Wireshark Demonstration

Aim: To observe data packets in real time and analyse them using wireshark

Procedure:

- Select one or more networks, then select Capture
- 3 panes will appear in captured data interface.
  - packet list pane (top section)
  - packet bytes pane (right section)
  - packet details pane (left section)
- Observe the packets with ARP, UDP etc protocols
- Observe the details.
- Press on ARP packet or UDP or any protocol to observe, source, destination, ttl, checksum and other details.
- Check IP of your system and observe which are the packets being sent through your side.

Observation:

→ In the details pane when captured a packe protocols and protocols fields of the selected packed could be seen.

→ In the bytes pane, raw data of selected packet in a hexadecimal view could be seen. Data which couldn't be printed were shown as a dot.

→ when right clicked on the hexadecimal data they were shown as bits.

Result for ARP packets –

Hardware type: Ethernet

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

opcode: request (1)

Sender MAC address: ExtremeN_7d:bf:69 (00:04:96:7b:bf:

Sender IP address: 10.124.0.9

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 10.124.10.201

No., time, source, destination, protocol, length info about a packet can be seen and analysed.