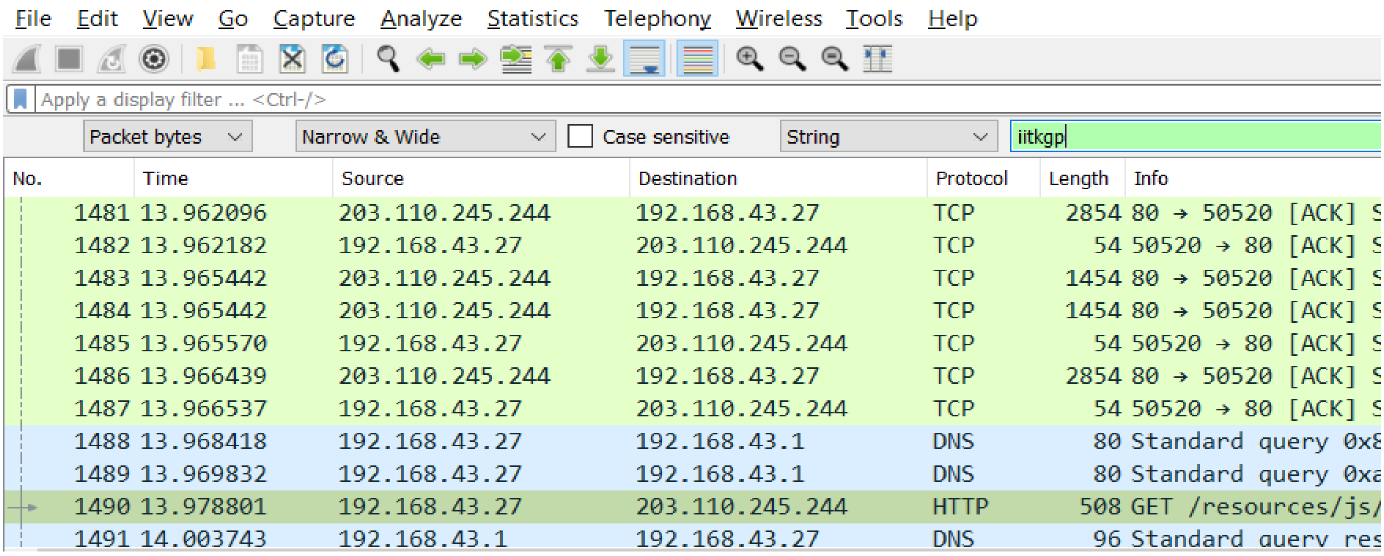
Q1 - Wireshark -> Statistics Menu -> Protocol Hierarchy

Q2 –

*Note: Maine pehle **nslookup** se ip nikala tha, doesn't work well if wireshark is using IPv6 for a website, isliye do the following*

1. Clear any display filter
2. Main toolbar me magnifying glass par click (button says Find a packet)
3. Change Filter to String, and select Packet Bytes. Search iitkgp

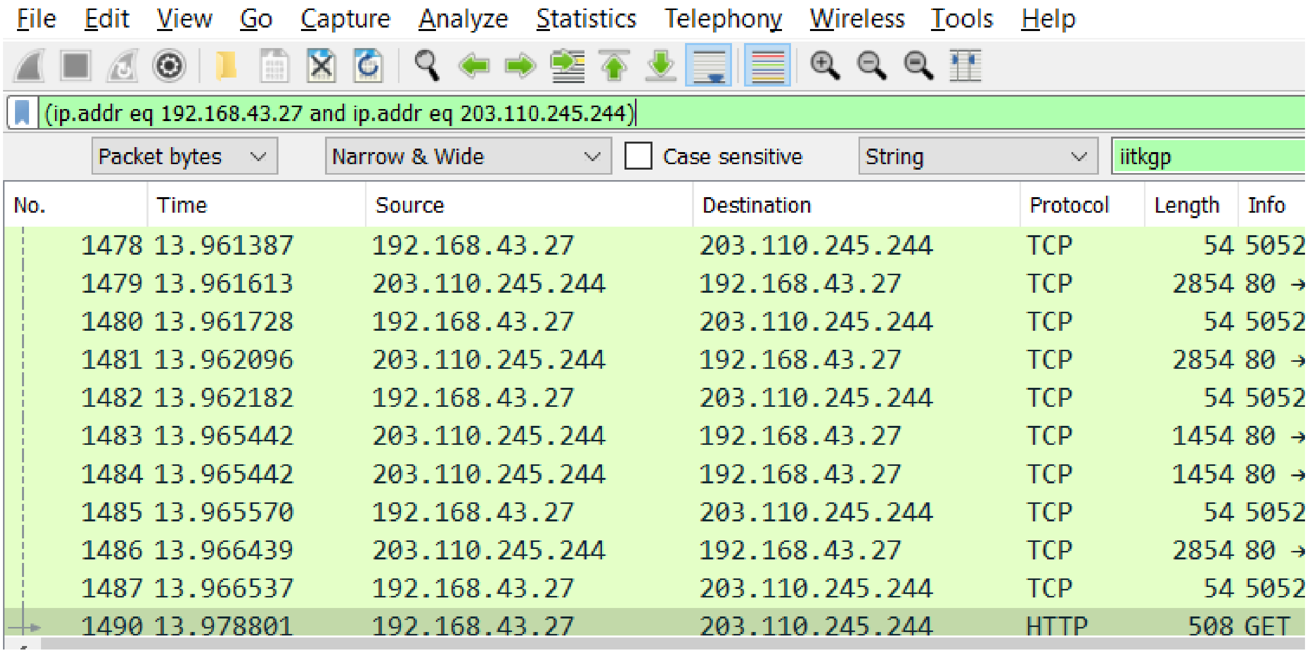


Packet bytes | Narrow & Wide | ☐ Case sensitive | String | iitkgp

No.	Time	Source	Destination	Protocol	Length	Info
1481	13.962096	203.110.245.244	192.168.43.27	TCP	2854	80 → 50520 [ACK] S
1482	13.962182	192.168.43.27	203.110.245.244	TCP	54	50520 → 80 [ACK] S
1483	13.965442	203.110.245.244	192.168.43.27	TCP	1454	80 → 50520 [ACK] S
1484	13.965442	203.110.245.244	192.168.43.27	TCP	1454	80 → 50520 [ACK] S
1485	13.965570	192.168.43.27	203.110.245.244	TCP	54	50520 → 80 [ACK] S
1486	13.966439	203.110.245.244	192.168.43.27	TCP	2854	80 → 50520 [ACK] S
1487	13.966537	192.168.43.27	203.110.245.244	TCP	54	50520 → 80 [ACK] S
1488	13.968418	192.168.43.27	192.168.43.1	DNS	80	Standard query 0x8
1489	13.969832	192.168.43.27	192.168.43.1	DNS	80	Standard query 0xa
1490	13.978801	192.168.43.27	203.110.245.244	HTTP	508	GET /resources/js/
1491	14.003743	192.168.43.1	192.168.43.27	DNS	96	Standard query res

4. Right click on the packet jiska protocol HTTP hai, Conversation filter -> TCP
5. Check the display filter bar, usme do filters honge, ek ip.addr wala, doosra tcp.port wala, remove the tcp.port filter

6. At this point aisa kuch dikhega display filter



(ip.addr eq 192.168.43.27 and ip.addr eq 203.110.245.244)

Packet bytes | Narrow & Wide | ☐ Case sensitive | String | iitkgp

No.	Time	Source	Destination	Protocol	Length	Info
1478	13.961387	192.168.43.27	203.110.245.244	TCP	54	5052
1479	13.961613	203.110.245.244	192.168.43.27	TCP	2854	80 →
1480	13.961728	192.168.43.27	203.110.245.244	TCP	54	5052
1481	13.962096	203.110.245.244	192.168.43.27	TCP	2854	80 →
1482	13.962182	192.168.43.27	203.110.245.244	TCP	54	5052
1483	13.965442	203.110.245.244	192.168.43.27	TCP	1454	80 →
1484	13.965442	203.110.245.244	192.168.43.27	TCP	1454	80 →
1485	13.965570	192.168.43.27	203.110.245.244	TCP	54	5052
1486	13.966439	203.110.245.244	192.168.43.27	TCP	2854	80 →
1487	13.966537	192.168.43.27	203.110.245.244	TCP	54	5052
1490	13.978801	192.168.43.27	203.110.245.244	HTTP	508	GET

7. Now you have filters from iitkgp displayed.
8. Statistics Menu -> Capture File Properties
9. Statistics -> Displayed se Packets and Bytes nikaal lo.

Do the same for cornell.edu.

Note: Cornell uses https, so you won’t be able to get read http content. So, in Step-3 right click on the packet jiske Info me **Client Hello** likha hai. Vaha se saare steps same.