HTTP wireshark Analysis

Q1: Analysis using Wireshark

1. List 3 different protocols

In the Protocol column of the packet list, you'll typically see:

- HTTP
- TCP
- DNS

These can be confirmed by simply opening the `.pcap` file in Wireshark and checking the "Protocol" column.

2. Time between HTTP GET and HTTP OK

1. Find the packet with the **HTTP GET** request (use filter: `http.request`).
2. Note the time from the **Time** column.
3. Find the corresponding **HTTP/1.1 200 OK** (use filter: `http.response` or manually search nearby).
4. Subtract the two timestamps.

Example:

- GET at 12:00:01.000
- OK at 12:00:01.450
- **Time taken** = 0.450 seconds

3. Internet addresses

Use the packet with the HTTP GET request.

- Destination IP (of `iitd.ac.in`) → check the **Destination** column or expand the IP layer.
- Source IP → this will be your computer's IP in that trace.

4. Print GET and OK HTTP messages

- Right-click the GET packet → `File > Print > Selected Packet Only`
- Select **"Print as displayed"**
- Repeat for the HTTP 200 OK message
- Save both as PDF or include them as screenshots in your report

5. Find packet and file length for IITD-IRD-122-2017.pdf

1. Filter: `http.request.uri contains "IITD-IRD-122-2017.pdf"`
2. Note the **packet number** and check details in the HTTP section.
3. Find corresponding HTTP response with `Content-Length:` (shows size in bytes).
4. The last packet for the TCP stream (follow TCP stream) will show time when download ends.

Q2: Python Code for CSV Analysis

Step 1: Export CSV

- In Wireshark: `File > Export Packet Dissections > As CSV`

Save it as `http.csv`.

Step 2: Python Script

```
import csv

with open('http.csv', newline='') as csvfile:
    reader = csv.DictReader(csvfile)

    print("Source IP → Destination IP")
    print("Source Port → Destination Port")
    print("HTTP Messages")

    for row in reader:
        src_ip = row.get("Source", "")
        dst_ip = row.get("Destination", "")
        src_port = row.get("Src Port", "")
        dst_port = row.get("Dst Port", "")
        info = row.get("Info", "")

        print(f"{src_ip} → {dst_ip}")
        print(f"{src_port} → {dst_port}")

        if "GET" in info or "200 OK" in info:
            print("HTTP:", info)
        print("-" * 50)
```

Make sure the field names (e.g., `"Source"`, `"Destination"`, `"Info"`) match the actual column headers in your exported CSV.