Test Report

Of

BitRaser Data erasing Tool V 1.2

For

Stellar Information Technology Pvt. Ltd,
D-16, Infocity Phase-II, Sector -33
Gurgaon -122001, India

STQC IT SERVICES
ERTL (E), Block - DN, Sector - V, Salt Lake
Kolkata – 700091

Job done during 18th June to 20th July 2016
Report released on: 26th July 2016

Tested by: Mr. Tapas Bandopadhyay, Sc 'F', Ms. Malabika Ghose, Sc 'F', and Mr. Sanjay Prusty, Sc 'B'

Reviewed by: Subhendu Das, Sc 'F'

Table of contents

1. Introduction

The STQC IT Services, Kolkata has tested the BitRaser V1.2 Data erasing tool on request of M/S Stellar Information Technology Pvt. Ltd. (P.O.:SITPL/PO/SITPL/May/010 dated 16-05-2016) to assess the secure erasing capability so that after erasing the data files contained in the memory devices could not be recovered. The testing is performed in 'black-box' mode.

2. The product

BitRaser is a portable and reliable application providing permanent data erasure of storage device. This application erases data in order to prevent recovery of sensitive data that is no more required. While formatting the hard drives, still found an open possibility of data being recovered. BitRaser solves this problem efficiently by using powerful algorithms that fill the storage device with useless binary data. This leaves no possibility of data being recovered.

3. Scope of Testing

Testing of BitRaser v1.2, an application providing permanent data erasure for different type storage devices. The STQC Lab will test the said software data erasing tool for its capability to erase data on different storage devices (SATA, PATA, SCSI hard drives, SSD & USB drives) and for the file systems NTFS, FAT (32/64), Ext3, Ext4) and verify whether data on the storage devices could not be recovered after erasure. The scope of this testing is limited to erasing of data through the algorithm, "NIST Clear" only on the said file systems, as requested by M/S Stellar Information Technology Pvt. Ltd.

3.1. Exclusion

a) The erasing techniques other than "NIST Clear" algorithm as defined in the scope.

b) The non-security features, like performance, Capability etc.

4. Test Objective and methodology

The software application BitRaser V1.2 is applied on the data on the storage devices (like SATA, PATA, SCSI hard drives, SSD, USB drives) with file systems NTFS, FAT (32/64), Ext3, Ext4 and it is to be verified that whether data on the storage devices could be recovered after erasure. The test environment, at STQC IT services, Kolkata, is simulated as per the device documentation (supplied by the customer). The storage devices are configured as per the manufacturer's installation and configuration guidelines. The test cases are prepared based on the security services, specified in the respective device documentation.

The devices are operated as per the Operating Guidance document (to be submitted along with the device). The testing is carried out in two phases, one after complete erasing of the data on the devices and other in disrupted state (incomplete erasing).

5. Test Setup

5.1 Test set up diagram

The BitRaser V1.2 data erasing tool is tested as depicted in the test set-up figure 1 and figure 2. The test set-up consists of a computer system with different storage devices and data recovery tools are installed for data recovery purpose. The storage devices (SATA, PATA, SCSI hard drives, SSD & USB drives) are mounted in the computer system as shown in figure1. The data recovery tools are installed in the computer system as shown in figure 2.

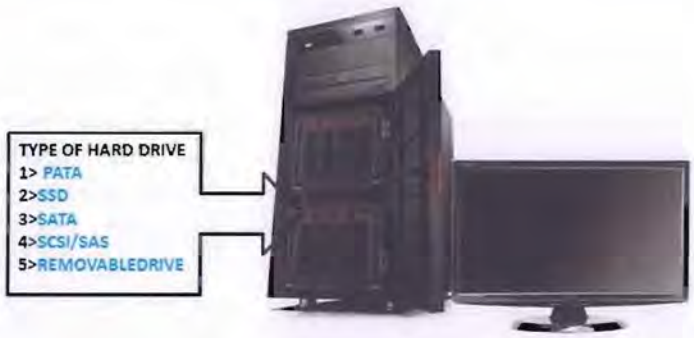

Figure1: Test set up for data erasing with different storage devices

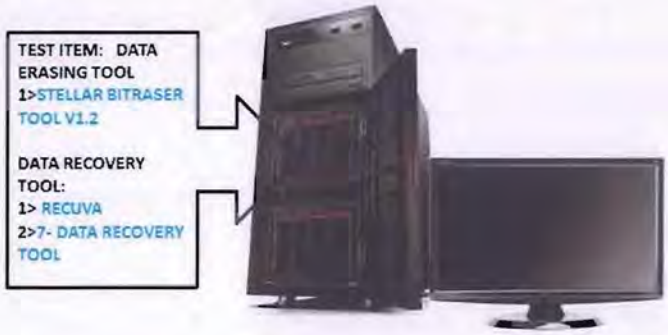

Figure 2: Test set up for attempting Data recovery with different tools

5.2 Tool Used for testing purpose:

For data recovery:

1. Recuva data recovery tool version 1.52.1086
2. 7 - data recovery tool Version 3.6

For content viewing of raw data on the drive:

3. WinHex Editor Version 18.8

6. Executive Summary

STQC IT service Kolkata tested the tool "BitRaser V1.2", in respect of its capability to erase the data files in different storage devices. The testing has been carried out with "BitRaser V1.2", using "NIST Clear" algorithm, on different storage devices like SATA, PATA, SCSI hard drives, SSD & USB drives with different file systems like NTFS, FAT (32/64), Ext3, Ext4. The results show that the erased data could not be recovered with the available data recovery tools used for the testing purpose. This report provides readers with validated evidence about a product's capability as secure data erasing features.

7. Detailed Test Reports (Annexure-I to V)

---- o ----

Annexure-I

Test cases related to USB drive

TC-1a: Data erasing in the USB drive by the stellar Bitraser tool for the NTFS file systems

Test Objective: Whether the data erased in the **USB drive** by the stellar Bitraser tool cannot be recovered for the **NTFS file systems:**

Scenario:

The figure TC-1a-1 shows the available file system in the test drive (USB). For the testing purpose some test files are loaded on the USB device as depicted in the Figure TC-1a 2. The files containing on the USB drive are erased using the "NIST Clear" algorithm of the "BitRaser V1.2". After erasing the data files, attempt was made to recover the erased files from the drive, using two separate data recovery tools, as mentioned in section 5.2.

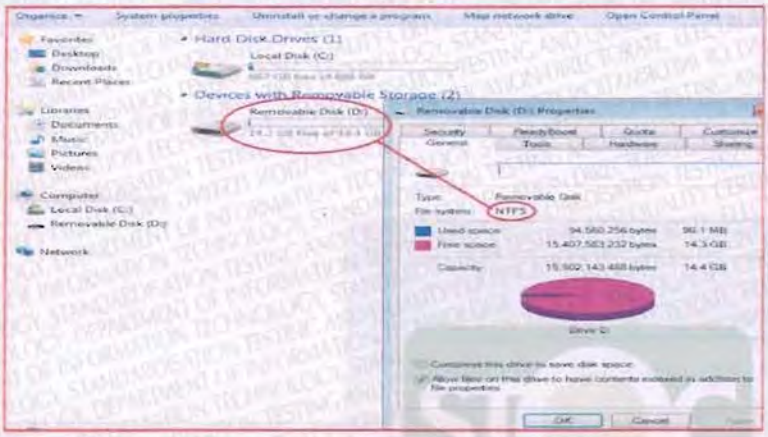

Figure TC-1a-1: Showing NTFS file system in the USB drive.

Figure TC-1a 2: Showing Files in the USB drive with NTFS file system before erase.

Test Procedure:

1. Connect Stellar BitRaser USB Drive to boot the computer.
2. Set boot priority to either boot computer from BitRaser CD or from USB stick in the Section 'Boot Device Priority' and save changes before exiting BIOS. Now system is ready to boot from bootable disc or USB drive.

3. After restarting the system, BitRaser home screen appears. All storage devices along with their information like model number, serial number, storage capacity, total sectors, attribute and interface are displayed.
4. Select the storage device (USB drive) to be erased by the tool and select the algorithm "NIST Clear" for the erasing of the files in the Drive.
5. Select Total Verification as erasure verification method under 'Advanced Option'.
6. Click Erase to start erasing the storage device.
7. After erasing the data files the drive will be attempted to recover using tools.

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Results:

Figure TC-1a -3a Stellar BitRaser Setup screen

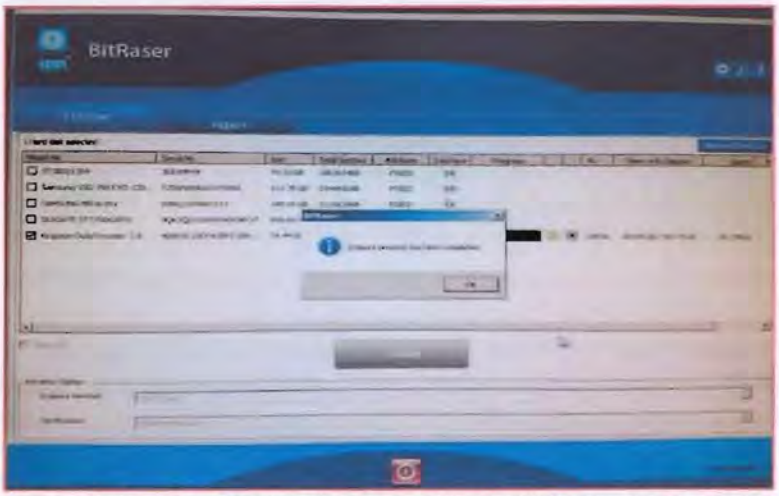

Figure TC-1a -3b: showing data erased in the USB drive by the stellar Bitraser tool.

Figure TC-1a -3d. Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

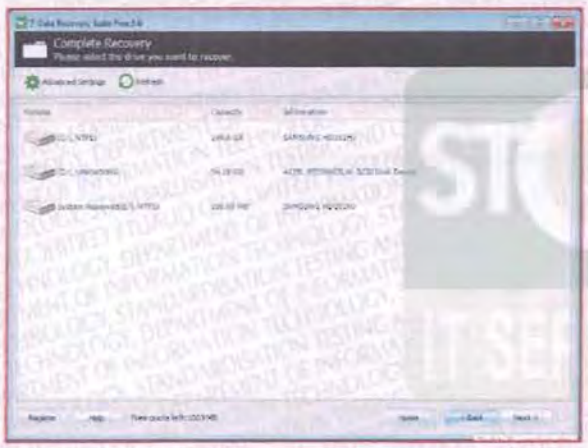

Figure TC-1a 3e. Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

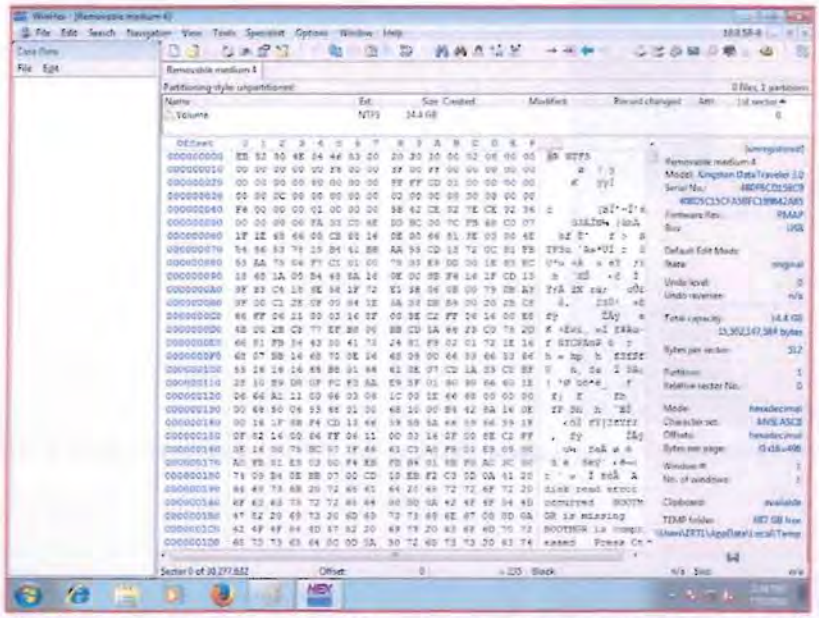

Figure TC-1a -3f: WinHex tool showing Data on USB drive before the data erasing action

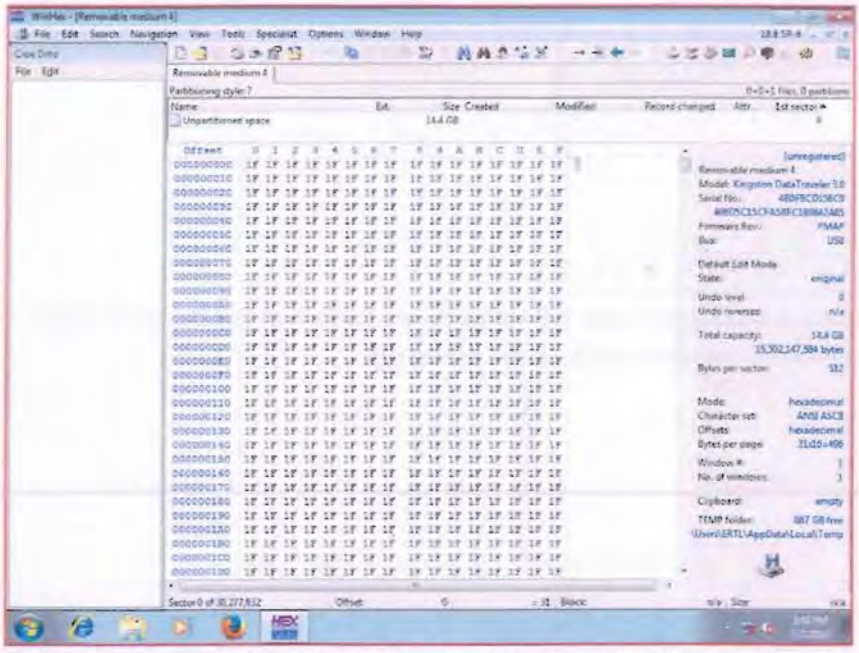

Figure TC-1a -3g: WinHex shows the drive content after data erasing, no data is there in the drive sectors

Remarks: Pass, the erased data in the drive could not be recovered.

TC-1b: Data erasing from the USB drive by the stellar Bitraser tool for the FAT32 file systems

Test Objective: Whether the data erased in the **USB drive** by the stellar Bitraser tool cannot be recovered for the **FAT32 file systems**:

Scenario:

The figure TC-1b-1 shows the available file system in the test drive (USB).For the testing purpose some test files are loaded in USB drive device, as depicted in the Figure TC-1b -2. The files on the USB drive are erased using the "NIST Clear" algorithm of the "BitRaser V1.2". After erasing of the data files, attempt was made to recover the data files using data recovery tools, as indicated in section 5.2.

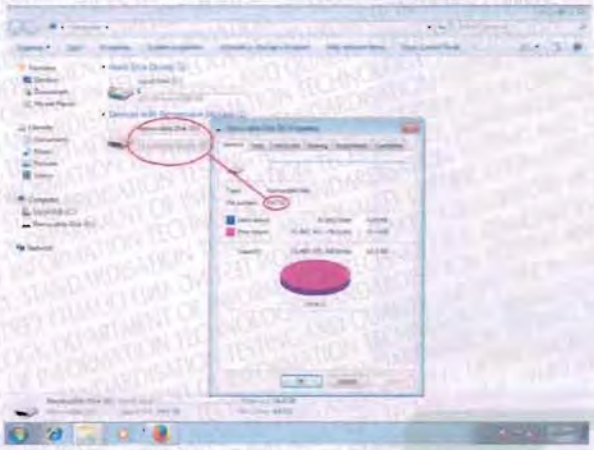

Figure TC-1b-1: Showing FAT32 file system in the USB drive.

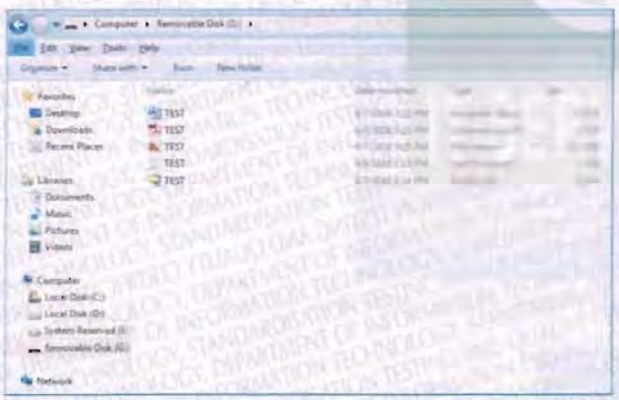

Figure TC-1b -2: Showing Files in the USB drive with **FAT32** file system before erase.

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Results:

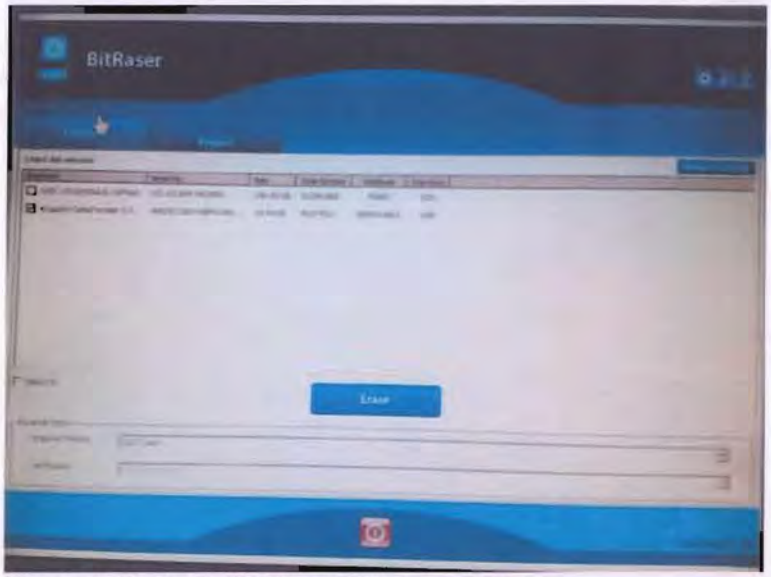

Figure TC-1b -3a Stellar BitRaser Setup screen

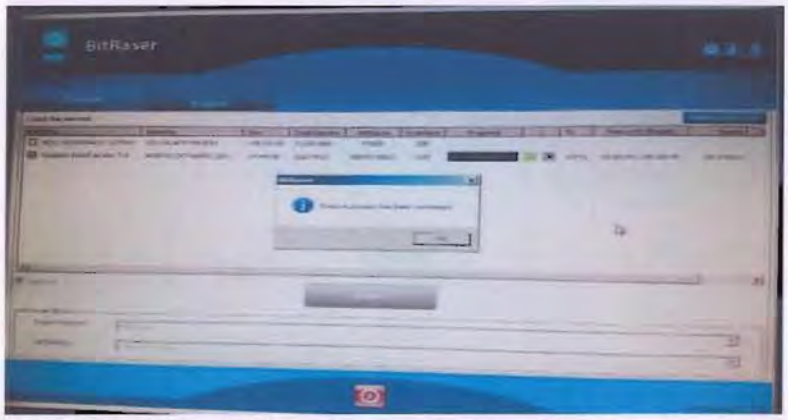

Figure TC-1b -3b: showing data erased in the USB drive by the stellar Bitraser tool.

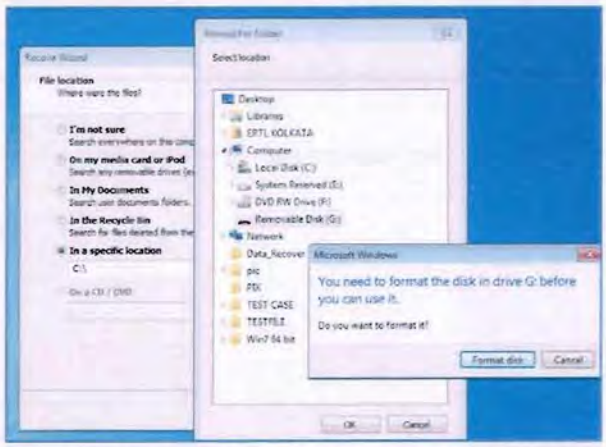

Figure TC-1b -3c: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

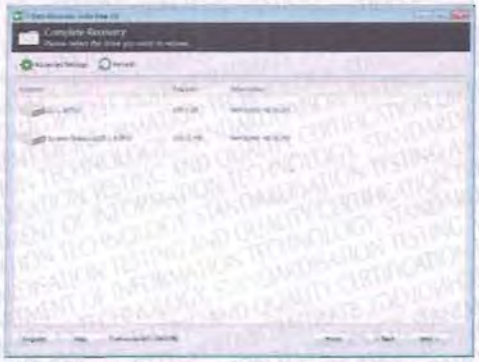

Figure TC-1b -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected)

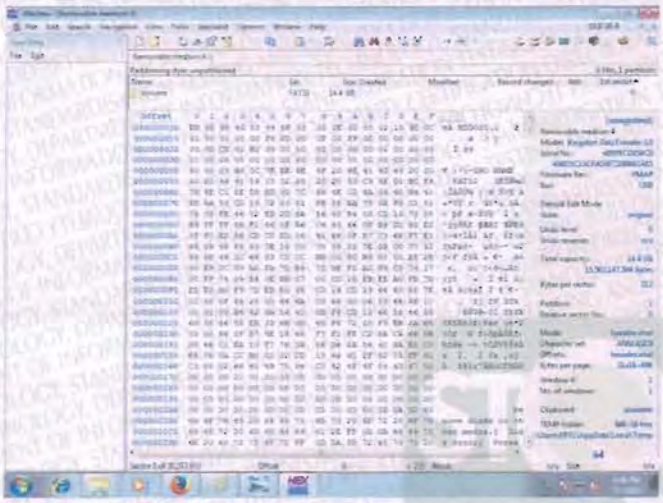

Figure TC-1b -3e: WinHex tool showing Data on USB drive before the data erasing action

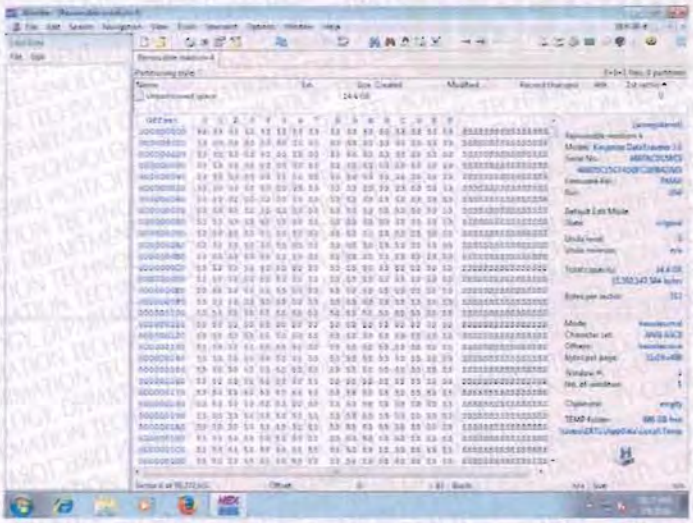

Figure TC-1b -3f: WinHex shows the drive content after data erasing, no data is there in the drive sectors

Remarks: Pass, the erased data in the drive could not be recovered.

TC-1c: Data erasing from the USB drive by the stellar Bitraser tool for the ext3 file systems

Test Objective: Whether the data erased in the **USB drive** by the stellar Bitraser tool cannot be recovered for the **ext3 file systems**:

Scenario:

The figure TC-1c-1 shows the available file system in the test drive (USB).For the testing purpose some test files are loaded in USB drive device as depicted in the Figure TC-1c -2. The files on the USB drive are erased using the "NIST Clear" algorithm of the "BitRaser V1.2". After erasing of the data files, attempt was made to recover the data files using data recovery tools, as indicated in section 5.2.

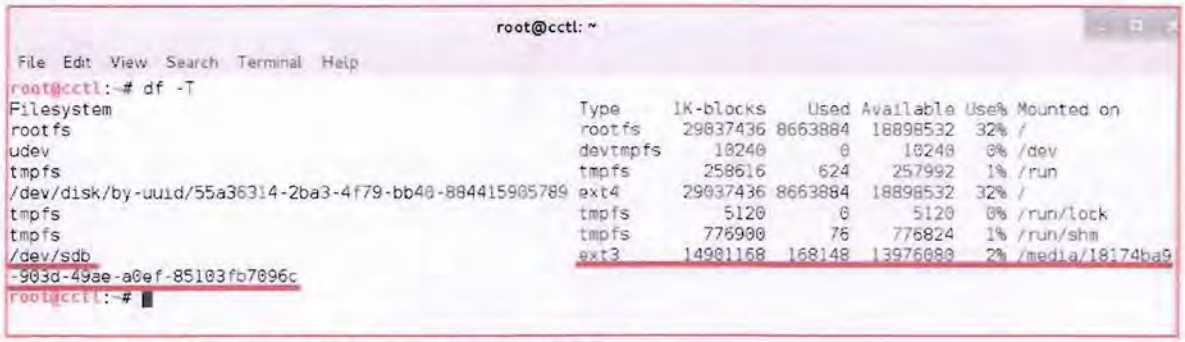

Figure TC-1c -1: Showing ext3 file system in the USB drive.

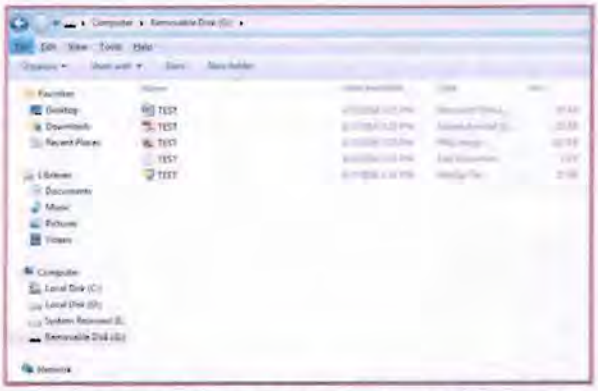

Figure TC-1c -2: Showing Files in the USB drive with **ext3** file system before erase.

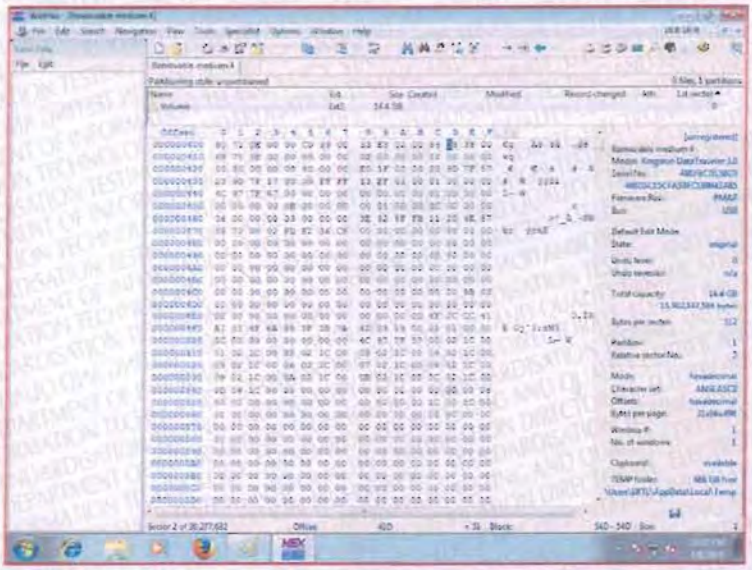

Figure TC-1c - 3: Data showing by WinHex tool before the erased data in the drive.

Expected Results: The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Results:

Figure TC-1b -3a Stellar BitRaser Setup screen

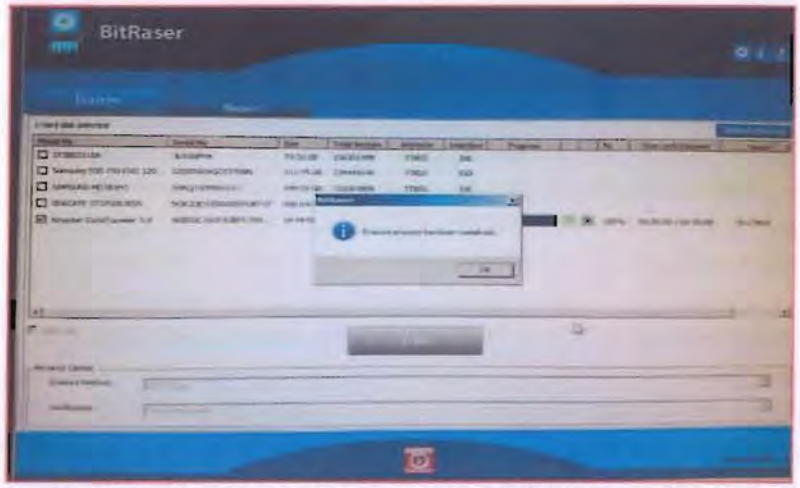

Figure TC-1c -3b: showing data erased in the USB drive by the stellar Bitraser tool.

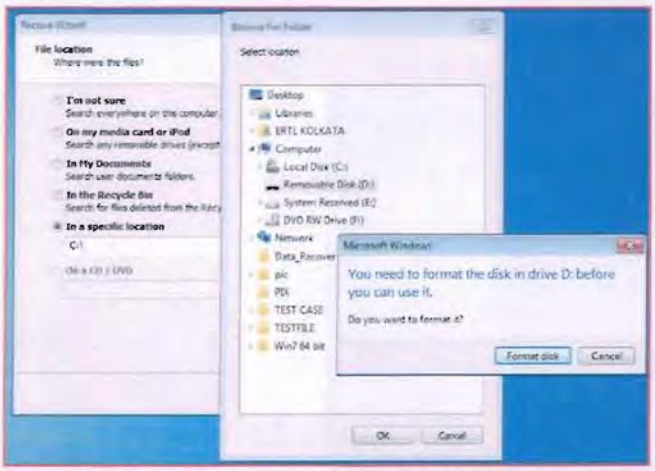

Figure TC-1c -3c. Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

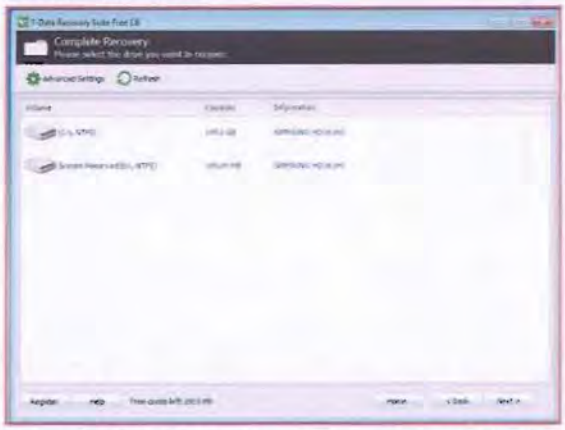

Figure TC-1c -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

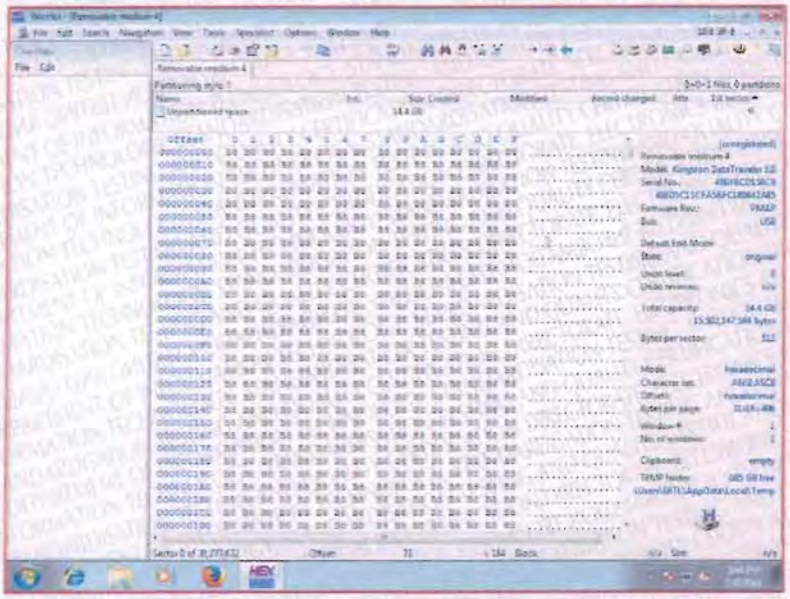

Figure TC-1c -3e: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

TC-1d: Data erasing from the USB drive by the stellar Bitraser tool for the ext4 file systems

Test Objective: Whether the data erased in the **USB drive** by the stellar Bitraser tool cannot be recovered for the **ext4 file systems**:

Scenario:

The figure TC-1d-1 shows the available file system in the test drive (USB).For the testing purpose some test files are loaded in USB drive device as depicted in the Figure TC-1d -2. The files on the USB drive are erased using the "NIST Clear" algorithm of the "BitRaser V1.2". After erasing of the data files, attempt was made to recover the data files using data recovery tools, as indicated in section 5.2.

```
root@cctl:~# df -T
Filesystem                                              Type     1K-blocks    Used Available Use% Mounted on
rootfs                                                  rootfs    29037436 8664076  18898340  32% /
udev                                                    devtmpfs     10240       0     10240   0% /dev
tmpfs                                                   tmpfs       258616     624    257992   1% /run
/dev/disk/by-uuid/55a36314-2ba3-4f79-bb40-884415905789 ext4      29037436 8664076  18898340  32% /
tmpfs                                                   tmpfs         5120       0      5120   0% /run/lock
tmpfs                                                   tmpfs       776900     224    776676   1% /run/shm
/dev/sdb                                                ext4      14901168  168016  13976212   2% /media/73206c8e
-db72-4dc4-abb0-86879c89b2c0
root@cctl:~#
```

Figure TC-1d- 1: Showing ext4 file system in the USB drive.

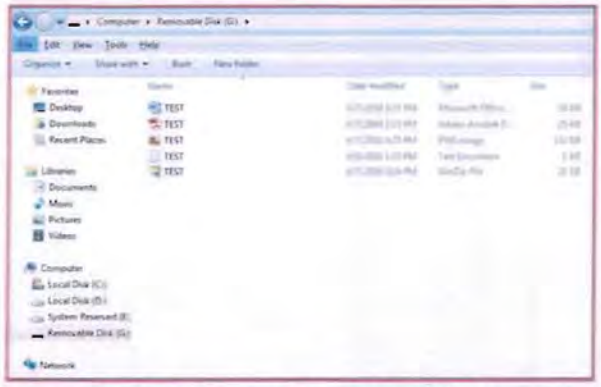

Figure TC-1d- 2: Showing Files in the USB drive with **ext4** file system before erase.

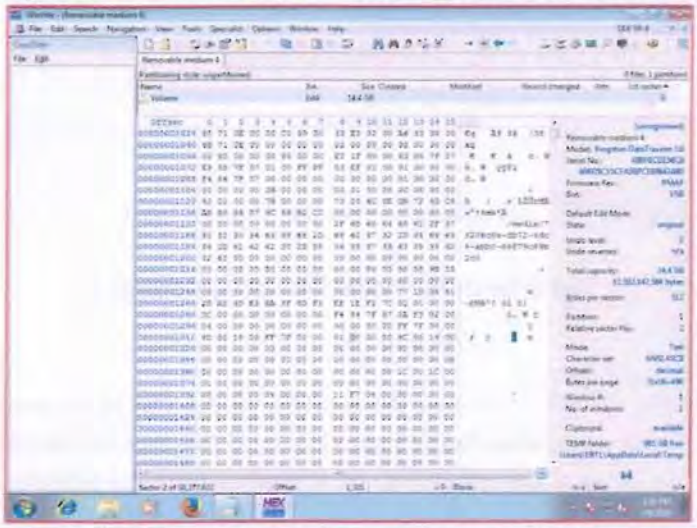

Figure TC-1d -2a: Data showing by WinHex tool before the erasing data from the drive.

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Results:

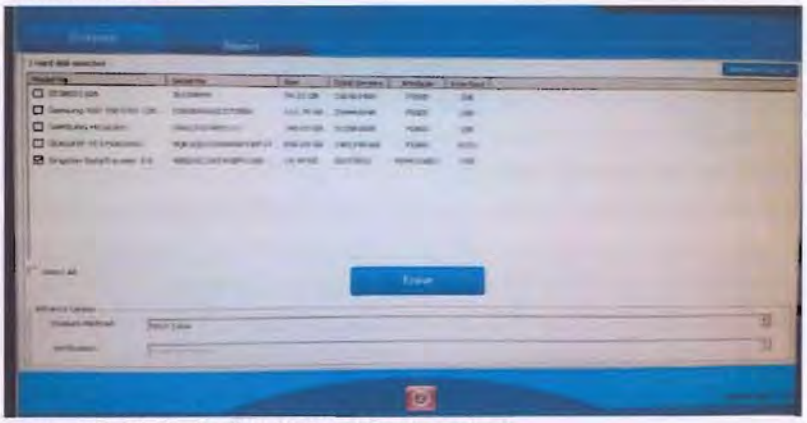

Figure TC-1d -3a Stellar BitRaser Setup screen

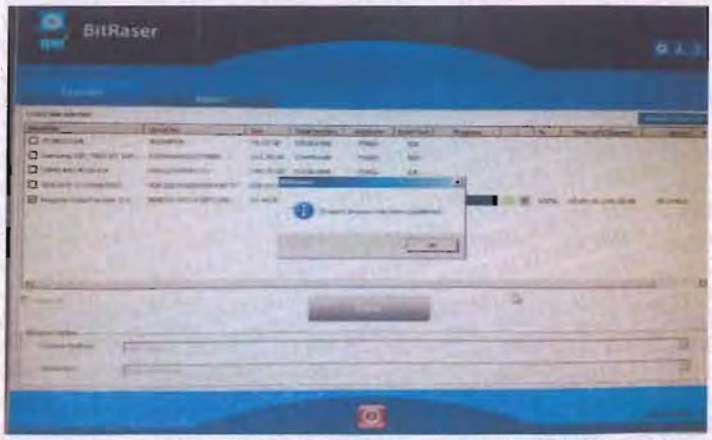

Figure TC-1d -3b: showing data erased in the USB drive by the stellar Bitraser tool.

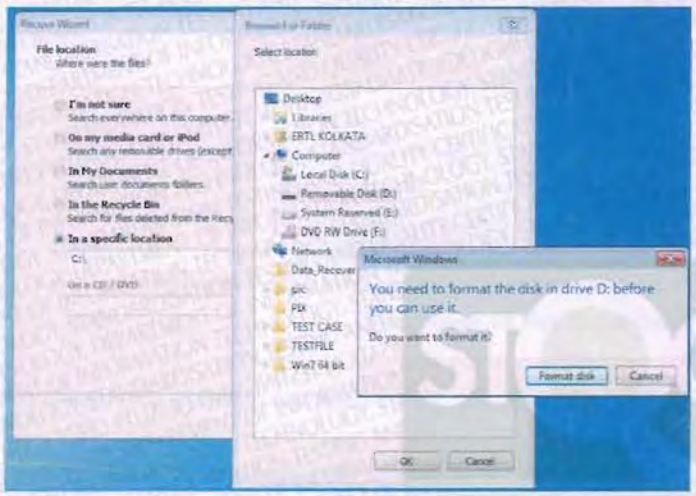

Figure TC-1d -3c: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

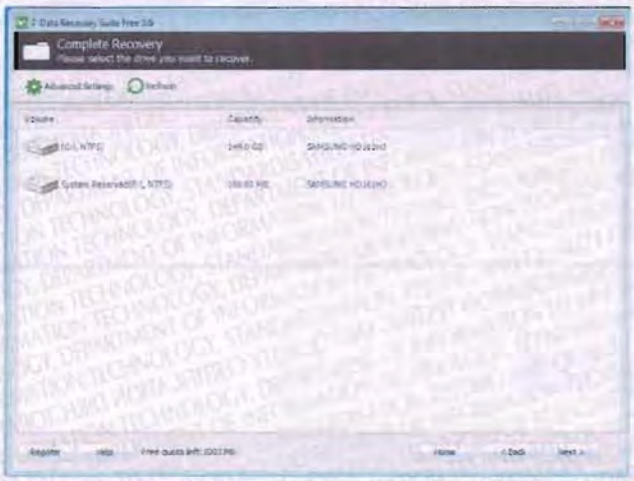

Figure TC-1d -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected.

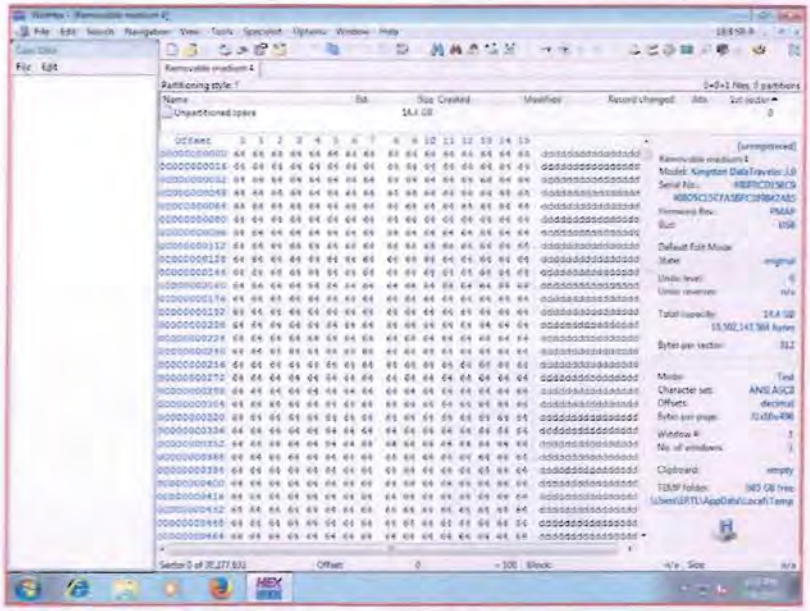

Figure TC-1d -3e: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

TC-1e: Data erasing process from the USB drive by the stellar Bitraser tool is disrupted for the NTFS file systems

Test Objective: If the data erasing process is disrupted ,whether the data erased in the USB drive by the stellar Bitraser tool cannot be recovered for the NTFS file systems:

Scenario:

The figure TC-1e-1 shows the available file system in the test drive (USB).For the testing purpose some test files are loaded in USB drive device as depicted in the Figure TC-1e -2. The files on the USB drive are started erasing using the "NIST Clear" algorithm of the "BitRaser V1.2". The data erasing process is now disrupted. After partial erasing of the data files of the drive, attempt was made to recover the data files using tools as mentioned in section 5.2.

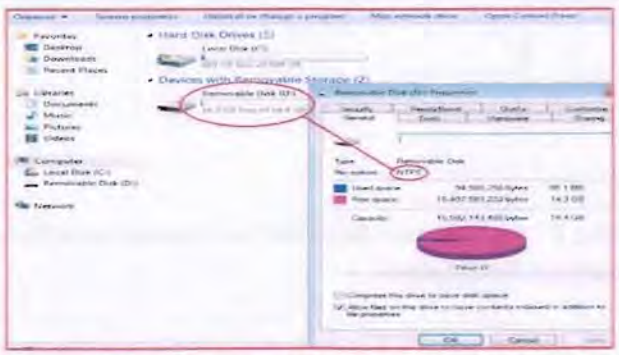

Figure TC-1e-1: Showing NTFS file system in the USB drive.

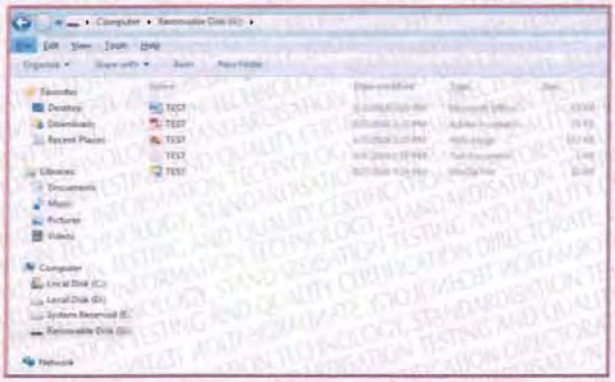

Figure TC-1e 2: Showing Files in the USB drive with NTFS file system before erase.

Figure TC-1e 2a: Disruption of erasing process of USB drive with NTFS file system

Figure TC-1e -3d. Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

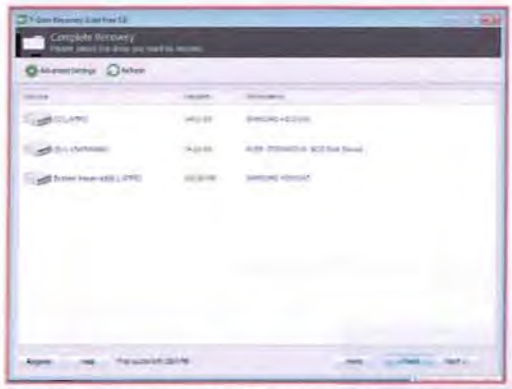

Figure TC-1e 3e. Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

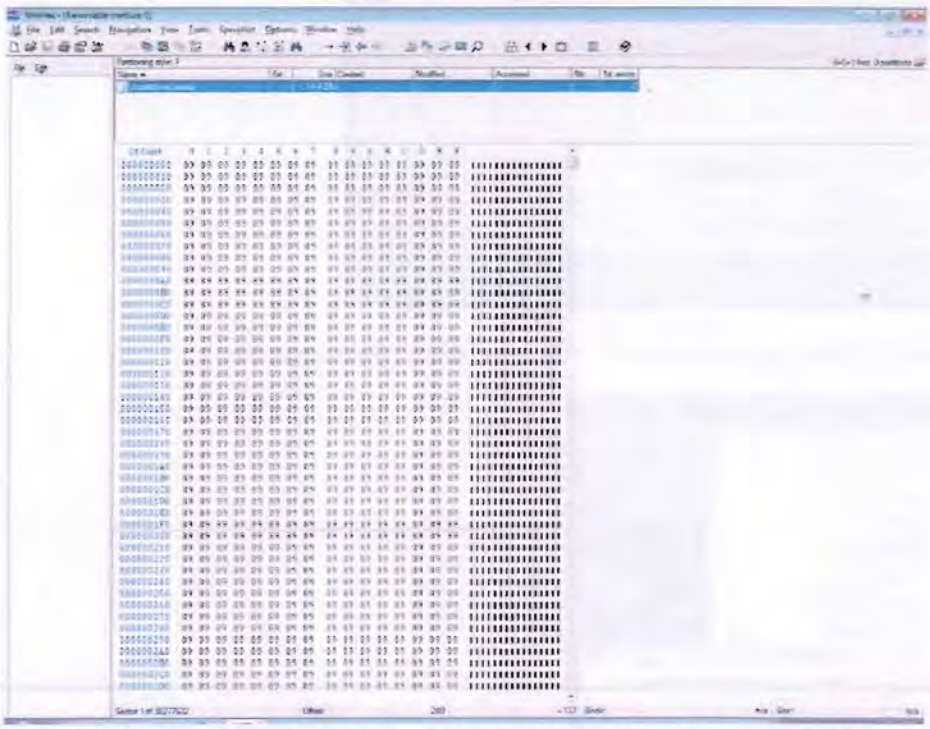

Figure TC-1e -3e: WinHex tool did not show any data of the files in the initialization sector

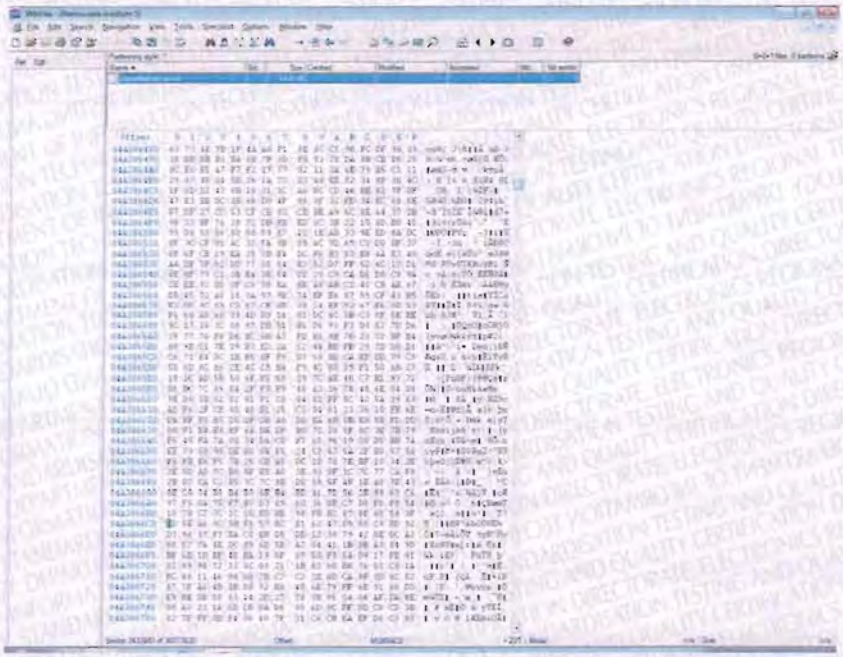

Figure TC-1e -3f: WinHex tool shows some data of the files of the drive

Remarks: Pass, the data from the drive could not be recovered after disrupting the erasing process

Annexure-II
Test cases related to PATA drive

TC-2a: Data erasing in the PATA drive by the stellar Bitraser tool for the NTFS file systems

Test Objective: Whether the data erased in the **PATA drive** by the stellar Bitraser tool cannot be recovered for the **NTFS file systems**:

Scenario:

Test files are loaded on PATA storage device as depicted in the Figure TC-2a -2. The files on the PATA drive are erased using the "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was made to recover the data files using tools, listed in section 5.2.

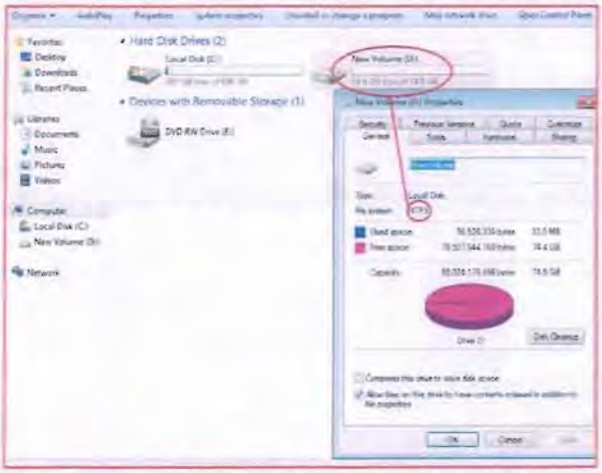

Figure TC-2a -1: Showing NTFS file system in the PATA drive.

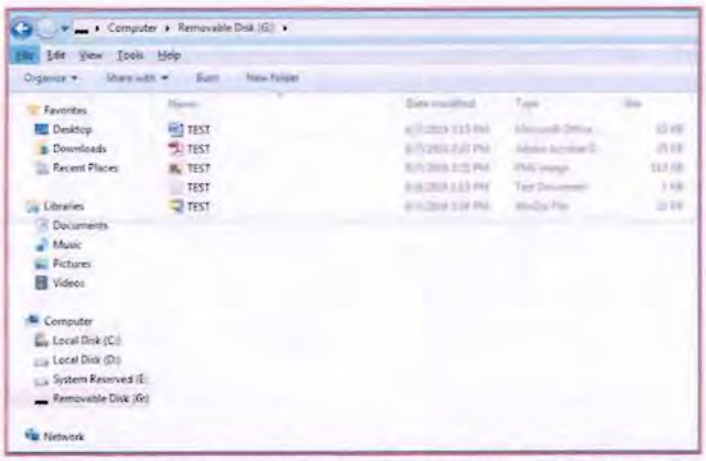

Figure TC-2a -2: Showing Files in the PATA drive with NTFS file system before erase.

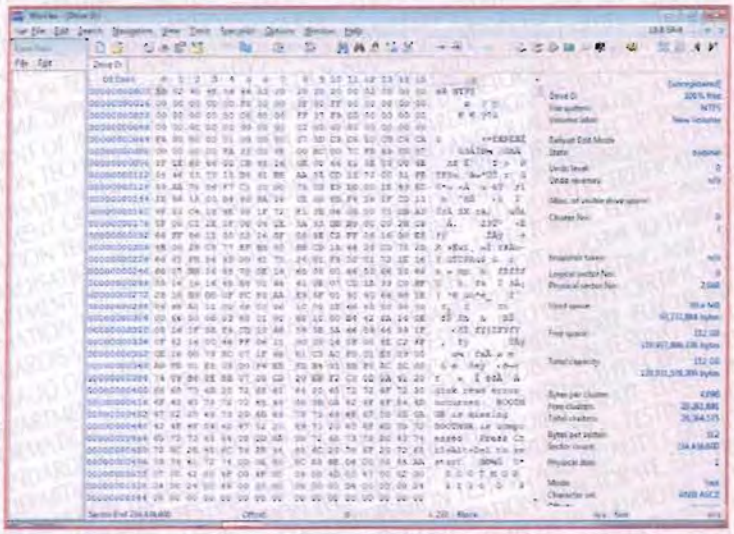

Figure TC-2a 2a: Data showing by WinHex tool before the erased data in the drive.

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Results:

Figure TC-2a -3a: Stellar BitRaser Setup screen

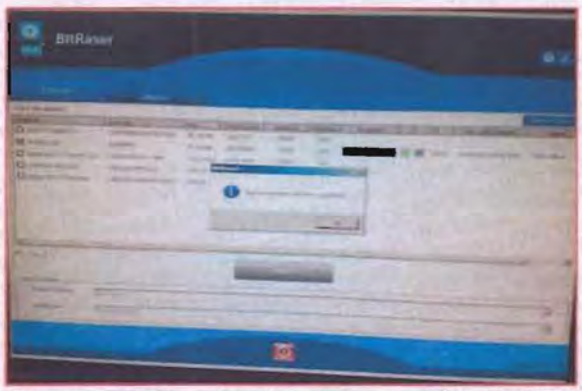

Figure TC-2a -3a: showing data erased in the PATA drive by the stellar Bitraser tool.

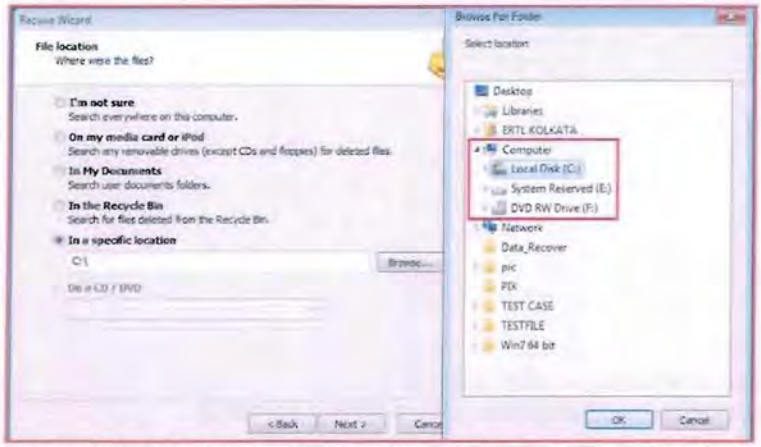

Figure TC-2a -3c: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered (The drive could not be detected) .

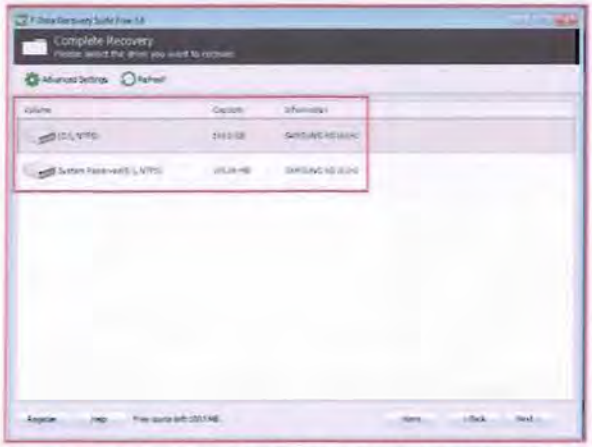

Figure TC-2a -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

Figure TC-2a -3e: The PATA Drive, after erasing, shows not initialized

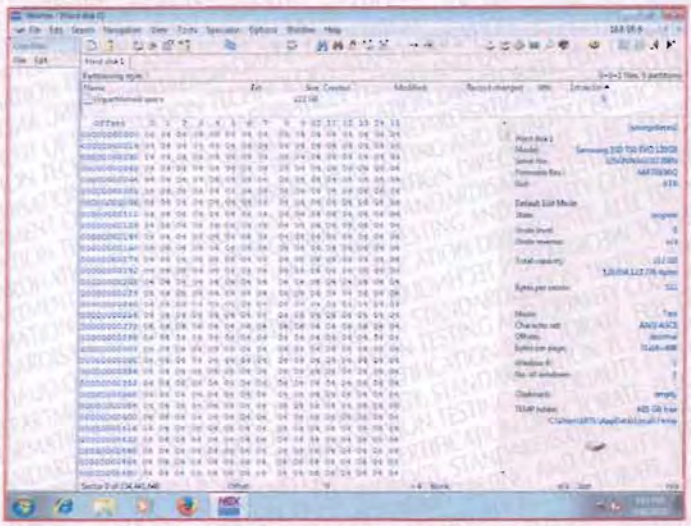

Figure TC-2a -3f: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

TC-2b: Data erasing in the PATA drive by the stellar Bitraser tool for the FAT file systems

Test Objective: Whether the data erased in the **PATA drive** by the stellar Bitraser tool cannot be recovered for the **FAT file systems**:

Scenario:

Test files are loaded in PATA drive device as depicted in the Figure TC-2b -1. The files on the PATA drive are erased using the "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files, attempt was made to recover the data files using tools, as listed in section 5.2.

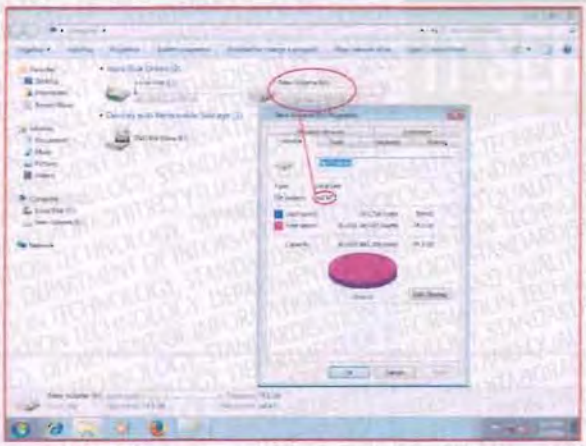

Figure TC-2b -1: Showing FAT files system in the PATA drive.

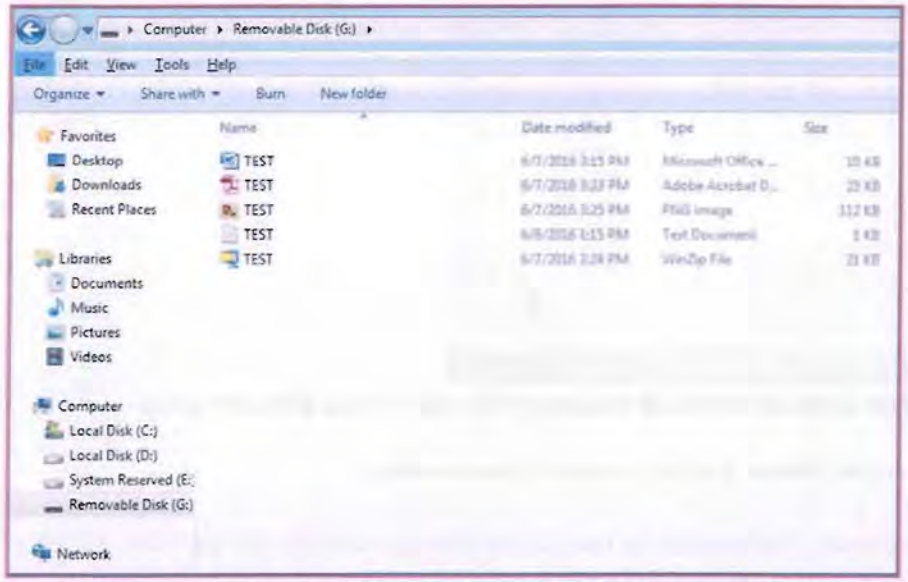

Figure TC-2b -2: Showing Files in the PATA drive with FAT file system before erase.

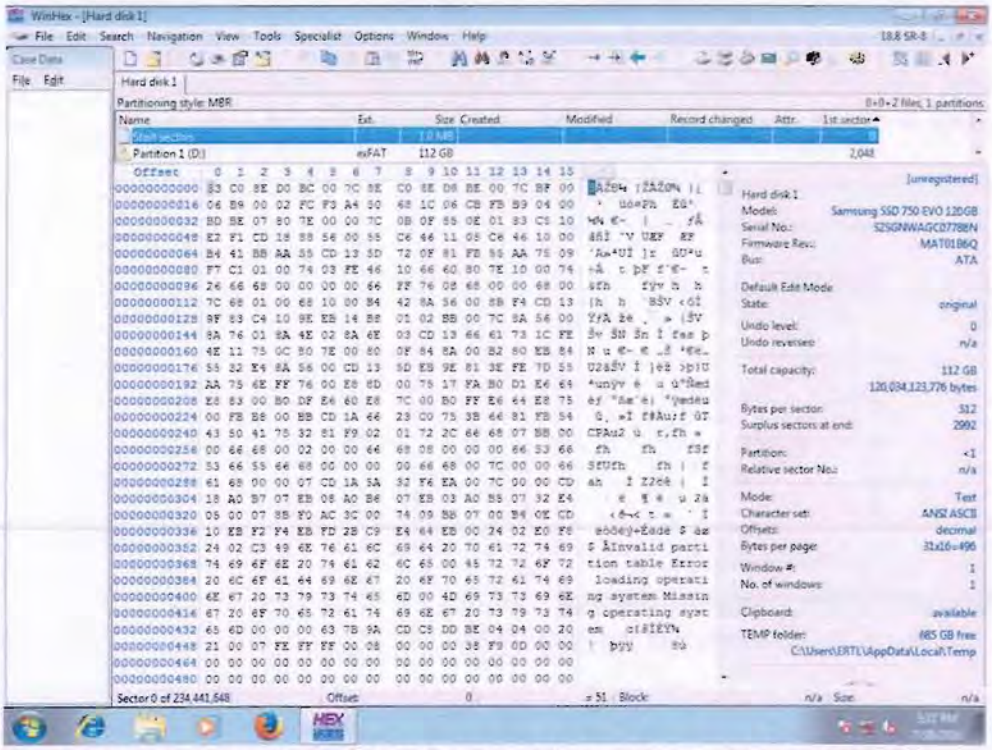

Figure TC-2b -2a: Data showing by WinHex tool before the erased data in the drive

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

Figure TC-2b -3a: Stellar BitRaser Setup screen

Figure TC-2b -3b: showing data erased in the PATA drive by the stellar Bitraser tool.

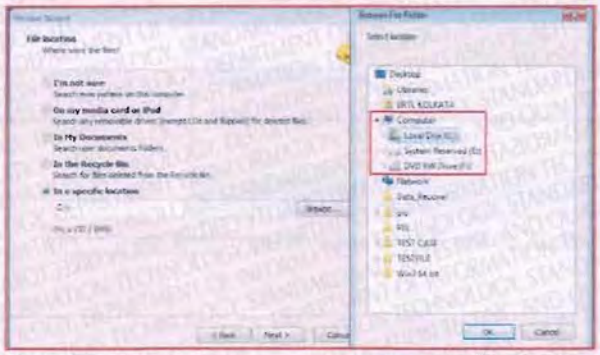

Figure TC-2b -3c: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered (The drive could not be detected).

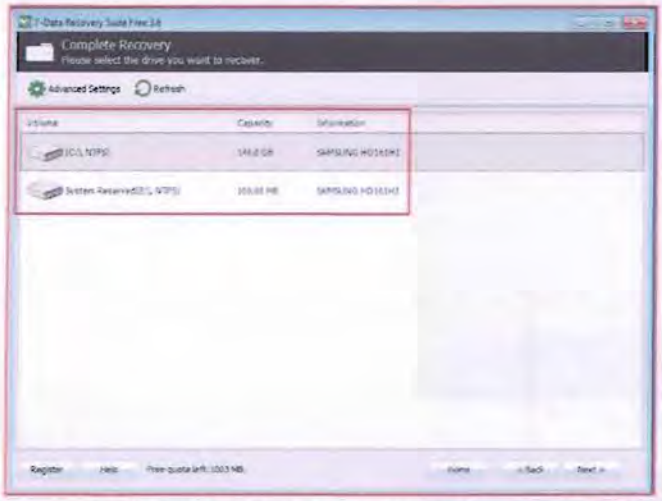

Figure TC-2b -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

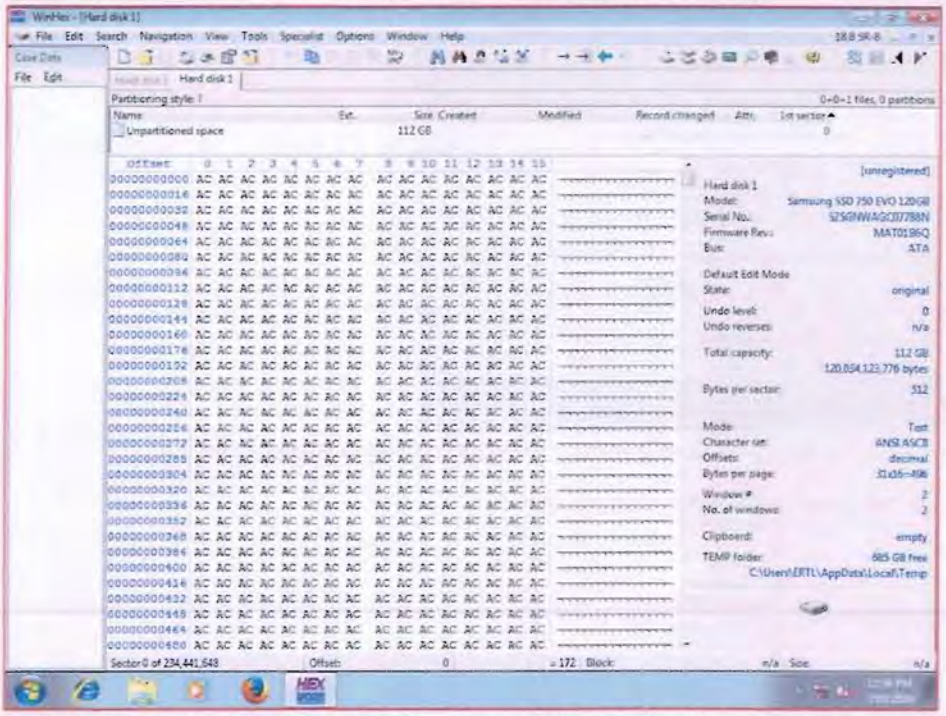

Figure TC-2b -3e: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

Annexure-III
Test cases related to SATA drive

TC-3a: Data erasing in the SATA drive by the stellar Bitraser tool for the NTFS file systems

Test Objective: Whether the data erased in the **SATA drive** by the stellar Bitraser tool cannot be recovered for the **NTFS file systems**:

Scenario:

Test files are loaded on SATA storage device as depicted in the Figure TC-3a -2. The files containing in the SATA storage drive are erased using the "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was made to recover the data files using tools, listed in section 5.2.

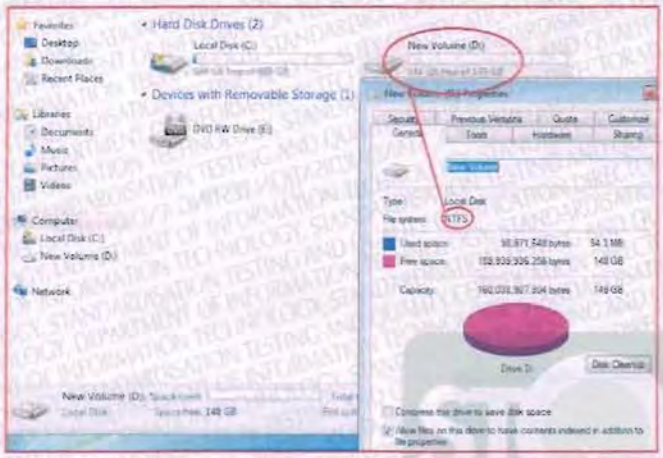

Figure TC-3a -1: Showing NTFS file system in the SATA drive.

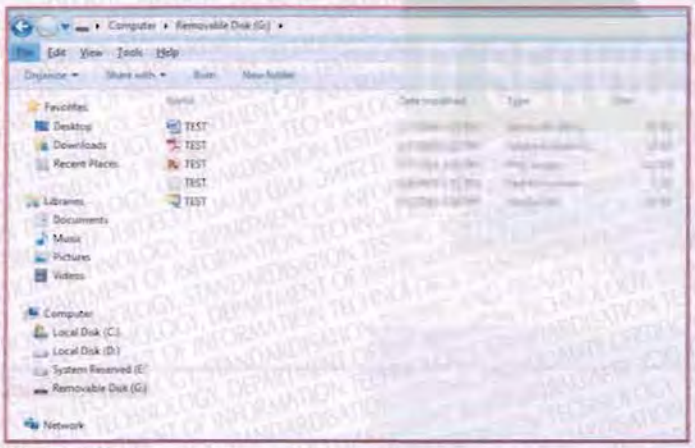

Figure TC-3a -2: Showing Files in the SATA drive with NTFS file system before erase.

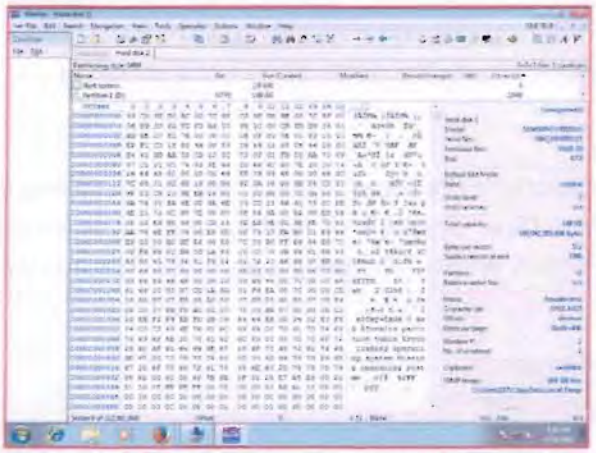

Figure TC-3a 2a: Data showing by WinHex tool before the erased data in the drive

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

Figure TC-3a -3a: Stellar BitRaser Setup screen

Figure TC-3a -3b: showing data erased in the SATA drive by the stellar Bitraser tool.

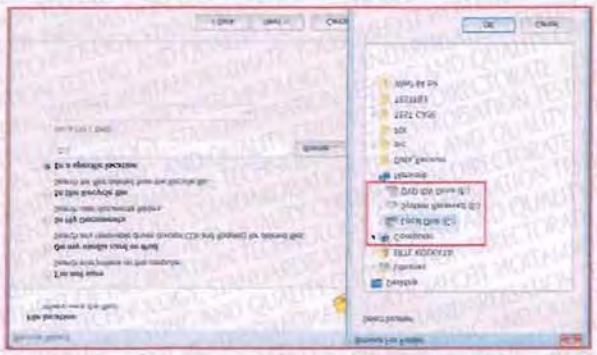

Figure TC-3a -3c. Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered (The drive could not be detected).

Figure TC-3a -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

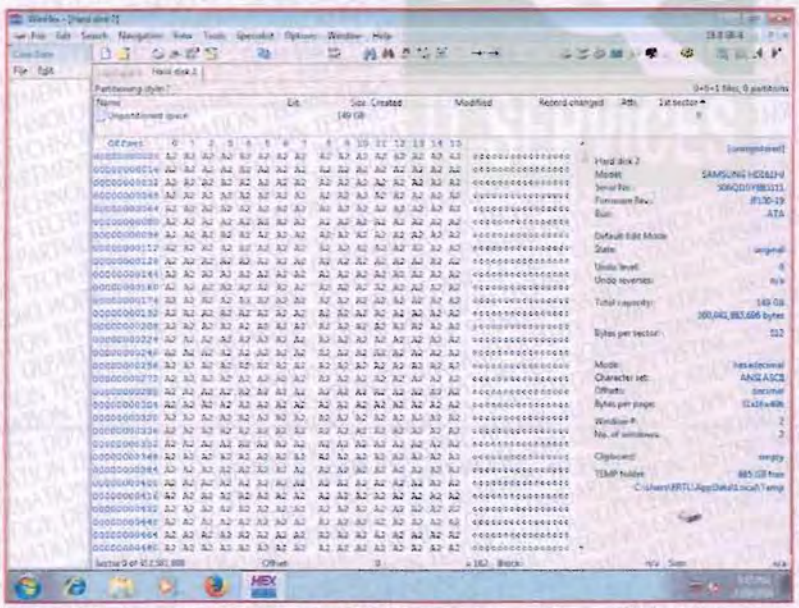

Figure TC-3a -3d: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

TC-3b: Data erased in the SATA drive by the stellar Bitraser tool for the FAT file systems

Test Objective: Whether the data erased in the **SATA drive** by the stellar Bitraser tool cannot be recovered for the **FAT file systems**:

Scenario:

Test files are loaded in SATA storage device as depicted in the Figure TC-3b -1. The files containing in the SATA storage drive are erased using the "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was made to recover the data files using tools, listed in section 5.2.

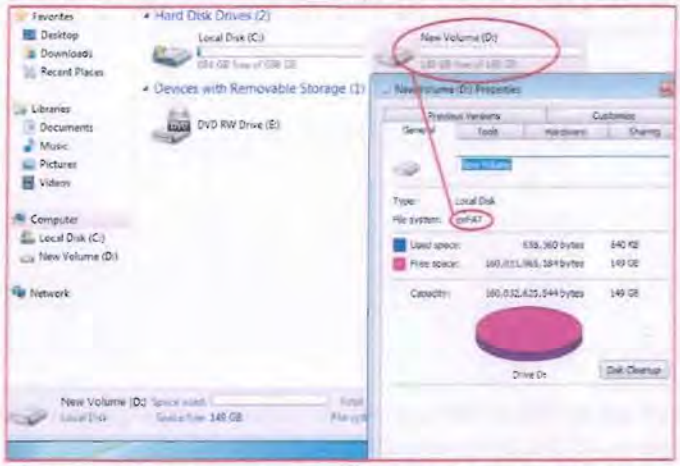

Figure TC-3b -1: Showing FAT file system in the SATA drive.

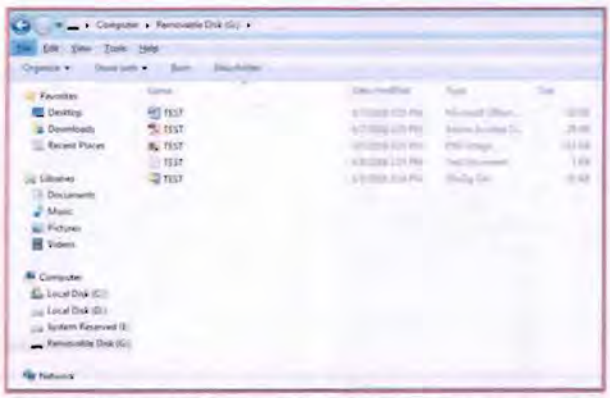

Figure TC-3b- 2: Showing Files in the SATA drive with FAT file system before erase.

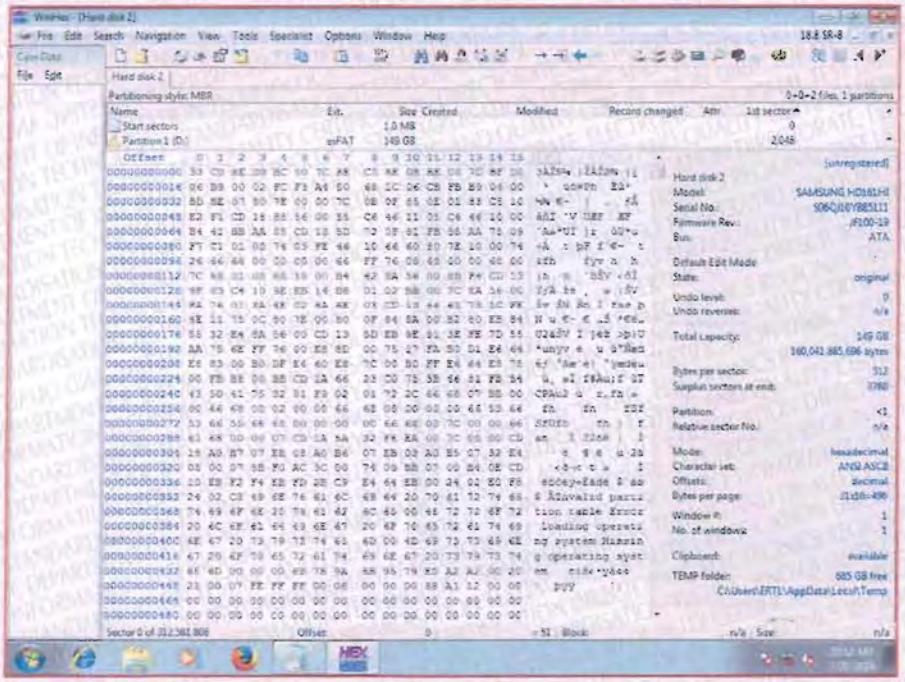

Figure TC-3b 2a: Data showing by WinHex tool before the erased data in the drive

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

Figure TC-3b -3a: Stellar BitRaser Setup screen

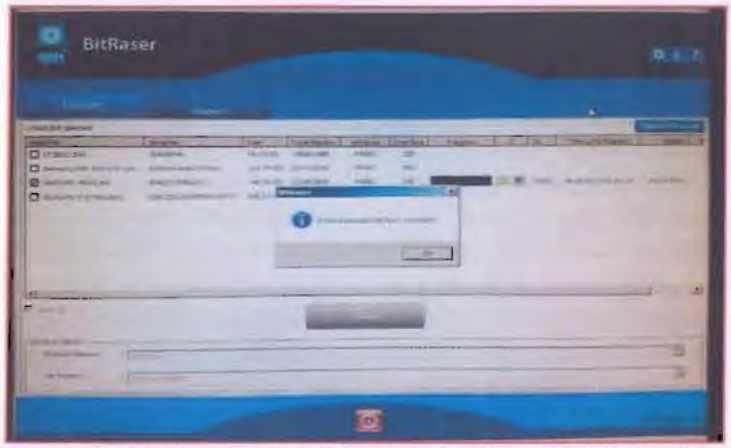

Figure TC-3b -3b: showing data erased in the SATA drive by the stellar Bitraser tool.

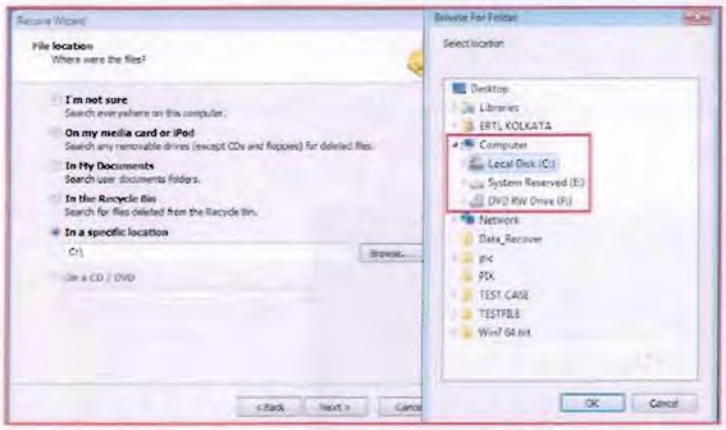

Figure TC-3b -3c: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered (The drive could not be detected).

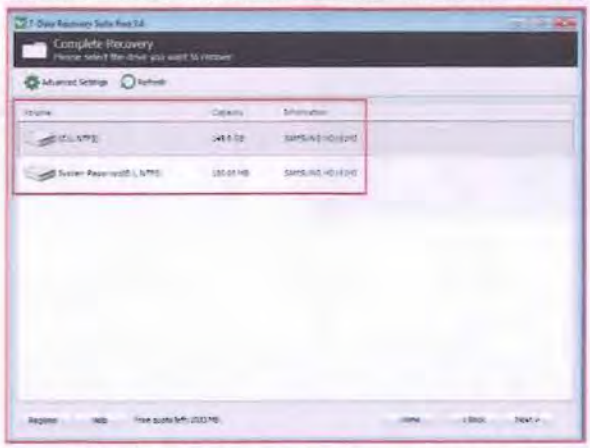

Figure TC-3b -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

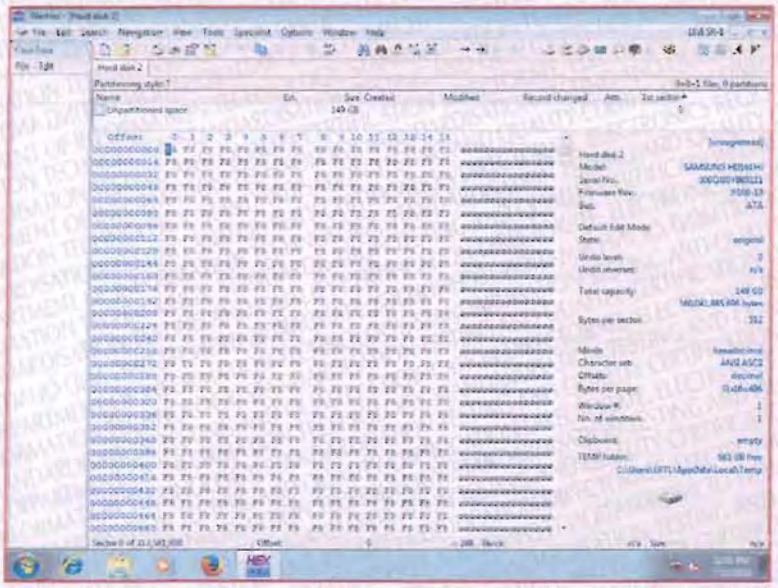

Figure TC-3b -3e: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

Annexure-IV
Test cases related to SSD drive

TC-4a: Whether the data erased in the SSD drive by the stellar Bitraser tool cannot be recovered

Test Objective: Whether the data erased in the **SSD drive** by the stellar Bitraser tool cannot be recovered for the **NTFS file systems**:

Scenario:

Test files are loaded in SSD storage device as depicted in the Figure TC-4a -1. The data files on the SSD storage drive are erased using "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was made to recover the data files using tools, listed in section 5.2.

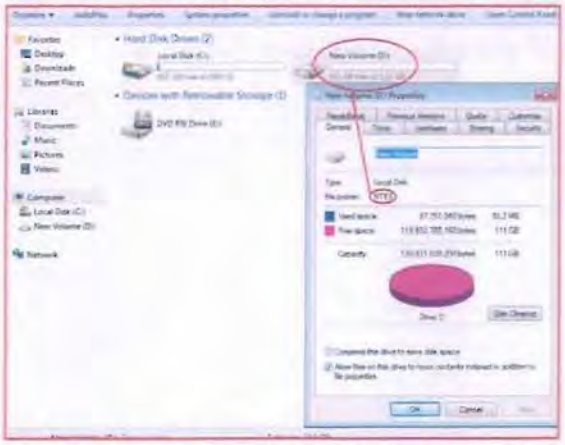

Figure TC-4a -1: Showing NTFS file system in the SSD drive.

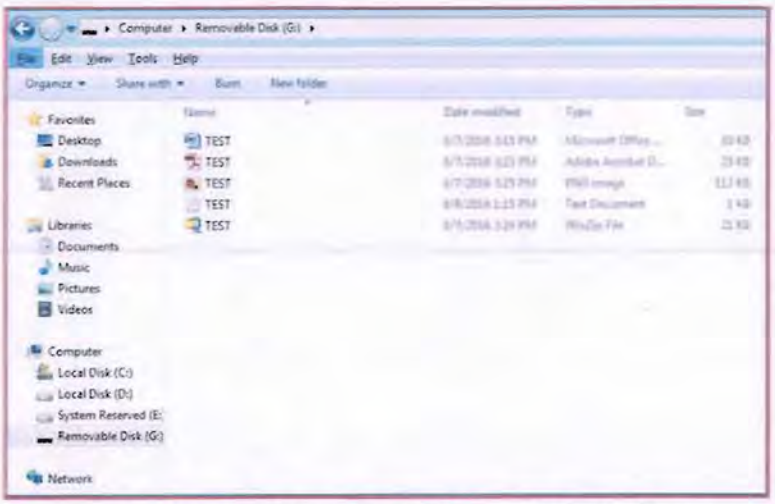

Figure TC-4a 2: Showing Files in the SSD drive with NTFS file system before erase.

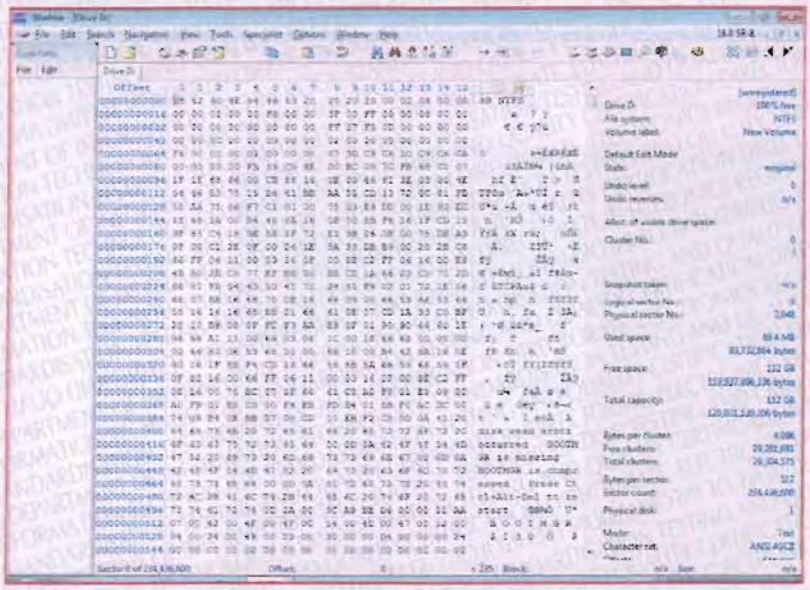

Figure TC-4a 2a: Data showing by WinHex tool before the erasing data on the drive .

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

Figure TC-4b -3a: Stellar BitRaser Setup screen

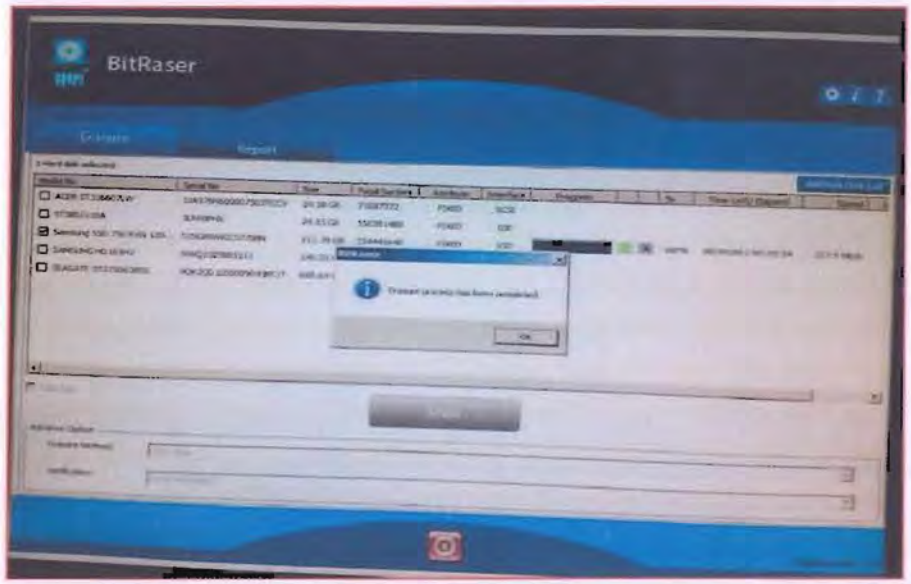

Figure TC-4b -3b: showing data erased in the SSD drive by the stellar Bitraser tool.

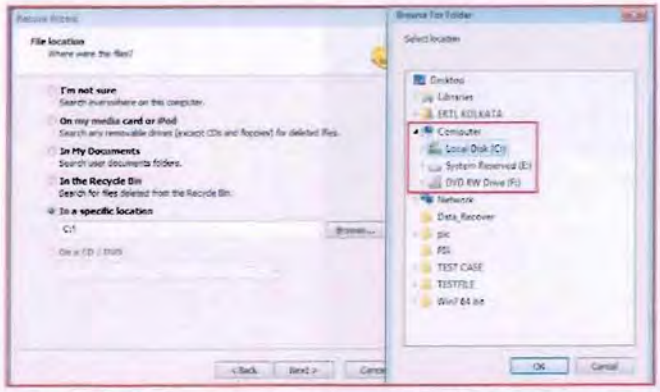

Figure TC-4b -3c . Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered (The drive could not be detected).

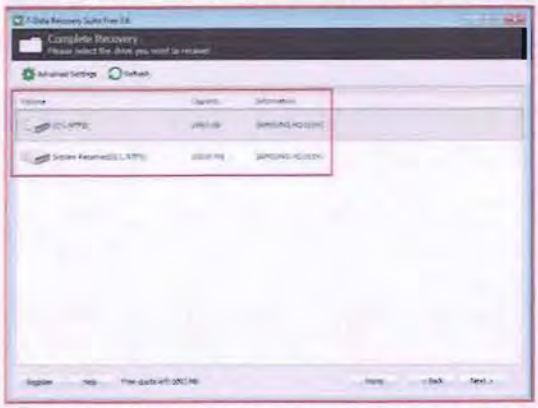

Figure TC-4b -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered (The drive could not be detected).

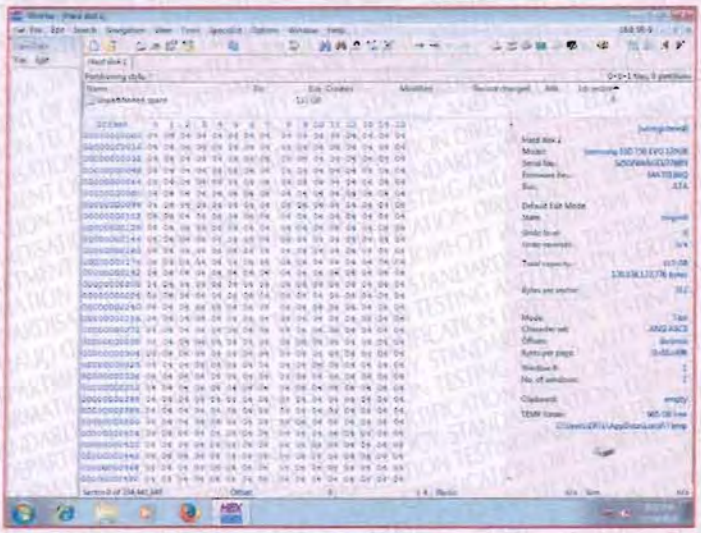

Figure TC-4b -3e : WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

TC-4b: Data erasing from the SSD drive by the stellar Bitraser tool for the FAT file systems

Test Objective: Whether the data erased in the **SSD drive** by the stellar Bitraser tool cannot be recovered for the **FAT file systems**:

Scenario:

Test files are loaded in SSD drive device as depicted in the Figure TC-4b-1. The files containing in the SSD drive is erased using the" NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was to recover the data files using tools.

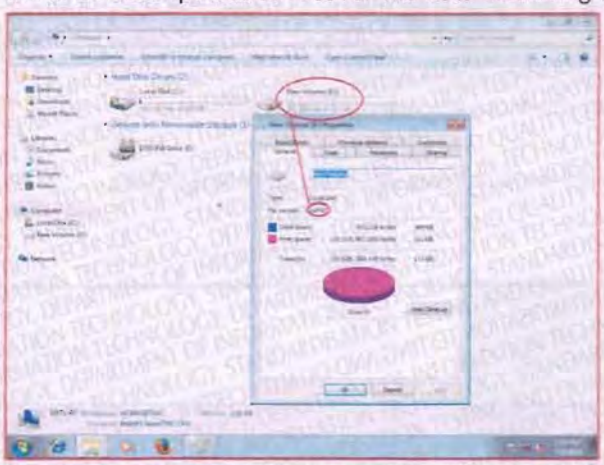

Figure TC-4b -1: Showing FAT files system in the SSD drive.

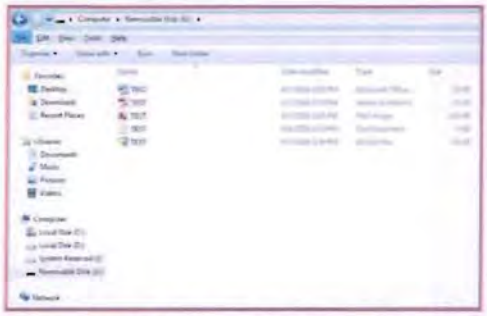

Figure TC-4b -2: Showing Files in the SSD drive with FAT file system before erase.

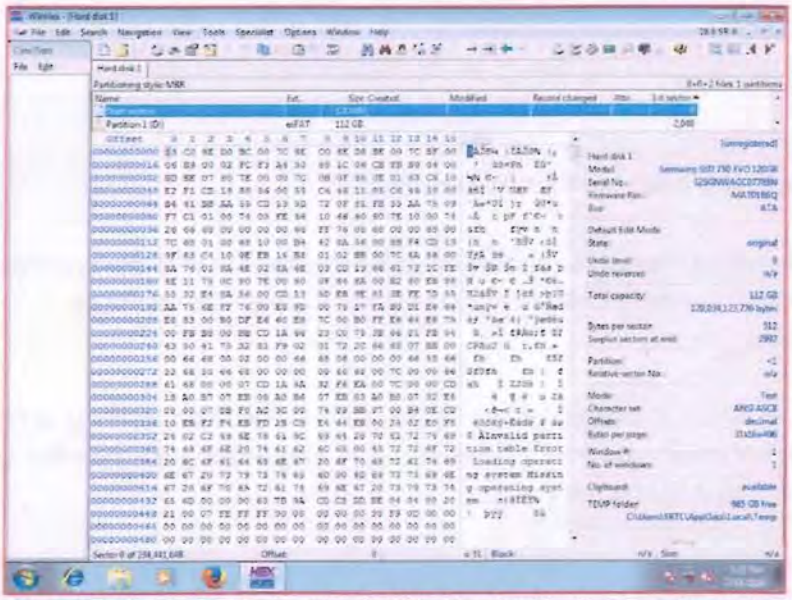

Figure TC-4b -2a: Data showing by WinHex tool before erasing data on the drive.

Expected Result:

The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

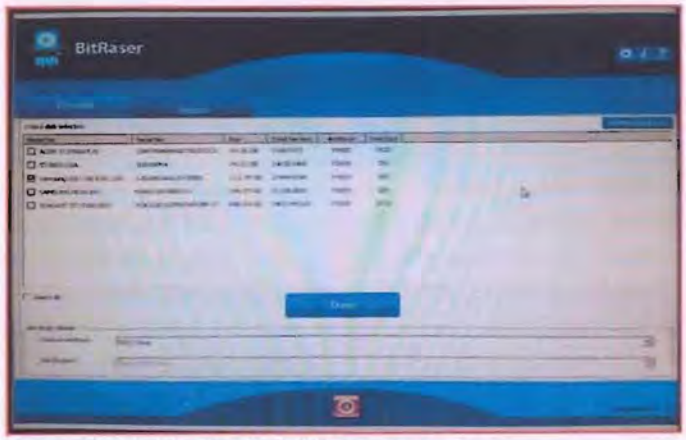

Figure TC-4b -3a: Stellar BitRaser Setup screen

Figure TC-4b -3b: showing data erased in the SSD drive by the stellar Bitraser tool.

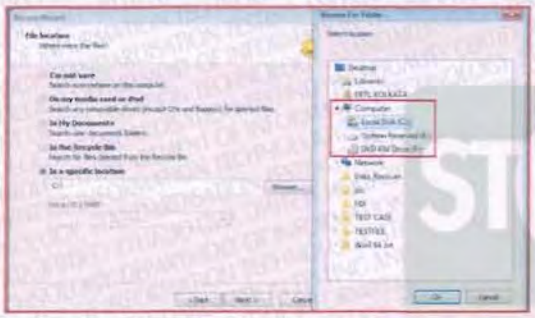

Figure TC-4b -3b: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

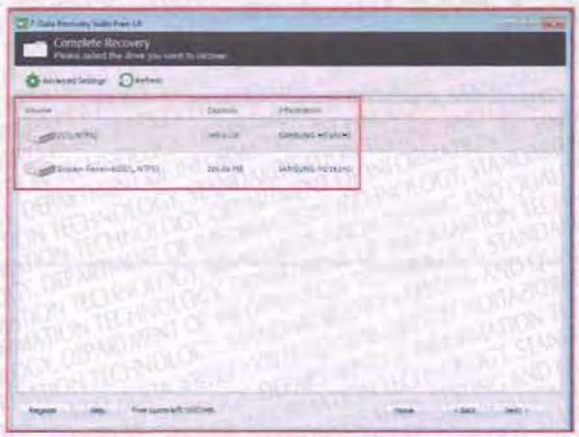

Figure TC-4b -3c: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered.

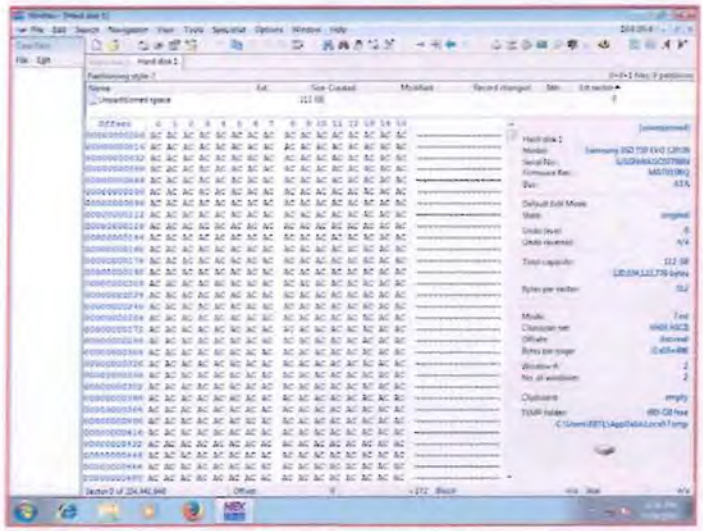

Figure TC-4b -3d: 6: WinHex tool did not show any data of the files erased data from drive

Remarks: Pass, the erased data in the drive could not be recovered.

Annexure-V
Test cases related to SCSI drive

TC-5a: Data erasing in the SCSI drive by the stellar Bitraser tool for the NTFS file systems

Test Objective: Whether the data erased in the **SCSI drive** by the stellar Bitraser tool cannot be recovered for the **NTFS file systems**:

Scenario:

Test files are loaded in SCSI storage device as depicted in the Figure TC-5a-1. The files containing in the SCSI storage device are erased using the "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was made to recover the data files using tools, as listed in section 5.2.

Figure TC-5a -1: Showing Files in the SCSI drive with NTFS file system before erase.

Expected Result: The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

Figure TC-5a -3a: Stellar BitRaser Setup screen

Figure TC-5a -3b : showing data erased in the SCSI drive by the stellar Bitraser tool.

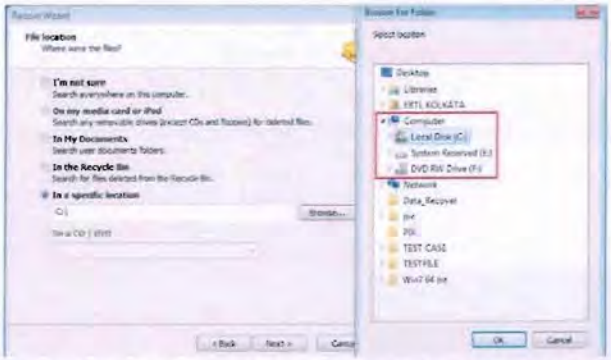

Figure TC-5a -3a : Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

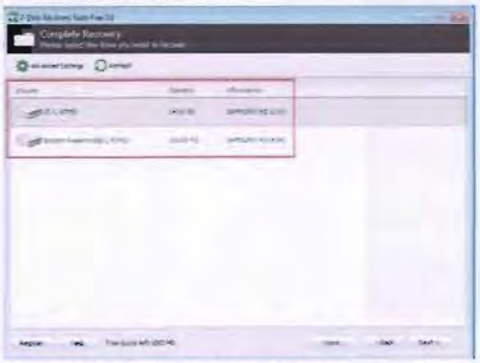

Figure TC-5a -3a : Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered.

Remarks: Pass, the erased data in the drive could not be recovered.

TC-5b: Data erasing from the SCSI drive by the stellar Bitraser tool for the FAT file systems

Test Objective: Whether the data erased in the **SCSI drive** by the stellar Bitraser tool cannot be recovered for the **FAT file systems**:

Scenario:

Test files are loaded in SCSI storage device as depicted in the Figure TC-5b-1. The files containing in the SCSI storage device is erased using the "NIST Clear" algorithm of "BitRaser V1.2". After erasing the data files of the drive attempt was to recover the data files using tools, as listed in section 5.2.

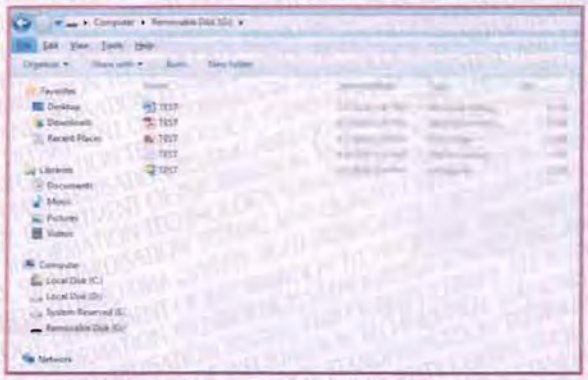

Figure TC-5b -1: Showing Files in the SCSI drive with FAT file system before erase.

Expected Result: The data erased in the drive shall not be recovered and the drive shall not show any Data.

Actual Result:

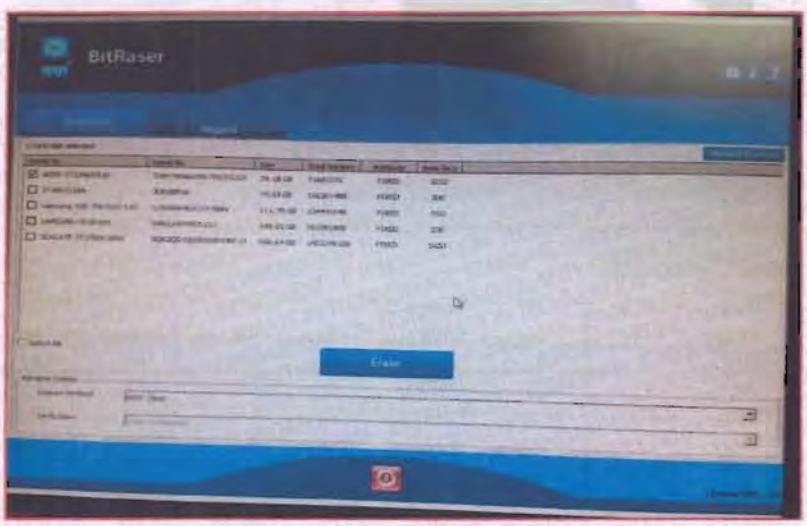

Figure TC-5b -3a: Stellar BitRaser Setup screen

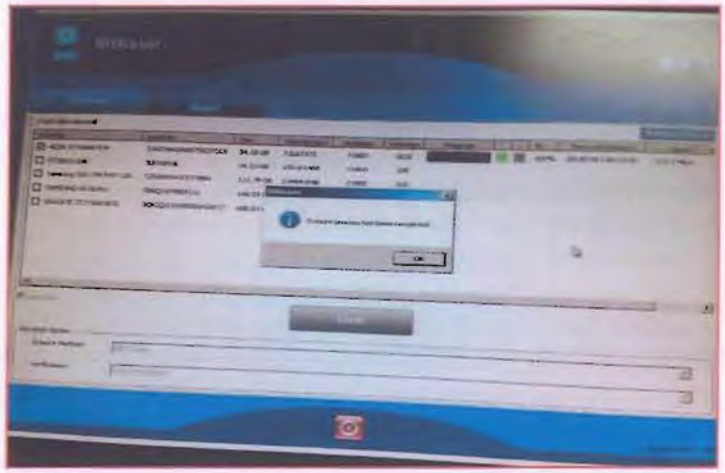

Figure TC-5b -3b : showing data erased in the SCSI drive by the stellar Bitraser tool.

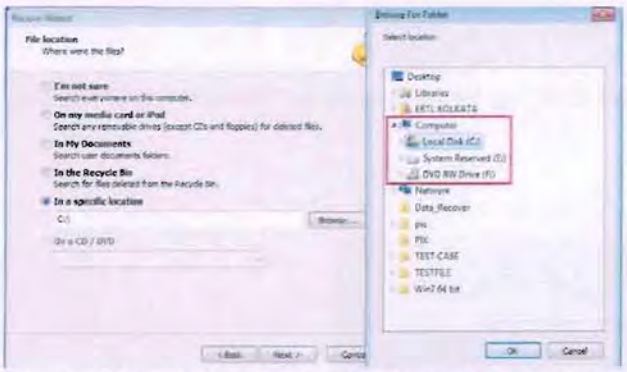

Figure TC-5b -3c: Data recovery attempted using Recuva tool but the erased data in the drive could not be recovered.

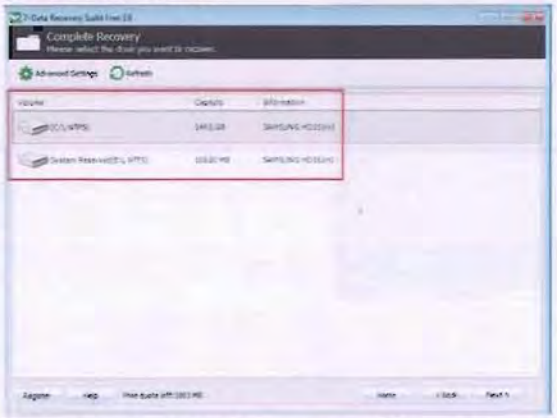

Figure TC-5b -3d: Data recovery attempted using 7-Data Recovery Suite tool but the erased data in the drive could not be recovered.

Remarks: Pass, the erased data in the drive could not be recovered.