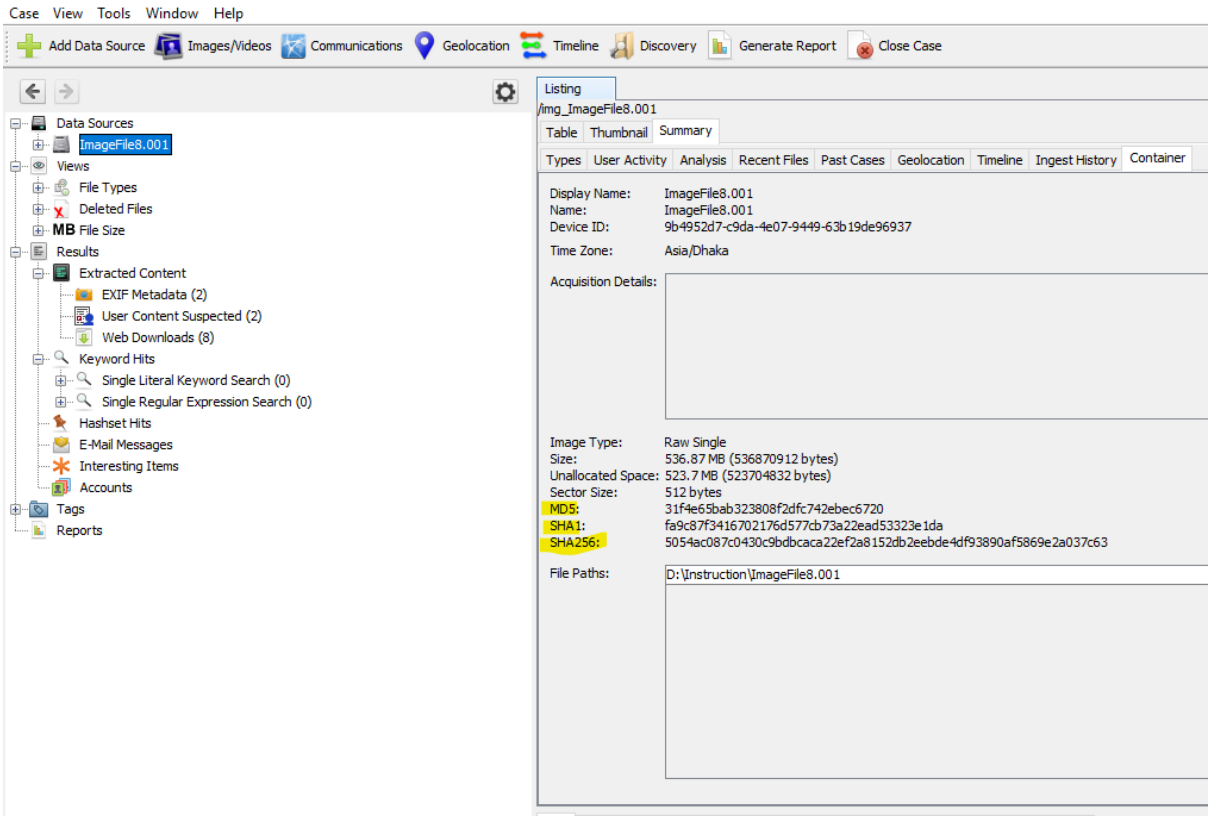
Blue Coursework Task 1: Imaging Exercise

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.

Filename	MD5	SHA1	File Size
ImageFile1.001	7ff11f43e208913d49893a9b0204c228	86a86378b4c439466c40ad4d9638bf0680421...	536,870,912
ImageFile10.001	aeee03e064404e1150adfe24bc782117	39fd5f3cb20e5a23c4cfb446b6e70792f6598b6c	536,870,912
ImageFile11.001	4119132dd8ded16a3e48b989968e4cfa	8358674dde3d01cda3bc31090c297720c88eb...	536,870,912
ImageFile12.001	5989bd16cb1a3fb796db6377311af4b7	1a9f47cefaaad8a2beca8a1f13ba585149269e03	536,870,912
ImageFile13.001	18339bb251f341d6a9b545ab83382b82	682b28744d0b0094f70e7efaf7e61277246778e8	536,870,912
ImageFile14.001	32a149707a363249495499be4d9e0215	670f684e4d7d7421008f10ab2d29c730bcd4d...	536,870,912
ImageFile15.001	66195ce870be7adcb2423297ae742afc	3a503ce0e69cab437f081eac80e054d09ccb50...	536,870,912
ImageFile16.001	8d2232282dd3353def48a4c4bd1ec9d8	a771944d8a97e05b516d35ece80d308a29cc2...	536,870,912
ImageFile17.001	3ebf5019c6eced28e07fc32bbd65019f	53d9df4437b6669ec5f3f6608e26bdb1938aab...	536,870,912
ImageFile18.001	430674553e120457ddbd0cb33db71dac	f2186d4bec1103b6593942c01fbe49d8e7f276...	536,870,912
ImageFile19.001	108ccf2172698ec1e251d3918d4cddc7	2e7db9fd2f91fc95dc78b5e5ae73f97079ef23b3	536,870,912
ImageFile2.001	dfa7681875b1ca72df54fb993ad635d1	1ccbc49b015ef7134b731f64236baf989ece6d...	536,870,912
ImageFile20.001	f98bd672c50635db065b1a305b233f46	28d1e970cf397c015d0da761c71464ede4cc6...	536,870,912
ImageFile21.001	12d5c547d8f7994ae55f6fc13861e93c	e540968d17cfa8c8f631d863a255cdd96b9bdf...	213,909,504
ImageFile22.001	0f1650774defa9e2d7bd567f25c51dba	feefc18a3ea8794bc07158af102dac615e883eaa	213,909,504
ImageFile23.001	db3ee2a58c3ec1489090c96a2c66090d	ffe068ce1a649af8aa473da50307508cf7b3b11a	213,909,504
ImageFile24.001	ba7b8e837b43392ac9c0dc5b0aef0413	bfd97693f439296895969dbedd3f62fcc51fe995	213,909,504
ImageFile25.001	d44bdcc3ff252de8459df09b314439a4	e55909a483ddf5c951dd2ba0fc86f7c1859a6a...	213,909,504
ImageFile3.001	c4b1e32018449f847e95e8824d4400ad	66a2b9bf2abd48fafe486f75141775c2adbe839a	536,870,912
ImageFile4.001	4cd92f1f92c3d7e0b89b3c380d6dcc2a	0f6a05276847dcef66a8d3ecee1d4769aca469...	536,870,912
ImageFile5.001	248992cc3fca198955281333c42fa193	3e8ccd08851dbf34c47795e32385469795c1fd...	536,870,912
ImageFile6.001	961c75a153d8e1889dd1c2158dc8e3ff	7dcb0290e9fc356c4b82db4670a5d828f2195...	536,870,912
ImageFile7.001	06a1d2ea82e49468e817ad1f4dfb6ca6	7ea13347198218e02bd80c34c0029f4bb0edfa...	536,870,912
ImageFile8.001	31f4e65bab323808f2dfc742ebec6720	fa9c87f3416702176d577cb73a22ead53323e1...	536,870,912
ImageFile9.001	3e8ef928518a4f4baff9e8b0fc8526fd	7c51010e9d544ccc9c2d8fb6ac7e2c472bfe6aef	536,870,912



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

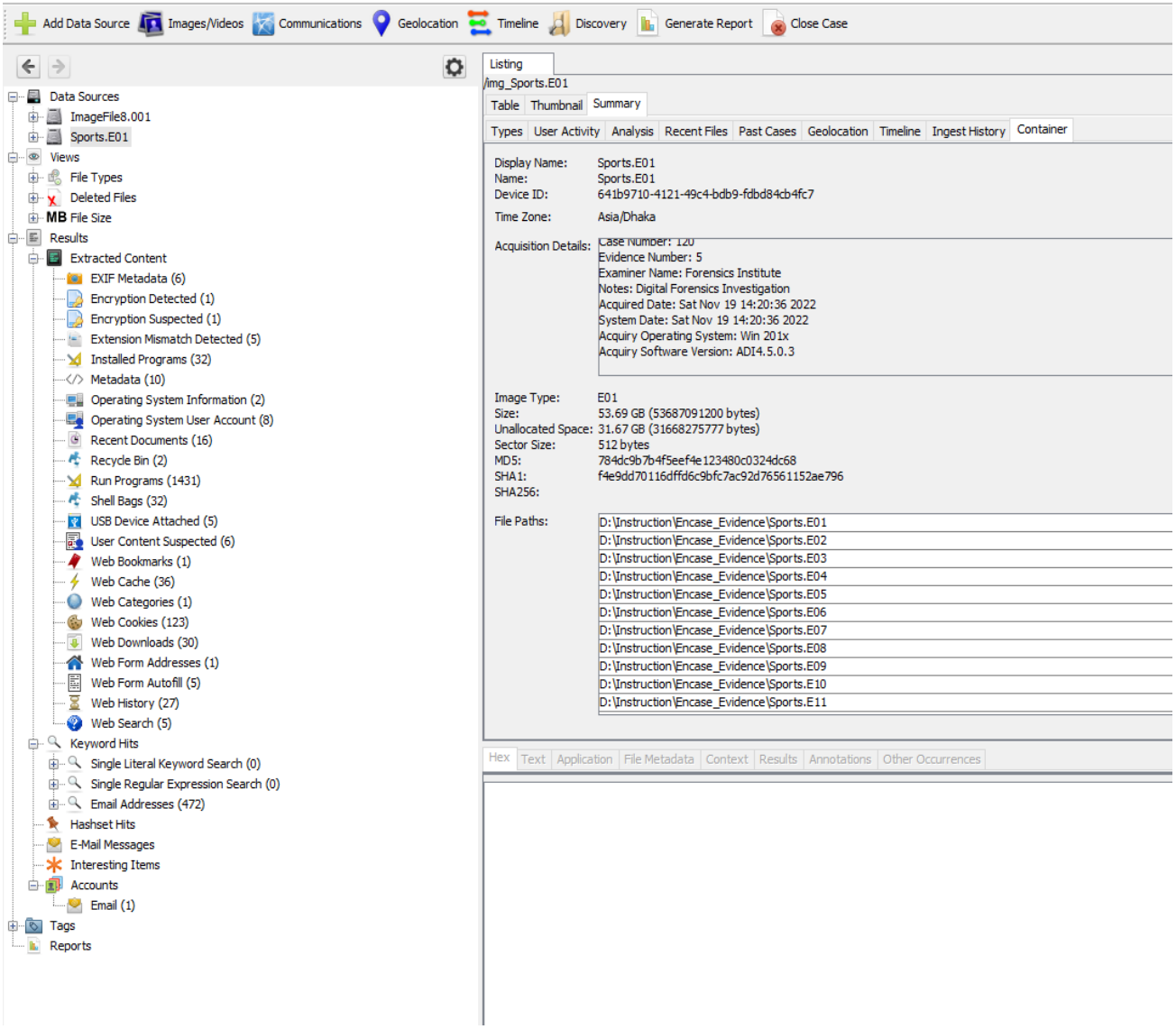
Image Information:
 Acquisition started: Sat Nov 19 20:20:36 2022
 Acquisition finished: Sat Nov 19 21:01:18 2022
 Segment list:
  E:\Encase_2\Sports.E01
  E:\Encase_2\Sports.E02
  E:\Encase_2\Sports.E03
  E:\Encase_2\Sports.E04
  E:\Encase_2\Sports.E05
  E:\Encase_2\Sports.E06

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.



```
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
```

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:

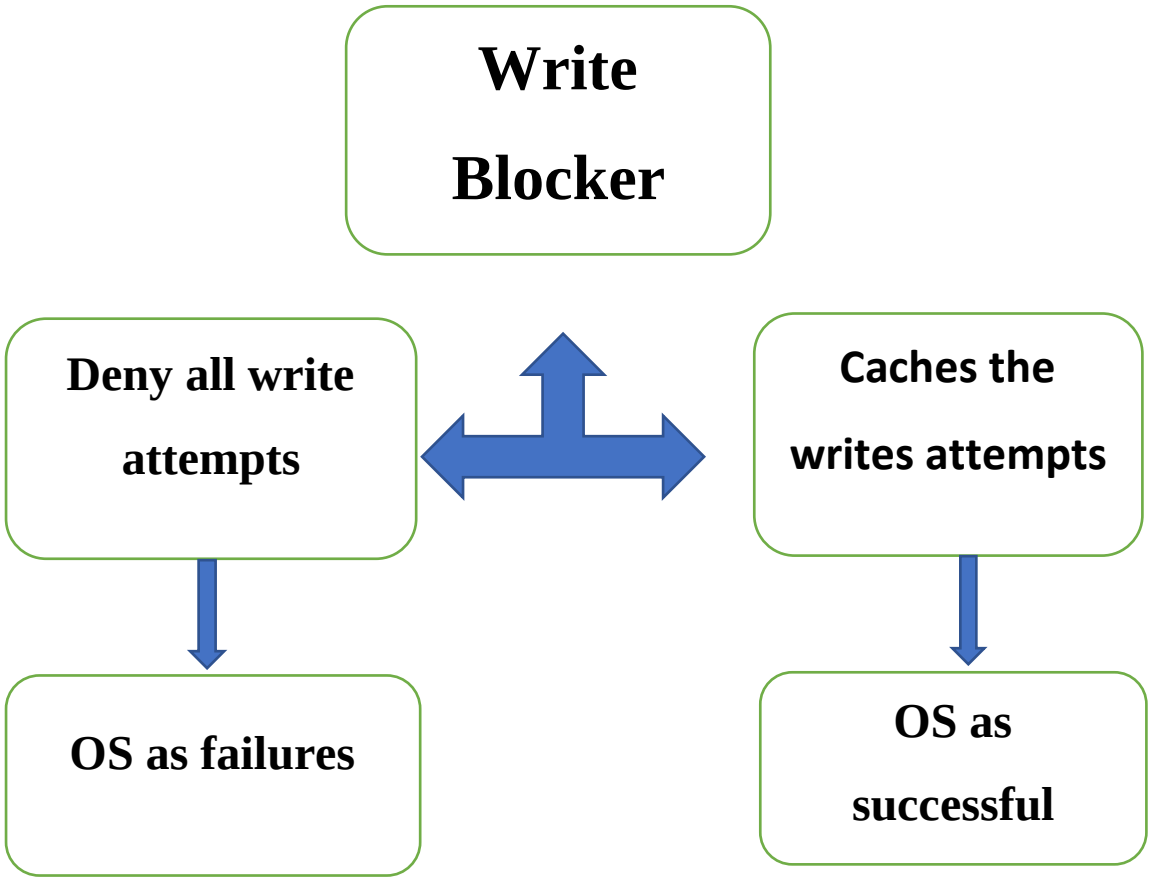
Write Blockers:

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:



- 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.