SeeShells

Case Study #1 Writeup

Background Information:

The present day is 03/15/2021 - you are working as a Digital Forensics and Incident Response (DFIR) analyst and are investigating an insider threat/intellectual property (IP) theft case. The company, Tehsla, said their own Cyber Threat Intelligence department found that a person or group is selling a folder on the deep web with intellectual property inside the folder. The forum post selling the information was posted at 9:34 PM on 03/08/2021. The Threat Intelligence team couldn't verify what exactly was being sold inside the folder, but they believe the claim is legitimate and only people working within the company could have accessed any confidential company information.

Therefore, the company's security department believes they have identified a suspect - a disgruntled employee who is not happy with their pay and needs the extra cash. However, the company does not have definitive proof that this employee was the one who did it, so they have hired you to help. They were able to get the suspected employee's computer and registry information - are you able to find any solid evidence and gather information on what exactly was stolen?

What we know:

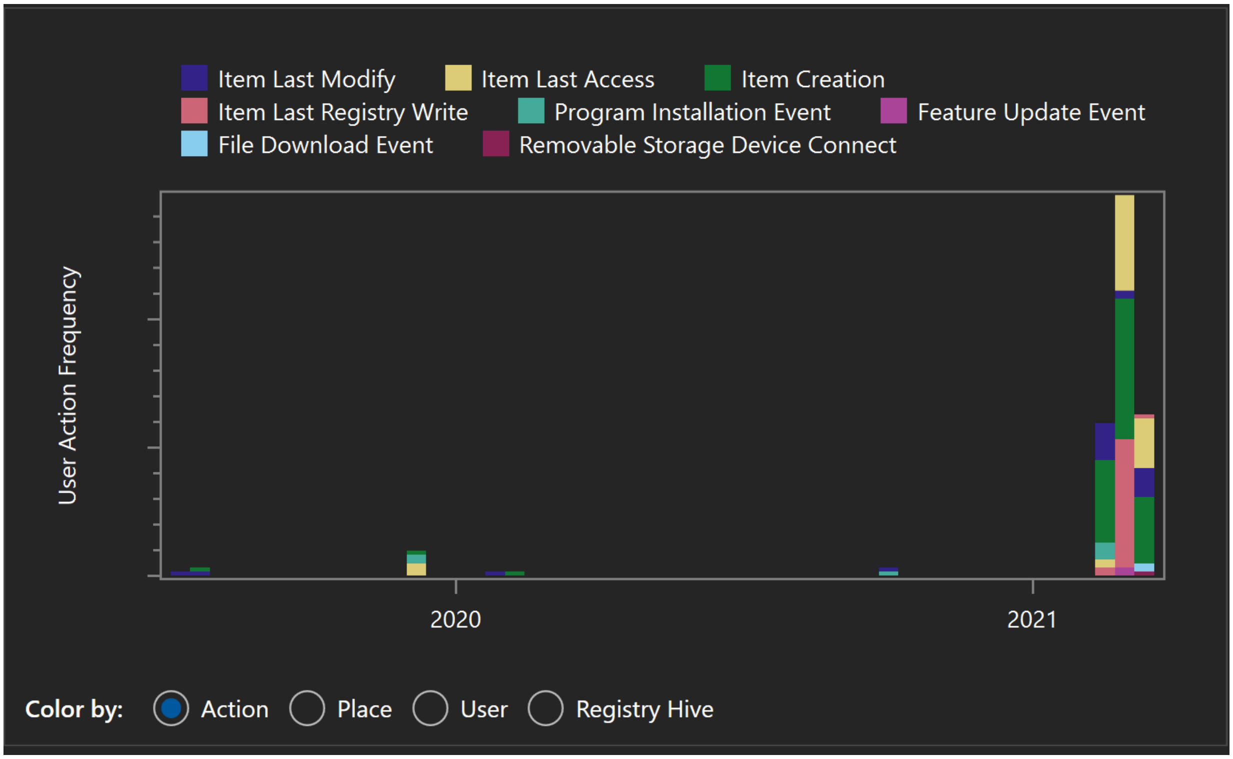
- Forum Post Date and Time - 9:34 PM on 03/08/2021
- Employees Registry Hive

What we need to find out:

- What private information might have been stolen?
- Is there evidence pertaining to exfiltration of files?
- If anything was stolen, what information is being sold on the web?

Guide:

One of the first things that can be seen is the large timeline of the events spanning from 2019 to March 2021. This shows a histogram of shell events that were created on this users registry.



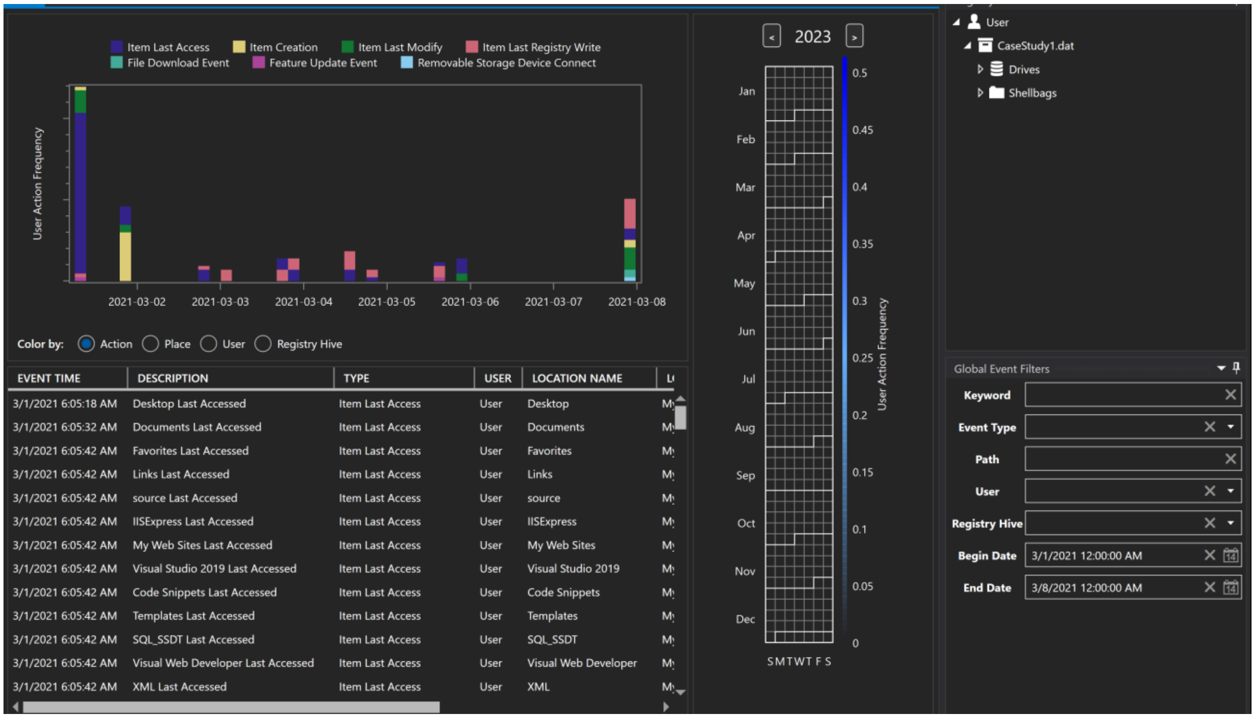
Color by: ● Action ○ Place ○ User ○ Registry Hive

Figure 1. Showing one of the first events in 2019

The first thing we want to do is narrow down our view so we are only looking at potentially useful data. We can do this by using filters. Since our main piece of information has to do with time, we can use the Begin Date and End Date Filters.

The company's Cyber Threat Intelligence team said the post was put up on 03/08/2021. Showing activity from a week before the incident date could show a list of events that lead up to it.

Within SeeShells, you can edit the *Start Date* and *End Date* fields to only show events within that time frame. For this, I set the Start Date on 03/01/2021 and End Date on 03/08/2021:



EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME	L
3/1/2021 6:05:18 AM	Desktop Last Accessed	Item Last Access	User	Desktop	M
3/1/2021 6:05:32 AM	Documents Last Accessed	Item Last Access	User	Documents	M
3/1/2021 6:05:42 AM	Favorites Last Accessed	Item Last Access	User	Favorites	M
3/1/2021 6:05:42 AM	Links Last Accessed	Item Last Access	User	Links	M
3/1/2021 6:05:42 AM	source Last Accessed	Item Last Access	User	source	M
3/1/2021 6:05:42 AM	IISExpress Last Accessed	Item Last Access	User	IISExpress	M
3/1/2021 6:05:42 AM	My Web Sites Last Accessed	Item Last Access	User	My Web Sites	M
3/1/2021 6:05:42 AM	Visual Studio 2019 Last Accessed	Item Last Access	User	Visual Studio 2019	M
3/1/2021 6:05:42 AM	Code Snippets Last Accessed	Item Last Access	User	Code Snippets	M
3/1/2021 6:05:42 AM	Templates Last Accessed	Item Last Access	User	Templates	M
3/1/2021 6:05:42 AM	SQL_SSDT Last Accessed	Item Last Access	User	SQL_SSDT	M
3/1/2021 6:05:42 AM	Visual Web Developer Last Accessed	Item Last Access	User	Visual Web Developer	M
3/1/2021 6:05:42 AM	XML Last Accessed	Item Last Access	User	XML	M

Keyword	
Event Type	
Path	
User	
Registry Hive	
Begin Date	3/1/2021 12:00:00 AM
End Date	3/8/2021 12:00:00 AM

Figure 2. Changing up the Event Date Filter

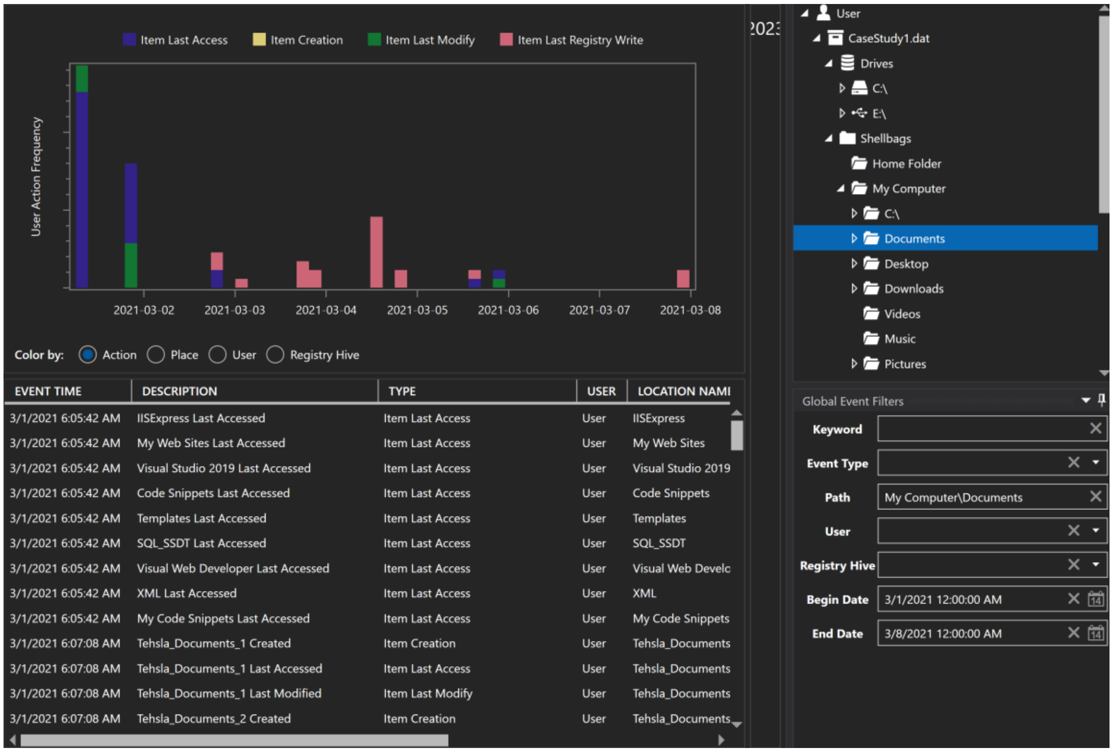
From the situation description, the company was not able to figure out what specific confidential information is found, so currently it is not possible to filter by event name. Looking around at the folder names could show what could potentially be intellectual property (IP). IP is any information, property, or asset that the company owns which is prohibited from outside use or distribution.

From the directory names, we can figure out the company, industry, and potential IP items. The following are directory names that were found that are indicative of the industry:

- *Self_Driving_Code*
- *2020 Car Designs*
- *Self Driving Comp Code*
- *Electric Motor Blueprint*

We see that the employee definitely had access to those files and was able to modify them. Though so far there’s no evidence that he took them from his work computer.

We can now use the Registry panel to navigate to ‘My Computer/Documents’ folder. If we click on this, the events will automatically filter all shell events pertaining to that folder. We now have further narrowed down the number of events we are looking at.



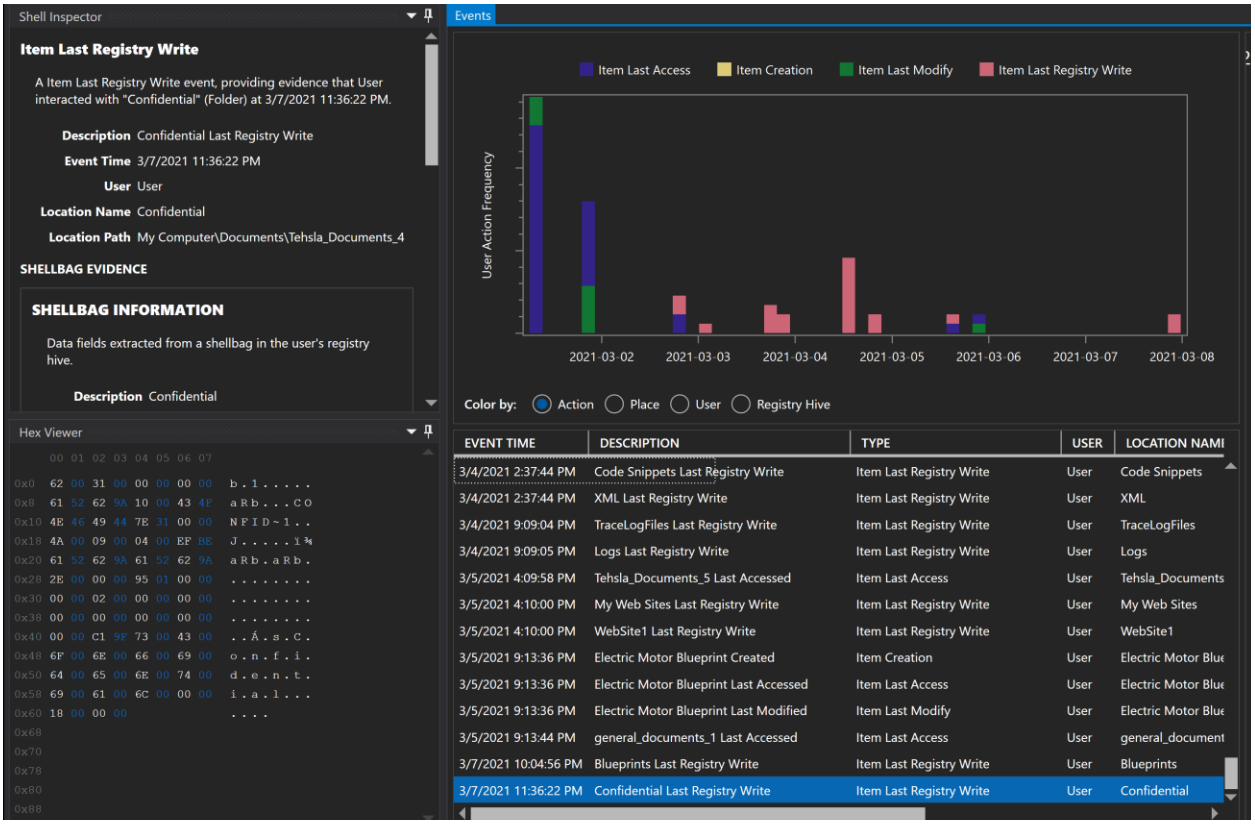
Color by: ● Action ○ Place ○ User ○ Registry Hive

EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAMI
3/1/2021 6:05:42 AM	IISExpress Last Accessed	Item Last Access	User	IISExpress
3/1/2021 6:05:42 AM	My Web Sites Last Accessed	Item Last Access	User	My Web Sites
3/1/2021 6:05:42 AM	Visual Studio 2019 Last Accessed	Item Last Access	User	Visual Studio 2019
3/1/2021 6:05:42 AM	Code Snippets Last Accessed	Item Last Access	User	Code Snippets
3/1/2021 6:05:42 AM	Templates Last Accessed	Item Last Access	User	Templates
3/1/2021 6:05:42 AM	SQL_SSDT Last Accessed	Item Last Access	User	SQL_SSDT
3/1/2021 6:05:42 AM	Visual Web Developer Last Accessed	Item Last Access	User	Visual Web Develc
3/1/2021 6:05:42 AM	XML Last Accessed	Item Last Access	User	XML
3/1/2021 6:05:42 AM	My Code Snippets Last Accessed	Item Last Access	User	My Code Snippets
3/1/2021 6:07:08 AM	Tehsla_Documents_1 Created	Item Creation	User	Tehsla_Documents
3/1/2021 6:07:08 AM	Tehsla_Documents_1 Last Accessed	Item Last Access	User	Tehsla_Documents
3/1/2021 6:07:08 AM	Tehsla_Documents_1 Last Modified	Item Last Modify	User	Tehsla_Documents
3/1/2021 6:07:08 AM	Tehsla_Documents_2 Created	Item Creation	User	Tehsla_Documents

Keyword	
Event Type	
Path	My Computer\Documents
User	
Registry Hive	
Begin Date	3/1/2021 12:00:00 AM
End Date	3/8/2021 12:00:00 AM

Figure 4. Adding more filtering to narrow down the events

On March 7th, it is observed that the employee viewed several directories within the folder labeled *Confidential*, created another folder *Files*, and copied directories under that *Confidential* folder into the new folder *Files*.



Item Last Registry Write

A Item Last Registry Write event, providing evidence that User interacted with "Confidential" (Folder) at 3/7/2021 11:36:22 PM.

Description Confidential Last Registry Write
Event Time 3/7/2021 11:36:22 PM
User User
Location Name Confidential
Location Path My Computer\Documents\Tehsla_Documents_4

SHELLBAG EVIDENCE

SHELLBAG INFORMATION

Data fields extracted from a shellbag in the user's registry hive.

Description Confidential

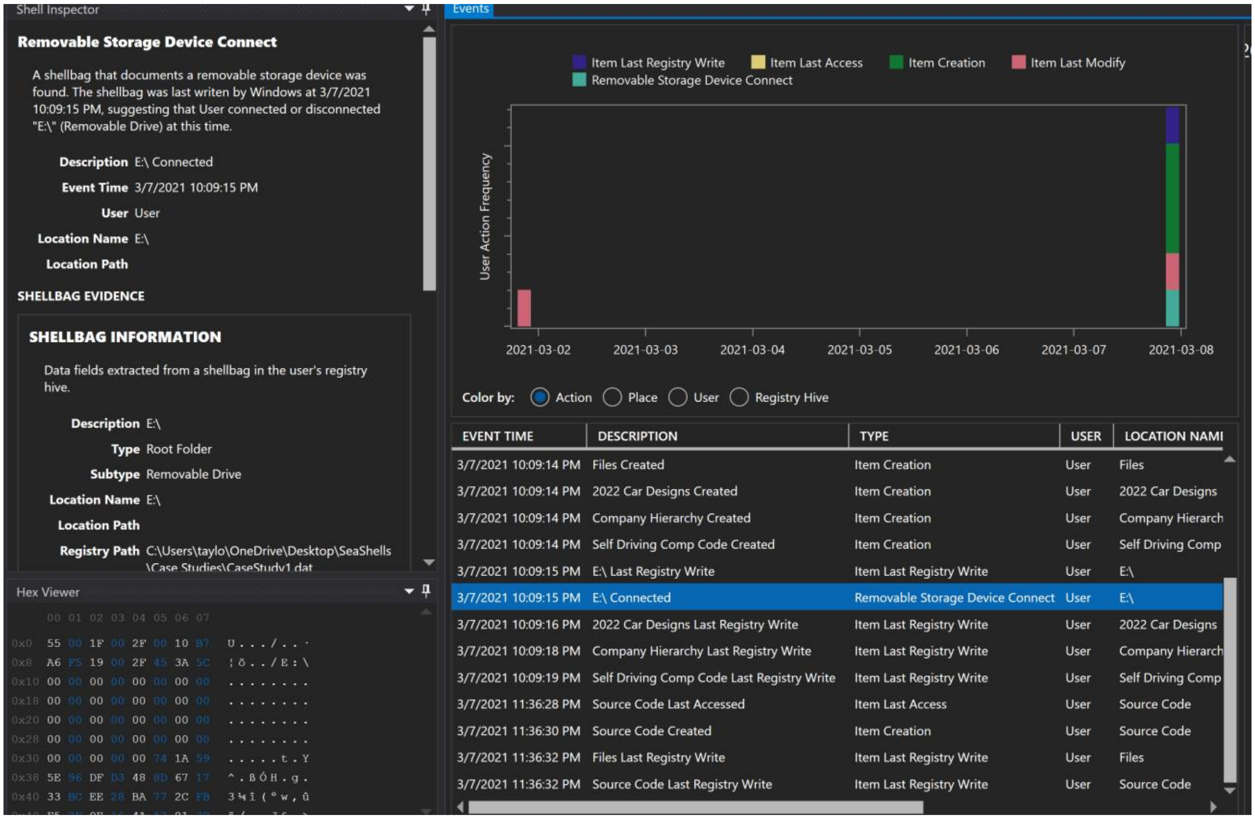
```
      00 01 02 03 04 05 06 07
0x0   62 00 31 00 00 00 00 00   b.1.....
0x8   61 52 62 9A 10 00 43 4F   aRb...CO
0x10  4E 46 49 44 7E 31 00 00   NFID~1..
0x18  4A 00 09 00 04 00 EF BE   J.....ï¾
0x20  61 52 62 9A 61 52 62 9A   aRb.aRb.
0x28  2E 00 00 00 95 01 00 00   ........
0x30  00 00 02 00 00 00 00 00   ........
0x38  00 00 00 00 00 00 00 00   ........
0x40  00 00 C1 9F 73 00 43 00   ..Á.s.C.
0x48  6F 00 6E 00 66 00 69 00   o.n.f.i.
0x50  64 00 65 00 6E 00 74 00   d.e.n.t.
0x58  69 00 61 00 6C 00 00 00   i.a.l...
0x60  18 00 00 00               ....
0x68
0x70
0x78
0x80
0x88
```

Color by: ● Action ○ Place ○ User ○ Registry Hive

EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAMI
3/4/2021 2:37:44 PM	Code Snippets Last Registry Write	Item Last Registry Write	User	Code Snippets
3/4/2021 2:37:44 PM	XML Last Registry Write	Item Last Registry Write	User	XML
3/4/2021 9:09:04 PM	TraceLogFiles Last Registry Write	Item Last Registry Write	User	TraceLogFiles
3/4/2021 9:09:05 PM	Logs Last Registry Write	Item Last Registry Write	User	Logs
3/5/2021 4:09:58 PM	Tehsla_Documents_5 Last Accessed	Item Last Access	User	Tehsla_Documents
3/5/2021 4:10:00 PM	My Web Sites Last Registry Write	Item Last Registry Write	User	My Web Sites
3/5/2021 4:10:00 PM	WebSite1 Last Registry Write	Item Last Registry Write	User	WebSite1
3/5/2021 9:13:36 PM	Electric Motor Blueprint Created	Item Creation	User	Electric Motor Blue
3/5/2021 9:13:36 PM	Electric Motor Blueprint Last Accessed	Item Last Access	User	Electric Motor Blue
3/5/2021 9:13:36 PM	Electric Motor Blueprint Last Modified	Item Last Modify	User	Electric Motor Blue
3/5/2021 9:13:44 PM	general_documents_1 Last Accessed	Item Last Access	User	general_document
3/7/2021 10:04:56 PM	Blueprints Last Registry Write	Item Last Registry Write	User	Blueprints
3/7/2021 11:36:22 PM	Confidential Last Registry Write	Item Last Registry Write	User	Confidential

Figure 5. Creation of a folder named Files

Furthermore, filtering out the types of events to Removable Storage Device Connect by clicking on it, will grey out everything and show that a drive named “E:\” was connected. Clicking on it will show that it is a removable storage device that was connected in the interested timeframe.



Removable Storage Device Connect

A shellbag that documents a removable storage device was found. The shellbag was last writen by Windows at 3/7/2021 10:09:15 PM, suggesting that User connected or disconnected "E:\" (Removable Drive) at this time.

Description E:\ Connected
Event Time 3/7/2021 10:09:15 PM
User User
Location Name E:\
Location Path

SHELLBAG EVIDENCE

SHELLBAG INFORMATION

Data fields extracted from a shellbag in the user's registry hive.

Description E:\
Type Root Folder
Subtype Removable Drive
Location Name E:\
Location Path
Registry Path C:\Users\taylo\OneDrive\Desktop\SeaShells\Case Studies\CaseStudy1.dat

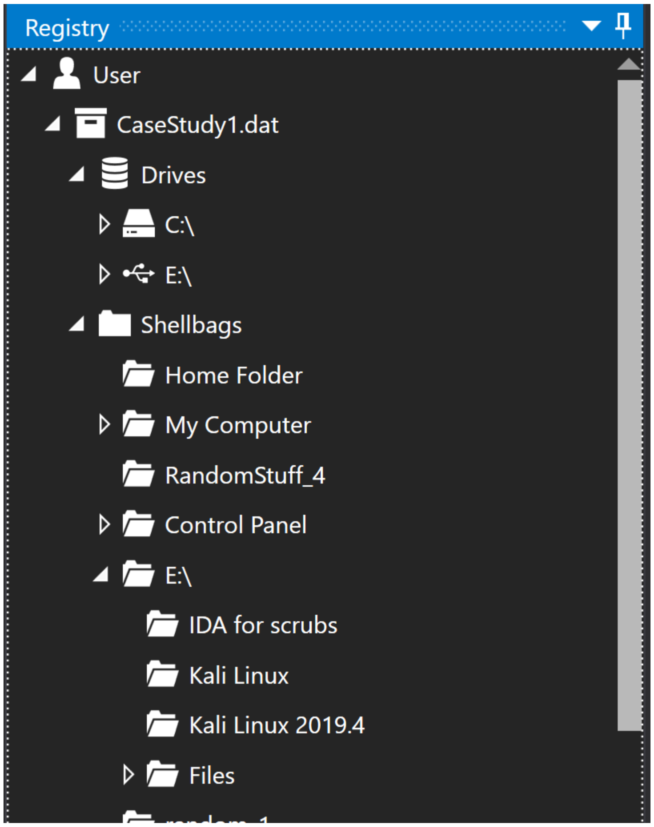
```
     00 01 02 03 04 05 06 07
0x0  55 00 1F 00 2F 00 10 B7   U . . . / . . ·
0x8  A6 F5 19 00 2F 45 3A 5C   ¦ õ . . / E : \
0x10 00 00 00 00 00 00 00 00   . . . . . . . .
0x18 00 00 00 00 00 00 00 00   . . . . . . . .
0x20 00 00 00 00 00 00 00 00   . . . . . . . .
0x28 00 00 00 00 00 00 00 00   . . . . . . . .
0x30 00 00 00 00 00 74 1A 59   . . . . . t . Y
0x38 5E 96 DF D3 48 8D 67 17   ^ . ß Ó H . g .
0x40 33 BC EE 28 BA 77 2C FB   3 ¼ î ( º w , û
```

Color by: ● Action ○ Place ○ User ○ Registry Hive

EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAMI
3/7/2021 10:09:14 PM	Files Created	Item Creation	User	Files
3/7/2021 10:09:14 PM	2022 Car Designs Created	Item Creation	User	2022 Car Designs
3/7/2021 10:09:14 PM	Company Hierarchy Created	Item Creation	User	Company Hierarch
3/7/2021 10:09:14 PM	Self Driving Comp Code Created	Item Creation	User	Self Driving Comp
3/7/2021 10:09:15 PM	E:\ Last Registry Write	Item Last Registry Write	User	E:\
3/7/2021 10:09:15 PM	E:\ Connected	Removable Storage Device Connect	User	E:\
3/7/2021 10:09:16 PM	2022 Car Designs Last Registry Write	Item Last Registry Write	User	2022 Car Designs
3/7/2021 10:09:18 PM	Company Hierarchy Last Registry Write	Item Last Registry Write	User	Company Hierarch
3/7/2021 10:09:19 PM	Self Driving Comp Code Last Registry Write	Item Last Registry Write	User	Self Driving Comp
3/7/2021 11:36:28 PM	Source Code Last Accessed	Item Last Access	User	Source Code
3/7/2021 11:36:30 PM	Source Code Created	Item Creation	User	Source Code
3/7/2021 11:36:32 PM	Files Last Registry Write	Item Last Registry Write	User	Files
3/7/2021 11:36:32 PM	Source Code Last Registry Write	Item Last Registry Write	User	Source Code

Figure 6. Getting proof some type of external device was last plugged in before the post date with confidential files within them

On the right hand side, the registry view will show what the filesystem looked like. We can expand "Drives" and see both the C drive (the main computer) and the E drive (the external device). We can expand on the E drive which shows a few folders, one of which is the same Files folder we found earlier. Expanding on that we see the following folders:



Registry

- User
  - CaseStudy1.dat
    - Drives
      - C:\
      - E:\
    - Shellbags
      - Home Folder
      - My Computer
      - RandomStuff_4
      - Control Panel
      - E:\
        - IDA for scrubs
        - Kali Linux
        - Kali Linux 2019.4
        - Files
      - random_1

Figure 7. The same files in that external hard drive can be found under the Confidential Folder

Conclusion:

There is definitive proof that this employee copied several confidential files from their work computer onto some type of external hard drive (E:) on 03/07/2021 at 22:09. Furthermore, using ShellBags information we were able to find evidence that several files such as the 2022 Car Designs, Corporate Hierarchy, Self Driving Computer Code, and Source Code were all taken from the company computer. Even though that external device is no longer attached to the system, the Windows Registry (more specifically ShellBags) was able to log information regarding folders that have existed on this device.