TASK # 01:

Set USB to "Read-Only" Mode When Inserted into a System

To prevent any accidental modifications or data tampering, the goal is to configure the USB drive so that it becomes read-only when connected to a system. This ensures that the data on the USB can only be viewed and not altered.

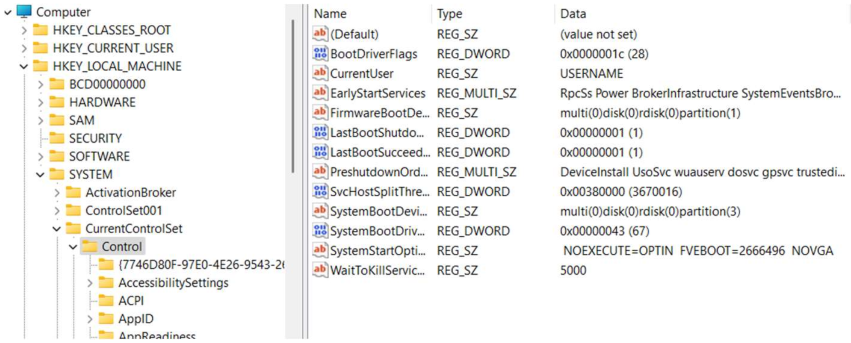
1.Open the Registry Editor:

- Press **Win + R** to open the **Run** dialog box.
- Type regedit and press **Enter**.

2. Navigate to the USB Storage Key:

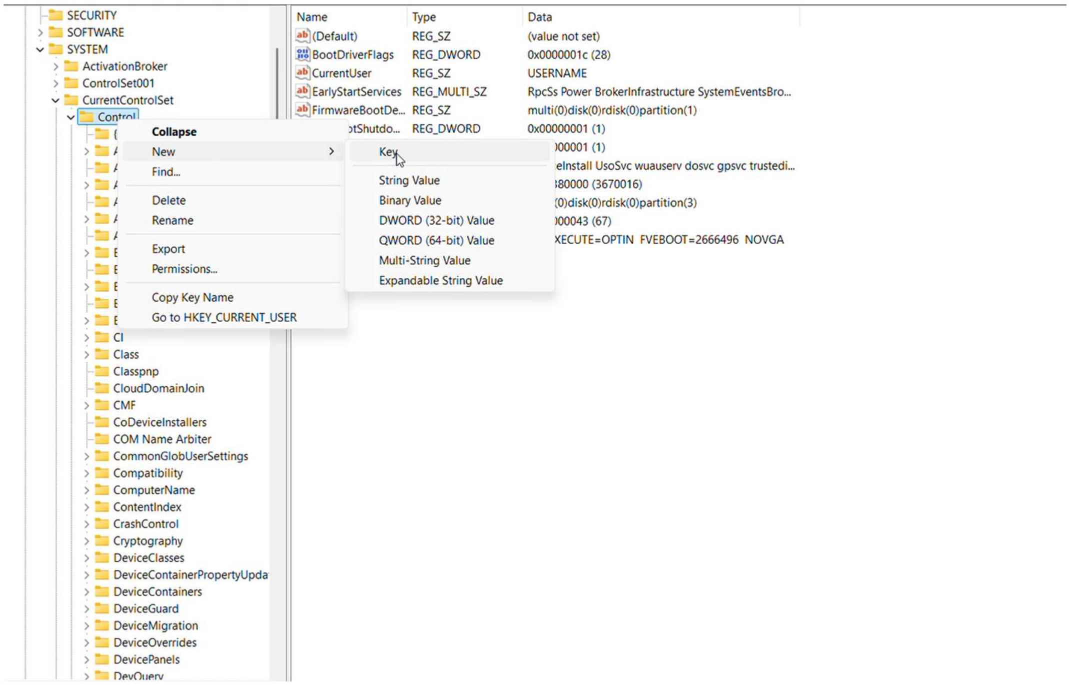
- In the Registry Editor, go to the following path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control



Name	Type	Data
(Default)	REG_SZ	(value not set)
BootDriverFlags	REG_DWORD	0x0000001c (28)
CurrentUser	REG_SZ	USERNAME
EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure SystemEventsBro...
FirmwareBootDe...	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)
LastBootShutdo...	REG_DWORD	0x00000001 (1)
LastBootSucceed...	REG_DWORD	0x00000001 (1)
PreshutdownOrd...	REG_MULTI_SZ	DeviceInstall UsoSvc wuauserv dosvc gpsvc trustedi...
SvcHostSplitThre...	REG_DWORD	0x00380000 (3670016)
SystemBootDevi...	REG_SZ	multi(0)disk(0)rdisk(0)partition(3)
SystemBootDriv...	REG_DWORD	0x00000043 (67)
SystemStartOpti...	REG_SZ	NOEXECUTE=OPTIN FVEBOOT=2666496 NOVGA
WaitToKillServic...	REG_SZ	5000

3. Scroll down and look for the **"StorageDevicePolicies"** key. If you don't see it, you may need to create it (right-click on **Control → New → Key**, and name it **StorageDevicePolicies**).

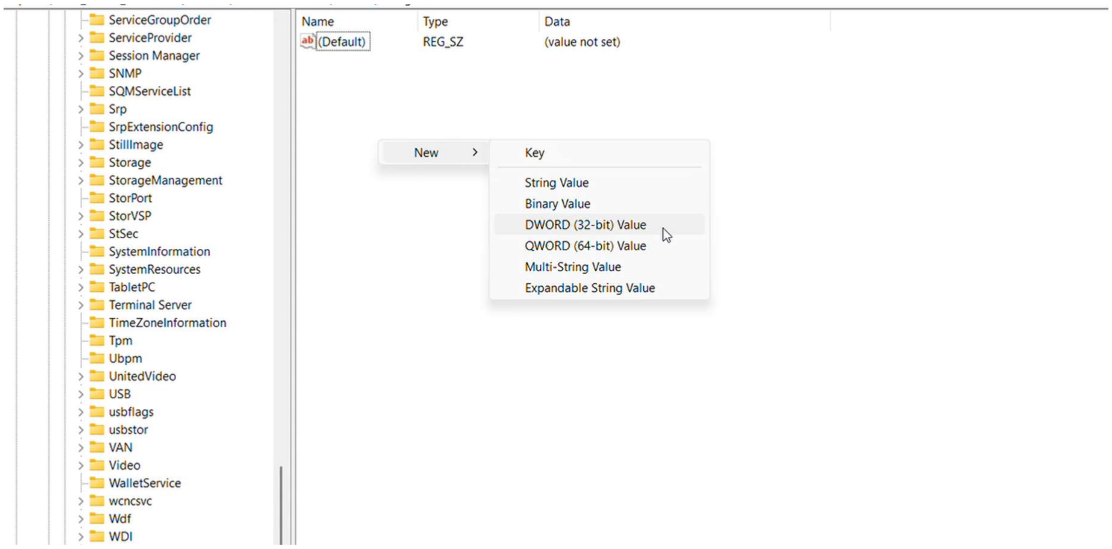


Name	Type	Data
(Default)	REG_SZ	(value not set)
BootDriverFlags	REG_DWORD	0x0000001c (28)
CurrentUser	REG_SZ	USERNAME
EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure SystemEventsBro...
FirmwareBootDe...	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)
otShutdo...	REG_DWORD	0x00000001 (1)
		)00001 (1)
		elnstall UsoSvc wuauserv dosvc gpsvc trustedi...
		380000 (3670016)
		(0)disk(0)rdisk(0)partition(3)
		)00043 (67)
		XECUTE=OPTIN FVEBOOT=2666496 NOVGA

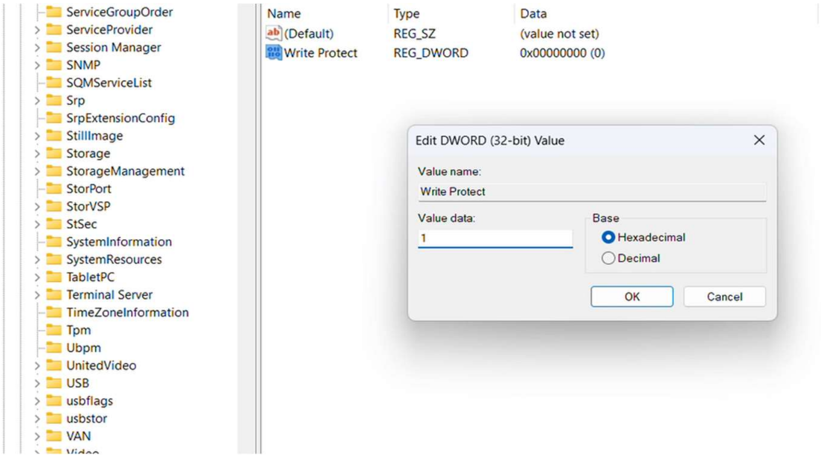
4.Create the WriteProtect Value:

Once inside the StorageDevicePolicies key, right-click in the right pane and choose New → DWORD (32-bit) Value.Name the new value WriteProtect.

5.**Set WriteProtect to 1**: Double-click on **WriteProtect** and change the **Value data** to 1 to enable read-only mode then click **OK**.



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



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

Edit DWORD (32-bit) Value

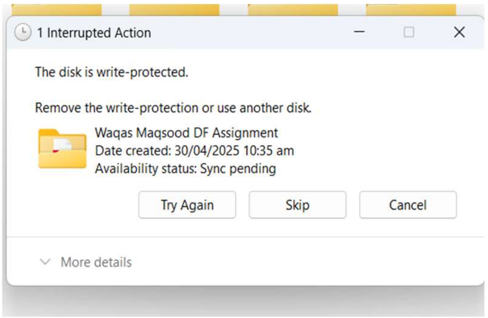
Value name: Write Protect

Value data: 1

Base
● Hexadecimal
○ Decimal

Conclusion:

In this task, we successfully created a **read-only environment for the USB device** to ensure the integrity of digital evidence. By modifying the Windows Registry and/or using diskpart, we prevented any accidental write operations. A **system restart** was required for the changes to take effect. This setup is crucial in digital forensics to maintain evidence in its original state.


1 Interrupted Action

The disk is write-protected.

Remove the write-protection or use another disk.

Waqas Maqsood DF Assignment
Date created: 30/04/2025 10:35 am
Availability status: Sync pending