Rob Stewart

Digital forensics

Table of Contents

[Tools Used 2](#_Toc21263525)

[Methodology 3](#_Toc21263526)

[Case 1 3](#_Toc21263527)

[Case 2 8](#_Toc21263528)

[Results 12](#_Toc21263529)

[Conclusion 13](#_Toc21263530)

# Tools Used

* Laptop
* Deft bootable USB
* Windows 10
* Evidence USB 1
* Evidence USB 2
* GetData forensic imager (Windows)
* Guymager (Deft Linux)

# Methodology

# Case 1

1. USB is mounted in read only mode, the USB is named Transcend and beside the name is a green circle with a black, pointing up arrow which indicates it’s in read only mode, furthermore, terminal highlights the USB and details about it such as size and file path identifiers.

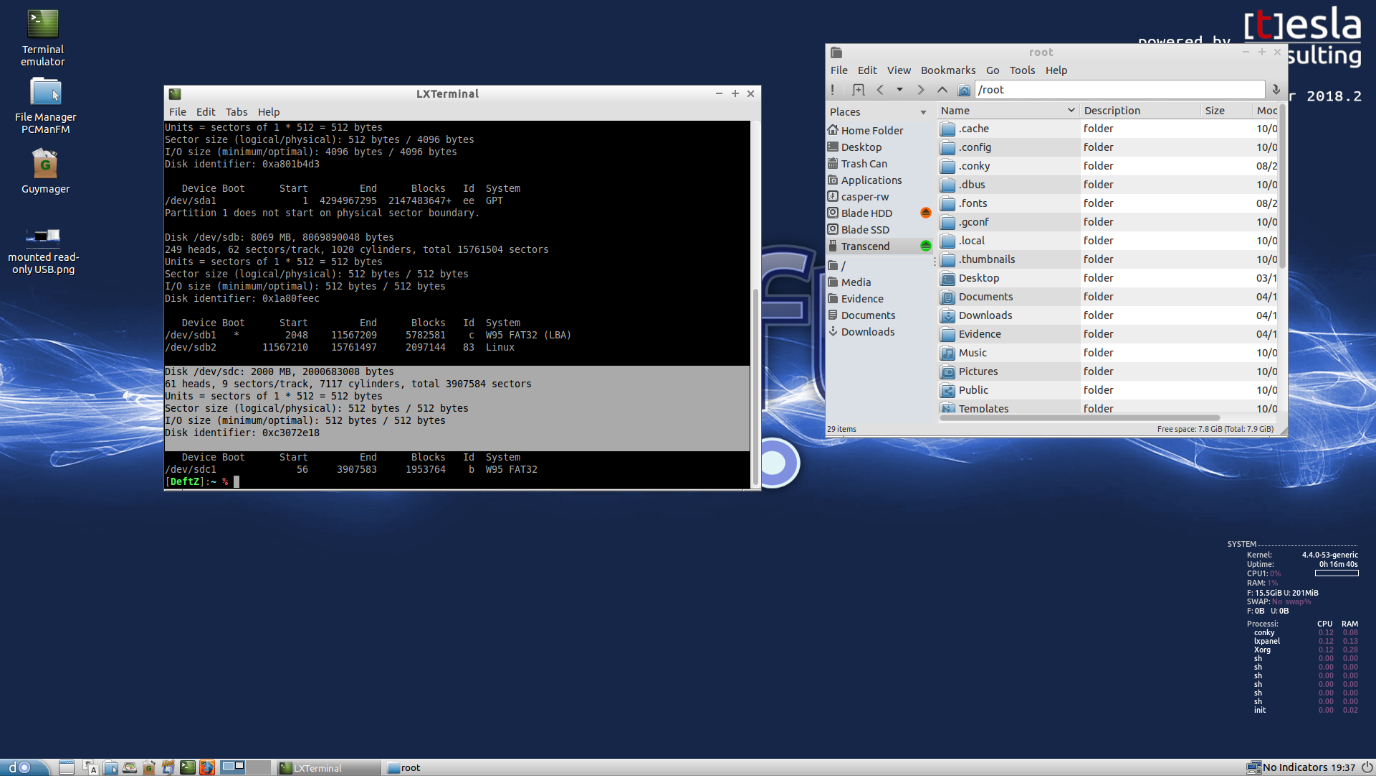


Figure 1: USB mounted in read-only mode

1. MD5 hash can be seen highlighted in the terminal and is also visible in the text file

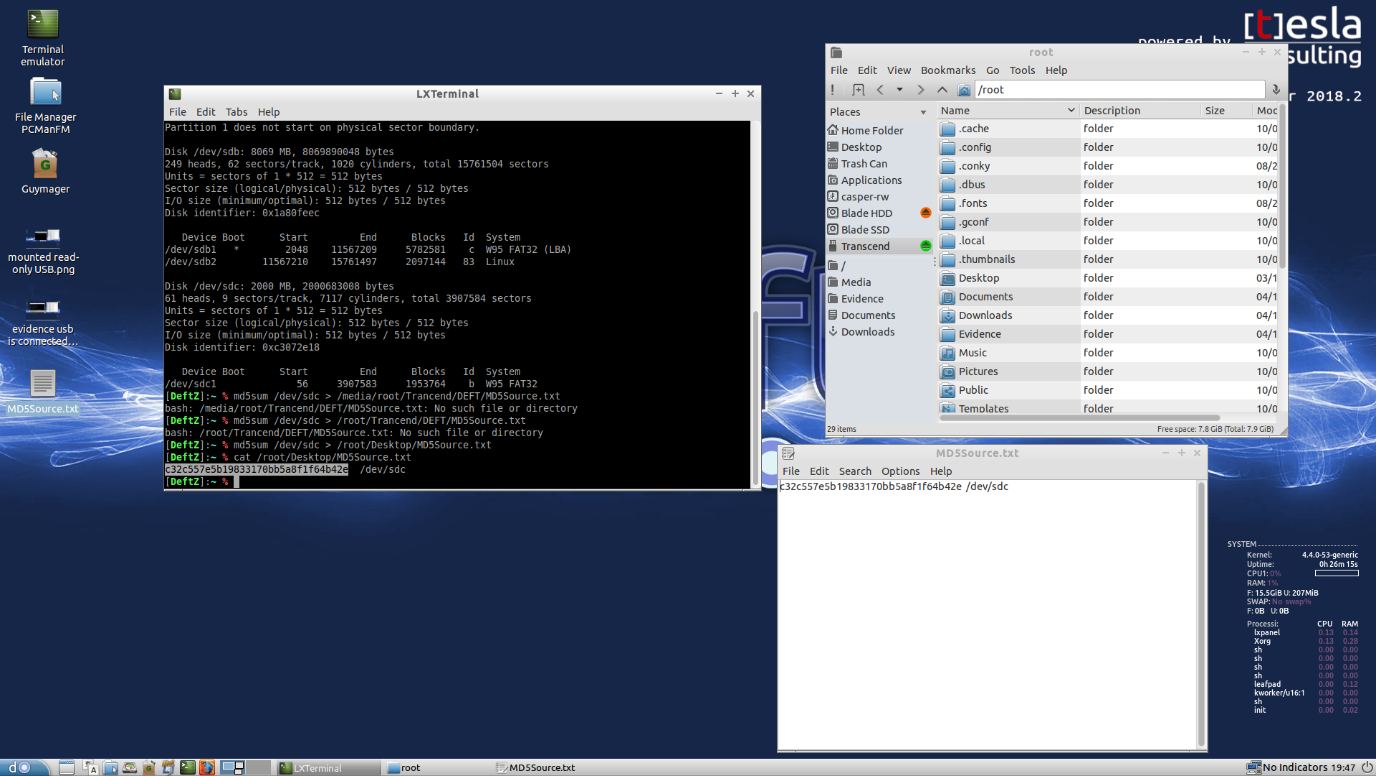


Figure 2: MD5 hash screenshot

1. SHA1 hash can be seen highlighted in the terminal and is also visible in the text file

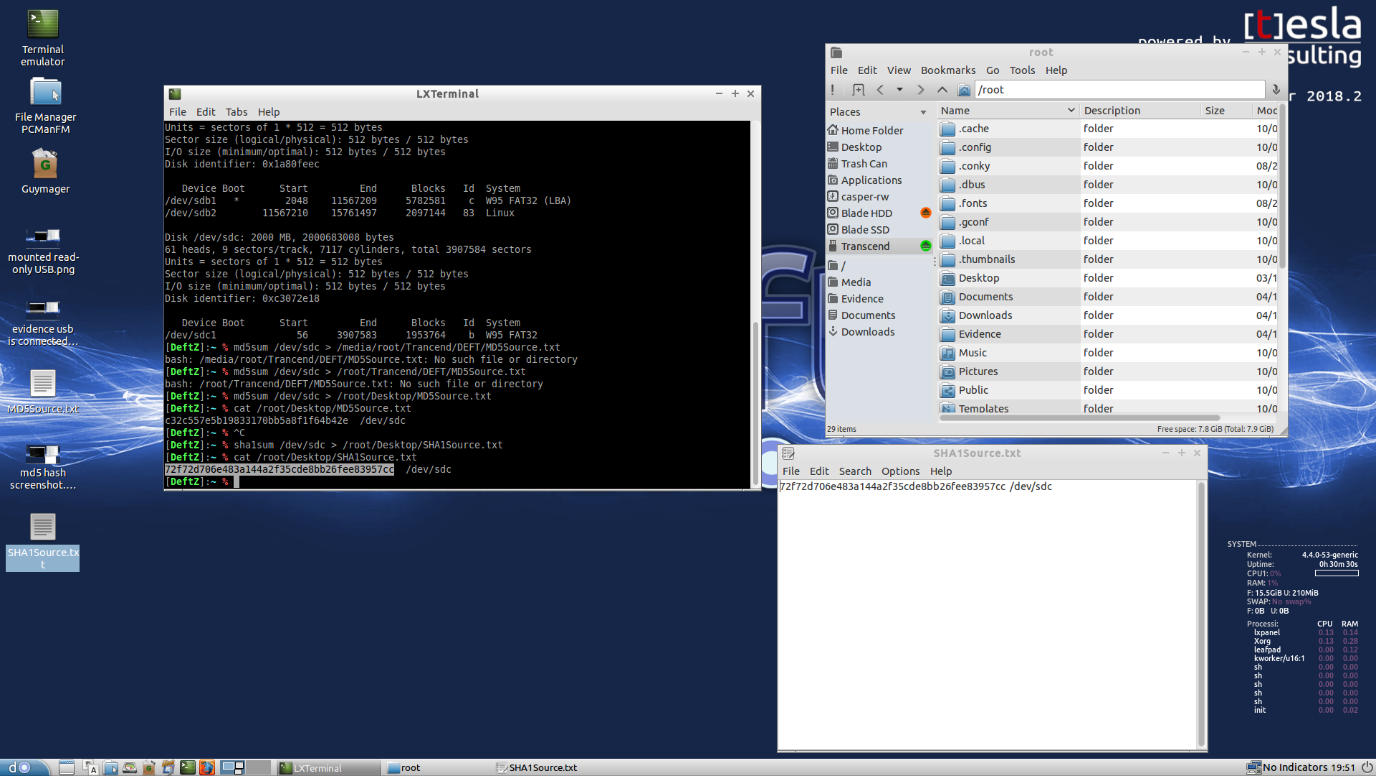


Figure 3: SHA1 hash screenshot

1. Guymager proves that the USB has not been modified since been plugged in as the MD5 and SHA1 hashes match the previous figures evidence, this can be seen in both the terminal and .info file.

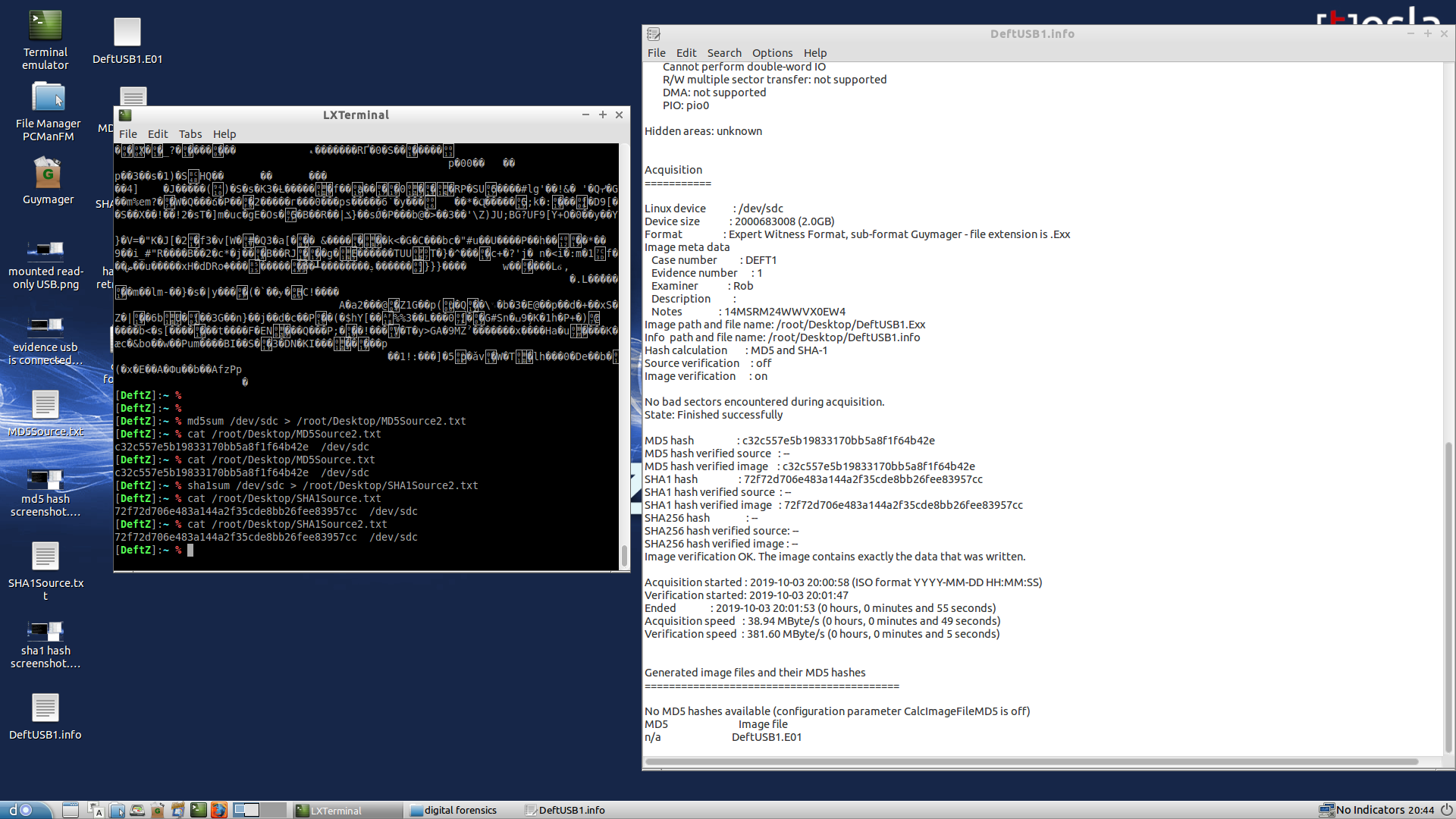


Figure 4: Guymager hashes

1. GetData forensic imager shows that the MD5 and SHA1 hashes have changed, they do not match what was seen in Deft, proving that windows definitely modifies the same USB once it’s inserted.

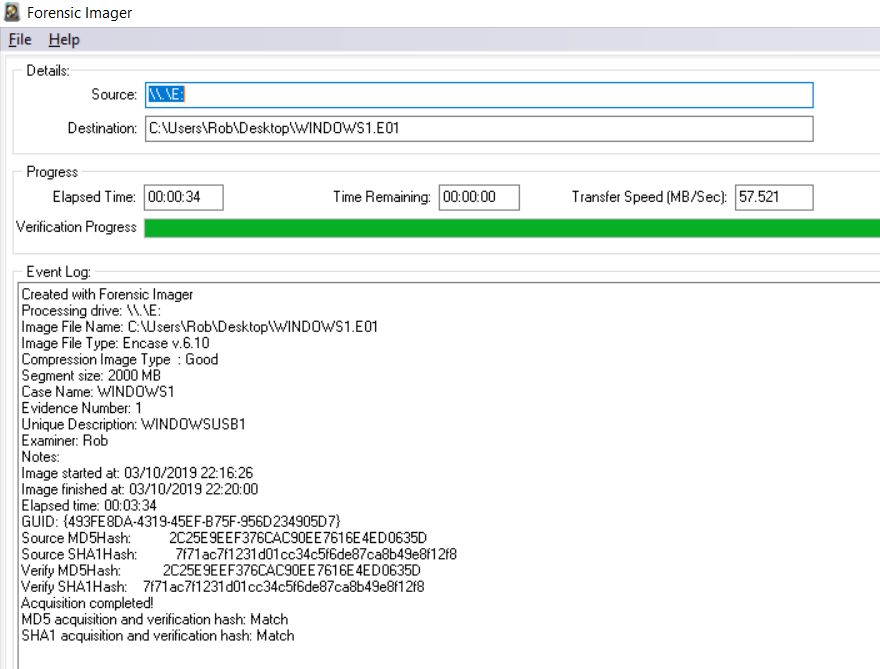


Figure 5: GetData MD5 & SHA1 hashes

1. A second check proves the new hashes are remaining unchanged, used the notepad version to make for easier reading.

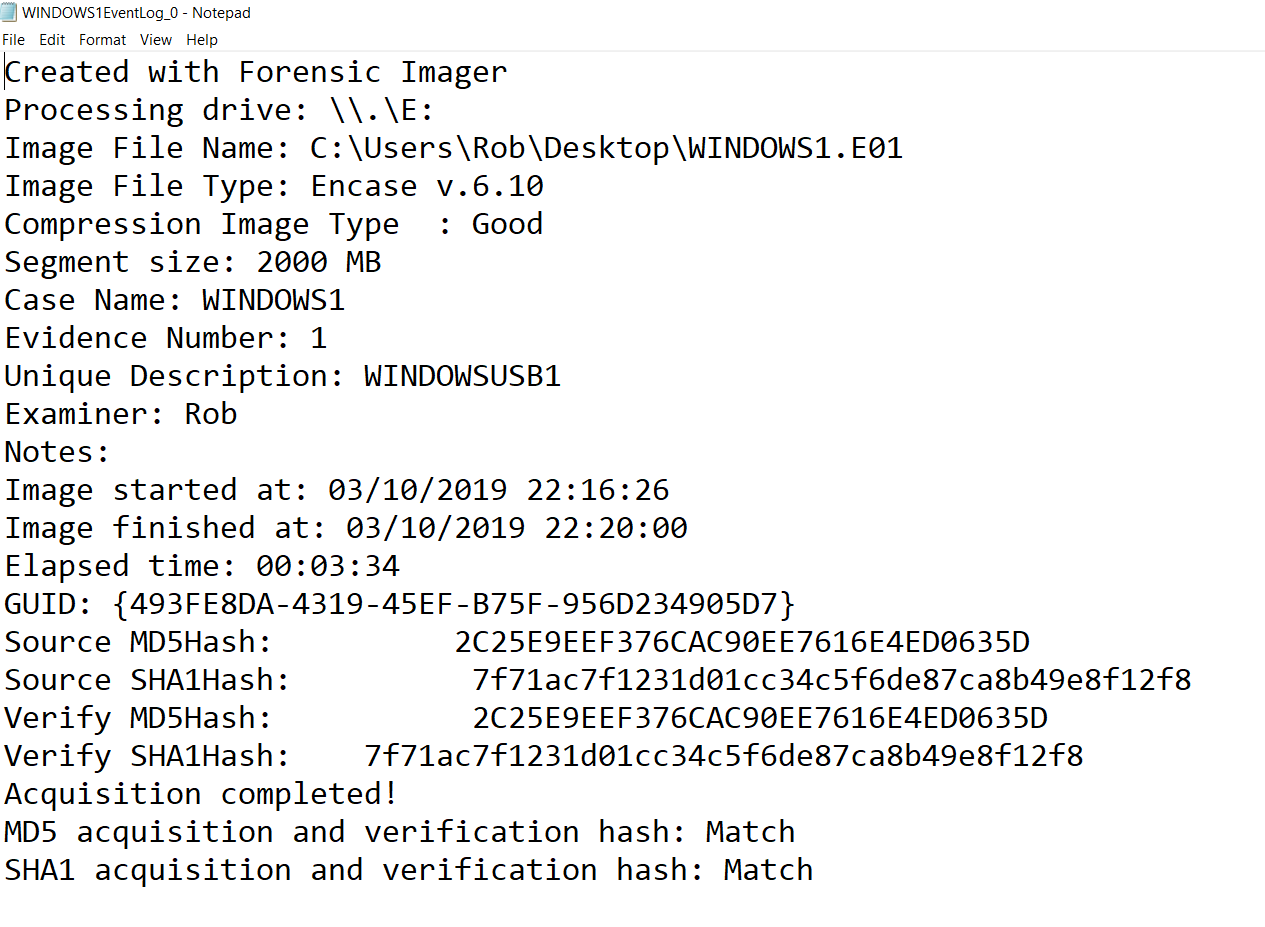


Figure 6: second Windows check

# Case 2

1. Like Windows case 1, GetData forensic imager was used to obtain the second USBs MD5 and SHA1 hashes.

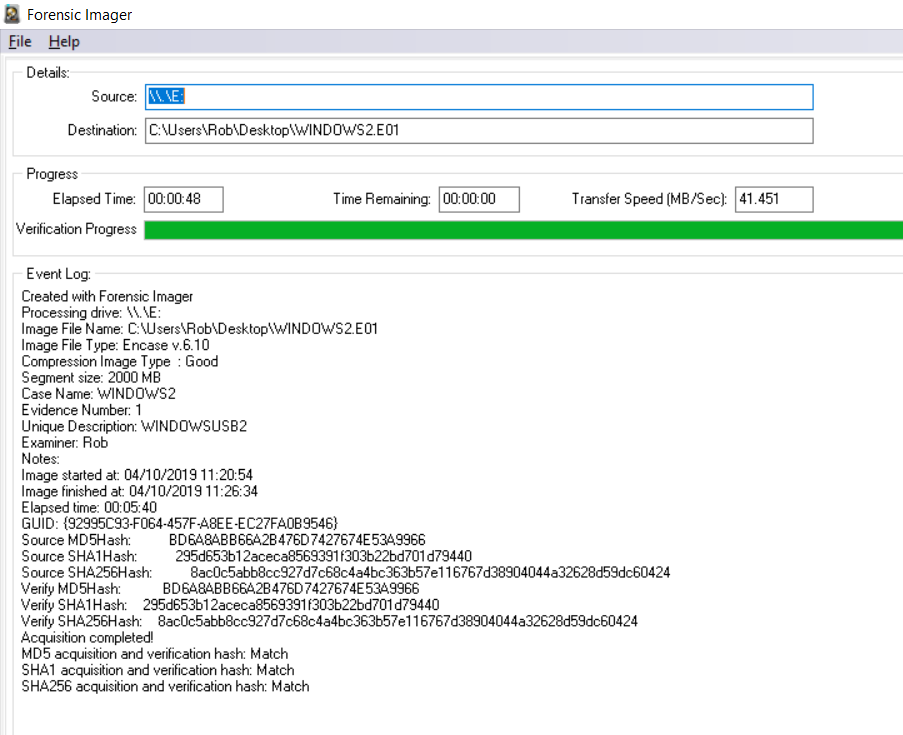


Figure 7: GetData MD5 & SHA1 hashes

1. Second scan shown in notepad for more clarity, the hashes here match the first hashes GetData obtained.

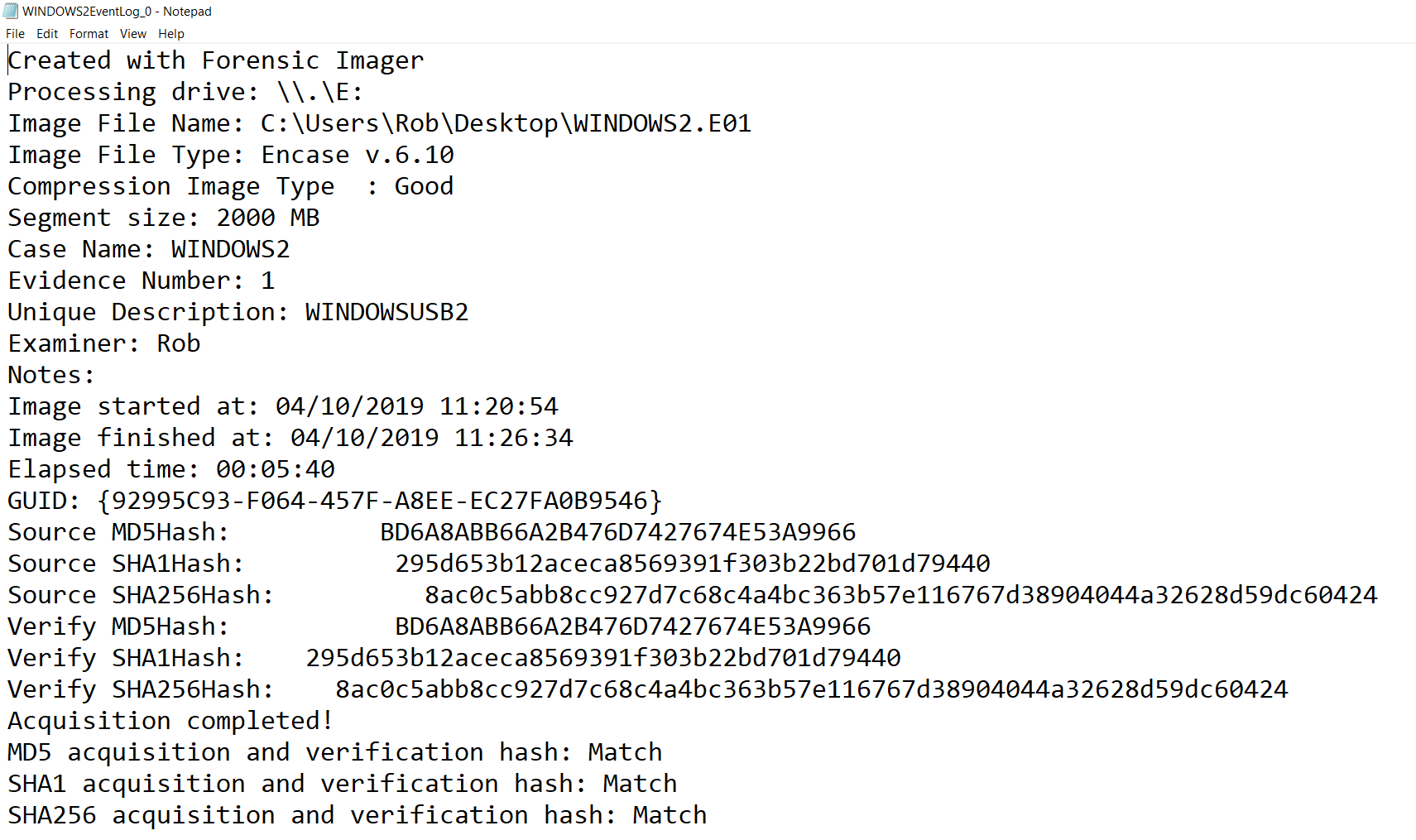


Figure 8: second Windows check

1. For the second Deft check the same steps are taken that were made in case1 figure 1, the name of evidence USB 2 is the same as evidence USB 1, all other details should match too as the size and format of both USBs are the same.

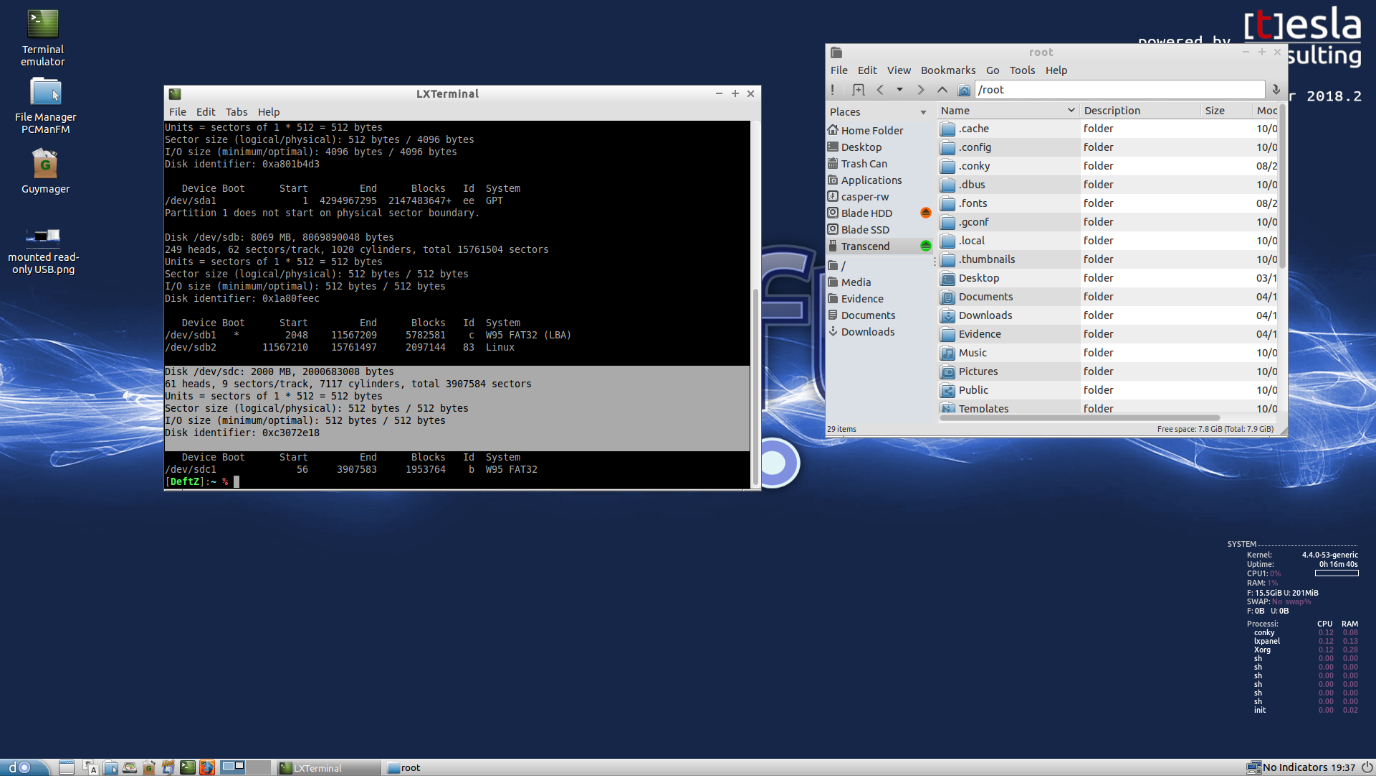


Figure 9: second USB mounted in read-only

1. MD5 hash is highlighted in the terminal window and is visible in the text file. Unexpectedly this hash does not match the MD5 hash seen in windows.

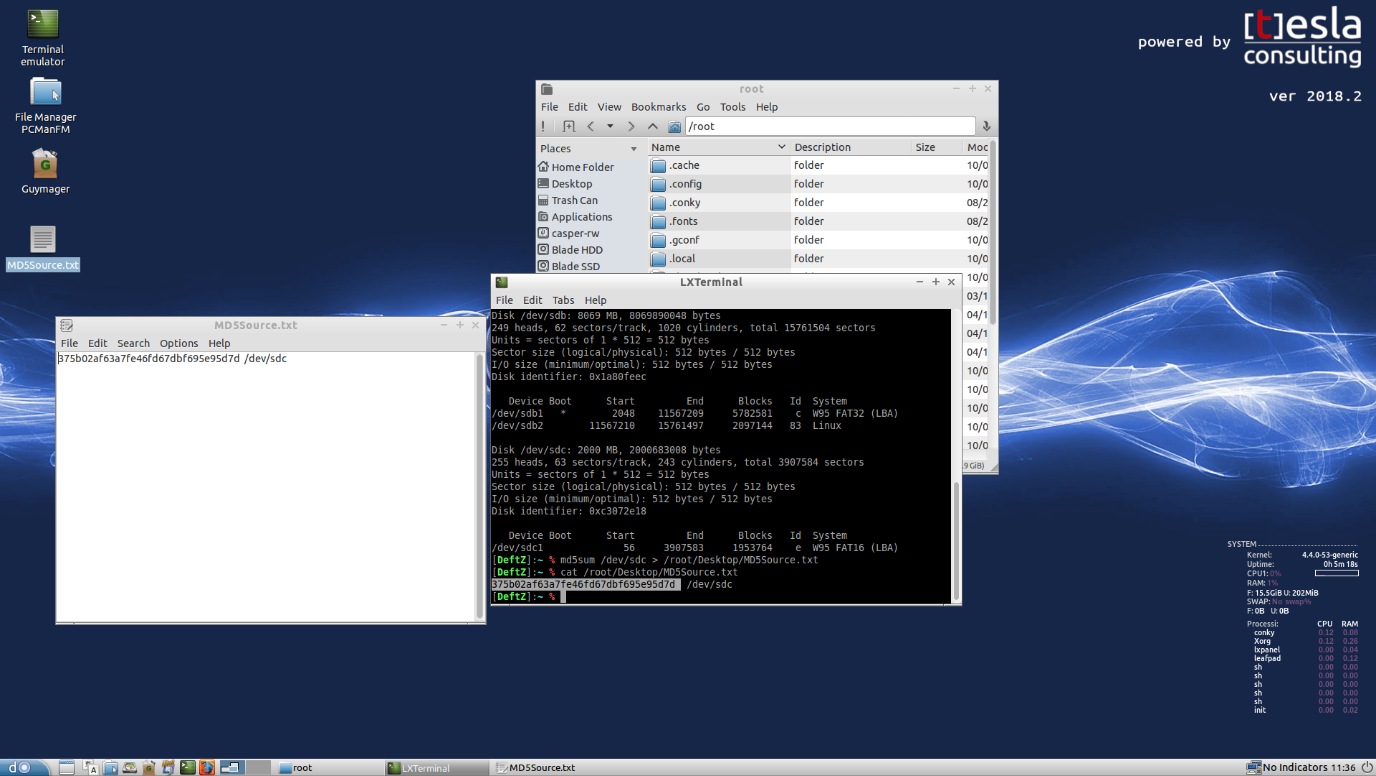


Figure 10: MD5 hash

1. SHA1 hash is highlighted in the terminal window and is visible in the text file. Expectedly this hash does not match the SHA1 hash seen in windows because the MD5 hash in the previous figure 10 does not match, overall this is unexpected.

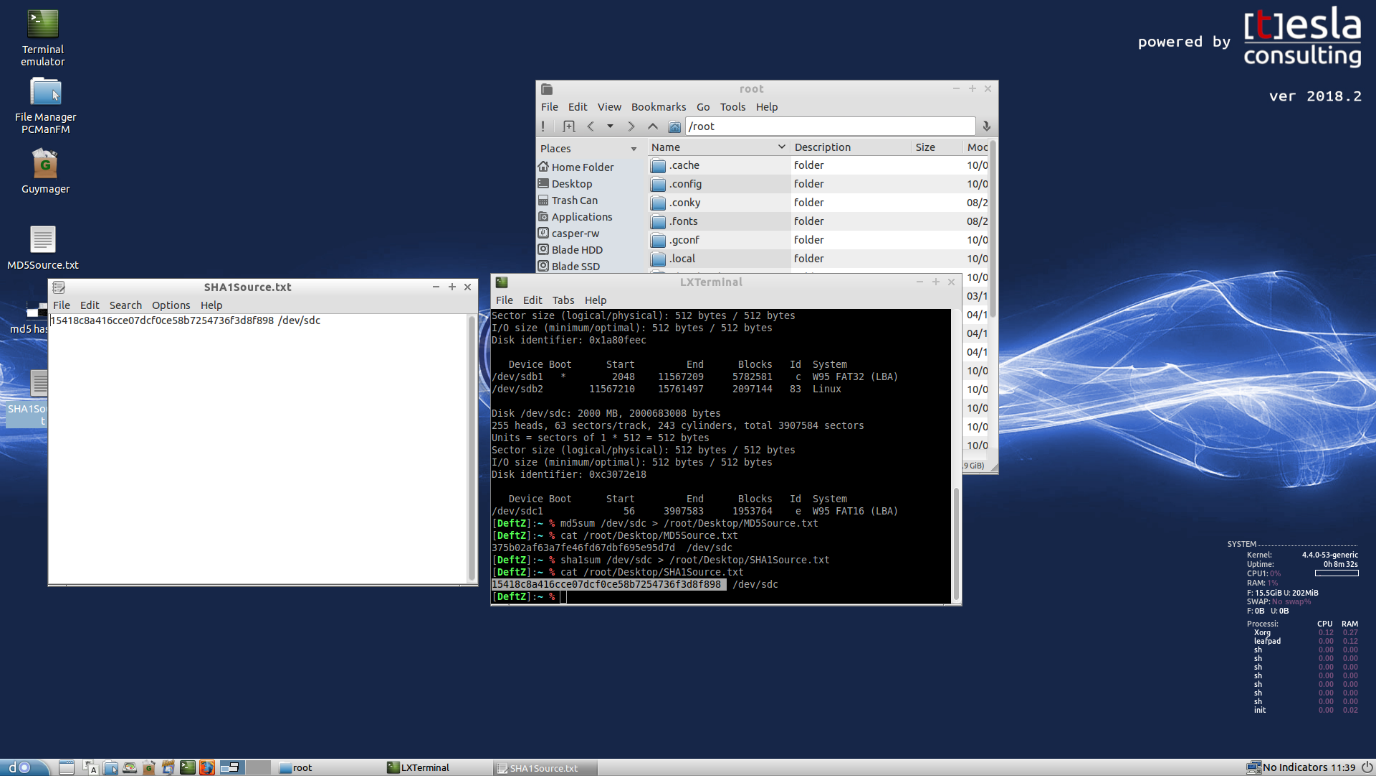


Figure 11: SHA1 hash

1. The second check hashes with Guymager do match the first checks as seen in the terminal and info file, but they still do not match the Windows hash values.

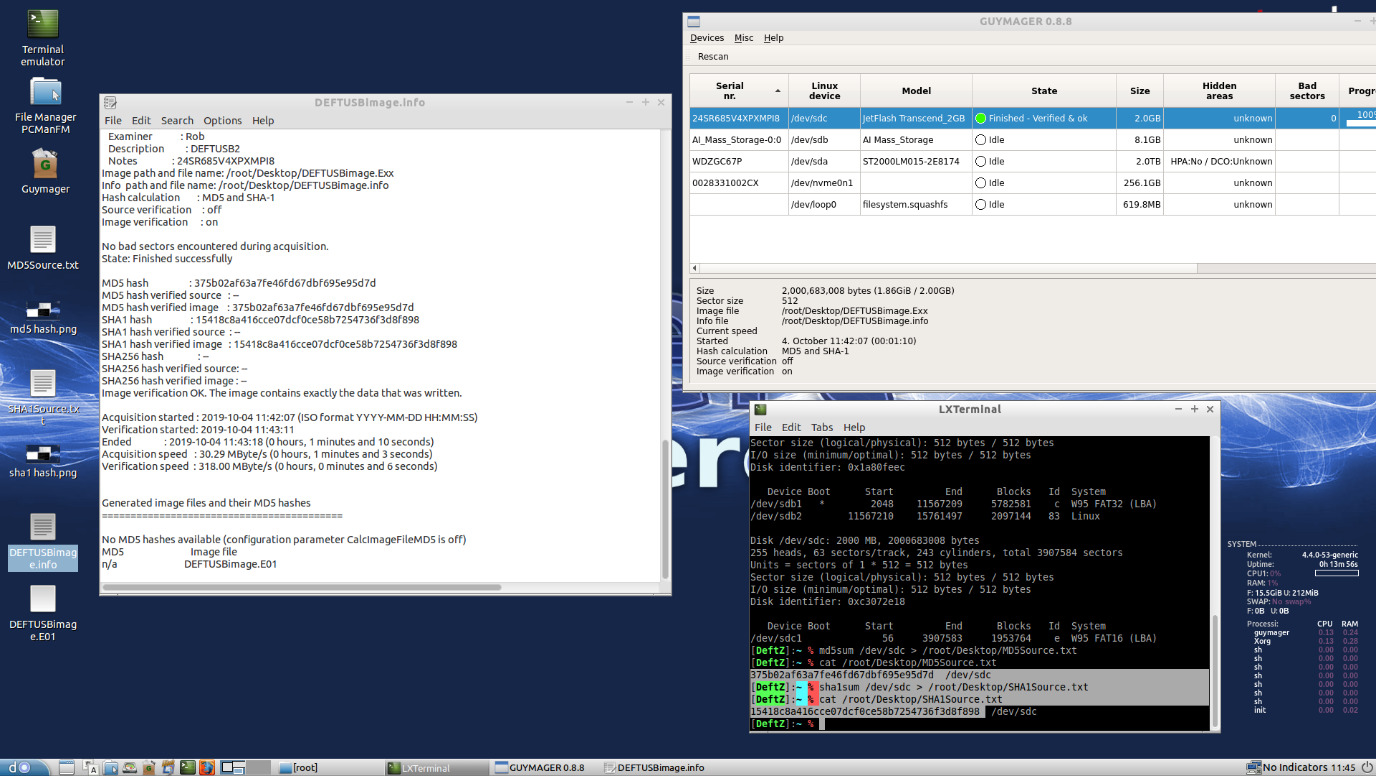


Figure 12: Guymager MD5 & Hash second check

# Results

With evidence USB 1, it was proven that Windows makes changes to the USB when plugged in.

With evidence USB 2, it was unexpectedly further proven that Deft makes changes to the USB, despite being mounted in read only mode.

Upon further investigation it was discovered that GetData was taking an image of the partition rather than an image of the entire drive, Guymager was getting an image of the entire drive. FTK Imager works around this problem and most importantly proves that Deft does not make changes to a USB mounted in read only mode, where windows will make changes the moment the USB is connected.

First hand evidence of this cannot be provided because FTK Imager while free, is requiring that personal details are entered before it can be downloaded, this is an unsatisfactory requirement on their behalf.

# 

# Conclusion

Windows should not be used to obtain a forensic image without using a write-blocker, as it makes changes to the USB which is evident in the different hashes.

Furthermore, going by the results from evidence USB 2, Deft should not be used either despite it being designed for forensic purposes.

Overall expected results weighed up against actual results, proves to be inconclusive.

**Update on original conclusion:**

GetData takes an image of the partition where Guymager takes an image of the entire drive, FTK Imager over comes this problem but requires personal data before it can be downloaded.

Final expected results, Windows will make changes to a USB unless a write-blocker is used, Deft will not make changes so long as it’s mounted in read-only mode.

Actual results prove true when FTK Imager is used.