INTERNSHIP REPORT

27th December to 30th June 2022/2023

(CYBER CRIME INVESTIGATOR)

Submitted by

(Priya Sandip Godse)

Student URN NO 2020-B-03102002

Under the Guidance of

(Mr. Nachiket Ajay Dandekar Director and Cyber Crime Investigator At Sana Cyber Forensics)

Ajeenkya D Y Patil University

Charholi Budruk, Lohegaon ,Pune 412105

Academic Year 2020-2023

DECLARATION

I hereby declare that the Internship work entitled “Cyber Crime Investigator” is an authentic record of my own work carried out at Sana Cyber Forensics Investigation & Data Security Services Pvt. Ltd, Pune as the requirement of the semester-long internship for the award of a degree of BCA. under the guidance of Mr. Nachiket Ajay Dandekar Managing Director and Cyber Crime Investigator at Sana Cyber Forensics Investigation & Data Security Services Pvt. Ltd from 27th December to 30th June 2022/2023

Priya Godse

Date: 27th December 2022

Mr. Nachiket Ajay Dandekar

Director and Cyber Crime Investigator

(Industry Mentor)

INDEX PAGE

Sr.No	Content
1	Introduction
2	About Company
3	Cyber Forensics
4	Field Work
5	Methods of Solving cases
6	Tools I learned
7	Types of Cases Encountered
8	Conclusion
9	Summary
10	Contribution
11	Benefits

INTERNSHIP REPORT

INTRODUCTION:

I Priya Sandip Godse BCA-CTIS student at Ajeenkya D Y PAtil University, Pune having URN.No 2020-B-03102002.

I am working as a Cyber Crime Investigator Intern at Sana Cyber Forensics Investigation & Data Security Services, Pvt. Ltd. from 27th December till 6 Months.

Under the guidance of Industry mentor Mr. Nachiket Ajay Dandekar Director and Cyber Crime Investigator at Sana Cyber Forensics Investigation and Data Security Services Pvt. Ltd.

Introduction of the Company:

About:

Sana Cyber Forensics Investigation and Data Security Services Pvt. Ltd is a Certified Cyber Forensics, Information Security Professional & Cyber – Crime Investigator company in India which is located in Pune. Mr.Nachiket Ajay Dandekar is the Founder and Director of Sana Cyber Forensics Investigation and Data Security Services Pvt. Ltd. He has been assisting as a Cyber-Crime investigator for Cybercrime police station, Pune City Police as well as Delhi Police for the past 15 years. He is regularly consulted by Pune City Police, Rural Police, Maharashtra Police, and other law and Enforcement agencies on Cyber Forensics & Cyber Crime Investigation issues. He has a never-ending passion for Cyber Crime Investigations and Information Security and he continues to rise above all.

Services:

- IT AUDITS
- PENETRATION TESTING
- CYBERCRIME INVESTIGATIONS
- MOBILE FORENSICS
- CYBER ADVOCACY LEGAL SERVICES
- VULNERABILITY ASSESSMENT
- IT SECURITY POLICIES
- DIGITAL FORENSICS

- DATA BREACH HANDLING
- TRAINING & AWARENESS PROGRAMS

Organizations:

- Law Enforcement
- DRI (Directorate of Revenue Intelligence)
- DGGI (Directorate General of GST Intelligence)
- GST (Good & Services Tax)
- Income Tax
- Personal Cases

Cyber Forensics:

What is Cyber Forensics?

Cyber forensics is a process of extracting data as proof of a crime that involves electronic devices while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

Types of Cyber Crime:

As mentioned above, crimes typically associated with the physical world, such as committing fraud or stealing intellectual property, have online versions as well. That transition is enabled by computers and digital tools and technologies. Below are examples of different types of cybercrime:

- **Computer Hacking**

The term “computer hacking” is often used as a catchall phrase to describe it. By definition, computer hacking means the modification of computer software and hardware to gain access to data such as passwords or introduce malware to computer systems and networks.
Ransomware, a type of cyber extortion, is a type of computer hack. So is phishing. In a phishing attempt, an email looks like it comes from a person or organization the user knows, but it’s an “e-scam.” The email message may look genuine and tricks the user into clicking on a link or downloading an attachment that compromises the computer with malware, such as a virus.

- **Copyright Infringement**

Copyright infringement is a type of cybercrime that involves the theft of intellectual property, which can range from technology, movies, and music to inventions, ideas, and creative expressions such as art. The proliferation of digital technologies that facilitate file sharing through internet networks has made this type o cybercrime a growing threat to individuals and businesses. The consequences of copyright infringement are typically monetary.
For example, a startup technology company can lose its advantage if a competitor steals its code. In conducting cybercrime investigations in this area, the FBI collaborates with copyright and trademark owners, as well as online marketplaces and payment service providers that may inadvertently facilitate this type of cybercrime

- **Cyber Stalking**

With the rise of social media, people can easily share life experiences, interests, restaurants they’ve visited, and even vacation pictures. However, this sharing may gain the attention of cyberstalkers. NordVPN reports that more than 40% of adults have experienced some type of cyberstalking with women being the most targeted.
It is important to distinguish cyberstalking from researching a person’s background on the internet. For example, an employer may want to learn a little more about a newly hired employee, so they may take a glance at the individual’s Instagram account. This is not cyberstalking, as it is not intended to result in a nefarious act. On the other hand, cyber stalkers surveil their victims to harass, embarrass, or threaten them.

- **DDoS Attacks**

Picture for a moment thousands of vehicles headed on the same highway in one direction — a traffic jam seemingly going nowhere. That’s how a DDoS (distributed denial-of-service) attack works, except that instead of cars and trucks, data is

bottlenecked. Another difference is that a DDoS attack is a malicious attempt to disrupt normal data traffic in the digital world.

A DDoS attack works by implementing malware that allows a hacker to target a network server and overwhelm it with an overflow of internet traffic. It affects the surrounding infrastructure of a server as well, causing systems and machines to crash. In a cybercrime investigation, a sudden surge of data patterns or suspicious amounts of traffic coming from a single IP address — a unique numerical identifier for a device on a computer network — can help point to the origin of a DDoS attack.

- **Extortion**

Extortion comes in various forms. One way a cyber criminal extorts online is through ransomware. Another form of extortion that has made the headlines is "cryptojacking." Organizations and individuals who fall victim to a successful cryptojack attack are placed in an unfavorable position and then forced to pay a hacker large sums of money using cryptocurrency such as bitcoins. Cryptojackers take advantage of the decentralized nature of cryptocurrency to operate anonymously and in the shadows. However, in the recent hack of the Colonial Pipeline in the U.S., the U.S. Justice Department was able to recover $2.3 million paid in bitcoins to hackers.

- **Fraud**

Fraud is described as a deceptive practice to gain an unfair advantage or for personal enrichment. For example, a company may include fictitious payments, invoices, or revenues to present a false picture of its financial state to acquire investment or tax advantages. In the digital world, credit and debit card fraud is a growing problem.

Fraud can take place in the physical world and be extended into the digital realm. For example, a fraudster can use a skimming device to steal information from individuals who are using their credit or debit card at a credit card processing device or ATM. A hacker can also use malware to acquire customer credit card information from card processing software. The information obtained about a consumer can then be sold online or used to make purchases.

- **Identity Theft**

Identity theft is an invasive online crime that can have long-term damaging effects on a person's finances, reputation, and more. For example, using your personal information, an identity thief can open new credit card accounts in your name without your knowledge. According to the Federal Trade Commission, signs of having been the victim of identity theft include inexplicable checking account withdrawals, getting refused by merchants, receiving debt collection calls for debts that are not yours, and seeing charges on your credit report that you never authorized.

- **Online Predators**

Online predators find targets, typically young children and adolescents, on popular social media sites. They often pretend to be the same or similar age as their target and, using fake profiles, earn the trust of the most vulnerable. Through this act of grooming, they may pressure a child to send explicit images of themselves or share information about themselves, which can lead to dnkidnappingviolent attacks and sexual exploitation.

The FBI reports that every year there are thousands of cases involving crimes against children, and this includes online predators. According to the National Center for Missing and Exploited Children, its tip line received over 21.7 million reports regarding exploited children in 2020.

- **Personal Data Breach**

A personal data breach describes when a hacker breaks into a computer system to steal records and data about individuals, such as user passwords, credit card information, and even health records. This type of cybercrime is most common in the business world. The biggest data breaches in history have affected the accounts of millions, and even billions, of users. An example includes the attack on Yahoo over three years which resulted in 3 billion accounts being breached. According to Norton, a data breach can occur in four ways: through system vulnerabilities, such as out-of-date software; weak passwords; drive-by downloads, which occur when a user visits a compromised website; and targeted malware attacks.

- **Prohibited/Illegal Content**

This type of cybercrime often coincides with online predator activity, which may involve individuals preying on children online to try to obtain sexually explicit images. But prohibited/illegal content on the internet also includes footage of criminal activity and real or simulated violence. Content that promotes illegal activity, such as making weapons or bombs and extreme political or hateful views that can radicalize vulnerable people to perform criminal acts, is also considered illegal content. In business, prohibited content can include content on streaming services that was accessed without authorization and IP addresses that were acquired to commit fraudulent activities.

Why is Cyber Forensics Important?

In today’s technology-driven generation, the importance of cyber forensics is immense. Technology combined with forensic forensics paves the way for quicker

investigations and accurate results. Below are the points depicting the importance of cyber forensics:

- Cyber forensics helps in collecting important digital evidence to trace the criminal.
- Electronic equipment stores massive amounts of data that a normal person fails to see. For example: in a smart house, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

Process Involved in Cyber Forensics.

1. Obtaining a digital copy of the system that is being or is required to be inspected.
2. Authenticating and verifying the reproduction.
3. Recovering deleted files (using Autopsy Tool).
4. Using keywords to find the information you need.
5. Establishing a technical report.

Working as Cyber Forensics Expert.

Cyber forensics is a field that follows certain procedures to find evidence to reach conclusions after a proper investigation of matters. The procedures that cyber forensic experts follow are:

- **Identification:** The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.
- **Preservation:** After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper with data.
- **Analysis:** After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to conclude.

- **Documentation:** Now after analyzing data a record is created. This record contains all the recovered and available (not deleted) data which helps in recreating the crime scene and reviewing it.
- **Presentation:** This is the final step in which the analyzed data is presented in front of the court to solve cases.

Types of Computer Forensics.

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract crucial information related to the case.

Tools Used:

Thunderbird, Outlook.

- **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyze data from mobile phones.

  Tools Used:

  UFED, MOBIL edit, Autopsy, Magnet, iTunes, Imazing, Imyphone(chat back).

- **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Tools Used:

FTK, UFED, MOBIL edit, Autopsy, Magnet, iTunes, Imazing, Imyphone(chat back).

Techniques Cyber Crime Investigators use.

Cyber forensic investigators use various techniques and tools to examine the data and some of the commonly used techniques are:

- **Live analysis:** In this technique, the computer of criminals is analyzed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.

- **Deleted file recovery:** This includes searching for memory to find fragments of a partially deleted file to recover it for evidence purposes.

- **Certifications of Evidence:** This includes certifications that conditions, as laid down in section 65B(2)(a), 65B(2)(b), 65B(2)(c),65B(2)(d) of the Indian Evidence Act, 1872 regarding the admissibility of computer outputs, have been compiled with in all aspects.

- **Investigation of Evidence:** This includes searching pieces of Digital evidence from various types of Devices. Such as Mobile Phones, Laptops, (HDD)Hard disks, (SSD)Solid State drives, IoT Devices various web applications, DVR & NVR.

- **Social Media Analysis:** In this technique, we analyze different social networking sites such as Facebook, Instagram, Snapchat, Twitter, WhatsApp, LinkedIn, etc.

Advantages of Cyber Forensics.

- Cyber forensics ensures the integrity of the computer.
- Through cyber forensics, many people, companies, etc get to know about such crimes, thus taking proper measures to avoid them.
- Cyber forensics finds evidence from digital devices and then presents them in court, which can lead to the punishment of the culprit.
- They efficiently track down the culprit anywhere in the world.
- They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.

Required set of Skills needed to be a cyber forensic expert.

- As we know, cyber forensics is based on technology. So, knowledge of various technologies, computers, mobile phones, network hacks, security breaches, etc. is required.
- The expert should be very attentive while examining a large amount of data to identify proof/evidence.
- The expert must be aware of criminal laws, criminal investigations, etc.
- As we know, over time technology always changes, so the experts must be updated with the latest technology.
- Cyber forensic experts must be able to analyze the data, derive conclusions from it and make proper interpretations.
- The communication skill of the expert must be good so that while presenting evidence in front of the court, everyone understands each detail with clarity.
- The expert must have strong knowledge of basic cyber security.

Limitations.

- Some facilities which are there within the browsers to save the WWW pages to disk are not perfect because they may save the texts but not the related images.
- There might be a difference between what is there on the screen which can be seen and what is saved on the disk.
- The method which has been used to save a particular file might not carry individual labeling regarding when and where it was obtained. Such files can be easily forged or modified.
- times it becomes difficult for the system to locate the page which was acquired at last. If the entire series is examined it becomes even more difficult to point out which one was later and which was earlier. Many ISPs use proxy servers to speed up their de- livery of pages that are popular on the web. Hence, the user might not be sure of what he has received from that particular website by his ISP.
- Common mistakes like altering the date and time stamps, killing rouge processes, patching the system before investigation, etc lead to loose of data from the disk resulting in the crashing of the e- files and evidence stored on the computer.

New technologies are helping engineers to develop and create more robust hardware and software to investigate computer-related crime. The advancement of encryption is one Discussing Foreign Cyber Forensics System With Their Indian Counterpart

India has tried to address the challenges that its security agencies are faced with in the areas of law and order and terrorism in a variety of ways. In 2011, a petition was filed by Yahoo! India Pvt Ltd. against the Union of India in the Delhi High Court.93

The petition records the government's repeated demands for access to IP addresses and email content, citing demands from the Intelligence Bureau (IB),94 India's premier internal intelligence organization. The petition records how the IB sought this data under section 28 of the Information Technology Act 2000, through the o Controller of Certifying Authority (CCA) offices under the Department of Information Technology, Government of India. Instances such as those detailed above have also sharpened India's approach favoring a multilateral approach to cybersecurity at the global level.

Efficiency Of Cyber Forensic Tools For Examining Evidence In India:

The tools of cyber forensic investigation are X- Ways WinHex, First on Scene, Rifiuti, Pasco, Galleta/Cookie, Forensic Acquisition Utilities, NMap, Ethereal, BinText, Encrypted disk detector, and MemGator. Rifiuti is a tool that helps in finding the last details of a system's recycle bin. It helps in collecting all the deleted and undeleted files. Pasco is a Latin word meaning browse.

Pasco helps in the analysis of the contents of all browsing that has been done from one’s computer. In short, it is particularly useful in gathering records of internet activities carried out from a targeted computer. There is one another technique used for cyber forensics not particularly falling under the ambit of the tools used is, Miscellaneous Steganography Tools. It is a technique where data or a text file is converted and then embedded into an im- age file to deceive others. There are some tools how- ever that help in detecting such injections.

Hackers and malicious users are coming up with such ideas to inject data files into not just image files but also music and video files. At times individuals try to hide their incriminating information by renaming a file of a particular type to another type by changing its extension. By doing so, it makes it difficult for one to determine the correct type of file. To flag such suspicious files Encase is used; running hash (#) functioning on the hard drive will interpret file headers and mark them as containing incorrect header information.

To make this information/evidence admissible in a court of law, it is very essential to create an exact image of the information. And for this, the specialists work very hard, with all patients and accuracy, with all confidentiality so that no one should know what they are working on, and with all dedication to collect vital information which can be produced ad as concrete evidence before the court.

Once the information and all evidence are gathered, a compiled report is made by the specialists that can be produced before the courts. As these people are experts and have

special training re- regarding the use of such complex tools and techniques they can also testify before the court regarding the matter they are working on.

Nowadays, angry employees with malicious intentions have assaulted many e-commerce websites, such as viruses, wiretapping, and financial frauds in various governments of independent firms and companies. This e-commerce attachment causes various financial hardships to the companies. This has been observed as a common trait among the individuals who have been fired or have been insulted by the head departments, independent of hackers and such cyber criminals.

No matter how effective any technology or system may be. There always has been a drawback to the same. Similarly, preserving data or information to serve as evidence is beneficial to the court but on the other hand, there may be certain technical and human barriers to such gathering of information.

Field Work:

Step 1: Firstly we visit the police station thereafter we visit the crime spot and do some legal documentation.

- Such as crime registered number, investigating officer, crime location, time & date of the crime, IPC Sections, and device information.

Step 2: We collect pieces of evidence without tampering with the shreds of evidence.

Step 3: Thereafter we do preserve pieces of evidence.

Step 4: After that, all the other processes are done at the backend such as Certificates, Technical Reports, logs & evidence printouts (if any).

Methods of Solving Cases:

1) **Identification**
   The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.

2) **Preservation**
   After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper with data.

3) **Analysis**
   After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the

evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to conclude.

4) **Documentation**
   Now after analyzing data a record is created. This record contains all the recovered and available (not deleted) data which helps in recreating the crime scene and reviewing it.

5) **Presentation**
   This is the final step in which the analyzed data is presented in front of the court to solve cases.

What did I learn?

Firstly I learned about the basics of Cyber Forensics, and the different methodologies needed for solving different types of cases that required Forensics Investigation.

- Different Imaging Techniques
- Different types of use cases concerning Forensics
- Investigation of cases with Government authorities.
- Investigation of CCTV Extraction

TOOLS I LEARNED:

1. ACCESS DATA FTK IMAGER (Image Creation)

Access Data FTK Imager is a widely used tool in forensic investigation. In this course, AccessData Forensic Toolkit (FTK) Imager, you'll learn how to quickly and accurately acquire and examine evidence as part of a computer-related investigation. First, you'll explore how to install and configure FTK Imager. Next, you'll discover how to acquire a variety of image types and maintain the integrity of the original data. Finally, you'll learn how to safely mount and examine the collected data and analyze captured evidence. When you're finished with this course, you'll have the skills and knowledge of using the FTK Imager needed to be confident in the process of forensically imaging and analyzing collected data as part of an investigation.

FTK Imager is a tool for creating disk images and is free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

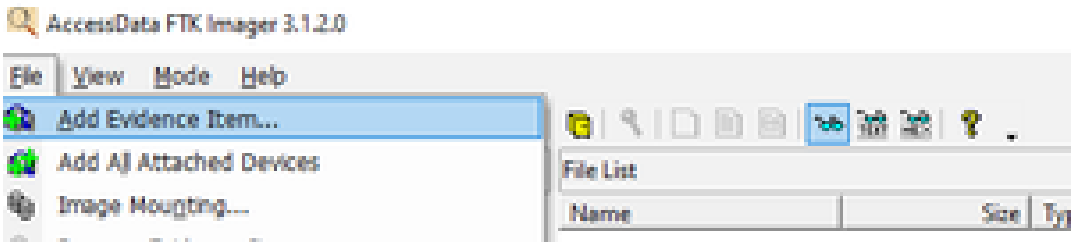
What can we do using FTK Imager:

- Create forensic images or perfect copies of local hard drives, floppy and Zip disks, DVDs, folders, individual files, etc. without making changes to the original evidence.

- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs.
- You can also preview the contents of the forensic images that might be stored on a local machine or drive.
- You can also mount an image for a read-only view that will also allow you to view the contents of the forensic image exactly as the user saw it on the original drive.
- Export files and folders from forensic images.
- View and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.

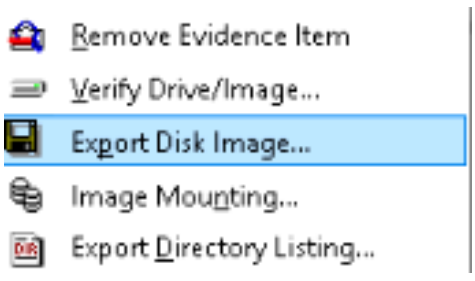
Steps for Creating Image:

- **Step 1:** Download and install the FTK imager on your machine.
- **Step 2:** Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.
- **Step 3:** In the menu navigation bar, you need to click on the File tab which will give you a drop-down, like given in the image below, just click on the first one that says, Add Evidence Item.



- **Step 4:** After that, there will be a pop-up window that will ask you to select the source of evidence. If you have connected a physical hard drive to the laptop/computer you are using to make the forensic image, then you will select the Physical Drive here. Click on Next. Now, Select the Physical Drive that you would like to use. Please make sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your OS drive.

- **Step 5:** Now, we will export the forensic images.
    1) Right-click on the Physical Drive that you would like to export in the FTK Imager window. Select Export Disk Image here.



2) Click the Add button for the Image Destination.
3) Select the Type of Forensic Image you would like to export. Select .E01 and Click Next.
4) After that, you will have to enter information regarding the case now. You can either leave them blank or keep them general, this part is totally upon you.
5) Next, you will need to Choose the Destination that you would like to export the forensic image and Name the Image.

Lastly, we will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has not been tampered with. Forensic Imaging is defined as the processes and tools used in copying electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, sector, partition, files, folder, master boot records, deleted files, and unallocated spaces. The image is an identical copy of all the drive structures and contents.

Pros Of FTK Imager:

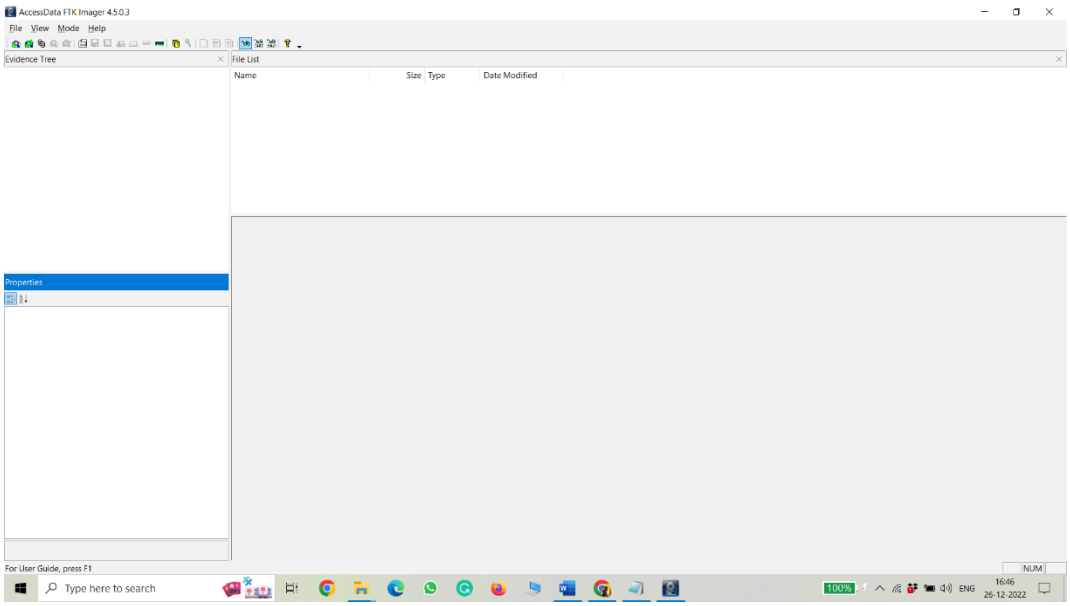
- It has a simple user interface and advanced searching capabilities.
- FTK supports EFS decryption.
- It produces a case log file.
- It has significant bookmarking and salient reporting features.
- FTK Imager is free.

Cons of FTK Imager:

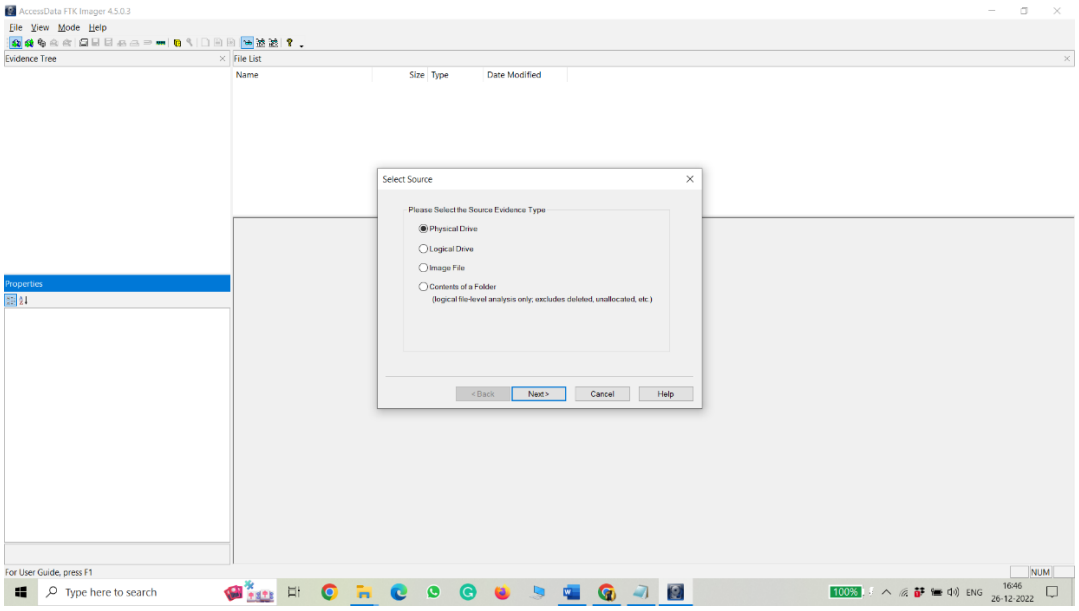
1. FTK does not support scripting features.
2. It does not have multitasking capabilities.
3. There is no progress bar to estimate the time remaining.
4. FTK does not have a timeline view.

Process of Verifying Disk Image:

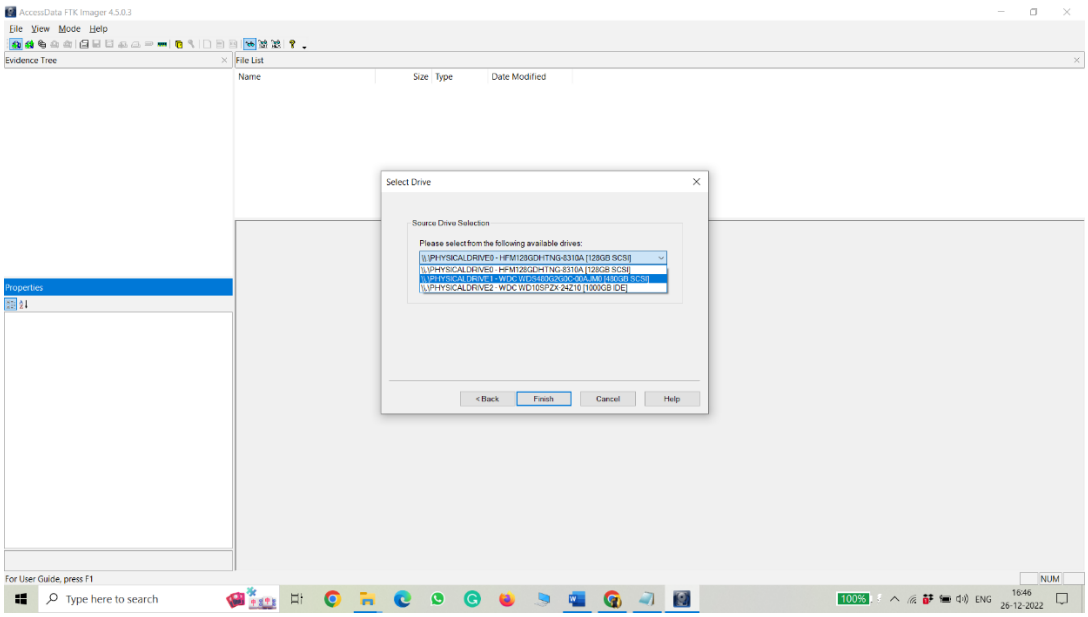
1) Step 1:



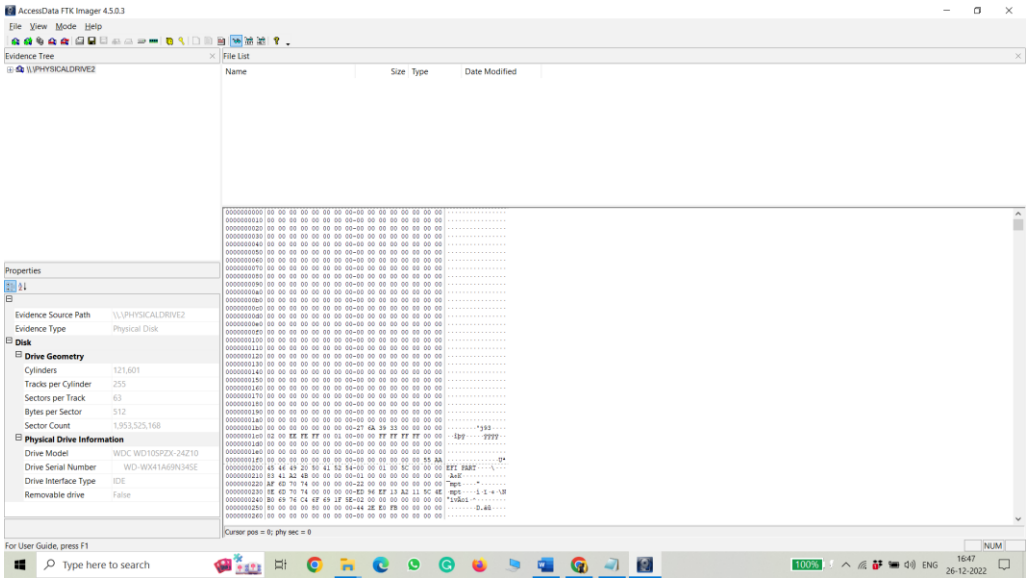
2) Step 2:



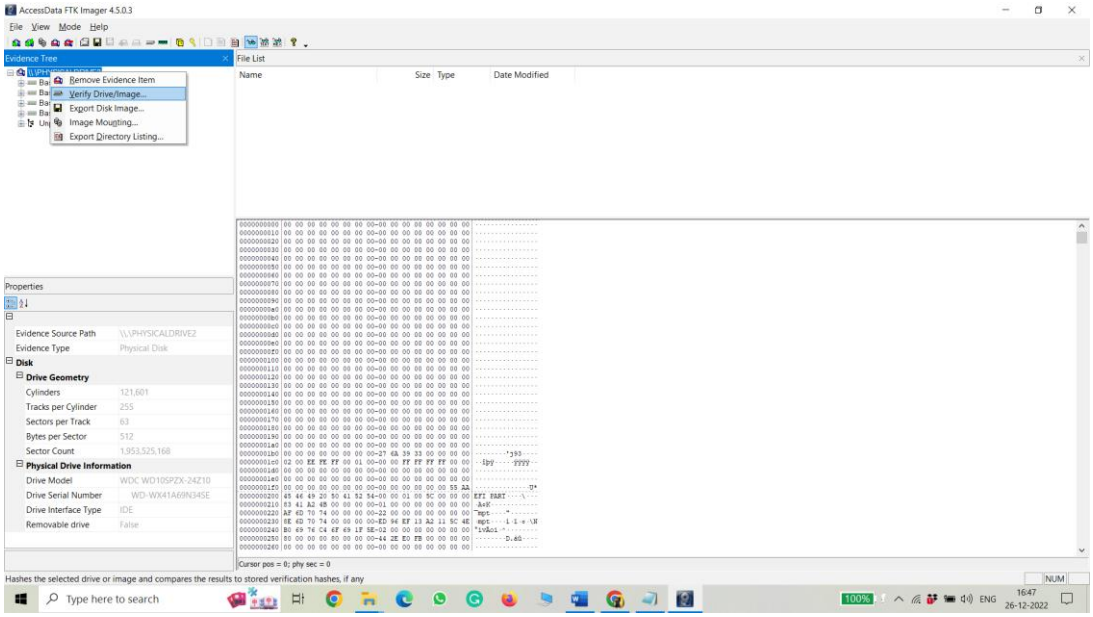
3) Step 3:



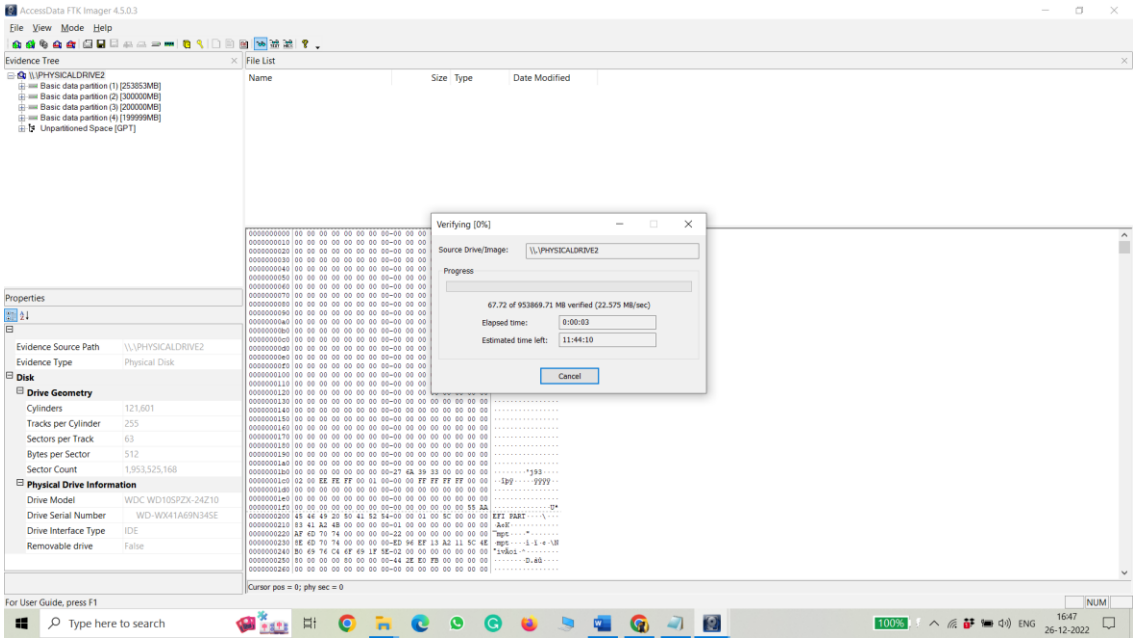
4) Step 4:



5) Step 5:



6) Step 6:



2. LOGICUBE TALON ULTIMATE (Hashing, Cloning, Wiping)

Designed for field or forensic lab use, the Talon® Ultimate delivers advanced, high-performance forensic imaging at a budget-friendly price. Featuring a compact footprint, user-friendly navigation, and unbeatable imaging speed it has been engineered specifically for digital forensic investigators, the Talon Ultimate meets all your forensic imaging, hashing, and wiping requirements.

- The Talon® Ultimate is an extremely fast forensic imaging solution, achieving speeds of over 40GB/min.
- Image and verify to multiple image formats; native copy, .dd image, .dmg image, e01, and ex01. The Talon Ultimate provides SHA1, SHA256, and dual hash (MD5+SHA1) authentication at extremely fast speeds.
- Talon Ultimate formats destination drives to NTFS, EXT4, FAT 32 or exFAT file systems. The unit supports imaging from source drives formatted to any major file system.
- Write-blocked source ports include 1 SATA (SAS optional), 1 USB 3.0, 1 FireWire, and 1 PCIe. SAS support is enabled via a software option, no additional

modules are required. 1 additional SATA (SAS optional) source port can be activated with the purchase of the MultiTask option.

- Destination ports include 2 SATA (SAS optional), 1 USB 3.0, and 1 FireWire. SAS support is enabled via a software option, no additional modules are required.
- PCIe Support. Support for imaging from M.2 PCIe (SATA, AHCI, and NVME types), PCIe, and mini-PCIe express cards, is available using the Talon Ultimate's PCIe source port and optional adapters.
- Networking Feature. Use the Talon Ultimate to image to a network location using CIFS protocol and/or image from a network location using iSCSI. Users can use iSCSI as a source or destination drive.
- Multi-Task option. This option adds 1 additional SATA source port (SAS optional) and allows you to image simultaneously from multiple sources to multiple destinations including a network repository. This option also provides support to image one drive while hashing and/or wiping a second drive simultaneously. Users can perform up to 5 tasks concurrently.
- Concurrent Image+Verify. Imaging and verifying concurrently take advantage of destination hard drives that may be faster than the source hard drive. The duration of the total image process time may be reduced by up to half.
- Parallel Imaging. Perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Clone to a network location or a destination drive using mirror copy mode while simultaneously imaging in e01 or .dd format to a different destination drive. Requires purchase of Multi-task option.
- Targeted Imaging/Logical Imaging feature allows you to create a logical image using pre-set, custom filters, file signature filters, and/or keyword search to capture only specific files needed. An MFT report can be generated that contains a potentially deleted file list. Format output to L01, LX01, ZIP, or directory tree. Users can browse and view directly on the Talon Ultimate display or manage and view on a networked Talon Ultimate from their laptop/desktop using a web browser. Requires the purchase of the Targeted Imaging option.
- Write-Blocked Drive Preview. Preview drive content directly on the Talon Ultimate. The file browser feature provides logical access to source or destination drives connected to Talon Ultimate. Users can view the drive's partitions and contents, and view text files, jpeg, PDF, XML, and HTML files.
- The Talon Ultimate provides built-in support for SATA/USB3/FireWire storage devices including solid-state drives. SAS devices are supported with the purchase of a software option. 2.5"/3.5" IDE drives are supported with an adapter included with Talon Ultimate. PCIe, 1.8" IDE, 1.8" ZIF, mSATA, Micro SATA, SATA, and flash drives are supported with optional adapters.
- Secure sensitive evidence data with whole drive AES 256-bit Encryption. Decryption can be performed using the Talon Ultimate or by using open-source software programs such as VeraCrypt, TrueCrypt, or FreeOTFE.

- Network Push Feature. Push evidence files from destination drives connected to the Talon Ultimate or from a Talon Ultimate repository to a network location. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by performing an MD5 or SHA hash during the push process.
- Users can capture from a MAC system booted in target disk mode using the FireWire port. An off-the-shelf Thunderbolt to FW cable is required for MACs with a Thunderbolt port. Supports MacBook Pro, and supports the capability to image from MACs with USB-C ports.
- Image from a PC/laptop without removing hard drives. Create a forensic bootable USB flash drive to image a source drive from a computer on the same network without booting the computer's native O/S. Supports Surface Pro 4 and above tablets.
- Use the USB 3.0 device port to provide write-blocked preview/triage of suspect drives connected to Talon Ultimate. Users can also copy files from drives to their PC with this feature. The Talon Ultimate can be used as a write-blocker.
- Administrative feature allows users to save configuration settings and set password-protected user profiles.
- A web-based user interface allows users to connect to the device from a web browser and manage all operations remotely. The browser features automatic page scaling for iPad-type devices and authentication.
- Features an internal, removable storage drive that stores O/S and audit trail/logs. The drive is easily removed for secure/classified locations.
- Image from a CD/DVD Blu-Ray. The Talon Ultimate can image CD/DVD/Blu-ray media by using a USB optical drive connected to the USB port on the Talon Ultimate. Supports multi-session CDs
- Additional features include HPA/DCO capture, drive spanning, color touchscreen display, on-screen keyboard, HDMI port, two USB 2.0 host ports for keyboard, mouse or printer connectivity, blank disk check feature, drive trim feature, and detailed information, including S.M.A.R.T. data, on drives connected to Talon Ultimate./DVDs.
- Wipe drives to DoD specifications or use secure erase to wipe drives.
- Audit Trail/Log files provide detailed information on each operation. Log files can be viewed on Talon Ultimate or via a web browser, exported to XML, HTML, or PDF format to a USB enclosure. Users can print the log files directly from their PC when connected to Talon Ultimate via a web browser.

3. MOBIL edit (Mobile Phone Extraction)

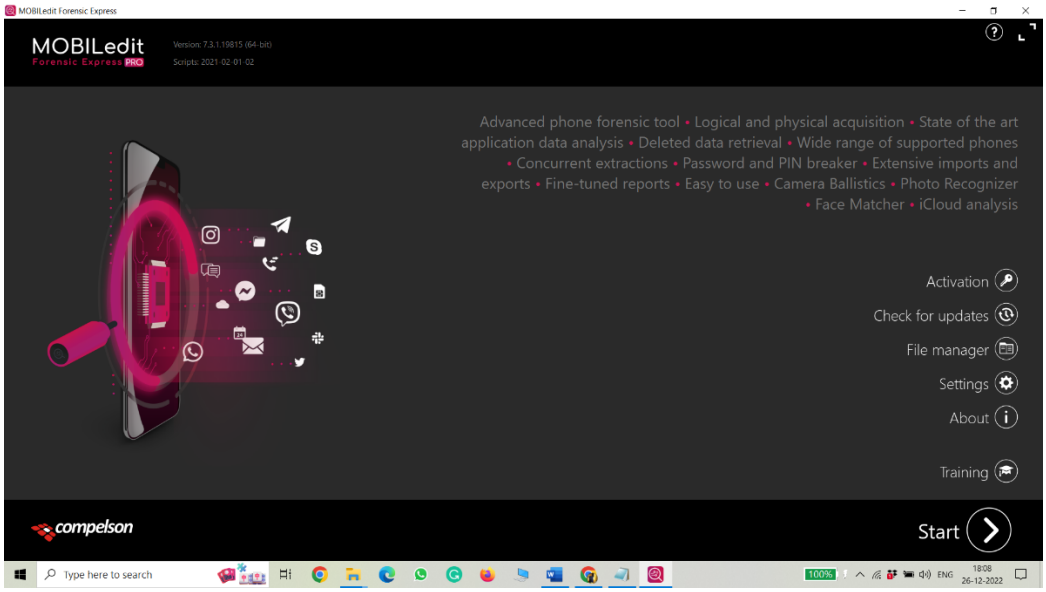
MOBILedit Forensic is a digital forensics product by Compelson Labs that searches, examines, and reports on data from GSM/CDMA/PCS cell phone devices. MOBILedit connects to cell phone devices via an Infrared (IR) port, a Bluetooth link, WiFi, or a cable interface. After connectivity has been established, the phone model is identified

by its manufacturer, model number, and serial number (IMEI) and with a corresponding picture of the phone.

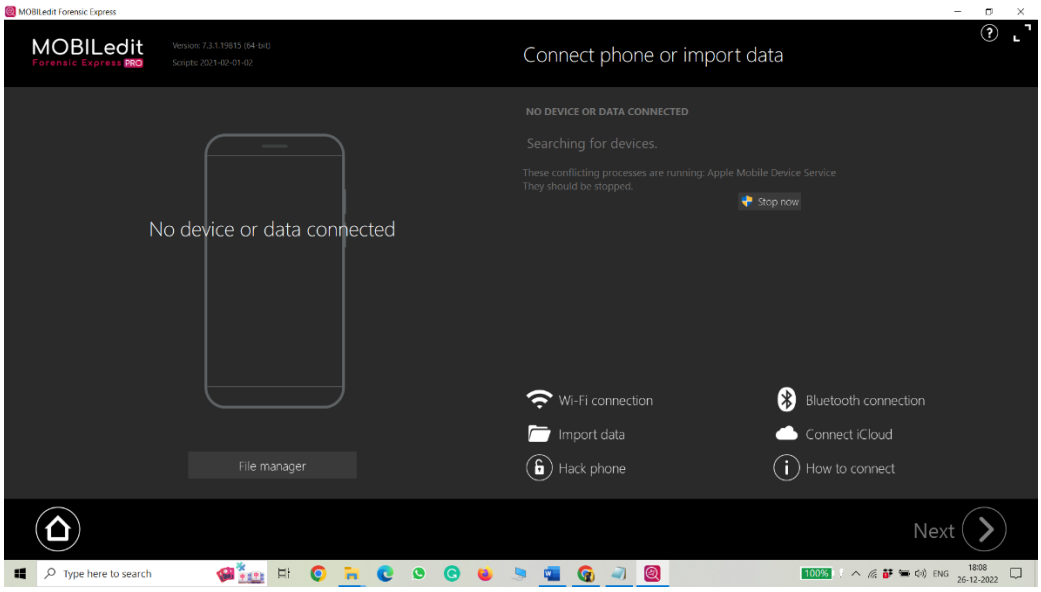
Data acquired from cell phone devices are stored in the .med file format. After a successful logical acquisition, the following fields are populated with data: subscriber information, device specifics, Phonebook, SIM Phonebook, Missed Calls, Last Numbers Dialed, Received Calls, Inbox, Sent Items, Drafts, and Files folder. Items present in the Files folder, ranging from Graphics files to Camera Photos and Tones, depend on the phone's capabilities. Additional features include the myPhoneSafe.com service, which provides access to the IMEI database to register and check for stolen phones.

MOBILedit is a platform that works with a variety of phones and smartphones (a complete list of supported handsets is available on the manufacturer's website) and explores the contents of the phone through an MS Outlook-like folder structure. This allows backup of the information stored on the phone, storing it on a PC or copying data to another phone via the Phone Copier feature.

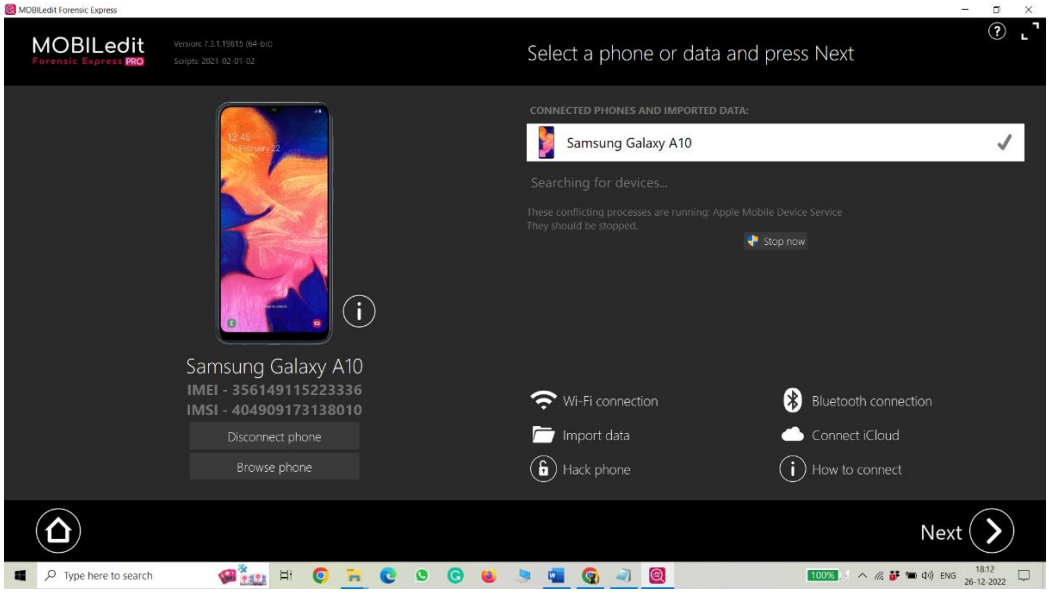
Step 1: Home page of MOBILedit application. Click on the start button.



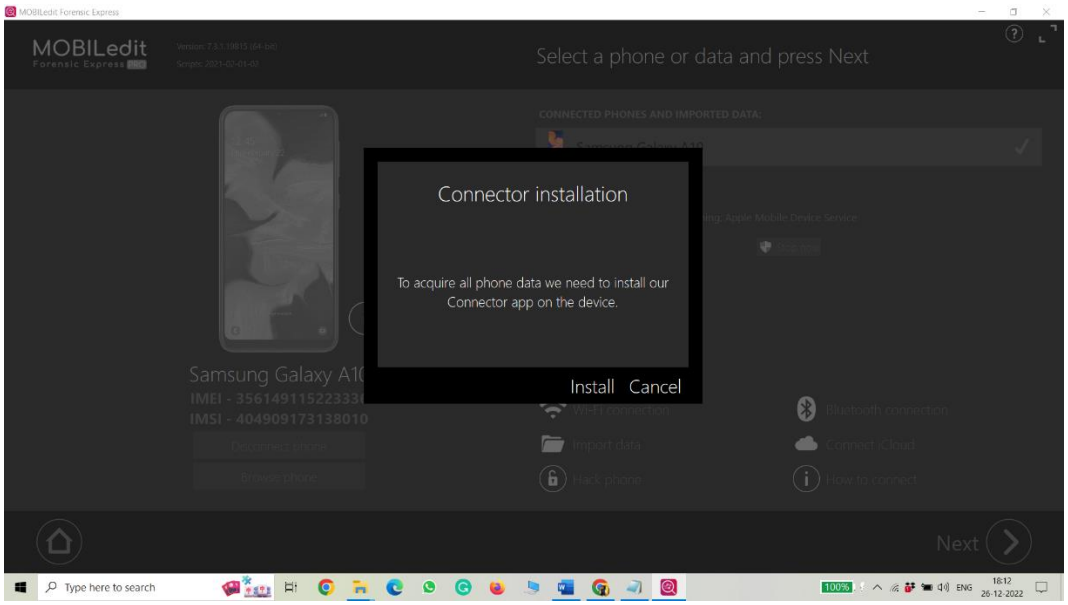
Step 2: Connect the Phone, note(switch on the developer mode and USB debugging)



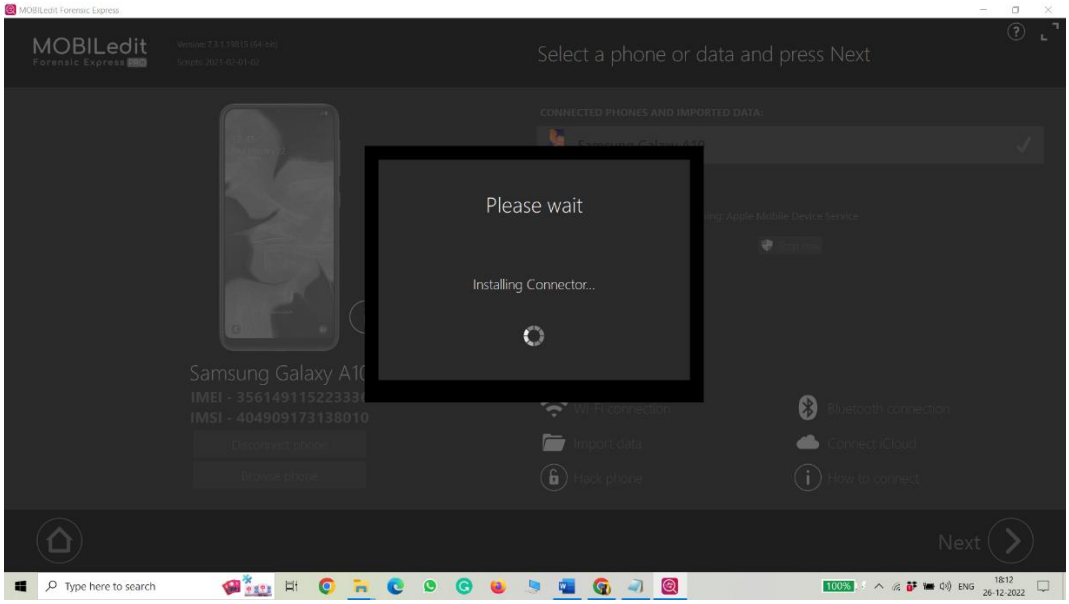
Step 3: The phone will be detected and details of the phone will be displayed.



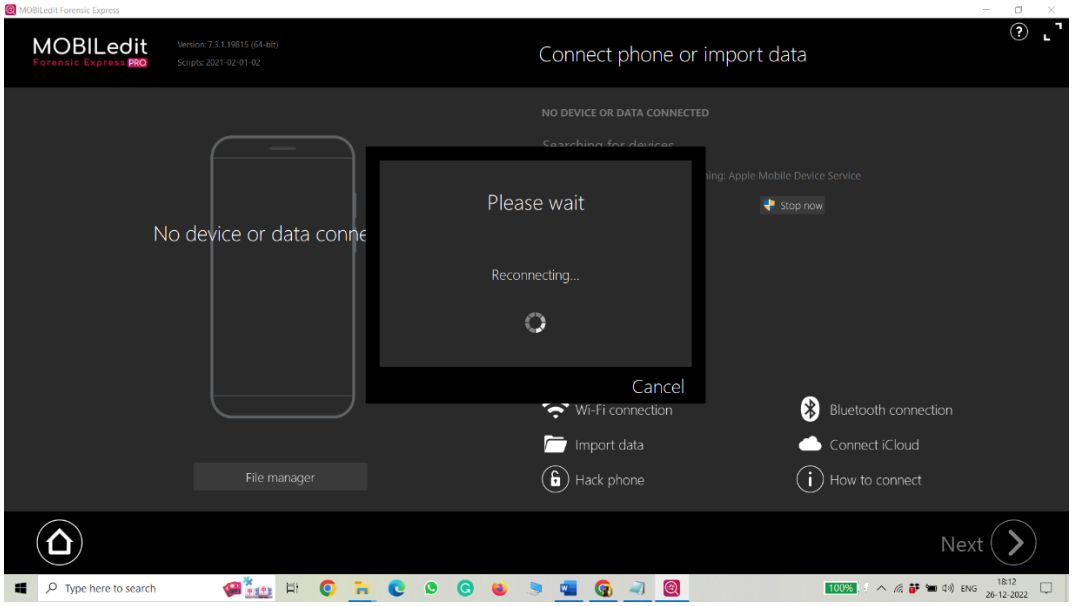
Step 4: Now it will show a popup for installing a forensic connector on the phone click on install.



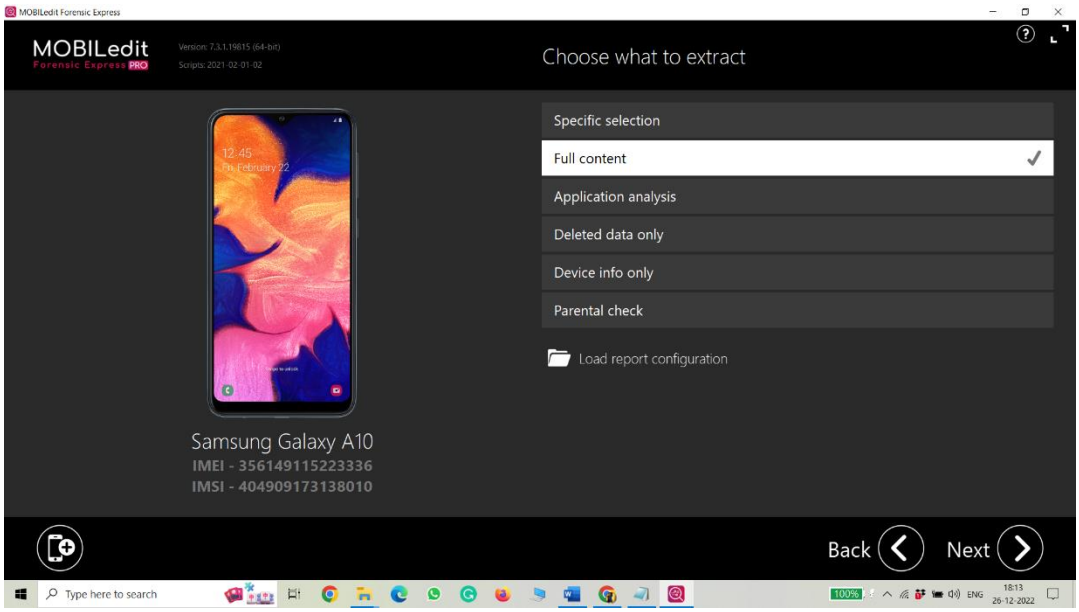
Step 5: Now the forensic connector will be installed wait till the connector is installed.



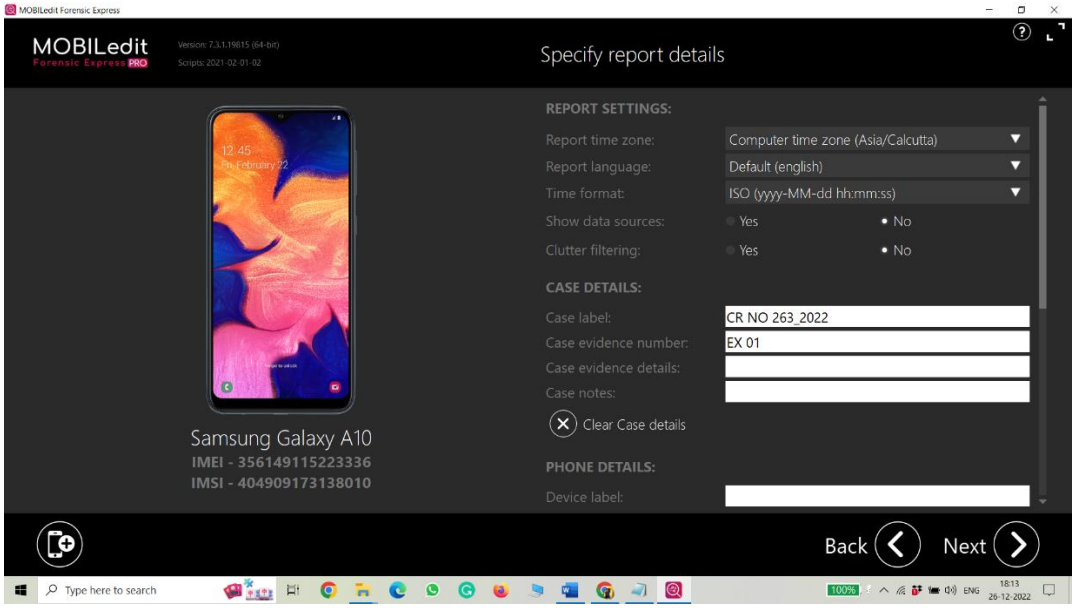
Step 6: Now it will be reconnected after giving access to all on phone for forensic connector



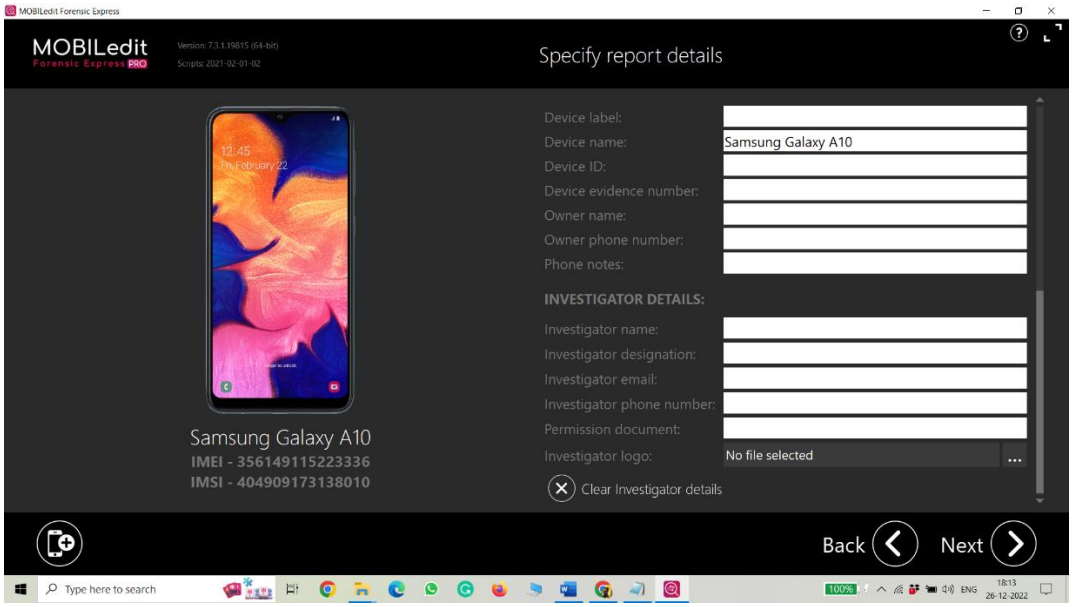
Step 7: Now we have to choose what we exactly want to extract.



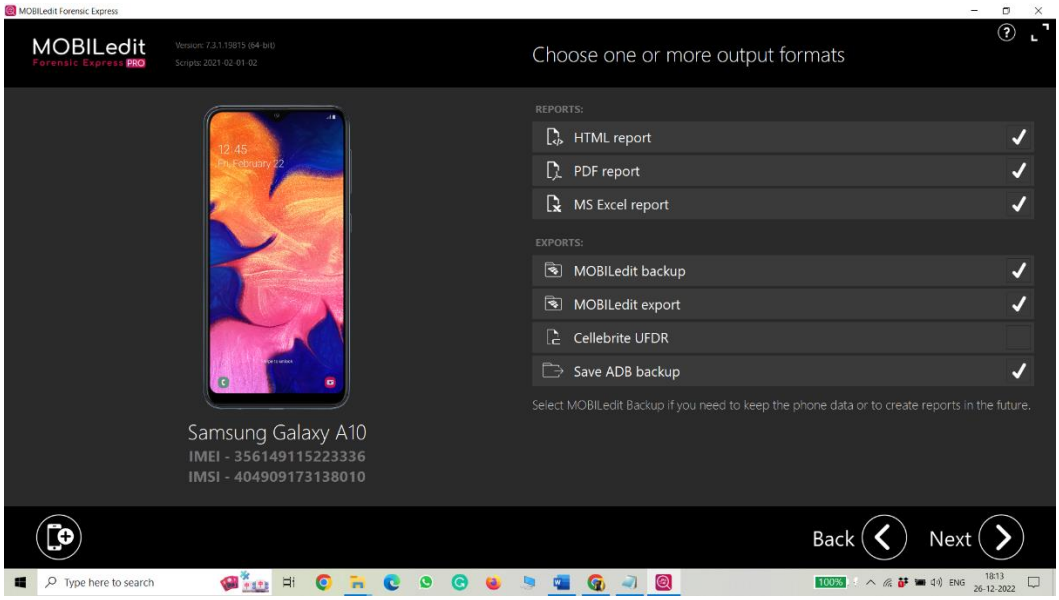
Step 8: Now enter the details as asked below.



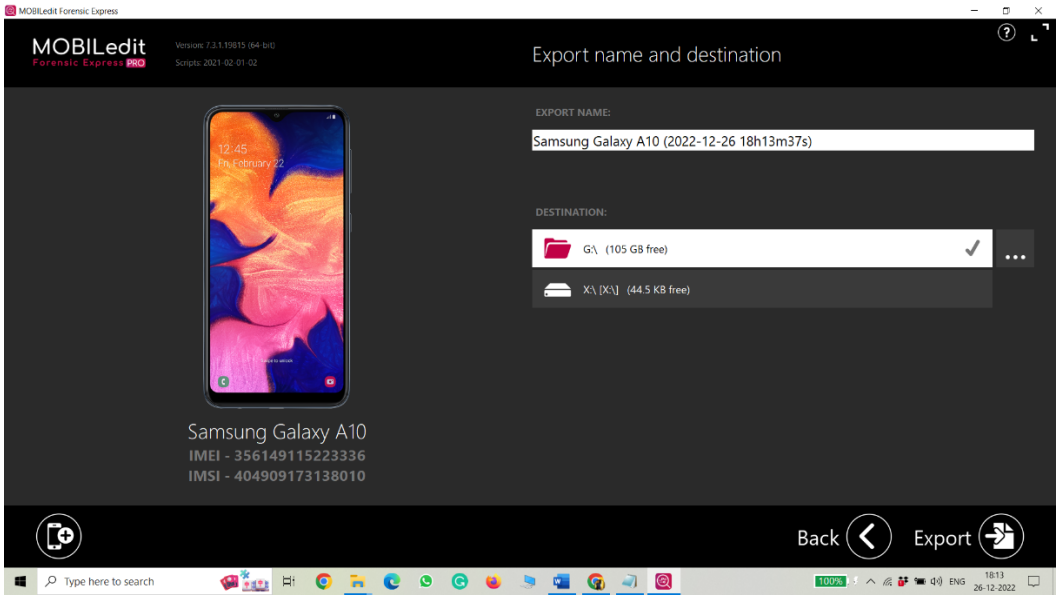
Step 9: Now enter the details as asked below.



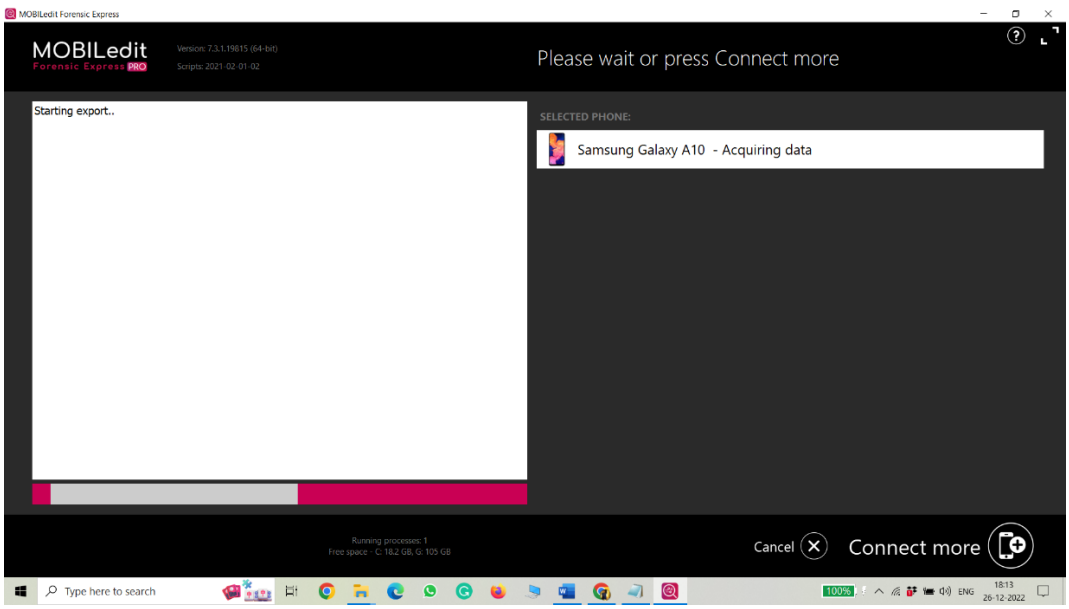
Step 10: Now choose the report format in which format you want the report.



Step 11: Now give the destination as per required.



Step 12: Now the exporting will start to wait till the complete exporting.



Last but not the least, phones will be exported to the given destination. We can access the report after completing the extraction.

4) Cellebrite UFED (Mobile Phone Extraction)

The **UFED** (**Universal Forensics Extraction Device**) is a product series of the Israeli company Cellebrite, which is used for the extraction and analysis of data from mobile devices by law enforcement agencies.

Features:

On the UFED Touch, it is possible to select extraction of data and choose from a wide list of vendors. After the data extraction is done, it is possible to analyze the data in the Physical Analyzer application.

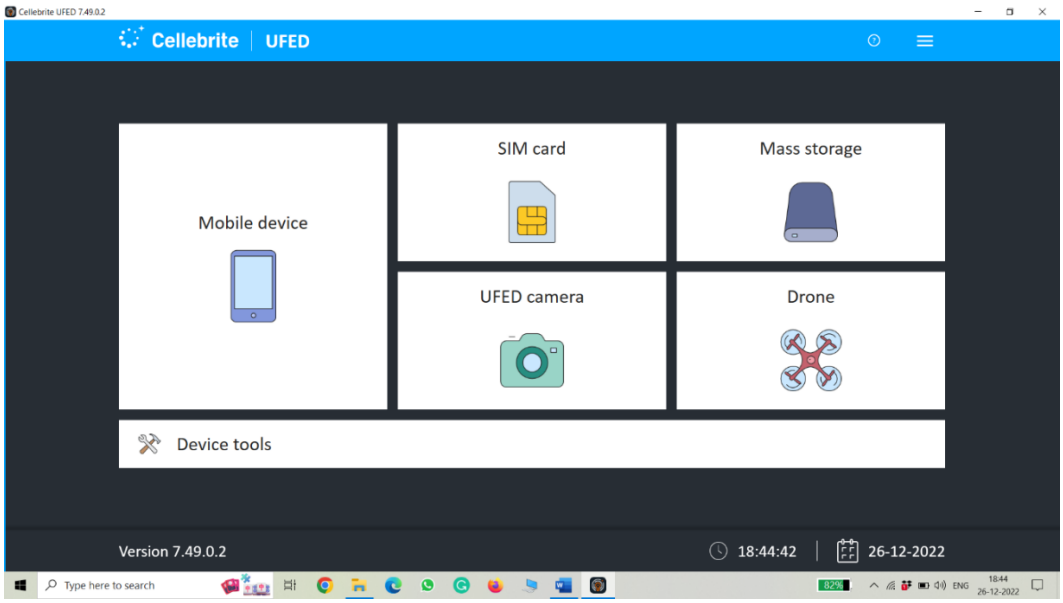
The Cellebrite UFED Physical Analyzer supports the following features:

- Extract device keys which can be used to decrypt raw disk images, as well as keychain items.
- Revealing device passwords, although this is not available for all locked devices
- Passcode recovery attacks
- Analysis and decoding of application data
- Generating reports in various formats such as PDF and HTML
- Dump the raw filesystem for analyzing it in other applications

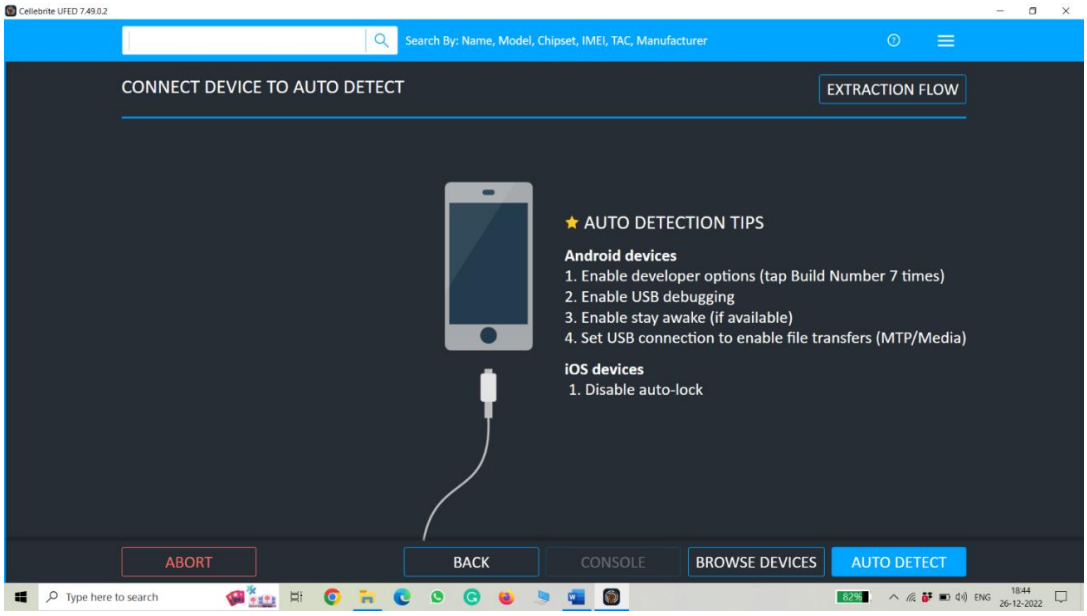
It contains more than 100 different cables to fit almost any phone, GPS, or tablet. The system is also capable of supporting more than 7,700 tested devices and regularly updates its list. Additionally, UFED supports more than 3,000 knock-off phones. UFED comes in a heavy-duty carrying case intended for field use. The product can auto-detect a large number of different devices. Once an apparatus is detected, UFED dumps its contents of it onto a USB drive or connected PC. The PC has a reporting application, available at no additional cost, that formats the dumped assets into a useful report.

Steps for connecting & Exporting Phones:

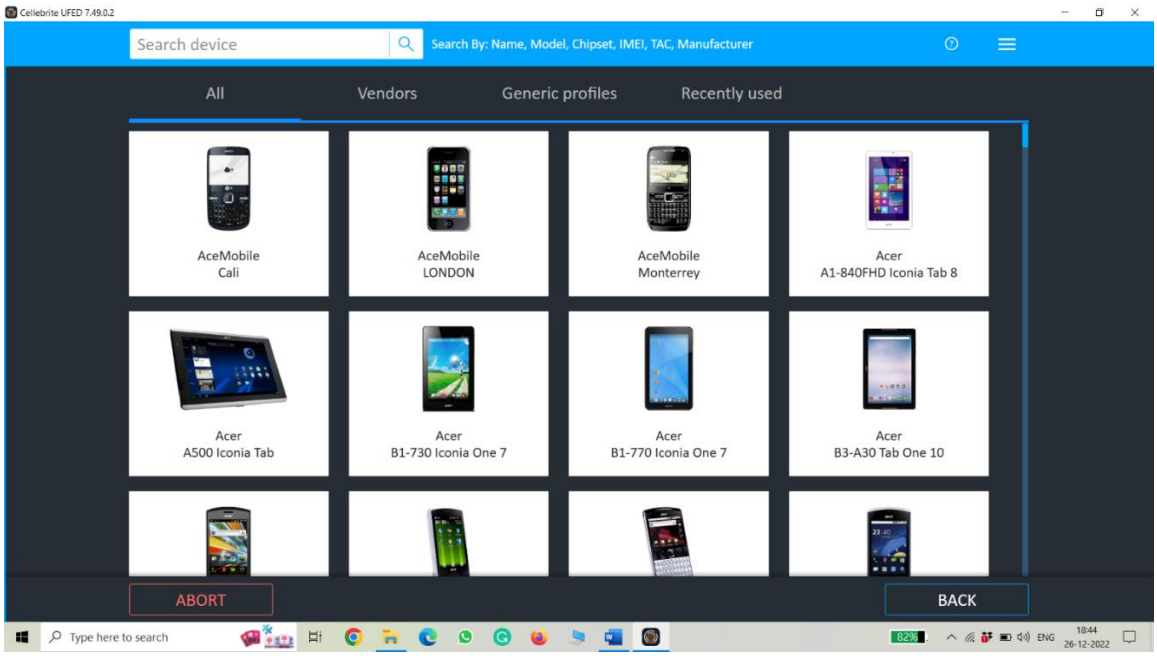
Step 1: Home page of cellebrite UFED application.



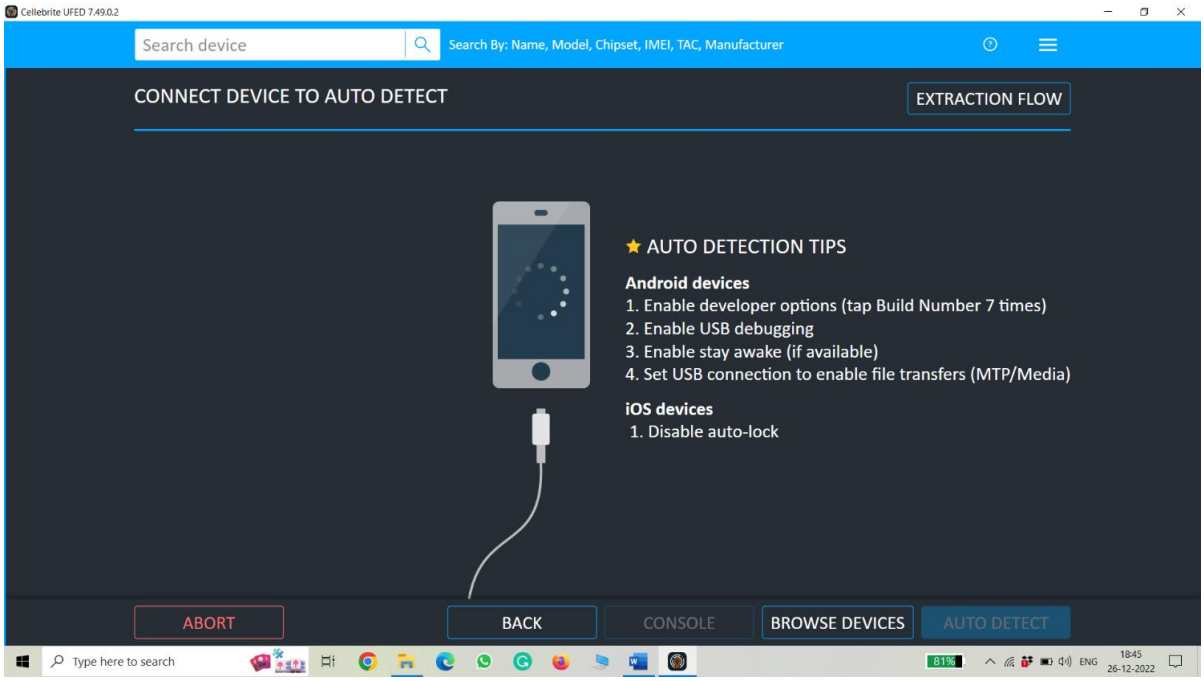
Step 2: Connecting device, note (Developer mode & USB debugging should be on)



Step 3: Connect the device manually. In these, we can select the device we want to export but, first, we have to check whether the device is available for which we have to export.



Step 4: If the device is not available we can Auto Detect the device by choosing the auto-detect option.



More About Cellibrite UFED:

Ever since early man put his handprints on the wall of a cave, humans have left a traceable trail of identifiers (evidence) behind. Nowhere has the identification of the suspects behind these trails been more sought after or tested than in the investigation of crimes. From fingerprint matching to handwriting analysis to DNA testing, law enforcement has continually sought new ways to identify the guilty and exonerate the innocent.

Today, identifying suspects in crimes is most easily done through the analysis of digital evidence. With smartphones now the primary evidence source in 96% of investigations*, developing ways to lawfully access data from mobile devices has

become critical in accelerating justice. As the global leader in Digital Intelligence solutions, Cellebrite has been at the forefront of providing law enforcement investigators with the tools to gain actionable intelligence for more than 20 years. (Digital Intelligence is the data collected and preserved from digital sources and data types [smartphones, computers, and the Cloud] and the process by which agencies collect, review, analyze, manage, and obtain insights from this data to run their investigations more efficiently.)
Long before the introduction of the first UFED (Universal Forensic Extraction Device), Cellebrite was leading the way with the development of solutions for transferring data from cell phone to cell phone when someone traded in or upgraded their device.
Since its introduction,

UFED has become the industry standard for lawfully accessing and collecting data, with thousands of units deployed globally. And UFEDs has been used in over 5 million investigations worldwide.

When we think about this from the examiner's point of view," Heather said, "they need to deal with more applications, more data sources, and they need to handle more data. The standard storage today on the iPhone is 128GB of data, and I'm putting aside the iCloud that you have as a backup to it, which is probably 200GB or maybe more. Think about how vast this data set is. Two years ago, it was 32GB, then it became 64GB. Now it doubled itself in a year. And it will keep doubling, or even multiplying by four or more times." Dealing with this much data is causing huge problems.

Examiners need a solution that allows them to extract the data they want (selective extraction) in the least amount of time from as wide a range of devices as possible including encrypted Android and iOS devices.

5. DISK DRILL (data recovery)

Many users experience data loss at some point or another. It may be due to user-inflicted mistakes such as accidental deletion, or uncontrollable factors such as a storage device dying or becoming logically corrupted. However, in most cases, the lost data is still recoverable.

Disk Drill is a data recovery program that helps you recover missing data, right from the comfort of your home. The sections below will describe in detail–what is Disk Drill and why it's the premier choice for users looking to retrieve their missing data.

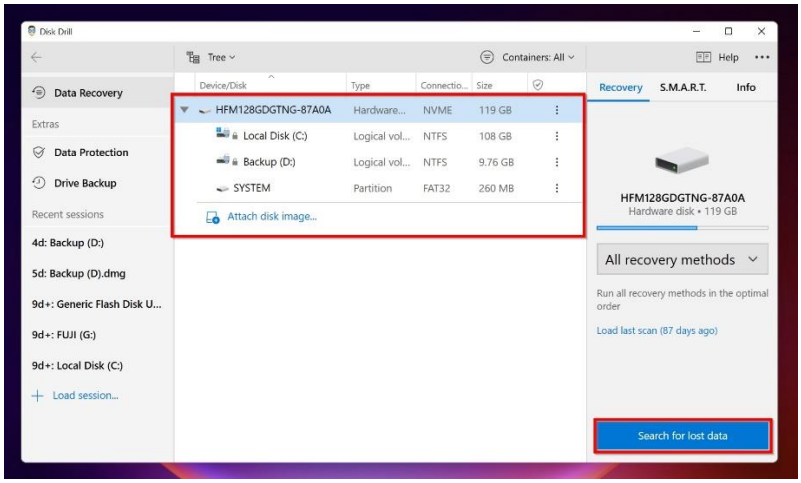
Why do we need Disk Drill:

There are numerous benefits to using a Disk Drill on your device. While being able to recover data from your device at a nominal cost is one of them, Disk Drill comes with lots of other tools that help you prevent data loss and monitor the health of your disk.

Let’s get an overview of the various benefits that Disk Drill offers to its users:

1) □ Recover Deleted Data on Any Device

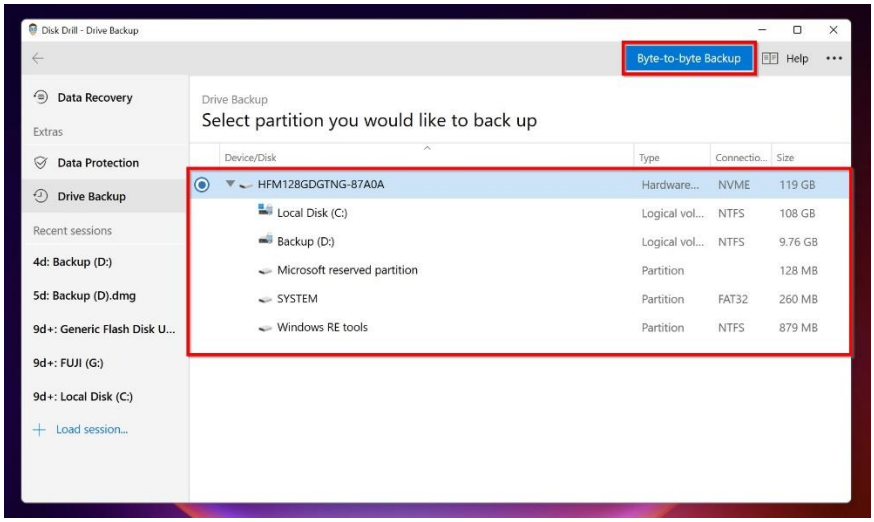
Since Disk Drill can be installed on both Windows and macOS and supports data recovery from Android and iOS as well, you can restore your missing data from virtually any device within a few clicks. Simply launch Disk Drill, select the storage device, and click on **Search for lost data**. After this, users just need to wait for Disk Drill to complete the scan and select the files they want to recover.



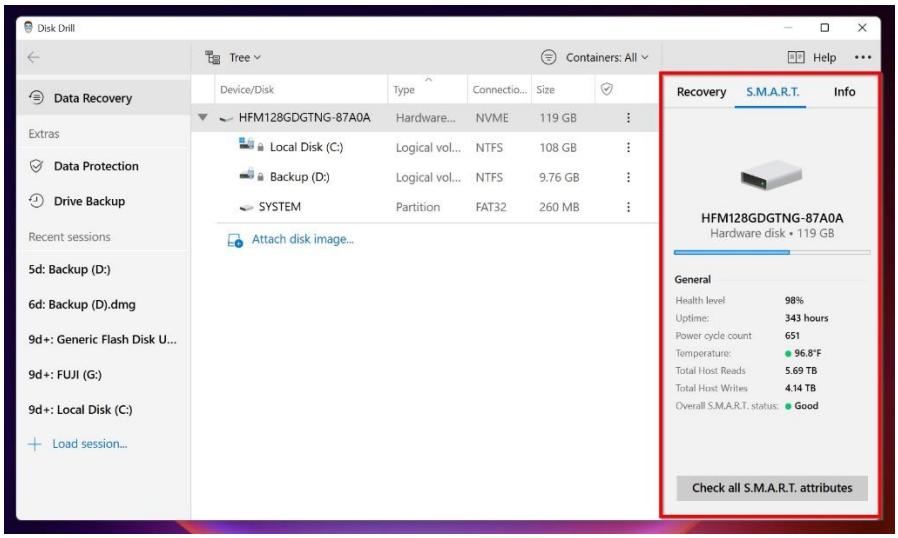
With multiple scan types and support for all major file systems at your disposal, users needn’t worry about compatibility issues when using Disk Drill. The actual recovery process is made even simpler with an intuitive file selection screen that has various filtering options and a preview feature.

2) □ Data Backup and Disk Monitoring

Regularly backing up your data is the most effective way to prevent data loss. Disk Drill allows you to create a disk image of your entire drive or individual partitions, making the process much easier. To create a disk image, users simply need to open Disk Drill, click on **Drive Backup**, choose the partition or drive, and then click on **Byte-to-byte backup**.



Disk Drill also allows you to view the S.M.A.R.T. status of your storage drive in an easy-to-understand manner. The SMART disk monitoring feature will display the health of your storage device under various parameters. To view the SMART status of your disk in Disk Drill, first, open Disk Drill, select the HDD or SSD and click on the **S.M.A.R.T.** option on the pane towards the right side.



□ Optimize Disk Space

Disk Drill for Mac has a highly useful feature called Clean Up, which analyzes your drive and finds redundant and duplicate files. Removing these files can improve the performance of your device, as well as free up a significant amount of disk space.

Using the Clean Up feature is easy: launch Disk Drill, choose the Clean Up mode, select a drive, and click Scan.

Who Can Use Disk Drill:

An essential criterion to gauge a data recovery program is its usability. Users are spoiled for choice when it comes to data recovery programs. However, most programs either

target advanced users or complete beginners. Disk Drill strikes the perfect balance between both.

Both beginners and seasoned PC users can use Disk Drill to recover their data. The minimalist UI with in-built tutorials makes sure that new users aren't overwhelmed, whereas an abundance of advanced features, scan types, data backup, and data protection features ensure that advanced users can decide how exactly they want to use Disk Drill.

Additionally, Disk Drill's wide spectrum of compatibility allows users on any major platform to perform data recovery. The program can be downloaded and installed on both Windows and macOS. Disk Drill also supports data recovery from Android and iOS, although users will have to connect their devices to a computer for the data recovery process.

Pros of Disk Drill:

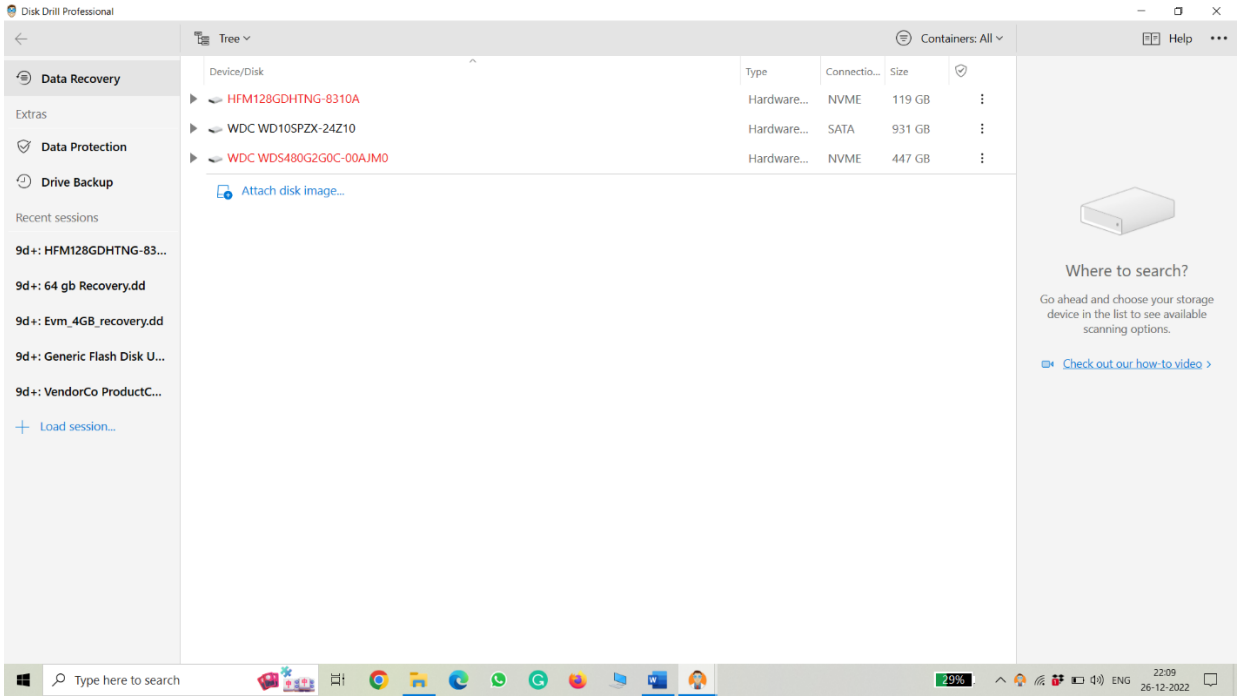
- Its interface is simple.
- It is easy to use.
- It has both Windows and Mac versions.
- It can work for recovering data from different file systems.
- It allows you to search for files by name.
- It allows you to preview some types of scanned files.

Cons of Disk Drill:

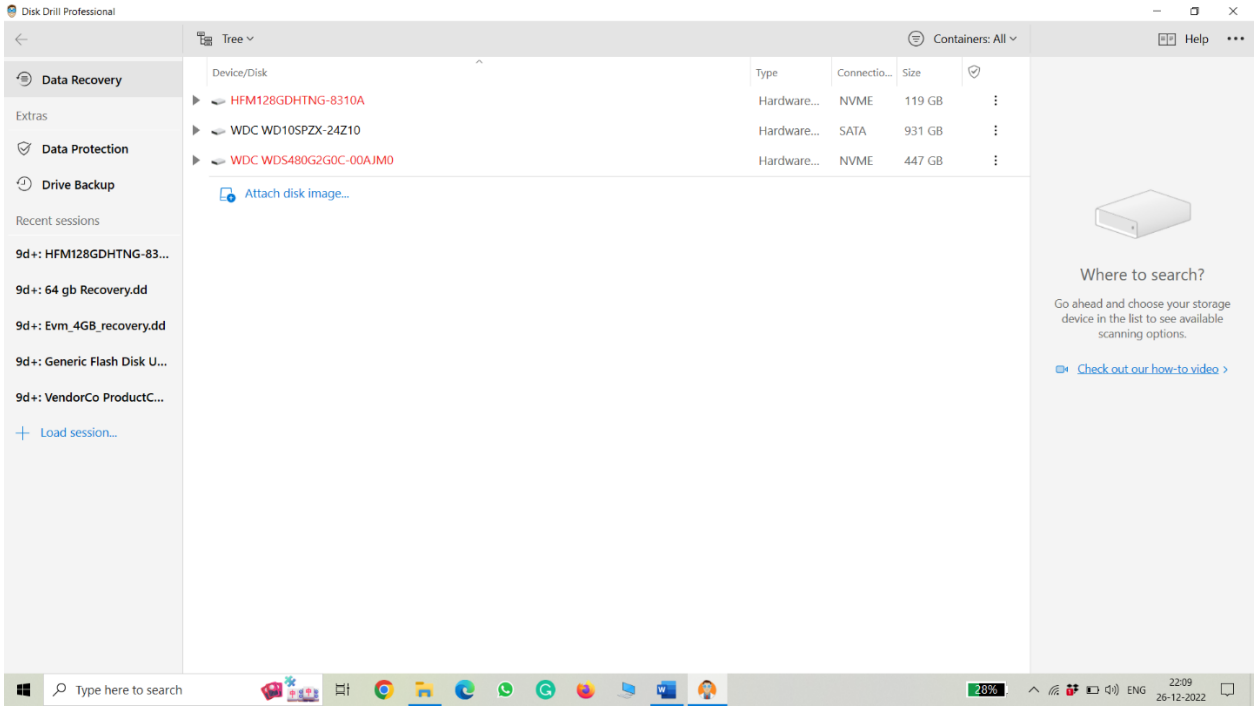
- It only allows you to recover 500MB of data with the free edition of Disk Drill.
- It doesn't show the file's condition or quality in the scan results.

Steps for using Disk Drill Software:

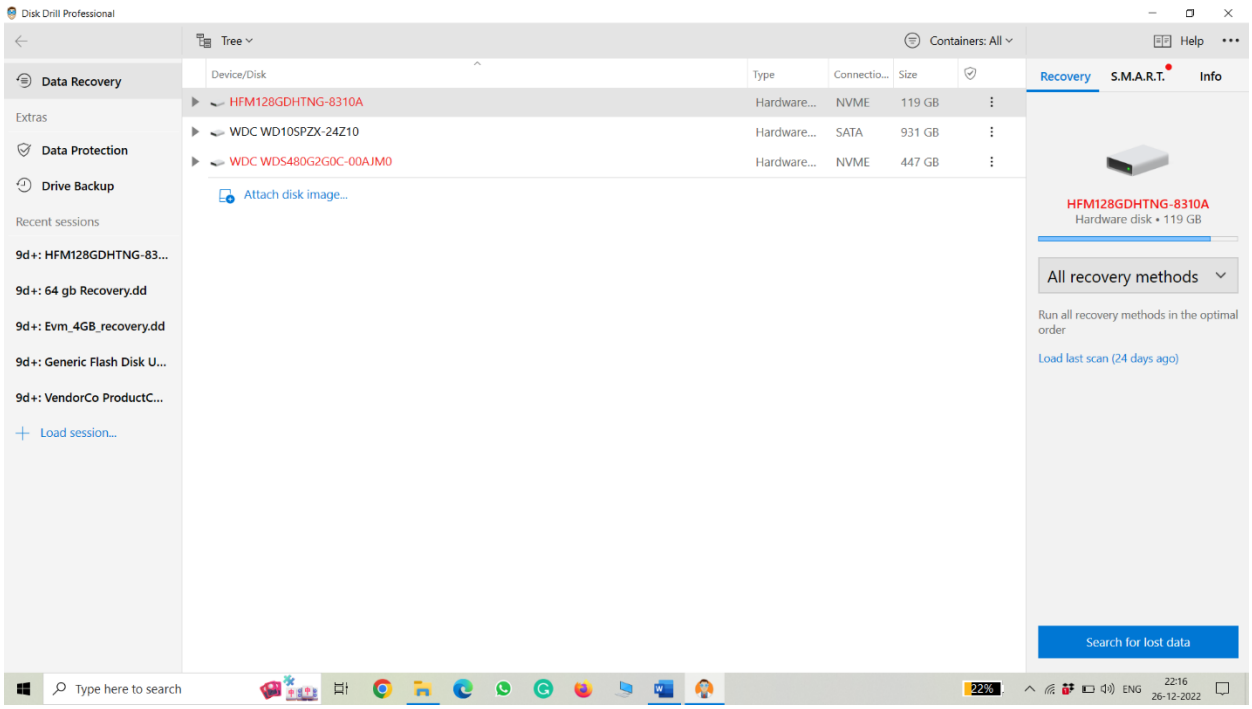
Step 1: Home page of Disk Drill software. Where we will see the drives available in the device we can also add any kind of disk image by just clicking on Attach Disk Image.



Step 2: Then we have to select the drive from which we want recovery.

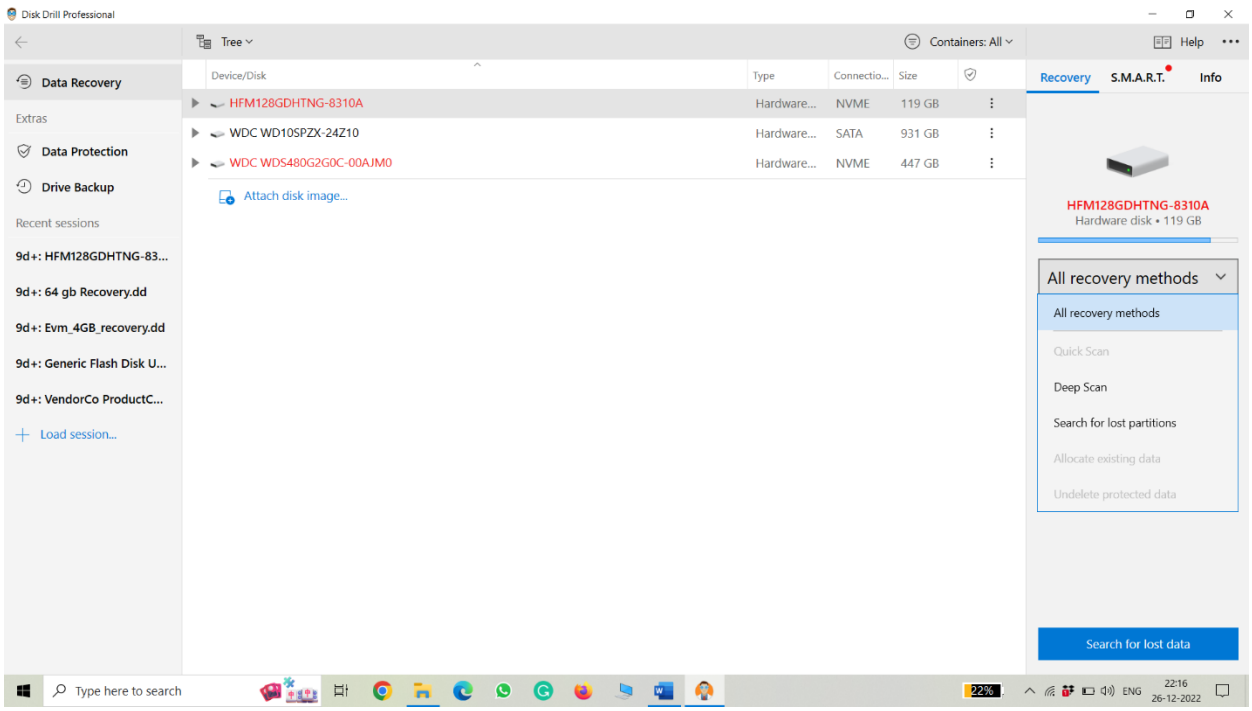


Step 3: After selecting drive we will see one option on the right-hand side bottom where all recovery methods will be shown we have to select the recovery method from it.

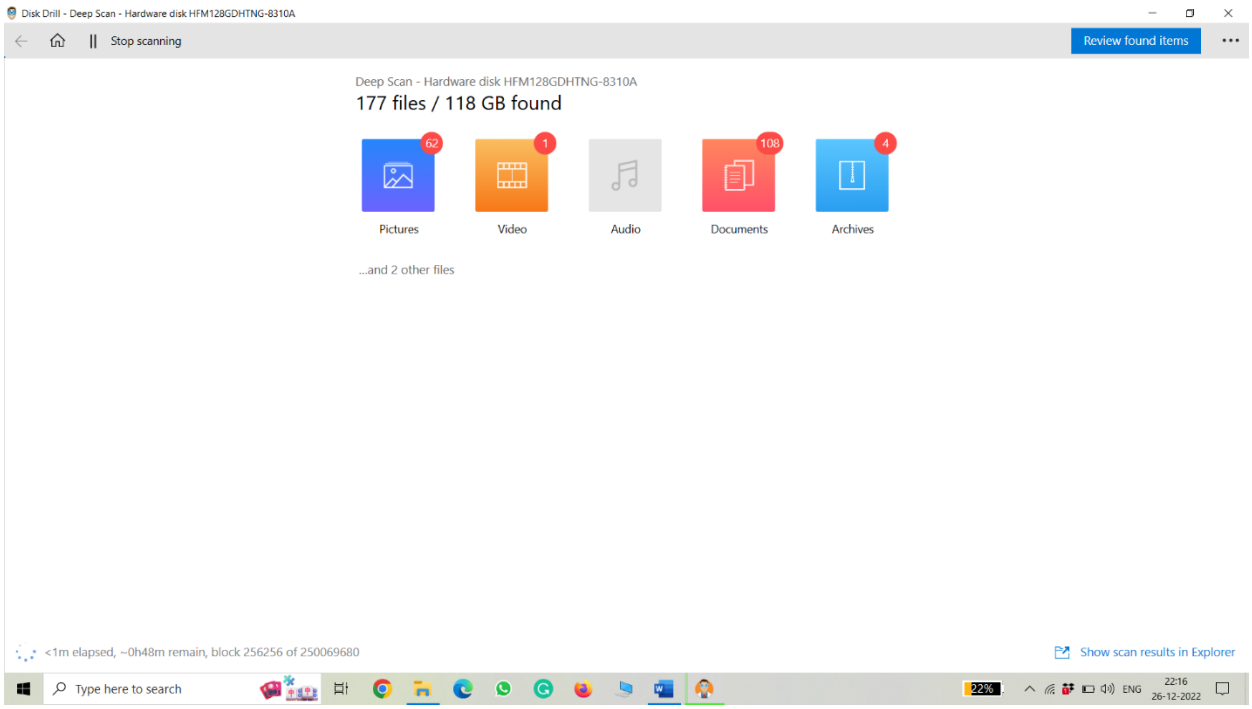


We will see 5 recovery methods as follows:

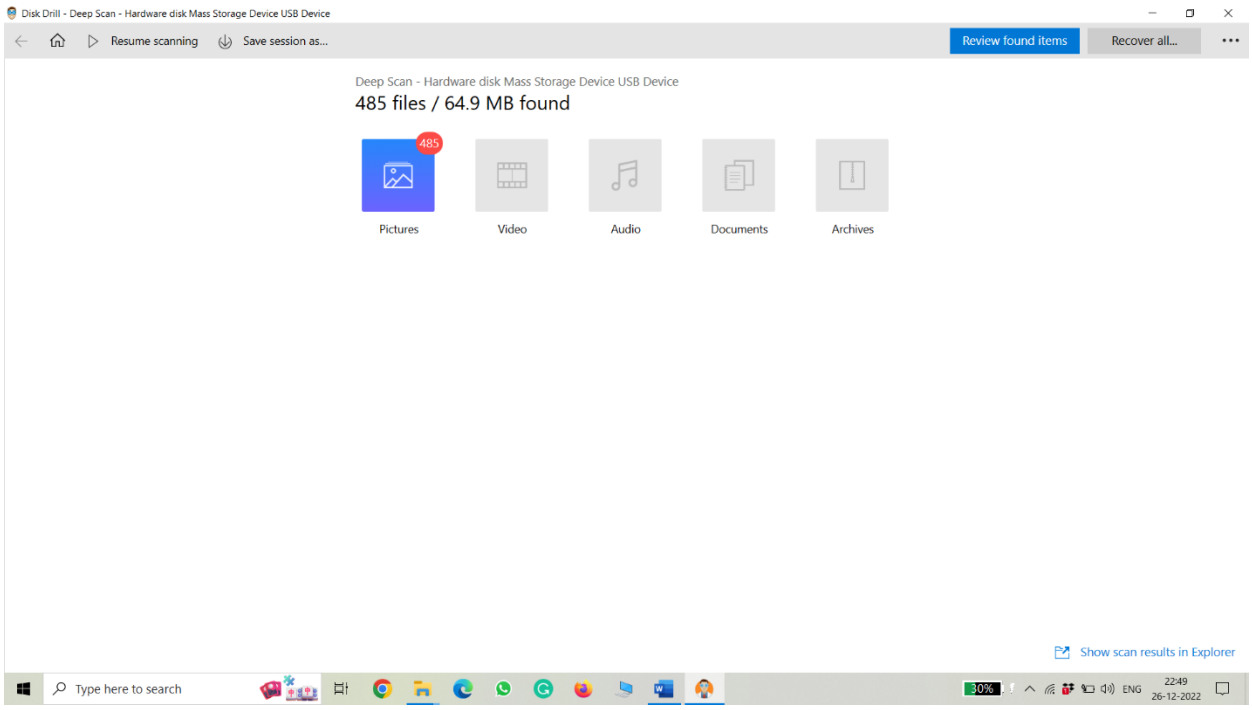
- Quick Scan
- Deep Scan
- Search for lost partitions
- Allocate existing data
- Undelete Protected data



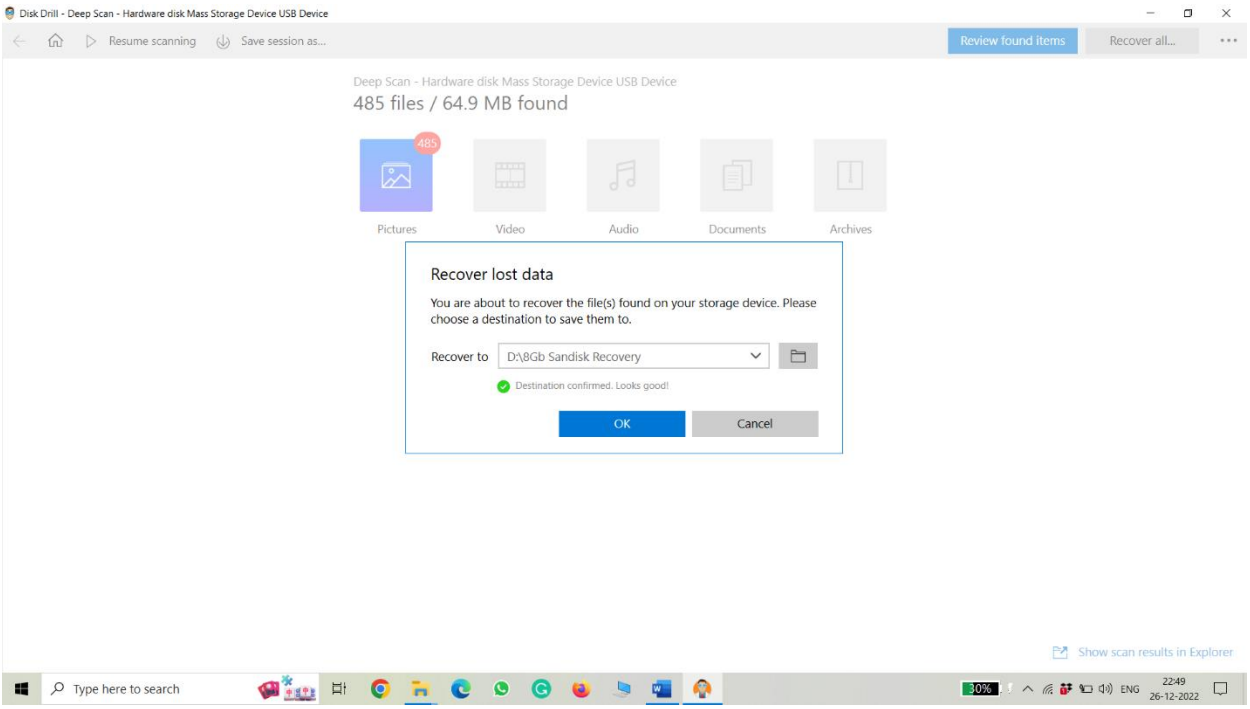
Step 4: After selecting the recovery method it will start scanning and find all files (pictures, documents, videos, audio, archives)



Step 5: After the completion of scanning it will show an option Recover all in the top right corner of the page.



Step 6: Last but not the list after clicking on Recover all it will show a pop-up in which we have to give the destination folder for recovering all the found data.



6. AUTOPSY (analysis report)

Autopsy® is the premier end-to-end open-source digital forensics platform. Built by Basis Technology with the core features you expect in commercial forensic tools, Autopsy is a fast, thorough, and efficient hard drive investigation solution that evolves with your needs.

An autopsy is computer software that makes it simpler to deploy many of the open-source programs and plugins used in The Sleuth Kit.[1] 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. The tool is largely maintained by Basis Technology Corp. with the assistance of programmers from the community. The company sells support services and training for using the product.[2]

The tool is designed with these principles in mind:

- Extensible — the user should be able to add new functionality by creating plugins that can analyze all or part of the underlying data source.
- Centralised — the tool must offer a standard and consistent mechanism for accessing all features and modules.
- Ease of Use — the Autopsy Browser must offer wizards and historical tools to make it easier for users to repeat their steps without excessive reconfiguration.
- Multiple Users — the tool should be usable by one investigator or coordinate the work of a team.

The core browser can be extended by adding modules that help scan the files (called "ingesting"), browse the results (called "viewing"), or summarize results (called "reporting"). A collection of open-source modules allow customization.

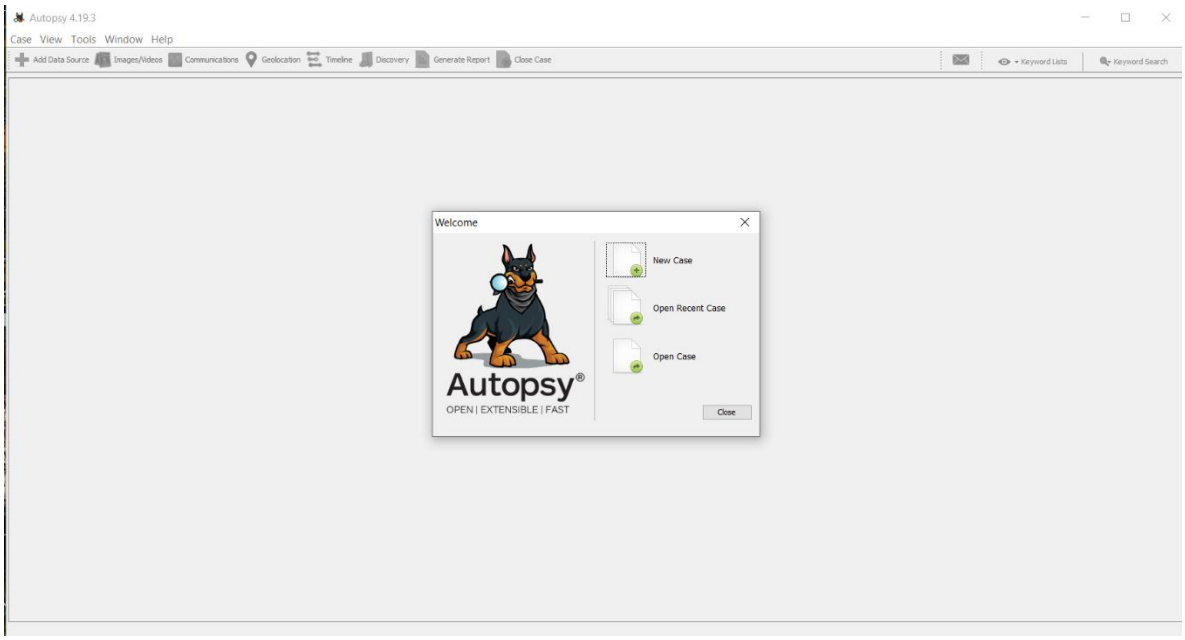
Process:

Autopsy analyzes major file systems (NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, YAFFS2) by hashing all files, unpacking standard archives (ZIP, JAR, etc.), extracting any EXIF values and putting keywords in an index. Some file types like standard email formats or contact files are also parsed and cataloged.

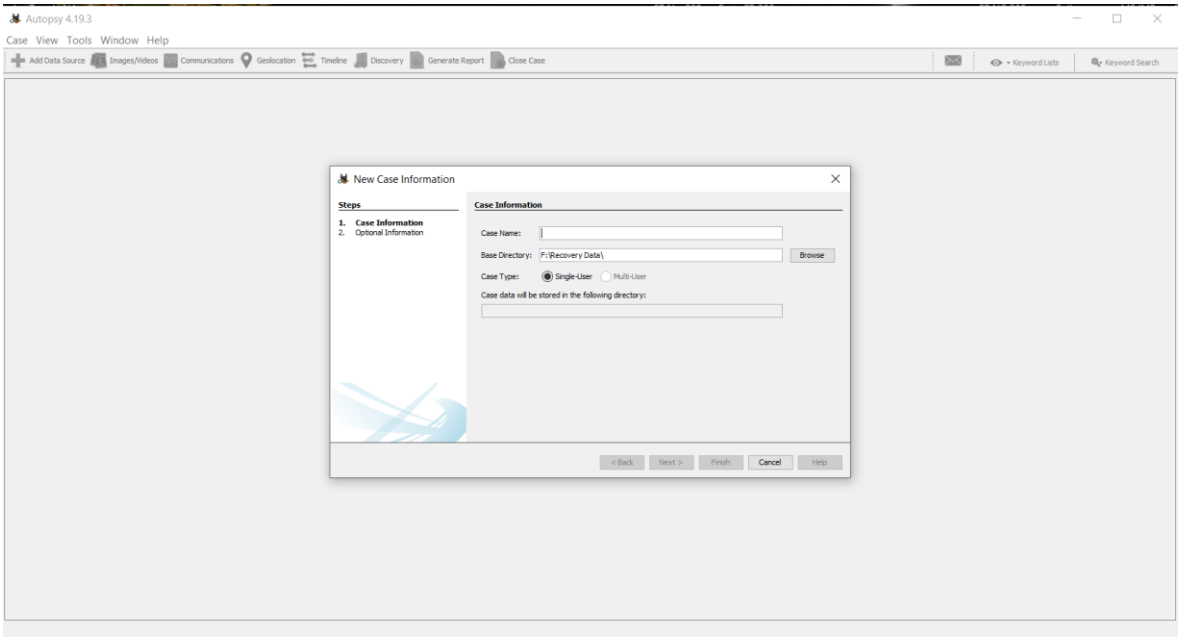
Users can search these indexed files for the recent activity or create a report in HTML or PDF summarizing important recent activity. If time is short, users may activate triage features that use rules to analyze the most important files first. An autopsy can save a partial image of these files in VHD format.

Steps of Autopsy:

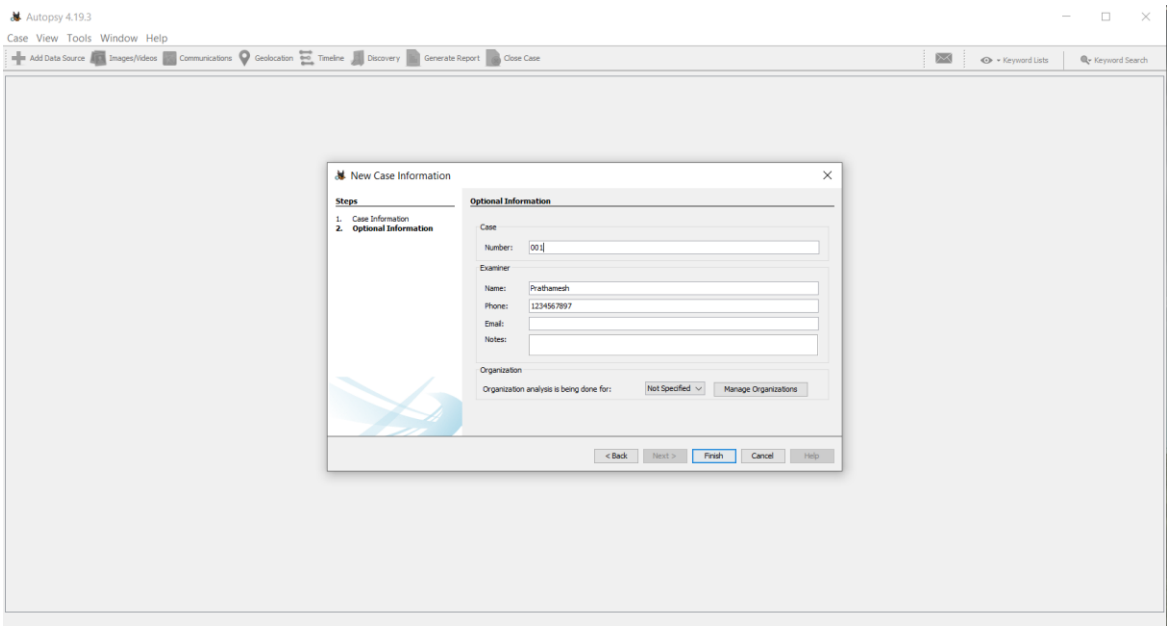
Step 1: Home page of Autopsy where we have to choose a case (New case, Open the recent case, open case)



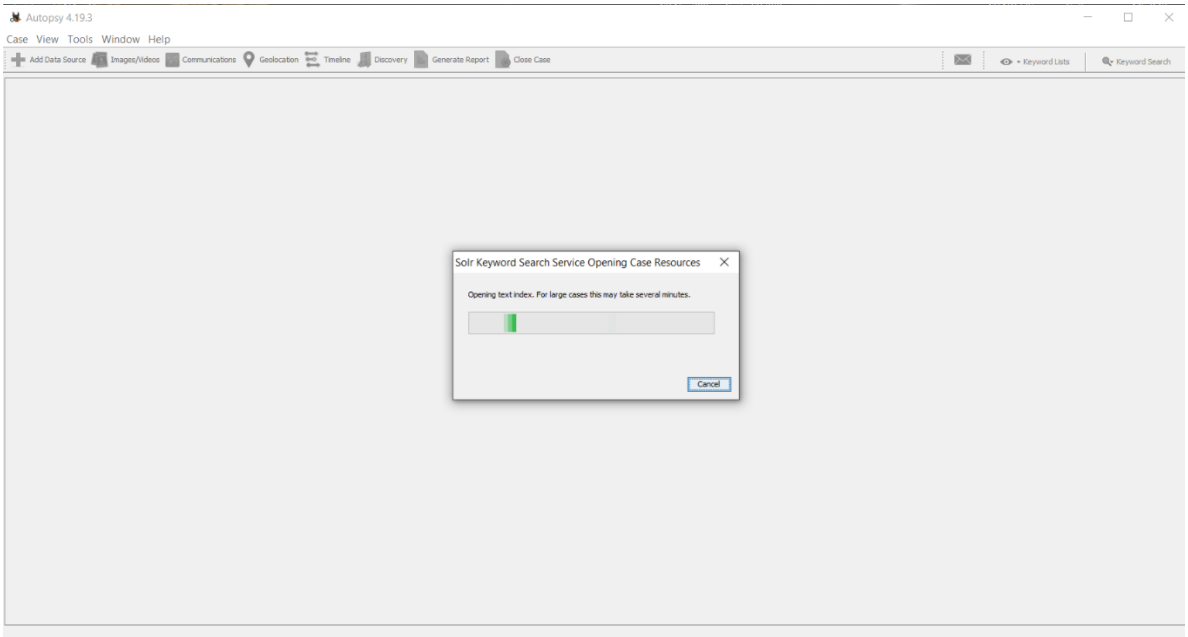
Step 2: Then we have to enter case information.



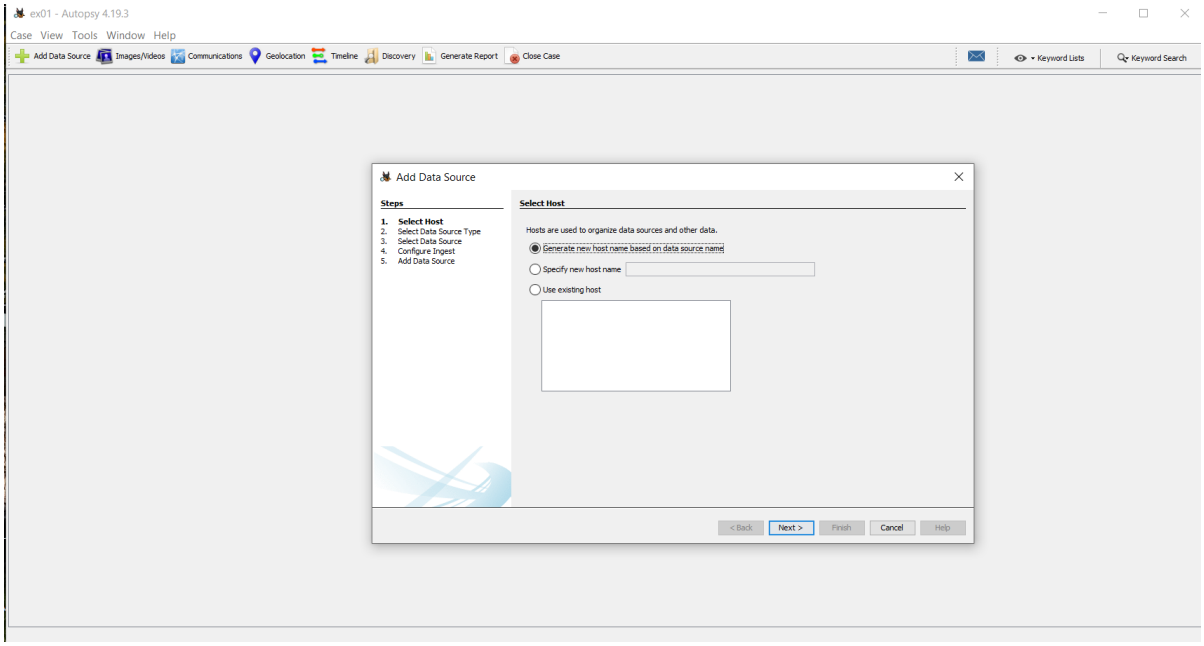
Step 3: Then the optional information page will come.



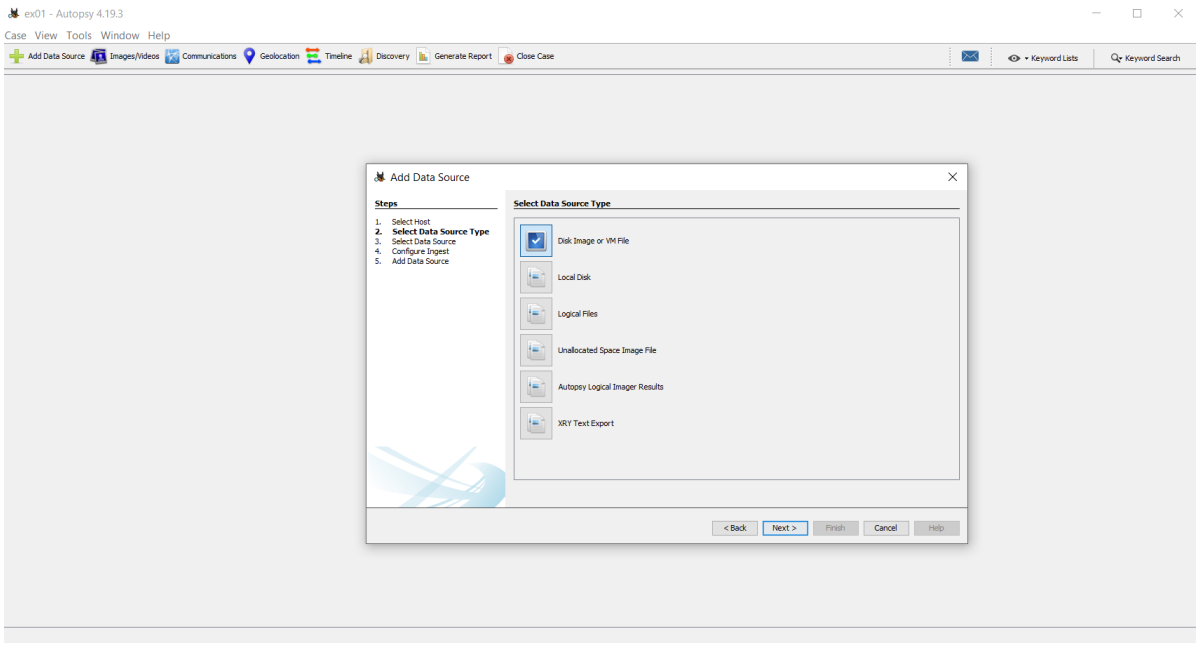
Step 4: After giving case information it will search for opening case resources.



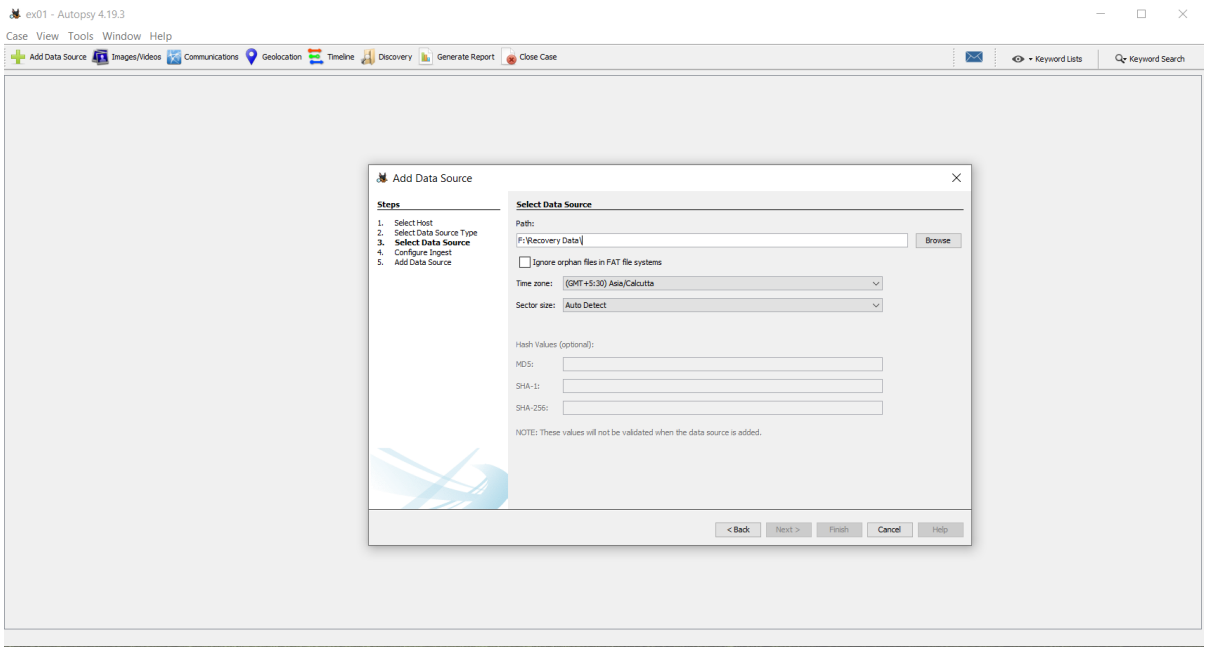
Step 5: After all these processes we have to select the host.

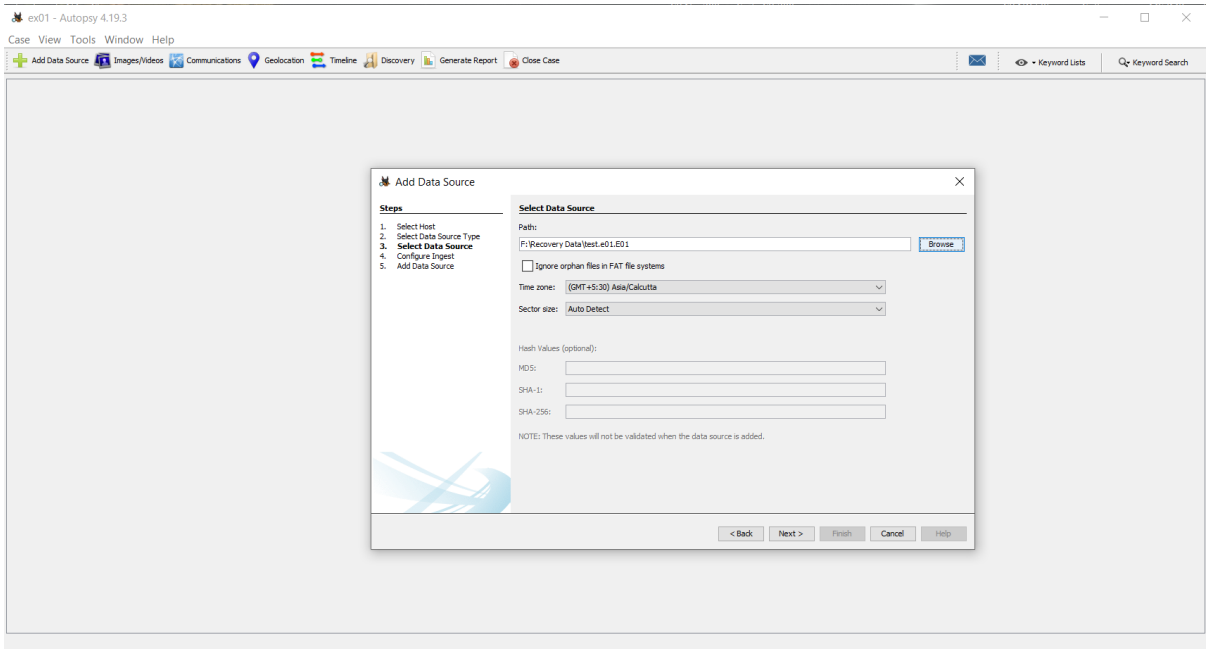


Step 6: Then we have to select the data source type.

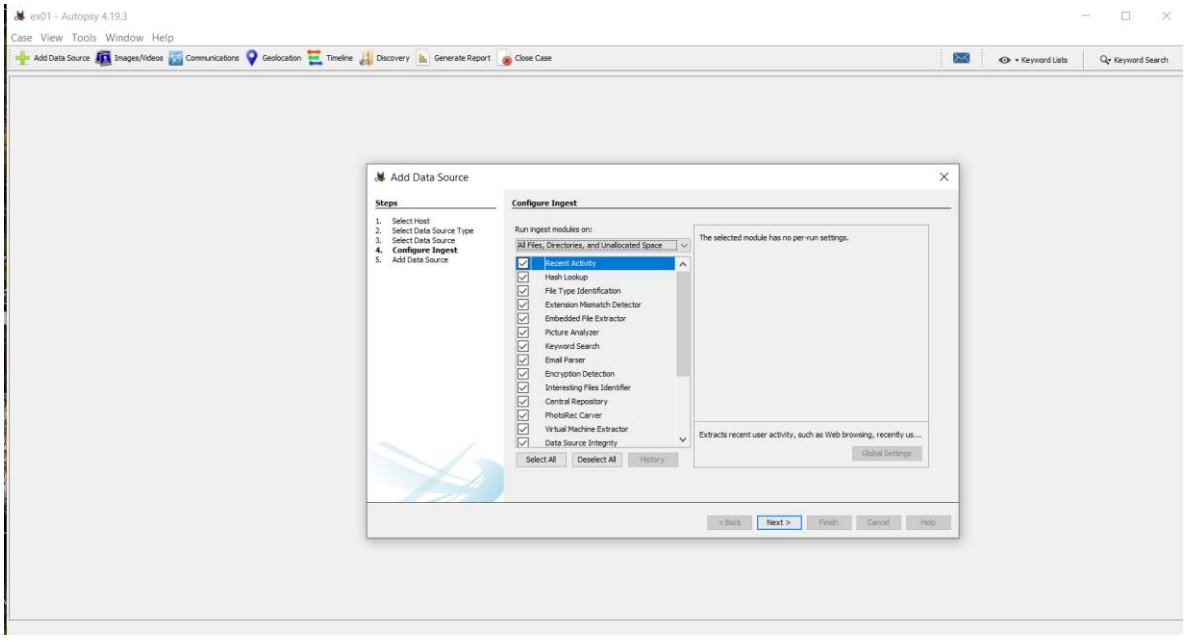


Step 7: Then we have to select the data source.

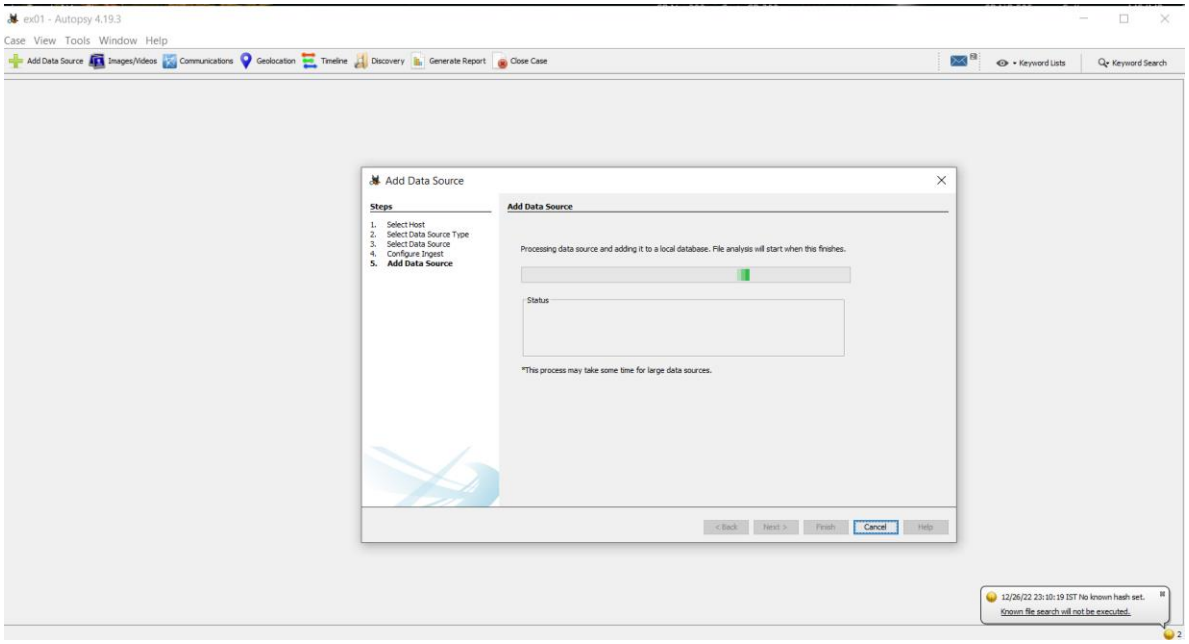




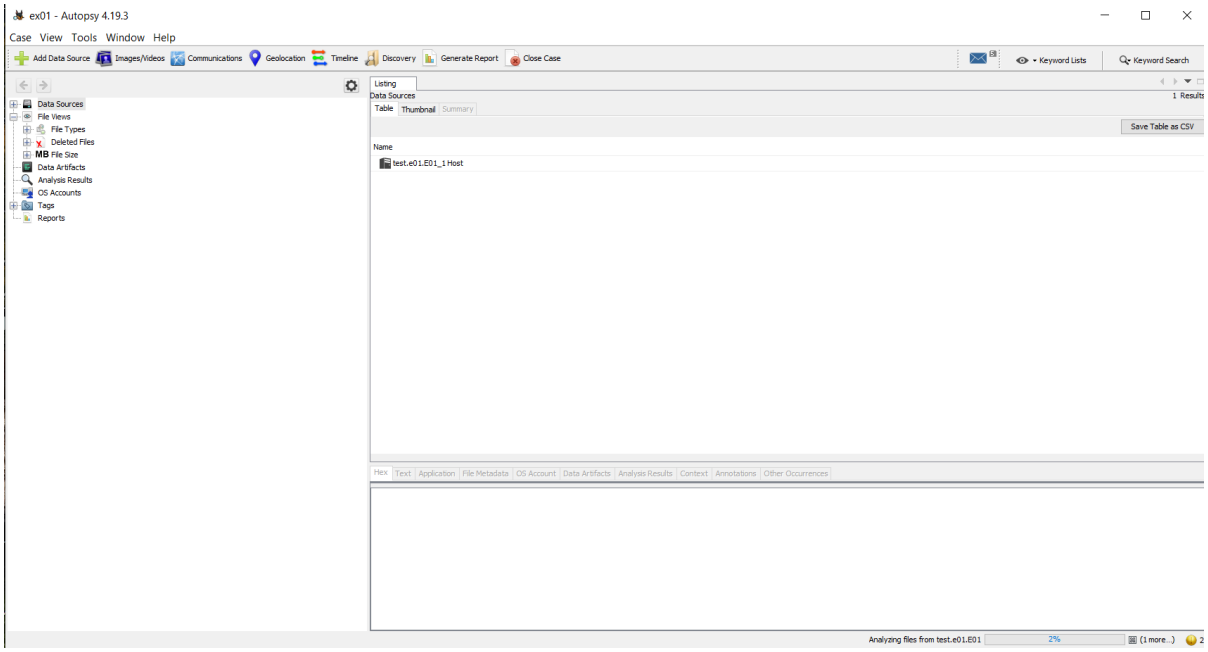
Step 8: Then we have to configure Ingest



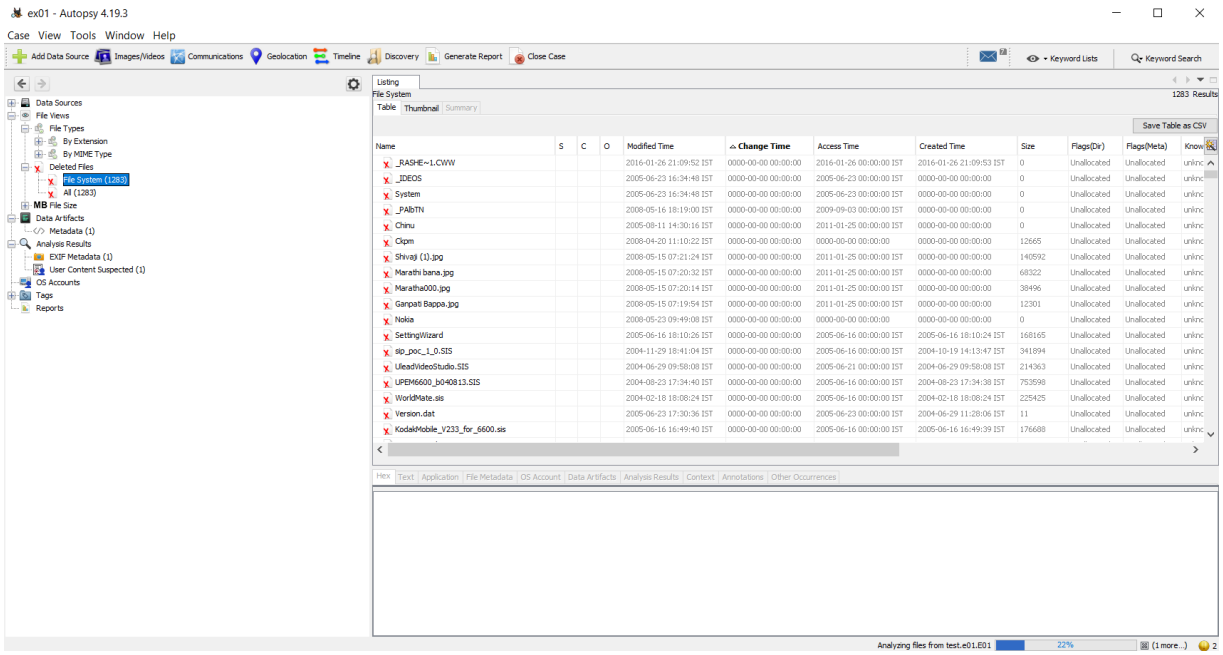
Step 9: After that, we have to add a data source.



Step 10: Then the analysis of data will get started.



Step 11: After the completion of the whole analysis we can see the data from the left top corner of the page.

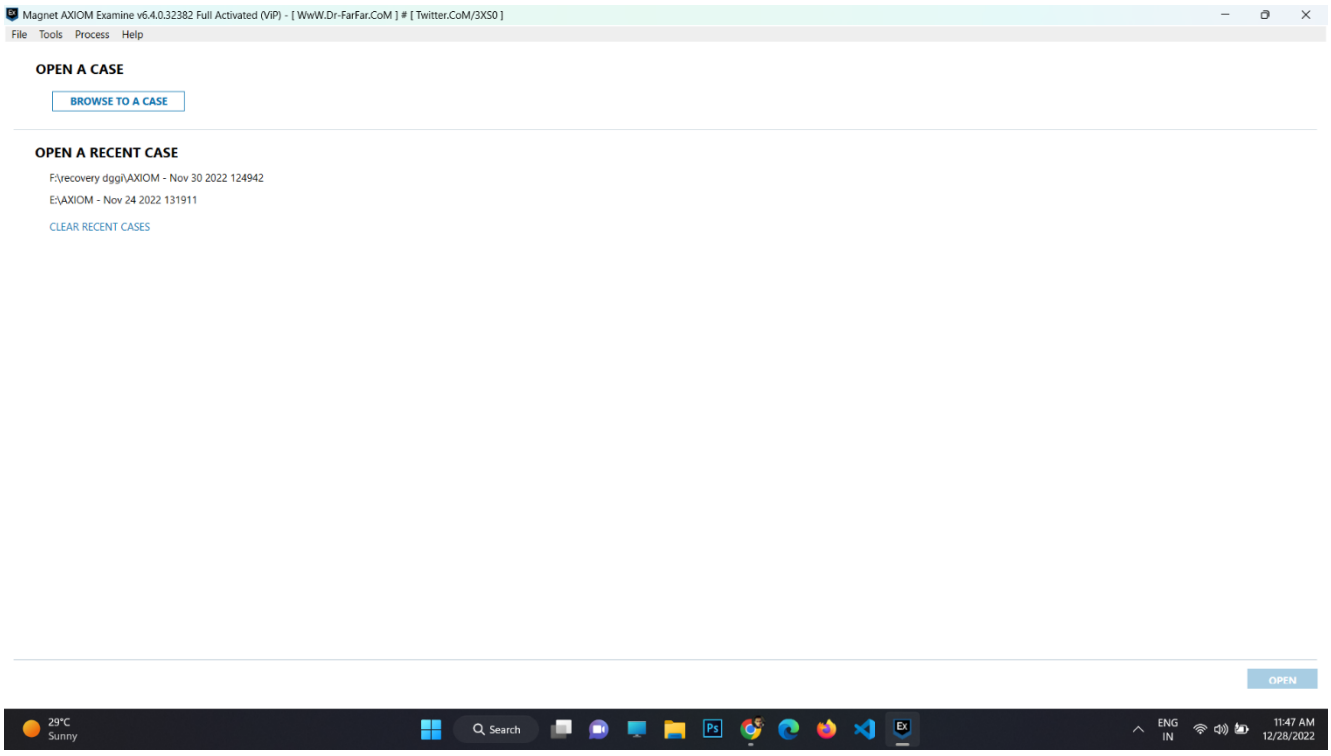


7. MAGNET (analysis report)

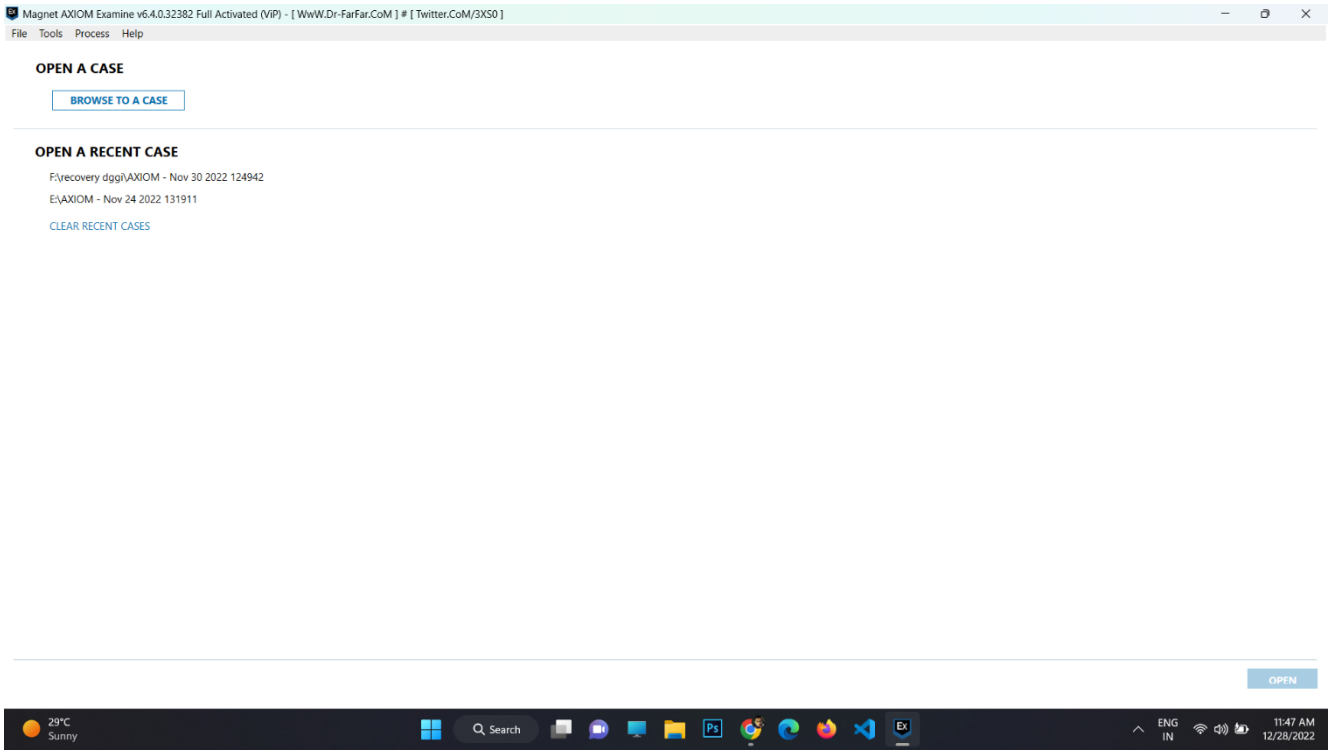
Magnet AXIOM is purpose-built to recover, process, and analyze digital evidence from a variety of sources regardless of whether you use AXIOM or third-party tools to acquire your data.

Steps:

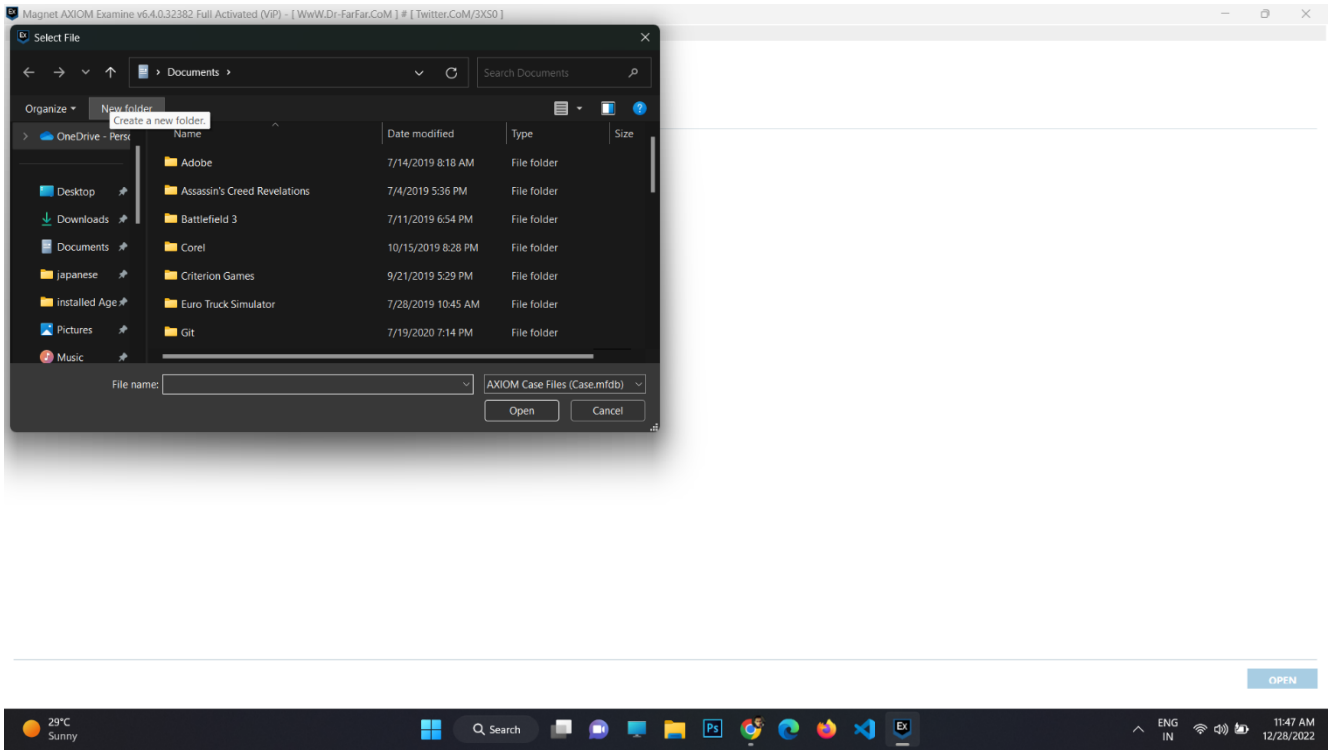
Step 1: Welcome page of AXIOM Magnet.



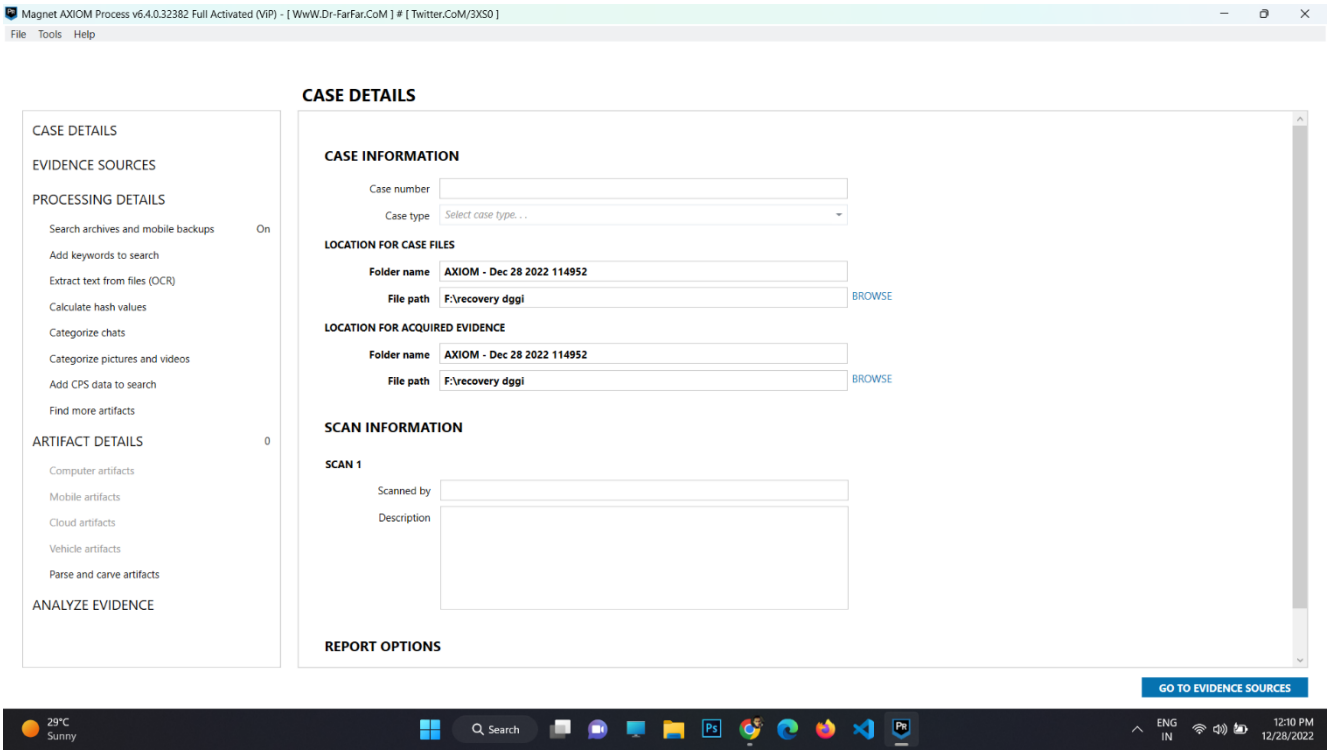
Step 2: We can create a new case or we can open a recent case.



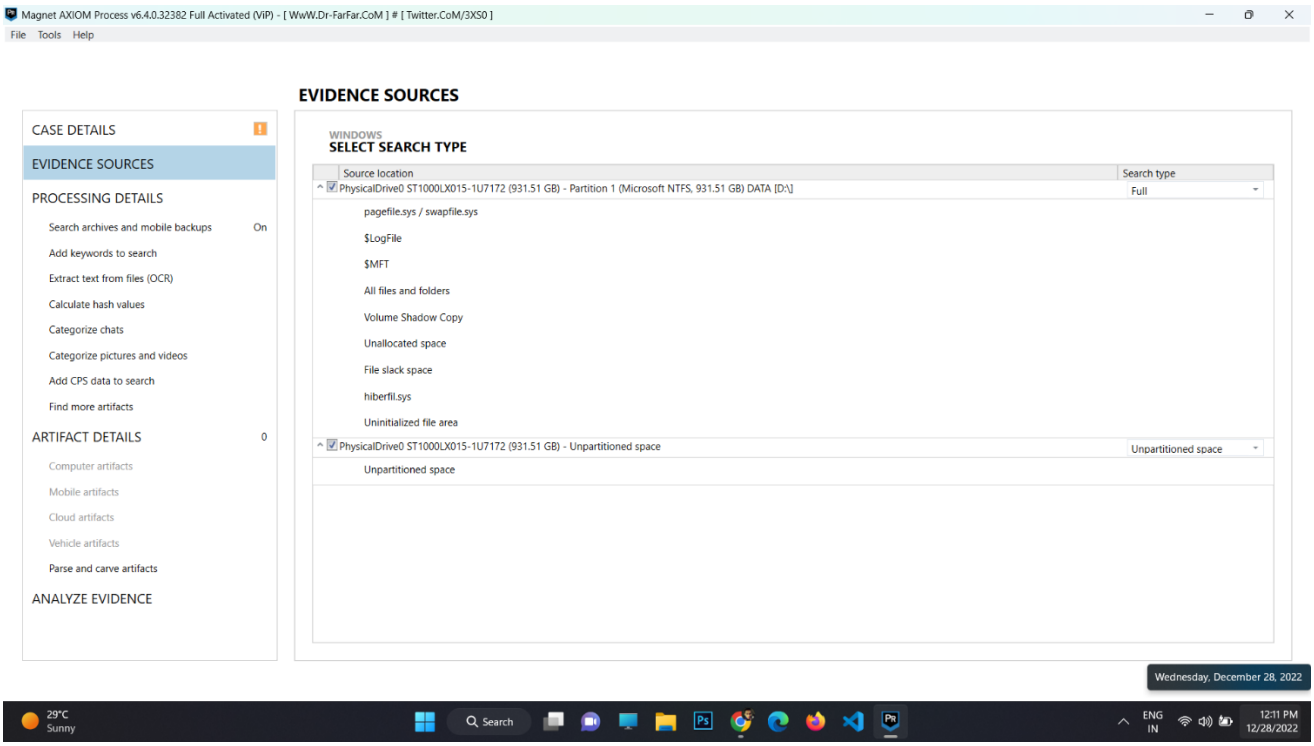
Step 3: After clicking a new case we need to give file location.

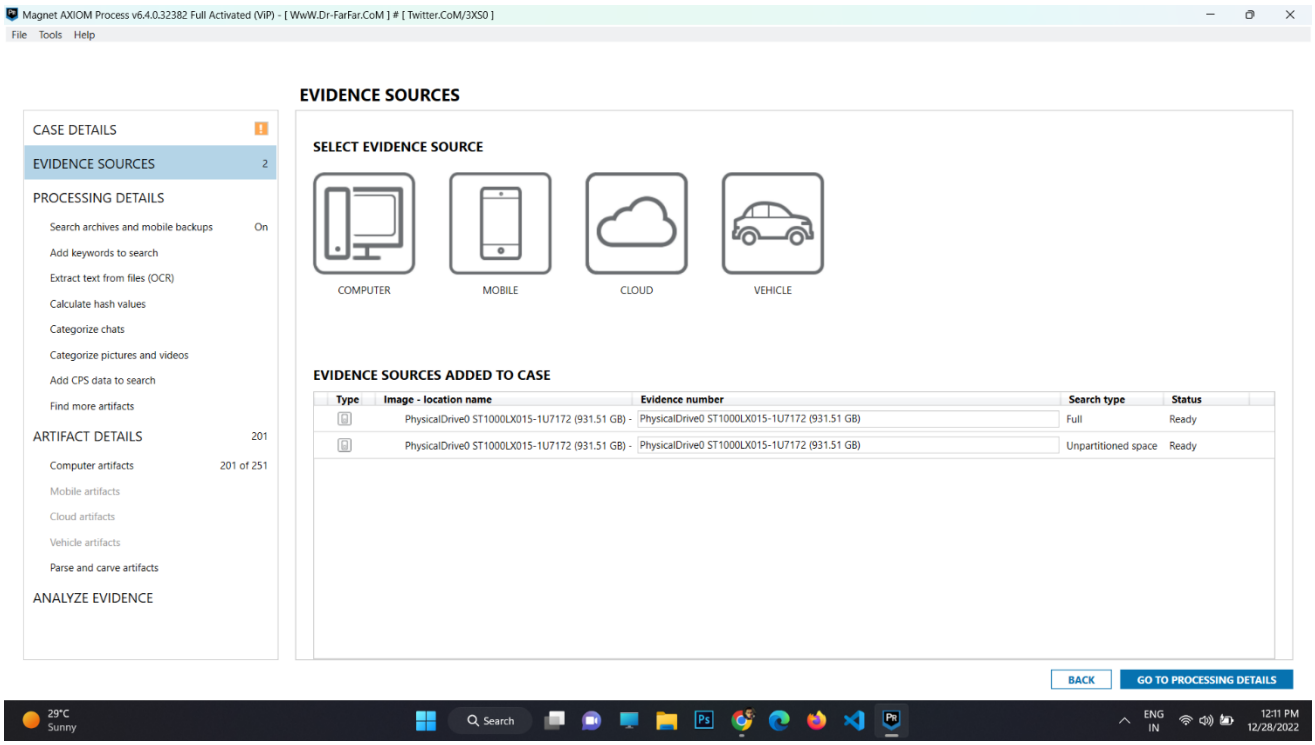


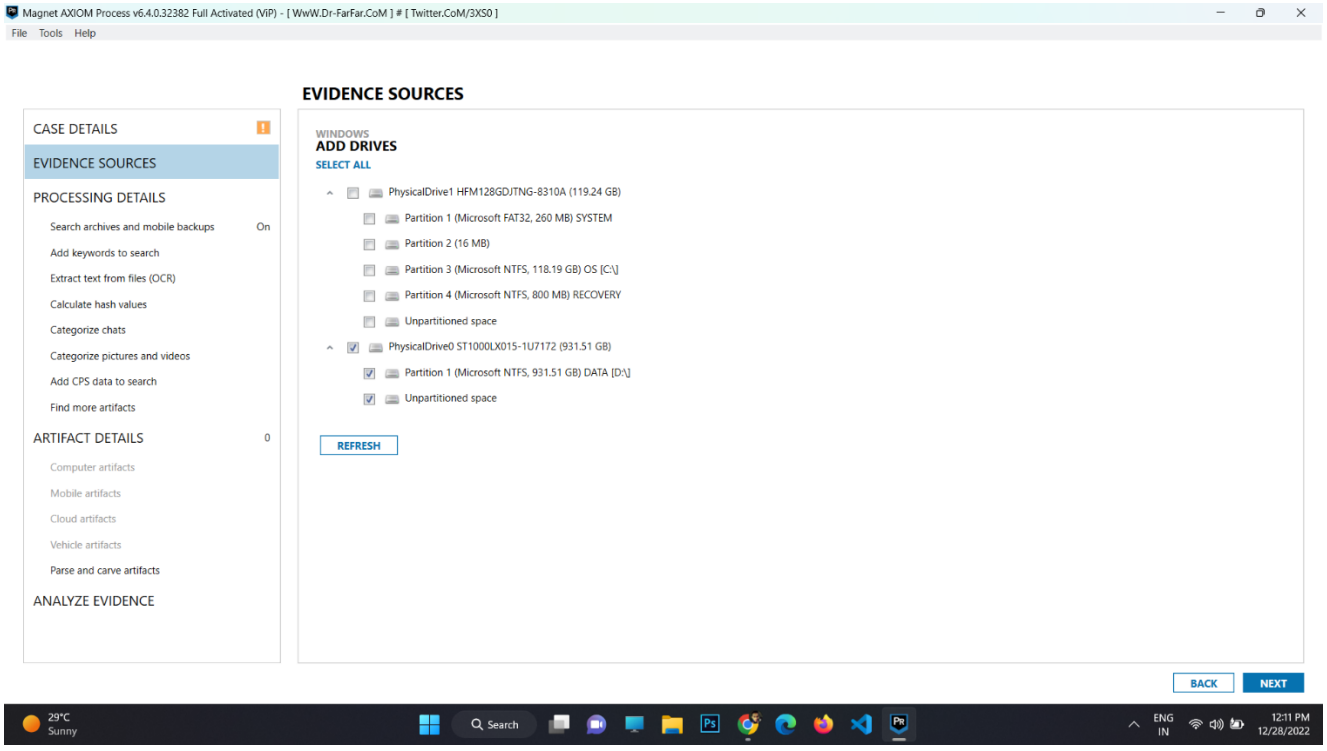
Step 4: Create case details.

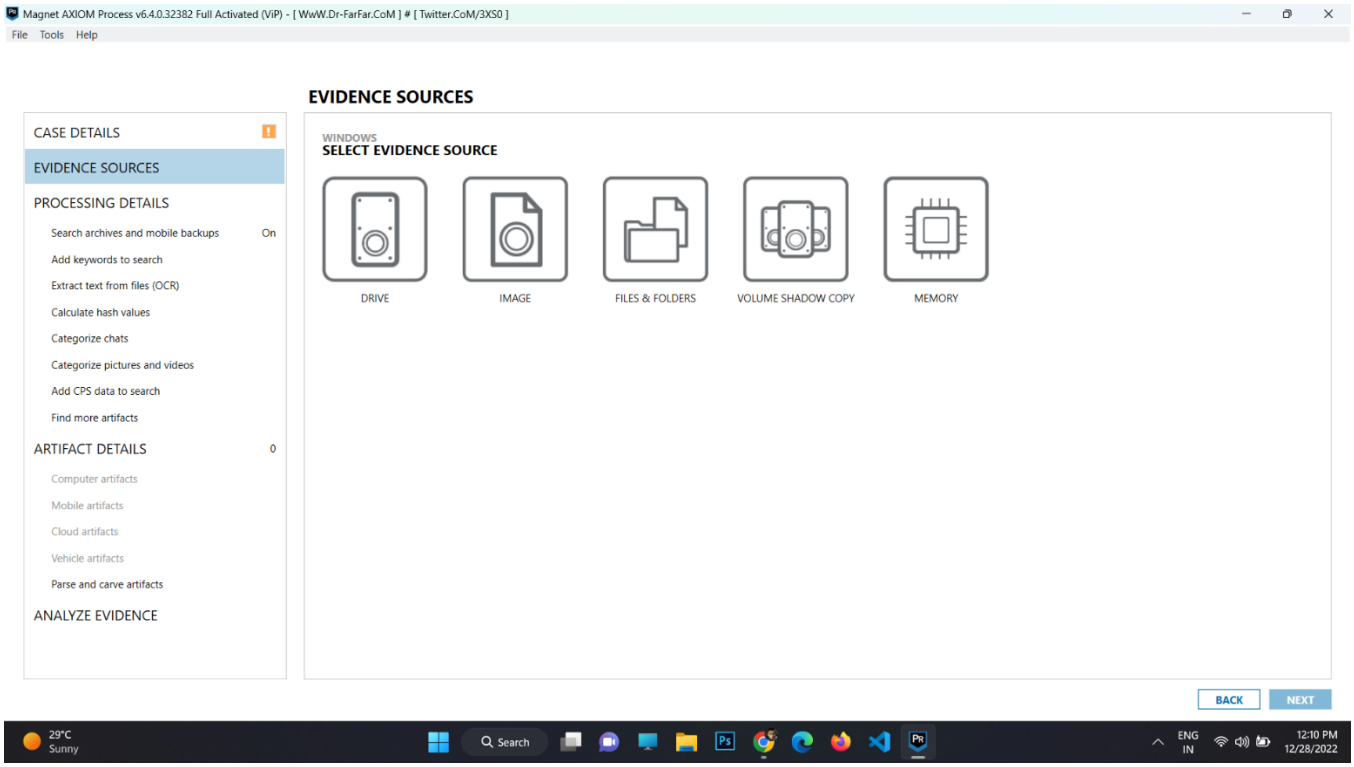


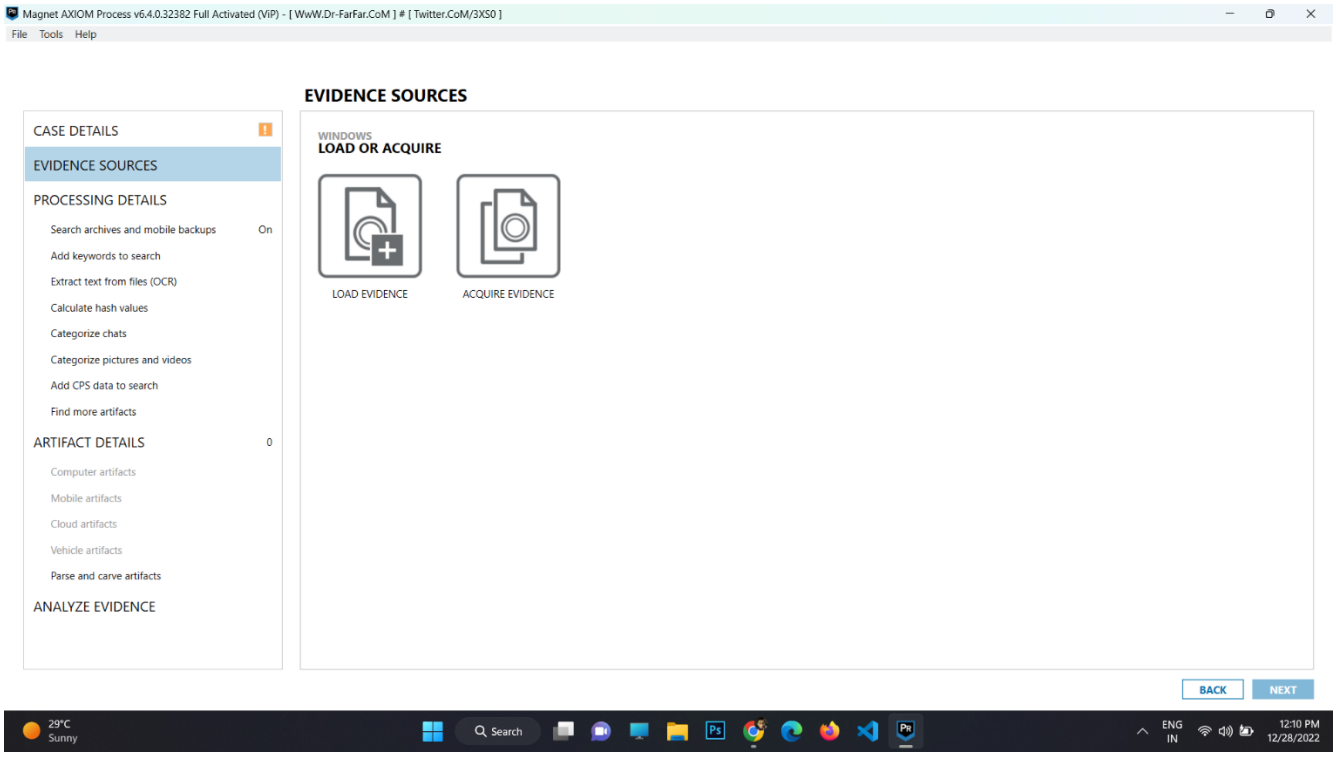
Step 5: Add evidence sources as per the given instruction on the screen

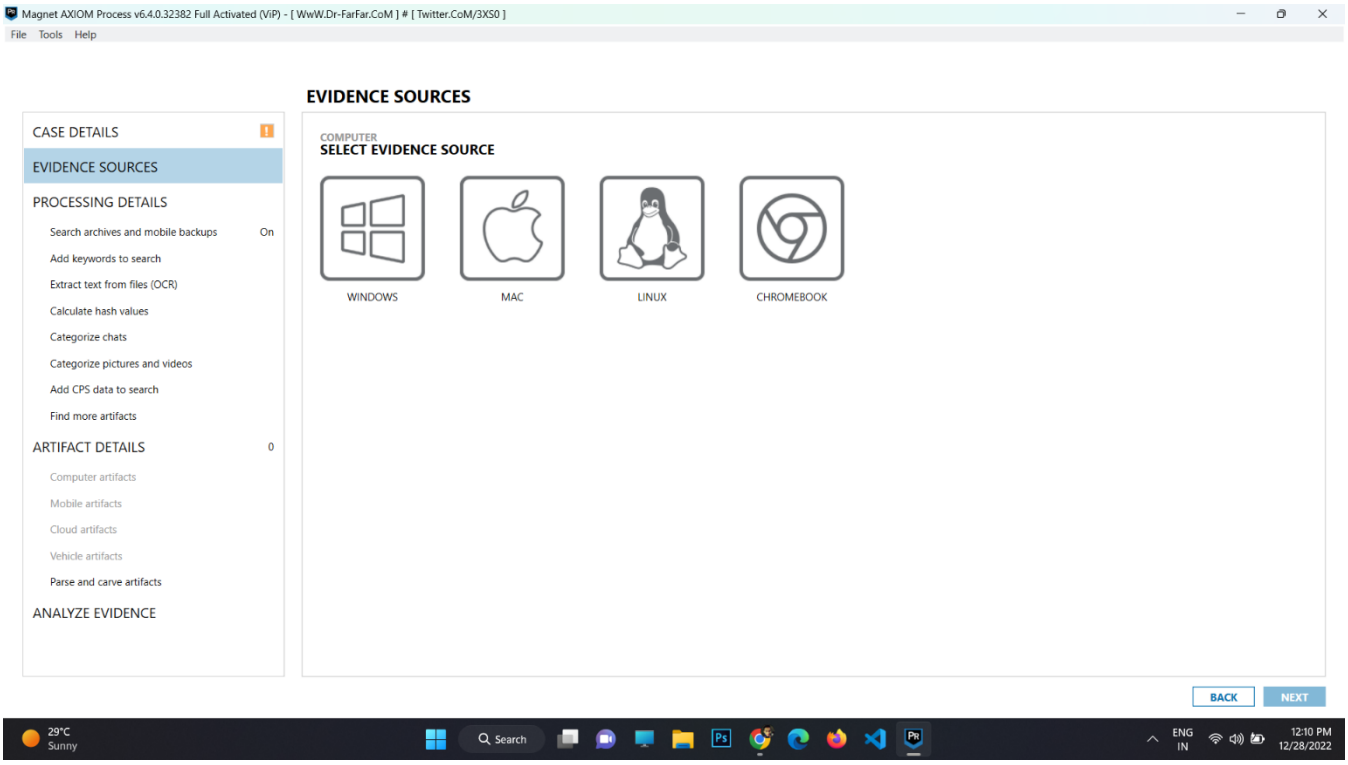


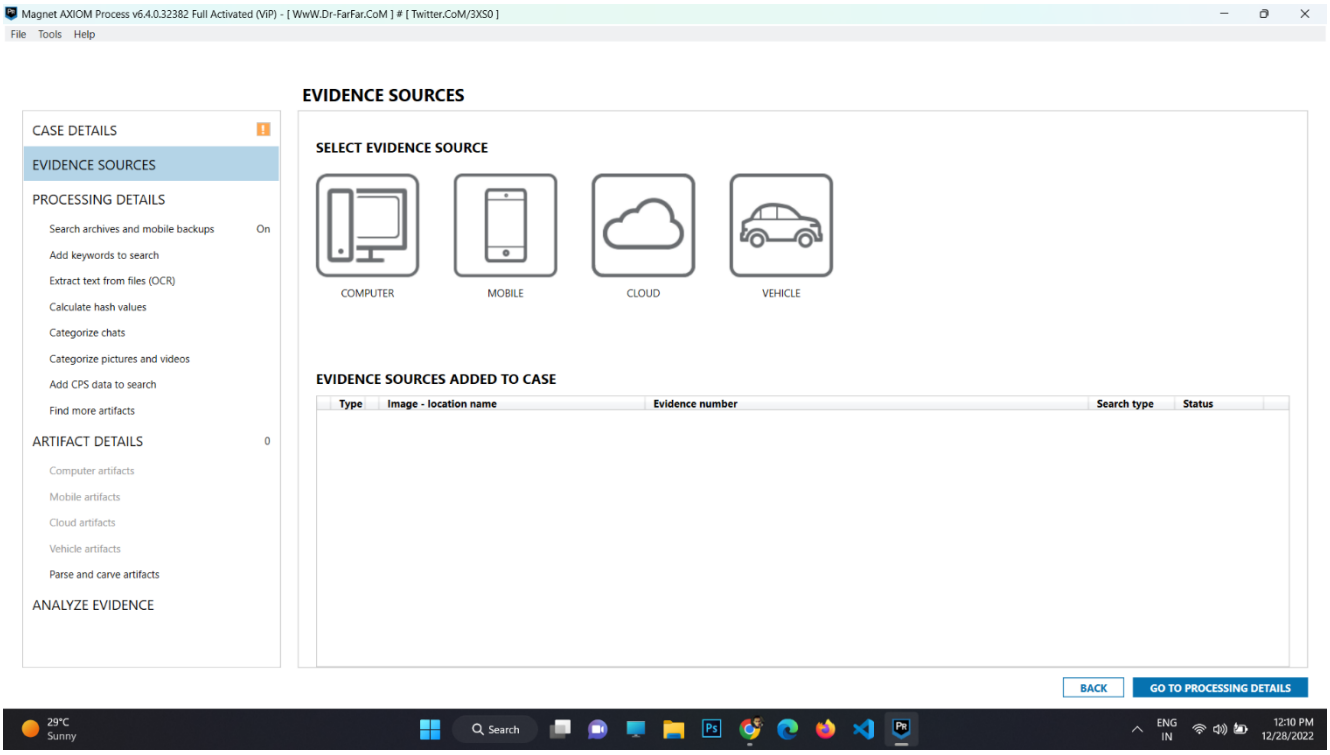

Magnet AXIOM Process v6.4.0.32382 Full Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0]
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES 2
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts
ARTIFACT DETAILS 201
Computer artifacts 201 of 251
Mobile artifacts
Cloud artifacts
Vehicle artifacts
Parse and carve artifacts
ANALYZE EVIDENCE
SELECT EVIDENCE SOURCE
COMPUTER
MOBILE
CLOUD
VEHICLE
EVIDENCE SOURCES ADDED TO CASE
Type
Image - location name
Evidence number
Search type
Status
PhysicalDrive0 ST1000LX015-1U7172 (931.51 GB) - PhysicalDrive0 ST1000LX015-1U7172 (931.51 GB) Full Ready
PhysicalDrive0 ST1000LX015-1U7172 (931.51 GB) - PhysicalDrive0 ST1000LX015-1U7172 (931.51 GB) Unpartitioned space Ready
BACK
GO TO PROCESSING DETAILS
29°C Sunny
Search
ENG IN
12:11 PM 12/28/2022


Magnet AXIOM Process v6.4.0.32382 Full Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0]
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
Vehicle artifacts
Parse and carve artifacts
ANALYZE EVIDENCE
WINDOWS
ADD DRIVES
SELECT ALL
PhysicalDrive1 HFM128GDJTNG-8310A (119.24 GB)
Partition 1 (Microsoft FAT32, 260 MB) SYSTEM
Partition 2 (16 MB)
Partition 3 (Microsoft NTFS, 118.19 GB) OS [C:\]
Partition 4 (Microsoft NTFS, 800 MB) RECOVERY
Unpartitioned space
PhysicalDrive0 ST1000LX015-1U7172 (931.51 GB)
Partition 1 (Microsoft NTFS, 931.51 GB) DATA [D:\]
Unpartitioned space
REFRESH
BACK
NEXT
29°C Sunny
Search
ENG IN
12:11 PM 12/28/2022

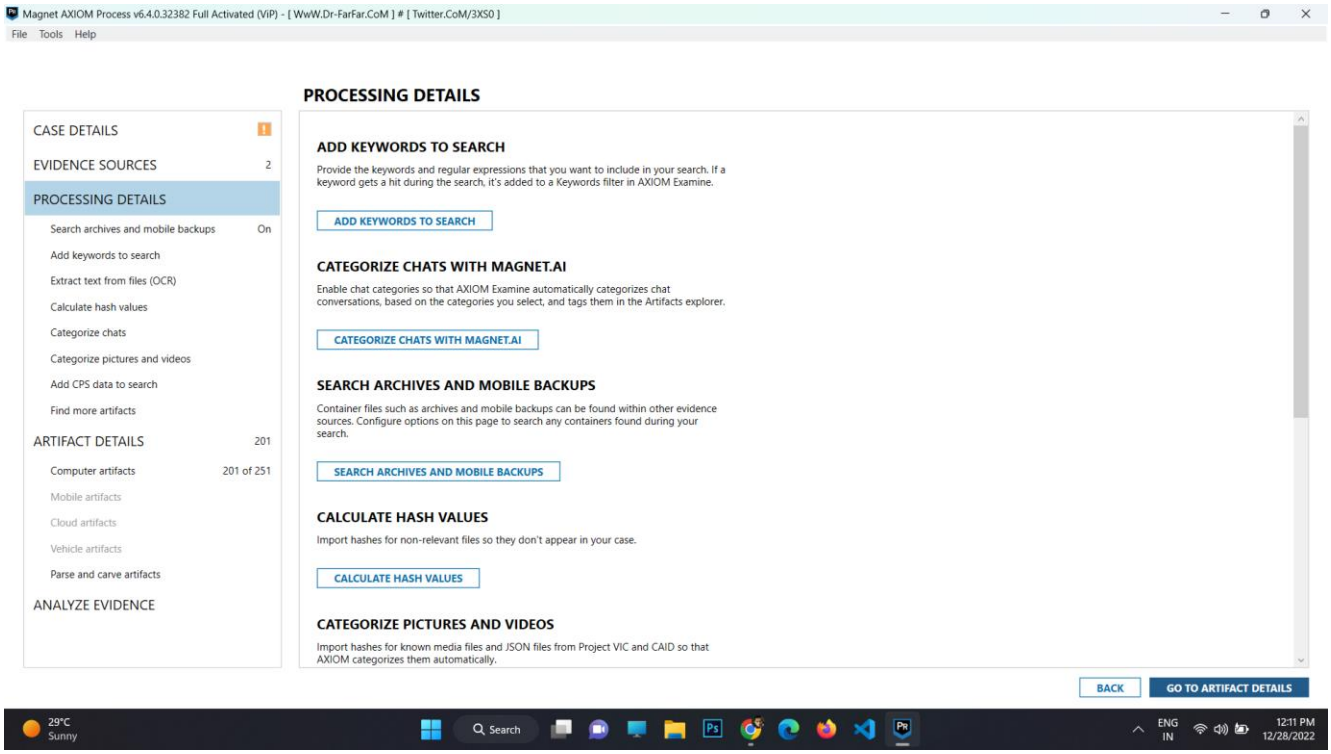

Magnet AXIOM Process v6.4.0.32382 Full Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0]
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
Vehicle artifacts
Parse and carve artifacts
ANALYZE EVIDENCE
WINDOWS
SELECT EVIDENCE SOURCE
DRIVE
IMAGE
FILES & FOLDERS
VOLUME SHADOW COPY
MEMORY
BACK
NEXT
29°C Sunny
Search
ENG IN
12:10 PM 12/28/2022


Magnet AXIOM Process v6.4.0.32382 Full Activated (ViP) - [WwW.Dr-FarFar.CoM] # [Twitter.CoM/3XS0]
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
Vehicle artifacts
Parse and carve artifacts
ANALYZE EVIDENCE
WINDOWS
LOAD OR ACQUIRE
LOAD EVIDENCE
ACQUIRE EVIDENCE
BACK
NEXT
29°C Sunny
Search
ENG IN
12:10 PM 12/28/2022

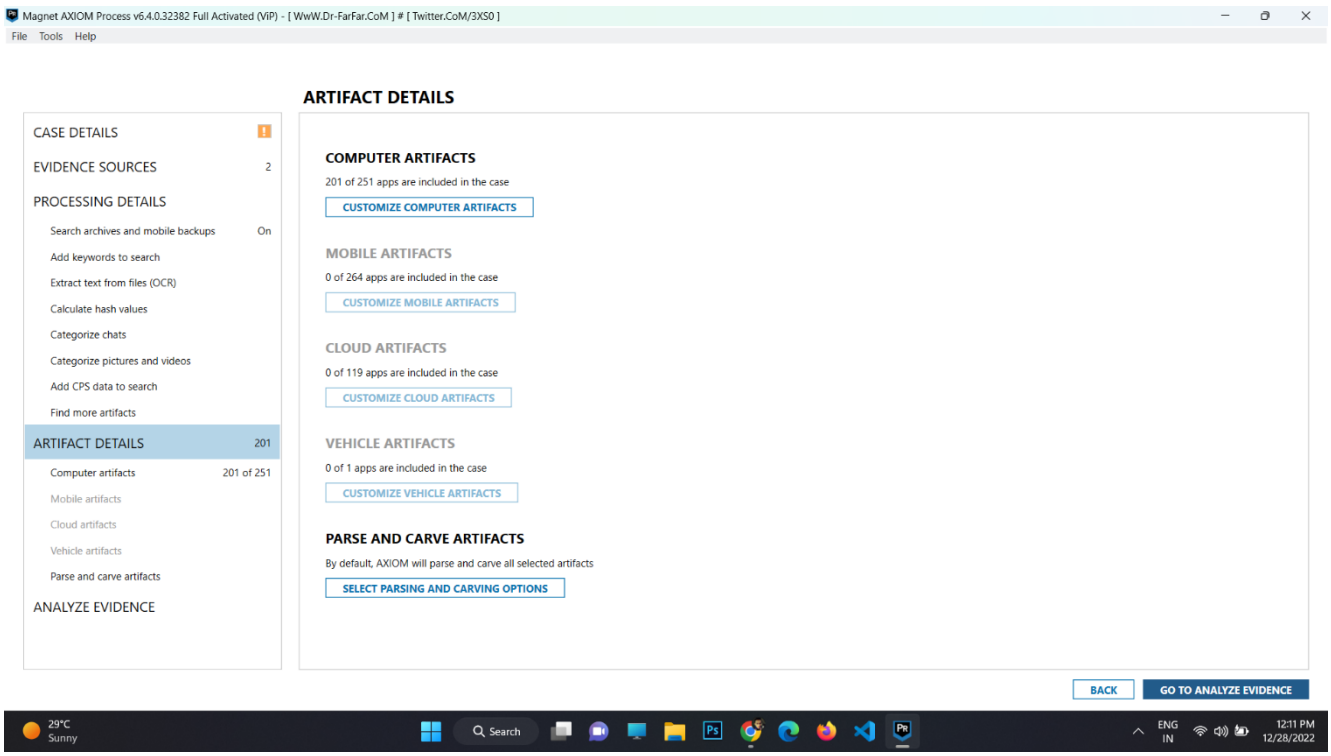




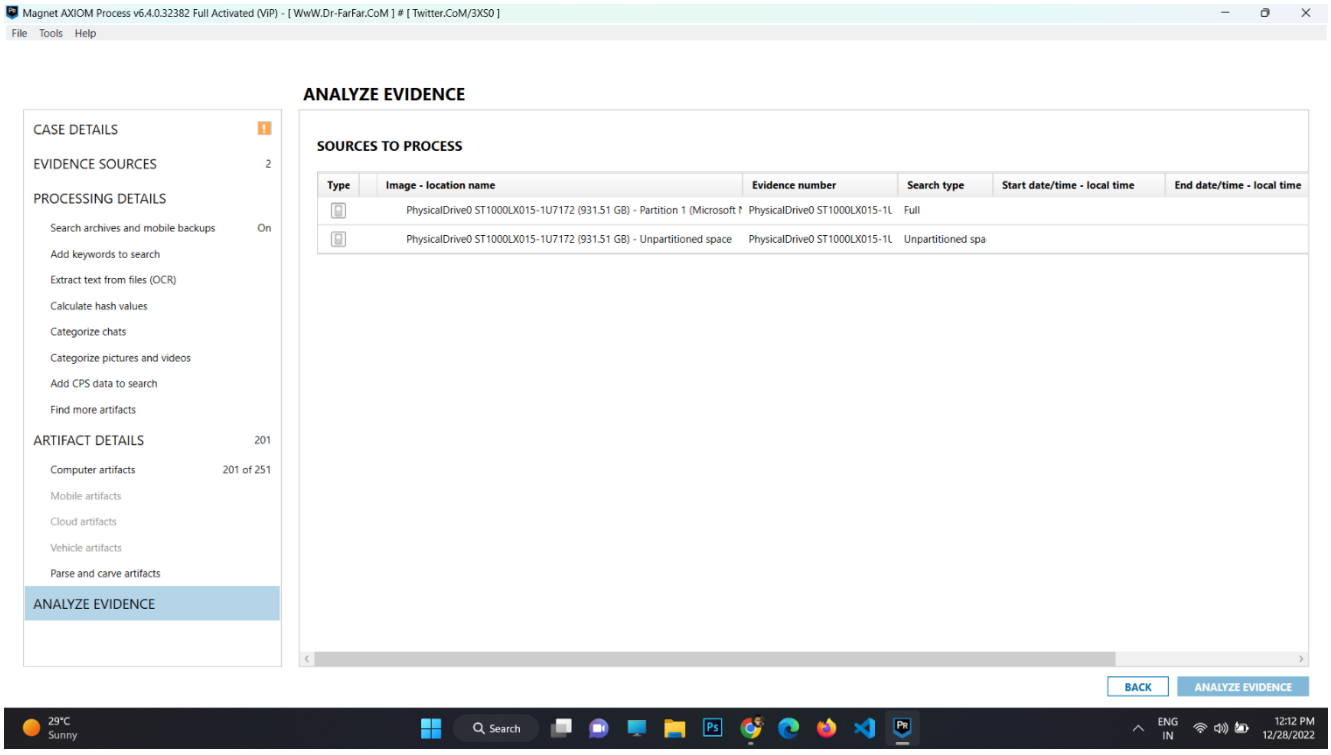
Step 6: Add Processing Details as per the given instruction on the screen



Step 7: Add Aircraft Details as per the given instruction on the screen



Step 8: Lastly click on Analyze Evidence



8. THUNDERBIRD (mail extraction)

Mozilla Thunderbird is a free and open-source cross-platform email client, personal information manager, news client, RSS, and chat client developed by the Mozilla Foundation and operated by subsidiary MZLA Technologies Corporation. The project strategy was originally modeled after that of Mozilla's Firefox web browser.

Features:

Thunderbird is an email, newsgroup, a news feed, and chat (XMPP/IRC) client with personal information manager (PIM) functionality, inbuilt since version 78.0 and previously available from the Lightning calendar extension. Additional features are available from extensions.

Message Management:

Thunderbird manages multiple emails, newsgroups, and news feed accounts and supports multiple identities within accounts. Features such as quick search, saved search folders ("virtual folders"), advanced message filtering, message grouping, and tags help manage and find messages. On Linux-based systems, system mail (move mail) accounts were supported until version 91.0. Thunderbird provides basic support for system-specific new email notifications and can be extended with advanced notification support using an add-on.

Extensions & Themes:

Extensions allow the addition of features through the installation of XPInstall modules (known as "XPI" or "zippy" installation) via the add-ons website that also features an update function to update the extensions.

Thunderbird supports a variety of themes for changing its overall look and feel. These packages of CSS and image files can be downloaded via the add-ons website at Mozilla Add-ons.

Supported File Format:

Thunderbird provides mailbox format support using plugins, but this feature is not yet enabled due to related work in progress.[16] The mailbox formats supported as of July 2014 are:

- mbox – Unix mailbox format (one file holding many emails)
- maildir – known as Maildir-lite (one file per email). As of August 2019 "there are still many bugs", so this is disabled by default.

Thunderbird also uses Mork and (since version 3) MozStorage (which is based on SQLite) for its internal database. Mork was due to be replaced with MozStorage in Thunderbird 3.0, but the 8.0 release still uses the Mork file format.

Limitations:

As with any software, there may be limitations to the number and sizes of files and objects represented. For example, POP3 folders are subject to filesystem design limitations, such as maximum file sizes on filesystems that do not have large-file support, as well as possible limitations of long filenames, and other issues.

Security:

Thunderbird provides security features such as TLS/SSL connections to IMAP and SMTP servers. It also offers inbuilt support for a secure email with digital signing and message encryption through OpenPGP (using public and private keys) or S/MIME (using certificates). Any of these security features can take advantage of smartcards with the installation of additional extensions.

Other security features may be added through extensions. Up to version 68, the Enigmail extension was required for OpenPGP support (now inbuilt).

Optional security protections also include disabling the loading of remote images within messages, enabling only specific media types (sanitizer), and disabling JavaScript.

The French military uses Thunderbird and contributes to its security features, which are claimed to match the requirements for NATO's closed messaging system.

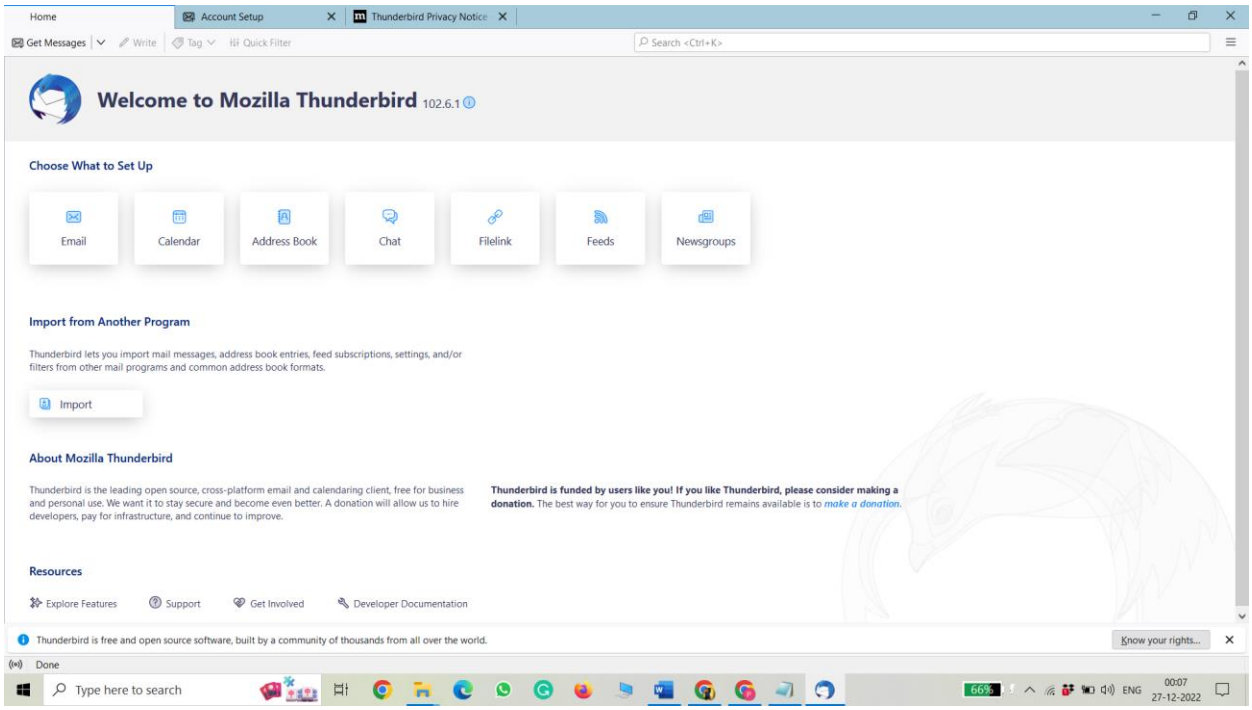
Advantages:

- User can open multiple tabs for navigation
- Fast and simple email archive by clicking the "A" button.
- Users can use several extensions with intended usability
- Mozilla Thunderbird is very reliable and got a huge number of plugins
- Consistent in design yet got greater flexibility

Disadvantages:

- No calendar and task list are available (users can add them separately
- Though focusing on stability and security modernization is at a slow pace
- Temporarily subject can disappear

Home Page of Thunderbird Application:



9. IMAZING (IOS WhatsApp)

iMazing is a mobile device management software that allows users to transfer files and data between iOS devices(iPhone, iPad,
and iPodTouch)and macOS or Windows computers, in addition to many other features beyond the scope of what Apple's tools enable.

Description:

With iMazing, an iPhone or iPad can be used similarly to an external hard drive. It performs tasks that iTunes doesn't offer, including incremental backups of iOS devices, browsing and exporting text and voicemail messages, managing apps, encryption, and migrating data from an old phone to a new one.

The menu bar app iMazing Mini enables automatic, wireless, and encrypted backups of iPhones. The iMazing HEIC Converter is a free desktop app for Mac and PC that lets users convert photos from HEIC format to JPG or PNG.

Getting Started with iMazing:

With thousands of stellar reviews from long-term users, iMazing has become a dependable data-device management tool for all Apple devices. The features it provides are something of a rarity in the ecosystem, succeeding even the limitations of Apple's very own iTunes app, and makes the process simple with straightforward instructions. The user experience is as narrowed down as it gets, with everything easily accessible. It gives the power users a robust settings window to do all of their tinkering with ease. The installation process is simple and can be done in under five minutes with the following steps:

Step 1: Head on to the iMazing website found here and continue the downloading process.

Step 2: Download the software, and don't worry about the device as the website automatically detects what OS you're using.

Step 3: Install or run the downloaded file and continue by clicking next.

Step 4: Complete the installation process by following the directions the installer provides.

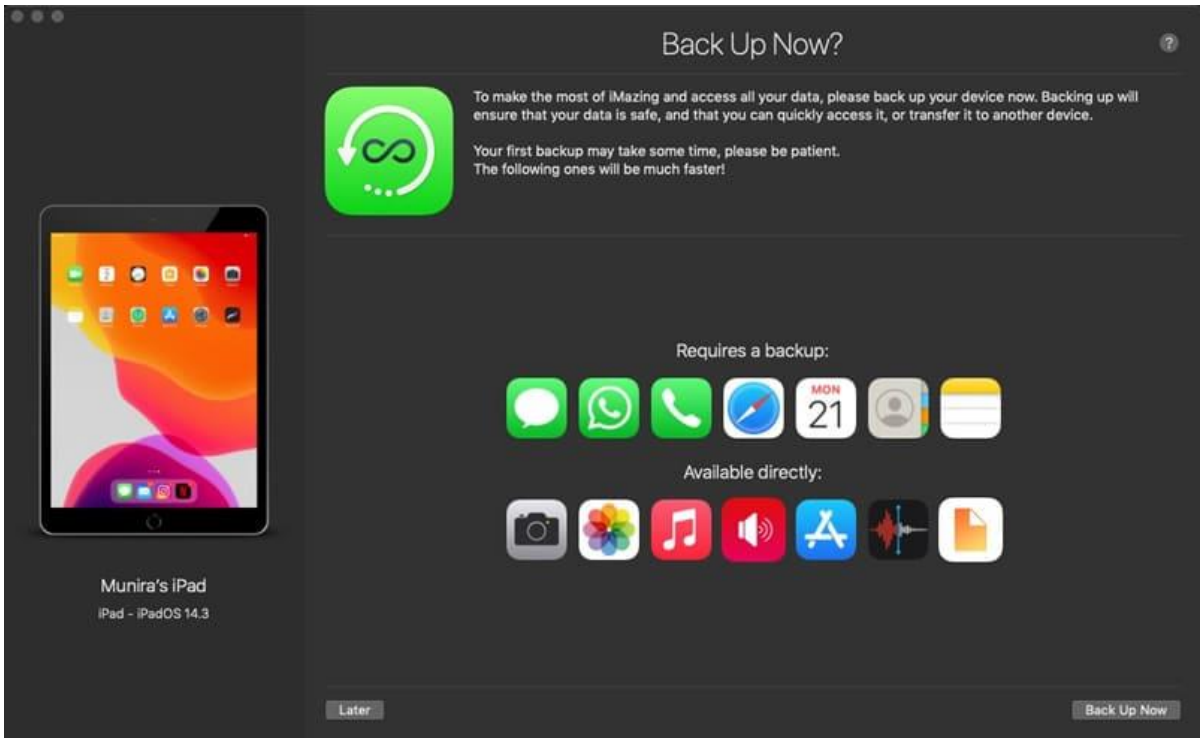
Step 5: After the installation process is completed, run the software and enjoy all its benefits and features with ease.

Note: iMazing provides some features that are free of cost, but for a full experience and all the exclusive features, you will need to get an activation key or license by buying the software.

With the installation steps covered, let’s get to the breakdown and what we think of iMazing as an iOS management tool.

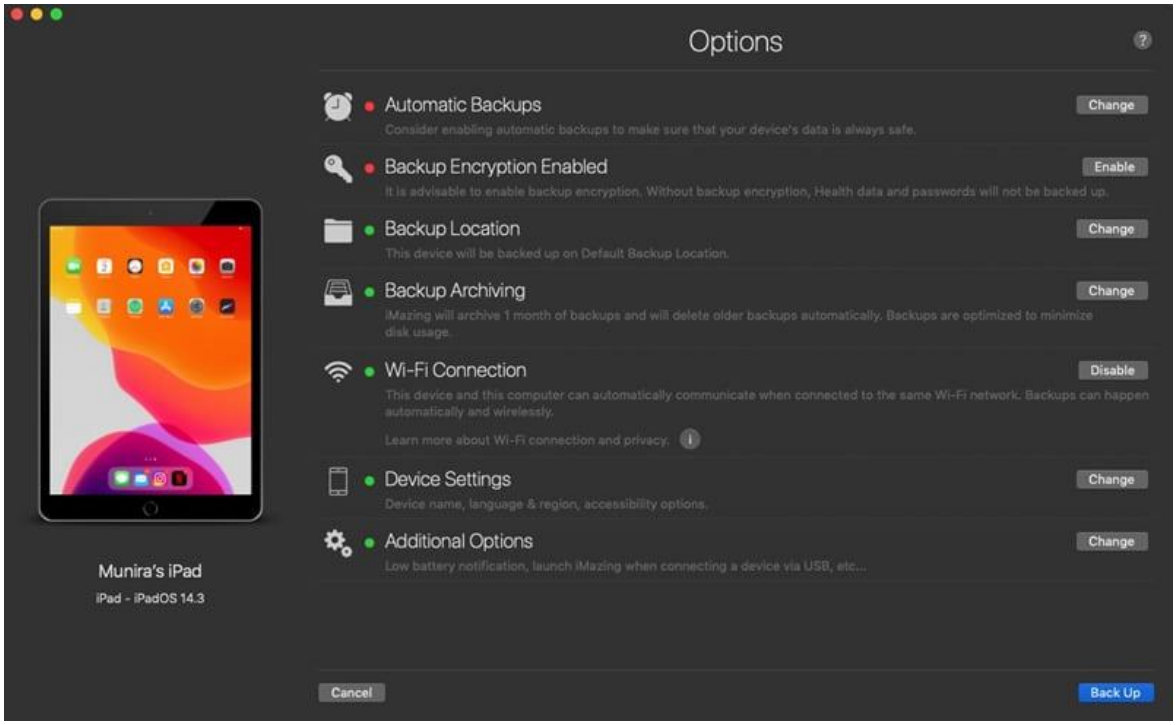
Data transfer and backups – all locked down:

With the newer iPhones, the brittle glass body makes a significant difference in durability, it is no wonder that most damages occur to the back, and a simple drop can ruin your device. So, being cautious and careful would be the primary choice, and using backups to your advantage is the crucial aspect you should be looking into.

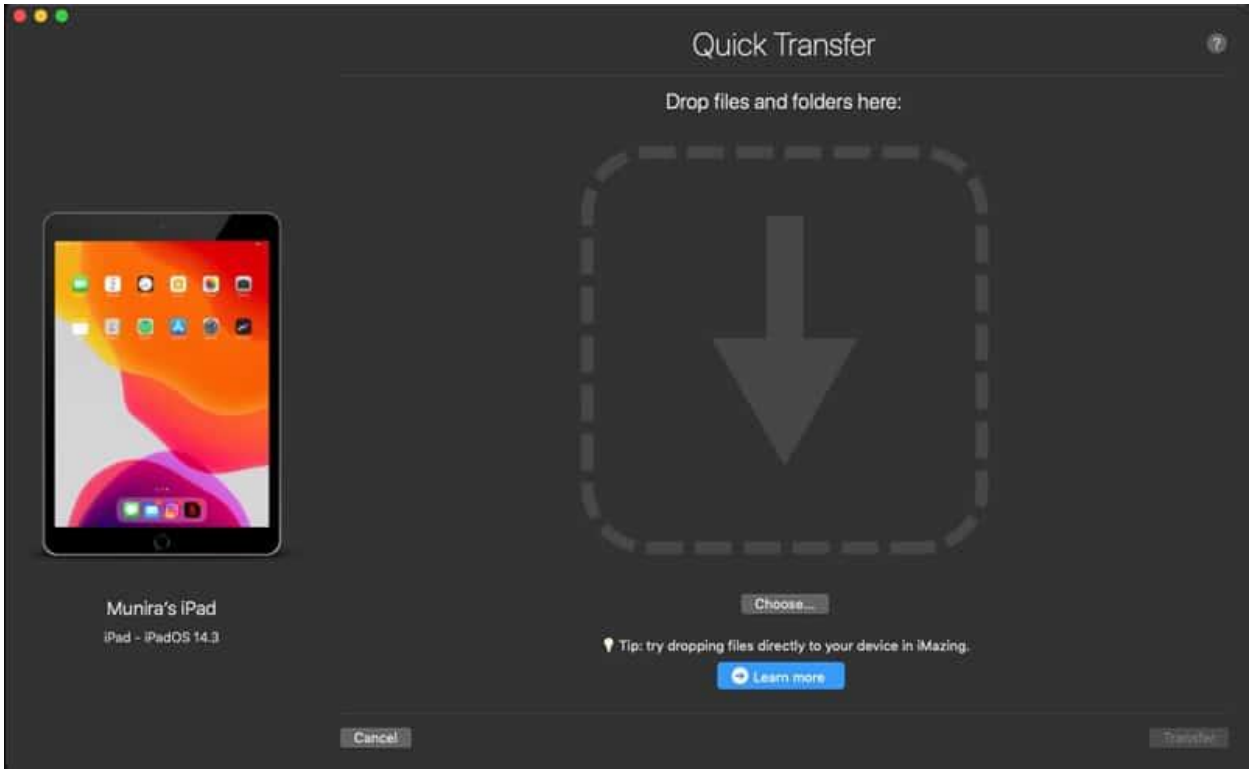


The same as iTunes, the backup feature will always be handy, and it proved to us the same. The backups we did were clean and fast with easy restoration ability, and they also provide a function that allows us to do incremental backups saving time and resources.

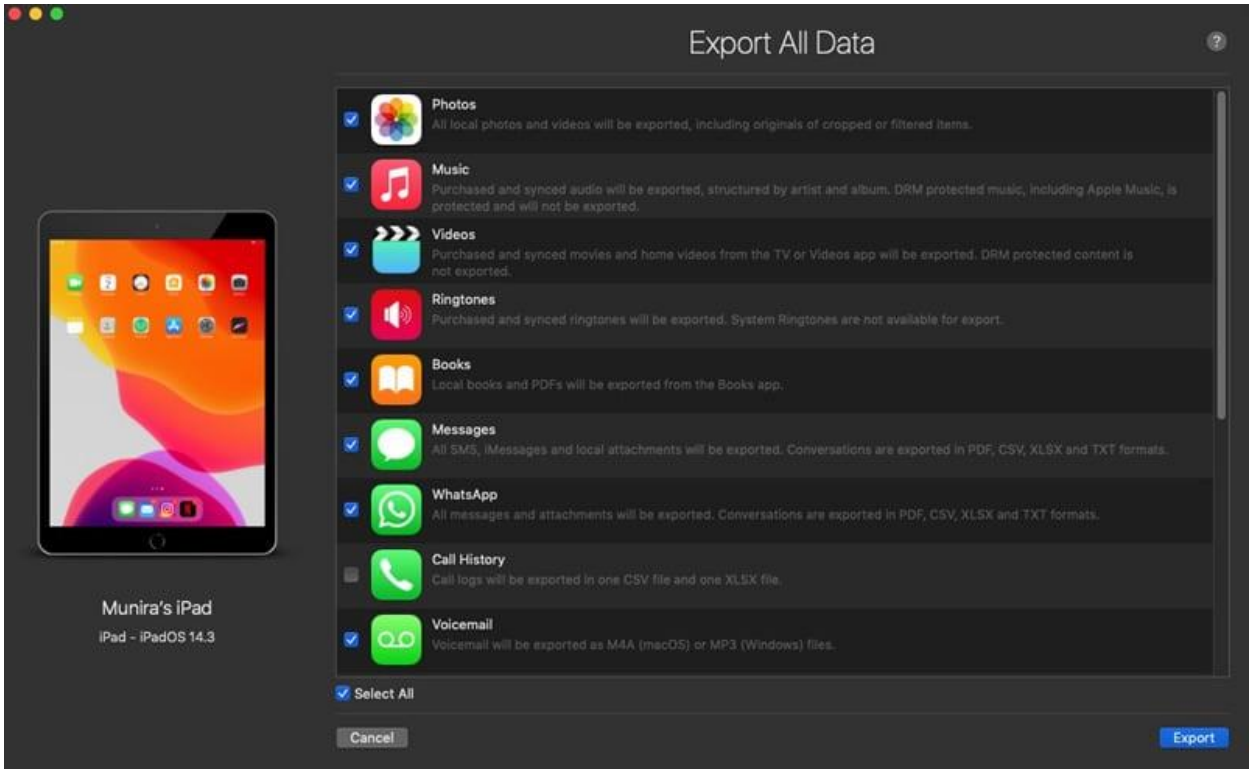
A winning feature of iMazing, in our opinion, was the ability to create Automatic Backups, which eliminates the need for the premium backup solution of Apple iCloud. Unlike iCloud which limits your ability to backup content and the amount of data you can backup, iMazing takes it a step further with the Wi-Fi Connection feature, which untethers your iPhone or iPad from the Mac and allows you to keep your contacts, messages, WhatsApp chats, music, and everything else backed up safely.



When it comes down to the Data Transfer ability, iMazing does not hold back, with a slew of features to not only transfer files between the macOS computer and the iDevice but across multiple devices. All you need to do is hit the Quick Transfer button to drag and drop files directly into the iPhone or iPad.



Additionally, the option to Transfer to another device enables you to swap content such as media photos videos, messages, contacts, calendar entries, and so much more. If you ever needed to just move the data out of your iPad and Export All Data to the computer, iMazing allows you to do so with just a click. However, unlike iTunes which bundles everything together into an encrypted backup file, iMazing lets you handpick elements such as Photos, Videos, Books, Call History, Voicemail, and so much more.



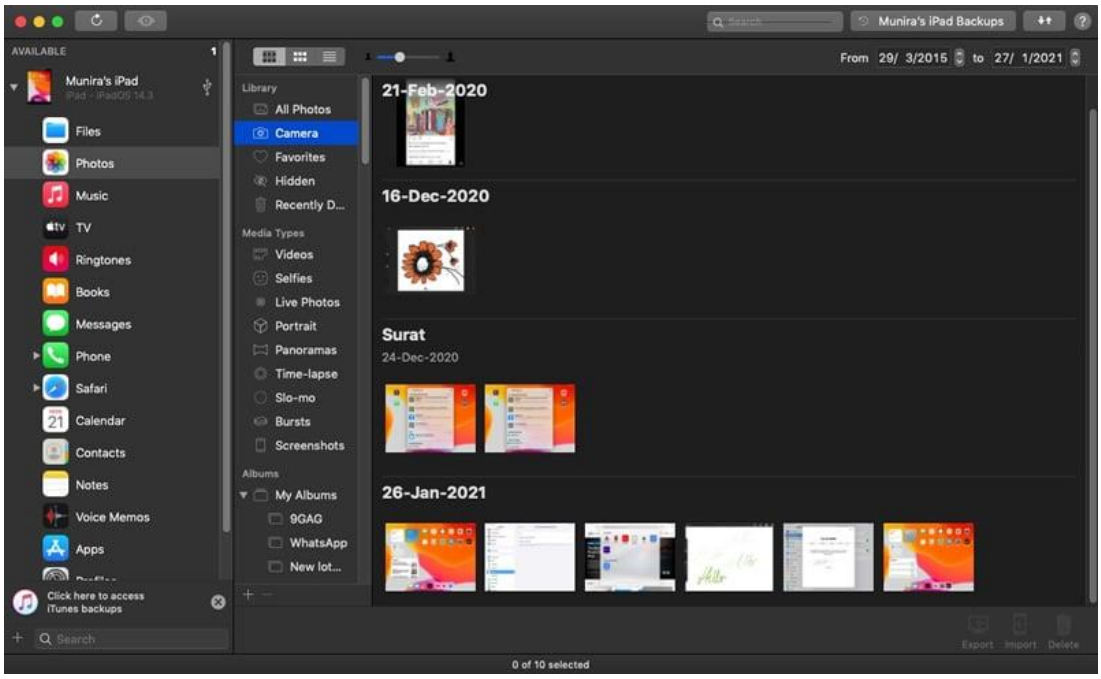
The transfers work as they are supposed to. It was seamless and quick, and the data transfers to the desktop or other iPhone and Android devices worked the same without any hiccups.

iMazing photos – for the pros:

I was very impressed with the amazing Photos. At first glance, it seemed to be another generic photo management tool that worked well, but with a more significant inspection, we realized that, and mind the pun, there was a bigger picture to look forward to.

The “iMazing Photos” feature brought a lot to the table with ease-of-life features that people like you and me will appreciate. We all have been in a situation where we want to clean our gallery, but the amount and bulk of unwanted photos may be a disaster to look at, and it was the same with me. However, the batch deletion worked a charm in getting unwanted images deleted with a single click that, trust me, saves a lot of time.

However, this is not the end, and with the ability to convert photos and manage the new ProRAW images, the entire section could be a fantastic app in itself.



The conversion feature allows you to save a ton of time and storage capacity when transferring thousands of high-resolution photos. Converting the images to lighter formats such as “.jpeg or .png” could lead to a faster transfer rate and more significant storage space.

As with ProRAW, as Apple states, it is a new file format for better and higher detailed RAW images that provide a tonne of data for further editing, and a tool that helps manage this file format becomes a gold choice in any design. This won’t be of any use to you if you don’t shoot in RAW and would only benefit the enthusiasts.

Device management – managing iOS straight from the desktop:

The iOS management feature didn't bring anything new, and the same can be done using iTunes. Still, the fact that it's present and works flawlessly with any update checks and re-installation will remain a boon to the users of iMazing. This is not something we base our review on entirely but is still a great feature to have, and well, the more you get for your money, the better.

Another niche and undervalued option that most people glance over. But my technical mind and curious side got the better of me, and if you're anything the same, the detailed

device information the software provides can help you learn a lot from the performance of the CPU to the health of your iPhone's battery.

Pros of iMazing:

- Easy and Reliable to use
- Provides features such as back-ups and restoration
- Can export app data and files
- It is an excellent replacement to iTunes as it excels in all fields and also delivers exclusive functions that iTunes doesn't have
- Can help to update and re-installing iOS with just a tap
- It doesn't require iTunes to work

Cons of iMazing:

- It has a cost and isn't completely free to use.

10.ITUNES

iTunes is a software program that acts as a media player, media library, mobile device management utility, and client app for the iTunes Store. Developed by Apple Inc., it is used to purchase, play, download, and organize digital multimedia, on personal computers running the macOS and Windows operating systems, and can be used to rip songs from CDs, as well as play content with the use of dynamic, smart playlists. Options for sound optimizations exist, as well as ways to wirelessly share the iTunes library.

Originally announced by Apple CEO Steve Jobs on January 9, 2001, iTunes' original and main focus was music, with a library offering organization and storage of Mac users' music collections. With the 2003 addition of the iTunes Store for purchasing and downloading digital music and a version of the program for Windows, it became a ubiquitous tool for managing music and configuring other features on Apple's line of iPod media players, which extended to the iPhone and iPad upon their introduction. Starting in 2005, Apple expanded on the core music features of iTunes with support for digital video, podcasts, e-books, and mobile apps purchased from the iOS App Store. Since the release of iOS 5 in 2011, these devices have become less dependent on iTunes, though they can still be used to back up their content.

Though well received in its early years, iTunes received increasing criticism for a bloated user experience, which incorporated features beyond its original focus on music. Beginning with Macs running macOS Catalina, iTunes was replaced by separate apps, namely Music, Podcasts, and TV, with Finder taking over the device management capabilities. (This change would not affect iTunes running on Windows or older macOS versions).

Sound Processing:

iTunes includes sound processing features, such as equalization, "sound enhancement" and crossfade. There is also a feature called Sound Check, which normalizes the playback volume of all songs in the library to the same level.

Advantages:

1) **Good Integration with iOS Devices**
   iTunes is also one of the best software platforms integrated with iOS devices in the marketplace. Though various third-party programs can upload audio recordings to iPhones, iPod Touches, and iPads, iTunes is the only program that can handle coordinating operating system upgrades while managing apps at the same time, making it a fast option when employees need to use it daily to exchange company-related media.

2) **Access to Business Content**
   iTunes also has a range of content that can be useful to employees for improved performance. Installing iTunes gives them access to a broad range of business podcasts, as well as business classes through the iTunes U education app and business books and audiobooks through the iTunes bookstore. Used properly, iTunes can be a gateway to information that makes your team more productive.

Disadvantages:

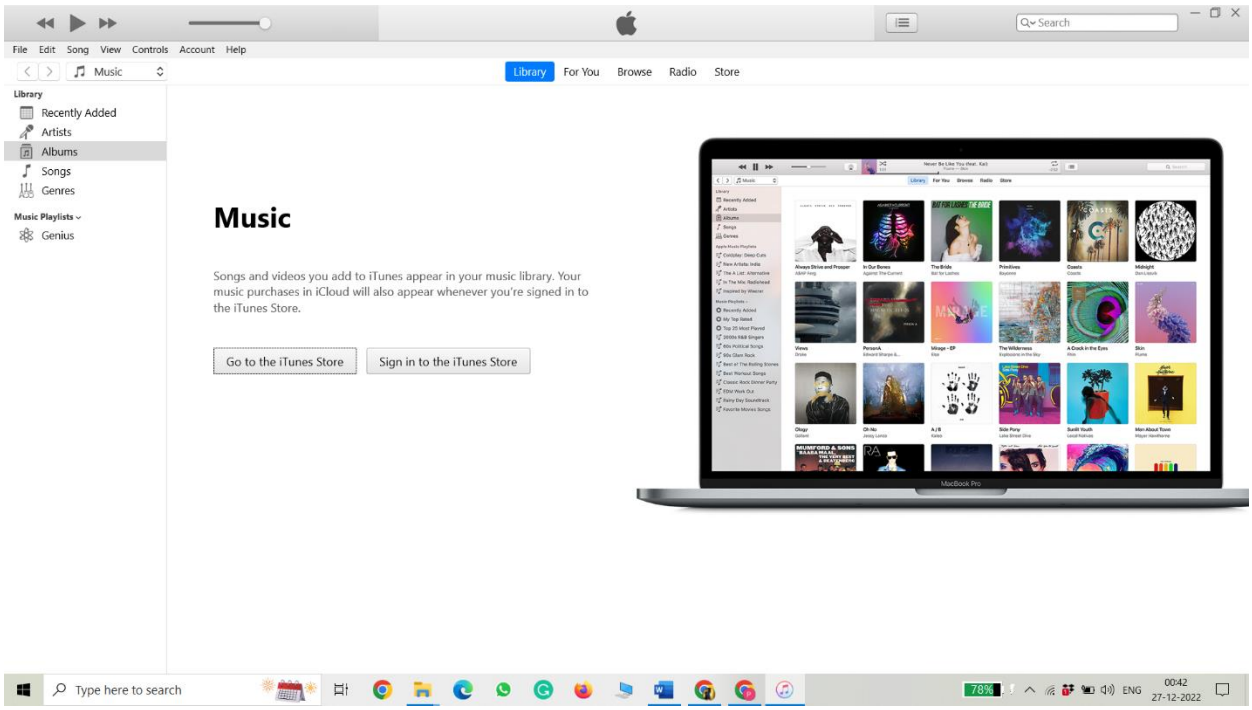
1) **Performance**
   One of the biggest problems with iTunes is its known reputation for running slowly on many computers, particularly on Windows software and consuming a great deal of system RAM. While there are some workarounds for some of its performance issues, iTunes still slows down your system and takes away from performance in other applications. This may be particularly problematic for businesses that upgrade their hardware infrequently and use slower computers with less memory.

2) **Non-Business Purpose**
   iTunes is overall a media manager, which means it can potentially lead to computers in the workplace having the ability to store inappropriate material. While non-business use of iTunes by employees might generally consist of their storage of legitimate, purchased media on their systems, it might also lead to their storage of illegally downloaded material. Additionally, non-business storage of music or video material will consume disk space and slow down a computer's ability to handle work transactions.

Security:

The Telegraph reported in November 2011 that Apple had been aware of a security vulnerability since 2008 that would let unauthorized third parties install "updates" to users' iTunes software. Apple fixed the issue before the Telegraph's report and told the media that "The security and privacy of our users are extremely important", though this was questioned by security researcher Brian Krebs, who told the publication that "A prominent security researcher warned Apple about this dangerous vulnerability in mid-2008, yet the company waited more than 1,200 days to fix the flaw."

iTunes welcome page:



Back up your iPhone, iPad, or iPod touch in iTunes on a PC

Backing up *means copying certain files and settings from your iPhone, iPad, or iPod touch to your computer. Backing up is one of the best ways to make sure you don't lose the information on your device if it's damaged or misplaced. It's also useful to have a backup if you get a new device and want to transfer your previous settings to it.*

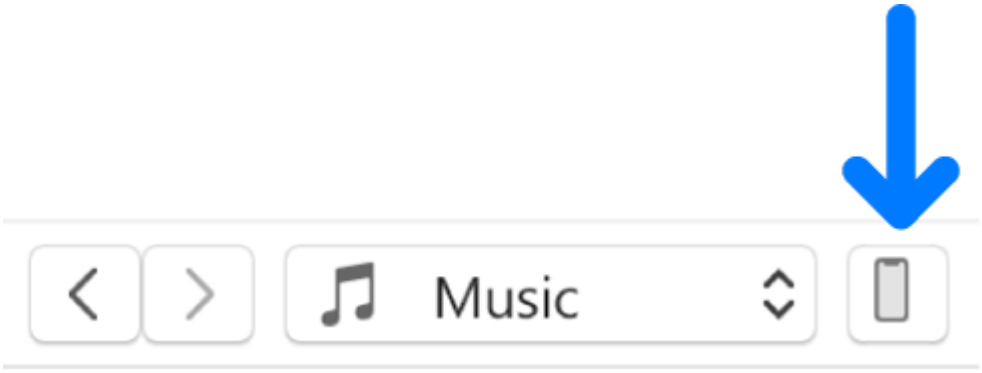
1) Back up your device

iTunes automatically backs up your device when you connect it to your computer. But you can also back up your device manually at any time. And if you have iOS 3.0 or later, iTunes can encrypt your backups to secure your data.

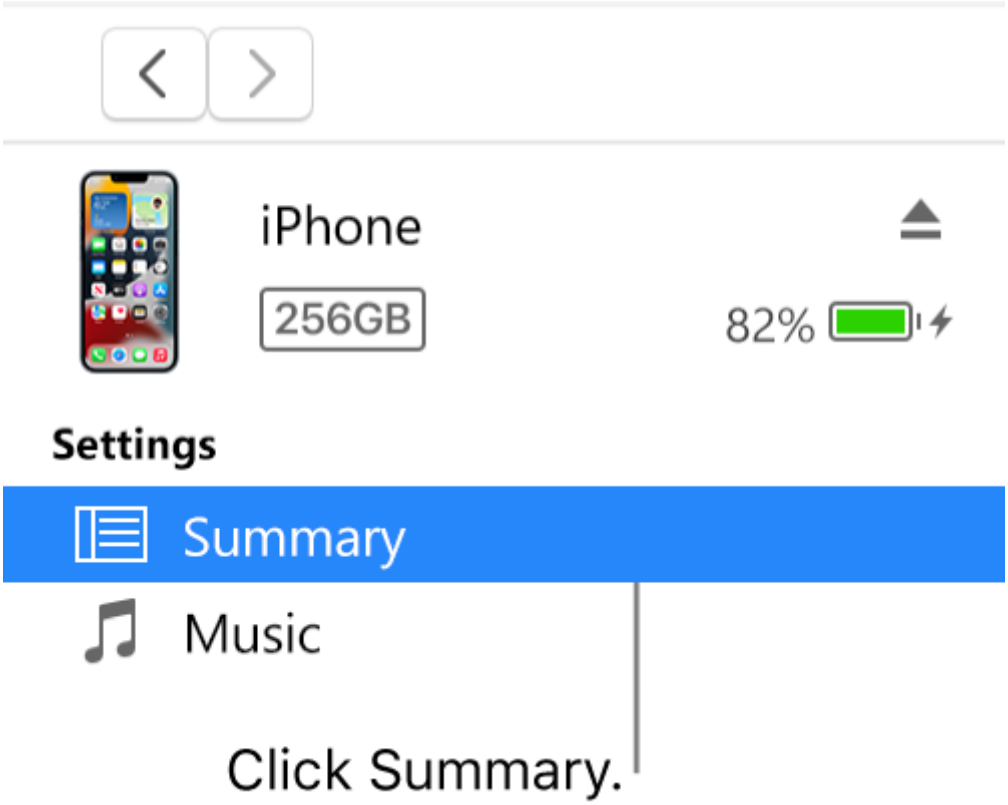
1) Connect your device to the computer you normally sync with.

You can connect your device using a USB or USB-C cable or a Wi-Fi connection. To turn on Wi-Fi syncing, see Sync iTunes content on PC with devices on Wi-Fi.

2) In the iTunes app on your PC, click the Device button near the top left of the iTunes window.



3) Click Summary.



4) Click Back Up Now (below Backups).

To encrypt your backups, select “Encrypt [*device*] backup”, type a password, then click Set Password.

To see the backups stored on your computer, choose Edit > Preferences, then click Devices. Encrypted backups have a lock icon in the list of backups.

11. CHAT BACK (Whatsapp Backup)

Retrieve WhatsApp Data to iOS/Android Devices or PC without overwriting.

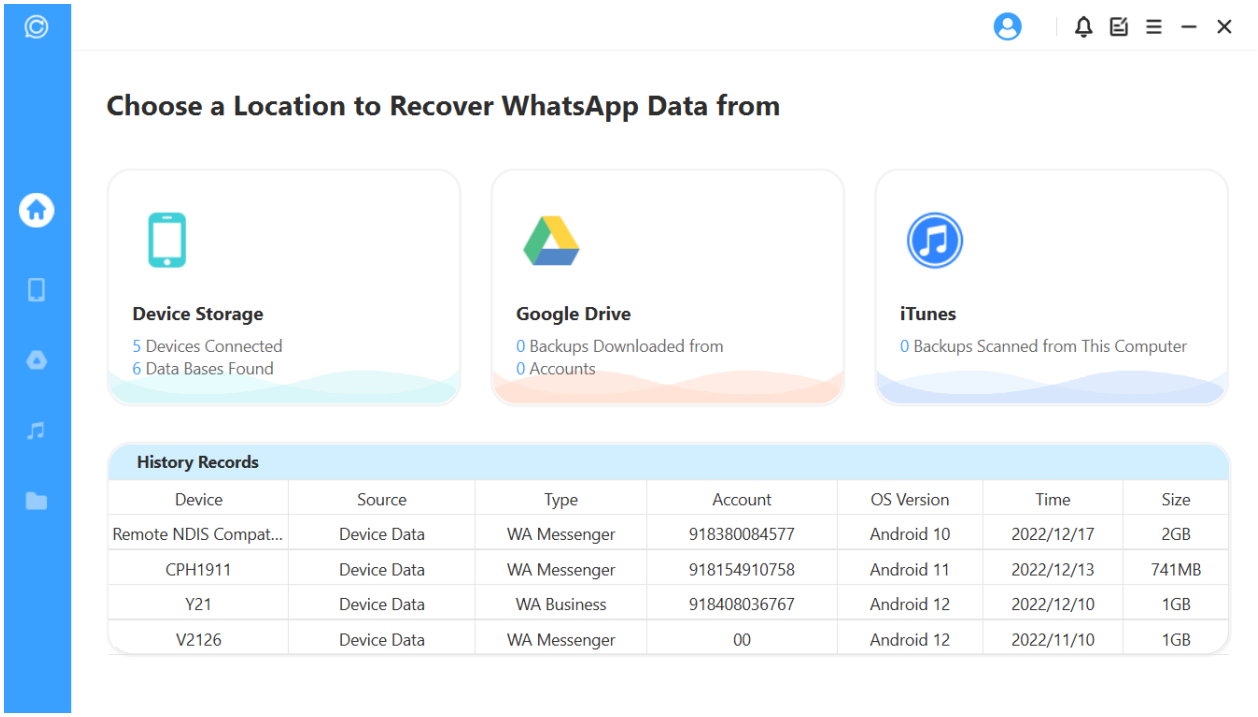
- Transfer WhatsApp from Android to iPhone without overwriting iPhone data.
- Transfer WhatsApp from iPhone to Android.
- Back up WhatsApp on Android and iPhone to a computer for free.
- Restore WhatsApp backup from Google Drive to iPhone.
- Export WhatsApp backup to HTML, PDF, and CSV/XLS.
- Transfer Data between WhatsApp and GB WhatsApp.

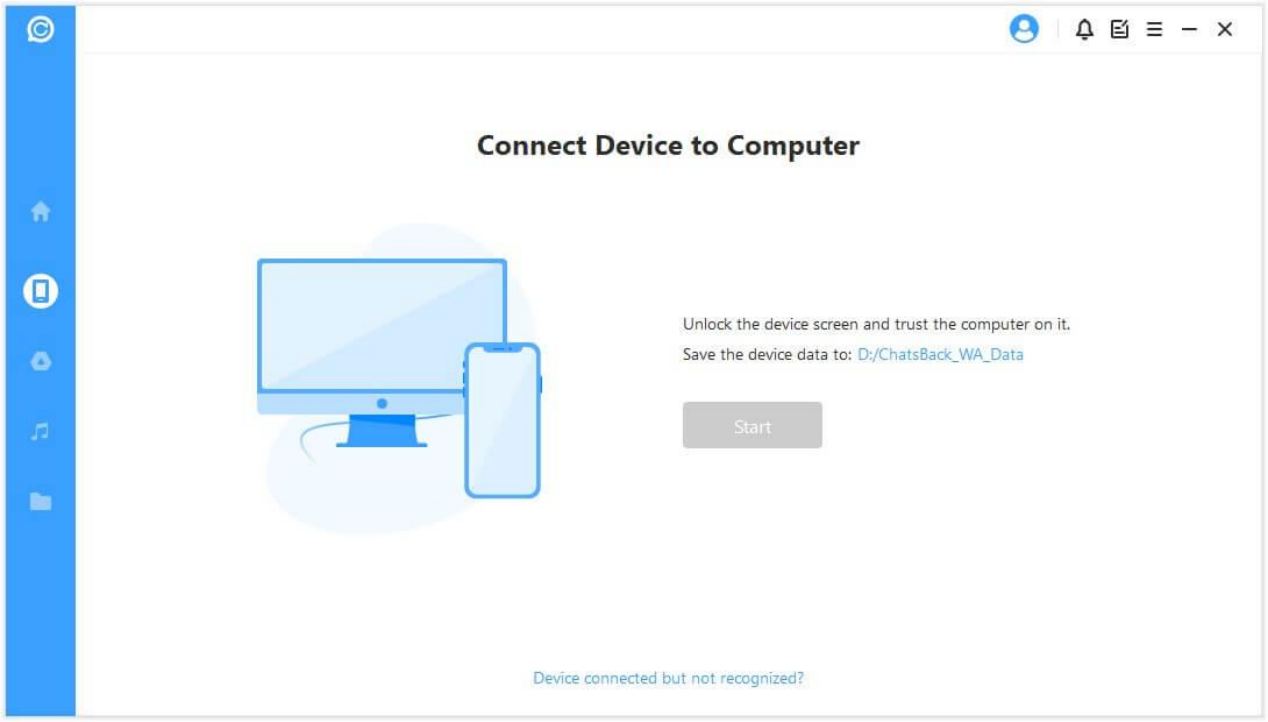
1) Full coverage of WhatsApp data types, including chats, photos, contacts, etc. Just feel free to recover iOS/Android device WhatsApp data to any OS phone.

2) Retrieve and download lost WhatsApp data to PC as HTML/PDF/Excel/CSV files for further use like reading or printing.

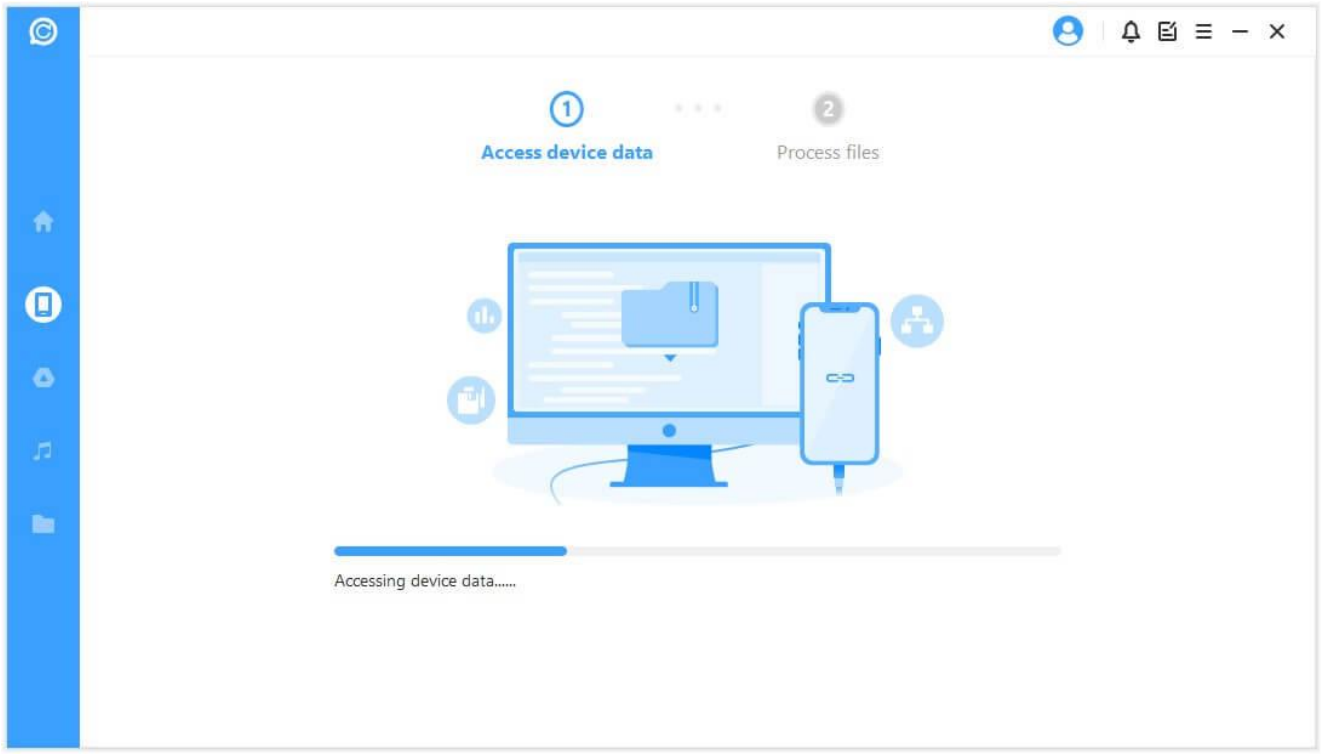
From Device Storage:

1) Step 1: Connect the phone and then after detecting the device click on the start option

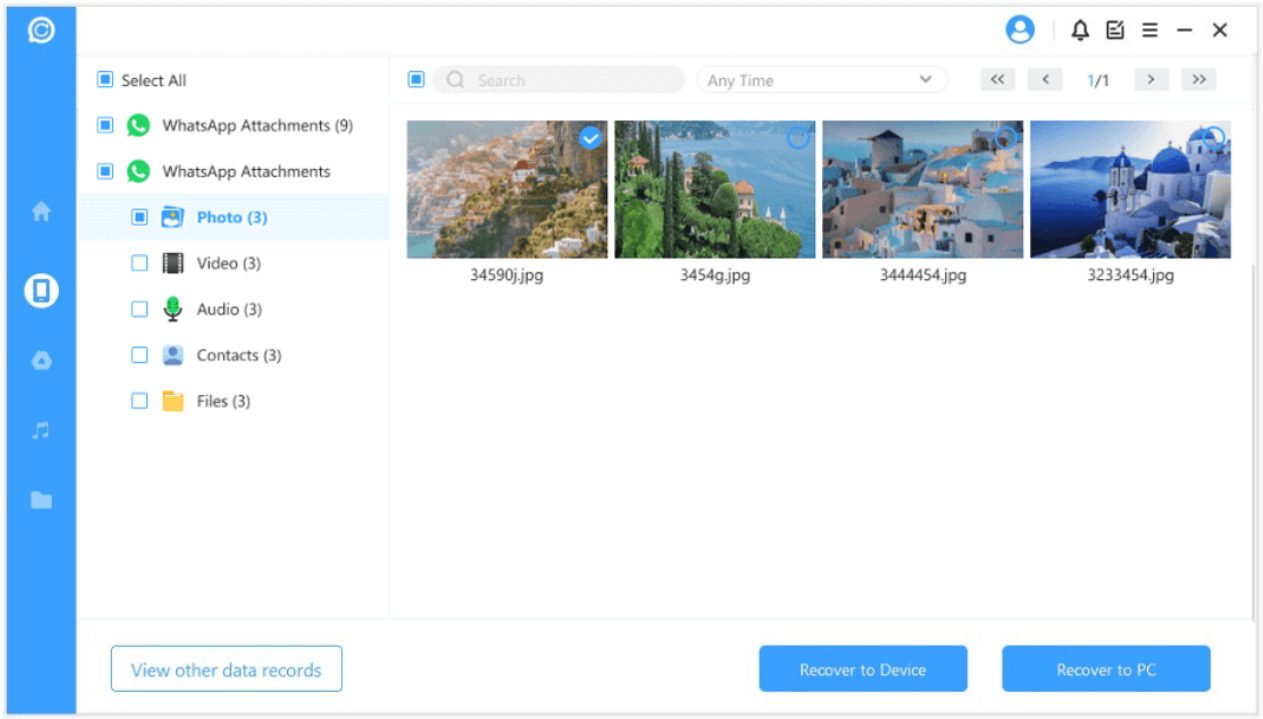




2) Step 2: After clicking on the start button it will access device data for further processes.

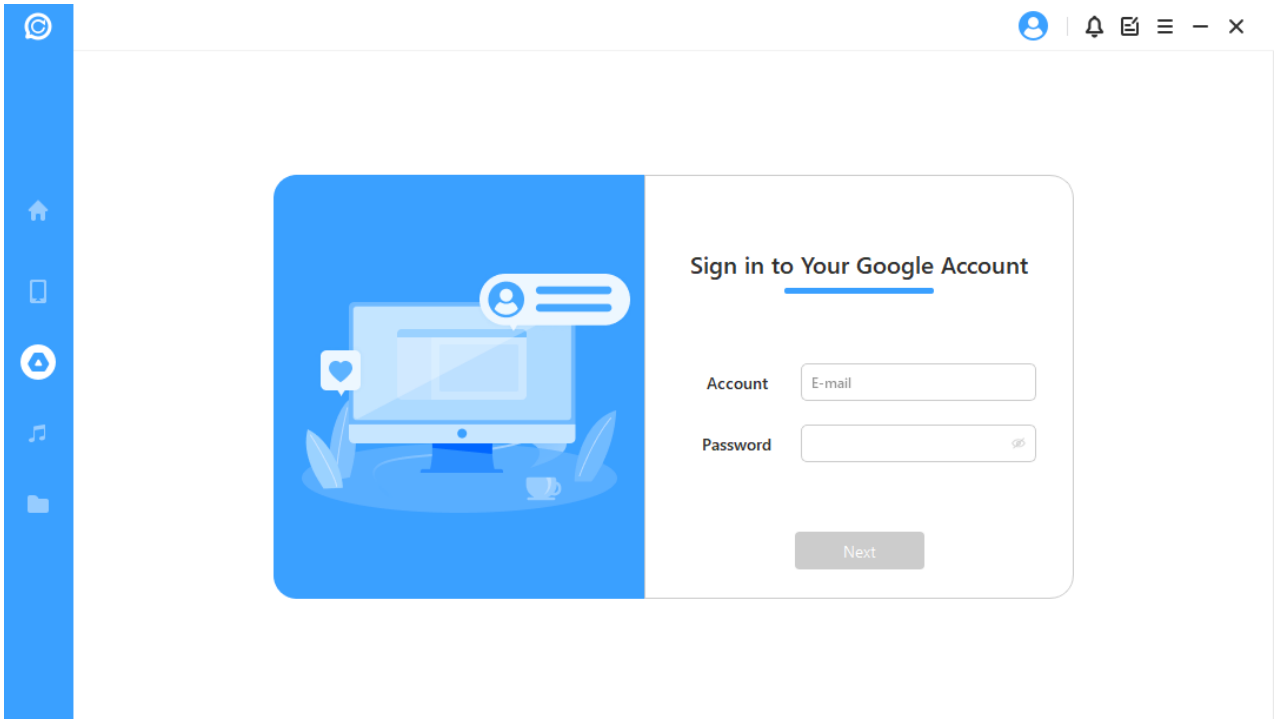


3) Step 3: After accessing the device data all the available WhatsApp chats, photos, videos, audio, contacts, and files will be displayed on the screen after that we can recover the complete chat or specific chat it to (device otherwise we can recover to PC also).

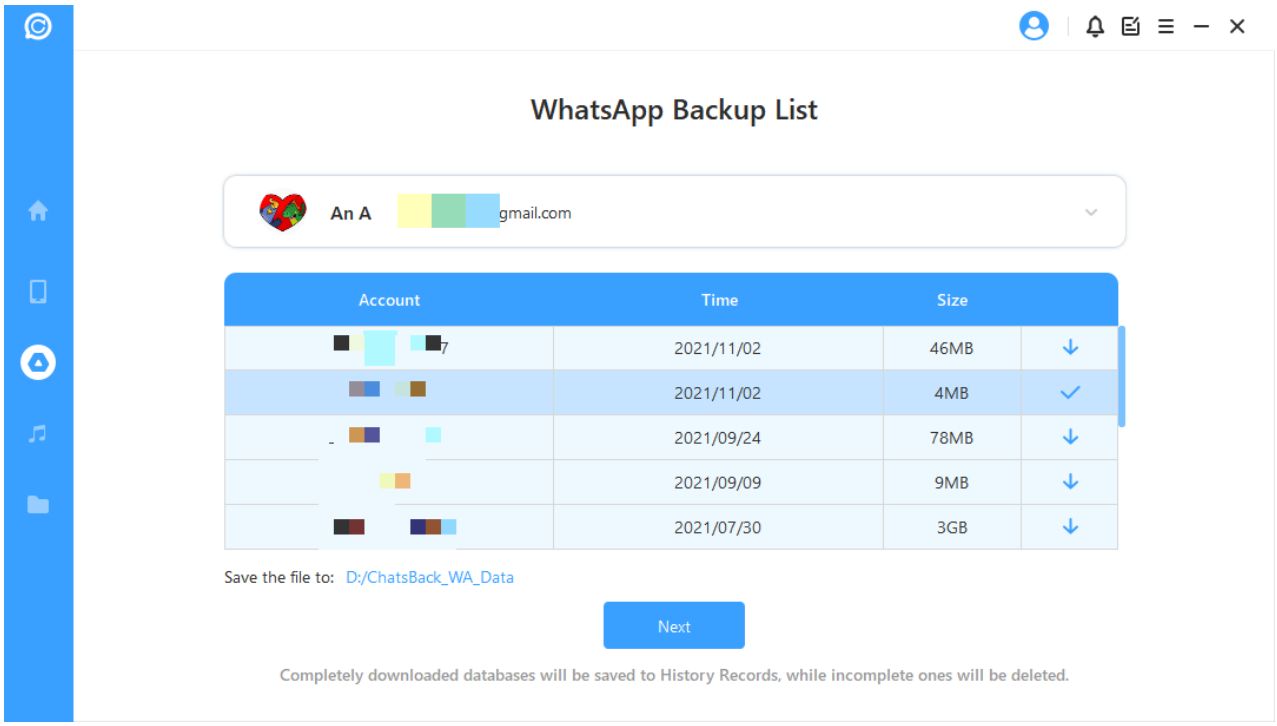


From Google Drive Backup:

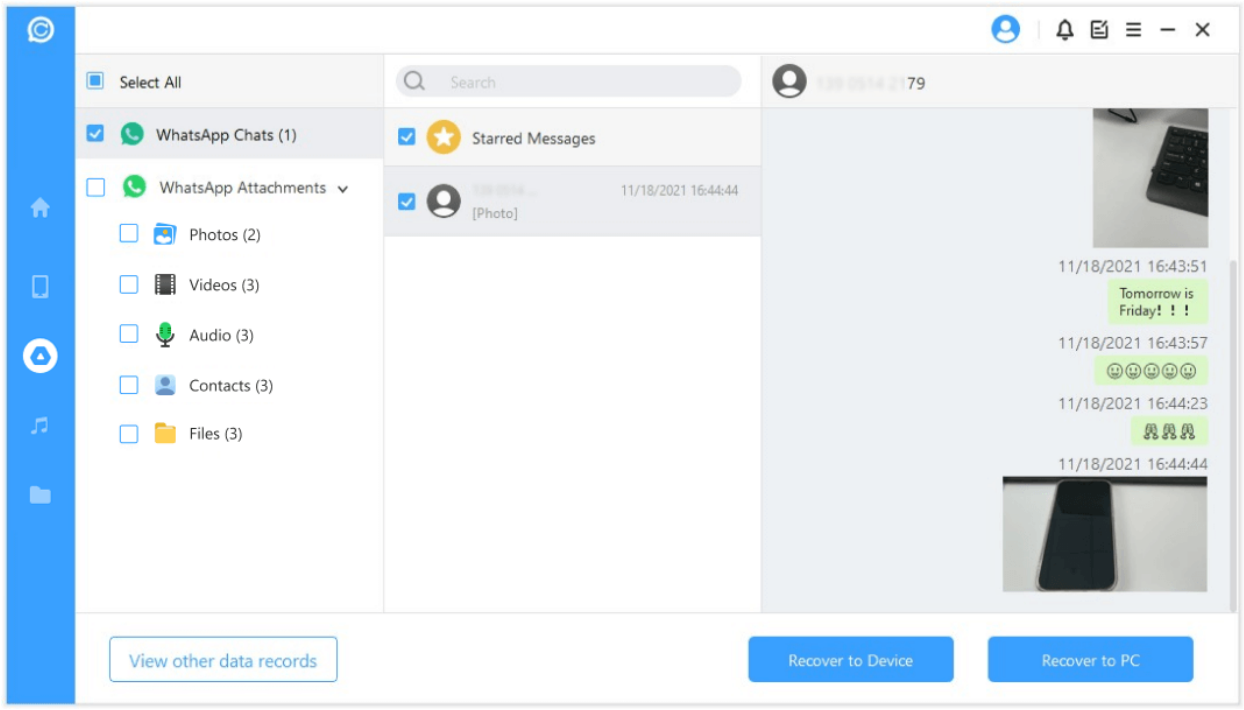
1) Step 1: Sign in to your Google account.



2) Step 2: Download WhatsApp backup

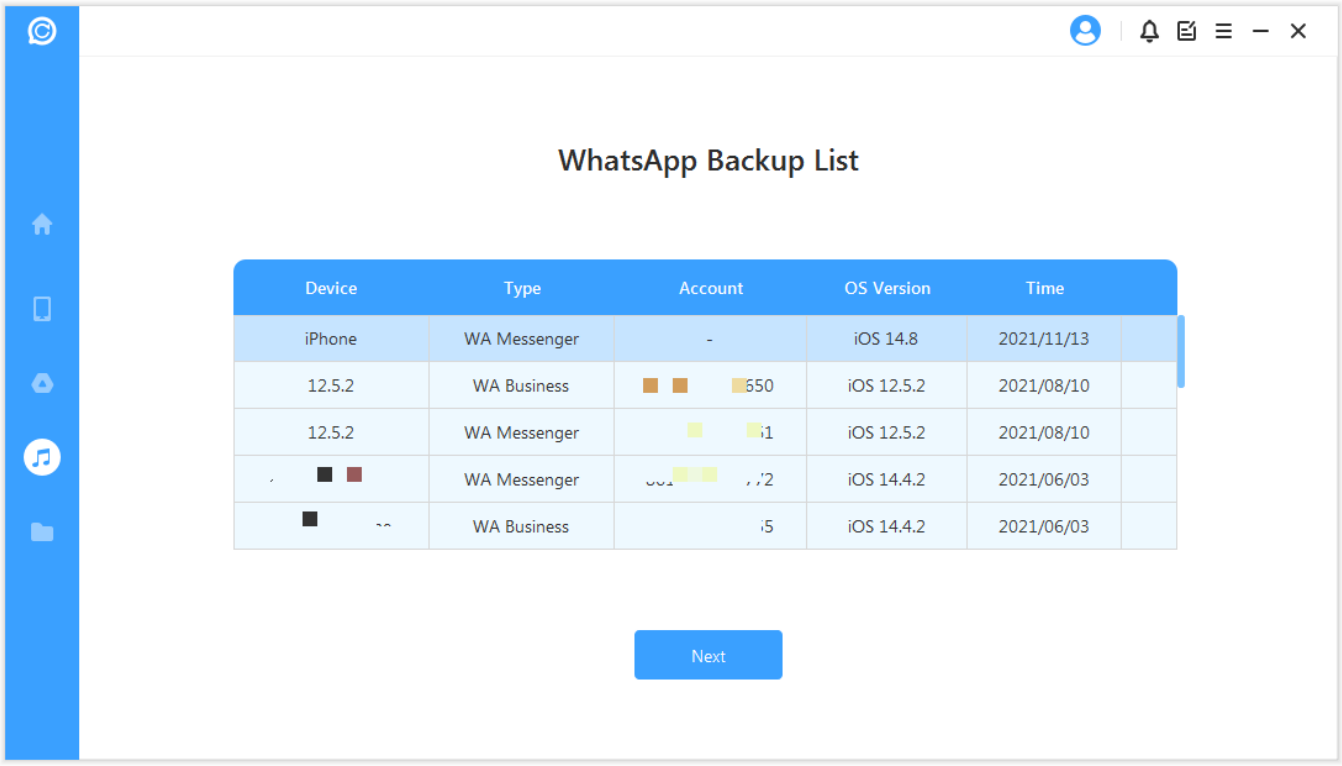


3) Step 3: Preview and recover

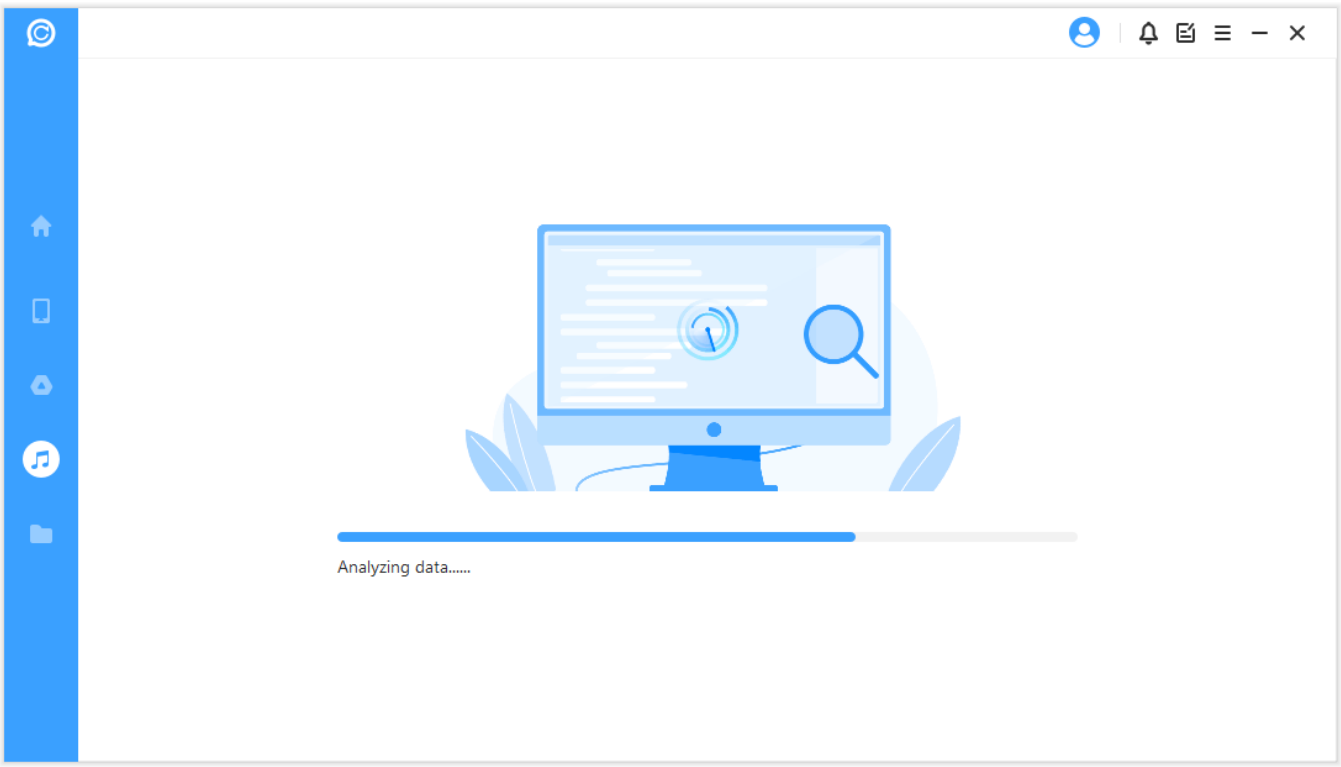


From iTunes Backup:

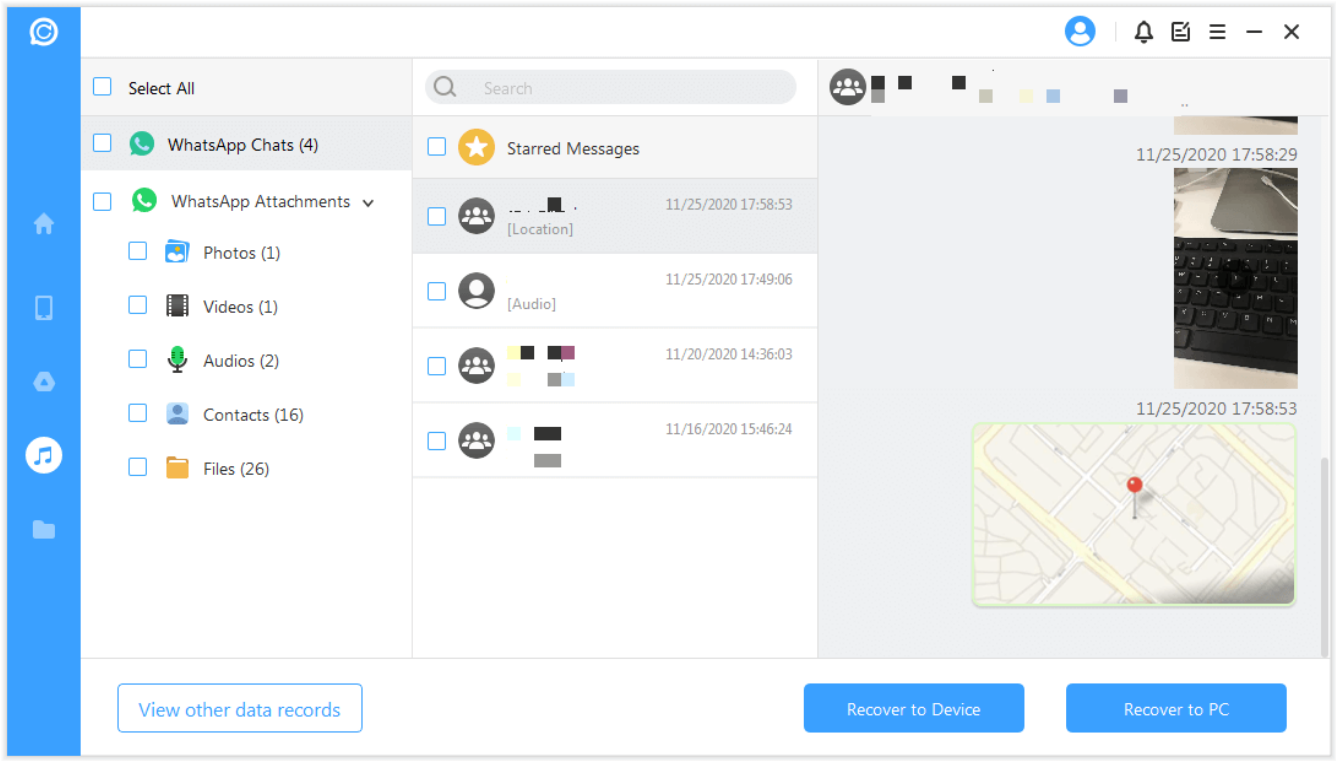
1) Step 1: Choose an iTunes backup from the WhatsApp backup list.



2) Step 2: Start to Analyze the data

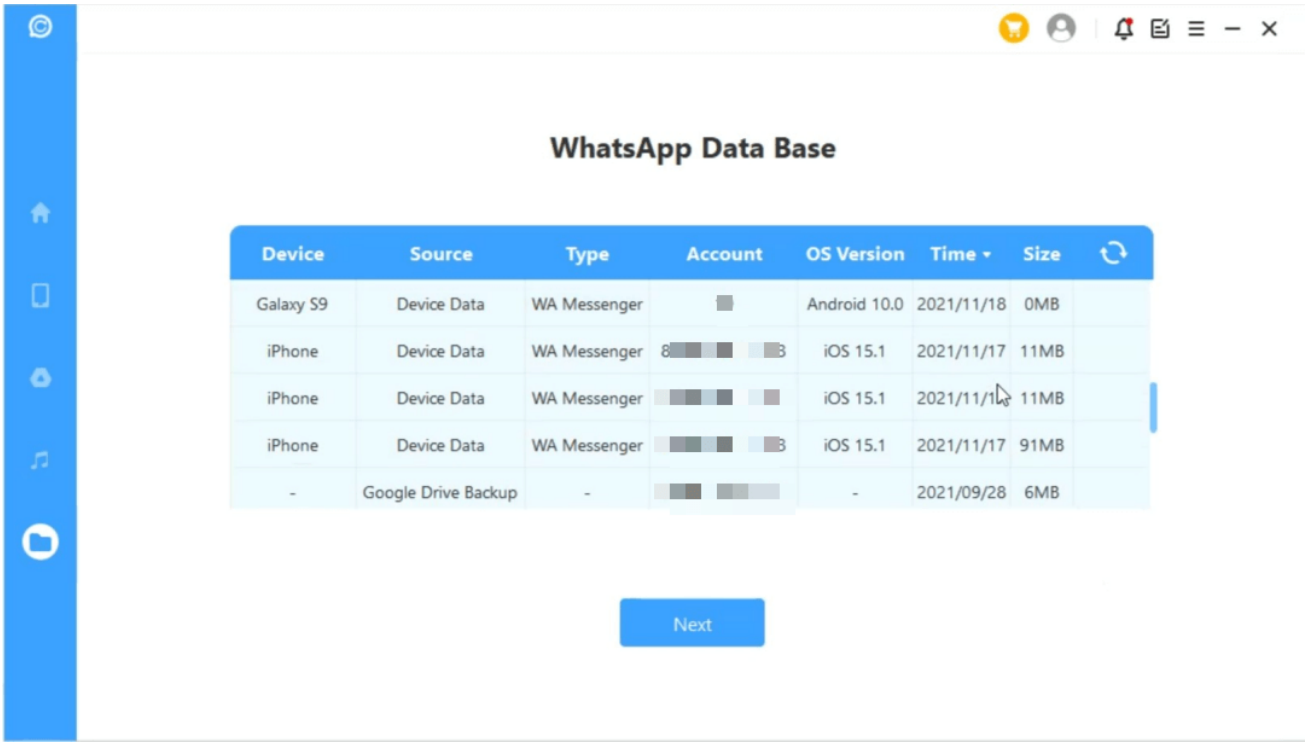


3) Step 3: Preview & Recover

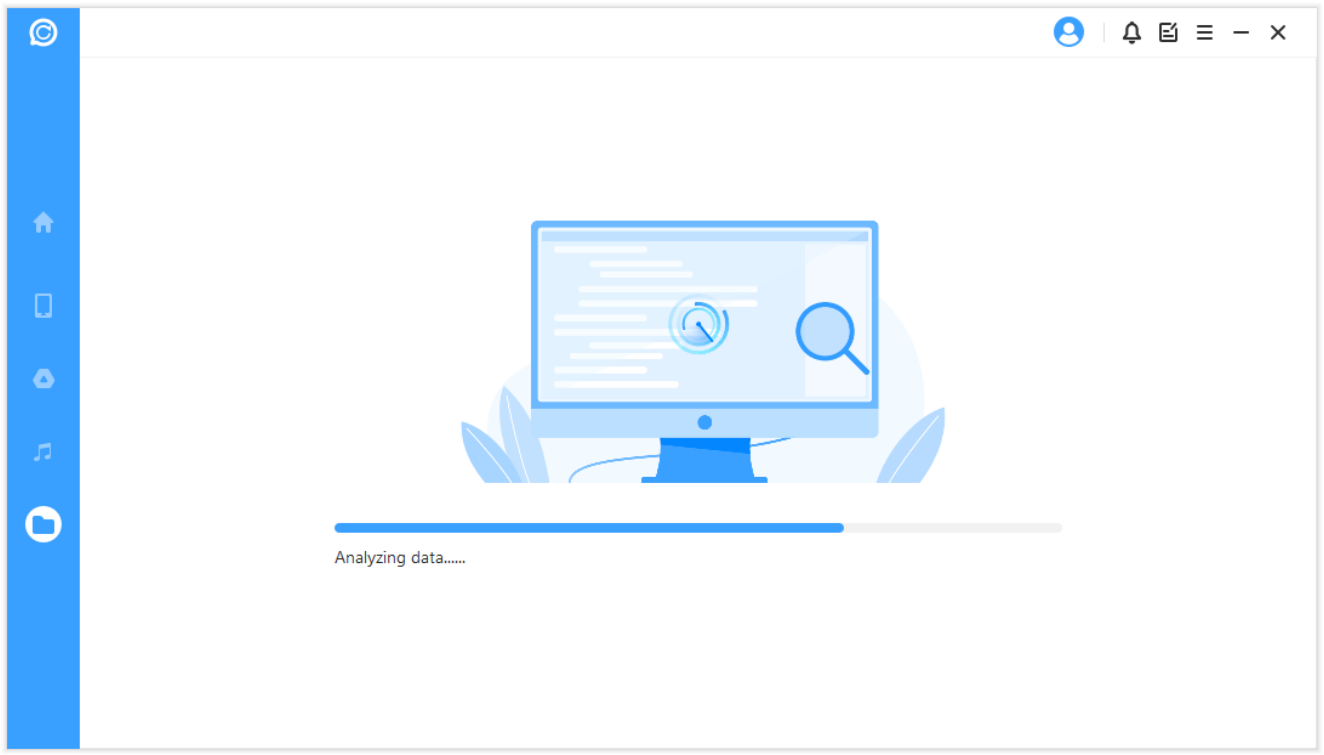


From History Records:

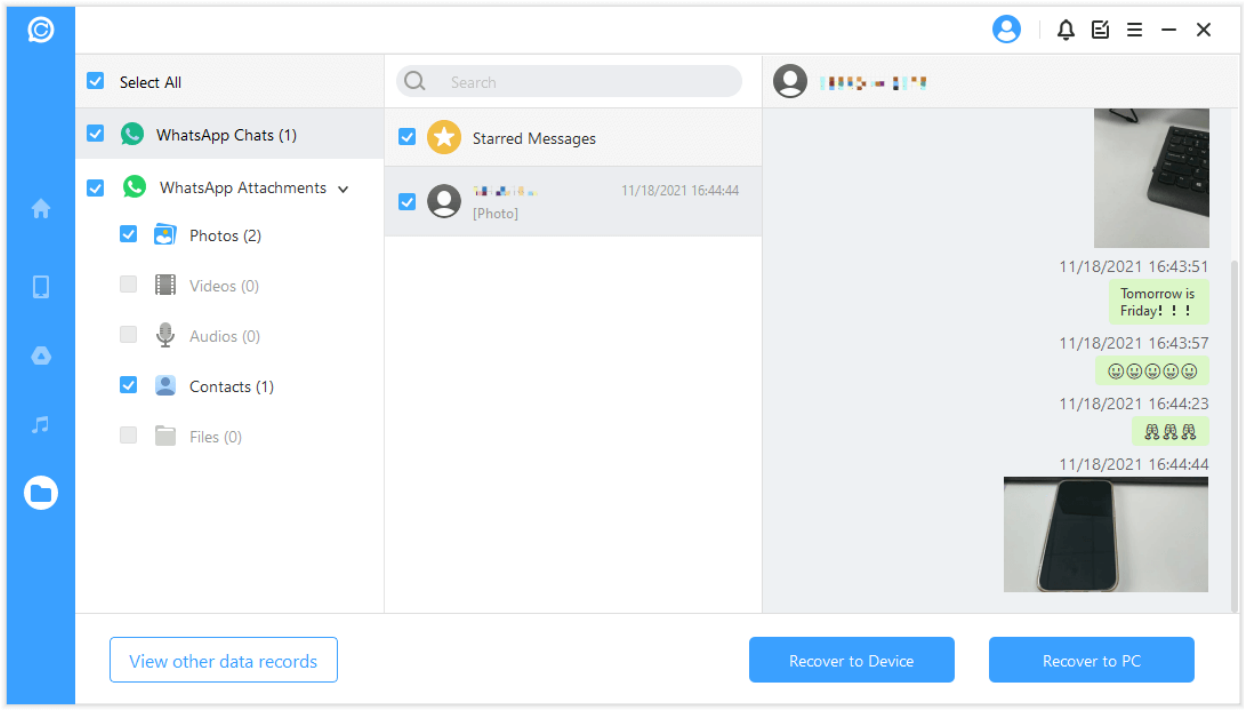
Step 1: Choose a Historical Database from WhatsApp Database



Step 2: Start to Analthe size data



Step 3: Preview & Recover



TYPES OF CASES ENCOUNTERED:

1) CCTV Forensics:

In CCTV Forensics actually, we take Closed Circuit Television (CCTV) footage for analysis & Evidence purposes whether it may be DVR or NVR.

Steps for CCTV Forensics:

Step 1: Analyse the footage on the DVR/NVR as per the requirement for Evidence purposes.

Step 2: Extract the finalized footage in new pen drives by giving names as per IO requirements for the pieces of evidence.

Step 3: Verifying the details

Step 4: After verifying we do file hash & lastly; we do PD hash.

Step 5: Documentation in which we submit the Hash Value Certificate along with the number of exhibits with the screenshot for evidence purposes.

2) Mobile Forensics:

In Mobile Forensics we do complete extraction using forensic software tools also we do WhatsApp extraction and mobile phone analysis as per the requirement.

Tools we used for Mobile Forensics:

1. MOBILeditdit
2. Cellibrite UFED
3. Disk Drill
4. iMazing
5. iTunes
6. Chat Back

3) Voice Sampling:

Voice Sampling is the process of taking voice samples of the complainant & culprits.

It may be Voice Recording, Call Recording, video recording, or CCTV video Recording.

Steps for Voice Sampling:

Step 1: We make transcripts as per the given Recordings.

Step 2: After that, we make a Hash Value certificate.

Step 3: We take voice sampling using voice recorder.

4) DGGI:

The Directorate General of GST Intelligence (DGGI) is a law enforcement agency under the Ministry of Finance responsible for fighting tax evasion in India. It was founded in 1979 as the Directorate General of Anti-

Evasion and was later renamed the Directorate General of Central Excise Intelligence. The agency was renamed as Directorate General of GST Intelligence (DGGI) after the introduction of the Goods and Services Tax. The agency is part of NATGRID. The organization is staffed by officers of the Central Board of Indirect Taxes and Customs.

The DGGI is the apex intelligence and investigative agency for matters relating to violation of the Goods & Services Tax, Central Excise Duty, and Service Tax. DGGI has been entrusted with the task of improving compliance with Indirect Tax laws. It has over the years established its reputation as a professional organization. Paying the right amount of tax is a social responsibility towards the nation. As taxes are the main source of Government finance, evasion of taxes hurts everybody & hampers the larger task of nation-building. We would urge all citizens to join hands with us in the task of bringing evaders of indirect taxes such as Central Excise Duty, Service Tax & GST to the books. Contact us through a letter, phone, e-mail, website, or in person wherever you feel that there is a tax evader in the shadows. We promise that we will take action. We promise you confidentiality and a monetary reward too in cases where your information has led to a recovery of taxes.

I worked on a Raid case with DGGI (Directorate General of GST Intelligence) which was carried out at Kolhapur for nearly 36 Hrs.

5) CID Case:

A Crime Investigation Department (CID) is a branch of the State Police Services of India responsible for the investigation of crime, based on the Criminal Investigation Departments of British police forces.

CID branches:

A CID may have several branches from state to state. These branches include:[4]

- CB-CID
- Anti-Human Trafficking & Missing Persons Cell
- Anti-Narcotics Cell
- Finger Print Bureau
- CID
- Anti-Terrorism squad

Crime Branch CID:

CB-CID is a special wing in a CID headed by the Additional Director General of Police (ADGP) and assisted by the Inspector General of Police (IGP). This branch investigates serious crimes including murder, riot, forgery, counterfeiting, and cases entrusted to CB-CID by the state government or the High Court.

6) Personal Cases:

In Personal cases, we provide all the pieces of evidence which are required for the further processing of the case.

7) Social Media Forensics:

In social media forensics, we need to refer complete data which are been deleted from WhatsApp, DCIM videos, etc.

8) Computer Forensics:

- Network forensics: This involves monitoring and analyzing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.

- Email forensics: In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract crucial information related to the case.

- Malware forensics: This branch of forensics involves hacking-related crimes. Here, the forensics expert examines the malware, and trojans to identify the hacker involved behind this.

- Memory forensics: This branch of forensics deals with collecting data from the memory (like cache, RAM, etc.) in raw and then retrieving information from that data.

- Mobile Phone forensics: This branch of forensics generally deals with mobile phones. They examine and analyze data from mobile phones.

- Database forensics: This branch of forensics examines and analyses the data from databases and their related metadata.

- Disk forensics: This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

CONCLUSION:

2) The forensic examination of electronic systems has undoubtedly been a huge success in the identification of cyber and computer-assisted crime. Organizations are placing increasing importance on the need to be equipped with appropriate incident management capabilities to handle the misuse of systems. Computer forensics is an invaluable tool in the process.

3) The domain of computer forensics has grown considerably in the last decade. Driven by industry, the focus was initially placed on developing tools and techniques to assist in the practical application of the technology. In more recent years, an increasing volume of academic research is being produced exploring various new approaches to obtaining forensic evidence.

4) With the emergence of science and technology, cyber forensics has played a very important role. Moreover, with the increase in crimes like hacking, etc, the need for cyber forensics have felt, thus various tools and techniques have been developed for tracing the crime, making the exact report to make it admissible in a court of law.

5) Various industries, corporations, and governmental agencies nowadays are keen on appointing an expert in this field to check out cyber malfunctioning done by the employees. Such experts are appointed to investigate computer-related crimes. After making an investigation, these specialists have to extract and prepare an exact report of the evidence gathered through various mediums before the authority who asked them to do.

6) The existing forensic tools play a vital role in the aspect of recovery. Each tool has its constraints and limitations. There is a need to make these tools and techniques more advance and enhanced to make computer forensics a full success and legally valid in law.

7) The future of computer forensics is limitless. With the expansion of technology, the field will continue to expand along it its benefits and barriers. Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability. The evidence so collected by the specialist has to be handled and preserved appropriately So that it can be produced before the court in its exact manner. Any process or methodology breakdown in the implementation of cyber forensics will ultimately lead to the jeopardy of the case.

Summary:

Cybercrime investigators need to be as intimately familiar with the internal workings of computers and the software that runs on them as homicide investigators must be with basic human pathology. That includes understanding the function of all the hardware components that go together to make up a computer and how these components interact with one another.

It would be difficult for an investigator to conduct a proper investigation in a foreign country where he or she does not speak the local language because many clues might go unnoticed if the investigator cannot understand the information being collected. Likewise, a cybercrime investigator must have a basic understanding of the "language" used by the machines to process data and communicate with each other. Even though an investigator in the field might not be able to speak all human languages, it is helpful to at least be able to recognize what language written evidence is in, because this evidence might be significant and will certainly help the investigator find someone who can translate it. Similarly, even though a cybercrime investigator is not expected to be able to program in binary, it helps to recognize the significance of data that is in binary or hexadecimal format and when it can or can't be valuable as evidence.

Computers today run a variety of operating systems and file systems, and the investigator's job of locating evidence will be performed differently depending on the system being used. A good cybercrime investigator is familiar with the most common operating systems and how their file systems organize the data on disk.

Regardless of the operating system or hardware platform, the majority of networks today run on TCP/IP protocols. TCP/IP is the most routable protocol stack and thus the most appropriate for large routed networks; it is required for connecting to the Internet. This chapter provided a basic overview of networking hardware and software and how TCP/IP communications are accomplished.

Contribution:

I had been working as a Cyber Crime Investigator at Sana Cyber Forensics Investigation & Data Security Services Pvt.Ltd from 27th December 2022 to 30th June 2023

Until now I had done in total 23-24 cases. I had worked with various police stations in Pune, also worked on a variety of personal cases, also had done transcripts, and also had solved sensitive cases such as CID (Crime Investigation Department) case, DGGI (Directorate General of GST Intelligence) Raid case, and Pune Railway Police, Police Station case.

Police Station Cases – 21

DGGI Raid Case – 1
CID Case – 1
Personal Cases – 2

I had been working with many high-profile government officers such as Additional Commissioner DGGI, SIO (Senior Intelligence Officer) DGGI, DYSP CID Unit, Assistant Commissioner of Police, Additional Superintendent of Police, Superintendent of Police & many - Senior Police Inspectors, Police Inspectors, Assistant Police Inspector, Police sub-Inspectors, Police Constables and many more.

Benefits:

1) Exposure to cyber-criminal cases and how to deal with them with several types of cases.
2) Acquaintance with various class police officers.
3) Contribution to law & enforcement agencies.
4) To gain knowledge of various forensics tools.
5) Learned how to deal with critical scenarios with proper guidelines.
6) Fostered my Personal Development growth.
7) Enhancement of team working skills.
8) Exposure to Personal cases and maintaining they're confidential.
9) Exposure to live cases (Raid Cases).
10) Learned to handle digital pieces of evidence.
11) Achieved real work experience.