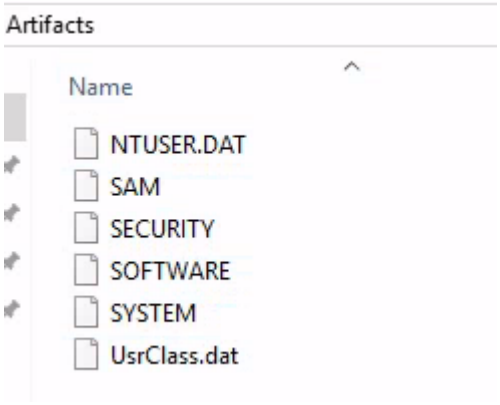
**TryHackMe: Secret Recipe**

The following is a writeup for the Secret Recipe room hosted on TryHackMe. This room involves investigating a suspected data exfiltration from a malicious IT specialist using tools like Registry Explorer to investigate a series of registry hives. It was a really fun room and is certainly beginner friendly. If you are looking to improve your fundamental window forensics I highly recommend completing this room.

**Scenario:** 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. 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.

**How many files are available in the Artifacts folder on the Desktop?**

6:

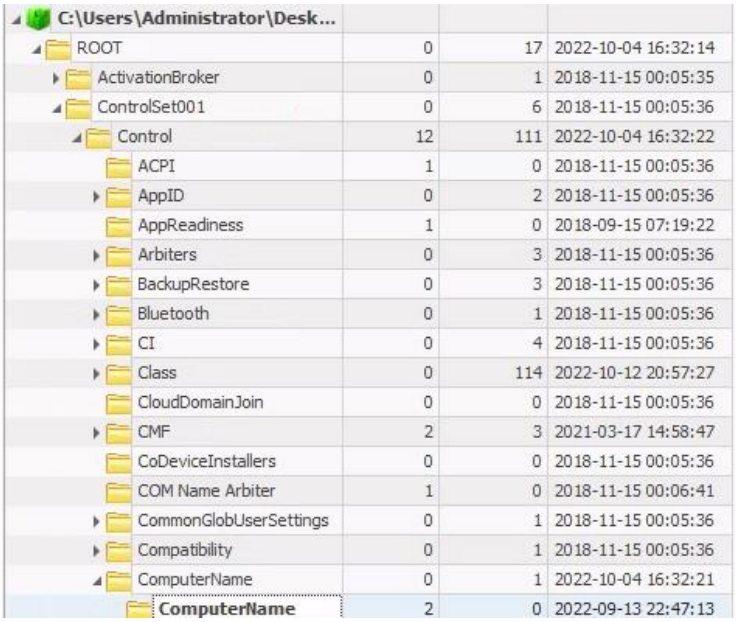



**What is the Computer Name of the Machine found in the registry?**

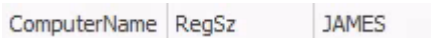
We can use Registry Explorer to read the registry key located at:

- SYSTEM\CurrentControlSet\Control\ComputerName \ComputerName

The above registry stores the Computer Name:




Once you have opened up the System Registry Hive and navigate to the key seen above, you can determine that the computer name is 'JAMES':

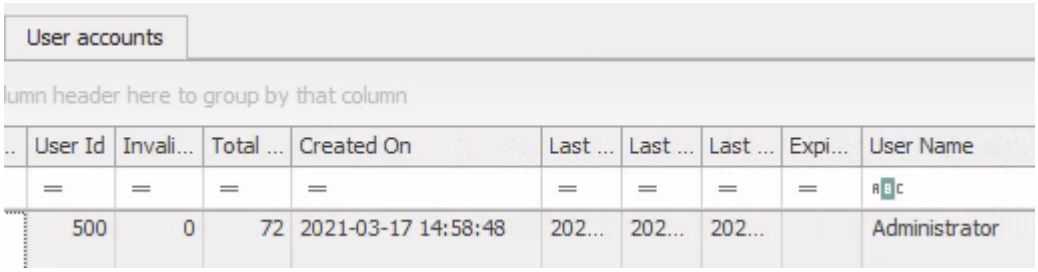



**When was the Administrator account created on this machine?**

To find the answer, we want to open up the SAM registry hive and navigate to SAM\Domains\Account\Users\Names\Administrator:

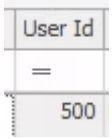

You can see when the account was created by looking at the value in the Last write timestamp column:

An even easier way to do this is by navigating to the Users key, selecting the User Accounts view and voila:



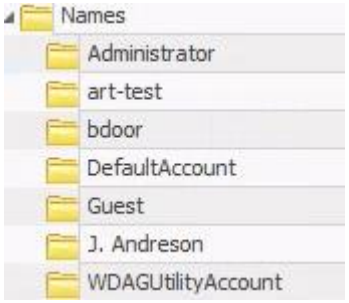

**What is the RID associated with the Administrator account?**

The RID is simply the User ID value that can be seen in the above question:




**How many User accounts were observed on this machine?**

There were 7 user accounts on this machine:




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

Back to the user key, we can see that the account with RID 1013 is bdoor:


**What is the VPN connection this host connected to?**

The past networks a given machine was connected to can be found in the following locations:

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

If you navigate to the Unmanaged registry key, you can quickly determine that the host was using ProtonVPN:

| | | |
|---|---|---|
| ProfileGuid | RegSz | {3EA38C7A-50AB-4C0B-8448-A11A3EC148E2} |
| Description | RegSz | ProtonVPN |
| Source | RegDword | 512 |
| DnsSuffix | RegSz | <none> |
| FirstNetwork | RegSz | ProtonVPN |
| DefaultGatewayMac | RegBinary | |

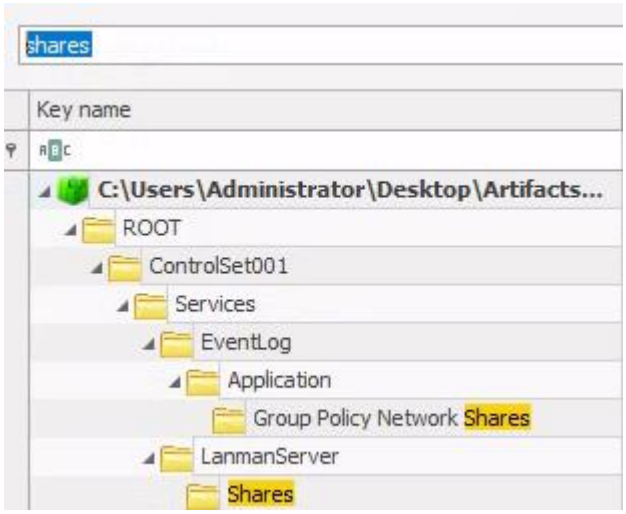
**When was the first VPN connection observed?**

The value associated with the last write timestamp is when the last connection was observed, so if you view the first key in the Unmanaged key, you can find the answer:

| | |
|---|---|
| Last write: | 2022-10-12 19:52:36 |

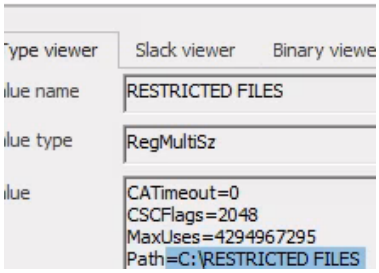
**There were three shared folders observed on his machine. What is the path of the third share?**

The SYSTEM hive contains information on shared folders. If you search for 'shares' you can quickly find shares for LanmanServer:




The name of path of the third share is C:\RESTRICTED FILES:

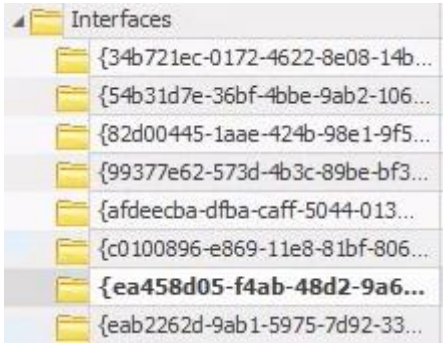
| | | |
|---|---|---|
| Users | RegMultiSz | CATime |
| Recipes | RegMultiSz | CATime |
| RESTRICTED FILES | RegMultiSz | CATime |




**What is the Last DHCP IP assigned to this host?**

You can find DHCP allocations in the following location:

- ControlSet001\Services\Tcpip\Parameters\Interfaces




| | | |
|---|---|---|
| DhcpIPAddress | RegSz | 172.31.2.197 |
| DhcpSubnetMask | RegSz | 255.255.240.0 |
| DhcpServer | RegSz | 172.31.0.1 |
| Lease | RegDword | 3600 |

**The suspect seems to have accessed a file containing the secret coffee recipe. Wha tis the name of the file?**

First off, open up the NTUSER.DAT registry hive in Registry Explorer. Then navigate to:

- NTUSER.DATA\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs


| | | | |
|---|---|---|---|
| .pdf | 5 | secret-recipe.pdf | secret-recipe.pdf.lnk |

**The suspect ran multiple commands in the run windows. What command was run to enumerate the network interfaces?**

Staying in the NTUSER.DAT registry hive, we can find what commands were run by the user in \RunMRU:


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

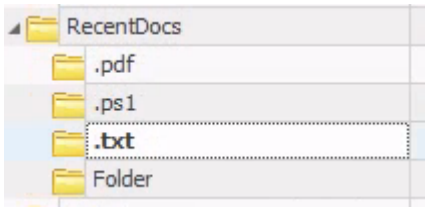
Navigate to the WordWheelQuery key in the NTUSER.DATA hive. This contains all the things the user has searched for in the file explorer:

| | | |
|---|---|---|
| secret files | 0 | WordWheelQuery |
| netcat | 1 | WordWheelQuery |
| recipe | 2 | WordWheelQuery |
| recipes | 3 | WordWheelQuery |

netcat is the answer.

**What is the recent text file opened by the suspect?**

Go back to RecentDocs but look at the .txt key:

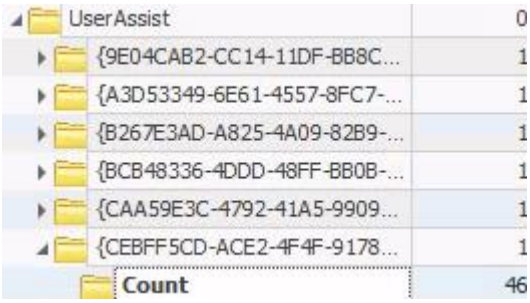



| | |
|---|---|
| secret-code.txt | secret-code.lnk |

**How many times was PowerShell executed on this host?**

To find evidence of execution and most important how many times a binary was executed, navigate to:

- Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist




| | |
|---|---|
| {System32}\WindowsPowerShell\v1.0\powershell.exe | 3 |

3 is the answer.

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

Staying in the UsserAssist key, you can see that the suspect executed Wireshark:

| |
|---|
| C:\Users\Administrator\Downloads\tools\Wireshark-win64-3.6.8.exe |
| {Program Files X64}\Wireshark\npcap-1.60.exe |

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

| | | | |
|---|---|---|---|
| {Program Files x86}\Proton Technologies\ProtonVPN\ProtonVPN.exe | 1 | 2 | 0d, 0h, 05m, 43s |

Make sure to convert it to seconds, aka the answer is 343 seconds.

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

| |
|---|
| C:\Users\Administrator\Downloads\tools\Everything\Everything.exe |