LAB MANUAL
ON
(True Back-Win 2.0)

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY
TRAINING TO TECHNICAL TEACHERS
DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION
SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

PREPARED BY:

Dr. Maitreyee Dutta (Principal Investigator)

Mr. Jaspreet Singh (Lab Attendant)

Table of Contents

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 insures 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. In order 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. This 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. In the Seize & Acquire mode, both Seize

process and Acquire process would be performed at the scene of crime itself. But it requires services of a computer expert at the scene of crime. In this mode also, an exact copy of the suspect's hard disk would be created from the scene of crime itself.

In addition to these three modes of operation, TrueBackWin has another feature named Verify Report. By this feature, the authenticity of the already available Seizure Report or Seizure & Acquisition Report can be checked.

A+ GUI based windowing system is provided as User Interface to TrueBackWin. This ensures a very user-friendly operation to the user. User can either use keypad keys or mouse for the traversal through TrueBackWin software. Hot-keys are also provided wherever possible to make the traversal quick and efficient.

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.

Getting Started

System Requirements

Hardware	:	Pentium III or higher 64 MB RAM or more. Floppy Drive.
Operating System	:	Windows XP or above.

User Pre-requisites

TrueBackWin is a disk imaging tool. It is expected that the user of TrueBackWin has fundamental knowledge about the computer usage as well as different storage media of a computer system. TrueBackWin is executed in a Forensic workstation, since TrueBackWin is expected to use for cyber forensics purposes.

Before executing True Back-Win, user should connect the necessary storage media to be seized with write block hardware.

Starting TrueBackWin

Before starting the True Back-Win, ensure that the Suspect's disk connected to the system is write blocked by external hardware.

Start TrueBackWin from the start ->programs->True Back

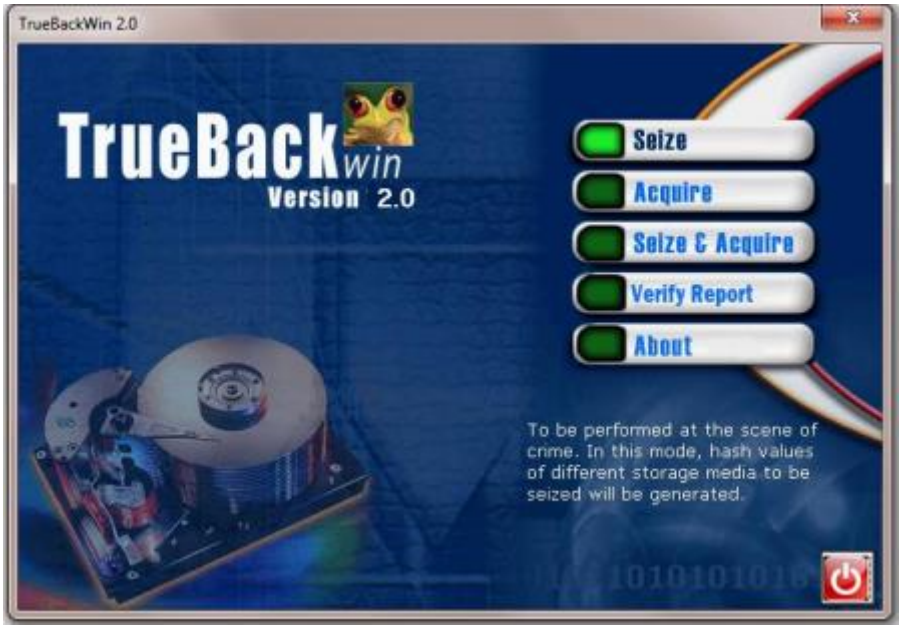
TrueBackWin supports Seizure, Acquisition and Seizure & Acquisition of all storage media installed in the system.

The following window will be displayed on the screen.

Seize Mode Selection

In the Seize mode, only a hash value of the storage media of the suspect's computer system is taken. From the main interface given in Following Figure.

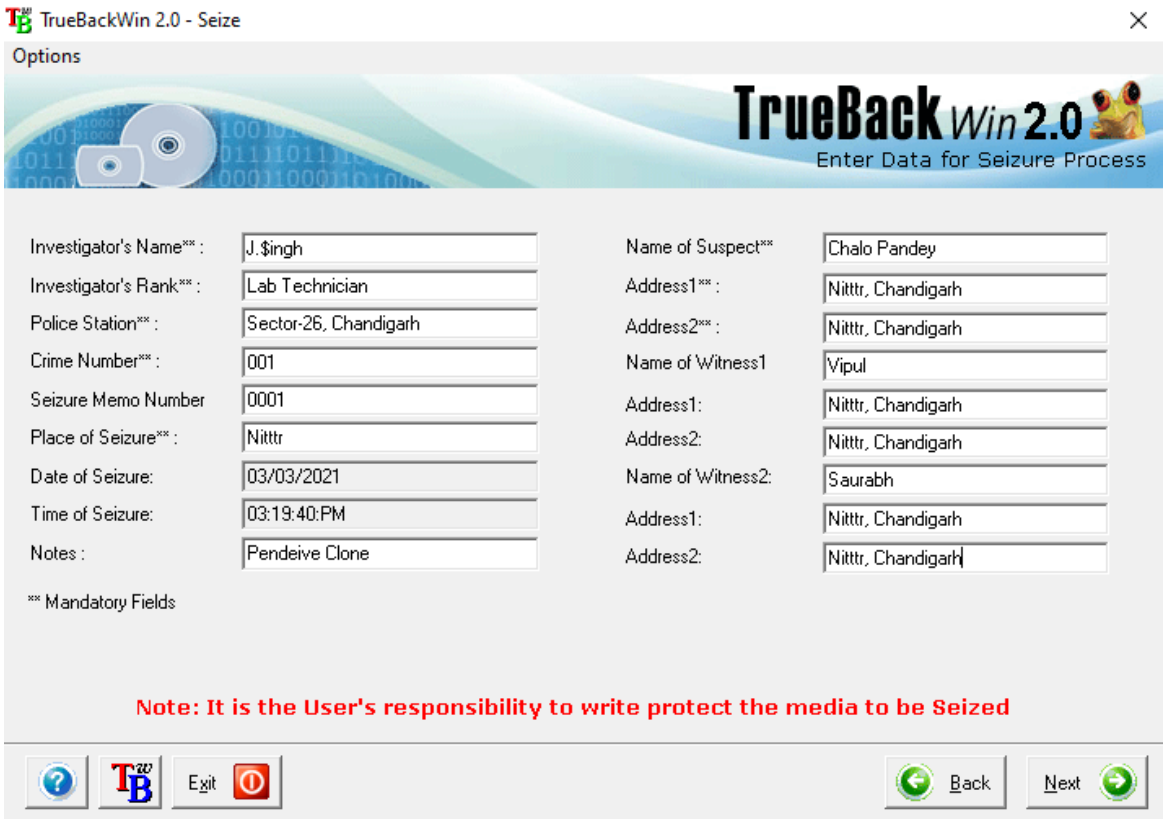
STEP 1- Select Seize button. You can use your mouse or Keyboard for selecting the desired mode.



STEP-2 Seize Information Collection

A seizure information collection window appears on the screen as shown in the Following Figure.

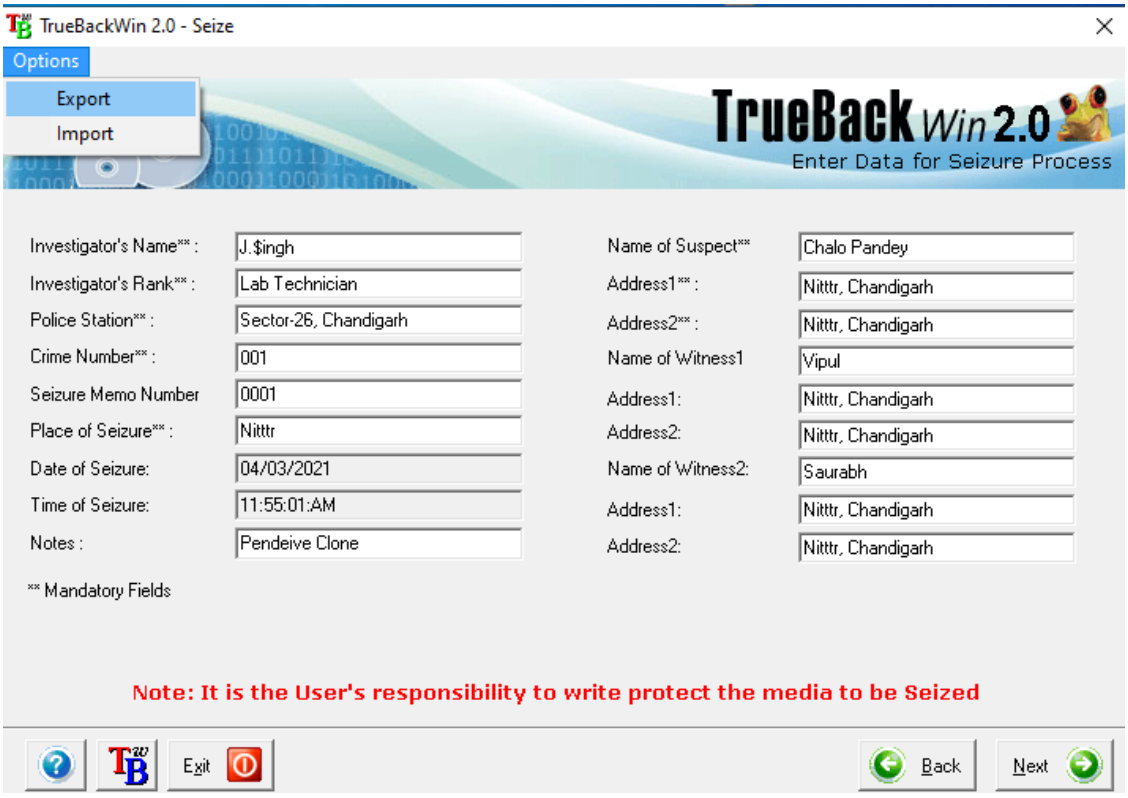
- All the field entries are mandatory.
- Proper Validation is done on all fields.



In this window, data can be entered in different ways. One way is to enter the data manually. Type of data to be entered in each field is self-explanatory. The Time of Seizure and Date of Seizure values are read from the system. Validation check on the data entered is performed when the Next button is pressed.

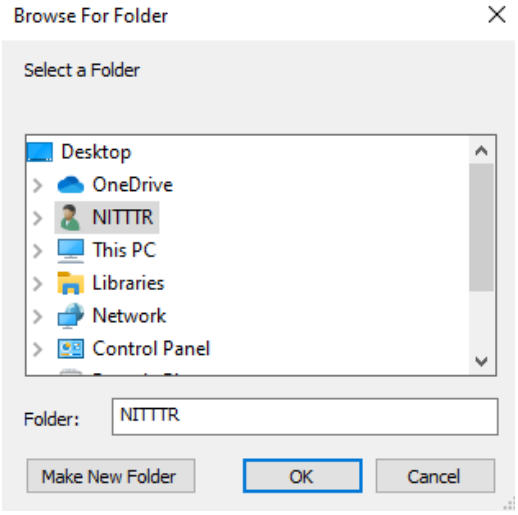
Step 3-

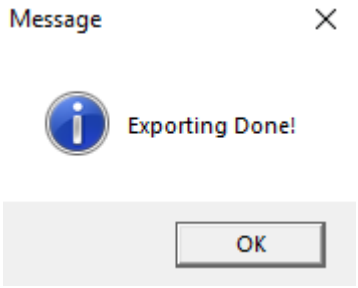
- In the Following Figure Options menu provides two functionalities VIZ Export and Import functions.
- The Export function allows the user to save the validated user entries entered into the data collection window.



Step 4-

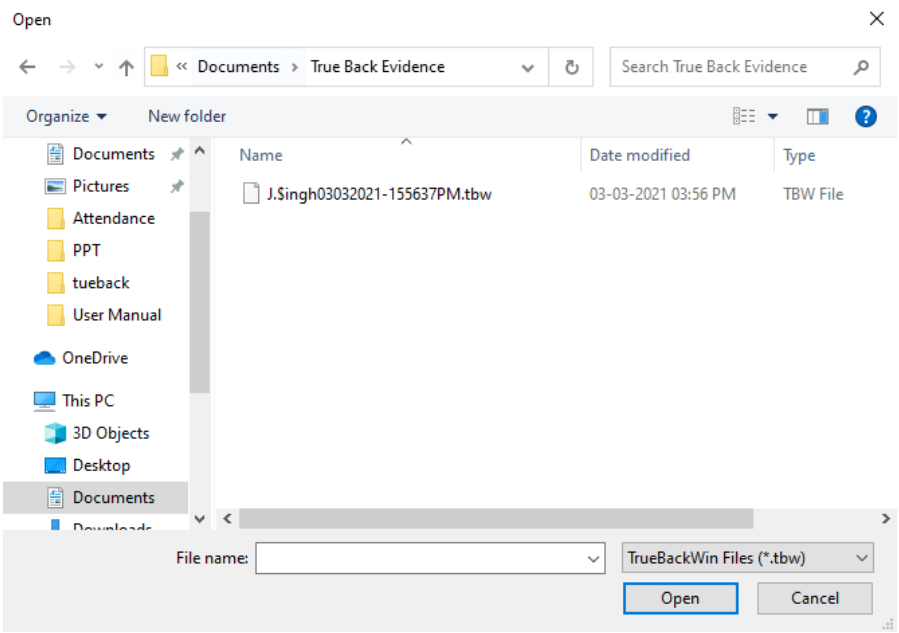
- Upon clicking the Export function, a dialog box will appear prompting the user to select a folder to save the data.
- Following Figures shows the folder selection window.
- On selecting a folder, the data will be saved in a Text file (.txt) and a message gets displayed as below.





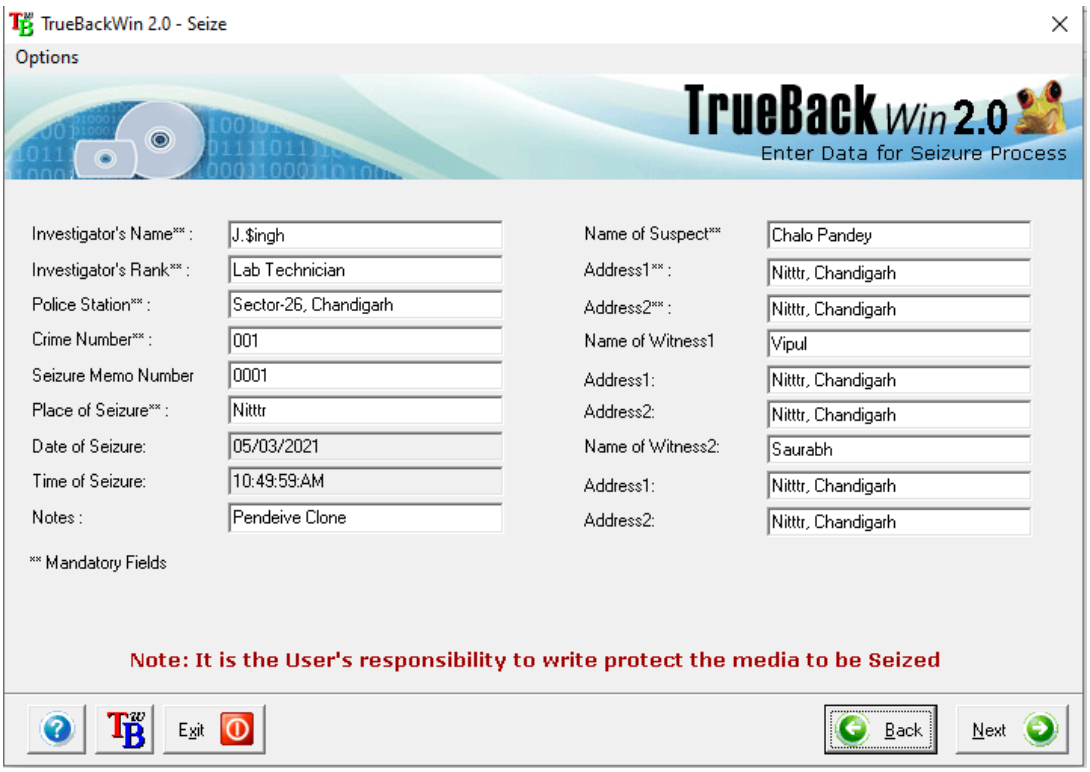
Step 5-

- Another way to fill the data collection window is using Import function in the Options.
- On clicking the Import function, a Text File selection window appears as in Following Figure.
- Now select an appropriate file and click Open. The data will get filled in the data collection window.



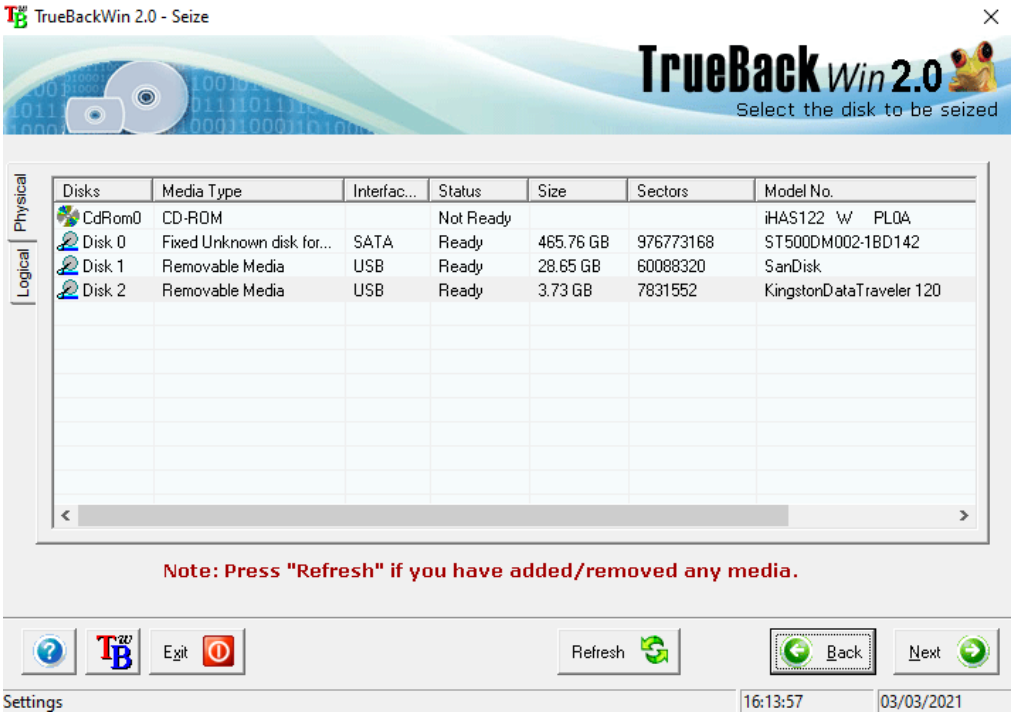
Step 6-

- After all the data has been entered in the data collection window that shown in following Figure
- Press the Next button.
- Now the control will move to the media type selection window.
- If the user wants to make any correction in the data collected in any of the previous windows, he/she can go to that window using Back button, wherever possible.
- Beside select the drive that listed.



Step 7- Source Media Selection

- Select a drive from the list and press next.
- The subsequent window enables the user to specify the settings with which the seizure process should be continued.



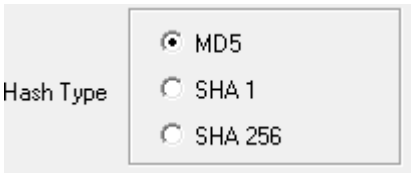
- If the user selects the Block Hash option, TrueBackWin divides the entire content of the source media into convenient block sizes before starting seizure process.
- Hash value of each block of data would be computed during seizure process and it would be logged into a file.
- This information is used while acquiring the hard disk in the Acquire mode of operation. Since each block has its own hash value, a distributed data integrity check

Step 8- Settings for seizure

- By default, for Floppy and CD, batch mode is selected by default. However this mode is disabled for all other devices.

Step 9- Hash Type Selection

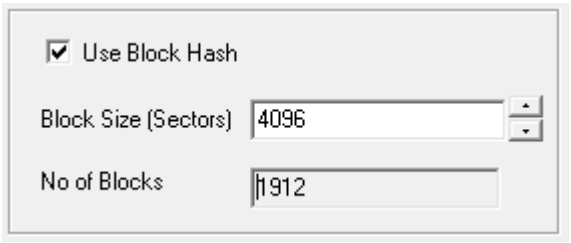
- TrueBackWin supports three types of hashing VIZ MD5, SHA1 and SHA256. The user is free to select any type of hashing.
- Following Figure shows the hash type selection part.



Step 10- Block Size Specification

- In the case of IDE, SCSI and USB storage devices, user can specify the size of a block in sectors for hash computation.
- The settings dialog box for specifying the block size is shown in The Following Figure.

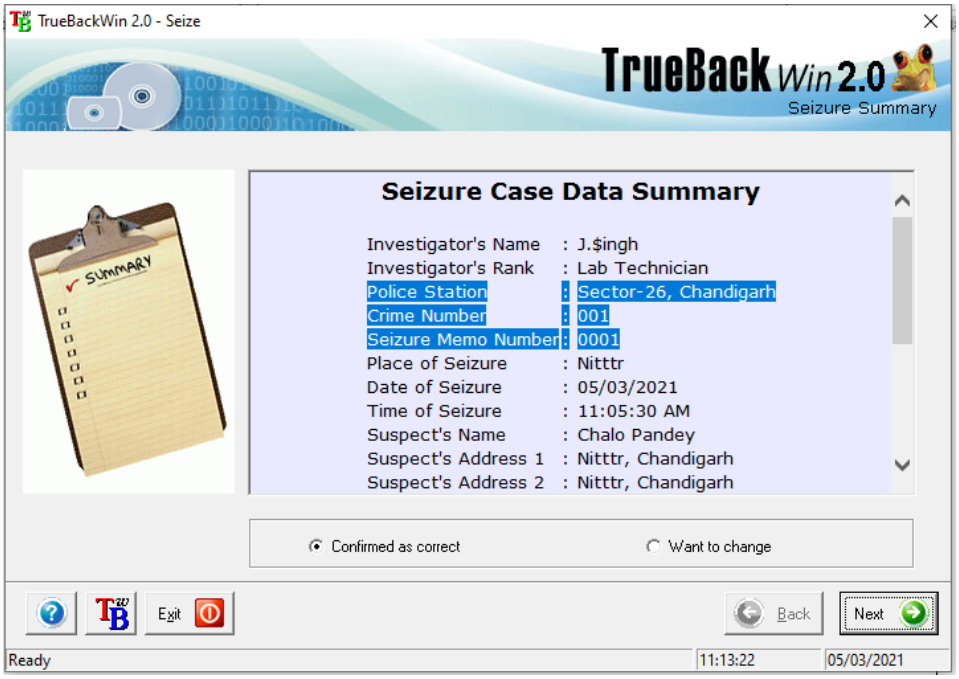
  By default, TrueBackWin displays a block size for a specified storage device depending upon its size. User can change this to a higher value subject to the conditions that the entered value must be less than or equal to the size of the selected hard disk.
- User cannot select a value greater than this. Further, user is limited to select a block size which is a multiple of 128 sectors (in case of IDE/SCSI/USB) or 32 sectors (in case of CD).



Step 11- Confirming Seizure Information

- Following Figure shows the window displaying all the details collected previously for confirmation.
- If you want to edit or change the collected information, press Back button until the required dialog appears.
- Choose Confirm as Correct option and press Next button to continue the seizing process.

- It will take you to the process dialog and the seizure process begins.



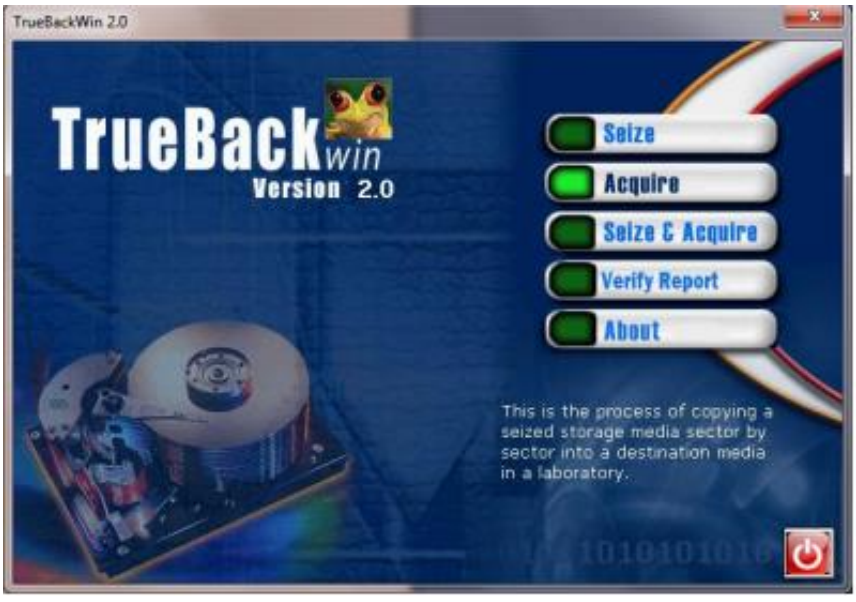
Step 12- Disk Seizure Progress-

- Following Figure given below shows the various progress Information of the seizure process.

Acquire Mode Operation

In the Acquire mode, user can specify the source media and destination media, 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 any of the available hash algorithms VIZ MD5, SHA1 and SHA256 will be performed on the data read. During acquisition, hash values of each block will be computed and compared with that generated during Seizure process. If there is any mismatch between hash values of any block, it will be reported and logged into a file. Block size for copy will be the same as that is used for seizing the storage media. Acquisition mode of operation can be initiated from the main window by selecting the Acquire button as shown in the Figure below.

Step 1 – Click on Acquire Button

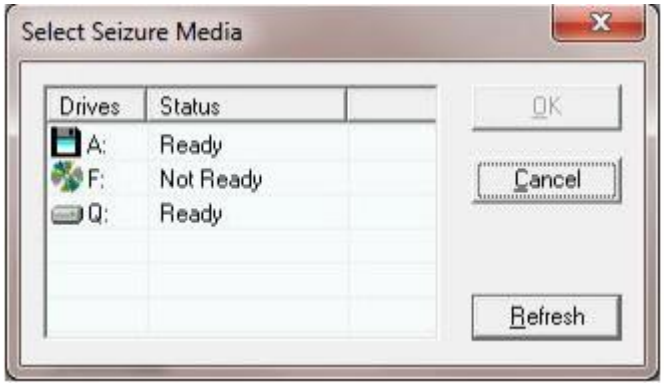


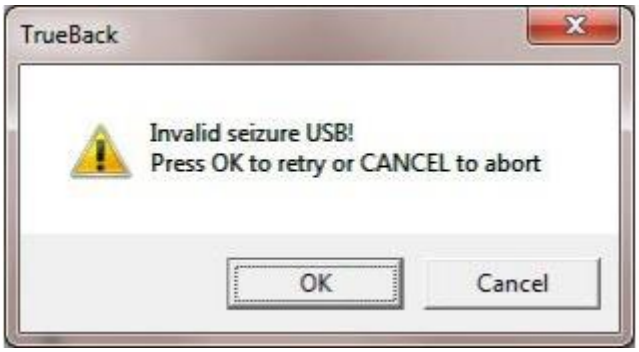
Step 2- Acquire Information Collection

Step 3-Request for Inserting Seizure Floppy

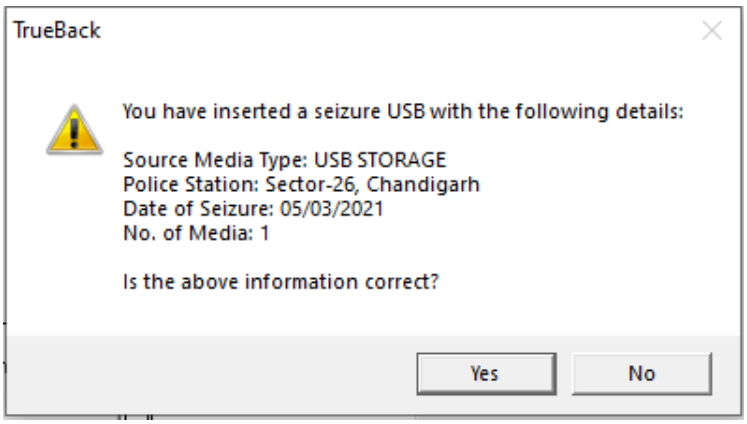
- As soon as you fill in the entire case details information, the Next button gets enabled.
- On pressing the Next button TrueBackWin will ask for the seizure media which was created by TrueBackWin while the same media was seized.

- Acquisition process cannot continue until you insert the correct seizure media.
- The seizure media can be a Floppy, CD-ROM or USB storage. The seizure media selection window is shown in Following Figure.
- On selecting a seizure media which is ready, the OK button gets enabled.
- On clicking the OK button, the selected seizure media is checked for valid seizure information.
- The process can continue only if it is a valid seizure media.
- Otherwise TrueBackWin will report that it is an invalid seizure media selection. Following Figure shows the message of an invalid seizure USB selection.





- If the correct seizure media was inserted then TrueBackWin will prompt you to confirm the information in the seizure media as shown below.



- If the No button is pressed then the process is suspended until the user presses the Next button again.
- On pressing the “Yes” button TrueBackWin will prompt you to insert or connect the required device with an ID number for acquisition. The following figure shows such a dialog box.

- Pressing cancel will let you to remain on the same Data
- Collection page.
- Pressing OK button will take you to the disk selection window

Step 4- Disk Selection

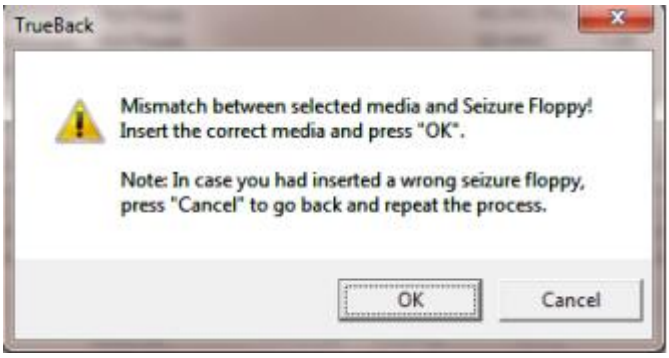
- Following Figure shows the dialog box that follows Just Upper Figure. This is the disk selection window.
- The listed media shows the source media information. It has two tabs showing physical partition listing and logical drives information.

- However, if there are sterile drives or the check box is unchecked, it lists all the available destination media which ful fills the necessary space requirements for acquisition of the selected source disk as show below Figure.

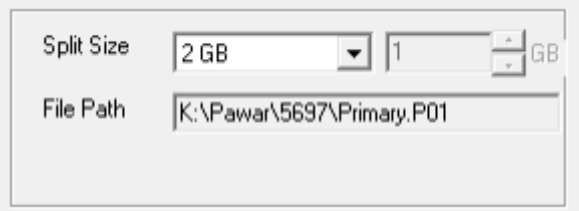
- The destination for a TrueBackWin acquire is normally a sterile media (it's a mass storage media {IDE Hard Disk /SCSI Hard Disk / USB Storage Device} with any formatted windows file systems (FAT16 / FAT32 / NTFS) partition having no data).

- If a destination storage media contains evidence file of a previous acquisition process, TrueBackWin will consider the media as a sterile media for another acquisition, if the crime number and police station name of the second acquisition process are same as that of the first acquisition. This means that TrueBackWin allows copying of multiple sources into a destination as long as the multiple sources are related with same crime and investigated under the purview of same police station.

- As the user press the next button TrueBackWin will does a cross check between the selected media and the information contained the seizure floppy. If the selected media differs from the one that was seized, a message window is displayed as shown below:



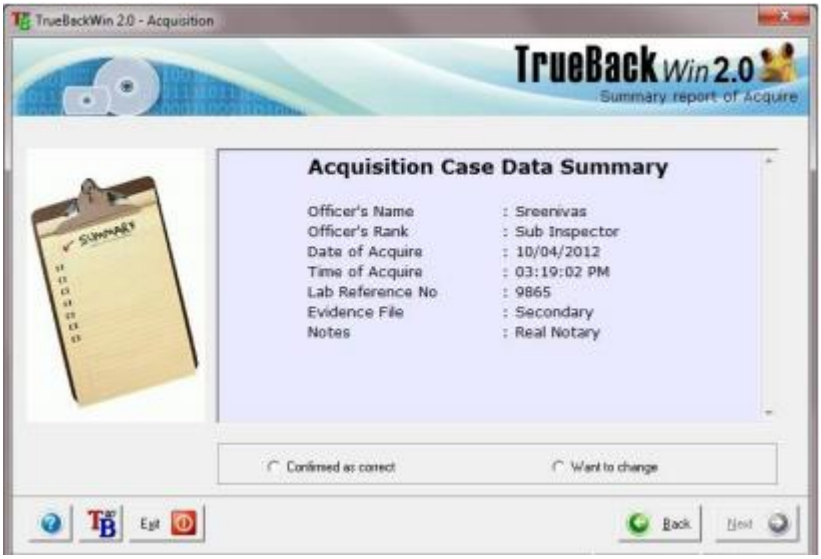
- If you press OK you can select the correct media from the media selection dialog again. If you press “Cancel” it will return to the Acquisition case data collection dialog.
- The settings dialog shows the split size and file path, where the acquisition is going to be done. Here you can change the split size by selecting from the combo box.



- You can also choose the type of the image file to be generated: TrueBackWin image or Raw Image. A TrueBackWin image can only be loaded in Cyber Check where as a Raw image can be loaded in most of the commercially available cyber forensic tools. That shown in Following Figure.

- If the user choice is for a TrueBackWin image, then he/she can opt for compression also. This feature is void for raw image that shown in Following Figure.

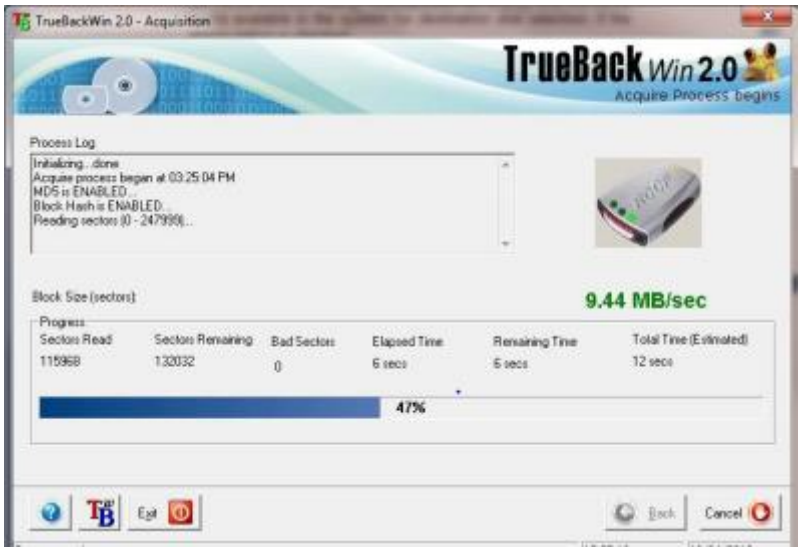
Step 5- Confirming Collected Information for Acquire



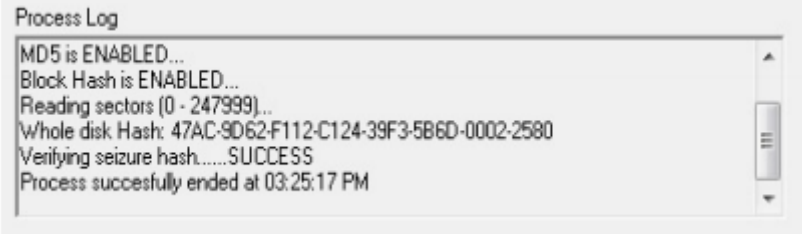
- On choosing “Confirmed as Correct” the Next button gets enabled. Pressing the Next button will take you to the process dialog.

Step 6- Acquire Progress

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



- When the process is complete, the process log will show the success and failure of hash computation in acquisition of the seized media. One such dialog is shown below.



Step 7- Acquire Report

- Once the acquisition process is over, an acquisition report will be generated and displayed in a window as shown in upper Figure.

- TrueBackWin saves the acquire report in an html file with evidence file name as its base name and .HTM as its extension. Also, TrueBackWin generates a log file containing details of the errors, if any, occurred in the acquisition of different blocks of data. This file also will have the evidence file name as its base name and .LOG as its extension. These files will be written in the destination media for the use in analysis process.

Seize and Acquire Mode Operation

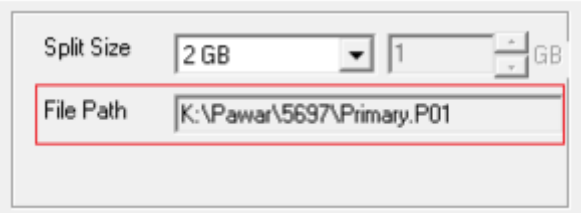
- The “Seize & Acquire” process is normally done by a computer expert at the scene of crime. Here the acquisition will be done along with seizure. The officer has to enter all the details regarding both seizure and acquire. At the end, a set of seizure floppies will be created. Figure given below shows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

Step1- Seize and Acquire Information

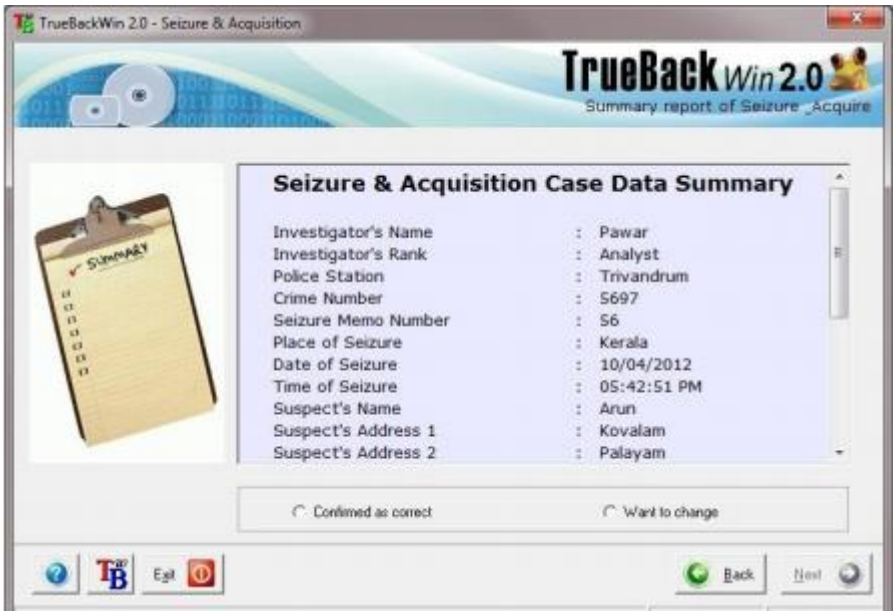
- The below Figure shows the information collection window of Seize & Acquire mode of operation.

- 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).

- 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).

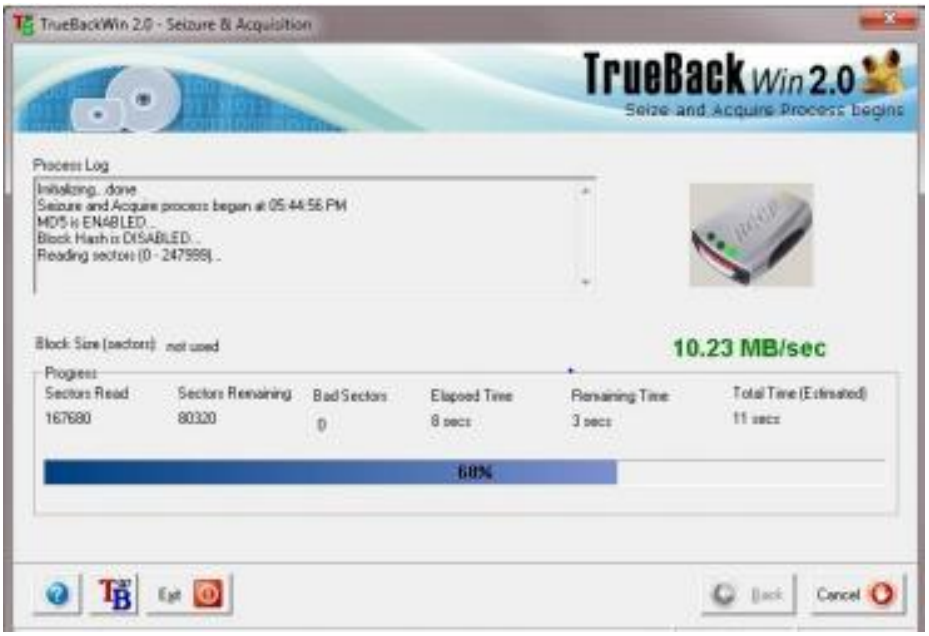


Step 2- Seize & Acquire Confirmation



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.



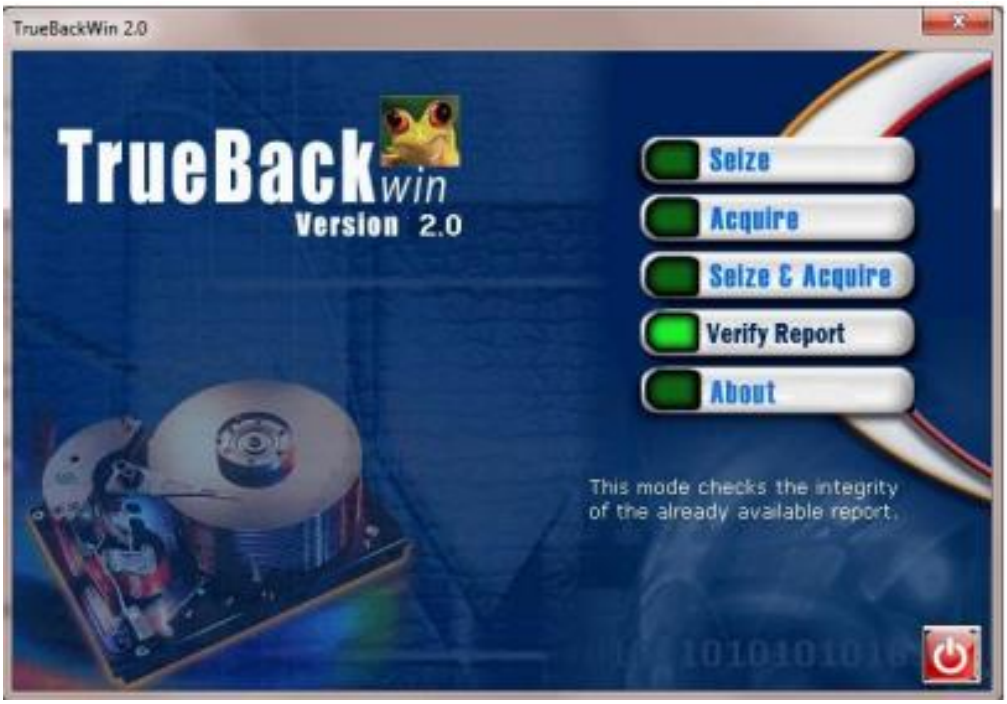
- When the process is complete, as in Seizure process the user will be prompted to label the media as shown below:

Step 4- Seize & Acquire Report

- 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.

Verify Report

- The “Verify Report” is a new feature introduced in TrueBackWin 2.0. This process authenticates an already available Seizure or Seizure and Acquisition Report. The officer needs to give the report name only. The Verify Report process will check the integrity of the report. Figure given below shows the starting of this mode.



Step 1- On clicking the Verify Report button, a window similar to Below Figure gets displayed.

Step 2- Clicking the Browse button, opens a file dialog box as Shown below.

Step 3- Selecting a HTML report file fills the File Name field similar to Figure Below.

Step 4- Now, you can click the Verify button. A log of the process Done and verification result will be printed in the Process Log part. A similar figure is shown in Below Figure.

Step 5- Clicking the Exit button takes you to the Confirmation Dialog shown in Below Figure. Clicking YES button in The Figure will let you move to the TrueBackWin main Window.