

Registry Forensics: Uncovering Insider Threats in the Secret Recipe Case

Table of Contents

- Introduction
- Objectives
- Lab Environment
- Tools and Technologies Used
- Step-by-Step Process
- Results and Analysis
- Challenges Faced
- Conclusion
- References

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.

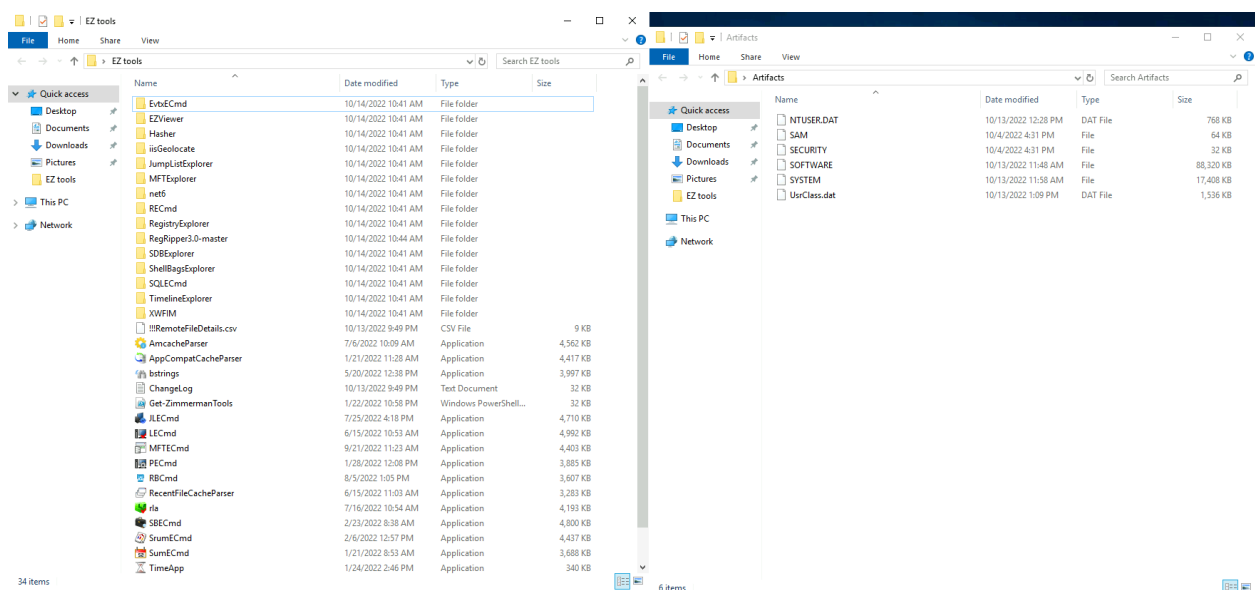
This lab is run using TryHackMe's "**Secret Recipe**" challenge, which provides a **Windows-based virtual machine (VM)** for forensic analysis. The VM contains **extracted registry hives** from James's system, and my task is to examine them for forensic evidence. The setup ensures a structured environment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

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.



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

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (30/0) View Help

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

Enter text to search... Find

Key name	# values	# subkeys	Last wr
C:\Users\Administrator\Desktop\Artifacts\NTUSER.DAT			
ROOT	0	10	2022-10
C:\Users\Administrator\Desktop\Artifacts\SAM			
ROOT	0	1	2018-11
Unassociated deleted values	2	0	
C:\Users\Administrator\Desktop\Artifacts\SECURITY			
ROOT	0	4	2022-10
C:\Users\Administrator\Desktop\Artifacts\UsrClass.dat			2018-11
S-1-5-21-1878275733-1507362348-1999605703-500_Classes	0	36	2022-10
Unassociated deleted values	529	0	
C:\Users\Administrator\Desktop\Artifacts\SYSTEM			
ROOT	0	17	2022-10
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	88	0	
C:\Users\Administrator\Desktop\Artifacts\SOFTWARE			
ROOT	0	15	2022-09
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	26	0	

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).



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

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure of the registry, with the path "ComputerName" selected under "SYSTEM\CurrentControlSet\Control\ComputerName". The right pane shows the "Values" list for the selected key, which contains a single value named "ComputerName" of type "RegSz" with the data "JAMES".

Key name	# values	# subkeys	Last write
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

Value Name	Value Type	Data
(default)	RegSz	James
ComputerName	RegSz	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 login, user ID, password, etc.

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...
📄	<input checked="" type="checkbox"/>	=		=	=	=			=	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

Va...	User...	...	Total Login...	Created On	Last Login Time	Ex...	User Name
<input checked="" type="checkbox"/>	=	=	=	=	=	=	=	=	Administrator
<input checked="" type="checkbox"/>	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:

```
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.

Key name	# values	# subkeys	Last write timestamp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList	3	6	2021-03-17 14:58:47

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	Wired	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.

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

```
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)				Values			
Shares				Find				Drag a column header here to group by that column			
Key name	# values	# subkeys	Last write timestamp					Value Name	Value Type	Data	Value Slack
Root	=	=	=					Users	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUse...	63-00
C:\Users\Administrator\Desktop\Artifacts\SYSTEM								Recipes	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUse...	1E-00
ROOT	0	17	2022-10-04 16:32:14					<u>RESTRICTED FILES</u>	RegMultiSz	CATimeout=0 CSCFlags=2048 MaxUse...	00-00-E8-35
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								

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

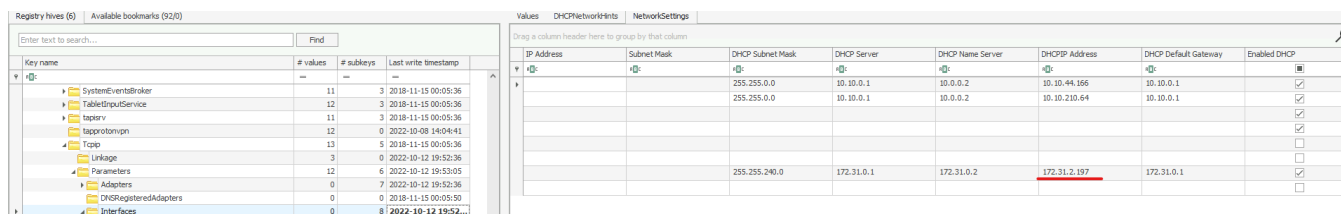
1. Open **RegistryExplorer** and load the **SYSTEM** hive.
2. Navigate to:

```
pgsql
```

Copy Edit

```
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.

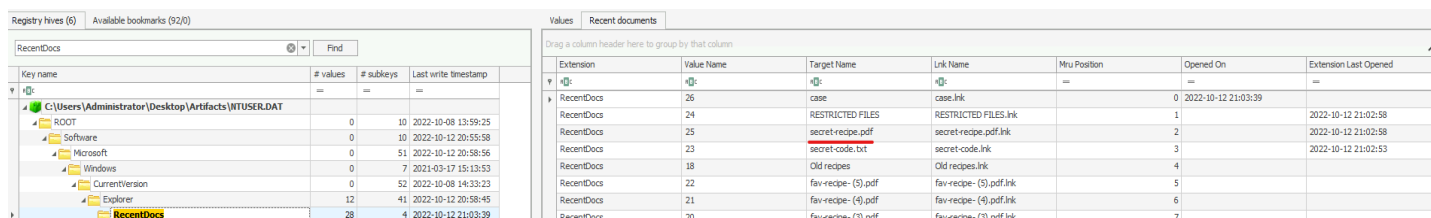
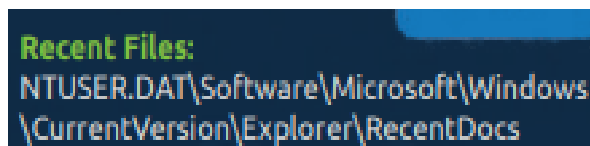


Key name	# values	# subkeys	Last write timestamp
SystemEventBroker	11	3	2018-11-13 00:05:36
TabletInputService	12	3	2018-11-15 00:05:36
Input	11	3	2018-11-15 00:05:36
InputProtocol	12	0	2022-10-08 14:04:41
Linkage	13	5	2018-11-15 00:05:36
Linkage	3	0	2022-10-12 19:52:36
Parameters	12	6	2022-10-12 19:53:05
Adapters	0	7	2022-10-12 19:52:36
DHCPRegisteredAdapters	0	0	2018-11-15 00:05:50
Interfaces	0	8	2022-10-12 19:52:36

Address	Subnet Mask	DHCP Subnet Mask	DHCP Server	DHCP Name Server	DHCP Address	DHCP Default Gateway	Enabled DHCP
	255.255.0.0	10.10.0.1	10.0.0.2	10.10.44.166	10.10.0.1	10.10.0.1	<input checked="" type="checkbox"/>
	255.255.0.0	10.10.0.1	10.0.0.2	10.10.210.64	10.10.0.1	10.10.0.1	<input checked="" type="checkbox"/>
							<input checked="" type="checkbox"/>
							<input checked="" type="checkbox"/>
							<input type="checkbox"/>
							<input type="checkbox"/>
	255.255.240.0	172.31.0.1	172.31.0.2	172.31.2.197	172.31.0.1	172.31.0.1	<input checked="" type="checkbox"/>
							<input type="checkbox"/>

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.



Key name	# values	# subkeys	Last write timestamp
ROOT	0	10	2022-10-08 13:59:25
Software	0	10	2022-10-12 20:55:58
Microsoft	0	51	2022-10-12 20:58:56
Windows	0	7	2021-03-17 15:13:53
CurrentVersion	0	52	2022-10-08 14:33:23
Explorer	12	41	2022-10-12 20:58:45
RecentDocs	28	4	2022-10-12 21:03:39

Extension	Value Name	Target Name	Link Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	26	case	case.link	0	2022-10-12 21:03:39	
RecentDocs	24	RESTRICTED FILES	RESTRICTED FILES.link	1		2022-10-12 21:02:58
RecentDocs	25	secret-recipe.pdf	secret-recipe.pdf.link	2		2022-10-12 21:02:58
RecentDocs	23	secret-code.txt	secret-code.link	3		2022-10-12 21:02:53
RecentDocs	18	Old recipes	Old recipes.link	4		
RecentDocs	22	fav-recipe- (5).pdf	fav-recipe- (5).pdf.link	5		
RecentDocs	21	fav-recipe- (4).pdf	fav-recipe- (4).pdf.link	6		
RecentDocs	20	fav-recipe- (3).pdf	fav-recipe- (3).pdf.link	7		

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.

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:

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

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

The screenshot shows the Registry Explorer interface. On the left, the tree view is expanded to **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**. The right pane shows the values of this registry path. The values are listed in a table with columns: Value Name, Mru Position, and Executable. The values are: 0: ncpa.cpl, 1: proutll /enum-interfaces, 2: proutll /enum-devices, 3: netcat, 4: msconfig, 5: wmic, 6: regedit, 7: ipconfig. The value 1 is circled in red.

Value Name	Mru Position	Executable
0	10	ncpa.cpl
1	10	proutll /enum-interfaces
2	10	proutll /enum-devices
3	10	netcat
4	10	msconfig
5	10	wmic
6	10	regedit
7	10	ipconfig

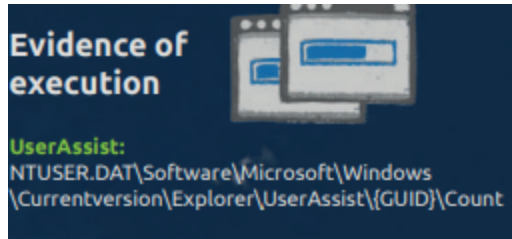
ChatGPT for the win yet again. Next, we are asked to find what the recent searches in file explorer can reveal about how the suspect transferred files over the network. Referencing the cheat sheet we can see that NTUser can show us this.

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

The screenshot shows the Registry Explorer interface. On the left, the tree view is expanded to **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery**. The right pane shows the values of this registry path. The values are listed in a table with columns: Search Term, Mru Position, and Key Name. The values are: secret files, netcat, recipe, recipes. The value 1 is circled in red.

Search Term	Mru Position	Key Name
secret files	0	WordWheelQuery
netcat	1	WordWheelQuery
recipe	2	WordWheelQuery
recipes	3	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.



Registry Hives (6) Available bookmarks (92/0)					Values UserAssist				
Enter text to search...					Drag a column header here to group by that column				
Key name	# values	# subkeys	Last write timestamp		Program Name	Run Counter	Focus Count	Focus Time	Last Executed
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{B0948336-4CDD-48FF-B866-03190DA39E32}	1	1	2021-03-17 15:13:26		(Programs)\Accessories\Notepad.lnk	2		0 0d, 0h, 00m, 00s	2021-03-17 15:11:41
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	2021-03-17 15:13:26		(Common Programs)\Server Manager.lnk	1		0 0d, 0h, 00m, 00s	2021-03-17 15:31:19
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{C3BFF5CD-ACE2-4F4F-9178-9926F41748EA}	1	1	2021-03-17 15:13:26		(Programs)\System Tools\Command Prompt.lnk	3		0 0d, 0h, 00m, 00s	2022-10-04 16:54:34
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F2A1CE5A-E3CC-4A2E-4F9D-505A7095D442}	1	1	2021-03-17 15:13:26		(User Pinned)\Taskbar\File Explorer.lnk	14		0 0d, 0h, 00m, 00s	2022-10-12 20:59:42
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}	1	1	2021-03-17 15:13:26		(User Pinned)\Taskbar\Internet Explorer.lnk	2		0 0d, 0h, 00m, 00s	2022-10-06 05:08:27
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}\Count	15	0	2022-10-12 21:03:11		(Programs)\System Tools\Control Panel.lnk	2		0 0d, 0h, 00m, 00s	2022-10-06 04:36:48
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}\Count	1	1	2021-03-17 15:13:26		(Programs)\Windows PowerShell\Windows PowerShell.lnk	3		0 0d, 0h, 00m, 00s	2022-10-04 16:49:37

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

Registry Hives (6) Available bookmarks (92/0)					Values UserAssist				
Enter text to search...					Drag a column header here to group by that column				
Key name	# values	# subkeys	Last write timestamp		Program Name	Run Counter	Focus Count	Focus Time	Last Executed
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{B0948336-4CDD-48FF-B866-03190DA39E32}	0	2	2022-10-04 16:55:14		(System32)\msconfig.exe	1		1 0d, 0h, 00m, 05s	2022-10-04 16:55:14
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	2	0	2022-10-04 16:55:45		(System32)\yesmon.exe	1		0 0d, 0h, 00m, 00s	2022-10-04 16:55:45
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{C3BFF5CD-ACE2-4F4F-9178-9926F41748EA}	0	2	2022-10-04 16:55:45		Microsoft.AutoGenerated (Unmapped GUID: C804B8A7-F43F-C8F7-8B55-2096E9F97C93)	0		2 0d, 0h, 02m, 40s	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F2A1CE5A-E3CC-4A2E-4F9D-505A7095D442}	1	0	2022-10-08 13:01:04		(System32)\msiutil.exe	0		3 0d, 0h, 01m, 42s	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}	5	1	2022-10-12 19:46:47		(System32)\inputifl.exe	2		0 0d, 0h, 00m, 00s	2022-10-08 13:01:04
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}\Count	0	1	2022-10-12 19:46:47		C:\Users\Administrator\Downloads\tools\ProtonVPN_win_v2.0.6.exe	2		5 0d, 0h, 02m, 38s	2022-10-12 19:46:47
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}\Count	3	0	2022-10-12 19:46:47		Microsoft.Windows.WindowsInstaller	0		0 0d, 0h, 00m, 04s	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-49F0-A9AB-4438CFE33D9F}\Count	20	0	2022-10-12 19:46:47		(Program Files x86)\Proton Technologies\ProtonVPN\ProtonVPN.exe	1		2 0d, 0h, 05m, 43s	2022-10-12 19:47:18

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.

Drag a column header here to group by that column	
	Program Name
▼	RIC
	C:\Users\Administrator\AppData\Local\Temp\2\{Un mapped 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\{Un mapped GUID: 5D4A904E-75C4-41D6-8F73-250D659F3D10}\AccessData_FTK_Imager_4.5.0_(x64).exe
	C:\Users\Administrator\AppData\Local\Temp\2\{Un mapped 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\ncn-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