Q1. Name different packet analyzers tools and explain the uses and features of any one packet analyzer tool in detail.

Ans. The different packet analyzers tools are:

1. Tcpdump
2. manage Engine NetFlow Analyzer
3. Solar Winds Network Performance Monitor
4. Network Miner
5. Fiddler
6. Paessler PRTG
7. Wireshark

→ Features:

1. Packet capture:
   - Captures packets on a network and converts them into a human-readable format.

2. Real-time analysis:
   - Provides a live view of network traffic

3. Filtering:
   - Allows users to focus on specific types of network traffic.

4. Graphical user interface (GUI):
   - Designed to be easy to use for both beginners and experts

→ Uses

1. It is used by network security engineers to

examine security problems.

2. It allows the users to watch all the traffic being passed over the network.

3. It is used by network engineers to troubleshoot network issues.

Q2. What is packet in computer network. Discuss different packet capturing expressions in Wireshark.

Ans. → Packet:

- A packet is a unit of data which is transmitted over a network between the origin and the destination.
- Network packets are small i.e. maximum 1.5 Kb for ethernet packets and 64 Kb for IP packets.

→ Packet capturing expressions:-

1. host: (capture the traffic through a single target)

2. net:
   - capture the traffic through a network or sub-network.
   - "net" can be prefixed with "src" or "dst" to indicate whether the data coming from or going to the target hosts.

3. port:
   - capture the traffic through or from a port.
   - "port" can be prefixed with "src" or "dst" to indicate whether the data coming from or going to the target port.

Q3. Discuss TCP and HTTP packet in detail.

Ans → TCP packet:

1. Source Port (16 bits):

- It holds the source / transmitting application's port number and helps in determining the application where the data delivery is ~~delivered~~ planned.

2. Destination Port (16 bits):

- This field has the port number of the transmitting application and helps to send the data to the appropriate application.

3. Acknowledgement number (32 bits):

- This field contains the upcoming sequence number and it acknowledges the feedback up to that.

→ HTTP packet:-

- The header of an HTTP ~~request~~ packet consists of a request line and header.
- The request line consists of the request type field, the URL field, and the HTTP version ~~field~~ field separated by spaces.
- When the length of an HTTP packet with body load exceeds the mss of TCP, the packet is fragmented.