

Write blocker

Digital Forensics

i22-1609

Ahmad abdullah

A grey logo on a black background

Description automatically generated

Table of Contents

[Introduction 2](#_Toc176553303)

[Details and Steps 2](#_Toc176553304)

[Summary 3](#_Toc176553305)

[References 4](#_Toc176553306)

# Introduction

In Cyber Security, Digital Forensics is an important field in which Digital Forensics Investigators (DFI) analyse any digital evidence that might be used to commit a crime. For this purpose, DFI must ensure the integrity of the evidence while also being able to analyse it.

One of the utilities that can be used to ensure the integrity of the evidence is a USB or other external drive is a Write Blocker. A Write Blocker blocks any writing that could be done on the external USB, by OS or any other program installed on the device, which is also evidence.

# Details and Steps

The first step of this assignment was to research how a write blocker works. I came across a journal ‘*A Study of Forensic Imaging in the Absence of Write-Blockers’* in which the authors described how to block writing to an external device in case a hardware write blocker is unavailable. The journal described that we can use the registry key ***HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect*** in Windows to block and unblock writing.

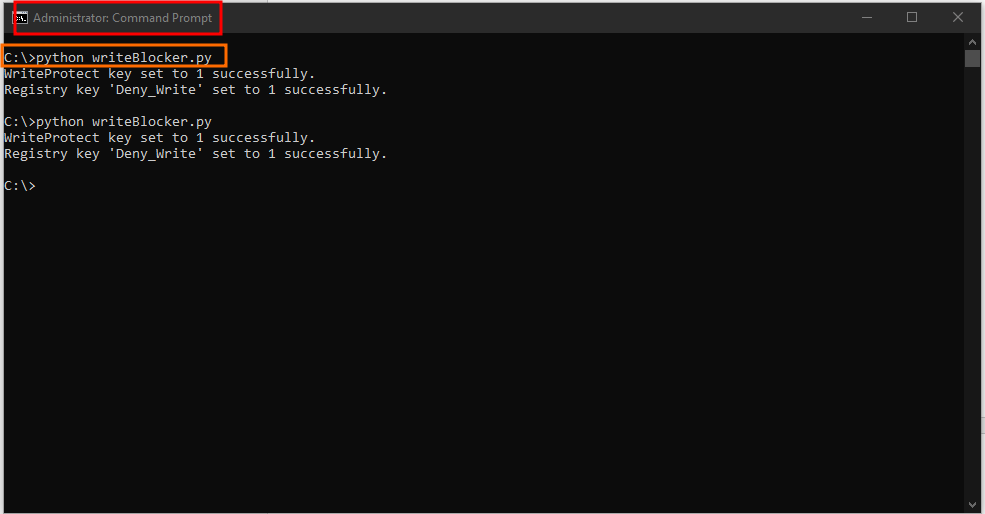
Upon further research Chat GPT said that this might get overridden by any program or user with admin privileges. It suggested using another approach to block writing, changing the Group Policy related to Removable Storage Access: Deny Write Access to Enabled using Group Policy Editor.

In short, we need to set

1. HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies > WriteProtect to 1
2. HKLM\Software\Policies\Microsoft\Windows\RemovableStorageDevices > DenyWrite to 1

These keys might not be there originally so you might need to create them manually or make a program to do that for you, which was my case.

After making the program using Python, we needed to execute the program using Administrator Privileges. You can do that by running cmd.exe as ‘Run As Administrator’ and then executing the program.



This will add those registry keys which will block write access to external drives.

# Summary

Write Blockers are very important in the Digital Forensics Domain to ensure that the Digital Evidence keeps its integrity while a DFI performs analysis on it. There are 2 ways to Write Block any external device when plugged into DFI’s machine. Although, write blocking software might temporarily do the job but Hardware/external write blockers are preferred to perform write blocking which is why they are called True Write. For this assignment we made a python program to write block which made two registry keys disabling the writing of drives that were plugged into our machine.

# References

<https://commons.erau.edu/cgi/viewcontent.cgi?article=1187&context=jdfsl>

[Digital Forensic | Free Write Blocker | Using Windows Registry | Software Write Blocker (youtube.com)](https://www.youtube.com/watch?v=2mWUUOsu2Tg)