Forensic Investigation: Shellbags

October 26, 2020 By Raj Chandel

In this article, we will be focusing on shellbags and its forensic analysis using shellbag explorer. Shellbags are created to enhance the users' experience by remembering user preferences while exploring folders, the information stored in shellbags is useful for forensic investigation.

Table of Contents

Introduction

Windows Shell Bags were introduced into Microsoft's Windows 7 operating system and are yet present on all later Windows platform. Shellbags are registry keys that are used to improve user experience and recall user's preferences whenever needed. The creation of shellbags relies upon the exercises performed by the user.

As a digital forensic investigator, with the help of shellbags, you can prove whether a specific folder was accessed by a particular user or not. You can even check whether the specific folder was created or was available or not. You can also find out whether external directories have been accessed on external devices or not.

For the most part, Shell Bags are intended to hold data about the user's activities while exploring Windows. This implies that if the user changes icon sizes from large icons to the grid, the settings get updated in Shell Bag instantly. At the point when you open, close, or change the review choice of any folder on your system, either from Windows Explorer or from the Desktop, even by right-clicking or renaming the organizer, a Shellbag record is made or refreshed.

Location of shellbags

Windows XP

The shellbags for Windows XP are stored in NTUSER.DAT

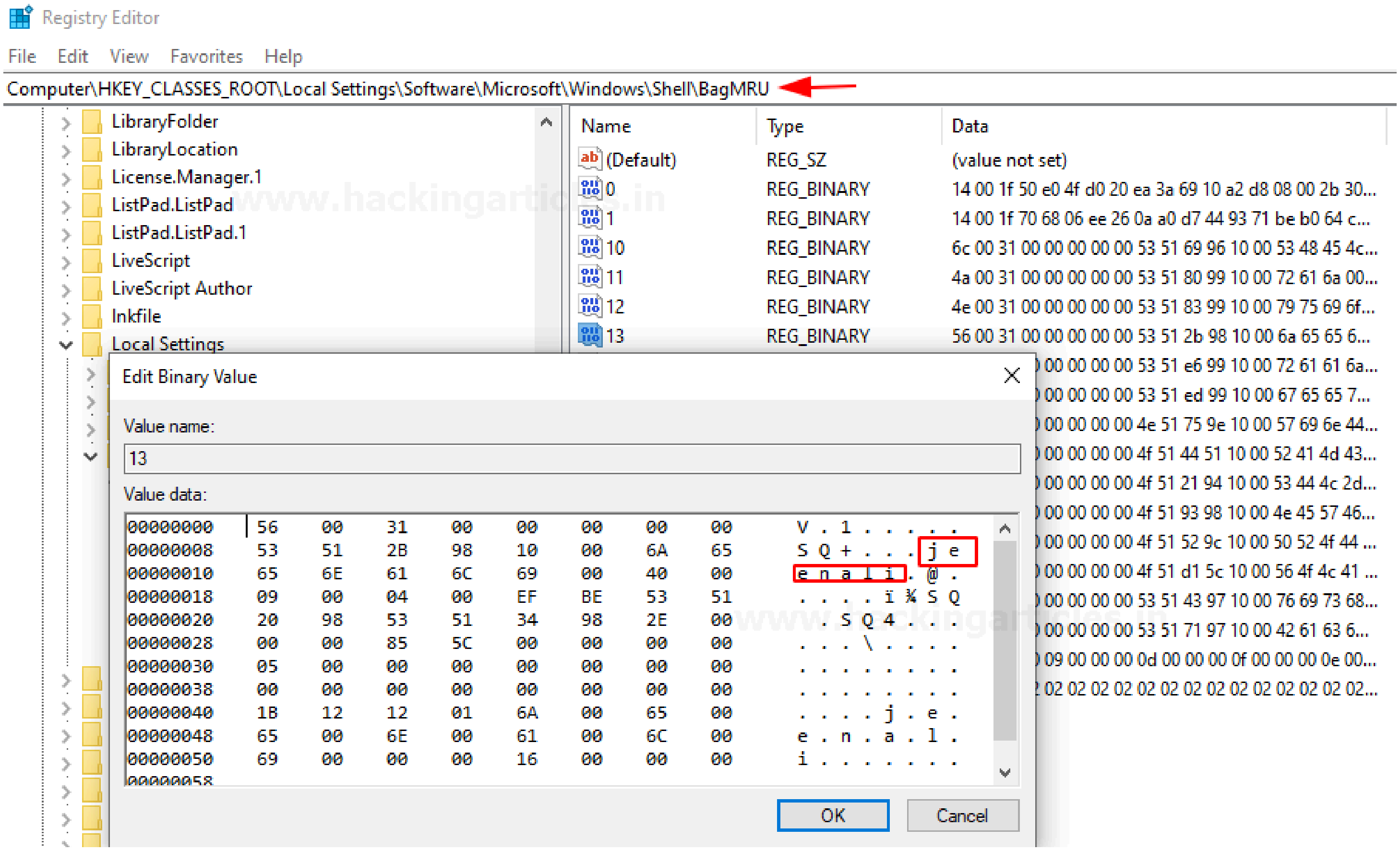
- Network folders references:\Software\Microsoft\Windows\Shell
- Local folder references: \Software\Microsoft\Windows\ShellNoRoam
- Removable device folders: \Software\Microsoft\Windows\StreamMRU

Windows 7 to Windows 10

Shellbags are a set of subkeys in the UsrClass.dat registry hive of Windows 10 systems. The shell bags are stored in both NTUSER.DAT and USRCLASS.DAT.

- NTUSER.DAT: HKCU\Software\Microsoft\Windows\Shell
- USRCLASS.DAT: HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell

The majority of the data is found in the USRCLASS.DAT hive-like local, removable, and network folders' data. You can manually check shellbags entry in the registry editor like so. In the following screenshot, a shellbag entry for a folder named jeenali is shown.



Computer\HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 08 00 2b 30...
1	REG_BINARY	14 00 1f 70 68 06 ee 26 0a a0 d7 44 93 71 be b0 64 c...
10	REG_BINARY	6c 00 31 00 00 00 00 00 53 51 69 96 10 00 53 48 45 4c...
11	REG_BINARY	4a 00 31 00 00 00 00 00 53 51 80 99 10 00 72 61 6a 00...
12	REG_BINARY	4e 00 31 00 00 00 00 00 53 51 83 99 10 00 79 75 69 6f...
13	REG_BINARY	56 00 31 00 00 00 00 00 53 51 2b 98 10 00 6a 65 65 6...
		00 00 00 00 53 51 e6 99 10 00 72 61 61 6a...
		00 00 00 00 53 51 ed 99 10 00 67 65 65 7...
		00 00 00 00 4e 51 75 9e 10 00 57 69 6e 44...
		00 00 00 00 4f 51 44 51 10 00 52 41 4d 43...
		00 00 00 00 4f 51 21 94 10 00 53 44 4c 2d...
		00 00 00 00 4f 51 93 98 10 00 4e 45 57 46...
		00 00 00 00 4f 51 52 9c 10 00 50 52 4f 44 ...
		00 00 00 00 4f 51 d1 5c 10 00 56 4f 4c 41 ...
		00 00 00 00 53 51 43 97 10 00 76 69 73 68...
		00 00 00 00 53 51 71 97 10 00 42 61 63 6...
		09 00 00 00 0d 00 00 00 0f 00 00 00 0e 00...
		02 02 02 02 02 02 02 02 02 02 02 02 02 02...

Value name:

13

Value data:

```
00000000  56  00  31  00  00  00  00  00    V . 1 . . . . .
00000008  53  51  2B  98  10  00  6A  65    S Q + . . . j e
00000010  65  6E  61  6C  69  00  40  00    e n a l i . @ .
00000018  09  00  04  00  EF  BE  53  51    . . . . ï ¾ S Q
00000020  20  98  53  51  34  98  2E  00    . S Q 4 . . .
00000028  00  00  85  5C  00  00  00  00    . . . \ . . . .
00000030  05  00  00  00  00  00  00  00    . . . . . . . .
00000038  00  00  00  00  00  00  00  00    . . . . . . . .
00000040  1B  12  12  01  6A  00  65  00    . . . . j . e .
00000048  65  00  6E  00  61  00  6C  00    e . n . a . l .
00000050  69  00  00  00  16  00  00  00    i . . . . . . .
00000058
```

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

- **BagMRU**: This stores 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 sub key's nested subkeys. All of these subkeys contain numbered values aside from the last child in each branch.
- **Bag**: These stores view preference such as the size of the window, location, and view mode.

We will be analyzing the shellbags using the shellbag explorer.

1. ShellBags explorer(SBECmd)
2. Shellbags explorer (GUI version)

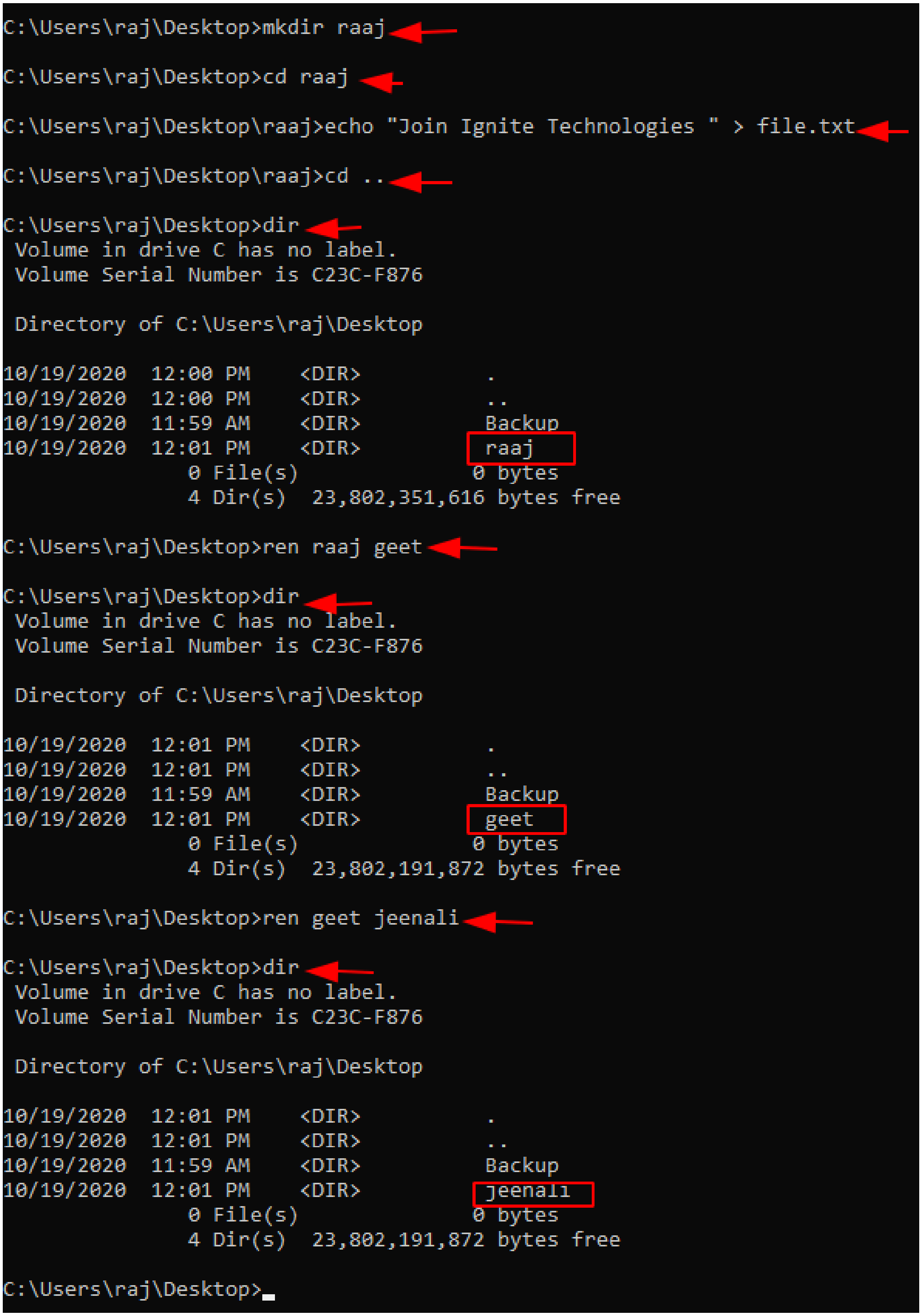
Shellbags explorer is a tool by Eric Zimmerman to analyze shellbags. The shellbags explorer is available in both versions cmd and GUI. You can download the tool from here.

Forensic Analysis of Shellbag

Analysis using SBECmd

Here we are using the SBECmd.exe (Cmd version of the shellbag explorer tool) by Eric Zimmerman. This cmd tool is great for command prompt lovers who prefer using commands over GUI.

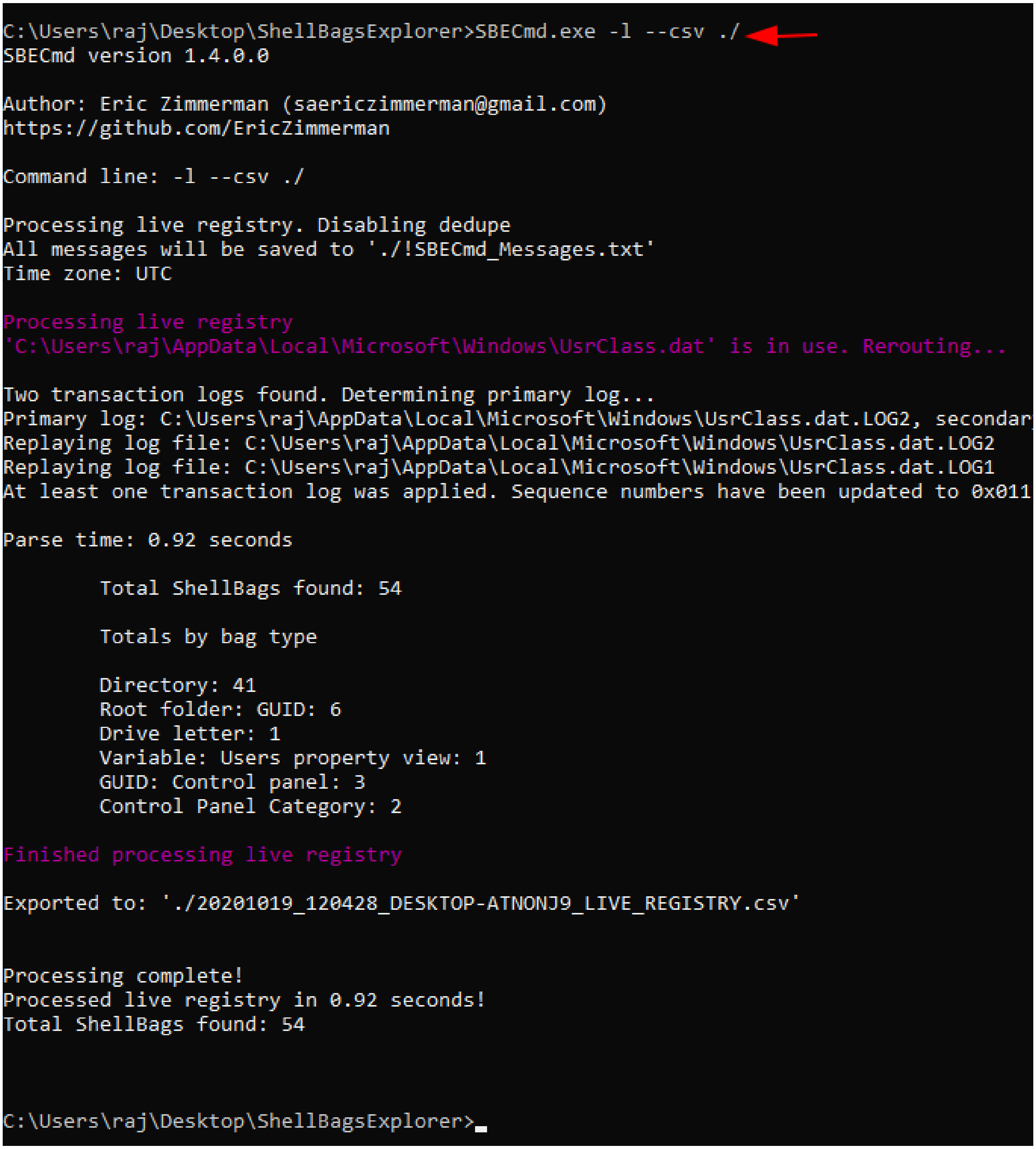
To get a clear idea about how shell bags work and store data and how you can analyze it I have created a new folder named “raaj” which consists of a text document. Further, we will be renaming it to geet and then to jeenali. Let’s analyze the shellbags entries for this.



```
C:\Users\raj\Desktop>mkdir raaj

C:\Users\raj\Desktop>cd raaj

C:\Users\raj\Desktop\raaj>echo "Join Ignite Technologies " > file.txt

C:\Users\raj\Desktop\raaj>cd ..

C:\Users\raj\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is C23C-F876

 Directory of C:\Users\raj\Desktop

10/19/2020  12:00 PM    <DIR>          .
10/19/2020  12:00 PM    <DIR>          ..
10/19/2020  11:59 AM    <DIR>          Backup
10/19/2020  12:01 PM    <DIR>          raaj
               0 File(s)              0 bytes
               4 Dir(s)  23,802,351,616 bytes free

C:\Users\raj\Desktop>ren raaj geet

C:\Users\raj\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is C23C-F876

 Directory of C:\Users\raj\Desktop

10/19/2020  12:01 PM    <DIR>          .
10/19/2020  12:01 PM    <DIR>          ..
10/19/2020  11:59 AM    <DIR>          Backup
10/19/2020  12:01 PM    <DIR>          geet
               0 File(s)              0 bytes
               4 Dir(s)  23,802,191,872 bytes free

C:\Users\raj\Desktop>ren geet jeenali

C:\Users\raj\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is C23C-F876

 Directory of C:\Users\raj\Desktop

10/19/2020  12:01 PM    <DIR>          .
10/19/2020  12:01 PM    <DIR>          ..
10/19/2020  11:59 AM    <DIR>          Backup
10/19/2020  12:01 PM    <DIR>          jeenali
               0 File(s)              0 bytes
               4 Dir(s)  23,802,191,872 bytes free

C:\Users\raj\Desktop>_
```

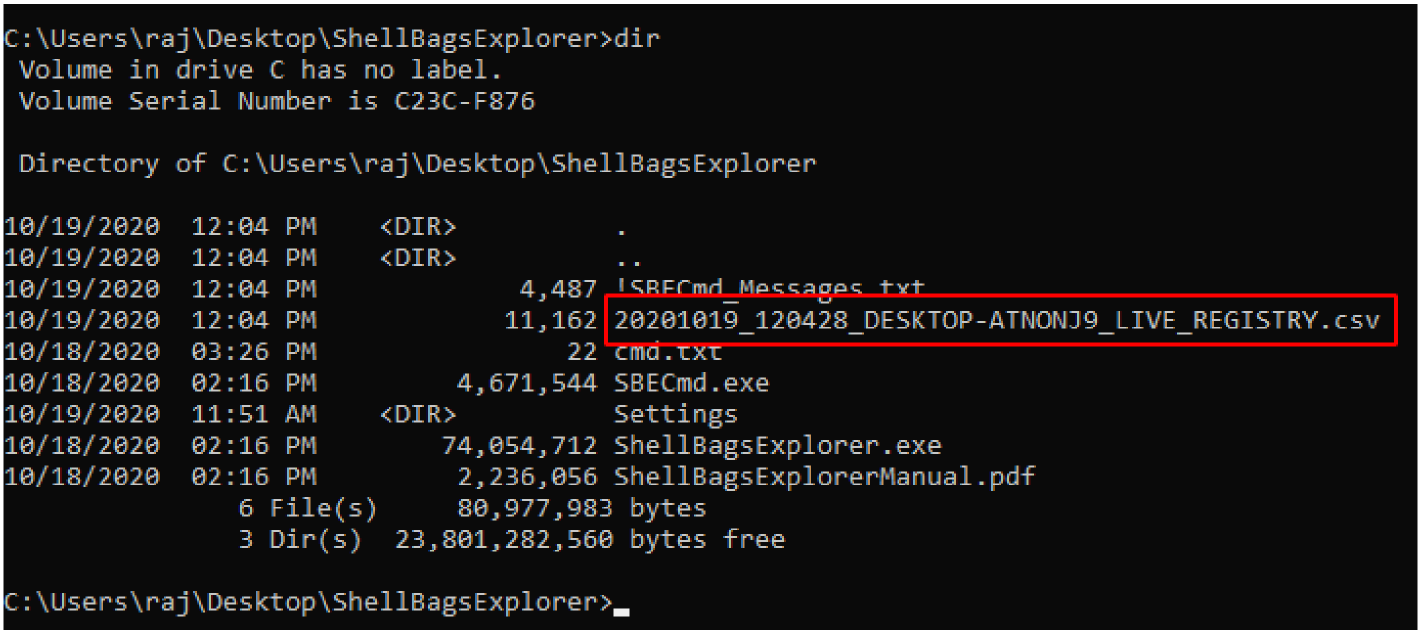
Run the executable file and browse to the directory where the executable is present. To extract the shellbags data into a .csv file use the following command:

```
SBECmd.exe –l --csv ./
```



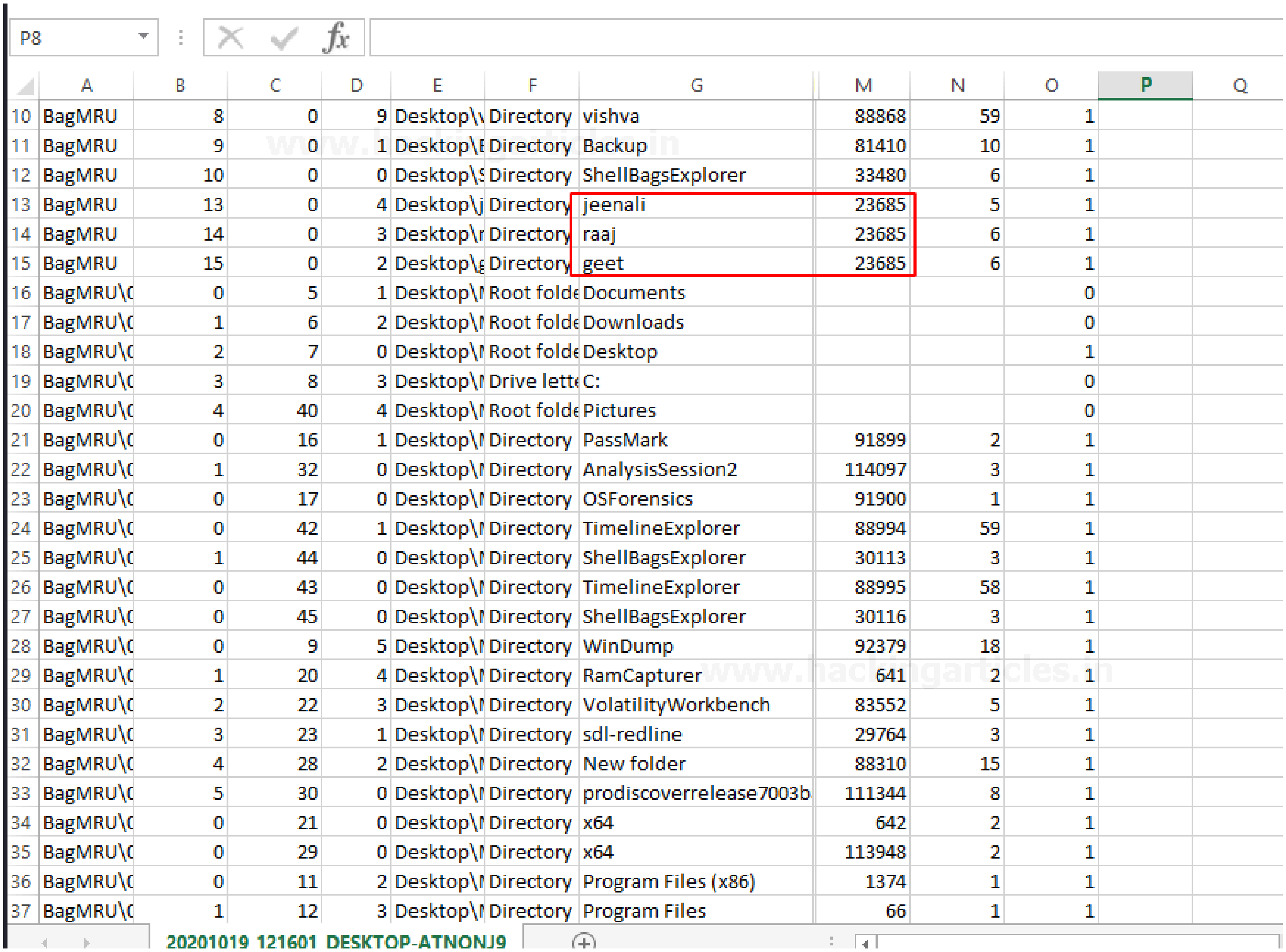
```
C:\Users\raj\Desktop\ShellBagsExplorer>SBECmd.exe -l --csv ./
SBECmd version 1.4.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman

Command line: -l --csv ./

Processing live registry. Disabling dedupe
All messages will be saved to './!SBECmd_Messages.txt'
Time zone: UTC

Processing live registry
'C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat' is in use. Rerouting...

Two transaction logs found. Determining primary log...
Primary log: C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2, secondar
Replaying log file: C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2
Replaying log file: C:\Users\raj\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x011

Parse time: 0.92 seconds

        Total ShellBags found: 54

        Totals by bag type

        Directory: 41
        Root folder: GUID: 6
        Drive letter: 1
        Variable: Users property view: 1
        GUID: Control panel: 3
        Control Panel Category: 2

Finished processing live registry

Exported to: './20201019_120428_DESKTOP-ATNONJ9_LIVE_REGISTRY.csv'


Processing complete!
Processed live registry in 0.92 seconds!
Total ShellBags found: 54



C:\Users\raj\Desktop\ShellBagsExplorer>_
```

As a result of the above command, a .csv file will be created in the directory.



```
C:\Users\raj\Desktop\ShellBagsExplorer>dir
 Volume in drive C has no label.
 Volume Serial Number is C23C-F876

 Directory of C:\Users\raj\Desktop\ShellBagsExplorer

10/19/2020  12:04 PM    <DIR>          .
10/19/2020  12:04 PM    <DIR>          ..
10/19/2020  12:04 PM             4,487 !SBECmd_Messages.txt
10/19/2020  12:04 PM            11,162 20201019_120428_DESKTOP-ATNONJ9_LIVE_REGISTRY.csv
10/18/2020  03:26 PM                22 cmd.txt
10/18/2020  02:16 PM         4,671,544 SBECmd.exe
10/19/2020  11:51 AM    <DIR>          Settings
10/18/2020  02:16 PM        74,054,712 ShellBagsExplorer.exe
10/18/2020  02:16 PM         2,236,056 ShellBagsExplorerManual.pdf
               6 File(s)     80,977,983 bytes
               3 Dir(s)  23,801,282,560 bytes free

C:\Users\raj\Desktop\ShellBagsExplorer>_
```

Lets' open the .csv file and analyze it.



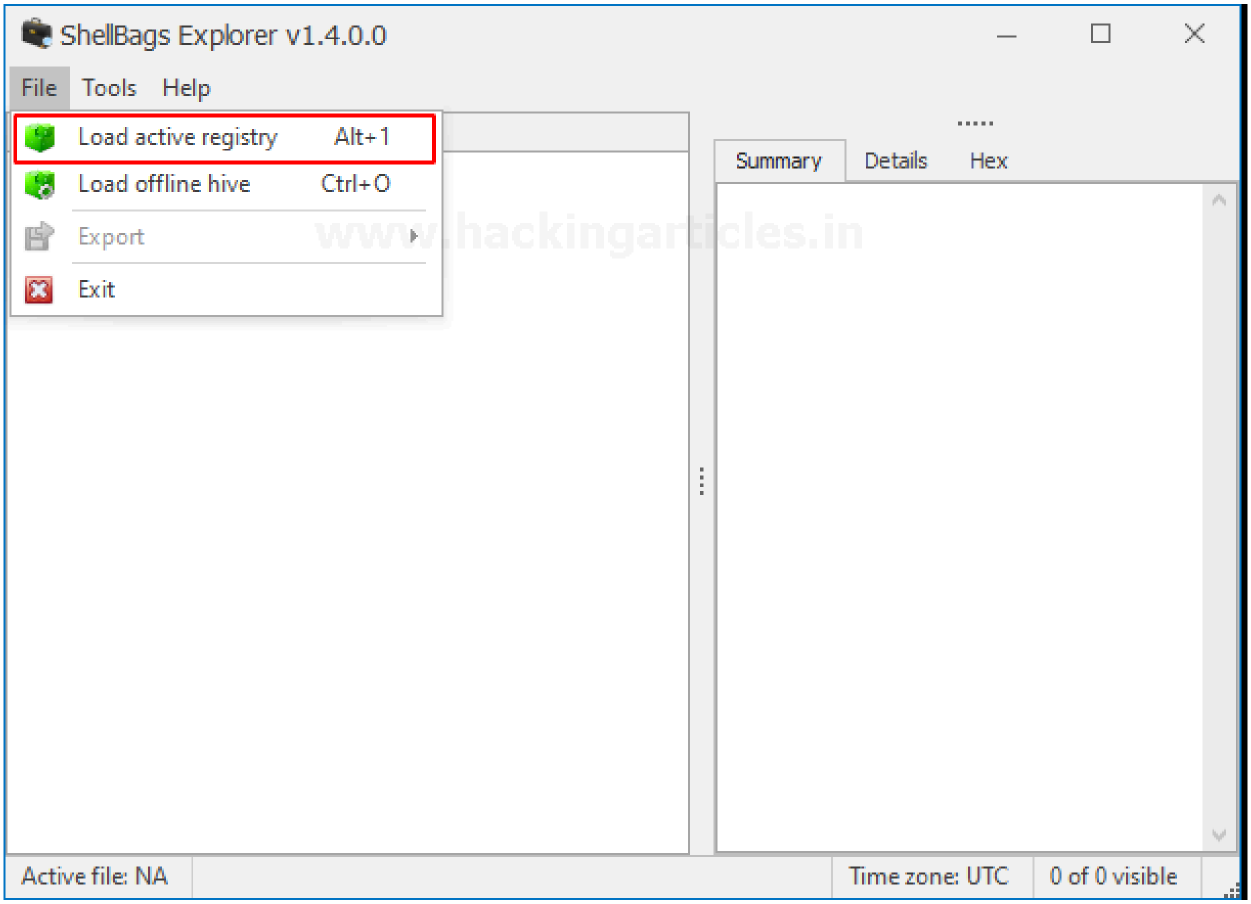
	A	B	C	D	E	F	G	M	N	O	P	Q
10	BagMRU	8	0	9	Desktop\\	Directory	vishva	88868	59	1		
11	BagMRU	9	0	1	Desktop\E	Directory	Backup	81410	10	1		
12	BagMRU	10	0	0	Desktop\S	Directory	ShellBagsExplorer	33480	6	1		
13	BagMRU	13	0	4	Desktop\j	Directory	jeenali	23685	5	1		
14	BagMRU	14	0	3	Desktop\r	Directory	raaj	23685	6	1		
15	BagMRU	15	0	2	Desktop\g	Directory	geet	23685	6	1		
16	BagMRU\(	0	5	1	Desktop\I	Root folde	Documents			0		
17	BagMRU\(	1	6	2	Desktop\I	Root folde	Downloads			0		
18	BagMRU\(	2	7	0	Desktop\I	Root folde	Desktop			1		
19	BagMRU\(	3	8	3	Desktop\I	Drive lette	C:			0		
20	BagMRU\(	4	40	4	Desktop\I	Root folde	Pictures			0		
21	BagMRU\(	0	16	1	Desktop\I	Directory	PassMark	91899	2	1		
22	BagMRU\(	1	32	0	Desktop\I	Directory	AnalysisSession2	114097	3	1		
23	BagMRU\(	0	17	0	Desktop\I	Directory	OSForensics	91900	1	1		
24	BagMRU\(	0	42	1	Desktop\I	Directory	TimelineExplorer	88994	59	1		
25	BagMRU\(	1	44	0	Desktop\I	Directory	ShellBagsExplorer	30113	3	1		
26	BagMRU\(	0	43	0	Desktop\I	Directory	TimelineExplorer	88995	58	1		
27	BagMRU\(	0	45	0	Desktop\I	Directory	ShellBagsExplorer	30116	3	1		
28	BagMRU\(	0	9	5	Desktop\I	Directory	WinDump	92379	18	1		
29	BagMRU\(	1	20	4	Desktop\I	Directory	RamCapturer	641	2	1		
30	BagMRU\(	2	22	3	Desktop\I	Directory	VolatilityWorkbench	83552	5	1		
31	BagMRU\(	3	23	1	Desktop\I	Directory	sdl-redline	29764	3	1		
32	BagMRU\(	4	28	2	Desktop\I	Directory	New folder	88310	15	1		
33	BagMRU\(	5	30	0	Desktop\I	Directory	prodiscoverrelease7003b	111344	8	1		
34	BagMRU\(	0	21	0	Desktop\I	Directory	x64	642	2	1		
35	BagMRU\(	0	29	0	Desktop\I	Directory	x64	113948	2	1		
36	BagMRU\(	0	11	2	Desktop\I	Directory	Program Files (x86)	1374	1	1		
37	BagMRU\(	1	12	3	Desktop\I	Directory	Program Files	66	1	1		

As I mentioned earlier, we have renamed the folder named “raaj” to “geet” and further to “jeenali” as highlighted in the screenshot the MFT entry number is the same for all three folders which depict that the folder was renamed.

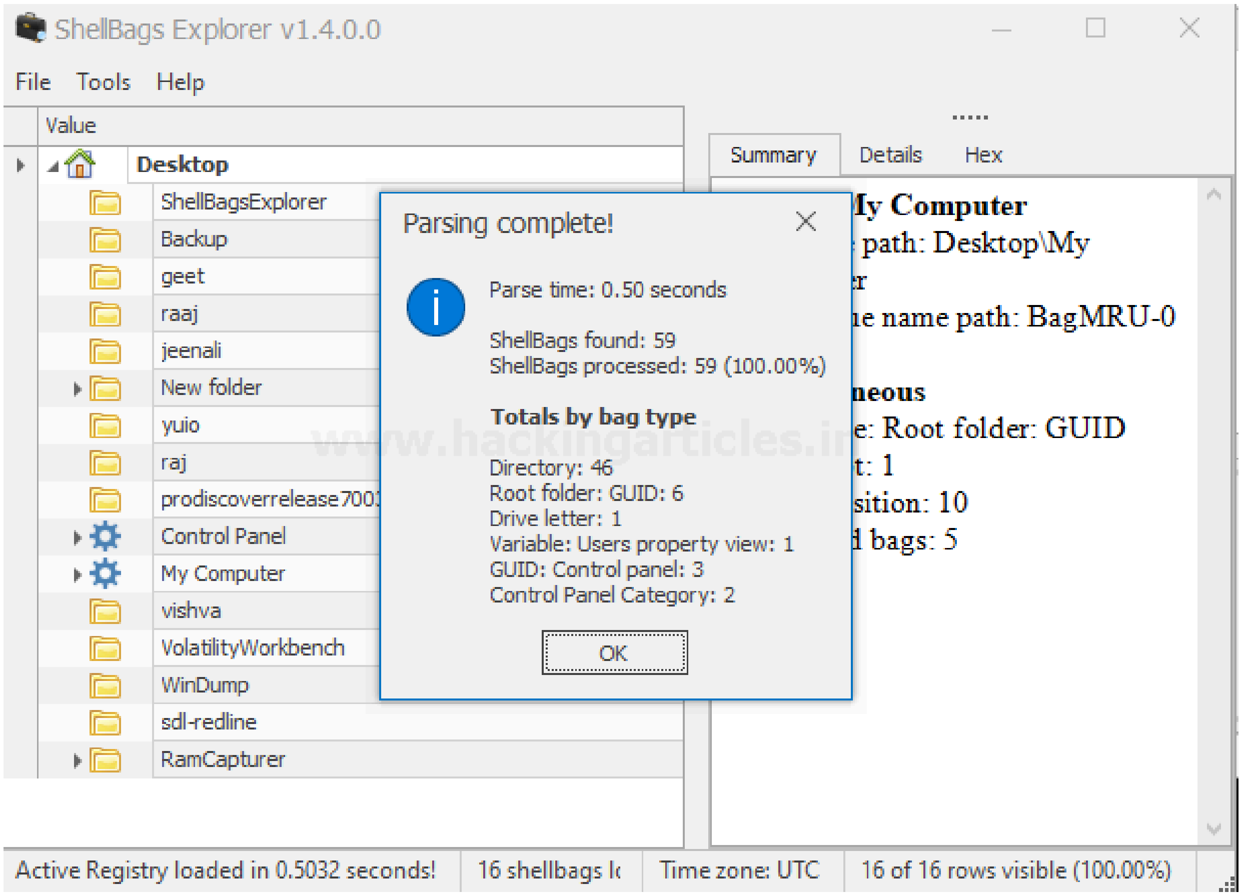
- **Shellbags explorer (GUI version)**

Active Registry Analysis

Using the shellbags explorer we can also analyze the active registry. Select load an active registry which will load the registry in use by the active user.



The shellbags are successfully parsed from the active registry.



Desktop
ShellBagsExplorer
Backup
geet
raaj
jeenali
New folder
yuio
raj
prodiscoverrelease700
Control Panel
My Computer
vishva
VolatilityWorkbench
WinDump
sdl-redline
RamCapturer

Parsing complete!

Parse time: 0.50 seconds

ShellBags found: 59
ShellBags processed: 59 (100.00%)

Totals by bag type

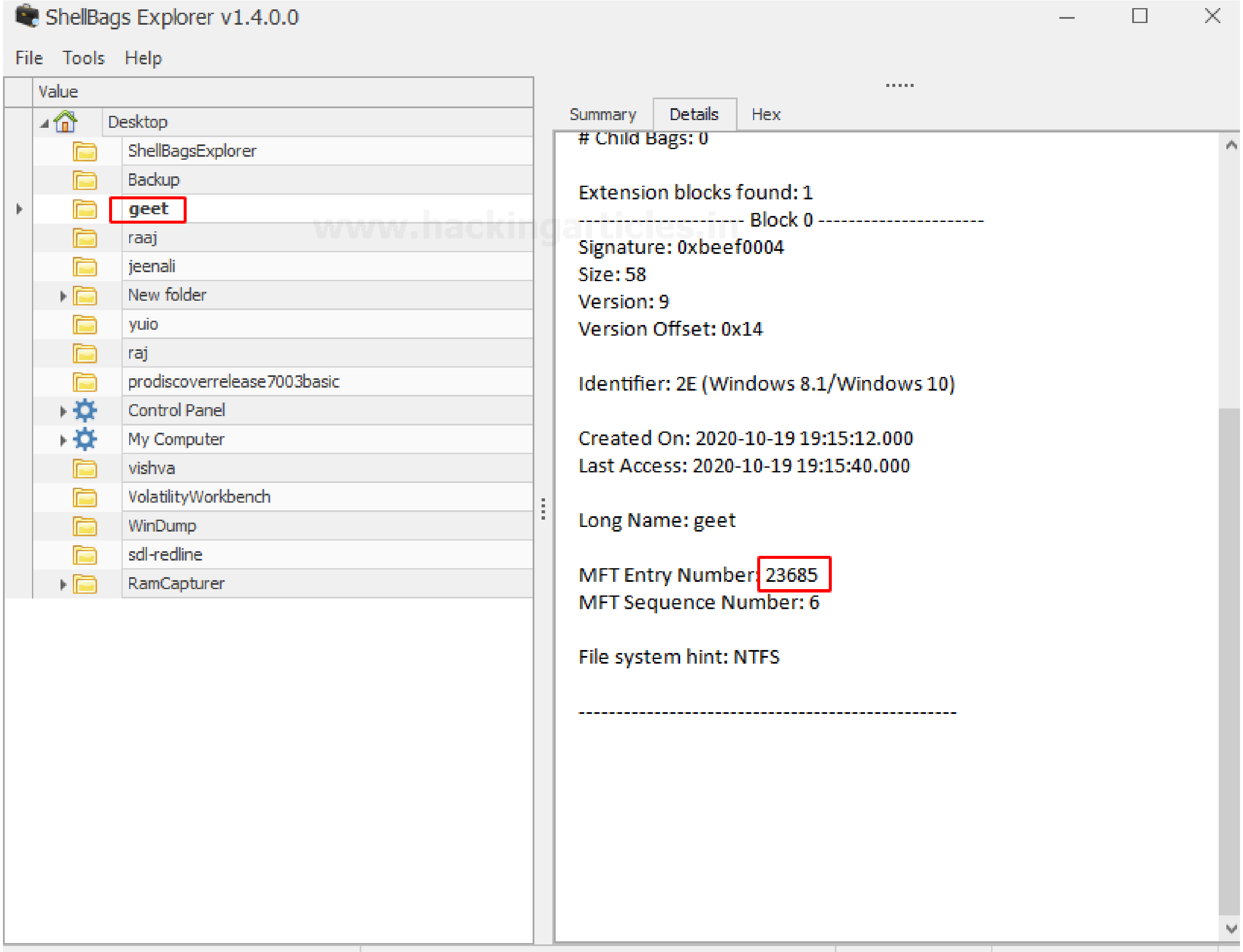
Directory: 46
Root folder: GUID: 6
Drive letter: 1
Variable: Users property view: 1
GUID: Control panel: 3
Control Panel Category: 2

ly Computer
: path: Desktop\My
r
ne name path: BagMRU-0

neous
e: Root folder: GUID
t: 1
sition: 10
d bags: 5

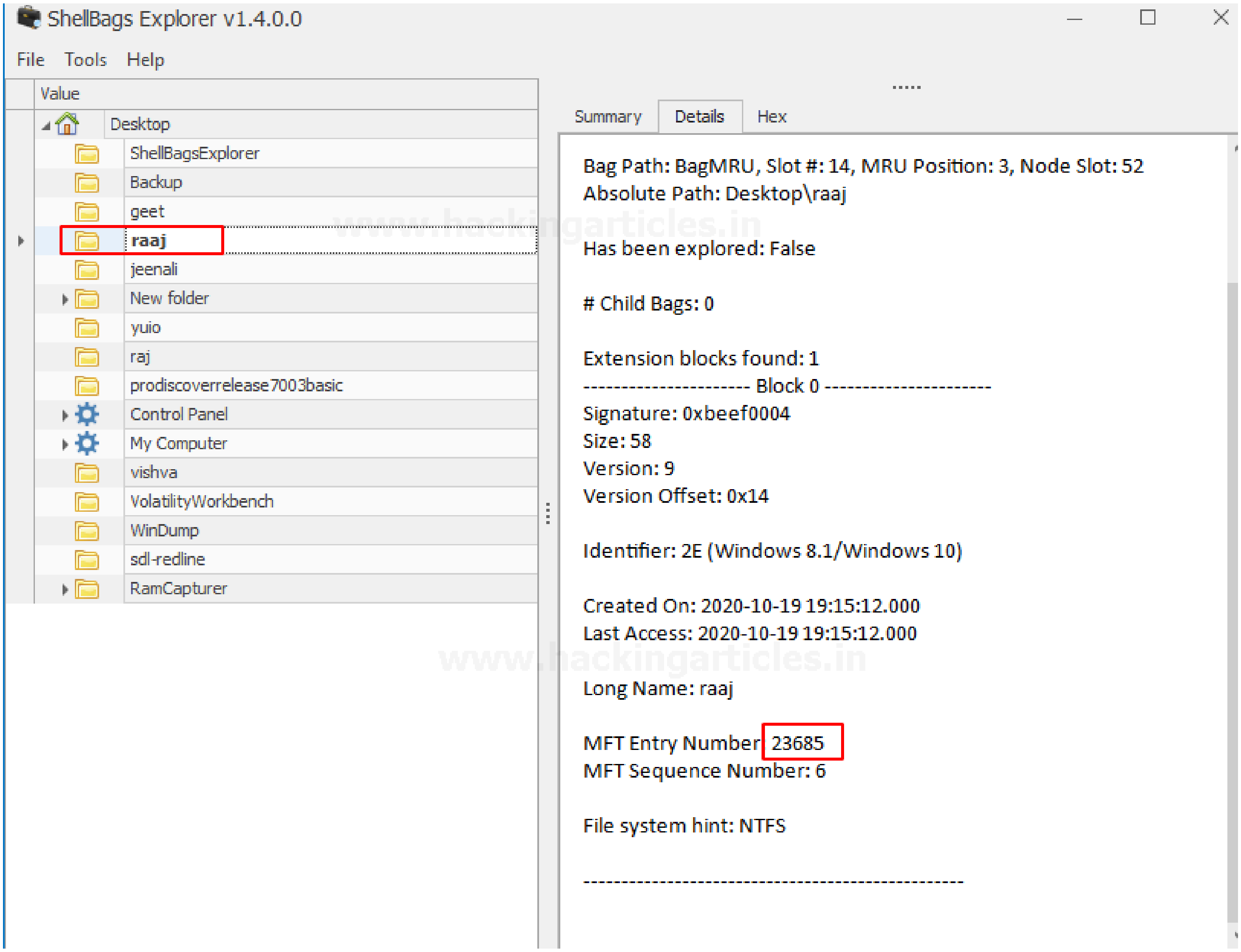
Active Registry loaded in 0.5032 seconds! | 16 shellbags lc | Time zone: UTC | 16 of 16 rows visible (100.00%)

The shellbags parse contains the shellbags entries created based on users' activities. As depicted earlier the folder renamed will have a similar MFT entry number. Here, I have created a folder named "raaj" and we will be further renaming it to "geet".



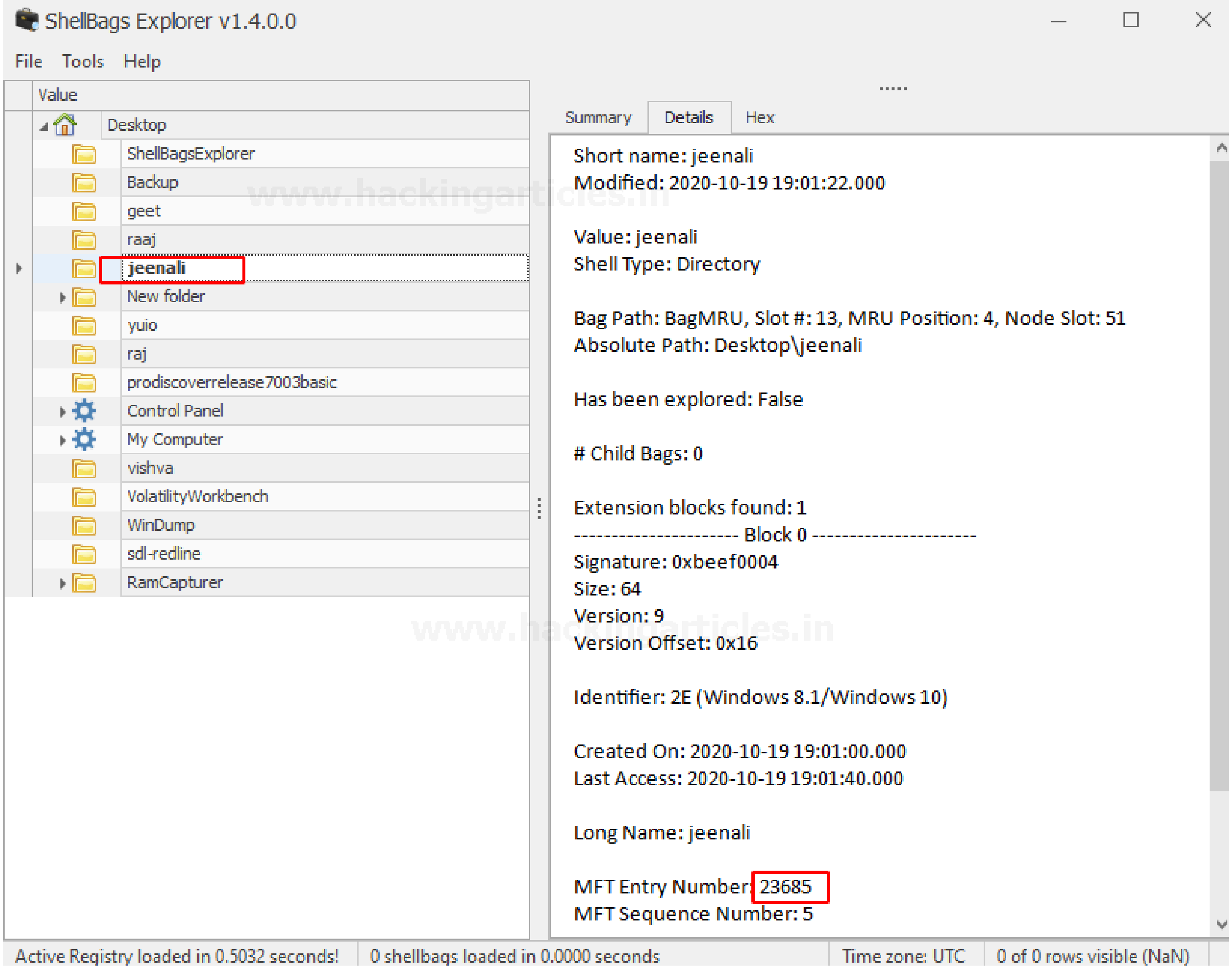
```
# Child Bags: 0

Extension blocks found: 1
--------------------- Block 0 ---------------------
Signature: 0xbeef0004
Size: 58
Version: 9
Version Offset: 0x14

Identifier: 2E (Windows 8.1/Windows 10)

Created On: 2020-10-19 19:15:12.000
Last Access: 2020-10-19 19:15:40.000

Long Name: geet

MFT Entry Number: 23685
MFT Sequence Number: 6

File system hint: NTFS

--------------------------------------------------
```

Whenever a folder is renamed an entry is stored in shellbag, the MFT entry number of both the folder will be the same.



```
Bag Path: BagMRU, Slot #: 14, MRU Position: 3, Node Slot: 52
Absolute Path: Desktop\raaj

Has been explored: False

# Child Bags: 0

Extension blocks found: 1
--------------------- Block 0 ---------------------
Signature: 0xbeef0004
Size: 58
Version: 9
Version Offset: 0x14

Identifier: 2E (Windows 8.1/Windows 10)

Created On: 2020-10-19 19:15:12.000
Last Access: 2020-10-19 19:15:12.000

Long Name: raaj

MFT Entry Number: 23685
MFT Sequence Number: 6

File system hint: NTFS

--------------------------------------------------
```

Now, once again rename the folder to jeenali. The MFT entry will be similar to the previous one.



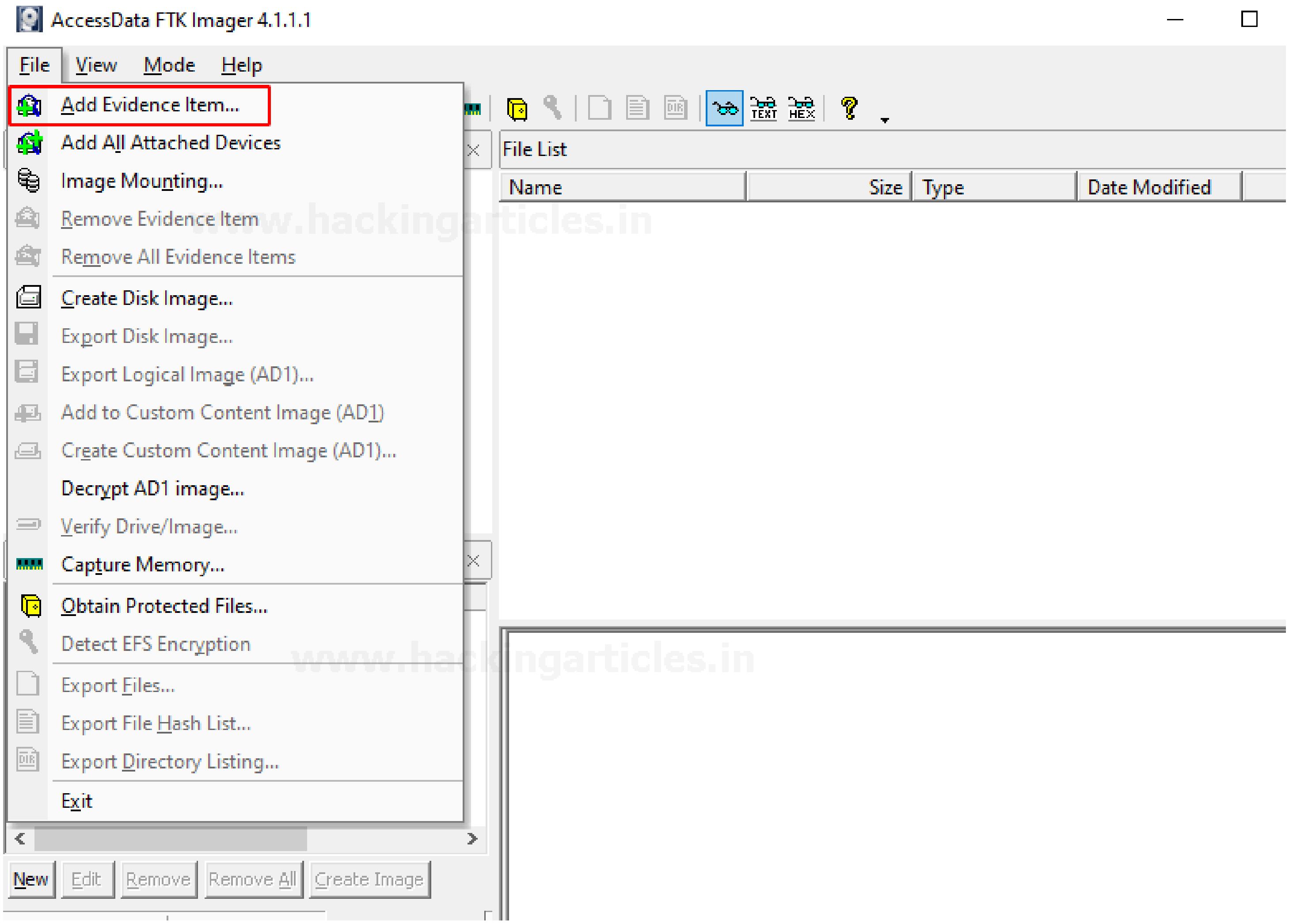
```
Short name: jeenali
Modified: 2020-10-19 19:01:22.000

Value: jeenali
Shell Type: Directory

Bag Path: BagMRU, Slot #: 13, MRU Position: 4, Node Slot: 51
Absolute Path: Desktop\jeenali

Has been explored: False

# Child Bags: 0

Extension blocks found: 1
--------------------- Block 0 ---------------------
Signature: 0xbeef0004
Size: 64
Version: 9
Version Offset: 0x16

Identifier: 2E (Windows 8.1/Windows 10)

Created On: 2020-10-19 19:01:00.000
Last Access: 2020-10-19 19:01:40.000

Long Name: jeenali

MFT Entry Number: 23685
MFT Sequence Number: 5
```

Active Registry loaded in 0.5032 seconds! | 0 shellbags loaded in 0.0000 seconds | Time zone: UTC | 0 of 0 rows visible (NaN)

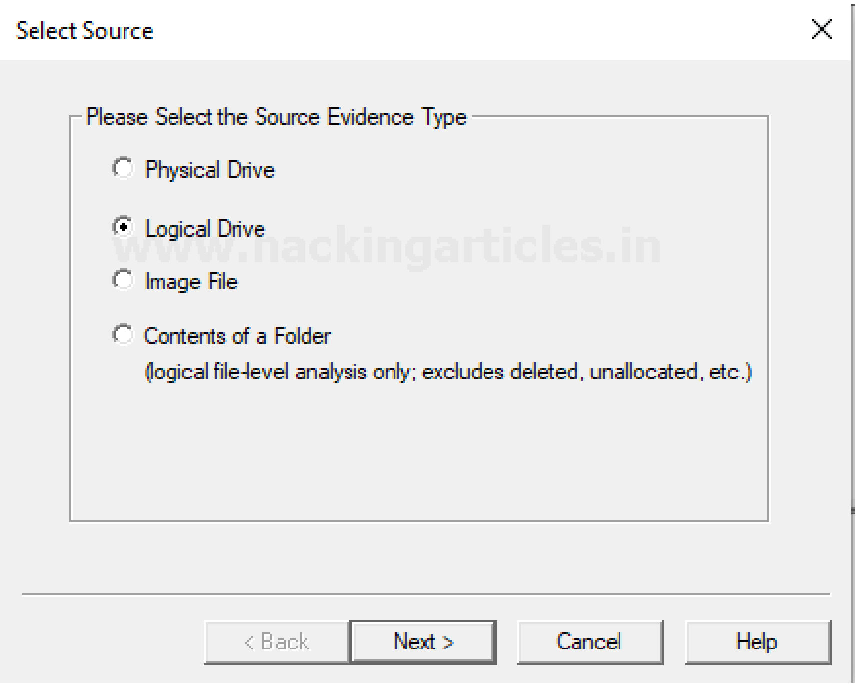
Offline registry analysis

For offline analysis, we first have to extract the shellbags file which is USRCLASS.DAT. Let's extract the shellbag file using FTK imager. Download FTK imager from **here**.

Lets' add in the evidence, go to the add evidence item.



Select the source for adding evidence as here I have selected the logical drive as usrclass.dat is present in the C drive.


Select Source

Please Select the Source Evidence Type

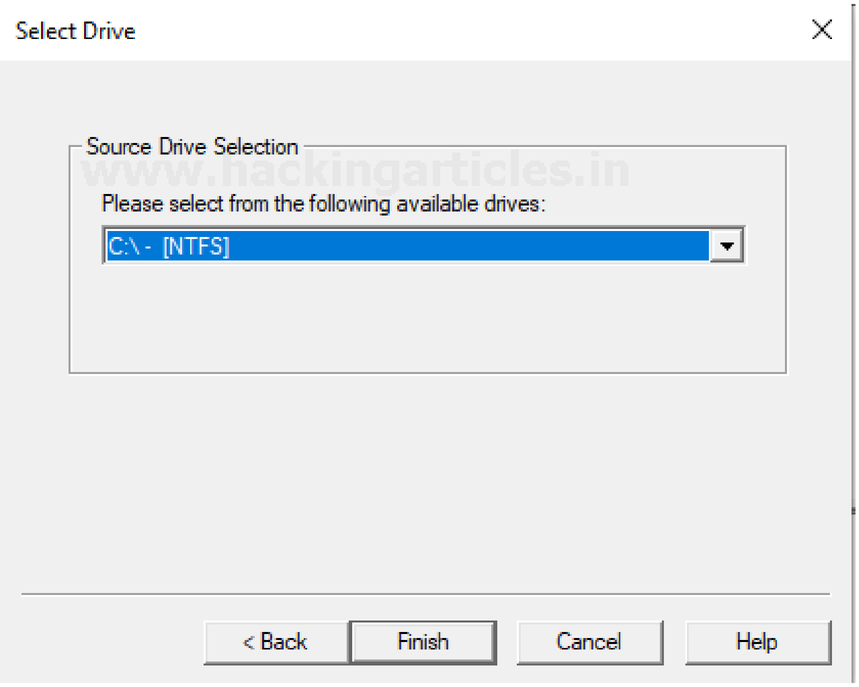
○ Physical Drive

● Logical Drive

○ Image File

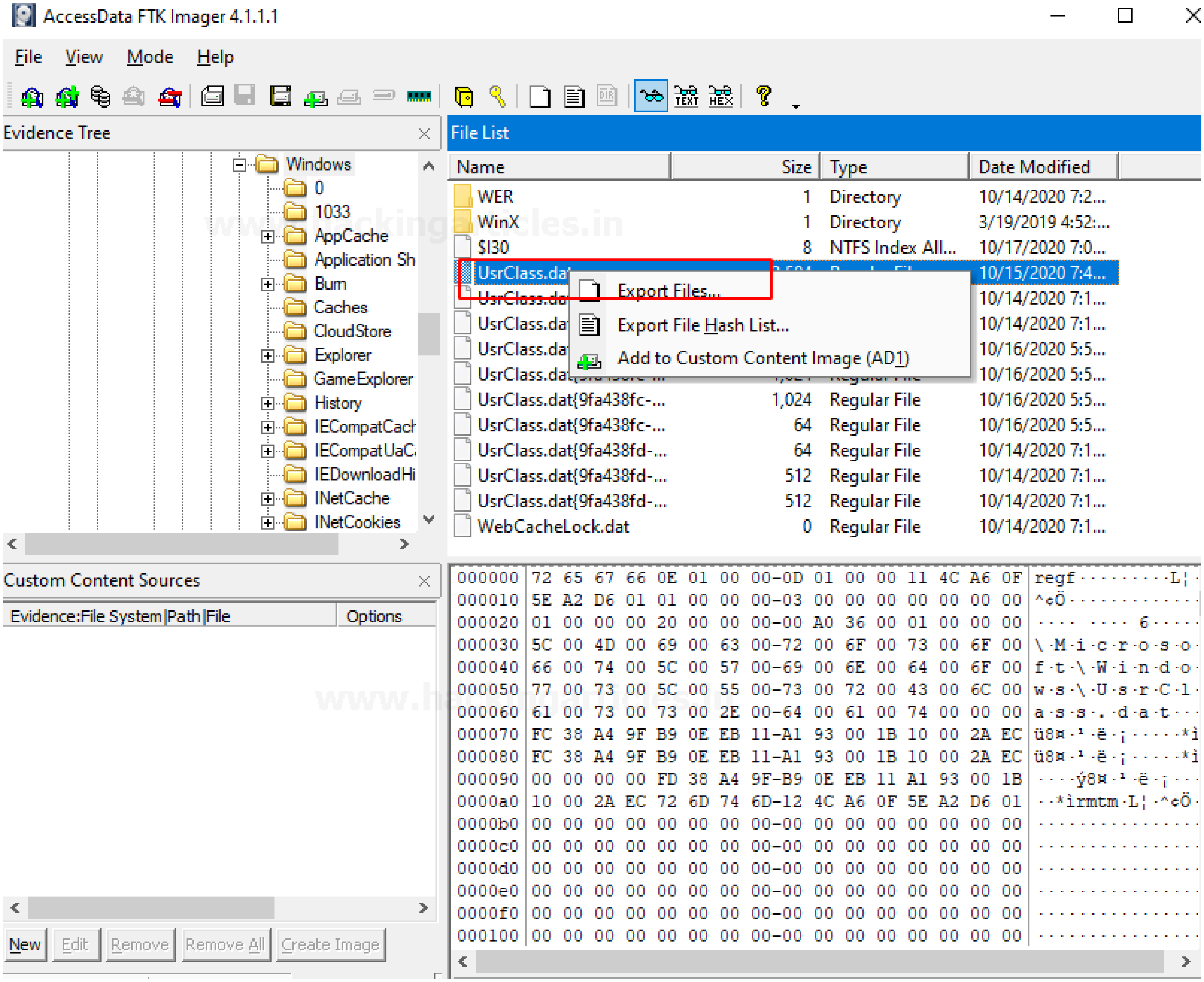
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Next, select the desired user drive. Click **Finish**.



Expand the window to the location of the usrclass.dat. Select the user you want to investigate go to the following path to extract the UsrClass.dat.

root > users > administrator >Appdata>Local>Microsoft>windows

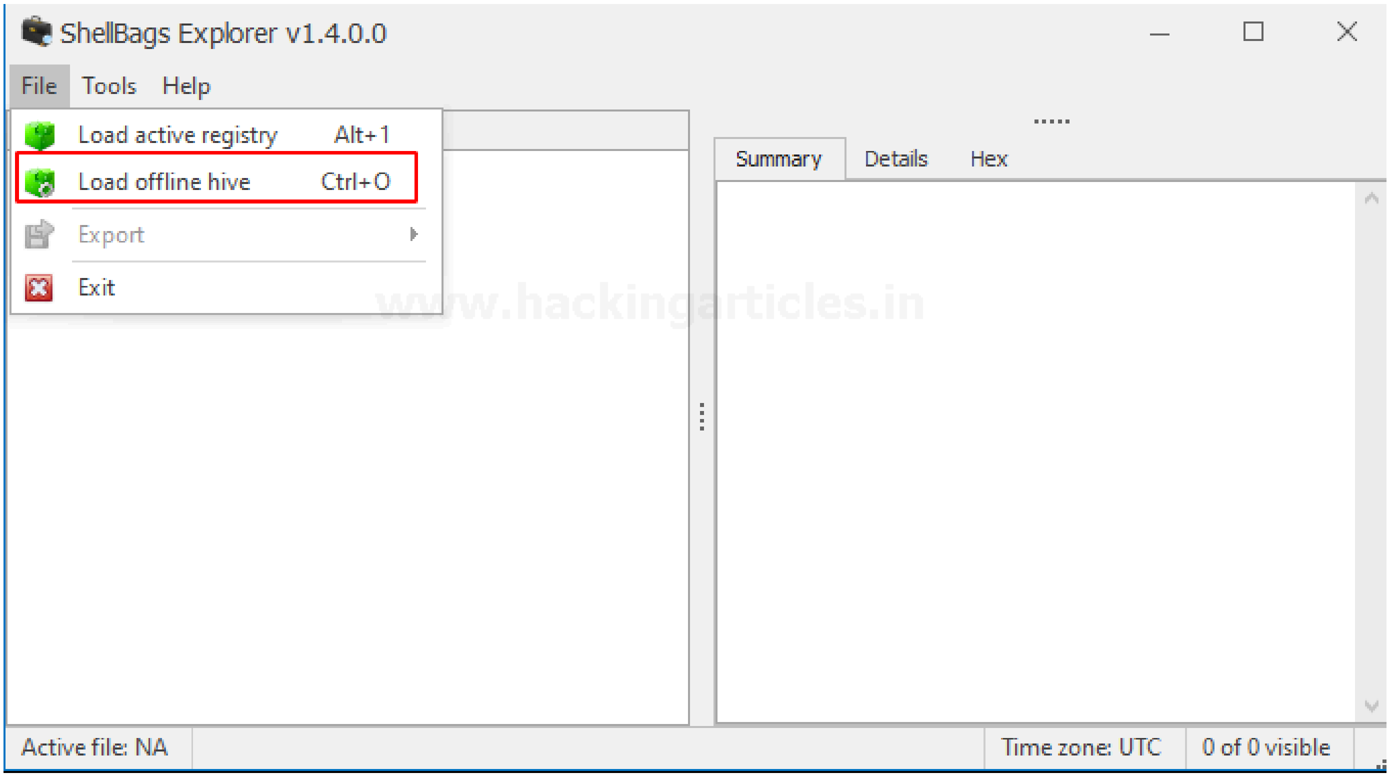


Name	Size	Type	Date Modified
WER	1	Directory	10/14/2020 7:2...
WinX	1	Directory	3/19/2019 4:52:...
$I30	8	NTFS Index All...	10/17/2020 7:0...
UsrClass.dat	[illegible]	[illegible]	10/15/2020 7:4...
UsrClass.da	[illegible]	[illegible]	10/14/2020 7:1...
UsrClass.da	[illegible]	[illegible]	10/14/2020 7:1...
UsrClass.da	[illegible]	[illegible]	10/16/2020 5:5...
UsrClass.dat	[illegible]	[illegible]	10/16/2020 5:5...
UsrClass.dat{9fa438fc-...	1,024	Regular File	10/16/2020 5:5...
UsrClass.dat{9fa438fc-...	64	Regular File	10/16/2020 5:5...
UsrClass.dat{9fa438fd-...	64	Regular File	10/14/2020 7:1...
UsrClass.dat{9fa438fd-...	512	Regular File	10/14/2020 7:1...
UsrClass.dat{9fa438fd-...	512	Regular File	10/14/2020 7:1...
WebCacheLock.dat	0	Regular File	10/14/2020 7:1...

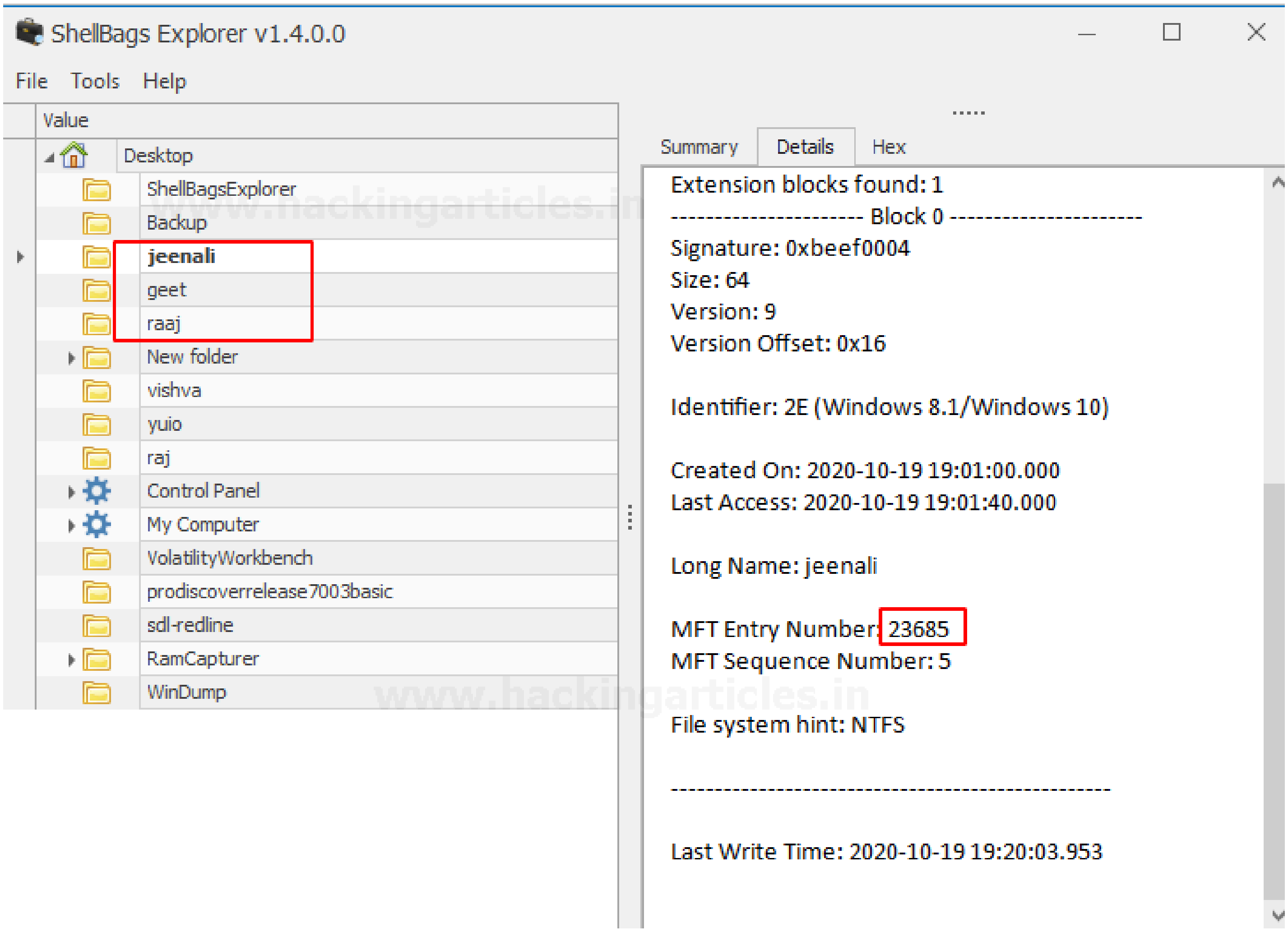
```
000000 72 65 67 66 0E 01 00 00-0D 01 00 00 11 4C A6 0F  regf········L¦·
000010 5E A2 D6 01 01 00 00 00-03 00 00 00 00 00 00 00  ^¢Ö·············
000020 01 00 00 00 20 00 00 00-00 A0 36 00 01 00 00 00  ····  ···· 6·····
000030 5C 00 4D 00 69 00 63 00-72 00 6F 00 73 00 6F 00  \·M·i·c·r·o·s·o·
000040 66 00 74 00 5C 00 57 00-69 00 6E 00 64 00 6F 00  f·t·\·W·i·n·d·o·
000050 77 00 73 00 5C 00 55 00-73 00 72 00 43 00 6C 00  w·s·\·U·s·r·C·l·
000060 61 00 73 00 73 00 2E 00-64 00 61 00 74 00 00 00  a·s·s·.·d·a·t···
000070 FC 38 A4 9F B9 0E EB 11-A1 93 00 1B 10 00 2A EC  ü8¤·¹·ë·¡·····*ì
000080 FC 38 A4 9F B9 0E EB 11-A1 93 00 1B 10 00 2A EC  ü8¤·¹·ë·¡·····*ì
000090 00 00 00 00 FD 38 A4 9F-B9 0E EB 11 A1 93 00 1B  ····ý8¤·¹·ë·¡···
0000a0 10 00 2A EC 72 6D 74 6D-12 4C A6 0F 5E A2 D6 01  ··*ìrmtm·L¦·^¢Ö·
0000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

We will be analyzing the usrclass.dat extracted from the above step using shell bag explorer by Eric Zimmerman.

As we have exported the registry hives we will choose "**load offline hive**"

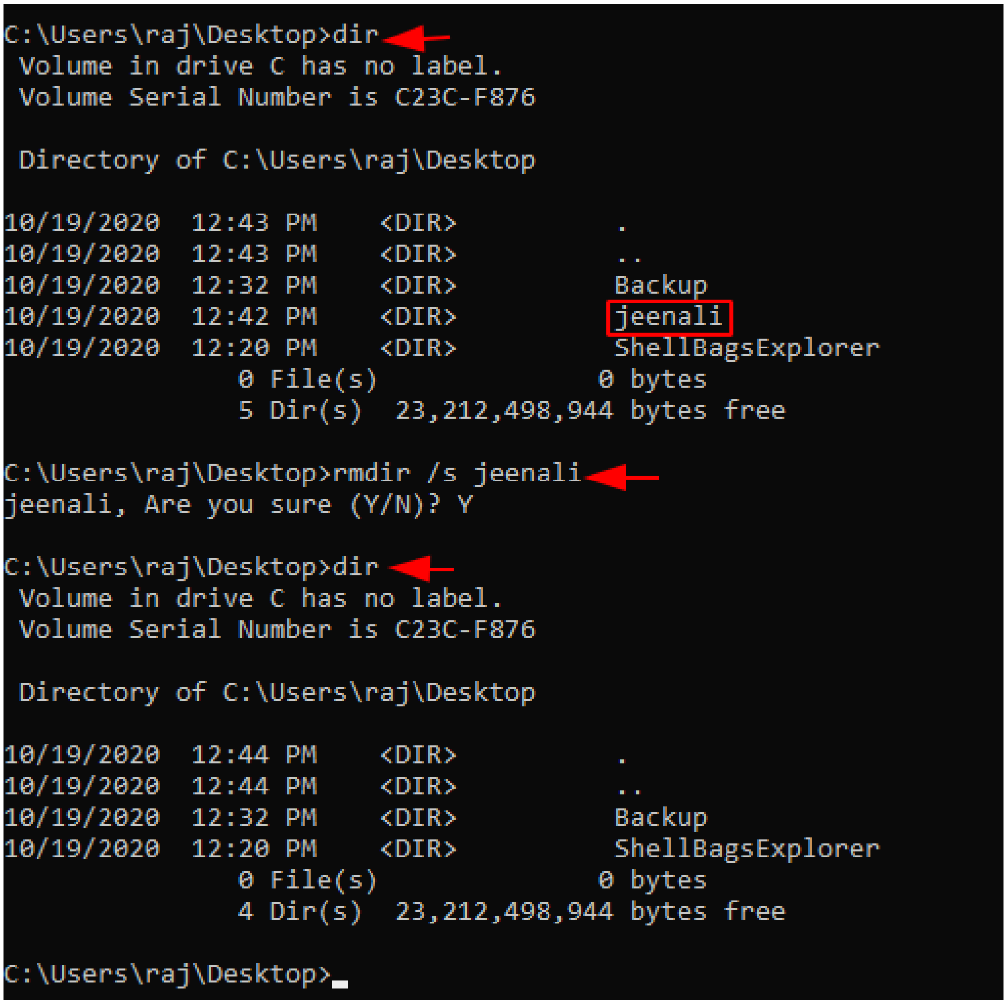


After successful parsing of the extracted shellbags file, you will be able to see the entries for folders browsed, created, deleted, etc. Here is the entry of the folders renamed earlier, the MFT entry number is the same for the three folders.



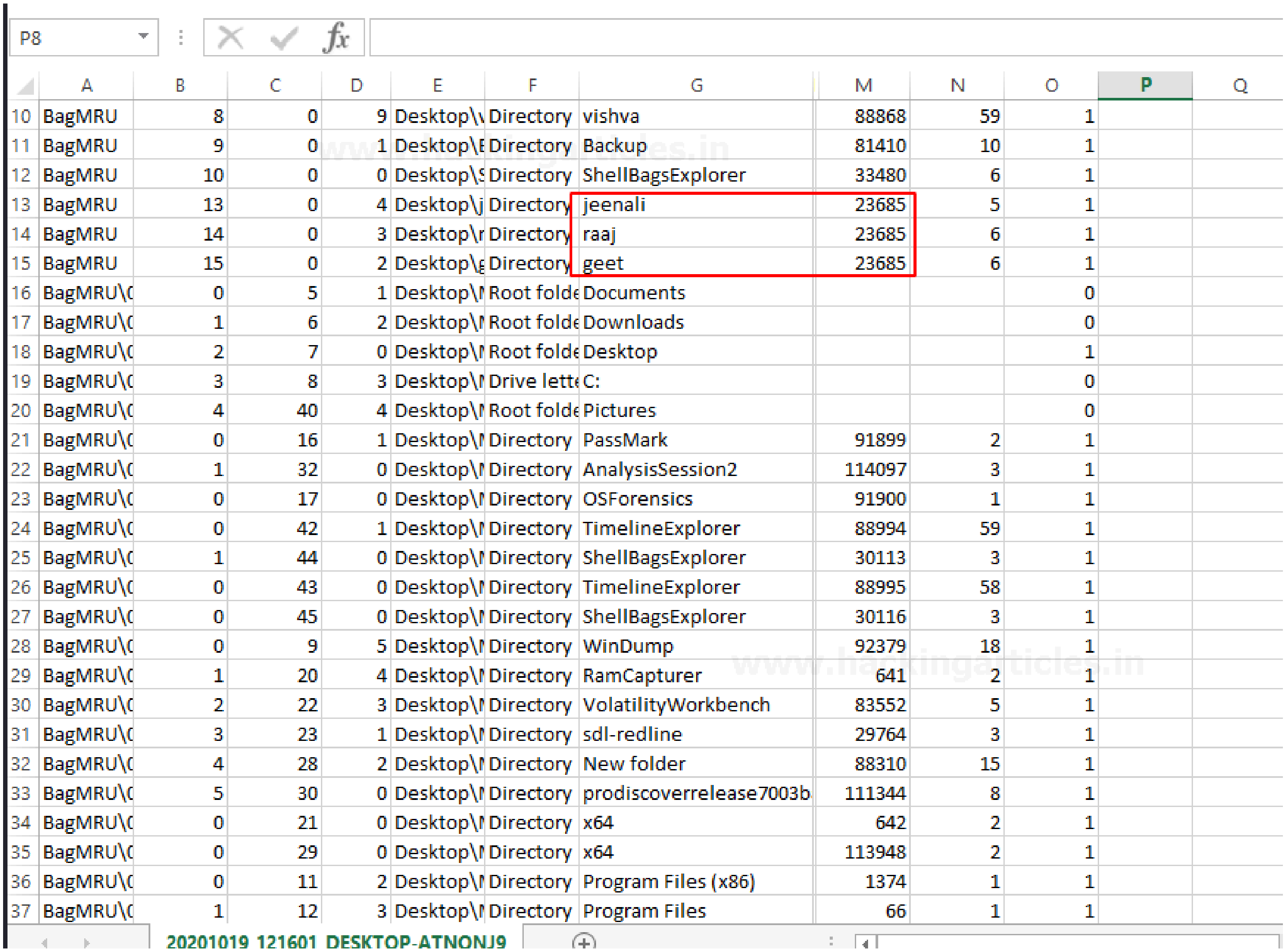
```
Extension blocks found: 1
---------------------- Block 0 ----------------------
Signature: 0xbeef0004
Size: 64
Version: 9
Version Offset: 0x16

Identifier: 2E (Windows 8.1/Windows 10)

Created On: 2020-10-19 19:01:00.000
Last Access: 2020-10-19 19:01:40.000

Long Name: jeenali

MFT Entry Number: 23685
MFT Sequence Number: 5

File system hint: NTFS

--------------------------------------------------

Last Write Time: 2020-10-19 19:20:03.953
```

Now here, I have deleted the folder named “jeenali”. Now lets’ check the shellbags data whether the deleted folder still exists or not.



```
C:\Users\raj\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is C23C-F876

 Directory of C:\Users\raj\Desktop

10/19/2020  12:43 PM    <DIR>          .
10/19/2020  12:43 PM    <DIR>          ..
10/19/2020  12:32 PM    <DIR>          Backup
10/19/2020  12:42 PM    <DIR>          jeenali
10/19/2020  12:20 PM    <DIR>          ShellBagsExplorer
               0 File(s)              0 bytes
               5 Dir(s)  23,212,498,944 bytes free

C:\Users\raj\Desktop>rmdir /s jeenali
jeenali, Are you sure (Y/N)? Y

C:\Users\raj\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is C23C-F876

 Directory of C:\Users\raj\Desktop

10/19/2020  12:44 PM    <DIR>          .
10/19/2020  12:44 PM    <DIR>          ..
10/19/2020  12:32 PM    <DIR>          Backup
10/19/2020  12:20 PM    <DIR>          ShellBagsExplorer
               0 File(s)              0 bytes
               4 Dir(s)  23,212,498,944 bytes free

C:\Users\raj\Desktop>
```

Yes, the shellbags store the entry even though the folder was deleted later.



	A	B	C	D	E	F	G	M	N	O	P	Q
10	BagMRU	8	0	9	Desktop\\	Directory	vishva	88868	59	1		
11	BagMRU	9	0	1	Desktop\E	Directory	Backup	81410	10	1		
12	BagMRU	10	0	0	Desktop\S	Directory	ShellBagsExplorer	33480	6	1		
13	BagMRU	13	0	4	Desktop\j	Directory	jeenali	23685	5	1		
14	BagMRU	14	0	3	Desktop\r	Directory	raaj	23685	6	1		
15	BagMRU	15	0	2	Desktop\g	Directory	geet	23685	6	1		
16	BagMRU\(	0	5	1	Desktop\I	Root folde	Documents			0		
17	BagMRU\(	1	6	2	Desktop\I	Root folde	Downloads			0		
18	BagMRU\(	2	7	0	Desktop\I	Root folde	Desktop			1		
19	BagMRU\(	3	8	3	Desktop\I	Drive lette	C:			0		
20	BagMRU\(	4	40	4	Desktop\I	Root folde	Pictures			0		
21	BagMRU\(	0	16	1	Desktop\I	Directory	PassMark	91899	2	1		
22	BagMRU\(	1	32	0	Desktop\I	Directory	AnalysisSession2	114097	3	1		
23	BagMRU\(	0	17	0	Desktop\I	Directory	OSForensics	91900	1	1		
24	BagMRU\(	0	42	1	Desktop\I	Directory	TimelineExplorer	88994	59	1		
25	BagMRU\(	1	44	0	Desktop\I	Directory	ShellBagsExplorer	30113	3	1		
26	BagMRU\(	0	43	0	Desktop\I	Directory	TimelineExplorer	88995	58	1		
27	BagMRU\(	0	45	0	Desktop\I	Directory	ShellBagsExplorer	30116	3	1		
28	BagMRU\(	0	9	5	Desktop\I	Directory	WinDump	92379	18	1		
29	BagMRU\(	1	20	4	Desktop\I	Directory	RamCapturer	641	2	1		
30	BagMRU\(	2	22	3	Desktop\I	Directory	VolatilityWorkbench	83552	5	1		
31	BagMRU\(	3	23	1	Desktop\I	Directory	sdl-redline	29764	3	1		
32	BagMRU\(	4	28	2	Desktop\I	Directory	New folder	88310	15	1		
33	BagMRU\(	5	30	0	Desktop\I	Directory	prodiscoverrelease7003b	111344	8	1		
34	BagMRU\(	0	21	0	Desktop\I	Directory	x64	642	2	1		
35	BagMRU\(	0	29	0	Desktop\I	Directory	x64	113948	2	1		
36	BagMRU\(	0	11	2	Desktop\I	Directory	Program Files (x86)	1374	1	1		
37	BagMRU\(	1	12	3	Desktop\I	Directory	Program Files	66	1	1		

Shellbags stores the entries of the directories accessed by the user, user preferences such as window size, icon size. Shellbags explorer parses the shellbags entries shows the absolute path of the directory accessed, creation time, file system, child bags. The tool classifies the folders accessed according to the location of the folder. Shellbags are created for compressed files (ZIP files), command prompt, search window, renaming, moving, and deleting a folder.