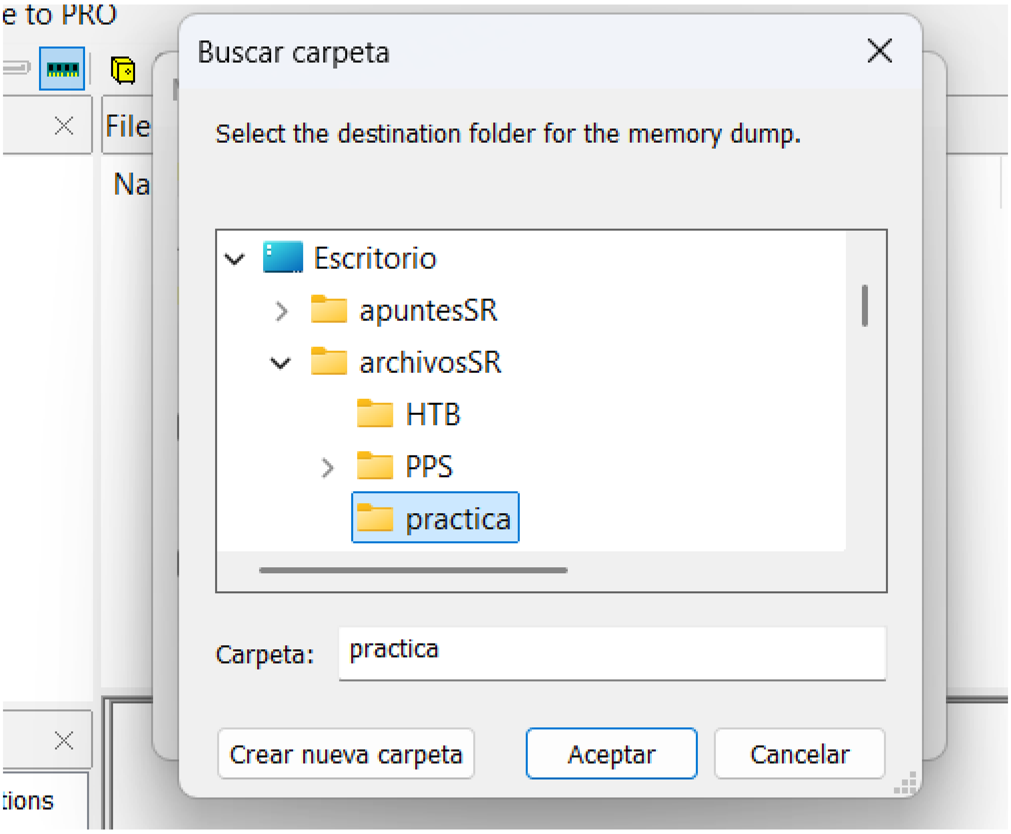
Tarea 2.1.1. Recopilación de evidencias con FTK

Trabajo realizado por:
Samuel Romero de los Reyes

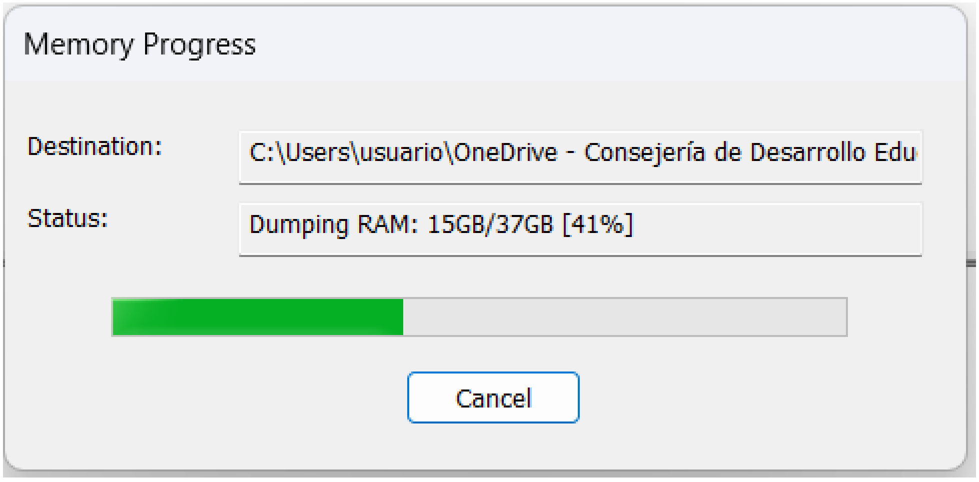
Para capturar la RAM, le damos a la RAM dibujada de arriba a la izquierda.



Buscar carpeta

Select the destination folder for the memory dump.

Carpeta: practica

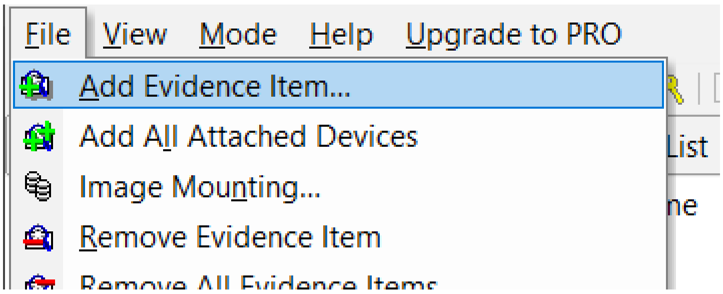


Memory Progress

Destination: C:\Users\usuario\OneDrive - Consejería de Desarrollo Edu

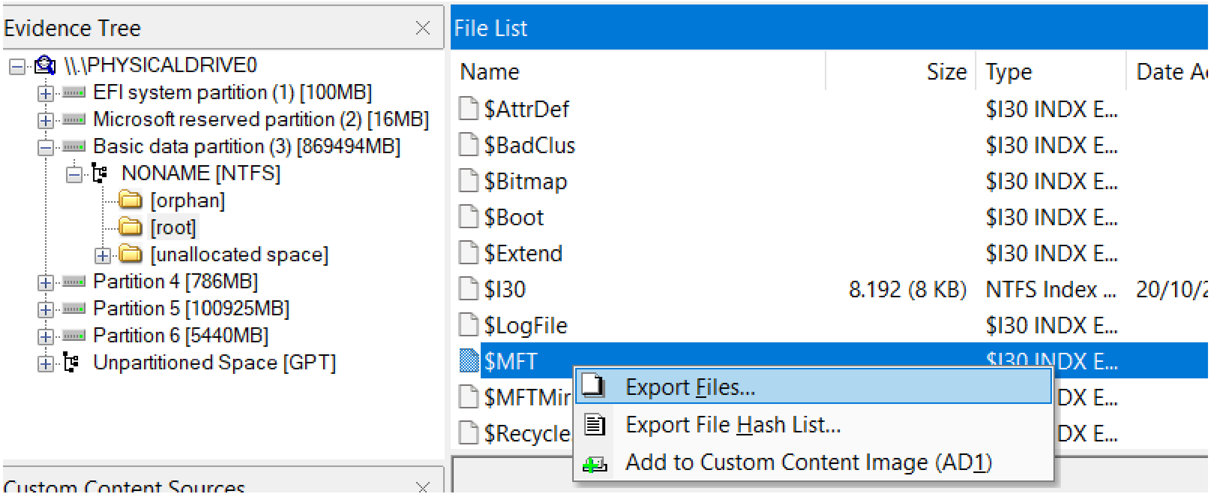
Status: Dumping RAM: 15GB/37GB [41%]

Para las siguientes, creamos una evidencia.



Una vez copiado, buscamos dentro de los directorios donde sale cada uno:

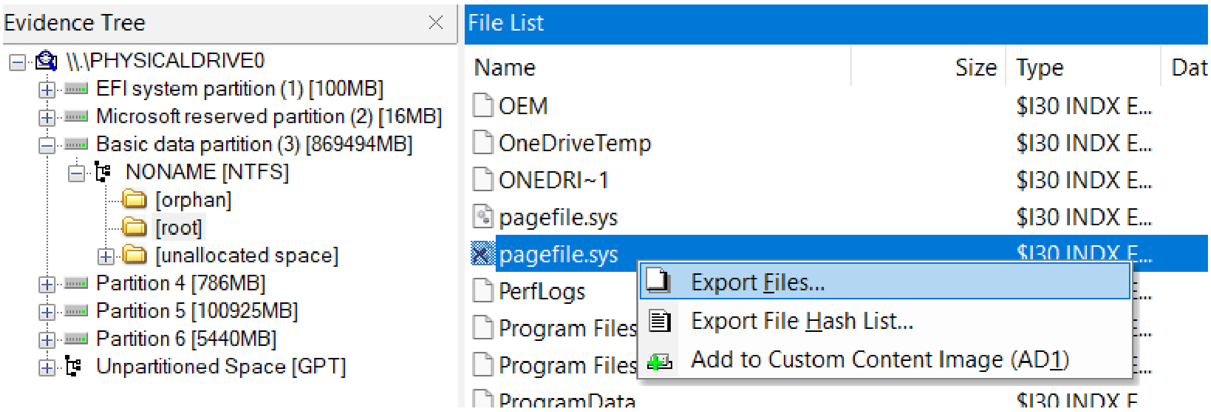
C:\$MFT



- \\.\PHYSICALDRIVE0
  - EFI system partition (1) [100MB]
  - Microsoft reserved partition (2) [16MB]
  - Basic data partition (3) [869494MB]
    - NONAME [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
  - Partition 4 [786MB]
  - Partition 5 [100925MB]
  - Partition 6 [5440MB]
  - Unpartitioned Space [GPT]

Name	Size	Type	Date A
$AttrDef		$I30 INDX E...	
$BadClus		$I30 INDX E...	
$Bitmap		$I30 INDX E...	
$Boot		$I30 INDX E...	
$Extend		$I30 INDX E...	
$I30	8.192 (8 KB)	NTFS Index ...	20/10/2
$LogFile		$I30 INDX E...	
$MFT		$I30 INDX E...	
$MFTMir		DX E...	
$Recycle		DX E...	

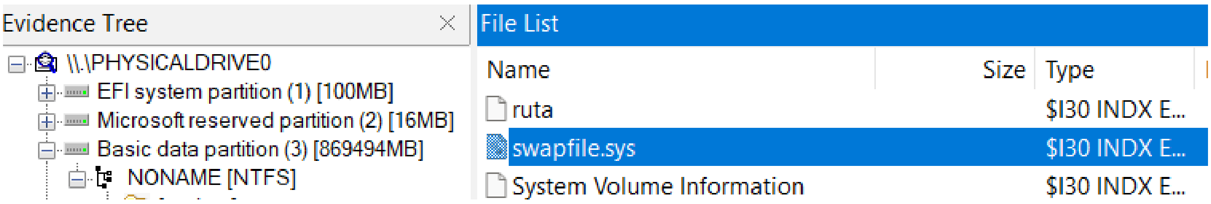
C:\pagefile.sys



- \\.\PHYSICALDRIVE0
  - EFI system partition (1) [100MB]
  - Microsoft reserved partition (2) [16MB]
  - Basic data partition (3) [869494MB]
    - NONAME [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
  - Partition 4 [786MB]
  - Partition 5 [100925MB]
  - Partition 6 [5440MB]
  - Unpartitioned Space [GPT]

Name	Size	Type	Dat
OEM		$I30 INDX E...	
OneDriveTemp		$I30 INDX E...	
ONEDRI~1		$I30 INDX E...	
pagefile.sys		$I30 INDX E...	
pagefile.sys		$I30 INDX E...	
PerfLogs		E...	
Program Files		E...	
Program Files		E...	
ProgramData		$I30 INDX E	

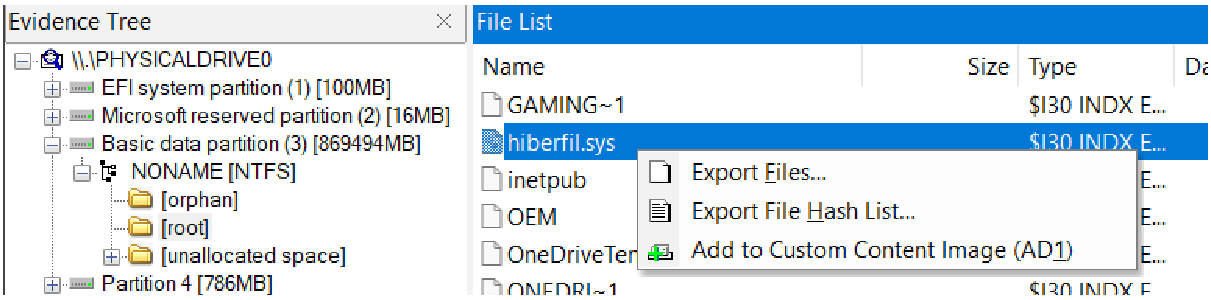
C:\swapfile.sys



- \\.\PHYSICALDRIVE0
  - EFI system partition (1) [100MB]
  - Microsoft reserved partition (2) [16MB]
  - Basic data partition (3) [869494MB]
    - NONAME [NTFS]

Name	Size	Type
ruta		$I30 INDX E...
swapfile.sys		$I30 INDX E...
System Volume Information		$I30 INDX E...

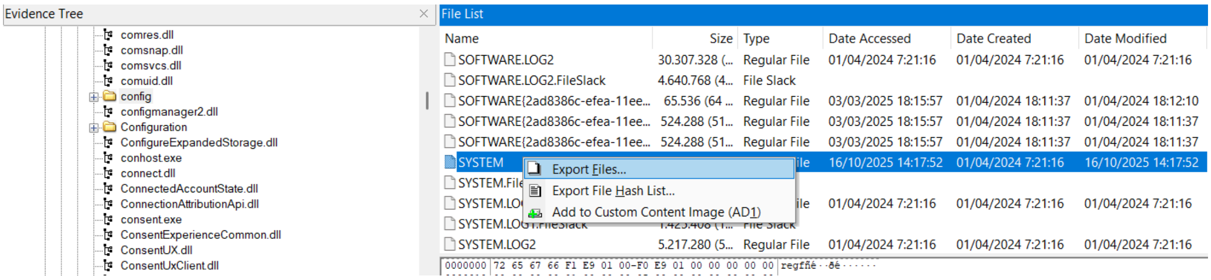
C:\hiberfil.sys



- \\.\PHYSICALDRIVE0
  - EFI system partition (1) [100MB]
  - Microsoft reserved partition (2) [16MB]
  - Basic data partition (3) [869494MB]
    - NONAME [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
  - Partition 4 [786MB]

Name	Size	Type	Da
GAMING~1		$I30 INDX E...	
hiberfil.sys		$I30 INDX E...	
inetpub		E...	
OEM		E...	
OneDriveTer		E...	
ONEDRI~1		$I30 INDX E	

C:\Windows\System32\config\SYSTEM



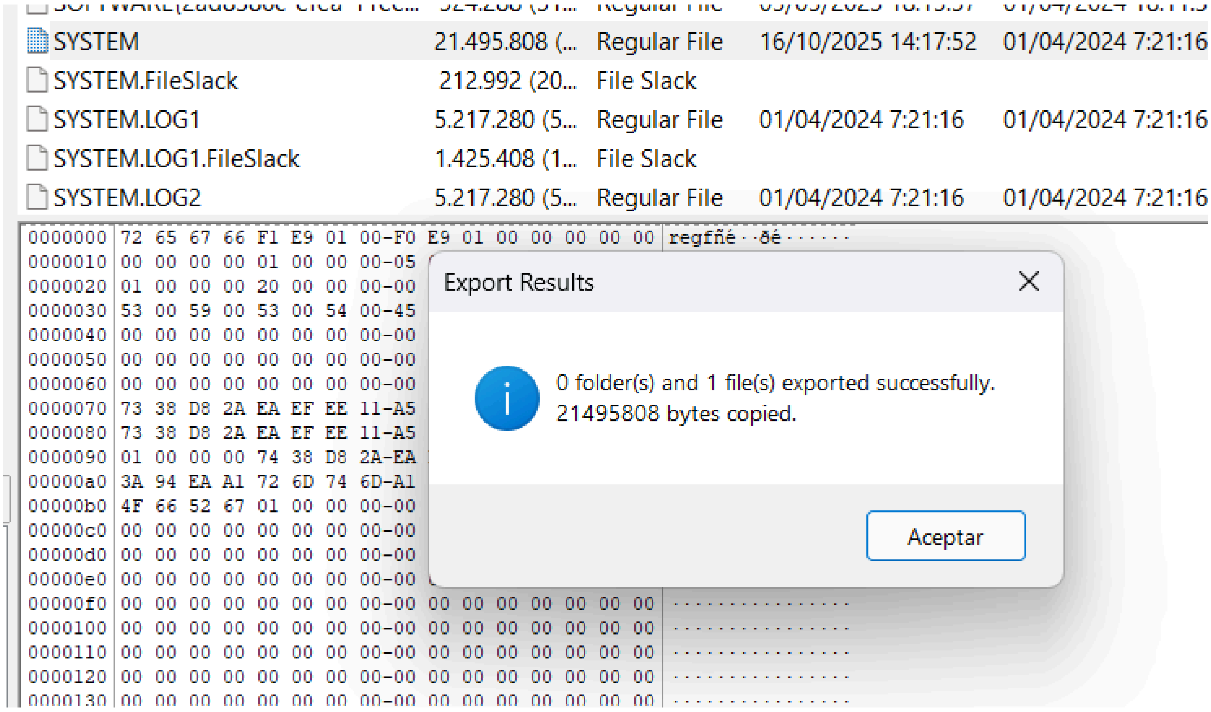
Evidence Tree

- comres.dll
- comsnap.dll
- comsvcs.dll
- comuid.dll
- config
- configmanager2.dll
- Configuration
- ConfigureExpandedStorage.dll
- conhost.exe
- connect.dll
- ConnectedAccountState.dll
- ConnectionAttributionApi.dll
- consent.exe
- ConsentExperienceCommon.dll
- ConsentUX.dll
- ConsentUxClient.dll

File List

Name	Size	Type	Date Accessed	Date Created	Date Modified
SOFTWARE.LOG2	30.307.328 (...	Regular File	01/04/2024 7:21:16	01/04/2024 7:21:16	01/04/2024 7:21:16
SOFTWARE.LOG2.FileSlack	4.640.768 (4...	File Slack			
SOFTWARE{2ad8386c-efea-11ee...	65.536 (64 ...	Regular File	03/03/2025 18:15:57	01/04/2024 18:11:37	01/04/2024 18:12:10
SOFTWARE{2ad8386c-efea-11ee...	524.288 (51...	Regular File	03/03/2025 18:15:57	01/04/2024 18:11:37	01/04/2024 18:11:37
SOFTWARE{2ad8386c-efea-11ee...	524.288 (51...	Regular File	03/03/2025 18:15:57	01/04/2024 18:11:37	01/04/2024 18:11:37
SYSTEM		ile	16/10/2025 14:17:52	01/04/2024 7:21:16	16/10/2025 14:17:52
SYSTEM.File					
SYSTEM.LO		ile	01/04/2024 7:21:16	01/04/2024 7:21:16	01/04/2024 7:21:16
SYSTEM.LOG1.FileSlack	1.425.408 (1...	File Slack			
SYSTEM.LOG2	5.217.280 (5...	Regular File	01/04/2024 7:21:16	01/04/2024 7:21:16	01/04/2024 7:21:16

```
0000000 72 65 67 66 F1 E9 01 00-F0 E9 01 00 00 00 00 00 regfñé··ðé······
```



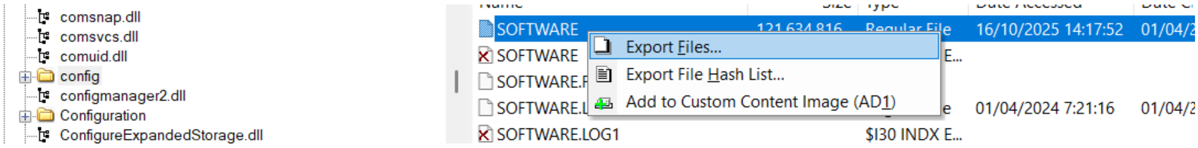
SYSTEM	21.495.808 (...	Regular File	16/10/2025 14:17:52	01/04/2024 7:21:16
SYSTEM.FileSlack	212.992 (20...	File Slack		
SYSTEM.LOG1	5.217.280 (5...	Regular File	01/04/2024 7:21:16	01/04/2024 7:21:16
SYSTEM.LOG1.FileSlack	1.425.408 (1...	File Slack		
SYSTEM.LOG2	5.217.280 (5...	Regular File	01/04/2024 7:21:16	01/04/2024 7:21:16

```
0000000 72 65 67 66 F1 E9 01 00-F0 E9 01 00 00 00 00 00 regfñé··ðé······
0000010 00 00 00 00 01 00 00 00-05
0000020 01 00 00 00 20 00 00 00-00
0000030 53 00 59 00 53 00 54 00-45
0000040 00 00 00 00 00 00 00 00-00
0000050 00 00 00 00 00 00 00 00-00
0000060 00 00 00 00 00 00 00 00-00
0000070 73 38 D8 2A EA EF EE 11-A5
0000080 73 38 D8 2A EA EF EE 11-A5
0000090 01 00 00 00 74 38 D8 2A-EA
00000a0 3A 94 EA A1 72 6D 74 6D-A1
00000b0 4F 66 52 67 01 00 00 00-00
00000c0 00 00 00 00 00 00 00 00-00
00000d0 00 00 00 00 00 00 00 00-00
00000e0 00 00 00 00 00 00 00 00-00
00000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

Export Results

0 folder(s) and 1 file(s) exported successfully.
21495808 bytes copied.

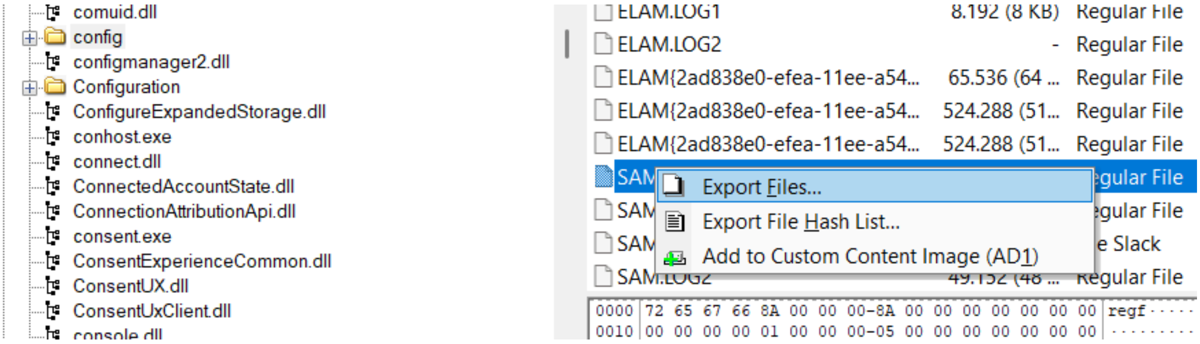
C:\Windows\System32\config\SOFTWARE



- comsnap.dll
- comsvcs.dll
- comuid.dll
- config
- configmanager2.dll
- Configuration
- ConfigureExpandedStorage.dll

SOFTWARE	121.634.816	Regular File	16/10/2025 14:17:52	01/04/2
SOFTWARE		E...		
SOFTWARE.F				
SOFTWARE.L		e	01/04/2024 7:21:16	01/04/2
SOFTWARE.LOG1		$I30 INDX E...		

C:\Windows\System32\config\SAM

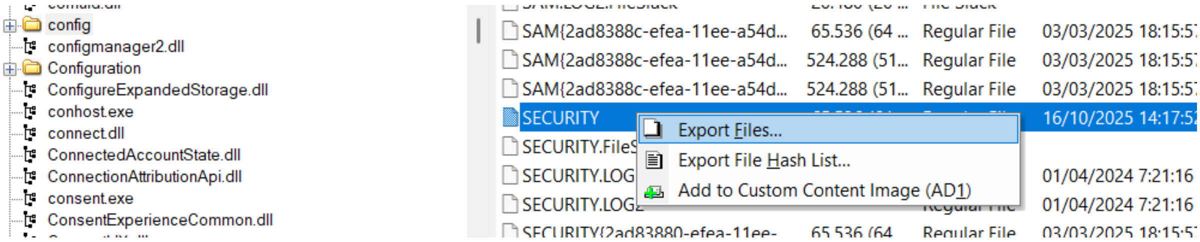


- comuid.dll
- config
- configmanager2.dll
- Configuration
- ConfigureExpandedStorage.dll
- conhost.exe
- connect.dll
- ConnectedAccountState.dll
- ConnectionAttributionApi.dll
- consent.exe
- ConsentExperienceCommon.dll
- ConsentUX.dll
- ConsentUxClient.dll
- console.dll

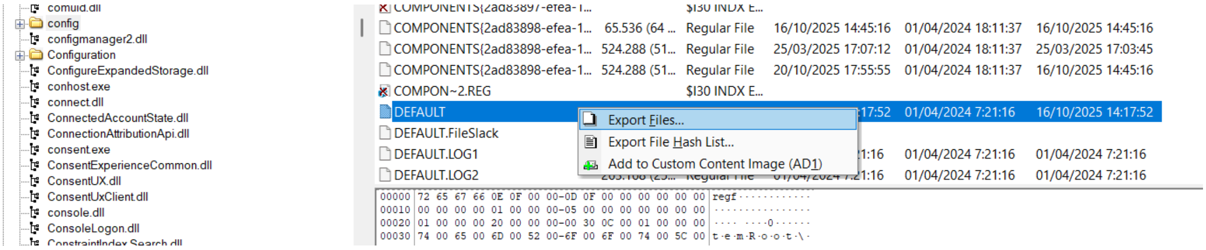
ELAM.LOG1	8.192 (8 KB)	Regular File
ELAM.LOG2	-	Regular File
ELAM{2ad838e0-efea-11ee-a54...	65.536 (64 ...	Regular File
ELAM{2ad838e0-efea-11ee-a54...	524.288 (51...	Regular File
ELAM{2ad838e0-efea-11ee-a54...	524.288 (51...	Regular File
SAM		gular File
SAM		gular File
SAM		e Slack
SAM.LOG2	49.152 (48 ...	Regular File

```
0000 72 65 67 66 8A 00 00 00-8A 00 00 00 00 00 00 00 regf·····
0010 00 00 00 00 01 00 00 00-05 00 00 00 00 00 00 00 ·········
```

C:\Windows\System32\config\SECURITY


config
configmanager2.dll
Configuration
ConfigureExpandedStorage.dll
conhost.exe
connect.dll
ConnectedAccountState.dll
ConnectionAttributionApi.dll
consent.exe
ConsentExperienceCommon.dll
Export Files...
Export File Hash List...
Add to Custom Content Image (AD1)

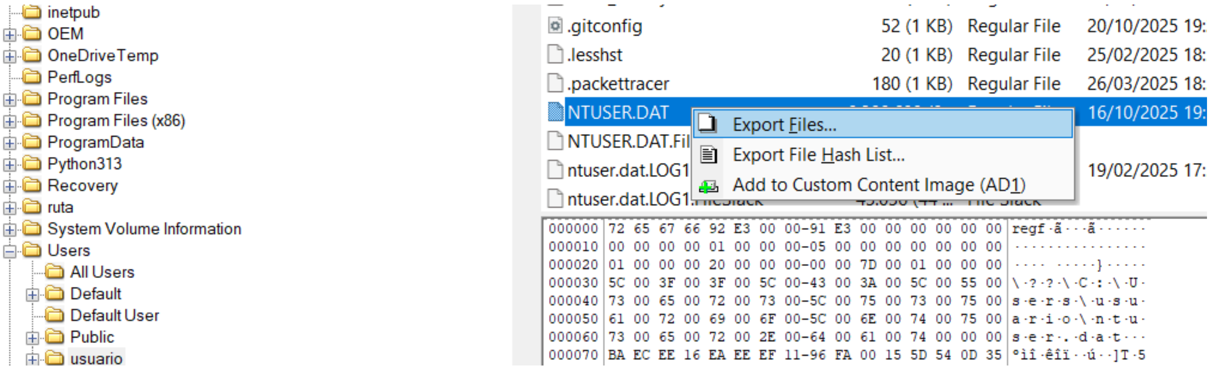
```
SAM{2ad8388c-efea-11ee-a54d...   65.536 (64 ...   Regular File   03/03/2025 18:15:5
SAM{2ad8388c-efea-11ee-a54d...   524.288 (51...   Regular File   03/03/2025 18:15:5
SAM{2ad8388c-efea-11ee-a54d...   524.288 (51...   Regular File   03/03/2025 18:15:5
SECURITY                                                         16/10/2025 14:17:5
SECURITY.FileS
SECURITY.LOG                                                     01/04/2024 7:21:16
SECURITY.LOG2                                                    01/04/2024 7:21:16
SECURITY{2ad83880-efea-11ee-     65.536 (64       Regular File   03/03/2025 18:15:5
```



```
COMPONENTS{2ad83897-efea-1...                $I30 INDX E...
COMPONENTS{2ad83898-efea-1...  65.536 (64 ...  Regular File  16/10/2025 14:45:16  01/04/2024 18:11:37  16/10/2025 14:45:16
COMPONENTS{2ad83898-efea-1...  524.288 (51...  Regular File  25/03/2025 17:07:12  01/04/2024 18:11:37  25/03/2025 17:03:45
COMPONENTS{2ad83898-efea-1...  524.288 (51...  Regular File  20/10/2025 17:55:55  01/04/2024 18:11:37  16/10/2025 14:45:16
COMPON~2.REG                                 $I30 INDX E...
DEFAULT                                                         17:52  01/04/2024 7:21:16   16/10/2025 14:17:52
DEFAULT.FileSlack
DEFAULT.LOG1                                                    1:16   01/04/2024 7:21:16   01/04/2024 7:21:16
DEFAULT.LOG2                                                    1:16   01/04/2024 7:21:16   01/04/2024 7:21:16
```

```
00000 72 65 67 66 0E 0F 00 00-0D 0F 00 00 00 00 00 00 regf············
00010 00 00 00 00 01 00 00 00-05 00 00 00 00 00 00 00 ················
00020 01 00 00 00 20 00 00 00-00 30 0C 00 01 00 00 00 ···· ····0······
00030 74 00 65 00 6D 00 52 00-6F 00 6F 00 74 00 5C 00 t·e·m·R·o·o·t·\·
```

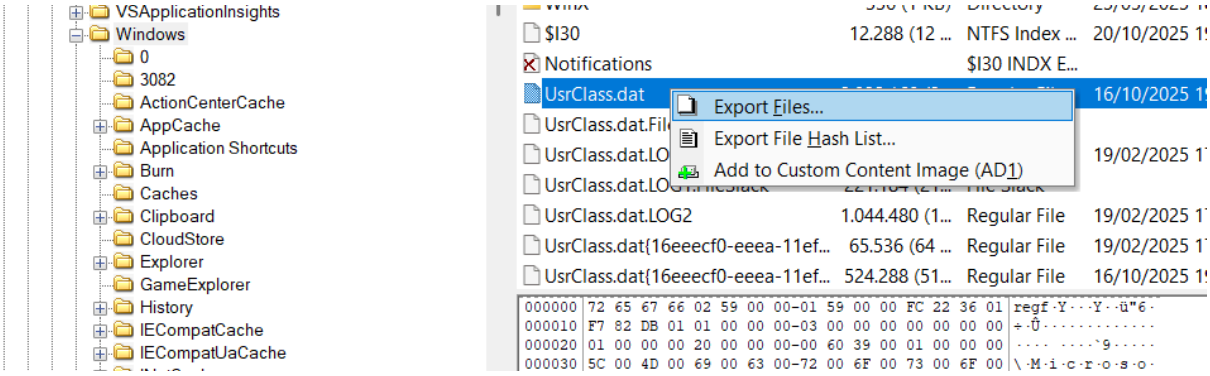
C:\Users\<nombre_de_usuario>\NTUSER.DAT



```
.gitconfig        52 (1 KB)    Regular File   20/10/2025 19:
.lesshst          20 (1 KB)    Regular File   25/02/2025 18:
.packettracer    180 (1 KB)    Regular File   26/03/2025 18:
NTUSER.DAT                                    16/10/2025 19:
NTUSER.DAT.Fil
ntuser.dat.LOG1                               19/02/2025 17:
ntuser.dat.LOG1.
```

```
000000 72 65 67 66 92 E3 00 00-91 E3 00 00 00 00 00 00 regf·ã···ã······
000010 00 00 00 00 01 00 00 00-05 00 00 00 00 00 00 00 ················
000020 01 00 00 00 20 00 00 00-00 00 7D 00 01 00 00 00 ···· ·····}·····
000030 5C 00 3F 00 3F 00 5C 00-43 00 3A 00 5C 00 55 00 \·?·?·\·C·:·\·U·
000040 73 00 65 00 72 00 73 00-5C 00 75 00 73 00 75 00 s·e·r·s·\·u·s·u·
000050 61 00 72 00 69 00 6F 00-5C 00 6E 00 74 00 75 00 a·r·i·o·\·n·t·u·
000060 73 00 65 00 72 00 2E 00-64 00 61 00 74 00 00 00 s·e·r·.·d·a·t···
000070 BA EC EE 16 EA EE EF 11-96 FA 00 15 5D 54 0D 35 ºìî·êîï··ú··]T·5
```

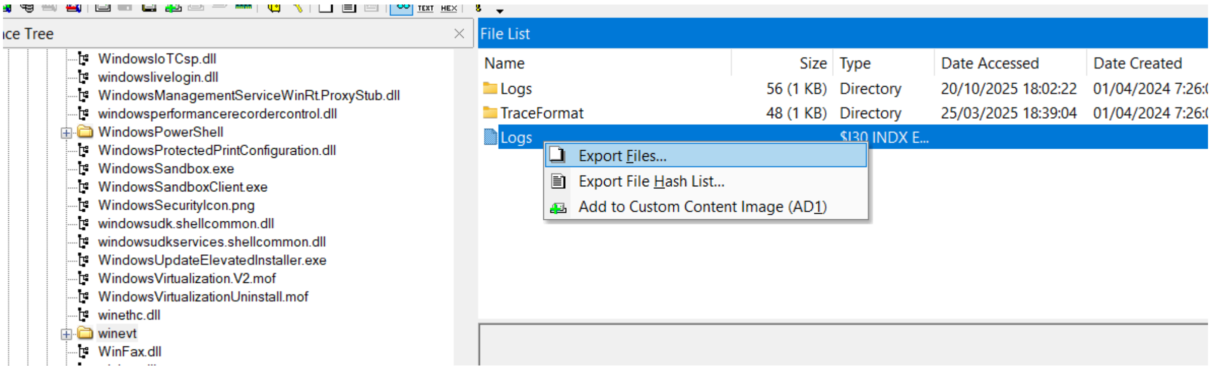
C:\Users\<nombre_de_usuario>\AppData\Local\Microsoft\Windows\UsrClass.dat



```
$I30                           12.288 (12 ...  NTFS Index ...  20/10/2025 1
Notifications                                  $I30 INDX E...
UsrClass.dat                                                   16/10/2025 1
UsrClass.dat.Fil
UsrClass.dat.LO                                                19/02/2025 1
UsrClass.dat.LO
UsrClass.dat.LOG2              1.044.480 (1...  Regular File   19/02/2025 1
UsrClass.dat{16eeecf0-eeea-11ef...  65.536 (64 ...  Regular File  19/02/2025 1
UsrClass.dat{16eeecf0-eeea-11ef...  524.288 (51...  Regular File  16/10/2025 1
```

```
000000 72 65 67 66 02 59 00 00-01 59 00 00 FC 22 36 01 regf·Y···Y··ü"6·
000010 F7 82 DB 01 01 00 00 00-03 00 00 00 00 00 00 00 ÷·Û·············
000020 01 00 00 00 20 00 00 00-00 60 39 00 01 00 00 00 ···· ····`9·····
000030 5C 00 4D 00 69 00 63 00-72 00 6F 00 73 00 6F 00 \·M·i·c·r·o·s·o·
```

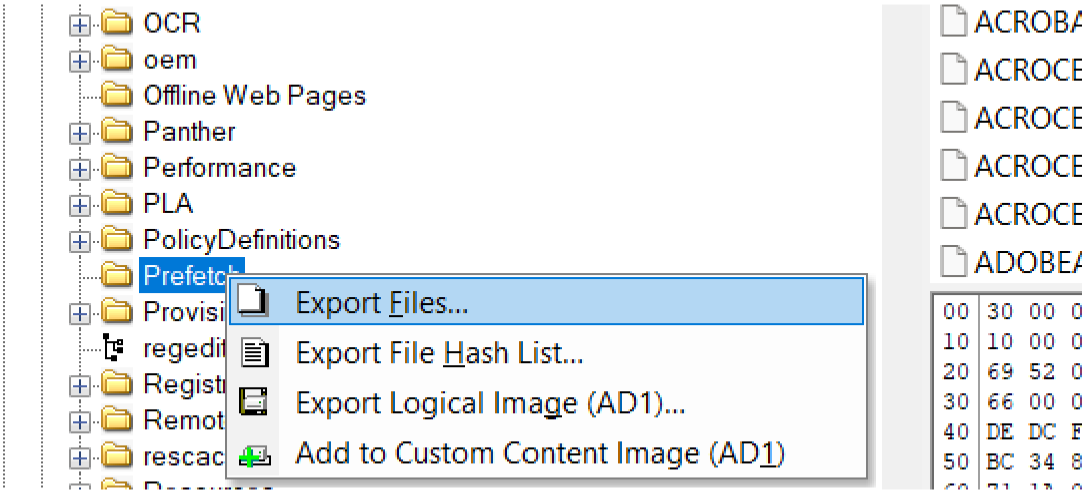
C:\Windows\System32\winevt\Logs\

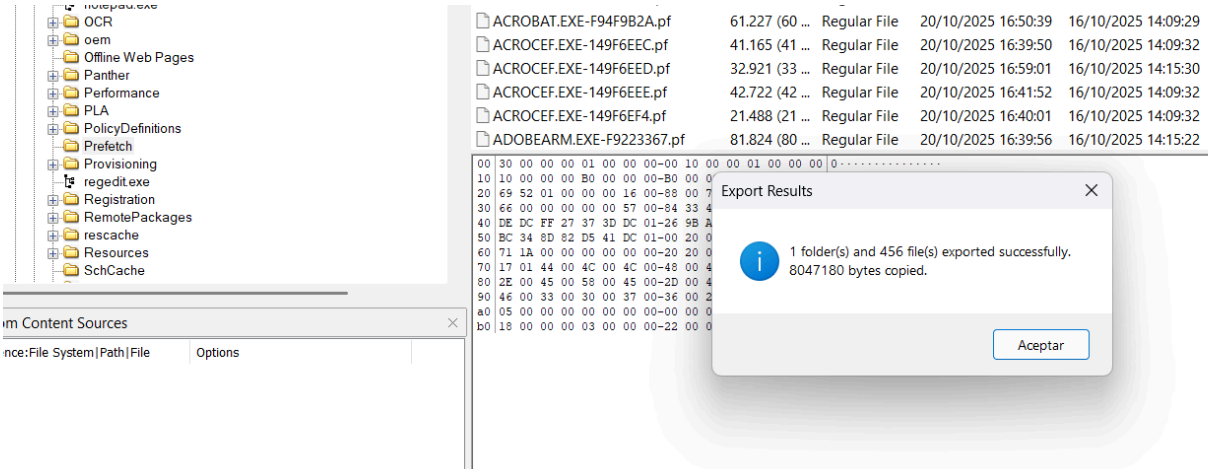


WindowsIoTCsp.dll
windowslivelogin.dll
WindowsManagementServiceWinRt.ProxyStub.dll
windowsperformancerecordercontrol.dll
WindowsPowerShell
WindowsProtectedPrintConfiguration.dll
WindowsSandbox.exe
WindowsSandboxClient.exe
WindowsSecurityIcon.png
windowsudk.shellcommon.dll
windowsudkservices.shellcommon.dll
WindowsUpdateElevatedInstaller.exe
WindowsVirtualization.V2.mof
WindowsVirtualizationUninstall.mof
winethc.dll
winevt
WinFax.dll

Name	Size	Type	Date Accessed	Date Created
Logs	56 (1 KB)	Directory	20/10/2025 18:02:22	01/04/2024 7:26:
TraceFormat	48 (1 KB)	Directory	25/03/2025 18:39:04	01/04/2024 7:26:
Logs		$I30 INDX E...		

C:\Windows\Prefetch\



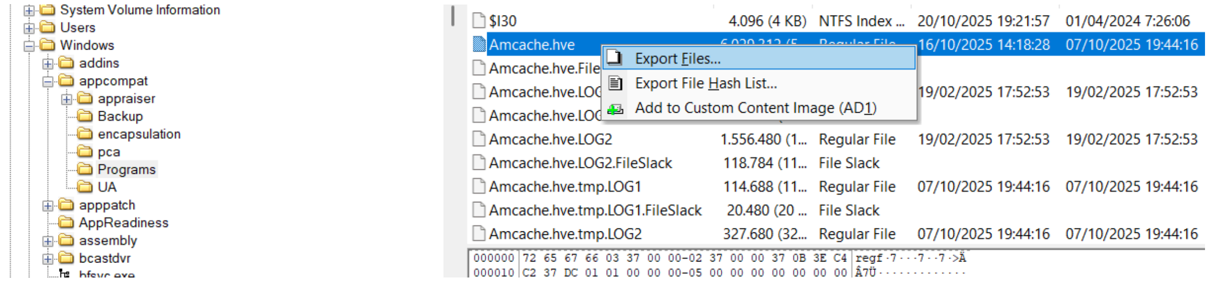


ACROBAT.EXE-F94F9B2A.pf	61.227 (60 ...	Regular File	20/10/2025 16:50:39	16/10/2025 14:09:29
ACROCEF.EXE-149F6EEC.pf	41.165 (41 ...	Regular File	20/10/2025 16:39:50	16/10/2025 14:09:32
ACROCEF.EXE-149F6EED.pf	32.921 (33 ...	Regular File	20/10/2025 16:59:01	16/10/2025 14:15:30
ACROCEF.EXE-149F6EEE.pf	42.722 (42 ...	Regular File	20/10/2025 16:41:52	16/10/2025 14:09:32
ACROCEF.EXE-149F6EF4.pf	21.488 (21 ...	Regular File	20/10/2025 16:40:01	16/10/2025 14:09:32
ADOBEARM.EXE-F9223367.pf	81.824 (80 ...	Regular File	20/10/2025 16:39:56	16/10/2025 14:15:22

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00
10 10 00 00 00 B0 00 00 00-B0 00 0
20 69 52 01 00 00 00 16 00-88 00 7
30 66 00 00 00 00 00 57 00-84 33 4
40 DE DC FF 27 37 3D DC 01-26 9B A
50 BC 34 8D 82 D5 41 DC 01-00 20 0
60 71 1A 00 00 00 00 00 00-20 20 0
70 17 01 44 00 4C 00 4C 00-48 00 4
80 2E 00 45 00 58 00 45 00-2D 00 4
90 46 00 33 00 30 00 37 00-36 00 2
a0 05 00 00 00 00 00 00 00-00 00 0
b0 18 00 00 00 03 00 00 00-22 00 0
```

1 folder(s) and 456 file(s) exported successfully.
8047180 bytes copied.

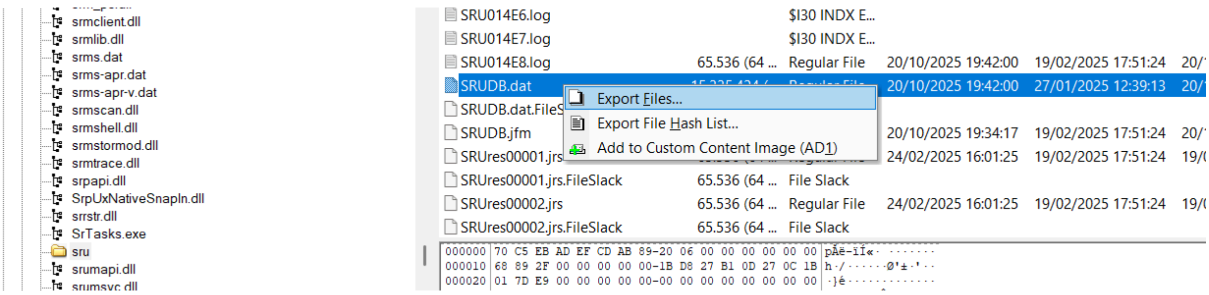
C:\Windows\AppCompat\Programs\Amcache.hve



$I30	4.096 (4 KB)	NTFS Index ...	20/10/2025 19:21:57	01/04/2024 7:26:06
Amcache.hve			16/10/2025 14:18:28	07/10/2025 19:44:16
Amcache.hve.File				
Amcache.hve.LOG			19/02/2025 17:52:53	19/02/2025 17:52:53
Amcache.hve.LOG				
Amcache.hve.LOG2	1.556.480 (1...	Regular File	19/02/2025 17:52:53	19/02/2025 17:52:53
Amcache.hve.LOG2.FileSlack	118.784 (11...	File Slack		
Amcache.hve.tmp.LOG1	114.688 (11...	Regular File	07/10/2025 19:44:16	07/10/2025 19:44:16
Amcache.hve.tmp.LOG1.FileSlack	20.480 (20 ...	File Slack		
Amcache.hve.tmp.LOG2	327.680 (32...	Regular File	07/10/2025 19:44:16	07/10/2025 19:44:16

```
000000 72 65 67 66 03 37 00 00-02 37 00 00 37 0B 3E C4 regf·7···7··7·>Ä
000010 C2 37 DC 01 01 00 00 00-05 00 00 00 00 00 00 00 Â7Ü·············
```

C:\Windows\System32\sru\SRUDB.dat

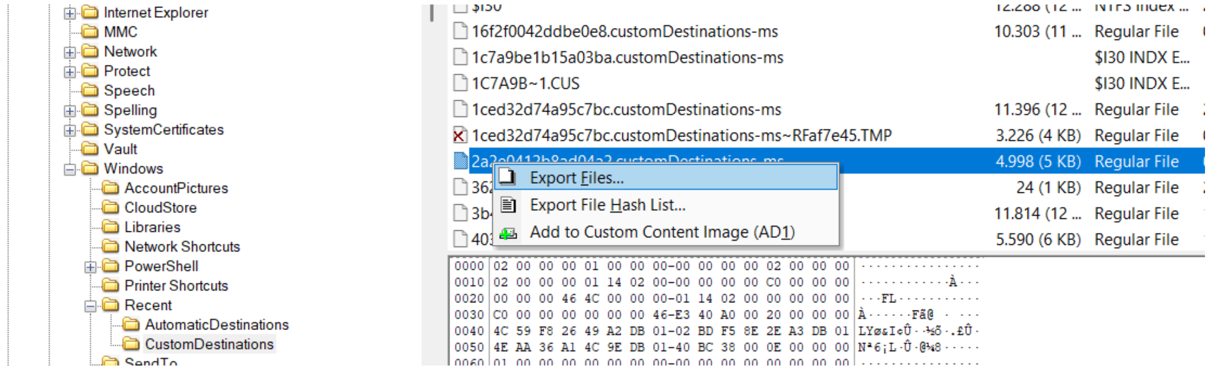


```
srmclient.dll
srmlib.dll
srms.dat
srms-apr.dat
srms-apr-v.dat
srmscan.dll
srmshell.dll
srmstormod.dll
srmtrace.dll
srpapi.dll
SrpUxNativeSnapIn.dll
srrstr.dll
SrTasks.exe
sru
srumapi.dll
srumsvc.dll
```

```
SRU014E6.log                                $I30 INDX E...
SRU014E7.log                                $I30 INDX E...
SRU014E8.log                 65.536 (64 ... Regular File  20/10/2025 19:42:00  19/02/2025 17:51:24  20/
SRUDB.dat                                                 20/10/2025 19:42:00  27/01/2025 12:39:13  20/
SRUDB.dat.FileS
SRUDB.jfm                                                 20/10/2025 19:34:17  19/02/2025 17:51:24  20/
SRUres00001.jrs                                           24/02/2025 16:01:25  19/02/2025 17:51:24  19/
SRUres00001.jrs.FileSlack    65.536 (64 ... File Slack
SRUres00002.jrs              65.536 (64 ... Regular File  24/02/2025 16:01:25  19/02/2025 17:51:24  19/
SRUres00002.jrs.FileSlack    65.536 (64 ... File Slack
```

```
000000 70 C5 EB AD EF CD AB 89-20 06 00 00 00 00 00 00 pÅë-ïÍ«· ·······
000010 68 89 2F 00 00 00 00 00-1B D8 27 B1 0D 27 0C 1B h·/······Ø'±·'··
000020 01 7D E9 00 00 00 00 00-00 00 00 00 00 00 00 00 ·}é·············
```

C:\Users\<usuario>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\
C:\Users\<usuario>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\



```
Internet Explorer
MMC
Network
Protect
Speech
Spelling
SystemCertificates
Vault
Windows
  AccountPictures
  CloudStore
  Libraries
  Network Shortcuts
  PowerShell
  Printer Shortcuts
  Recent
    AutomaticDestinations
    CustomDestinations
  SendTo
```

```
$I30                                                  12.288 (12 ...  NTFS Index ...
16f2f0042ddbe0e8.customDestinations-ms                10.303 (11 ...  Regular File
1c7a9be1b15a03ba.customDestinations-ms                                $I30 INDX E...
1C7A9B~1.CUS                                                          $I30 INDX E...
1ced32d74a95c7bc.customDestinations-ms                11.396 (12 ...  Regular File
1ced32d74a95c7bc.customDestinations-ms~RFaf7e45.TMP   3.226 (4 KB)    Regular File
2a2e0412b8ad04a2.customDestinations-ms                4.998 (5 KB)    Regular File
362                                                   24 (1 KB)       Regular File
3b                                                    11.814 (12 ...  Regular File
403                                                   5.590 (6 KB)    Regular File
```

```
0000 02 00 00 00 01 00 00 00-00 00 00 00 02 00 00 00 ················
0010 02 00 00 00 01 14 02 00-00 00 00 00 C0 00 00 00 ············À···
0020 00 00 00 46 4C 00 00 00-01 14 02 00 00 00 00 00 ···FL···········
0030 C0 00 00 00 00 00 00 46-E3 40 A0 00 20 00 00 00 À······Fã@ · ···
0040 4C 59 F8 26 49 A2 DB 01-02 BD F5 8E 2E A3 DB 01 LYø&I¢Û··½õ·.£Û·
0050 4E AA 36 A1 4C 9E DB 01-40 BC 38 00 0E 00 00 00 Nª6¡L·Û·@¼8·····
0060 01 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```