Assignment on Packet Snipping using Wireshark

Submitted To

Mr. Mohammad Zainal Abedin

Assistant Professor

Department of CSE, IIUC

Submitted By

Mohammad Forkan

Id: MC-231106

Introduction:

Wireshark is an open-source network protocol analysis software program.Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.

Capture Details:

The network interface is used for capturing :NDISDriver2016D879B022

Used Channel 1(2.4GHz)

Channel width:20Mhz

Summary of Captured Packets:

Total number of packets captured: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Breakdown of packet types (TCP, UDP, ICMP, etc.).

Top Talkers:

96.45.83.61

192.168.0.113

52.149.21.60

20.114.189.135

20.78.118.165

51.104.15.252

Used Protocol:

TCP, ARP, SSDP, DNS, TLSV1.2 ,MDNS, QUIC.

Frame 4:

54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Section number: 1

Interface id: 0 (\Device\NPF_{D2AC0D25-48E6-41E2-86DF-807F9D8C849F})

Encapsulation type: Ethernet (1)

Arrival Time: Jan 1, 2024 22:13:31.864357000 Bangladesh Standard Time

UTC Arrival Time: Jan 1, 2024 16:13:31.864357000 UTC

Epoch Arrival Time: 1704125611.864357000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 2.203871000 seconds]

[Time delta from previous displayed frame: 2.854491000 seconds]

[Time since reference or first frame: 2.854491000 seconds]

Frame Number:

Frame Length: 54 bytes (432 bits)

Capture Length: 54 bytes (432 bits)

Ethernet II,

Src: LiteonTechno_79:b0:22 (20:16:d8:79:b0:22),

Dst: TpLinkTechno_08:58:f2 (c0:25:e9:08:58:f2)

Destination: TpLinkTechno_08:58:f2 (c0:25:e9:08:58:f2)

Source: LiteonTechno_79:b0:22 (20:16:d8:79:b0:22)

Type: IPv4 (0x0800)

Internet Protocol Version 4,

Src: 192.168.0.113,

Dst: 20.106.86.13

Total Length: 40

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x5856 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.113

Destination Address: 20.106.86.13

Transmission Control Protocol

Source Port: 56516

Destination Port: 443

[Stream index: 1]

[Conversation completeness: Incomplete (36)]

[TCP Segment Len: 0]

Sequence Number: 1   (relative sequence number)

Sequence Number (raw): 79551120

[Next Sequence Number: 1   (relative sequence number)]

Acknowledgment Number: 1   (relative ack number)

Acknowledgment number (raw): 1305125858