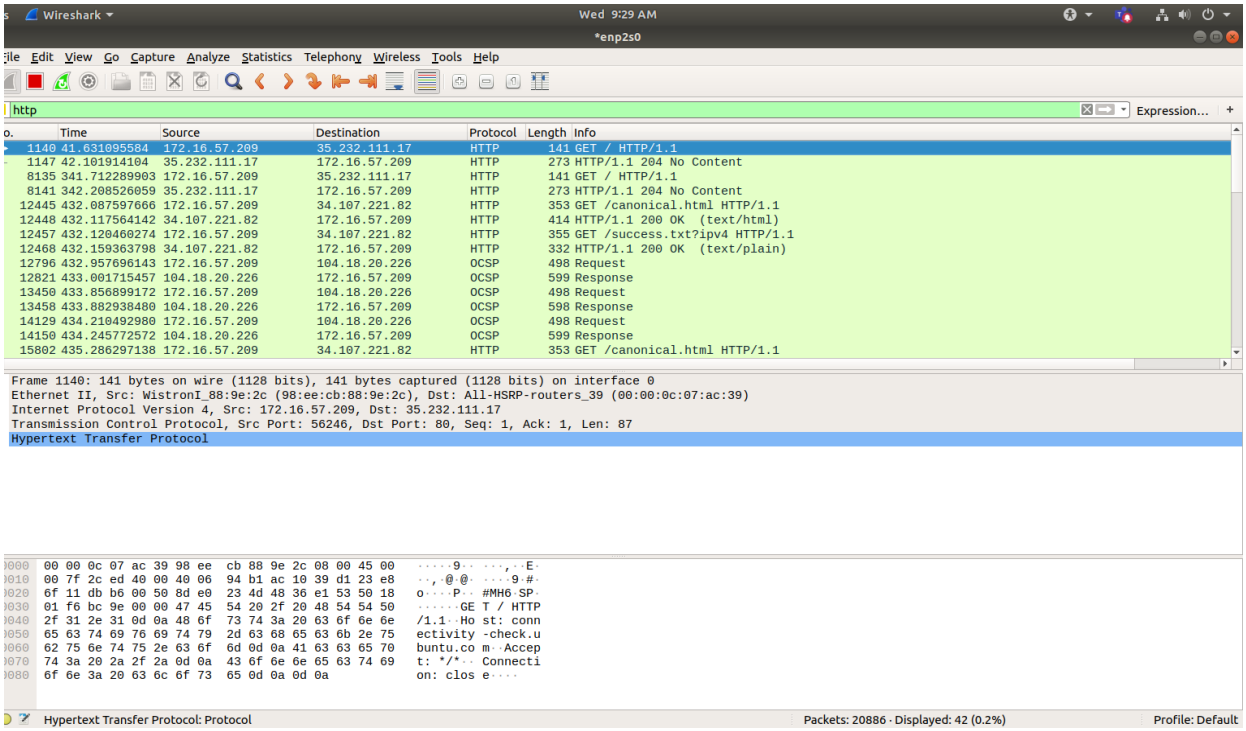
SEC : A | CN LAB: 03 | BATCH : A3

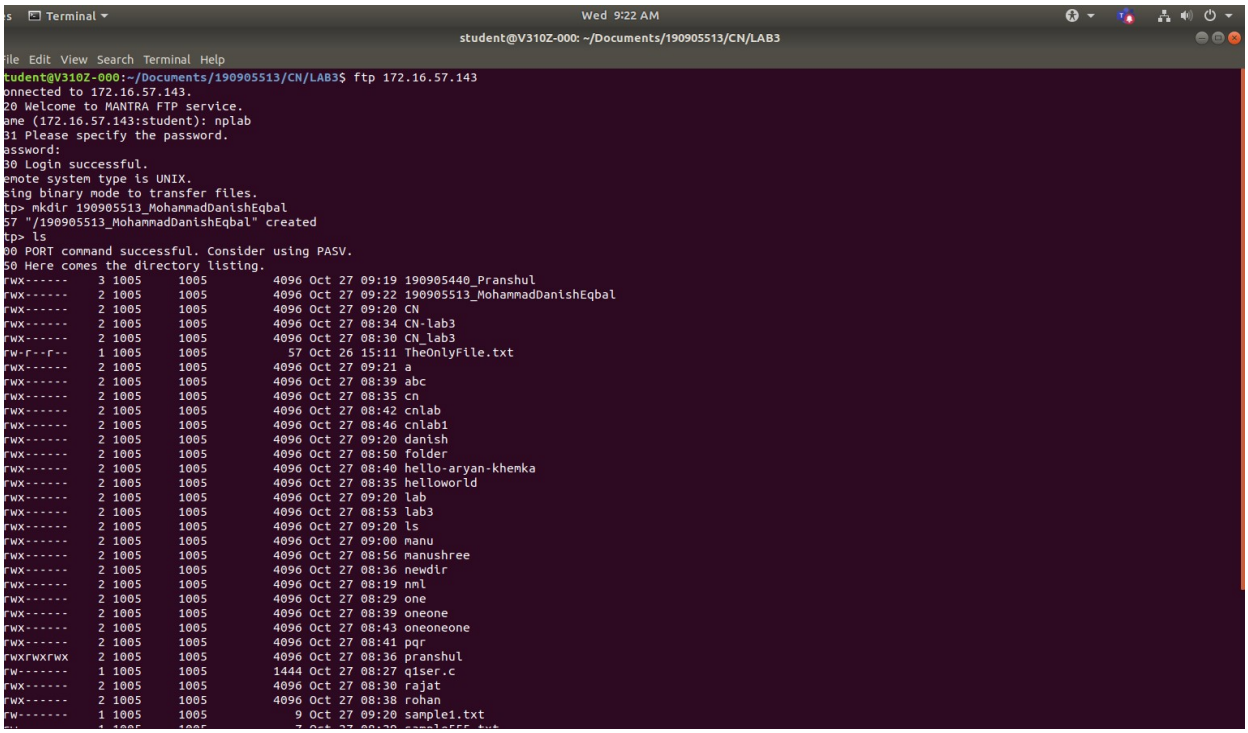
REG: 190905513 | CSE 3113 | NAME: MOHAMMAD DANISH EQBAL

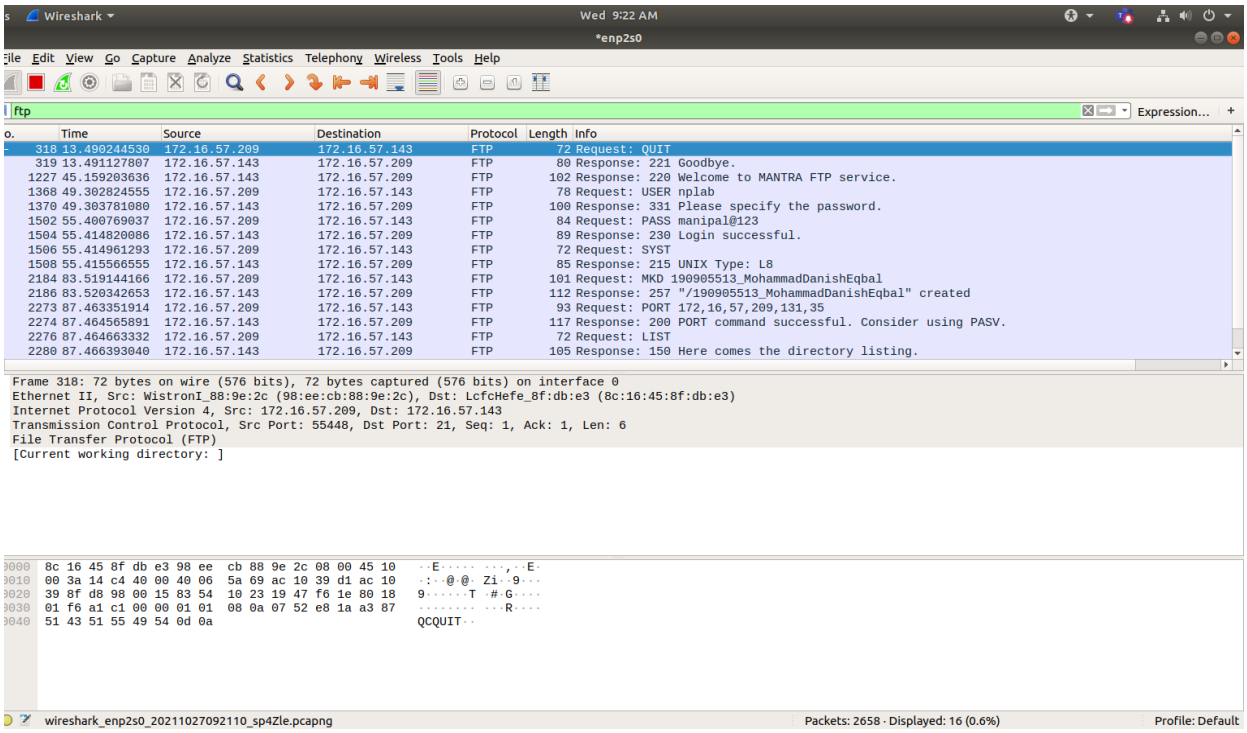
PART-1 STUDY OF APPLICATION LAYER PROTOCOLS USING WIRESHARK.

Q 3.1. Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about most common HTTP messages. Also capture response messages and analyze them. During the lab session, also examine and analyze some HTTP headers.

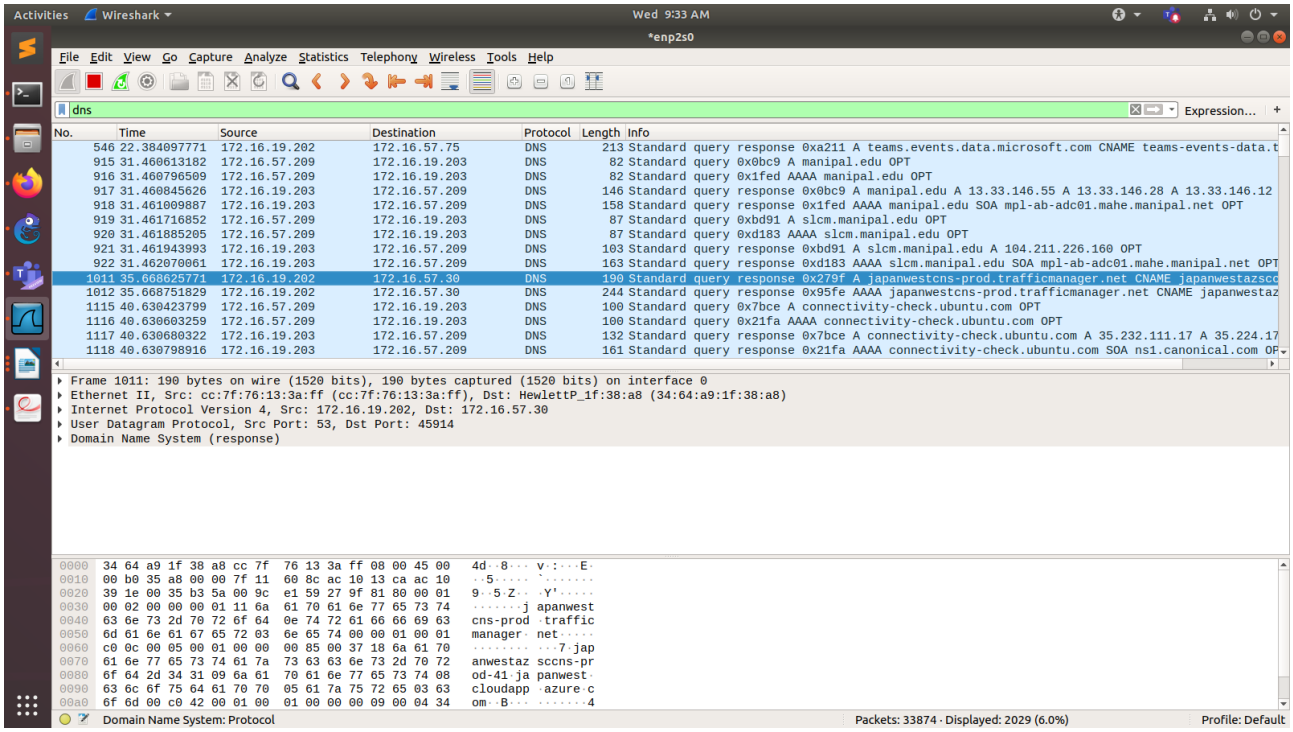


Q 3.2 Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.





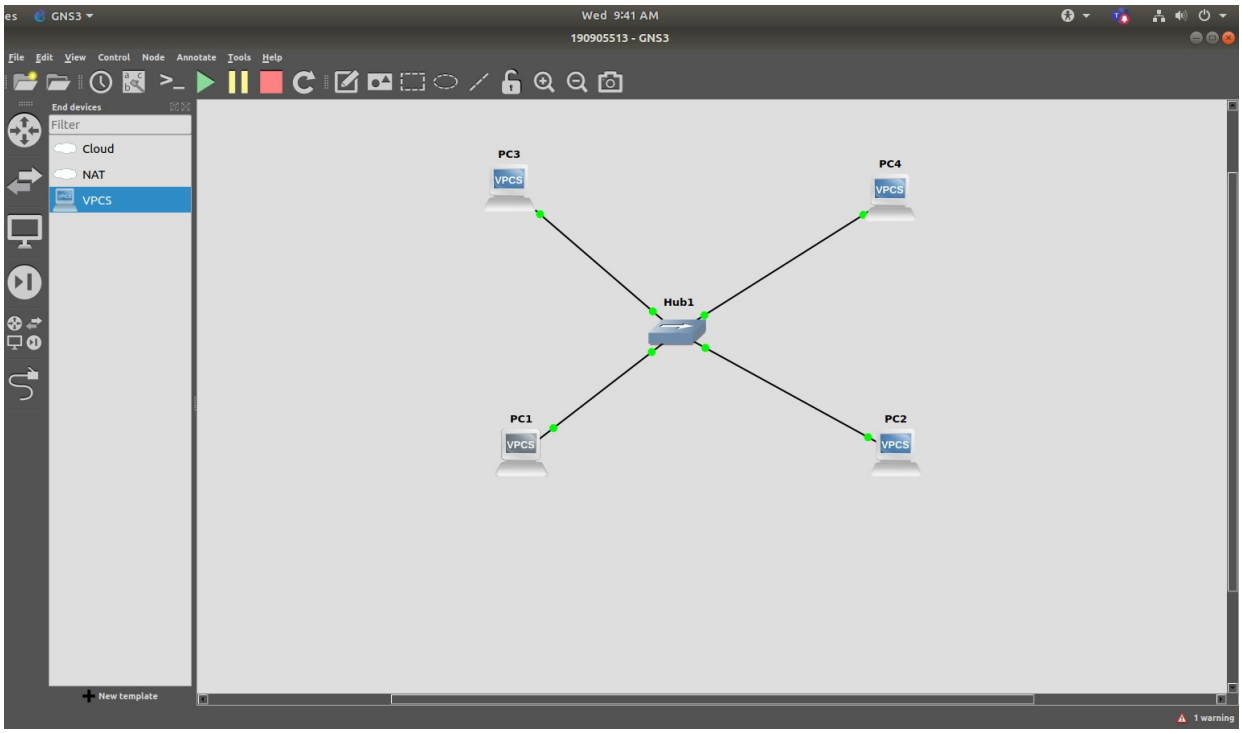
Q 3.3 Analyze the behavior of the DNS protocol. In addition to Wireshark [Several network utilities are available for finding some information stored in the DNS servers. Eg.dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.]

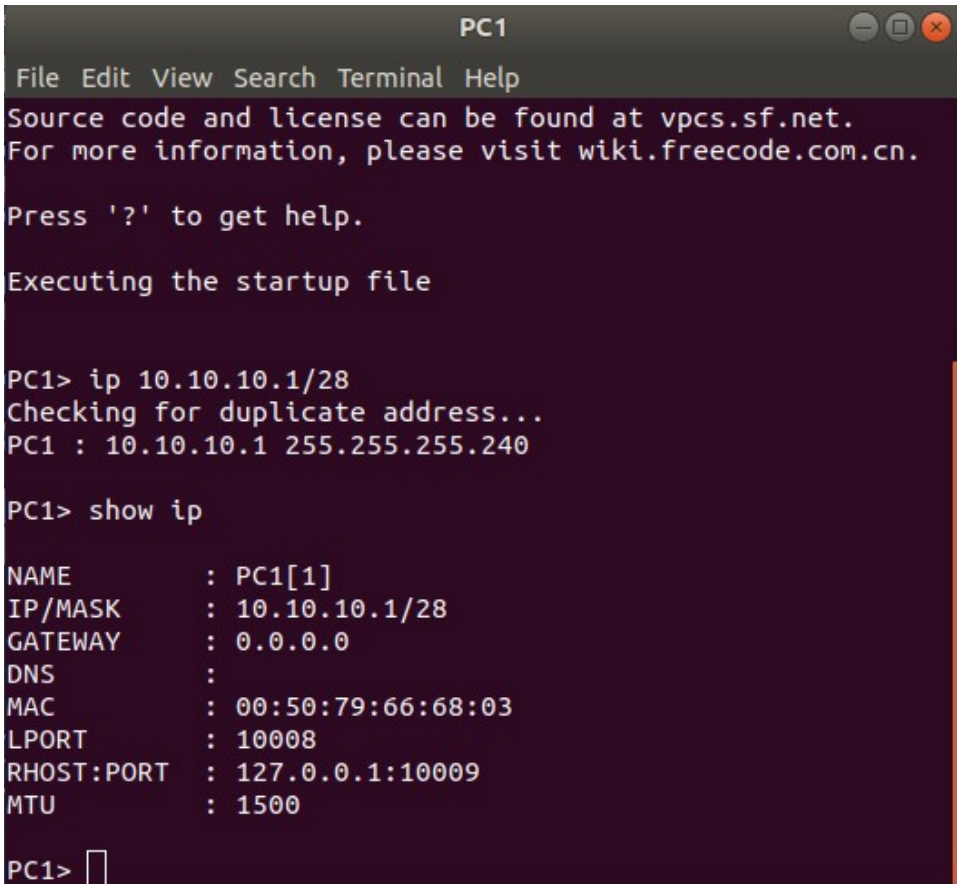


PART-2 STUDY OF NETWORK DEVICES IN GNS3

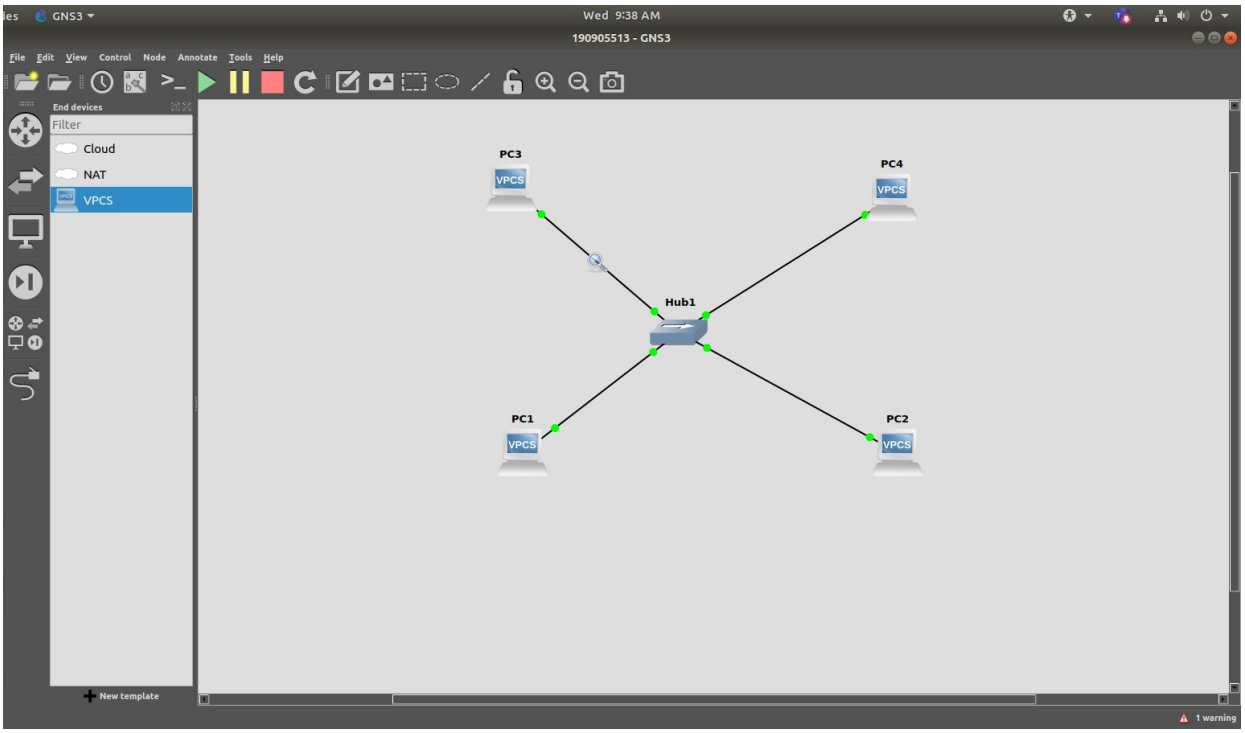
Q 4.1 (a,b,c,d,e) and Q 4.3

Design network configuration shown in Figure 4.1 for all parts. Connect all four VMs to a single Ethernet segment via a single hub as shown in Figure 4.1. Configure the IP addresses for the PCs as shown in Table 4.1.

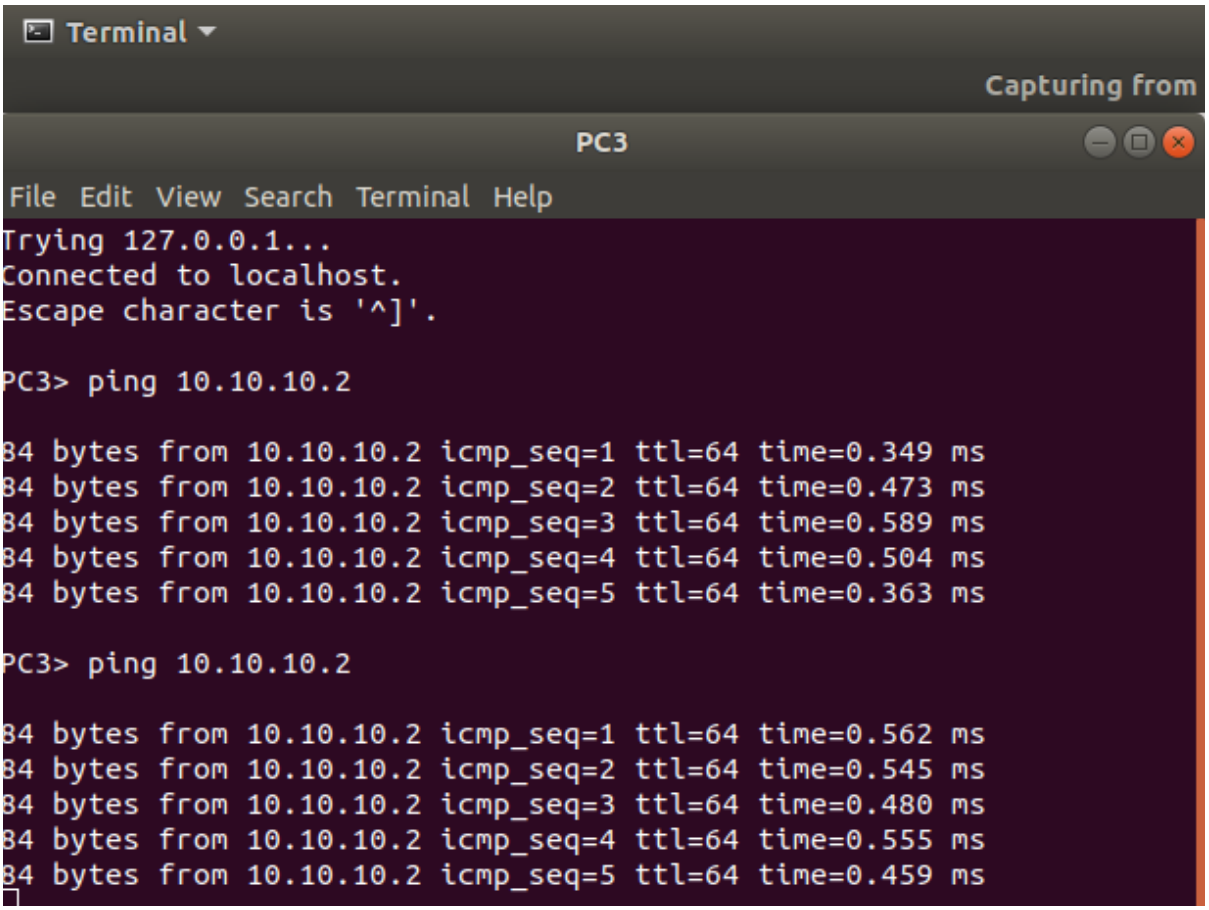


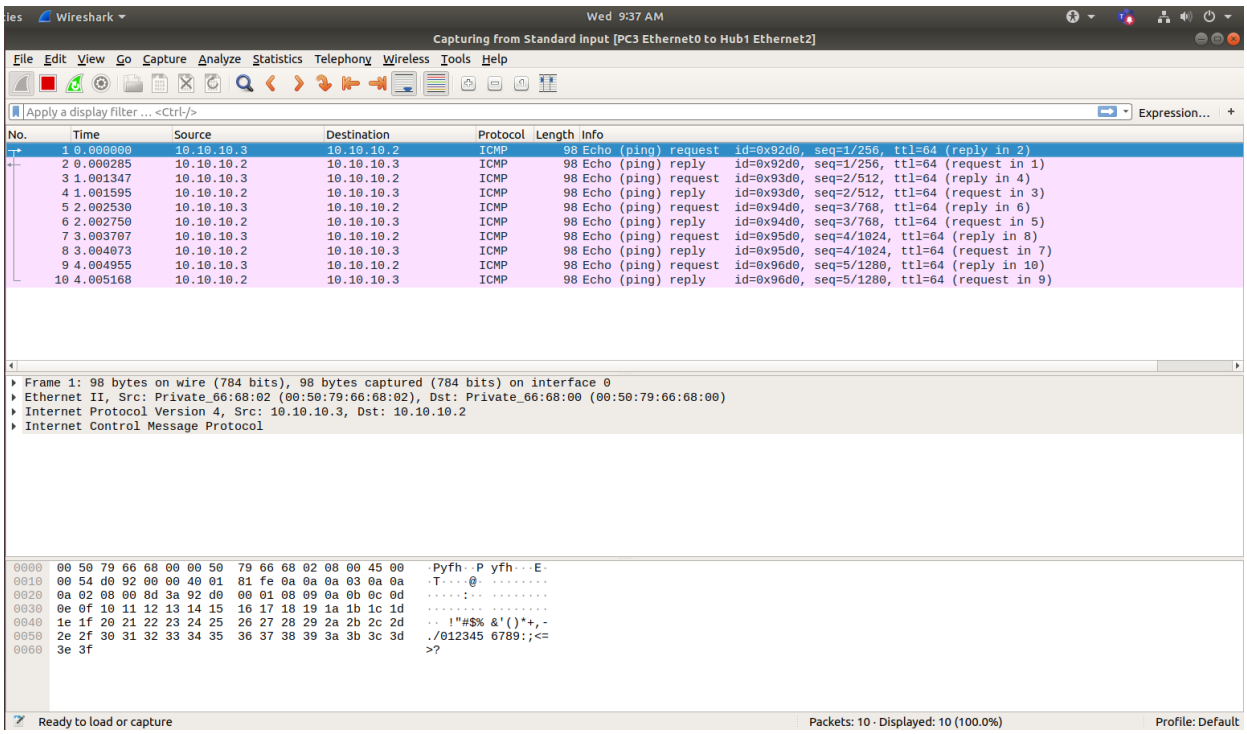


b. Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address ofPC2.

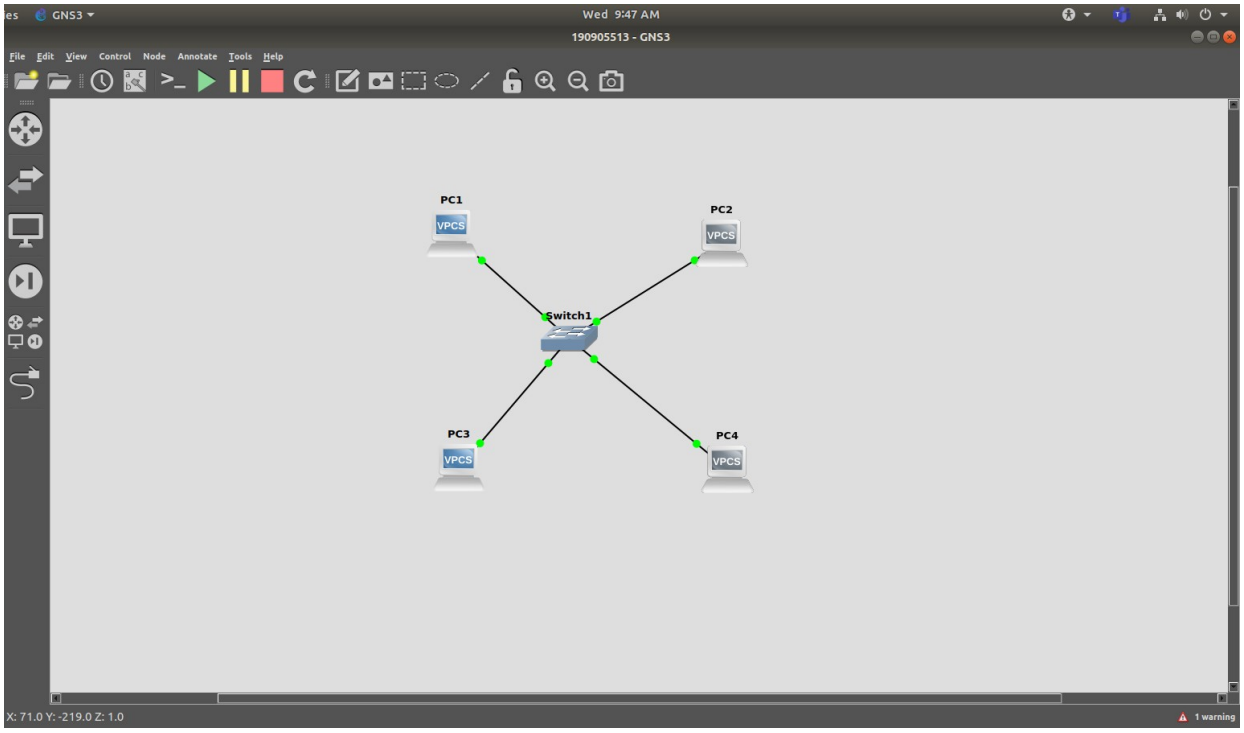


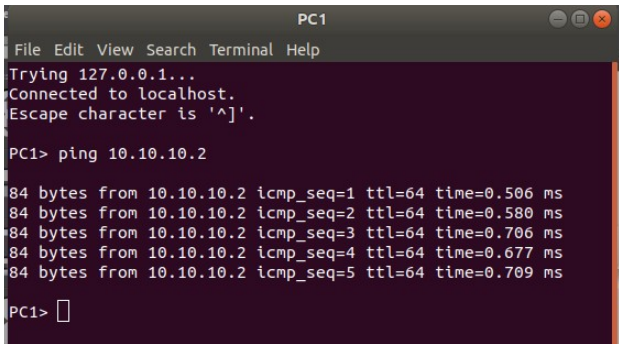
c. Issue a ping command from PC1toPC2:

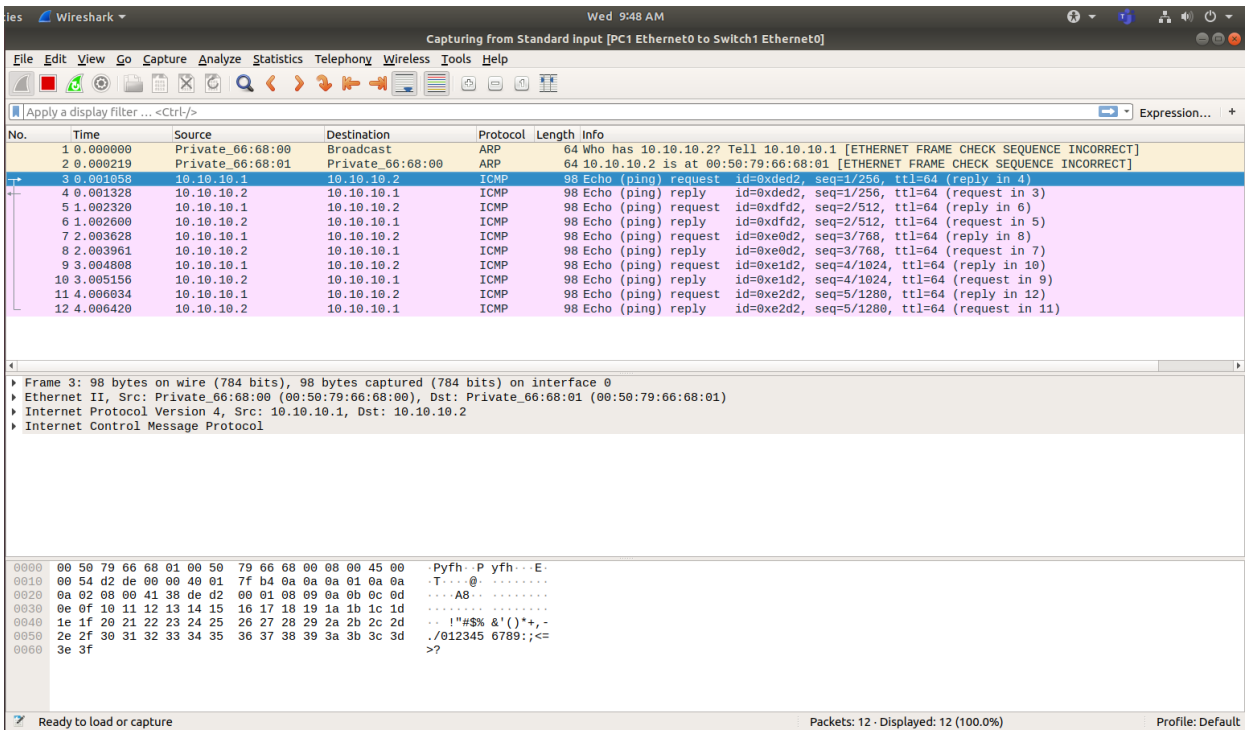




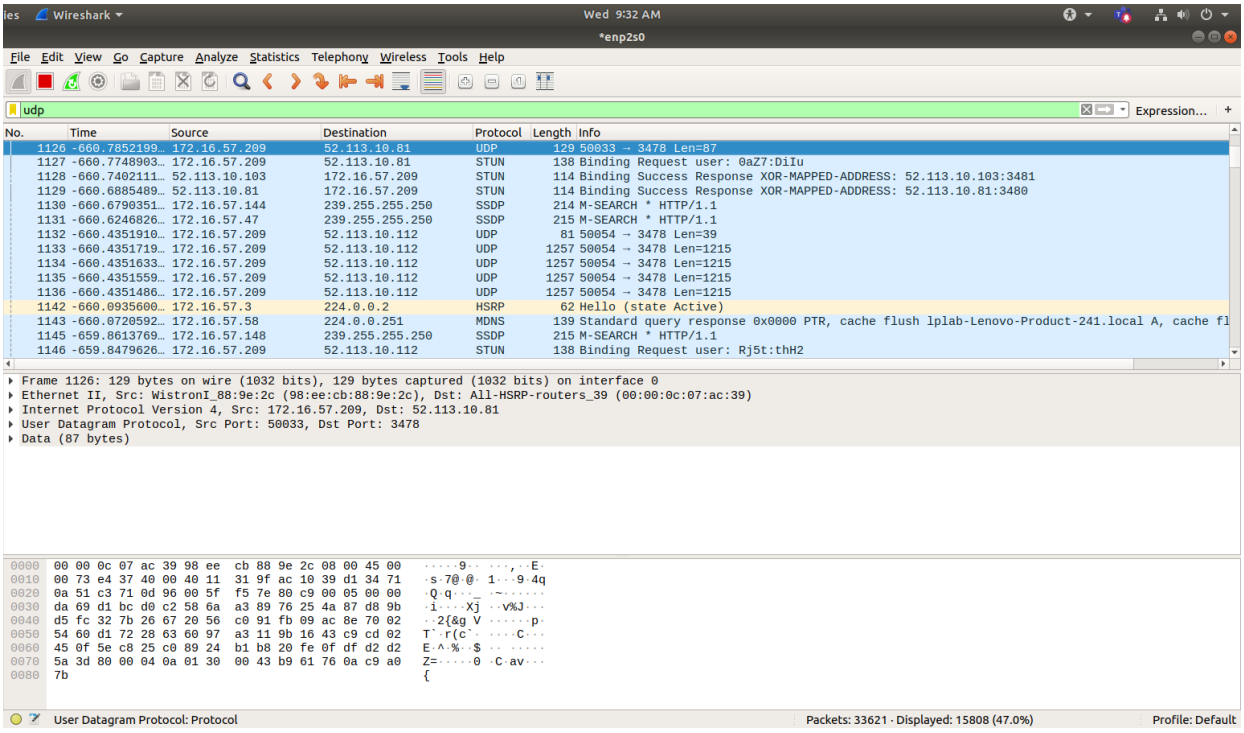
// Same Network Topology Using Switch



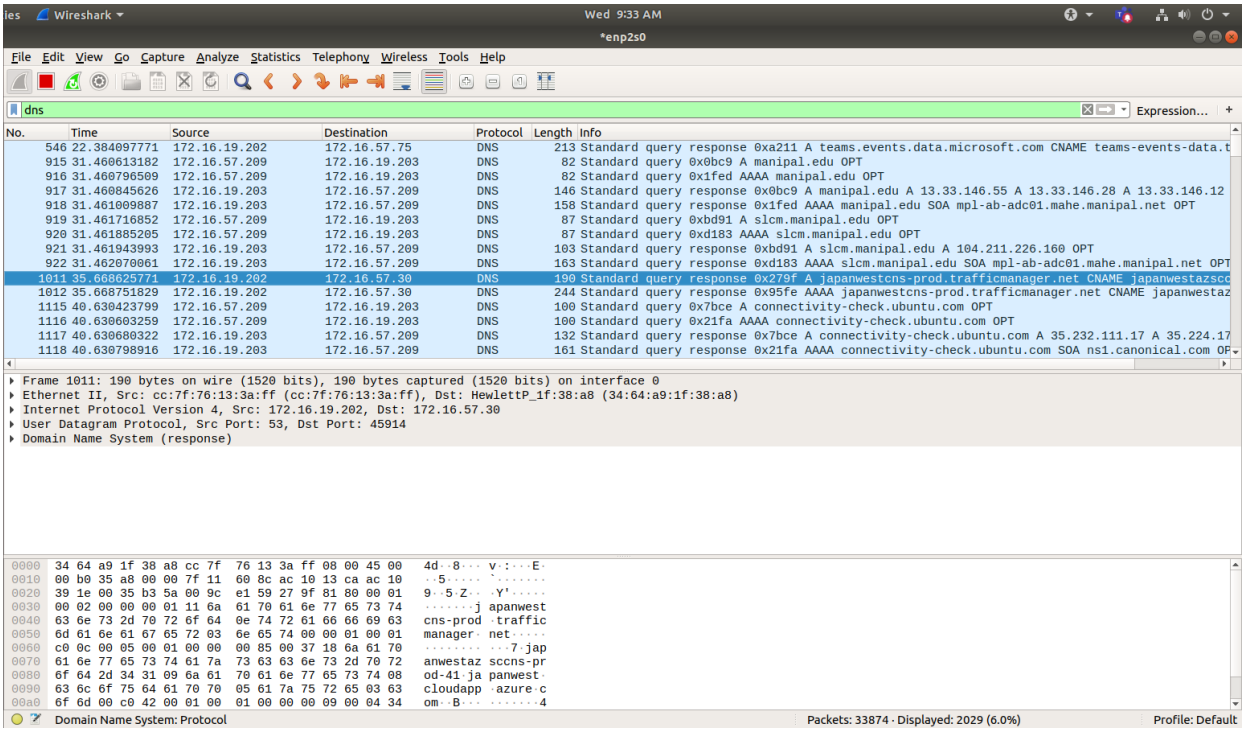



Wireshark
Wed 9:48 AM
Capturing from Standard input [PC1 Ethernet0 to Switch1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
No. Time Source Destination Protocol Length Info
1 0.000000 Private_66:68:00 Broadcast ARP 64 Who has 10.10.10.2? Tell 10.10.10.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
2 0.000219 Private_66:68:01 Private_66:68:00 ARP 64 10.10.10.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
3 0.001058 10.10.10.1 10.10.10.2 ICMP 98 Echo (ping) request id=0xded2, seq=1/256, ttl=64 (reply in 4)
4 0.001328 10.10.10.2 10.10.10.1 ICMP 98 Echo (ping) reply id=0xded2, seq=1/256, ttl=64 (request in 3)
5 1.002320 10.10.10.1 10.10.10.2 ICMP 98 Echo (ping) request id=0xdfd2, seq=2/512, ttl=64 (reply in 6)
6 1.002600 10.10.10.2 10.10.10.1 ICMP 98 Echo (ping) reply id=0xdfd2, seq=2/512, ttl=64 (request in 5)
7 2.003628 10.10.10.1 10.10.10.2 ICMP 98 Echo (ping) request id=0xe0d2, seq=3/768, ttl=64 (reply in 8)
8 2.003961 10.10.10.2 10.10.10.1 ICMP 98 Echo (ping) reply id=0xe0d2, seq=3/768, ttl=64 (request in 7)
9 3.004808 10.10.10.1 10.10.10.2 ICMP 98 Echo (ping) request id=0xe1d2, seq=4/1024, ttl=64 (reply in 10)
10 3.005156 10.10.10.2 10.10.10.1 ICMP 98 Echo (ping) reply id=0xe1d2, seq=4/1024, ttl=64 (request in 9)
11 4.006034 10.10.10.1 10.10.10.2 ICMP 98 Echo (ping) request id=0xe2d2, seq=5/1280, ttl=64 (reply in 12)
12 4.006420 10.10.10.2 10.10.10.1 ICMP 98 Echo (ping) reply id=0xe2d2, seq=5/1280, ttl=64 (request in 11)
Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2
Internet Control Message Protocol
0000 00 50 79 66 68 01 00 50 79 66 68 00 08 00 45 00 ·Pyfh··P yfh···E·
0010 00 54 d2 de 00 00 40 01 7f b4 0a 0a 0a 01 0a 0a ·T····@· ····· ····
0020 0a 02 08 00 41 38 de d2 00 01 08 09 0a 0b 0c 0d ····A8·· ····· ····
0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d ····· ····· ····
0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ··· !"#$% &'()*+,-
0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789:;<=
0060 3e 3f >?
Ready to load or capture
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default

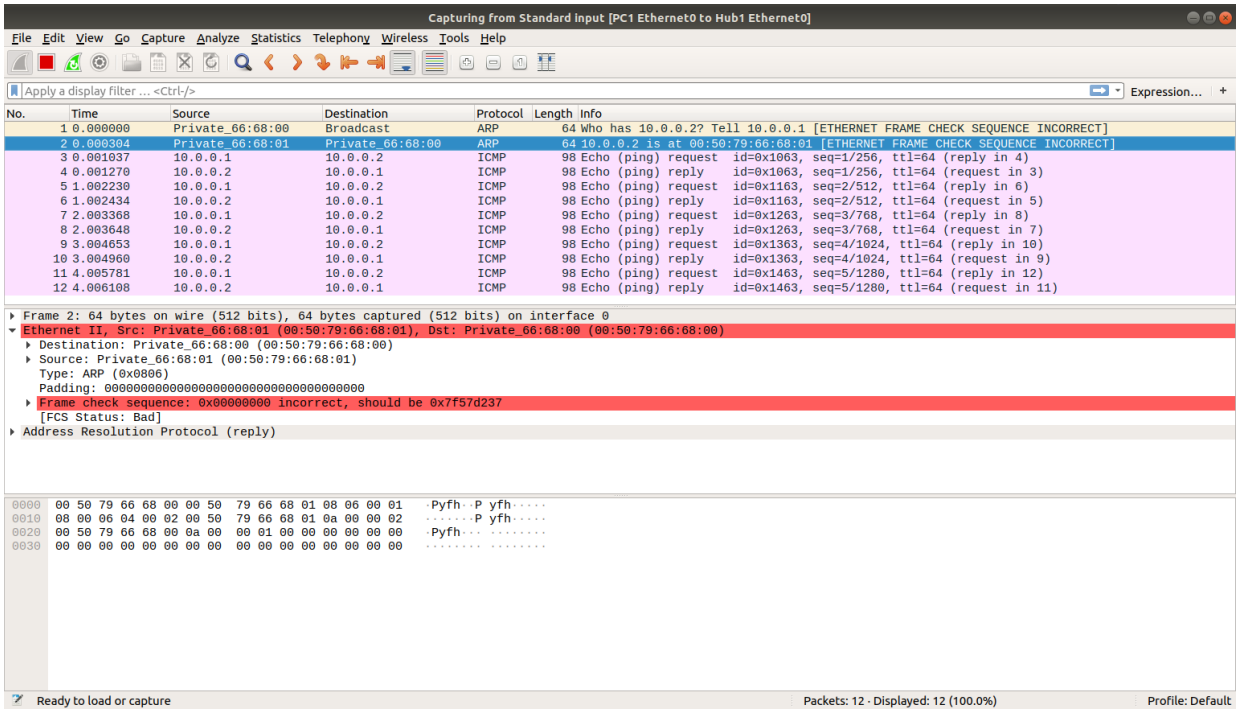
//UDP


Wireshark
Wed 9:32 AM
*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
Expression…
No. Time Source Destination Protocol Length Info
1126 -660.7852199… 172.16.57.209 52.113.10.81 UDP 129 50033 → 3478 Len=87
1127 -660.7748903… 172.16.57.209 52.113.10.81 STUN 138 Binding Request user: 0aZ7:DiIu
1128 -660.7402111… 52.113.10.103 172.16.57.209 STUN 114 Binding Success Response XOR-MAPPED-ADDRESS: 52.113.10.103:3481
1129 -660.6885489… 52.113.10.81 172.16.57.209 STUN 114 Binding Success Response XOR-MAPPED-ADDRESS: 52.113.10.81:3480
1130 -660.6790351… 172.16.57.144 239.255.255.250 SSDP 214 M-SEARCH * HTTP/1.1
1131 -660.6246826… 172.16.57.47 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
1132 -660.4351910… 172.16.57.209 52.113.10.112 UDP 81 50054 → 3478 Len=39
1133 -660.4351719… 172.16.57.209 52.113.10.112 UDP 1257 50054 → 3478 Len=1215
1134 -660.4351633… 172.16.57.209 52.113.10.112 UDP 1257 50054 → 3478 Len=1215
1135 -660.4351559… 172.16.57.209 52.113.10.112 UDP 1257 50054 → 3478 Len=1215
1136 -660.4351486… 172.16.57.209 52.113.10.112 UDP 1257 50054 → 3478 Len=1215
1142 -660.0935600… 172.16.57.3 224.0.0.2 HSRP 62 Hello (state Active)
1143 -660.0720592… 172.16.57.58 224.0.0.251 MDNS 139 Standard query response 0x0000 PTR, cache flush lplab-Lenovo-Product-241.local A, cache fl
1145 -659.8613769… 172.16.57.148 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
1146 -659.8479626… 172.16.57.209 52.113.10.112 STUN 138 Binding Request user: Rj5t:thH2
Frame 1126: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0
Ethernet II, Src: WistronI_88:9e:2c (98:ee:cb:88:9e:2c), Dst: All-HSRP-routers_39 (00:00:0c:07:ac:39)
Internet Protocol Version 4, Src: 172.16.57.209, Dst: 52.113.10.81
User Datagram Protocol, Src Port: 50033, Dst Port: 3478
Data (87 bytes)
0000 00 00 0c 07 ac 39 98 ee cb 88 9e 2c 08 00 45 00 ·····9·· ···,··E·
0010 00 73 e4 37 40 00 40 11 31 9f ac 10 39 d1 34 71 ·s·7@·@· 1···9·4q
0020 0a 51 c3 71 0d 96 00 5f f5 7e 80 c9 00 05 00 00 ·Q·q···_ ·~·····
0030 da 69 d1 bc d0 c2 58 6a a3 89 76 25 4a 87 d8 9b ·i····Xj ··v%J···
0040 d5 fc 32 7b 26 67 20 56 c0 91 fb 09 ac 8e 70 02 ··2{&g V ····· p·
0050 54 60 d1 72 28 63 60 97 a3 11 9b 16 43 c9 cd 02 T`·r(c`· ····C···
0060 45 0f 5e c8 25 c0 89 24 b1 b8 20 fe 0f df d2 d2 E·^·%··$ ·· ·····
0070 5a 3d 80 00 04 0a 01 30 00 43 b9 61 76 0a c9 a0 Z=·····0 ·C·av···
0080 7b {
User Datagram Protocol: Protocol
Packets: 33621 · Displayed: 15808 (47.0%)
Profile: Default

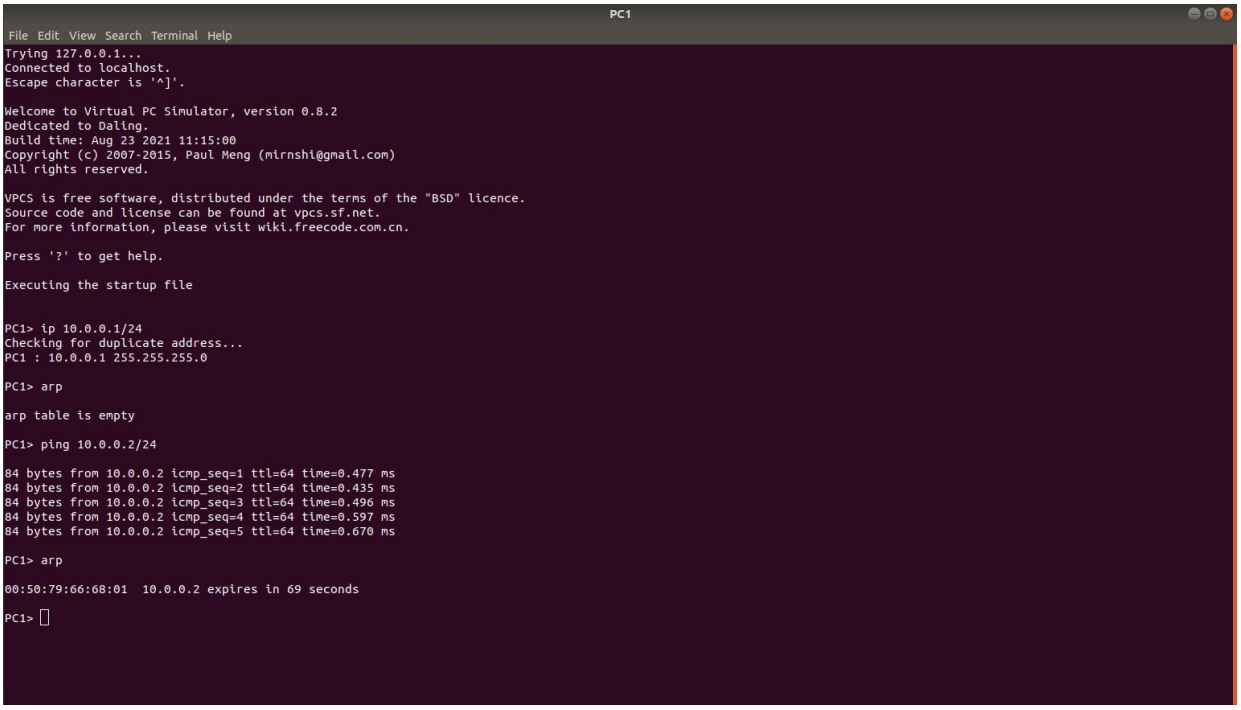
//DNS



ARP packets in the Wireshark window with the MAC addresses in the Ethernet headers of the captured packets.



Destination MAC address of the ARP Request packets: 00:50:79:66:68:00
Type field in the ethernet headers is ARP(0x0860)



ARP packets for PC1