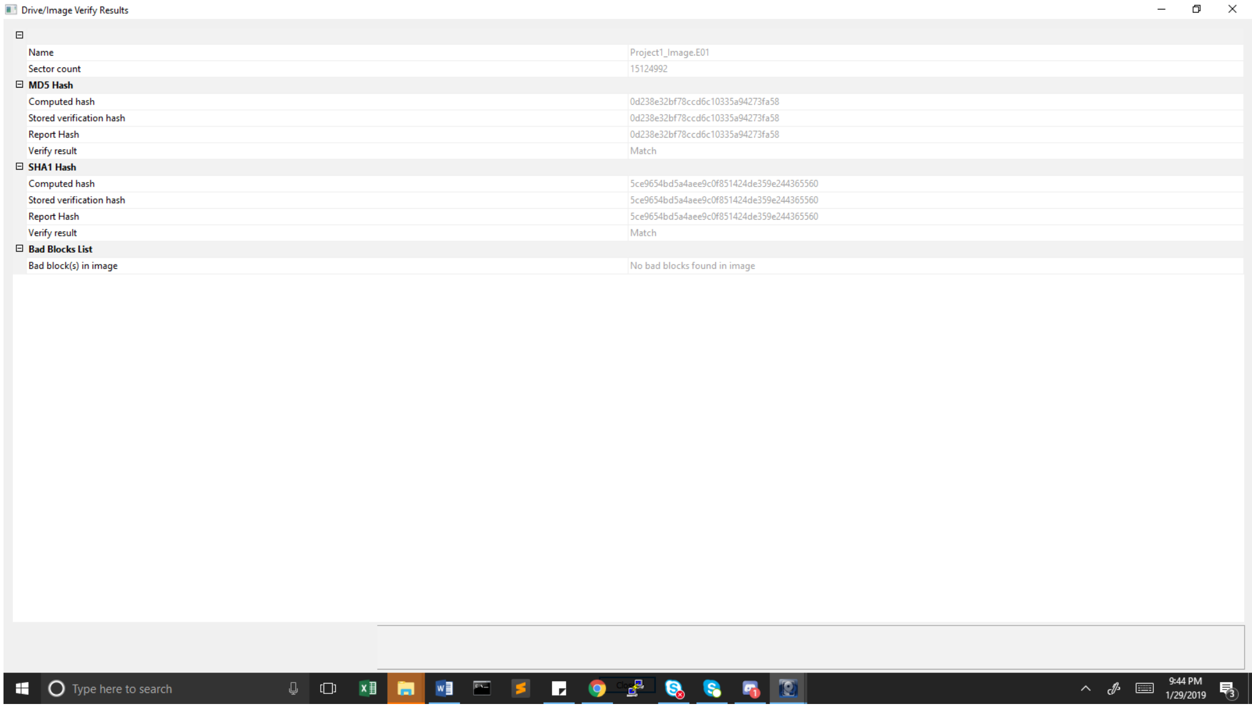
Edgar DeGuzman

CIS484

-

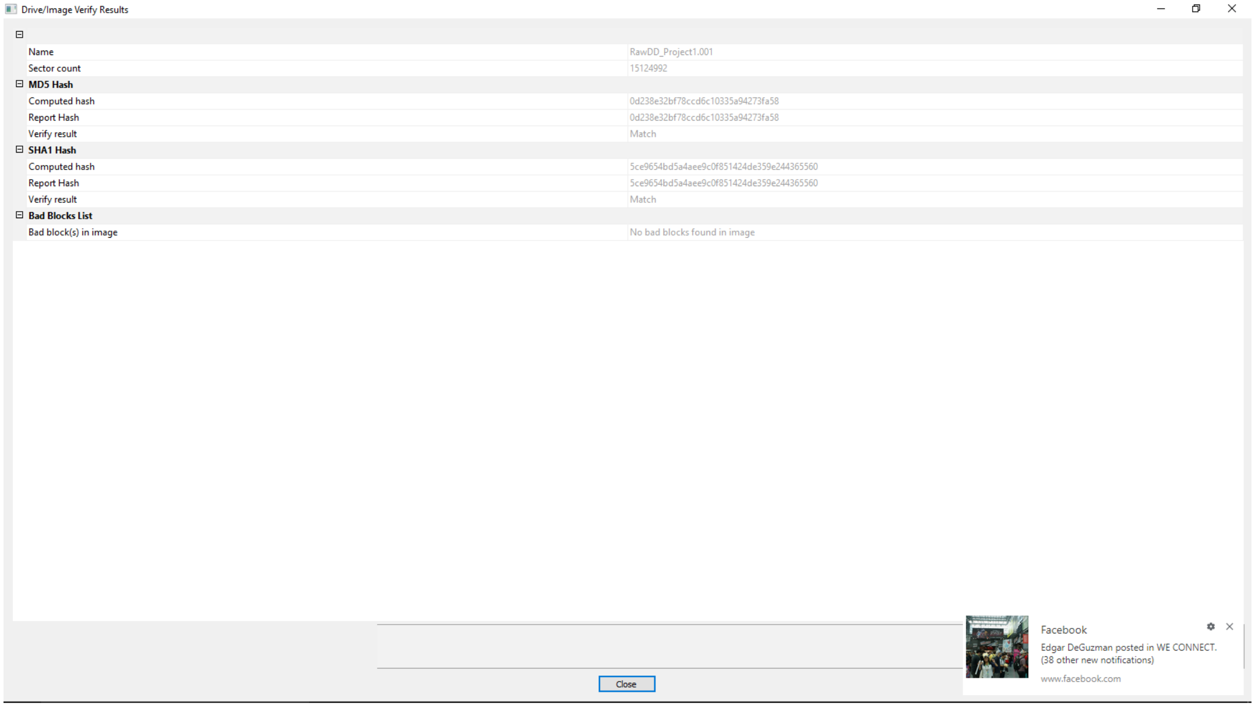
a. 

Drive/Image Verify Results

Name	Project1_Image.E01
Sector count	15124992
MD5 Hash	
Computed hash	0d238e32bf78ccd6c10335a94273fa58
Stored verification hash	0d238e32bf78ccd6c10335a94273fa58
Report Hash	0d238e32bf78ccd6c10335a94273fa58
Verify result	Match
SHA1 Hash	
Computed hash	5ce9654bd5a4aee9c0f851424de359e244365560
Stored verification hash	5ce9654bd5a4aee9c0f851424de359e244365560
Report Hash	5ce9654bd5a4aee9c0f851424de359e244365560
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

b. The verification option indicates that the creation of the disk image was successful. This option lets you see the information in relation to the file such as the hash and other significant properties. This lets the user compare the hash values to ensure that there was no corruption of the file. This is important in acquiring evidence for the real-world application.

c. When you make the directory listing, it makes several folders that are under Partition and Unpartitioned. The partition folder has two subfolders that are root and unallocated space. The unpartitioned space allows space for unallocated files. Under root, it lists the files that are in the USB drive. This drive only has two folders designated for lab assignments in prior classes. This can be applied to a forensic examination when trying to retrieve digital evidence within these drives or other types of hardware.

- 

Drive/Image Verify Results

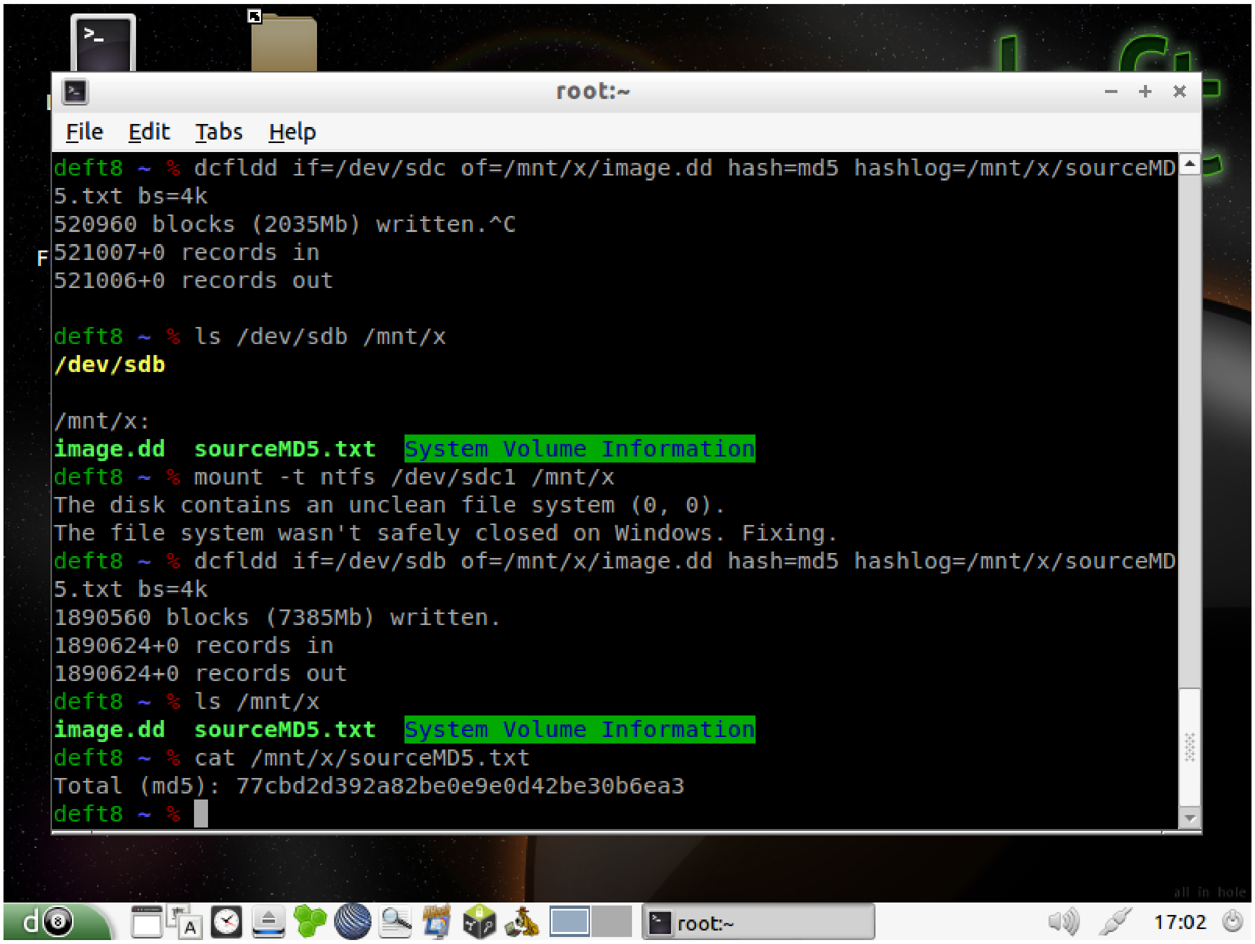
⊟	
Name	RawDD_Project1.001
Sector count	15124992
⊟ **MD5 Hash**	
Computed hash	0d238e32bf78ccd6c10335a94273fa58
Report Hash	0d238e32bf78ccd6c10335a94273fa58
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	5ce9654bd5a4aee9c0f851424de359e244365560
Report Hash	5ce9654bd5a4aee9c0f851424de359e244365560
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

Facebook

Edgar DeGuzman posted in WE CONNECT. (38 other new notifications)

www.facebook.com

The benefit in using a raw is having the ability to investigate the image using standard Linux tools. However, the disadvantage with raw files is that it does not contain any metadata. It is just a copy of the original data. However, the E01 is able to list the properties and data of the image.

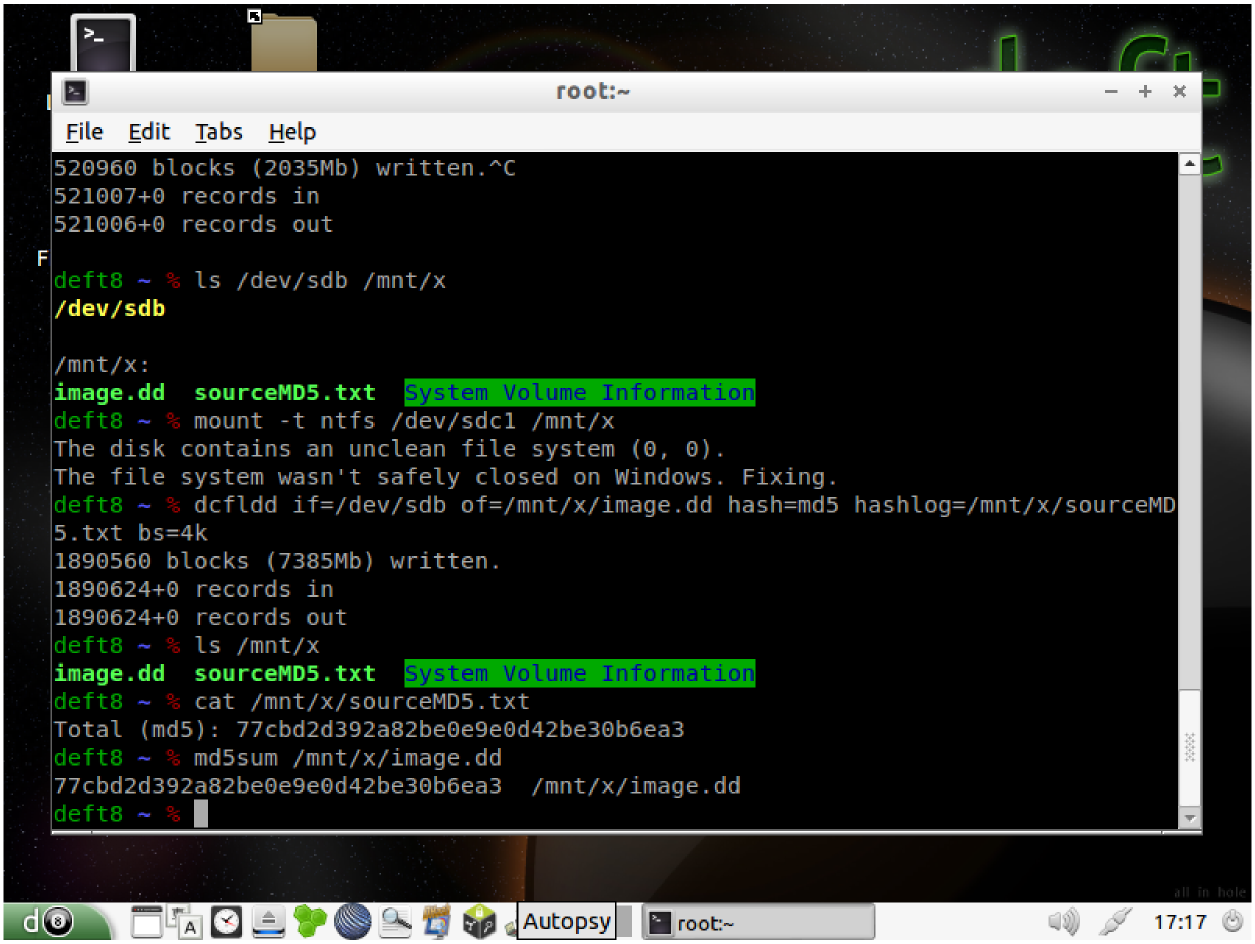


```
deft8 ~ % dcfldd if=/dev/sdc of=/mnt/x/image.dd hash=md5 hashlog=/mnt/x/sourceMD
5.txt bs=4k
520960 blocks (2035Mb) written.^C
521007+0 records in
521006+0 records out

deft8 ~ % ls /dev/sdb /mnt/x
/dev/sdb

/mnt/x:
image.dd  sourceMD5.txt  System Volume Information
deft8 ~ % mount -t ntfs /dev/sdc1 /mnt/x
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
deft8 ~ % dcfldd if=/dev/sdb of=/mnt/x/image.dd hash=md5 hashlog=/mnt/x/sourceMD
5.txt bs=4k
1890560 blocks (7385Mb) written.
1890624+0 records in
1890624+0 records out
deft8 ~ % ls /mnt/x
image.dd  sourceMD5.txt  System Volume Information
deft8 ~ % cat /mnt/x/sourceMD5.txt
Total (md5): 77cbd2d392a82be0e9e0d42be30b6ea3
deft8 ~ %
```

- The difference between imaging “dev/sdc” and “dev/sdc1 is that sdc1 is a partitioned drive while the other is not. If it is partitioned, then it is hard to retrieve the image when executing the dcfldd command

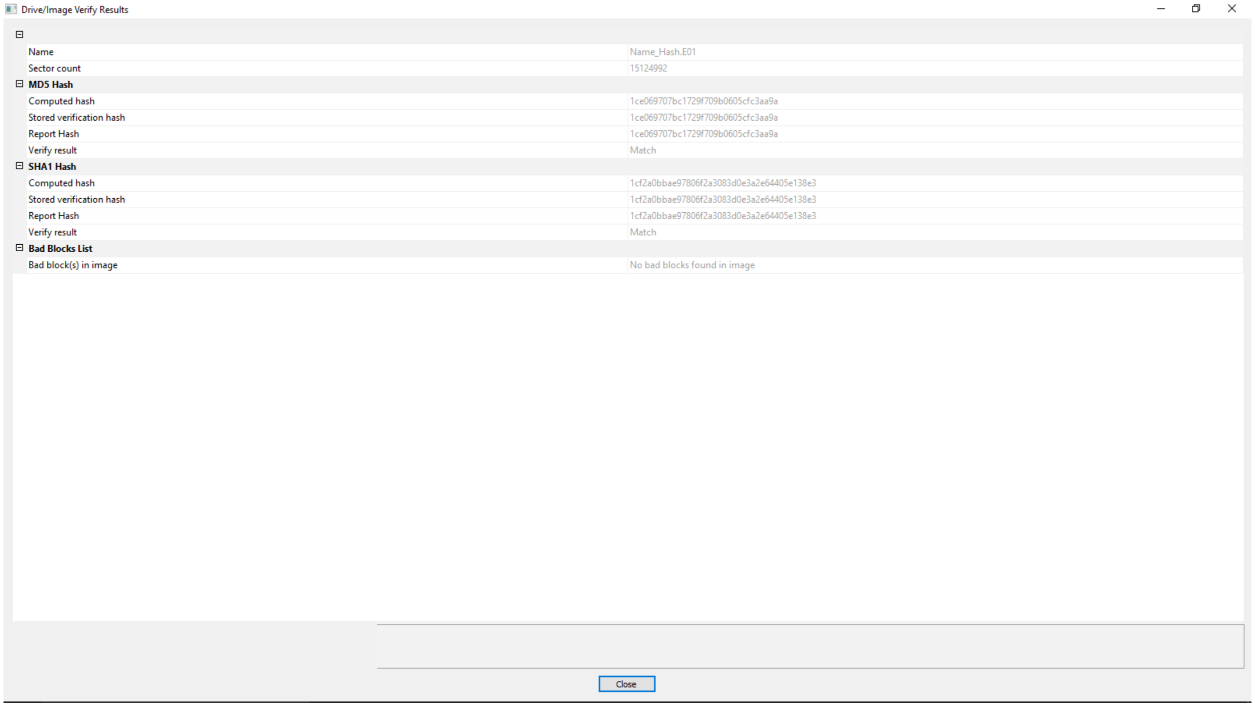
- 

```
520960 blocks (2035Mb) written.^C
521007+0 records in
521006+0 records out

deft8 ~ % ls /dev/sdb /mnt/x
/dev/sdb

/mnt/x:
image.dd  sourceMD5.txt  System Volume Information
deft8 ~ % mount -t ntfs /dev/sdc1 /mnt/x
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
deft8 ~ % dcfldd if=/dev/sdb of=/mnt/x/image.dd hash=md5 hashlog=/mnt/x/sourceMD
5.txt bs=4k
1890560 blocks (7385Mb) written.
1890624+0 records in
1890624+0 records out
deft8 ~ % ls /mnt/x
image.dd  sourceMD5.txt  System Volume Information
deft8 ~ % cat /mnt/x/sourceMD5.txt
Total (md5): 77cbd2d392a82be0e9e0d42be30b6ea3
deft8 ~ % md5sum /mnt/x/image.dd
77cbd2d392a82be0e9e0d42be30b6ea3  /mnt/x/image.dd
deft8 ~ %
```

  - Md5sum /mnt/x/image.dd
  - Hash Value: 77cbd2d392a82be0e9e0d42be30b6ea3
- After executing the cat command for the small flash drive, the output of the hash value of the image and the calculated hash value match. This means that the image is the same and was not corrupted.

- 

Drive/Image Verify Results

⊟	
Name	Name_Hash.E01
Sector count	15124992
⊟ **MD5 Hash**	
Computed hash	1ce069707bc1729f709b0605cfc3aa9a
Stored verification hash	1ce069707bc1729f709b0605cfc3aa9a
Report Hash	1ce069707bc1729f709b0605cfc3aa9a
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	1cf2a0bbae97806f2a3083d0e3a2e64405e138e3
Stored verification hash	1cf2a0bbae97806f2a3083d0e3a2e64405e138e3
Report Hash	1cf2a0bbae97806f2a3083d0e3a2e64405e138e3
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

  - The hashes do match. This means that this is the same image that is being used and has not been corrupted.
  - When enabling the USB write-blocker I was not able to write a file to the thumb drive when I had it to read-only. When I calculated the hash value of the USB device, it outputted the same hash value as the previous value that is shown above. This is a forensically sound process because the USB device is protected and remains the same, while the investigator is conducting forensics on it.

5. Comparing FTK and dcfldd
   a. The advantage in using FTK Imager is that it is fairly easy to use, especially for those who do not have a strong technical knowledge. It allows the use of a GUI to navigate through and use. It gives you different options of formatting such as E01 and RawDD. Depending on what is needed, the appropriate format can be chosen for that situation. However, depending on how large the image is, it can take a while to load. The advantage in dcfldd is that it can be faster as it uses the terminal. The disadvantage in using this tool is that it requires a lot of technical knowledge as there is no GUI, but rather a terminal to enter commands. If the user is inexperienced with this tool, then it can be difficult. Also, you would have to mount the devices so that you can navigate between them.
   b. If I were a forensic imager, I would use FTK imager. This allows me to choose the type of image format and have access to the different drives I have connected to my machine rather than mounting them.
6. Hardware and Software Used
   a. Fujitsu Lifebook T902
   b. Sandisk 16.0 GB USB Drive
   c. USB Drive 2.0 USB Device 8.0GB
   d. VMWorkstation
   e. Deft 2018

f. USB Write-Blocker
g. FTK Imager