Cyber security

Digital Assignment – 1

(Report Day 1)

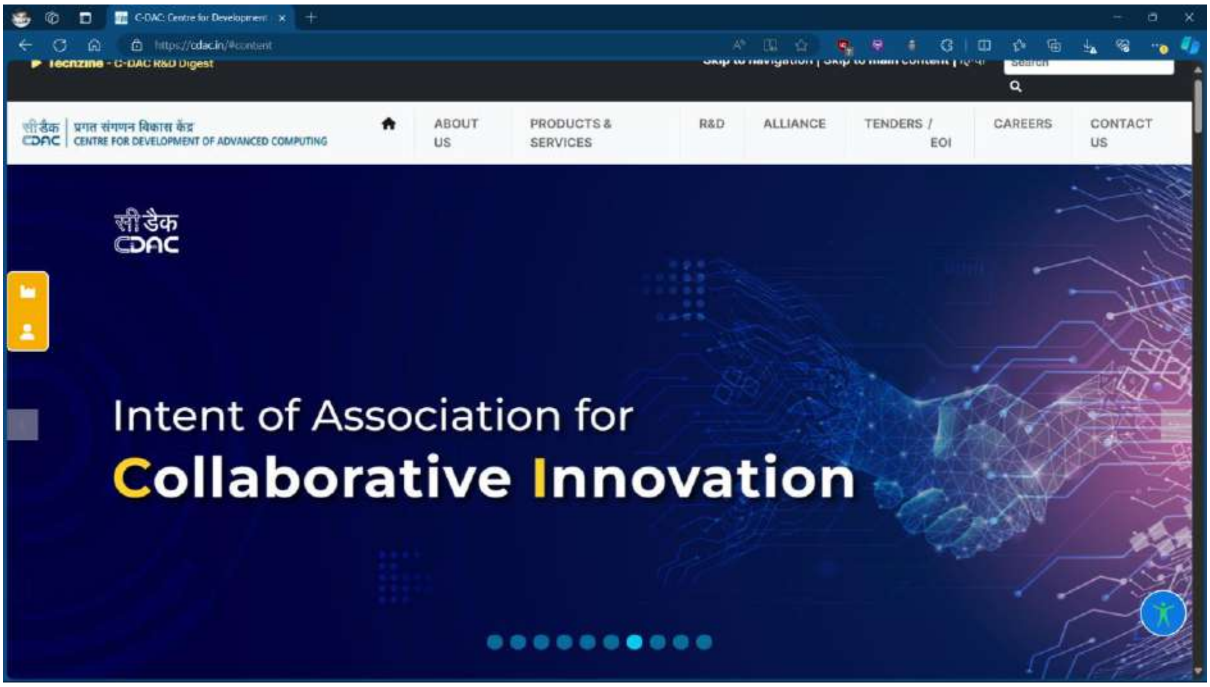
Name – Nilay
Registration no. – 21BT0219
Course code – BITE413L
Faculty – DR. GITANJALI J

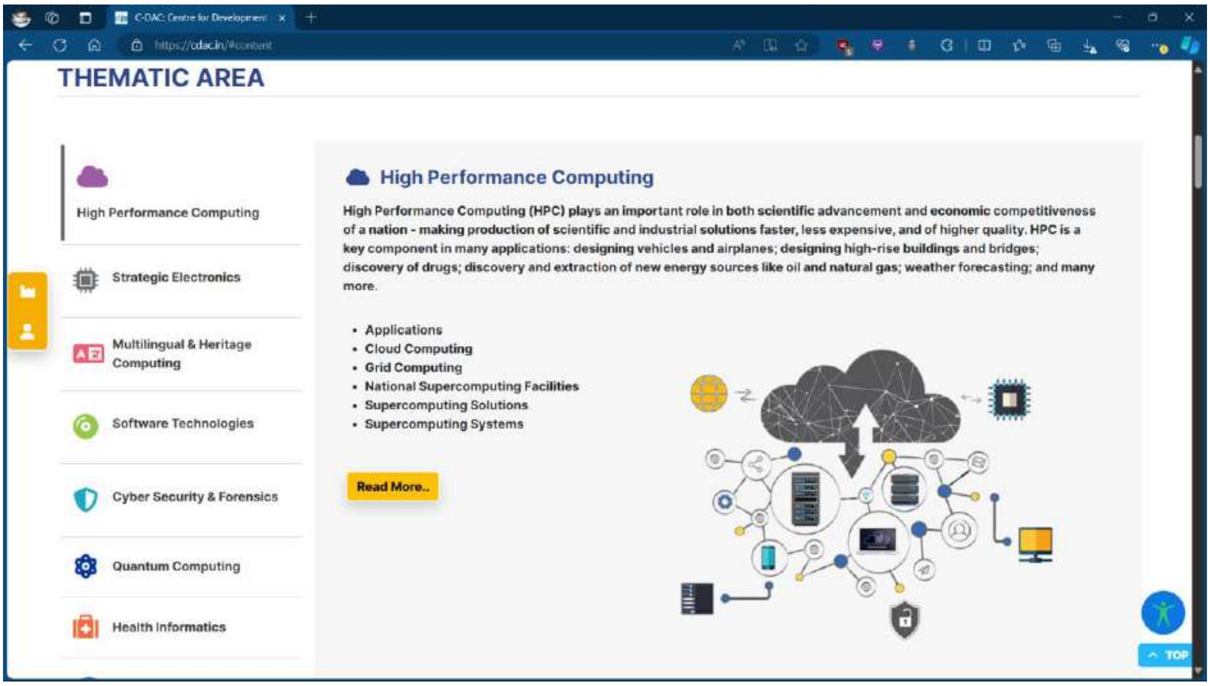
Report Day – 1

Introduction to C-DAC

- CDAC, Centre for Development of Advanced Computing, is pivotal in India's pursuit of cutting-edge computing technologies.
- Established with a mission to lead research and development initiatives.
- Significant milestones and achievements mark its rich history.
- Focus areas encompass high-performance computing, grid and cloud computing, software technology, multilingual computing, cybersecurity, and embedded systems.
- Robust collaborations with academia, industry, and government bodies have led to notable contributions in computing technologies.
- Comprehensive training programs cater to professionals and students, providing hands-on experience.
- State-of-the-art infrastructure and facilities across nationwide centers facilitate innovation and technology transfer.
- Partnerships and collaborations bolster CDAC's impact, shaping the future computing landscape.
- With forward-thinking strategies, CDAC aims to drive India's technological growth and innovation to greater heights.

Link to the official website: [C-DAC: Centre for Development of Advanced Computing, India (cdac.in)](https://cdac.in)


C-DAC: Centre for Development
https://cdac.in/#content
Tecnzine - C-DAC R&D Digest
Skip to navigation | Skip to main content | हिन्दी
Search
सी-डैक | प्रगत संगणन विकास केंद्र
CDAC | CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
ABOUT US
PRODUCTS & SERVICES
R&D
ALLIANCE
TENDERS / EOI
CAREERS
CONTACT US
सी-डैक
CDAC
Intent of Association for
Collaborative Innovation



THEMATIC AREA

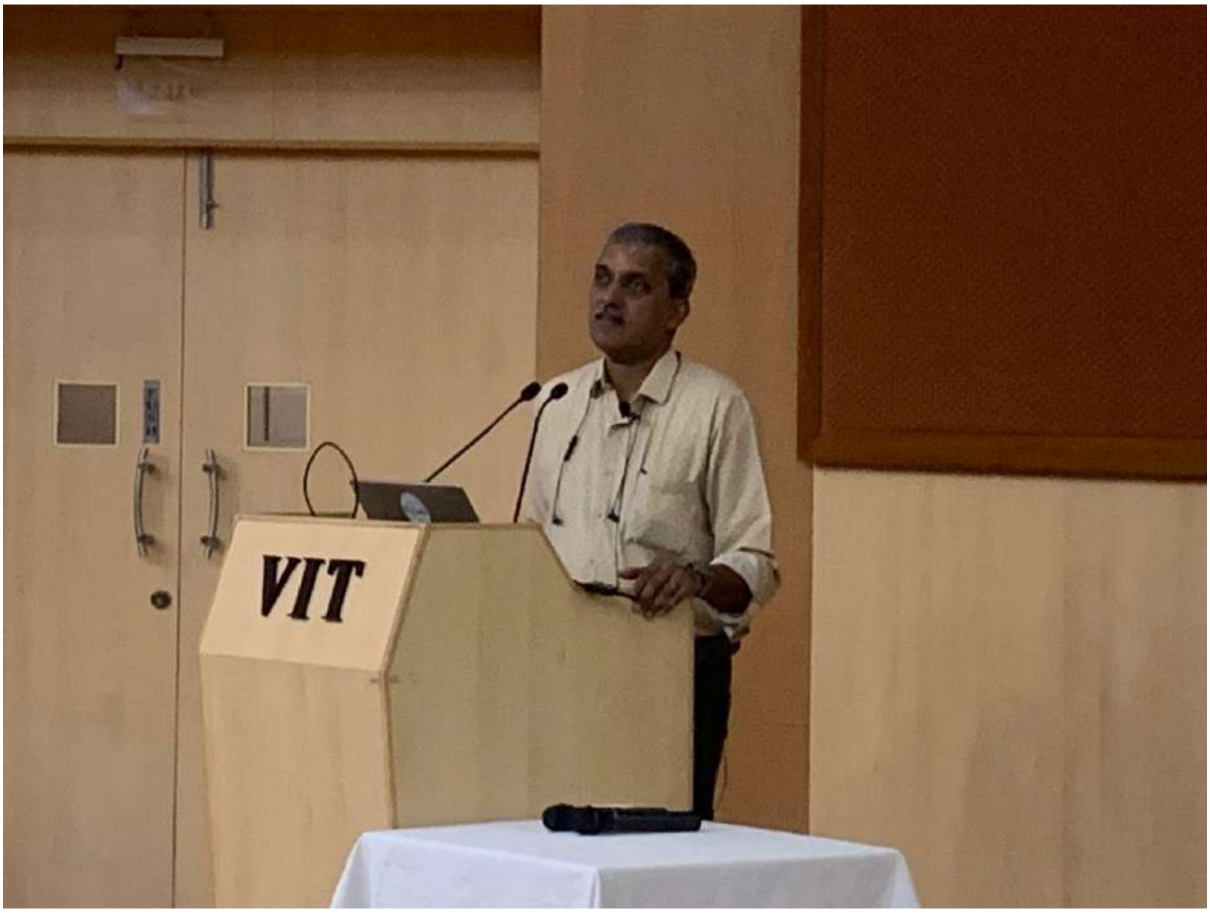
- High Performance Computing
- Strategic Electronics
- Multilingual & Heritage Computing
- Software Technologies
- Cyber Security & Forensics
- Quantum Computing
- Health Informatics

High Performance Computing

High Performance Computing (HPC) plays an important role in both scientific advancement and economic competitiveness of a nation - making production of scientific and industrial solutions faster, less expensive, and of higher quality. HPC is a key component in many applications: designing vehicles and airplanes; designing high-rise buildings and bridges; discovery of drugs; discovery and extraction of new energy sources like oil and natural gas; weather forecasting; and many more.

- Applications
- Cloud Computing
- Grid Computing
- National Supercomputing Facilities
- Supercomputing Solutions
- Supercomputing Systems

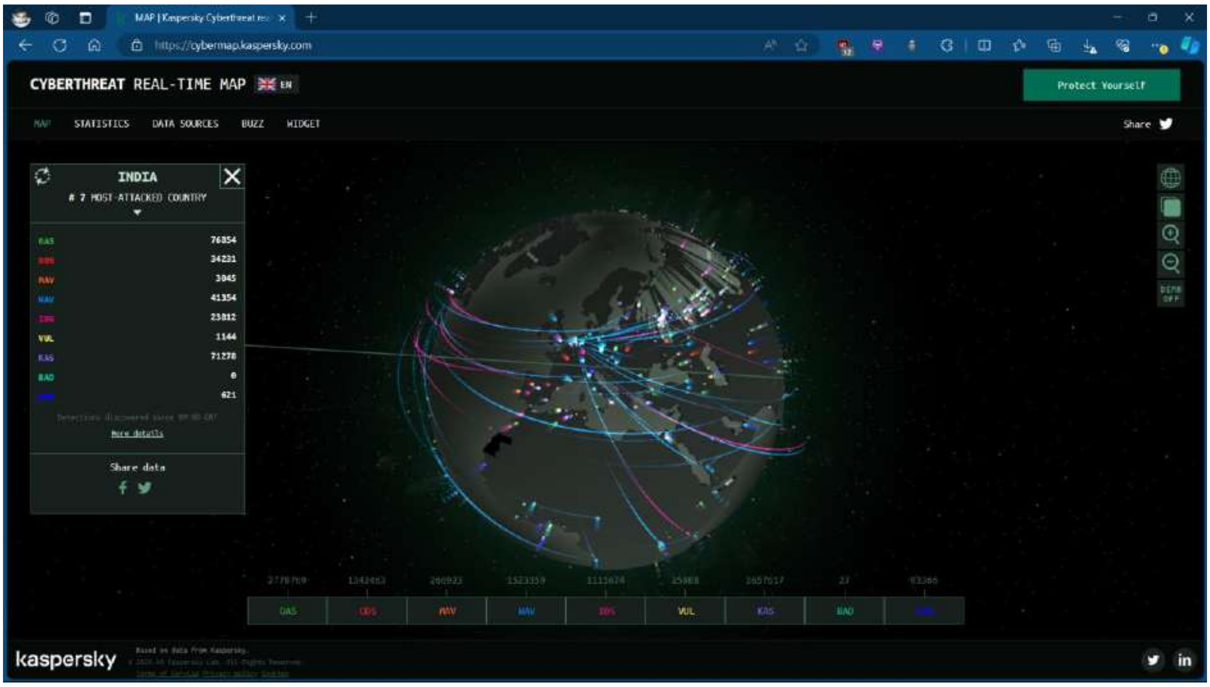
Read More..



Introduction to Cyber forensics

- **Cyber forensics**, also known as digital or computer forensics, is a branch of forensic science.
- It involves investigating, analyzing, and recovering digital evidence from electronic devices and digital systems.
- Cyber forensics is crucial in law enforcement, cybersecurity, and legal proceedings in our increasingly digitized world.
- The discipline encompasses techniques and tools for gathering, preserving, examining, and presenting digital evidence while maintaining its integrity and admissibility in court.
- Experts in cyber forensics are trained to recover data from various sources such as computers, mobile devices, networks, and digital storage media.
- They analyze this data to uncover evidence of criminal activity, security breaches, or unauthorized actions.
- Cyber forensics is continually evolving alongside technological advancements, requiring innovative approaches to address new challenges like **encrypted communications and IoT**.

Kaspersky – Cybermap



The **Cybermap** tool by Kaspersky is a visual representation of real-time cyber threats and attacks worldwide. It provides users with a dynamic map that displays various types of cyber incidents, including malware infections, phishing attempts, and network intrusions, as they occur across different regions and countries. The tool gathers data from Kaspersky's vast network of sensors, honeypots, and security technologies deployed globally, offering users valuable insights into the current cybersecurity landscape. With **Cybermap**, users can observe patterns, trends, and emerging threats in near real-time, helping organizations and individuals stay informed and vigilant against cyber threats. This tool serves as a valuable resource for cybersecurity professionals, researchers, and anyone interested in understanding the global cyber threat landscape.

Link : [MAP | Kaspersky Cyberthreat real-time map]

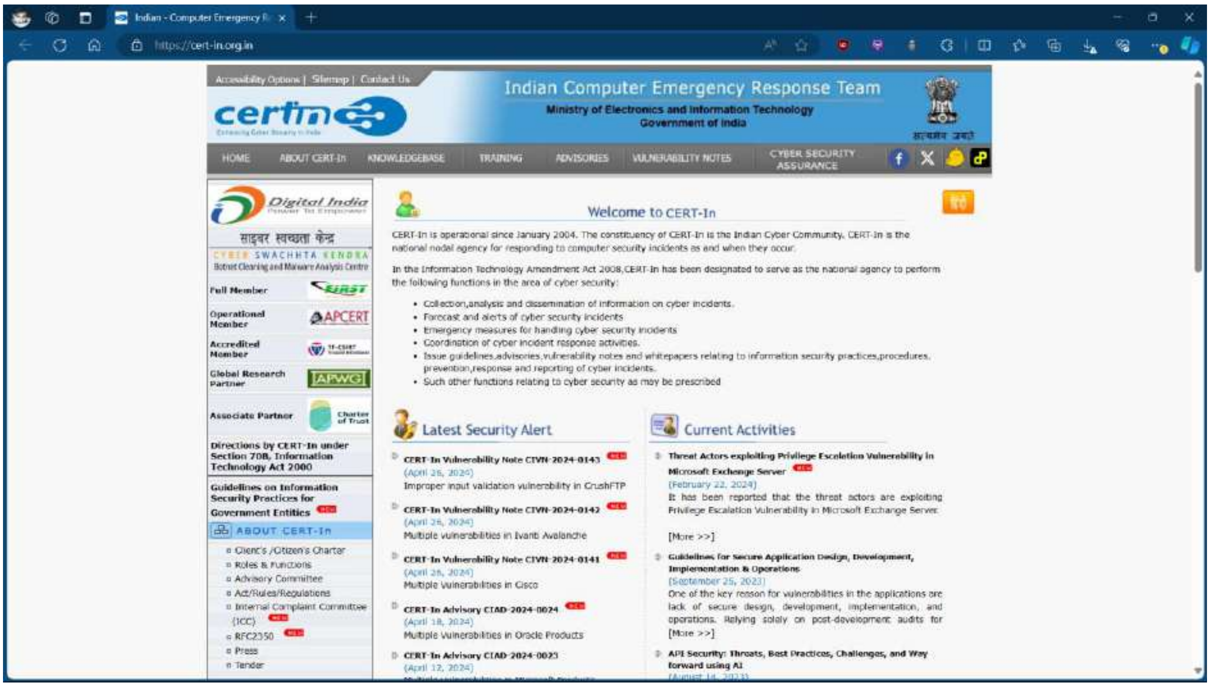
What are attackers and victims?

- ***Attackers:*** Attackers are individuals or groups who perpetrate cyberattacks. They are often motivated by various factors such as financial gain, political motives, espionage, or personal vendettas. Attackers employ a variety of techniques and tools to compromise the security of computer systems, networks, and data. These techniques may include malware deployment, phishing attacks, social engineering tactics, exploitation of software vulnerabilities, and denial-of-service (DoS) attacks, among others. Attackers continuously evolve their tactics to bypass security measures and achieve their malicious objectives.
- ***Victims:*** Victims are individuals, organizations, or entities whose systems, networks, or data are compromised or targeted in a cyberattack. Victims can range from individuals whose personal information is stolen through phishing scams to large corporations experiencing data breaches that result in financial losses, reputational damage, and legal liabilities. Victims of cyberattacks may suffer various consequences, including financial harm, loss of sensitive information, disruption of operations, damage to reputation, and violation of privacy rights.

Common cyber attacks in india

- ***Phishing Attacks:*** Phishing attacks are prevalent in India, where attackers send deceptive emails or messages pretending to be from legitimate organizations to trick individuals into providing sensitive information such as login credentials, financial details, or personal information.
- ***Ransomware:*** Ransomware attacks encrypt victims' files or systems and demand payment (usually in cryptocurrency) for decryption keys. India has seen several high-profile ransomware incidents targeting organizations across various sectors, including healthcare, finance, and government.
- ***Malware Infections:*** Malware, including viruses, worms, Trojans, and spyware, is commonly used by cybercriminals to compromise systems and steal data or disrupt operations. Malware infections in India have been reported in both individual users and organizations.
- ***Distributed Denial of Service (DDoS) Attacks:*** DDoS attacks aim to disrupt the availability of online services by overwhelming target systems with a flood of traffic. These attacks have targeted Indian websites and online services, causing downtime and financial losses.
- ***Data Breaches:*** Data breaches involve unauthorized access to and theft of sensitive information such as personal data, financial records, or intellectual property. Indian organizations have experienced data breaches resulting from vulnerabilities in their systems or insider threats.
- ***Social Engineering Attacks***: Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. These attacks include techniques like pretexting, baiting, and tailgating and have been used in various cyber incidents in India.
- ***Cryptojacking:*** Cryptojacking involves unauthorized use of victims' computing resources to mine cryptocurrencies. Attackers infect systems with malicious code, exploiting their processing power for cryptocurrency mining without permission.

Cert-in



Welcome to CERT-In

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection,analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

Latest Security Alert

CERT-In Vulnerability Note CIVN-2024-0143
(April 26, 2024)
Improper input validation vulnerability in CrushFTP

CERT-In Vulnerability Note CIVN-2024-0142
(April 26, 2024)
Multiple vulnerabilities in Ivanti Avalanche

CERT-In Vulnerability Note CIVN-2024-0141
(April 26, 2024)
Multiple Vulnerabilities in Cisco

CERT-In Advisory CIAD-2024-0024
(April 18, 2024)
Multiple Vulnerabilities in Oracle Products

CERT-In Advisory CIAD-2024-0023
(April 12, 2024)

Current Activities

Threat Actors exploiting Privilege Escalation Vulnerability in Microsoft Exchange Server
(February 22, 2024)
It has been reported that the threat actors are exploiting Privilege Escalation Vulnerability in Microsoft Exchange Server.

[More >>]

Guidelines for Secure Application Design, Development, Implementation & Operations
(September 25, 2023)
One of the key reason for vulnerabilities in the applications are lack of secure design, development, implementation, and operations. Relying solely on post-development audits for
[More >>]

API Security: Threats, Best Practices, Challenges, and Way forward using AI

- The CERT-In website serves as India's primary platform for cybersecurity-related information, advisories, and resources.
- It offers timely alerts and advisories on emerging cyber threats, vulnerabilities, and incidents affecting Indian cyberspace.
- Organizations and individuals can report cybersecurity incidents through its online portal for assistance and guidance.
- The website provides a wealth of cybersecurity guidelines, best practices, and recommendations to enhance stakeholders' cybersecurity posture.
- CERT-In conducts training programs, workshops, and capacity-building initiatives to raise awareness and build skills among cybersecurity professionals and IT administrators.
- It hosts research papers, reports, and publications on cybersecurity topics, offering insights into the evolving threat landscape.
- Through international collaborations, CERT-In strengthens global cybersecurity cooperation and shares threat intelligence and expertise.
- Overall, the CERT-In website plays a vital role in promoting cybersecurity awareness, facilitating incident response, and enhancing cybersecurity capabilities across India.

Link: Cert-In - Home Page

Vulnerability and exploits

Vulnerabilities:

A vulnerability refers to a weakness or flaw in a system, network, application, or device that can be exploited by attackers to compromise its security.

Types of Vulnerabilities:

- **Software Vulnerabilities:** These are flaws in software code that can be exploited to gain unauthorized access, execute arbitrary code, or perform other malicious actions.
- **Hardware Vulnerabilities:** Weaknesses in hardware components or designs that can be exploited to bypass security mechanisms or gain unauthorized access.
- **Configuration Vulnerabilities:** Incorrectly configured systems or networks that expose security vulnerabilities, such as default passwords, open ports, or unnecessary services.
- **Human Vulnerabilities:** Weaknesses related to human behavior, such as lack of awareness, susceptibility to social engineering attacks, or improper handling of sensitive information.

Examples of Vulnerabilities:

Buffer overflow vulnerabilities
Cross-site scripting (XSS)
SQL injection
Authentication bypass
Insecure deserialization

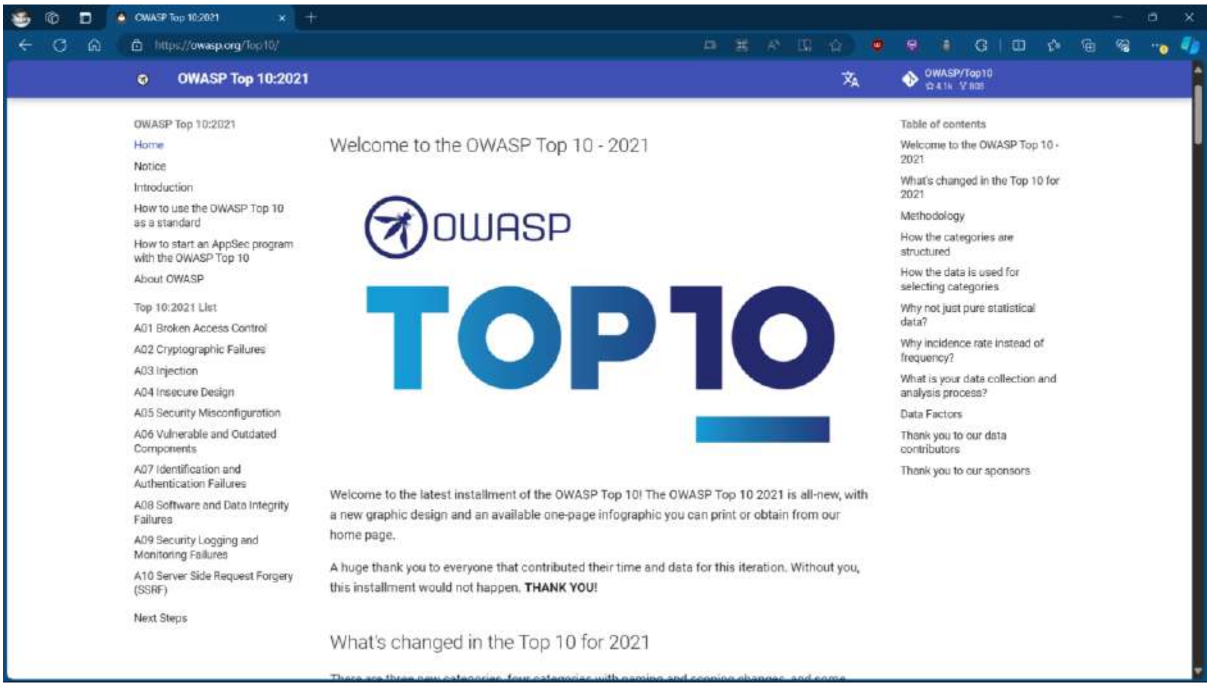
Exploits:

An exploit is a piece of software, code, or technique used to take advantage of a vulnerability in a system, application, or device to achieve a specific malicious goal.

Types of Exploits:

- **Remote Exploits:** Exploits that can be executed over a network without physical access to the target system.
- **Local Exploits:** Exploits that require local access to the target system, such as physical access or prior compromise of a user account.
- **Zero-Day Exploits:** Exploits that target vulnerabilities for which no patch or fix is available, making them particularly dangerous as defenders have no prior knowledge of the vulnerability.

OWASP TOP 10



OWASP Top 10:2021
Home
Notice
Introduction
How to use the OWASP Top 10 as a standard
How to start an AppSec program with the OWASP Top 10
About OWASP

Top 10:2021 List
A01 Broken Access Control
A02 Cryptographic Failures
A03 Injection
A04 Insecure Design
A05 Security Misconfiguration
A06 Vulnerable and Outdated Components
A07 Identification and Authentication Failures
A08 Software and Data Integrity Failures
A09 Security Logging and Monitoring Failures
A10 Server Side Request Forgery (SSRF)

Next Steps

Welcome to the OWASP Top 10 - 2021

Welcome to the latest installment of the OWASP Top 10! The OWASP Top 10 2021 is all-new, with a new graphic design and an available one-page infographic you can print or obtain from our home page.

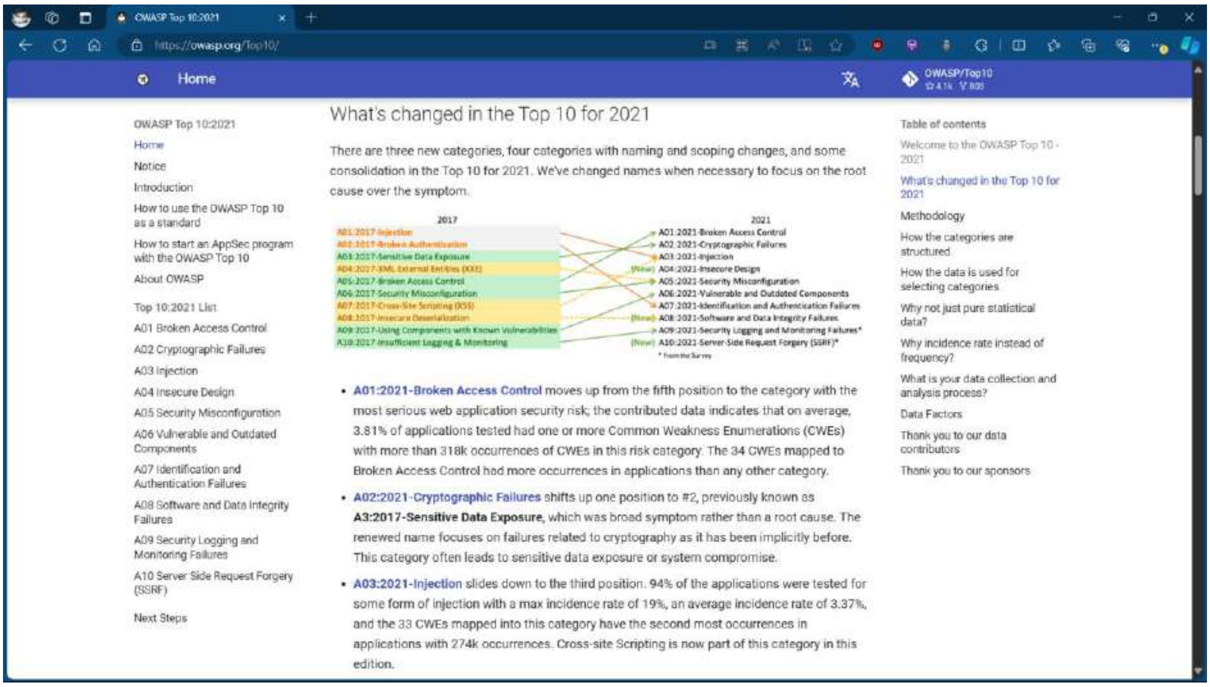
A huge thank you to everyone that contributed their time and data for this iteration. Without you, this installment would not happen. **THANK YOU!**

What's changed in the Top 10 for 2021

There are three new categories, four categories with naming and scoping changes, and some

Table of contents
Welcome to the OWASP Top 10 - 2021
What's changed in the Top 10 for 2021
Methodology
How the categories are structured
How the data is used for selecting categories
Why not just pure statistical data?
Why incidence rate instead of frequency?
What is your data collection and analysis process?
Data Factors
Thank you to our data contributors
Thank you to our sponsors

Changes in the Trends



OWASP Top 10:2021
Home
Notice
Introduction
How to use the OWASP Top 10 as a standard
How to start an AppSec program with the OWASP Top 10
About OWASP

Top 10:2021 List
A01 Broken Access Control
A02 Cryptographic Failures
A03 Injection
A04 Insecure Design
A05 Security Misconfiguration
A06 Vulnerable and Outdated Components
A07 Identification and Authentication Failures
A08 Software and Data Integrity Failures
A09 Security Logging and Monitoring Failures
A10 Server Side Request Forgery (SSRF)

Next Steps

What's changed in the Top 10 for 2021

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021. We've changed names when necessary to focus on the root cause over the symptom.

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

- **A01:2021-Broken Access Control** moves up from the fifth position to the category with the most serious web application security risk; the contributed data indicates that on average, 3.81% of applications tested had one or more Common Weakness Enumerations (CWEs) with more than 318k occurrences of CWEs in this risk category. The 34 CWEs mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as **A3:2017-Sensitive Data Exposure**, which was broad symptom rather than a root cause. The renewed name focuses on failures related to cryptography as it has been implicitly before. This category often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3.37%, and the 33 CWEs mapped into this category have the second most occurrences in applications with 274k occurrences. Cross-site Scripting is now part of this category in this edition.

Table of contents
Welcome to the OWASP Top 10 - 2021
What's changed in the Top 10 for 2021
Methodology
How the categories are structured
How the data is used for selecting categories
Why not just pure statistical data?
Why incidence rate instead of frequency?
What is your data collection and analysis process?
Data Factors
Thank you to our data contributors
Thank you to our sponsors

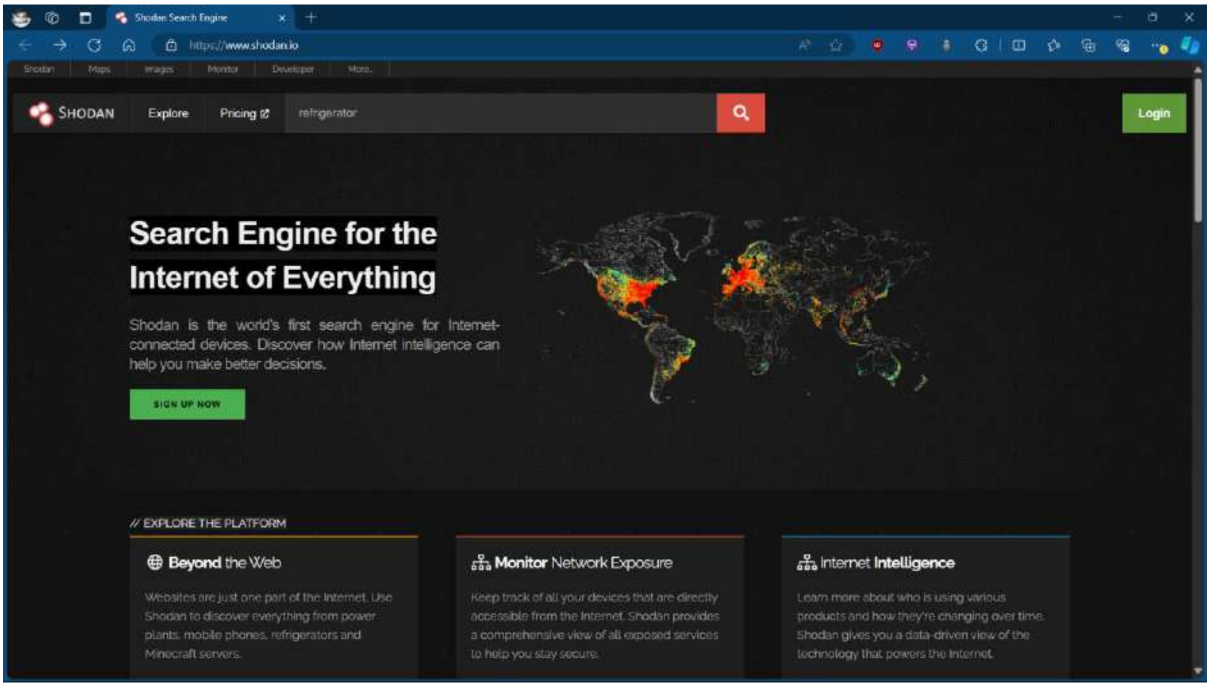
Link: OWASP Top 10:2021

The OWASP Top 10 is a widely recognized list of the most critical security risks facing web applications. Here's a brief overview of the OWASP Top 10:

1. ***Injection:*** Injection flaws occur when untrusted data is sent to an interpreter as part of a command or query, leading to arbitrary code execution. This includes SQL injection, NoSQL injection, OS command injection, and LDAP injection.
2. ***Broken Authentication:*** Broken authentication vulnerabilities allow attackers to compromise user accounts, session tokens, or passwords, enabling unauthorized access to sensitive data or functionality.
3. ***Sensitive Data Exposure:*** This risk involves the exposure of sensitive data, such as financial information, personal data, or authentication credentials, due to inadequate protection or encryption.
4. ***XML External Entities (XXE):*** XXE vulnerabilities occur when XML input containing a reference to an external entity is processed by a weakly configured XML parser, leading to unauthorized data disclosure, server-side request forgery (SSRF), or denial of service (DoS).
5. ***Broken Access Control:*** Broken access control vulnerabilities allow attackers to bypass access controls and gain unauthorized access to resources or functionality they should not have access to.
6. ***Security Misconfiguration:*** Security misconfiguration occurs when security settings are not properly configured or are left in their default state, leaving systems vulnerable to attacks such as unauthorized access, data leaks, or denial of service.
7. ***Cross-Site Scripting (XSS):*** XSS vulnerabilities enable attackers to inject malicious scripts into web applications, which are then executed in the context of unsuspecting users' browsers, leading to theft of session cookies, account hijacking, or defacement of websites.
8. ***Insecure Deserialization:*** Insecure deserialization vulnerabilities allow attackers to manipulate serialized objects to execute arbitrary code, perform denial of service attacks, or bypass authentication mechanisms.
9. ***Using Components with Known Vulnerabilities***: This risk involves the use of outdated or vulnerable components, libraries, or frameworks in web applications, exposing them to known security flaws that can be exploited by attackers.
10. ***Insufficient Logging & Monitoring:*** Insufficient logging and monitoring make it difficult to detect and respond to security incidents, allowing attackers to carry out attacks without being detected, and enabling them to persist within systems undetected.

The OWASP Top 10 serves as a valuable resource for developers, security professionals, and organizations to prioritize security efforts and mitigate the most critical risks in their web applications.

Shodan.io



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

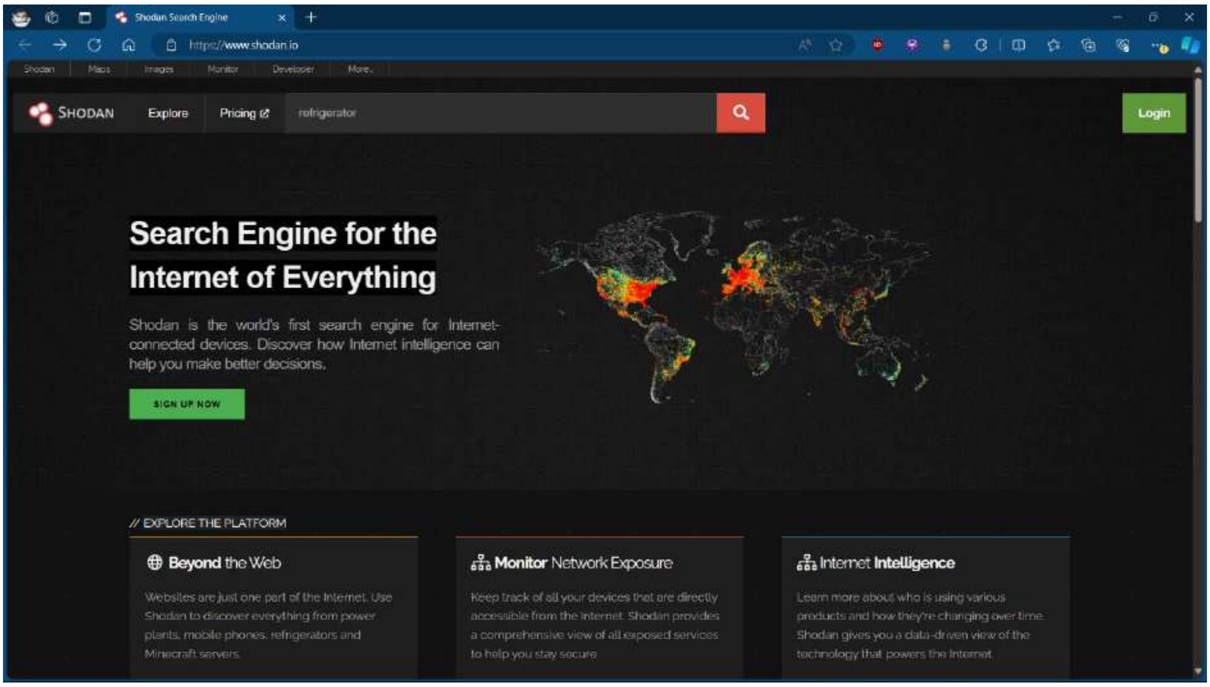
Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

Link : Shodan Search Engine

- Shodan.io is a search engine designed to locate and catalog internet-connected devices and systems.
- Users can search for specific devices or services using keywords, filters, or advanced search queries.
- The platform provides detailed information such as open ports, banners, and services running on discovered devices.
- It enables security professionals, researchers, and individuals to assess the security posture of organizations, identify misconfigured systems, and explore potential attack surfaces.
- Shodan.io offers features like Shodan Exploits, which provides information on known vulnerabilities and exploits, and Shodan Images, allowing users to search for screenshots of internet-connected devices.
- While Shodan.io offers valuable insights into the security landscape, it also raises privacy and ethical concerns.

Example : Refrigerator connected on internet



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

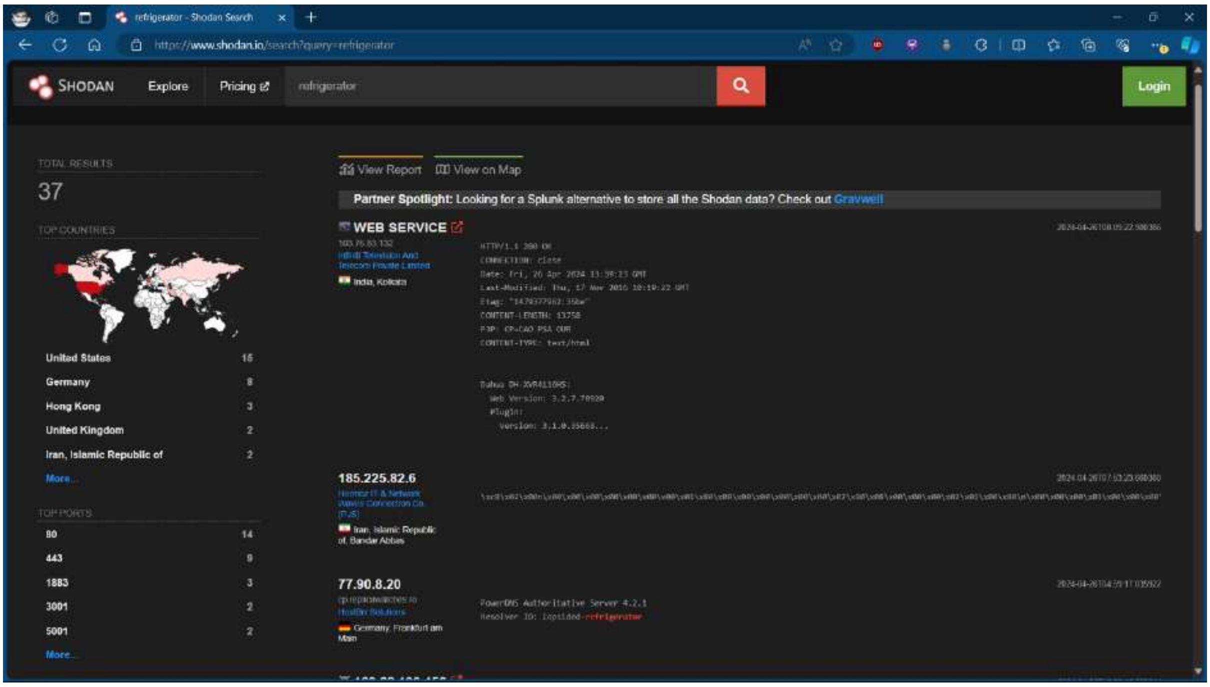
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet **Intelligence**

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.


refrigerator - Shodan Search
https://www.shodan.io/search?query=refrigerator
SHODAN
Explore
Pricing
refrigerator
Login
View Report
View on Map

TOTAL RESULTS

37

TOP COUNTRIES

United States	16
Germany	8
Hong Kong	3
United Kingdom	2
Iran, Islamic Republic of	2
More...	

TOP PORTS

80	14
443	9
1883	3
3001	2
5001	2
More...	

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

WEB SERVICE
103.76.83.132
Hathway Television And Telecom Private Limited
India, Kolkata
2024-04-26T08:05:22.980386

```
HTTP/1.1 200 OK
CONNECTION: close
Date: Fri, 26 Apr 2024 13:38:23 GMT
Last-Modified: Thu, 17 Nov 2016 10:19:22 GMT
Etag: "1479377962:35be"
CONTENT-LENGTH: 13758
P3P: CP=CAO PSA OUR
CONTENT-TYPE: text/html


Dahua DH-XVR4116HS:
  Web Version: 3.2.7.70920
  Plugin:
    Version: 3.1.0.35663...
```

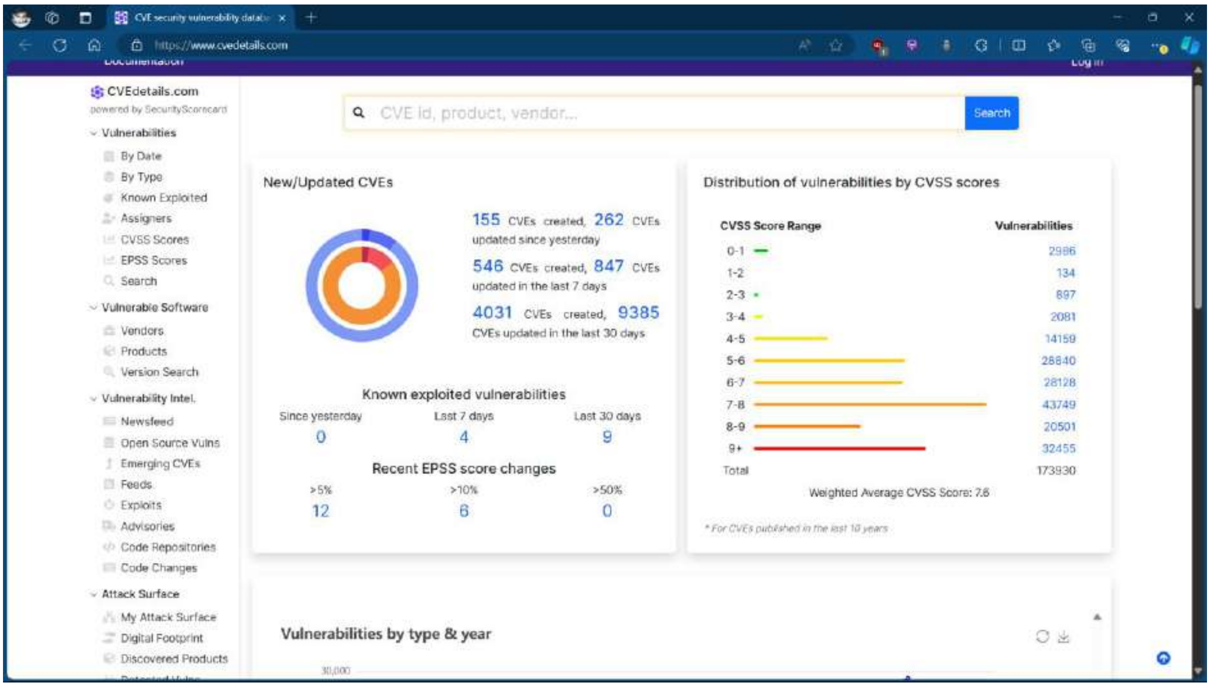
185.225.82.6
Hormoz IT & Network Waves Connection Co. (PJS)
Iran, Islamic Republic of, Bandar Abbas
2024-04-26T07:53:23.980360

```
[illegible]
```

77.90.8.20
cp.replicawatches.io
HostDin Solutions
Germany, Frankfurt am Main
2024-04-26T04:59:17.035922

```
PowerDNS Authoritative Server 4.2.1
Resolver ID: lopidded-refrigerator
```

CVE Security



New/Updated CVEs

155 CVEs created, 262 CVEs updated since yesterday

546 CVEs created, 847 CVEs updated in the last 7 days

4031 CVEs created, 9385 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
0	4	9

Recent EPSS score changes

>5%	>10%	>50%
12	6	0

Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	2986
1-2	134
2-3	897
3-4	2081
4-5	14159
5-6	28840
6-7	28128
7-8	43749
8-9	20501
9+	32455
Total	173930

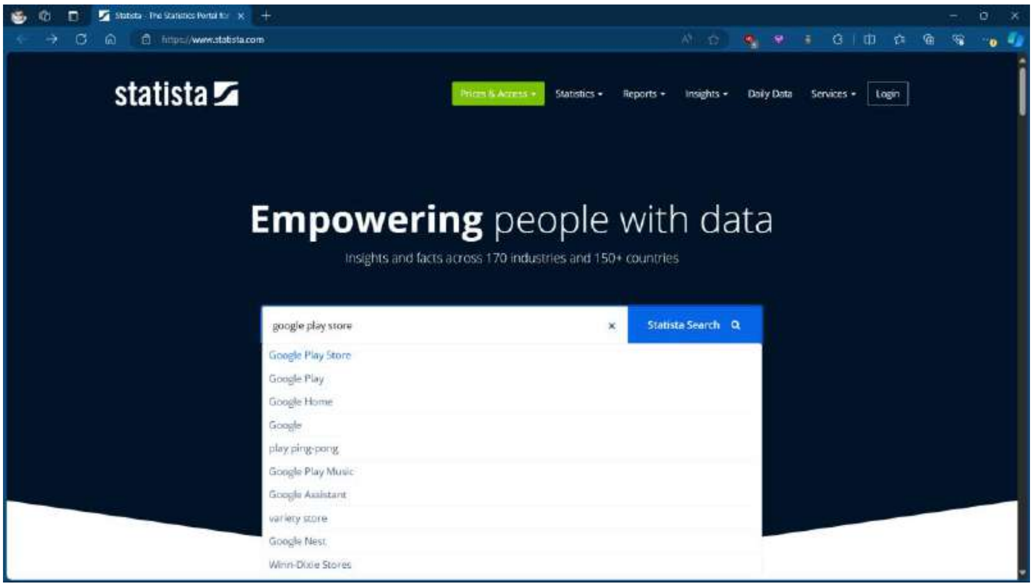
Weighted Average CVSS Score: 7.8

* For CVEs published in the last 10 years

Link: CVE security vulnerability database. Security vulnerabilities, exploits, references and more (cvedetails.com)

- CVE Details is a website providing information about Common Vulnerabilities and Exposures (CVE).
- It hosts a database of known vulnerabilities in software and hardware products.
- Users can search for specific vulnerabilities by keyword, vendor, product, or vulnerability type.
- Each CVE entry includes detailed information such as the CVE ID, vulnerability type, affected product versions, severity level, and publication date.
- The website also offers statistics and trends based on the data in its database, providing insights into the frequency of vulnerabilities, common vulnerability types, and affected vendors and products over time.
- CVE Details is a valuable resource for security professionals, researchers, and organizations to stay informed about known vulnerabilities and assess the security posture of their systems effectively.

Statista.com



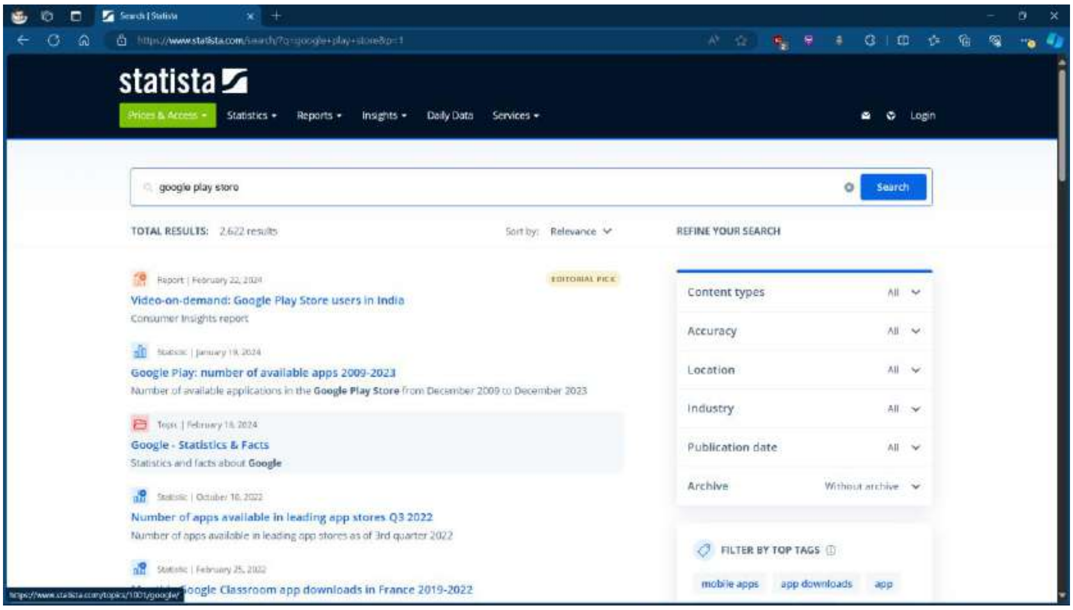
Empowering people with data

Insights and facts across 170 industries and 150+ countries

google play store

Link : [Search | Statista]()

- CVE Details is a website providing information about Common Vulnerabilities and Exposures (CVE).
- It hosts a database of known vulnerabilities in software and hardware products.
- Users can search for specific vulnerabilities by keyword, vendor, product, or vulnerability type.
- Each CVE entry includes detailed information such as the CVE ID, vulnerability type, affected product versions, severity level, and publication date.
- The website also offers statistics and trends based on the data in its database, providing insights into the frequency of vulnerabilities, common vulnerability types, and affected vendors and products over time.
- CVE Details is a valuable resource for security professionals, researchers, and organizations to stay informed about known vulnerabilities and assess the security posture of their systems effectively.



google play store

TOTAL RESULTS: 2,622 results

Sort by: Relevance

Report | February 22, 2024
Video-on-demand: Google Play Store users in India
Consumer Insights report

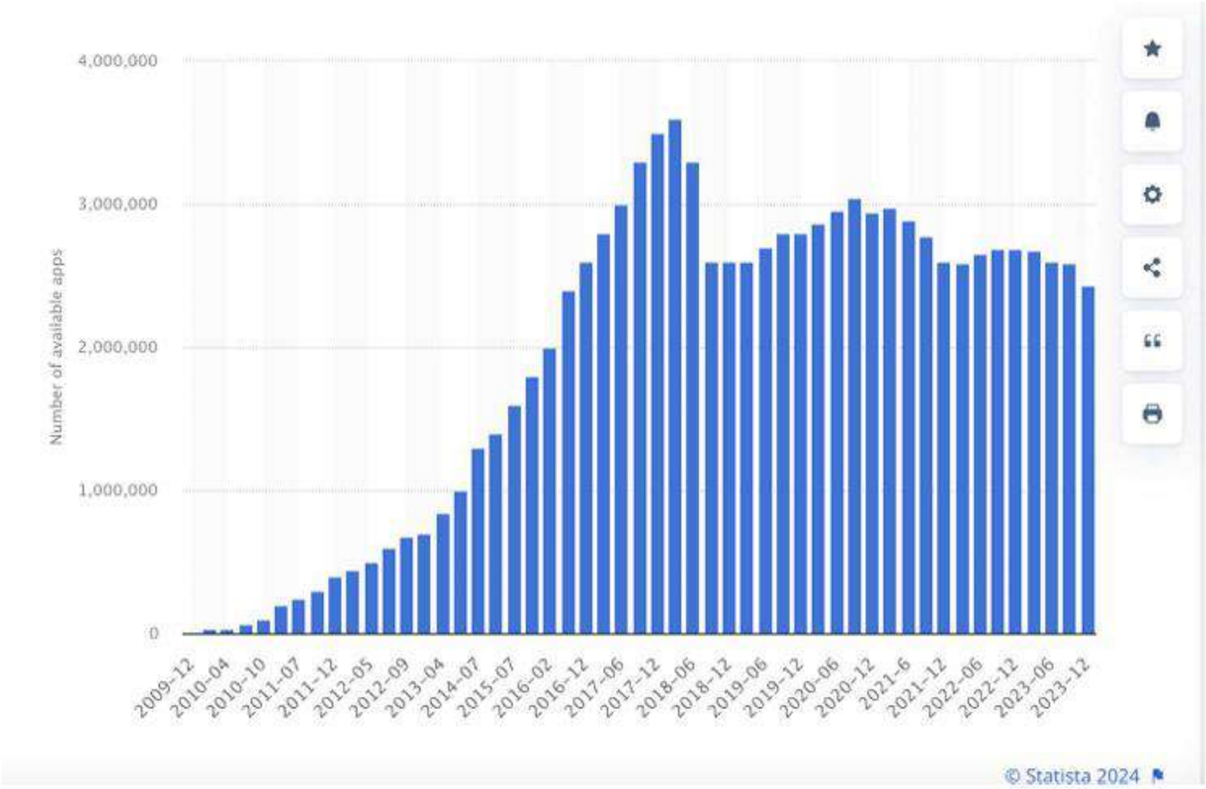
Statistic | January 19, 2024
Google Play: number of available apps 2009-2023
Number of available applications in the **Google Play Store** from December 2009 to December 2023

Topic | February 16, 2024
Google - Statistics & Facts
Statistics and facts about **Google**

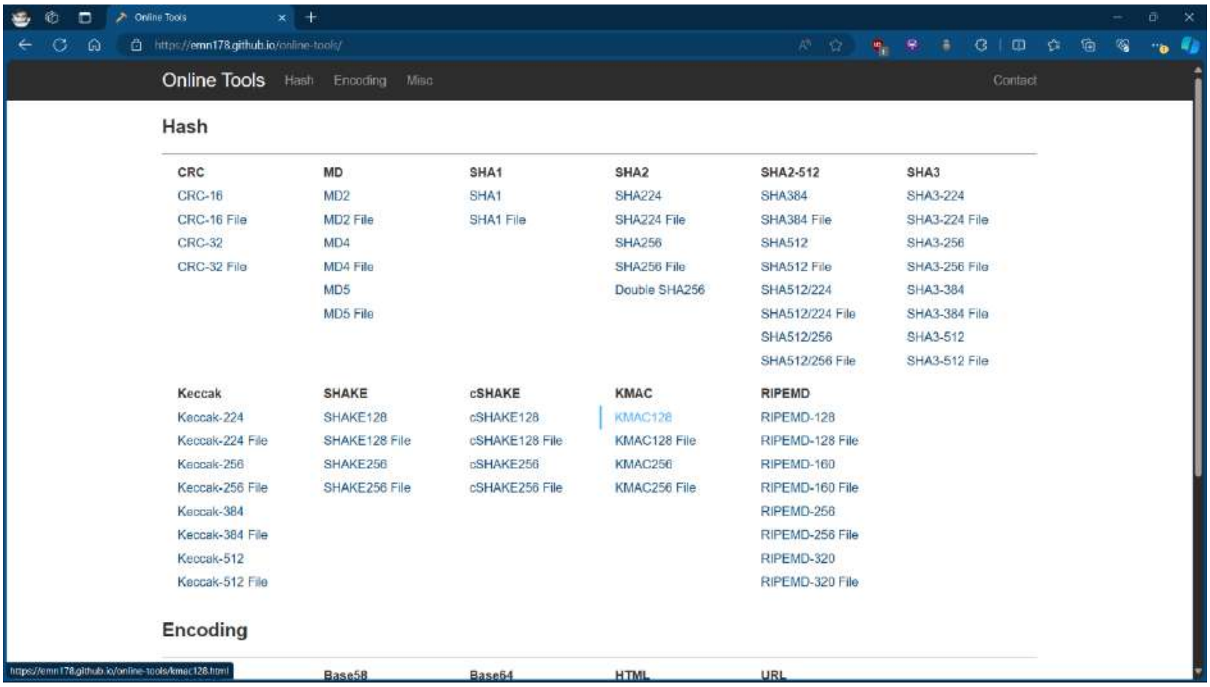
Statistic | October 10, 2022
Number of apps available in leading app stores Q3 2022
Number of apps available in leading app stores as of 3rd quarter 2022

Statistic | February 25, 2022
oogle Classroom app downloads in France 2019-2022

Content types	All
Accuracy	All
Location	All
Industry	All
Publication date	All
Archive	Without archive


4,000,000
3,000,000
2,000,000
1,000,000
0
Number of available apps
2009-12
2010-04
2010-10
2011-07
2011-12
2012-05
2012-09
2013-04
2014-07
2015-07
2016-02
2016-12
2017-06
2017-12
2018-06
2018-12
2019-06
2019-12
2020-06
2020-12
2021-6
2021-12
2022-06
2022-12
2023-06
2023-12
© Statista 2024

Online-hashing app



Hash

CRC
CRC-16
CRC-16 File
CRC-32
CRC-32 File

MD
MD2
MD2 File
MD4
MD4 File
MD5
MD5 File

SHA1
SHA1
SHA1 File

SHA2
SHA224
SHA224 File
SHA256
SHA256 File
Double SHA256

SHA2-512
SHA384
SHA384 File
SHA512
SHA512 File
SHA512/224
SHA512/224 File
SHA512/256
SHA512/256 File

SHA3
SHA3-224
SHA3-224 File
SHA3-256
SHA3-256 File
SHA3-384
SHA3-384 File
SHA3-512
SHA3-512 File

Keccak
Keccak-224
Keccak-224 File
Keccak-256
Keccak-256 File
Keccak-384
Keccak-384 File
Keccak-512
Keccak-512 File

SHAKE
SHAKE128
SHAKE128 File
SHAKE256
SHAKE256 File

cSHAKE
cSHAKE128
cSHAKE128 File
cSHAKE256
cSHAKE256 File

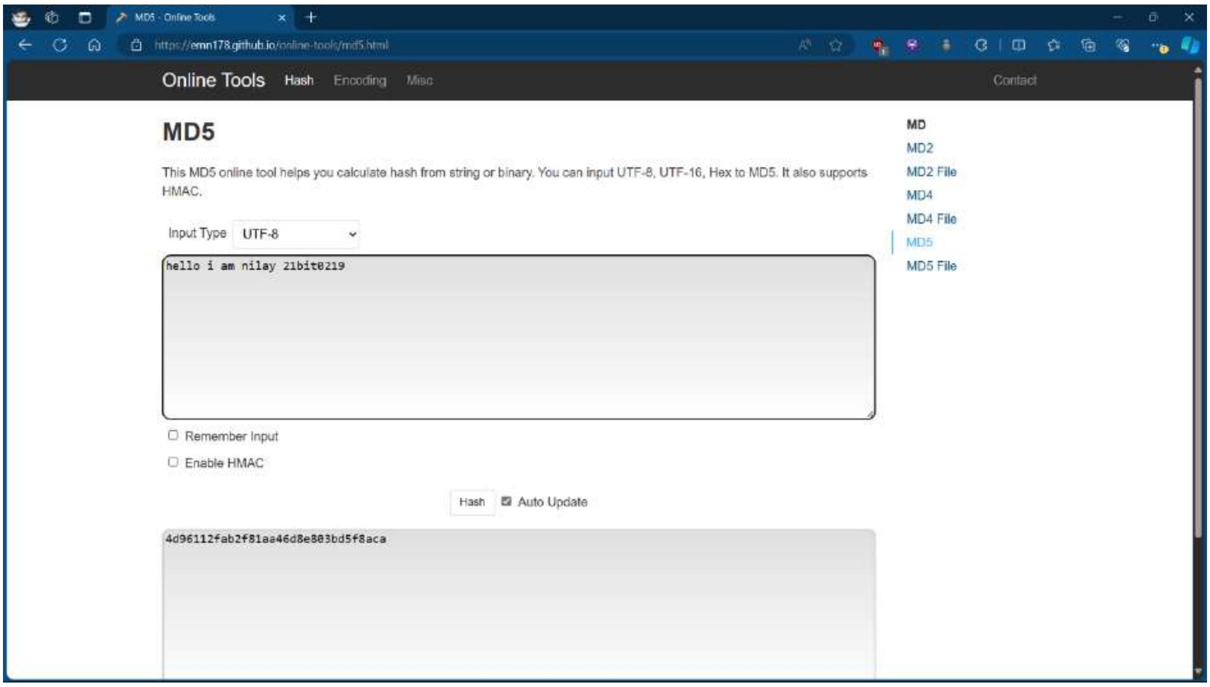
KMAC
KMAC128
KMAC128 File
KMAC256
KMAC256 File

RIPEMD
RIPEMD-128
RIPEMD-128 File
RIPEMD-160
RIPEMD-160 File
RIPEMD-256
RIPEMD-256 File
RIPEMD-320
RIPEMD-320 File

Encoding

Base58 Base64 HTML URL

MD5 Hashing demonstration:



MD5

This MD5 online tool helps you calculate hash from string or binary. You can input UTF-8, UTF-16, Hex to MD5. It also supports HMAC.

Input Type UTF-8

```
hello i am nilay 21bit0219
```

□ Remember Input

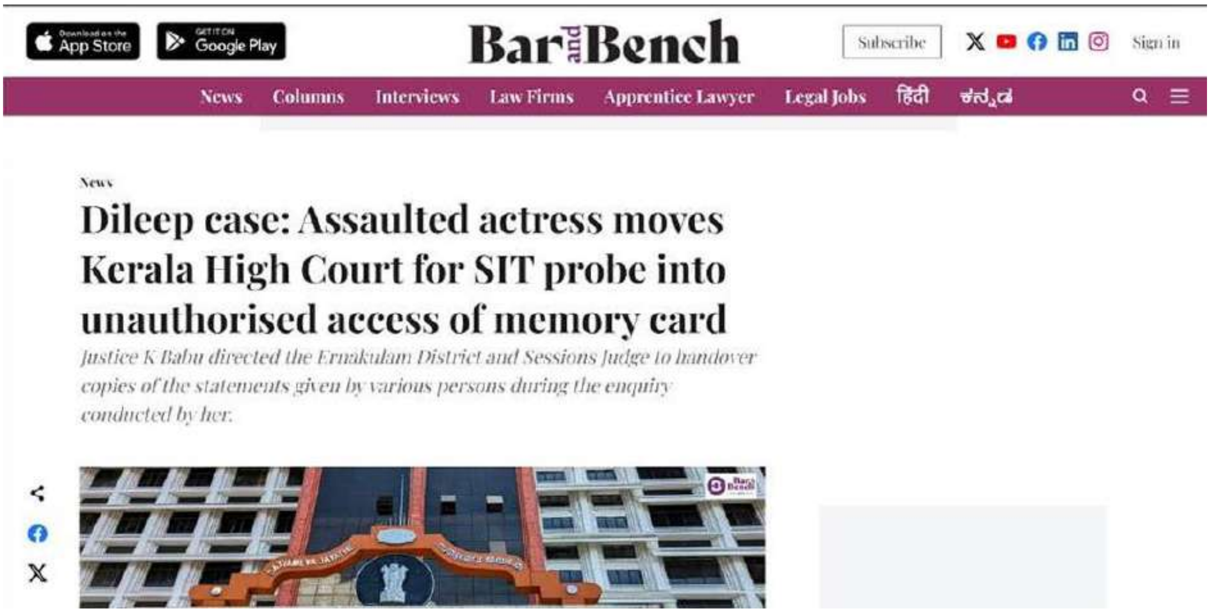
□ Enable HMAC

Hash ☑ Auto Update

```
4d96112fab2f81aa46d8e803bd5f8aca
```

Link: [MD5 - Online Tools (emn178.github.io)](https://emn178.github.io/online-tools/md5.html)

Case study : Dileep case



News

Dileep case: Assaulted actress moves Kerala High Court for SIT probe into unauthorised access of memory card

Justice K Babu directed the Ernakulam District and Sessions Judge to handover copies of the statements given by various persons during the enquiry conducted by her.

Bhavana Menon, a popular actress from the southern Indian state of Kerala, who was abducted and sexually assaulted in 2017, has broken her silence after five years, describing her "difficult journey from being a victim to a survivor".

Menon, who has worked in more than 80 films in southern Indian languages and won a number of prestigious awards, was assaulted by a group of men while travelling from Thrissur to Kochi in February 2017.

Her assault made headlines, especially after Dileep, one of the Malayalam-language film industry's biggest actors and Menon's co-star in half a dozen films, was named as an accused and charged with criminal conspiracy. He denied the charges against him, but was arrested and held in custody for three months before being released on bail. The case is being heard in a trial court.

"I was just a normal fun-loving girl and then this one incident happened that turned my life upside down. Most people see the smiling photos I post on social media, but I have been to hell and back," Menon told me on the phone from the southern city of Bangalore.

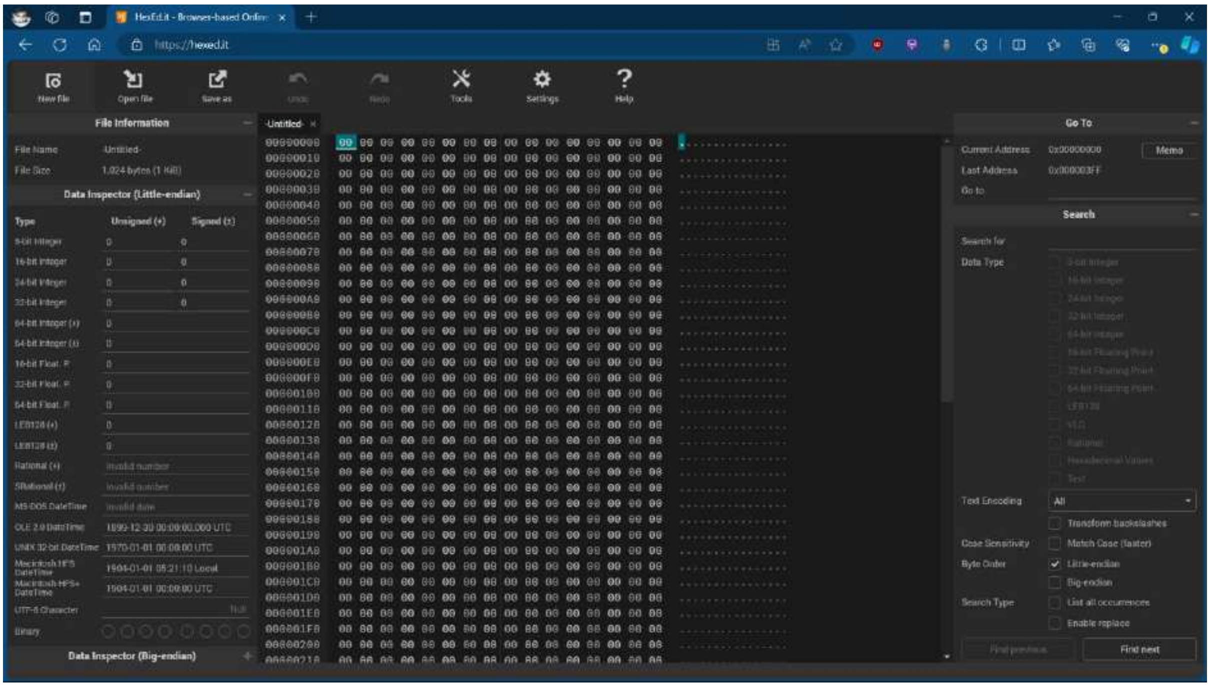
"I became this victim, this 'assaulted actress'. And for long, I kept asking, 'Why me?' I was blaming myself and I was looking for a way out," she said.

"But in 2020, after the trial began, I spent 15 days giving evidence in court. And that's when things changed. Here I was, wanting to forget and move on, but then I had to remember everything, every tiny detail about the case."

On the day of her assault, Menon was travelling from her hometown Thrissur to the city of Kochi, where she was to dub for a film the next morning, when she was kidnapped. Her attackers made videos of the assault - "maybe they wanted to blackmail me", she told me.

Hexed.it

Converts a file into hexcode.



File Information

File Name	-Untitled-
File Size	1,024 bytes (1 KiB)

Data Inspector (Little-endian)

Type	Unsigned (+)	Signed (±)
8-bit Integer	0	0
16-bit Integer	0	0
24-bit Integer	0	0
32-bit Integer	0	0
64-bit Integer (+)	0	
64-bit Integer (±)	0	
16-bit Float. P	0	
32-bit Float. P	0	
64-bit Float. P	0	
LEB128 (+)	0	
LEB128 (±)	0	
Rational (+)	invalid number	
SRational (±)	invalid number	
MS-DOS DateTime	invalid date	
OLE 2.0 DateTime	1899-12-30 00:00:00.000 UTC	
UNIX 32-bit DateTime	1970-01-01 00:00:00 UTC	
Macintosh HFS DateTime	1904-01-01 05:21:10 Local	
Macintosh HFS+ DateTime	1904-01-01 00:00:00 UTC	
UTF-8 Character	NUL	
Binary	○○○○○○○○	

Data Inspector (Big-endian)

```
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

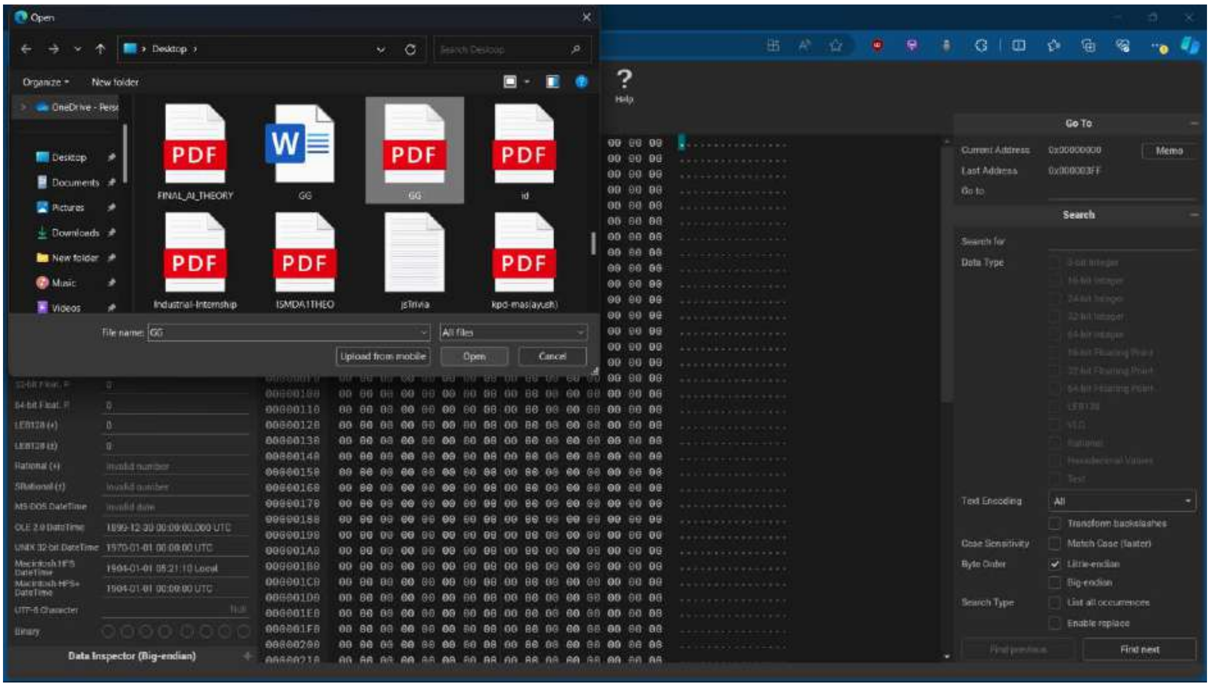
Go To

Current Address	0x00000000
Last Address	0x000003FF
Go to	

Search

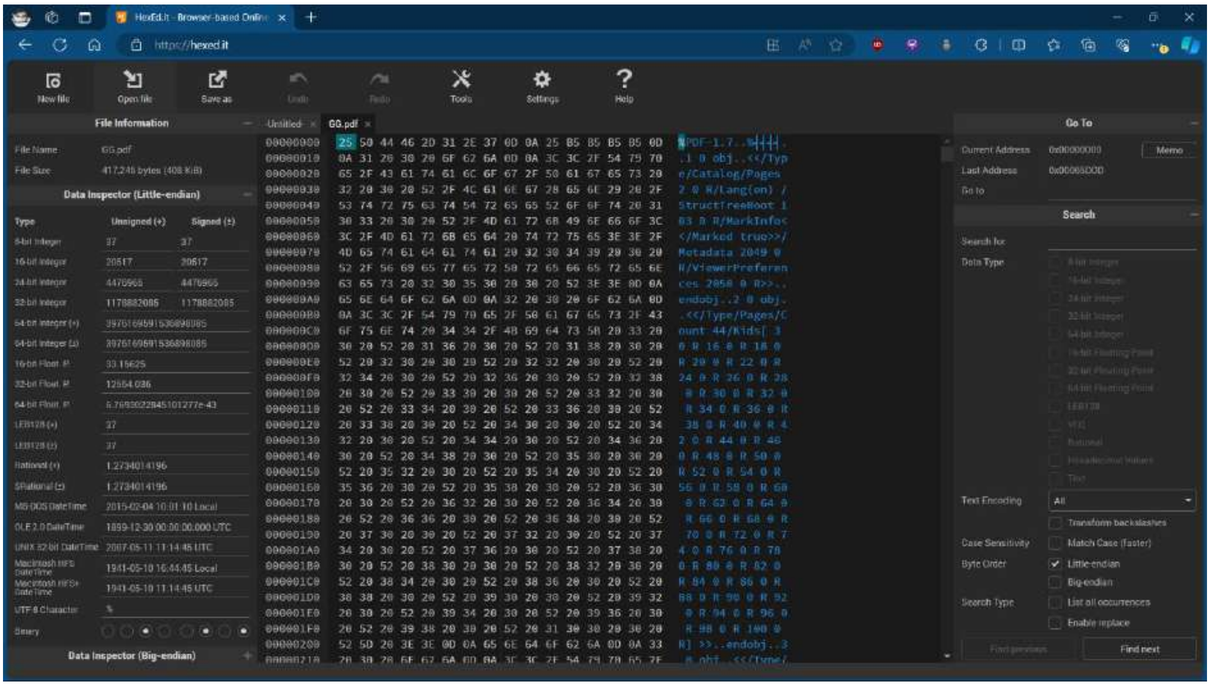
Search for	
Data Type	□ 8-bit Integer □ 16-bit Integer □ 24-bit Integer □ 32-bit Integer □ 64-bit Integer □ 16-bit Floating Point □ 32-bit Floating Point □ 64-bit Floating Point □ LEB128 □ VLQ □ Rational □ Hexadecimal Values □ Text
Text Encoding	All
	□ Transform backslashes
Case Sensitivity	□ Match Case (faster)
Byte Order	☑ Little-endian □ Big-endian
Search Type	□ List all occurrences □ Enable replace

Select a file



File name: GG

All files



File Information

File Name	GG.pdf
File Size	417,245 bytes (408 KiB)

Data Inspector (Little-endian)

Type	Unsigned (+)	Signed (±)
8-bit Integer	37	37
16-bit Integer	20517	20517
24-bit Integer	4470965	4470965
32-bit Integer	1178882085	1178882085
64-bit Integer (+)	3976169591536898085	
64-bit Integer (±)	3976169591536898085	
16-bit Float. P	33.15625	
32-bit Float. P	12554.036	
64-bit Float. P	6.7693022845101277e-43	
LEB128 (+)	37	
LEB128 (±)	37	
Rational (+)	1.2734014196	
SRational (±)	1.2734014196	
MS-DOS DateTime	2015-02-04 10:01:10 Local	
OLE 2.0 DateTime	1899-12-30 00:00:00.000 UTC	
UNIX 32-bit DateTime	2007-05-11 11:14:45 UTC	
Macintosh HFS Date Time	1941-05-10 16:44:45 Local	
Macintosh HFS+ Date Time	1941-05-10 11:14:45 UTC	
UTF-8 Character	%	
Binary	○ ○ ● ○ ○ ● ○ ●	

Data Inspector (Big-endian)

```
00000000  25 50 44 46 2D 31 2E 37 0D 0A 25 B5 B5 B5 B5 0D  %PDF-1.7..%╡╡╡╡.
00000010  0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70  .1 0 obj..<</Typ
00000020  65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20  e/Catalog/Pages 
00000030  32 20 30 20 52 2F 4C 61 6E 67 28 65 6E 29 20 2F  2 0 R/Lang(en) /
00000040  53 74 72 75 63 74 54 72 65 65 52 6F 6F 74 20 31  StructTreeRoot 1
00000050  30 33 20 30 20 52 2F 4D 61 72 6B 49 6E 66 6F 3C  03 0 R/MarkInfo<
00000060  3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E 3E 2F  </Marked true>>/
00000070  4D 65 74 61 64 61 74 61 20 32 30 34 39 20 30 20  Metadata 2049 0 
00000080  52 2F 56 69 65 77 65 72 50 72 65 66 65 72 65 6E  R/ViewerPreferen
00000090  63 65 73 20 32 30 35 30 20 30 20 52 3E 3E 0D 0A  ces 2050 0 R>>..
000000A0  65 6E 64 6F 62 6A 0D 0A 32 20 30 20 6F 62 6A 0D  endobj..2 0 obj.
000000B0  0A 3C 3C 2F 54 79 70 65 2F 50 61 67 65 73 2F 43  .<</Type/Pages/C
000000C0  6F 75 6E 74 20 34 34 2F 4B 69 64 73 5B 20 33 20  ount 44/Kids[ 3 
000000D0  30 20 52 20 31 36 20 30 20 52 20 31 38 20 30 20  0 R 16 0 R 18 0 
000000E0  52 20 32 30 20 30 20 52 20 32 32 20 30 20 52 20  R 20 0 R 22 0 R 
000000F0  32 34 20 30 20 52 20 32 36 20 30 20 52 20 32 38  24 0 R 26 0 R 28
00000100  20 30 20 52 20 33 30 20 30 20 52 20 33 32 20 30   0 R 30 0 R 32 0
00000110  20 52 20 33 34 20 30 20 52 20 33 36 20 30 20 52   R 34 0 R 36 0 R
00000120  20 33 38 20 30 20 52 20 34 30 20 30 20 52 20 34   38 0 R 40 0 R 4
00000130  32 20 30 20 52 20 34 34 20 30 20 52 20 34 36 20  2 0 R 44 0 R 46 
00000140  30 20 52 20 34 38 20 30 20 52 20 35 30 20 30 20  0 R 48 0 R 50 0 
00000150  52 20 35 32 20 30 20 52 20 35 34 20 30 20 52 20  R 52 0 R 54 0 R 
00000160  35 36 20 30 20 52 20 35 38 20 30 20 52 20 36 30  56 0 R 58 0 R 60
00000170  20 30 20 52 20 36 32 20 30 20 52 20 36 34 20 30   0 R 62 0 R 64 0
00000180  20 52 20 36 36 20 30 20 52 20 36 38 20 30 20 52   R 66 0 R 68 0 R
00000190  20 37 30 20 30 20 52 20 37 32 20 30 20 52 20 37   70 0 R 72 0 R 7
000001A0  34 20 30 20 52 20 37 36 20 30 20 52 20 37 38 20  4 0 R 76 0 R 78 
000001B0  30 20 52 20 38 30 20 30 20 52 20 38 32 20 30 20  0 R 80 0 R 82 0 
000001C0  52 20 38 34 20 30 20 52 20 38 36 20 30 20 52 20  R 84 0 R 86 0 R 
000001D0  38 38 20 30 20 52 20 39 30 20 30 20 52 20 39 32  88 0 R 90 0 R 92
000001E0  20 30 20 52 20 39 34 20 30 20 52 20 39 36 20 30   0 R 94 0 R 96 0
000001F0  20 52 20 39 38 20 30 20 52 20 31 30 30 20 30 20   R 98 0 R 100 0 
00000200  52 5D 20 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 33  R] >>..endobj..3
00000210  20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F   0 obj..<</Type/
```

Go To

Current Address	0x00000000
Last Address	0x00065DDD
Go to	

Search

Search for

Data Type
□ 8-bit Integer
□ 16-bit Integer
□ 24-bit Integer
□ 32-bit Integer
□ 64-bit Integer
□ 16-bit Floating Point
□ 32-bit Floating Point
□ 64-bit Floating Point
□ LEB128
□ VLQ
□ Rational
□ Hexadecimal Values
□ Text

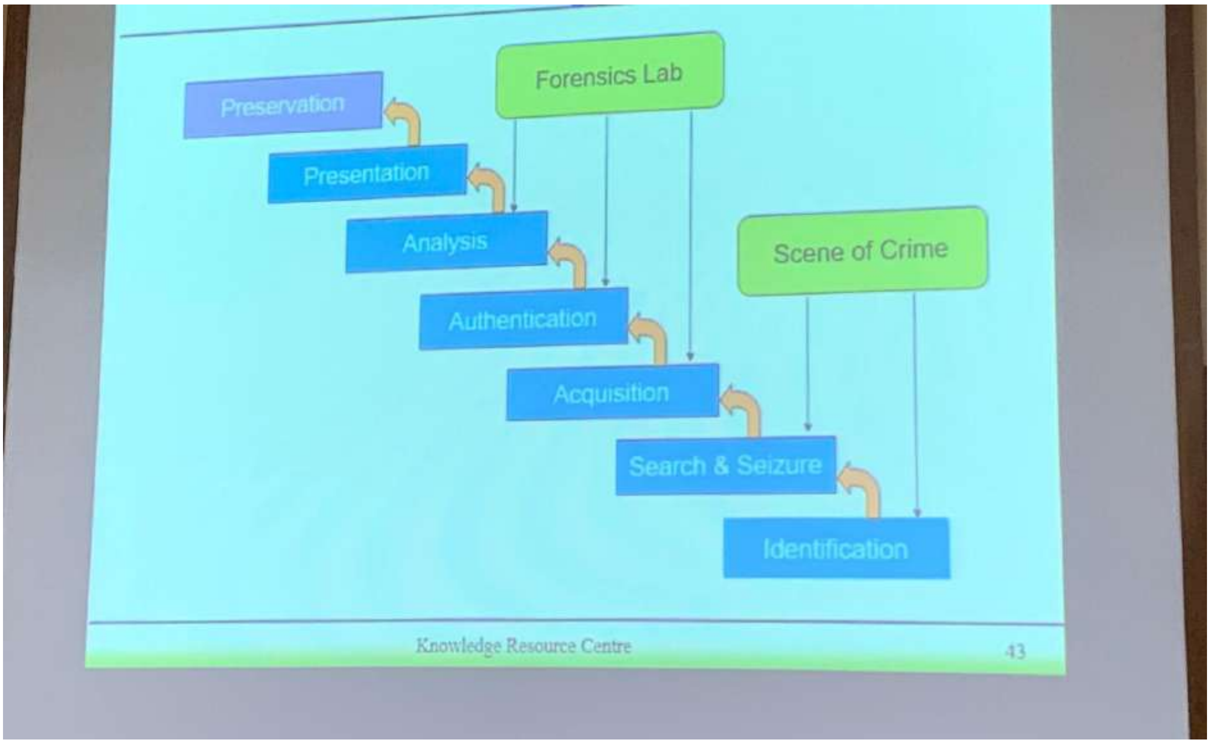
Text Encoding: All
□ Transform backslashes

Case Sensitivity: □ Match Case (faster)

Byte Order: ☑ Little-endian
□ Big-endian

Search Type: □ List all occurrences
□ Enable replace

Cyber forensics step



Forensics Lab

Scene of Crime

Preservation

Presentation

Analysis

Authentication

Acquisition

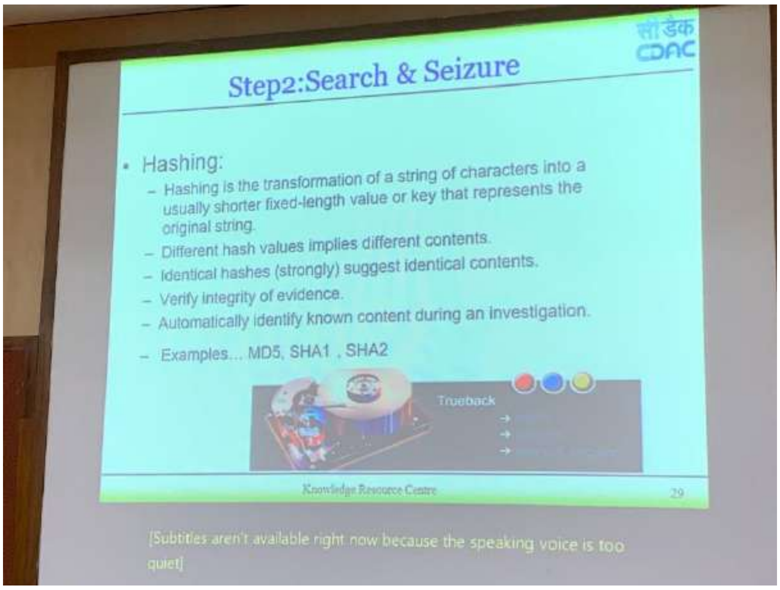
Search & Seizure

Identification

Knowledge Resource Centre 43

Identification: This step involves identifying potential sources of digital evidence, such as computers, mobile devices, servers, networks, and storage media, that may contain relevant information related to the investigation.

Search and Seize: Once potential sources of evidence are identified, the next step is to conduct a search and seizure operation to locate and secure the devices or media. Proper procedures and chain of custody protocols must be followed to ensure the admissibility of evidence in legal proceedings.



सी-डैक CDAC

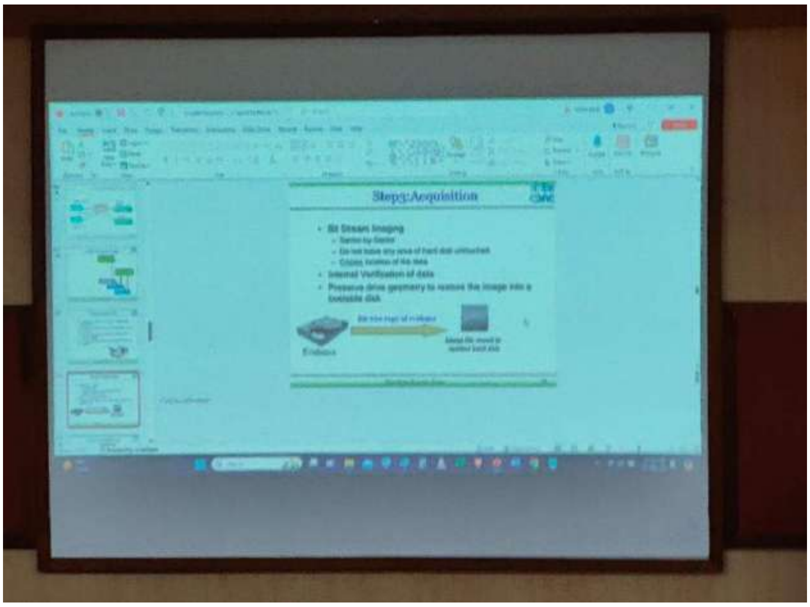
Step2:Search & Seizure

- Hashing:
  - Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.
  - Different hash values implies different contents.
  - Identical hashes (strongly) suggest identical contents.
  - Verify integrity of evidence.
  - Automatically identify known content during an investigation.
  - Examples... MD5, SHA1 , SHA2

Knowledge Resource Centre 29

[Subtitles aren't available right now because the speaking voice is too quiet]

Acquisition: After seizing the devices or media, forensic experts acquire a forensic image or copy of the data using specialized tools and techniques. This process involves creating an exact bit-for-bit copy of the original storage media to preserve the integrity of the evidence.

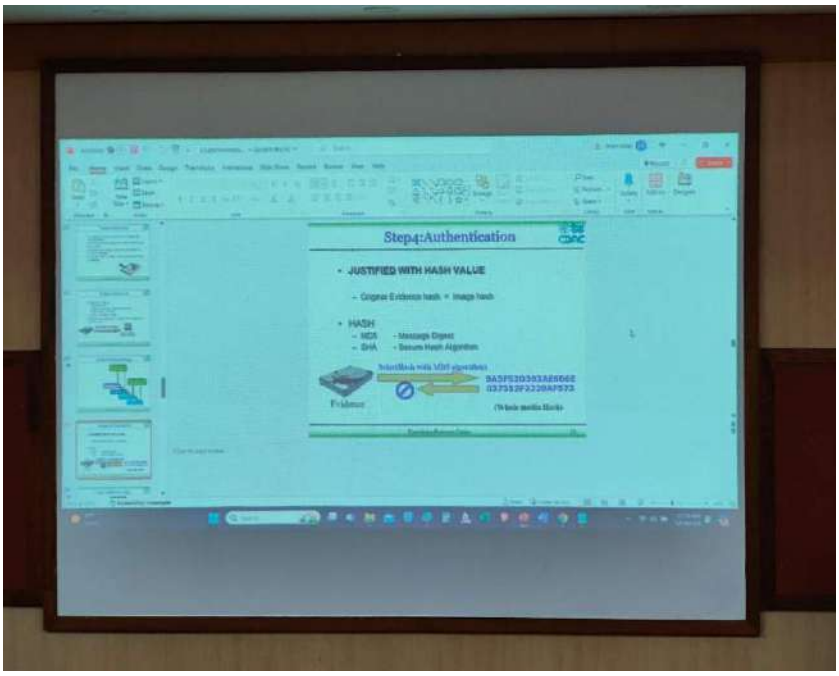


Step3:Acquisition

- Bit Stream Imaging
  - Sector by Sector
  - Do not leave any area of hard disk untouched
  - Copies locations of file data
- Internal Verification of data
- Preserve drive geometry to restore the image into a bootable disk

Bit wise copy of evidence
Evidence
Image file stored in another hard disk

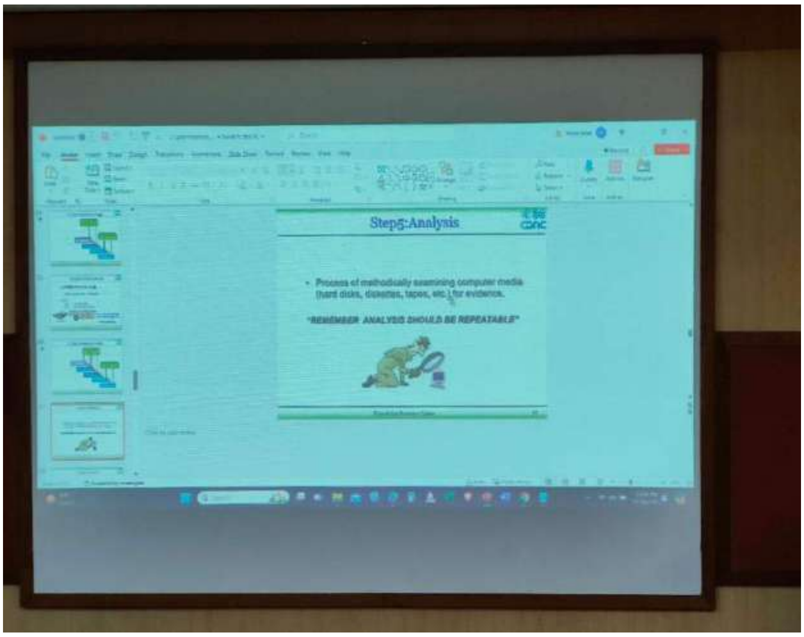
Authentication: The acquired data is then authenticated to verify its integrity and ensure that it has not been altered or tampered with since its acquisition. This step is crucial for establishing the reliability and admissibility of the evidence in legal proceedings.



Step4:Authentication

- JUSTIFIED WITH HASH VALUE
  - Original Evidence hash = Image hash
- HASH
  - MD5 - Message Digest
  - SHA - Secure Hash Algorithm

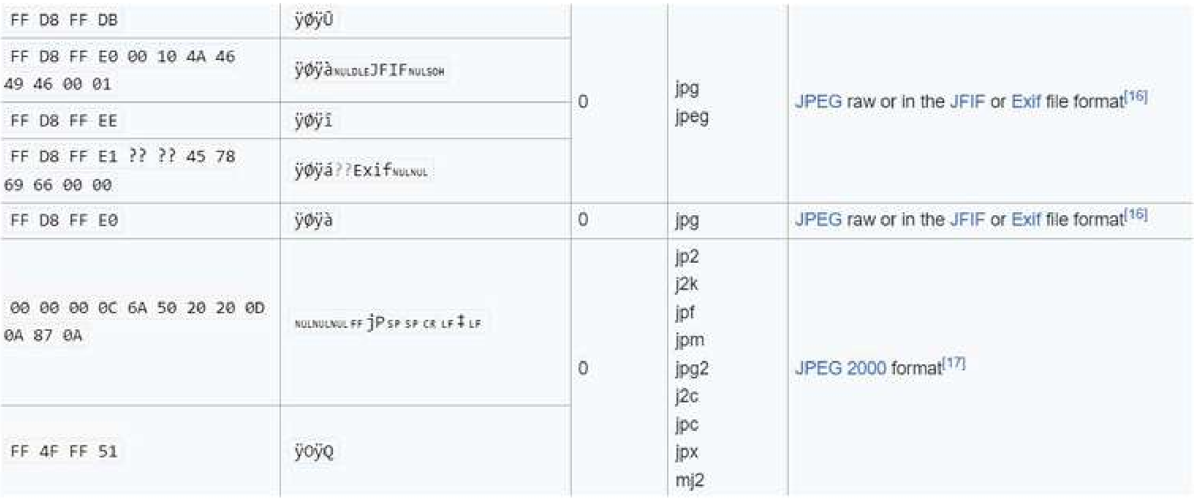
Analysis: With the authenticated data, forensic analysts conduct a thorough examination to identify relevant information related to the investigation. Various tools and methodologies are used to analyze files, documents, system logs, internet history, emails, and other digital artifacts for evidence of illegal activities or security breaches.



Step5:Analysis

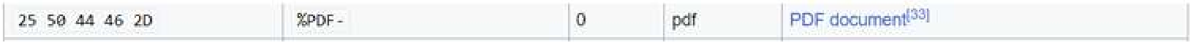
- Process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.

"REMEMBER ANALYSIS SHOULD BE REPEATABLE"



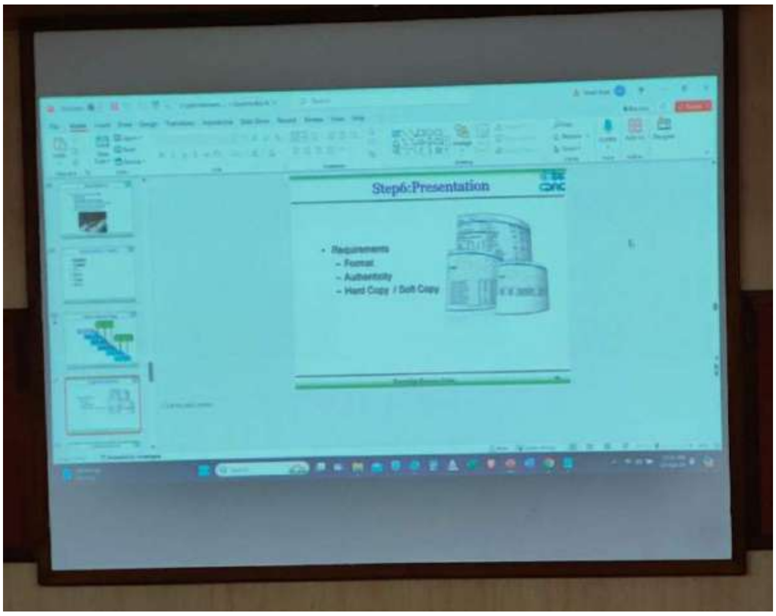
FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format[16]
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà NUL DLE JFIF NUL SOH			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá ? ? Exif NUL NUL			
FF D8 FF E0	ÿØÿà	0	jpg	JPEG raw or in the JFIF or Exif file format[16]
00 00 00 0C 6A 50 20 20 0D 0A 87 0A	NUL NUL NUL FF jP SP SP CR LF ‡ LF	0	jp2 j2k jpf jpm jpg2 j2c jpc jpx mj2	JPEG 2000 format[17]
FF 4F FF 51	ÿOÿQ			

Pdf format:



25 50 44 46 2D	%PDF-	0	pdf	PDF document[33]

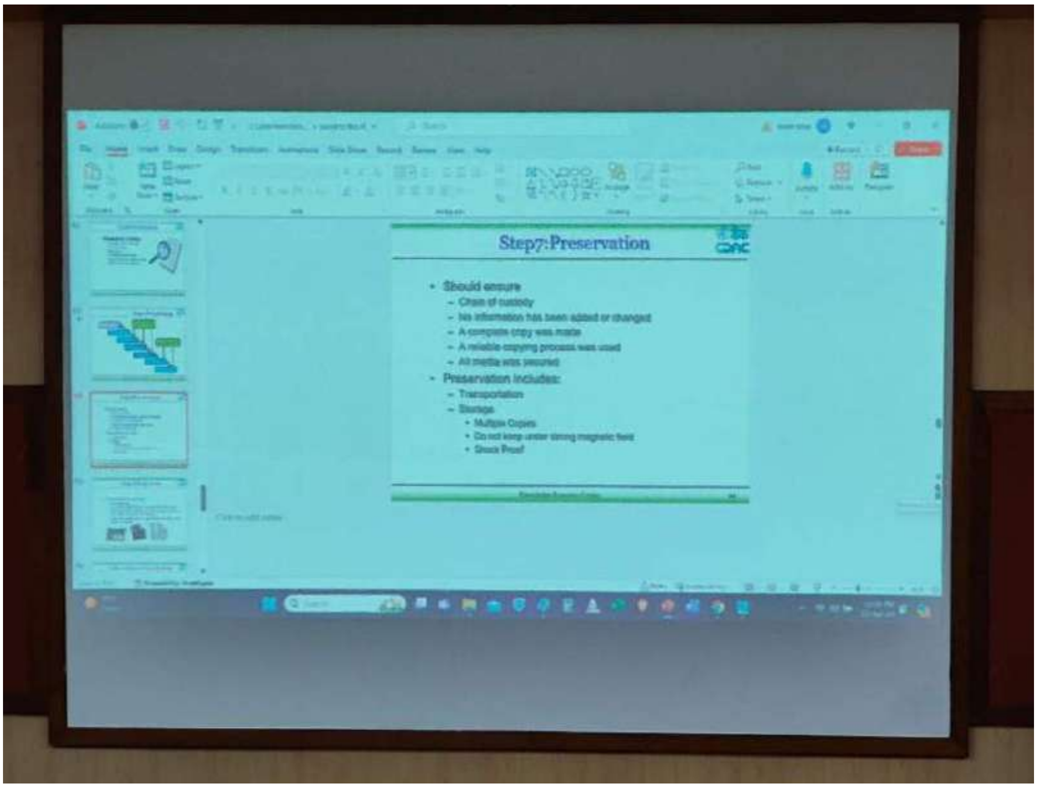
Presentation: Once the analysis is complete, forensic experts may present their findings and analysis in a clear and concise manner, often in the form of reports, presentations, or expert testimony. This presentation of evidence may be required in legal proceedings, disciplinary actions, or internal investigations.



Step6:Presentation

- Requirements
  - Format
  - Authenticity
  - Hard Copy / Soft Copy

Preservation: After the investigation is concluded, the preserved evidence must be securely stored and maintained to ensure its integrity and prevent any accidental loss or alteration. Proper conservation practices are essential for preserving the evidentiary value of the data for future reference or use.

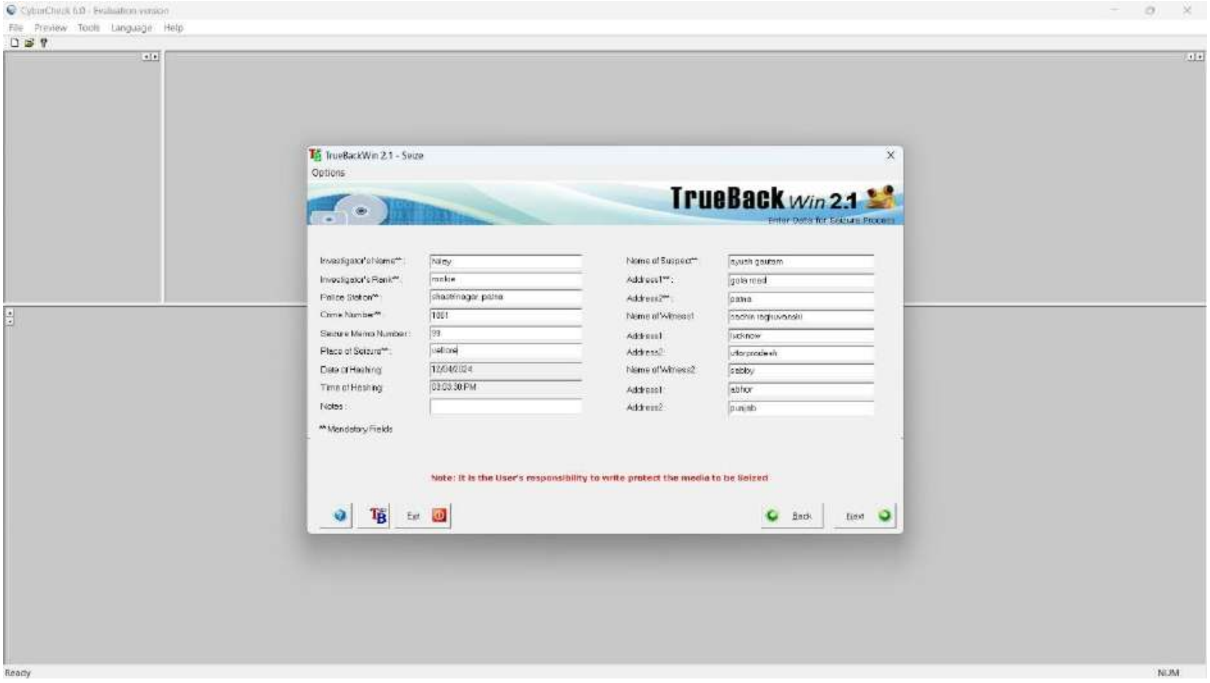


Step7:Preservation

- Should ensure
  - Chain of custody
  - No information has been added or changed
  - A complete copy was made
  - A reliable copying process was used
  - All media was secured
- Preservation includes:
  - Transportation
  - Storage
    - Multiple Copies
    - Do not keep under strong magnetic field
    - Shock Proof

Seize and Acquire practical using TrueBack application

Open software select seize and acquire option.

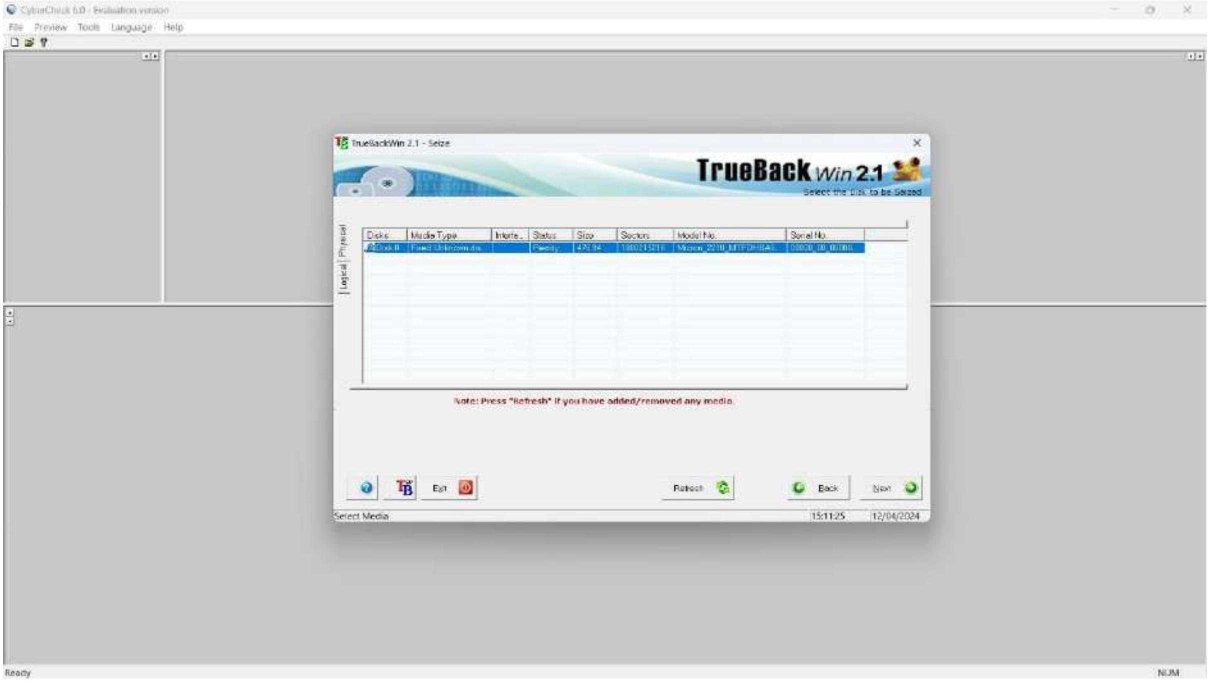

CyberCheck 6.0 - Evaluation version
File Preview Tools Language Help
TrueBackWin 2.1 - Seize
Options
TrueBack Win 2.1
Enter Data for Seizure Process
Exit
Back
Next
Ready
NUM

Investigator's Name** :	Nitey	Name of Suspect**	ayush gautam
Investigator's Rank** :	rookie	Address1** :	gola road
Police Station** :	shastrinagar patna	Address2** :	patna
Crime Number** :	1001	Name of Witness1	sachin raghuvanshi
Seizure Memo Number :	99	Address1	lucknow
Place of Seizure** :	vellore	Address2	uttarpradesh
Date of Hashing	12/04/2024	Name of Witness2	sabby
Time of Hashing	03:03:30 PM	Address1	abhor
Notes :		Address2	punjab

** Mandatory Fields

Note: It is the User's responsibility to write protect the media to be Seized

Select the created disk

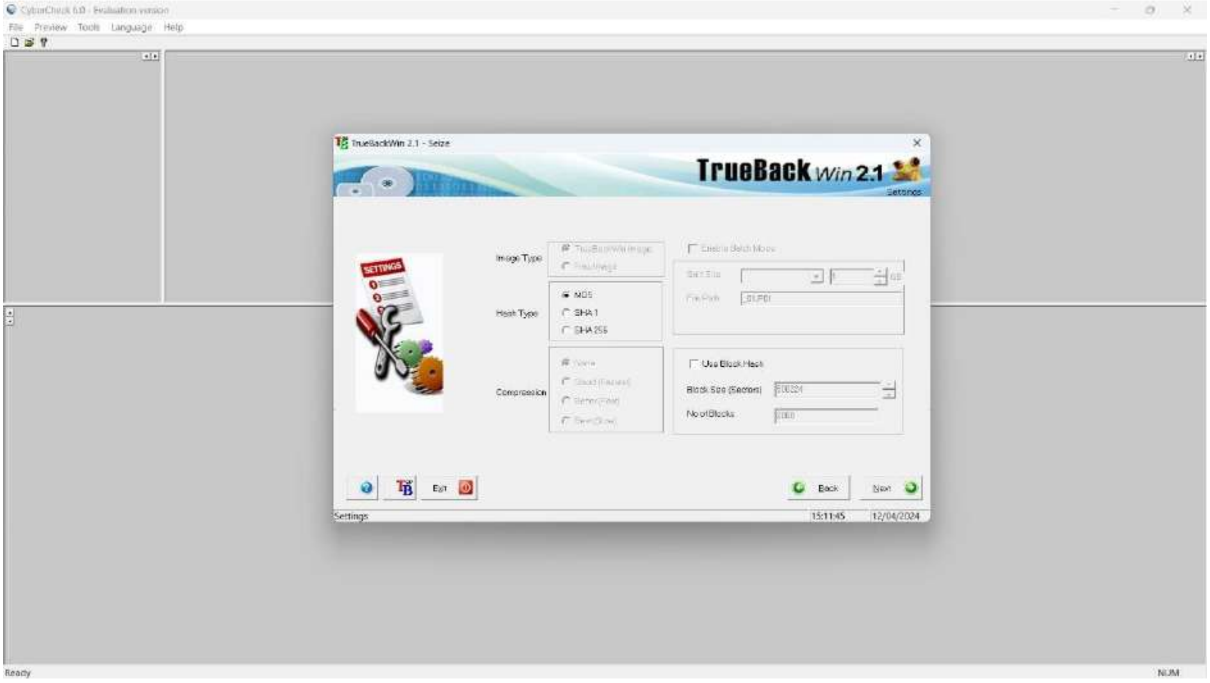

CyberCheck 6.0 - Evaluation version
File Preview Tools Language Help
TrueBackWin 2.1 - Seize
TrueBack Win 2.1
Select the Disk to be Seized
Physical
Logical
Exit
Refresh
Back
Next
Ready
NUM

Disks	Media Type	Interfa...	Status	Size	Sectors	Model No.	Serial No.
Disk 0	Fixed Unknown dis...		Ready	476.94	1000215216	Micron_2210_MTFDHBA5...	0000_00_0000...

Note: Press "Refresh" if you have added/removed any media.

Select Media 15:11:25 12/04/2024

Select a Hashing algorithm for converting the seized data.



CyberCheck 6.0 - Evaluation version
File Preview Tools Language Help
TrueBackWin 2.1 - Seize
TrueBack Win 2.1
Settings
Exit
Back
Next
Ready
NUM

Image Type: ● TrueBackWin Image ○ Raw Image

Hash Type: ● MD5 ○ SHA 1 ○ SHA 256

Compression: ● None ○ Good (Faster) ○ Better (Fast) ○ Best (Slow)

□ Enable Batch Mode

Split Size: 1 GB

File Path: .01.PDI

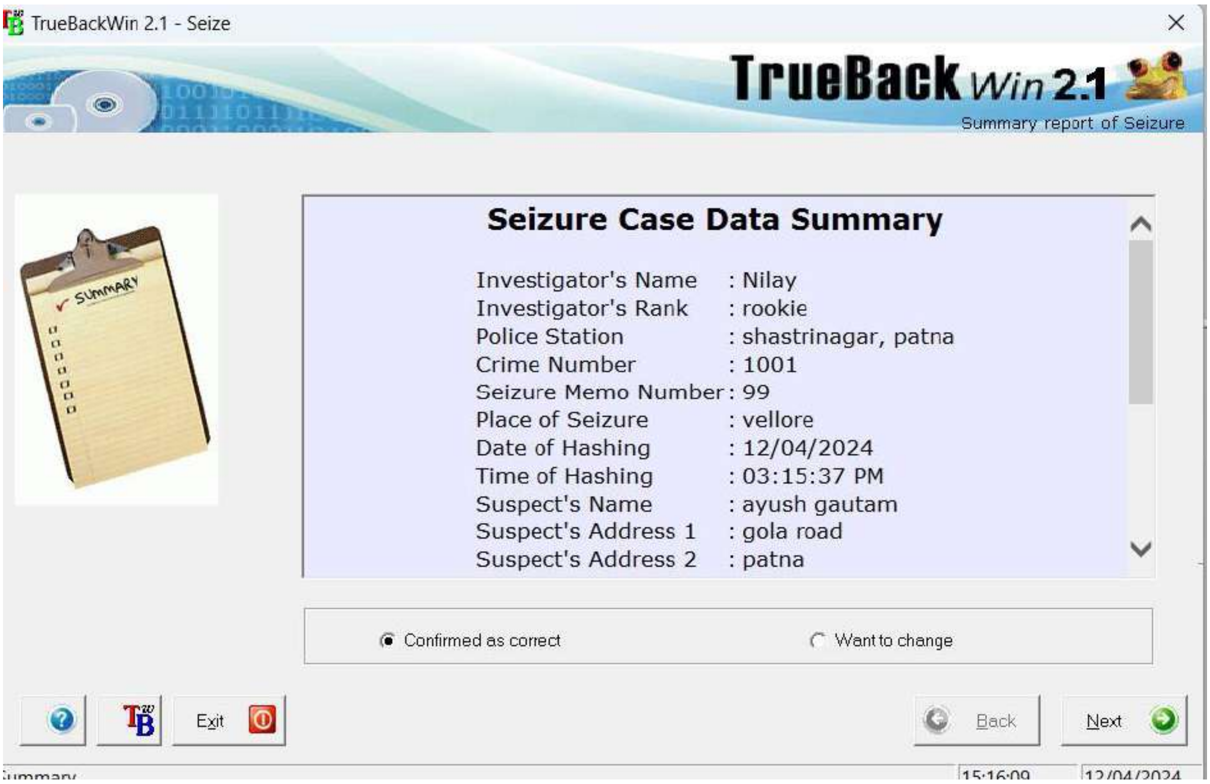
□ Use Block Hash

Block Size (Sectors): 500024

No of Blocks: 1000

Settings 15:11:45 12/04/2024

Summary for confirmation



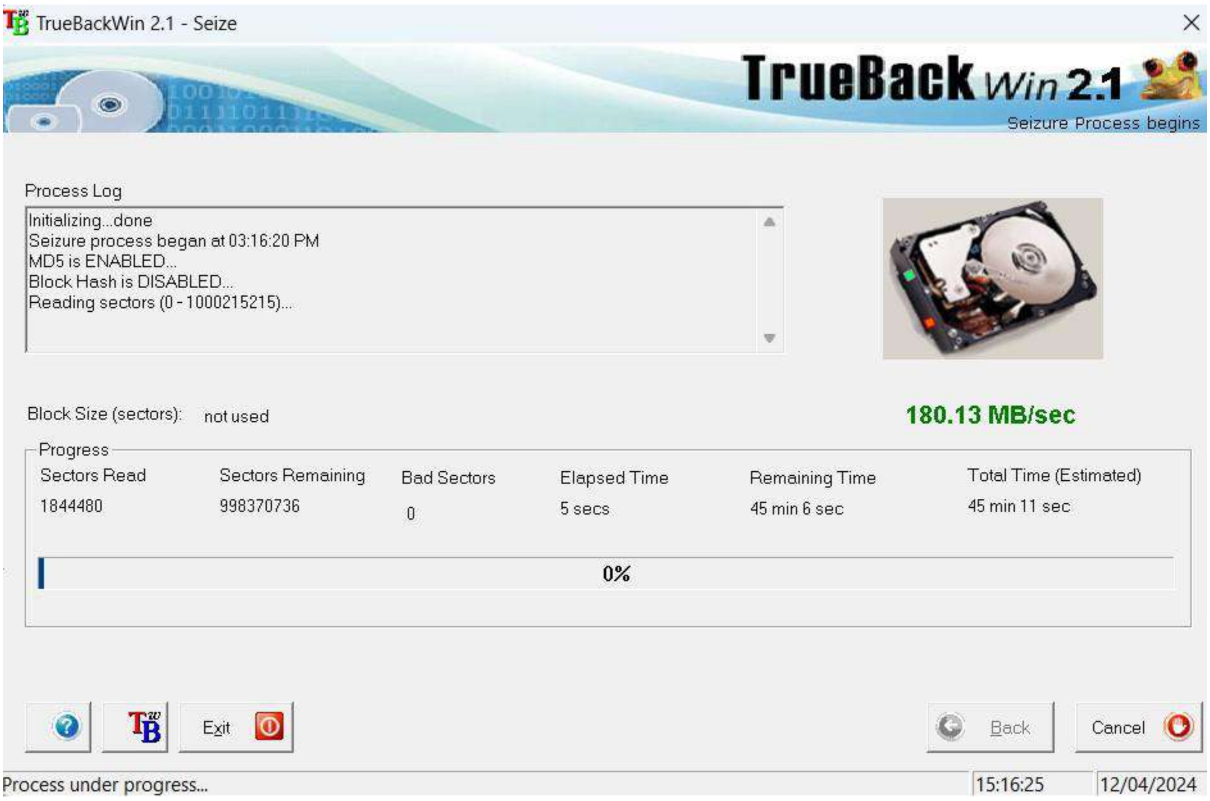
Seizure Case Data Summary

Investigator's Name : Nilay
Investigator's Rank : rookie
Police Station : shastrinagar, patna
Crime Number : 1001
Seizure Memo Number : 99
Place of Seizure : vellore
Date of Hashing : 12/04/2024
Time of Hashing : 03:15:37 PM
Suspect's Name : ayush gautam
Suspect's Address 1 : gola road
Suspect's Address 2 : patna

● Confirmed as correct ○ Want to change

Summary 15:16:09 12/04/2024

Start the seizure process



Process Log

```
Initializing...done
Seizure process began at 03:16:20 PM
MD5 is ENABLED...
Block Hash is DISABLED...
Reading sectors (0 - 1000215215)...
```

Block Size (sectors): not used

180.13 MB/sec

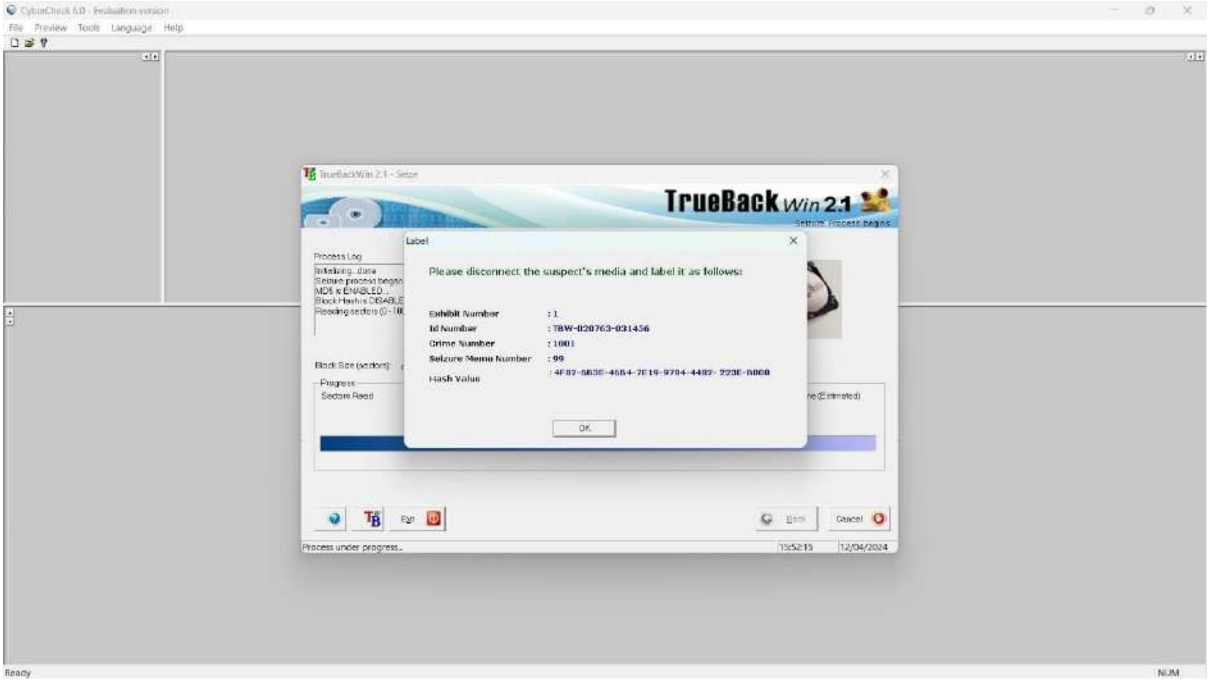
Progress

Sectors Read	Sectors Remaining	Bad Sectors	Elapsed Time	Remaining Time	Total Time (Estimated)
1844480	998370736	0	5 secs	45 min 6 sec	45 min 11 sec

0%

Process under progress... | 15:16:25 | 12/04/2024

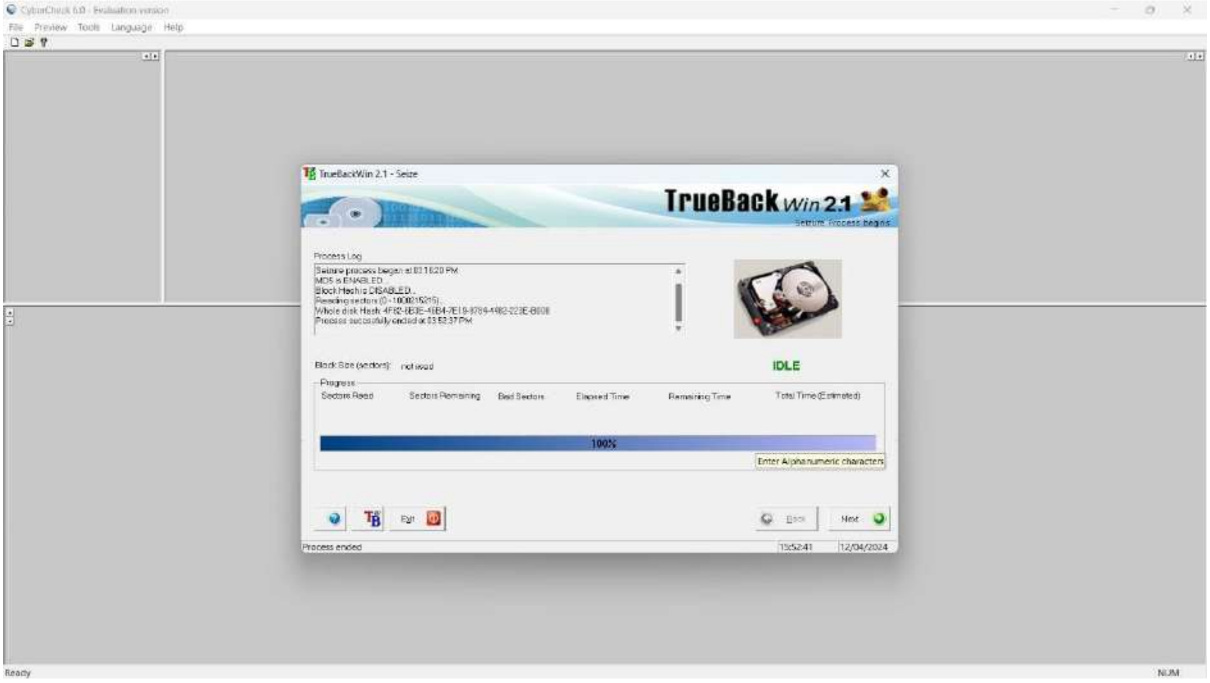
Completion of the process



Please disconnect the suspect's media and label it as follows:

Exhibit Number	: 1
Id Number	: TBW-020763-031456
Crime Number	: 1001
Seizure Memo Number	: 99
Hash Value	: 4F02-5B3E-45B4-7E19-9704-4402-223E-B0D8

Process under progress... | 15:52:15 | 12/04/2024



Process Log

```
Seizure process began at 03:16:20 PM
MD5 is ENABLED..
Block Hash is DISABLED..
Reading sectors (0 - 1000215215)..
Whole disk Hash: 4F62-6B3E-46B4-7E19-8784-4982-223E-B008
Process successfully ended at 03:52:37 PM
```

Block Size (sectors): not read

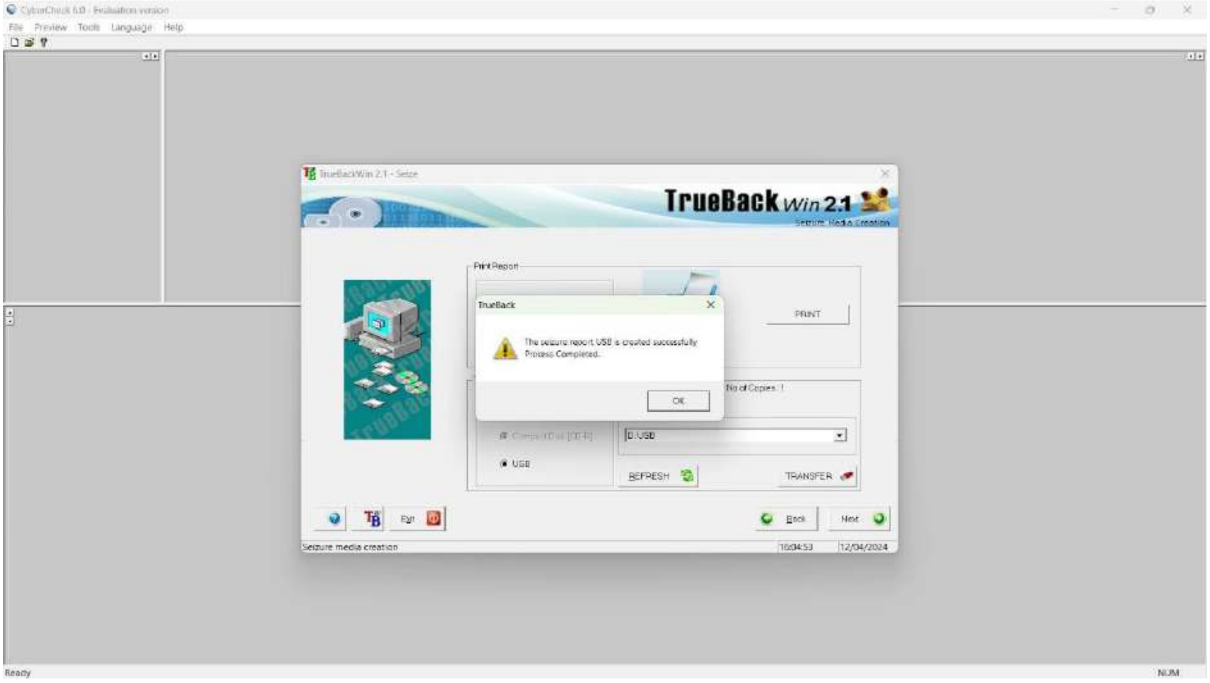
Progress

Sectors Read | Sectors Remaining | Bad Sectors | Elapsed Time | Remaining Time | Total Time (Estimated)

100%

Enter Alphanumeric characters

Process ended 15:52:41 12/04/2024



TrueBack

The seizure report USB is created successfully
Process Completed.

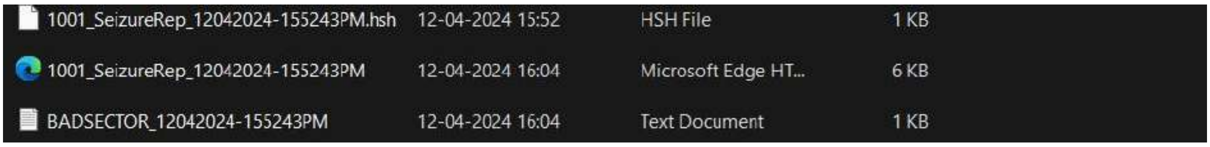
No of Copies : 1

○ Compact Disk [CD-R]
● USB

D:USB

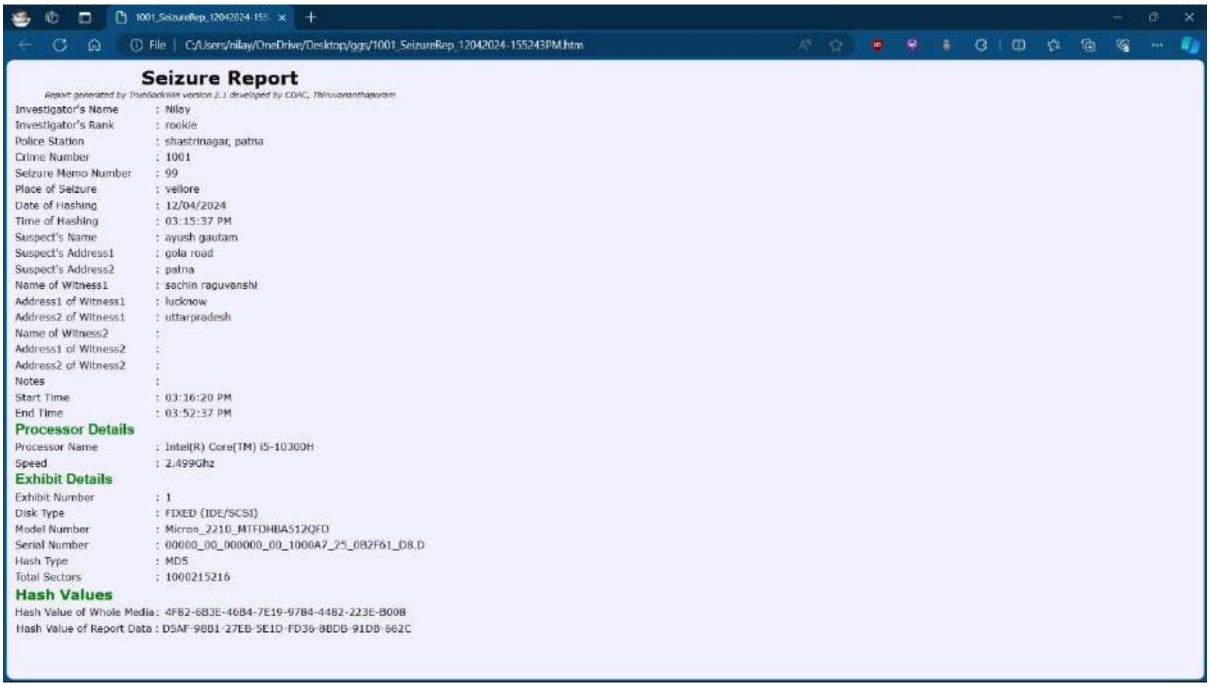
Seizure media creation 16:04:53 12/04/2024

Seizure report successfully created in the pen drive.



1001_SeizureRep_12042024-155243PM.hsh	12-04-2024 15:52	HSH File	1 KB
1001_SeizureRep_12042024-155243PM	12-04-2024 16:04	Microsoft Edge HT...	6 KB
BADSECTOR_12042024-155243PM	12-04-2024 16:04	Text Document	1 KB

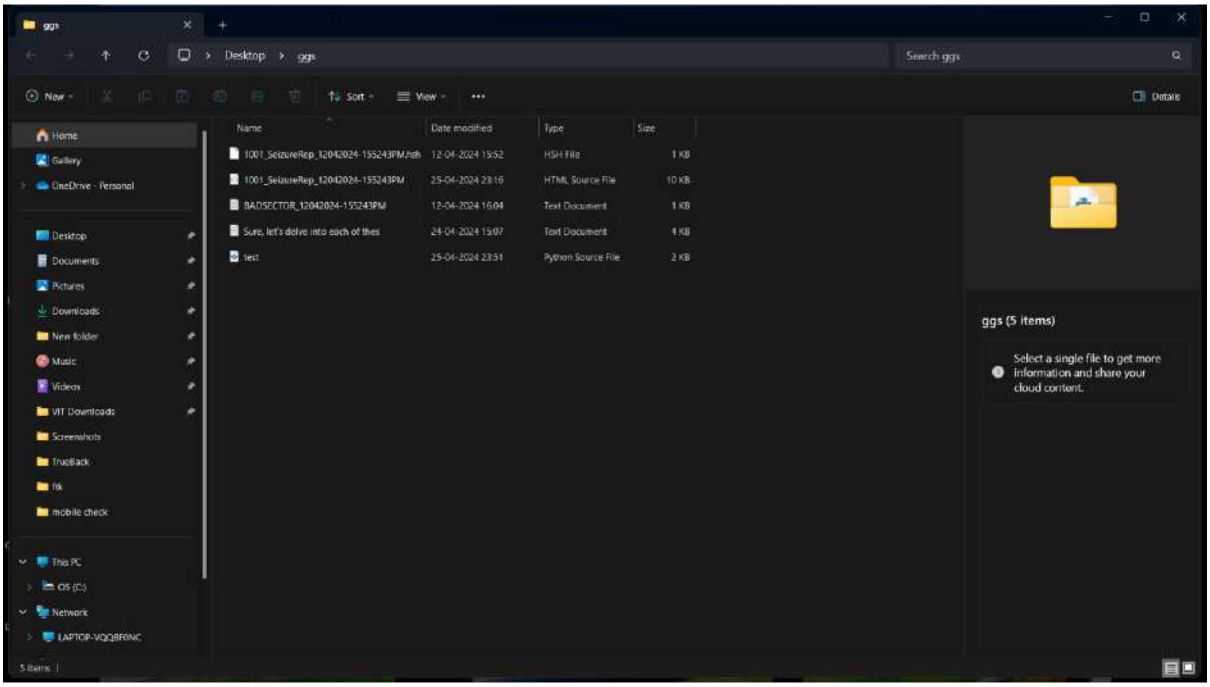
Seizure report:


1001_SeizureRep_12042024-155
File | C:/Users/nilay/OneDrive/Desktop/ggs/1001_SeizureRep_12042024-155243PM.htm

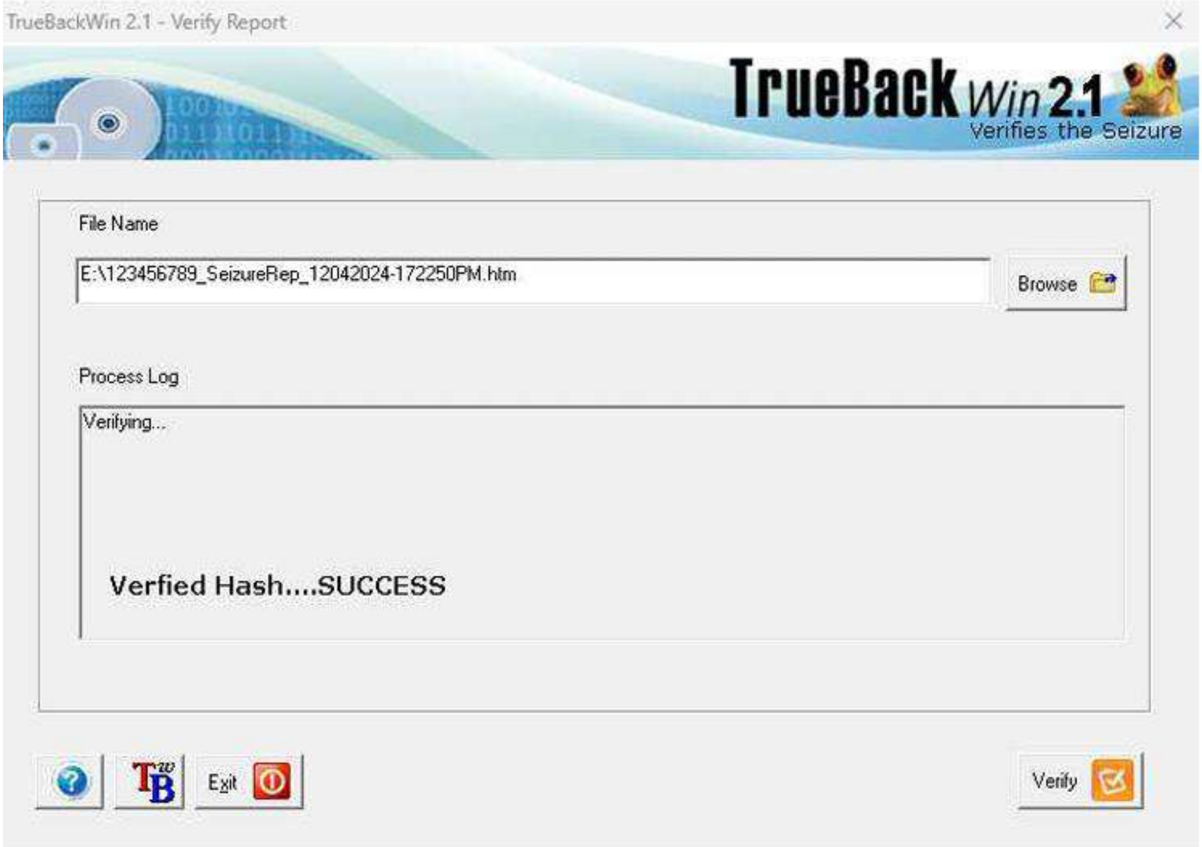
```
Seizure Report
Report generated by TrueBackWin version 2.1 developed by CDAC, Thiruvananthapuram
Investigator's Name     : Nilay
Investigator's Rank     : rookie
Police Station          : shastrinagar, patna
Crime Number            : 1001
Seizure Memo Number     : 99
Place of Seizure        : vellore
Date of Hashing         : 12/04/2024
Time of Hashing         : 03:15:37 PM
Suspect's Name          : ayush gautam
Suspect's Address1      : gola road
Suspect's Address2      : patna
Name of Witness1        : sachin raguvanshi
Address1 of Witness1    : lucknow
Address2 of Witness1    : uttarpradesh
Name of Witness2        :
Address1 of Witness2    :
Address2 of Witness2    :
Notes                   :
Start Time              : 03:16:20 PM
End Time                : 03:52:37 PM
Processor Details
Processor Name          : Intel(R) Core(TM) i5-10300H
Speed                   : 2.499Ghz
Exhibit Details
Exhibit Number          : 1
Disk Type               : FIXED (IDE/SCSI)
Model Number            : Micron_2210_MTFDHBA512QFD
Serial Number           : 00000_00_000000_00_1000A7_25_0B2F61_D8.D
Hash Type               : MD5
Total Sectors           : 1000215216
Hash Values
Hash Value of Whole Media: 4FB2-6B3E-46B4-7E19-9784-4482-223E-B008
Hash Value of Report Data : D5AF-98B1-27EB-5E1D-FD36-8BDB-91DB-662C
```

Acquisition

We open directory in which seized file is present then we select the file which is to be acquired.



Name	Date modified	Type	Size
1001_SeizureRep_12042024-155243PM.hsh	12-04-2024 15:52	HSH File	1 KB
1001_SeizureRep_12042024-155243PM	25-04-2024 23:16	HTML Source File	10 KB
BADSECTOR_12042024-155243PM	12-04-2024 16:04	Text Document	1 KB
Sure, let's delve into each of thes	24-04-2024 15:07	Text Document	4 KB
test	25-04-2024 23:51	Python Source File	2 KB



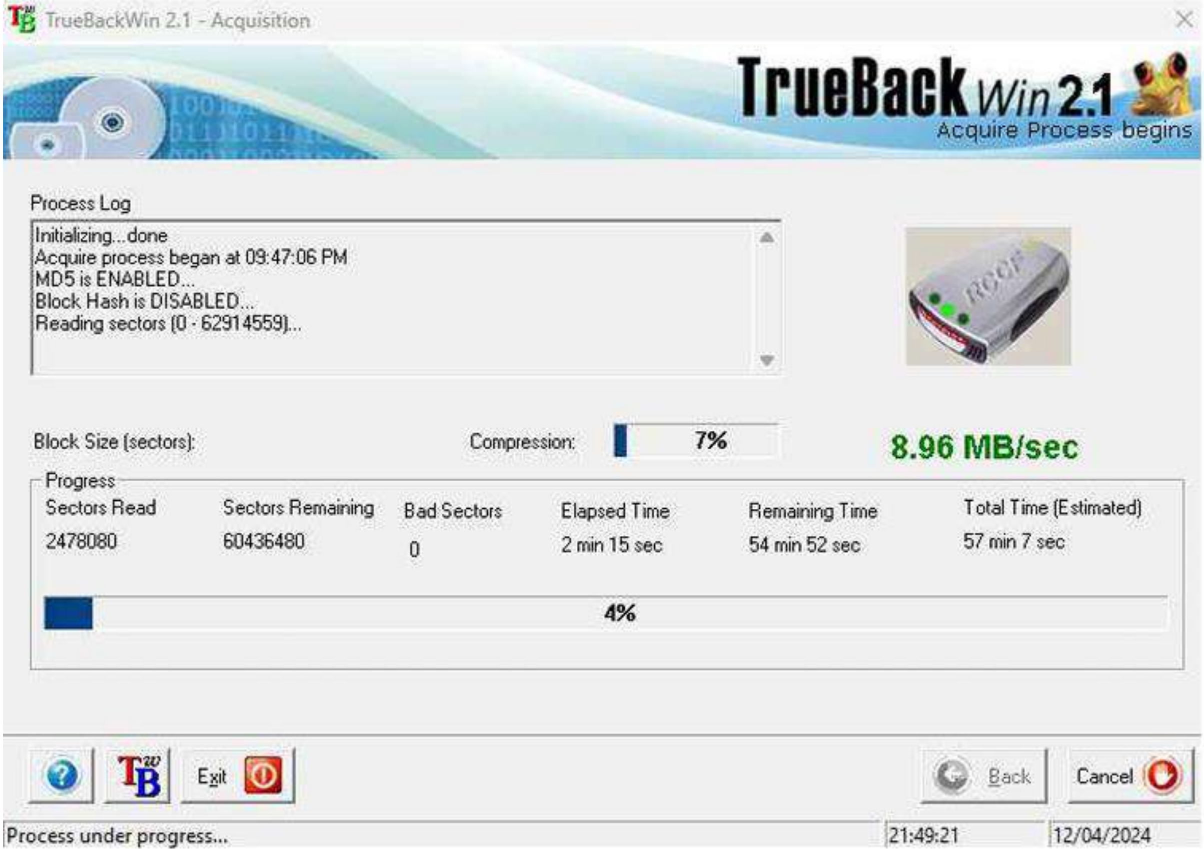
File Name

E:\123456789_SeizureRep_12042024-172250PM.htm

Process Log

```
Verifying...

Verfied Hash....SUCCESS
```



Process Log

```
Initializing...done
Acquire process began at 09:47:06 PM
MD5 is ENABLED...
Block Hash is DISABLED...
Reading sectors (0 - 62914559)...
```

Block Size (sectors):

Compression: 7%

8.96 MB/sec

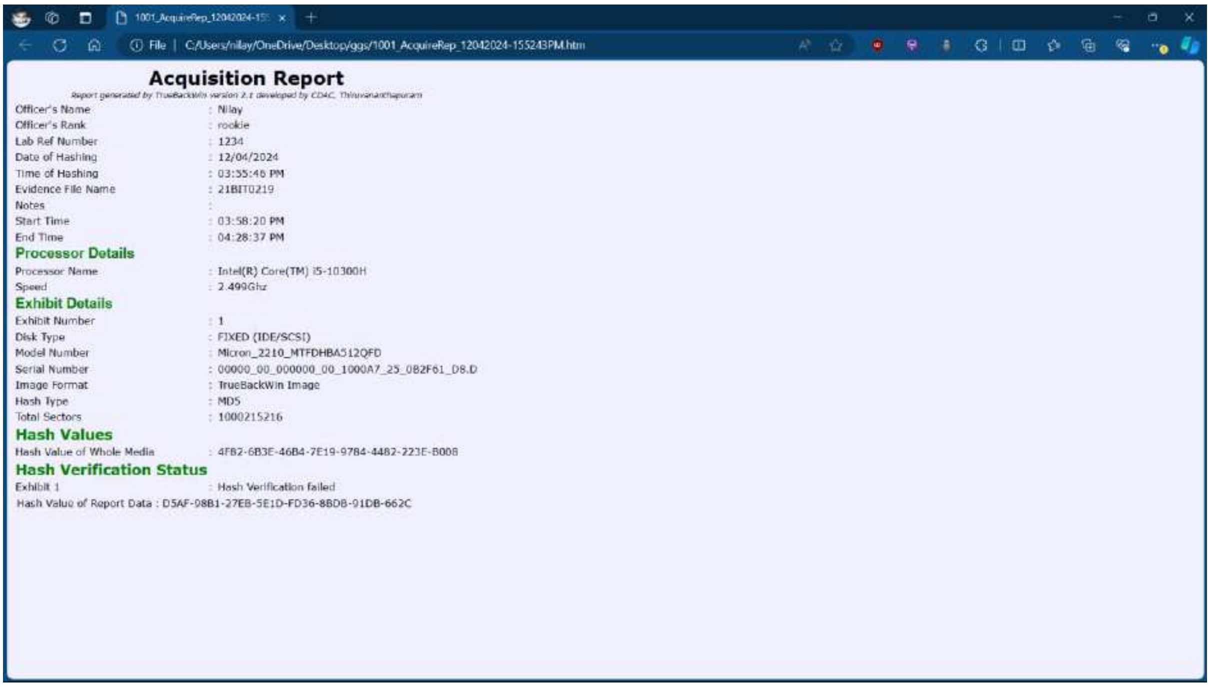
Progress

Sectors Read	Sectors Remaining	Bad Sectors	Elapsed Time	Remaining Time	Total Time (Estimated)
2478080	60436480	0	2 min 15 sec	54 min 52 sec	57 min 7 sec

4%

Process under progress... 21:49:21 12/04/2024

Acquisition Report:


1001_AcquireRep_12042024-15
File | C:/Users/nilay/OneDrive/Desktop/ggs/1001_AcquireRep_12042024-155243PM.htm

Acquisition Report

Report generated by TrueBackWin version 2.1 developed by CDAC, Thiruvananthapuram

Officer's Name	: Nilay
Officer's Rank	: rookie
Lab Ref Number	: 1234
Date of Hashing	: 12/04/2024
Time of Hashing	: 03:55:46 PM
Evidence File Name	: 21BIT0219
Notes	:
Start Time	: 03:58:20 PM
End Time	: 04:28:37 PM

Processor Details

Processor Name	: Intel(R) Core(TM) i5-10300H
Speed	: 2.499Ghz

Exhibit Details

Exhibit Number	: 1
Disk Type	: FIXED (IDE/SCSI)
Model Number	: Micron_2210_MTFDHBA512QFD
Serial Number	: 00000_00_000000_00_1000A7_25_0B2F61_D8.D
Image Format	: TrueBackWin Image
Hash Type	: MD5
Total Sectors	: 1000215216

Hash Values

Hash Value of Whole Media	: 4FB2-6B3E-46B4-7E19-9784-4482-223E-B008

Hash Verification Status

Exhibit 1	: Hash Verification failed

Hash Value of Report Data : D5AF-08B1-27EB-5E1D-FD36-8BDB-91DB-662C

Cardinal Rules

Cyber forensics, also known as digital forensics, involves investigating and analyzing digital devices and data to uncover evidence of cybercrime. Here are some cardinal rules or key principles in cyber forensics:

1. ***Preservation of Evidence:*** Maintain the integrity of digital evidence by ensuring it remains unchanged from the moment of collection throughout the investigation process. Use write-blocking hardware or software to prevent any alterations to the original data.
2. ***Chain of Custody:*** Document and track the handling of evidence from the time of collection to its presentation in court. This ensures accountability and reliability of the evidence, establishing its admissibility in legal proceedings.
3. ***Forensic Soundness:*** Conduct investigations following established forensic methodologies and standards to ensure accuracy, reliability, and legality of the findings. Use validated tools and techniques to collect, analyze, and interpret digital evidence.
4. ***Minimization of Contamination:*** Prevent contamination of digital evidence by handling it with care and avoiding actions that could modify or destroy it. Work in a controlled environment to minimize the risk of inadvertent changes to the evidence.
5. ***Documentation and Reporting:*** Thoroughly document all investigative steps, findings, and conclusions in a clear and organized manner. Prepare detailed reports that can be understood by both technical and non-technical audiences, providing a comprehensive overview of the investigation process and results.
6. ***Legal Compliance:*** Conduct investigations in accordance with applicable laws, regulations, and guidelines, respecting the privacy rights of individuals and adhering to rules of evidence. Obtain proper authorization before accessing and collecting digital evidence.
7. ***Continuous Learning and Adaptation:*** Stay updated on evolving technologies, techniques, and threats in cyber forensics through ongoing training, research, and collaboration with peers. Adapt investigative practices to address new challenges and emerging trends in digital crime.

CARDINAL RULES

Confined Space Entry
Always obtain written authorization before entering a confined space.

Drug & Alcohol Policy
Do not work while fatigued or under the influence of alcohol, drugs/prescription medication which may impair your ability to work safely.

Energy Isolation
Always verify that hazardous energy has been isolated and tagged (lock out/tag out) before performing work or maintenance.

Fall Protection
Always protect against a fall when working from heights greater that 1.88 meters (6 feet) or as otherwise specified by the customer or jurisdictional requirements.

Ground Disturbance
Always follow procedure for locating, identifying and excavating buried facilities.

Incident Reporting
Always report incidents and near-misses in accordance with our incident management procedure.

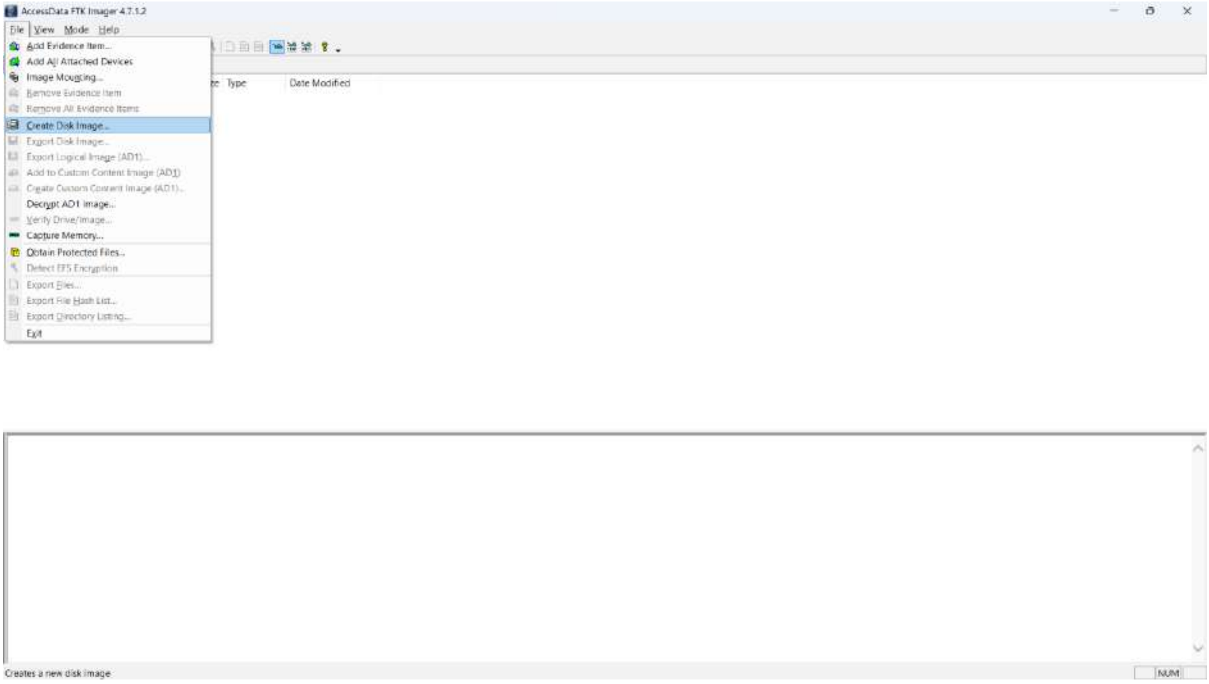
Field Level Risk Assessment (FLRA)
Always complete an FLRA to identify hazards prior to starting work.

Personal Protective Equipment (PPE)
Always wear appropriate PPE for the task at hand.

Safe Driving
Do not drive while fatigued or under the influence of alcohol, drugs/prescription medication or other substance which may impair your ability to drive safely.

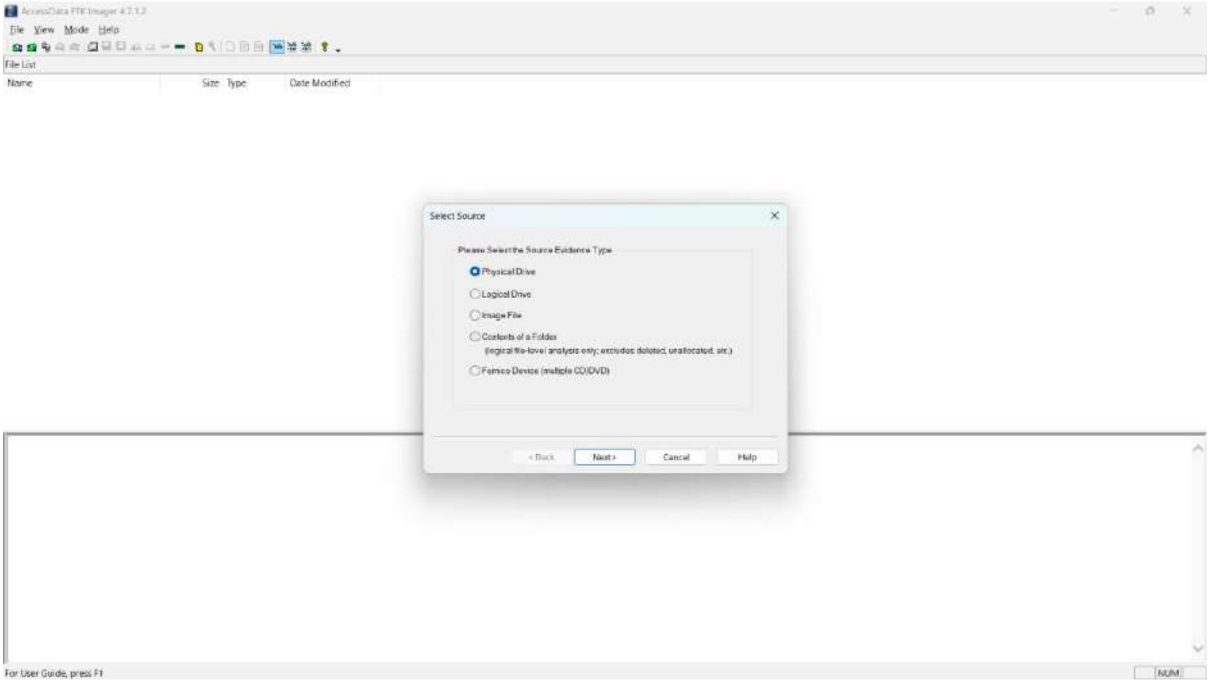
CORROSION SERVICE

FTK imager Application:



Creates a new disk image

Create a disk



Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

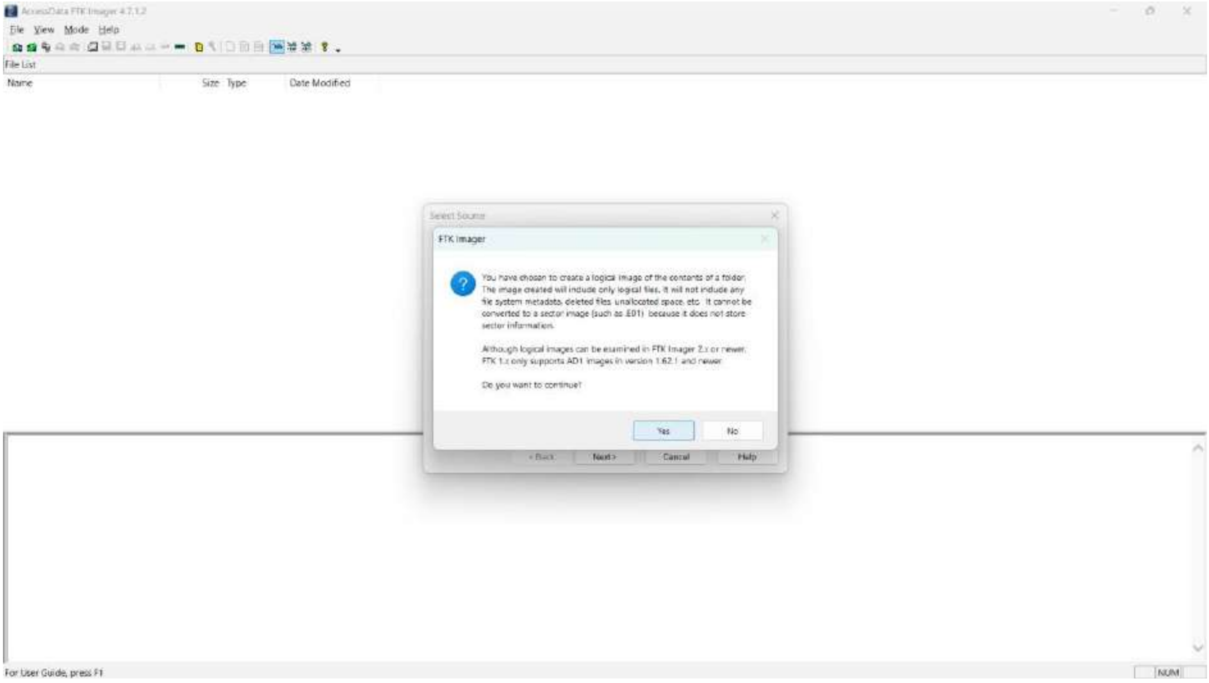
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

For User Guide, press F1

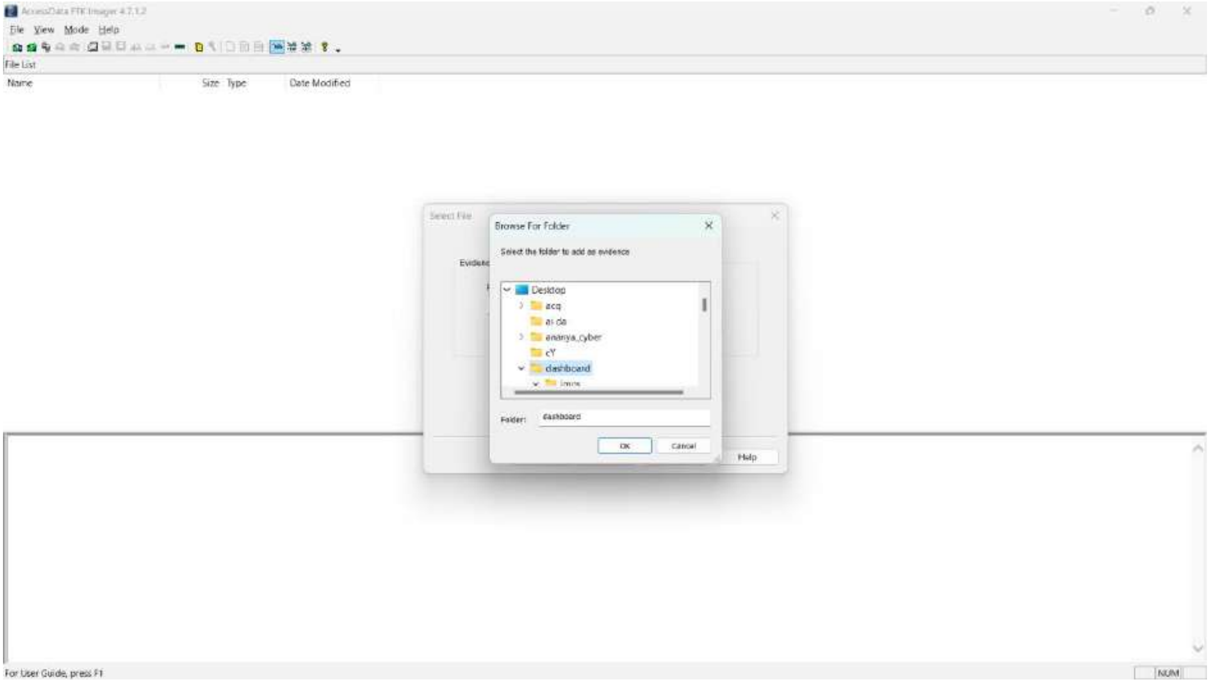
Select a Source evidence



You have chosen to create a logical image of the contents of a folder. The image created will include only logical files. It will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector information.

Although logical images can be examined in FTK Imager 2.x or newer, FTK 1.x only supports AD1 images in version 1.62.1 and newer.

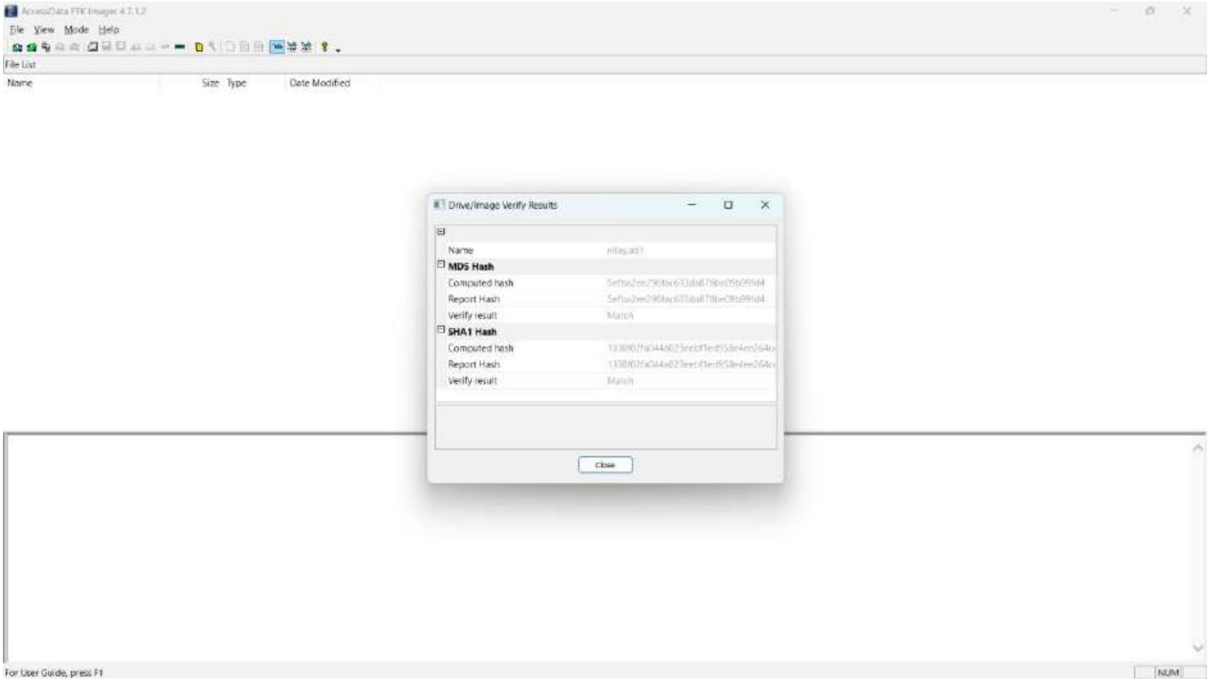
Do you want to continue?



Select the folder to add as evidence

Folder: dashboard

Select a source destination for the application



Drive/Image Verify Results

Name	nilay.ad1
MD5 Hash	
Computed hash	5efba2ee256fac633dab78be09b99fd4
Report Hash	5efba2ee256fac633dab78be09b99fd4
Verify result	Match
SHA1 Hash	
Computed hash	1338f02fa044a023eebf1ed958e4ee264c
Report Hash	1338f02fa044a023eebf1ed958e4ee264c
Verify result	Match

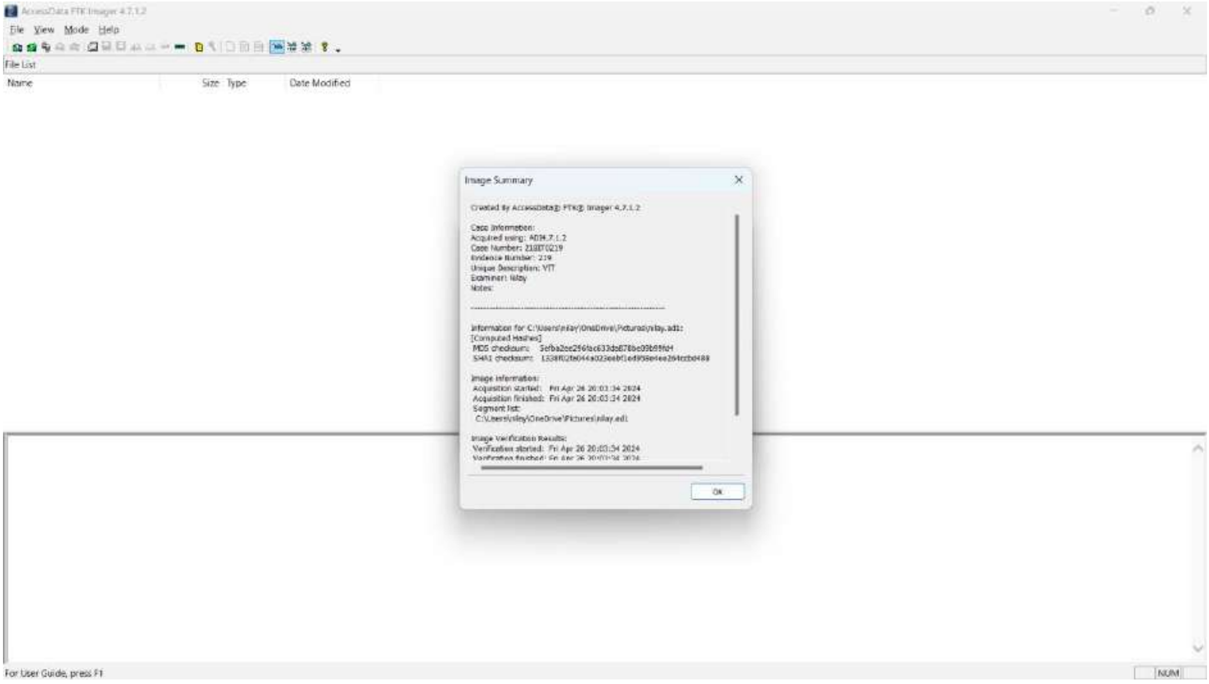


Image Summary

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 21BIT0219
Evidence Number: 219
Unique Description: VIT
Examiner: Nilay
Notes:

--------------------------------------------------------------

Information for C:\Users\nilay\OneDrive\Pictures\nilay.ad1:
[Computed Hashes]
 MD5 checksum:    5efba2ee256fac633dab78be09b99fd4
 SHA1 checksum:   1338f02fa044a023eebf1ed958e4ee264ccbd488

Image Information:
 Acquisition started:   Fri Apr 26 20:03:34 2024
 Acquisition finished:  Fri Apr 26 20:03:34 2024
 Segment list:
  C:\Users\nilay\OneDrive\Pictures\nilay.ad1

Image Verification Results:
 Verification started:  Fri Apr 26 20:03:34 2024
 Verification finished: Fri Apr 26 20:03:34 2024
```

Generated summary of the directory converted

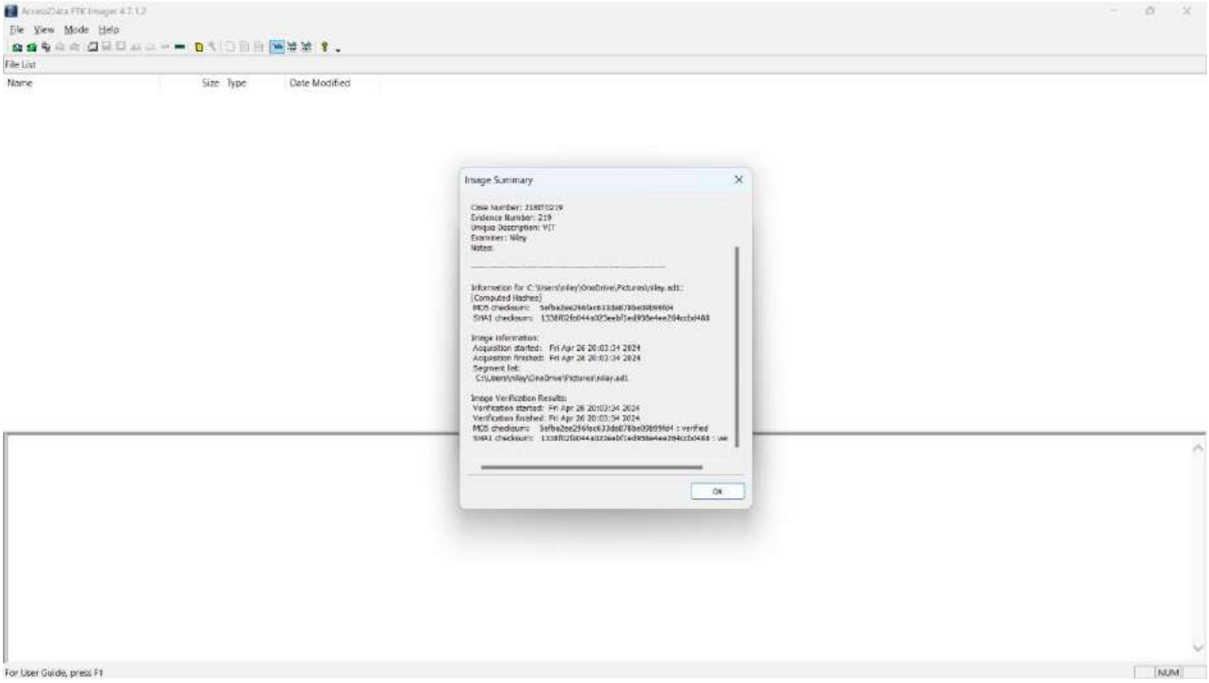


Image Summary

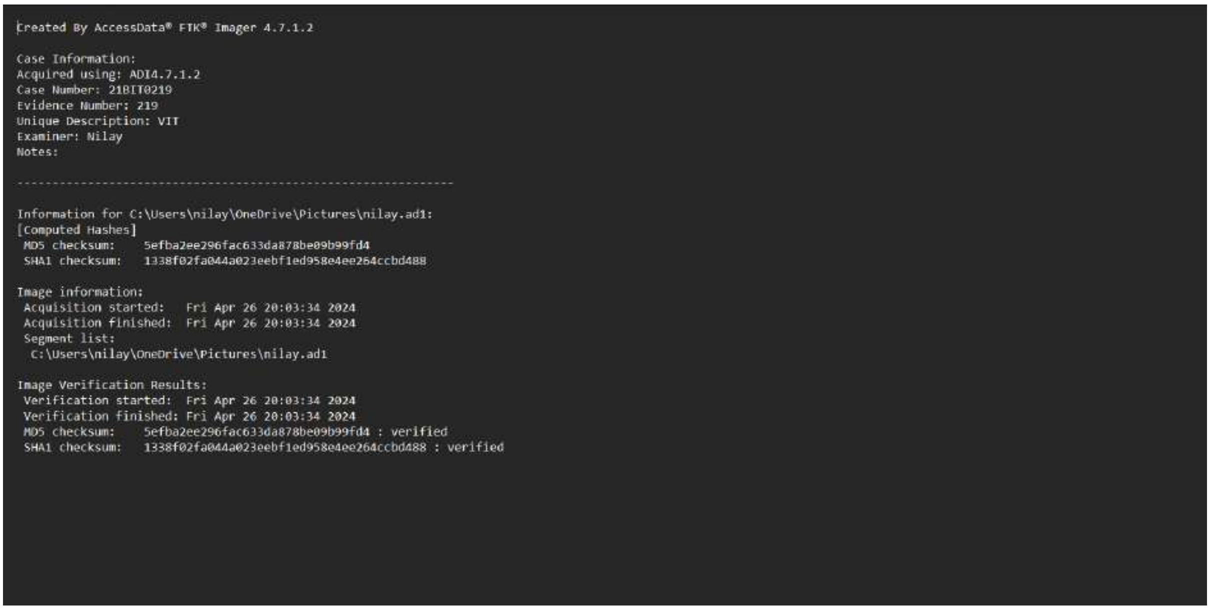
```
Case Number: 21BIT0219
Evidence Number: 219
Unique Description: VIT
Examiner: Nilay
Notes:

------------------------------------------------------------

Information for C:\Users\nilay\OneDrive\Pictures\nilay.ad1:
[Computed Hashes]
 MD5 checksum:    5efba2ee296fac633da878be09b99fd4
 SHA1 checksum:   1338f02fa044a023eebf1ed958e4ee264ccbd488

Image information:
 Acquisition started:   Fri Apr 26 20:03:34 2024
 Acquisition finished:  Fri Apr 26 20:03:34 2024
 Segment list:
  C:\Users\nilay\OneDrive\Pictures\nilay.ad1

Image Verification Results:
 Verification started:  Fri Apr 26 20:03:34 2024
 Verification finished: Fri Apr 26 20:03:34 2024
 MD5 checksum:    5efba2ee296fac633da878be09b99fd4 : verified
 SHA1 checksum:   1338f02fa044a023eebf1ed958e4ee264ccbd488 : ve
```



```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 21BIT0219
Evidence Number: 219
Unique Description: VIT
Examiner: Nilay
Notes:

--------------------------------------------------------------

Information for C:\Users\nilay\OneDrive\Pictures\nilay.ad1:
[Computed Hashes]
 MD5 checksum:    5efba2ee296fac633da878be09b99fd4
 SHA1 checksum:   1338f02fa044a023eebf1ed958e4ee264ccbd488

Image information:
 Acquisition started:   Fri Apr 26 20:03:34 2024
 Acquisition finished:  Fri Apr 26 20:03:34 2024
 Segment list:
  C:\Users\nilay\OneDrive\Pictures\nilay.ad1

Image Verification Results:
 Verification started:  Fri Apr 26 20:03:34 2024
 Verification finished: Fri Apr 26 20:03:34 2024
 MD5 checksum:    5efba2ee296fac633da878be09b99fd4 : verified
 SHA1 checksum:   1338f02fa044a023eebf1ed958e4ee264ccbd488 : verified
```

This is the required file.