Adhithya shivanesh- as3423. Karthik Ganeshan- kg426 Ketaki kakade- kk524

CS-696, Fall 2018, 1st Assignment

1. (3.6 points) A company has been assigned a **class B** address. A subnet of this company has network address 148.78.161.0 and direct broadcast address 148.78.167.31. **a)** Based on the previous information, provide the two smallest network addresses that can be assigned to a subnet of this company. **b)** Provide the smallest and largest IP address that can be assigned to a host of each subnets of question "a)". **c)** Provide the two largest network address that can be assigned to a subnet of this company. **d)** Provide the smallest and largest IP address that can be assigned to a host of each subnet of previous question "c)". **You must provide** the values of all derived **network addresses** and **IP addresses** in **Dotted Decimal Notation. You must show your derivations.**

Net Address: **148.78.1010 0001.0000 0000**

Broadcast Address: **148.78.1010 0111.0001 1111**

AND: **148.78.1010 0001.00000000**

Red bits are host bits, as they are 0 in the net address and 1 in the broadcast address. The bits in black are net bits.

Smallest Net addresses:

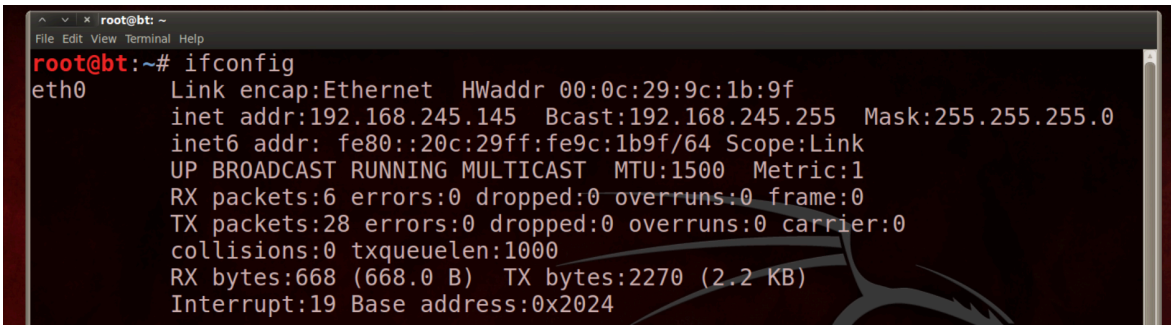
NNNN NHHN NNNH HHHH		IP addresses assigned to hosts:		
148.78.0000 0000. 0000 0000	148.78.0.0	Smallest IP	148.78.0000 0000.0000 0001	148.78.0.1
		Largest IP	148.78.0000 0110.0001 1110	148.78.6.30
148.78.0000 0000. 0010 0000	148.78.0.32	Smallest IP	148.78.0000 0000.0010 0001	148.78.0.33
		Largest IP	148.78.0000 0110.0011 1110	148.78.6.62

Largest Net addresses:

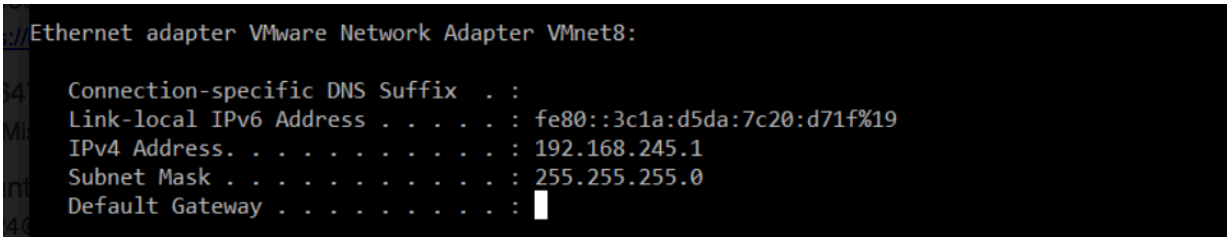
148.78.1111 1001.1100 0000	148.78.249.192	Smallest IP	148.78.1111 1001.1100 0001	148.78.249.193
		Largest IP	148.78.1111 1111.1101 1110	148.78.255.222
148.78.1111 1001.1110 0000	148.78.249.224	Smallest IP	148.78.1111 1001.1110 0001	148.78.249.225

2. (4 points) Start your **Bt5, Kali** (or other Linux virtual machine) that has **hping3** tool installed. Now use **ifconfig** to find its IP address; to find the IP address of your **host OS** you can also use **ifconfig** (if it is Linux) or **ipconfig** (if it is Windows). **Capture** screenshots of your **ifconfig** (or **ipconfig**) commands and corresponding outputs; showing the two IP addresses. Now start ***Wireshark*** in both **Bt5** and **host OS** and select **non-promiscuous** mode. In both **Bt5** and **host OS Wireshark** add a **SrcPort** and a **DestPort** column in the **Packet List Pane**. In the ***Wireshark*** of the **host OS**, apply a **capture** filter that will capture **only** the **TCP packets** whose **source port** is **40** and its **source IP address** is the one of ***Bt5.*** **Type** this capture filter. Also **capture** a screenshot of this filter in the Wireshark filter box of the **host OS**. In the ***Wireshark*** of ***Bt5*** apply a packet **capture** filter that will **capture** only TCP packets that have **ALL** of the following properties: **a)** source port **40**, **b)** destination port **82**, **c)** TCP **ECN, URG, PSH, RST** bits set
to 1, **d) 1380** TCP data bytes **e) IP Identification** field **7746, f)** a **TCP window** size of **48000**. **Type** this capture filter. Also **capture** a screenshot of this applied filter in the Wireshark filter box of the **Bt5.** Now start the packet capturing process in both **host OS** and **Bt5 Wiresharks**. Next, use (in **Bt5) one hping3** command that will transmit **8 TCP packets** to the **Host OS** with source port 40 and destination ports **78,79,80,81,82,83,84** and **85**. **Moreover,** each one of these packets **must** have the **ECN, URG, PSH,** and **RST** bits set to 1, its **IP Identification field** equal to **7746**, **1380** TCP data bytes and a **TCP window of 48000**. **Type** the **hping3** command you have used. Also **capture** a screenshot of this **hping3** command and its output. Stop the packet capturing process in both ***Wiresharks***. **Capture a screenshot** of the **packet list pane** of the **Bt5 Wireshark** and **a screenshot** of the **packet list pane** of the **Host OS Wireshark** showing the captured packets. Your screenshots in **Bt5** and **Host OS must show** the **port numbers** of the transmitted packets. How many packets have been captured by **Bt5 Wireshark** and how many by the **Host OS Wireshark**? Is that what you expected? **Explain** why or why not.

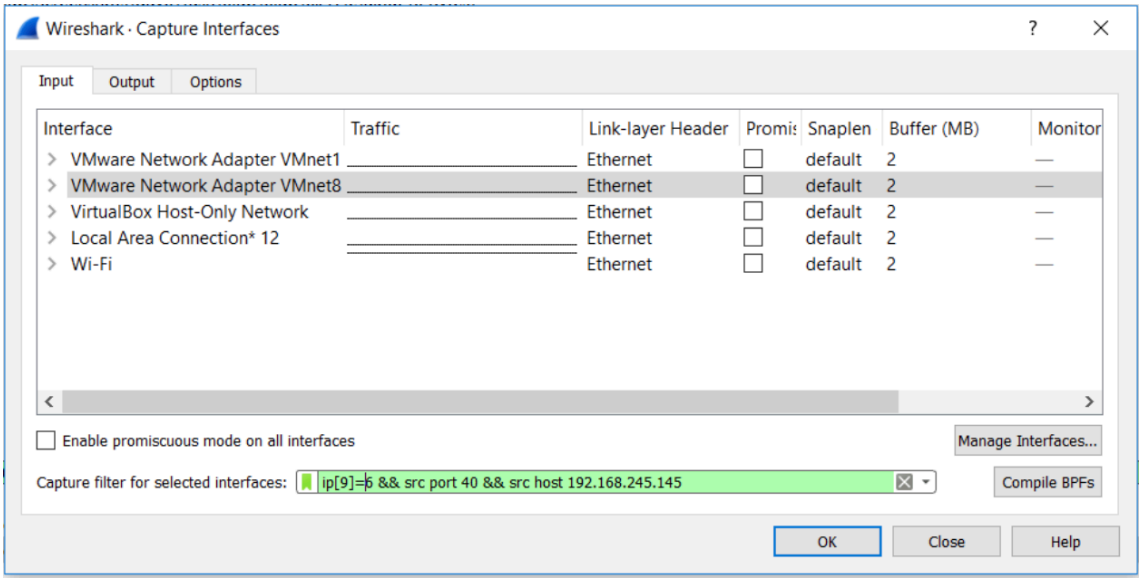
Screenshot-2-1: Bt5 ifconfig command and its output; Bt5 IP address is **192.168.245.145.**



Screenshot-2-2: Windows (host OS) ifconfig command and its output; Windows IP address is **192.168.183.1**

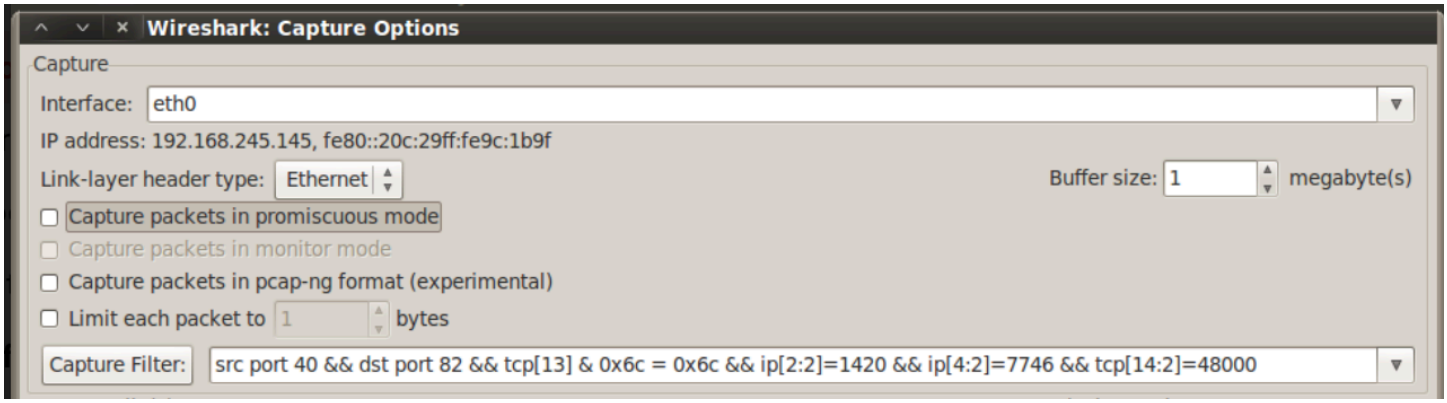


Screenshot-2-3: Wireshark capture filter in Windows: ip[9]=6 && src port 40 &&src host 192.168.245.145

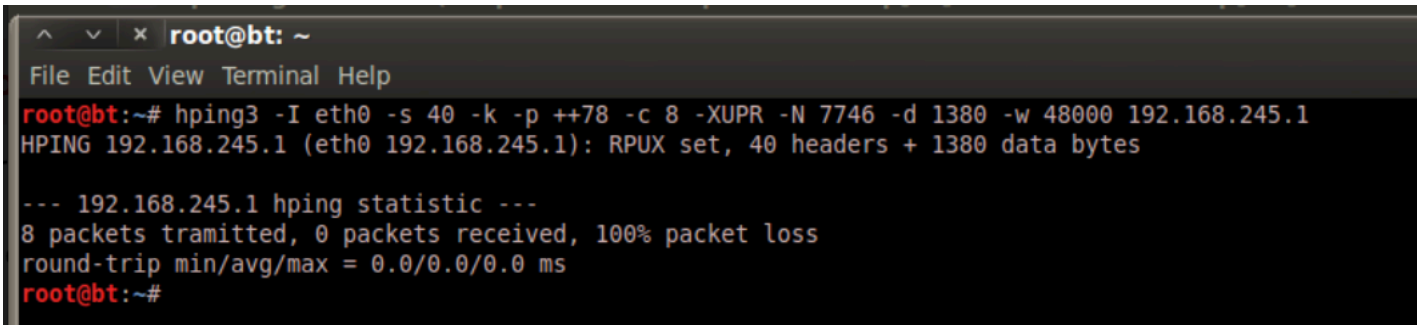


Bt5 Wireshark Capture Filter components:
A) Source port 40: src port 40
B) Destination port 82: dst port 82
C) TCP ECN, URG, PSH, RST bits set: tcp[13] & 0x6c = 0x6c
D) 1380 TCP data bytes: adding 20 bytes TCP Header and 20 bytes IP Header: 1420
ip[2:2]=1420
E) IP Identification field 7746: ip[4:2]=7746
F) a TCP window size of 48000: tcp[14:2]=48000
Complete filter:
src port 40 && dst port 82 && tcp[13] & 0x6c = 0x6c && ip[2:2]=1420 && ip[4:2]=7746 && tcp[14:2]=48000

Screenshot-2-4: Shows a) eth0 is used in Bt5 with IP 192.168.245.145 b) Capture Filter used



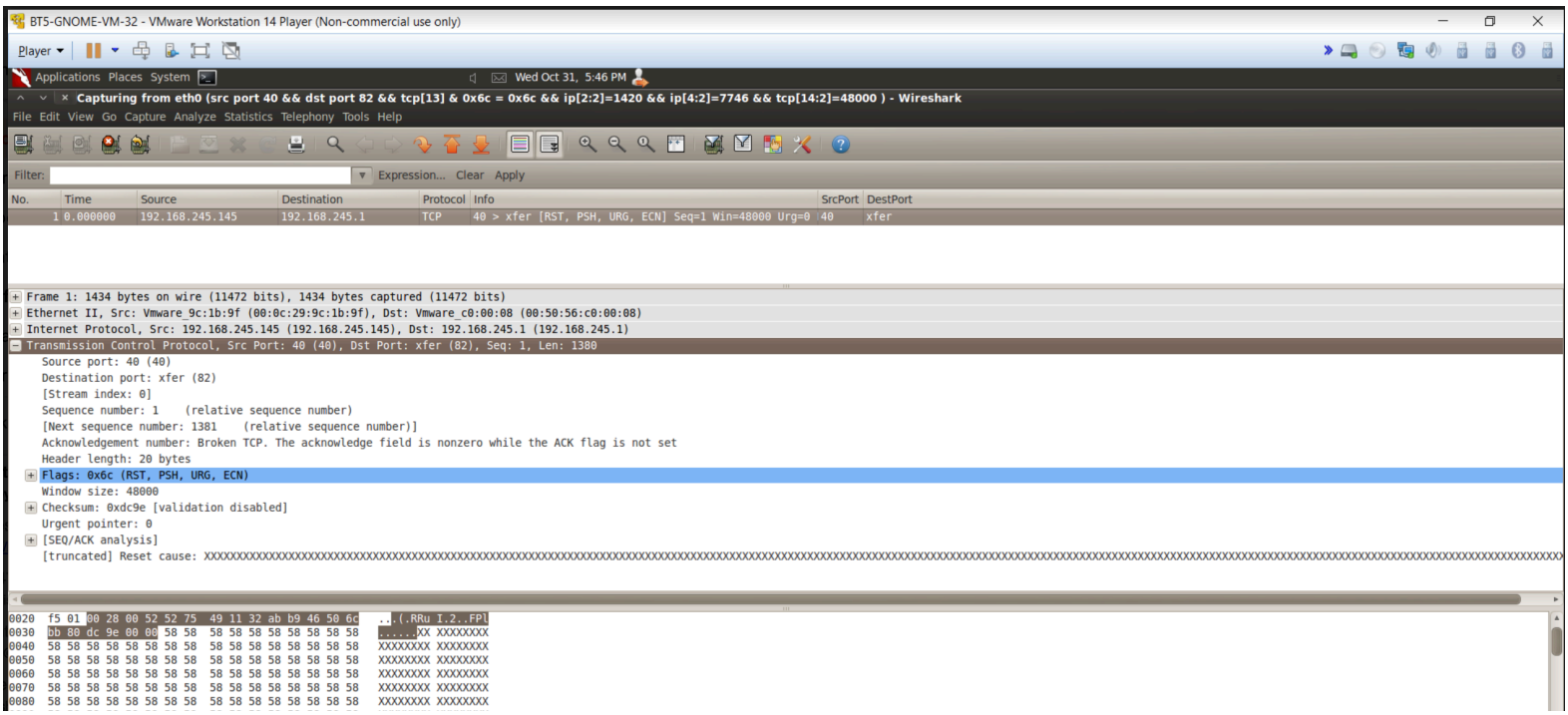
Screenshot-2-5: Shows hping3 command and its output; 8 packets have been transmitted



```
root@bt:~# hping3 -I eth0 -s 40 -k -p ++78 -c 8 -XUPR -N 7746 -d 1380 -w 48000 192.168.245.1
HPING 192.168.245.1 (eth0 192.168.245.1): RPUX set, 40 headers + 1380 data bytes

--- 192.168.245.1 hping statistic ---
8 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@bt:~#
```

Screenshot-2-6: Shows that in Bt5 only packet with src port 40 dest port number 82 has been captured.



```
Capturing from eth0 (src port 40 && dst port 82 && tcp[13] & 0x6c = 0x6c && ip[2:2]=1420 && ip[4:2]=7746 && tcp[14:2]=48000 ) - Wireshark
```

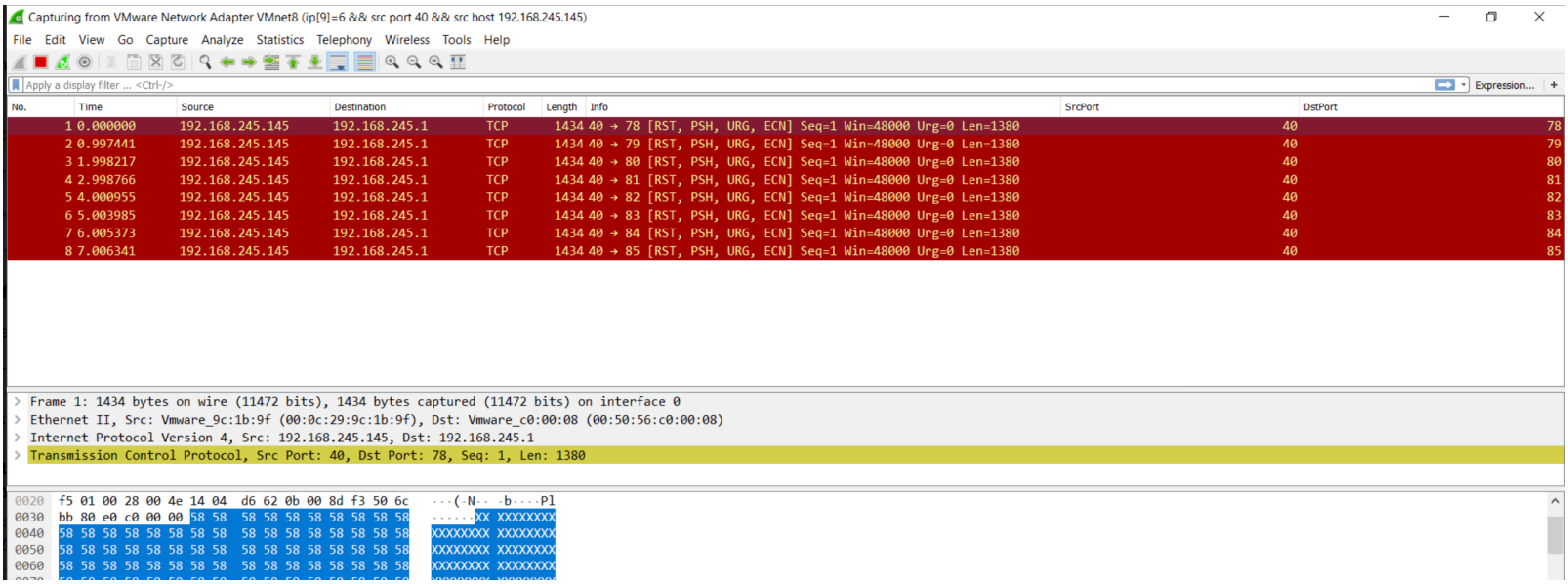
No.	Time	Source	Destination	Protocol	Info	SrcPort	DestPort
1	0.000000	192.168.245.145	192.168.245.1	TCP	40 > xfer [RST, PSH, URG, ECN] Seq=1 Win=48000 Urg=0	40	xfer

```
+ Frame 1: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits)
+ Ethernet II, Src: Vmware_9c:1b:9f (00:0c:29:9c:1b:9f), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
+ Internet Protocol, Src: 192.168.245.145 (192.168.245.145), Dst: 192.168.245.1 (192.168.245.1)
- Transmission Control Protocol, Src Port: 40 (40), Dst Port: xfer (82), Seq: 1, Len: 1380
    Source port: 40 (40)
    Destination port: xfer (82)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1381    (relative sequence number)]
    Acknowledgement number: Broken TCP. The acknowledge field is nonzero while the ACK flag is not set
    Header length: 20 bytes
  + Flags: 0x6c (RST, PSH, URG, ECN)
    Window size: 48000
  + Checksum: 0xdc9e [validation disabled]
    Urgent pointer: 0
  + [SEQ/ACK analysis]
    [truncated] Reset cause: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

0020  f5 01 00 28 00 52 52 75  49 11 32 ab b9 46 50 6c   ...(.RRu I.2..FPl
0030  bb 80 dc 9e 00 00 58 58  58 58 58 58 58 58 58 58   ......XX XXXXXXXX
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0060  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0070  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0080  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
```

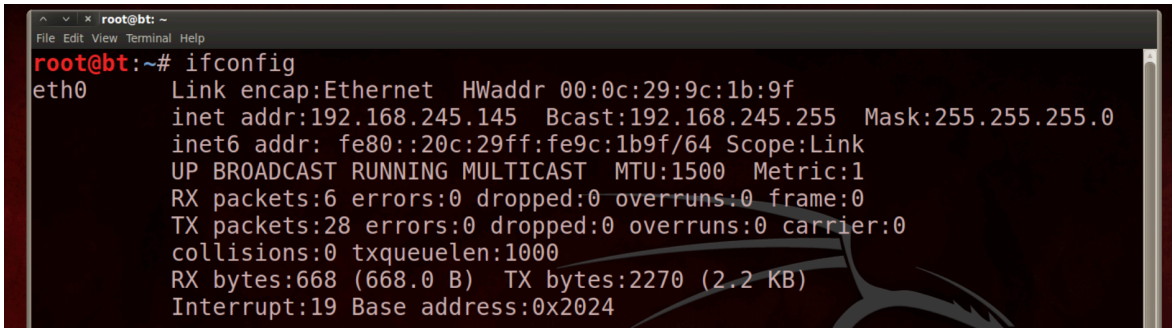
In screenshot 2-6, we can see that we have captured only one packet on our Bt5 even though we sent multiple packets (8 packets) using hping3 command . This is because we have a capture filter which will only capture the packet with source port as 40 and destination port as 82 i.e only one packet with these specifications. While on the windows machine we have a capture filter which is suppose to capture 8 packets with port number from 78 to 85. Hence we expect the host OS to capture 8 packets and the Bt5 machine to capture only one packet with given details.

Screenshot-2-7: Shows that in host OS all 8 packets (ports 78,79….85) have been captured.

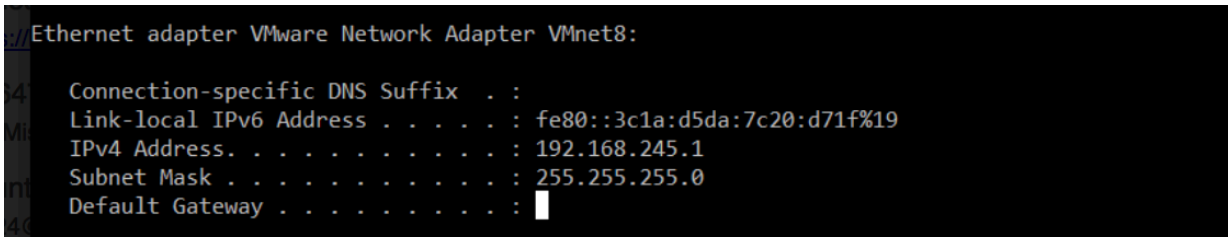


3. (2.4 points) Start your **Bt5 (or Kali)** and **host OS** system and use **ifconfig** or **ipconfig** to find their IP addresses. **Capture** screenshots of your **ifconfig** (or **ipconfig**) commands and corresponding outputs; showing the IP addresses of **Bt5** and **host OS**. In your **Bt5**, type the **hping3** command that will transmit to the **host OS one** TCP packet that has only its **SYN, PSH,** and **ACK** bits set to 1 (and all other TCP flags set to 0), **52000** TCP data bytes and a destination port number **1234**. **Type** the **hping3** command you must use. In your **Bt5**, also apply a **capture** filter that will only capture the **17th**, **28th** and **32nd** fragments of the transmitted packet. **Type** the **capture** filter that you must use. Also **capture** a screenshot of this filter in the Wireshark filter box of **Bt5.** In the **host OS** start **Wireshark** and apply a **capture** filter that will **only capture TCP packets** with source IP address, the IP address of **Bt5**. **Capture** a screenshot of this filter. Now start **both** Wiresharks in **Bt5** and **host OS** and, then, run the above **hping3** command. **Capture** a screenshot of the **hping3** command and its output. **Capture** a screenshot of the packet list pane of the **host OS Wireshark** showing in the packet list pane all fragments. **Finally**, **capture** a screenshot of the **Bt5 Wireshark** showing in the packet list pane the captured **17th**, **28th** and **32nd** fragments, and in the **packet detailed pane** the fragmentation offset of the **32nd fragment**.

Screenshot-3-1: Bt5 ifconfig command and its output; Bt5 IP address is 192.168.245.145

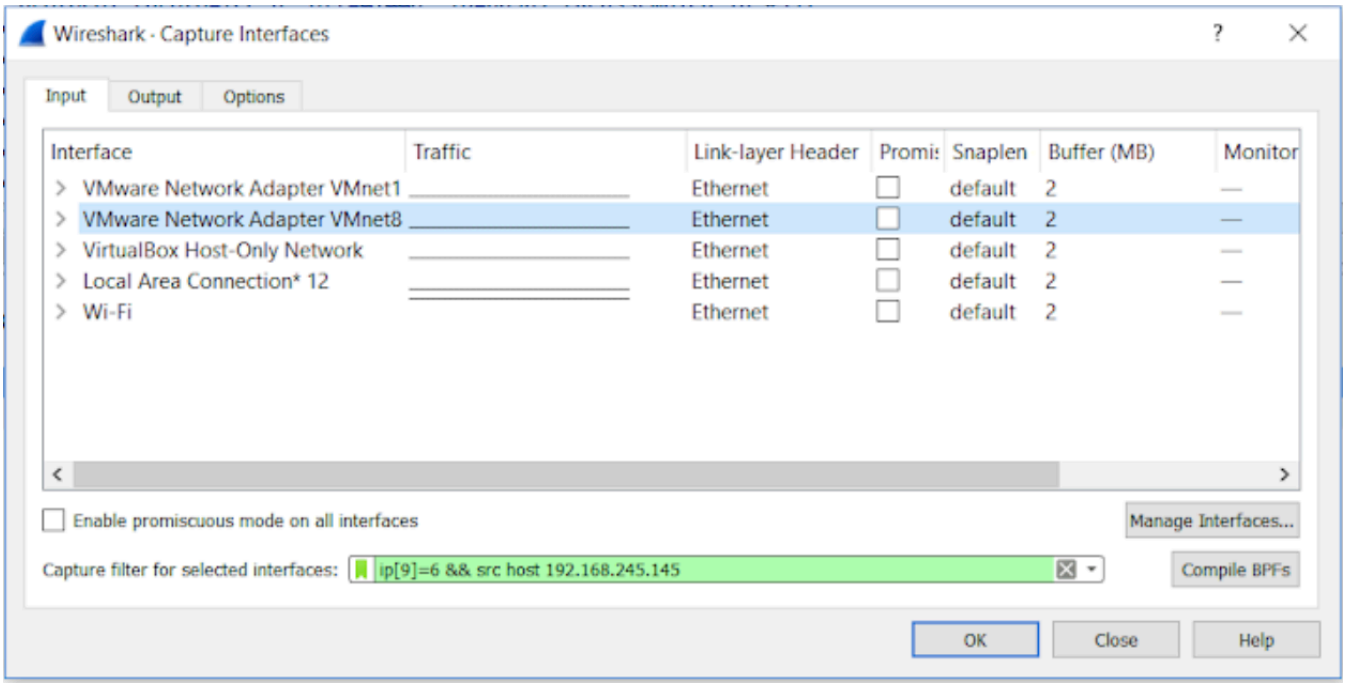


Screenshot-3-2: Host OS ifconfig command and its output; Windows IP address is 192.168.245.1

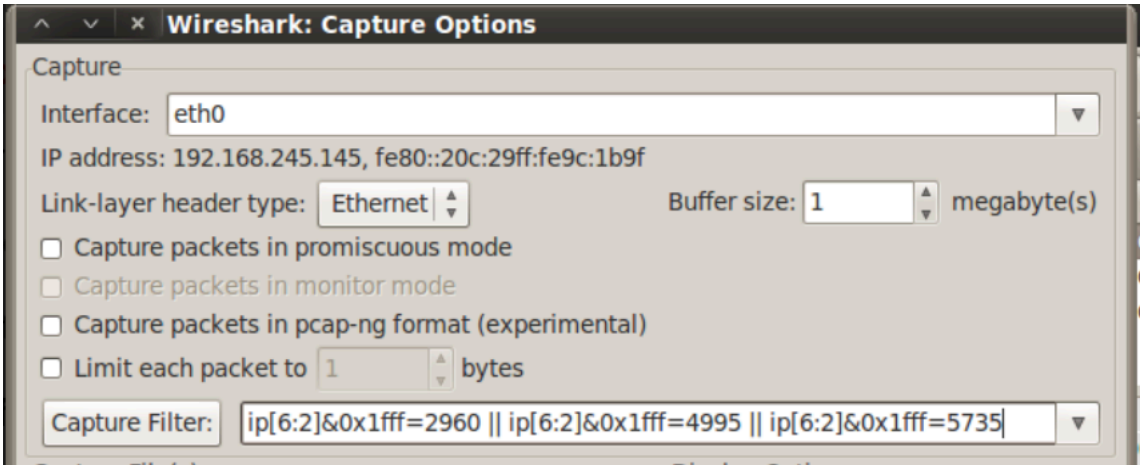


Hping command: hping3 -I eth1 -p 1234 c 1 -SPA -d 52000 192.168.245.1
In Bt5 we have to apply a filter that will capture the 17th , 28th and 32nd fragments.
Since there are no IP options the IP fragment size will be 1500-20 = 1480 bytes. So, the offsets will be: OF1 =0, OF2 = 1480/8 = 185, OF3 = 185*2 = 370…. Similarly, OF17=16*185=2960, OF28=185*27=4995, OF32=31*185=5735
So, the filter will be: ip[6:2]&0x1fff=2960 || ip[6:2]&0x1fff=4995 || ip[6:2]&0x1fff=5735
The capture filter on host would be ip[9]=6 and src host 192.168.245.145

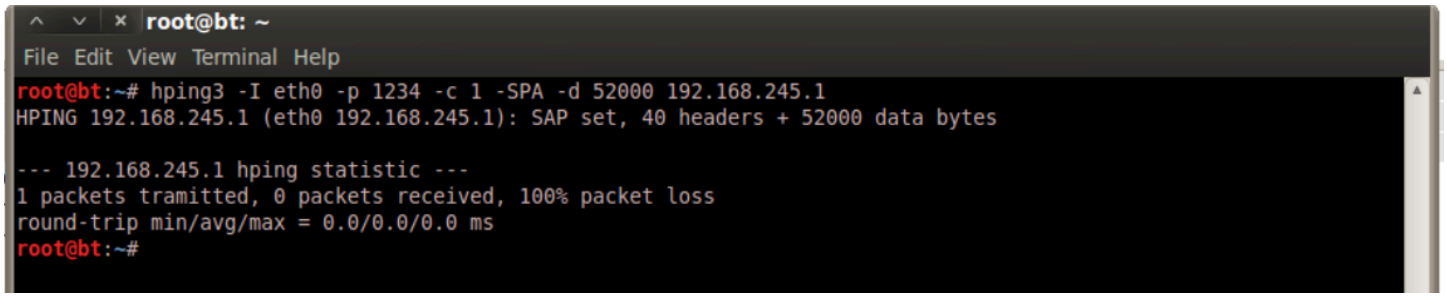
Screenshot-3-3: Wireshark capture filter in Windows: ip[9]=6 and src host 192.168.245.145



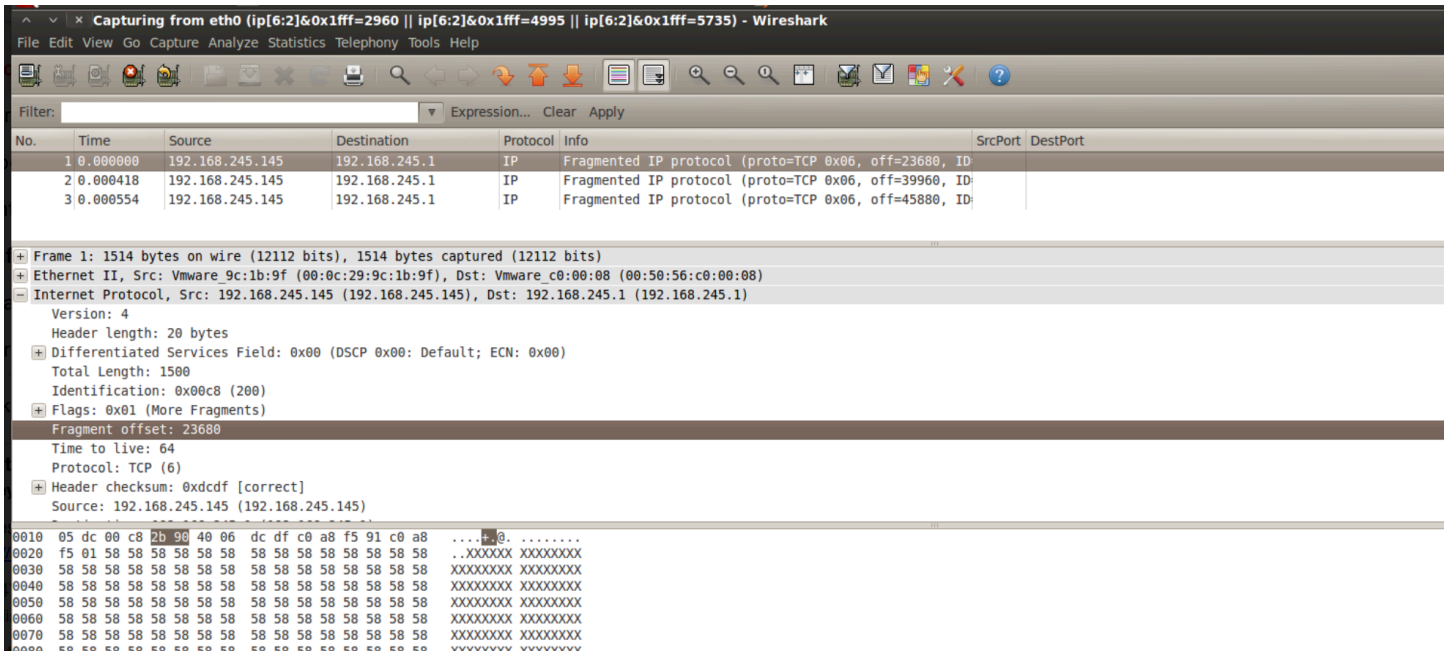
Screenshot-3-4: Bt5 capture filter: ip[6:2]&0x1fff=2960 || ip[6:2]&0x1fff=4995 || ip[6:2]&0x1fff=5735



Screenshot-3-5: Bt5 hping3 command and its output



Screenshot-3-6: Shows the 2 fragments captured by Bt5 with offsets: 23680, 39960 and 45880
23680/8 = 2960 and 2960/185=16, hence it is the 17th fragment
39960/8= 4995 and 4995/185=27, hence it is the 28th fragment
45880/8=5735 and 5735/185=31, hence it is the 32nd fragment.



Screenshot-3-7: Shows all the fragments captured by the MAC Wireshark with their corresponding fragmentation offset values.