CS 5700 -- Computer Security and Information Assurance
Fall 2018

Prof. Leszek Lilien / TA: Abduljaleel Al-Hasnawi
Department of Computer Science
Western Michigan University

LAB ASSIGNMENT - 2

NAME: SAMPATH TALLURI

TABLE OF CONTENTS

1. Introductory Part: Enable Inbound Rules for IPv4 and IPv6 3

1.1. Step 1: Enable Inbound Rules for IPv4 and IPv6 on Win8.1. 3

1.2. Step 2: Enable Inbound Rules for IPv4 and IPv6 on W2K12. 4

2. Lab 1.1w: Windows Client Configuration 5

2.1. Step 1: Start Win8.1 5

2.2. Step 2: View and Record the Network Configuration 6

2.3. Step 3: Change the IP Address of Win8.1 8

2.4. Step 4: Change the IP Address of W2K12 Server. 10

2.5. Step 5: From Win8.1 Ping the W2K12 Server 12

2.6. Step 6: View and Modify the ARP Table 13

3. Lab 1.2w: Name Resolution in Windows 14

3.1. Step 1: Login to Win8.1 as administrator 14

3.2. Step 2: Ping Win8.1 15

3.3. Step 3: View and Modify the Host File..... 15

4. Lab 1.3w: Windows IPv6 Basics 18

4.1. Step1: Verify IPv6 Setting for Win8.1 and W2K12 18

4.2. Step2: Install Wireshark on Win8.1 19

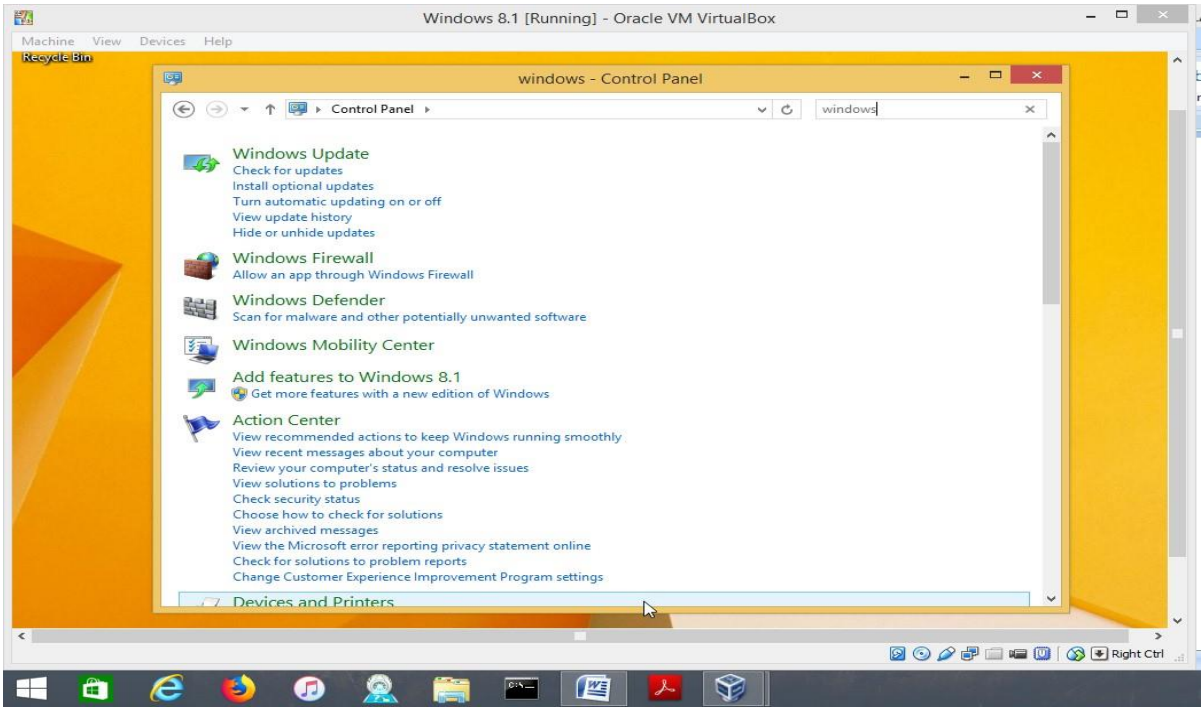
5.Issues.....21

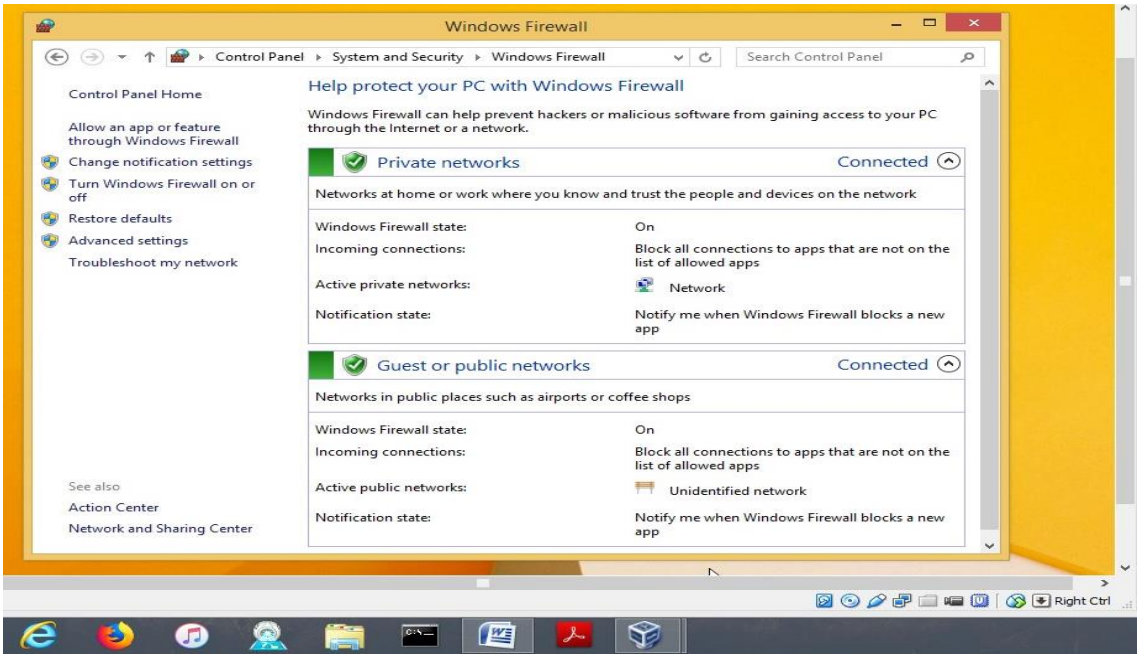
6.Recorded Time.....22

1. Introductory Part: Enable Inbound Rules for IPv4 and IPv6

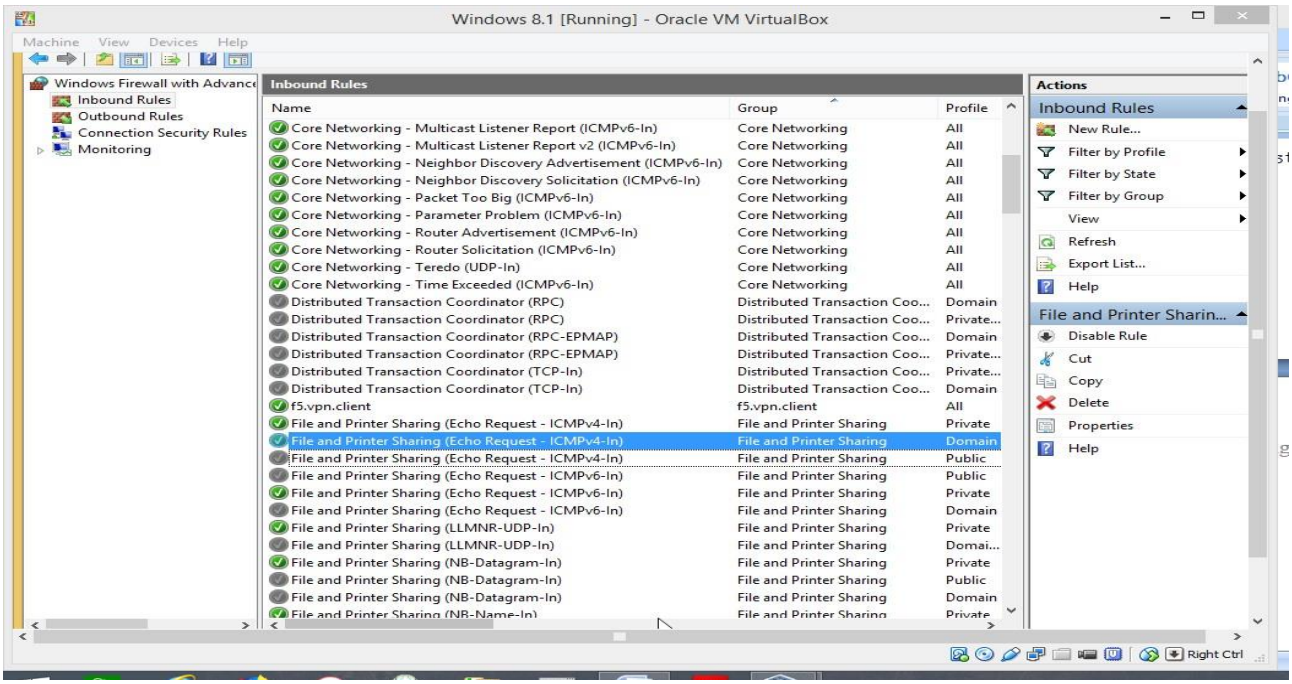
->Step1: Enable Inbound Rules for IPv4 and IPv6 on Win8.1.

-Run Windows 8.1 on VM ware, and go to Control Panel ->Windows Firewall to make changes in the advanced settting on the system.



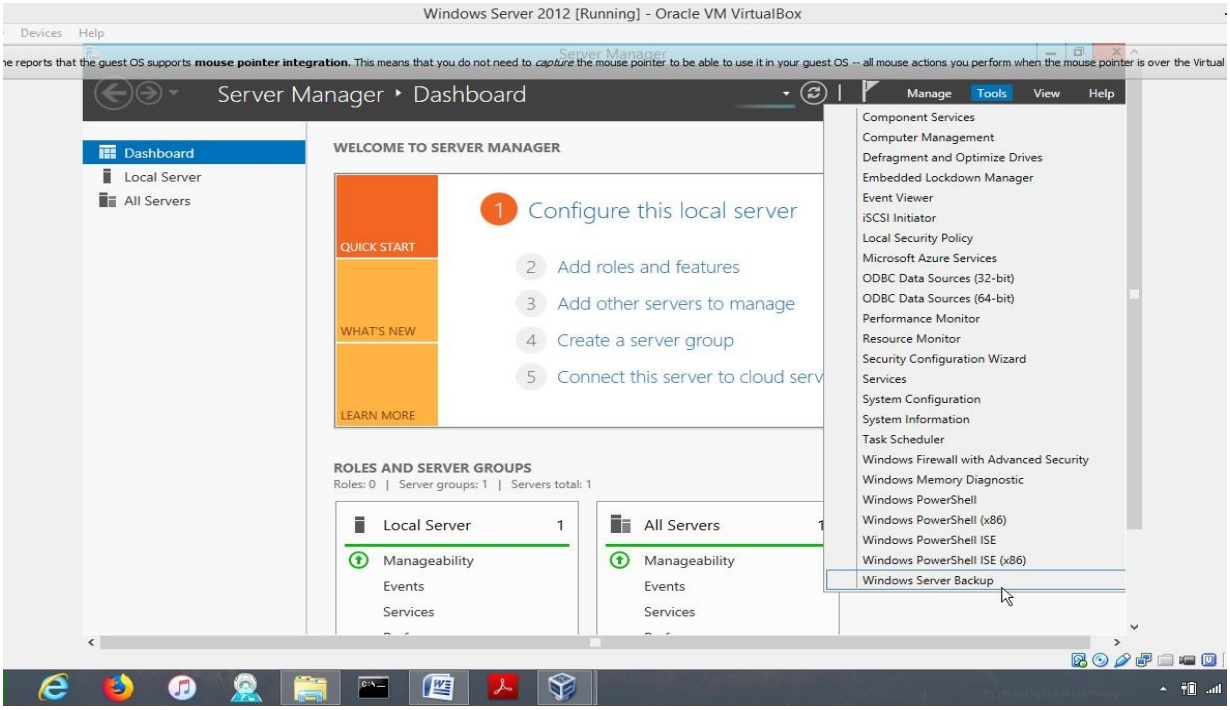


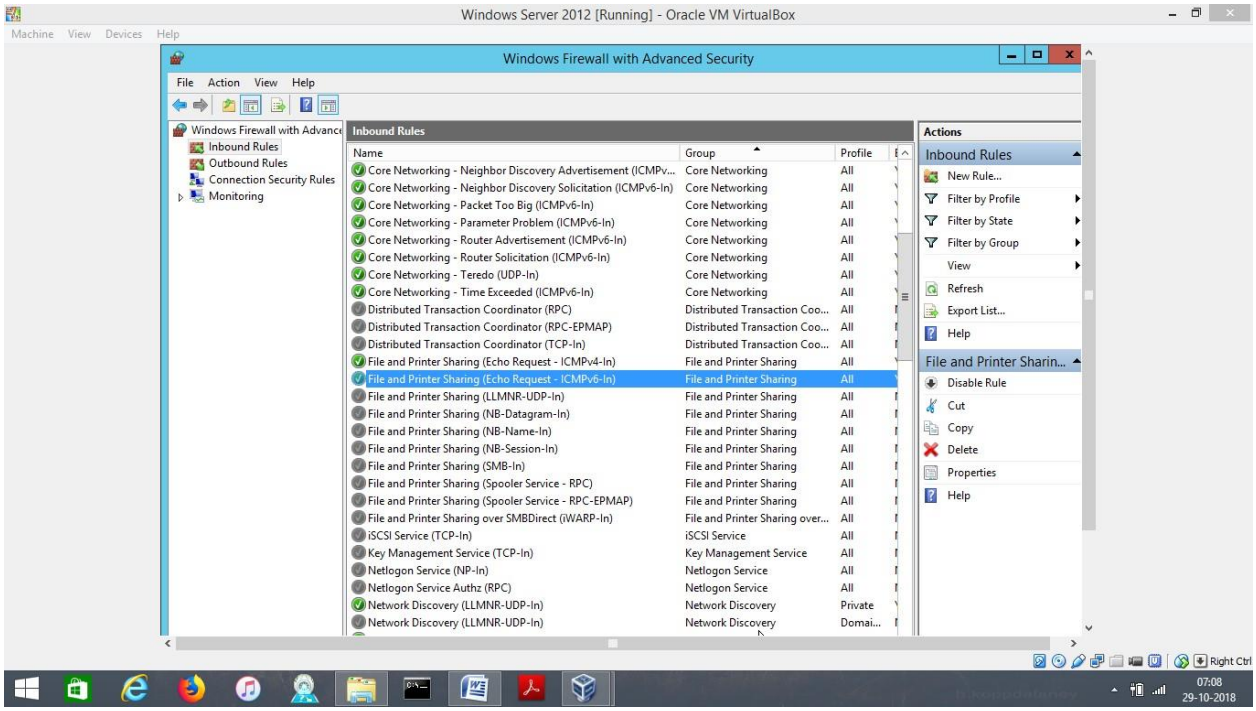
-Go to Advanced setting and select inboundRules, which will display set of settings in which we need to enable the rules for both IPv4 and IPV6 (File and sharing) as shown below



Step2: Enable Inbound Rules for IPv4 and IPv6 on W2K12.

Follow the same steps on Windows Server 2012 to enable the rules.

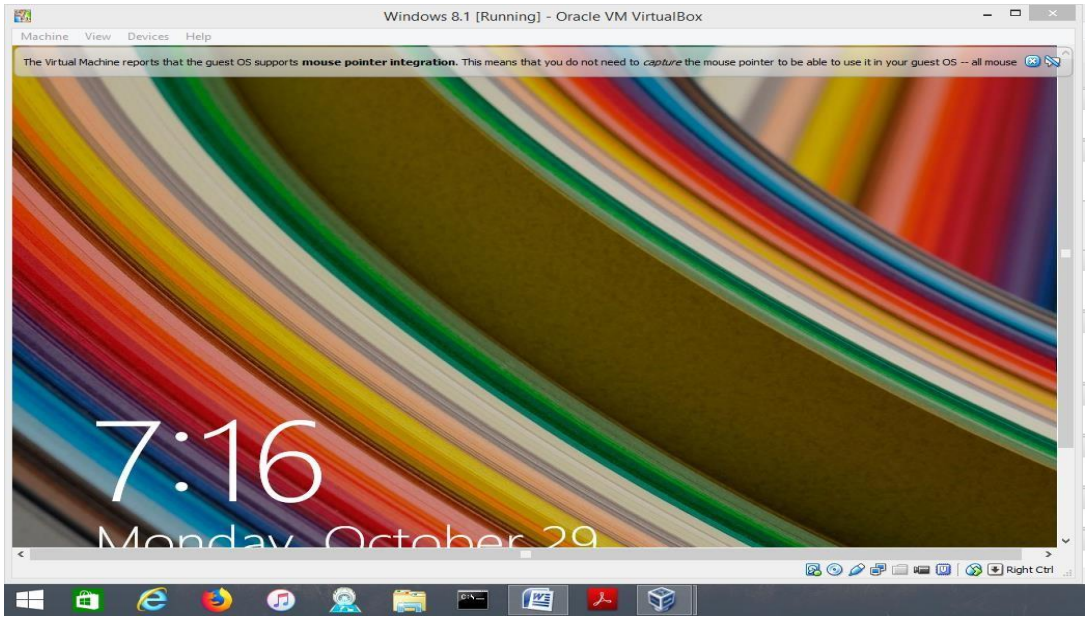




2 .Lab 1.1w: Windows Client Configuration

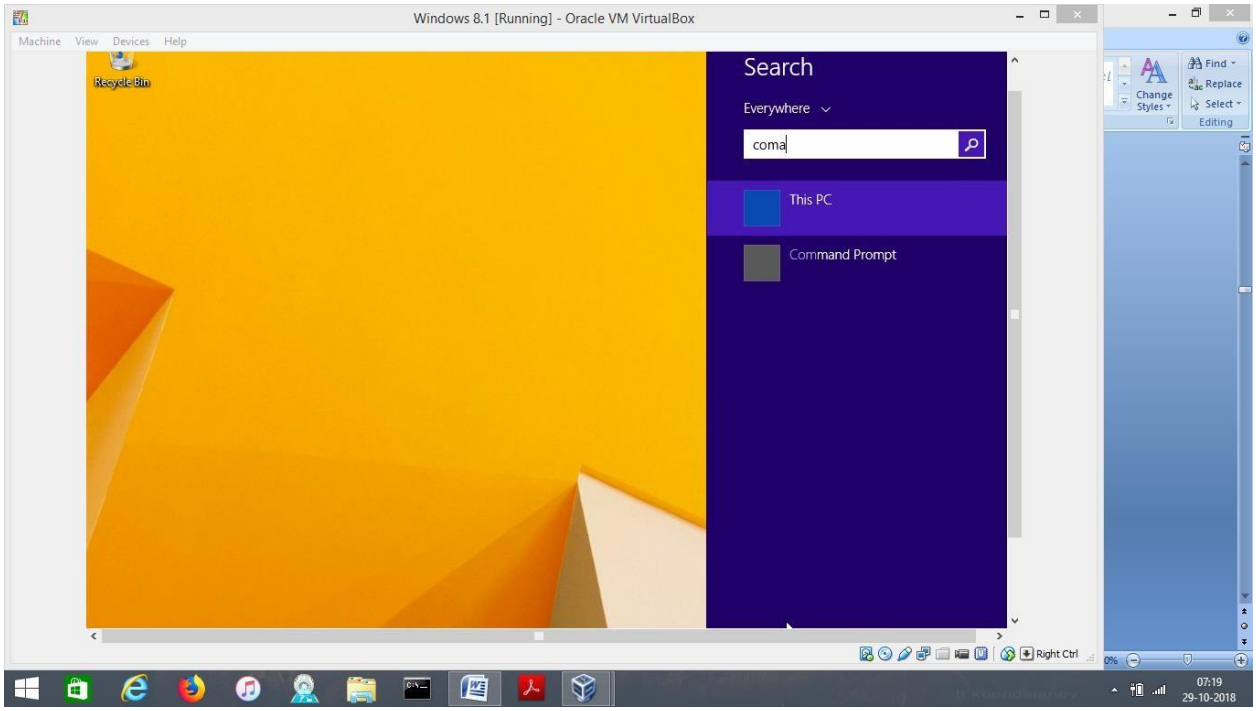
2.1. Step 1: Start Win8.1.

Start Windows 8.1.

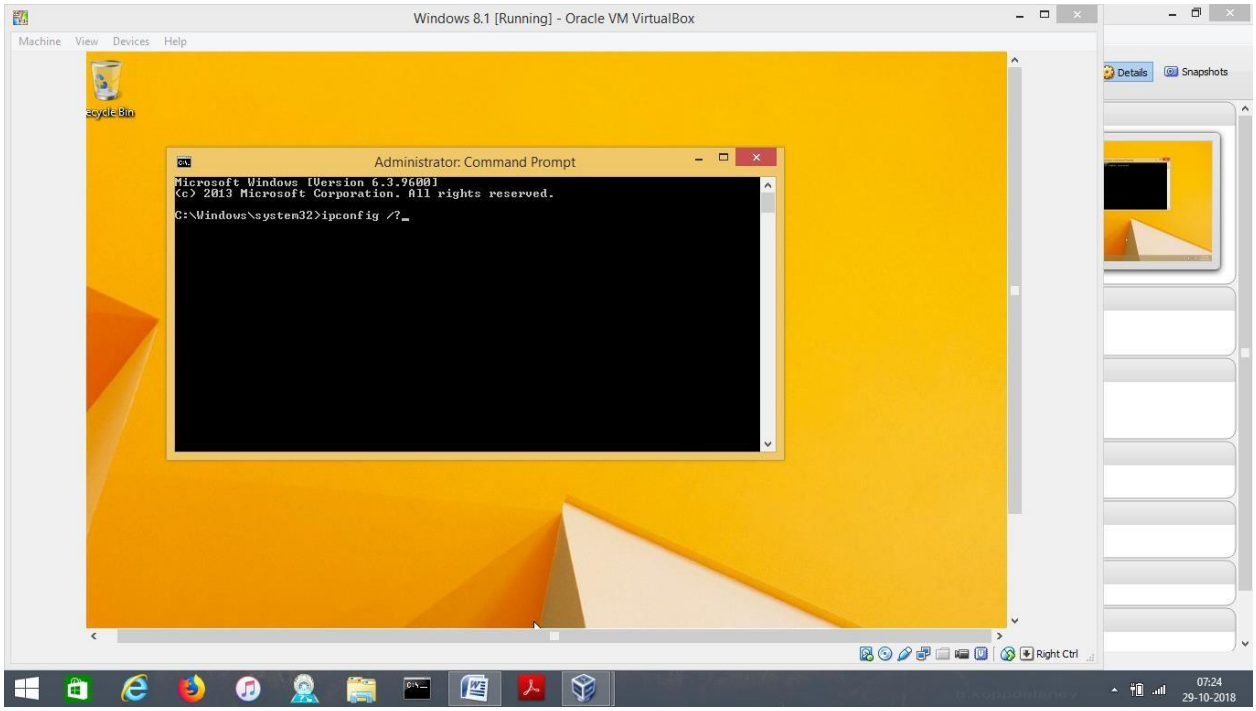


Step 2: View and Record the Network Configuration.

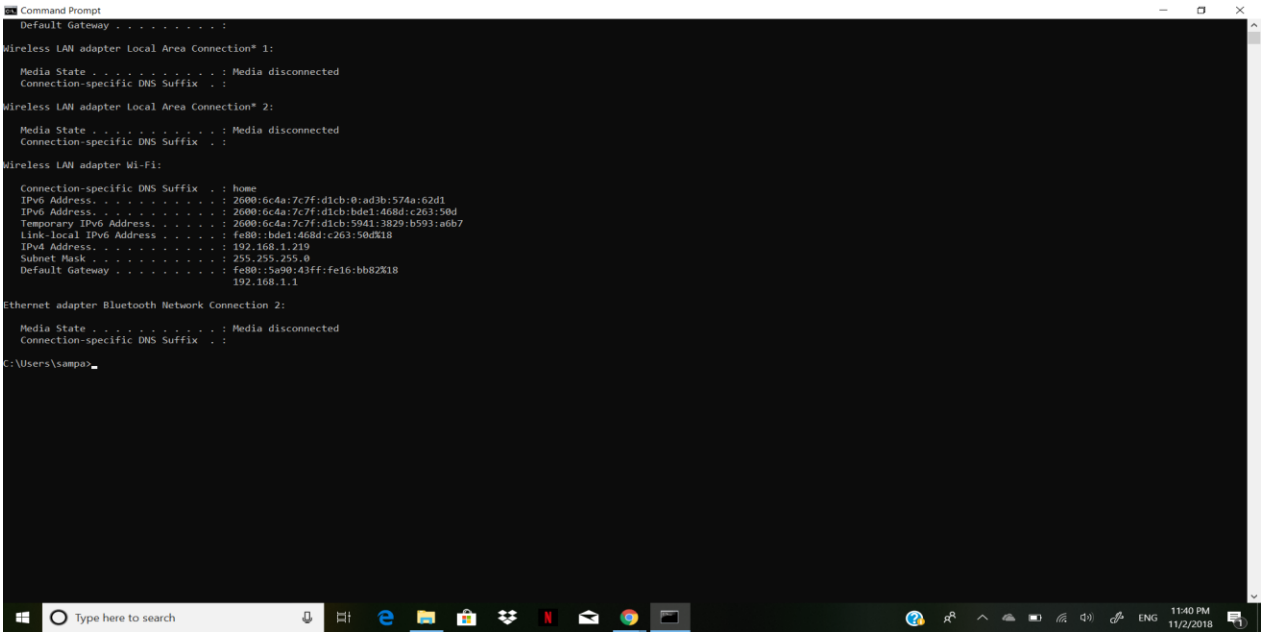
On Windows 8.1, open command Prompt and run as administrator as shown below.



-Type ipcofig /?, which will display you the ip confirguration of the guest system.

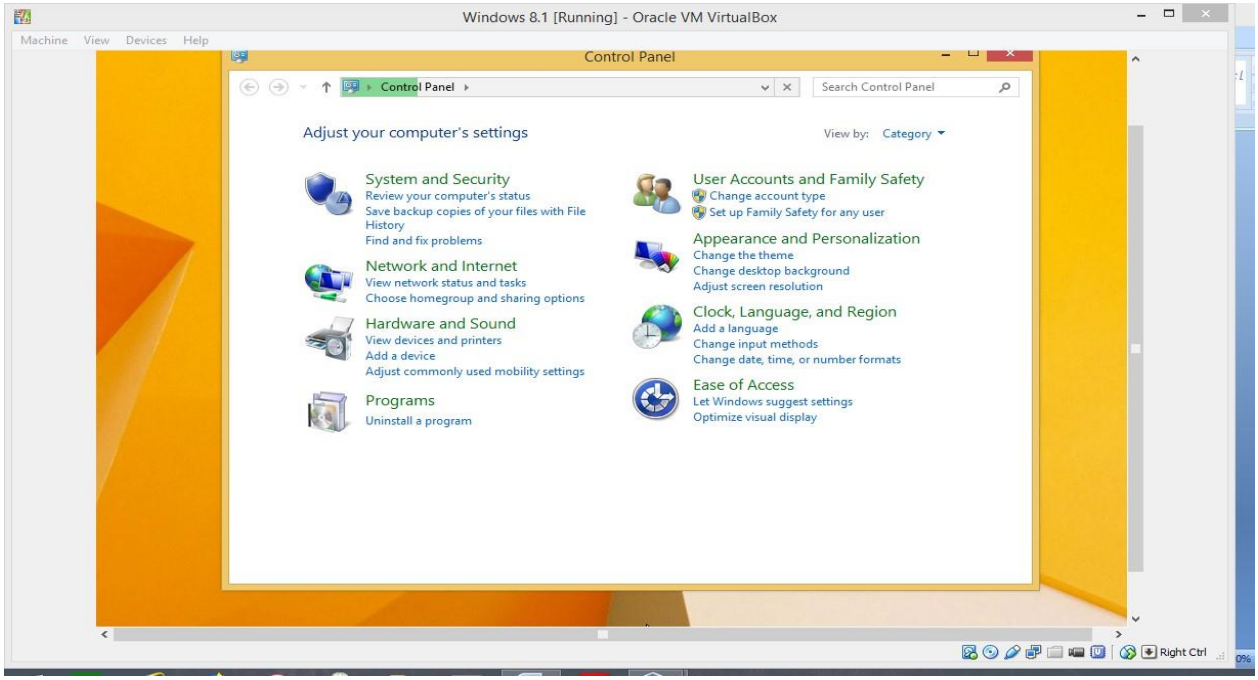


-Type ipconfig /all, which will then show you the overall system configurations, connections (Ethernet Adaptor configurations)

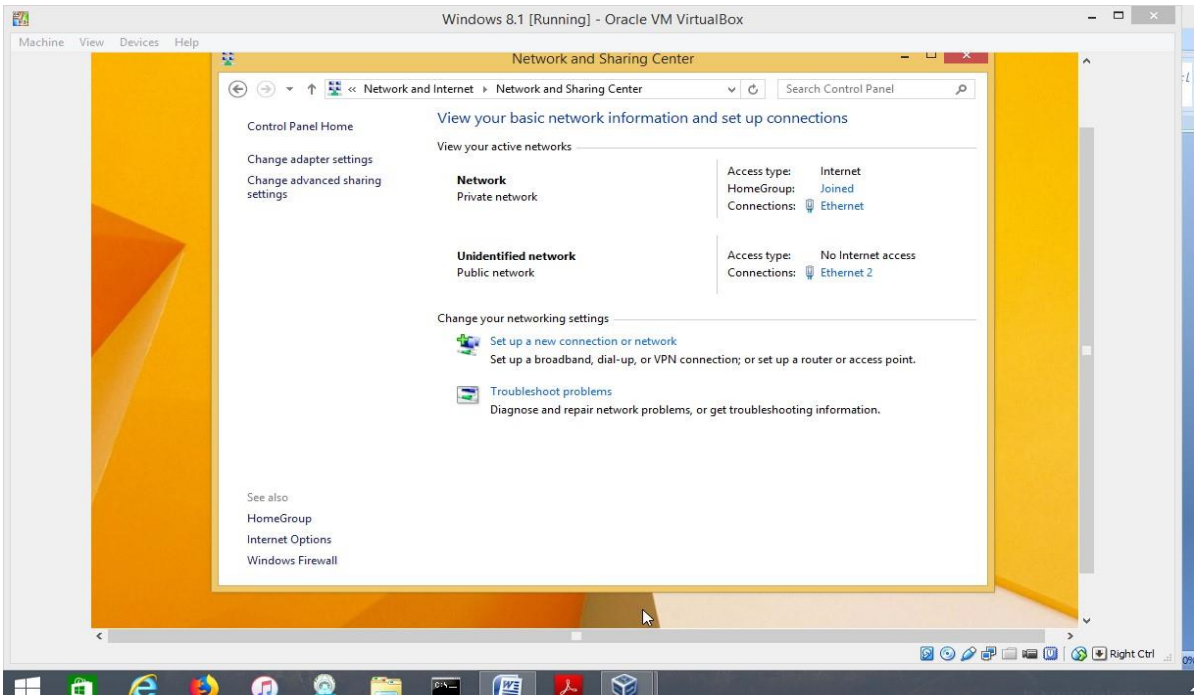


Step 3: Change the IP Address of Win8.1.

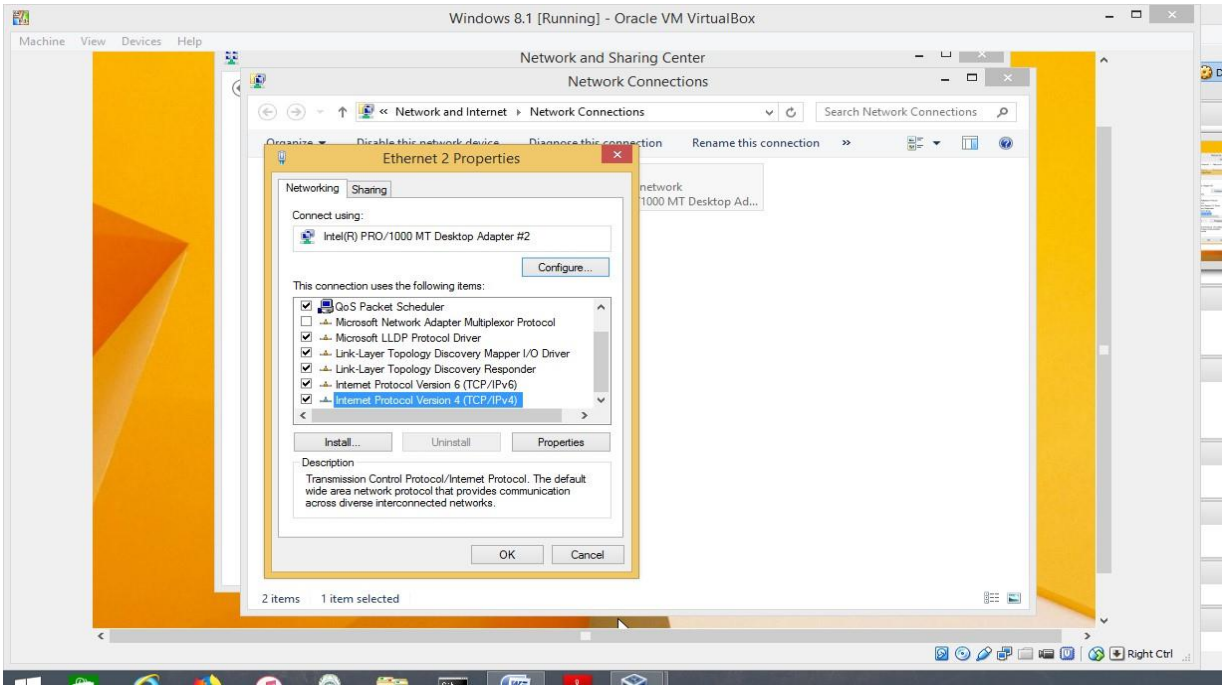
-On Windows 8.1, Go to Control Panel and then go to Network And Internet.



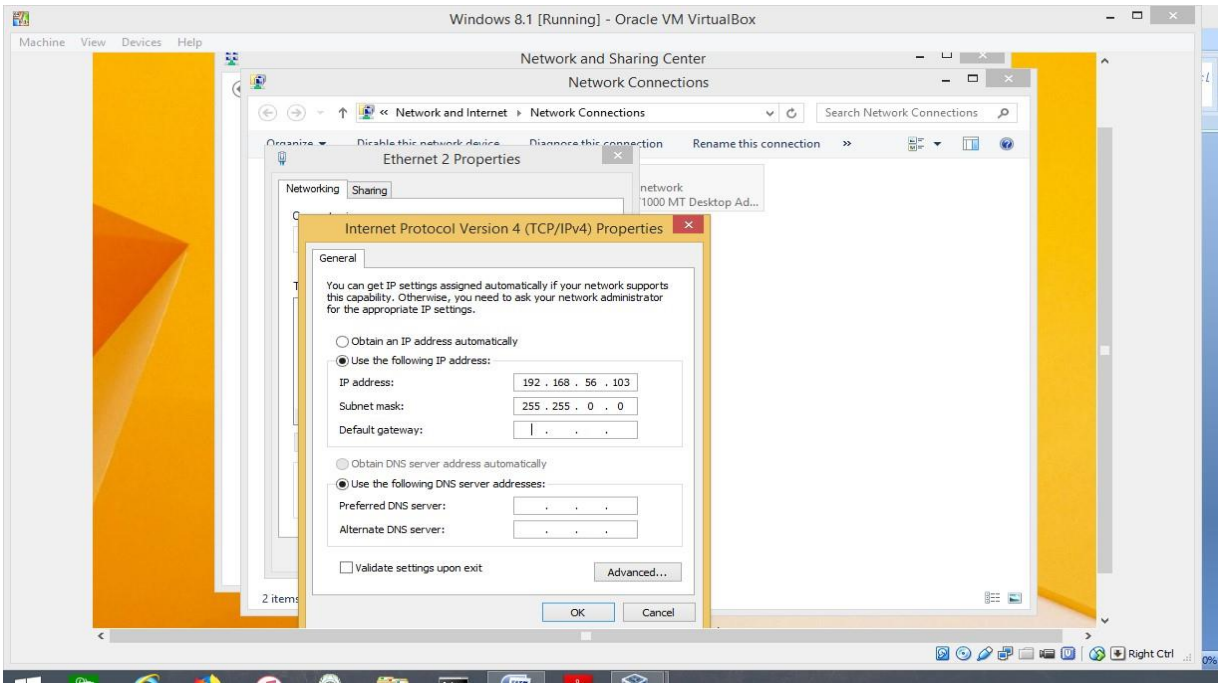
-SELECT NETWORK AND SHARING CENTER.



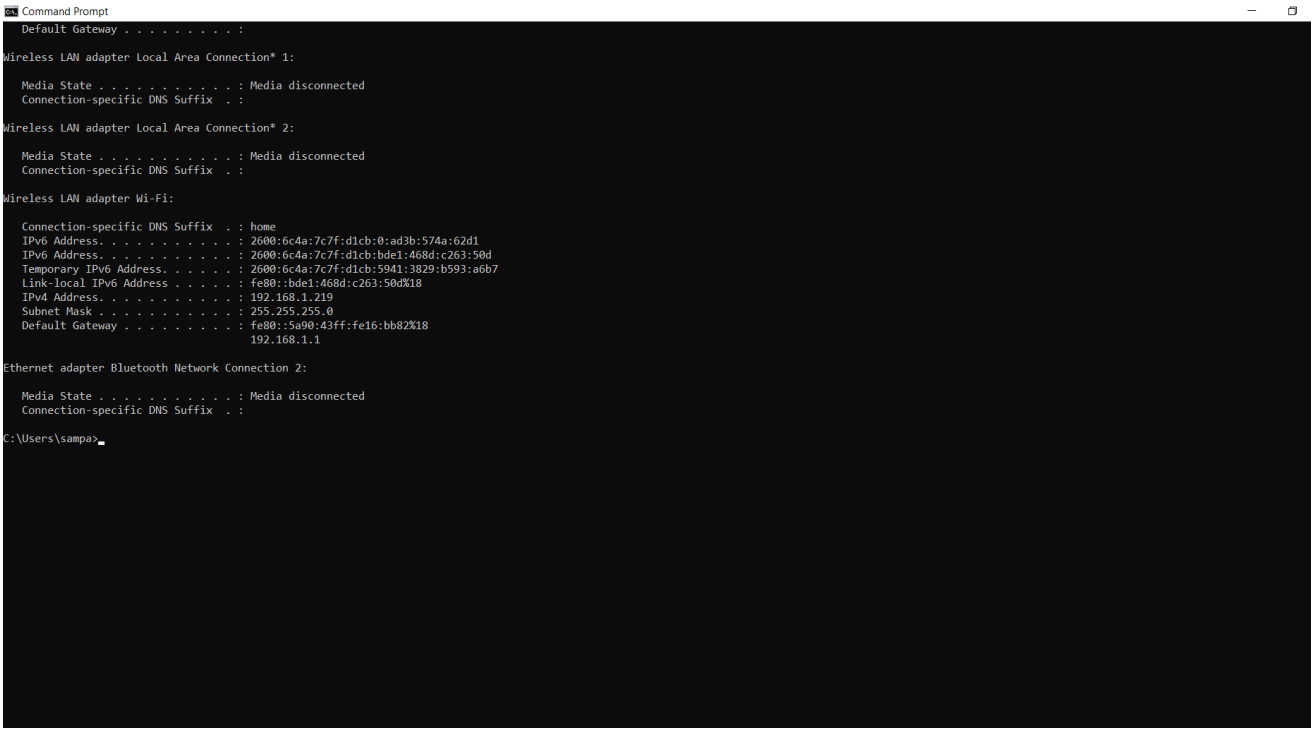
-HERE WE NEED TO GO TO CHANGE ADAPTER SETTINGS. AND GO TO ETHERNET PROPERTIES TO SELECT (INTERNET PROTOCOL VERSION 4)



GO TO THE PROPERTY SETTINGS AND CHANGE THE IP ADDRESS AS SHOWN IN THE FIGURE.

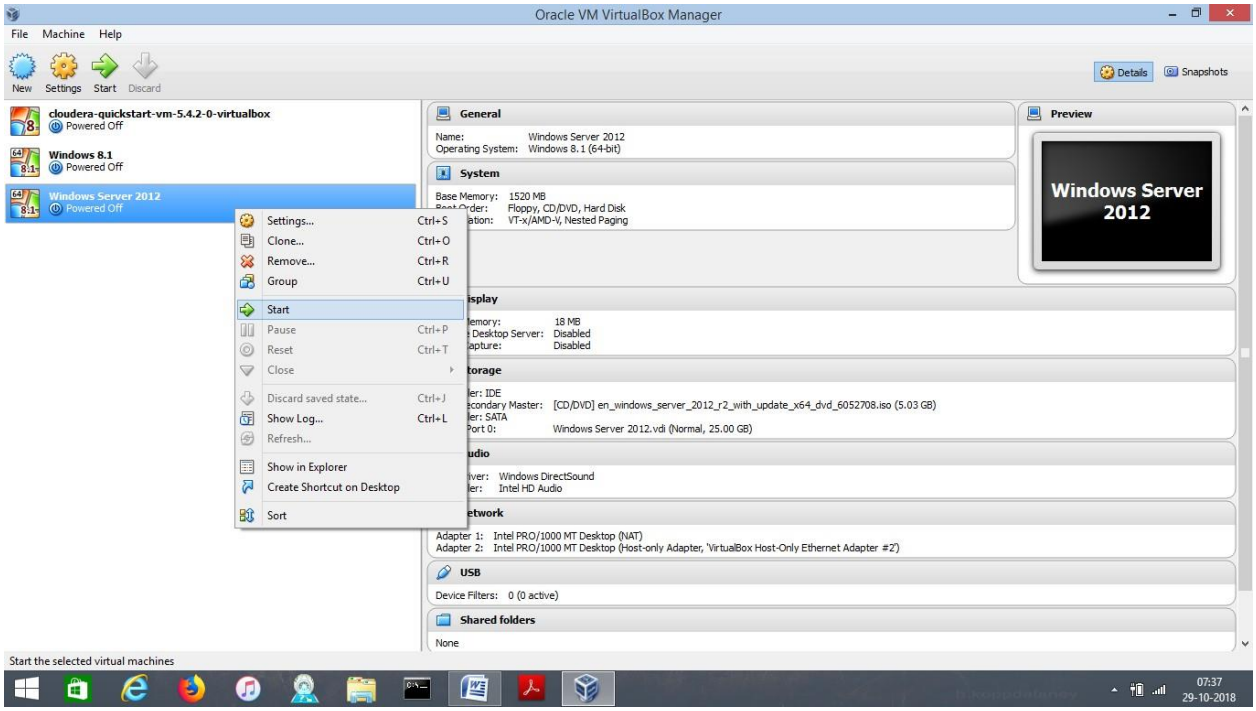


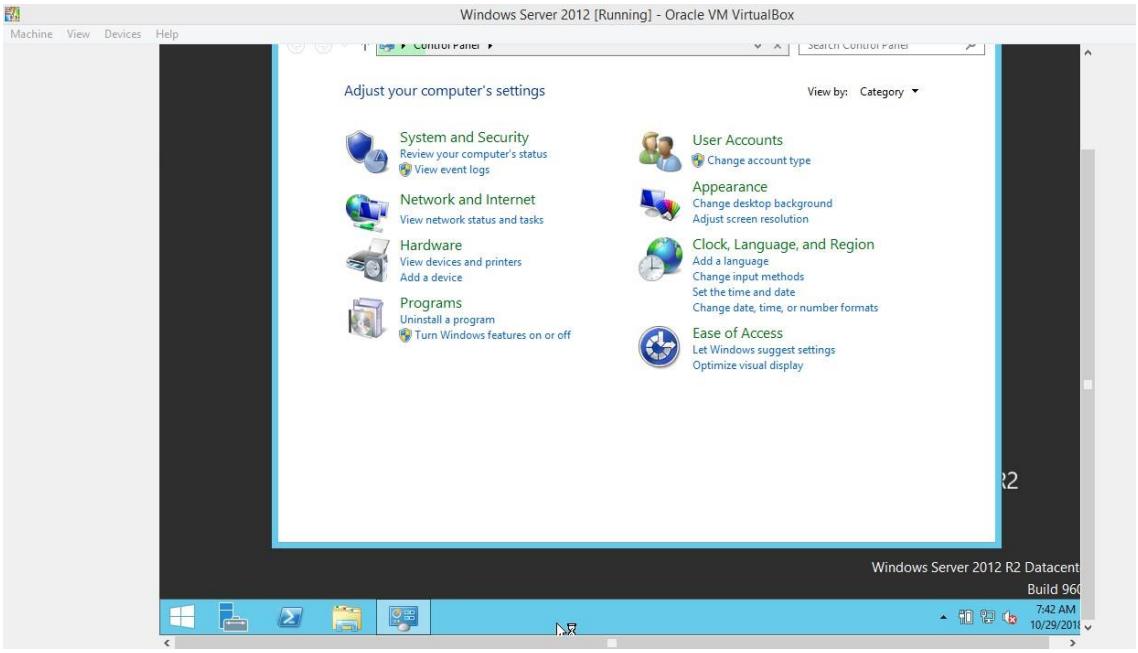
-AGAIN GO TO COMMAND PROMPT AND CHECK THE IP CONFIGURATION CHANGE BY TYPING (IPCONFIG)

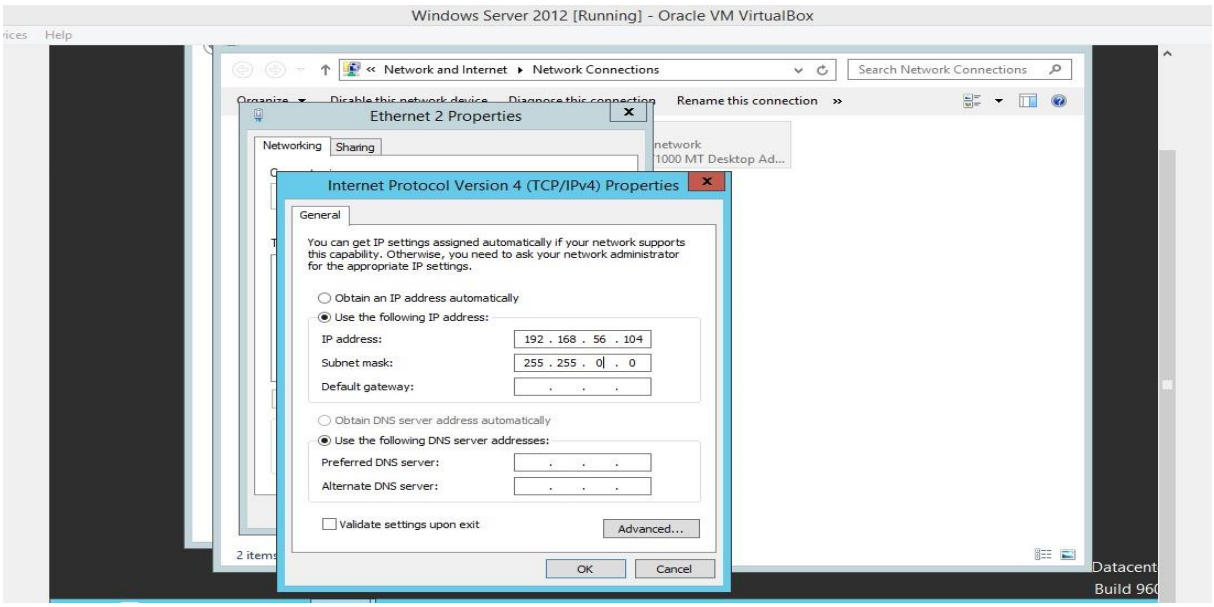


Step 4: Change the IP Address of W2K12.

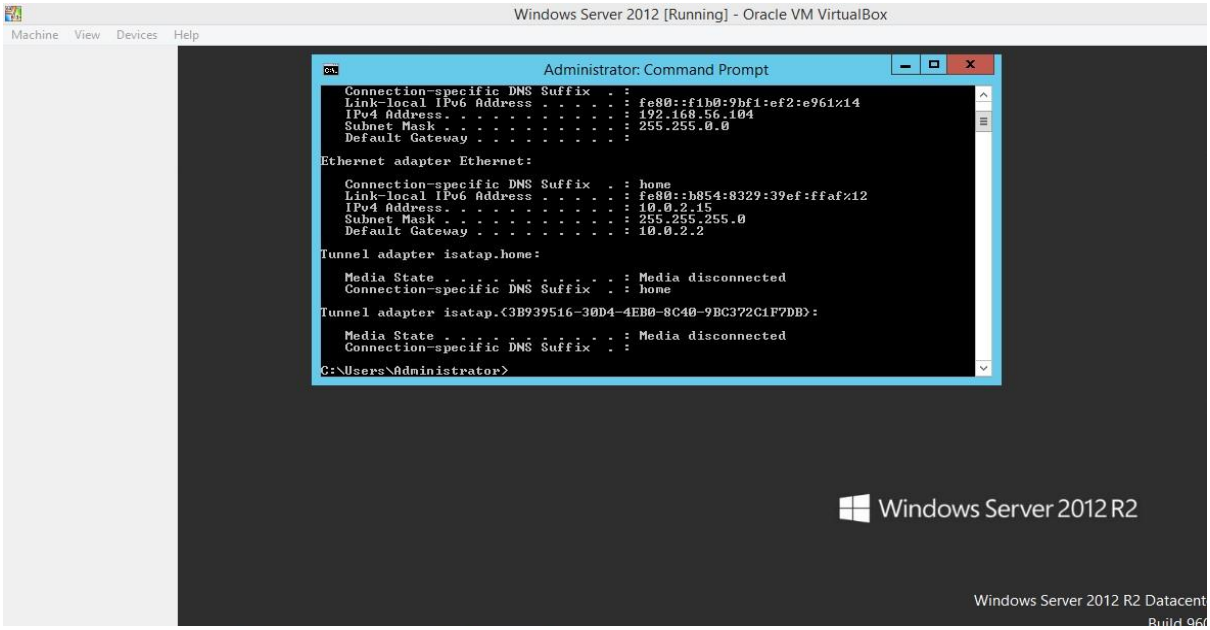
-Follow the same steps and change ip address of W2k12 as shown below.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Start Discard
Details Snapshots
cloudera-quickstart-vm-5.4.2-0-virtualbox
Powered Off
Windows 8.1
Powered Off
Windows Server 2012
Powered Off
Settings... Ctrl+S
Clone... Ctrl+O
Remove... Ctrl+R
Group Ctrl+U
Start
Pause Ctrl+P
Reset Ctrl+T
Close
Discard saved state... Ctrl+J
Show Log... Ctrl+L
Refresh...
Show in Explorer
Create Shortcut on Desktop
Sort
General
Name: Windows Server 2012
Operating System: Windows 8.1 (64-bit)
System
Base Memory: 1520 MB
Floppy, CD/DVD, Hard Disk
VT-x/AMD-V, Nested Paging
Preview
Windows Server 2012
18 MB
Disabled
Disabled
[CD/DVD] en_windows_server_2012_r2_with_update_x64_dvd_6052708.iso (5.03 GB)
Windows Server 2012.vdi (Normal, 25.00 GB)
Windows DirectSound
Intel HD Audio
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter #2')
USB
Device Filters: 0 (0 active)
Shared folders
None
Start the selected virtual machines
07:37
29-10-2018


Windows Server 2012 [Running] - Oracle VM VirtualBox
Machine View Devices Help
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
View event logs
Network and Internet
View network status and tasks
Hardware
View devices and printers
Add a device
Programs
Uninstall a program
Turn Windows features on or off
User Accounts
Change account type
Appearance
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Add a language
Change input methods
Set the time and date
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display
Windows Server 2012 R2 Datacent
Build 960
7:42 AM
10/29/2018

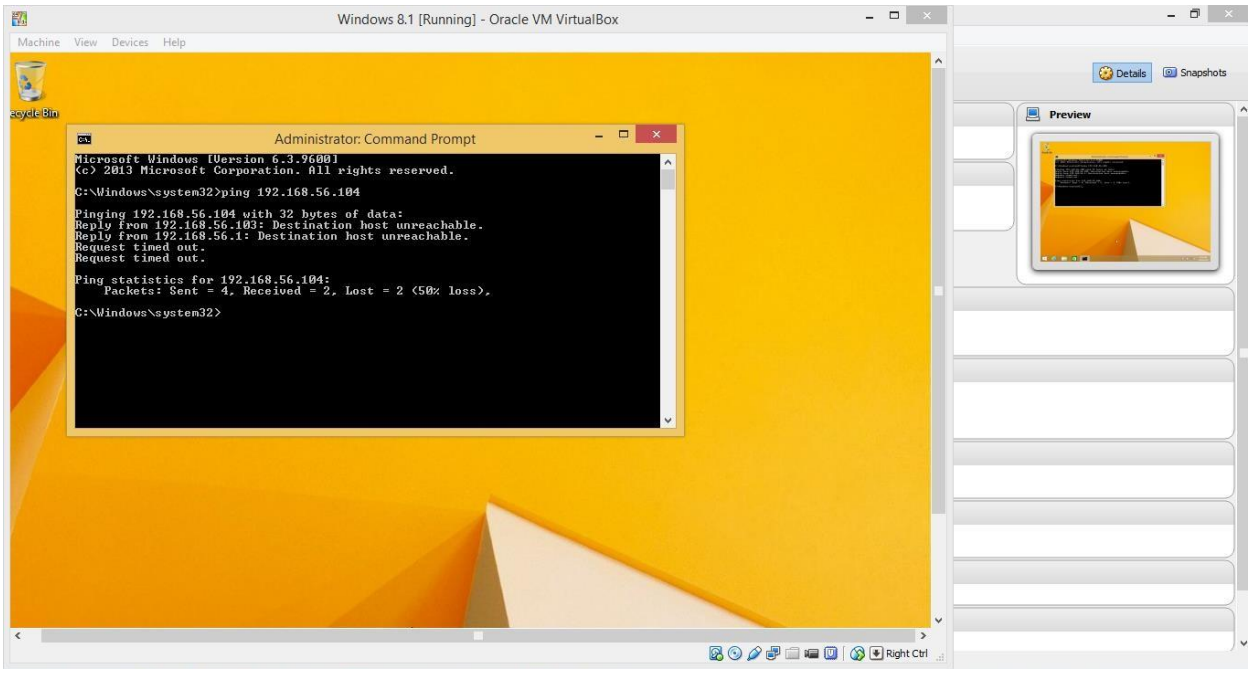


-GO TO COMMAND PROMPT TO OBSERVE THE CHANGES MADE IN THE IP ADDRESS BY TYPING 'IPCONFIG'.



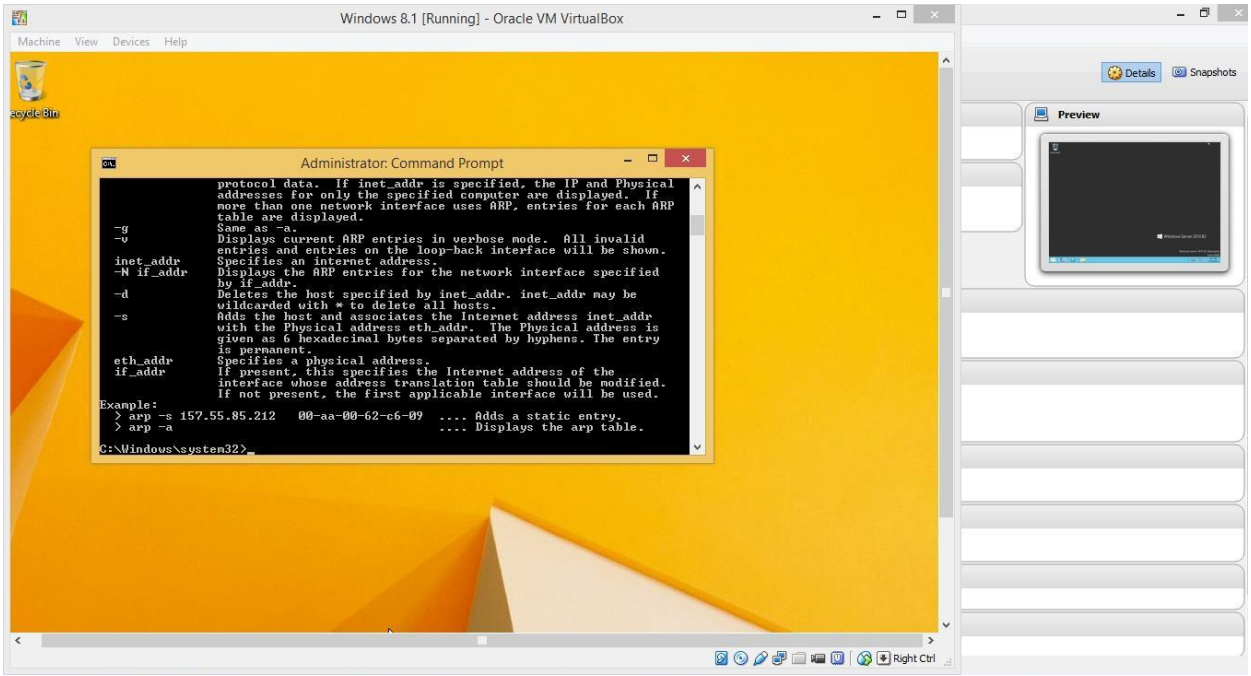
Step 5: From Win8.1, Ping the W2K12 Server

In this step we need to ping server w2k12 from 8.1, on windows 8.1 , command prompt type ping 192.168.56.104

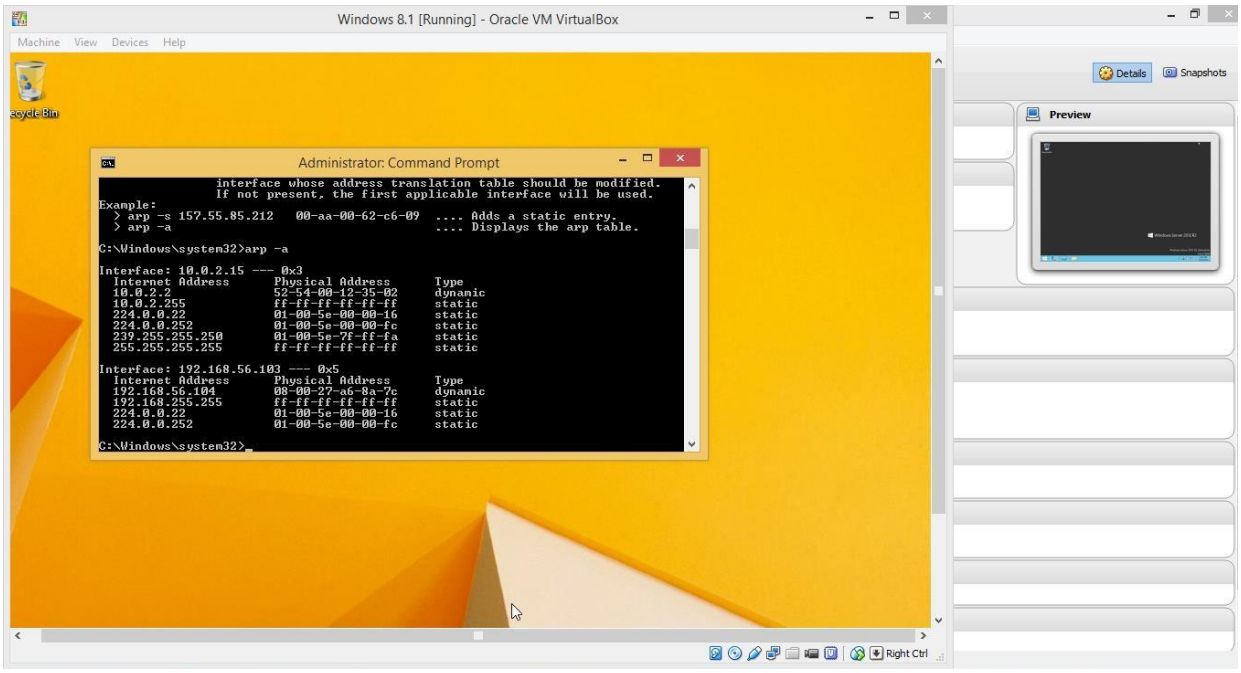


Step 6: View and Modify the ARP Table.

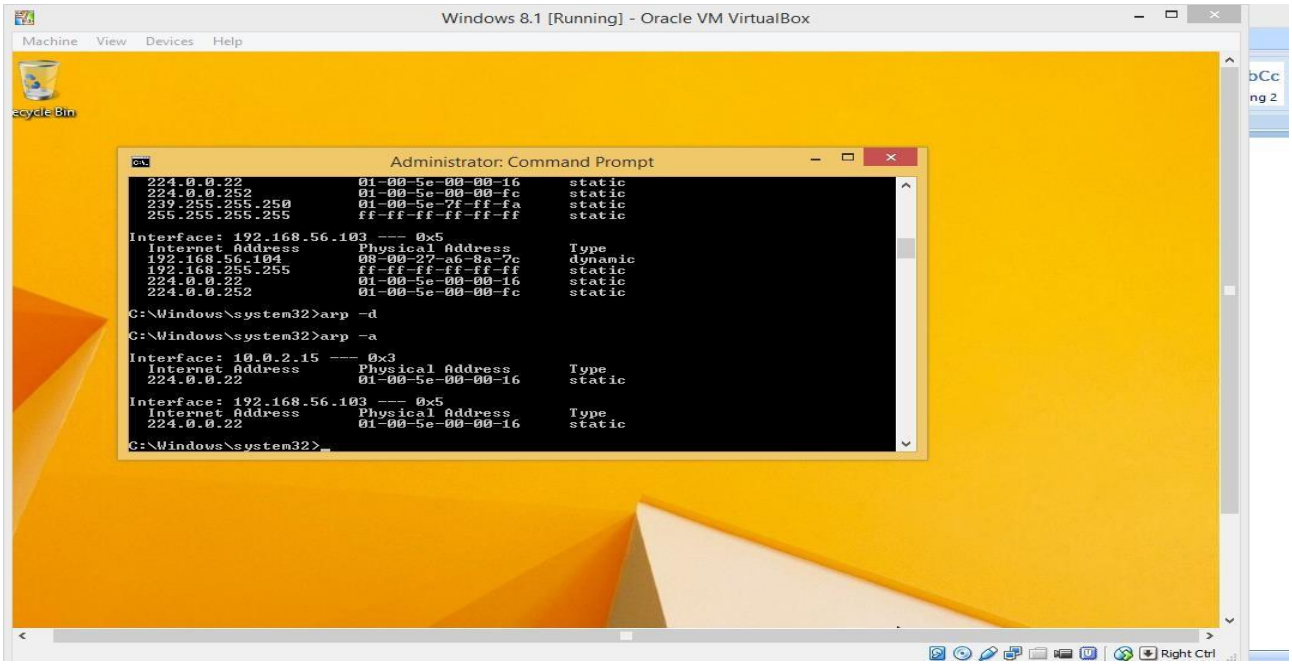
-Type arp /?



-Type arp -a

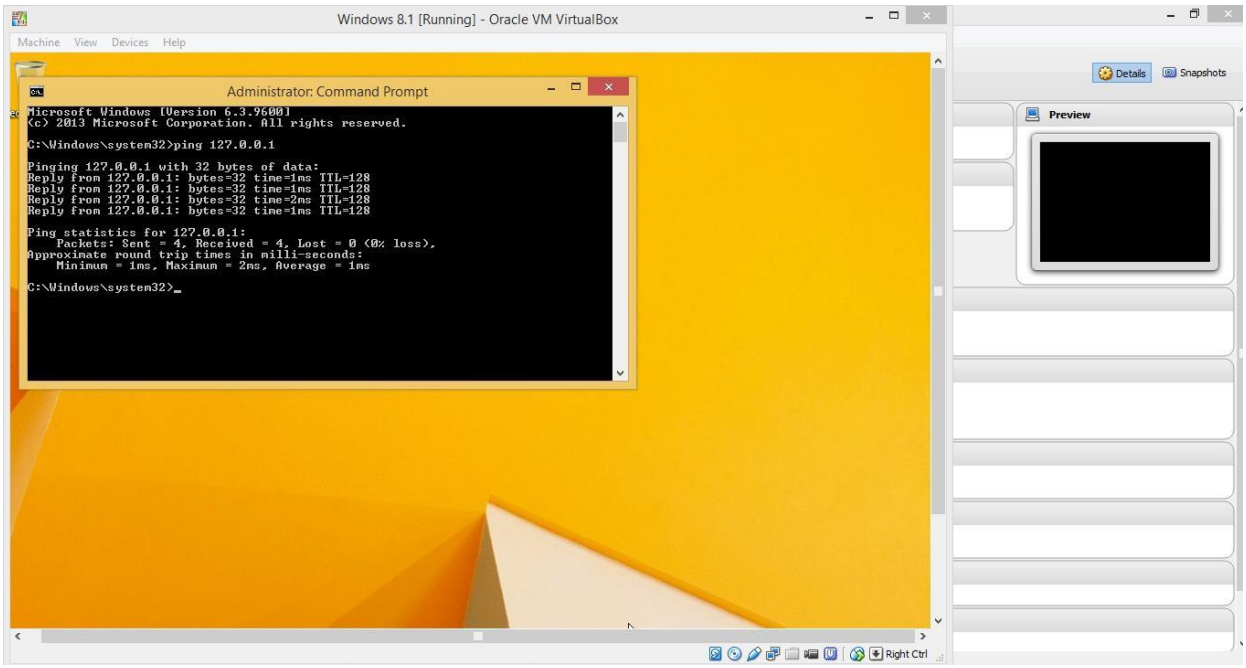


-Type arp –d and arp –a, and observe.

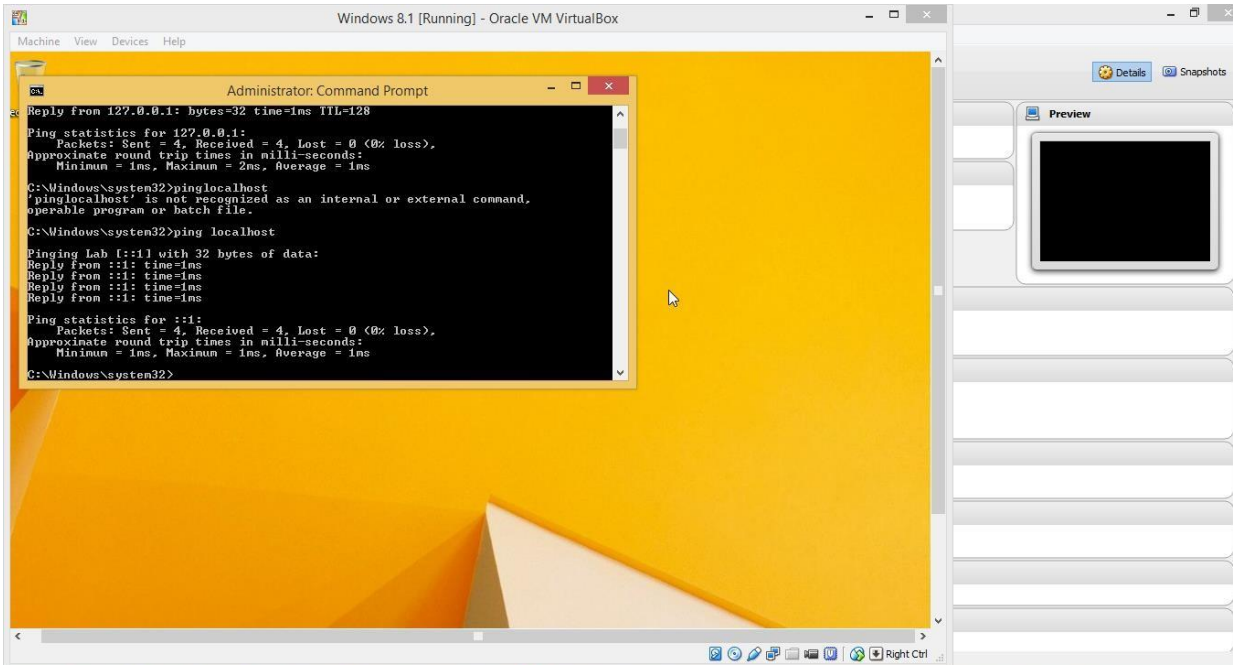


3 Lab 1.2w: Name Resolution in Windows

Step 1: Login to Win8.1 as administrator and ping local host -ping 127.0.0.1, and you can see the transactions.

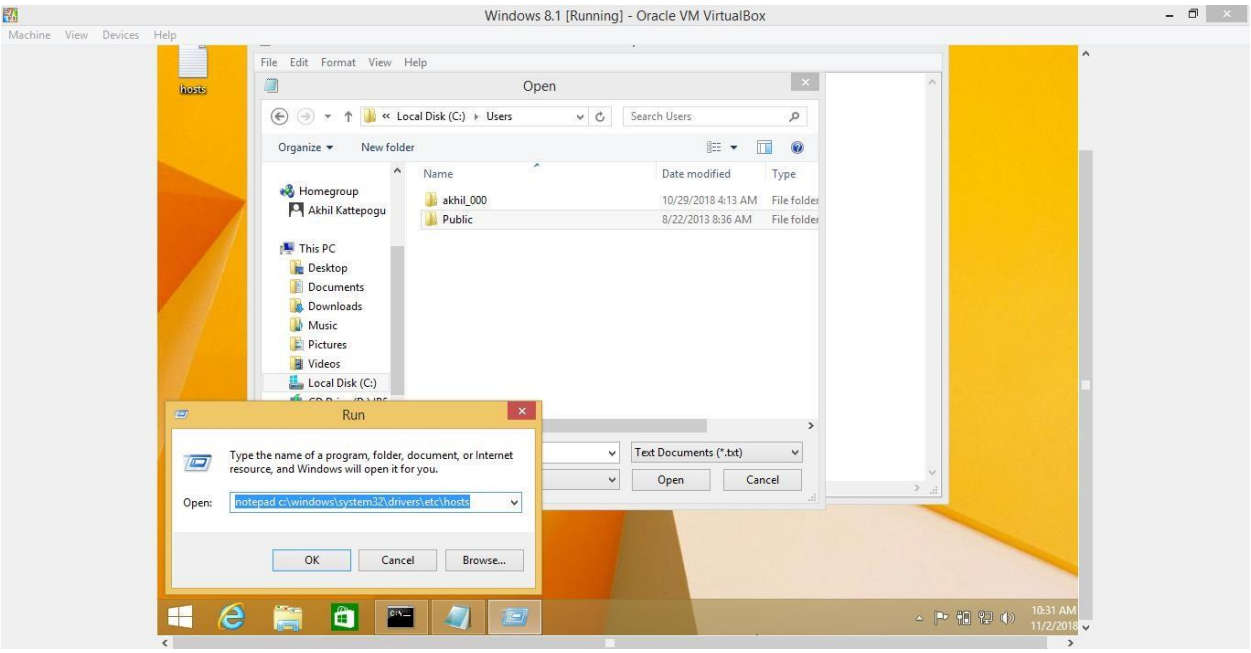


-Type ping localhost.

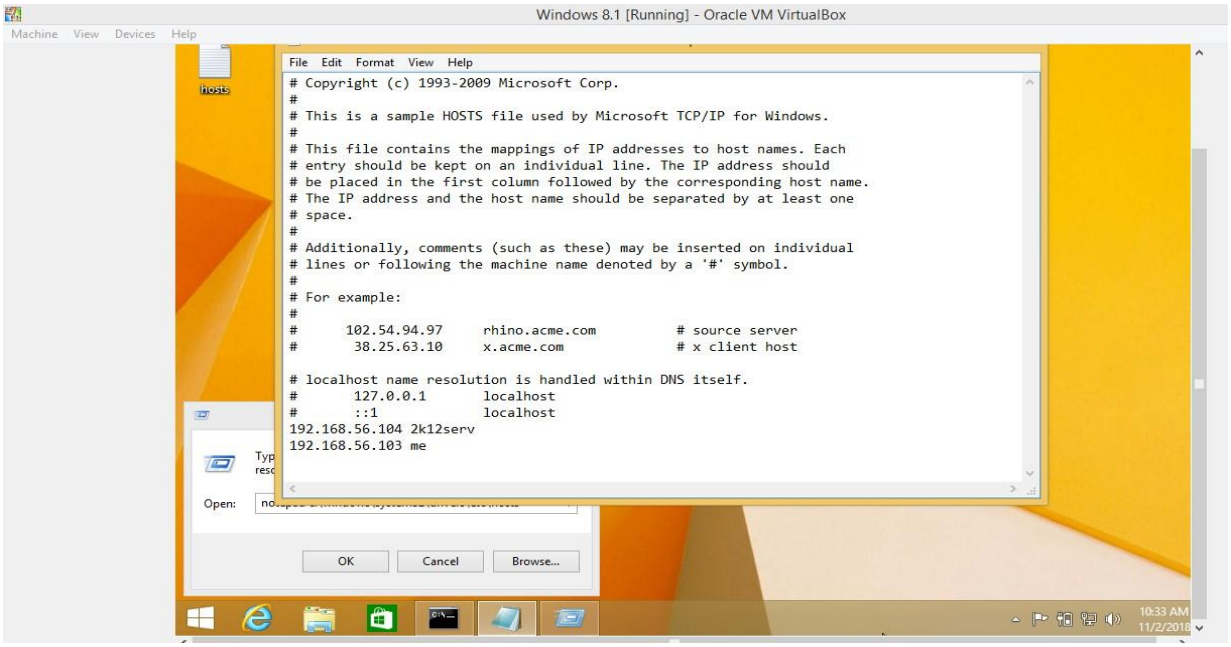


Step 3: View and Modify the Host File.

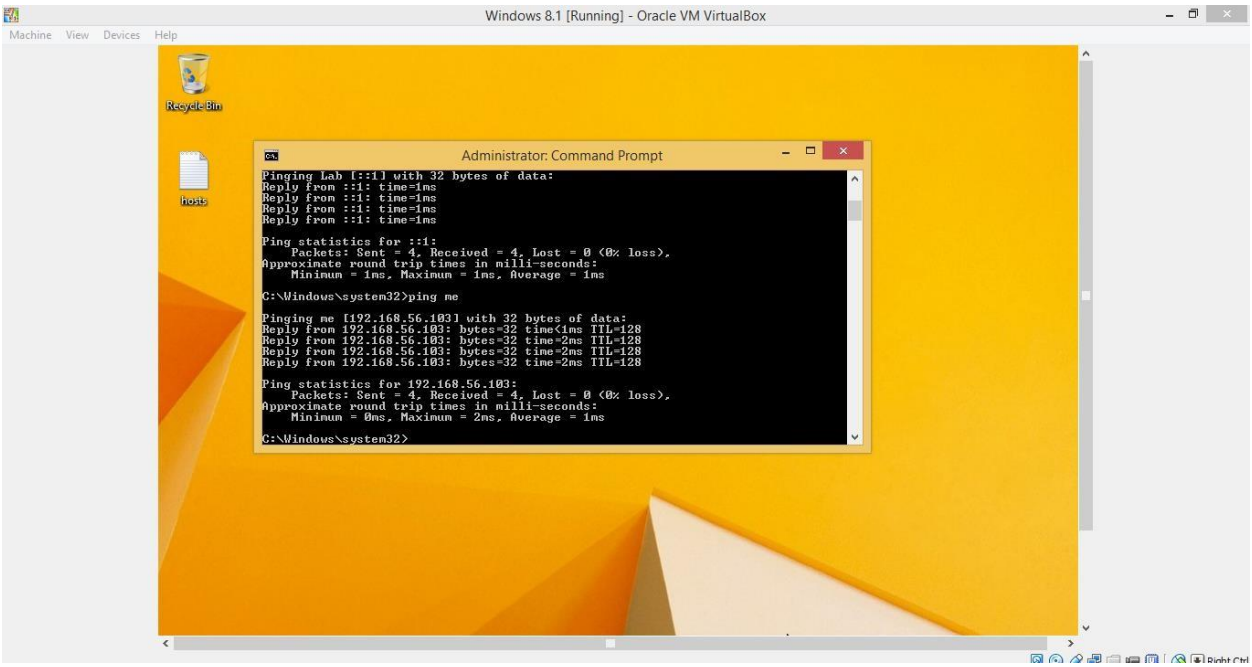
-On Windows 8.1, go to run and type notepad c:\windows\system32\drivers\etc\hosts and a hosts file opens



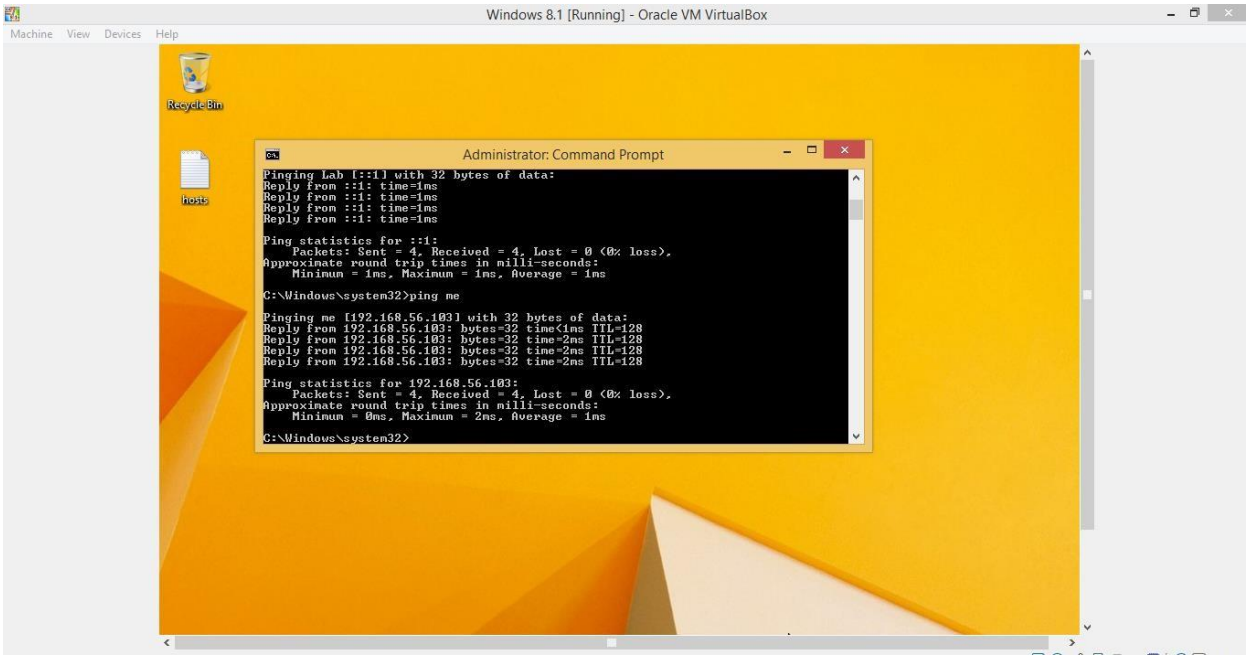
-Add ip address as shown below to the hosts file and save the changes.



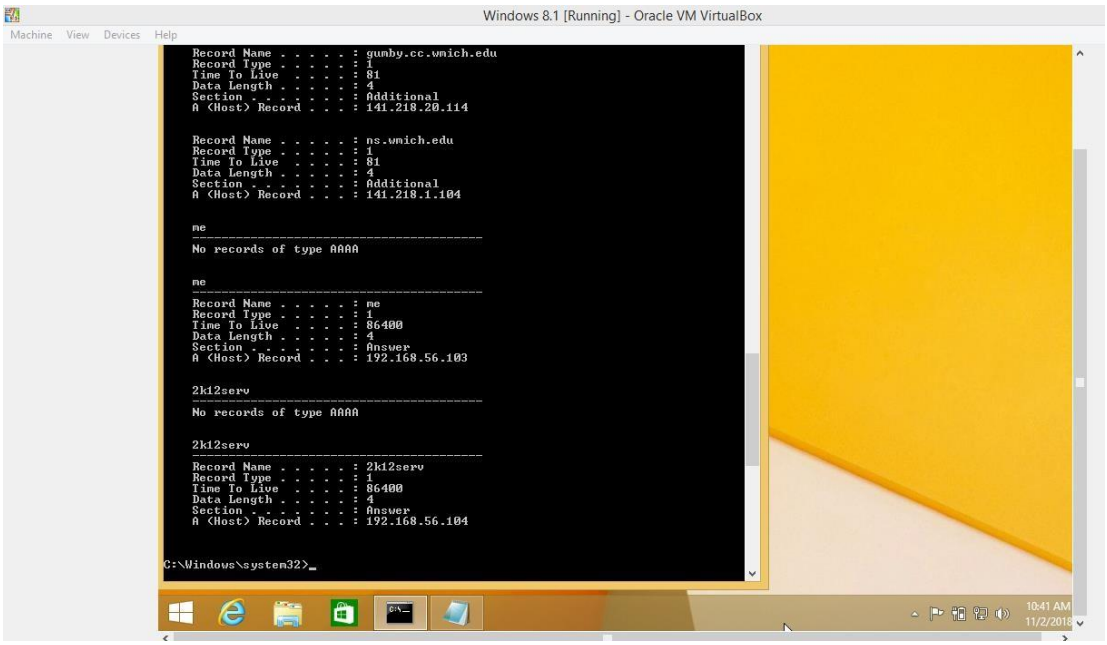
-Type ping me on command prompt



-Type ping 2k12serv on CMD and we can see the reply from the server.



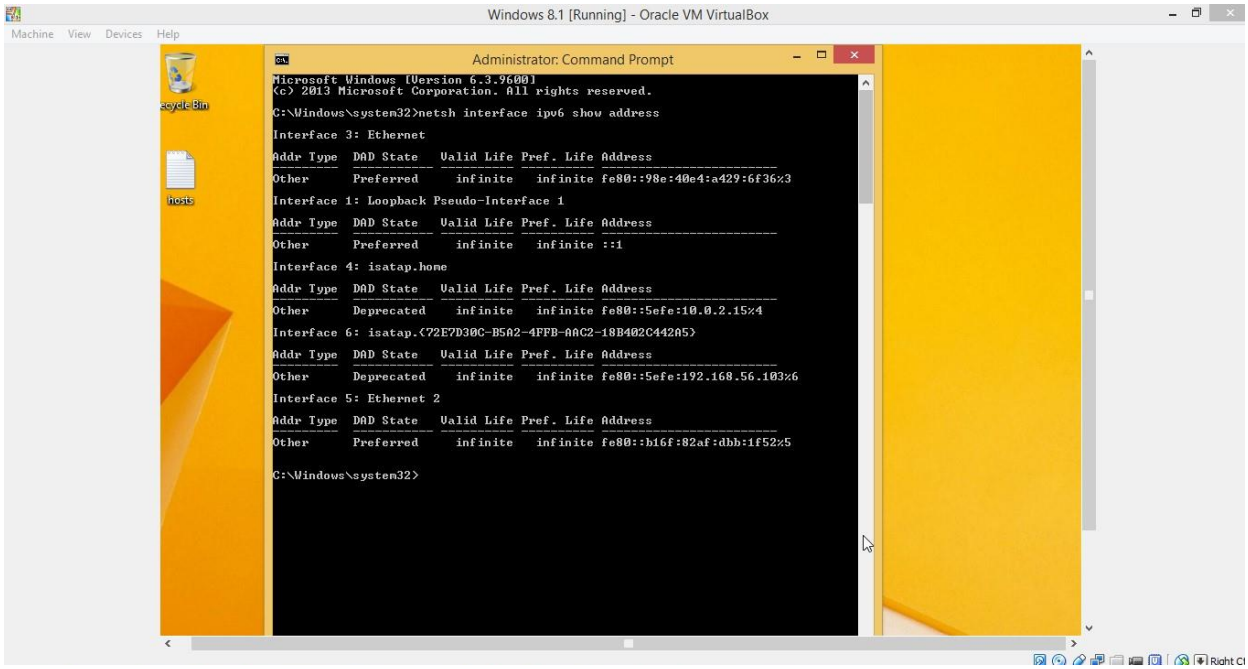
-Type ipcofig /displaydns



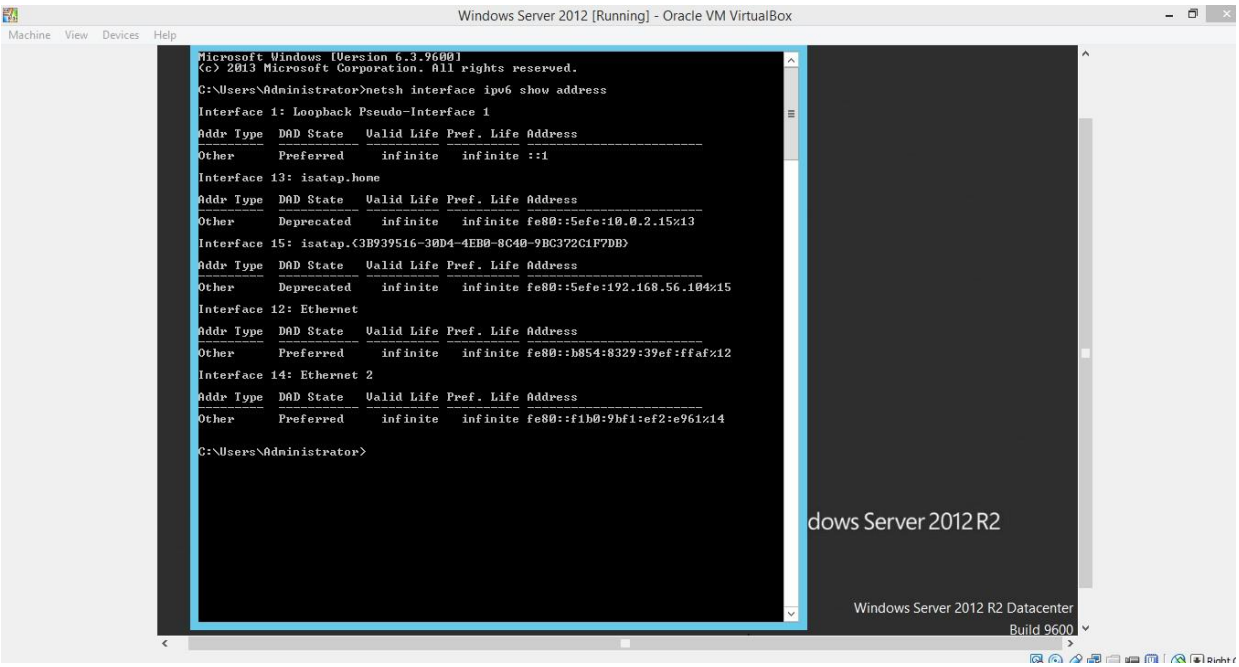
4 Lab 1.3w: Windows IPv6 Basics

Step 1: Verify IPv6 Setting for Win8.1 and W2K12.

-Type netsh interface ipv6 show address, on command prompt on Windows8.1

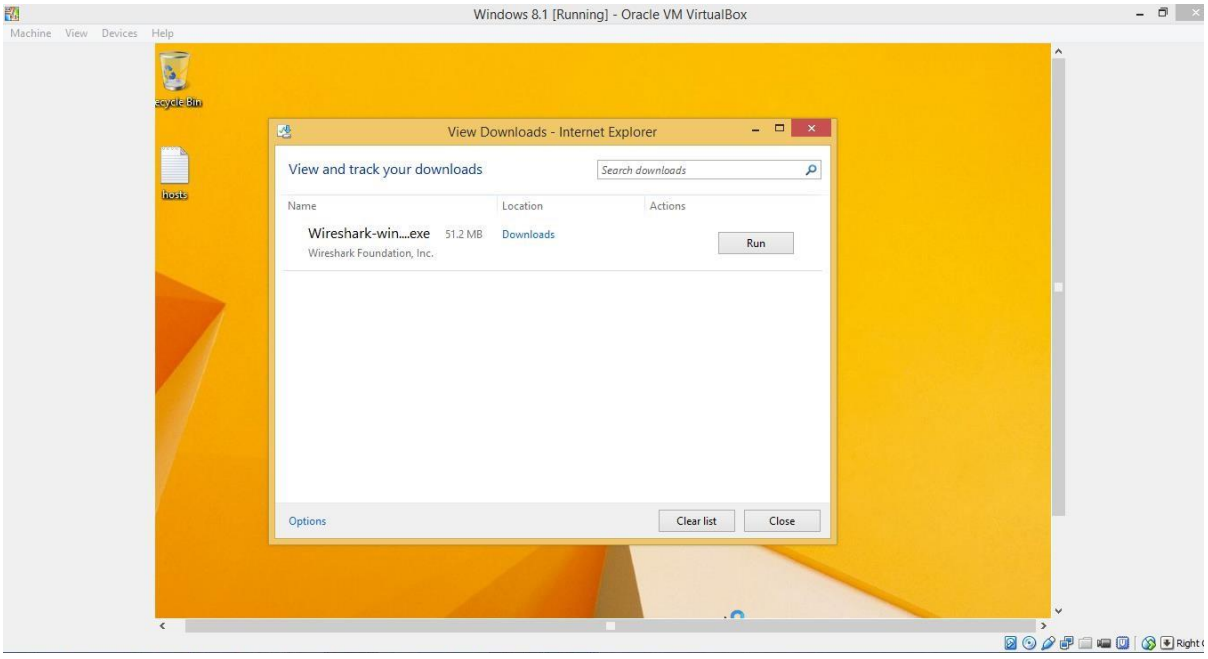


On W2k12, type netsh interface ipv6 show address on command prompt.

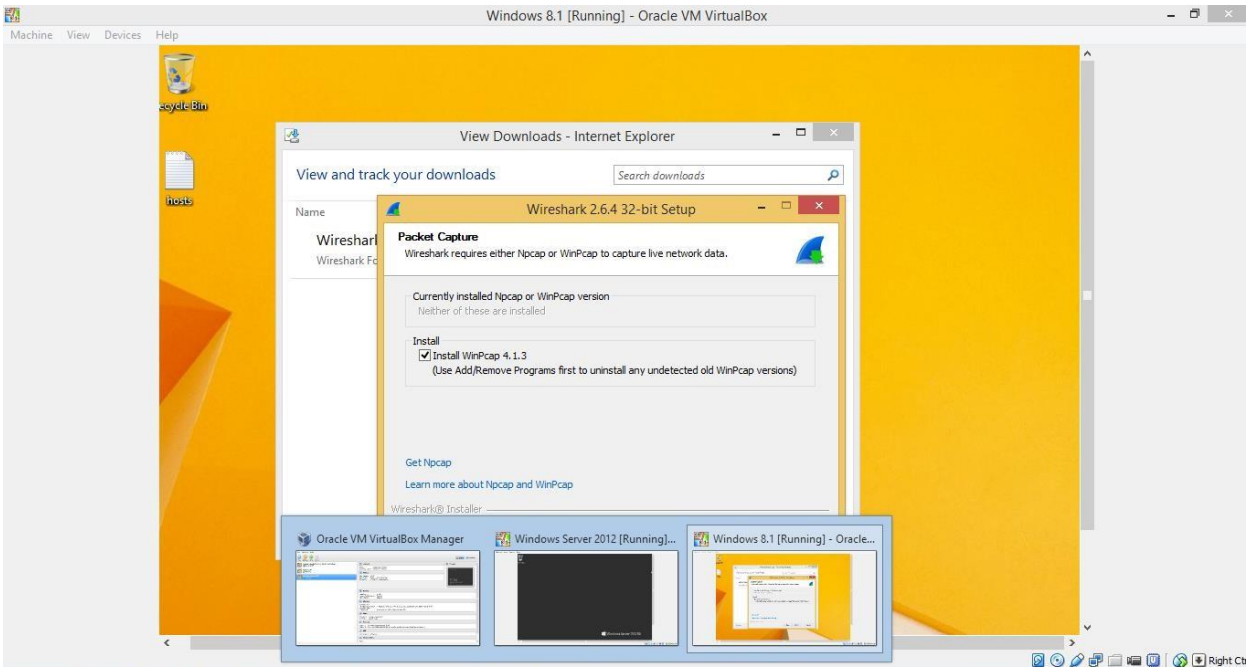


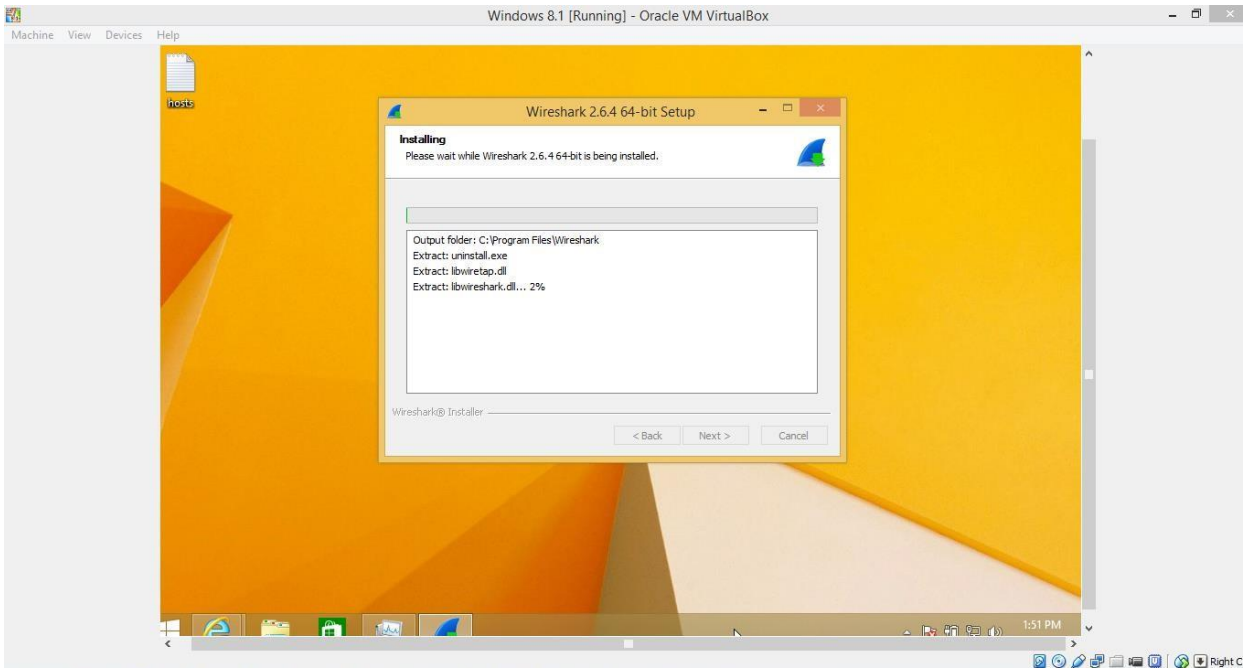
Step 2: Install Wireshark on Win8.1.

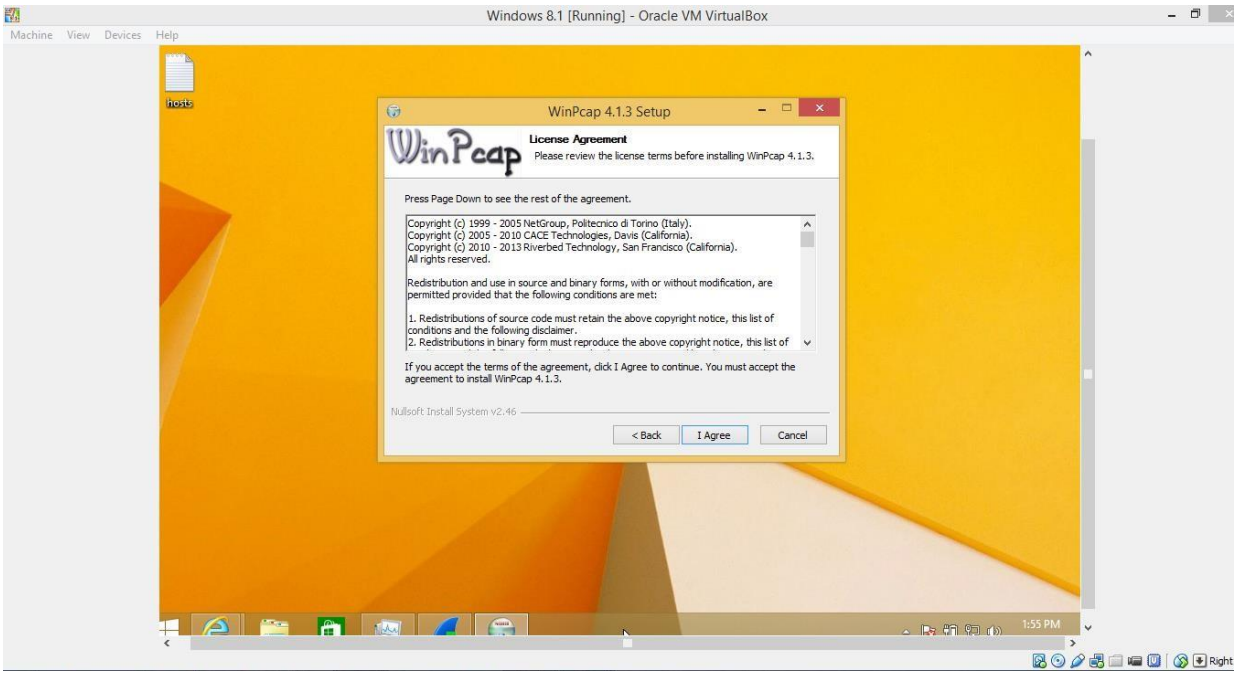
-From website www.wireshark.org/download.html , download wireshark.

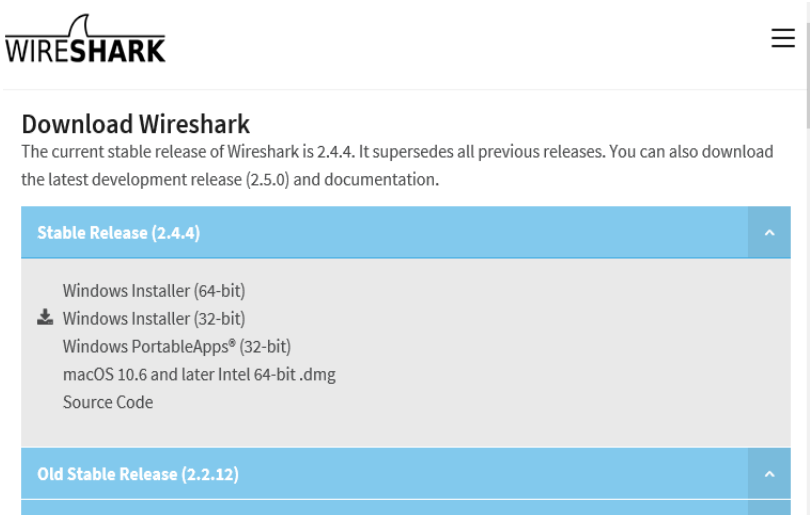


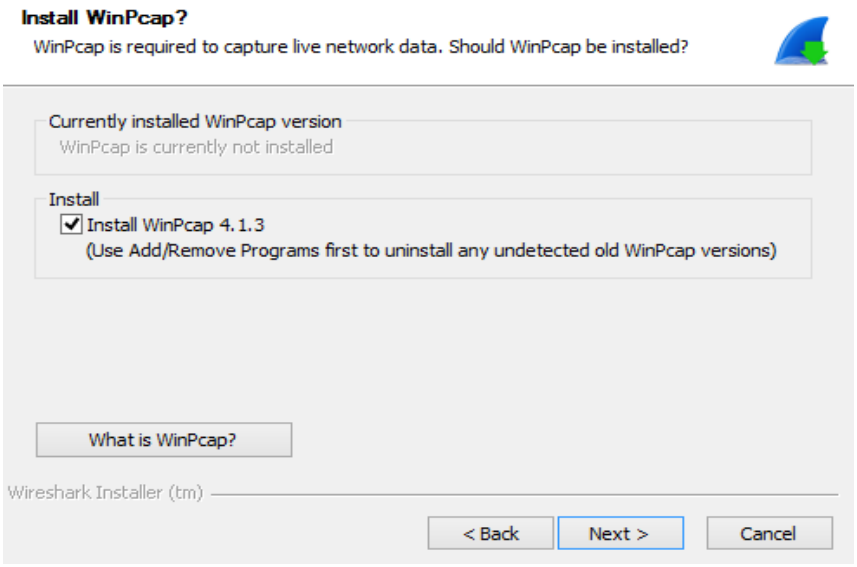
-Follow the steps and install wireshark.

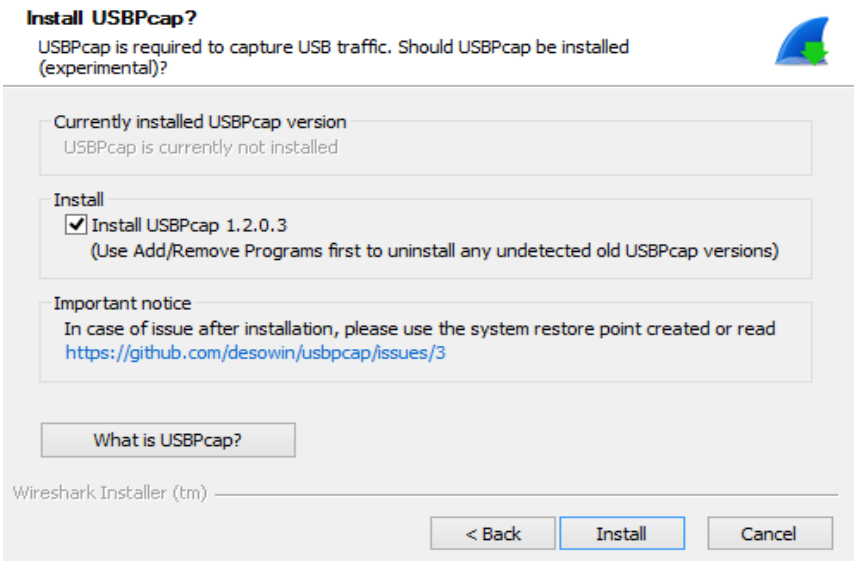

Windows 8.1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
Recycle Bin
hosts
View Downloads - Internet Explorer
View and track your downloads
Search downloads
Name
Wireshark 2.6.4 32-bit Setup
Packet Capture
Wireshark requires either Npcap or WinPcap to capture live network data.
Currently installed Npcap or WinPcap version
Neither of these are installed
Install
Install WinPcap 4.1.3
(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)
Get Npcap
Learn more about Npcap and WinPcap
Wireshark® Installer
Oracle VM VirtualBox Manager
Windows Server 2012 [Running]...
Windows 8.1 [Running] - Oracle...


Windows 8.1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
hosts
Wireshark 2.6.4 64-bit Setup
Installing
Please wait while Wireshark 2.6.4 64-bit is being installed.
Output folder: C:\Program Files\Wireshark
Extract: uninstall.exe
Extract: libwiretap.dll
Extract: libwireshark.dll... 2%
Wireshark® Installer
< Back
Next >
Cancel
1:51 PM

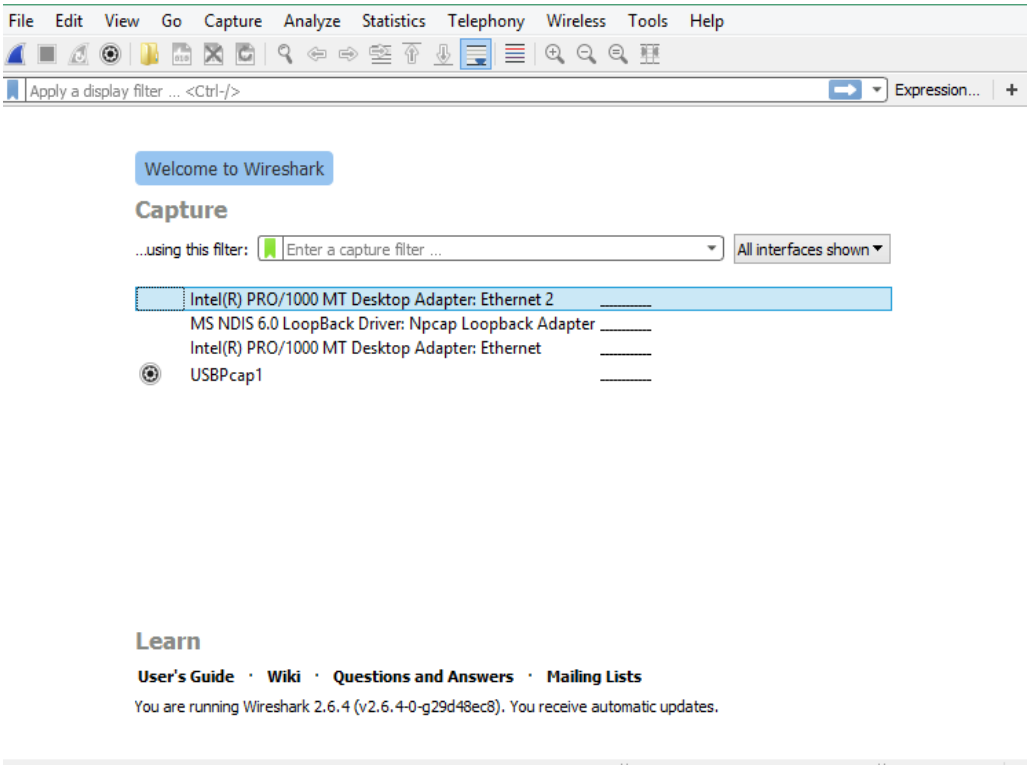

Windows 8.1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
hosts
WinPcap 4.1.3 Setup
WinPcap
License Agreement
Please review the license terms before installing WinPcap 4.1.3.
Press Page Down to see the rest of the agreement.
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.
Nullsoft Install System v2.46
< Back
I Agree
Cancel
1:55 PM
Right


WIRESHARK
Download Wireshark
The current stable release of Wireshark is 2.4.4. It supersedes all previous releases. You can also download the latest development release (2.5.0) and documentation.
Stable Release (2.4.4)
Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS 10.6 and later Intel 64-bit .dmg
Source Code
Old Stable Release (2.2.12)

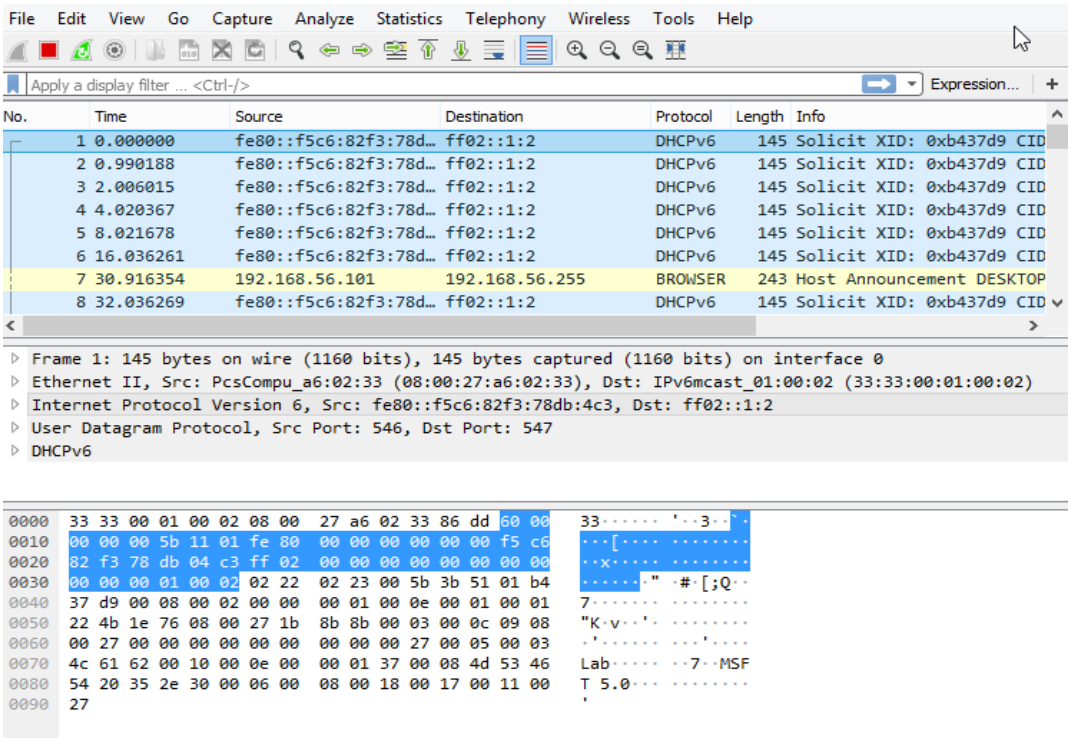




OPENING WIRESHARK 10:17 PM



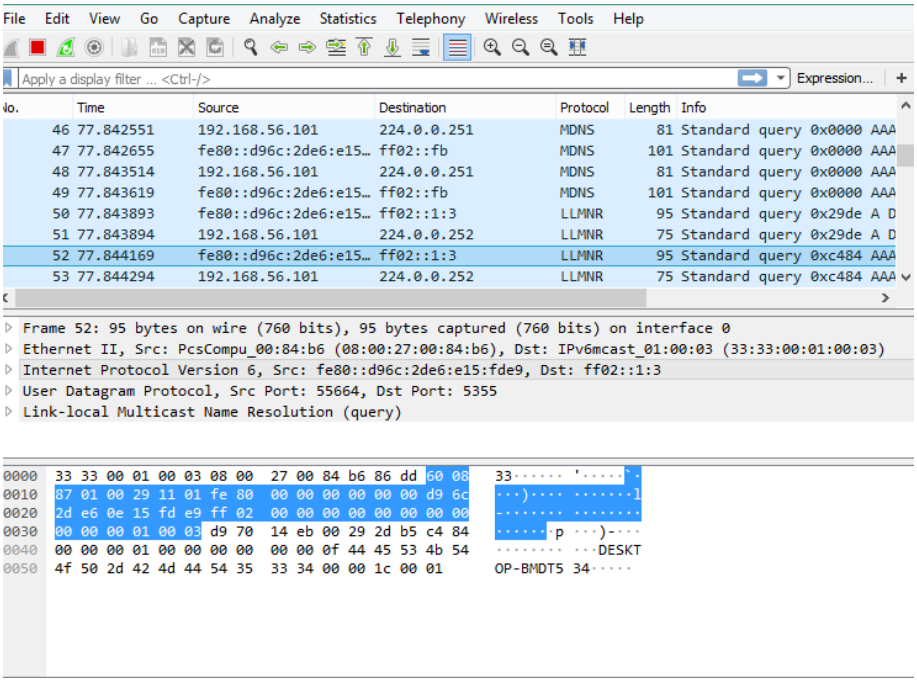
STARTING CONFIGURATION 10:31 PM



PING -6 COMMAND 10:39 PM

```
C:\Users\Administrator>netsh interface ipv6 show address
Interface 3: Ethernet
Addr Type  DAD State    Valid Life Pref. Life Address
---------  -----------  ---------- ---------- ------------------------
Other      Preferred      infinite   infinite fe80::55ae:5bf3:fc25:cc6c%3
Interface 1: Loopback Pseudo-Interface 1
Addr Type  DAD State    Valid Life Pref. Life Address
---------  -----------  ---------- ---------- ------------------------
Other      Preferred      infinite   infinite ::1
Interface 5: isatap.{1D9BBEA2-D02B-4E39-B223-D39D5E2CB302}
Addr Type  DAD State    Valid Life Pref. Life Address
---------  -----------  ---------- ---------- ------------------------
Other      Deprecated     infinite   infinite fe80::5efe:192.168.56.103%5
Interface 8: isatap.{CC6770F5-E342-4F7C-B327-E8C998D1AECD}
Addr Type  DAD State    Valid Life Pref. Life Address
---------  -----------  ---------- ---------- ------------------------
Other      Deprecated     infinite   infinite fe80::5efe:169.254.16.15%8
Interface 6: Ethernet 2
Addr Type  DAD State    Valid Life Pref. Life Address
---------  -----------  ---------- ---------- ------------------------
Other      Preferred      infinite   infinite fe80::f5c6:82f3:78db:4c3%6
Interface 7: Npcap Loopback Adapter
Addr Type  DAD State    Valid Life Pref. Life Address
---------  -----------  ---------- ---------- ------------------------
Other      Preferred      infinite   infinite fe80::ac5f:c0eb:d3b1:100f%7

C:\Users\Administrator>_
```

SESSION CAPTURED IN WIRESHARK 10:46 PM



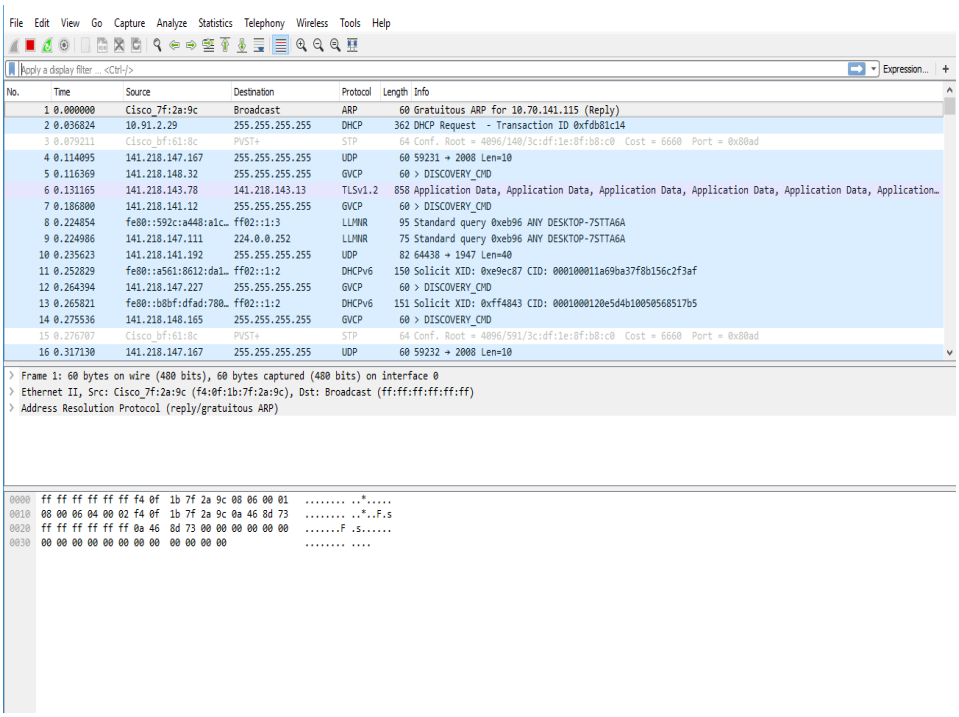
CLEARING THE ARP CASH,TYPE ARP-A 10:51 PM

```
---------  ----------- ---------- ---------- -------------------------
Other      Deprecated    infinite   infinite fe80::5efe:169.254.16.15%8

Interface 6: Ethernet 2

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- -------------------------
Other      Preferred     infinite   infinite fe80::f5c6:82f3:78db:4c3%6

Interface 7: Npcap Loopback Adapter

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- -------------------------
Other      Preferred     infinite   infinite fe80::ac5f:c0eb:d3b1:100f%7


C:\Users\Administrator>arp -a

Interface: 10.0.2.15 --- 0x3
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.103 --- 0x6
  Internet Address      Physical Address      Type
  192.168.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 169.254.16.15 --- 0x7
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>
```

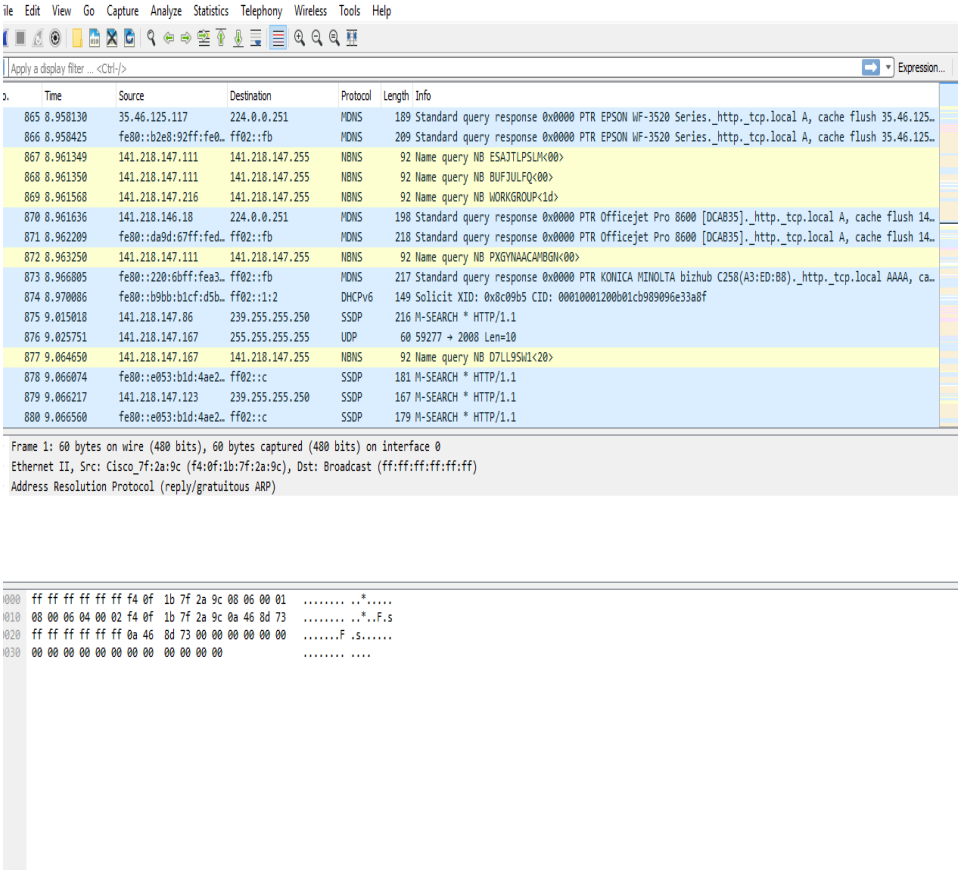
TYPING ARP-P AND ARP-A AGAIN IN COMMAND PROMPT 10:59 PM

```
---------  ----------- ---------- ---------- -------------------------
Other      Deprecated    infinite   infinite fe80::5efe:169.254.16.15%8

Interface 6: Ethernet 2

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- -------------------------
Other      Preferred     infinite   infinite fe80::f5c6:82f3:78db:4c3%6

Interface 7: Npcap Loopback Adapter

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- -------------------------
Other      Preferred     infinite   infinite fe80::ac5f:c0eb:d3b1:100f%7


C:\Users\Administrator>arp -a

Interface: 10.0.2.15 --- 0x3
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.103 --- 0x6
  Internet Address      Physical Address      Type
  192.168.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 169.254.16.15 --- 0x7
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>
```

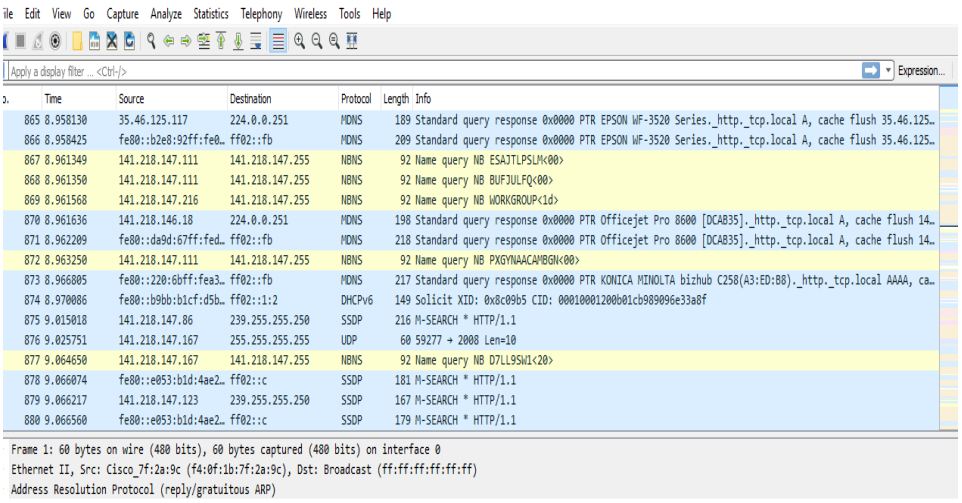
START CAPTURING WIRESHARK SESSION 11:00PM

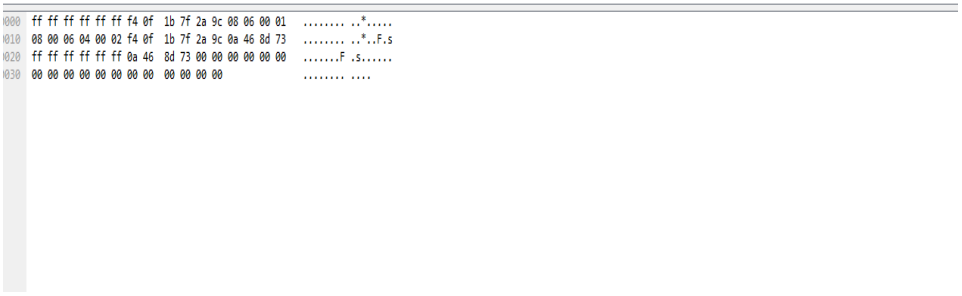


STOP CAPTURING SESSION 11:01 PM



SESSION





PORT CONNECTION STATUS 011: 14 PM

TYPE NETSTAT IN COMMAND PROMPT

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

TYPE NETSTAT-A 06:21 PM

```
C:\Users\Administrator>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49160          0.0.0.0:0              LISTENING
  TCP    169.254.118.237:139    0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:554               [::]:0                 LISTENING
  TCP    [::]:2869              [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:10243             [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  TCP    [::]:49160             [::]:0                 LISTENING
  UDP    0.0.0.0:68             *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:5004           *:*
  UDP    0.0.0.0:5005           *:*
  UDP    0.0.0.0:56866          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:57851        *:*
  UDP    169.254.118.237:137    *:*
  UDP    169.254.118.237:138    *:*
  UDP    169.254.118.237:1900   *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:5004              *:*
  UDP    [::]:5005              *:*
  UDP    [::]:56867             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:57850            *:*
  UDP    [fe80::c8ea:f3ee:6e7c:76ed%3]:1900  *:*

C:\Users\Administrator>_
```

I THINK YOU ARE ASKED TO DO HERE.SO ,IT IS DONE TILL HERE

Best Sampath Talluri.