CS212 - Computer Networks

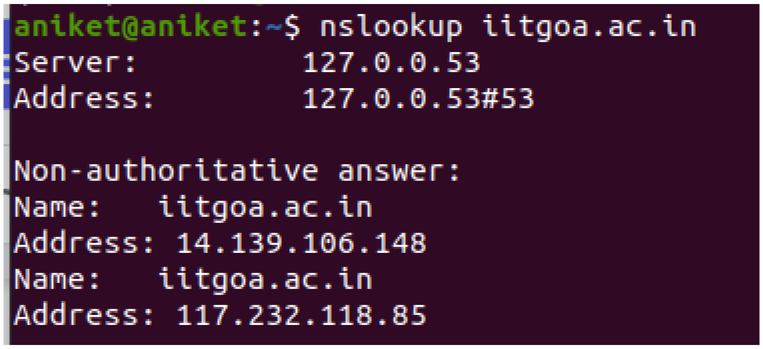
Name - ANIKET CHAUDHRI
ADARSH ANAND
Date - Sep 1, 2022
Course instructor - Neha Karanjkar
TA - Tushar Lone

LAB 2: Wireshark

Read up about Wireshark in the introductory reference material provided to you.

7. Find out the IP address of “www.iitgoa.ac.in”. Now start up wireshark selecting “any” interface.

Apply a filter “ip.addr == <the ip address you found for iitgoa>” for example, “ip.addr==10.250.36.36”. Now, open a web browser and open IIT Goa’s website. Observe the traffic captured in Wireshark for this filter.



```
aniket@aniket:~$ nslookup iitgoa.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   iitgoa.ac.in
Address: 14.139.106.148
Name:   iitgoa.ac.in
Address: 117.232.118.85
```

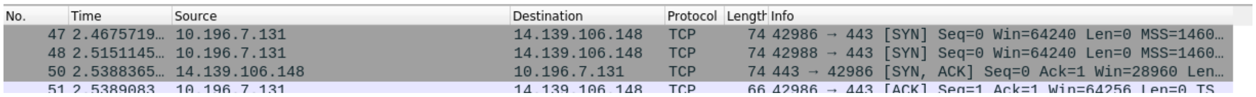
a) Look out for the SYN, SYN/ACK, ACK sequence of packets. What protocol is being used at the Transport Layer?

Ans.

A 3-way Handshake is performed over TCP in the following manner:

1. Client (my computer) sends a request to the iitgoa server with seq=0
2. Server responds with a seq=0 and ack (acknowledgement) flag=1
3. Client again responds to server with seq=1 and ack=1 to confirm successful connection

Protocol used in the transport layer is TCP.



No.	Time	Source	Destination	Protocol	Length	Info
47	2.4675719…	10.196.7.131	14.139.106.148	TCP	74	42986 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460…
48	2.5151145…	10.196.7.131	14.139.106.148	TCP	74	42988 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460…
50	2.5388365…	14.139.106.148	10.196.7.131	TCP	74	443 → 42986 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len…
51	2.5389083	10.196.7.131	14.139.106.148	TCP	66	42986 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS

b) Examine the first SYN packet. Observe how the packet corresponding to each layer of The TCP/IP stack is wrapped inside the packet of the lower layers. Examine the IP datagram and its header. What are the source and destination IP addresses for this packet? Check if the destination IP address matches that of iitgoa.ac.in. List your observation.

Ans.)

1. Transport Layer: Using TCP, Source Port: 38478, Destination Port: 443
2. Network Layer: IPv4, Header length: 20 bytes, Source: 10.196.7.131, Destination: 117.232.118.85
3. Ethernet: 14 bytes, Source MAC address: IntelCor_c3:16:67, Destination MAC address: ExtremeN_9a:82:da
4. Link layer: 74 bytes, Interface wlo1

IP datagram:
IPv4, Length 60 bytes, Identification flag=0xe8a9, Don't fragment flag=1, Time to live=64, Protocol: TCP, checksum=0x538e, Source: 10.196.7.131, Destination: 117.232.118.85

Destination address matches with that of IIT Goa address

c) Examine the transport-layer segment in the first SYN packet. What are the source and the destination port numbers for the first SYN message?
Ans.) Source Port: 38478, Destination Port: 443

d) Now remove all filters, and take a broad view of all packets flowing through the interface. What kind of packets make up a majority of the traffic to your computer/device?
Ans.) TCP packets make up the majority of the traffic and in ubuntu wireshark, ip.src == 185.125.190.36 is the most frequent ip address communicated which when passed through reverse DNS gives canonical.com (Publisher of Ubuntu)

8. In wireshark, you can apply a filter that displays packets only belonging to a certain protocol (such as TCP or UDP) as follows:

Two or more conditions can be combined using and/or to create more complex filters. For example:

a) Now, you wish to find out whether YouTube operates over the TCP protocol or the UDP protocol. Open YouTube in Firefox browser and filter out its traffic in Wireshark using the appropriate IP address in the filter. Observe the packets. Does YouTube use TCP or UDP?

Ans.) In Google Chrome, Youtube server (172.217.166.78) is transferring data over TCP protocol. While in Firefox, the data is exchanged over both UDP and TCP protocol

b) Does your conclusion change if you open YouTube in Google Chrome, instead of Firefox? List your observations. Check if your conclusion is correct, using a web search about what protocol YouTube actually uses.

Ans.) Yes, according to wireshark, youtube uses UDP when accessed through Firefox and TCP when accessed through Chrome.

From web search, Youtube uses TCP but according to a project paper “Video Streaming Traffic Study in India”, Youtube uses both UDP and TCP with 62.5% sessions using UDP and only 37.5% using TCP.

9. [Bonus question] Try connecting two different devices in the same network. For example, connect your mobile phone on the same network as your laptop. Apply the filter ip.addr=<other device’s IP addr>. Check if you can sniff packets meant for another device on the same local network.

Ans.)

Yes, I was able to sniff packets meant for another devices (for eg. my mobile). The steps I followed were:

1. Change the network interface (wlo1) mode to monitor
2. Start sniffing packets
3. Look for EAPOL protocol packets which meant a new device just connected to the same network
4. Get the MAC address of the newly connected device
5. Use that MAC address to filter out packets for that device

References

- Neha Ma'am slides
- Vinsloev Academy - Youtube
- Listen to Network packets on public WiFi
- Video Streaming Traffic Study in India
- TCP/IP Training IPv4 Header
- Linux man pages
- IPinfo.io

- The Complete Wireshark Course Beginner To Advanced [Complete Course]
- Learn Wireshark in 10 minutes - Wireshark Tutorial for Beginners
- Wireshark