

Windows Forensics- Part 2: User Behavior Analysis

Scope : Tracking User Activity & System Interactions

Now that we've identified **WHO** was on the system (**Part 1**), we'll discover **WHAT** they did by analyzing user **behavior artifacts** that track **application usage, file access, and system navigation**.

What We'll Cover in This Part

User Behavior Artifacts

- **UserAssist:** Applications opened and execution times
- **RecentDocs:** Files and folders accessed
- **Open/Save MRU:** Files opened or saved through applications
- **Last-Visited MRU:** Applications used to open specific files
- **Shellbags:** Locations browsed in Windows Explorer

Analysis Tools

- **Registry Explorer**
- **RegRipper** with specialized plugins
- **Notepad++** for bulk data analysis

Investigation Goals

- Reconstruct user activity timeline
- Identify suspicious application usage
- Track file and folder access patterns
- Build comprehensive user behavior profile

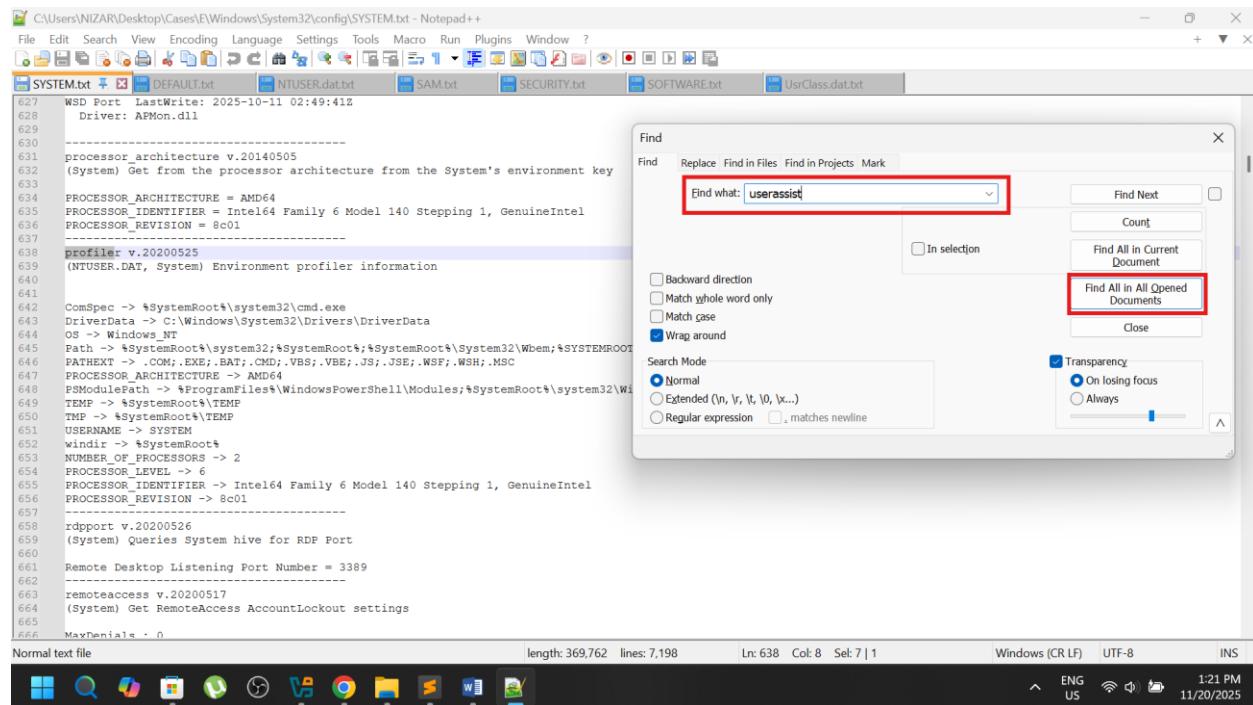
1. UserAssist Analysis

What is UserAssist ?

Tracks applications executed by the user, including timestamps and frequency counts.

Registry Location :

⇒ Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist



The screenshot shows a Notepad++ window displaying a text file named 'SYSTEM.txt'. The file contains system configuration data, including processor architecture and environment profiler information. A search dialog box is open over the window, with the search term 'userassist' highlighted in red. The search dialog includes options for 'Find Next', 'Count', 'Find All in Current Document', and 'Find All in All Opened Documents'. The 'Find All in All Opened Documents' option is also highlighted in red. The status bar at the bottom of the Notepad++ window shows file statistics: length: 369,762, lines: 7,198, Ln: 638, Col: 8, Set: 7 | 1, and system information: Windows (CR LF), UTF-8, INS. The taskbar at the bottom of the screen shows various application icons.

Searching for **UserAssist** entries in **Notepad++** to analyze application execution history and timestamps

```

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt - Notepad+
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SYSTEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UsrClass.dat.txt
894 -----
895 -----
896 [UserAssist]
897 Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
898 LastWrite Time: 2025-10-10 16:57:35Z
899 {9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}
900 {A3D53349-6E61-4557-8FC7-0028EDCEEBF6}
901 {B267E3AD-A825-4A09-82B9-EEC22AA3B847}
902 {BCB48336-4ADD-40FF-BB0B-D3190DACB3E2}
903 {CAA59E3C-4792-41A5-9909-6A6A8D32490E}
904 {CEBF5FCD-ACE2-4F4F-9178-9926F41749EA}
905 2025-10-10 17:41:05Z
906 Microsoft.Windows.Explorer (6)
907 Microsoft.Windows.ControlPanel (2)
908 2025-10-10 17:22:50Z
909 {(AC14E77-02E7-4E5D-B744-2EB1AE5198B7)}WindowsPowerShellV1.0\powershell.exe (2)
910 2025-10-10 17:16:44Z
911 Microsoft.Windows.SecHealthUI_cw5nh2txyewy!SecHealthUI (1)
912 2025-10-10 17:05:38Z
913
914
915
916
917
918
Search results - (7 hits)
Search "userassist" (7 hits in 2 files of 7 searched) [Normal]
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\DEFAULT.txt (3 hits)
Line 92: disableuserassist v.20230710
Line 93: (NTUSER.DAT) Get Start_TrackEnabled and Start_TrackProgs values which confirm if UserAssist was disabled.
Line 98: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist not found.
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt (4 hits)
Line 49: disableuserassist v.20230710
Line 49: (NTUSER.DAT) Get Start_TrackEnabled and Start_TrackProgs values which confirm if UserAssist was disabled.
Line 86: [UserAssist]
Line 89: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
Search "userassist" (7 hits in 2 files of 7 searched) [Normal]
Normal text file length: 38,770 lines: 989 Ln: 896 Col: 11 Sel: 10 | 1 Windows (CR LF) ANSI INS
^ ENG US 1:22 PM 11/20/2025

```

UserAssist data showing executed applications with timestamps, including powershell.exe

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UIME_CTLUIAConstructor	0	—	00:00:00,00s	—
Microsoft.GetStarted_Bwekyh3dbbwv!App	14	21	0d, 0h, 0m, 00s	2025-10-10 16:55:58
UIME_CTSSESSION	97	156	0d, 0h, 0m, 28s	2025-10-10 16:55:58
Microsoft.WindowsFeedbackHub_Bwekyh3dbbwv!App	13	19	0d, 0h, 0m, 08s	2025-10-10 16:55:58
Microsoft.WindowsMaps_Bwekyh3dbbwv!App	12	17	0d, 0h, 0m, 17s	2025-10-10 16:55:58
Microsoft.People_Bwekyh3dbbwv!vK7c3b7j2188y6d4ya362y1hac5a5b05e5	11	15	0d, 0h, 0m, 25s	2025-10-10 16:55:58
Microsoft.MicrosoftStickyNotes_Bwekyh3dbbwv!App	10	13	0d, 0h, 0m, 34s	2025-10-10 16:55:58
System32\GrapplingTool.exe	9	11	0d, 0h, 0m, 42s	2025-10-10 16:55:58
Microsoft.WindowsCalculator_Bwekyh3dbbwv!App	8	9	0d, 0h, 0m, 51s	2025-10-10 16:55:58
System32\Imprint.exe	7	7	0d, 0h, 0m, 00s	2025-10-10 16:55:58
Microsoft.Windows.ShellExperienceHost_cw5nh2txyewy!App	0	1	0d, 0h, 0m, 13s	—
MSEdge	1	7	0d, 0h, 0m, 59s	2025-10-10 17:05:38
Microsoft.Windows.Explorer	6	7	0d, 0h, 0m, 32s	2025-10-10 17:41:05
D:\fbox\WindowsAdditions.exe	1	0	0d, 0h, 0m, 00s	2025-10-10 17:01:11
D:\fbox\WindowsAdditions-smd4.exe	0	4	0d, 0h, 0m, 05s	—
(Program Files)\Oracle\VirtualBox\Guest Additions\Tools\lBoxDrv\linst.exe	0	0	0d, 0h, 0m, 01s	—
System32\cmd.exe	0	0	0d, 0h, 0m, 01s	—
windows.immersivecontrolpanel_cw5nh2txyewy!microsoft.windows.immersivecontrolpanel	0	3	0d, 0h, 0m, 25s	—
Microsoft.Windows.Search_cw5nh2txyewy!Control	0	6	0d, 0h, 0m, 79s	—
Microsoft.Windows.SecHealthUI_cw5nh2txyewy!SecHealthUI	1	1	0d, 0h, 0m, 34s	2025-10-10 17:16:44
System32\WindowsPowerShellV1.0\powershell.exe	2	12	0d, 0h, 0m, 36s	2025-10-10 17:22:50

Total rows: 32

Type viewer

Bookmark information:

- Hive: C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.DAT
- Category: Program execution
- Name: UserAssist
- Key path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
- Short description: Recently accessed items
- Long description: Contains a list of ROT-13 encoded values for things like shortcuts, programs, etc.

Selected hive: NTUSER.DAT Last write: 10/10/2025 4:57:35 PM +00:00 Key contains no values

Value: None Collapse all hives Hidden keys: 0

span style="float: right;">^ ENG US 1:25 PM 11/20/2025

UserAssist entries viewed in Registry Explorer showing application execution counts and timestamps

UserAssist Analysis Results

System & Command Line Tools :

- **Windows PowerShell (2 executions)** - Last run: 2025-10-10 17:22:50Z
- **CMD.EXE** - Command prompt execution
- **File Explorer (6 executions)** - Frequent file navigation
- **Control Panel (2 executions)** - System configuration access

Windows Built-in Applications :

- **Snipping Tool (9 executions)** - Screenshot capability
- **Paint (mspaint.exe) (7 executions)** - Image editing
- **Notepad** - Text file editing
- **Windows Calculator (8 executions)** - Utility usage

Windows Store & System Apps :

- **Microsoft Edge** - Web browsing activity
- **Windows Security (SecHealthUI)** - Security settings check
- **Feedback Hub (13 executions)** - System feedback
- **Maps (12 executions)** - Location services
- **People (11 executions)** - Contacts access
- **Sticky Notes (10 executions)** - Note-taking
- **Get Started (14 executions)** - Windows tutorial
- **Windows Search/Cortana** - File searching

- **Shell Experience Host** - UI interactions
- **Immersive Control Panel** - Settings access

Virtualization Tools :

- **VirtualBox Guest Additions** - VM tools installation
- **VBoxDrvInst.exe** - VirtualBox driver installer

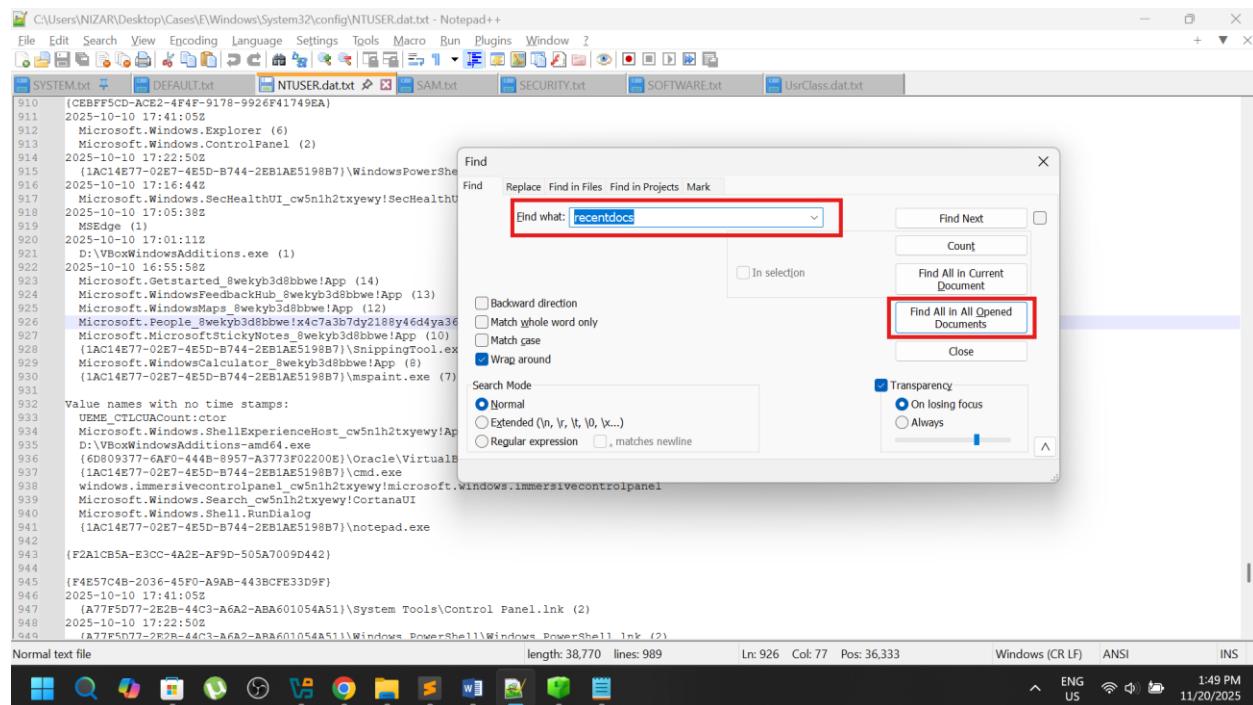
2. RecentDocs Analysis

What is RecentDocs ?

Tracks recently accessed files, folders, and locations in Windows Explorer, showing user file browsing habits and accessed resources.

Registry Location :

⇒ Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



Searching for **RecentDocs** entries in **Notepad++** to analyze recently accessed files and folders

```

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt - Notepad+
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SYSTEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UsrClass.dat.txt
740 Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found.
741 -----
742 recentdocs v.20200427
743 (NTUSER.DAT) Gets contents of user's RecentDocs key
744
745 RecentDocs
746 **All values printed in MRUListEx order.
747 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
748 LastWrite Time: 2025-10-10 17:41:12Z
749 7 = Network and Internet
750 6 = ::{18E908FC-9ECC-40F6-915B-F4CA0E70D03D}
751 5 = The Internet
752 4 = network
753 2 = C:\
754 3 = This PC
755 1 = Local Disk (C:)
756 0 = Atomic Red Team
757
758 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
759 LastWrite Time: 2025-10-10 17:41:12Z
760 MRUListEx = 3,2,1,0
761 3 = Network and Internet
762 2 = The Internet
763 1 = This PC
764 0 = Local Disk (C:)

Search results - (9 hits)
Search "recentdocs" (9 hits in 3 files of 7 searched) [Normal]
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\DEFAULT.txt (3 hits)
Line 281: recentdocs v.20200427
Line 282: (NTUSER.DAT) Gets contents of user's RecentDocs key
Line 284: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs not found.
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt (5 hits)
Line 742: recentdocs v.20200427
Line 743: (NTUSER.DAT) Gets contents of user's RecentDocs key
Line 745: RecentDocs
Line 747: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Line 758: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder

Normal text file length: 38,770 lines: 989 Ln: 745 Col: 11 Sel: 10 | 1 Windows (CR LF) ANSI INS

```

RecentDocs analysis revealing accessed files and folders including suspicious "Atomic Red Team" folder

Extension	Value Name	Target Name	Link Name	Menu Position	Opened On	Extension Last Opened
RecentDocs	7	Network and Internet	Network and Internet.link	---	0 2025-10-10 17:41:12	2025-10-10 17:41:12
RecentDocs	6	::{18E908FC-9ECC-40F6-915B-F4CA0E70D03D}	Network and Sharing	1		
RecentDocs	5	The Internet	The Internet.link	2		
RecentDocs	4	network	ms-settings:network.link	3		
RecentDocs	2	C:\	Local Disk (C:) (2).link	4		
RecentDocs	3	The PC	The PC.link	5		
RecentDocs	1	Local Disk (C:)	Local Disk (C:).link	6		
RecentDocs	0	Atomic Red Team	Atomic_Red_Team.link	7		
Folder	3	Network and Internet	Network and Internet.link	0 2025-10-10 17:41:12		
Folder	2	The Internet	The Internet.link	1		
Folder	1	This PC	This PC.link	2		
Folder	0	Local Disk (C:)	Local Disk (C:).link	3		

Total rows: 12

Type viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 000000000007 00 00 06 00 00 00 05 00 00 04 00 00 00 02 00 00 03 00 00 01 00 00 00 00 FF FF FF FF 00000001E000 FF FF FF FF ...9999

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Data interpreter ? Value: MBUI.info[] Collapse all hives Hidden keys: 0 ENG US 1:52 PM 11/20/2025

RecentDocs entries viewed in Registry Explorer showing accessed files including suspicious "Atomic Red Team" folder

RecentDocs Analysis Results

Recent Documents (Main Key)

- **LastWrite Time:** 2025-10-10 17:41:12Z
- **Network and Internet** - Network settings access
- **The Internet** - Web browsing activity
- **network** - Network location browsing
- ****C:**** - Root directory access
- **This PC** - Computer management
- **Local Disk (C:)** - Primary drive navigation
- **Atomic_Red_Team** - SUSPICIOUS - Red team tool folder

Folder Access (SubKey)

LastWrite Time: 2025-10-10 17:41:12Z

- **Network and Internet**
- **The Internet**
- **This PC**
- **Local Disk (C:)**

⚠ Important Note: During RecentDocs analysis, we discovered a suspicious auto-start entry in the Run registry key pointing to C:\Path\AtomicRedTeam.exe - indicating persistence mechanism. This significantly increases the suspiciousity of the Atomic Red Team artifacts we found earlier, suggesting active malicious persistence establishment.

```

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt - Notepad+
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SYSTEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UsrClass.dat.txt
754 3 = This PC
755 1 = Local Disk (C:)
756 0 = Atomic_Red_Team
757
758 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
759 LastWrite Time 2025-10-10 17:41:12Z
760 MRUListEx = 3,2,1,0
761 3 = Network and Internet
762 2 = The Internet
763 1 = This PC
764 0 = Local Disk (C:)
765
766 -----
767 run v.20200511
768 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive
769
770 Software\Microsoft\Windows\CurrentVersion\Run
771 LastWrite Time 2025-10-10 17:37:26Z
772 MicrosoftEdgeAutoLaunch 67FFE22564D4D759228549F974A6340D = "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
773 OneDrive = "C:\Users\K83L_D\OneDrive\Local\Microsoft\OneDrive\OneDrive.exe" /background
774 Atomic Red Team - C:\Path\AtomicRedTeam.exe
775
776 Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
777
778 Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.

Search results - (9 hits)
Search "recentdocs" (9 hits in 3 files of 7 searched) [Normal]
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\DEFAULT.txt (3 hits)
Line 281: recentdocs v.20200427
Line 282: (NTUSER.DAT) Gets contents of user's RecentDocs key
Line 284: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs not found.
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt (5 hits)
Line 742: recentdocs v.20200427
Line 743: (NTUSER.DAT) Gets contents of user's RecentDocs key
Line 745: RecentDocs
Line 747: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Line 748: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder

```

Normal text file length: 38,770 lines: 989 Ln: 776 Col: 62 Pos: 30,936 Windows (CR LF) ANSI INS

ENG US 2:12 PM 11/20/2025

Persistence mechanism found in Run registry key with *AtomicRedTeam.exe* - increasing suspicion of malicious activity

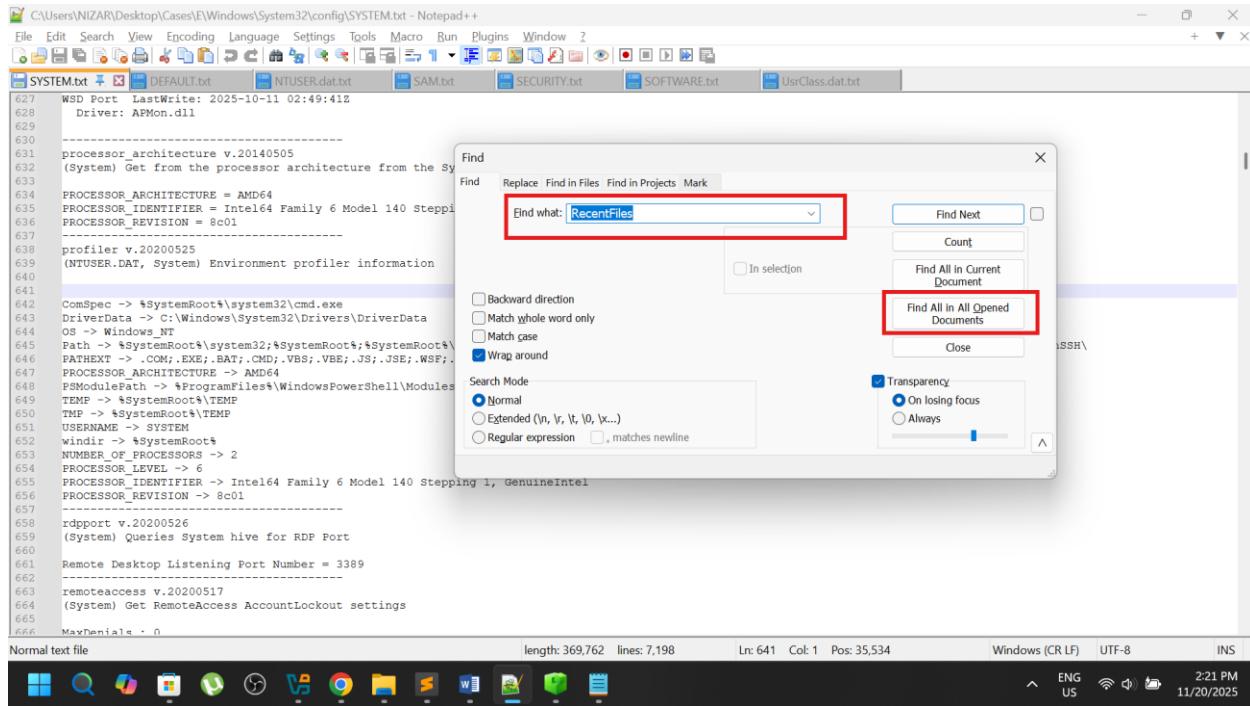
3. Open/Save MRU Analysis

What is Open/Save MRU?

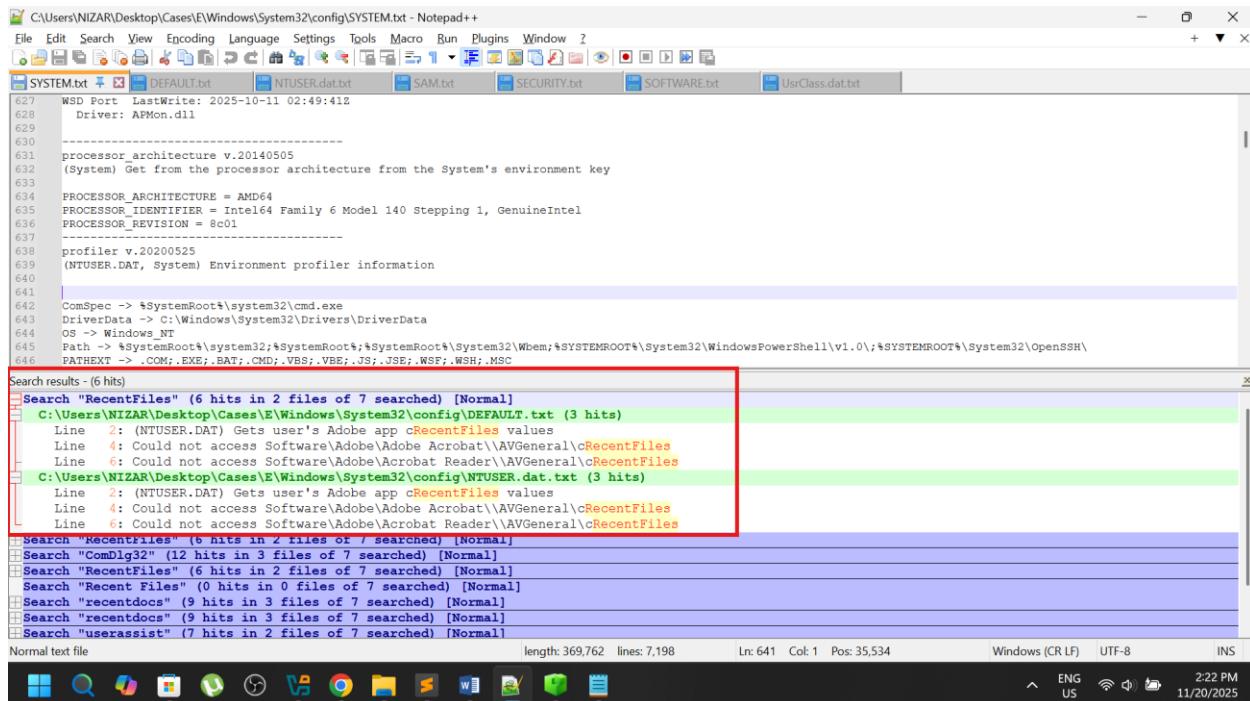
Tracks files recently opened or saved within specific applications (not Windows Explorer), showing document workflow and application usage patterns.

Registry Locations :

⇒ Software\[Application Name]\Recent Files



Searching for "RecentFiles" in Notepad++ to analyze application-specific file opening history



Adobe Acrobat and Acrobat Reader CRecentFiles entries found, but showing no recent PDF file activity

Open/Save MRU Analysis Results

Applications Checked

- **Adobe Acrobat** - No recent PDF files tracked
- **Adobe Acrobat Reader** - No recent PDF files tracked

Missing Applications (No Recent Files Found)

- **Microsoft Office Suite** (Word, Excel, PowerPoint)
- **Image Editors** (Photoshop, GIMP, Paint.NET)
- **Development Tools** (VS Code, Notepad++)
- **Archive Utilities** (WinRAR, 7-Zip)
- **Media Players** (VLC, Windows Media Player)

4. Last-Visited MRU Analysis

What is Last-Visited MRU ?

Tracks which applications were last used to open specific file types, showing file association preferences and application usage patterns.

Registry Location :

⇒ Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt - Notepad++

```

627 WSD Port LastWrite: 2025-10-11 02:49:41Z
628 Driver: AFMON.dll
629
630 -----
631 processor_architecture v.20140505
632 (System) Get from the processor architecture from the Sy
633
634 PROCESSOR_ARCHITECTURE = AMD64
635 PROCESSOR_IDENTIFIER = Intel64 Family 6 Model 140 Steppi
636 PROCESSOR_REVISION = 8c01
637
638 profiler v.20200525
639 (NTUSER.DAT, System) Environment profiler information
640
641 ComSpec -> %SystemRoot%\system32\cmd.exe
642 DriverData -> C:\Windows\System32\Drivers\DriverData
643 OS -> Windows_NT
644 Path -> %SystemRoot%\system32;%SystemRoot%\PATHEXT -> .COM;.EXE;.BAT;.CMD;.VBS;.JS;.JSE;.WSF;.

```

Find what: ComDlg32

Find All in All Opened Documents

Search results (6 hits)

- C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt
 - Line 2: (NTUSER.DAT) Gets user's Adobe app cRecentFiles values
 - Line 4: Could not access Software\Adobe\Adobe Acrobat\AVGeneral\cRecentFiles
 - Line 6: Could not access Software\Adobe\Acrobat Reader\AVGeneral\cRecentFiles
- C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt
 - Line 2: (NTUSER.DAT) Gets user's Adobe app cRecentFiles values
 - Line 4: Could not access Software\Adobe\Adobe Acrobat\AVGeneral\cRecentFiles
 - Line 6: Could not access Software\Adobe\Acrobat Reader\AVGeneral\cRecentFiles
- Search "RecentFiles" (6 hits in 2 files of 7 searched) [Normal]
- Search "ComDlg32" (12 hits in 3 files of 7 searched) [Normal]
- Search "RecentFiles" (6 hits in 2 files of 7 searched) [Normal]
- Search "RecentFiles" (0 hits in 0 files of 7 searched) [Normal]
- Search "recentdocs" (9 hits in 3 files of 7 searched) [Normal]
- Search "recentdocs" (9 hits in 3 files of 7 searched) [Normal]
- Search "userassist" (7 hits in 2 files of 7 searched) [Normal]

Normal text file length: 369,762 lines: 7,198 Ln: 641 Col: 1 Pos: 35,534 Windows (CR LF) UTF-8 INS

Searching for "ComDlg32" in Notepad++ to analyze file association and application usage history

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt - Notepad++

```

453 cmdproc v.20200515
454 (NTUSER.DAT) Autostart - get Command Processor\AutoRun value from NTUSER.DAT hive
455
456 Software\Microsoft\Command Processor not found.
457
458 comdlg32 v.20200517
459 Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
460 LastWrite Time: 2025-10-10 17:17:05Z
461 CIDBsizeMRU
462 LastWrite: 2025-10-10 17:17:05Z
463 Note: All value names are listed in MRUListEx order.
464
465 PickerHost.exe
466
467 LastVisitedPidMRU
468 LastWrite time: 2025-10-10 17:17:05Z
469 Note: All value names are listed in MRUListEx order.
470
471 PickerHost.exe - My Computer\c:
472
473 OpenSavePidMRU
474 LastWrite time: 2025-10-10 17:17:05Z
475 OpenSavePidMRU*
476 LastWrite Time: Fri Oct 10 17:17:05 2025
477 Note: All value names are listed in MRUListEx order.
478
479 My Computer\c:
480
481
482

```

Search results (-12 hits)

- C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\DEFAULT.txt (2 hits)
 - Line 74: comdlg32 v.20200517
 - Line 75: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 not found.
- C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\NTUSER.dat.txt (2 hits)
 - Line 458: comdlg32 v.20200517
 - Line 460: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
- C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SOFTWARE.txt (8 hits)
 - Line 9901: 2019-12-07 09:16:01Z (725F645B-EAED-4fc5-B1C5-D9AD0ACCBAA5)\InprocServer32: %SystemRoot%\System32\comdlg32.dll

Normal text file length: 38,770 lines: 989 Ln: 458 Col: 9 Sel: 8 | 1 Windows (CR LF) ANSI INS

ComDlg32 registry entries showing PickerHost.exe usage for file operations on C: drive

Last-Visited MRU Analysis Results

Application Usage Patterns

- **PickerHost.exe** - Windows file picker dialog usage
- **Used for file selection operations**
- **Accessed locations:** My Computer\C:

File Dialog Activity

- **Open/Save Dialogs:** Accessed through PickerHost.exe
- **Primary Location:** C:\ drive root directory
- **Last Activity:** 2025-10-10 17:17:05Z

Note: **PickerHost.exe** is a legitimate Windows component for file dialogs.

5. Shellbags Analysis

What are Shellbags ?

Shellbags are Windows registry artifacts **that store information about folders a user has opened in Windows Explorer**, including **view settings, window positions, and timestamps - even for deleted folders**.

Registry Locations :

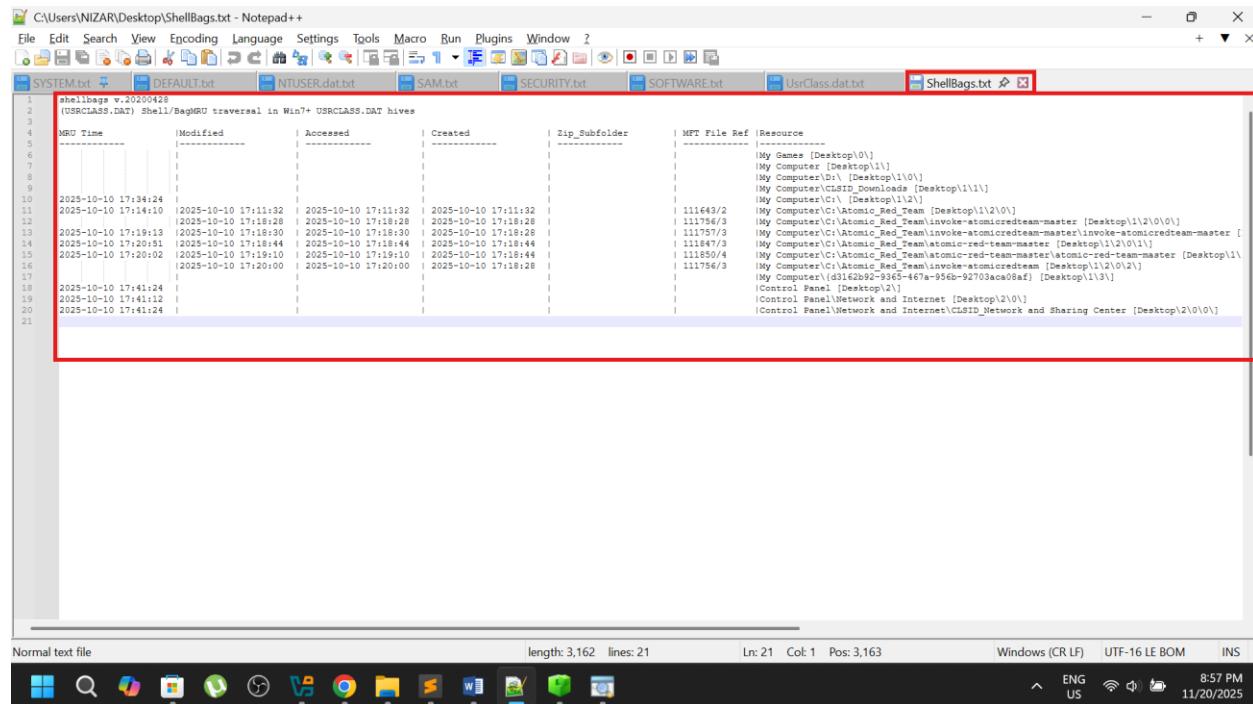
- ⇒ HKCU\Software\Microsoft\Windows\Shell\Bags
- ⇒ HKCU\Software\Microsoft\Windows\Shell\BagMRU
- ⇒ HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

Analysis Method

We'll use **RegRipper** to parse **Shellbags** from the **USRCLASS.DAT** hive:

```
⇒ rip.exe -r C:\Users\NIZAR\Desktop\Cases\Analysis\Registry\USRCLASS.DAT -p  
shellbags > ShellBags.txt
```

This will reveal all **folder locations** the user navigated to in **Windows Explorer**.



MBX Time	Modified	Accessed	Created	Zip_Subfolder	MFT File Ref	Resource
2025-10-10 17:34:24	[2025-10-10 17:11:32]	[2025-10-10 17:11:32]	[2025-10-10 17:11:32]			My Places [Desktop\0\]
2025-10-10 17:14:10	[2025-10-10 17:18:28]	[2025-10-10 17:18:28]	[2025-10-10 17:18:28]			My Computer [Desktop\1\0\1\]
2025-10-10 17:19:13	[2025-10-10 17:18:30]	[2025-10-10 17:18:30]	[2025-10-10 17:18:28]			My Computer\CLSID_Download\ [Desktop\1\1\]
2025-10-10 17:20:02	[2025-10-10 17:19:10]	[2025-10-10 17:19:10]	[2025-10-10 17:18:44]			My Computer\CLSID_Download\ [Desktop\1\1\]
2025-10-10 17:20:00	[2025-10-10 17:20:00]	[2025-10-10 17:18:28]	[2025-10-10 17:18:28]			My Computer\CLSID_Download\ [Desktop\1\1\]
2025-10-10 17:41:24						My Computer\CLSID_Download\ [Desktop\1\1\]
2025-10-10 17:41:12						Control Panel [Desktop\2\]
2025-10-10 17:41:24						Control Panel\Network and Internet [Desktop\2\0\0\]
						Control Panel\Network and Internet\CLSID_Network and Sharing Center [Desktop\2\0\0\]

Shellbags data showing folder navigation history including Atomic Red Team directory access

(USRCLASS.DAT) ShellBagMRU traversal in Win7+ USRCLASS.DAT hives						
MRU Time	Modified	Accessed	Created	Zip_Subfolder	MFT File Ref	Resource
2025-10-10 17:34:24						[My Computer\G:\[Desktop\1\2\]
2025-10-10 17:14:10	[2025-10-10 17:11:32]	[2025-10-10 17:11:32]	[2025-10-10 17:11:32]		111643/2	[My Computer\C:\Atomic_Red_Team\[Desktop\1\2\0\]
	[2025-10-10 17:18:28]	[2025-10-10 17:18:28]	[2025-10-10 17:18:28]		111756/3	[My Computer\C:\Atomic_Red_Team\invoke-atomicredteam-master\[Desktop\1\2\0\0\]
2025-10-10 17:19:13	[2025-10-10 17:18:30]	[2025-10-10 17:18:30]	[2025-10-10 17:18:28]		111757/3	[My Computer\C:\Atomic_Red_Team\invoke-atomicredteam-master\invoke-atomicredteam-m
2025-10-10 17:20:51	[2025-10-10 17:18:44]	[2025-10-10 17:18:44]	[2025-10-10 17:18:44]		111847/3	[My Computer\C:\Atomic_Red_Team\atomic-red-team-master\[Desktop\1\2\0\1\]
2025-10-10 17:20:02	[2025-10-10 17:19:10]	[2025-10-10 17:19:10]	[2025-10-10 17:18:44]		111850/4	[My Computer\C:\Atomic_Red_Team\atomic-red-team-master\atomic-red-team-master [Des
	[2025-10-10 17:20:00]	[2025-10-10 17:20:00]	[2025-10-10 17:18:28]		111756/3	[My Computer\C:\Atomic_Red_Team\invoke-atomicredteam\[Desktop\1\2\0\2\]
						[My Computer\{d3162b92-9365-4678-956b-92703ac08af\} [Desktop\1\3\]
2025-10-10 17:41:24						[Control Panel [Desktop\2\]
2025-10-10 17:41:12						[Control Panel\Network and Internet [Desktop\2\0\]
2025-10-10 17:41:24						[Control Panel\Network and Internet\CLSID_Network and Sharing Center [Desktop\2\0\]

Shellbags analysis in Timeline Explorer application showing folder access chronology and Atomic Red Team activity timeline

Shellbags Analysis Results

Atomic Red Team Activity SUSPICIOUS

- C:\Atomic_Red_Team - Accessed: 2025-10-10 17:14:10
 - C:\Atomic_Red_Team\invoke-atomicredteam-master - Multiple subfolders accessed
 - C:\Atomic_Red_Team\atomic-red-team-master - Deep navigation into framework
 - **Timeline:** Extensive activity between 17:14:10 - 17:20:51

System Locations

- ****C:**** - Root directory accessed
 - ****D:**** - Secondary drive accessed

- **My Games** - User profile folder
- **Downloads** - User download folder

Network & Control Panel

- **Control Panel\Network and Internet** - Network configuration
- **Network and Sharing Center** - Network settings management
- **Last accessed:** 2025-10-10 17:41:24