Assignment #1: Forensic Analysis of Windows Registry (20th Jan'25)

Objective:

To delve deeper into Windows Registry Forensics, focusing on advanced techniques, artifact recovery, and the application of forensic tools to investigate complex scenarios.

Section 1: Practical Scenarios

1. **Scenario 1: A USB device was used to exfiltrate data from a system.**
    - Locate the Registry keys showing when the USB was connected.
    - Identify the drive letter assigned and the volume information.
2. **Scenario 2: A malicious program was set to run at startup.**
    - Use the **Run** and **RunOnce** keys to identify suspicious entries.
    - Find the program's path and analyze its metadata.
3. **Scenario 3: Recovery of User password.**
    - Extract the User password hash.

Section 3: Scenario & Questions

Extract the SYSTEM and SOFTWARE hives from your Windows system. (Hint: look in C:\Windows\System32\Config\) using **FTK Imager.** You can use any Registry parser (E.g. **RegRipper/Registry Explorer**) and then select the appropriate hive file to answer these questions (put a snapshot for each answer):

i. What is the computer name of the system?
ii. What is the name of the Operating System?
iii. What date/time (in UTC) was the Operating System installed? Hint: you may have to convert epoch time to human readable time using **DCode** tool.
iv. Is Remote Desktop service enabled? How do you know?
v. What is the IP address of the system?
vi. When was the system last shutdown?
vii. List out program names launching at startup.
viii. What are the name of USB drives (drive letter & volume information) you have plugged in to your system?
ix. List out the programs executed in your Windows system using **UserAssist** Registry key. You can create a table with program details like program name, execution path and last execution timestamp.
x. Extract the plain NTLM hash from the SAM & SYSTEM registry hives for currently logged-in user.