PALLAVI ENGINEERING COLLEGE
Kuntloor(V), Abdullapurmet(M), Hyderabad, R.R. Dist. - 501 505.
Affiliated to JNTUH, Hyderabad & Approved by the AICTE, New Delhi
NAAC Accredited with "A" grade, Certified by ISO 9001:2015, ISO 14001:2015 & ISO 50001:2018
http://www.pallaviengineeringcollege.ac.in

Department of CSE-CYBER SECURITY

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS LAB

III B. Tech – II Semester

Branch: CSE-Cyber Security

Mr. SABAVATH RAJU

Assistant Professor

Pallavi Engineering College
Kuntloor(v), Abdullapurmet(M), Hyderabad, R.R. District

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS LAB

B.Tech. III Year II Sem. **L T P C**
0 0 3 1.5

Course Objectives:

1. To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices, emails, browsers, and mobile devices using different Forensics tools.
2. To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis.
3. Understand some of the tools of e-discovery.
4. To understand the network analysis, Registry analysis and analyze attacks using different forensics tools.

Course Outcomes:

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing.
2. To learn the file system storage mechanisms and retrieve files in hidden format.
3. Learn the use of computer forensics tools used in data analysis.
4. Learn how to find data that may be clear or hidden on a computer disk, find out the open ports for the attackers through network analysis, Registry analysis.

List of Experiments

1. **Perform email analysis** using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders.
2. **Perform Browser history analysis** and get the downloaded content, history, saved logins, searches, websites visited etc using Foxton Forensics tool, Dumpzilla..
3. **Perform mobile analysis** in the form of retrieving call logs, SMS log, all contacts list using the forensics tool like SAFT.
4. **Perform Registry analysis** and get boot time logging using process monitor tool.
5. **Perform Disk imaging and cloning** using the X-way Forensics tools.
6. **Perform Data Analysis i.e** History about open file and folder, and view folder actions using Lastview activity tool.
7. **Perform Network analysis** using the Network Miner tool.
8. **Perform information for incident response** using the crowd Response tool.
9. **Perform File type detection using** Autopsy tool.
10. **Perform Memory capture and analysis** using the Live RAM capture or any forensic tool.

TEXT BOOKS:

1. Real Digital Forensics for Handheld Devices, E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

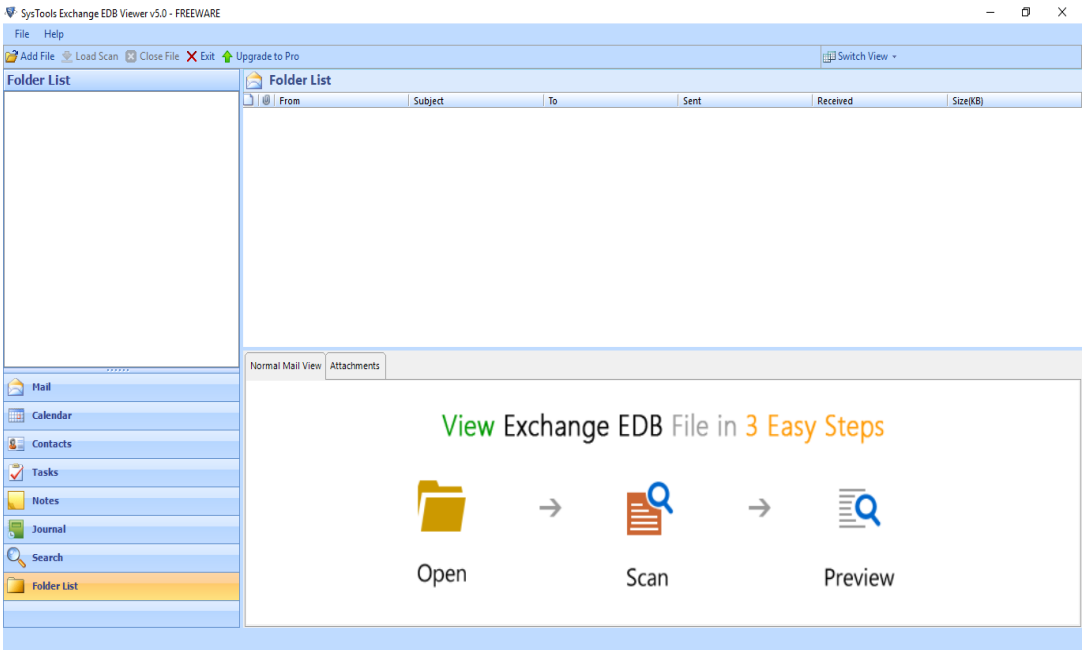
REFERENCE BOOKS:

1. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010.
2. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012.
3. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A.Reyes, Syngress, 2007.

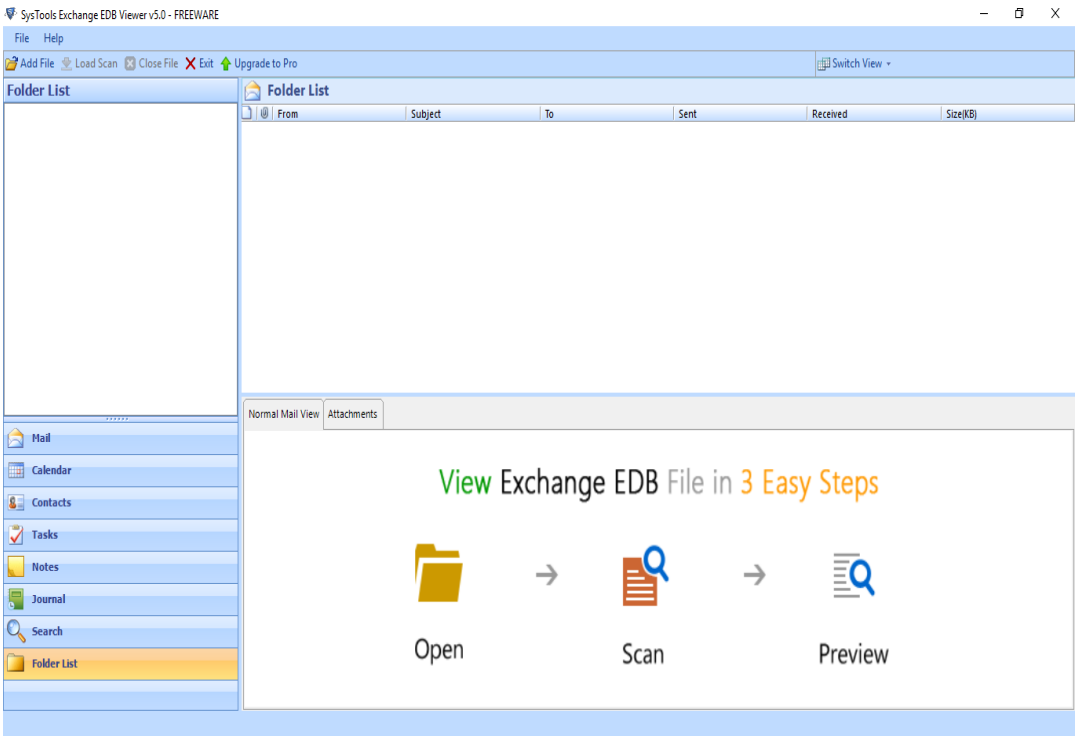
1. **Perform email analysis** using the tools like Exchange EDB viewer, MBOX viewer and View user mailboxes and public folders, Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders.

Solution:

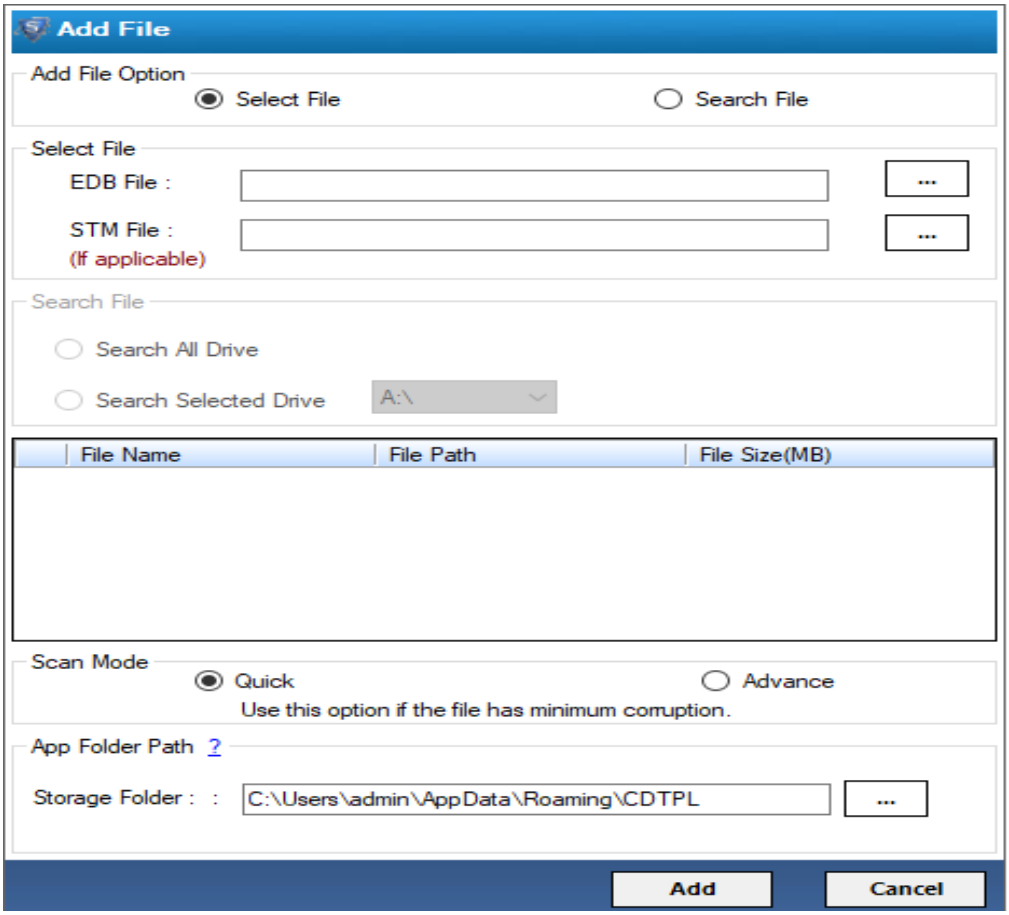
Open the **"SysTools Exchange EDB Viewer"** Application:



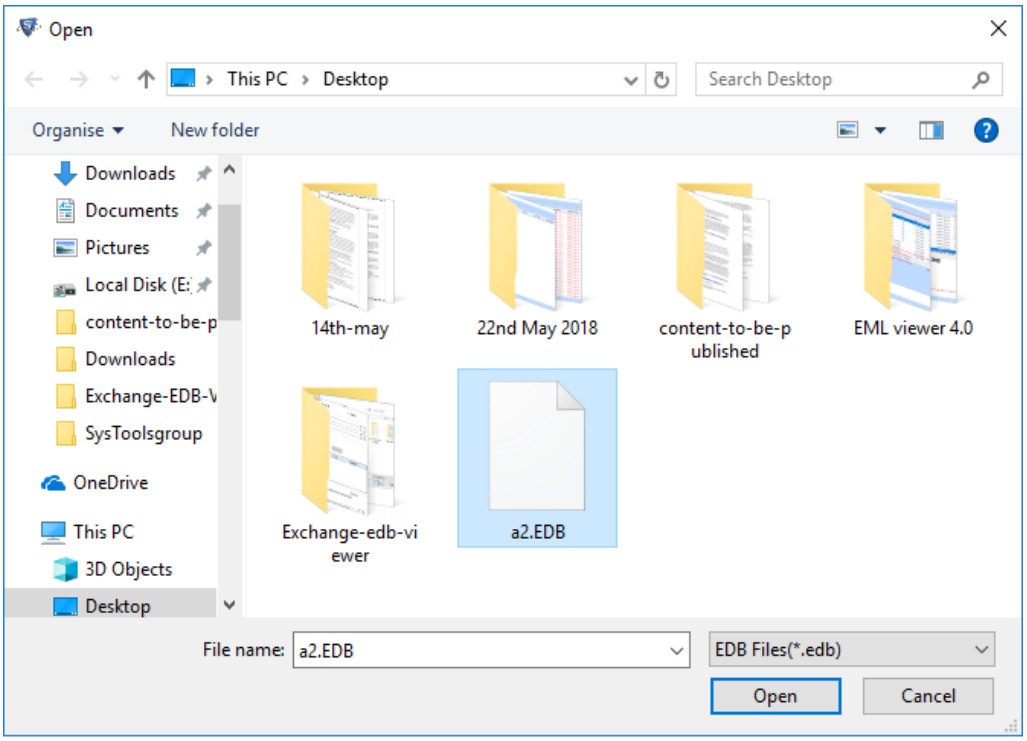
Click on the "**Add File**" button:



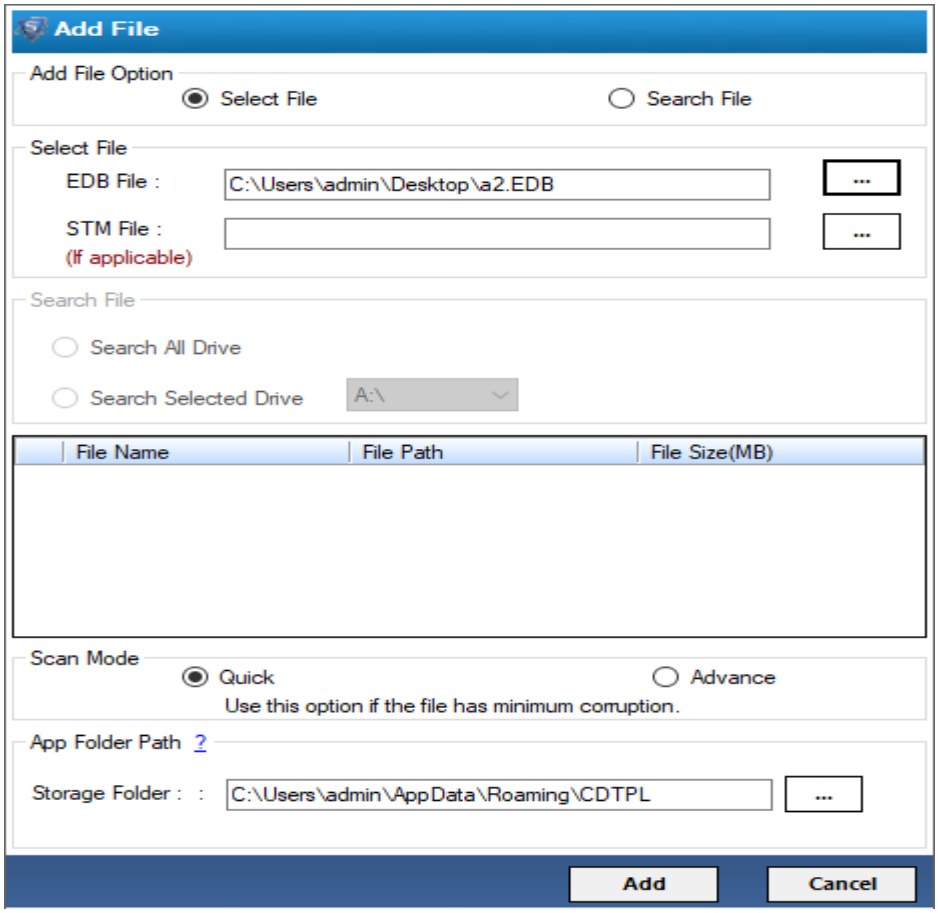
Click on the button "**...**" button.



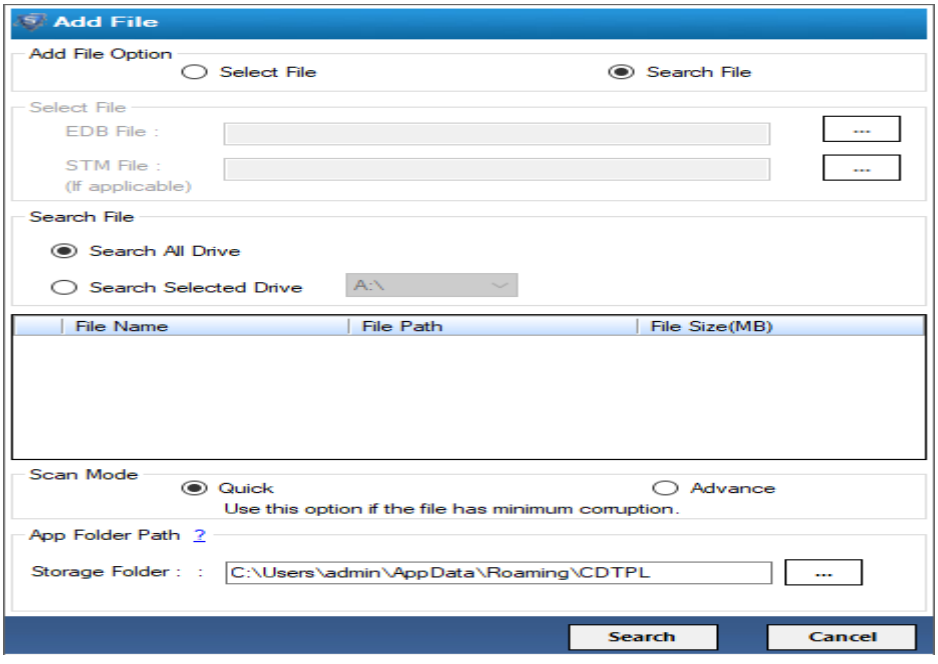
Navigate and select the EDB file, Click on the "**Open**" button.



Location of the file will be shown as follows:

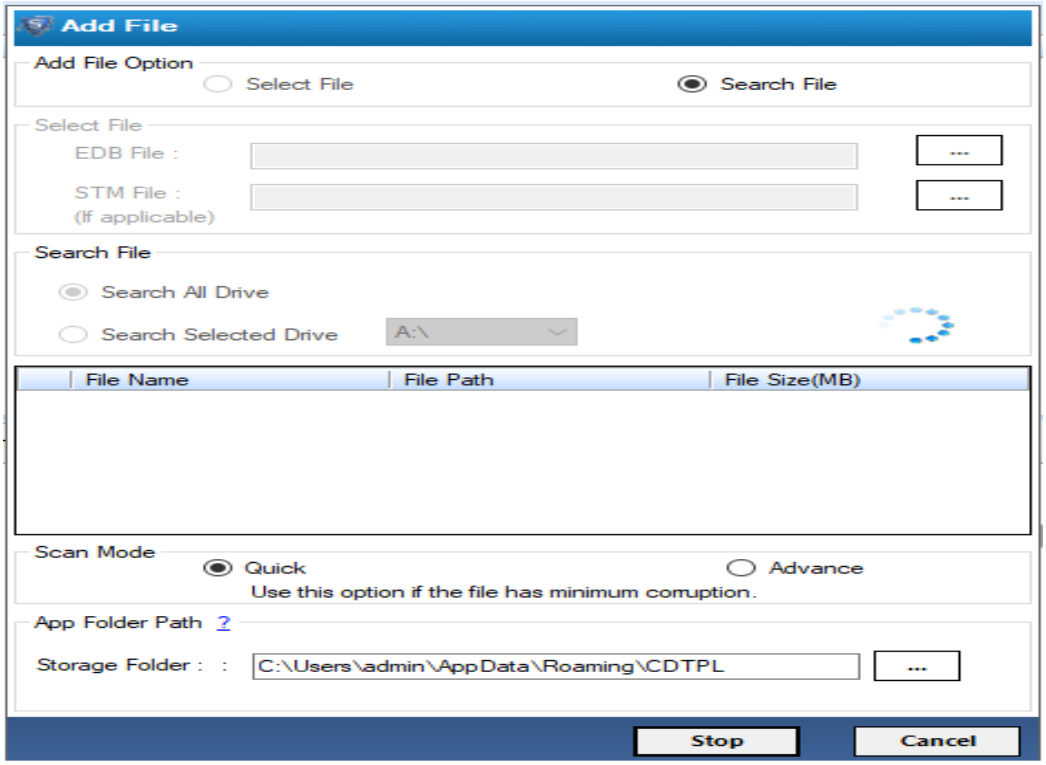


Click on the "**Search File**" radio button.



Search All Drive: Search for all drive on the computer for EDB files.

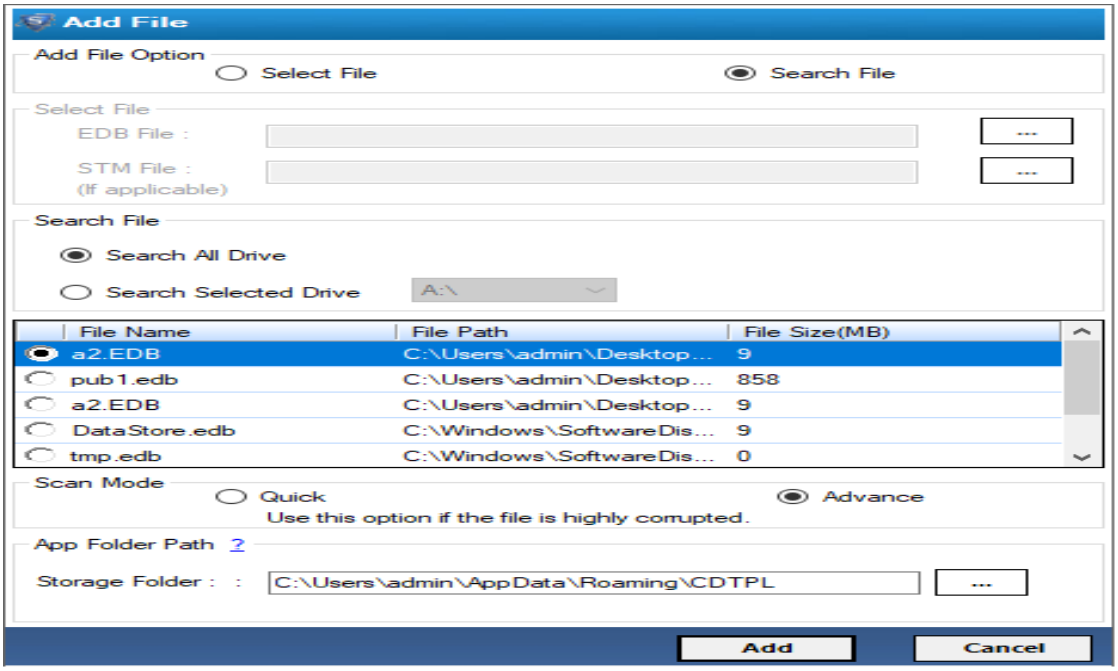
Search Selected Drive: Search the selected drive for the EDB files.



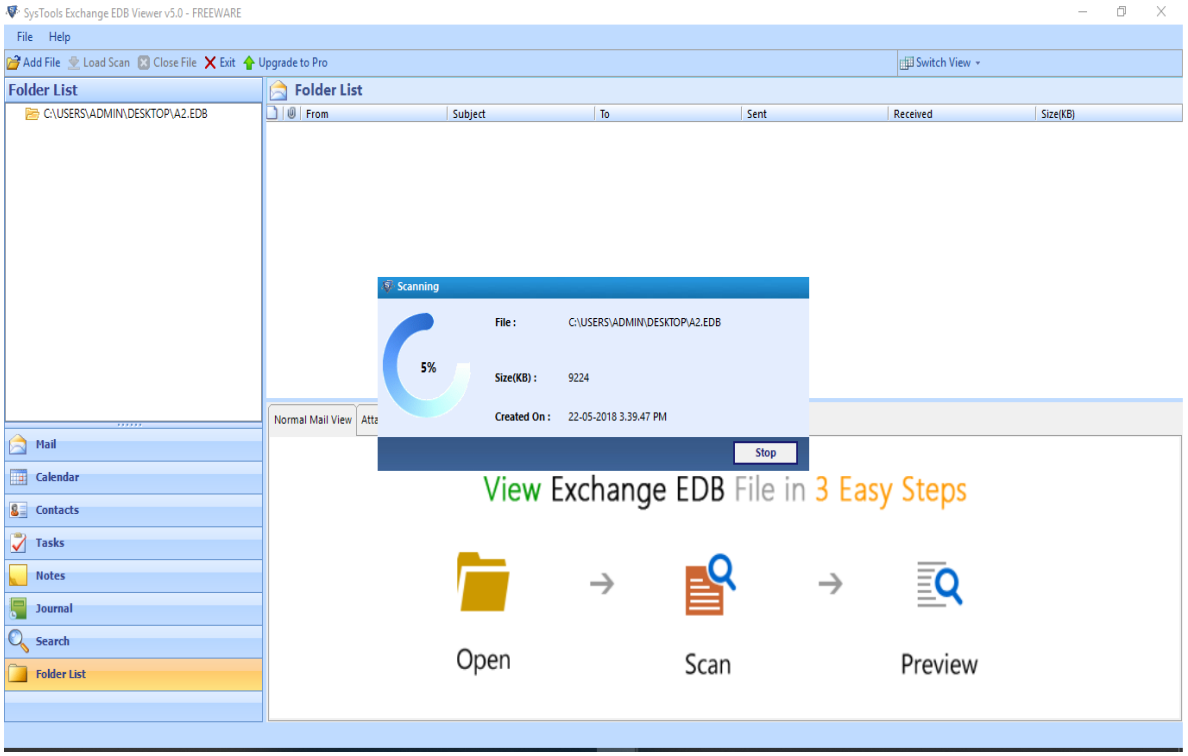
Quick Scan: Save time by quickly scanning the file; if it is not corrupt.

Advance Scan: Select this mode if the EDB file is severely corrupt.

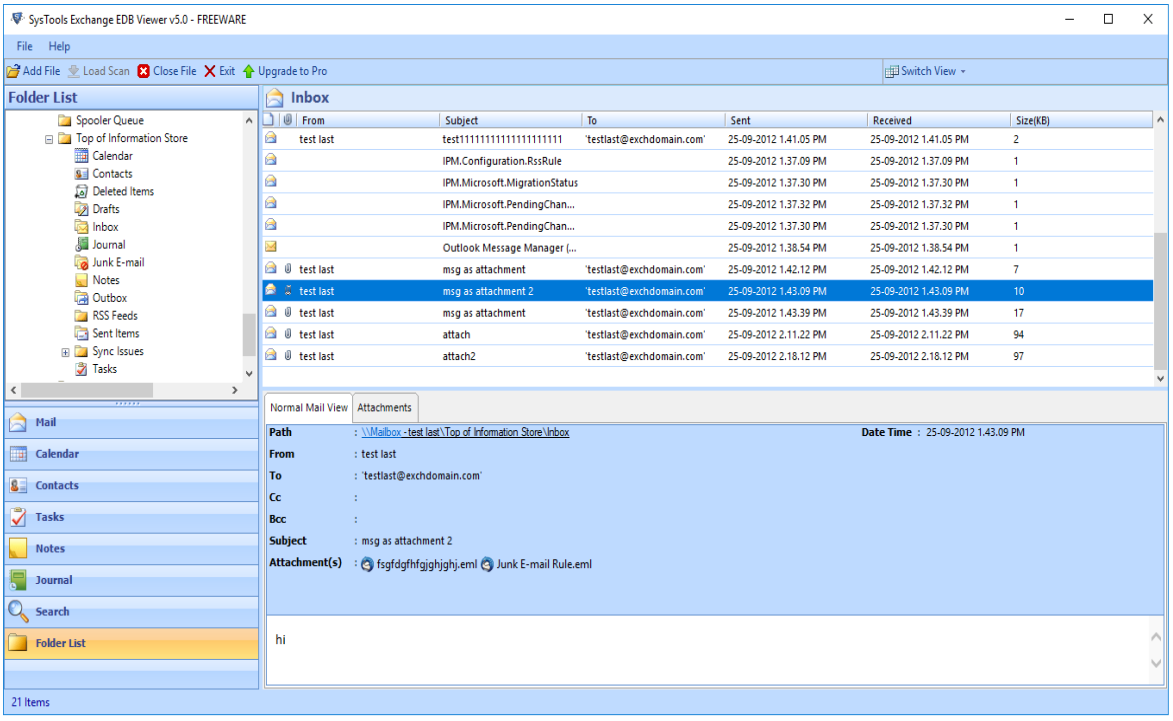
Click on the "**Add**" button to complete the adding process.



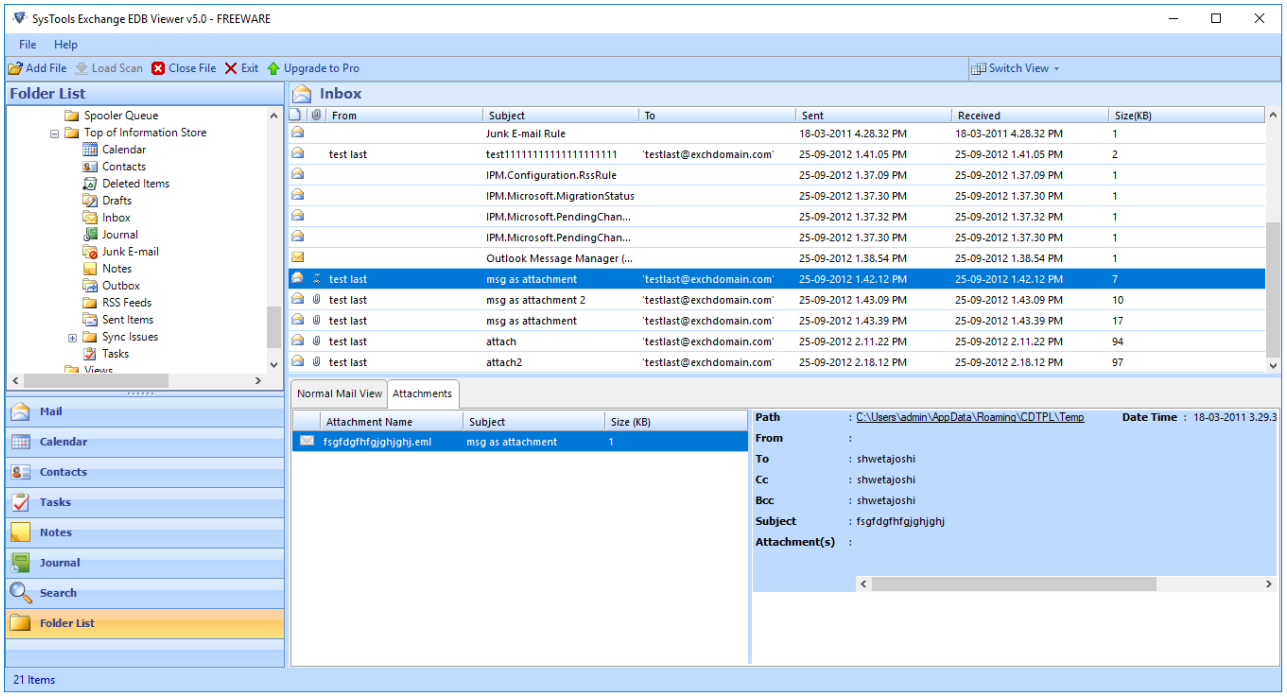
The software will start the process to add the files:



The software will preview the data in the EDB file format:



The software will also show the attachments of the added EDB file:

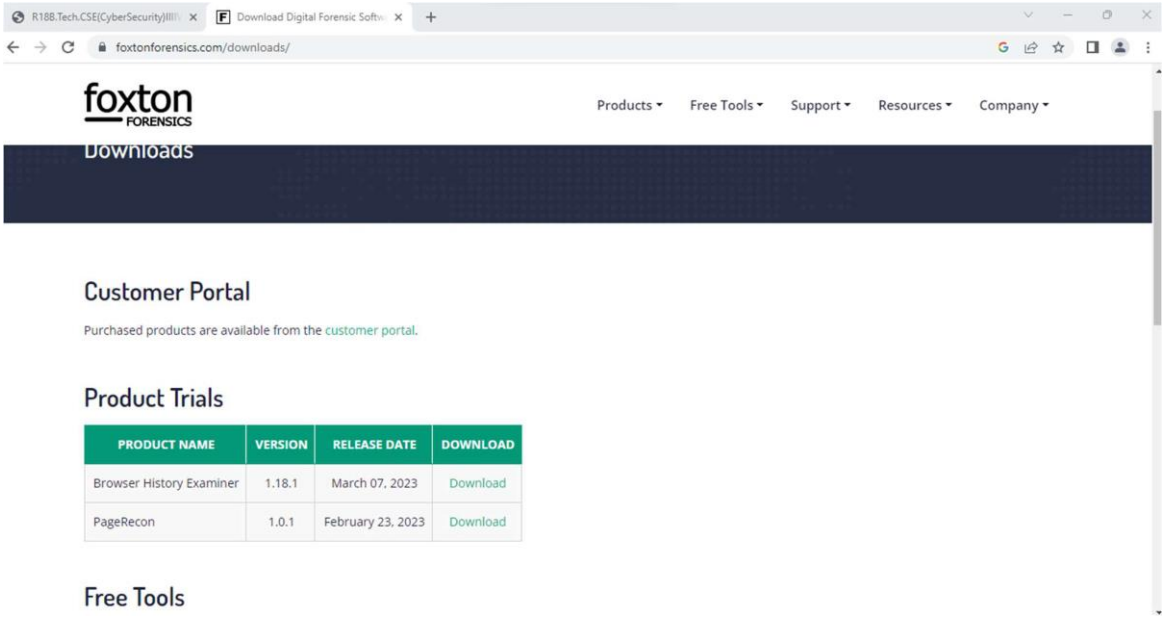


2. **Perform Browser history analysis and get the downloaded content, history, saved logins, searches, websites visited etc using Foxton Forensics tool, Dumpzilla.**

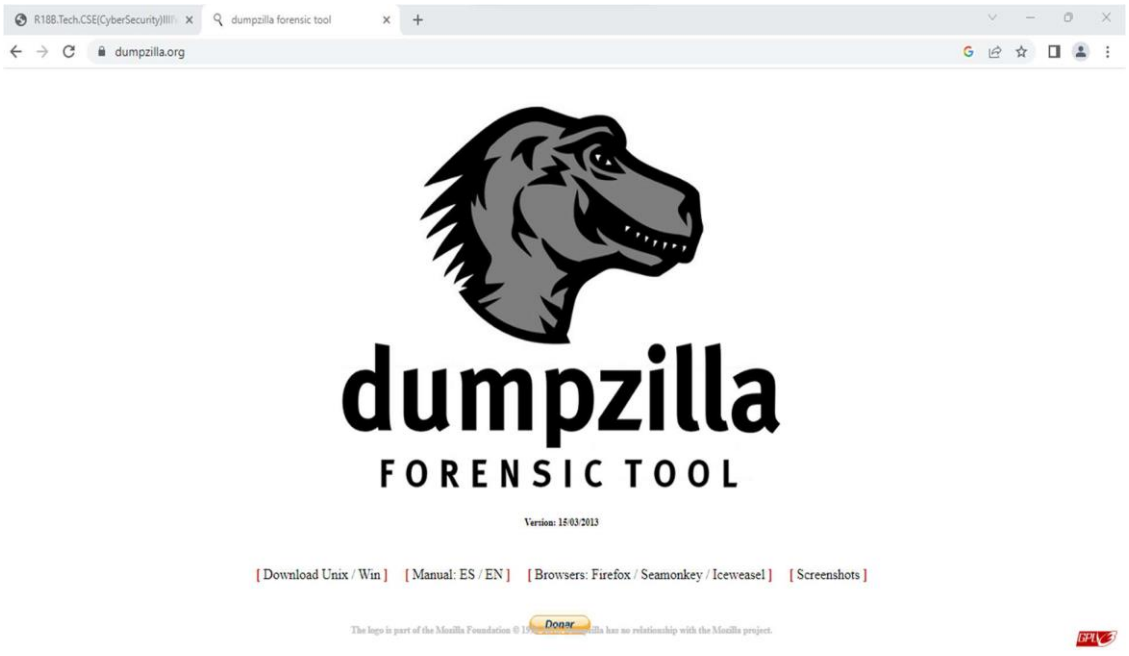
Solution:

Step 1: Download the Foxton Forensics tool and Dumpzilla.

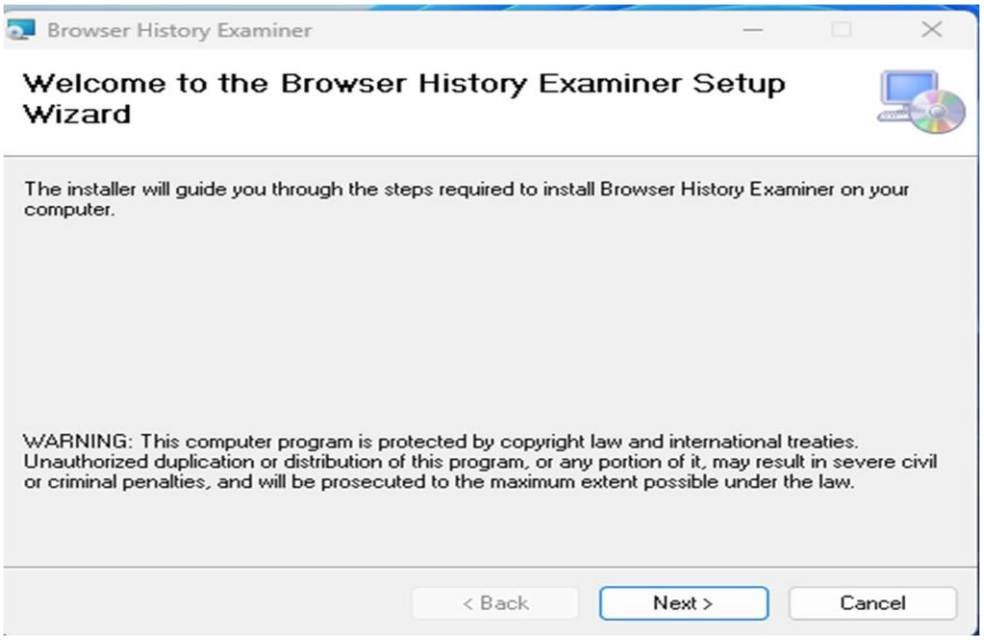
Download link: https://www.foxtonforensics.com/downloads/



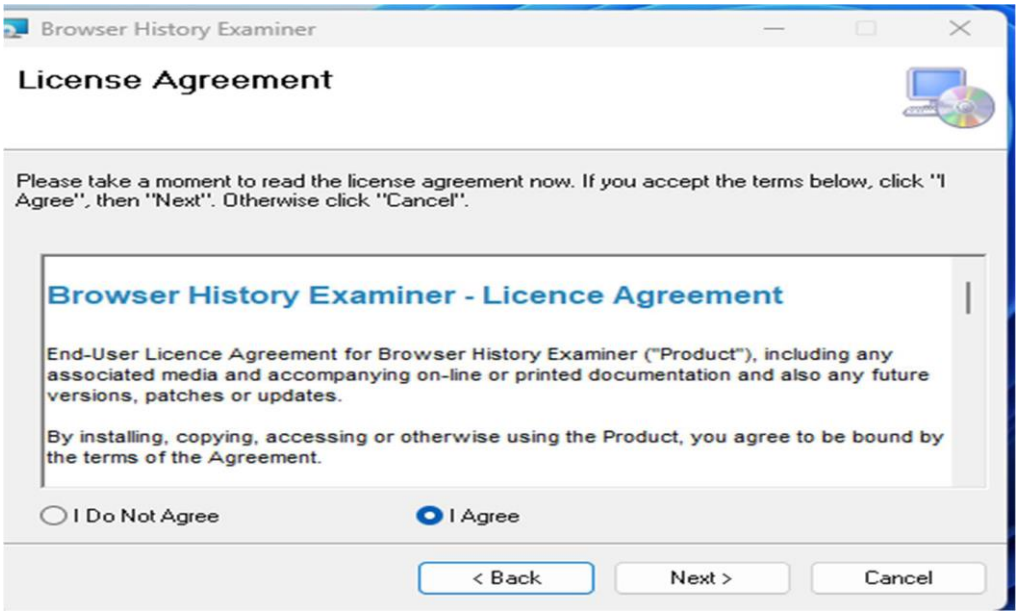
Download link: https://www.dumpzilla.org/



Step 2: Installation Process
Welcome to the Browser history Examiner setup wizard. Click on Next to continue



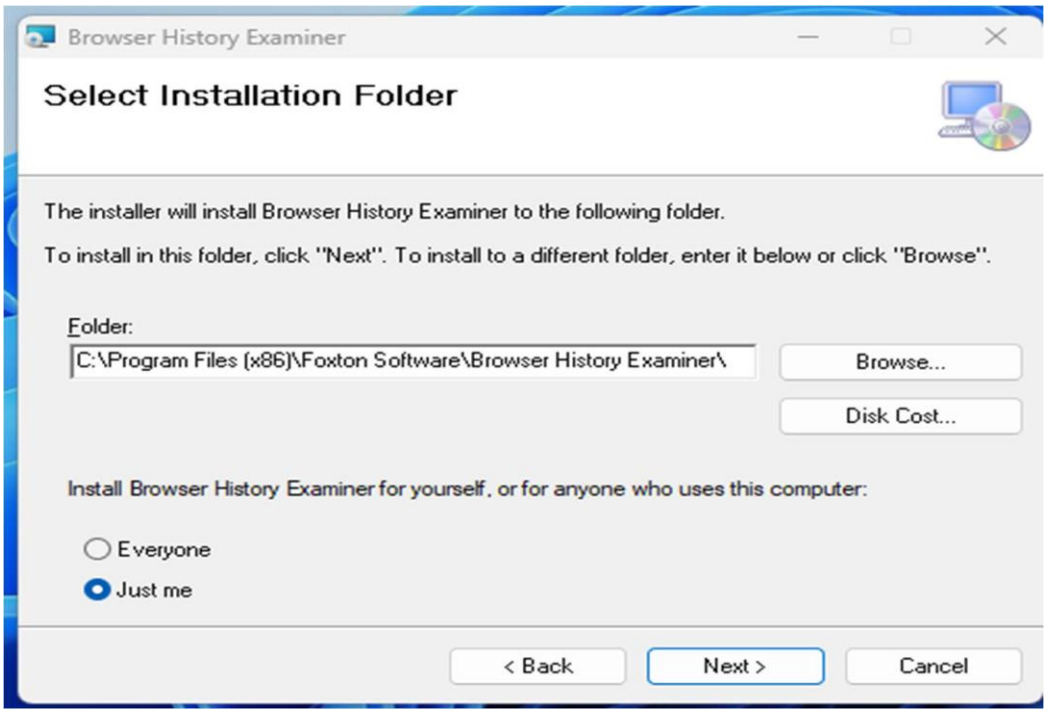
- After clicking on Next, the set up will offer you a License agreement and you have to I Agree that agreement to proceed further.



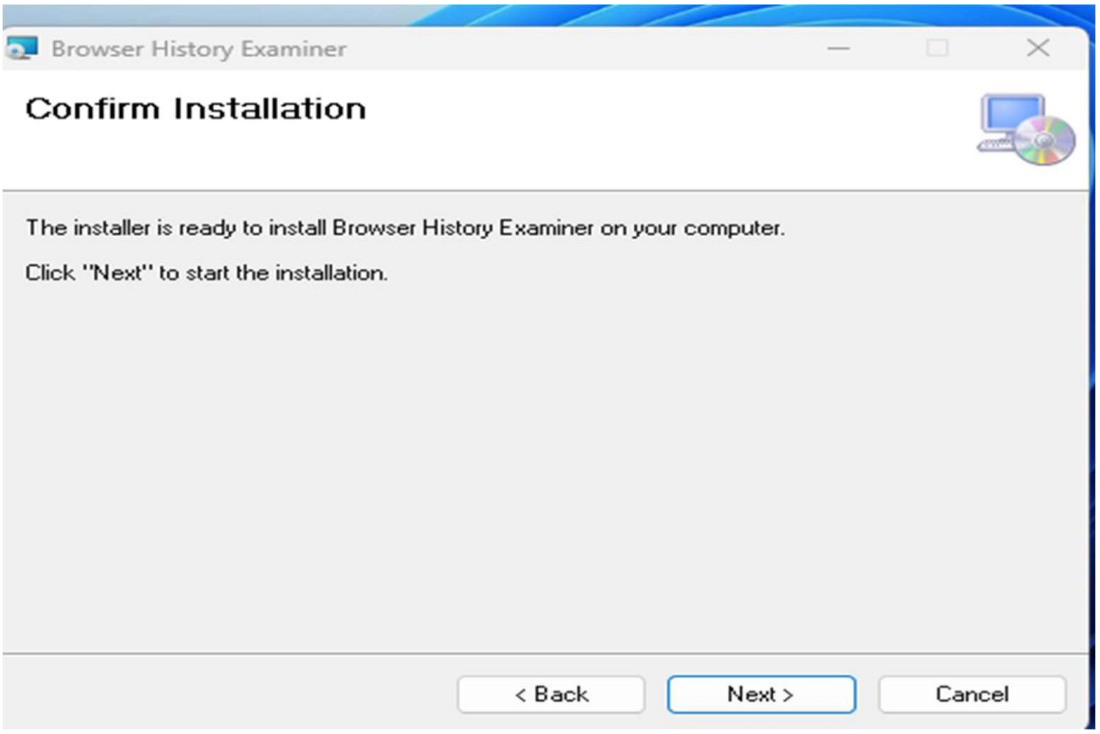
- Once you will I Agree the agreement, the next screen will let you select the Destination Location.

C:\Program Files (x86) \Foxton So□ware\Browser History Examiner\.

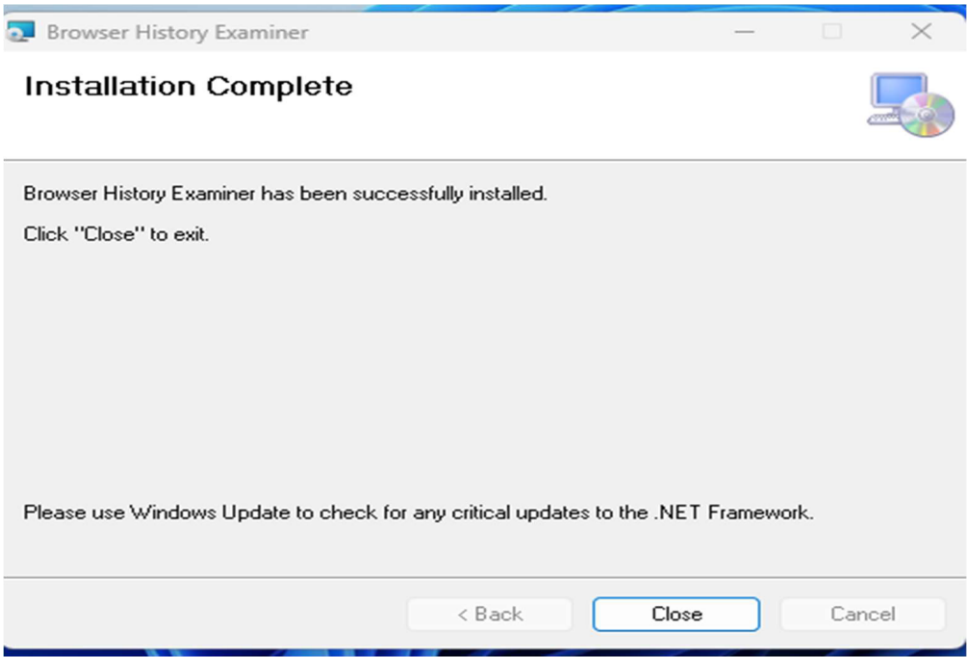
- If you would like to select a different folder. Click on Next.



- After pressing Next Button, you will get confirm to installation process.



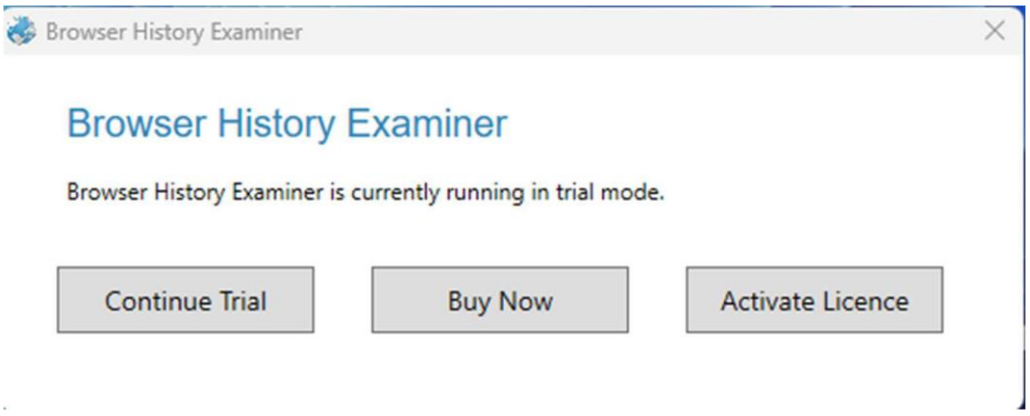
- After click next button Installation process started and after installation confirm installation press next button.



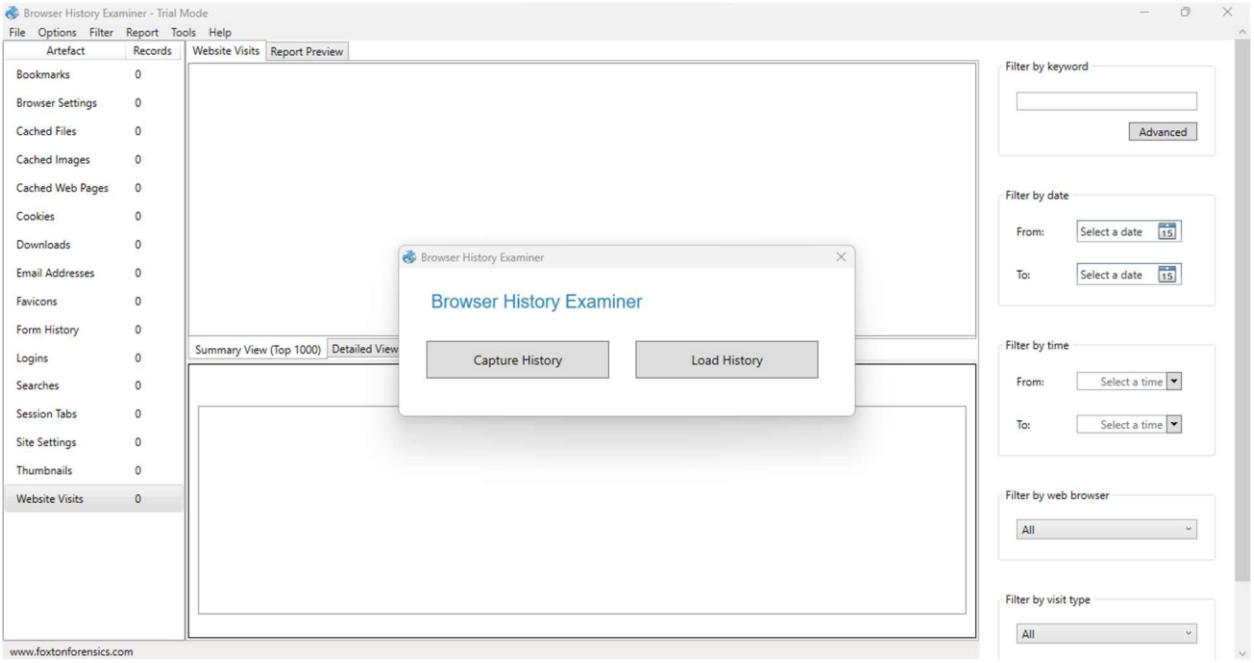
- After installation complete. Click “close to exit.

Step 1:
Press windows button search for browser history examiner and open.

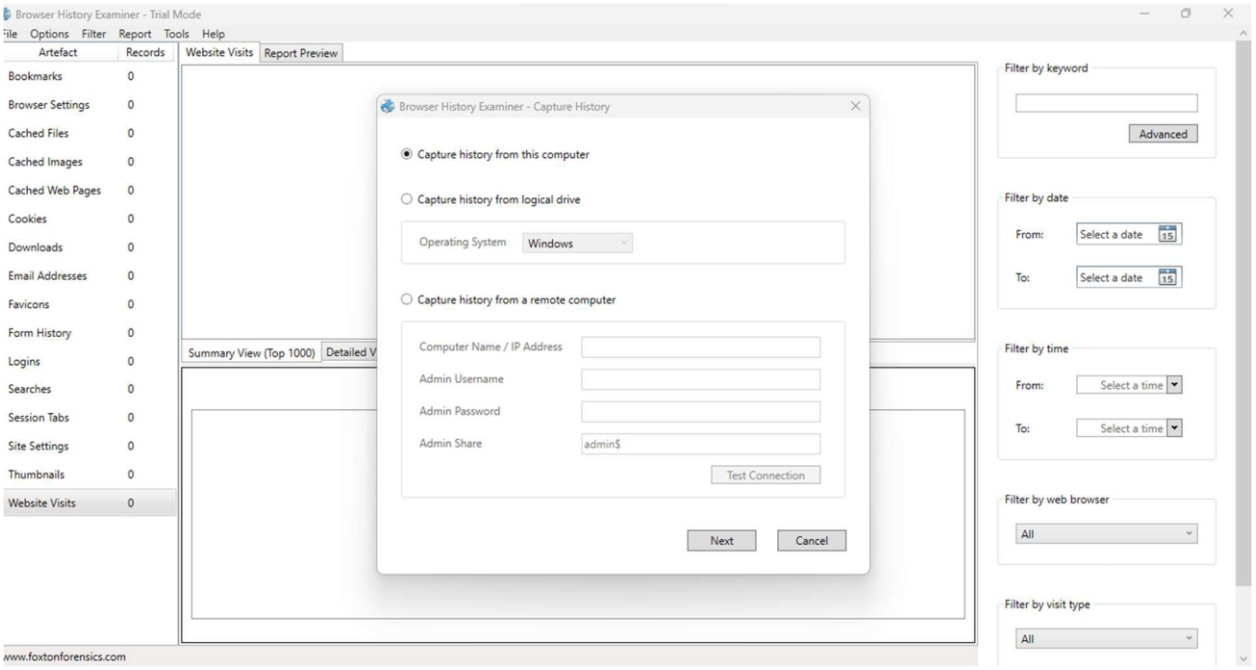
Step 2:
Click continue to trail



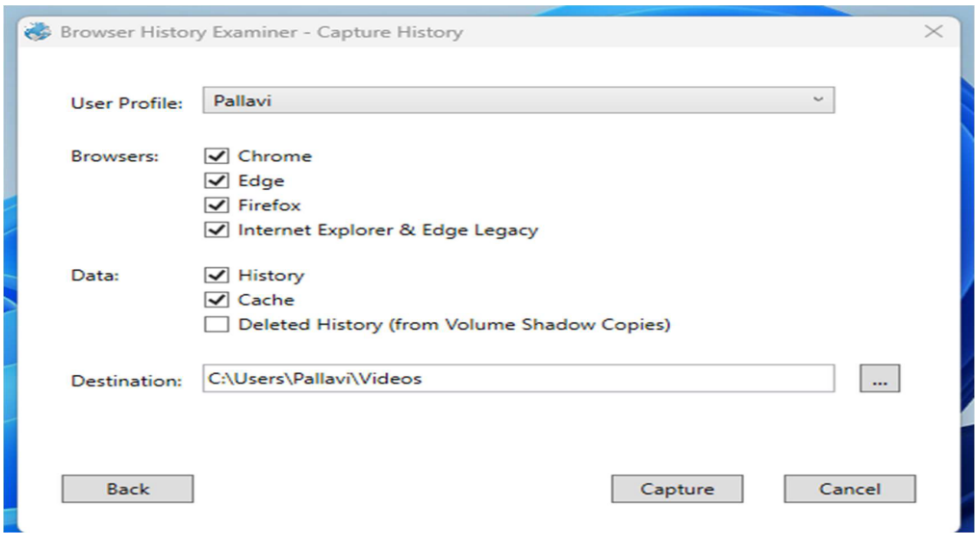
- After continue to trail version it displays



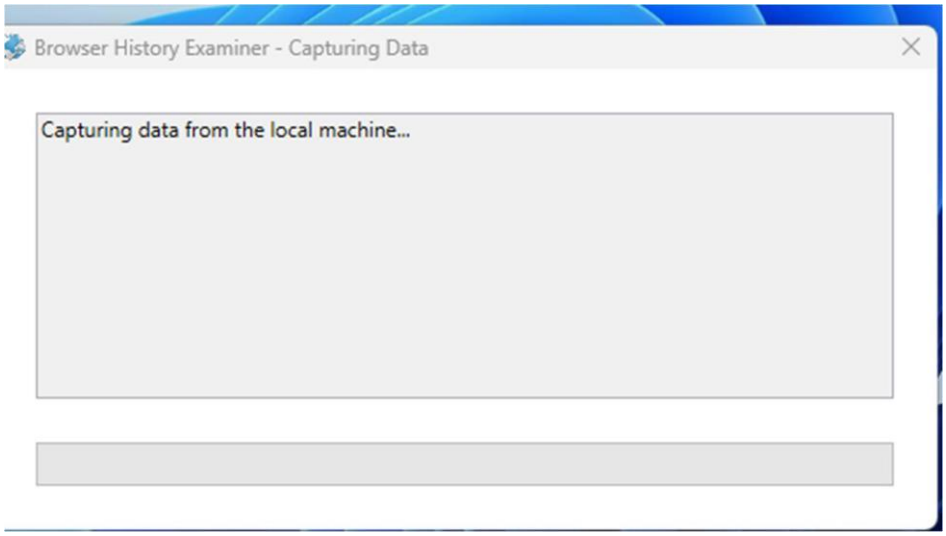
- After that click Capture History and continue.
- Select capture history from this computer and click next.

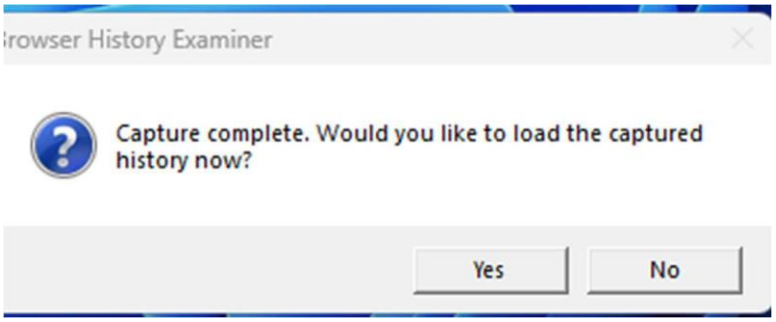


- After that asking destination location. Added the destination location



- After that click capture.





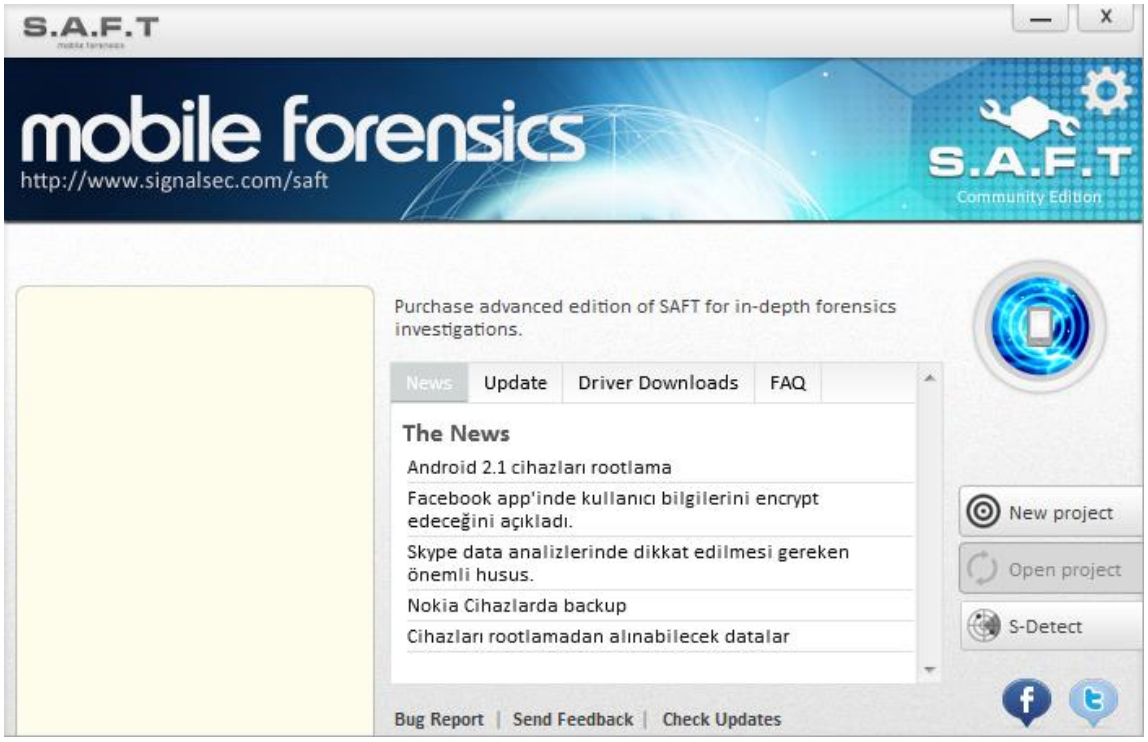
- After that Press “Yes”.
- Finally Check the Destination Folder for result.

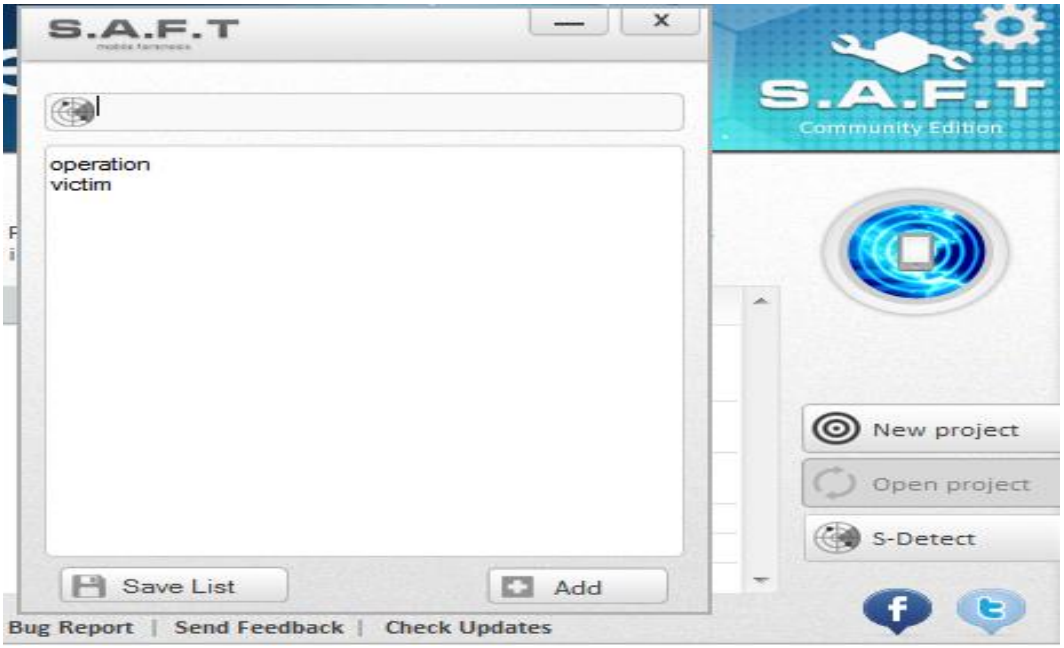
3. **Perform mobile analysis in the form of retrieving call logs, SMS log, and all contacts list using the forensics tool like SAFT.**

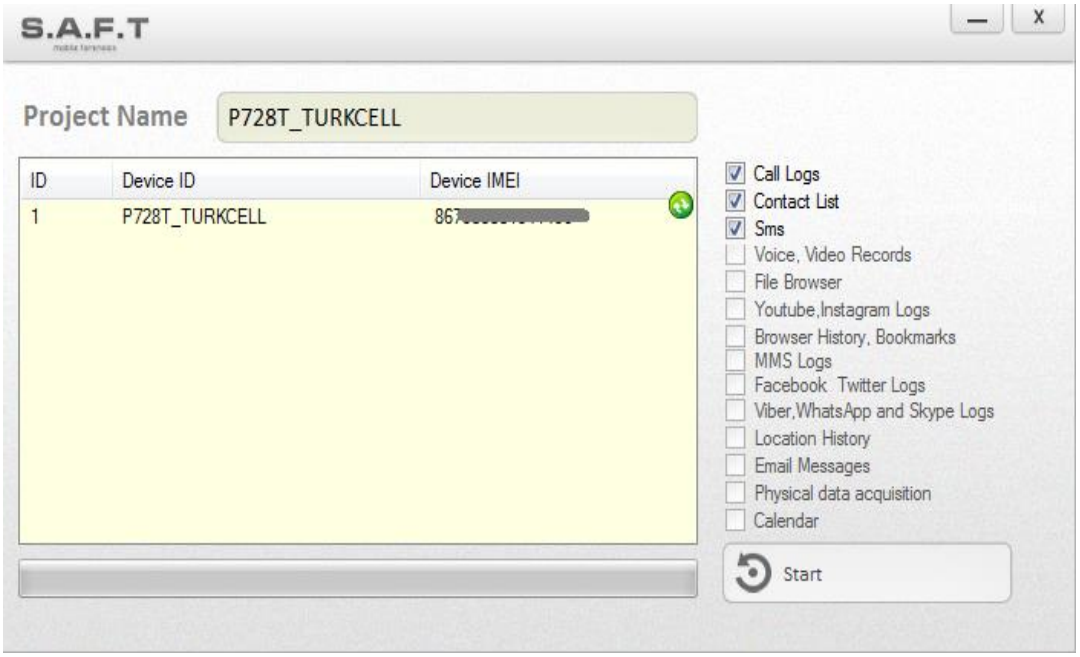
Solution:

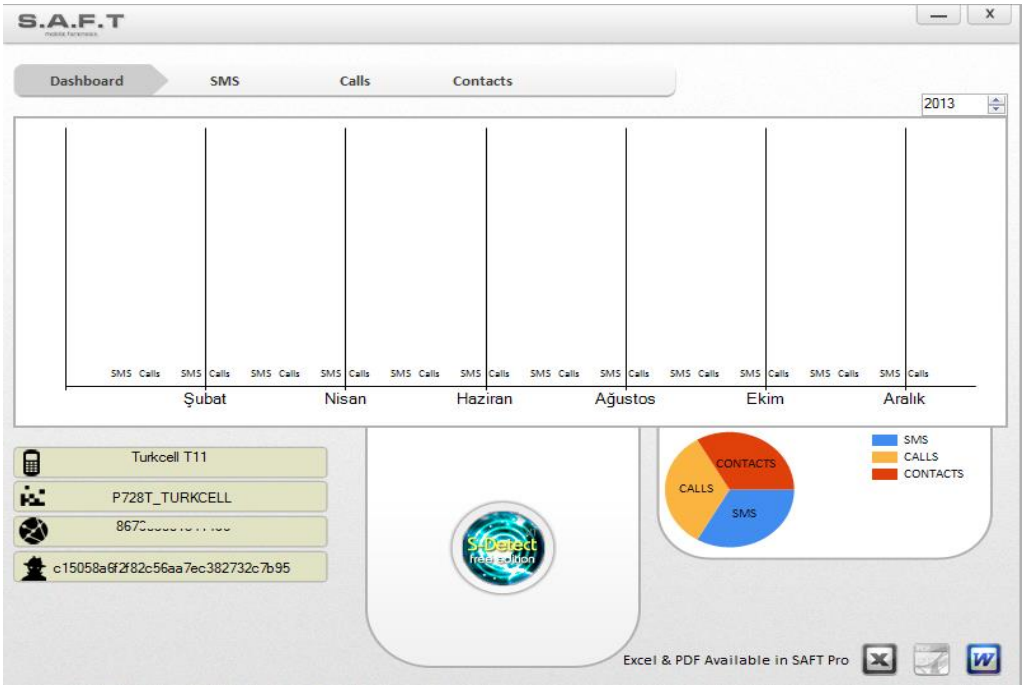
- **Install Software**
  Download SAFT installer and run it.
- **Connect Device**
  Be sure the phone is connected to computer via USB.
- **Create Project**
  Create a new project and select the forensics options.
- **It's done**
  All necessary data is extracted.
- **Analyze Results**
  Analyze the results and complete the investigation.

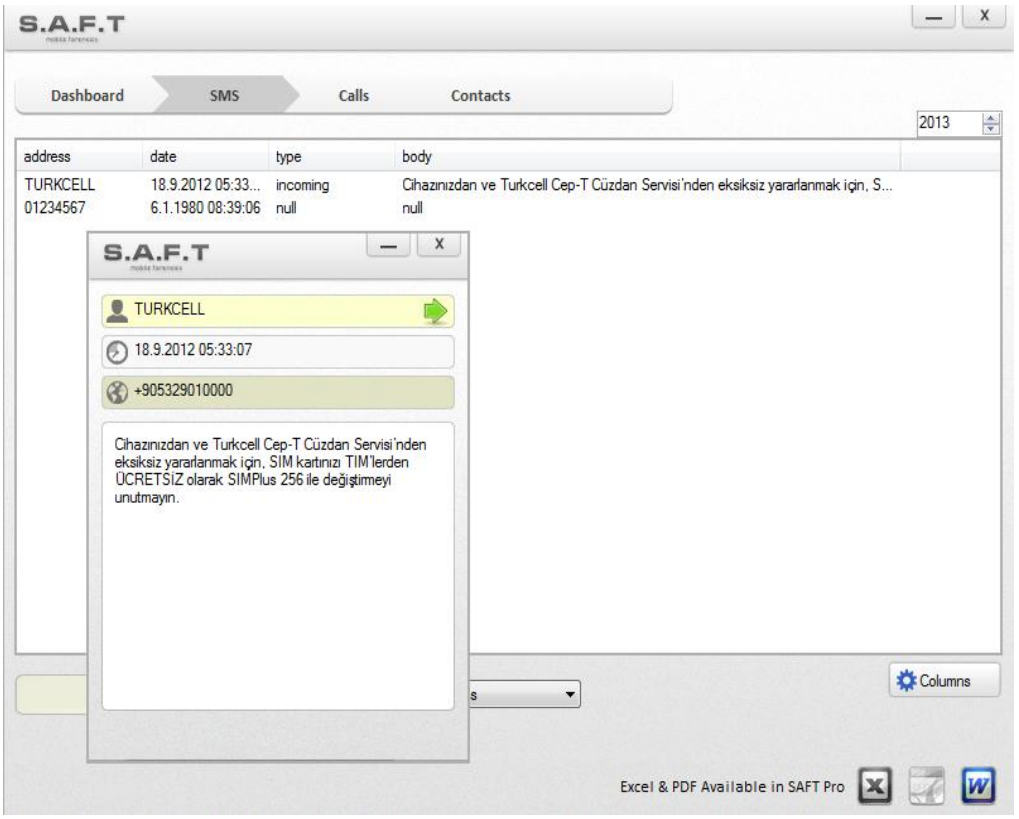
Output Screenshots:




S.A.F.T
operation
victim
Save List
Add
Bug Report | Send Feedback | Check Updates
S.A.F.T
Community Edition
New project
Open project
S-Detect


S.A.F.T
Project Name
P728T_TURKCELL
ID
Device ID
Device IMEI
1
P728T_TURKCELL
Call Logs
Contact List
Sms
Voice, Video Records
File Browser
Youtube,Instagram Logs
Browser History, Bookmarks
MMS Logs
Facebook Twitter Logs
Viber,WhatsApp and Skype Logs
Location History
Email Messages
Physical data acquisition
Calendar
Start


S.A.F.T
Dashboard
SMS
Calls
Contacts
2013
SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls SMS Calls
Şubat
Nisan
Haziran
Ağustos
Ekim
Aralık
Turkcell T11
P728T_TURKCELL
c15058a6f2f82c56aa7ec382732c7b95
CONTACTS
CALLS
SMS
SMS
CALLS
CONTACTS
Excel & PDF Available in SAFT Pro


S.A.F.T
Dashboard
SMS
Calls
Contacts
2013
address
date
type
body
TURKCELL
18.9.2012 05:33...
incoming
Cihazınızdan ve Turkcell Cep-T Cüzdan Servisi'nden eksiksiz yararlanmak için, S...
01234567
6.1.1980 08:39:06
null
null
S.A.F.T
TURKCELL
18.9.2012 05:33:07
+905329010000
Cihazınızdan ve Turkcell Cep-T Cüzdan Servisi'nden eksiksiz yararlanmak için, SIM kartınızı TIM'lerden ÜCRETSİZ olarak SIMPlus 256 ile değiştirmeyi unutmayın.
Columns
Excel & PDF Available in SAFT Pro

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

Solution:

PROCESS MONITOR TOOL:

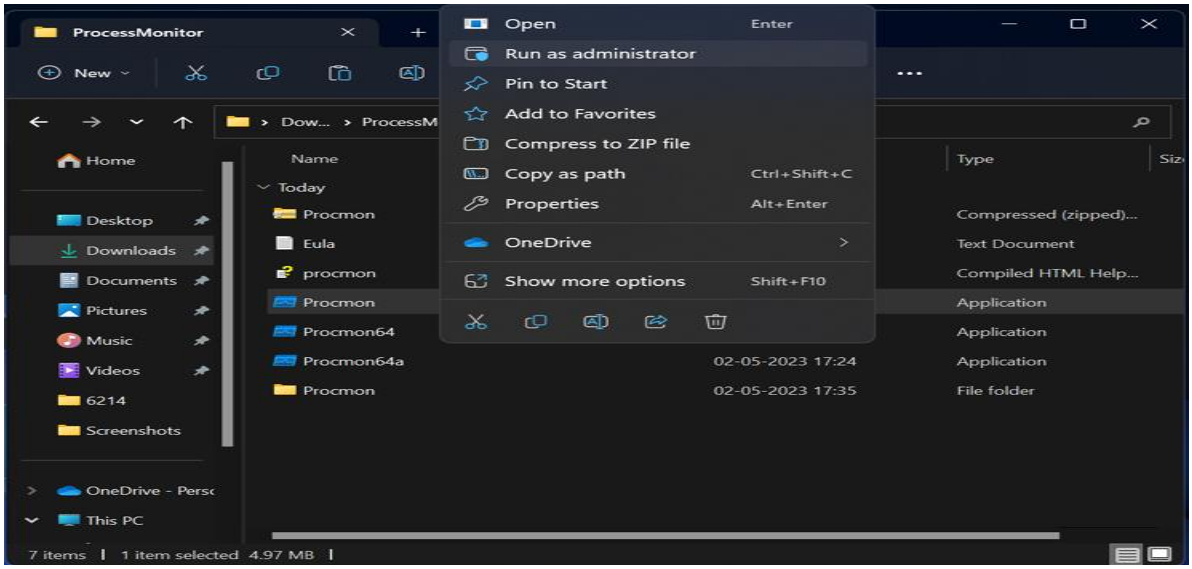
Process monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.

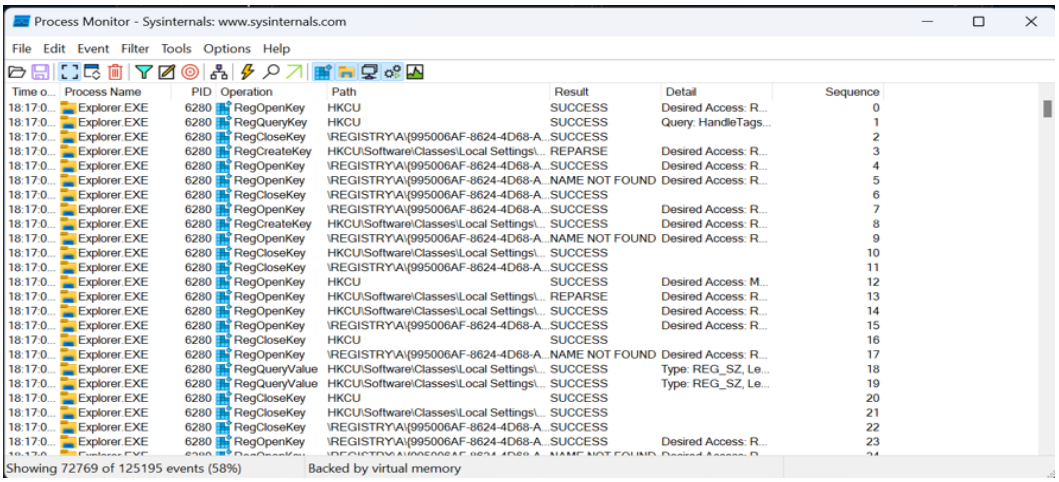
Process monitor is an excellent troubleshooting tool from windows sysinternals that displays the files and registry keys that applications access in real time. The results can be saved to a log file, which you can send to an expert for analyzing a problem and troubleshooting it.

Registry analysis:

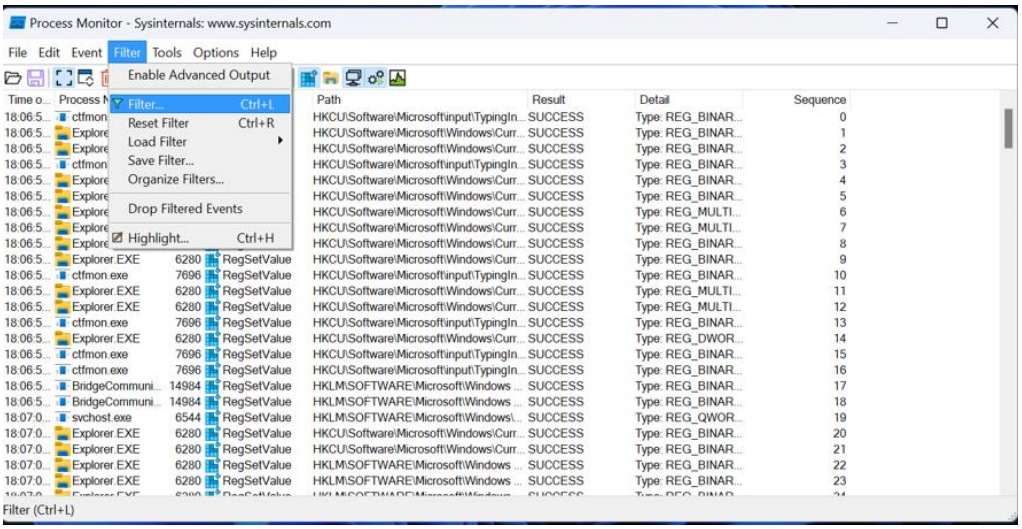
The windows registry tracks so much information about the user's activities. In most cases, these registry keys are designed to make windows run more efficiently.

1. Download process monitor from Microsoft.
2. Extract the zip file contents to a folder of your choice.
3. Run process monitor.
4. Click on run as administrator



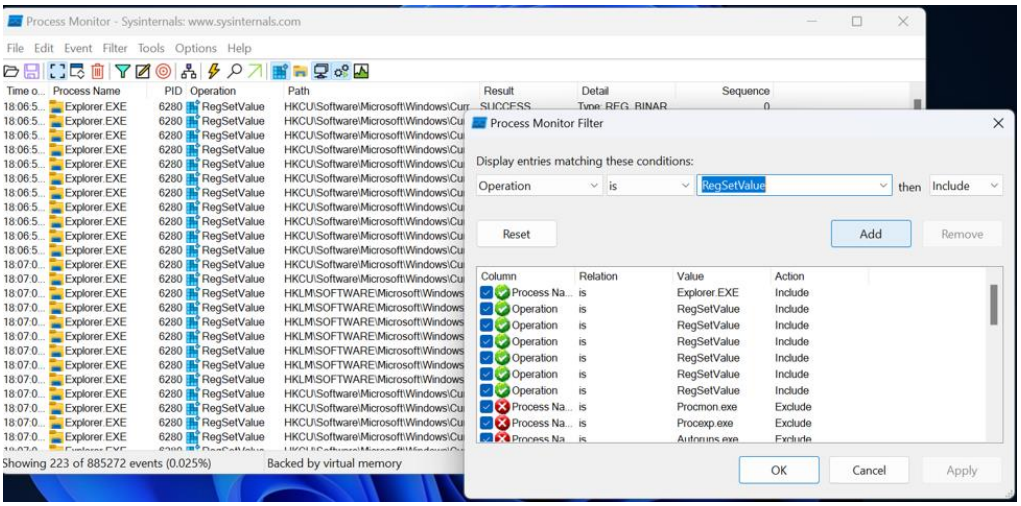


5. If the filter dialog doesn't open automatically, press ctrl + L open the process monitor filter dialog.

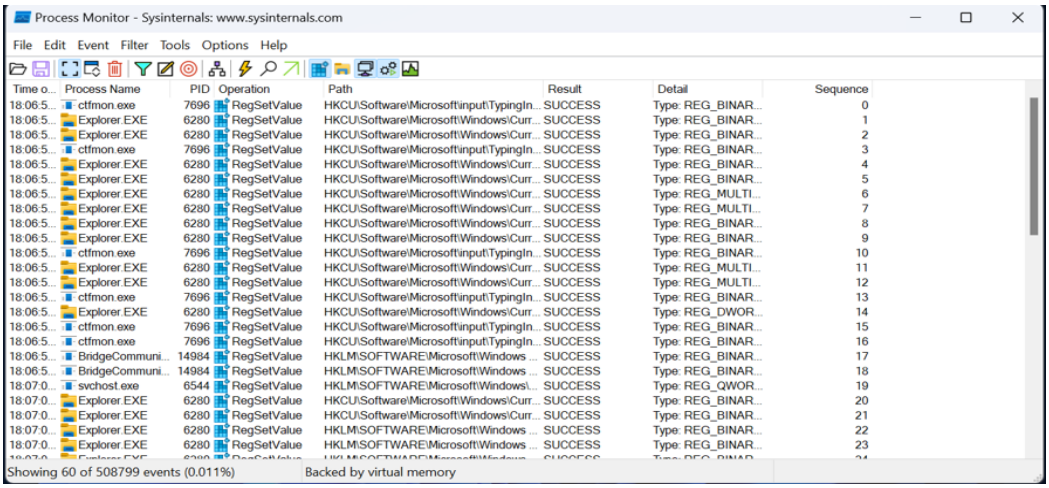


6. Click "Reset" to clear the existing filter

7. Click Add, and click ok.



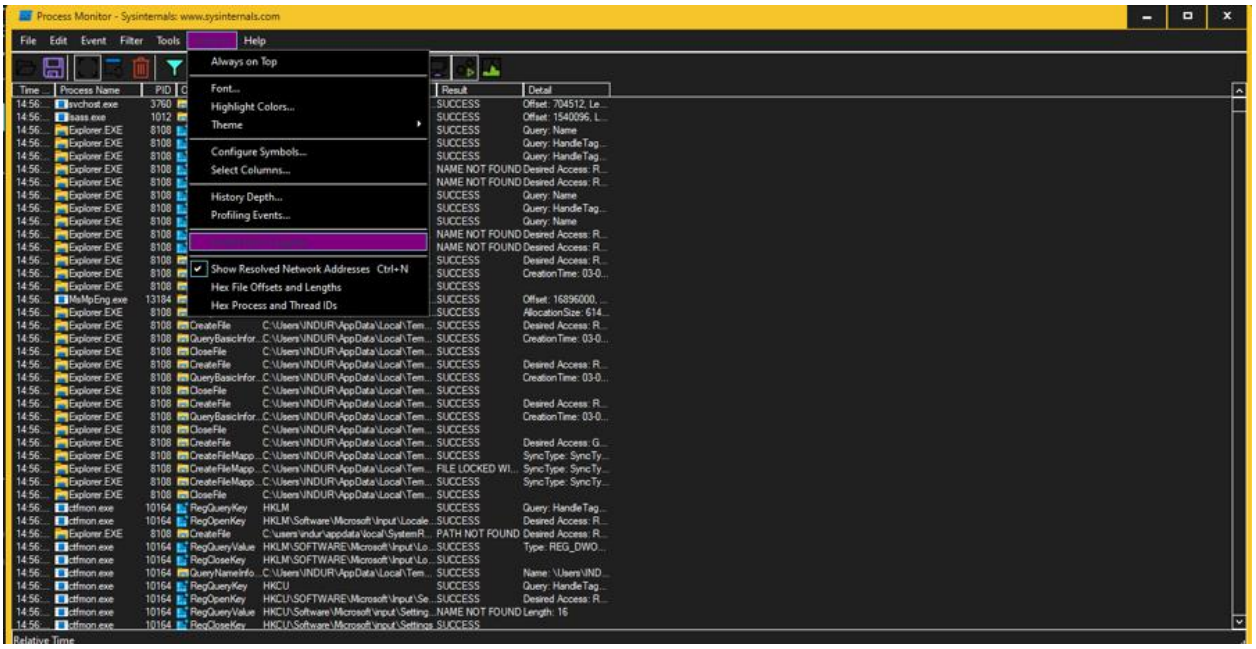
8. After clicking on ok, all the registers will be displayed according to the filter is applied.



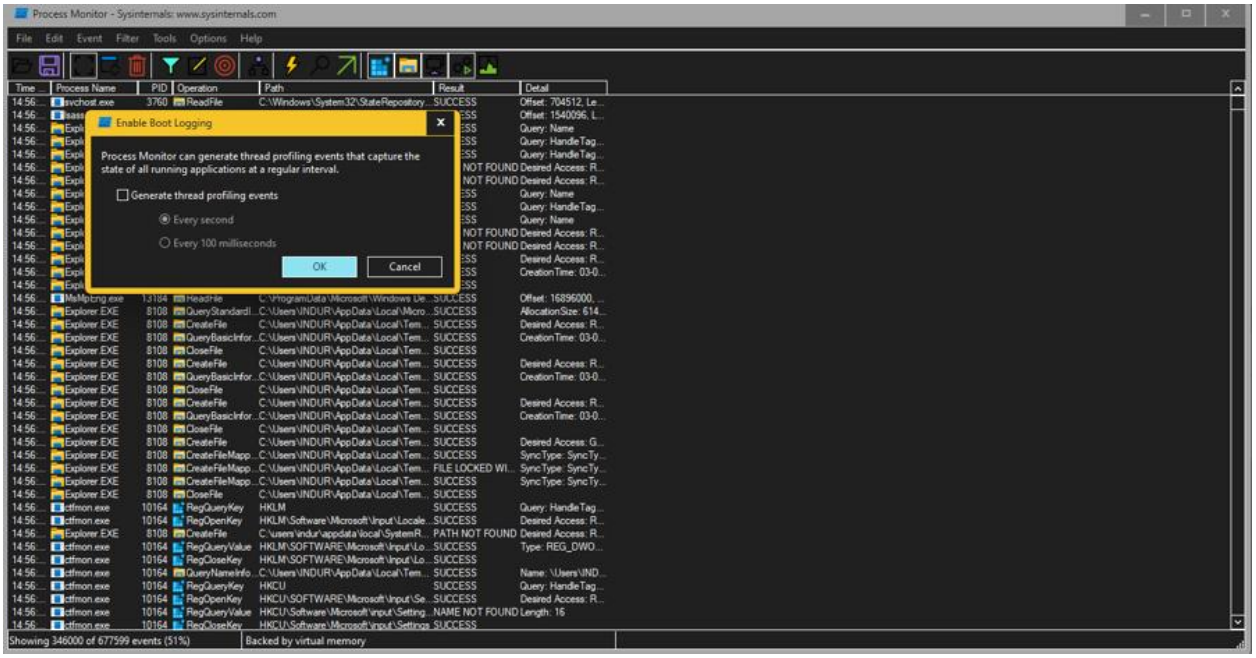
Boot time logging:

The boot log or system initialization log is a text file that can be generated during your computer's boot sequence.

1. Click on options.
2. Select Enable boot logging.

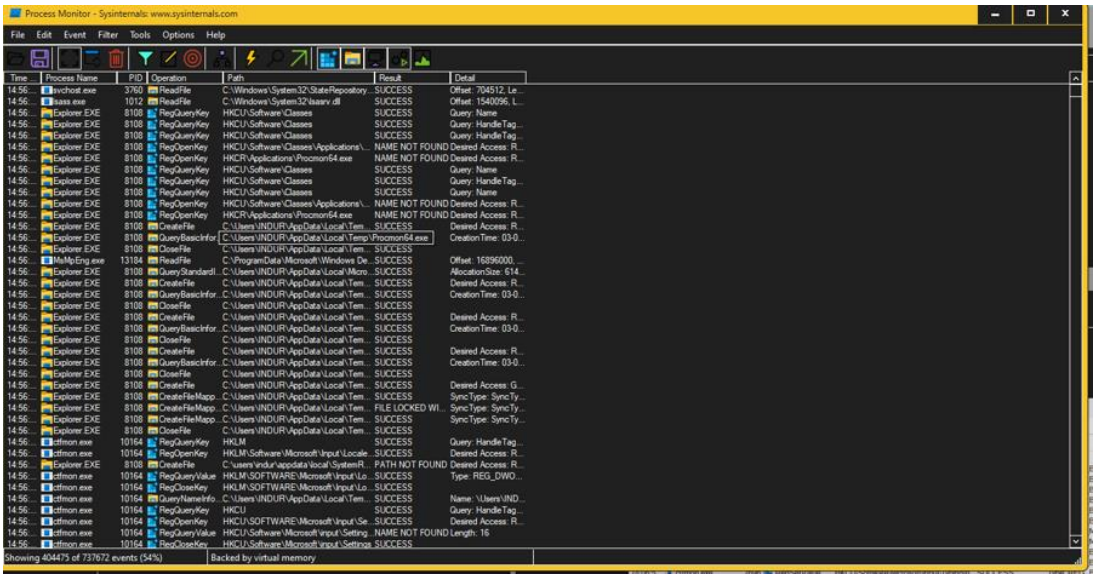


3. It automatically displays Enable boot logging dialog box.
4. Now click on ok.



5. Restart the system.
6. By default it displays the list of all the drivers that are loaded during boot.

Output:



Result: Performed registry analysis and get boot time login using process monitor tool successfully.

5. **Perform Disk imaging and cloning the using the X-way Forensics tools.**

Solution:

Setting up X-Ways Forensics involves several steps to ensure it's correctly installed and configured on your system. Here's a basic guide to get started:

Installation Steps for X-Ways Forensics

1. **Download X-Ways Forensics:**

   Visit the X-Ways website or use the download link provided to obtain the installer.

2. **Run the Installer:**

   Locate the downloaded installer file (usually a .exe file) and double-click it to start the installation process.

3. **Follow Installation Wizard:**

   The installation wizard will guide you through the setup process. Click "Next" or "Continue" where appropriate.

4. **Choose Installation Location:**

   Select the destination folder where you want X-Ways Forensics to be installed. The default location is usually fine unless you have specific preferences.

5. **Select Components:**

   Choose the components you want to install. Typically, this includes the main application and possibly additional tools or plugins.

6. **Finish Installation:**

   Once installation is complete, click "Finish" to exit the wizard.

Post-Installation Configuration

7. **License Activation:**

   If required, activate your license using the provided license key. This step ensures you have access to all features of the software.

8. **Configure Case Management:**

   Set up your case management preferences, including default settings for new cases and storage locations for case data.

9. **Review and Adjust Settings:**

   Explore the settings menu to customize X-Ways Forensics according to your workflow and forensic analysis requirements.

10. **Update Software (Optional):**

    Check for updates to ensure you have the latest features and security patches. X-Ways Forensics may prompt you automatically or provide an update option in the software menu.

Getting Started with X-Ways Forensics

11. **Create a New Case:**

    Begin by creating a new case within X-Ways Forensics. This will allow you to organize and manage data related to a specific investigation.

12. **Start Analyzing Data:**

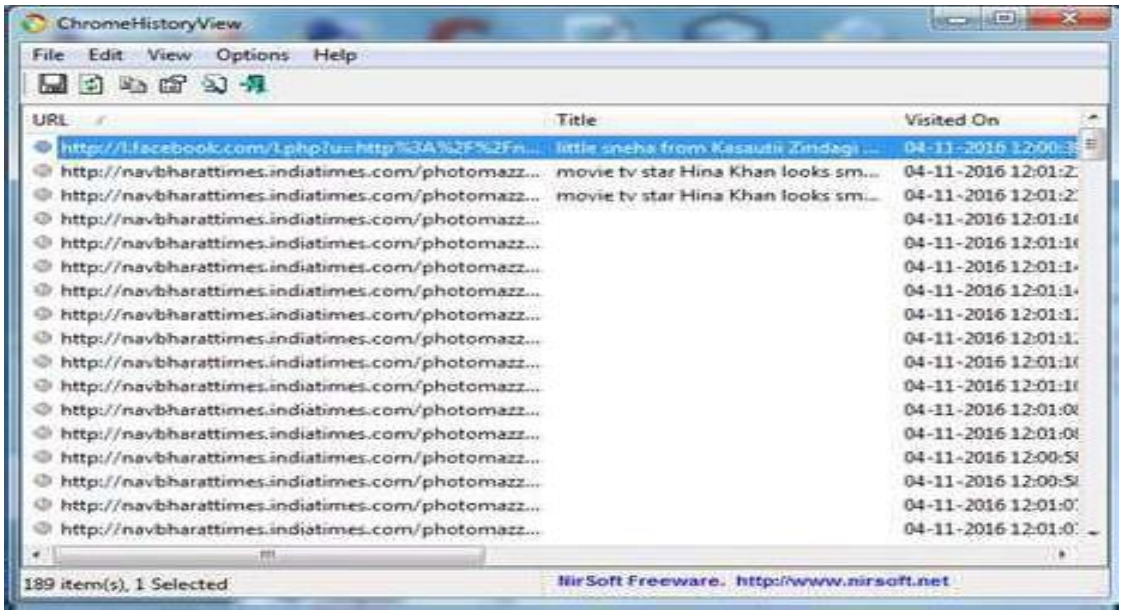
    Use the various tools and features of X-Ways Forensics to analyze digital evidence, generate reports, and draw conclusions based on your findings.

By following these steps, you should be able to successfully install X-Ways Forensics and begin using it for digital forensic analysis. Adjust the settings and workflows as needed to fit your specific investigative needs.

6. **Perform Data Analysis i.e History about open file and folder, and view folder actions using Lastview activity tool.**

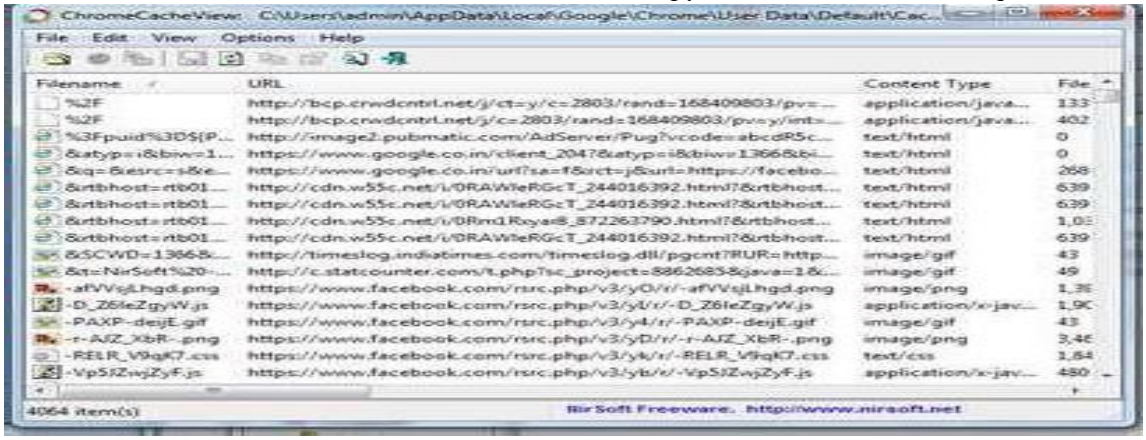
Solution:

ChromeHistoryView: is a small utility that reads the history data file of Google Chrome Web browser, and displays the list of all visited Web pages in the last days. For each visited Webpage, the following information is displayed: URL, Title, Visit Date/Time, Number of visits, number of times that the user typed this address (Typed Count), Referrer, and Visit ID.

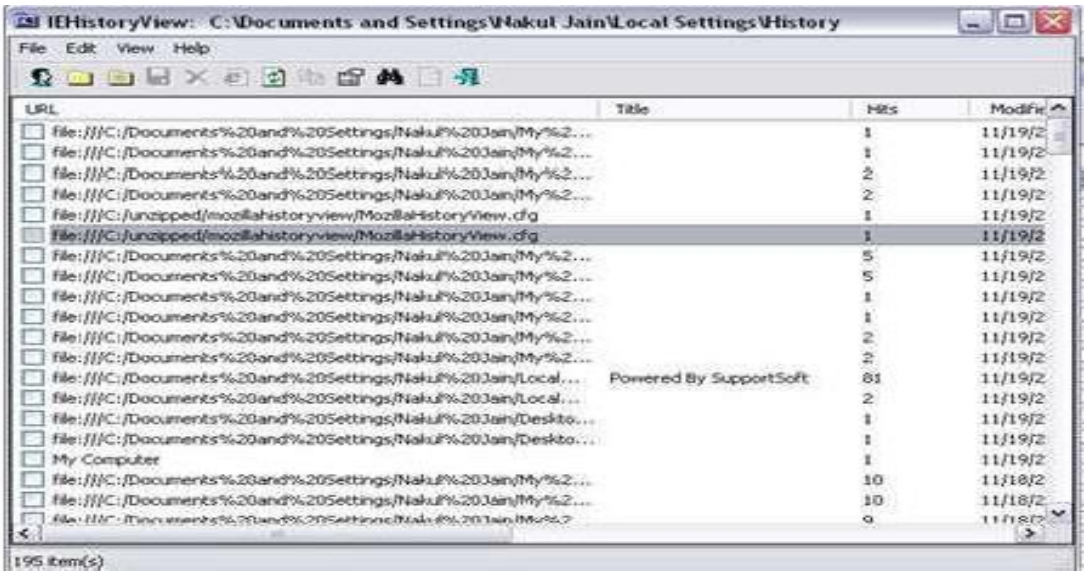


ChromeCacheView: Chromecacheview is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache.

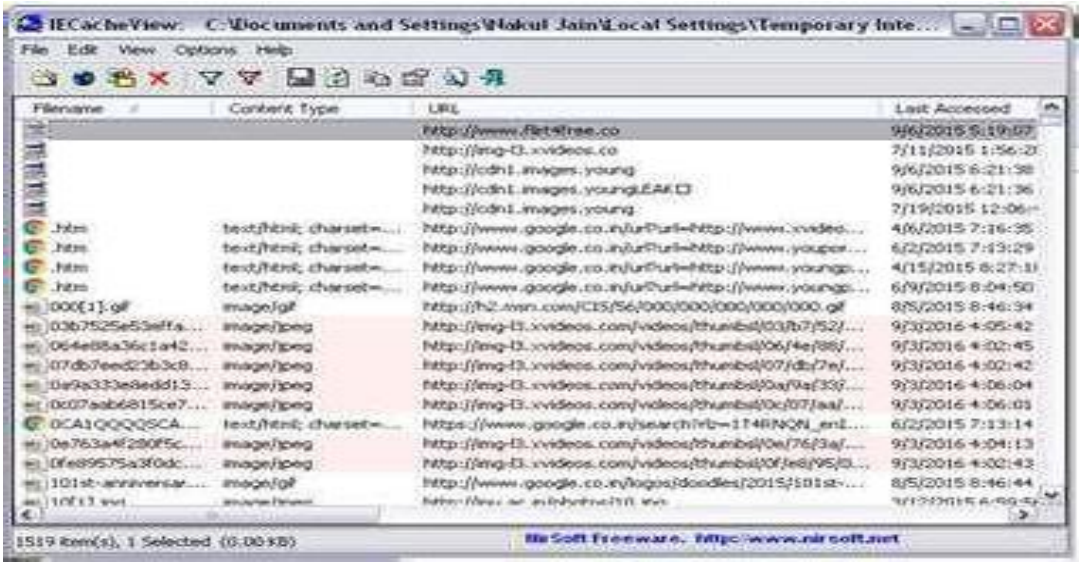
For each cache file, the following information is displayed:
URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, and more. You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.



IEHistoryView: This utility reads all information from the history file on your computer, and displays the list of all URLs that you have visited in the last few days. It also allows you to select one or more URL addresses, and then remove them from the history file or save them into text, HTML or XML file.



IECacheView: IECacheView is a small utility that reads the cache folder of Internet Explorer, and displays the list of all files currently stored in the cache. For each cache file, the following information is displayed: Filename, Content Type, URL, Last Accessed Time, Last Modified Time, Expiration Time, Number of Hits, File Size, Folder Name, and full path of the cache filename.



7. Perform Network analysis using the Network Miner tool.

Solution:

Aim:

To perform network analysis using the network miner tool.

About the tool:

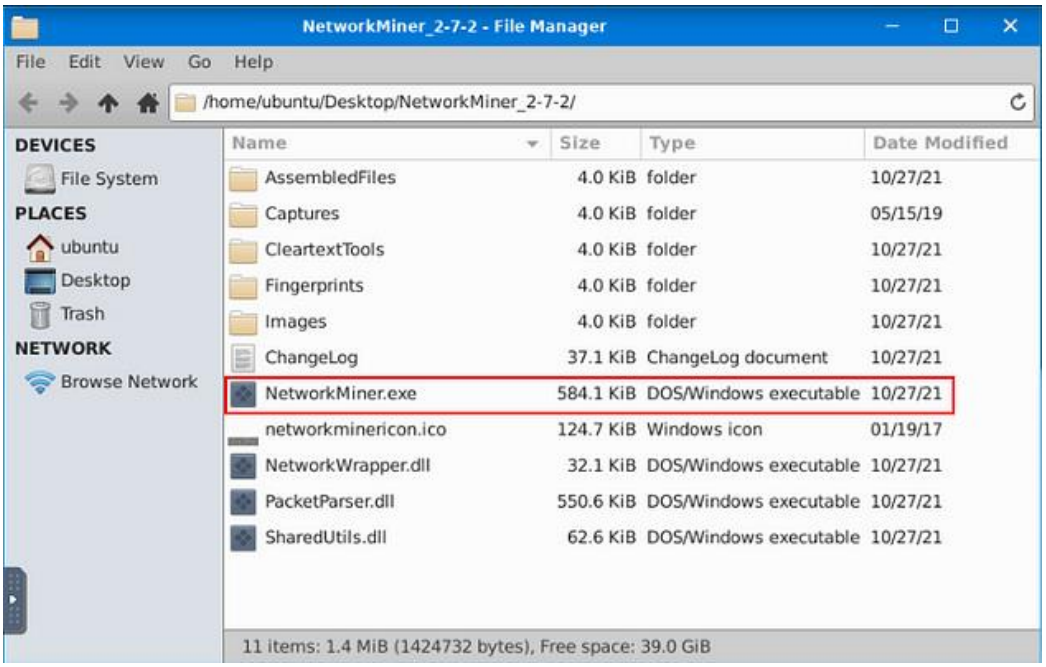
NetMiner is an application software for exploratory analysis and visualization of large **network** data based on SNA (Social **Network** Analysis). Manage LAN, WAN, Bandwidth, VoIP Agentless **tool**, deploys in minutes! Detect, diagnose, & resolve **network** performance issues. Download Now. Recognized by EMA Radar. Recognized by InfoTech. Install in mins. Enterprise-class Solution. **NetworkMiner** is an open source network forensics **tool** that extracts artifacts, such as files, images, emails and passwords, from captured network. it uses as a passive **network** sniffer/packet capturing **tool** in order to detect operating systems, sessions, hostnames, open ports etc.

Step 1: Download and Install NetworkMiner

Download NetworkMiner: Go to the NetworkMiner website (https://www.netresec.com/?page=NetworkMiner)

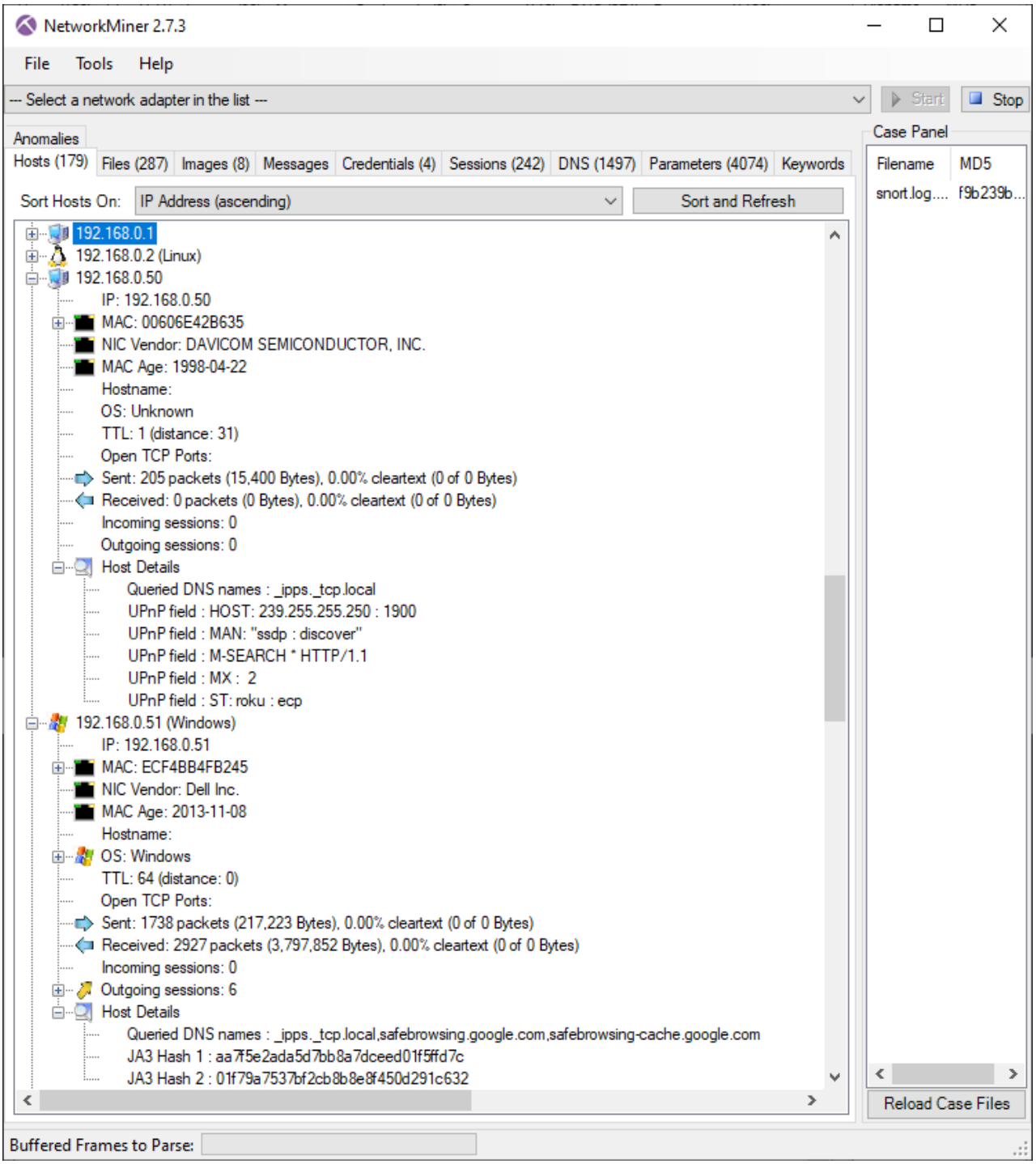
and download the latest version of NetworkMiner. Choose the appropriate installer for your Windows system (32-bit or 64-bit).

1. **Install NetworkMiner**: Once downloaded, run the installer and follow the installation instructions. The installation process is straightforward and typically involves accepting the license agreement and choosing the installation directory.



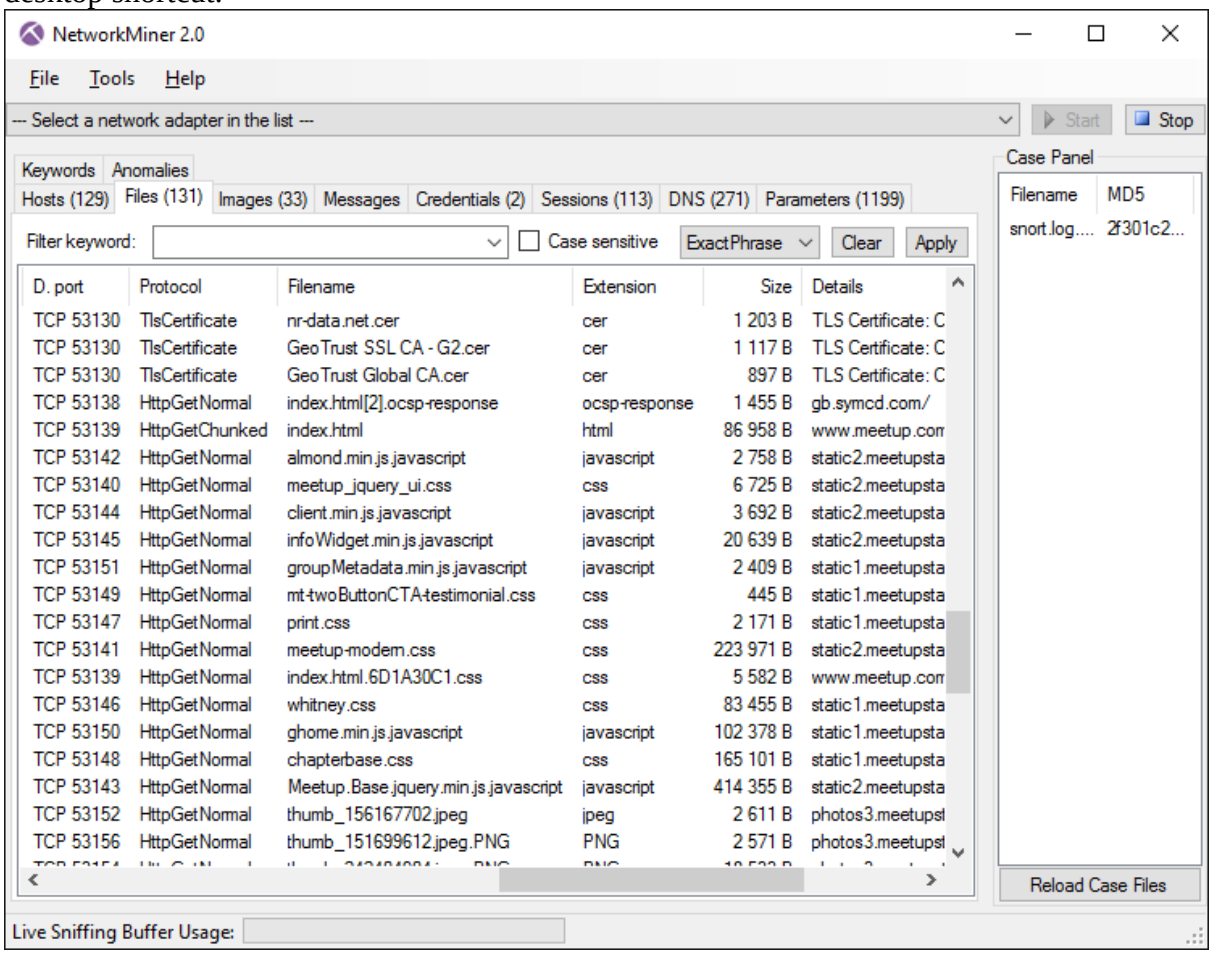
Step 2: Capture or Import PCAP Files

NetworkMiner primarily works with PCAP files (packet capture files). You can capture network traffic using tools like Wireshark and save it as a PCAP file, or you can use existing PCAP files for analysis.



Step 3: Launch NetworkMiner

1. **Open NetworkMiner**: After installation, launch NetworkMiner from the Start menu or desktop shortcut.



Step 4: Analyze Network Traffic

1. **Import PCAP File**:

   Click on File > Open to import a PCAP file. Navigate to the location where your PCAP file is stored and select it.

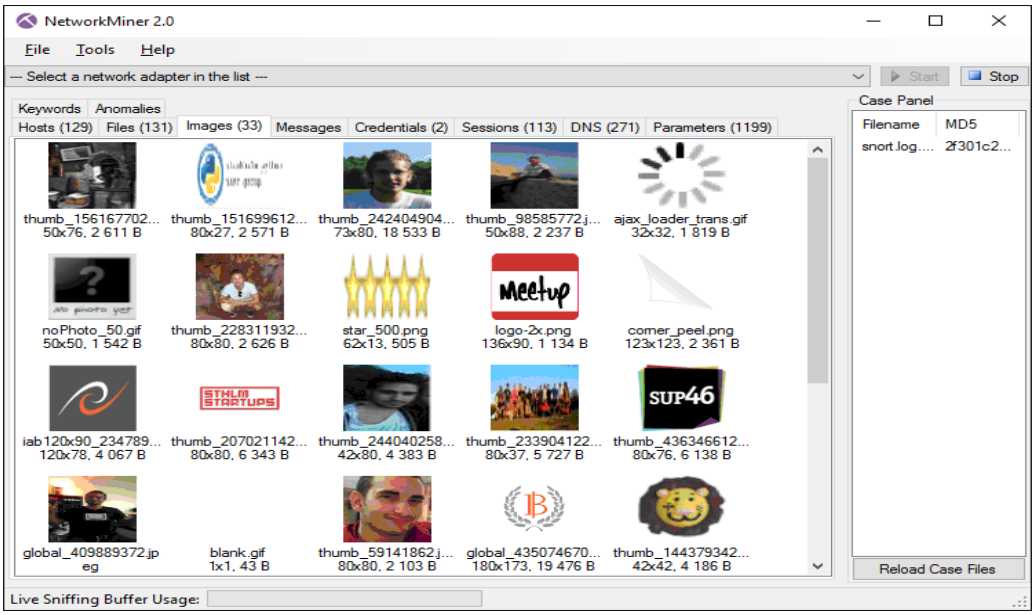
2. **View Captured Data**:

   NetworkMiner will start parsing the PCAP file and display various tabs such as Hosts, Sessions, Files, Parameters, etc.
   Explore different tabs to view extracted information. For example:

   - **Hosts**: Shows a list of hosts detected in the network traffic along with IP addresses, MAC addresses, and other details.
   - **Sessions**: Displays network sessions such as HTTP, FTP, SMTP, etc., with details like source and destination IP addresses, ports, etc.
   - **Files**: Lists files extracted from the network traffic, such as images, documents, etc.

3. **Export Data**:

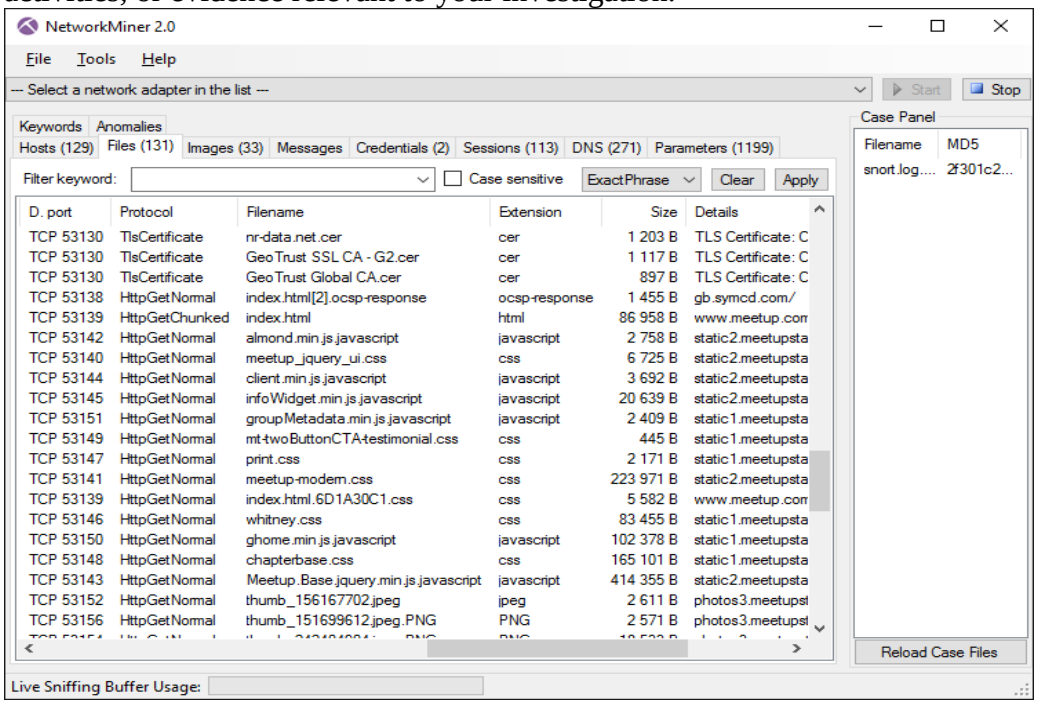
   You can export captured data by clicking on File > Export All. NetworkMiner allows you to export captured files, extracted content, and other relevant data.



Step 5: Interpret Results

1. **Analyze Results**:

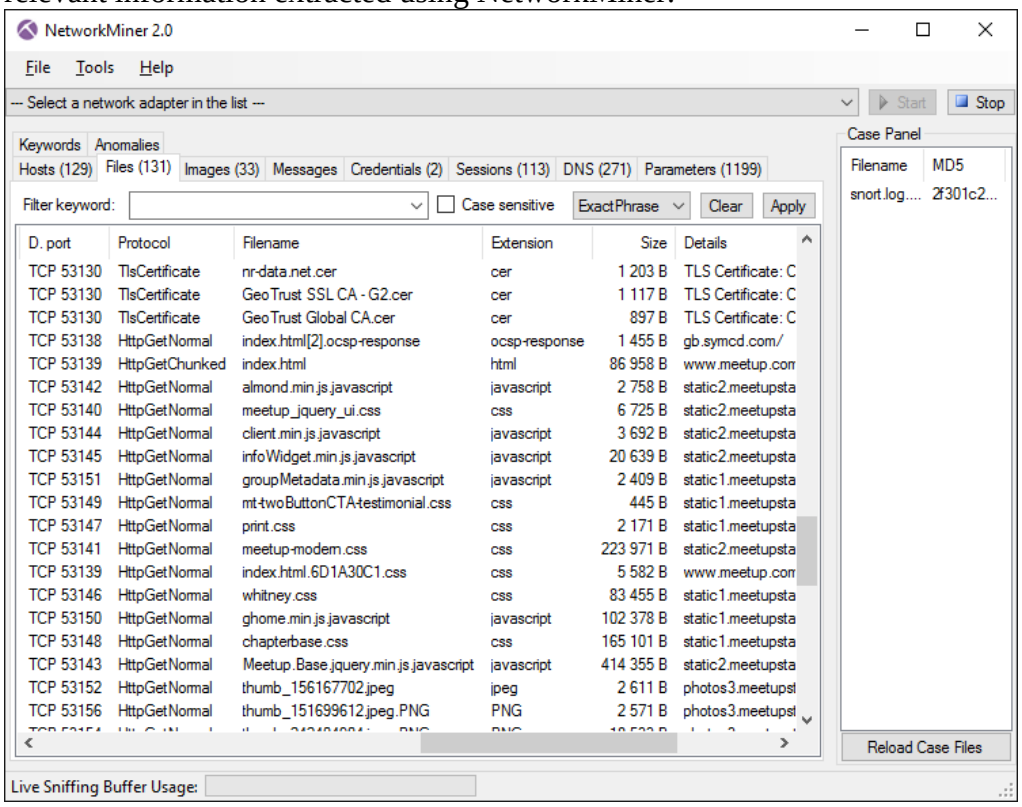
   Interpret the information extracted by NetworkMiner. Look for anomalies, suspicious activities, or evidence relevant to your investigation.



Step 6: Document Findings

1. **Document Findings**:

   Document your findings in a detailed report. Include screenshots, extracted files, and any relevant information extracted using NetworkMiner.



Step 7: Exit NetworkMiner

Close NetworkMiner: Once you have completed your analysis and extracted the necessary information, close NetworkMiner.

Result:

Performed network analysis using the network miner tool successfully.

8. Perform information for incident response using the crowd Response tool.

Solution:

Aim: To perform information for incident response using the crowd response tool.

About the tool:

CrowdResponse is a free, lightweight Windows console application designed to aid the gathering of system information for incident **response** & security.CrowdResponse is a free tool written by Robin Keir from CrowdStrike. Robin has a long history of developing excellent tools for the community including SuperScan, BinText, Fpipe, and CrowdInspect.

1. Download Crowd Response Tool

- Go to the CrowdStrike GitHub repository for Crowd Response Tool.
- Download the latest release of the tool from the releases section.

2. Prepare Your Environment

- Ensure you have a Windows system to run the tool (Crowd Response Tool is primarily for Windows environments).
- Make sure you have administrative privileges on the system where you'll install the tool.

3. Install Crowd Response Tool

- Extract the downloaded Crowd Response Tool zip file to a directory on your system.
- There is no formal installation process; you just need to extract the contents to a folder where you want to run the tool from.

4. Configure Crowd Response Tool (Optional)

- The tool may require specific configuration based on your forensic investigation needs.
- Check the tool's documentation or readme file for any specific configuration instructions.

5. Run Crowd Response Tool

- Navigate to the directory where you extracted the tool.
- Double-click on the executable file (usually named CrowdResponse.exe) to launch the tool.
- Follow any on-screen prompts or instructions provided by the tool.

6. Capture System Data

- Once the tool is running, you can start capturing system data.
- Depending on your investigation requirements, configure the tool to collect the necessary information (e.g., system processes, network connections, installed software).

7. Analyze and Export Results

- After data collection, the tool typically provides options to analyze or export the collected data.

- Follow the tool’s interface or documentation to export results in a format suitable for your forensic analysis.

8. Interpret Results

- Analyze the exported data using forensic analysis tools or methods appropriate for your investigation.
- Interpret the results to draw conclusions relevant to your investigation goals.

9. Documentation and Reporting

- Document the findings and analysis process thoroughly.
- Prepare a report summarizing your findings, methodology, and any relevant forensic artifacts.

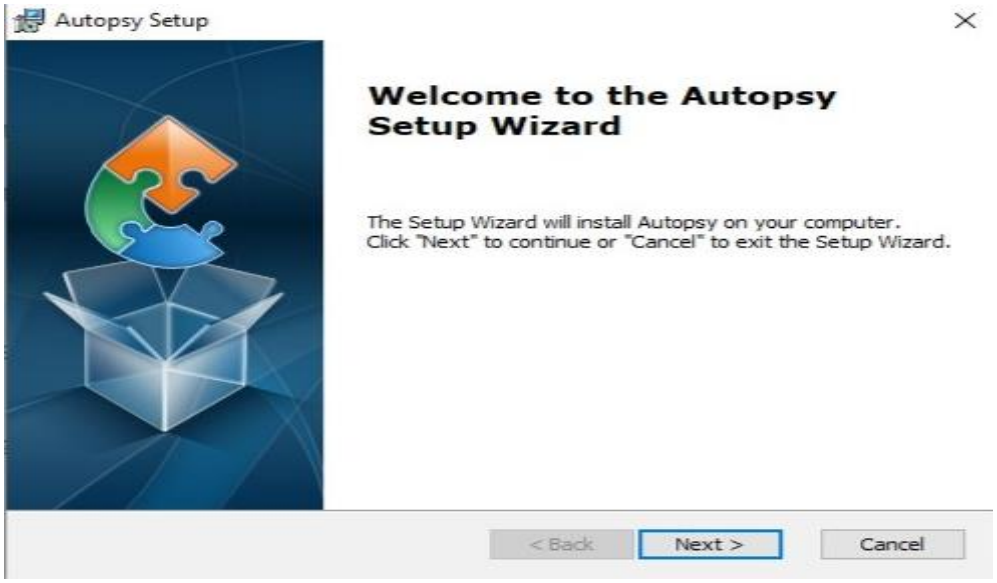
9. Perform File type detection using Autopsy tool.

Solution:

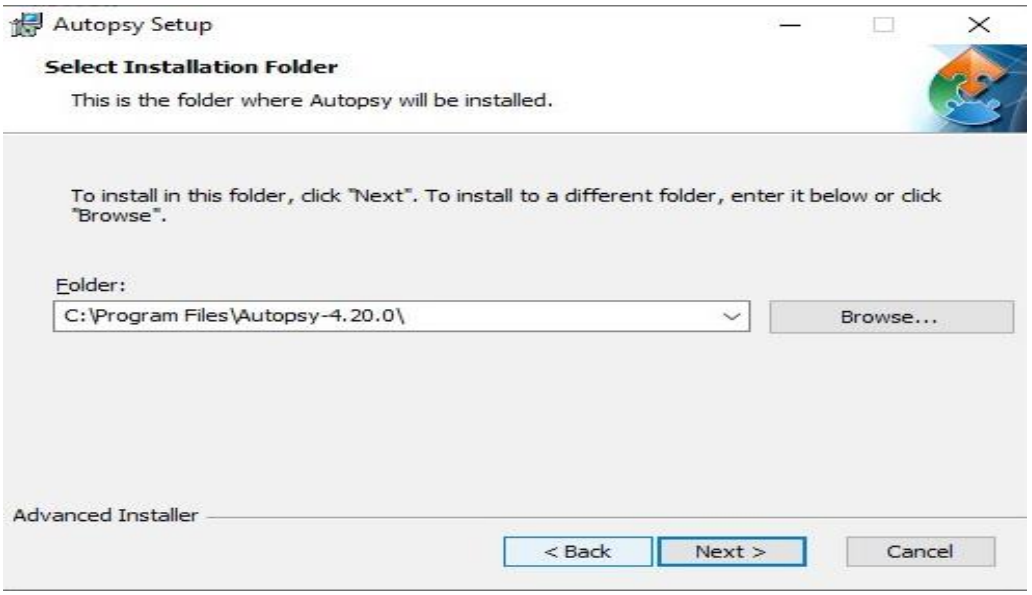
Aim: To perform file type detection using Autopsy tool.

Installation of Autopsy:

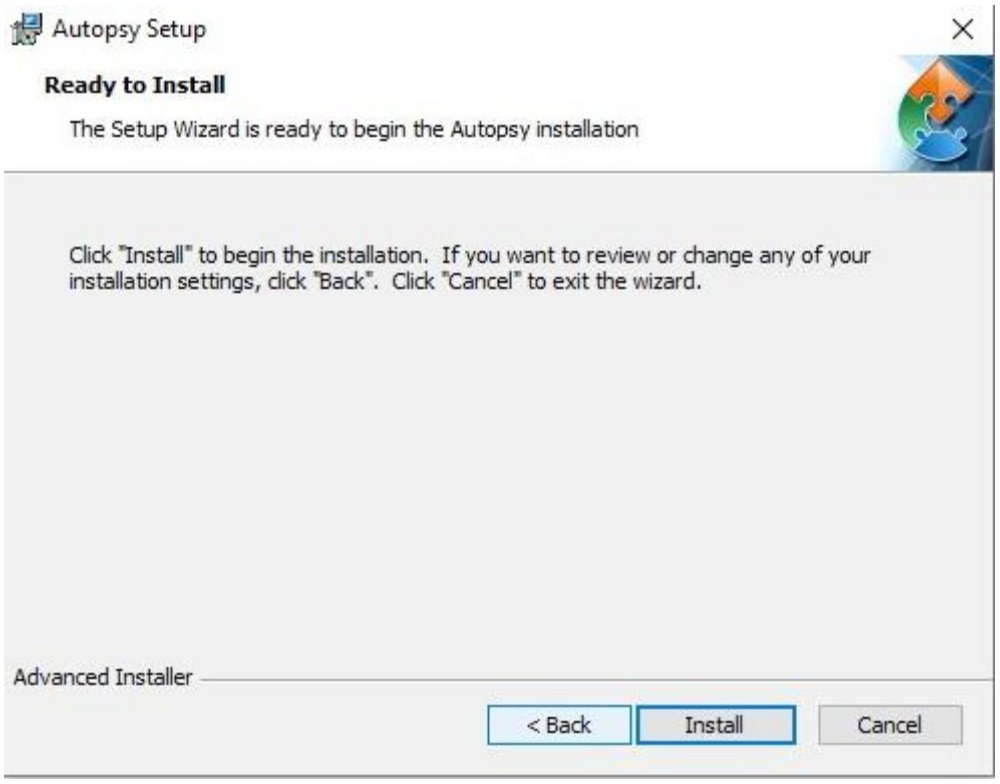
- Download the Autopsy installer from the official website at https://www.sleuthkit.org/autopsy/download.php.
- Select the appropriate version for your operating system (32-bit or 64-bit).
- Double-click on the downloaded executable file to start the installation process.
- Follow the instructions in the installation wizard to install Autopsy.



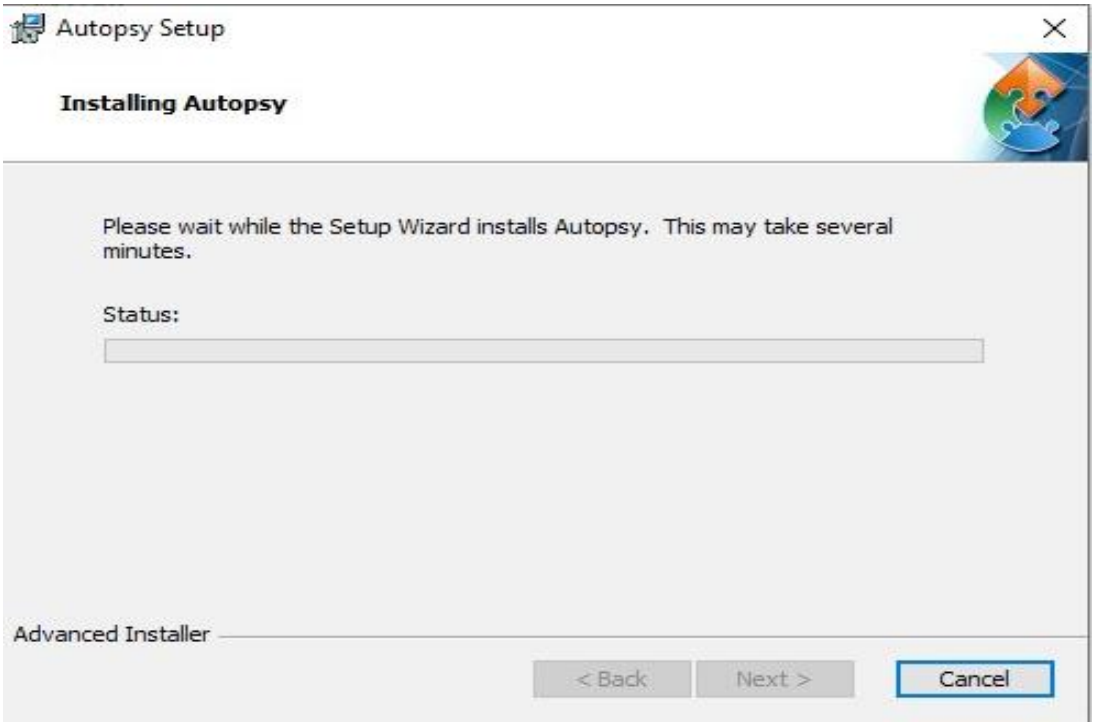
Click Next to continue…

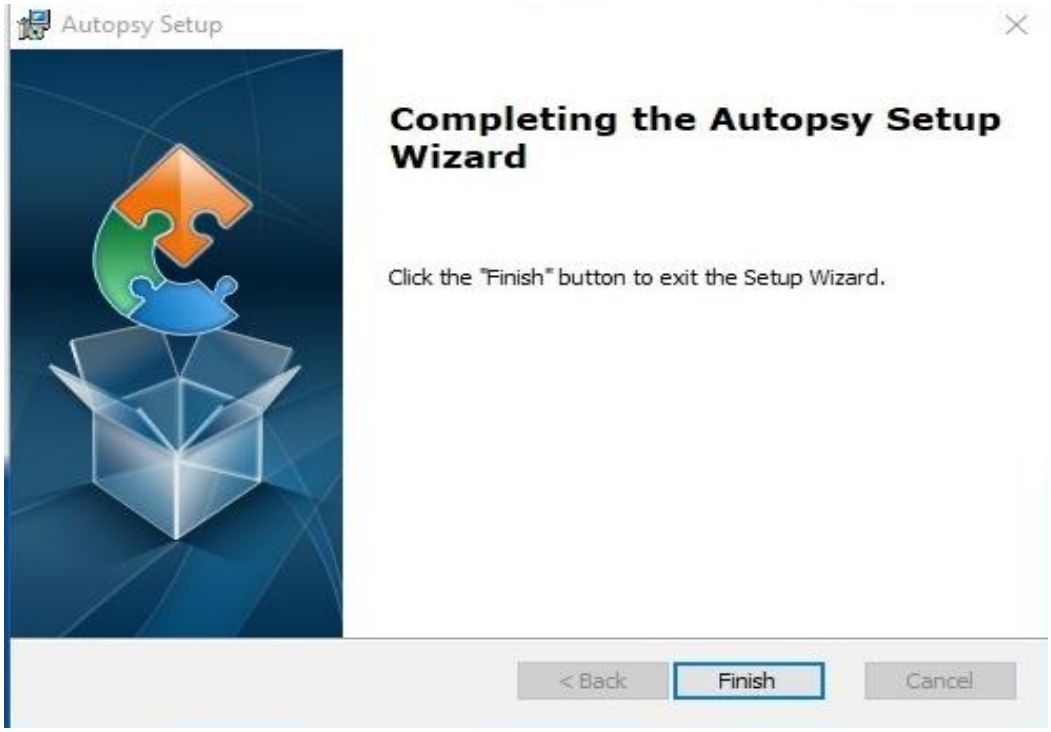


Click on next…



Click on install…





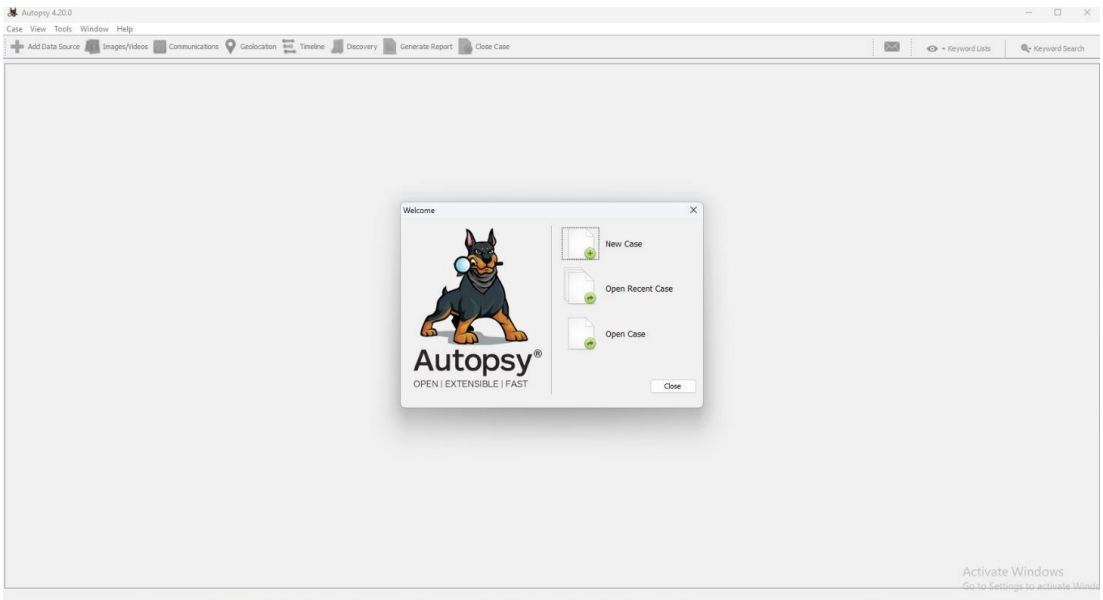
Click on **finish**.

Once the installation is complete, you can launch Autopsy bydouble-clicking on the Autopsy icon on your desktop.

Autopsy is computer software that makes it simplerto deploy many of the open source programs and plugins used in The Sleuth Kit. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.

1. Getting Started

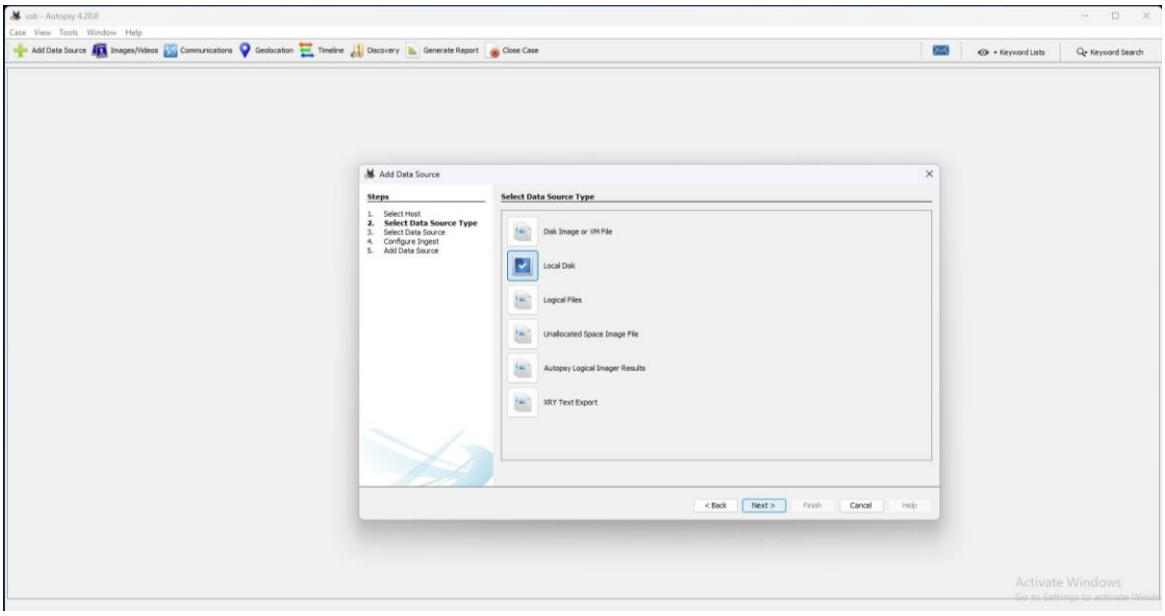
Open Autopsy and create a new case.

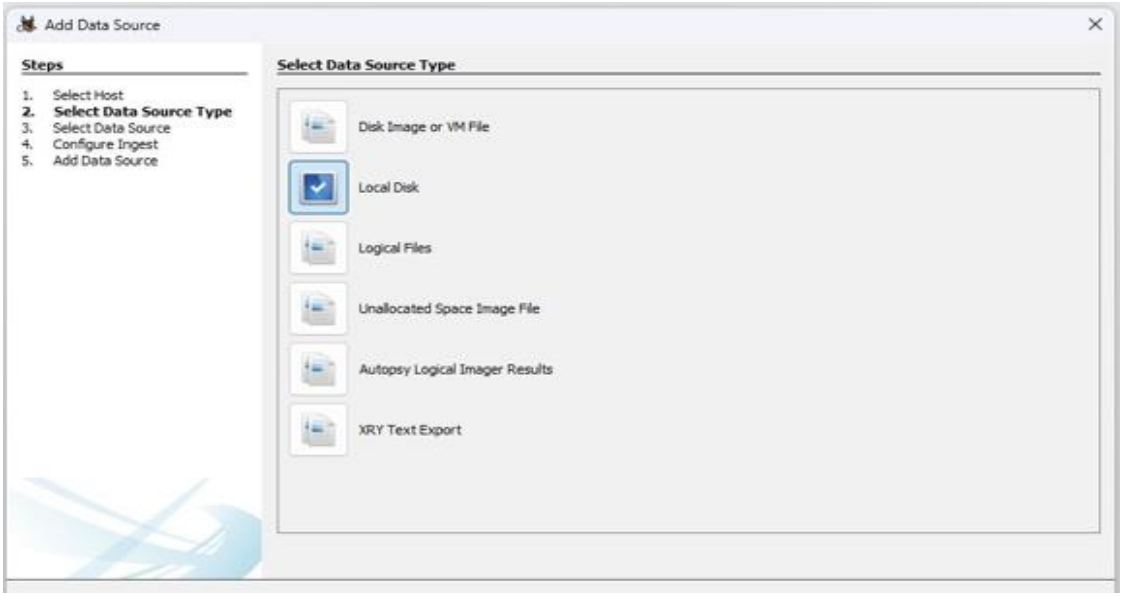


Click on Finish after completing both the steps.

2. Add a data source.

Select the appropriate data source type.





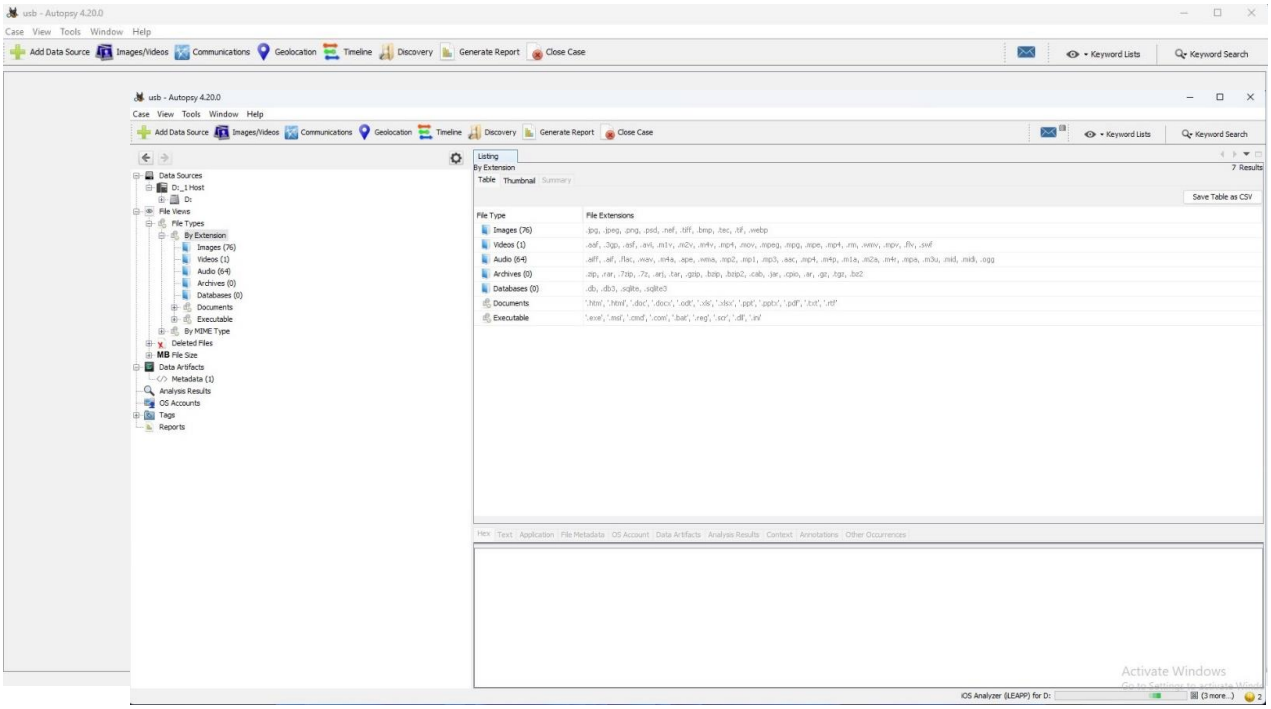
- Disk Image or VM file: Includes images that are an exact copy of a hard drive or media card, or a virtualmachine image.
- Local Disk: Includes Hard disk, Pen drive, memorycard, etc.
- Logical Files. : Includes local folders or files. Unallocated Space Image File: Includes files that donot contain a file system but need to run through ingest.

The data source used here is a USB. Add the data sourcedestination.

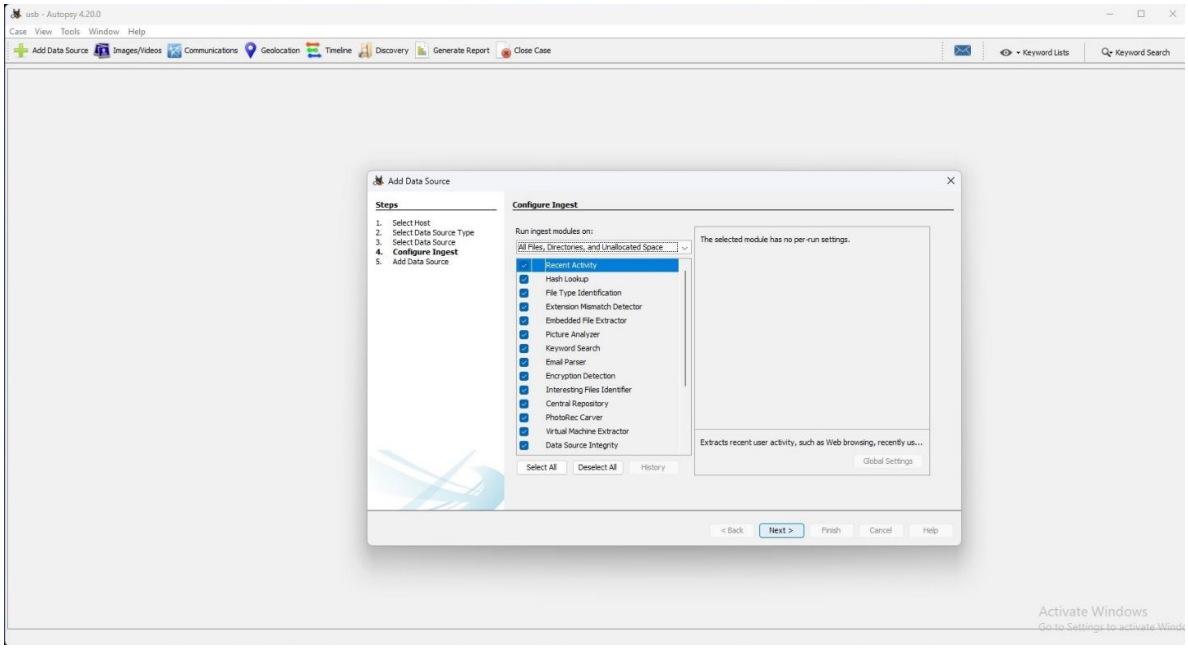
Configure ingest modules.

The ingest modules determine factors for which the datain the data source is to be analyzed.

3. Exploring the data source:



The Data Source information: Here the basic metadata isshown. A detailed analysis is displayed in the bottom section. These details can be extracted in the form of Hexvalues, Results, File Metadata, etc.



The disk image is then broken down based upon its volumepartitions.

Output:

Each volume can be browsed for its contents, results for which are displayed in the section at the bottom.

10. Perform Memory capture and analysis using the Live RAM capture or any forensic tool.

Solution:

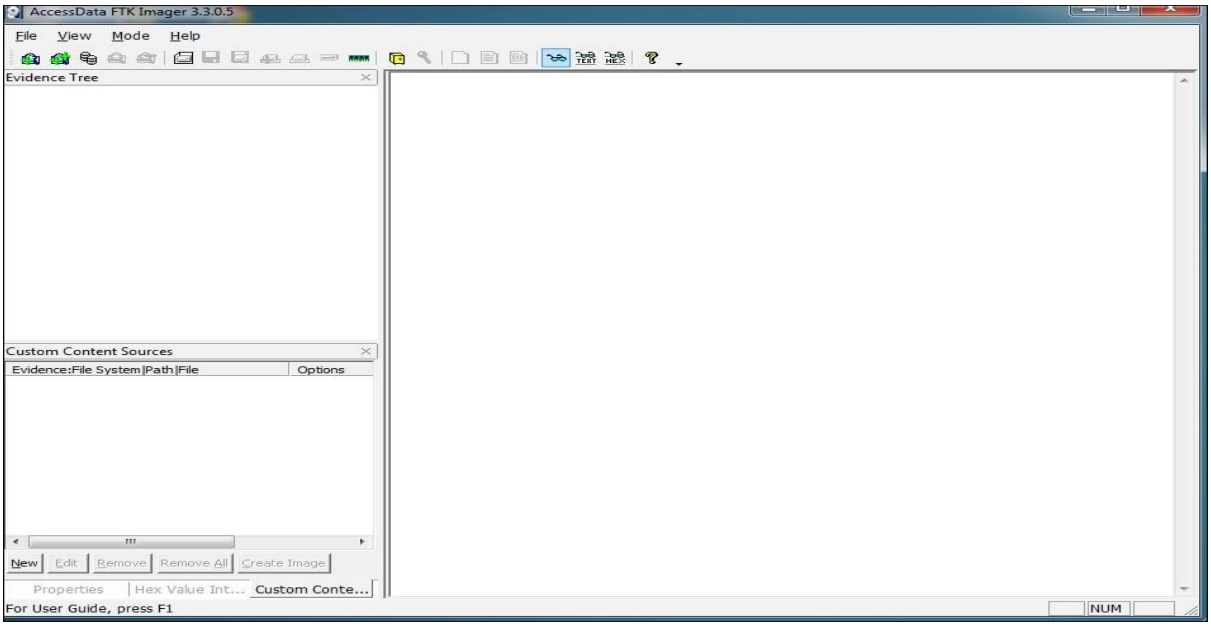
Aim: To perform memory capture and analysis using Live Ram tool.

Memory is a very important source of evidence in an investigation process. All activities that happen on a system are usually reflected in the memory at the time.

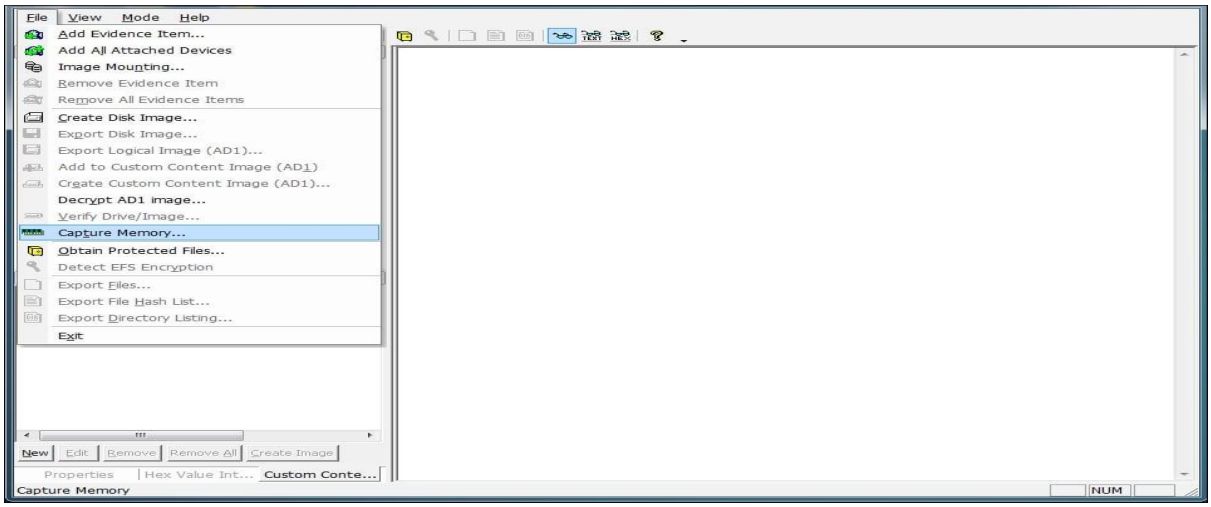
The following is a step-by-step guide to acquire a system's volatile memory using the product FTK Imager.

This can be downloaded for free at: https://accessdata-ftk-imager.software.informer.com/

1. Run FTK Imager as an administrator, as shown in the following screenshot:

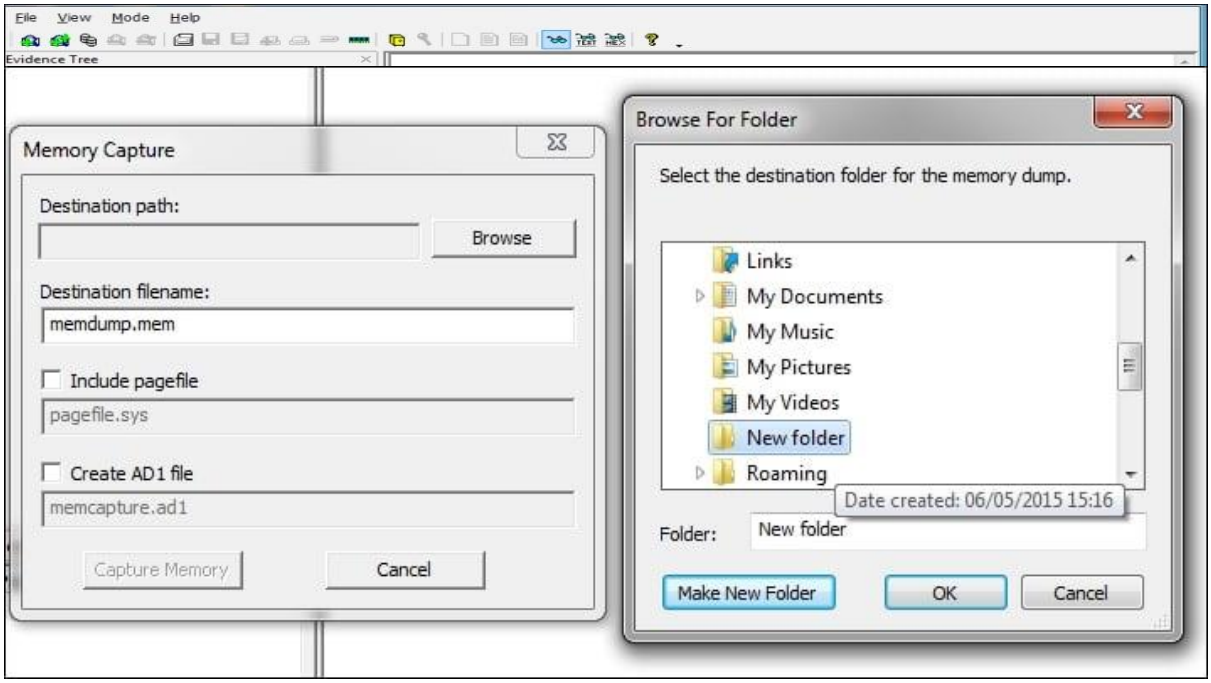


2. Click on the File menu and select Capture Memory, as shown in the following screenshot:



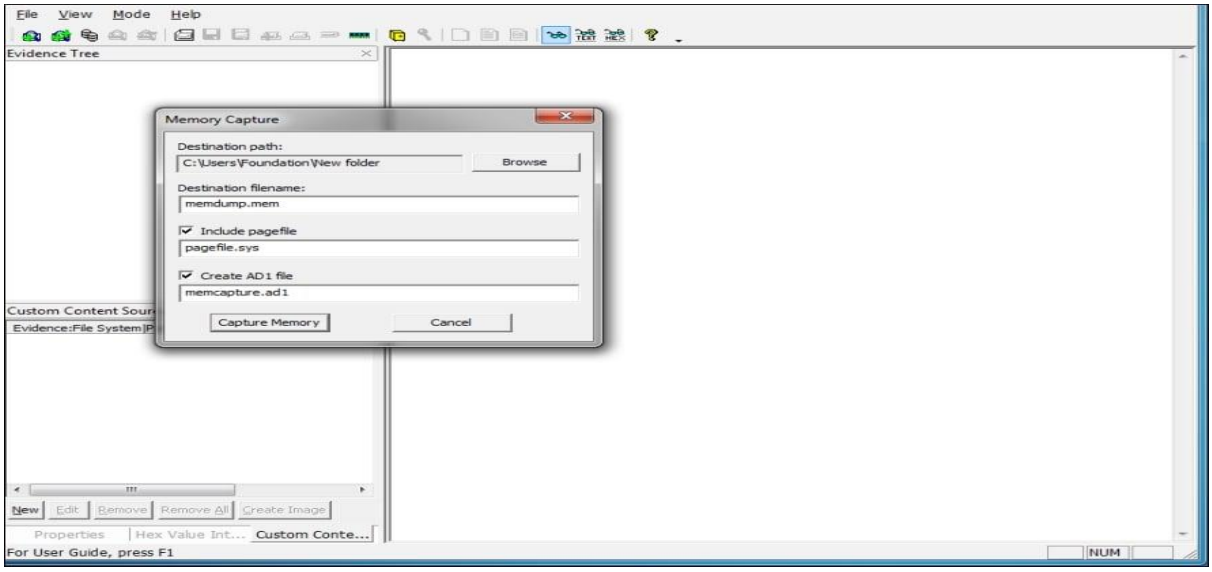
3. Browse the destination folder, where you want to save the acquired memory dump, as shown in the following screenshot:

4. Click on Browse and create a destination folder, as shown in the following screenshot:



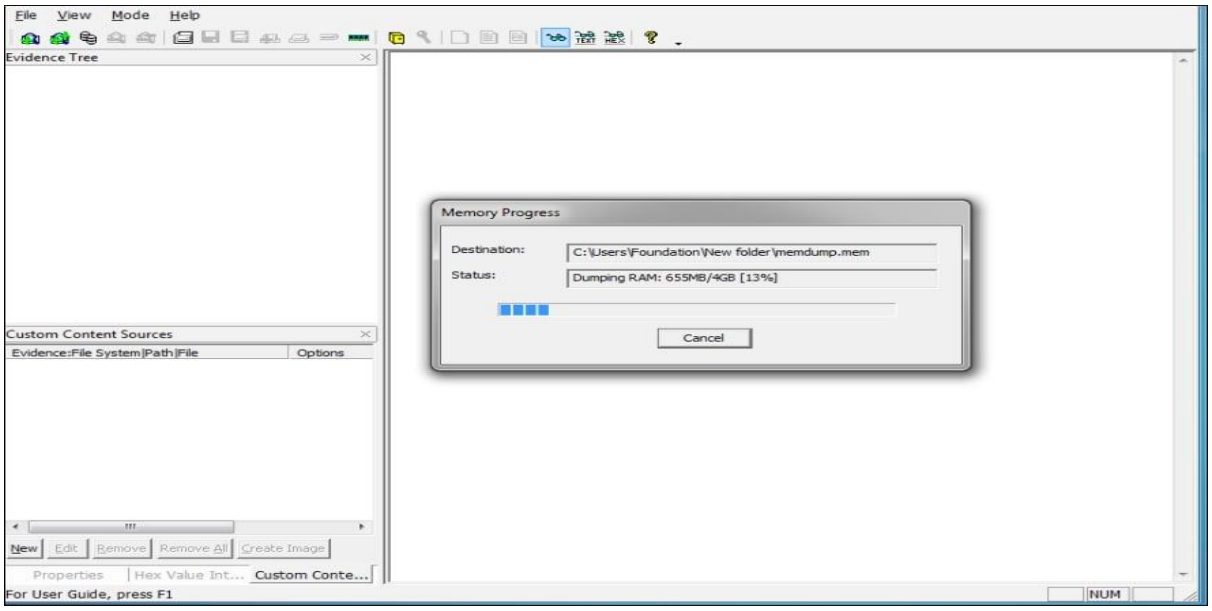
5. After creating the destination folder, click on Capture Memory, as shown in the following screenshot:

6. Click on Capture Memory and the memory dumping will start, as shown in the following screenshot.



7. Memory Capture Dumping PageFile and completed successfully:

Output:



Result: Performed memory capture and analysis using Live Ram tool successfully.