Sheikh Ghulam Muhammad Ali 2020-10-0186

Assignment 1

Question 1:

http://www.descon.com/en/ has been used for this part

A) What location did you run this experiment from? (e.g. Home or some building on campus).

Home

B) Using the captured information only; what is the IP address of your machine?

IP address shown for machine is private type which is 192.168.0.101.

C) What is the IP address of the Server hosting website? How did you find it from the captured data? A very brief answer is needed.

IP address of the Server hosting descon website is 166.62.12.228. It can be found in details of IPv4 section of packet in wireshark.

D) Do you also see other source and destination IP addresses in the packet trace? What do you think are these?

Yes! There are multiple reasons. Some are packets for communication between router and machine.

E) Will the captured packet trace show a different IP address for your machine if you change your location (to another building on campus or a different home location)?

Public IP can change from session to session, but private IP will remain same on same network. But private IP address will change if I change my local network location.

F) Will the captured packet trace show a different IP address for website if you change your location (to another building on campus or a different home location)?

It depends on scenario. Usually, servers have static IP. So, if I'm connecting to same server, then its IP won't be different. But if machine gets connected to a different server hosting same website, then two IPs will be different. Two servers won't have same IP addresses.

G) What are the source and destination hardware addresses (or physical addresses or MAC addresses) in the http GET request? Which one belongs to your machine? To which machine/device does the other belong?

Since servers are host, we cannot directly access their mac address. Anyhow, in GET request, my machine is source which has machine address 60:14:B3:XX:XX:XX. Other mac address

70:4f:57:XX:XX:XX belongs to router I’m connected with which is destination in Ethernet II section.

H) What are the source and destination hardware addresses in the http response? Which one belongs to your machine?

Same addresses as in previous question but now source and destination is exchanged as now my machine is destination (mac address 60:14:B3:XX:XX:XX) and source is router (mac address 70:4f:57:XX:XX:XX).

I) What are the source and destination IP addresses in the http response? Which one belongs

to your machine? To which machine/device does the other belong?

In http response., Source IP address is 166.62.12.228 which belongs to server hosting descon website. Destination IP address is 192.168.0.101 which belongs to my machine.