

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

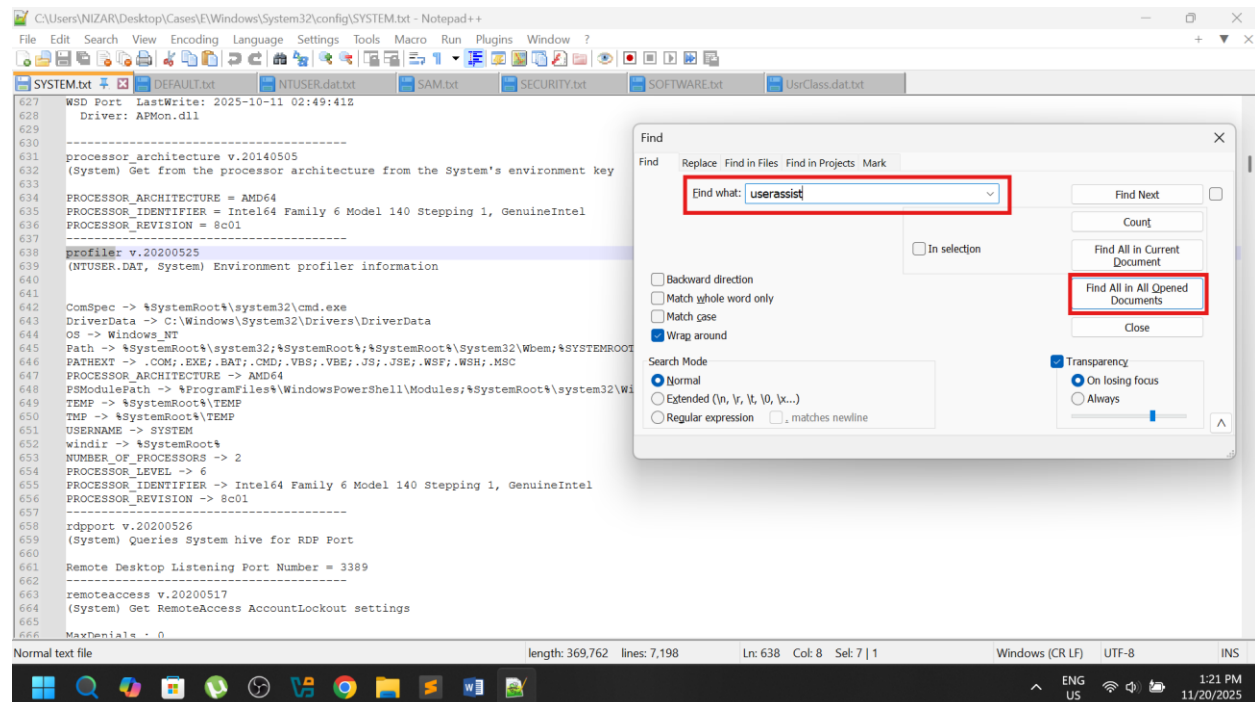
1. UserAssist Analysis

What is UserAssist ?

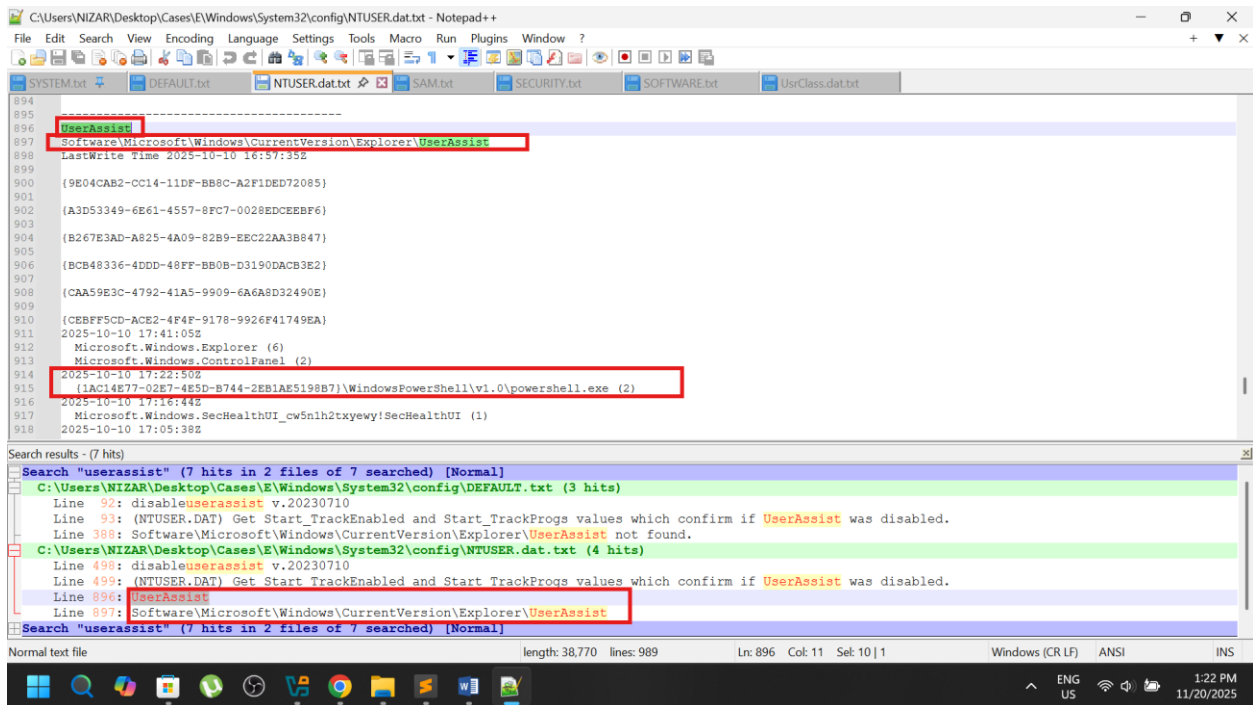
Tracks applications executed by the user, including timestamps and frequency counts.

Registry Location :

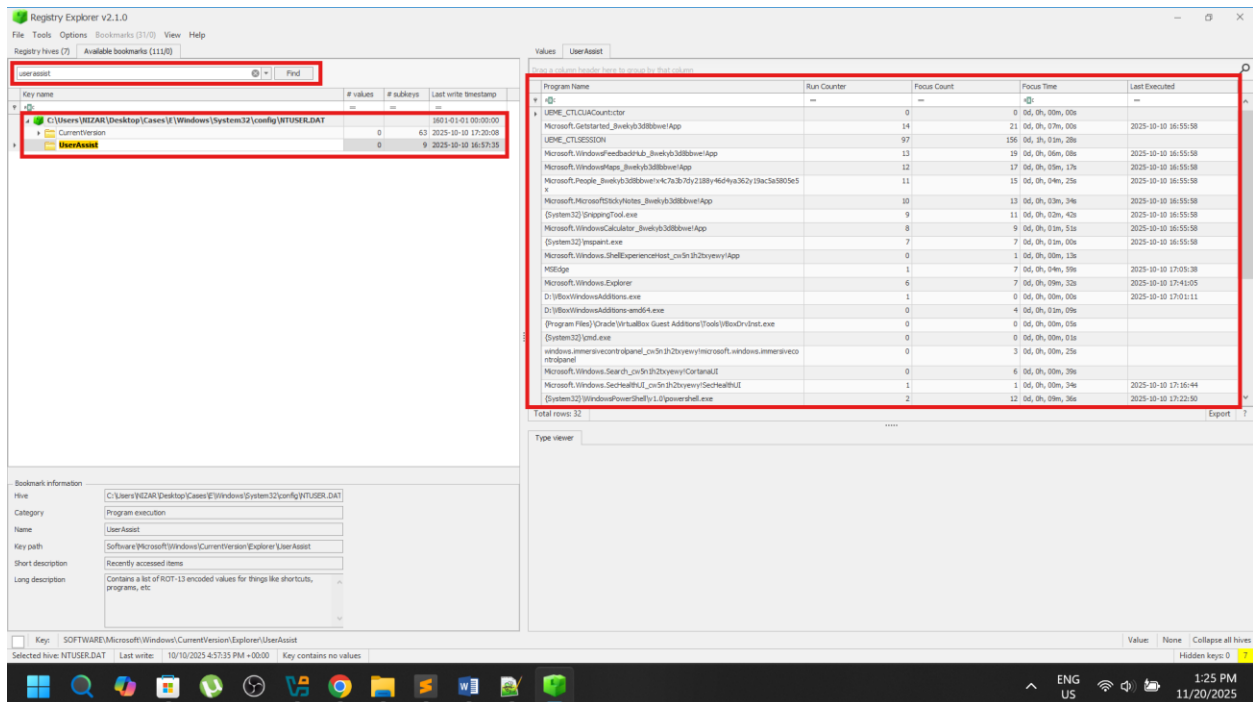
⇒ Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist



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



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



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

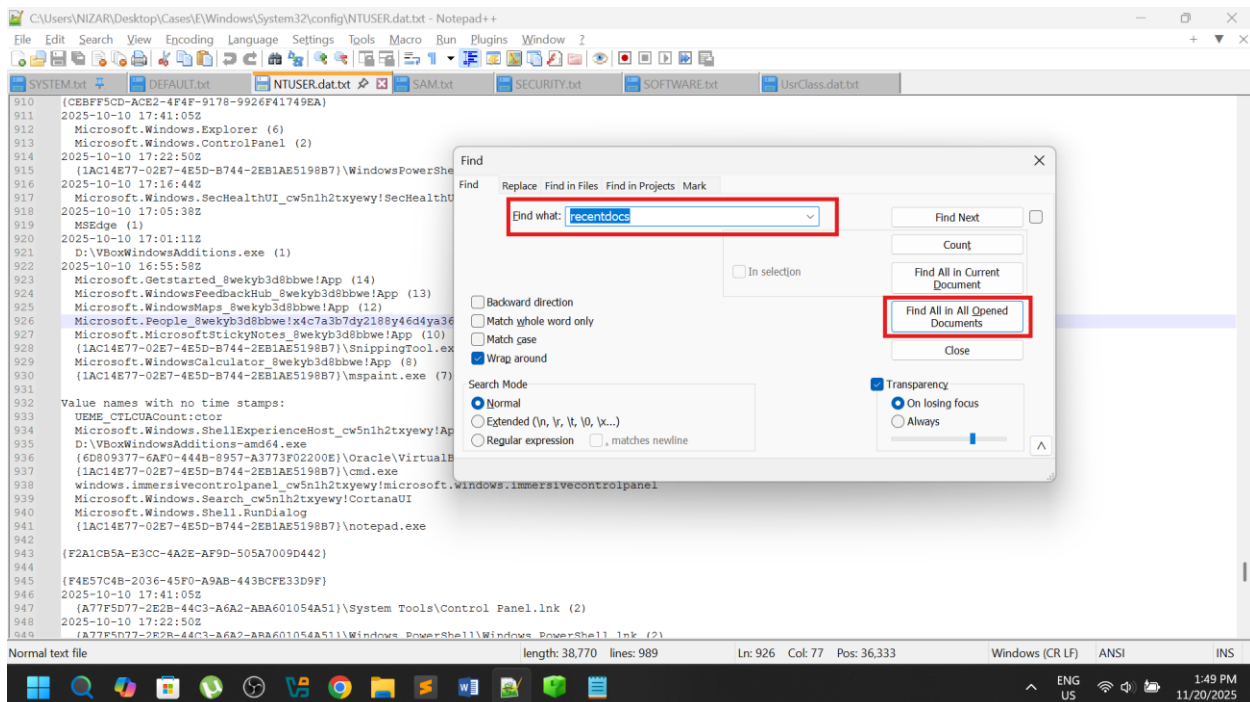
2. RecentDocs Analysis

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\EWindows\System32\config\NTUSER.dat.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window 2
SYSTEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UserClass.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 MRUList\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 = ::(8E908FC9-BECC-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\EWindows\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\EWindows\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 Lnc: 745 Col: 11 Sel: 10 | 1 Windows (CR LF) ANSI INS
ENG US 1:50 PM 11/20/2025
```

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

Registry Explorer v2.1.0

File Tools Options Bookmarks (31/0) View Help

Registry Hives (7) Available bookmarks (111/0)

Key name	# values	# subkeys	Last write timestamp
C:\Users\NIZAR\Desktop\Cases\EWindows\System32\config\NTUSER.DAT	0	63	2025-10-10 17:30:08
RecentDocs	9	1	2025-10-10 17:41:12
Software\Microsoft\Windows\CurrentVersion\Explorer	11	153	2025-10-10 17:15:46

Extension	Value Name	Target Name	Link Name	File Position	Opened On	Extension Last Opened
RecentDocs	7	Network and Internet	Network and Internet.lnk	0	2025-10-10 17:41:12	2025-10-10 17:41:12
RecentDocs	6	::(8E908FC9-BECC-40F6-915B-F4CA0E70D03D)	Network and Sharing Center.lnk	1		
RecentDocs	5	The Internet	The Internet.lnk	2		
RecentDocs	4	network	ms-settings-network.lnk	3		
RecentDocs	2	C:\	Local Disk (C:) (2).lnk	4		
RecentDocs	3	This PC	This PC.lnk	5		
RecentDocs	1	Local Disk (C:)	Local Disk (C:).lnk	6		
RecentDocs	0	Atomic Red Team	Atomic_Red_Team.lnk	7		
Folder	5	Network and Internet	Network and Internet.lnk	0	2025-10-10 17:41:12	
Folder	2	The Internet	The Internet.lnk	1		
Folder	1	This PC	This PC.lnk	2		
Folder	0	Local Disk (C:)	Local Disk (C:).lnk	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
0000001E00 00 FF FF FF FF

Current offset: 0 (0x0) Bytes selected: 0 (0x0) Value: MRUListEx Collapse all Hives Hidden keys: 0

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Selected hive: NTUSER.DAT Last write: 10/10/2025 5:41:12 PM +0000 9 of 9 values shown (100.00%)

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**.

The screenshot shows a Notepad++ window with the file path `C:\Users\NIZAR\Desktop\Cases\EWindows\System32\config\NTUSER.dat.txt`. The main text area displays the contents of the NTUSER.DAT file, which includes registry information for the user's RecentDocs folder and the Run registry key. Two specific entries are highlighted with red boxes: `Software\Microsoft\Windows\CurrentVersion\Run` and `Atomic Red Team - C:\Path\AtomicRedTeam.exe`. Below the main text area, a search results pane shows 9 hits for the term "recentdocs". The search results are organized into three sections: "Search 'recentdocs' (9 hits in 3 files of 7 searched) [Normal]", "C:\Users\NIZAR\Desktop\Cases\EWindows\System32\config\DEFAULT.txt (3 hits)", and "C:\Users\NIZAR\Desktop\Cases\EWindows\System32\config\NTUSER.dat.txt (5 hits)". The search results for the NTUSER.dat.txt file are highlighted in green. The status bar at the bottom indicates the file is a "Normal text file" with a length of 38,770 bytes and 989 lines. The system tray shows the date and time as 11/20/2025, 2:12 PM.

```
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\NIZAR\AppData\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\EWindows\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\EWindows\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 Lnc: 776 Col: 62 Pos: 30,936 Windows (CR LF) ANSI INS

2:12 PM 11/20/2025

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

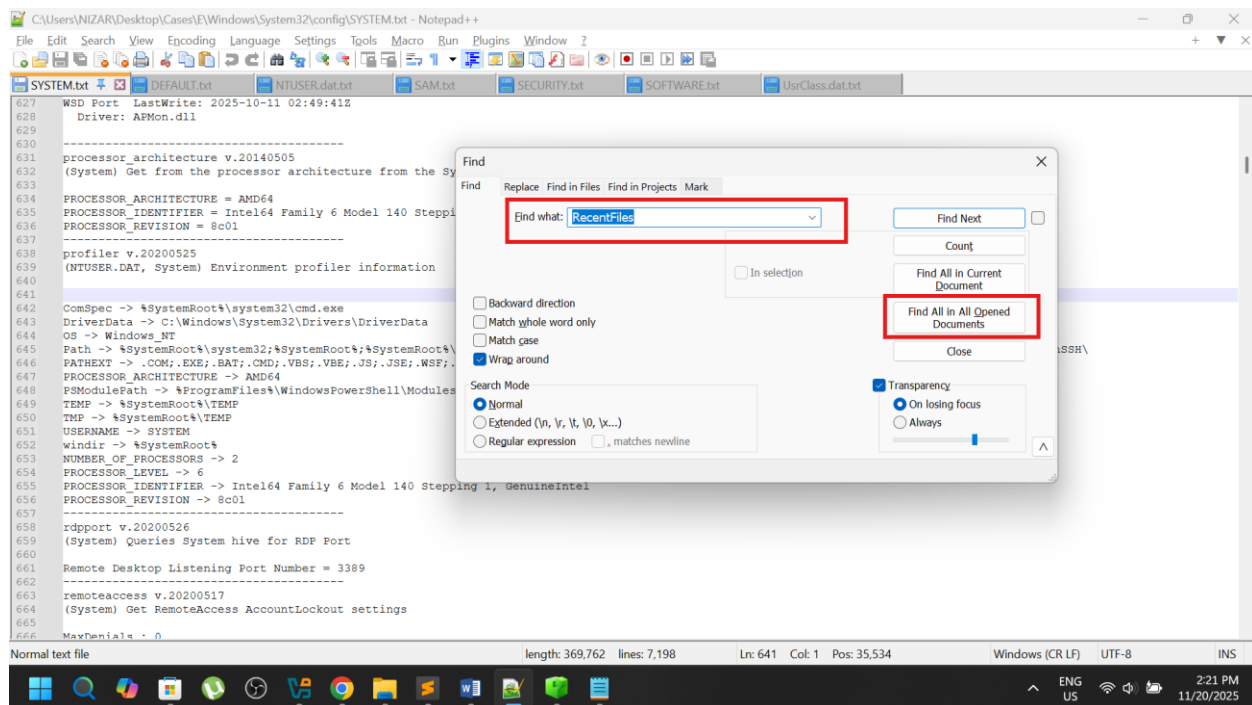
3. Open/Save MRU Analysis

What is Open/Save MRU?

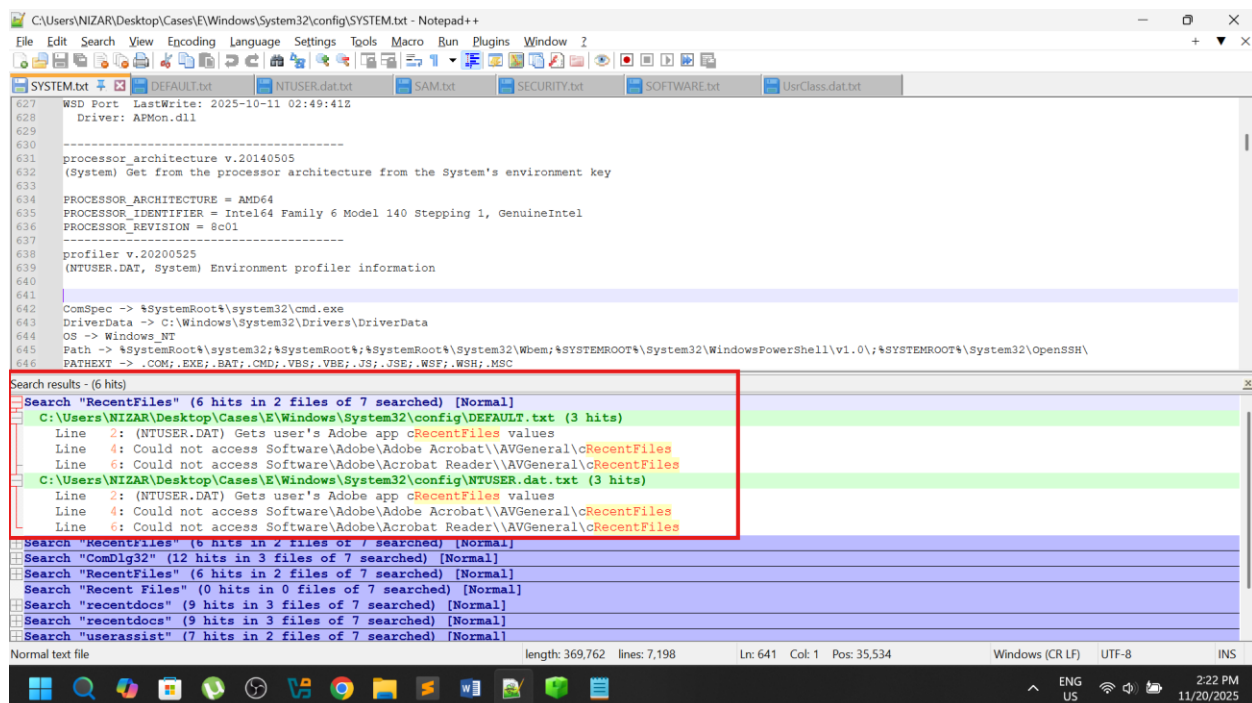
Tracks files recently opened or saved within specific applications (not Windows Explorer), showing document workflow and application usage patterns.

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)

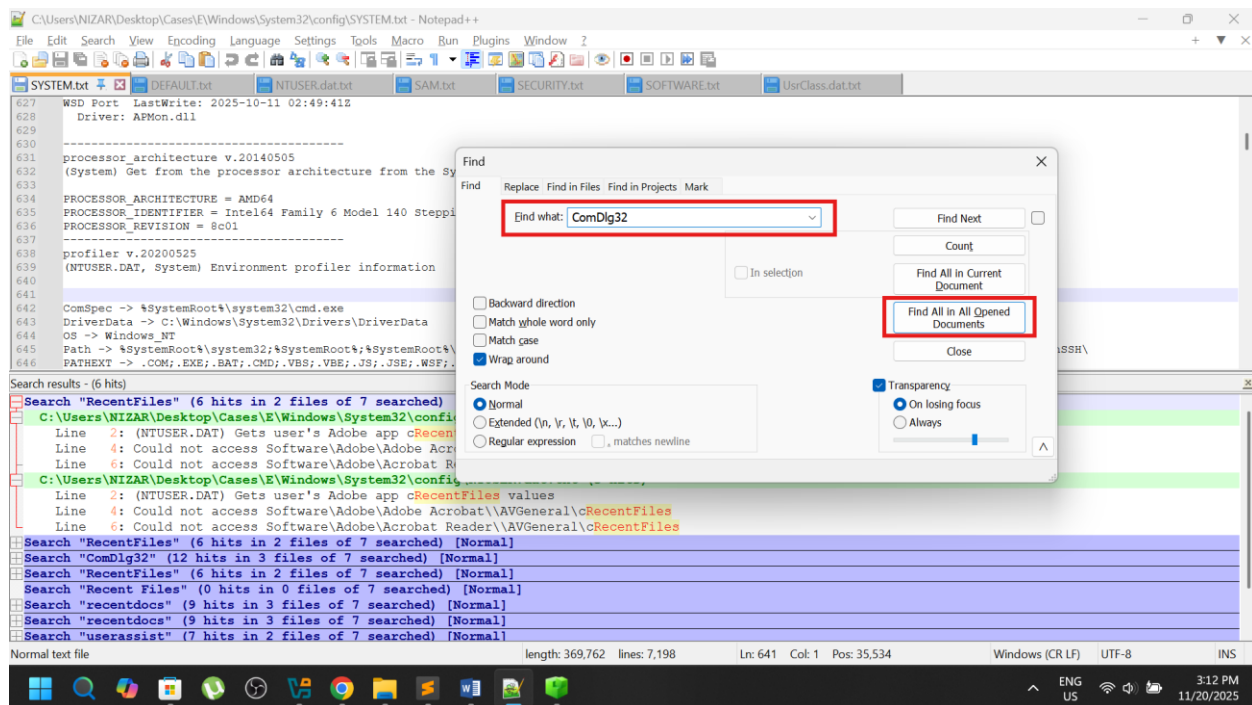
4. Last-Visited MRU Analysis

What is Last-Visited MRU ?

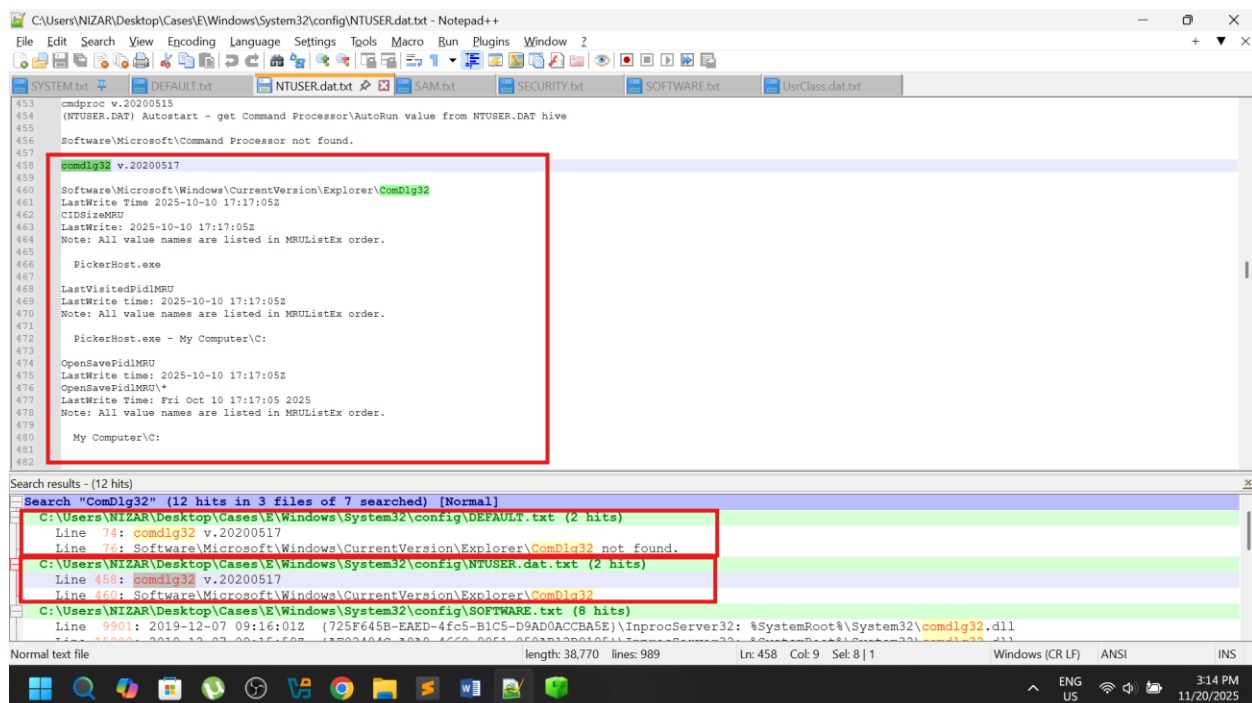
Tracks which applications were last used to open specific file types, showing file association preferences and application usage patterns.

Registry Location :

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



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



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 :

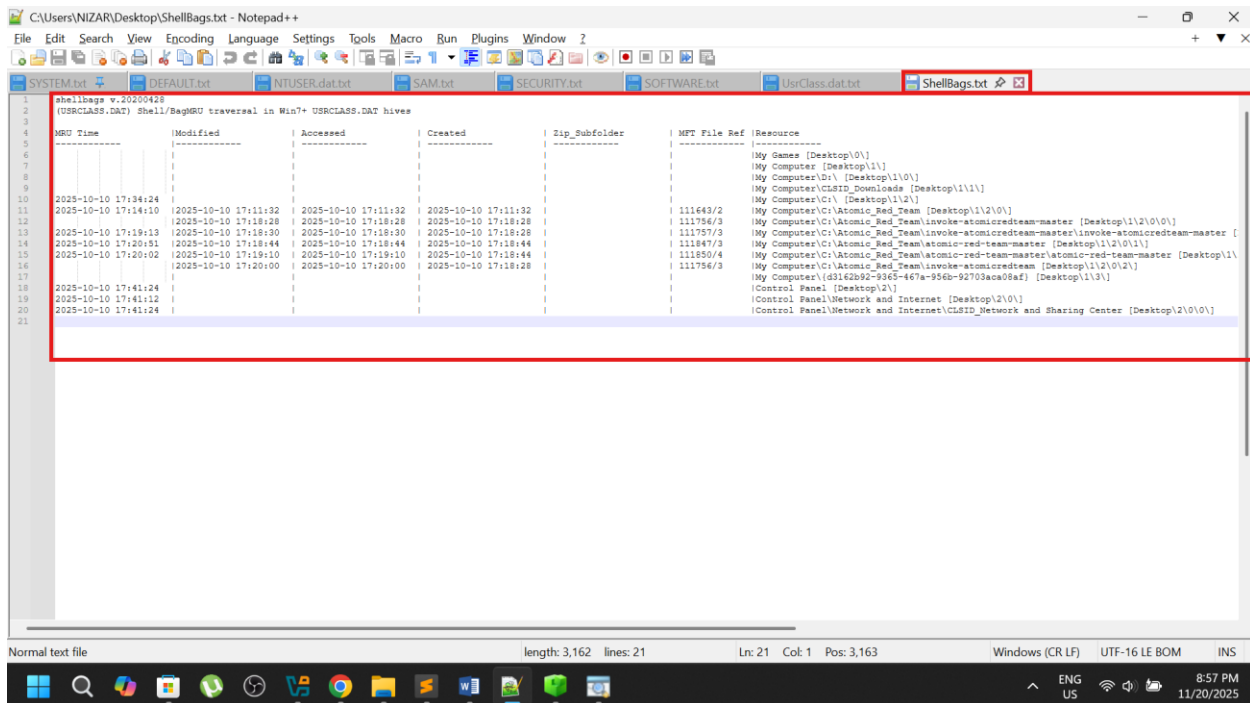
- ⇒ HKCU\Software\Microsoft\Windows\Shell\Bags
- ⇒ HKCU\Software\Microsoft\Windows\Shell\BagMRU
- ⇒ HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

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**.



```
1 shellbags v.20200428
2 (USRCLASS.DAT) Shell/BagRU traversal in Win7+ USRCLASS.DAT hives
3
4 MSO Time      Modified      Accessed      Created      Zip_Subfolder  MFT File Ref  Resource
5 -----
6
7
8
9
10 2025-10-10 17:34:24 | | | | | | My Games [Desktop\0\]
11 2025-10-10 17:14:10 | | | | | | My Computer [Desktop\1\]
12 | | | | | | My Computer\0\ [Desktop\1\0\]
13 | | | | | | My Computer\CSID_Downloads [Desktop\1\1\]
14 | | | | | | My Computer\0\ [Desktop\1\2\]
15 2025-10-10 17:19:13 | 2025-10-10 17:11:32 | 2025-10-10 17:11:32 | 2025-10-10 17:11:32 | | 111643/2 | My Computer\Atomic_Red_Team [Desktop\1\2\0\]
16 2025-10-10 17:20:11 | 2025-10-10 17:18:28 | 2025-10-10 17:18:28 | 2025-10-10 17:18:28 | | 111756/3 | My Computer\Atomic_Red_Team\invoke-atomicredteam-master [Desktop\1\2\0\0\]
17 2025-10-10 17:20:02 | 2025-10-10 17:18:30 | 2025-10-10 17:18:30 | 2025-10-10 17:18:28 | | 111757/3 | My Computer\Atomic_Red_Team\invoke-atomicredteam-master\invoke-atomicredteam-master [Desktop\1\2\0\1\]
18 | | | | | | My Computer\Atomic_Red_Team\atomic-red-team-master [Desktop\1\2\0\1\]
19 | | | | | | My Computer\Atomic_Red_Team\atomic-red-team-master\atomic-red-team-master [Desktop\1\2\0\2\]
20 | | | | | | My Computer\0\ [Desktop\1\3\]
21 | | | | | | Control Panel [Desktop\2\]
22 | | | | | | Control Panel\Network and Internet [Desktop\2\0\]
23 | | | | | | Control Panel\Network and Internet\CSID_Network and Sharing Center [Desktop\2\0\0\]
```

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

Timeline Explorer v2.1.0

File Tools Tabs View Help

ShellBags.txt

Drag a column header here to group by that column

Enter text to search... Find

shellbags v.20200428

(USRCCLASS.DAT) Shell\Bag\MRU traversal in Win7+ USRCCLASS.DAT hives

MRU Time	Modified	Accessed	Created	Zip_Subfolder	NFT File Ref	Resource
						My Games [Desktop\0\]
						My Computer [Desktop\1\]
						My Computer\0\ [Desktop\1\0\]
						My Computer\CLSID_Downloads [Desktop\1\1\]
2025-10-10 17:14:24						My Computer\C:\ [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-92703aca00af} [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\]

C:\Users\NIZAR\Desktop\ShellBags.txt

Total lines 18 | Visible lines 18 | Open files: 1 | Search options

ENG US 8:59 PM 11/20/2025

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