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**

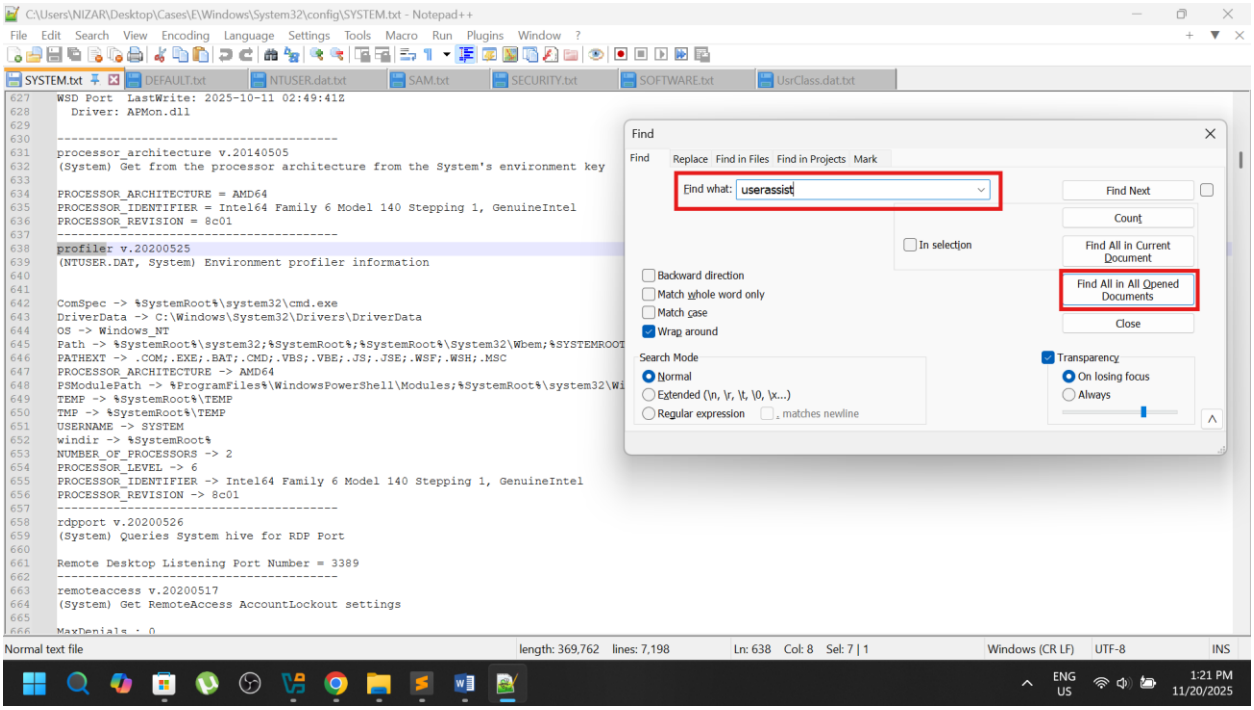
1. UserAssist Analysis

What is UserAssist ?

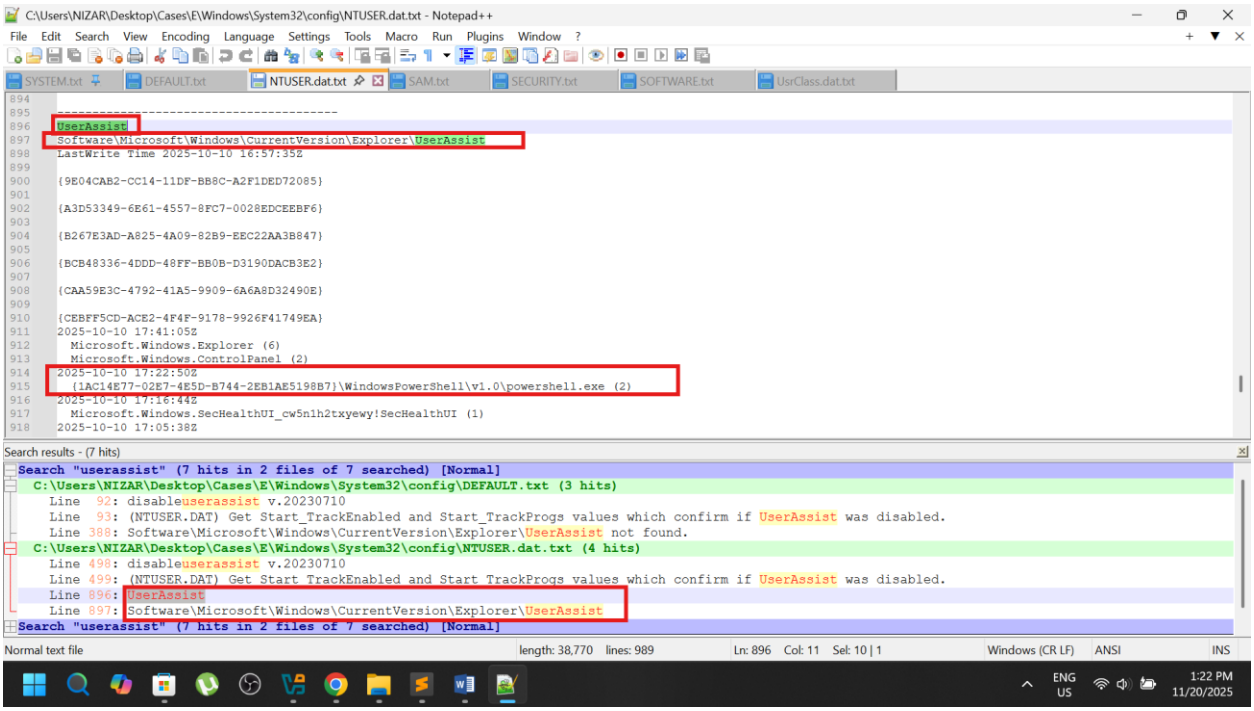
Tracks applications executed by the user, including **timestamps** and **frequency counts**.

Registry Location :

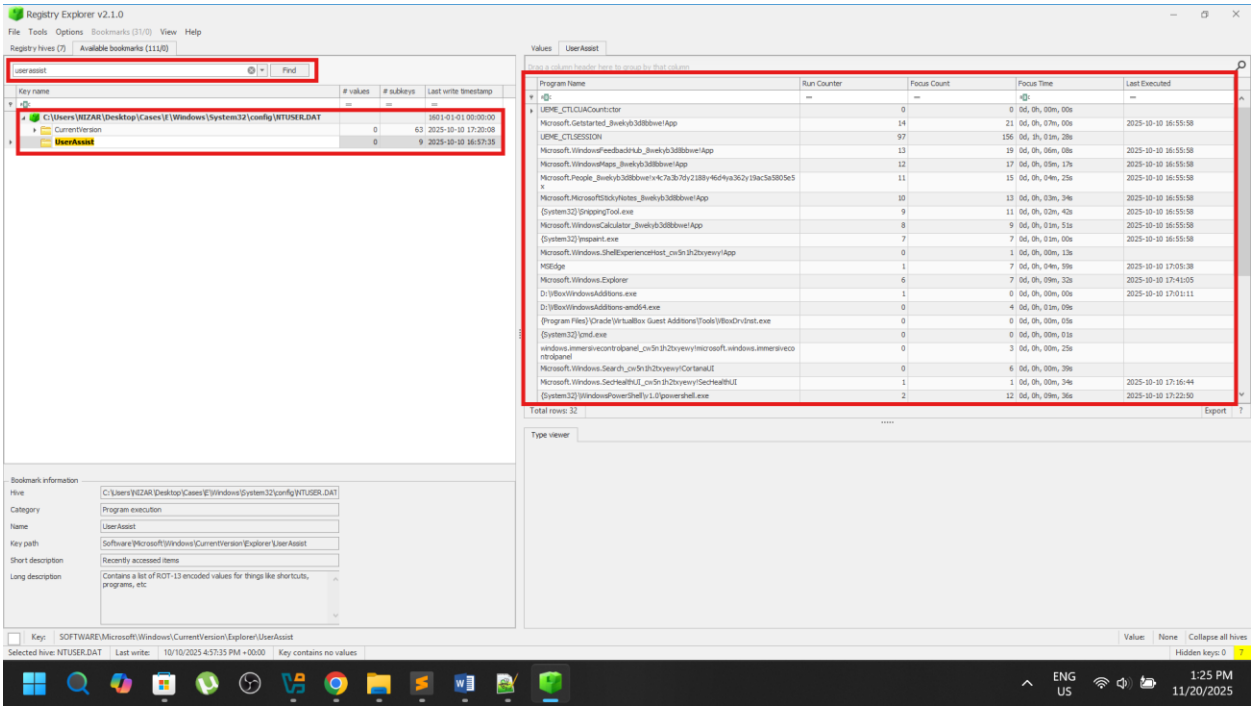
⇨ Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist



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

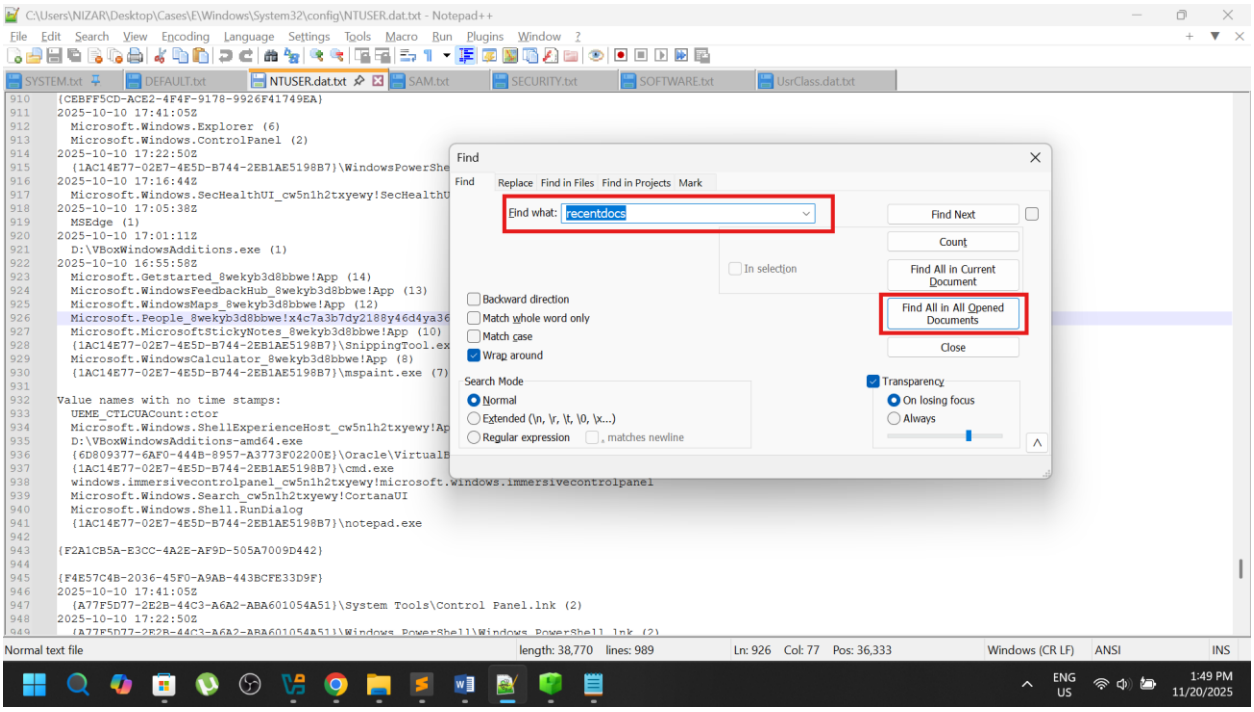
2. RecentDocs Analysis

What is RecentDocs ?

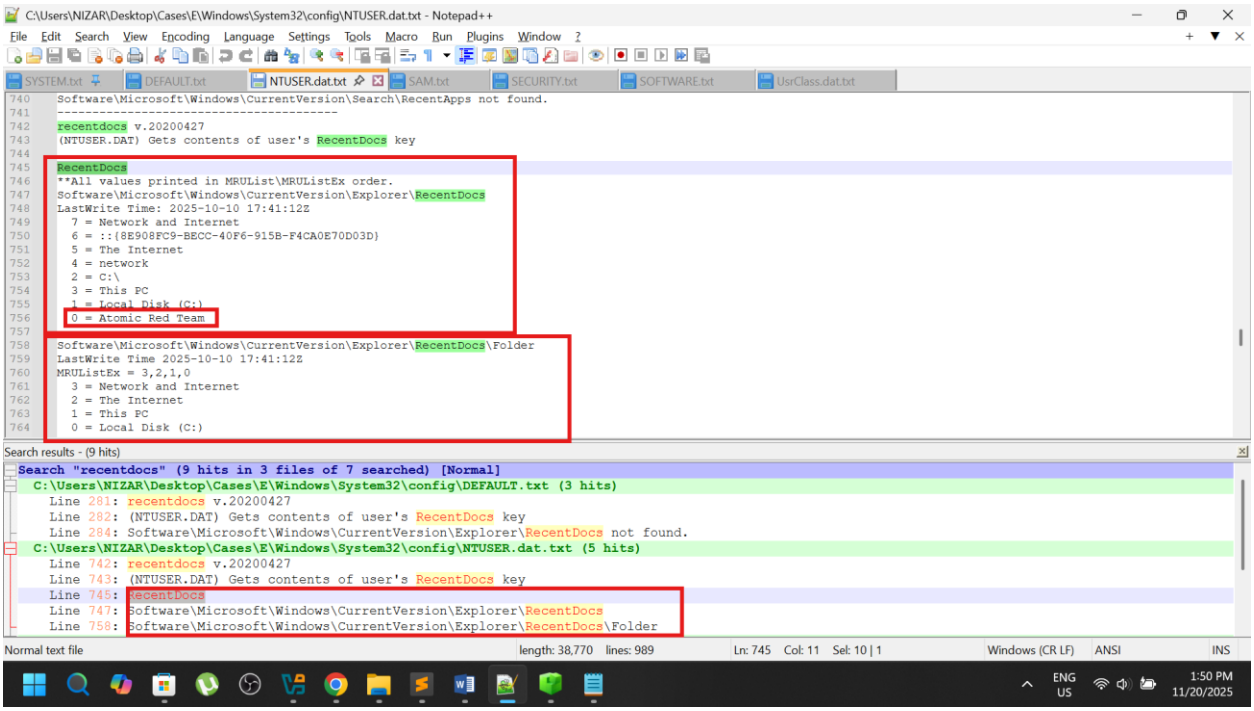
Tracks recently accessed files, folders, and locations in Windows Explorer, showing **user file browsing habits and accessed resources.**

Registry Location :

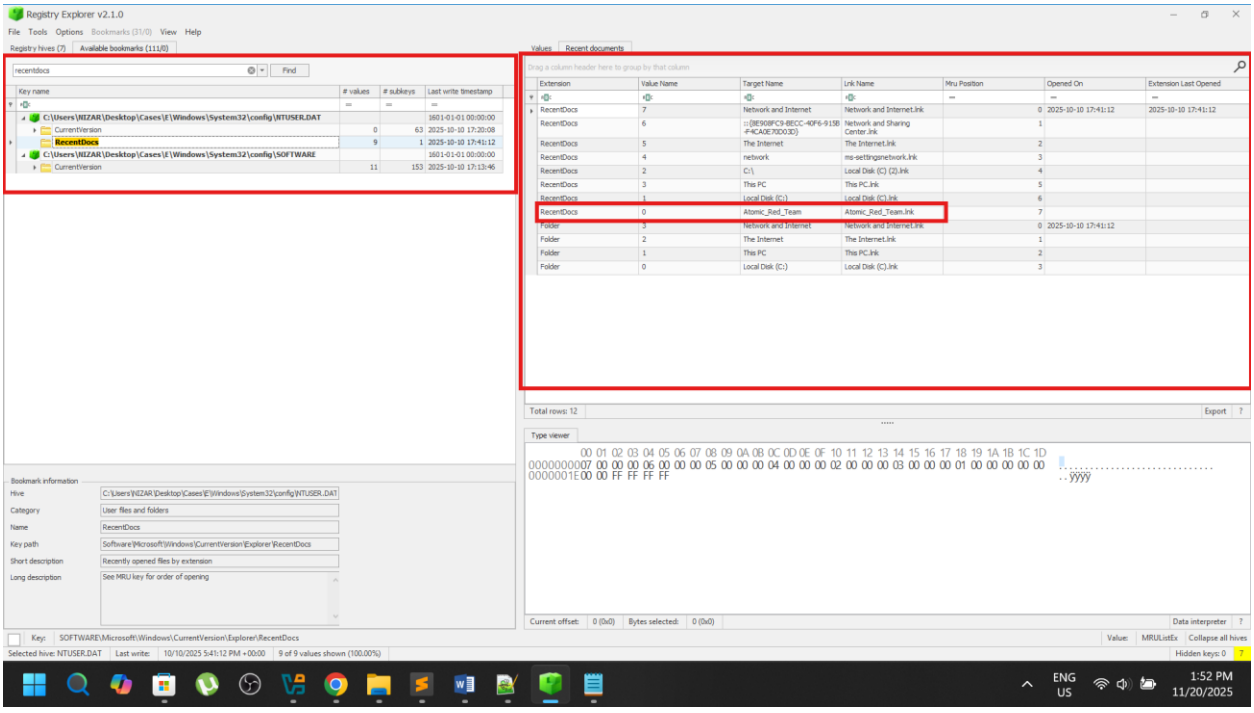
⇨ Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



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



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



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

RecentDocs Analysis Results

Recent Documents (Main Key)

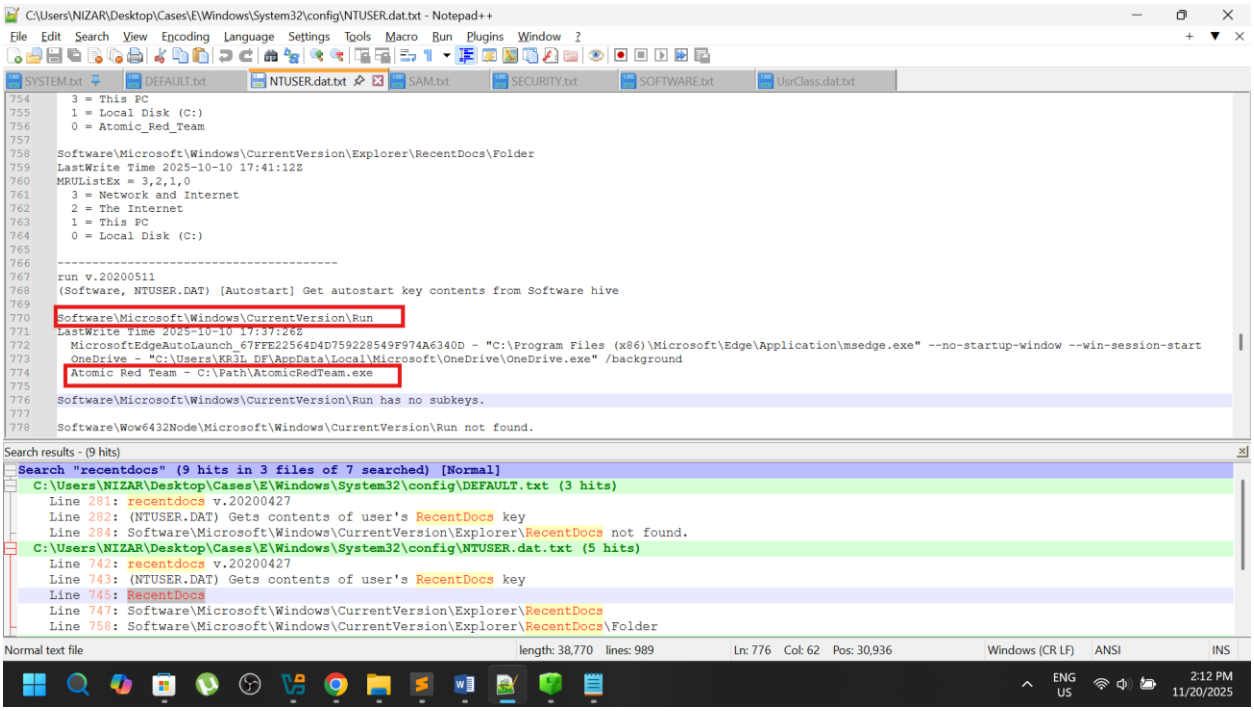
- **LastWrite Time:** 2025-10-10 17:41:12Z
- **Network and Internet** - Network settings access
- **The Internet** - Web browsing activity
- **network** - Network location browsing
- ****C:**** - Root directory access
- **This PC** - Computer management
- **Local Disk (C:)** - Primary drive navigation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



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

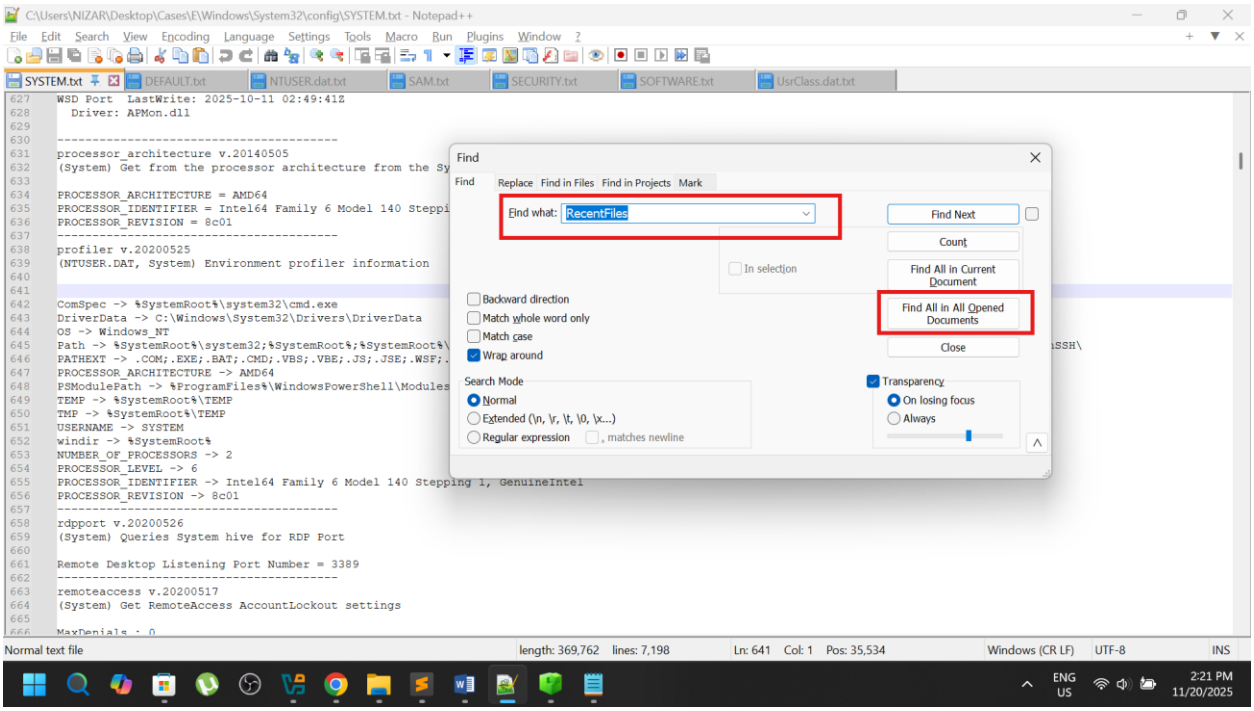
3. Open/Save MRU Analysis

What is Open/Save MRU?

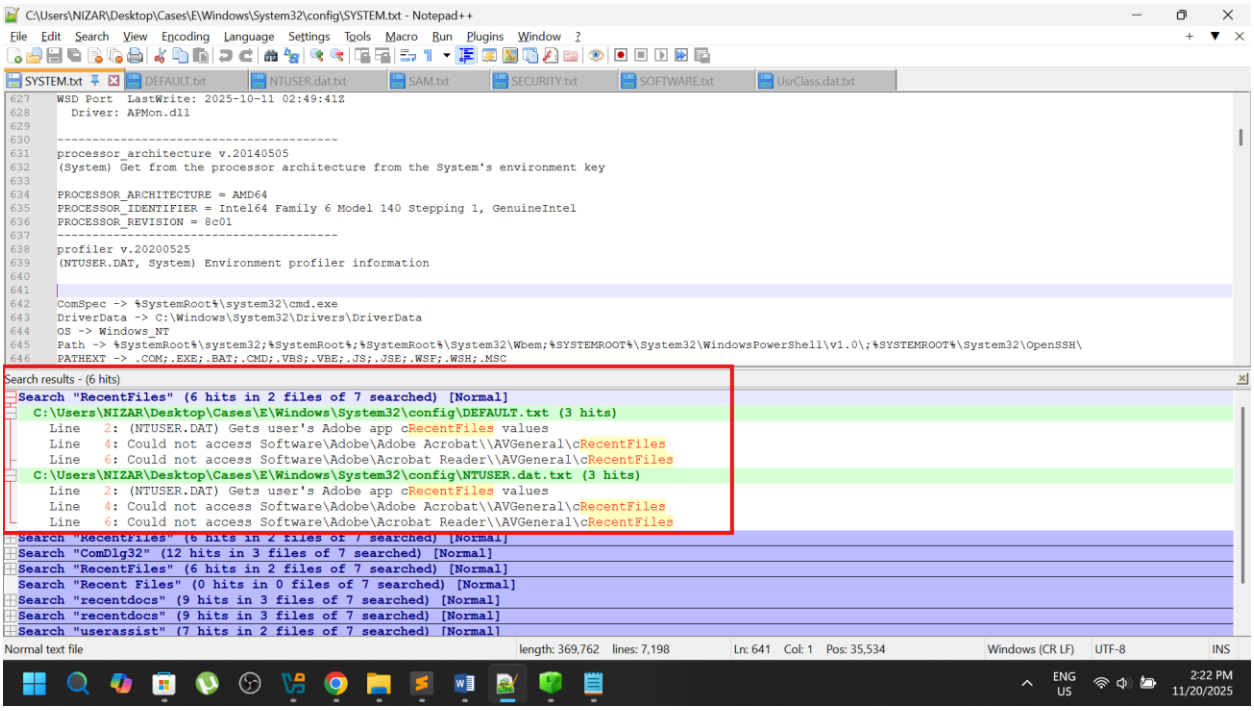
Tracks files recently opened or saved within specific applications (not Windows Explorer), showing document workflow and application usage patterns.

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)

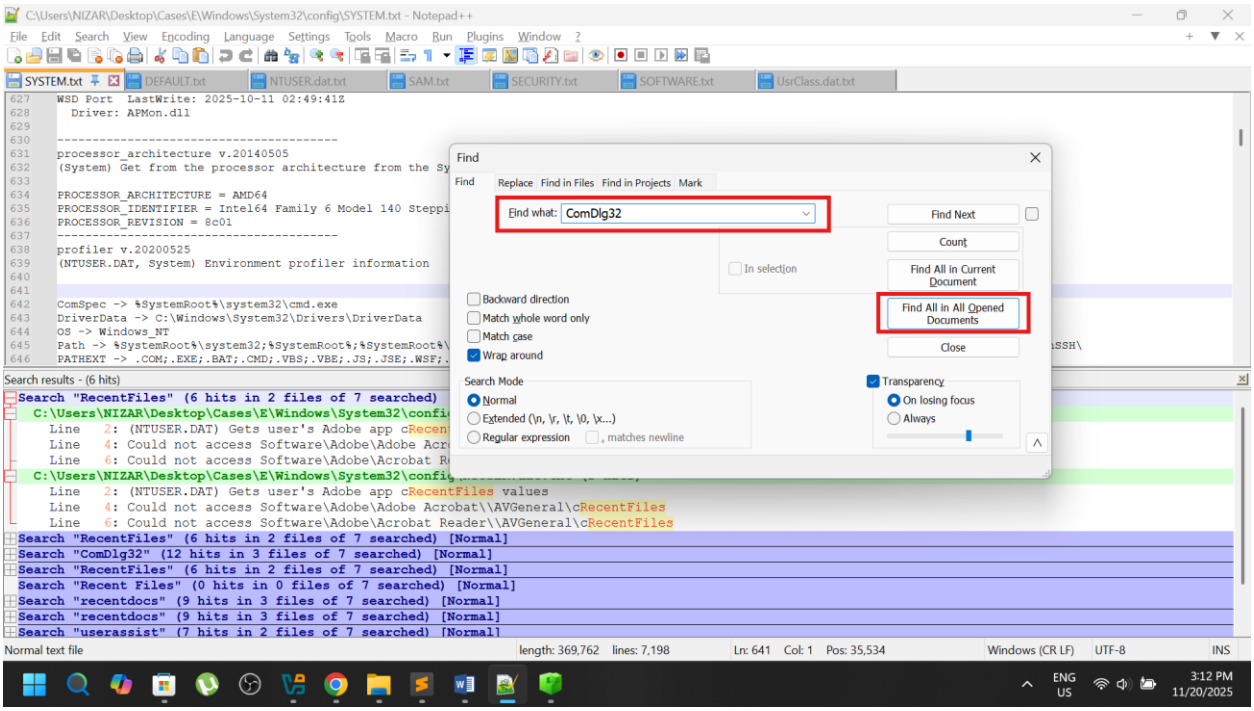
4. Last-Visited MRU Analysis

What is Last-Visited MRU ?

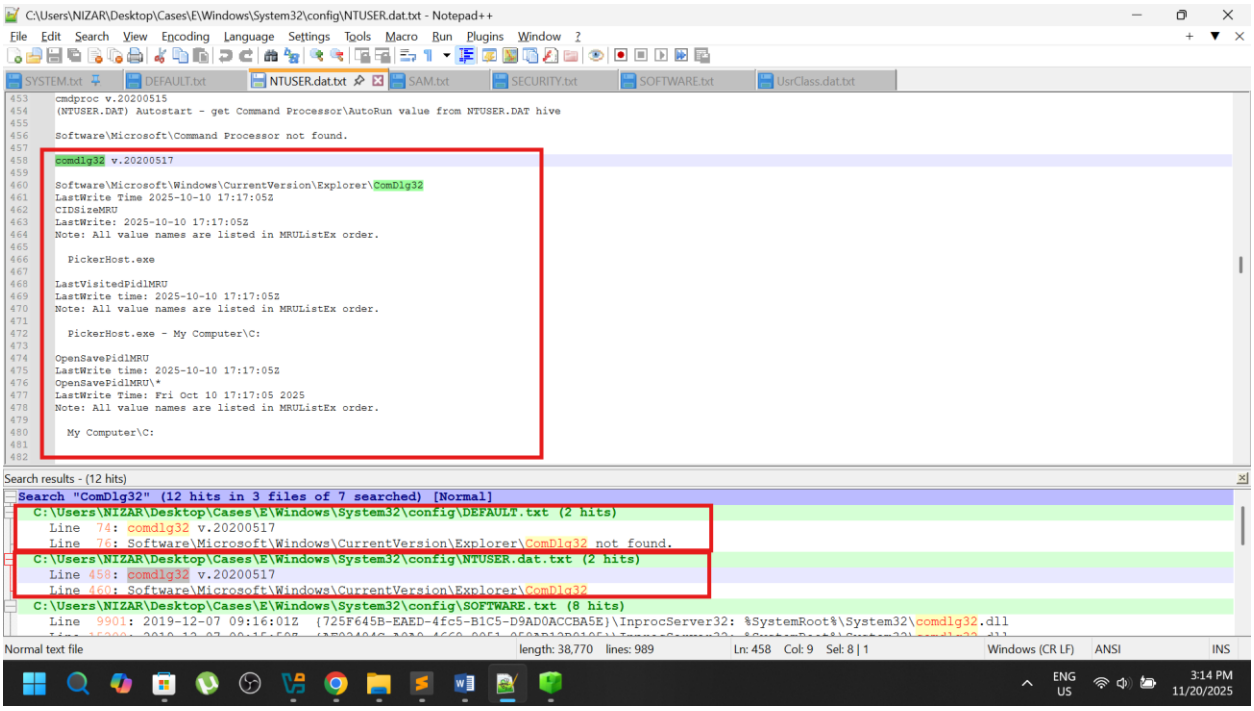
Tracks which applications were last used to open specific file types, showing file **association preferences** and **application usage patterns.**

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 :

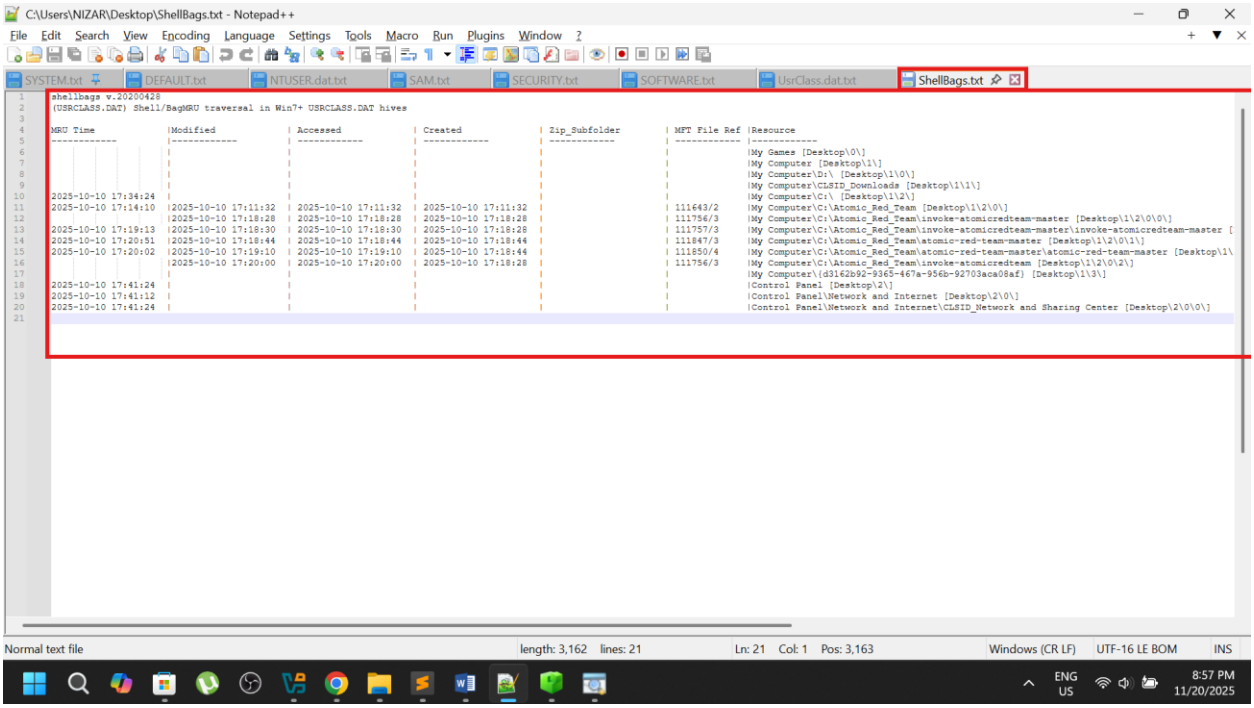
- ⇨ HKCU\Software\Microsoft\Windows\Shell\Bags
- ⇨ HKCU\Software\Microsoft\Windows\Shell\BagMRU
- ⇨ HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

Analysis Method

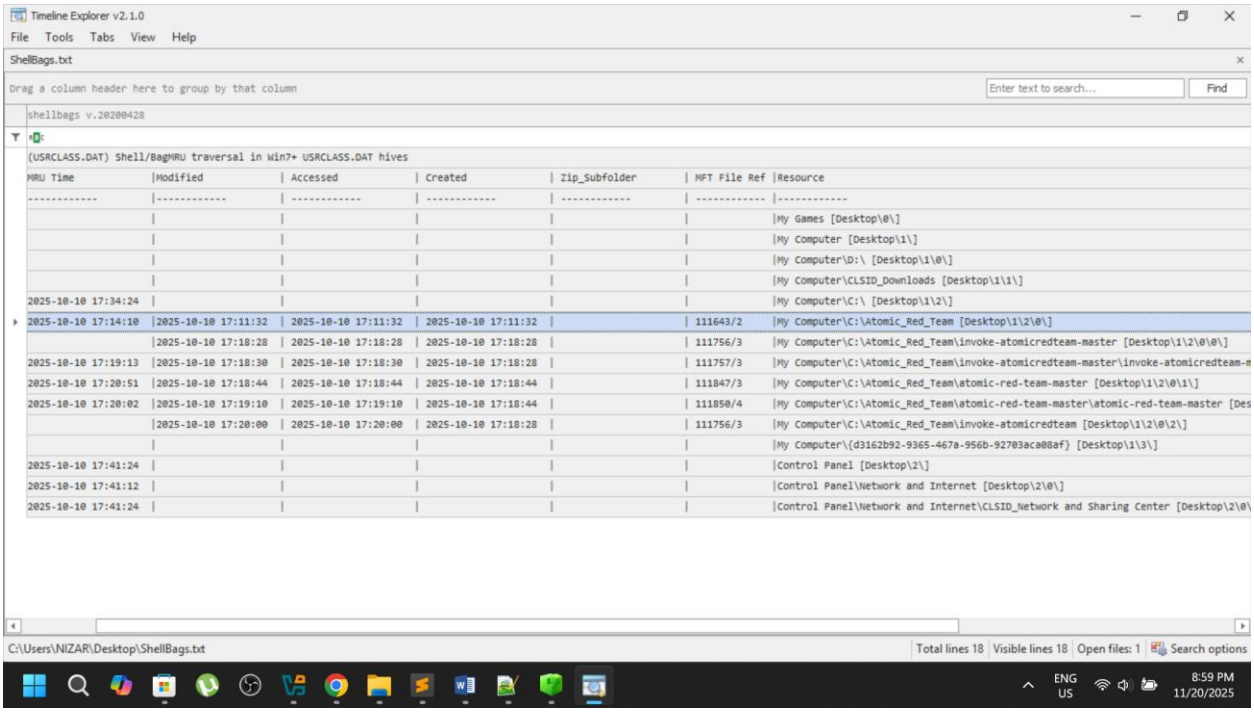
We'll use **RegRipper** to parse **Shellbags** from the **USRCLASS.DAT hive:**

- ⇨ **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**.



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



***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