

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

The image shows a screenshot of the Windows Registry Editor. The left pane displays a tree view of the registry structure. The right pane shows a list of registry values with their names, data types, and data.

Hives: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE

Keys: BCD00000000, HARDWARE, SAM, SECURITY, SOFTWARE

Subkeys: Classes, Clients, CVSM, DefaultUserEnvironment, Google, Intel, Microsoft, ODBC, OEM, OpenSSH, Partner, Policies, RegisteredApplications, Splunk, VMware, Inc., Windows, WOW6432Node

Value Names: (Default), ProductCode, ProductName, UpgradeCode

Data Types: REG_SZ

Values: (value not set), {F74E...}, Splunk Enterprise, {9C8D...}

Name	Type	Data
(Default)	REG_SZ	(value not set)
ProductCode	REG_SZ	{F74E...}
ProductName	REG_SZ	Splunk Enterprise
UpgradeCode	REG_SZ	{9C8D...}

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\\
 - USERCLASS.DAT (mounted on HKEY_CURRENT_USER\Software\CLASSES)
 - C:\Users\\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. User's most recently used files (MRU). 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

The screenshot shows the Autoruns utility window from Sysinternals. The window title is "Autoruns - Sysinternals: www.sysinternals.com". The interface includes a menu bar (File, Entry, Options, Help), a toolbar with icons for file operations and a filter input, and a main pane with a tree view of system components. The main pane displays a list of Autorun entries with columns for the entry name, description, publisher, image path, timestamp, and VirusTotal status. The "NimiPlaces" entry is highlighted in blue, and the "SunJavaUpdat..." entry is highlighted in red. The status bar at the bottom shows "Ready." and "Signed Microsoft Entries Hidden."

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				8/22/2013 5:37 PM	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Proces...	(Verified) Microsoft Windows	c:\windows\system32\cmd...	8/22/2013 12:03 PM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				4/7/2015 2:07 PM	
<input checked="" type="checkbox"/> Classic Start M...	Classic Start Menu	(Not verified) IvoSoft	c:\program files\classic shel...	1/19/2014 3:11 AM	
<input checked="" type="checkbox"/> openvpn-gui		(Verified) OpenVPN Techno...	c:\program files\openvpn\b...	8/22/2013 3:24 PM	
<input checked="" type="checkbox"/> VMware User ...	VMware Tools Core Service	(Verified) VMware	c:\program files\vmware\v...	3/22/2014 1:44 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				10/16/2015 6:51 AM	
<input checked="" type="checkbox"/> SunJavaUpdat...	Java Update Scheduler	(Verified) Oracle America	c:\program files (x86)\comm...	6/9/2015 4:08 AM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/14/2014 3:08 AM	
<input checked="" type="checkbox"/> NimiPlaces	Nimi Places	(Not verified) Nimi projects	c:\program files\nimi places...	2/12/2014 3:43 PM	0/51
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				2/12/2014 11:47 PM	
<input checked="" type="checkbox"/> CodeMeter Co...	CodeMeter Control Center	(Verified) WIBU-SYSTEMS ...	c:\program files (x86)\code...	9/6/2012 7:39 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2/13/2014 12:53 AM	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google Inc	c:\program files (x86)\googl...	11/7/2015 3:09 AM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler				4/1/2014 11:53 AM	
<input checked="" type="checkbox"/> SolDisk Mount ...	CBDisk Mount Notifier	(Verified) EldoS Corporation	c:\windows\system32\cbdi...	10/18/2013 1:22 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler				4/1/2014 11:53 AM	
<input checked="" type="checkbox"/> SolDisk Mount ...	CBDisk Mount Notifier	(Verified) EldoS Corporation	c:\windows\syswow64\cbd...	10/18/2013 1:22 PM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects				4/1/2014 11:53 AM	
<input checked="" type="checkbox"/> SolDisk Mount ...	CBDisk Mount Notifier	(Verified) EldoS Corporation	c:\windows\system32\cbdi...	10/18/2013 1:22 PM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects				4/1/2014 11:53 AM	
<input checked="" type="checkbox"/> SolDisk Mount ...	CBDisk Mount Notifier	(Verified) EldoS Corporation	c:\windows\syswow64\cbd...	10/18/2013 1:22 PM	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad				4/1/2014 11:53 AM	

Tools - Procmon

The image shows two overlapping windows of Process Monitor. The top window is partially obscured by the bottom window. In the top window, the 'Filter' menu item in the menu bar and the filter icon in the toolbar are circled in red. The bottom window shows a list of events with a context menu open over a selected row. The context menu includes options like 'Properties...', 'Stack...', 'Toggle Bookmark', 'Jump To...', 'Search Online...', 'Include 'RegOpenKey'', 'Exclude 'RegOpenKey'', 'Highlight 'RegOpenKey'', 'Copy 'RegOpenKey'', 'Edit Filter 'RegOpenKey'', 'Exclude Events Before', 'Exclude Events After', 'Include', 'Exclude', and 'Highlight'. The status bar at the bottom indicates 'Showing 10,007 of 77,237 events (12%)' and 'Backed by virtual memory'.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path

No events (capture disabled)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
1:49:0...	nessusd.exe	1548	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	
1:49:0...	nessusd.exe	1548	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	
1:49:0...	Explorer.EXE	124	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
1:49:0...	Explorer.EXE	124	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
1:49:0...	Explorer.EXE	124	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
1:49:0...	nessusd.exe	1548	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	REPARSE	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	SUCCESS	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	SUCCESS	Desired Access: Q...
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Type: REG_DWO...
1:49:0...	nessusd.exe	1548	RegClose	\Servi...	SUCCESS	
1:49:0...	nessusd.exe	1548	RegClose	\Servi...	SUCCESS	
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	REPARSE	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	SUCCESS	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	SUCCESS	Desired Access: Q...
1:49:0...	nessusd.exe	1548	RegClose	\Servi...	SUCCESS	Type: REG_DWO...
1:49:0...	nessusd.exe	1548	RegClose	\Servi...	SUCCESS	Type: REG_DWO...
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	REPARSE	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegOpen	\Servi...	SUCCESS	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegClose	\Servi...	SUCCESS	Desired Access: Q...
1:49:0...	nessusd.exe	1548	RegClose	\Servi...	SUCCESS	Desired Access: Q...
1:49:0...	nessusd.exe	1548	RegQuery	\Servi...	SUCCESS	Query: Handle Tag...
1:49:0...	nessusd.exe	1548	RegOpen	\Set\Ser...	REPARSE	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Desired Access: R...
1:49:0...	nessusd.exe	1548	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	BUFFER OVERFLOW	Length: 144
1:49:0...	nessusd.exe	1548	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	BUFFER OVERFLOW	Length: 144
1:49:0...	nessusd.exe	1548	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Type: REG_MULT...

Showing 10,007 of 77,237 events (12%) Backed by virtual memory

DIGITAL FORENSICS INCIDENT RESPONSE 1:50 PM 12/7/2015

Tools – FTK Imager

The image displays the FTK Imager 3.4.0.1 interface with several windows open:

- Obtain System Files:** A dialog box with a warning: "Warning: Please be aware that FTK Imager is obtaining the system files from the live system and not the acquired image." The destination is set to "C:\Users\sansforensics408\Desktop\CC15_VM". The "Options" section has "Password recovery and all registry files" selected.
- Select Source:** A dialog box with "Physical Drive" selected as the source evidence type.
- AccessData FTK Imager 3.4.0.1:** The main application window showing an evidence tree on the left and a file list on the right. The file list includes files like "sensorshidclassdriver.inf" and "setupapi.dev". A context menu is open over the file list with options like "Export Files..." and "Add to Custom Content Image (AD1)".

The main window also shows a "Custom Content Sources" dialog and a log window at the bottom right with the following content:

```
[Device Install Log]
OS Version = 6.3.9600
Service Pack = 0.0
Suite = 0x0300
ProductType = 1
Architecture = amd64

[BeginLog]

[Boot Session: 2014/02/12 08:40:07.120]

>>> [Device Install (Hardware initiated)] - SWD\IP_TUNNEL_VB
>>> Section start 2014/02/12 08:41:31.925
dvi: (Build Driver List) 08:41:32.815
dvi: Searching for hardware ID(s):
```

Tools – DCode

The image shows a Windows Registry Editor window with the path `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{60870F96-8FAF-4149-8DDD-95E6487BB420}` selected. The right pane displays a list of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	<u>e2 07 08 00 05 00 03 00 15 00 09 00 10 00 bf 01</u>
DateLastConne...	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

A red arrow points from the underlined hex value in the 'DateCreated' row to the 'Value to Decode' field of the DCode v4.02a (Build: 9306) application window. The DCode window shows the following configuration:

- Add Bias: UTC 00:00
- Decode Format: Windows: 128 bit SYSTEM Structure
- Example: D9070B00010002000600090013000000
- Value to Decode: E207080005000300150009001000BF01
- Date & Time: Fri, 03 August 2018 21:09:16.447

The DCode window also includes a 'Decode' button and the website www.digital-detective.co.uk.

Tools – RegRipper

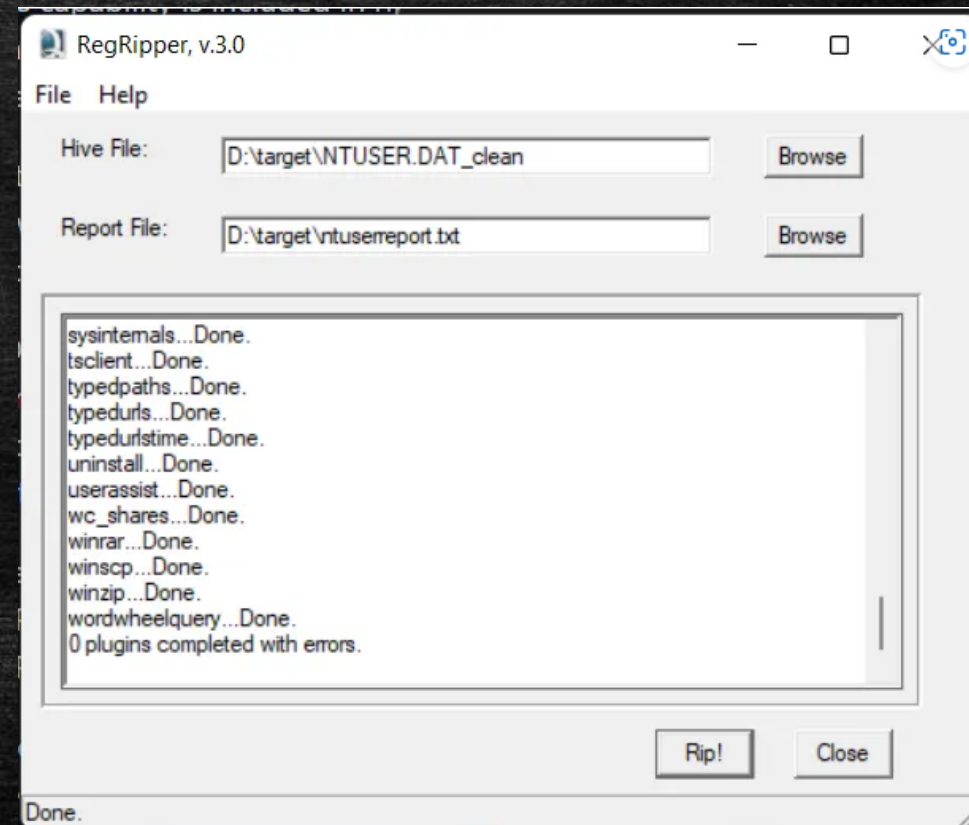
```
Administrator: Command Prompt
C:\Users\sansforensics408\Desktop\Forensic Tools\Registry Tools\regripper\tools>rip.exe
Rip v.2.8 20130801 - CLI RegRipper tool
Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]
Parse Windows Registry files, using either a single module, or a plugins file.

-r Reg hive file...Registry hive file to parse
-g .....Guess the hive file (experimental)
-f [profile].....use the plugin file (default: plugins\plugins)
-p plugin module...use only this module
-l .....list all plugins
-c .....Output list in CSV format (use with -l)
-s system name.....Server name (TLN support)
-u username.....User name (TLN support)
-h.....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.
copyright 2013 Quantum Analytics Research, LLC

C:\Users\sansforensics408\Desktop\Forensic Tools\Registry Tools\regripper\tools>
```



Tools – Registry Explorer

The screenshot displays the Registry Explorer application window. The left pane shows a tree view of the registry, with the path `C:\Users\User\Desktop\Re...` expanded to show the `Users` subkey. The right pane shows the `Values` pane, which is currently empty. The status bar at the bottom indicates the selected key is `SAM\Domains\Account\Users\Names\User` and shows 1 of 1 values shown.

Key name	# values	# subkeys	Last write timestamp
ROOT	0	1	2018-08-03 20:02:59
SAM	2	3	2018-08-03 20:02:59
Domains	1	2	2018-08-03 20:02:59
Account	2	3	2019-01-23 20:57:18
Aliases	1	2	2018-08-03 20:02:59
Groups	1	2	2018-08-03 20:02:59
Users	1	6	2018-08-03 20:52:15
000001F4	3	0	2018-08-03 20:07:09
000001F5	3	0	2018-08-03 20:07:09
000001F7	4	0	2018-08-03 20:07:09
000001F8	5	0	2018-08-03 20:07:09
000003E9	5	0	2019-03-17 17:50:40
Names	1	6	2018-08-03 20:52:15
Admini...	1	0	2018-08-03 20:10:25
Defaul...	1	0	2018-08-03 20:10:25
Guest	1	0	2018-08-03 20:10:25
User	1	0	2018-08-03 20:14:22
WDAG...	1	0	2018-08-03 20:10:25
default...	0	0	2018-08-03 20:09:37
Builtin	2	3	2018-08-03 22:55:51
Aliases	1	21	2018-08-03 20:02:59
00000220	1	0	2018-08-03 20:14:52
00000221	1	0	2018-08-03 20:52:15
00000222	1	0	2018-08-03 20:02:59
00000223	1	0	2018-08-03 20:02:59
00000227	1	0	2018-08-03 20:02:59
00000228	1	0	2018-08-03 20:02:59

Value Name	Value Type	Data	Valu...	Is Deleted	Data Record Realloc.
(default)	RegUnknown	00-00-00-00		<input type="checkbox"/>	<input type="checkbox"/>

Key: SAM\Domains\Account\Users\Names\User
Value: (default) Collapse all hives
Selected hive: REGISTRY_MACHINE_SAM Last write: 2018-08-03 20:14:22 1 of 1 values shown (100.00%) Load complete Hidden keys: 0 1

Security Hive File

Security – System and Domain SIDs

- SECURITY/Policy/Accounts
- S-R-X-Y₁-Y₂-Y_{n-1}-Y_n-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/PoIAdtEv
 - 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

The image shows a screenshot of the Windows Registry Editor. On the left, the tree view shows the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`, with the `CurrentVersion` folder highlighted by a red circle. On the right, a list of registry values is displayed, with `InstallDate`, `ProductName`, and `ReleaseId` highlighted by red circles.

Value Name	Value Type	Data	Value Slack
SystemRoot	RegSz	C:\WINDOWS	00-00-00-00-00-00
BaseBuildRevisionNumber	RegDword	1	
BuildBranch	RegSz	vb_release	00-00-00-00-00-00
BuildGUID	RegSz	fffffff-ffff-ffff-ffffffffffff	00-00
BuildLab	RegSz	19041.vb_release.191206-1406	00-00
BuildLabEx	RegSz	19041.1.amd64fre.vb_release.191206-1...	00-00-00-00
CompositionEditionID	RegSz	Enterprise	00-00-00-00-00-05
CurrentBuild	RegSz	19044	
CurrentBuildNumber	RegSz	19044	
CurrentMajorVersionNumber	RegDword	10	
CurrentMinorVersionNumber	RegDword	0	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00
CurrentVersion	RegSz	6.3	00-00-00-00
EditionID	RegSz	Professional	00-00
EditionSubManufacturer	RegSz		
EditionSubstring	RegSz		
EditionSubVersion	RegSz		
InstallationType	RegSz	Client	00-00-00-00-00-00
InstallDate	RegDword	1637778211	
ProductName	RegSz	Windows 10 Pro	72-00-70-00-72-00-69-00-73-00-65-00-0...
ReleaseId	RegSz	2009	00-00
SoftwareType	RegSz	System	00-00-00-00-00-00

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

Computer\HKEY_LOCAL_MACHINE\SYSTEM>Select

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000001 (1)

System – ComputerName and TimeZoneInformation

Path	# values	# subkeys	Last write timestamp
C:\Windows\system32\config\SYSTEM			
ROOT	0	17	2023-11-03 06:59:24
ControlSet001	0	5	2019-12-07 09:15:07
Control	12	127	2023-11-03 07:00:51
ComputerName	0	1	2023-11-03 07:00:19
ComputerName	2	0	2022-08-24 06:28:33

Value Name	Value Data	Value Data Raw
ComputerName	REG_SZ	DESKTOP-E4NUK4Q
(default)	REG_SZ	mnmsrvc

Key name	# values	# subkeys	Last write timestamp
C:\Windows\system32\config\SYSTEM			
ROOT	0	17	2023-11-03 06:59:24
ControlSet001	0	5	2019-12-07 09:15:07
Control	12	127	2023-11-03 07:00:51
TimeZoneInformation	10	0	2023-10-29 01:00:00

Value Name	Value Data	Value Data Raw
Bias	-120	4294967176
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-361	@tzres.dll,-361
DaylightStart	Month 3, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 3:0:0:0	00-00-03-00-05-00-03-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-362	@tzres.dll,-362
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 4:0:0:0	00-00-0A-00-05-00-04-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	GTB Standard Time	GTB Standard Time
ActiveTimeBias	-120	4294967176

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

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AJRouter

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	@%SystemRoot%\system32\AJRouter.dll,-1
DisplayName	REG_SZ	@%SystemRoot%\system32\AJRouter.dll,-2
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 b8 0b...
ImagePath	REG_EXPAND_SZ	%SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted -p
ObjectName	REG_SZ	NT AUTHORITY\LocalService
ServiceSid type	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000020 (32)

System – CurrentControlSet\Services

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StateRepository\parameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\windows.staterepository.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000000 (0)

System – Network Elements

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

System – Interfaces

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{115c13db-8e2b-477c-806e-1f029a08b61e}

- Adapters
- DNSRegisteredAdapters
- Interfaces
 - {0c54b95b-c7fd-4600-8050-4ebfc836ccf2}
 - {115c13db-8e2b-477c-806e-1f029a08b61e}
 - {552cc8dd-73d2-404a-bc9c-6240213b8513}
 - {6E06F030-7526-11D2-BAF4-00600815A4BD}
 - {8837712b-96cf-4529-b0e3-80cbfd385ed0}
 - {88b5ac91-2a3a-11eb-b696-806e6f6e6963}
 - {8beecddb-c2f9-41a8-a8f5-d5ae424b03b9}
 - {adf0adf1-af8d-11e6-a8c1-806e6f6e6963}
 - {d4142bc6-3304-48e3-bd19-414c029937bc}
 - {d7dbd904-e2a6-4339-8428-db9ef9f250b3}
 - {f828e607-8e8d-497f-a985-806239e7988d}
- NsiObjectSecurity
- PersistentRoutes
- Winsock
- Performance
- Security
- ServiceProvider
- Tcpip6
- TCPIP6TUNNEL
- tcpipreg
- TCPIPTUNNEL
- tdx
- Telemetry

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000001 (1)
DhcpDefaultGateway	REG_MULTI_SZ	192.168.24.1
DhcpDomain	REG_SZ	agora.cdd
DhcpGatewayHardware	REG_BINARY	c0 a8 18 01 06 00 00 00 40 62 31 0b 8b 10
DhcpGatewayHardwareCount	REG_DWORD	0x00000001 (1)
DhcpInterfaceOptions	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DhcpIPAddress	REG_SZ	192.168.24.51
DhcpNameServer	REG_SZ	192.168.24.3 192.168.24.1
DhcpServer	REG_SZ	192.168.24.1
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000001 (1)
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x00001c20 (7200)
LeaseObtainedTime	REG_DWORD	0x654a26db (1699358427)
LeaseTerminatesTime	REG_DWORD	0x654a42fb (1699365627)
NameServer	REG_SZ	
T1	REG_DWORD	0x654a34eb (1699362027)
T2	REG_DWORD	0x654a3f77 (1699364727)

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: – 31d6cfeod16aeg31b73c59d7e0oco89co

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
KINagSvc	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

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

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\...ar\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

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:::
```

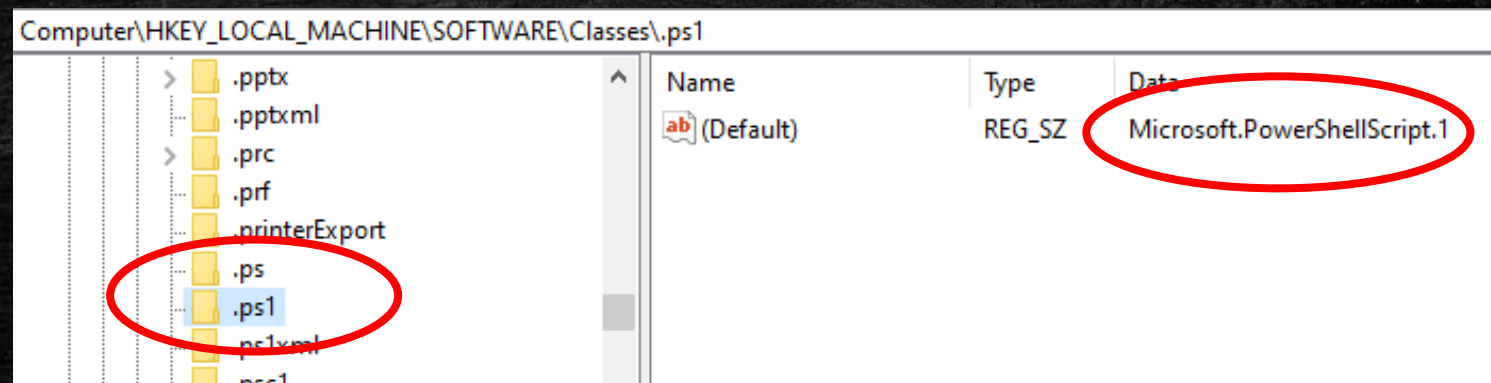
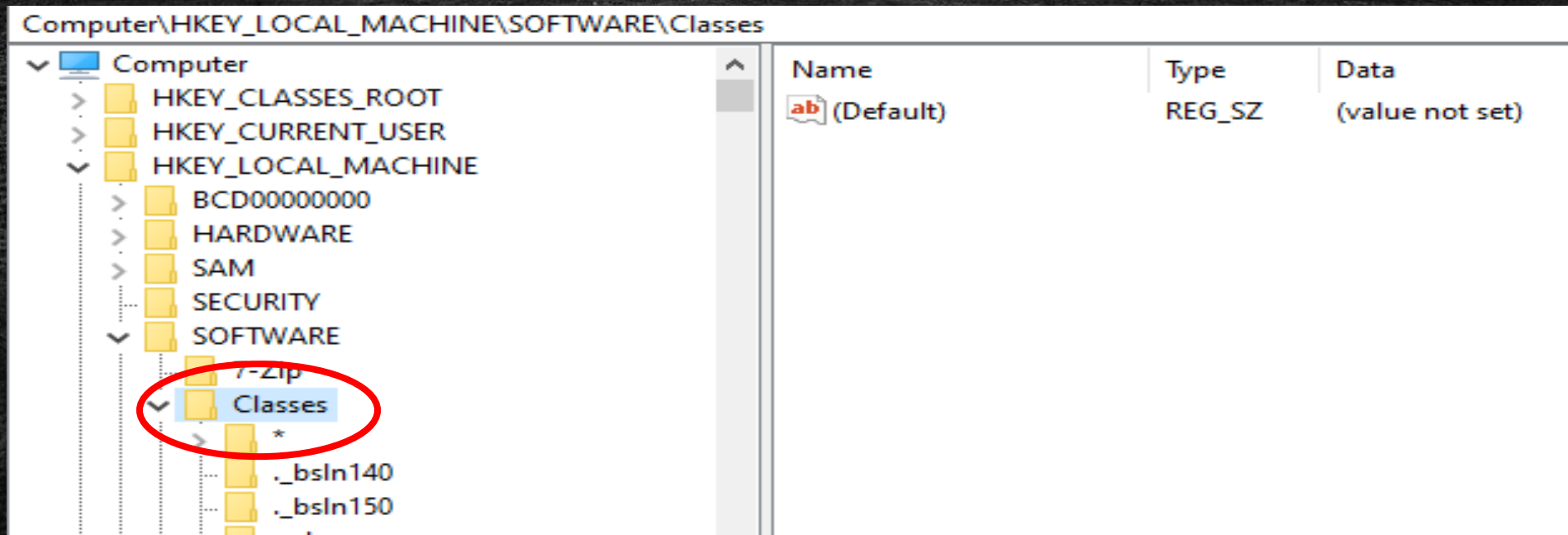
Software

- 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

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet\Google Chrome\shell\open\command

Name	Type	Data
(Default)	REG_SZ	"C:\Program Files\Google\Chrome\Application\chrome.exe"

Software – Past Networks

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

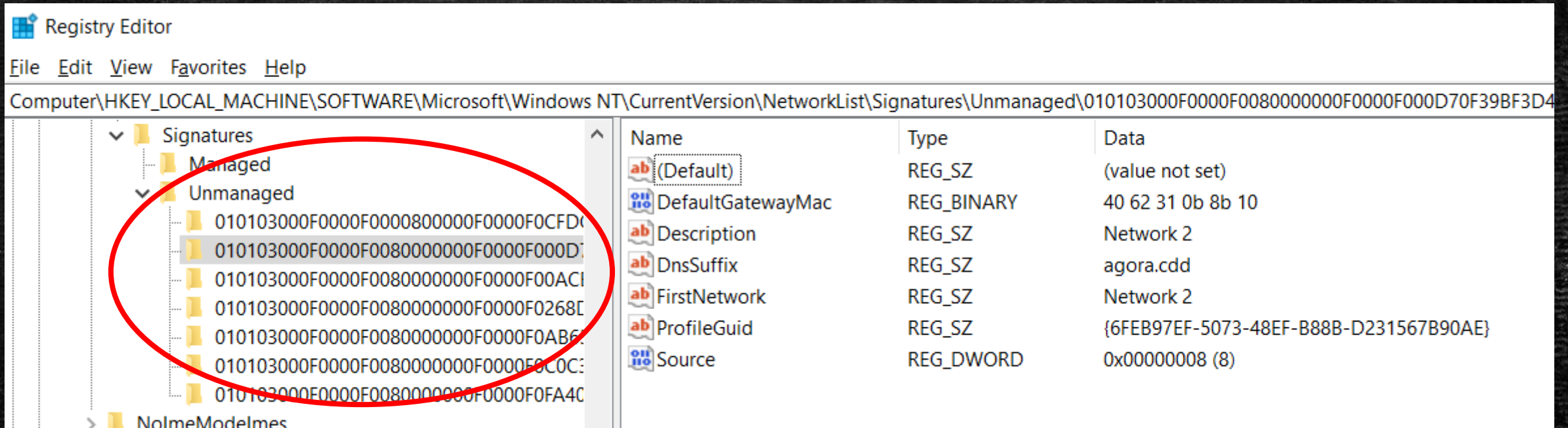
Software – Past Networks

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\010103000F0000F0080000000F0000F000D70F39BF3D4

Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	40 62 31 0b 8b 10
Description	REG_SZ	Network 2
DnsSuffix	REG_SZ	agora.cdd
FirstNetwork	REG_SZ	Network 2
ProfileGuid	REG_SZ	{6FEB97EF-5073-48EF-B88B-D231567B90AE}
Source	REG_DWORD	0x00000008 (8)



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

The screenshot displays the Windows Registry Editor interface. On the left, the tree view shows the path `Software\CurrentVersion\Run` selected, with the `Run` folder highlighted by a red circle. The right pane shows the values for this key, also circled in red. The values table is as follows:

Value Name	Value Type	Data
<code>egui</code>	RegSz	"C:\Program Files\ESET\ESET Security\ecmds.exe" /run /hide /proxy
<code>RTHDVCPL</code>	RegSz	"C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe" -s
<code>SecurityHealth</code>	RegExpandSz	%windir%\system32\SecurityHealthSystray.exe
<code>ISCT Tray</code>	RegSz	C:\Program Files\Intel\Intel(R) Smart Connect Technology Agent\SCTsysTray8.exe
<code>RtsCM</code>	RegSz	RTSCM64.EXE

Software – Other Autoruns Locations

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

Key name	# values	# subkeys	Last write timestamp
C:\Windows\system32\config\SYSTEM	=	=	=
ROOT	0	17	2023-11-03 06:59:24
ActivationBroker	0	1	2019-12-07 09:15:08
ControlSet001	0	5	2019-12-07 09:15:07
Control	12	127	2023-11-03 07:00:51
Enum	35	15	2023-10-17 04:59:52
Hardware Profiles	0	2	2023-11-03 06:59:24
Policies	0	0	2023-06-07 11:09:08
Services	0	793	2023-11-07 07:17:37
DriverDatabase	6	4	2023-10-18 21:20:05
HardwareConfig	2	1	2023-11-03 06:59:24
Input	0	2	2019-12-07 09:15:07
Keyboard Layout	0	2	2019-12-07 09:49:45
Mouse	0	2	2023-08-24 07:40:56

Name	Description	Display Name	Start Mode	Service Type	Name Key Last Write	Parameters Key La...
.NET CLR Data			Disabled	Adapter	2022-09-14 04:50:...	
.NET CLR Networking			Disabled	Adapter	2022-09-14 04:50:...	
.NET CLR Networking 4.0.0.0			Disabled	Adapter	2019-12-07 09:15:...	
.NET Data Provider for Oracle			Disabled	Adapter	2019-12-07 09:15:...	
.NET Data Provider for SqlServer			Disabled	Adapter	2019-12-07 09:15:...	
.NET Memory Cache 4.0			Disabled	Adapter	2019-12-07 09:15:...	
.NETFramework			Disabled	Adapter	2019-12-07 09:15:...	
1394ohci		@1394.inf,%PCI\CC_OC0010.DeviceDesc%;1394 OHCI Compliant Host Controller	Manual	KernelDriver	2020-11-19 07:45:...	

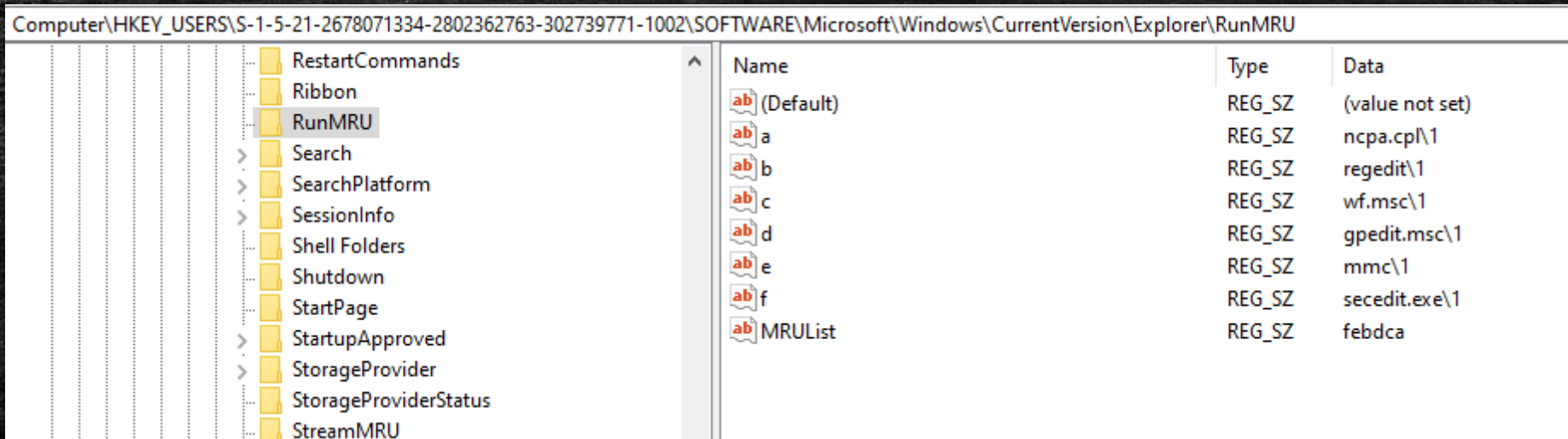
Usage of Files/Folders

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



The screenshot shows the Windows Registry Editor window with the path `Computer\HKEY_USERS\S-1-5-21-2678071334-2802362763-302739771-1002\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU` selected. The left pane shows a tree view of folders, with `RunMRU` highlighted. The right pane displays a list of registry values.

Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	ncpa.cpl\1
b	REG_SZ	regedit\1
c	REG_SZ	wf.msc\1
d	REG_SZ	gpedit.msc\1
e	REG_SZ	mmc\1
f	REG_SZ	secedit.exe\1
MRUList	REG_SZ	febdca

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

Computer\HKEY_USERS\S-1-5-21-2678071334-2802362763-302739771-1002\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BIN...	53 00 70 00 6c 00 75 00 6e 00 6b 00 00 00
1	REG_BIN...	57 00 49 00 4e 00 41 00 44 00 48 00 44 00 00 00

Value name: 0

Value data:

00000000	53	00	70	00	6C	00	75	00	S . p . l . u .
00000008	6E	00	6B	00	00	00			n . k . . .

OK Cancel

NTUSER.DAT & USRCLASS.DAT - RecentDocs

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (31/0) View Help

Registry hives (2) Available bookmarks (59/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
HKEY_CURRENT_USER	=	=	=
Package Installation	1	0	2023-10-19 04:55:04
RecentDocs	151	89	2023-11-07 12:18:41
RestartCommands	0	0	2023-10-19 04:44:53
Ribbon	2	0	2022-11-30 15:58:21
RunMRU	7	0	2023-06-07 11:22:29
Search	0	2	2022-08-24 07:40:22
SearchPlatform	0	1	2022-08-24 06:37:37
Shell Folders	31	0	2022-08-24 07:51:57
Shutdown	1	0	2023-11-03 07:04:42
StartupPage	2	0	2022-08-24 07:40:23
StartupApproved	0	2	2022-09-16 04:55:02
StorageProvider	0	1	2023-05-19 05:26:52
StorageProviderStatus	1	0	2023-09-18 11:34:44
StreamMRU	3	0	2023-05-16 08:20:02
Streams	0	3	2022-10-18 08:53:03
StuckRects3	1	0	2022-08-24 07:40:23
TabletMode	1	0	2022-08-24 07:53:57

Values Recent documents

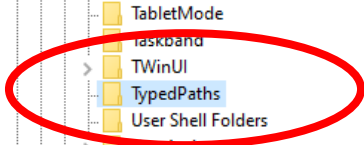
Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Open
HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	HKEY_CURRENT_USER	=	=
.xlsx	1	20230526131733_LECmd_Output.xlsx	20230526131733_LECmd_Output.xlsx.lnk		10
.vmx	1	SOF-ELK.vmx	SOF-ELK.lnk		2
.txt	1	result2.txt	result2.txt.lnk		17
.tgz	1	alert-manager_2011.tgz	alert-manager_3011.lnk		7
.sql	1	VelociraptorForensicAnalysis.sql	VelociraptorForensicAnalysis.lnk		1
.sh	1	install.sh	install.sh.lnk		1
.rules	1	blacklist.rules	blacklist.rules.lnk		2
.rtf	1	CompTIA CySA_Cybersecurity Analyst Certif - Brent Chapman.rtf	CompTIA CySA_Cybersecurity Analyst Certif - Brent Chapman.lnk		5
.rar	1	q6BIE8s_WindowsSecurityCrashCourse.1.4.part2.rar	q6BIE8s_WindowsSecurityCrashCourse.1.4.part2.lnk		9
.qradar	1	th.mpenos.QRadar	th.mpenos.QRadar (2).lnk		1
.py	1	use_extracted_parts.py	use_extracted_parts.py.lnk		19
.ps1	1	Update_SavedSearches_From_Sigma_YML.ps1	Update_SavedSearches_From_Sigma_YML.ps1.lnk		8
.pptx	1	(NU-EPG) CC22 MPC - SL100.pptx	(NU-EPG) CC22 MPC - SL100.lnk		2

Total rows: 710

NTUSER.DAT & USRCLASS.DAT - TypedPaths

Computer\HKEY_USERS\S-1-5-21-2678071334-2802362763-302739771-1002\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths



Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	C:\Windows\System32\config
url10	REG_SZ	C:\Program Files (x86)\Free RAR Password Recovery
url11	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\sysmon
url12	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\registry
url13	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\raw_access_thread
url14	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\process_creation
url15	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\process_access
url16	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\placeholder\process_creation
url17	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\pipe_created
url18	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\network_connection
url19	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\image_load
url2	REG_SZ	C:\Program Files\Velociraptor
url20	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\file
url21	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\emerging-threats
url22	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\driver_load
url23	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\dns_query
url24	REG_SZ	C:\sigma_rules\hayabusa-2.7.0-win-64-bit\rules\sigma\sysmon\create_stream_hash
url25	REG_SZ	C:\Windows\System32\winevt
url3	REG_SZ	C:\Program Files
url4	REG_SZ	C:\Users\thoma\Downloads\loki
url5	REG_SZ	C:\Users\thoma\OneDrive\Documents\Virtual Machines\Cisco VMs
url6	REG_SZ	Documents
url7	REG_SZ	C:\Users\thoma\VirtualBox VMs
url8	REG_SZ	C:\Users\thoma\OneDrive\Documents\Virtual Machines
url9	REG_SZ	C:\Windows\System32\drivers

NTUSER.DAT & USRCLASS.DAT - ComDlg32

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

NTUSER.DAT & USRCLASS.DAT - OpenSavePidIMRU

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (31/0) View Help

Registry hives (2) Available bookmarks (59/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Computer	=	=	=
CISave	0	1	2022-08-25 05:01:13
CLSID	0	5	2022-08-24 06:39:36
ComDlg32	0	5	2022-11-30 16:06:43
CISizeMRU	43	0	2023-11-07 10:55:01
FirstFolder	5	0	2023-10-24 11:37:15
LastVisitedPidIMRU	25	0	2023-11-07 10:54:51
LastVisitedPidIMRULegacy	2	0	2022-12-01 13:01:54
OpenSavePidIMRU	0	58	2023-10-31 10:53:32
Desktop	0	1	2022-08-24 06:39:36
Discardable	0	1	2022-08-24 07:51:17
DiskSpaceChecking	1	0	2023-02-08 05:54:50
ExtractionWizard	1	0	2022-09-20 09:57:04
FeatureUsage	1	5	2022-09-16 04:34:21
FileExts	0	320	2023-11-03 09:42:38
HideDesktopIcons	0	1	2022-08-24 06:39:37
LogonStats	2	0	2022-08-24 07:51:01
LowRegistry	0	0	2022-08-24 07:51:18

Values ComDlg32 OpenSavePidIMRU

Drag a column header here to group by that column

Extension	Value Name	Mru Position	Absolute Path	Opened On
*	3	0	My Computer\C:\Windows\System32\config\system	2023-11-07 10:36:12
0-linux-amd64-musl	0	0	My Computer\Downloads\Org_SOCLab_velociraptor-v0.7.0-linux-amd64-musl	2023-09-13 07:55:12
api	0	0	OneDrive\IDRtools\SysinternalsSuite\key.api	2022-10-25 09:35:21
bat	13	0	My Computer\C:\sigma_rules\MITRE_SIGMA\auditpolicy.bat	2023-06-09 09:06:17
cer	0	0	My Computer\F:\Horizon\UCA_root.cer	2023-07-28 07:47:01
conf	0	0	My Computer\C:\sigma_rules\savedsearches.conf	2023-08-07 16:13:19
config	0	0	My Computer\C:\Snort\etc\classification1.config	2023-04-18 08:43:46
csv	10	0	My Computer\Downloads\2023-11-07-data_export.csv	2023-11-07 08:14:21
db	1	0	My Computer\Downloads\welm_combined.db	2023-08-11 08:28:24
deb	0	0	My Computer\Downloads\velociraptor_0.6.9_client.deb	2023-08-01 11:57:38
dmp	0	0	My Computer\Desktop\sass.dmp	2023-08-17 11:01:13
doc	0	0	OneNote\https://d.docs.live.net/6bdb6832da013598/\Προσωπικό Αρχείο\Εγγραφα\Army\ΓΕΕΘΑ Ε5\ΑΝΑΦΟΡΑ ΑΔΕΙΑΣ ΓΙΑ ΕΞΩΤΕΡΙΚΟ (Πολωνία).doc	2022-10-13 05:38:42
docx	9	0	OneDrive\Προσωπικό Αρχείο\Εγγραφα\Homework\RangeForce\Server Protection Overview.docx	2023-10-04 06:38:15
eml	1	0	My Computer\Documents\mail.eml	2023-06-14 16:50:14

Total rows: 366

NTUSER.DAT & USRCLASS.DAT - LastVisitedPidMRU

Values		ComDlg32 LastVisitedPidMRU			
Drag a column header here to group by that column					
	Value Name	Mru Position	Executable	Absolute Path	Opened On
▼	ntuser.dat	=	ntuser.dat	ntuser.dat	
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\Eγγραφα\Army\ΓΕΕΘΑ E5\Deployment\Velociraptor	
22		4	{D6637525-53BD-49E9-9E1B-D5E744F7A9DF}	OneDrive\Προσωπικό Αρχείο\Eγγραφα\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\Eγγραφα\Army\ΓΕΕΘΑ E5	
0		9	chrome.exe	My Computer\Downloads	
3		10	{EC04B61C-3E7B-4750-B9C5-95446FA443B2}	OneDrive\Προσωπικό Αρχείο\Eγγραφα\Homework\RangeForce	
▶		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

Computer\HKEY_USERS\S-1-5-21-2678071334-2802362763-302739771-1002\SOFTWARE\Microsoft\Windows\Shell\BagMRU\0\0\0\4\0\0

Name	Type	Data
(Default)	REG_SZ	(value not set)
MRUListEx	REG_BIN...	ff ff ff ff
NodeSlot	REG_DW...	0x00000119 (281)

NTUSER.DAT & USRCLASS.DAT - ShellBags

ShellBags Explorer v1.4.0.0

File Tools Help

Value

Desktop

- @user.home
 - engage
 - osgi
- Computers and Devices
- Control Panel
- E:\ul>- tools
 - forecopy
 - kape
 - SysinternalsSuite
 - ZimmermanTools**

- F:\
- Home Folder
- My Computer
- 3D Objects
- C:\ul>- Intel
- MGLauncher
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- swsetup
- SP101955
- SP112162
- sp138267
- sp74656
- SP74763
- System.sav
- Users
- Windows
- Desktop
- Documents
- Downloads
- @user.home
- HP Downloads

Drag a column header here to group by that column

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On
...	No im...	...	=	=	=	=

Summary Details Hex

Name: ZimmermanTools
Absolute path: Desktop\E:\tools\ZimmermanTools
Key-Value name path: BagMRU9\0-1
Registry last write time: 2023-11-06 08:42:22.731

Target timestamps
Created on: 2022-09-27 06:03:20.000
Modified on: 2022-09-27 06:03:48.000
Last accessed on: 2023-11-06 07:20:42.000

Miscellaneous
Shell type: Directory
Node slot: 195
MRU position: 2

'UsrClass.dat' Registry hive loaded in 0.9121 seconds! 0 shellbags loaded in 0.0000 seconds Time zone: UTC 0 of 0 rows visible (NaN)

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}

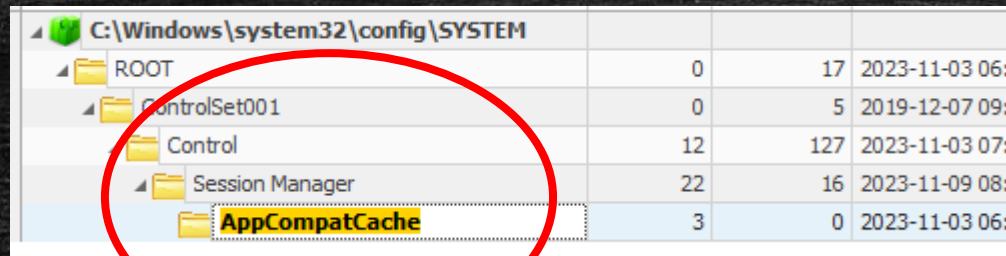
System – BAM/DAM

Key name	# values	# subkeys	Last write time	Program	Execution Time
HKEY_LOCAL_MACHINE	=	=	=	HKEY_LOCAL_MACHINE	=
bam	7	1	2020-11-19 0	Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy	2023-11-03 07:05:11
State	0	1	2020-11-19 0	Microsoft.Windows.Client.CBS_cw5n1h2txyewy	2023-11-09 14:28:53
UserSettings	0	11	2023-10-01 0	Microsoft.Windows.Search_cw5n1h2txyewy	2023-11-09 13:27:20
S-1-5-18	6	0	2023-11-09 1	Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy	2023-11-07 08:50:08
S-1-5-21-2678071334-2...	75	0	2023-11-09 1	Microsoft.WindowsStore_8wekyb3d8bbwe	2023-11-09 05:42:21
S-1-5-21-2678071334-28023...	3	0	2022-09-22 0	Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2023-11-03 07:06:41
S-1-5-21-2678071334-28023...	5	0	2022-08-24 0	Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	2023-11-09 14:29:48
S-1-5-90-0-1	3	0	2023-11-03 0	Microsoft.SkypeApp_kzf8qxf38zg5c	2023-11-07 10:55:27
S-1-5-90-0-2	2	0	2023-10-19 2	Microsoft.LockApp_cw5n1h2txyewy	2023-11-03 13:11:12
S-1-5-90-0-3	2	0	2023-10-24 2	microsoft.windowscommunicationsapps_8wekyb3d8bbwe	2023-11-09 13:54:16
S-1-5-90-0-4	2	0	2023-10-04 0	windows.immersivecontrolpanel_cw5n1h2txyewy	2023-10-19 04:55:51
S-1-5-90-0-5	2	0	2023-10-05 2	Microsoft.GetHelp_8wekyb3d8bbwe	2023-05-16 07:20:01
S-1-5-90-0-6	2	0	2023-10-07 2	Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	2023-11-02 23:48:41
S-1-5-90-0-8	2	0	2023-10-08 2	Microsoft.Windows.Photos_8wekyb3d8bbwe	2023-09-20 07:38:28
BasicDisplay	7	2	2023-11-03 0		

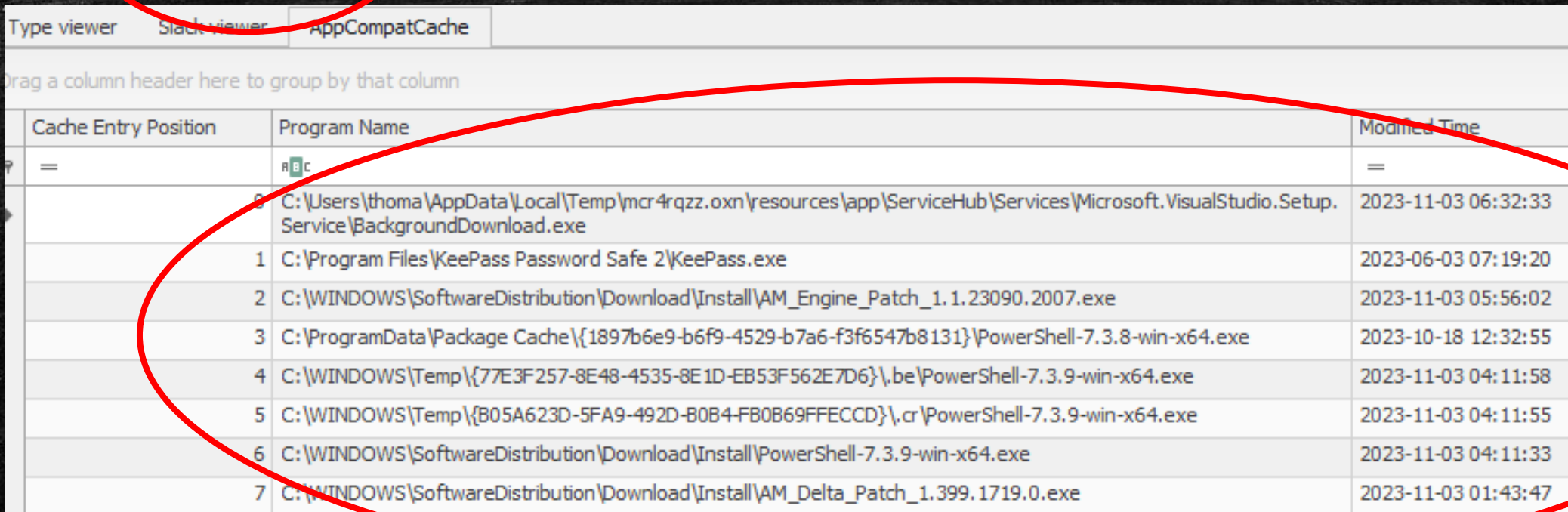
System – ShimCache

- 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



Folder Name	Attributes	Size	Count	Modified Time
ROOT		0	17	2023-11-03 06:32:33
ControlSet001		0	5	2019-12-07 09:00:00
Control		12	127	2023-11-03 07:00:00
Session Manager		22	16	2023-11-09 08:00:00
AppCompatCache		3	0	2023-11-03 06:32:33



Type viewer	ShimCache viewer	AppCompatCache
Drag a column header here to group by that column		
Cache Entry Position	Program Name	Modified Time
=	REG	=
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-FB0B69FFECDD}\.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

Values Amcache-InventoryApplicationFile

Drag a column header here to group by that column

Key name	# values	# subkeys	Last write time	Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
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							
InventoryDevicePnp	4	131	2023-11-09 11:4							
				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	f926cfe6bbe698d0e293ffd6eff3addfc6c195a

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

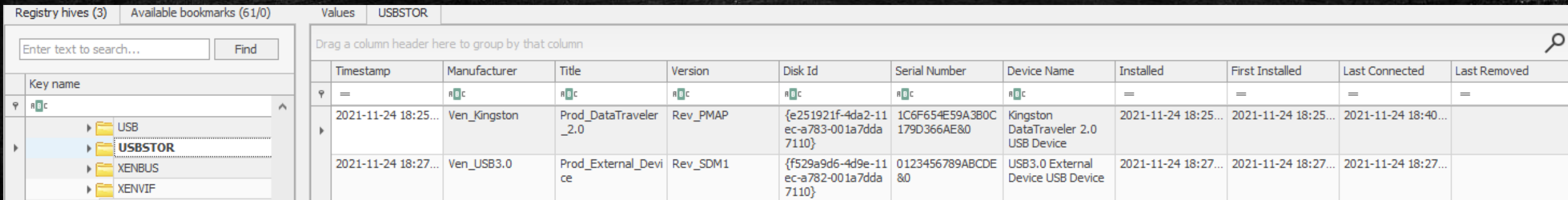
UserAssist	0	9	2022-08-24 06:38:51
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}	1	1	2022-08-24 06:38:50
{A3D53349-6E61-4557-8FC7-0028EDCEE6F6}	1	1	2022-08-24 06:38:50
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	1	1	2022-08-24 06:38:50
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}	1	1	2022-08-24 06:38:50
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	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
{E2A1CB5A-F3CC-4A2E-AF9D-505A7009D442}	1	1	2022-08-24 06:38:51

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



The screenshot shows the Windows Registry Editor with the path \CurrentControlSet\Enum\USBSTOR selected. The left pane shows the tree structure with USBSTOR highlighted. The right pane displays a table of registry values for USBSTOR, which correspond to USB devices.

Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 18:25...	2021-11-24 18:25...	2021-11-24 18:40...	
2021-11-24 18:27...	Ven_USB3.0	Prod_External_Device	Rev_SDM1	{f529a9d6-4d9e-11ec-a782-001a7dda7110}	0123456789ABCDE&0	USB3.0 External Device USB Device	2021-11-24 18:27...	2021-11-24 18:27...	2021-11-24 18:27...	

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 Methodology

- 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 Methodology

- 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\SetUpapi.dev.log
 - First and last time connected through Serial #

USBSTOR in Registry Explorer 2

The screenshot shows the Windows Registry Editor with the path `C:\Windows\system32\config\SYSTEM` expanded to `ControlSet001\Control\Enum\USBSTOR`. The right pane displays the values for the `USBSTOR` registry key, which are organized into a table with columns for various device attributes.

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	2009081519810000&0	Generic- SD/MMC USB Device	{4353d00b-535b-11ed-a8da-ecb1d7545af8}	2022-10-25 06:...	2022-10-25 06:...	2022-10-25 06:...	2022-10-25 07:0...

Thank you for your patience!
