# User Behavior Analysis:

- User Behavior
- UserAssist
- RecentDocs
- ShellBags

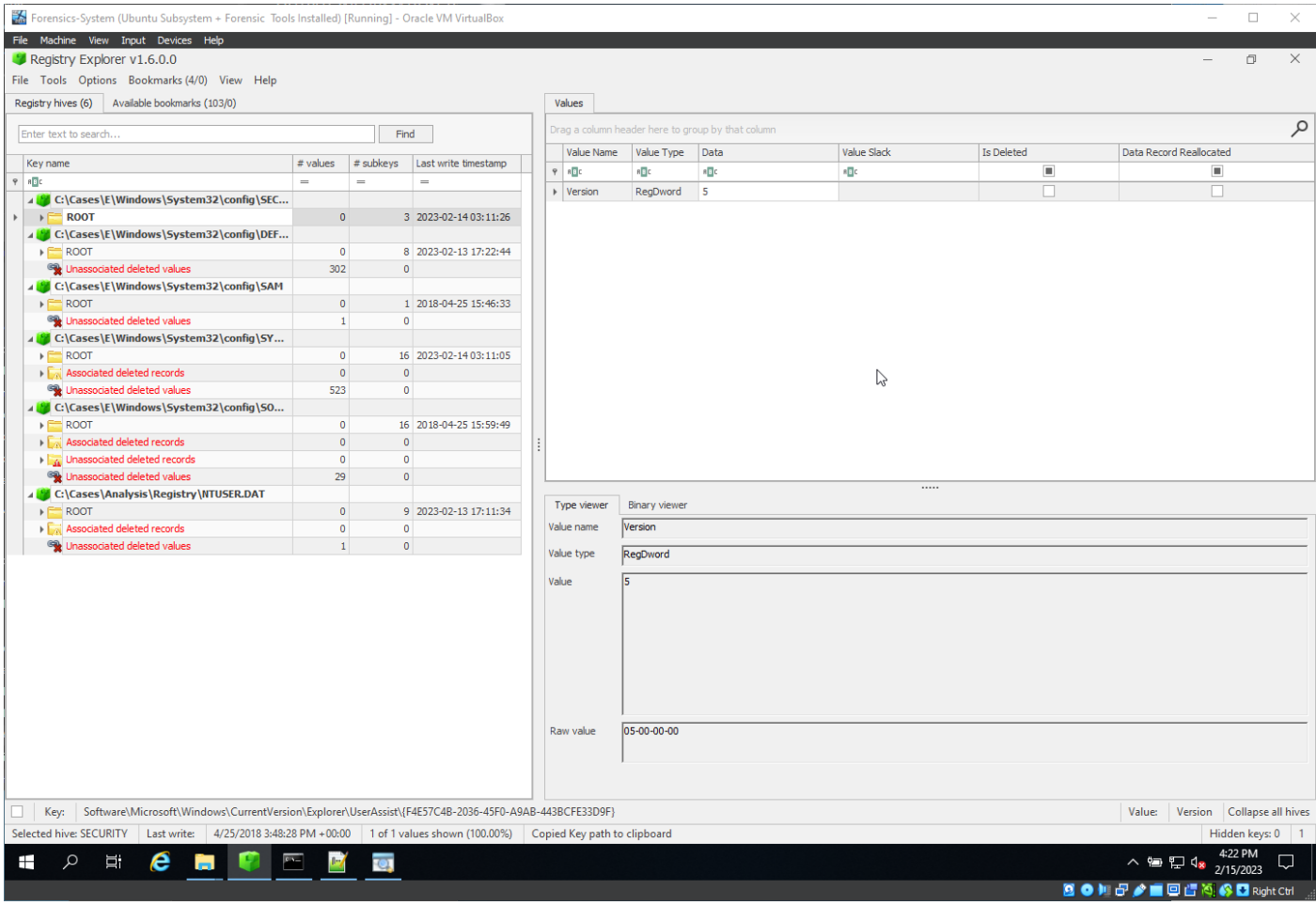
## User Behavior

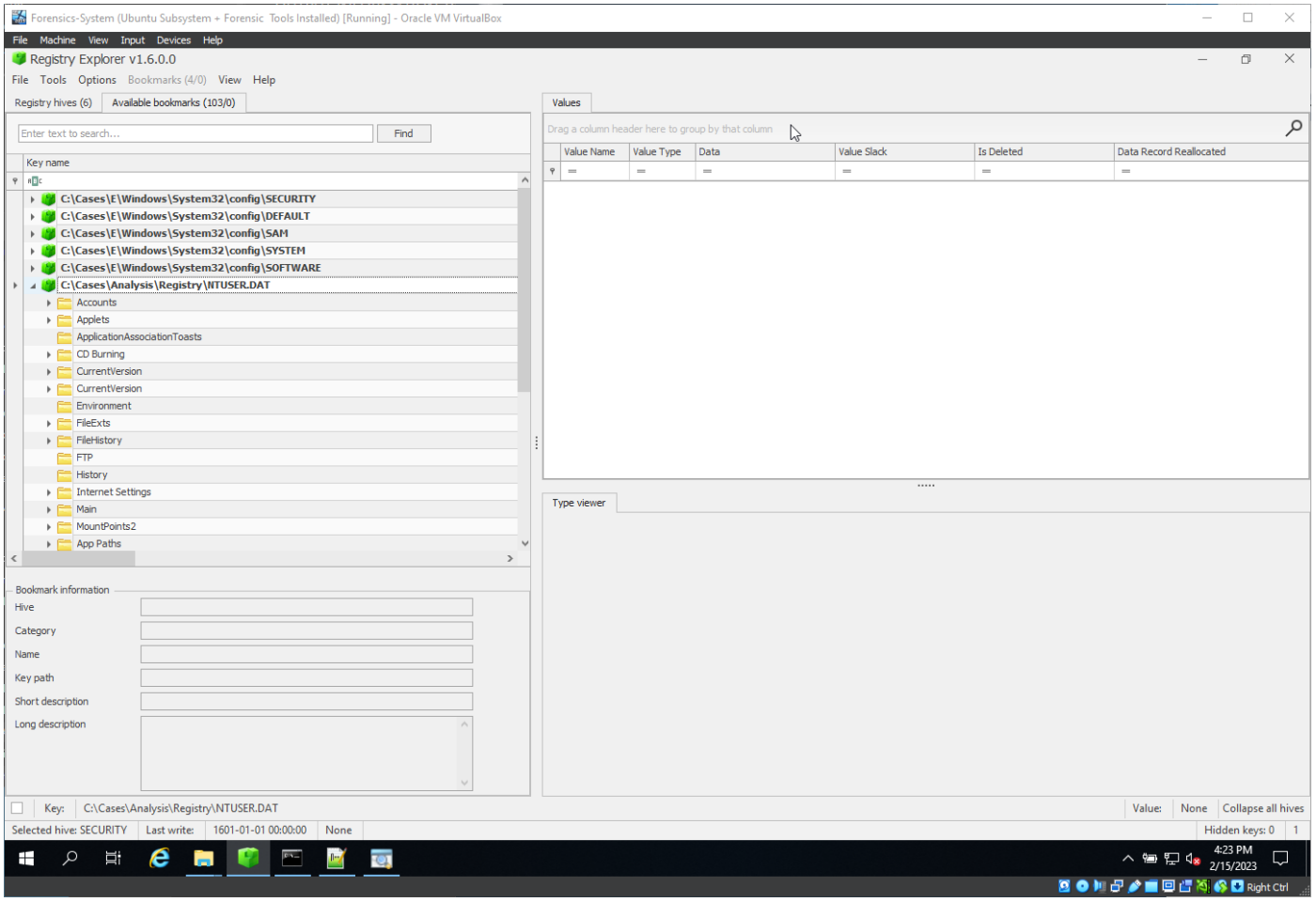
- UserAssist – applications opened
- RecentDocs – files and folders opened
- Shellbags – locations browsed by the user
- Open / Save MRU – files that were opened
- Last-Visited MRU – applications used to open files

## UserAssist

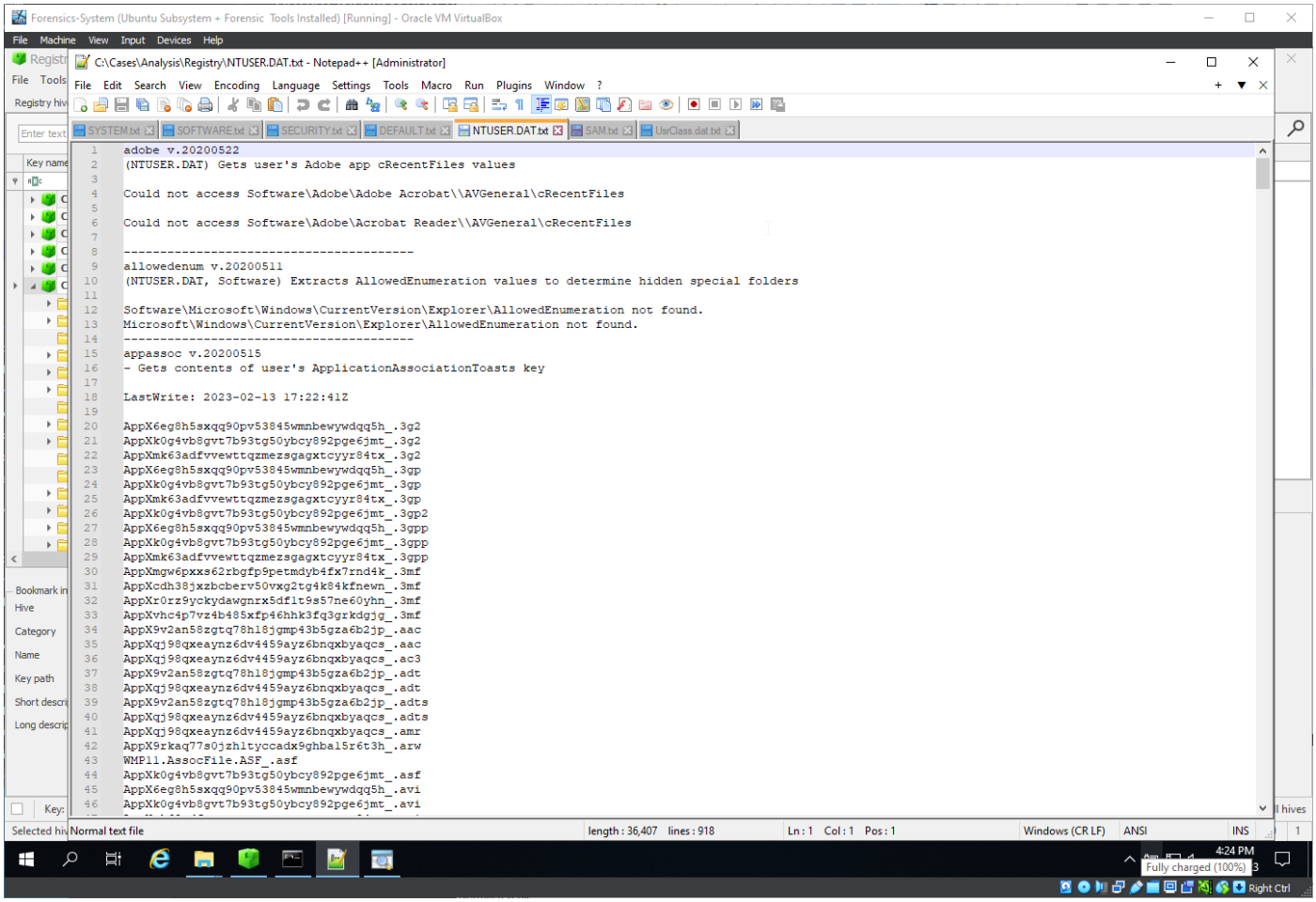
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\

- {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} - List of applications, files, links, and another objects that have been accessed.
- {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} - Lists the shortcut links used to start programs.
- Drag and drop the NTUSER.DAT registry hive in Registry Explorer, then move to Available Bookmarks.
- You can use Registry Explorer or the text file NTUSER.DAT.txt for information, either option is good.

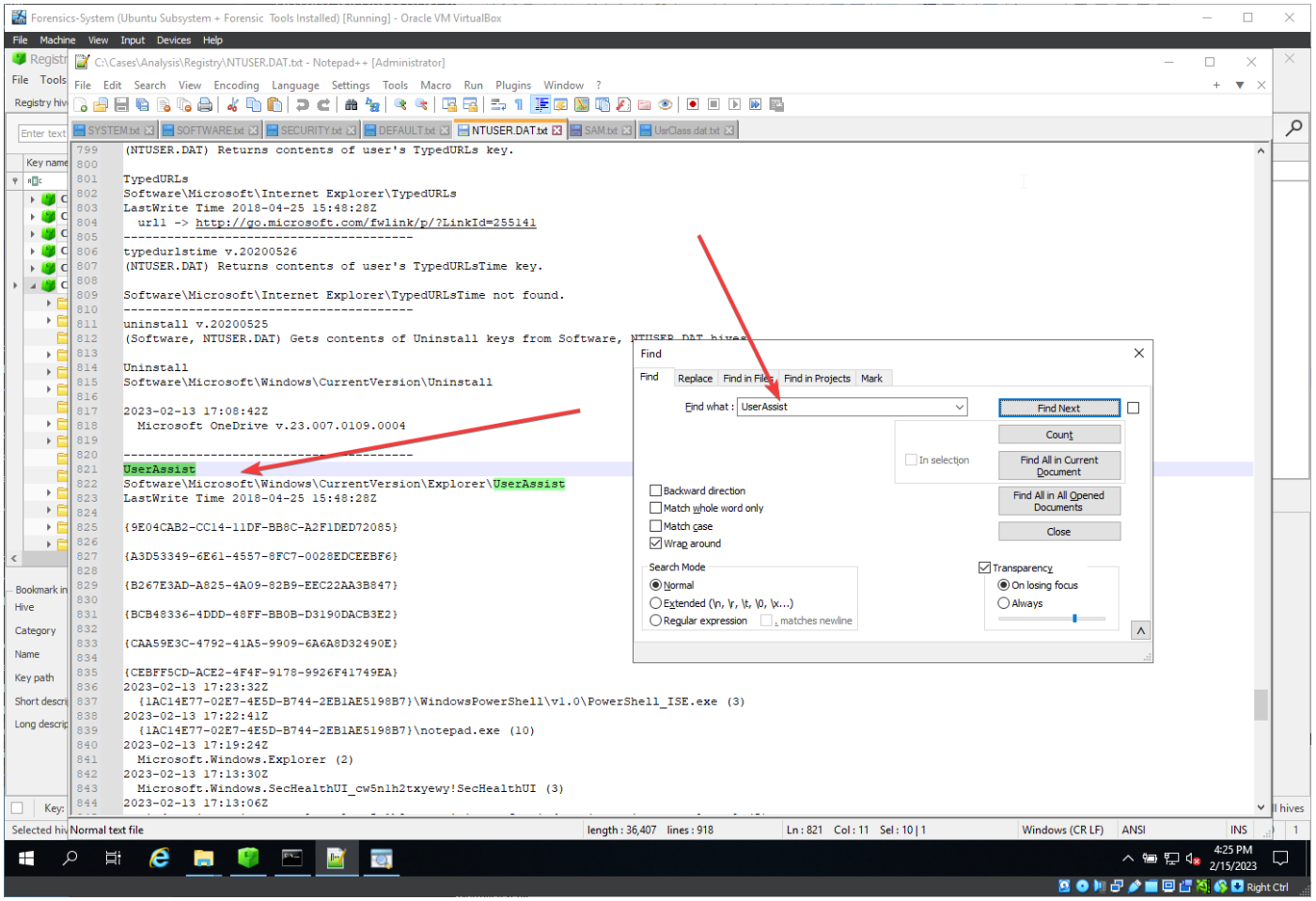

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (6)
Available bookmarks (103/0)
Enter text to search...
Find
Key name
# values
# subkeys
Last write timestamp
C:\Cases\E\Windows\System32\config\SEC...
ROOT 0 3 2023-02-14 03:11:26
C:\Cases\E\Windows\System32\config\DEF...
ROOT 0 8 2023-02-13 17:22:44
Unassociated deleted values 302 0
C:\Cases\E\Windows\System32\config\SAM
ROOT 0 1 2018-04-25 15:46:33
Unassociated deleted values 1 0
C:\Cases\E\Windows\System32\config\SY...
ROOT 0 16 2023-02-14 03:11:05
Associated deleted records 0 0
Unassociated deleted values 523 0
C:\Cases\E\Windows\System32\config\SO...
ROOT 0 16 2018-04-25 15:59:49
Associated deleted records 0 0
Unassociated deleted records 0 0
Unassociated deleted values 29 0
C:\Cases\Analysis\Registry\NTUSER.DAT
ROOT 0 9 2023-02-13 17:11:34
Associated deleted records 0 0
Unassociated deleted values 1 0
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value Slack
Is Deleted
Data Record Reallocated
Version RegDword 5
Type viewer
Binary viewer
Value name Version
Value type RegDword
Value 5
Raw value 05-00-00-00
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
Value: Version
Collapse all hives
Selected hive: SECURITY
Last write: 4/25/2018 3:48:28 PM +00:00
1 of 1 values shown (100.00%)
Copied Key path to clipboard
Hidden keys: 0
4:22 PM
2/15/2023
Right Ctrl



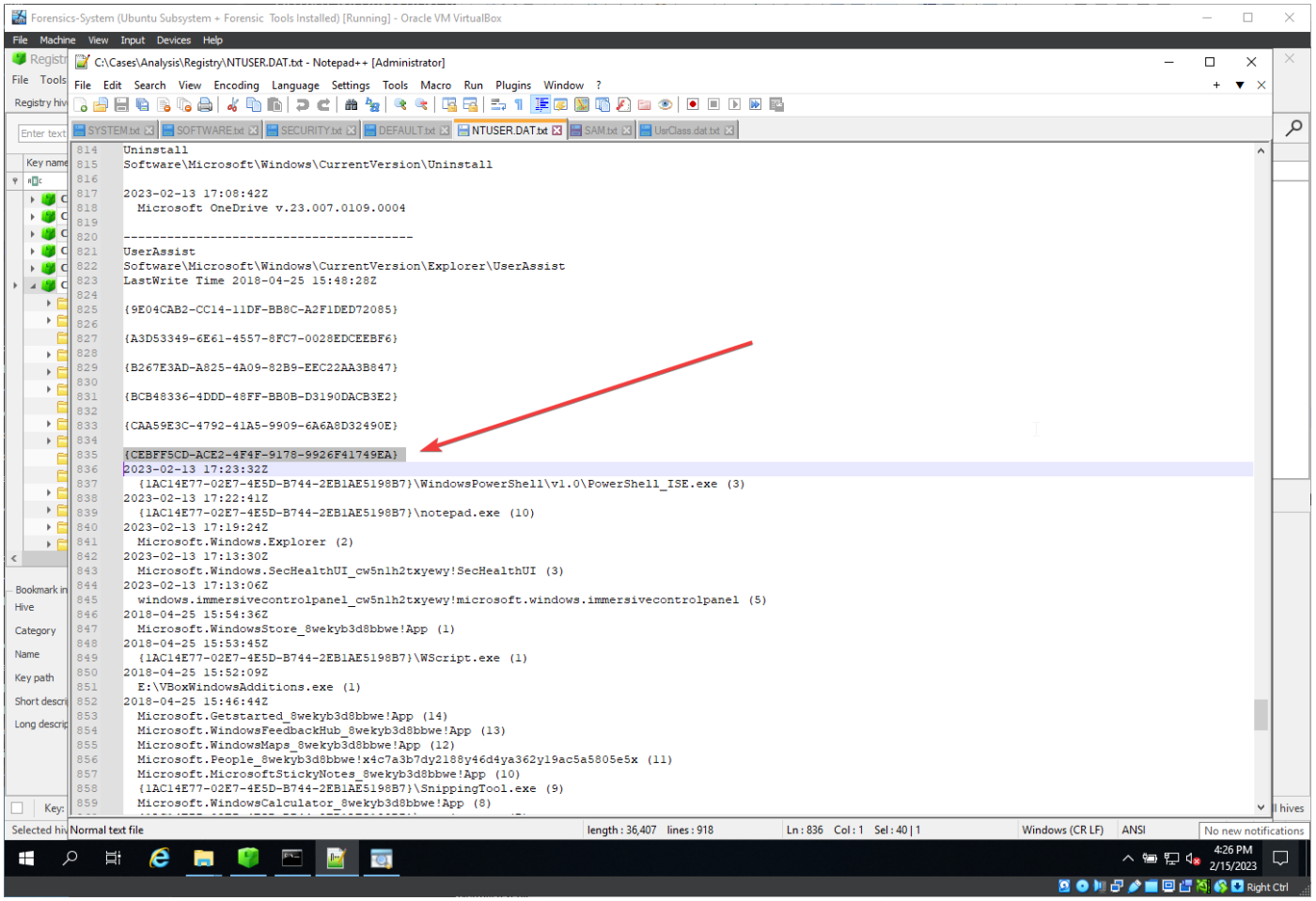

- NTUSER.DAT.txt:



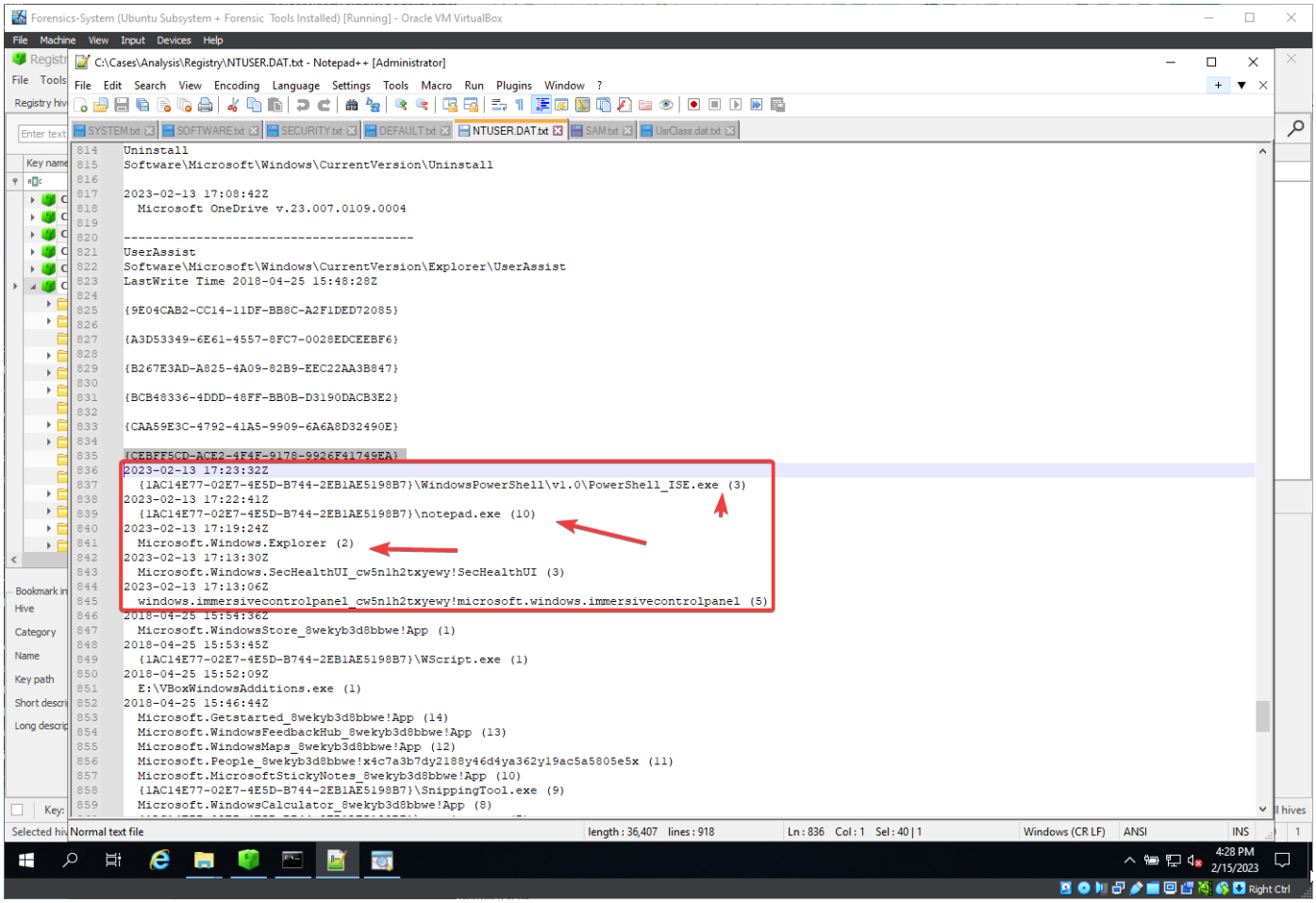

- Search for UserAssist:

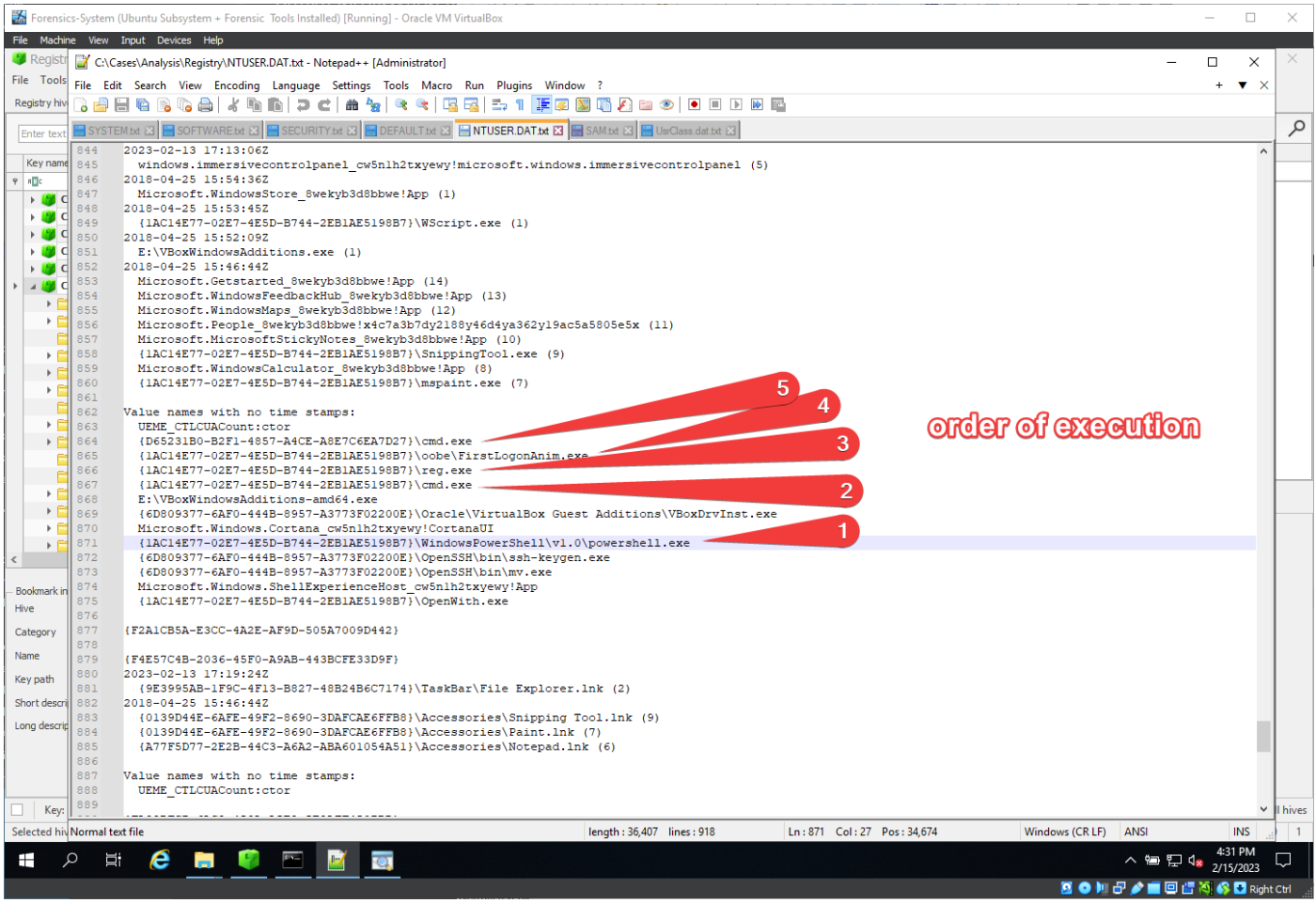



- Search for the particular subkey we want to see for the investigation:

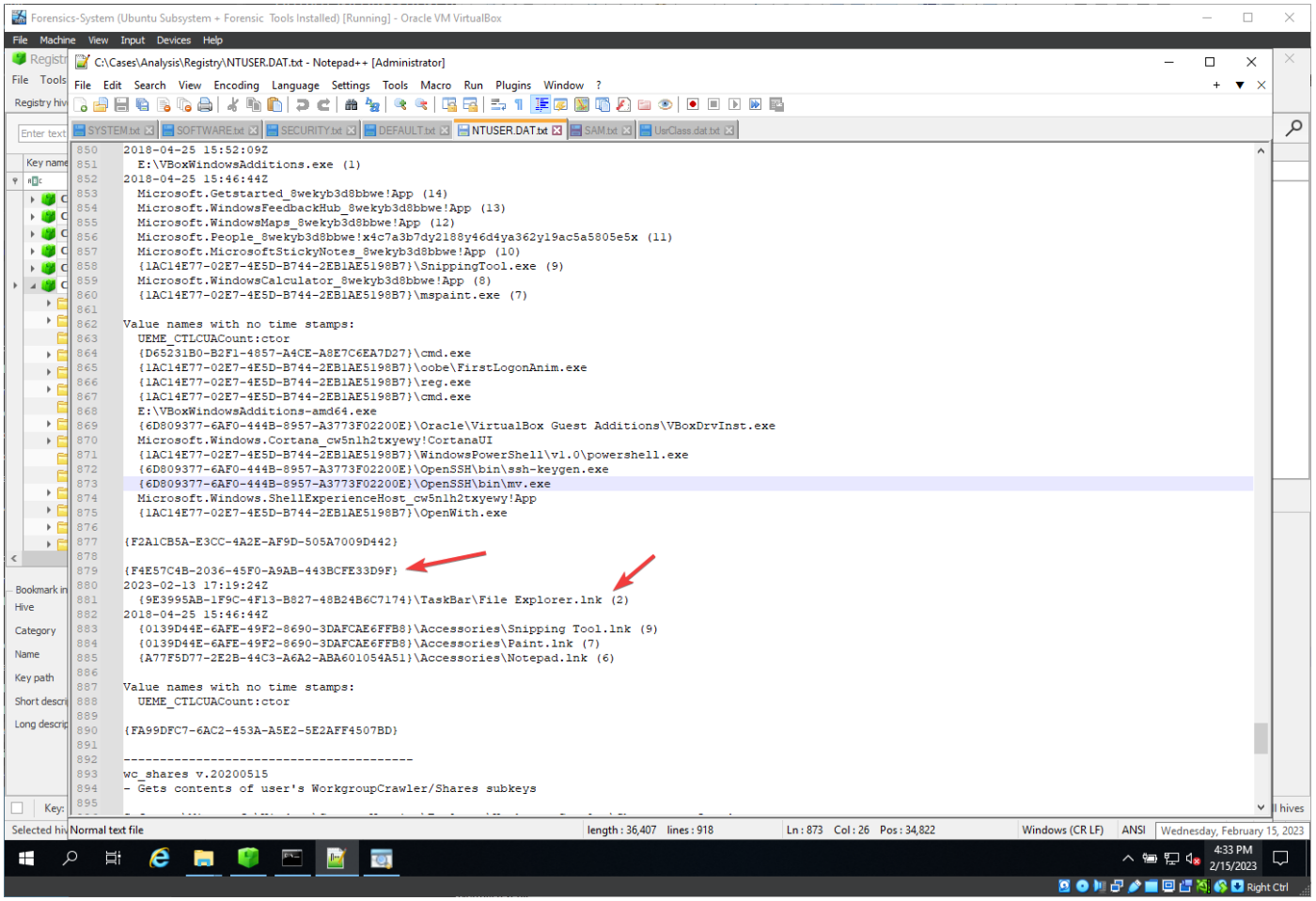



- We need to search for interesting executables accessed in the timeline we want to see:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
C:\Cases\Analysis\Registry\NTUSER.DAT.txt - Notepad++ [Administrator]
SYSTEM.txt
SOFTWARE.txt
SECURITY.txt
DEFAULT.txt
NTUSER.DAT.txt
SAM.txt
UsrClass.dat.txt
Uninstall
Software\Microsoft\Windows\CurrentVersion\Uninstall
2023-02-13 17:08:42Z
Microsoft OneDrive v.23.007.0109.0004
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2018-04-25 15:48:28Z
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2023-02-13 17:23:32Z
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\PowerShell_ISE.exe (3)
2023-02-13 17:22:41Z
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (10)
2023-02-13 17:19:24Z
Microsoft.Windows.Explorer (2)
2023-02-13 17:13:30Z
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI (3)
2023-02-13 17:13:06Z
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel (5)
2018-04-25 15:54:36Z
Microsoft.WindowsStore_8wekyb3d8bbwe!App (1)
2018-04-25 15:53:45Z
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WScript.exe (1)
2018-04-25 15:52:09Z
E:\VBoxWindowsAdditions.exe (1)
2018-04-25 15:46:44Z
Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (11)
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (8)
Normal text file
length : 36,407 lines : 918
Ln : 836 Col : 1 Sel : 40 | 1
Windows (CR LF)
ANSI
INS
4:28 PM
2/15/2023
Right Ctrl

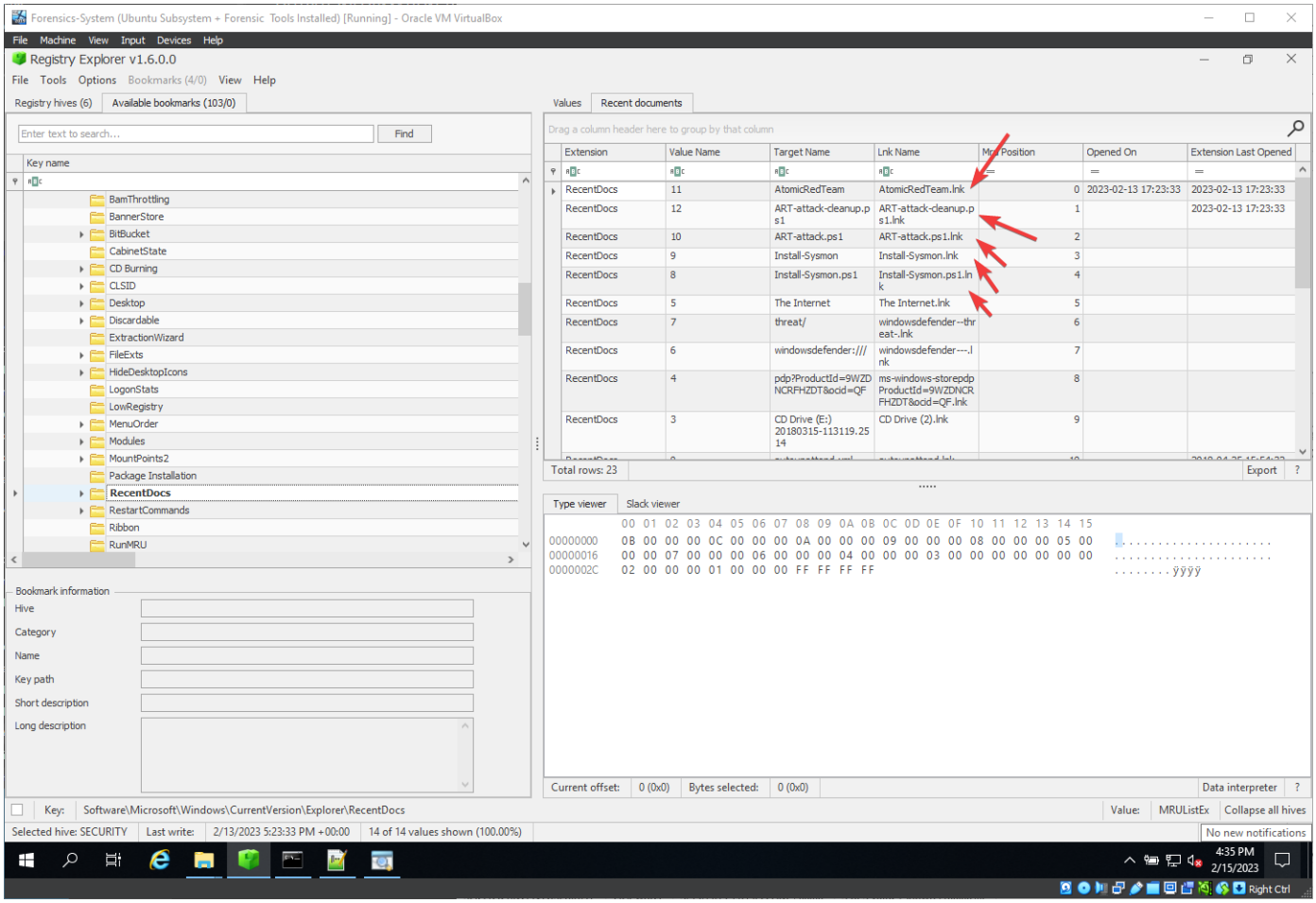



- Search for the particular subkey we want to see for the investigation:

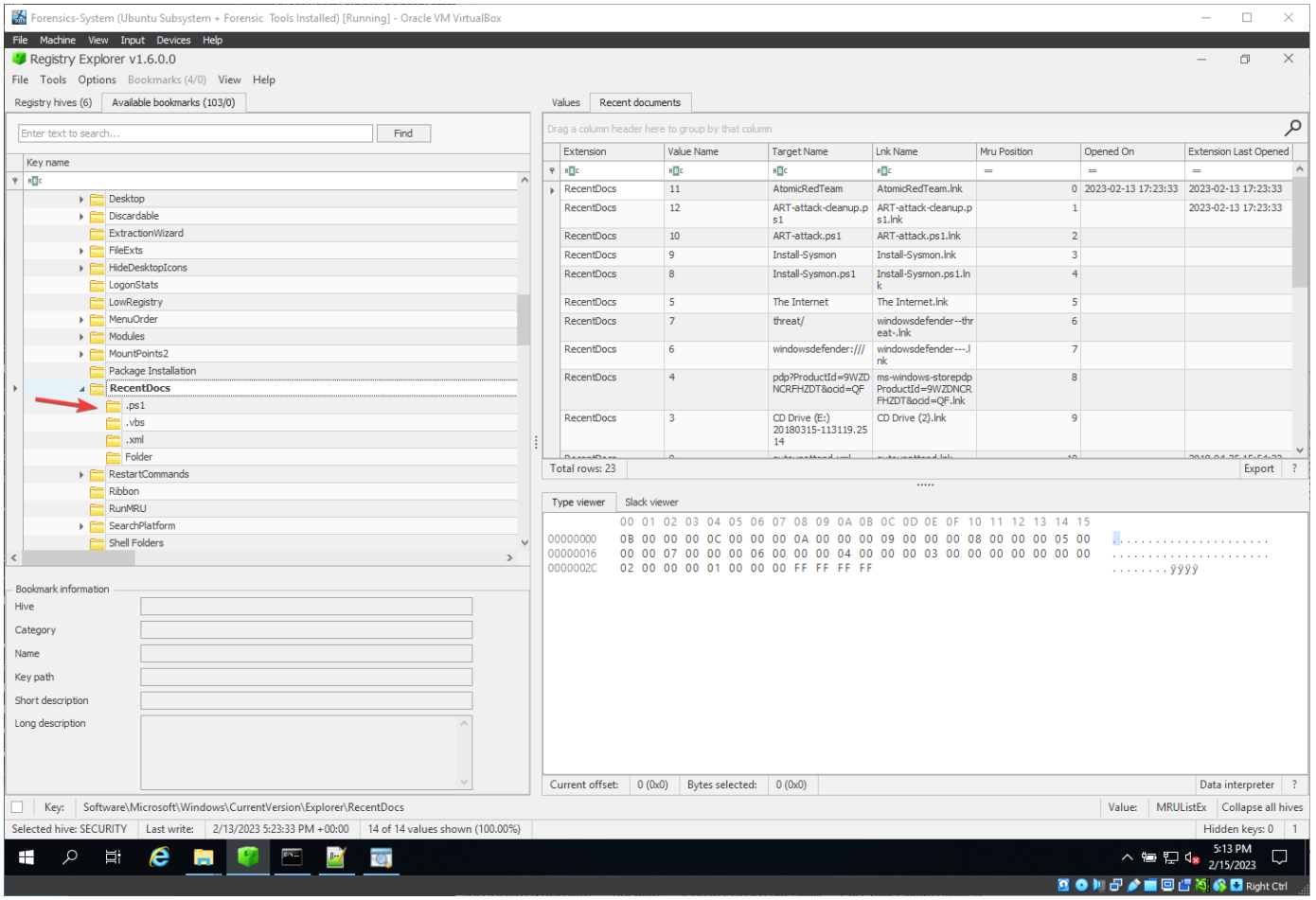


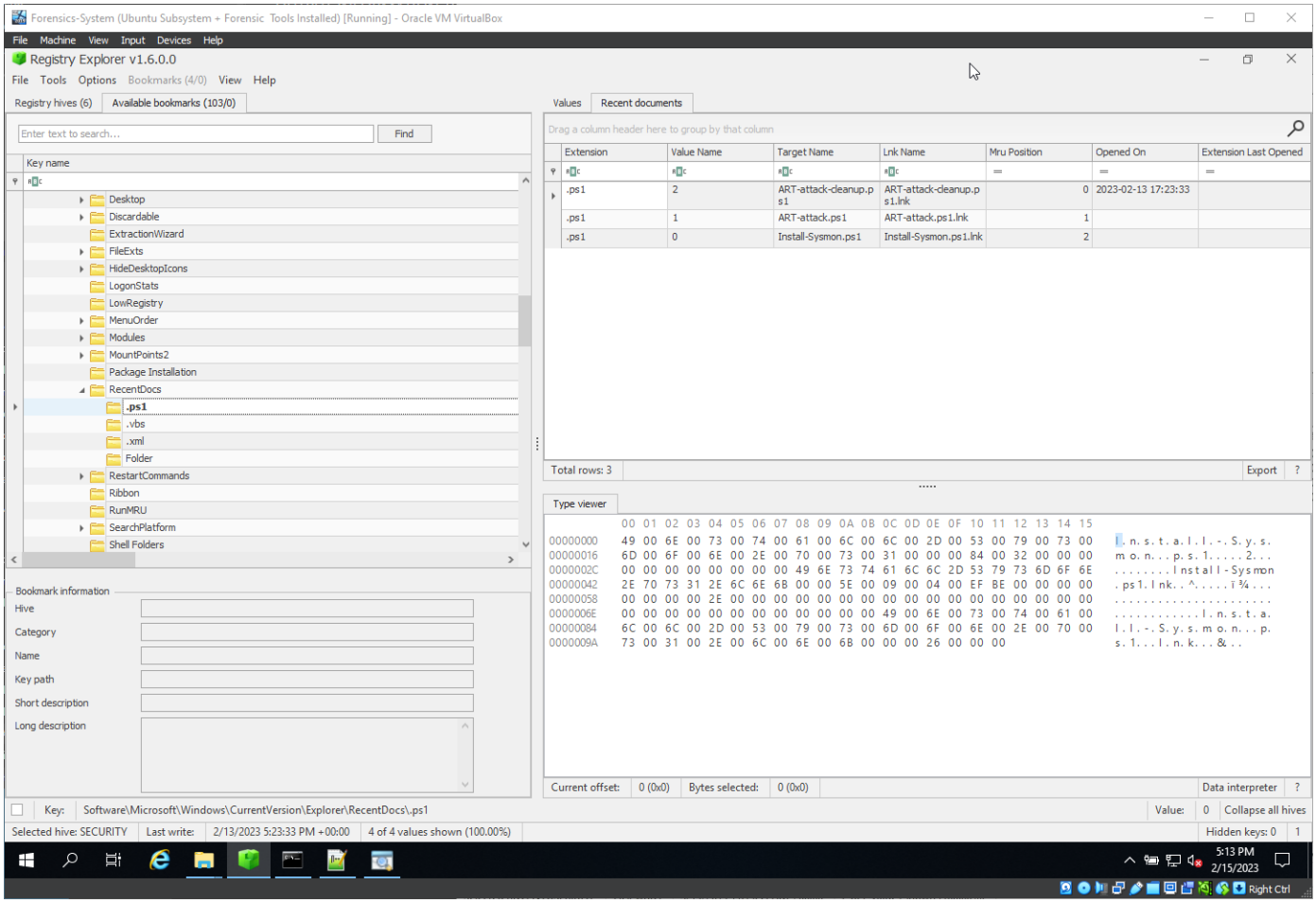

# RecentDocs

- Can be found at:
  - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs




- You can see applications that has been accessed above.
- Application extensions used:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (6)
Available bookmarks (103/0)
Enter text to search...
Find
Key name
Desktop
Discardable
ExtractionWizard
FileExts
HideDesktopIcons
LogonStats
LowRegistry
MenuOrder
Modules
MountPoints2
Package Installation
RecentDocs
.ps1
.vbs
.xml
Folder
RestartCommands
Ribbon
RunMRU
SearchPlatform
Shell Folders
Bookmark information
Hive
Category
Name
Key path
Short description
Long description
Values
Recent documents
Drag a column header here to group by that column
Extension
Value Name
Target Name
Lnk Name
Mru Position
Opened On
Extension Last Opened
RecentDocs 11 AtomicRedTeam AtomicRedTeam.lnk 0 2023-02-13 17:23:33 2023-02-13 17:23:33
RecentDocs 12 ART-attack-cleanup.ps1 ART-attack-cleanup.ps1.lnk 1 2023-02-13 17:23:33
RecentDocs 10 ART-attack.ps1 ART-attack.ps1.lnk 2
RecentDocs 9 Install-Sysmon Install-Sysmon.lnk 3
RecentDocs 8 Install-Sysmon.ps1 Install-Sysmon.ps1.lnk 4
RecentDocs 5 The Internet The Internet.lnk 5
RecentDocs 7 threat/ windowsdefender--threat-.lnk 6
RecentDocs 6 windowsdefender:/// windowsdefender---.lnk 7
RecentDocs 4 pdp?ProductId=9WZDNCRFHZDT&ocid=QF ms-windows-storepdpProductId=9WZDNCRFHZDT&ocid=QF.lnk 8
RecentDocs 3 CD Drive (E:) 20180315-113119.2514 CD Drive (2).lnk 9
Total rows: 23
Export
Type viewer
Slack viewer
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15
00000000 0B 00 00 00 0C 00 00 00 0A 00 00 00 09 00 00 00 08 00 00 00 05 00
00000016 00 00 07 00 00 00 06 00 00 00 04 00 00 00 03 00 00 00 00 00 00 00
0000002C 02 00 00 00 01 00 00 00 FF FF FF FF ÿÿÿÿ
Current offset: 0 (0x0)
Bytes selected: 0 (0x0)
Data interpreter
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Value: MRUListEx
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:23:33 PM +00:00
14 of 14 values shown (100.00%)
Hidden keys: 0
5:13 PM
2/15/2023
Right Ctrl




# ShellBags

- 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.
- If chaning a path, on windows explorer , change view settings or resize, this whole information is stored in shell bags , for the user experience.

- Can be found in:
- NTUSER.DAT:
    - HKCU\Software]Microsoft\Windows\Shell\BagMRU

    - HKCU\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT:
    - Software\Classes\Local Settings\Software\Microsoft\WIndows\Shell\BagMRU
    - Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags

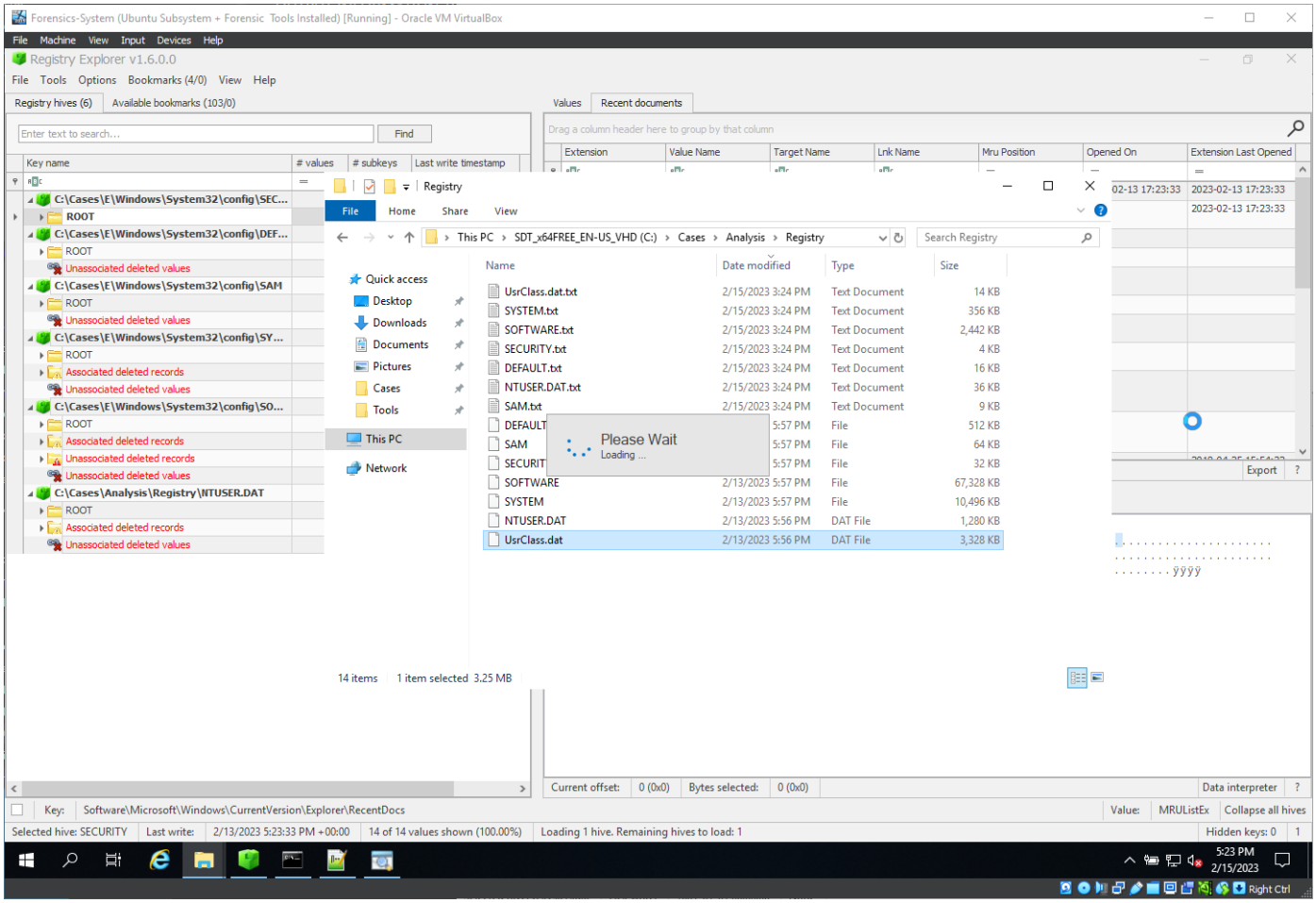
- Search for the shellbags regripper plugin in USRCLASS.dat:
- Evidence of opening folders:

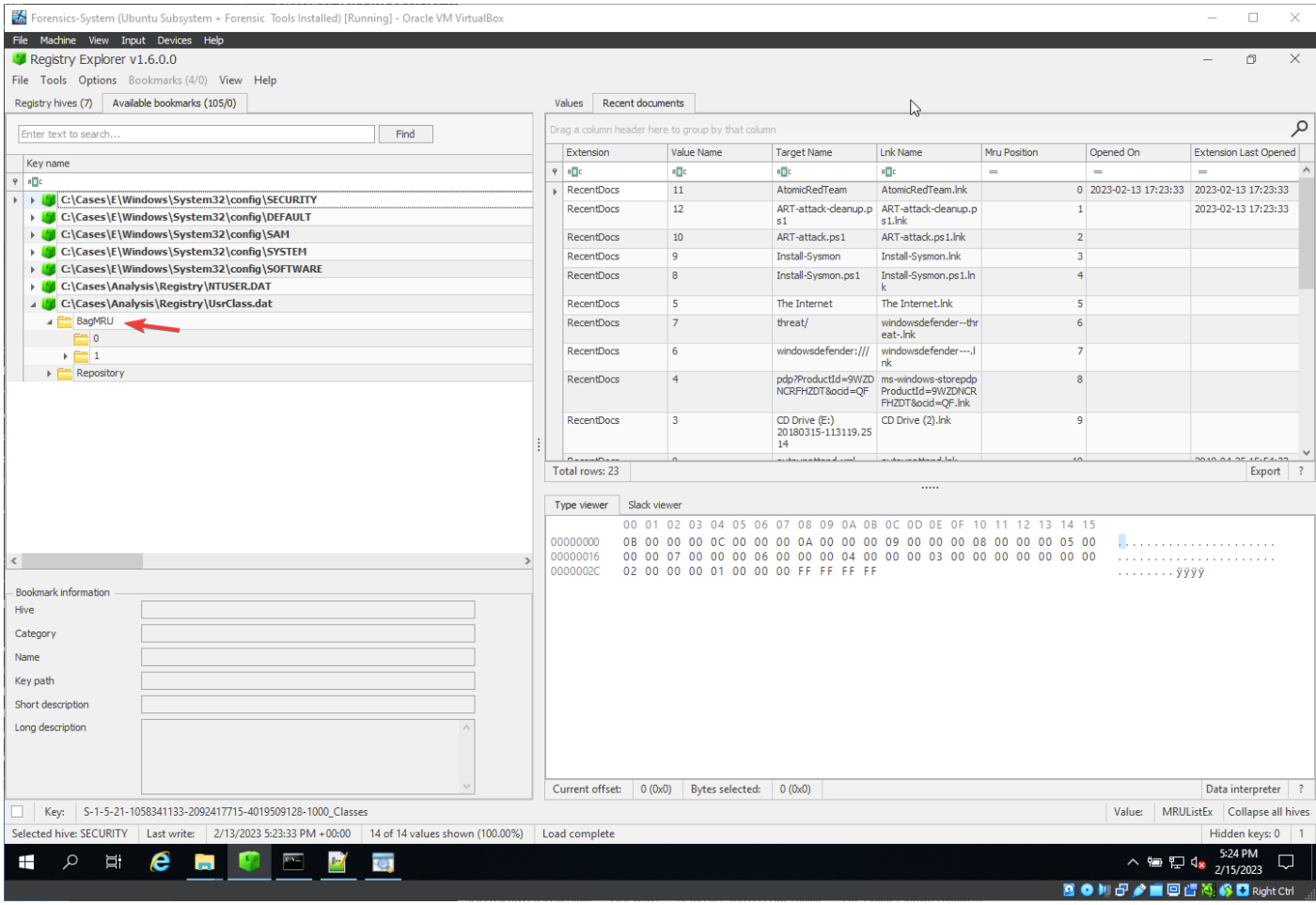
```
----------------------------------------
shellbags v.20200428
(USRCLASS.DAT) Shell/BagMRU traversal in Win7+ USRCLASS.DAT hives

MRU Time            |Modified            | Accessed            | Created             | Zip_Subfolder       | MFT File Ref |Resource
--------------------|--------------------|---------------------|---------------------|---------------------|--------------|------------
                    |                    |                     |                     |                     |              |My Games [Desktop\0\]
2023-02-13 17:21:42 |                    |                     |                     |                     |              |My Computer [Desktop\1\]
                    |                    |                     |                     |                     |              |My Computer\D:\ [Desktop\1\0\]
                    |                    |                     |                     |                     |              |My Computer\E:\ [Desktop\1\1\]
                    |                    |                     |                     |                     |              |My Computer\Z:\ [Desktop\1\2\]
2023-02-13 17:26:02 |                    |                     |                     |                     |              |My Computer\CLSID_Desktop [Desktop\1\3\]
2023-02-13 17:21:03 |2023-02-13 17:21:04 | 2023-02-13 17:21:04 | 2023-02-13 17:21:04 |                     | 22968/2      |My Computer\CLSID_Desktop\PWF-main [Deskto
2023-02-13 17:21:06 |2023-02-13 17:21:04 | 2023-02-13 17:21:04 | 2023-02-13 17:21:04 |                     | 23026/2      |My Computer\CLSID_Desktop\PWF-main\PWF-mai
                    |2023-02-13 17:21:04 | 2023-02-13 17:21:04 | 2023-02-13 17:21:04 |                     | 28680/2      |My Computer\CLSID_Desktop\PWF-main\PWF-mai
2023-02-13 17:26:03 |2023-02-13 17:21:04 | 2023-02-13 17:21:04 | 2023-02-13 17:21:04 |                     | 28668/2      |My Computer\CLSID_Desktop\PWF-main\PWF-mai
----------------------------------------
```

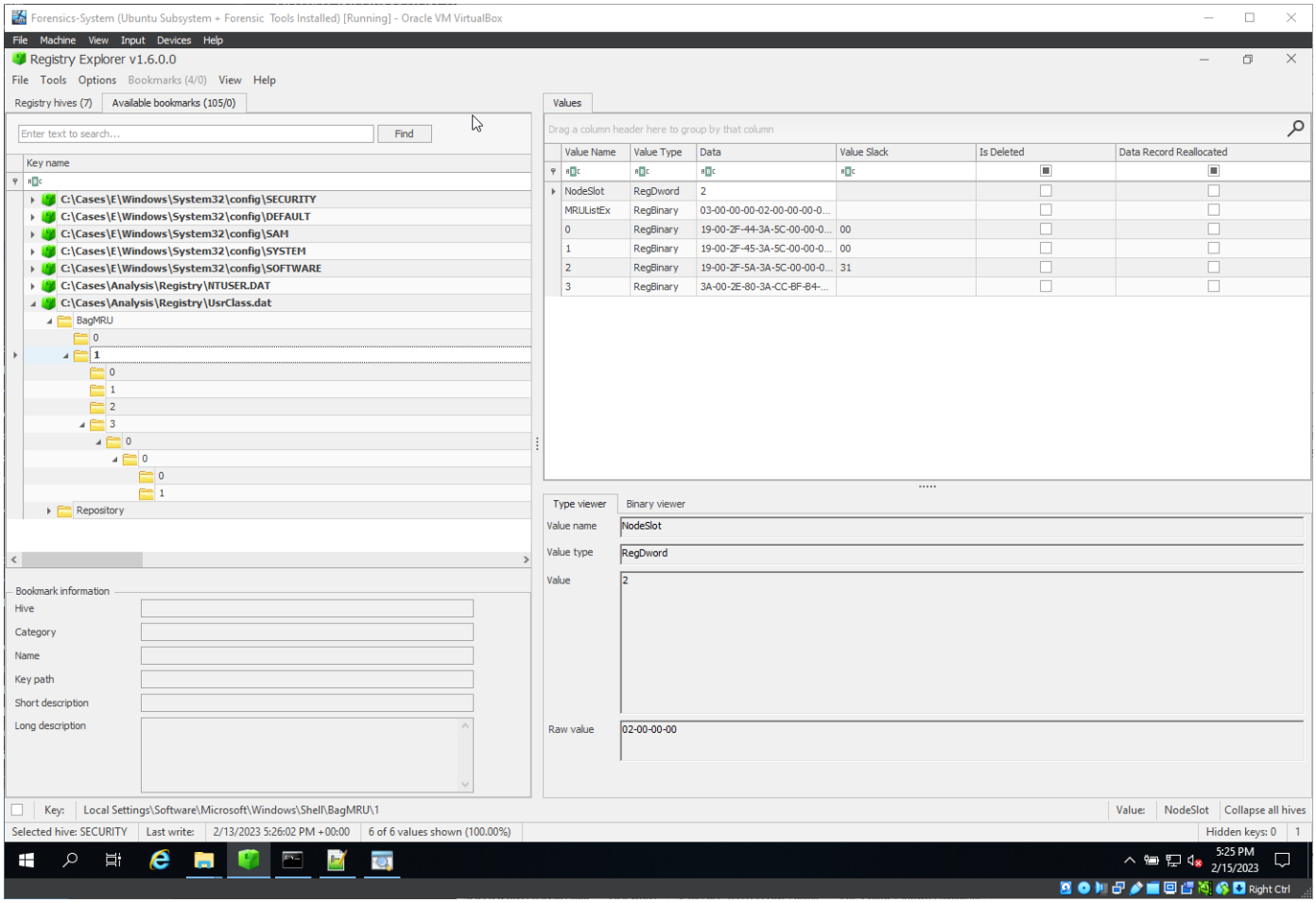
```
| MFT File Ref |Resource
| ------------ |------------
|              |My Games [Desktop\0\]
|              |My Computer [Desktop\1\]
|              |My Computer\D:\ [Desktop\1\0\]
|              |My Computer\E:\ [Desktop\1\1\]
|              |My Computer\Z:\ [Desktop\1\2\]
|              |My Computer\CLSID_Desktop [Desktop\1\3\]
| 22968/2      |My Computer\CLSID_Desktop\PWF-main [Desktop\1\3\0\]
| 23026/2      |My Computer\CLSID_Desktop\PWF-main\PWF-main [Desktop\1\3\0\0\]
| 28680/2      |My Computer\CLSID_Desktop\PWF-main\PWF-main\Install-Sysmon [Desktop\1\3\0\0\0\]
| 28668/2      |My Computer\CLSID_Desktop\PWF-main\PWF-main\AtomicRedTeam [Desktop\1\3\0\0\1\]
```

- Upload UsrClass.dat in the registry explorer:

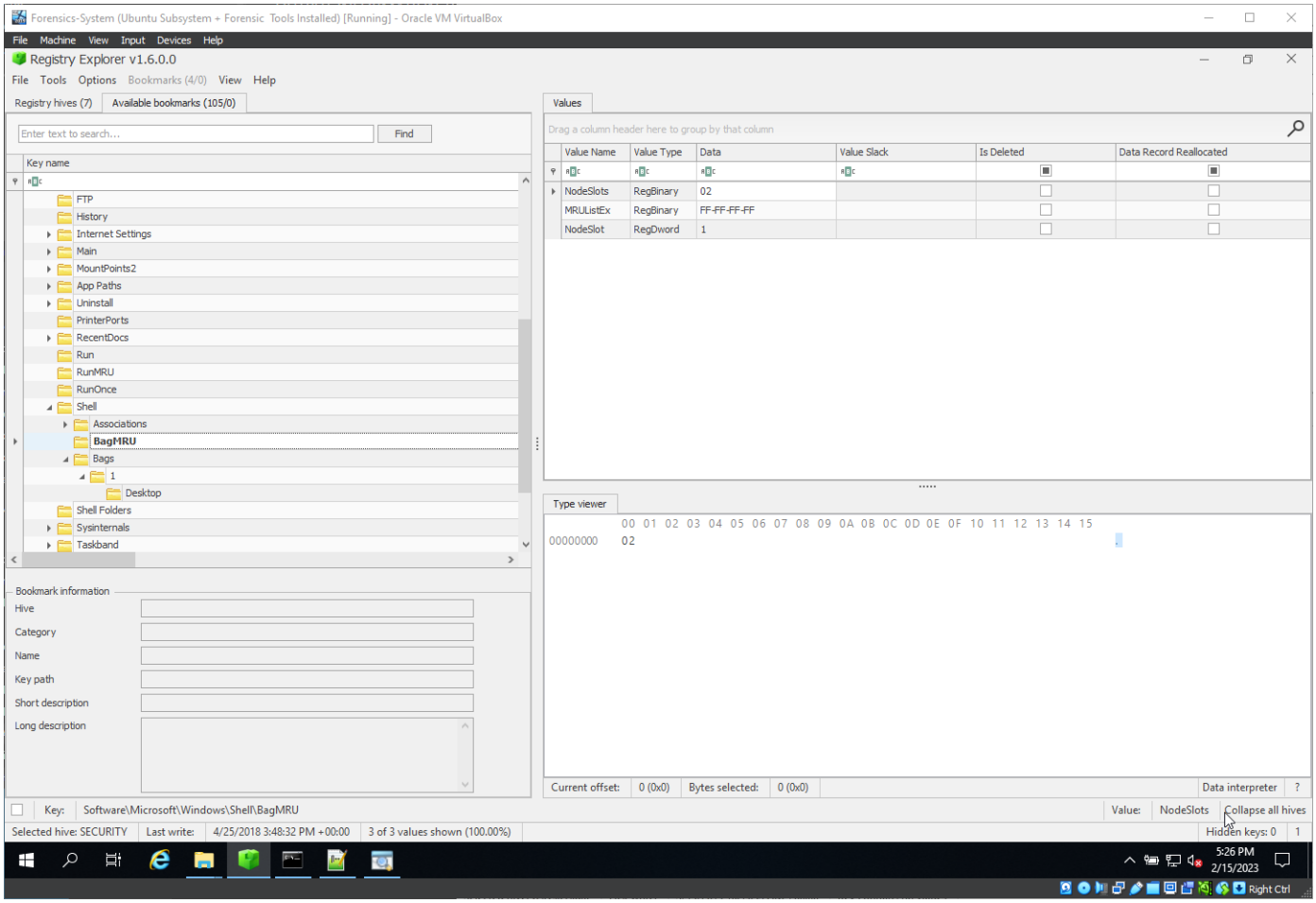

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (6)
Available bookmarks (103/0)
Enter text to search...
Find
Key name
# values
# subkeys
Last write timestamp
C:\Cases\E\Windows\System32\config\SEC...
ROOT
C:\Cases\E\Windows\System32\config\DEF...
ROOT
Unassociated deleted values
C:\Cases\E\Windows\System32\config\SAM
ROOT
Unassociated deleted values
C:\Cases\E\Windows\System32\config\SY...
ROOT
Associated deleted records
Unassociated deleted values
C:\Cases\E\Windows\System32\config\SO...
ROOT
Associated deleted records
Unassociated deleted records
Unassociated deleted values
C:\Cases\Analysis\Registry\NTUSER.DAT
ROOT
Associated deleted records
Unassociated deleted values
Values
Recent documents
Drag a column header here to group by that column
Extension
Value Name
Target Name
Lnk Name
Mru Position
Opened On
Extension Last Opened
02-13 17:23:33
2023-02-13 17:23:33
Registry
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis › Registry
Search Registry
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
UsrClass.dat.txt 2/15/2023 3:24 PM Text Document 14 KB
SYSTEM.txt 2/15/2023 3:24 PM Text Document 356 KB
SOFTWARE.txt 2/15/2023 3:24 PM Text Document 2,442 KB
SECURITY.txt 2/15/2023 3:24 PM Text Document 4 KB
DEFAULT.txt 2/15/2023 3:24 PM Text Document 16 KB
NTUSER.DAT.txt 2/15/2023 3:24 PM Text Document 36 KB
SAM.txt 2/15/2023 3:24 PM Text Document 9 KB
DEFAULT 5:57 PM File 512 KB
SAM 5:57 PM File 64 KB
SECURIT 5:57 PM File 32 KB
SOFTWARE 2/13/2023 5:57 PM File 67,328 KB
SYSTEM 2/13/2023 5:57 PM File 10,496 KB
NTUSER.DAT 2/13/2023 5:56 PM DAT File 1,280 KB
UsrClass.dat 2/13/2023 5:56 PM DAT File 3,328 KB
Please Wait
Loading ...
14 items
1 item selected 3.25 MB
Export
Current offset: 0 (0x0)
Bytes selected: 0 (0x0)
Data interpreter
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Value:
MRUListEx
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:23:33 PM +00:00
14 of 14 values shown (100.00%)
Loading 1 hive. Remaining hives to load: 1
Hidden keys: 0
5:23 PM
2/15/2023
Right Ctrl

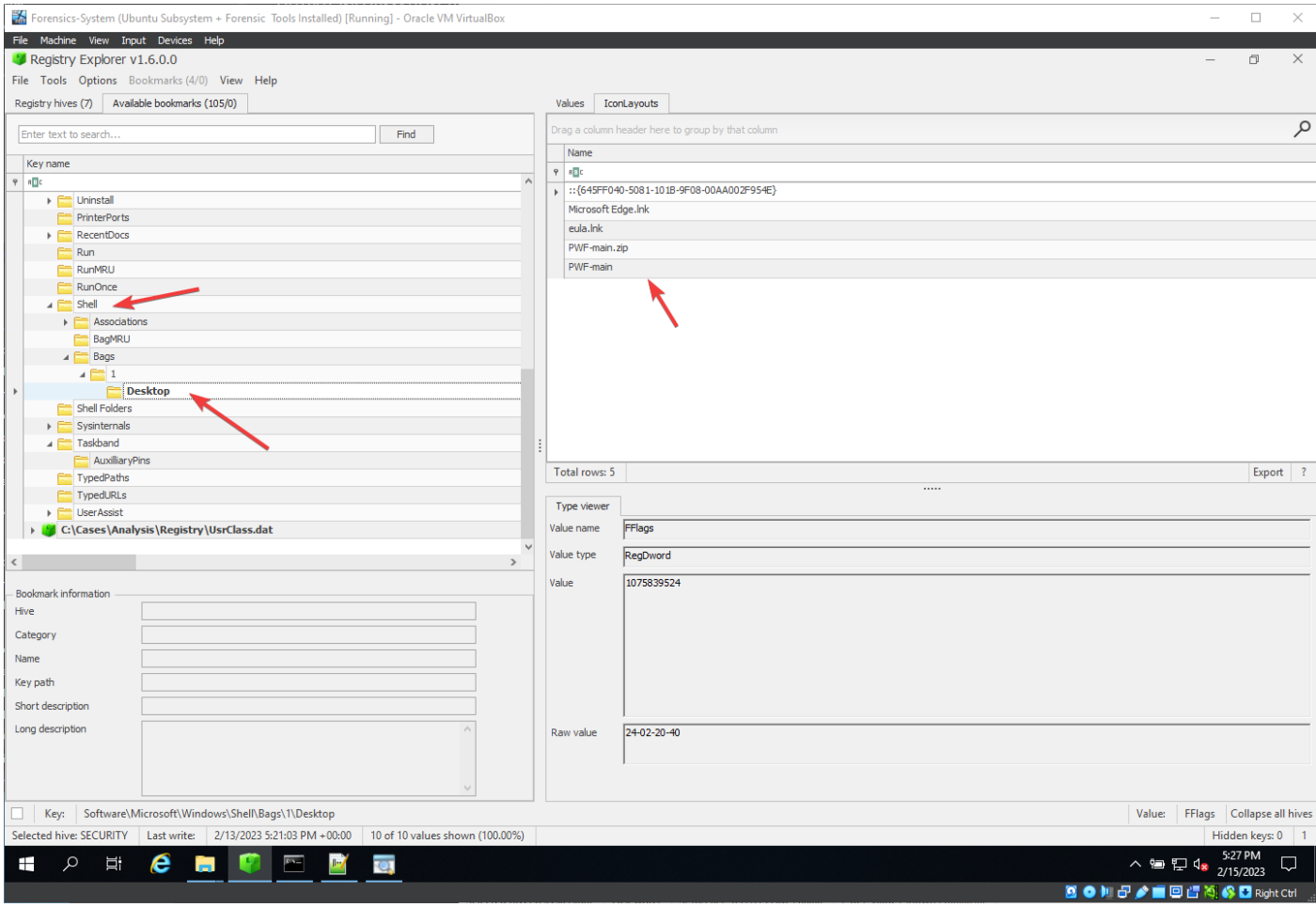



- BagMRU remembers folders names, folder paths accesed

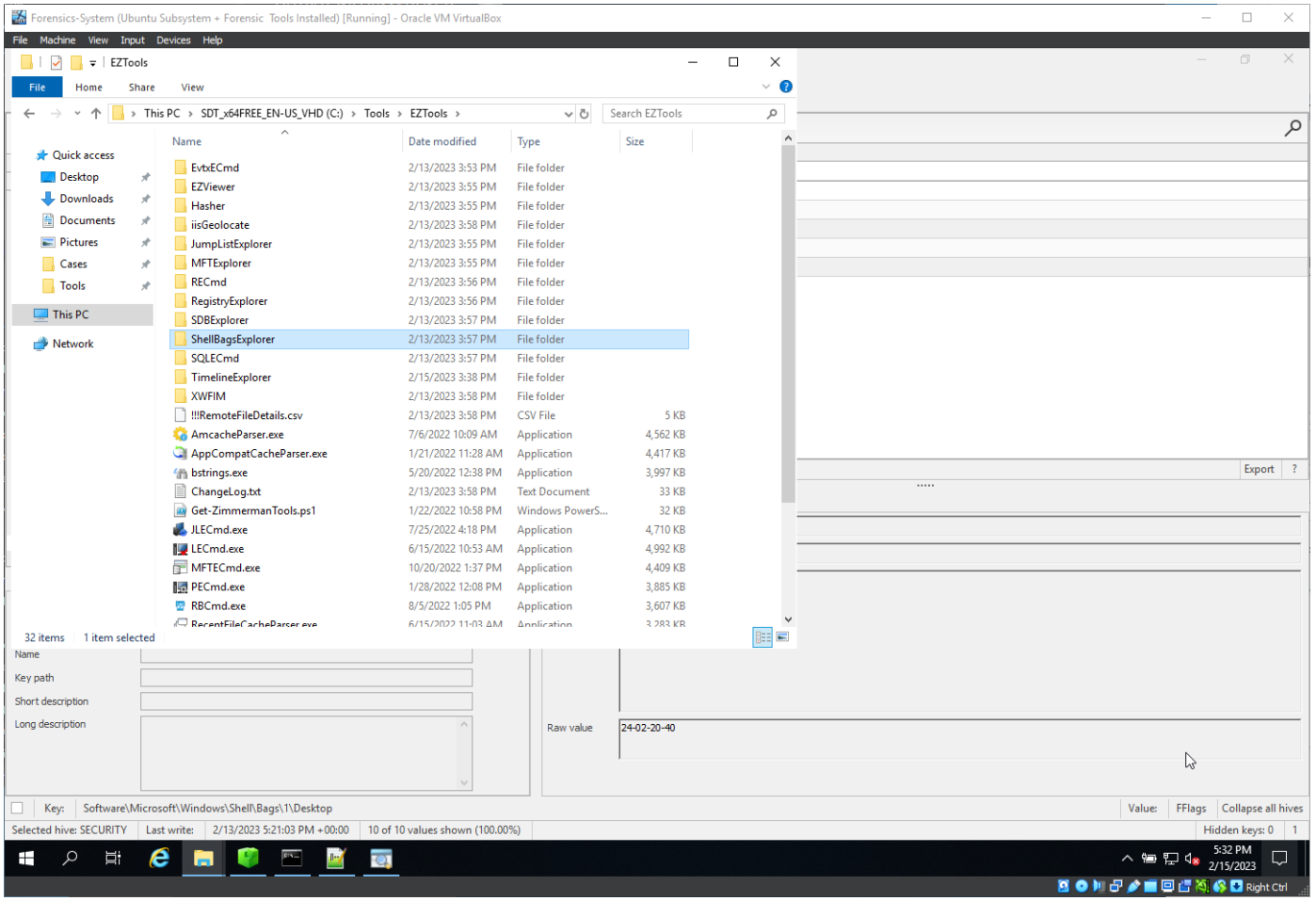


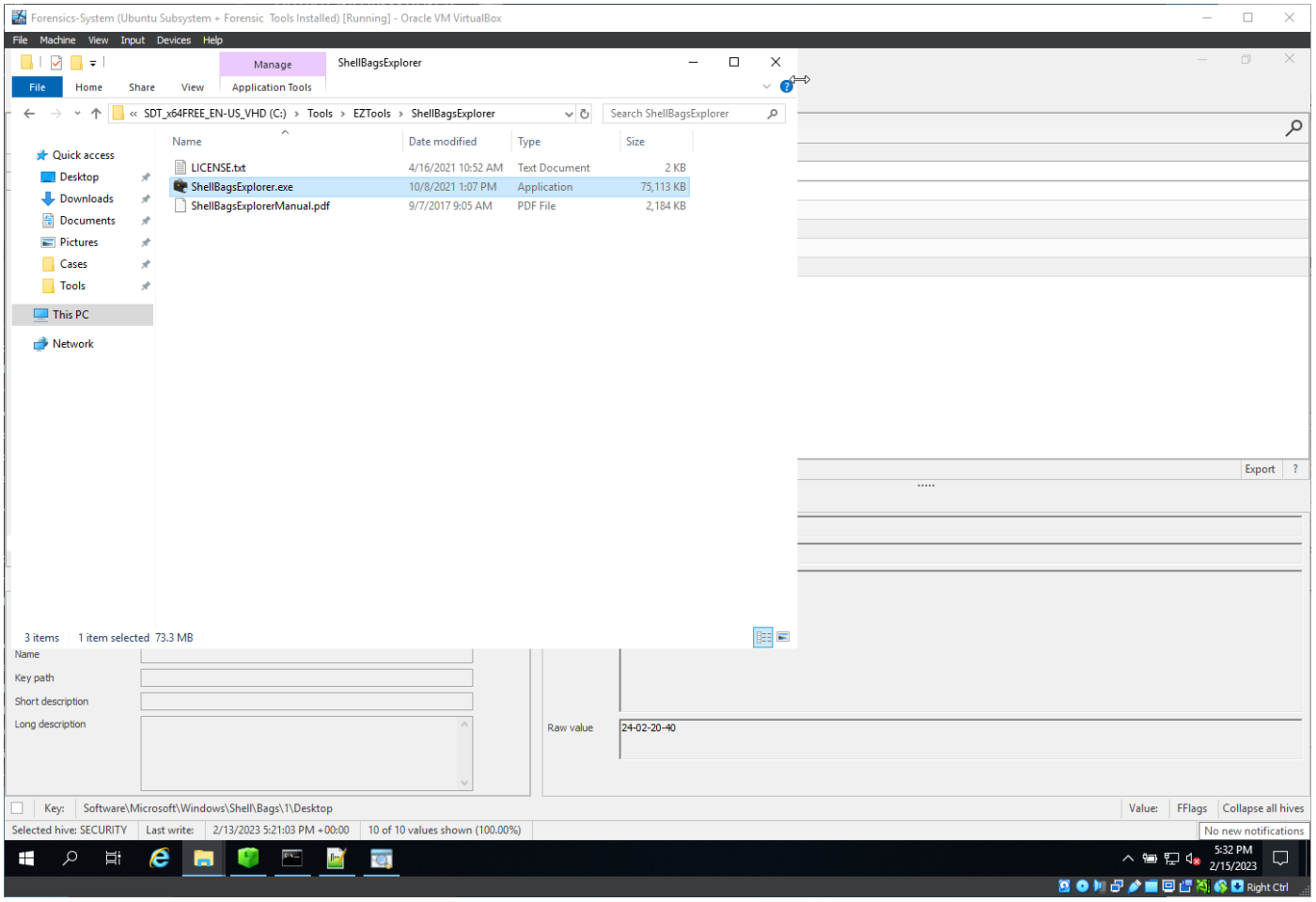

- Switch to NTUSER.DAT:

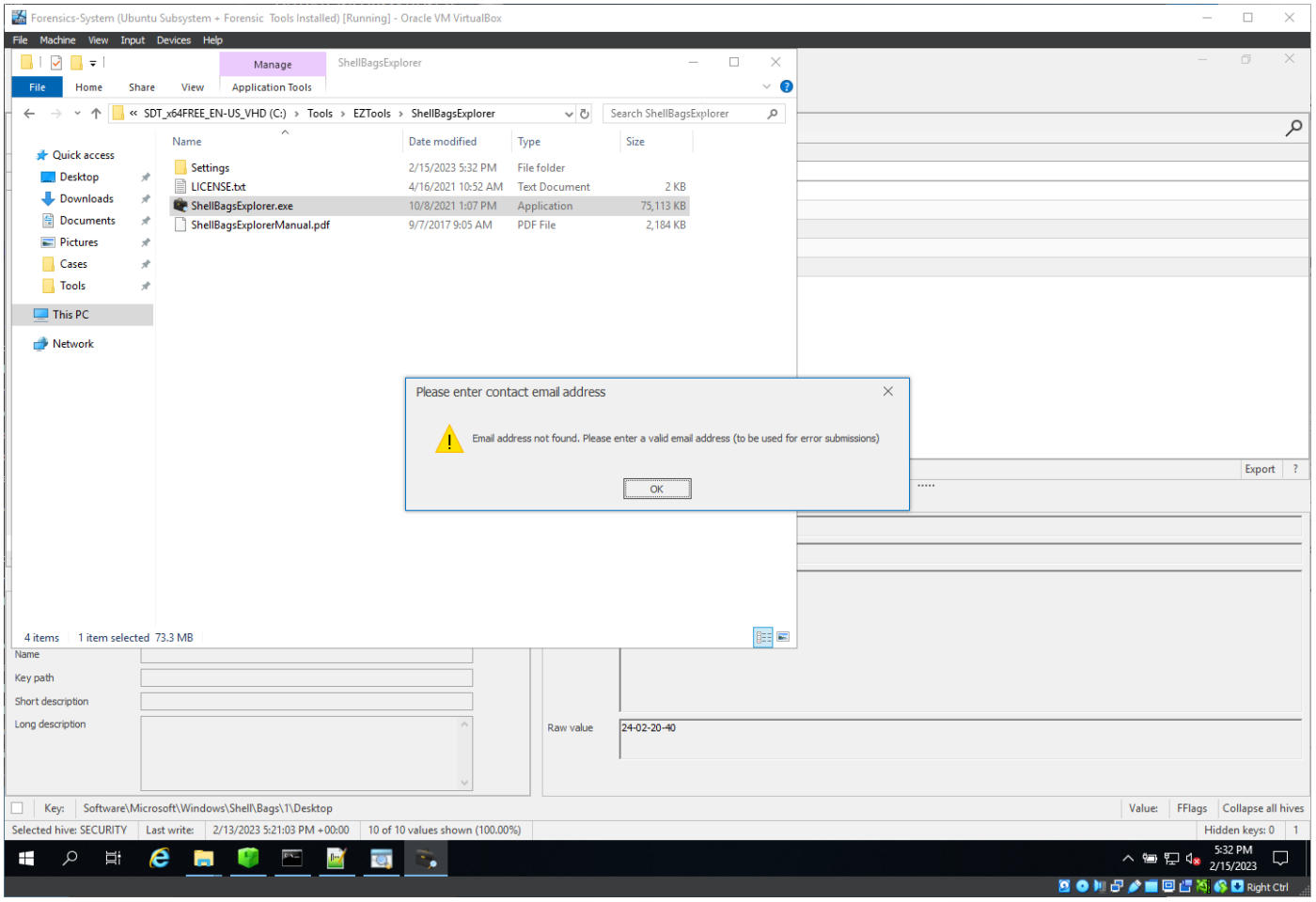

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Explorer v1.6.0.0
File Tools Options Bookmarks (4/0) View Help
Registry hives (7)
Available bookmarks (105/0)
Enter text to search...
Find
Key name
FTP
History
Internet Settings
Main
MountPoints2
App Paths
Uninstall
PrinterPorts
RecentDocs
Run
RunMRU
RunOnce
Shell
Associations
BagMRU
Bags
1
Desktop
Shell Folders
Sysinternals
Taskband
Bookmark information
Hive
Category
Name
Key path
Short description
Long description
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value Slack
Is Deleted
Data Record Reallocated
NodeSlots
RegBinary
02
MRUListEx
RegBinary
FF-FF-FF-FF
NodeSlot
RegDword
1
Type viewer
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15
00000000 02
Current offset: 0 (0x0)
Bytes selected: 0 (0x0)
Data interpreter
Key: Software\Microsoft\Windows\Shell\BagMRU
Value: NodeSlots
Collapse all hives
Selected hive: SECURITY
Last write: 4/25/2018 3:48:32 PM +00:00
3 of 3 values shown (100.00%)
Hidden keys: 0
5:26 PM
2/15/2023
Right Ctrl

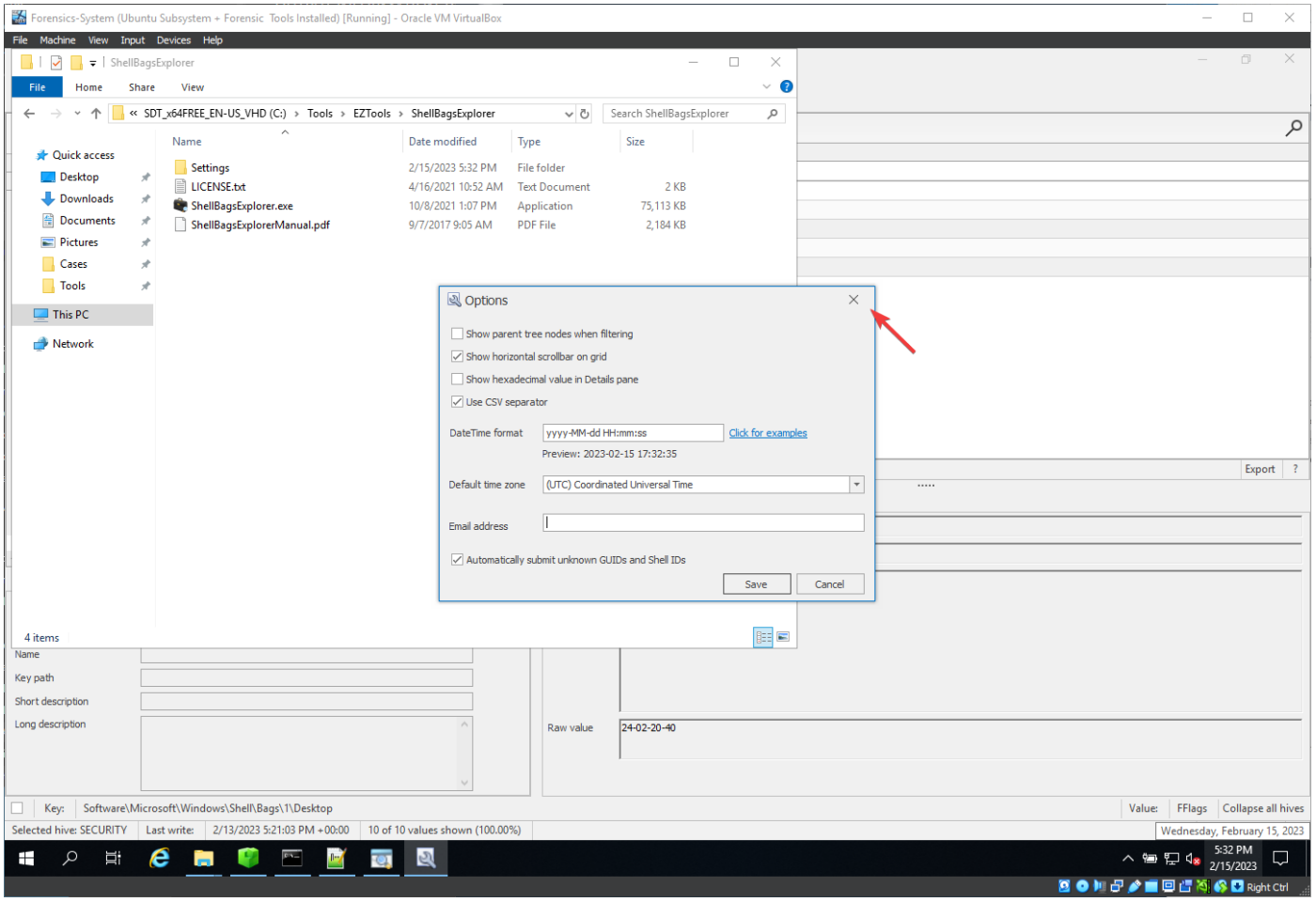


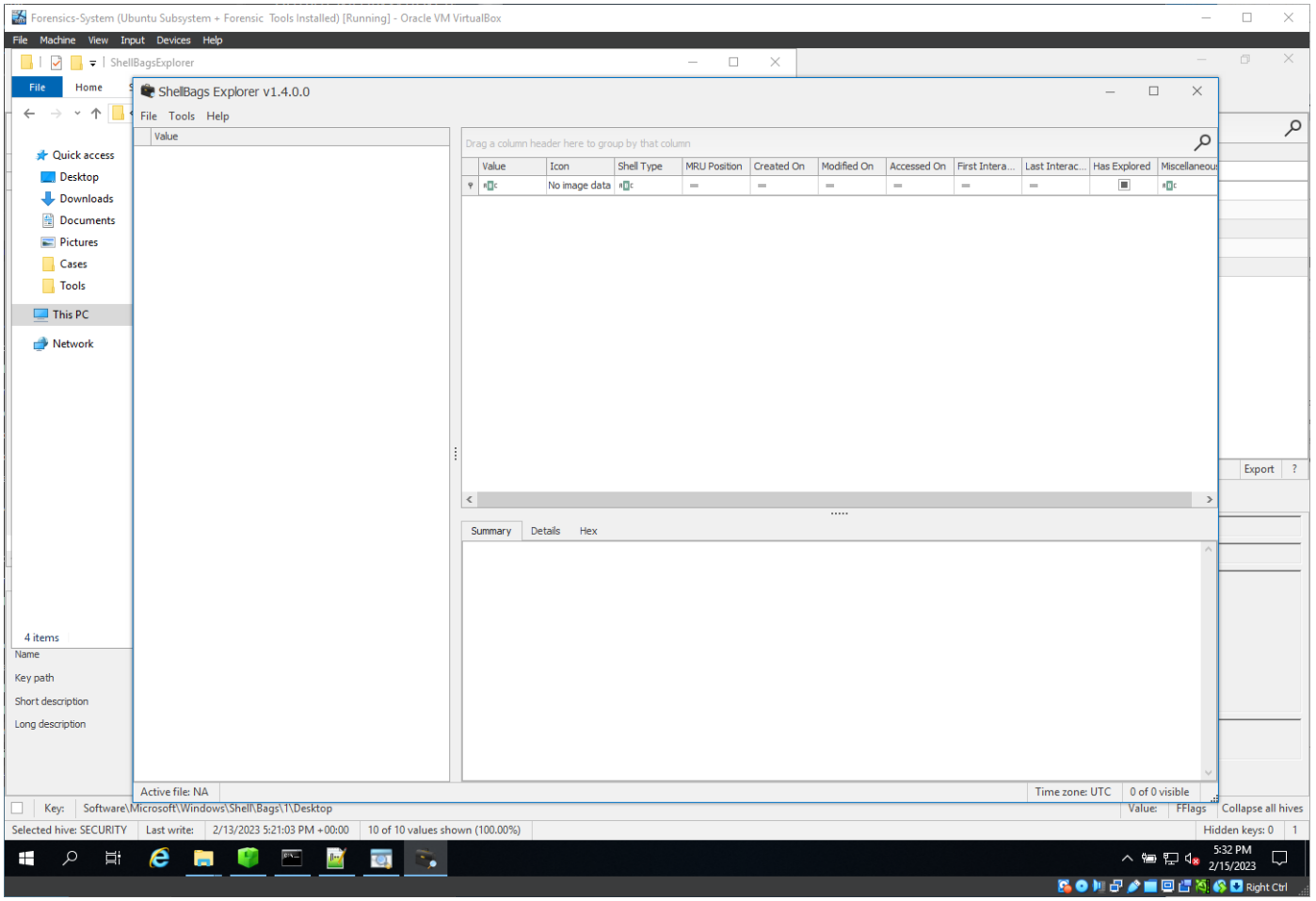

- In Bags , there exists the preferences of the user, the size of a window, path locations, etc
- IconLayouts, in the Desktop folder, explains that there was an Icon on the Desktop for that particular values.
- Different applications/tools can be used for ShellBags, for example : ShellBagsExplorer:

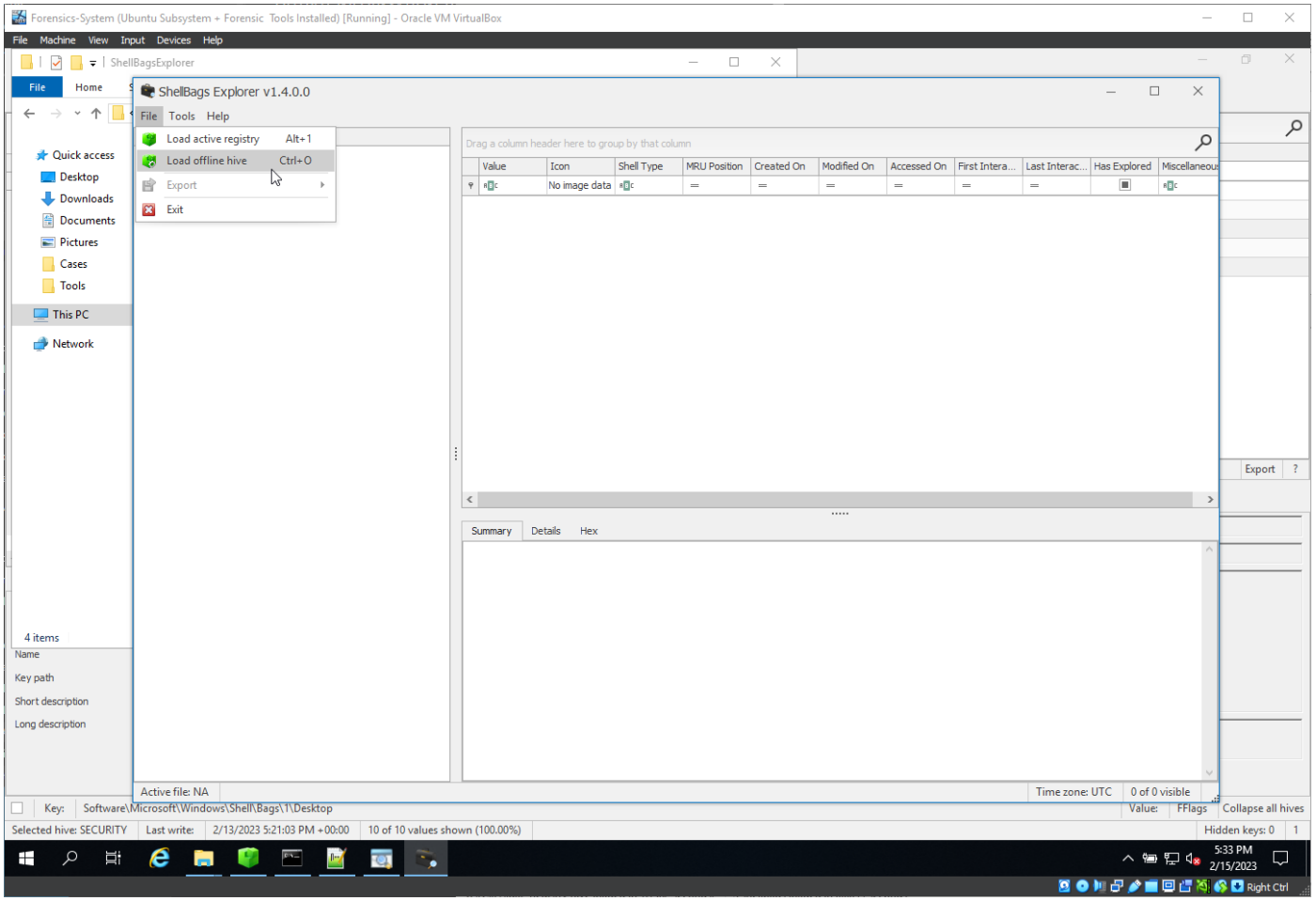

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
EZTools
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Tools › EZTools ›
Search EZTools
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
EvtxECmd 2/13/2023 3:53 PM File folder
EZViewer 2/13/2023 3:55 PM File folder
Hasher 2/13/2023 3:55 PM File folder
iisGeolocate 2/13/2023 3:58 PM File folder
JumpListExplorer 2/13/2023 3:55 PM File folder
MFTExplorer 2/13/2023 3:55 PM File folder
RECmd 2/13/2023 3:56 PM File folder
RegistryExplorer 2/13/2023 3:56 PM File folder
SDBExplorer 2/13/2023 3:57 PM File folder
ShellBagsExplorer 2/13/2023 3:57 PM File folder
SQLECmd 2/13/2023 3:57 PM File folder
TimelineExplorer 2/15/2023 3:38 PM File folder
XWFIM 2/13/2023 3:58 PM File folder
!!!RemoteFileDetails.csv 2/13/2023 3:58 PM CSV File 5 KB
AmcacheParser.exe 7/6/2022 10:09 AM Application 4,562 KB
AppCompatCacheParser.exe 1/21/2022 11:28 AM Application 4,417 KB
bstrings.exe 5/20/2022 12:38 PM Application 3,997 KB
ChangeLog.txt 2/13/2023 3:58 PM Text Document 33 KB
Get-ZimmermanTools.ps1 1/22/2022 10:58 PM Windows PowerS... 32 KB
JLECmd.exe 7/25/2022 4:18 PM Application 4,710 KB
LECmd.exe 6/15/2022 10:53 AM Application 4,992 KB
MFTECmd.exe 10/20/2022 1:37 PM Application 4,409 KB
PECmd.exe 1/28/2022 12:08 PM Application 3,885 KB
RBCmd.exe 8/5/2022 1:05 PM Application 3,607 KB
32 items 1 item selected
Export
Name
Key path
Short description
Long description
Raw value
24-02-20-40
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value: FFlags Collapse all hives
Selected hive: SECURITY Last write: 2/13/2023 5:21:03 PM +00:00 10 of 10 values shown (100.00%)
Hidden keys: 0
5:32 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Manage
ShellBagsExplorer
File Home Share View Application Tools
SDT_x64FREE_EN-US_VHD (C:) › Tools › EZTools › ShellBagsExplorer
Search ShellBagsExplorer
Name Date modified Type Size
LICENSE.txt 4/16/2021 10:52 AM Text Document 2 KB
ShellBagsExplorer.exe 10/8/2021 1:07 PM Application 75,113 KB
ShellBagsExplorerManual.pdf 9/7/2017 9:05 AM PDF File 2,184 KB
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
3 items 1 item selected 73.3 MB
Export
Name
Key path
Short description
Long description
Raw value
24-02-20-40
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value: FFlags Collapse all hives
Selected hive: SECURITY Last write: 2/13/2023 5:21:03 PM +00:00 10 of 10 values shown (100.00%)
No new notifications
5:32 PM
2/15/2023
Right Ctrl

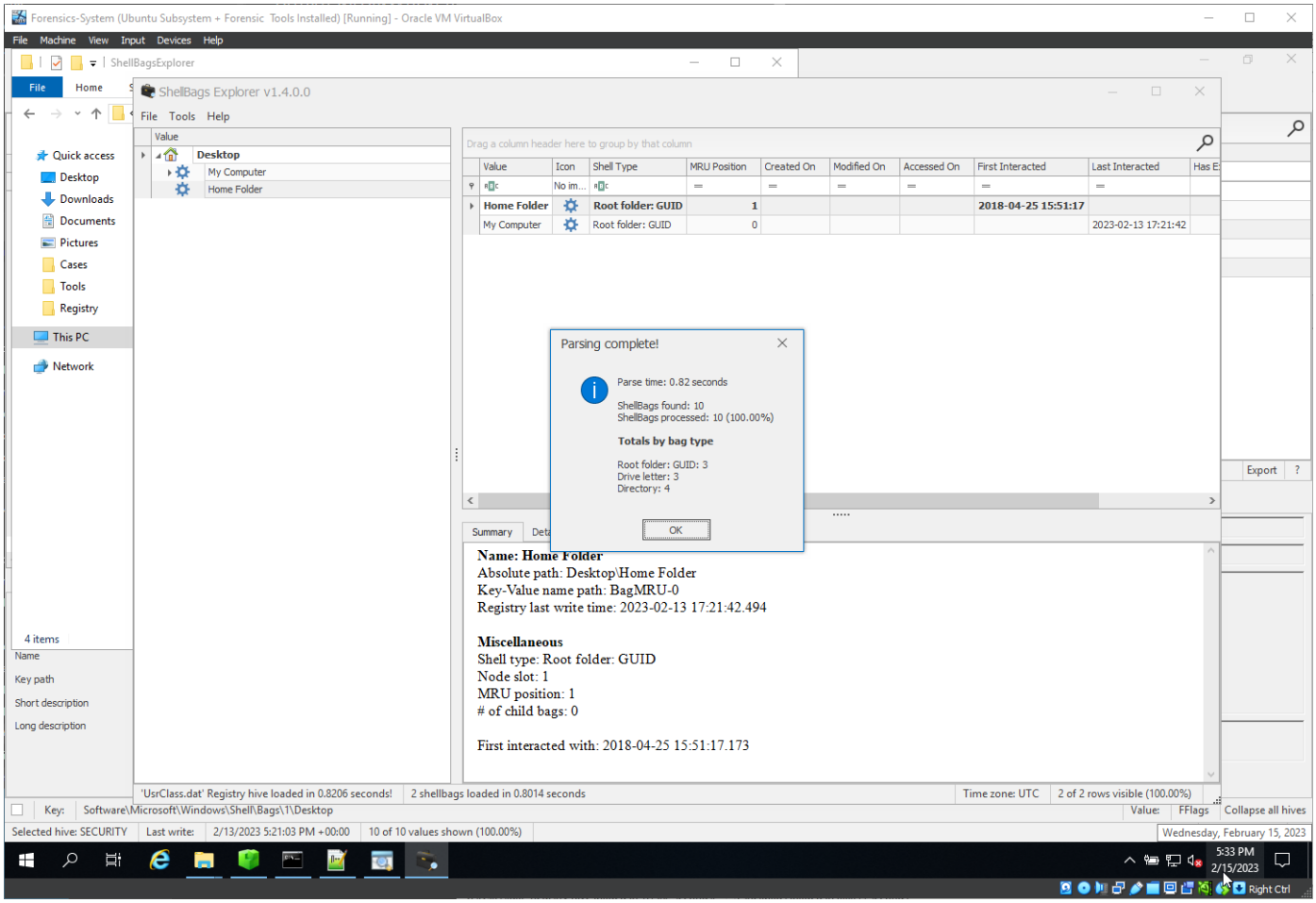

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ShellBagsExplorer
Manage
File Home Share View Application Tools
SDT_x64FREE_EN-US_VHD (C:) › Tools › EZTools › ShellBagsExplorer
Search ShellBagsExplorer
Name Date modified Type Size
Settings 2/15/2023 5:32 PM File folder
LICENSE.txt 4/16/2021 10:52 AM Text Document 2 KB
ShellBagsExplorer.exe 10/8/2021 1:07 PM Application 75,113 KB
ShellBagsExplorerManual.pdf 9/7/2017 9:05 AM PDF File 2,184 KB
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
4 items 1 item selected 73.3 MB
Please enter contact email address
Email address not found. Please enter a valid email address (to be used for error submissions)
OK
Export
Name
Key path
Short description
Long description
Raw value
24-02-20-40
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value: FFlags Collapse all hives
Selected hive: SECURITY Last write: 2/13/2023 5:21:03 PM +00:00 10 of 10 values shown (100.00%)
Hidden keys: 0
5:32 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ShellBagsExplorer
File Home Share View
SDT_x64FREE_EN-US_VHD (C:) › Tools › EZTools › ShellBagsExplorer
Search ShellBagsExplorer
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
Settings 2/15/2023 5:32 PM File folder
LICENSE.txt 4/16/2021 10:52 AM Text Document 2 KB
ShellBagsExplorer.exe 10/8/2021 1:07 PM Application 75,113 KB
ShellBagsExplorerManual.pdf 9/7/2017 9:05 AM PDF File 2,184 KB
4 items
Options
Show parent tree nodes when filtering
Show horizontal scrollbar on grid
Show hexadecimal value in Details pane
Use CSV separator
DateTime format
yyyy-MM-dd HH:mm:ss
Click for examples
Preview: 2023-02-15 17:32:35
Default time zone
(UTC) Coordinated Universal Time
Email address
Automatically submit unknown GUIDs and Shell IDs
Save
Cancel
Export
Name
Key path
Short description
Long description
Raw value
24-02-20-40
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value:
FFlags
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:21:03 PM +00:00
10 of 10 values shown (100.00%)
Wednesday, February 15, 2023
5:32 PM
2/15/2023
Right Ctrl

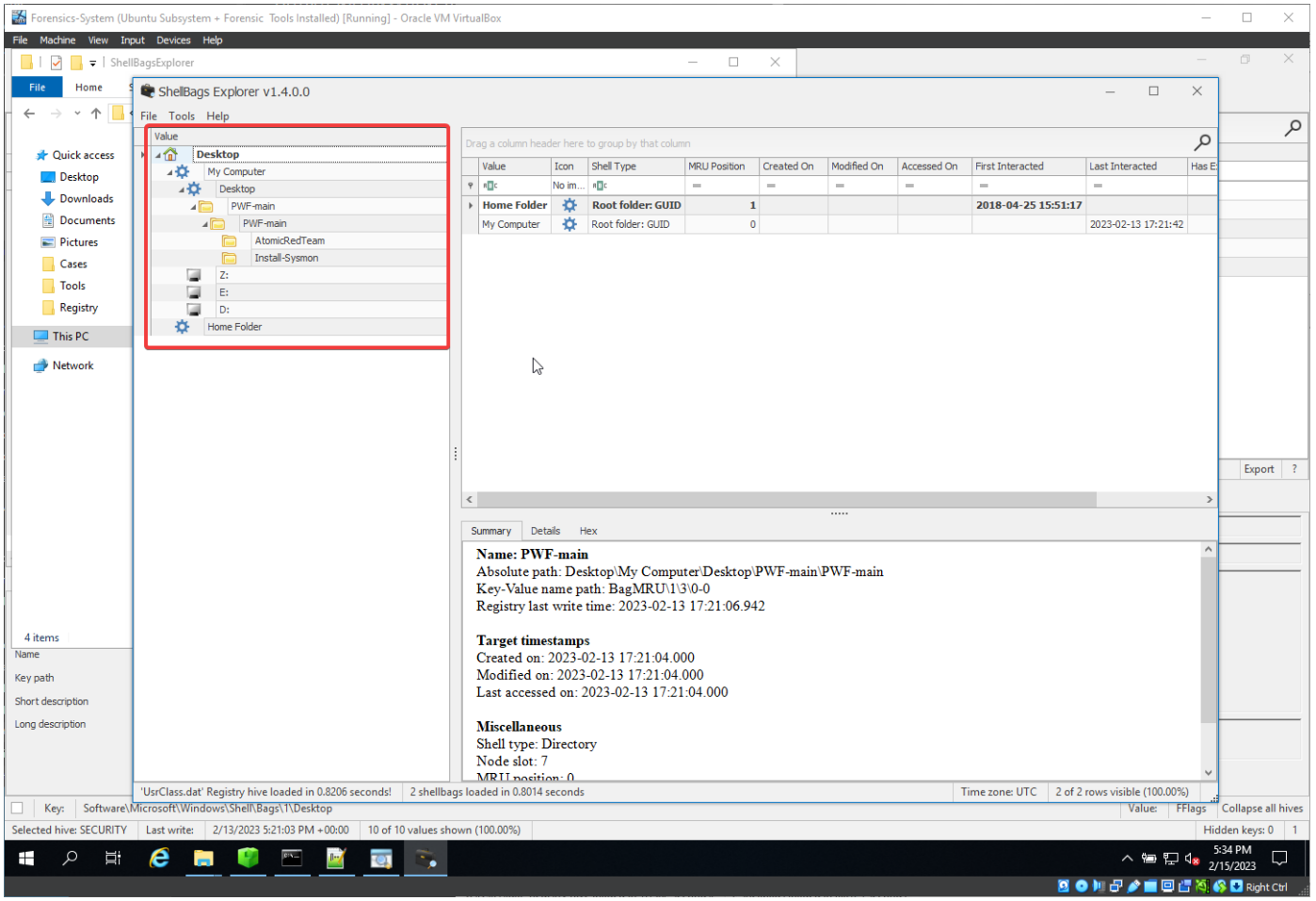

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ShellBagsExplorer
File Home
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
4 items
Name
Key path
Short description
Long description
ShellBags Explorer v1.4.0.0
File Tools Help
Value
Drag a column header here to group by that column
Value Icon Shell Type MRU Position Created On Modified On Accessed On First Intera... Last Interac... Has Explored Miscellaneous
No image data
Summary Details Hex
Active file: NA
Time zone: UTC
0 of 0 visible
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value: FFlags
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:21:03 PM +00:00
10 of 10 values shown (100.00%)
Hidden keys: 0
Export
5:32 PM
2/15/2023
Right Ctrl

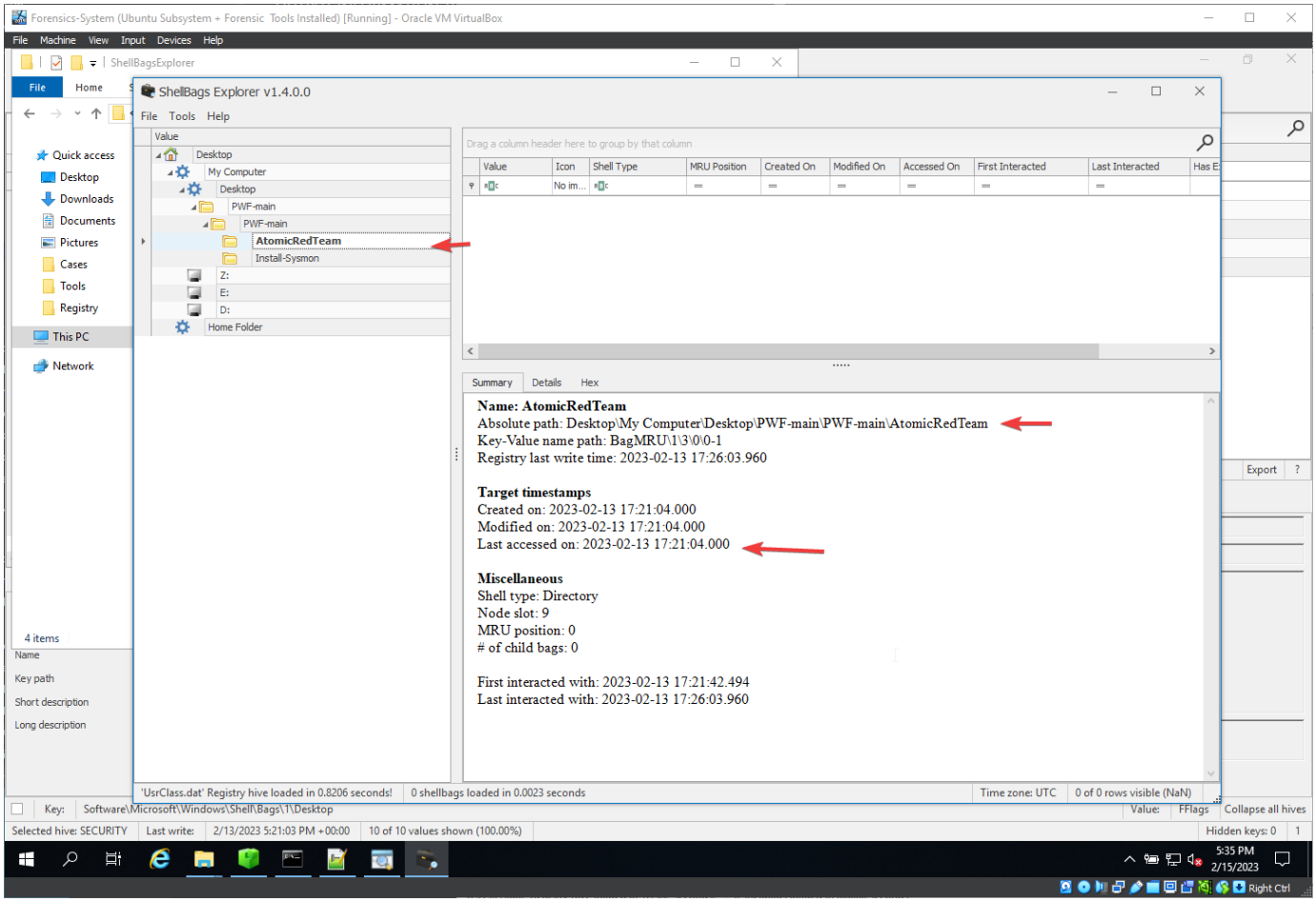



- Upload the UsrClass.dat file:




- This application helps us to see a tree structured view of the user preferences:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ShellBagsExplorer
ShellBags Explorer v1.4.0.0
File Tools Help
Value
Desktop
My Computer
Desktop
PWF-main
PWF-main
AtomicRedTeam
Install-Sysmon
Z:
E:
D:
Home Folder
Drag a column header here to group by that column
Value Icon Shell Type MRU Position Created On Modified On Accessed On First Interacted Last Interacted
Home Folder Root folder: GUID 1 2018-04-25 15:51:17
My Computer Root folder: GUID 0 2023-02-13 17:21:42
Summary Details Hex
Name: PWF-main
Absolute path: Desktop\My Computer\Desktop\PWF-main\PWF-main
Key-Value name path: BagMRU\1\3\0-0
Registry last write time: 2023-02-13 17:21:06.942
Target timestamps
Created on: 2023-02-13 17:21:04.000
Modified on: 2023-02-13 17:21:04.000
Last accessed on: 2023-02-13 17:21:04.000
Miscellaneous
Shell type: Directory
Node slot: 7
'UsrClass.dat' Registry hive loaded in 0.8206 seconds!
2 shellbags loaded in 0.8014 seconds
Time zone: UTC
2 of 2 rows visible (100.00%)
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value:
FFlags
Collapse all hives
Selected hive: SECURITY
Last write: 2/13/2023 5:21:03 PM +00:00
10 of 10 values shown (100.00%)
Hidden keys: 0
5:34 PM
2/15/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
ShellBagsExplorer
ShellBags Explorer v1.4.0.0
File Tools Help
Value
Desktop
My Computer
Desktop
PWF-main
PWF-main
AtomicRedTeam
Install-Sysmon
Z:
E:
D:
Home Folder
Drag a column header here to group by that column
Value Icon Shell Type MRU Position Created On Modified On Accessed On First Interacted Last Interacted
Summary Details Hex
Name: AtomicRedTeam
Absolute path: Desktop\My Computer\Desktop\PWF-main\PWF-main\AtomicRedTeam
Key-Value name path: BagMRU\1\3\0\0-1
Registry last write time: 2023-02-13 17:26:03.960
Target timestamps
Created on: 2023-02-13 17:21:04.000
Modified on: 2023-02-13 17:21:04.000
Last accessed on: 2023-02-13 17:21:04.000
Miscellaneous
Shell type: Directory
Node slot: 9
MRU position: 0
# of child bags: 0
First interacted with: 2023-02-13 17:21:42.494
Last interacted with: 2023-02-13 17:26:03.960
'UsrClass.dat' Registry hive loaded in 0.8206 seconds!
0 shellbags loaded in 0.0023 seconds
Time zone: UTC
0 of 0 rows visible (NaN)
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Value: FFlags Collapse all hives
Selected hive: SECURITY Last write: 2/13/2023 5:21:03 PM +00:00
10 of 10 values shown (100.00%)
Hidden keys: 0
5:35 PM
2/15/2023
Right Ctrl