

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.

The screenshot shows the AccessData Registry Viewer interface with the title bar "AccessData Registry Viewer - [NTUSER.DAT]". The left pane displays a tree view of registry keys under "Software\Microsoft\Internet Explorer". One key, "TypedURLs", is expanded, showing subkeys like "Type", "Time", "SearchHooks", "User Preferences", and "VersionManager". The right pane shows a table of seven entries (url1 to url7) with columns "Name", "Type", and "Data". Each entry corresponds to a URL. Below the table is a hex dump of the registry data. The bottom left pane shows "Key Properties" with "Last Written Time" set to "11/28/2025 19:46:30 UTC".

Name	Type	Data
url1	REG_SZ	https://www.file-examples.com/wp-content/storage/2017/10/file_example_PNG_500kB.png
url2	REG_SZ	https://file-examples.com/wp-content/storage/2017/10/file_example_JPG_1MB.jpg
url3	REG_SZ	https://www.file-examples.com/wp-content/storage/2017/10/file-example_JPG_1MB.jpg
url4	REG_SZ	https://www.file-examples.com/wp-content/storage/2017/10/file-sample_150kB.pdf
url5	REG_SZ	https://mrevilrepository.com/
url6	REG_SZ	https://www.tryhekme.com/
url7	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

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
- CLISave
- CLSID
- ComDlg32
- Desktop
- Discardable
- FileExts
- HideDesktopIcons
- LogonStats
- LowRegistry
- MenuOrder
- Modules
- MountPoints2
 - (1d7ef16a-0000-0000-0000-602200000000)
 - (73ff1ef-cc47-11f0-87a0-806effe6963)
 - (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

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

Offset: 0

Hex Dump:

Offset	Value	Hex	ASCII
00	22	22	00 45 00 3A 00 5C 00-61 00 75 00 74 00 6F 00
10	72	72	00 75 00 E8 00 2E 00-69 00 E8 00 22 00
20	20	20	00 00 00 00

Binary Dump:

..E.:..\autorun.
run...1.co..

AccessData Registry Viewer - [NTUSER.DAT]

File Edit Report View Window Help

Explorer

- Accent
- Advanced
- AppContract
- AutoplayHandlers
- BamThrottling
- BannerStore
- BitBucket
- CabinetState
- CD Burning
- CLISave
- CLSID
- ComDlg32
- Desktop
- Discardable
- FileExts
- HideDesktopIcons
- LogonStats
- LowRegistry
- MenuOrder
- Modules
- MountPoints2
 - (1d7ef16a-0000-0000-0000-602200000000)
 - (73ff1ef-cc47-11f0-87a0-806effe6963)
 - (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

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

Offset: 0

Hex Dump:

Offset	Value	Hex	ASCII
0	44	44	D-E-T-S...

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

The screenshot shows two instances of the AccessData Registry Viewer interface. Both windows are titled "AccessData Registry Viewer - [NTUSER.DAT]" and are displaying the "RecentDocs" key under the "Windows\CurrentVersion\Explorer" path.

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.Ink

Data View:

The data view shows a table with columns: Name, Type, and Data. One entry is visible:

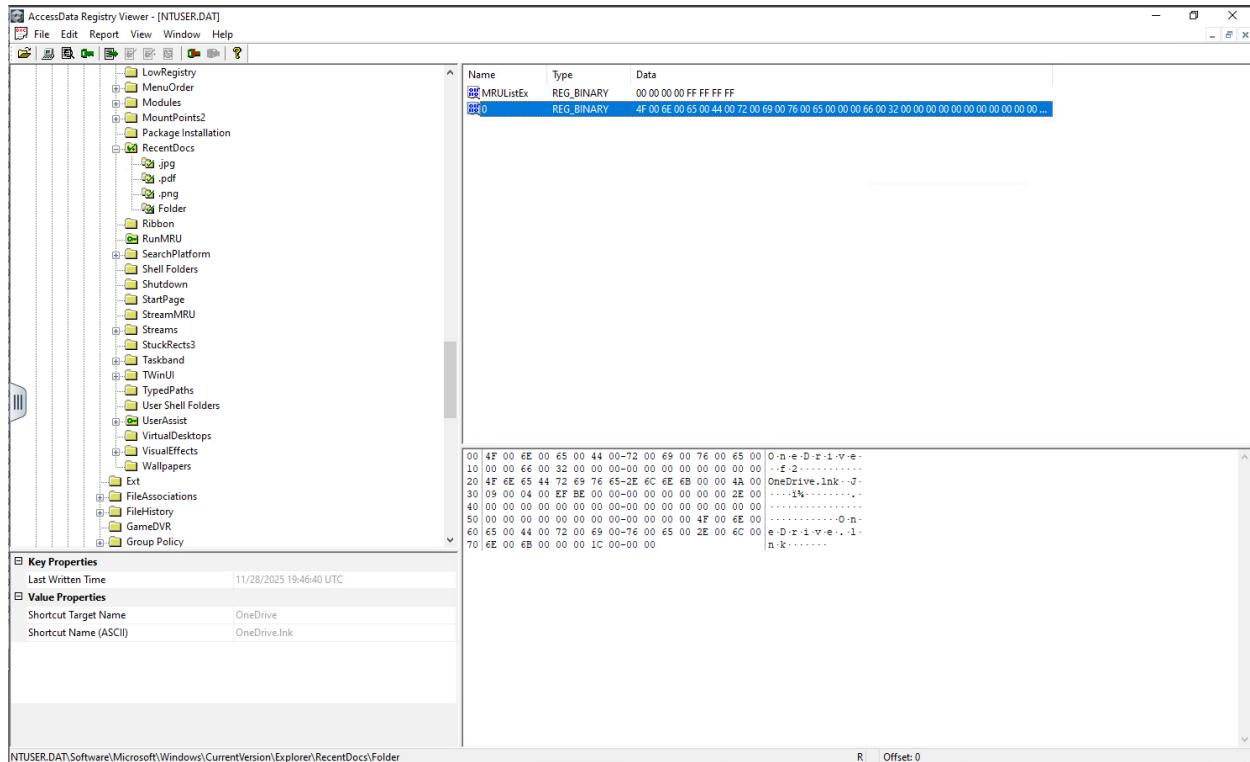
Name	Type	Data
MRUListEx	REG_BINARY	00 00 00 FF FF FF 00 60 69 00 6C 00 65 00 2D 00 73 00 61 00 6D 00 70 00 6C 00 65 00 5F 00 31 00 35 00 6B 00 ...

Hex View:

The hex view displays the binary data corresponding to the MRUListEx entry. The data starts with 00 60 69 00 6C 00 65 00 2D 00 73 00 61 00 6D 00 70 00 6C 00 65 00 5F 00 31 00 35 00 6B 00 ... and continues with various file signatures like ".JPG", ".PDF", and ".INK".

Bottom Window:

This window shows the same registry key structure and properties as the top one. The data view shows the same MRUListEx entry with the same hex dump. The hex view shows the same binary data starting with 00 60 69 00 6C 00 65 00 2D 00 73 00 61 00 6D 00 70 00 6C 00 65 00 5F 00 31 00 35 00 6B 00 ... and containing file signatures.



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:\

AccessData Registry Viewer - [SYSTEM]

File Edit Report View Window Help

File Edit View Insert Options Tools Help

ROOT

SCSI

STORAGE

SW

SWD

USB

 ROOT_HUB30

 VID_6557&PID_2231

 0700277D2C26ED80

 VID_80E6&PID_0021

 5&12c94c080&1

USBSTOR

 Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP

 0700277D2C26ED80&0

Hardware Profiles

 Policies

 Services

 Software

DriverDatabase

HardwareConfig

Input

Keyboard Layout

Maps

MountedDevices

ResourceManager

ResourcePolicyStore

RNG

Select

Setup

Software

WPA

Key Properties

Last Written Time: 11/28/2025 19:20:26 UTC

Name

Type

Data

00|5F 00 3F 00 3F 00 5F 00-55 00 53 00 42 00 53 00| -?-.-U-S-B-S-

10|54 00 4F 00 52 00 23 00-44 00 69 00 73 00 6B 00| T-O-R-#-D-i-s-k-

20|26 00 56 00 65 00 6E 00-5F 00 26 00 50 00 72 00| & V-e-n-.-s P-r-

30|6F 00 64 00 5F 00 55 00-53 00 42 00 5F 00 44 00| o-d-.-U-S-B-.-D-

40|49 00 53 00 4B 00 5F 00-33 00 2E 00 30 00 26 00| I-S-K-.-3-.-0-4-

50|52 00 65 00 76 00 5F 00-50 00 4D 00 41 00 50 00| R-e-v-.-P-H-A-P-

60|23 00 30 00 37 00 30 00-30 00 32 00 37 00 37 00| #-0-7-0-0-2-7-7-

70|44 00 32 00 43 00 32 00-36 00 45 00 44 00 38 00| D-2-C-2-6-E-D-8-

80|30 00 26 00 30 00 23 00-7B 00 35 00 33 00 60 00| 0-&-0-#-(5-3-f-

90|30 00 36 00 33 00 30 00-37 00 2D 00 62 00 38 00| 5-6-3-0-7-.-b-6-

a0|62 00 66 00 2D 00 31 00-31 00 64 00 30 00 2D 00| b-f-.-1-1-d-0-.-

b0|39 00 34 00 66 00 32 00-2D 00 30 00 30 00 61 00| 9-4-f-2-.-0-0-a-

c0|30 00 63 00 39 00 31 00-65 00 66 00 62 00 38 00| 0-c-9-1-e-f-b-8-

d0|62 00 7D 00| b- .

C Offset: 0

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

AccessData Registry Viewer - [SYSTEM]

File Edit Report View Window Help

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_80E8&PID_0021
 - 5&1c2cf4c:0&0:81
 - USBSTOR
 - Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP
 - 0700277D2C26ED80&0
 - Device Parameters
 - MediaChangeNotification
 - Partmgr
 - Properties
 - Hardware Profiles
 - Driver

Key Properties

Last Written Time: 11/28/2025 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_MULTI_SZ	USBSTOR\Disk_____USB_DISK_3.0____PMAP USBSTOR\Disk_____USB_DISK_3.0_____
CompatibleIDs	REG_MULTI_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\%genmanufacure%\{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 @-d-i-s-k-.-i-n-
 10 66 00 2C 00 25 00 64 00-69 00 73 00 6B 00 5F 00 f-, %d-i-s-k-_-
 20 64 00 65 00 76 00 64 00-65 00 73 00 63 00 25 00 d-e-v-d-e-s-o-
 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- i-v-e-..

R | Offset: 0

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

Forensic Findings from Windows Event Viewer

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists 'Event Viewer (Local)', 'File', 'Action', 'View', and 'Help'. Under 'Saved Logs', there is a folder named 'Event logon_logoff' containing 190 events. The main pane displays a table of events with columns: Level, Date and Time, Source, Event ID, and Task Category. Most events are 'Information' level, occurring at 28/11/2025 14:17:20, with Source 'Microsoft Windows security auditing.' and Task Category 'Logoff'. One event is highlighted in yellow, labeled 'Event 4634, Microsoft Windows security auditing.' with a timestamp of 28/11/2025 14:17:20. Below this, the XML View tab is selected, showing the detailed XML structure of the event.

Level	Date and Time	Source	Event ID	Task Category
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4624	Logon
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4634	Logoff
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4634	Logoff
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4634	Logoff
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4624	Logon
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4624	Logon
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4624	Logon
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4647	Logoff
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4634	Logoff
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4634	Logoff
Information	28/11/2025 14:17:20	Microsoft Windows security auditing.	4624	Logon

Event 4634, Microsoft Windows security auditing.

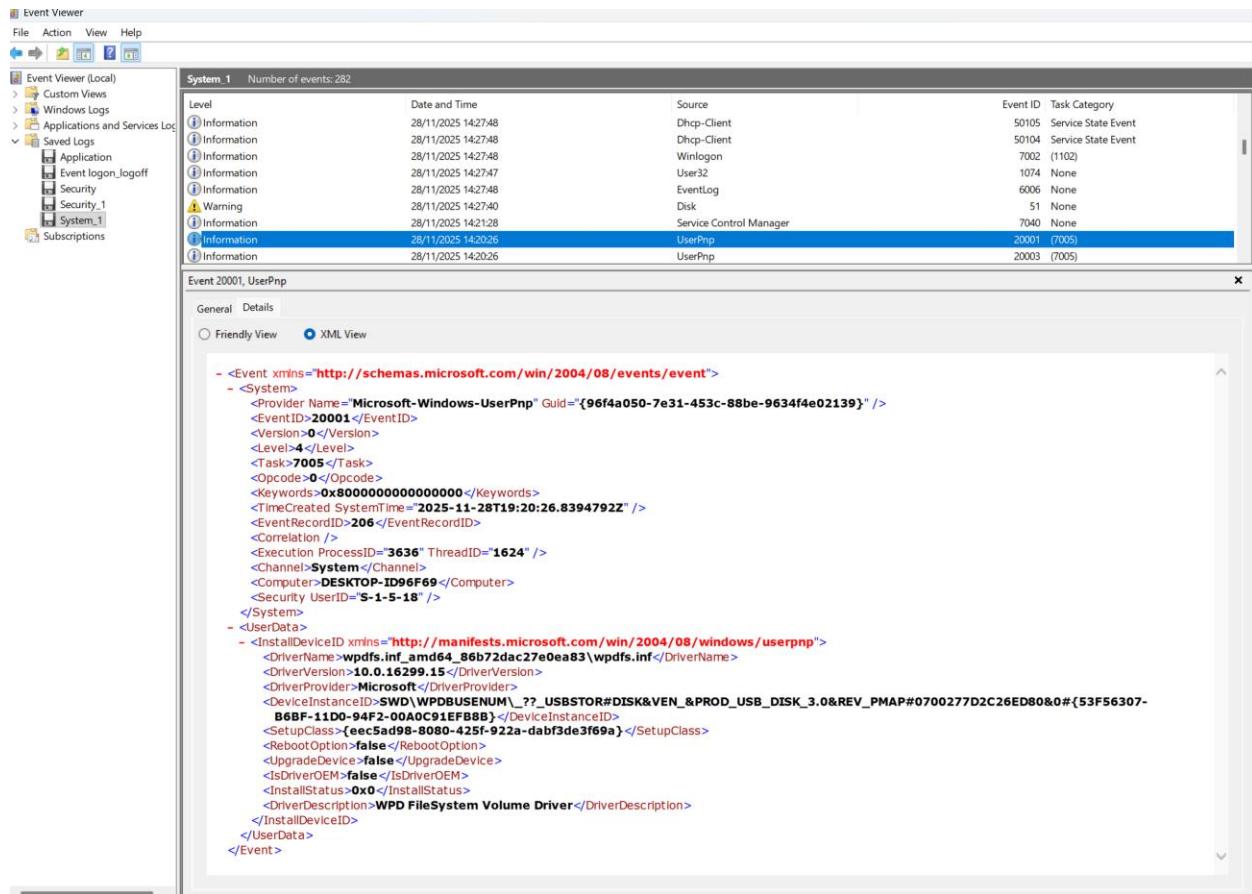
General Details

Friendly View XML View

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />
    <EventID>4634</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>12545</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2025-11-28T19:17:20.6271088Z" />
    <EventRecordID>419</EventRecordID>
    <Correlation />
    <Execution ProcessID="556" ThreadID="604" />
    <Channel>Security</Channel>
    <Computer>DESKTOP-ID96F69</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="TargetUserSid">S-1-5-21-103958281-1538515461-1913949916-1001</Data>
    <Data Name="TargetUserName">MREVIL</Data>
    <Data Name="TargetDomainName">DESKTOP-ID96F69</Data>
    <Data Name="TargetLogonId">0x10b11d</Data>
    <Data Name="LogonType">2</Data>
  </EventData>
</Event>
```

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.



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 shows the Windows Event Viewer interface. On the left, the navigation pane lists categories like Event Viewer (Local), Windows Logs, Applications and Services Logs, and Saved Logs. The Applications and Services Logs section is expanded, showing sub-categories Application, Event logon_logeoff, Security, Security_1, and System.1. The System.1 category is selected, displaying 282 events. A specific event, Event 20003, is selected and expanded. The event details show it was generated by UserPnp at 2025-11-28T19:20:26.6861522Z. The XML view shows the event structure:

```

<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#{5F56307-86BF-11D0-94F2-00A0C91EFBBB}</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.