Sanjana Asrani **DF**
D17B/01/Batch B **Lab 08: USBDeview**

Aim: To perform USB Device Forensics

Theory:

1. USB Device History in Windows Registry:

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR*: This registry key contains information about USB storage devices previously connected to the system. It includes details such as the vendor ID, product ID, device serial number, and timestamps of device connections. The presence of each entry in this key indicates a unique USB storage device that has been plugged into the system.
- *HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices*: The MountedDevices subkey stores drive letter allocations, which map USB device serial numbers to specific drive letters or volumes that were mounted during device insertion. This mapping provides insights into the drive letters assigned to USB devices and their corresponding serial numbers.
- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2*: This registry key records user accounts associated with connected USB devices. It contains information about which user was logged into Windows when a specific USB device was connected, along with timestamps indicating the last write time for each device entry.
- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Usb*: This registry key holds technical information about connected USB devices, including hardware details and timestamps of device connections. It provides additional insights into the configuration and characteristics of USB devices connected to the system.

2. Identifying First Connection Time:

The first connection time of a USB device can be determined by analyzing specific log files stored on the system:
For Windows Vista, 7, and 8: \Windows\inf\setupapi.dev.log
For Windows 10: \Windows\inf\setupapi.upgrade.log
For Windows XP: \Windows\setupapi.log
By searching for the USB device's serial number in the log file, forensic analysts can retrieve the timestamp of the device's initial connection to the system. This

information helps establish a timeline of events and track the usage history of the USB device.

3. Automating Forensic Analysis:

Tools like USBDeview by Nirsoft simplify the process of extracting information about connected USB devices. USBDeview provides detailed information about each connected USB device, including its name, description, type, serial number, and connection timestamps. By using USBDeview, forensic analysts can efficiently gather and analyze USB device data for investigative purposes.

Features such as Last Plug/Unplug Date in USBDeview help identify the first connection time of a USB device. Additionally, the Created Date indicates the last connection time, aiding in the reconstruction of the device's usage history.

4. Handling USB Devices with MTP Protocol:

USB devices that utilize Media Transfer Protocol (MTP), such as modern smartphones and tablets, present challenges for traditional USB device forensics. Unlike traditional USB storage devices, MTP-connected devices do not leave traces in the Windows Registry.

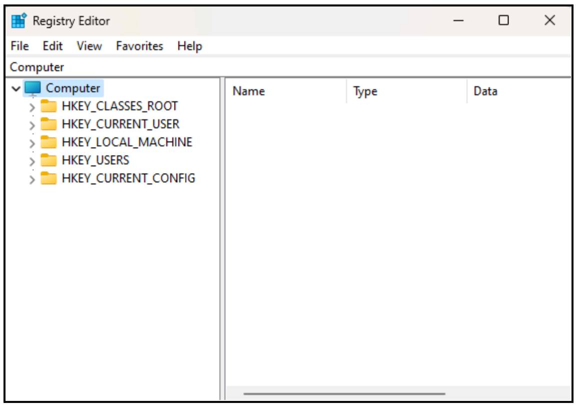
Specialized forensic tools like USB Detective are required to investigate MTP-connected devices and extract relevant information. USB Detective offers advanced features for analyzing MTP-connected devices, including creating timelines of connection/disconnection events and deletion timestamps.

5. Additional Reading:

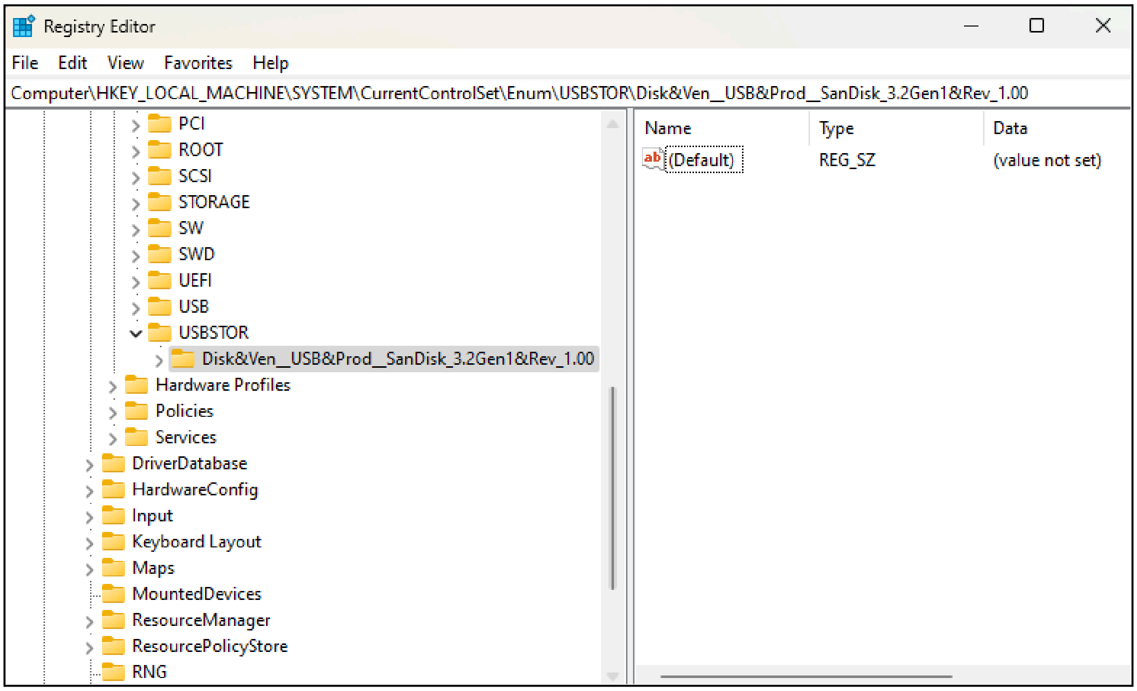
The SANS DFIR Summit presentation and Nicole Ibrahim's blog posts provide additional information about USB devices and Media Transfer Protocol (MTP). USB Forensic Tracker (USBFT) is a free comprehensive suite for investigating USB devices, supporting Windows, Linux, and Mac operating systems. It can retrieve USB device connection artifacts from live systems, mounted forensic images, or volume shadow copies.

Practical:

1. Open Registry Editor in windows



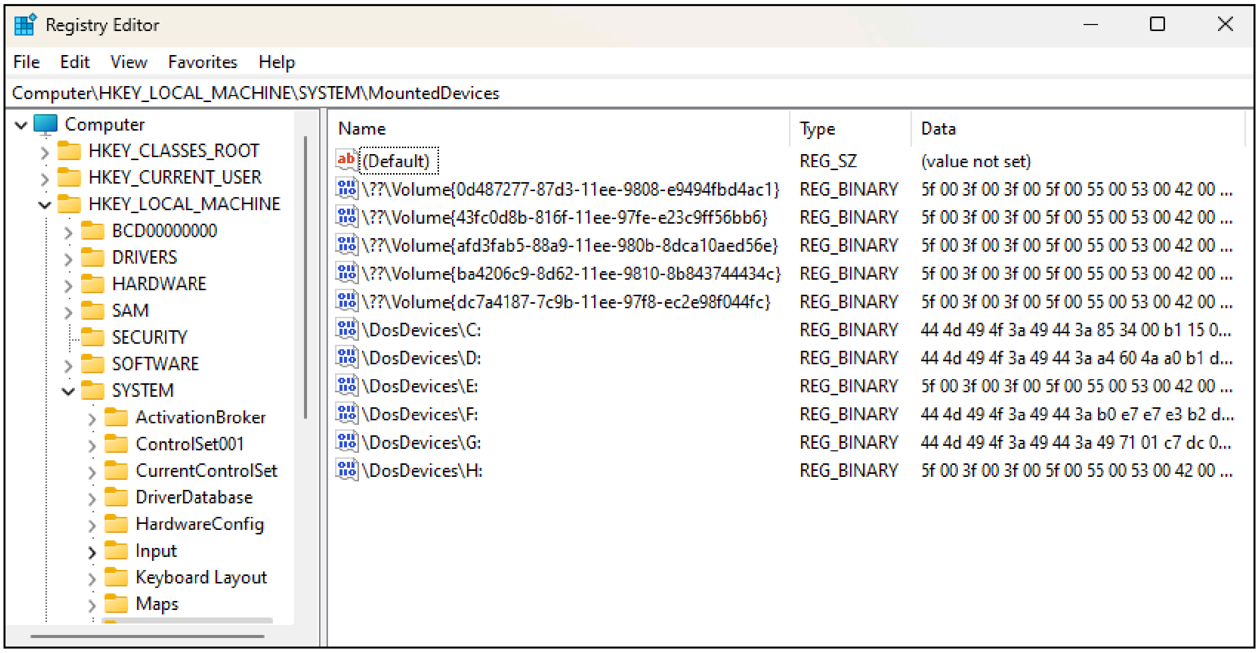
2. USBSTOR → Here you will find all USB devices that have been plugged into the operating system



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven__USB&Prod__SanDisk_3.2Gen1&Rev_1.00

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

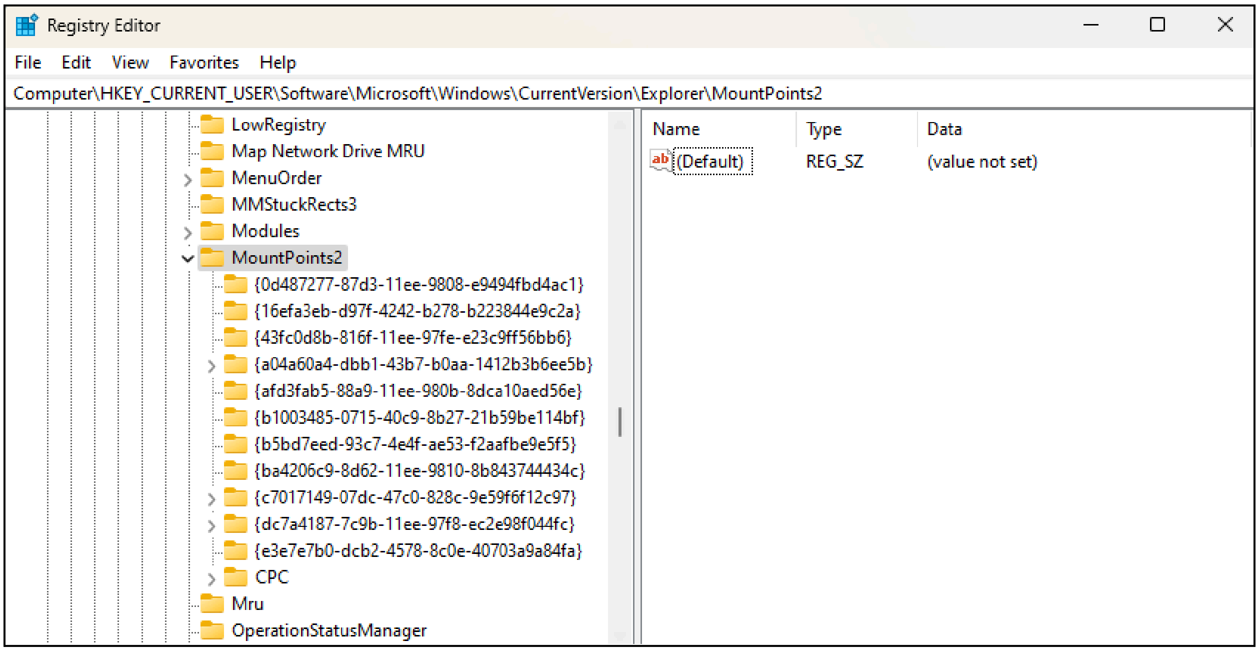
3. MountedDevices → stores the drive letter allocations



Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{0d487277-87d3-11ee-9808-e9494fbd4ac1}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...
\??\Volume{43fc0d8b-816f-11ee-97fe-e23c9ff56bb6}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...
\??\Volume{afd3fab5-88a9-11ee-980b-8dca10aed56e}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...
\??\Volume{ba4206c9-8d62-11ee-9810-8b843744434c}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...
\??\Volume{dc7a4187-7c9b-11ee-97f8-ec2e98f044fc}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...
\DosDevices\C:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 85 34 00 b1 15 0...
\DosDevices\D:	REG_BINARY	44 4d 49 4f 3a 49 44 3a a4 60 4a a0 b1 d...
\DosDevices\E:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...
\DosDevices\F:	REG_BINARY	44 4d 49 4f 3a 49 44 3a b0 e7 e7 e3 b2 d...
\DosDevices\G:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 49 71 01 c7 dc 0...
\DosDevices\H:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 ...

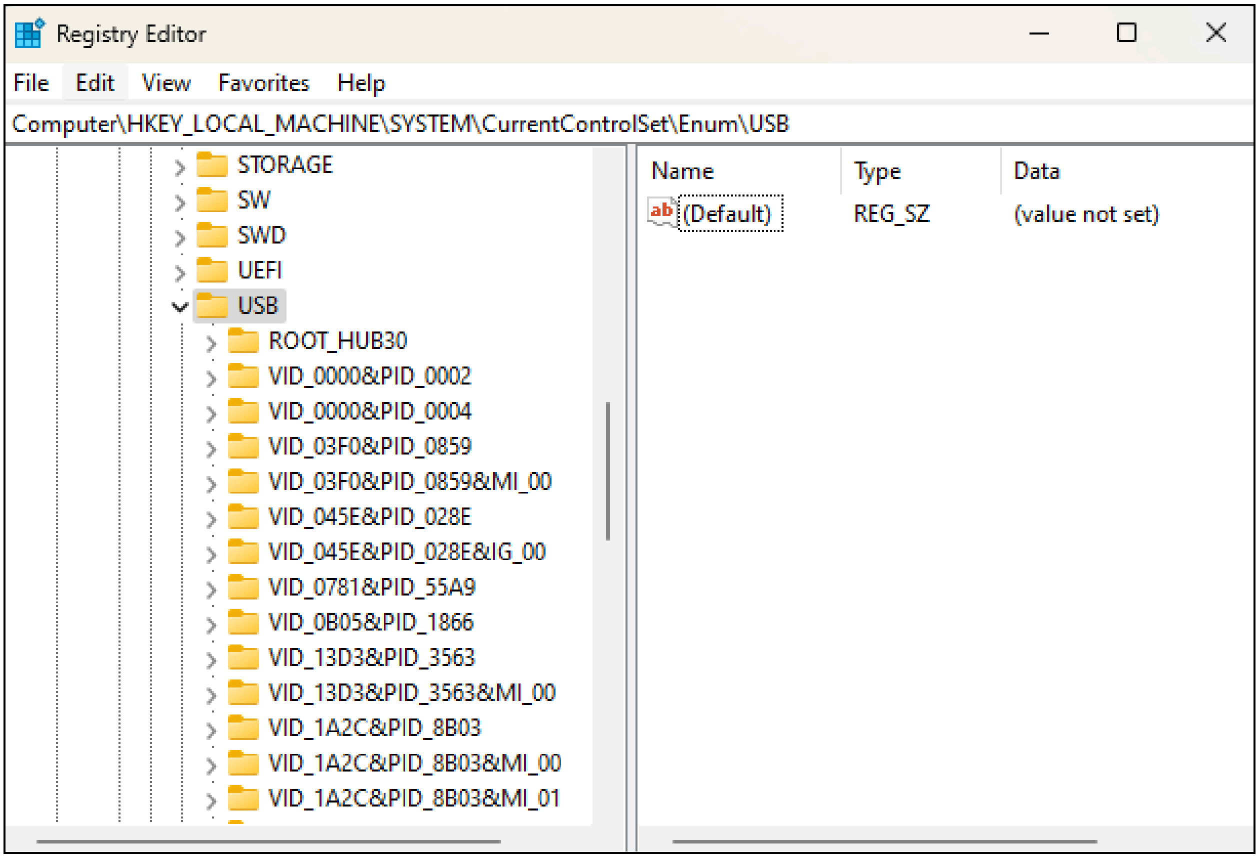
4. MountPoints2 → This key will record which user was logged into Windows when a specific USB device was connected


Registry Editor
File
Edit
View
Favorites
Help
LowRegistry
Map Network Drive MRU
MenuOrder
MMStuckRects3
Modules
MountPoints2
{0d487277-87d3-11ee-9808-e9494fbd4ac1}
{16efa3eb-d97f-4242-b278-b223844e9c2a}
{43fc0d8b-816f-11ee-97fe-e23c9ff56bb6}
{a04a60a4-dbb1-43b7-b0aa-1412b3b6ee5b}
{afd3fab5-88a9-11ee-980b-8dca10aed56e}
{b1003485-0715-40c9-8b27-21b59be114bf}
{b5bd7eed-93c7-4e4f-ae53-f2aafbe9e5f5}
{ba4206c9-8d62-11ee-9810-8b843744434c}
{c7017149-07dc-47c0-828c-9e59f6f12c97}
{dc7a4187-7c9b-11ee-97f8-ec2e98f044fc}
{e3e7e7b0-dcb2-4578-8c0e-40703a9a84fa}
CPC
Mru
OperationStatusManager

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

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

5. Usb → This key holds technical information about each connected USB device

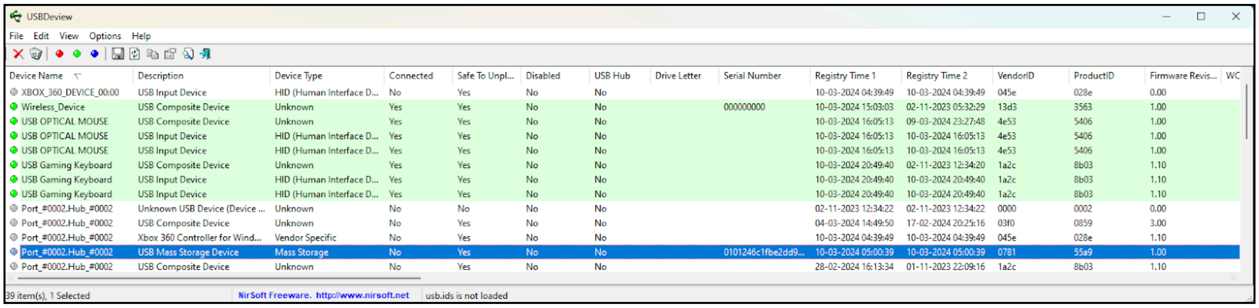


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

- STORAGE
- SW
- SWD
- UEFI
- USB
  - ROOT_HUB30
  - VID_0000&PID_0002
  - VID_0000&PID_0004
  - VID_03F0&PID_0859
  - VID_03F0&PID_0859&MI_00
  - VID_045E&PID_028E
  - VID_045E&PID_028E&IG_00
  - VID_0781&PID_55A9
  - VID_0B05&PID_1866
  - VID_13D3&PID_3563
  - VID_13D3&PID_3563&MI_00
  - VID_1A2C&PID_8B03
  - VID_1A2C&PID_8B03&MI_00
  - VID_1A2C&PID_8B03&MI_01

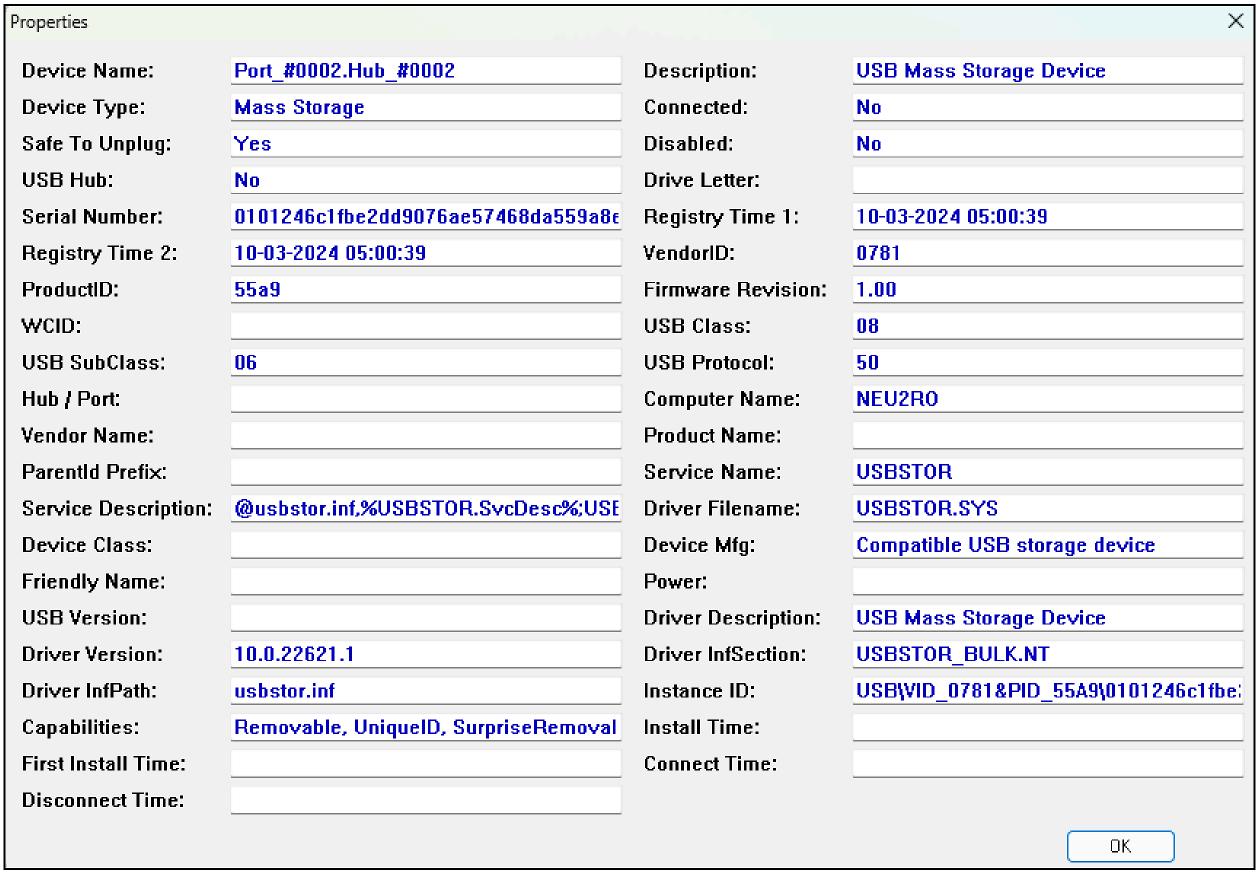
Name	Type	Data
(Default)	REG_SZ	(value not set)

6. Using USBDeview to look for the information of a specific USB device



Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1	Registry Time 2	VendorID	ProductID	Firmware Revis...	WC
XBOX_360_DEVICE_00:00	USB Input Device	HID (Human Interface D...	No	Yes	No	No			10-03-2024 04:39:49	10-03-2024 04:39:49	045e	028e	0.00	
Wireless_Device	USB Composite Device	Unknown	Yes	Yes	No	No		000000000	10-03-2024 15:03:03	02-11-2023 05:32:29	13d3	3563	1.00	
USB OPTICAL MOUSE	USB Composite Device	Unknown	Yes	Yes	No	No			10-03-2024 16:05:13	09-03-2024 23:27:48	4e53	5406	1.00	
USB OPTICAL MOUSE	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			10-03-2024 16:05:13	10-03-2024 16:05:13	4e53	5406	1.00	
USB OPTICAL MOUSE	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			10-03-2024 16:05:13	10-03-2024 16:05:13	4e53	5406	1.00	
USB Gaming Keyboard	USB Composite Device	Unknown	Yes	Yes	No	No			10-03-2024 20:49:40	02-11-2023 12:34:20	1a2c	8b03	1.10	
USB Gaming Keyboard	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			10-03-2024 20:49:40	10-03-2024 20:49:40	1a2c	8b03	1.10	
USB Gaming Keyboard	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			10-03-2024 20:49:40	10-03-2024 20:49:40	1a2c	8b03	1.10	
Port_#0002.Hub_#0002	Unknown USB Device (Device ...	Unknown	No	No	No	No			02-11-2023 12:34:22	02-11-2023 12:34:22	0000	0002	0.00	
Port_#0002.Hub_#0002	USB Composite Device	Unknown	No	Yes	No	No			04-03-2024 14:49:50	17-02-2024 20:25:16	03f0	0859	3.00	
Port_#0002.Hub_#0002	Xbox 360 Controller for Wind...	Vendor Specific	No	Yes	No	No			10-03-2024 04:39:49	10-03-2024 04:39:49	045e	028e	1.10	
Port_#0002.Hub_#0002	USB Mass Storage Device	Mass Storage	No	Yes	No	No		0101246c1fbe2dd9...	10-03-2024 05:00:39	10-03-2024 05:00:39	0781	55a9	1.00	
Port_#0002.Hub_#0002	USB Composite Device	Unknown	No	Yes	No	No			28-02-2024 16:13:34	01-11-2023 22:09:16	1a2c	8b03	1.10	

39 item(s), 1 Selected | NirSoft Freeware. http://www.nirsoft.net | usb.ids is not loaded



Device Name:	Port_#0002.Hub_#0002	Description:	USB Mass Storage Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	
Serial Number:	0101246c1fbe2dd9076ae57468da559a8e	Registry Time 1:	10-03-2024 05:00:39
Registry Time 2:	10-03-2024 05:00:39	VendorID:	0781
ProductID:	55a9	Firmware Revision:	1.00
WCID:		USB Class:	08
USB SubClass:	06	USB Protocol:	50
Hub / Port:		Computer Name:	NEU2RO
Vendor Name:		Product Name:	
ParentId Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USE	Driver Filename:	USBSTOR.SYS
Device Class:		Device Mfg:	Compatible USB storage device
Friendly Name:		Power:	
USB Version:		Driver Description:	USB Mass Storage Device
Driver Version:	10.0.22621.1	Driver InfSection:	USBSTOR_BULK.NT
Driver InfPath:	usbstor.inf	Instance ID:	USB\VID_0781&PID_55A9\0101246c1fbe
Capabilities:	Removable, UniqueID, SurpriseRemoval	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			

Conclusion: