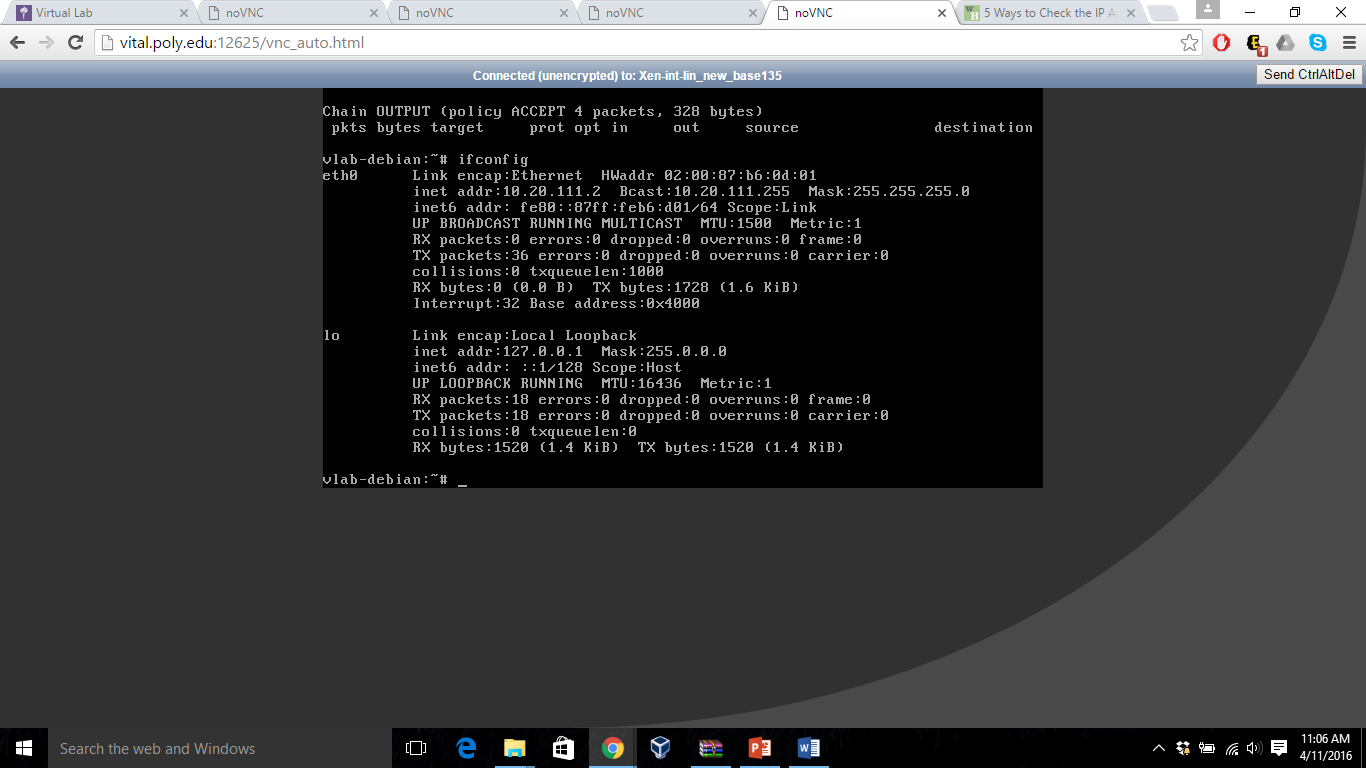
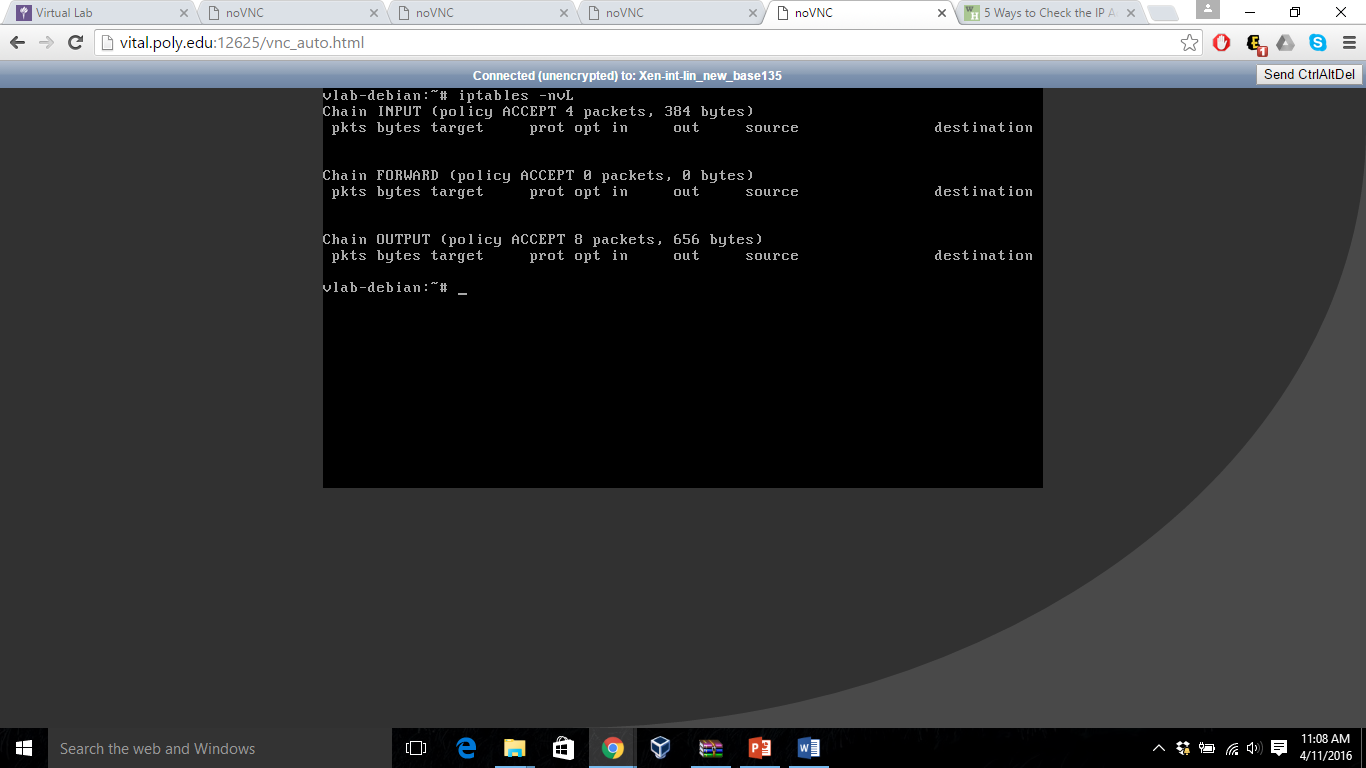
Internal Linux: IP configuration



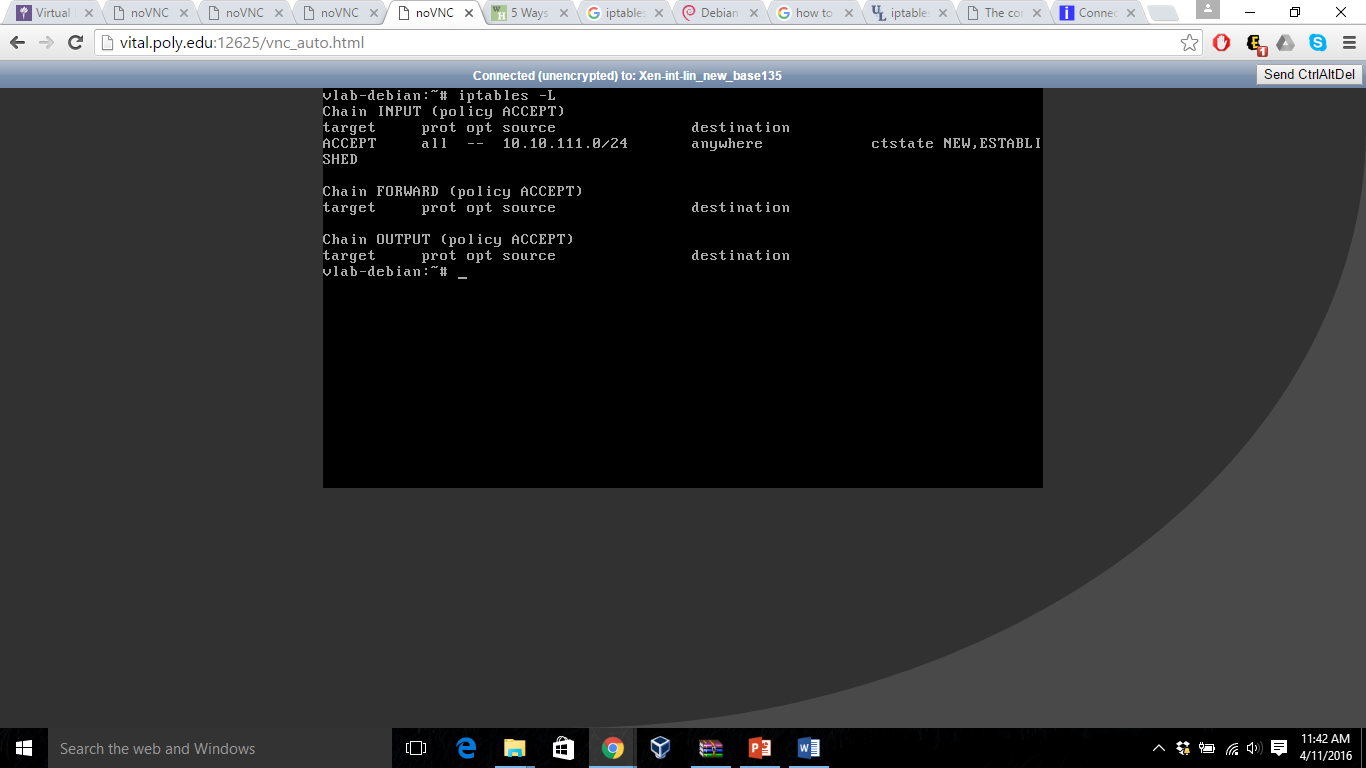
Initial IP Table:



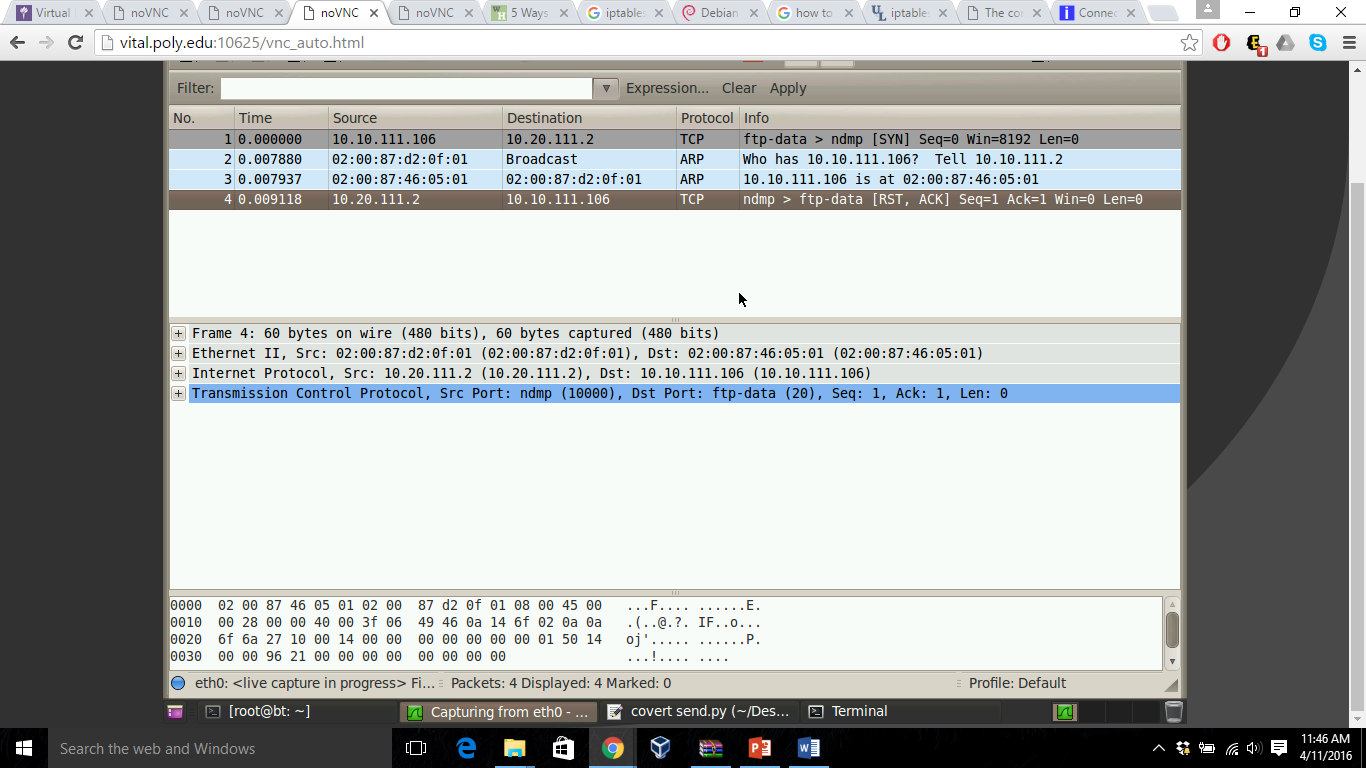
**PART A**

**1) [15 pts] The internal machine should respond to a ping from 10.10.111.0/24:**

-> iptables -A INPUT -s 10.10.111.0/24 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT



TCP Packet sent from BT5 and monitored using WIRESHARK

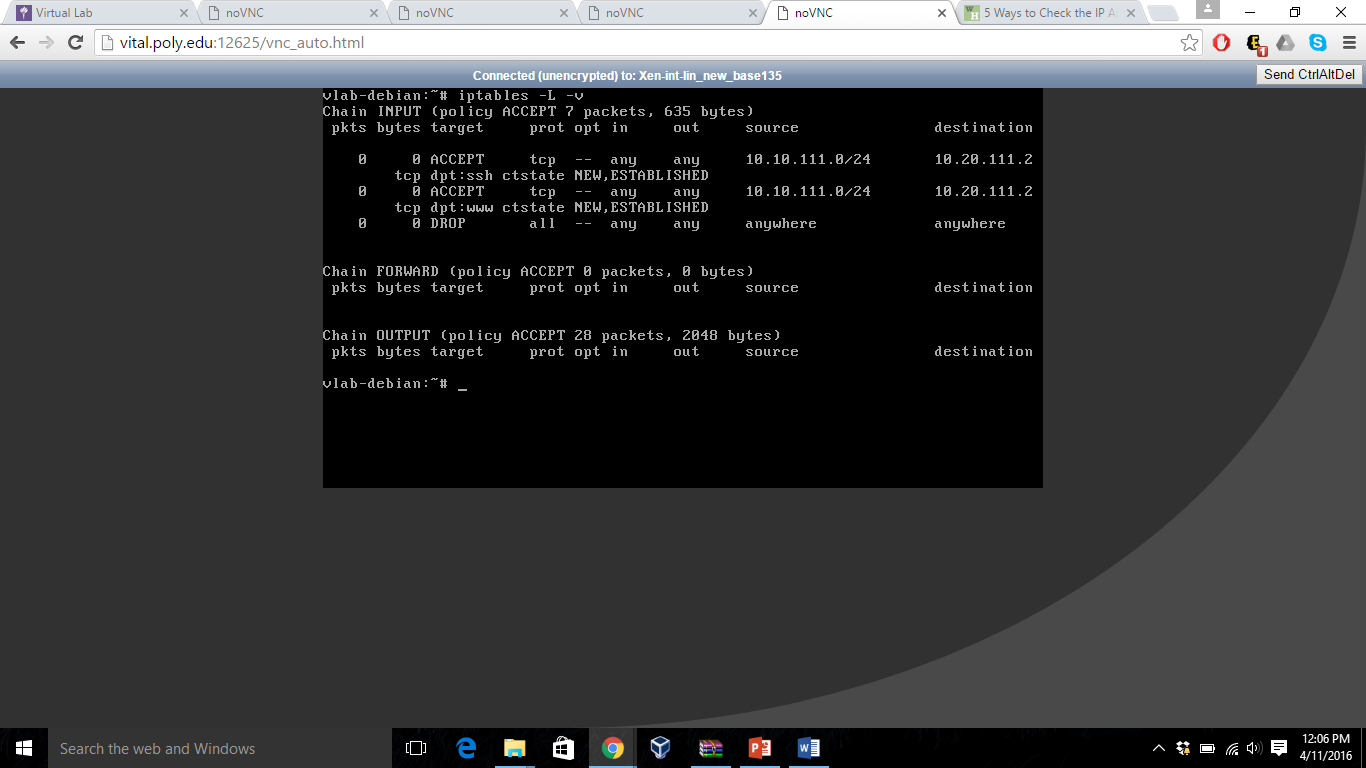


**2) [15 pts] The internal machine (10.20.111.2) should accept all incoming SSH and http requests from 10.10.111.0/24.**

-> iptables -A INPUT -p tcp –dport ssh -d 10.20.111.2 -s 10.10.111.0/24 -m conntrack –ctstate NEW,EXTABLISHED -j ACCEPT

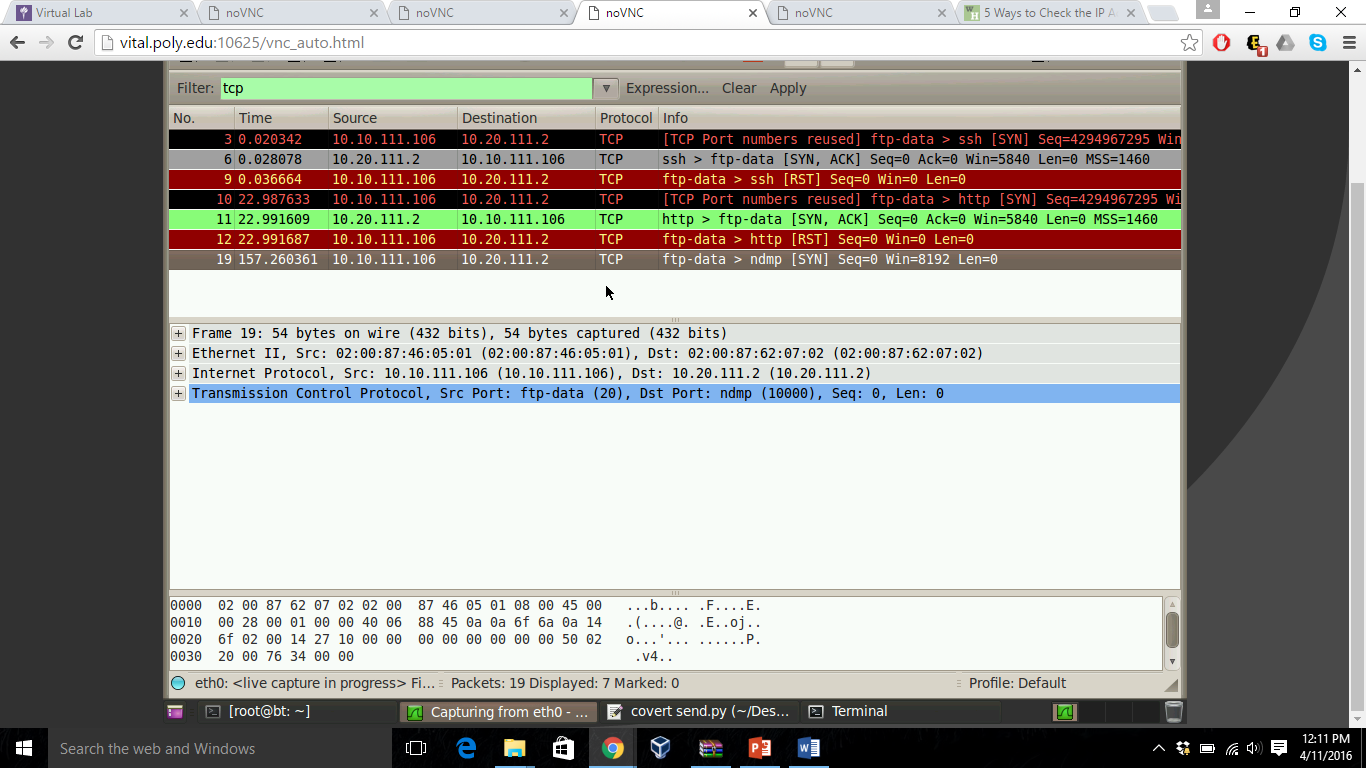
-> iptables -A INPUT -p tcp --dport 80 -d 10.20.111.2 -s 10.10.111.0/24 -m conntrack –ctstate NEW,EXTABLISHED -j ACCEPT

-> iptables -A INPUT -j DROP {to drop any other request other than SSH and WWW}



After sending 3 packets to the internal linux router i.e., at port 22(SSH), port 80(WWW) and port 10000, we received response for the first 2 packets but no response for the last one as the iptable has DROP entry for anything other than port 22 and port 80.

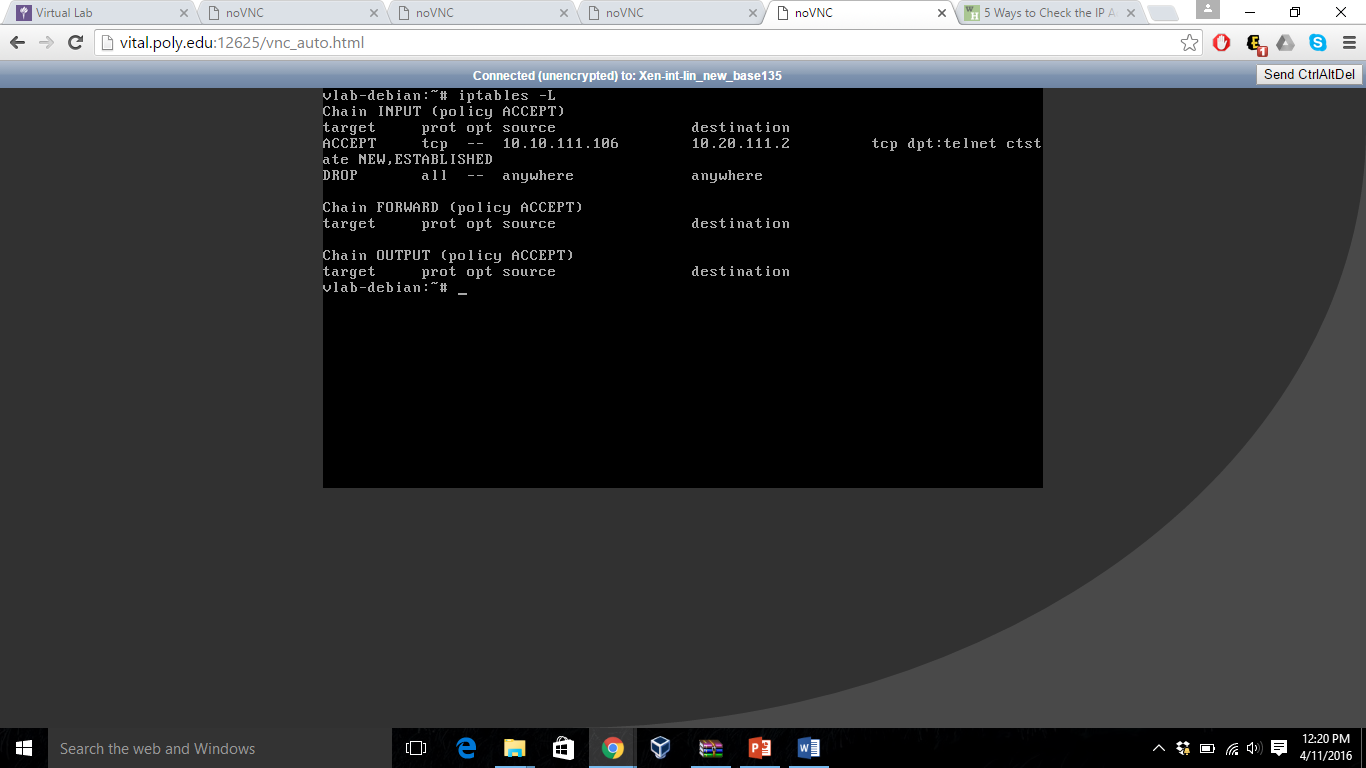
Wireshark shows the same in below screenshot



**3) [20 pts] The internal machine should accept telnet connections from the BT Machine only.**

-> iptables -A INPUT -p tcp –dport telnet -d 10.20.111.2 -s 10.10.111.106 -m conntrack –ctstate NEW,EXTABLISHED -j ACCEPT

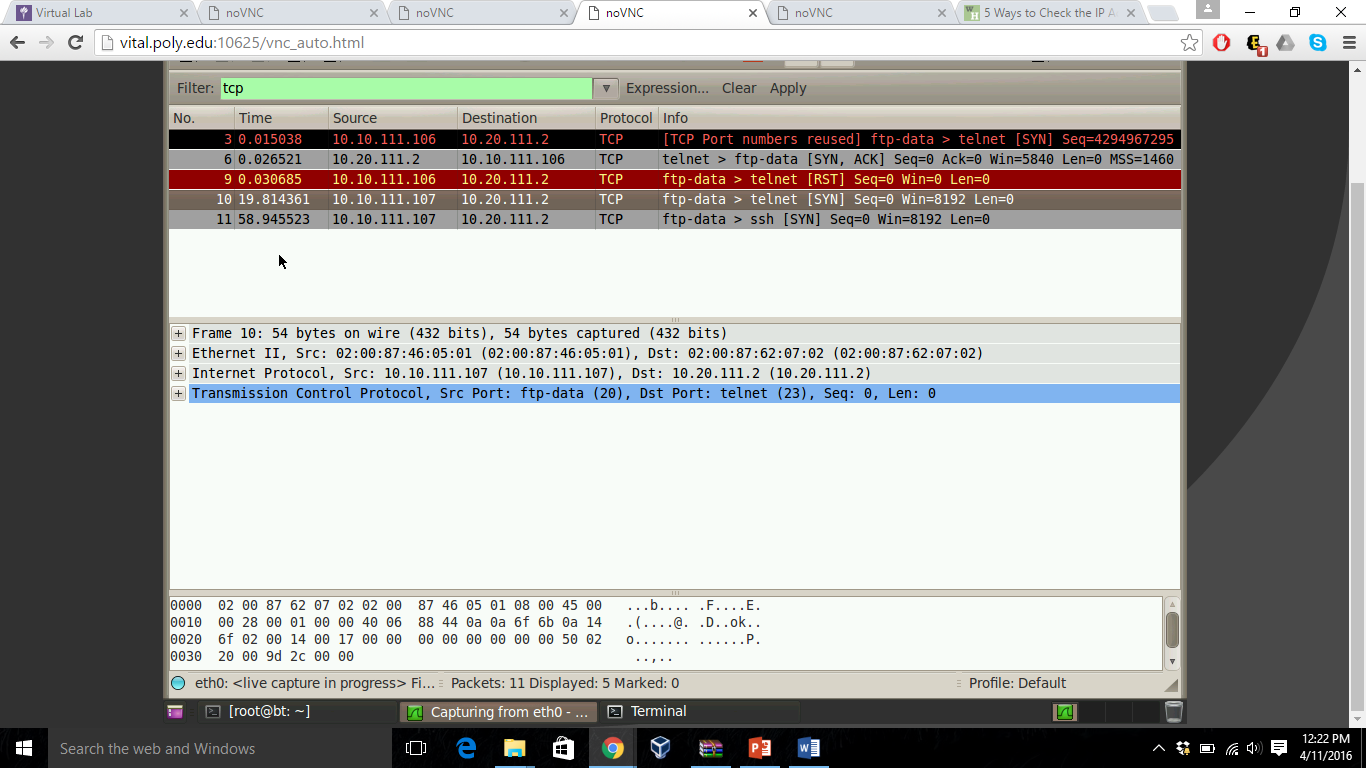
-> iptables -A INPUT -j DROP {to drop any other request other than TELNET}



First packet sent with BT5 IP address i.e., 10.10.111.106 to port 23 and in Wireshark it is observed that a response is obtained from Internal Linux machine.

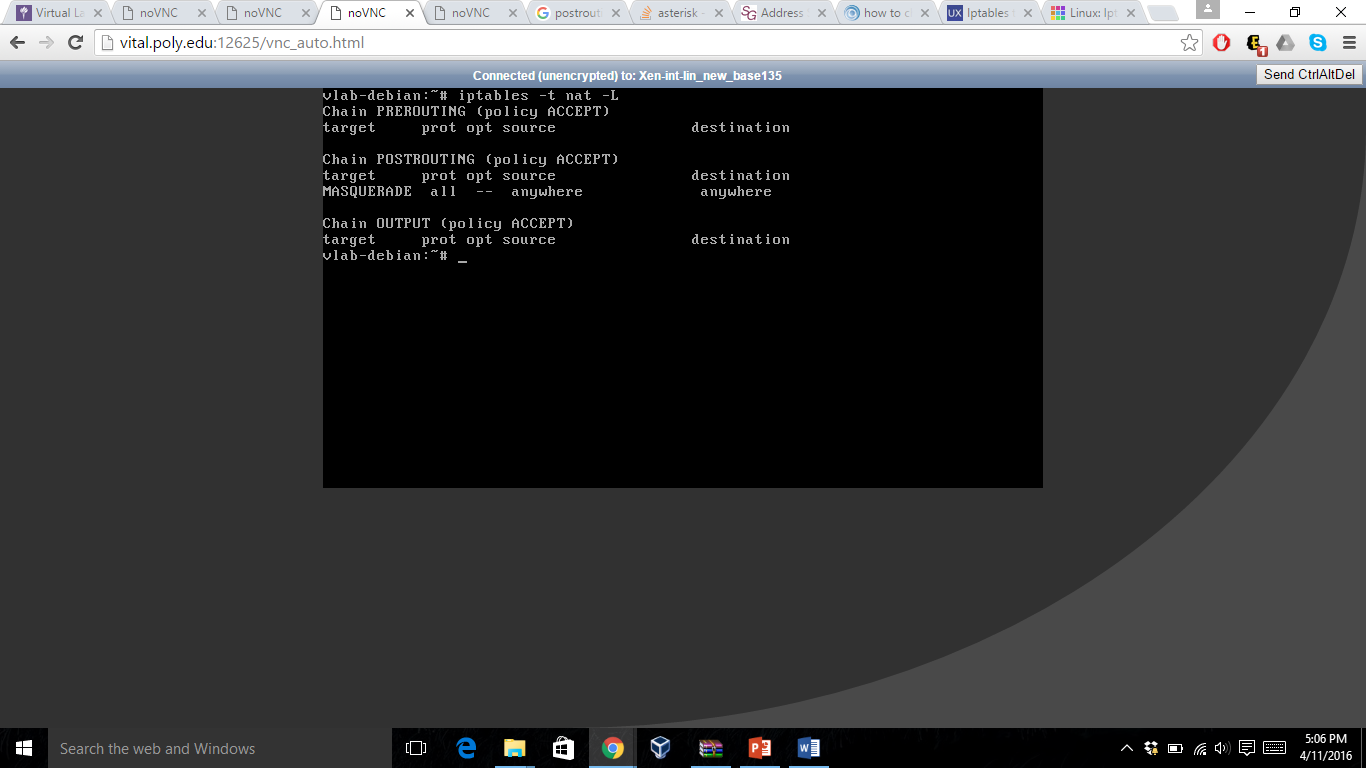
Other than this 2 more packets were sent one with IP address 10.10.111.107 and one with IP address as 10.10.111.107, port=22, for both of the packet no response obtained from the Linux machine as we have used Drop which drops all the packets that are not from BT5 and to port 23.

Wireshark shows the same in the below screenshot.

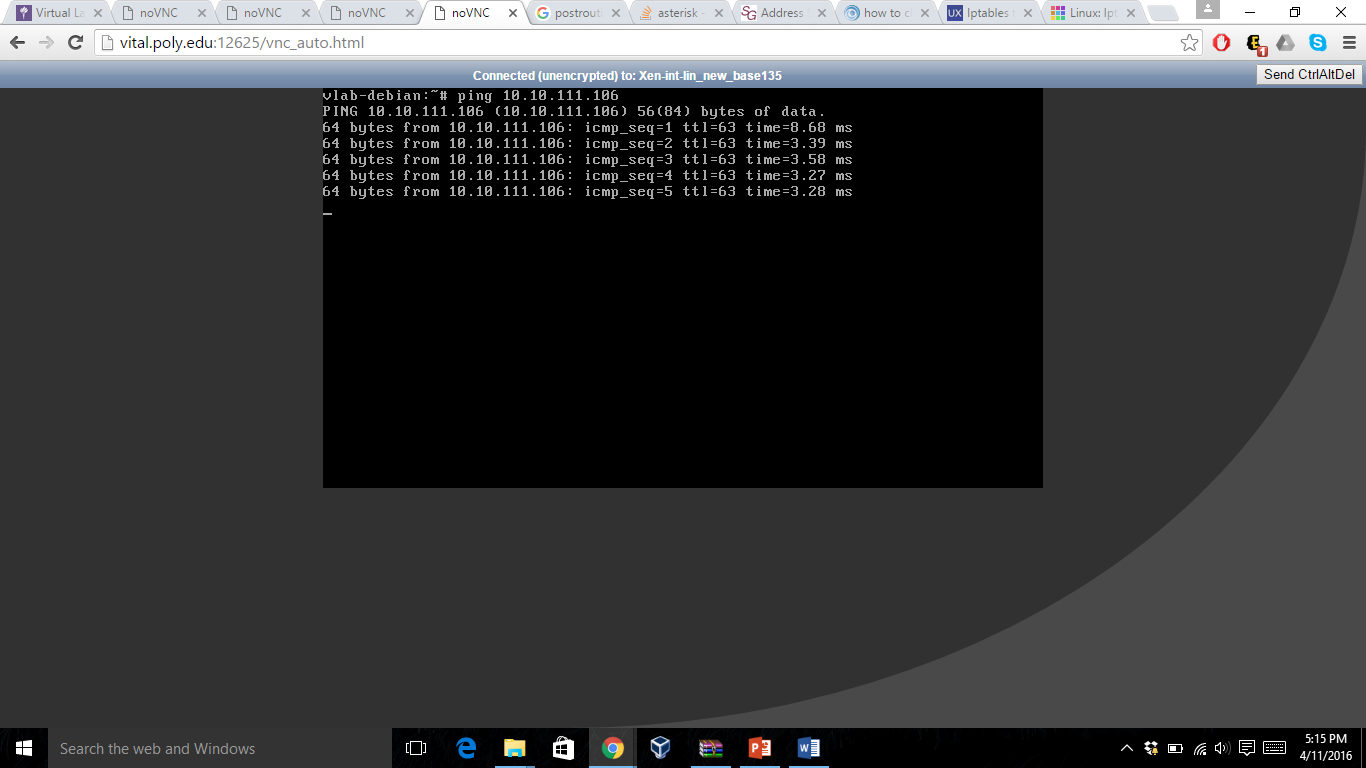


**PART B**

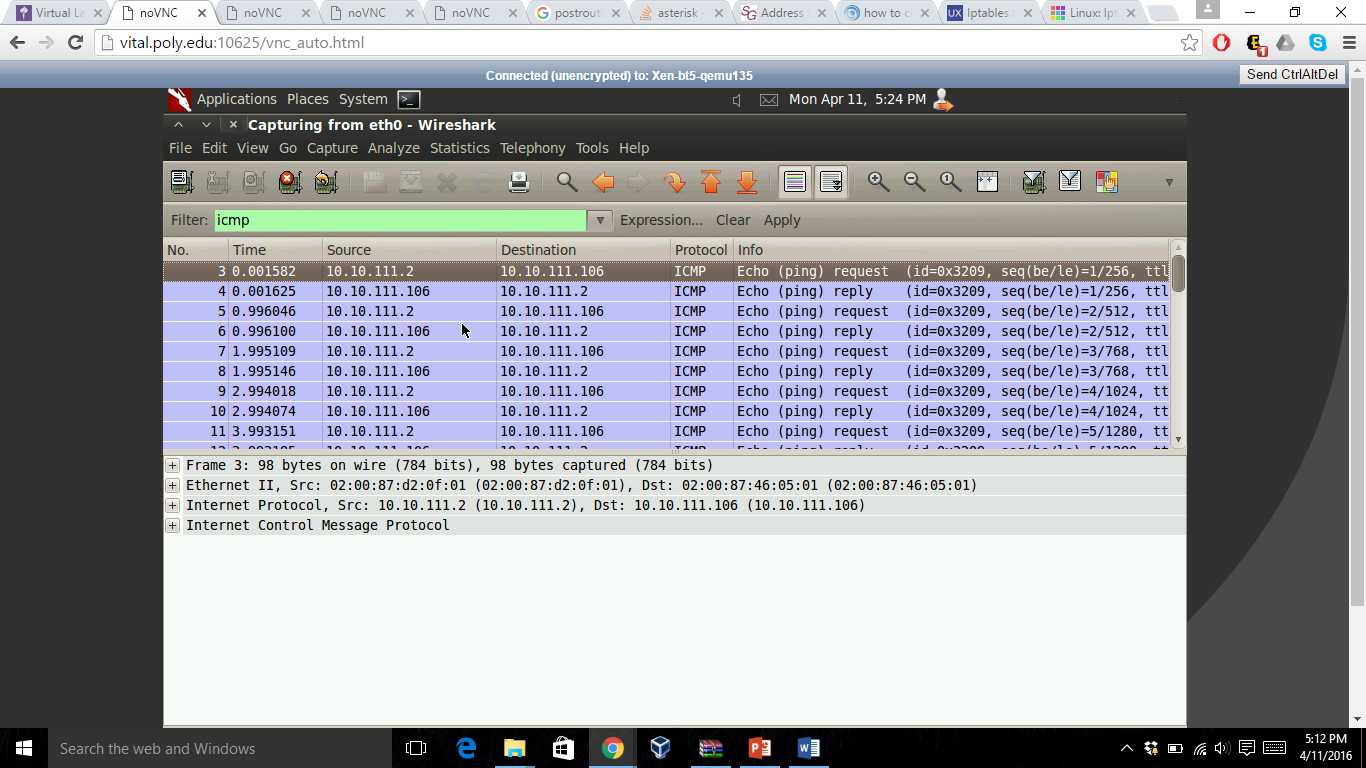
-> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE



ICMP packets were sent using PING from Linux machine (10.20.111.2) to my BT5 machine (10.10.111.106) using command ‘ping 10.10.111.106’.



For the internal router interface eth0 has IP (10.10.111.2)



The packets reached at BT5 seen using Wireshark shows the source IP for ICMP as 10.10.111.2 which is the IP of the eth0 interface of the internal router.

**PART C**

**1) [5 pts] In your own words describe how iptables works?**

Ans: IPTables consists of set of rules which governs the network traffic at the firewall. Every packet that reaches the firewall must match the rules mentioned in the iptables to pass through. If the packet does not match any rule, the packet is rejected or dropped based on the iptables settings.

When the packet matches any rule, the action takes place that is mentioned in the rule as target.

**2) [5 pts] What is the difference between input, output and forward chains?**

Ans: INPUT: This chain handles all the packets that are addressed to your server.

OUTPUT: This chain handles the response/traffic generated by your server

FORWARD: This chain is used to deal with traffic destined for other servers that are not created on your server.

**3) [5 pts] What is the difference between deny, reject and accept?**

Ans: DENY(DROP): This is the target mentioned in the IPTables, the packet matching the rules containing this as target will drop the packet without any reply to the sender.

REJECT: This is the target mentioned in the IPTables, the packet matching the rules containing this as target will drop the packet but will also send a reply to the sender mentioning the packet is rejected.

ACCEPT: This the target mentioned in the IPTables, the packet matching the rule containing this as target will accept the packet and will perform the action based on the type of chain.