



Date: 21/08 /2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

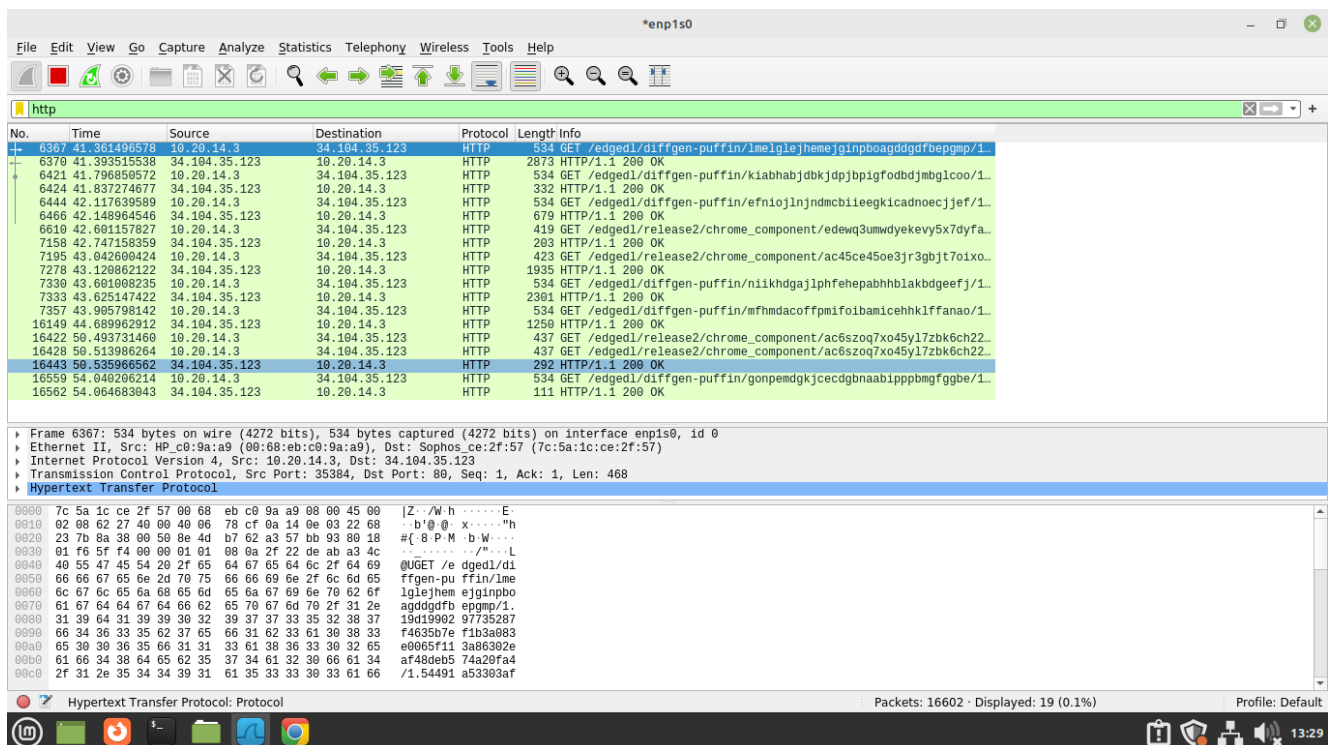
Practical Assignment #08:

1. Explain usage of Wireshark tool.

Wireshark is an open-source tool very widely used to traffic in a network in real time. It helps us to analyse the data packets flowing in the network thus providing valuable information about the network behaviour and its performance as well as security.

Wireshark is a network analyzer that captures and examines network traffic. It operates by capturing packets from a network interface or reading packets from a capture file. It then decodes and analyzes these packets, providing detailed information about the protocols, conversations, and network behavior.

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)





DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

Semester 5th | Practical Assignment | Computer Networks (2101CS501)

Date: 21/08/2024

Wireshark interface showing a packet capture of TCP traffic. The packet list shows a sequence of packets, including a reset (RST) packet. The packet details pane shows the structure of the captured packet, including the Ethernet II header, Internet Protocol Version 6 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the packet.

Frame 1418: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0

Interface id: 0 (any)

Encapsulation type: Linux cooked-mode capture (25)

Arrival Time: Aug 21, 2024 13:24:02.516603870 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1724226842.516603870 seconds

[Time delta from previous captured frame: 0.000003850 seconds]

[Time delta from previous displayed frame: 0.000003850 seconds]

[Time since reference or first frame: 43.670595088 seconds]

Frame Number: 1418

Frame Length: 76 bytes (608 bits)

Capture Length: 76 bytes (608 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: sll:ethertype:ipv6:tcp]

[Coloring Rule Name: TCP RST]

[Coloring Rule String: tcp.flags.reset eq 1]

Linux cooked capture

Internet Protocol Version 6, Src: ::1, Dst: ::1

Transmission Control Protocol, Src Port: 4101, Dst Port: 58308, Seq: 1, Ack: 1, Len: 0

Wireshark interface showing a packet capture of UDP traffic. The packet list shows a sequence of packets, including a standard query (PTR) packet. The packet details pane shows the structure of the captured packet, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane shows the raw data of the packet.

Frame 1511: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface any, id 0

Interface id: 0 (any)

Encapsulation type: Linux cooked-mode capture (25)

Arrival Time: Aug 21, 2024 13:24:05.161542933 IST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1724226845.161542933 seconds

[Time delta from previous captured frame: 0.017996128 seconds]

[Time delta from previous displayed frame: 0.017996128 seconds]

[Time since reference or first frame: 46.315534151 seconds]

Frame Number: 1511

Frame Length: 279 bytes (2232 bits)

Capture Length: 279 bytes (2232 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: sll:ethertype:ip:udp:data]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Linux cooked capture

Internet Protocol Version 4, Src: 10.20.59.111, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 64975, Dst Port: 5050

Data (235 bytes)



DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

Semester 5th | Practical Assignment | Computer Networks (2101CS501)

Date: 21/08/2024

