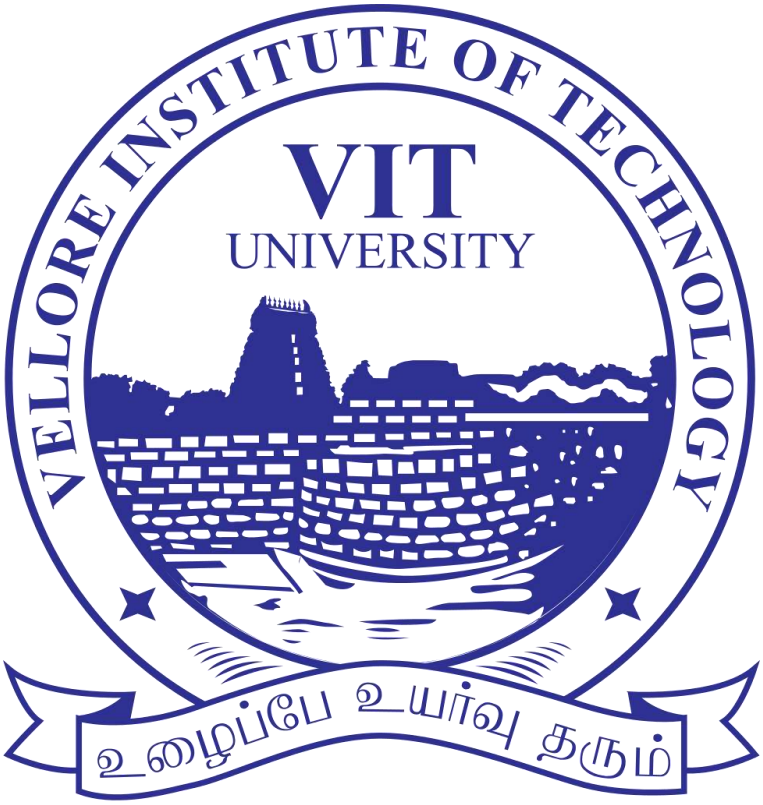
Cyber Security

Digital Assignment – 2

(Report Day 2)



Name – Nilay
Registration no. – 21BIT0219
Slot – A1 + TA1
Faculty – DR. GITANJALI J

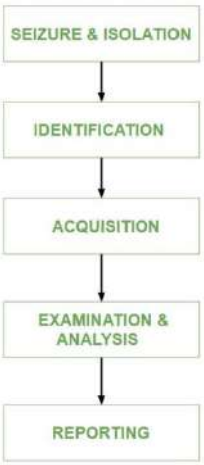
Introduction to Mobile forensic

Mobile forensics, a subset of digital forensics, is the process of recovering digital evidence from mobile devices such as smartphones, tablets, and wearables. With the proliferation of mobile technology and the increasing use of mobile devices for communication, productivity, and entertainment, mobile forensics has become crucial in investigating a wide range of crimes, including cybercrime, fraud, theft, and terrorism.

The primary goal of mobile forensics is to extract, analyze, and interpret data stored on mobile devices to uncover evidence relevant to an investigation. This data can include text messages, call logs, emails, photos, videos, location information, application data, and more. Mobile forensic analysts use specialized tools and techniques to access both user-generated content and system files on mobile devices while maintaining the integrity of the evidence.

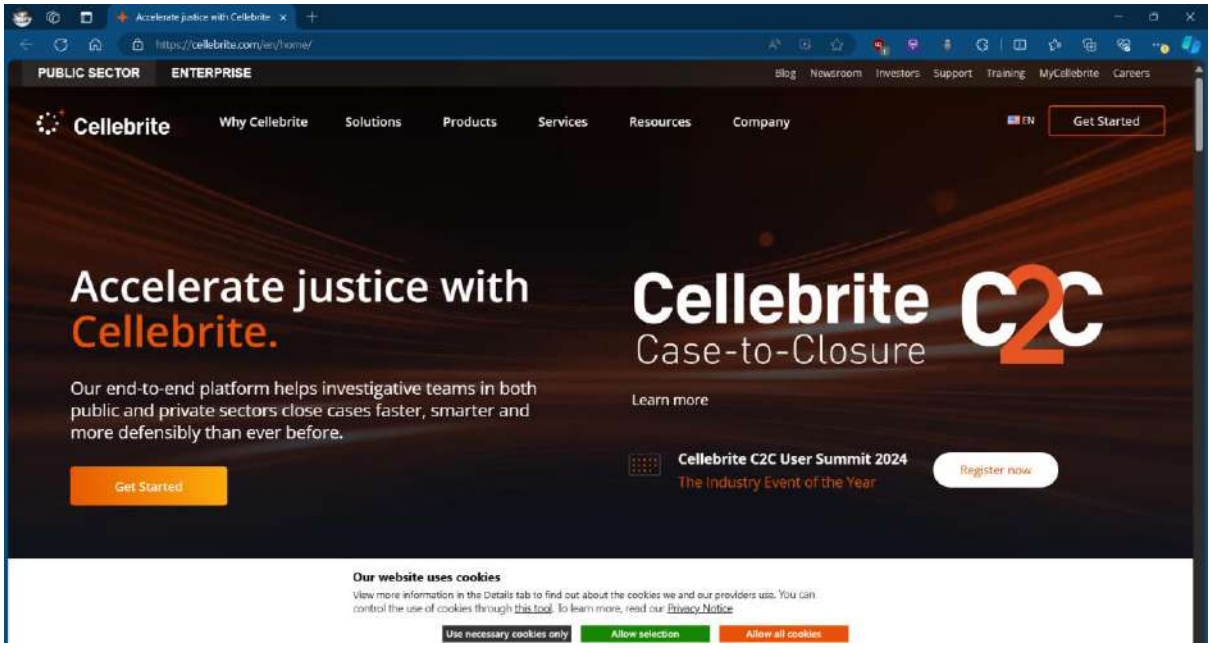
Mobile forensic investigations typically follow a structured process that includes:

1. Acquisition: The first step is to acquire a forensic image or extract data from the mobile device. This can be done using physical or logical acquisition methods, depending on the device's make, model, and state (locked or unlocked). Physical acquisition involves creating a bit-by-bit copy of the device's storage, while logical acquisition focuses on extracting specific files and data from the device.
2. Analysis: Once the data is acquired, forensic analysts analyze the extracted information to identify relevant evidence. This may involve examining communication logs, browsing history, installed applications, media files, and other artifacts to reconstruct the user's activities and interactions.
3. Interpretation: After analyzing the data, forensic analysts interpret the findings in the context of the investigation. They look for patterns, correlations, and anomalies that may provide insights into the events under scrutiny. Interpretation may involve linking digital evidence to physical locations, timelines, and individuals involved in the case.
4. Reporting: Finally, forensic analysts document their findings in detailed reports that summarize the investigation process, analysis methodology, and key findings. These reports may be used to support legal proceedings, law enforcement actions, or internal investigations.




Evidence @ a Crime

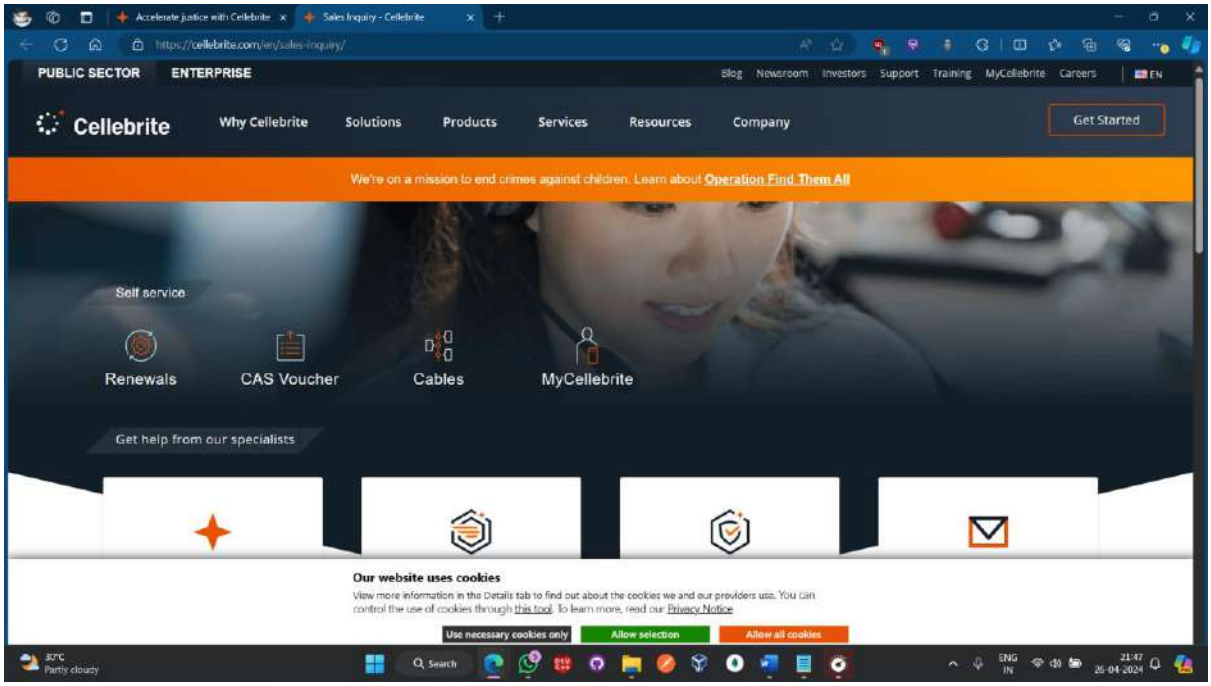
Cellebrite.com



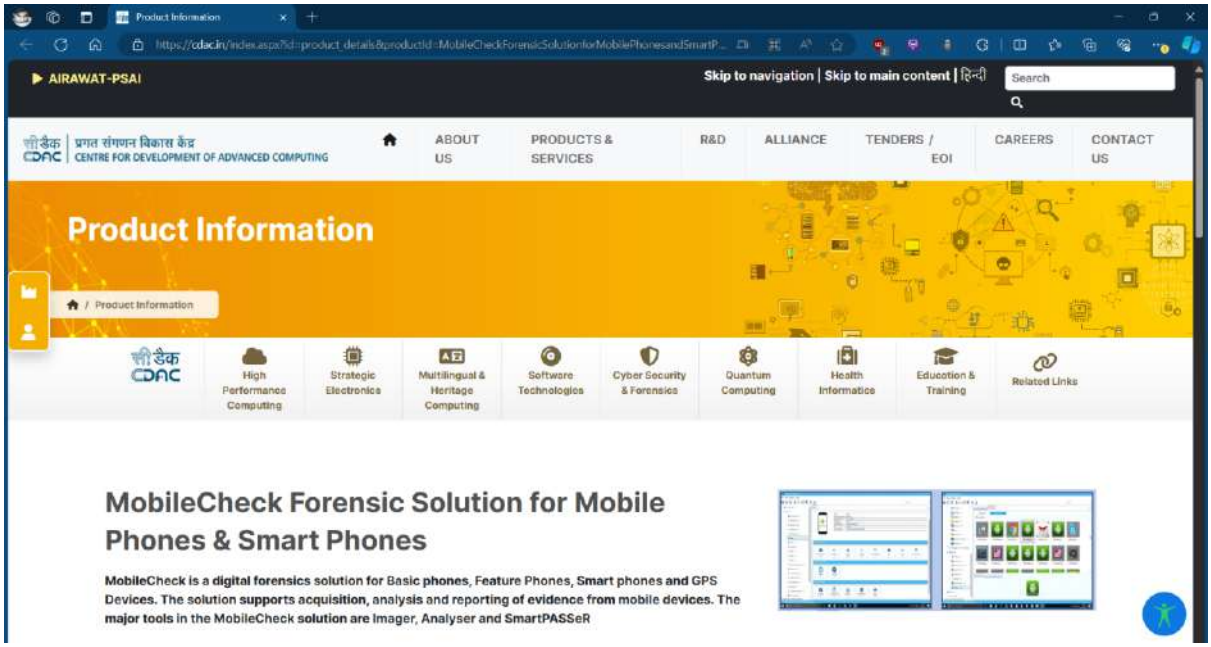
1. Cellebrite is a digital intelligence company that provides solutions for mobile data extraction, analysis, and intelligence. Their technology is often used by law enforcement agencies, intelligence services, and private sector organizations for forensic investigations and data recovery from mobile devices.
2. **Company Background**: Cellebrite was founded in 1999 and has since become a global leader in digital intelligence solutions. The company is headquartered in Israel, with offices and subsidiaries worldwide, including in the United States, Europe, Asia-Pacific, and Latin America.
3. **Products and Solutions**:
    a. **UFED (Universal Forensic Extraction Device):** Cellebrite's UFED series is a range of hardware and software solutions designed for extracting, decoding, and analyzing data from mobile devices, including smartphones, tablets, and GPS devices. UFED devices support a wide range of mobile operating systems, including iOS, Android, BlackBerry, and more.
    b. **Physical Analyzer**: This software tool allows forensic examiners to perform in-depth analysis of extracted data, including decoding proprietary file formats, recovering deleted data, and generating comprehensive reports.
    c. **UFED Cloud Analyzer:** Cellebrite's cloud analysis solution enables investigators to access and analyze data stored in cloud services such as iCloud, Google Drive, and Dropbox.
    d. **UFED Touch2:** The UFED Touch2 is a portable forensic device equipped with touch-screen capabilities, designed for on-site data extraction and analysis.
    e. **UFED 4PC:** UFED 4PC is a software-based forensic solution that runs on standard PCs, offering similar capabilities to Cellebrite's hardware devices.

f. **BlackBag:** Cellebrite acquired BlackBag Technologies in 2021, expanding its portfolio to include digital forensic solutions for Mac and Windows operating systems.
g. **Analytics Platform**: Cellebrite offers an analytics platform that enables organizations to extract actionable insights from digital data for investigative and intelligence purposes.

4. **Training and Certification**: Cellebrite offers training and certification programs for digital forensic professionals, law enforcement personnel, and corporate investigators. These programs cover topics such as mobile device forensics, data extraction techniques, legal considerations, and best practices in digital evidence handling.
5. **Research and Development**: Cellebrite invests significantly in research and development to stay ahead of emerging trends and technologies in digital forensics. The company continuously updates its products to support new mobile devices, operating system versions, and encryption methods.

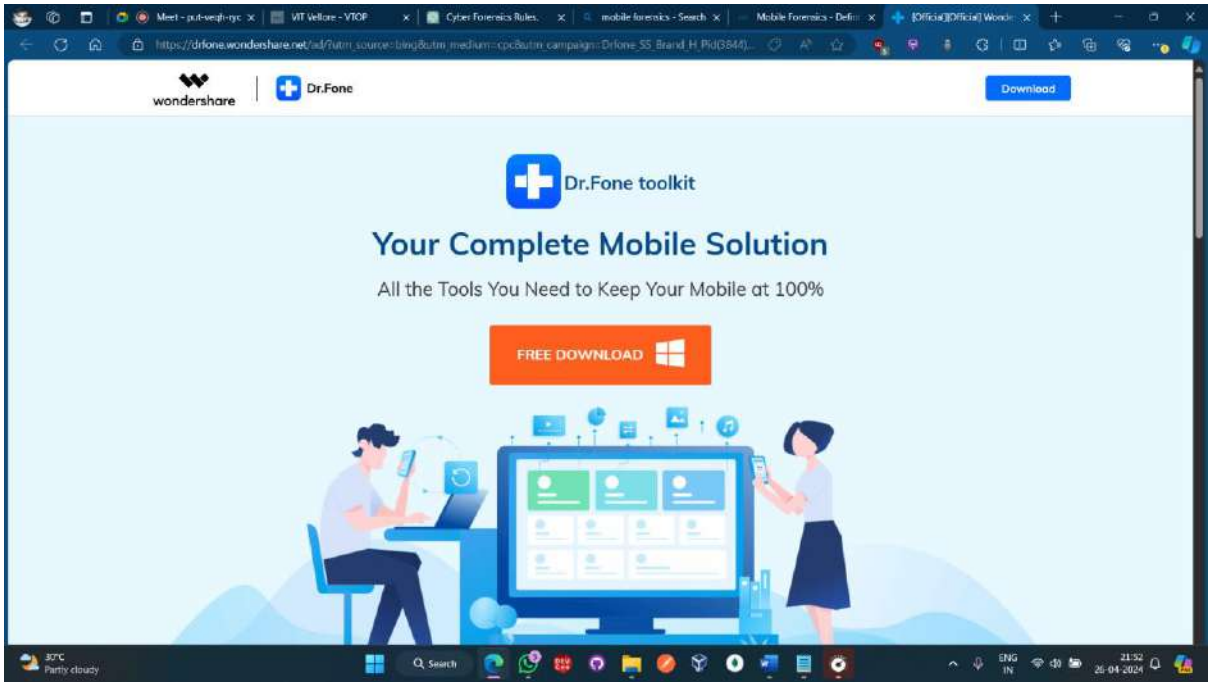


Centre for Development of Advanced Computing (CDAC)



CDAC is an Indian government organization that focuses on research and development in the field of information technology. The link provided likely leads to a page about their Mobile Check Forensic Solution, which is a tool used for forensic analysis of mobile phones and smartphones.

dr.fone by Wondershare

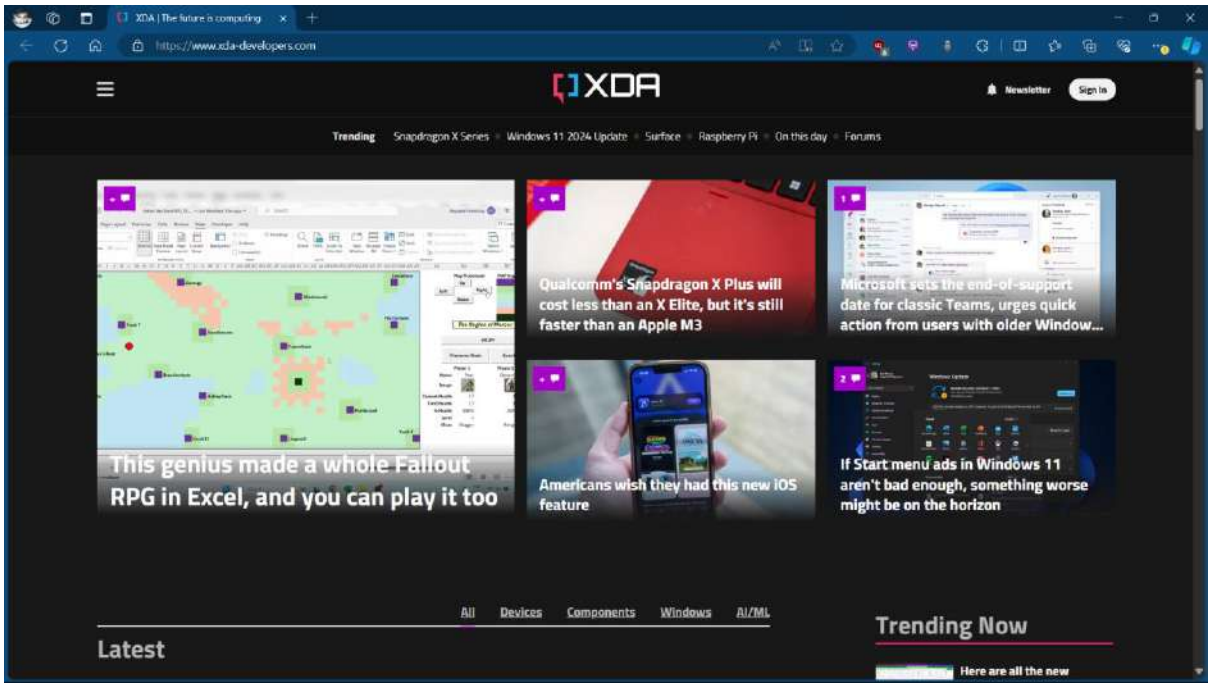


dr.fone is a software toolkit developed by Wondershare, which offers a range of tools for data management, recovery, and transfer for mobile devices. It includes features for recovering lost data, transferring data between devices, and fixing various issues with iOS and Android devices.

- DrFone is mobile device management software that provides solutions for managing, transferring, backing up, and recovering data on iOS and Android phones.
- The software includes features to unlock screens, erase data, repair system issues, transfer social media chats, manage contacts and media files, and mirror device screens.
- DrFone aims to simplify phone management with its suite of user-friendly tools for personal and business use.

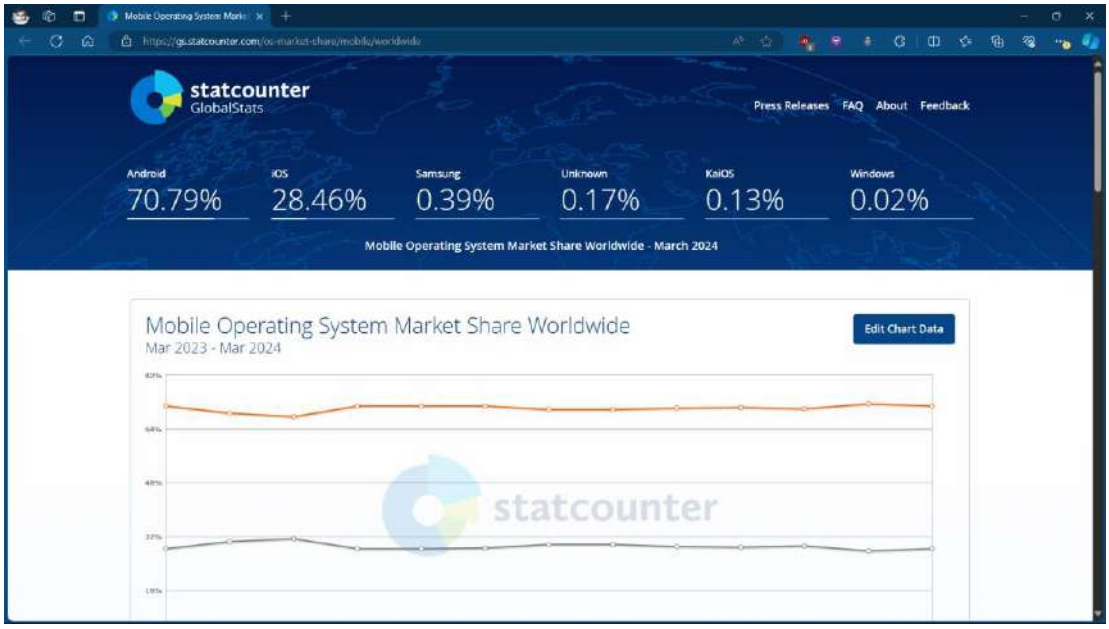
XDA Developers:

XDA Developers is a community-driven forum and website dedicated to the development and customization of Android devices. It provides a platform for users, developers, and enthusiasts to discuss and share information about custom ROMs, kernels, apps, and modifications for Android devices.

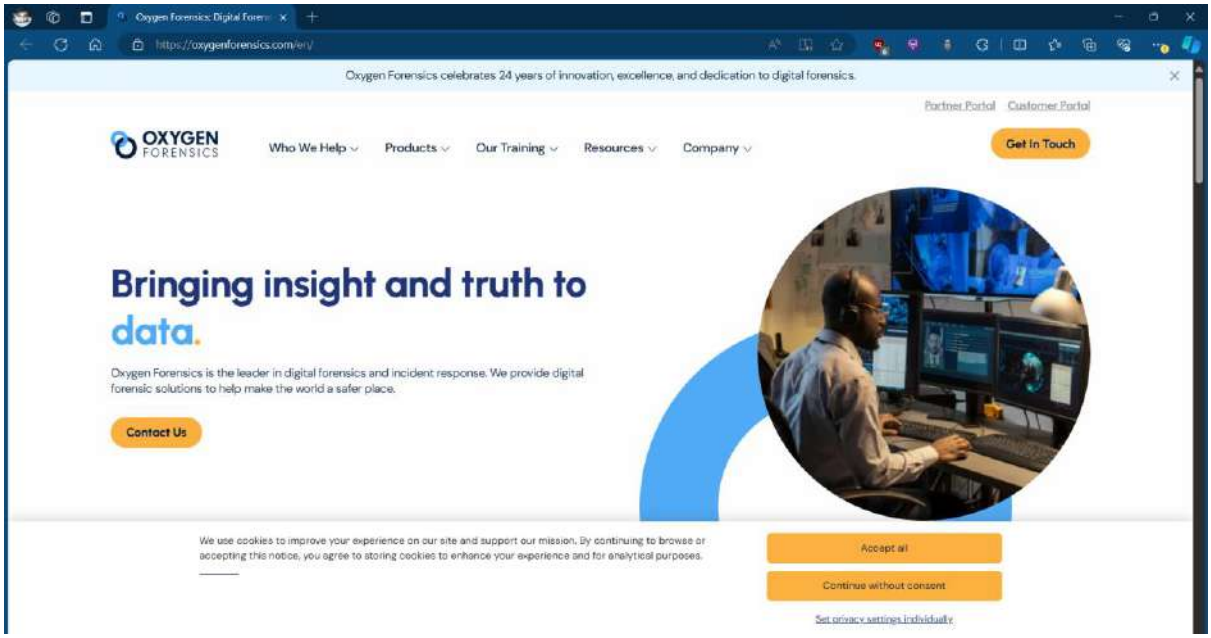


StatCounter:

StatCounter is a web analytics service that tracks and reports website traffic, including market share statistics for operating systems and browsers. The links provided lead to pages showing the market share of mobile operating systems worldwide and in India, based on data collected by StatCounter.



Oxygen forensics:



Oxygen Forensics is a leading provider of digital forensic investigation software and solutions for law enforcement agencies, government organizations, corporate security teams, and digital forensic professionals. Here's a detailed overview of Oxygen Forensics:

1. <u>Company Background:</u>

- Founded in 2000, Oxygen Forensics has established itself as a trusted name in the digital forensics industry, offering innovative solutions for data extraction, analysis, and reporting.

- The company is headquartered in Alexandria, Virginia, USA, with a global presence through regional offices and authorized partners worldwide.

2. <u>Products and Solutions</u>:

- Oxygen Forensic Detective: Oxygen Forensic Detective is the company's flagship software solution, designed for comprehensive digital forensic investigations across various devices and platforms.

- Mobile Forensics: Oxygen Forensic Detective supports the extraction and analysis of data from a wide range of mobile devices, including smartphones, tablets, feature phones, and IoT devices. It covers all major mobile operating systems, including iOS, Android, BlackBerry OS, Windows Phone, and more.

- Cloud Forensics: The software enables forensic examiners to extract and analyze data stored in cloud services such as iCloud, Google Drive, Dropbox, Microsoft OneDrive, and social media platforms.

- Computer Forensics: Oxygen Forensic Detective extends its capabilities to computer forensics, allowing investigators to analyze digital evidence from computers and storage media, including Windows, macOS, and Linux systems.

- Social Media Analysis: The software includes tools for extracting and analyzing data from popular social media platforms, messaging apps, email accounts, and web browser histories.

- Geolocation Analysis: Oxygen Forensic Detective provides geolocation analysis features, allowing investigators to map out device locations, movements, and geographic patterns based on GPS data, Wi-Fi networks, and cell tower information.

- Reporting and Collaboration: The software offers robust reporting capabilities, allowing users to generate detailed forensic reports, timelines, and visualizations. It also supports collaboration among forensic examiners and stakeholders through case sharing and annotation features.

3. Key Features and Capabilities:

- Advanced Data Extraction: Oxygen Forensic Detective employs advanced extraction techniques to retrieve both user and system-level data from mobile devices and digital media, including deleted files, call logs, text messages, contacts, photos, videos, location data, and app usage information.

- Timeline Analysis: The software enables investigators to create chronological timelines of events and activities based on extracted data, helping to reconstruct sequences of events and establish timelines for investigations.

- Keyword Search and Filtering: Users can perform keyword searches and apply filters to quickly identify relevant information within large datasets, speeding up the analysis process and focusing on critical evidence.

- Data Visualization: Oxygen Forensic Detective offers visualization tools to present forensic findings in a clear and intuitive manner, including charts, graphs, maps, and interactive timelines.

- Data Carving and Recovery: The software includes data carving capabilities to recover deleted files and fragmented data from storage media, allowing investigators to retrieve valuable evidence that may have been intentionally or unintentionally deleted.

4. Training and Support:

- Oxygen Forensics provides comprehensive training programs, certifications, and workshops to help forensic professionals master the use of their software and stay updated on the latest techniques and best practices in digital forensics.

- The company offers ongoing technical support, product updates, and access to a knowledge base and community forums to assist users with troubleshooting, case challenges, and knowledge sharing.

File Systems:

In cyber forensics, understanding file systems is crucial as it forms the backbone of digital storage and organization on computing devices. Here's an overview of file systems in the context of cyber forensics:

1. Definition: A file system is a method used by operating systems and software to organize, store, and retrieve data on storage devices such as hard drives, solid-state drives (SSDs), and removable media. It provides a structured way to manage files and directories, enabling efficient storage and access to digital information.

2. Types of File Systems:

- ***FAT (File Allocation Table):*** FAT is a simple file system commonly used on removable storage media such as USB drives, memory cards, and older hard drives. It's known for its compatibility across different operating systems but lacks advanced features like journaling and support for large file sizes.

- ***NTFS (New Technology File System):*** NTFS is a robust and feature-rich file system introduced by Microsoft for use in Windows operating systems. It supports features such as file encryption, compression, access control lists (ACLs), and journaling, making it suitable for both personal and enterprise use.

- ***exFAT (Extended File Allocation Table):*** exFAT is an extension of the FAT file system designed to support large file sizes and volumes, making it suitable for use in flash drives, SD cards, and other portable storage devices.

- ***HFS+ (Hierarchical File System Plus):*** HFS+ is a file system used on macOS and Mac OS X systems. It supports features like journaling, file compression, and encryption, making it suitable for Mac computers and storage devices.

- ***APFS (Apple File System):*** APFS is the successor to HFS+ and is designed specifically for use on Apple devices running macOS, iOS, watchOS, and tvOS. It offers features such as snapshotting, cloning, encryption, and improved performance for flash storage.

- ***EXT (Extended File System):*** The EXT family of file systems (e.g., EXT2, EXT3, EXT4) is commonly used in Linux and Unix-like operating systems. They offer features like journaling, access control, and support for large file systems and volumes.

- ***Others:*** There are numerous other file systems used in various computing environments, including ZFS (used in some Unix-based systems), ReFS (used in Windows Server environments), and UDF (used for optical discs).

3. Forensic Analysis of File Systems:

- ***File System Metadata:*** File systems store metadata such as file names, timestamps, file sizes, permissions, and directory structures. Forensic examiners analyze this metadata to reconstruct file activity, identify file ownership, and establish timelines of events.

- ***Data Recovery:*** File systems often leave remnants of deleted files and file fragments on storage devices. Forensic tools and techniques are used to recover deleted data and reconstruct files from these remnants, which can provide valuable evidence in investigations.

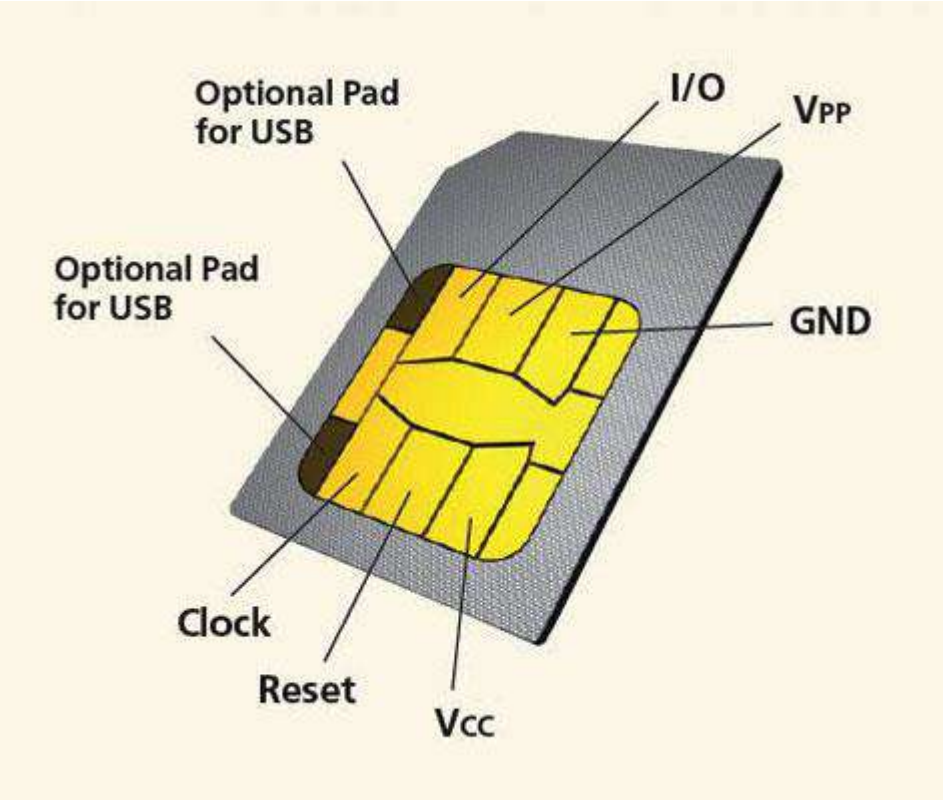
- ***File System Artifacts:*** File systems generate various artifacts during normal operation, including log files, cache files, and system files. Forensic analysis of these artifacts can reveal information about user activities, system events, and potential security incidents.

- ***Journaling:*** File systems with journaling capabilities, such as NTFS and ext4, maintain transaction logs that record changes to the file system. Forensic examiners analyze these journal entries to track file modifications, file deletions, and other file system activities.

- ***File System Forensics Tools:*** There are numerous specialized forensic tools and utilities available for analyzing and extracting data from different file systems. These tools offer features for disk imaging, data carving, file system analysis, and metadata extraction.

Digital Forensics with SIM:

Digital forensics involving SIM cards is a crucial aspect of modern investigations, especially in cases involving mobile devices and telecommunications. Here's a detailed overview of digital forensics with SIM cards:



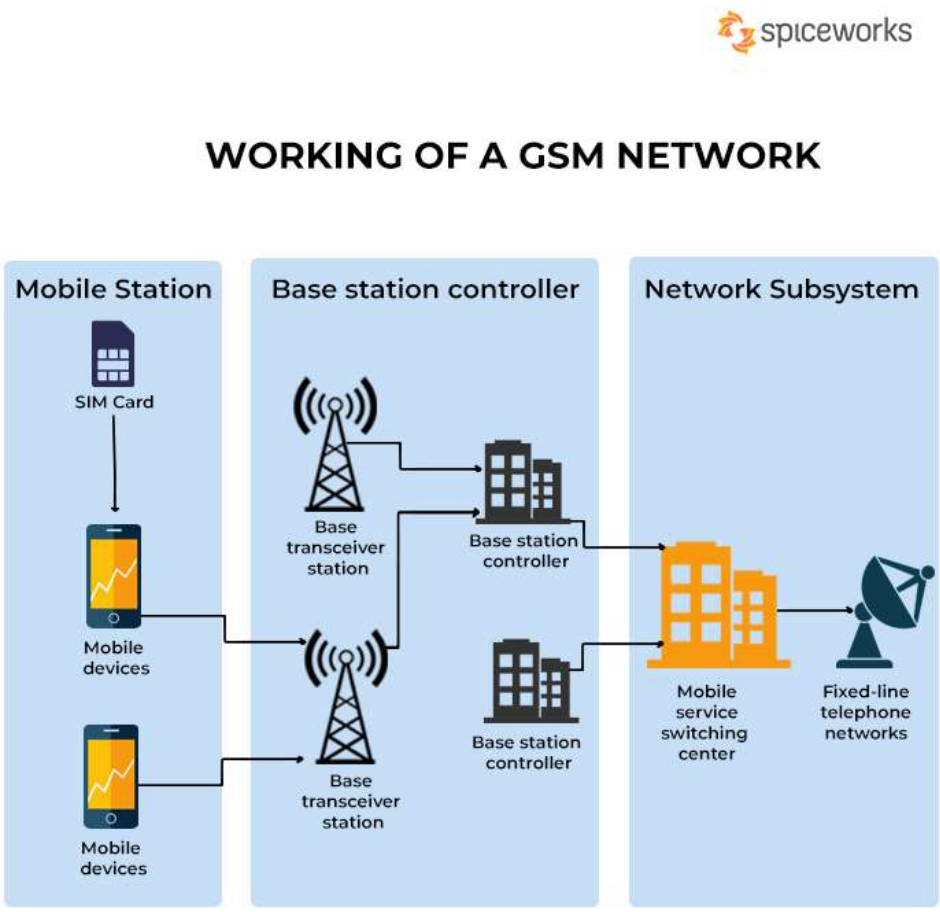
What is a SIM Card?

A Subscriber Identity Module (SIM) card is a small, removable smart card used in mobile phones and other cellular-enabled devices to securely store subscriber identity and related information.

SIM cards contain data such as the unique IMSI (International Mobile Subscriber Identity) number, ICCID (Integrated Circuit Card Identifier), authentication keys, network access information, and sometimes contacts and SMS messages.

1. **Role of SIM Cards in Digital Forensics:**
   - SIM cards play a crucial role in digital forensic investigations involving mobile devices. They can contain valuable evidence related to call logs, text messages, contacts, and network registration events.
   - Forensic analysis of SIM cards can provide insights into the user's communication patterns, contacts, location history, and interactions with cellular networks, which can be critical in criminal investigations, civil litigation, and intelligence gathering.
2. ***Types of Forensic Analysis with SIM Cards:***
   - Logical Analysis: Logical forensic analysis involves accessing the data stored on the SIM card using standard protocols and commands supported by the mobile device. This typically includes extracting call logs, SMS messages, contact information, and network-related data.
   - Physical Analysis: Physical forensic analysis involves a deeper examination of the SIM card's internal memory using specialized forensic tools and techniques. This may include recovering deleted data, examining hidden files, and analyzing the SIM card's file system structure.
   - Chip-Off Forensics: In cases where standard forensic methods are ineffective, chip-off forensics may be employed. This involves physically removing the memory chip from the SIM card and directly accessing its contents using specialized equipment.
3. ***Forensic Techniques and Tools:***
   - SIM Card Readers: Forensic examiners use SIM card readers to access and extract data from SIM cards. These readers connect to computers via USB and allow for the extraction of data using forensic software.
   - Forensic Software: There are specialized forensic software tools designed for analyzing SIM card data, such as Oxygen Forensic Detective, Cellebrite UFED, XRY, and MOBILedit Forensic Express. These tools enable examiners to extract, parse, and analyze SIM card data efficiently.
   - Data Parsing and Interpretation: Forensic software tools often include parsers and analyzers specifically designed for SIM card data formats. These tools can interpret the extracted data, reconstruct communication timelines, and present the findings in a clear and structured manner.
   - Data Recovery Techniques: In cases of data loss or deletion, forensic examiners may employ data recovery techniques to retrieve deleted data from SIM cards. This may involve searching for residual data fragments, examining unused memory space, and reconstructing deleted records.

4. ***Legal Considerations:***
    - Adherence to legal and regulatory requirements is essential in SIM card forensics. Investigators must obtain appropriate legal authorization (e.g., search warrants) before accessing and analyzing SIM card data.
    - Privacy considerations also come into play, particularly regarding the handling of sensitive personal information stored on SIM cards. Forensic examiners must follow established procedures to ensure the confidentiality and integrity of the data during the investigation process.
5. ***Challenges and Limitations:***
    - SIM card forensics can pose several challenges, including encryption of data, limited storage capacity, and compatibility issues with different mobile devices and SIM card standards (e.g., GSM, CDMA).
    - Additionally, newer technologies such as embedded SIMs (eSIMs) and secure elements introduce complexities that may require specialized expertise and tools for forensic analysis.



MobileCheckV4

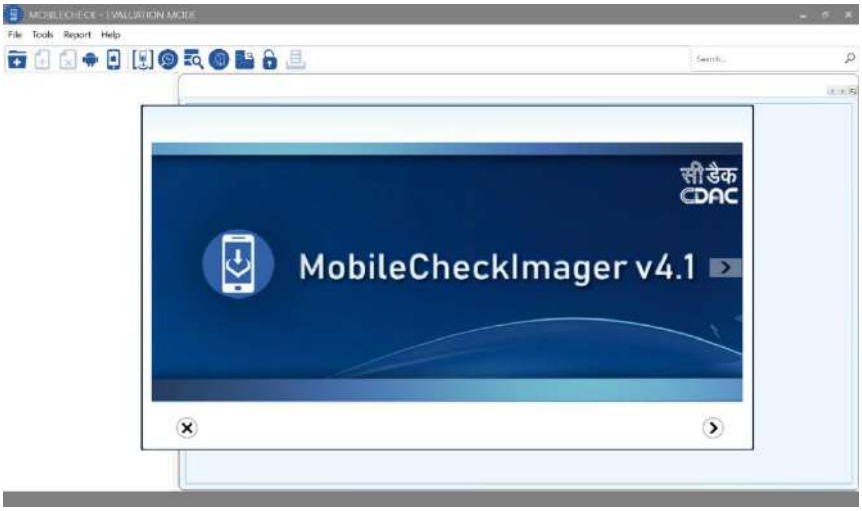
In digital forensics, mobile data can be acquired from devices through two primary methods: physical acquisition and logical acquisition. Physical acquisition involves extracting a complete image of the device's storage, capturing all data stored on it, including system files, deleted data, and hidden partitions. For instance, in the case mentioned, a physical acquisition of a 128GB device would entail capturing the entire 128GB of data, covering all aspects of the device's storage. On the other hand, logical acquisition focuses on obtaining specific user data and files without capturing the entire storage image. This method is often used when the investigation requires only certain types of data or when time and resources are limited. In the scenario provided, a logical acquisition of the same 128GB device resulted in the capture of 39GB of data, representing a subset of the device's contents that are relevant to the investigation. Logical acquisitions are typically faster and more targeted compared to physical acquisitions, making them suitable for many forensic investigations.

We first need to enable developer options and root the phone in order to perform these steps.

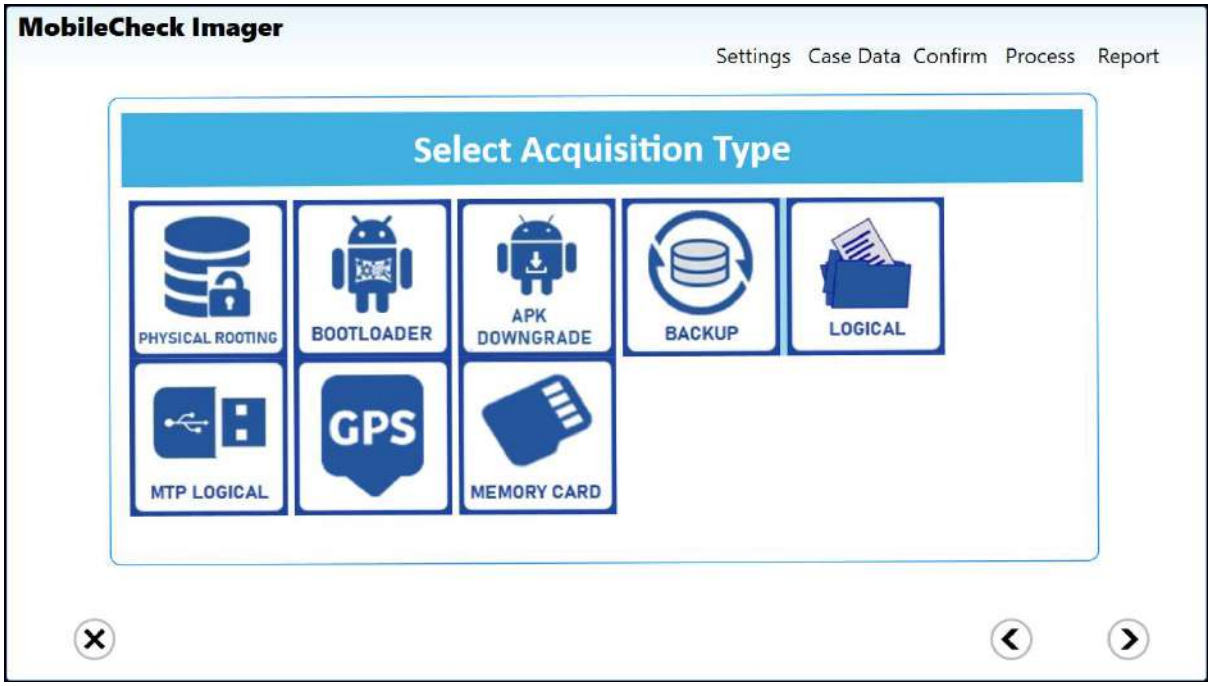
Steps -

- Go to logical
- Select android
- Connect your phone
- Select what you want to import e.g. calls, sms etc
- Next fill the details - hash type and select location where it will be stored (.pmg extension file)
- Click confirm as connect
- By doing this we are acquiring calls, sms, mms etc
- Now image will be generated - there will be 2 files - 1. Html in which report will be there and 2. pmg file

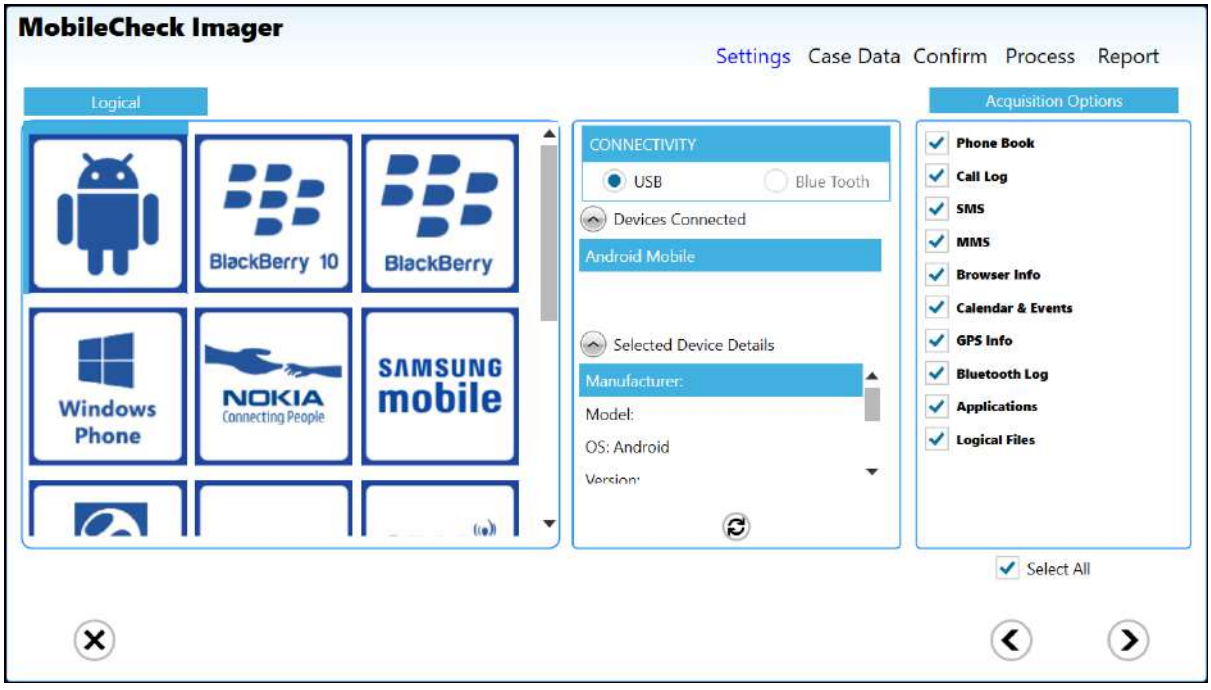
Now in mobile check we need to add image file using new case option there will be review screen displaying timestamp also and then we can see acquired data.



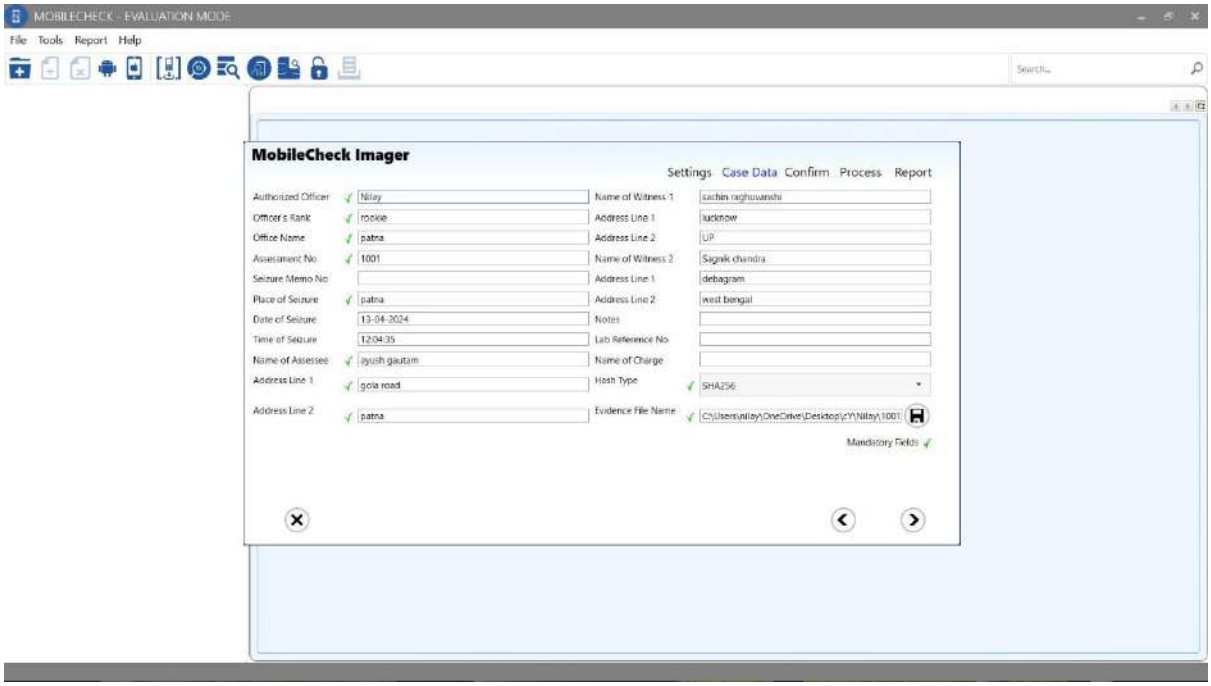
Select a acquisition type



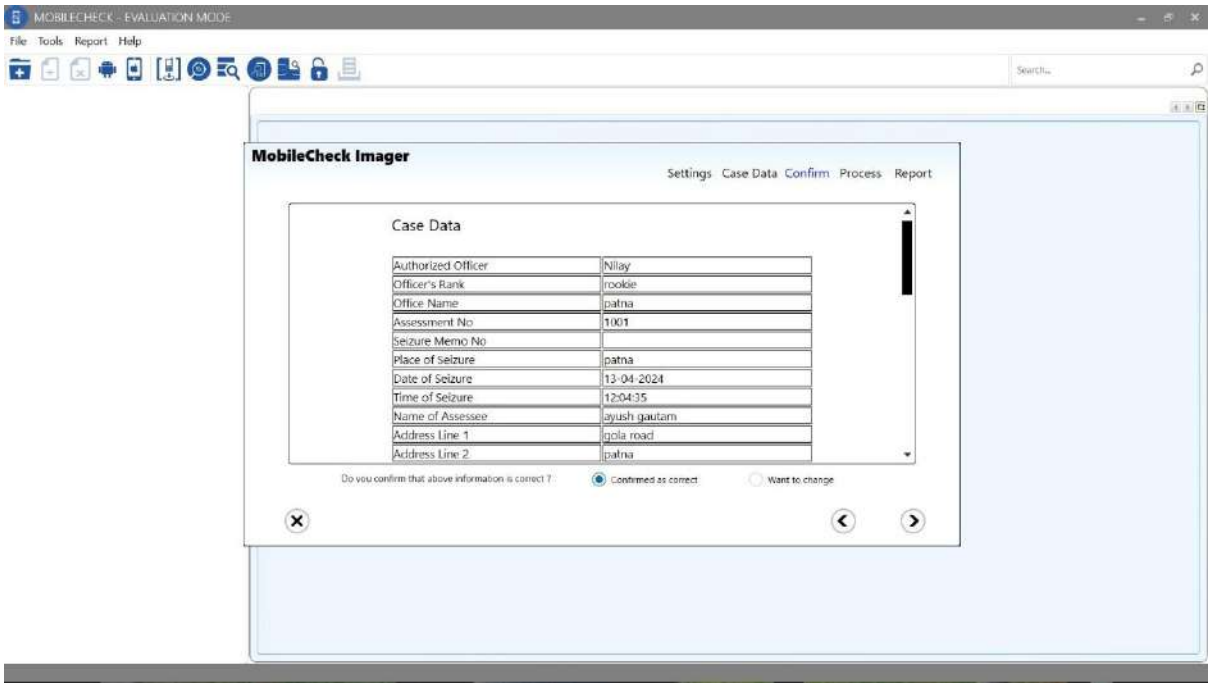
Select a device type

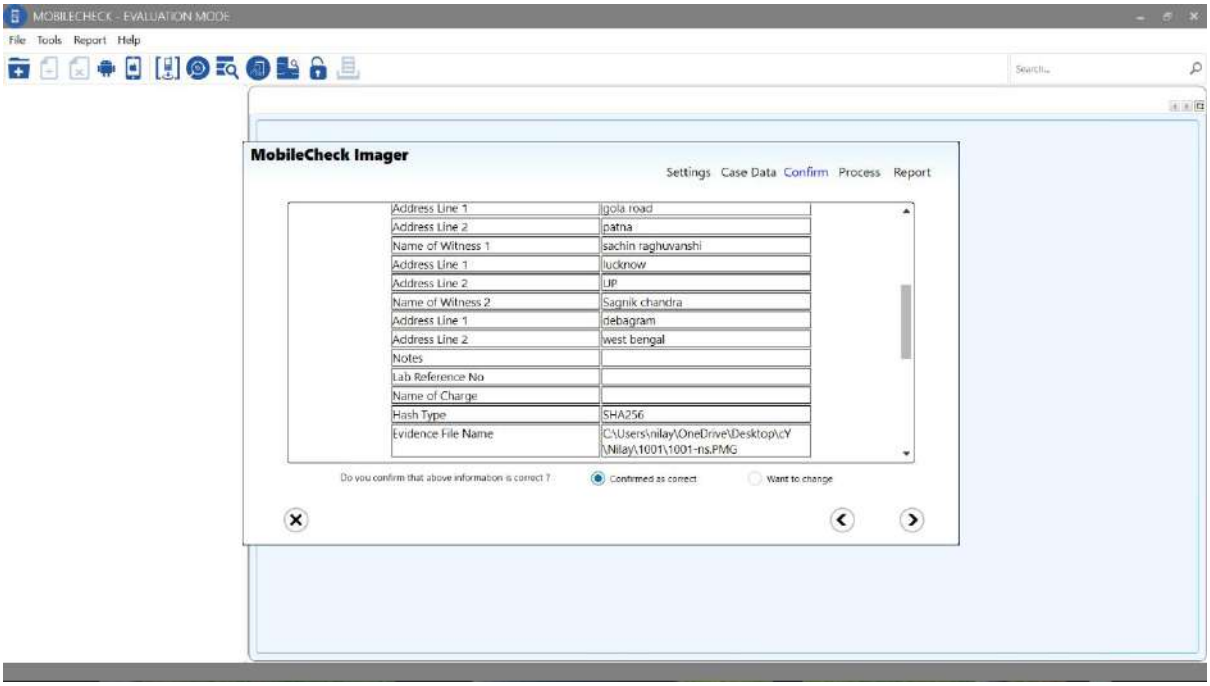


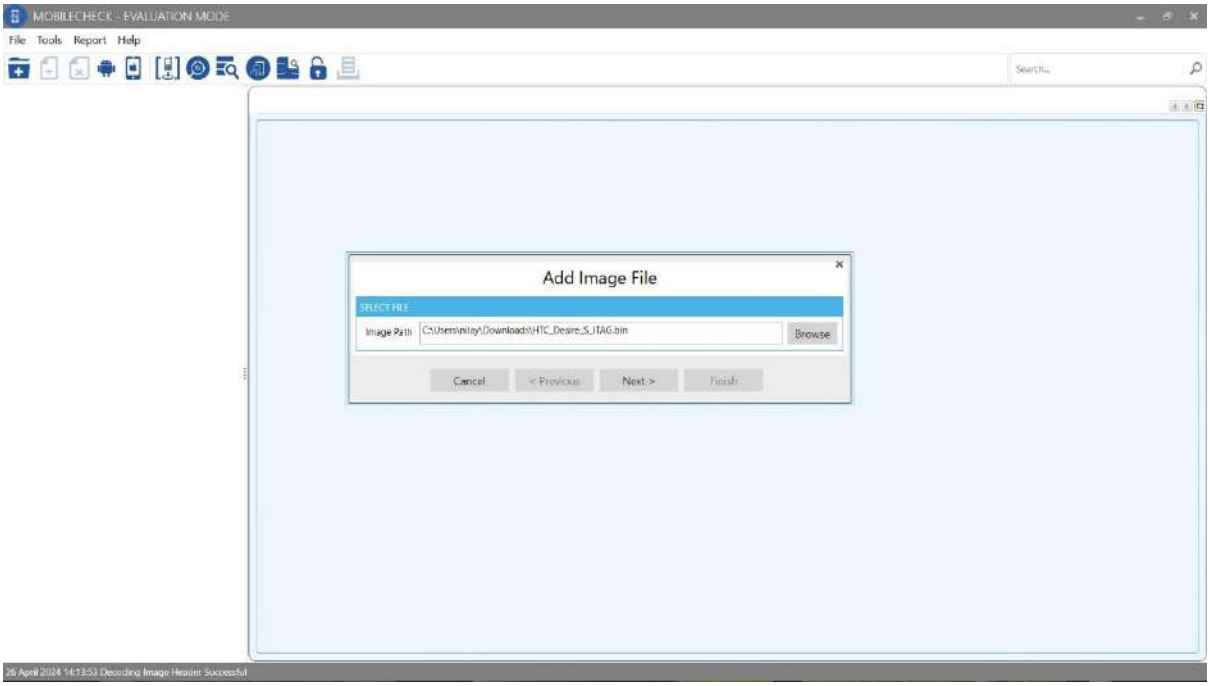
Enter case detail

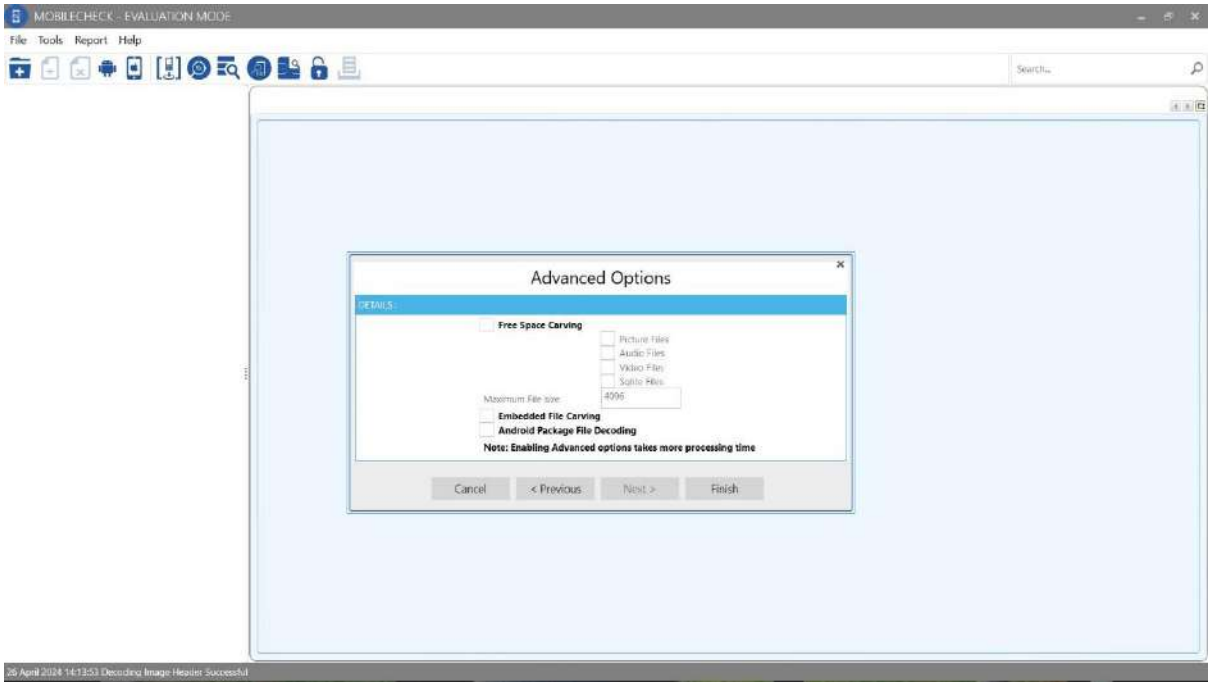


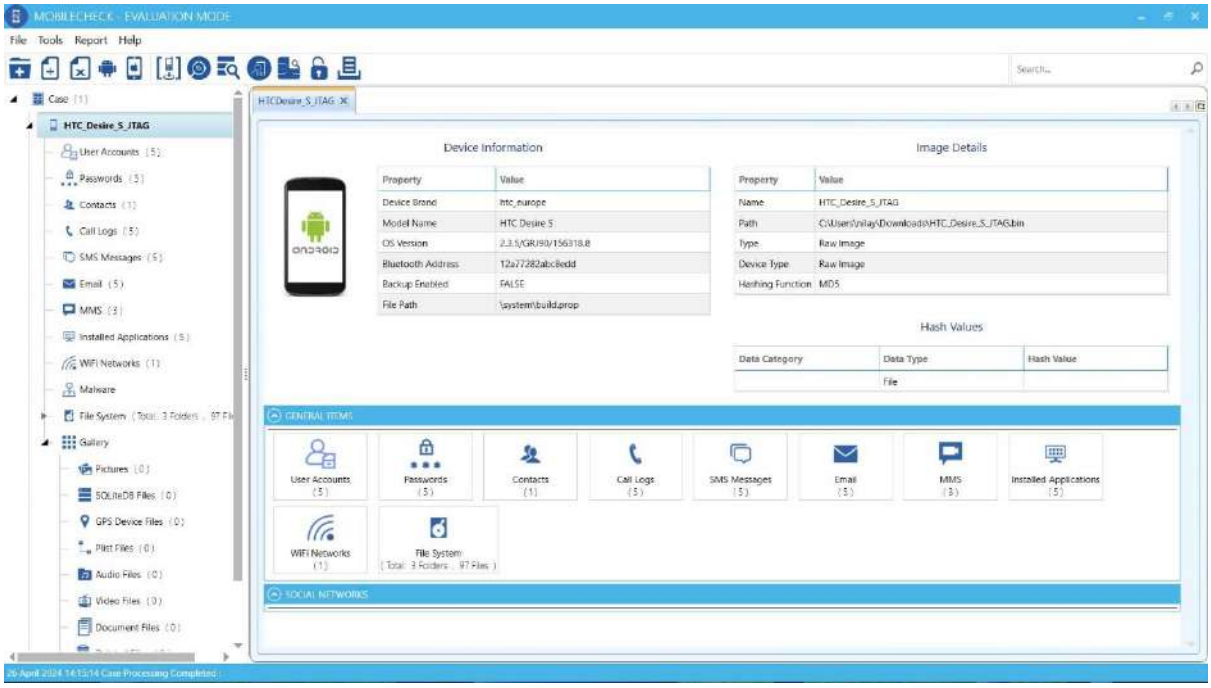
Review case data

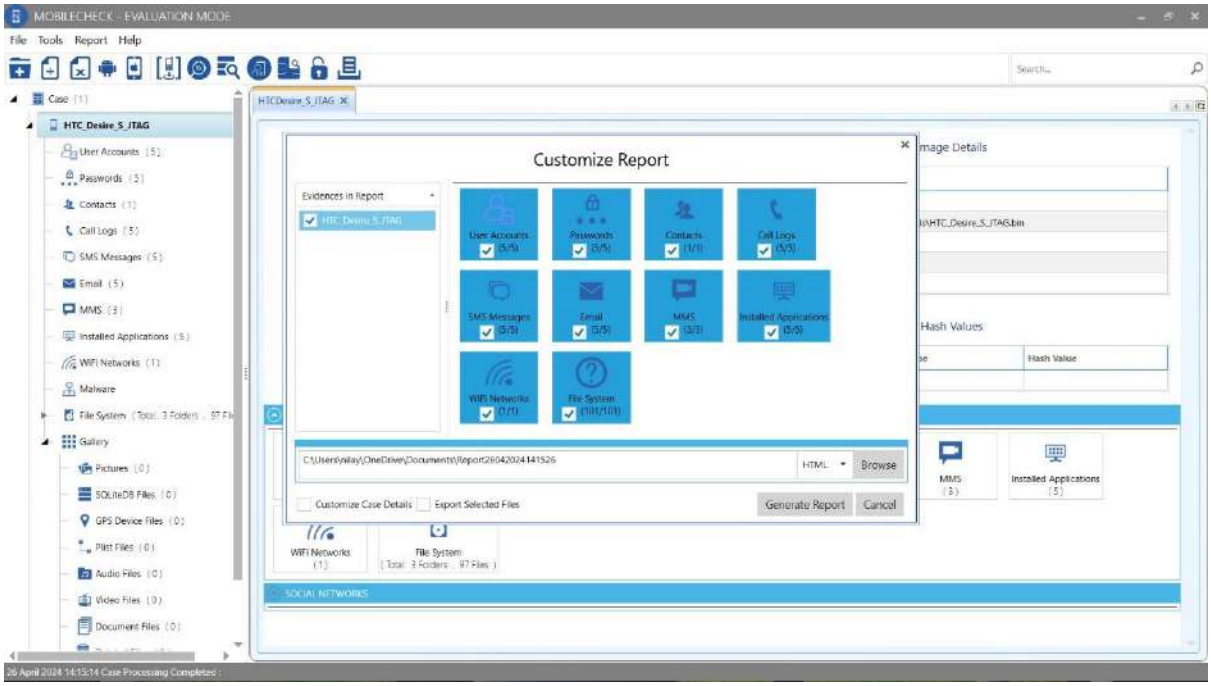



MOBILECHECK - EVALUATION MODE
File Tools Report Help
MobileCheck Imager
Settings Case Data Confirm Process Report
Address Line 1 igola road
Address Line 2 patna
Name of Witness 1 sachin raghuvanshi
Address Line 1 lucknow
Address Line 2 UP
Name of Witness 2 Sagnik chandra
Address Line 1 debagram
Address Line 2 west bengal
Notes
Lab Reference No
Name of Charge
Hash Type SHA256
Evidence File Name C:\Users\nilay\OneDrive\Desktop\cY\Nilay\1001\1001-ns.PMG
Do you confirm that above information is correct ?
Confirmed as correct
Want to change

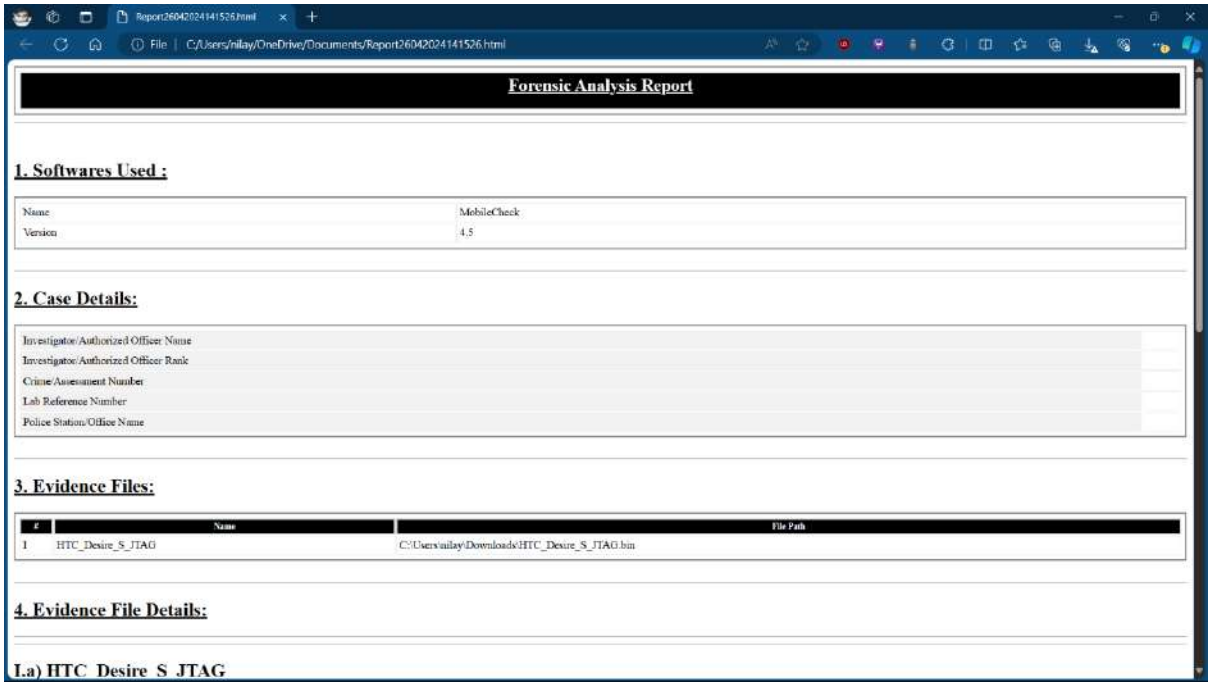

MOBILECHECK - EVALUATION MODE
File Tools Report Help
Add Image File
SELECT FILE
Image Path C:\Users\nilay\Downloads\HTC_Desire_S_JTAG.bin
Browse
Cancel
< Previous
Next >
Finish
26 April 2024 14:13:53 Decoding Image Header Successful

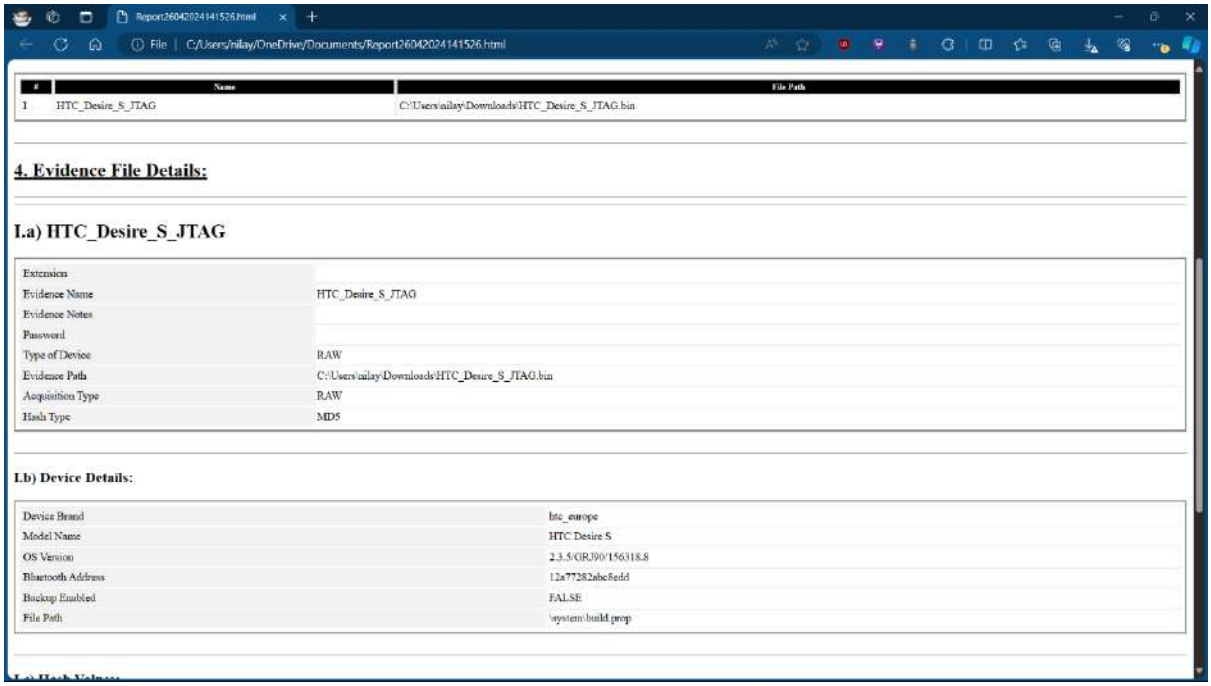

MOBILECHECK - EVALUATION MODE
File Tools Report Help
Search...
Advanced Options
DETAILS
Free Space Carving
Picture Files
Audio Files
Video Files
Sqlite Files
Maximum File size
4096
Embedded File Carving
Android Package File Decoding
Note: Enabling Advanced options takes more processing time
Cancel
< Previous
Next >
Finish
26 April 2024 14:13:53 Decoding Image Header Successful


MOBILECHECK - EVALUATION MODE
File Tools Report Help
Search...
Case (1)
HTC_Desire_S_JTAG
User Accounts (5)
Passwords (5)
Contacts (1)
Call Logs (5)
SMS Messages (5)
Email (5)
MMS (3)
Installed Applications (5)
WiFi Networks (1)
Malware
File System (Total: 3 Folders , 97 Fil
Gallery
Pictures (0)
SQLiteDB Files (0)
GPS Device Files (0)
Plist Files (0)
Audio Files (0)
Video Files (0)
Document Files (0)
HTCDesire_S_JTAG
Device Information
Property
Value
Device Brand
htc_europe
Model Name
HTC Desire S
OS Version
2.3.5/GRJ90/156318.8
Bluetooth Address
12a77282abc8edd
Backup Enabled
FALSE
File Path
\system\build.prop
Image Details
Property
Value
Name
HTC_Desire_S_JTAG
Path
C:\Users\vijay\Downloads\HTC_Desire_S_JTAG.bin
Type
Raw Image
Device Type
Raw Image
Hashing Function
MD5
Hash Values
Data Category
Data Type
Hash Value
File
GENERAL ITEMS
User Accounts (5)
Passwords (5)
Contacts (1)
Call Logs (5)
SMS Messages (5)
Email (5)
MMS (3)
Installed Applications (5)
WiFi Networks (1)
File System (Total: 3 Folders , 97 Files)
SOCIAL NETWORKS
26 April 2024 14:15:14 Case Processing Completed



Required report of the backup file





#	Name	File Path
1	HTC_Desire_S_JTAG	C:\Users\nilay\Downloads\HTC_Desire_S_JTAG.bin

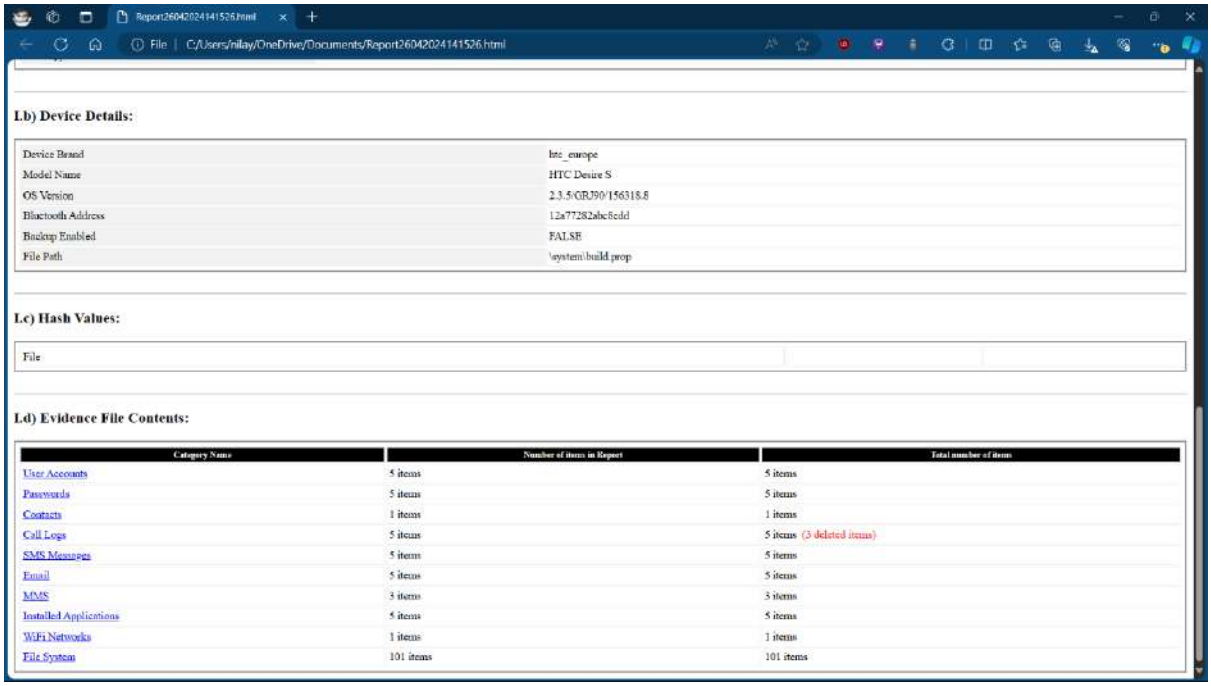
4. Evidence File Details:

I.a) HTC_Desire_S_JTAG

Extension	
Evidence Name	HTC_Desire_S_JTAG
Evidence Notes	
Password	
Type of Device	RAW
Evidence Path	C:\Users\nilay\Downloads\HTC_Desire_S_JTAG.bin
Acquisition Type	RAW
Hash Type	MD5

I.b) Device Details:

Device Brand	htc_europe
Model Name	HTC Desire S
OS Version	2.3.5/GRJ90/156318.8
Bluetooth Address	12a77282abc8edd
Backup Enabled	FALSE
File Path	\system\build.prop



I.b) Device Details:

Device Brand	htc_europe
Model Name	HTC Desire S
OS Version	2.3.5/GRJ90/156318.8
Bluetooth Address	12a77282abc8edd
Backup Enabled	FALSE
File Path	\system\build.prop

I.c) Hash Values:

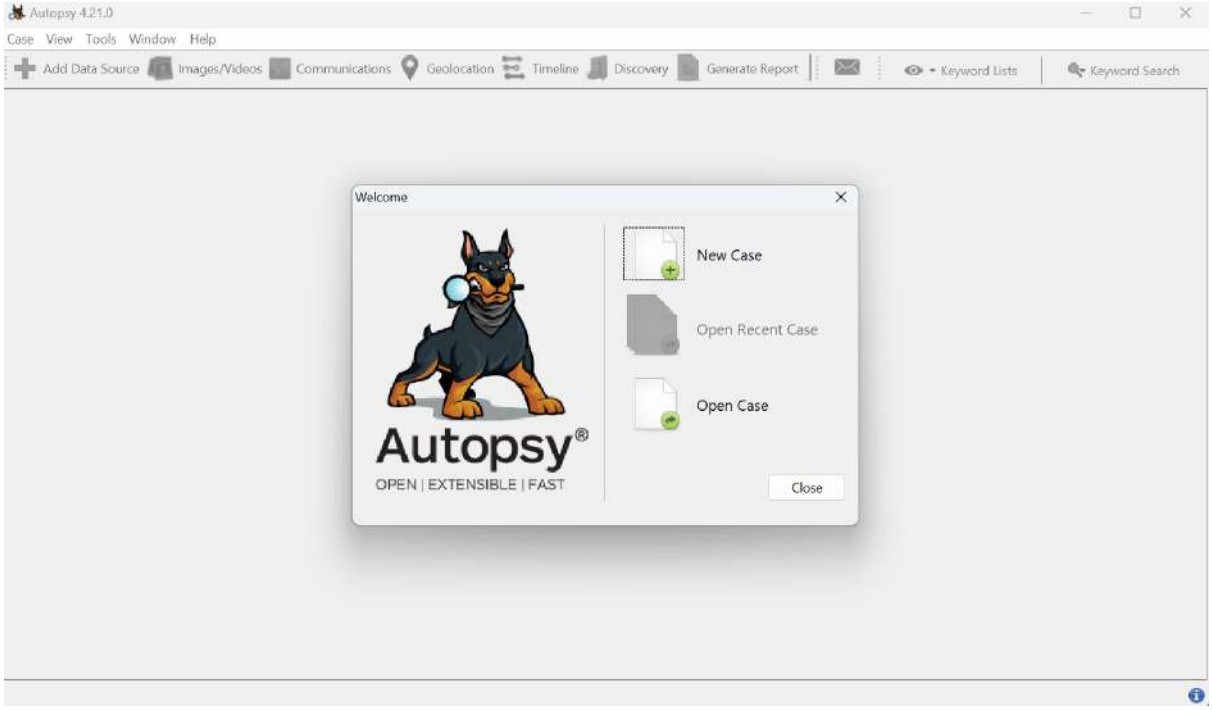
File

I.d) Evidence File Contents:

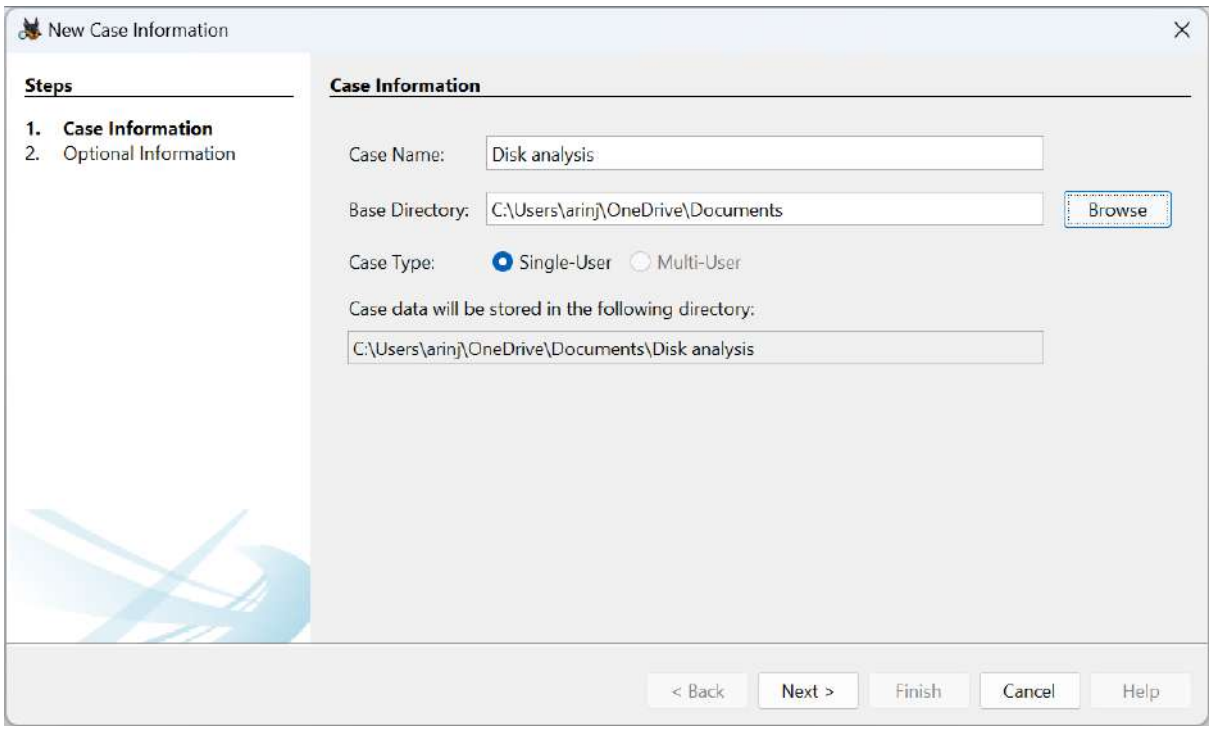
Category Name	Number of items in Report	Total number of items
User Accounts	5 items	5 items
Passwords	5 items	5 items
Contacts	1 items	1 items
Call Logs	5 items	5 items (3 deleted items)
SMS Messages	5 items	5 items
Email	5 items	5 items
MMS	3 items	3 items
Installed Applications	5 items	5 items
WiFi Networks	1 items	1 items
File System	101 items	101 items

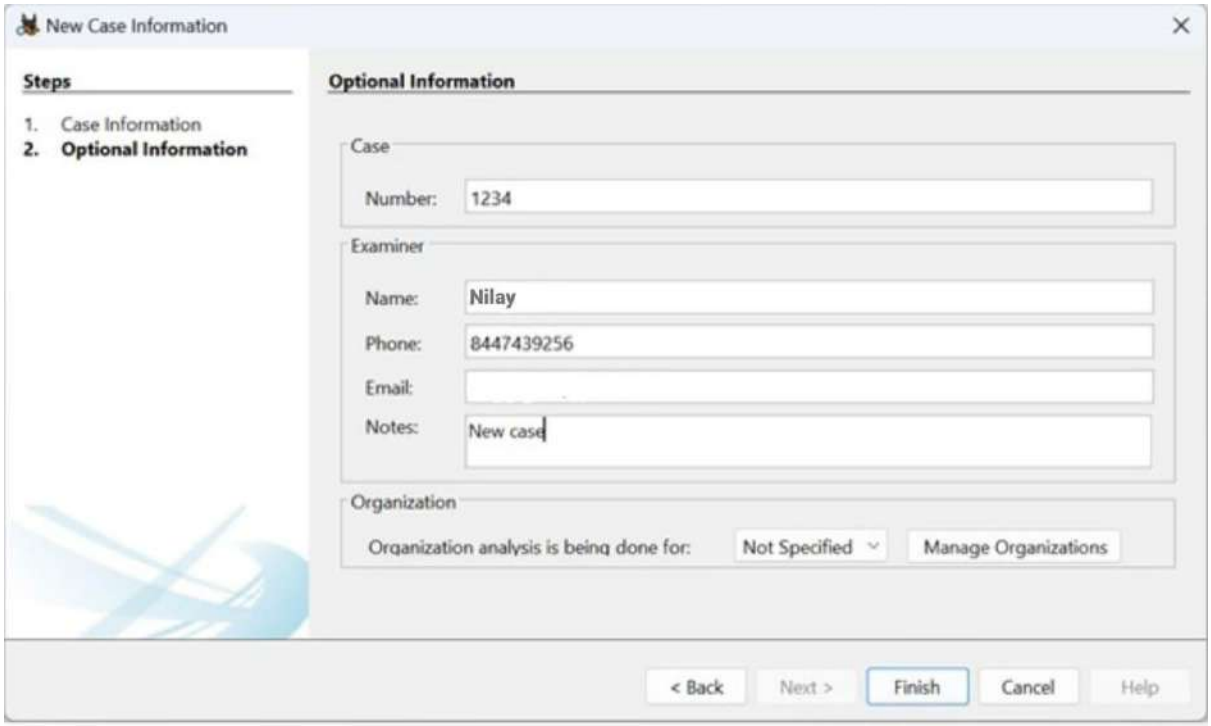
Steps to follow to operate Autopsy

- ***Open autopsy and create a new Case***

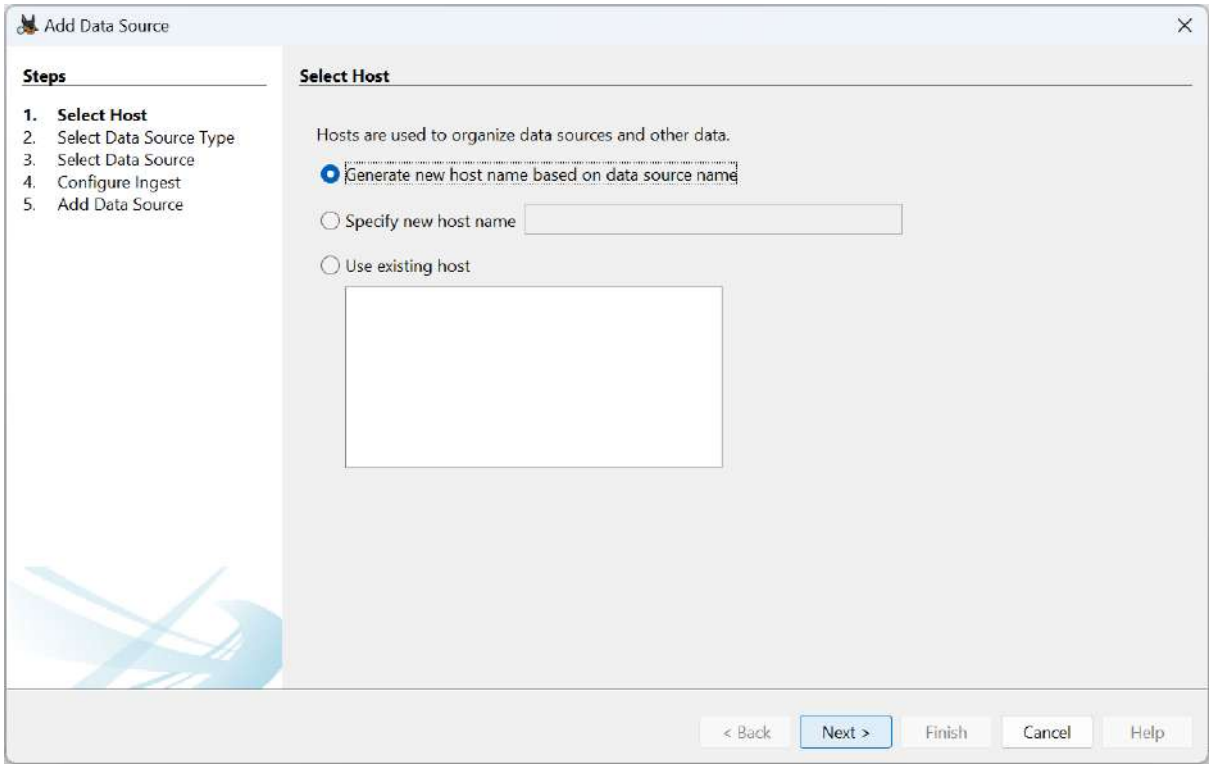


- **Enter Case information**

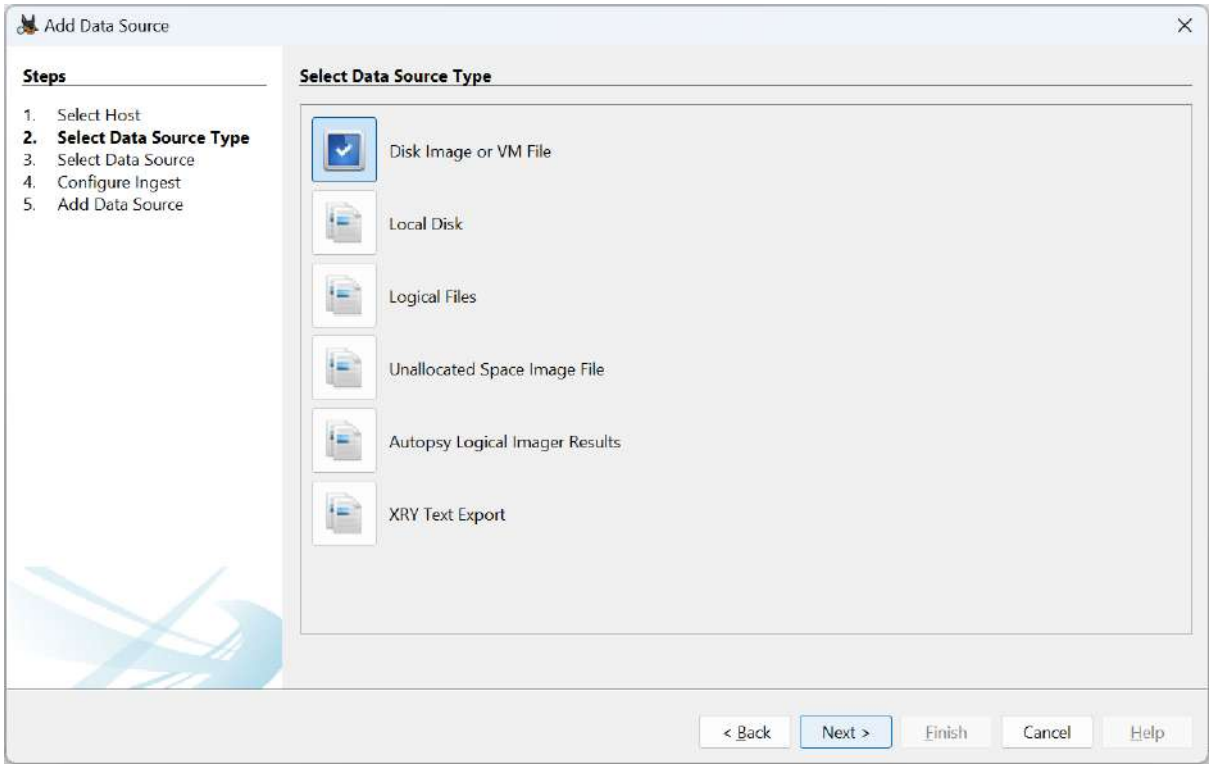



New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 1234
Examiner
Name: Nilay
Phone: 8447439256
Email:
Notes: New case
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

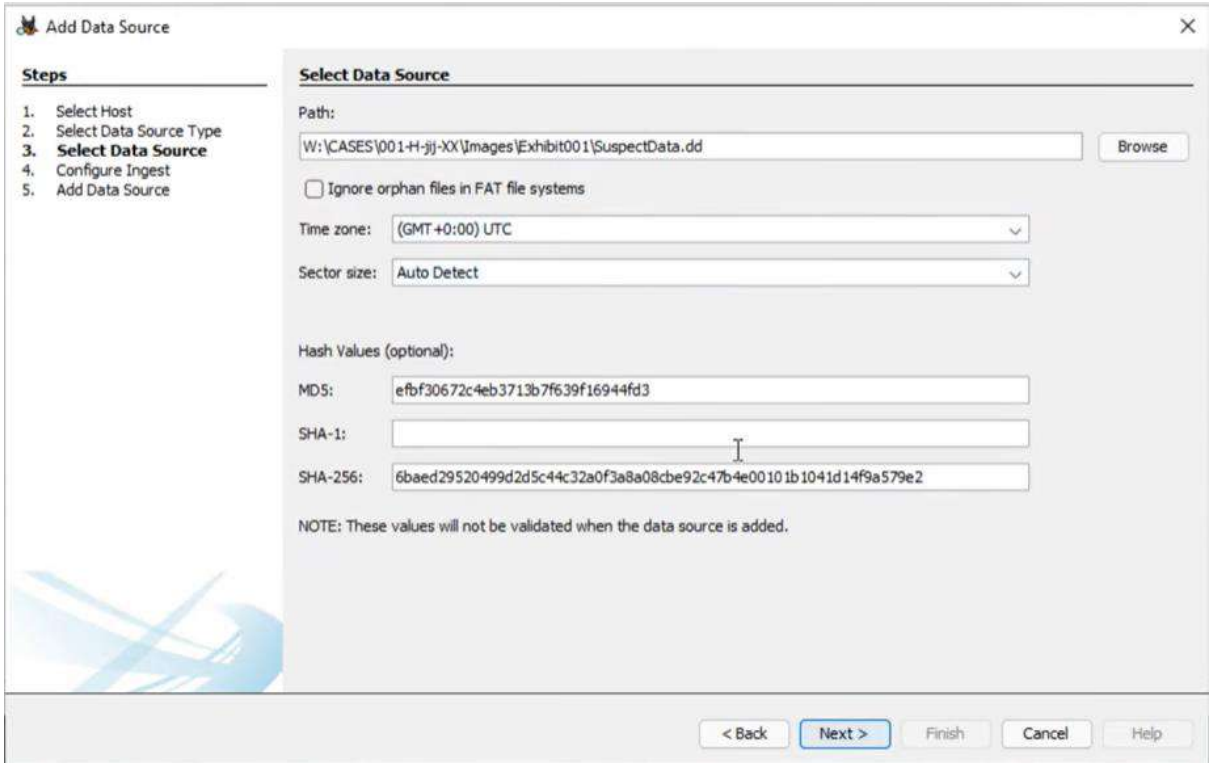
➢ ***Select Host***


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

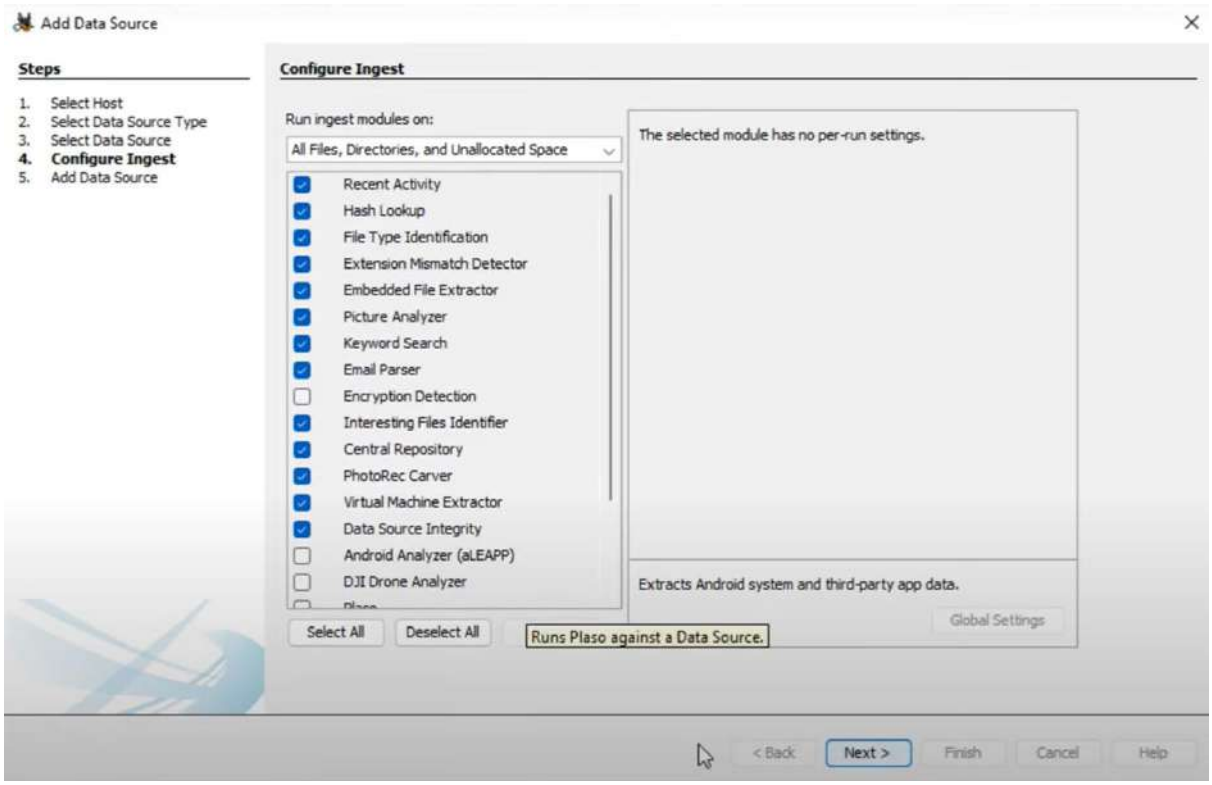
➢ ***Select the appropriate data source type***



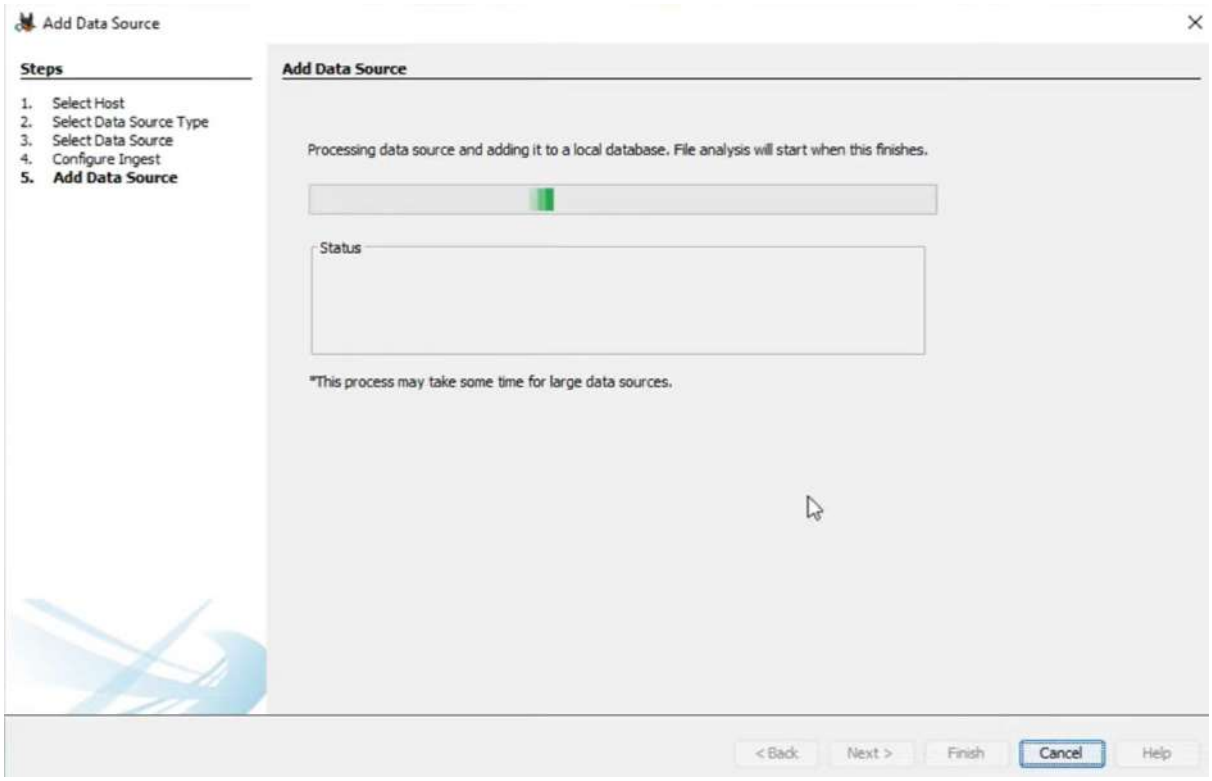
➢ ***Select data source location and enter the hash values.***



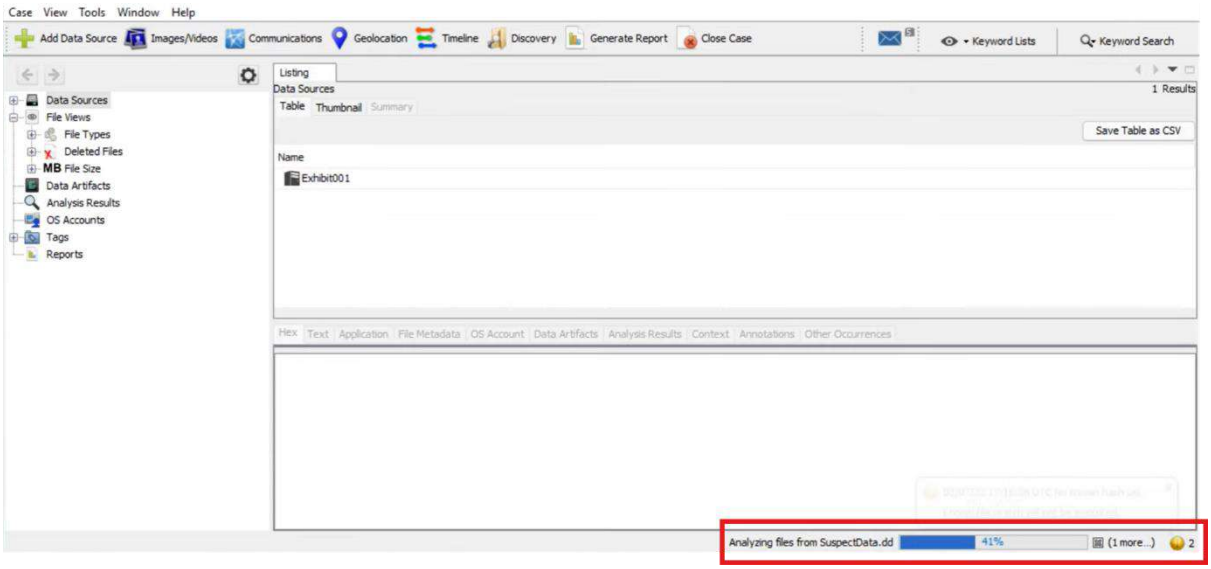
➢ *Configure the ingest*



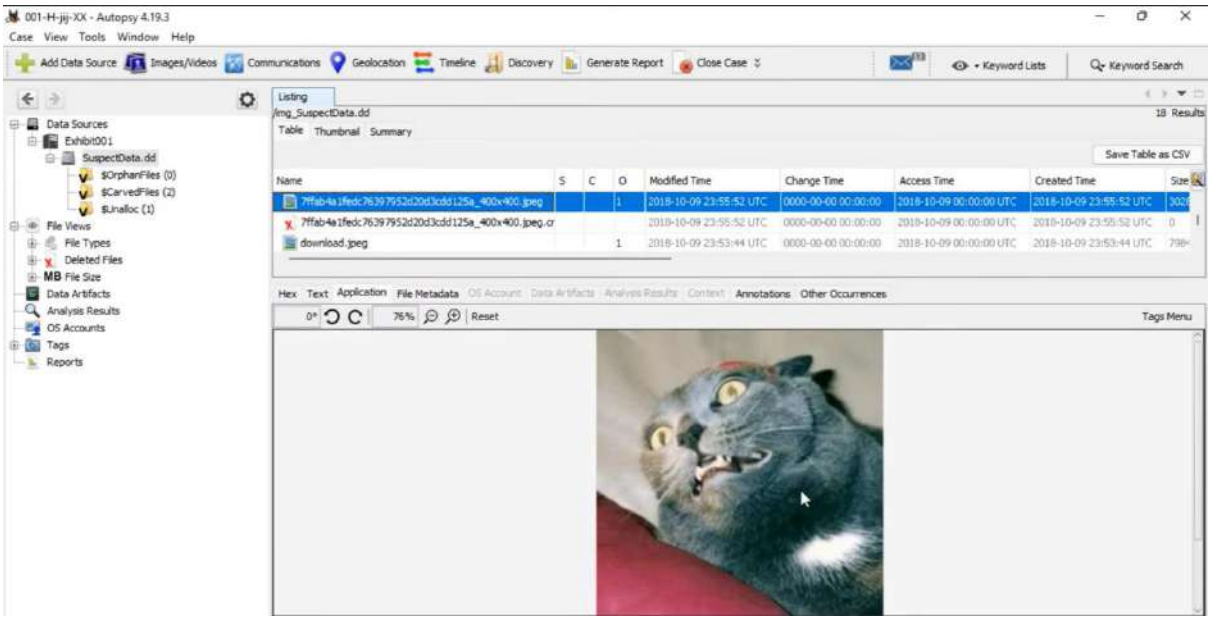
➢ *Add data source*



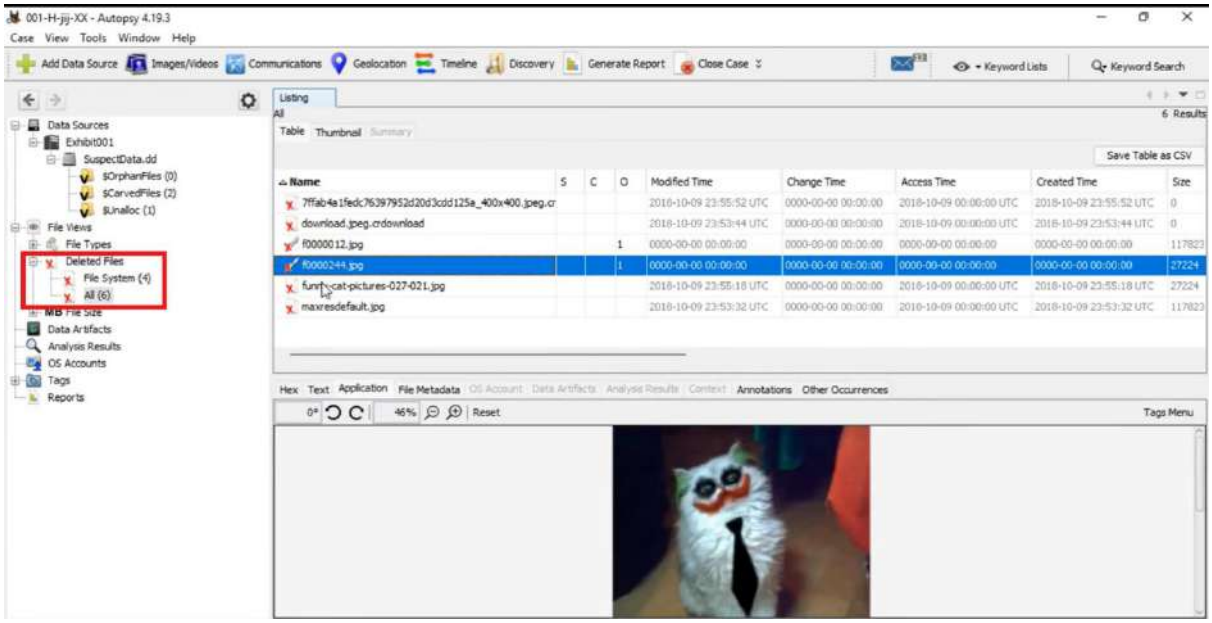
➢ ***Start the analysis***



➢ ***Access the files recovered***



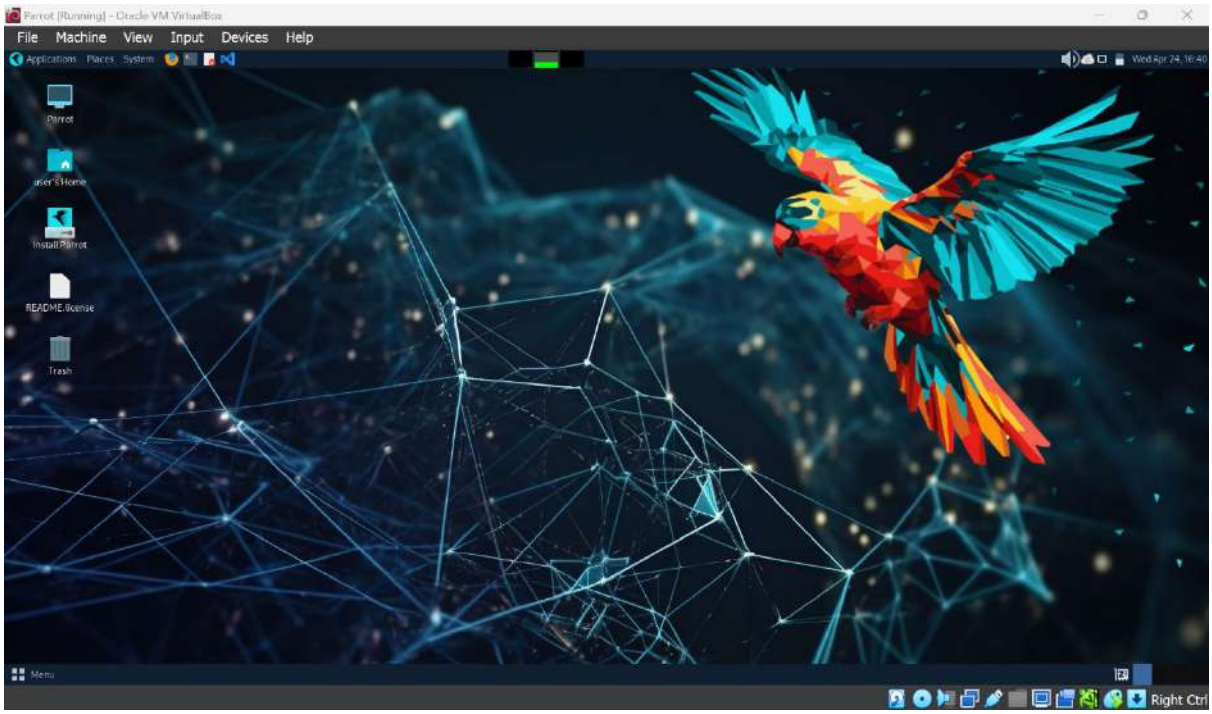
- ***We can also access deleted files***



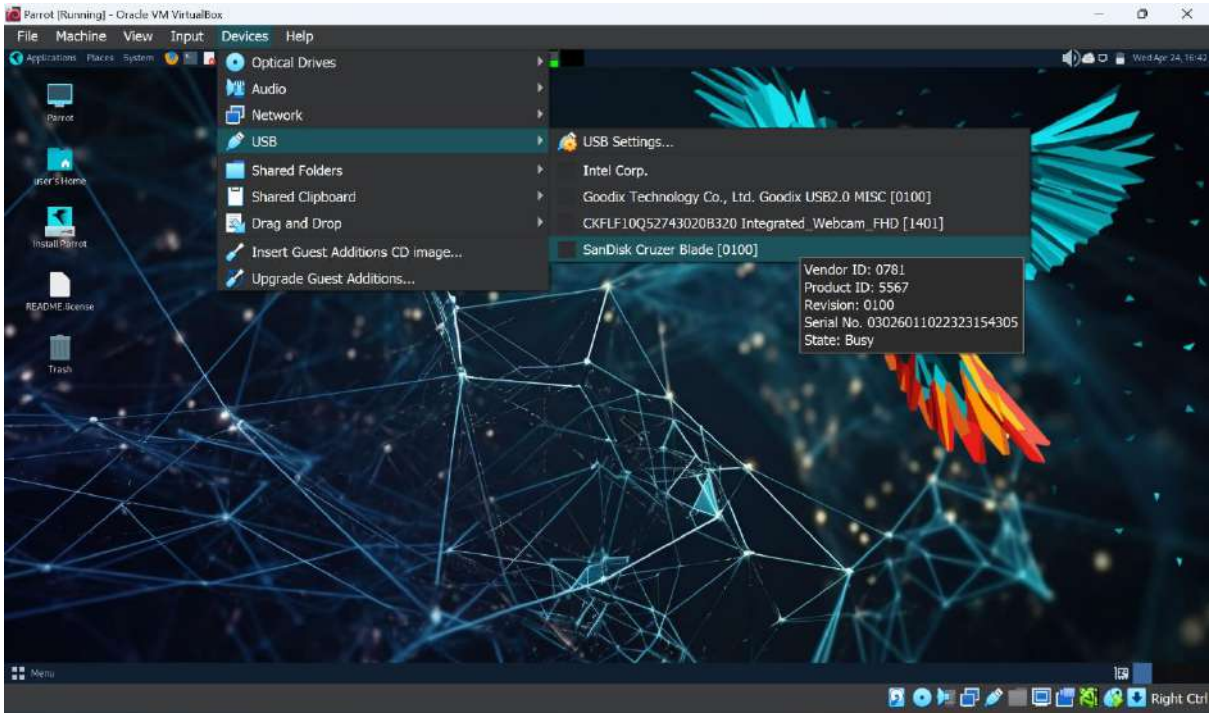
Parrot OS

Parrot OS is a unique and versatile Linux distribution that has gained popularity among cybersecurity professionals, enthusiasts, and privacy-conscious users. It's designed to provide a platform for various security tasks, including penetration testing, digital forensics, and reverse engineering.

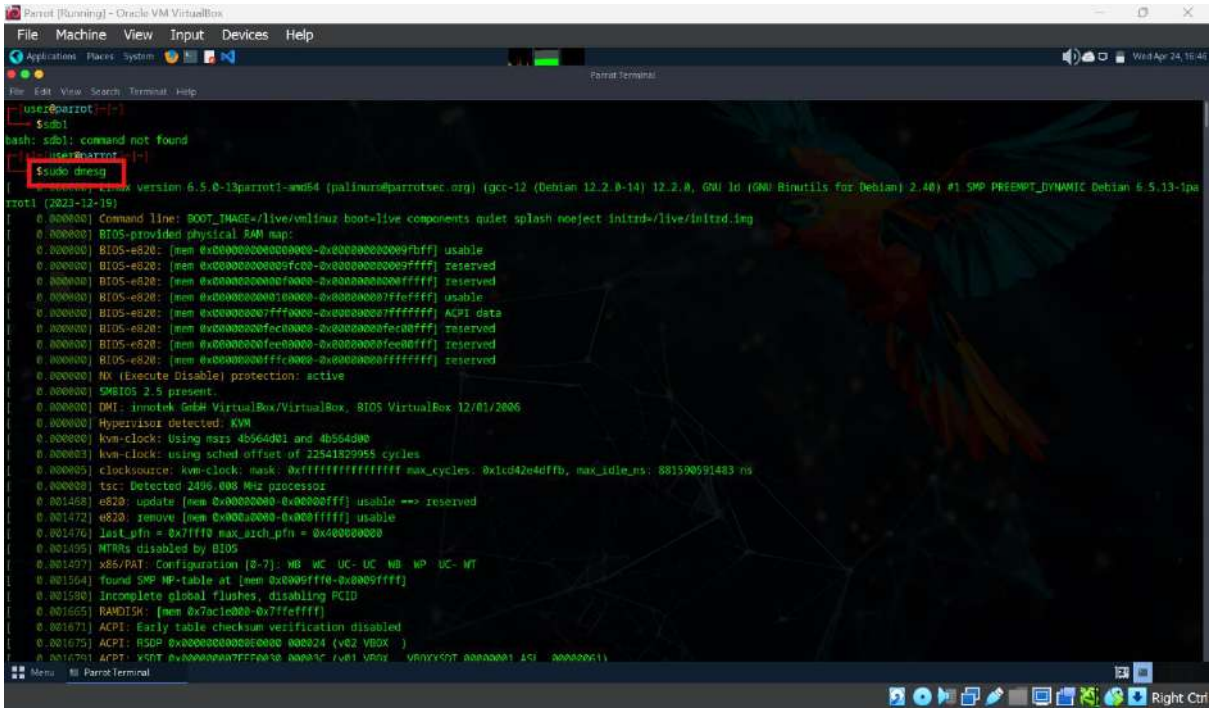
Interface of Parrot OS – (run using VM Box by Oracle)



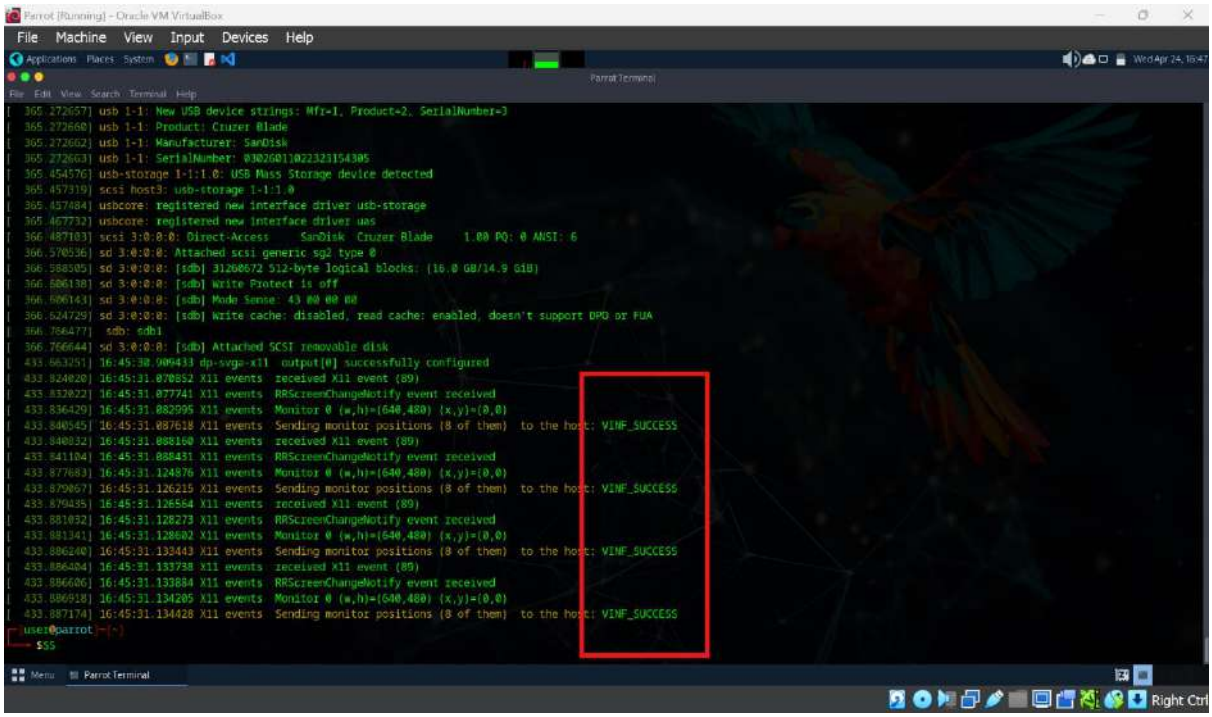
- *Go to devices -> USB -> Select the connected USB device*



- *Now go to terminal and type commands*
  Sudo dmesg – (dmesg is a kernel buffer)



Success message –



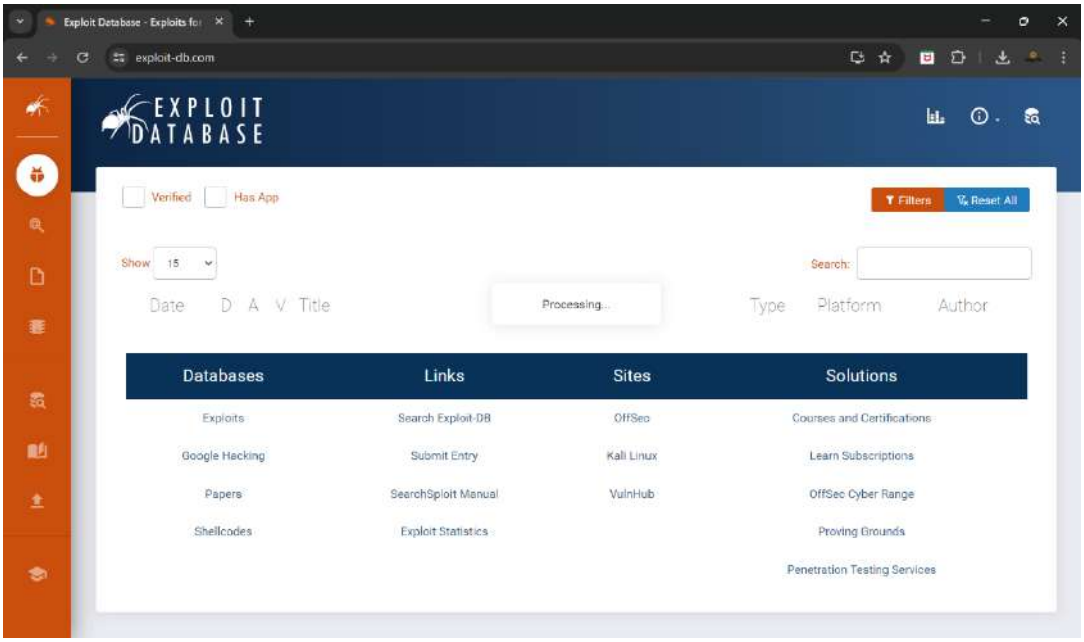
Sdb1 is in the USB and we need to hash it –

sudo md5sum /dev/sdb1

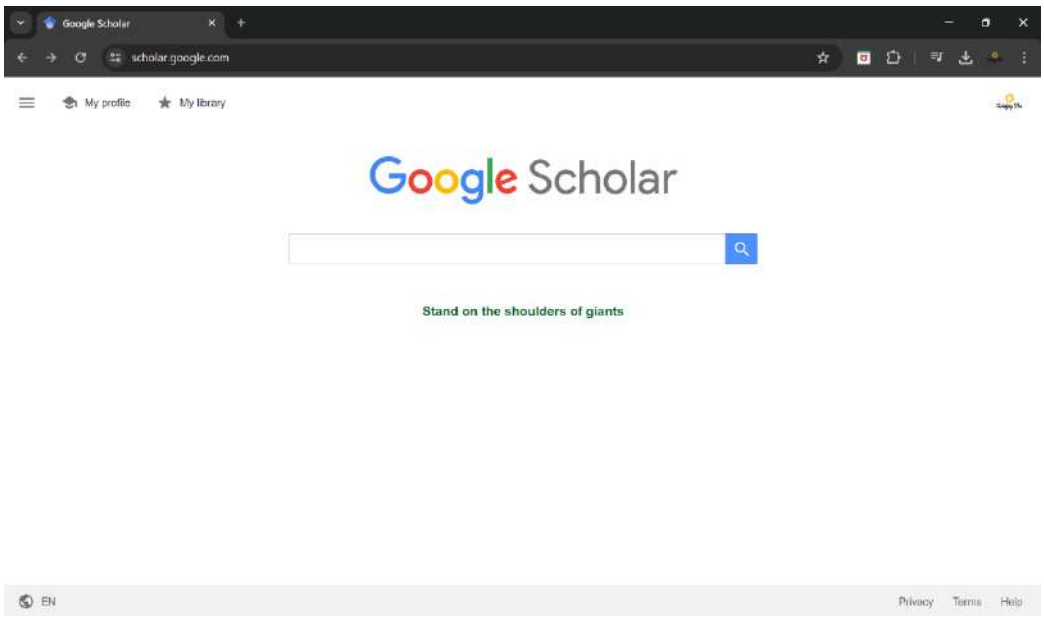
Hash value obtained –

Important websites and tools

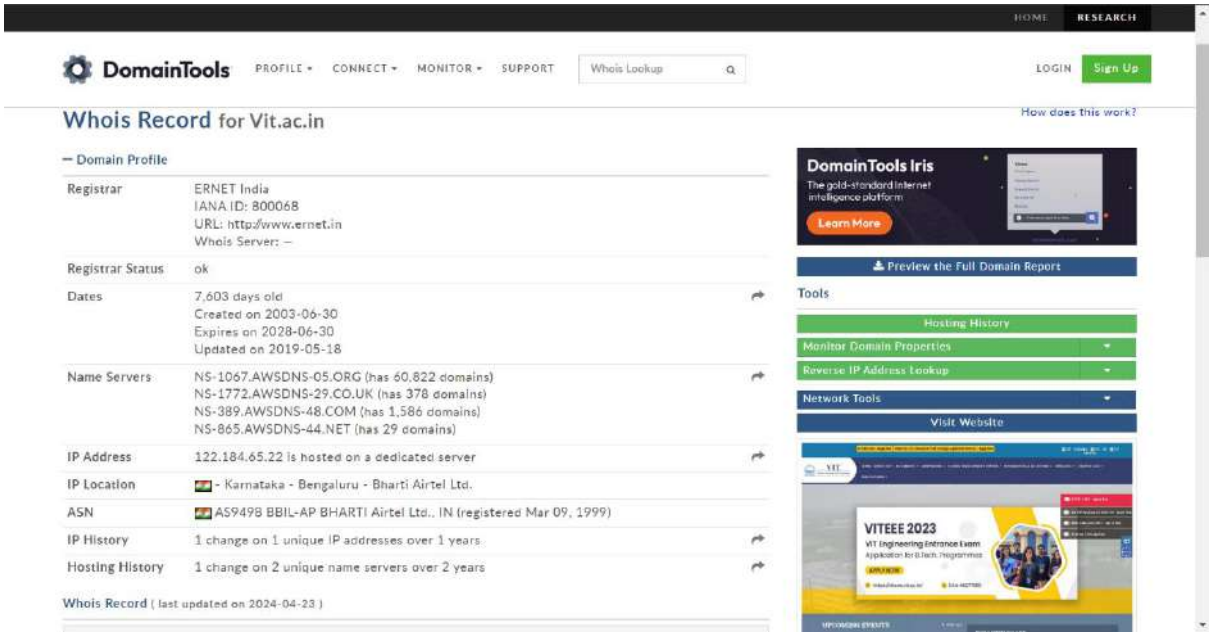
6. ***Google Hacking Database - The [Google Hacking Database (GHDB)]*** on Exploit Database is a collection of search queries, or "dorks," that are used to find publicly available information on the internet. These dorks are intended for use by penetration testers and security researchers to find potential vulnerabilities and misconfigurations in systems.



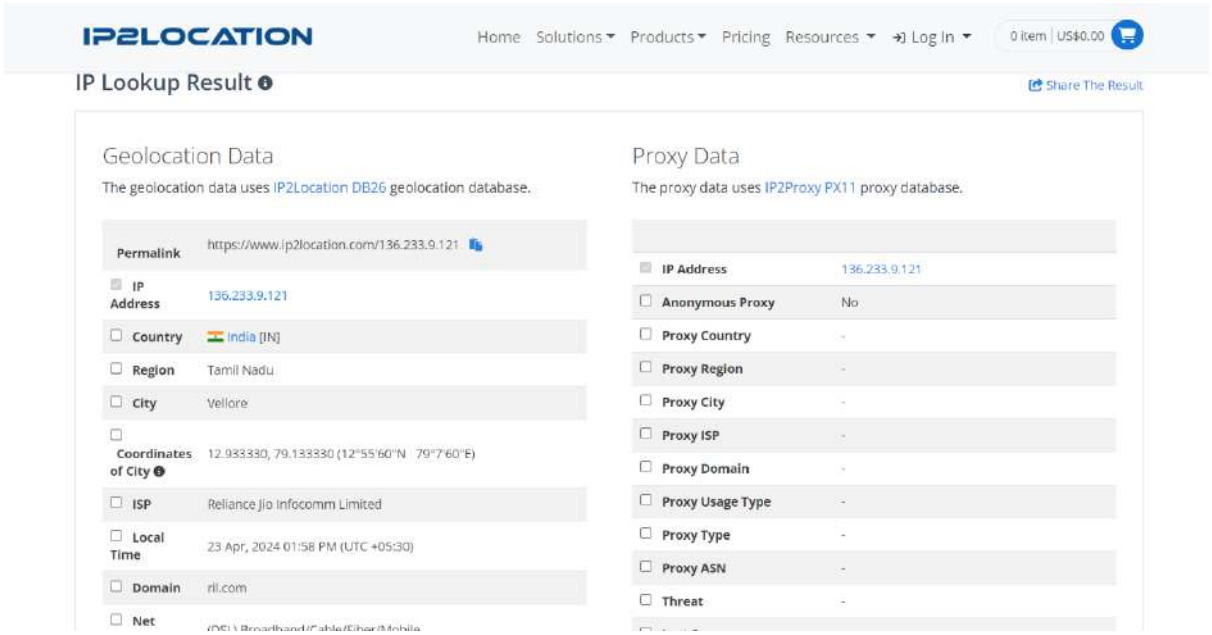
7. ***Google Scholar – Google Scholar*** is a freely accessible web search engine that indexes the full text or metadata of scholarly literature across an array of publishing formats and disciplines.



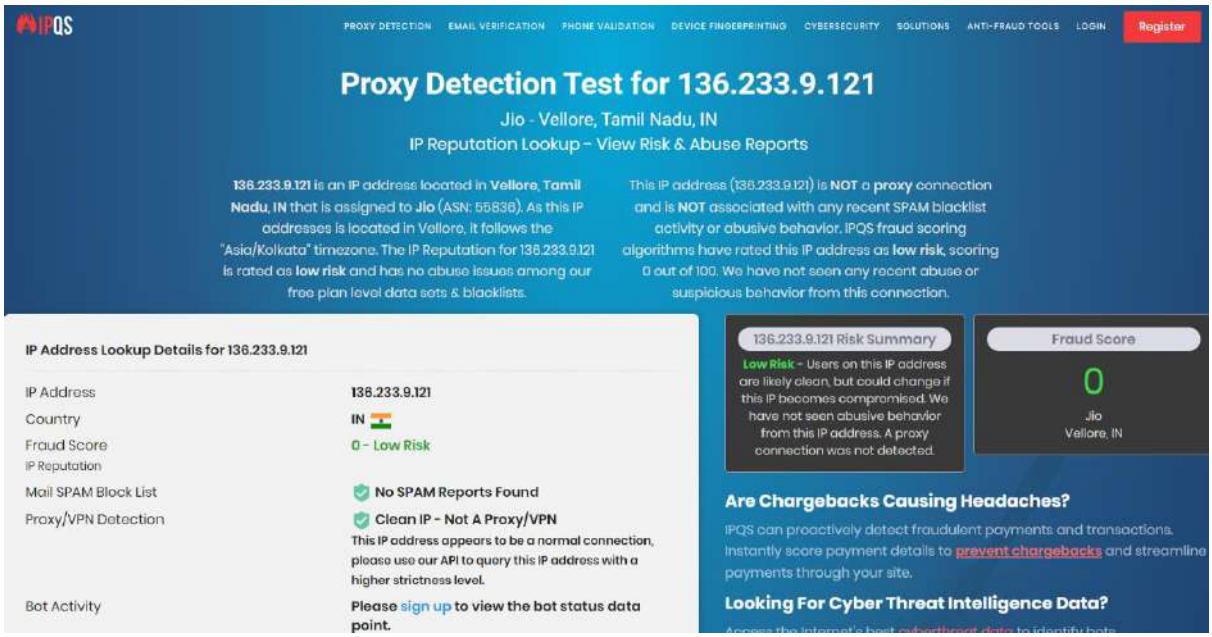
8. ***[Whois.domaintools.com]*** is a tool that allows you to research domain ownership. It provides information such as ownership info, IP address history, rank, traffic, SEO, and more. It can also help find available domains and domains for sale.



9. ***[IP2Location.com]*** is a non-intrusive IP location lookup technology that retrieves geolocation information without explicit permission required from users. It supports both IPv4 and IPv6 and provides precise IP geolocation information using IP database, REST API, and SDK.

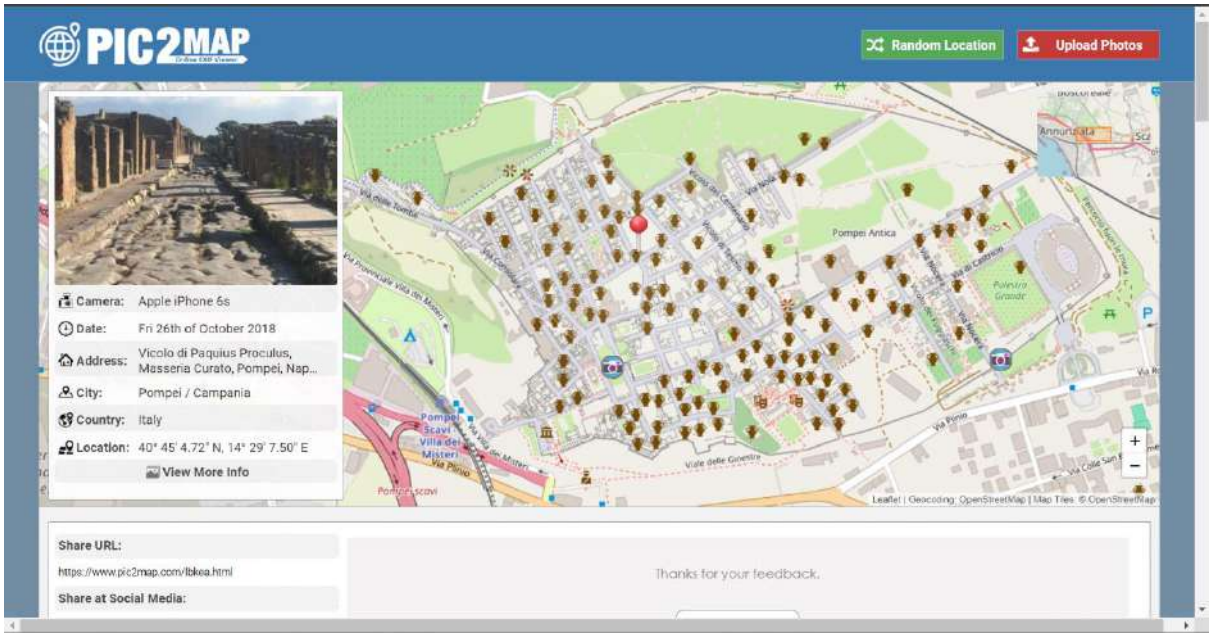


10. ***ipqualityscore.com –*** IPQualityScore.com is an online platform that offers a range of tools and services related to IP address intelligence and fraud prevention. It provides businesses and individuals with valuable insights into the reputation and characteristics of IP addresses, helping them identify and mitigate various types of online fraud, abuse, and security threats.

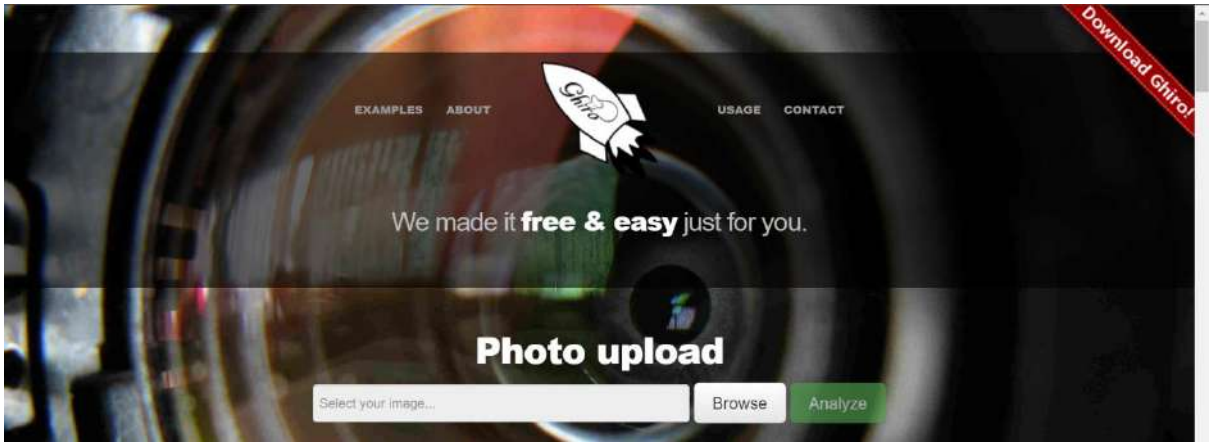


11. ***viewdns.info – [ViewDNS.info]*** is a DNS related tool that provides a variety of services such as reverse IP lookup, domain/IP reverse Whois lookup, IP history, DNS report, reverse MX lookup, reverse NS lookup, IP location finder, and more.

12. ***pic2map.com –*** Pic2Map is a web-based service that allows users to geotag their photos by adding location information to them. Geotagging involves attaching geographical metadata, such as latitude and longitude coordinates, to a photo. This metadata can then be used to pinpoint the exact location where the photo was taken on a map.

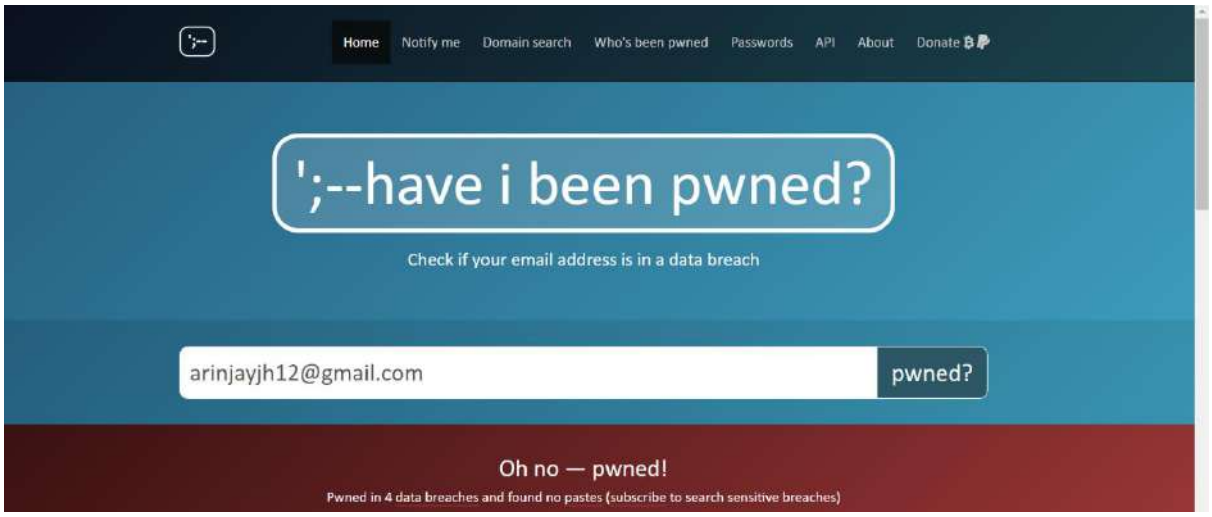


13. ***imageforensic.org – [ImageForensic.org]*** is a digital image forensic analyzer. It provides a service for forensics investigators and security professionals to analyze images for metadata and other information.

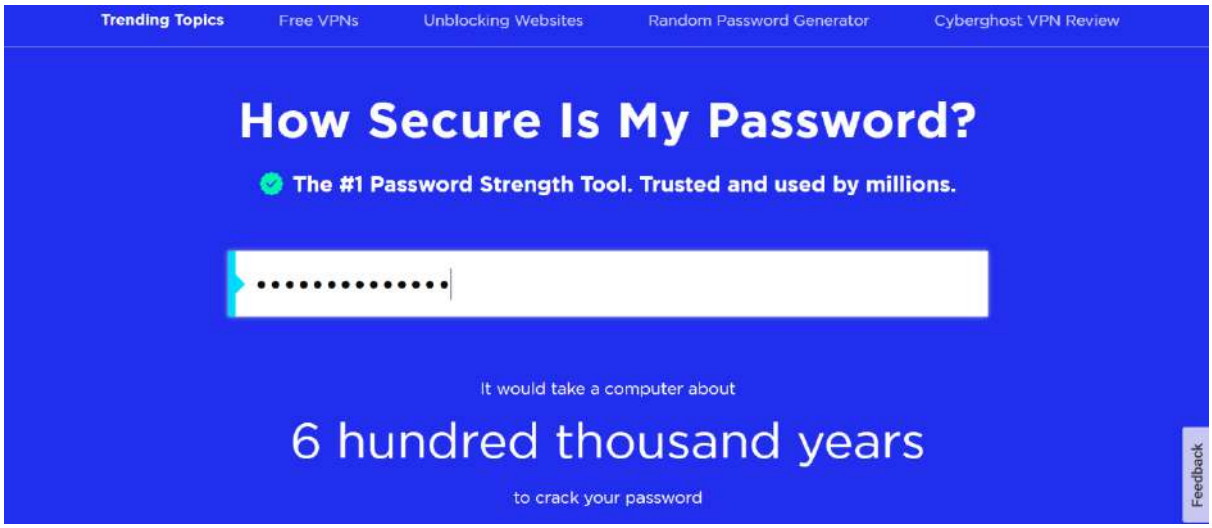


14. ***tineye.com – [TinEye.com]*** is a reverse image search engine that uses image identification technology. It allows users to search for their own information by entering their username or email address. Users can also sign up to be notified if their email address appears in future dumps.

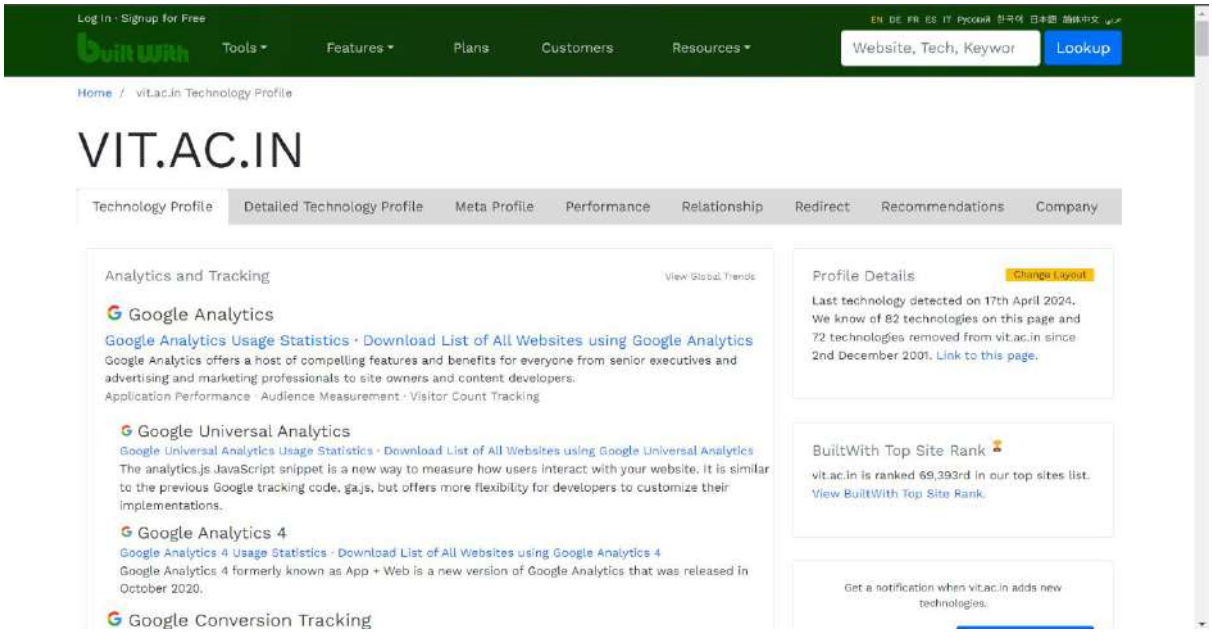
15. ***haveibeenpwned.com – [HaveIBeenPwned.com]*** allows you to search across multiple data breaches to see if your email address or phone number has been compromised. It collects and analyzes hundreds of database dumps and pastes containing information about billions of leaked accounts.



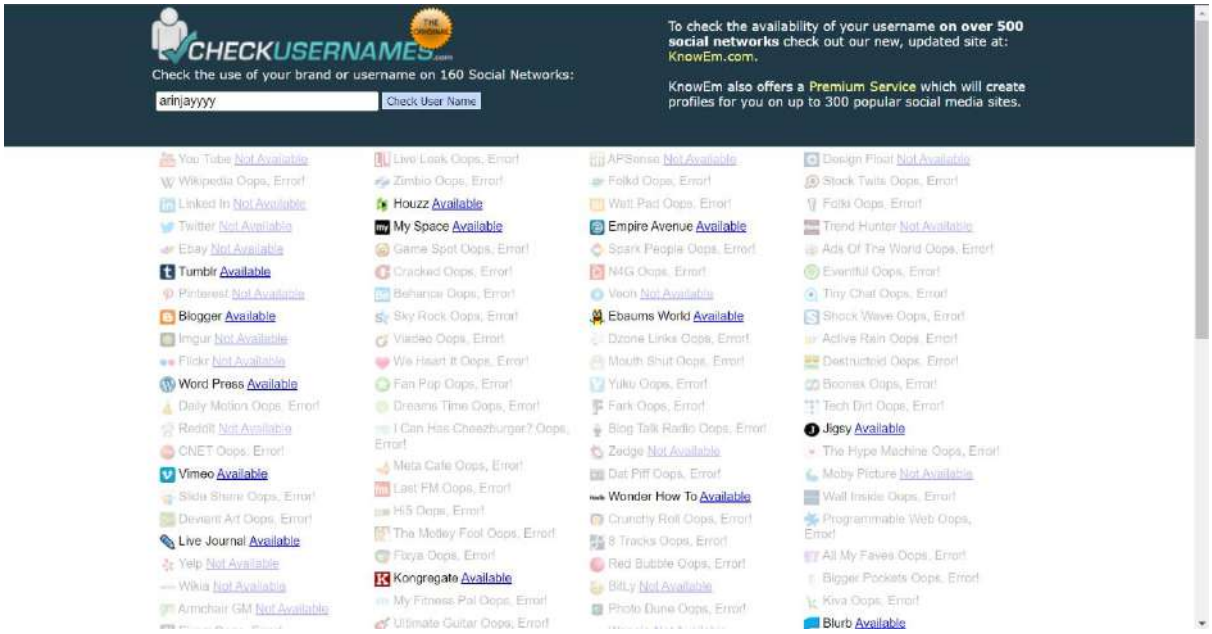
16. ***security.org/how-secure-is-my-password – [Security.org]*** provides a password strength checker tool that checks users' passwords against a database of common weak passwords. It evaluates each password based on key factors such as the number of characters, use of letters, numbers, and characters, and more.



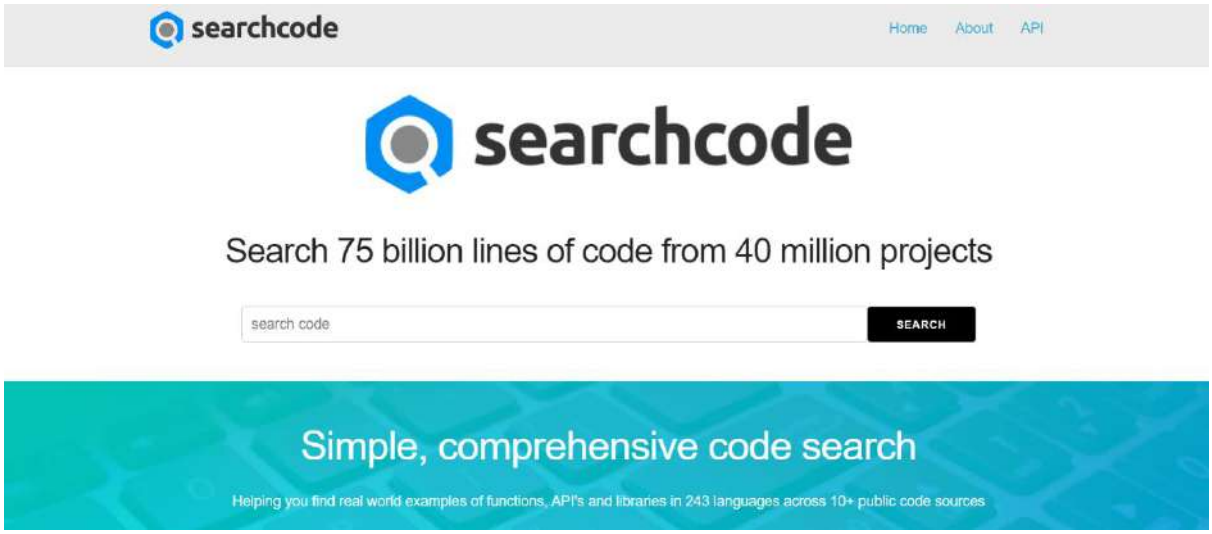
17. ***builtwith.com*** – BuiltWith.com is a powerful online tool designed to provide insights into the technology stack behind websites. It offers a comprehensive database of websites and the technologies they utilize, ranging from content management systems (CMS) and web frameworks to analytics tools, advertising networks, and much more.



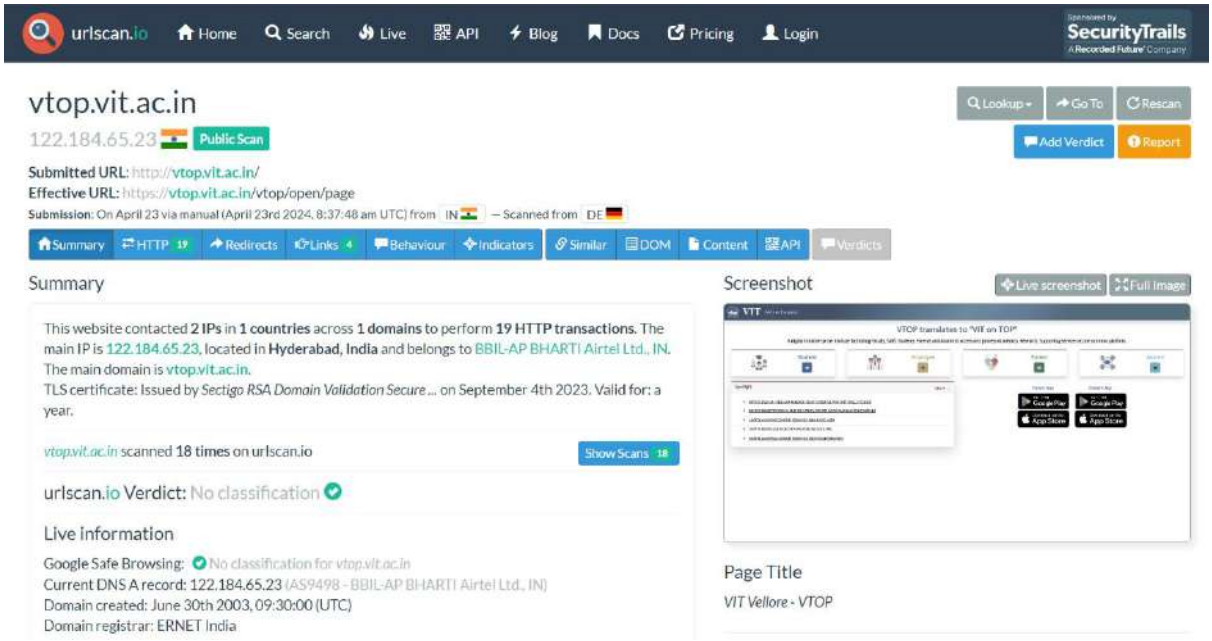
18. ***checkusernames.com –*** Checkusernames.com is an online platform that provides a convenient way for individuals, businesses, and organizations to check the availability of usernames across various social media platforms, domain names, and popular online services. It serves as a valuable tool for those looking to establish a consistent online presence or brand identity.



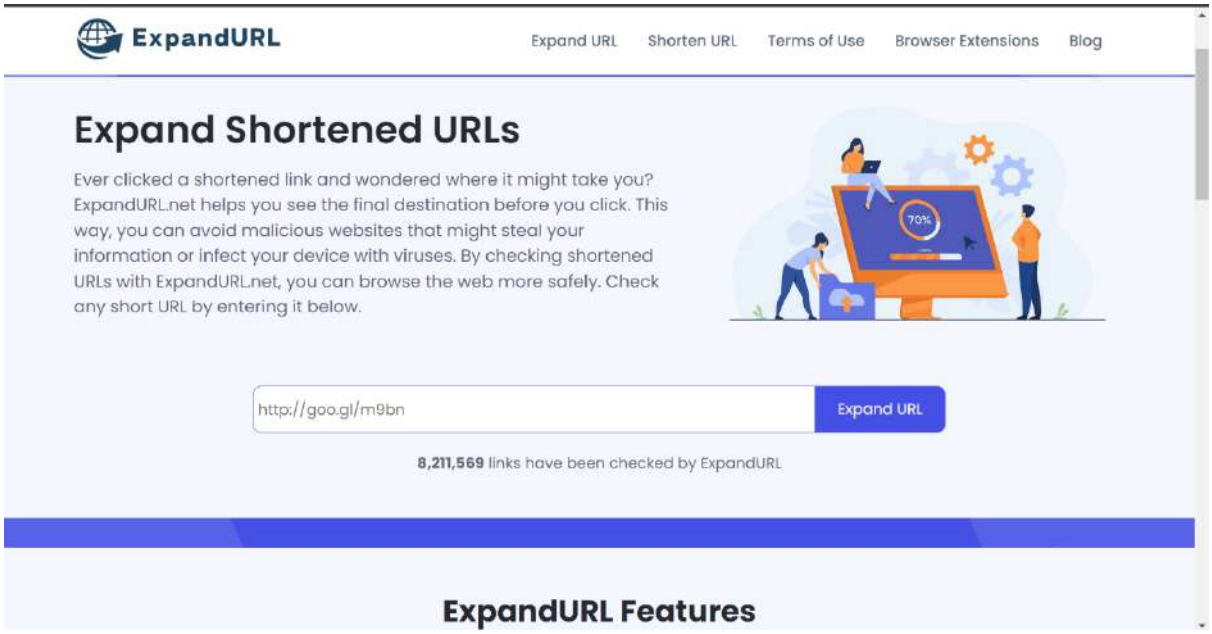
19. ***searchcode.com – [Searchcode.com]*** is a free source code search engine that indexes and makes searchable code snippets and open-source repositories. It helps you find real-world examples of functions, APIs, and libraries across over 10 public code sources in 243 languages. It's a valuable resource for developers looking to understand how certain functions and libraries are used in practice.



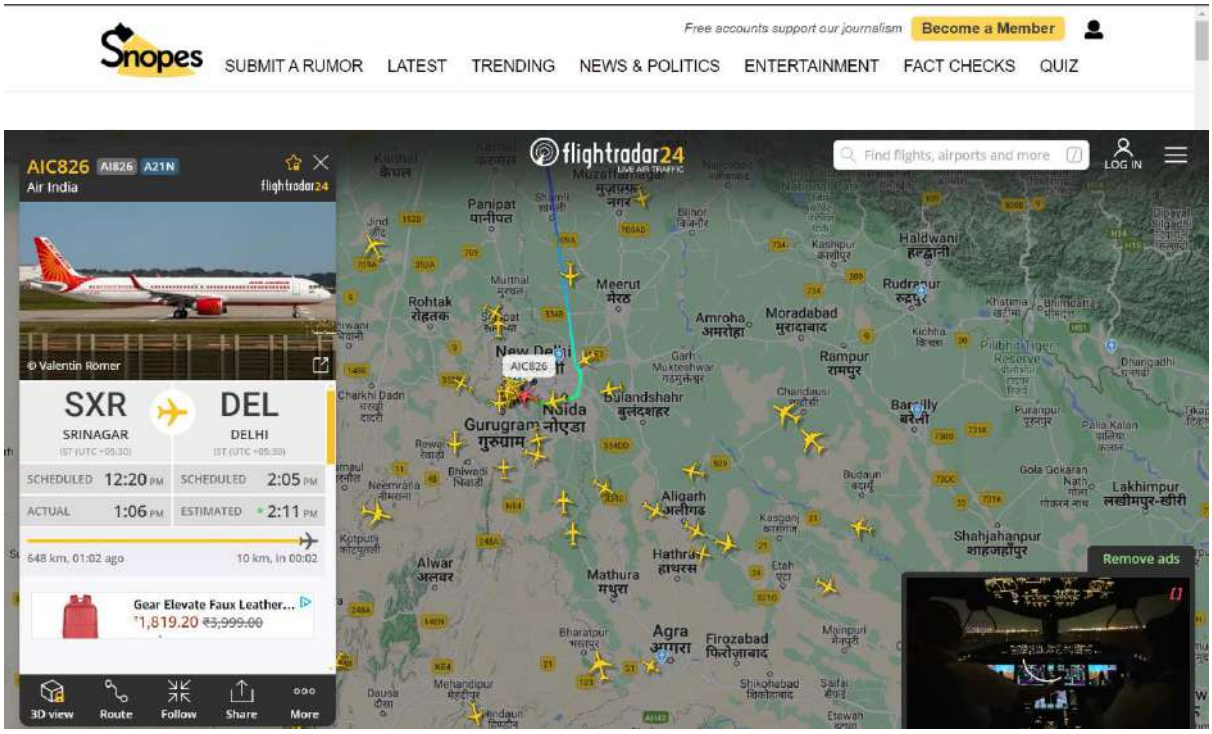
20. ***urlscan.io – [urlscan.io]*** is a free service that allows you to scan and analyze websites. When a URL is submitted, an automated process browses to the URL like a regular user and records the activity that this page navigation creates. This includes the domains and IPs contacted, the resources requested from those domains, and additional information about the page itself.



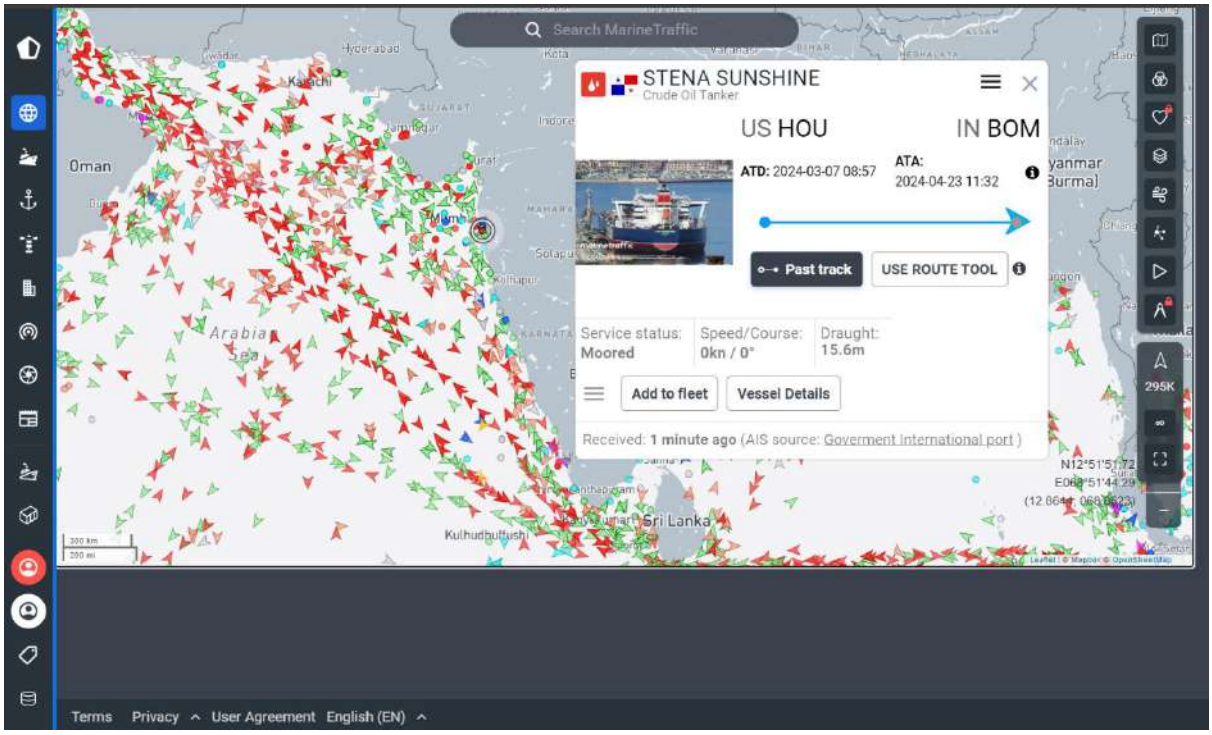
21. ***expandurl.net*** – ExpandURL.net helps you see the final destination before you click. This way, you can avoid malicious websites that might steal your information or infect your device with viruses. By checking shortened URLs with ExpandURL.net, you can browse the web more safely.



22. ***snopes.com*** – Snopes.com is a fact-checking website that debunks urban legends, myths, rumors, and misinformation circulating on the internet. Founded in 1994 by David Mikkelson and Barbara Mikkelson, Snopes employs a team of editors and researchers who investigate and verify the accuracy of various claims and stories. It has become a popular resource for individuals seeking to verify the truthfulness of information they encounter online.

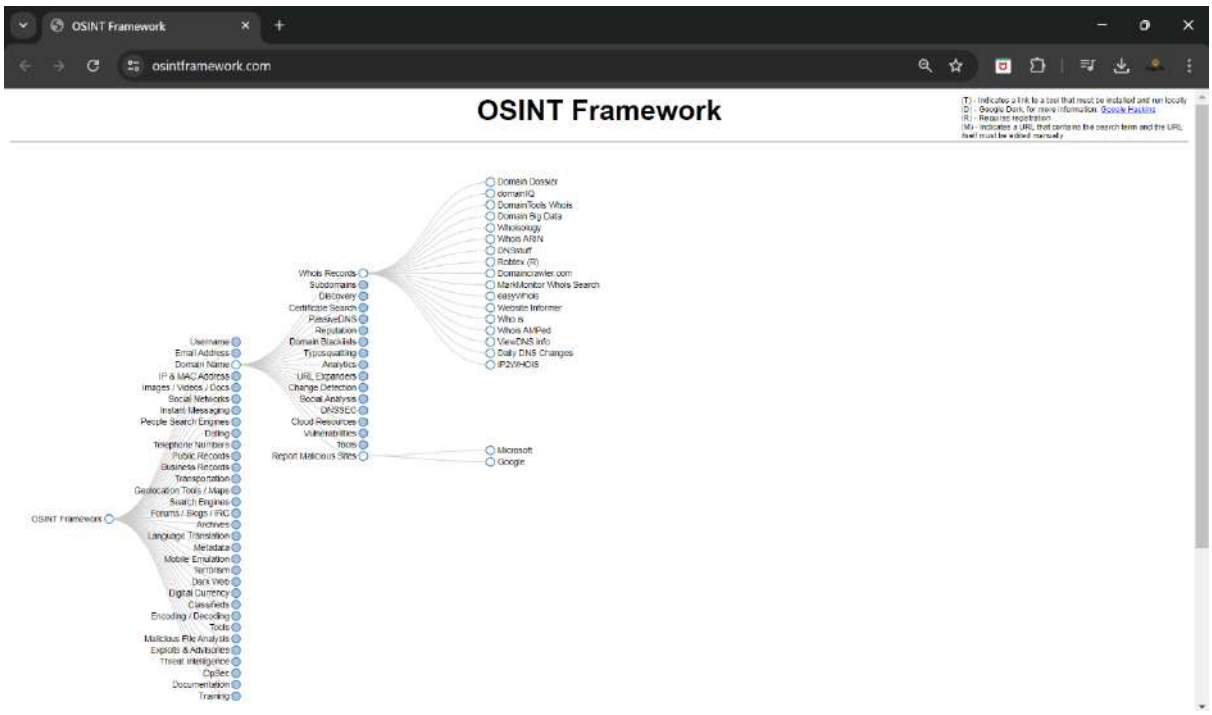


23. ***marinetraffic.com/en/ais/home – [MarineTraffic]*** is a global ship tracking intelligence service that uses AIS (Automatic Identification System) data to provide real-time information about ship movements worldwide. It allows you to discover information and vessel positions for vessels around the world

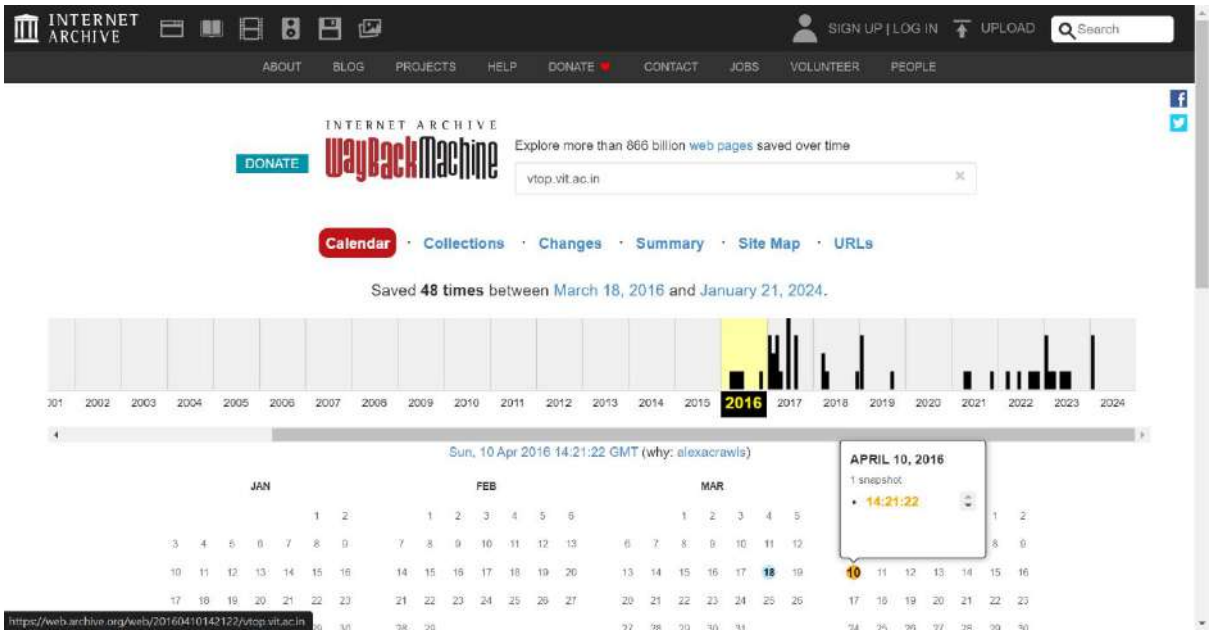


24. ***osintframework.com***

An OSINT framework is a tool for gathering information from free resources to help find OSINT resources. It aims to provide access to information without cost, although some sites may require registration or offer additional data for a fee.



25. ***web.archive.org – [Web Archive]*** or the Wayback Machine is a digital archive of the World Wide Web. It allows users to see archived versions of web pages across time, which can be useful for viewing the history of a particular website or webpage.



26. ***tails.net*** – [Tails] is a portable operating system that protects against surveillance and censorship. It uses the Tor network to protect your privacy online and help you avoid censorship. Tails leaves no trace on the computer when shut down.