

LAB 2: Examining Packets using Wireshark

PACKET SNIFFING USING WIRESHARK

Q1)

A) TCP

B) IP addresses of first SYN packet are:

Source IP address: 10.196.6.245

Destination IP address: 10.250.200.7

Yes, the destination IP address is matching with iitgoa.ac.in.

C) Source Port:58012

Destination port: 443

D) UDP is the protocol that is in majority.

Q2)

A) for chrome it is UDP

B) for Firefox it is both UDP and TCP

Q3)

A) url: daystar.ac.ke

Application layer: HTTPS, NA

Transport layer: TCP, src port: 59813, Dst port:80

Network layer: - IPv4, src: 10.196.6.245, Dst:41.204.160.15

Data link layer: - IPv4, src: 78:af:08:9b:2d:05 , Dst: 00:04:96:9a:82:da

Physical layer:- NA

B) Total Data packets: 170

Time taken: 0.431ms

Bonus question

Q4)

First we connected our both laptops with same mobile network, then from one laptop we took ip address with the help of ifconfig, then in second laptop in wireshark we filtered with the help of ip.addr==<ip address of first of laptop>, and then the packets that were flowing in first laptop were shown in the second laptops wireshark.

The image shows a Wireshark packet capture interface. The top pane displays a list of captured packets, filtered by 'ip.addr==192.168.250.232'. The packets are SSDP M-SEARCH requests from 192.168.250.232 to 239.255.255.250. The bottom pane shows a detailed view of the selected packet (No. 1074), which is an HTTP request. The packet details include Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. The packet list pane shows the packet details in a structured format.

No.	Time	Source	Destination	Protocol	Length	Info
1074	86.750151	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1086	87.746063	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1099	88.744424	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1107	89.745666	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2838	206.754058	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2847	207.767559	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2863	208.760745	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2872	209.769831	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5474	326.770683	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5476	327.777882	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5510	329.798570	192.168.250.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 1074: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface [Device]NPF_{20603247-1342-4C56-...} (01:00:5e:7f:ff:fa)

Ethernet II, Src: AzureWaveTec_dFica:5e (b4:8c:9d:df:ce:5e), Dst: IPmulticast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.250.232, Dst: 239.255.255.250

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 203

Identification: 0x06bb (1723)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 1

Protocol: UDP (17)

Header checksum: 0x06dc [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.250.232

Destination Address: 239.255.255.250

User Datagram Protocol, Src Port: 56972, Dst Port: 1900

HTTP Request HTTP-Version (http.request.version), 8 bytes

Packets: 5687 - Displayed: 11 (0.2%)

Profile: Default