Case Study #1 Writeup

Situation:

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 wasn’t able to 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 crash. However, the company does not have definitive proof that this particular employee was the one who did it so they 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?

Guide:

One of the first things that can be seen is the large timeline of the events spanning from 2019 to March 2021:

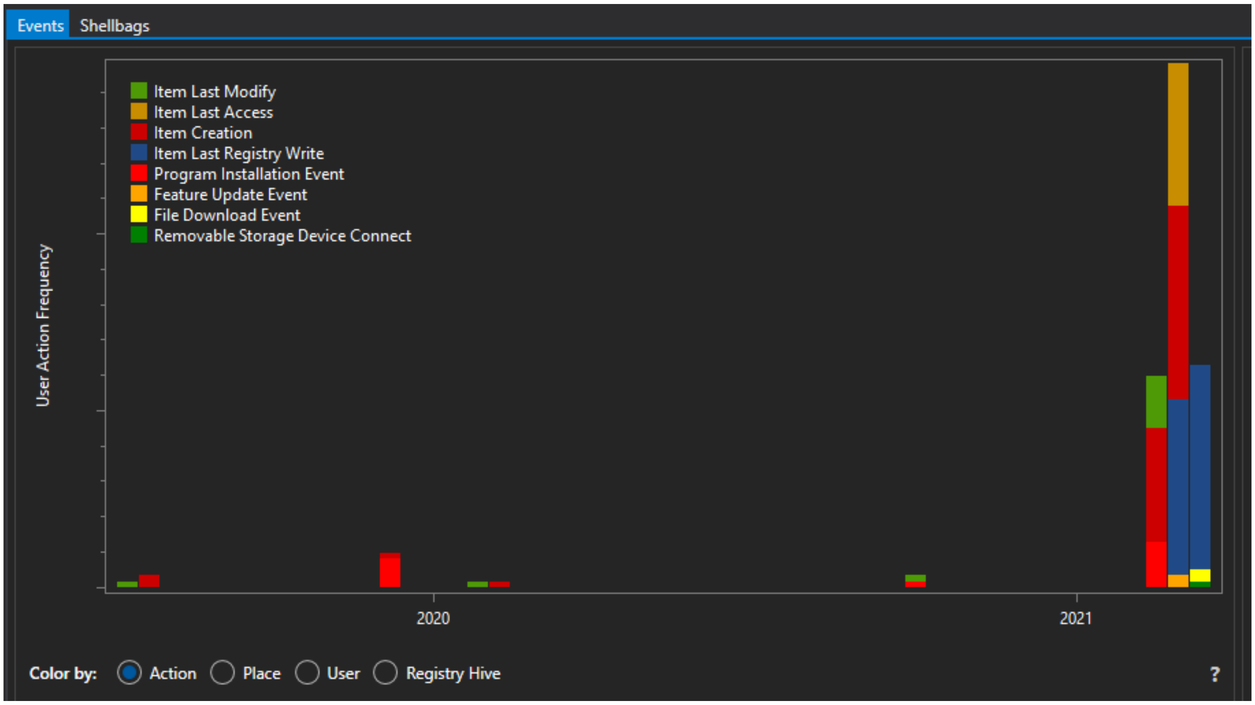
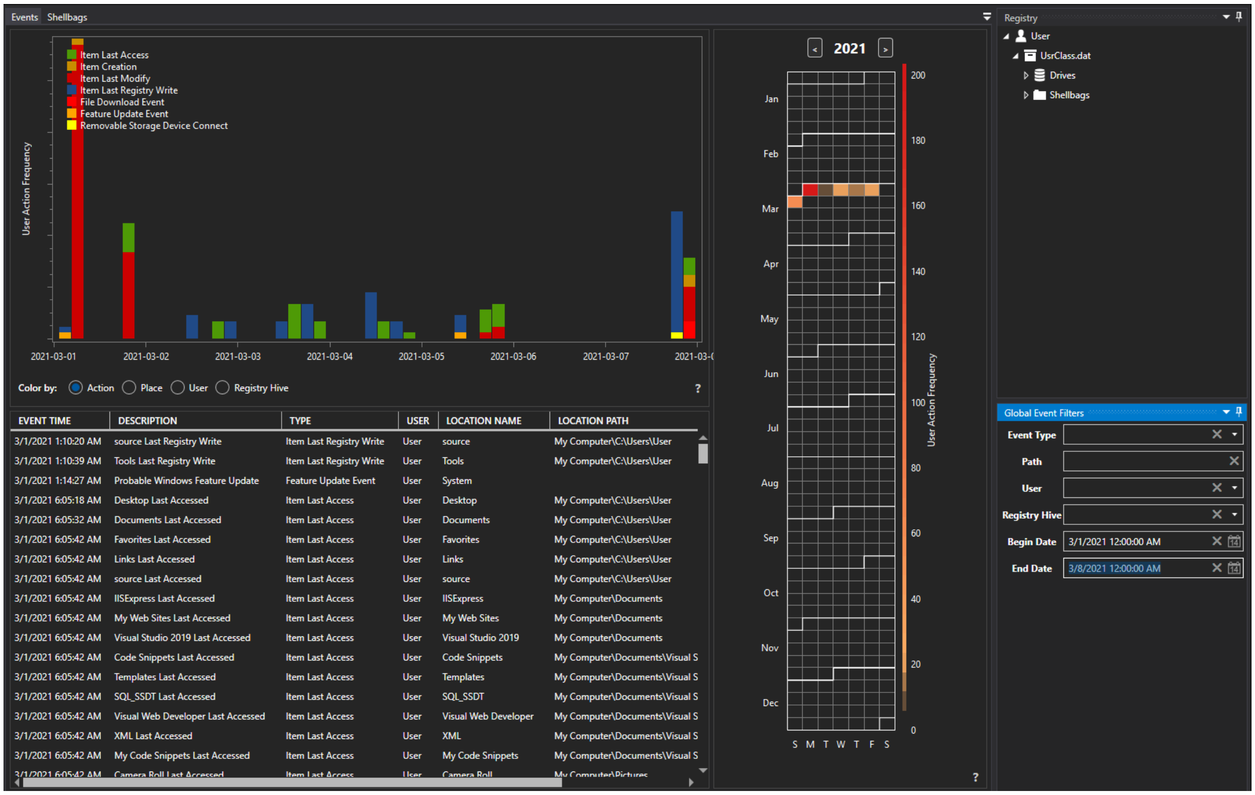


Figure 1. Showing one of the first events in 2019

One thing that can be done to reduce the amount of events shown and to filter out some events, we can use SeeShells *Global Events Filter*. One of the key details about the investigation is the timeline of incidents. 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:



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

EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME	LOCATION PATH
3/1/2021 1:10:20 AM	source Last Registry Write	Item Last Registry Write	User	source	My Computer\C:\Users\User
3/1/2021 1:10:39 AM	Tools Last Registry Write	Item Last Registry Write	User	Tools	My Computer\C:\Users\User
3/1/2021 1:14:27 AM	Probable Windows Feature Update	Feature Update Event	User	System	
3/1/2021 6:05:18 AM	Desktop Last Accessed	Item Last Access	User	Desktop	My Computer\C:\Users\User
3/1/2021 6:05:32 AM	Documents Last Accessed	Item Last Access	User	Documents	My Computer\C:\Users\User
3/1/2021 6:05:42 AM	Favorites Last Accessed	Item Last Access	User	Favorites	My Computer\C:\Users\User
3/1/2021 6:05:42 AM	Links Last Accessed	Item Last Access	User	Links	My Computer\C:\Users\User
3/1/2021 6:05:42 AM	source Last Accessed	Item Last Access	User	source	My Computer\C:\Users\User
3/1/2021 6:05:42 AM	IISExpress Last Accessed	Item Last Access	User	IISExpress	My Computer\Documents
3/1/2021 6:05:42 AM	My Web Sites Last Accessed	Item Last Access	User	My Web Sites	My Computer\Documents
3/1/2021 6:05:42 AM	Visual Studio 2019 Last Accessed	Item Last Access	User	Visual Studio 2019	My Computer\Documents
3/1/2021 6:05:42 AM	Code Snippets Last Accessed	Item Last Access	User	Code Snippets	My Computer\Documents\Visual S
3/1/2021 6:05:42 AM	Templates Last Accessed	Item Last Access	User	Templates	My Computer\Documents\Visual S
3/1/2021 6:05:42 AM	SQL_SSDT Last Accessed	Item Last Access	User	SQL_SSDT	My Computer\Documents\Visual S
3/1/2021 6:05:42 AM	Visual Web Developer Last Accessed	Item Last Access	User	Visual Web Developer	My Computer\Documents\Visual S
3/1/2021 6:05:42 AM	XML Last Accessed	Item Last Access	User	XML	My Computer\Documents\Visual S
3/1/2021 6:05:42 AM	My Code Snippets Last Accessed	Item Last Access	User	My Code Snippets	My Computer\Documents\Visual S
3/1/2021 6:05:42 AM	Camera Roll Last Accessed	Item Last Access	User	Camera Roll	My Computer\Pictures

Global Event Filters

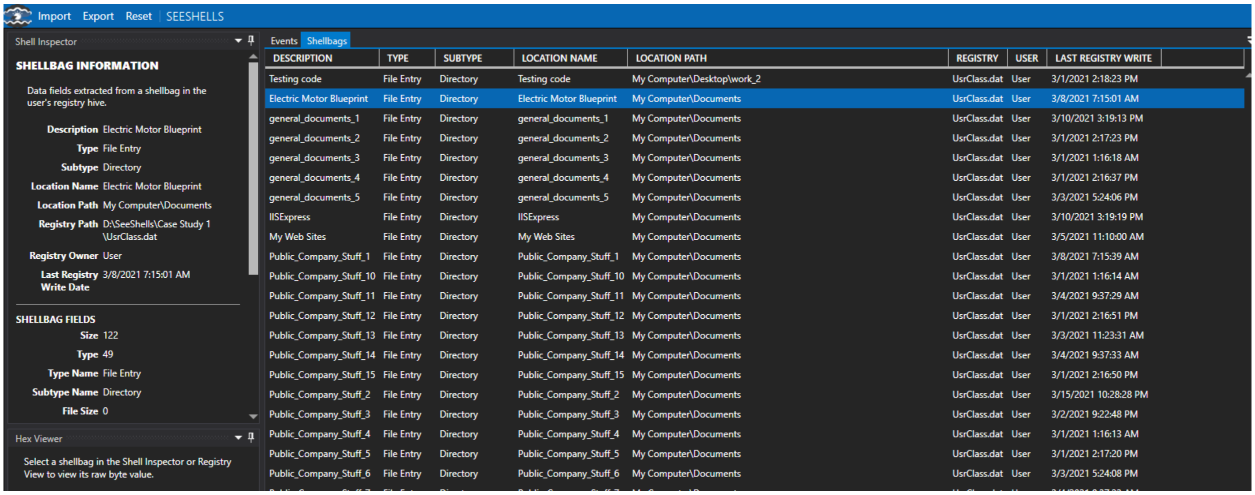
Event Type	
Path	
User	
Registry Hive	
Begin Date	3/1/2021 12:00:00 AM
End Date	3/8/2021 12:00:00 AM

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*



SHELLBAG INFORMATION

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

Description: Electric Motor Blueprint
Type: File Entry
Subtype: Directory
Location Name: Electric Motor Blueprint
Location Path: My Computer\Documents
Registry Path: D:\SeeShells\Case Study 1\UsrClass.dat
Registry Owner: User
Last Registry Write Date: 3/8/2021 7:15:01 AM

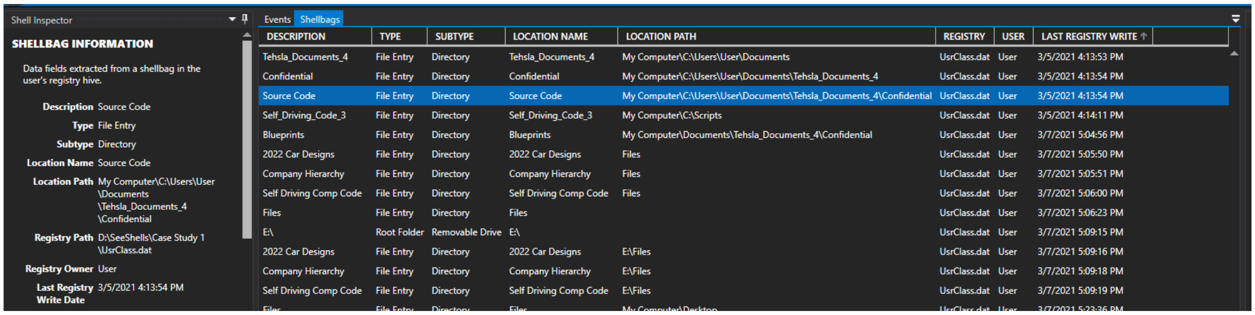
SHELLBAG FIELDS
Size: 122
Type: 49
Type Name: File Entry
Subtype Name: Directory
File Size: 0

Select a shellbag in the Shell Inspector or Registry View to view its raw byte value.

DESCRIPTION	TYPE	SUBTYPE	LOCATION NAME	LOCATION PATH	REGISTRY	USER	LAST REGISTRY WRITE
Testing code	File Entry	Directory	Testing code	My Computer\Desktop\work_2	UsrClass.dat	User	3/1/2021 2:18:23 PM
Electric Motor Blueprint	File Entry	Directory	Electric Motor Blueprint	My Computer\Documents	UsrClass.dat	User	3/8/2021 7:15:01 AM
general_documents_1	File Entry	Directory	general_documents_1	My Computer\Documents	UsrClass.dat	User	3/10/2021 3:19:13 PM
general_documents_2	File Entry	Directory	general_documents_2	My Computer\Documents	UsrClass.dat	User	3/1/2021 2:17:23 PM
general_documents_3	File Entry	Directory	general_documents_3	My Computer\Documents	UsrClass.dat	User	3/1/2021 1:16:18 AM
general_documents_4	File Entry	Directory	general_documents_4	My Computer\Documents	UsrClass.dat	User	3/1/2021 2:16:37 PM
general_documents_5	File Entry	Directory	general_documents_5	My Computer\Documents	UsrClass.dat	User	3/3/2021 5:24:06 PM
IISExpress	File Entry	Directory	IISExpress	My Computer\Documents	UsrClass.dat	User	3/10/2021 3:19:19 PM
My Web Sites	File Entry	Directory	My Web Sites	My Computer\Documents	UsrClass.dat	User	3/5/2021 11:10:00 AM
Public_Company_Stuff_1	File Entry	Directory	Public_Company_Stuff_1	My Computer\Documents	UsrClass.dat	User	3/8/2021 7:15:39 AM
Public_Company_Stuff_10	File Entry	Directory	Public_Company_Stuff_10	My Computer\Documents	UsrClass.dat	User	3/1/2021 1:16:14 AM
Public_Company_Stuff_11	File Entry	Directory	Public_Company_Stuff_11	My Computer\Documents	UsrClass.dat	User	3/4/2021 9:37:29 AM
Public_Company_Stuff_12	File Entry	Directory	Public_Company_Stuff_12	My Computer\Documents	UsrClass.dat	User	3/1/2021 2:16:51 PM
Public_Company_Stuff_13	File Entry	Directory	Public_Company_Stuff_13	My Computer\Documents	UsrClass.dat	User	3/3/2021 11:23:31 AM
Public_Company_Stuff_14	File Entry	Directory	Public_Company_Stuff_14	My Computer\Documents	UsrClass.dat	User	3/4/2021 9:37:33 AM
Public_Company_Stuff_15	File Entry	Directory	Public_Company_Stuff_15	My Computer\Documents	UsrClass.dat	User	3/1/2021 2:16:50 PM
Public_Company_Stuff_2	File Entry	Directory	Public_Company_Stuff_2	My Computer\Documents	UsrClass.dat	User	3/15/2021 10:28:28 PM
Public_Company_Stuff_3	File Entry	Directory	Public_Company_Stuff_3	My Computer\Documents	UsrClass.dat	User	3/2/2021 9:22:48 PM
Public_Company_Stuff_4	File Entry	Directory	Public_Company_Stuff_4	My Computer\Documents	UsrClass.dat	User	3/1/2021 1:16:13 AM
Public_Company_Stuff_5	File Entry	Directory	Public_Company_Stuff_5	My Computer\Documents	UsrClass.dat	User	3/1/2021 2:17:20 PM
Public_Company_Stuff_6	File Entry	Directory	Public_Company_Stuff_6	My Computer\Documents	UsrClass.dat	User	3/3/2021 5:24:08 PM

Figure 3. Finding one of the folders that can potentially be IP

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.



SHELLBAG INFORMATION

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

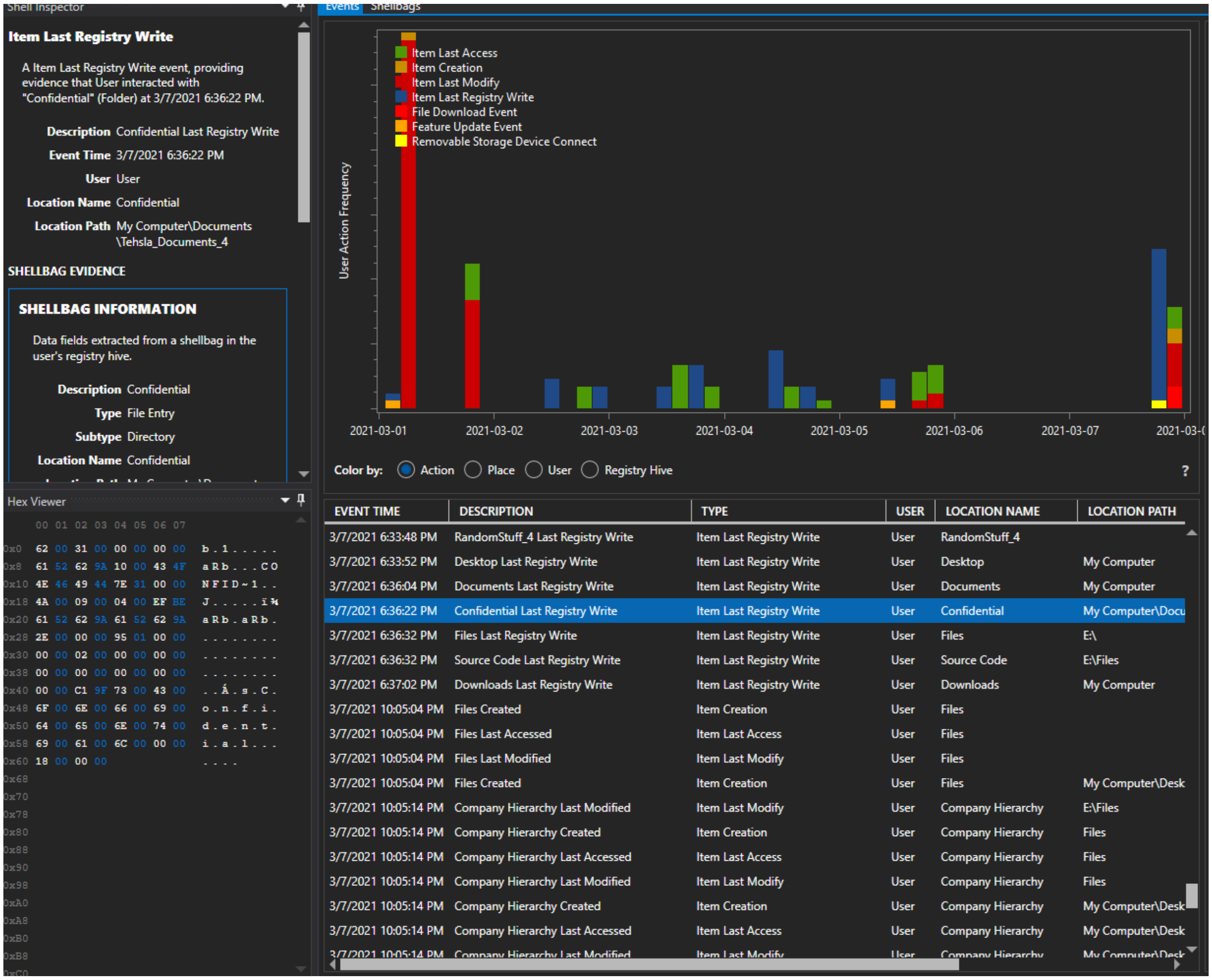
Description Source Code
Type File Entry
Subtype Directory
Location Name Source Code
Location Path My Computer\C:\Users\User\Documents\Tehsla_Documents_4\Confidential
Registry Path D:\SeeShells\Case Study 1\UsrClass.dat
Registry Owner User
Last Registry Write Date 3/5/2021 4:13:54 PM

DESCRIPTION	TYPE	SUBTYPE	LOCATION NAME	LOCATION PATH	REGISTRY	USER	LAST REGISTRY WRITE ↑
Tehsla_Documents_4	File Entry	Directory	Tehsla_Documents_4	My Computer\C:\Users\User\Documents	UsrClass.dat	User	3/5/2021 4:13:53 PM
Confidential	File Entry	Directory	Confidential	My Computer\C:\Users\User\Documents\Tehsla_Documents_4	UsrClass.dat	User	3/5/2021 4:13:54 PM
Source Code	File Entry	Directory	Source Code	My Computer\C:\Users\User\Documents\Tehsla_Documents_4\Confidential	UsrClass.dat	User	3/5/2021 4:13:54 PM
Self_Driving_Code_3	File Entry	Directory	Self_Driving_Code_3	My Computer\C:\Scripts	UsrClass.dat	User	3/5/2021 4:14:11 PM
Blueprints	File Entry	Directory	Blueprints	My Computer\Documents\Tehsla_Documents_4\Confidential	UsrClass.dat	User	3/7/2021 5:04:56 PM
2022 Car Designs	File Entry	Directory	2022 Car Designs	Files	UsrClass.dat	User	3/7/2021 5:05:50 PM
Company Hierarchy	File Entry	Directory	Company Hierarchy	Files	UsrClass.dat	User	3/7/2021 5:05:51 PM
Self Driving Comp Code	File Entry	Directory	Self Driving Comp Code	Files	UsrClass.dat	User	3/7/2021 5:06:00 PM
Files	File Entry	Directory	Files		UsrClass.dat	User	3/7/2021 5:06:23 PM
E:\	Root Folder	Removable Drive	E:\		UsrClass.dat	User	3/7/2021 5:09:15 PM
2022 Car Designs	File Entry	Directory	2022 Car Designs	E:\Files	UsrClass.dat	User	3/7/2021 5:09:16 PM
Company Hierarchy	File Entry	Directory	Company Hierarchy	E:\Files	UsrClass.dat	User	3/7/2021 5:09:18 PM
Self Driving Comp Code	File Entry	Directory	Self Driving Comp Code	E:\Files	UsrClass.dat	User	3/7/2021 5:09:19 PM
Files	File Entry	Directory	Files	My Computer\Desktop	UsrClass.dat	User	3/7/2021 5:23:36 PM

Figure 4. Showing another interesting directory within the timeframe

It is clear that this company is an electric vehicle company that also has specialization in self driving technology which is highly valued. Though it is worth noting that there are other directories within the environment and not all are suspicious files, such as general folders like *Tehsla_Documents_1*. Also since he was an internal employee, he is allowed legitimate access to those internal documents and so far there's no evidence he has taken anything outside the company's work environment. By continuing to walk up the dates there is interesting activity found the day before the IP is posted online for sale on the deep web (03/08/2021).

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 6:36:22 PM.

Description Confidential Last Registry Write
Event Time 3/7/2021 6:36:22 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
Type File Entry
Subtype Directory
Location Name Confidential

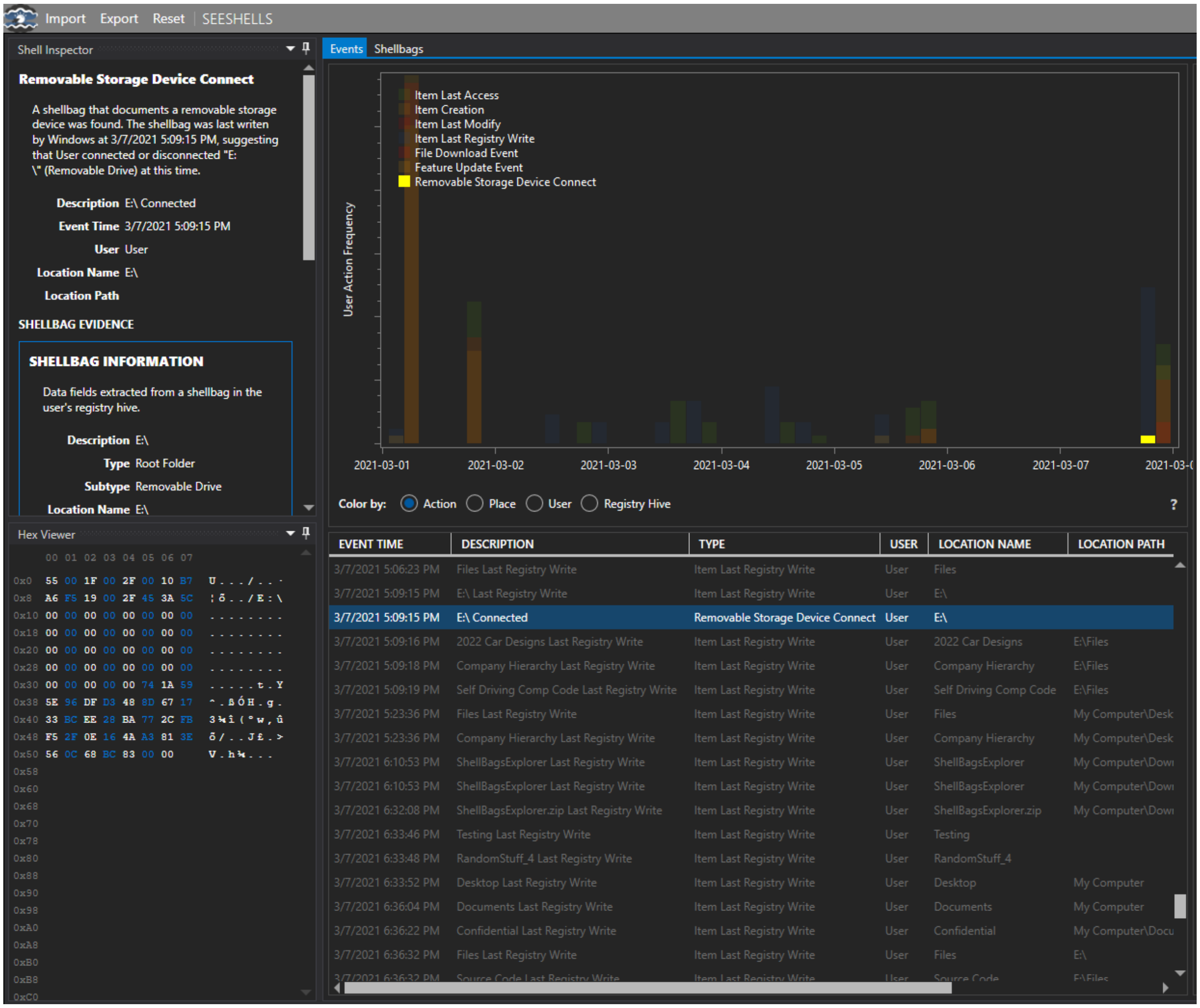
```
      00 01 02 03 04 05 06 07
0x0   62 00 31 00 00 00 00 00   b.1.....
0x8   61 52 62 9A 10 00 43 4F   aRb...CO
0x10  4E 46 49 44 7E 31 00 00   NFID~1..
0x18  4A 00 09 00 04 00 EF BE   J.....ï¾
0x20  61 52 62 9A 61 52 62 9A   aRb.aRb.
0x28  2E 00 00 00 95 01 00 00   ........
0x30  00 00 02 00 00 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
0x90
0x98
0xA0
0xA8
0xB0
0xB8
0xC0
```

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

EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME	LOCATION PATH
3/7/2021 6:33:48 PM	RandomStuff_4 Last Registry Write	Item Last Registry Write	User	RandomStuff_4	
3/7/2021 6:33:52 PM	Desktop Last Registry Write	Item Last Registry Write	User	Desktop	My Computer
3/7/2021 6:36:04 PM	Documents Last Registry Write	Item Last Registry Write	User	Documents	My Computer
3/7/2021 6:36:22 PM	Confidential Last Registry Write	Item Last Registry Write	User	Confidential	My Computer\Docu
3/7/2021 6:36:32 PM	Files Last Registry Write	Item Last Registry Write	User	Files	E:\
3/7/2021 6:36:32 PM	Source Code Last Registry Write	Item Last Registry Write	User	Source Code	E:\Files
3/7/2021 6:37:02 PM	Downloads Last Registry Write	Item Last Registry Write	User	Downloads	My Computer
3/7/2021 10:05:04 PM	Files Created	Item Creation	User	Files	
3/7/2021 10:05:04 PM	Files Last Accessed	Item Last Access	User	Files	
3/7/2021 10:05:04 PM	Files Last Modified	Item Last Modify	User	Files	
3/7/2021 10:05:04 PM	Files Created	Item Creation	User	Files	My Computer\Desk
3/7/2021 10:05:14 PM	Company Hierarchy Last Modified	Item Last Modify	User	Company Hierarchy	E:\Files
3/7/2021 10:05:14 PM	Company Hierarchy Created	Item Creation	User	Company Hierarchy	Files
3/7/2021 10:05:14 PM	Company Hierarchy Last Accessed	Item Last Access	User	Company Hierarchy	Files
3/7/2021 10:05:14 PM	Company Hierarchy Last Modified	Item Last Modify	User	Company Hierarchy	Files
3/7/2021 10:05:14 PM	Company Hierarchy Created	Item Creation	User	Company Hierarchy	My Computer\Desk
3/7/2021 10:05:14 PM	Company Hierarchy Last Accessed	Item Last Access	User	Company Hierarchy	My Computer\Desk
3/7/2021 10:05:14 PM	Company Hierarchy Last Modified	Item Last Modify	User	Company Hierarchy	My Computer\Desk

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 5:09:15 PM, suggesting that User connected or disconnected "E:\" (Removable Drive) at this time.

Description	E:\ Connected
Event Time	3/7/2021 5:09:15 PM
User	User
Location Name	E:\
Location Path	

SHELLBAG EVIDENCE

SHELLBAG INFORMATION

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

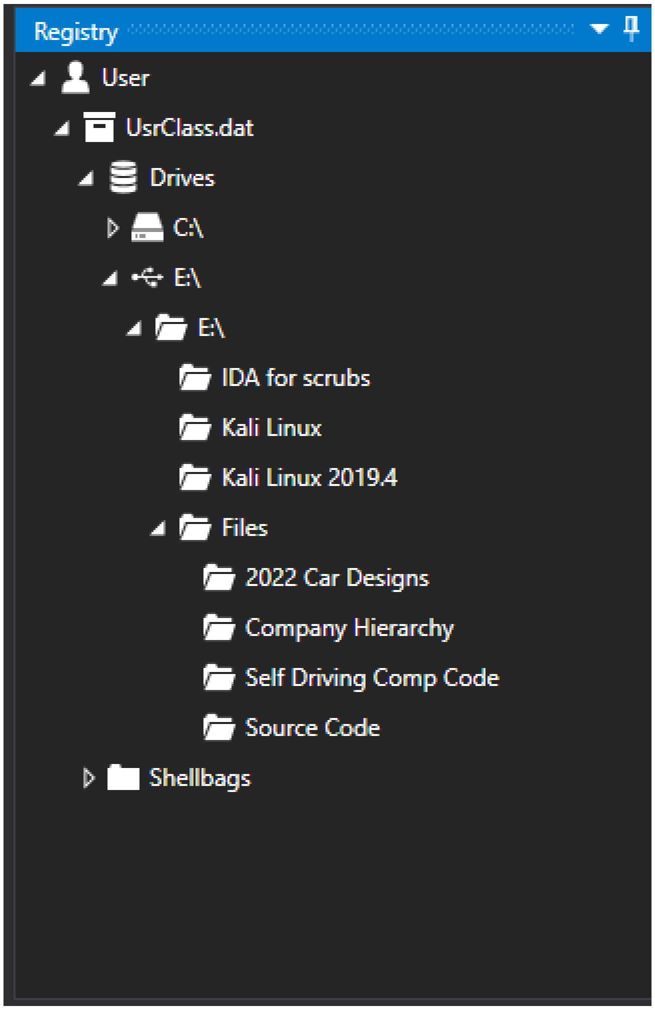
Description	E:\
Type	Root Folder
Subtype	Removable Drive
Location Name	E:\

```
      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 ( ° w , û
0x48  F5 2F 0E 16 4A A3 81 3E   õ / . . J £ . >
0x50  56 0C 68 BC 83 00 00      V . h ¼ . . .
0x58
0x60
0x68
0x70
0x78
0x80
0x88
0x90
0x98
0xA0
0xA8
0xB0
0xB8
0xC0
```

EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME	LOCATION PATH
3/7/2021 5:06:23 PM	Files Last Registry Write	Item Last Registry Write	User	Files	
3/7/2021 5:09:15 PM	E:\ Last Registry Write	Item Last Registry Write	User	E:\	
3/7/2021 5:09:15 PM	E:\ Connected	Removable Storage Device Connect	User	E:\	
3/7/2021 5:09:16 PM	2022 Car Designs Last Registry Write	Item Last Registry Write	User	2022 Car Designs	E:\Files
3/7/2021 5:09:18 PM	Company Hierarchy Last Registry Write	Item Last Registry Write	User	Company Hierarchy	E:\Files
3/7/2021 5:09:19 PM	Self Driving Comp Code Last Registry Write	Item Last Registry Write	User	Self Driving Comp Code	E:\Files
3/7/2021 5:23:36 PM	Files Last Registry Write	Item Last Registry Write	User	Files	My Computer\Desk
3/7/2021 5:23:36 PM	Company Hierarchy Last Registry Write	Item Last Registry Write	User	Company Hierarchy	My Computer\Desk
3/7/2021 6:10:53 PM	ShellBagsExplorer Last Registry Write	Item Last Registry Write	User	ShellBagsExplorer	My Computer\Dowı
3/7/2021 6:10:53 PM	ShellBagsExplorer Last Registry Write	Item Last Registry Write	User	ShellBagsExplorer	My Computer\Dowı
3/7/2021 6:32:08 PM	ShellBagsExplorer.zip Last Registry Write	Item Last Registry Write	User	ShellBagsExplorer.zip	My Computer\Dowı
3/7/2021 6:33:46 PM	Testing Last Registry Write	Item Last Registry Write	User	Testing	
3/7/2021 6:33:48 PM	RandomStuff_4 Last Registry Write	Item Last Registry Write	User	RandomStuff_4	
3/7/2021 6:33:52 PM	Desktop Last Registry Write	Item Last Registry Write	User	Desktop	My Computer
3/7/2021 6:36:04 PM	Documents Last Registry Write	Item Last Registry Write	User	Documents	My Computer
3/7/2021 6:36:22 PM	Confidential Last Registry Write	Item Last Registry Write	User	Confidential	My Computer\Docu
3/7/2021 6:36:32 PM	Files Last Registry Write	Item Last Registry Write	User	Files	E:\
3/7/2021 6:36:32 PM	Source Code Last Registry Write	Item Last Registry Write	User	Source Code	E:\Files

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:



```
User
  UsrClass.dat
    Drives
      C:\
      E:\
        E:\
          IDA for scrubs
          Kali Linux
          Kali Linux 2019.4
          Files
            2022 Car Designs
            Company Hierarchy
            Self Driving Comp Code
            Source Code
    Shellbags
```

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.