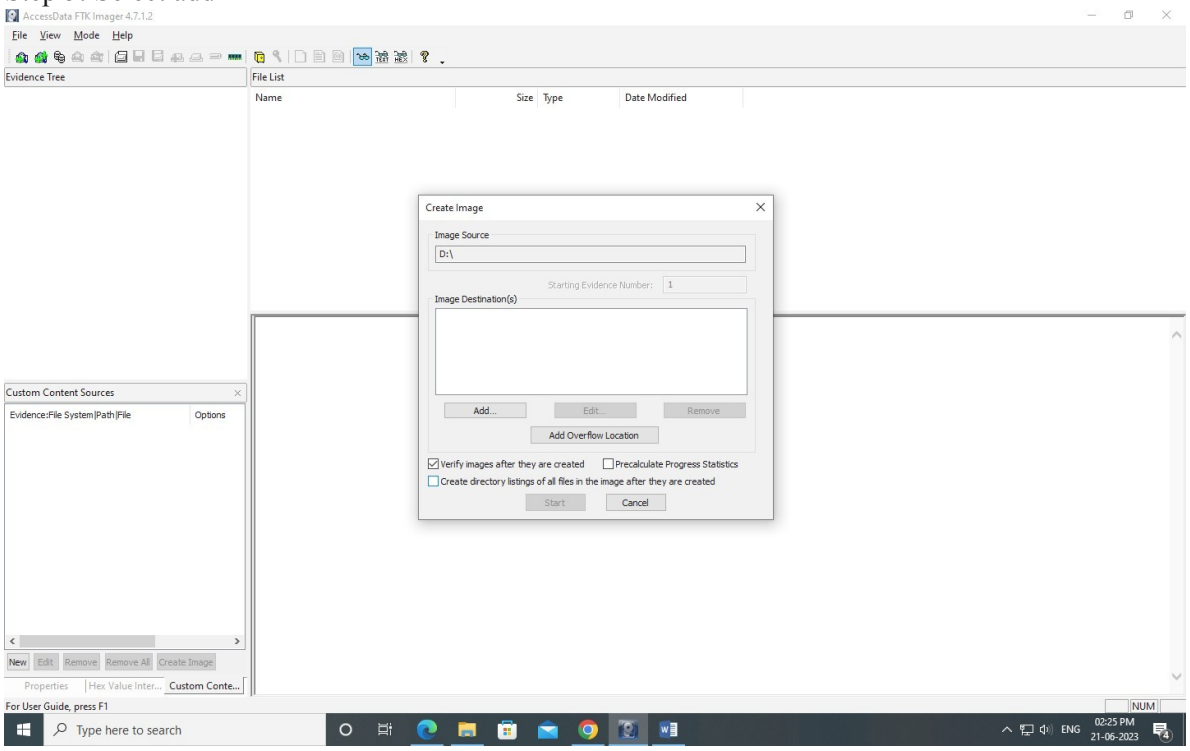
Step 3: Select Logical drive (to make an image of existing drives in the computer). Select the drive to create image of that drive



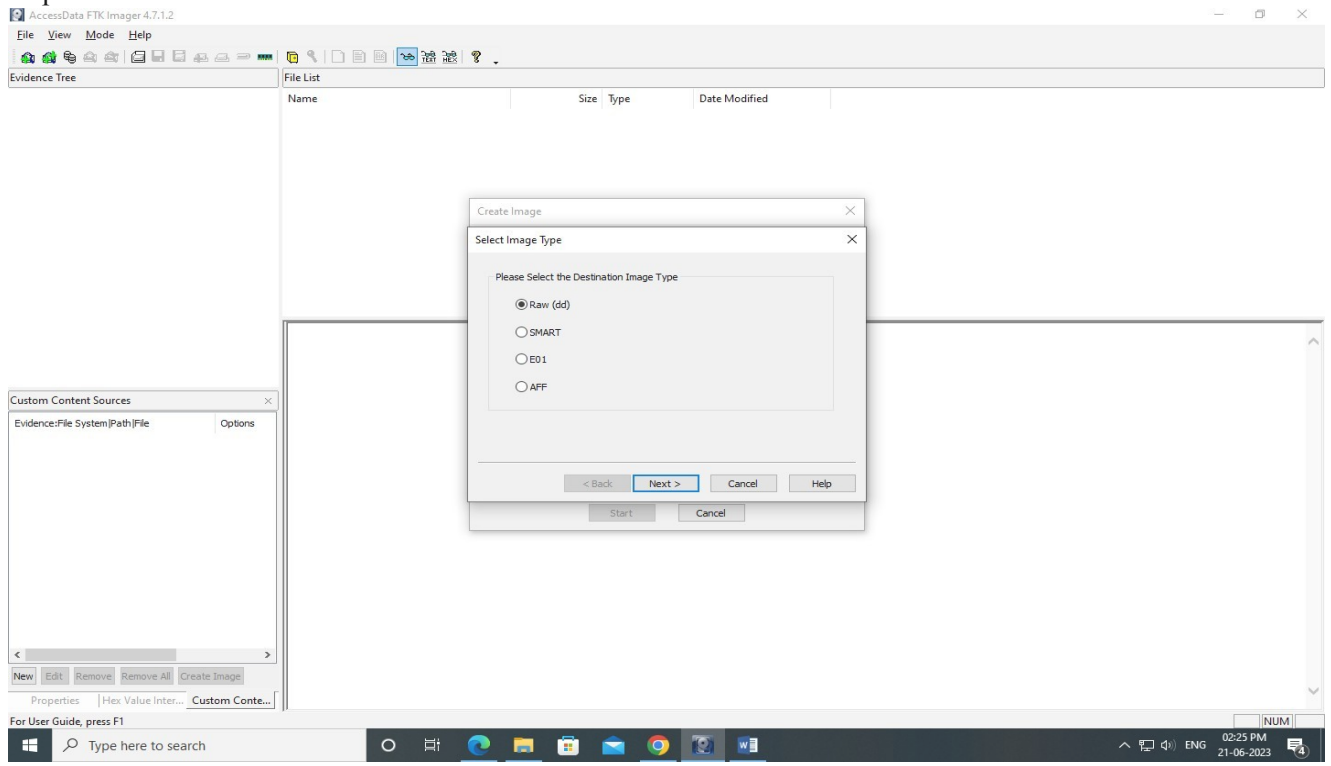
Step 4:Select Finish



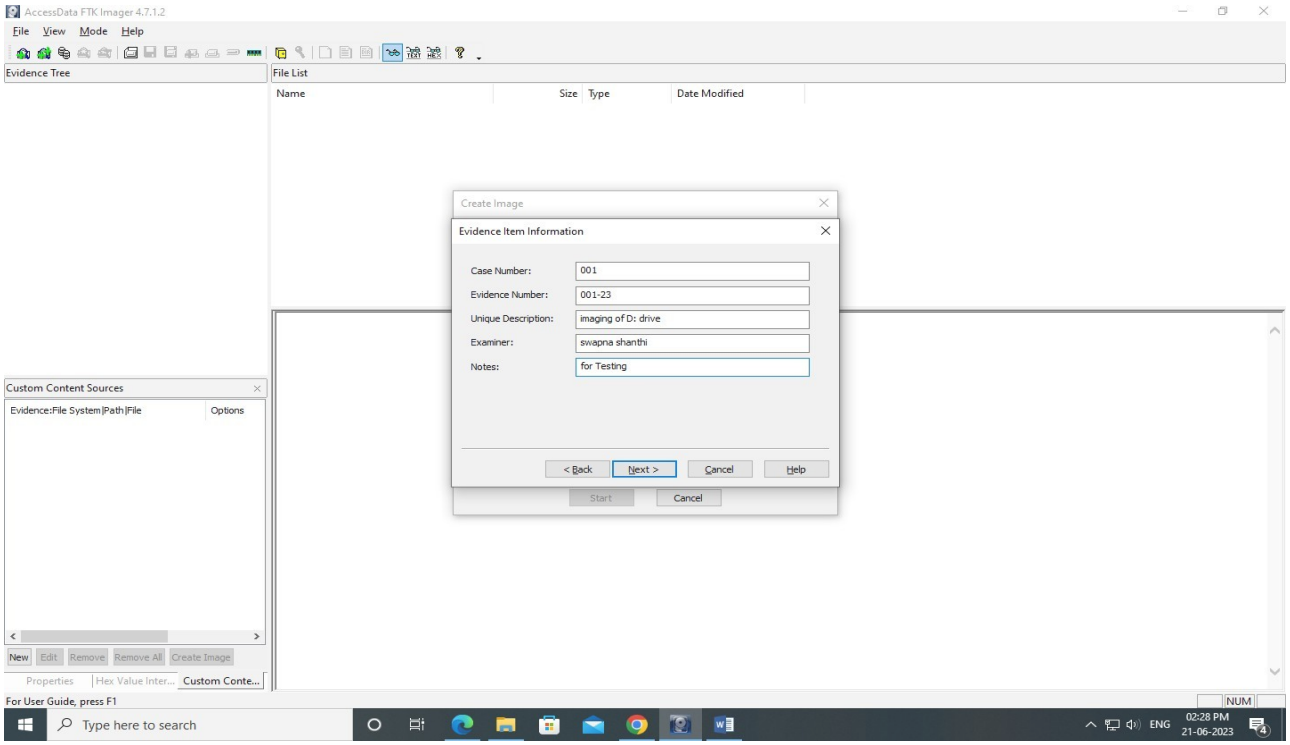
Step 5: Select add

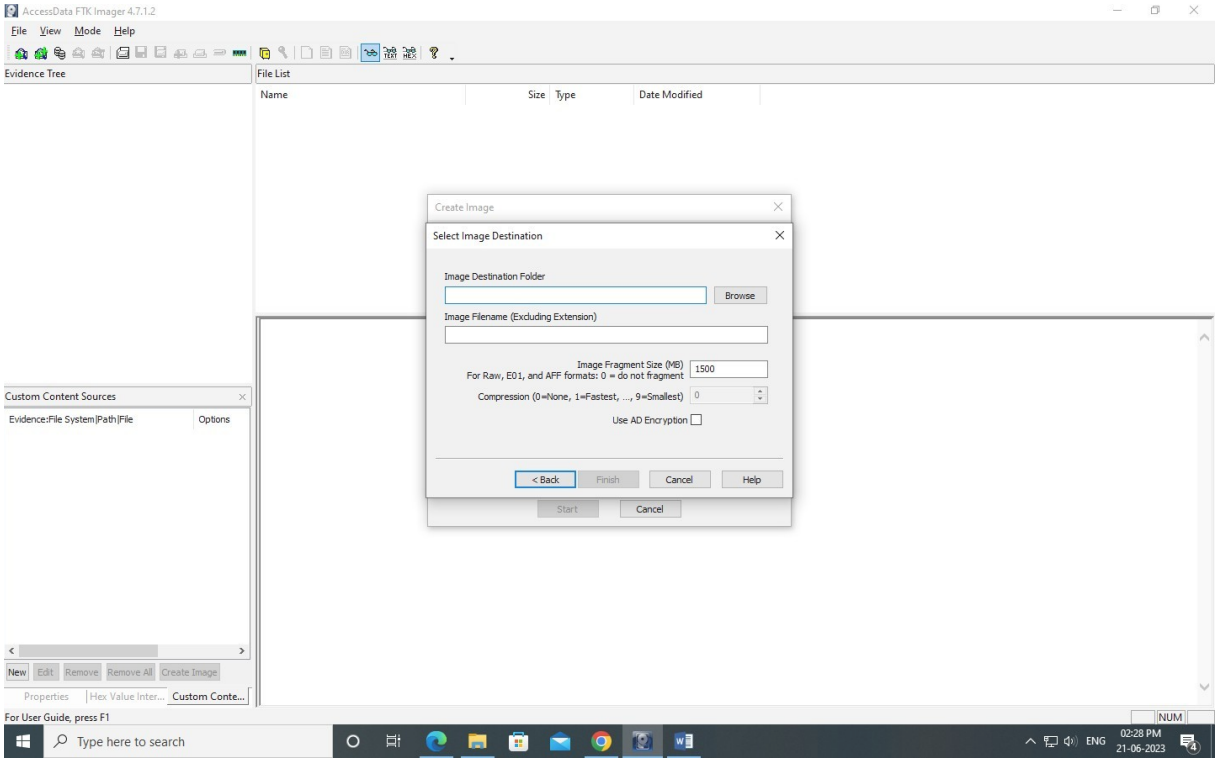


Step 6: Select Raw

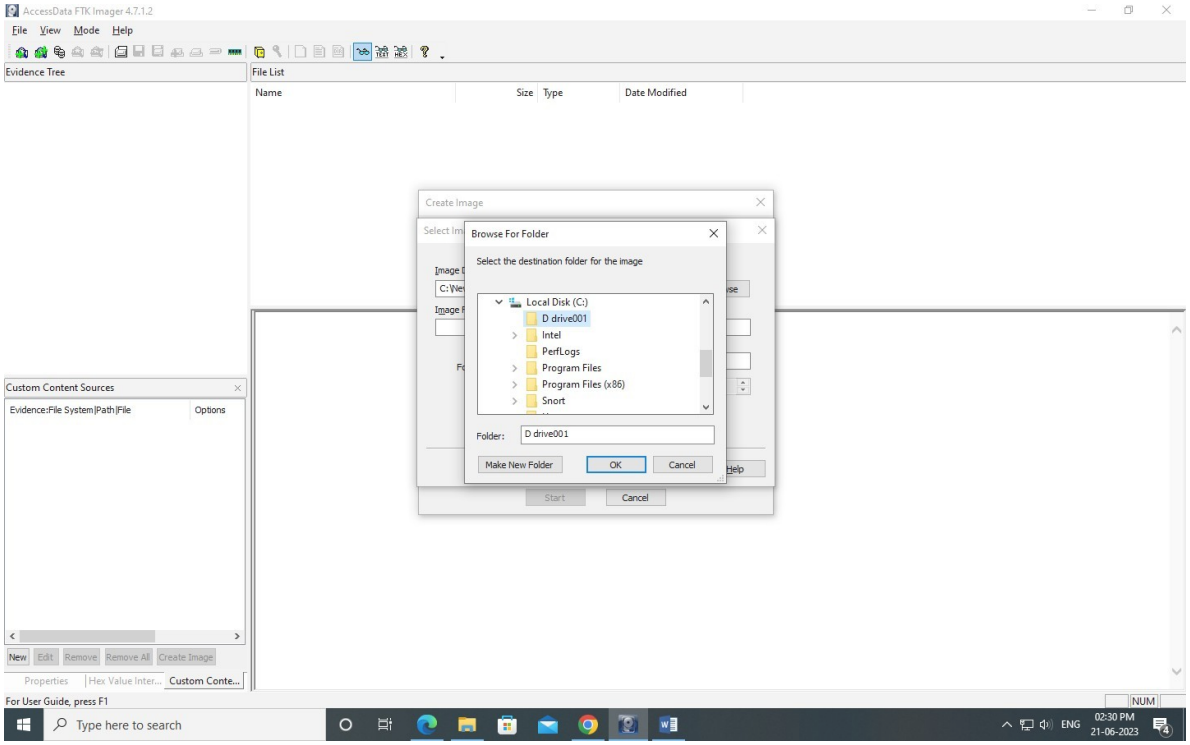


Step 7: Enter details

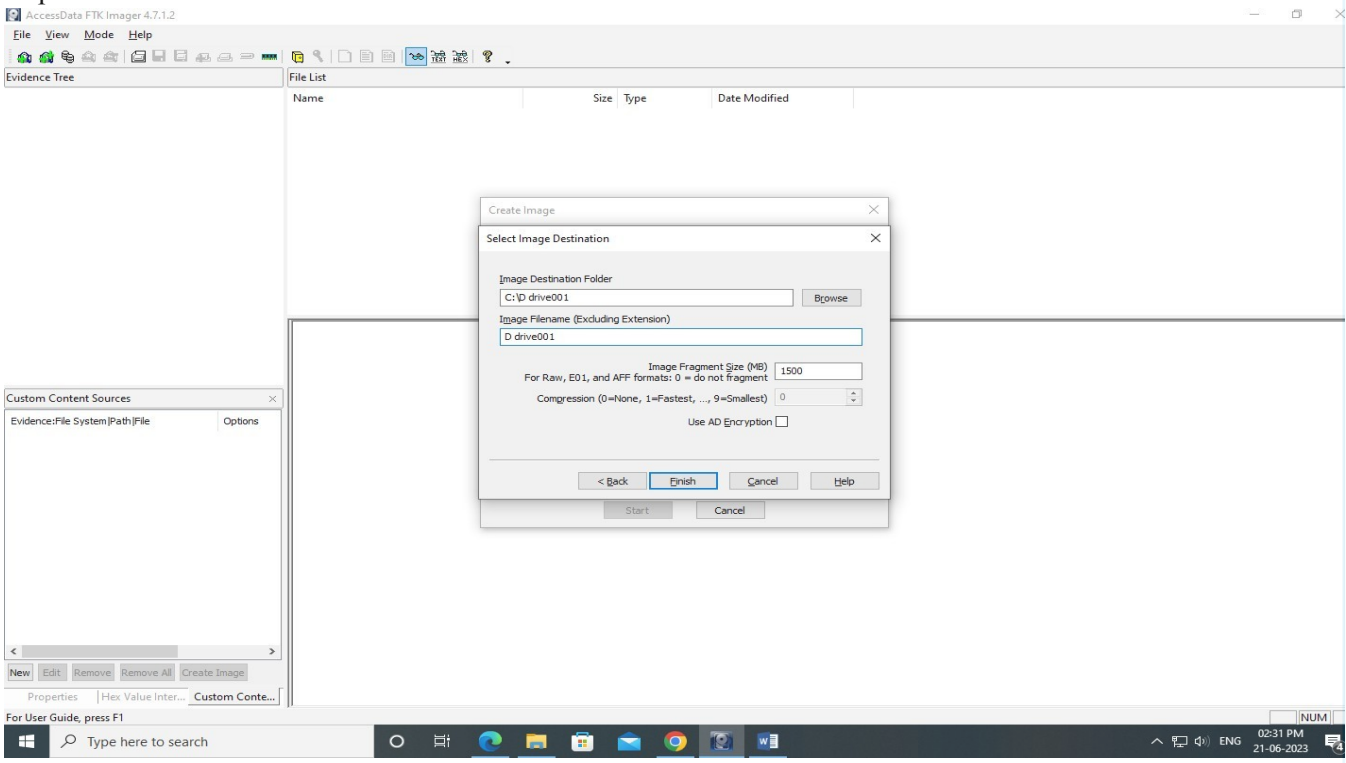




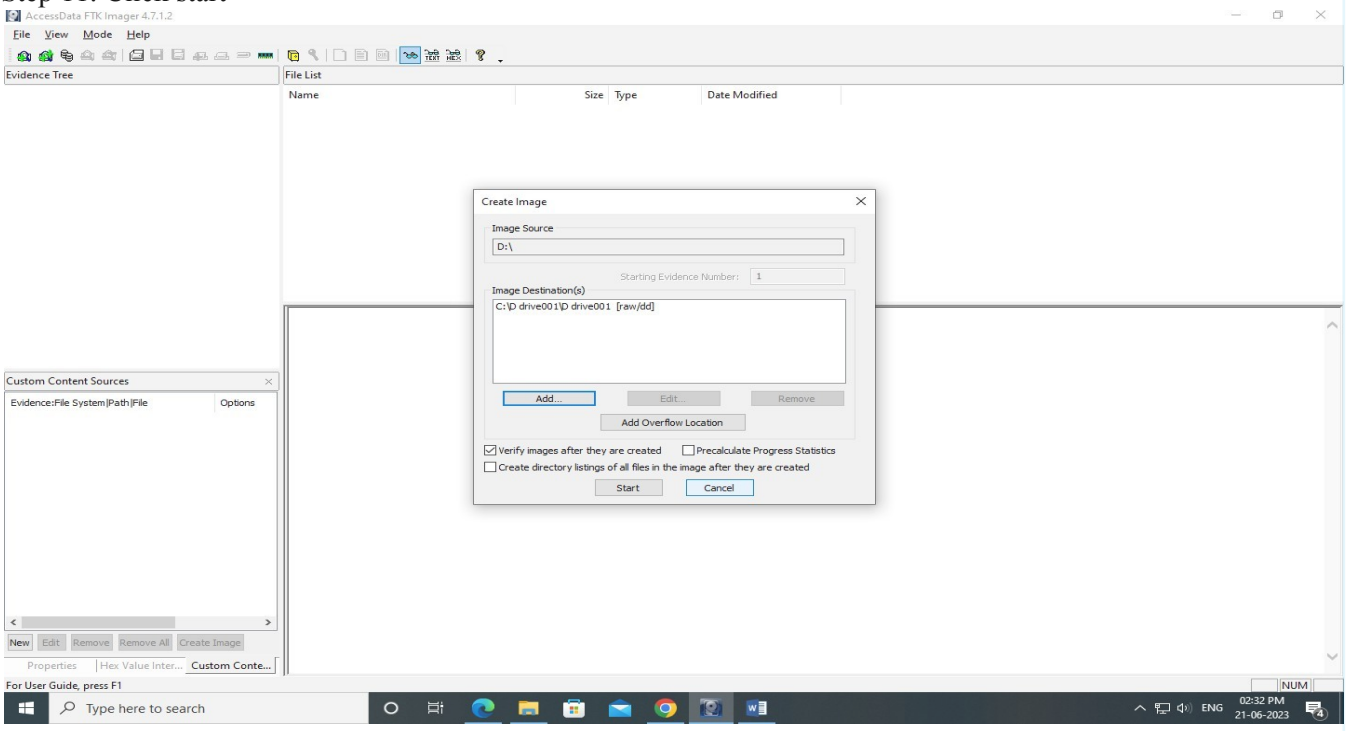
Step 9: Select destination where image should be created

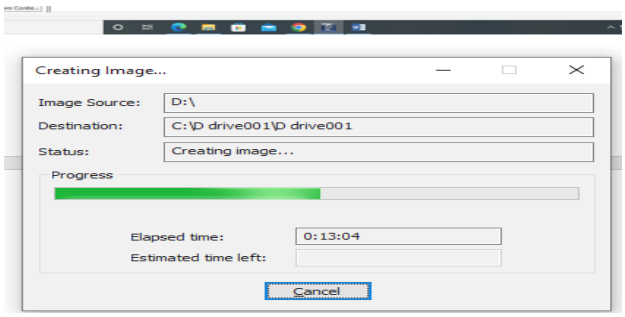


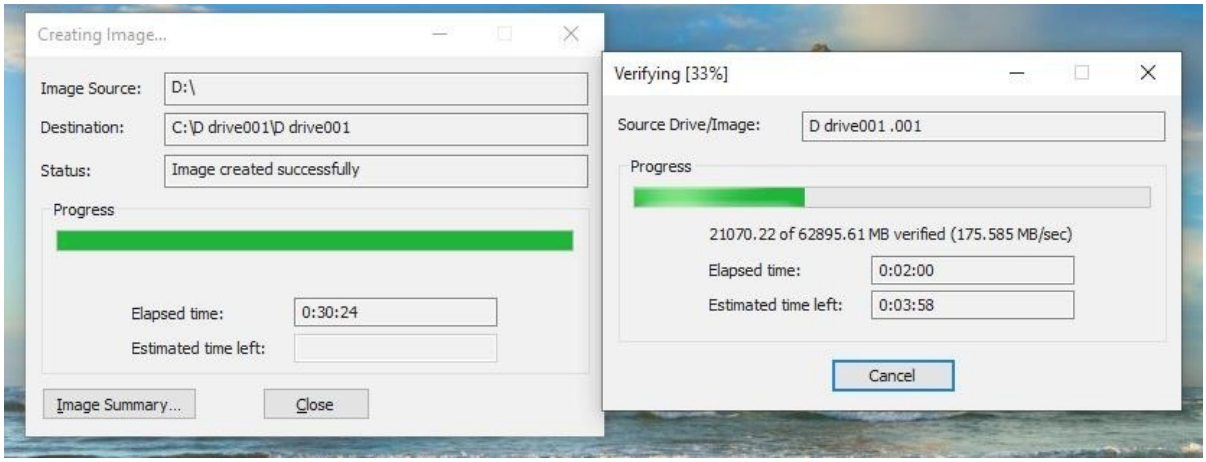
Step 10: Click finish



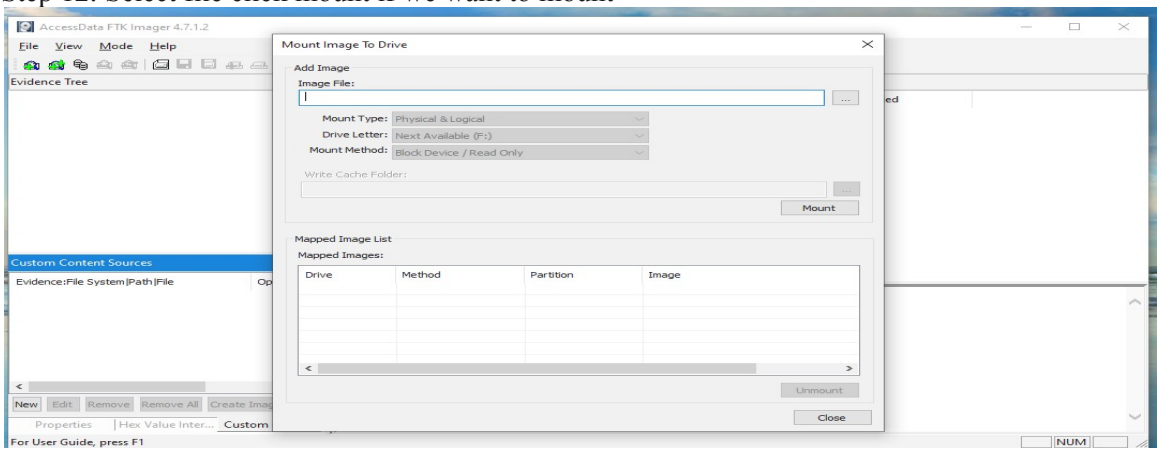
Step 11: Click start



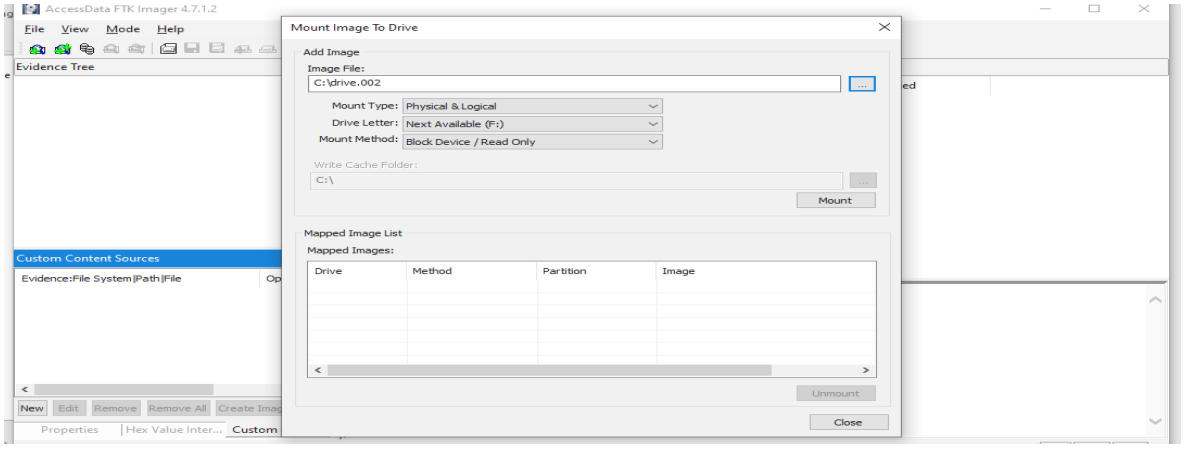




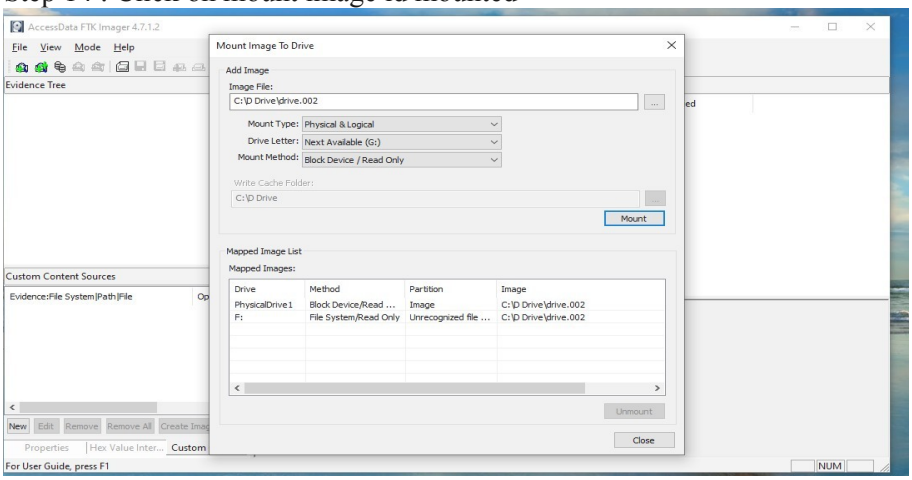
Step 12: Select file click mount if we want to mount

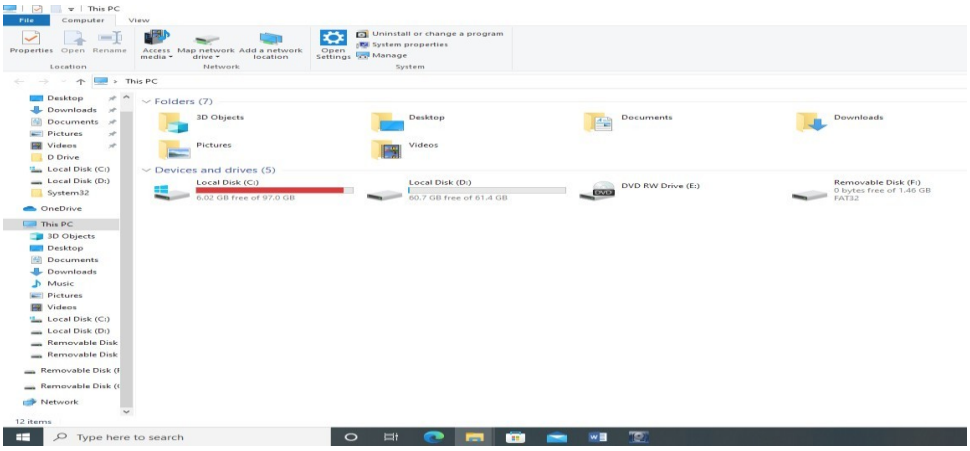


Step 13: Click browse select image (second file) that need to be mounted



Step 14 : Click on mount image id mounted

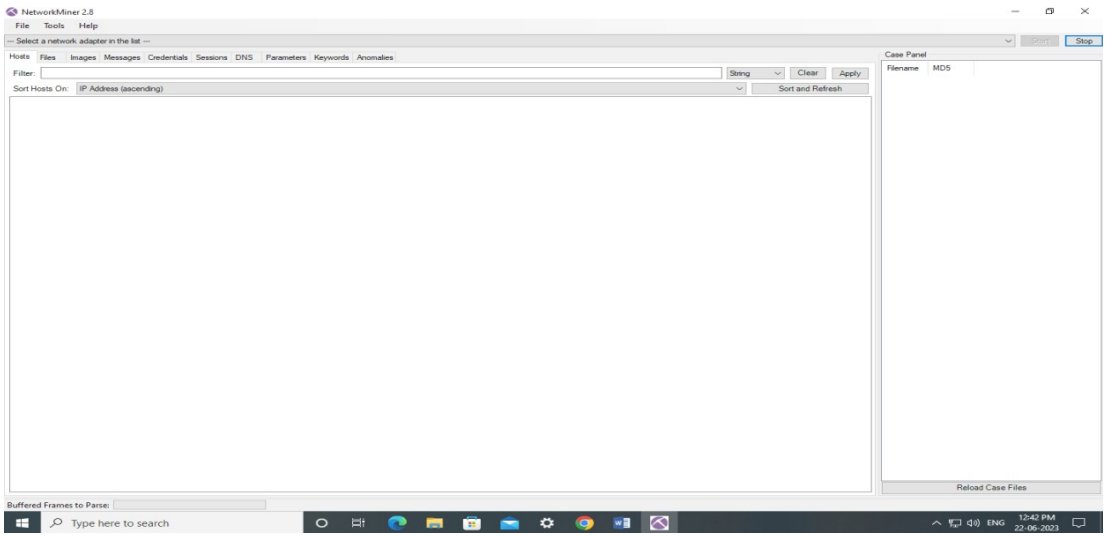




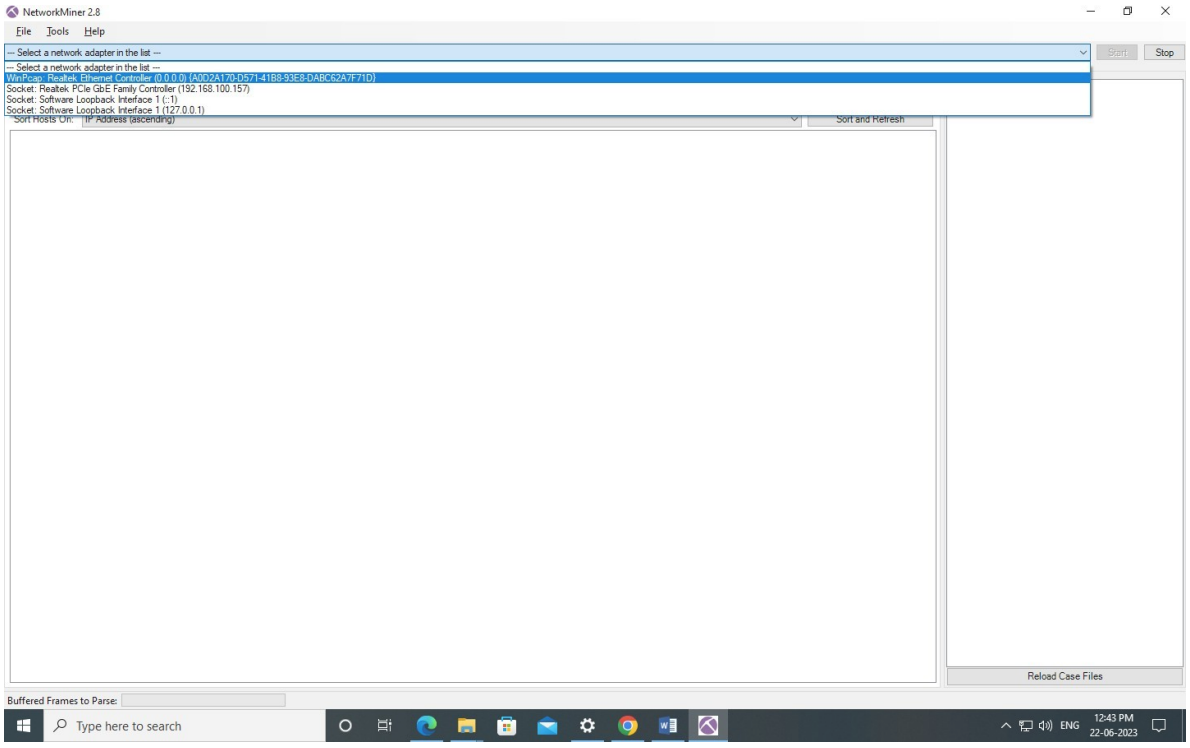
Program 12. Perform Network analysis using the Network Miner too

- Network Miner is an open source network forensics tool that extracts artifacts, such as files, images, emails and passwords, from captured network traffic in PCAP files.
- Network Miner can also be used to capture live network traffic by sniffing a network interface.
- Detailed information about each IP address in the analyzed network traffic is aggregated to a network host inventory, which can be used for passive asset discovery as well as to get an overview of which devices that are communicating.

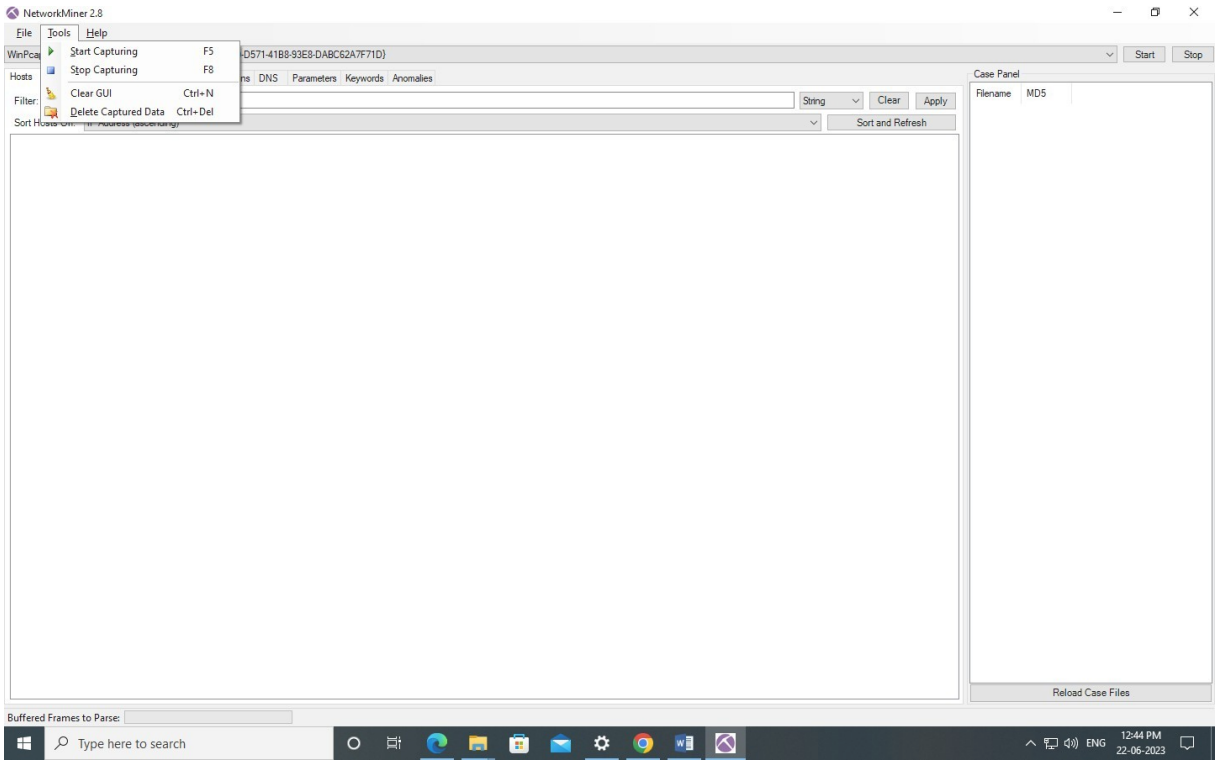
1. Open network miner tool to perform network anlaysis



2. Select WinCap : Realteck Ethernet controller



3. Click tool option and select start capturing



4, List is displayed