F20FO Lab 2

Digital Forensic Foundations

Chandrashekhar R (cr2007)

Contents

Lab 2.3: Software write blocker

What does a system restore point do?

A system restore point is a backup copy of important Windows OS files and systems used to recover the system to an earlier point of time in the event of system failure. It creates a snapshot of the current working state of the computer and saves it as a "restore point" when any significant system changes are detected.

Lab 2.4: FTK Imager

Acquiring Evidence

What is a chain of custody?

It is a process documenting how (here) digital evidence is processed and a log of the steps taken from the time it is obtained till it is presented in court. It is well-documented to ensure that one can follow the exact same steps and obtain the same results.

A chain of custody documentation contains details such as Case Number, Name, Investigation details, Packaging Information, etc.

Logical Acquisition

1. How can we guarantee that evidence has not been modified?

One can guarantee that evidence has not been modified using a **write-blocker**. A **write-blocker** restricts any write operations to a hard disk, allowing read-only access to the storage device and maintaining data integrity. Write-blockers can be a hardware or software tool.

When used properly, write-blockers can guarantee the preservation of the evidence.

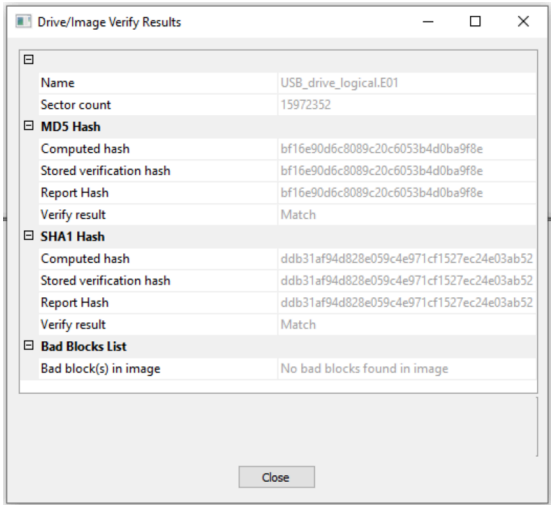

Figure 1: The result of the Logical Acquisition of a file

What is MD5 and SHA1, and why are they important?

MD5 (**M**essage **D**igest 5) and SHA-1 (**S**ecure **H**ashing **A**lgorithm) are two different types of hash functions that create a unique, fixed length output for each input. They are important as they help to verify the integrity of the data by comparing the output with the expected fingerprint, checking whether the data has been altered during transmission.

---

2. What is meant by a physical acquisition? How is it different from logical acquisition?

A **physical acquisition** is the process of creating a bit-for-bit copy of the original storage device to perform forensic analysis. It is different from a logical acquisition, which involves capturing only the active files and folders on the device. A physical acquisition captures the most amount of data possible from the device, but also requires more time, space, and processing power. Physical Acquisitions are preferred in high-stakes investigations like criminal cases, where the integrity of the evidence is of high priority.

---

3. Create a physical acquisition of the USB drive you used and upload a screenshot of the 'Drive/Image Verify Results'

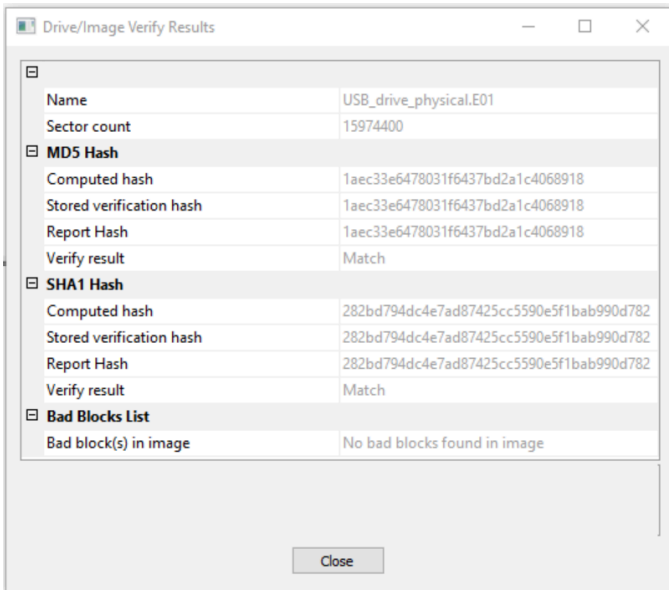

Figure 2: Results of the Physical Acquisition of the file

What is an SID folder?

A **S**ecurity **ID**entifier folder is a folder that contains unique identifiers for a user account or a group in Windows. Windows OS creates a new folder with the user's SID as the name and stores the user's data and settings there.

---

4. How is the SID folder used by Microsoft operating systems?

The SID folder is used to store the data and settings of a user account or a group that has a unique security identifier (SID) in Windows. The SID folder is also found in the Recycler folder (Recycle Bin) where it contains the deleted files of any user/group. It can reveal the owner and the contents of the deleted files too.

---

5. What did you find out about SID folders with names ending with a number like this (1004)?

The number '1004' is the relative identifier (RID) for SID folders of the user account/group that was manually created (i.e. not included in Windows default).

It is a unique number assigned to each account or group.[1]

---

6. What does a SID folder with a name ending in 500 indicate?

A SID folder with a name ending in '500' indicates that it belongs to the **Administrator** account within the computer. It has the highest level of privilege and access to all resources in the system.

The '500' is the relative ID of the Administrator account, which is a unique number assigned to each account/group within a computer.

---

7. Give the name of a file that has been restored

- rock-on.jpg
- Image1.jpg

---

8. Can you match the content of `index.dat` with some of the images in the other folders? If yes, provide the filenames.

- cnct_t[1].gif
- delete[1].gif

[1] https://www.lifewire.com/what-is-an-sid-number-2626005

- icon_add[1].gif
- icon_in[1].gif
- icon_tf[1].gif
- r[1].gif