Telecome 4   200027 R   Group 02

Group 01 – 200010J
200014B

Task 02

time taken = received time – sent time

before browsing data cleared

time taken =

= 05:47:47.219781 – 05:47:46.955699

= 0.264082 s

After browsing data cleared

time taken =

= 13:21:21.908404 – 13:21:21.633622

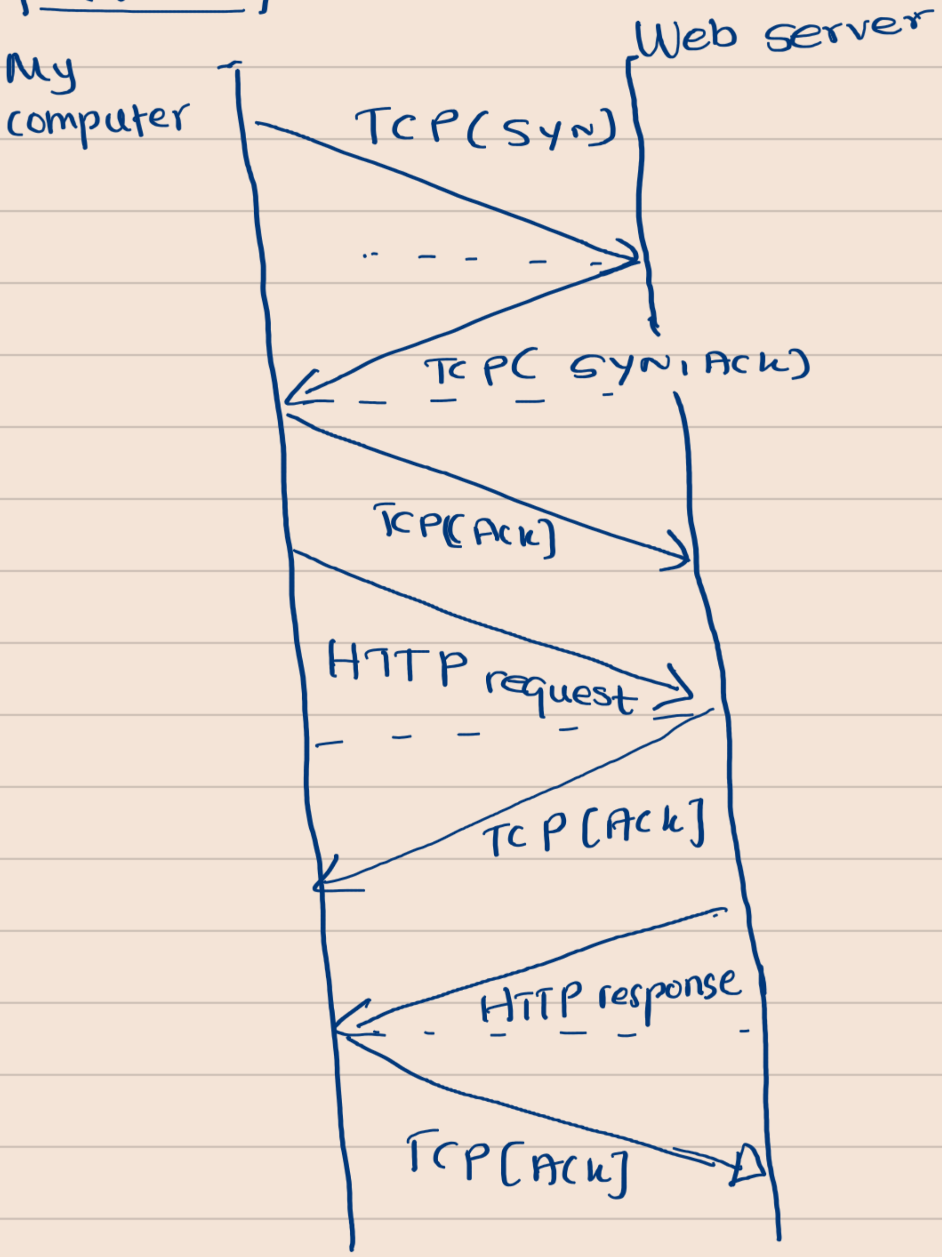
= 0.274782 s

Task 03

IP address of the gain.cs.umass.edu
= destination IP address of request
= 128.119.245.12

My computer's IP address
= Source IP address of request
= 192.168.179.187

Task 04



Task 05

DNS , SSDP, ICMP , TCP

Task 06

New destinations

192.248.126.145
192.168.179.48
35.197.154.200

New protocols

DNS : DNS server translate requests for names into IP addresses

SSDP : discover plug and play devices
SSDP uses unicast and multicast address

ICMP : used to determine if data is getting to its destination and at the right time

QUIC : experimental transport layer network protocal designed by Google. reduce latency compared to that of TCP

Task 07

wireshark available in multiple platforms like windows and UNIX. wireshark is the software that analysis packets sent throughout a network. we can observe packets and the details with in the packets. wireshark has so many key features such as, it can catch packets in a real-time network. wireshark can save packets and the packets are shown on a very clear GUI

we can see packets travelling through the network from the 'source' and 'destination' address. The protocol column shows, us which protocol is being used with in the packet and further information about it. we can clearly see the packet in detail and easily identify the situation. we capture traffic from a router, server or another computer in a different location on the network.

We can see frame detail, Ethernet details of source and destination, Internet protocol Version, TCP details HTTP details by clicking a packet in the wireshark captures. everything was clearly showed for us by instructors and that was very helpful.

As a improvement for us, more exercises will be usefull to understand the role doing by other protocols. Then we can learn to analyse in detail those packet captures.