

Date: 02/ 10 / 2023

Lab Practical #08:

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

Practical Assignment #08:

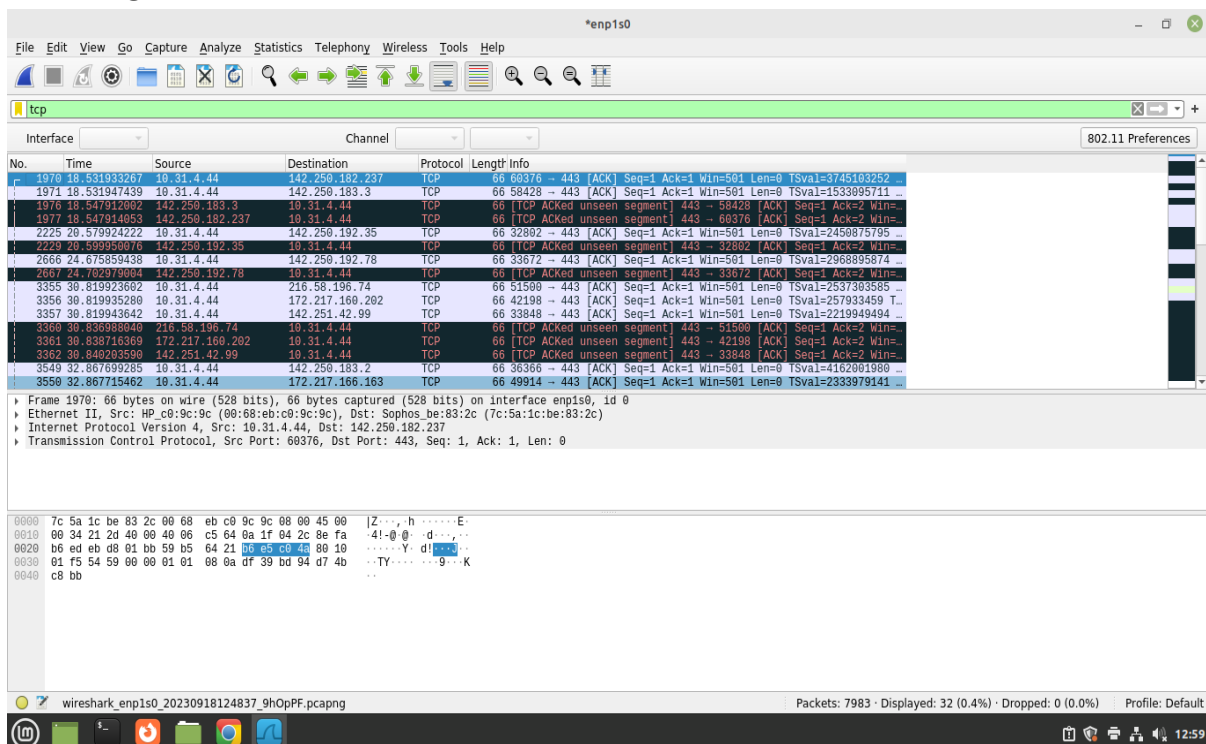
1. Explain usage of Wireshark tool.

➤ Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting.**

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyse dropped packets.
- It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

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

TCP



Wireshark packet capture interface showing TCP traffic. The packet list shows several TCP segments, including a SYN packet (Seq=1, Win=501) and an ACK packet (Seq=1, Win=501). The packet details pane shows the selected packet's structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.



DARSHAN INSTITUTE OF ENGINEERING & TECHNOLOGY

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

Date: 02/ 10 / 2023

UDP

Wireshark capture of UDP traffic on interface enp1s0. The packet list shows various DNS queries and responses. The packet details pane shows the structure of a UDP packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1954	18.412398925	fe80::ce9:b092:727d...	ff02::fb	MDNS	179	Standard query 0x0000 ANY MAC 04_31_25's iMac_smb_tcp.local...
1955	18.431932756	10.31.11.8	224.0.0.251	MDNS	71	Standard query 0x0000 A 10_04.local, "QM" question
1956	18.431934358	fe80::c265:ced7:beb...	ff02::fb	MDNS	91	Standard query 0x0000 A 10_04.local, "QM" question
1957	18.432239631	10.31.11.8	224.0.0.251	MDNS	71	Standard query 0x0000 AAAA 10_04.local, "QM" question
1958	18.432240495	fe80::c265:ced7:beb...	ff02::fb	MDNS	91	Standard query 0x0000 AAAA 10_04.local, "QM" question
1959	18.434308014	fe80::c265:ced7:beb...	ff02::1:3	LLMNR	85	Standard query 0xab0e A 10_04
1960	18.434309128	10.31.11.8	224.0.0.252	LLMNR	65	Standard query 0xab0e A 10_04
1961	18.434309601	fe80::c265:ced7:beb...	ff02::1:3	LLMNR	85	Standard query 0xcebe AAAA 10_04
1962	18.434309772	10.31.11.8	224.0.0.252	LLMNR	65	Standard query 0xcebe AAAA 10_04
1964	18.459914187	10.31.10.5	224.0.0.251	MDNS	71	Standard query 0x0000 A 10_04.local, "QM" question
1965	18.459915960	fe80::d96d:73c6:84e...	ff02::fb	MDNS	91	Standard query 0x0000 A 10_04.local, "QM" question
1966	18.459916189	10.31.10.5	224.0.0.251	MDNS	71	Standard query 0x0000 AAAA 10_04.local, "QM" question
1967	18.459916374	fe80::d96d:73c6:84e...	ff02::fb	MDNS	91	Standard query 0x0000 AAAA 10_04.local, "QM" question
1968	18.460942257	10.31.11.8	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1969	18.509958550	10.31.15.10	10.31.255.255	NBNS	92	Name query NB 10_04<00>
1972	18.535377363	10.3.16.8	224.0.0.251	MDNS	360	Standard query 0x0000 PTR airport_tcp.local, "QU" question ...

Frame 1969: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface enp1s0, id 0
Ethernet II, Src: 48:9e:bd:a4:49:f1 (48:9e:bd:a4:49:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.31.5.10, Dst: 10.31.255.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

0000 ff ff ff ff ff ff ff bd a4 49 f1 08 00 45 00H...I...E
0010 00 4e e2 13 00 00 00 11 3f 44 0a f1 05 0a 0a 1f .N.....?D.....
0020 ff ff 00 00 00 00 00 00 3a b5 c2 e5 f2 01 10 00 01:.....
0030 00 00 00 00 00 00 20 44 42 44 41 46 50 44 41 44D BDAPFPDAD
0040 45 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ECACACAC ACACACAC
0050 41 43 41 43 41 41 41 00 00 20 00 00 01 ACACAAA

User Datagram Protocol: Protocol Packets: 7983 · Displayed: 7387 (92.5%) · Dropped: 0 (0.0%) Profile: Default

IP

Wireshark capture of IP traffic on interface enp1s0. The packet list shows various DNS queries and responses. The packet details pane shows the structure of an IP packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1851	14.868485228	10.31.11.10	224.0.0.252	LLMNR	65	Standard query 0x649c AAAA 10_04
1852	14.868485408	10.31.11.10	10.31.255.255	NBNS	92	Name query NB 10_04<00>
1853	14.908008398	10.31.5.2	10.31.255.255	NBNS	92	Name query NB 10_04<00>
1854	14.917400219	10.31.5.9	224.0.0.251	MDNS	71	Standard query 0x0000 A 10_04.local, "QM" question
1855	14.917401513	fe80::7a9b:d1db:21f...	ff02::fb	MDNS	91	Standard query 0x0000 A 10_04.local, "QM" question
1856	14.917401734	10.31.5.9	224.0.0.251	MDNS	71	Standard query 0x0000 AAAA 10_04.local, "QM" question
1857	14.917401917	fe80::7a9b:d1db:21f...	ff02::fb	MDNS	91	Standard query 0x0000 AAAA 10_04.local, "QM" question
1858	14.939866638	10.31.5.6	224.0.0.251	MDNS	71	Standard query 0x0000 A 10_04.local, "QM" question
1859	14.939866896	fe80::1183:105:68a5...	ff02::fb	MDNS	91	Standard query 0x0000 A 10_04.local, "QM" question
1860	14.940393104	10.31.5.6	224.0.0.251	MDNS	71	Standard query 0x0000 AAAA 10_04.local, "QM" question
1861	14.940882358	fe80::1183:105:68a5...	ff02::fb	MDNS	91	Standard query 0x0000 AAAA 10_04.local, "QM" question
1862	14.941411581	fe80::1183:105:68a5...	ff02::1:3	LLMNR	85	Standard query 0x7aba A 10_04
1863	14.941934390	10.31.5.6	224.0.0.252	LLMNR	65	Standard query 0x7aba A 10_04
1864	14.941935230	fe80::1183:105:68a5...	ff02::1:3	LLMNR	85	Standard query 0x71f0 AAAA 10_04
1865	14.942479251	10.31.5.6	224.0.0.252	LLMNR	65	Standard query 0x71f0 AAAA 10_04
1866	14.976080242	10.31.3.18	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface enp1s0, id 0
Ethernet II, Src: 48:9e:bd:a4:49:6a (48:9e:bd:a4:49:6a), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 10.31.5.2, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 52893, Dst Port: 1990
Simple Service Discovery Protocol

0020 ff fa ce 9d 07 6c 00 b7 b5 df 4d 2d 53 45 41 521...M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 32 2e 31 00 0a 48 CH * HTTP/1.1 - H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239_255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 250:1900-MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a MX: 1 - ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 63 63 72 65 65 6e dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:service:dia
00a0 6c 3a 31 0d 0a 53 54 54 52 20 f1 47 49 4d 34 20 1:1-USERAGENT:
00b0 20 47 6f 6f 6f 65 20 43 68 72 6f 6d 65 2f 31 Google Chrome/2
00c0 31 36 2e 30 2e 35 38 34 35 2e 31 38 38 20 57 69 16.0.584.5.188 W
00d0 6e 64 6f 77 73 0d 0a 0d 0a ndows...

User Datagram Protocol: Protocol Packets: 2226 · Displayed: 1859 (83.5%) · Dropped: 0 (0.0%) Profile: Default