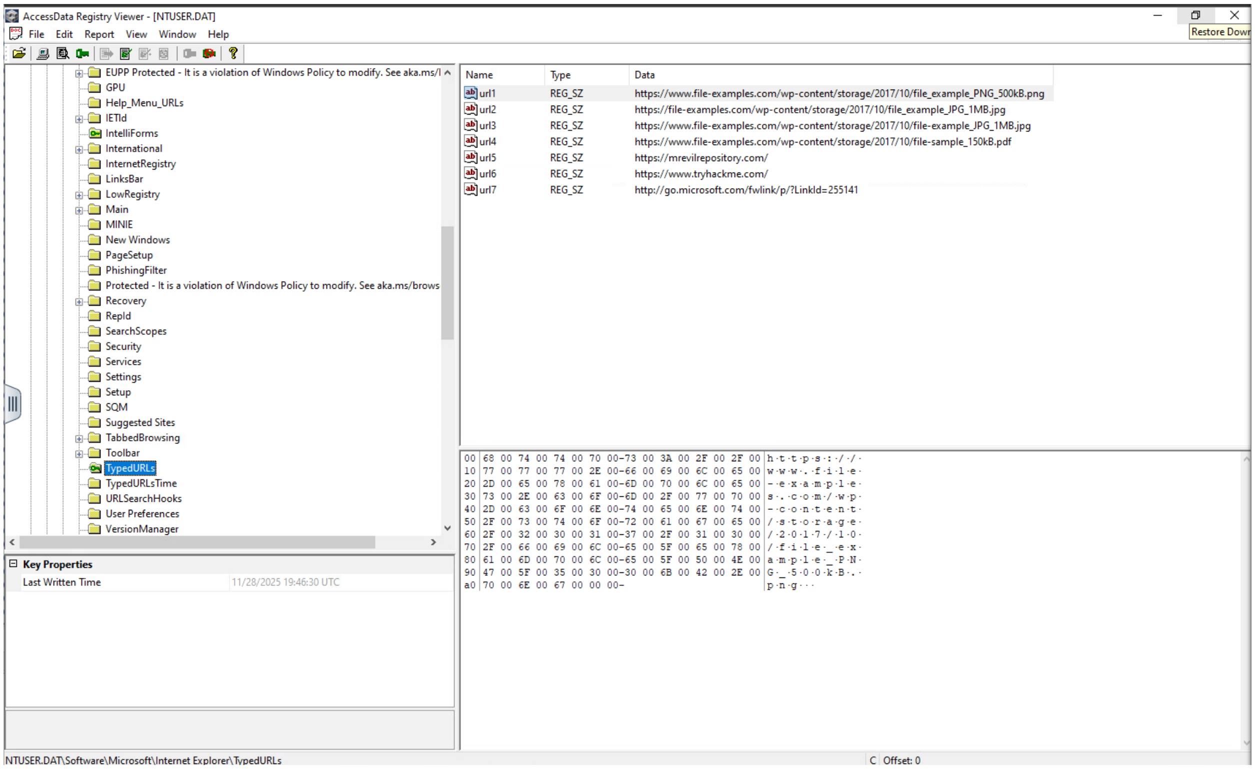
MREVIL NTUSER.DAT file evidence:

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.



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.tryhackme.com/
url7	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

```
00 68 00 74 00 74 00 70 00-73 00 3A 00 2F 00 2F 00 h·t·t·p·s·:·/·/·
10 77 00 77 00 77 00 2E 00-66 00 69 00 6C 00 65 00 w·w·w·.·f·i·l·e·
20 2D 00 65 00 78 00 61 00-6D 00 70 00 6C 00 65 00 -·e·x·a·m·p·l·e·
30 73 00 2E 00 63 00 6F 00-6D 00 2F 00 77 00 70 00 s·.·c·o·m·/·w·p·
40 2D 00 63 00 6F 00 6E 00-74 00 65 00 6E 00 74 00 -·c·o·n·t·e·n·t·
50 2F 00 73 00 74 00 6F 00-72 00 61 00 67 00 65 00 /·s·t·o·r·a·g·e·
60 2F 00 32 00 30 00 31 00-37 00 2F 00 31 00 30 00 /·2·0·1·7·/·1·0·
70 2F 00 66 00 69 00 6C 00-65 00 5F 00 65 00 78 00 /·f·i·l·e·_·e·x·
80 61 00 6D 00 70 00 6C 00-65 00 5F 00 50 00 4E 00 a·m·p·l·e·_·P·N·
90 47 00 5F 00 35 00 30 00-30 00 6B 00 42 00 2E 00 G·_·5·0·0·k·B·.·
a0 70 00 6E 00 67 00 00 00-                         p·n·g···
```

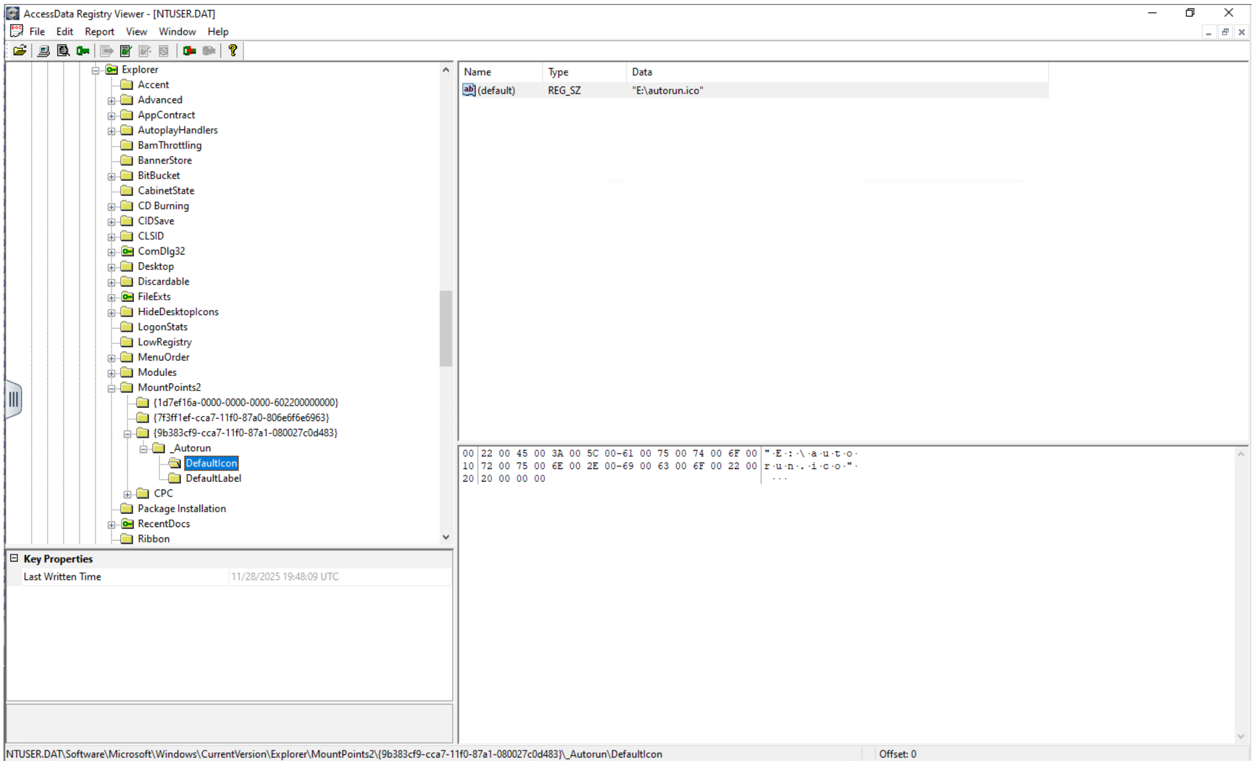
Key Properties

Last Written Time	11/28/2025 19:46:30 UTC

NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs

C Offset: 0

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.



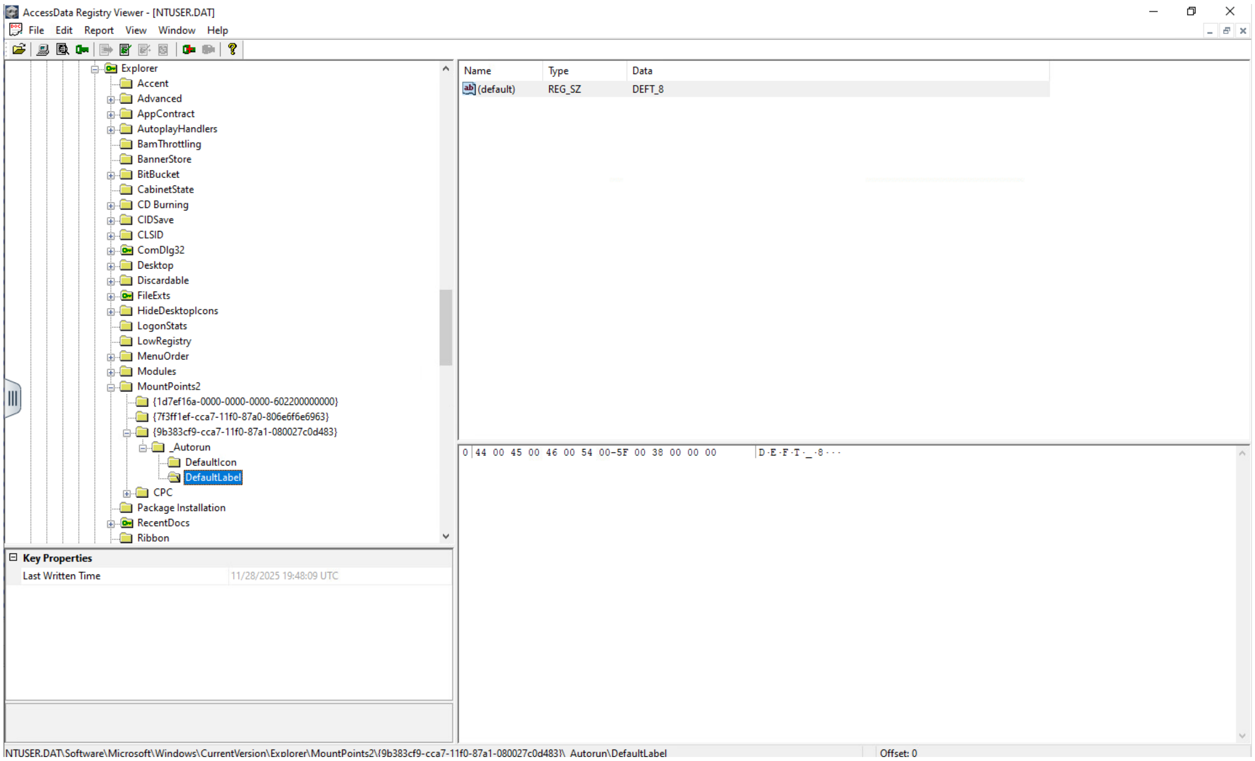
Name	Type	Data
(default)	REG_SZ	"E:\autorun.ico"

```
00 22 00 45 00 3A 00 5C 00-61 00 75 00 74 00 6F 00 "·E·:·\·a·u·t·o·
10 72 00 75 00 6E 00 2E 00-69 00 63 00 6F 00 22 00 r·u·n·.·i·c·o·"·
20 20 00 00 00                                      ···
```

Key Properties

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

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



Name	Type	Data
(default)	REG_SZ	DEFT_8

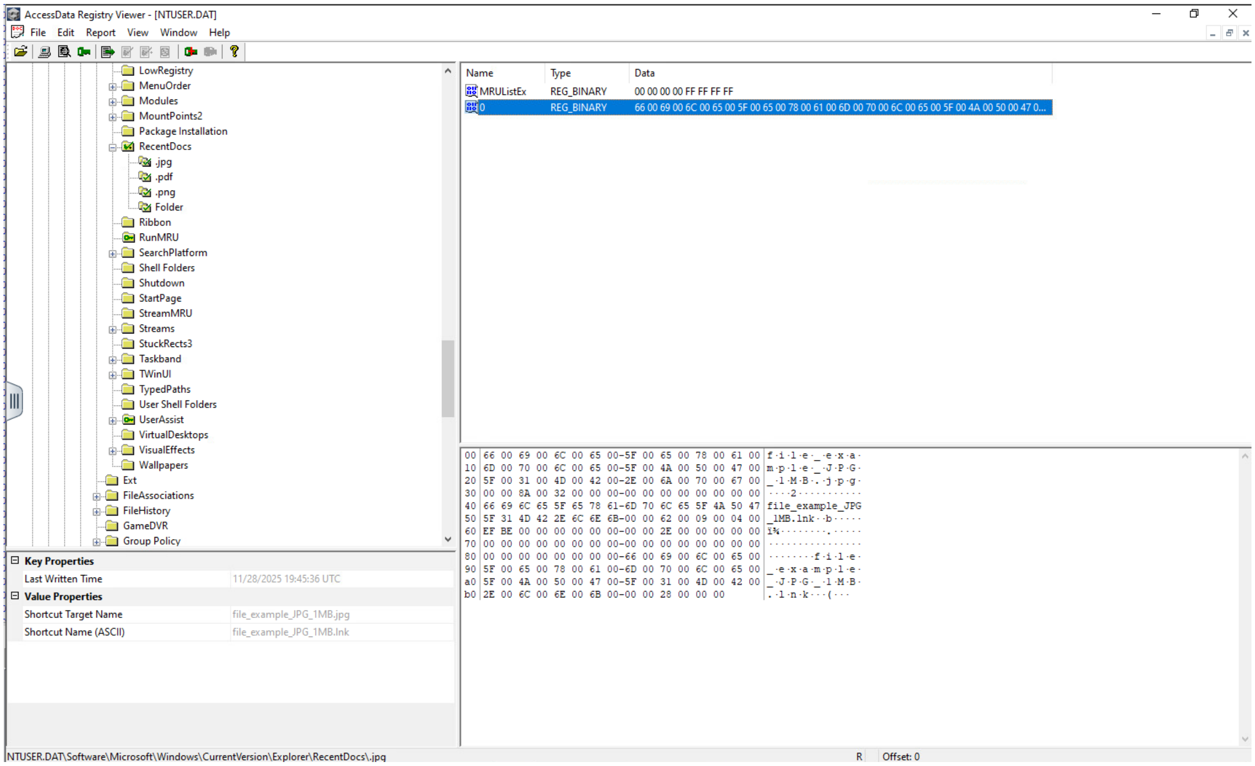
```
0 44 00 45 00 46 00 54 00-5F 00 38 00 00 00        D·E·F·T·_·8···
```

Key Properties

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

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.

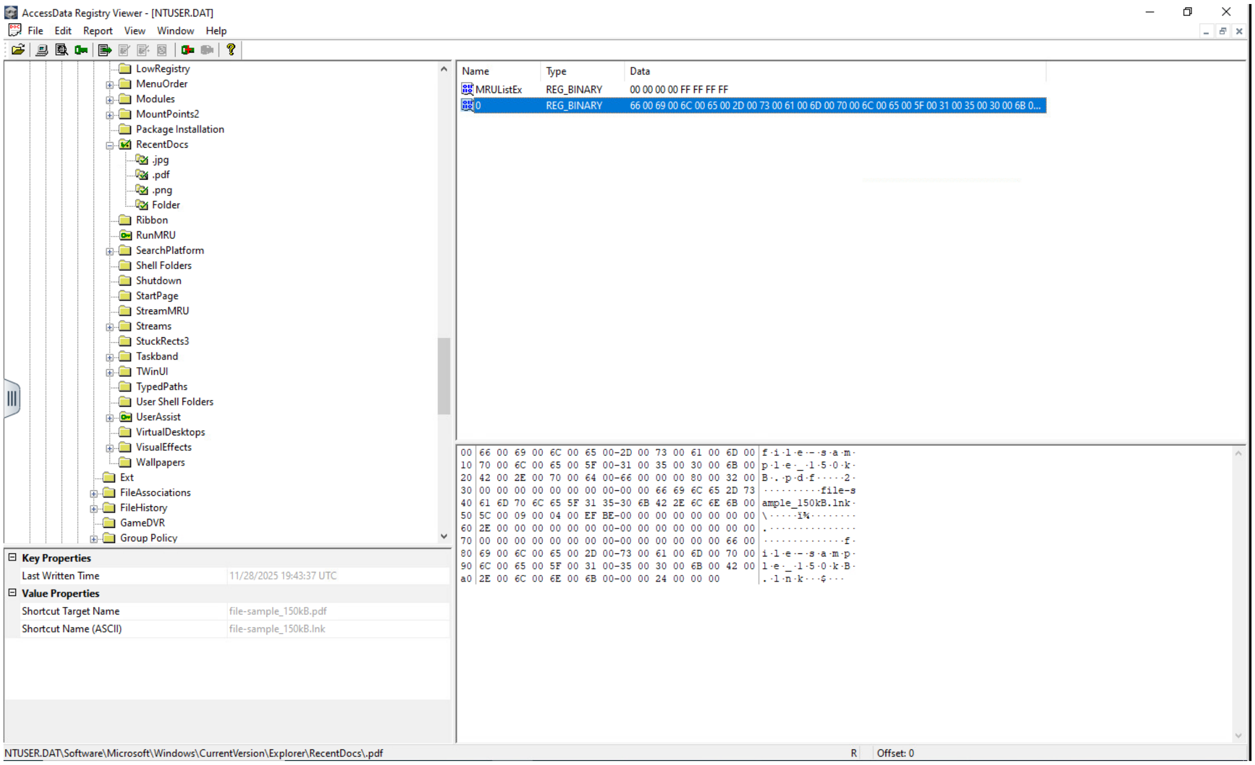


Name	Type	Data
MRUListEx	REG_BINARY	00 00 00 00 FF FF FF FF
0	REG_BINARY	66 00 69 00 6C 00 65 00 5F 00 65 00 78 00 61 00 6D 00 70 00 6C 00 65 00 5F 00 4A 00 50 00 47 0...

```
00 66 00 69 00 6C 00 65 00-5F 00 65 00 78 00 61 00 f·i·l·e·_·e·x·a·
10 6D 00 70 00 6C 00 65 00-5F 00 4A 00 50 00 47 00 m·p·l·e·_·J·P·G·
20 5F 00 31 00 4D 00 42 00-2E 00 6A 00 70 00 67 00 _·1·M·B·.·j·p·g·
30 00 00 8A 00 32 00 00 00-00 00 00 00 00 00 00 00 ····2···········
40 66 69 6C 65 5F 65 78 61-6D 70 6C 65 5F 4A 50 47 file_example_JPG
50 5F 31 4D 42 2E 6C 6E 6B-00 00 62 00 09 00 04 00 _1MB.lnk··b·····
60 EF BE 00 00 00 00 00 00-00 00 2E 00 00 00 00 00 ï¾········.·····
70 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
80 00 00 00 00 00 00 00 00-66 00 69 00 6C 00 65 00 ········f·i·l·e·
90 5F 00 65 00 78 00 61 00-6D 00 70 00 6C 00 65 00 _·e·x·a·m·p·l·e·
a0 5F 00 4A 00 50 00 47 00-5F 00 31 00 4D 00 42 00 _·J·P·G·_·1·M·B·
b0 2E 00 6C 00 6E 00 6B 00-00 00 28 00 00 00       .·l·n·k···(···
```

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

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg R Offset: 0

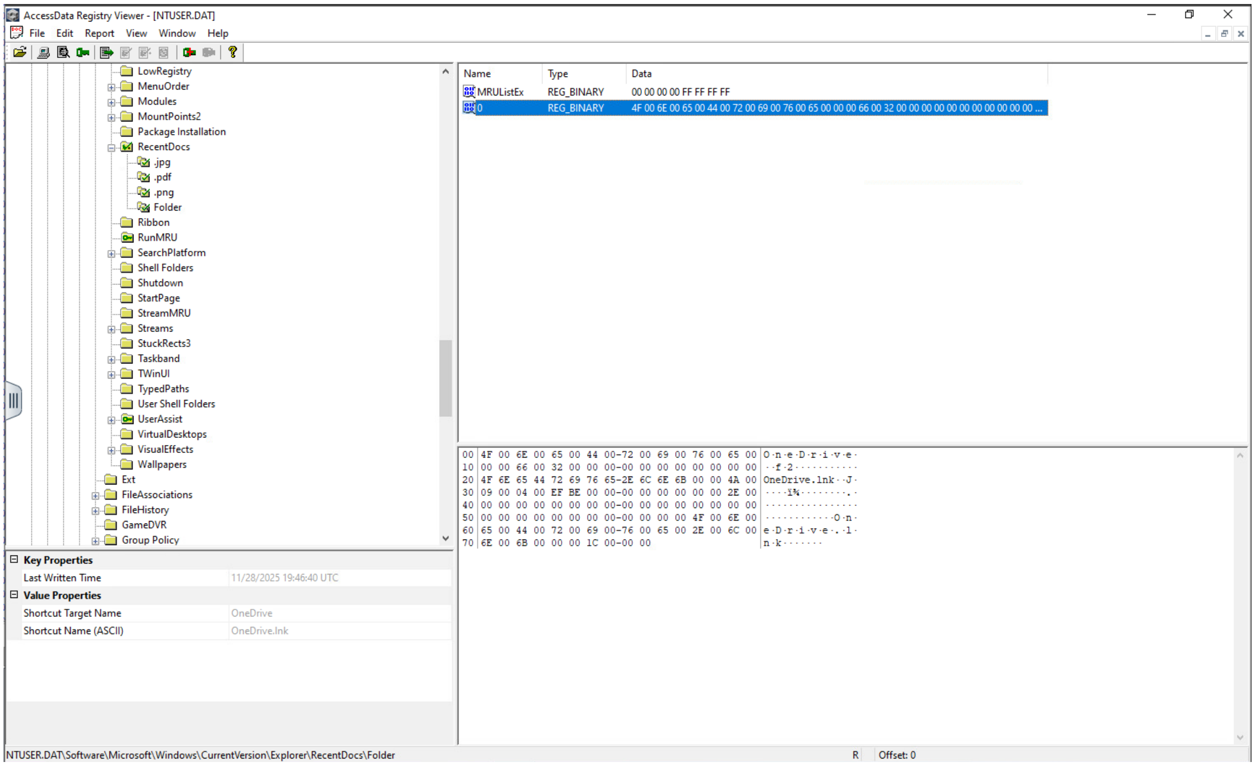


Name	Type	Data
MRUListEx	REG_BINARY	00 00 00 00 FF FF FF FF
0	REG_BINARY	66 00 69 00 6C 00 65 00 2D 00 73 00 61 00 6D 00 70 00 6C 00 65 00 5F 00 31 00 35 00 30 00 6B 0...

```
00 66 00 69 00 6C 00 65 00-2D 00 73 00 61 00 6D 00 f·i·l·e·-·s·a·m·
10 70 00 6C 00 65 00 5F 00-31 00 35 00 30 00 6B 00 p·l·e·_·1·5·0·k·
20 42 00 2E 00 70 00 64 00-66 00 00 00 80 00 32 00 B·.·p·d·f·····2·
30 00 00 00 00 00 00 00 00-00 00 66 69 6C 65 2D 73 ··········file-s
40 61 6D 70 6C 65 5F 31 35-30 6B 42 2E 6C 6E 6B 00 ample_150kB.lnk·
50 5C 00 09 00 04 00 EF BE-00 00 00 00 00 00 00 00 \·····ï¾········
60 2E 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .···············
70 00 00 00 00 00 00 00 00-00 00 00 00 00 00 66 00 ··············f·
80 69 00 6C 00 65 00 2D 00-73 00 61 00 6D 00 70 00 i·l·e·-·s·a·m·p·
90 6C 00 65 00 5F 00 31 00-35 00 30 00 6B 00 42 00 l·e·_·1·5·0·k·B·
a0 2E 00 6C 00 6E 00 6B 00-00 00 24 00 00 00       .·l·n·k···$···
```

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

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf R Offset: 0



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 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

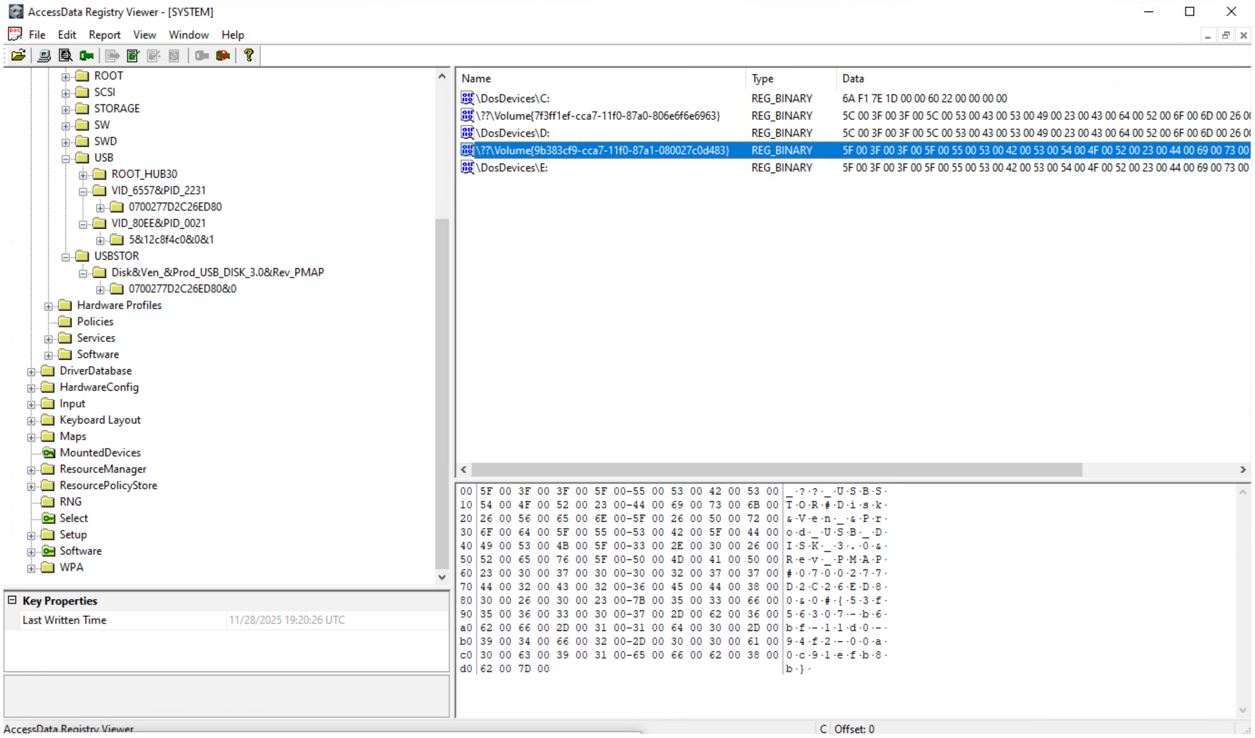
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder R Offset: 0

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:\



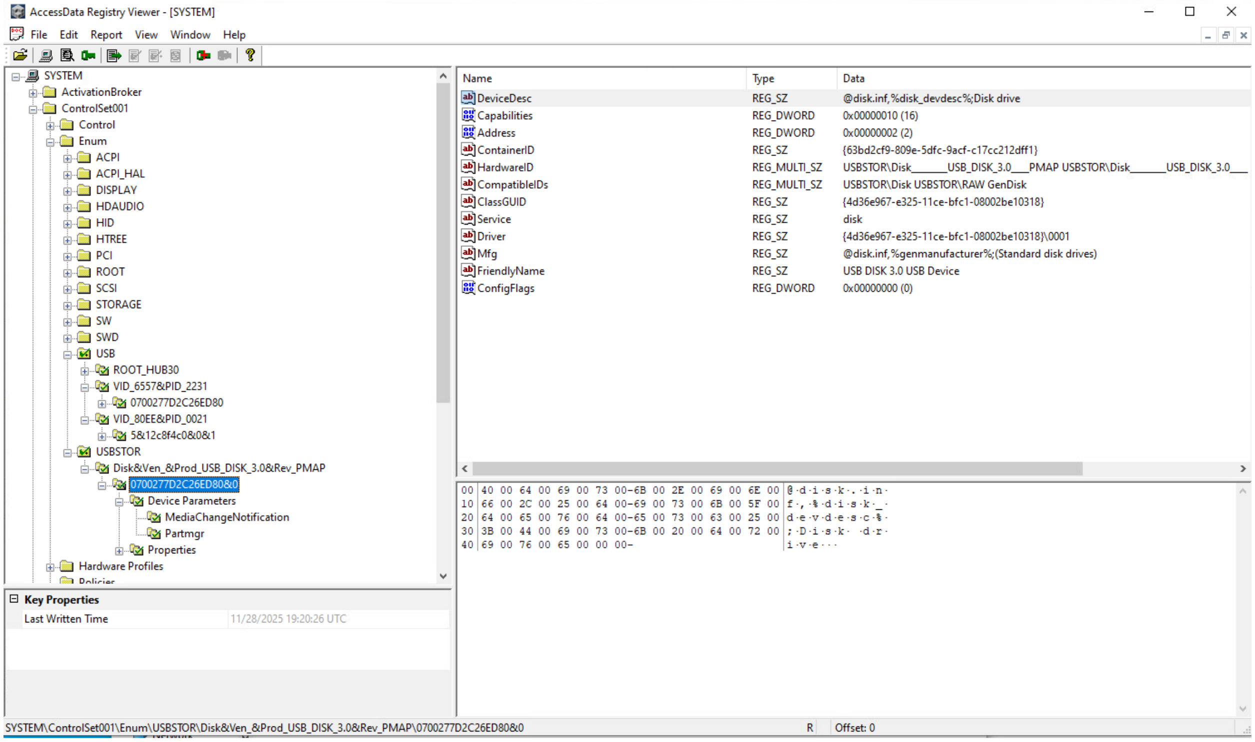
Name	Type	Data
\DosDevices\C:	REG_BINARY	6A F1 7E 1D 00 00 60 22 00 00 00 00
\??\Volume{7f3ff1ef-cca7-11f0-87a0-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 49 00 23 00 43 00 64 00 52 00 6F 00 6D 00 26 0
\DosDevices\D:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 49 00 23 00 43 00 64 00 52 00 6F 00 6D 00 26 0
\??\Volume{9b383cf9-cca7-11f0-87a1-080027c0d483}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23 00 44 00 69 00 73 00
\DosDevices\E:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4F 00 52 00 23 00 44 00 69 00 73 00

```
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·_·&·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·&·
50 52 00 65 00 76 00 5F 00-50 00 4D 00 41 00 50 00  R·e·v·_·P·M·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 66 00  0·&·0·#·{·5·3·f·
90 35 00 36 00 33 00 30 00-37 00 2D 00 62 00 36 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·}·
```

Key Properties

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

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



```
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
```

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···
```

⊟ **Key Properties**

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

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