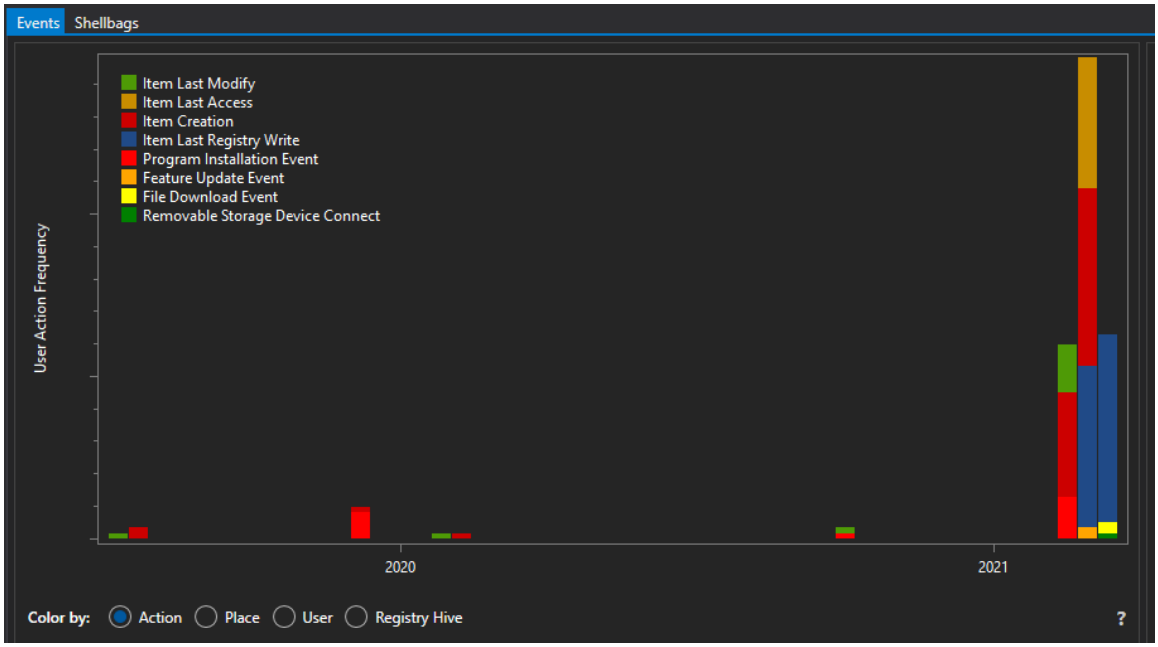
To demonstrate how SeeShells can provide an effectively rich interface for finding shellbag information, a situation, analysis, and results are presented below:

Situation

Assuming the present day is 03/15/2021, while working as a Digital Forensics and Incident Response (DFIR) analyst, you are investigating an insider threat of Intellectual Property (IP) theft case. The company, Tehsla, said their own Cyber Threat Intelligence department found that a person or group was selling a folder on the dark 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. However, the company does not have definitive proof that this 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?

Analysis

Using SeeShells and opening the registry file provided by Tehsla security department, one of the first things that can be seen is the large timeline of the events spanning from 2019 to March 2021 shown in Fig 3.



SeeShells showing one of the first events in 2019.

One thing that can be done to reduce the number of events shown, is to filter out some events using the 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 led 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 as shown in Fig 4.

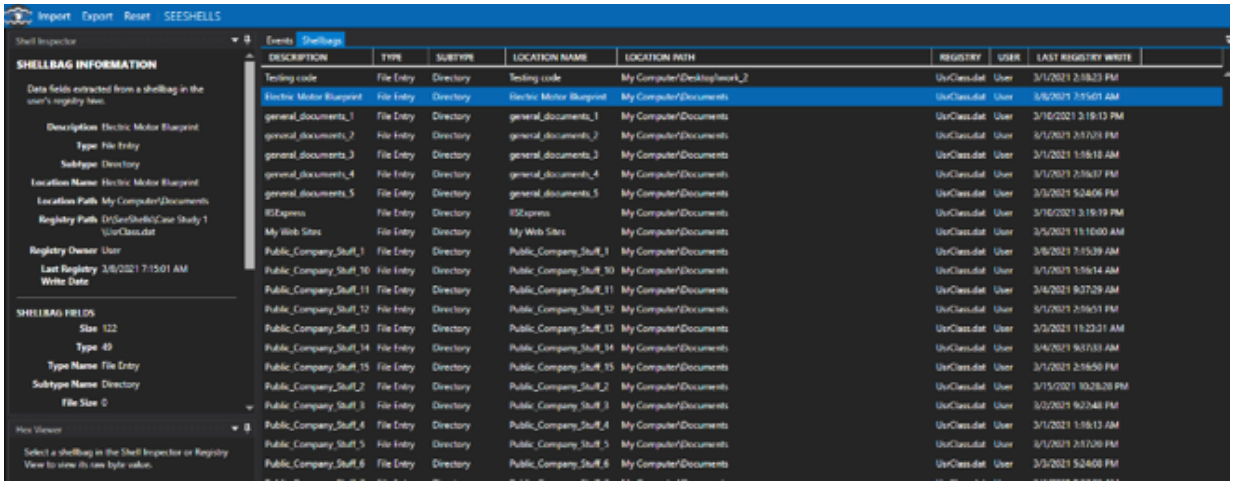
SeeShells using a Start and End Date in the Global Events Filter.

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:

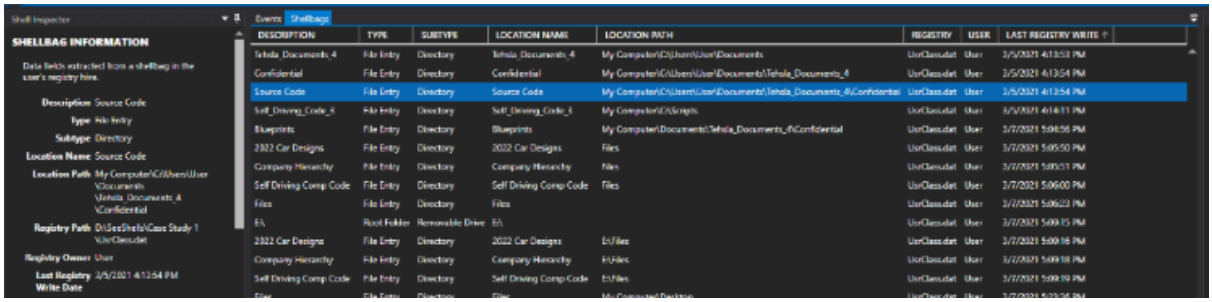
- Self_Driving_Code
- 2020CarDesigns
- SelfDrivingCompCode
- ElectricMotorBlueprint

We see that the employee had access to those files and was able to modify them, shown in Fig 5. Though so far there's no evidence that the employee took them from his or her work computer.



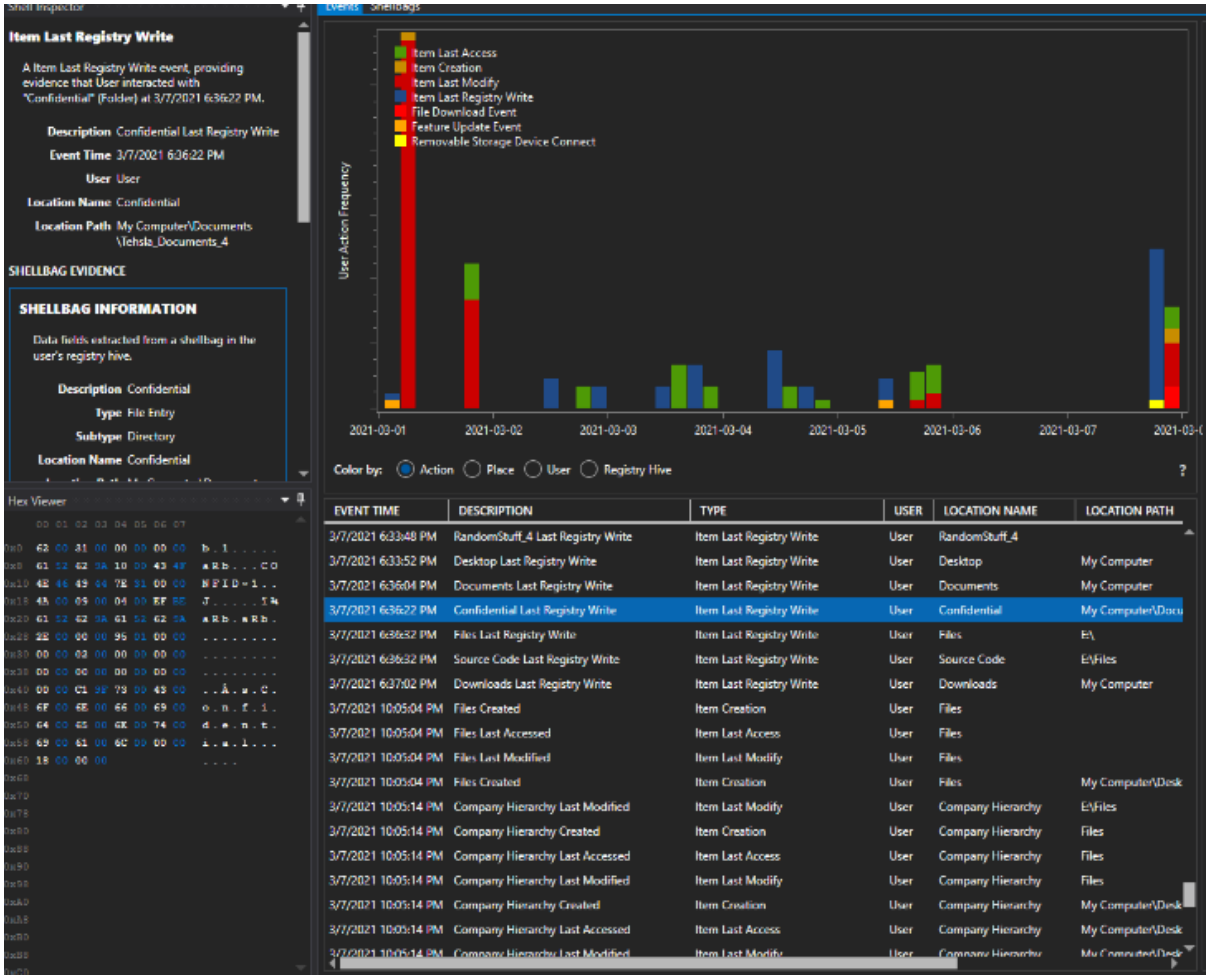
Finding one of the folders that can potentially be IP.

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 the suspect was an internal employee, he or she is allowed legitimate access to those internal documents and so far, there's no evidence they have 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) as shown in Fig 6.



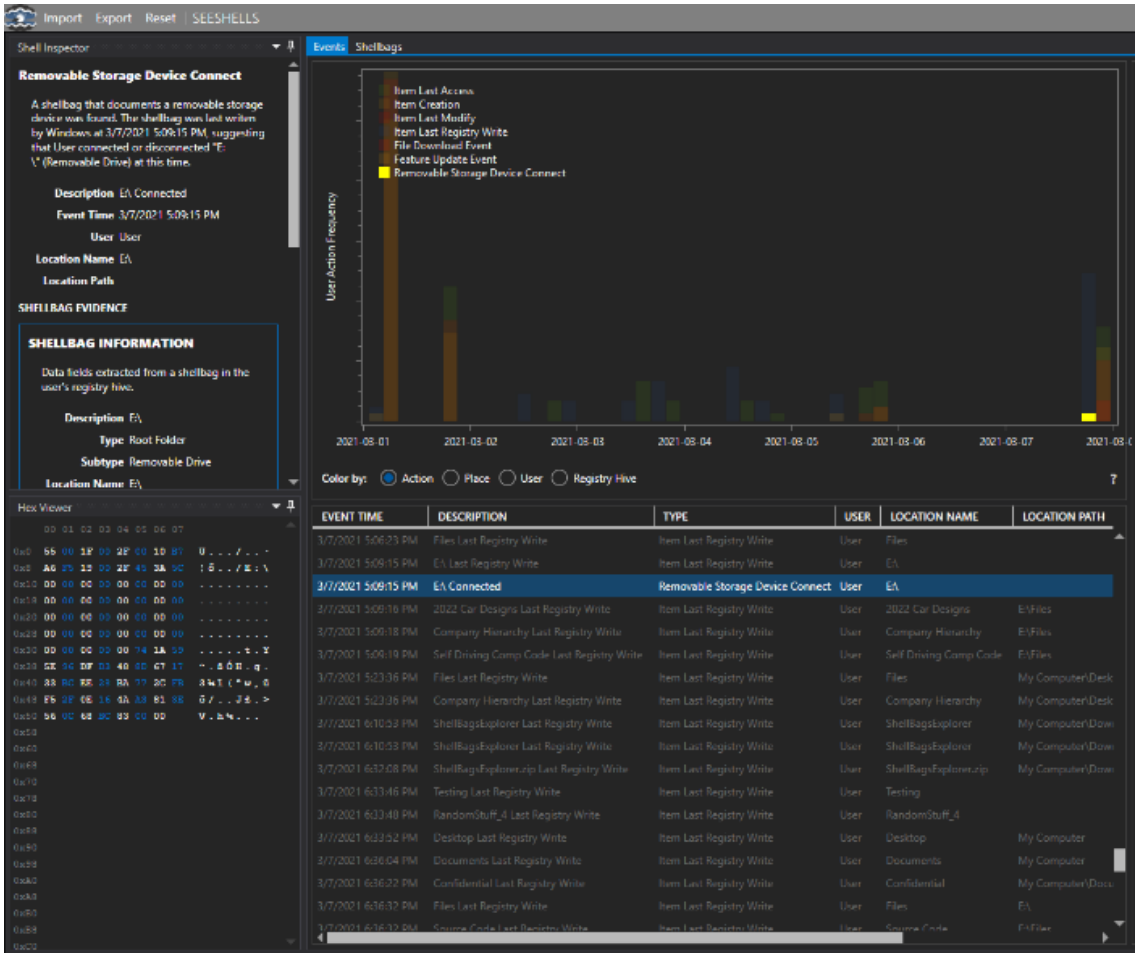
Showing another interesting directory within the timeframe.

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 called "Files". This is highlighted and shown in Fig 7.



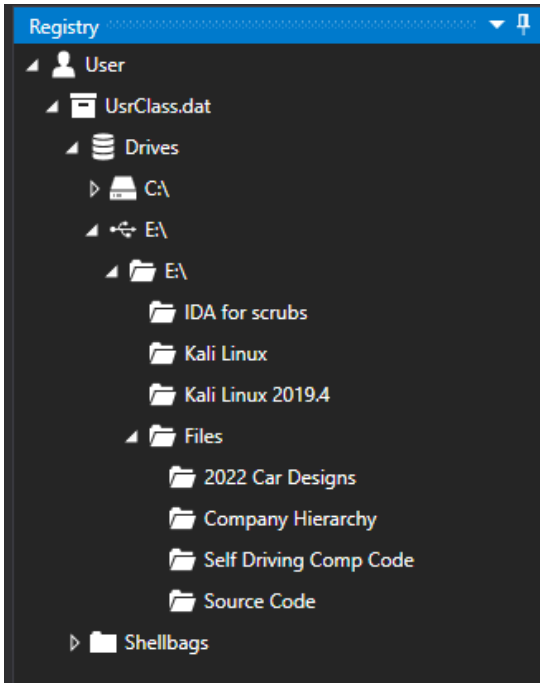
Creation of a folder named Files.

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 and is shown in Fig 8.



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

On the top right-hand side of the SeeShells explorer, 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 as shown in Fig 9.



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

Analysis Conclusion

The data analyzed from Shellbags in the Windows Registry clearly indicates that the employee copied several confidential files from their work computer onto some type of external storage device (E:) on 03/07/2021 at 22:09. In our case study, using SeeShells we were able to quickly 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's 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 had previously existed on this device. This data should be a lead to other artifact files or data within the OS to corroborate this assertion. Examples may include, but are not limited to, link or shortcut files, file system artifacts, event logs, etc.