Batch:A2

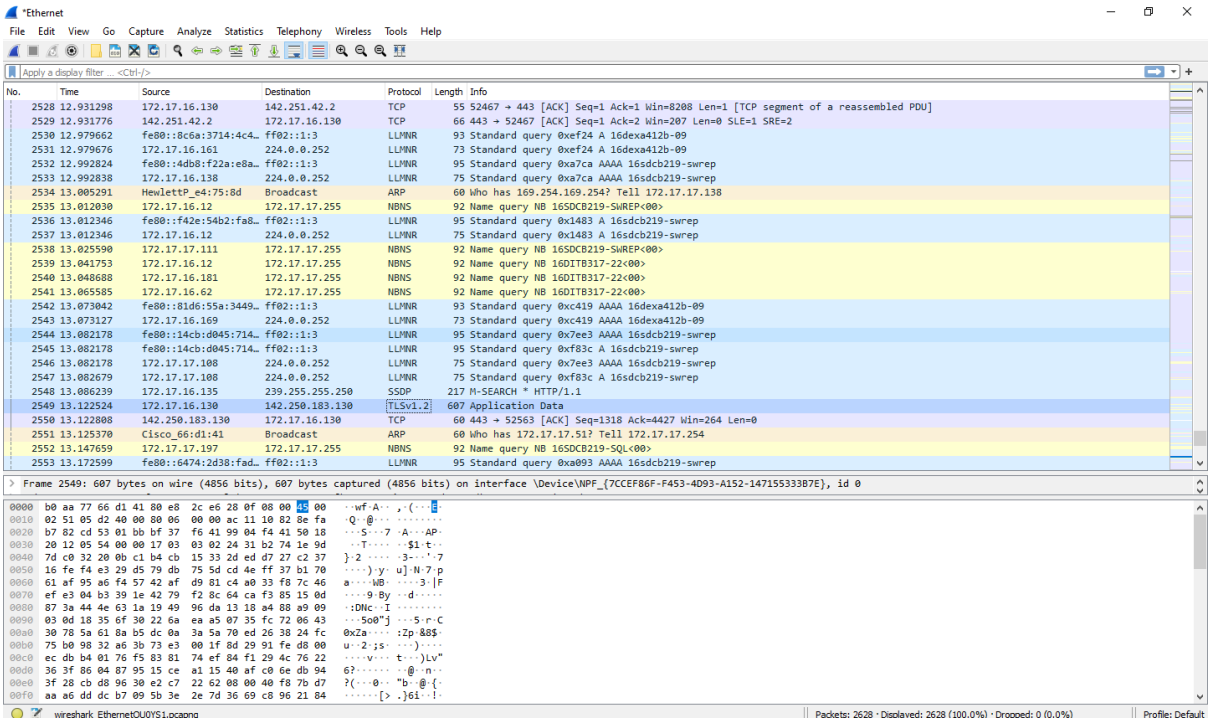
Roll Number: 16010421063 **Experiment Number:3**

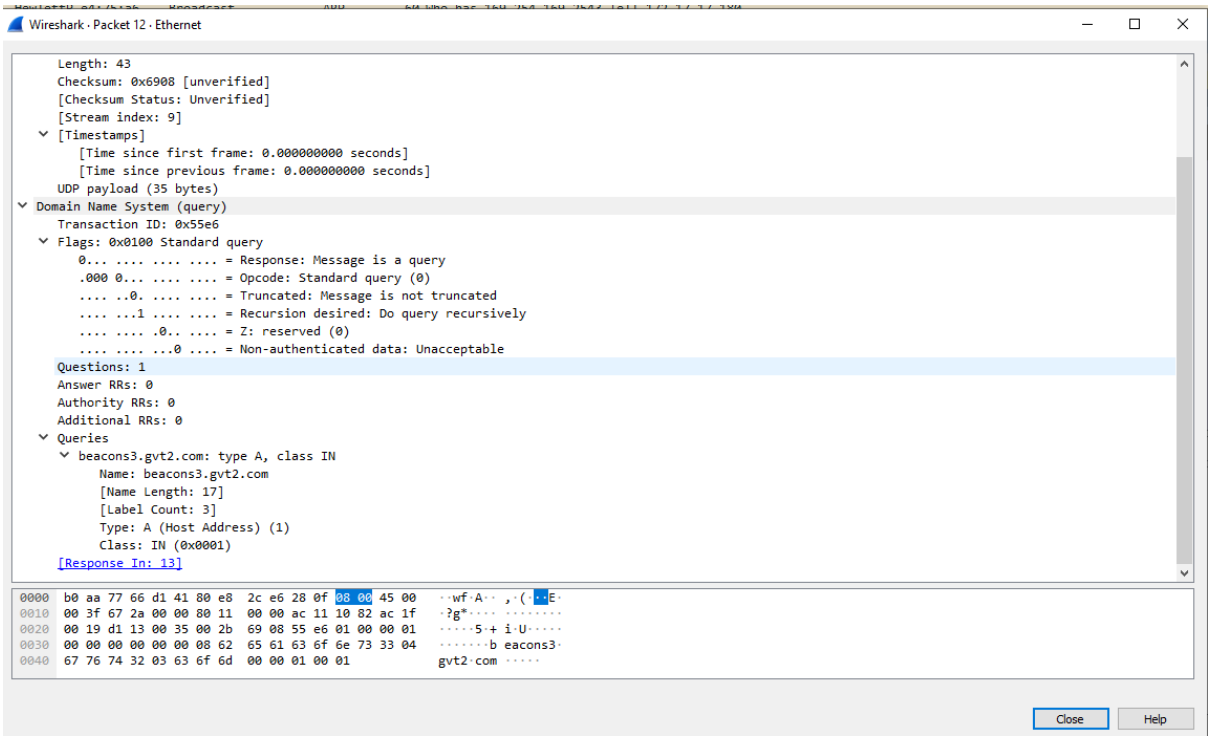
Name:Arya Nair

Title of the Experiment:Application layer protocols.

Program:

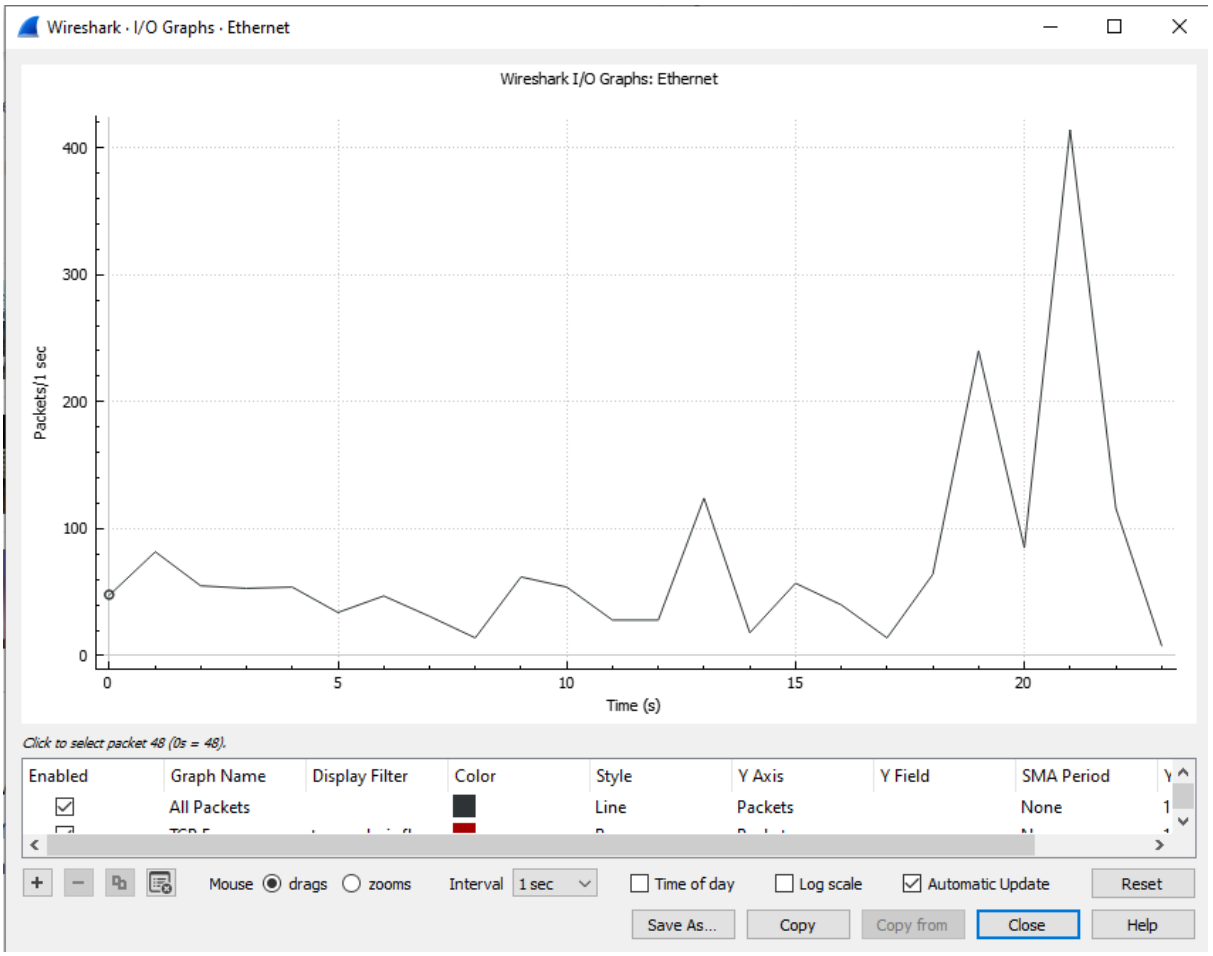
Output:



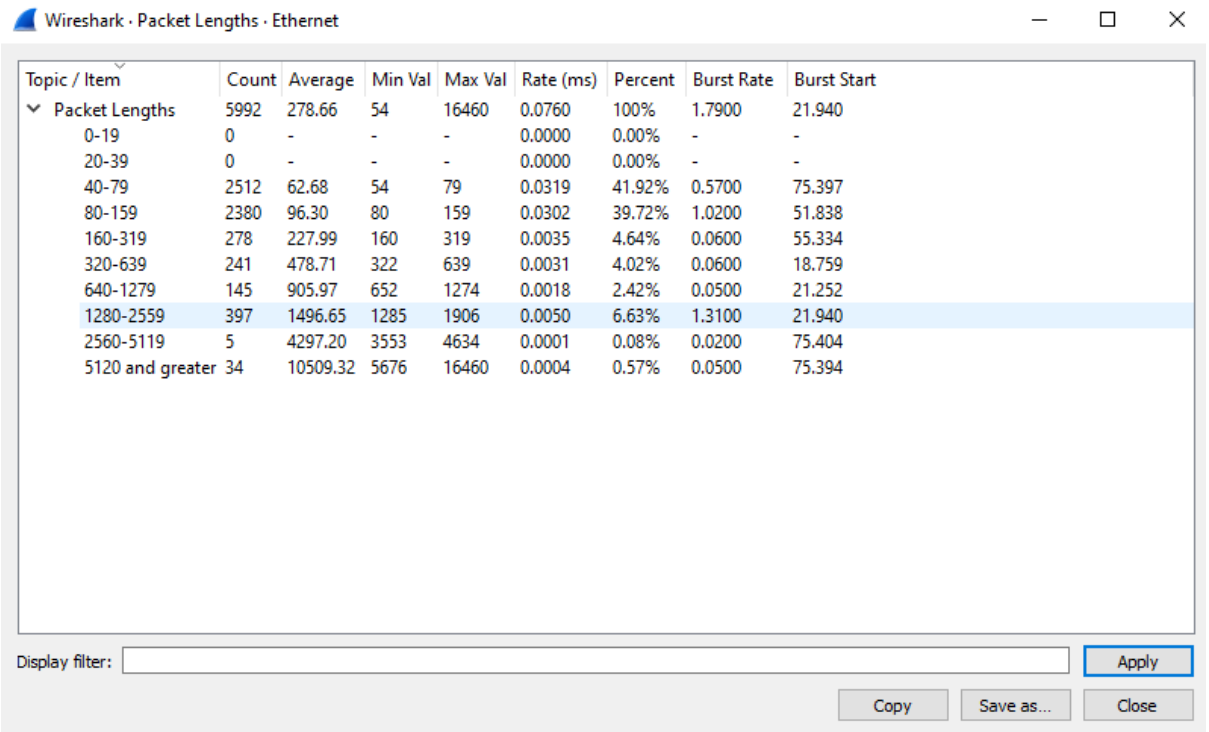


Identification- 0x55e6	**Flags-** **dns.flags.response- 0** **dns.flags.opcode- 0** **dns.flags.truncated- 0** **dns.flags.recdesired- 1** **dns.flags.z- 0** **dns.flags.checkdisable- 0**
number of questions- **Questions: 1**	**Answer RRs: 0**
Authority RRs: 0	**Additional RRs: 0**

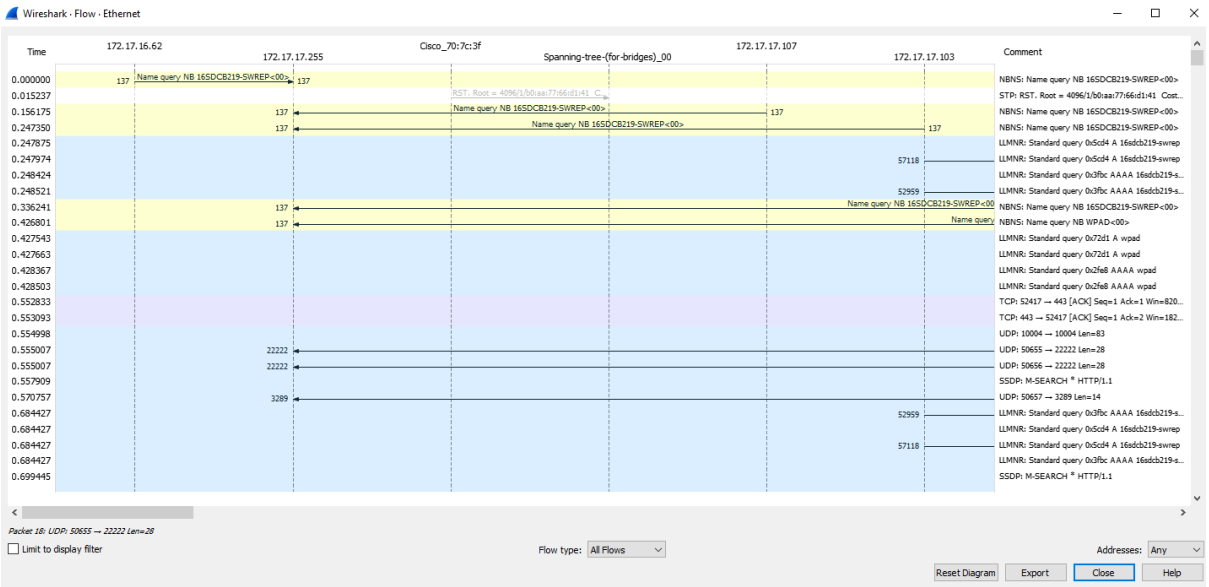
IO GRAPH



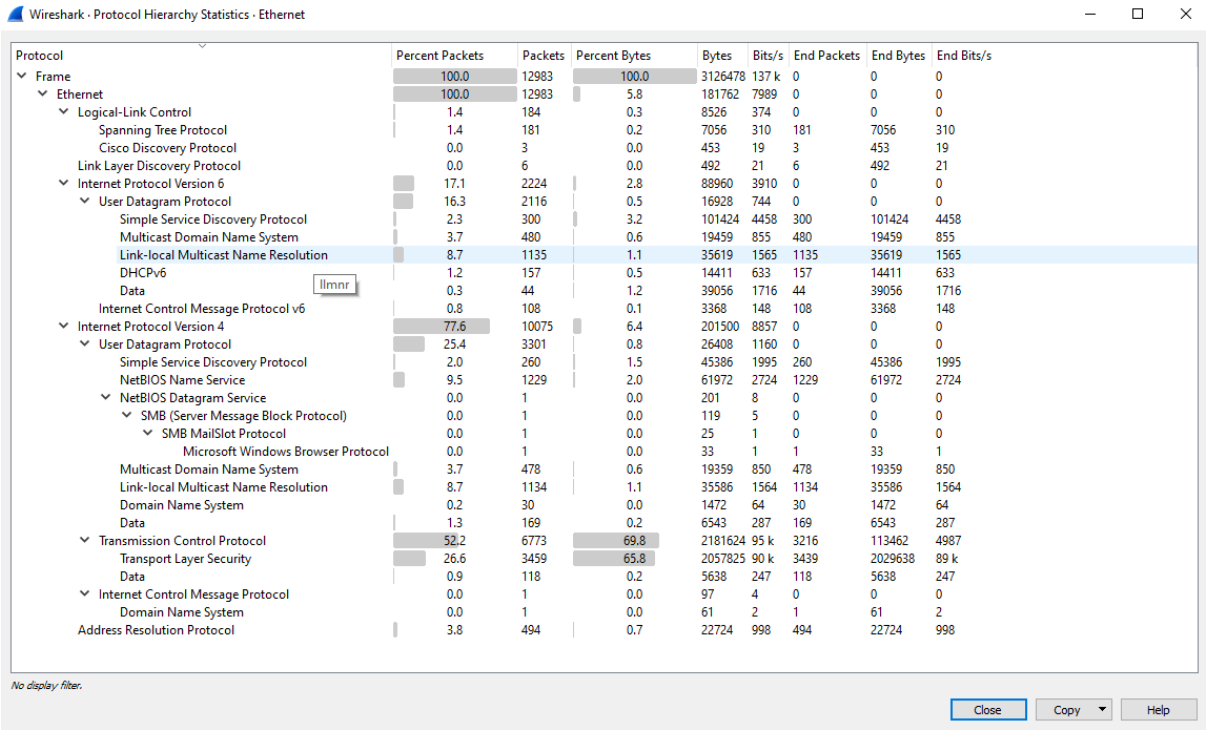
Packet Length



Flow

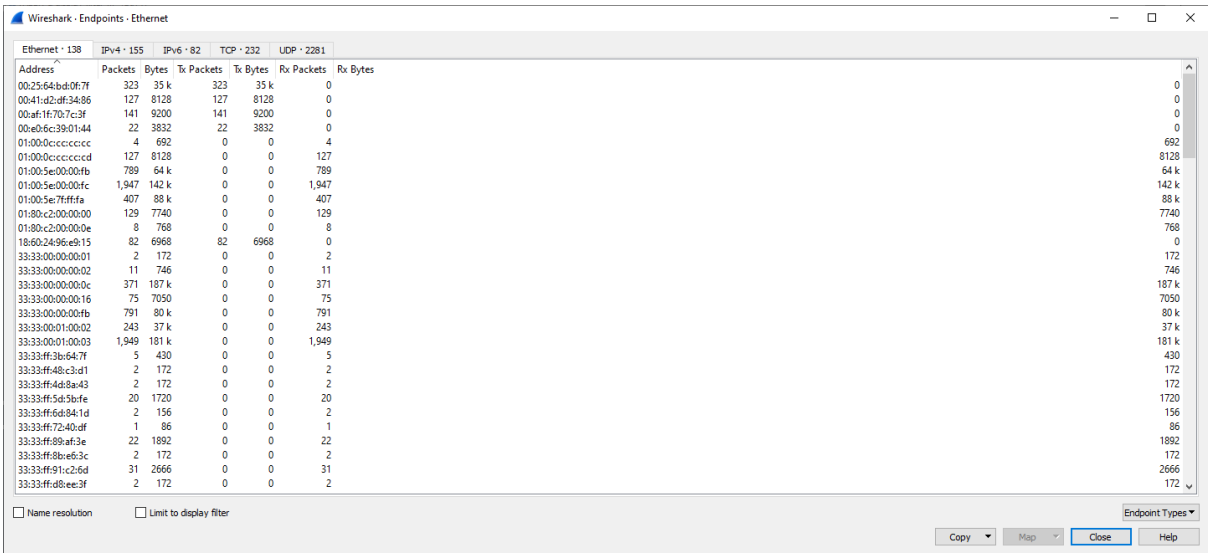


Protocol hierarchy



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	12983	100.0	3126478	137 k	0	0	0
Ethernet	100.0	12983	5.8	181762	7989	0	0	0
Logical-Link Control	1.4	184	0.3	8526	374	0	0	0
Spanning Tree Protocol	1.4	181	0.2	7056	310	181	7056	310
Cisco Discovery Protocol	0.0	3	0.0	453	19	3	453	19
Link Layer Discovery Protocol	0.0	6	0.0	492	21	6	492	21
Internet Protocol Version 6	17.1	2224	2.8	88960	3910	0	0	0
User Datagram Protocol	16.3	2116	0.5	16928	744	0	0	0
Simple Service Discovery Protocol	2.3	300	3.2	101424	4458	300	101424	4458
Multicast Domain Name System	3.7	480	0.6	19459	855	480	19459	855
Link-local Multicast Name Resolution	8.7	1135	1.1	35619	1565	1135	35619	1565
DHCPv6	1.2	157	0.5	14411	633	157	14411	633
Data	0.3	44	1.2	39056	1716	44	39056	1716
Internet Control Message Protocol v6	0.8	108	0.1	3368	148	108	3368	148
Internet Protocol Version 4	77.6	10075	6.4	201500	8857	0	0	0
User Datagram Protocol	25.4	3301	0.8	26408	1160	0	0	0
Simple Service Discovery Protocol	2.0	260	1.5	45386	1995	260	45386	1995
NetBIOS Name Service	9.5	1229	2.0	61972	2724	1229	61972	2724
NetBIOS Datagram Service	0.0	1	0.0	201	8	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	5	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	1	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	1	1	33	1
Multicast Domain Name System	3.7	478	0.6	19359	850	478	19359	850
Link-local Multicast Name Resolution	8.7	1134	1.1	35586	1564	1134	35586	1564
Domain Name System	0.2	30	0.0	1472	64	30	1472	64
Data	1.3	169	0.2	6543	287	169	6543	287
Transmission Control Protocol	52.2	6773	69.8	2181624	95 k	3216	113462	4987
Transport Layer Security	26.6	3459	65.8	2057825	90 k	3439	2029638	89 k
Data	0.9	118	0.2	5638	247	118	5638	247
Internet Control Message Protocol	0.0	1	0.0	97	4	0	0	0
Domain Name System	0.0	1	0.0	61	2	1	61	2
Address Resolution Protocol	3.8	494	0.7	22724	998	494	22724	998

Endpoint



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:25:64:bd:0f:7f	323	35 k	323	35 k	0	0
00:41:d2:df:34:86	127	8128	127	8128	0	0
00:af:1f:70:7c:3f	141	9200	141	9200	0	0
00:e0:6c:39:01:44	22	3832	22	3832	0	0
01:00:0c:cc:cc:cc	4	692	0	0	4	692
01:00:0c:cc:cc:cd	127	8128	0	0	127	8128
01:00:5e:00:00:fb	789	64 k	0	0	789	64 k
01:00:5e:00:00:fc	1,947	142 k	0	0	1,947	142 k
01:00:5e:7f:ff:fa	407	88 k	0	0	407	88 k
01:80:c2:00:00:00	129	7740	0	0	129	7740
01:80:c2:00:00:0e	8	768	0	0	8	768
18:60:24:96:e9:15	82	6968	82	6968	0	0
33:33:00:00:00:01	2	172	0	0	2	172
33:33:00:00:00:02	11	746	0	0	11	746
33:33:00:00:00:0c	371	187 k	0	0	371	187 k
33:33:00:00:00:16	75	7050	0	0	75	7050
33:33:00:00:00:fb	791	80 k	0	0	791	80 k
33:33:00:01:00:02	243	37 k	0	0	243	37 k
33:33:00:01:00:03	1,949	181 k	0	0	1,949	181 k
33:33:ff:3b:64:7f	5	430	0	0	5	430
33:33:ff:48:c3:d1	2	172	0	0	2	172
33:33:ff:4d:8a:43	2	172	0	0	2	172
33:33:ff:5d:5b:fe	20	1720	0	0	20	1720
33:33:ff:6d:84:1d	2	156	0	0	2	156
33:33:ff:72:40:df	1	86	0	0	1	86
33:33:ff:89:af:3e	22	1892	0	0	22	1892
33:33:ff:8b:e6:3c	2	172	0	0	2	172
33:33:ff:91:c2:6d	31	2666	0	0	31	2666
33:33:ff:d8:ee:3f	2	172	0	0	2	172

Post Lab Question- Answers (If Any):

1. What is the difference between Wireshark software and NMAP software?

Nmap is primarily chosen for the use case of network scanners. Network scanner enables information regarding groups, shares, services, usernames of the computers in the network to be fetched and saved for future processing.

Wireshark falls into the category of packet scanner. The objective is similar to network sniffing where network traffic that is a part of the entire larger network of the system is intercepted and logged for future processing.

2. At which of the OSI layer Wireshark runs?

Wireshark OSI layer 2. Layer 2 of The OSI Model: Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer.

3. Just write down the names of the softwares which have similar functionality as

Wireshark. (open source or proprietary)

1. **tcpdump**
2. **NetworkMiner**
3. **Packet Capture**
4. **Sysdig**
5. **CloudShark**
6. **Colasoft Capsa**

CO: Enumerate the layers of OSI model and TCP/IP model, their functions and protocols

---

Conclusion: We understood how to capture packets using wireshark . Mapped the various fields of packet header from wireshark to header diagram of DNS application layer. Also used various statistical tools available in wireshark

---