

Assignment 2 – Sterilize Media & Document

Student: Zach Brown

Course: Digital Forensics

Date: February 12, 2026

Evidence Description

On February 12, 2026, I identified and documented a removable USB storage device for the purpose of forensic sterilization and reformatting pursuant to Assignment 2 requirements.

The device is physically branded as SanDisk, as observed on the exterior casing of the device.

The USB device was connected to an HP Envy x360 laptop and examined using native Windows administrative utilities.

Physical and Logical Identification

Device Type:

Removable USB flash drive

Manufacturer:

SanDisk (confirmed via physical branding and Windows device listing)

Model / Friendly Name:

SanDisk Cruzer Glide USB Device

Disk Number:

Disk 1 (Removable)

Hardware Serial Number:

20051941900572C079B2

(Source: PowerShell Get-Disk output)

Volume Serial Number:

38B4-950D

(Source: `vol` `D:` command output)

Storage Characteristics

Reported Capacity:

8,000,372,736 bytes

(Approximately 7.45 GB usable capacity)

Partition Layout:

Single Primary Partition

File System:

FAT32

Drive Letter:

D:

Current Usage:

- Used Space: 59,817,984 bytes (57.0 MB)
- Free Space: 7,940,554,752 bytes (7.39 GB)

Disk Management Confirmation

Disk Management confirms:

- Disk 1 is removable media
- Capacity: 7.46 GB
- One primary partition

- File system: FAT32
- Status: Healthy (Primary Partition)

The device is operational and recognized by the operating system as functioning properly.

Appendix A – Photographic Evidence

Figure 1 – External view of SanDisk USB device:



Appendix B – Logical Identification Screenshots

Figure 2 – Disk Management (showing Disk 1):

The screenshot displays the Windows Disk Management console. The top section shows a list of volumes with the following data:

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(D:)	Simple	Basic	FAT32	Healthy (P...	7.45 GB	7.40 GB	99 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	260 MB	260 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	864 MB	864 MB	100 %
Windows (C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	1906.61 GB	1553.54 GB	81 %

The bottom section shows the graphical representation of the disks. Disk 0 is a Basic disk with a capacity of 1907.71 GB, containing three partitions: a 260 MB EFI System Partition, a 1906.61 GB NTFS (BitLocker Encrypted) partition for Windows (C:), and an 864 MB Recovery Partition. Disk 1 is a Removable disk with a capacity of 7.46 GB, containing a single 7.45 GB FAT32 Primary Partition labeled (D:). The (D:) partition is highlighted with a yellow background.

Legend: ■ Unallocated ■ Primary partition

Figure 3.1 – USB Properties window (Capacity & File System):

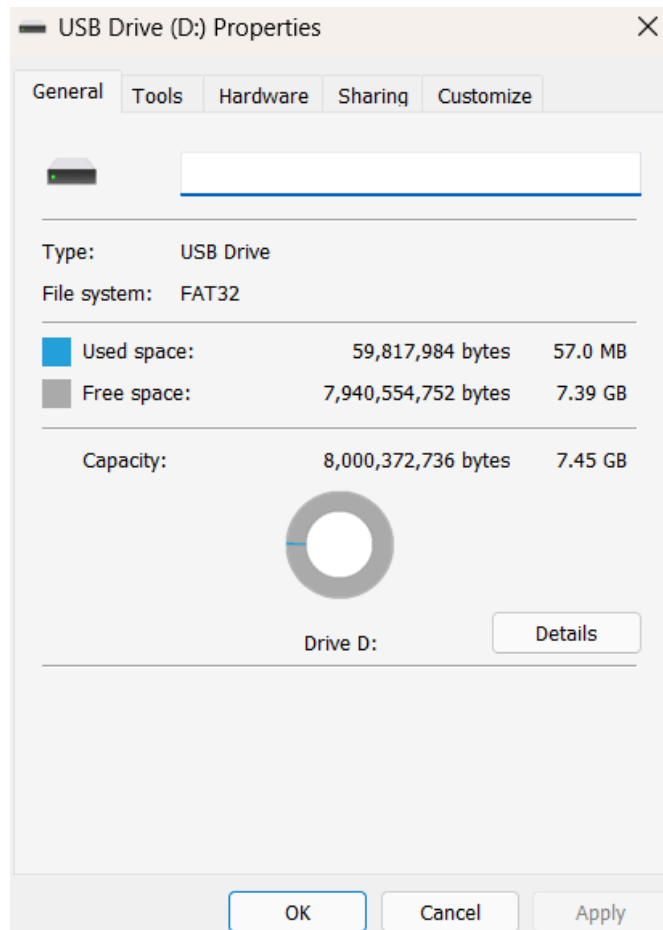


Figure 3.2 - USB Properties window (Capacity & File System):

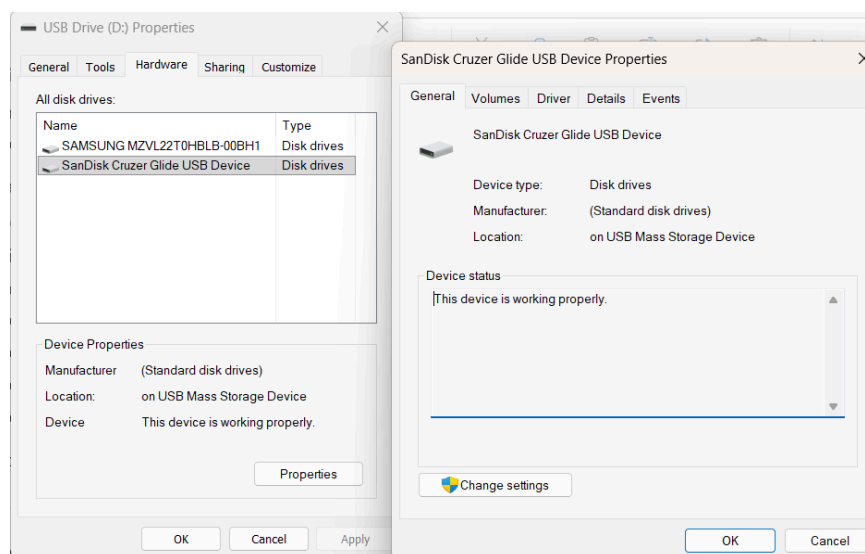
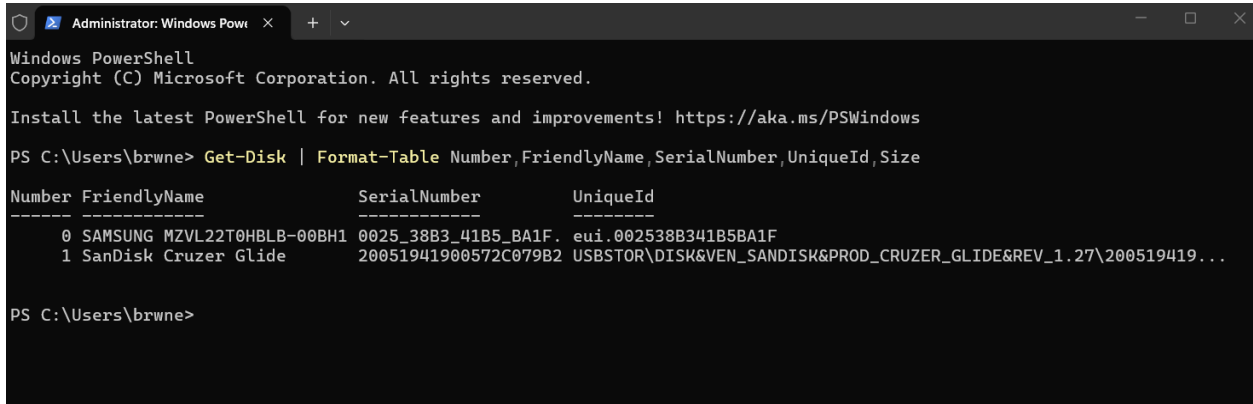


Figure 4 – PowerShell Get-Disk output:



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the output of the `Get-Disk` command, which has been formatted into a table. The table has four columns: `Number`, `FriendlyName`, `SerialNumber`, and `UniqueId`. There are two rows of data. The first row represents a Samsung disk, and the second row represents a SanDisk disk. The prompt is `PS C:\Users\brwne>`.

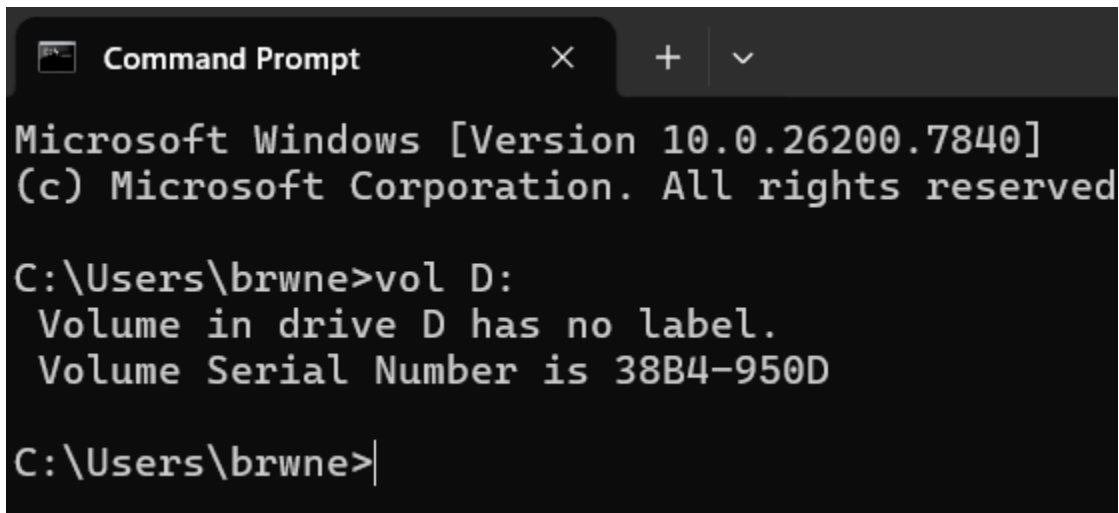
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\brwne> Get-Disk | Format-Table Number,FriendlyName,SerialNumber,UniqueId,Size

Number FriendlyName                SerialNumber                UniqueId
-----
0 SAMSUNG MZVL22T0HBLB-00BH1 0025_38B3_41B5_BA1F. eui.002538B341B5BA1F
1 SanDisk Cruzer Glide         20051941900572C079B2 USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.27\200519419...
```

Figure 5 – Command Prompt vol D: output:



A screenshot of a Windows Command Prompt window titled "Command Prompt". The window shows the output of the `vol D:` command. The output indicates that the volume in drive D has no label and provides the volume serial number as 38B4-950D. The prompt is `C:\Users\brwne>`.

```
Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. All rights reserved

C:\Users\brwne>vol D:
Volume in drive D has no label.
Volume Serial Number is 38B4-950D

C:\Users\brwne>
```

Sterilization Methodology

Sterilization Tool Used

Sterilization was performed using:

- **Tool:** Microsoft DiskPart Utility
- **Execution Context:** Administrator PowerShell
- **Method:** `clean all` command

The `clean all` command was selected because it writes zeros to every sector on the disk, effectively overwriting all previous data and rendering the media forensically sterile.

Commands Executed

The following commands were issued:

```
diskpart
```

```
list disk
```

```
select disk 1
```

```
attributes disk
```

```
clean
```

```
clean all
```

- The `clean` command removed partition information.
- The `clean all` command performed a full zero-write across the disk.

Administrator: Windows Powe × + ▾

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

PS C:\Users\brwne> diskpart

Microsoft DiskPart version 10.0.26100.1150

Copyright (C) Microsoft Corporation.
On computer: ENVYX360

DISKPART> list disk

Disk ###	Status	Size	Free	Dyn	Gpt
Disk 0	Online	1907 GB	6144 KB		*
Disk 1	Online	7633 MB	0 B		

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> detail disk

SanDisk Cruzer Glide USB Device
 Disk ID: 00000000
 Type : USB
 Status : Online
 Path : 0
 Target : 0
 LUN ID : 0
 Location Path : UNAVAILABLE
 Current Read-only State : No
 Read-only : No
 Boot Disk : No
 Pagefile Disk : No
 Hibernation File Disk : No
 Crashdump Disk : No
 Clustered Disk : No

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 3	D		FAT32	Removable	7633 MB	Healthy	

DISKPART>


```
DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> attributes disk
Current Read-only State : No
Read-only      : No
Boot Disk     : No
Pagefile Disk  : No
Hibernation File Disk : No
Crashdump Disk : No
Clustered Disk : No

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> clean all

DiskPart succeeded in cleaning the disk.

DISKPART>

DISKPART> |
```

- *Figure 6 & 7 - DiskPart succeeded in cleaning the disk*

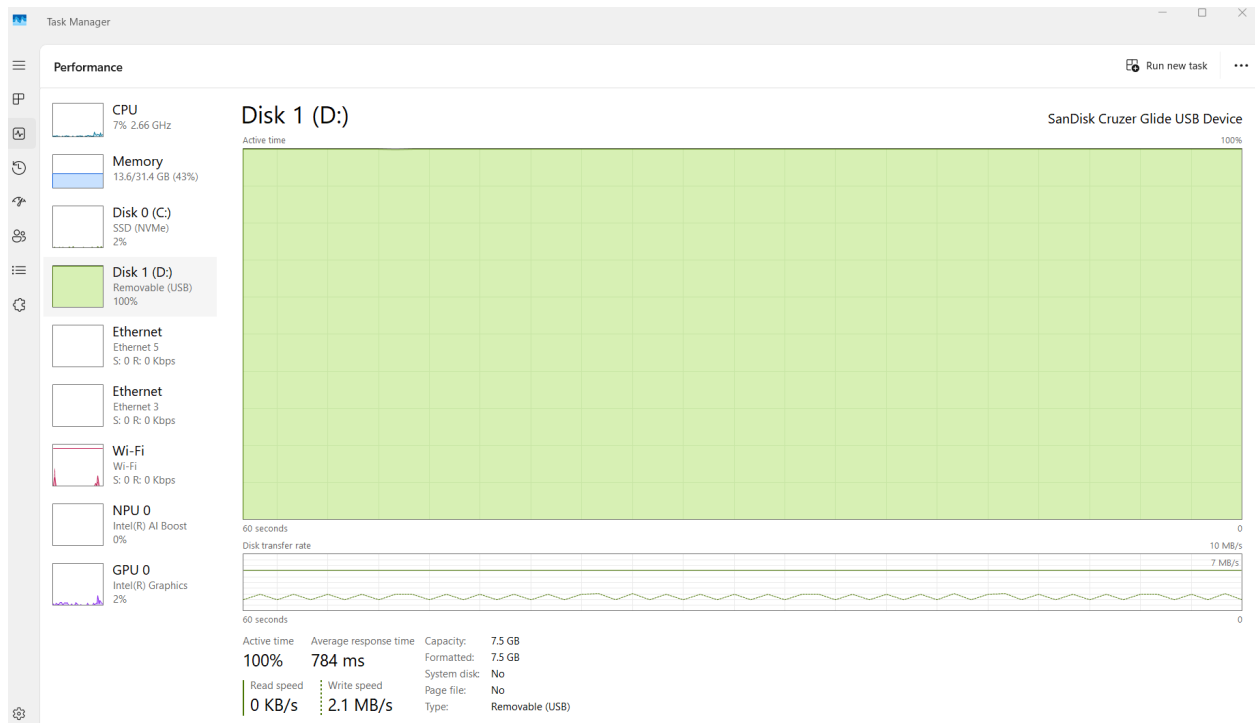
Observed System Behavior During Sterilization

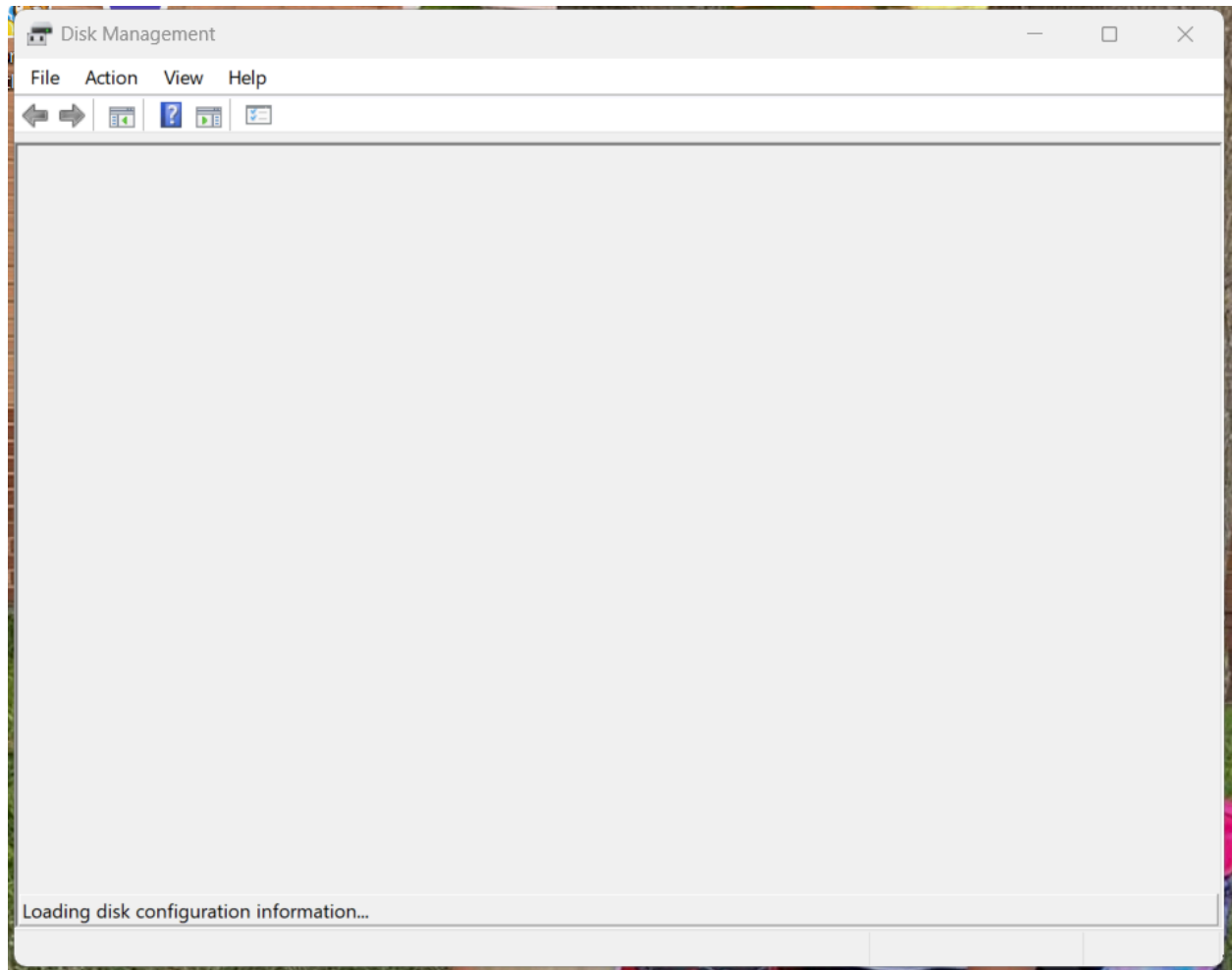
During execution of `clean all`:

- Disk 1 showed 100% Active Time in Task Manager.
- Write speed averaged approximately 2.1 MB/s.

- Disk Management temporarily displayed “Unallocated” space.
- Disk Management interface temporarily paused while disk configuration updated.

This behavior is consistent with full-sector overwrite operations.



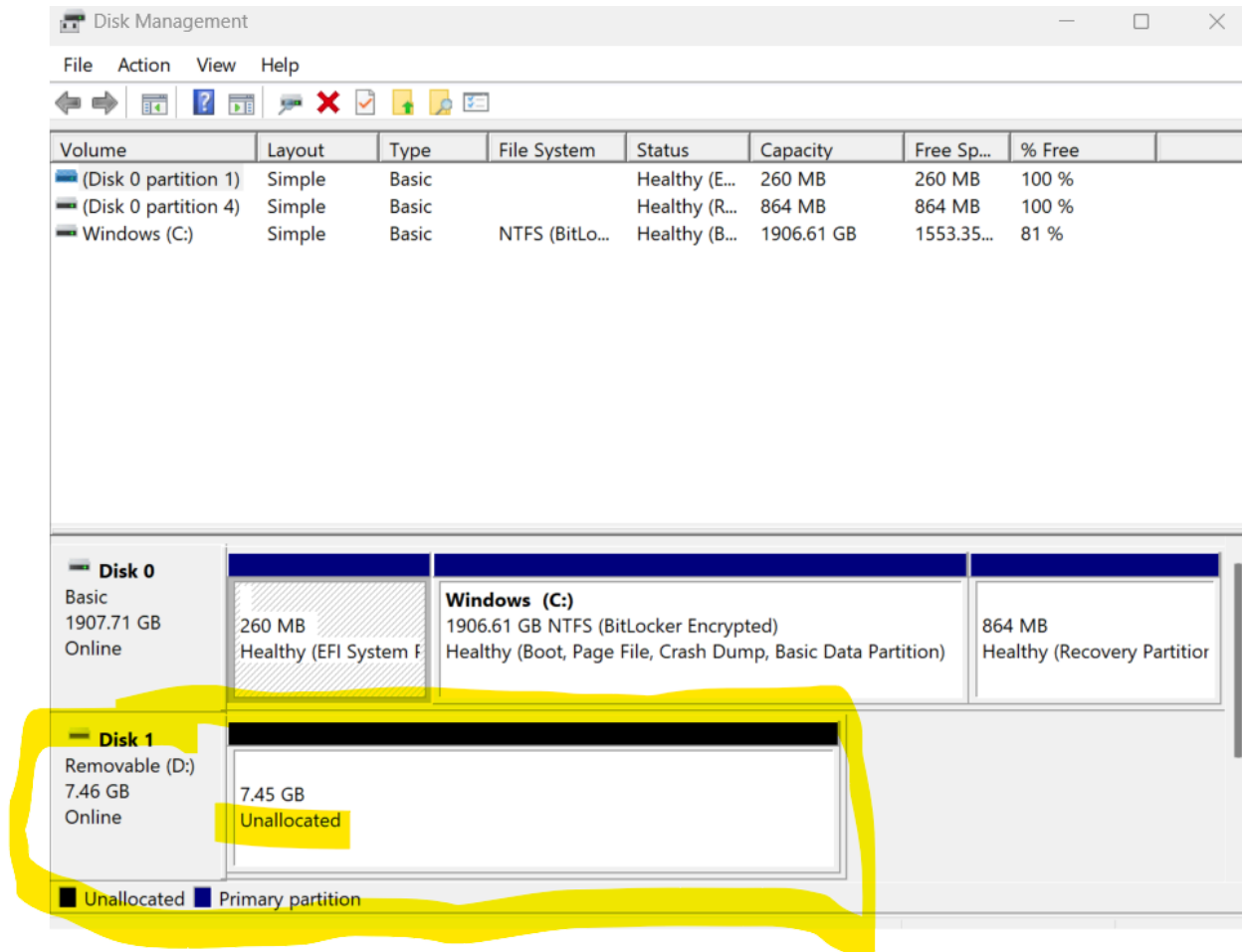


- *Figure 7 & 8 - Task Manager Disk Manager observation during Sterilization*

Post-Sterilization Verification

After sterilization completed successfully:

- Disk 1 showed 0 B free prior to reinitialization.
- Disk Management displayed the entire disk as Unallocated.
- No partitions were present.
- No file system was assigned.



- Figure 9 - Disk Management screenshot showing Unallocated

Media Reinitialization and Formatting

After confirming sterilization, the disk was re-prepared for future evidence collection.

New Volume Creation

Using Disk Management:

- Created New Simple Volume
- Assigned Drive Letter: **E**
- Selected File System: **NTFS**

- Allocation Unit Size: Default
- Volume Label: **STERILIZED_MEDIA**
- Quick Format: **Not selected** (Full format performed)

New Simple Volume Wizard ✕

Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

☒ Assign the following drive letter: E ▾

☐ Mount in the following empty NTFS folder:
 Browse...

☐ Do not assign a drive letter or drive path

< Back Next > Cancel

New Simple Volume Wizard ✕

Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS ▾

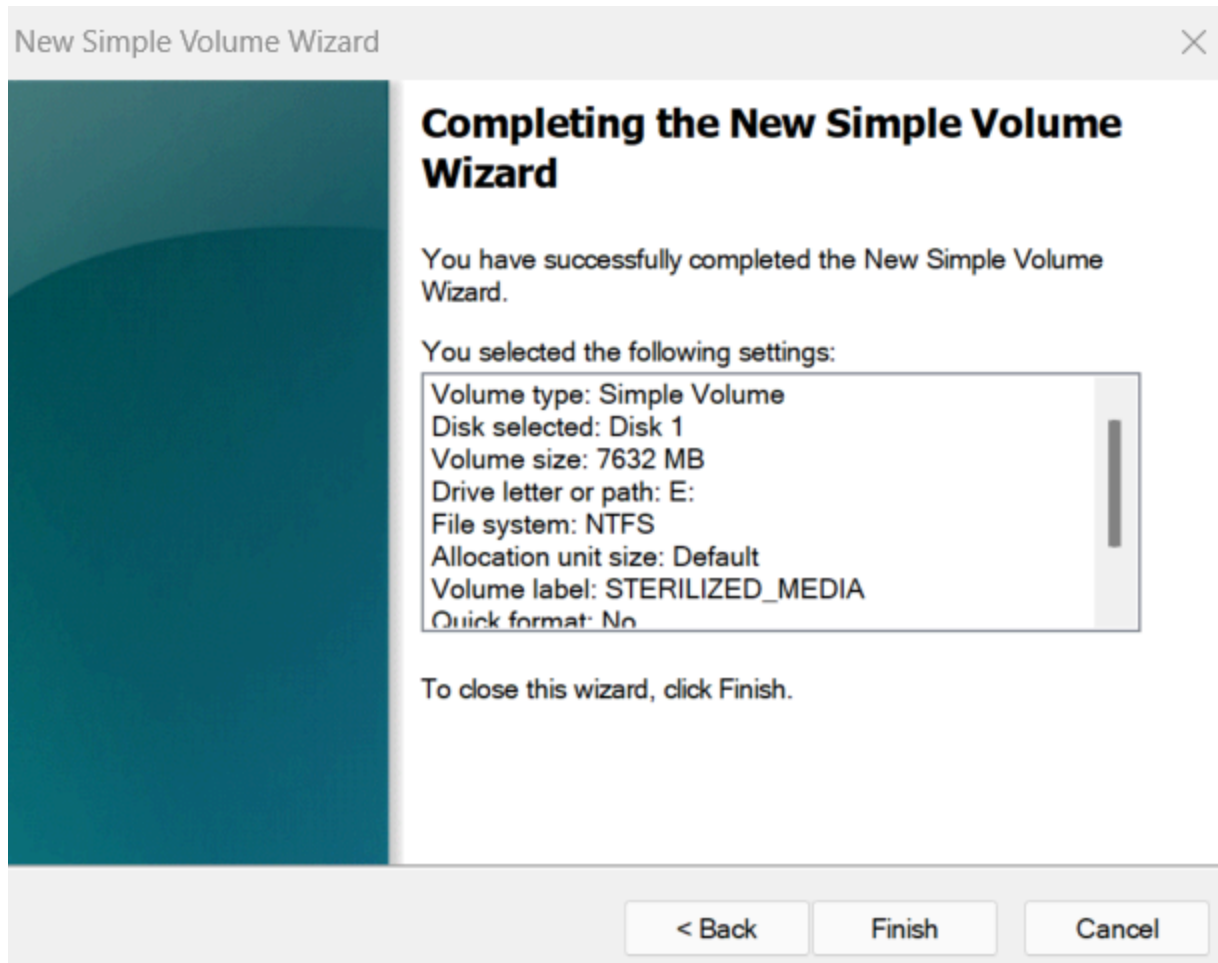
Allocation unit size: Default ▾

Volume label: STERILIZED_MEDIA

☐ Perform a quick format

☐ Enable file and folder compression

< Back Next > Cancel

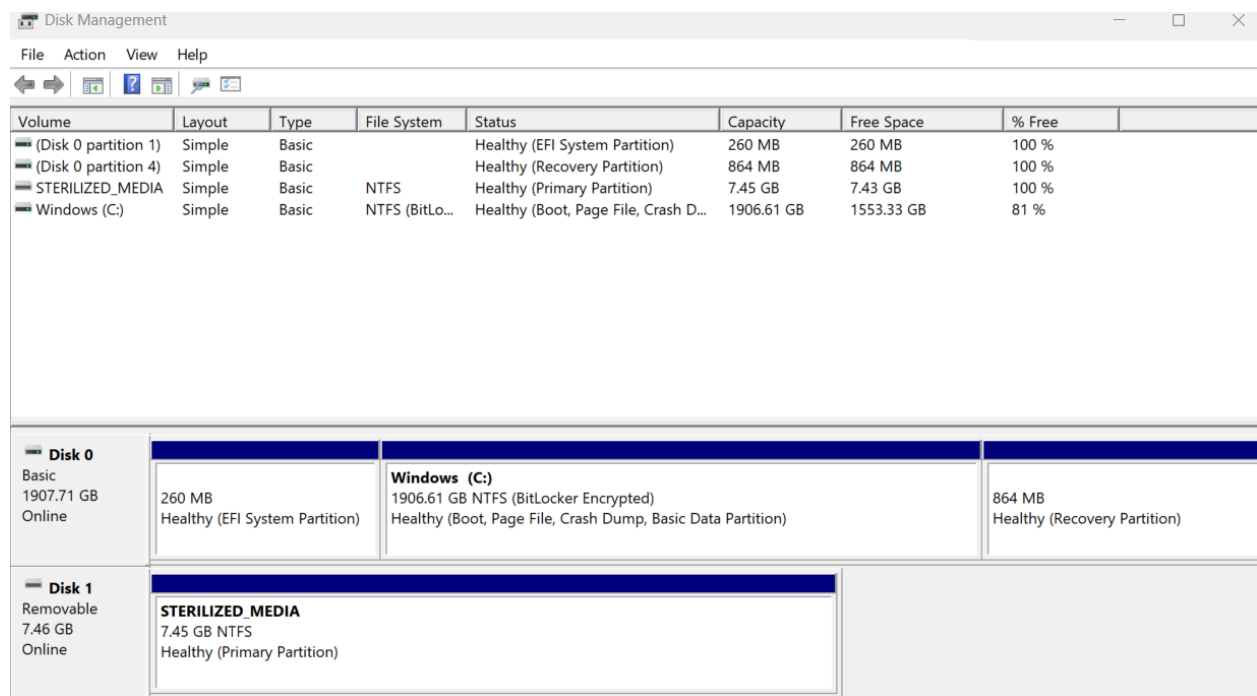
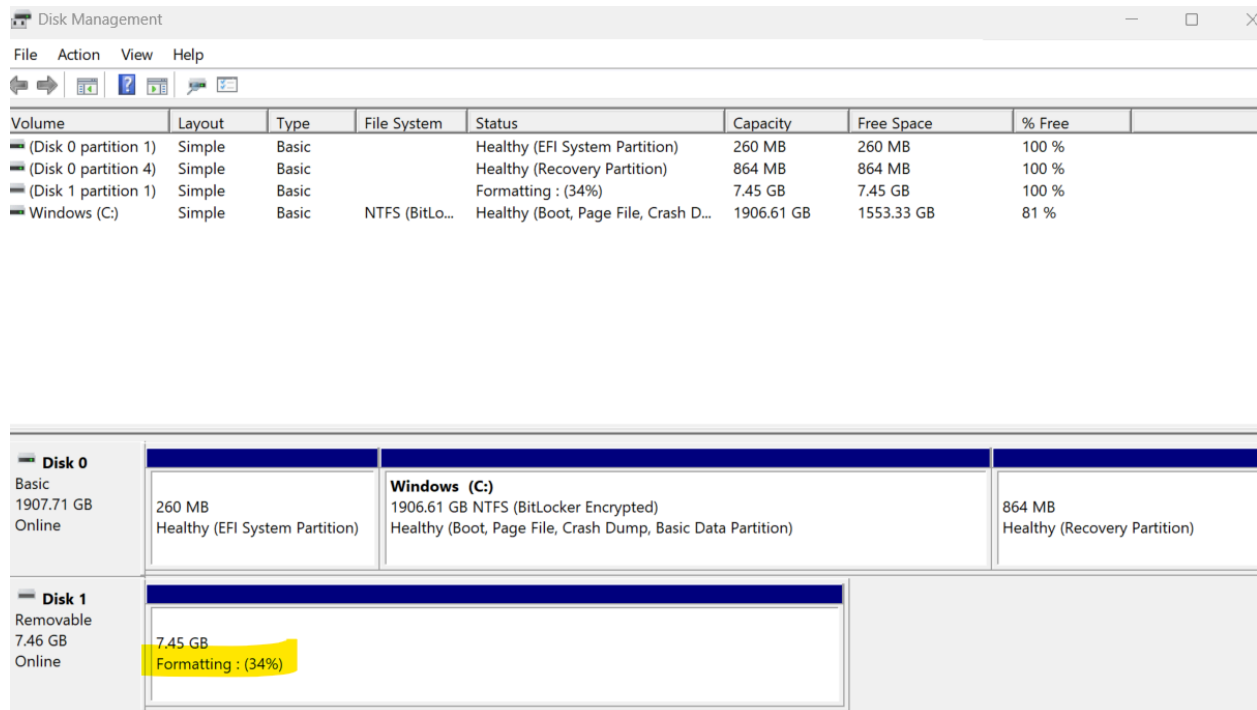


- Figures 10, 11 & 12 - Simple Volume Wizard Setup/Settings

Final Disk State

Final disk configuration:

- **Volume Label:** STERILIZED_MEDIA
- **File System:** NTFS
- **Partition Type:** Primary Partition
- **Capacity:** 7.45 GB
- **Status:** Healthy



- Figures 13 & 14 - Disk Management formatting & finalized state

Conclusion

On February 12, 2026, a SanDisk Cruzer Glide 7.5 GB USB flash drive was successfully forensically sterilized using the DiskPart `clean all` command.

The sterilization process:

- Overwrote all sectors with zeros
- Removed all partition structures
- Eliminated previous FAT32 file system
- Rendered the disk fully unallocated
- Confirmed successful zero-write completion

The device was then reinitialized and formatted with the NTFS file system under the label **STERILIZED_MEDIA**, preparing it for future forensic acquisition.

Based on documented observations and system confirmation messages, the media is considered forensically sterile and suitable for evidentiary use.