Exp:04 **Name: Madhan kumar**

Roll no:231901028

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**
    - Download the **USBDeview** portable tool from Nirsoft official site.
    - Extract and run USBDeview.exe as **Administrator**.
2. **View Device List** o The main interface lists all USB devices ever connected to the system.
    - Columns include:
        - Device Name / Description

- Device Type
- Connected Status
- Serial Number
- Registry Time 1 (first installation date)
- Registry Time 2 (last plug/unplug date)

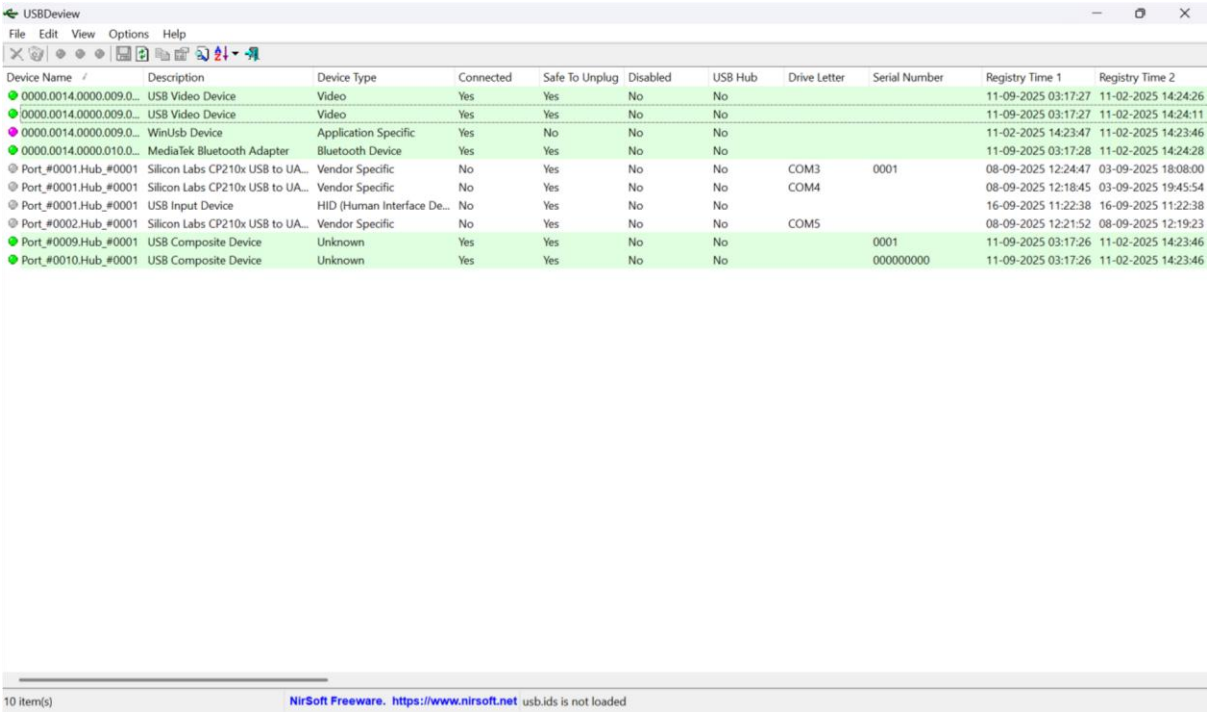
3. **Identify Last Connected Device** ○ Sort results by **Registry Time 2** (last plug/unplug time). ○ Note the **most recent USB device** entry.
    - Collect information such as Device Type, Drive Letter, Serial Number.
4. **Preserve Evidence** ○ Take screenshots of the results.
    - Export results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



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.