**Password cracking using Pwdump7 and Ophcrack**

**Course Name**: FRS301-Digital Forensics

**Student Name**: Nguyễn Trần Vinh – SE160258

**Instructor Name**: Lê Tiến Dũng

**Lab Due Date**: 17/2/2023

1. **Introduction**

In this experiment, we use Windows 7 and Windows 10 together with Pwdump7 and Ophcrack. There are a lot of users set up on the Windows 7 platform. Using managed access, we will access the encrypted hashes and forward them to the Windows 10 platform containing Ophcrack to crack the password.

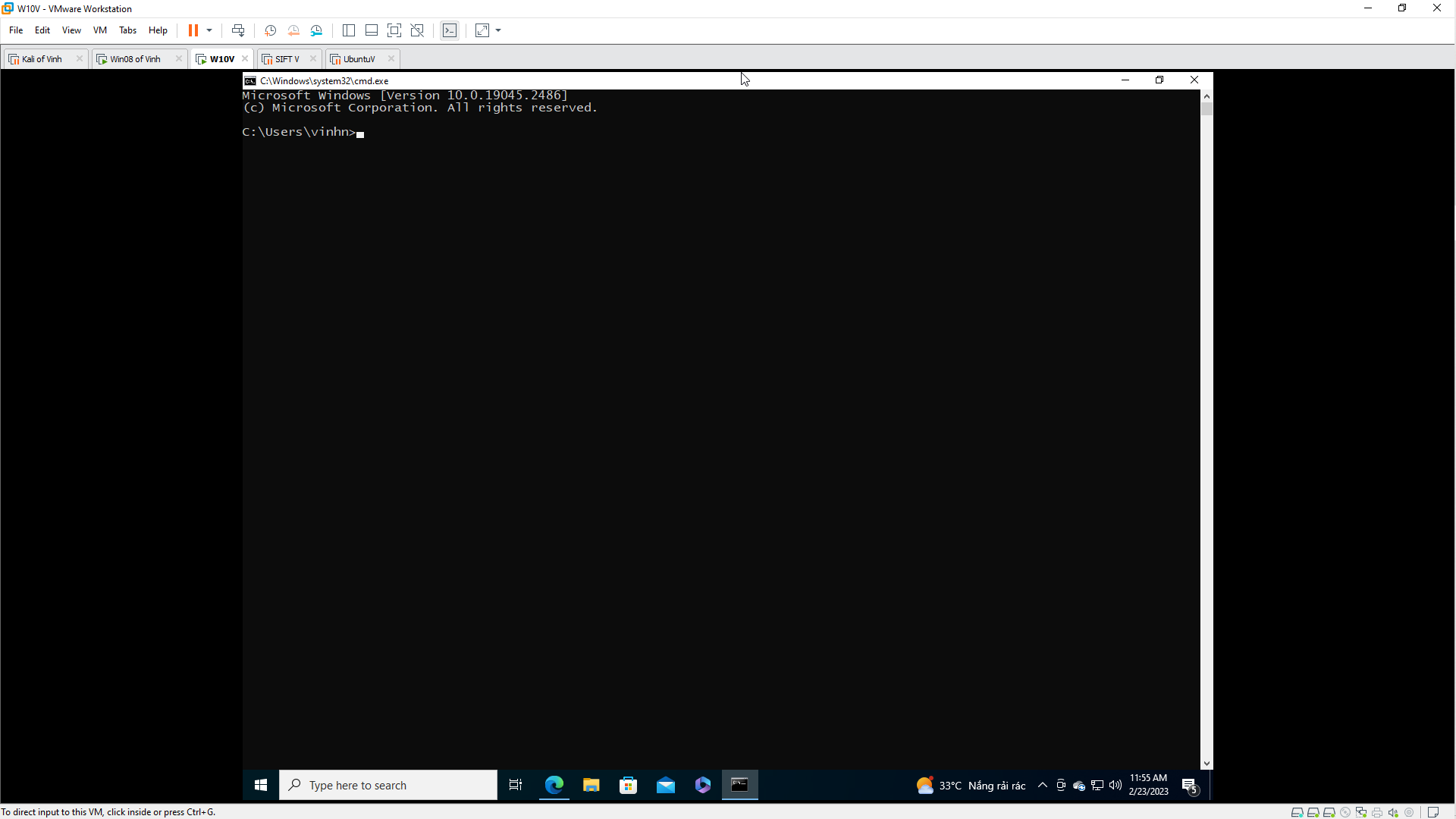
1. **Preparation**

<https://www.tarasco.org/security/pwdump_7/>

<https://ophcrack.sourceforge.io/download.php>

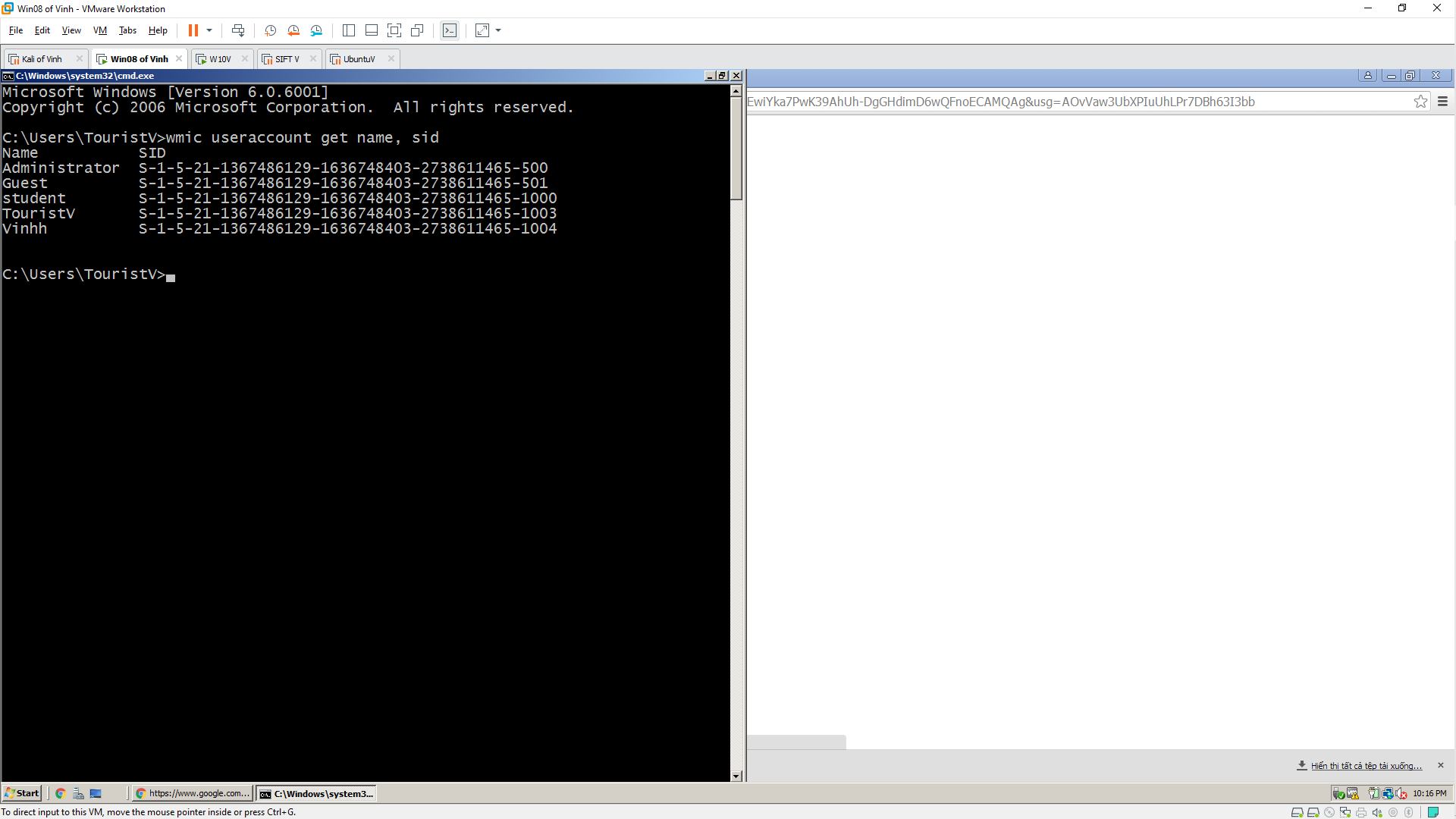
Computer running windows operating system 7, 10, disable virus and firewall

1. **Implementation steps**
2. Go to Windows 7 machine and run Command Prompt with administrative privileges.



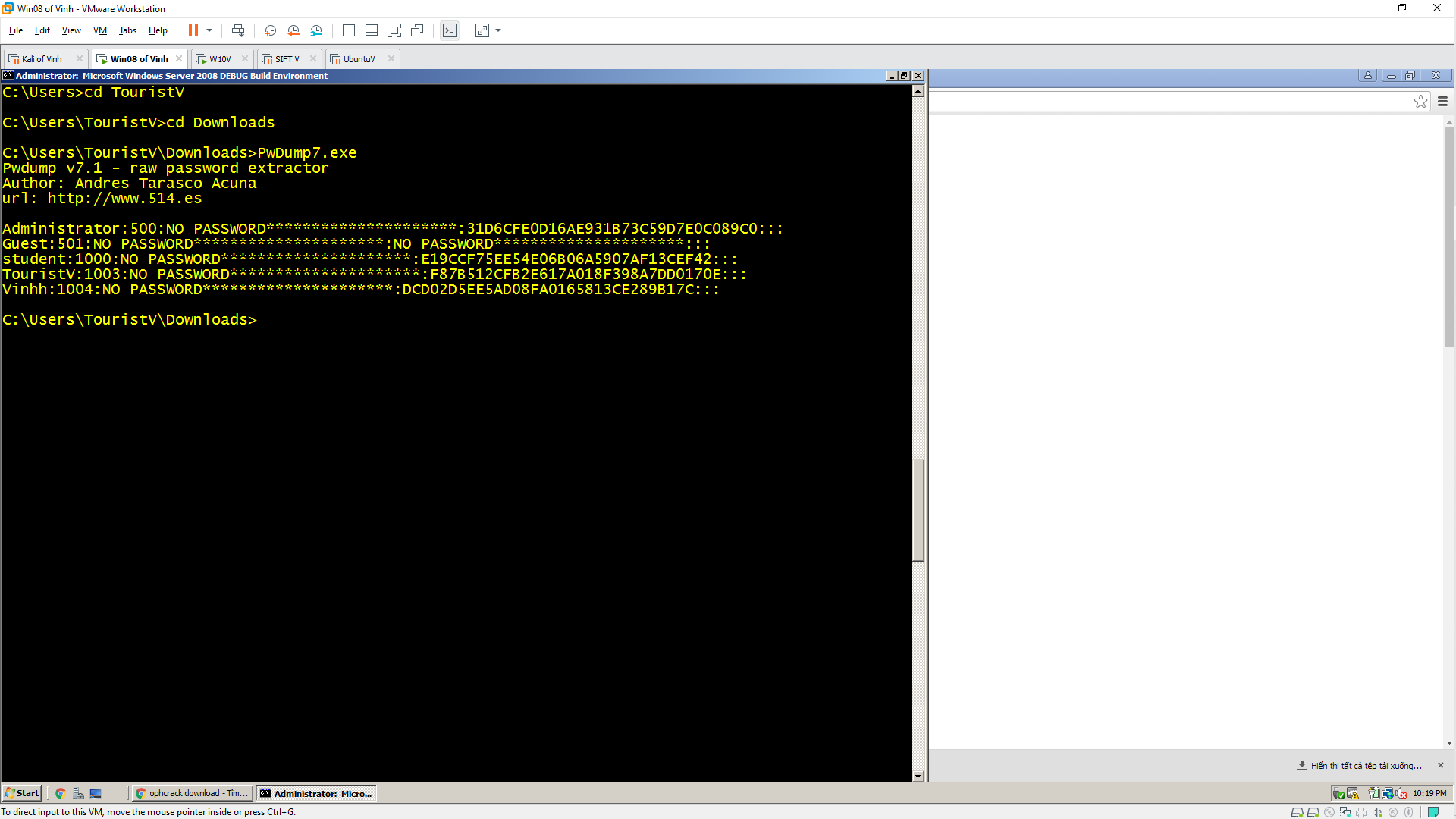
1. Input command below :

C:\Users\Win7-1>wmic useraccount get name, sid



1. Go to the directory containing pwdump7 and run the application. In our case pwdump7 is located on the desktop.

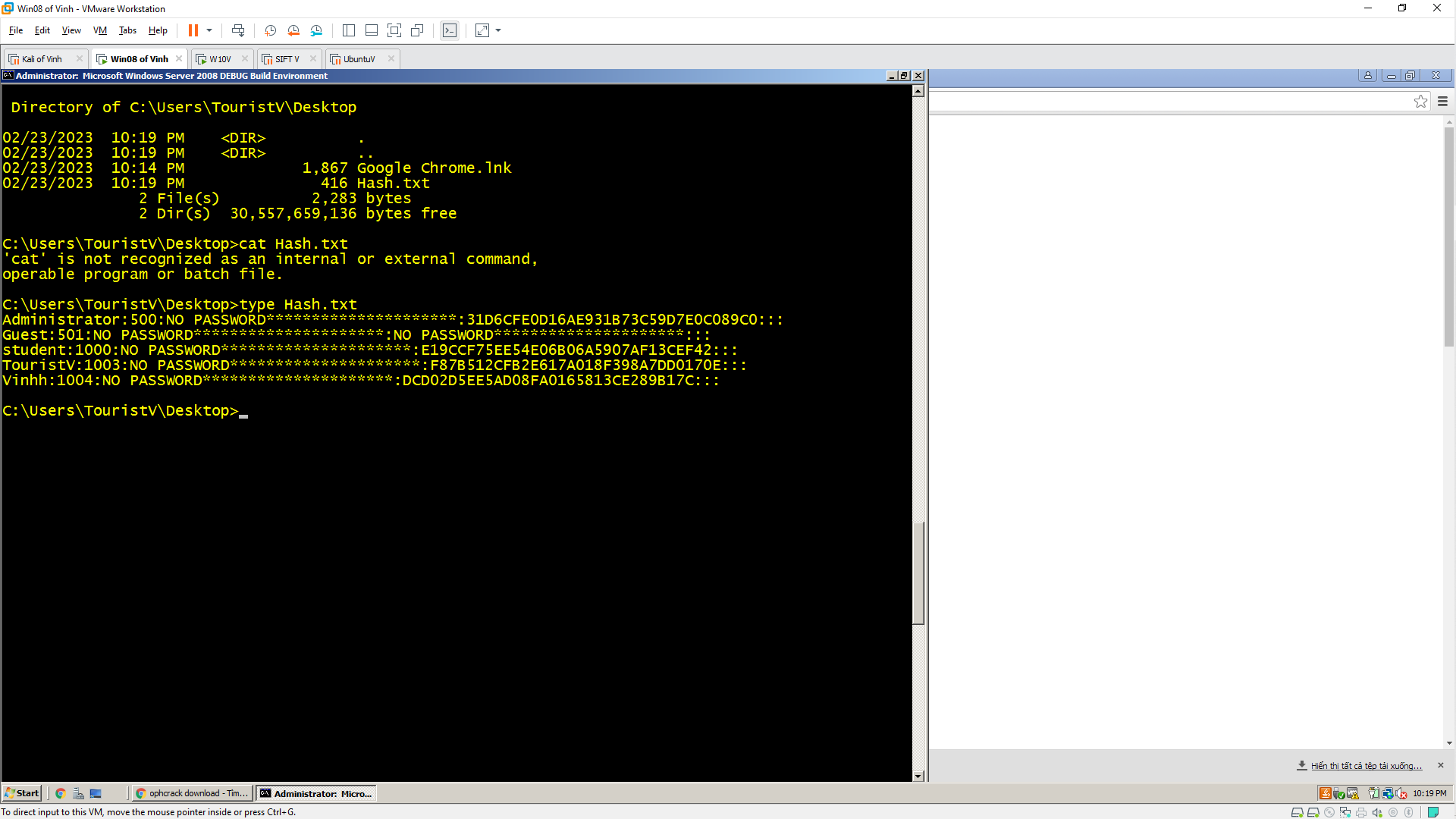
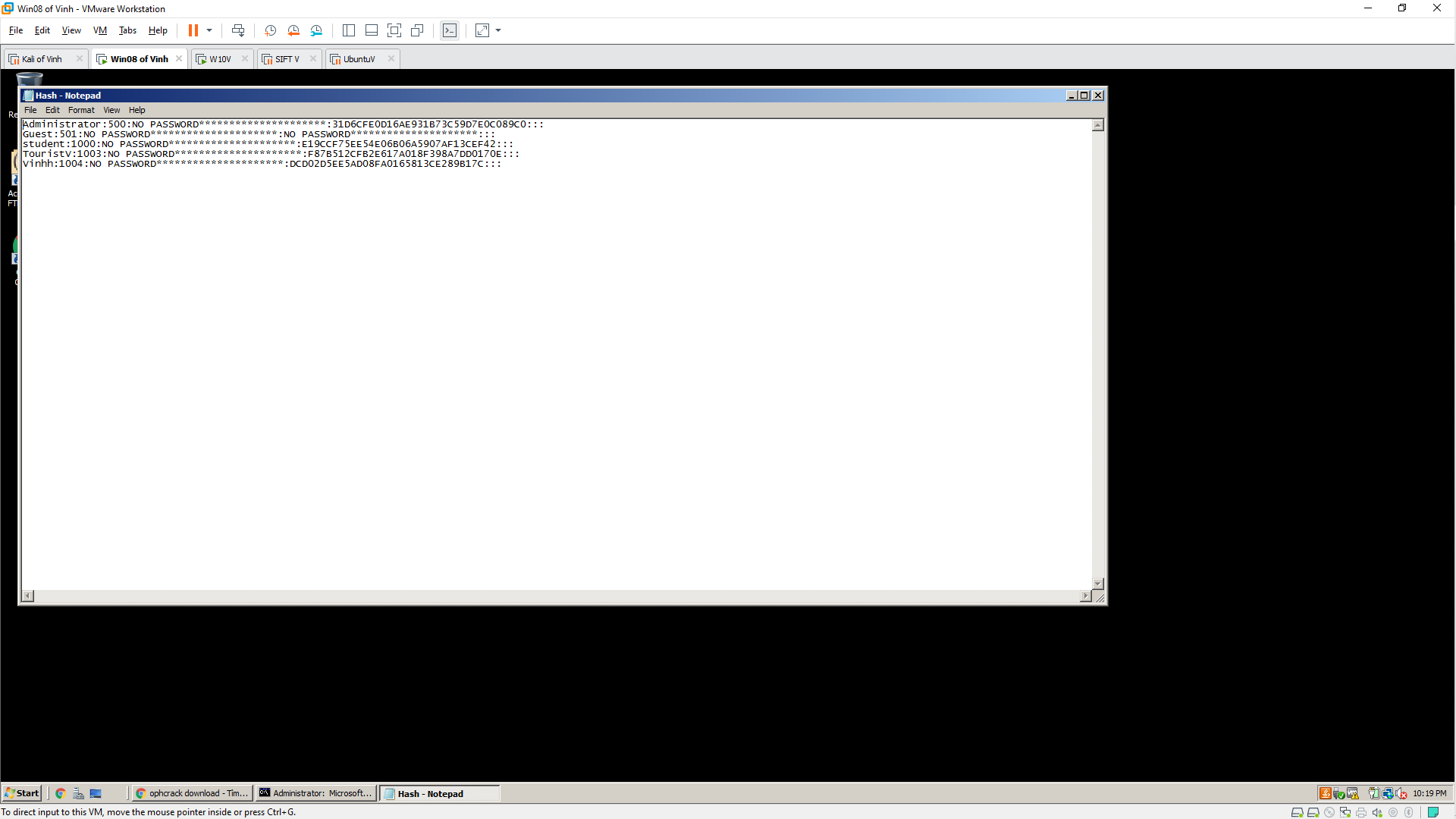
C:\Users\Win7-1\Desktop\pwdump7>pwdump7.exe



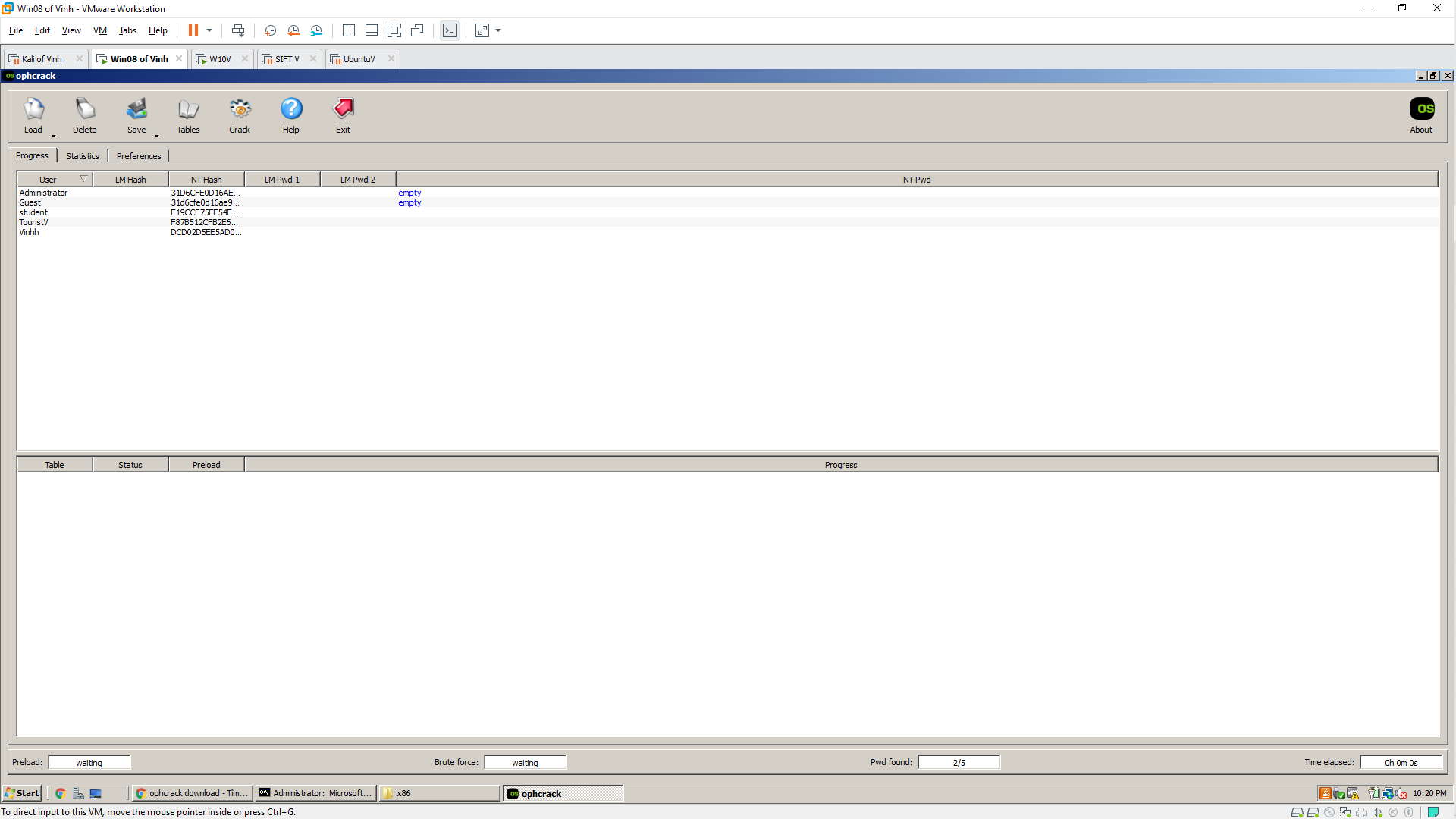
1. Copy the result to a text file using the command:

pwdump7.exe > C:\Users\Win71\Desktop\Hashes.txt

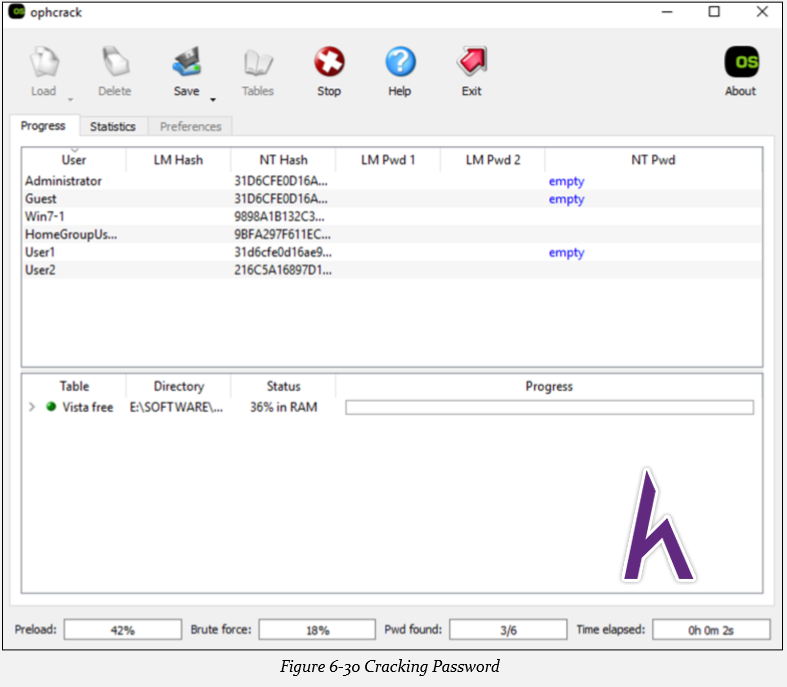
1. Check the Hashes.txt file on the desktop.

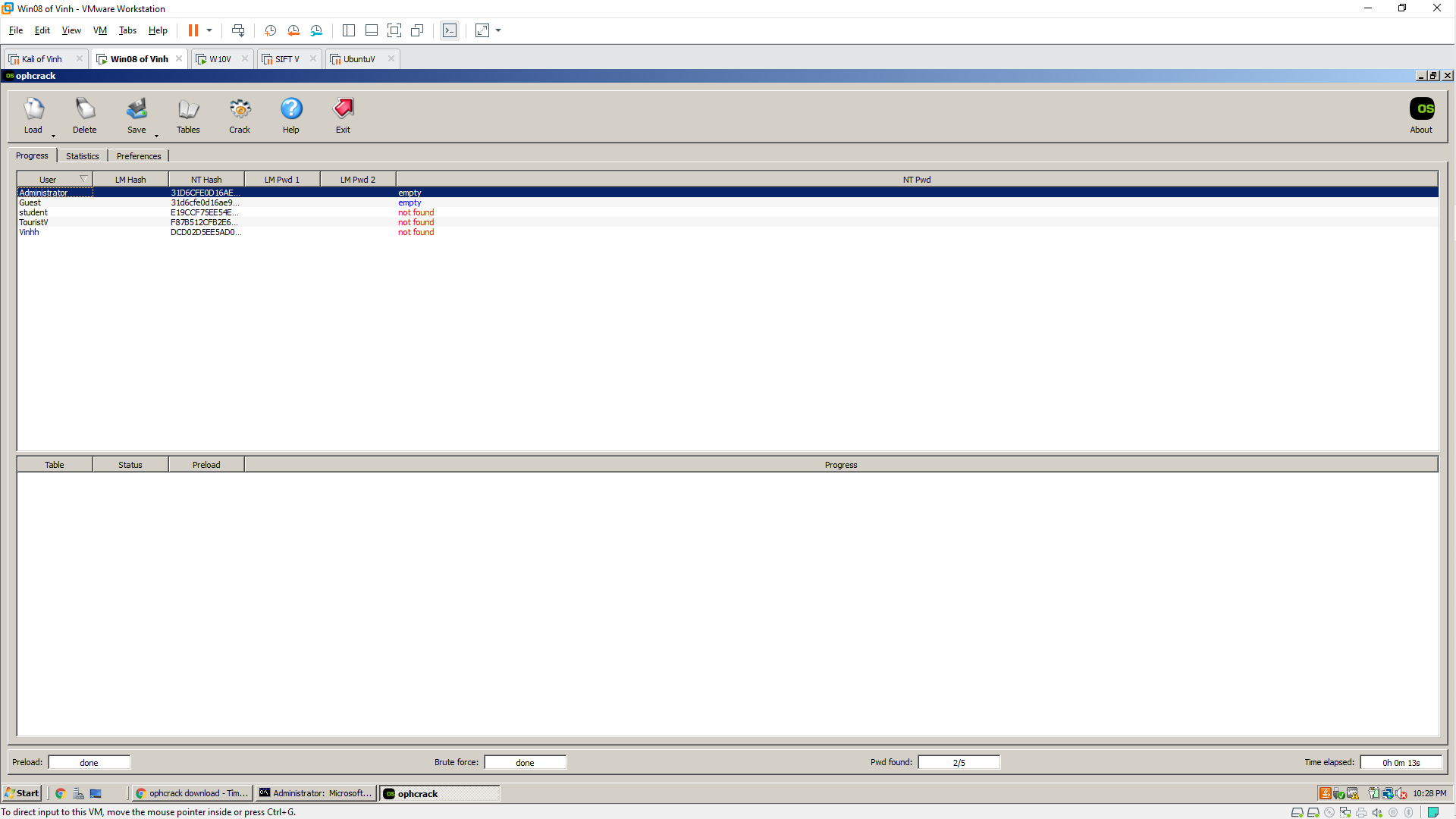
1. Transfer files to a remote machine (Windows 10). You can also install Ophrack on the same machine.
2. Run Ophrack on Windows 10 platform.
3. Click Load \ select PWDUMP File
4. Hashes have been loaded in the application as shown below.



1. Click the Table button to load/insert the table.
2. Select table. In this case, we choose Vista free table.
3. Select and press Install.
4. Choose a location for the folder containing the table. We use the default table of the application so the folder is in the same location as the application.
5. Click Ok



1. Press the Crack button to start the jailbreak.



1. The results show that the user does not set a password, the user with a cracked password. In the result there may be uncracked passwords, you can try other tables to crack.