Write-blocking for Evidence Preservation

8

By the end of the practical session, the students should be able to:

- Understand the function of write-blocker
- Protect the evidence using well-tested write-blocker
- Implement USB write-blocking with the windows registry

This lab will cover topics on understanding how to perform the data acquisition and protect the digital evidence using write-blocker in order to ensure the integrity of the evidence is not tampered.

8.0 Introduction

The first item that should consider for a forensic workstation is a write-blocker. Write-blockers protect evidence disks by preventing data from being written to them. Software and hardware write-blockers perform the same function but in a different fashion.

Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode (such as a Windows CLI). PDBlock changes interrupt 13 of a workstation's BIOS to prevent writing to the specified drive. If you attempt to write data to the blocked drive, an alarm sounds, advising that no writes have occurred. PDBlock can run only in a true DOS mode, however, not in a Windows CLI.

With hardware write-blockers, you can connect the evidence drive to your workstation and start the OS as usual. Hardware write-blockers, which act as a bridge between the suspect drive and the forensic workstation, are ideal for GUI forensics tools. They prevent Windows or Linux from writing data to the blocked drive.

Lab 8.1: USB Write-Blocking with the Windows Registry

8.1.1 Requirements

In this lab, you are require:

- Any Windows computer, real or virtual.
- A USB thumbdrive or external hard drive.
- The instructions below assume you are using a Windows 7 computer.
- Submit your JPEG images through ULearn.

8.1.2 Task 1: Creating a Restore Point on the Windows 7 Machine

1. Regedit is a dangerous tool to use. If you make mistakes with it, you can damage your Windows OS. So to be safe, the first thing is to create a restore point, which backs up the Registry and other system files.
2. On the Windows 7 machine, Click **Start**, and type **RESTORE** into the Search box.
3. Click **"Create a Restore Point".**
4. In the "System Properties" box, click **"Create".**
5. In the "Create a restore point" box, enter a name of ***"Your Name - Before registry edits"*** and click the **Create** button. Wait while the restore point is created.
6. A box appears saying "The restore point was created successfully". Click **Close**.
7. Close "System Properties".

8.1.3 Task 2: Writing to the USB Device

8. Plug in the USB thumbdrive or hard drive.
9. Click **Start, Computer**. Double-click the USB device
10. In the USB device's window, right-click an empty portion and click **New, Folder**. Name the folder ***"Your Name USB Write Test"***, 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 in Figure 8.1.

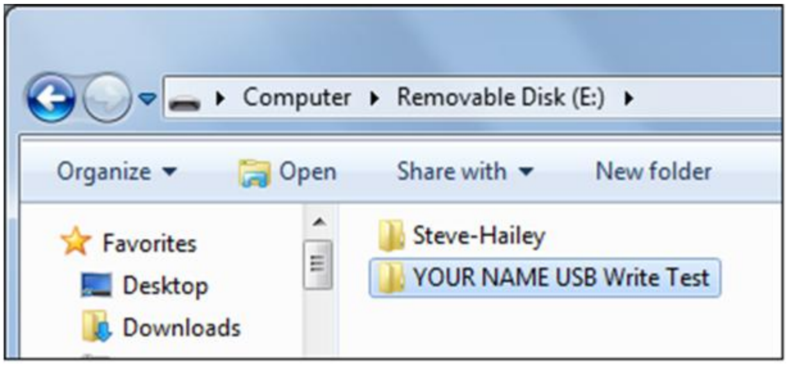


Figure 8.1 Writing to USB device

8.1.4 Task 3: Using Regedit to Block USB Writing

11. Click **Start**. In the search box, type REGEDIT and then press the Enter key.
12. Registry Editor, in the left pane, expand **HKEY_ LOCAL_ MACHINE, SYSTEM, CurrentControlSet,** and **Control** keys, as shown in Figure 8.2.

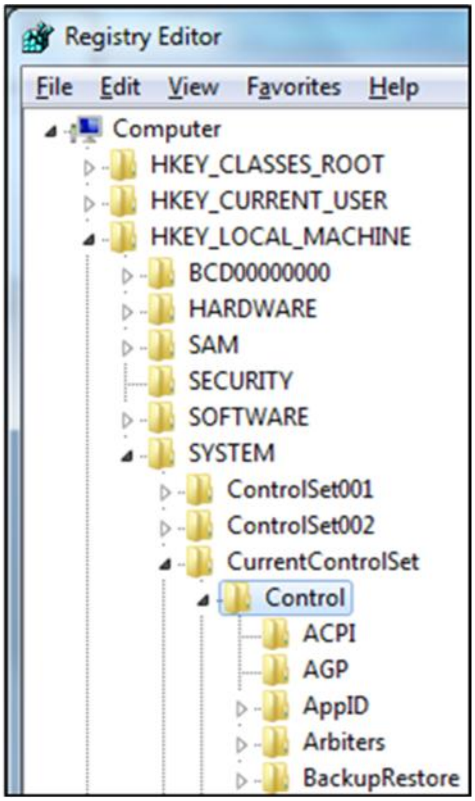


Figure 8.2 Regedit to block USB writing

13. Scroll down and see if there is a subkey named **StorageDevicePolicies** in the Control key. It is probably not there.
14. If the StorageDevicePolicies key is not present, scroll back up, right-click the **Control key** and click **New, Key.**
15. A new key appears at the bottom of the list: Type in the name **StorageDevicePolicies**, as shown in Figure 8.3, and press the Enter key.

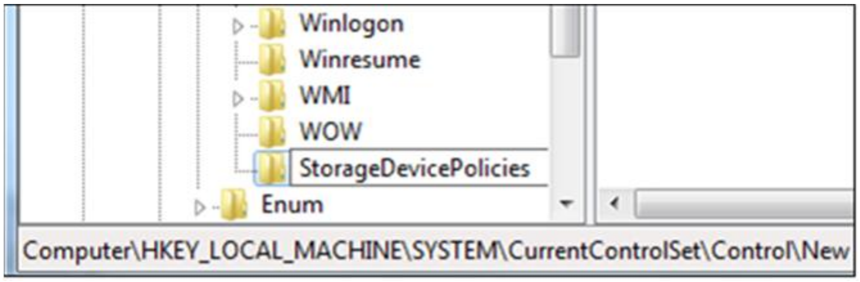

Winlogon
Winresume
WMI
WOW
StorageDevicePolicies
Enum
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\New

Figure 8.3 StorageDevicePolicies key

16. In the left pane of Registry Editor, click **StorageDevicePolicies** to select it.
17. In the right pane, right-click an empty portion of the window and click **New,** "**DWORD 32-bit) Value**", as shown in Figure 8.4.

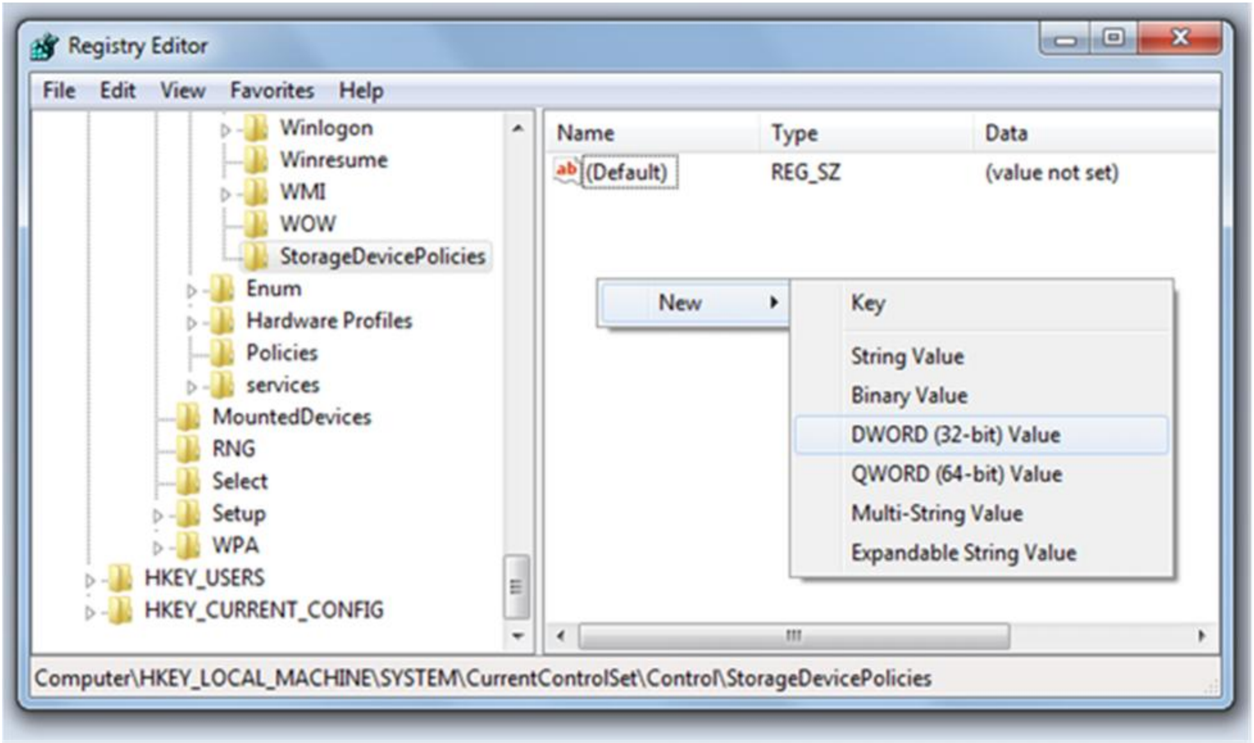
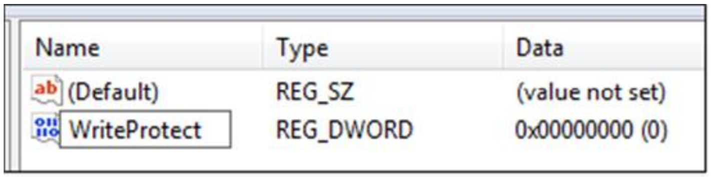


Figure 8.4 Setting key value for StorageDevicePolicies

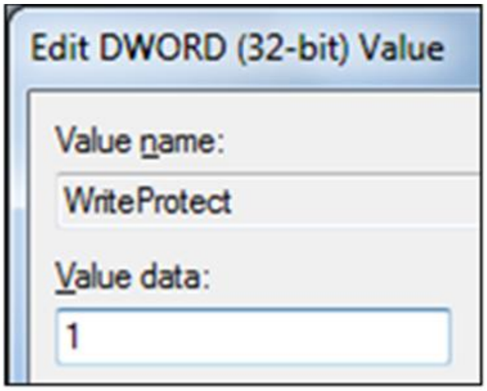
18. Type the name **WriteProtect** into the name field for the new value, as shown in Figure 8.5, and press the Enter key.



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

Figure 8.5 Key value setting

19. Double-click the **WriteProtect** value. In the "Edit DWORD (32-bit) Value" box, enter a "Value data" of **1**, as shown in Figure 7.6. Click **OK**.



Edit DWORD (32-bit) Value

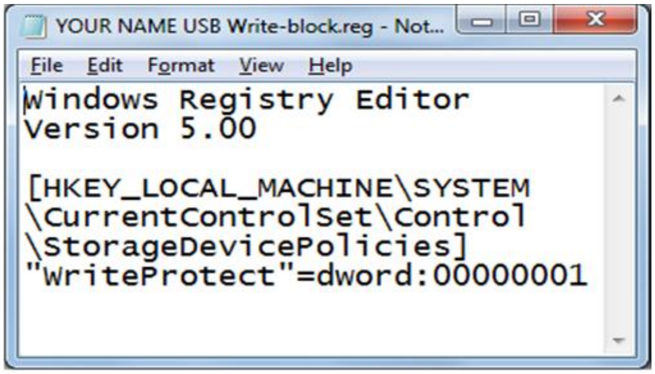
Value name:
WriteProtect

Value data:
1

Figure 8.6 Setting value data

7.1.5 Task 4: Creating a REG File

20. In the left pane of Registry Editor, right-click **StorageDevicePolicies** click Export.
21. 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.
22. Click **Start, Documents**. Right-click the "**YOUR NAME USB Write-block.REG**" file and click **Edit**. The REG file opens in Notepad, as shown in Figure 8.7.


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

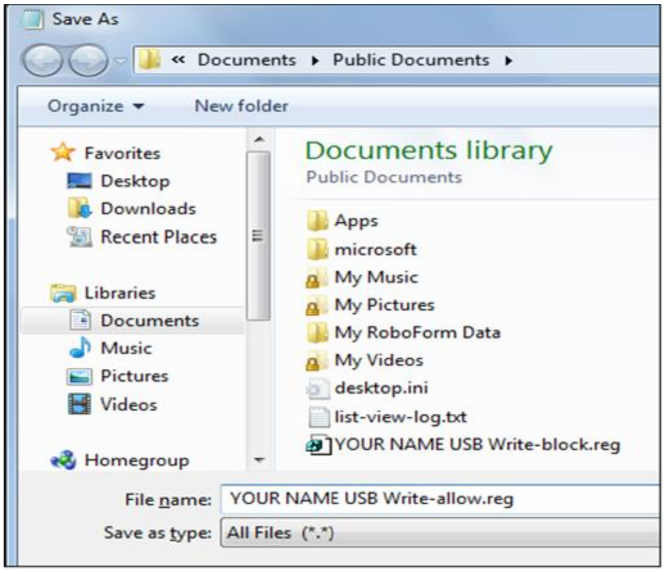
```
Windows Registry Editor
Version 5.00

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

Figure 8.7 REG file opens

23. Make sure your screen shows the exact text shown in Figure 8.7.
24. Press the **PrintScrn** key. Open Paint and paste in the image. Save it with the filename **Your Name Lab7a**. Select a **Save as** type of **JPEG** or **PNG**.

8.1.6 Task 5: Editing the REG File

25. In the "**YOUR NAME USB Write-block.REG**" window, carefully change the last character in the file from 1 to **0**.
26. Click File, "**Save As...**". Navigate to your Documents folder, and enter a file name of "**YOUR NAME USB Write-allow.reg**".
27. Change the "Save as type" to "**All Files (*.*)**", as shown in Figure 8.8.



File name: YOUR NAME USB Write-allow.reg

Save as type: All Files (*.*)

Figure 8.8 Editing REG file

28. Click **Save**. Close Notepad
29. Close all windows and restart your computer.

7.1.7 Task 6: Trying to Write to the USB Device

30. Plug in the USB thumbdrive or hard drive.
31. Click **Start, Computer**. Double-click the USB device.
32. In the USB device's window as shown in Figure 8.9, right-click an empty portion. The option **New** is no longer available.

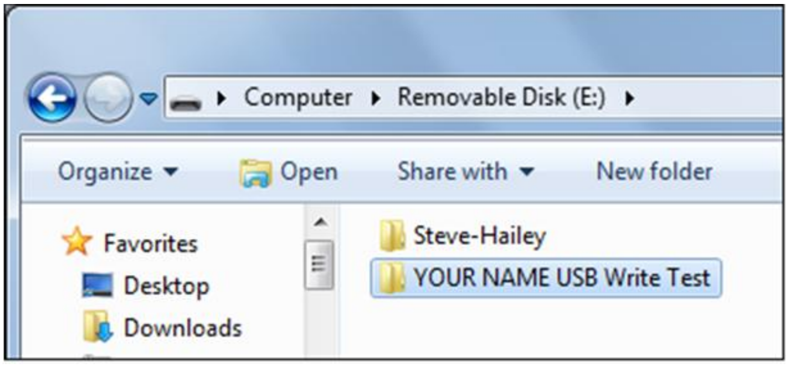
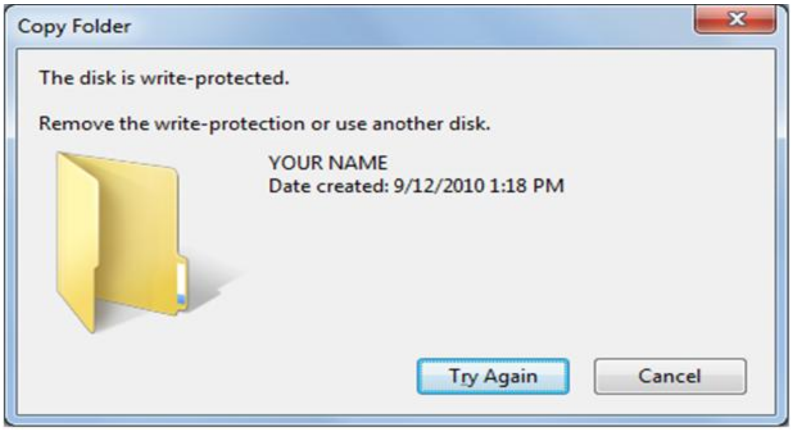


Figure 8.9 USB device's window

33. On your desktop, right-click an empty space and click New, Folder.
34. 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.
35. Drag the ***"Your Name"*** folder and drop it in the USB device's window.
36. A box pops up saying "**The disk is write-protected",** with your name on it, as shown in Figure 8.10.


Copy Folder

The disk is write-protected.

Remove the write-protection or use another disk.

YOUR NAME
Date created: 9/12/2010 1:18 PM

Figure 8.10 Warning on disk is write-protected

37. Make sure your screen shows the "**The disk is write-protected**" message.
38. Press the **PrintScrn** key. Open Paint and paste in the image. Save it with the filename **Your Name Lab7b**. Select a **Save as type** of **JPEG** or **PNG**.

7.1.8 Task 7: Restoring USB Devices to Normal Operation

39. 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.