# Windows Registry Forensics

**Thomas Benos**

MSc UniWA, Cisco CyberOps
GR CSIRT Incident Responder
thomasbenos1291@gmail.com

# Agenda

- Introduction to Windows Registry
- Registry Structure
- Tools for Registry Acquisition & Analysis
- Security Registry File
- System Info & User Accounts
- Usage of Files/Folders
- Evidence of Execution
- External Device/USB Forensics

# Introduction to Windows Registry

# What is Windows Registry?


- The registry is a hierarchical database that contains data that is critical for the operation of Windows and the applications and services that run on Windows. The data is structured in a tree format. Each node in the tree is called a key. Each key can contain both subkeys and data entries called values. A key can have any number of values, and the values can be in any form.
- Sources:
  - *https://learn.microsoft.com/en-us/windows/win32/sysinfo/structure-of-the-registry*
  - *http://support.microsoft.com/kb/256986*

# What is Windows Registry?

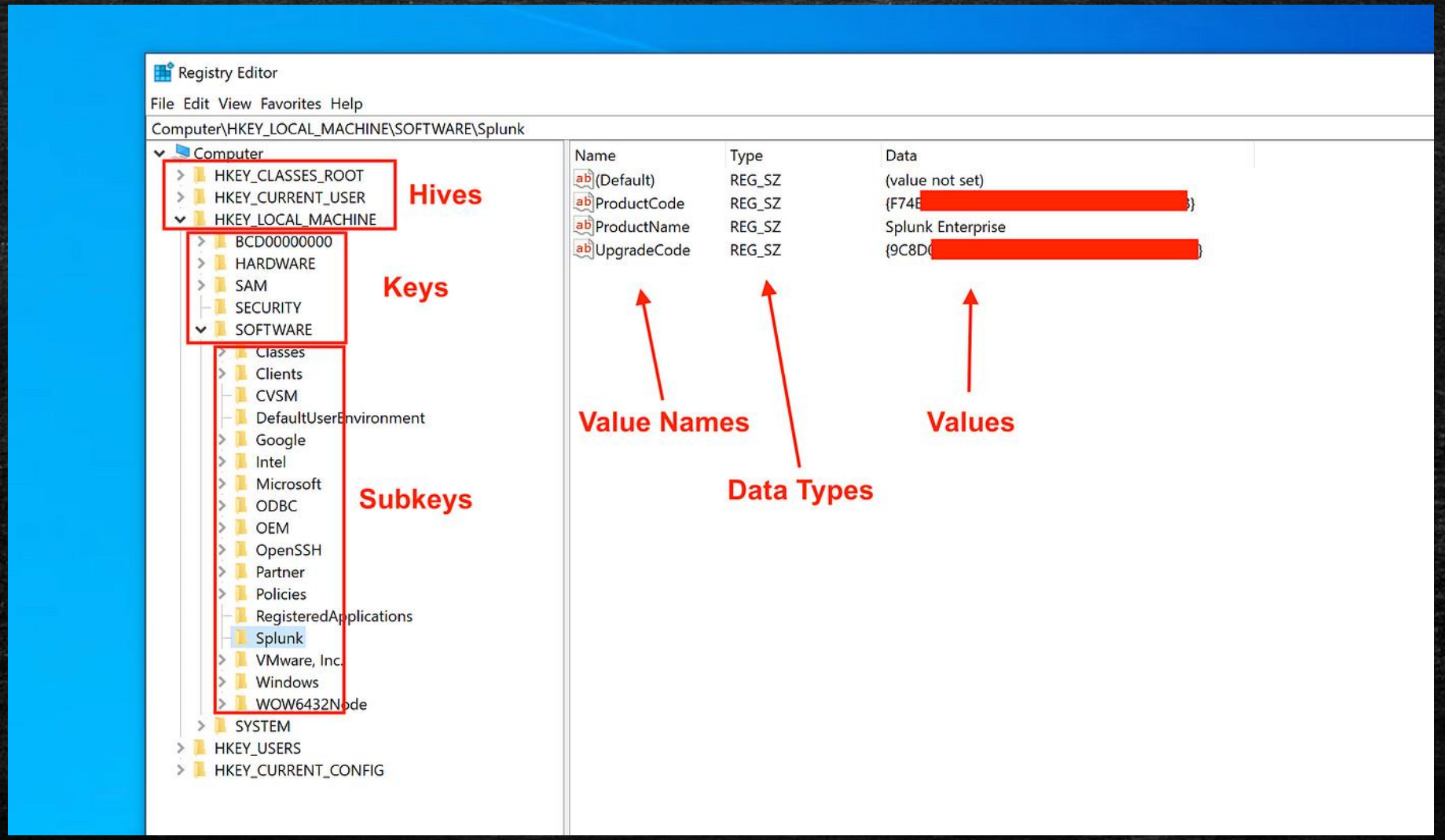
- Core Component: Centralized, Hierarchical, configuration Database
- Configuration Information
  - ✓ User Activity
  - ✓ Applications Installed, configurations and opened files
  - ✓ User Names
  - ✓ Computer Names
  - ✓ Last shutdown
  - ✓ Startup application
  - ✓ Browser data, Start Page
  - ✓ USB and Appliances
  - ✓ Wireless or not Networks
  - ✓ Passwords
  - ✓ Application specific information
  - ✓ e.t.c

# Windows Registry Attack Impact

- ✓ Alter or disable File System Metadata
- ✓ Modify System Crash Dump, Prefetcher, and System Restore
- ✓ Clear the page file when the system is shut down
- ✓ Enable or disable Event log auditing
- ✓ Enable or disable the Windows firewall

# Registry Structure

# Registry Hierarchical Structure



# Registry Hives / Root Keys

- **HKEY_CLASSES_ROOT (HKCR)** → SymLink to HKEY_LOCAL_MACHINE \ SOFTWARE \Classes.
  - Class registration and file name extension information
- **HKEY_CURRENT_USER (HKCU)** → SymLink to a key under HKEY_USERS
  - Volatile - Current User Configuration.
- **HKEY_LOCAL_MACHINE (HKLM)** → Placeholder
  - System Configuration.
  - HKLM/Hardware -> Volatile
- **HKEY_CURRENT_CONFIG (HKCC)** → SymLink to HKEY_LOCAL_MACHINE \ SYSTEM CurrentControlSet\ Control\IDConfigDB\Hardware
  - Hardware Configuration on Boot.
- **HKEY_USERS (HKU)** → Placeholder
  - All Users Profile Configurations.

# Registry Files

- The Windows registry is stored in a series of files. Registry files store the Registry data persistently. They are loaded into memory when the operating system starts, and changes are periodically written back to these files.
- General system information (C:\Windows\System32\config)
  - DEFAULT (mounted on HKEY_USERS\DEFAULT)
  - SAM (mounted on HKEY_LOCAL_MACHINE\SAM)
  - SECURITY (mounted on HKEY_LOCAL_MACHINE\Security)
  - SOFTWARE (mounted on HKEY_LOCAL_MACHINE\Software)
  - SYSTEM (mounted on HKEY_LOCAL_MACHINE\System)
- User information
  - NTUSER.DAT (mounted on HKEY_CURRENT_USER when a user logs in)
    - C:\Users\<username>\
  - USRCLASS.DAT (mounted on HKEY_CURRENT_USER\Software\CLASSES)
    - C:\Users\<username>\AppData\Local\Microsoft\Windows

# Registry Files

| File name | Path | Details |
|---|---|---|
| Ntuser.dat (for every user) | C:\Users\{USER_NAME}\NTUSER.DAT | Protected area for the user.<br>User's most recently used files (MRU).<br>Personal settings |
| Default | C:\Windows\system32\config\DEFAULT | System settings |
| SAM | C:\Windows\system32\config\SAM | User account management and security settings (passwords) |
| Security | C:\Windows\system32\config\SECURITY | System settings |
| Software | C:\Windows\system32\config\SOFTWARE | Installed software and configuration |
| System | C:\Windows\system32\config\SYSTEM | System settings |
| USRCLASS.dat | C:\Users\{USER_NAME}AppData\Local\Microsoft\Windows\USRCLASS.DAT | Information about the user's actions |
| BCD (C:\Boot) | C:\Boot\BCD | Boot configuration data |
| Amcache | C:\Windows\AppCompat\Programs | Internal Application Compatibility |

# Registry Files

- Registry Files consist of:
  - Primary files
  - Transaction log files
    - Every hive has a number of transaction log files: .LOG, which holds the changes and then passes them to the primary file.
    - e.g SECURITY.LOG, SECURITY.LOG1, SECURITY.LOG2
    - If changes are not passed to main hive -> hive is **dirty**
  - Backup copies of primary files (every 10 days)

# Registry Files

- **Windows 10: System hive Primary file:**
  - C:\Windows\System32\config\SYSTEM
- **Transaction log files:**
  - C:\Windows\System32\config\SYSTEM.LOG
  - C:\Windows\System32\config\SYSTEM.LOG1
  - C:\Windows\System32\config\SYSTEM.LOG2
- **Backup copy of a primary file:**
  - C:\Windows\System32\config\RegBack\SYSTEM

# Registry Value Data Types

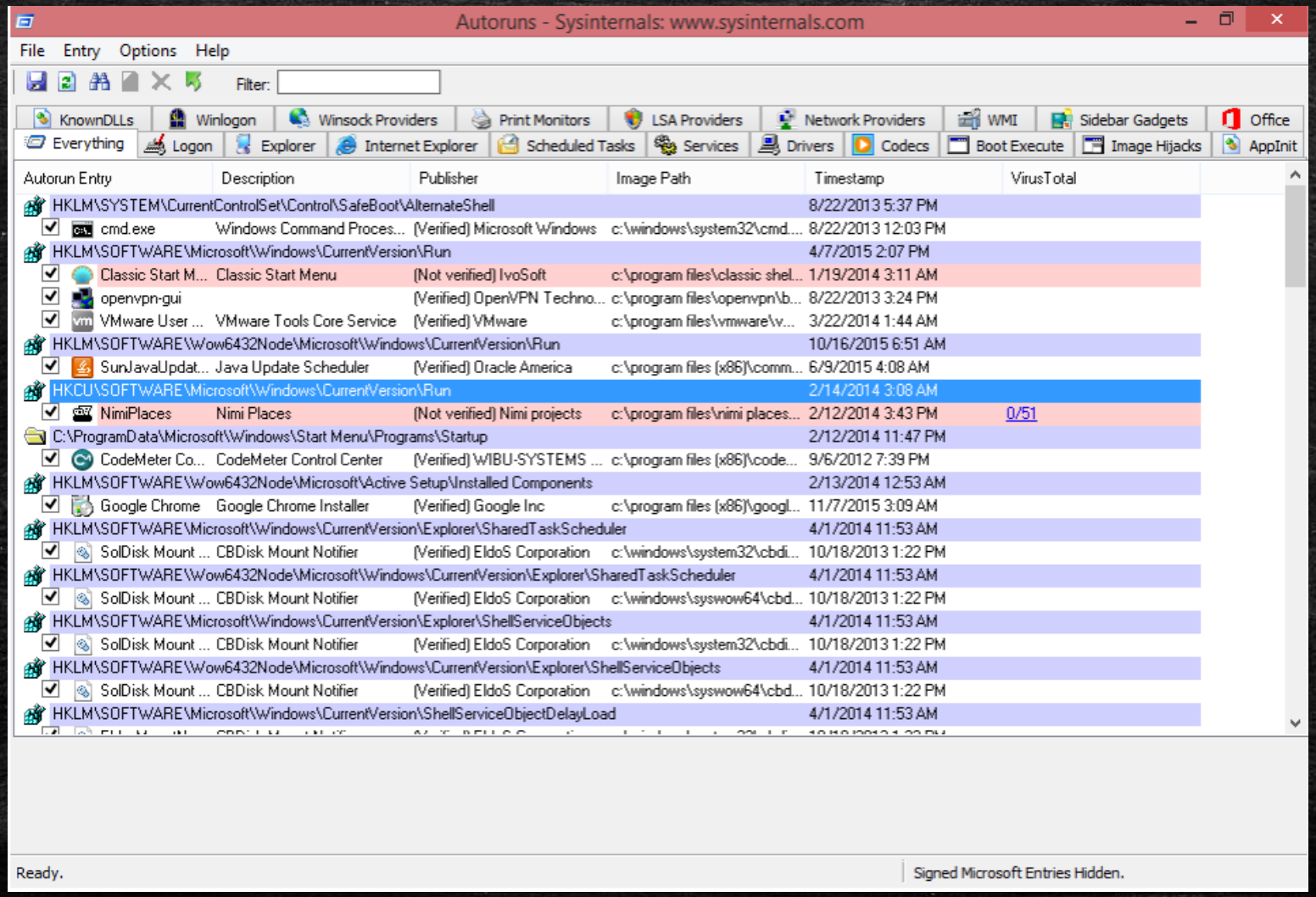
| Data Type | Explanation |
|---|---|
| REG_BINARY | Binary data in any form. |
| REG_DWORD | A 32 bit number. |
| REG_DWORD_LITTLE_ENDIAN | A 32 bit number in little endian format. |
| REG_DWORD_BIG_ENDIAN | A 32 bit number in big endian format. |
| REG_EXPAND_SZ | A null-terminated string that contains unexpanded references to environment variables. |
| REG_LINK | A null-terminated Unicode string that contains the target path of a symbolic link that was created by calling the RegCreateKeyEx function with REG_OPTION_CREATE_LINK |
| REG_MULTI_SZ | A sequence of null-terminated strings, terminated by an empty string. |
| REG_NONE | No defined value type. |
| REG_QWORD | A 64-bit number. |
| REG_QWORD_LITTLE_ENDIAN | A 64-bit number in little endian format. |
| REG_SZ | A null-terminated string (Unicode or ANSI). |

# Tools for Registry Acquisition & Analysis

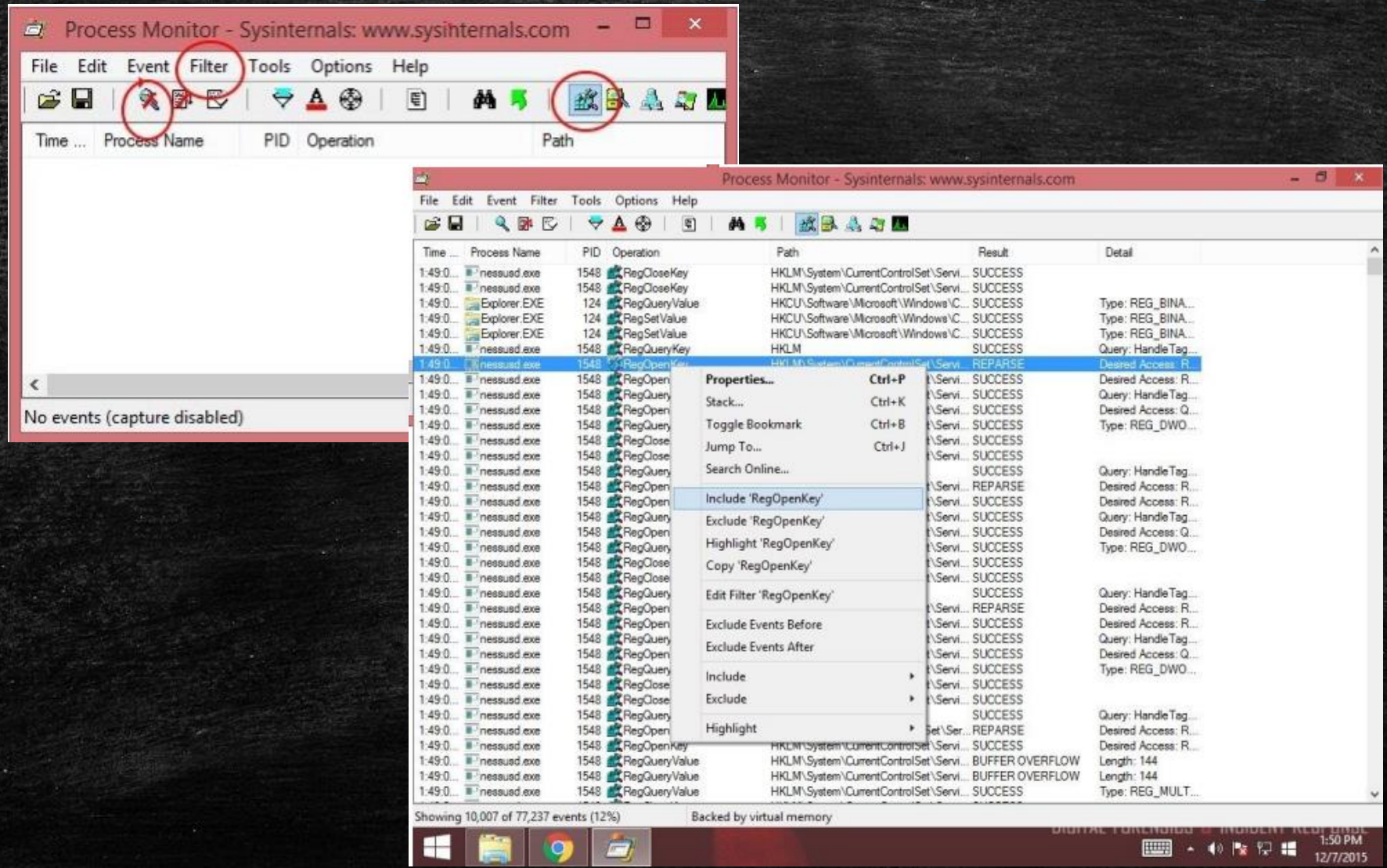
# Tools for Registry

- reg.exe
  - *Reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run*
- regedit
- Autoruns (SysInternals)
- Procmon.exe (SysInternals)
- FTK Imager
- Velociraptor
- DCode
- AccessData Registry Viewer
- **RegRipper**
- **Registry Explorer (Zimmerman Tools)**
- **Autopsy**

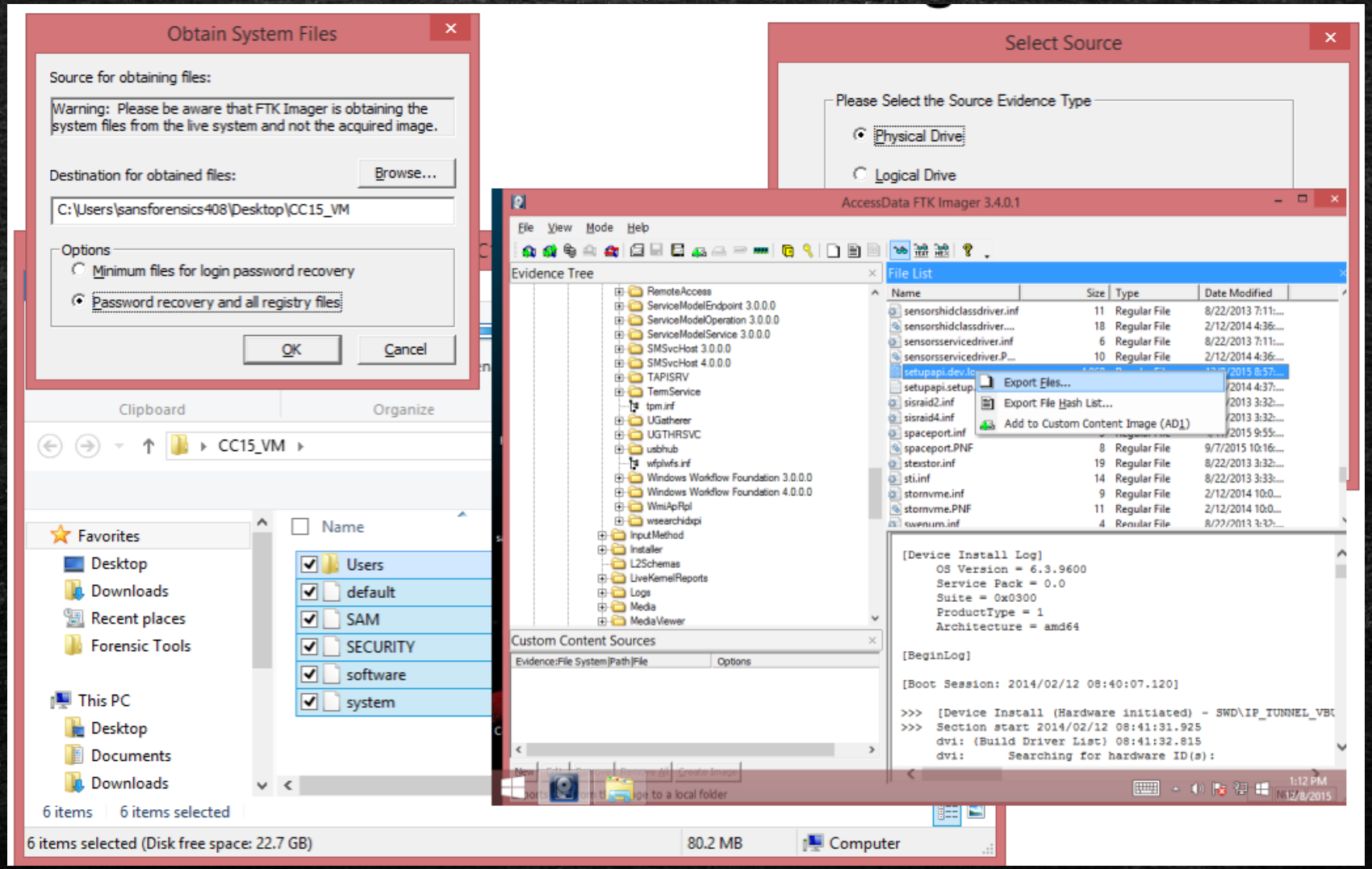
# Tools - Autoruns



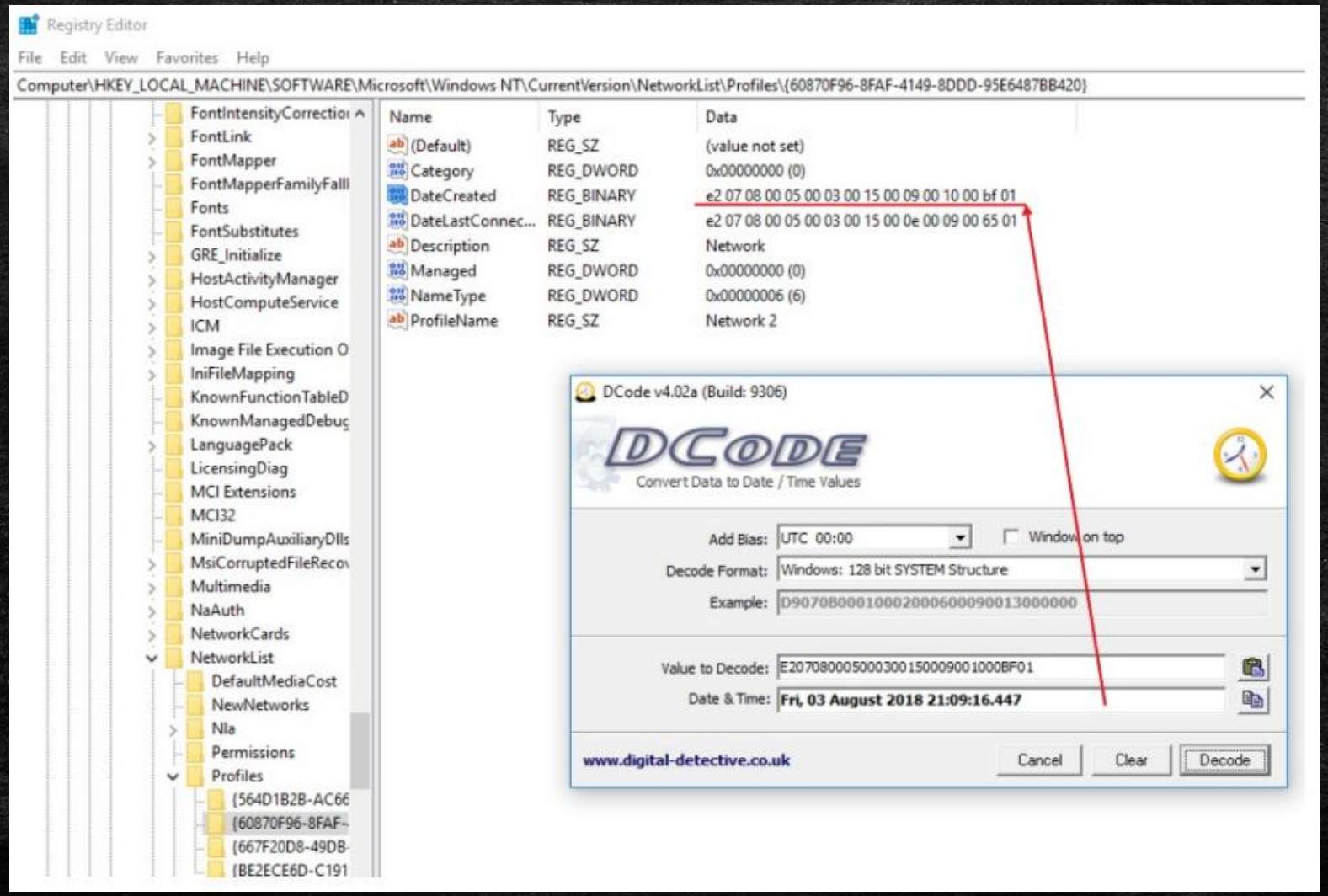
# Tools - Procmon



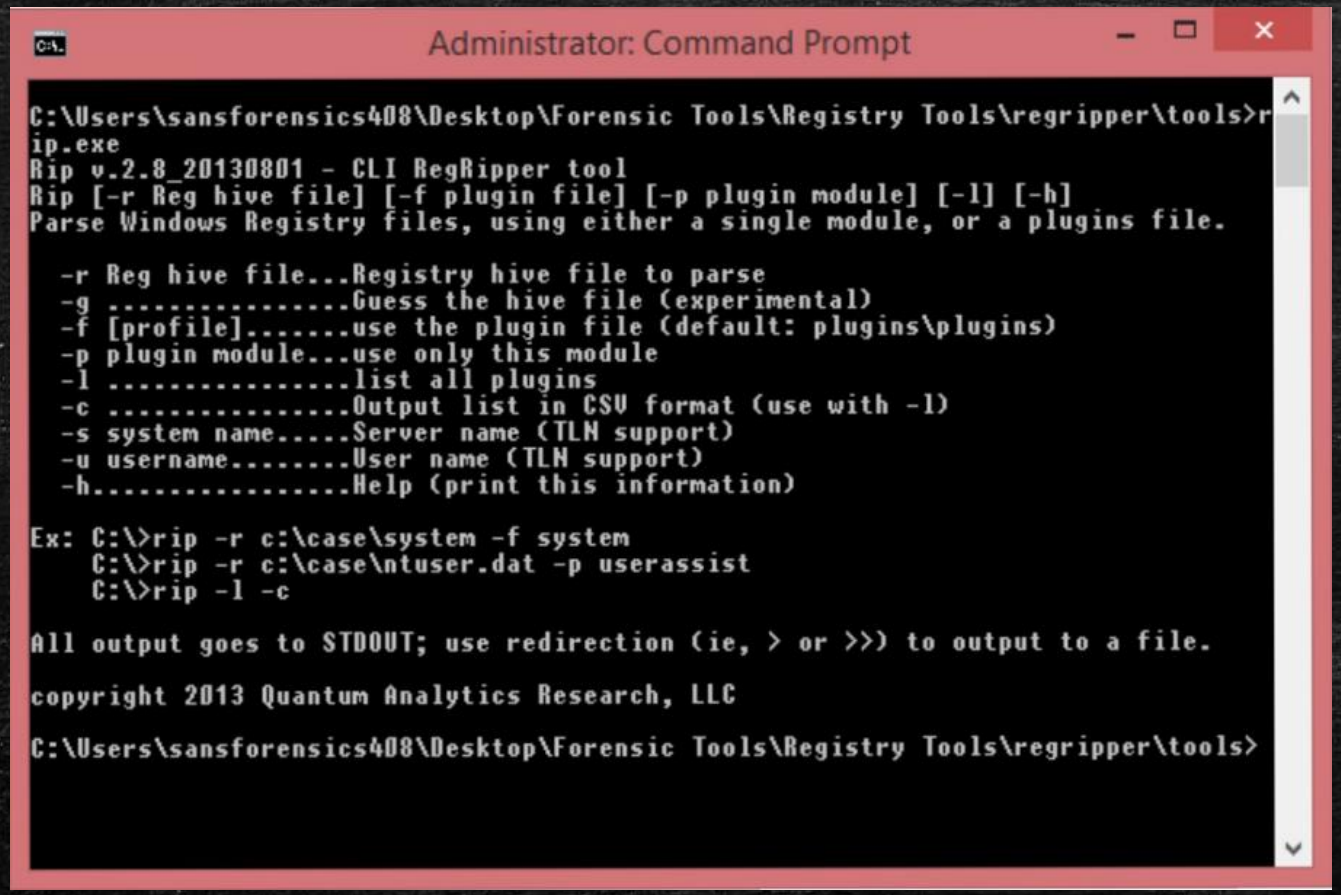
# Tools – FTK Imager

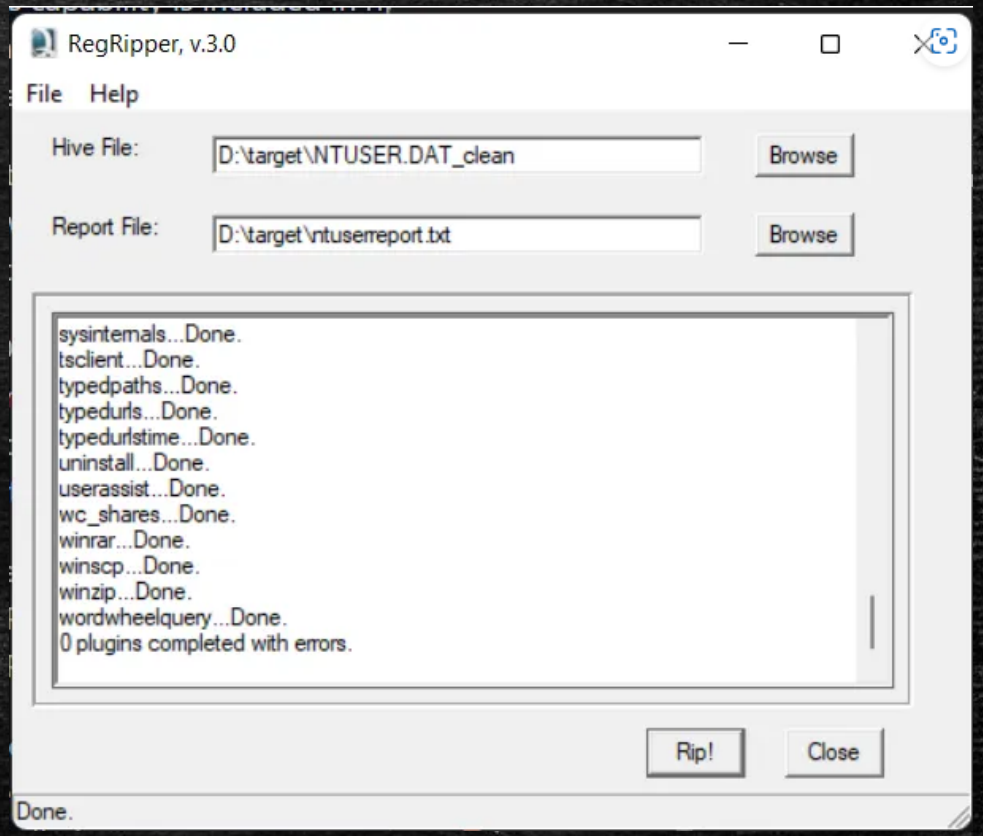


# Tools – DCode

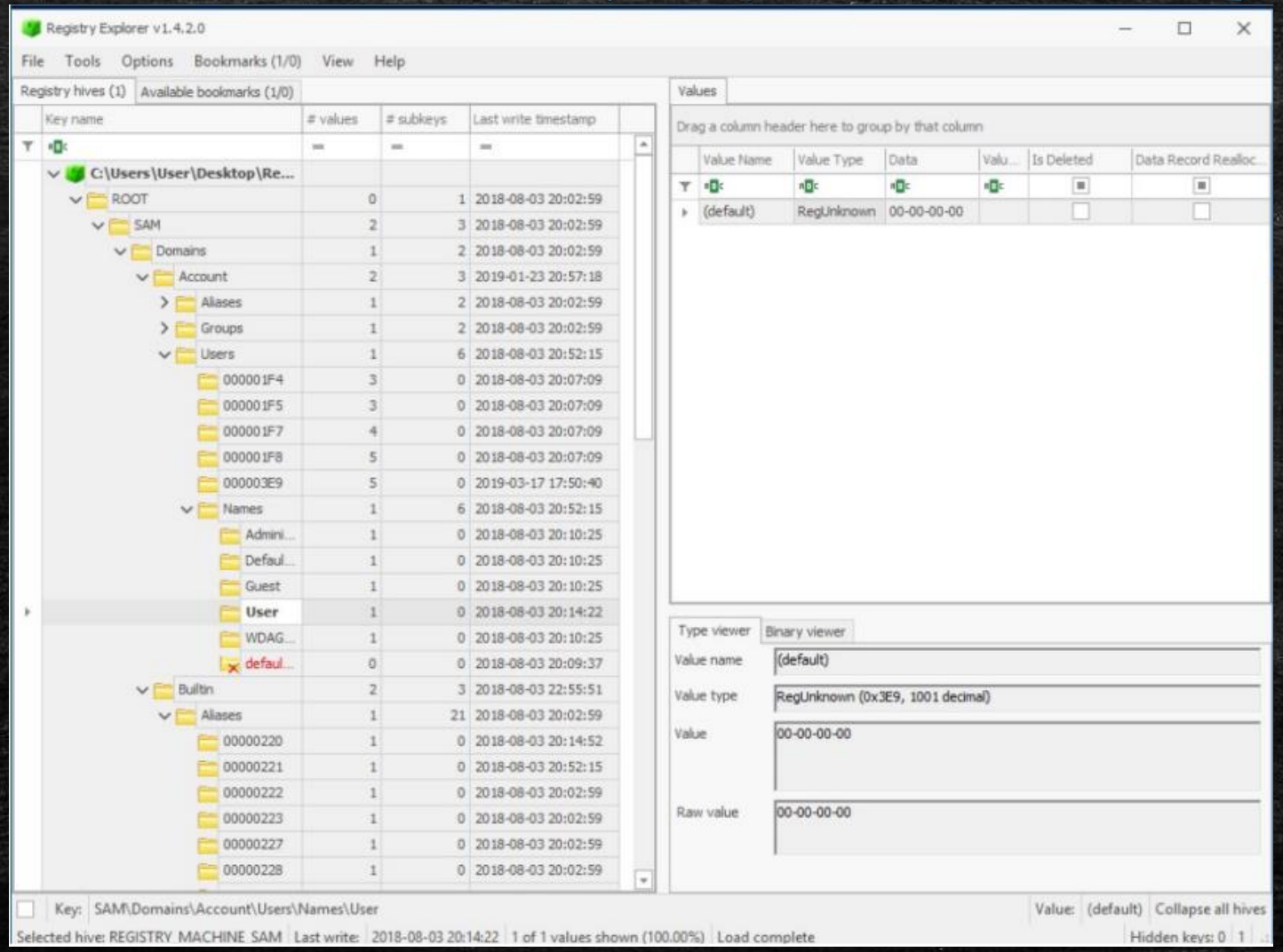

Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{60870F96-8FAF-4149-8DDD-95E6487BB420}
FontIntensityCorrectio
FontLink
FontMapper
FontMapperFamilyFallI
Fonts
FontSubstitutes
GRE_Initialize
HostActivityManager
HostComputeService
ICM
Image File Execution O
IniFileMapping
KnownFunctionTableD
KnownManagedDebug
LanguagePack
LicensingDiag
MCI Extensions
MCI32
MiniDumpAuxiliaryDlls
MsiCorruptedFileReco
Multimedia
NaAuth
NetworkCards
NetworkList
DefaultMediaCost
NewNetworks
Nla
Permissions
Profiles
{564D1B2B-AC66
{60870F96-8FAF-
{667F20D8-49DB-
{BE2ECE6D-C191
Name Type Data
(Default) REG_SZ (value not set)
Category REG_DWORD 0x00000000 (0)
DateCreated REG_BINARY e2 07 08 00 05 00 03 00 15 00 09 00 10 00 bf 01
DateLastConnec... REG_BINARY e2 07 08 00 05 00 03 00 15 00 0e 00 09 00 65 01
Description REG_SZ Network
Managed REG_DWORD 0x00000000 (0)
NameType REG_DWORD 0x00000006 (6)
ProfileName REG_SZ Network 2
DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values
Add Bias: UTC 00:00
Window on top
Decode Format: Windows: 128 bit SYSTEM Structure
Example: D9070B0001000200060009001300000
Value to Decode: E2070800050003001500090010008F01
Date & Time: Fri, 03 August 2018 21:09:16.447
www.digital-detective.co.uk
Cancel
Clear
Decode

# Tools – RegRipper



# Tools – Registry Explorer



# Security Hive File

# Security – System and Domain SIDs

- SECURITY/Policy/Accounts
- S-R-X-Y1-Y2-Yn-1-Yn-RID
  - S: indicates that the string is SID
  - R: indicates the version level
  - X: indicates the identifier authority value
  - Y: represents a series of subauthority values
    - First value (Y1):
      - 21: Domain SID
      - 32: Builtin accounts and groups
  - RID: indicates the relative identifier

# Security – System and Domain SIDs

- S-**1**-**5**-**21**-1004336348-1177238915-682003330-**512**
  - 1 – Revision level
  - 5 – Identifier Authority (SECURITY_NT_AUTHORITY)
  - **21**-1004336348-1177238915-682003330 – domain identifier
  - 512 – Relative Identifier (Domain Admins).

- Well known identifier authorities:
  - S-1-0: SECURITY_NULL_SID_AUTHORITY
  - S-1-1: SECURITY_WORLD_SID_AUTHORITY
  - S-1-2: SECURITY_LOCAL_SID_AUTHORITY
  - S-1-3: SECURITY_CREATOR_SID_AUTHORITY
  - S-1-5: SECURITY_NT_AUTHORITY

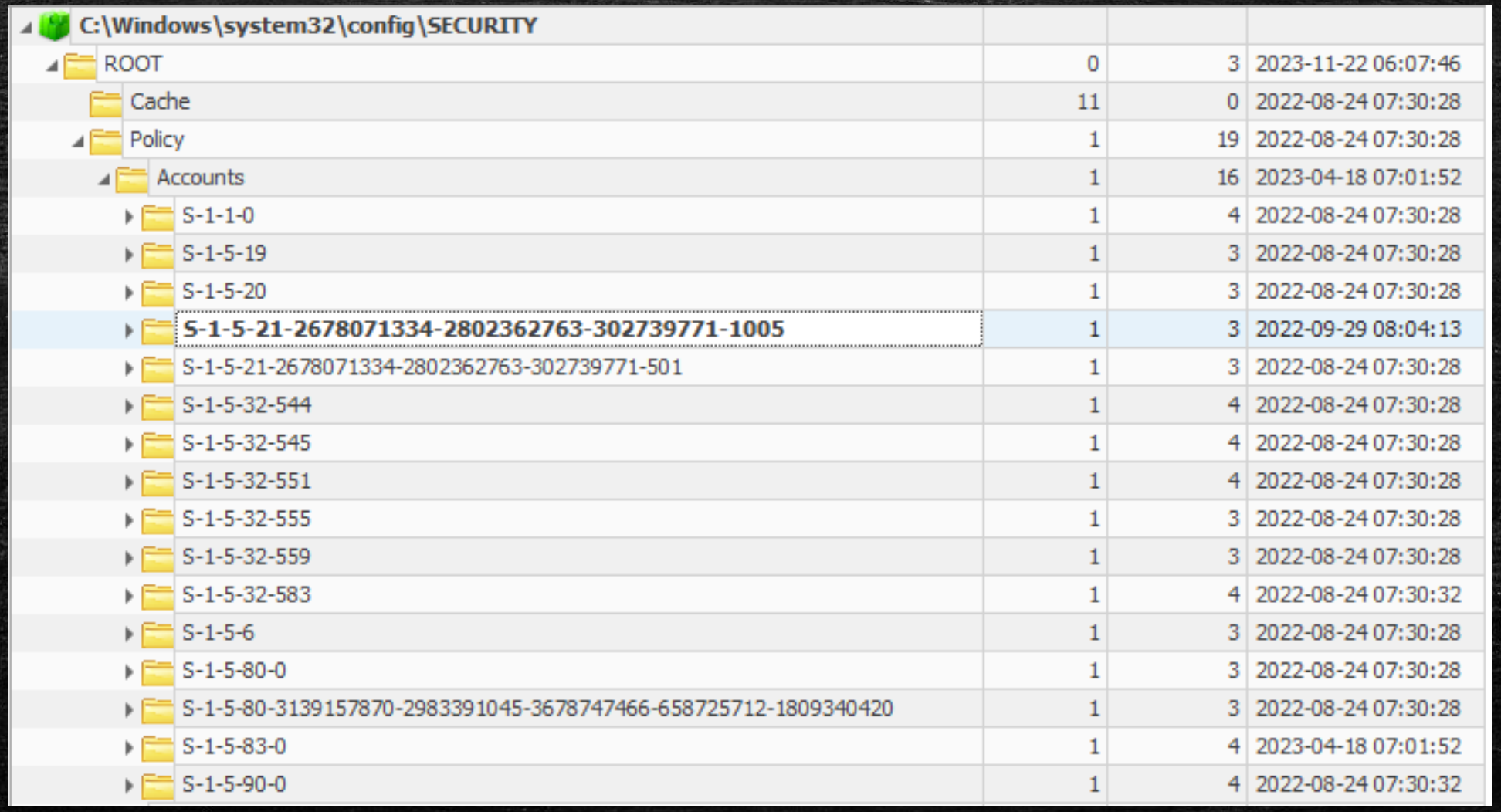
# Security – Well Known SIDs

| SID | Name | Description |
|---|---|---|
| S-1-0-0 | Nobody | No security principal. |
| S-1-1-0 | Everyone | A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system. |
| S-1-2-0 | Local | A group that includes all users who have logged on locally. |
| S-1-5-2 | Network | A group that includes all users that have logged on through a network connection. Membership is controlled by the operating system. |
| S-1-5-4 | Interactive | A group that includes all users that have logged on interactively. Membership is controlled by the operating system. |
| S-1-5-6 | Service | A group that includes all security principals that have logged on as a service. Membership is controlled by the operating system. |
| S-1-5-9 | Enterprise Domain Controllers | A group that includes all domain controllers in a forest that uses an Active Directory directory service. Membership is controlled by the operating system. |
| S-1-5-19 | NT Authority | Local Service |
| S-1-5-20 | NT Authority | Network Service |
| S-1-5-21-(any) | | Domain Account |
| S-1-5-32-(any) | | Builtin Users/Groups |
| S-1-5-80-0 | All Services | A group that includes all service processes configured on the system. Membership is controlled by the operating system. |

# Security – RIDs

- **Domain Users (21-…-…)**
  - DOMAINNAME\Administrator – **500**
  - DOMAINNAME\Guest – **501**
  - DOMAINNAME\Domain Admins – **512**
  - DOMAINNAME\Domain Users – **513**
  - DOMAINNAME\Domain Guests – **514**
- **Builtin Users and Groups (32-…-…)**
  - BUILTIN\Administrators - **544**
  - BUILTIN\Users - **545**
  - BUILTIN\Groups - **546**
  - BUILTIN\Account Operators - **548**
  - BUILTIN\Server Operators - **549**
  - BUILTIN\Print Operators - **550**
  - BUILTIN\Backup Operators - **551**

# Security – System and Domain SIDs



| C:\Windows\system32\config\SECURITY | | | |
|---|---|---|---|
| ROOT | 0 | 3 | 2023-11-22 06:07:46 |
| Cache | 11 | 0 | 2022-08-24 07:30:28 |
| Policy | 1 | 19 | 2022-08-24 07:30:28 |
| Accounts | 1 | 16 | 2023-04-18 07:01:52 |
| S-1-1-0 | 1 | 4 | 2022-08-24 07:30:28 |
| S-1-5-19 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-20 | 1 | 3 | 2022-08-24 07:30:28 |
| **S-1-5-21-2678071334-2802362763-302739771-1005** | 1 | 3 | 2022-09-29 08:04:13 |
| S-1-5-21-2678071334-2802362763-302739771-501 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-32-544 | 1 | 4 | 2022-08-24 07:30:28 |
| S-1-5-32-545 | 1 | 4 | 2022-08-24 07:30:28 |
| S-1-5-32-551 | 1 | 4 | 2022-08-24 07:30:28 |
| S-1-5-32-555 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-32-559 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-32-583 | 1 | 4 | 2022-08-24 07:30:32 |
| S-1-5-6 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-80-0 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420 | 1 | 3 | 2022-08-24 07:30:28 |
| S-1-5-83-0 | 1 | 4 | 2023-04-18 07:01:52 |
| S-1-5-90-0 | 1 | 4 | 2022-08-24 07:30:32 |

# Security – Audit Policy

- SECURITY/Policy/PolAdtEv
  - auditpol /get /category:*

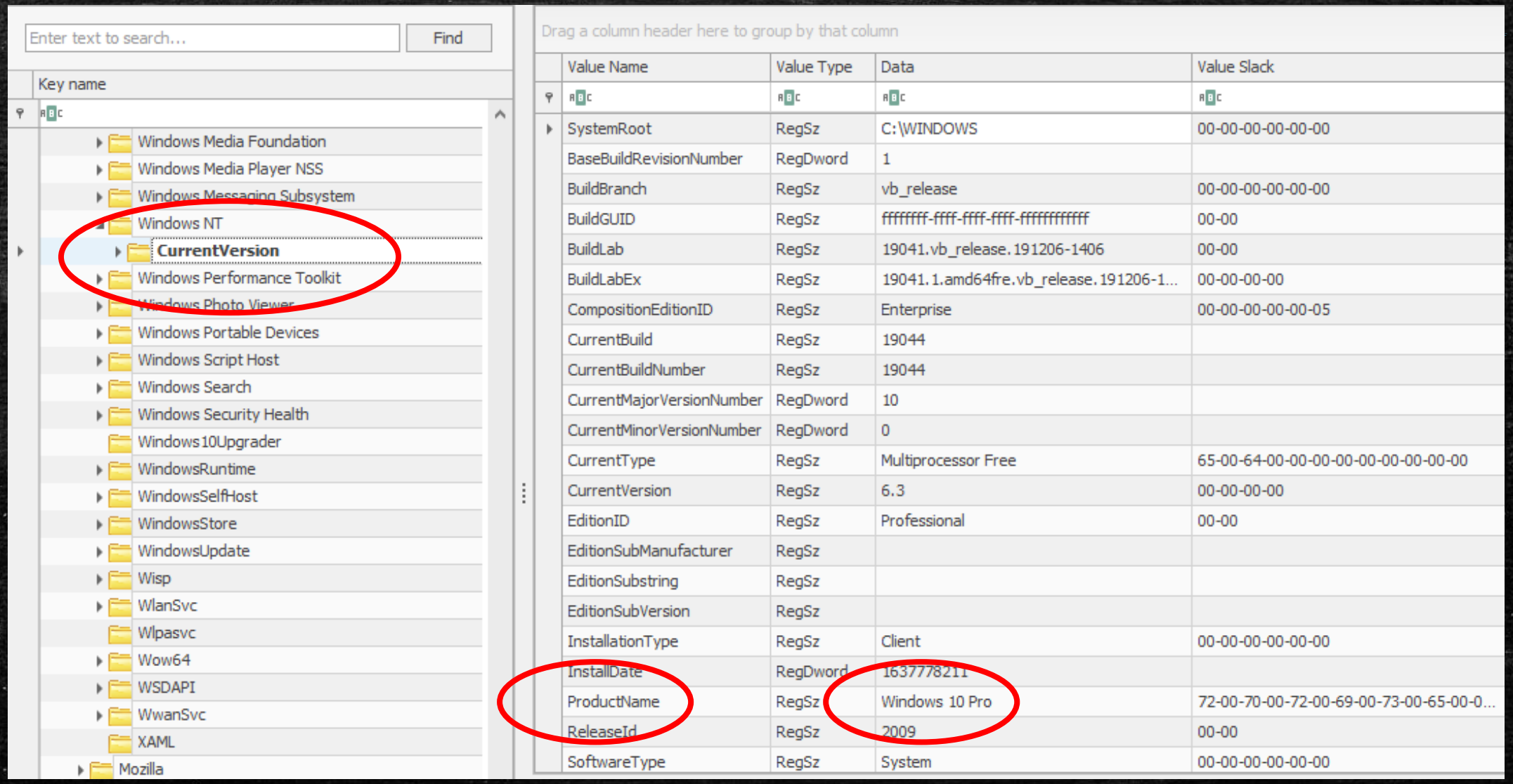
```
C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
```

# System Info & User Accounts

# System

- Computer name
- Dynamic Disks
- Install Dates
- Last User Logged In
- Mounted Devices
- Startup Programs - Autoruns
- System's USB Devices
- …e.t.c.

# System – OS Version

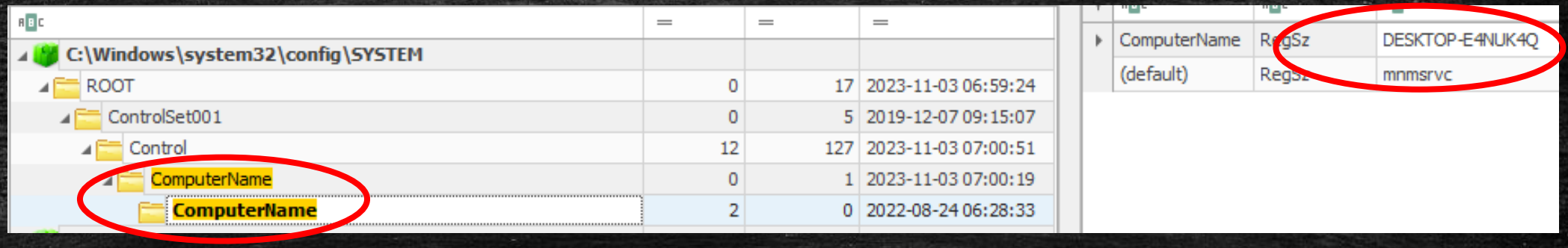


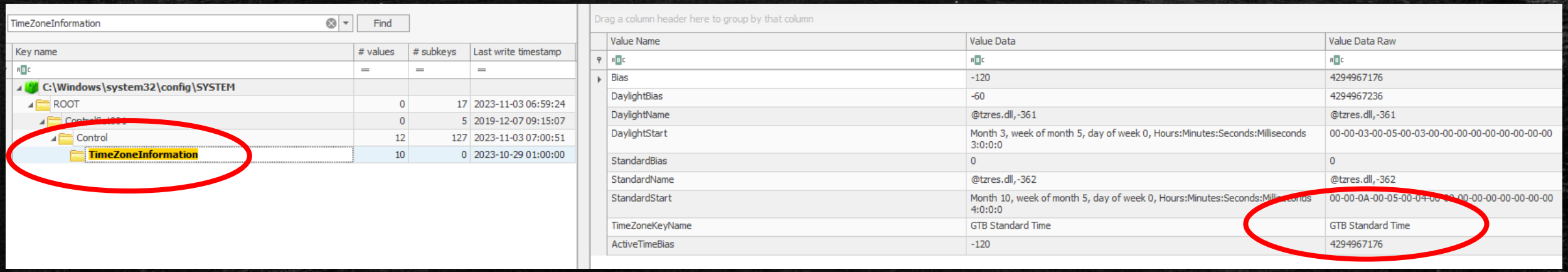
# System – Control Sets

- **Control Sets**
  - SYSTEM\ControlSet001
  - SYSTEM\ControlSet002
- **CurrentControlSet**
  - Contains Configuration information, drivers and services information
  - Volatile Key
  - SYSTEM\Select\Current
  - SYSTEM\Select\LastKnownGood
  - \SYSTEM\CurrentControlSet\Control
    - \ComputerName\ComputerName
    - \TimeZoneInformation
    - \Windows
      - Shutdown time

# System - CurrentControlSet

# System – ComputerName and TimeZoneInformation

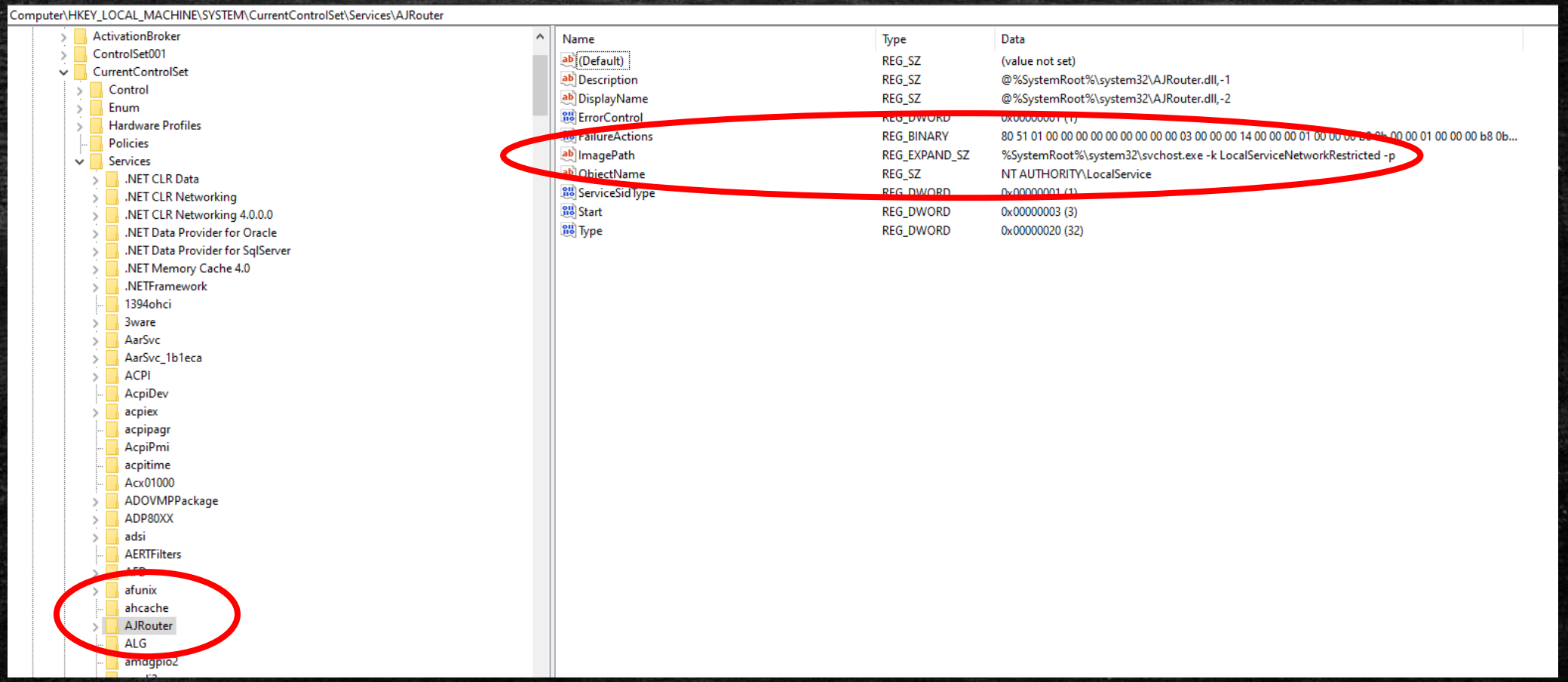


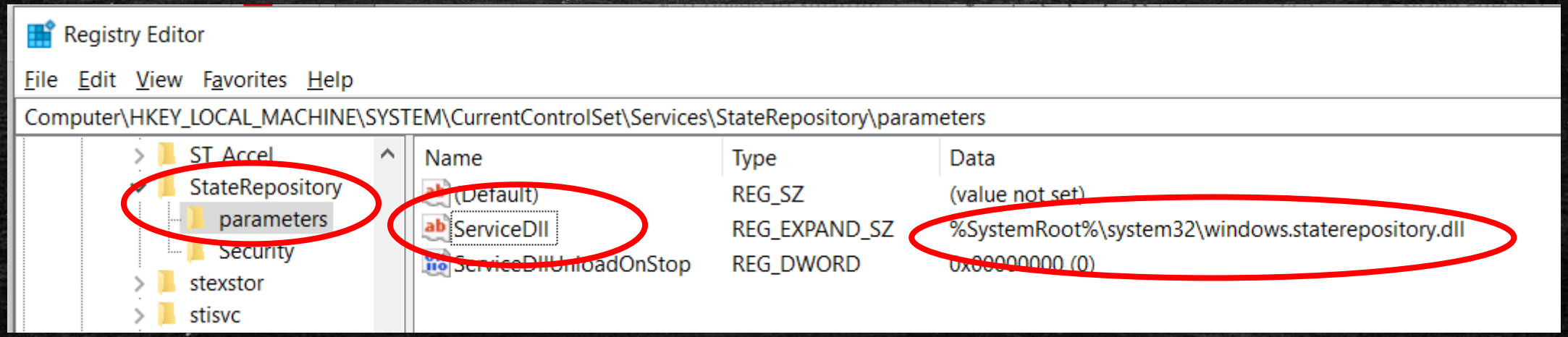
# System – CurrentControlSet\Services

- \Services\LanmanServer\shares
- Services:\Start = 0x02 (Auto), 0x03 (Manual), 0x04 (Disabled)
  - SVCHost (Windows Services)
    - \ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
    - SOFTWARE\Microsoft\Windows NT\CurrentVersion\svchost
  - \Services\{service_name}\Parameters -> ServiceDll

# System – CurrentControlSet\Services



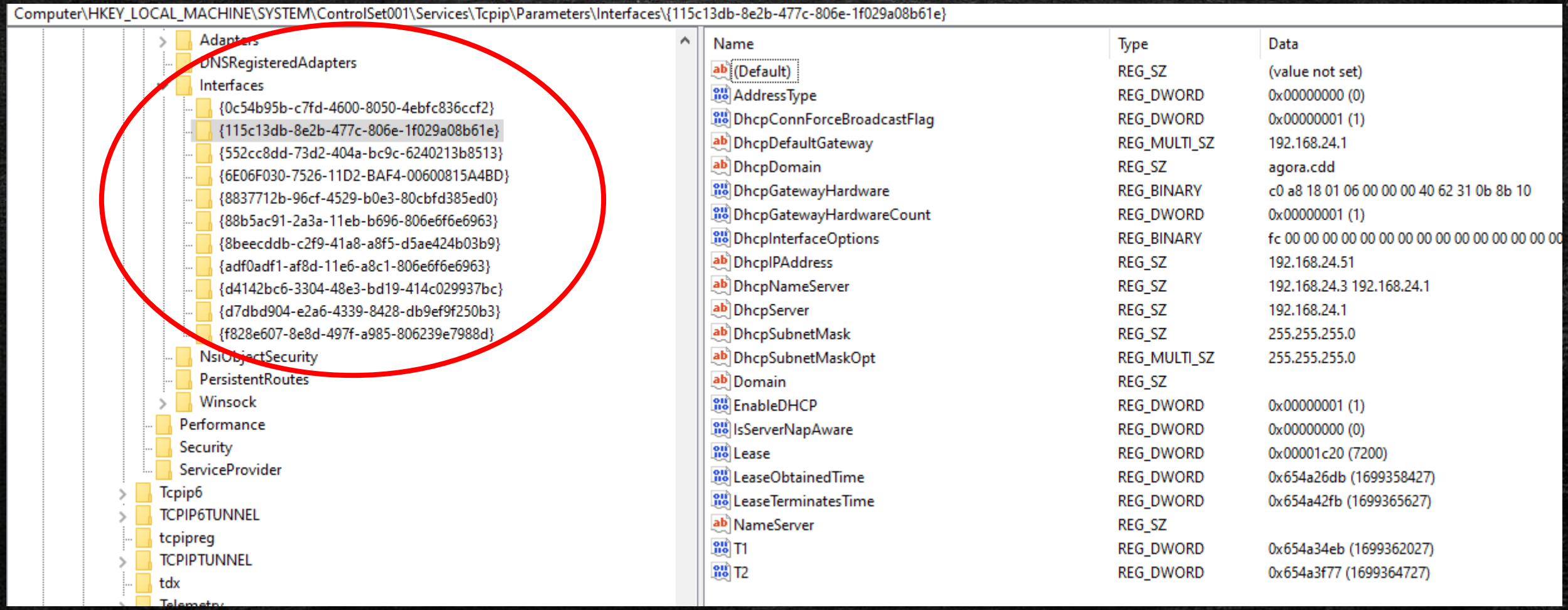
# System – CurrentControlSet\Services



# System – Network Elements

- ControlSet(number)\Services\Tcpip\Parameters\Interfaces (Network Interface)
  - GUIDs, Ips, Gateways,…

# System – Interfaces



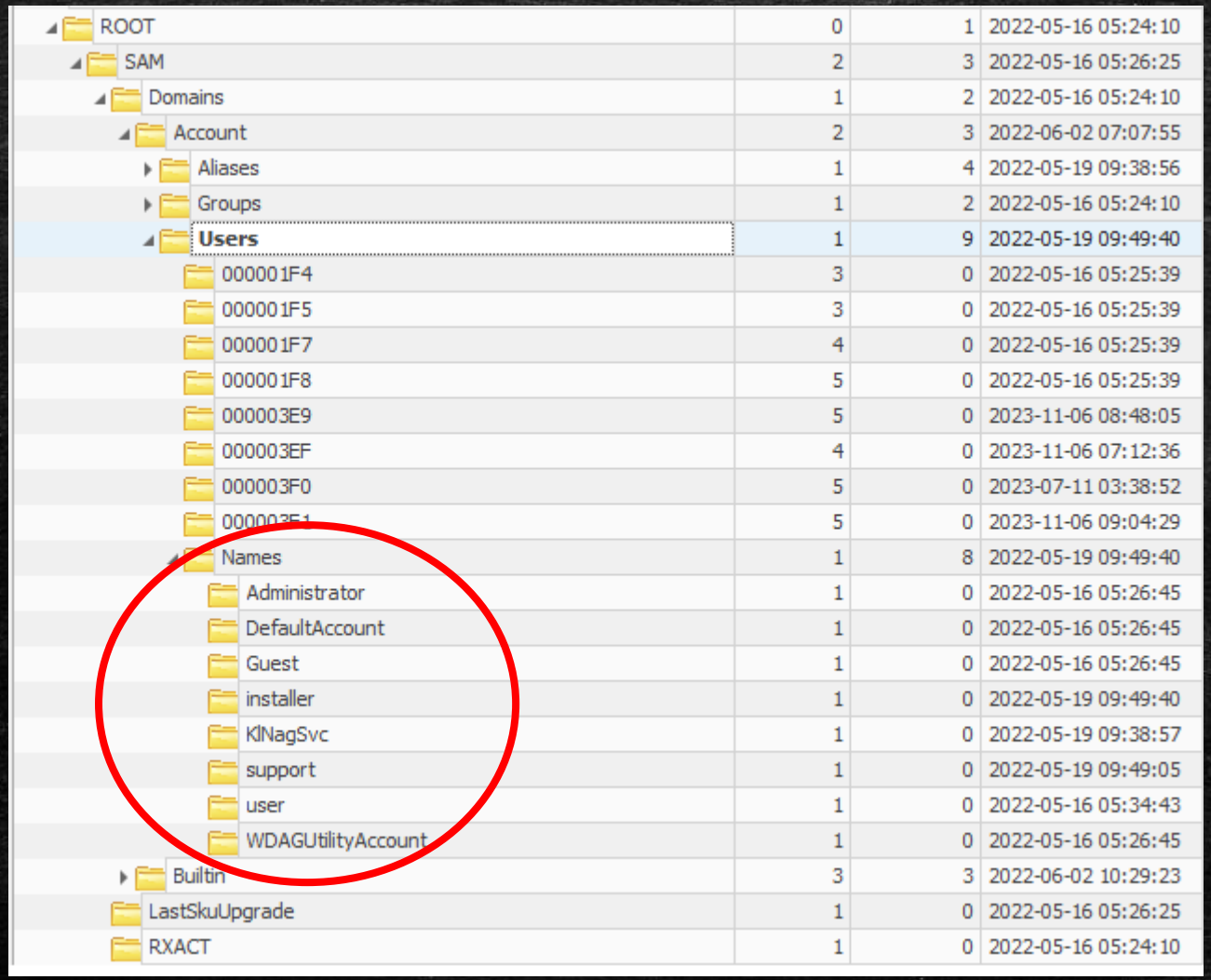
# SAM (Security Account Manager)

- SAM\Domains\Account\Users
  - Username
  - SID (Security Identifier)
  - User Login Information
  - Last Login
  - Last failed login
  - Logon Count
  - Password policy
  - Group Information
  - Administrators
  - Users
  - Remote Desktop Users
  - …e.t.c.

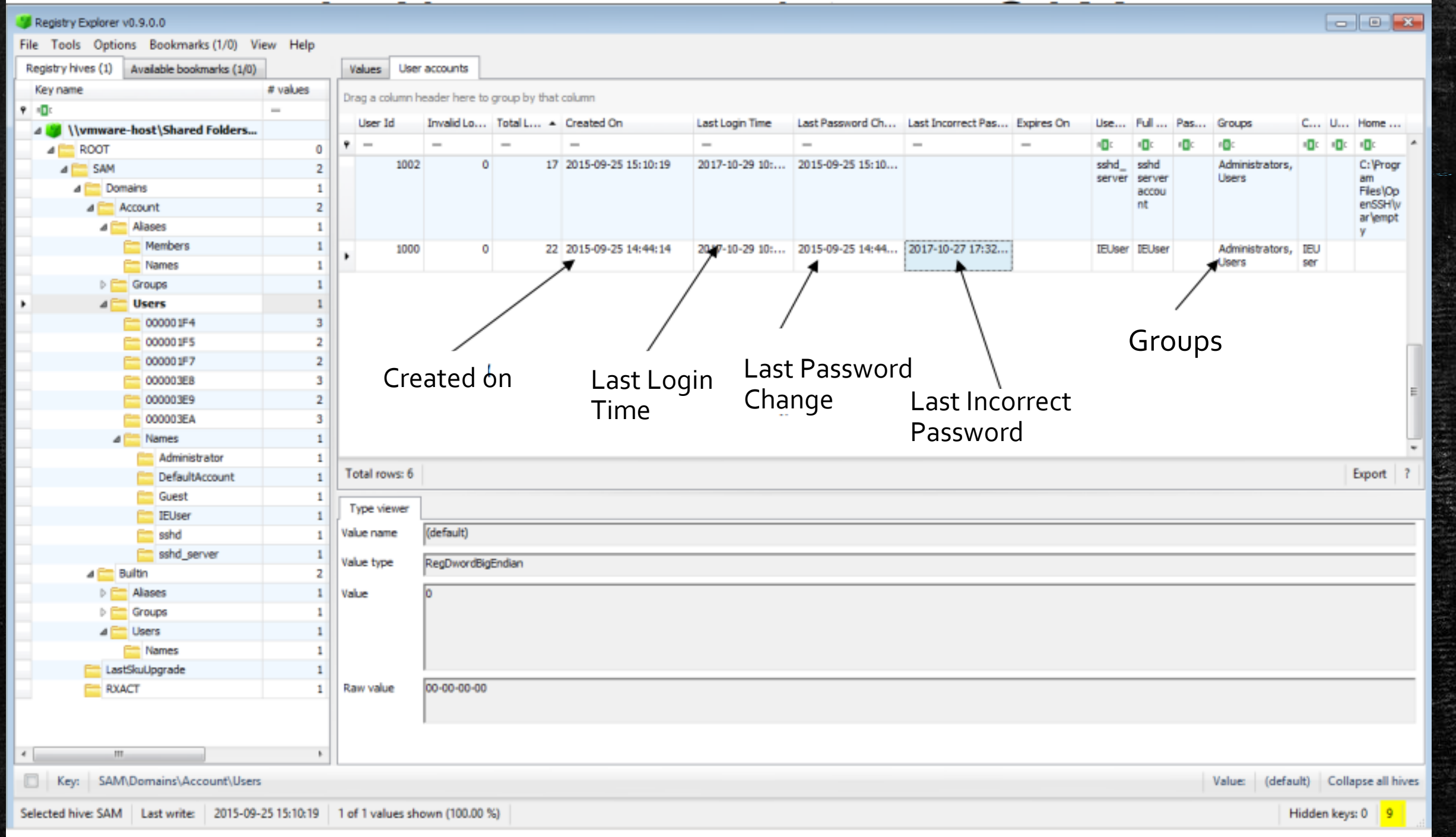
# SAM

- SAM\Domains\Account\Users\Names
- SAM\Domains\Account\ Users\(RID) (User Information)
  - regripper (plugin: samparse )
  - pwdump
- Empty pass: – 31d6cfe0d16ae931b73c59d7e0c089c0

# SAM



| | | | |
|---|---|---|---|
| ROOT | 0 | 1 | 2022-05-16 05:24:10 |
| SAM | 2 | 3 | 2022-05-16 05:26:25 |
| Domains | 1 | 2 | 2022-05-16 05:24:10 |
| Account | 2 | 3 | 2022-06-02 07:07:55 |
| Aliases | 1 | 4 | 2022-05-19 09:38:56 |
| Groups | 1 | 2 | 2022-05-16 05:24:10 |
| **Users** | 1 | 9 | 2022-05-19 09:49:40 |
| 000001F4 | 3 | 0 | 2022-05-16 05:25:39 |
| 000001F5 | 3 | 0 | 2022-05-16 05:25:39 |
| 000001F7 | 4 | 0 | 2022-05-16 05:25:39 |
| 000001F8 | 5 | 0 | 2022-05-16 05:25:39 |
| 000003E9 | 5 | 0 | 2023-11-06 08:48:05 |
| 000003EF | 4 | 0 | 2023-11-06 07:12:36 |
| 000003F0 | 5 | 0 | 2023-07-11 03:38:52 |
| 000003F1 | 5 | 0 | 2023-11-06 09:04:29 |
| Names | 1 | 8 | 2022-05-19 09:49:40 |
| Administrator | 1 | 0 | 2022-05-16 05:26:45 |
| DefaultAccount | 1 | 0 | 2022-05-16 05:26:45 |
| Guest | 1 | 0 | 2022-05-16 05:26:45 |
| installer | 1 | 0 | 2022-05-19 09:49:40 |
| KlNagSvc | 1 | 0 | 2022-05-19 09:38:57 |
| support | 1 | 0 | 2022-05-19 09:49:05 |
| user | 1 | 0 | 2022-05-16 05:34:43 |
| WDAGUtilityAccount | 1 | 0 | 2022-05-16 05:26:45 |
| Builtin | 3 | 3 | 2022-06-02 10:29:23 |
| LastSkuUpgrade | 1 | 0 | 2022-05-16 05:26:25 |
| RXACT | 1 | 0 | 2022-05-16 05:24:10 |


Registry Explorer v0.9.0.0
File Tools Options Bookmarks (1/0) View Help
Registry hives (1) Available bookmarks (1/0)
Key name # values
\\vmware-host\Shared Folders...
ROOT 0
SAM 2
Domains 1
Account 2
Aliases 1
Members 1
Names 1
Groups 1
Users 1
000001F4 3
000001F5 2
000001F7 2
000003E8 3
000003E9 2
000003EA 3
Names 1
Administrator 1
DefaultAccount 1
Guest 1
IEUser 1
sshd 1
sshd_server 1
Builtin 2
Aliases 1
Groups 1
Users 1
Names 1
LastSkuUpgrade 1
RXACT 1
Values User accounts
Drag a column header here to group by that column
User Id Invalid Lo... Total L... Created On Last Login Time Last Password Ch... Last Incorrect Pas... Expires On Use... Full ... Pas... Groups C... U... Home ...
1002 0 17 2015-09-25 15:10:19 2017-10-29 10:... 2015-09-25 15:10... sshd_server sshd server account Administrators, Users C:\Program Files\OpenSSH\var\empty
1000 0 22 2015-09-25 14:44:14 2017-10-29 10:... 2015-09-25 14:44... 2017-10-27 17:32... IEUser IEUser Administrators, Users IEUser
Created on
Last Login Time
Last Password Change
Last Incorrect Password
Groups
Total rows: 6 Export ?
Type viewer
Value name (default)
Value type RegDwordBigEndian
Value 0
Raw value 00-00-00-00
Key: SAM\Domains\Account\Users Value: (default) Collapse all hives
Selected hive: SAM Last write: 2015-09-25 15:10:19 1 of 1 values shown (100.00 %) Hidden keys: 0 9

# SAM

```
samparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info


User Information
------------------------
Username        : Administrator [500]
SID             : S-1-5-21-2725696290-2759209594-2886217957-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    :
Account Created : Mon May 16 05:26:45 2022 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

# SAM.dat

*pwdump7 –s <sam_hive> <system_hive>*

*C:\Users\sansforensics408\Downloads\pwdump7>pwdump7 -s C:\Users\sansforensics408*
*\Desktop\CC15_VM\SAM C:\Users\sansforensics408\Desktop\CC15_VM\SYSTEM*
*Pwdump v7.1 - raw password extractor*
*Author: Andres Tarasco Acuna*
*url: http://www.514.es*

*Administrator:500:NO PASSWORD**********************:31D6CFE0D16AE931B73C59D7E0C089C0:::*
*Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::*
*Mike:1000:NO PASSWORD**********************:31D6CFE0D16AE931B73C59D7E0C089C0:::*

# Software

- A lot of system configurations
- Application configuration
- A lot of the software keys, also exist in NTUSER.dat, where they are user specific

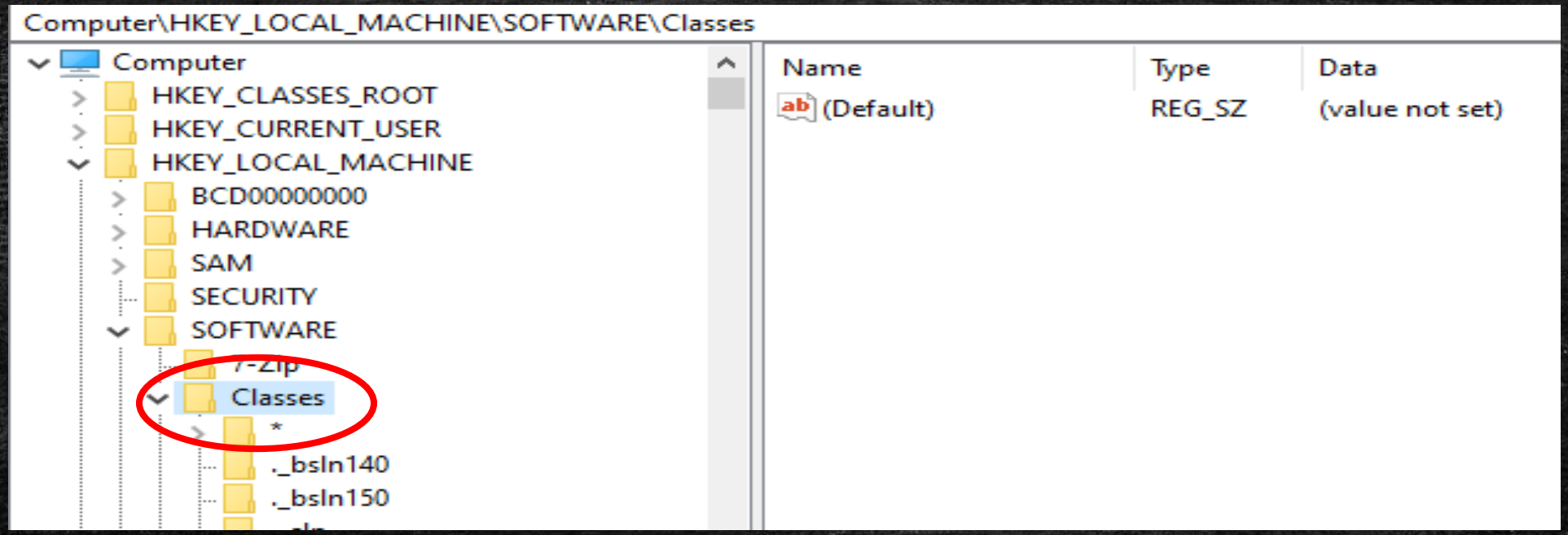
# Software – CurrentVersion \ Classes

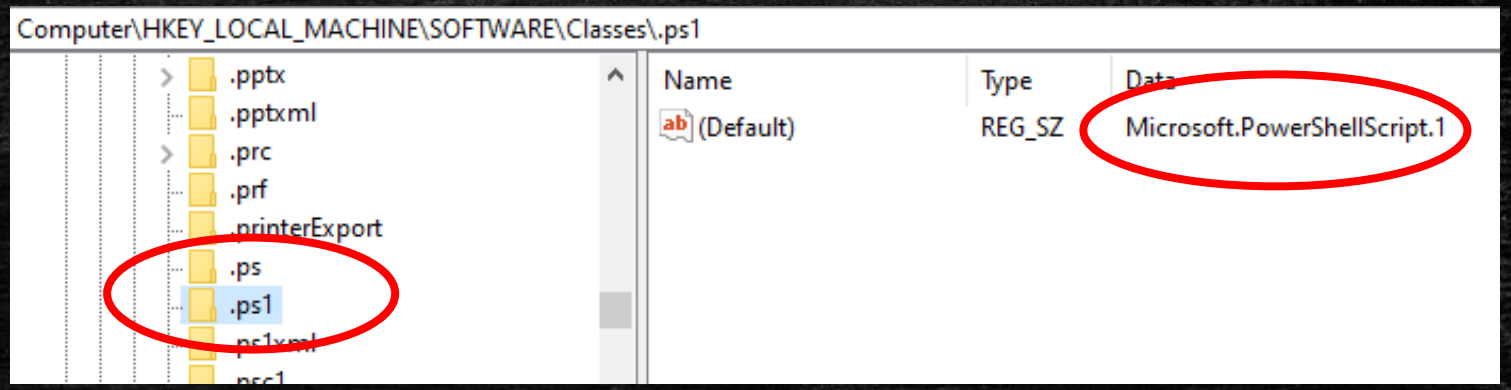
- \Microsoft\Windows NT\CurrentVersion
  - ProductName
  - \App Paths : installed applications
  - \Uninstall : installed applications

- \Classes (File Association)
  - The program that will open a file

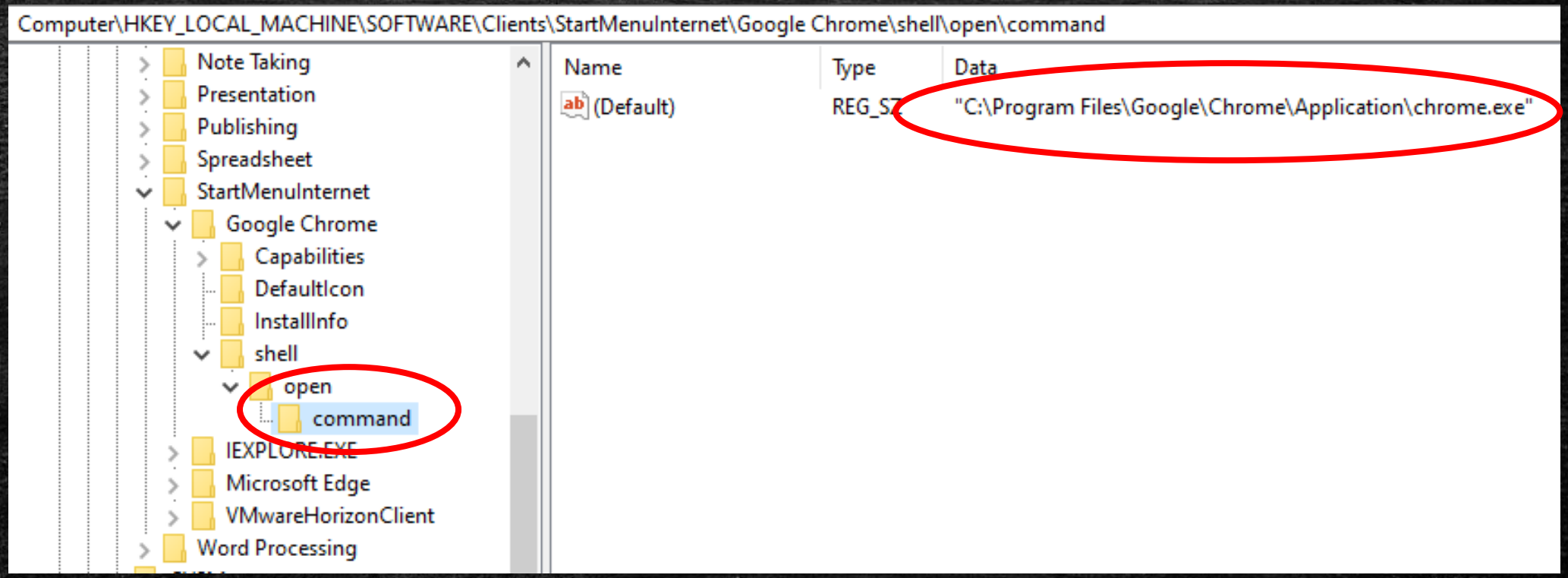
- \Clients\StartMenuInternet &
  \Classes\HTTP\shell\open\command (Default Browser)

# Software – Classes



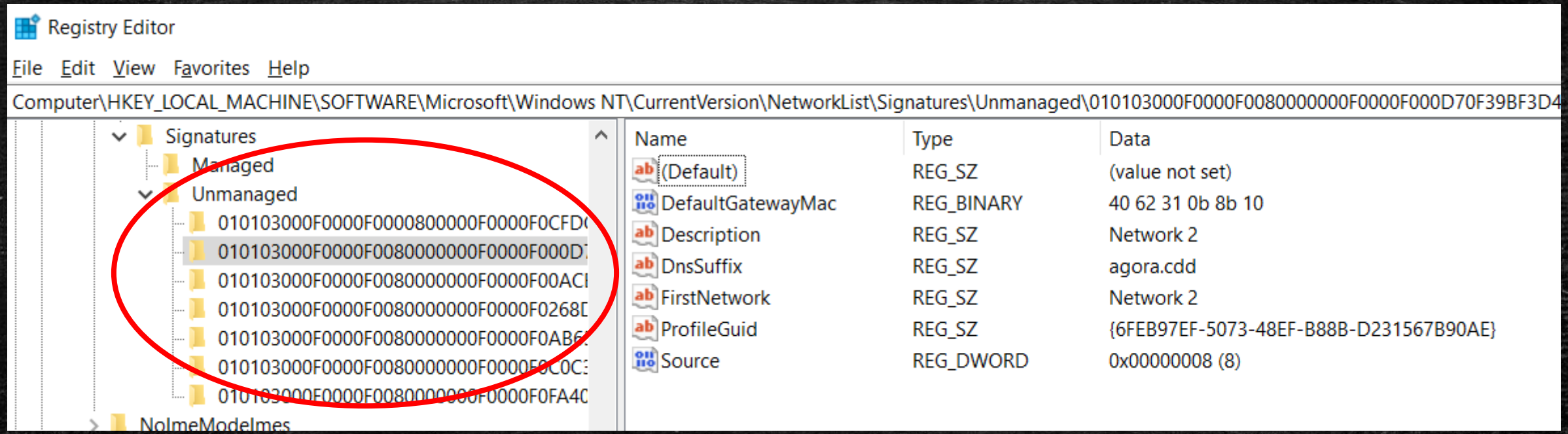
# Software – Clients\StartMenuInternet



# Software – Past Networks

- Past Networks:
  - SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
  - SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

# Software - Past Networks

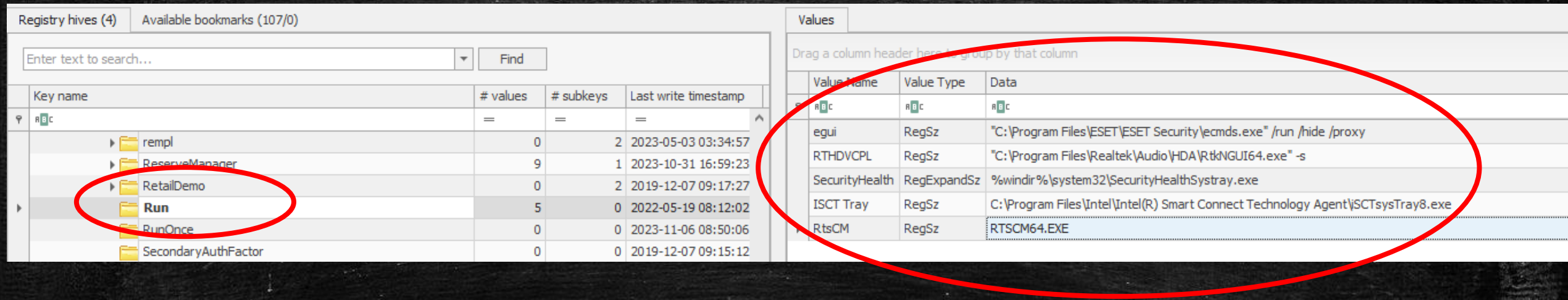


# Software - Autoruns

Autoruns:

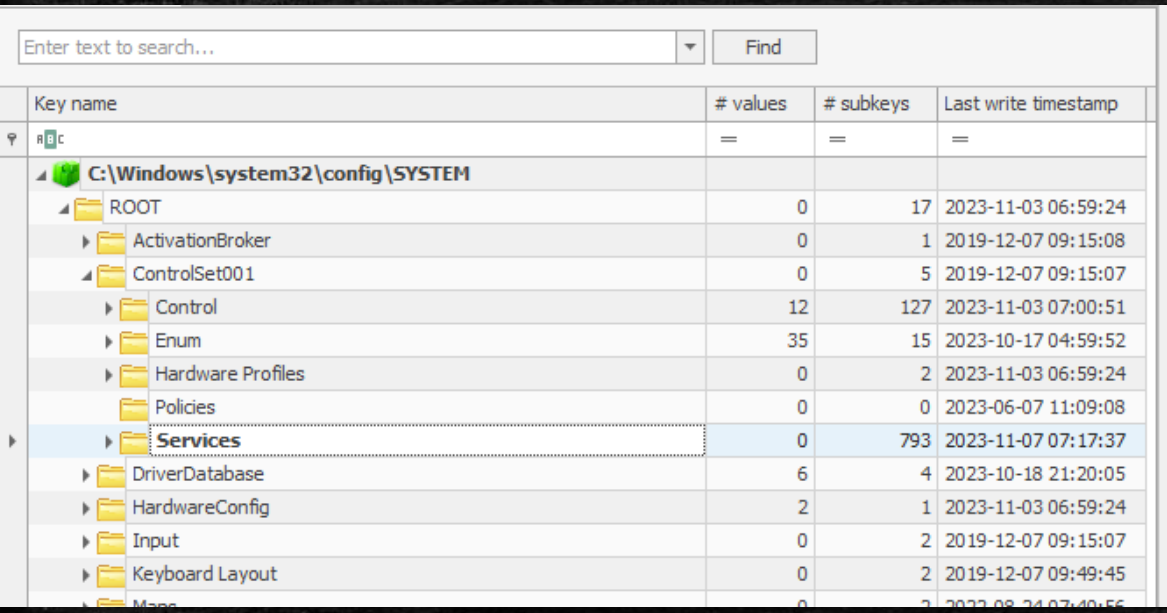
- Microsoft\Windows\CurrentVersion\Run
- Microsoft\Windows\CurrentVersion\policies\Explorer\Run
- Microsoft\Windows\CurrentVersion\RunOnce
- Microsoft\Windows NT\CurrentVersion\Winlogon\
  - Notify (dll files during logon) (No default)
  - UserInit
- Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
  - Shell Extensions: Windows search dlls first in “%Windows%” then in “%Windows%\System32” (If not stated)

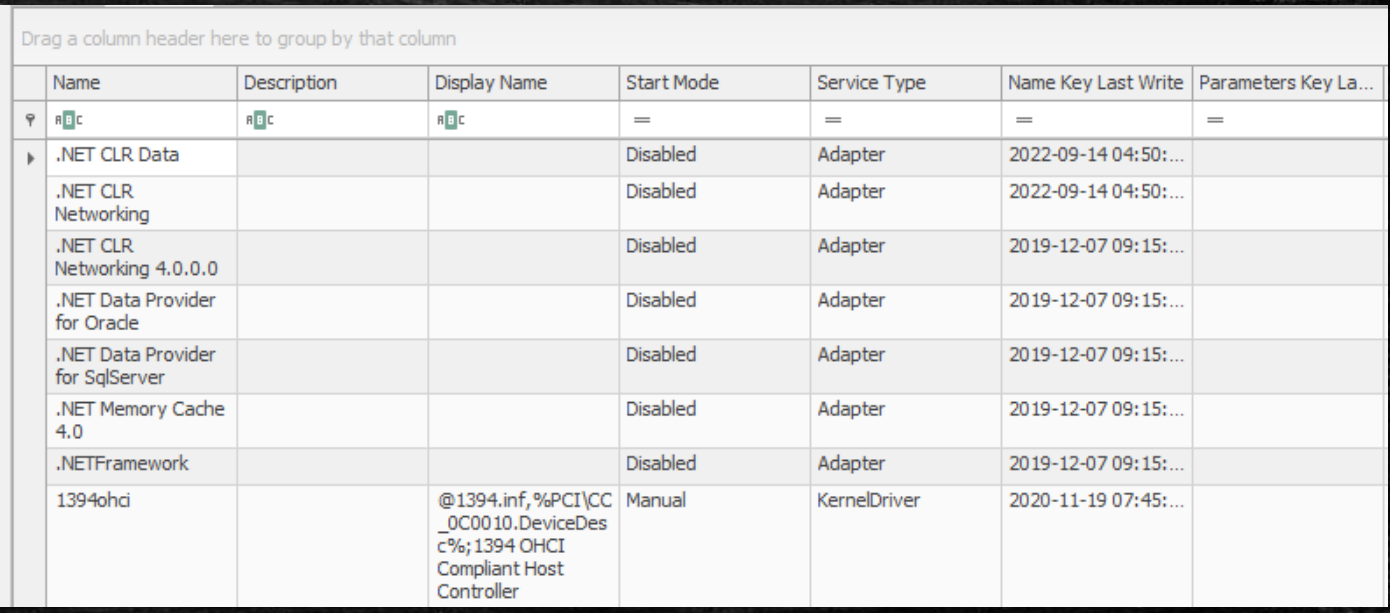
# Software – CurrentVersion\Run



# Software – Other Autoruns Locations

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
- SYSTEM\CurrentControlSet\Services



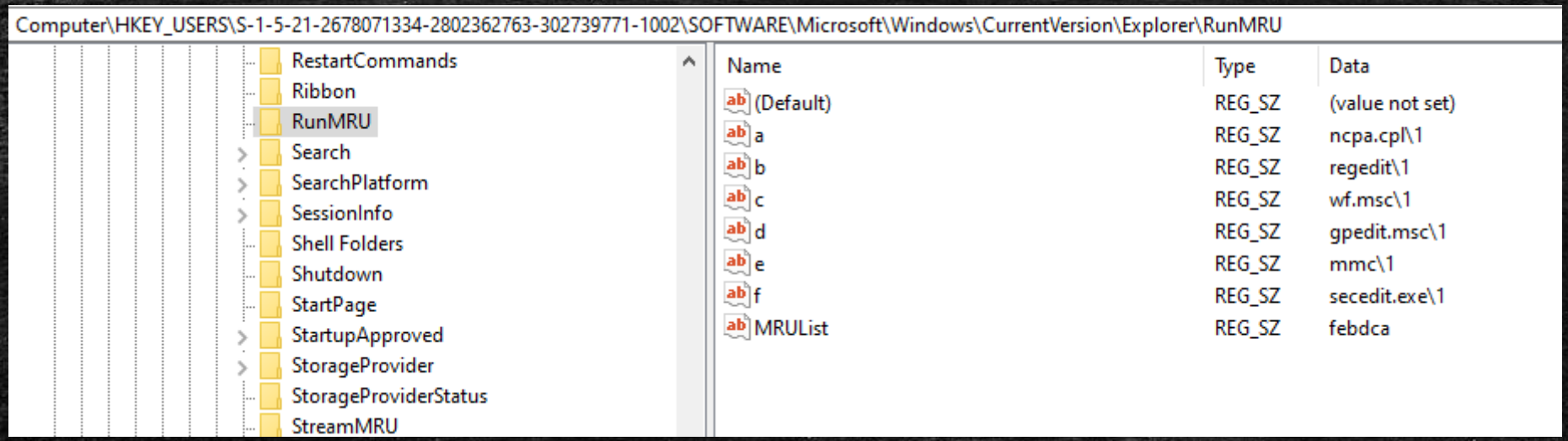
# Usage of Files/Folders

# NTUSER.DAT & USRCLASS.DAT

- User information
- Some keys in NTUSER.dat have same path, name and values with SOFTWARE
  - ➢ But user specific information
- NTUSER.dat \Software\Microsoft\Windows\CurrentVersion\Run
- NTUSER.dat \Software\Microsoft\Windows\CurrentVersion\RunOnce

# NTUSER.DAT & USRCLASS.DAT - MRUs

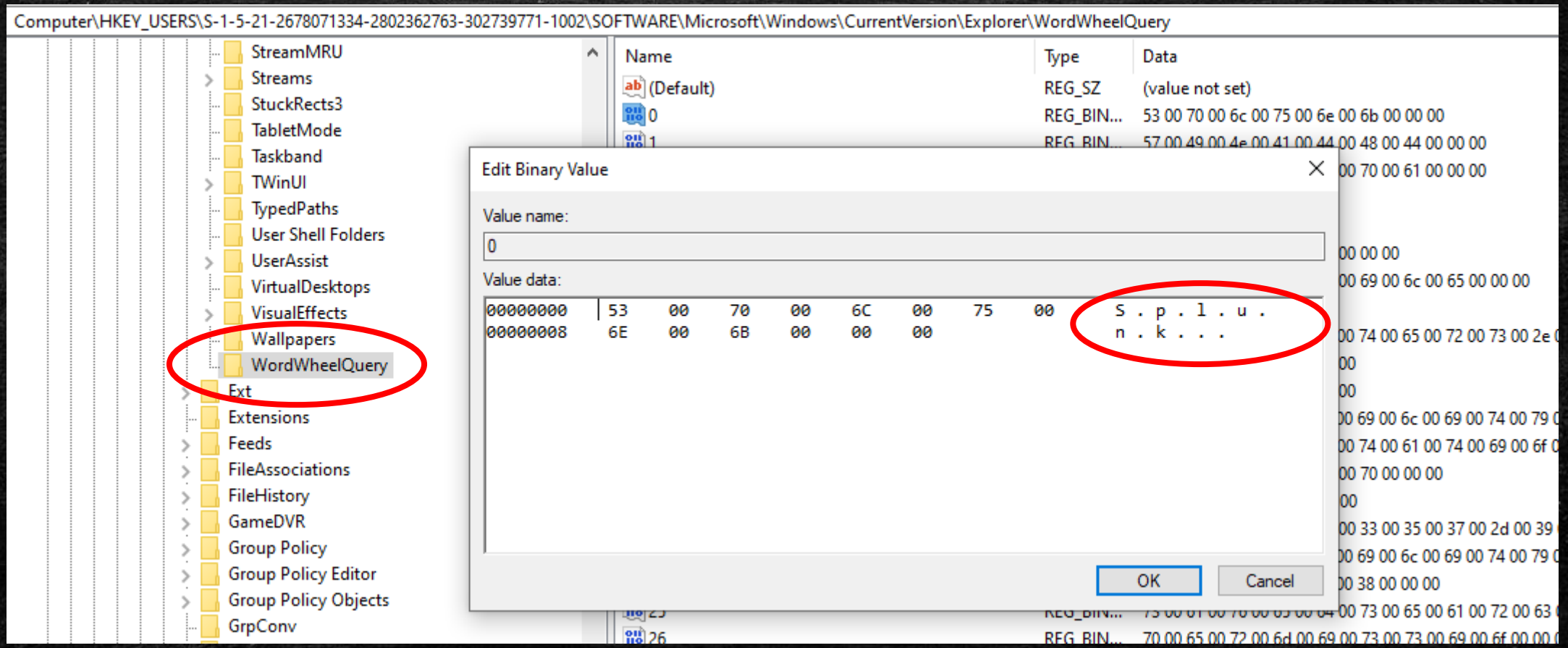
- MRU



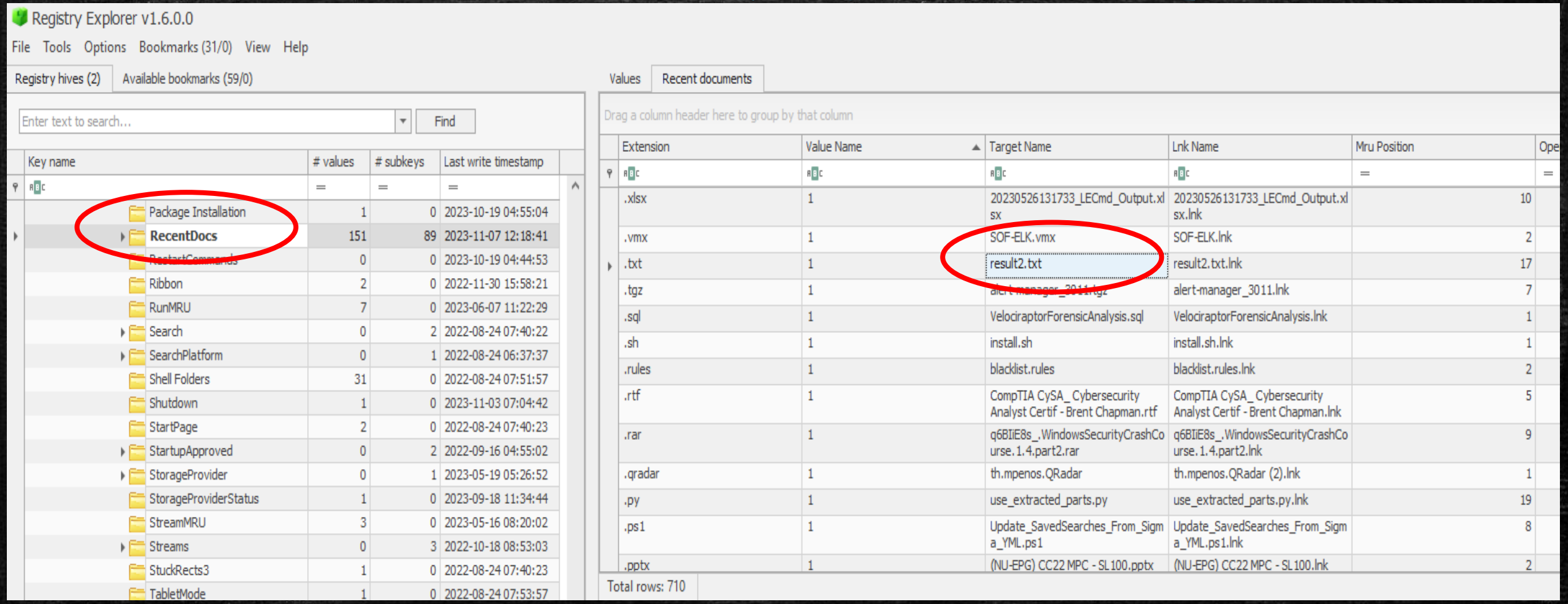
# NTUSER.DAT & USRCLASS.DAT - MRUs

- MRUs
  - Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
    - Most recently searches
  - Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
  - Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
  - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
    - All values remain even when the file is deleted
    - An mru list for all kinds of files
  - Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
  - Software\Microsoft\Office\VERSION

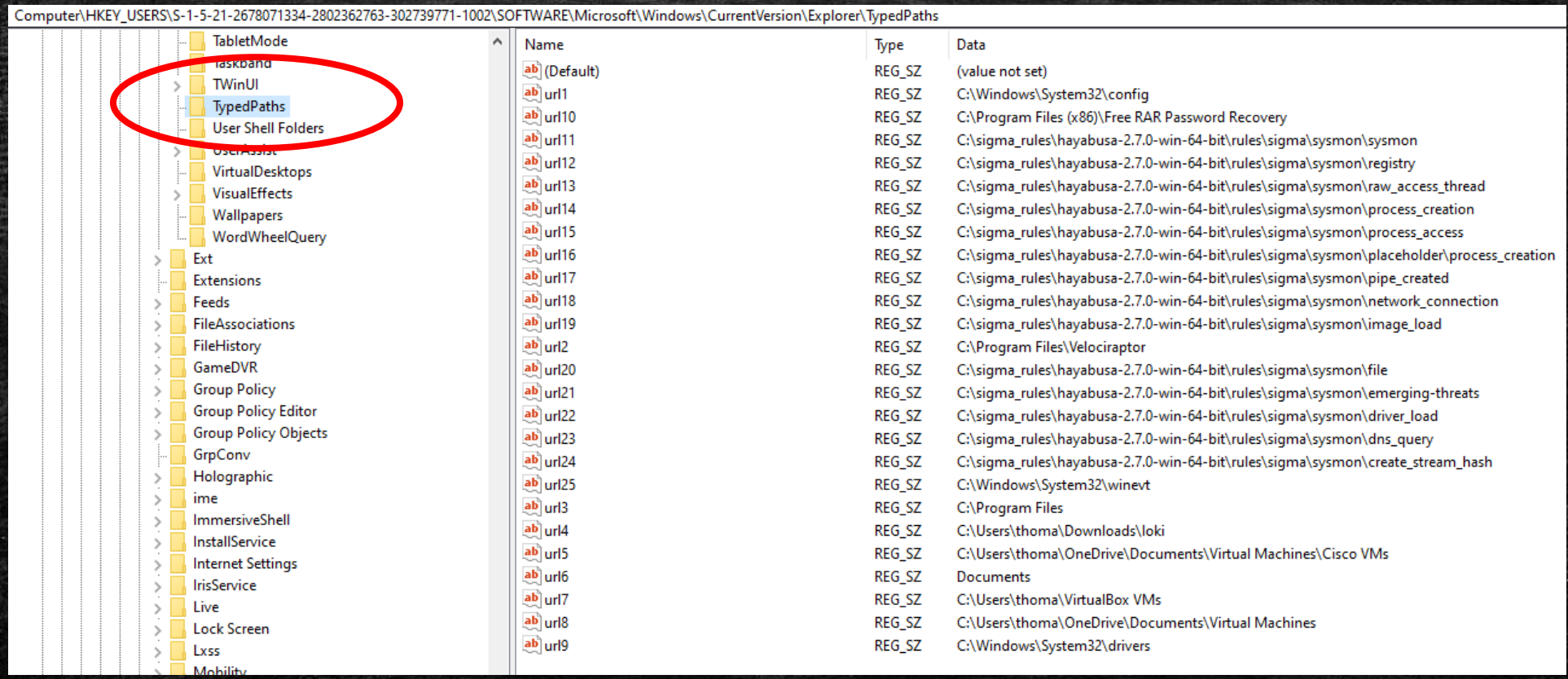
# NTUSER.DAT & USRCLASS.DAT - WordWheelQuery



# NTUSER.DAT & USRCLASS.DAT - RecentDocs



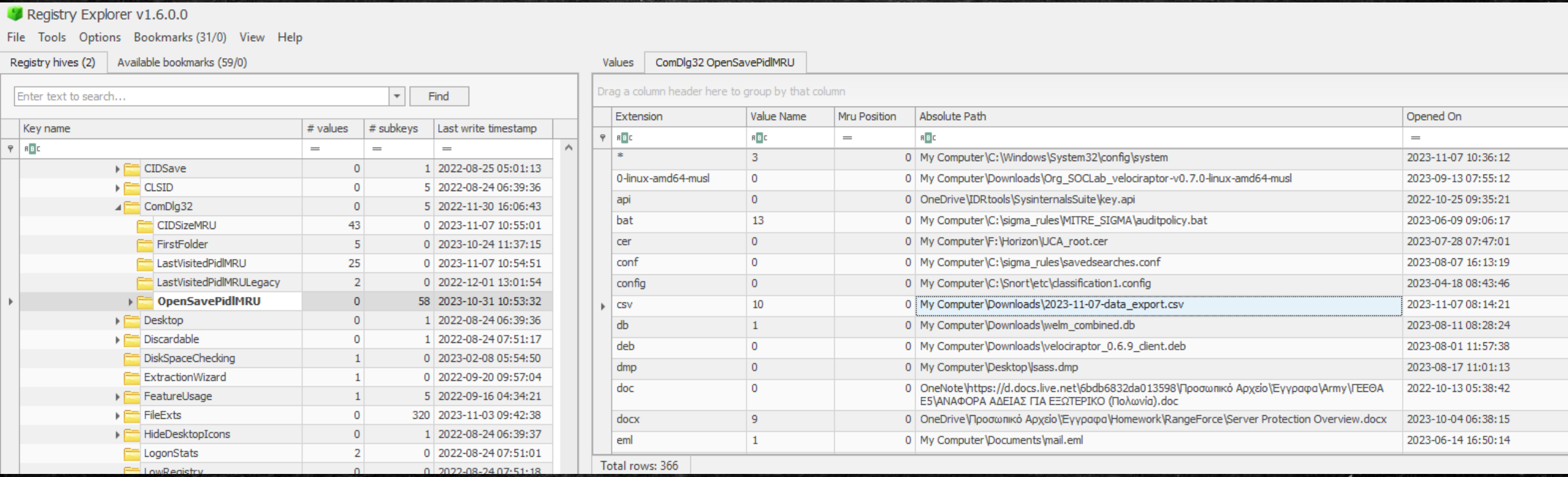
# NTUSER.DAT & USRCLASS.DAT - TypedPaths



# NTUSER.DAT & USRCLASS.DAT - ComDlg32

- Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
  - OpenSavePidlMRU (Open and Save As …)
  - LastVisitedPidMRU (Last Used Application to access file and folder recorded by OpenSavePidMRU)

# NTUSER.DAT & USRCLASS.DAT - OpenSavePidlMRU



# NTUSER.DAT & USRCLASS.DAT - LastVisitedPidMRU

Values | ComDlg32 LastVisitedPidlMRU

Drag a column header here to group by that column

| Value Name | Mru Position | Executable | Absolute Path | Opened On |
|---|---|---|---|---|
| 8 | 0 | RegistryExplorer.exe | My Computer\C:\Windows\System32\config | 2023-11-07 10:54:51 |
| 12 | 1 | msedge.exe | My Computer\Desktop | |
| 5 | 2 | {8480A1E8-D4C0-43D5-B689-72D214AB4DFC} | My Computer\C:\Users\thoma\Downloads | |
| 1 | 3 | notepad++.exe | OneDrive\Προσωπικό Αρχείο\Εγγραφα\Army\ΓΕΕΘΑ E5\Deployment\Velociraptor | |
| 22 | 4 | {D6637525-53BD-49E9-9E1B-D5E744F7A9DF} | OneDrive\Προσωπικό Αρχείο\Εγγραφα\Army\ΓΕΕΘΑ E5\ESDC | |
| 23 | 5 | vmware.exe | My Computer\Documents\Virtual Machines | |
| 14 | 6 | VirtualBox.exe | My Computer\Documents\Virtual Machines\CyberOps | |
| 6 | 7 | KeePass.exe | My Computer\C:\Users\thoma\OneDrive\Προσωπικό Αρχείο | |
| 18 | 8 | Code.exe | OneDrive\Προσωπικό Αρχείο\Εγγραφα\Army\ΓΕΕΘΑ E5 | |
| 0 | 9 | chrome.exe | My Computer\Downloads | |
| 3 | 10 | {EC04B61C-3E7B-4750-B9C5-95446FA443B2} | OneDrive\Προσωπικό Αρχείο\Εγγραφα\Homework\RangeForce | |
| 20 | 11 | PickerHost.exe | My Computer\Desktop | |
| 13 | 12 | mspaint.exe | My Computer\Desktop | |
| 21 | 13 | procexp64.exe | My Computer\Desktop | |

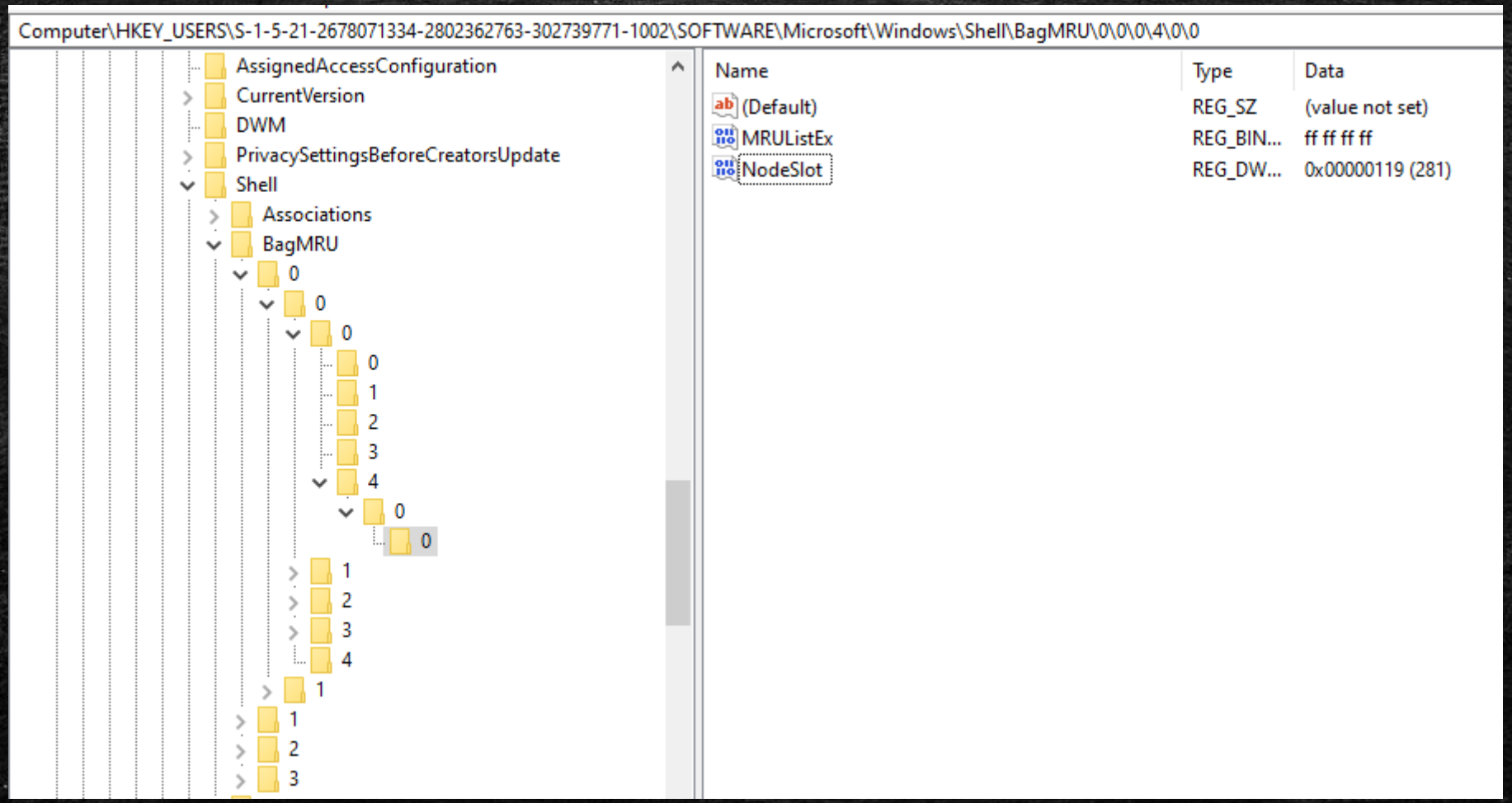
# NTUSER.DAT & USRCLASS.DAT - ShellBags

- Contains user-specific Windows OS folder and viewing preferences to Windows Explorer
- Which folders were accessed on the local machine, network, and/or removable devices
  - Evidence of previously existing folders after deletion/overwrite
  - When certain folders were accessed
- Explorer Access:
  - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
  - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- Desktop Access:
  - NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
  - NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

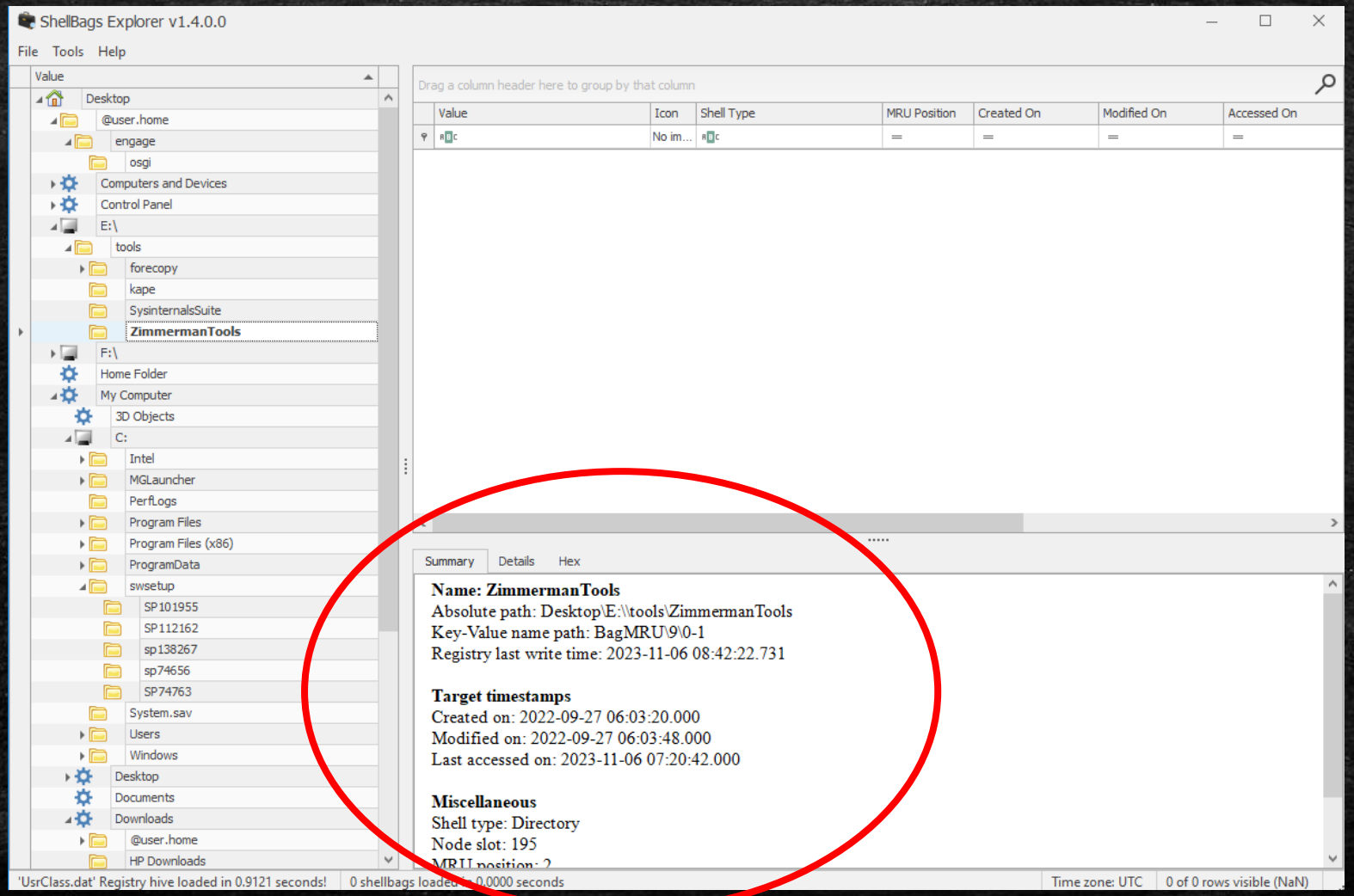
# NTUSER.DAT & USRCLASS.DAT - ShellBags

*\Shell*
*\BagMRU*
*\0 (Desktop)*
*\0 (Computer)*
*\0 (C:\)*
*\0 (Users)*
*\0 (username)*
*\0 (Documents)*
*\1 (AppData)*
*\2 (Links)*
*\3 …*
*…*
*\1 (ProgramFiles)*
*\2 …*
*…*

# NTUSER.DAT & USRCLASS.DAT - ShellBags



# NTUSER.DAT & USRCLASS.DAT - ShellBags

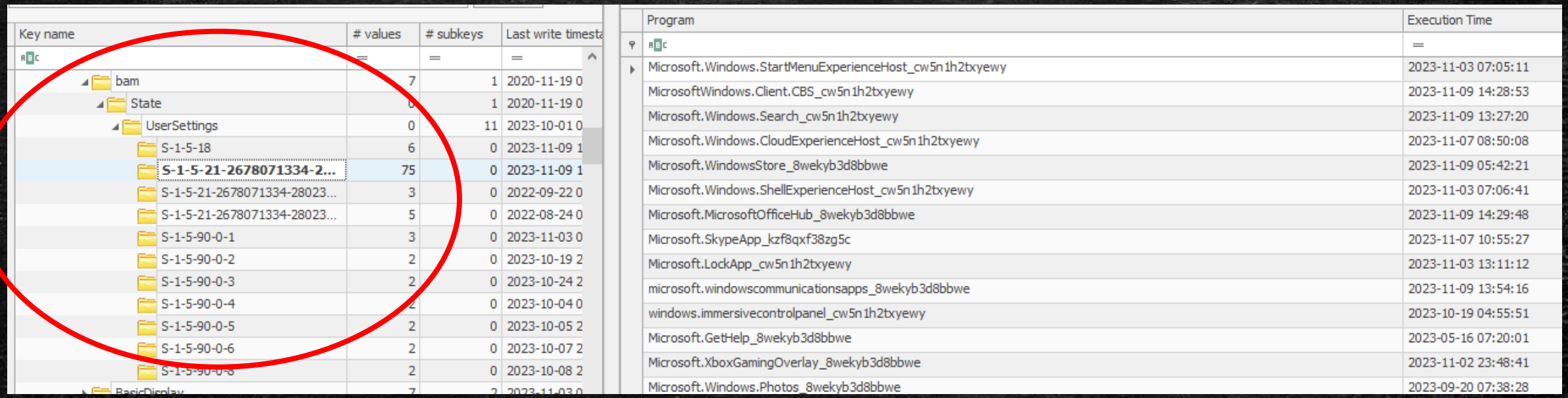


# Evidence Of Execution

# System – BAM/DAM

- BAM
  - Activity of background applications
  - SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\{SID}
- DAM
  - Optimizes power consumption of the device
  - SYSTEM\CurrentControlSet\Services\dam\State\UserSettings\{SID}

# System – BAM/DAM



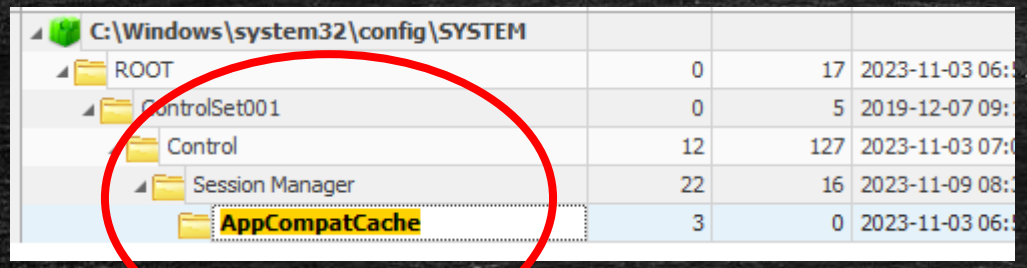
| Key name | # values | # subkeys | Last write timesta |
|---|---|---|---|
| bam | 7 | 1 | 2020-11-19 0 |
| State | 6 | 1 | 2020-11-19 0 |
| UserSettings | 0 | 11 | 2023-10-01 0 |
| S-1-5-18 | 6 | 0 | 2023-11-09 1 |
| **S-1-5-21-2678071334-2...** | 75 | 0 | 2023-11-09 1 |
| S-1-5-21-2678071334-28023... | 3 | 0 | 2022-09-22 0 |
| S-1-5-21-2678071334-28023... | 5 | 0 | 2022-08-24 0 |
| S-1-5-90-0-1 | 3 | 0 | 2023-11-03 0 |
| S-1-5-90-0-2 | 2 | 0 | 2023-10-19 2 |
| S-1-5-90-0-3 | 2 | 0 | 2023-10-24 2 |
| S-1-5-90-0-4 | 2 | 0 | 2023-10-04 0 |
| S-1-5-90-0-5 | 2 | 0 | 2023-10-05 2 |
| S-1-5-90-0-6 | 2 | 0 | 2023-10-07 2 |
| S-1-5-90-0-8 | 2 | 0 | 2023-10-08 2 |
| BasicDisplay | 7 | 2 | 2023-11-03 0 |

| Program | Execution Time |
|---|---|
| Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy | 2023-11-03 07:05:11 |
| MicrosoftWindows.Client.CBS_cw5n1h2txyewy | 2023-11-09 14:28:53 |
| Microsoft.Windows.Search_cw5n1h2txyewy | 2023-11-09 13:27:20 |
| Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy | 2023-11-07 08:50:08 |
| Microsoft.WindowsStore_8wekyb3d8bbwe | 2023-11-09 05:42:21 |
| Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy | 2023-11-03 07:06:41 |
| Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe | 2023-11-09 14:29:48 |
| Microsoft.SkypeApp_kzf8qxf38zg5c | 2023-11-07 10:55:27 |
| Microsoft.LockApp_cw5n1h2txyewy | 2023-11-03 13:11:12 |
| microsoft.windowscommunicationsapps_8wekyb3d8bbwe | 2023-11-09 13:54:16 |
| windows.immersivecontrolpanel_cw5n1h2txyewy | 2023-10-19 04:55:51 |
| Microsoft.GetHelp_8wekyb3d8bbwe | 2023-05-16 07:20:01 |
| Microsoft.XboxGamingOverlay_8wekyb3d8bbwe | 2023-11-02 23:48:41 |
| Microsoft.Windows.Photos_8wekyb3d8bbwe | 2023-09-20 07:38:28 |

# System – ShimCache

- ShimCache (or AppCompatCache)
  - Keeps track of OS application compatibility
  - Tracks applications launched
  - File name, file size, and last modified time
  - SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

# System – ShimCache




Type viewer | Slack viewer | AppCompatCache

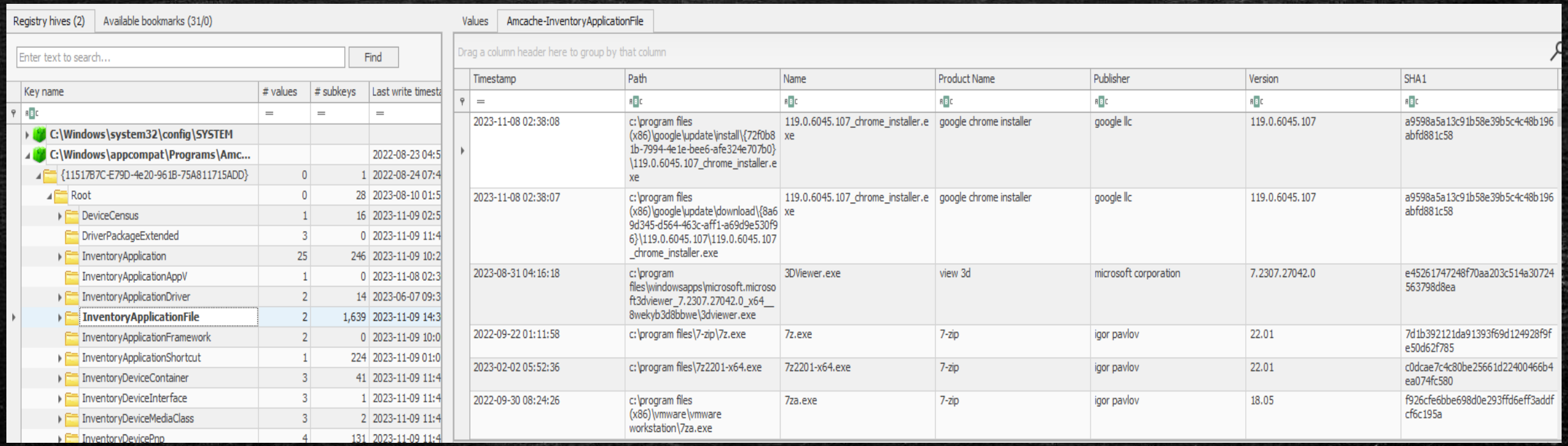
Drag a column header here to group by that column

| Cache Entry Position | Program Name | Modified Time |
|---|---|---|
| 0 | C:\Users\thoma\AppData\Local\Temp\mcr4rqzz.oxn\resources\app\ServiceHub\Services\Microsoft.VisualStudio.Setup.Service\BackgroundDownload.exe | 2023-11-03 06:32:33 |
| 1 | C:\Program Files\KeePass Password Safe 2\KeePass.exe | 2023-06-03 07:19:20 |
| 2 | C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Engine_Patch_1.1.23090.2007.exe | 2023-11-03 05:56:02 |
| 3 | C:\ProgramData\Package Cache\{1897b6e9-b6f9-4529-b7a6-f3f6547b8131}\PowerShell-7.3.8-win-x64.exe | 2023-10-18 12:32:55 |
| 4 | C:\WINDOWS\Temp\{77E3F257-8E48-4535-8E1D-EB53F562E7D6}\.be\PowerShell-7.3.9-win-x64.exe | 2023-11-03 04:11:58 |
| 5 | C:\WINDOWS\Temp\{B05A623D-5FA9-492D-B0B4-FB0B69FFECCD}\.cr\PowerShell-7.3.9-win-x64.exe | 2023-11-03 04:11:55 |
| 6 | C:\WINDOWS\SoftwareDistribution\Download\Install\PowerShell-7.3.9-win-x64.exe | 2023-11-03 04:11:33 |
| 7 | C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.399.1719.0.exe | 2023-11-03 01:43:47 |

# AmCache

- Similar function to ShimCache
- Stores additional data related to program executions
  - Execution path
  - Installation, execution and deletion times
  - SHA1 hashes
- C:\Windows\appcompat\Programs\Amcache.hve
- \Root\File\{Volume GUID}\

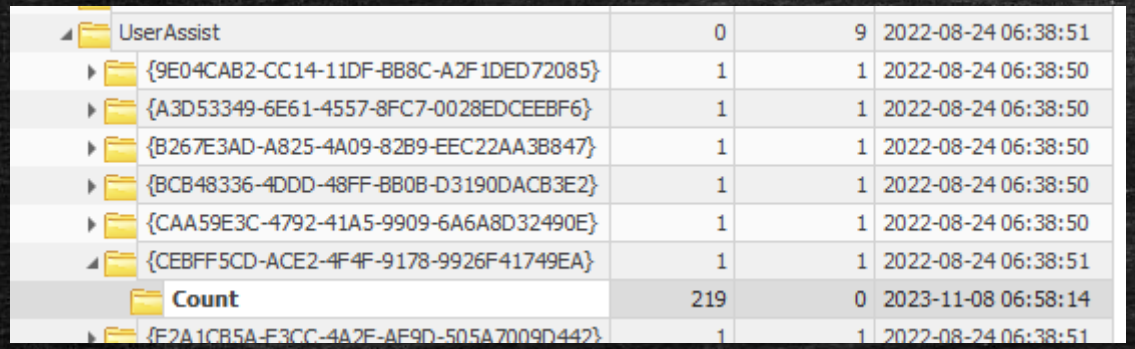
# AmCache


Registry hives (2)
Available bookmarks (31/0)
Enter text to search...
Find
Key name
# values
# subkeys
Last write timesta
C:\Windows\system32\config\SYSTEM
C:\Windows\appcompat\Programs\Amc...
2022-08-23 04:5
{11517B7C-E79D-4e20-961B-75A811715ADD}
0
1
2022-08-24 07:4
Root
0
28
2023-08-10 01:5
DeviceCensus
1
16
2023-11-09 02:5
DriverPackageExtended
3
0
2023-11-09 11:4
InventoryApplication
25
246
2023-11-09 10:2
InventoryApplicationAppV
1
0
2023-11-08 02:3
InventoryApplicationDriver
2
14
2023-06-07 09:3
InventoryApplicationFile
2
1,639
2023-11-09 14:3
InventoryApplicationFramework
2
0
2023-11-09 10:0
InventoryApplicationShortcut
1
224
2023-11-09 01:0
InventoryDeviceContainer
3
41
2023-11-09 11:4
InventoryDeviceInterface
3
1
2023-11-09 11:4
InventoryDeviceMediaClass
3
2
2023-11-09 11:4
Values
Amcache-InventoryApplicationFile
Drag a column header here to group by that column
Timestamp
Path
Name
Product Name
Publisher
Version
SHA1
2023-11-08 02:38:08
c:\program files (x86)\google\update\install\{72f0b81b-7994-4e1e-bee6-afe324e707b0}\119.0.6045.107_chrome_installer.exe
119.0.6045.107_chrome_installer.exe
google chrome installer
google llc
119.0.6045.107
a9598a5a13c91b58e39b5c4c48b196abfd881c58
2023-11-08 02:38:07
c:\program files (x86)\google\update\download\{8a69d345-d564-463c-aff1-a69d9e530f96}\119.0.6045.107\119.0.6045.107_chrome_installer.exe
119.0.6045.107_chrome_installer.exe
google chrome installer
google llc
119.0.6045.107
a9598a5a13c91b58e39b5c4c48b196abfd881c58
2023-08-31 04:16:18
c:\program files\windowsapps\microsoft.microsoft3dviewer_7.2307.27042.0_x64__8wekyb3d8bbwe\3dviewer.exe
3DViewer.exe
view 3d
microsoft corporation
7.2307.27042.0
e45261747248f70aa203c514a30724563798d8ea
2022-09-22 01:11:58
c:\program files\7-zip\7z.exe
7z.exe
7-zip
igor pavlov
22.01
7d1b392121da91393f69d124928f9fe50d62f785
2023-02-02 05:52:36
c:\program files\7z2201-x64.exe
7z2201-x64.exe
7-zip
igor pavlov
22.01
c0dcae7c4c80be25661d22400466b4ea074fc580
2022-09-30 08:24:26
c:\program files (x86)\vmware\vmware workstation\7za.exe
7za.exe
7-zip
igor pavlov
18.05
f926cfe6bbe698d0e293ffd6eff3addfcf6c195a

# NTUSER.DAT & USRCLASS.DAT – UserAssist

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
  → Record user daily activity (When the user clicks an object)
  - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} → files
  - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} → shortcuts
  - Also has a count of times that file or shortcut was used

# NTUSER.DAT & USRCLASS.DAT - UserAssist



| | | | |
|---|---|---|---|
| UserAssist | 0 | 9 | 2022-08-24 06:38:51 |
| {9E04CAB2-CC14-11DF-BB8C-A2F1DED72085} | 1 | 1 | 2022-08-24 06:38:50 |
| {A3D53349-6E61-4557-8FC7-0028EDCEEBF6} | 1 | 1 | 2022-08-24 06:38:50 |
| {B267E3AD-A825-4A09-82B9-EEC22AA3B847} | 1 | 1 | 2022-08-24 06:38:50 |
| {BCB48336-4DDD-48FF-BB0B-D3190DACB3E2} | 1 | 1 | 2022-08-24 06:38:50 |
| {CAA59E3C-4792-41A5-9909-6A6A8D32490E} | 1 | 1 | 2022-08-24 06:38:50 |
| {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} | 1 | 1 | 2022-08-24 06:38:51 |
| **Count** | 219 | 0 | 2023-11-08 06:58:14 |
| {F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442} | 1 | 1 | 2022-08-24 06:38:51 |

Values | UserAssist

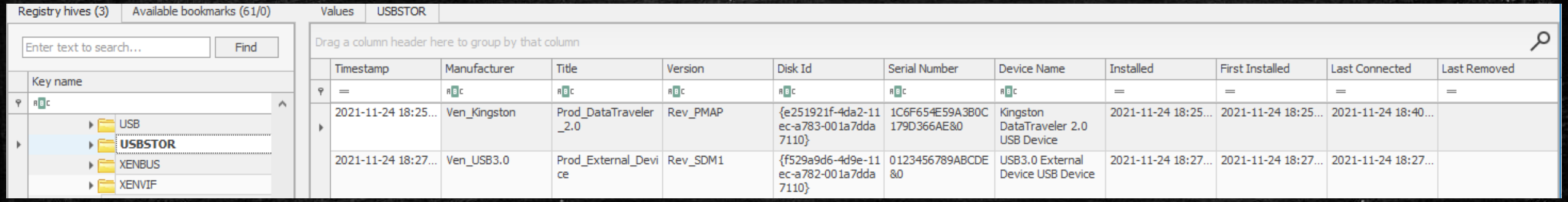
Drag a column header here to group by that column

| Program Name | Run Counter | Focus Count | Focus Time | Last Executed |
|---|---|---|---|---|
| UEME_CTLCUACount:ctor | 0 | 0 | 0d, 0h, 00m, 00s | |
| UEME_CTLSESSION | 120 | 3343 | 1d, 19h, 41m, 54s | |
| {System32}\SnippingTool.exe | 0 | 0 | 0d, 0h, 00m, 00s | 2023-07-02 14:53:54 |
| Microsoft.WindowsCalculator_8wekyb3d8bbwe!App | 0 | 0 | 0d, 0h, 00m, 00s | 2023-10-27 05:07:17 |
| {System32}\mspaint.exe | 0 | 0 | 0d, 0h, 00m, 00s | 2023-09-18 11:40:49 |
| {System32}\notepad.exe | 13 | 22 | 0d, 0h, 04m, 41s | 2023-11-07 12:18:39 |
| Microsoft.Windows.Explorer | 12 | 242 | 0d, 1h, 33m, 19s | 2023-11-07 10:22:25 |
| windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel | 0 | 0 | 0d, 0h, 00m, 00s | 2023-10-01 07:24:43 |
| Chrome | 12 | 515 | 0d, 4h, 50m, 24s | 2023-11-07 10:23:20 |
| Microsoft.SkyDrive.Desktop | 0 | 1 | 0d, 0h, 00m, 18s | 2023-10-24 04:55:10 |
| {Program Files X64}\VideoLAN\VLC\vlc.exe | 0 | 0 | 0d, 0h, 00m, 00s | 2023-06-20 05:09:54 |

# External Device/USB Forensics

# System – USBSTOR & USB

- \CurrentControlSet\Enum\USBSTOR
- \CurrentControlSet\Enum\USB
- Keep track of USB devices plugged into a system
  - Vendor id
  - Product id
  - Version



# System – First/Last Times

- \CurrentControlSet\Enum\USBSTOR\{Ven_Prod_Version}\{USBSerial#}\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####
  - 0064 – First Connection Time
  - 0066 – Last Connection Time
  - 0067 – Last Removal Time

# Setupapi dev logs for USB devices

- C:\Windows\inf\setupapi.dev.log

setupapi.dev.log - Notepad

File Edit Format View Help

```
>>>  [Device Install (Hardware initiated) - USB\VID_413C&PID_2113\5&34e9dd7a&0&1]
>>>  Section start 2023/10/17 07:59:50.398
     utl: {Select Drivers - USB\VID_413C&PID_2113\5&34e9dd7a&0&1} 07:59:50.797
     utl:      Driver Node:
     utl:           Status         - Selected
     utl:           Driver INF     - usb.inf (C:\WINDOWS\System32\DriverStore\FileRepository\usb.inf_amd64_e3c43be04fc074b6\usb.inf)
     utl:           Class GUID     - {36fc9e60-c465-11cf-8056-444553540000}
     utl:           Driver Version - 06/21/2006,10.0.19041.2546
     utl:           Configuration  - USB\COMPOSITE [Composite.Dev.NT]
     utl:           Driver Rank    - 00FF2003
     utl:           Signer Score   - Inbox (0D000003)
     utl: {Select Drivers - exit(0x00000000} 07:59:50.873
     dvi: {Core Device Install} 07:59:50.911
     dvi:      {Configure Device - USB\VID_413C&PID_2113\5&34e9dd7a&0&1} 07:59:50.914
     dvi:           Device Status: 0x01806400 [0x01 - 0xc0000495]
     dvi:           Parent Device: USB\ROOT_HUB30\4&2ca2a8ce&0&0
     sto:           {Configure Driver Package: C:\WINDOWS\System32\DriverStore\FileRepository\usb.inf_amd64_e3c43be04fc074b6\usb.inf}
     sto:                Source Filter  = USB\COMPOSITE
     inf:                Class GUID     = {36fc9e60-c465-11cf-8056-444553540000}
     inf:                Class Options  = Configurable BootCritical
     inf:                {Configure Driver: USB Composite Device}
     inf:                     Section Name = Composite.Dev.NT
```

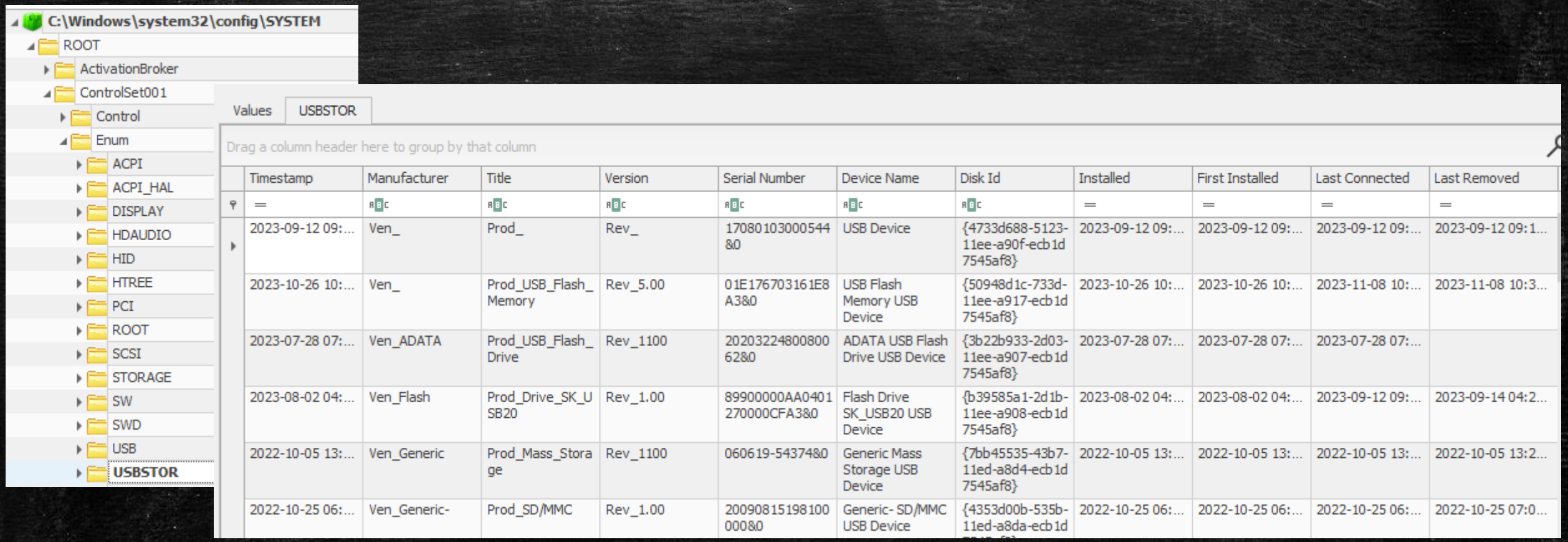
# USB Forensics Methology

- SYSTEM\CurrentControlSet\Enum\USBSTOR
  - Ven, Prod, Rev, Serial #, Device Name
- SYSTEM\CurrentControlSet\Enum\USB
  - VID & PID
- SOFTWARE\Microsoft\Windows Portable Device\Devices
  - Friendly Name through Serial #
- SYSTEM\MountedDevices
  - Drive Letter through Serial #
  - Volume GUID through Serial #

# USB Forensics Methology

- SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Versio\USB iSerial #\Properties\{83da6326-97a6-4088-9453-a1923f573b29\
  - 0064 → First Install (Also in setupapi.dev.log)
  - 0066 → Last connected (Win 8+) (also in ENUM\USB and MountPoints2 last write time)
  - 0067 → Last Removal (win 8+)
- C:Windows\inf\SetUpaapi.dev.log
  - First and last time connected through Serial #

# USBSTOR in Registry Explorer 2




| Timestamp | Manufacturer | Title | Version | Serial Number | Device Name | Disk Id | Installed | First Installed | Last Connected | Last Removed |
|---|---|---|---|---|---|---|---|---|---|---|
| 2023-09-12 09:... | Ven_ | Prod_ | Rev_ | 17080103000544&0 | USB Device | {4733d688-5123-11ee-a90f-ecb1d7545af8} | 2023-09-12 09:... | 2023-09-12 09:... | 2023-09-12 09:... | 2023-09-12 09:1... |
| 2023-10-26 10:... | Ven_ | Prod_USB_Flash_Memory | Rev_5.00 | 01E176703161E8A3&0 | USB Flash Memory USB Device | {50948d1c-733d-11ee-a917-ecb1d7545af8} | 2023-10-26 10:... | 2023-10-26 10:... | 2023-11-08 10:... | 2023-11-08 10:3... |
| 2023-07-28 07:... | Ven_ADATA | Prod_USB_Flash_Drive | Rev_1100 | 2020322480080062&0 | ADATA USB Flash Drive USB Device | {3b22b933-2d03-11ee-a907-ecb1d7545af8} | 2023-07-28 07:... | 2023-07-28 07:... | 2023-07-28 07:... | |
| 2023-08-02 04:... | Ven_Flash | Prod_Drive_SK_USB20 | Rev_1.00 | 89900000AA0401270000CFA3&0 | Flash Drive SK_USB20 USB Device | {b39585a1-2d1b-11ee-a908-ecb1d7545af8} | 2023-08-02 04:... | 2023-08-02 04:... | 2023-09-12 09:... | 2023-09-14 04:2... |
| 2022-10-05 13:... | Ven_Generic | Prod_Mass_Storage | Rev_1100 | 060619-54374&0 | Generic Mass Storage USB Device | {7bb45535-43b7-11ed-a8d4-ecb1d7545af8} | 2022-10-05 13:... | 2022-10-05 13:... | 2022-10-05 13:... | 2022-10-05 13:2... |
| 2022-10-25 06:... | Ven_Generic- | Prod_SD/MMC | Rev_1.00 | 200908151981000000&0 | Generic- SD/MMC USB Device | {4353d00b-535b-11ed-a8da-ecb1d | 2022-10-25 06:... | 2022-10-25 06:... | 2022-10-25 06:... | 2022-10-25 07:0... |

# Thank you for your patience!