Storyline

Jasmine owns a famous New York coffee shop Coffely which is famous city-wide for its unique taste. Only Jasmine keeps the original copy of the recipe, and she only keeps it on her work laptop. Last week, James from the IT department was consulted to fix Jasmine's laptop. But it is suspected he may have copied the secret recipes from Jasmine's machine and is keeping them on his machine.Image showing a Laptop with a magnifying glass

His machine has been confiscated and examined, but no traces could be found. The security department has pulled some important registry artifacts from his device and has tasked you to examine these artifacts and determine the presence of secret files on his machine.

Registry Recap

Windows Registry is like a database that contains a lot of juicy information about the system, user, user activities, processes executed, the files accessed or deleted, etc.Image showing Registry icon

Following Registry Hives have been pulled from the suspect Host and placed in the C:\Users\Administrator\Desktop\Artifacts folder. All required tools are also placed on the path. C:\Users\Administrator\Desktop\EZ Tools.

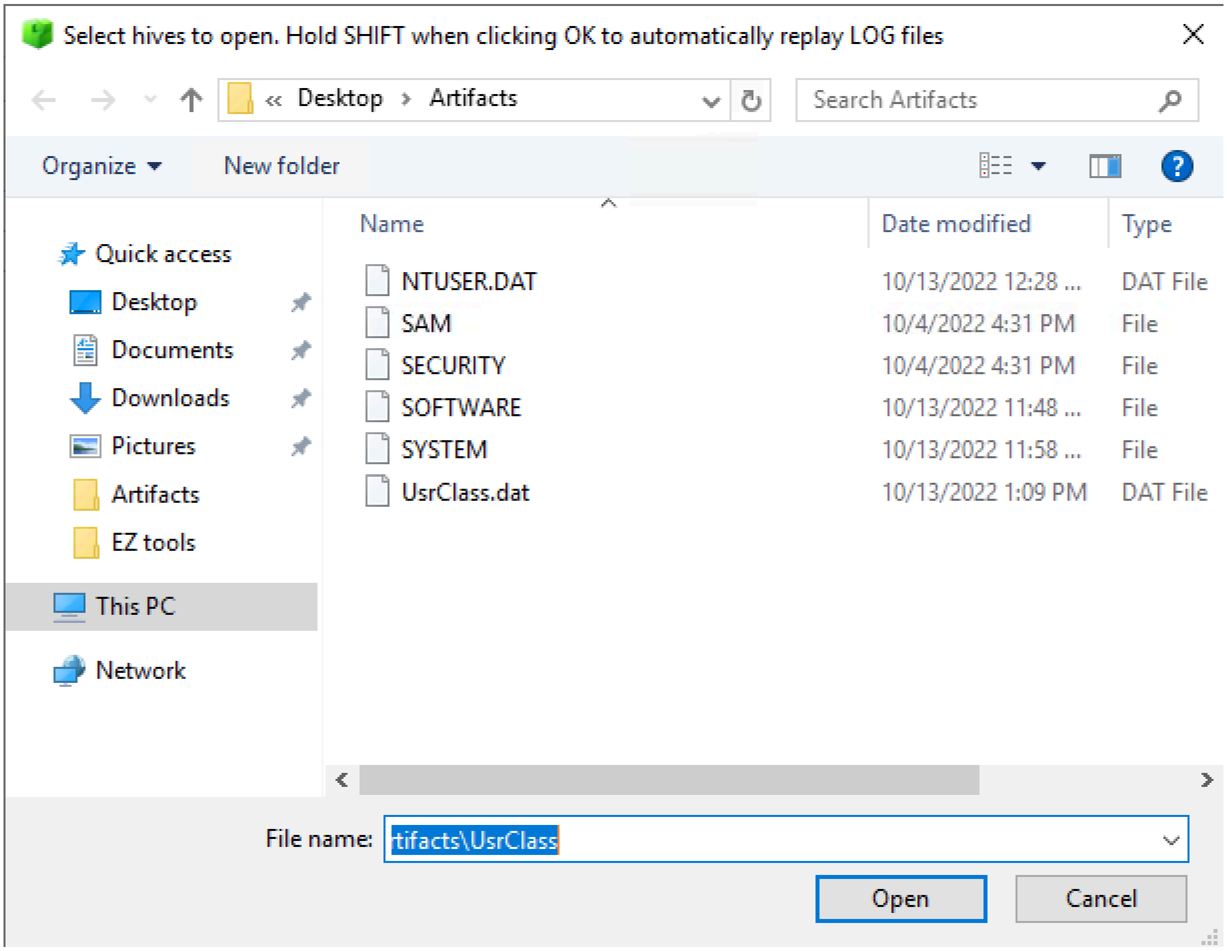
Your challenge is to examine the registry hives using the tools provided, observe the user's activities and answer the questions.

Registry Hives

SYSTEM
SECURITY
SOFTWARE
SAM
NTUSER.DAT
UsrClass.dat
Note: The Download Task Files button has a cheat sheet, which can be used as a reference to answer the questions.

What is the computer name of the machine found in the registry?

First we will load the hives into Registry Explorer.



Select hives to open. Hold SHIFT when clicking OK to automatically replay LOG files

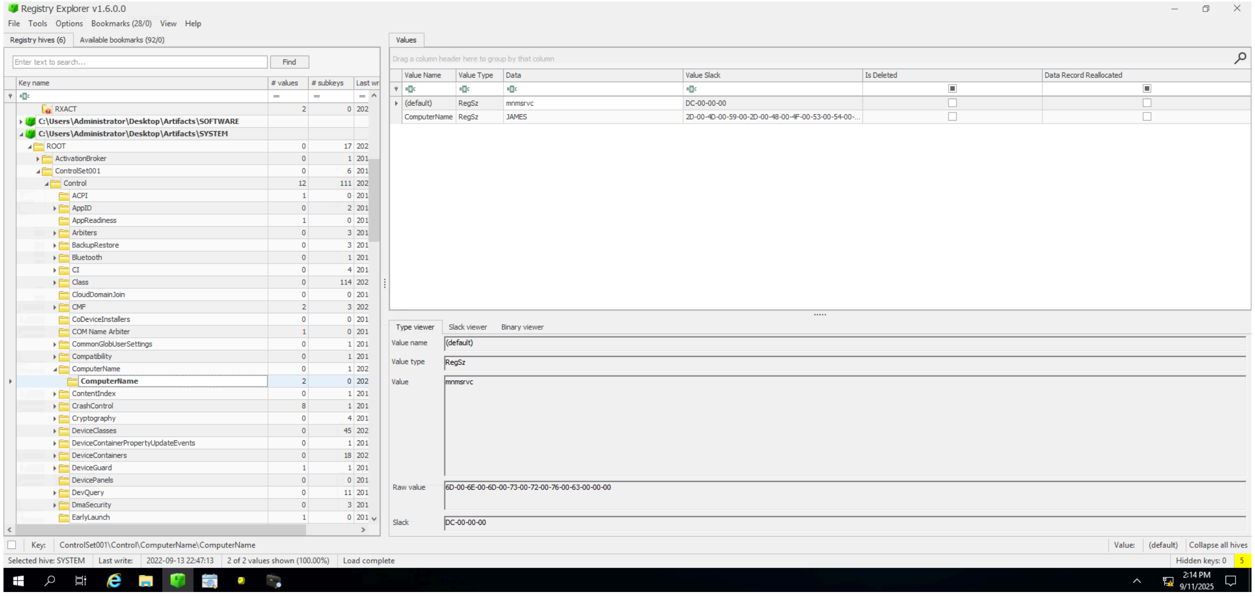
« Desktop › Artifacts

Name	Date modified	Type
NTUSER.DAT	10/13/2022 12:28 ...	DAT File
SAM	10/4/2022 4:31 PM	File
SECURITY	10/4/2022 4:31 PM	File
SOFTWARE	10/13/2022 11:48 ...	File
SYSTEM	10/13/2022 11:58 ...	File
UsrClass.dat	10/13/2022 1:09 PM	DAT File

File name: tifacts\UsrClass

We can then search into SYSTEM\CurrentControlSet\Control\ComputerName \ComputerName to find the computer name.

From this we can see the computer name is: **James**


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (28/0) View Help
Registry hives (6) Available bookmarks (92/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column
Type viewer Slack viewer Binary viewer
Collapse all hives

Key name	# values	# subkeys	Last wr
RXACT	2	0	202
C:\Users\Administrator\Desktop\Artifacts\SOFTWARE			
C:\Users\Administrator\Desktop\Artifacts\SYSTEM			
ROOT	0	17	202
ActivationBroker	0	1	201
ControlSet001	0	6	201
Control	12	111	202
ACPI	1	0	201
AppID	0	2	201
AppReadiness	1	0	201
Arbiters	0	3	201
BackupRestore	0	3	201
Bluetooth	0	1	201
CI	0	4	201
Class	0	114	202
CloudDomainJoin	0	0	201
CMF	2	3	202
CoDeviceInstallers	0	0	201
COM Name Arbiter	1	0	201
CommonGlobUserSettings	0	1	201
Compatibility	0	1	201
ComputerName	0	1	202
ComputerName	2	0	202
ContentIndex	0	1	201
CrashControl	8	1	201
Cryptography	0	4	201
DeviceClasses	0	45	202
DeviceContainerPropertyUpdateEvents	0	1	201
DeviceContainers	0	18	202
DeviceGuard	1	1	201
DevicePanels	0	0	201
DevQuery	0	11	201
DmaSecurity	0	3	201
EarlyLaunch	1	0	201

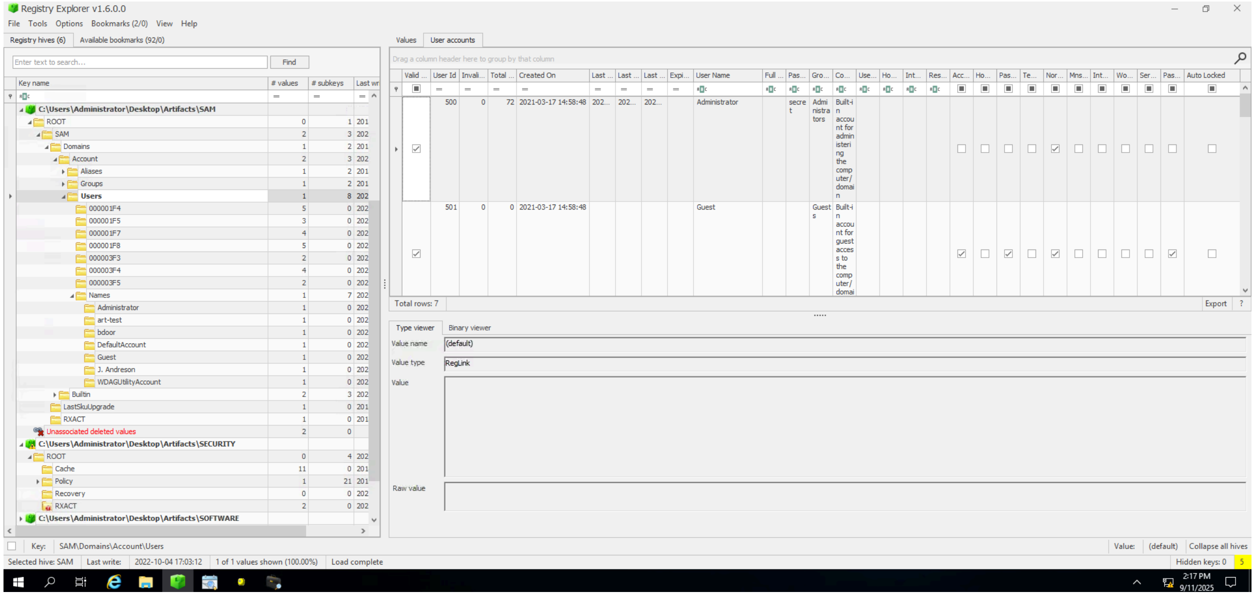
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
(default)	RegSz	mnmsrvc	DC-00-00-00	☐	☐
ComputerName	RegSz	JAMES	2D-00-4D-00-59-00-2D-00-48-00-4F-00-53-00-54-00-...	☐	☐

Value name: (default)
Value type: RegSz
Value: mnmsrvc
Raw value: 6D-00-6E-00-6D-00-73-00-72-00-76-00-63-00-00-00
Slack: DC-00-00-00

Key: ControlSet001\Control\ComputerName\ComputerName
Value: (default)
Selected hive: SYSTEM | Last write: 2022-09-13 22:47:13 | 2 of 2 values shown (100.00%) | Load complete
Hidden keys: 0
2:14 PM 9/11/2025

When was the Administrator account created on this machine? (Format: yyyy-mm-dd hh:mm:ss)

Staying in registry explorer, but this time searching in SAM\Domains\Account\Users, when looking at the Administrator account we can see it was created on 2021-03-17 14:58:48


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (2/0) View Help
Registry hives (6) Available bookmarks (92/0)
Enter text to search...
Find
Values User accounts
Drag a column header here to group by that column
Export ?
Type viewer Binary viewer
Collapse all hives

Key name	# values	# subkeys	Last wr
C:\Users\Administrator\Desktop\Artifacts\SAM			
ROOT	0	1	201
SAM	2	3	202
Domains	1	2	201
Account	2	3	202
Aliases	1	2	201
Groups	1	2	201
Users	1	8	202
000001F4	5	0	202
000001F5	3	0	202
000001F7	4	0	202
000001F8	5	0	202
000003F3	2	0	202
000003F4	4	0	202
000003F5	2	0	202
Names	1	7	202
Administrator	1	0	202
art-test	1	0	202
bdoor	1	0	202
DefaultAccount	1	0	202
Guest	1	0	202
J. Andreson	1	0	202
WDAGUtilityAccount	1	0	202
Builtin	2	3	202
LastSkuUpgrade	1	0	201
RXACT	1	0	201
Unassociated deleted values	2	0	
C:\Users\Administrator\Desktop\Artifacts\SECURITY			
ROOT	0	4	202
Cache	11	0	201
Policy	1	21	201
Recovery	0	0	202
RXACT	2	0	202
C:\Users\Administrator\Desktop\Artifacts\SOFTWARE			

Valid ...	User Id	Invali...	Total ...	Created On	Last ...	Last ...	Last ...	Expi...	User Name	Full ...	Pas...	Gro...	Co...	Use...	Ho...	Int...	Res...	Acc...	Ho...	Pas...	Te...	Nor...	Mns...	Int...	Wo...	Ser...	Pas...	Auto Locked
☑	500	0	72	2021-03-17 14:58:48	202...	202...	202...		Administrator		secret	Administrators	Built-in account for administering the computer/domain					☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐
☑	501	0	0	2021-03-17 14:58:48					Guest			Guests	Built-in account for guest access to the computer/domai					☑	☐	☑	☐	☑	☐	☐	☐	☐	☑	☐

Total rows: 7

Value name: (default)
Value type: RegLink
Value:
Raw value:

Key: SAM\Domains\Account\Users
Value: (default)
Selected hive: SAM | Last write: 2022-10-04 17:03:12 | 1 of 1 values shown (100.00%) | Load complete
Hidden keys: 0
2:17 PM 9/11/2025

What is the RID associated with the Administrator account?

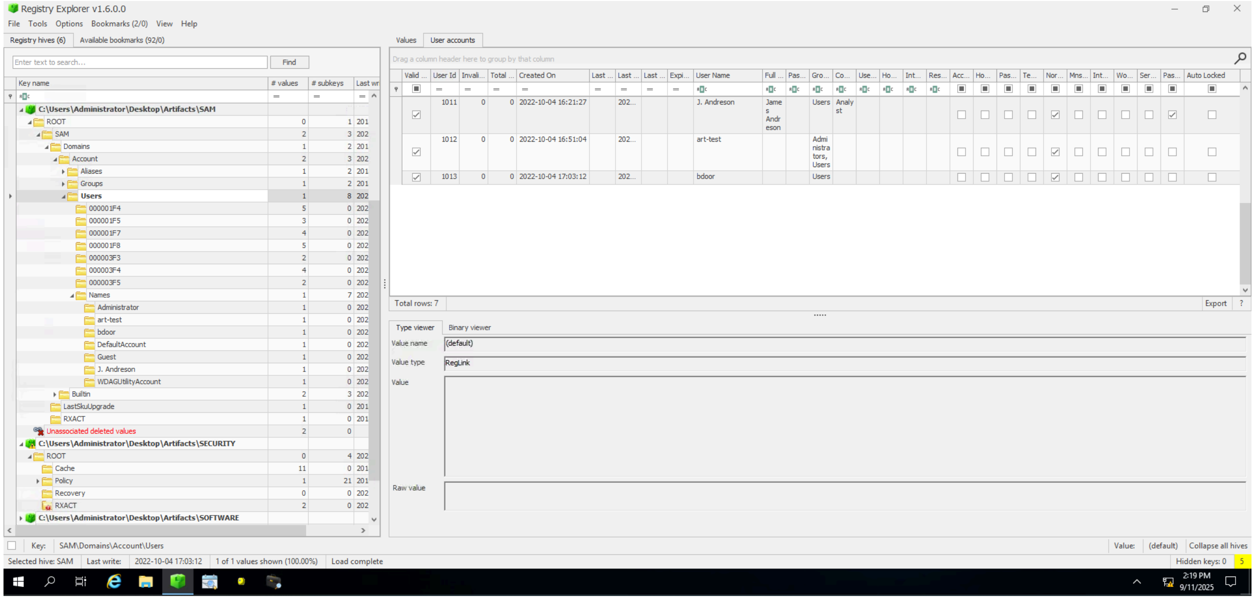
Using the same screenshot from above, we can see that the RID is 500.

How many user accounts were observed on this machine?

Staying in the same view, and looking at the total rows shown above, we can see that there are 7 user accounts on the machine.

There seems to be a suspicious account created as a backdoor with RID 1013. What is the account name?

Now scrolling down on the same view, and looking at RID 1013, we can see that the account ‘bdoor’ was created.



Registry Explorer v1.6.0.0

File Tools Options Bookmarks (2/0) View Help

Registry hives (6) | Available bookmarks (92/0)

```
Key name                                              # values  # subkeys  Last wr
C:\Users\Administrator\Desktop\Artifacts\SAM
  ROOT                                                       0          1  201
    SAM                                                      2          3  202
      Domains                                                1          2  201
        Account                                              2          3  202
          Aliases                                            1          2  201
          Groups                                             1          2  201
          Users                                              1          8  202
            000001F4                                         5          0  202
            000001F5                                         3          0  202
            000001F7                                         4          0  202
            000001F8                                         5          0  202
            000003F3                                         2          0  202
            000003F4                                         4          0  202
            000003F5                                         2          0  202
            Names                                            1          7  202
              Administrator                                  1          0  202
              art-test                                       1          0  202
              bdoor                                          1          0  202
              DefaultAccount                                 1          0  202
              Guest                                          1          0  202
              J. Andreson                                    1          0  202
              WDAGUtilityAccount                             1          0  202
        Builtin                                              2          3  202
      LastSkuUpgrade                                         1          0  201
      RXACT                                                  1          0  201
  Unassociated deleted values                                2          0
C:\Users\Administrator\Desktop\Artifacts\SECURITY
  ROOT                                                       0          4  202
    Cache                                                   11          0  201
    Policy                                                   1         21  201
    Recovery                                                 0          0  202
    RXACT                                                    2          0  202
C:\Users\Administrator\Desktop\Artifacts\SOFTWARE
```

Values | User accounts

Valid ...	User Id	Invali...	Total ...	Created On	Last ...	Last ...	Last ...	Expi...	User Name	Full ...	Pas...	Gro...	Co...	Use...	Ho...	Int...	Res...	Acc...	Ho...	Pas...	Te...	Nor...	Mns...	Int...	Wo...	Ser...	Pas...	Auto Locked
☑	1011	0	0	2022-10-04 16:21:27		202...			J. Andreson	James Andreson		Users	Analyst					□	□	□	□	☑	□	□	□	□	☑	□
☑	1012	0	0	2022-10-04 16:51:04		202...			art-test			Administrators, Users						□	□	□	□	☑	□	□	□	□	□	□
☑	1013	0	0	2022-10-04 17:03:12		202...			bdoor			Users						□	□	□	□	☑	□	□	□	□	□	□

Total rows: 7

Type viewer | Binary viewer

Value name: (default)

Value type: RegLink

Value:

Raw value:

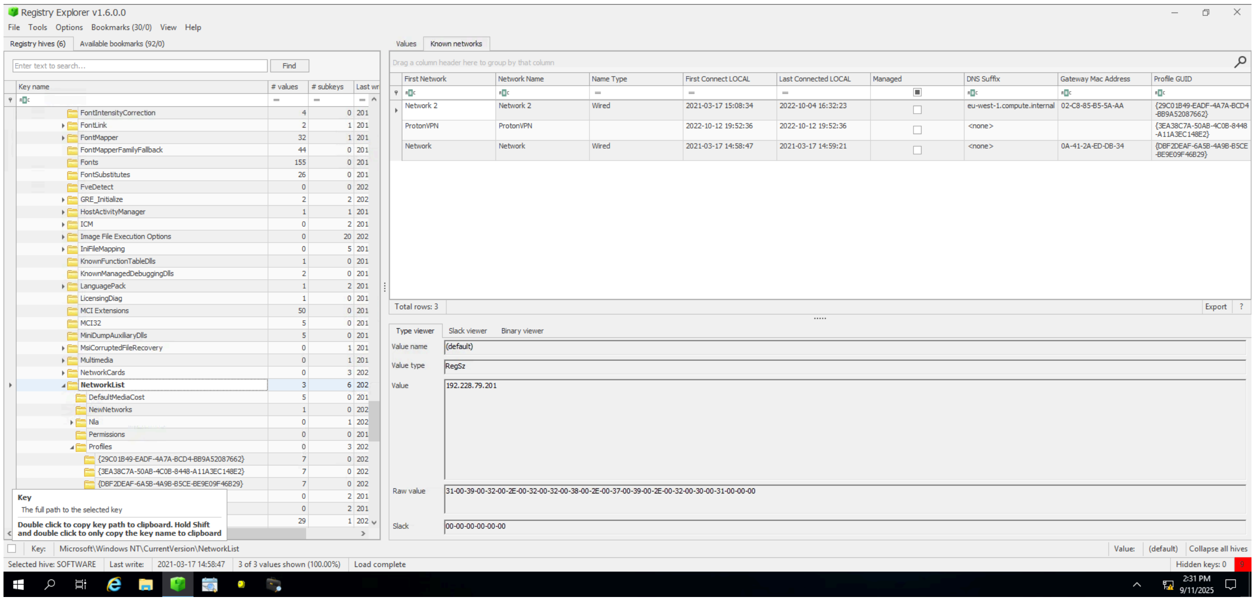
Key: SAM\Domains\Account\Users

Selected hive: SAM | Last write: 2022-10-04 17:03:12 | 1 of 1 values shown (100.00%) | Load complete

Value: (default) | Collapse all hives | Hidden keys: 0

What is the VPN connection this host connected to?

After doing some research for this one, I came up with the following path to find the VPN connection: \SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList. Once in here, I can see that the host is connected to ProtonVPN.



Registry Explorer v1.6.0.0

File Tools Options Bookmarks (30/0) View Help

Registry hives (6) | Available bookmarks (92/0)

```
Key name                                              # values  # subkeys  Last wr
      FontIntensityCorrection                                4          0  201
      FontLink                                               2          1  201
      FontMapper                                            32          1  201
      FontMapperFamilyFallback                              44          0  201
      Fonts                                                155          0  201
      FontSubstitutes                                       26          0  201
      FveDetect                                              0          0  202
      GRE_Initialize                                         2          2  202
      HostActivityManager                                    1          1  201
      ICM                                                    0          2  201
      Image File Execution Options                           0         20  202
      IniFileMapping                                         0          5  201
      KnownFunctionTableDlls                                 1          0  201
      KnownManagedDebuggingDlls                              2          0  201
      LanguagePack                                           1          2  201
      LicensingDiag                                          1          0  201
      MCI Extensions                                        50          0  201
      MCI32                                                  5          0  201
      MiniDumpAuxiliaryDlls                                  5          0  201
      MsiCorruptedFileRecovery                               0          1  201
      Multimedia                                             0          1  201
      NetworkCards                                           0          3  202
      NetworkList                                            3          6  202
        DefaultMediaCost                                     5          0  201
        NewNetworks                                          1          0  202
        Nla                                                  0          1  202
        Permissions                                          0          0  201
        Profiles                                             0          3  202
          {29C01B49-EADF-4A7A-BCD4-BB9A52087662}             7          0  202
          {3EA38C7A-50AB-4C0B-8448-A11A3EC148E2}             7          0  202
          {DBF2DEAF-6A5B-4A9B-B5CE-BE9E09F46B29}             7          0  202
                                                             0          2  201
                                                             0          2  201
                                                            29          1  202
```

Key
The full path to the selected key
Double click to copy key path to clipboard. Hold Shift and double click to only copy the key name to clipboard

Values | Known networks

First Network	Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL	Managed	DNS Suffix	Gateway Mac Address	Profile GUID
Network 2	Network 2	Wired	2021-03-17 15:08:34	2022-10-04 16:32:23	□	eu-west-1.compute.internal	02-C8-85-B5-5A-AA	{29C01B49-EADF-4A7A-BCD4-BB9A52087662}
ProtonVPN	ProtonVPN		2022-10-12 19:52:36	2022-10-12 19:52:36	□	<none>		{3EA38C7A-50AB-4C0B-8448-A11A3EC148E2}
Network	Network	Wired	2021-03-17 14:58:47	2021-03-17 14:59:21	□	<none>	0A-41-2A-ED-DB-34	{DBF2DEAF-6A5B-4A9B-B5CE-BE9E09F46B29}

Total rows: 3

Type viewer | Slack viewer | Binary viewer

Value name: (default)

Value type: RegSz

Value: 192.228.79.201

Raw value: 31-00-39-00-32-00-2E-00-32-00-32-00-38-00-2E-00-37-00-39-00-2E-00-32-00-30-00-31-00-00-00

Slack: 00-00-00-00-00-00

Key: Microsoft\Windows NT\CurrentVersion\NetworkList

Selected hive: SOFTWARE | Last write: 2021-03-17 14:58:47 | 3 of 3 values shown (100.00%) | Load complete

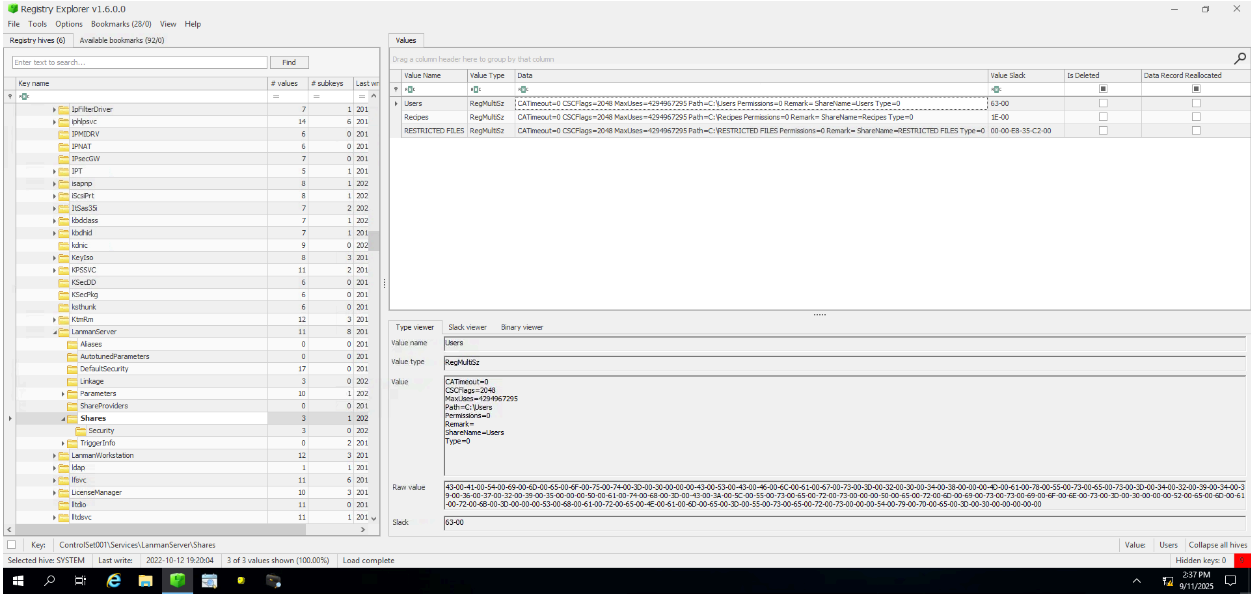
Value: (default) | Collapse all hives | Hidden keys: 0

When was the first VPN connection observed? (Format: YYYY-MM-DD HH:MM:SS)

Looking right next to ProtonVPN under ‘First Connect LOCAL’, we can see that the first connection was observed at 2022-10-12 19:52:36.

There were three shared folders observed on his machine. What is the path of the third share?

Doing a little bit of research on where to locate this in registry explorer, I ended up searching in the following path to find the answer:
SYSTEM\CurrentControlSet\Services\LanmanServer\Shares
There, the third folder is shown under the path: C:\RESTRICTED FILES


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (28/0) View Help
Registry hives (6) Available bookmarks (92/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column
Type viewer
Slack viewer
Binary viewer
Collapse all hives
Hidden keys: 0

Key name	# values	# subkeys	Last wr
IpFilterDriver	7	1	201
iphlpsvc	14	6	201
IPMIDRV	6	0	201
IPNAT	6	0	201
IPsecGW	7	0	201
IPT	5	1	201
isapnp	8	1	202
iScsiPrt	8	1	202
ItSas35i	7	2	202
kbdclass	7	1	202
kbdhid	7	1	201
kdnic	9	0	202
KeyIso	8	3	201
KPSSVC	11	2	201
KSecDD	6	0	201
KSecPkg	6	0	201
ksthunk	6	0	201
KtmRm	12	3	201
LanmanServer	11	8	201
Aliases	0	0	201
AutotunedParameters	0	0	201
DefaultSecurity	17	0	201
Linkage	3	0	202
Parameters	10	1	202
ShareProviders	0	0	201
Shares	3	1	202
Security	3	0	202
TriggerInfo	0	2	201
LanmanWorkstation	12	3	201
ldap	1	1	201
lfsvc	11	6	201
LicenseManager	10	3	201
lltdio	11	0	201
lltdsvc	11	1	201

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
Users	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUses=4294967295 Path=C:\Users Permissions=0 Remark= ShareName=Users Type=0	63-00	□	□
Recipes	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUses=4294967295 Path=C:\Recipes Permissions=0 Remark= ShareName=Recipes Type=0	1E-00	□	□
RESTRICTED FILES	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUses=4294967295 Path=C:\RESTRICTED FILES Permissions=0 Remark= ShareName=RESTRICTED FILES Type=0	00-00-E8-35-C2-00	□	□

Value name: Users

Value type: RegMultiSz

Value:

```
CATimeout=0
CSCFlags=2048
MaxUses=4294967295
Path=C:\Users
Permissions=0
Remark=
ShareName=Users
Type=0
```

Raw value:

```
43-00-41-00-54-00-69-00-6D-00-65-00-6F-00-75-00-74-00-3D-00-30-00-00-00-43-00-53-00-43-00-46-00-6C-00-61-00-67-00-73-00-3D-00-32-00-30-00-34-00-38-00-00-00-4D-00-61-00-78-00-55-00-73-00-65-00-73-00-3D-00-34-00-32-00-39-00-34-00-3
9-00-36-00-37-00-32-00-39-00-35-00-00-00-50-00-61-00-74-00-68-00-3D-00-43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-00-00-50-00-65-00-72-00-6D-00-69-00-73-00-73-00-69-00-6F-00-6E-00-73-00-3D-00-30-00-00-00-52-00-65-00-6D-00-61
-00-72-00-6B-00-3D-00-00-00-53-00-68-00-61-00-72-00-65-00-4E-00-61-00-6D-00-65-00-3D-00-55-00-73-00-65-00-72-00-73-00-00-00-54-00-79-00-70-00-65-00-3D-00-30-00-00-00-00-00
```

Slack: 63-00

Key: ControlSet001\Services\LanmanServer\Shares

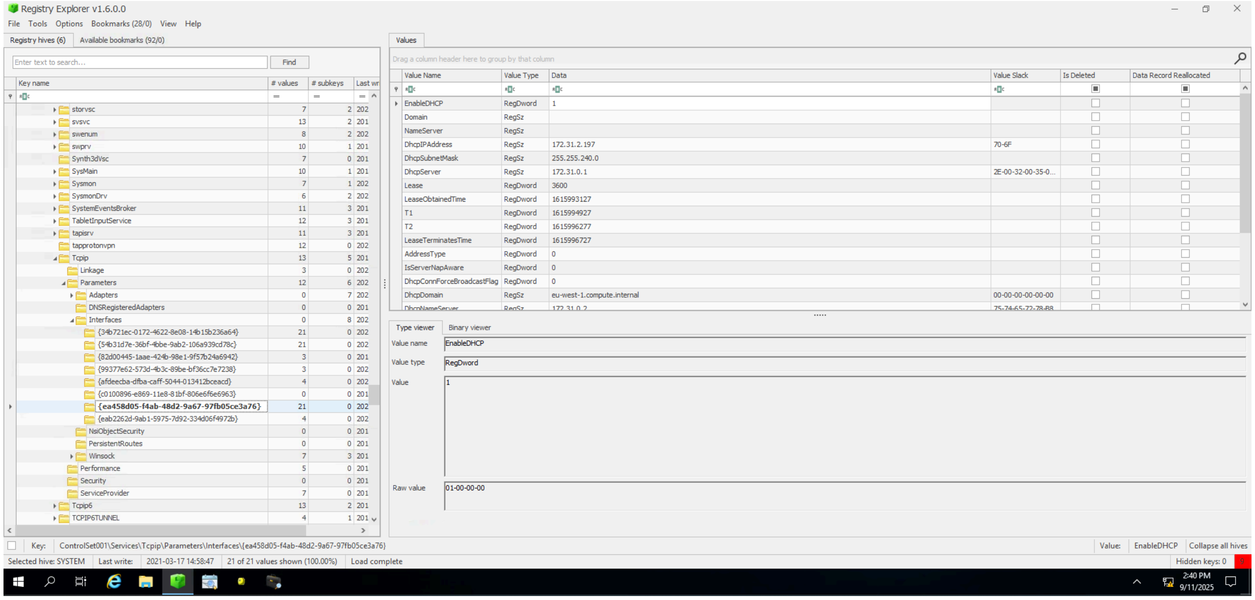
Value: Users

Selected hive: SYSTEM | Last write: 2022-10-12 19:20:04 | 3 of 3 values shown (100.00%) | Load complete

2:37 PM
9/11/2025

What is the last DHCP IP assigned to this host?

Looking into the path SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces, we find the DHCP IP assigned to the host is 172.31.2.197.



Registry Explorer v1.6.0.0

Registry hives (6) | Available bookmarks (92/0)

Key name	# values	# subkeys	Last wr
storvsc	7	2	202
svsvc	13	2	201
swenum	8	2	202
swprv	10	1	201
Synth3dVsc	7	0	201
SysMain	10	1	201
Sysmon	7	1	202
SysmonDrv	6	2	202
SystemEventsBroker	11	3	201
TabletInputService	12	3	201
tapisrv	11	3	201
tapprotonvpn	12	0	202
Tcpip	13	5	201
Linkage	3	0	202
Parameters	12	6	202
Adapters	0	7	202
DNSRegisteredAdapters	0	0	201
Interfaces	0	8	202
{34b721ec-0172-4622-8e08-14b15b236a64}	21	0	202
{54b31d7e-36bf-4bbe-9ab2-106a939cd78c}	21	0	202
{82d00445-1aae-424b-98e1-9f57b24a6942}	3	0	201
{99377e62-573d-4b3c-89be-bf36cc7e7238}	3	0	202
{afdeecba-dfba-caff-5044-013412bceacd}	4	0	202
{c0100896-e869-11e8-81bf-806e6f6e6963}	0	0	201
{ea458d05-f4ab-48d2-9a67-97fb05ce3a76}	21	0	202
{eab2262d-9ab1-5975-7d92-334d06f4972b}	4	0	202
NsiObjectSecurity	0	0	201
PersistentRoutes	0	0	201
Winsock	7	3	201
Performance	5	0	201
Security	0	0	201
ServiceProvider	7	0	201
Tcpip6	13	2	201
TCPIP6TUNNEL	4	1	201

Values

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	1		□	□
Domain	RegSz			□	□
NameServer	RegSz			□	□
DhcpIPAddress	RegSz	172.31.2.197	70-6F	□	□
DhcpSubnetMask	RegSz	255.255.240.0		□	□
DhcpServer	RegSz	172.31.0.1	2E-00-32-00-35-0...	□	□
Lease	RegDword	3600		□	□
LeaseObtainedTime	RegDword	1615993127		□	□
T1	RegDword	1615994927		□	□
T2	RegDword	1615996277		□	□
LeaseTerminatesTime	RegDword	1615996727		□	□
AddressType	RegDword	0		□	□
IsServerNapAware	RegDword	0		□	□
DhcpConnForceBroadcastFlag	RegDword	0		□	□
DhcpDomain	RegSz	eu-west-1.compute.internal	00-00-00-00-00-00	□	□
DhcpNameServer	RegSz	172.31.0.2	75-74-65-72-78-88	□	□

Type viewer | Binary viewer

Value name: EnableDHCP

Value type: RegDword

Value: 1

Raw value: 01-00-00-00

Key: ControlSet001\Services\Tcpip\Parameters\Interfaces\{ea458d05-f4ab-48d2-9a67-97fb05ce3a76}

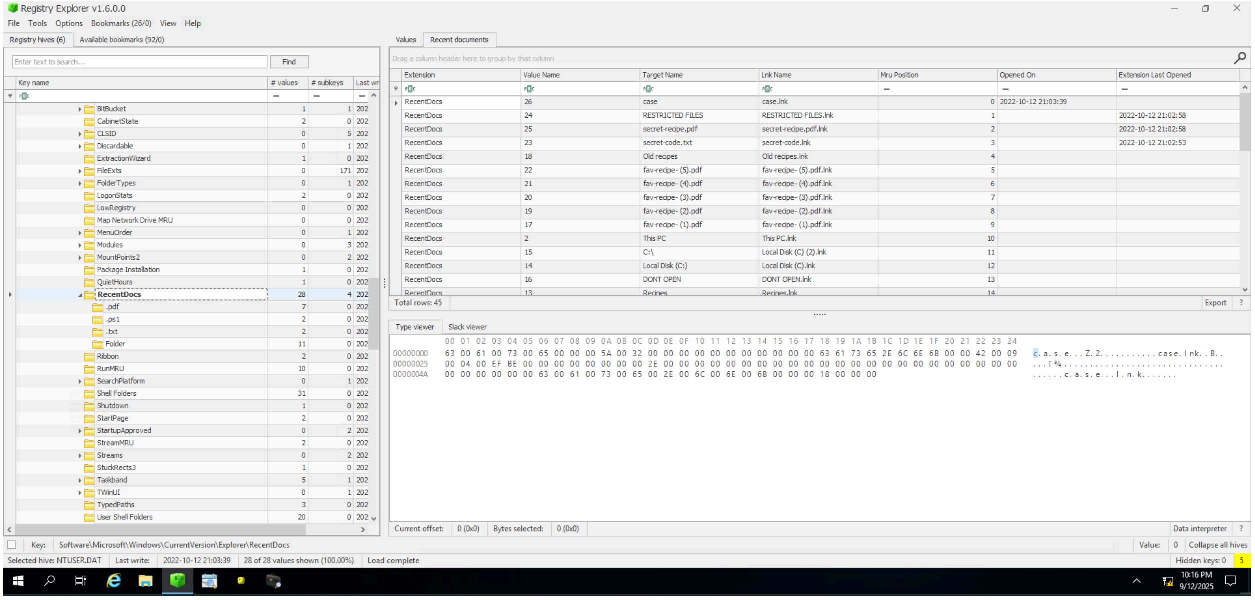
Value: EnableDHCP

Selected hive: SYSTEM | Last write: 2021-03-17 14:58:47 | 21 of 21 values shown (100.00%) | Load complete | Hidden keys: 0

File Tools Options Bookmarks (28/0) View Help
Enter text to search...
Find
Drag a column header here to group by that column
Collapse all hives
2:40 PM
9/11/2025

The suspect seems to have accessed a file containing the secret coffee recipe. What is the name of the file?

Looking under NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs, we can see that the file is secret-recipe.pdf.



Registry Explorer v1.6.0.0

Registry hives (6) | Available bookmarks (92/0)

Key name	# values	# subkeys	Last wr
BitBucket	1	1	202
CabinetState	2	0	202
CLSID	0	5	202
Discardable	0	1	202
ExtractionWizard	1	0	202
FileExts	0	171	202
FolderTypes	0	1	202
LogonStats	2	0	202
LowRegistry	0	0	202
Map Network Drive MRU	0	0	202
MenuOrder	0	1	202
Modules	0	3	202
MountPoints2	0	2	202
Package Installation	1	0	202
QuietHours	1	0	202
RecentDocs	28	4	202
.pdf	7	0	202
.ps1	2	0	202
.txt	2	0	202
Folder	11	0	202
Ribbon	2	0	202
RunMRU	10	0	202
SearchPlatform	0	1	202
Shell Folders	31	0	202
Shutdown	1	0	202
StartPage	2	0	202
StartupApproved	0	2	202
StreamMRU	2	0	202
Streams	0	2	202
StuckRects3	1	0	202
Taskband	5	1	202
TWinUI	0	1	202
TypedPaths	3	0	202
User Shell Folders	20	0	202

Values | Recent documents

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	26	case	case.lnk	0	2022-10-12 21:03:39	
RecentDocs	24	RESTRICTED FILES	RESTRICTED FILES.lnk	1		2022-10-12 21:02:58
RecentDocs	25	secret-recipe.pdf	secret-recipe.pdf.lnk	2		2022-10-12 21:02:58
RecentDocs	23	secret-code.txt	secret-code.lnk	3		2022-10-12 21:02:53
RecentDocs	18	Old recipes	Old recipes.lnk	4		
RecentDocs	22	fav-recipe- (5).pdf	fav-recipe- (5).pdf.lnk	5		
RecentDocs	21	fav-recipe- (4).pdf	fav-recipe- (4).pdf.lnk	6		
RecentDocs	20	fav-recipe- (3).pdf	fav-recipe- (3).pdf.lnk	7		
RecentDocs	19	fav-recipe- (2).pdf	fav-recipe- (2).pdf.lnk	8		
RecentDocs	17	fav-recipe- (1).pdf	fav-recipe- (1).pdf.lnk	9		
RecentDocs	2	This PC	This PC.lnk	10		
RecentDocs	15	C:\	Local Disk (C) (2).lnk	11		
RecentDocs	14	Local Disk (C:)	Local Disk (C).lnk	12		
RecentDocs	16	DONT OPEN	DONT OPEN.lnk	13		
RecentDocs	13	Recipes	Recipes.lnk	14		

Total rows: 45

Type viewer | Slack viewer

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  63 00 61 00 73 00 65 00 00 00 5A 00 32 00 00 00 00 00 00 00 00 00 00 63 61 73 65 2E 6C 6E 6B 00 00 42 00 09   c.a.s.e...Z.2..........case.lnk..B..
00000025  00 04 00 EF BE 00 00 00 00 00 00 00 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ...ï¾................................
0000004A  00 00 00 00 00 00 63 00 61 00 73 00 65 00 2E 00 6C 00 6E 00 6B 00 00 00 18 00 00 00                             ......c.a.s.e...l.n.k.......
```

Current offset: 0 (0x0) | Bytes selected: 0 (0x0)

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

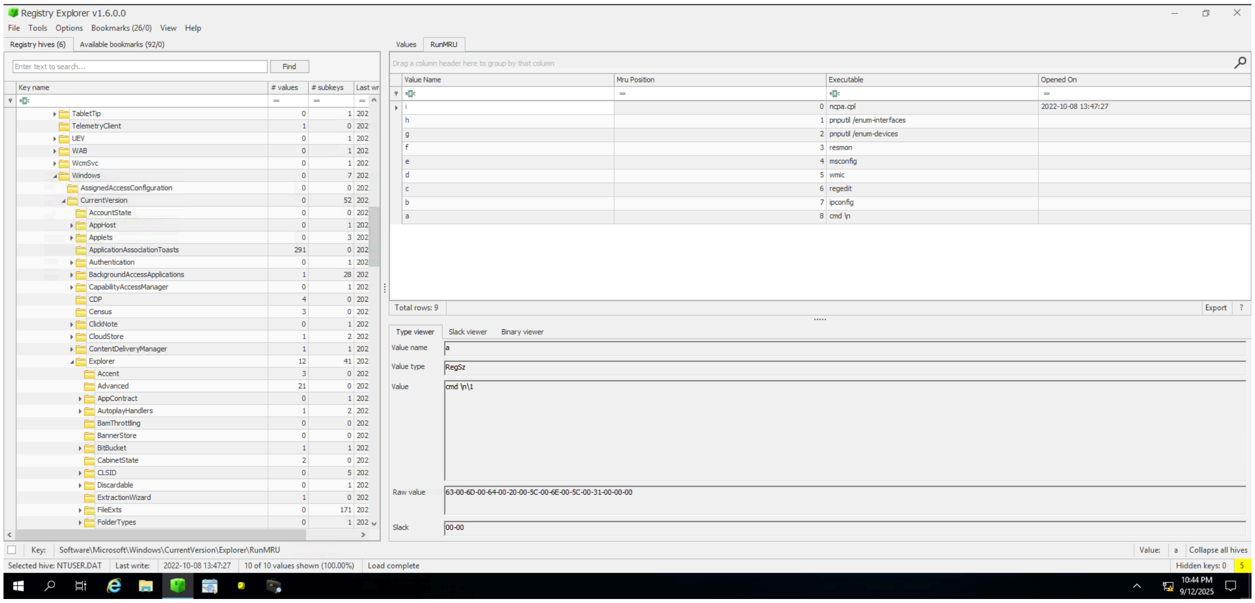
Value: 0

Selected hive: NTUSER.DAT | Last write: 2022-10-12 21:03:39 | 28 of 28 values shown (100.00%) | Load complete | Hidden keys: 0

File Tools Options Bookmarks (26/0) View Help
Enter text to search...
Find
Drag a column header here to group by that column
Export
Data interpreter
Collapse all hives
5
10:16 PM
9/12/2025

The suspect executed multiple commands using the Run window. What command was used to enumerate the network interfaces?

After doing some digging around in Registry Explorer, I was able to locate ‘pnputil/enum-interfaces’ under NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.


Registry Explorer v1.6.0.0
File
Tools
Options
Bookmarks (26/0)
View
Help
Registry hives (6)
Available bookmarks (92/0)
Enter text to search...
Find
Values
RunMRU
Drag a column header here to group by that column

Key name	# values	# subkeys	Last wr
TabletTip	0	1	202
TelemetryClient	1	0	202
UEV	0	1	202
WAB	0	1	202
WcmSvc	0	1	202
Windows	0	7	202
AssignedAccessConfiguration	0	0	202
CurrentVersion	0	52	202
AccountState	0	0	202
AppHost	0	1	202
Applets	0	3	202
ApplicationAssociationToasts	291	0	202
Authentication	0	1	202
BackgroundAccessApplications	1	28	202
CapabilityAccessManager	0	1	202
CDP	4	0	202
Census	3	0	202
ClickNote	0	1	202
CloudStore	1	2	202
ContentDeliveryManager	1	1	202
Explorer	12	41	202
Accent	3	0	202
Advanced	21	0	202
AppContract	0	1	202
AutoplayHandlers	1	2	202
BamThrottling	0	0	202
BannerStore	0	0	202
BitBucket	1	1	202
CabinetState	2	0	202
CLSID	0	5	202
Discardable	0	1	202
ExtractionWizard	1	0	202
FileExts	0	171	202
FolderTypes	0	1	202

Value Name	Mru Position	Executable	Opened On
i	0	ncpa.cpl	2022-10-08 13:47:27
h	1	pnputil /enum-interfaces	
g	2	pnputil /enum-devices	
f	3	resmon	
e	4	msconfig	
d	5	wmic	
c	6	regedit	
b	7	ipconfig	
a	8	cmd \n	

Total rows: 9

Value name: a

Value type: RegSz

Value: cmd \n\1

Raw value: 63-00-6D-00-64-00-20-00-5C-00-6E-00-5C-00-31-00-00-00

Slack: 00-00

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Value: a

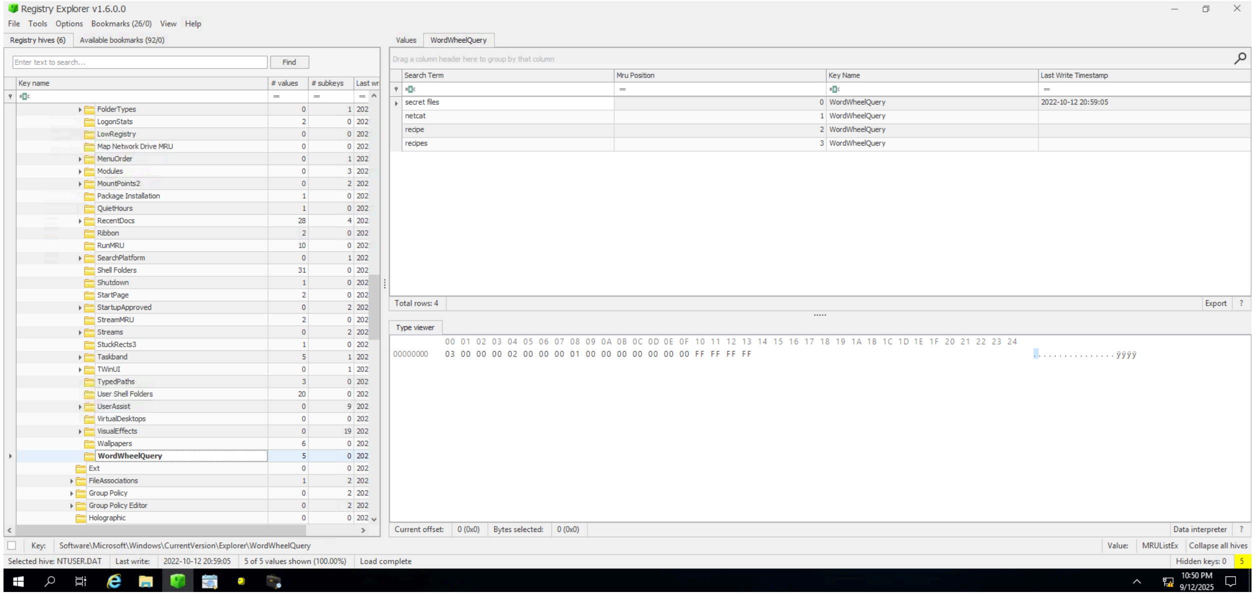
Selected hive: NTUSER.DAT | Last write: 2022-10-08 13:47:27 | 10 of 10 values shown (100.00%) | Load complete

Hidden keys: 0 | 5

10:44 PM
9/12/2025

The user searched for a network utility tool to transfer files using the file explorer. What is the name of that tool?

I was able to locate that the user searched for ‘netcat’ by searching in the following path on registry explorer NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery.


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (26/0) View Help
Registry hives (6) Available bookmarks (92/0)
Enter text to search...
Find
Values WordWheelQuery
Drag a column header here to group by that column
Type viewer
Export
Data interpreter

Key name	# values	# subkeys	Last wr
FolderTypes	0	1	202
LogonStats	2	0	202
LowRegistry	0	0	202
Map Network Drive MRU	0	0	202
MenuOrder	0	1	202
Modules	0	3	202
MountPoints2	0	2	202
Package Installation	1	0	202
QuietHours	1	0	202
RecentDocs	28	4	202
Ribbon	2	0	202
RunMRU	10	0	202
SearchPlatform	0	1	202
Shell Folders	31	0	202
Shutdown	1	0	202
StartPage	2	0	202
StartupApproved	0	2	202
StreamMRU	2	0	202
Streams	0	2	202
StuckRects3	1	0	202
Taskband	5	1	202
TWinUI	0	1	202
TypedPaths	3	0	202
User Shell Folders	20	0	202
UserAssist	0	9	202
VirtualDesktops	0	0	202
VisualEffects	0	19	202
Wallpapers	6	0	202
WordWheelQuery	5	0	202
Ext	0	0	202
FileAssociations	1	2	202
Group Policy	0	2	202
Group Policy Editor	0	2	202
Holographic	0	0	202

Search Term	Mru Position	Key Name	Last Write Timestamp
secret files	0	WordWheelQuery	2022-10-12 20:59:05
netcat	1	WordWheelQuery	
recipe	2	WordWheelQuery	
recipes	3	WordWheelQuery	

Total rows: 4

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF                                                      ................ÿÿÿÿ
```

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

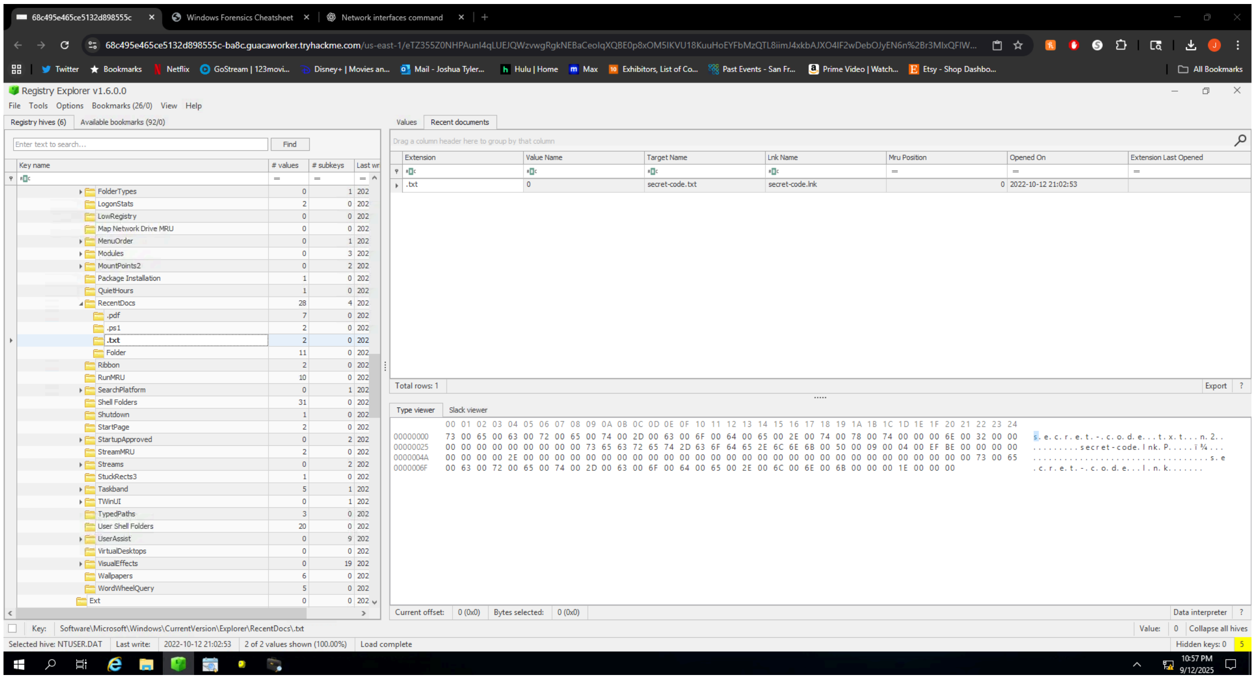
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery Value: MRUListEx Collapse all hives

Selected hive: NTUSER.DAT Last write: 2022-10-12 20:59:05 5 of 5 values shown (100.00%) Load complete Hidden keys: 0 5

10:50 PM 9/12/2025

What is the recent text file opened by the suspect?

I was able to locate that the user opened the file ‘secret-code.txt’ under the following path: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt


68c495e465ce5132d898555c
Windows Forensics Cheatsheet
Network interfaces command
68c495e465ce5132d898555c-ba8c.guacaworker.tryhackme.com/us-east-1/eTZ355Z0NHPAunl4qLUEJQWzvwgRgkNEBaCeolqXQBE0p8xOM5IKVU18KuuHoEYFbMzQTL8iimJ4xkbAJXO4lF2wDebOJyEN6n%2Br3MlxQFIW...
Twitter
Bookmarks
Netflix
GoStream | 123movi...
Disney+ | Movies an...
Mail - Joshua Tyler...
Hulu | Home
Max
Exhibitors, List of Co...
Past Events - San Fr...
Prime Video | Watch...
Etsy - Shop Dashbo...
All Bookmarks
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (26/0) View Help
Registry hives (6) Available bookmarks (92/0)
Enter text to search...
Find
Values Recent documents
Drag a column header here to group by that column
Type viewer Slack viewer
Export
Data interpreter

Key name	# values	# subkeys	Last wr
FolderTypes	0	1	202
LogonStats	2	0	202
LowRegistry	0	0	202
Map Network Drive MRU	0	0	202
MenuOrder	0	1	202
Modules	0	3	202
MountPoints2	0	2	202
Package Installation	1	0	202
QuietHours	1	0	202
RecentDocs	28	4	202
.pdf	7	0	202
.ps1	2	0	202
.txt	2	0	202
Folder	11	0	202
Ribbon	2	0	202
RunMRU	10	0	202
SearchPlatform	0	1	202
Shell Folders	31	0	202
Shutdown	1	0	202
StartPage	2	0	202
StartupApproved	0	2	202
StreamMRU	2	0	202
Streams	0	2	202
StuckRects3	1	0	202
Taskband	5	1	202
TWinUI	0	1	202
TypedPaths	3	0	202
User Shell Folders	20	0	202
UserAssist	0	9	202
VirtualDesktops	0	0	202
VisualEffects	0	19	202
Wallpapers	6	0	202
WordWheelQuery	5	0	202
Ext	0	0	202

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
.txt	0	secret-code.txt	secret-code.lnk	0	2022-10-12 21:02:53	

Total rows: 1

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  73 00 65 00 63 00 72 00 65 00 74 00 2D 00 63 00 6F 00 64 00 65 00 2E 00 74 00 78 00 74 00 00 00 6E 00 32 00 00  s.e.c.r.e.t.-.c.o.d.e...t.x.t...n.2..
00000025  00 00 00 00 00 00 00 00 00 73 65 63 72 65 74 2D 63 6F 64 65 2E 6C 6E 6B 00 50 00 09 00 04 00 EF BE 00 00 00 00  .........secret-code.lnk.P.....ï¾....
0000004A  00 00 00 00 2E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 00 65  ..................................s.e
0000006F  00 63 00 72 00 65 00 74 00 2D 00 63 00 6F 00 64 00 65 00 2E 00 6C 00 6E 00 6B 00 00 00 1E 00 00 00              .c.r.e.t.-.c.o.d.e...l.n.k.......
```

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

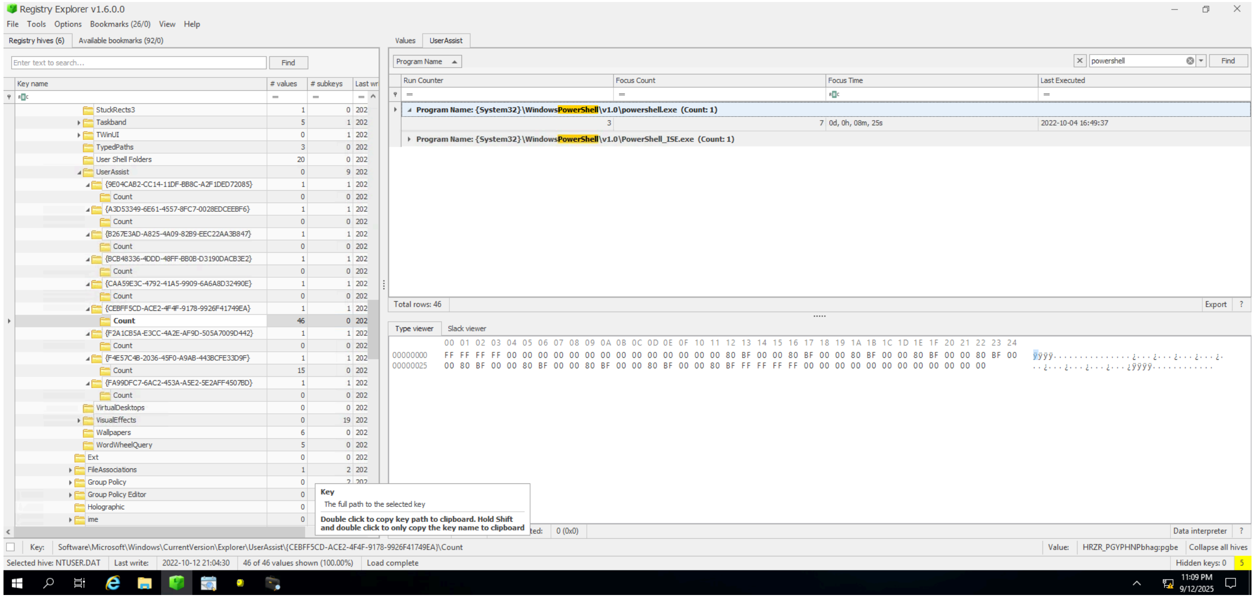
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt Value: 0 Collapse all hives

Selected hive: NTUSER.DAT Last write: 2022-10-12 21:02:53 2 of 2 values shown (100.00%) Load complete Hidden keys: 0 5

10:57 PM 9/12/2025

How many times was PowerShell executed on this host?

Going to NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count, and filtering the program name for 'powershell', we're able to see that it was ran 3 times.



Run Counter	Focus Count	Focus Time	Last Executed
Program Name: {System32}\WindowsPowerShell\v1.0\powershell.exe (Count: 1)			
3	7	0d, 0h, 08m, 25s	2022-10-04 16:49:37
Program Name: {System32}\WindowsPowerShell\v1.0\PowerShell_ISE.exe (Count: 1)			

Total rows: 46

```
         00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00
00000025 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
```

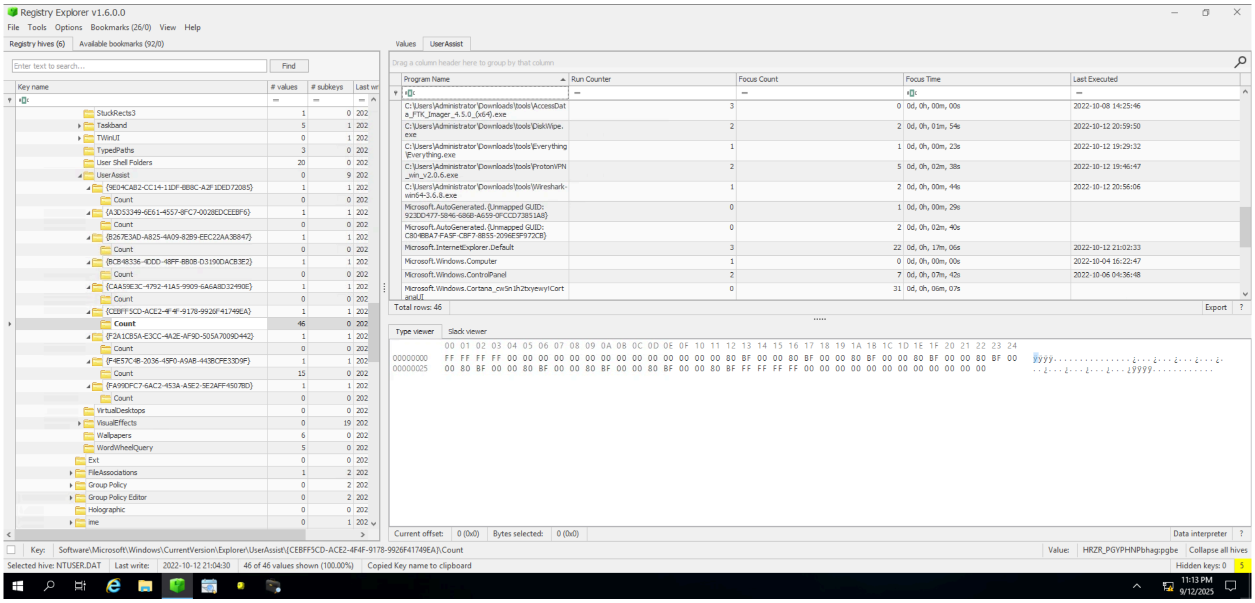
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

Value: HRZR_PGYPHNPbhag:pgbe

Selected hive: NTUSER.DAT Last write: 2022-10-12 21:04:30 46 of 46 values shown (100.00%) Load complete

The suspect also executed a network monitoring tool. What is the name of the tool?

Staying in the same path as the previous question, and taking some time to scroll through the program names, we see that the user executed Wireshark.



Program Name	Run Counter	Focus Count	Focus Time	Last Executed
C:\Users\Administrator\Downloads\tools\AccessData_FTK_Imager_4.5.0_(x64).exe	3	0	0d, 0h, 00m, 00s	2022-10-08 14:25:46
C:\Users\Administrator\Downloads\tools\DiskWipe.exe	2	2	0d, 0h, 01m, 54s	2022-10-12 20:59:50
C:\Users\Administrator\Downloads\tools\Everything\Everything.exe	1	1	0d, 0h, 00m, 23s	2022-10-12 19:29:32
C:\Users\Administrator\Downloads\tools\ProtonVPN_win_v2.0.6.exe	2	5	0d, 0h, 02m, 38s	2022-10-12 19:46:47
C:\Users\Administrator\Downloads\tools\Wireshark-win64-3.6.8.exe	1	2	0d, 0h, 00m, 44s	2022-10-12 20:56:06
Microsoft.AutoGenerated.{Unmapped GUID: 923DD477-5846-686B-A659-0FCCD73851A8}	0	1	0d, 0h, 00m, 29s	
Microsoft.AutoGenerated.{Unmapped GUID: C804BBA7-FA5F-CBF7-8B55-2096E5F972CB}	0	2	0d, 0h, 02m, 40s	
Microsoft.InternetExplorer.Default	3	22	0d, 0h, 17m, 06s	2022-10-12 21:02:33
Microsoft.Windows.Computer	1	0	0d, 0h, 00m, 00s	2022-10-04 16:22:47
Microsoft.Windows.ControlPanel	2	7	0d, 0h, 07m, 42s	2022-10-06 04:36:48
Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI	0	31	0d, 0h, 06m, 07s	

Total rows: 46

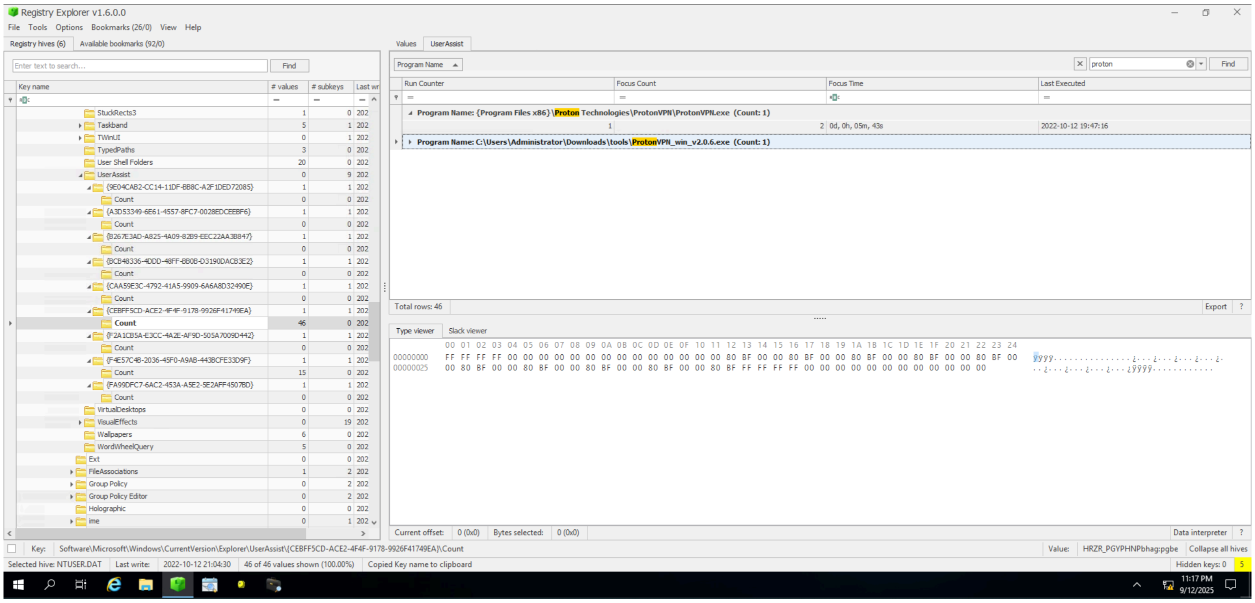
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

Value: HRZR_PGYPHNPbhag:pgbe

Selected hive: NTUSER.DAT Last write: 2022-10-12 21:04:30 46 of 46 values shown (100.00%) Copied Key name to clipboard

Registry Hives also note the amount of time a process is in focus. Examine the Hives and confirm for how many seconds was ProtonVPN executed?

Staying in the same paths as the previous questions, and filtering the program name for ProtonVPN, were able to see that the VPN was in focus for 5m 43s, or 343s



Registry Explorer v1.6.0.0

Registry hives (6) | Available bookmarks (92/0)

Key name	# values	# subkeys	Last wr
StuckRects3	1	0	202
Taskband	5	1	202
TWinUI	0	1	202
TypedPaths	3	0	202
User Shell Folders	20	0	202
UserAssist	0	9	202
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}	1	1	202
Count	0	0	202
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}	1	1	202
Count	0	0	202
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	1	1	202
Count	0	0	202
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}	1	1	202
Count	0	0	202
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	202
Count	0	0	202
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	202
Count	46	0	202
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	202
Count	0	0	202
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	202
Count	15	0	202
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}	1	1	202
Count	0	0	202
VirtualDesktops	0	0	202
VisualEffects	0	19	202
Wallpapers	6	0	202
WordWheelQuery	5	0	202
Ext	0	0	202
FileAssociations	1	2	202
Group Policy	0	2	202
Group Policy Editor	0	2	202
Holographic	0	0	202
ime	0	1	202

Values | UserAssist — Program Name — Search: proton

Run Counter	Focus Count	Focus Time	Last Executed
Program Name: {Program Files x86}\Proton Technologies\ProtonVPN\ProtonVPN.exe (Count: 1)			
1	2	0d, 0h, 05m, 43s	2022-10-12 19:47:16
Program Name: C:\Users\Administrator\Downloads\tools\ProtonVPN_win_v2.0.6.exe (Count: 1)			

Total rows: 46

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00   ÿÿÿÿ...............¿...¿...¿...¿...¿.
00000025  00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00          ..¿...¿...¿...¿...¿ÿÿÿÿ............
```

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

Value: HRZR_PGYPHNPbhag:pgbe

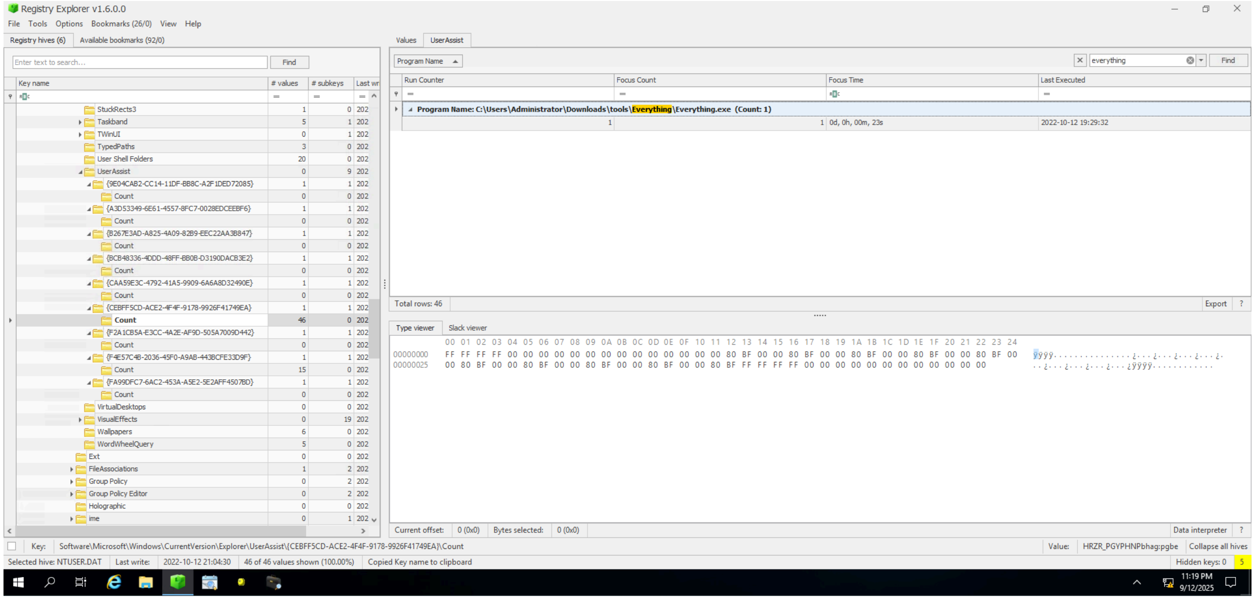
Selected hive: NTUSER.DAT Last write: 2022-10-12 21:04:30 46 of 46 values shown (100.00%) Copied Key name to clipboard

Hidden keys: 0

11:17 PM 9/12/2025

Everything.exe is a utility used to search for files in a Windows machine. What is the full path from which everything.exe was executed?

Staying in the same location as before, and filtering the program name for Everything.exe, we see the full path as C:\Users\Administrator\Downloads\tools\Everything\Everything.exe



Registry Explorer v1.6.0.0

Key name	# values	# subkeys	Last wr
StuckRects3	1	0	202
Taskband	5	1	202
TWinUI	0	1	202
TypedPaths	3	0	202
User Shell Folders	20	0	202
UserAssist	0	9	202
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}	1	1	202
Count	0	0	202
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}	1	1	202
Count	0	0	202
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	1	1	202
Count	0	0	202
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}	1	1	202
Count	0	0	202
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	202
Count	0	0	202
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	202
Count	46	0	202
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	202
Count	0	0	202
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	202
Count	15	0	202
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}	1	1	202
Count	0	0	202
VirtualDesktops	0	0	202
VisualEffects	0	19	202
Wallpapers	6	0	202
WordWheelQuery	5	0	202
Ext	0	0	202
FileAssociations	1	2	202
Group Policy	0	2	202
Group Policy Editor	0	2	202
Holographic	0	0	202
ime	0	1	202

Values | UserAssist — Program Name — Search: everything

Run Counter	Focus Count	Focus Time	Last Executed
Program Name: C:\Users\Administrator\Downloads\tools\Everything\Everything.exe (Count: 1)			
1	1	0d, 0h, 00m, 23s	2022-10-12 19:29:32

Total rows: 46

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00   ÿÿÿÿ...............¿...¿...¿...¿...¿.
00000025  00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00          ..¿...¿...¿...¿...¿ÿÿÿÿ............
```

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

Value: HRZR_PGYPHNPbhag:pgbe

Selected hive: NTUSER.DAT Last write: 2022-10-12 21:04:30 46 of 46 values shown (100.00%) Copied Key name to clipboard

Hidden keys: 0

11:19 PM 9/12/2025

Conclusion:

This was an interesting lab to dig into, and gave me some more good exposure to Windows Registry. There was a lot to navigate through, but fortunately the Windows Forensics Cheatsheet that was provided before the lab gave me some good guidance on where to search in the Registry. I’m definitely starting to get more comfortable with Windows Forensics, and through trial and error throughout this lab, I was able to advance my skills and knowledge in this area.