Lab 1 – Evidence Aquisition

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 09/17/2019

About the Lab

The objective of the lab is to acquire two image of the file/ evidence, in this case a USB drive, using FTK Imager where one of them is a Logical Image and the other is a Physical Image.

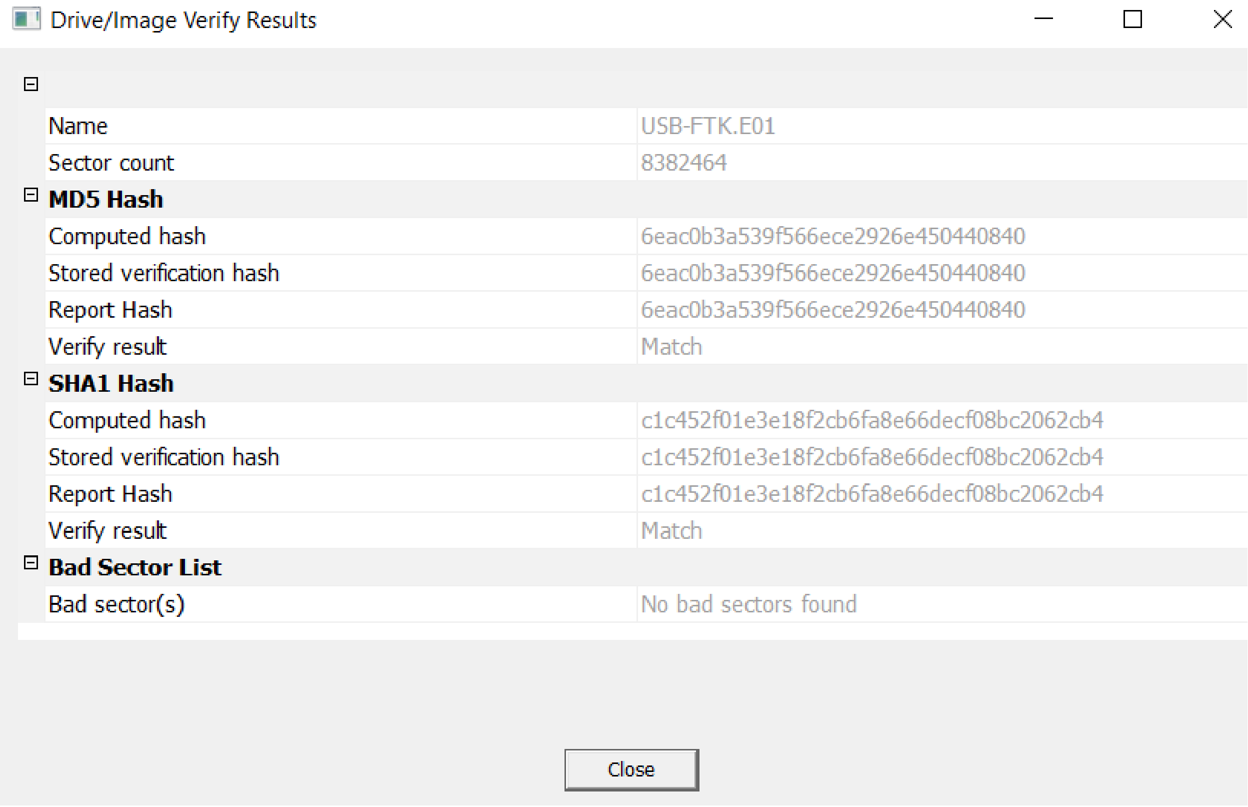
Part 1

1. *What is the resulting File format of the image?*

   The resulting file format is .e01, also known as Encase Image File Format. A more simple explanation is that EnCase is used to compress the data/ evidence and the data is stored in sector 1

2. *What is the hash of the image?*

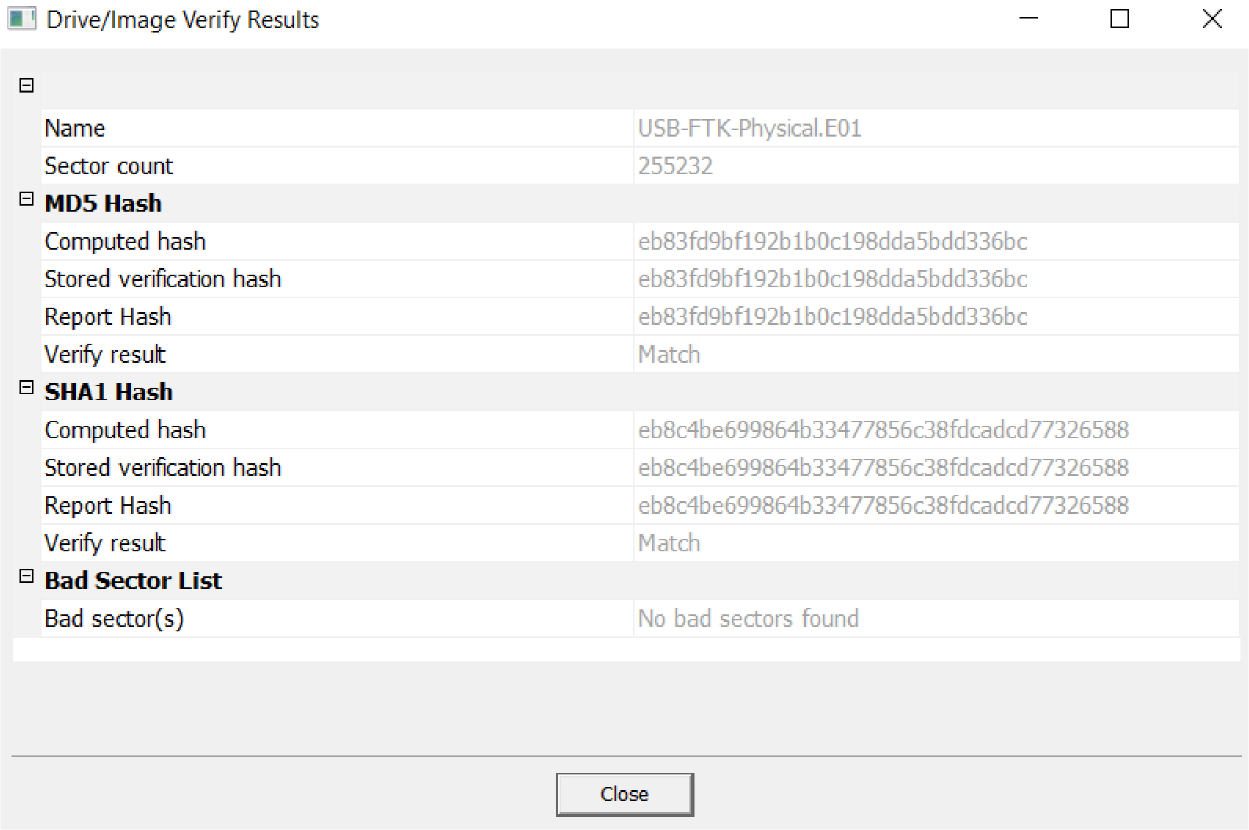
Logical Image



Drive/Image Verify Results

Name	USB-FTK.E01
Sector count	8382464
MD5 Hash	
Computed hash	6eac0b3a539f566ece2926e450440840
Stored verification hash	6eac0b3a539f566ece2926e450440840
Report Hash	6eac0b3a539f566ece2926e450440840
Verify result	Match
SHA1 Hash	
Computed hash	c1c452f01e3e18f2cb6fa8e66decf08bc2062cb4
Stored verification hash	c1c452f01e3e18f2cb6fa8e66decf08bc2062cb4
Report Hash	c1c452f01e3e18f2cb6fa8e66decf08bc2062cb4
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Physical Image



Name	USB-FTK-Physical.E01
Sector count	255232
MD5 Hash	
Computed hash	eb83fd9bf192b1b0c198dda5bdd336bc
Stored verification hash	eb83fd9bf192b1b0c198dda5bdd336bc
Report Hash	eb83fd9bf192b1b0c198dda5bdd336bc
Verify result	Match
SHA1 Hash	
Computed hash	eb8c4be699864b33477856c38fdcadcd77326588
Stored verification hash	eb8c4be699864b33477856c38fdcadcd77326588
Report Hash	eb8c4be699864b33477856c38fdcadcd77326588
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

3. *Difference between Physcial and Logical Image*

   Physical Image: In a layman's language physical is the exact copy of all the data that is present in a file system/ evidence. It copies all the data bit by bit, even if something doesn't make sense or not accessible.

   Logical Image: It copies all the accessible data from one file system to another and presents in a user-friendly manner that is very easy to access. The only disadvantage is that if there are any sections in the file system that are not accessible, it will not copy that section of data.

Conclusion

From this lab I learnt what is the difference between logical and physical image and how important imaging tools are for forensic investigators and also how to create an image of an evidence.