CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC), THIRUVANANTHAPURAM, KERALA

A MINOR PROJECT REPORT ON

"Digital Forensics and Data Recovery"

SUBMITTED TOWARDS THE

PG-DCSF September 2023

BY

Group Number - 07

Patil Lokesh Dinkar	**PRN: 230960940034**
Patil Sarvesh Dinkar	**PRN: 230960940036**
Pendhe Shrawan Anil	**PRN: 230960940038**
Shubham Patel	**PRN: 230960940049**
Waghole Nikita Vitthal	**PRN: 230960940059**

Under The Guidance Of

Mr. Hiron Bose **Mr. Jayaram P.**

Table of Contents

Table of Figures i

Abstract ii

1. Introduction 1

1.1. Data Analysis 1

1.2. Data Recovery 1

1.3. System requirements 1

1.3.1. Hardware.....1

1.3.2. Software.....1

1.4. Features..... 2

2. Cyber Forensics Procedure 3

2.1. Steps for imaging..... 3

2.2. Seizure & Acquisition Report generated by TrueBack win Version 2.1 for evidence drive 8

2.3. Steps for analyzing and processing bitstream image(.P01) 9

2.3.1. Steps to open a P01 file in cybercheck suite file 9

2.3.2. Steps for verifying hash value of the file 11

2.3.3. Analyzing deleted data 12

2.3.4. Finding Steganographed data 13

2.3.5. Finding File mismatch data (i.e unsupported files due to different file extensions) 14

3. Generated Report by Cybercheck Suite tool 15

Table of Figures

Figure 1 Checking space in USB 3
Figure 2 Cyber Check 6.0 - Evaluation version 3
Figure 3 TrueBack win version 2.1..... 4
Figure 4 TrueBack win Seize & acquire 4
Figure 5 selecting destination path for image file 5
Figure 6 Selecting Image type and Hash type 5
Figure 7 seizuring and acqusition case data summary..... 6
Figure 8 Progress bar of seizure and acqustion 6
Figure 9 Information to be labeled.....7
Figure 10 Report generation 7
Figure 11 Partitions 9
Figure 12 Path allocation 9
Figure 13 Selecting partition 10
Figure 14 List of all files and folders 10
Figure 15 Verifying hash value 11
Figure 16 Successful verification of hash value 11
Figure 17 Analysing deleted video 12
Figure 18 Analysing deleted photo 12
Figure 19 Check Steganographed file option 13
Figure 20 showing steganographed file 13
Figure 21 Check file signature option 14
Figure 22 Showing Signature mismatch files 14

Abstract

This project aims to identify the evidence device, secure and acquire data from a USB drive, analyze and recover the data, note observations, and generate a report of the investigation. The report will include details of authentication, analysis, presentation, and preservation of the evidence.

The summary outlines the different elements of cyber forensics, including data collection, analysis, interpretation, and reporting. It emphasizes the importance of preserving the integrity and authenticity of digital evidence, dealing with legal challenges, and following ethical principles. By using digital traces, network logs, system artifacts, and volatile memory, cyber forensics professionals create a clear story that helps in both reactive response and proactive threat prevention.

However, the summary also discusses the obstacles that cyber forensics professionals face. The fast pace of technological change, encryption, tools for anonymity, and jurisdictional boundaries present significant challenges in collecting and interpreting evidence. The summary suggests possible solutions such as improvements in data recovery methods, frameworks for international cooperation, and ongoing professional development to keep up with new threats.

In conclusion, cyber forensics is a vital and ever-changing field in the contemporary digital world. Its role in maintaining the integrity of digital ecosystems, ensuring accountability, and facilitating justice is undeniable. As cyber threats become more complex and widespread, cyber forensics serves as a source of strength, allowing investigators to reveal the hidden aspects of digital wrongdoing and protect the digital realm.

1. Introduction

Cyber forensics is a crucial field within digital investigation that helps solve complex cybercrimes and digital wrongdoings. With the growing dependence on digital technologies, it has become essential to have effective ways to find, gather, protect, and examine digital evidence. This summary explores the world of cyber forensics and explains its importance in both proactive and reactive approaches to cybersecurity.

Cyber forensics involves a methodical process of finding, preserving, and presenting digital evidence for use in legal cases, incident response, and threat intelligence. This interdisciplinary field combines principles from computer science, law, and investigation techniques to unravel the complex web of cyber incidents. Cyber forensics experts use advanced tools and methods based on strict methodologies to trace the sources of cyberattacks and attribute them.

1.1. Data Analysis

CyberCheck can analyze TrueBack Images, EnCase Images, Raw disk images, Virtual disk images, and RAM dumps. The tool can generate a detailed report on the analysis findings, which is very handy for the investigating officers to submit before the court of law. The tool can extract unallocated and disk slack areas, perform data carving on slack areas, and provides options to do analysis based on file hashes and the file's signature.

1.2. Data Recovery

CyberCheck can recover deleted files/folders, deleted partitions, and formatted data on a partition. All of this information can be added to the report to record the findings.

1.3. System requirements

1.3.1. Hardware Requirements

High-performance CPU: Multi-core processors with sufficient processing power for data analysis and decryption.

Ample RAM: A minimum of 8 GB RAM is recommended for efficient processing of large datasets and memory analysis.

Storage Space: Sufficient storage to accommodate acquired evidence and analysis results. Solid-state drives (SSDs) are preferable for faster data access (minimum 512Gb).

Graphics Processing Unit (GPU): A powerful GPU can accelerate certain data processing tasks, such as password cracking or cryptographic operations.

Operating System : minimum windows 7 and above and linux Os

1.3.2. Software Requirements

Cybercheck suite

CyberCheck Suite is a comprehensive collection of disk forensics tools to perform the acquisition of digital evidence, analysis, data recovery, and reporting of digital evidence.

TrueBack - Disk Imaging Tool

Performs Seize, Acquire or both Seize and Acquire in compliance with NIST standards. TrueBack is available for both Windows and Linux Operating Systems. The tool creates a report on the Seize and Acquire process, which contain details of the entire process like hash values, exhibit details, and system details.

1.4 Features

MD5,SHA1,SHA2 hash algorithms

Block hash

Lossless compression of acquired image file

Generates detailed reports on suspect device seizure and acquisition

Bootable solution in Linux on USB & CD with Disk Preview

2. Cyber Forensics Procedure

2.1 Steps for imaging

1. To insert and modify information on a USB drive for forensic analysis. This involves adding data to the drive and making changes to it as needed. The purpose of this is to use the drive in a forensic investigation, where the data on the drive can provide valuable evidence. This process must be done carefully and accurately to ensure the integrity of the data and its usefulness in an investigation.

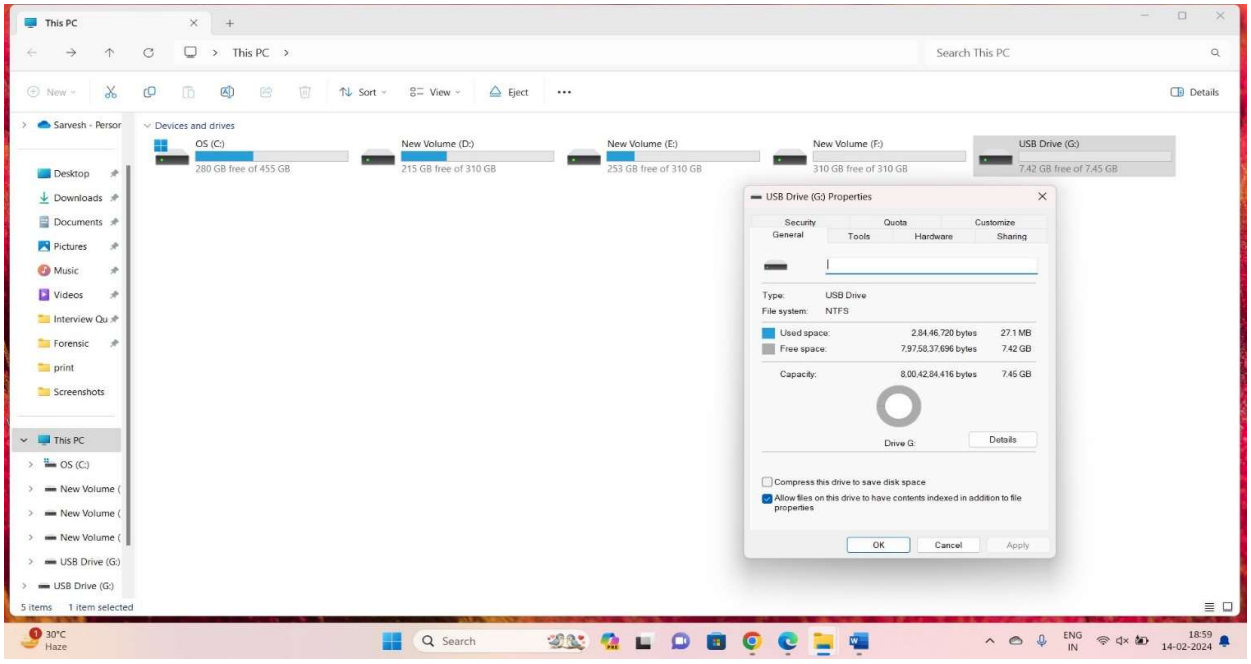
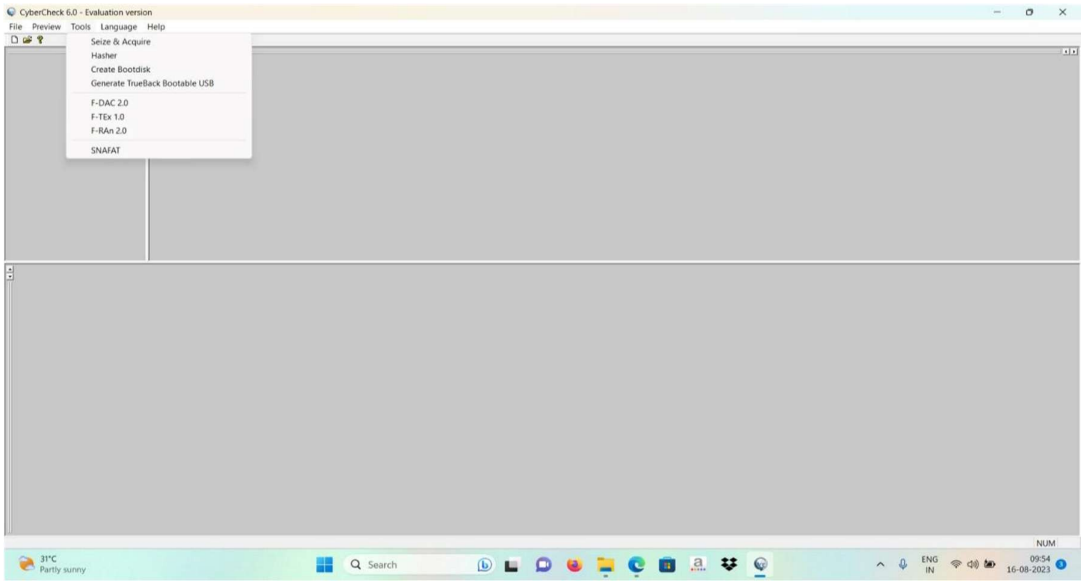


Figure 1 Checking space in USB

2. For imaging USB drive Open the Cyber check suite and go to "**tools"** and select the "seize and Acquire option .



3.In a new window "**TrueBack win version 2.1"** imager will be opened then select the "**Seize and Acquire**" option for acquiring and seizing the particular evidence drive.

Figure 3 TrueBack win version 2.1

2. Enter the requested data by TrueBack win version2.1 such as investigators name, rank, police station, crime number, place of seizure, name of suspect and witnesses, notes, lab reference numbers, and evidence file name, for seizure and acquisition process to be carried out

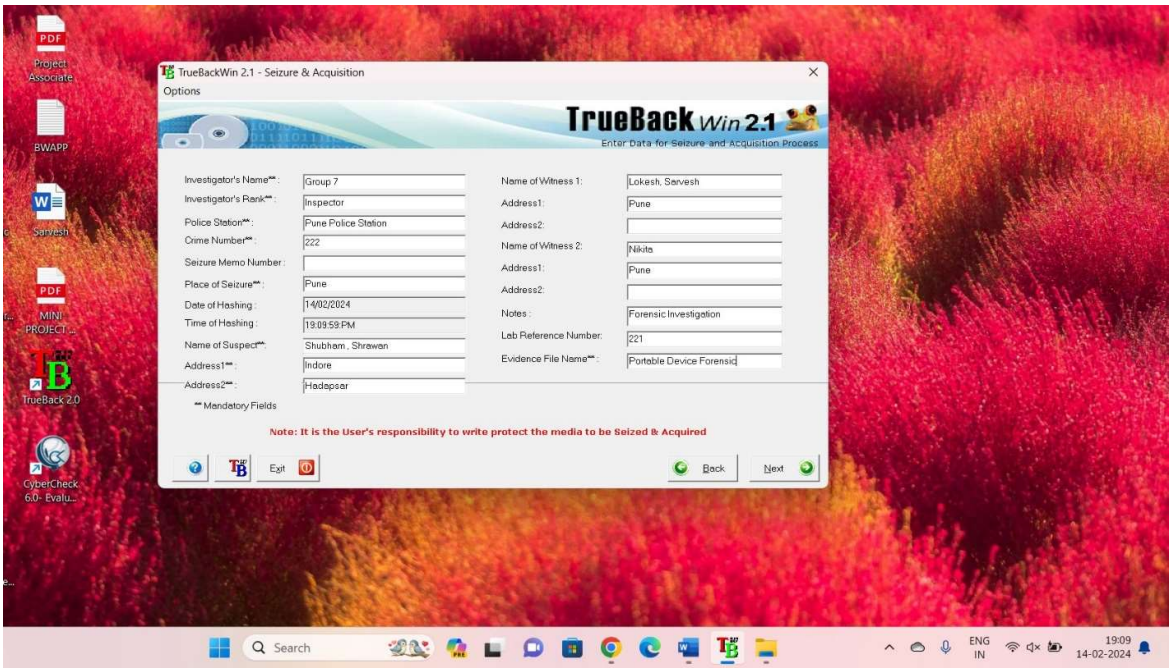


Figure 4 TrueBack win Seize & acquire

3. Choose the location or directory where you would like to store the Trueback Win file that you have obtained for analysis. This is where the file will be saved and can be accessed for further examination.

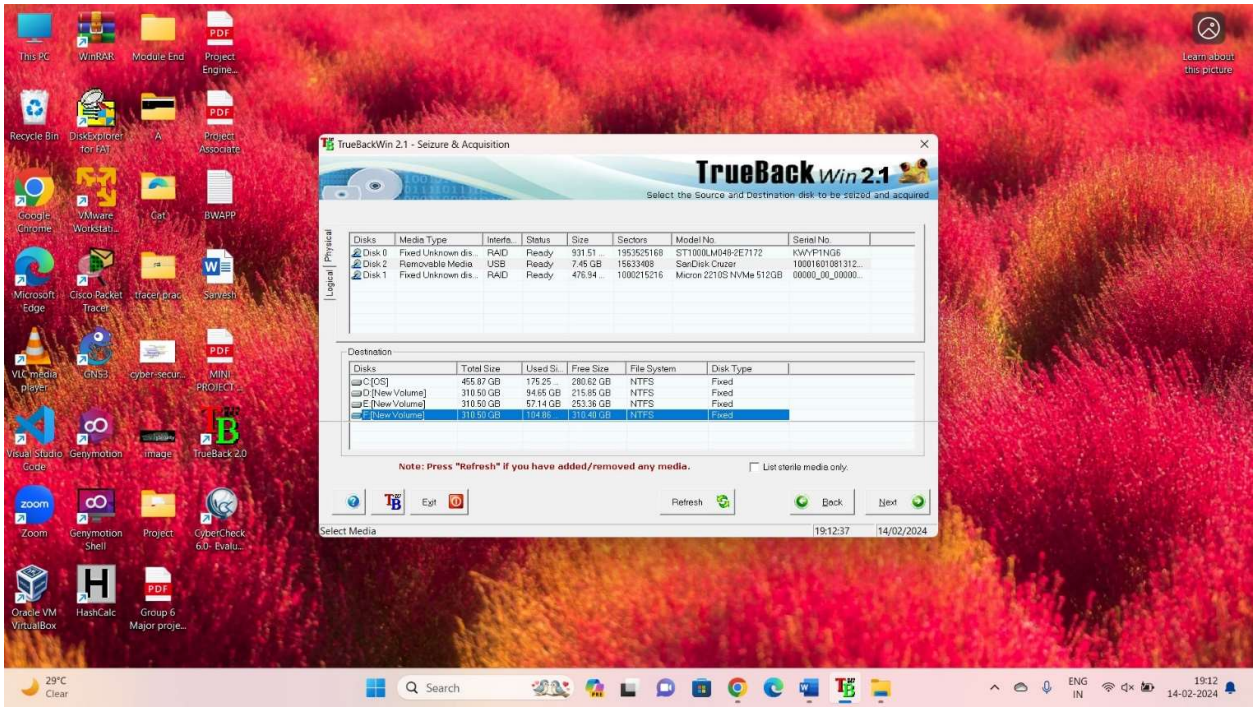


Figure 5 selecting destination path for image file

4. Choose the desired image format, hash algorithm, and block hash/block size settings. These options allow you to customize the way the data is processed and analyzed and can be adjusted to meet your specific needs.

Figure 6 Selecting Image type and Hash type

5. Verify the information presented in the Seizure & Acquisition Case Data Summary window. Once you have confirmed that the details are correct, select the “Confirmed as correct” radio button and click the “Next” button to proceed.

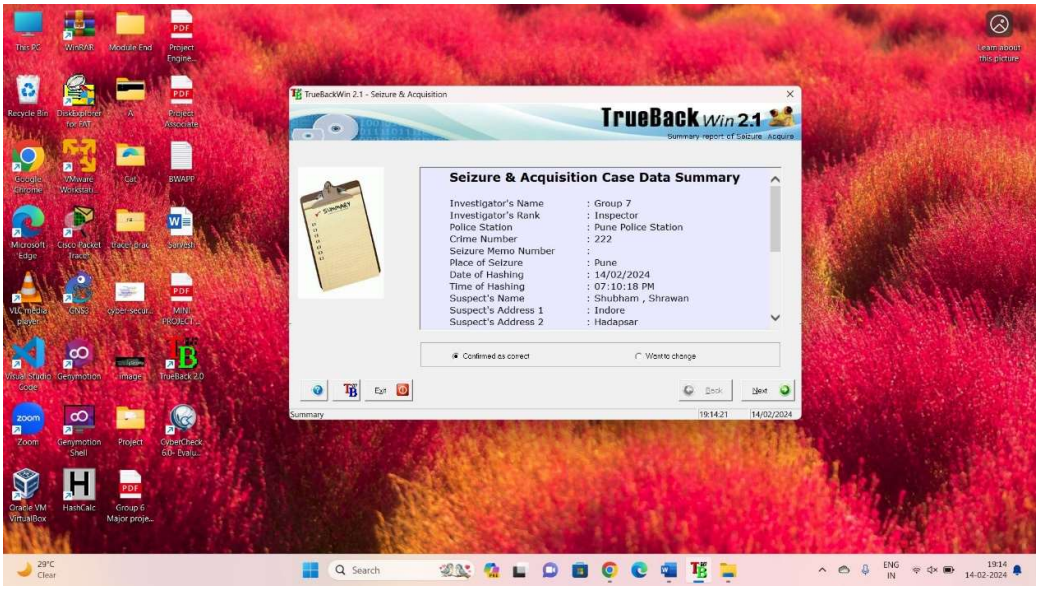


Figure 7 seizuring and acqusition case data summary

6. The progress bar for the seizure and acquisition process will start to show the logs of the ongoing process and provide an estimate of the time remaining until completion.

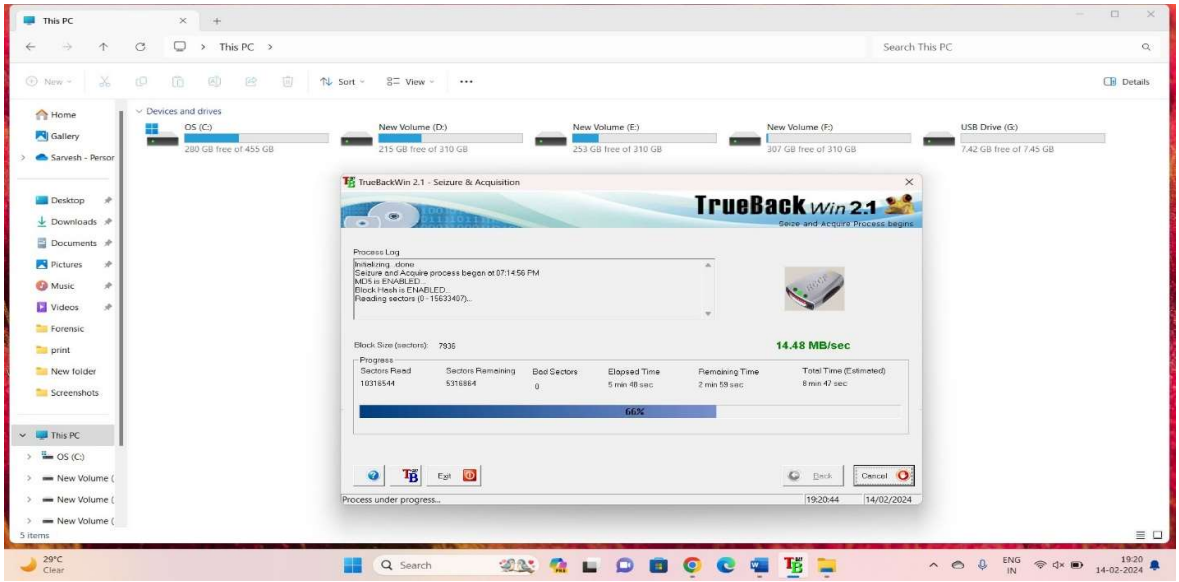


Figure 8 Progress bar of seizure and acqustion

Mark the evidence drive with the provided information, including the Exhibit number, ID number, Crime number, Seizure memo number, and Hash value. This should be done physically, by writing or printing the information onto a label and affixing it to the drive. This ensures that the drive can be easily identified and tracked throughout the investigation process.

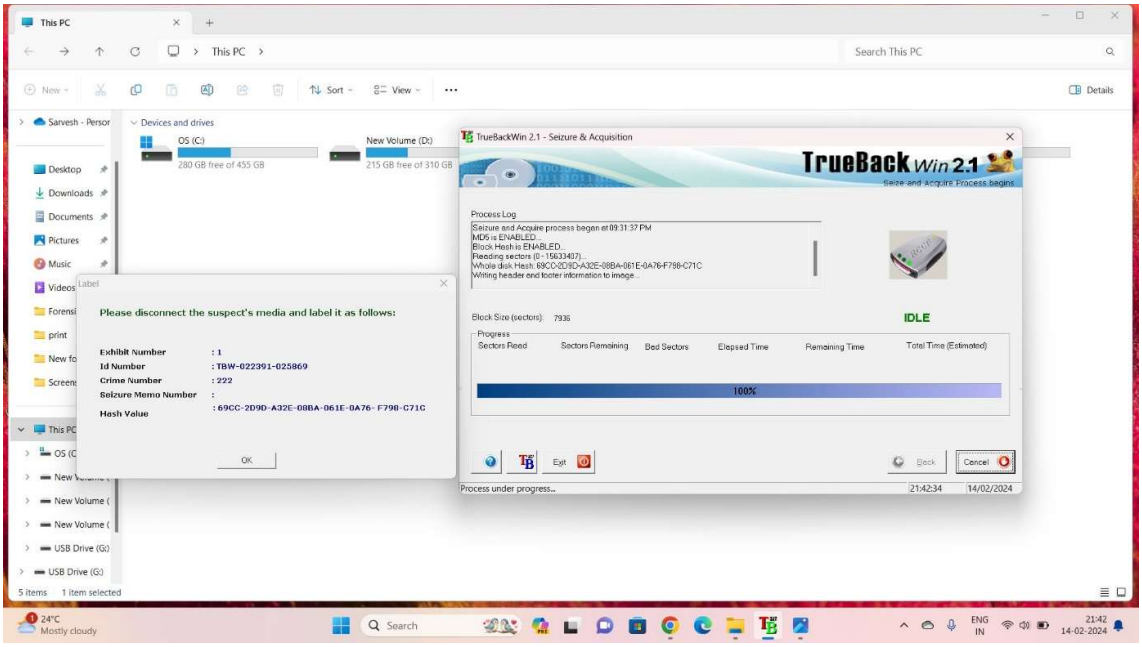


Figure 9 Information to be labeled

7. After imaging the device using the TrueBack Win version 2.1 tool, a seizure and acquisition report will be generated. This report should be printed out for documentation and reference purposes.

2.2 Seizure & Acquisition Report generated by TrueBack win Version 2.1 for evidence drive

Seizure & Acquisition Report

Report generated by TrueBackWin version 2.1 developed by CDAC, Thiruvananthapuram

Investigator's Name	: Group 7
Investigator's Rank	: Inspector
Police Station	: Pune Police Station
Crime Number	: 222
Seizure Memo Number	:
Lab Ref Number	: 221
Place of Seizure	: Pune
Date of Hashing	: 14/02/2024
Time of Hashing	: 09:28:42 PM
Suspect's Name	: Shubham , Shrawan
Suspect's Address1	: Indore
Suspect's Address2	: Hadapsar
Name of Witness1	: Lokesh , Sarvesh
Address1 of Witness1	: Pune
Address2 of Witness1	:
Name of Witness2	: Nikita
Address1 of Witness2	: Pune
Address2 of Witness2	:
Evidence File Name	: Portable Device forensic
Start Time	: 09:31:37 PM
End Time	: 09:44:25 PM

Processor Details

Processor Name	: 11th Gen Intel(R) Core(TM) i5-1135G7 92r¸ =ÌÙob92r`
Speed	: 2.428Ghz

Exhibit Details

Exhibit Number	: 1
Disk Type	: USB STORAGE
Model Number	: SanDisk Cruzer
Serial Number	: 10001601081312125 0DF
Image Format	: TrueBackWin Image
Hash Type	: MD5
Total Sectors	: 15633408
Bytes per Sector	: 512
Block Size	: 7936 sectors
Number of Blocks	: 1970

Hash Values

Hash Value of Whole Media	: 69CC-2D9D-A32E-08BA-061E-0A76-F79B-C71C
Hash Value of Block Hashes	: F385-6F51-D114-774B-8ABB-9A52-6EA6-1FFE
Hash Value of Report Data	: FFDE-9F3A-DBBF-A2BB-2DF9-77C0-D624-45FB

2.3 Steps for analyzing and processing bitstream image(.P01)

2.3.1 Steps to open a P01 file in cybercheck suite file

1. To begin using the Cyber Check tool, first open the program and navigate to the “File” menu. From there, click on the “New” option and enter the required information, such as the investigator’s name and password, the lab reference number, and the name of the evidence file. This will allow you to create a new case and begin working with the tool.

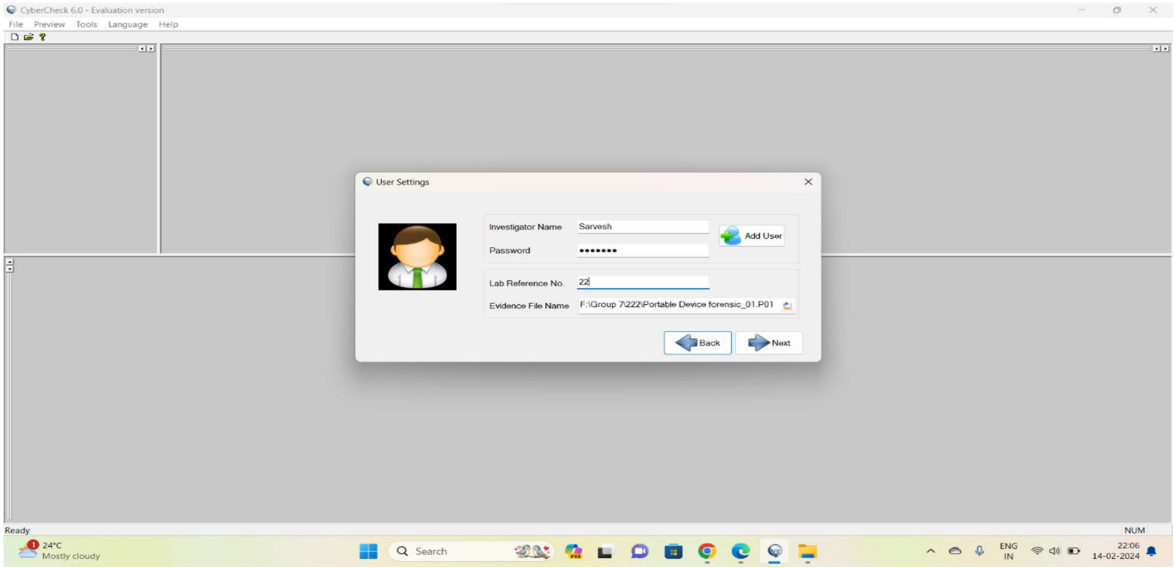


Figure 11 Partitions

2. Specify the location for the report folder by providing the path to the desired directory. Once the path has been entered, review the available options and select those that are most suitable for your needs. This will ensure that the report is saved in the correct location and that the appropriate settings are applied

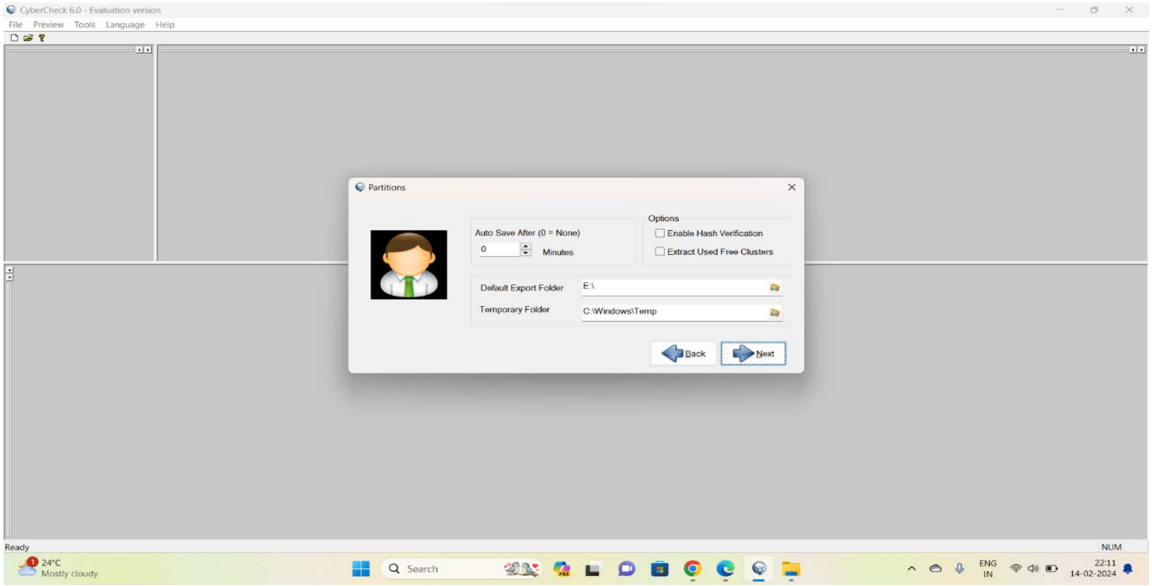


Figure 12 Path allocation

3. Choose the partitions that you would like to include in the analysis and report generation process.

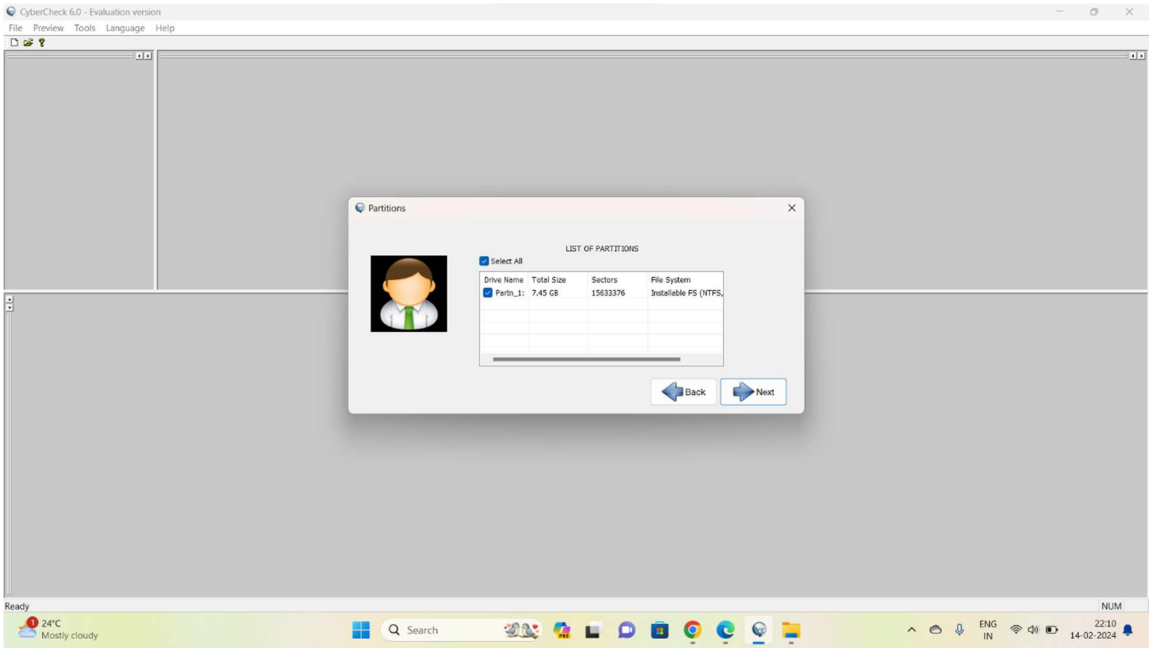


Figure 13 Selecting partition

4. A list of all files and folders, along with their respective details, will be displayed. This includes information about all present, deleted, and overwritten files and folders. This allows you to see a comprehensive overview of the data and its current state.

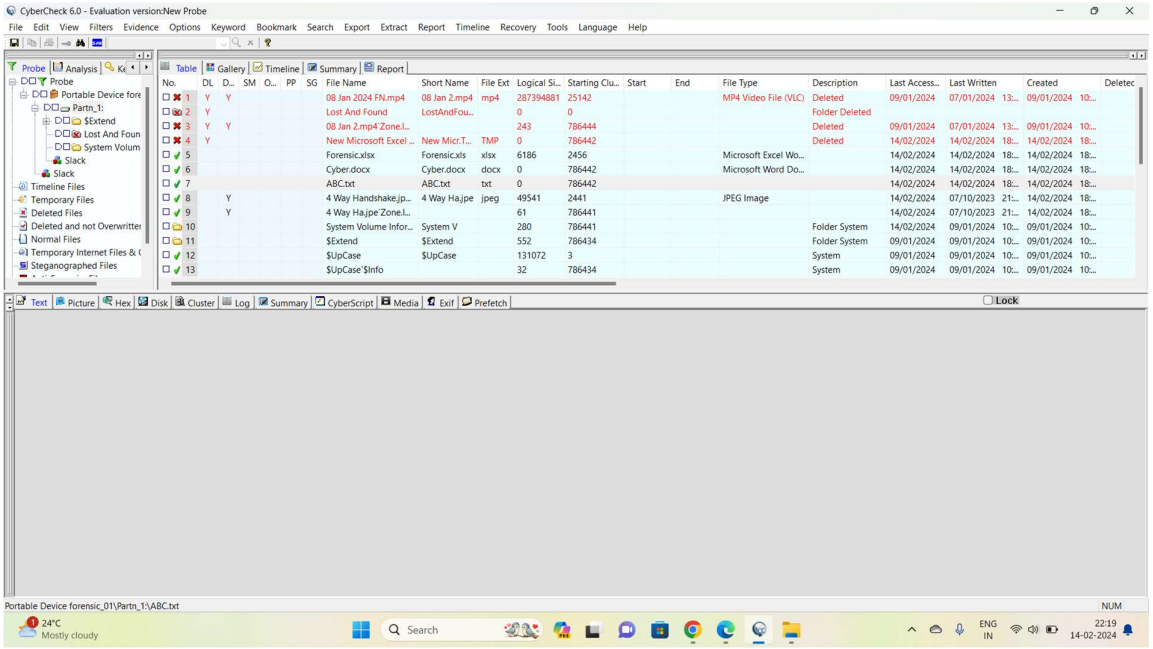


Figure 14 List of all files and folders

2.3.2 Steps for verifying hash value of the file

1. To verify the authenticity of the evidence image file, the first step is to check its hash value. This can be done by going to the “Options” menu and selecting the “Verify Image Hash” option. This will allow you to compare the hash value of the image file with the expected value to ensure that it has not been altered or tampered with.

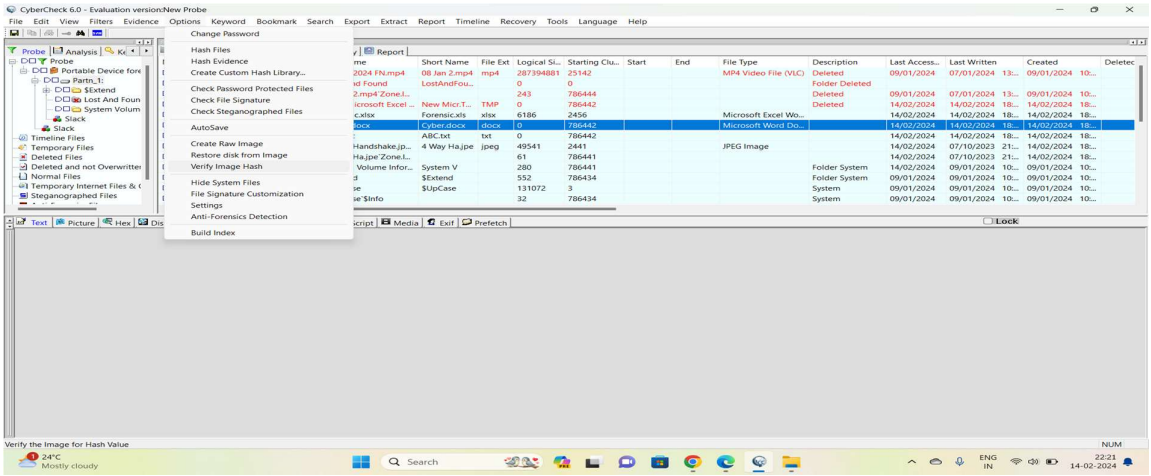


Figure 15 Verifying hash value

2. Once the hash value of the evidence image file has been verified, the results will be displayed in a dialogue box. This box will show the details of the blocks that were verified, including information about their status and any relevant data. These details will also be included in the final report, providing a record of the verification process and its outcome.

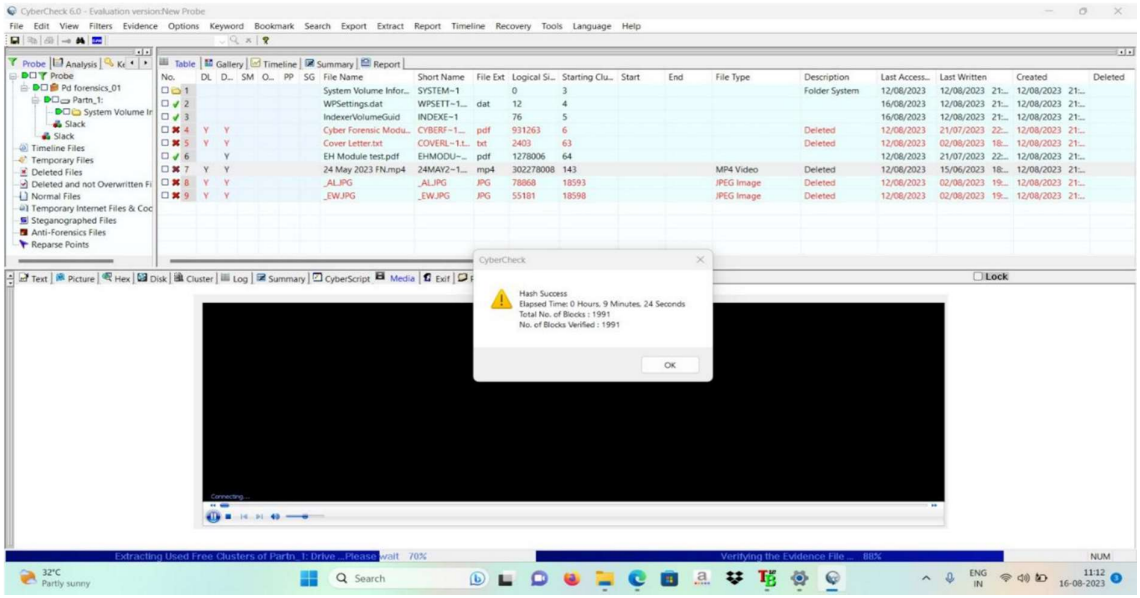


Figure 16 Successful verification of hash value

2.3.3 Analyzing deleted data

1. Analyzing and recovering the deleted PDF file data.

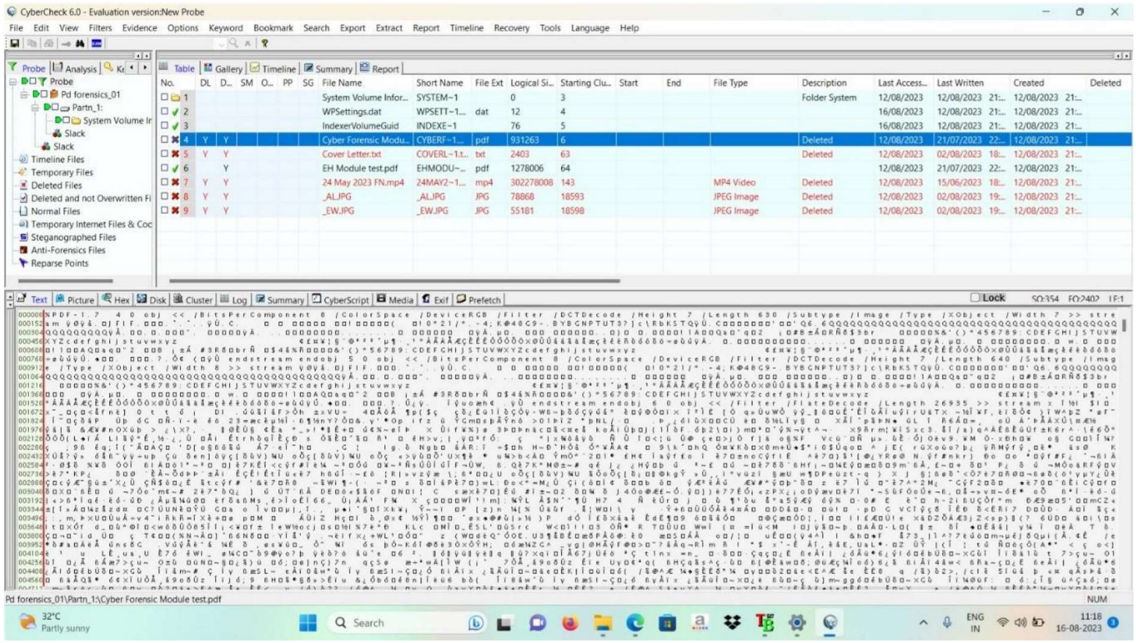


Figure 17 Analysing delete

2. Analyzing and recovering deleted video file.

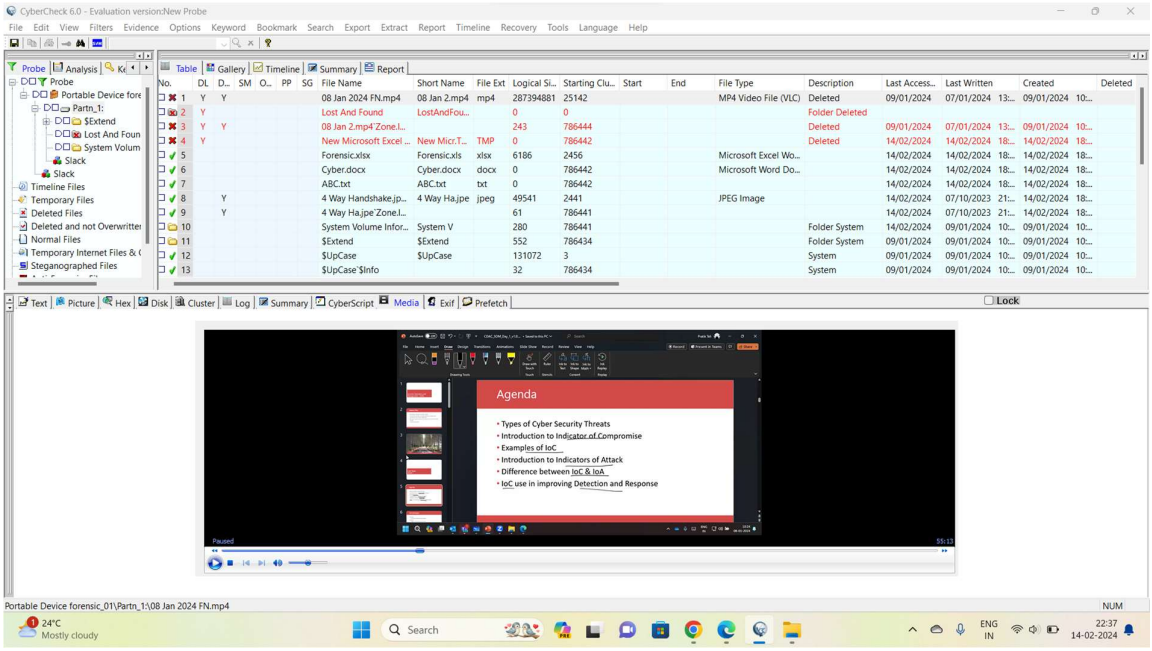


Figure 18 Analysing deleted video

2.3.4 Finding Steganographed data

1. Go to options then select the “check steganography files” option

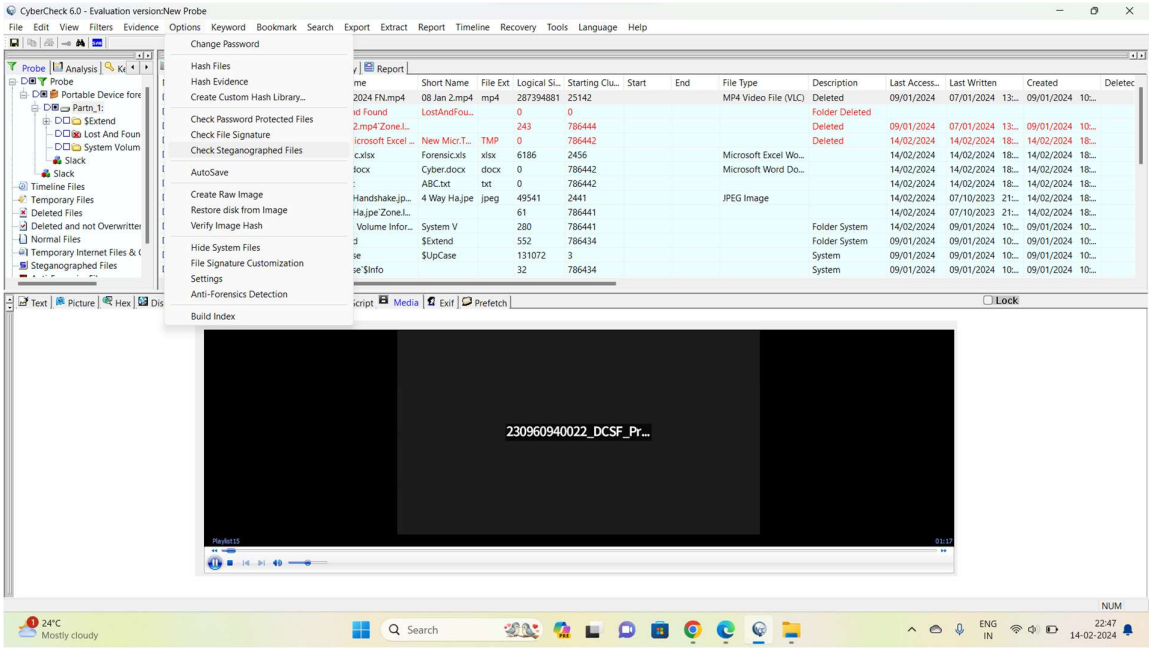
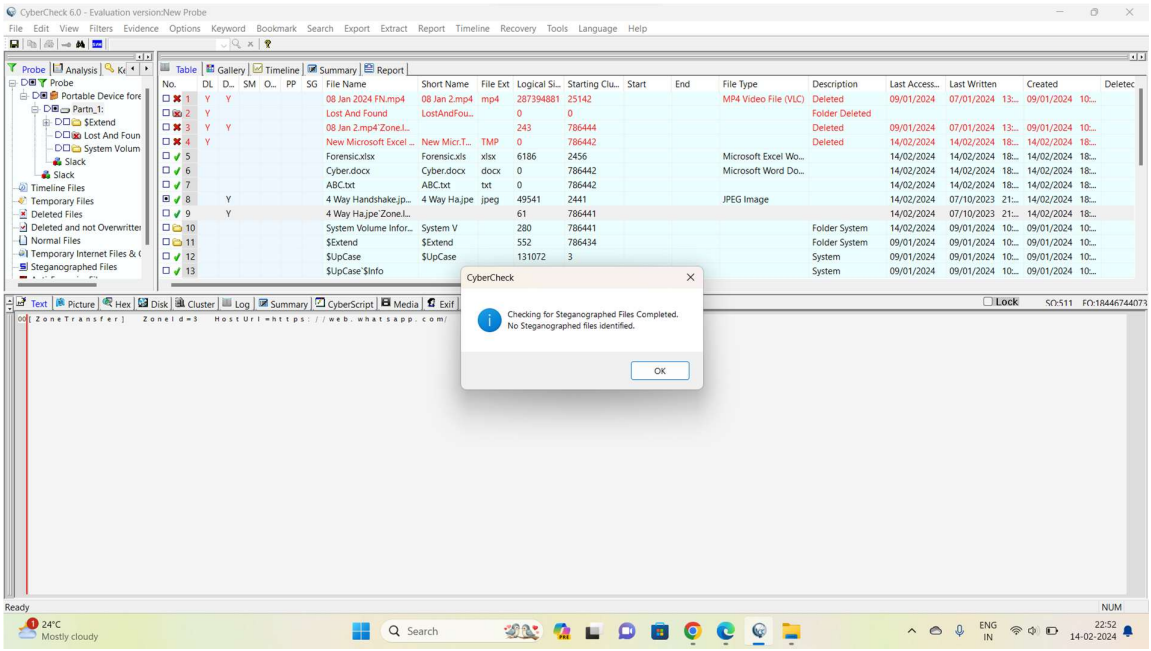


Figure 19 Check Steganographed file option

2. A scan will be carried out after selecting the “check steganography files” option. After the completion of the scan for steganographed files the column with name SG will indicate with a “Y” symbol in the table if the file is steganograpghed.



2.3.5 Finding File mismatch data (i.e unsupported files due to different file extensions)

1. Go to options then select the “check file signature” option

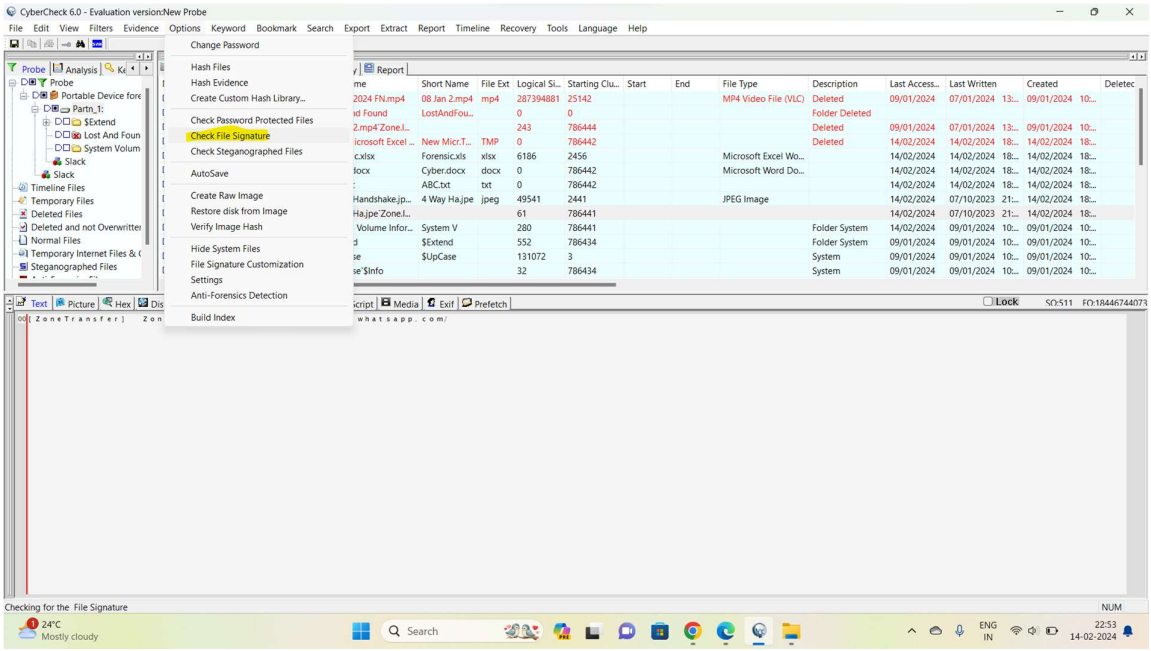


Figure 21 Check file signature option

2. A scan will be carried out after selecting the “check file signature” option. After the completion of the scan for file signature the column with name SM will indicate with a “Y” symbol in the table.

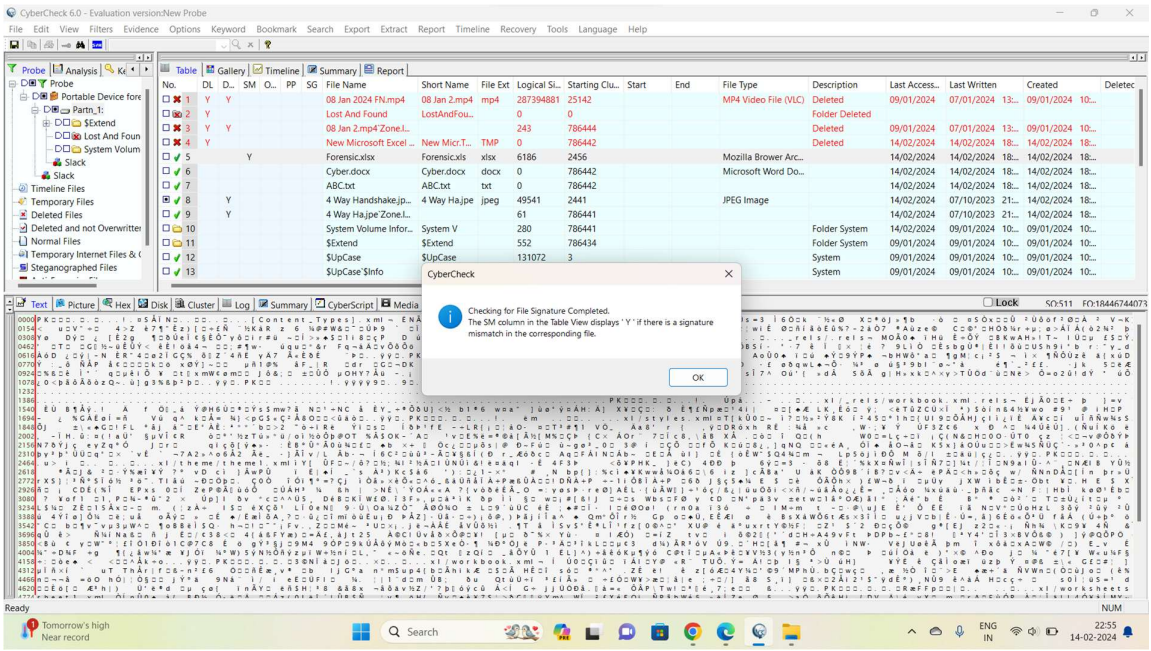


Figure 22 Showing Signature mismatch files

CyberCheck Report

Probe : NewProbe

Evidence Name : Portable Device forensic_01.P01

File **F:\Group 7\222\Portable Device forensic_01.P01** was acquired by **Group 7,Inspector** at **14/2/2024 21:28:42**

Evidence acquired using **TrueBackWin** version **2.0**

During acquisition the suspect's media was **Write Protected**

Crime Number	:	222
Lab Reference Number	:	221
Police Station	:	Pune Police Station
Acquisition Notes	:	Forensic Investigation
Media Type	:	USB Storage Device

Drive Geometry :

Total Capacity	7.45 GB
Total Sectors	15633408
Bytes per Sector	512
Cylinders	62260
Heads	1
Sectors per Track	63

File Integrity :

Acquisition Hash (MD5)	:	69CC-2D9D-A32E-08BA-061E-0A76-F798-C71C
Hash Verification Status	:	Verified and mismatch encountered.

Block Hash Details :

Total Number of Blocks	:	1970
Number of Mismatched Blocks	:	1

Mismatched Block Details :

Block Number	Block Size	Block Hash		
		Seize	Source	Image
834	7936	Match	Match	Mismatch

Partition Details :

Volume Partn_1: Parameters			

Volume Label		Volume Serial	1E30-AF31
File System	Installable FS (NTFS, HPFS,exFAT,Ad.Unix)	Partition Type	07
Total Capacity	7.45 GB	Total Sectors	15633375
Number of Folders	7	Number of Files	34
Sectors per Track	63	Cluster Size	4096
Sectors per Cluster	8	Free Clusters	1948250
Heads	255	Starting MFT Cluster	0

Logged in by Sarvesh with Lab Reference Number 222 on Wednesday, February 14, 2024 at 10:09:55 PM