USB Forensics: Finding Last Connected USB Device

Aim:

To identify the last connected USB devices on a system using **USBDeview** forensic tool.

Introduction:

USB forensics is important for tracking the use of **removable storage devices** (such as pen drives, hard disks, or input devices) which may contain or transfer sensitive information. Windows maintains registry entries whenever a USB device is connected. Tools like **USBDeview** parse and present this information in a readable format, helping investigators determine:

- Which devices were connected

- Connection timestamps

- Device types and serial numbers

This evidence helps in insider threat investigations, data theft cases, and chain-of-custody tracking.

Procedure:

1. **Download & Launch USBDeview**

   o   Download the **USBDeview** portable tool from Nirsoft official site.

   o   Extract and run USBDeview.exe as **Administrator**.

2. **View Device List** o The main interface lists all USB devices ever connected to the system.

   o   Columns include:

       Device Name / Description

◻ Device Type

◻ Connected Status

◻ Serial Number

◻ Registry Time 1 (first installation date)

◻ Registry Time 2 (last plug/unplug date)

3. **Identify Last Connected Device** ○ Sort results by **Registry Time 2** (last plug/unplug time). ○ Note the **most recent USB device** entry.
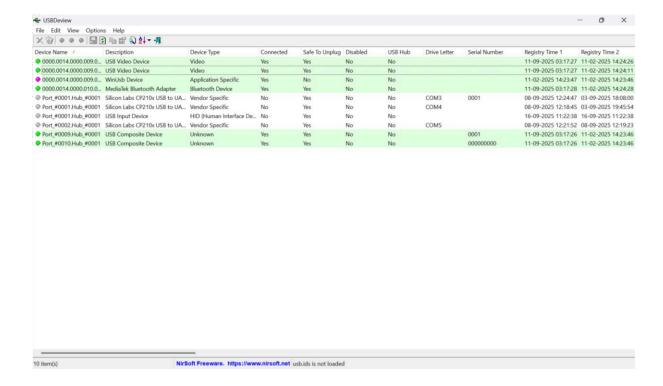
   ○ Collect information such as Device Type, Drive Letter, Serial Number.

4. **Preserve Evidence** ○ Take screenshots of the results.

   ○ Export results to **CSV/HTML/TXT** format using the "Save Selected Items" option.

   ○ Record hashes of exported reports to maintain evidence integrity.

Output (Observation):

From the screenshot provided:

- **Total Devices Detected**: 10 USB devices (Video devices, Bluetooth adapter, Silicon Labs CP210x USB-to-UART, Input devices, Composite devices).

- **Last Connected Device (Registry Time 2)**:

  ○ **USB Video Device** – connected at 11-09-2025 14:24:26 ○ **USB Composite Device** – connected at 11-09-2025 14:24:36

- **Details Captured**:

  ○ Device Type: Video / Composite ○ Drive Letters: COM3, COM4, COM5 (for UART devices) ○ Serial Numbers: (0001, 00000000 etc.) ○ Connection status: "Yes" (currently connected)

This proves the tool successfully recorded both active and historical USB device usage.

Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1	Registry Time 2
0000.0014.0000.009.0...	USB Video Device	Video	Yes	Yes	No	No			11-09-2025 03:17:27	11-02-2025 14:24:26
0000.0014.0000.009.0...	USB Video Device	Video	Yes	Yes	No	No			11-09-2025 03:17:27	11-02-2025 14:24:11
0000.0014.0000.009.0...	WinUsb Device	Application Specific	Yes	No	No	No			11-02-2025 14:23:47	11-02-2025 14:23:46
0000.0014.0000.010.0...	MediaTek Bluetooth Adapter	Bluetooth Device	Yes	Yes	No	No			11-09-2025 03:17:28	11-02-2025 14:24:28
Port_#0001.Hub_#0001	Silicon Labs CP210x USB to UA...	Vendor Specific	No	Yes	No	No	COM3	0001	08-09-2025 12:24:47	03-09-2025 18:08:00
Port_#0001.Hub_#0001	Silicon Labs CP210x USB to UA...	Vendor Specific	No	Yes	No	No	COM4		08-09-2025 12:18:45	03-09-2025 19:45:54
Port_#0001.Hub_#0001	USB Input Device	HID (Human Interface De...	No	Yes	No	No			16-09-2025 11:22:38	16-09-2025 11:22:38
Port_#0002.Hub_#0001	Silicon Labs CP210x USB to UA...	Vendor Specific	No	Yes	No	No	COM5		08-09-2025 12:21:52	08-09-2025 12:19:23
Port_#0009.Hub_#0001	USB Composite Device	Unknown	Yes	Yes	No	No		0001	11-09-2025 03:17:26	11-02-2025 14:23:46
Port_#0010.Hub_#0001	USB Composite Device	Unknown	Yes	Yes	No	No		000000000	11-09-2025 03:17:26	11-02-2025 14:23:46

10 item(s)   NirSoft Freeware. https://www.nirsoft.net usb.ids is not loaded

Result:

Using **USBDeview**, we successfully identified the **last connected USB devices** on the system, along with details such as **type, serial number, connection time, and status**. This information can be preserved as part of a forensic case report to establish timelines of external device usage.