CSE 3501

INFORMATION SECURITY ANALYSIS & AUDIT

Lab Assessment – 3

L9+L10 | PLBG04

FALL SEMESTER 2021-22

by

SHARADINDU ADHIKARI

19BCE2105

Experiment 1: Firewall

1. **Aim:** To demonstrate a Firewall implementation in Cisco Packet Tracer®.

2. **Description:** A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

   Firewalls have been a first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

3. **Benefits of Firewall:**
   - Monitors Network Traffic. All of the benefits of firewall security start with the ability to monitor network traffic.
   - Stops Virus Attacks. Nothing can shut your digital operations down faster and harder than a virus attack.
   - Prevents Hacking.
   - Stops Spyware.
   - Promotes Privacy.

4. **Procedure:**

   Device Configuration:
   - select 3 PCs, 1 Hub-PT, 1 Server-PT, & a copper straight through connection cable for the connection's b/w PCs, Hub and Server.
   - Connect fastethernet0 port of server with fastethernet0 port of hub.
   - Connect fastethernet0 port of PC0 with fastethernet1 port of hub.
   - Connect fastethernet0 port of PC1 with fastethernet2 port of hub.
   - Connect fastethernet0 port of PC2 with fastethernet3 port of hub.

   Server Configuration:
   - Go to router and then config.
   - Select FastEthernet0/0 under interface tab.
   - Set IP address and subnet mask for the selected router (i.e., 20.0.0.1).
   - Go to services then select HTTP. Turn on both radio buttons.
   - Now select DHCP, turn on service beside fastethernet0.
   - Save all the changes.

   PC Configuration:
   - Go to Desktop, then to: IP configuration on each PC.
   - Select Fastethernet0 from interface dropdown menu.
   - Select the DHCP radio button. (It will prompt DHCP request successful).

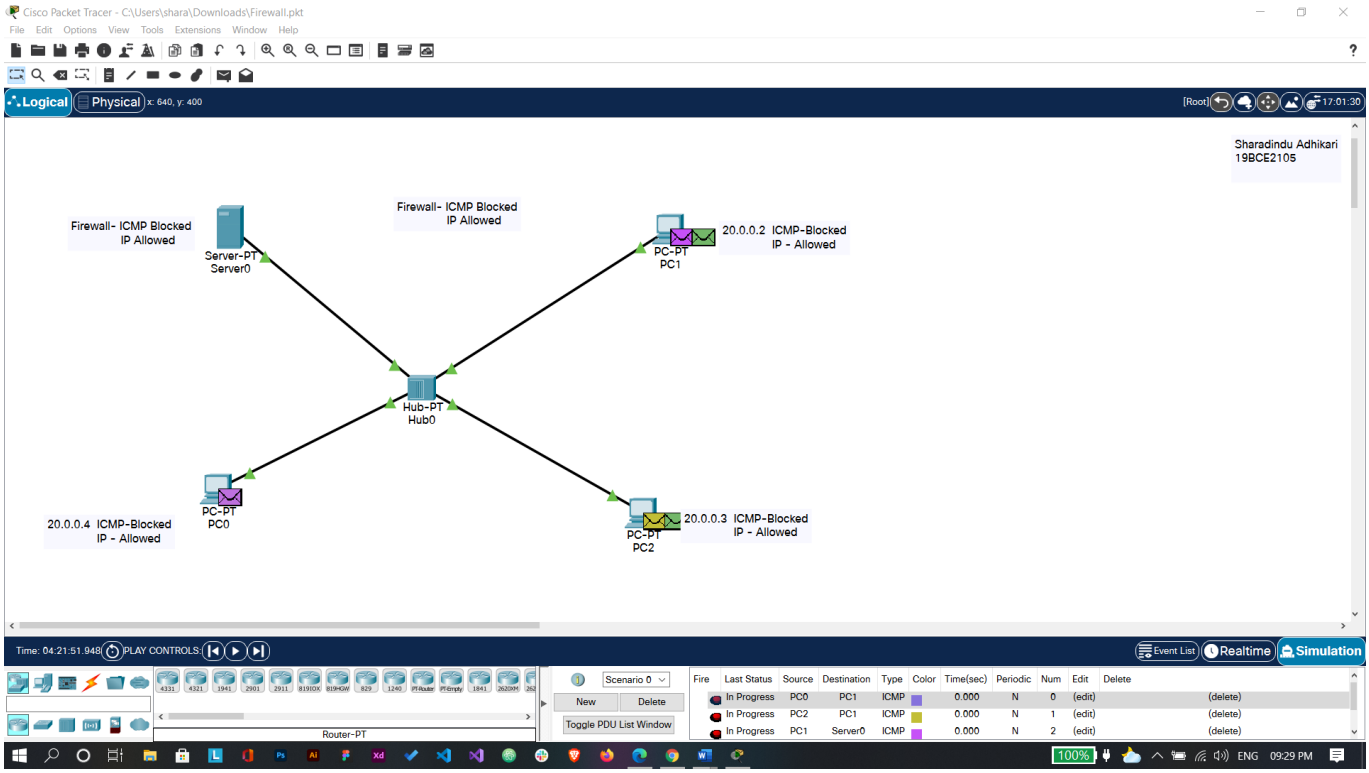
   Firewall Configuration (for the Server):
   - Go to desktop and select IPV4 firewall.
   - Turn the service radio button on.
   - Select Action->Deny and Protocol->ICMP.
   - Set Remote-IP to 0.0.0.0 and Remote Wildcard Mask to 255.255.255.255.
   - Click on Add to append the changes and then Save.
   - Repeat the above 2 steps for Action->Allow and Protocol->IP.

5. Testing:

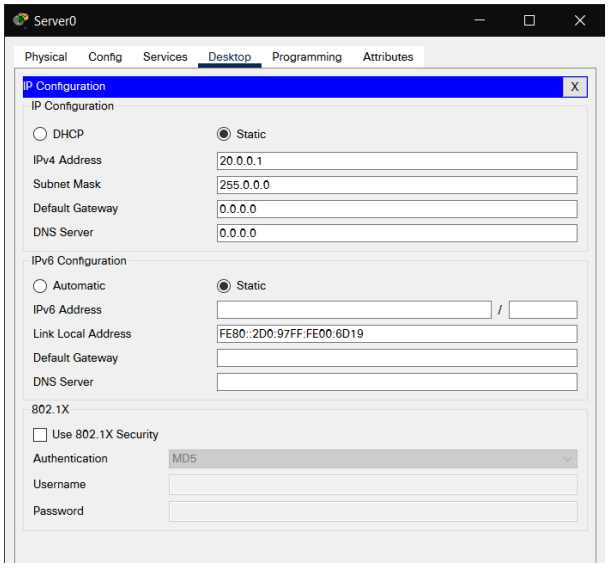
- For testing ICMP protocol go to Desktop->Command Prompt for any PC and enter the ping command followed by the IP address of the Server to analyse the working of the firewall.
- For testing IP protocol go to Desktop->Web Browser and enter the IP address of the Server, if it leads to the CISCO Homepage then firewall is set-up successfully.

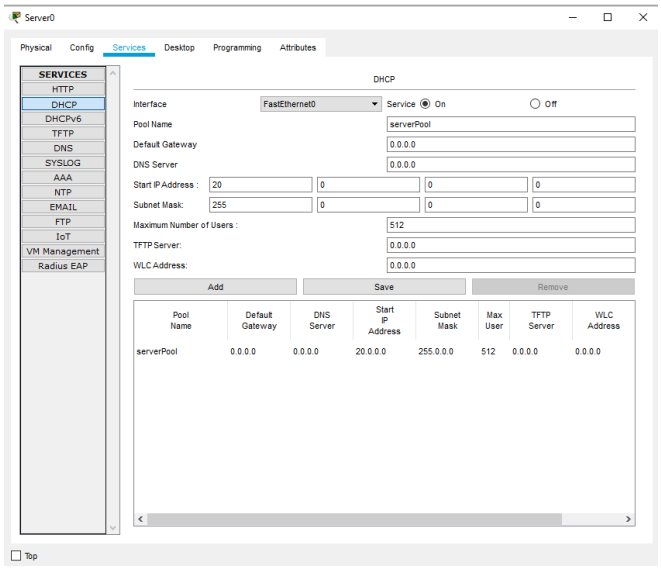
6. Screenshots:

Device configuration:

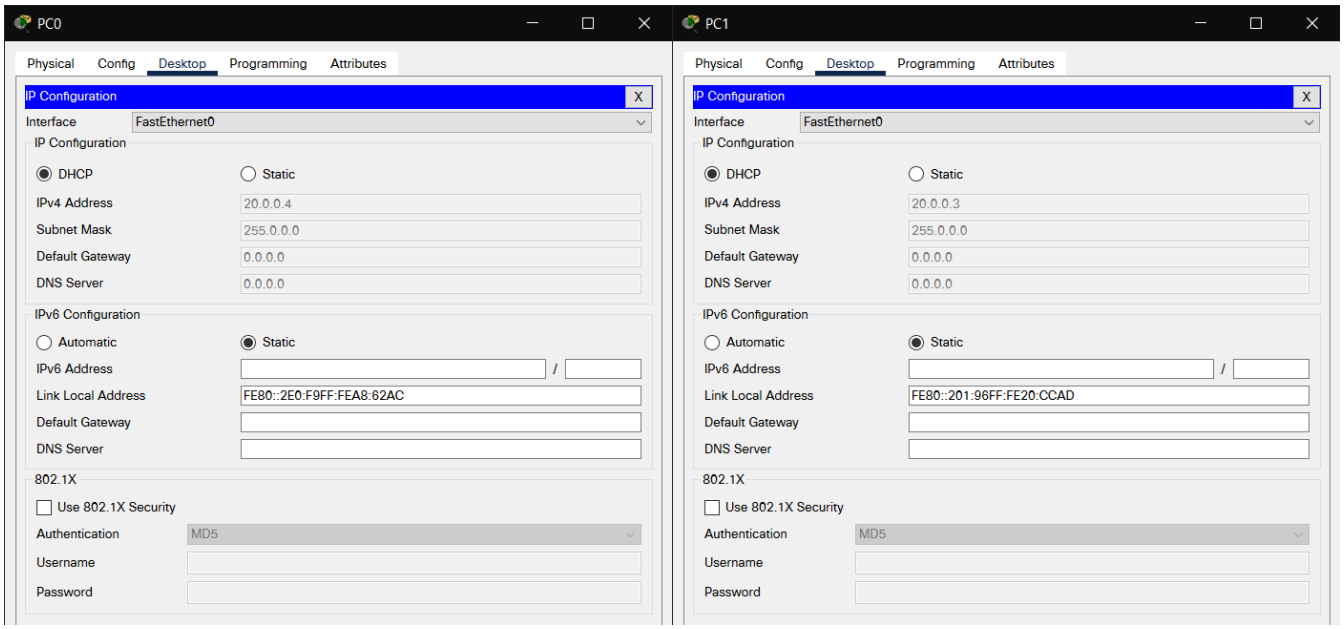


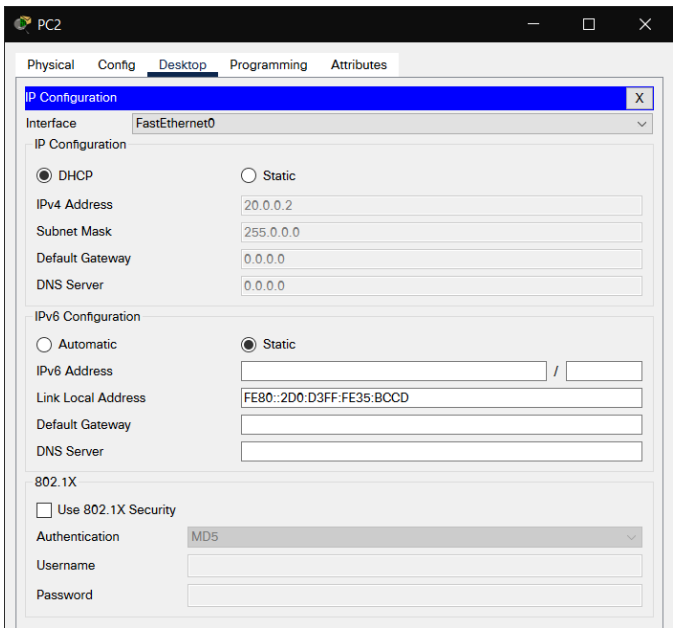
Server configuration:



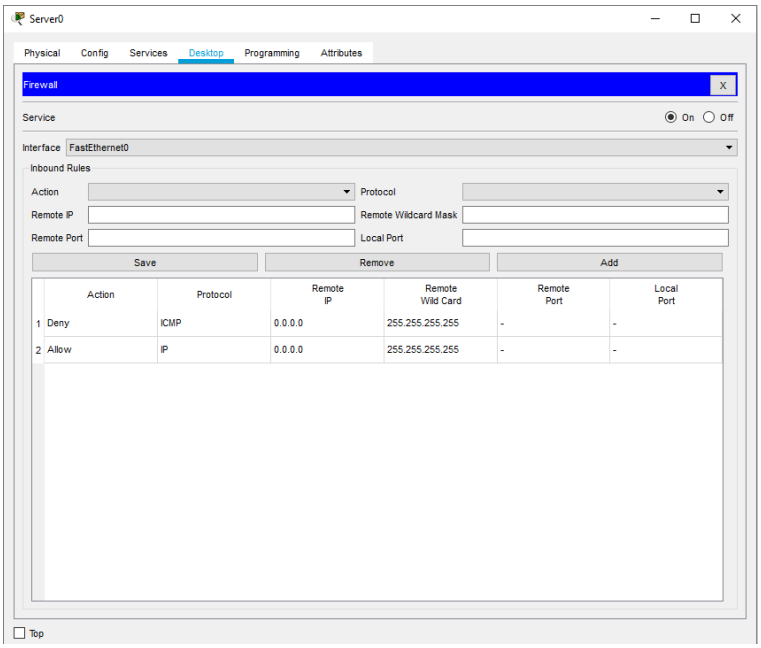


PC configurations:

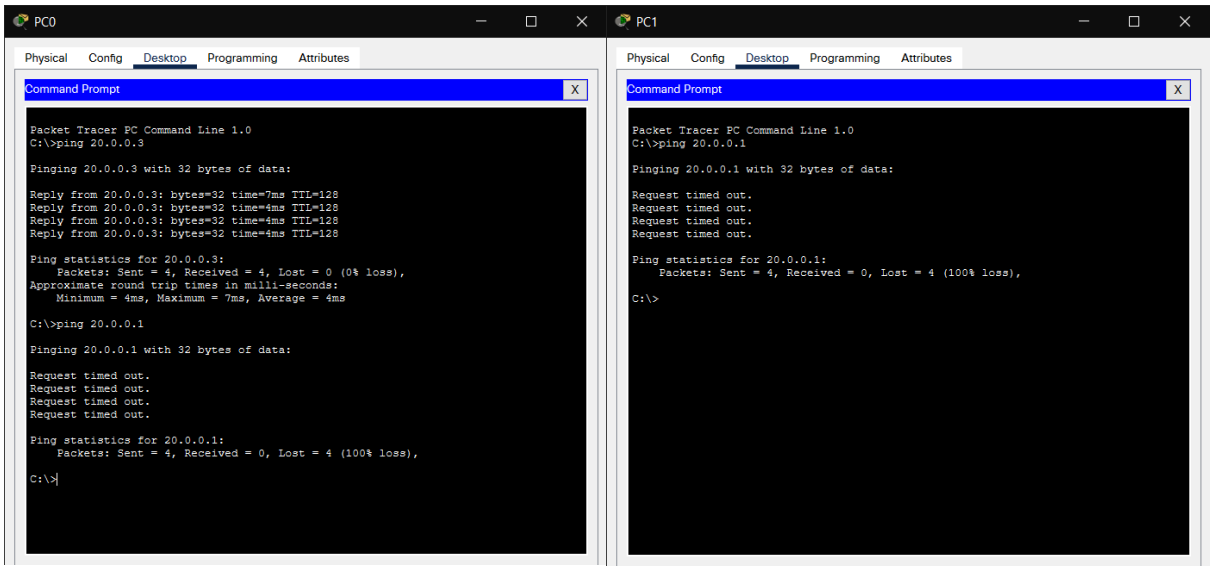


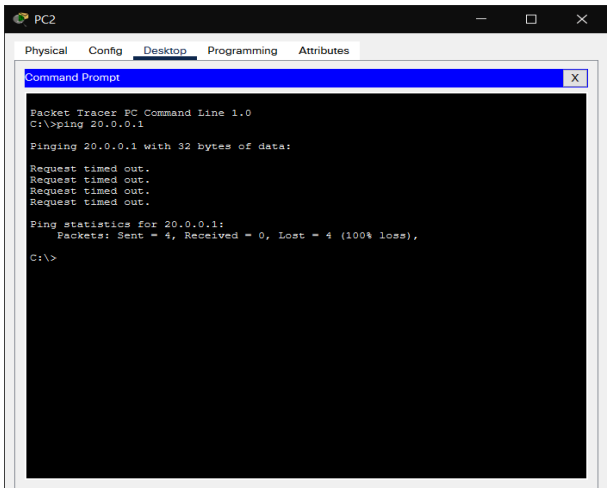


Firewall configuration:

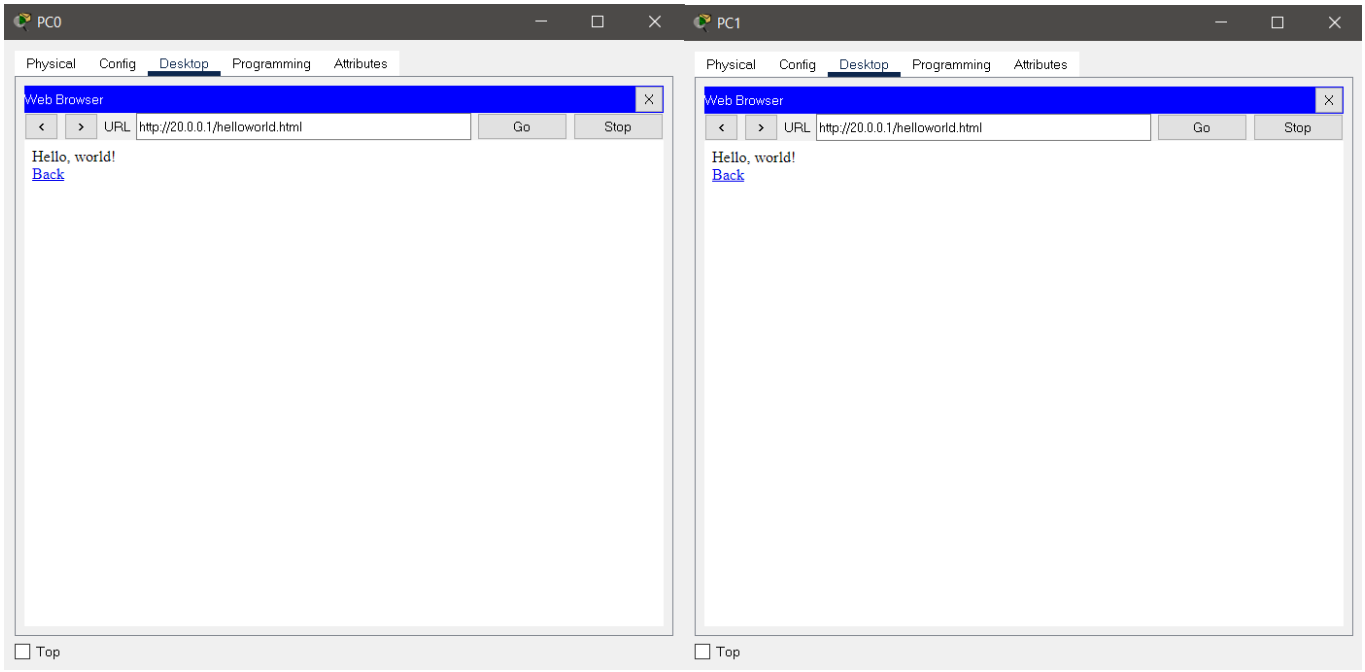


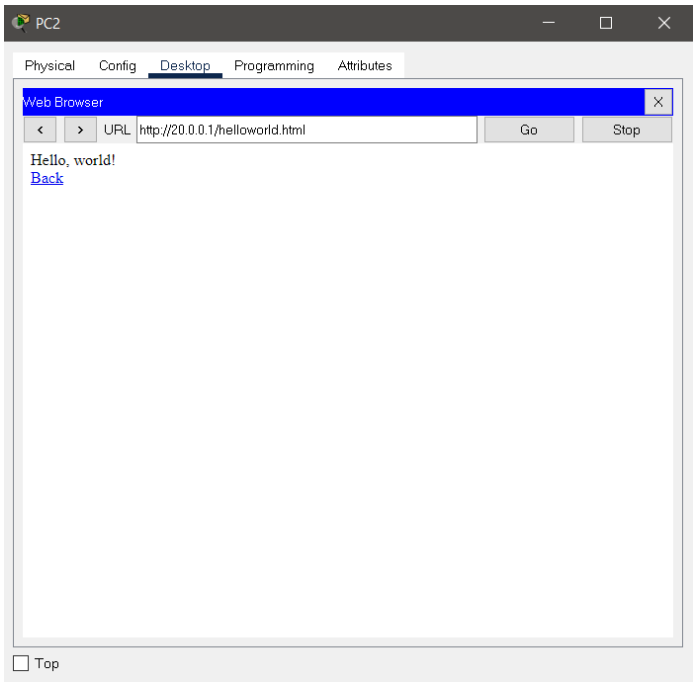
Testing ICMP Protocol:





Testing IP Protocol:





7. **Observation:** It is clear that some form of security for private networks connected to the internet is essential. A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions. That being said, our firewall implemented in this system is working well, as has been demonstrated.

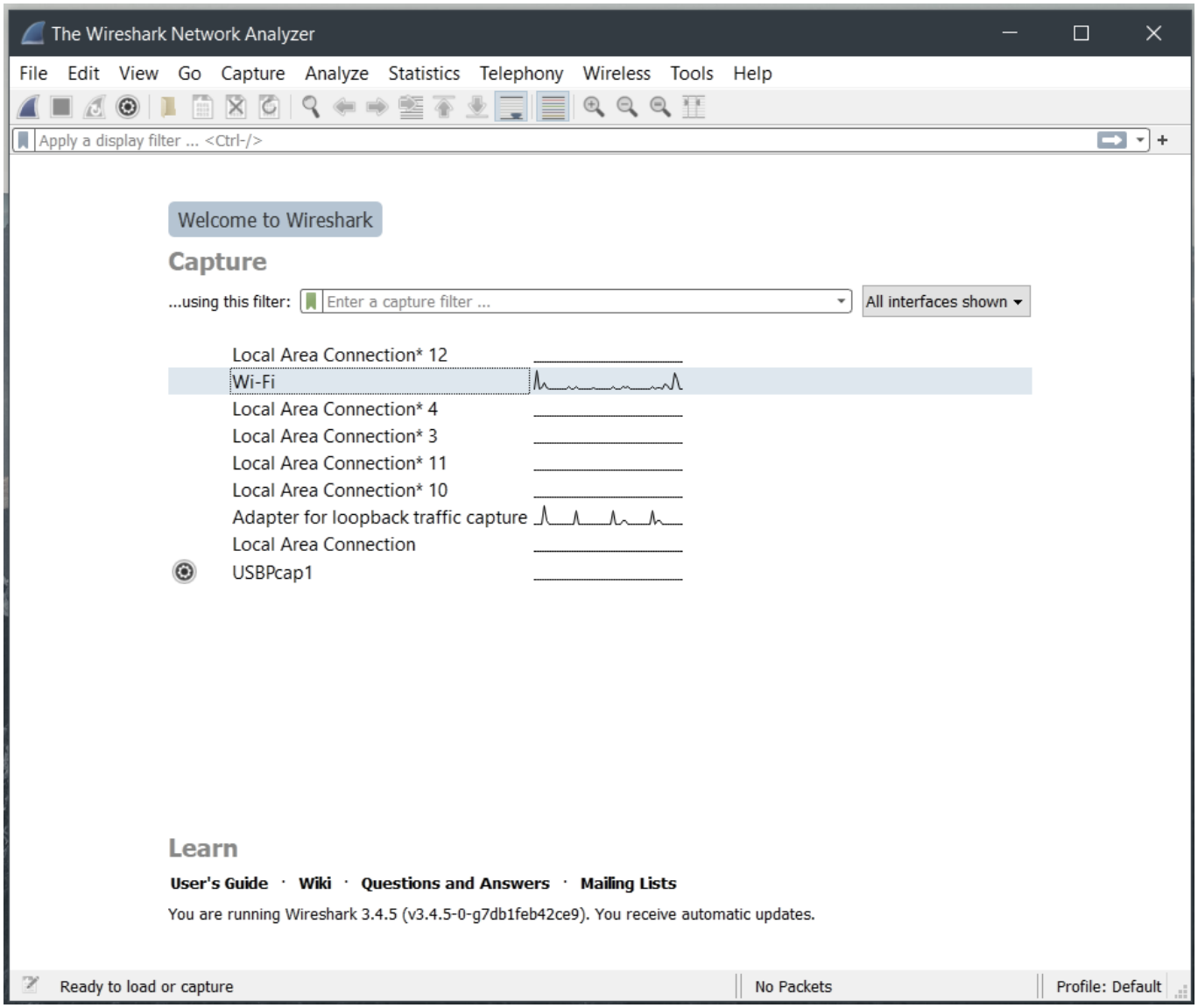
Experiment 2: Wireshark Filters

Aim: To analyse the Wireshark capture filter.

Introduction: Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

We could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

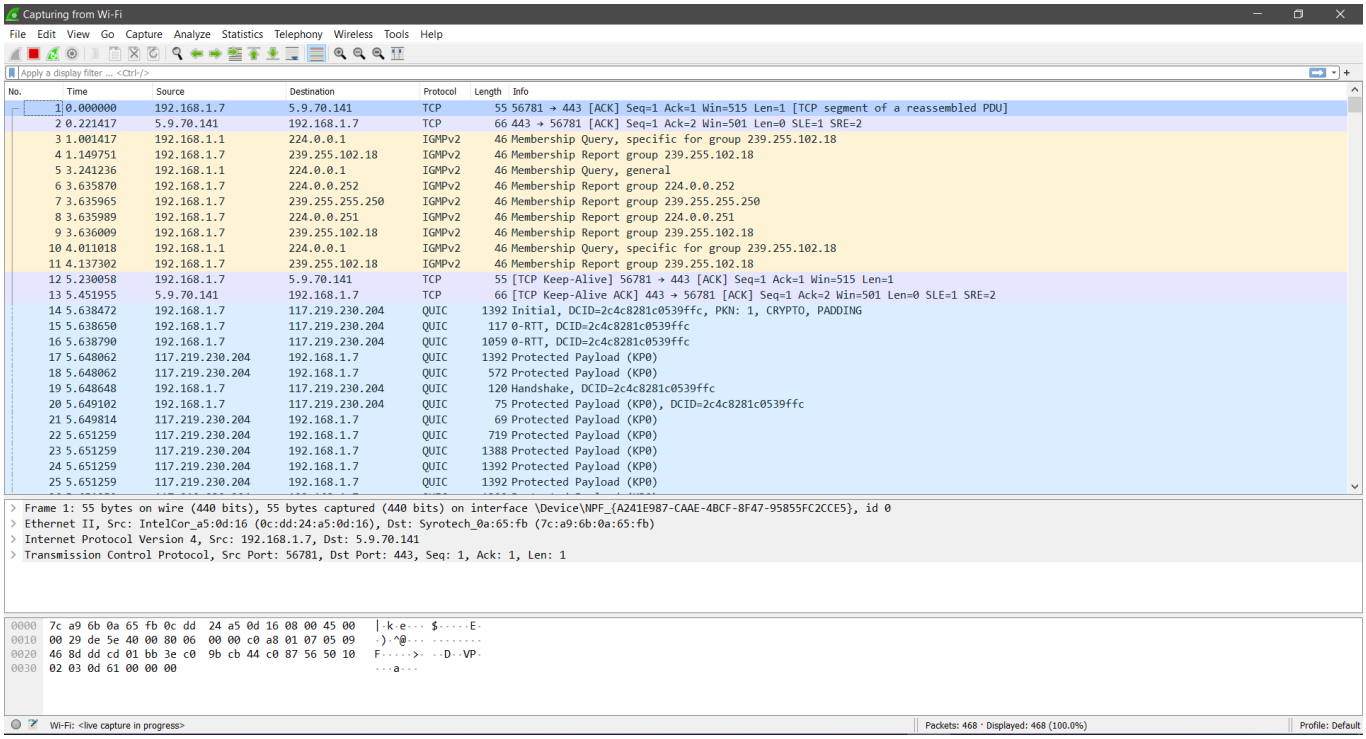
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.



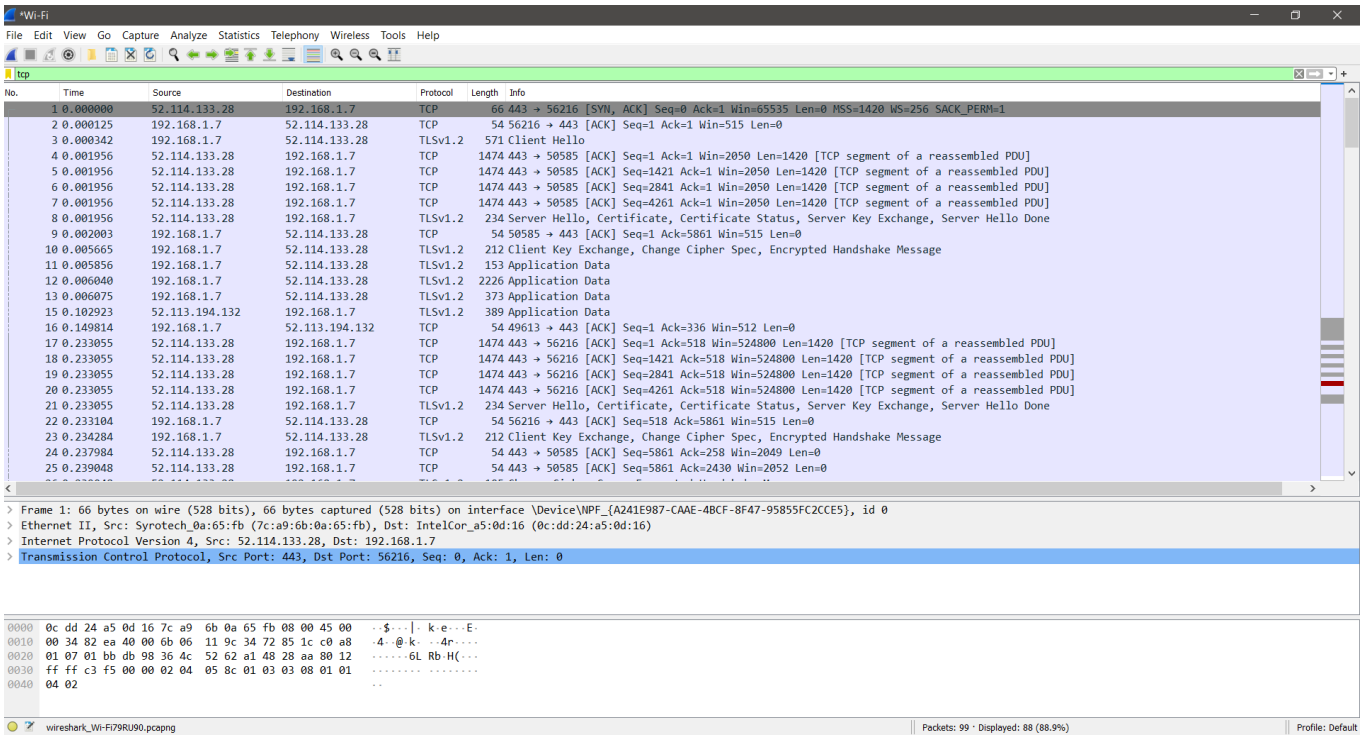
Once we have completed the intro steps and finished the capture process, the Wireshark main window should be alive with data. As a matter of fact, we might get overwhelmed by the amount of data that

appears, but it will all start to make sense very quickly as we break down the main window of Wireshark – one piece at a time.

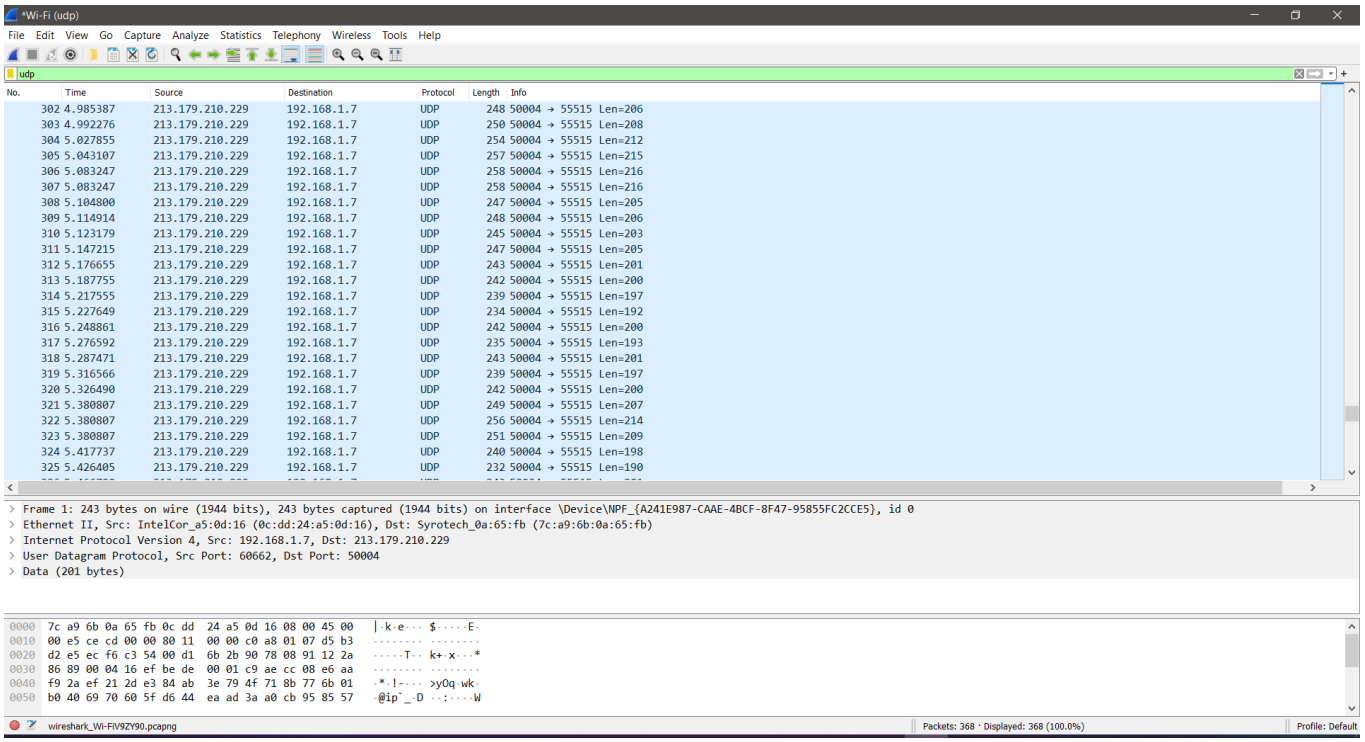
Capturing from WiFi:



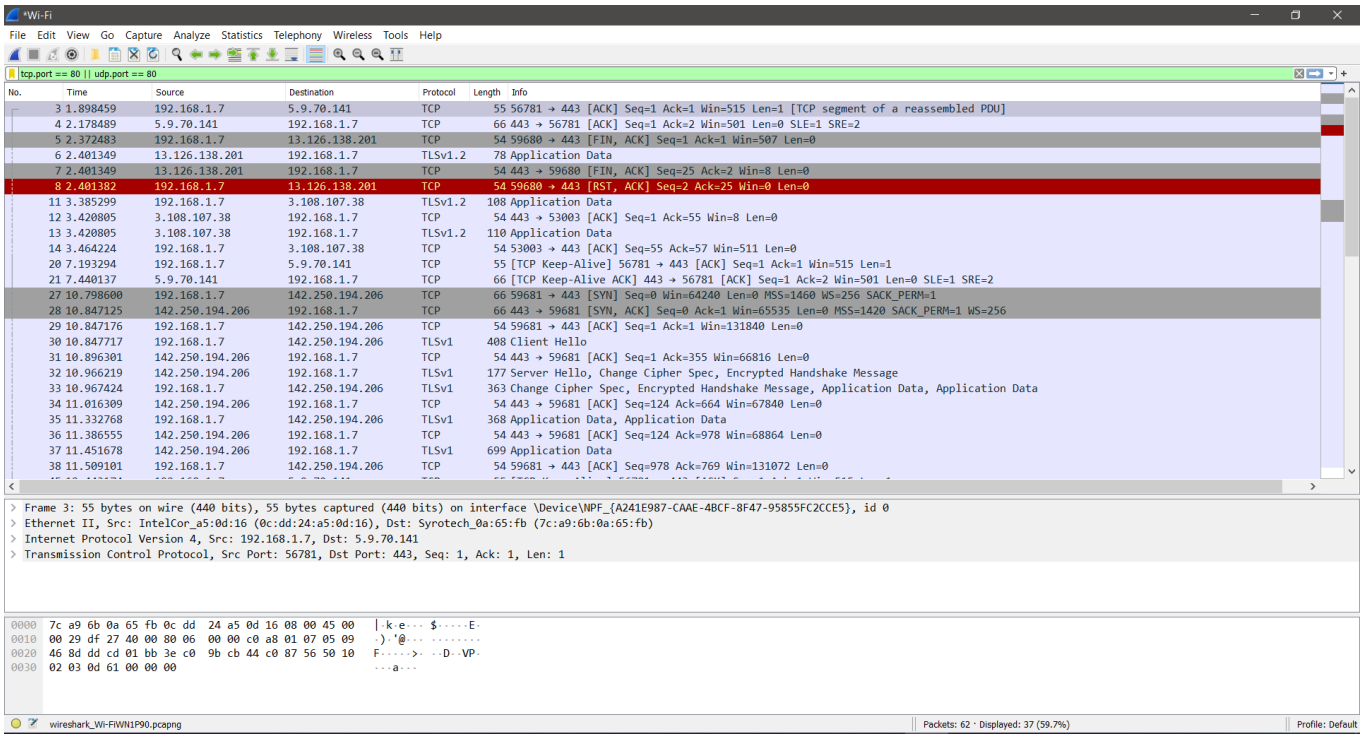
Filter TCP:



Filter UDP:

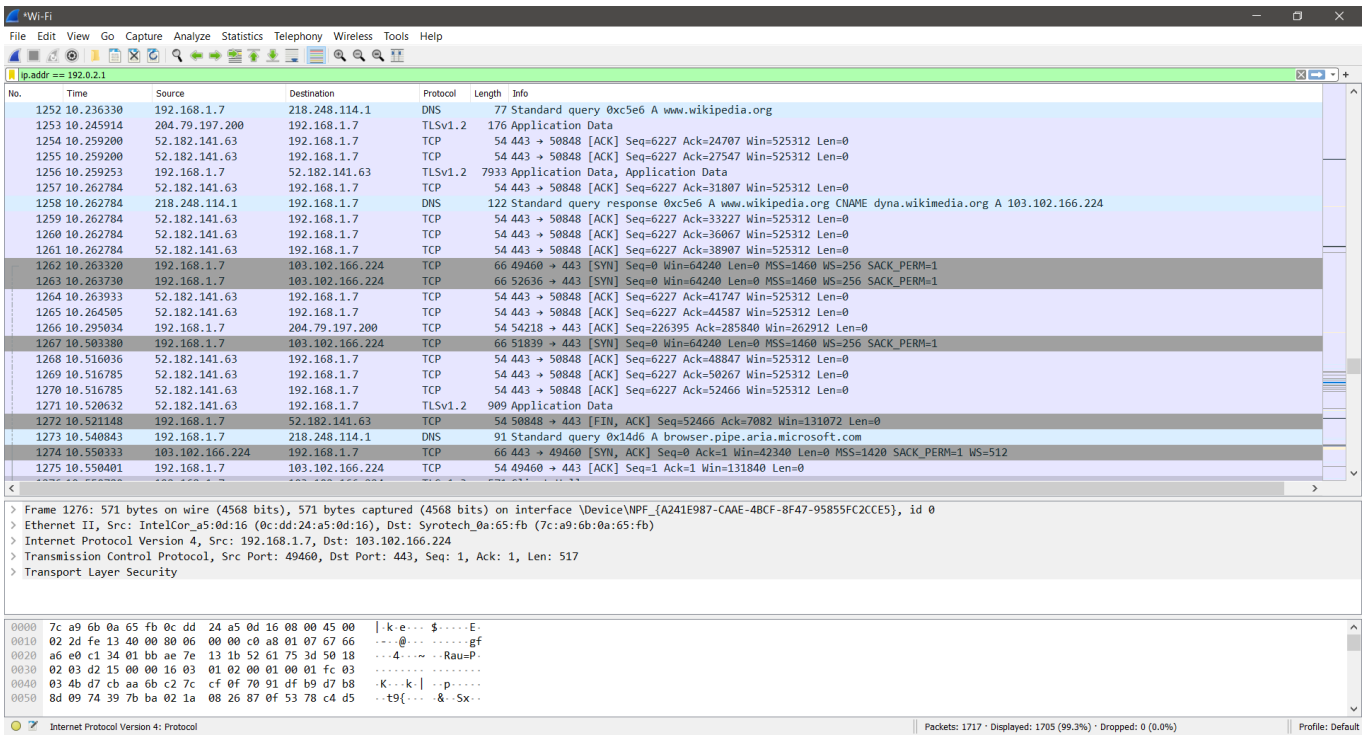


Filter TCP Port 80, UDP Port 80:



IP address 192.168.1.7

(Displays all traffic for the entered subnet, this will match on source or destination)



Conclusion: By usage of Wireshark, we can track and see all the possible packets, and the main focus of this tool is observing the data traffic within a network, as has been demonstrated here. Such a tool thus allows the user to examine his/her own computer for protocol errors and problems within the network architecture.
