SHELLBAG ANALYSIS

Shellbags are a feature in the Windows operating system that tracks and maintains the settings of windows in the Windows Explorer.

To perform the analysis of shellbags from the user set found from our image, we made use of Shellbags Explorer by pointing it to the files extracted from our image in Autopsy. Based on our image, we were able to locate 4 users. We then extracted two files (Usrclass.dat & Ntuser.dat) for every user and stored it in the system for further investigation.

'**Usrclass.dat**' is a binary file in the Windows operating system that stores the user-specific registry settings and preferences for a particular user account. '**NTUser.dat**' is a binary file in the Windows operating system that stores the user-specific registry settings and preferences for a particular user account. While 'ntuser.dat' and 'usrclass.dat' are related files, they serve different purposes. **NTUser.dat** contains user-specific registry settings, while **Usrclass.dat** contains settings specific to the user's current active profile.

Here's the location for the hives that contain the shellbags:

```
%systemroot%\Users\\ntuser.dat

%systemroot%\Users\\AppData\Local\Microsoft\Windows\UsrClass.dat
```

As seen previously, the four users observed in that image were 'Ted Roethke', 'John Macrae', 'Willy B' and 'YeatsW'. We began examining the shellbags for each user. It was seen that there were no shellbags present for any of the four users in the file '**NTUser.dat**'.

Upon checking the '**Usrclass.dat**' file, we were able to find shellbags for two users i.e., 'YeatsW' and 'Willy B'. We explored shellbags for both these users individually. The following are the observations for the two users.

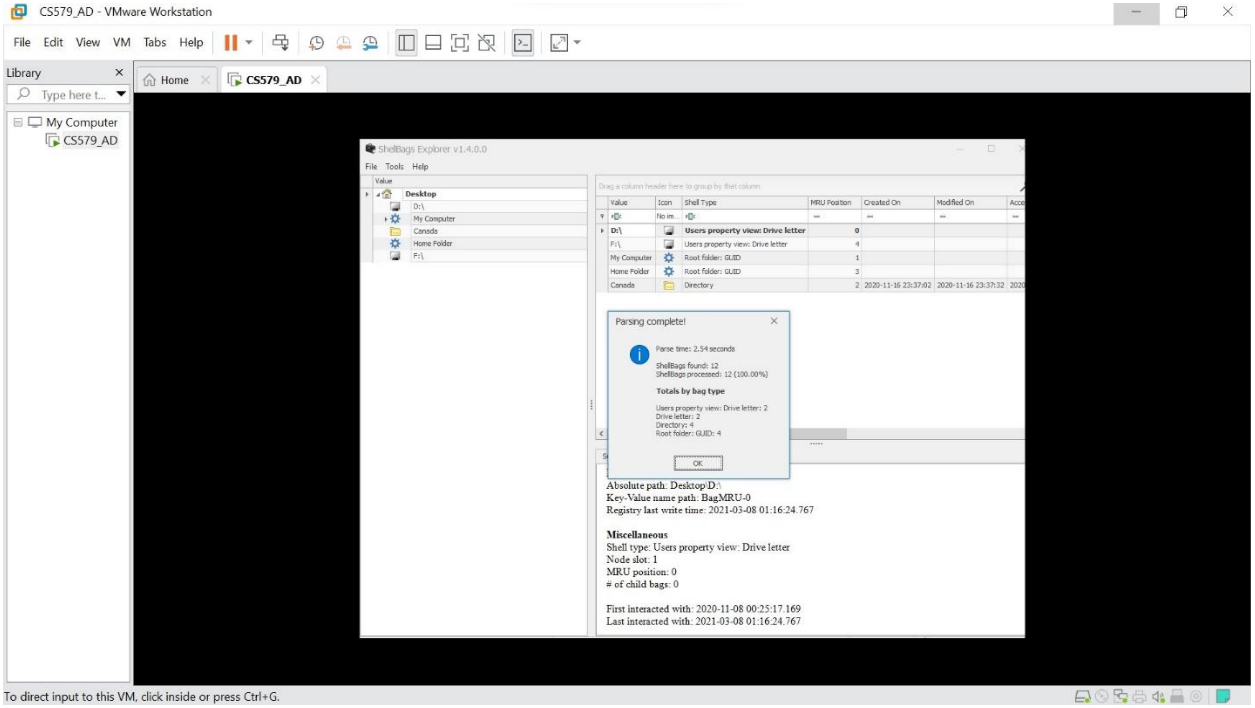
1. **YeatsW**: -

   As mentioned before, we were not able to find any shellbags for this user in '**NTUser.dat**'. However, upon passing the '**Usrclass.dat**' file, we were able to view 12 shellbags for this user. It was observed that there were two disk drives (D:\ and F\) for this user. The last registry write time for this user was 2021-03-08 01:16:24.767. There was another empty directory in the desktop named 'Canada' which was last accessed on 2021-03-07 08:16:24.767 (a day prior when the laptop was tossed into a dumpster).

   We found out some information about the Canada directory. The MFT Entry number for that directory is 150630 which indicates the unique identifier of that MFT record which contains information about the file or directory. MFT Sequence number for the same folder is 18 which tells us about the order in which the MFT record was created for the file or directory.

On further investigation, we found out that D drive was last accessed, on 2021-03-08 01:16:24.767. Last write time for that user registry was same as that of last time D drive was accessed.

The number of child bags for the D drive was seen to be 0. However, there were 4 childbags seen for the 'My Computer' directory.


CS579_AD - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
CS579_AD
Home
CS579_AD
ShellBags Explorer v1.4.0.0
File Tools Help
Value
Desktop
D:\
My Computer
Canada
Home Folder
F:\
Drag a column header here to group by that column
OK
To direct input to this VM, click inside or press Ctrl+G.

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Acce
D:\		Users property view: Drive letter	0			
F:\		Users property view: Drive letter	4			
My Computer		Root folder: GUID	1			
Home Folder		Root folder: GUID	3			
Canada		Directory	2	2020-11-16 23:37:02	2020-11-16 23:37:32	2020

```
Parsing complete!

Parse time: 2.54 seconds

ShellBags found: 12
ShellBags processed: 12 (100.00%)

Totals by bag type

Users property view: Drive letter: 2
Drive letter: 2
Directory: 4
Root folder: GUID: 4
```

```
Absolute path: Desktop\D:\
Key-Value name path: BagMRU-0
Registry last write time: 2021-03-08 01:16:24.767

Miscellaneous
Shell type: Users property view: Drive letter
Node slot: 1
MRU position: 0
# of child bags: 0

First interacted with: 2020-11-08 00:25:17.169
Last interacted with: 2021-03-08 01:16:24.767
```

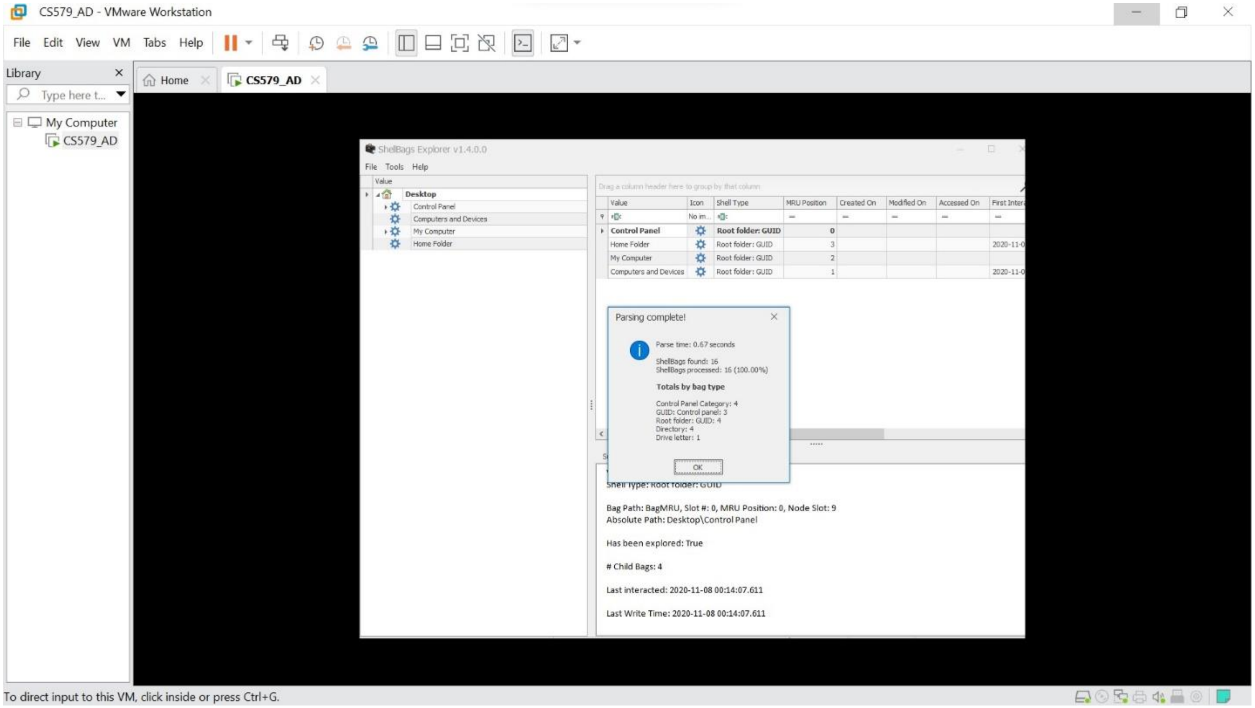
Shellbags for YeatsW in file 'UsrClass.dat'

2. **WillyB**: -

As mentioned before, we were not able to find any shellbags for this user in '**NTUser.dat**'. However, upon passing the '**Usrclass.dat**' file, we were able to view 16 shellbags for this user. It was observed that only one disk drive was present for this user. The last write time was same as that of the last interacted time which was 2020-11-08 00:14:07.611.

After exploring more into this drive, it was observed that the 'My Computer' directory was last accessed by this user. 'My Computer' had 1 child bag. As we examined any further bags, we were able to see where it pointed to. It finally went to Log files which is observed to be a NTFS file.

Overall, it was observed that all files were being recorded in the UsrClass.dat files instead of the ntuser.dat files.


CS579_AD - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
CS579_AD
Home
CS579_AD
ShellBags Explorer v1.4.0.0
File Tools Help
Value
Desktop
Control Panel
Computers and Devices
My Computer
Home Folder
Drag a column header here to group by that column
OK
To direct input to this VM, click inside or press Ctrl+G.

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Intera
Control Panel		Root folder: GUID	0				
Home Folder		Root folder: GUID	3				2020-11-0
My Computer		Root folder: GUID	2				
Computers and Devices		Root folder: GUID	1				2020-11-0

Parsing complete!

Parse time: 0.67 seconds

ShellBags found: 16
ShellBags processed: 16 (100.00%)

Totals by bag type

Control Panel Category: 4
GUID: Control panel: 3
Root folder: GUID: 4
Directory: 4
Drive letter: 1

Shell Type: Root folder: GUID

Bag Path: BagMRU, Slot #: 0, MRU Position: 0, Node Slot: 9
Absolute Path: Desktop\Control Panel

Has been explored: True

Child Bags: 4

Last interacted: 2020-11-08 00:14:07.611

Last Write Time: 2020-11-08 00:14:07.611

Shellbags for WillyB in file ‘UsrClass.dat’