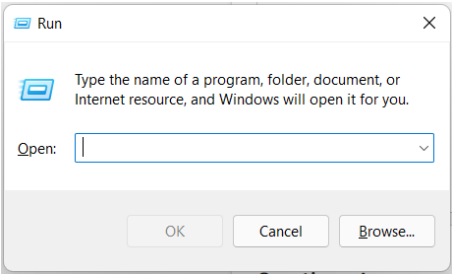
# Windows Forensics

lien du cours : https://tryhackme.com/r/room/windowsforensics1

# Regedit

## appuyez simultanément sur les touches Windows et R.

Une fenêtre d'exécution s'ouvre alors, qui ressemble à ceci :




```
regedit.exe
```

Structure du registre :

Le registre d'un système Windows contient les cinq clés racine suivantes :

1. HKEY_CURRENT_USER
2. HKEY_USERS
3. HKEY_LOCAL_MACHINE
4. HKEY_CLASSES_ROOT
5. HKEY_CURRENT_CONFIG

If you are accessing a live system, you will be able to access the registry using regedit.exe, and you will be greeted with all of the standard root keys we learned about in the previous task. However, if you only have access to a disk image, you must know where the registry hives are located on the disk. The majority of these hives are located in the `C:\Windows\System32\Config` directory and are:

1. **DEFAULT** (mounted on `HKEY_USERS\DEFAULT`)
2. **SAM** (mounted on `HKEY_LOCAL_MACHINE\SAM`)
3. **SECURITY** (mounted on `HKEY_LOCAL_MACHINE\Security`)
4. **SOFTWARE** (mounted on `HKEY_LOCAL_MACHINE\Software`)
5. **SYSTEM** (mounted on `HKEY_LOCAL_MACHINE\System`)

**Hives containing user information:**

Apart from these hives, two other hives containing user information can be found in the User profile directory. For Windows 7 and above, a user's profile directory is located in `C:\Users\<username>\` where the hives are:

1. **NTUSER.DAT** (mounted on HKEY_CURRENT_USER when a user logs in)
2. **USRCLASS.DAT** (mounted on HKEY_CURRENT_USER\Software\CLASSES)

The USRCLASS.DAT hive is located in the directory `C:\Users\<username>\AppData\Local\Microsoft\Windows`

The NTUSER.DAT hive is located in the directory `C:\Users\<username>\`

---

Revision #3
Created 11 October 2024 16:14:45 by Foufure
Updated 11 October 2024 18:57:27 by Foufure