Experiment: 7

Aim: To perform USB Device Forensics

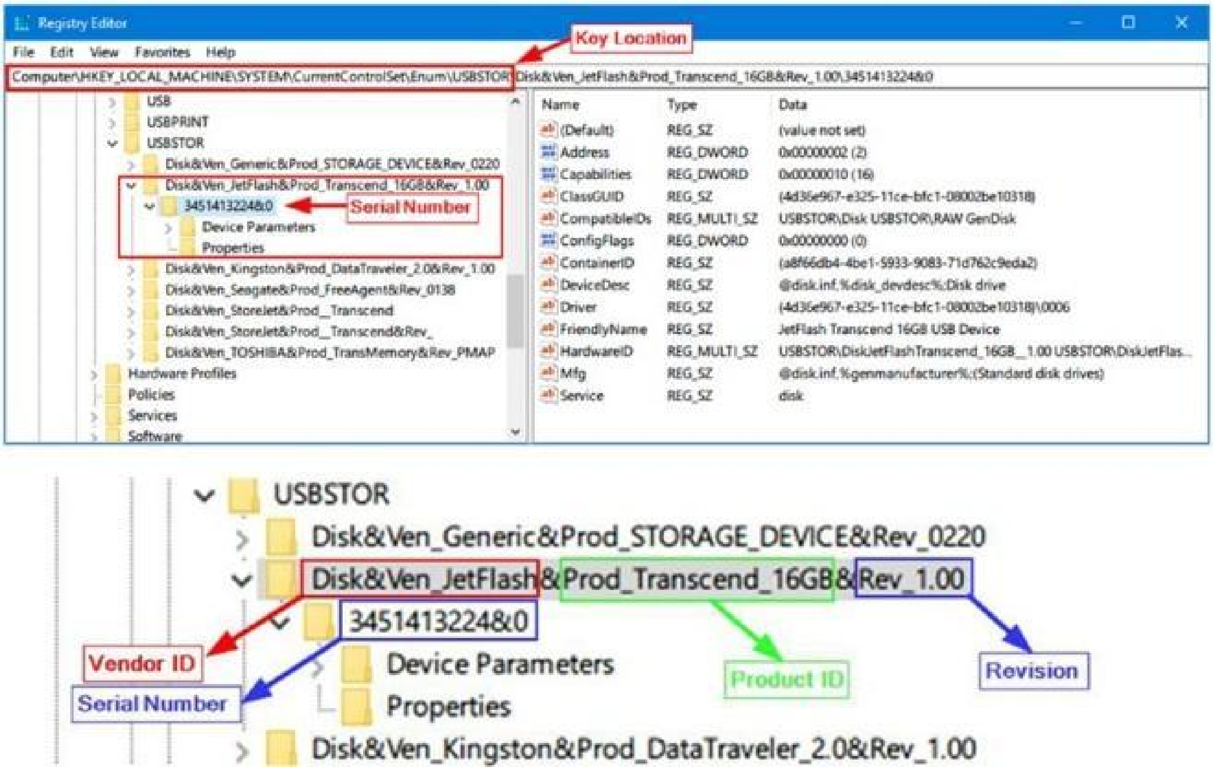
Theory:

Windows keeps a history log of all previously connected USB devices along with their connection times in addition to the associated user account which installs them. The Windows registry also stores important technical information for each connected USB device such as vendor ID, product ID, revision, and serial number.

Windows stores USB history-related information using five registry keys, where each key offers a different piece of information about the connected device. By merging this information together, investigators will have an idea of how an offender has used removable devices such as a USB to conduct/facilitate his/her actions.

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR Here you will find all USB devices that have been plugged into the operating system since its installation. It shows the USB vendor ID (manufacturer name), product ID, and the device serial number (note that if the second character of the device serial number is “&,” it means the connected device does not have a serial number and the device ID has been generated by the system). See Figure

8.1 for a list of previously connected USB devices on the author’s machine.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_1.00\3451413224&0

```
USB
USBPRINT
USBSTOR
    Disk&Ven_Generic&Prod_STORAGE_DEVICE&Rev_0220
    Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_1.00
        3451413224&0
            Device Parameters
            Properties
    Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_1.00
    Disk&Ven_Seagate&Prod_FreeAgent&Rev_0138
    Disk&Ven_StoreJet&Prod__Transcend
    Disk&Ven_StoreJet&Prod__Transcend&Rev_
    Disk&Ven_TOSHIBA&Prod_TransMemory&Rev_PMAP
Hardware Profiles
Policies
Services
Software
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000002 (2)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{a8f66db4-4be1-5933-9083-71d762c9eda2}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0006
FriendlyName	REG_SZ	JetFlash Transcend 16GB USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskJetFlashTranscend_16GB__1.00 USBSTOR\DiskJetFlas...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

```
USBSTOR
    Disk&Ven_Generic&Prod_STORAGE_DEVICE&Rev_0220
    Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_1.00
        3451413224&0
            Device Parameters
            Properties
    Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_1.00
```

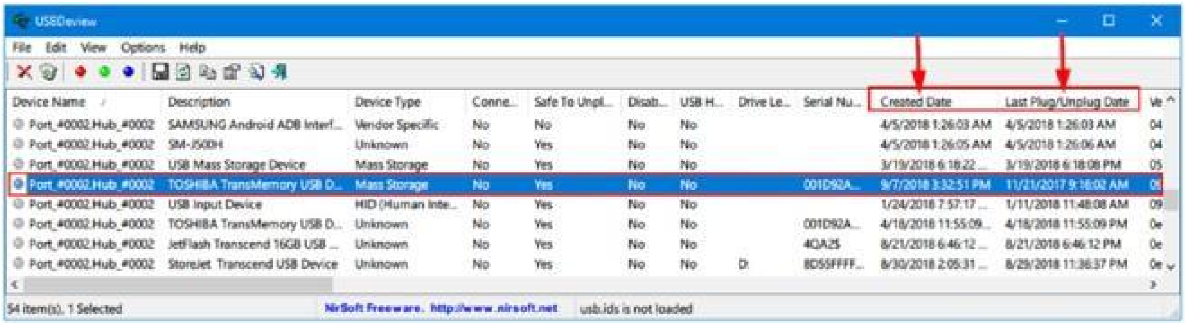
Expt 8.1 History of USB connected devices

2. HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices The MountedDevices subkey stores the drive letter allocations; it matches the serial number of a USB device to a given drive letter
or volume that was mounted when the USB device was inserted.
3.
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints 2 This key will record which user was logged into Windows when a specific USB device was connected. The key also includes the “Last Write Time” for each device that was connected to the system.
4. HKEY_LOCAL_MACHINE\SYSTEM\Currentcontrolset\Enum\Usb This key holds technical information about each connected USB device in addition to the last time the subject USB was
connected to the investigated computer.

5. Identify the first time device was connected: Check this file at \Windows\inf\setupapi.dev.log for Windows Vista, 7, and 8, and at \Windows\inf\setupapi.upgrade.log for Windows 10.
On Windows XP, this file will be located at \Windows\setupapi.log. Search in this file for a particular USB device’s serial number to learn when it was first connected to the subject system (in local time).

To automate the process of finding information about the current and previous USB connected devices, you can download a free tool by Nirsoft that can perform all the tasks we just did manually; this tool is called USBDeview (www.nirsoft.net/utils/usb_devices_view.html). After executing this tool on the target system, extended information (e.g., device name/description, device type, serial number, and much more) about each connected USB device will appear.

In Figure8.2, the Last Plug/Unplug Date represents the first time that the device was connected to the system. This date does not change when the same device is repeatedly reinserted. The “Created Date” represents the last time that the same device was attached to the system.



Device Name	Description	Device Type	Conne...	Safe To Unpl...	Disab...	USB H...	Drive Le...	Serial Nu...	Created Date	Last Plug/Unplug Date	Ve
Port_#0002.Hub_#0002	SAMSUNG Android ADB Interf...	Vendor Specific	No	No	No	No			4/5/2018 1:26:03 AM	4/5/2018 1:26:03 AM	04
Port_#0002.Hub_#0002	SM-J500H	Unknown	No	Yes	No	No			4/5/2018 1:26:05 AM	4/5/2018 1:26:06 AM	04
Port_#0002.Hub_#0002	USB Mass Storage Device	Mass Storage	No	Yes	No	No			3/19/2018 6:18:22 ...	3/19/2018 6:18:08 PM	05
Port_#0002.Hub_#0002	TOSHIBA TransMemory USB D...	Mass Storage	No	Yes	No	No		001D92A...	9/7/2018 3:32:51 PM	11/21/2017 9:16:02 AM	0
Port_#0002.Hub_#0002	USB Input Device	HID (Human Inte...	No	Yes	No	No			1/24/2018 7:57:17 ...	1/11/2018 11:48:08 AM	09
Port_#0002.Hub_#0002	TOSHIBA TransMemory USB D...	Unknown	No	Yes	No	No		001D92A...	4/18/2018 11:55:09...	4/18/2018 11:55:09 PM	0e
Port_#0002.Hub_#0002	JetFlash Transcend 16GB USB ...	Unknown	No	Yes	No	No		4QA25	8/21/2018 6:46:12 ...	8/21/2018 6:46:12 PM	0e
Port_#0002.Hub_#0002	StoreJet Transcend USB Device	Unknown	No	Yes	No	No	D:	8D55FFFF...	8/30/2018 2:05:31 ...	8/29/2018 11:36:37 PM	0e

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

Figure 8.2 Using USBDeview to view different artifacts about previously connected USB devices

Unfortunately, not all USB device types will leave traces in Windows registry as we have described, for instance, USB devices that use media transfer protocol (MTP) when connecting with computers. Devices equipped with the modern Android OS versions in addition to Windows phones and Blackberry all use the MTP protocol; this protocol does not leave traces in the Windows registry when a USB device is connected to a Windows computer. This necessitates a specialized tool to handle the investigation of such artifacts.

USB Detective (https://usbdetective.com) supports detecting USB devices that use the MTP protocol to connect to Windows. It also offers rich features for thoroughly investigating connected USB devices, like creating timelines of all unique connection/disconnection and deletion timestamps for each device; however, you need to upgrade to the professional paid version to use all features.

To conclude this section, a USB device connected through an MTP connection needs special treatment to acquire its traces from a Windows machine; consult your computer forensic software documentation for the availability of such a feature.

ADDITIONAL READING

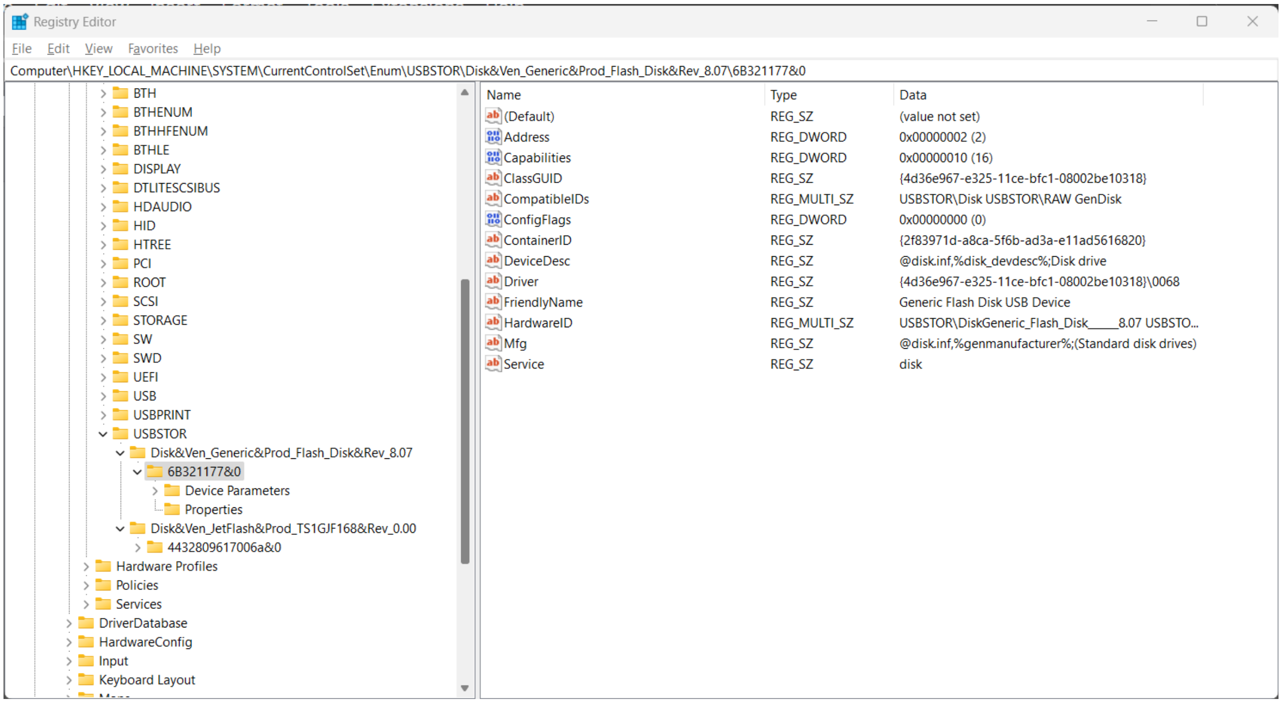
More information about USB devices and MTP can be found at

- SANS DFIR Summit presentation: https://digital-forensics.sans.org/summit-archives/dfir14/USB_Devices_and_Media_Transfer_Protocol_Nicole_Ibrahim.pdf
- Nicole Ibrahim's series of blog posts about this topic: http://nicoleibrahim.com/part-1-mtp-and-ptp-usb-device-research/

Note! USB Forensic Tracker (USBFT), available at http://www.orionforensics.com/forensics-tools/usb-forensic-tracker/ , is a free, comprehensive suite for investigating USB devices. It supports Windows, Linux, and Mac and can retrieve USB device connection artifacts from live systems, mounted forensic images, or volume shadow copies.

Output:

Using Registry editor

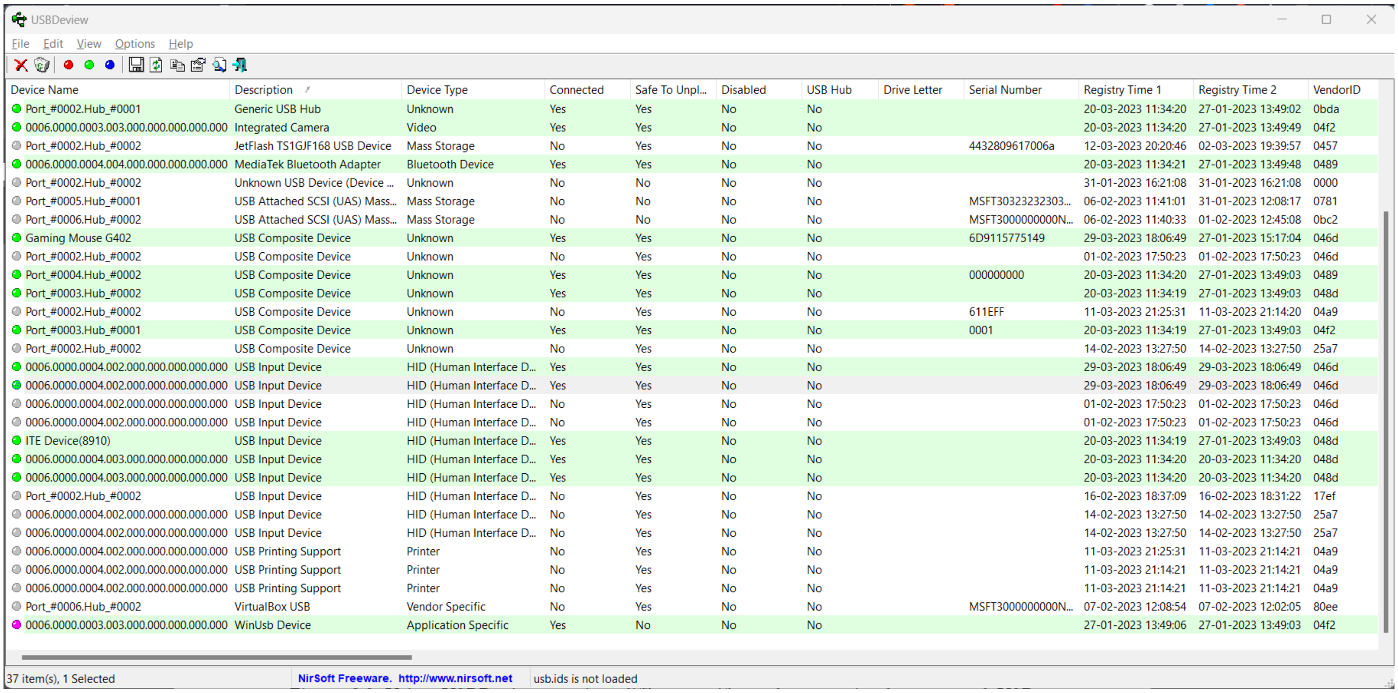


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07\6B321177&0

```
        > BTH
        > BTHENUM
        > BTHHFENUM
        > BTHLE
        > DISPLAY
        > DTLITESCSIBUS
        > HDAUDIO
        > HID
        > HTREE
        > PCI
        > ROOT
        > SCSI
        > STORAGE
        > SW
        > SWD
        > UEFI
        > USB
        > USBPRINT
        v USBSTOR
            v Disk&Ven_Generic&Prod_Flash_Disk&Rev_8.07
                v 6B321177&0
                    > Device Parameters
                      Properties
            v Disk&Ven_JetFlash&Prod_TS1GJF168&Rev_0.00
                > 4432809617006a&0
    > Hardware Profiles
    > Policies
    > Services
  > DriverDatabase
  > HardwareConfig
  > Input
  > Keyboard Layout
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000002 (2)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{2f83971d-a8ca-5f6b-ad3a-e11ad5616820}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0068
FriendlyName	REG_SZ	Generic Flash Disk USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskGeneric_Flash_Disk_____8.07 USBSTO...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

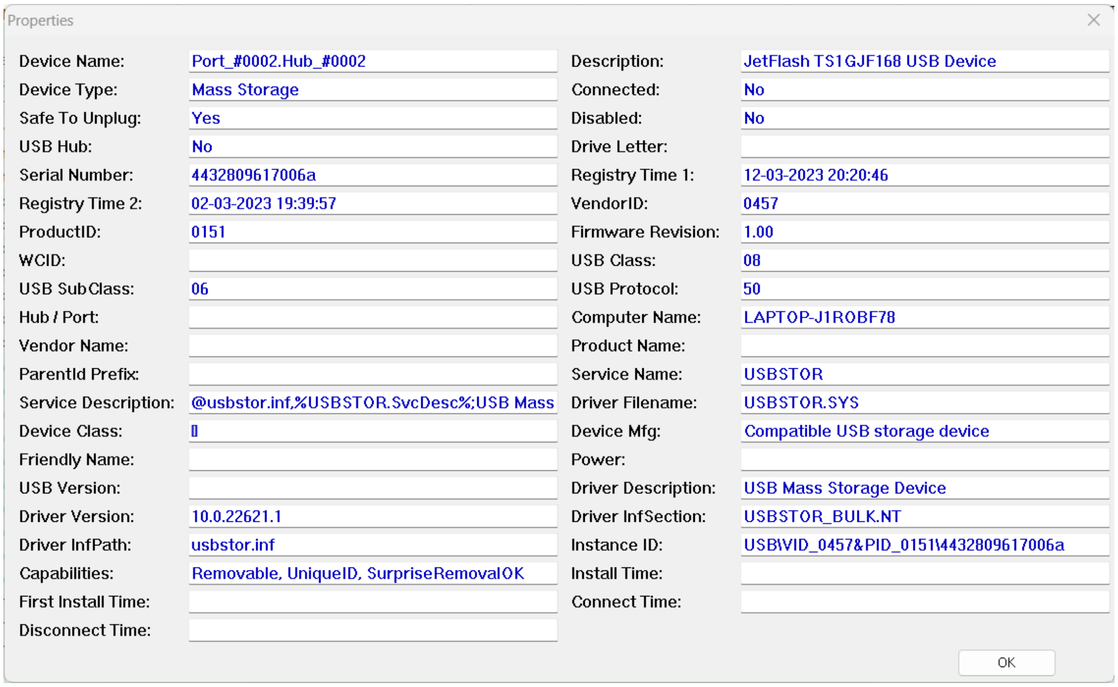
Using USBDeview(Automated tool)



Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1	Registry Time 2	VendorID
Port_#0002.Hub_#0001	Generic USB Hub	Unknown	Yes	Yes	No	No			20-03-2023 11:34:20	27-01-2023 13:49:02	0bda
0006.0000.0003.003.000.000.000.000.000	Integrated Camera	Video	Yes	Yes	No	No			20-03-2023 11:34:20	27-01-2023 13:49:49	04f2
Port_#0002.Hub_#0002	JetFlash TS1GJF168 USB Device	Mass Storage	No	Yes	No	No		4432809617006a	12-03-2023 20:20:46	02-03-2023 19:39:57	0457
0006.0000.0004.004.000.000.000.000.000	MediaTek Bluetooth Adapter	Bluetooth Device	Yes	Yes	No	No			20-03-2023 11:34:21	27-01-2023 13:49:48	0489
Port_#0002.Hub_#0002	Unknown USB Device (Device ...	Unknown	No	No	No	No			31-01-2023 16:21:08	31-01-2023 16:21:08	0000
Port_#0005.Hub_#0001	USB Attached SCSI (UAS) Mass...	Mass Storage	No	No	No	No		MSFT30323232303...	06-02-2023 11:41:01	31-01-2023 12:08:17	0781
Port_#0006.Hub_#0002	USB Attached SCSI (UAS) Mass...	Mass Storage	No	No	No	No		MSFT3000000000N...	06-02-2023 11:40:33	01-02-2023 12:45:08	0bc2
Gaming Mouse G402	USB Composite Device	Unknown	Yes	Yes	No	No		6D9115775149	29-03-2023 18:06:49	27-01-2023 15:17:04	046d
Port_#0002.Hub_#0002	USB Composite Device	Unknown	No	Yes	No	No			01-02-2023 17:50:23	01-02-2023 17:50:23	046d
Port_#0004.Hub_#0002	USB Composite Device	Unknown	Yes	Yes	No	No		000000000	20-03-2023 11:34:20	27-01-2023 13:49:03	0489
Port_#0003.Hub_#0002	USB Composite Device	Unknown	Yes	Yes	No	No			20-03-2023 11:34:19	27-01-2023 13:49:03	048d
Port_#0002.Hub_#0002	USB Composite Device	Unknown	No	Yes	No	No		611EFF	11-03-2023 21:25:31	11-03-2023 21:14:20	04a9
Port_#0003.Hub_#0001	USB Composite Device	Unknown	Yes	Yes	No	No		0001	20-03-2023 11:34:19	27-01-2023 13:49:03	04f2
Port_#0002.Hub_#0002	USB Composite Device	Unknown	No	Yes	No	No			14-02-2023 13:27:50	14-02-2023 13:27:50	25a7
0006.0000.0004.002.000.000.000.000.000	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			29-03-2023 18:06:49	29-03-2023 18:06:49	046d
0006.0000.0004.002.000.000.000.000.000	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			29-03-2023 18:06:49	29-03-2023 18:06:49	046d
0006.0000.0004.002.000.000.000.000.000	USB Input Device	HID (Human Interface D...	No	Yes	No	No			01-02-2023 17:50:23	01-02-2023 17:50:23	046d
0006.0000.0004.002.000.000.000.000.000	USB Input Device	HID (Human Interface D...	No	Yes	No	No			01-02-2023 17:50:23	01-02-2023 17:50:23	046d
ITE Device(8910)	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			20-03-2023 11:34:19	27-01-2023 13:49:03	048d
0006.0000.0004.003.000.000.000.000.000	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			20-03-2023 11:34:20	20-03-2023 11:34:20	048d
0006.0000.0004.003.000.000.000.000.000	USB Input Device	HID (Human Interface D...	Yes	Yes	No	No			20-03-2023 11:34:20	20-03-2023 11:34:20	048d
Port_#0002.Hub_#0002	USB Input Device	HID (Human Interface D...	No	Yes	No	No			16-02-2023 18:37:09	16-02-2023 18:31:22	17ef
0006.0000.0004.002.000.000.000.000.000	USB Input Device	HID (Human Interface D...	No	Yes	No	No			14-02-2023 13:27:50	14-02-2023 13:27:50	25a7
0006.0000.0004.002.000.000.000.000.000	USB Input Device	HID (Human Interface D...	No	Yes	No	No			14-02-2023 13:27:50	14-02-2023 13:27:50	25a7
0006.0000.0004.002.000.000.000.000.000	USB Printing Support	Printer	No	Yes	No	No			11-03-2023 21:25:31	11-03-2023 21:14:21	04a9
0006.0000.0004.002.000.000.000.000.000	USB Printing Support	Printer	No	Yes	No	No			11-03-2023 21:14:21	11-03-2023 21:14:21	04a9
0006.0000.0004.002.000.000.000.000.000	USB Printing Support	Printer	No	Yes	No	No			11-03-2023 21:14:21	11-03-2023 21:14:21	04a9
Port_#0006.Hub_#0002	VirtualBox USB	Vendor Specific	No	Yes	No	No		MSFT3000000000N...	07-02-2023 12:08:54	07-02-2023 12:02:05	80ee
0006.0000.0003.003.000.000.000.000.000	WinUsb Device	Application Specific	Yes	No	No	No			27-01-2023 13:49:06	27-01-2023 13:49:03	04f2

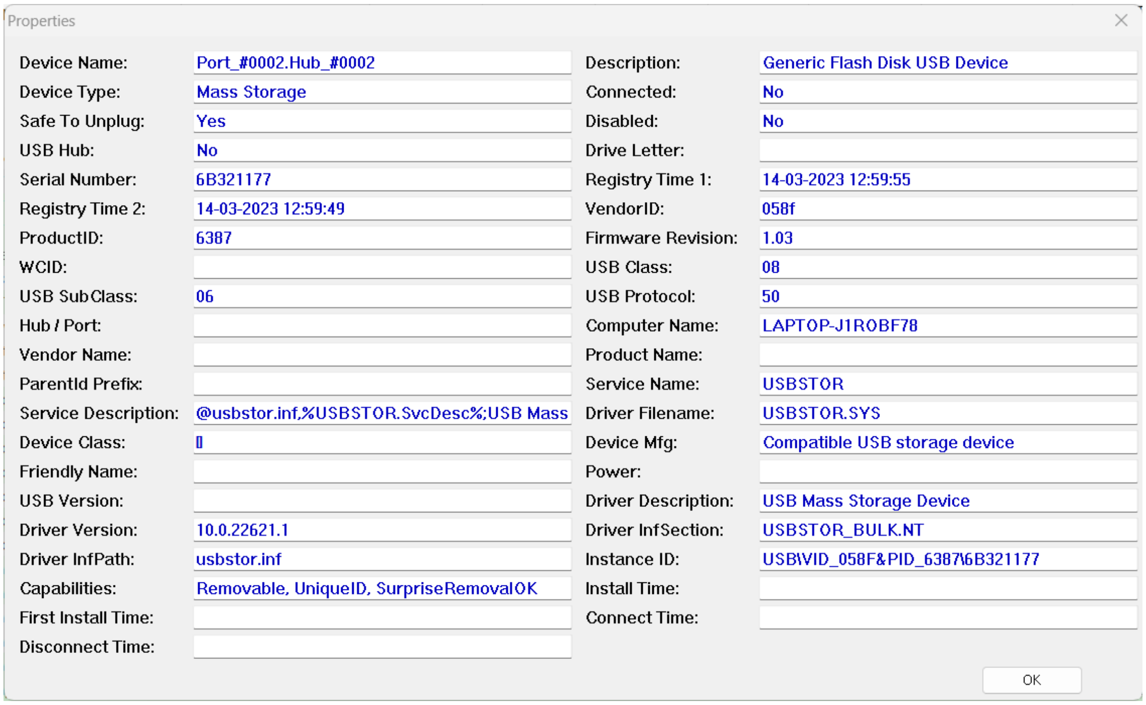
37 item(s), 1 Selected   NirSoft Freeware. http://www.nirsoft.net   usb.ids is not loaded

Jetflash Device Properties



Device Name:	Port_#0002.Hub_#0002	Description:	JetFlash TS1GJF168 USB Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	
Serial Number:	4432809617006a	Registry Time 1:	12-03-2023 20:20:46
Registry Time 2:	02-03-2023 19:39:57	VendorID:	0457
ProductID:	0151	Firmware Revision:	1.00
WCID:		USB Class:	08
USB SubClass:	06	USB Protocol:	50
Hub / Port:		Computer Name:	LAPTOP-J1ROBF78
Vendor Name:		Product Name:	
ParentId Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USB Mass	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_0457&PID_0151\4432809617006a
Capabilities:	Removable, UniqueID, SurpriseRemovalOK	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			

Generic Flash Disk Properties



Device Name:	Port_#0002.Hub_#0002	Description:	Generic Flash Disk USB Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	
Serial Number:	6B321177	Registry Time 1:	14-03-2023 12:59:55
Registry Time 2:	14-03-2023 12:59:49	VendorID:	058f
ProductID:	6387	Firmware Revision:	1.03
WCID:		USB Class:	08
USB SubClass:	06	USB Protocol:	50
Hub / Port:		Computer Name:	LAPTOP-J1ROBF78
Vendor Name:		Product Name:	
ParentId Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USB Mass	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_058F&PID_6387\6B321177
Capabilities:	Removable, UniqueID, SurpriseRemovalOK	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			

Conclusion: In conclusion, USB device forensics is an important aspect of digital forensics that involves the examination and analysis of USB devices and their usage on a computer system.Forensic tools like USB Detective can be used to examine and analyze different artifacts related to previously connected USB devices, including device information, connection history, file activity, and registry entries.