

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

**A PROJECT REPORT ON**

**“Digital Evidence Collection Using The Trueback  
Application”**

**SUBMITTED TOWARDS THE**



**PG-DCSF September 2023**

**BY**

**Group Number – 04**

**Amit Kotwal**

**Pranay Anil Karanjakar**

**Satnam Singh**

**Lalit Yeshwant Maske**

**Shubham Manohar Patil**

**PRN: 230960940004**

**PRN: 230960940022**

**PRN: 230960940023**

**PRN: 230960940026**

**PRN: 230960940037**

**Under The Guidance Of**

**Mr. Jayaram Peggam  
( Centre Co- Ordinator)**

**Dr. Hiron Bose  
(Project Guide)**

# **TABLE OF CONTENTS**

<b>Topic</b>	<b>Page No</b>
<u>Abstract.....</u>	<u>03</u>
<u>Certificate .....</u>	<u>04</u>
<u>Introduction.....</u>	<u>05</u>
<u>Feature of Trueback .....</u>	<u>06</u>
<u>Starting TruebackWin .....</u>	<u>06</u>
<u>Seize and Acquire Mode Operation.....</u>	<u>07</u>
<u>Conclusion .....</u>	<u>13</u>

## **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.

## **Objective**

The objective of this project is to conduct digital evidence collection at a crime scene utilizing the Trueback application. 'Trueback' is a digital forensic tool designed to facilitate the collection, preservation, and analysis of digital evidence from various sources, including computers, mobile devices, and storage media.



# ***CERTIFICATE***

THIS IS CERTIFY THAT,

Amit Kotwal

PRN: 230960940004

Pranay Anil Karanjakar

PRN: 230960940022

Satnam Singh

PRN: 230960940023

Lalit Yeshwant Maske

PRN: 230960940026

Shubham Manohar Patil

PRN: 230960940037

Have Satisfactory completed the project work Entitled, “**Digital Evidence Collection Using the Trueback Application**” to Centre for Advanced Computing in the partial fulfilment of the requirement of Post-Graduate Diploma (PG-Diploma), is a record of project work carried out by them under my guidance and supervision. The matter presented in this project report has not been submitted either in part or full to any University or Institute for award of any degree.

**Mr. Jayram Peggam**  
(Centre Co-ordinator)

**Dr.Hiron Bose**  
(Project Guide)

## **Introduction**

Cyber Forensics deals with the preservation, identification, extraction, and documentation of computer related evidences utilizing secure, controlled methodologies. Cyber Forensics involves the detailed examination of a computer hard drive-in order to discover evidence of wrongdoing. An exact copy of the drive is made and all examinations are done on the copy.

This ensures that any evidence that is found is preserved on the original so that it can be later used in a court of law. Deleted files, deleted e-mail, old instant messages, hidden files, and a history of Internet activity are all items that can be recovered this way.

Because of the way the hard drive file system works, there is no guarantee that any of these items will be recovered. It is possible to collect sufficient evidence from a suspect's computer if the computer is seized immediately after the execution of the crime.

In solving computer crime cases, computer forensics is used to gather evidence, which will be analyzed and presented to a court of law to prove the illegal activity. It is important that when doing computer forensics no alteration, virus introduction, damages or data corruption should occur to the original source of evidence. To do a good analysis, the first step is to do secure collection of computer evidence. Secure collection of evidence is important to guarantee the evidential integrity and security of information. The best approach for this matter is to use disk-imaging tools. Choosing and using the right tool is very important in computer forensics investigation. TrueBackWin is a cyber-forensics tool, developed by Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram.

This tool enables the user to create a Bit Stream duplicate of a storage media (IDE/SCSI hard disks, Floppy Disks, CD, USB drives) to another media as an image. Windows version of True Back cannot write protect the source media. Therefore, it is the user's responsibility to adequately write protecting the source storage media of which image will be taken by the software.

TrueBackWin ensures the data integrity of the image by comparing the hash values of both source and image media using MD5, SHA1 or SHA256 hashing algorithms. TrueBackWin provides three modes of operation, Viz., Seize, Acquire, and Seize & Acquire. In the Seize mode, only a hash value of the hard disk of the suspect's computer system is taken. These speeds up the seizure process of the

suspect's machine and also an easy process that an Investigating Officer can follow.

In the Acquire mode, user can specify the source media, destination media and case details. TrueBackWin creates an image of the source media into the destination media by reading the source contents sector by sector and writing it on to the destination. Meanwhile, a hash computation using MD5 hash algorithm will be performed on the data read. All these information can be saved into a report file for legal use. A computer expert in an analysis laboratory could perform the Acquire process with the details collected at the time of Seize process.

## **Features of TrueBackWin**

Standard Windows based application.

- Extraction of system information.
- Three modes of operation:
  - Seize
  - Acquire
  - Seize and Acquire
- Block by Block acquisition with data integrity check on each block.
- IDE Hard Disks, SCSI Hard Disk, USB Storage Device, CD and Floppy acquisition.
- Supports True Back image and Raw image Acquisition
- Acquisition of Floppies / CDs in Batch mode.
- Acquisition of multiple hard disks and usb storage devices
- Checking for sterile destination media.
- Progress Bar display on all modes of operation.
- Report generation on all modes of operation.
- Print support for the generated report.
- Authentication for the available report.

## **Starting TrueBackWin**

Before starting the TrueBackWin, ensure that the Suspect's disk connected to the system is write blocked by external hardware. Start TrueBackWin from the start - >programs->True Back TrueBackWin supports Seizure, Acquisition and Seizure & Acquisition of all storage media installed in the system. The following window will be displayed on the screen.



## Seize and Acquire Mode Operation

- The “Seize & Acquire” process is normally done by a computer expert at the scene of crime. Here the acquisition will be done along with seizure. The officer must enter all the details regarding both seizure and acquire. At the end, a set of seizure floppies will be created. Figure given below shows the starting of this mode of operation.



Fig no: 1



## Step1- Seize and Acquire Information

- The below Figure shows the information collection window of Seize & Acquire mode of operation.

Options	
Investigator's Name <sup>**</sup> :	Group 4
Investigator's Rank <sup>**</sup> :	Student
Police Station <sup>**</sup> :	CDAC TVM
Crime Number <sup>**</sup> :	1
Seizure Memo Number:	
Place of Seizure <sup>**</sup> :	Kerala
Date of Hashing:	18/02/2024
Time of Hashing:	18:34:34 PM
Name of Suspect <sup>**</sup> :	Saham Singh
Address1 <sup>**</sup> :	Bhusawal
Address2 <sup>**</sup> :	Maharashtra
Name of Witness 1:	Pranay
Address1:	Abc
Address2:	mumbai
Name of Witness 2:	Shubham
Address1:	Def
Address2:	Jalgaon
Notes:	
Lab Reference Number:	Lab001
Evidence File Name <sup>**</sup> :	Minor Project

<sup>\*\*</sup> Mandatory Fields

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

Buttons: ? TB Exit Back Next

Fig no: 2

- Just like as in the earlier processes TrueBackWin checks all the fields for invalid data. User cannot proceed without entering proper data in all the fields.
- The Options menu is similar to that of Seizure process.
- On pressing the Next button, it will take you to the Media Selection dialog. The media selection process is just the same as that in the Acquire process.
- On pressing the Next button in the Media Selection dialog, it will take you to the settings dialog (Figure Below).



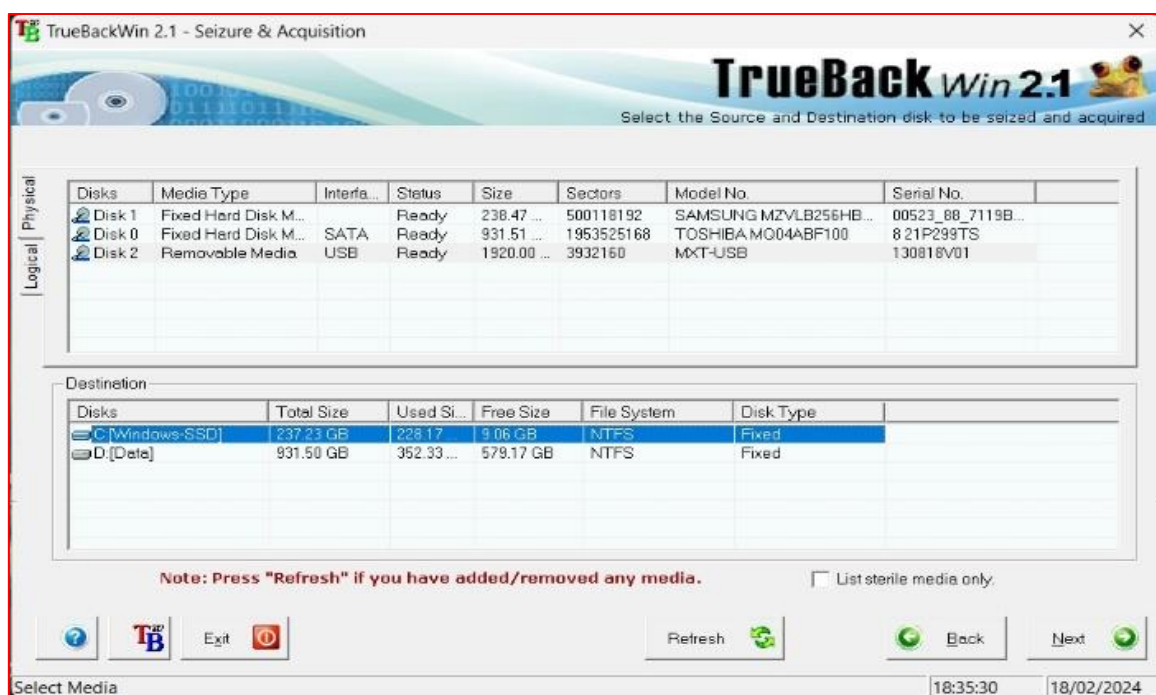


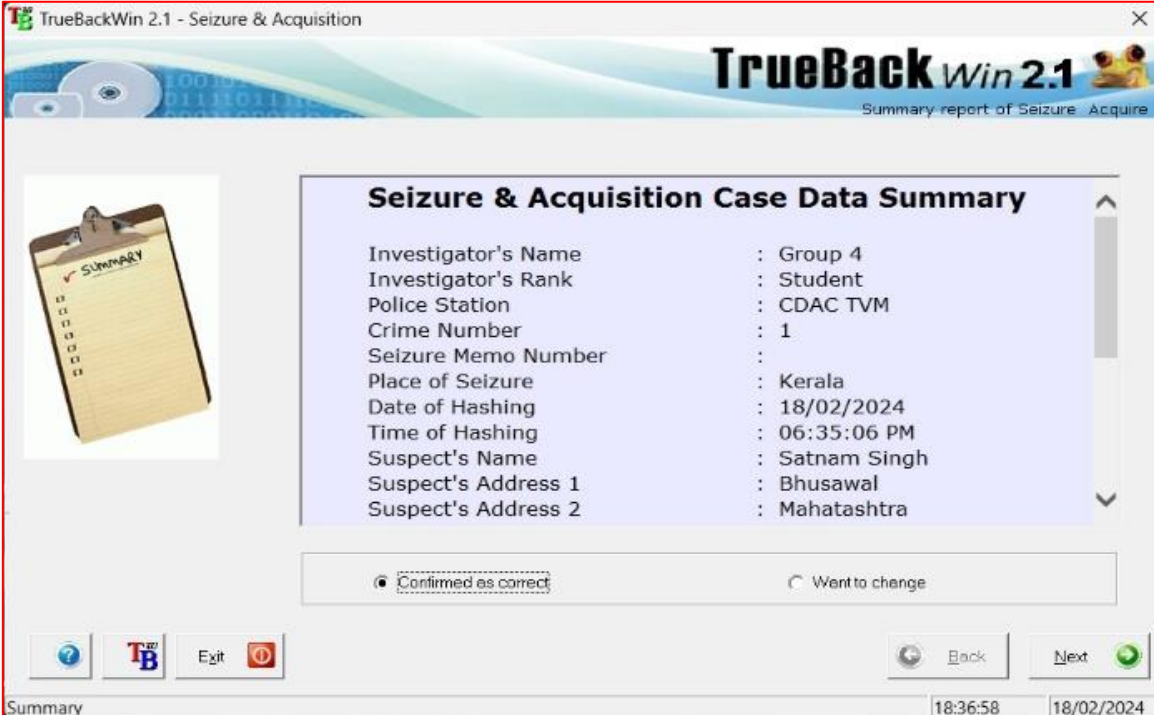
Fig no: 3



Fig no: 4

- In the settings dialog you can choose block hash mode or non-block hash mode by checking or un-checking the Enable Block Hash check button.
- If you check this option then the block size field gets enabled and you can use the up-down button to change the block size. Corresponding to the block size you choose; the total number of blocks will be automatically displayed in the Total Blocks field.
- Again, if you are seizing and acquiring Floppy or CD, you may also choose batch mode operation (by default batch mode is selected), but in this case the block hash option is unavailable and it will be disabled.
- The destination image path will be automatically generated by TrueBackWin from the destination drive chosen by the user, the investigator's name and the crime number (Figure Below).

## Step 2- Seize & Acquire Confirmation



The screenshot shows the TrueBackWin 2.1 - Seizure & Acquisition window. The title bar reads "TrueBackWin 2.1 - Seizure & Acquisition". The main window has a header with "TrueBackWin 2.1" and "Summary report of Seizure Acquire". On the left, there is an icon of a clipboard with a checklist. The central area is titled "Seizure & Acquisition Case Data Summary" and contains the following data:

Investigator's Name	: Group 4
Investigator's Rank	: Student
Police Station	: CDAC TVM
Crime Number	: 1
Seizure Memo Number	:
Place of Seizure	: Kerala
Date of Hashing	: 18/02/2024
Time of Hashing	: 06:35:06 PM
Suspect's Name	: Satnam Singh
Suspect's Address 1	: Bhusawal
Suspect's Address 2	: Mahatashtra

Below the summary table, there are two radio buttons: "Confirmed as correct" (selected) and "Want to change". At the bottom, there are buttons for "Back" and "Next". The status bar at the bottom shows "Summary", "18:36:58", and "18/02/2024".

Fig no: 5

### Step 3- Seize & Acquire Progress

- After confirmation of seize and acquire information, TrueBackWin starts the Seize and acquire process. The progress of the process is shown below.

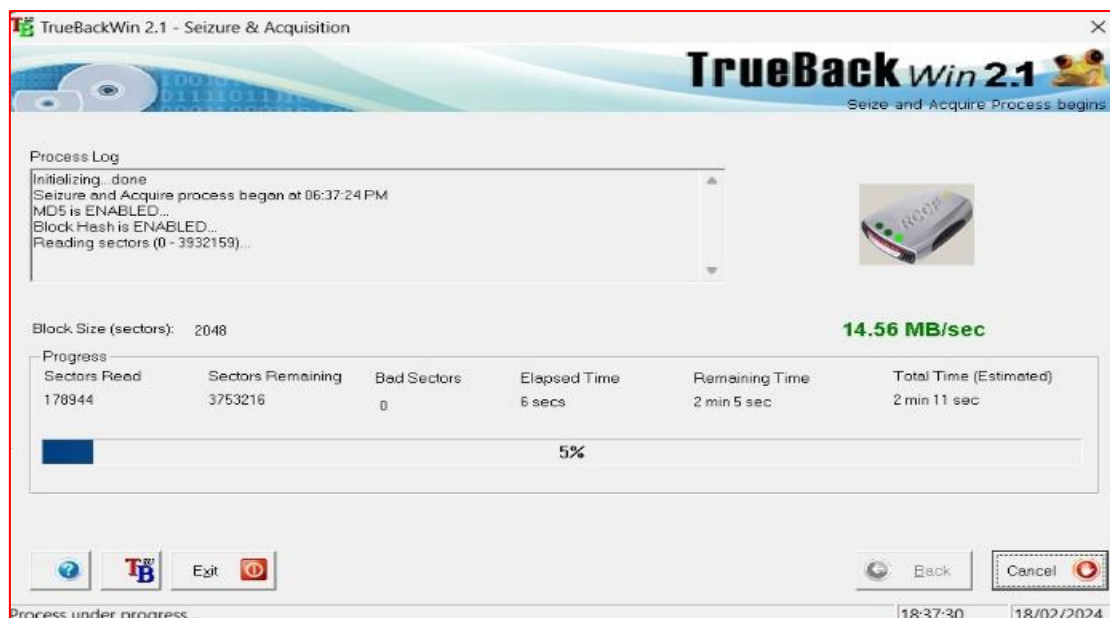


Fig no: 6

- When the process is complete, as in Seizure process the user will be prompted to label the media as shown below:

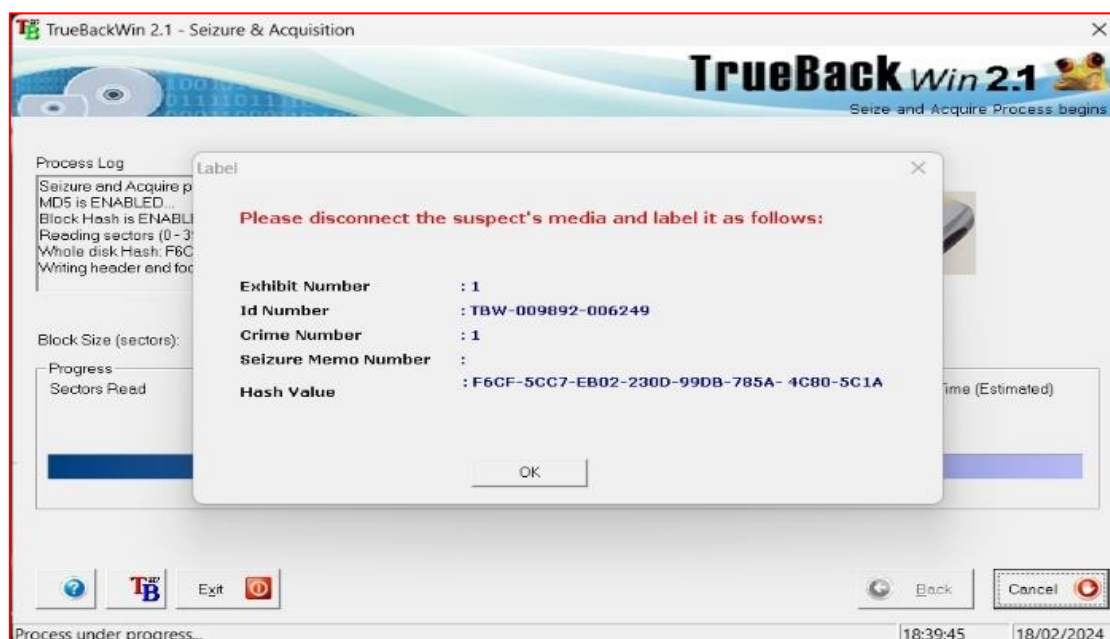


Fig no: 7

## Step 4- Seize & Acquire Report

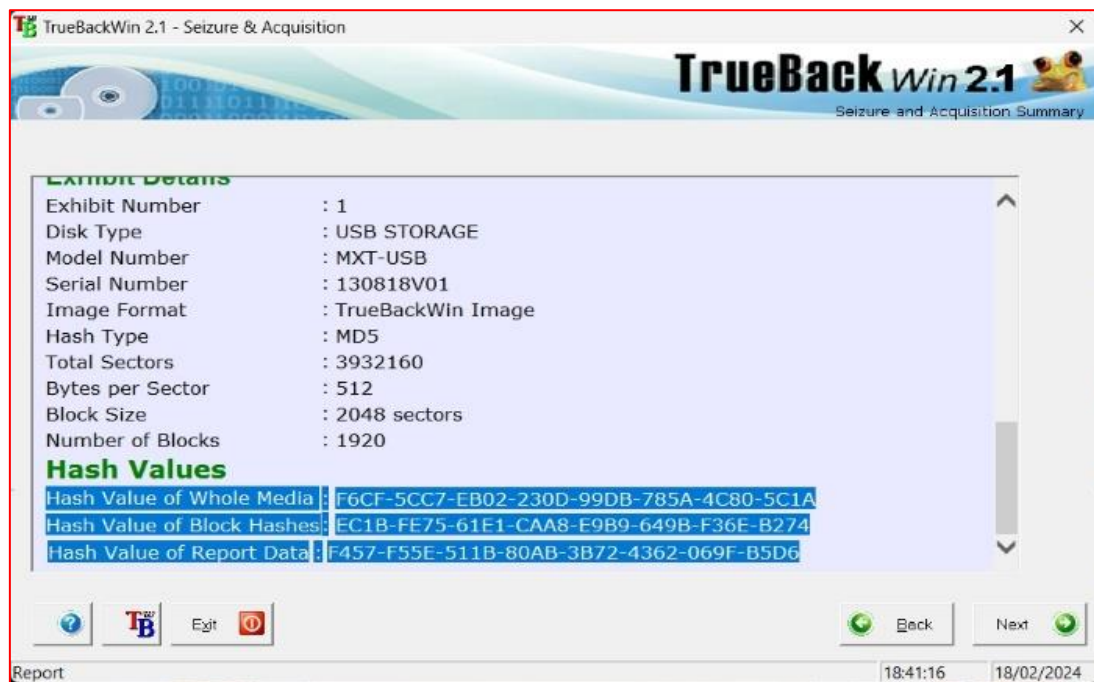


Fig no: 8

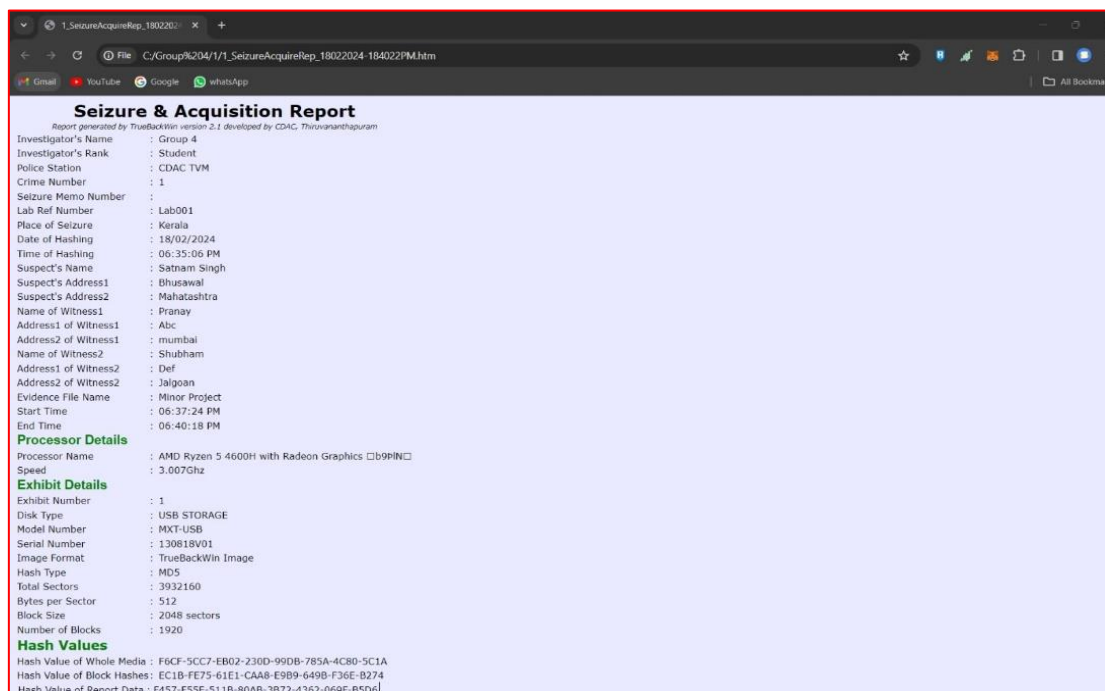


Fig no: 9

- When the seizure and acquire process is over it shows the Seizure and Acquire Report as shown in upper Figure.
- On pressing the Next button, it will take you to the seizure floppy creation dialog just as in the seizure process.
- The Seize & Acquire process is now complete.

## **Conclusion**

The utilization of the Trueback application for digital evidence collection in our forensic project has proven to be highly effective and efficient. The application's robust features, such as its ability to capture and preserve digital data without altering the original files, its compatibility with various operating systems and file types, and its user-friendly interface, have greatly facilitated the collection process.

Using Trueback, we were able to gather relevant digital evidence with precision and accuracy, ensuring its integrity for further analysis and investigation. The application's timestamping and hashing functionalities provided crucial documentation of the chain of custody, enhancing the credibility and admissibility of the evidence in legal proceedings.

Moreover, Trueback's comprehensive reporting capabilities enabled us to document our findings thoroughly, providing clear and concise documentation of the collected evidence, actions taken, and analysis conducted. This has proven invaluable in communicating our findings to stakeholders, including law enforcement agencies, legal teams, and other relevant parties.

Overall, the Trueback application has significantly enhanced our digital forensic capabilities, streamlined the evidence collection process while maintained the highest standards of integrity and reliability. We highly recommend its use in future digital forensic investigations due to its effectiveness, reliability, and user-friendly interface.