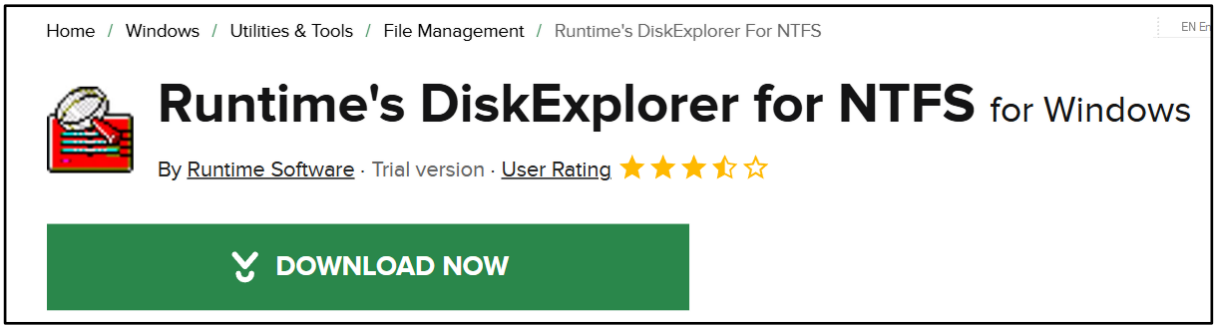
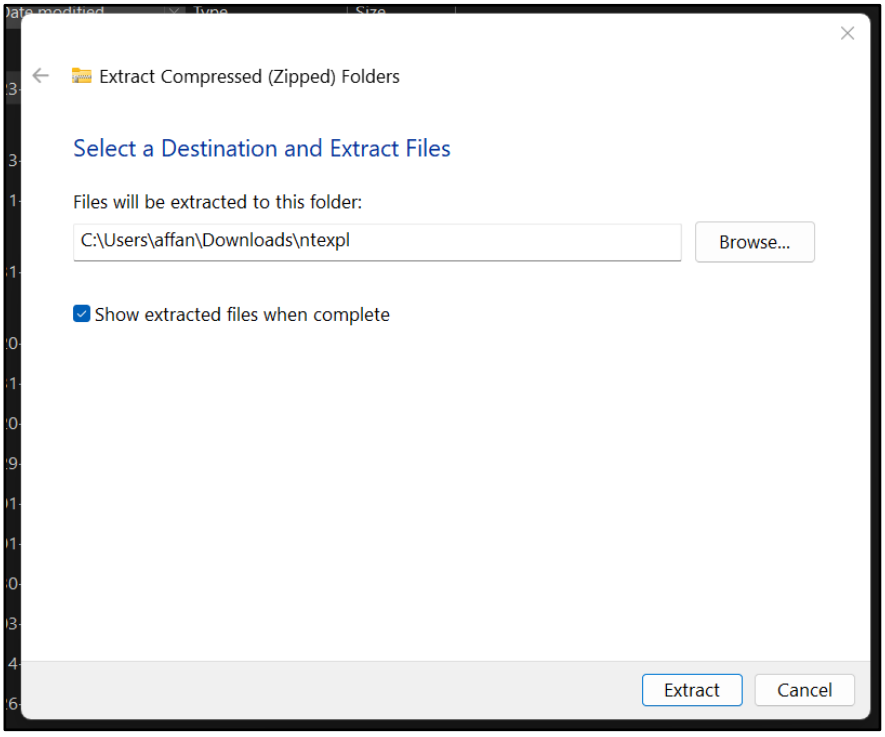
# DATA ACQUISITION AND DUPLICATION

## a) Investigating NTFS Drive Using DiskExplorer for NTFS.

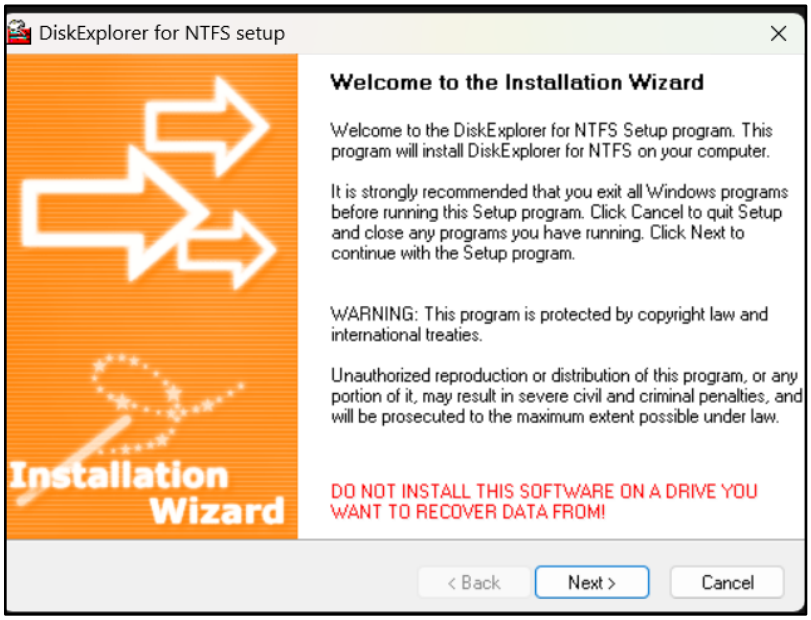
**Go to Google → Download RUN TIME DISK EXPLORER FOR NTFS**

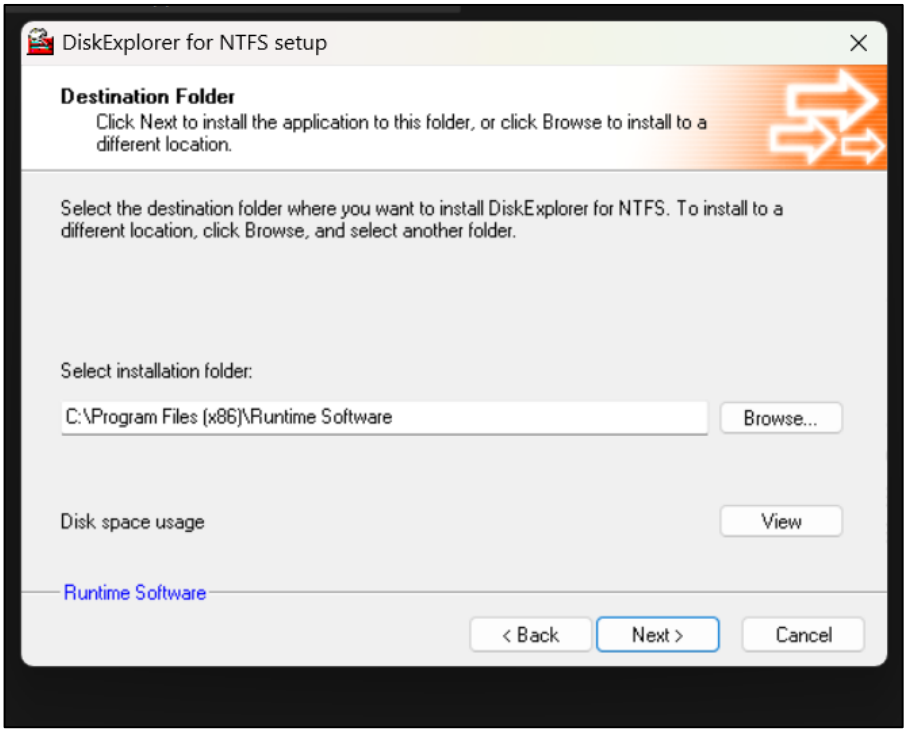


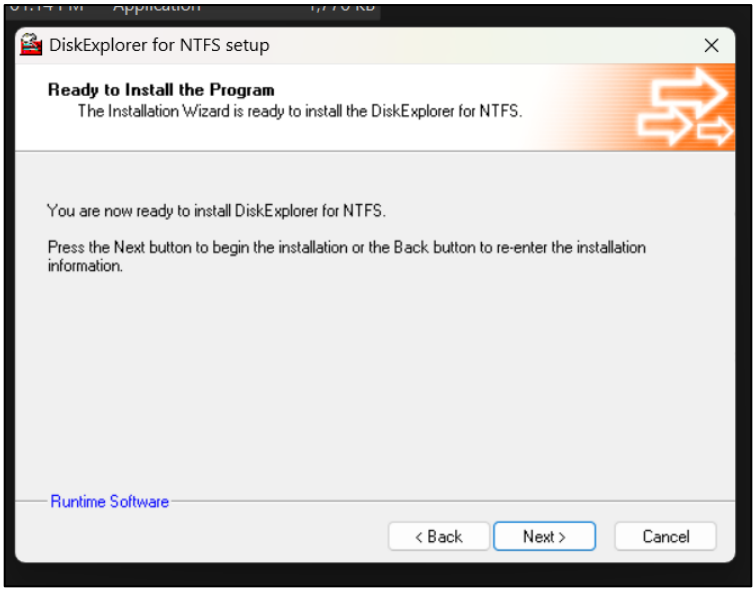

**→ Install the Applicaion → Extract file**

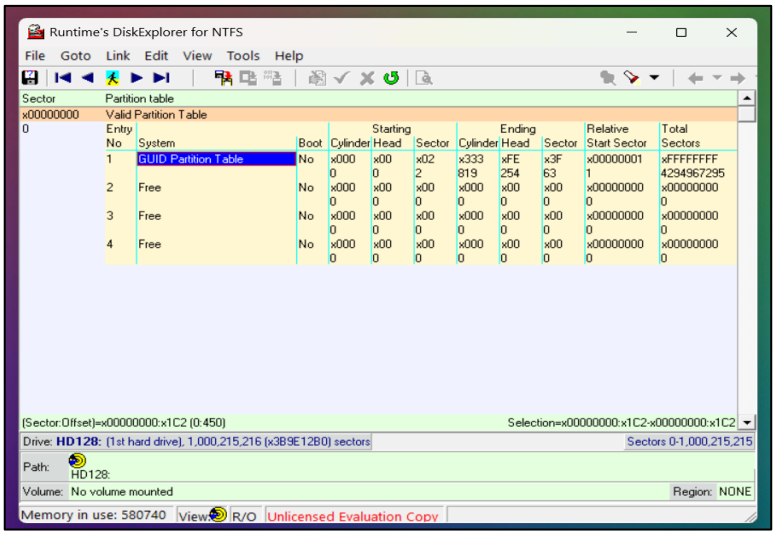



**Next → Next→ Next→Finished**.

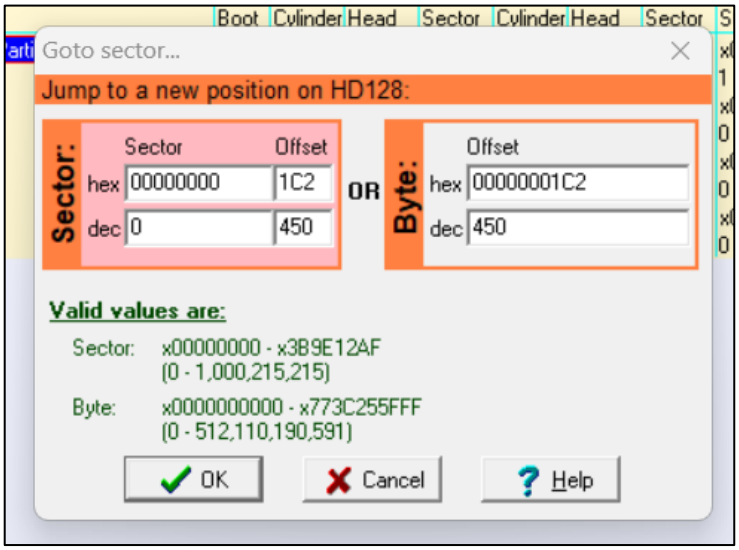

DiskExplorer for NTFS setup
Welcome to the Installation Wizard
Welcome to the DiskExplorer for NTFS Setup program. This program will install DiskExplorer for NTFS on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program. Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
DO NOT INSTALL THIS SOFTWARE ON A DRIVE YOU WANT TO RECOVER DATA FROM!
Installation Wizard
< Back
Next >
Cancel


DiskExplorer for NTFS setup
Destination Folder
Click Next to install the application to this folder, or click Browse to install to a different location.
Select the destination folder where you want to install DiskExplorer for NTFS. To install to a different location, click Browse, and select another folder.
Select installation folder:
C:\Program Files (x86)\Runtime Software
Browse...
Disk space usage
View
Runtime Software
< Back
Next >
Cancel

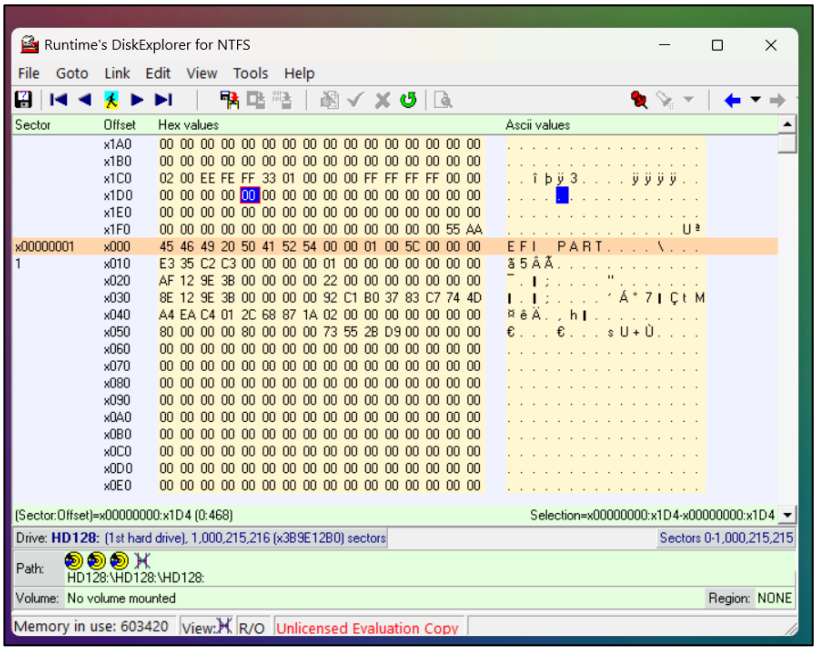


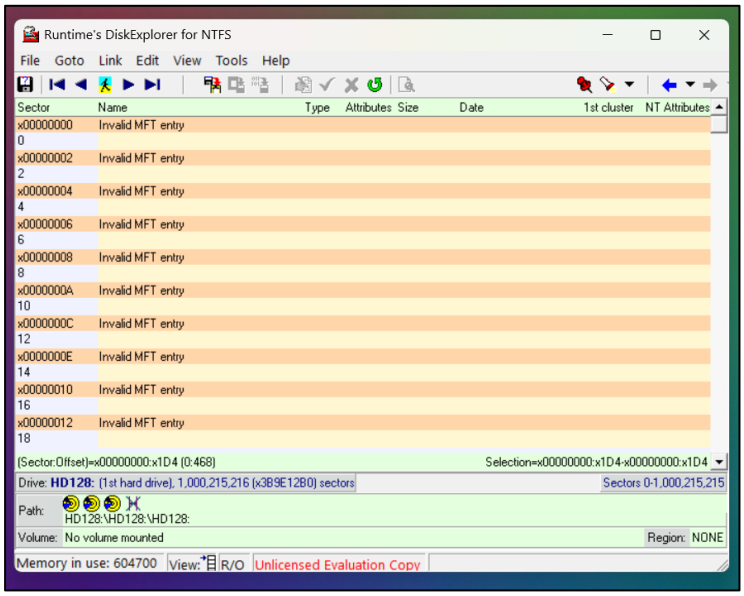

## GO to Certain SECTOR (User-ICon)

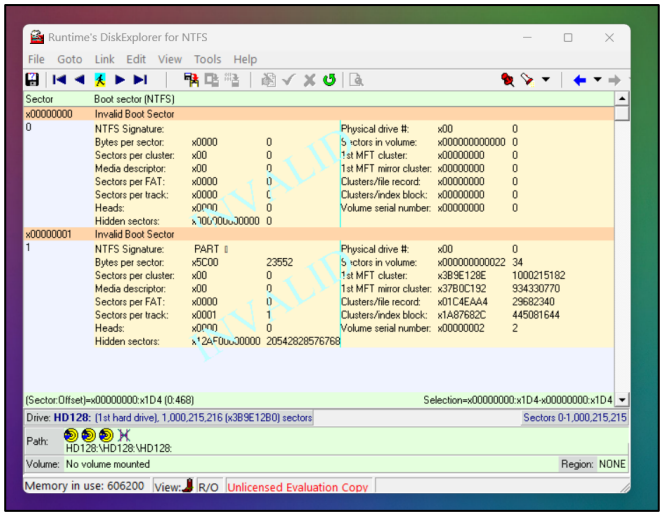


**Click OK → Then Go to FORWARD Button Click 3times → Then Click on GOTO Menu bar Select Partition Table Option → Then Click on BOOT Record → then Click on Cluster Option → OK.**

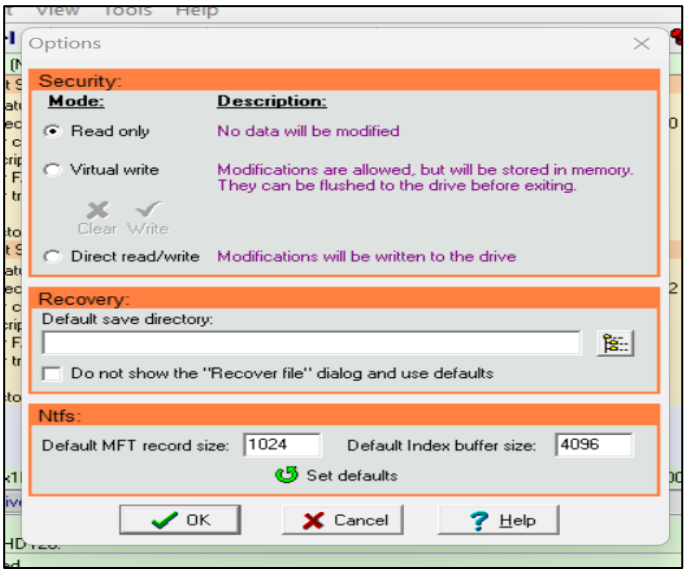



**Click on VIEW Menu Bar → Click on FILE ENTRY option → Again Click on VIEW Menu → Select as PARTITION Table Option → Again Clcik on VIEW Menu → Click on as BOOT RECORD (NTFS).**

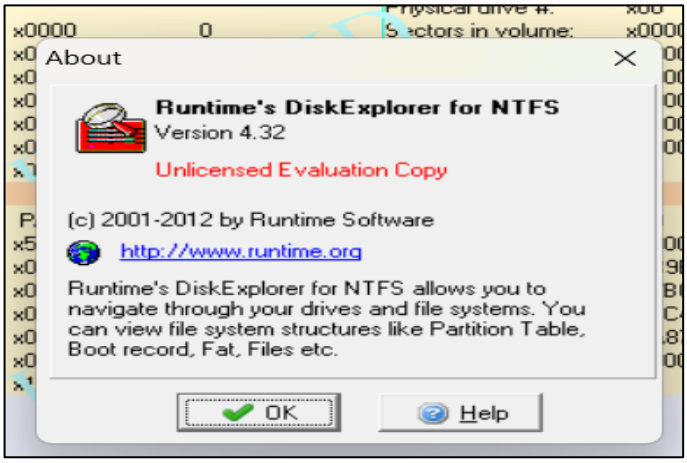





**Goto TOOLS Menu Bar → Select OPTIONS → OK → goto HELP Menu bar → Click on ABOUT Option.**



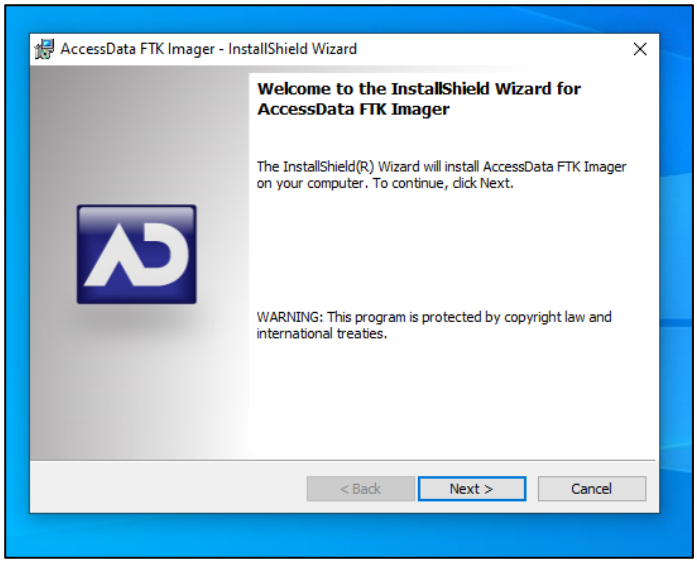

## OUTPUT SLIDE:



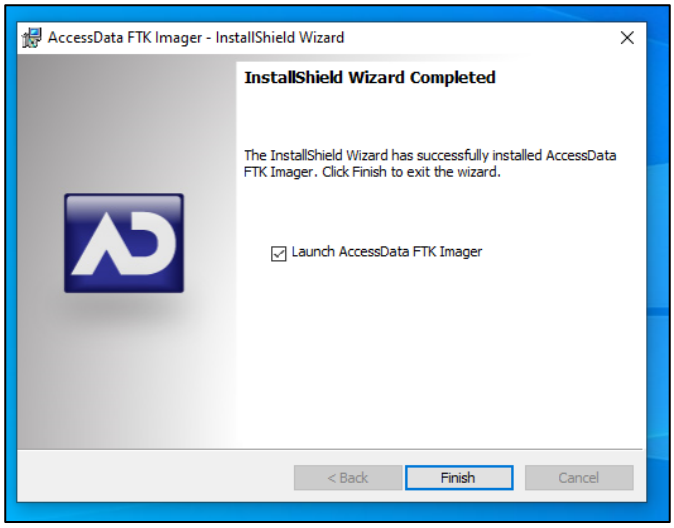
## b) Viewing Content of Forensic Image Using Access Data FTK Imager Tool

**Go to Google → Download FTK Imager.**

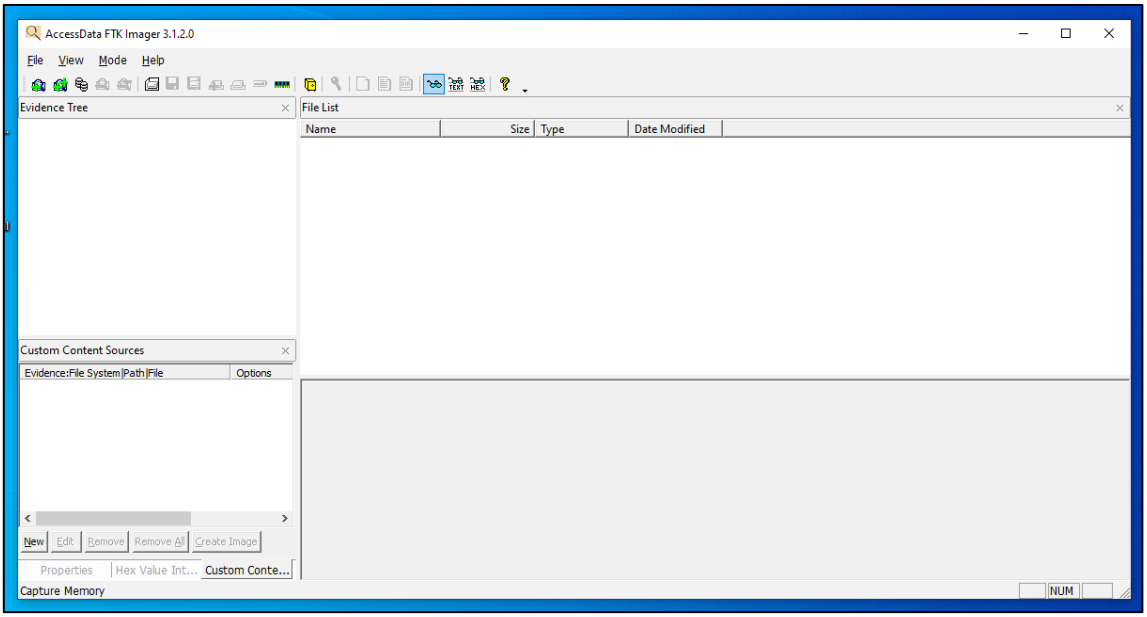

**Make one Folder With Name IP/USB on Desktop**



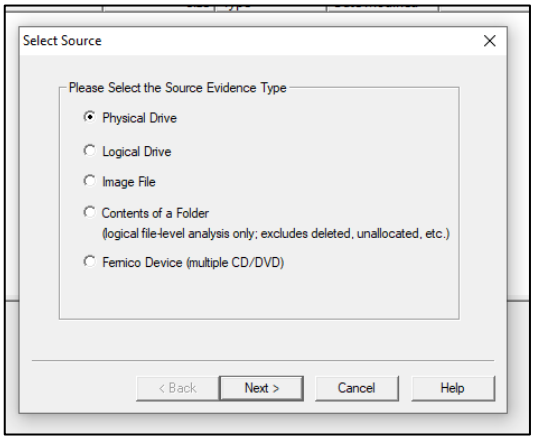

**Next → Next →Install →Finished**.



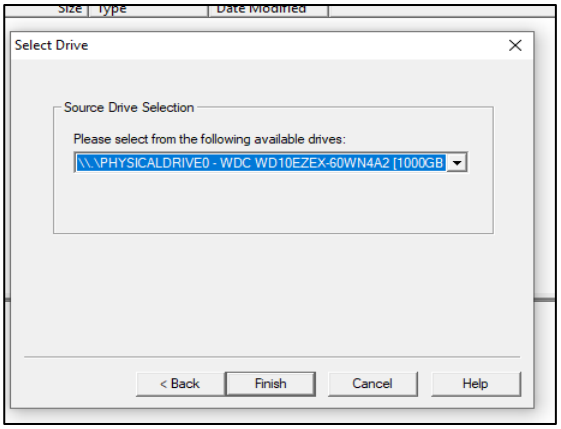
**Open the ACCESSData FTK Imager.**

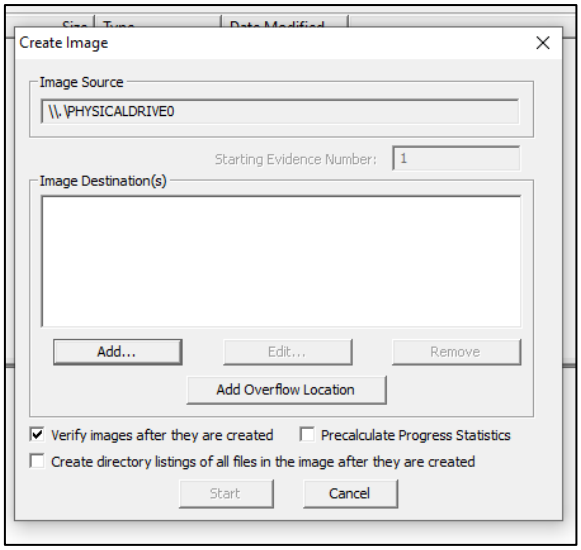



**Go to File → Create DISK IMAGER → Select PHYSICAL Drive**

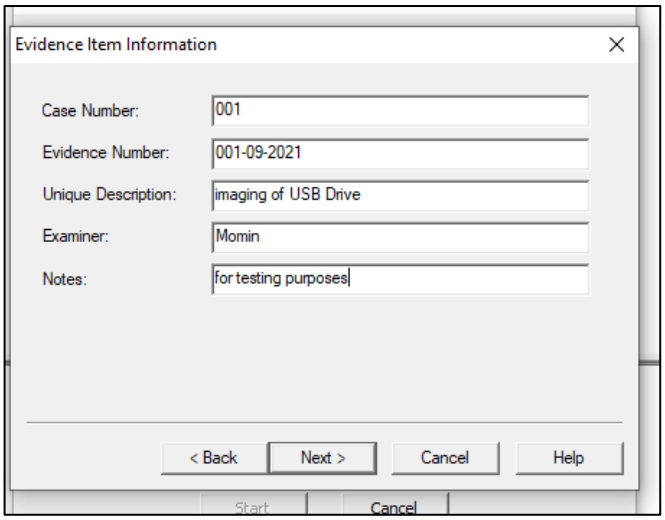



**Next → Select Path → Finish.**

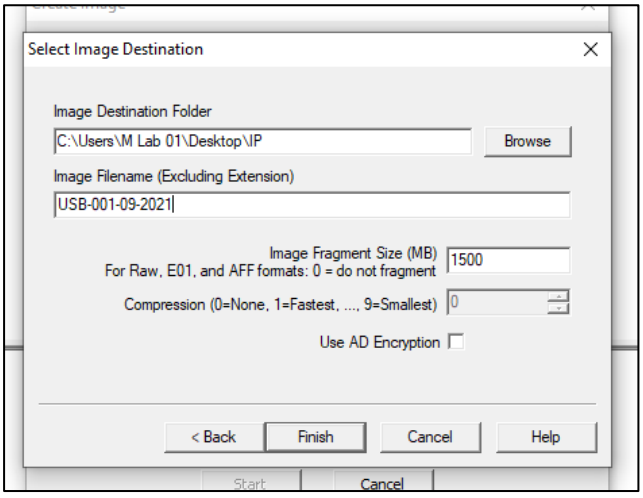


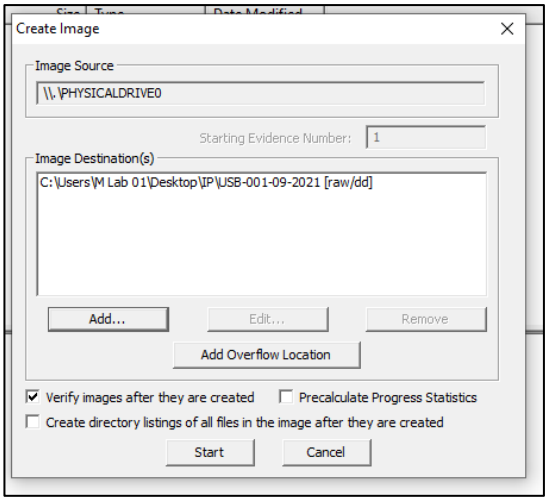



**Click on ADD → Select RAW (DD) Option → Next → Fill the Details given below.**

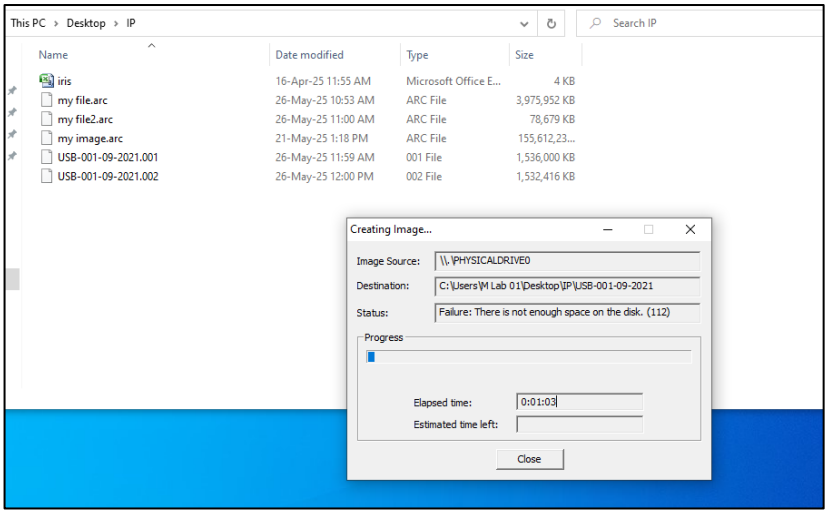



**Next → Browse → Select IP Folder →**



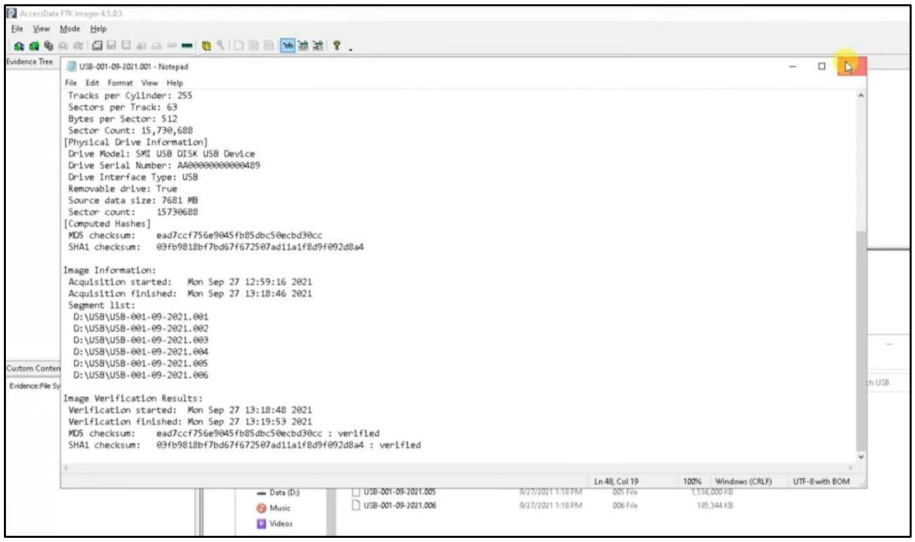



**Click on START**




**Click on any single file which show the details of an image.**

## OUTPUT SLIDE:



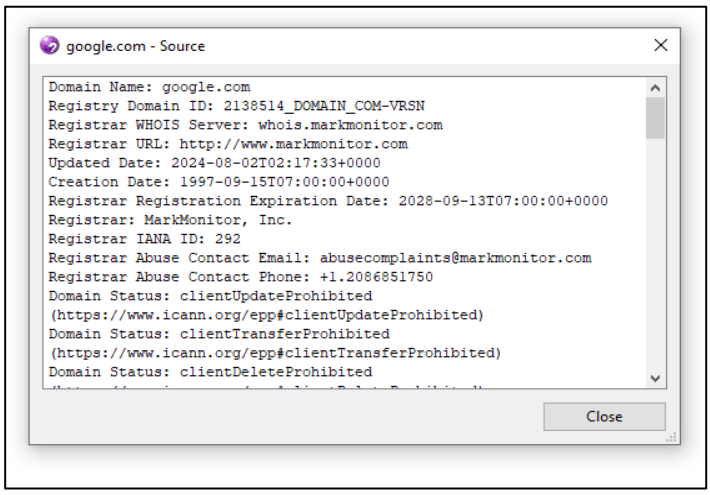
# INVESTIGATING WEB ATTACKS

## a) Analyzing Domain and IP Address Queries Using SmartWhois Tool

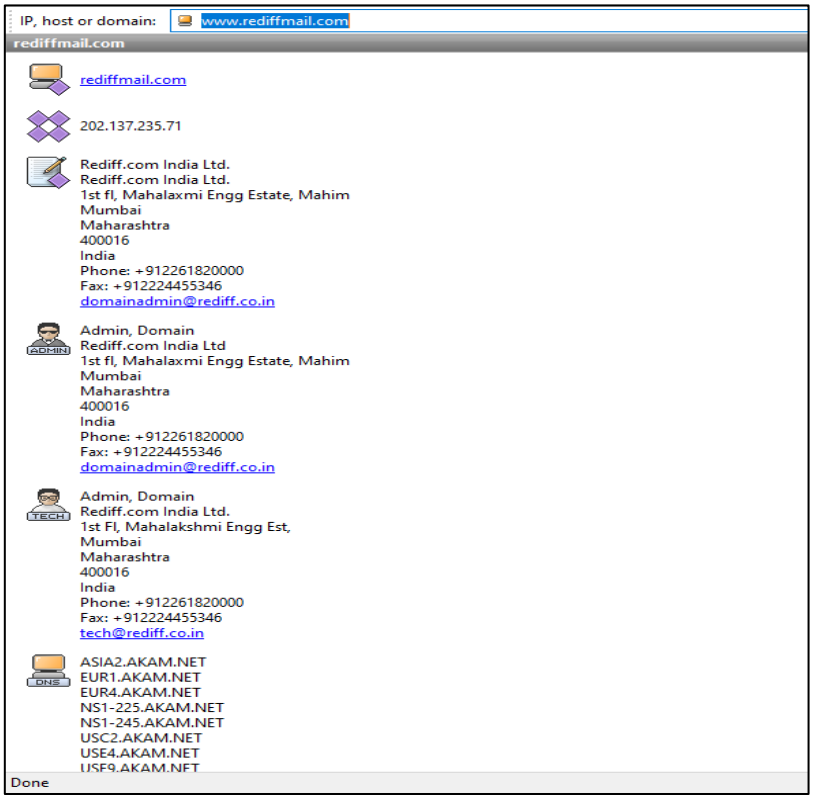
**Go to Google → Download Smart Whois.**



**Open Smart Whois → Search WWW.GOOGLE.Com → Click on Query Button → Click on View Source → Click on Close Button.**

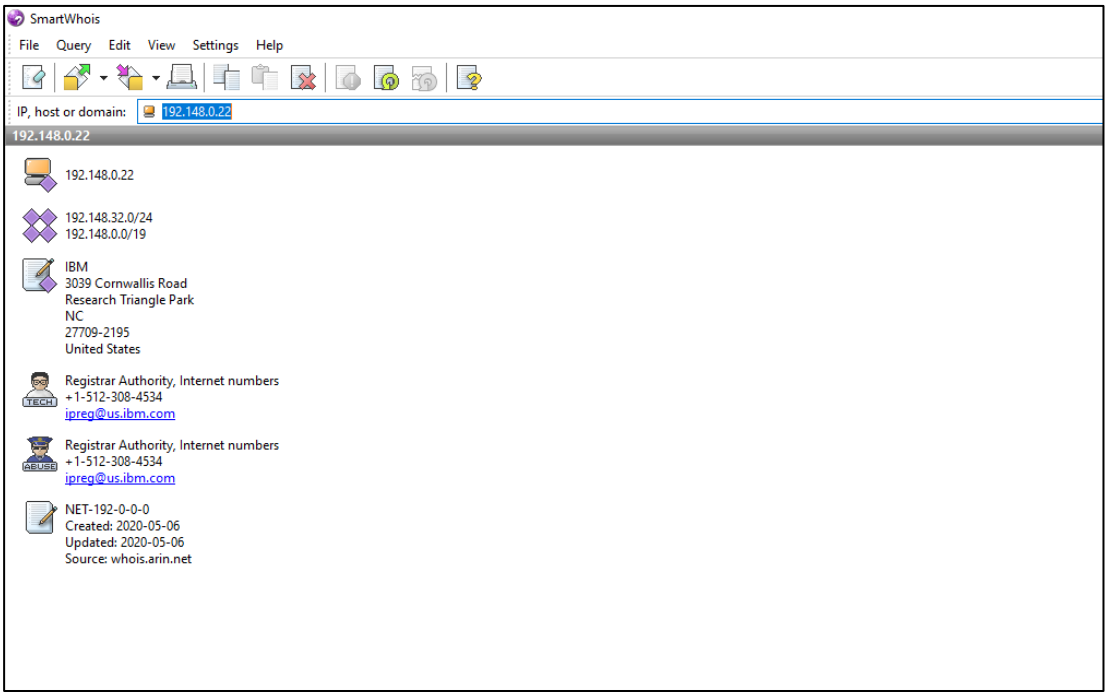


**Search www.rediffmail.com → Click on Query Button**




**Again Search 192.148.0.22 → Click on Query → Goto File Menu Bar → Click on EXIT option.**

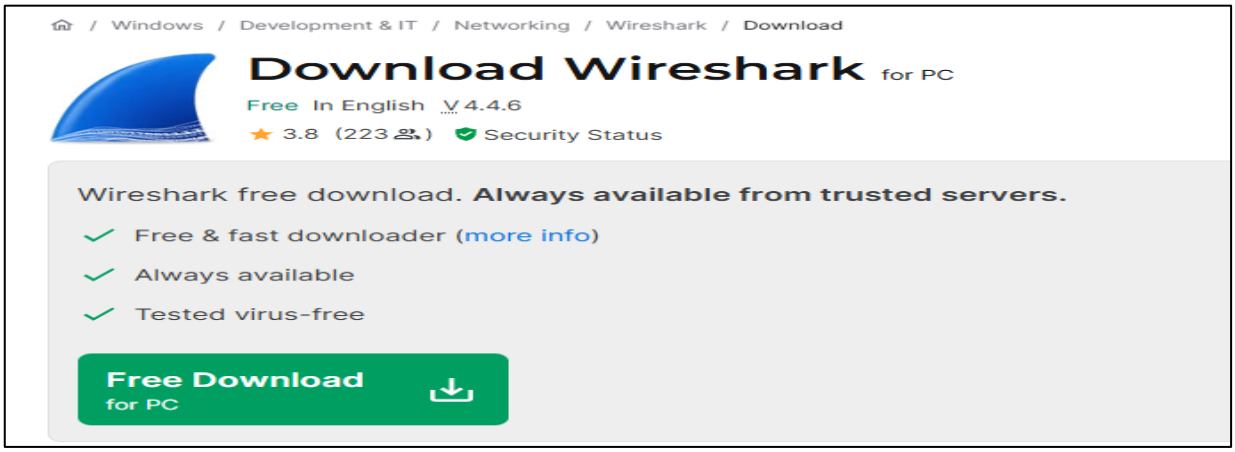
## OUTPUT SLIDE:

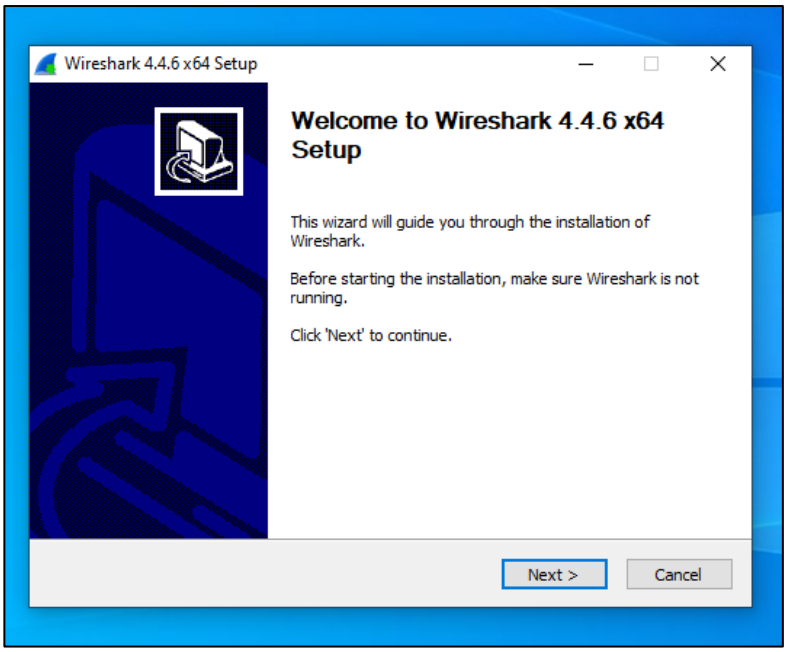


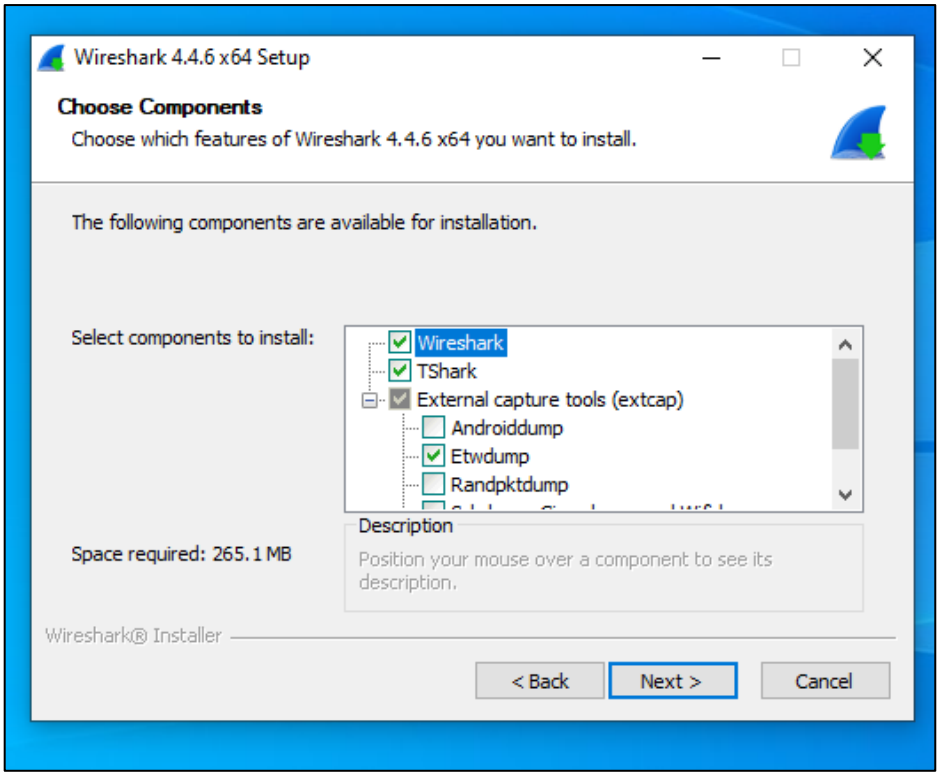
# NETWORK FORENSICS

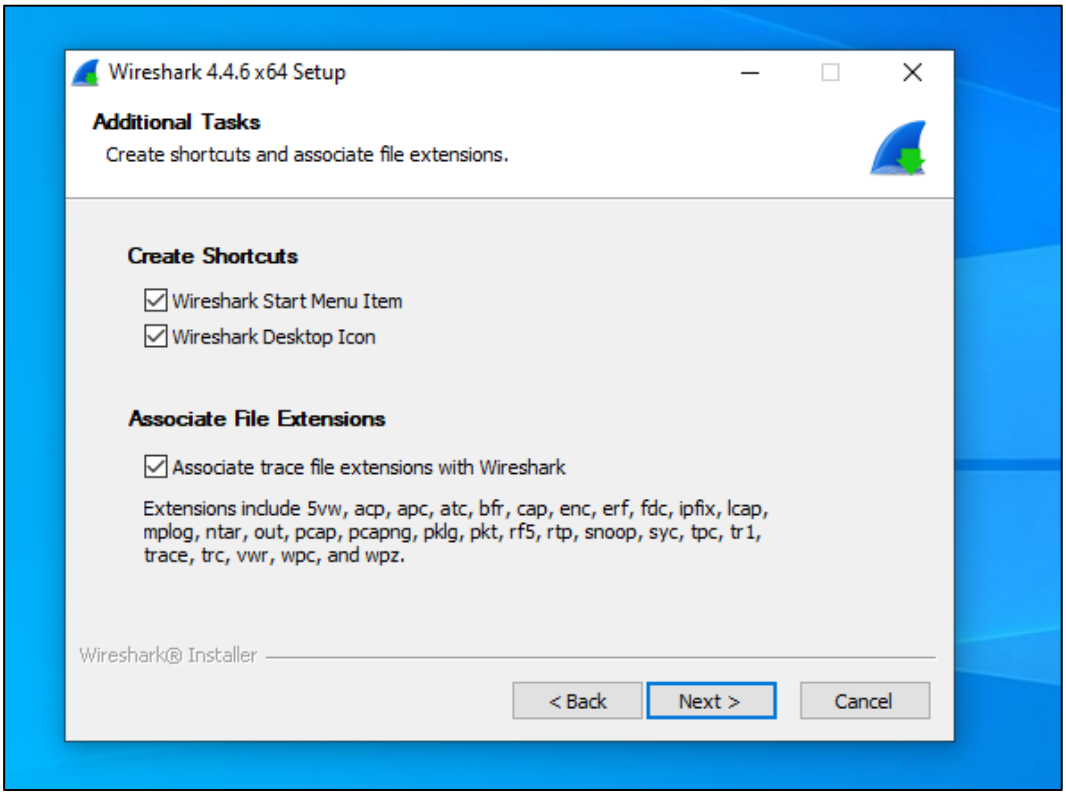
## a) Investigating Network Traffic Using Wireshark

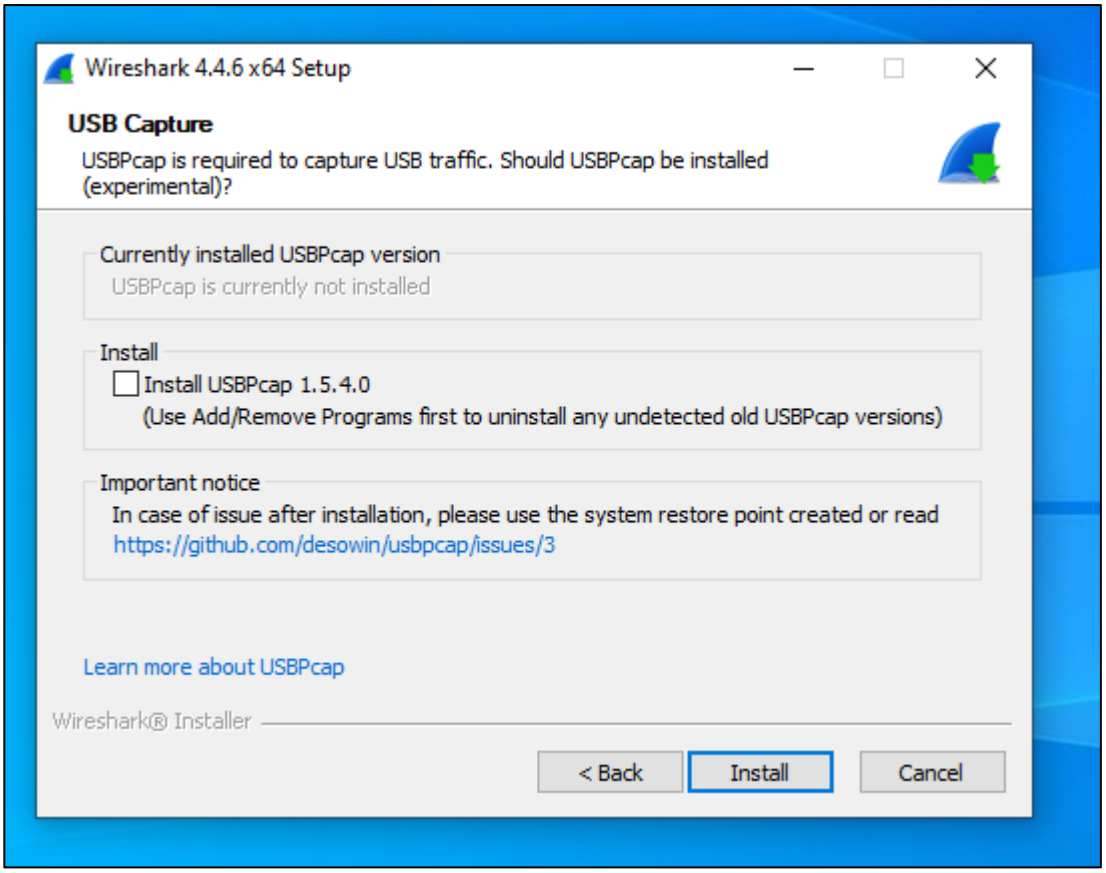
**Go to Google → Download WireShark**




Wireshark 4.4.6 x64 Setup
Choose Components
Choose which features of Wireshark 4.4.6 x64 you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
External capture tools (extcap)
Androiddump
Etwdump
Randpktdump
Description
Position your mouse over a component to see its description.
Space required: 265.1 MB
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 4.4.6 x64 Setup
Additional Tasks
Create shortcuts and associate file extensions.
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Associate File Extensions
Associate trace file extensions with Wireshark
Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, ntar, out, pcap, pcapng, pklg, pkt, rf5, rtp, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.
Wireshark® Installer
< Back
Next >
Cancel

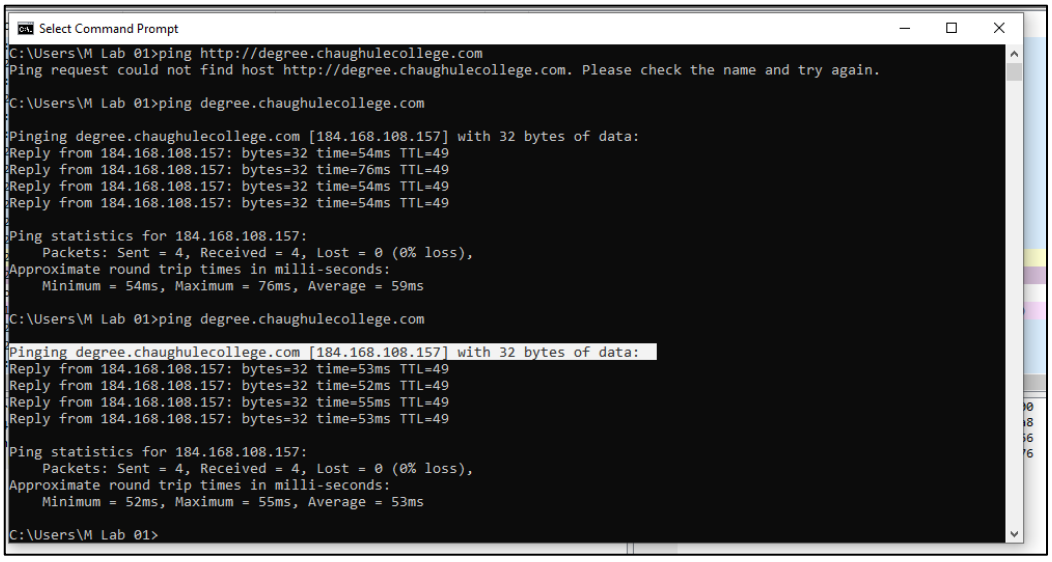



**Next → Next →Install →Finished**.

**Open Wire Shark → Select Interface as ETHERNET 4 →**

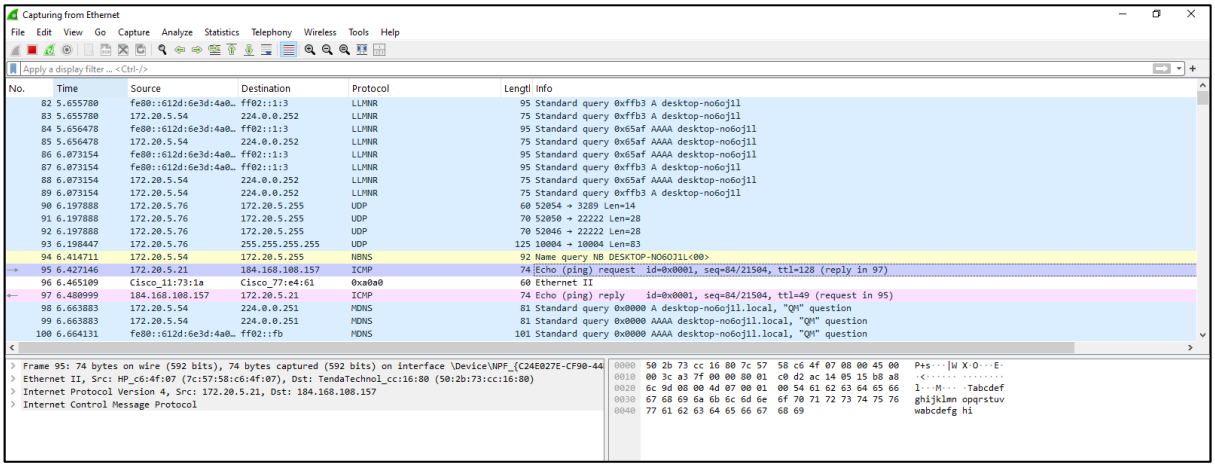
**Goto Browser → HTTP website Local Server IP Address/Port no. 192.168.56.105:8080**

**Open WireShark → Stop capturing TRAFFIC → Apply filter (HTTP)**



**Go to File → Click on Quit to Stop.**

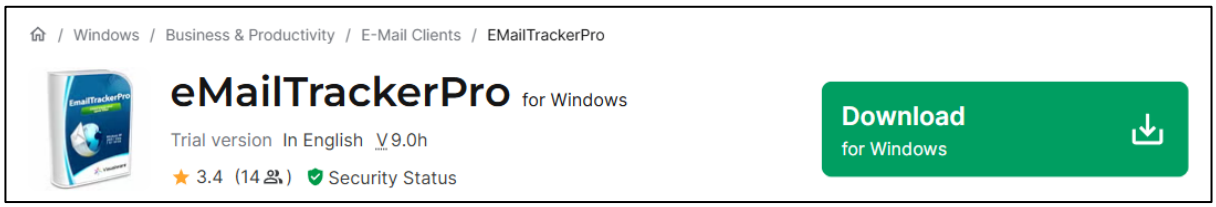
# OUTPUT SLIDE:

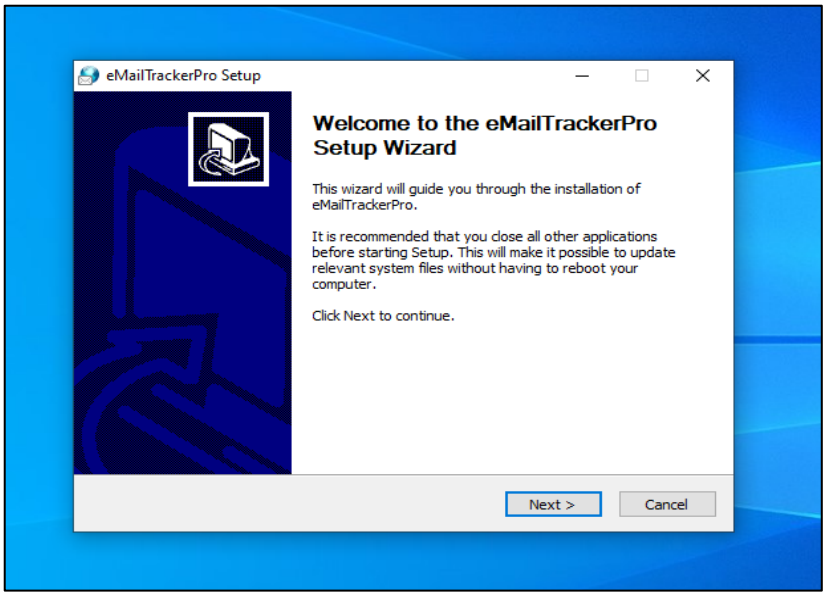


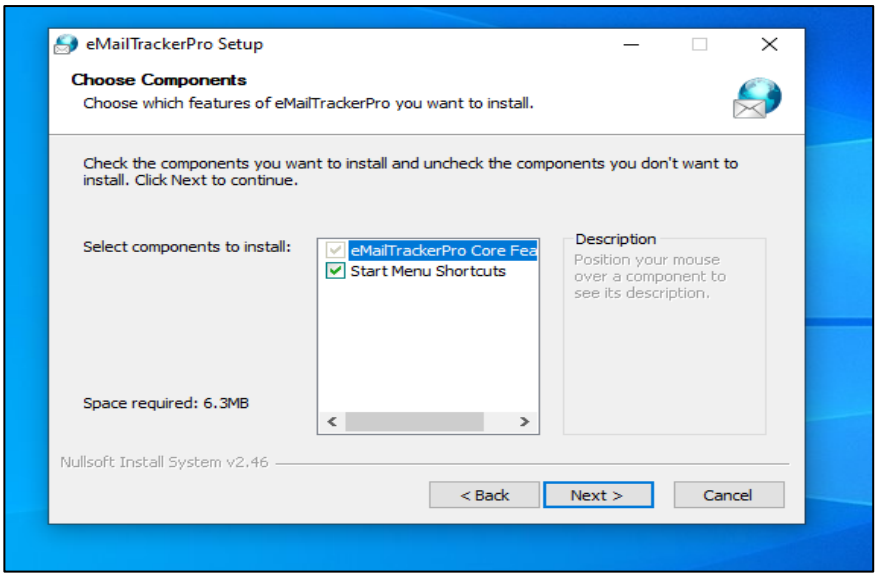
# INVESTIGATING EMAIL CRIMES

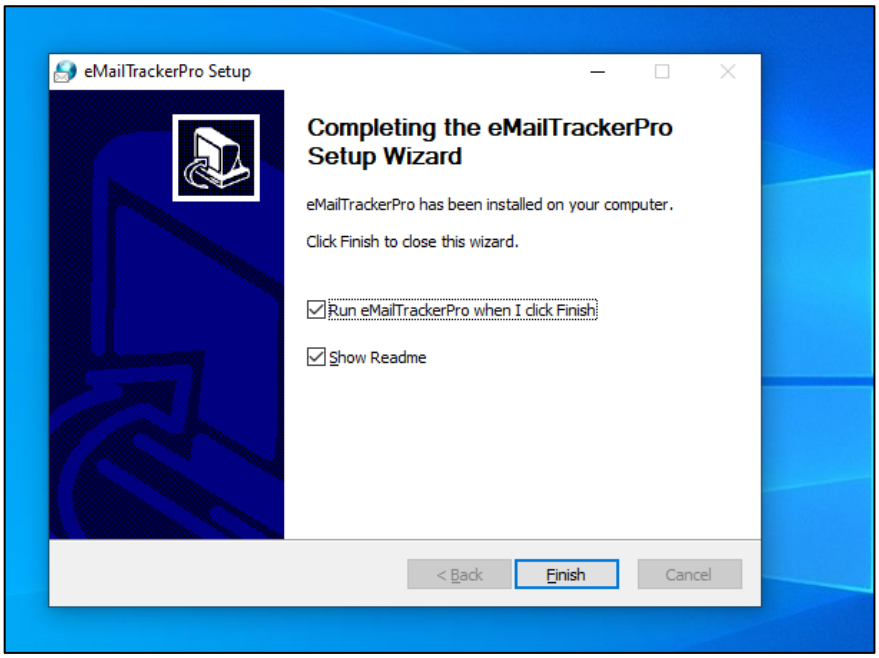
## a) Tracing an Email Using the eMailTrackerPro Tool

**Go to Google → Download eMailTracker Pro**



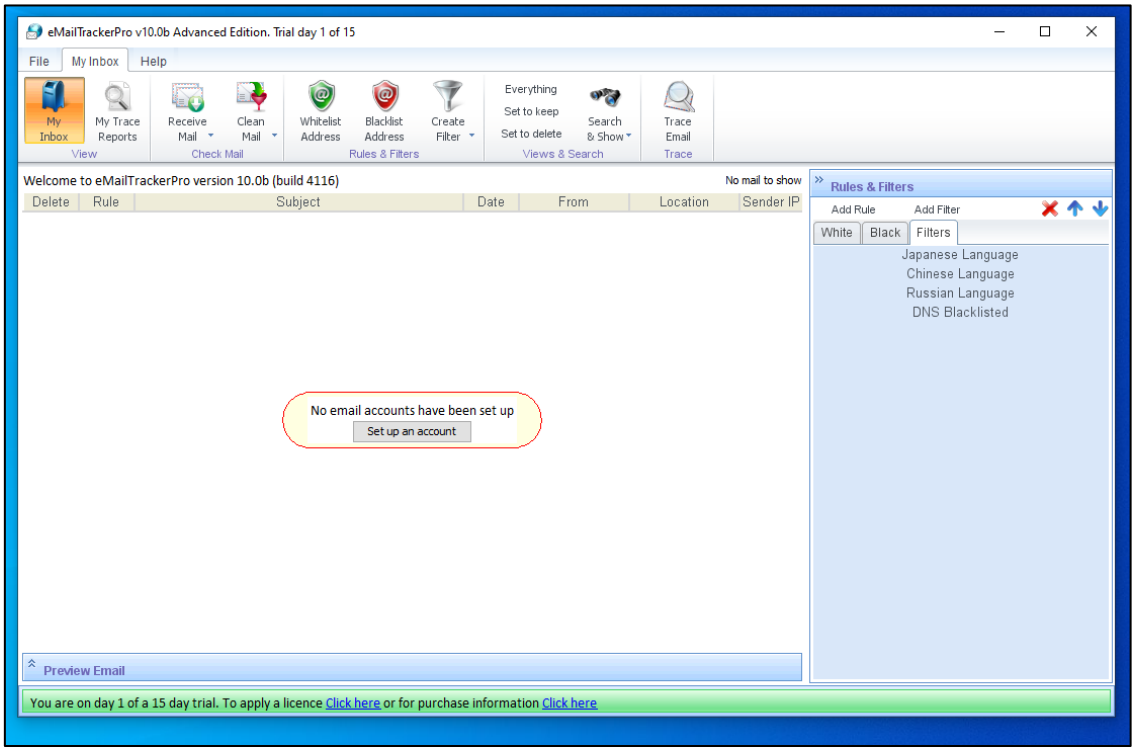



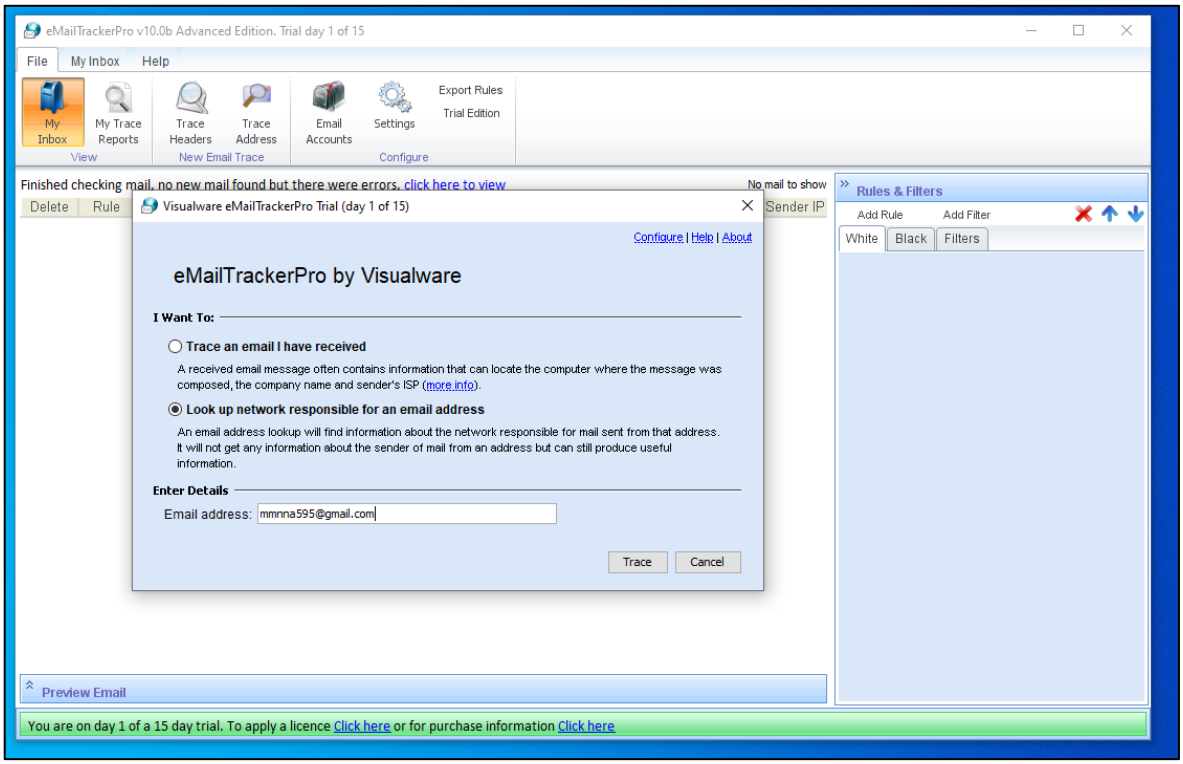



**Next → Next →Install →Finished**

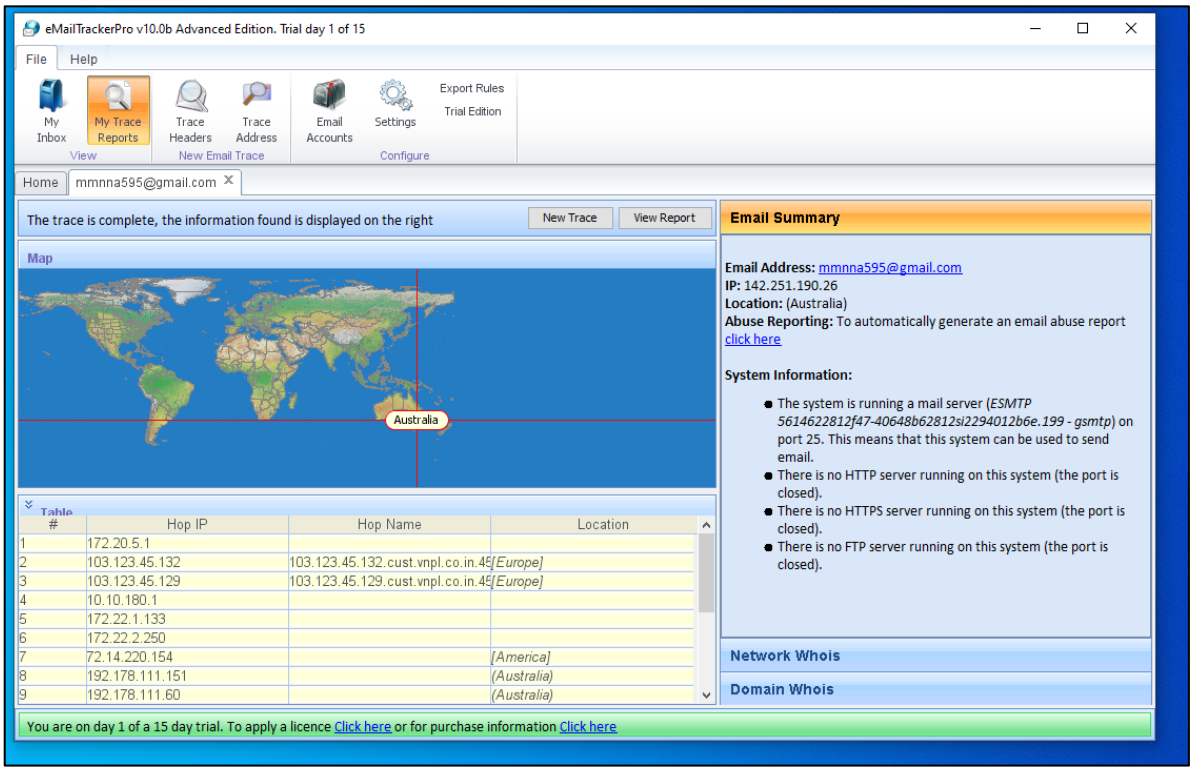
**Open the eMailTracker Pro**



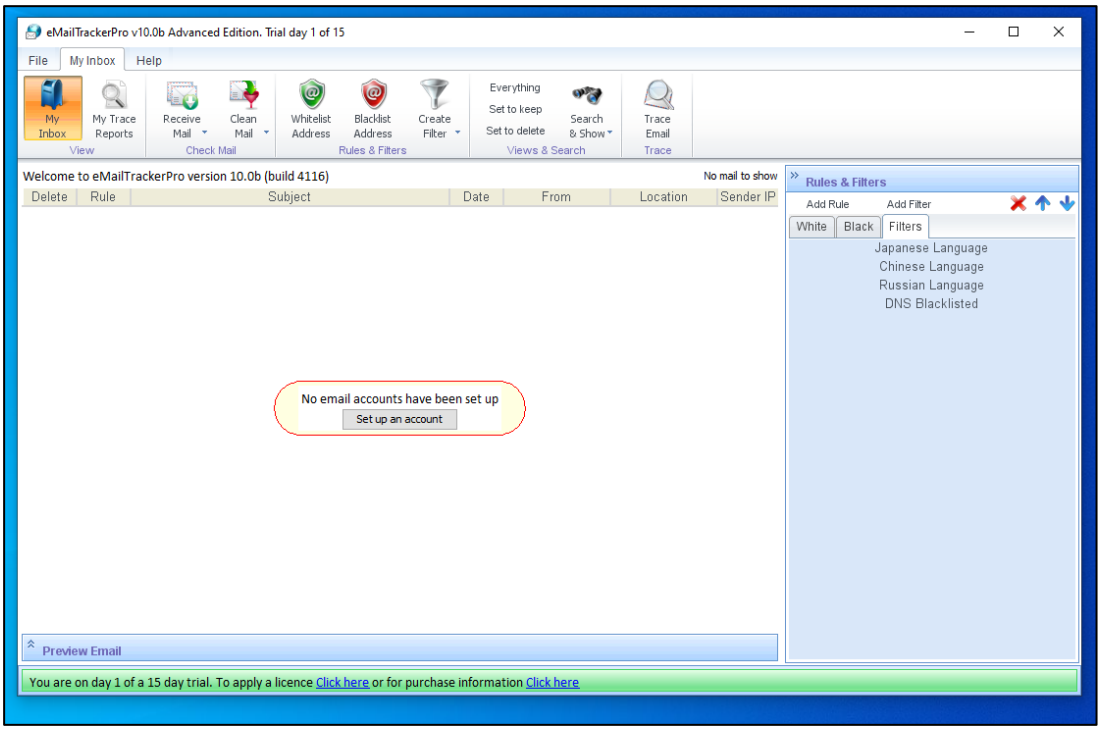
**Goto START here → Change some Settings → Enter Email Address → Trace**



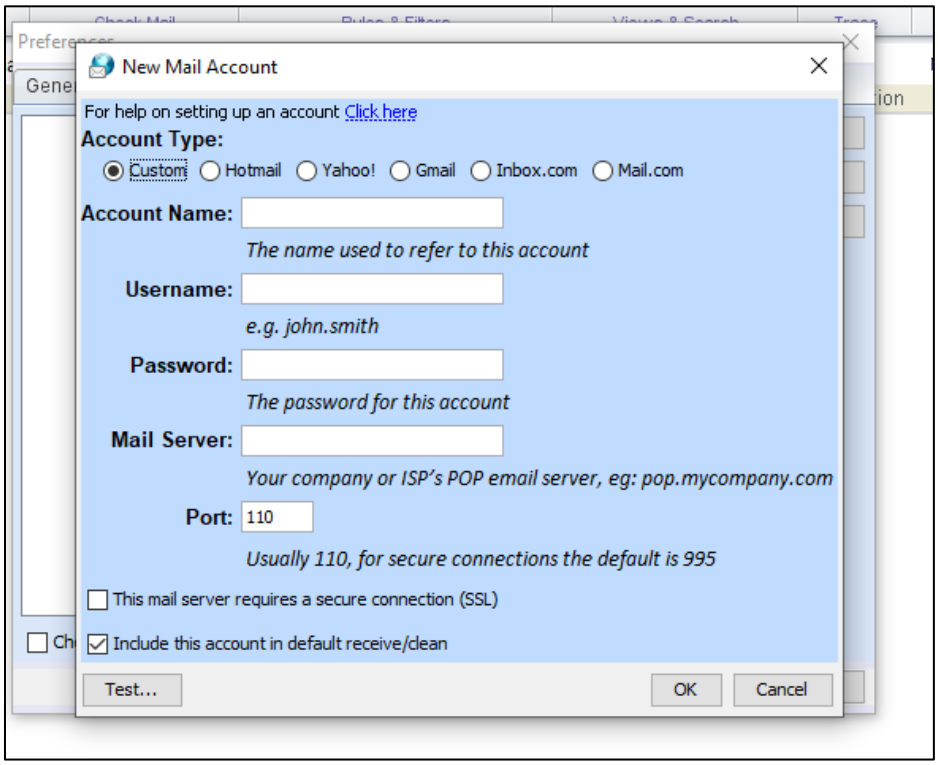

**Check the Table Which is Given the MAP**

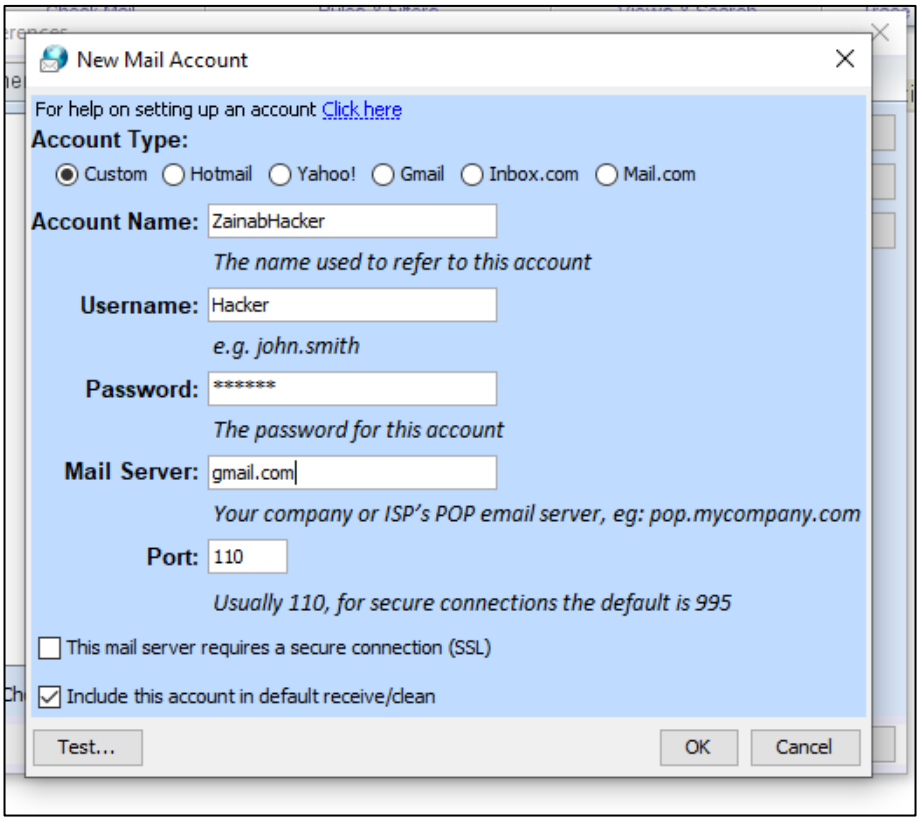


## Goto My Inbox → Setup an Account

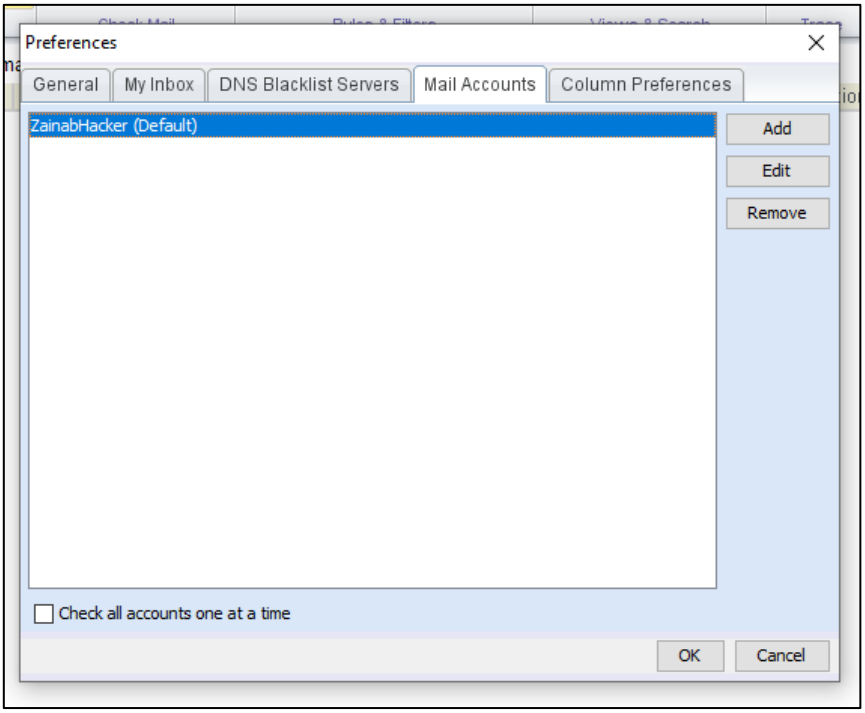



## Click on Setup an Account → Fill all the Details

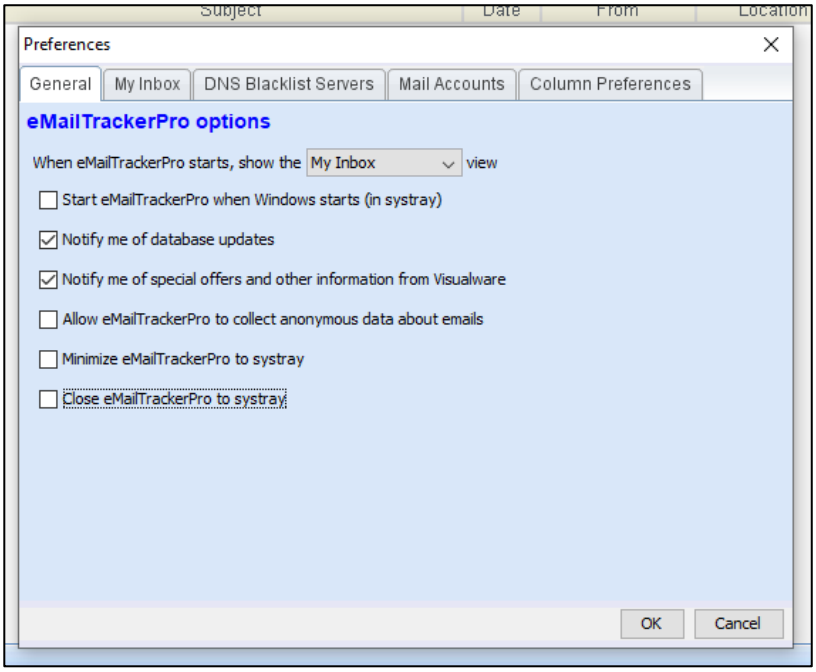





**Click on OK → Select the Email which is display in front of you →**

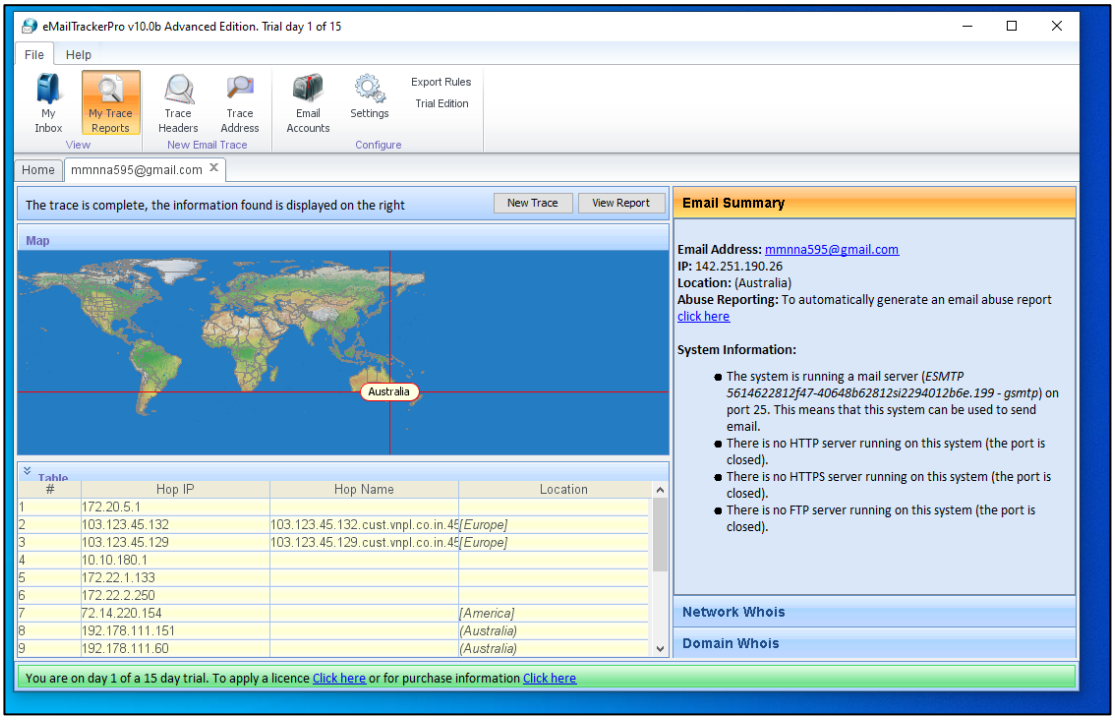


**Select 2nd and 4th Options → OK**




**Goto My Trace Report → Then Goto File → Click on EXIT**

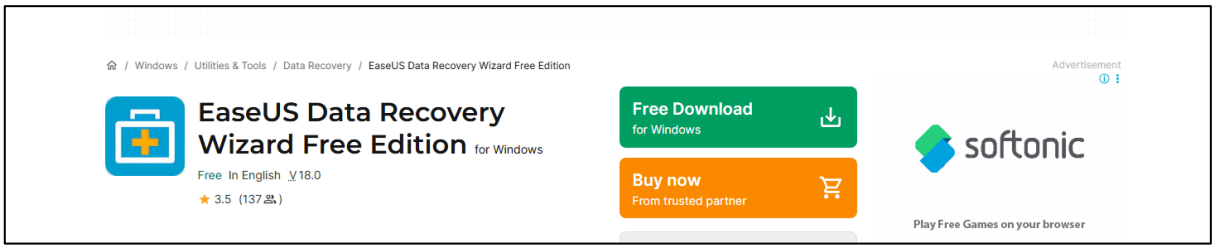
# OUTPUT SLIDE:



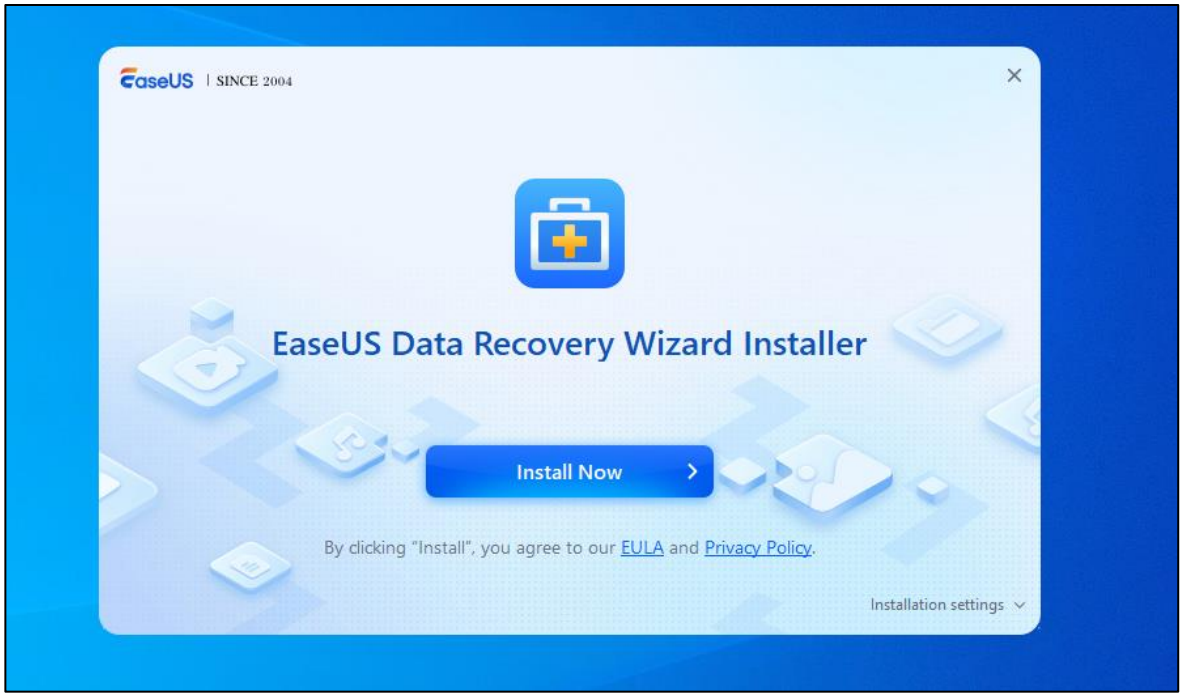
# COMPUTER FORENSICS INVESTIGATION PROCESS

## a) Recovering Data using the EaseUS Data Recovery Wizard.

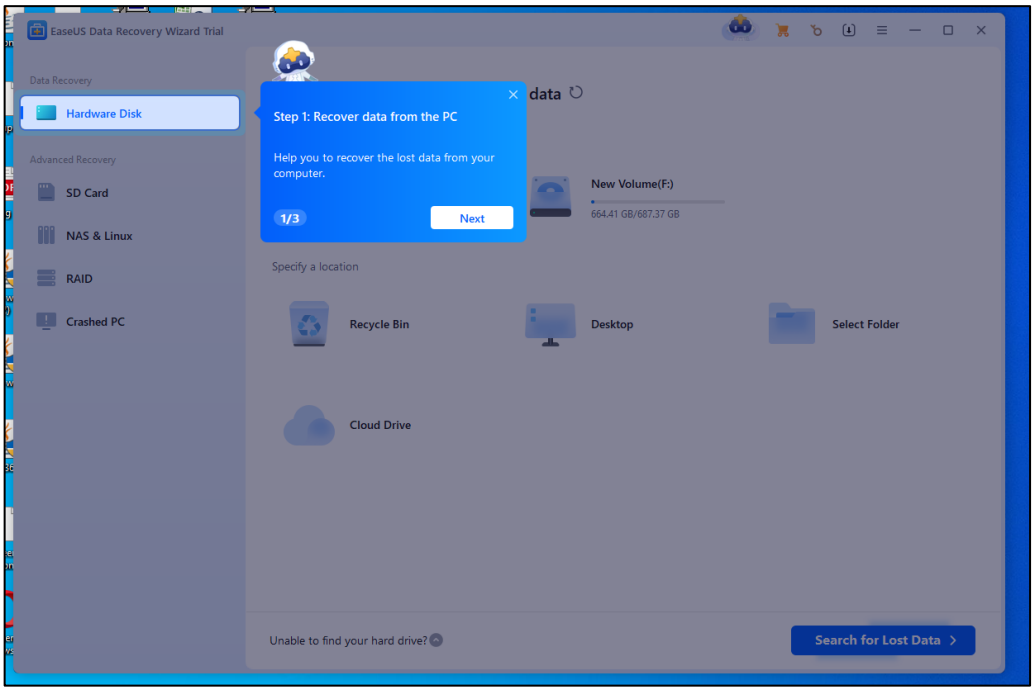
**Go to Google → Download EaseUs Data Recovery**



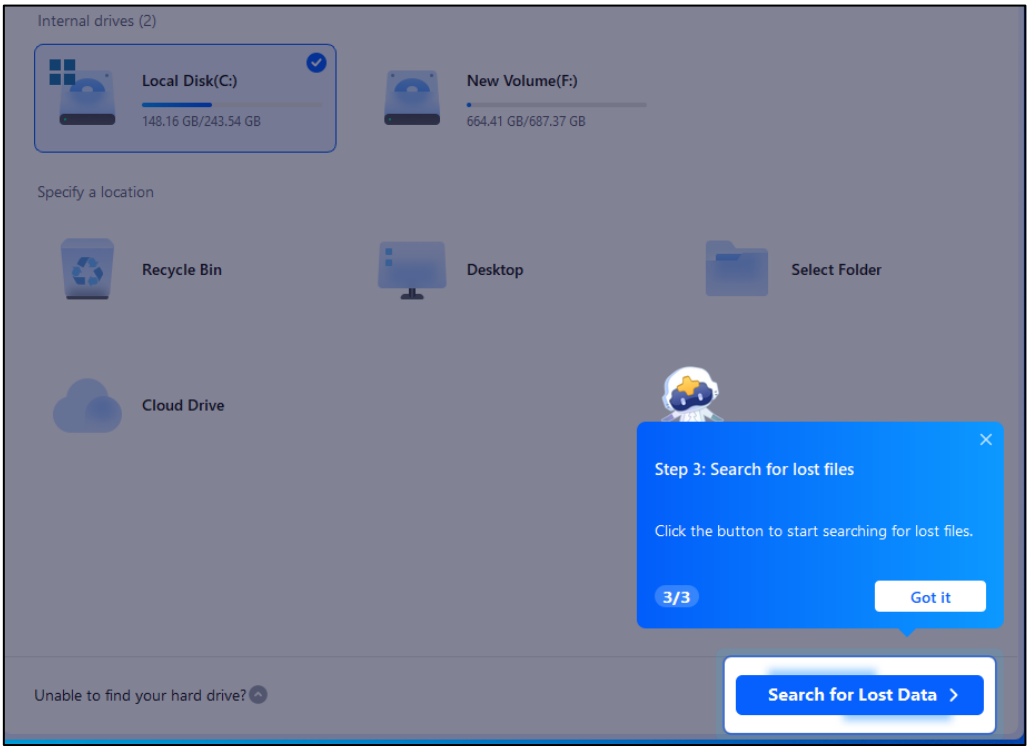

**Install**



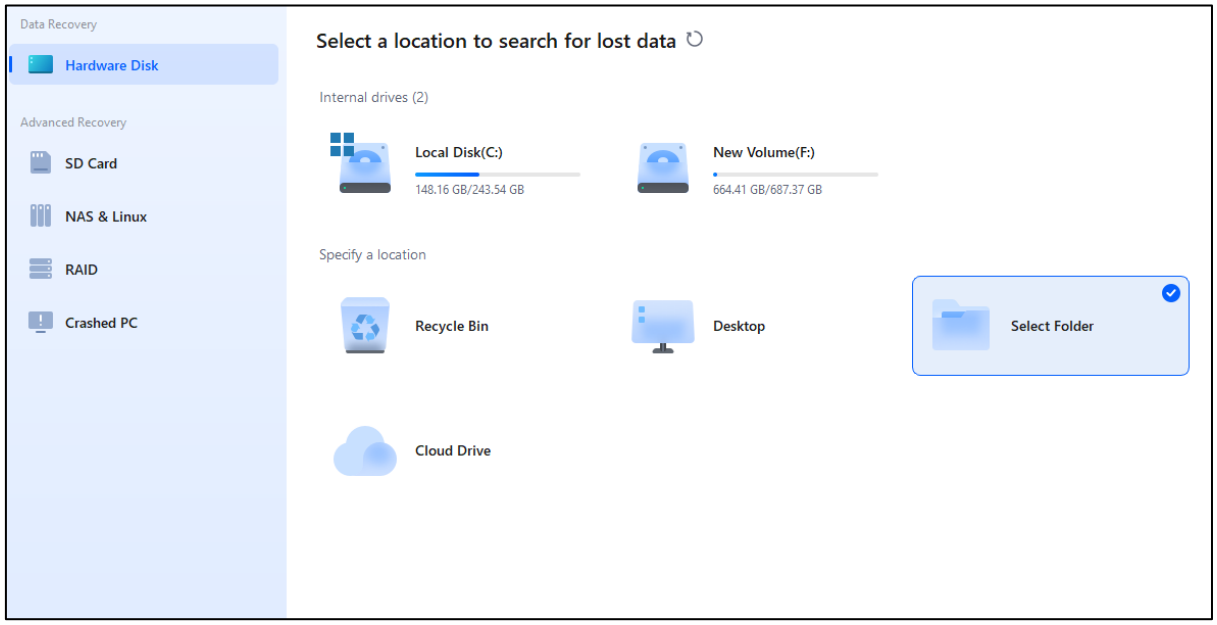
## Open EaseUs Data Recovery → Showing All Disk

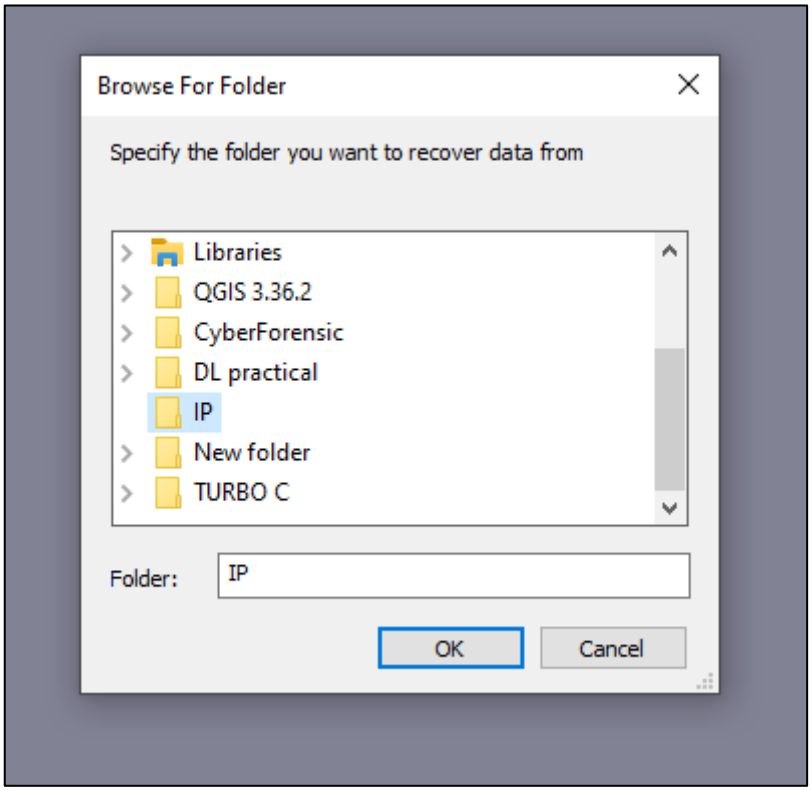



## Search for LOST DATA

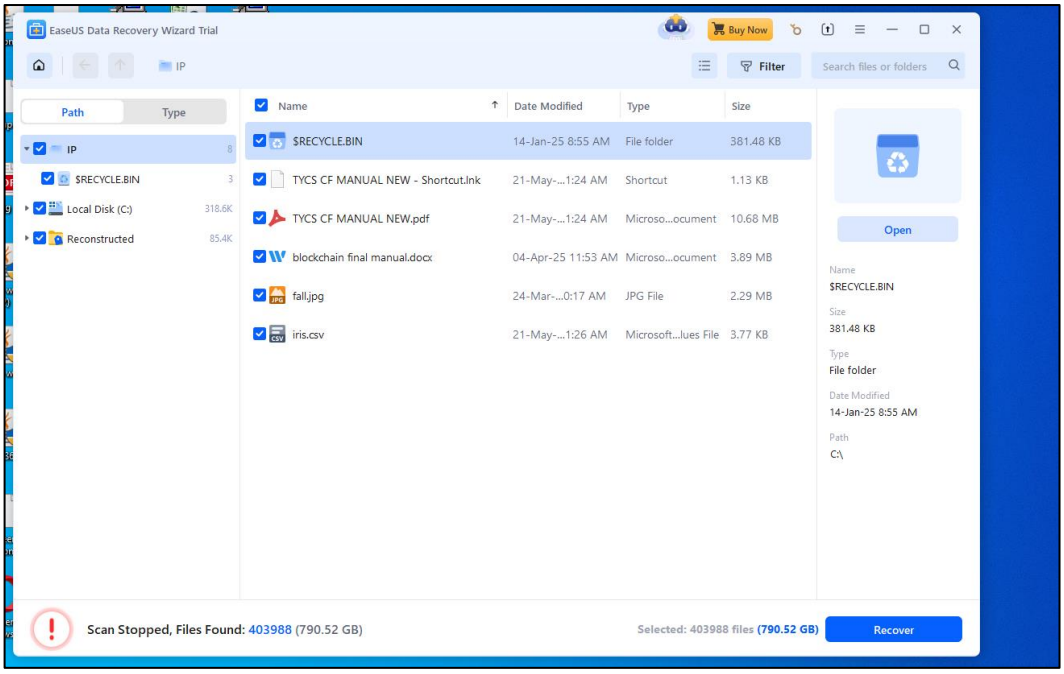


**Select Folder → Create a one FOLDER (IP) → OK**



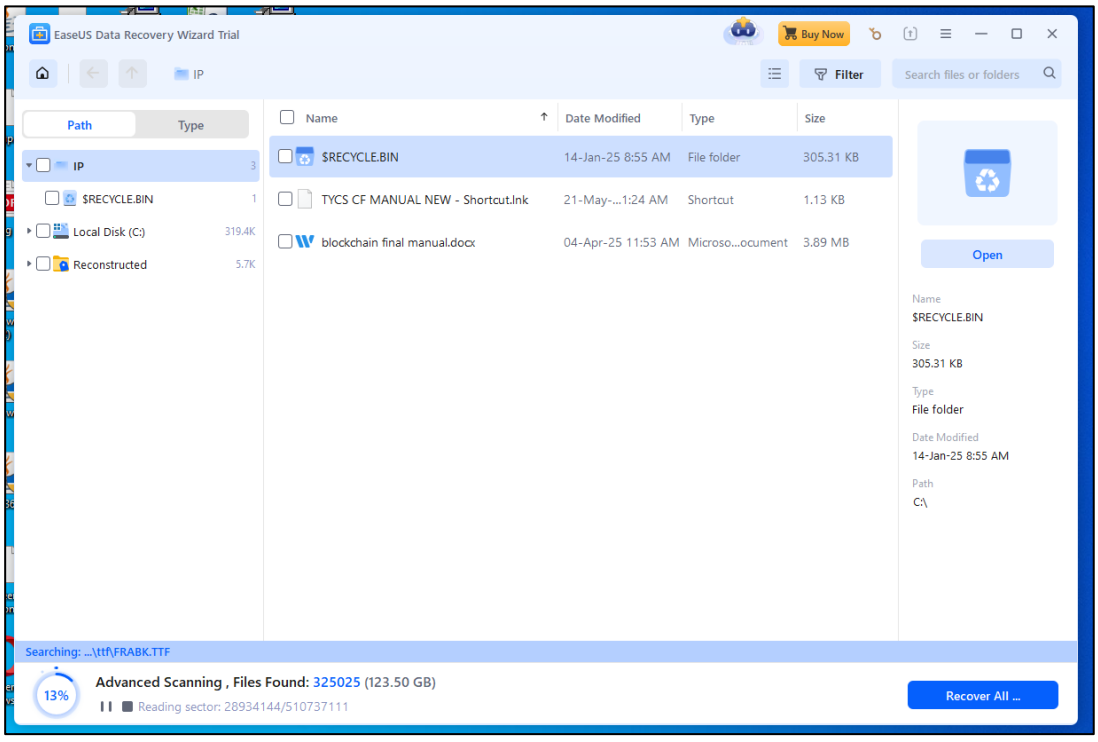



**Delete all FILE → Then RECOVER all**



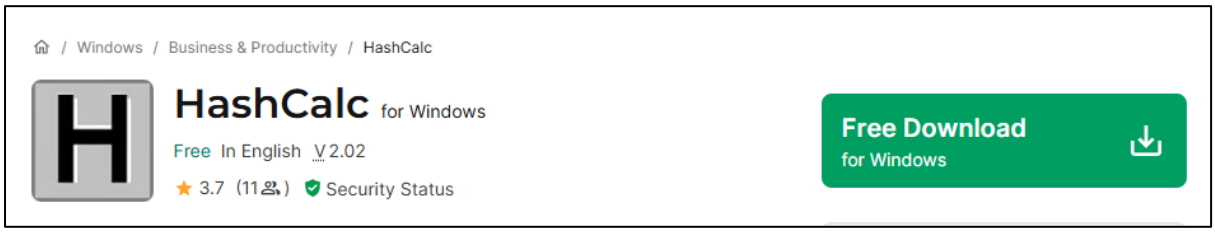

**ADVANCE SCANNING**

**OUTPUT SLIDE:**

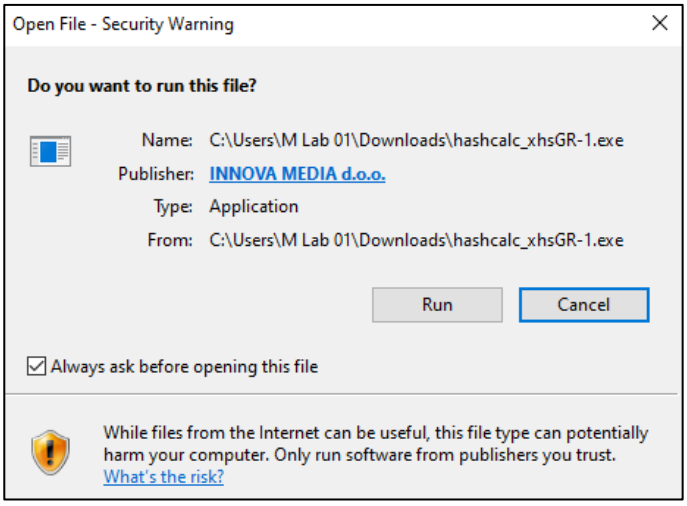


## b) Performing Hash, Checksum, or HMAC Calculations using the HashCalc.

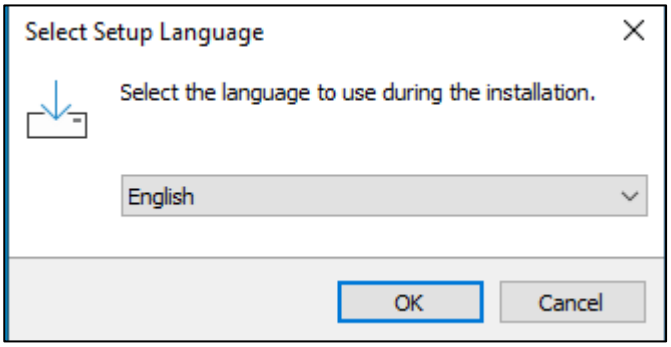
**Go to Google → Download HashCalc**

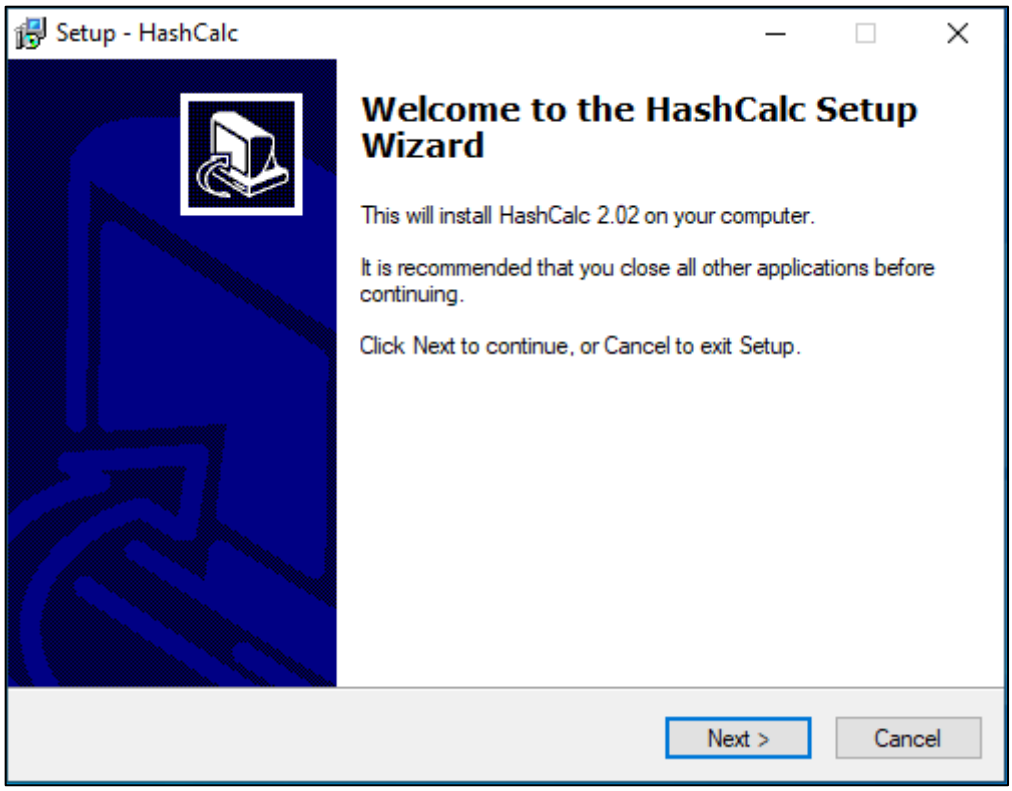



**Open the HashCalc → Click on RUN**



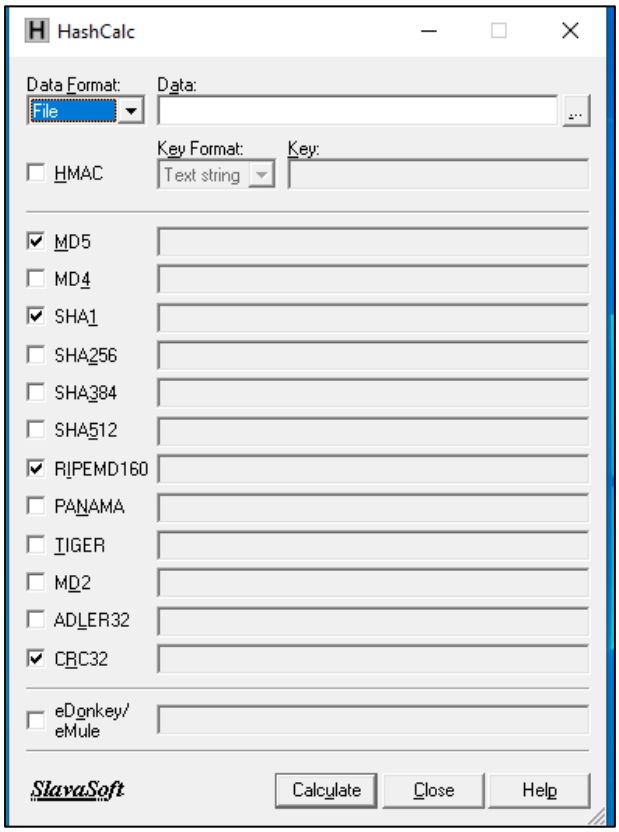

**Select ENGLISH Language → Click on OK**



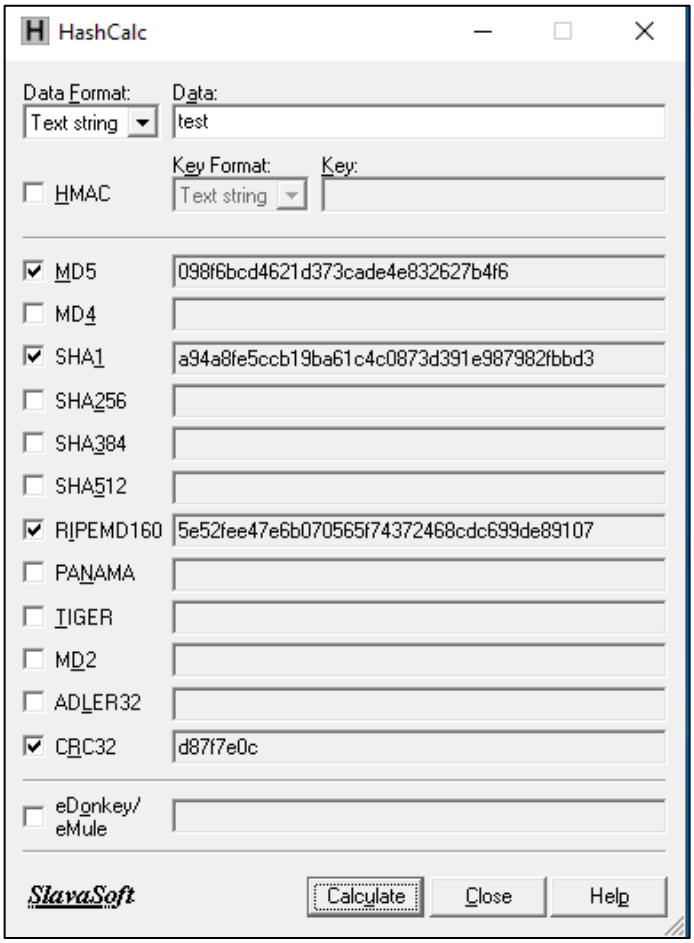



**Next → Next → Next → Install → Finish.**

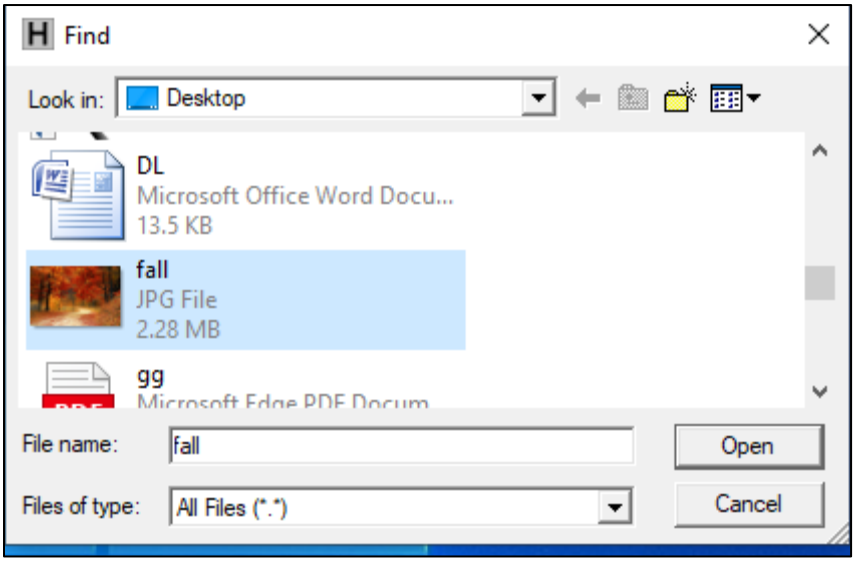
**Open HashCalc Software**



**Data Format change File into Text String → Put some DATA (Test) → Calculate**

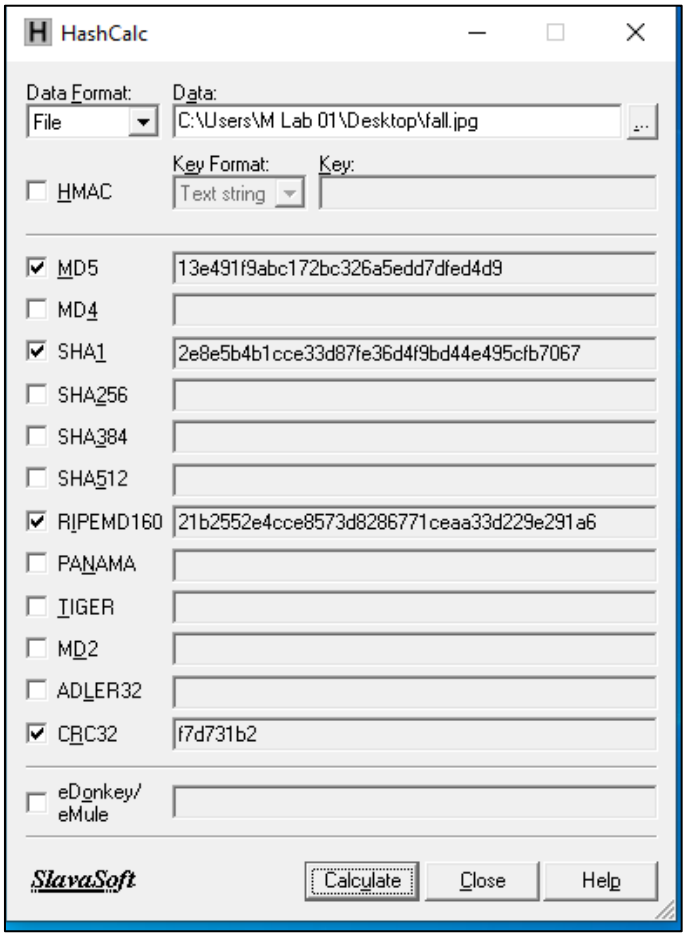



**Data Format is FILE → Browse the FILE → File Name (Fall.jpg) → Calculate →**



**Check the ALGORITHM → SHA-1, MD5 and so on → Tally the OUTPUT value with the Google Value.**

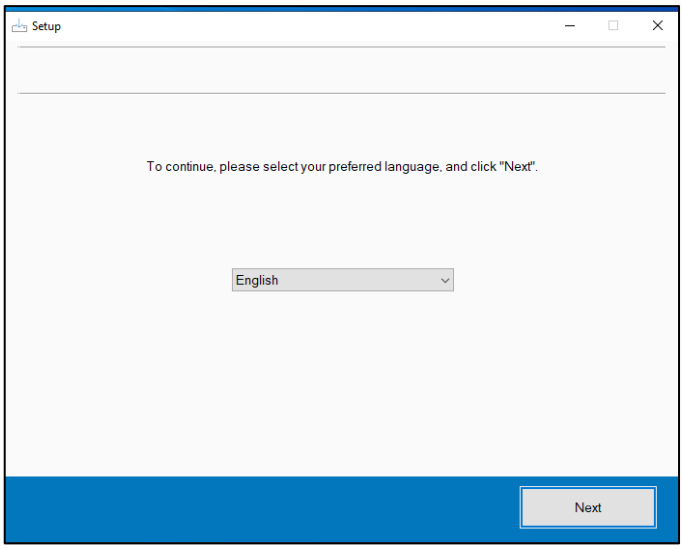
## OUTPUT SLIDE:



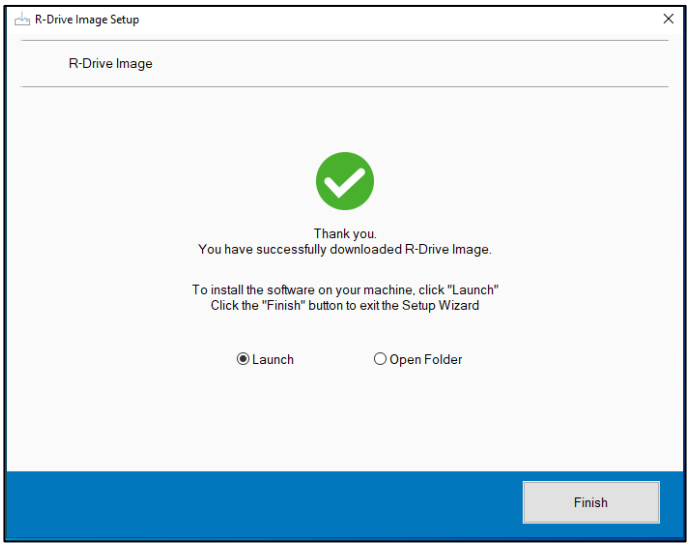
## c) Creating a Disk Image File of a Hard Disk Partition using the R-drive Image Tool.

**Go to Google → Download R-Drive Image**

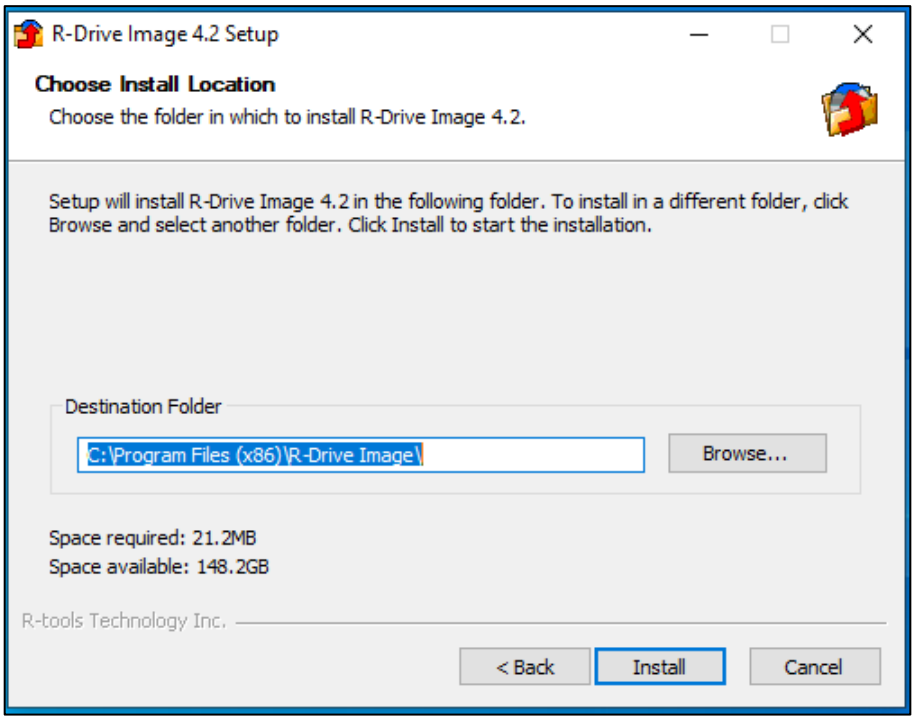

**Set the Langauge(ENGLISH) → Next**

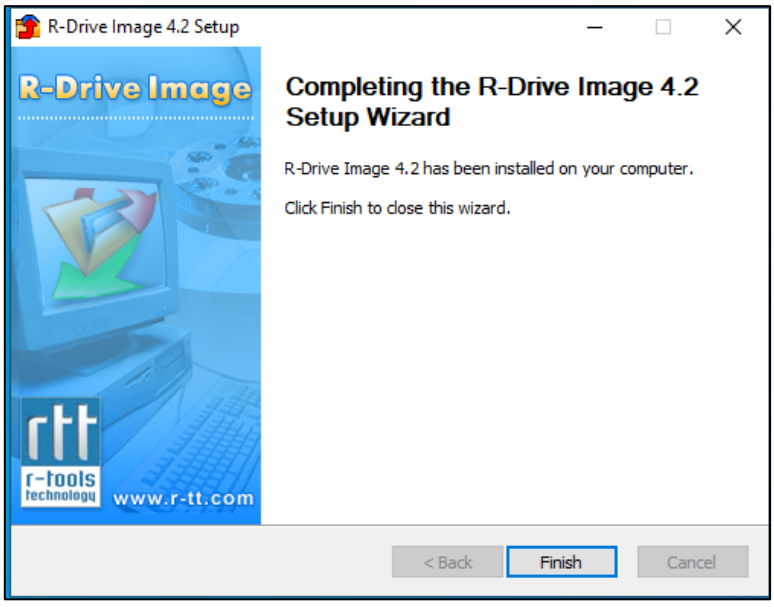



**Next → Finish**

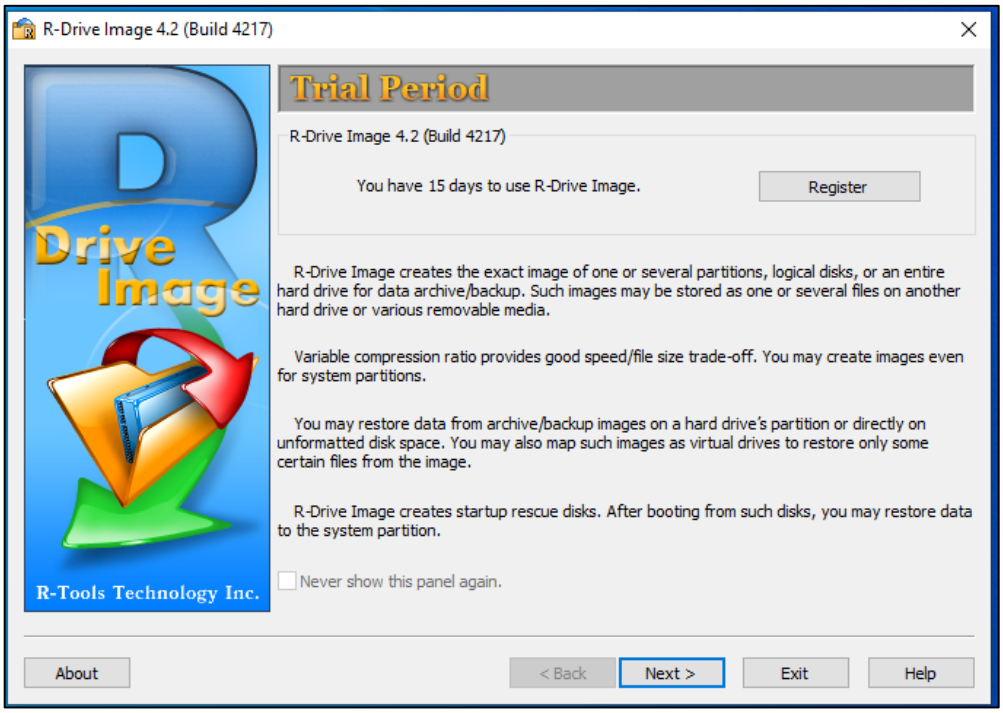


**Next → Next → Next → Install → Finish**

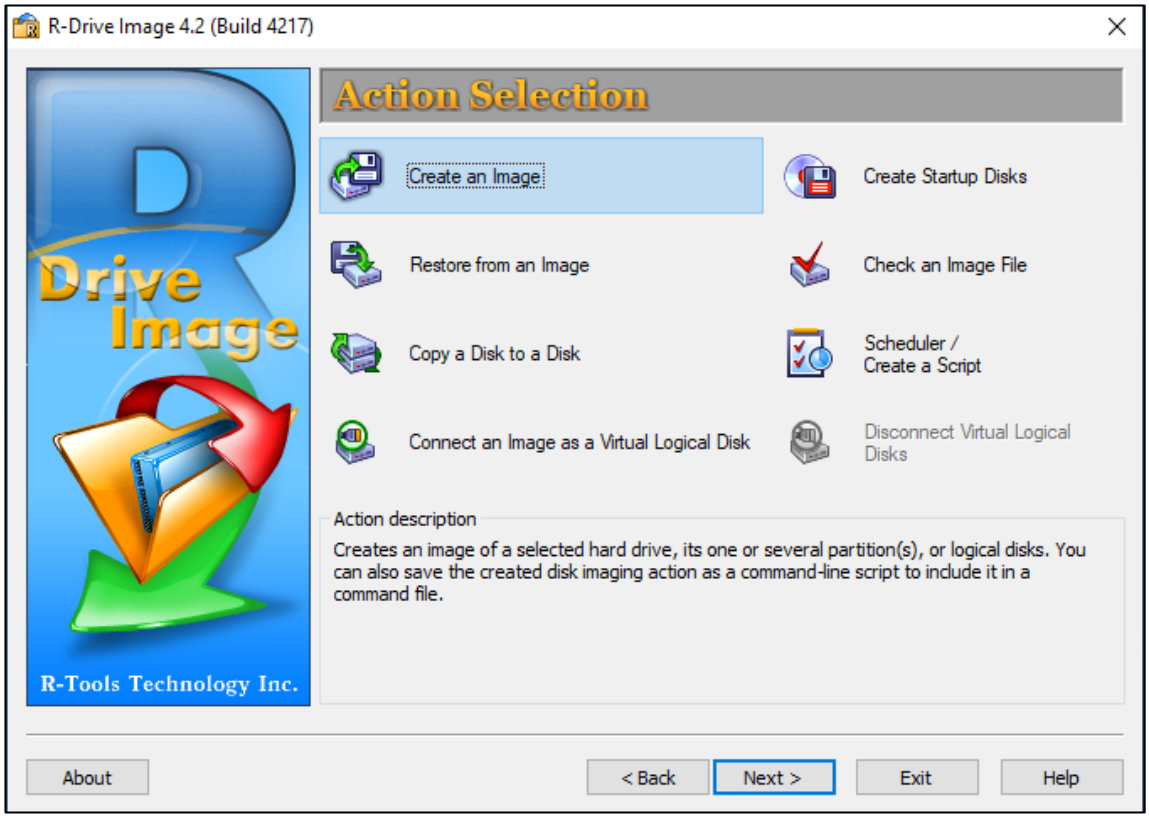


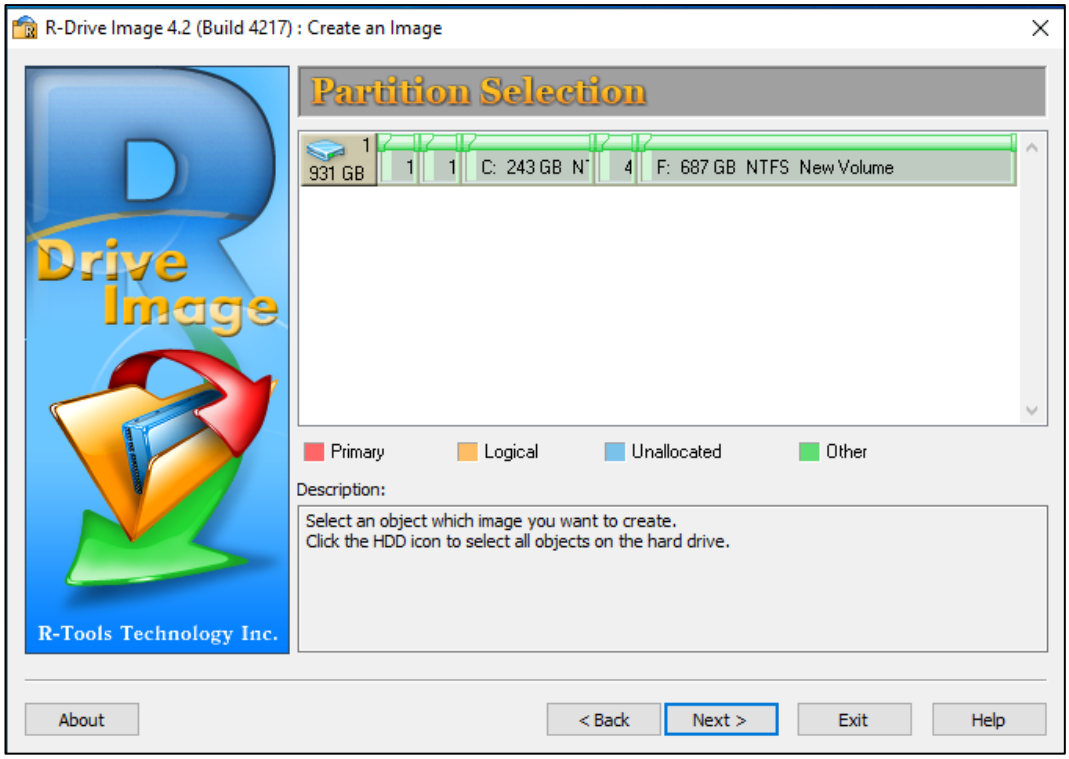
**Open R-Drive Image → Next**



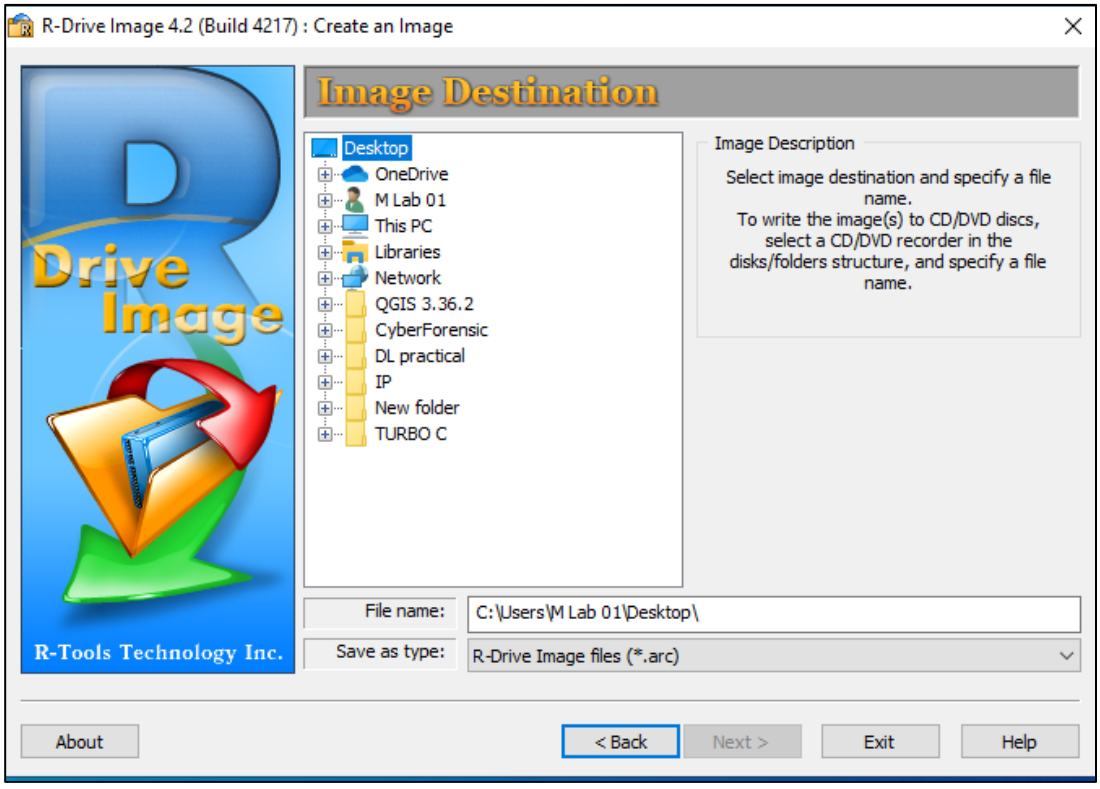

**Create an Image → Next**

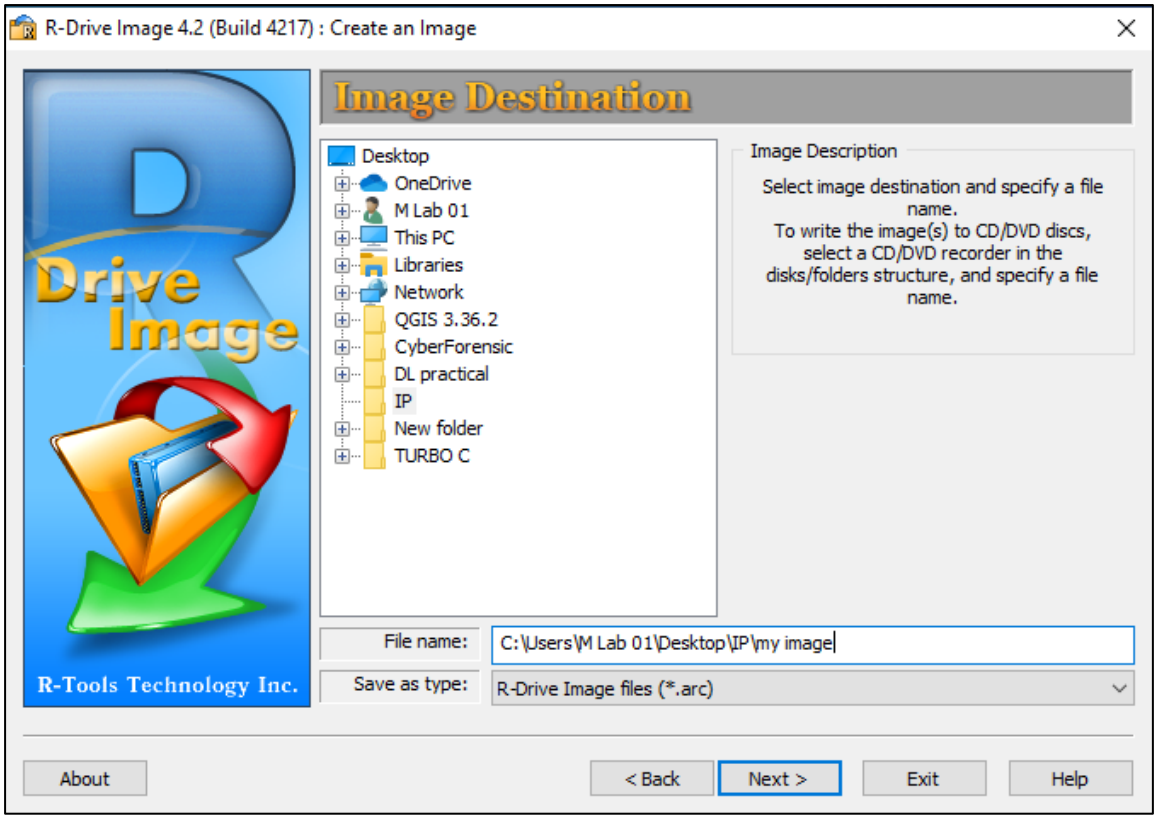


**Click on PARTITION SELECTION → Next**

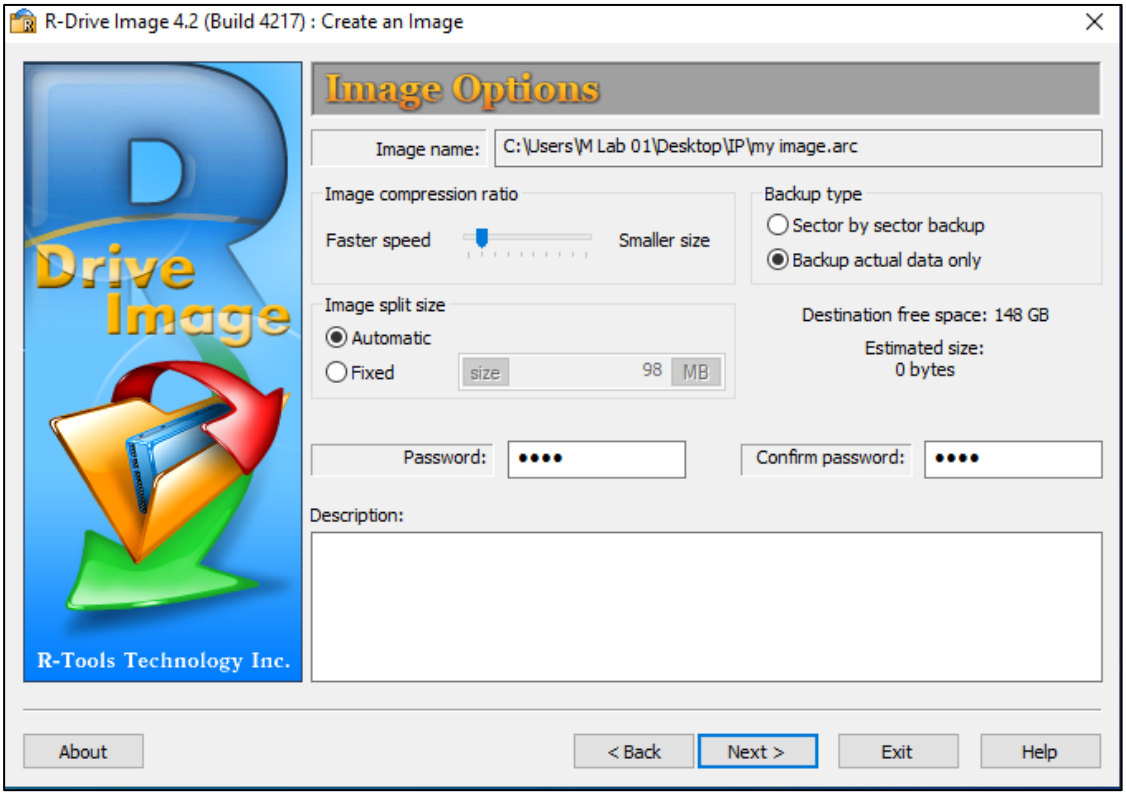



**Click on IMAGE DESTINATION → Type FILE NAME → Next**

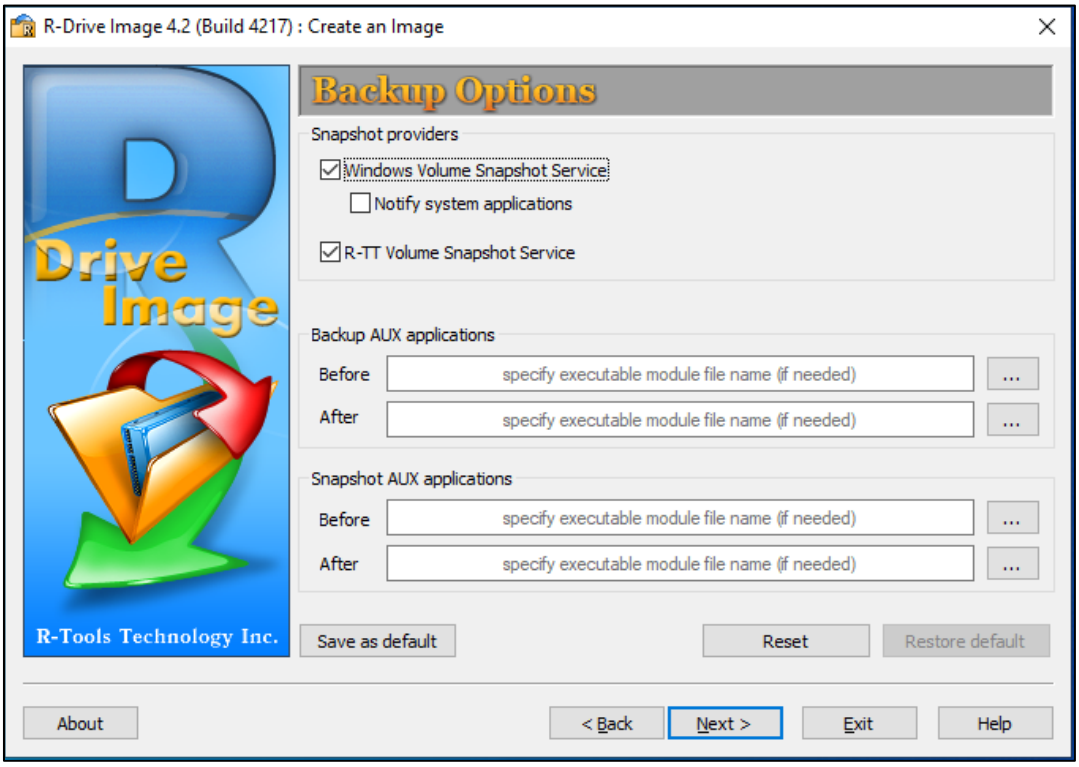




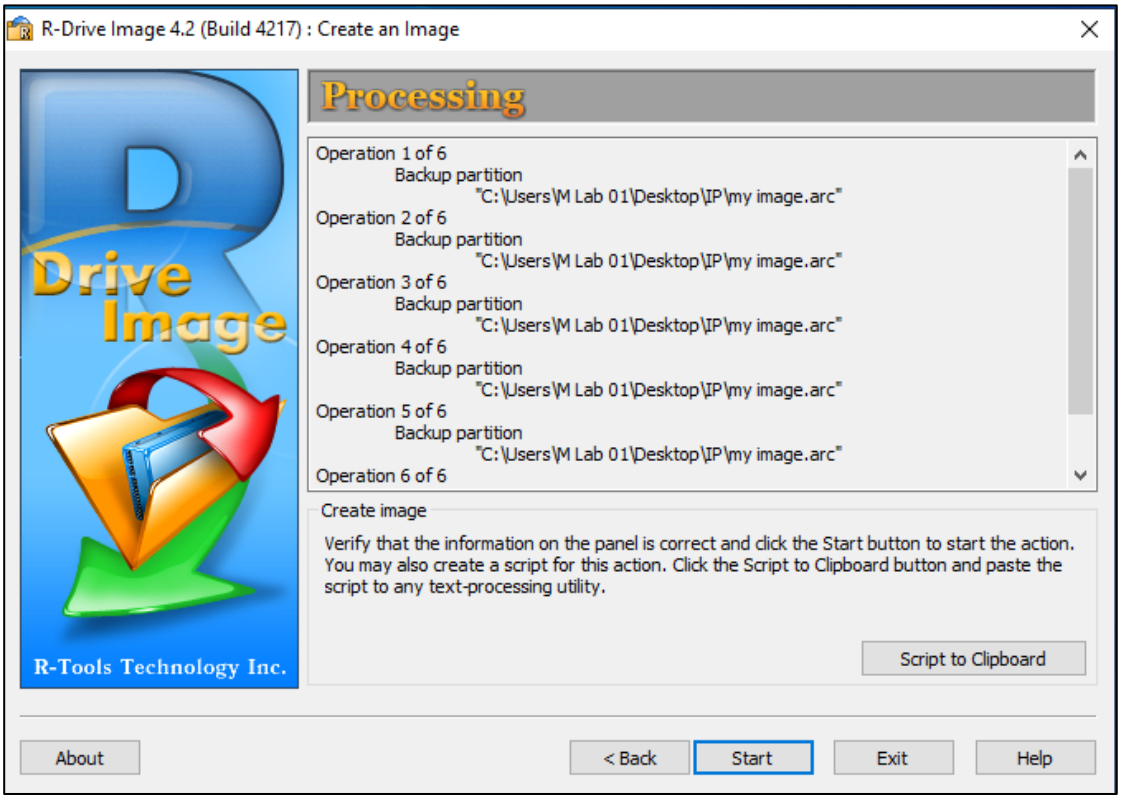

**Click on IMAGE OPTION → Set a PASSWORD → Next**



**Click on BACKUP OPTIONS → Save as Default → Next**

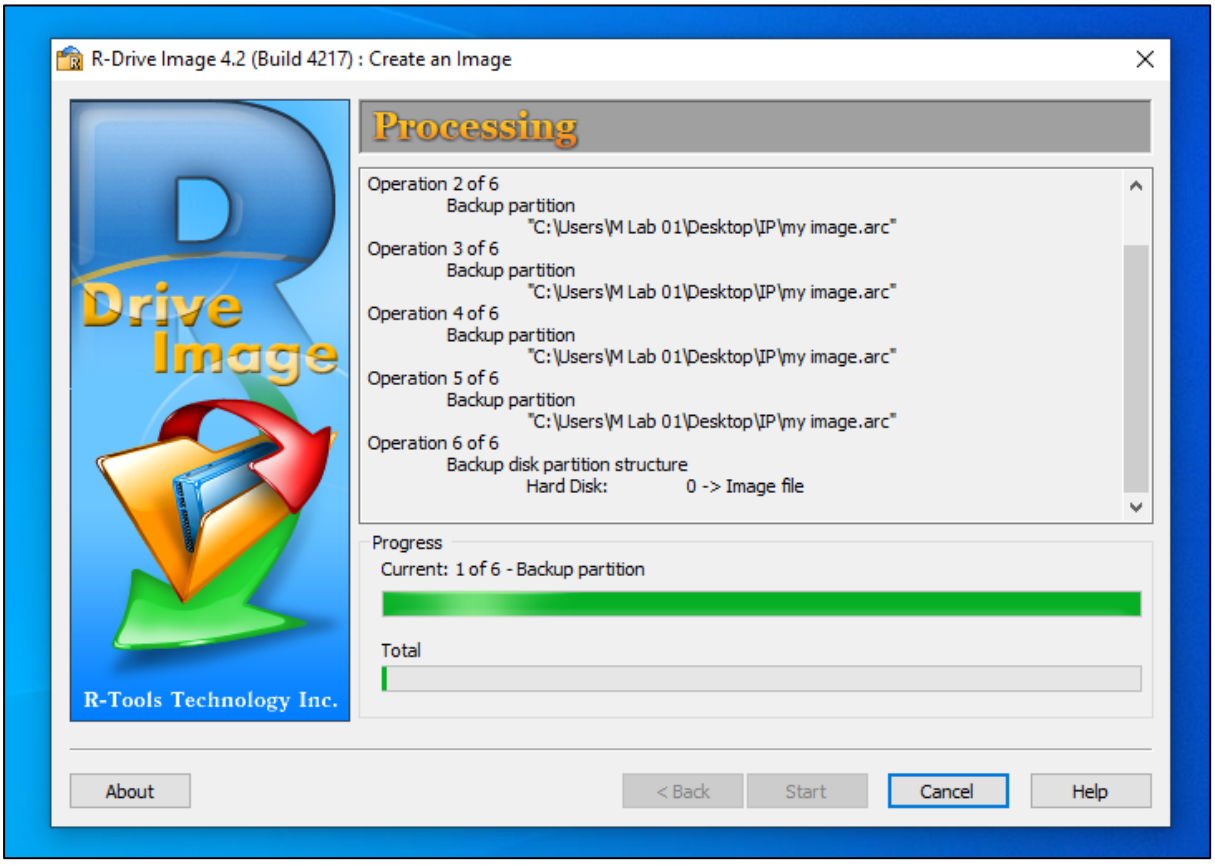



**Click on START**



## OUTPUT SLIDE:

**After Completion of Loading → IMAGE FILE IS CREATED**

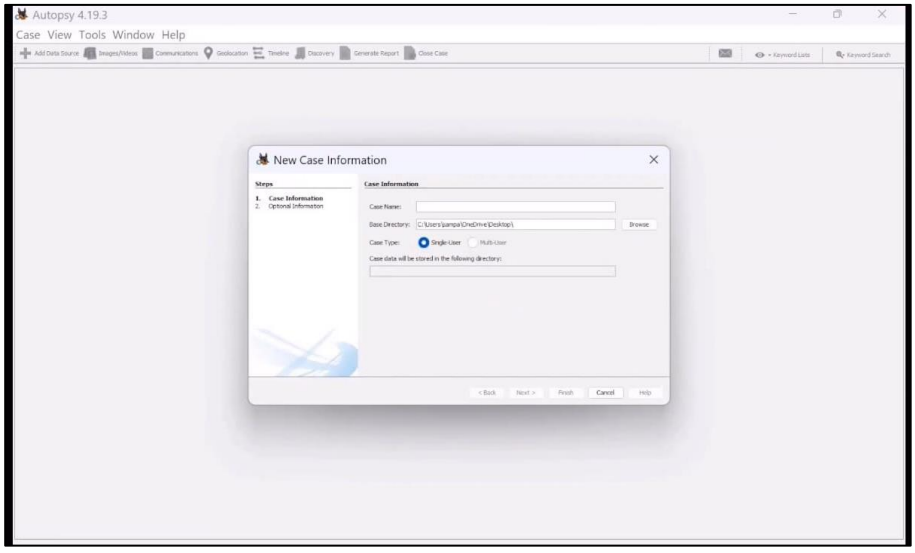


# MOBILE FORENSICS

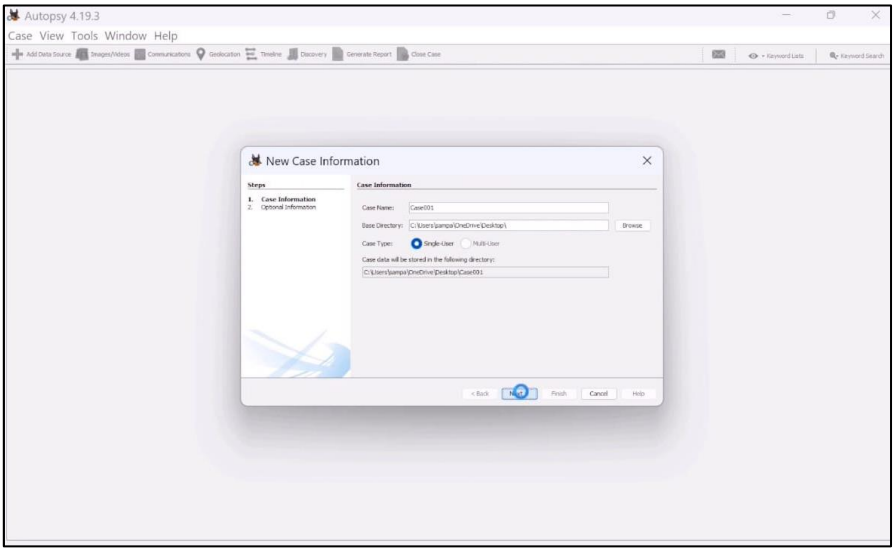
## a) Analysing the Forensic Image and Carving the Deleted Files Using Autopsy.

**Go to Google → Download AUTOPSY**

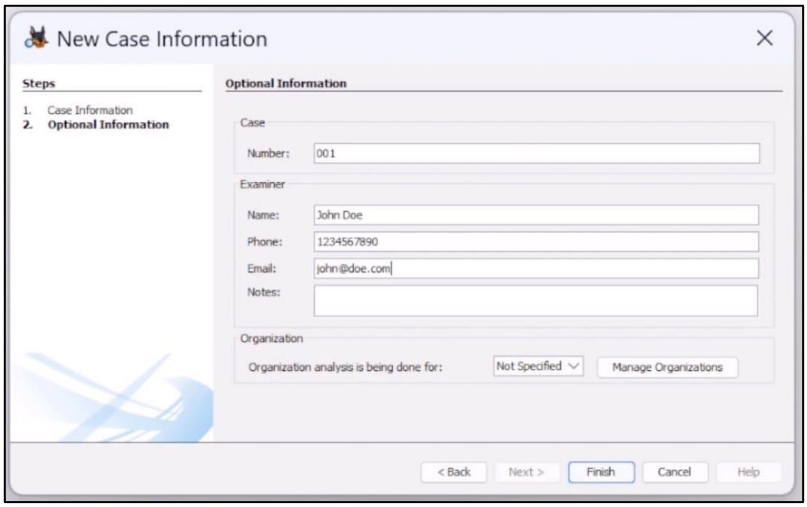

**Open the AUTOPSY → Create a NEW CASE**



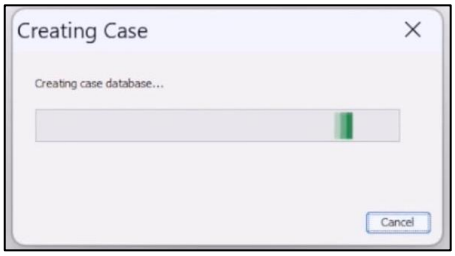
**Write down the CASE NAME → Browse the DIRECTORY → Next**



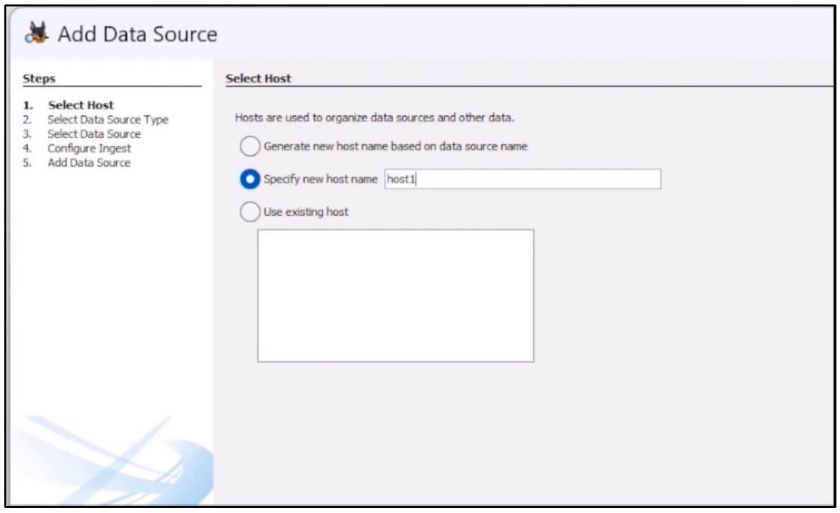

**Fill all the INFORMATION → Click on Finish**



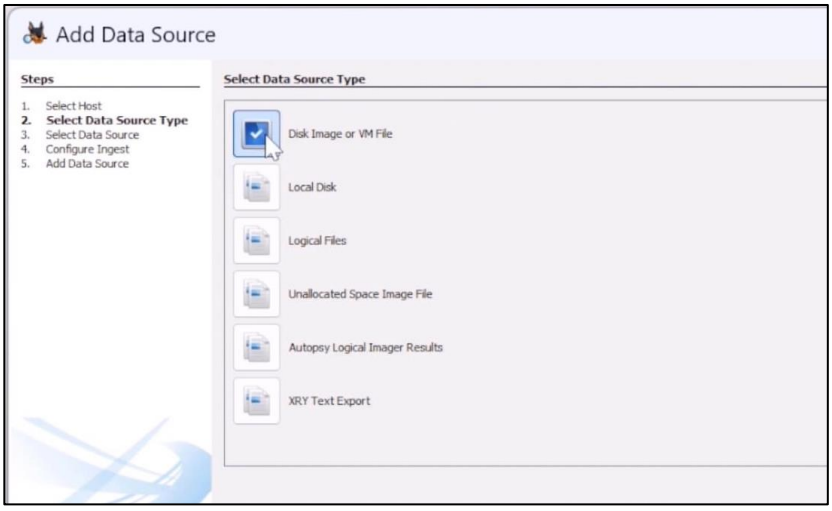

**Creation Case → Loading**



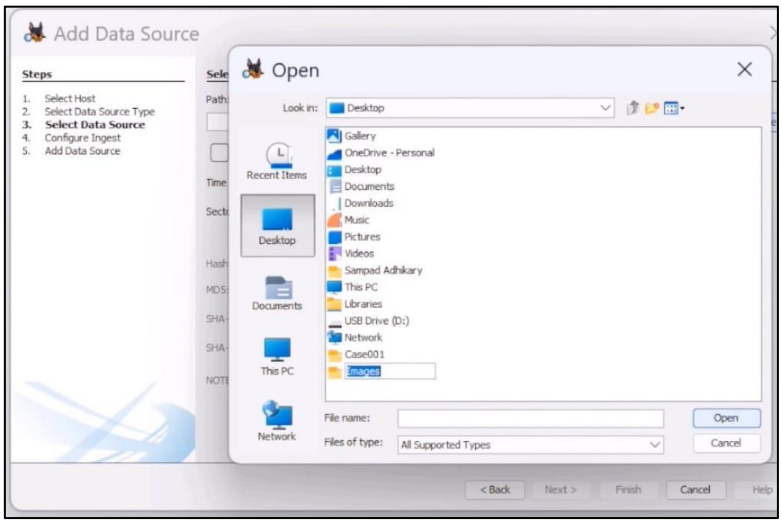
**Add DATA SOURCE → Select Host → Type HOST NAME → host1 → Next**



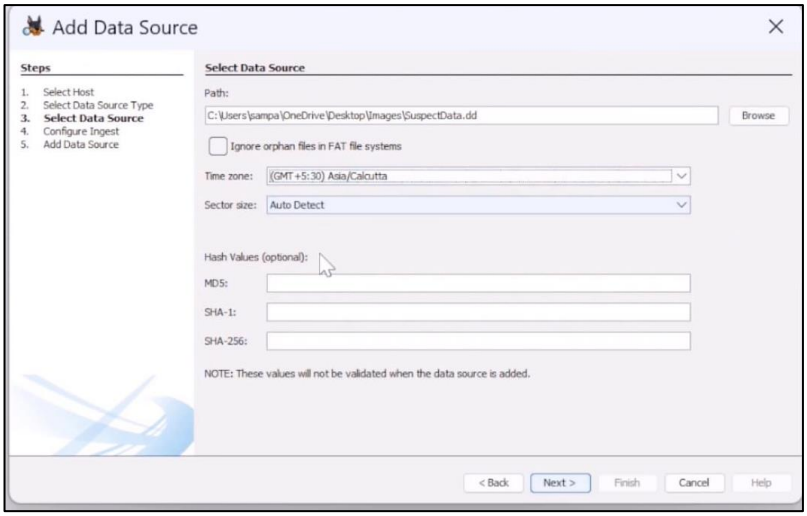

**Click on Disk Image or VM File → Next → Browse**



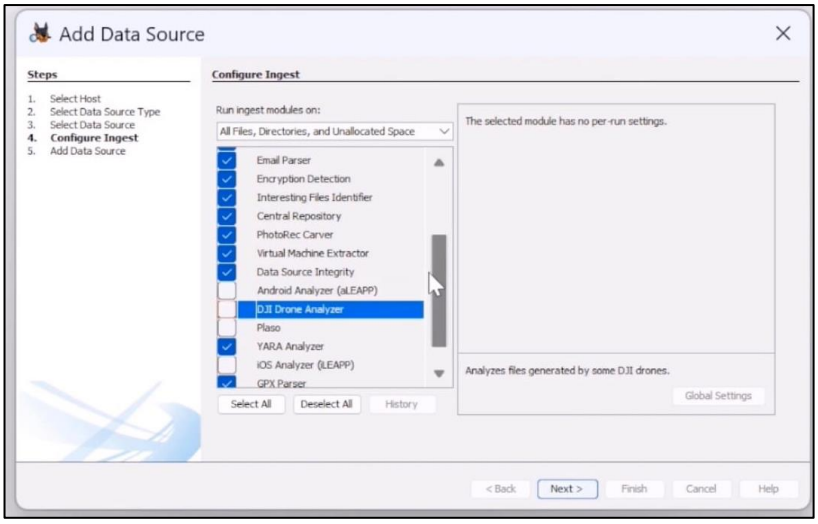

**Select IMAGE Folder on Desktop → Select IMAGE File → Click on Open**



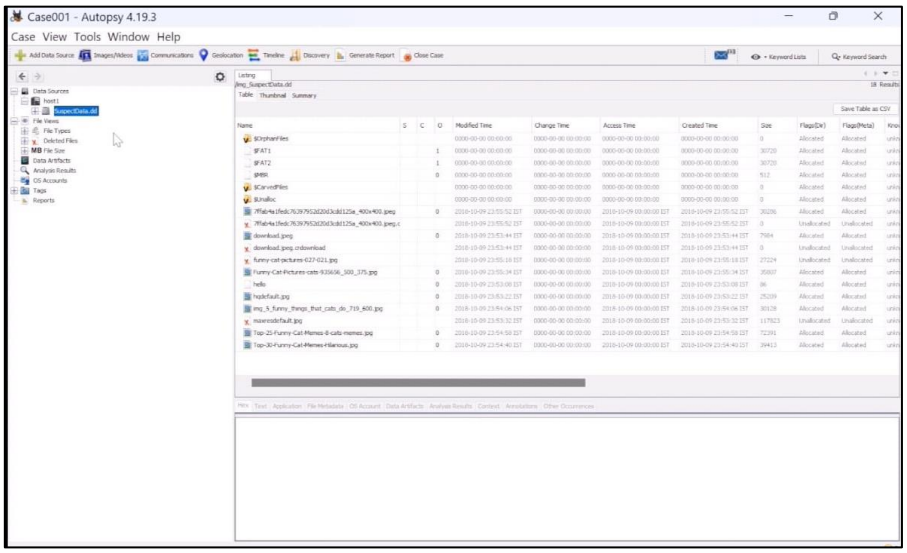
**Change the TIME ZONE → Next**



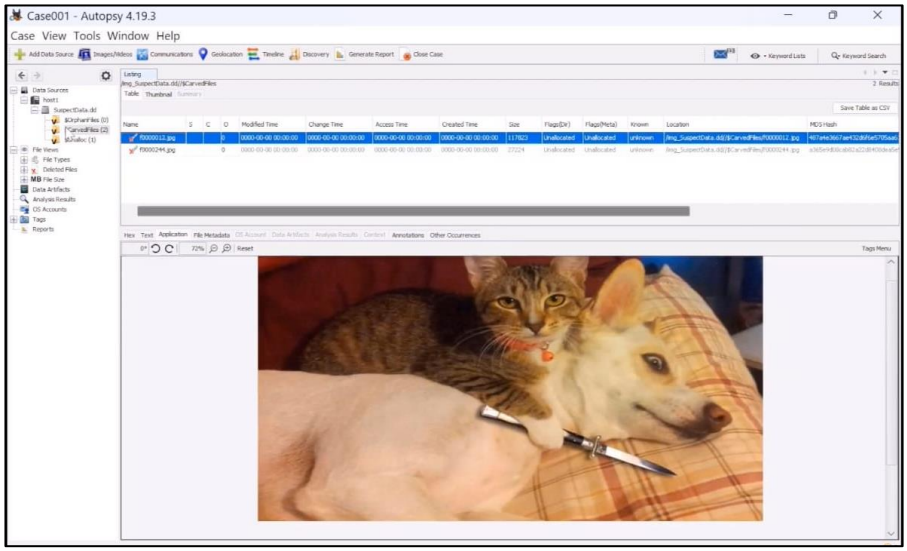

**Un Select the Unnecessary MODULE → Next → Finish**




**Goto HOST1 File → Click on + sign → Select Main FILE FOLDER → Open the IMAGES**



## OUTPUT SLIDE:




Click on Generate Report Menu Bar → Next → Next → Finish