

**CY2002**

**Digital Forensics**

**Write Blocker**

**Submitted by:** Muhammad Bilal Ikram

**Roll number:** 22i-1636

**Date:** 8 September 2024

**Table of Contents**

[ **Introduction** 2](#_Toc176716196)

[ **Details and Steps** 2](#_Toc176716197)

[ **Summary** 3](#_Toc176716198)

[ **References** 3](#_Toc176716199)

# **Introduction**

This assignment aims to develop a software-based write blocker for the Windows operating system, which ensures write protection for externally connected devices while allowing read access. The solution is implemented in Python and uses Windows registry modifications to manage USB ports, with an optional graphical user interface (GUI) for ease of use.

# **Details and Steps**

The USB Write Blocker tool is developed in Python and is designed to modify the Windows registry to enable or disable write protection on external USB devices. Below are the detailed steps and explanations for the tool:

1. **Checking for Administrative Privileges**:
   * The tool checks if it is running with administrative privileges using the ctypes library. Modifying the Windows registry requires elevated permissions, and the user is prompted to restart the tool as an administrator if necessary.
2. **Registry Modification**:
   * The tool modifies the Windows registry key SYSTEM\CurrentControlSet\Control\StorageDevicePolicies to enable or disable USB write protection:
     + **Enable Write Protection**: The registry value WriteProtect is set to 1, which prevents any data from being written to connected USB devices.
     + **Disable Write Protection**: The registry value WriteProtect is set to 0, which allows data to be written to connected USB devices.
   * If the registry key does not exist, the tool creates it using the create\_storage\_device\_policies\_key() function.
3. **Graphical User Interface (GUI)**:
   * A simple GUI is implemented using the tkinter library. It includes two buttons: "Enable Write Protection" and "Disable Write Protection," allowing the user to easily control USB write protection.
4. **Usage Instructions**:
   * **Run the Tool**: Ensure that the script is run with administrative privileges.
   * **Enable Write Protection**: Click the "Enable Write Protection" button to activate write protection on USB devices.
   * **Disable Write Protection**: Click the "Disable Write Protection" button to deactivate write protection.

# **Summary**

The USB Write Blocker tool developed in Python provides an easy-to-use solution for managing USB write protection on Windows systems. By modifying specific registry settings, the tool ensures that data on USB devices remains unaltered during forensic investigations or other secure operations. The tool supports Windows OS (version 10/11) and features a graphical user interface for ease of use, making it accessible to both technical and non-technical users.

# **References**

<https://github.com/digitalsleuth/Registry-Write-Block/blob/master/USB-Write-Blocker.cmd>

<https://samsclass.info/121/proj/p5-USB-writeblock-registry.pdf>

Chat-Gpt