Year/Sem/Batch: III /V / P **Date:** 17-Sep-2026

Course Instructor : Dr. M.S.Karthika Devi, Asst. Prof, DCSE

Network Traffic Analysis Using Wireshark

Aim

To capture, filter, and analyze network packets using Wireshark and identify important parameters such as IP addresses, protocols, port numbers, packet length, and TCP connection establishment.

Workphase 1

Basic Packet Capture Using Wireshark

- Open Wireshark and select the active network interface (Wi-Fi/Ethernet).
- Start the packet capture.
- Open a web browser and access any website.
- Allow the packets to be captured for about 30 seconds.
- Stop the packet capture.
- Observe the captured packets in the packet list.
- Select any five packets and note the following details:
  - Source IP address
  - Destination IP address
  - Protocol
  - Packet length
- Select one packet and expand the protocol layers in the Packet Details pane.
- Record the observations in the given table.
- Save the captured packet file (.pcapng) for submission.

Observation Table

S.No.	Source IP	Destination IP	Protocol	Packet Length
1				
2				
3				
4				
5				

Workphase 2 : Identifying IP Information Using Wireshark

- Open the captured packet file in Wireshark.
- In the Display Filter box, enter:
- ip
- Press Enter to display only IPv4 packets.

- Select any one of the displayed packets.
- In the Packet Details pane, expand Internet Protocol Version 4 (IPv4).
- Identify and record the following information:
    - Source IP Address
    - Destination IP Address
    - IP Version
    - Header Length
    - Time to Live (TTL)
    - Protocol
    - Total Length
- Repeat the observation for at least five packets.
- Record the details in the observation table.

Observation Table:

S.No.	Source IP	Destination IP	Version	Header Length	TTL	Protocol	Total Length
1							
2							
3							
4							
5							

Workphase 3 : Identifying TCP Three-Way Handshake Using Wireshark

- Open the captured packet file in Wireshark.
- In the Display Filter box, enter:
    - tcp
- Press Enter to display only TCP packets.
- Identify a TCP connection between a client and server.
- Look for the first three packets containing the following TCP flags:
    - SYN
    - SYN, ACK
    - ACK
- Select the SYN packet and record the:
- Source IP address
- Destination IP address
- Source port
- Destination port
- Sequence number
- Select the SYN, ACK packet and record the corresponding details.
- Select the ACK packet and record the corresponding details.

Workphase 4: Identifying Source and Destination Port Numbers

- Open the captured packet file in Wireshark.
- In the Display Filter box, enter:
- tcp

- Press Enter to display TCP packets.
- Select any TCP packet from the packet list.
- In the Packet Details pane, expand Transmission Control Protocol.
- Identify the following fields:
    - Source Port
    - Destination Port
- Note the corresponding Source IP Address and Destination IP Address from
- the IPv4 section.
- Repeat the observation for at least five TCP packets.
- Record the details in the observation table.

S.No.	Source IP	Destination IP	Source Port	Destination Port	Protocol
1					TCP
2					TCP
3					TCP
4					TCP
5					TCP

Workphase 5: DNS Packet Analysis

- Open Wireshark and select the active Wi-Fi/Ethernet interface.
- Start the packet capture.
- Open a web browser and enter a website address, such as
- www.google.com.
- Allow the webpage to load completely and return to Wireshark.
- Stop the packet capture.
- In the Display Filter box, enter:
    - dns
- Press Enter to display only DNS packets.
- Select a DNS Query packet from the packet list.
- In the Packet Details pane, expand Domain Name System.
- Identify and record:
    - Source IP address
    - Destination IP address
    - DNS server address
    - Query name/domain name
    - Query type (A, AAAA, etc.)
    - UDP source port
    - UDP destination port
- Select the corresponding DNS Response packet.
- Examine the Answers section and identify the IP address returned for the
- requested domain.

Record the observations in the table below.

S.No.	Query/Response	Domain Name	Source IP	Destination IP	Query Type	Port
1	Query					
2	Response					

Task :

1. **Select any captured packet and explore its protocol details using Wireshark.**
   Identify the following layers from the **Packet Details** pane:
   - Frame
   - Ethernet
   - IP
   - TCP/UDP
   - Application layer protocol

   Record the information observed at each layer.

2. Using **Wireshark**, capture and analyze the network packets generated while accessing a website using HTTP/HTTPS.
3. **Capture TCP traffic and examine the TCP header fields.**
   Identify:
   - Source port
   - Destination port
   - Sequence number
   - Acknowledgement number
   - TCP flags
   - Window size
4. **Capture network traffic and identify different protocols appearing in the capture.**
   Identify at least **five different protocols**, such as:
   - DNS
   - TCP
   - UDP
   - TLS
   - ICMP

   Record the number of packets observed for each protocol.
5. Capture and analyze UDP packets using Wireshark.
   Identify:
   - Source IP
   - Destination IP
   - Source port
   - Destination port
   - Packet length

6. Apply Basic Filters

Use Wireshark display filters to isolate different types of packets.

Apply the following filters one by one:
- Ip
- tcp
- udp
- dns
- icmp