

1.1 List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

-> ARP, TCP, DNS

No.	Time	Source	Destination	Protocol	Length	Info
1	12:47:51.337617	XiaomiCo_9e:9c:c3	Broadcast	ARP	42	Who has 192.168.43.153? Tell 192.168.43.1
2	12:47:51.337650	HonHaiPr_8c:90:55	XiaomiCo_9e:9c:c3	ARP	42	192.168.43.153 is at e0:06:e6:8c:90:55
3	12:47:54.925341	192.168.43.153	103.27.9.20	TCP	74	34573 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=995258 TSecr=0 WS=128
4	12:47:55.176068	192.168.43.153	192.168.43.1	DNS	74	Standard query 0x9f1d A www.iitd.ac.in
5	12:47:55.178179	192.168.43.1	192.168.43.153	DNS	90	Standard query response 0x9f1d A www.iitd.ac.in A 103.27.9.20
6	12:47:55.178615	192.168.43.153	103.27.9.20	TCP	74	34574 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM TSval=995321 TSecr=0 WS=128
7	12:47:55.414077	103.27.9.20	192.168.43.153	TCP	74	80 → 34574 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1260 SACK_PERM TSval=2043376632 TS...

1.2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

->

Time taken from when the HTTP GET message was sent until the HTTP OK reply was received is 12:47:56.188990 - 12:47:55.414218 = .774772 sec

No.	Time	Source	Destination	Protocol	Length	Info
9	12:47:55.414218	192.168.43.153	103.27.9.20	HTTP	491	GET / HTTP/1.1
21	12:47:56.171838	192.168.43.153	103.27.9.20	HTTP	591	GET /sites/default/files/ctools/css/2d4fe1c1412881a73110e50a115127de.css?Y HTTP/1.1
32	12:47:56.188990	103.27.9.20	192.168.43.153	HTTP	945	HTTP/1.1 200 OK (text/html)

1.3. What is the Internet address of the iitd.ac.in? What is the Internet address of your computer?

-> Internet address of the iitd.ac.in 103.27.9.20

Internet address of 192.168.43.153

No.	Time	Source	Destination	Protocol	Length	Info
9	12:47:55.414218	192.168.43.153	103.27.9.20	HTTP	491	GET / HTTP/1.1

1.4 4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

->

No.	Time	Source	Destination	Protocol	Length	Info
9	12:47:55.414218	192.168.43.153	103.27.9.20	HTTP	491	GET /

HTTP/1.1

Frame 9: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits)

Ethernet II, Src: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55), Dst: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3)

Internet Protocol Version 4, Src: 192.168.43.153, Dst: 103.27.9.20

Transmission Control Protocol, Src Port: 34574, Dst Port: 80, Seq: 1, Ack: 1, Len: 425

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

32	12:47:56.188990	103.27.9.20	192.168.43.153	HTTP	945	HTTP/1.1 200 OK (text/html)
----	-----------------	-------------	----------------	------	-----	--------------------------------

Frame 32: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)

Ethernet II, Src: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3), Dst: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55)

Internet Protocol Version 4, Src: 103.27.9.20, Dst: 192.168.43.153

Transmission Control Protocol, Src Port: 80, Dst Port: 34574, Seq: 8737, Ack: 426, Len: 879

[8 Reassembled TCP Segments (9615 bytes): #13(1248), #15(1248), #17(1248), #19(1248), #23(1248), #28(1248), #30(1248), #32(879)]

Hypertext Transfer Protocol

Line-based text data: text/html (709 lines)

5. Find the packet number that includes HTTP GET message for a file IITD-IRD-122-2017.pdf. Also find the length of the file in bytes and time when file is downloaded successfully.

->

478 is the packet number that includes HTTP GET message for a file IITD-IRD-122-2017.pdf.

-	478	12:49:13.44...	192.168.43.153	103.27.9.167	HTTP	602	GET /sites/default/files/jobs/project/IITD-IRD-122-2017.pdf	HTTP/1.1
+	503	12:49:13.70...	103.27.9.167	192.168.43.153	HTTP	243	HTTP/1.1 200 OK	(application/pdf)

Length of the file 18533 Bytes.

```
> Frame 503: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
> Ethernet II, Src: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3), Dst: HonHaiPr_8c:90:55 (e0:06:e6:
> Internet Protocol Version 4, Src: 103.27.9.167, Dst: 192.168.43.153
> Transmission Control Protocol, Src Port: 80, Dst Port: 33426, Seq: 44742, Ack: 4373, Len:
> [16 Reassembled TCP Segments (18897 bytes): #479(1248), #480(1248), #482(1248), #483(1248)
> Hypertext Transfer Protocol
  Media Type
    Media type: application/pdf (18533 bytes)
```