

Validation Testing

Purpose

Thumbscrew is a Software USB Write Blocker that allows you to quickly enable or disable writing to all USB mass storage devices on your Windows System. Which, in other words, means that you can make a USB flash drive, hard drive, or IDE/SATA drive in an enclosure read-only. So, I plan to use it to secure that my OS does not make any change in an external drive to avoid manipulation.

Equipment Necessary

- Access Data FTK Imager
- HashCalc
- HxD
- USB FlashDrive
- thumbscrew

Procedure

I will start with the simplest thing, I will plug a USB Flash Drive to see if it works. I will use both functions and try to write data in the device to see if it works. I plan to create a forensic image of the instance

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect to compare if the problem is doing the job or not. The program owner claims that what the program does to succeed is flipping a bit in the registry of this instance. So, after creating the forensic image for both the program working and not. After this, I will check the hash values for both forensic images to see if they have changed or not using HashCalc. After this process, I will

use HxD to check if there is a change in a bit. After all these tests, I will be able to realize if the program is working or not.

Expected results

I expect that both functions of the application work. I expect that “Make USB read-only” and “Make USB Writeable” do their work as expected, changing the bit in the registry.

