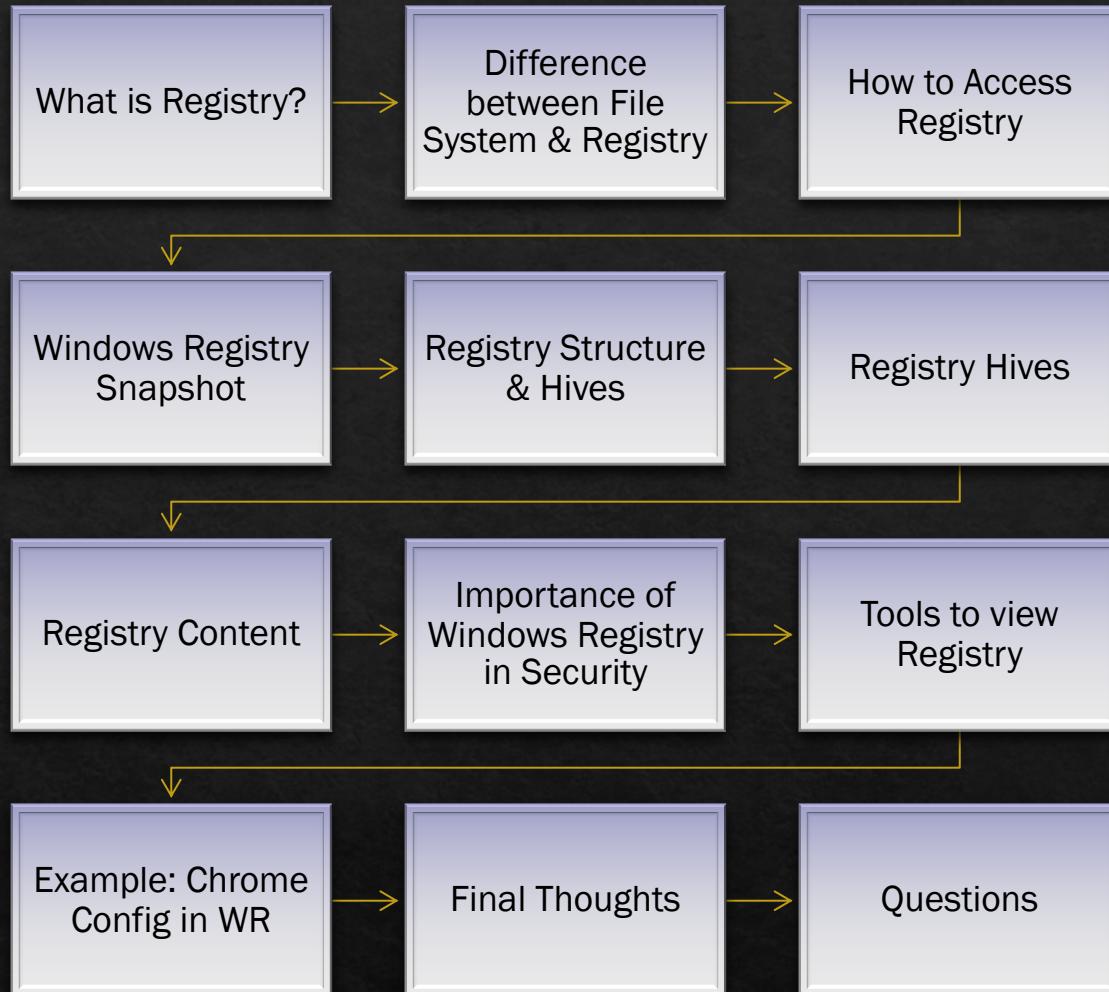


# Windows Registry

By

Aastha Sahni

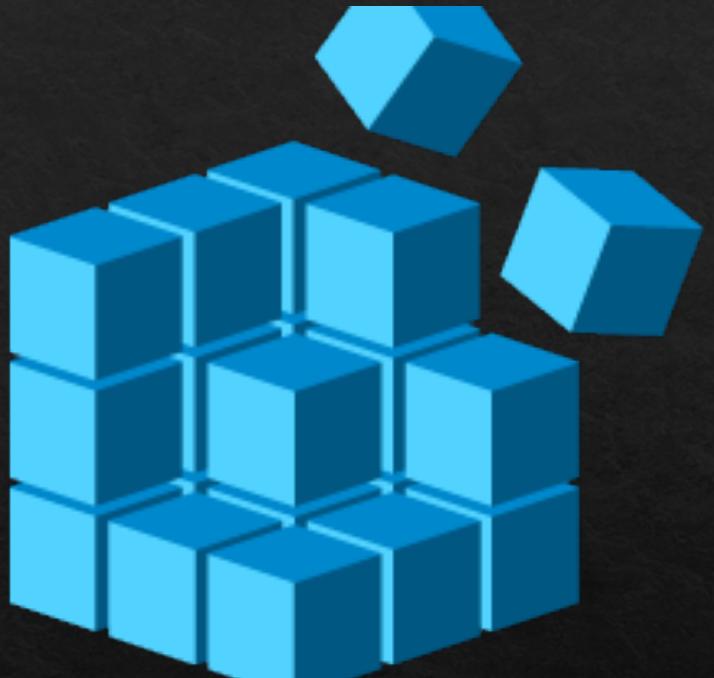
# Agenda



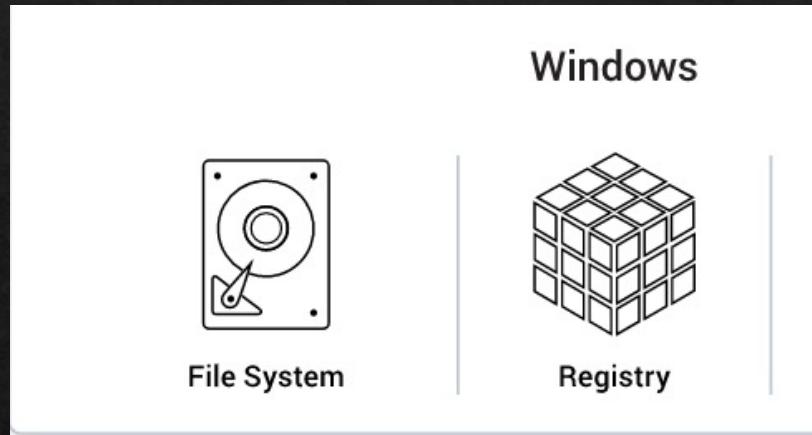
# What is Registry?

- ❖ A central hierarchical database used in Windows used to store information that is necessary to configure the system for one or more users, applications, and hardware devices.
- ❖ The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

- Microsoft Documentation



# Difference between File System & Registry

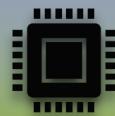


- ❖ The windows registry is like a file system.
- ❖ A file system has files and folders whereas registry has keys and within keys we have either more keys or key -value pairs, storing information.
- ❖ Registry cannot be access by any user, it requires admin access!

# How to Access Registry

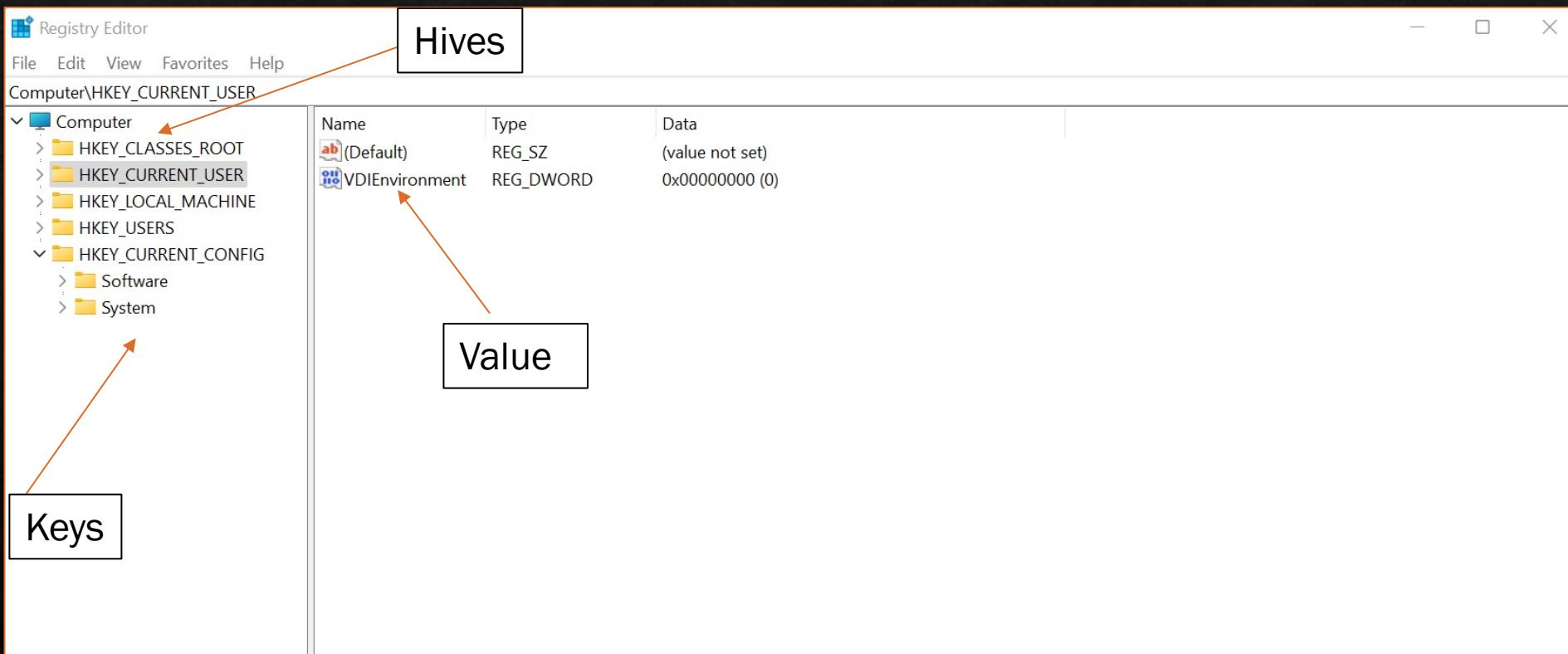


To access windows registry, run utility **regedit**.



It is a graphical tool that lets you view and monitor the Windows operating system's registry and edit if necessary.

# Windows Registry



# Registry Files

C:/windows/system32/config/

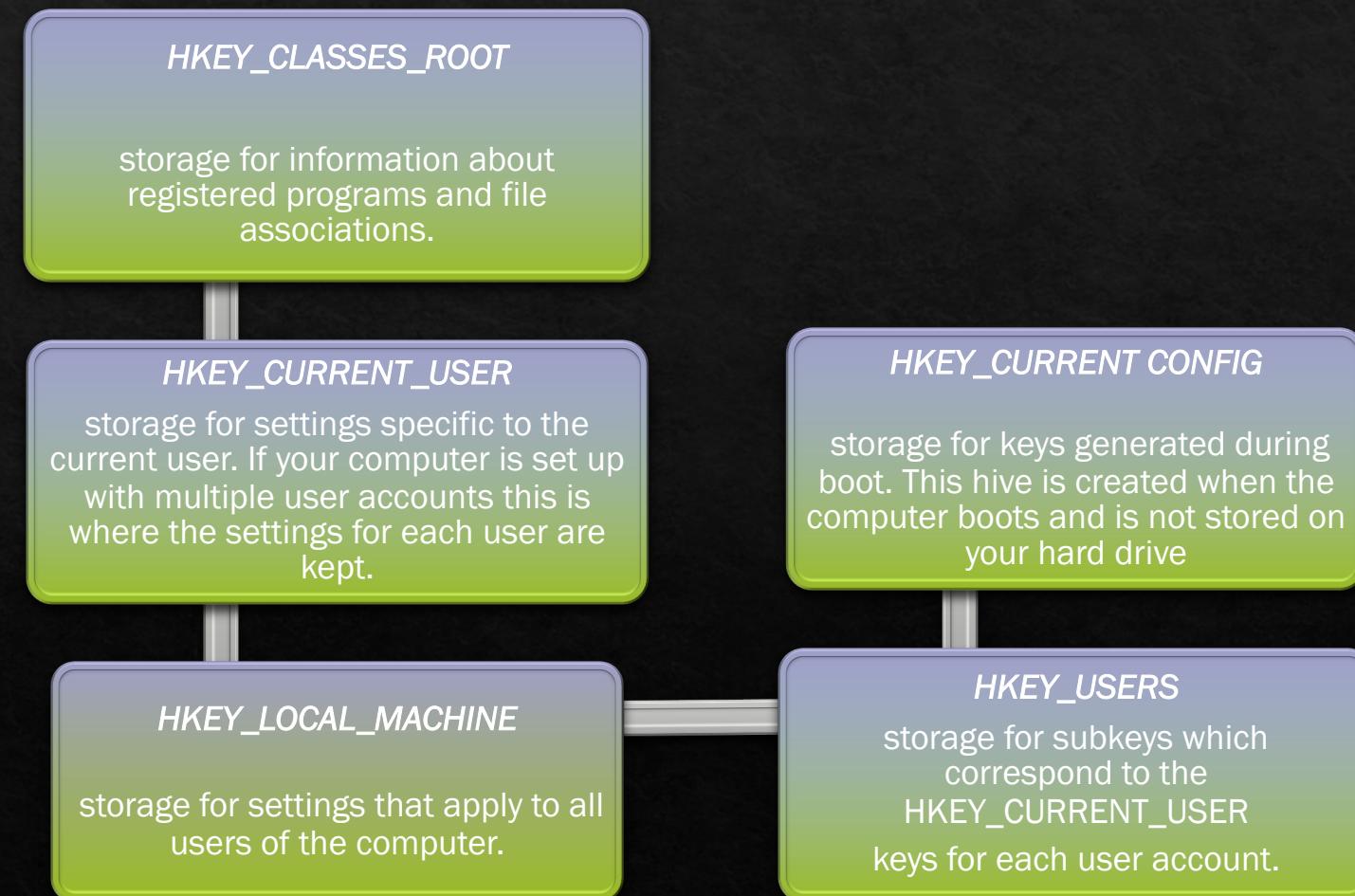
| Name          | Date modified     | Type        | Size       |
|---------------|-------------------|-------------|------------|
| Journal       | 6/5/2021 8:10 AM  | File folder |            |
| RegBack       | 6/5/2021 8:10 AM  | File folder |            |
| systemprofile | 6/5/2021 8:10 AM  | File folder |            |
| TxR           | 10/6/2021 1:52 PM | File folder |            |
| BBI           | 1/24/2022 6:46 PM | File        | 768 KB     |
| BCD-Template  | 10/6/2021 5:51 PM | File        | 28 KB      |
| COMPONENTS    | 2/2/2022 12:48 AM | File        | 31,744 KB  |
| DEFAULT       | 1/24/2022 6:46 PM | File        | 1,280 KB   |
| DRIVERS       | 1/30/2022 3:54 AM | File        | 7,580 KB   |
| SAM           | 10/6/2021 2:01 PM | File        | 32 KB      |
| SECURITY      | 1/24/2022 6:46 PM | File        | 128 KB     |
| SOFTWARE      | 1/24/2022 6:46 PM | File        | 64 KB      |
| SYSTEM        | 1/24/2022 6:46 PM | File        | 124,928 KB |
|               |                   |             | 24,320 KB  |

# Registry Structure & Hives

## Components of Windows Registry

- Hives
- Root Keys
- Keys
- Sub-Keys
- Value

# Registry Hives



# Registry Content

The registry stores critical system information about user, system and installed applications.

- Operating system information - build number, version user and registered user.
- Information about properly installed applications
- Installed services
- Maps network addresses to host machines
- Security information - trojan, ransomware, malware

# Importance of Windows Registry in Security.

Windows registry is a great source of forensic evidence.

Images of windows registry are extracted for more detailed analysis of incident by DFIR teams.

Identifying malware and ransomware information for forensic analysis

Tools for extracting detailed information which otherwise not possible with usual editor.

Window Registry is often used by attackers to hide malwares and APTs

# Tools to Access Windows Registry

RegScanner

RegistryChanges  
View

RegFromApp

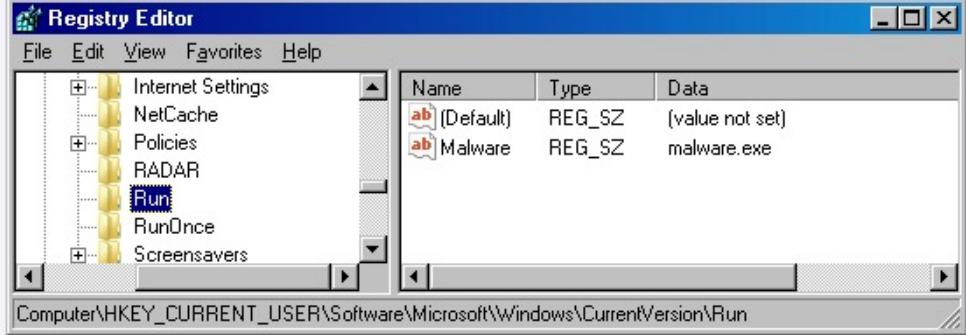
RegDIIView

ActiveXHelper

RegFileExport

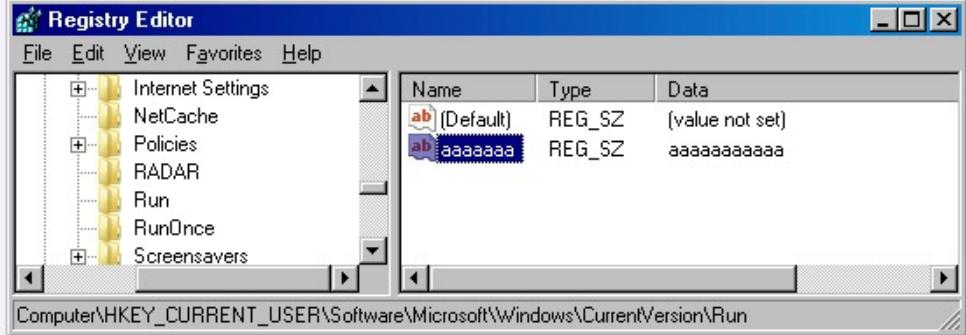
Where to find these tools <https://www.nirsoft.net/>

# Example: How attackers can misuse Registry



The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run'. One of the keys is labeled 'Run'. The right pane is a table with three columns: 'Name', 'Type', and 'Data'. There are two entries: '(Default)' with type 'REG\_SZ' and data '(value not set)', and 'Malware' with type 'REG\_SZ' and data 'malware.exe'.

Figure 1: A malicious actor creates a value in the Run key



The screenshot shows the same Windows Registry Editor window as Figure 1. The 'Run' key is expanded. The table in the right pane now shows two entries: '(Default)' with type 'REG\_SZ' and data '(value not set)', and a new entry 'aaaaaaaa' with type 'REG\_SZ' and data 'aaaaaaaaaa'. The original 'Malware' entry has been removed.

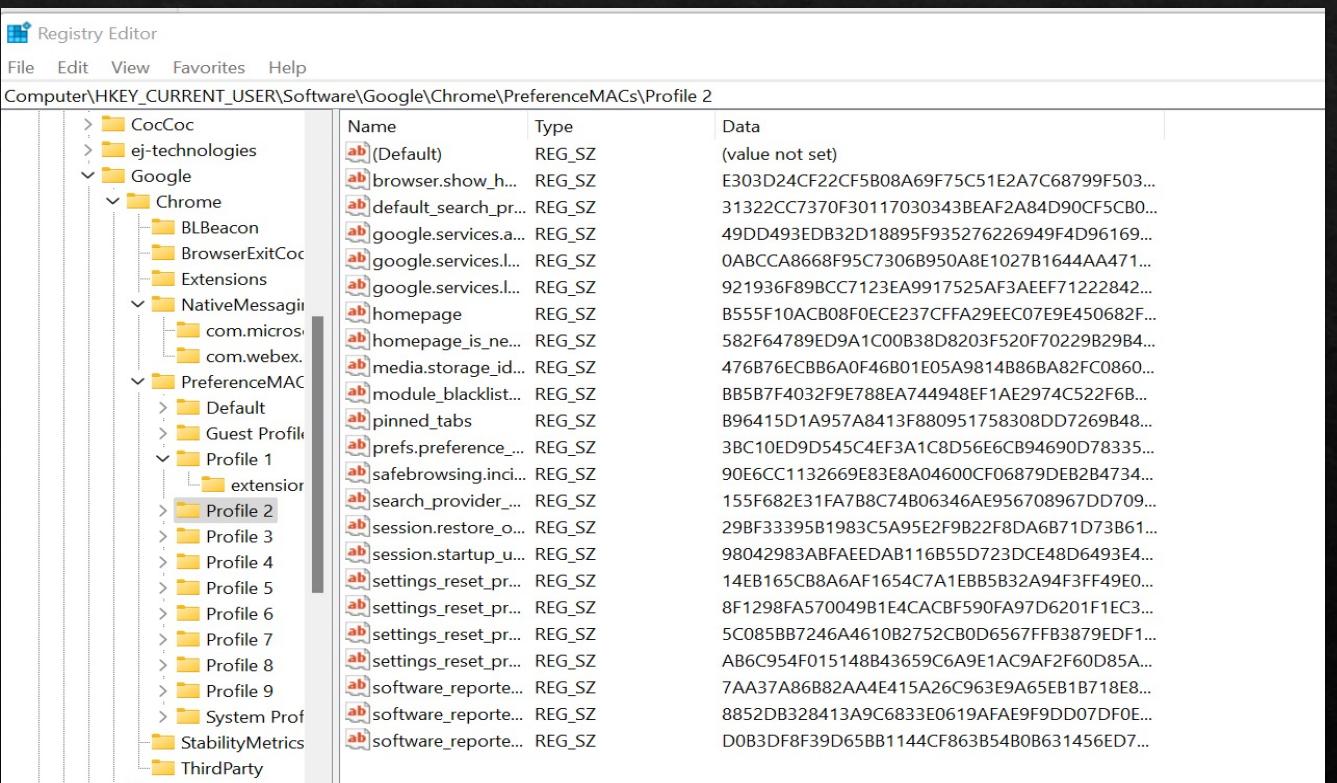
At a later point in time the malware is removed from the system. The registry value is overwritten before being deleted.

Figure 2: The malicious value is overwritten and deleted

# Example: Chrome Config in WR

To check your Chrome setting you can go to:

1. Type Regedit in your search
2. It will open the windows registry and HKEY\_CURRENT\_USER\Software\Google\Chrome contains the Chrome settings



The screenshot shows the Windows Registry Editor window. The title bar reads "Registry Editor" and the path "Computer\HKEY\_CURRENT\_USER\Software\Google\PreferenceMACs\Profile 2". The left pane displays a tree view of registry keys under "Profile 2", including "CocCoc", "ej-technologies", "Google", "Chrome", "BLBeacon", "BrowserExitCoc", "Extensions", "NativeMessaging", "com.microsoft", "com.webex", "PreferenceMAC", "Default", "Guest Profile", "Profile 1", "extension", "Profile 2", "Profile 3", "Profile 4", "Profile 5", "Profile 6", "Profile 7", "Profile 8", "Profile 9", "System Prof", "StabilityMetrics", and "ThirdParty". The right pane shows a table with columns "Name", "Type", and "Data". The "Name" column lists various registry entries such as "(Default)", "browser.show\_h...", "default\_search\_pr...", "google.services.a...", "google.services.l...", "homepage", "homepage\_is\_ne...", "media.storage\_id...", "module\_blacklist...", "pinned\_tabs", "prefs.preference...", "safebrowsing.inc...", "search\_provider...", "session.restore\_o...", "session.startup\_u...", "settings\_reset\_pr...", "settings\_reset\_pr...", "settings\_reset\_pr...", "settings\_reset\_pr...", "software\_reporte...", "software\_reporte...", and "software\_reporte...". The "Type" column shows most entries as REG\_SZ. The "Data" column contains long hexadecimal strings representing the values.

| Name                 | Type   | Data  |
|----------------------|--------|---|
| (Default)            | REG_SZ | (value not set)                               |
| browser.show_h...    | REG_SZ | E303D24CF22CF5B08A69F75C51E2A7C68799F503...   |
| default_search_pr... | REG_SZ | 31322CC7370F30117030343BEAF2A84D90CF5CB0...   |
| google.services.a... | REG_SZ | 49DD493EDB32D18895F935276226949F4D96169...    |
| google.services.l... | REG_SZ | 0ABCBA8668F95C7306B950A8E1027B1644AA471...    |
| homepage             | REG_SZ | 921936F89BCC7123EA9917525AF3AEFF71222842...   |
| homepage_is_ne...    | REG_SZ | B555F10ACB808F0ECE237CFFA29EFC07E9E450682F... |
| media.storage_id...  | REG_SZ | 582F64789ED9A1C00B38D8203F520F70229B29B4...   |
| module_blacklist...  | REG_SZ | 476B76ECBB6A0F46B01E05A9814B86BA82FC0860...   |
| pinned_tabs          | REG_SZ | BB5B7F4032F9E788EA744948EF1AE2974C522F6B...   |
| prefs.preference...  | REG_SZ | B96415D1A957A8413F880951758308DD7269B48...    |
| safebrowsing.inc...  | REG_SZ | 38C10ED9D545C4EF3A1C8D56E6CB94690D78335...    |
| search_provider...   | REG_SZ | 90E6CC1132669E83E8A04600CF06879DEB2B4734...   |
| session.restore_o... | REG_SZ | 155F682E31FA7B8C74B06346AE956708967DD709...   |
| session.startup_u... | REG_SZ | 29BF33395B1983C5A95E2F9B22F8DA6B71D73861...   |
| settings_reset_pr... | REG_SZ | 98042983ABFAEEDAB116B55D723DCE48D6493E4...    |
| settings_reset_pr... | REG_SZ | 14EB165CB8A6AF1654C7A1EBB5B32A94F3FF49E0...   |
| settings_reset_pr... | REG_SZ | 8F1298FA570049B1E4CACBF590FA97D6201F1EC3...   |
| settings_reset_pr... | REG_SZ | 5C085BB7246A4610B2752CB0D6567FFB3879EDF1...   |
| settings_reset_pr... | REG_SZ | AB6C954F015148B43659C6A9E1AC9AF2F60D85A...    |
| software_reporte...  | REG_SZ | 7AA37A86B82AA4E415A26C963E9A65EB1B718E8...    |
| software_reporte...  | REG_SZ | 8852DB328413A9C6833E0619AFAE9F9DD07DF0E...    |
| software_reporte...  | REG_SZ | D0B3DF8F39D65BB1144CF863B54B0B631456ED7...    |

# Final Thoughts!

Can we change settings in Windows Registry?

YES !!!!!!! If you know what you are doing and carefully changing values, there should not be and problem.



BUT - If you starting editing, deleting or adding registry keys with no proper knowledge you might damage you whole windows installation





Questions

# References

- ❖ <https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>
- ❖ <https://www.nirsoft.net/>
- ❖ <https://medium.com/@lucideus/windows-registry-forensic-analysis-part-1-windows-forensics-manual-2018-2cb4da210125>
- ❖ <https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>
- ❖ <https://www.mandiant.com/resources/digging-up-the-past-windows-registry-forensics-revisited>

# Questions