Assignment 1: Chanakya Gaur: Computer Forensics

1. Use FTK Imager to create an .E01 “Logical” image copy (“create disk image”) of the red Seagate mock evidence hard drive, the drive named MANTOOTH [NTFS]. \*Image the drive as a “Logical Drive.” “Do not fragment” the image. Do not select “Verify images after they are created.” Do not select “Precalculate progress statistics.” Do not select “Create directory listings of all files in the image after they are created.” You can save your image files to a folder that you create on the desktop of the computer you are working with. However, be sure to erase these files, and empty the Recycle Bin before you logoff the computer, if others will also have access to your computer.]

Created By AccessData® FTK® Imager 3.1.5.0

Case Information:

Acquired using: ADI3.1.5.0

Case Number: 2

Evidence Number: 1

Unique description: hdd

Examiner: gaur

Notes:

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

Information for \\SITATUNGA\Users\cgaur1\Desktop\gaur.E01:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Logical

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 224,847

[Physical Drive Information]

Removable drive: False

Source data size: 109 MB

Sector count: 224847

[Computed Hashes]

MD5 checksum: f767eb23c9aa214a0099784b456a7d8f

SHA1 checksum: 9d87b218f4d89d7f5b043d4be2b2ca1b068c2ba2

Image Information:

Acquisition started: Mon Sep 11 16:49:58 2017

Acquisition finished: Mon Sep 11 16:52:27 2017

Segment list:

\\SITATUNGA\Users\cgaur1\Desktop\gaur.E01.E01

Image Verification Results:

Verification started: Mon Sep 11 16:54:33 2017

Verification finished: Mon Sep 11 16:54:36 2017

MD5 checksum: f767eb23c9aa214a0099784b456a7d8f : verified

SHA1 checksum: 9d87b218f4d89d7f5b043d4be2b2ca1b068c2ba2 : verified

Click on the Image Summary button. What is the MD5 hash value of this image? (A print-screen of the value is sufficient if you do not want to copy all of the alpha-numeric characters.) [5 points]

MD5 checksum: f767eb23c9aa214a0099784b456a7d8f

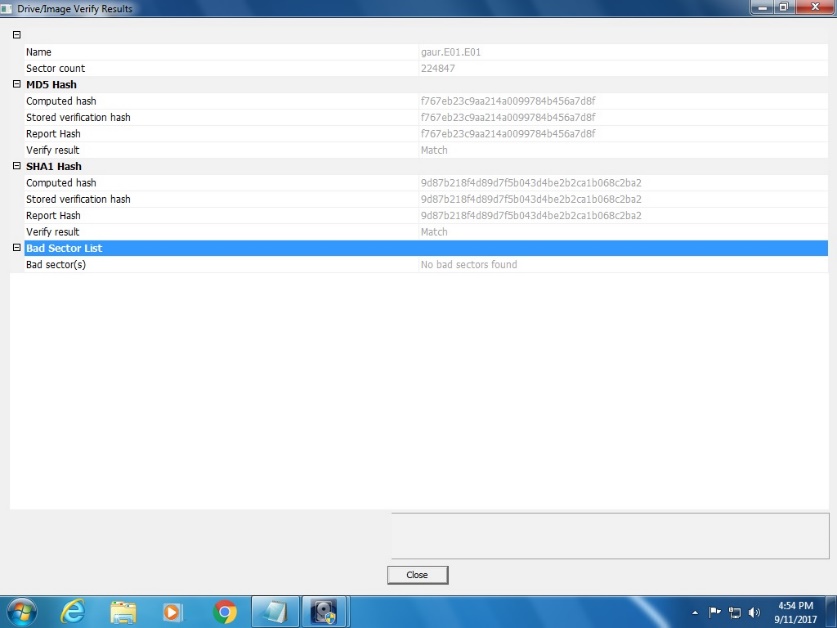
What is the SHA1 hash value of this image? (A print-screen of the value is sufficient if you do not want to copy all of the alpha-numeric characters.) [5 points]

SHA1 checksum: 9d87b218f4d89d7f5b043d4be2b2ca1b068c2ba2

2. Close FTK Imager. This will remove the image file from FTK Imager. Open FTK Imager again, add the image file (“File” > “Add Evidence Item” > “Image File”) that you just created, and calculate the MD5 and SHA1 values for this file again (Right-click on the top of the evidence navigation tree and select “Verify Drive/Image”). These values should match the previous values. (If the values match, you have demonstrated that the image file has not been altered since the previous hash values were calculated.)

What is the MD5 hash value of this image? (A print-screen of the value is sufficient if you do not want to copy all of the alpha-numeric characters.) [5 points]

What is the SHA1 hash value of this image? (A print-screen of the value is sufficient if you do not want to copy all of the alpha-numeric characters.) [5 points]



3. Close any programs that are accessing the red Seagate mock evidence hard drive, turn off the Tableau Forensic USB Bridge, detach the red Seagate mock evidence hard drive and put it away. You are done with this piece of mock evidence.

Attached the USB thumb drive with the tag that states “35” (provided with this exercise) to the Tableau Forensic USB Bridge and turn on the write-block device. Verify that the green light shows the thumb drive is being write-blocked.

Create a “Physical” (not “Logical”) image copy of the entire USB thumb drive. You can save the image files on the computer’s desktop as you did in part 1. Since the thumb drive is relatively small, it will not take long to make a bit-for-bit copy of every bit that is on the device (This process might take about 2 minutes, which is longer than it took to do a logical image data on the 2 TB hard drive).

Created By AccessData® FTK® Imager 3.1.5.0

Case Information:

Acquired using: ADI3.1.5.0

Case Number: 1

Evidence Number: 2

Unique description: thumb

Examiner: gaur

Notes:

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

Information for \\SITATUNGA\Users\cgaur1\Desktop\thumb.E01:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 33

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 539,000

[Physical Drive Information]

Drive Model: General UDisk USB Device

Drive Serial Number: 14040916372308565140

Drive Interface Type: USB

Removable drive: True

Source data size: 263 MB

Sector count: 539000

[Computed Hashes]

MD5 checksum: 1568dd5210c5faa25226b64e012184e4

SHA1 checksum: bcc660ebf0bb4c8437e6a7e730ac6dd3c2d8f567

Image Information:

Acquisition started: Mon Sep 11 16:58:53 2017

Acquisition finished: Mon Sep 11 17:01:38 2017

Segment list:

[\\SITATUNGA\Users\cgaur1\Desktop\thumb.E01.E01](file:///\\SITATUNGA\Users\cgaur1\Desktop\thumb.E01.E01)

What is the MD5 hash value of this image? (A print-screen of the value is sufficient if you do not want to copy all of the alpha-numeric characters.) [5 points]

MD5 checksum: 1568dd5210c5faa25226b64e012184e4

What is the SHA1 hash value of this image? (A print-screen of the value is sufficient if you do not want to copy all of the alpha-numeric characters.) [5 points]

SHA1 checksum: bcc660ebf0bb4c8437e6a7e730ac6dd3c2d8f567

4. Open FTK Imager and add the Mantooth.E01 file, which is found in a directory on your shared drive (probably Shared: S), in a folder named “Forensics” in a sub-folder named “Evidence Files”.

Review the partition structure. Besides the “unpartitioned space”, how many partitions are there and what are their names? (Note: Their names are not “Partition 1” and “Partition 2”. You need to click on the plus-sign in from of each partition to reveal the names.) [4 points]

1.Mantooth

2.Noname

5. What file system is on each partition? [ 4 points]

1. Mantooth – Windows File system - NTFS

2. Noname - Linux File System – Ext

6. Click on the root of the evidence tree. What version of FTKImager was used to acquire this image? [Note: Look in the bottom left corner of FTK Imager, in the Properties window]. [2 points]

FTKI 2.5.3.14

7. Navigate to the Partition 1 > MANTOOTH > root > Users > Wes Mantooth directory. There are several thumbnail pictures present within the “Pictures” directory. (Change the View to “Thumbnails”). What is the name of the file associated with the picture of the tail of a whale? [5 points]

Humpback Whale.jpg

8. Within the same directory as the picture of the whale tail, what is the date when the file named “Toco Tucan.jpg” was modified? (Change the view to “Details”.)[ 5 points]

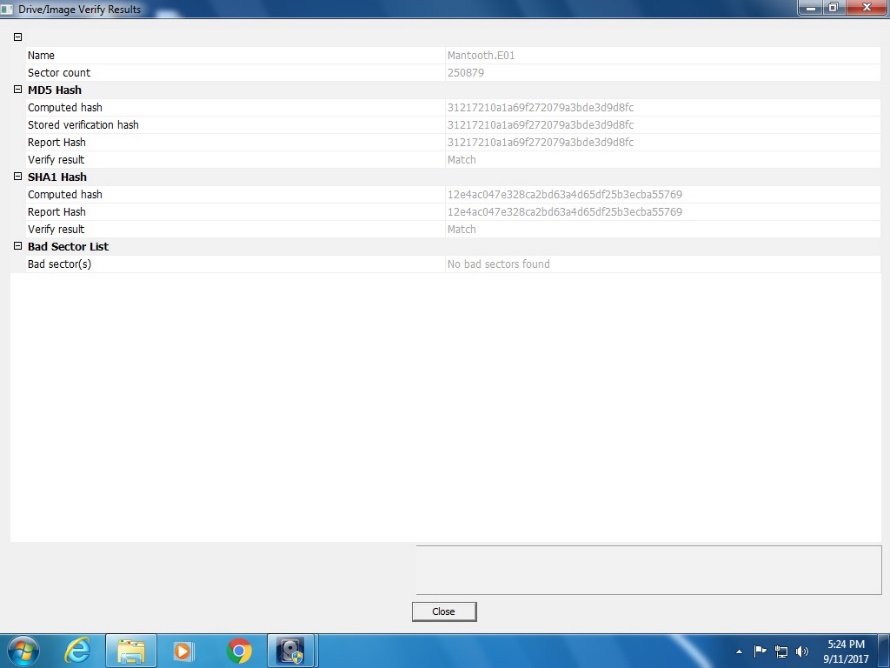
11/02/2006 12:35:22 PM

9. Within the same directory as the picture of the whale tail, what are the MD5 and SHA1 hash values for the file named “Dock.jpg”. [Note: You need to right-click on the name of the picture while it is in the “Details” view, and select “Export File Hash List”. If you were not able to figure this process out for yourself, I encourage you to get the AccessData Forensics training manual that is available in the bookstore.] [5 points]

MD5: 8a57237b7ebab405afa76f2b81b3f165

SHA1: 939c4b90a5b9dcfce5001db4abdd3c69e6733a3b

10. The image file you are working with is currently in the .E01 format. Right-click “Mantooth.E01” at the top of the evidence tree and selecting “Verify Drive/Image”. What is the MD5 and SHA1 of the E01 image when it is verified in this manner? [5 points]



11. Export a copy of the image in the RAW(dd) format by right-clicking “Mantooth.E01” and select “Export Disk Image”. Export the image in the Raw(dd) format. This will create a file with the .001 file extension. If you add this image to FTK Imager and select “verify Drive/Image”, you can calculate the hash values. What is the MD5 and SHA1 value of this new image file? [5 points]

Created By AccessData® FTK® Imager 3.1.5.0

Case Information:

Acquired using: ADI3.1.5.0

Case Number: 1

Evidence Number: 3

Unique description: mantooh raw

Examiner: gaur

Notes:

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

Information for \\SITATUNGA\Users\cgaur1\Desktop\mantoothraw:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Verification Hashes]

MD5 verification hash: 31217210a1a69f272079a3bde3d9d8fc

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 250,879

[Image]

Image Type: E01

Case number:

Evidence number:

Examiner:

Notes:

Acquired on OS: Windows XP

Acquired using: FTKI2.5.3.14

Acquire date: 7/2/2008 9:09:34 PM

System date: 7/2/2008 9:09:34 PM

Unique description: untitled

Source data size: 122 MB

Sector count: 250879

[Computed Hashes]

MD5 checksum: 31217210a1a69f272079a3bde3d9d8fc

SHA1 checksum: 12e4ac047e328ca2bd63a4d65df25b3ecba55769

Image Information:

Acquisition started: Mon Sep 11 17:26:02 2017

Acquisition finished: Mon Sep 11 17:26:06 2017

Segment list:

\\SITATUNGA\Users\cgaur1\Desktop\mantoothraw.001

Image Verification Results:

Verification started: Mon Sep 11 17:27:22 2017

Verification finished: Mon Sep 11 17:28:28 2017

MD5 checksum: 31217210a1a69f272079a3bde3d9d8fc : verified

SHA1 checksum: 12e4ac047e328ca2bd63a4d65df25b3ecba55769 : verified

12. Place the two image files (Mantooth.E01 and the .001 image file that you created from Mantooth.E01) into the same folder and use FTK Imager to calculate the hash value of each file. [Note: You will need to select “Contents of a Folder” as the source target.] Are the hash values the same or different? [5 points]

Mantooth.E01:

MD5 checksum: 9ab5fe980d66b0452479321ec96d3d10

SHA1 checksum: ee9be79d81db8b63a940e43328448449d78cc964

Mantoothraw.001

MD5: 31217210a1a69f272079a3bde3d9d8fc

SHA1: 12e4ac047e328ca2bd63a4d65df25b3ecba55769

13. In step 12 above, you should notice that the MD5 and SHA1 values calculated for the E01 image are different than the MD5 and SHA1 values associated with the Raw(dd) .001 image. Since the cryptographic hash values do not match, does this mean the evidence has been altered? [5 points]

No. Since the files are of a different format, their hash values will be different.

14. When you create a forensic image of a hard drive, why should you make sure you use a hardware-based write-block device? [5 points]

It is necessary to use a hardware based write-blocker to prevent any software or operating system to inadvertently write on the disk. Any alteration in the disk will make the evidence invalid.

IN THEORY, which image file format takes more time to generate, E01 or Raw? Why? [Note: the question is, which file format requires more overhead. If you conduct some timed tests on small files, you might get a different answer. However, for large files, the extra overhead associated with the E01 image format should be obvious.] [5 points]

It will take more time to generate an E01 file compared to a Raw file as E01 files contain metadata and result in lossless compression which is why the overhead increases for E01.