OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Michael Hegarty

Forensics

Software Write-Blocker

You do not have to create a software write blocker or take screen shots for this Lab.

The purpose of the exercise is for you to be familiar with Write-Blockers and the role they play in a forensic investigation.

Deliverable

Answer the questions at the end of the lab, save them to a Word document and upload to Brightspace by Sunday @ 8pm

Lab1a should also be completed and uploaded in the same MS Word document

Contents

Requirements

A Windows machine (real or virtual)

A USB device (thumb drive or external hard drive)

Instructions in this lab are based on Windows 7, there are additional resources available on the WWW that you can adapt to suit your version of Windows.

Why do we need write blockers?

When a digital forensics professional investigates a storage device they must use “write blocking” to ensure that the media is not altered during the investigation.

This will be discussed in further detail throughout the module.

Creating a Restore Point on the Windows 7 Machine

- Regedit is a risky tool to use. If you make errors with it, you can damage your Windows OS. So to be safe, the first thing to do is to create a restore point, which backs up the Registry and other system files.

- On the Windows 7 machine, Click Start, and type RESTORE into the Search box (You can search how to create a Restore point for your version of Windows)

- Click ”Create a Restore Point”

- In the ”System Properties” box, click ”Create”

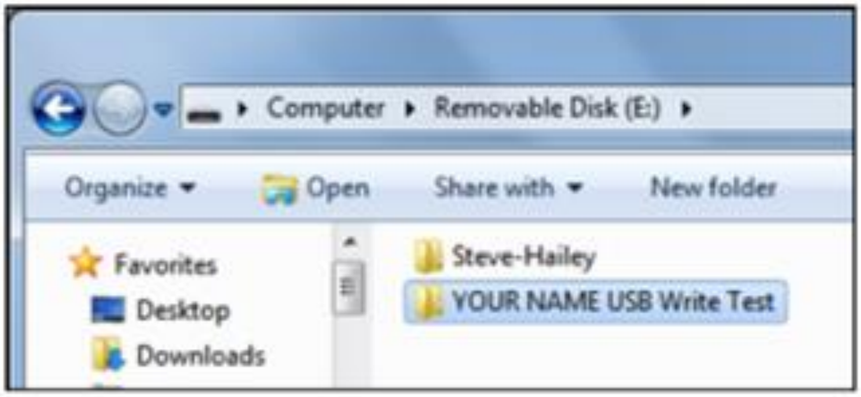
- In the ”Create a restore point” box, enter a name of ”YourName - Before registry edits” and click the Create button.

- Wait while the restore point is created

- A box appears saying “The restore point was created successfully”. Click Close
- Close “System Properties”

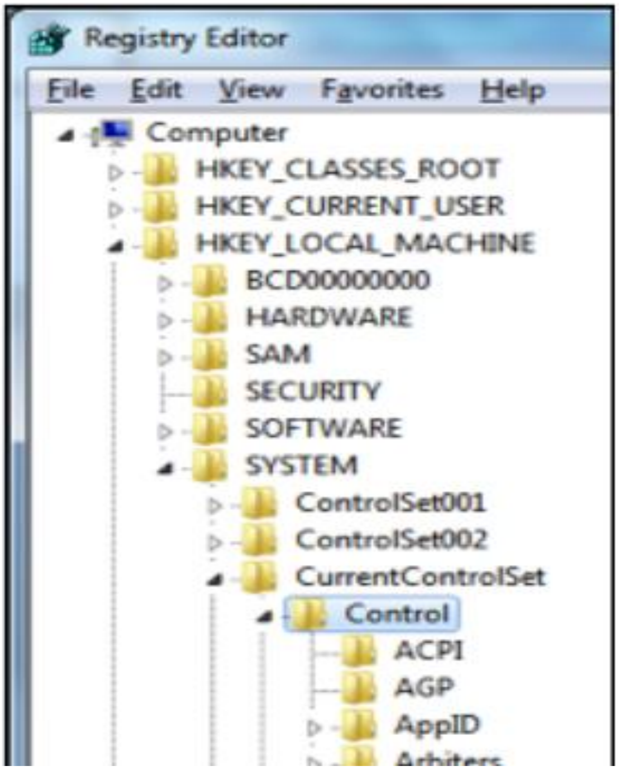
Writing to the USB Device

- Plug in the USB thumb drive or hard drive
- Click Start, Computer. Double-click the USB device
- In the USB devices window, right-click an empty portion and click New, Folder. Name the folder ”Your Name USB WriteTest”, replacing ”Your Name” with your own name. Press the Enter key to make sure the folder’s new name is written to the USB device, as shown above and to the right on this page



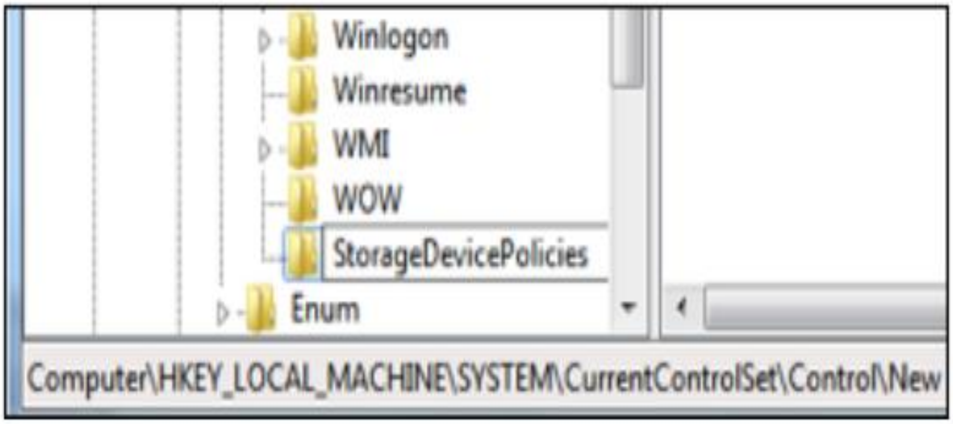
Using Regedit to Block USB Writing (1/4)

- Click Start. In the search box, type REGEDIT and then press the Enter key.
- In Registry Editor, in the left pane, expand HKEY LOCAL MACHINE, SYSTEM, CurrentControlSet, and Control keys., as shown in the image at the bottom of this page.
- Scroll down and see if there is a subkey named StorageDevicePolicies in the Control key. It is probably not there.



Using Regedit to Block USB Writing (2/4)

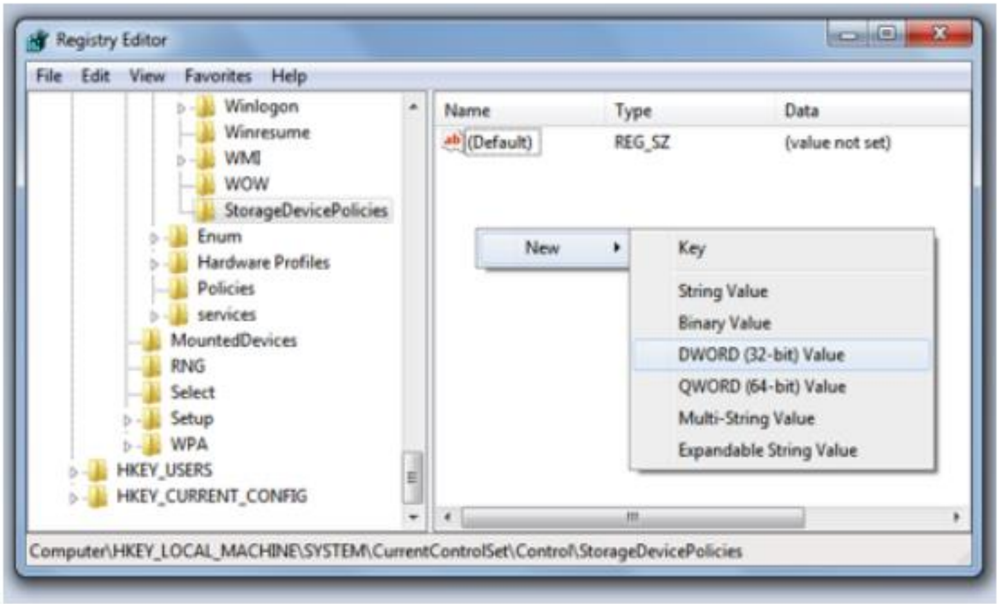
- If the StorageDevicePolicies key is not present, scroll back up, right-click the Control key and click New, Key.
- A new key appears at the bottom of the list: Type in the name StorageDevicePolicies, as shown at the bottom of this page, and press the Enter key.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\New

Using Regedit to Block USB Writing (3/4)

- In the left pane of Registry Editor, click StorageDevicePolicies to select it.
- In the right pane, right-click an empty portion of the window and click New, “DWORD (32-bit) Value”, as shown below on this page.

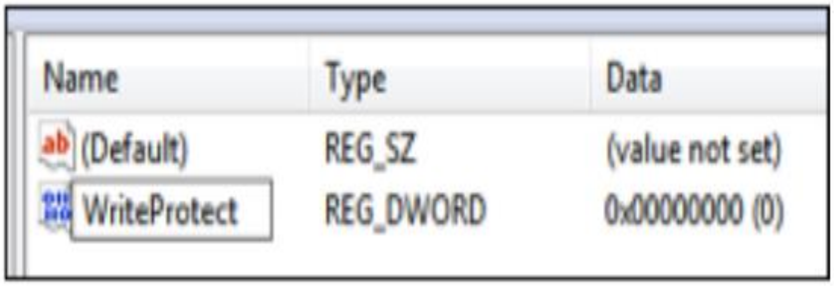


Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

Using Regedit to Block USB Writing (4/4)

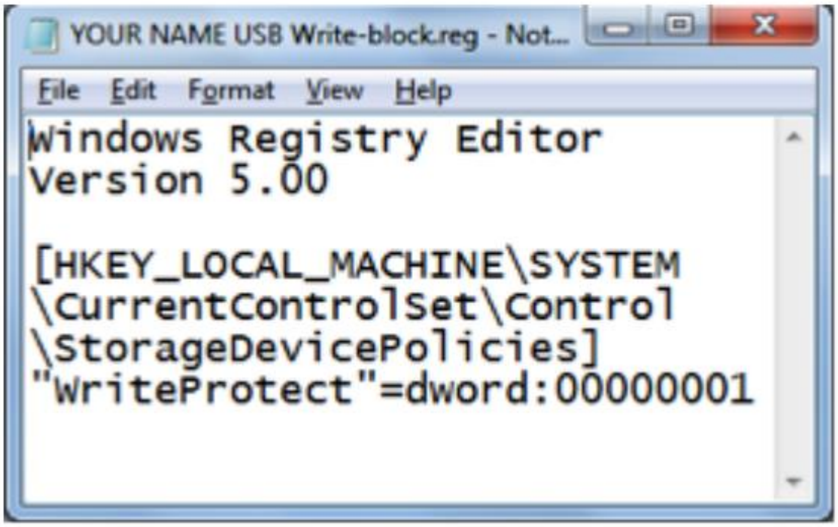
- Type the name WriteProtect into the name field for the new value, as shown to the right on this page, and press the Enter key.
- Double-click the WriteProtect value. In the ”Edit DWORD (32-bit) Value” box, enter a ”Value data” of 1. Click OK.



Name	Type	Data
(Default)	REG_SZ	(value not set)
WriteProtect	REG_DWORD	0x00000000 (0)

Creating a REG File

- In the left pane of Registry Editor, right-click StorageDevicePolicies click Export.
- In the Export Registry File dialog box, navigate to your Documents folder, and enter a file name of ”YOUR NAME USB Write-block”. Click Save. Close Registry Editor.
- Click Start, Documents. Right-click the ”YOUR NAME USB Write-block.REG” file and click Edit. The REG file opens in Notepad, as shown on this page.


YOUR NAME USB Write-block.reg - Not...
File Edit Format View Help

```
Windows Registry Editor
Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Control
\StorageDevicePolicies]
"WriteProtect"=dword:00000001
```

Taking a Screen Shot

Make sure your screen shows the exact text shown above.

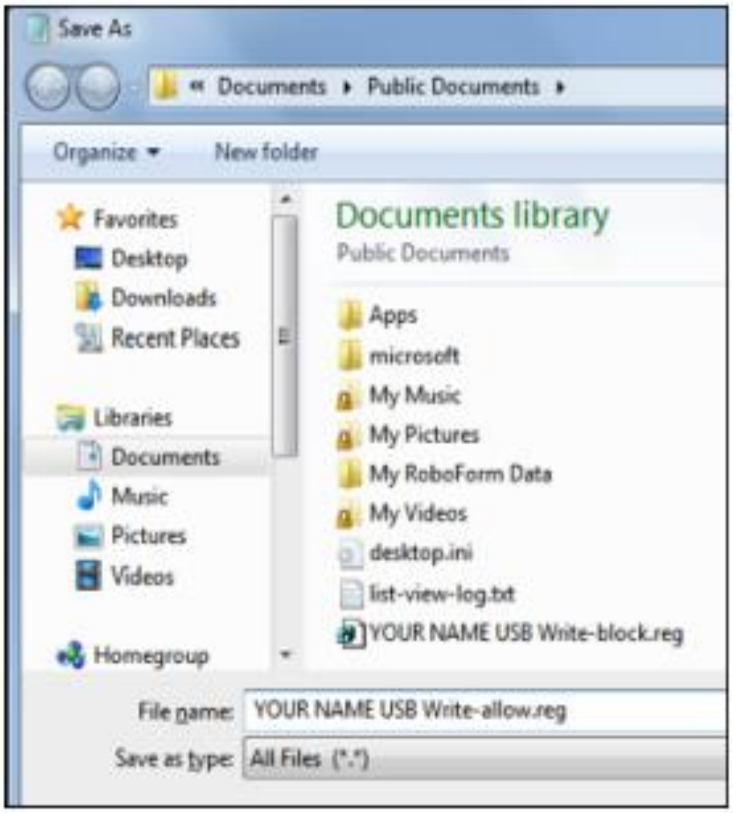
Press the PrintScrn key. Open Paint and paste in the image.

Save it with the filename ’fistname lastname image1 lab1’.

Save as type of JPEG or PNG.

Editing the REG File

- In the ”YOUR NAME USB Write-block.REG” window, carefully change the last character in the file from 1 to 0
- Click File, ”Save As”. Navigate to your Documents folder, and enter a file name of ”YOUR NAME USB Write-allow.reg” Change the ”Save as type” to ”All Files (*.*)”, as shown on the bottom of this page.
- Click Save. Close Notepad.



File name: YOUR NAME USB Write-allow.reg

Save as type: All Files (*.*)

Restarting the Computer

- Close all windows and restart your computer.

Trying to Write to the USB Device

- Plug in the USB thumbdrive or hard drive.
- Click Start, Computer. Double-click the USB device.
- In the USB devices window, right-click an empty portion. The option New is no longer available.

- On your desktop, right-click an empty space and click New, Folder.
- Name the folder ”Your Name ”, replacing ”Your Name” with your own name. Press the Enter key to make sure the folder’s new name is saved.
- Drag the ”Your Name” folder and drop it in the USB device’s window.
- A box pops up saying ”The disk is write-protected”, with your name on it.

Restoring your Machine

- Click Start, Documents. Double-click the ”YOUR NAME USB Write-allow.reg”.file. In the ”User Account Control” box, click Yes. In the ”Registry Editor” box, click Yes. In the ”Registry Editor” box, click OK. The next time the machine starts, USB writing will be allowed again.

Questions.

Please write 300 words minimum (In total) to explain the below

1. Why are write blockers essential in a forensics investigation?

2. What are the main types of write blockers?

3. What are the main challenges of write blocking for forensics investigators?

4. Discuss the implications of using open-source technologies for write blocking.

Save you answers to a word document and upload to our Brightspace page by Sunday @ 8pm