Information Gathering and Digital Foot Printing.

Dr.Anil Kumar

Asso. Professor

PIET

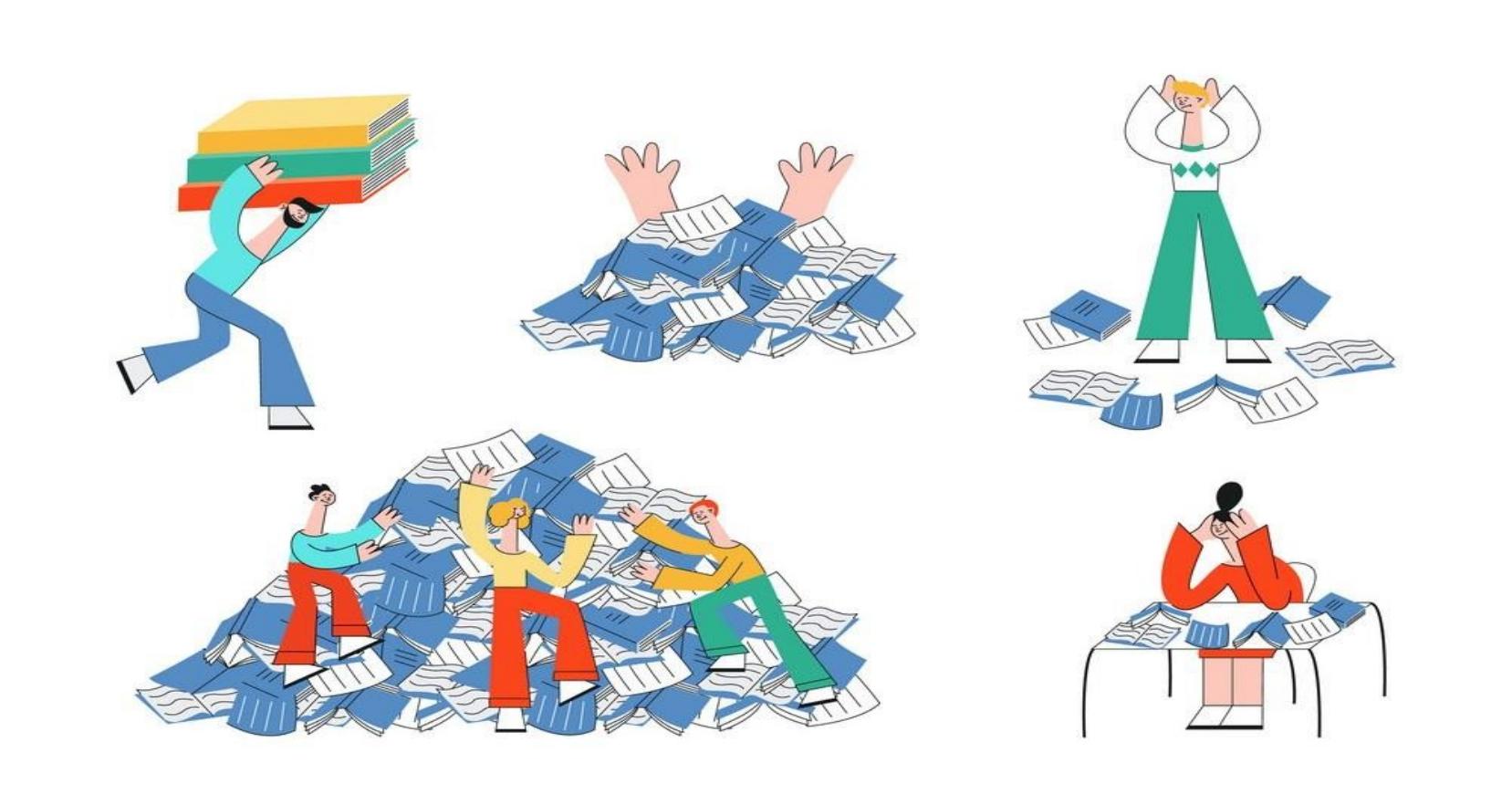
Introduction

- For just a simple hack and a well good and big hack, there are 5 phases which are needed to be followed for performing a successful hack.

1. Information Gathering
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

- Phase 1 and Phase 2 ---> Pre Exploitation
- Phase 3 ---> Exploitation
- Phase 4 and Phase 5 ---> Post Exploitation

The more information we get the more easy it will be in exploiting.



What is Information Gathering?

- Information gathering is the process of collecting the information from different places about any individual company, organization, server, IP address or person.

- Information gathering is the first step of hacking and most of the time of hacker spend his time in this process. 90% of time of a hacker spend in information gathering.

- Information gathering plays a very vital role for both investigating and attacking purposes.

Attacker's Point of View

- Attacker will first gather information like domain name, IP address, IP range, operating system, services, control panel, vulnerable services etc and later on exploit it.

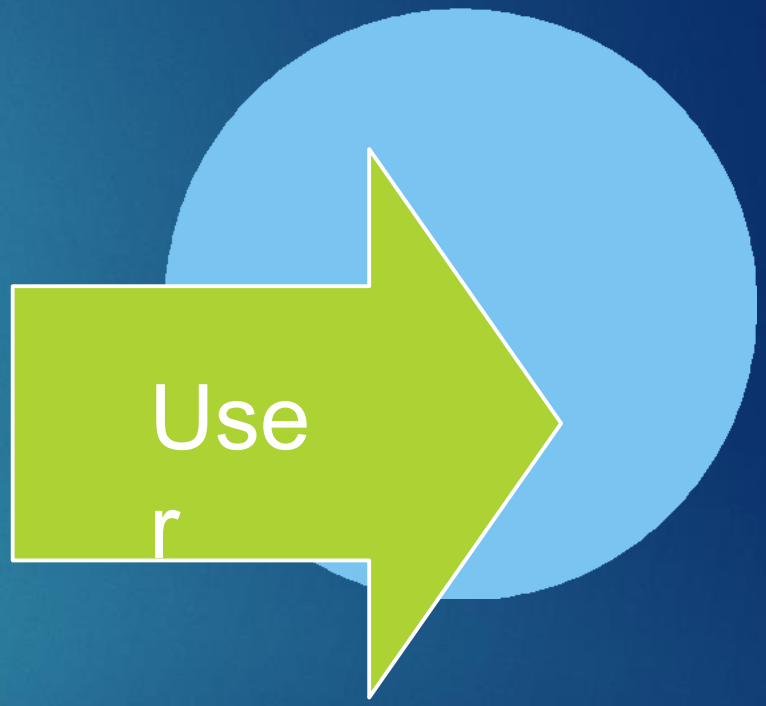
- Attackers use tools and social engineering to gather information.

- For attacking an individual person he will find his name, address, date of birth, phone no and his personal information and then use that information for attacking that person.

Investigator's Point of View

- It is powerful tool used in investigation process.
- Investigator will gather information like traces of criminal, name, address, contact no, company information etc before taking any legal action.
- Investigators use tools and social networking sites to gather information about criminal.

Example

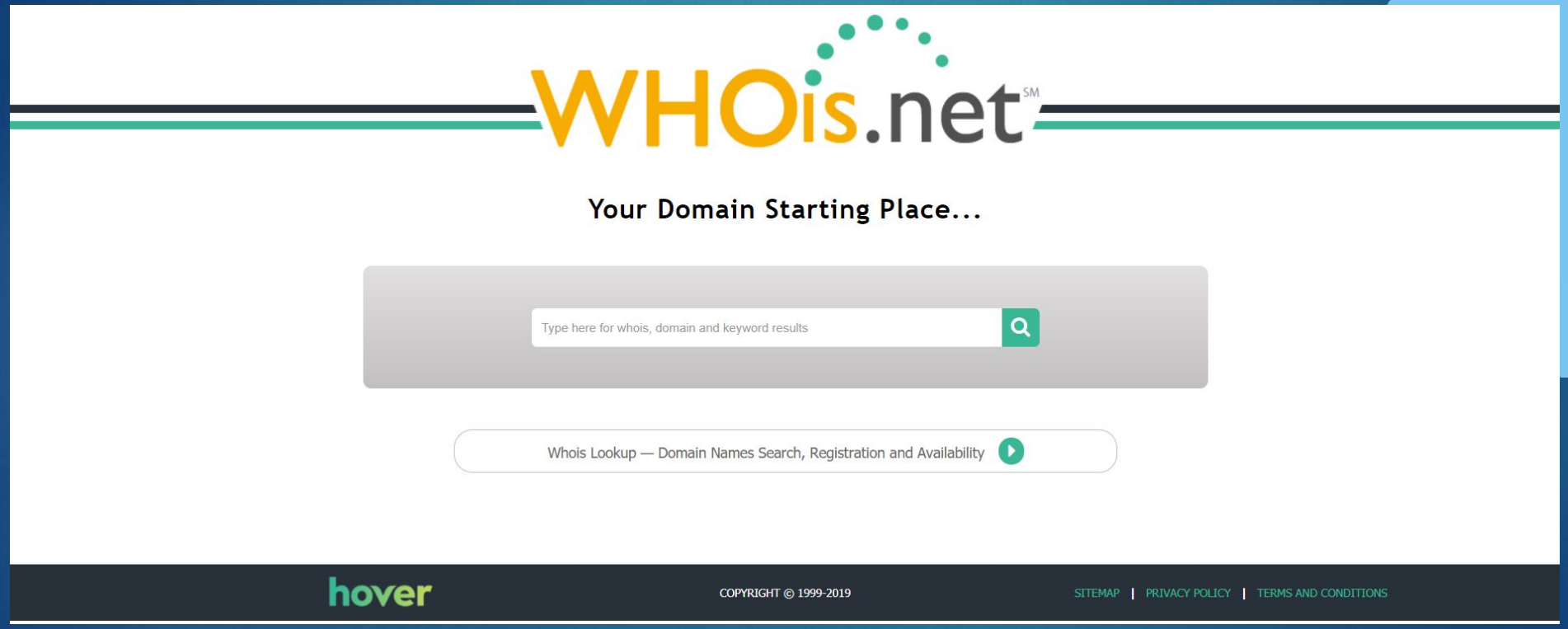


1. Whois

- Whois is query to database to get following information.

- Owner of website.
- Email id used to register domain.
- Domain registrar.
- Domain name server information.
- Related websites

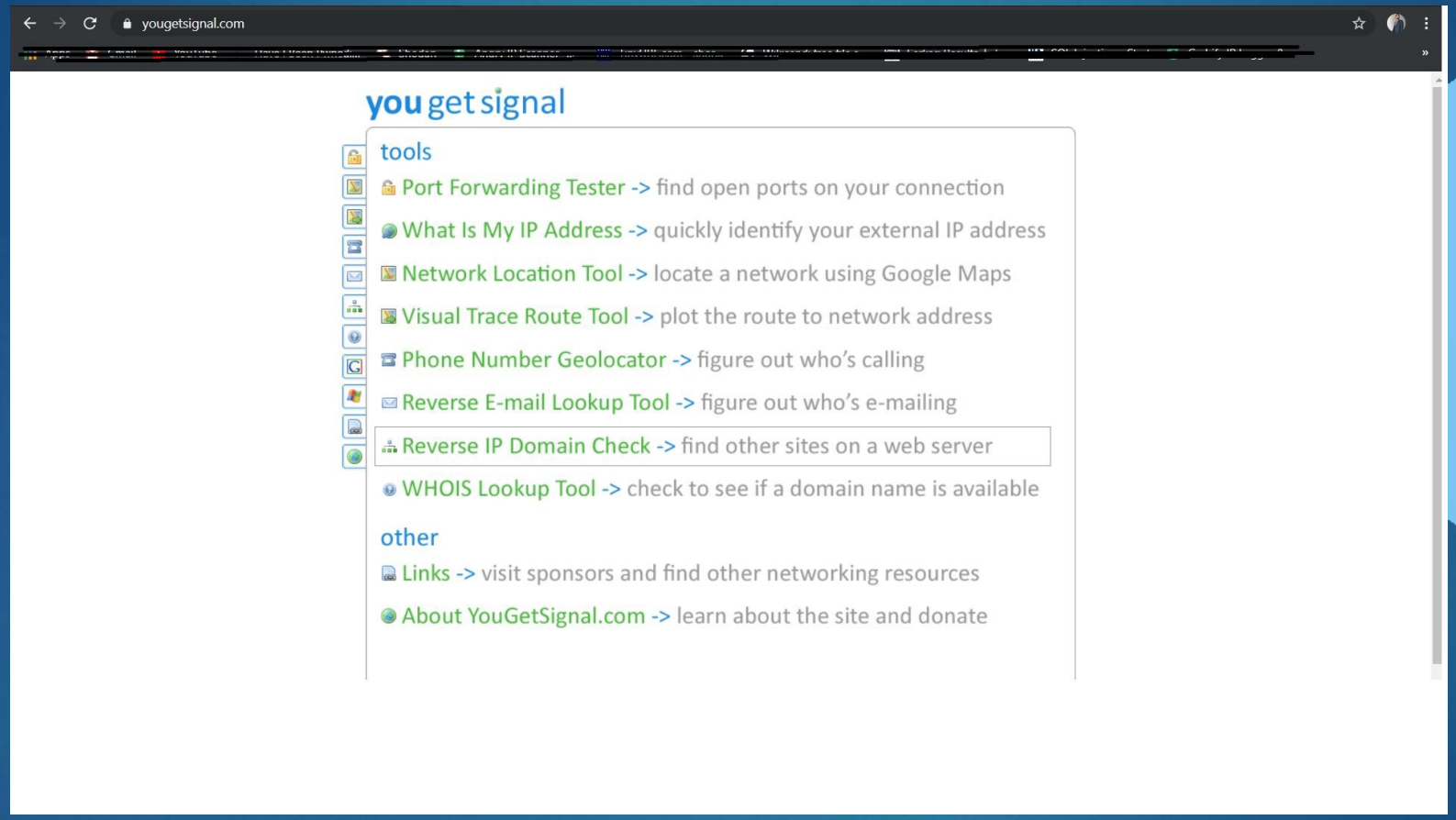
Whois.net has official database of all domains.



2. Reverse IP mapping

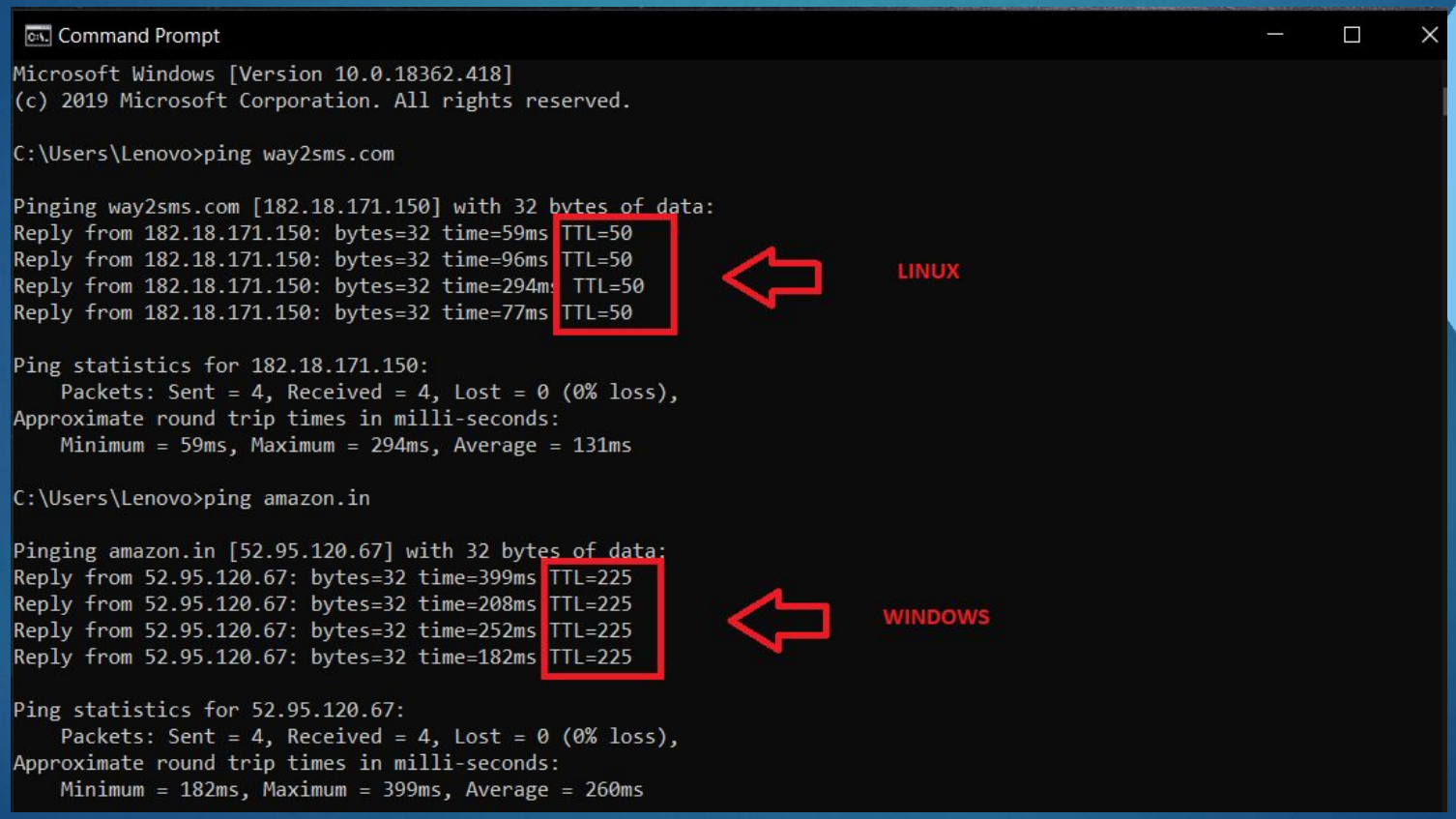
- Reverse IP will give number of websites hosted on same server.
- If one website is vulnerable on the server then hacker can easily root the server.
- With the help of this website one can get the information that the website is on shared or dedicated server.

Yougetsignal.com



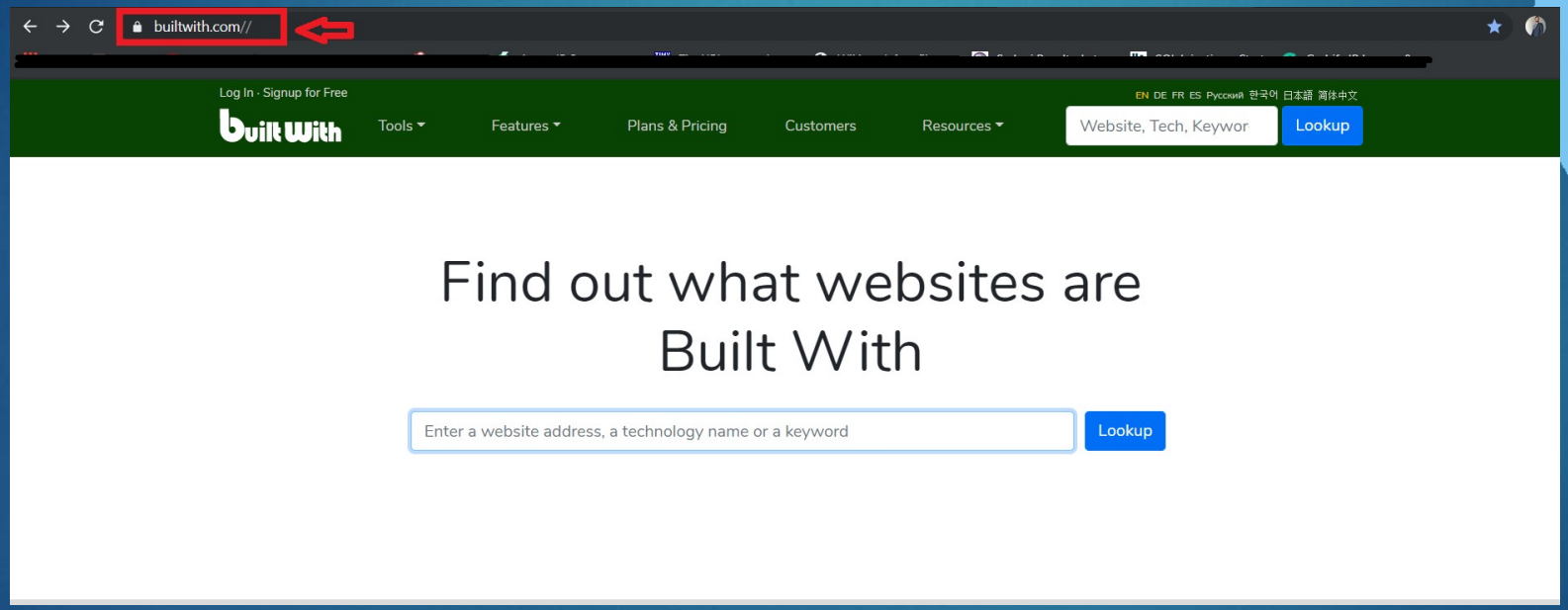
If our target is webserver itself then we will find open ports, Services and server OS.

3. To find the operating system on which the website is hosted.



4. Platform Information

- To get the information on which platform the website hosted/Running like- PHP and other information too.



If target is a person

Information about the user.

- Information through Image.
- Information through mail received.
- Information hacked data.
- Information through social media apps, job portal and matrimonial sites.
- Information through third party app like True caller, Maltego

Computer Forensics: A Brief Overview

- Scientific process of preserving, identifying, extracting, documenting, the data on computer
- The field of computer forensics began to evolve more than 30 years ago in the United States.
- With the growth of the Internet and increasing usage of technology devices connected to the Internet, computer crimes are increasing at a great speed

Computer Crimes

Computer Crime

Pure Computer Crime

- Ilegal access to a system or network
- Illegal transmission of data
- Data deletion, damage, alteration
- Serious hindrance to computer

Computer is medium of crime

- Identity theft
- Fraud
- E-theft

Computer content related crime

- Diddling of data stored in computer
- Child pornography
- Information that unleashes hostility/violence

Tools for computer Forensics

Computer Forensic tools

Integrated GUI Based tools

Specialized single task tools

i. Process Information
ii. Network Connection Information
iii. Process of Port mapping
iv. Executable file analysis

Three Branches

1. Network Forensic
2. Database Forensic
3. Mobile Device Forensic

Network Forensic

- Network Forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

Two Systems

1. Catch-it-as-you-can.
2. Stop, look and listen

Database forensic

- Forensic study of databases .
- Currently many database software tools are in general not reliable and precise enough to be used for forensic work.

Mobile Device Forensics

- Using such things as cell phones, digital cameras, psp's, and I pods to find stored evidence.
- Mobile devices can be used to save several types of personal information like contacts, photos, calendar and notes.
- Therefore it can be supposed that these devices will play an important role in forensics.

Common Types of cases

1. Financial crimes
2. Drug crimes
3. Child Pornography
4. Adultery
5. Murders/ Suicides

How it is performed

There are **five** basic steps to the computer forensic

1. Preparation (of the investigator, not the data)
2. Collection (the data)
3. Examination
4. Analysis
5. Reporting

Preparation

1. Proper training for investigation.
2. Must use validated tools.
3. Proper interview of the user because user can yield valuable information.
4. Investigator must have legal authority to do any change if required.

Collection

1. Collection sources include computers, cell phones, digital cameras, hard drives, CD-ROM, and USB memory devices.
2. Special care must be taken when handling computer evidence. Most digital information is easily changed, and once changed it is usually impossible to detect that a change has taken place.
3. Documenting everything that has been done.

Examination

1. Computer evidence represented by physical items such as chips, boards, central processing units, storage media, monitors, and printers can be described easily and correctly as a unique form of physical evidence.
2. Examiner must make a decision as to how to implement this principle on a case-by-case basis.

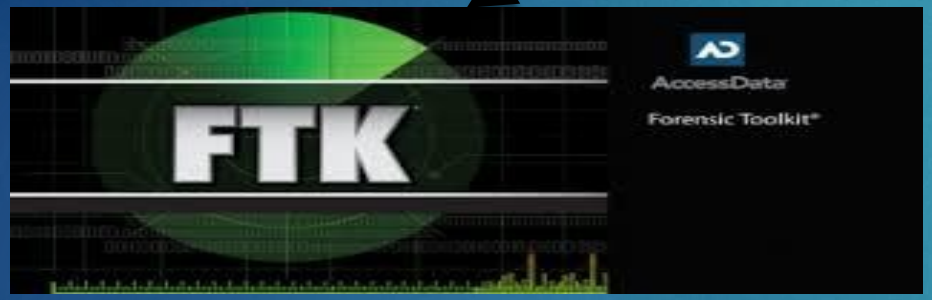
Analysis

1. All digital evidence must be analyzed to determine the type of
information that is stored upon it.
2. Specialty tools are used that can display information.

Reporting

1. Once the analysis is complete, a report is generated.
2. This report may be a written report, oral testimony, some or combination of the two.

TOOLS


FTK
AccessData
Forensic Toolkit

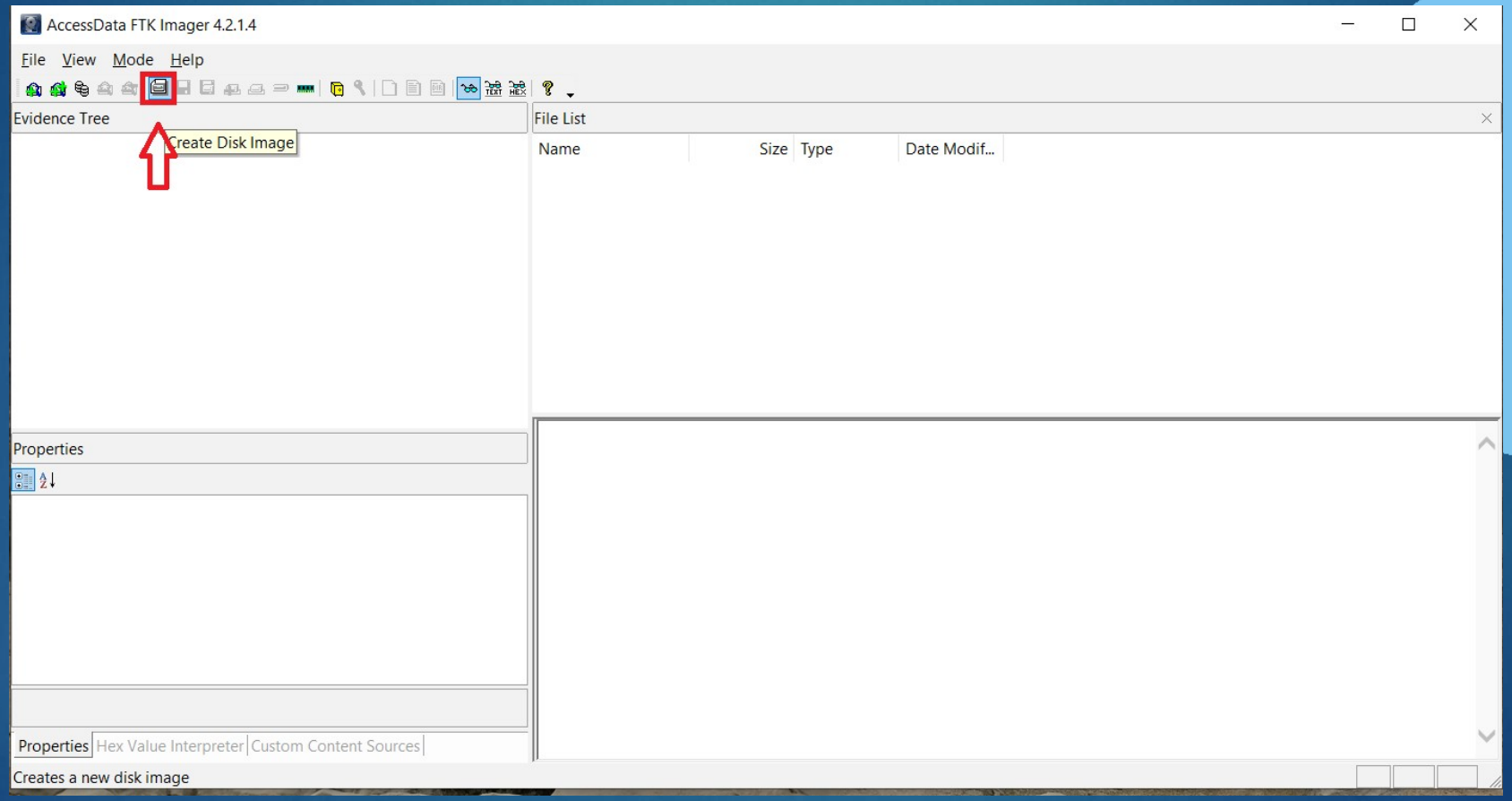

AUTOPSY
DIGITAL FORENSICS

What is Access Data FTK Imager ?

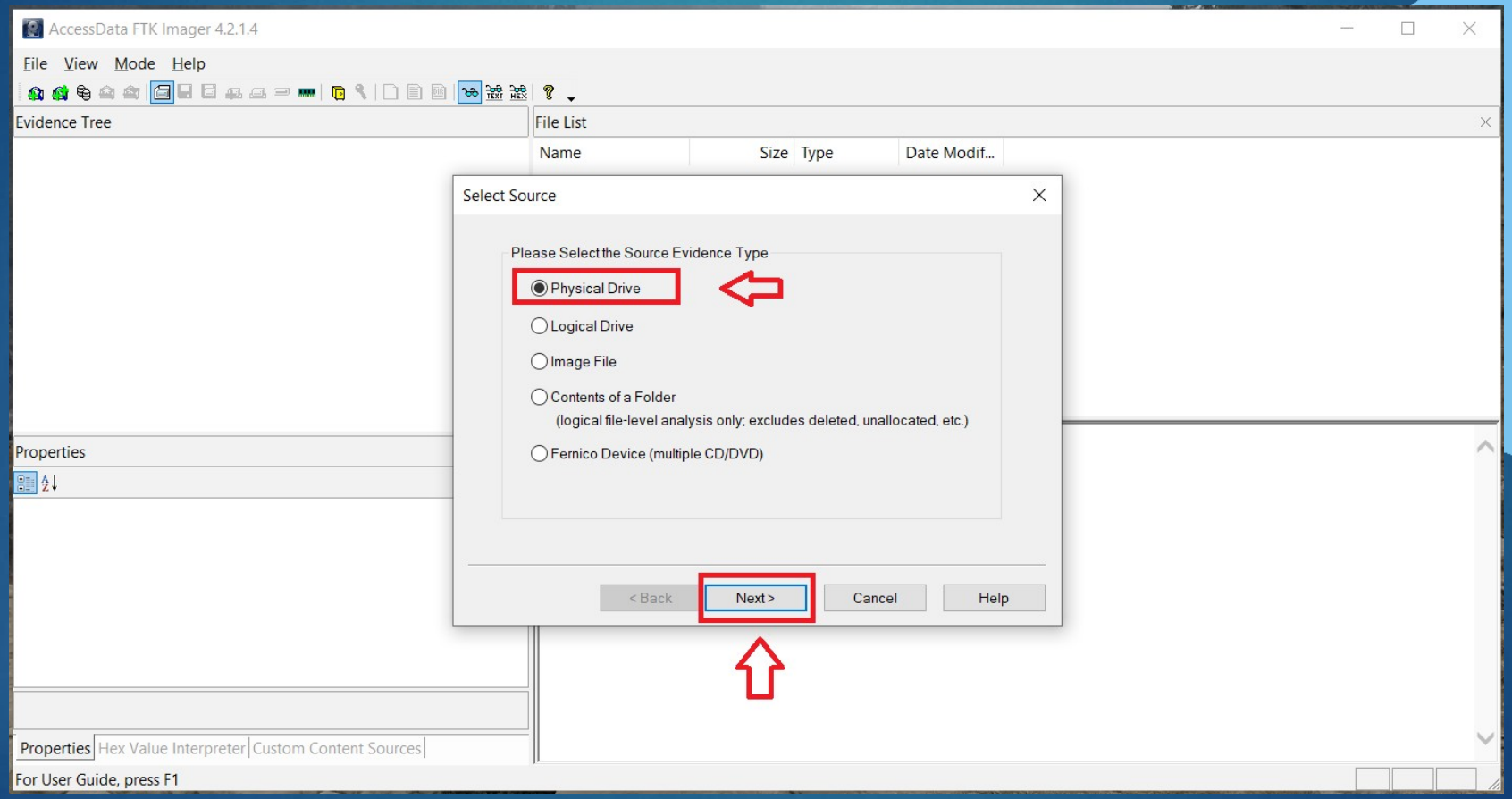
- **FTK Imager** is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence.

- **Create forensic images**
- **Preview the contents**

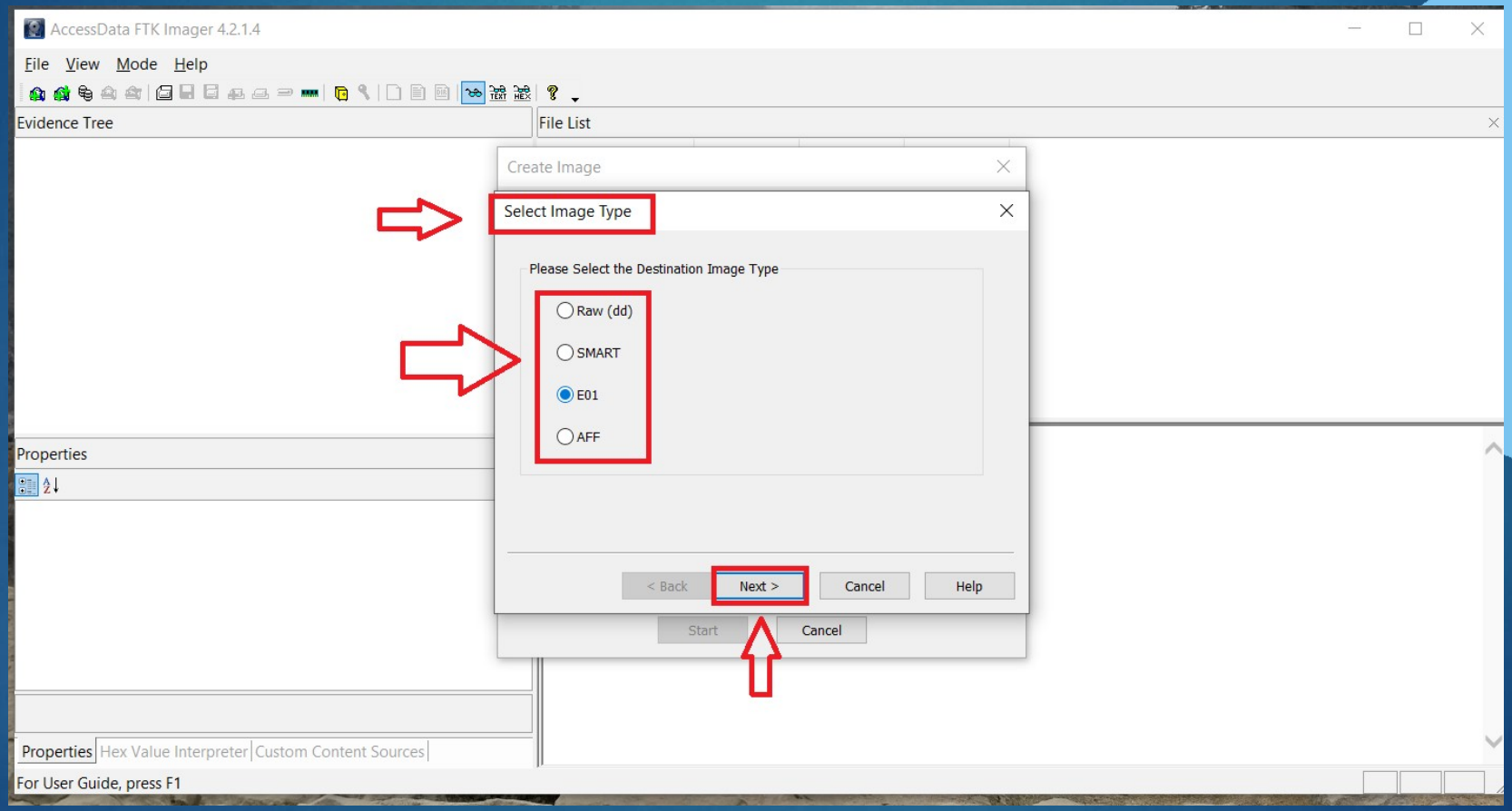
Step 1 Start creating Imager



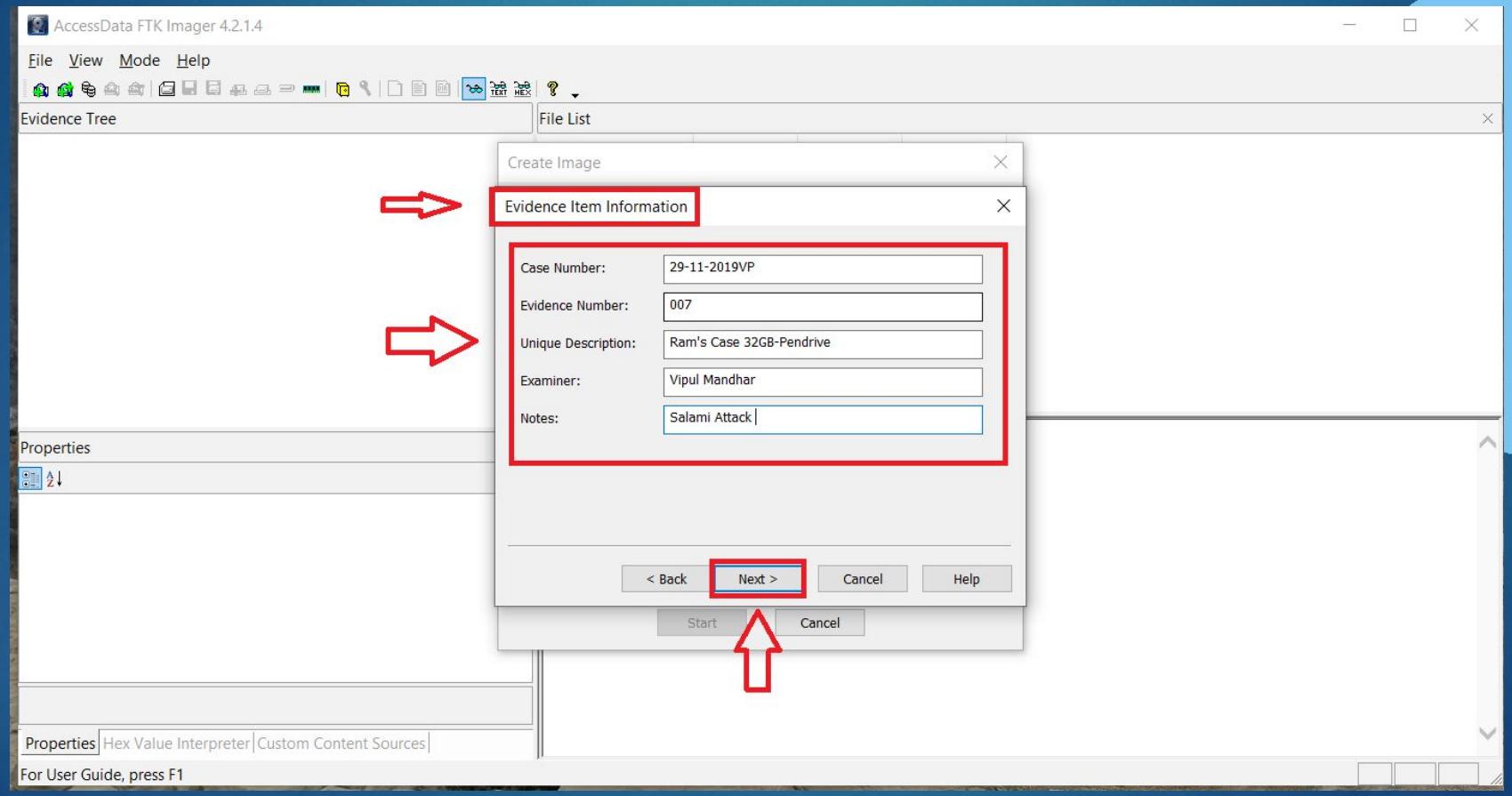
Step 2 Select Source File



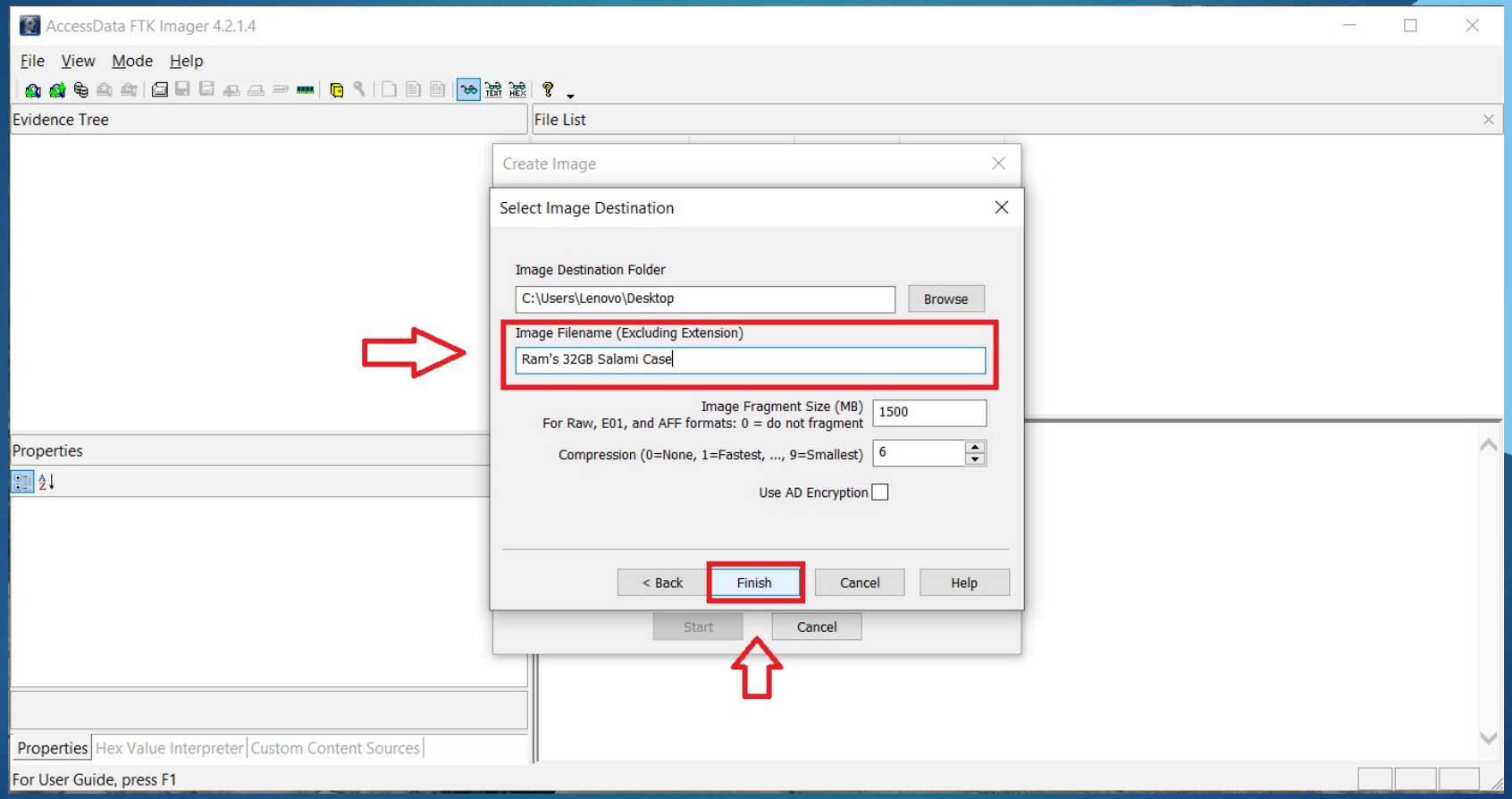
Step 3 Select the destination Image type



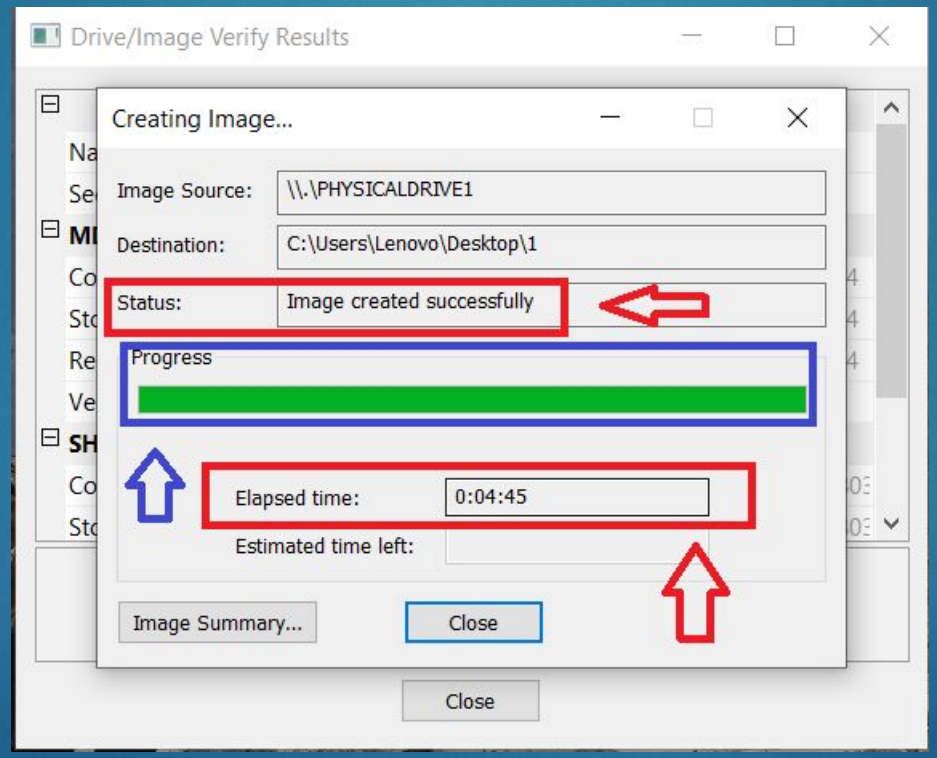
Step 4 Give Evidence Item information



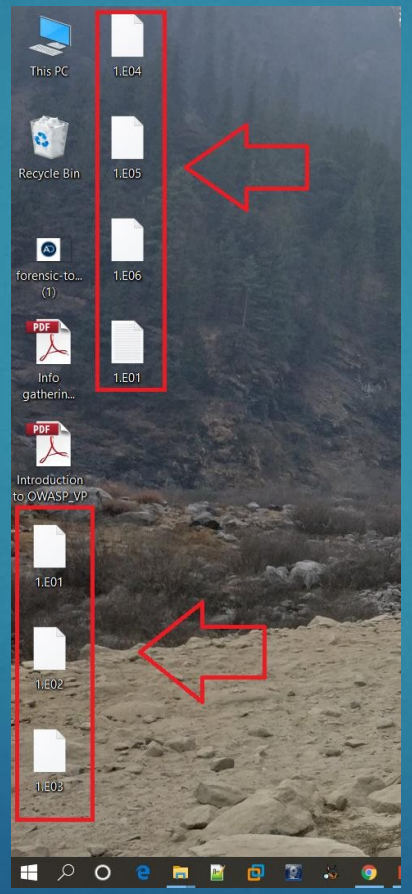
Step 5 Select Destination folder and Image file name



Step 6 Finalization



Total no of file created by Access data FTK imager



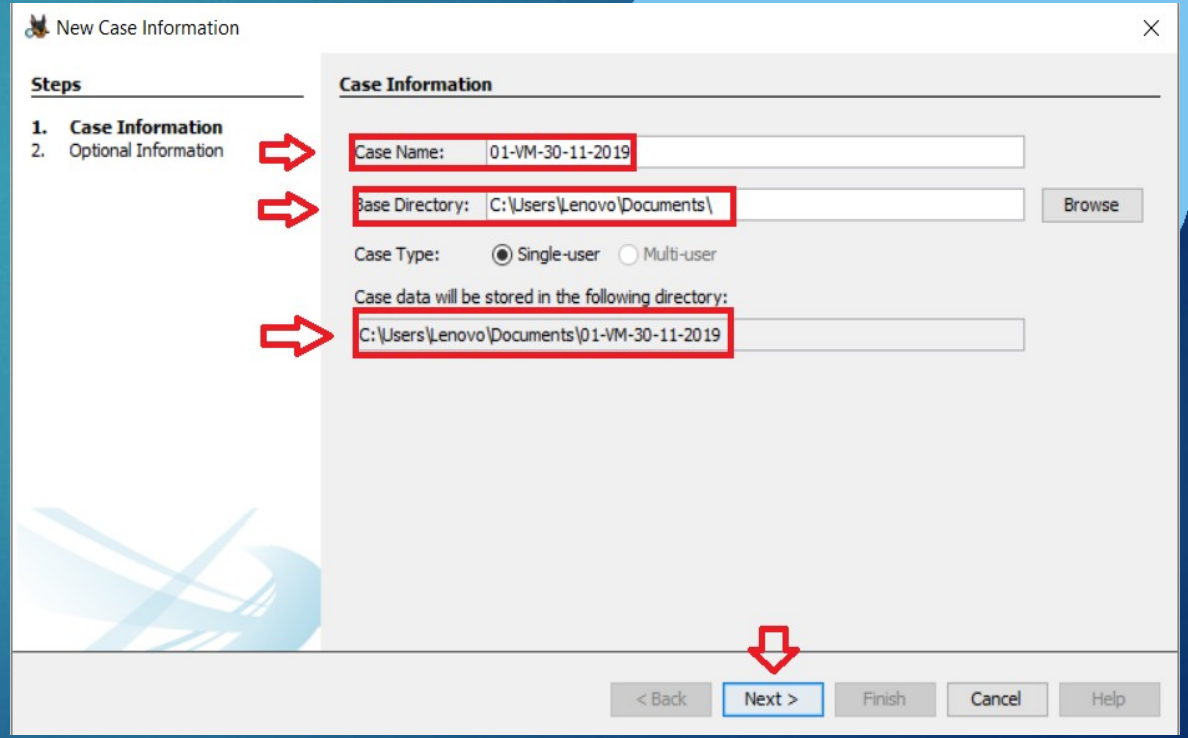
What is Autopsy ?

- Autopsy is an open source tool used for digital forensics investigations to conduct disk image, local drive, and folder and file analysis.
- Some of the Autopsy features include timeline analysis, keyword search, registry analysis, email analysis, file type sorting, hash set filtering, and various ingest modules that look for evidence.

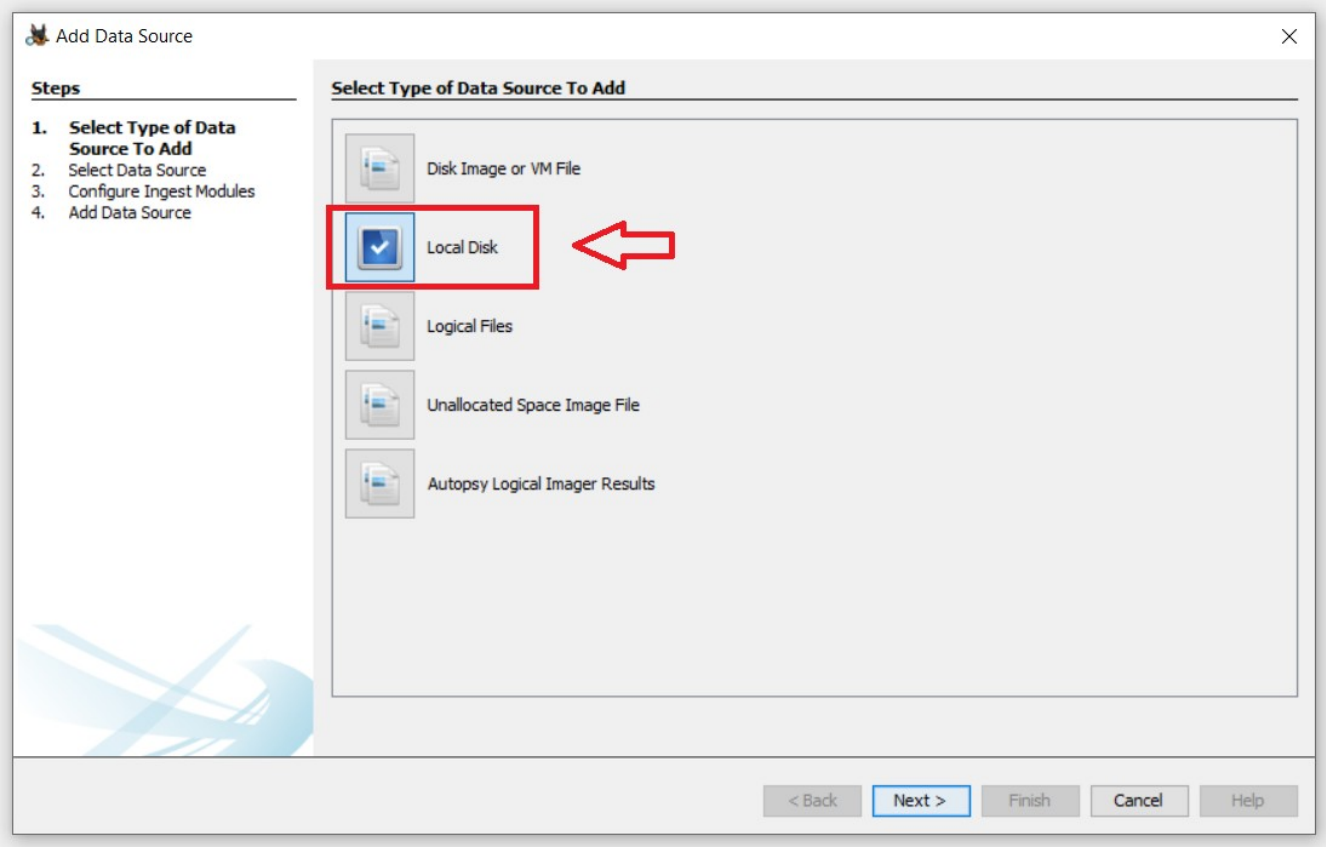
Step 1. Initialization process

- Select the type of case

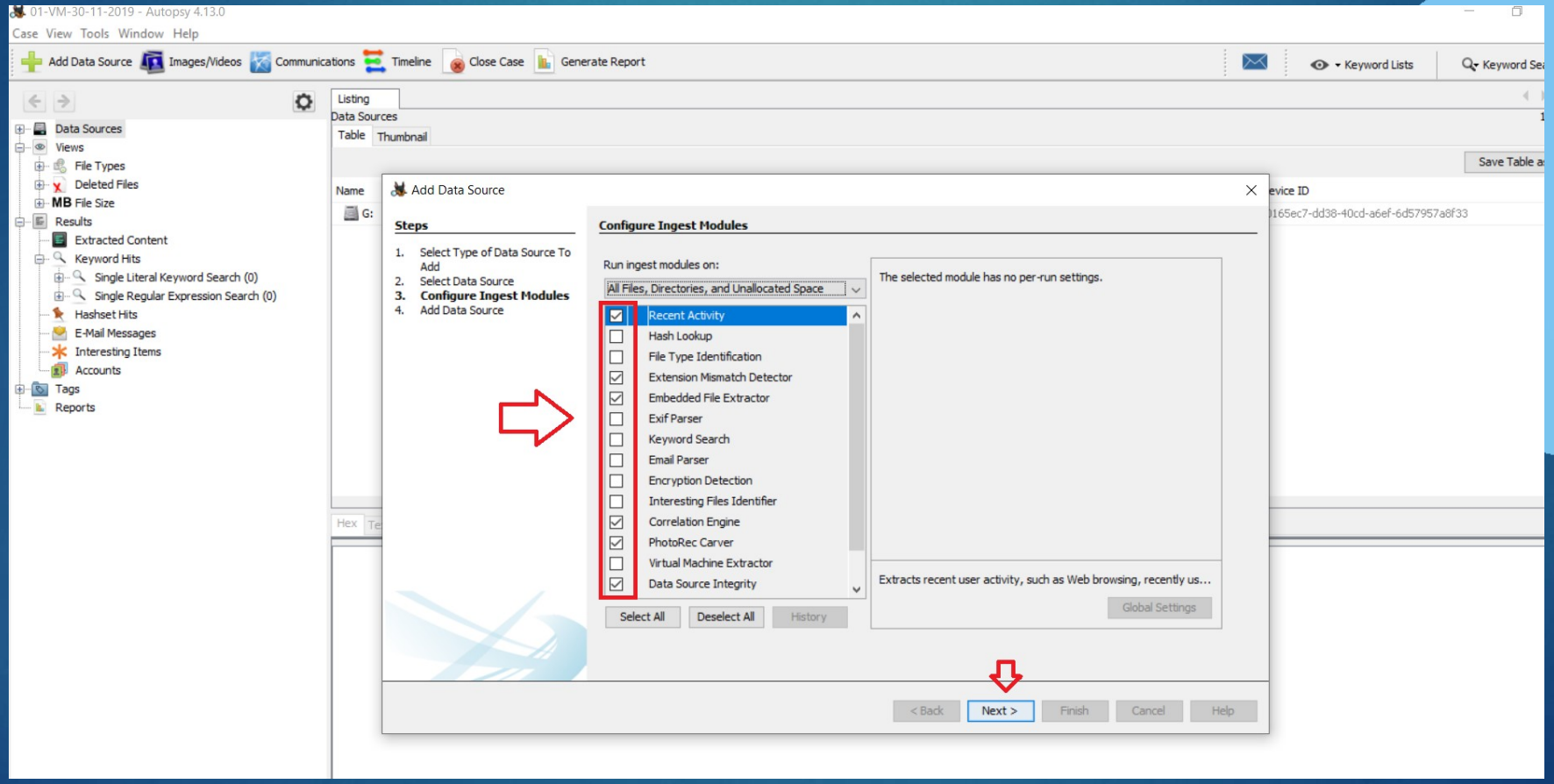
- Give Case Information



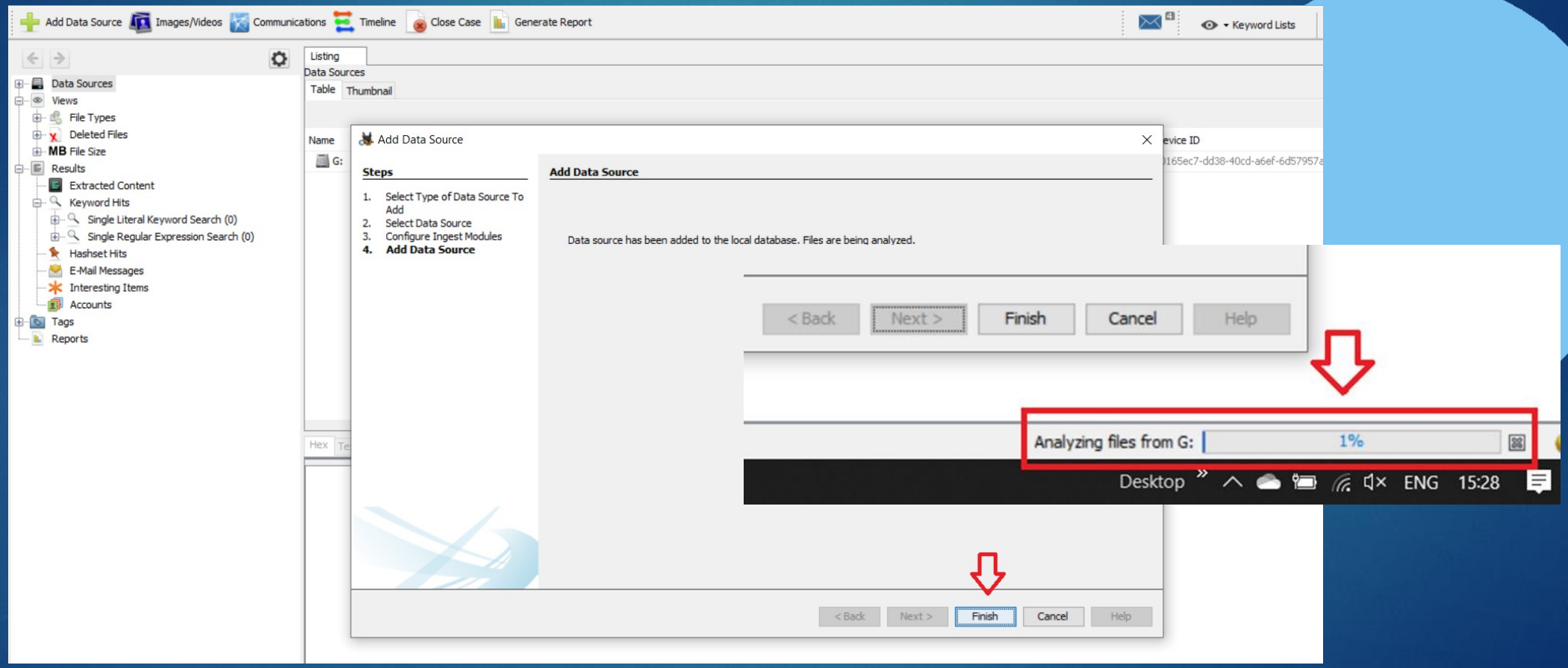
Step 2. Select source from where you want to grab information



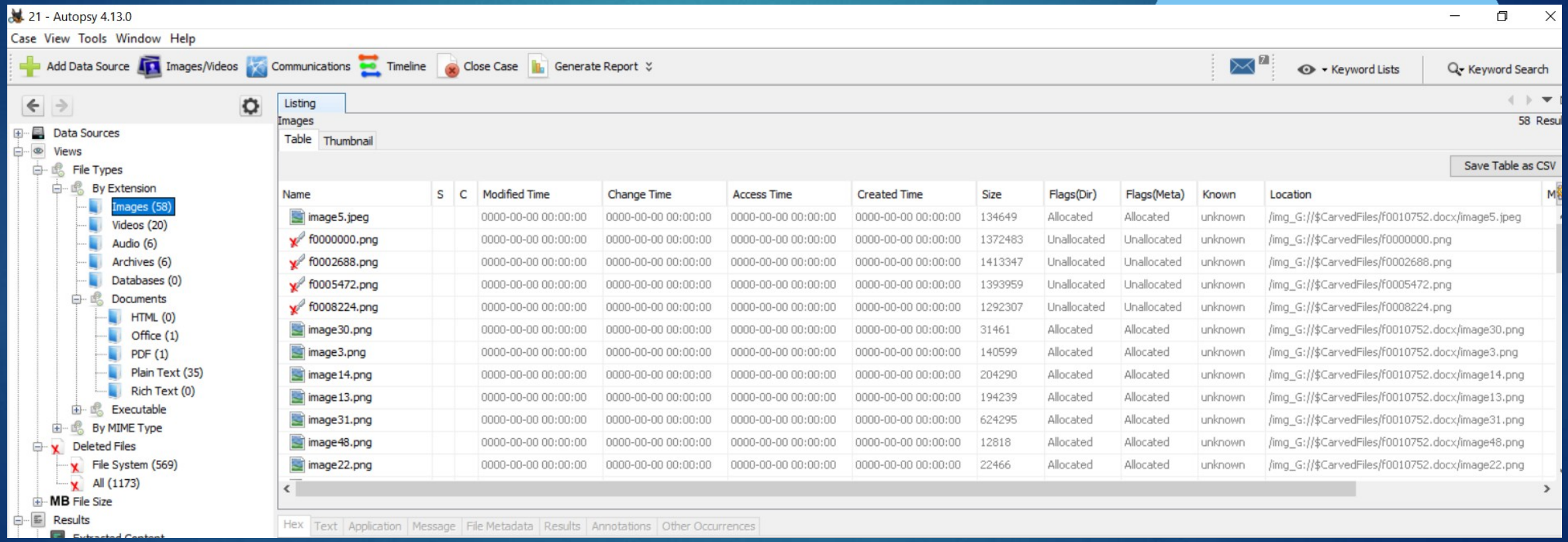
Step 3 Select or Deselect Ingest Modules



Step 4 Final step of Collecting the Evidence from Source

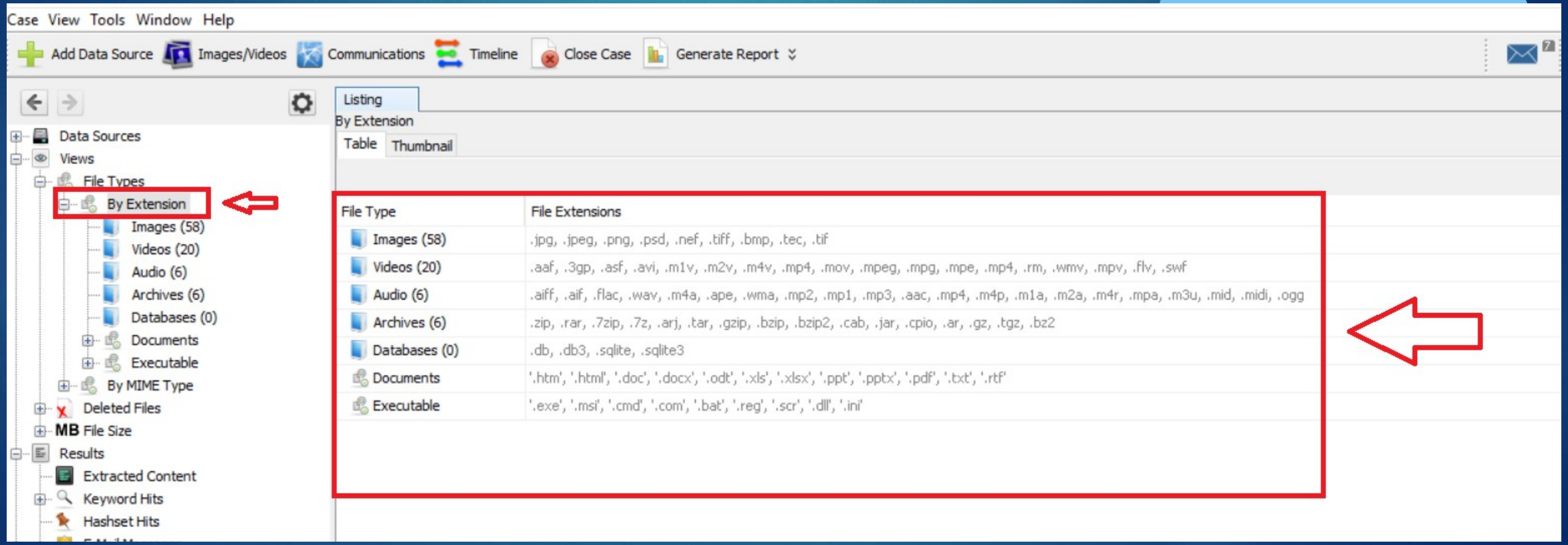


Result: Recovered data from External device

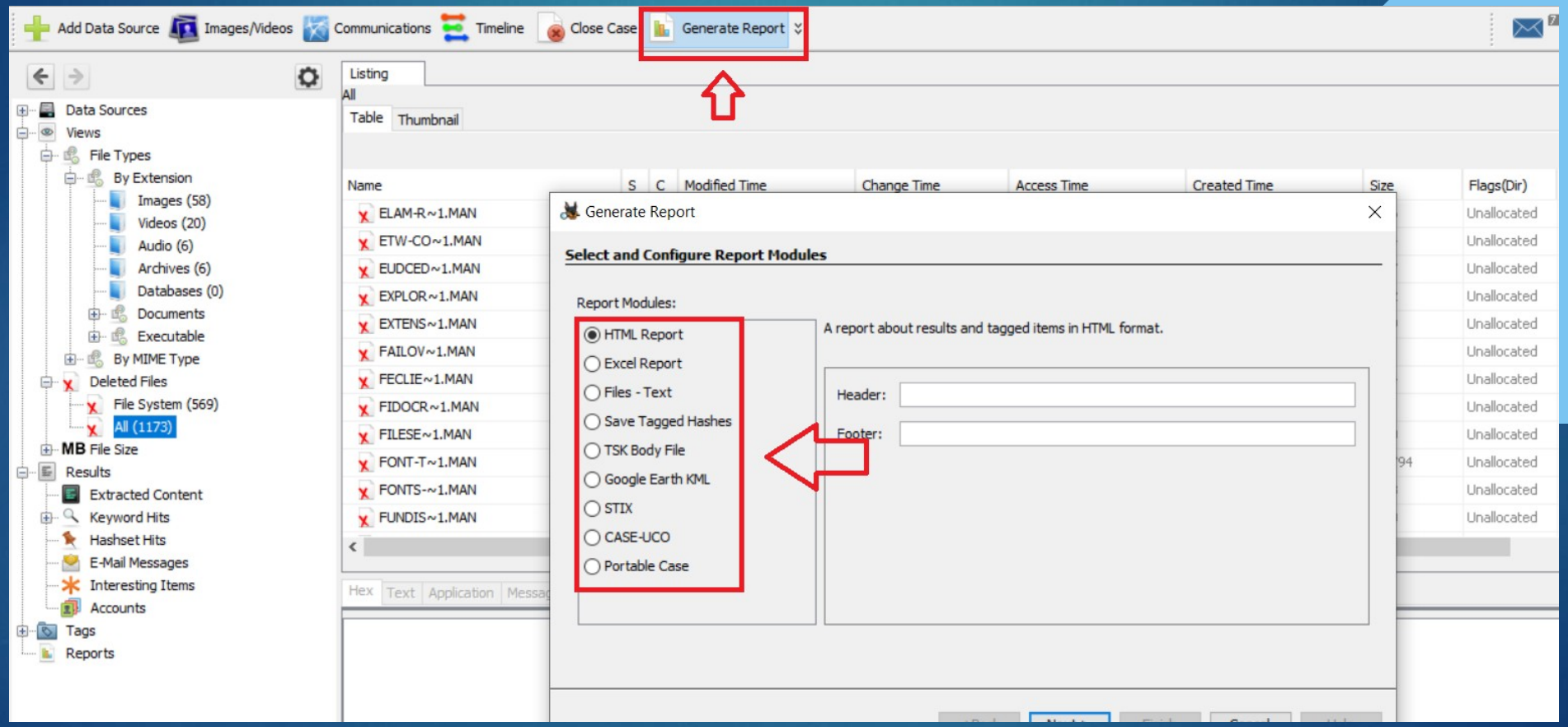


Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
image5.jpeg			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	134649	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image5.jpeg
f0000000.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1372483	Unallocated	Unallocated	unknown	/img_G://$CarvedFiles/f0000000.png
f0002688.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1413347	Unallocated	Unallocated	unknown	/img_G://$CarvedFiles/f0002688.png
f0005472.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1393959	Unallocated	Unallocated	unknown	/img_G://$CarvedFiles/f0005472.png
f0008224.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1292307	Unallocated	Unallocated	unknown	/img_G://$CarvedFiles/f0008224.png
image30.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	31461	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image30.png
image3.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	140599	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image3.png
image14.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	204290	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image14.png
image13.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	194239	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image13.png
image31.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	624295	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image31.png
image48.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12818	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image48.png
image22.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22466	Allocated	Allocated	unknown	/img_G://$CarvedFiles/f0010752.docx/image22.png

User is also able to view the recovered data by Extension



Report Generation of the Case



Thanks ☺