**Digital Forensics Analysis of Windows 11 Shellbag with Comparative Tools**

2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)

Published: 2021

Intro-

We also conduct in-depth forensics examinations on Shellbag entries using three tools of three different types, i.e., open-source, freeware, and proprietary tools. Lastly, we compared the capabilities of tools utilized in Shellbag forensics investigations.

Literature Review-

All the files on a local system, network system, and attached external devices like USB devices are tracked using Shellbag

The research aims to answer important questions such as Under what conditions of folder interaction are the date-time key values of the Shellbag created and updated. Moreover, how can user access to a folder be differentiated from operating system interactions of the folder in the registry artifacts, and how is the integrity of Shellbag maintained through analysis of the artifacts. This research shows that ShellBag information is created through the selection of a folder by the user and interactions with the folder. These conditions were unknown to the digital forensic community. Thus, the paper aims to update the defined use of Shellbag in digital forensic investigations.

NTUSER.DAT and UsrClass.DAT files contain two important subkeys, BagMRU and Bags. BagMRU subkey shows the directory structures of the folders that were interacted with within the numbered subkey/value hierarchy format. Bag subkey constitutes numbered subkeys for each hierarchical corresponding child subkey under BagMRU.

We conducted our experiment on a Windows 11 v21H2 system running on Samsung 970 Evo Plus NVMe SSD.

A. Shellbag Entries for Desktop Folder and in C:\Drive

B. Shellbag Entries for USB Drives

C. Shellbag Entries for Compressed Files

A. Analysis Using OSForensics Tool

OSForensics is a proprietary tool that we used to forensically analyze our Shellbag entries for all folder customizations. The tool can scan both the live operating system and offline registry hives to parse the Shellbag information. Furthermore, it also can export registry files for later analysis.

B. Analysis Using ShellBags Explorer Tool

ShellBags Explorer is an open-source, easy-to-use tool authored by Eric Zimmerman, which is the most comprehensive tool for forensically analyzing Windows Shellbag information. It can analyze offline and online registries. ShellBags Explorer tool, demonstrates the different forensics analysis information such as the absolute path, last write time and modified-access-created timestamps.

C. Analysis Using ShellBagsView Tool

ShellBagsView is a lightweight software by Nirsoft. This tool thoroughly analyzes Shellbag entries from the Windows Registry. It cannot handle offline registry analysis for Shellbags as this feature is not supported. The tool by default displays seven default columns: path, slot number, last modified time, mode, icon size, slot key, slot modified time, windows position, windows size, type, and username.



However, future work on Shellbag forensics analysis will include tools like Cellebrite Inspector, Oxygen Forensics Detector, Magnet AXIOM, Belkasoft Evidence Center, and further cumulative updates of Windows 11 operating system.