

(Title)



Introduction

Digital forensics is a branch of forensic science that deals with investigations and recovery of useful materials found in digital devices particularly in cases of computer crime. In our experiment we will concentrate in different methods of creating disk images for forensic purposes.

The purpose of this experiment is to demonstrate how to use the dd command and the FTK Imager tools for the purpose of creating “forensically sound” disk images using windows 7 x86 platform as well as using Hex editor to analyze differences in image parameters.

This will be achieved through the usage of several Imaging tools, comparing them after the images are created. The images will then be compared using a Hex editor HxD so as to bring out the offset differences.

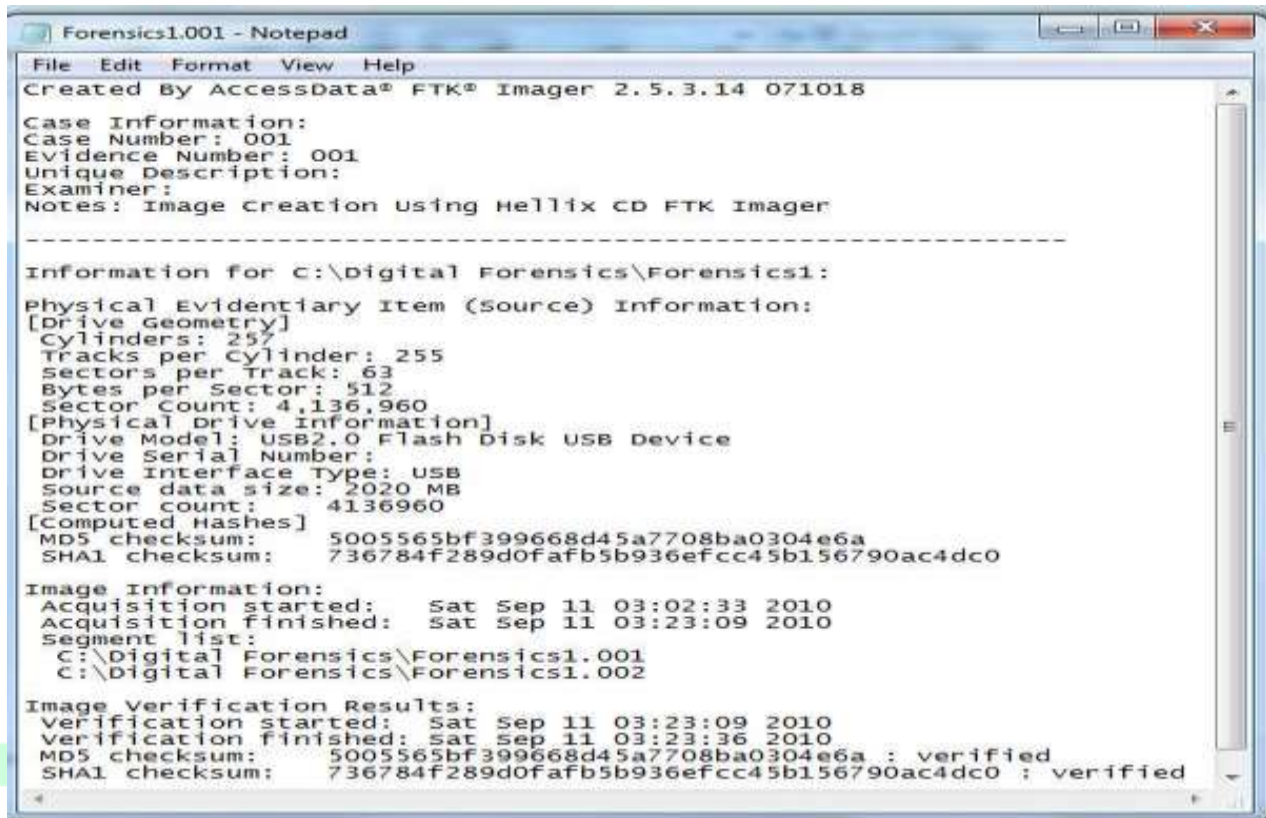
Materials / Tools Used

1. Computer with Windows 7 x86 bit platform.
2. Helix bootable CD (Version 2009 R1)
3. FTK Imager ver. 2.9.0
4. The dd.exe program from the Forensic Acquisition Utilities (FAU)
5. USB Thumb Drive
6. Hex Editor HxD

METHODOLOGY

Part I: Using the Helix CD FTK Imager to image a USB thumb drive

- a. The registry fix disableUSBwrite was run so as to write protect the device
- b. The Windows 7 x86 platform was then started and the USB thumb drive was inserted
- c. The Helix CD was inserted and the “live” Windows system was started.
- d. Under Quick Launch, the FTK Imager was chosen.
- e. Under the file menu, I chose “create disk image” where I chose the physical drive as the evidence source since I was using a USB thumb drive. The appropriate USB thumb drive was then selected and I clicked finish.
- f. Under the image destination, I clicked add, chose the raw (dd) format, entered the case number – 001, evidence number 001, chose the destination folder to be c:\Digital Forensics and gave the file name as “forensics” and the image creation was started
- g. After the image creation was complete, an image file with the name “Forensics1.001” and a text file with the name Forensics.txt containing MD5 and SHA1 has values was seen.



```
Forensics1.001 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 2.5.3.14 071018
Case Information:
Case Number: 001
Evidence Number: 001
Unique Description:
Examiner:
Notes: Image Creation Using Hellix CD FTK Imager

-----

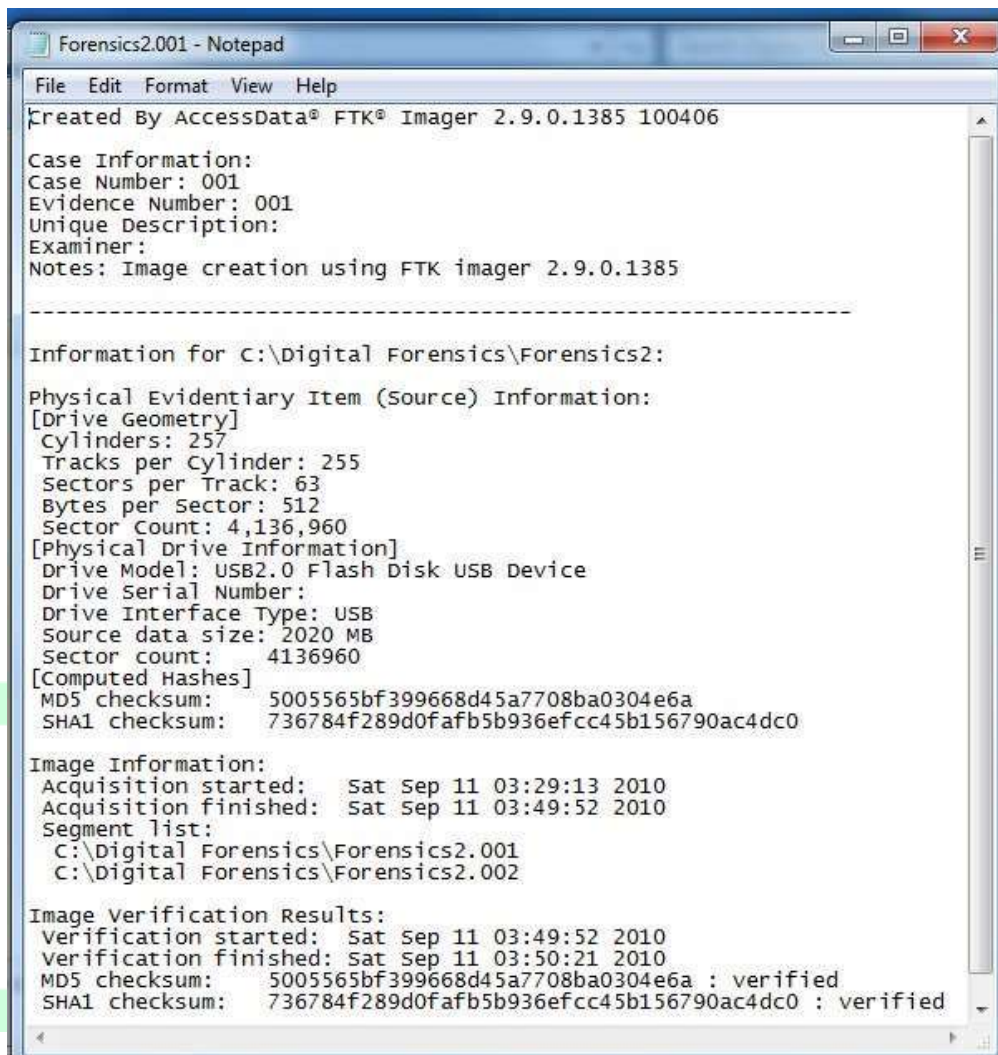
Information for c:\Digital Forensics\Forensics1:
Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 257
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 4,136,960
[Physical Drive Information]
Drive Model: USB2.0 Flash Disk USB Device
Drive Serial Number:
Drive Interface Type: USB
Source data size: 2020 MB
Sector count: 4136960
[Computed Hashes]
MD5 checksum: 5005565bf399668d45a7708ba0304e6a
SHA1 checksum: 736784f289d0fafb5b936efcc45b156790ac4dc0

Image Information:
Acquisition started: Sat Sep 11 03:02:33 2010
Acquisition finished: Sat Sep 11 03:23:09 2010
Segment list:
C:\Digital Forensics\Forensics1.001
C:\Digital Forensics\Forensics1.002

Image Verification Results:
Verification started: Sat Sep 11 03:23:09 2010
Verification finished: Sat Sep 11 03:23:36 2010
MD5 checksum: 5005565bf399668d45a7708ba0304e6a : verified
SHA1 checksum: 736784f289d0fafb5b936efcc45b156790ac4dc0 : verified
```

Part II: Using the FTK Imager ver. 2.9.0 to image a USB thumb drive

- a. FTK Imager ver. 2.9.0 was installed
- b. Under the file menu, I chose “create disk image” where I chose the physical drive as the evidence source since I was using a USB thumb drive. The appropriate USB thumb drive was then selected and I clicked finish.
- c. Under the image destination, I clicked add, chose the raw (dd) format, entered the case number – 001, evidence number 001, chose the destination folder to be c:\Digital Forensics and gave the file name as “forensics” and the image creation was started.
- d. After the image creation was complete, an image file with the name “Forensics2.001” and a text file with the name Forensics.txt containing MD5 and SHA1 has values was seen.



```
Forensics2.001 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:
Case Number: 001
Evidence Number: 001
Unique Description:
Examiner:
Notes: Image creation using FTK imager 2.9.0.1385

-----

Information for C:\Digital Forensics\Forensics2:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 257
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 4,136,960
[Physical Drive Information]
Drive Model: USB2.0 Flash Disk USB Device
Drive Serial Number:
Drive Interface Type: USB
Source data size: 2020 MB
Sector count: 4136960
[Computed Hashes]
MD5 checksum: 5005565bf399668d45a7708ba0304e6a
SHA1 checksum: 736784f289d0fafb5b936efcc45b156790ac4dc0

Image Information:
Acquisition started: Sat Sep 11 03:29:13 2010
Acquisition finished: Sat Sep 11 03:49:52 2010
Segment list:
C:\Digital Forensics\Forensics2.001
C:\Digital Forensics\Forensics2.002

Image Verification Results:
Verification started: Sat Sep 11 03:49:52 2010
Verification finished: Sat Sep 11 03:50:21 2010
MD5 checksum: 5005565bf399668d45a7708ba0304e6a : verified
SHA1 checksum: 736784f289d0fafb5b936efcc45b156790ac4dc0 : verified
```

Part III: Using the Forensic Acquisition Utility (FAU) to image a USB thumb drive

- The Forensic Acquisition Utility (FAU) Latest ver. FAU-1.3.0.2390a was installed.
- The Folder C:\CGS5131HW1 was created on the computer where the downloaded FAU software was uncompressed and saved at. This created a series of subfolders which are; C:\CGS5131HW1\fau-1.3.0.2390a\fau\FAU.
- The command line window was opened by accessing the folder C:\Windows\system32 and then right-clicking the cmd.exe application then selecting “Run as administrator” as shown below.

ORDER NOW

Disk1: USB2.0 Flash Disk (S/N ▼)

HWDetect: \\?\usbstor#disk&ven_usb2.0&prod_flash_disk&rev_2.60#1000000000008
997&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Geometry:

Cylinders: 257

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Total Size: 2118123520

Media Type: Removable media other than floppy

9/11/2010 7:18:12 AM (UTC)

9/11/2010 10:18:12 AM (local time)

- g. The command “dd.exe” was run so as to make a forensic copy of the USB thumb drive. With the USB thumb drive still write protected, the “dd.exe” command was run by entering the following command “dd.exe /?” or “dd.exe --help ” so as to see the help manual. The output that describe the options; if, of, conv, bs, count, skip, --localwrt and --cryptsum was recorded as follows:

bs=[BYTES] Set 'ibs' and 'obs' equal to BYTES.

conv=[KEYWORDS] Convert the input as per the comma separated keyword list.

The following are valid keywords:

noerror Continue reading after errors.

comp Compress the output.

decomp Decompress the output.

swab Swap each pair of bytes.

notrunc Don't truncate the output file.

resume Resume a broken copy operation (Enterprise level only).

count=[BLOCKS] Copy only the specified number of input blocks.

if=[SOURCE] Specifies the source for input; the default is stdin.

of=[DESTINATION] Specifies the destination for output; the default is stdout.

--cryptsum [ALGORITHM] Includes one or more cryptographic checksums in the output. "md2", "md4", "md5" and "sha" or "sha1" are supported on all platforms "sha_256", "sha_384" and "sha_512" are supported on Windows Server 2003 and later.B

--localwrt Enables writing output to a local fixed drive.

--count [BYTES] Stop after acquiring the specified number of bytes.

- h. The USB thumb drive name is \\.\PhysicalDrive1. The dd.exe command below was used to make a USB thumb drive image which was saved to the hard drive while computing the MD5 and SHA1 hashes concurrently.

```
dd.exe -localwrt if=\\.\Physicaldrive1 of=C:\Digital Forensics conv=noerror -cryptsum
MD5 - cryptsum SHA1
```

```
<?xml version="1.0" encoding="UTF-16" standalone="no" ?>
```

```
- <Security_catalog xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:forensic_acquisition_utilities
  http://www.gmgsystemsinc.com/fau/forensic_acquisition_utilities.xsd"
  xmlns="urn:forensic_acquisition_utilities" xmlns:fau="urn:forensic_acquisition_utilities"
  Version="1.2" SchemaVersion="1.0.0.21"
  List_Identifier="71d1feb869a75d517b452f77709322a3" Effective_Date="2010-09-
  11T07:31:29Z" Toolset="Forensic Acquisition Utilities, 1, 3, 0, 2390" Tool="dd, 5, 3, 0, 2390"
  Command_line="dd.exe --localwrt if=\\.\PhysicalDrive1 of=C:\ conv=noerror --cryptsum md5 --
  cryptsum sha1" Logged_on_user="Edgar-PC\Administrator" Collection_id="{CEB1A26C-
  FBD5-4A7D-A773-B2AF4F7A3380}">
- <Security_entry Path="EDGAR-PC_PhysicalDrive1.img" ReferenceNumber="0" Abstract="0"
  Physical="0" Changed="0">
- <Thumbprint Algorithm="md5" Physical="0" Compressed="0" Changed="0">
  <Hash_value>5005565bf399668d45a7708ba0304e6a</Hash_value>
  </Thumbprint>
- <Thumbprint Algorithm="sha1" Physical="0" Compressed="0" Changed="0">
  <Hash_value>736784f289d0fafb5b936efcc45b156790ac4dc0</Hash_value>
  </Thumbprint>
  </Security_entry>
</Security_catalog>
```

It was noted that for all the above software's and methods used to create an image, the image log results were the same in Part I, Part II and Part III in terms of the thumbprint algorithm md5 and sha1.

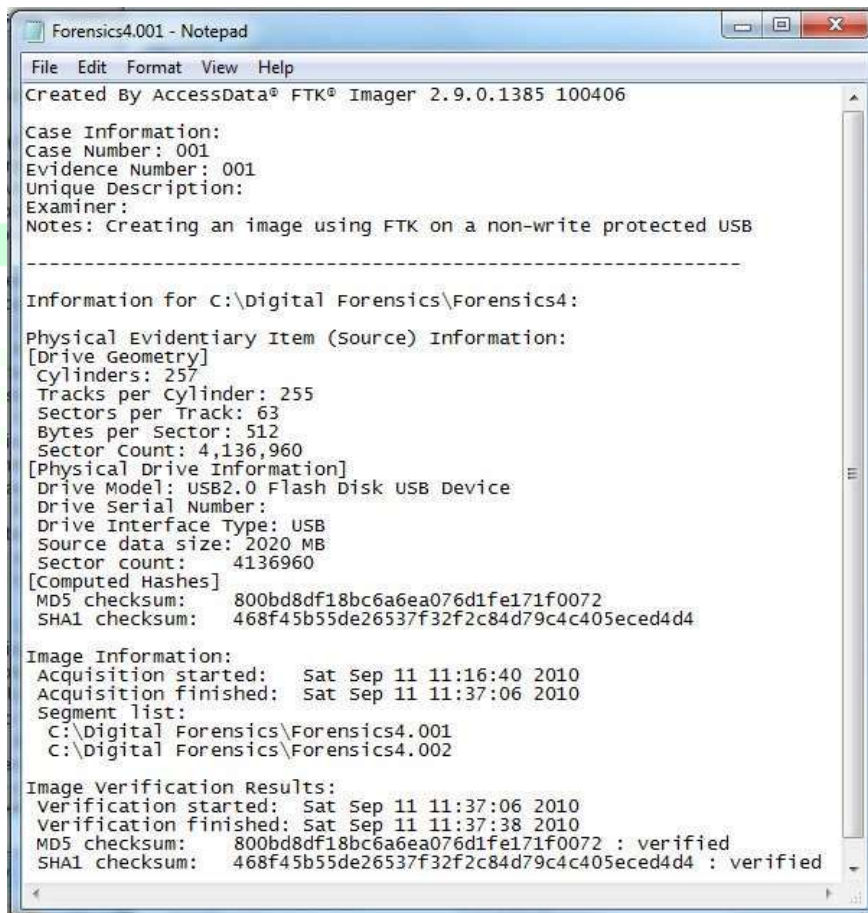
Part IV

- a. Write protection was removed by running enabling the USB write using the "enableUSBwrite" registry fix.

A text file named CGS5131HW1Q4.txt and it was saved under the USB thumb drive's root directory. The date/time stamps were reported as follows;

Created: Today, September 11, 2010, 11:05:09 AM
Modified: Today, September 11, 2010, 11:05:10 AM
Accessed: Today, September 11, 2010

- b. The FTK imager ver. 2.9.0 in part II was used to create a dd image using the procedure in part 2 while it was not write protected. The image log file results containing MD5 and SHA1 were as follows;



```
Forensics4.001 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:
Case Number: 001
Evidence Number: 001
Unique Description:
Examiner:
Notes: Creating an image using FTK on a non-write protected USB

-----

Information for C:\Digital Forensics\Forensics4:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 257
Tracks per cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 4,136,960
[Physical Drive Information]
Drive Model: USB2.0 Flash Disk USB Device
Drive Serial Number:
Drive Interface Type: USB
Source data size: 2020 MB
Sector count: 4136960
[Computed Hashes]
MD5 checksum: 800bd8df18bc6a6ea076d1fe171f0072
SHA1 checksum: 468f45b55de26537f32f2c84d79c4c405eced4d4

Image Information:
Acquisition started: Sat Sep 11 11:16:40 2010
Acquisition finished: Sat Sep 11 11:37:06 2010
Segment list:
C:\Digital Forensics\Forensics4.001
C:\Digital Forensics\Forensics4.002

Image Verification Results:
Verification started: Sat Sep 11 11:37:06 2010
Verification finished: Sat Sep 11 11:37:38 2010
MD5 checksum: 800bd8df18bc6a6ea076d1fe171f0072 : verified
SHA1 checksum: 468f45b55de26537f32f2c84d79c4c405eced4d4 : verified
```

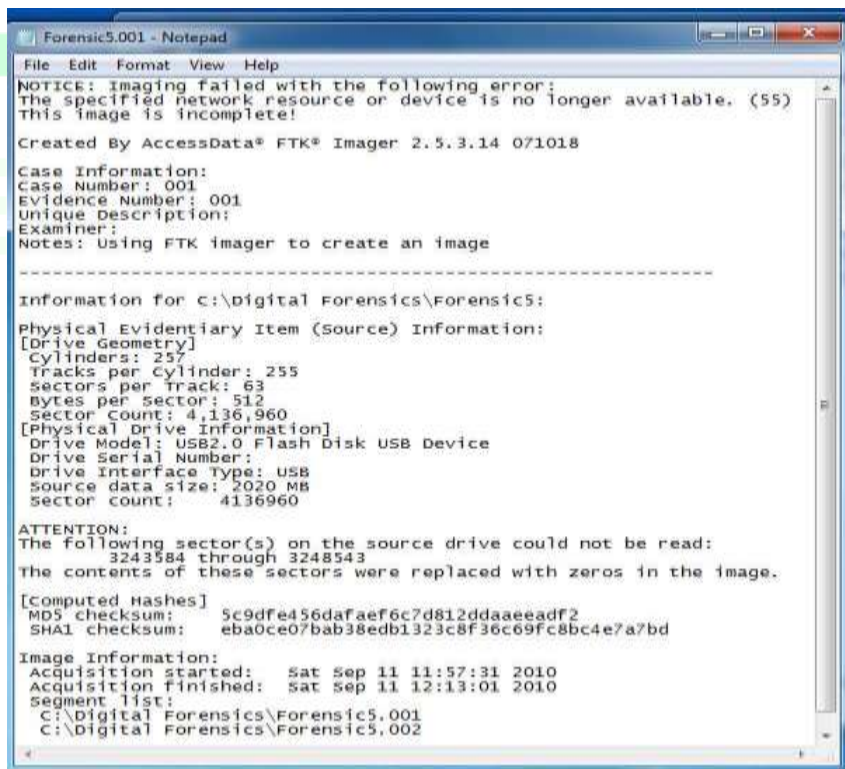
- c. The created text file “CGS5131HW1Q4.txt” was accessed without being modified, moving, renaming or re-saving it. The date/time stamp were recorded as follows;

Created: Today, September 11, 2010, 11:05:09 AM
 Modified: Today, September 11, 2010, 11:05:10 AM
 Accessed: Today, September 11, 2010

- d. There were no changes in the date/time stamps reported in (c) compared to those in step (a). Therefore i opened the saved text file in the USB thumb drive, and saved it back to itself without modifying it. The Date and time stamps were then recorded as follows;

Created: Today, September 11, 2010, 45 minutes ago
 Modified: Today, September 11, 2010, 11:50:36 AM
 Accessed: Today, September 11, 2010

- e. The FTK Imager used in Part II was used to create an image using the procedure in part II and the Image log file reports were as follows.



```
Forensic5.001 - Notepad
File Edit Format View Help
NOTICE: imaging failed with the following error:
The specified network resource or device is no longer available. (55)
This image is incomplete!

Created By AccessData® FTK® Imager 2.5.3.14 071018

Case Information:
Case Number: 001
Evidence Number: 001
Unique Description:
Examiner:
Notes: Using FTK imager to create an image

-----
Information for c:\digital Forensics\Forensic5:
Physical Evidentiary Item (source) Information:
[Drive Geometry]
Cylinders: 257
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 4,136,960
[Physical Drive Information]
Drive Model: USB2.0 Flash Disk USB Device
Drive Serial Number:
Drive Interface Type: USB
Source data size: 2020 MB
Sector count: 4136960

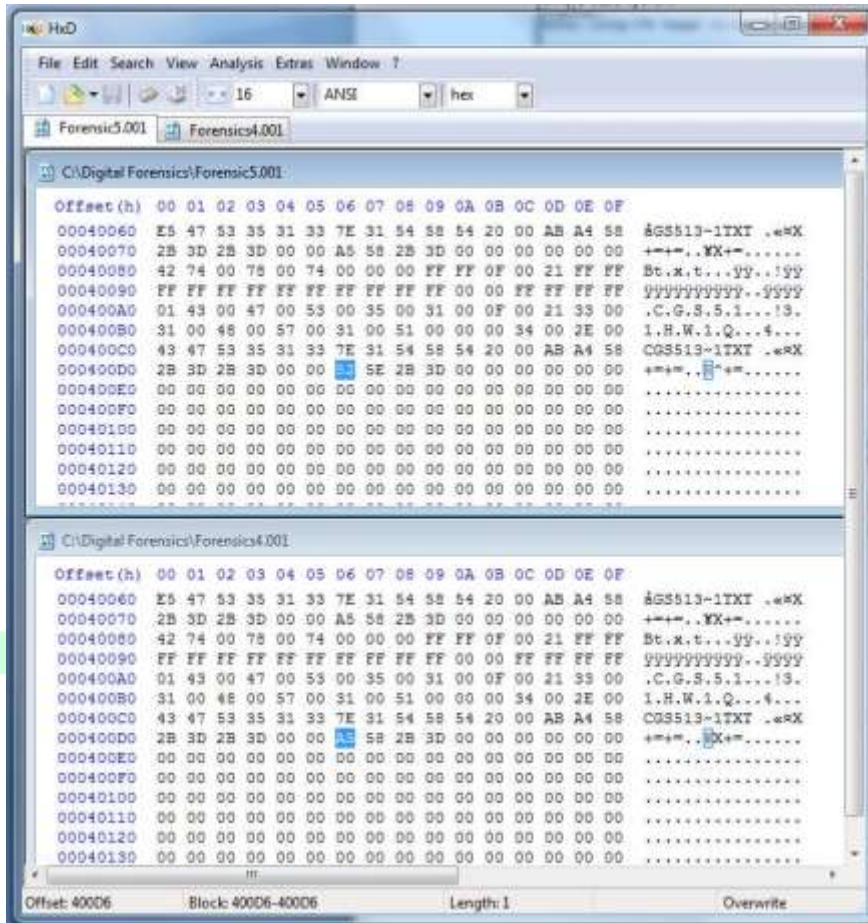
ATTENTION:
The following sector(s) on the source drive could not be read:
3243584 through 3248543
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
MD5 checksum: 5c9dfe456daf6c7d812ddaeeadf2
SHA1 checksum: eba0ce07bab38edb1323c8f36c69fc8bc4e7a7bd

Image Information:
Acquisition started: Sat Sep 11 11:57:31 2010
Acquisition finished: Sat Sep 11 12:13:01 2010
Segment list:
C:\Digital Forensics\Forensic5.001
C:\Digital Forensics\Forensic5.002
```

- f. The Hex editor HxD was used to identify the differences between two images of (b) and (d).

This was achieved through selecting Analysis > File-Compare > Compare and then selecting the 2 images to be compared.



There was only one bit offset that had a difference as shown in the figure above.

Offset 000400D0 - 06 was 52 in the image of step (d) while it was A5 in the image of step (b).