SheHacks_KE

297 Followers About Follow

Windows ShellBags (Part 1)

SheHacks_KE Jul 14 · 6 min read

Introduction

Ever noticed when a user in a windows operating system modifies a folder size by e.g., resizing the window itself. Then going back to that folder at a later date, the customization remains? That is shellbags in action!

There are many sources of digital evidence and they are divided into three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers/devices and mobile devices. In this article, we will focus on stand-alone computers. **Digital artifacts** in digital **forensics** are pieces of data that can be used as good information when **digital** crimes occur so that they can be used as evidence for re-analysis by **forensic** teams.

Windows Shellbags artefact can be used to answer the difficult questions of data enumeration in intrusion cases, identify the contents of long-gone removable devices, and show the contents of previously mounted encrypted volumes.

What are ShellBags?

Microsoft Windows registry keeps track of folder settings in order to enhance the user experience using ShellBags. Windows ShellBags primary purpose is to improve user

experience and “remember” preferences while browsing folders. Information stored in ShellBags can be critical during forensic investigation.

Windows ShellBags were introduced into Microsoft’s operating system Windows XP, and are still present on all Windows 10 system releases. When you open, close or change viewing options of any folder on your computer, either from Windows Explorer, or from the Desktop (even by right-clicking or renaming the folder), a ShellBag record is created or updated.

Why are ShellBags Important in Digital Forensics Investigations?

For any digital forensic investigator, it is crucial to note the following:

- If any directory is mentioned in Windows ShellBags, it must have been present on the system at some point in time (even if it is not present anymore). This is valid for local filesystems including compressed archives, as well as for network locations e.g., remote mapped shares and removable devices e.g., USB flash drive.
- As these actions and viewing preferences are tied to the user’s registry hives, we can connect specific user accounts and specific folders. Moreover, we can get information about when the folder has been last accessed from MAC timestamps contained in ShellBags.

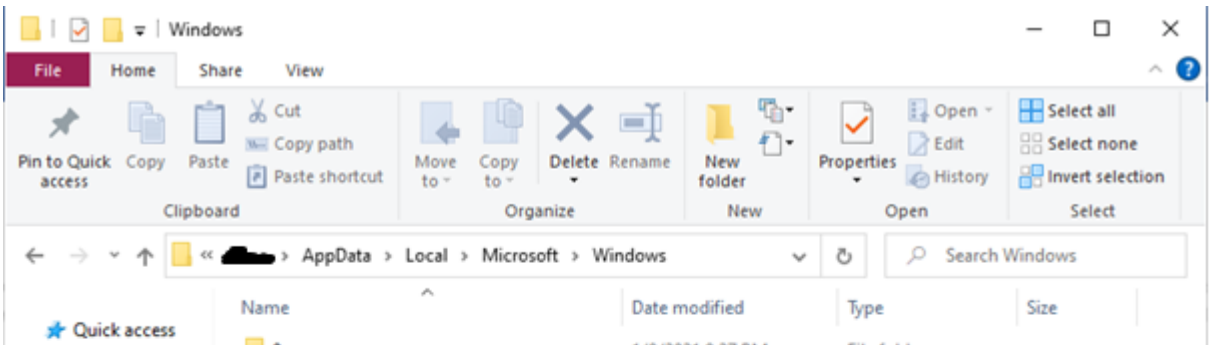
Where Do We Get ShellBags From?

It is buried deep in the system; it is a user specific file.

Follow the path:

C:\Users\…..\AppData\Local\Microsoft\Windows

The below user profile within my computer has administrative permission.



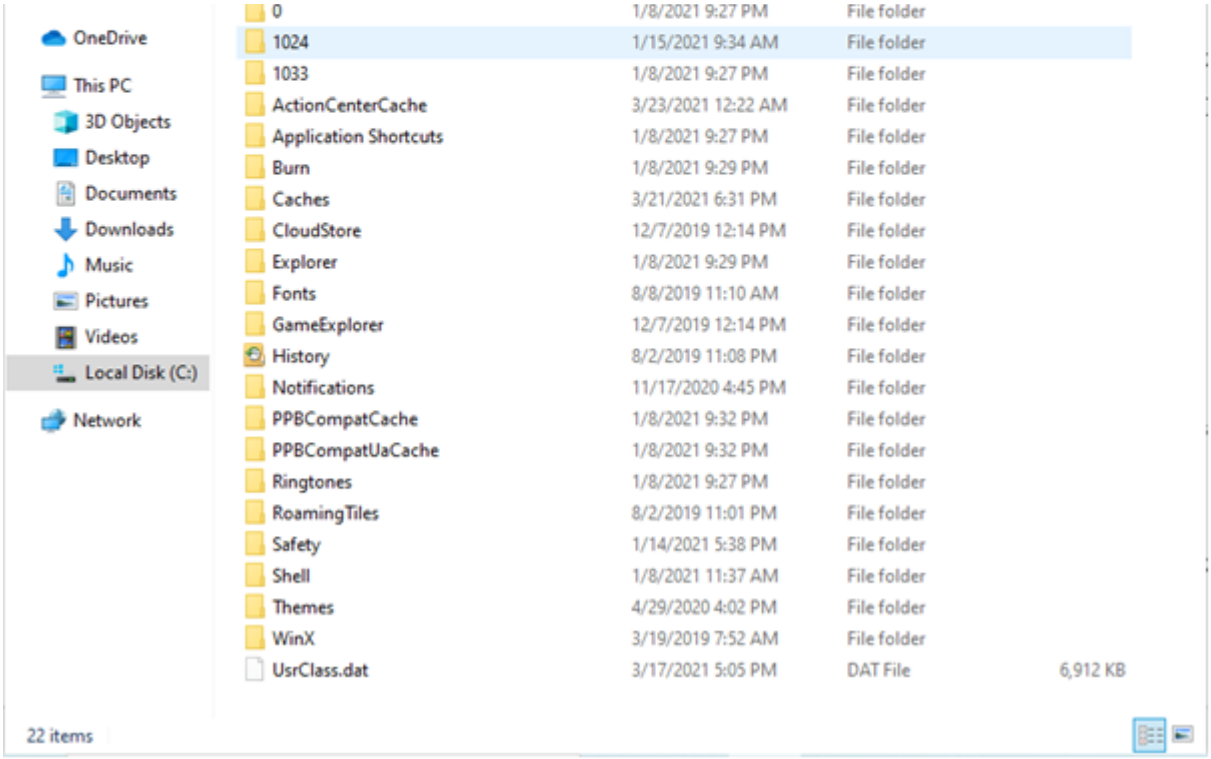


Figure 1 ShellBag File Location

The above screenshot shows what you should see once you follow the path to the Shellbags folder, at the bottom is a data file named **UsrClass.dat**.

For Windows 7 and later, shellbags are also found in the UsrClass.dat hive in the registry:

- HKCRLocal SettingsSoftwareMicrosoftWindowsShellBags
- HKCRLocal SettingsSoftwareMicrosoftWindowsShellBagMRU

Please note that if you cannot find the *AppData* folder after *C:\Users*\….\ Then change the folder view settings to include 'Hidden Items' by checking that box as shown in the screenshot below.

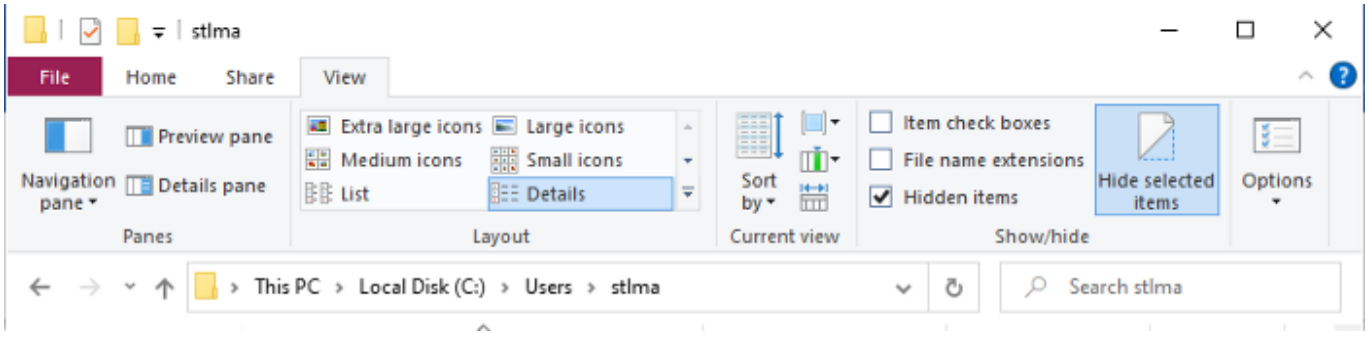


Figure 2 View Hidden Items

Now let's access ShellBags from the registry hive. Go to your windows menu and type "run". Then type 'regedit'. The command gives the user registry editing capabilities.

See screenshot of the run window.

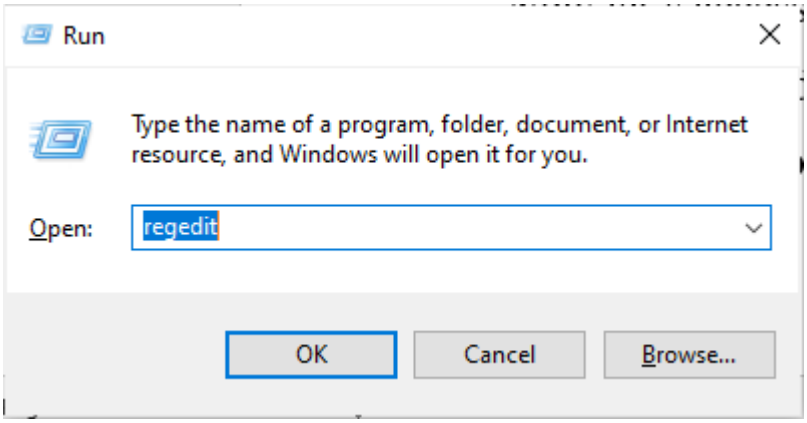


Figure 3 Run window

Now follow the path *Computer\HKEY_CLASSES_ROOT\LocalSettings\Software\Microsoft\Windows\Shell\Bags*

See screenshot below:

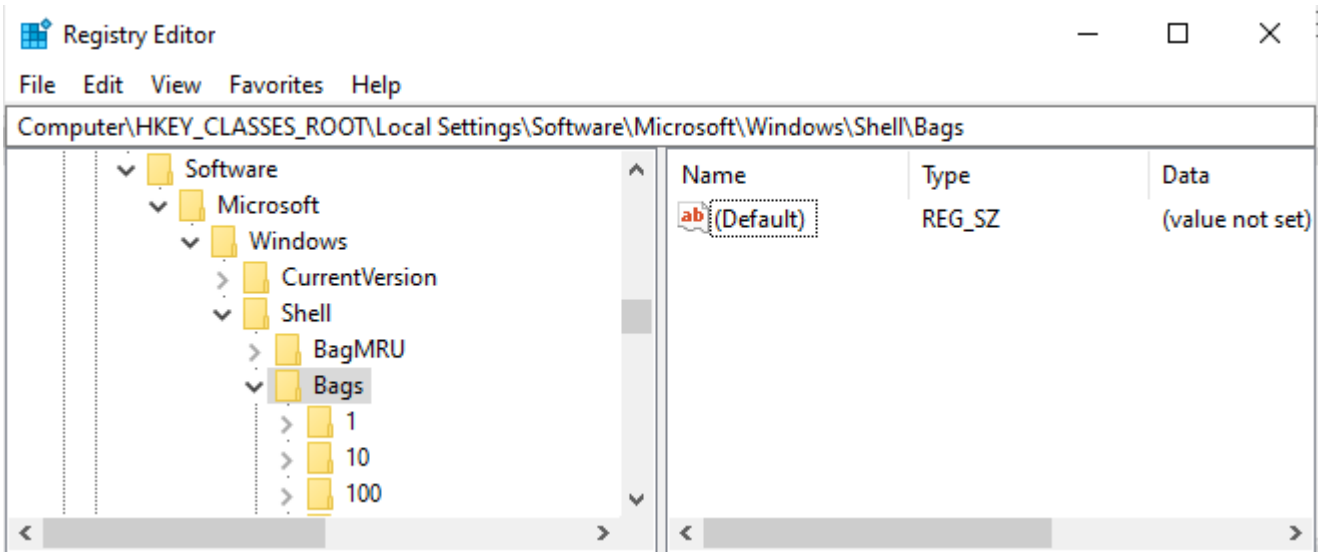


Figure 4 ShellBags in registry

Try opening any numbered folders under *Shell\Bags* or *\Shell\BagMRU* within the *Computer\HKEY_CLASSES_ROOT\LocalSettings\Software\Microsoft\Windows* path. You will see something that doesn't make sense like the below:

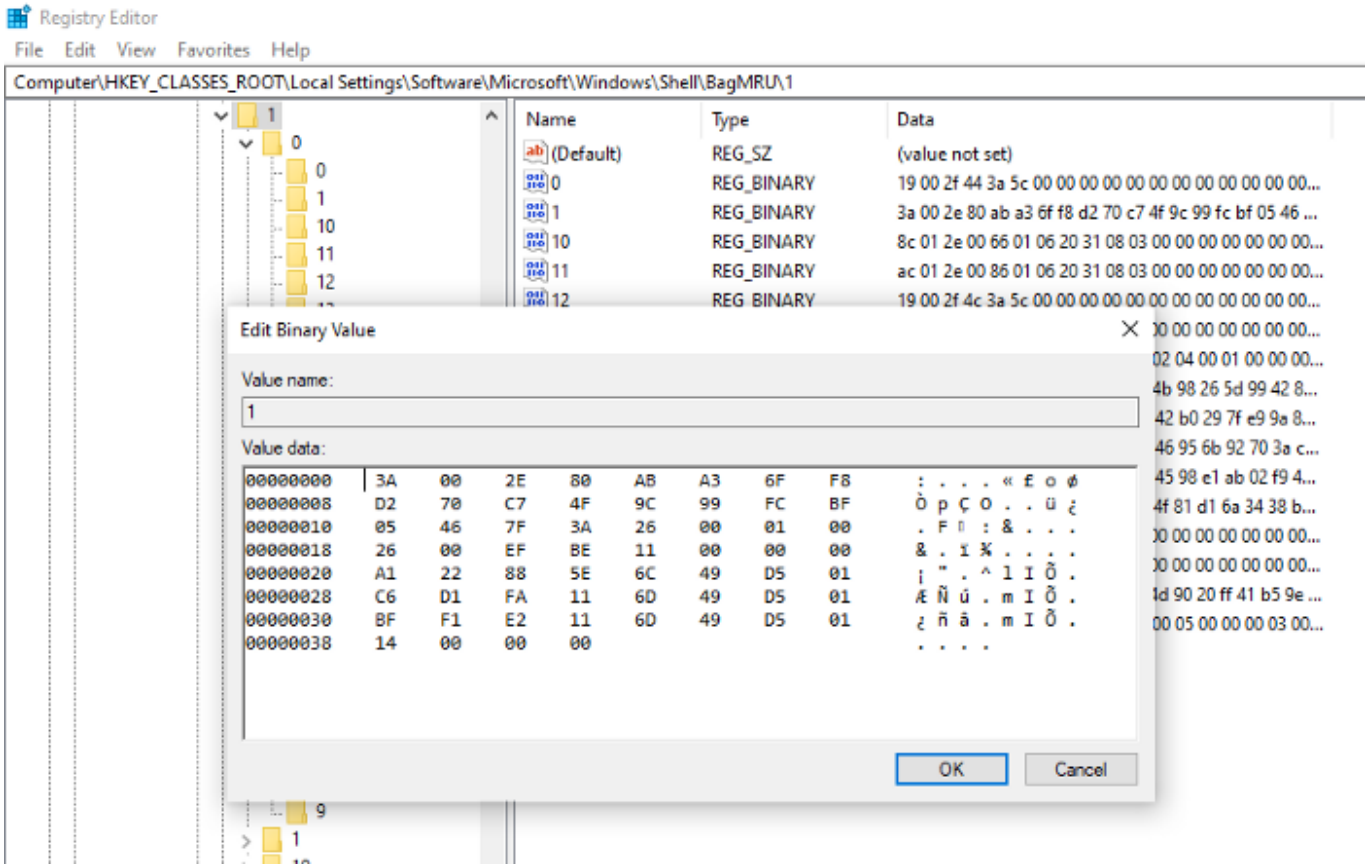


Figure 5 raw ShellBag data

The ShellBag data contains two main registry keys, BagMRU and Bags

BagMRU: This store folder names and folder path similar to the tree structure. The root directory is represented by the first bagMRU key i.e., 0. BagMRU contains numbered values that compare to say subkeys' nested subkeys. All of these subkeys contain numbered values aside from the last child in each branch.

Bag: This stores view preferences such as the size of the window, location, and view mode.

We will be analysing the shellbags using the ShellBag explorer GUI version.

Shellbags explorer is a tool by Eric Zimmerman to analyse shellbags. The shellbags explorer is available in both Command Line versions and GUI. You can download the tool from here.

How to Pull Forensics Goodness from This Data?

We shall use an Eric Zimmerman Tool called ShellBag Explorer.

Download link https://ericzimmerman.github.io/#!index.md.

From the forensics tool list choose ShellBags Explore. I downloaded version 1.4.0.0

The tool will open up and parse the data to make it understandable for me and you. Data parsing is converting data into comprehensible and understandable information.

In this tutorial, we shall use the GUI version of the Eric Zimmerman ShellBag explorer tool.

Make sure to launch the tool as an administrator in order to get the full capabilities of the tool.

This is how the GUI interface of the tool looks like

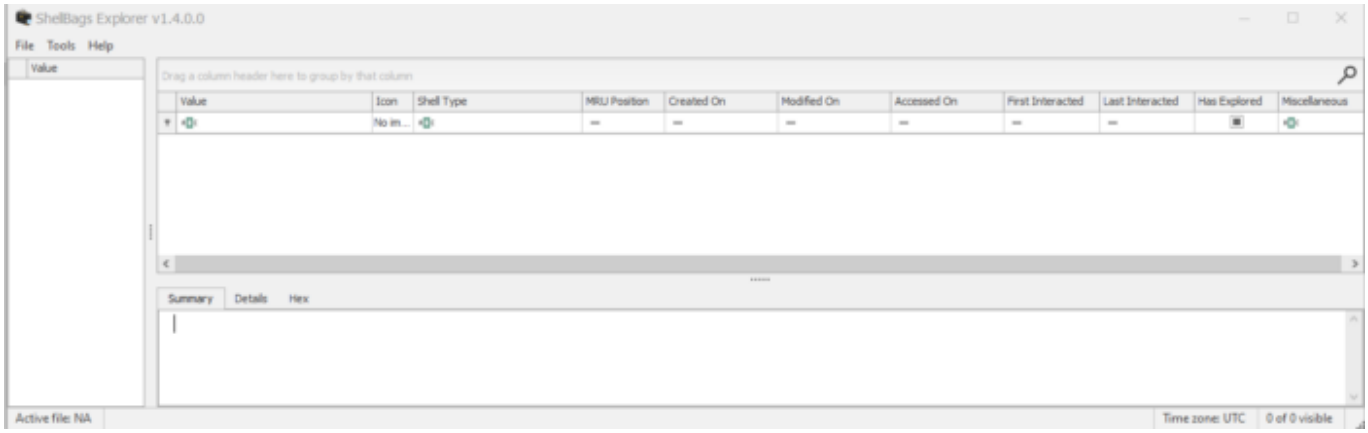


Figure 6 Shell Explorer by Eric Zimmerman

Active Registry Analysis

Using the shellbags explorer one can analyse the active registry. Select load an active registry which will load the registry in use by the active user. Always **Run as Administrator**!

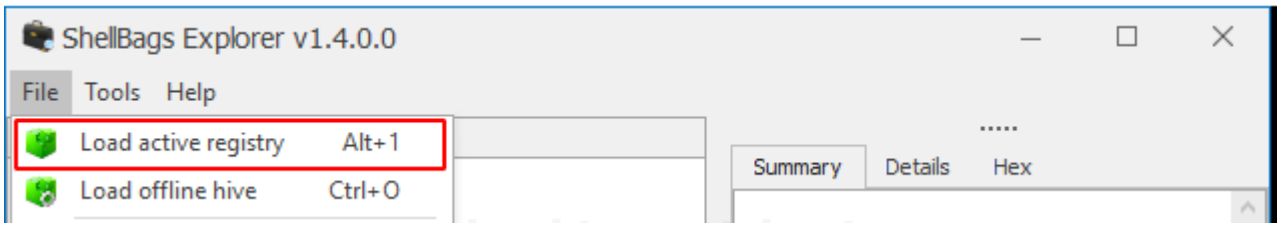


Figure 7 Load Active Registry

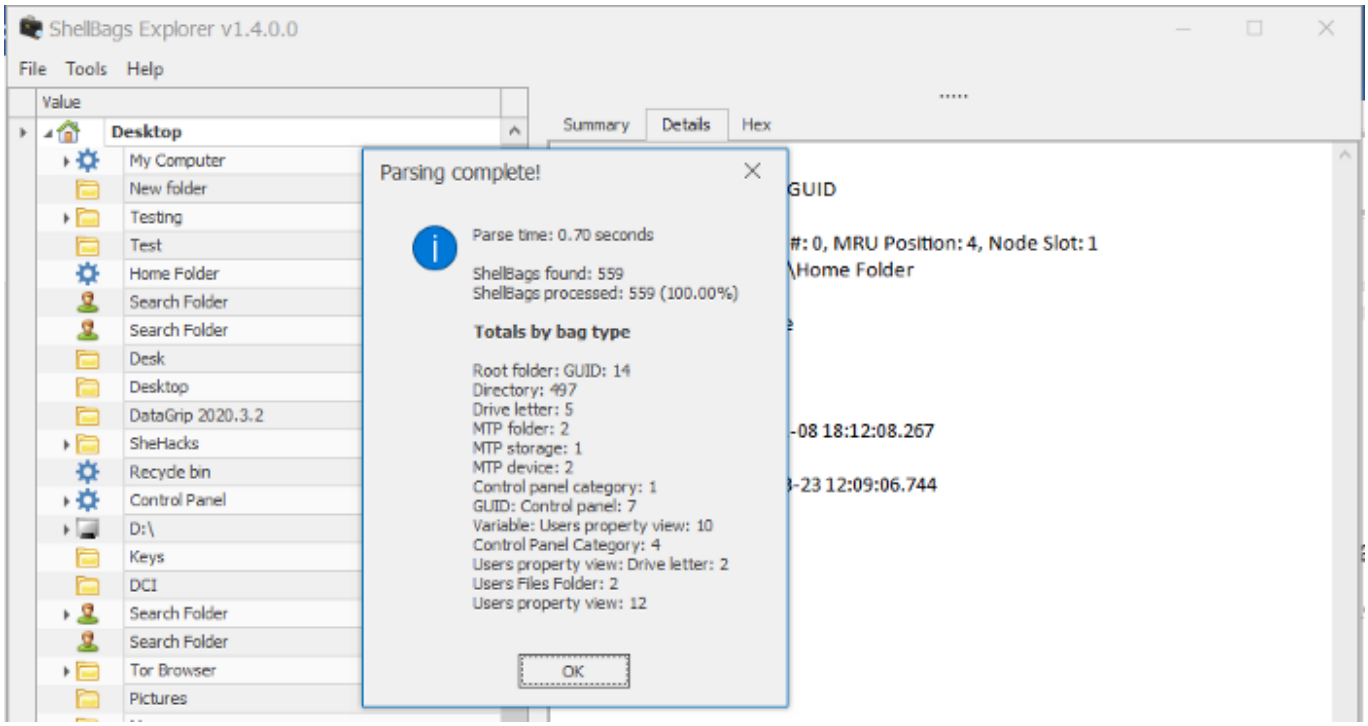
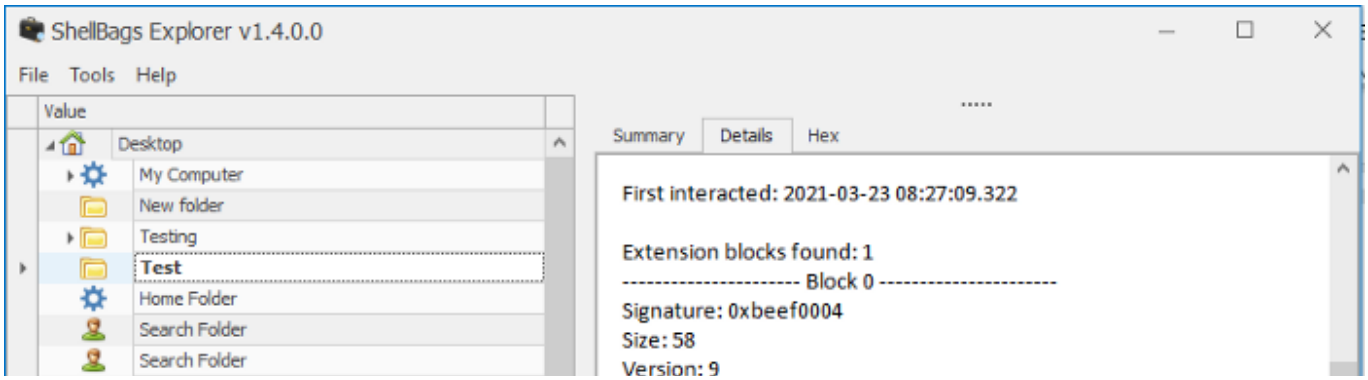


Figure 8 Parsed Active Registry

The shellbags are successfully parsed from the active registry.

To get a clear idea about how shell bags work and store data and how you can analyse it I have created a new folder named “Test” which consists of an empty folder. Further, I will be renaming it to “Testing”. Let’s analyse the shellbags entries for this.



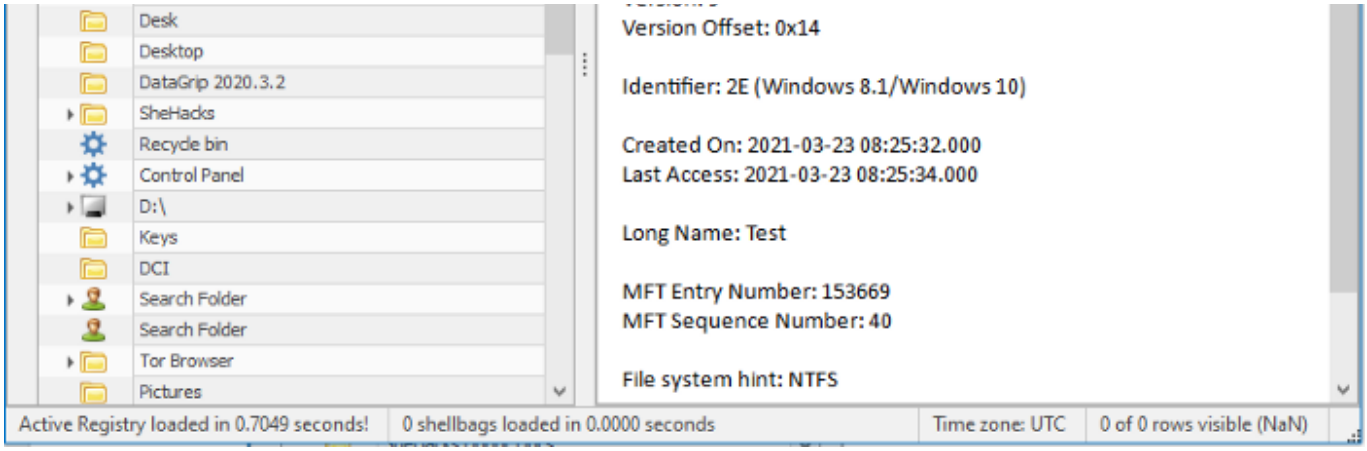


Figure 9 'Test' MFT Entry Number: 153669

As I mentioned earlier, I have renamed the folder named "Test" to "Testing" as highlighted in the screenshot below. The MFT entry number is the same for all two folders which depict that the folder was renamed.

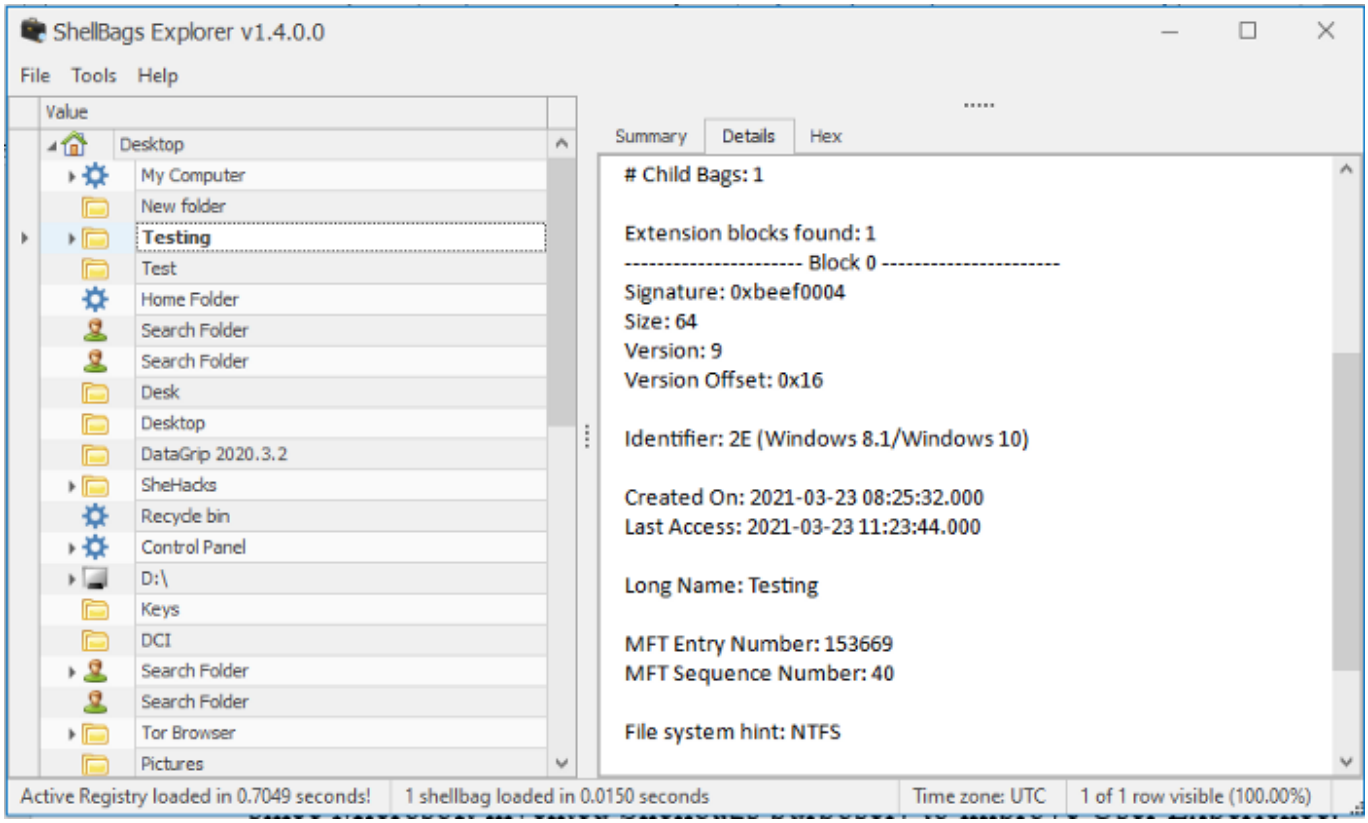


Figure 10 'Testing' MFT Entry Number: 153669

Conclusion:

We have covered what ShellBags are, they are categorized as a hidden forensic data source since Microsoft invented Shellbags purposely to improve User Experience.

They are located deep in the computer system and do not make sense without being parsed. The tool used to open and parse this data is the ShellBag Explorer by Eric Zimmerman. The GUI version is easy to use and understand.

In our scenario above, one can tell when, by whom and what changes were made.

Our user renamed the 'Test' folder to 'Testing' as indicated by the MFT Entry Number: 153669.

In part two, we will look at loading an offline hive.

References:

https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/

https://www.hackingarticles.in/forensic-investigation-shellbags/

https://www.sans.org/blog/computer-forensic-artifacts-windows-7-shellbags/

https://www.youtube.com/watch?v=86tzZWcQH60&ab_channel=SANSDigitalForensicsandIncidentResponse

https://www.youtube.com/watch?v=crh1uAqxeoU&ab_channel=SANSDigitalForensicsandIncidentResponse

by Stella Magana

Twitter: @STLmagana

Windows Shellbags Computer System Cybersecurity Shehacks