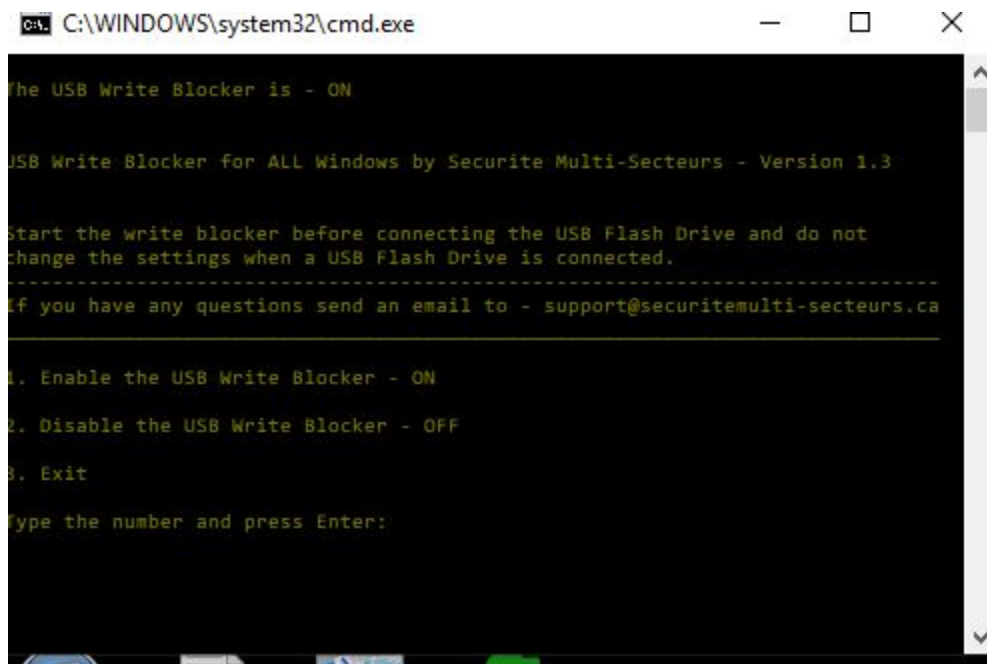


Philip Herman  
DFR 1001  
Professor Schmeelk  
7 October 2019

## Lab 2

The first thing I did was to make sure the USB was write blocked. I did this so no damage could be potentially done to the USB when analyzing the data. Here is a picture of the USB being write blocked.



```
C:\WINDOWS\system32\cmd.exe

The USB Write Blocker is - ON

USB Write Blocker for ALL Windows by Securite Multi-Secteurs - Version 1.3

Start the write blocker before connecting the USB Flash Drive and do not
change the settings when a USB Flash Drive is connected.
-----
If you have any questions send an email to - support@securitemulti-secteurs.ca

1. Enable the USB Write Blocker - ON
2. Disable the USB Write Blocker - OFF
3. Exit

Type the number and press Enter:
```

The next step I took was to use FTK imager and analyze the data on the hard drive under .dd file. Here is the image of the data being analyzed in FTK imager. The results show the MD5 and SHA1 hash.

Drive/Image Verify Results	
Name	bb2.001
Sector count	983040
MD5 Hash	
Computed hash	0b39b299f0d6b113e6ea1112775fa128
Report Hash	0b39b299f0d6b113e6ea1112775fa128
Verify result	Match
SHA1 Hash	
Computed hash	4d9ca10fe5d527a0251ccea00dba103187d2558c
Report Hash	4d9ca10fe5d527a0251ccea00dba103187d2558c
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

Lastly I hashed the images using MD5summer and here are the results. It shows the MD5 hash of each image on the USB drive.

fs.eventsnd/fs.eventsnd-uuid	ab270e6349a0b1d0ba05fa04a30092EE0
fs.eventsnd/00000000000594957	3ed219e7b22136141a5647507e6dF9
fs.eventsnd/0000000000059498	bacl20f2596ac259441d44d81ce5f2cb9
Spotlight-V100/VolumeConfiguration.plist	82a3d4312a73d56dcf47e445e2ddc8f
pics2/24200.jpg	754db4905c4e512da75e030e0b5f9d0
pics2/birthday_party.jpg	55a940210e2f5fe706ac2020e031764
pics2/delorean.JPG	75c3499e4c6c6739c0688ba070448ca1
pics2/delorean1.jpg	35159b442770159750b44d1839f720ae
pics2/Lightning-McQueen.jpg	bd5fca0d6f9cf71240dF40f64abbf3f
pics2/yard.jpg	21a70fb67db495ba4f9cf6ddcccd9f0
System Volume Information/WFSettings.dat	b9369e668c314b1b3da1fc66aaccff635
System Volume Information/IndexedVolumeGuid	b824a235c739c97266a1750051cf300

The difference between this part of the lab 1 and lab 2 is that it hashed different files in the MD5summer. As you can see in this picture below the results from Lab 1.

MD5sums: Generating...	
File	MD5 Hash
cat breeds.jpg	6e47146b10f0099de211f9d2c5f66b22
cat_kitten_cute.jpeg	3e786ebc792ff7f657fc33b5019ad2e
cats grass kittens tree trunk.jpg	d6e9f43fab4a4e3573f150fd62a5f3b
cats=cat.jpg	17ab203ca4f0b274205c324e9014c04e
Cute-3-cats.jpg	3539c0ec581d9ec5573b2f5155e67004
Cute-Cats-cats.jpg	20d3fda484aa2aa930ecfa595f75f194
Cute-cats-cuddling-1.jpg	de93a0e4337b1777695f30f6c0e4a9b
Cute-Cats.jpg	67f1f0c01954b1b1b5dc5c308da20b42
cute_cat.jpg	f6b0557d60043c10432c6a994da10
Halloween-1.jpg	bae4038f0c12b7593e9656a835273aa7
lots-of-cats.jpg	a9e7d68c0c5970778896d6902b51a93b