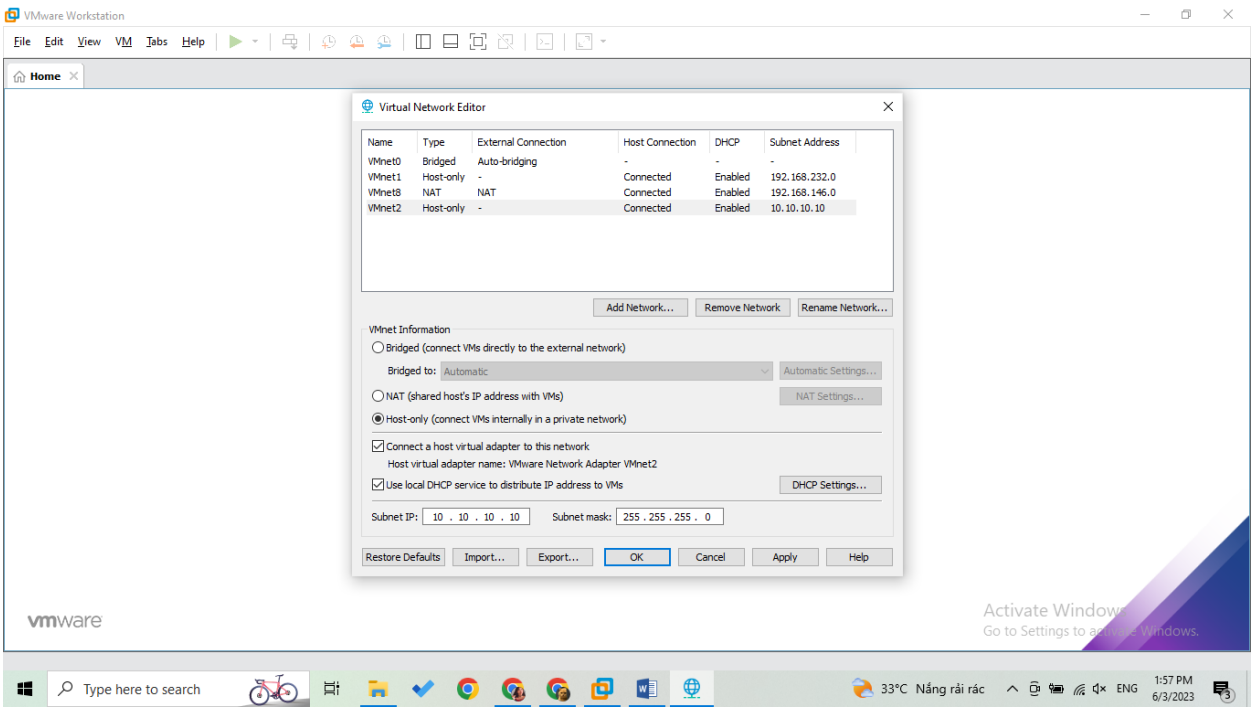
*Từ Ánh Minh*
*SE171699*

# LAB 7-1: Using Deep Freeze to Preserve Physical Systems

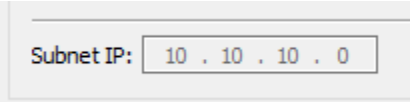
In this lab, we need to launch 3 virtual machines in the system, therefore I'm going to use Ubuntu, Kali Linux and Sansift. Three virtual machines are going to connect through and internal local network VMNet2

But first of all, I create a new VMNet2 :




Go to edit virtual machine

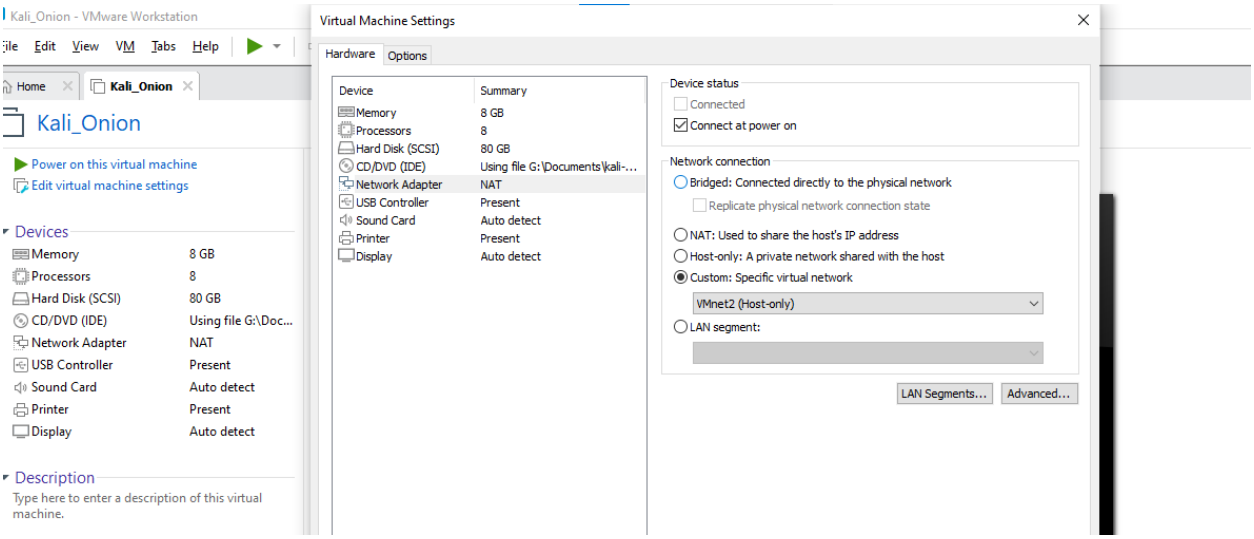
Running as an administrator => change the subnet IP to 10.10.10.0




⇨ Click OK for finishing

## Configuration for Kali:

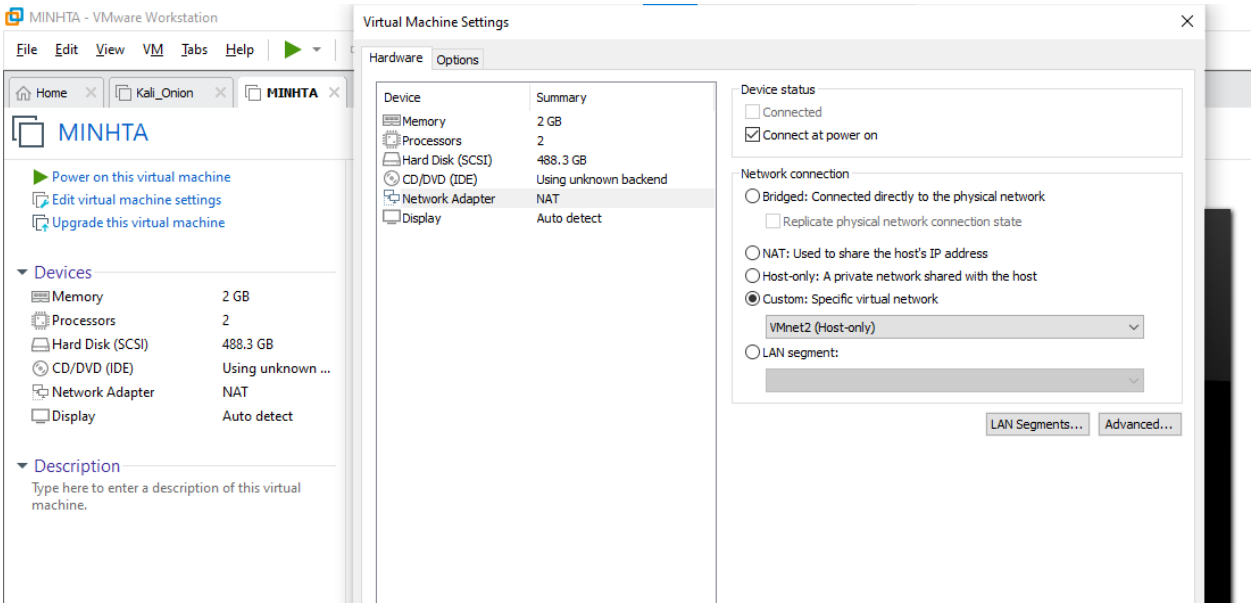
Turn on the kali




Click edit virtual machine setting

- ⇨ Go to the network adapter
- ⇨ Choose custom: VMnet2 (Host-only) as above
- ⇨ Ok

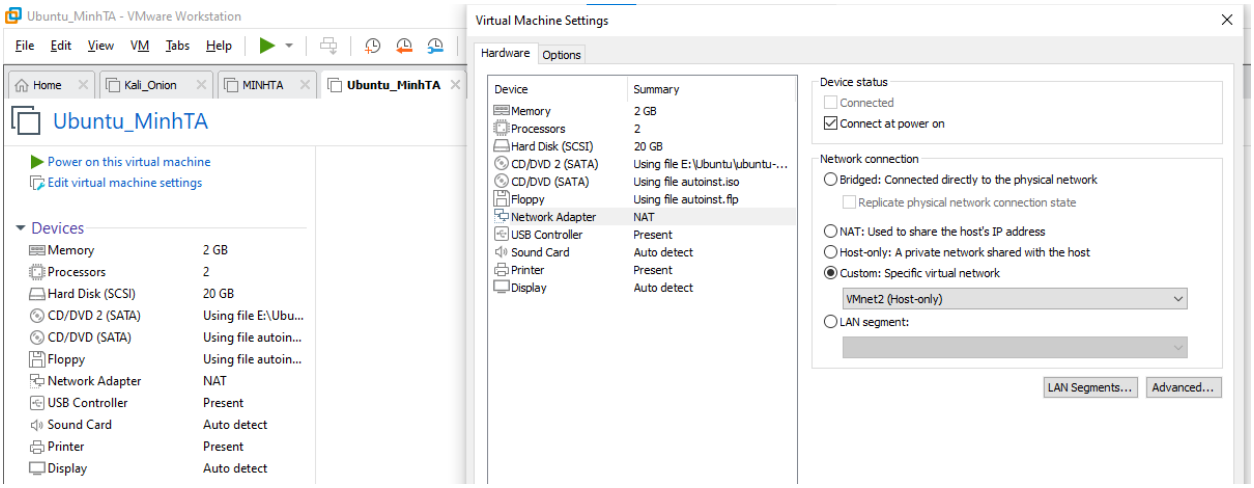
## Configuration for San:



⇨ Do the same for sansift virtual machine

⇨ Done

**Configuration for Ubuntu:**



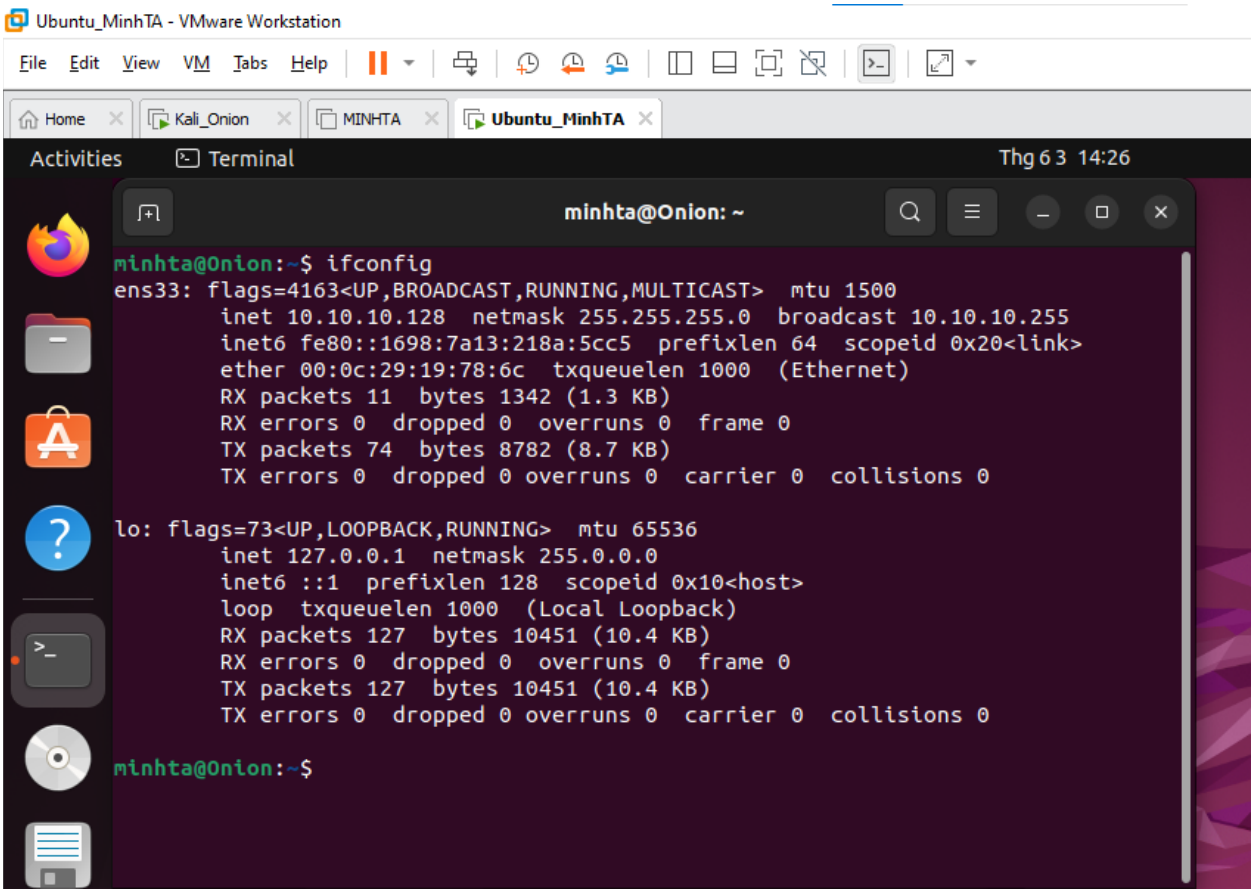

⇨ Do the same for sansift virtual machine

⇨ Done

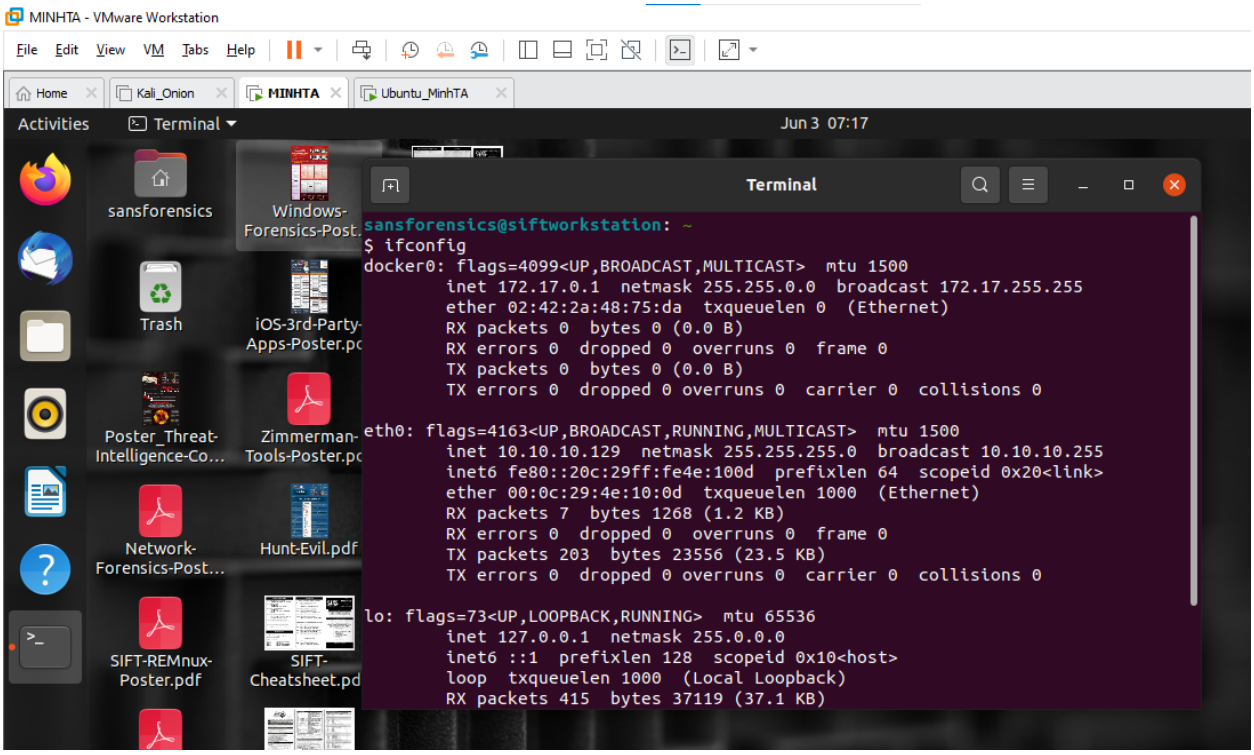
Then the next step is that we are going to check if these virtual machines are in the same network:

**Ubuntu: 10.10.10.128**

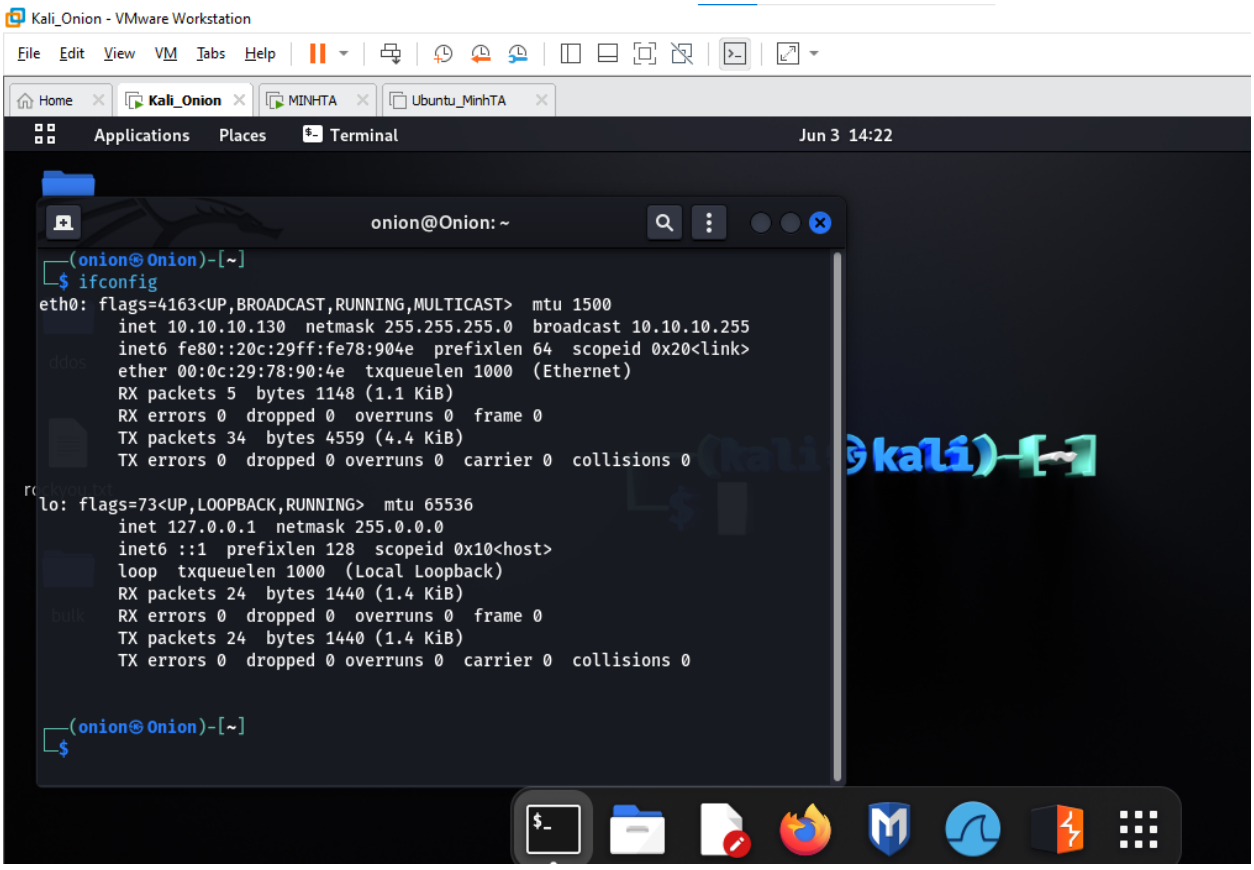
Use “ifconfig” command



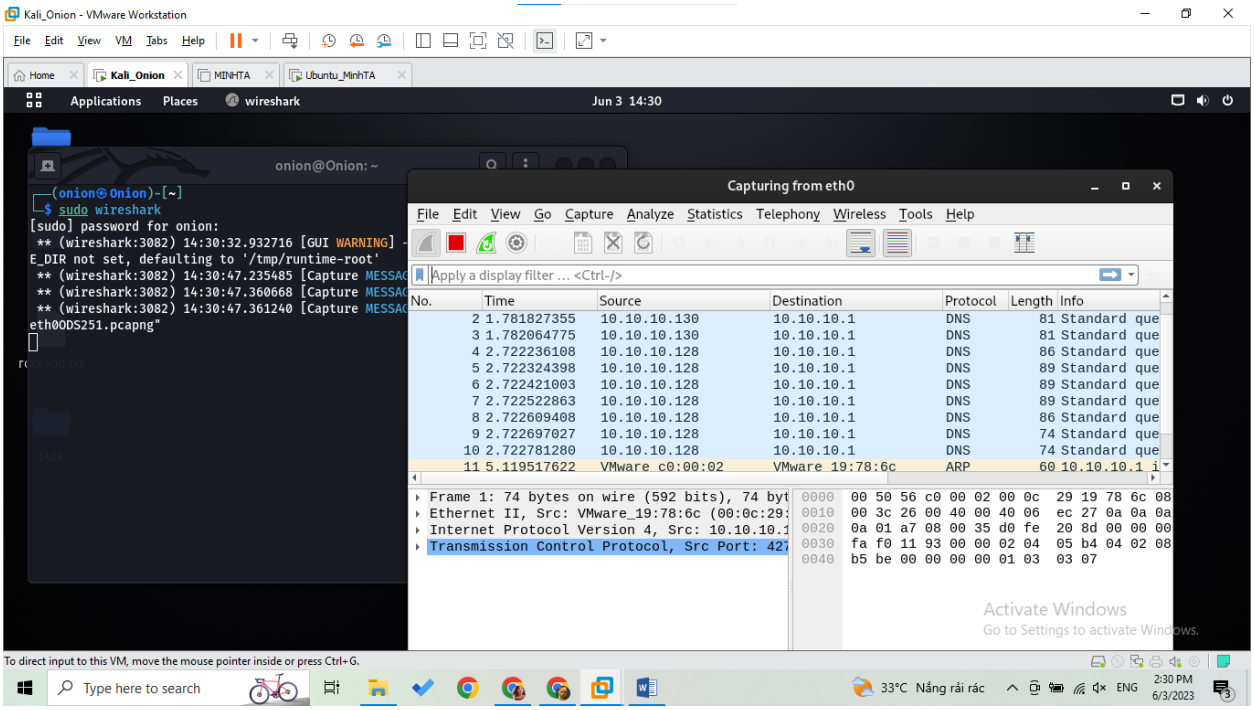

**Sansift: 10.10.10.129**




# Kali: 10.10.10.130



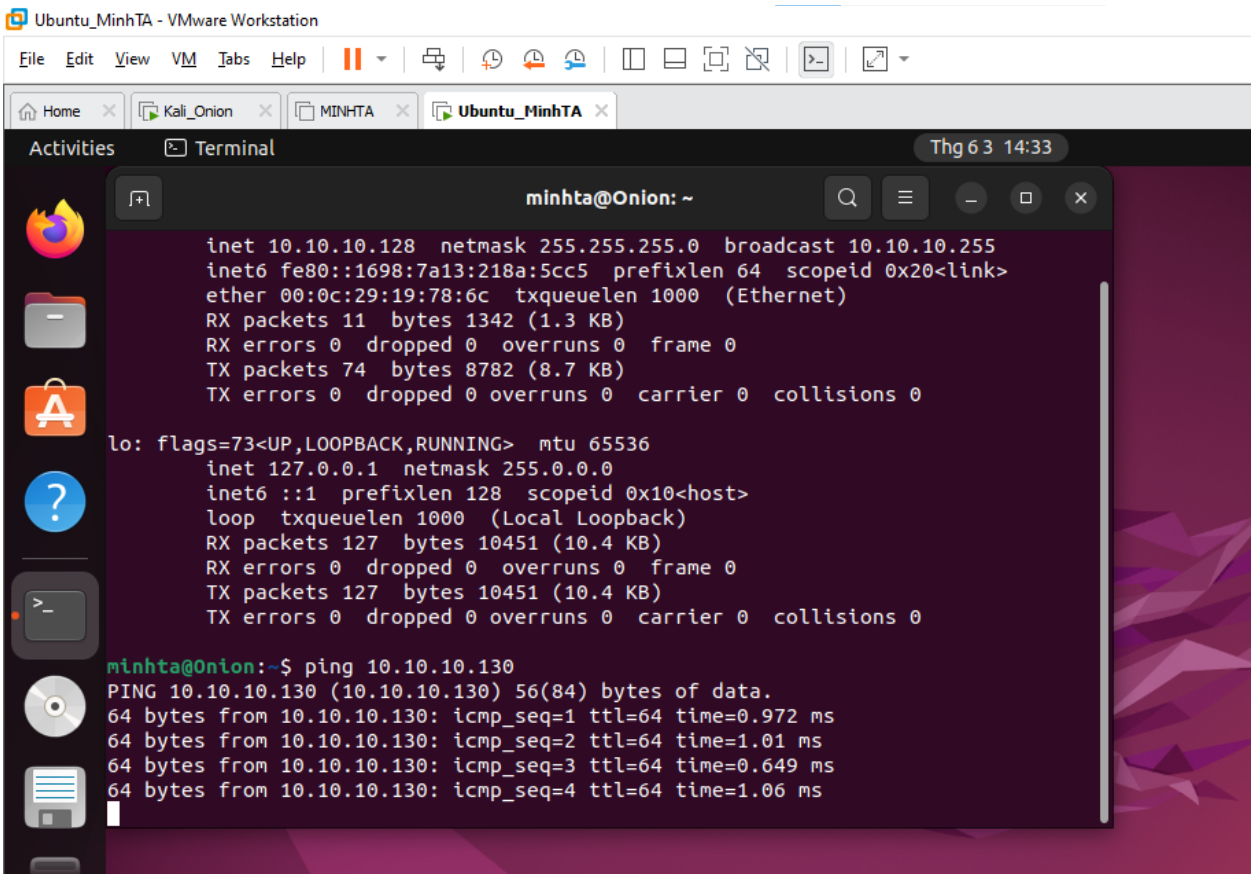
We sudo wireshark to turn on wireshark to catch:




⇨ Catch on the nic eth0

Then I am going send a package by ping from the Ubuntu to the kali linux

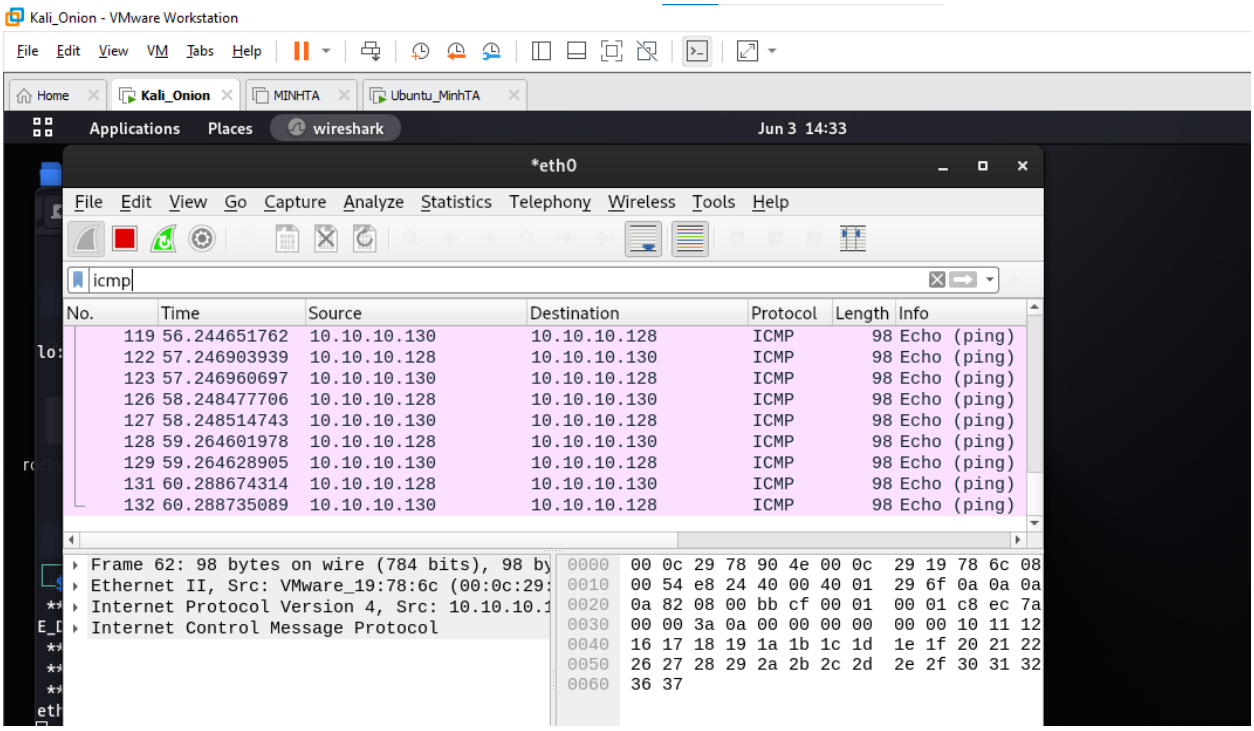
**ping 10.10.10.130**




⇨

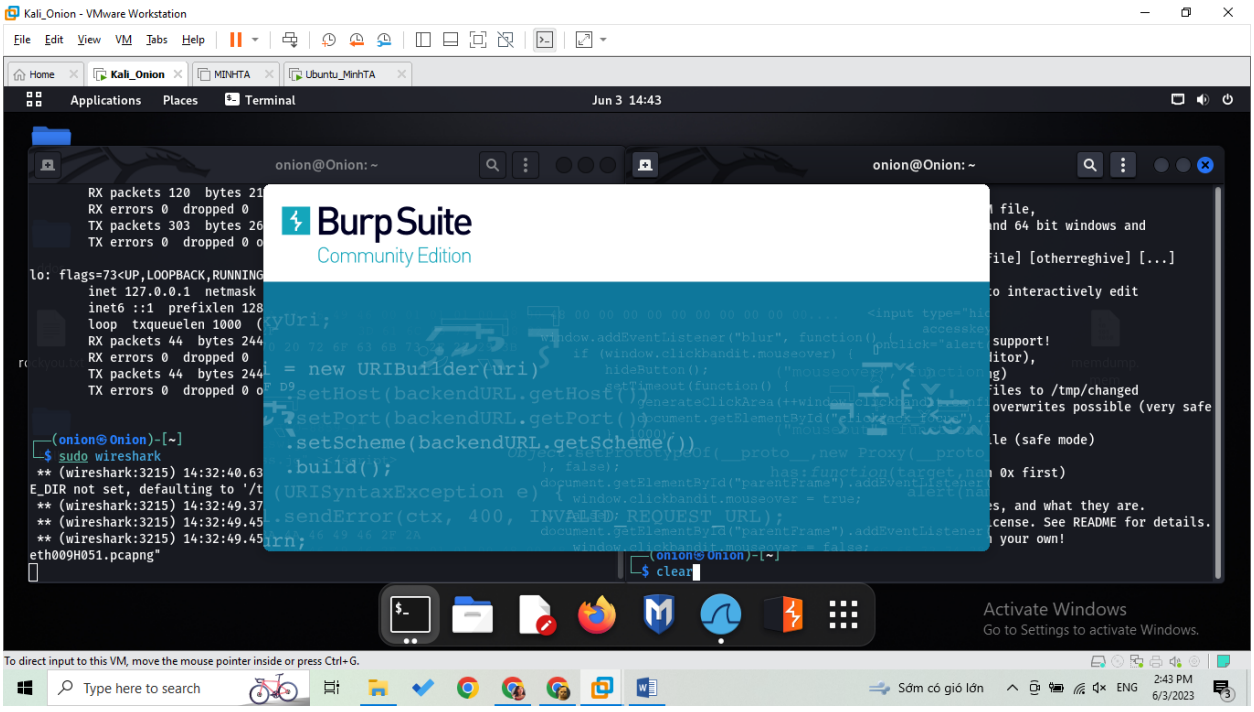
Switch to the kali to check

There are a bunch of package are just delivered



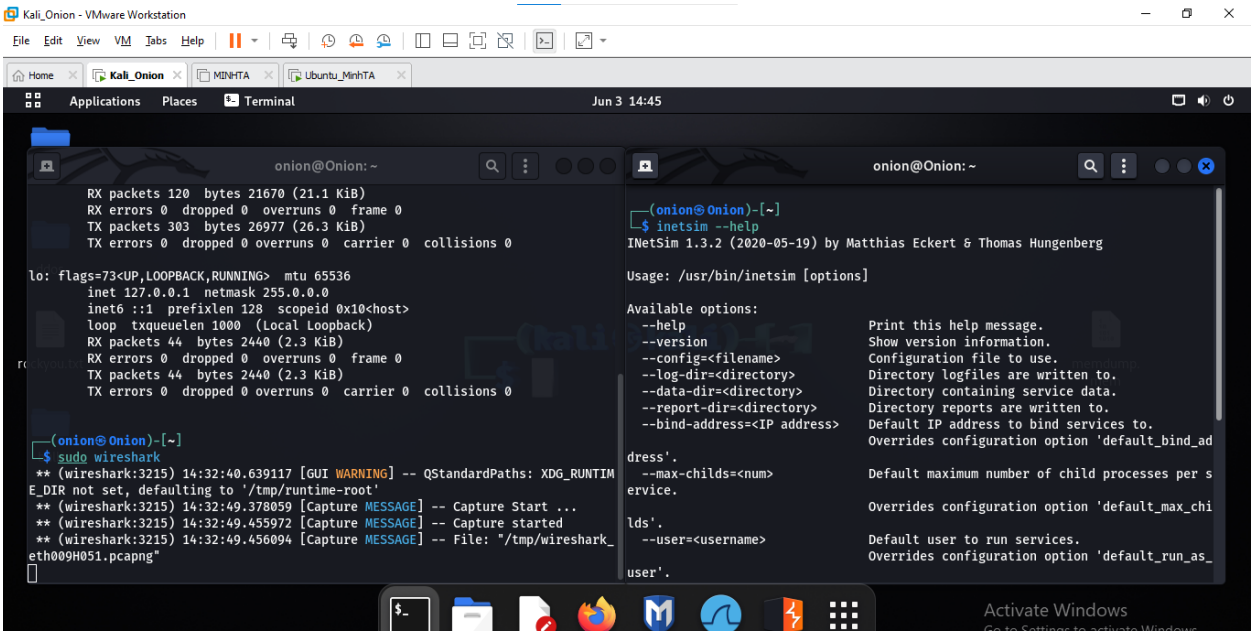

⇨ Catch successfully

# Start to install burpsuite



⇨ **I installed burpsuite successfully**

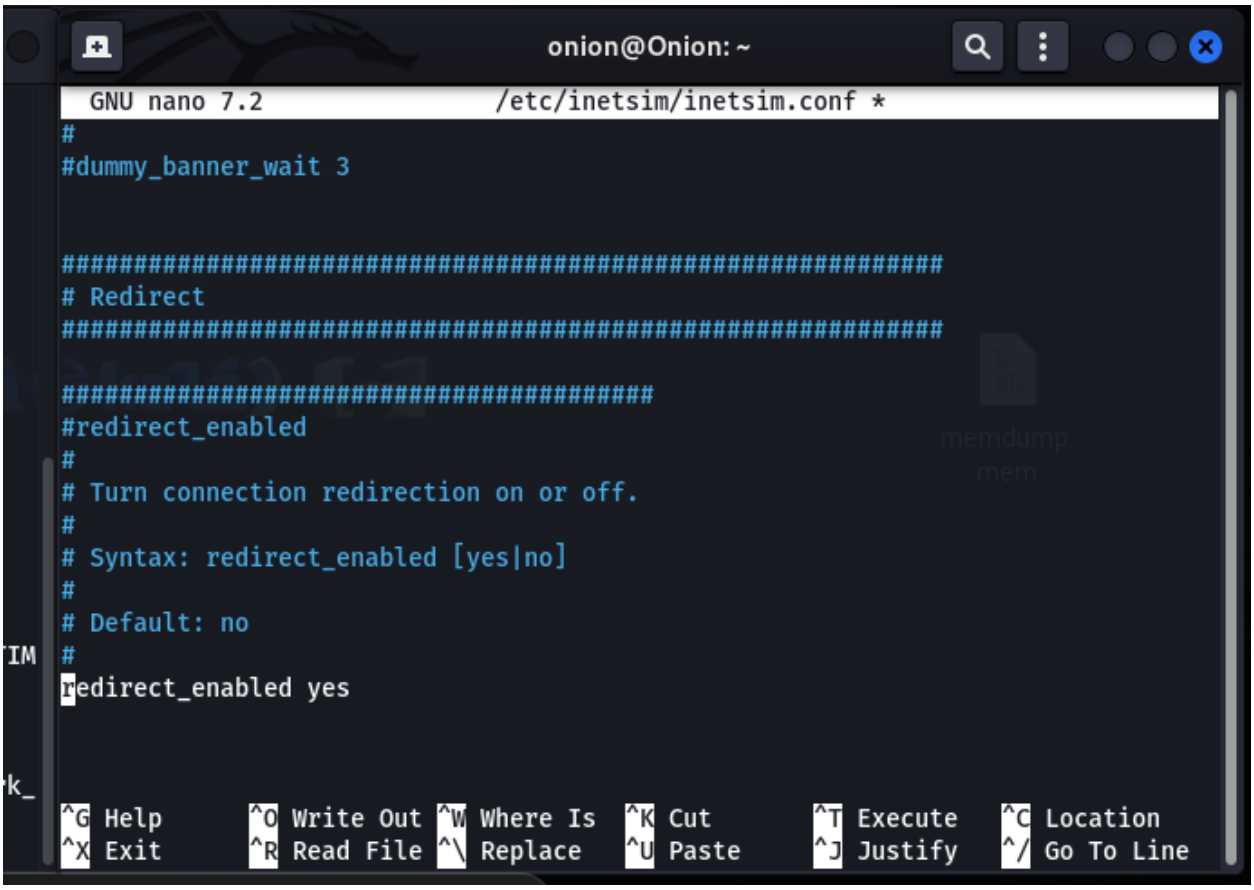
## Start to install inetsim:



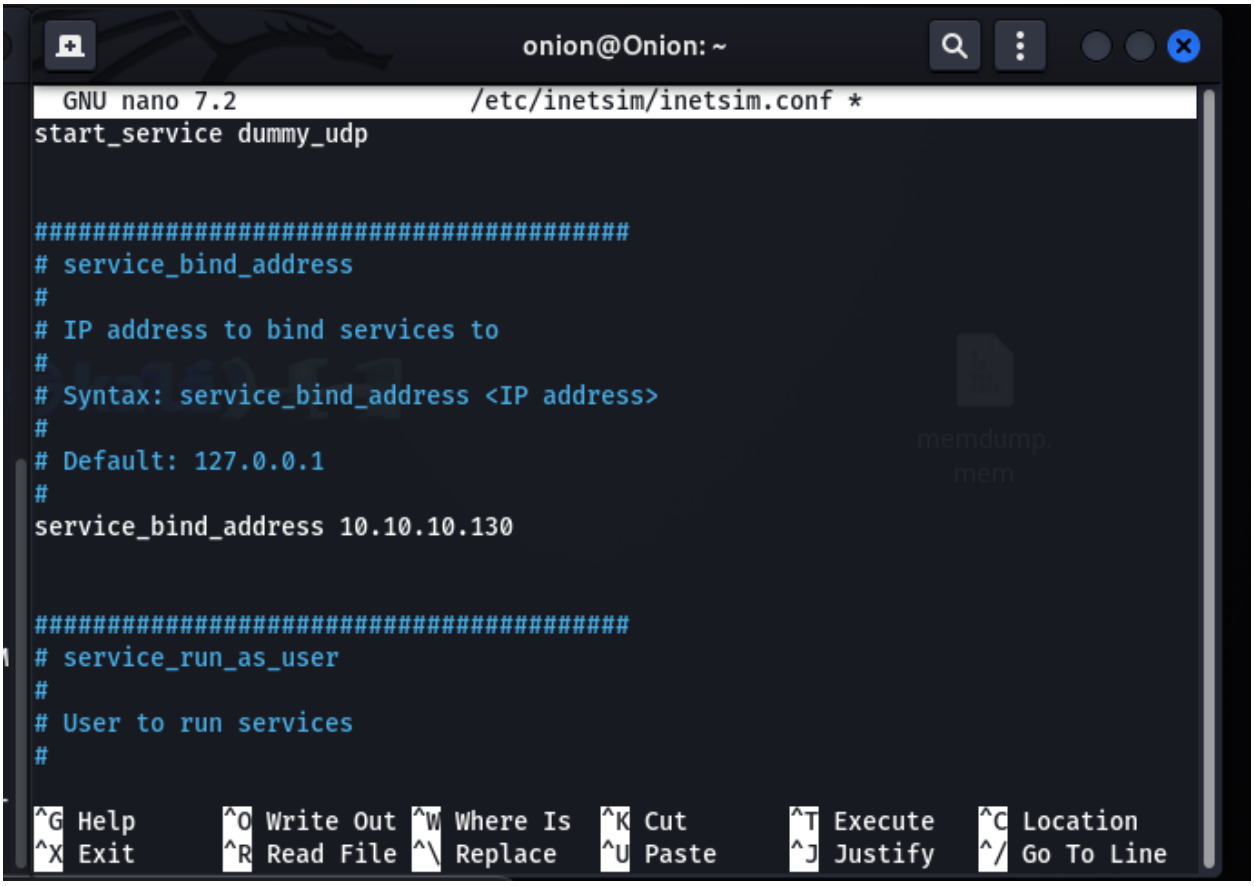

⇨ **I installed inetsim successfully**

Then we use sudo nano /etc/inetsim/inetsim.conf command to change these values:

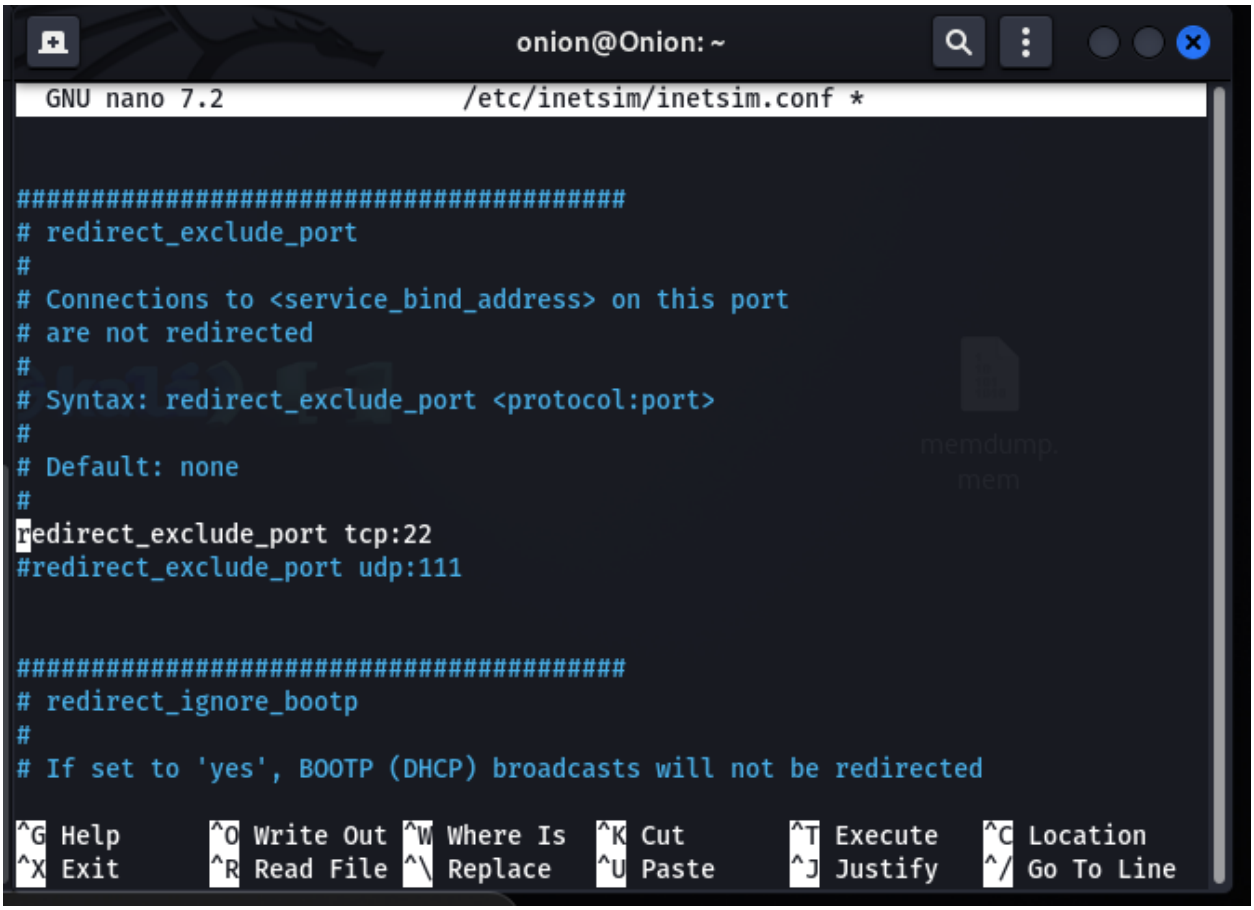
**Redirect_enable**




**Service_bind_address:**

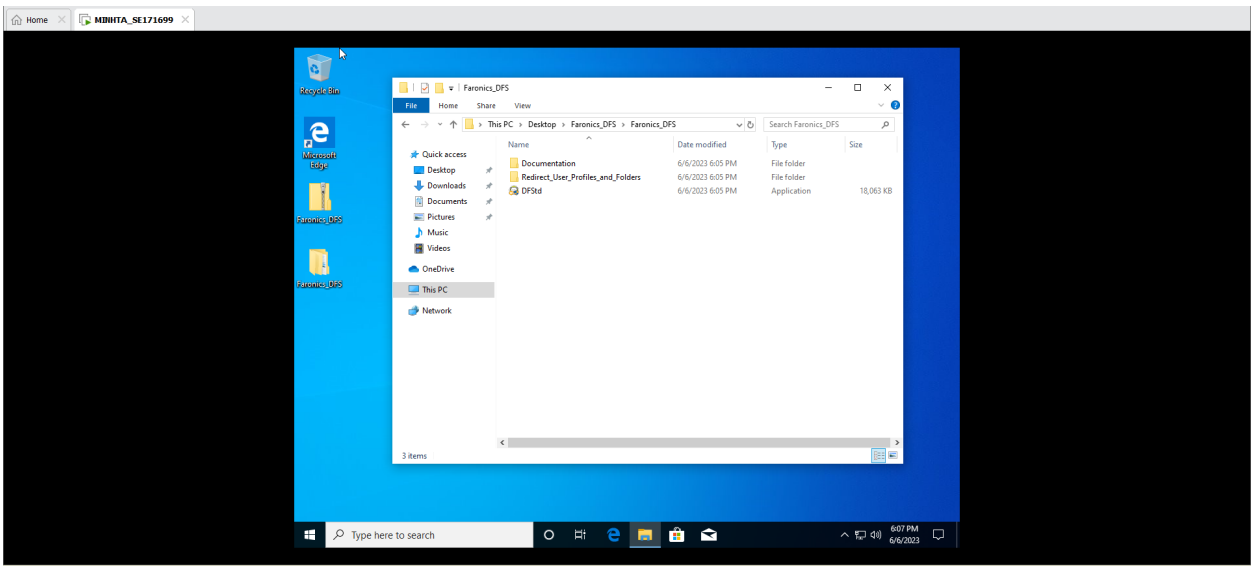



**Redirect port tcp 22:**



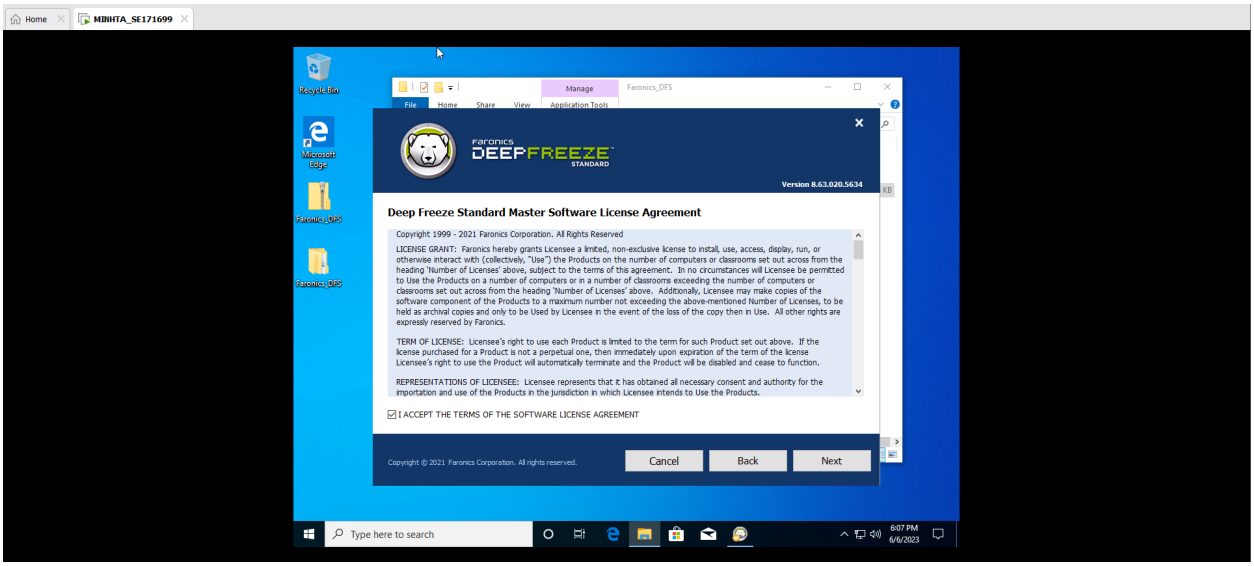

⇨ **Save and exit**

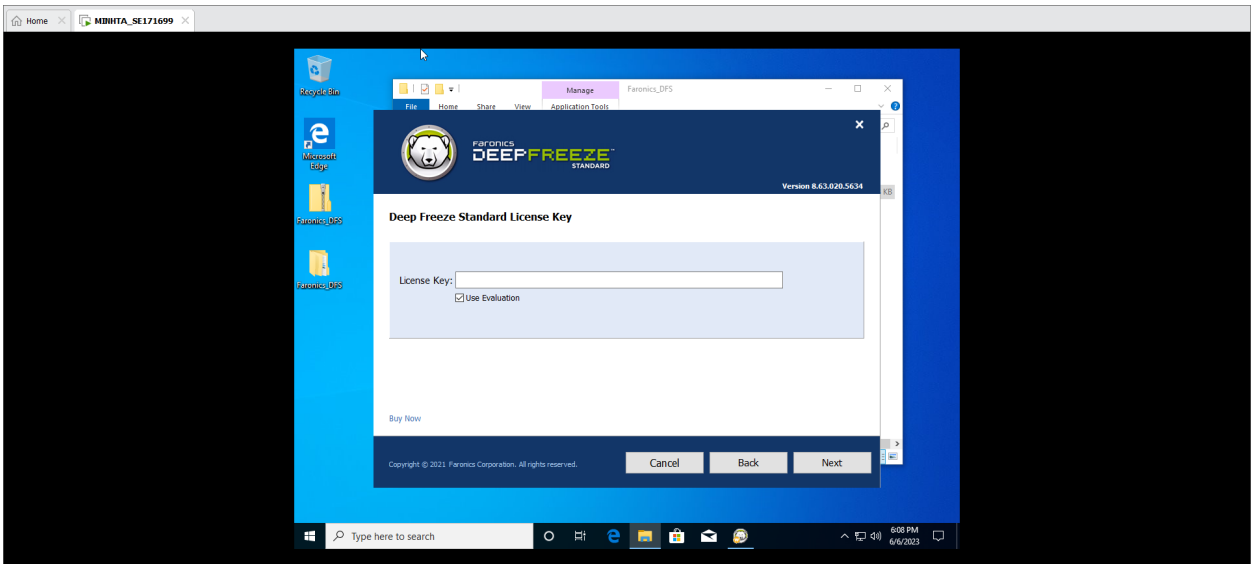
## Next I will install Deep Freeze



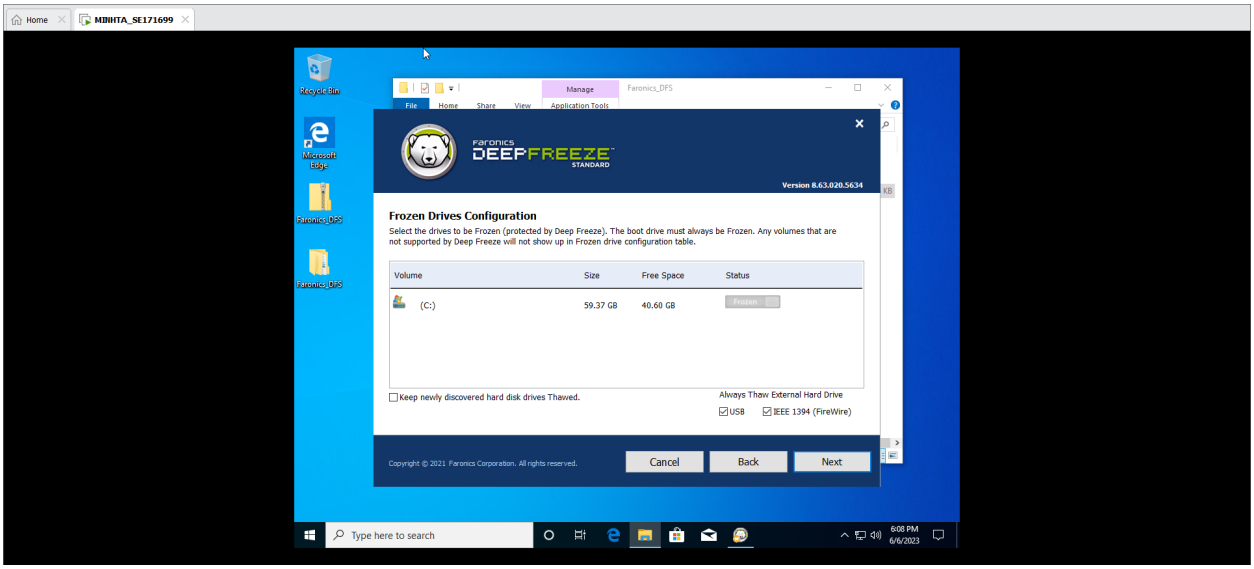

Download setup file from the internet

Press next and accept the term

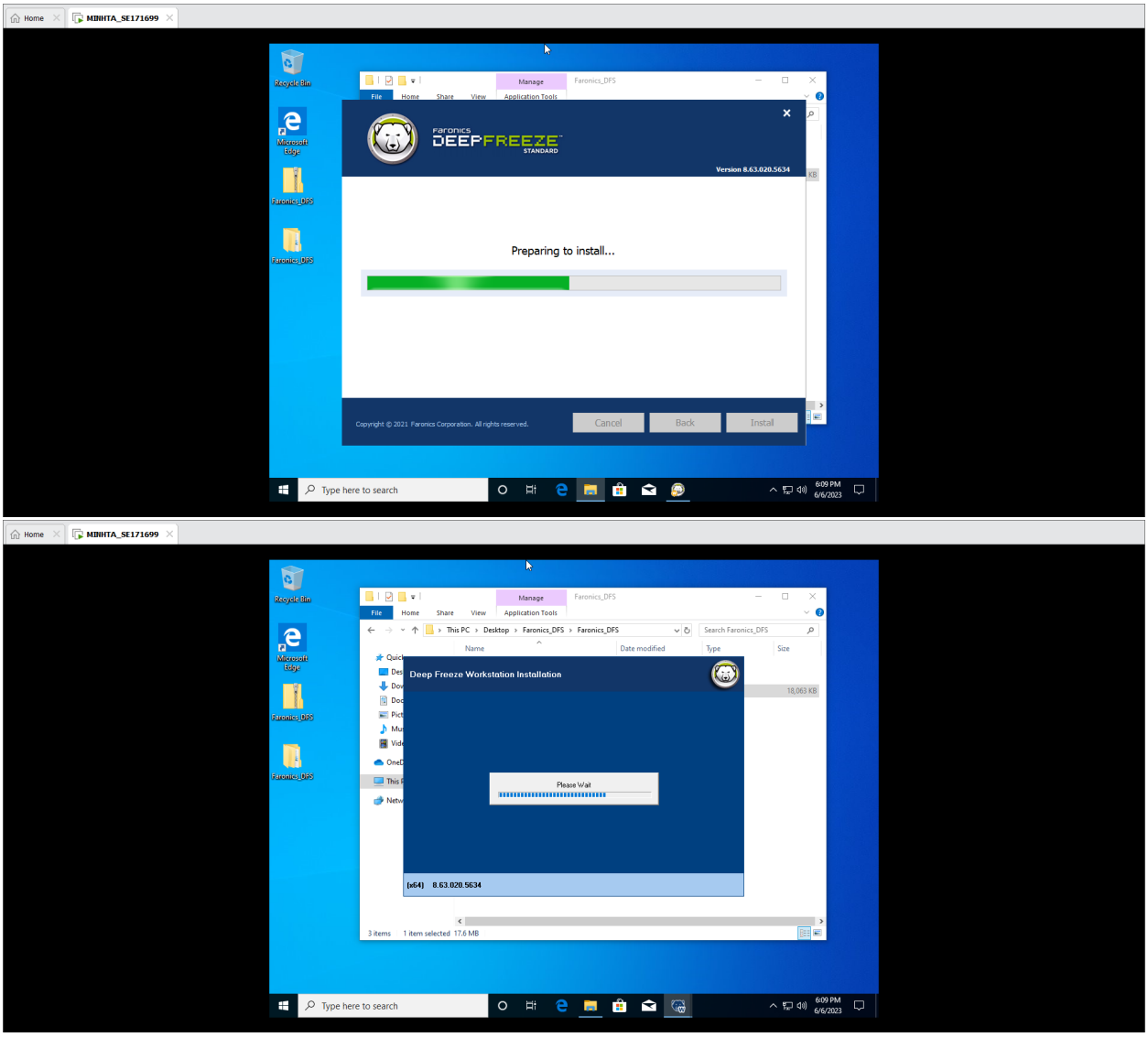


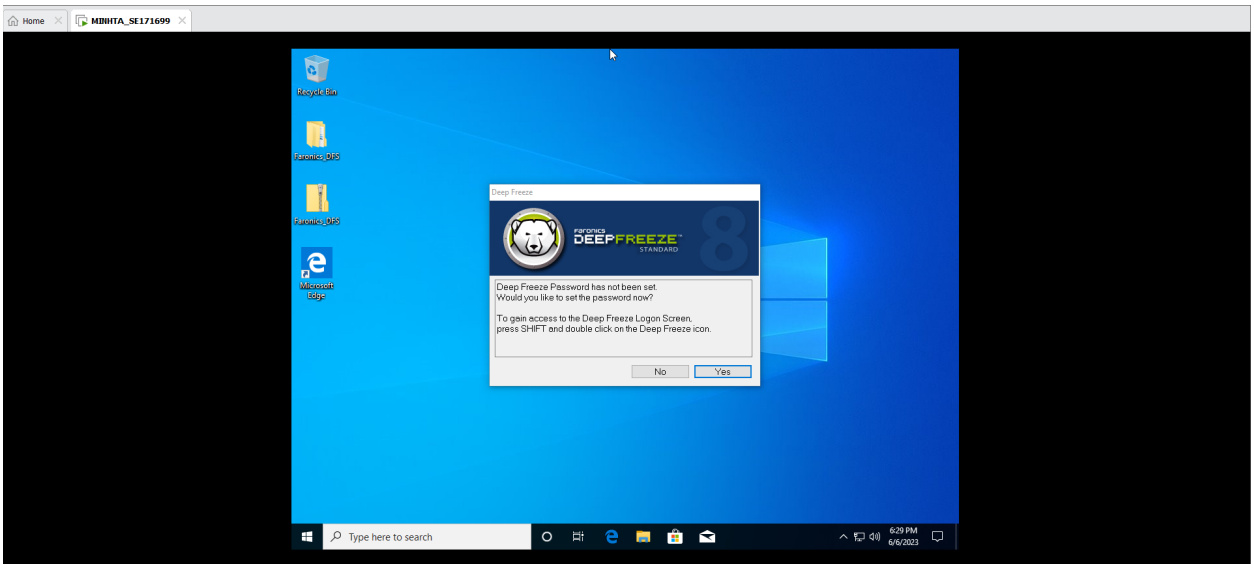

Do not have license key so I will use evaluation



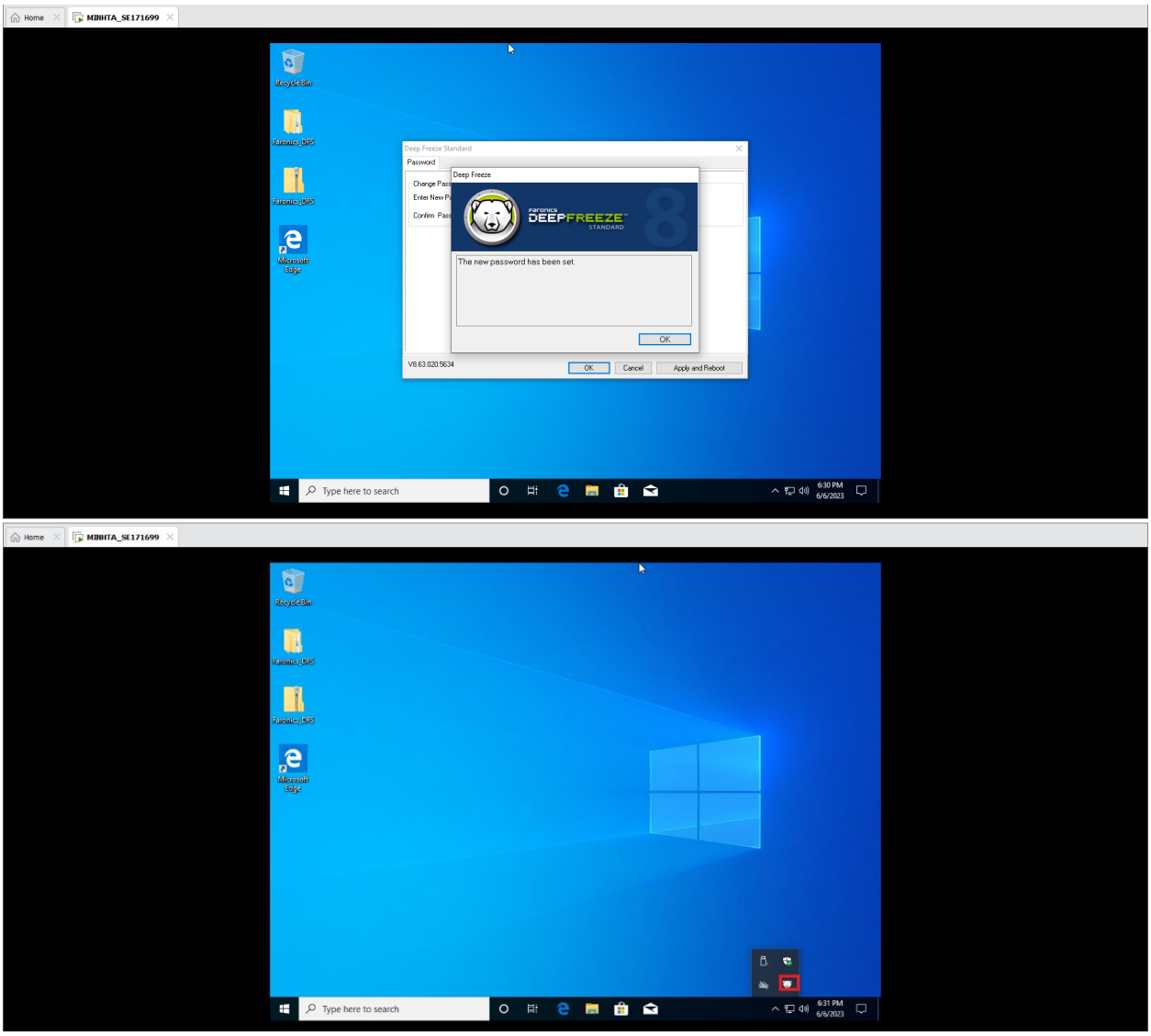

Let everything as default and press next




Deep freeze is installing, after a few seconds it will restart our computer.



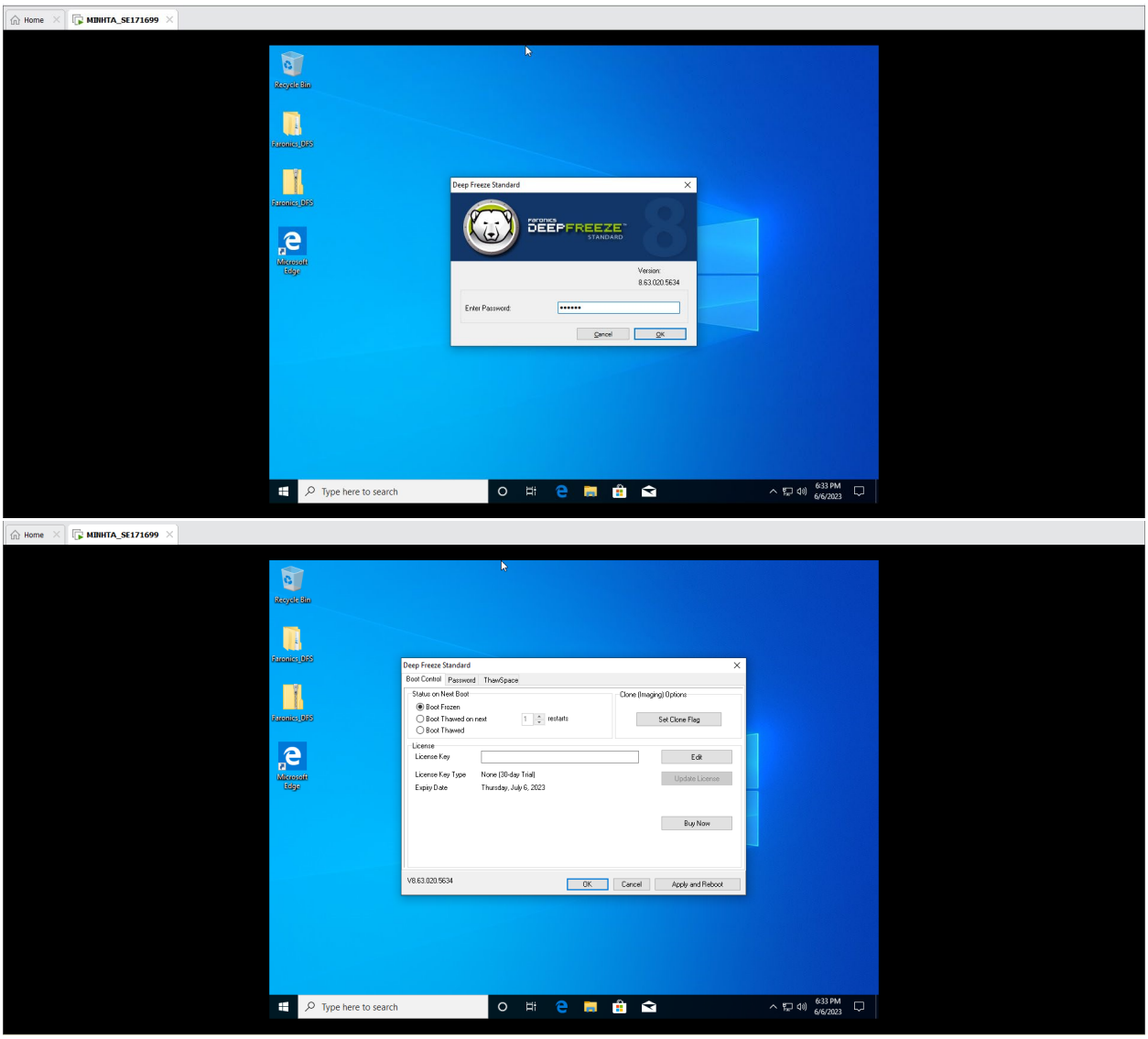

Login again, the Deepfreeze windows will open for us to setup our password. I will set my password to 123456.




Look at the under icon, that is the sign tell us that DeepFreeze is working correctly.

We can press shift and double click this icon to open Deepfreeze.

Otherwise, we can use shortcurt Ctrl+Alt+Shift+F6 to open it.

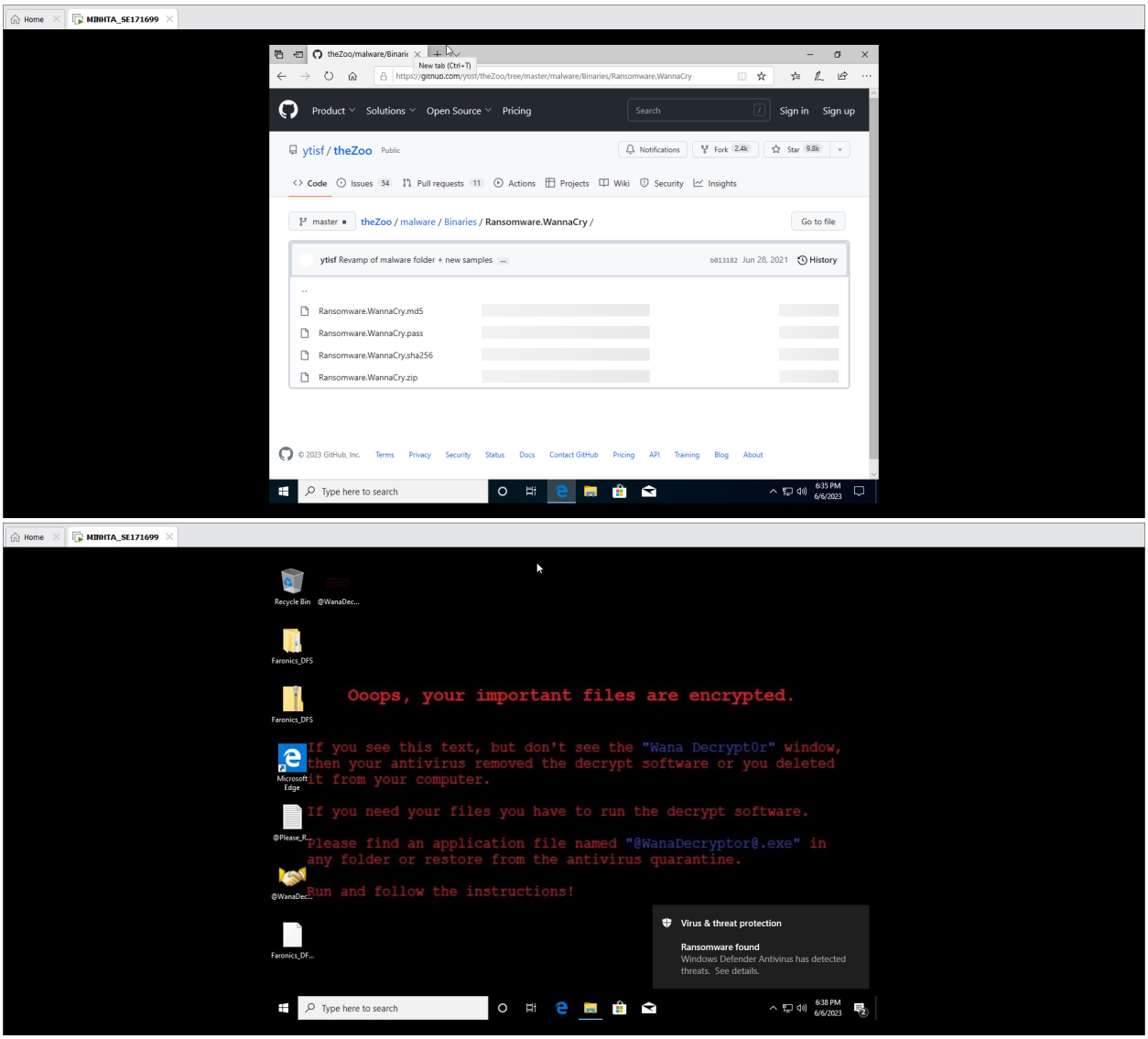






Choose Boot Frozen and then click OK

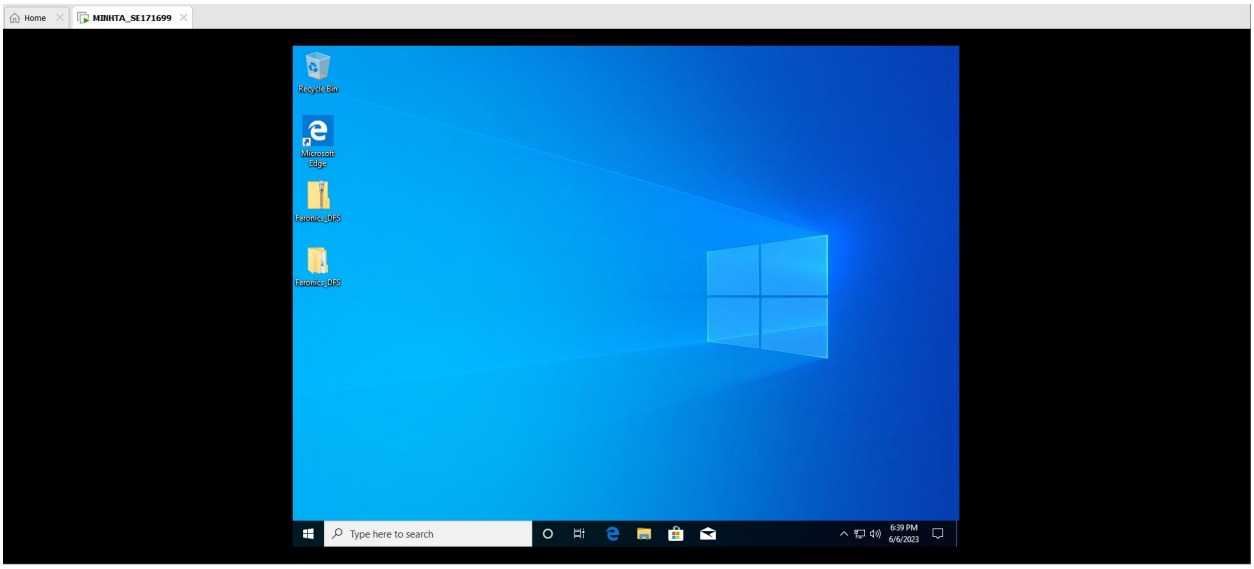
Now we will test the Frozen disk by activate a malware.







We have been infected with this malware. Let’s restart the amchine to test Deepfreeze.




The machine clean again. That is because Deepfreeze have frozen our disk that make no change on writing, delete or change on disk.