Data is found on the drive after a successful erasure

Created date	Updated date	Affects version	Fix version
27 Jul 2018	15 Apr 2024		

Problem

In some occasions, a verification of a drive using Blancco Drive Verifier or via a hex/disk editor (for example the Blancco Drive Eraser Hex Viewer), after a successful erasure, shows that there are unexpected patterns on the drive. For example a non-zero pattern or random data. There can be several reasons for that.

Cause

1. Some erasure standards include aperiodic random or periodic/pseudo-random overwriting steps that write random data throughout the whole drive. Some standards include firmware based erasure steps and the execution and result of those steps depend purely on drive firmware. Some drives write a non-zero pattern or non-periodic (random) data during firmware-based erasure.
    - Check the used erasure standard from the erasure report.
    - See the list of erasure standards and the execution steps from the Drive Eraser user manual.
    - For example, Seagate ST1000LM035-1RK172 1TB SATA HDD is known to write a repeating '33 CC 55 AA' pattern with NIST 800-88 Purge standard. The erasure method calls a NIST specified firmware erasure command which triggers the special pattern. The execution of the firmware based erasure command is out of software's control and it depends on how the drive firmware works.

2. Check if the erasure process has written a Fingerprint onto the drive. The Fingerprint is a summary of the erasure report that is written in one of the sectors (sector 200 by default) of the drive.
    - To check if you had this feature on, you can load the image (used for the erasure) in Blancco Drive Eraser Configuration Tool and check if the setting in question is enabled or not.
    - By default, the Fingerprint is written on sector 200, and it contains following data separated by spaces and semicolons:
        - Blancco software license owner / customer name
        - Date & time of wipe finish (yyyy-mm-dd hh:mm)
        - Blancco software version
        - Hard drive serial number
        - Erasure status (Erased, Erased with exceptions or Not Erased)
        - Unique report ID
        - Digital signature
    - For more information about the Fingerprint*, see the Drive Eraser user manual.
    - It has been noticed only on a specific ATA SSD model (CT1000MX500SSD1) with a specific firmware revision (M3CR023). As part of the erasure, BDE executes a firmware-based erasure command on the drive that successfully zeroes it, ensuring that no data is left. The BDE verification following this erasure (that simply reads data) is also successful (because the drive is full of zeroes). However, after the first write attempt (e.g., with the Fingerprint information), the entire drive becomes filled with random data. Any subsequent verification fails, because random data is found on the drive. This behavior is extremely rare.

3. Check if the erasure process has written a Bootable Asset Report onto the drive. The Bootable Asset Report is a short asset report visible as a splash screen when the machine is rebooted.
    - The Bootable Asset Report information is typically written on sectors 0 and 2-53 or 2-130 of the drive, depending on the size of the report information.
        - Sector 0 (MBR) contains the partition table information and Blancco's "tool" to read the Asset Report image file when the computer starts.
        - Sectors 2-130 contain the image file for the Bootable Asset Report. This image file data typically looks "random".
    - To check if you had this feature on, you can either boot the machine/drive without any CD/USB/PXE (the Bootable Asset Report should be displayed) or load the image (used for the erasure) in Blancco Drive Eraser Configuration Tool and check if the setting in question is enabled or not
    - For more information about the Bootable Asset Report*, see the Drive Eraser user manual.

4. Check if the erasure process has formatted the erased drive. Blancco Drive Eraser can be configured to format a drive, after erasing it, with the exFAT, FAT32 or NTFS file systems. Formatting a drive leaves some data in some sectors, and this data can fail a subsequent verification.

5. In server environments, some RAID controllers write metadata onto the drive after the erasure has complete. This can also cause verification failures (more information in this article).

6. Check if the erasure has (or has not) erased the remapped sectors and/or the hidden areas of the drive. If these sectors have not been erased, some tools may find some data there.
    - Check the erasure report for more information.

7. Check if the erasure has been a full erasure or a partial one. Partial erasures are possible in case the software is configured to automatically preserve Windows recovery partitions or in case the user has erased individual drive partitions only. Check the erasure report for more information, a partial erasure is accompanied with a disclaimer.

8. Some 3rd party software used to audit erased drives (or attempt to recover data from them) can write data in it during its validation process, especially if such tools restore the file system (e.g. NTFS) of the drive (via formatting). If such tools are used for erasure validation or recovery, please be aware of the data that can be left.

Resolution

In case of 1. firmware based erasure command:

Workaround 1: Use an erasure standard doing normal overwriting, or make sure that the erasure standard writes a static pattern other than 0x00 in the end.

In case of 2. with Fingerprint:

Workaround 2: Disable the Fingerprint. This means that no write operation will be performed after the erasure, and the disk will remain in a zeroed state, passing verification by third-party tools.

If you are still unsure about the erasure result, please contact the Technical Support team. Make sure that you include, at least, the erasure report in XML format and detailed information description of the case (issue report is also helpful/necessary in many cases).

* Note: Whenever Blancco Drive Eraser writes this information, it does it on a drive that has been erased and that does not contain any data anymore. When data is written in a drive, it cannot be written in small amounts: the minimum amount that is written is a sector of the drive (usually 512 or 4096 bytes). Then, the drive (especially SSDs) can put this information within a page (usually 16KB or 64KB in size i.e. several sectors) which is the one written in the end. So, when Blancco Drive Eraser writes a Bootable Asset Report or a Fingerprint in a drive, many adjacent sectors can also be written during the operation: internally, the drive has to fill those sectors with something (e.g. the pattern 0xB5). Therefore it should not be a surprise if some sectors contiguous to the Bootable Asset Report or a Fingerprint sector(s) contain some unexpected patterns (patterns that depend entirely on the drive controller). In order to check how the drive behaves, run a Blancco Drive Eraser erasure with the Bootable Asset Report or the Fingerprint enabled and check the patterns of the adjacent sectors. Then, run a new erasure with the Bootable Asset Report and the Fingerprint disabled: those adjacent sectors should contain this time the patterns corresponding to your chosen erasure standard.