Worcester Polytechnic Institute

Department of Computer Science

Module 5: Windows Registry

What's Windows Registry?

Windows Registry is a database design for fast reads and writes and efficient storage

It's always loaded into RAM as Windows boots.

The registry contains two basic elements: keys and values.

Registry keys are container objects similar to folders.

Registry values are non-container objects similar to files.

There are five root keys:

HKEY_CLASSES_ROOT (HKCR) contains information about registered applications, such as file associations

HKEY_CURRENT_USER (HKCU) stores settings that are specific to the currently logged-in user

HKEY_LOCAL_MACHINE (HKLM) stores settings that are specific to the local computer

Seven subkeys:

SAM (security accounts manager) * hacker looking for

Security (not accessible except by administrator)

System (critical boot process and other kernel functions)

Software (third party software settings are stored)

Hardware (Created dynamically during boot)

Components

BCD.dat (in the \boot folder in the system partition)

HKEY_USERS (HKU) contains subkeys corresponding to the HKCU keys for each user profile

HKEY_CURRENT_CONFIG (HKCC) contains information gathered at runtime; information stored in this key is not permanently stored on disk.

Who uses the Windows Registry?

- kernel
- Device drivers
- Services
- SAM
- User interface
- Third party applications

Who does not use the Windows Registry?

- .NET Framework applications use XML files for configuration
- Portable applications usually keep their configuration data within files in the directory/folder where the application executable resides.

Control panel is the safe way to modify Windows settings

** Make sure you have a good backup before playing with regedit.exe **

You may also interest:

What If You Delete the Windows Registry?

What If You Delete the Windows Registry?

The "HKLM\SAM" key usually appears as empty for most users (unless they are granted access by administrators of the local system or administrators of domains managing the local system). It is used to reference all "Security Accounts Manager" (SAM) databases for all domains into which the local system has been administratively authorized or configured (including the local domain of the running system, whose SAM database is stored in a subkey also named "SAM": other subkeys will be created as needed, one for each supplementary domain). Each SAM database contains all builtin accounts (mostly group aliases) and configured accounts (users, groups and their aliases, including guest accounts and administrator accounts) created and configured on the respective domain, for each account in that domain, it notably contains the user name which can be used to log on that domain, the internal unique user identifier in the domain, a cryptographic hash of each user's password for each enabled authentication protocol, the location of storage of their user registry hive, various status flags (for example if the account can be enumerated and be visible in the logon prompt screen), and the list of domains (including the local domain) into which the account was configured.

Objectives:

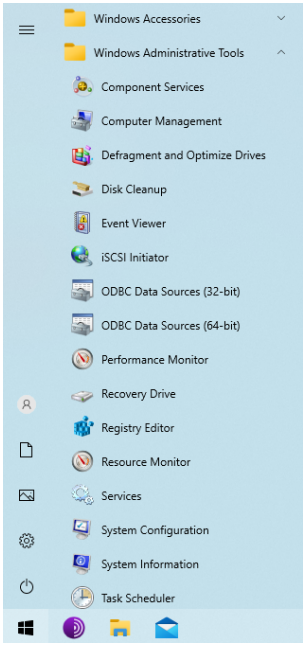
- Learn how to backup Windows registry
- Understand the basic of Windows registry
- Search, create, delete keys/subkeys

Tasks

We recommend to do this lab on a Windows VM (Windows 7 or above is preferred)

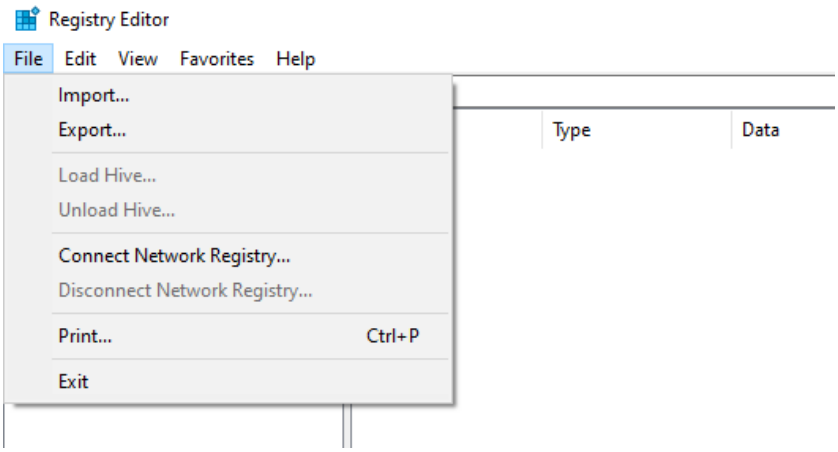
Task 1: Backup the registry

1. Open Start menu → Windows Administrative Tools → Registry Editor

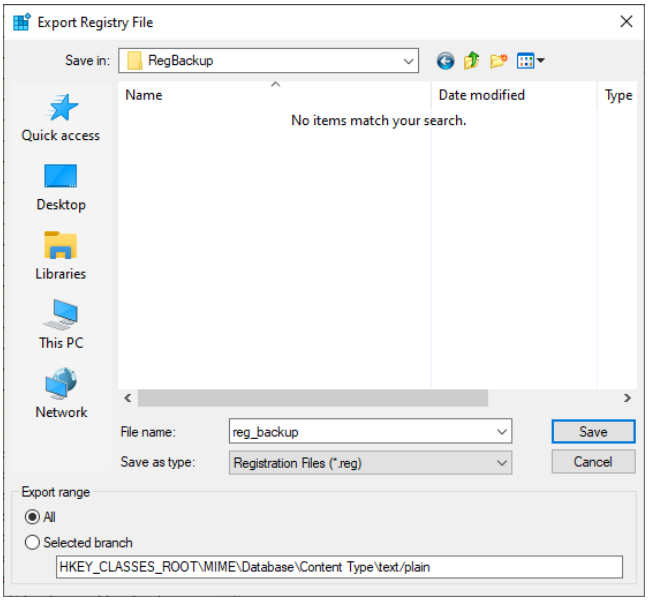


Export registry file

2. Select File → Export



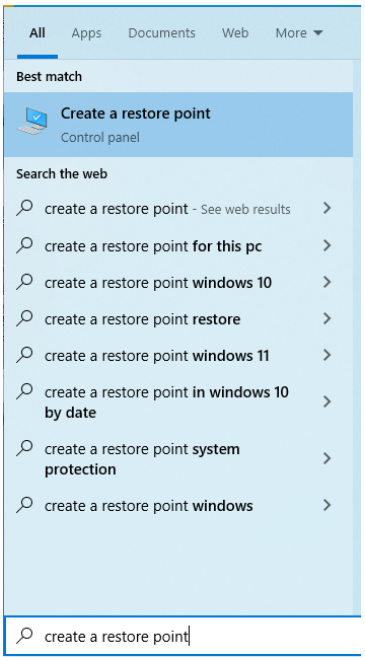
3. Select the location that you want to save, enter the file name and select “All” for the export range.



The process may take some time.

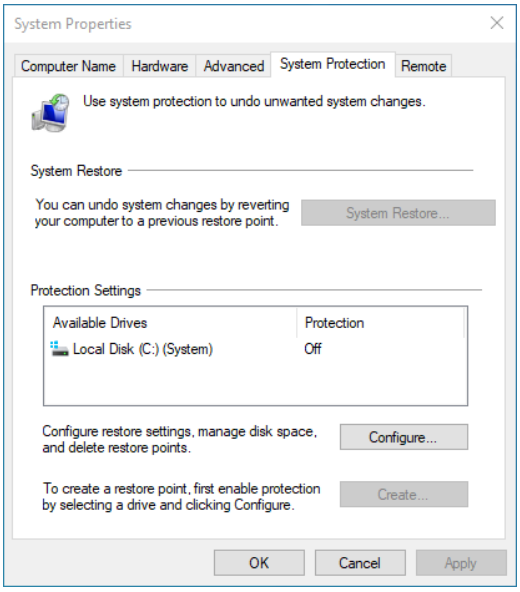
Create restore point

4. Open Start menu → type “Create a restore point”

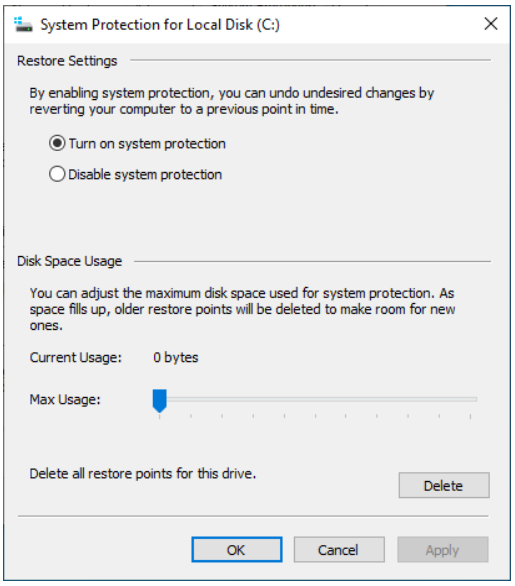


5. After windows has pop out, you should be able to see the system properties

   Notice that the disk protection is currently off, to enable it, click “Configure”

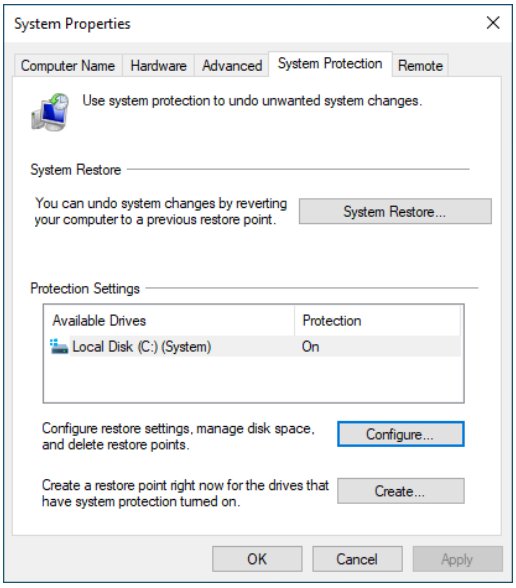


6. Select “Turn on system protection” and click OK.

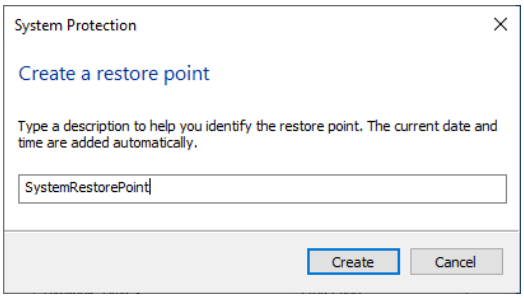


7. Now the create restore point button should be enabled.

   Click on “Create”

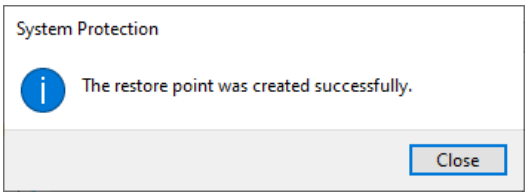


8. Enter a name for the restore point, then click “Create”



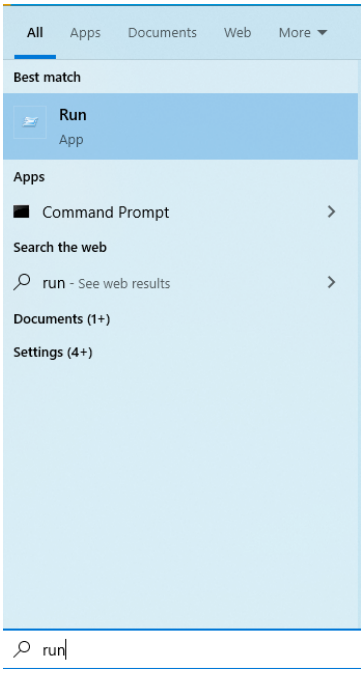
   The process should take a while.

After it finishes, you should see the message. Click “Close”.

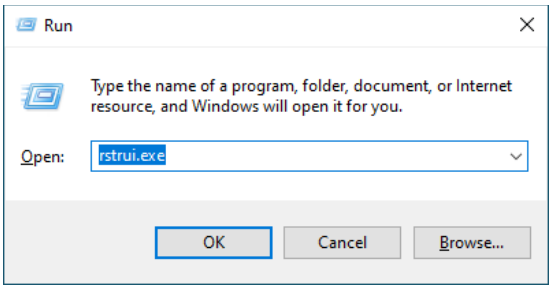


(Not required) To use the restore point:

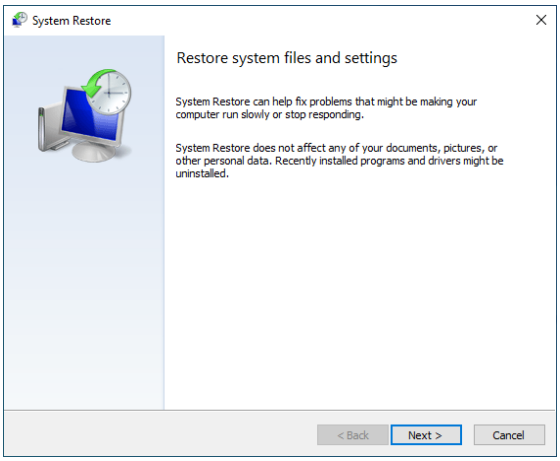
Open Start menu → type run



Type “rstrui.exe”

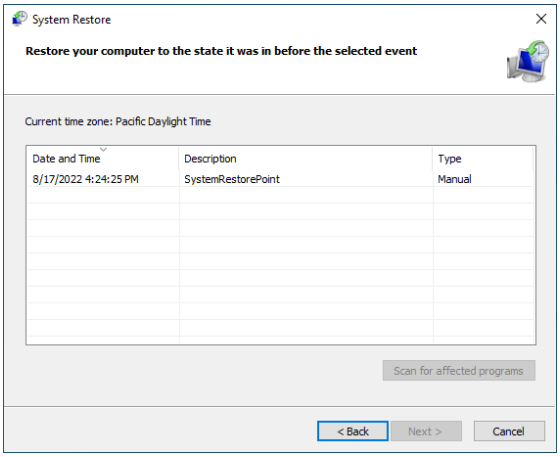


System Restore windows should then opened



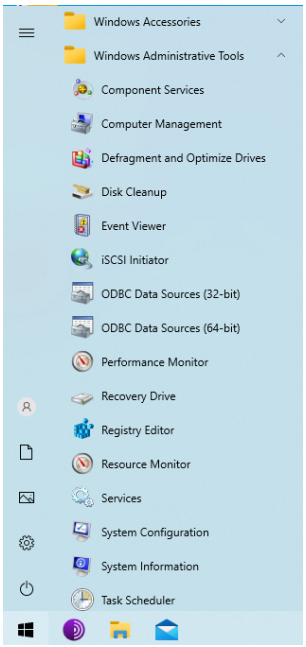
Now you can see the system restore point we created previously.

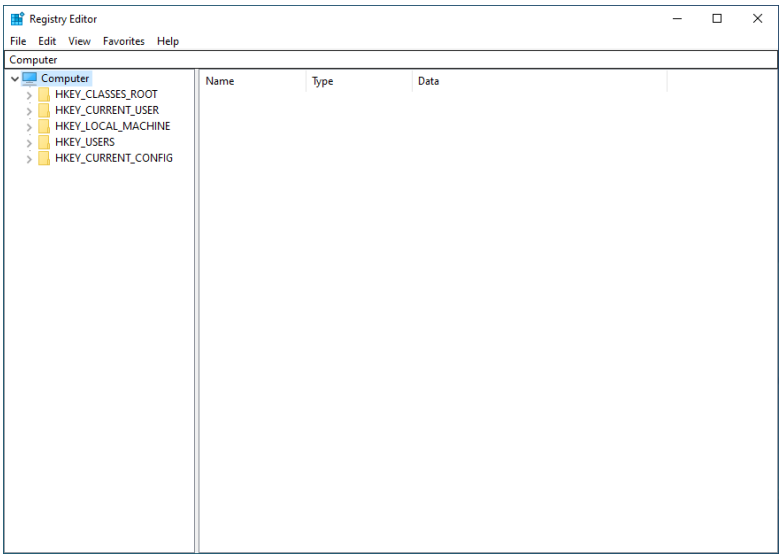
Select the restore point and keep following the instructions to finish the system restore.



Task 2: View five root keys

9. Open Start menu → Windows Administrative Tools → Registry Editor





10. Recall the function of the five root keys. Explore each key and see what it contains.

    Be Careful to not change any key value or delete any key from the registry.

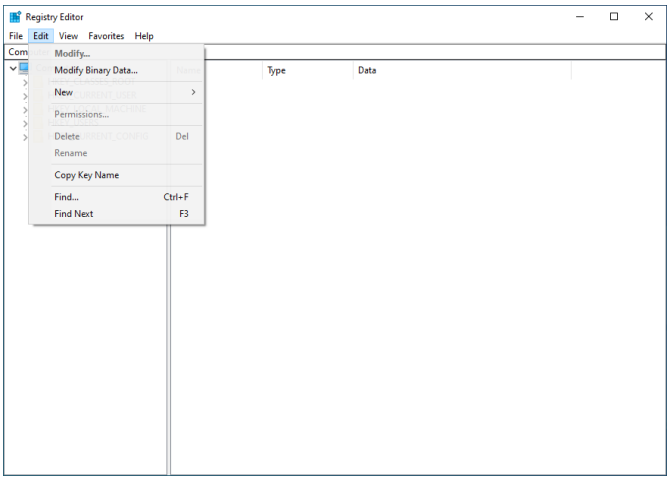
    Some focus point:

- HKEY_CLASSES_ROOT (HKCR) view extension .txt
- HKEY_LOCAL_MACHINE/ SAM/SECURITY subkeys

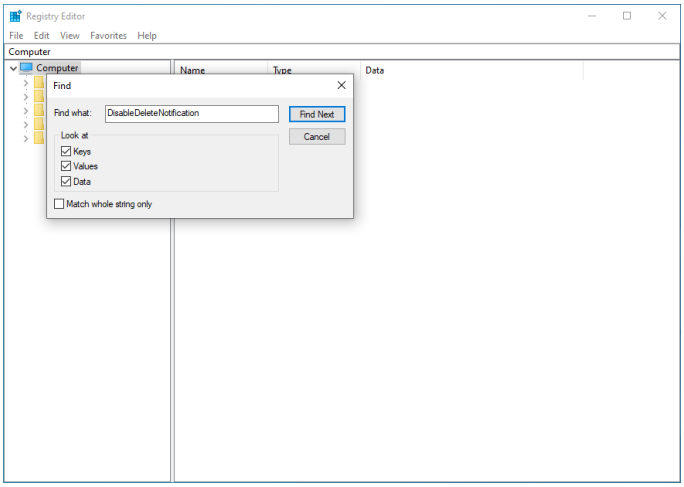
Task 3: Search, Create, Delete key/subkey

To search for key or content,

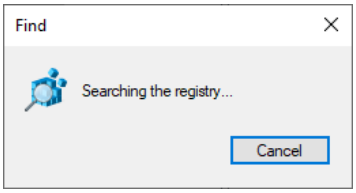
11. Click “Edit” → Find. Or press “Ctrl + f”



12. Type “DisableDeleteNotification” and click “Find Next”

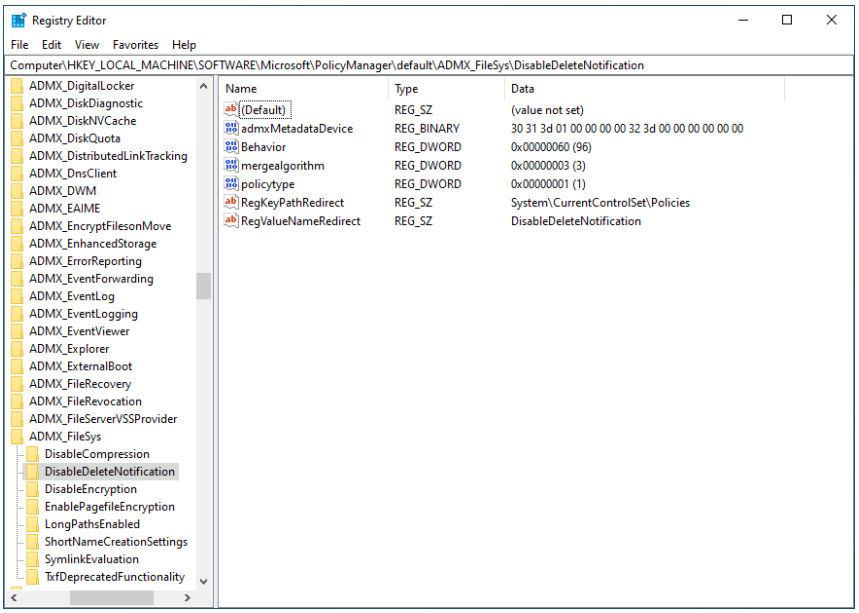


It may take a while for the search process.

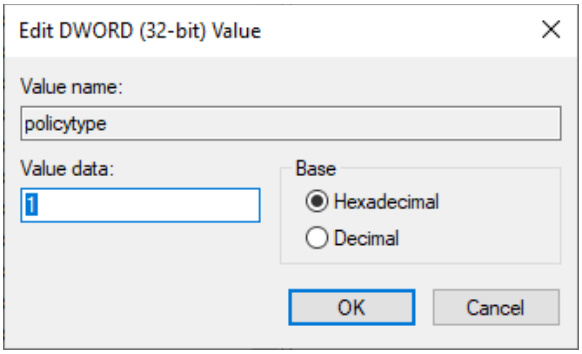


Before you change any setting from the registry editor, you should fully understand the content of the key.

https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.FileSys::DisableDeleteNotification



13. Double click to open and view the setting of the key

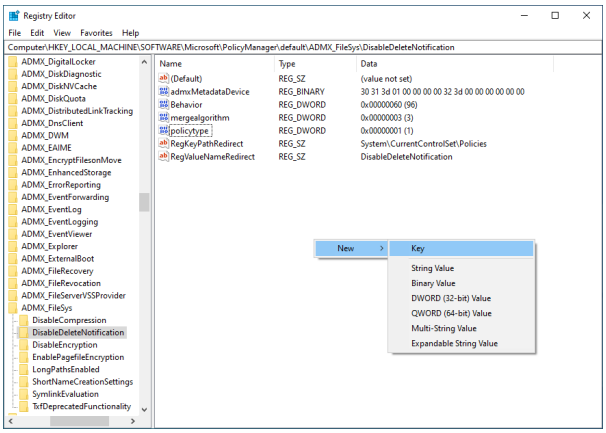


DO NOT change any setting. Click “Cancel” or close the windows to exit

If you change the value and click “OK”, the setting will be automatically saved and applied to the system.

(Not required) To create a key or key value,

Right click → New → Key

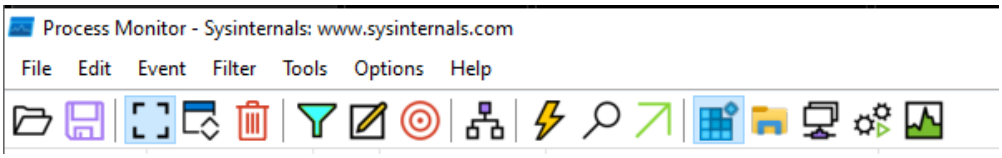


Task 4: View keys activity

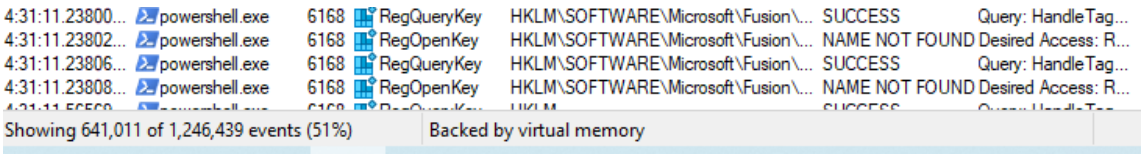
14. Download Process monitor (system tool) from microsoft official website

    https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

15. After opening the Process monitor, uncheck the file system, network, and process activity icons from the top bar.



You can see how frequently your system uses registry keys even if your system is in idle.



Question:

1. Where is the registry stored on the Hard Disk?

2. What does restore point for? Can restore points restore user data or documents?

3. Can you see anything under the SAM key (take a screenshot)? Why? (Google the answer if needed)

4. What is the safe way to modify Windows settings?