Computer Networks Laboratory

Assignment 2

Name: Anirban Das Class: BCSE-III Roll: 001910501077 Group: A3

Problem Statement:

Packet tracer and traffic analysis with Wireshark

OVERVIEW:

Wireshark is an open-source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

SYSTEM DETAILS:

OS: 64-bit Windows 10

Wireshark Version: 3.4.9

QUESTIONS:

1. **Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighboring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.**

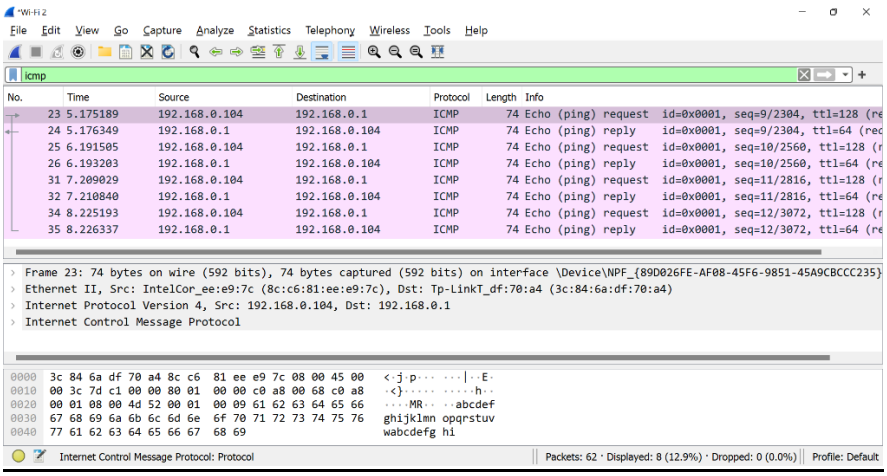
COMMAND PROMPT

```
PS C:\Users\ASUS> ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\ASUS>
```

WIRESHARK CAPTURES



The destination (the default gateway address of my machine) is 192.168.0.1 and the source address (the router ip) is 192.168.0.104.

2. **Generate some web traffic and:**
   a. **find the list the different protocols that appear in the protocol column in the unfiltered packet listing window of Wireshark.**
   b. **How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of day).**

   c. **What is the Internet address of the website? What is the Internet address of your computer?**

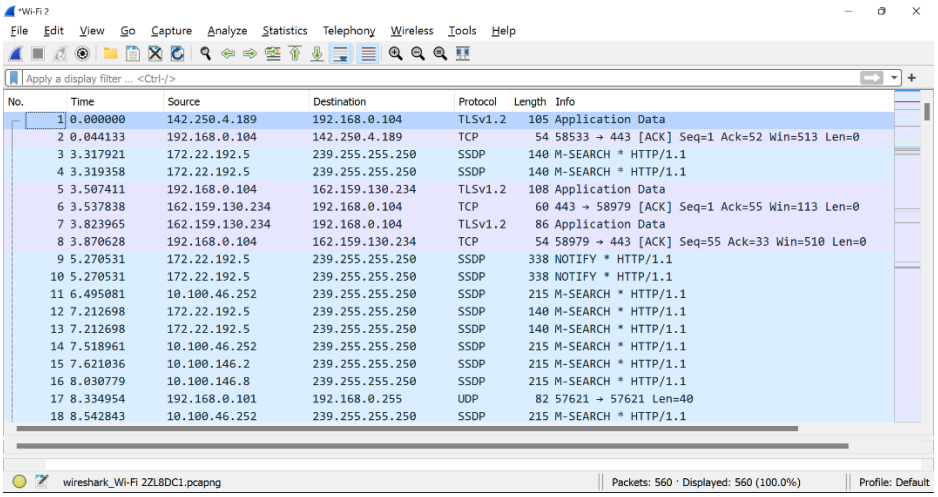
   d. **Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.**

   e. **Find out the value of the Host from the Packet Details Panel, within the GET command.**

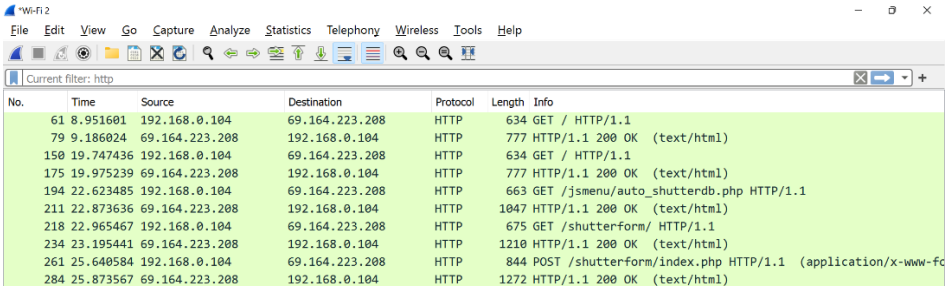
ANSWERS:

a. List of different protocols appearing in the Protocol column:
   1. UDP -> User Datagram Protocol
   2. TLSv1.3 -> Transport Layer Security (Version 1.3)
   3. TCP -> Transmission Control Protocol
   4. SSDP -> Multicast DNS
   5. QUIC -> Quick UDP Internet Connection
   6. DNS -> Domain Name System
   7. ARP -> Address Resolution Protocol
   8. ICMP -> Internet Control Message Protocol

WIRESHARK CAPTURES



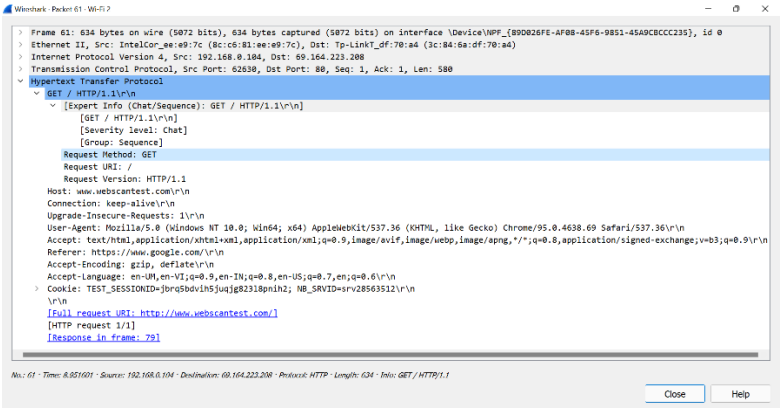
b.



Time taken from when HTTP GET was sent until the receipt of HTTP OK message = 9.186024 – 8.951601 = 0.234423s

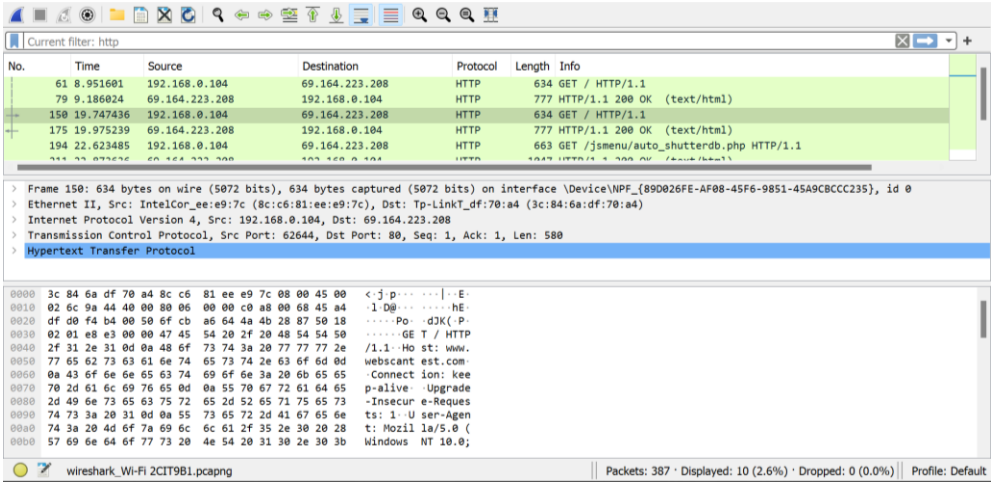
c. Internet address of the destination: 69.164.223.208
Internet address of my machine : 192.168.0.104

d.



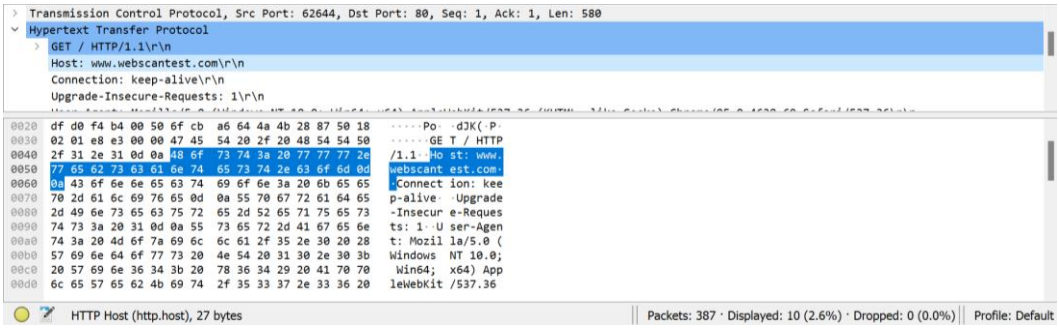
e. The value of the host is "www.webscantest.com\r\n" as seen in the above screenshot.

3. Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.



|-------HEX REPRESENTATION------| |----ASCII----|

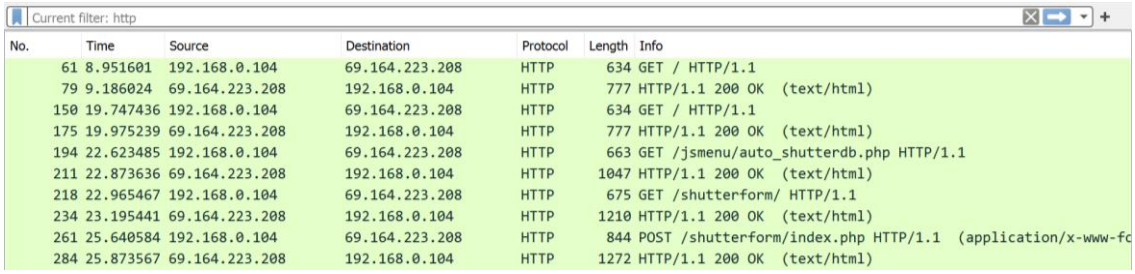
4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.



The highlighted portion of the HEX Representation of the packet is for the host parameter. The first 4 bytes are 48 6f 73 74.

5. Filter packets with http, TCP, DNS and other protocols.

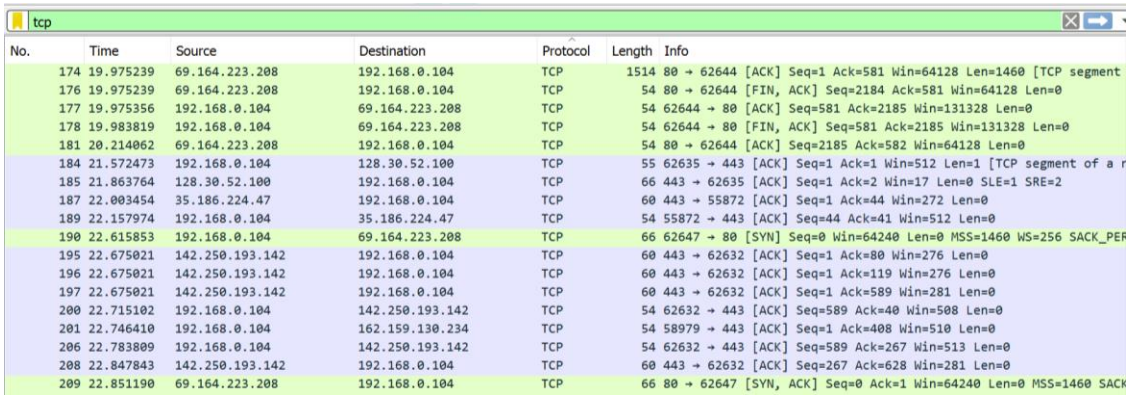
HTTP



Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
61	8.951601	192.168.0.104	69.164.223.208	HTTP	634	GET / HTTP/1.1
79	9.186024	69.164.223.208	192.168.0.104	HTTP	777	HTTP/1.1 200 OK (text/html)
150	19.747436	192.168.0.104	69.164.223.208	HTTP	634	GET / HTTP/1.1
175	19.975239	69.164.223.208	192.168.0.104	HTTP	777	HTTP/1.1 200 OK (text/html)
194	22.623485	192.168.0.104	69.164.223.208	HTTP	663	GET /jsmenu/auto_shutterdb.php HTTP/1.1
211	22.873636	69.164.223.208	192.168.0.104	HTTP	1047	HTTP/1.1 200 OK (text/html)
218	22.965467	192.168.0.104	69.164.223.208	HTTP	675	GET /shutterform/ HTTP/1.1
234	23.195441	69.164.223.208	192.168.0.104	HTTP	1210	HTTP/1.1 200 OK (text/html)
261	25.640584	192.168.0.104	69.164.223.208	HTTP	844	POST /shutterform/index.php HTTP/1.1 (application/x-www-fo
284	25.873567	69.164.223.208	192.168.0.104	HTTP	1272	HTTP/1.1 200 OK (text/html)

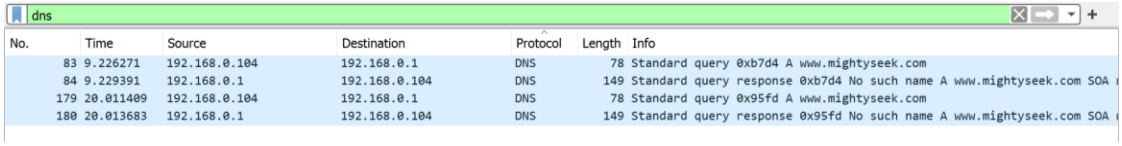
TCP



tcp

No.	Time	Source	Destination	Protocol	Length	Info
174	19.975239	69.164.223.208	192.168.0.104	TCP	1514	80 → 62644 [ACK] Seq=1 Ack=581 Win=64128 Len=1460 [TCP segment
176	19.975239	69.164.223.208	192.168.0.104	TCP	54	80 → 62644 [FIN, ACK] Seq=2184 Ack=581 Win=64128 Len=0
177	19.975356	192.168.0.104	69.164.223.208	TCP	54	62644 → 80 [ACK] Seq=581 Ack=2185 Win=131328 Len=0
178	19.983819	192.168.0.104	69.164.223.208	TCP	54	62644 → 80 [FIN, ACK] Seq=581 Ack=2185 Win=131328 Len=0
181	20.214062	69.164.223.208	192.168.0.104	TCP	54	80 → 62644 [ACK] Seq=2185 Ack=582 Win=64128 Len=0
184	21.572473	192.168.0.104	128.30.52.100	TCP	55	62635 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a r
185	21.863764	128.30.52.100	192.168.0.104	TCP	66	443 → 62635 [ACK] Seq=1 Ack=2 Win=17 Len=0 SLE=1 SRE=2
187	22.003454	35.186.224.47	192.168.0.104	TCP	60	443 → 55872 [ACK] Seq=1 Ack=44 Win=272 Len=0
189	22.157974	192.168.0.104	35.186.224.47	TCP	54	55872 → 443 [ACK] Seq=44 Ack=41 Win=512 Len=0
190	22.615853	192.168.0.104	69.164.223.208	TCP	66	62647 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER
195	22.675021	142.250.193.142	192.168.0.104	TCP	60	443 → 62632 [ACK] Seq=1 Ack=80 Win=276 Len=0
196	22.675021	142.250.193.142	192.168.0.104	TCP	60	443 → 62632 [ACK] Seq=1 Ack=119 Win=276 Len=0
197	22.675021	142.250.193.142	192.168.0.104	TCP	60	443 → 62632 [ACK] Seq=1 Ack=589 Win=281 Len=0
200	22.715102	192.168.0.104	142.250.193.142	TCP	54	62632 → 443 [ACK] Seq=589 Ack=40 Win=508 Len=0
201	22.746410	192.168.0.104	162.159.130.234	TCP	54	58979 → 443 [ACK] Seq=1 Ack=408 Win=510 Len=0
206	22.783809	192.168.0.104	142.250.193.142	TCP	54	62632 → 443 [ACK] Seq=589 Ack=267 Win=513 Len=0
208	22.847843	142.250.193.142	192.168.0.104	TCP	60	443 → 62632 [ACK] Seq=267 Ack=628 Win=281 Len=0
209	22.851190	69.164.223.208	192.168.0.104	TCP	66	80 → 62647 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK

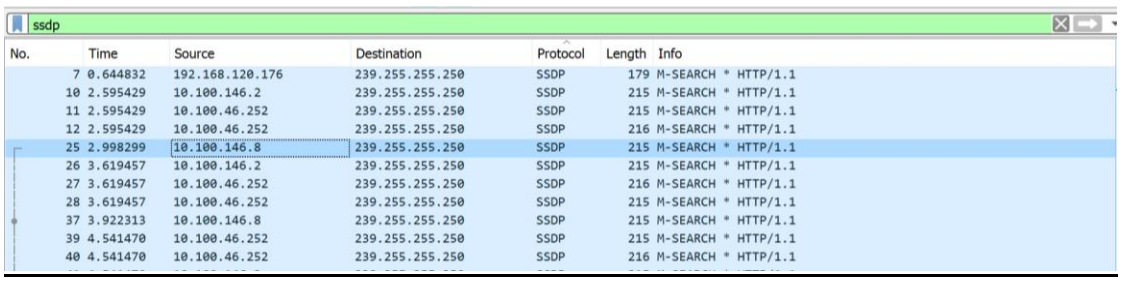
DNS



dns

No.	Time	Source	Destination	Protocol	Length	Info
83	9.226271	192.168.0.104	192.168.0.1	DNS	78	Standard query 0xb7d4 A www.mightyseek.com
84	9.229391	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0xb7d4 No such name A www.mightyseek.com SOA
179	20.011409	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x95fd A www.mightyseek.com
180	20.013683	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0x95fd No such name A www.mightyseek.com SOA

SSDP

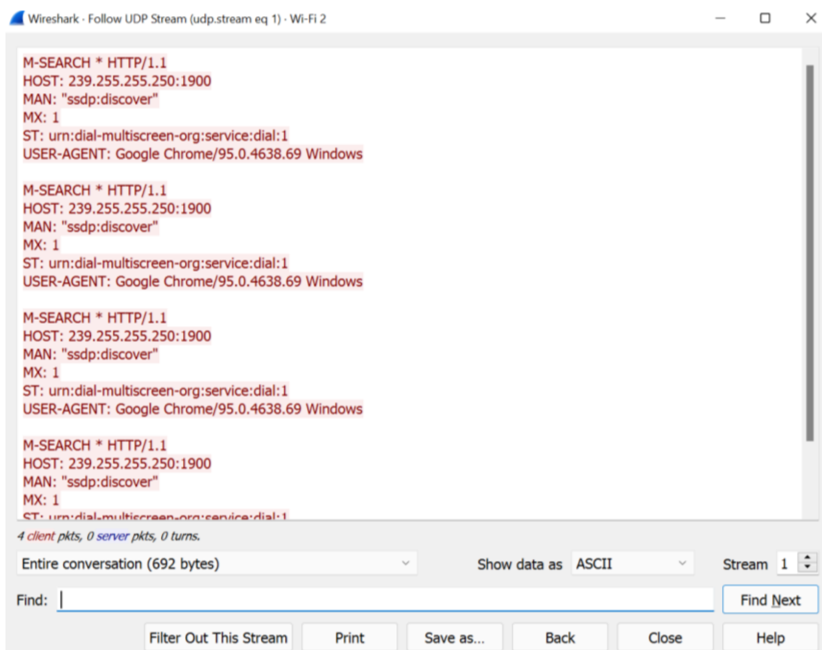


ssdp

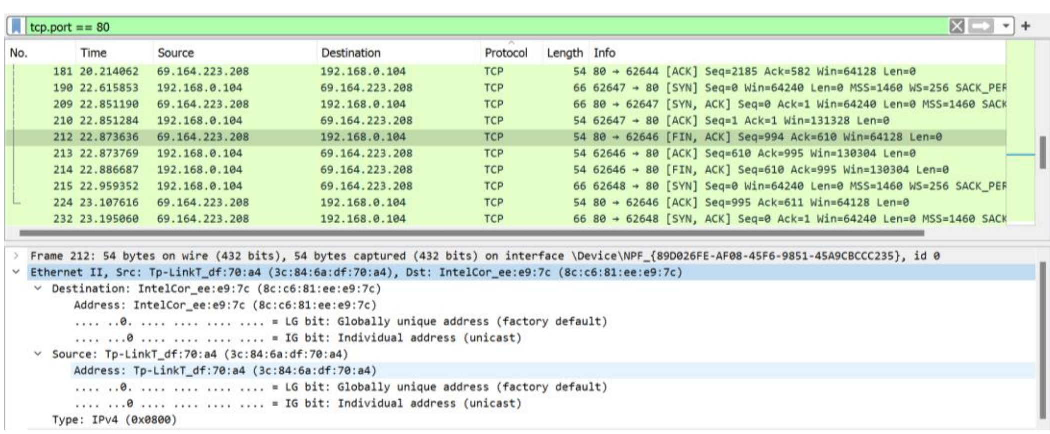
No.	Time	Source	Destination	Protocol	Length	Info
7	0.644832	192.168.120.176	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
10	2.595429	10.100.146.2	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
11	2.595429	10.100.46.252	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
12	2.595429	10.100.46.252	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
25	2.998299	10.100.146.8	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
26	3.619457	10.100.146.2	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
27	3.619457	10.100.46.252	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
28	3.619457	10.100.46.252	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
37	3.922313	10.100.146.8	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
39	4.541470	10.100.46.252	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
40	4.541470	10.100.46.252	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

a. **Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button -> click on follow.**

<u>Clicking on SSDP packet and following UDP stream</u>



6. **Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.**



<u>Packet 212 is an HTTP packet coming back from the server (tcp source port ==80)</u>

7. **What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?**

Manufacturer of my PC's Network Interface Card (NIC)

IntelCor
MAC Address: 8c:c6:81:ee:e9:7c

Manufacturer of my PC's Network Interface Card (NIC)

Tp-LinkT
MAC Address: 3c:84:6a:df:70:a4

8. **What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?**

PC: **ee:e9:7c**
Server: **df:70:a4**

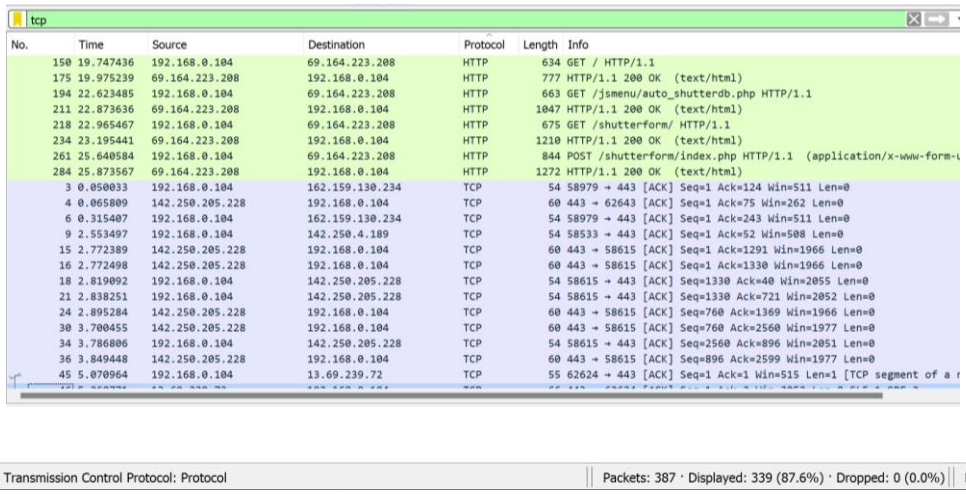
9. **Find the following statistics:**

   a. **What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?**

   b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?

ANSWERS

a. Out of 387 packets captured, 339 were TCP packets, i.e., TCP packets accounted for 87.6% of the total packets captured. HTTP (Hypertext Transfer Protocol) uses TCP.

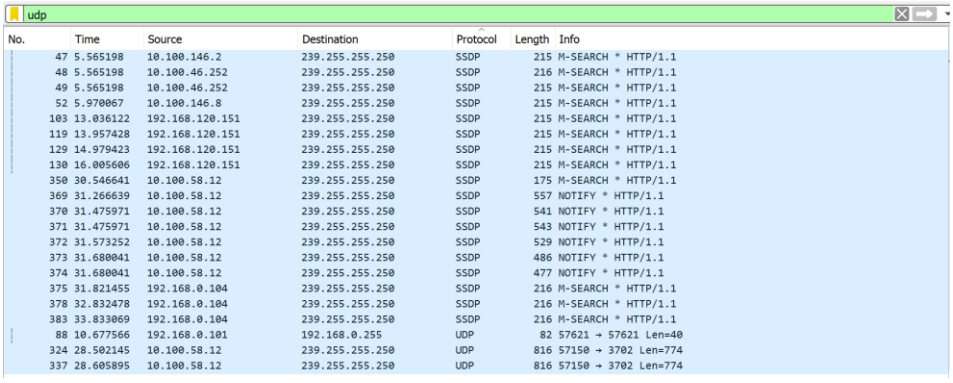


tcp

No.	Time	Source	Destination	Protocol	Length	Info
150	19.747436	192.168.0.104	69.164.223.208	HTTP	634	GET / HTTP/1.1
175	19.975239	69.164.223.208	192.168.0.104	HTTP	777	HTTP/1.1 200 OK (text/html)
194	22.623485	192.168.0.104	69.164.223.208	HTTP	663	GET /jsmenu/auto_shutterdb.php HTTP/1.1
211	22.873636	69.164.223.208	192.168.0.104	HTTP	1047	HTTP/1.1 200 OK (text/html)
218	22.965467	192.168.0.104	69.164.223.208	HTTP	675	GET /shutterform/ HTTP/1.1
234	23.195441	69.164.223.208	192.168.0.104	HTTP	1210	HTTP/1.1 200 OK (text/html)
261	25.640584	192.168.0.104	69.164.223.208	HTTP	844	POST /shutterform/index.php HTTP/1.1 (application/x-www-form-u
284	25.873567	69.164.223.208	192.168.0.104	HTTP	1272	HTTP/1.1 200 OK (text/html)
3	0.050033	192.168.0.104	162.159.130.234	TCP	54	58979 → 443 [ACK] Seq=1 Ack=124 Win=511 Len=0
4	0.065809	142.250.205.228	192.168.0.104	TCP	60	443 → 62643 [ACK] Seq=1 Ack=75 Win=262 Len=0
6	0.315407	192.168.0.104	162.159.130.234	TCP	54	58979 → 443 [ACK] Seq=1 Ack=243 Win=511 Len=0
9	2.553497	192.168.0.104	142.250.4.189	TCP	54	58533 → 443 [ACK] Seq=1 Ack=52 Win=508 Len=0
15	2.772389	142.250.205.228	192.168.0.104	TCP	60	443 → 58615 [ACK] Seq=1 Ack=1291 Win=1966 Len=0
16	2.772498	142.250.205.228	192.168.0.104	TCP	60	443 → 58615 [ACK] Seq=1 Ack=1330 Win=1966 Len=0
18	2.819092	192.168.0.104	142.250.205.228	TCP	54	58615 → 443 [ACK] Seq=1330 Ack=40 Win=2055 Len=0
21	2.838251	192.168.0.104	142.250.205.228	TCP	54	58615 → 443 [ACK] Seq=1330 Ack=721 Win=2052 Len=0
24	2.895284	142.250.205.228	192.168.0.104	TCP	60	443 → 58615 [ACK] Seq=760 Ack=1369 Win=1966 Len=0
30	3.700455	142.250.205.228	192.168.0.104	TCP	60	443 → 58615 [ACK] Seq=760 Ack=2560 Win=1977 Len=0
34	3.786806	192.168.0.104	142.250.205.228	TCP	54	58615 → 443 [ACK] Seq=2560 Ack=896 Win=2051 Len=0
36	3.849448	142.250.205.228	192.168.0.104	TCP	60	443 → 58615 [ACK] Seq=896 Ack=2599 Win=1977 Len=0
45	5.070964	192.168.0.104	13.69.239.72	TCP	55	62624 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a r

Transmission Control Protocol: Protocol | Packets: 387 · Displayed: 339 (87.6%) · Dropped: 0 (0.0%) | Profile: Default

b. Out of 387 packets captured, 42 were UDP packets, i.e., UDP packets accounted for 10.9% of the total packets captured. SSDP (Simple Service Discovery Protocol) uses UDP.



udp

No.	Time	Source	Destination	Protocol	Length	Info
47	5.565198	10.100.146.2	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
48	5.565198	10.100.46.252	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
49	5.565198	10.100.46.252	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
52	5.970067	10.100.146.8	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
103	13.036122	192.168.120.151	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
119	13.957428	192.168.120.151	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
129	14.979423	192.168.120.151	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
130	16.005606	192.168.120.151	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
350	30.546641	10.100.58.12	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
369	31.266639	10.100.58.12	239.255.255.250	SSDP	557	NOTIFY * HTTP/1.1
370	31.475971	10.100.58.12	239.255.255.250	SSDP	541	NOTIFY * HTTP/1.1
371	31.475971	10.100.58.12	239.255.255.250	SSDP	543	NOTIFY * HTTP/1.1
372	31.573252	10.100.58.12	239.255.255.250	SSDP	529	NOTIFY * HTTP/1.1
373	31.680041	10.100.58.12	239.255.255.250	SSDP	486	NOTIFY * HTTP/1.1
374	31.680041	10.100.58.12	239.255.255.250	SSDP	477	NOTIFY * HTTP/1.1
375	31.821455	192.168.0.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
378	32.832478	192.168.0.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
383	33.833069	192.168.0.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
88	10.677566	192.168.0.101	192.168.0.255	UDP	82	57621 → 57621 Len=40
324	28.502145	10.100.58.12	239.255.255.250	UDP	816	57150 → 3702 Len=774
337	28.605895	10.100.58.12	239.255.255.250	UDP	816	57150 → 3702 Len=774

User Datagram Protocol: Protocol | Packets: 387 · Displayed: 42 (10.9%) · Dropped: 0 (0.0%) | Profile: Default

10. Find the traffic flow. Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.

Graph Snippets