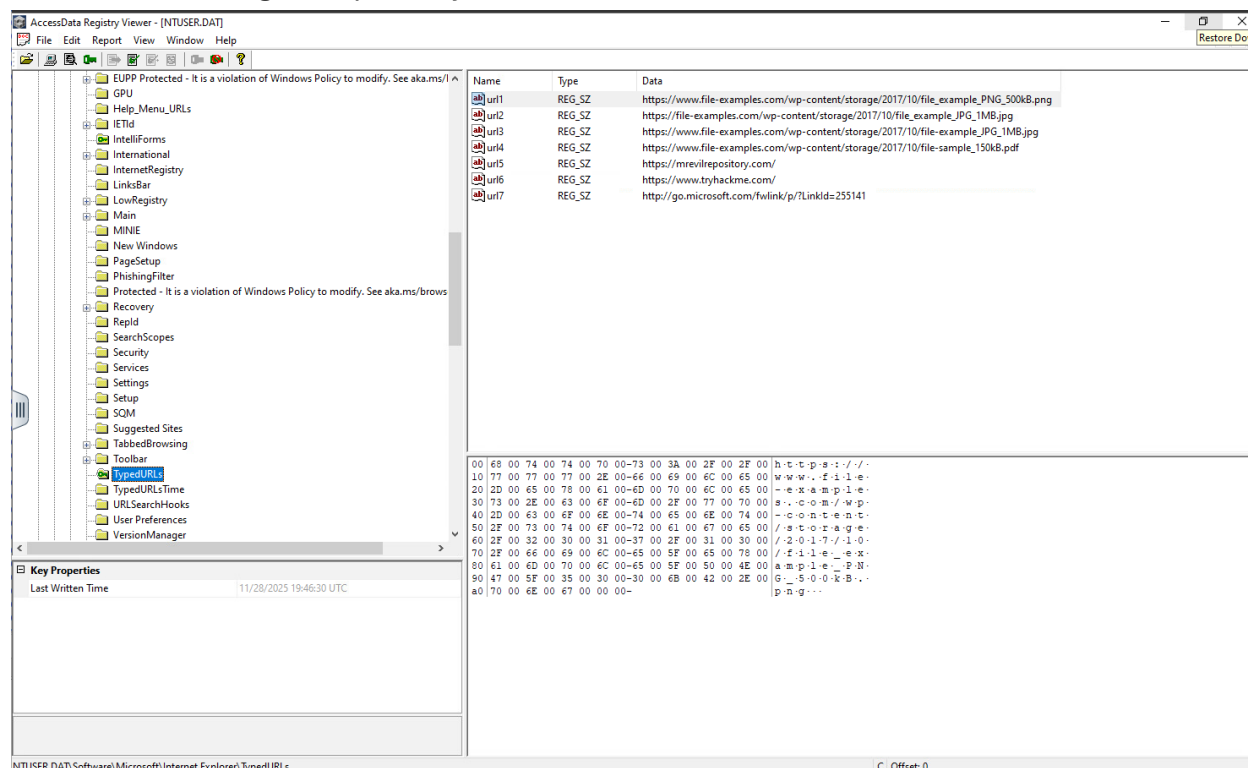


MREVIL NTUSER.DAT file evidence:

Located at: Software -> Microsoft -> Internet Explorer -> TypedURLs are the recent search history of the user inside of microsofts internet explorer. The following image shows the visited URLs from most recent (url1) to oldest (url7). We can see that MREVIL visited a few domains, including his repository, and visited sites where he downloaded some files.



Located at: Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> MountPoints2 -> {9b383cf9-cca7-11f0-87a1-080027c0d483} -> _Autorun -> DefaultIcon / DefaultLabel contains information about mounted devices used by the user associated with the examined NTUSER.DAT file. The DefaultIcon file contains the mount point E:\ and DefaultLabel contains the name of the device: DEFT_8. This is evidence of the use of the export drive to extract the evidence.

AccessData Registry Viewer - [NTUSER.DAT]

File Edit Report View Window Help

Explorer

- Accent
- Advanced
- AppContract
- AutoplayHandlers
- BamThrottling
- BannerStore
- BitBucket
- CabinetState
- CD Burning
- CIDSave
- CLSID
- ComDlg32
- Desktop
- Discardable
- FileExts
- HideDesktopIcons
- LogonStats
- LowRegistry
- MenuOrder
- Modules
- MountPoints2
 - (1d7ef16a-0000-0000-0000-602200000000)
 - (7f3f1ef-cca7-11f0-87a0-806e6f6e6963)
 - (9b383cf9-cca7-11f0-87a1-080027c0d483)
 - _Autorun
 - DefaultIcon
 - DefaultLabel
 - CPC
 - Package Installation
 - RecentDocs
 - Ribbon

Key Properties

Last Written Time 11/28/2025 19:48:09 UTC

Name	Type	Data
(default)	REG_SZ	"E:\autorun.ico"

00 22 00 45 00 3a 00 5c 00 61 00 75 00 74 00 6f 00 "E:\a u t o r u n . i c o ."
10 72 00 75 00 6e 00 2e 00 69 00 63 00 6f 00 22 00 z u n . i c o ."
20 20 00 00 00

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{9b383cf9-cca7-11f0-87a1-080027c0d483}_Autorun\DefaultIcon Offset: 0

AccessData Registry Viewer - [NTUSER.DAT]

File Edit Report View Window Help

Explorer

- Accent
- Advanced
- AppContract
- AutoplayHandlers
- BamThrottling
- BannerStore
- BitBucket
- CabinetState
- CD Burning
- CIDSave
- CLSID
- ComDlg32
- Desktop
- Discardable
- FileExts
- HideDesktopIcons
- LogonStats
- LowRegistry
- MenuOrder
- Modules
- MountPoints2
 - (1d7ef16a-0000-0000-0000-602200000000)
 - (7f3f1ef-cca7-11f0-87a0-806e6f6e6963)
 - (9b383cf9-cca7-11f0-87a1-080027c0d483)
 - _Autorun
 - DefaultIcon
 - DefaultLabel
 - CPC
 - Package Installation
 - RecentDocs
 - Ribbon

Key Properties

Last Written Time 11/28/2025 19:48:09 UTC

Name	Type	Data
(default)	REG_SZ	DEFT_8

0 44 00 45 00 46 00 54 00 5f 00 38 00 00 00 D E F T _ 8 . . .

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{9b383cf9-cca7-11f0-87a1-080027c0d483}_Autorun\DefaultLabel Offset: 0

Located at: Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> RecentDocs -> .jpg / .png / .pdf / Folder is data containing the documents and folders accessed through internet explorer by MREVL. This evidence likely suggests that the files were downloaded to MREVL Onedrive folder, and then transferred to the export drive.

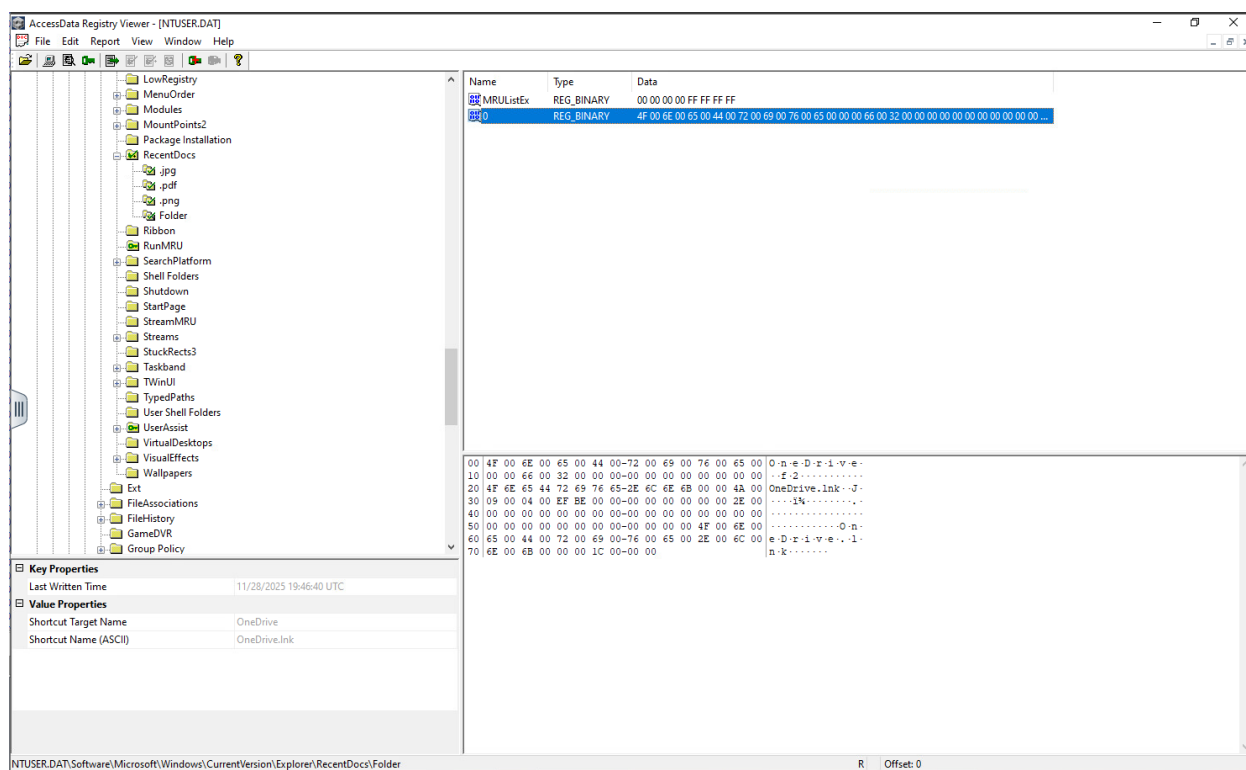
The image displays two screenshots of the AccessData Registry Viewer (NTUSER.DAT) showing registry data for the RecentDocs folder. The top screenshot shows the registry path NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\jpg. The bottom screenshot shows the registry path NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\pdf.

Top Screenshot (RecentDocs\jpg):

- Key Properties:** Last Written Time: 11/28/2025 19:45:36 UTC
- Value Properties:** Shortcut Target Name: file_example_JPG_1MB.jpg, Shortcut Name (ASCII): file_example_JPG_1MB.lnk
- Registry Data:** The registry value is a REG_BINARY type. The data is a hex string: 00 00 00 00 FF FF FF FF. The hex dump shows the file path: file_example_JPG_1MB.lnk.

Bottom Screenshot (RecentDocs\pdf):

- Key Properties:** Last Written Time: 11/28/2025 19:43:37 UTC
- Value Properties:** Shortcut Target Name: file-sample_150kB.pdf, Shortcut Name (ASCII): file-sample_150kB.lnk
- Registry Data:** The registry value is a REG_BINARY type. The data is a hex string: 00 00 00 00 FF FF FF FF. The hex dump shows the file path: file-sample_150kB.lnk.

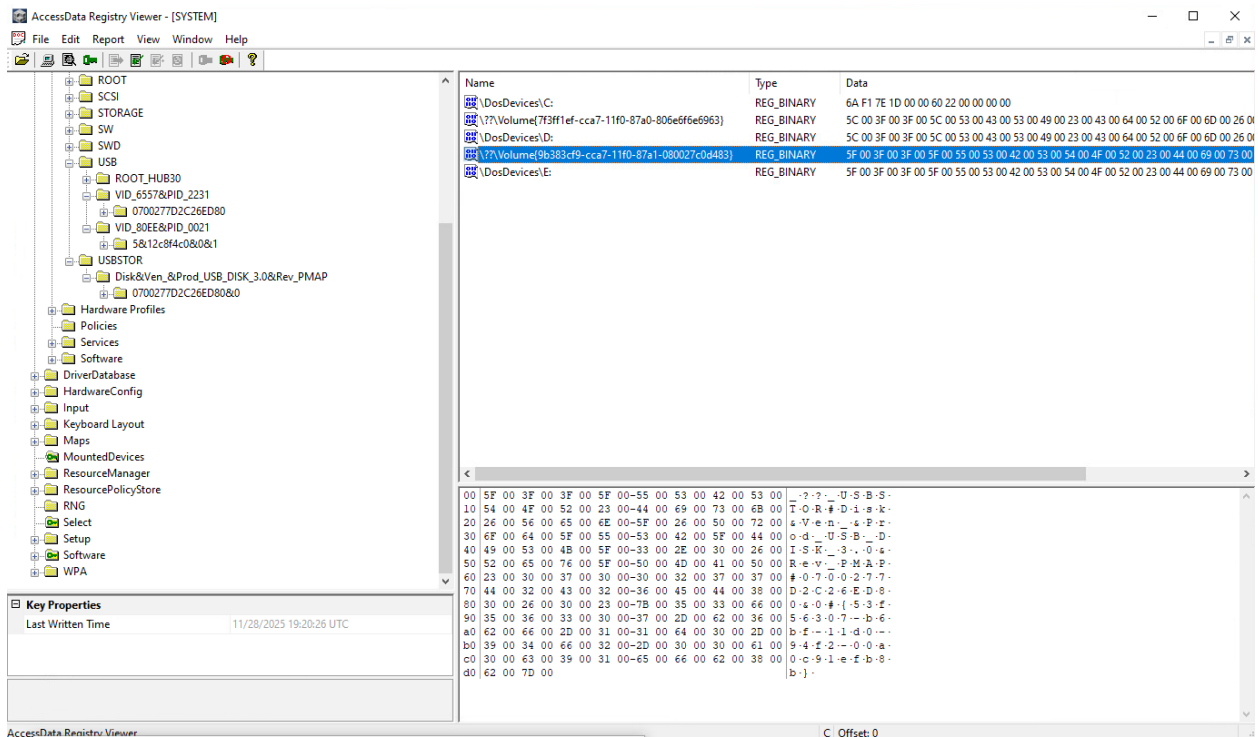


SYSTEM file evidence:

MountedDevices here we see Disk ID matching the id discovered in MREVIL NTUSER.DAT file.

9b383cf9-cca7-11f0-87a1-080027c0d483

This corroborates that the export drive was mounted at point E:\



ControlSet001 -> Enum -> USBSTOR -> contains further information about the USB drive.

AccessData Registry Viewer - [SYSTEM]

FileEditReportViewWindowHelp

SYSTEM

ActivationBroker

ControlSet001

Control

Enum

ACPI

ACPI_HAL

DISPLAY

HDAUDIO

HID

HTREE

PCI

ROOT

SCSI

STORAGE

SW

SWD

USB

ROOT_HUB30

VID_6557&PID_2231

0700277D2C26ED80

VID_80EE&PID_0021

5&12c8f4c0&0&1

USBSTOR

Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP

0700277D2C26ED80

Device Parameters

MediaChangeNotification

Partmgr

Properties

Hardware Profiles

Default

Key Properties

Last Written Time11/28/2025 19:20:26 UTC

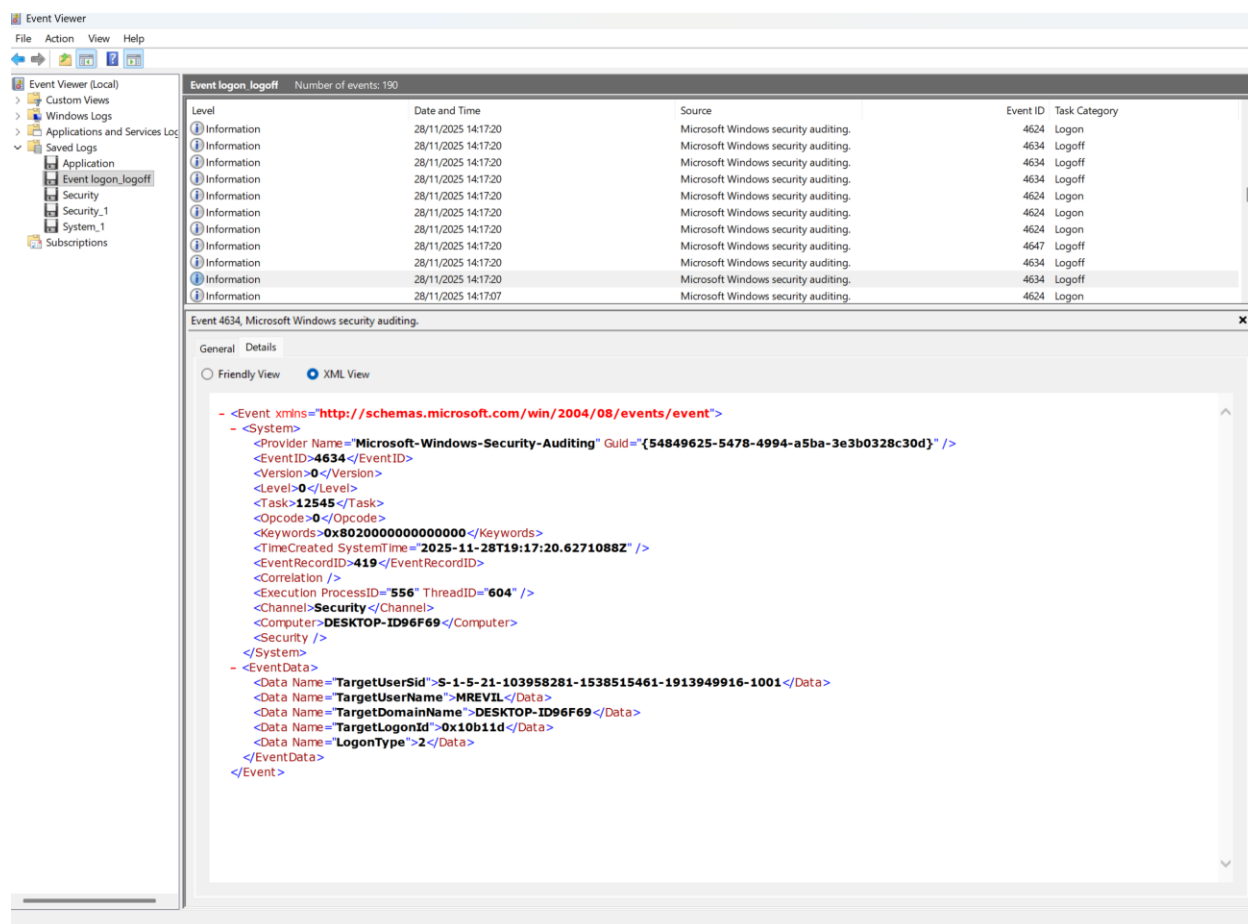
Name	Type	Data
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
Address	REG_DWORD	0x00000002 (2)
ContainerID	REG_SZ	(63bd2cf9-809e-5dfc-9acf-c17cc212dff1)
HardwareID	REG_MULT_SZ	USBSTOR\Disk____USB_DISK_3.0_PMAP USBSTOR\Disk____USB_DISK_3.0
CompatibleIDs	REG_MULT_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	REG_SZ	disk
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}.0001
Mfg	REG_SZ	@disk.inf,%genmanufacturer%(Standard disk drives)
FriendlyName	REG_SZ	USB DISK 3.0 USB Device
ConfigFlags	REG_DWORD	0x00000000 (0)

<

00 40 00 64 00 69 00 73 00-6B 00 2E 00 69 00 6E 00 08-d-i-s-k-.i-n-
10 66 00 2C 00 25 00 64 00-69 00 73 00 6B 00 5F 00 f-.k-d-i-s-k-_-
20 64 00 65 00 76 00 64 00-65 00 73 00 63 00 25 00 d-e-v-e-s-c-k-
30 3B 00 44 00 69 00 73 00-6B 00 20 00 64 00 72 00 ;-D-i-s-k--d-r-
40 69 00 76 00 65 00 00 00- |v-e-...
>

SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP\0700277D2C26ED80&0R Offset: 0

Forensic Findings from Windows Event Viewer



Security Event (Event ID 4634)

This screenshot shows a Security event (Event ID **4634**) recording an interactive logoff for the account **MREVIL** on computer **DESKTOP-ID96F69**. The XML details include the **TargetUserName = MREVIL**, the **TargetLogonId (0x10b11d)**, the **LogonType = 2** (interactive/local console), and an exact timestamp. This is relevant because it proves that the MREVIL account ended an interactive session at a precise time and provides a Logon ID that can be used to correlate other events (process creation, file access, USB activity) within the same session.

The screenshot shows the Windows Event Viewer interface. The left pane displays the 'System' log. The main pane shows a list of events, with Event ID 20001 selected. The details pane shows the XML data for this event.

Level	Date and Time	Source	Event ID	Task Category
Information	28/11/2025 14:27:48	Dhcp-Client	50105	Service State Event
Information	28/11/2025 14:27:48	Dhcp-Client	50104	Service State Event
Information	28/11/2025 14:27:48	Winlogon	7002	(1102)
Information	28/11/2025 14:27:47	User32	1074	None
Information	28/11/2025 14:27:48	EventLog	6006	None
Warning	28/11/2025 14:27:40	Disk	51	None
Information	28/11/2025 14:21:28	Service Control Manager	7040	None
Information	28/11/2025 14:20:26	UserPnp	20001	(7005)
Information	28/11/2025 14:20:26	UserPnp	20003	(7005)

Event 20001, UserPnp

General Details

☐ Friendly View ☒ XML View

```
<?xml version="1.0" encoding="UTF-16"?>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-UserPnp" Guid="{96f4a050-7e31-453c-88be-9634f4e02139}" />
    <EventID>20001</EventID>
    <Version>0</Version>
    <Level>4</Level>
    <Task>7005</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8000000000000000</Keywords>
    <TimeCreated SystemTime="2025-11-28T19:20:26.8394792Z" />
    <EventRecordID>206</EventRecordID>
    <Correlation />
    <Execution ProcessID="3636" ThreadID="1624" />
    <Channel>System</Channel>
    <Computer>DESKTOP-ID96F69</Computer>
    <Security UserID="S-1-5-18" />
  </System>
  <UserData>
    <InstallDeviceID xmlns="http://manifests.microsoft.com/win/2004/08/windows/userpnp">
      <DriverName>wpdfs.inf_amd64_86b72dac27e0ea83\wpdfs.inf</DriverName>
      <DriverVersion>10.0.16299.15</DriverVersion>
      <DriverProvider>Microsoft</DriverProvider>
      <DeviceInstanceID>SWD\WPDBUSENUM\??_USBSTOR#DISK&VEN_&PROD_USB_DISK_3.0&REV_PMAP#0700277D2C26ED80&0#{53F56307-B6BF-11D0-94F2-00A0C91EFB88}</DeviceInstanceID>
      <SetupClass>{eec5ad98-8080-425f-922a-dabf3de3f69a}</SetupClass>
      <RebootOption>false</RebootOption>
      <UpgradeDevice>false</UpgradeDevice>
      <IsDriverOEM>false</IsDriverOEM>
      <InstallStatus>0x0</InstallStatus>
      <DriverDescription>WPD FileSystem Volume Driver</DriverDescription>
    </InstallDeviceID>
  </UserData>
</Event>
```

System/UserPnp Event (Event ID 20001)

This screenshot captures a System UserPnp event (Event ID **20001**) showing the operating system recognized a removable storage device. The event's DeviceInstanceID contains USBSTOR and PROD_USB_DISK_3.0, indicating a USB mass-storage device was attached. The timestamp is shown in the XML. This is relevant because it documents the connection of an external USB storage device (vendor/product info and instance ID), which can be correlated to user activity and used to investigate files that may have been copied to/from the device.

The screenshot displays the Windows Event Viewer interface. On the left, the 'Event Viewer (Local)' tree shows 'System' logs. The main pane lists several events, with Event ID 20003, 'UserPnp', selected. Below this, the 'XML View' tab is active, showing the raw XML data for the event.

Level	Date and Time	Source	Event ID	Task Category
Information	28/11/2025 14:27:48	Dhcp-Client	50104	Service State Event
Information	28/11/2025 14:27:48	Winlogon	7002	(1102)
Information	28/11/2025 14:27:47	User32	1074	None
Information	28/11/2025 14:27:48	EventLog	6006	None
Warning	28/11/2025 14:27:40	Disk	51	None
Information	28/11/2025 14:21:28	Service Control Manager	7040	None
Information	28/11/2025 14:20:26	UserPnp	20001	(7005)
Information	28/11/2025 14:20:26	UserPnp	20003	(7005)
Information	28/11/2025 14:20:26	Service Control Manager	7045	None

```

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-UserPnp" Guid="{96f4a050-7e31-453c-88be-9634f4e02139}" />
  <EventID>20003</EventID>
  <Version>0</Version>
  <Level>4</Level>
  <Task>7005</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2025-11-28T19:20:26.6861522Z" />
  <EventRecordID>205</EventRecordID>
  <Correlation />
  <Execution ProcessID="3636" ThreadID="1624" />
  <Channel>System</Channel>
  <Computer>DESKTOP-ID96F69</Computer>
  <Security UserID="S-1-5-18" />
</System>
- <UserData>
- <AddServiceID xmlns="http://manifests.microsoft.com/win/2004/08/windows/userpnp">
  <ServiceName>WUDFWpdFs</ServiceName>
  <DriverFileName>SystemRoot\system32\DRIVERS\WUDFRd.sys</DriverFileName>
  <DeviceInstanceID>SWD\WPDBUSENUM\??_USBSTOR#DISK&VEN_&PROD_USB_DISK_3.0&REV_PMAP#0700277D2C26ED80&0#{53F56307-
    B6BF-11D0-94F2-00A0C91EFB8B}</DeviceInstanceID>
  <PrimaryService>true</PrimaryService>
  <UpdateService>false</UpdateService>
  <AddServiceStatus>0</AddServiceStatus>
</AddServiceID>
</UserData>
</Event>

```

System/UserPnp Event (Event ID 20003)

This screenshot shows a closely-timed System UserPnp event (Event ID **20003**) that records the WPD/WDF driver (WUDFRd.sys / WPD FileSystem Volume Driver) being started or associated with the same device instance. The XML lists driver and device identifiers and the same approximate timestamp as the other PnP event. This is relevant because it corroborates the USB device installation sequence (driver initialization and device enumeration) and strengthens the evidence that a removable storage device was mounted and became accessible to the OS at that time.