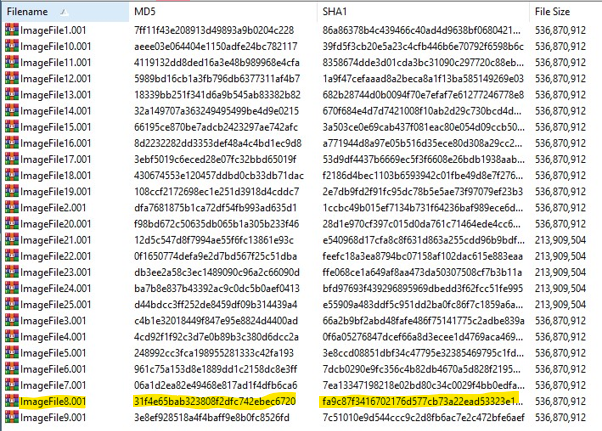
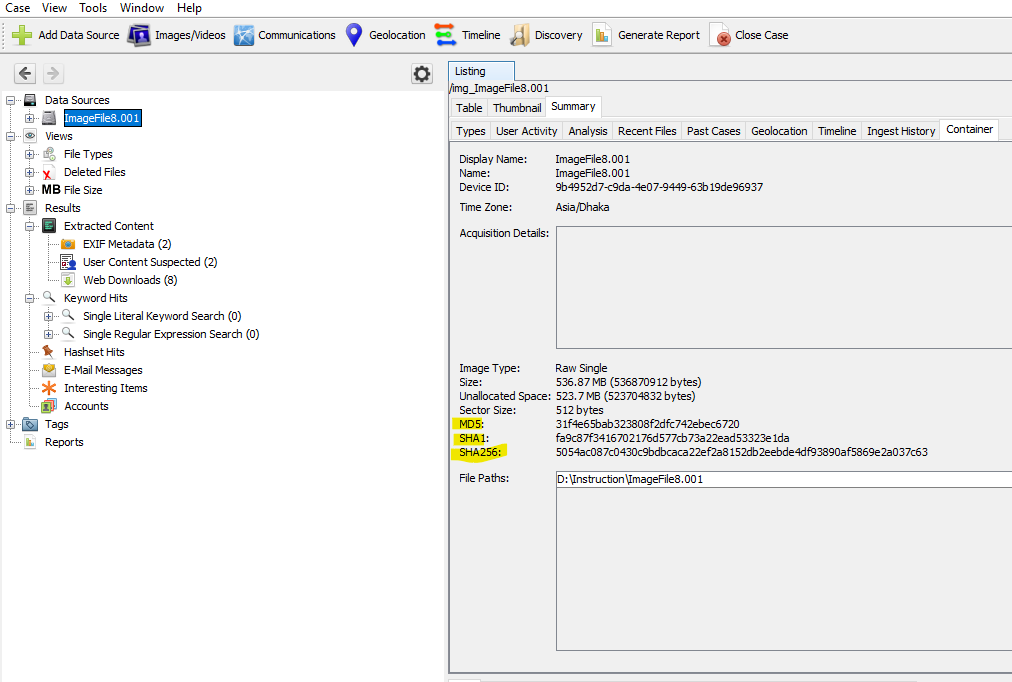
**Blue Coursework Task 1: Imaging Exercise**

**Part A:**

The image file which was provided to me was named “ImageFile8.001”. In the image file, I analyzed it with Autopsy tools and got some hash values. And this hash value is perfectly similar to the provided image file.





So it would be proven that I am working on a correct image file.

I created an image file named “Sports.E01” by FTK Imager. Which has a total of 12 parts.

The details of FTK imager tools-

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:

Acquired using: ADI4.5.0.3

Case Number: 120

Evidence Number: 5

Unique description: Sports Car Stealing

Examiner: Forensics Institute

Notes: Digital Forensics Investigation

--------------------------------------------------------------

Information for E:\Encase\_2\Sports:

Physical Evidentiary Item (Source) Information:

[Device Info]

 Source Type: Physical

[Drive Geometry]

 Cylinders: 6,527

 Tracks per Cylinder: 255

 Sectors per Track: 63

 Bytes per Sector: 512

 Sector Count: 104,857,600

[Physical Drive Information]

 Drive Model: VBOX HARDDISK

 Drive Serial Number: VB58036779-832520e8

 Drive Interface Type: IDE

 Removable drive: False

 Source data size: 51200 MB

 Sector count:    104857600

[Computed Hashes]

 MD5 checksum:    784dc9b7b4f5eef4e123480c0324dc68

 SHA1 checksum:   f4e9dd70116dffd6c9bfc7ac92d76561152ae796

Image Information:

 Acquisition started:   Sat Nov 19 20:20:36 2022

 Acquisition finished:  Sat Nov 19 21:01:18 2022

 Segment list:

  E:\Encase\_2\Sports.E01

  E:\Encase\_2\Sports.E02

  E:\Encase\_2\Sports.E03

  E:\Encase\_2\Sports.E04

  E:\Encase\_2\Sports.E05

  E:\Encase\_2\Sports.E06

  E:\Encase\_2\Sports.E07

  E:\Encase\_2\Sports.E08

  E:\Encase\_2\Sports.E09

  E:\Encase\_2\Sports.E10

  E:\Encase\_2\Sports.E11

  E:\Encase\_2\Sports.E12

Image Verification Results:

 Verification started:  Sat Nov 19 21:01:19 2022

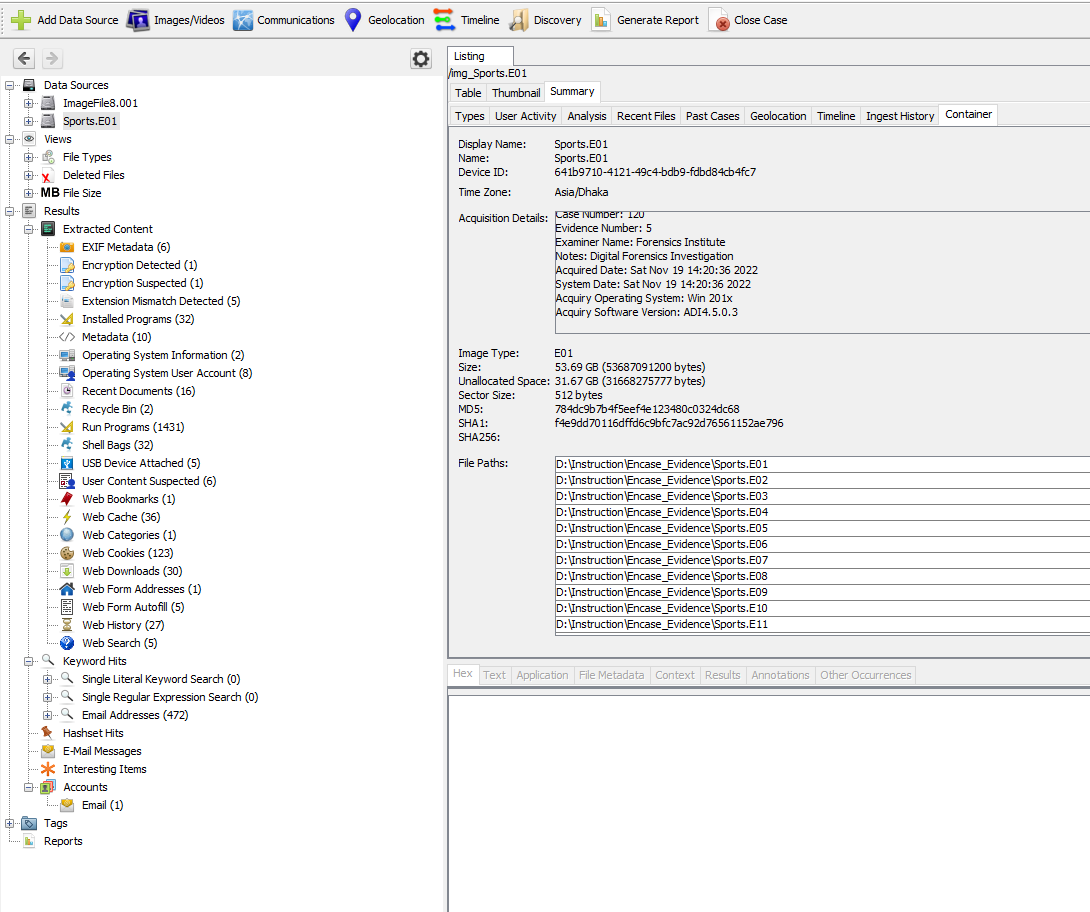
 Verification finished: Sat Nov 19 21:20:32 2022

 MD5 checksum:    784dc9b7b4f5eef4e123480c0324dc68 : verified

 SHA1 checksum:   f4e9dd70116dffd6c9bfc7ac92d76561152ae796 : verified

**Part B:**

I analyze the Sports.E01 image file from both of autopsy and FTK Imager tools.





Here we can see that both tools' hash values are the same. So we can say that the image file is dual tool verified.

**Part C:**

**Write Blockers:**

A tool called Write Blocker is intended to stop any write access to the hard drive, allowing read-only access to the data storage devices without jeopardizing the data's integrity. If utilized properly, a write blocking can ensure that the chain of custody is protected. A set of general principles for write-blocking restrictions have been published by NIST:

* The write-blocker tool must prevent any changes to a protected drive.
* No activities on a disk that is not protected may be stopped by the write-blocker utility.
* The write-blocker program must not obstruct access to or collection of data from any drive.

Hardware and software write blockers are the two main categories of write blockers. The same goal of both varieties of write blockers is to stop any writes to storage devices.

**The block diagram of write blockers:**

**Write Blocker**

**Deny all write attempts**

**Caches the writes attempts**

**OS as failures**

**OS as successful**

* A hardware write blocker (HWB) is a hardware device that attaches to a computer system with the primary purpose of intercepting and preventing (or ‘blocking’) any modifying command operation from ever reaching the storage device. Physically, the device is connected between the computer and a storage device. The gadget is physically connected to a storage device and a computer.
* By observing and filtering drive I/O commands transmitted by an application or OS over a specific access interface, a software write block tool performs its function.