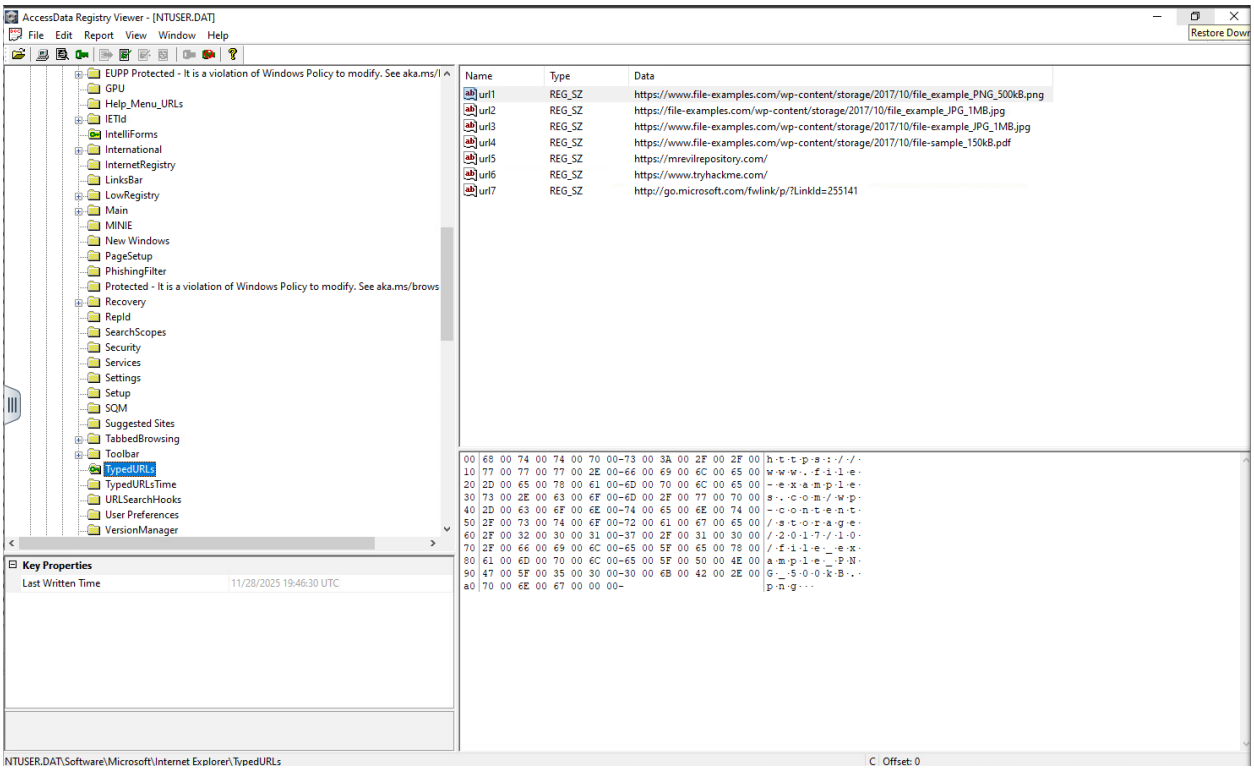
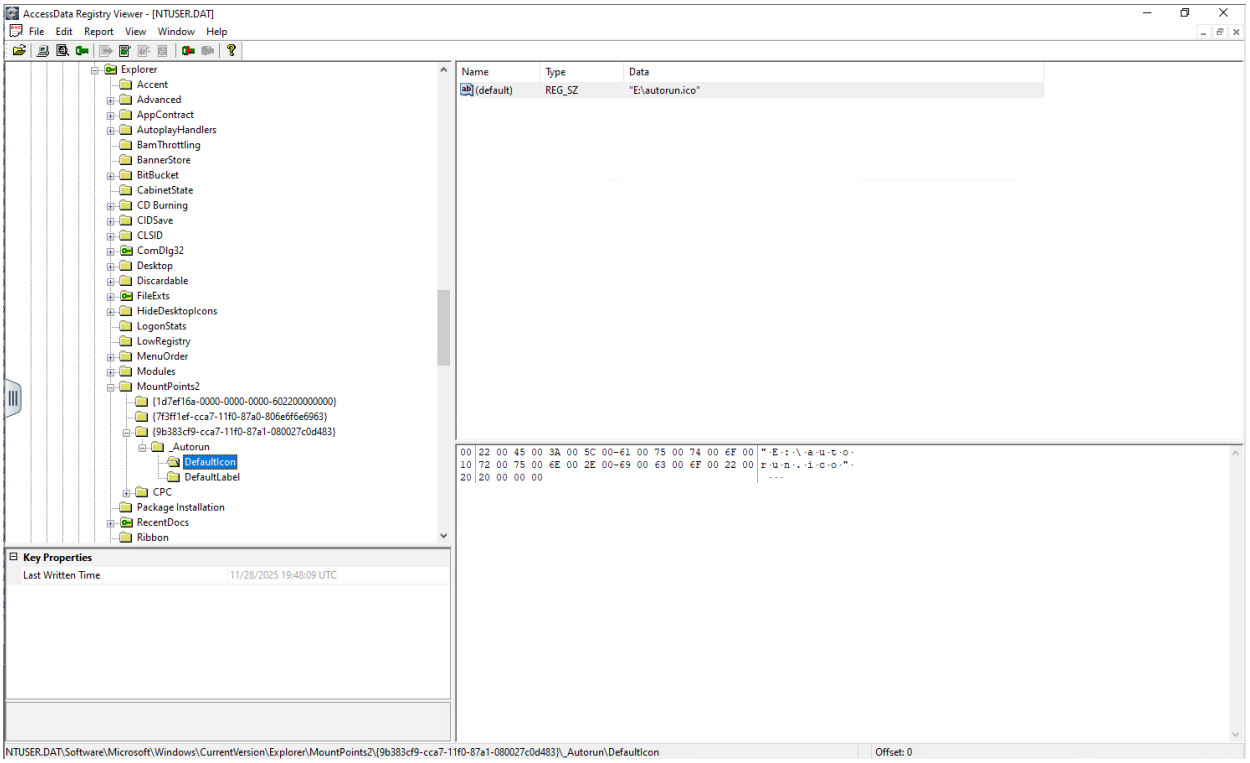
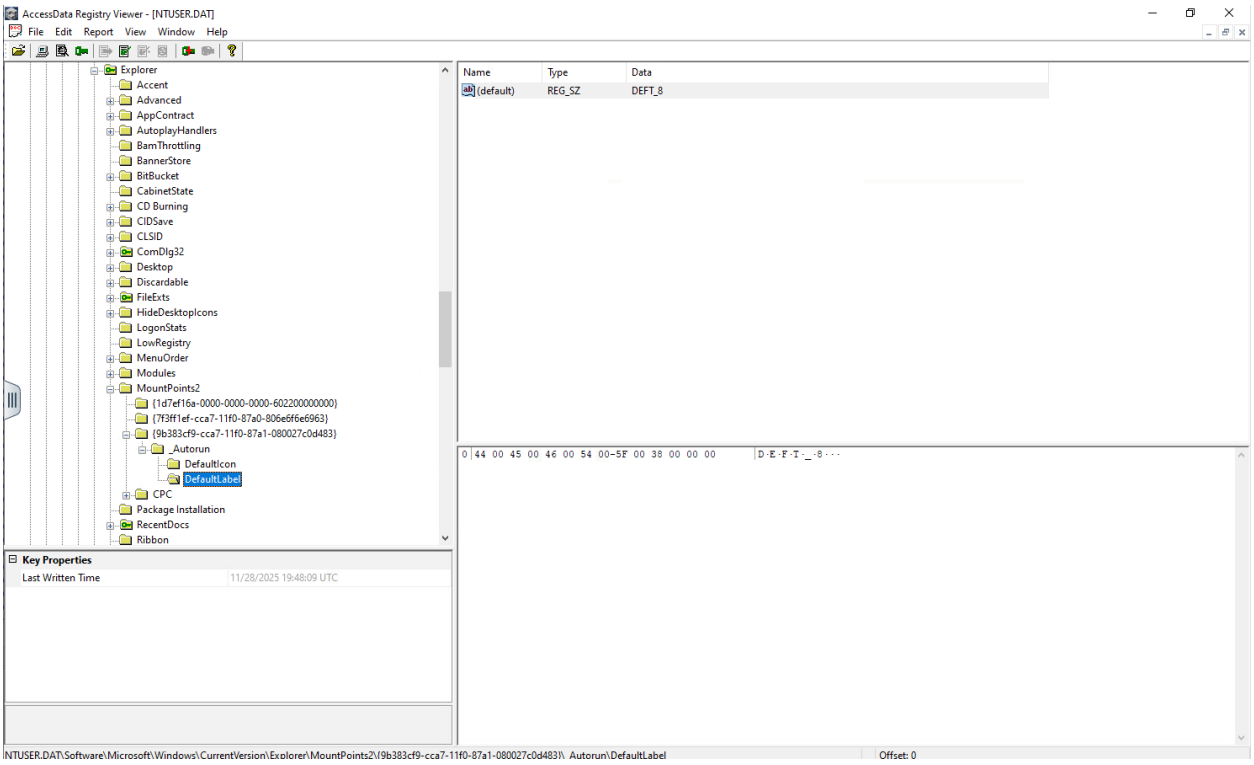
MREVIL NTUSER.DAT file evidence:

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.

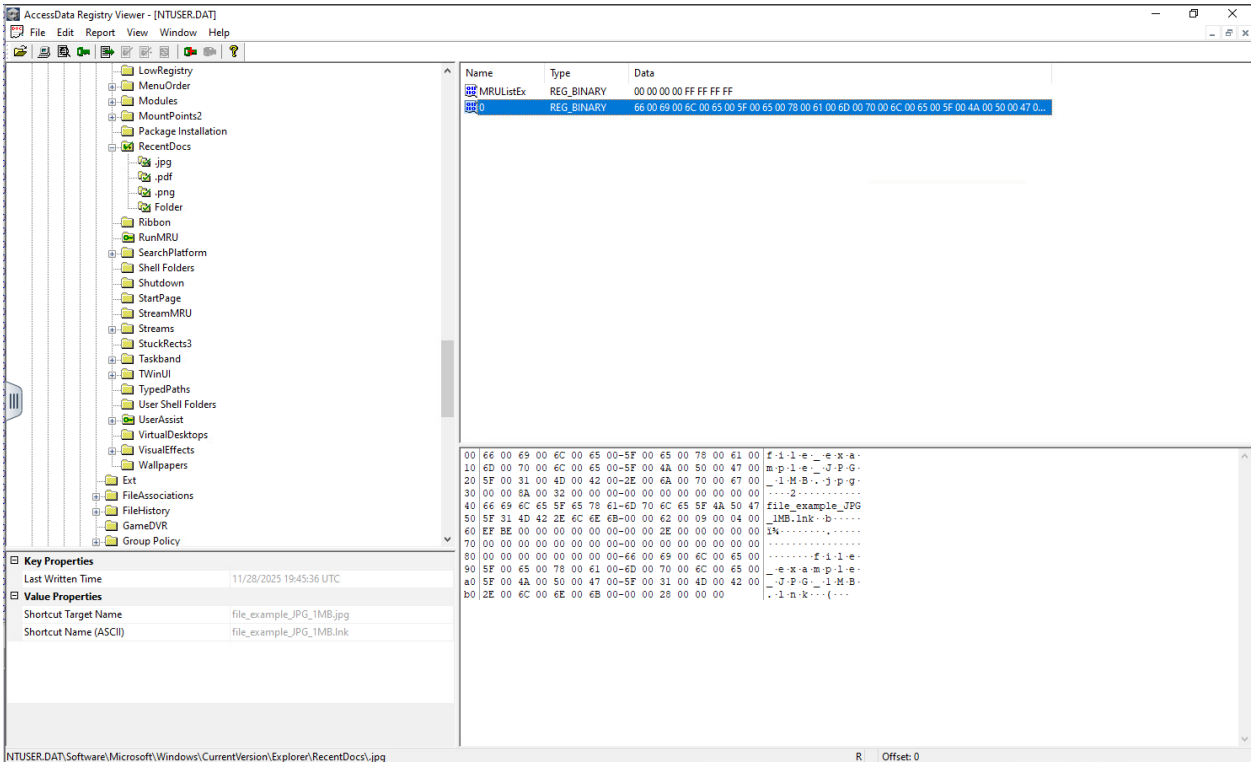


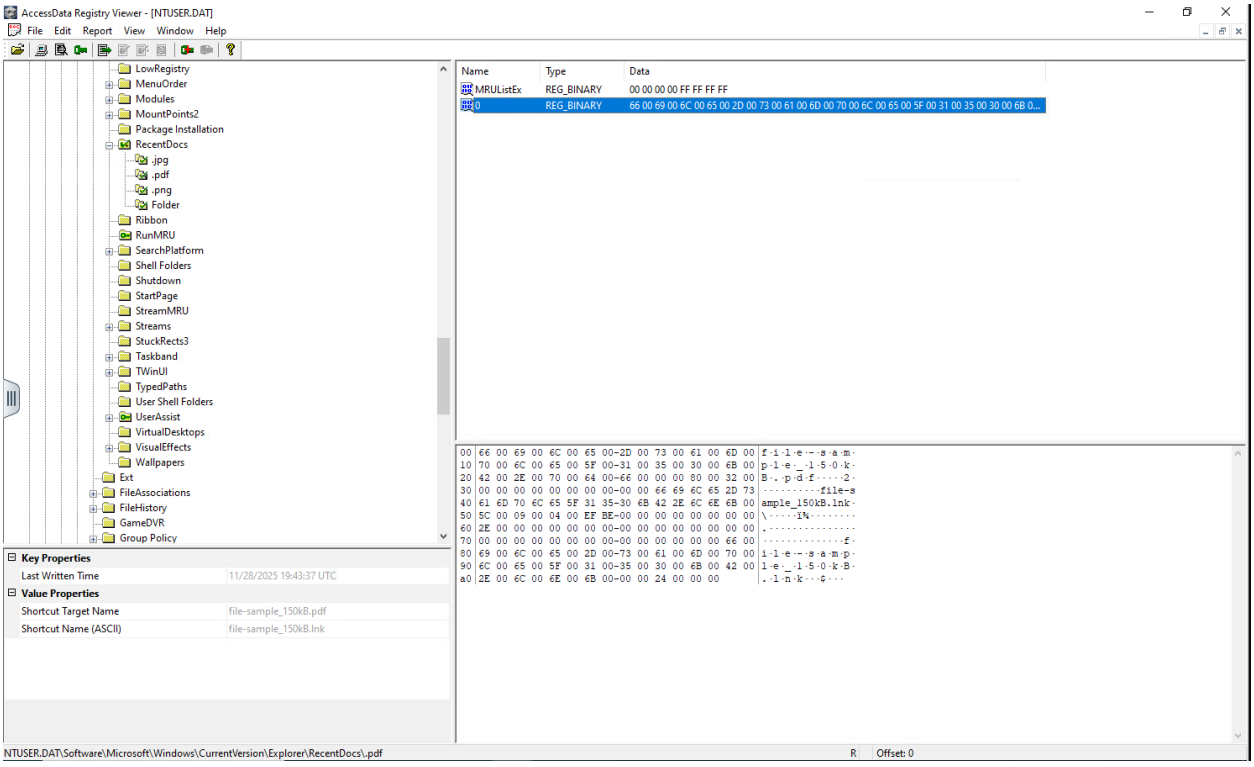
Located at: Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> MountPoints2 -> {9b383cf9-cca7-11f0-87a1-080027c0d483} -> _Autorun -> DefaultIcon / DefaultLabel contains information about mounted devices used by the user associated with the examined NTUSER.DAT file. The DefaultIcon file contains the mount pint 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.

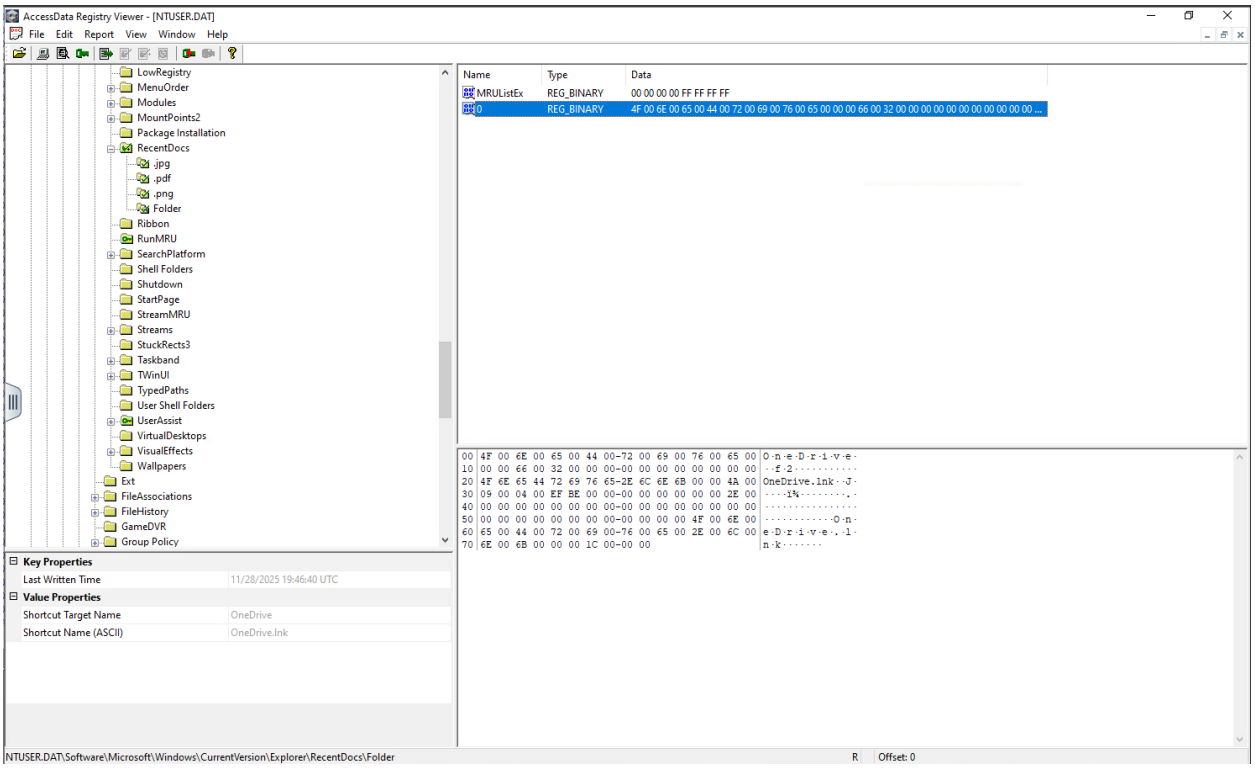

AccessData Registry Viewer - [NTUSER.DAT]
File Edit Report View Window Help
Explorer
Accent
Advanced
AppContract
AutoplayHandlers
BamThrottling
BannerStore
BitBucket
CabinetState
CD Burning
CIDSave
CLSID
ComDlg32
Desktop
Discardable
FileExts
HideDesktopIcons
LogonStats
LowRegistry
MenuOrder
Modules
MountPoints2
{1d7ef16a-0000-0000-0000-602200000000}
{7f3ff1ef-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
10 72 00 75 00 6E 00 2E 00-69 00 63 00 6F 00 22 00
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}
{7f3ff1ef-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
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 MREVIL. This evidence likely suggests that the files were downloaded to MREVIL Onedrive folder, and then transferred to the export drive.





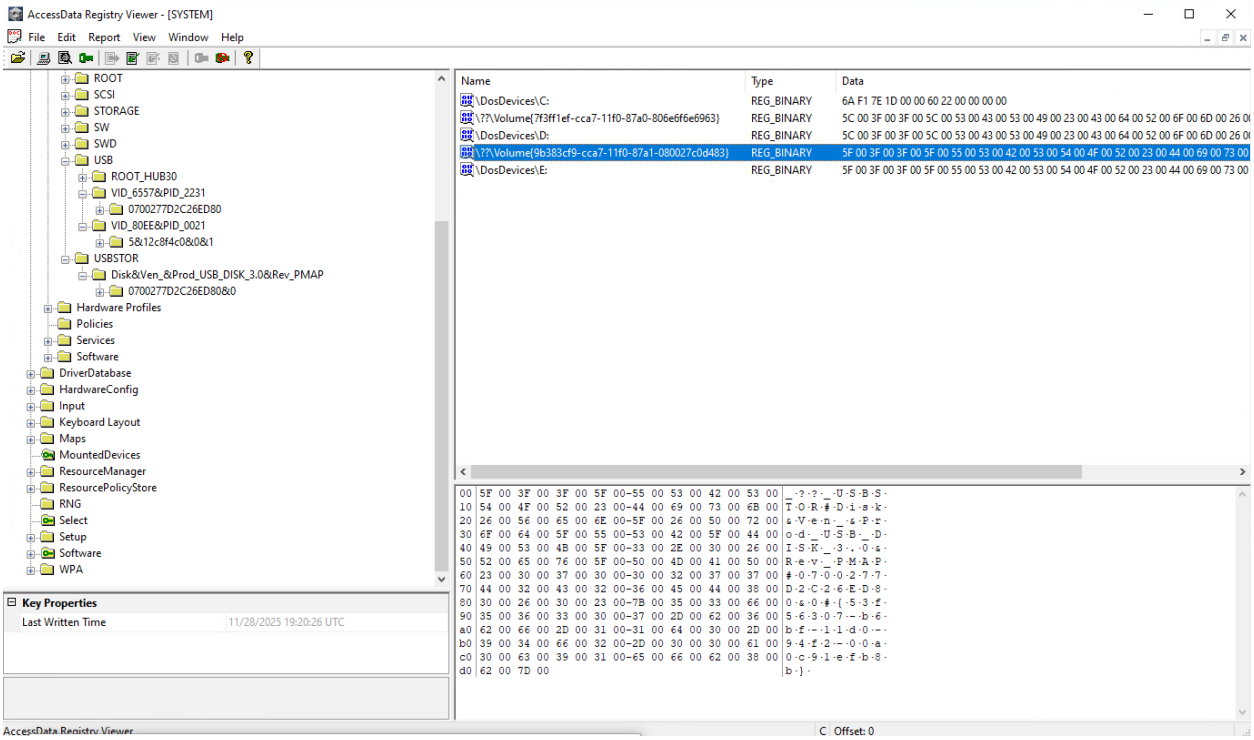

AccessData Registry Viewer - [NTUSER.DAT]
File Edit Report View Window Help
LowRegistry
MenuOrder
Modules
MountPoints2
Package Installation
RecentDocs
.jpg
.pdf
.png
Folder
Ribbon
RunMRU
SearchPlatform
Shell Folders
Shutdown
StartPage
StreamMRU
Streams
StuckRects3
Taskband
TWinUI
TypedPaths
User Shell Folders
UserAssist
VirtualDesktops
VisualEffects
Wallpapers
Ext
FileAssociations
FileHistory
GameDVR
Group Policy
Name Type Data
MRUListEx REG_BINARY 00 00 00 00 FF FF FF FF
0 REG_BINARY 4F 00 6E 00 65 00 44 00 72 00 69 00 76 00 65 00 00 00 66 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
00 4F 00 6E 00 65 00 44 00-72 00 69 00 76 00 65 00 O·n·e·D·r·i·v·e·
10 00 00 66 00 32 00 00 00-00 00 00 00 00 00 00 00 ··f·2···········
20 4F 6E 65 44 72 69 76 65-2E 6C 6E 6B 00 00 4A 00 OneDrive.lnk··J·
30 09 00 04 00 EF BE 00 00-00 00 00 00 00 00 2E 00 ····ï¾·····.·
40 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····************
50 00 00 00 00 00 00 00 00-00 00 00 00 4F 00 6E 00 ···········O·n·
60 65 00 44 00 72 00 69 00-76 00 65 00 2E 00 6C 00 e·D·r·i·v·e·.·l·
70 6E 00 6B 00 00 00 1C 00-00 00 n·k·····
Key Properties
Last Written Time 11/28/2025 19:46:40 UTC
Value Properties
Shortcut Target Name OneDrive
Shortcut Name (ASCII) OneDrive.lnk
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
R
Offset: 0

SYSTEM file evidence:

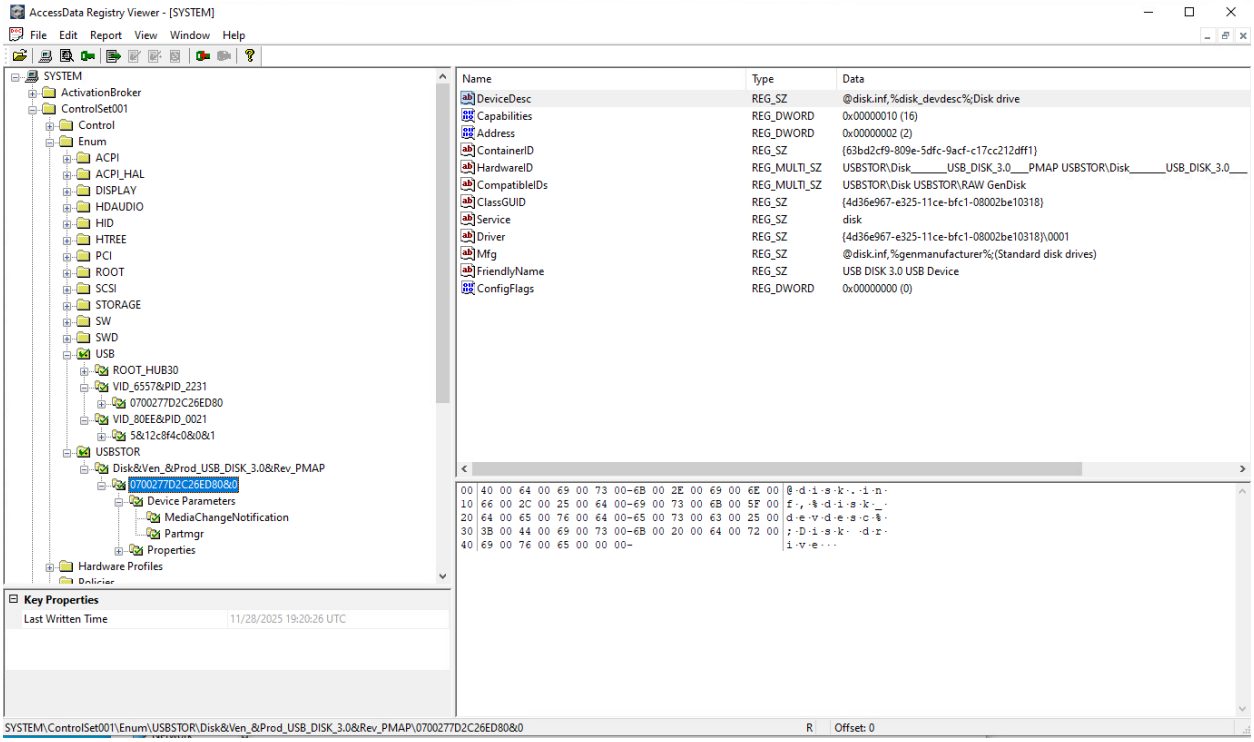
MountedDevices here we see Disk ID matching the id discovered in MREVIL NTUSER.DAT file.

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

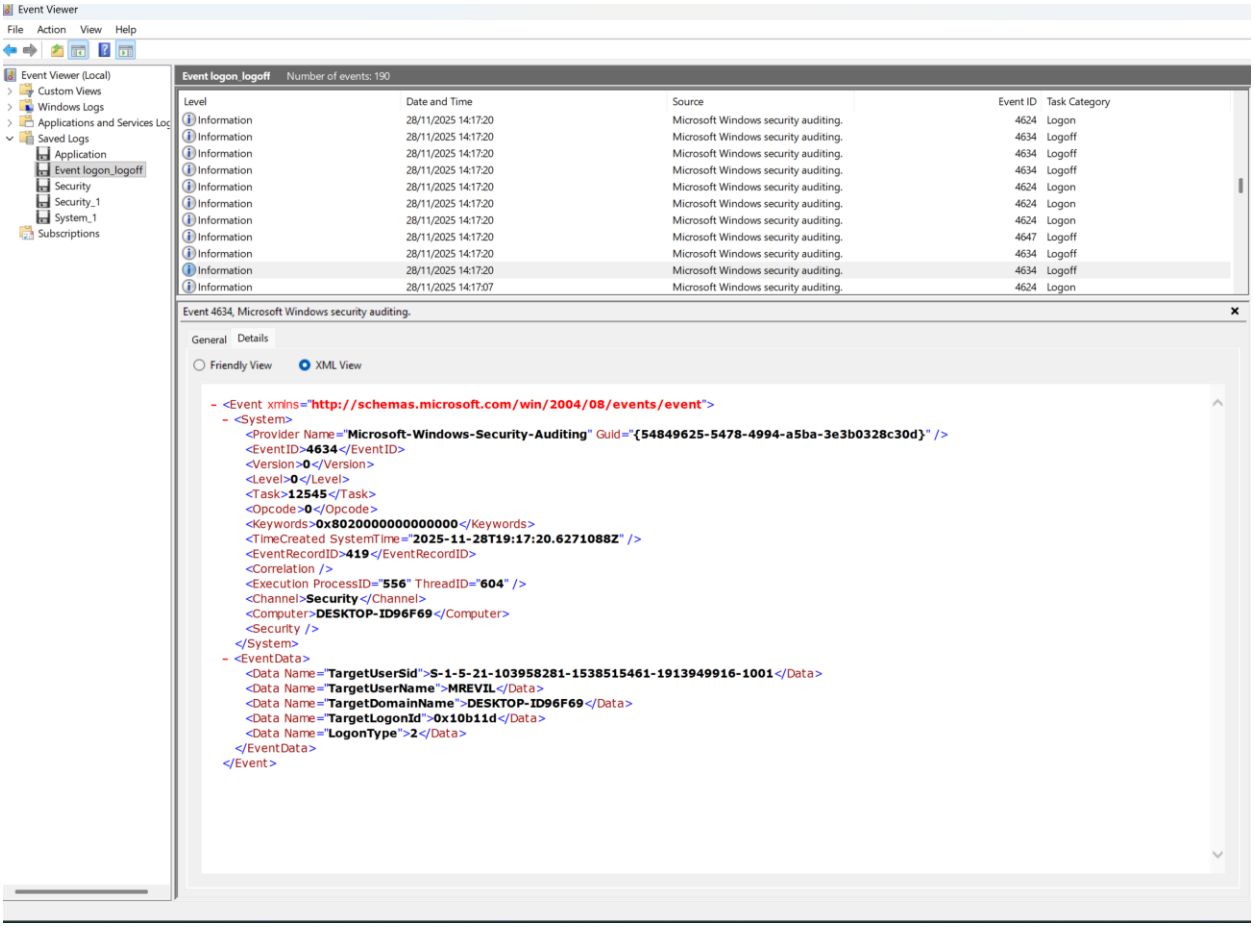
This corroborates that the export drive was mounted at point E:\



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

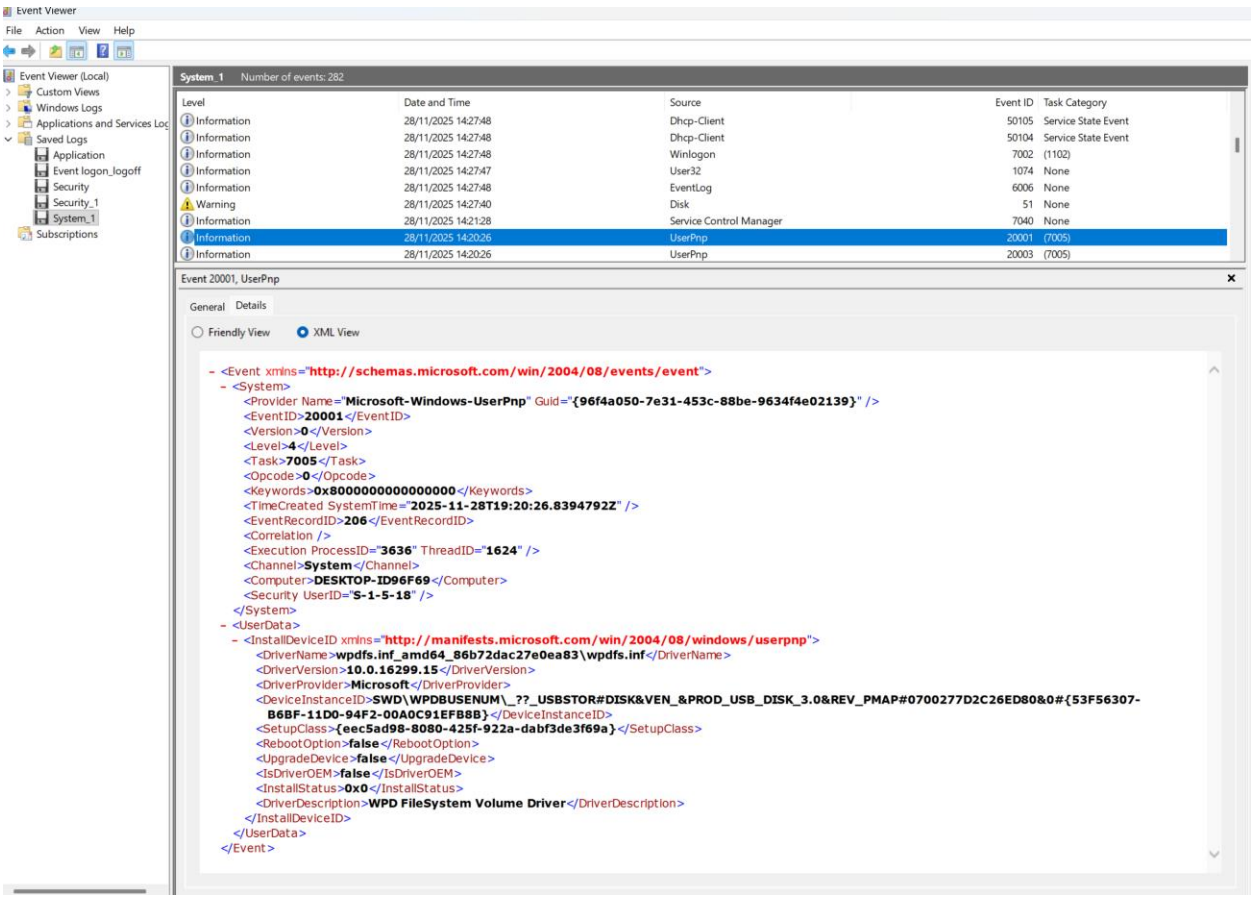

AccessData Registry Viewer - [SYSTEM]
File Edit Report View Window Help
SYSTEM
ActivationBroker
ControlSet001
Control
Enum
ACPI
ACPI_HAL
DISPLAY
HDAUDIO
HID
HTREE
PCI
ROOT
SCSI
STORAGE
SW
SWD
USB
ROOT_HUB30
VID_6557&PID_2231
0700277D2C26ED80
VID_80EE&PID_0021
5&12c8f4c0&0&1
USBSTOR
Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP
0700277D2C26ED80&0
Device Parameters
MediaChangeNotification
Partmgr
Properties
Hardware Profiles
Policies
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,%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 @·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·c·%·
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···
SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP\0700277D2C26ED80&0
R
Offset: 0

Forensic Findings from Windows Event Viewer



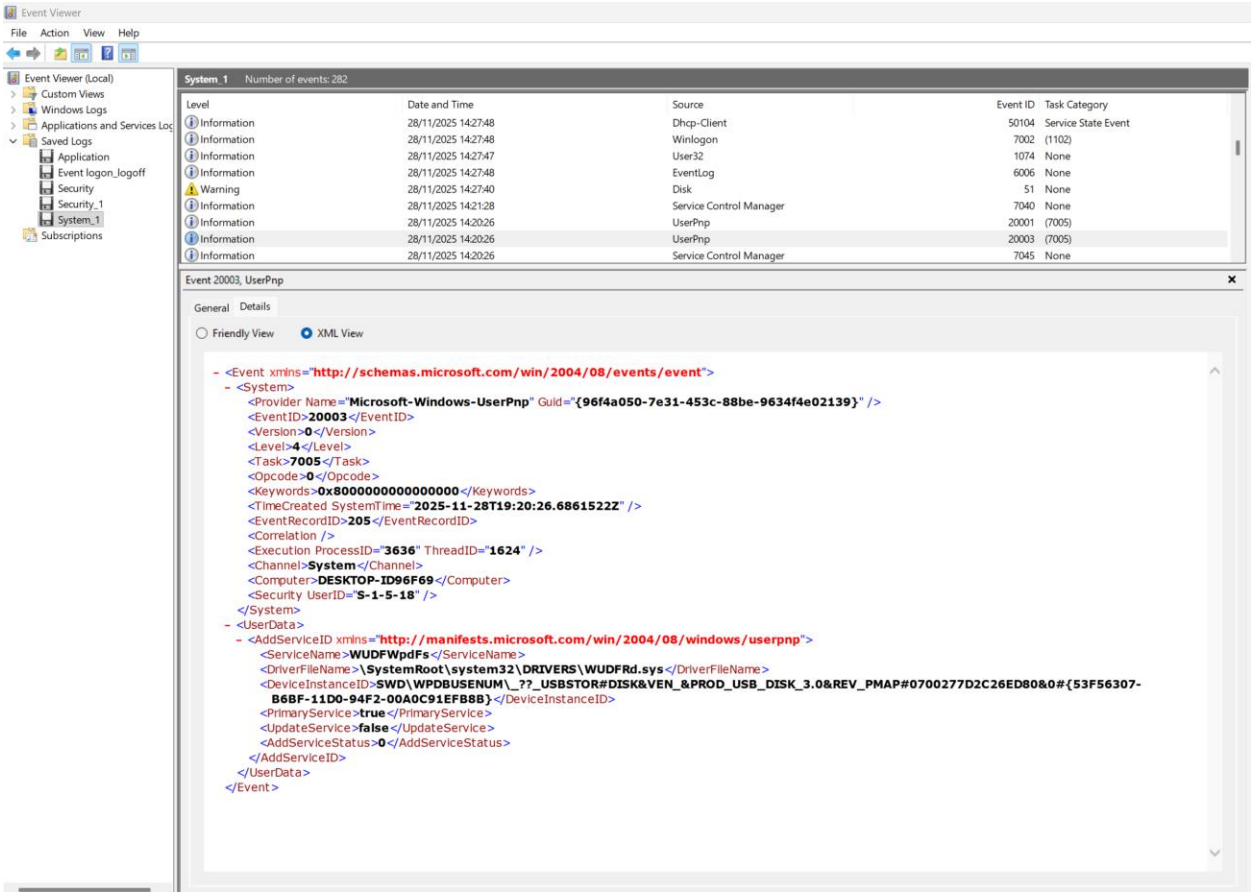
Security Event (Event ID 4634)

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.



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.



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.