Computer Forensic Investigation

---

1. Computer Forensic using Autopsy

What is Autopsy?

Autopsy is an open source digital forensics tool developed by Basis Technology, first released in 2000. It is a free to use and quite efficient tool for hard drive investigation with features like multi-user cases, timeline analysis, registry analysis, keyword search, email analysis, media playback, EXIF analysis, malicious file detection and much more.

How to install Autopsy?

Step 1: Download Autopsy from this link => https://www.autopsy.com/download/

Step 2: Run the Autopsy msi installer file.

Step 3: If you get a Windows prompt, click Yes.

Step 4: Click through the dialog boxes until you click a button that says Finish.

Step 5: Autopsy should be installed now.

Basic Concept

This section will outline the following basic concepts:

- Investigation Workflow
- Deployment Types
- Central Repository

Features Of Autopsy

Multi-User Cases: Collaborate with fellow examiners on large cases.

Timeline Analysis: Displays system events in a graphical interface to help identify activity.

Keyword Search: Text extraction and index searched modules enable you to find files that mention specific terms and find regular expression patterns.

Web Artifacts: Extracts web activity from common browsers to help identify user activity.

Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.

LNK File Analysis: Identifies short cuts and accessed documents

Email Analysis: Parses MBOX format messages, such as Thunderbird.

EXIF: Extracts geo location and camera information from JPEG files.

File Type Sorting: Group files by their type to find all images or documents.

Media Playback: View videos and images in the application and not require an external viewer.

Thumbnail viewer: Displays thumbnail of images to help quick view pictures.

Robust File System Analysis: Support for common file systems, including NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.

Hash Set Filtering: Filter out known good files using NSRL and flag known bad files using custom hashsets in HashKeeper, md5sum, and EnCase formats.

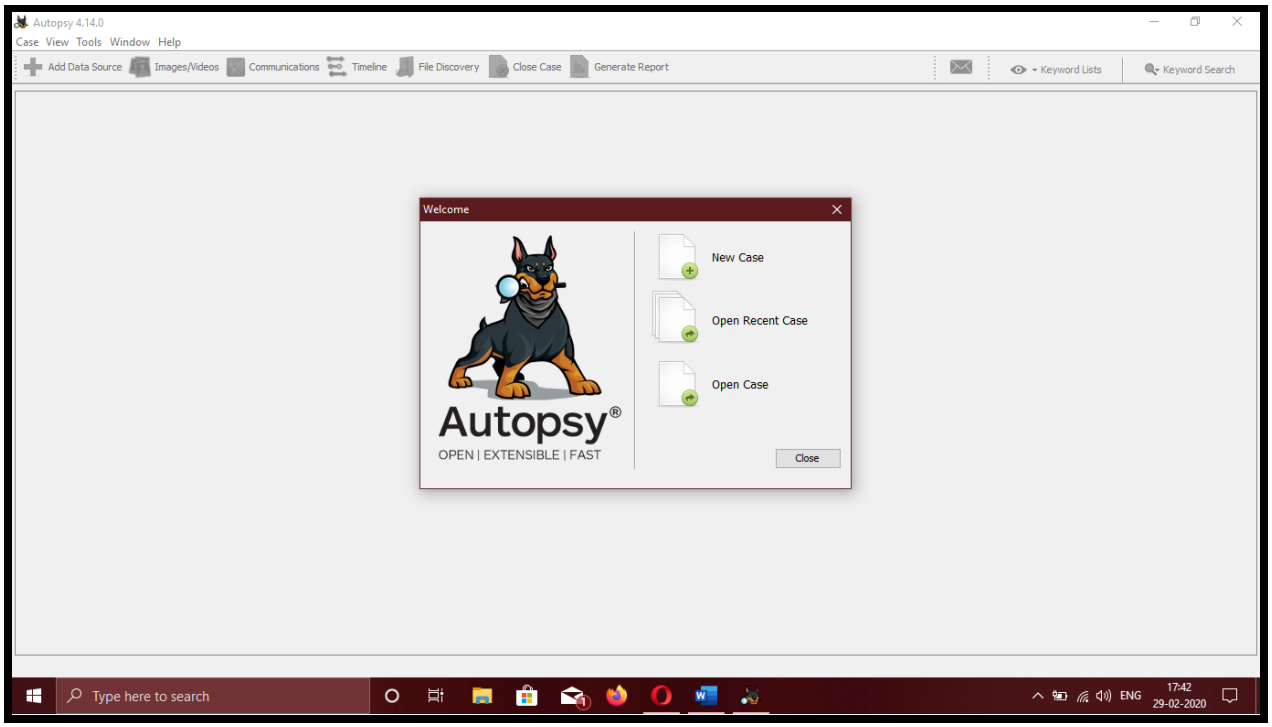
Tags: Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.

Unicode Strings Extraction: Extracts strings from unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).

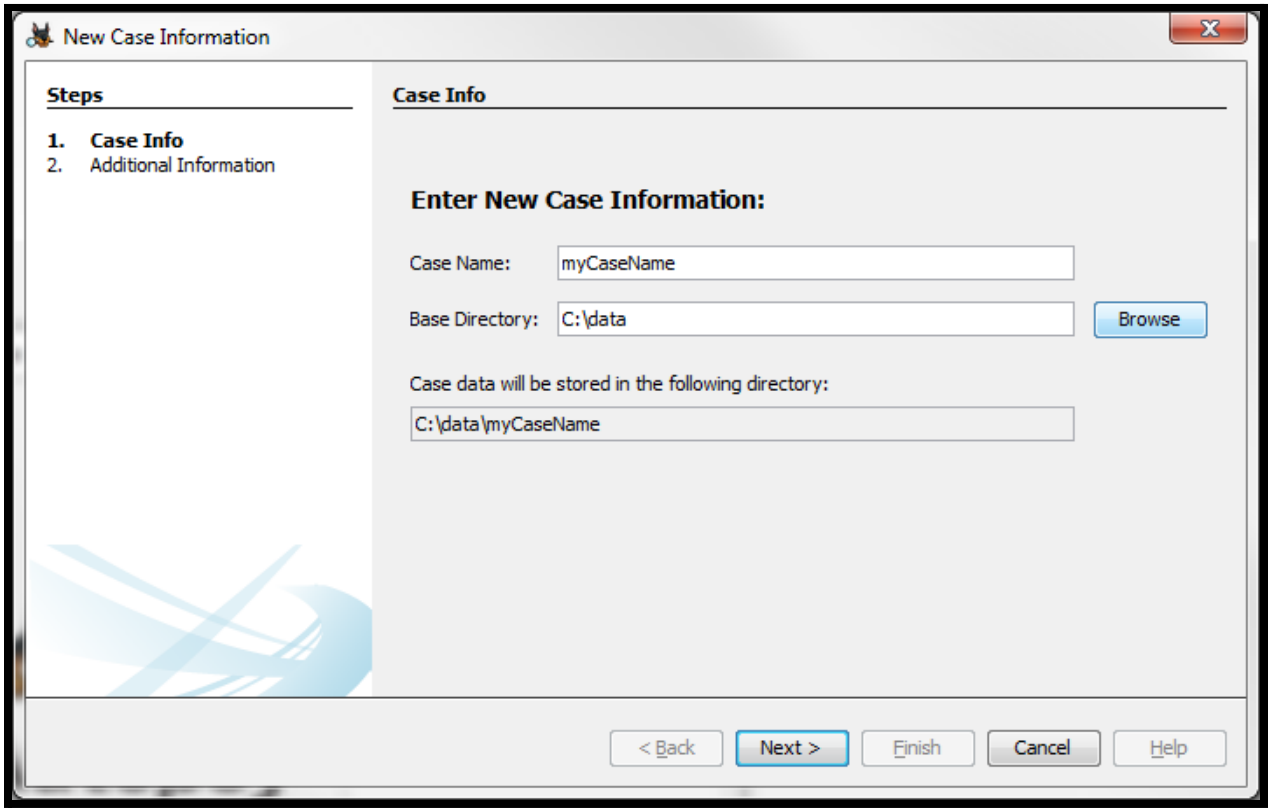
Android Support: Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.

How Can I Use..?

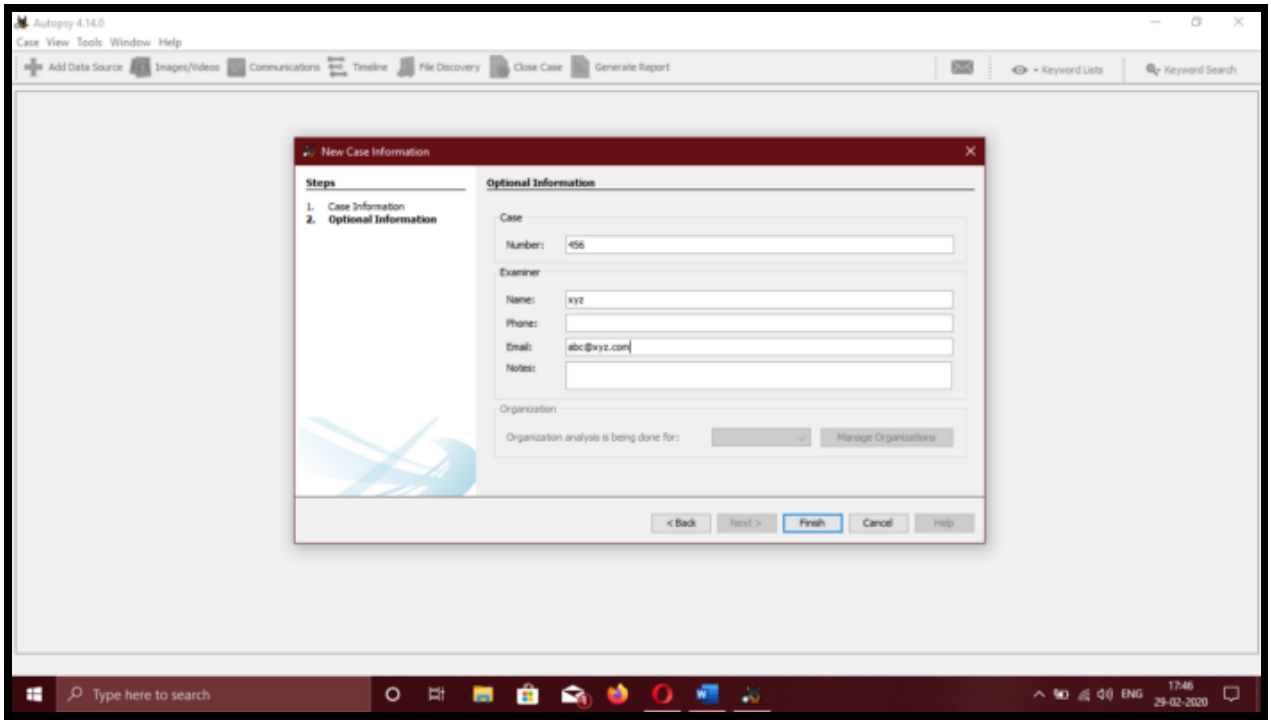
Step 1: Run Autopsy and select New Case.



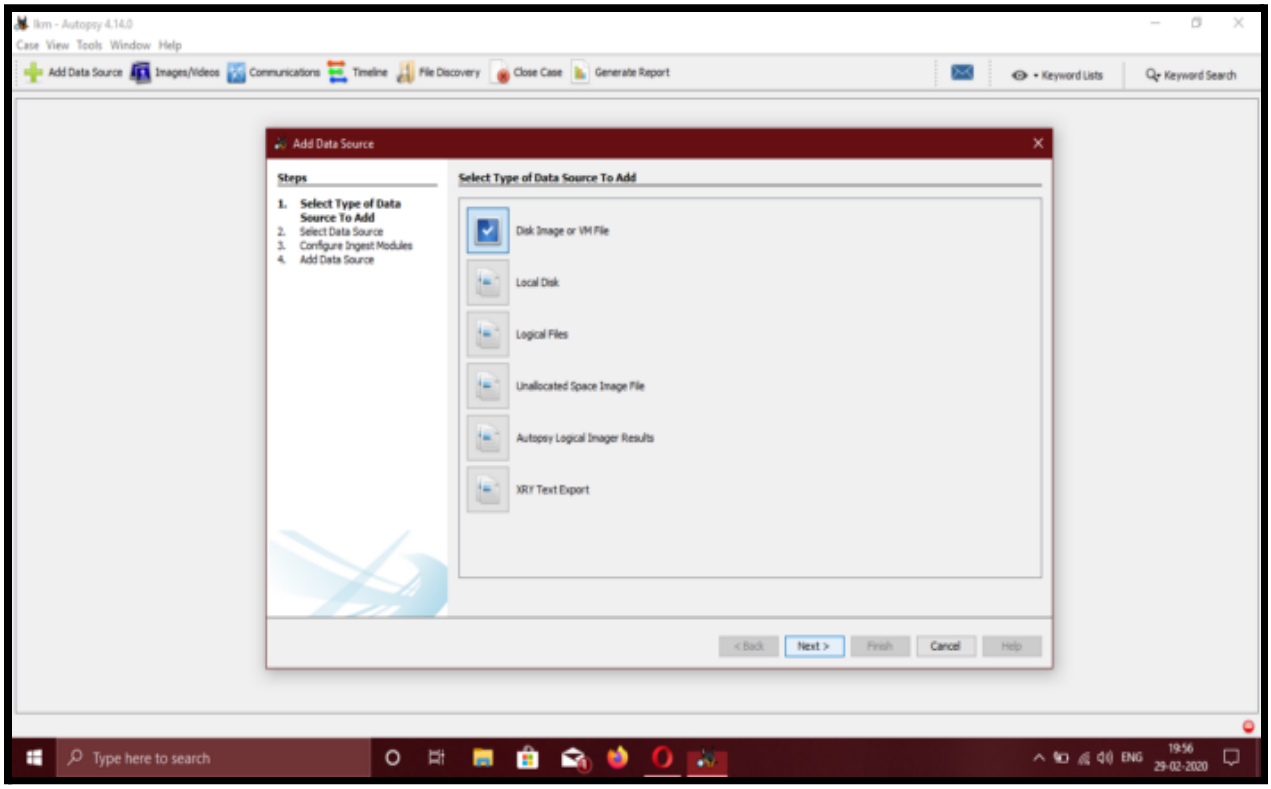
Step 2: Provide the Case Name and the directory to store the case file. Click on Next.



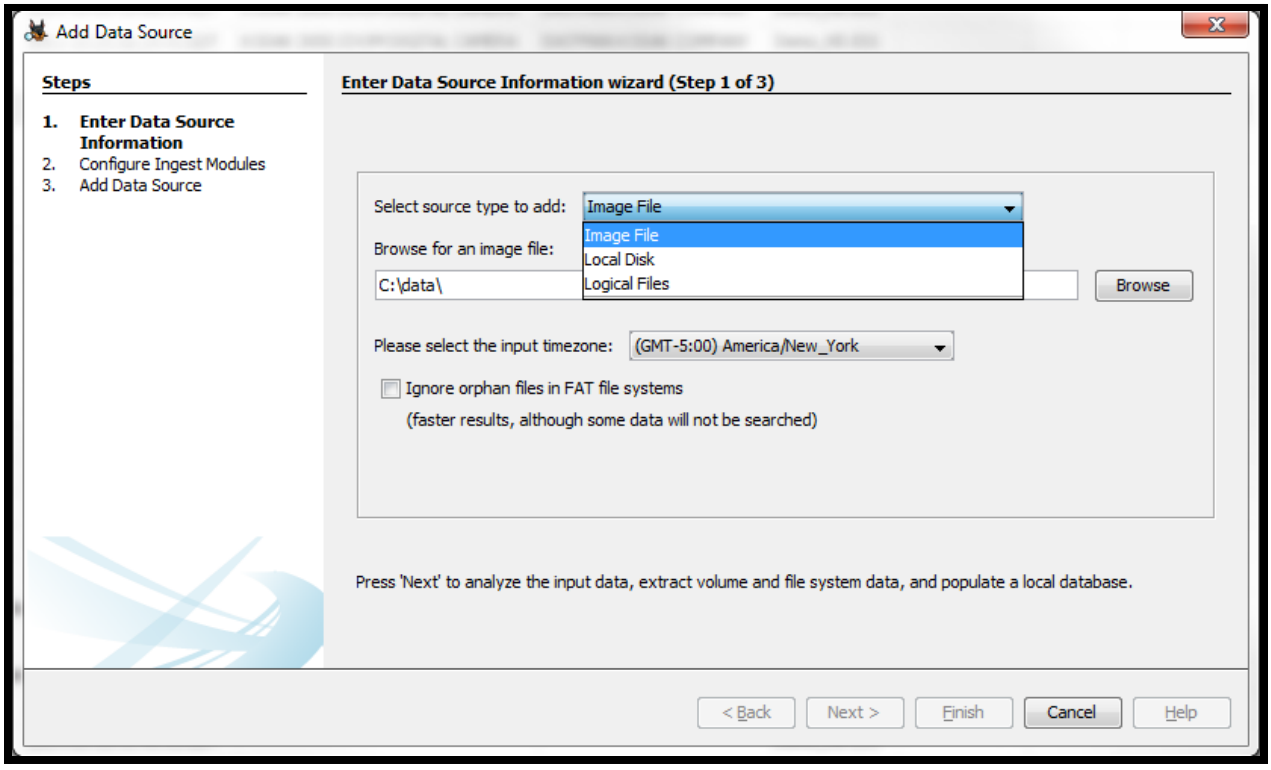
Step 3: Add Case Number and Examiner's details, then click on Finish.



Step 4: Choose the required data source type, in this case Disk Image and click on Next.

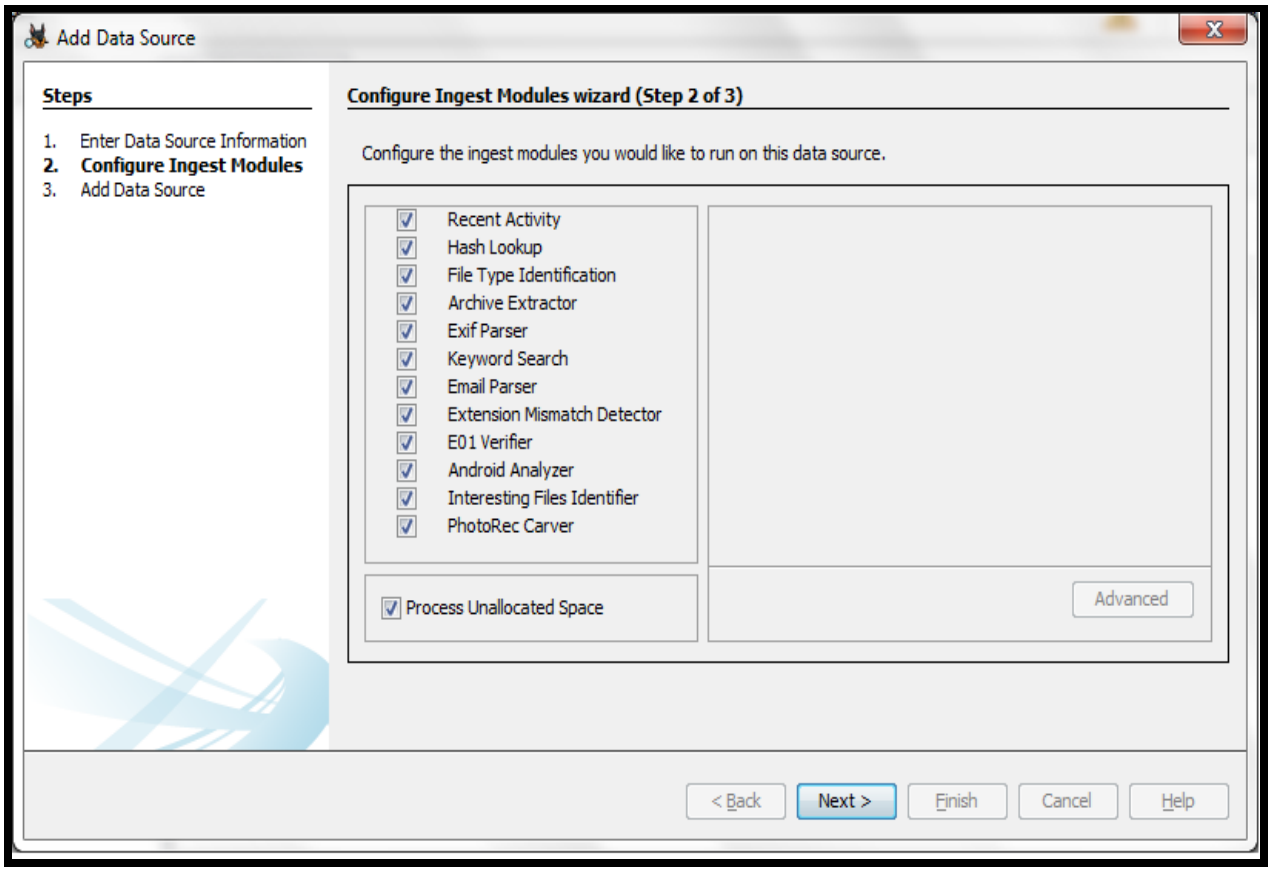


Step 5: Give path of the data source and click on Next.



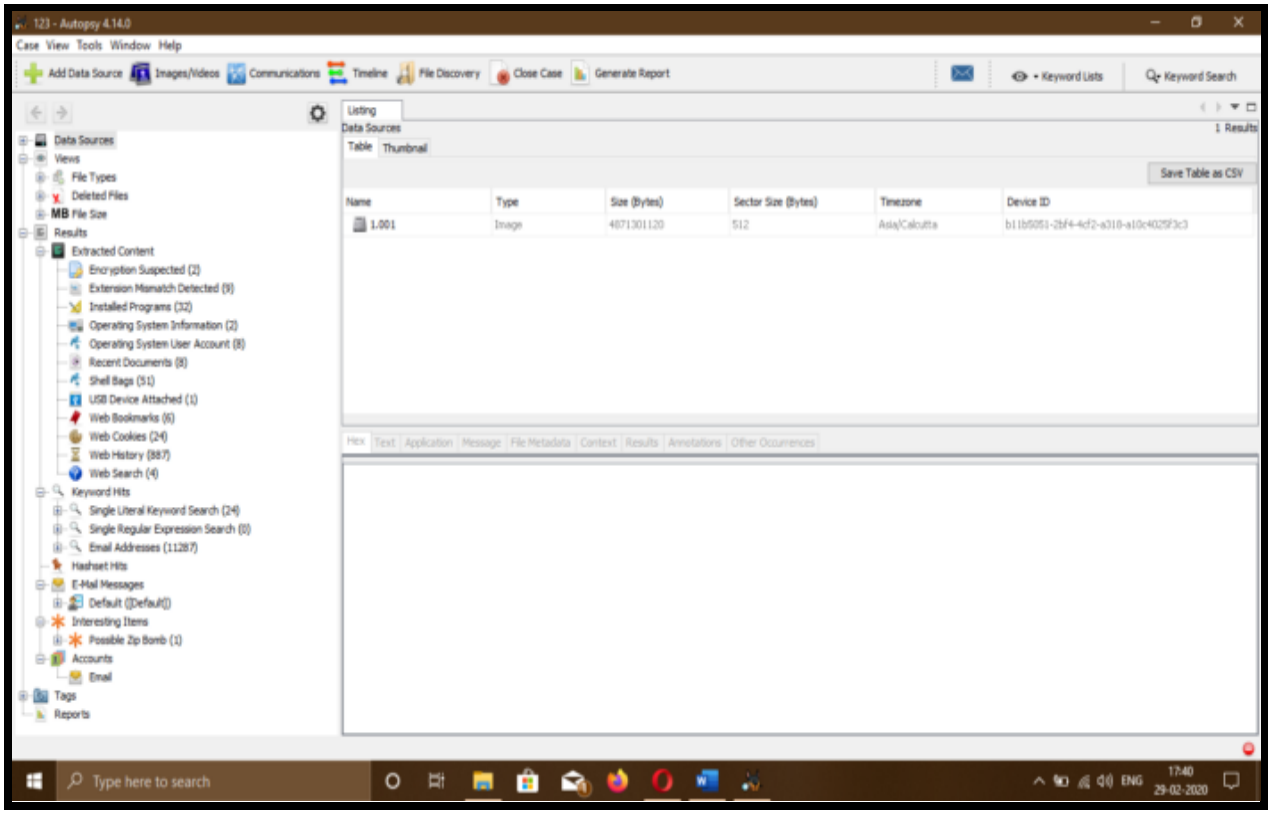
Step 6: Configure Ingest Modules

After the data source is included, ingest modules work out of sight to break down the information. Results are presented on the interface continuously and give cautions as important. Model ingests modules incorporate hash count and query, watchword looking, and web relic extraction. Third party modules can be created and added to the pipelines.



Step 7: After the data source has been added, click on Finish.

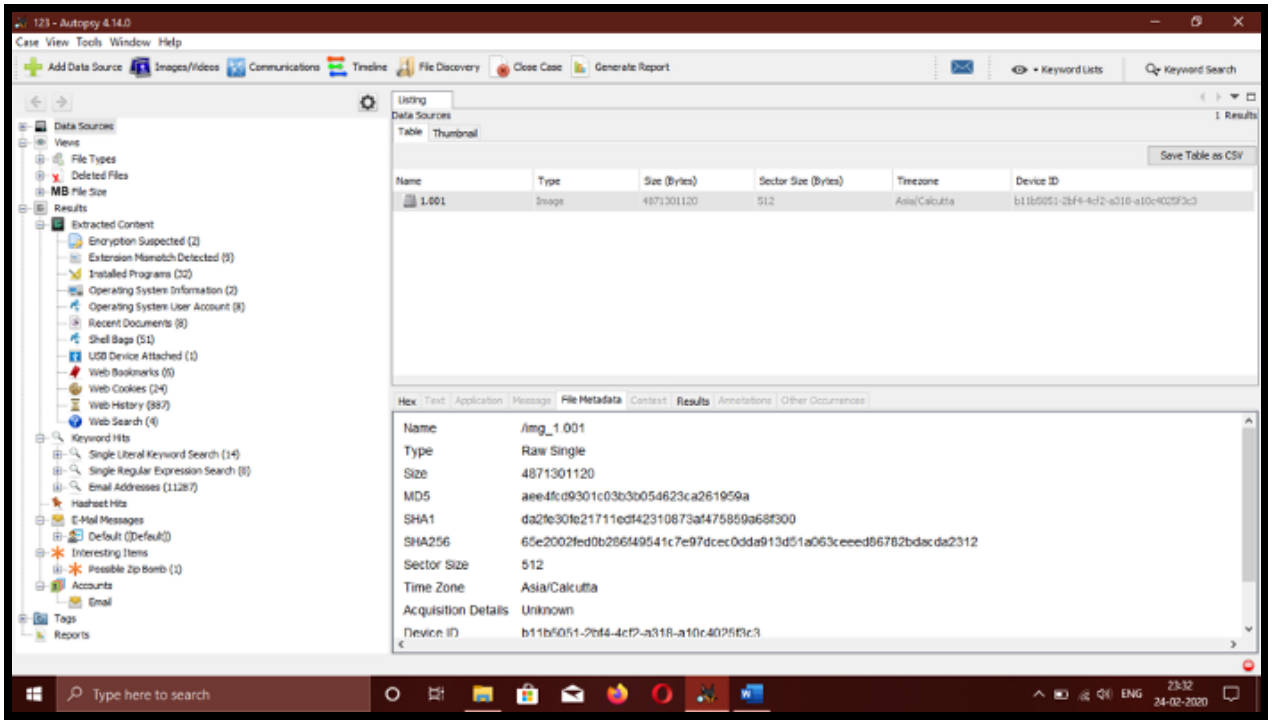
Step 8: You reach here once all the modules have been ingested. You can begin investigating but i recommend waiting until analysis and integrity check is complete.



Q1. What is the image hash?

Soln. AEE4FCD9301C03B3B054623CA261959A.

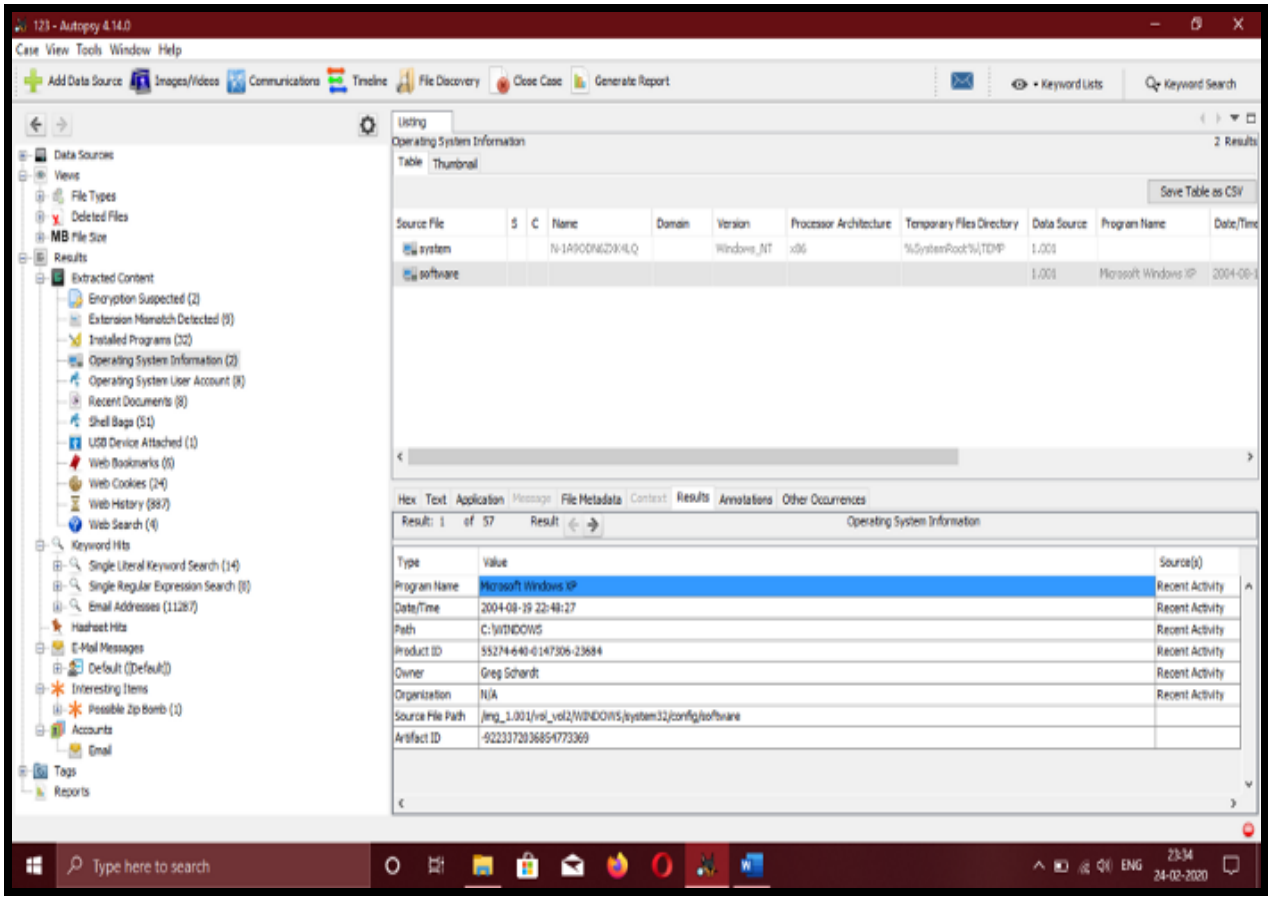
To check the image hash, click on image and go to File Metadata tab. (We check the image hash in order to verify that it is the same as the hash created during the time when the image was created.



Q2: What operating system was used on the computer?

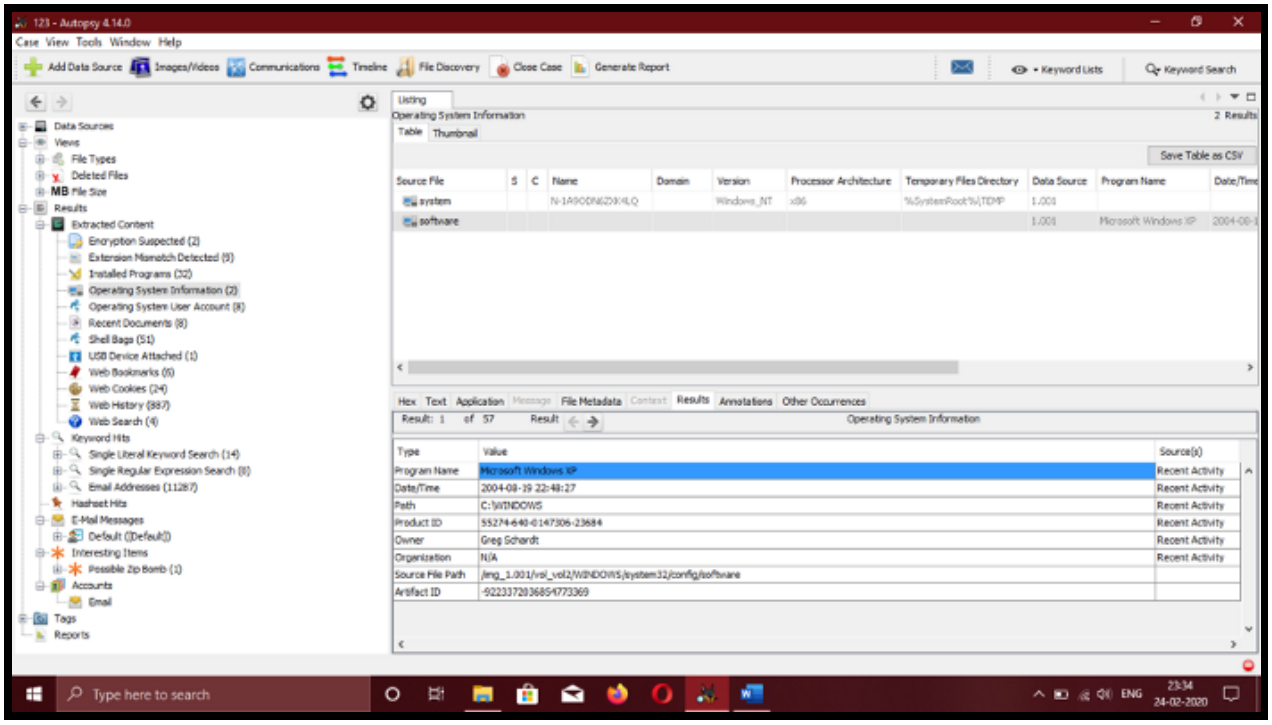
Soln: Microsoft Windows XP.

For this, in the left side panel, we go to Results > Extracted Content > Operating System Information.



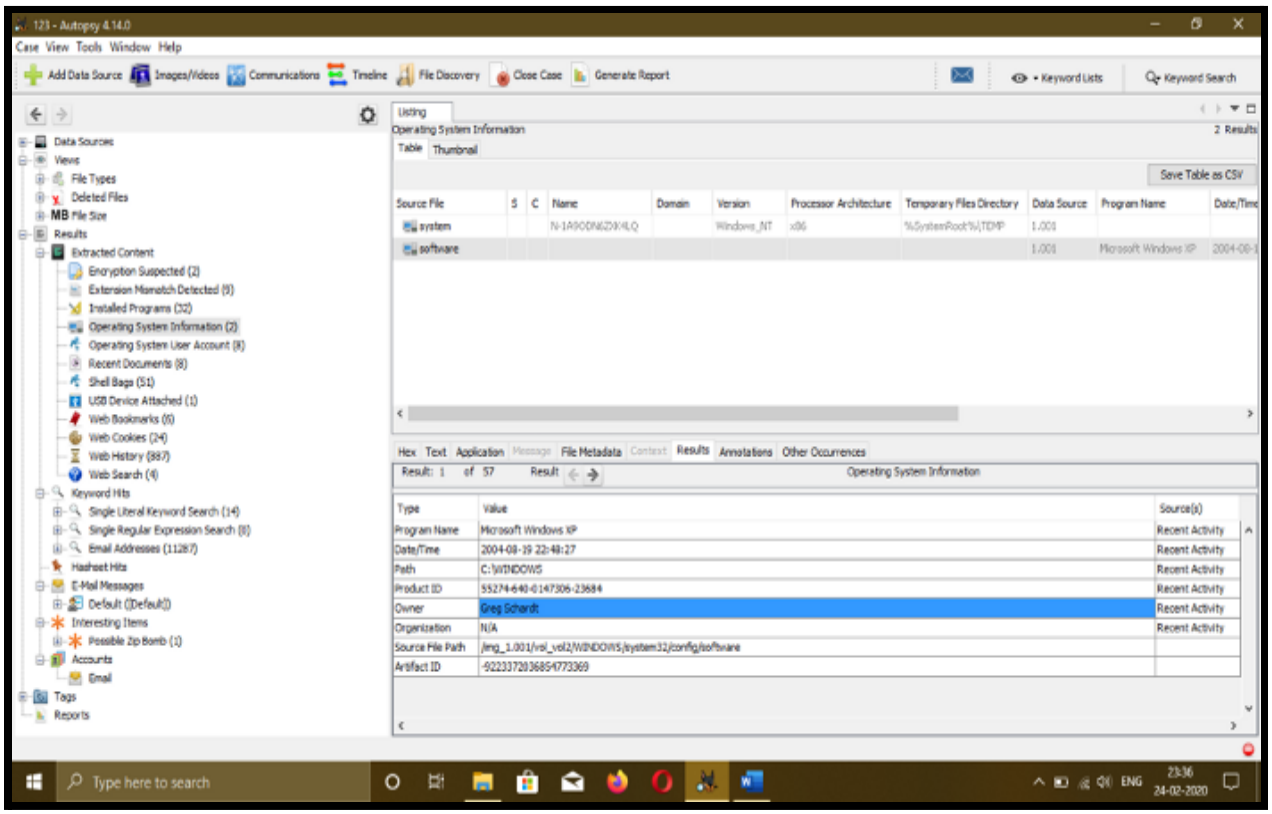
Q3: When was the install date?

Soln: GMT: Thursday, August 19, 2004 10:48:27 PM



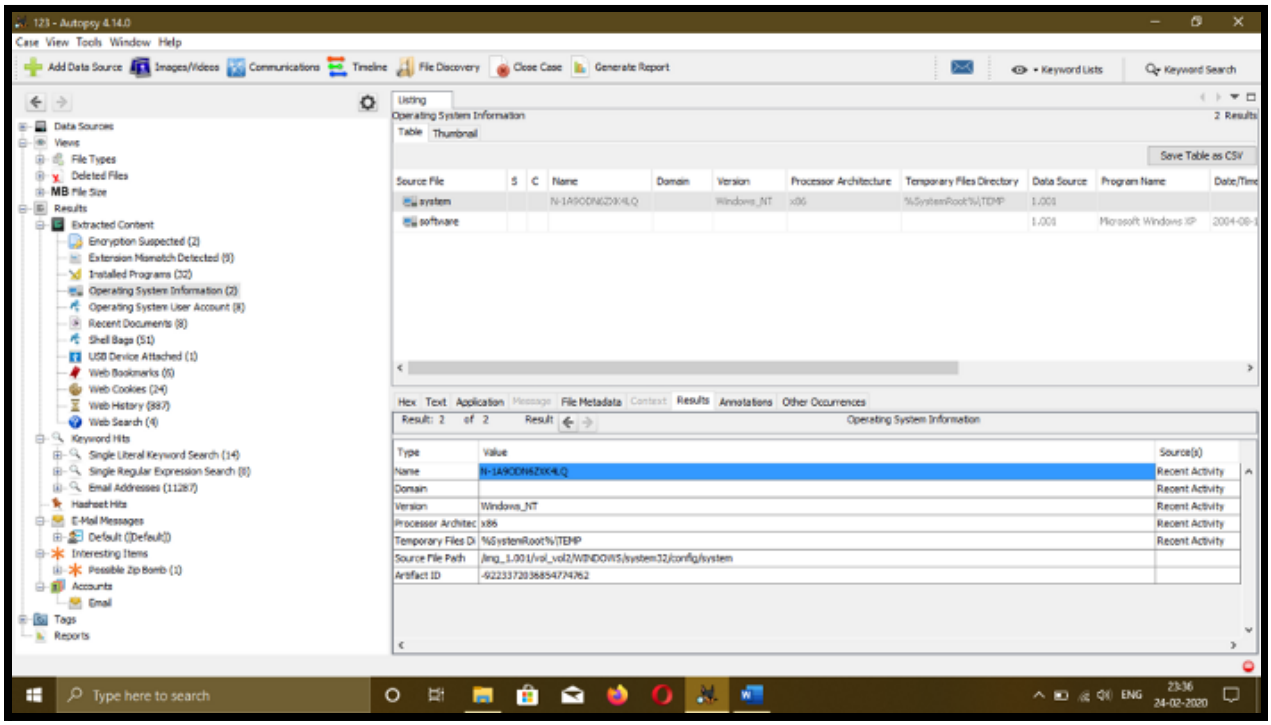
Q4. Who is the registered owner?

Soln. Greg Schard



Q5. What is the computer account name?

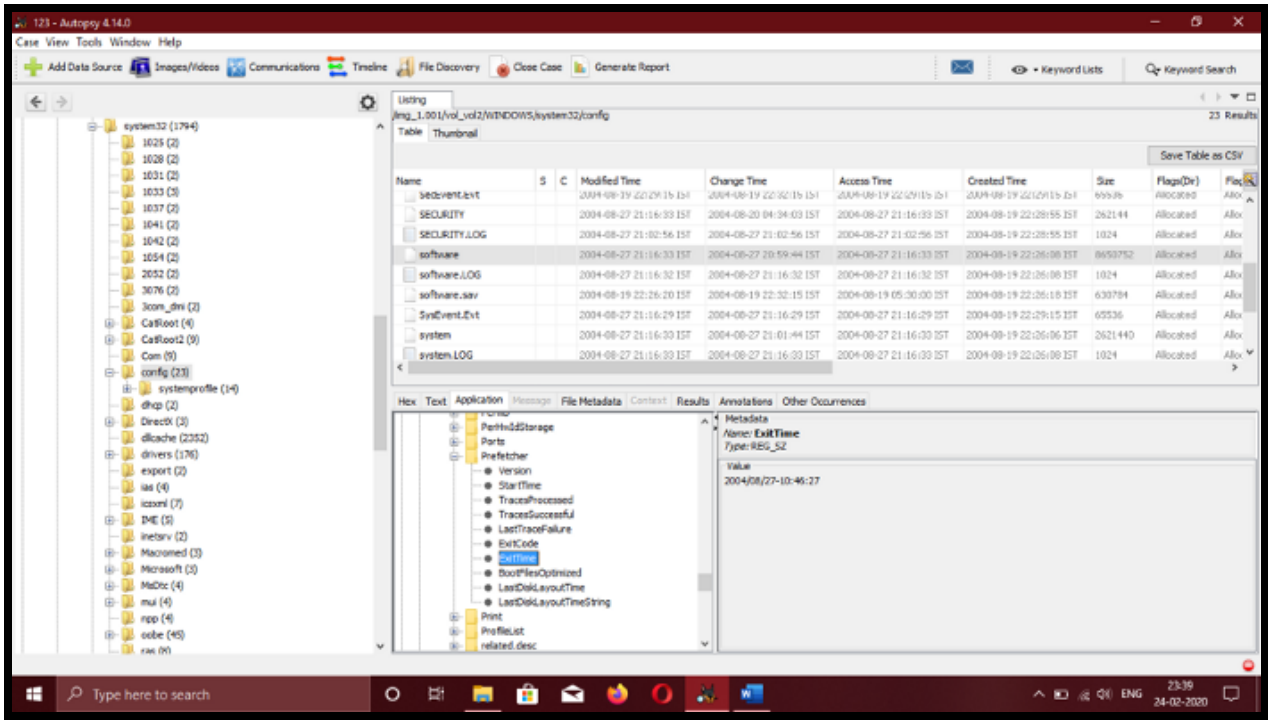
Soln. N-1A9ODN6ZXK4LQ (Click on System file)



Q6. When was the last recorded computer shutdown date/time?

Soln. 2004/08/27–10:46:27

To find this we go to C:\WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Prefetcher\ExitTime



Q7. How many accounts are recorded (total number)?

Soln. 5 accounts: Administrator, Guest, HelpAssistant, Mr. Evil, and SUPPORT_388945a0 (Look at the Account Type column).

In the left side panel, we go to Results > Extracted Content > Operating System User Account