Lucas McMahon
3/5/25

Registry Forensics: Uncovering Insider Threats in the Secret Recipe Case

Table of Contents

Introduction

This project focuses on performing a **Windows registry forensic investigation** to determine if James, an IT technician, copied Coffely's secret recipe onto his machine. His computer has already been searched, but no direct evidence was found. Now, I'll be analyzing **registry artifacts** pulled from his system to uncover traces of the files, network activity, and other potential evidence of data theft.

To get this done, I'll be using **Eric Zimmerman's forensic tools**, including **Registry Explorer** to analyze registry hives. By looking at things like recent file access, network connections, and execution history, I'll figure out if James had the stolen files on his device and whether he tried to cover his tracks.

Objectives

- Identify user accounts on James's machine, including any suspicious accounts.
- Investigate VPN connections and shared folders that may have been used to transfer files.
- Determine if and when the **secret recipe files** were accessed.
- Analyze recent commands, file transfers, and PowerShell execution.
- Uncover traces of network enumeration and potential exfiltration methods.

Lab Environment.

This lab is run using TryHackMe's **"Secret Recipe"** challenge, which provides a **Windows-based virtual machine (VM)** for forensic analysis. The VM contains **extracted registry hives** from James's system, and my task is to examine them for forensic evidence. The setup ensures a structured environment for analyzing user activity, file access history, and network connections.

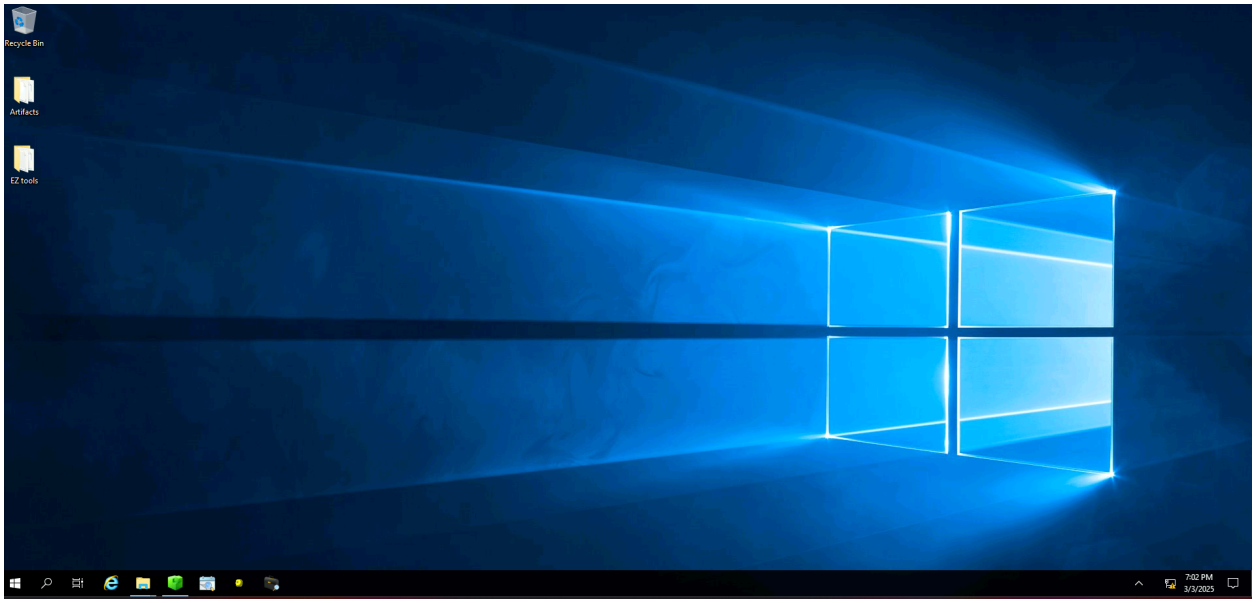
Lucas McMahon
3/5/25

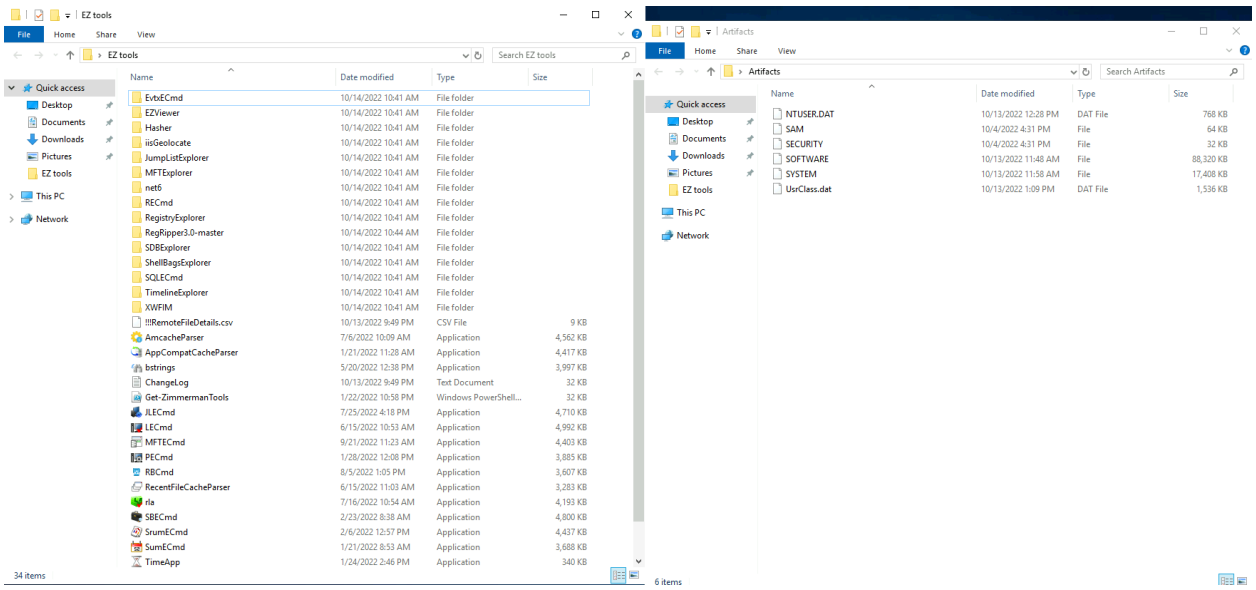
Tools and Technologies Used

- **RegistryExplorer** – Analyze Windows registry hives (SAM, SYSTEM, NTUSER.dat).
- **Autopsy** – A digital forensics platform for deeper file analysis.
- **ChatGPT & Documentation** – Used for additional research on registry keys and forensic techniques.

Step-by-Step Process

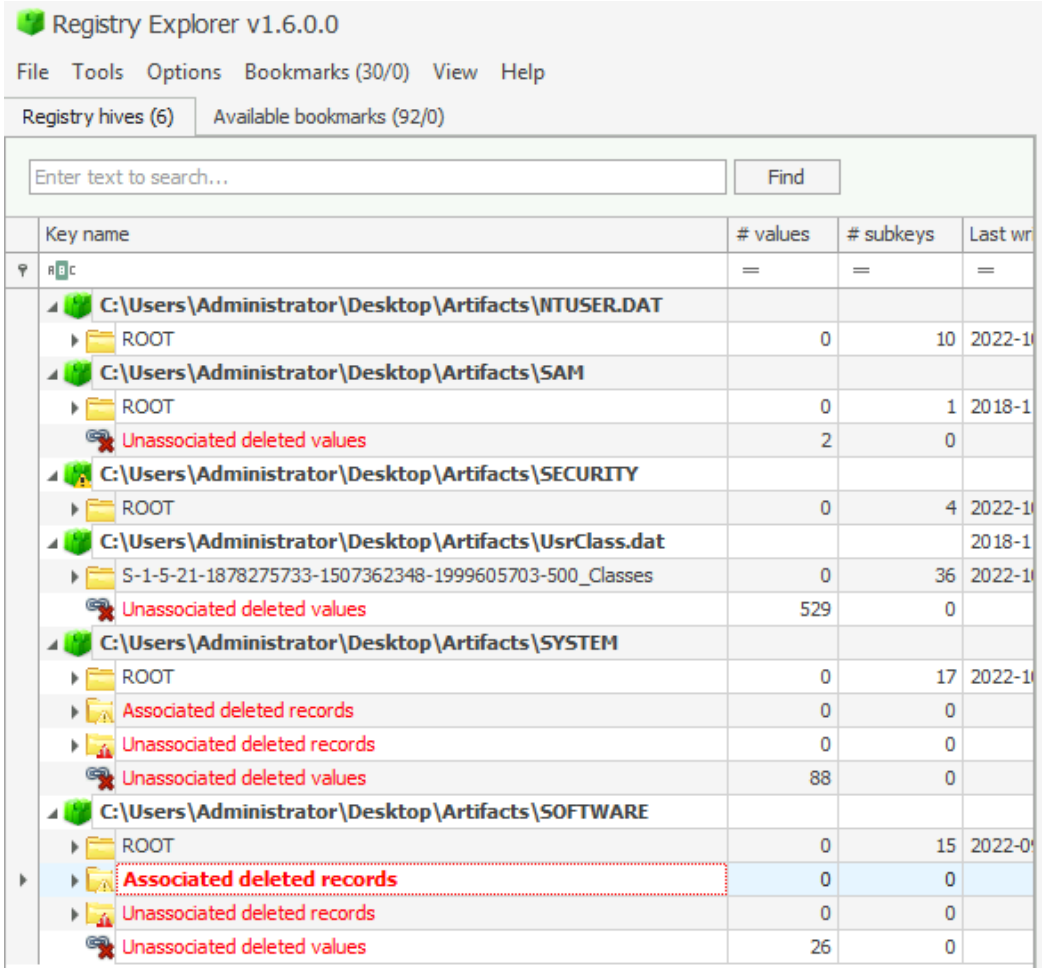
Loading up the virtual machine, I can see on the desktop the provided artifacts that will be investigated and the tools at my disposal.





Lucas McMahon
3/5/25

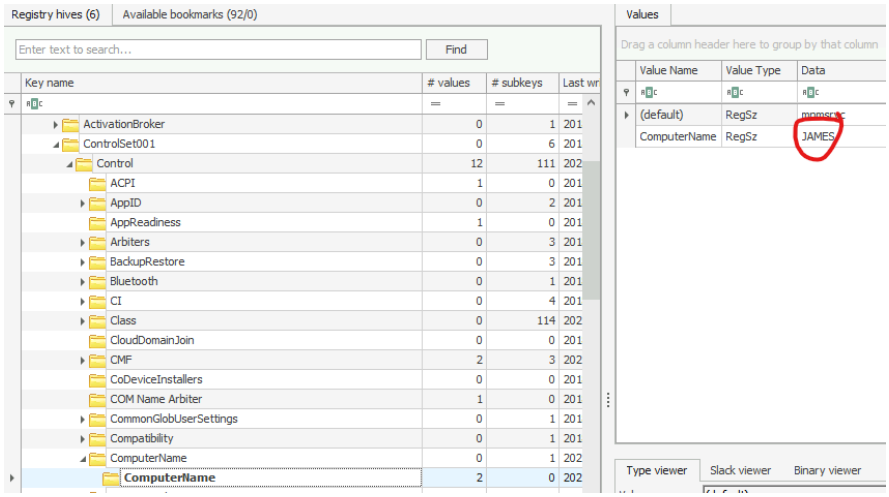
I will mostly be working out of Registry Explorer, so first I load up all the artifacts into the tool to begin the investigation.



First, I am going to start the investigation by getting the computer name and other account information. From the initial view, it is very intimidating to see that and to know where to go to find anything. Luckily, the following document can give a great reference for performing forensic analysis (and ChatGPT for extra help).

Lucas McMahon
3/5/25

I start by following the path to find the computer name, and come to find it is listed under **James**.



Next, investigating the SAM (Security Account Manager) hive will reveal to us information about the accounts present on this device with information such as the account creation date, last logon, user ID, password, etc.

Lucas McMahon
3/5/25

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

Enter text to search... | Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\Administrator\Desktop\Artifacts\NTUSER.DAT			
ROOT	0	10	2022-10-08 13:59:25
C:\Users\Administrator\Desktop\Artifacts\SAM			
ROOT	0	1	2018-11-15 00:04:12
SAM	2	3	2020-04-15 06:32:53
Domains	1	2	2018-11-15 00:04:12
Account	2	3	2022-10-04 17:03:12
Aliases	1	2	2018-11-15 00:04:12
Groups	1	2	2018-11-15 00:04:12
Users	1	8	2022-10-04 17:03:12
000001F4	5	0	2022-10-12 19:26:09
000001F5	3	0	2021-03-17 14:57:32
000001F7	4	0	2021-03-17 14:57:32
000001F8	5	0	2021-03-17 14:57:32
000003F3	2	0	2022-10-04 16:21:27
000003F4	4	0	2022-10-04 16:51:04
000003F5	2	0	2022-10-04 17:03:12
Names	1	7	2022-10-04 17:03:12
Administrator	1	0	2021-03-17 14:58:48
art-test	1	0	2022-10-04 16:51:04
bdoor	1	0	2022-10-04 17:03:12
DefaultAccount	1	0	2021-03-17 14:58:48
Guest	1	0	2021-03-17 14:58:48
J. Andreson	1	0	2022-10-04 16:21:27
WDAGUtilityAccount	1	0	2021-03-17 14:58:48

Values | User accounts

Drag a column header here to group by that column

Va...	User...	...	Total Login...	Created On	Last Login Time	...	...	Ex...	User Name	F...	Password...
☑	=		=	=	=			=	ABC	ABC	ABC
	500	0	72	2021-03-17 14...	2022-10-12 19...	...	...		Administrator		secret

Looks like there was an **admin** account created on march 17th, 2021, with a userID of 500, 72 total logins, and a password of “secret”.

Names	1	7	2022-10-04 17:03:12
Administrator	1	0	2021-03-17 14:58:48
art-test	1	0	2022-10-04 16:51:04
bdoor	1	0	2022-10-04 17:03:12
DefaultAccount	1	0	2021-03-17 14:58:48
Guest	1	0	2021-03-17 14:58:48
J. Andreson	1	0	2022-10-04 16:21:27
WDAGUtilityAccount	1	0	2021-03-17 14:58:48

Lucas McMahon
3/5/25

Va...	User...	...	Total Login...	Created On	Last Login Time	...	...	Ex...	User Name
☑	=		=	=	=			=	abc
☑	1013	0	0	2022-10-04 17...		...			bdoor

Another look at the list of users will reveal a suspicious account name of ‘bdoor’ with more information revealed similar to the admin account. Surely it will be valuable information for the company's investigation.

Next we are asked to find out VPN connection information regarding this host. My cheat sheet didn’t tell me anything directly about where to find VPN connection information, so a quick ChatGPT prompt will reveal to me that the **NetworkList** directory will contain the information I need.

Windows stores network connection history in the **SOFTWARE** hive under the **NetworkList** key.

Using RegistryExplorer to Find VPN Connection Timestamps

1. Open **RegistryExplorer** and load the **SOFTWARE** hive.
2. Navigate to:

Copy Edit

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
```

- Each **GUID** under this key represents a different **network connection.**
- Look for **ProfileName** values related to your **VPN provider** or a **virtual network adapter.**
- Check **DateCreated** and **DateLastConnected** for timestamps.

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

network list | Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\Administrator\Desktop\Artifacts\SOFTWARE			
ROOT	0	15	2022-09-13 06:00:33
Microsoft	0	209	2022-10-12 16:32:33
Windows NT	0	1	2018-09-15 07:20:45
CurrentVersion	29	86	2022-10-04 16:34:18
NetworkList	3	6	2021-03-17 14:58:47

Values | Known networks

Drag a column header here to group by that column

First Network	Network Name	Name Type	First Connect LOCAL	Last Connected LOCAL
Network 2	Network 2	Wired	2021-03-17 15:08:34	2022-10-04 16:32:23
ProtonVPN	ProtonVPN		2022-10-12 19:52:36	2022-10-12 19:52:36
Network	Network	Wired	2021-03-17 14:58:47	2021-03-17 14:59:21

This shows me that there is a VPN software called **ProtonVPN** and reveals information such as the first and last connection.

Next, we are asked to located the information regarding shared folders, again our cheat sheet does not provide this specifically so ChatGPT shares the following.

Lucas McMahon
3/5/25

Windows stores **shared folder settings** primarily in the **SYSTEM** and **SOFTWARE** hives.

1. Find Shared Folders in the SYSTEM Hive

- Open **RegistryExplorer** and load the **SYSTEM** hive.
- Navigate to:

sql Copy Edit

```sql
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares
```

  - This key contains **all shared folders** on the system.
  - Each share name corresponds to a **folder being shared**.
  - The **path** of the shared folder is stored as a value.

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

Shares Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\Administrator\Desktop\Artifacts\SYSTEM			
ROOT	0	17	2022-10-04 16:32:14
ControlSet001	0	6	2018-11-15 00:05:36
Services	0	622	2022-10-12 20:57:27
EventLog	16	9	2018-11-15 00:05:43
LanmanServer	11	8	2018-11-15 00:05:57
Shares	3	1	2022-10-12 19:20:04

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack
Users	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUse...	63-00
Recipes	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUse...	1E-00
RESTRICTED FILES	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUse...	00-00-E8-35

Looks like there is a shared folder named **Restricted Files** that could be of interest.

Next, we are asked to look into information regarding DHCP assignments and find out the last assigned IP address. ChatGPT reveals the following.

The **last assigned DHCP IP address** is stored in the **SYSTEM** hive under the **network interface settings**.

Using RegistryExplorer to Find the Last DHCP IP

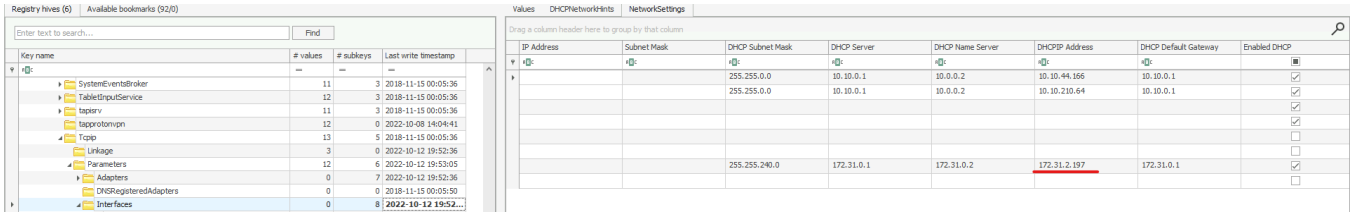
1. Open **RegistryExplorer** and load the **SYSTEM** hive.
2. Navigate to:

pgsql Copy Edit

```pgsql
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{GUID}
```

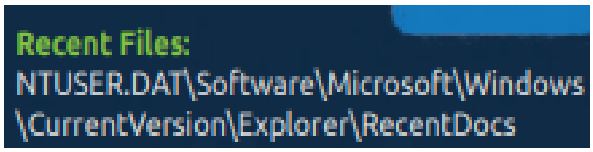
- `{GUID}` represents each **network adapter** on the system.
- Look for **DhcpIPAddress** → This is the **last assigned DHCP IP**.
- Also, check **DhcpSubnetMask** and **DhcpServer** for more details.

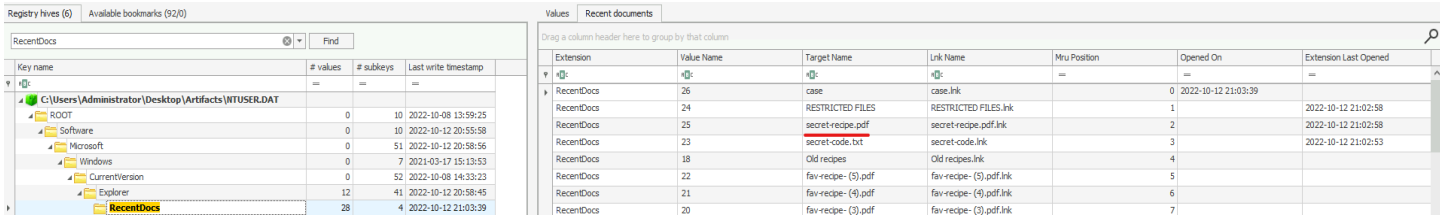
Lucas McMahon
3/5/25



The image might be hard to read, but the **DHCP IP Address column** reveals the 3 IP addresses it had assigned, with the latest one being **172.31.2.197**.

The team suggests that the suspect accessed a file containing the secret recipe, and are asking to find out the name of the file. NTUSER.dat is a hive collection of the window registry that contains user information such as recently accessed files, folders, dialog history and searches. The cheatsheet reveals that we can find the recently accessed files in a specific place.





A file named **secret-recipe.pdf and secret-code.txt** were last opened on **October 12th, 2022, 9:02PM**. Let's keep investigating.

Now we are looking for recently run commands from the suspect, specifically what command was used to enumerate network interfaces, possibly revealing to the suspect what weakness the system had to exploit. Again, we are looking for User activity.

Lucas McMahon
3/5/25

Windows stores a history of commands executed via **Run** and **Command Prompt (cmd.exe)** in the **NTUSER.DAT** hive.

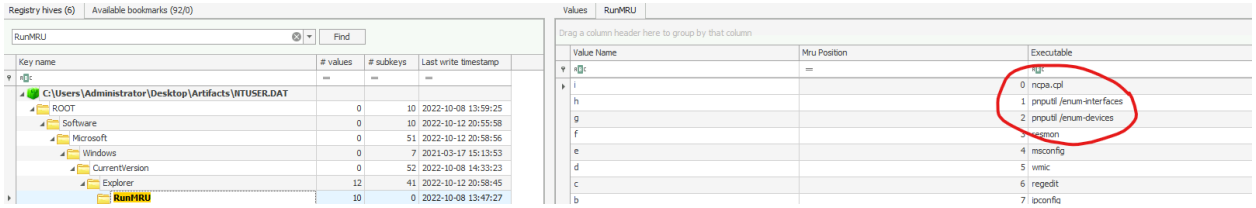
Using RegistryExplorer to Find Run and Command Prompt History

1. Open **RegistryExplorer.exe** and load the **NTUSER.DAT** hive.
2. Navigate to:

Copy Edit

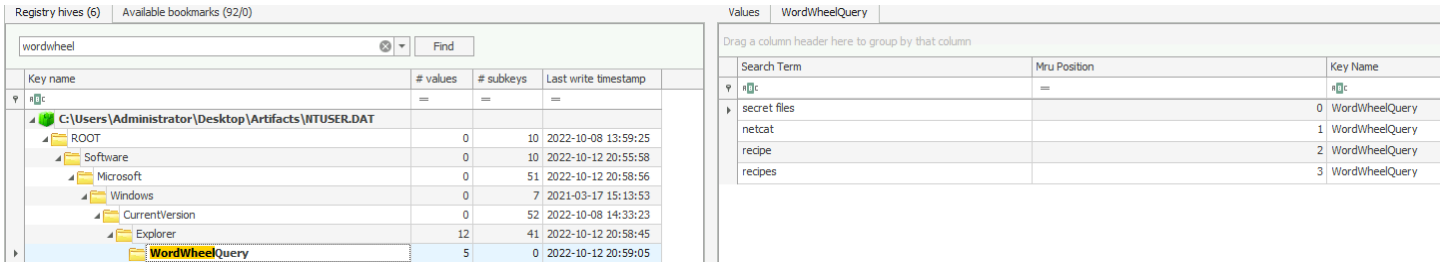
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
```

- This stores the history of commands run via the **Run dialog** (Win + R).



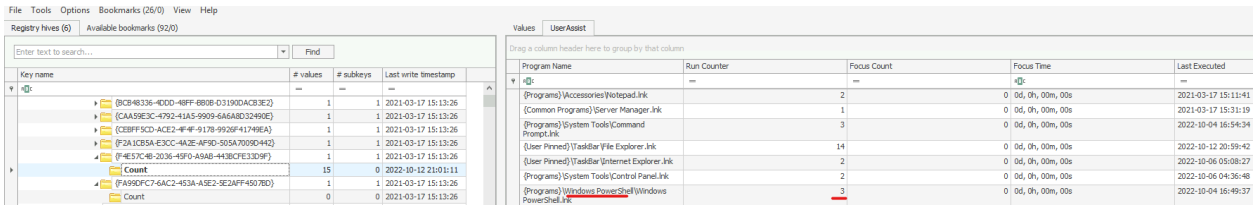
ChatGPT for the win yet again. Next, we are asked to find what the recent searches in file explorer can reveal about how the suspect transferred files over the network. Referencing the cheat sheet we can see that NTUser can show us this.

Windows Explorer Address/Search Bars:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery



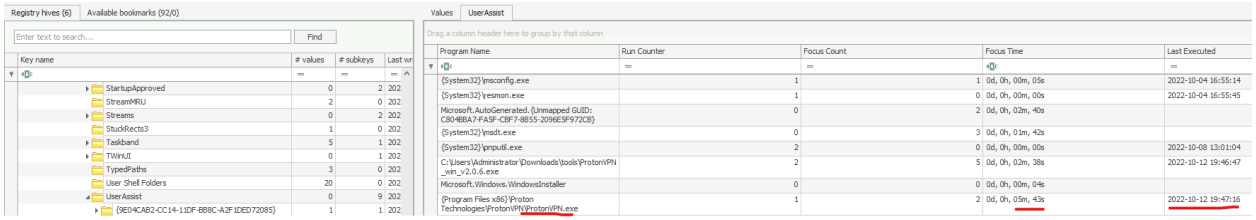
Looks like **netcat** was used over the network to transfer "**secret files**". Next, we are asked to investigate evidence of powershell execution on the device. Referencing the cheat sheet, we can see NTUser also contains this.

Lucas McMahon
3/5/25



Windows Powershell was **executed 3 times** on **October 4th 4:49 PM**.

Next, we need to look into **ProtonVPN**, specifically when, and how long it was used for. While we are still on the same topic of executed processes, we can stay in this same folder, and scroll through to find Proton.exe



Again, might be hard to read but it shows us that on **October 12th, 7:47PM** ProtonVPN was executed and used for **5 minutes and 43 seconds.**

Lastly, we are asked to locate the full file location for **Everything.exe**, a tool used to locate any file on a windows machine. Staying in the same folder, we can see the full path listed below.

Lucas McMahon
3/5/25

Drag a column header here to group by that column

Program Name
C:\Users\Administrator\AppData\Local\Temp\2\{Unmapped GUID: BD2C55F5-E418-4D9A-8860-CC7A6DB0EE16}\AccessData_FTK_Imager_4.5.0_(x64).exe
{Program Files X64}\AccessData\FTK Imager\FTK Imager.exe
C:\Users\Administrator\AppData\Local\Temp\2\{Unmapped GUID: 5D4A904E-75C4-41D6-8F73-250D659F3D10}\AccessData_FTK_Imager_4.5.0_(x64).exe
C:\Users\Administrator\AppData\Local\Temp\2\{Unmapped GUID: CDF018BB-74B5-4098-BB2D-A1B5B0B29AE4}\AccessData_FTK_Imager_4.5.0_(x64).exe
C:\Users\Administrator\Downloads\tools\Everything\Everything.exe
C:\Users\Administrator\Downloads\tools\DiskWipe.exe
C:\Users\Administrator\Downloads\tools\Wireshark-win64-3.6.8.exe
{Program Files X64}\Wireshark\npcap-1.60.exe

Results and Analysis

After going through James's registry artifacts, I found several pieces of evidence confirming suspicious activity:

- **Unauthorized Accounts**: A hidden user account named **"bdoor"** was created, likely for persistence.
- **VPN Activity**: James used **ProtonVPN** on **October 12th, 2022, at 7:47 PM** for about 5 minutes, possibly to mask data exfiltration.
- **Secret File Access**: The files **secret-recipe.pdf** and **secret-code.txt** were last opened on **October 12th, 2022, at 9:02 PM**.
- **File Transfer via Netcat**: James executed **netcat** to send files over the network.
- **PowerShell Execution**: Windows **PowerShell was used three times** on **October 4th at 4:49 PM**, possibly for scripting or automation.
- **Network Enumeration**: Commands were run to list network interfaces, likely to find weaknesses.
- **Shared Folder**: A folder named **"Restricted Files"** was shared, which could have been used for unauthorized access.

Challenges Faced

Registry Complexity: Knowing where to look in the registry was tricky without a clear guide, but using **ChatGPT** and forensic cheat sheets helped narrow down key locations.

Interpreting VPN & Network Logs: Finding timestamps and determining VPN session lengths required careful analysis of execution history and timestamps.

File Transfer Evidence: Netcat logs weren't directly available, so I had to piece together evidence from multiple registry entries.

Conclusion

The investigation strongly suggests James accessed **Coffely's secret recipe files**, used **Netcat** to transfer them, and attempted to cover his tracks with **ProtonVPN** and a hidden **"bdoor"** account. This case highlights the importance of **registry forensics** in detecting insider threats and tracking unauthorized data access.

References

Eric Zimmerman's Tools: https://www.ericzimmerman.com/tools/

TryHackMe – Secret Recipe Challenge: https://tryhackme.com/

TryHackMe - Windows Registry Forensics Cheat Sheet