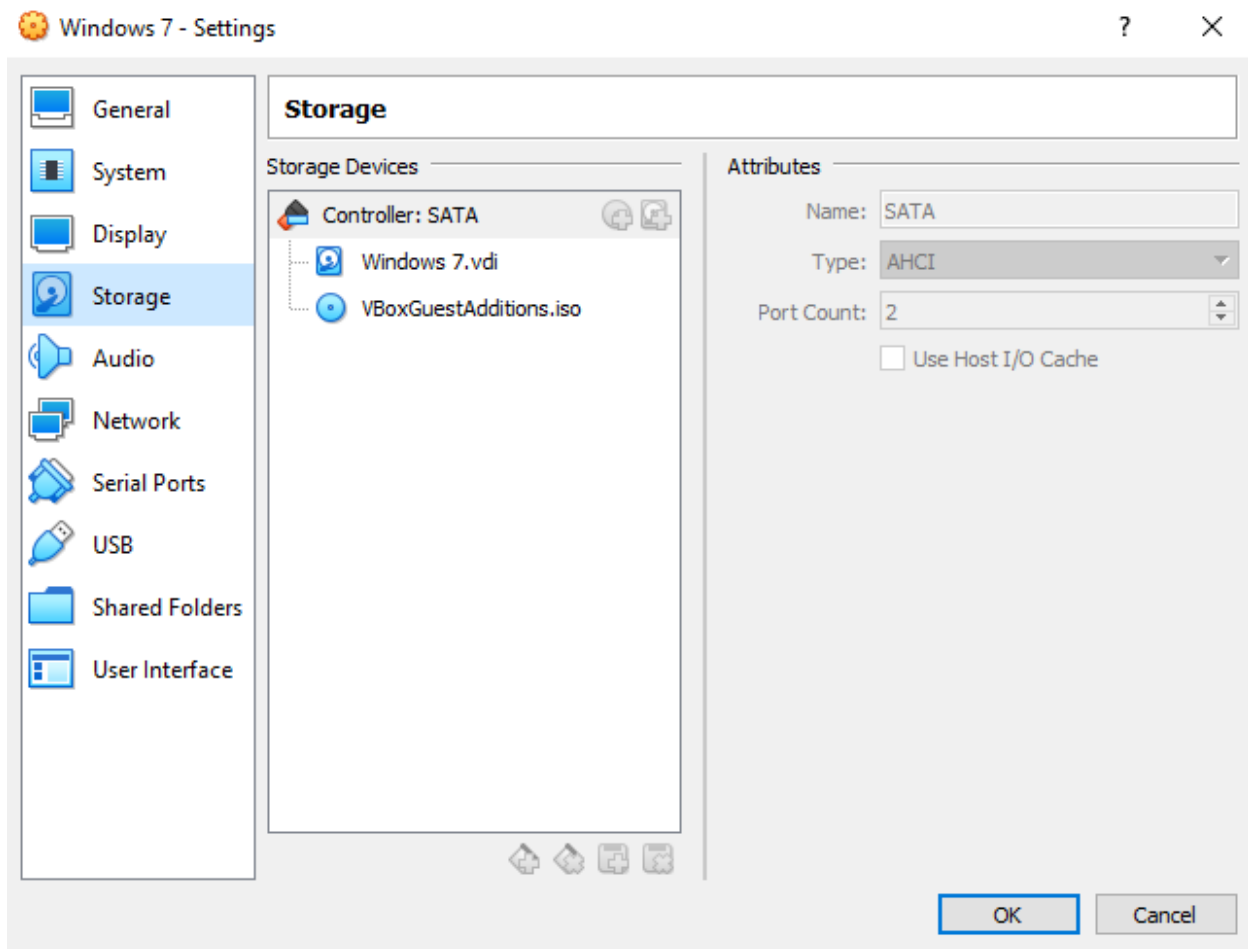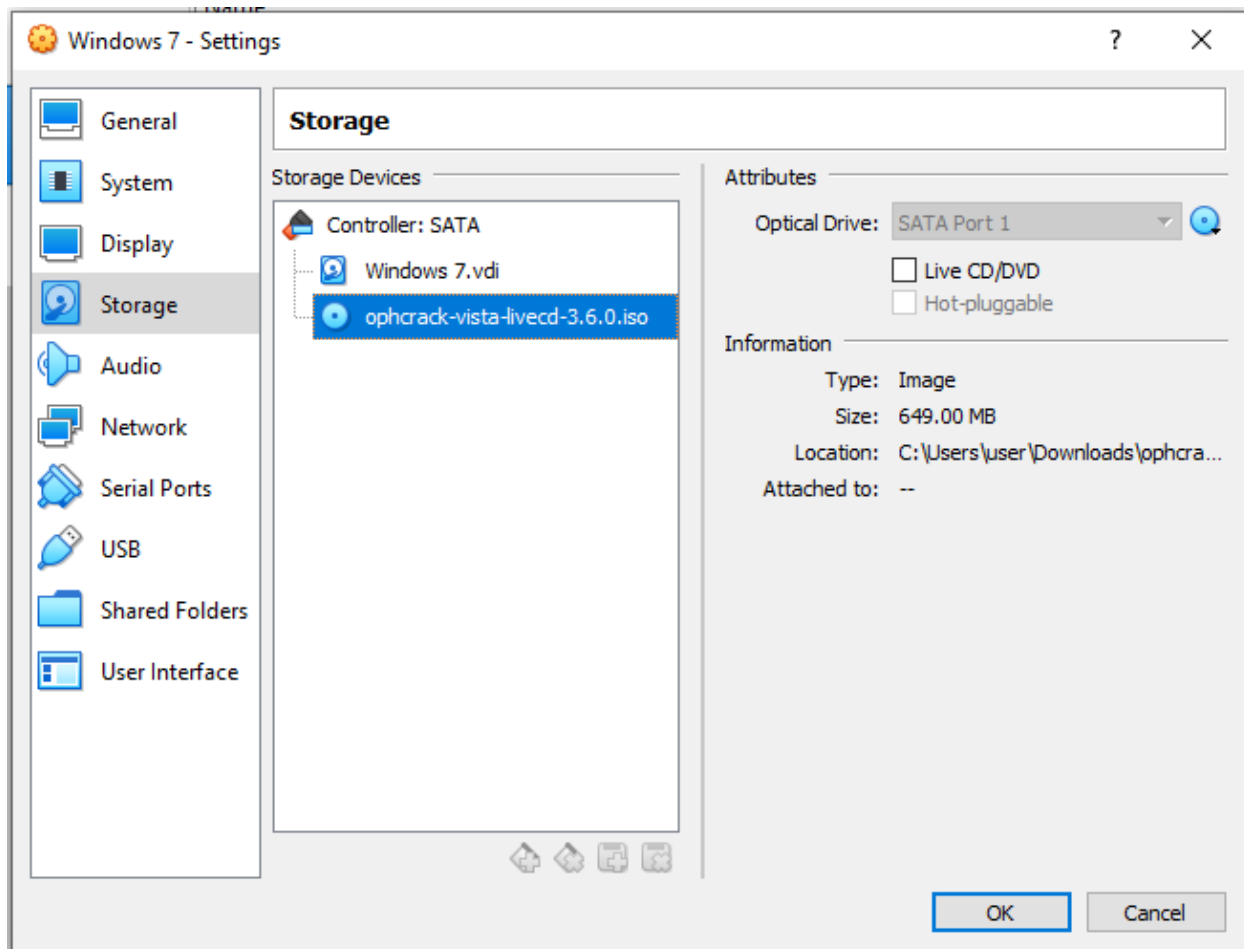# CS-MAJOR MAY

TASK 7

In this task we have to crack the password of windows machine by using a tool called ophcrack in virtual machine and try to get the password, along with mention the path of SAM file.

Step 1: First we have to download ophcrack tool from website https://ophcrack.sourceforge.io . Open the virtual machine and go to settings --> storage and upload the iso file.

Step 2: Reboot the machine and the first priority of the booting is from optical disk.
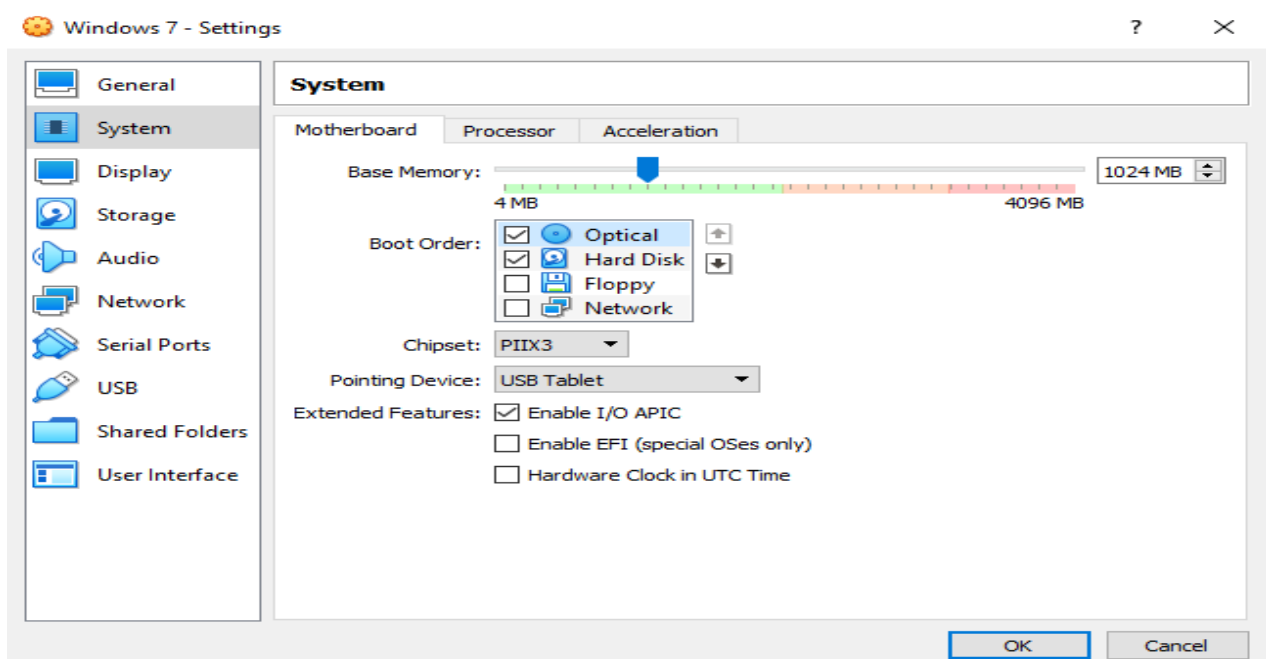
Step 3: start the machine and click the yes options out there and then the ophcrack tool automatically cracks the windows password.
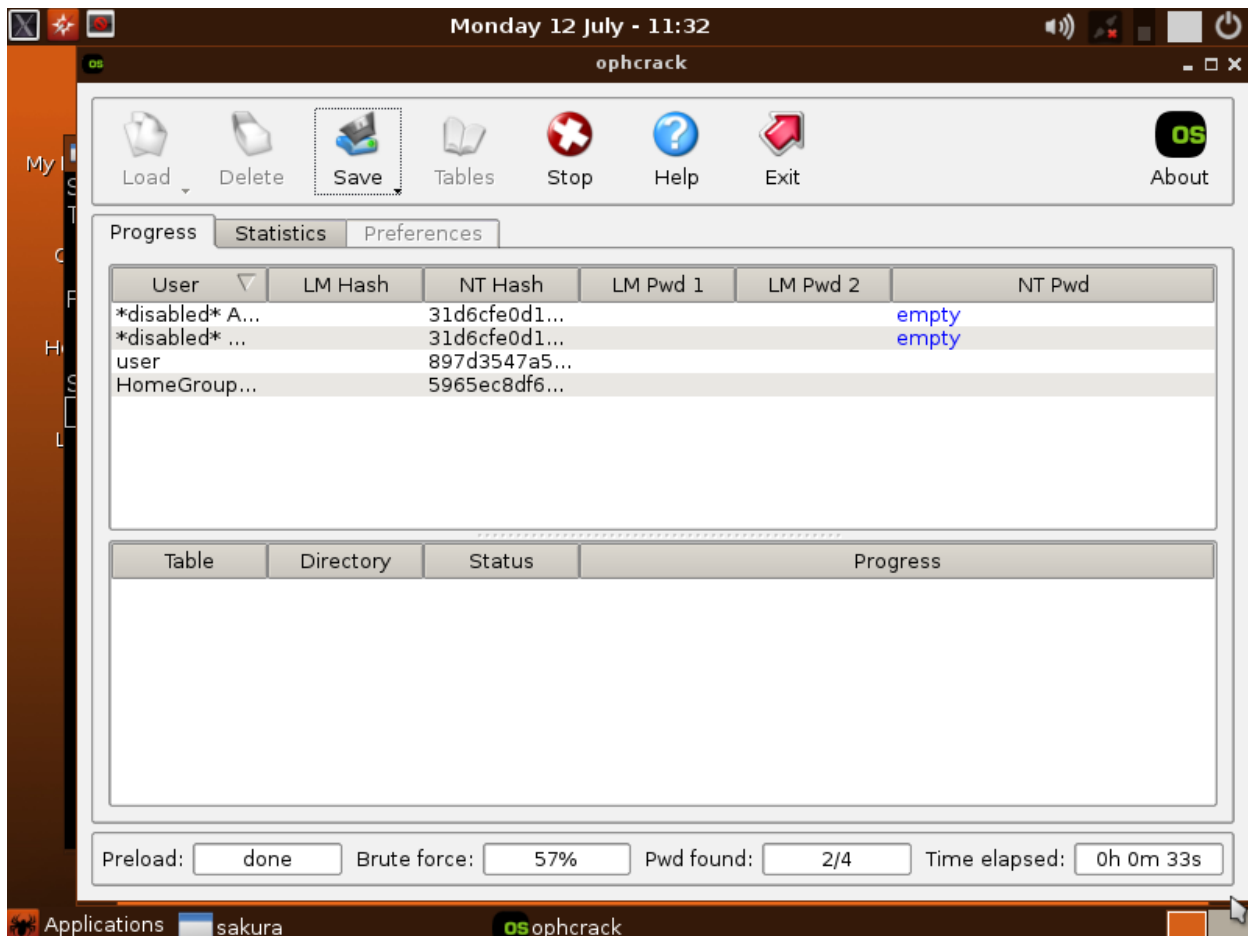
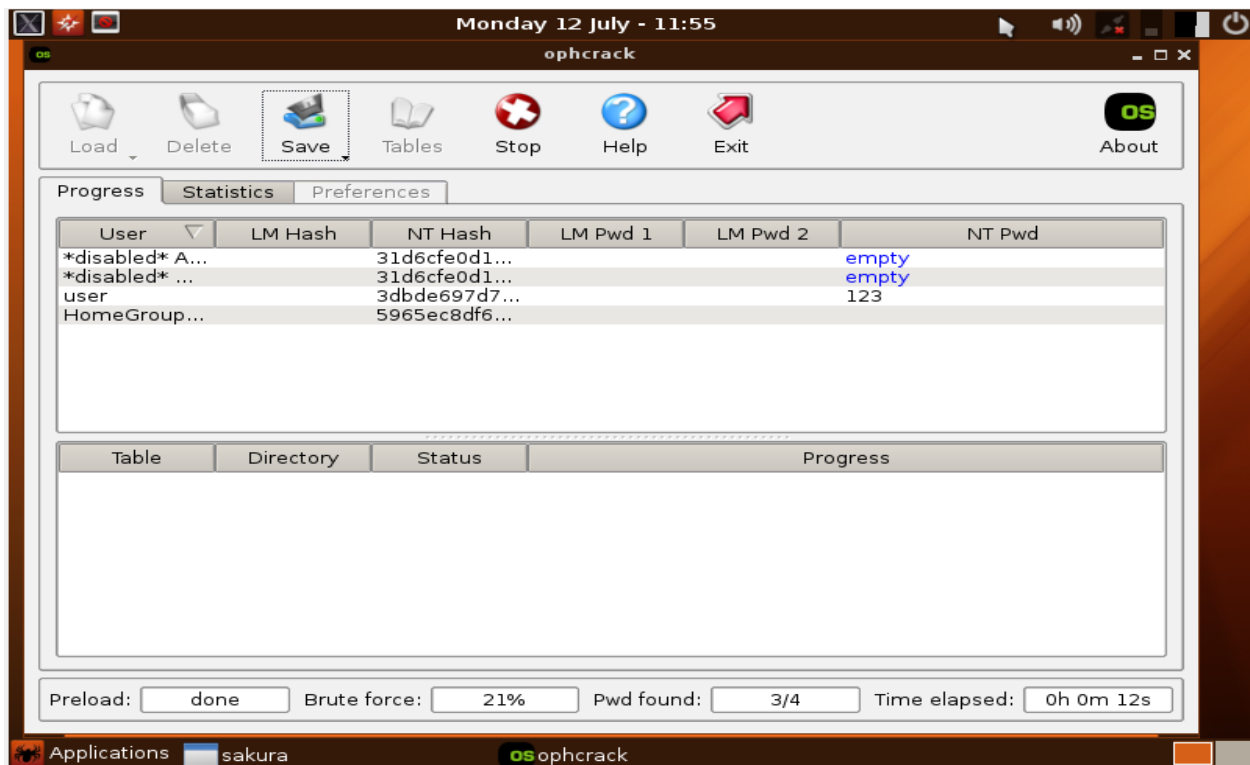The path of SAM file in windows is **%WinDir%\system32\config\sam.**
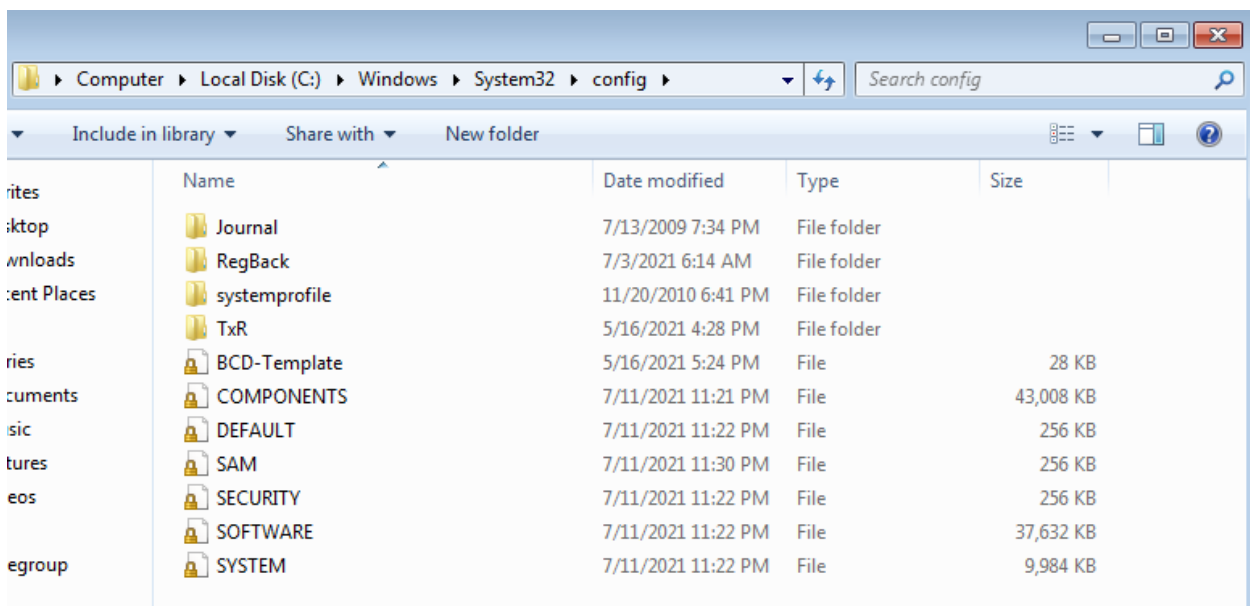
Usage of SAM file:

The **Security Account Manager (SAM)** is a database file in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users. The user passwords are stored in a hashed format in a registry hive either as

a LM hash or as an NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

Ophcrack tool search for SAM file in windows, it loads the encrypted SAM file in his interface, it searches for the password in the SAM file and when it is found it shows it to the users.