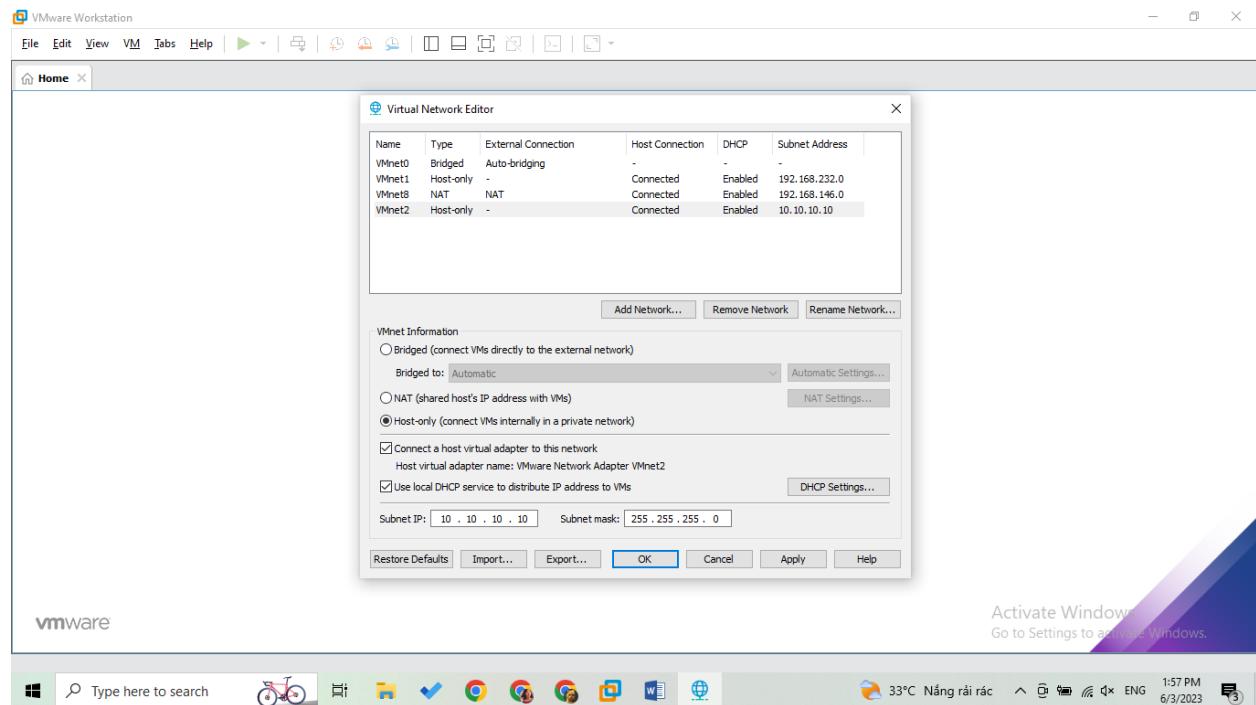


LAB 7-1: Using Deep Freeze to Preserve Physical Systems

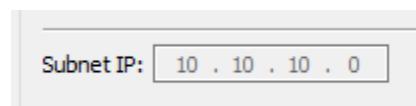
In this lab, we need to launch 3 virtual machines in the system, therefore I'm going to use Ubuntu, Kali Linux and Sansift. Three virtual machines are going to connect through and internal local network VMNet2

But first of all, I create a new VMNet2 :



Go to edit virtual machine

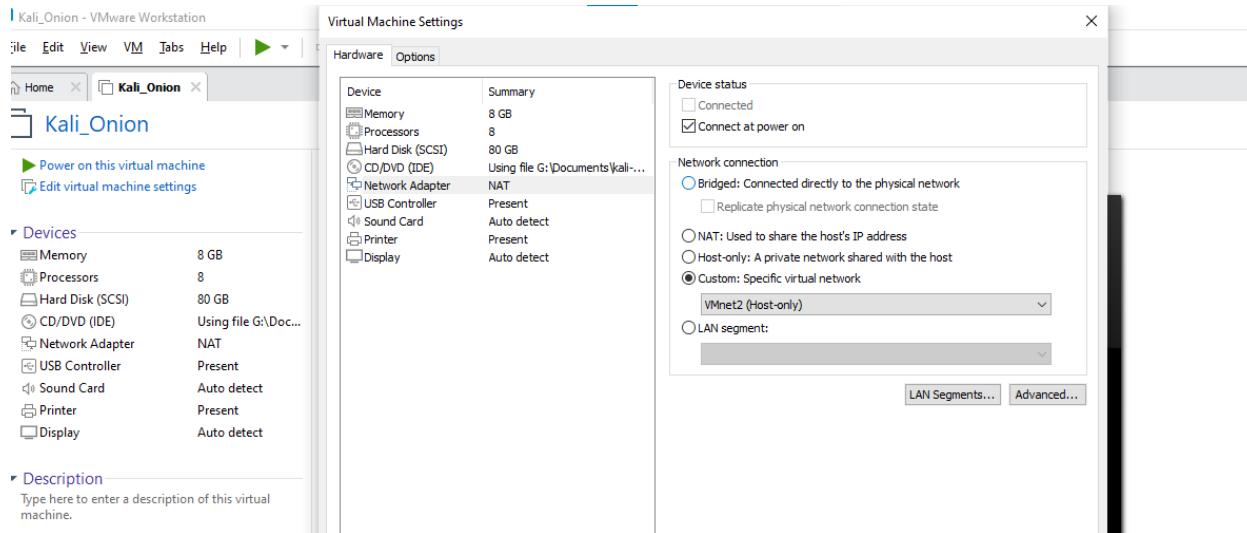
Running as an administrator => change the subnet IP to 10.10.10.0



⇒ Click OK for finishing

Configuration for Kali:

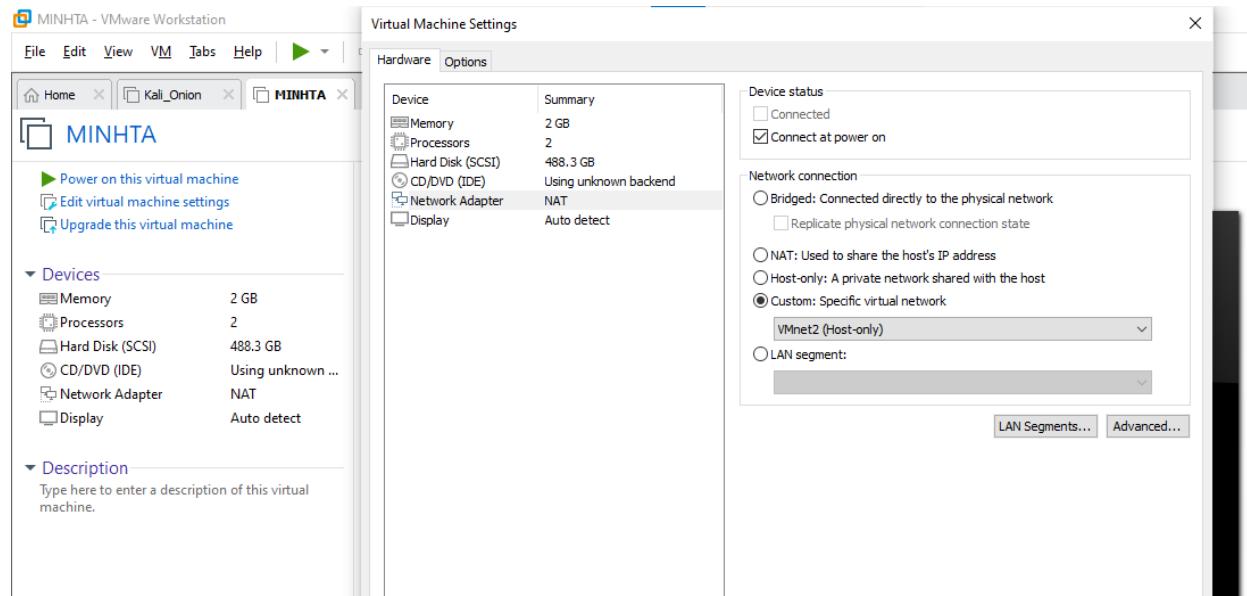
Turn on the kali



Click edit virtual machine setting

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

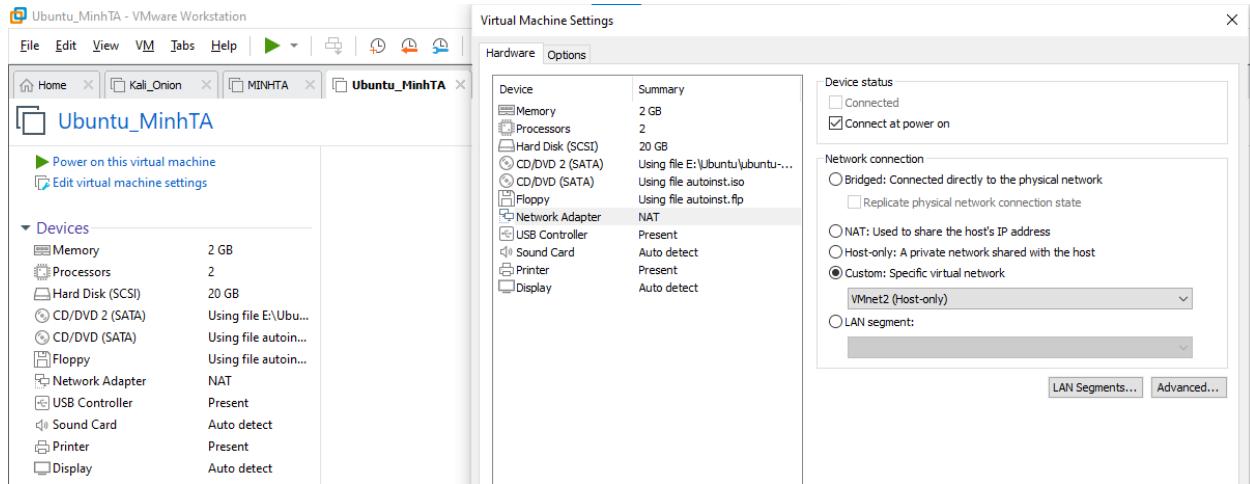
Configuration for San:



⇒ Do the same for sansift virtual machine

⇒ Done

Configuration for Ubuntu:



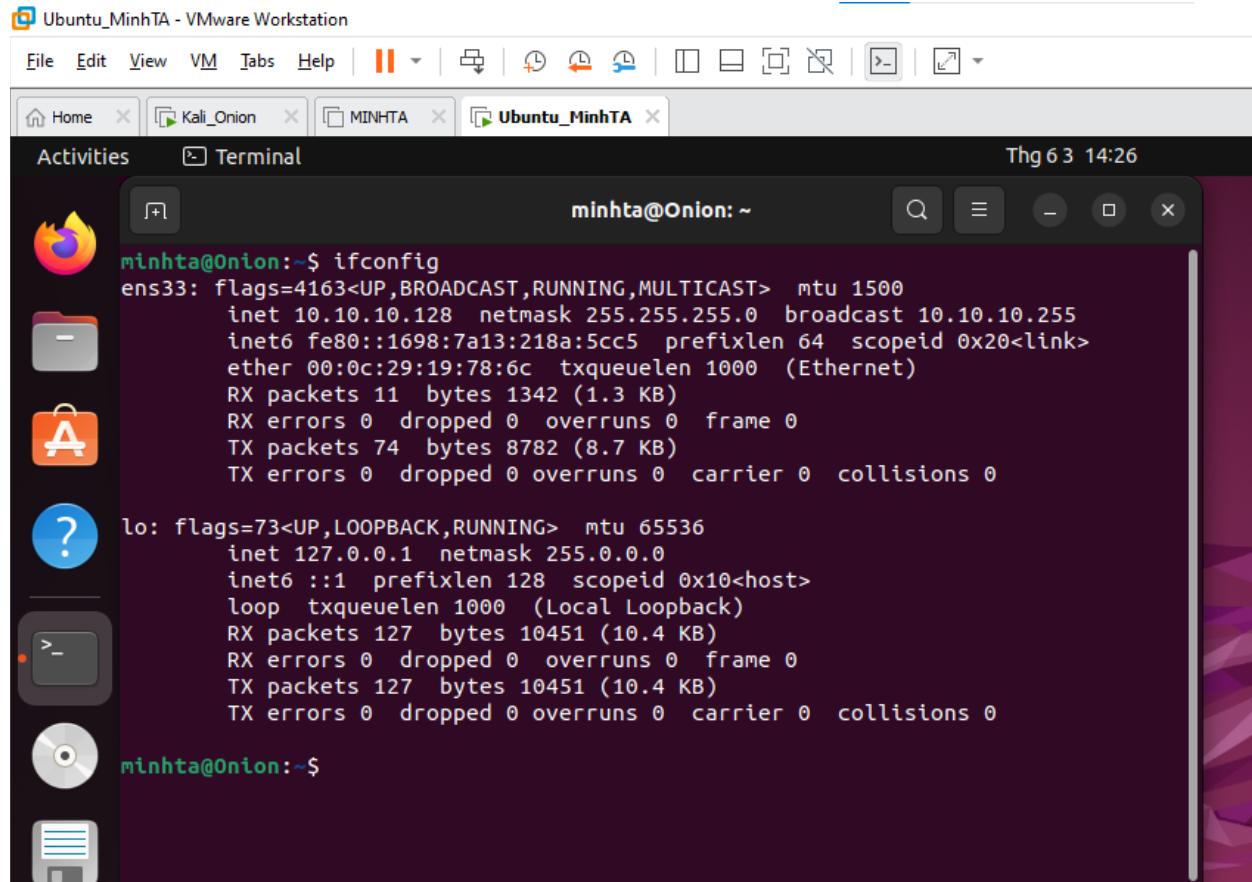
⇒ Do the same for sansift virtual machine

⇒ 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



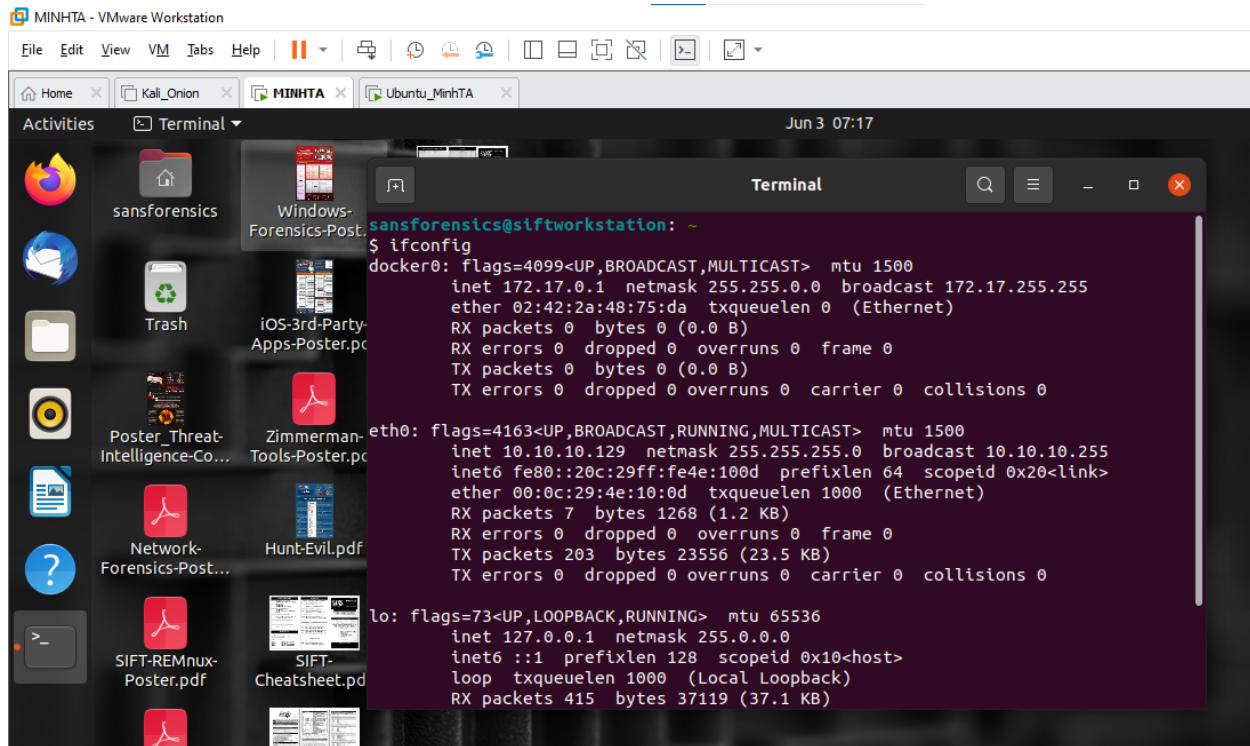
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "minhta@Onion: ~". The terminal displays the output of the "ifconfig" command:

```
minhta@Onion:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.128  netmask 255.255.255.0  broadcast 10.10.10.255
              inet6 fe80::1698:7a13:218a:5cc5  prefixlen 64  scopeid 0x20<link>
                ether 00:0c:29:19:78:6c  txqueuelen 1000  (Ethernet)
                  RX packets 11  bytes 1342 (1.3 KB)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 74  bytes 8782 (8.7 KB)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

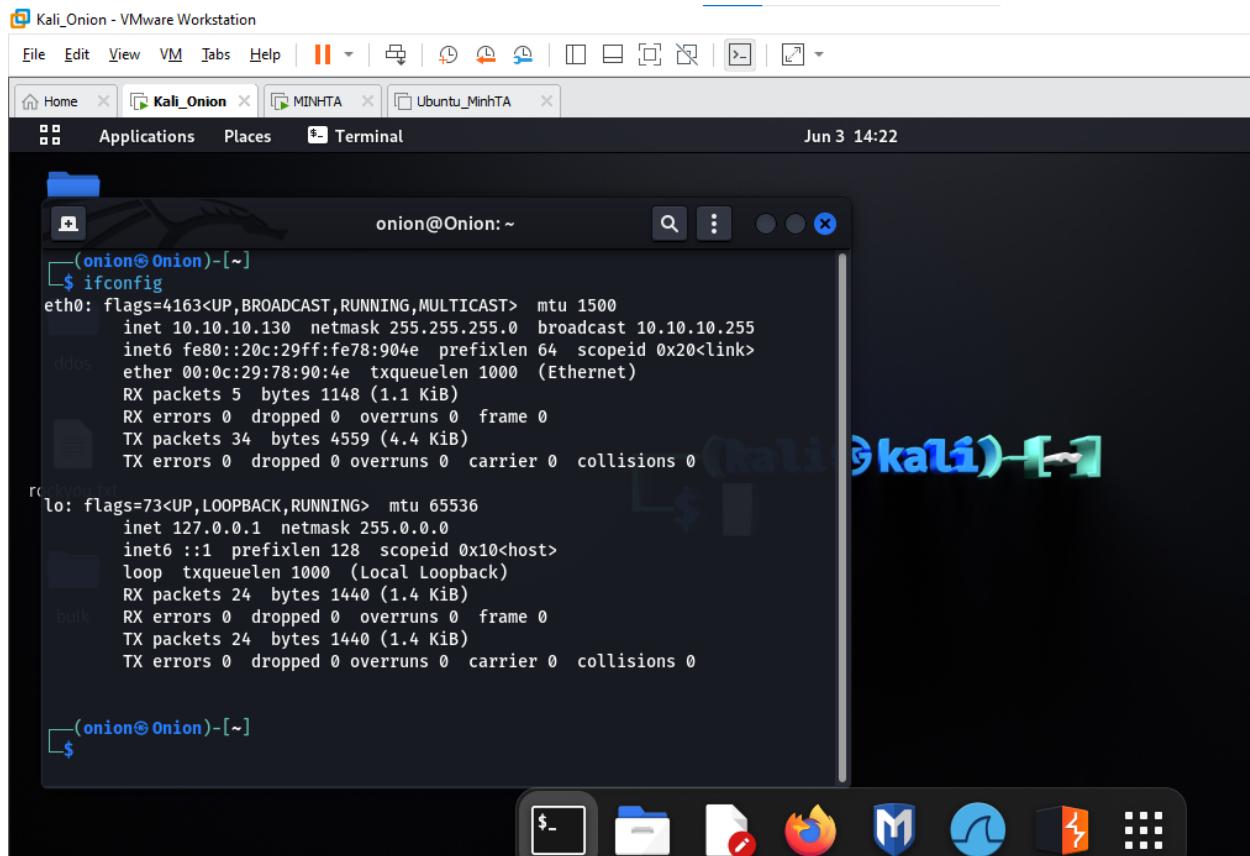
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
              inet6 ::1  prefixlen 128  scopeid 0x10<host>
                loop  txqueuelen 1000  (Local Loopback)
                  RX packets 127  bytes 10451 (10.4 KB)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 127  bytes 10451 (10.4 KB)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

minhta@Onion:~$
```

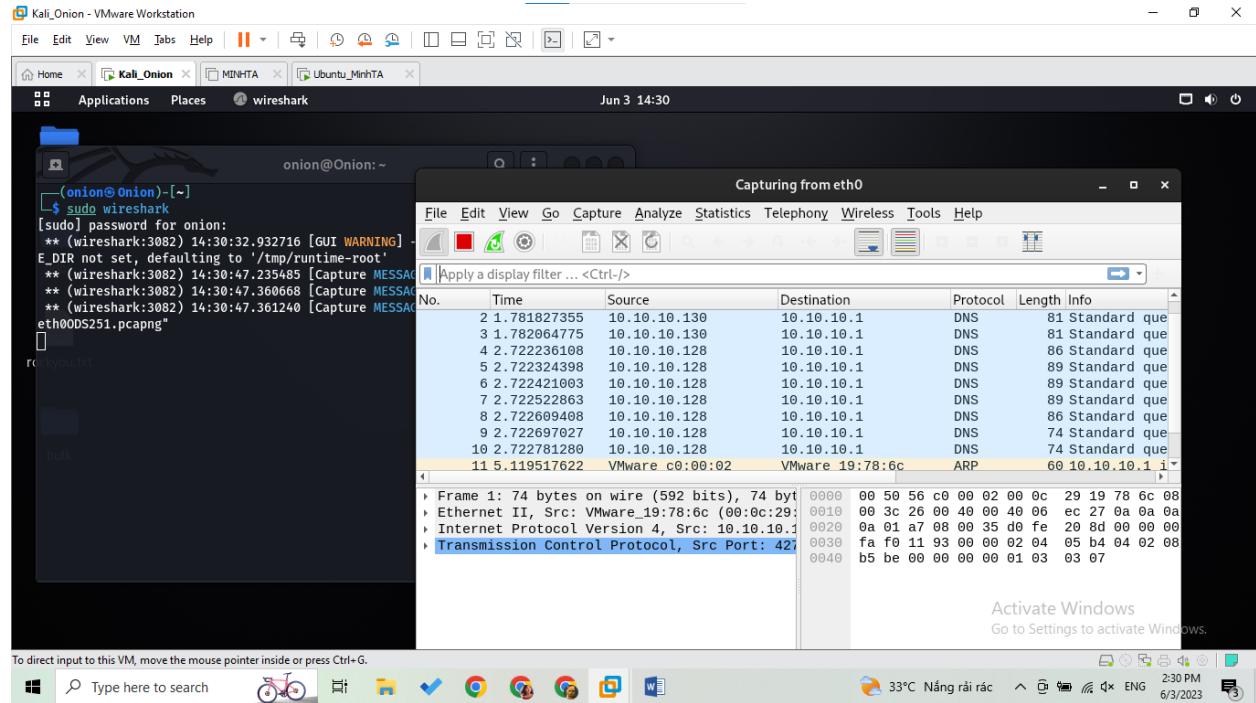
Sansift: 10.10.10.129



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

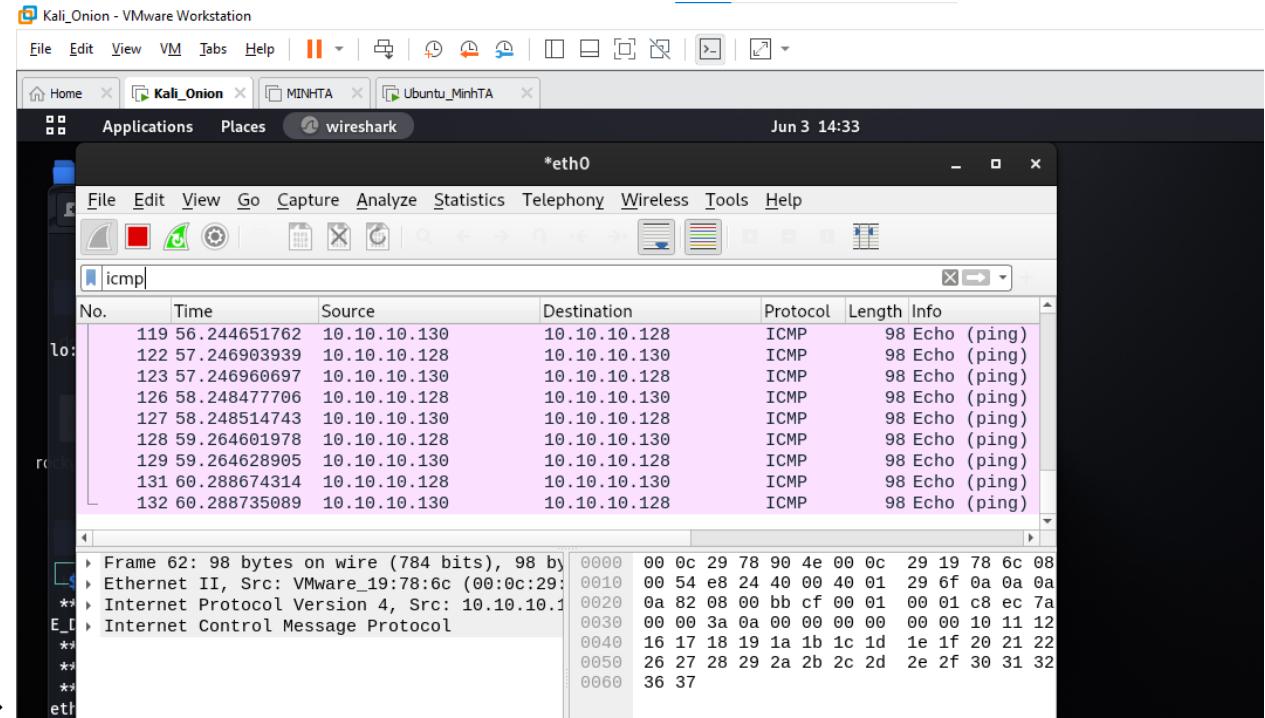
```
inet 10.10.10.128 netmask 255.255.255.0 broadcast 10.10.10.255
inet6 fe80::1698:7a13:218a:5cc5 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:19:78:6c txqueuelen 1000 (Ethernet)
RX packets 11 bytes 1342 (1.3 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 74 bytes 8782 (8.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 127 bytes 10451 (10.4 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 127 bytes 10451 (10.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

minhta@Onion:~$ ping 10.10.10.130
PING 10.10.10.130 (10.10.10.130) 56(84) bytes of data.
64 bytes from 10.10.10.130: icmp_seq=1 ttl=64 time=0.972 ms
64 bytes from 10.10.10.130: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 10.10.10.130: icmp_seq=3 ttl=64 time=0.649 ms
64 bytes from 10.10.10.130: icmp_seq=4 ttl=64 time=1.06 ms
```

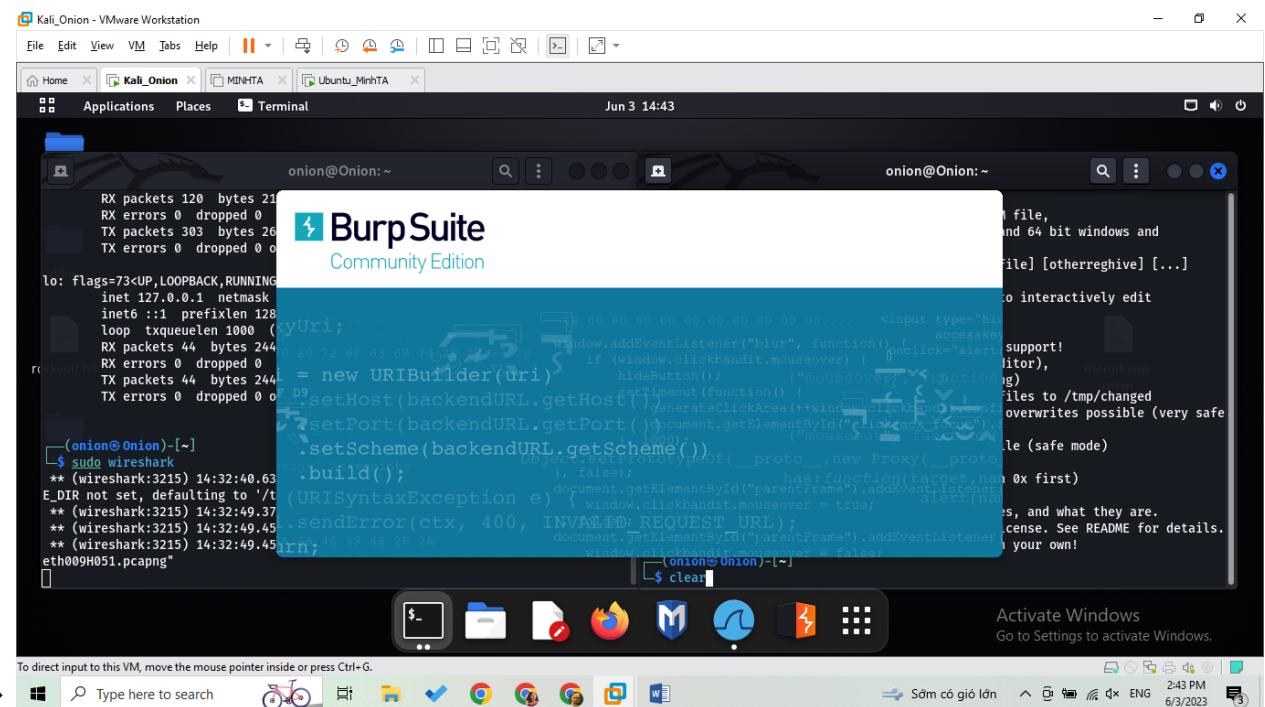
Switch to the kali to check

There are a bunch of package are just delivered



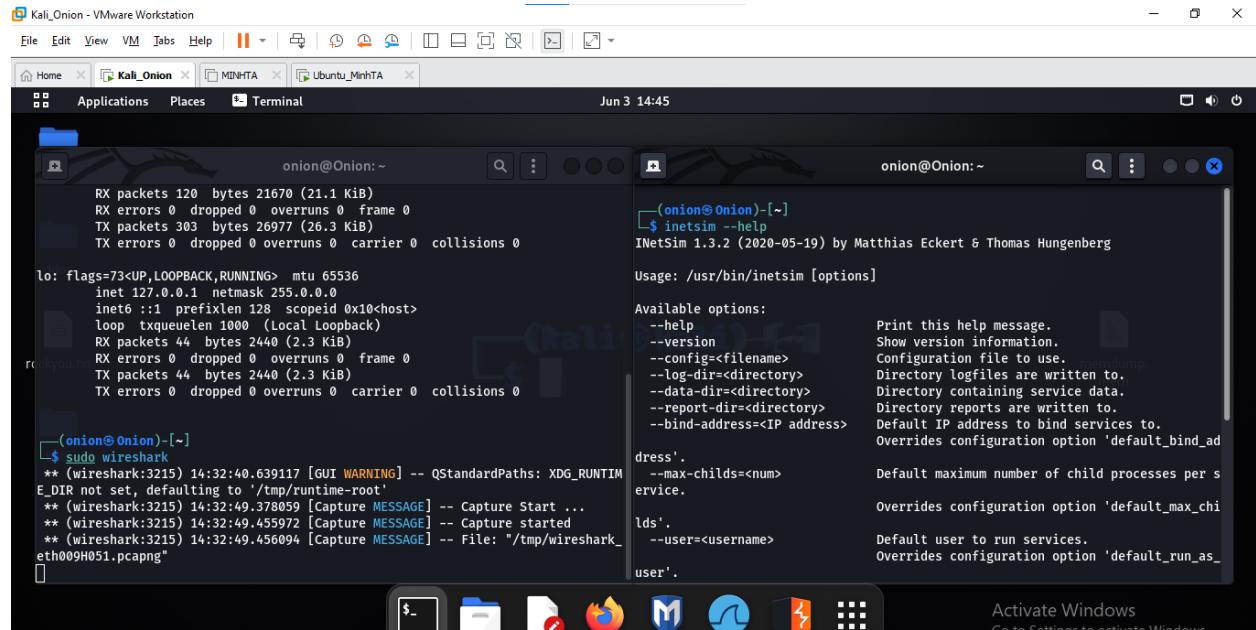
⇒ Catch successfully

Start to install burpsuite



⇒ I installed burpsuite successfully

Start to install inetsim:



The screenshot shows a Kali Linux VM interface with two terminal windows. The left window displays network statistics and a Wireshark capture session. The right window shows the inetsim help documentation.

```
onion@Onion:~$ ifconfig
RX packets 120 bytes 21670 (21.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 303 bytes 26977 (26.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 44 bytes 2440 (2.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 44 bytes 2440 (2.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(onion@Onion)-[~]
└─$ sudo wireshark
** (wireshark:3215) 14:32:40.639117 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'.
** (wireshark:3215) 14:32:49.378059 [Capture MESSAGE] -- Capture Start ...
** (wireshark:3215) 14:32:49.455972 [Capture MESSAGE] -- Capture started
** (wireshark:3215) 14:32:49.456094 [Capture MESSAGE] -- File: '/tmp/wireshark_eth009H051.pcapng'

(onion@Onion)-[~]
└─$ inetsim --help
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg

Usage: /usr/bin/inetsim [options]

Available options:
--help Print this help message.
--version Show version information.
--config=<filename> Configuration file to use.
--log-dir=<directory> Directory logfiles are written to.
--data-dir=<directory> Directory containing service data.
--report-dir=<directory> Directory reports are written to.
--bind-address=<IP address> Overrides configuration option 'default_bind_address'.
--max-childs=<num> Default maximum number of child processes per service.
--user=<username> Overrides configuration option 'default_run_as_user'.
```

⇒ I installed inetsim successfully

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

Redirect_enable

The screenshot shows a terminal window titled "onion@Onion:~". The file being edited is "/etc/inetsim/inetsim.conf". The content of the file is as follows:

```
GNU nano 7.2          /etc/inetsim/inetsim.conf *

#
#dummy_banner_wait 3

#####
# Redirect
#####

#####
#redirect_enabled
#
# Turn connection redirection on or off.
#
# Syntax: redirect_enabled [yes|no]
#
# Default: no
#
#redirect_enabled yes

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line
```

Service_bind_address:

```
onion@Onion:~
```

```
GNU nano 7.2          /etc/inetsim/inetsim.conf *
```

```
start_service dummy_udp

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 10.10.10.130

#####
# service_run_as_user
#
# User to run services
#
^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Redirect port tcp 22:

```
onion@Onion: ~
GNU nano 7.2      /etc/inetsim/inetsim.conf *

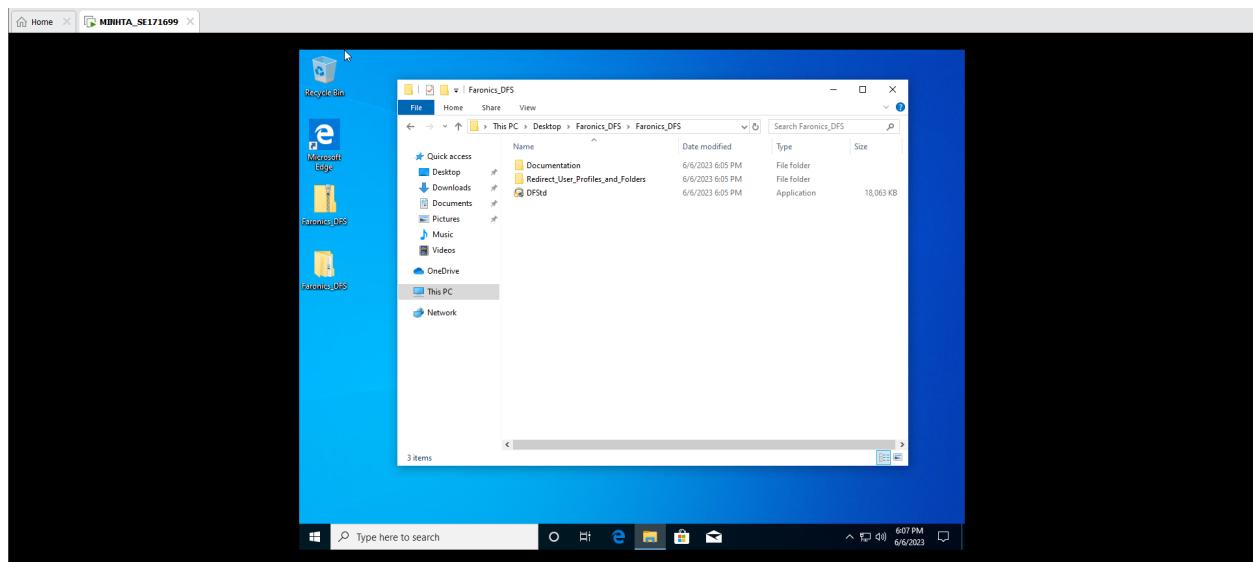
#####
# redirect_exclude_port
#
# Connections to <service_bind_address> on this port
# are not redirected
#
# Syntax: redirect_exclude_port <protocol:port>
#
# Default: none
#
#redirect_exclude_port tcp:22
#redirect_exclude_port udp:111

#####
# redirect_ignore_bootp
#
# If set to 'yes', BOOTP (DHCP) broadcasts will not be redirected

^G Help      ^O Write Out  ^W Where Is   ^K Cut      ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste    ^J Justify    ^/ Go To Line
```

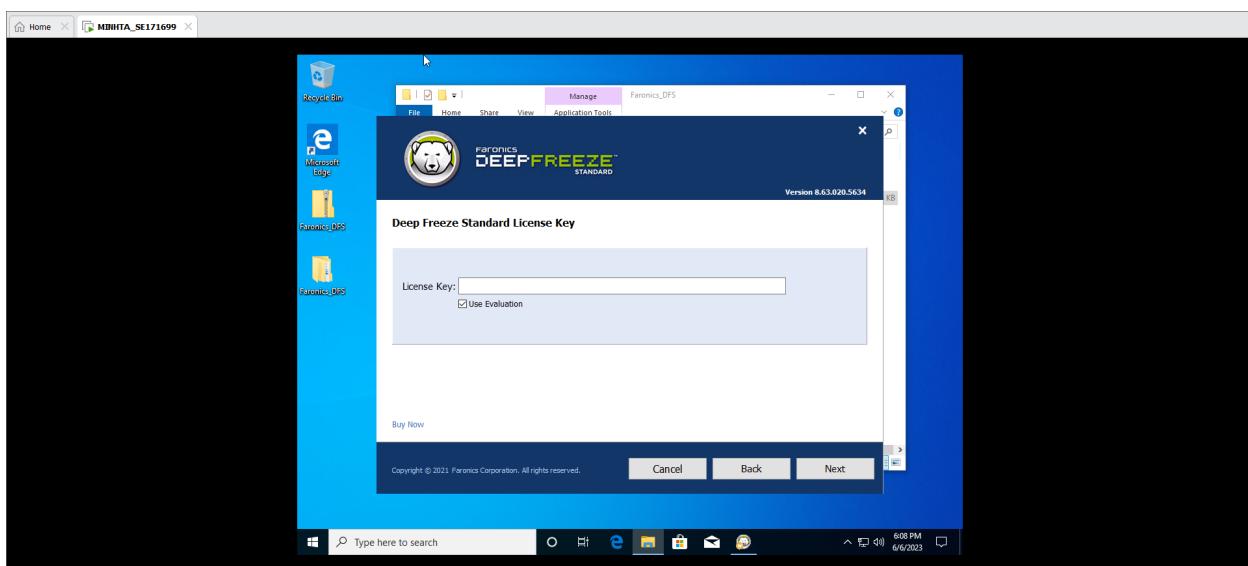
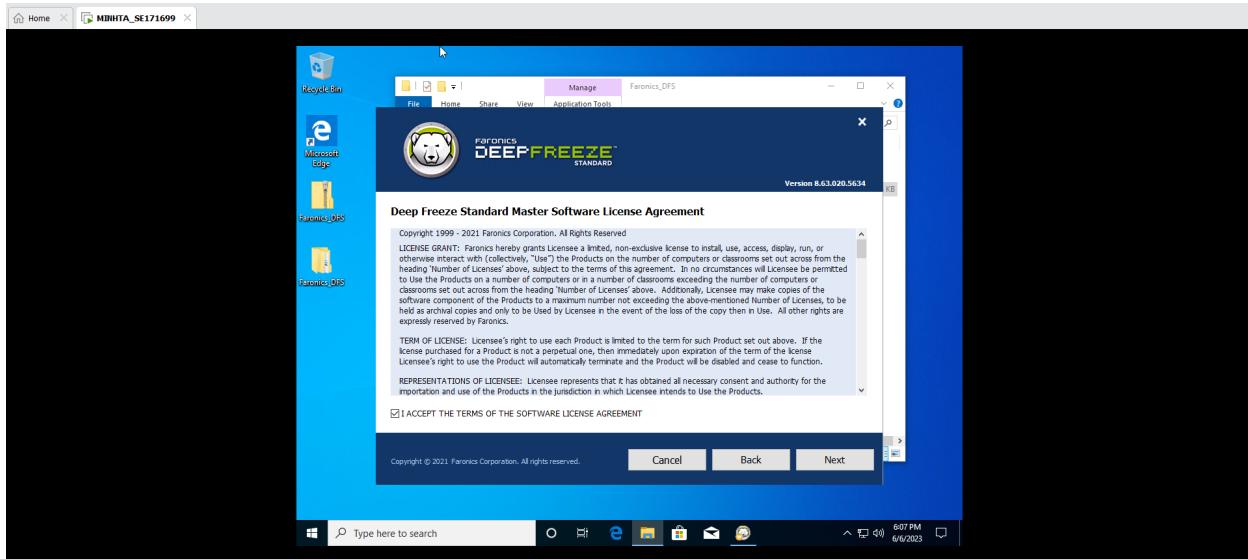
⇒ Save and exit

Next I will install Deep Freeze

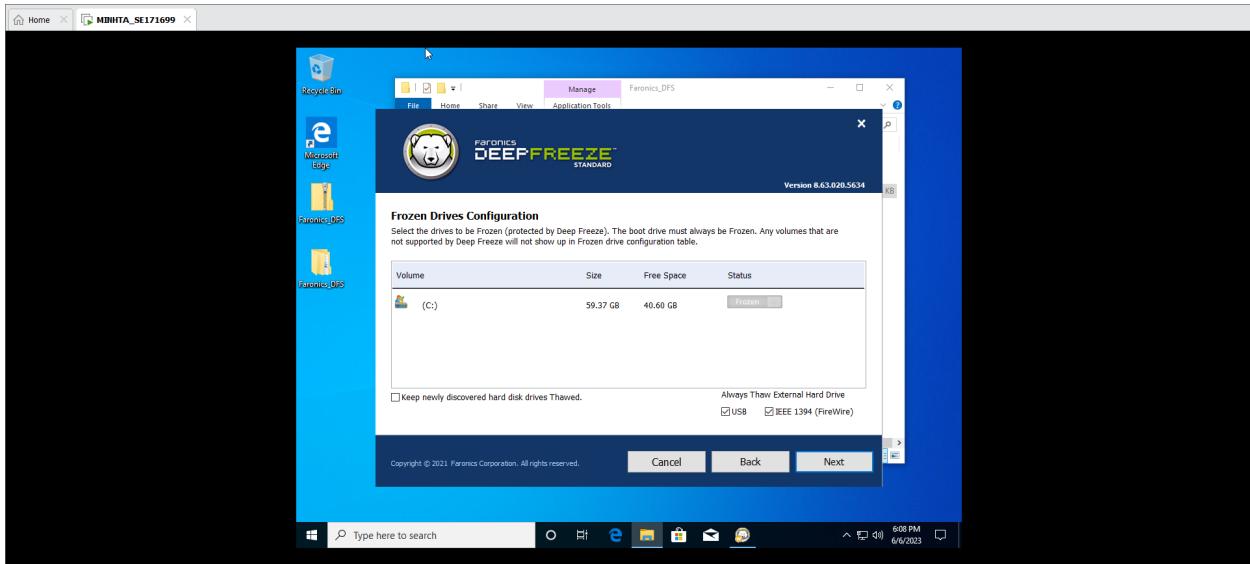


Download setup file from the internet

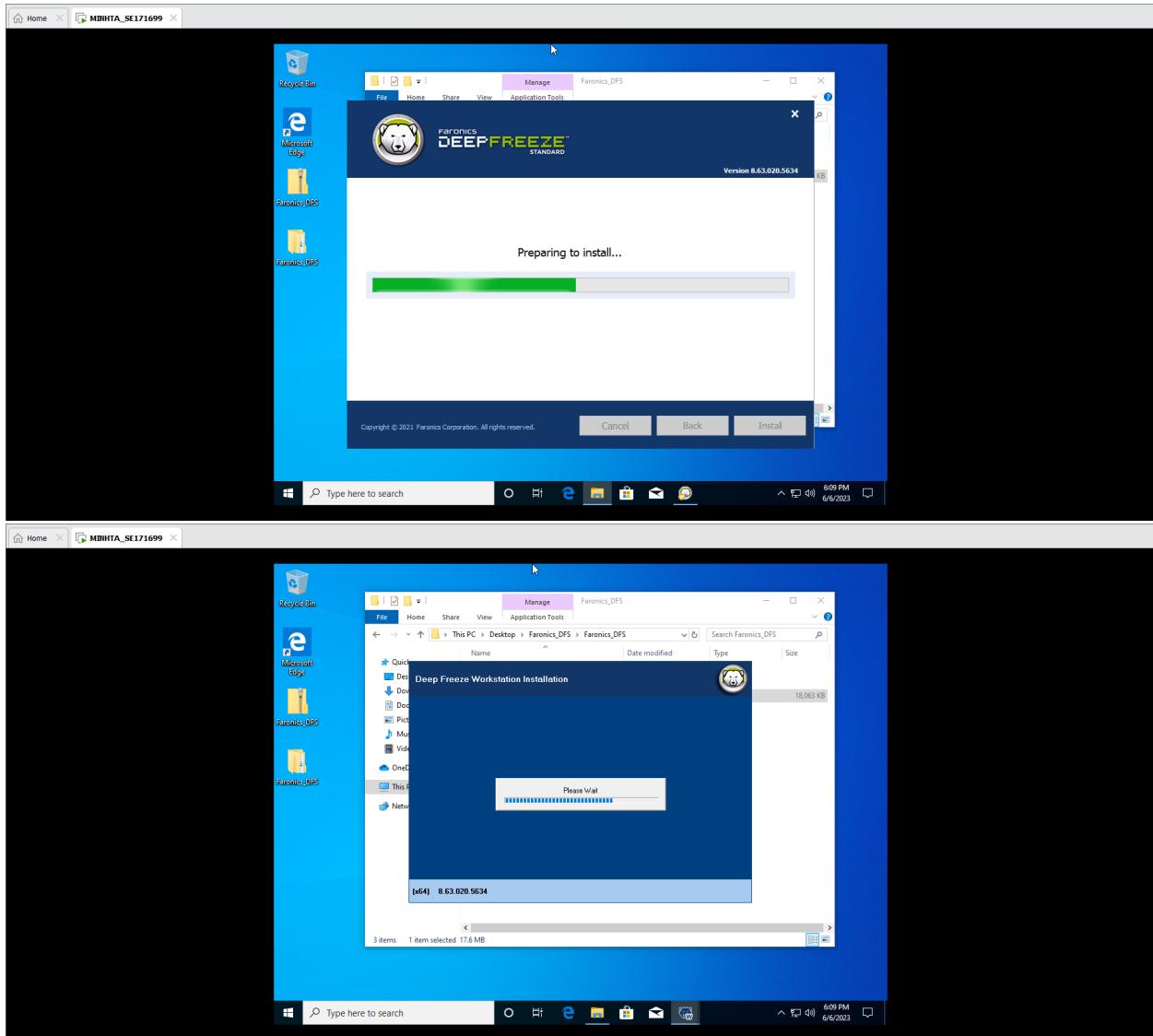
Press next and accept the term



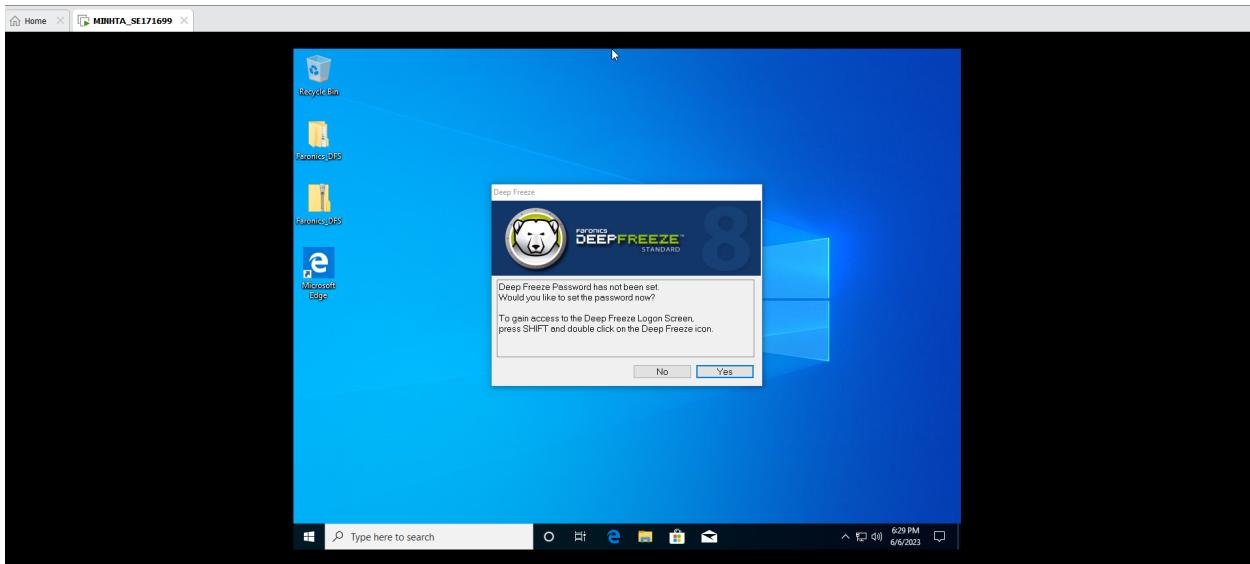
Do not have license key so I will use evaluation



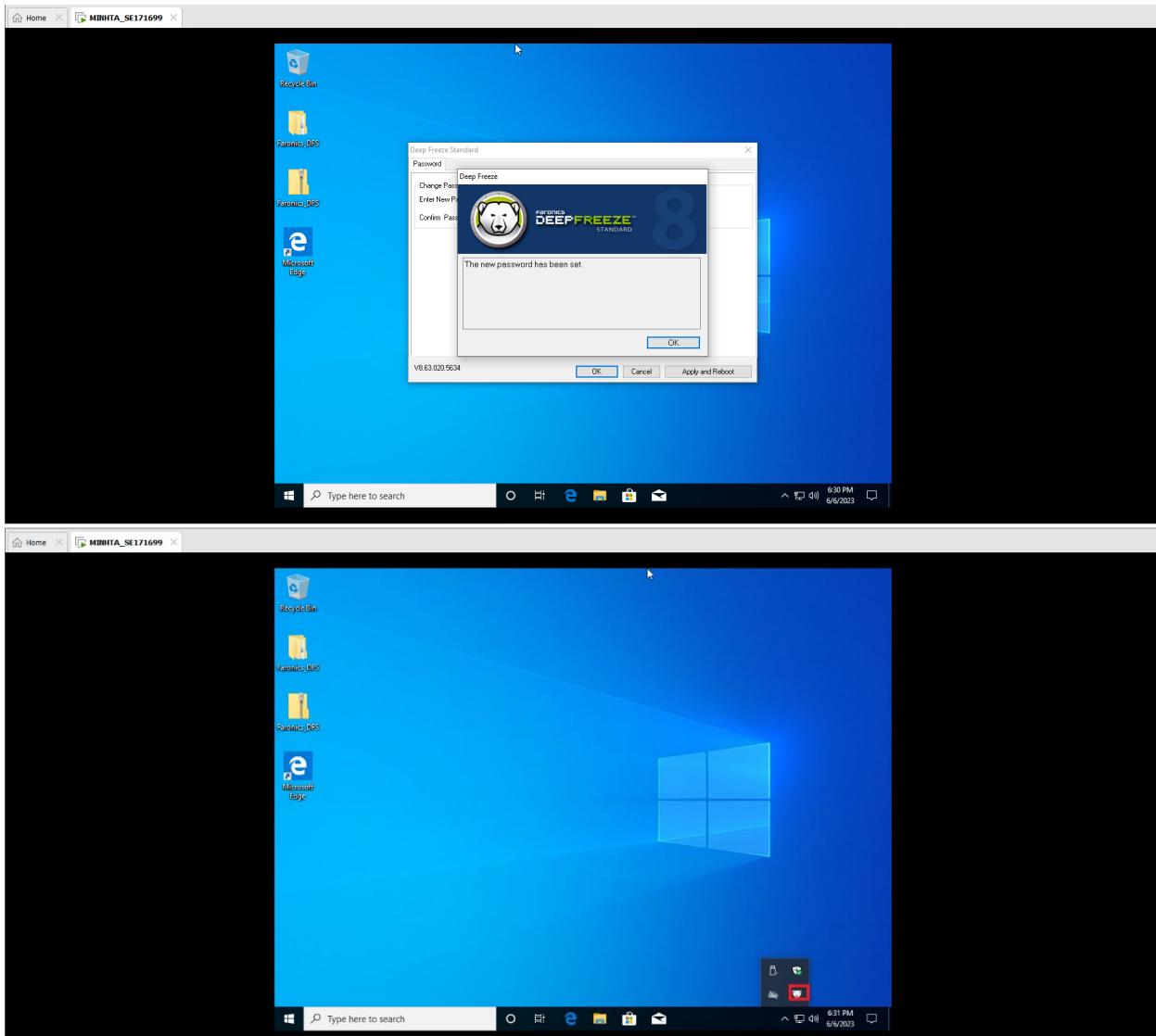
Let everything as default and press next



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



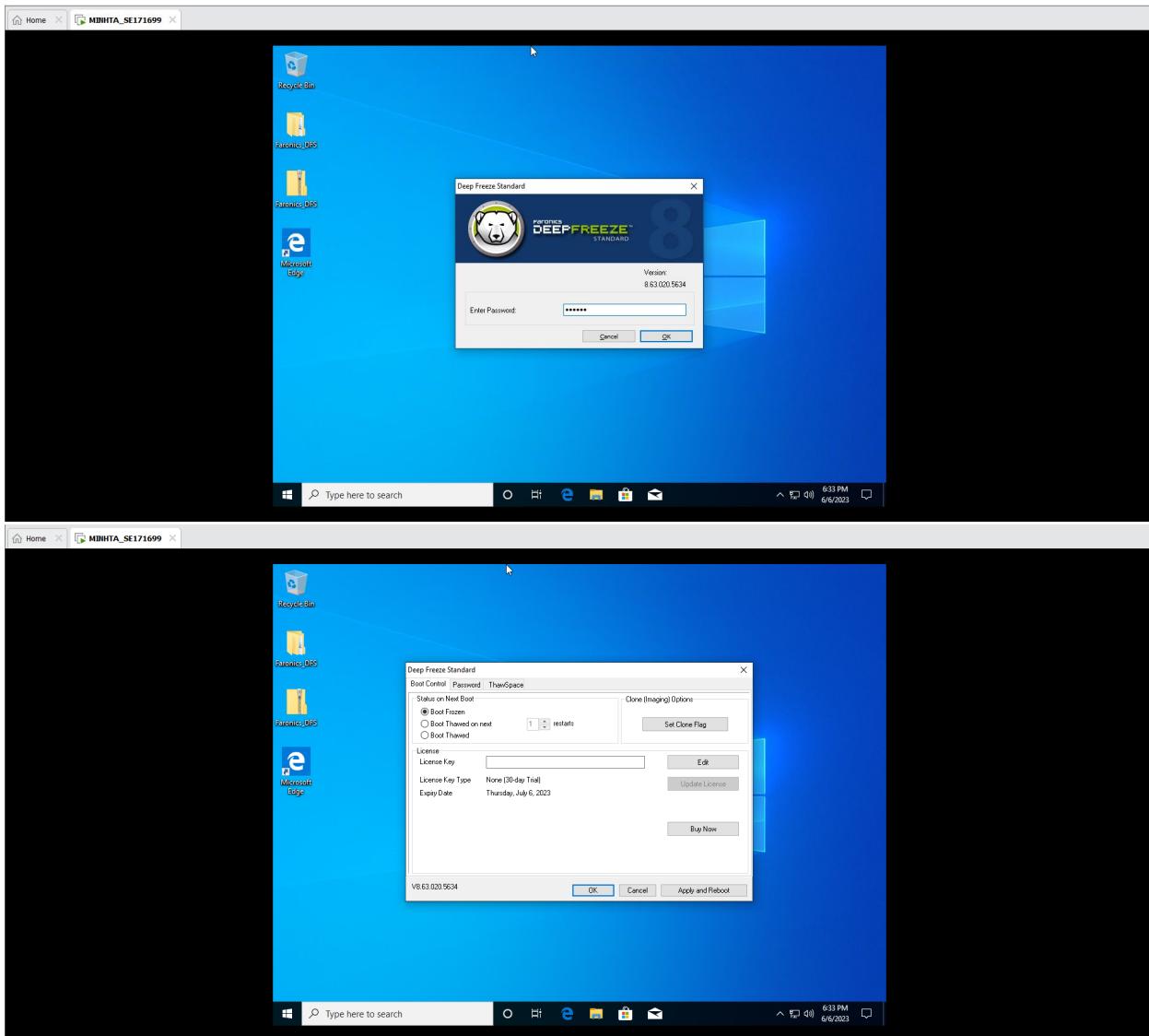
Login again, the Deepfreeze windows will open for us to setup our password. I will set my password to 123456.



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

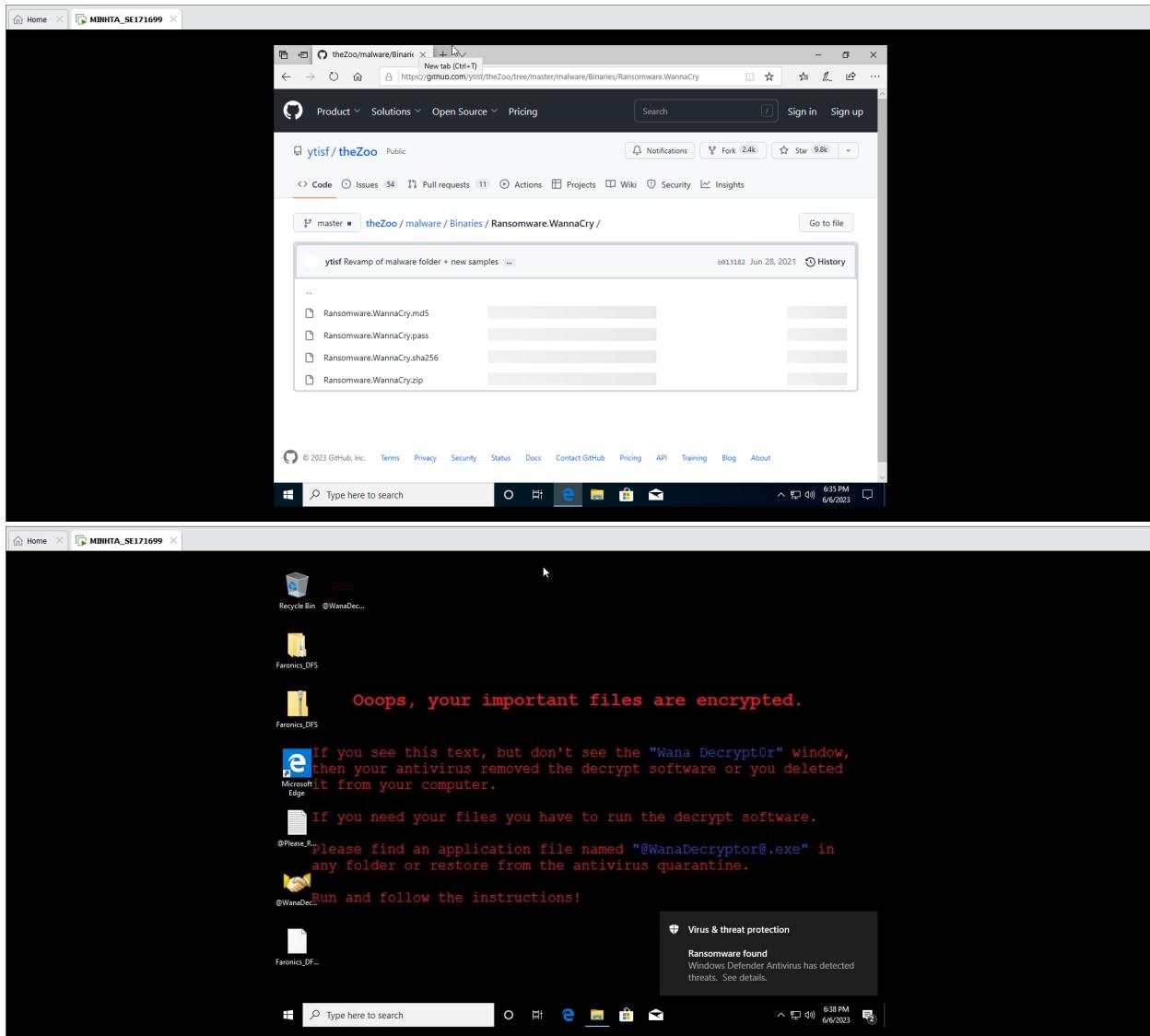
We can press shift and double click this icon to open Deepfreeze.

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

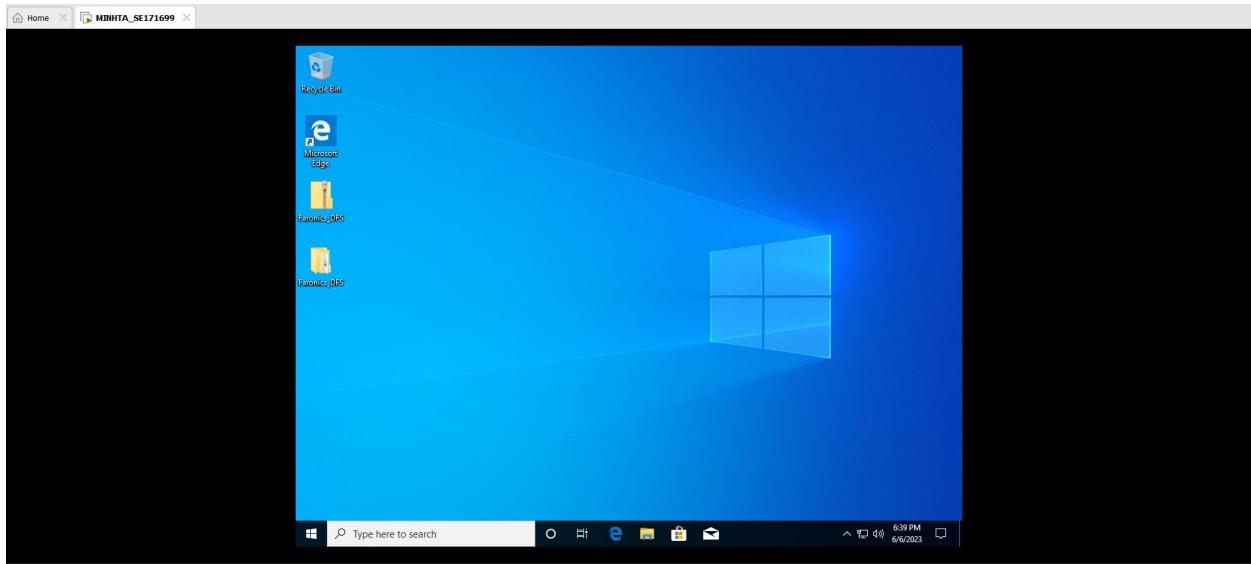


Choose Boot Frozen and then click OK

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.