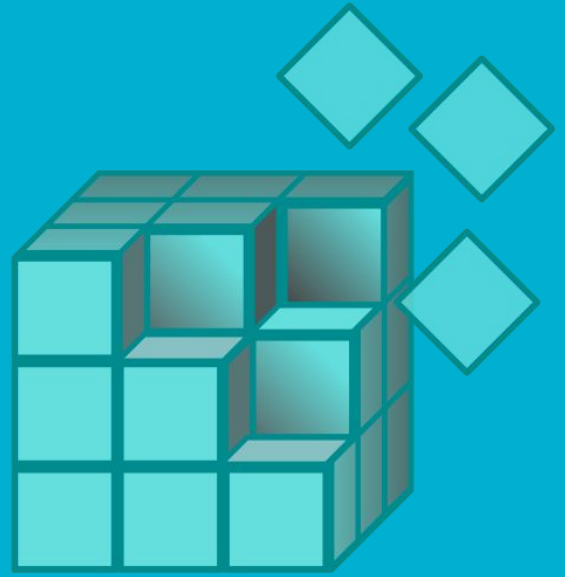


Windows Registry



What is Windows Registry

- Where all the system data is stored
 - setting configurations
 - software programs
 - hardware devices
 - user preferences
- essentially it is the DNA of the windows operating system



Why is Registry important

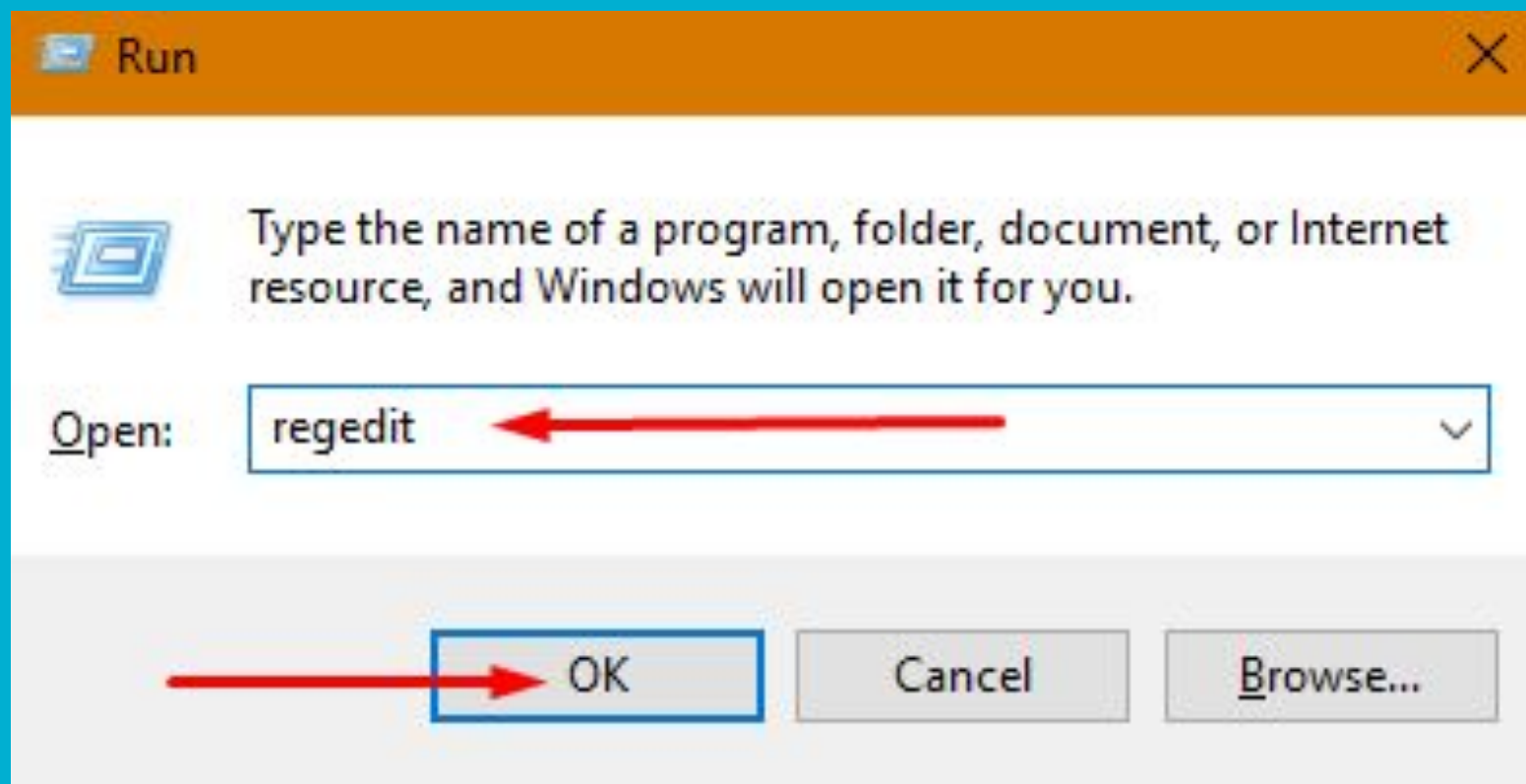
- stores all the vital information about your windows system
- Basically a minefield



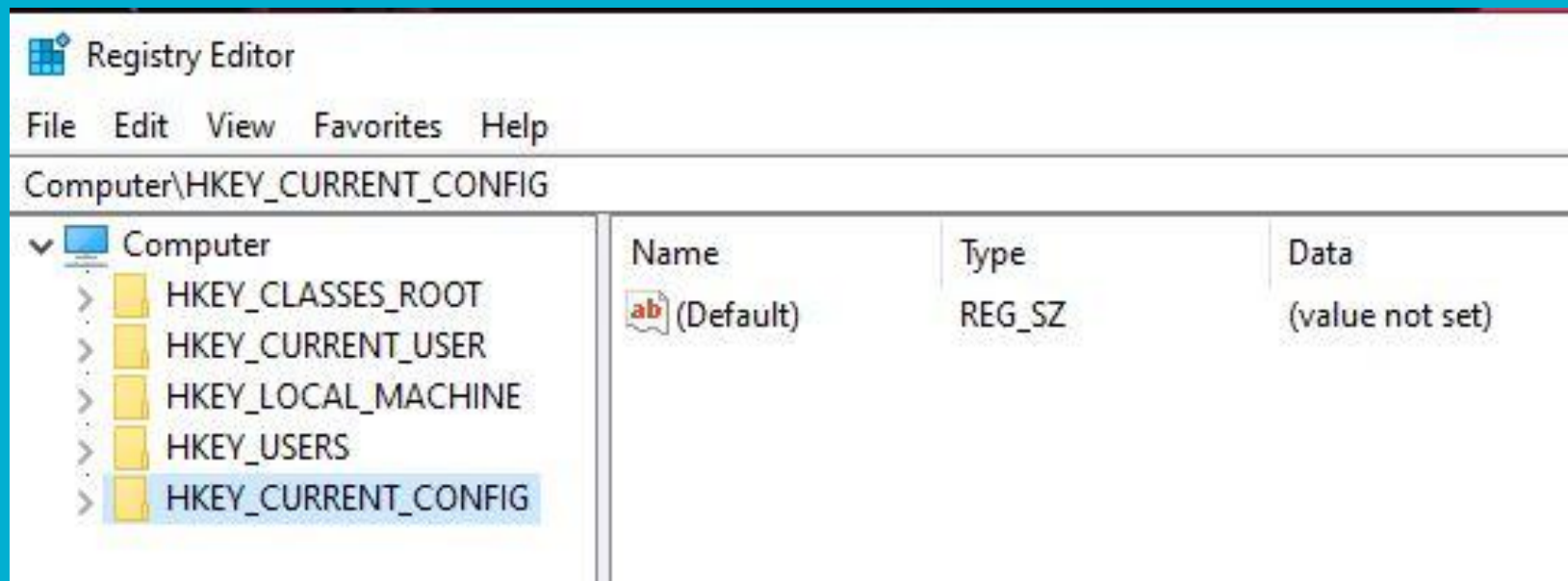
How to access Registry

- activate windows run win + r and type in regedit
- run command prompt as an administrator (search for command prompt and then right click on the icon and select run as administrator)
 - then type “reg /?” (ignore the quotations when typing the command)
 - can be used for scripting

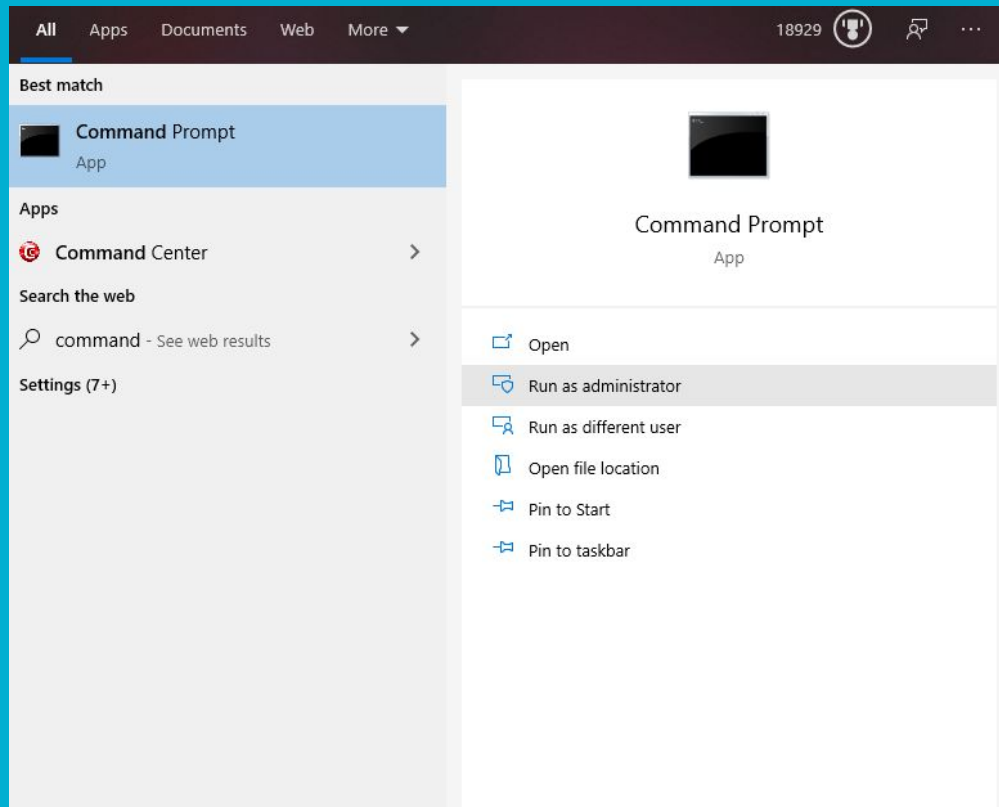
Win + R method



You should get to this screen



Command prompt method



This is the result after typing in reg/?

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>reg/?

REG Operation [Parameter List]

    Operation  [ QUERY   | ADD     | DELETE  | COPY    |
                SAVE    | LOAD    | UNLOAD  | RESTORE |
                COMPARE | EXPORT  | IMPORT  | FLAGS   ]

Return Code: (Except for REG COMPARE)

    0 - Successful
    1 - Failed

For help on a specific operation type:

    REG Operation /?

Examples:

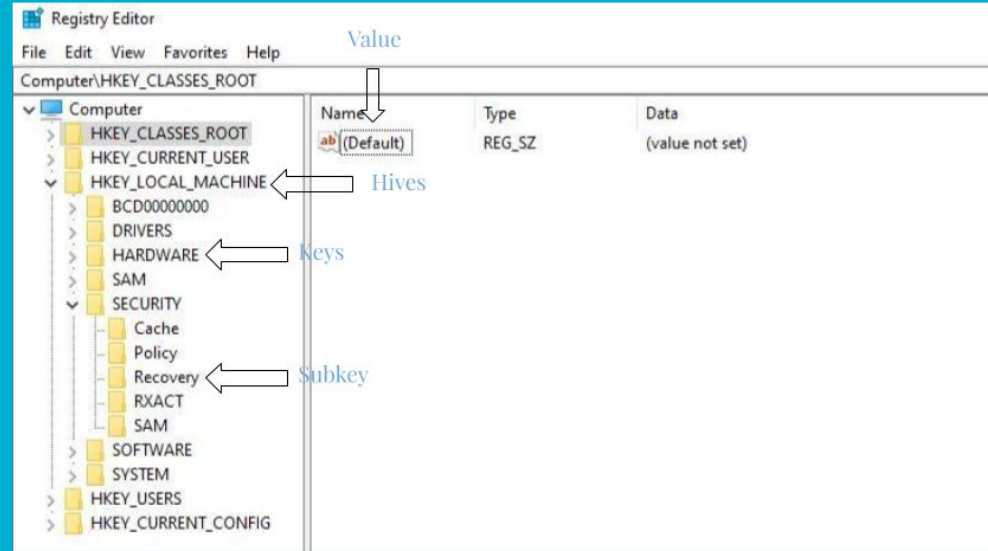
    REG QUERY /?
    REG ADD /?
    REG DELETE /?
    REG COPY /?
    REG SAVE /?
    REG RESTORE /?
    REG LOAD /?
    REG UNLOAD /?
    REG COMPARE /?
    REG EXPORT /?
    REG IMPORT /?
    REG FLAGS /?

C:\WINDOWS\system32>regedit

C:\WINDOWS\system32>
```


How to use Registry

- contains registry values
- registry keys
- registry hives
 - Changing the values change the settings
 - you can change registry configurations using the registry editor or through a REG file



How to edit REG files

- An REG file is a file that can be opened in plaintext programs such as notepad
 - Right click the file and open with plaintext program
- to create a REG file create a new notepad file and use the syntax
 - Windows Registry Editor Version 5.00
 - [<Hive name>\<Key name>\<Subkey name>]
 - "Value name"=<Value type>:<Value data>
 - this will create a new registry value and change it automatically
 - once you type in the registry setting then click file and save as and then set the save as type to all files and type the name with the extension .REG
- to import the registry file created just double click and click yes
- some registry files may need you to restart your computer to take effect

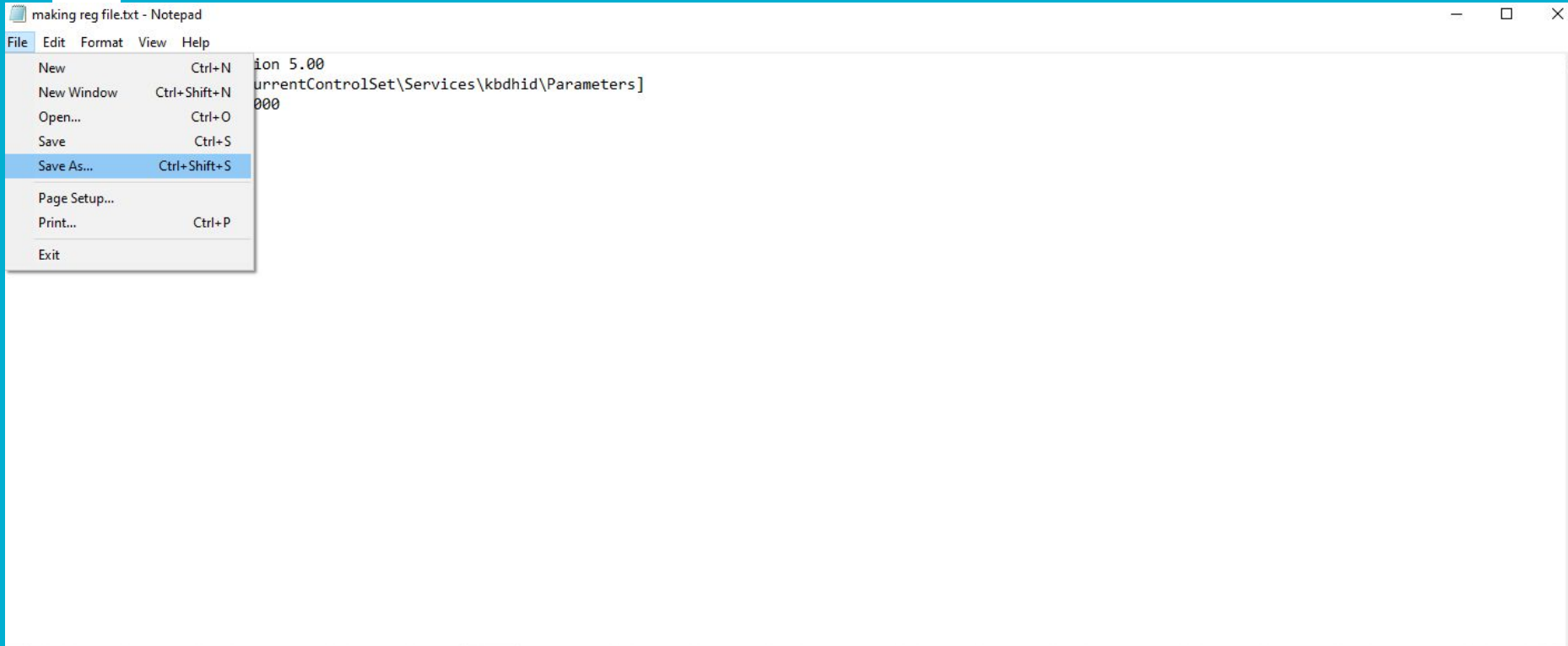
Creating a REG file



The image shows a Notepad window titled "*Untitled - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text content is a Windows Registry Editor script, starting with "Windows Registry Editor Version 5.00", followed by a path in square brackets: "[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters]", and then a registry value: "\"CrashOnCtrlScroll\"=dword:000000". A vertical cursor is positioned at the end of the text on the third line.

```
*Untitled - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters]
"CrashOnCtrlScroll"=dword:000000
|
```

Saving as a REG file





Save As



> This PC > Pictures > Reg files



Search Reg files

Organize ▾

New folder



★ Quick access

Desktop ↗

Downloads ↗

Documents ↗

Pictures ↗

Reg files ↗

FrogSimulation

online_examples

Screenshots

System32

OneDrive

This PC ▾

No items match your search.

File name: making reg file.reg ▾

Save as type: All Files (*.*) ▾

Text Documents (*.txt)

All Files (*.*)

▲ Hide Folders

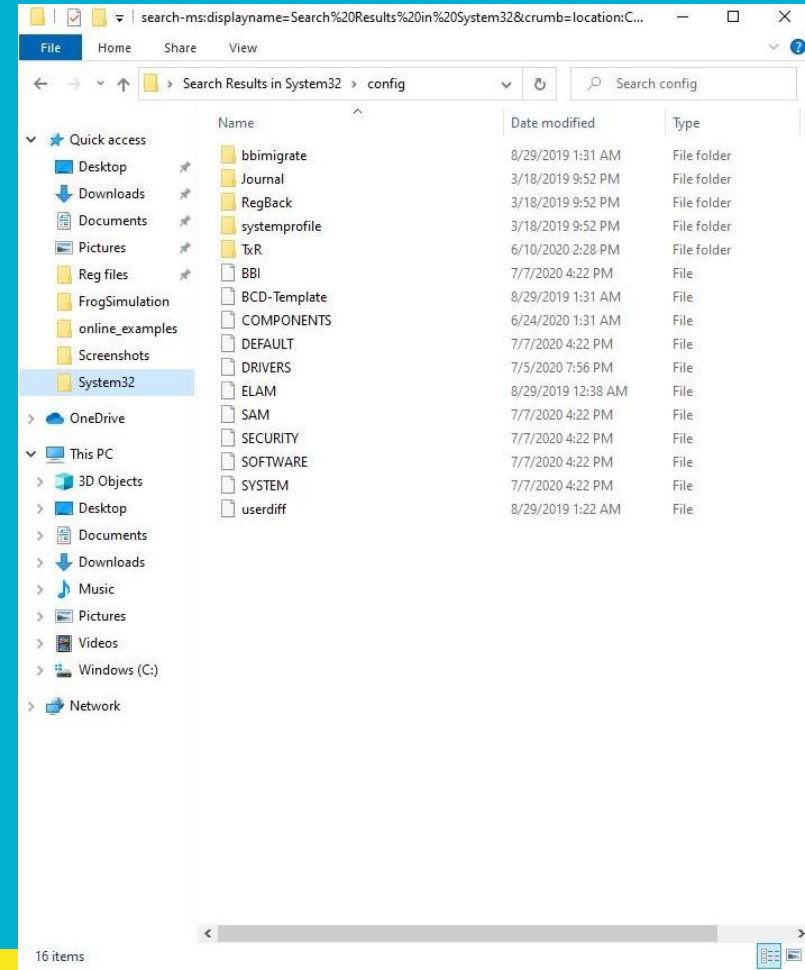
Encoding: UTF-8 ▾

Save

Cancel

Where Registry is stored

- SAM, SECURITY< SOFTWARE, SYSTEM, and DEFAULT registry files are stored in %SystemRoot%\System32\Config\folder
- older version of windows use the %WINDIR% folder to store registry data as DAT files
- windows registry backup files are saved as REG files
 - REG files contain hives, keys and values



Registry Hives

HKEY_CURRENT_USER

- = HKCU
- contains root configs of the user who is currently logged on
- user's folder, screen colors, and control panel settings stored here
- information associated with user profile

HKEY_USERS

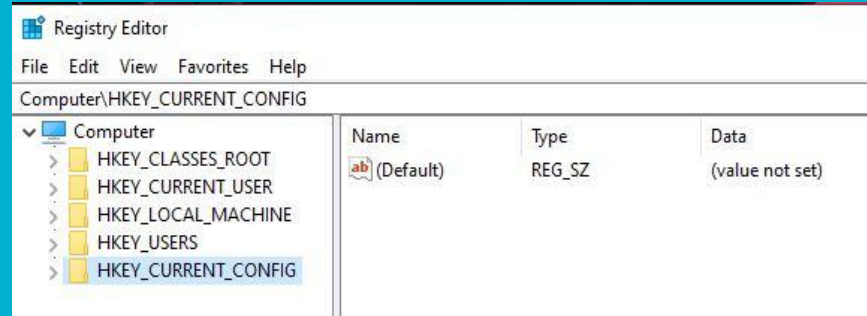
- contains all actively loaded user profiles

HKEY_LOCAL_MACHINE

- = HKLM
- contains configuration information particular to the computer
- like user personalized settings something you set

HKEY_CURRENT_CONFIG

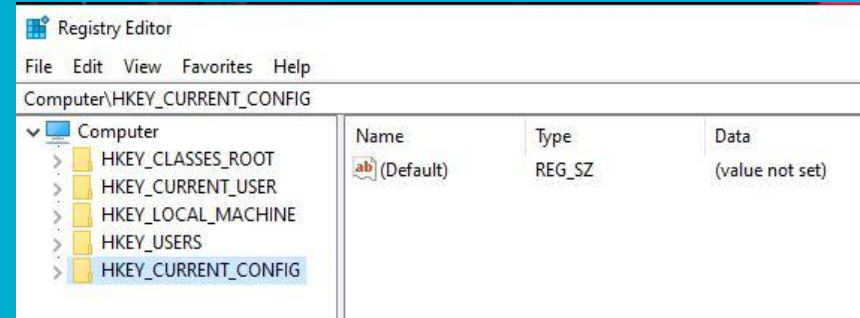
- contains information about the hardware profile



Registry Hives

HKEY_CLASSES_ROOT

- information stored here ensures the correct program opens when using file explorer
- stored under both HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE\Software\Classes contains default settings that apply to all users on the local computer
- HKEY_CURRENT_USER\Software\Classes contains settings that override the default settings and apply only to the interactive user
- HKEY_CLASSES_ROOT provides merged view for programs that are designed for earlier versions of windows



Keys

HKEY_LOCAL_MACHINE\SAM

- contains sam files which stands for security authentication manager which holds passwords for local and remote authentication

HKEY_LOCAL_MACHINE\Security

- contains security files

HKEY_LOCAL_MACHINE\Software

- software files

HKEY_LOCAL_MACHINE\System

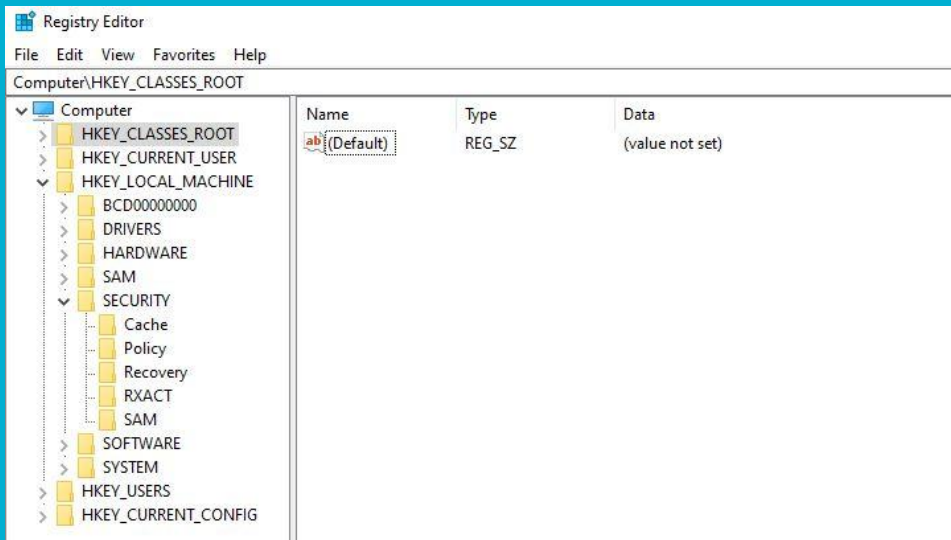
- system files

HKEY_CURRENT_CONFIG

- system files along with ntuser.dat
- ntuser.dat contains user profile settings

HKEY_USERS\DEFAULT

- contains default files



Values

REG_BINARY

- raw binary data
- 0 and 1
- 0 means off and 1 means on

REG_DWORD

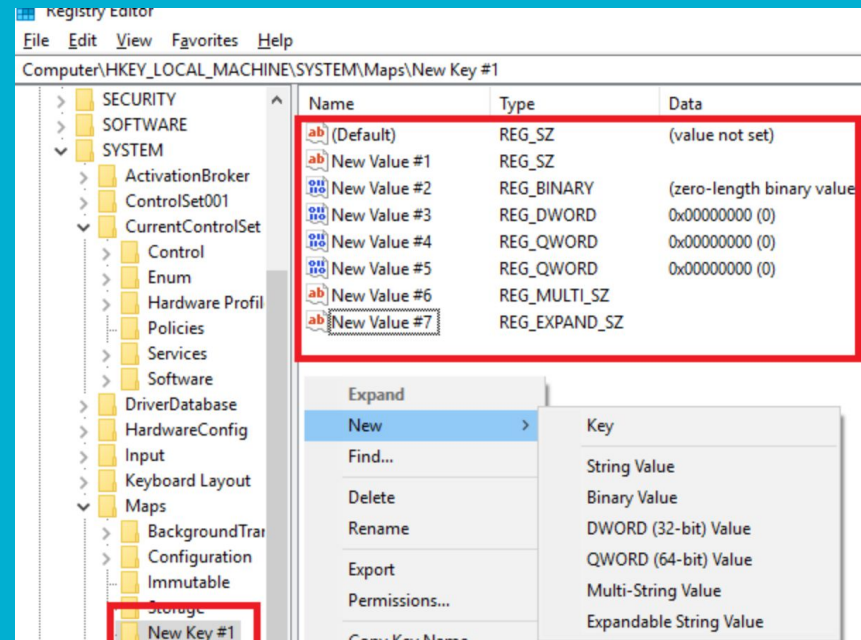
- data represented by a number that is 4 bytes
- hexadecimal and decimal
- hexadecimal is a representation of binary

REG_EXPAND_SZ

- variable length data string
- includes variables that are resolved when a program or service uses data

REG_MULTI_SZ

- multiple string
- values that contain lists or multiple values



Values

REG_SZ

- fixed length text string

REG_RESOURCE_LIST

- series of nested arrays that is designed to store a resource list used by a hardware device or physical devices it controls

REG_RESOURCES_REQUIREMENTS_LIST

- series of nested arrays that is designed to store a device driver's resource list of possible hardware resources

REG_FULL_RESOURCE_DESCRIPTOR

- a series of nested arrays designed to store a resource list
- data as detected and written in \hardwareDescription

REG_NONE

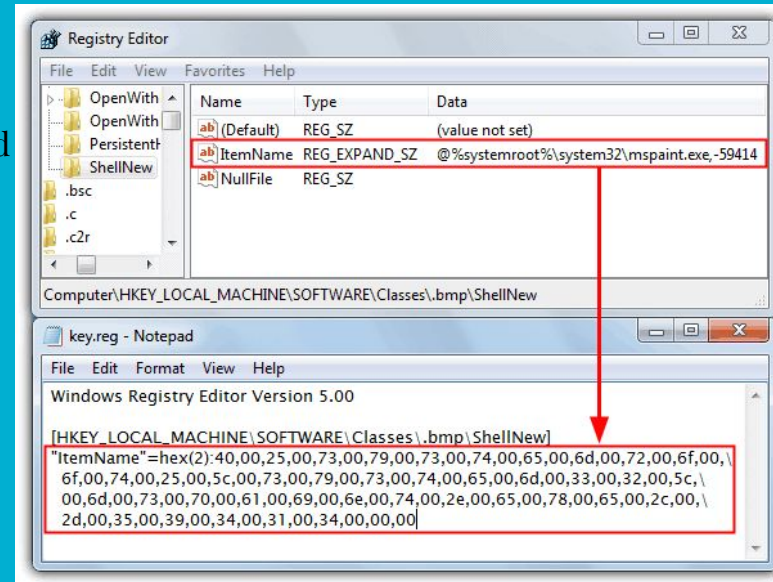
- data without particular type

REG_LINK

- unicode string naming a symbolic link

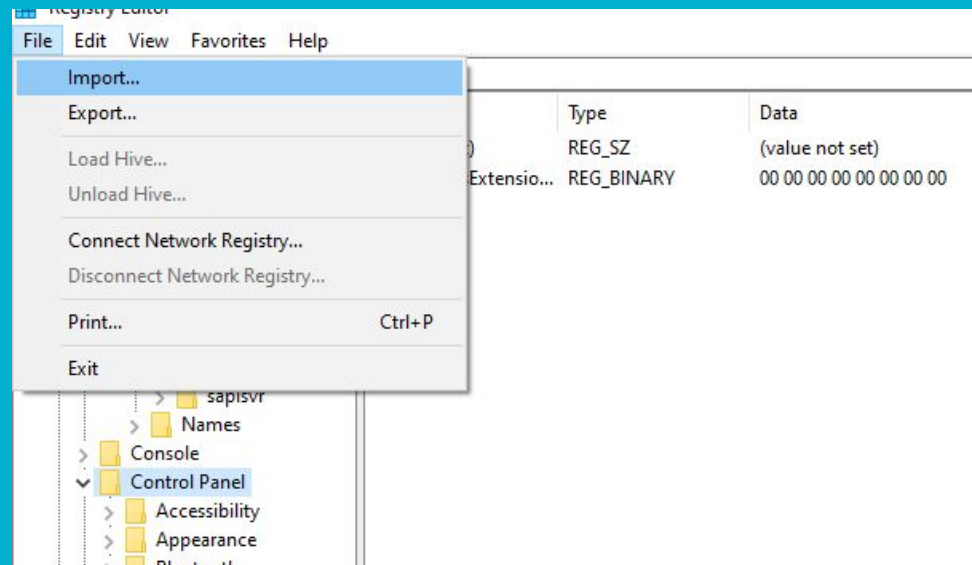
REG_QWORD

- data represented by a number that is a 64 bit integer



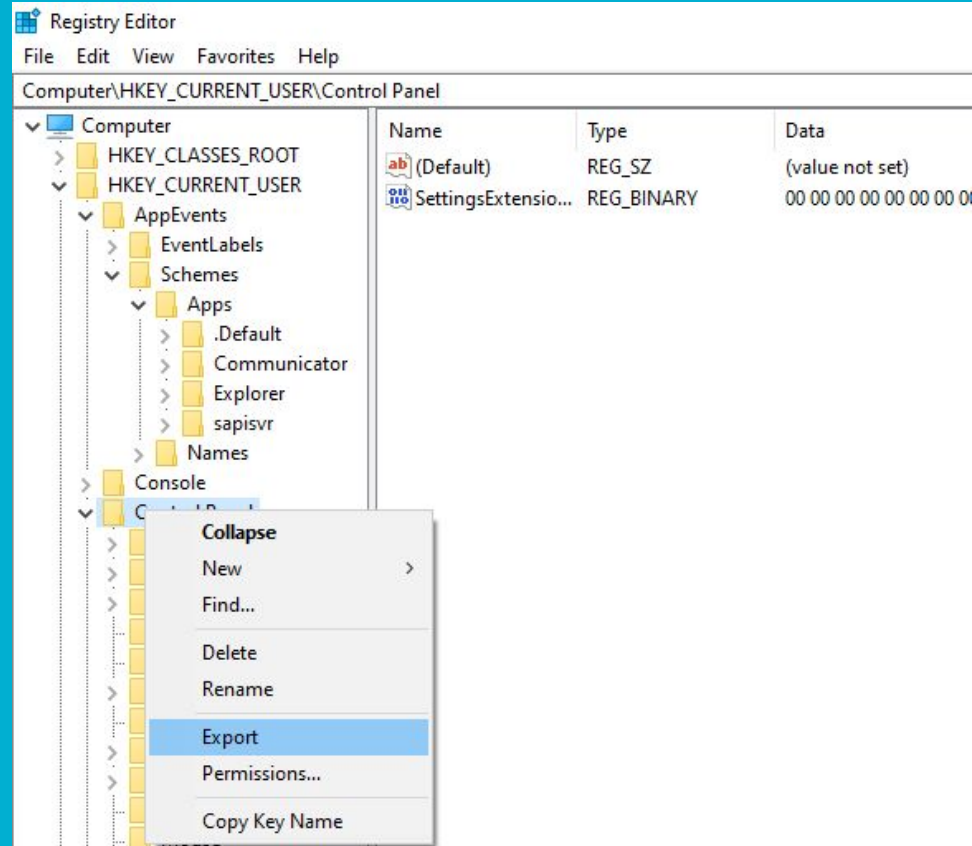
Importing keys

- Double clicking a REG file will automatically merge it into registry
- go into registry
- click on file in the top left corner and click import
- then find a .reg file to import and click open and it will give you a message saying the information in the filename has been entered into the registry



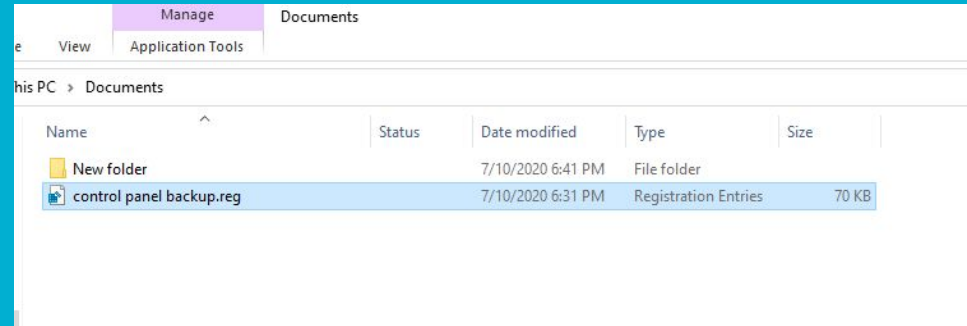
Exporting Keys

- go to registry (go to run and type in regedit)
- then locate the registry branch you want to change (a branch is the folders you see once you expand the hive keys)
- click file and click export and save it with a descriptive name



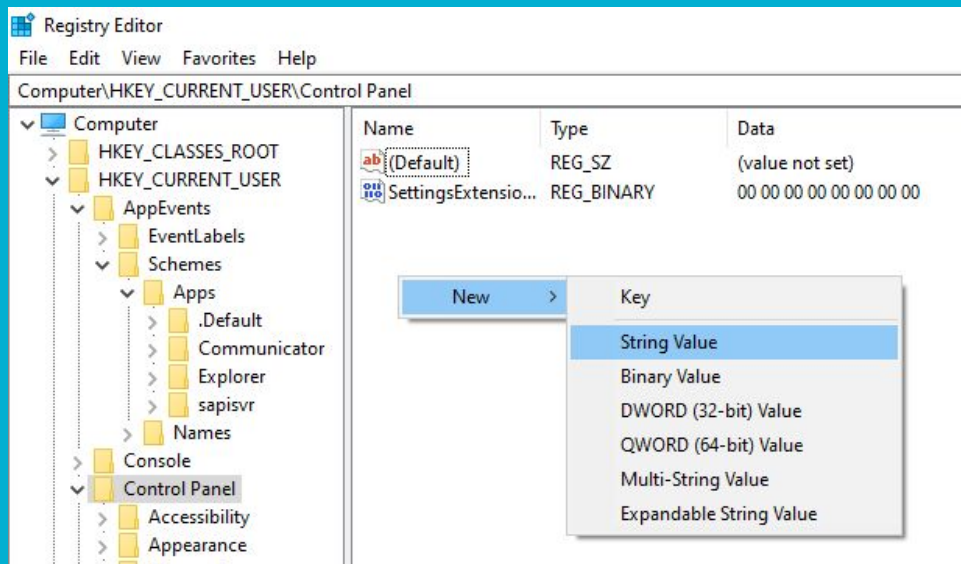
Important things to keep in mind

- If you are missing windows components like control panel the problem might be a registry key missing or value
- You might have to restart your computer in order for changes to take effect
- Make sure to have a backup of the file you edit just in case you mess up
- To make a backup export the original reg file and name it backup or something descriptive
- then export the file you want to change and open it in any text file editor



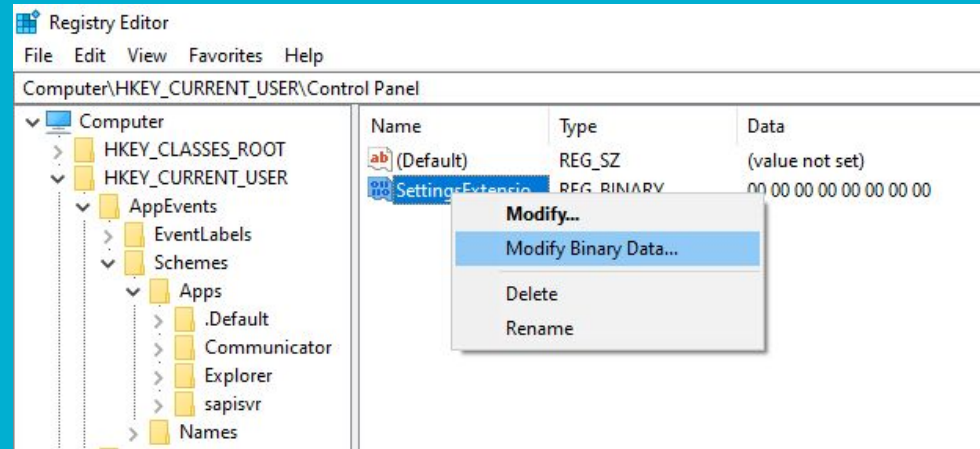
Adding values

- Adding values in regedit
 - right click any white space in the key you are in and select the type of values you want your new configuration to be
 - name it and then modify the value to your liking
- Adding values in REG files
 - Add this template and edit it
 - Windows Registry Editor Version 5.00
 - [<Hive name>\<Key name>\<Subkey name>]
 - "Value name"=<Value type>:<Value data>



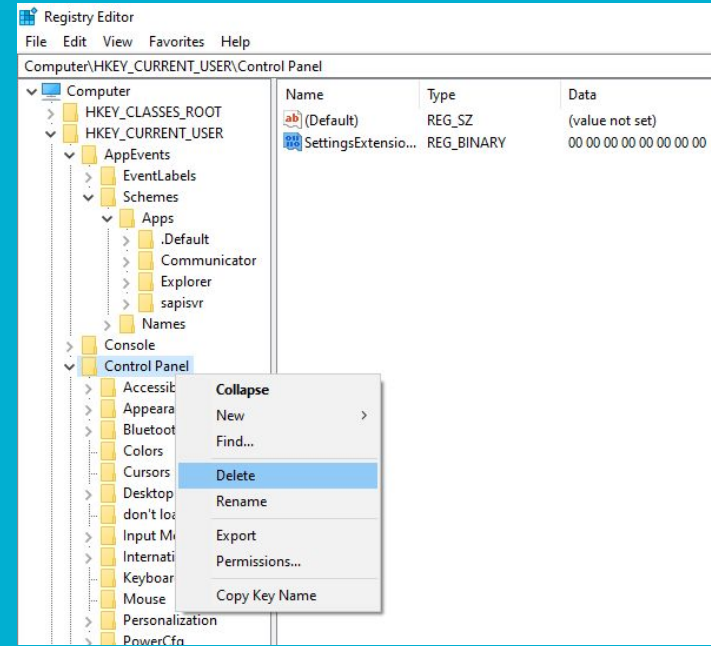
Editing values

- find the configuration name you want to change
 - look at the value type before changing it for binary keys normally 0 means off and 1 means on
 - For dword value it is a hexadecimal value set it to what you see fit for the key



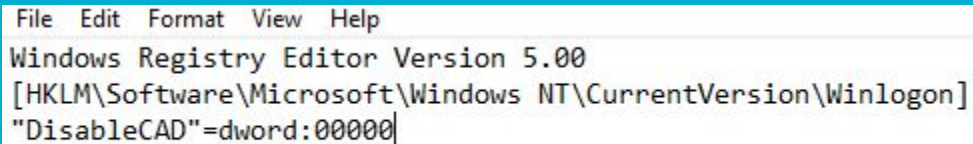
Deleting values

- To delete a registry key within regedit right click the key and click delete
- to delete a registry key within a .reg file put a hyphen (-) in front of the registry path in the .reg file or use the registry gui to delete a value by right clicking it and hitting delete
 - HKEY_LOCAL_MACHINE\Software\Test
 - [-HKEY_LOCAL_MACHINE\Software\Test]
 - to change a dataitemname in the file add a hyphen after the equal sign
 - HKEY_LOCAL_MACHINE\Software\Test
 - "TestValue"=-



Some security configs with registry

- require ctrl-alt-delete to log in
 - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
 - Value: DisableCAD
 - Type: REG_DWORD
 - Data: [see below]
 - 0 = Users must press Ctl-Alt-Delete to log into the system. (Default for domain joined systems)
 - 1 = Users do not need to press Ctl-Alt-Delete to log into the system. (Default for nondomain joined systems)

A screenshot of the Windows Registry Editor window. The title bar reads "File Edit Format View Help". The main text area shows the path "Windows Registry Editor Version 5.00" followed by "[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]" and the value "DisableCAD" set to "dword:000001".

```
File Edit Format View Help
Windows Registry Editor Version 5.00
[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
"DisableCAD"=dword:000001
```

Security configs part 2 electric boogaloo

- disabling auto admin login
 - *already done in cypat images
 - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
 - Value: Autoadminlogin
 - Type: REG_SZ
 - Data:
 - 0 = Auto Admin Login is not enabled (default)
 - 1 = Auto Admin Login is enabled

```
File Edit Format View Help
Windows Registry Editor Version 5.00
[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
"Autoadminlogin"=sz:00001
```

ThAnK

Slides made by Zachary Dang

