Validation Results Report

Purpose

As mentioned before, this is a tool that either allows or does not devices to write data. So, based on my research, if you plug a USB with the program on, you will not be able to add any information to the USB. If the program is off, you can use the USB as you are used to. The program changes a bit in the registry of HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect, making this possible to happen.

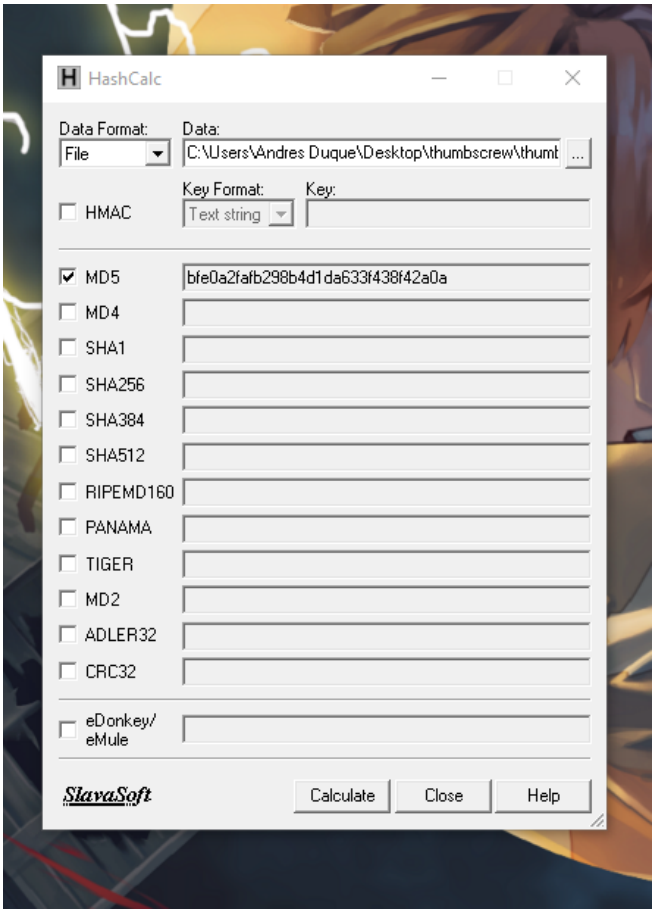
Equipment used

- Windows Registry Editor
- HashCalc
- HxD
- USB FlashDrive
- thumbscrew

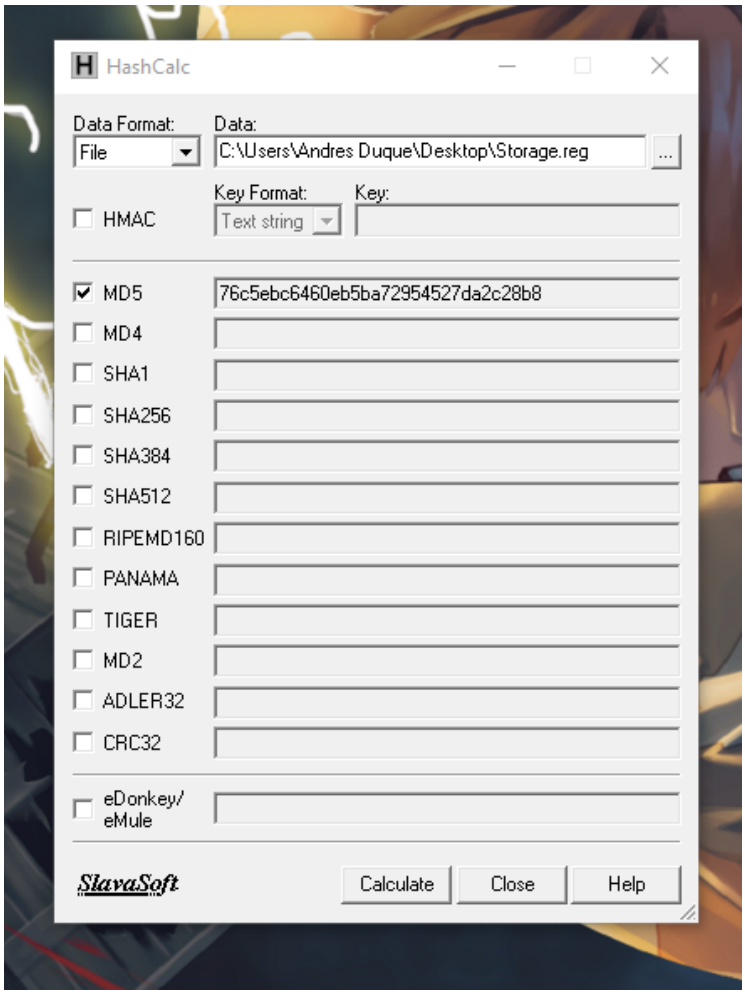
Procedure / Results Observed

The beginning of the testing was pretty simple; I used a USB Flash Drive and thumbscrew. Firstly, I execute the program thumbscrew, which by default set the USB as writable. Then, I plugged my USB into the computer to see if the USB was working correctly. As expected, I was allowed to do what a user can usually do with a USB. But, when I switched the program to make the USB read-only, there was a change. When I try to add a file to the USB, the OS shows a warning that does not allow me to add any files to the USB. So, I realized that the program was doing the job. In the beginning, I was thinking about creating a forensic image of the file "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteP

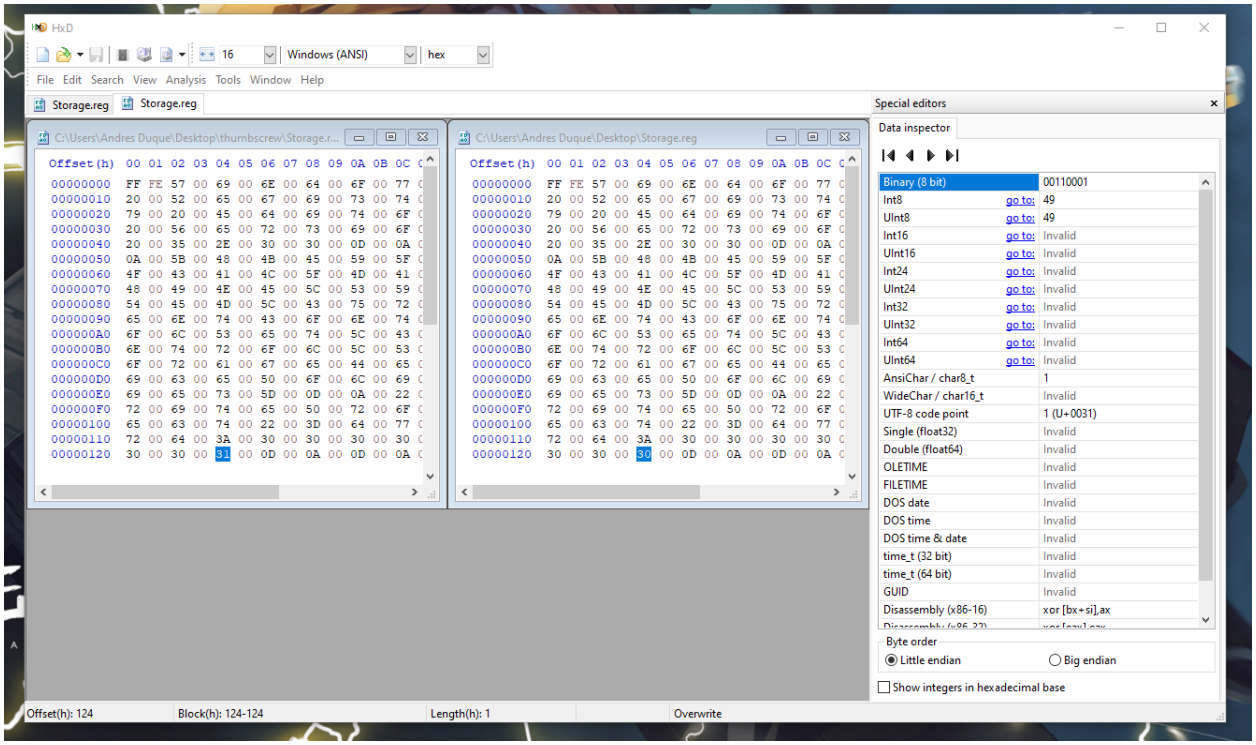
rotect" until I realized that accessing the file was not as easy as I thought. So, doing some research, I found that this file is accessible using other methods that I wasnt aware of at the beginning. So, I run the Run command using the Windows Key + R writing regedit in the command line. This command opens the Windows Registry Editor, where I was finally assemble to find HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect. After reaching out to WriteProtect, I decided to export the file to my desktop. Right after, I execute the program in the other mode and also export the results. First, I used the HashCalculator to check if the hash values were the same depending on if the program was on or not. Which I realized that using the program makes changes in that exact file generating different hash values. **Bfe0a2fafb298b4d1da633f438f42a0a** was the MD5 hash value found with the USB being writable.



While **76c5ebc6460eb5ba72954527da2c28b8** was the MD5 hash value found with the program in reading mode only.



After checking the hash values, I went to HxD to see the difference between those two. Where I found that in offset 124, the bit was changing.



So, I realized that what the owner said about the program just changing one bit was accurate, which is how the program works.

Conclusion

The program cannot be a reliable forensic tool because of some flaws, as the software owner mentioned. But, it does the job that it is target to do. The software changed one bit in the registry, making the write blocker effective.

Validation Details

Test Perform by: Andres Duque

Cyber Criminology Student at Florida State University

Test Performed in-house using a Mac Bootcamp windows machine on 10/15/2021.