Computer Networks Lab Report – Assignment 5

TITLE

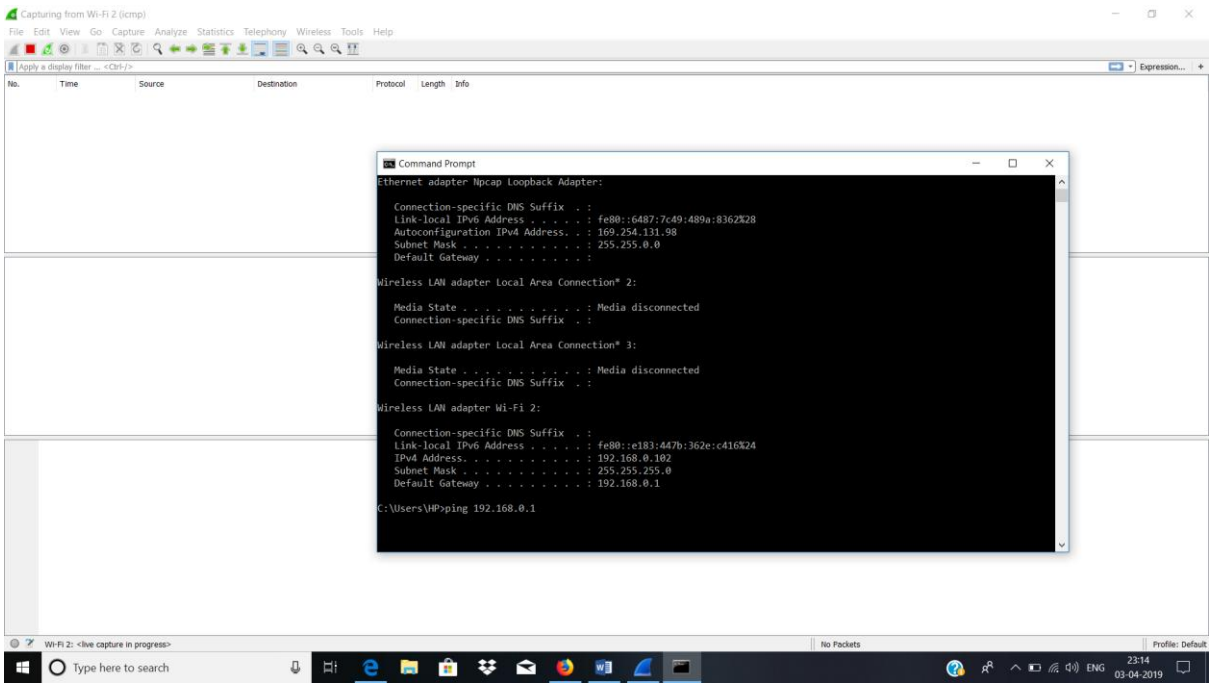
Name – Sourav Dutta
Roll – 001610501076
Class – BCSE 3rd year
Group – A3
Assignment Number – 5

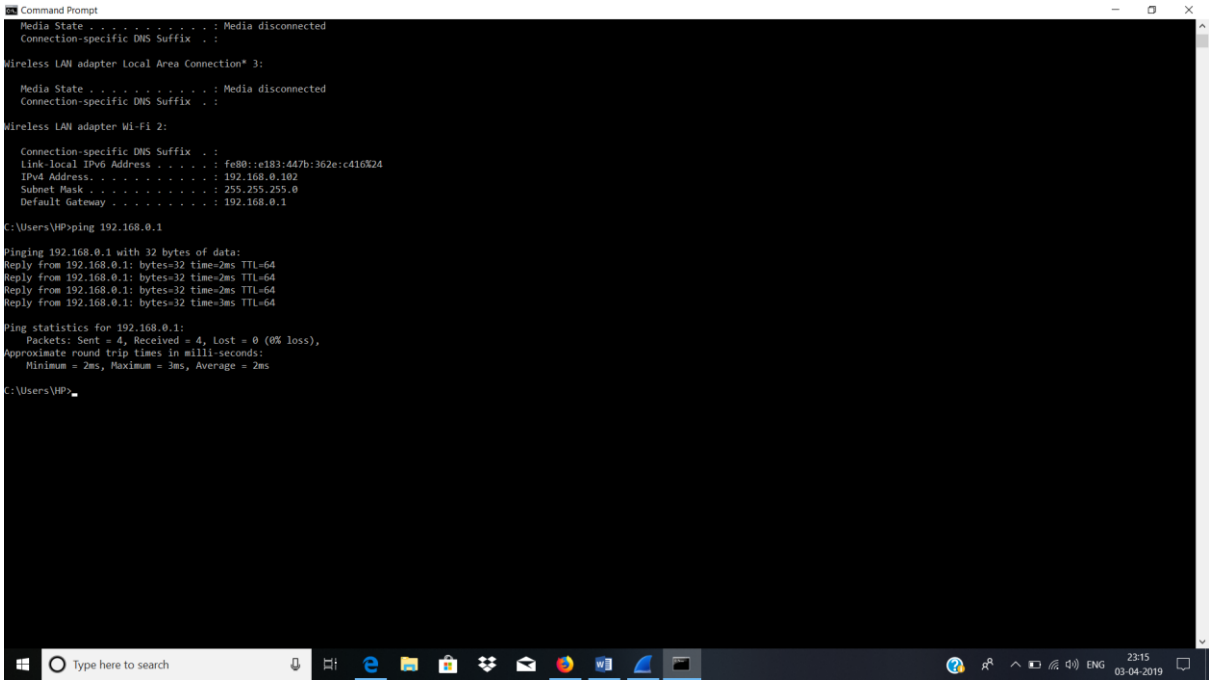
Problem Statement – Packet tracer and traffic analysis with Wireshark.

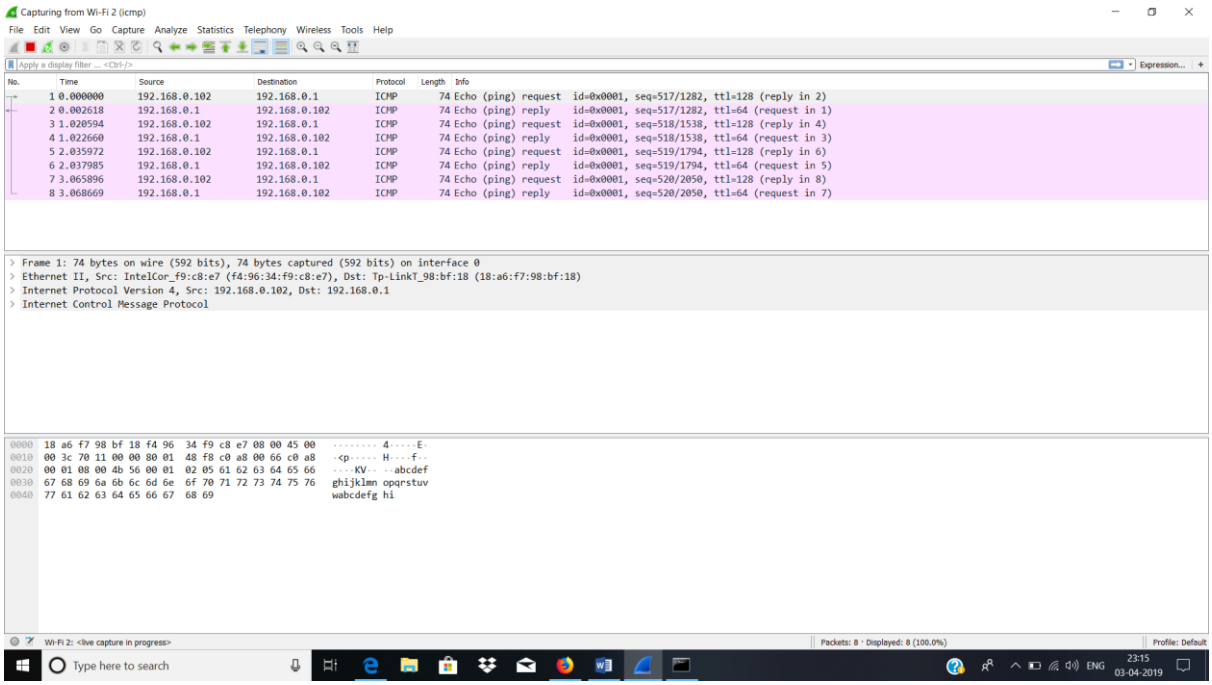
Overview:
Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and 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.

Submission date – 01/04/2019

Q 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 neighbouring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.

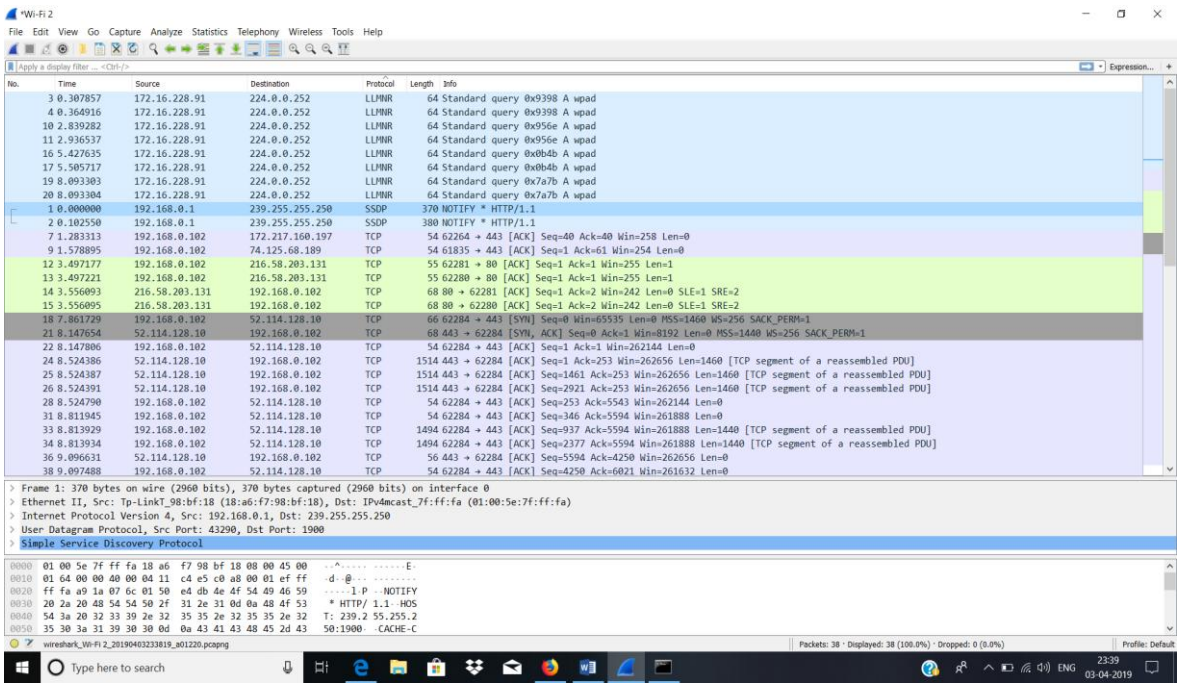


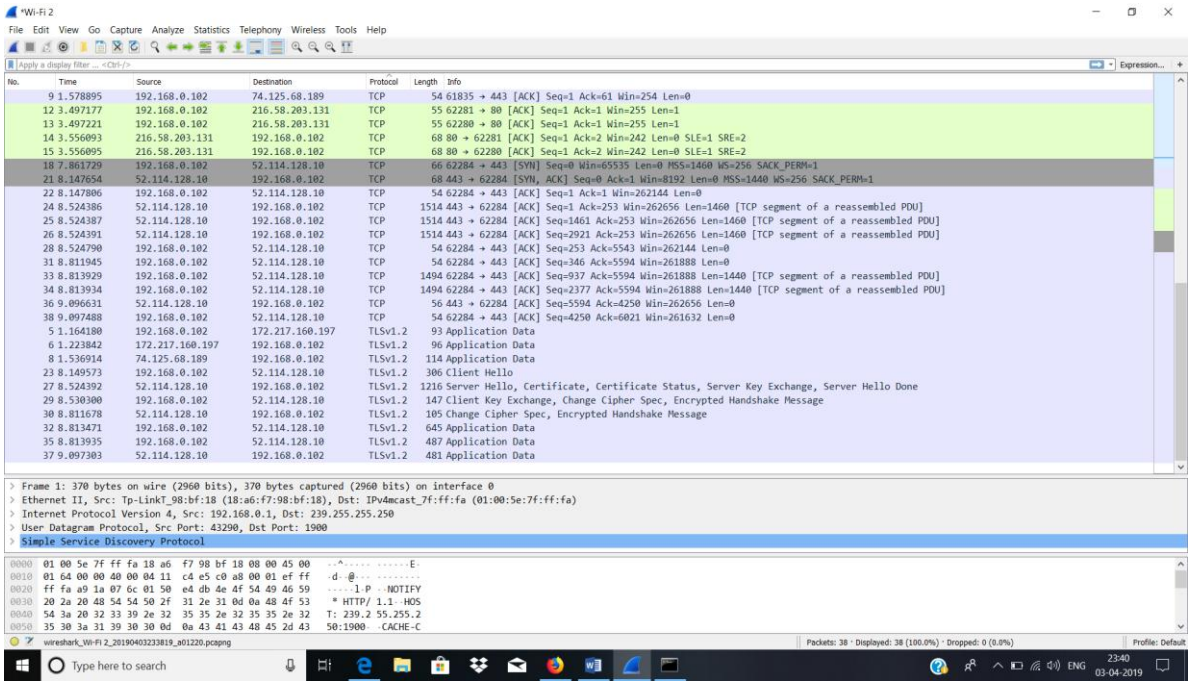




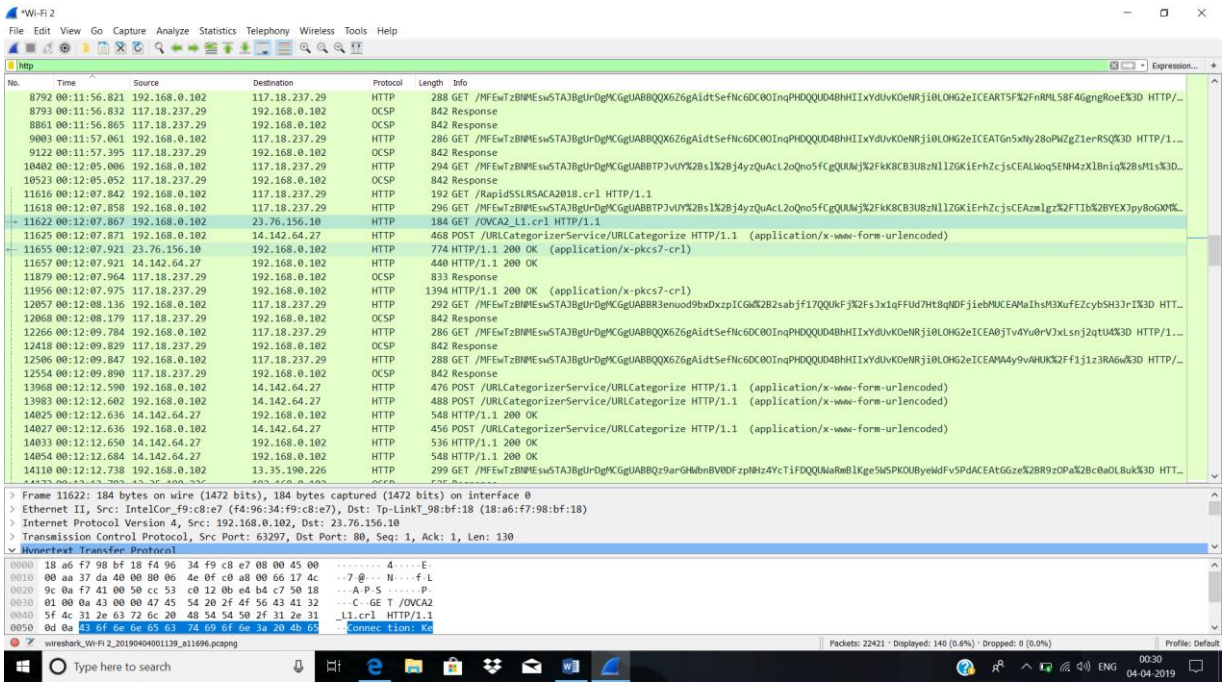
Q 2: Generate some web traffic and

a) find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.



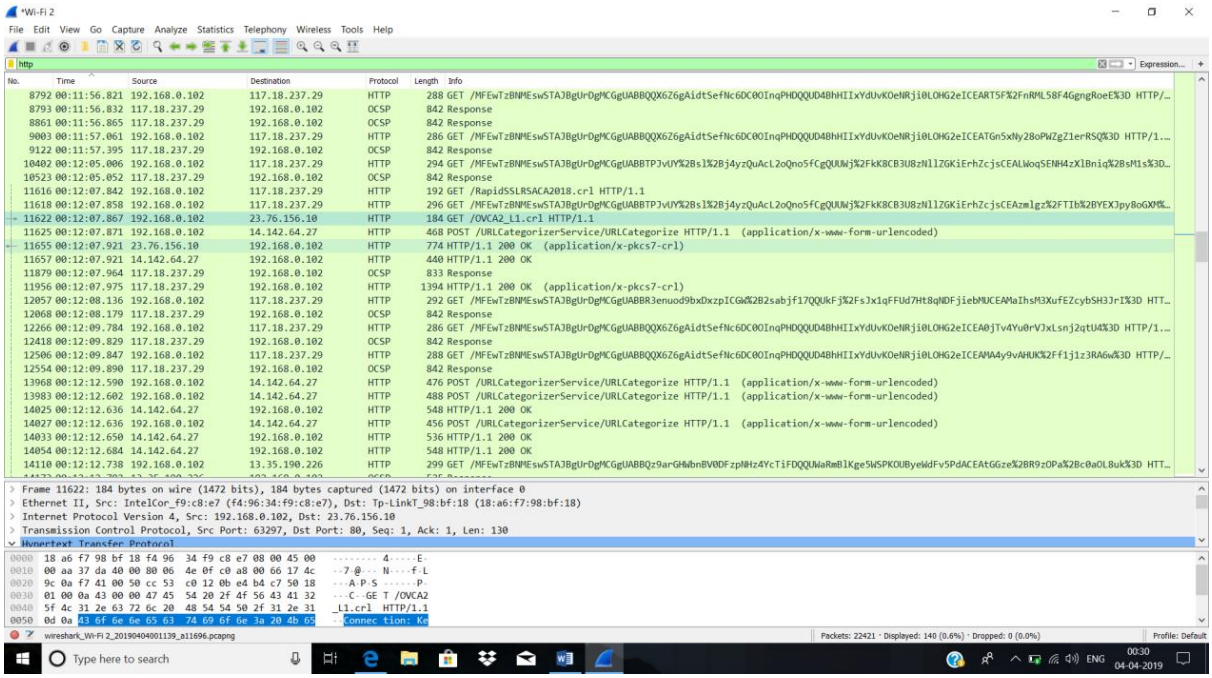


b) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.



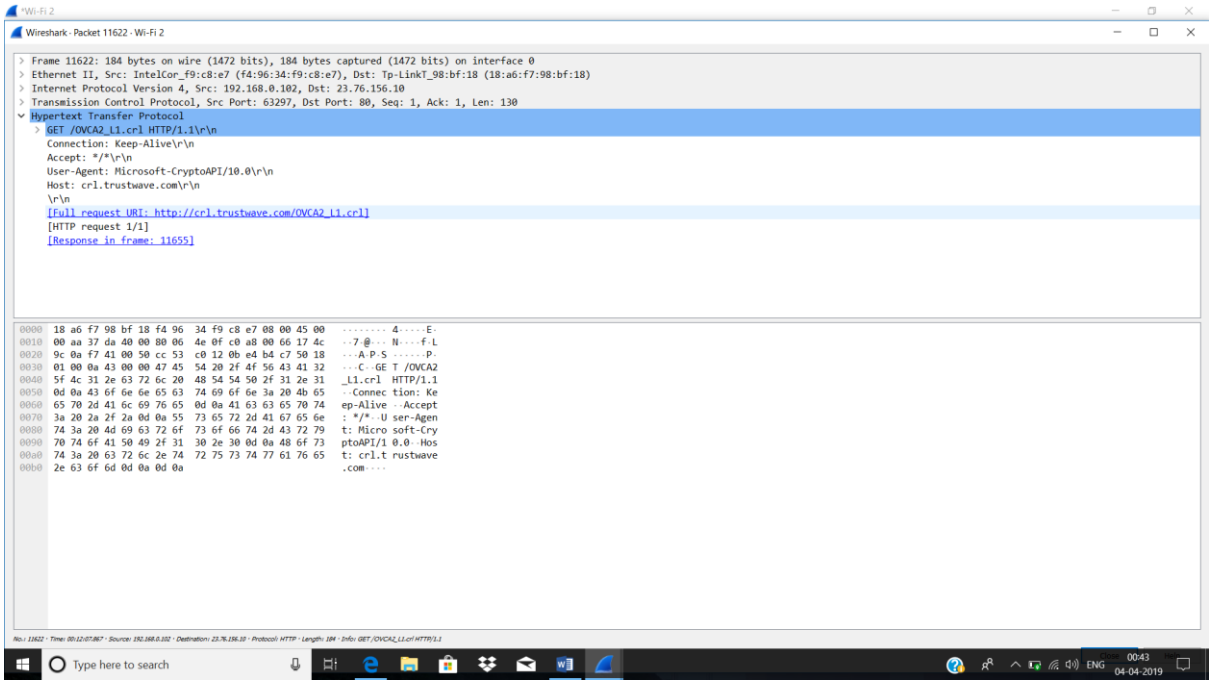
As shown in the screen shot above the GET(11622) was sent at 12 hrs 07 min 867 milliseconds and the reply OK(11655) was received at 12 hrs 07 min 921 milliseconds. The delay was thus 54 milliseconds

c) What is the Internet address of the website? What is the Internet address of your computer?

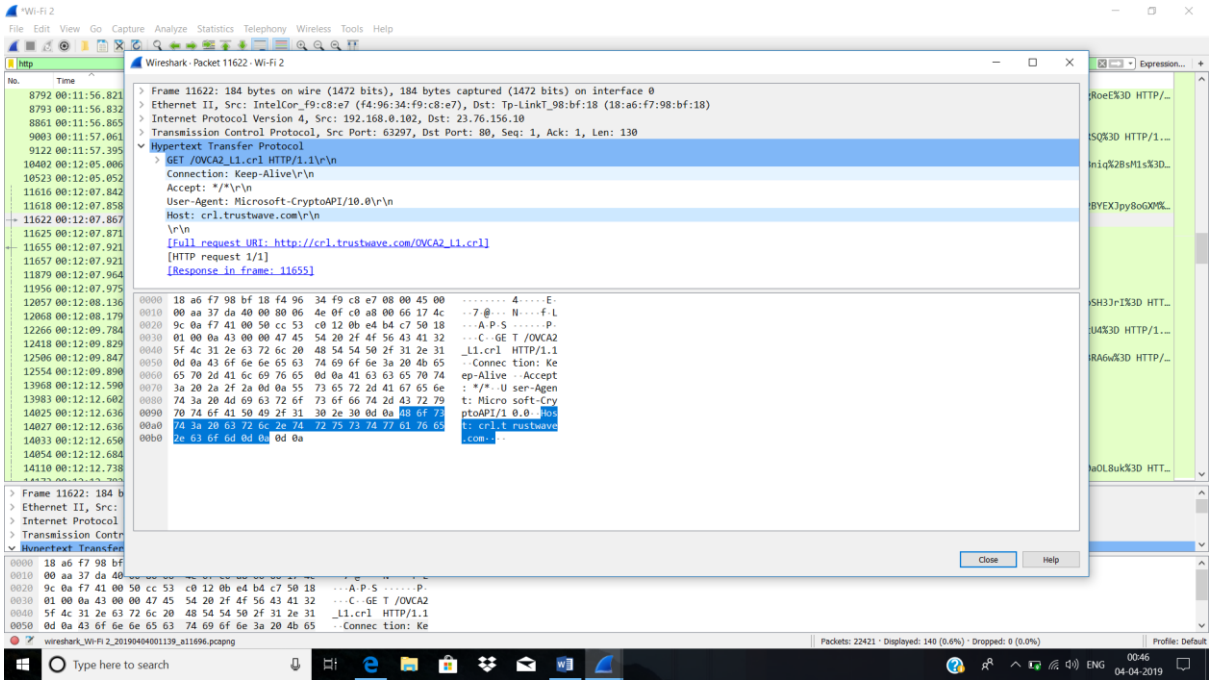


As shown in the screen shot above the IP address of the website is 23.76.156.10 the IP address of my laptop is 192.168.0.102 .

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.

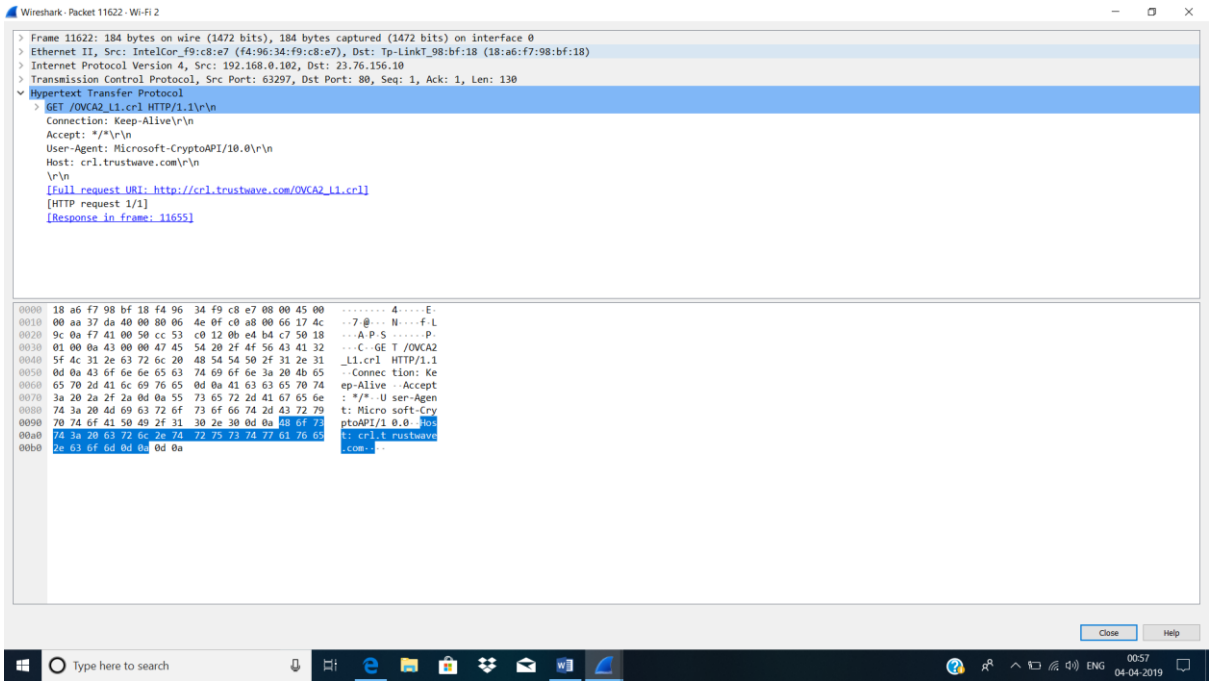


e) Find out the value of the Host from the Packet Details Panel, within the GET command.



As shown in above screen shot the Host is : crl.trustwave.com\r\n.

<u>Problem 3:</u> Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.



The Hex and ASCII representations of the packet in the Packet Bytes Panel are:

0000 18 a6 f7 98 bf 18 f4 96 34 f9 c8 e7 08 00 45 00 ....4.....E.

0010 00 aa 37 da 40 00 80 06 4e 0f c0 a8 00 66 17 4c ..7.@...N....f.L

0020 9c 0a f7 41 00 50 cc 53 c0 12 0b e4 b4 c7 50 18 ...A.P.S......P.

0030 01 00 0a 43 00 00 47 45 54 20 2f 4f 56 43 41 32 ...C..GET /OVCA2

0040 5f 4c 31 2e 63 72 6c 20 48 54 54 50 2f 31 2e 31 _L1.crl HTTP/1.1

0050 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 ..Connection: Ke

0060 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 70 74 ep-Alive..Accept

0070 3a 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e : */*..User-Agen

0080 74 3a 20 4d 69 63 72 6f 73 6f 66 74 2d 43 72 79 t: Microsoft-Cry

0090 70 74 6f 41 50 49 2f 31 30 2e 30 0d 0a 48 6f 73 ptoAPI/10.0..Hos

00a0 74 3a 20 63 72 6c 2e 74 72 75 73 74 77 61 76 65 t: crl.trustwave

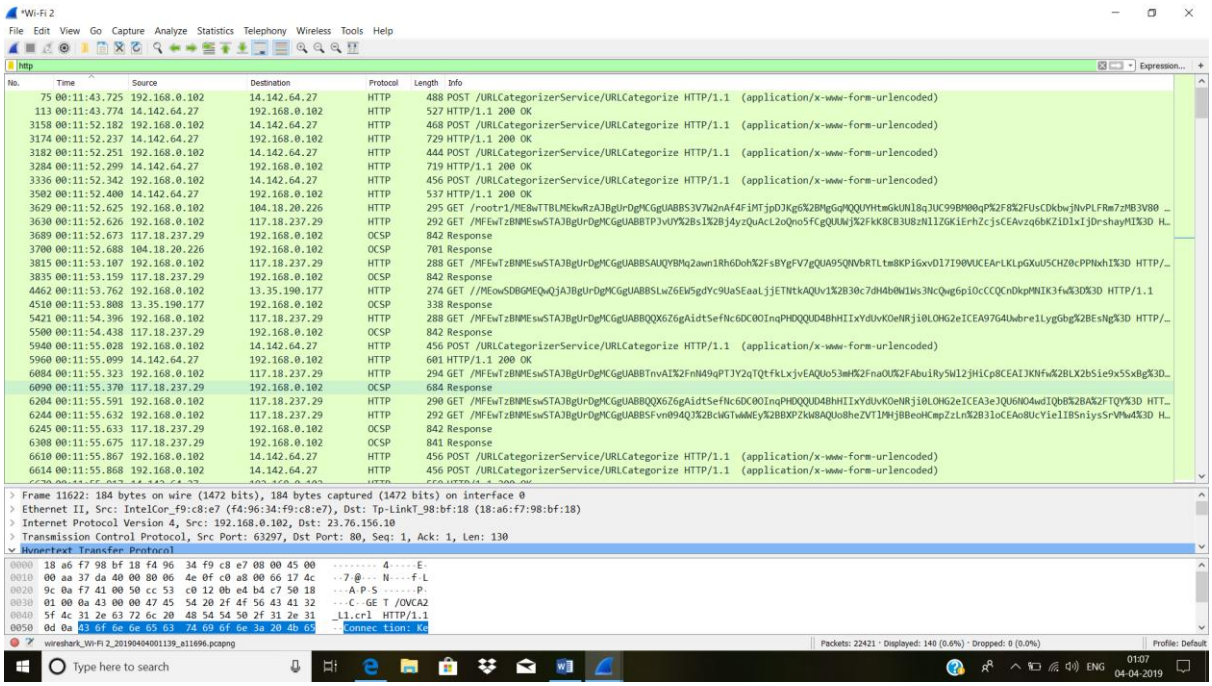
00b0 2e 63 6f 6d 0d 0a 0d 0a .com....

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

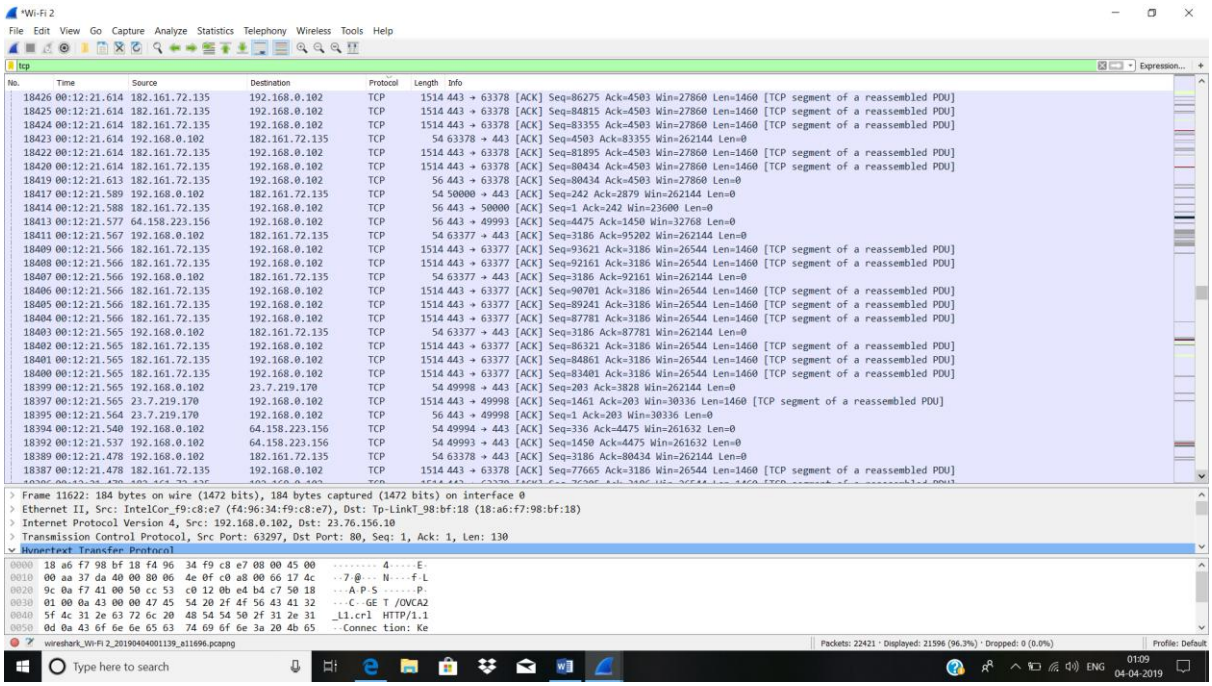
The 1st four bytes of the Hex value of the Host parameter from the Packet Bytes Panel are: **48 6f 73 74.**

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

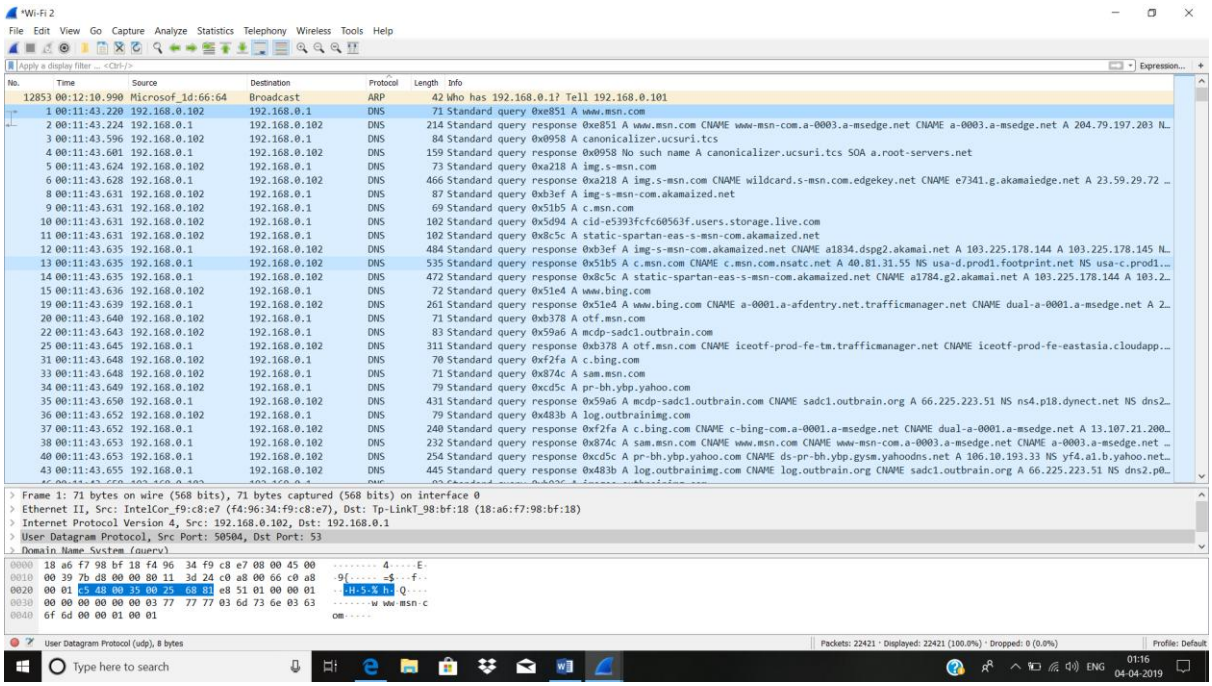
HTTP:


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
75 00:11:43.725 192.168.0.102 14.142.64.27 HTTP 488 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
113 00:11:43.774 14.142.64.27 192.168.0.102 HTTP 527 HTTP/1.1 200 OK
3158 00:11:52.182 192.168.0.102 14.142.64.27 HTTP 468 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
3174 00:11:52.237 14.142.64.27 192.168.0.102 HTTP 729 HTTP/1.1 200 OK
3182 00:11:52.251 192.168.0.102 14.142.64.27 HTTP 444 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
3284 00:11:52.299 14.142.64.27 192.168.0.102 HTTP 719 HTTP/1.1 200 OK
3336 00:11:52.342 192.168.0.102 14.142.64.27 HTTP 456 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
3502 00:11:52.400 14.142.64.27 192.168.0.102 HTTP 537 HTTP/1.1 200 OK
3629 00:11:52.625 192.168.0.102 104.18.20.226 HTTP 295 GET /rootr1/ME8wTTBLMEkwRzAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUVHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDkbwjNvPLFRm7zMB3V80 …
3630 00:11:52.626 192.168.0.102 117.18.237.29 HTTP 292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bs1%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNllZGKiErhZcjsCEAvzq6bKZiDlxljDrshayMI%3D H…
3689 00:11:52.673 117.18.237.29 192.168.0.102 OCSP 842 Response
3700 00:11:52.688 104.18.20.226 192.168.0.102 OCSP 701 Response
3815 00:11:53.107 192.168.0.102 117.18.237.29 HTTP 288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEArLKLpGXuU5CHZ0cPPNxhI%3D HTTP/…
3835 00:11:53.159 117.18.237.29 192.168.0.102 OCSP 842 Response
4462 00:11:53.762 192.168.0.102 13.35.190.177 HTTP 274 GET //MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fw%3D%3D HTTP/1.1
4510 00:11:53.808 13.35.190.177 192.168.0.102 OCSP 338 Response
5421 00:11:54.396 192.168.0.102 117.18.237.29 HTTP 288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEA97G4Uwbre1LygGbg%2BEsNg%3D HTTP/…
5500 00:11:54.438 117.18.237.29 192.168.0.102 OCSP 842 Response
5940 00:11:55.028 192.168.0.102 14.142.64.27 HTTP 456 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
5960 00:11:55.099 14.142.64.27 192.168.0.102 HTTP 601 HTTP/1.1 200 OK
6084 00:11:55.323 192.168.0.102 117.18.237.29 HTTP 294 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2FnN49qPTJY2qTQtfkLxjvEAQUo53mH%2FnaOU%2FAbuiRy5Wl2jHiCp8CEAIJKNFw%2BLX2bSie9x5SxBg%3D…
6090 00:11:55.370 117.18.237.29 192.168.0.102 OCSP 684 Response
6204 00:11:55.591 192.168.0.102 117.18.237.29 HTTP 290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEA3eJQU6NO4wdIQbB%2BA%2FTQY%3D HTT…
6244 00:11:55.632 192.168.0.102 117.18.237.29 HTTP 292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSFvn094QJ%2BcWGTw4WEy%2BBXPZkW8AQUo8heZVT1MHjBBeoHCmpZzLn%2B3loCEAo8UcYielIBSniysSrVMw4%3D H…
6245 00:11:55.633 117.18.237.29 192.168.0.102 OCSP 842 Response
6308 00:11:55.675 117.18.237.29 192.168.0.102 OCSP 841 Response
6610 00:11:55.867 192.168.0.102 14.142.64.27 HTTP 456 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
6614 00:11:55.868 192.168.0.102 14.142.64.27 HTTP 456 POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
Frame 11622: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
Ethernet II, Src: IntelCor_f9:c8:e7 (f4:96:34:f9:c8:e7), Dst: Tp-LinkT_98:bf:18 (18:a6:f7:98:bf:18)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 23.76.156.10
Transmission Control Protocol, Src Port: 63297, Dst Port: 80, Seq: 1, Ack: 1, Len: 130
Hypertext Transfer Protocol
0000 18 a6 f7 98 bf 18 f4 96 34 f9 c8 e7 08 00 45 00 .... 4.....E.
0010 00 aa 37 da 40 00 80 06 4e 0f c0 a8 00 66 17 4c ..7.@... N....f.L
0020 9c 0a f7 41 00 50 cc 53 c0 12 0b e4 b4 c7 50 18 ...A.P.S ......P.
0030 01 00 0a 43 00 00 47 45 54 20 2f 4f 56 43 41 32 ...C..GE T /OVCA2
0040 5f 4c 31 2e 63 72 6c 20 48 54 54 50 2f 31 2e 31 _L1.crl HTTP/1.1
0050 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 ..Connec tion: Ke
wireshark_Wi-Fi 2_20190404001139_a11696.pcapng
Packets: 22421 · Displayed: 140 (0.6%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG
01:07
04-04-2019

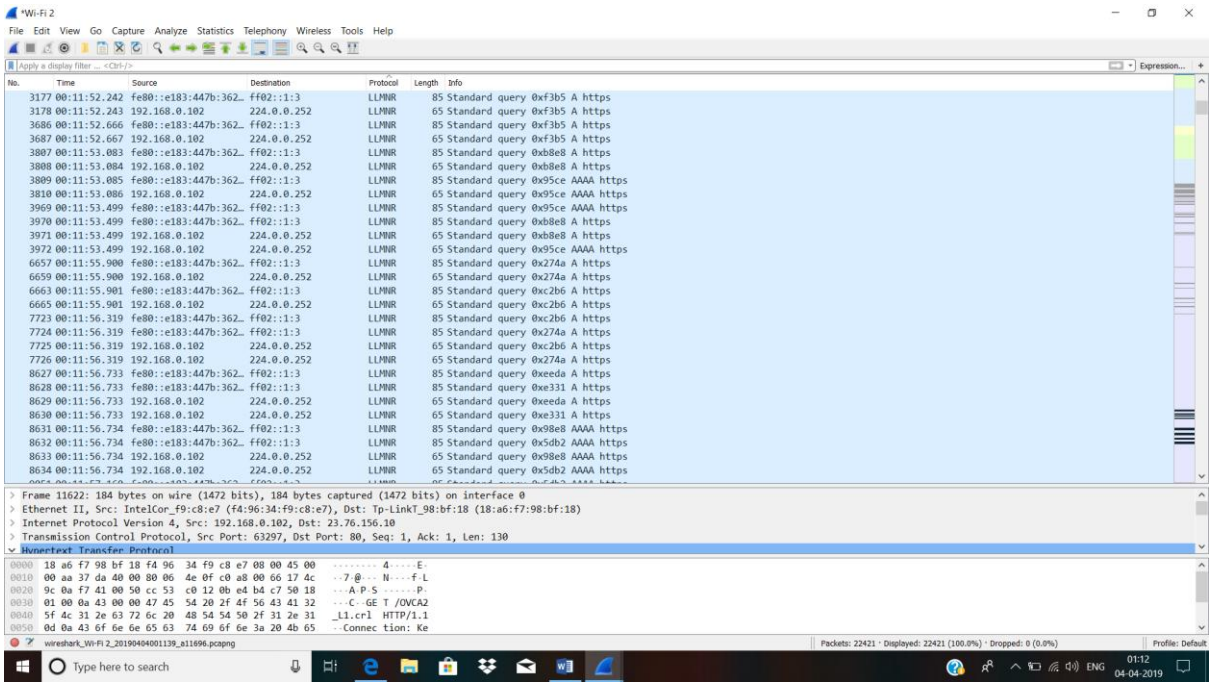
TCP:


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
18426 00:12:21.614 182.161.72.135 192.168.0.102 TCP 1514 443 → 63378 [ACK] Seq=86275 Ack=4503 Win=27860 Len=1460 [TCP segment of a reassembled PDU]
18425 00:12:21.614 182.161.72.135 192.168.0.102 TCP 1514 443 → 63378 [ACK] Seq=84815 Ack=4503 Win=27860 Len=1460 [TCP segment of a reassembled PDU]
18424 00:12:21.614 182.161.72.135 192.168.0.102 TCP 1514 443 → 63378 [ACK] Seq=83355 Ack=4503 Win=27860 Len=1460 [TCP segment of a reassembled PDU]
18423 00:12:21.614 192.168.0.102 182.161.72.135 TCP 54 63378 → 443 [ACK] Seq=4503 Ack=83355 Win=262144 Len=0
18422 00:12:21.614 182.161.72.135 192.168.0.102 TCP 1514 443 → 63378 [ACK] Seq=81895 Ack=4503 Win=27860 Len=1460 [TCP segment of a reassembled PDU]
18420 00:12:21.614 182.161.72.135 192.168.0.102 TCP 1514 443 → 63378 [ACK] Seq=80434 Ack=4503 Win=27860 Len=1460 [TCP segment of a reassembled PDU]
18419 00:12:21.613 182.161.72.135 192.168.0.102 TCP 56 443 → 63378 [ACK] Seq=80434 Ack=4503 Win=27860 Len=0
18417 00:12:21.589 192.168.0.102 182.161.72.135 TCP 54 50000 → 443 [ACK] Seq=242 Ack=2879 Win=262144 Len=0
18414 00:12:21.588 182.161.72.135 192.168.0.102 TCP 56 443 → 50000 [ACK] Seq=1 Ack=242 Win=23600 Len=0
18413 00:12:21.577 64.158.223.156 192.168.0.102 TCP 56 443 → 49993 [ACK] Seq=4475 Ack=1450 Win=32768 Len=0
18411 00:12:21.567 192.168.0.102 182.161.72.135 TCP 54 63377 → 443 [ACK] Seq=3186 Ack=95202 Win=262144 Len=0
18409 00:12:21.566 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=93621 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18408 00:12:21.566 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=92161 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18407 00:12:21.566 192.168.0.102 182.161.72.135 TCP 54 63377 → 443 [ACK] Seq=3186 Ack=92161 Win=262144 Len=0
18406 00:12:21.566 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=90701 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18405 00:12:21.566 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=89241 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18404 00:12:21.566 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=87781 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18403 00:12:21.565 192.168.0.102 182.161.72.135 TCP 54 63377 → 443 [ACK] Seq=3186 Ack=87781 Win=262144 Len=0
18402 00:12:21.565 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=86321 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18401 00:12:21.565 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=84861 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18400 00:12:21.565 182.161.72.135 192.168.0.102 TCP 1514 443 → 63377 [ACK] Seq=83401 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
18399 00:12:21.565 192.168.0.102 23.7.219.170 TCP 54 49998 → 443 [ACK] Seq=203 Ack=3828 Win=262144 Len=0
18397 00:12:21.565 23.7.219.170 192.168.0.102 TCP 1514 443 → 49998 [ACK] Seq=1461 Ack=203 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
18395 00:12:21.564 23.7.219.170 192.168.0.102 TCP 56 443 → 49998 [ACK] Seq=1 Ack=203 Win=30336 Len=0
18394 00:12:21.540 192.168.0.102 64.158.223.156 TCP 54 49994 → 443 [ACK] Seq=336 Ack=4475 Win=261632 Len=0
18392 00:12:21.537 192.168.0.102 64.158.223.156 TCP 54 49993 → 443 [ACK] Seq=1450 Ack=4475 Win=261632 Len=0
18389 00:12:21.478 192.168.0.102 182.161.72.135 TCP 54 63378 → 443 [ACK] Seq=3186 Ack=80434 Win=262144 Len=0
18387 00:12:21.478 182.161.72.135 192.168.0.102 TCP 1514 443 → 63378 [ACK] Seq=77665 Ack=3186 Win=26544 Len=1460 [TCP segment of a reassembled PDU]
Frame 11622: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
Ethernet II, Src: IntelCor_f9:c8:e7 (f4:96:34:f9:c8:e7), Dst: Tp-LinkT_98:bf:18 (18:a6:f7:98:bf:18)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 23.76.156.10
Transmission Control Protocol, Src Port: 63297, Dst Port: 80, Seq: 1, Ack: 1, Len: 130
Hypertext Transfer Protocol
0000 18 a6 f7 98 bf 18 f4 96 34 f9 c8 e7 08 00 45 00 .... 4.....E.
0010 00 aa 37 da 40 00 80 06 4e 0f c0 a8 00 66 17 4c ..7.@... N....f.L
0020 9c 0a f7 41 00 50 cc 53 c0 12 0b e4 b4 c7 50 18 ...A.P.S ......P.
0030 01 00 0a 43 00 00 47 45 54 20 2f 4f 56 43 41 32 ...C..GE T /OVCA2
0040 5f 4c 31 2e 63 72 6c 20 48 54 54 50 2f 31 2e 31 _L1.crl HTTP/1.1
0050 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 ..Connec tion: Ke
wireshark_Wi-Fi 2_20190404001139_a11696.pcapng
Packets: 22421 · Displayed: 21596 (96.3%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG
01:09
04-04-2019

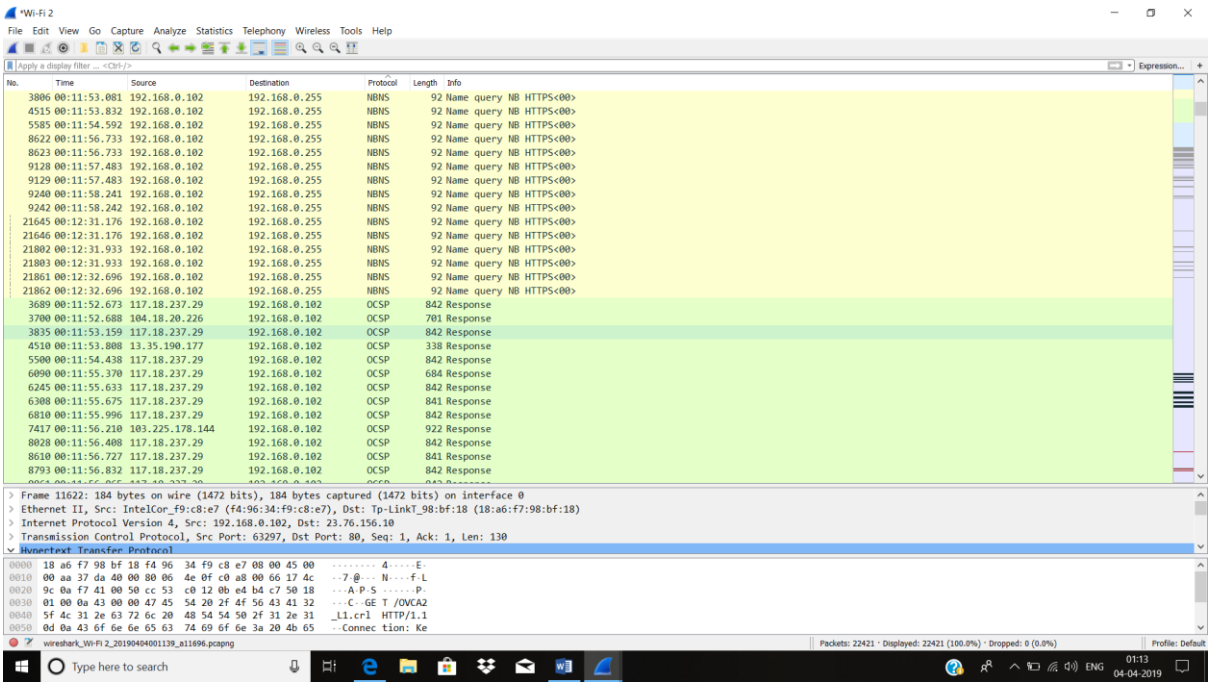
ARP & DNS:



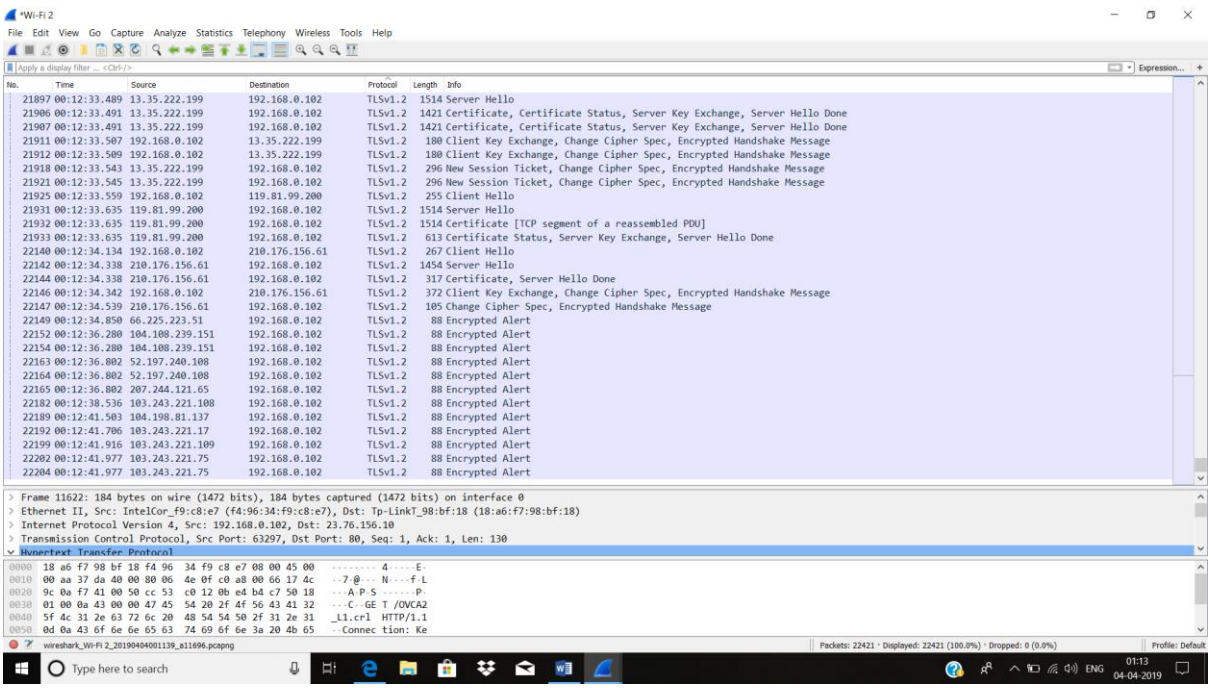
LLMNR:



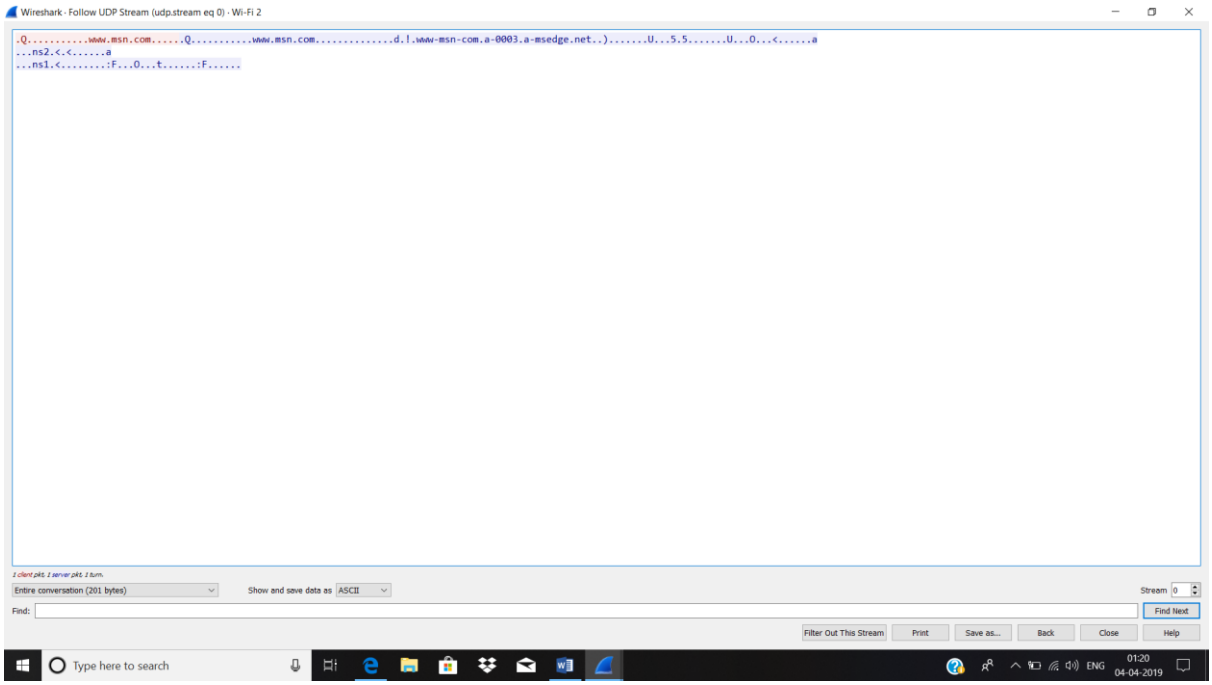
NBNS & OCSP:

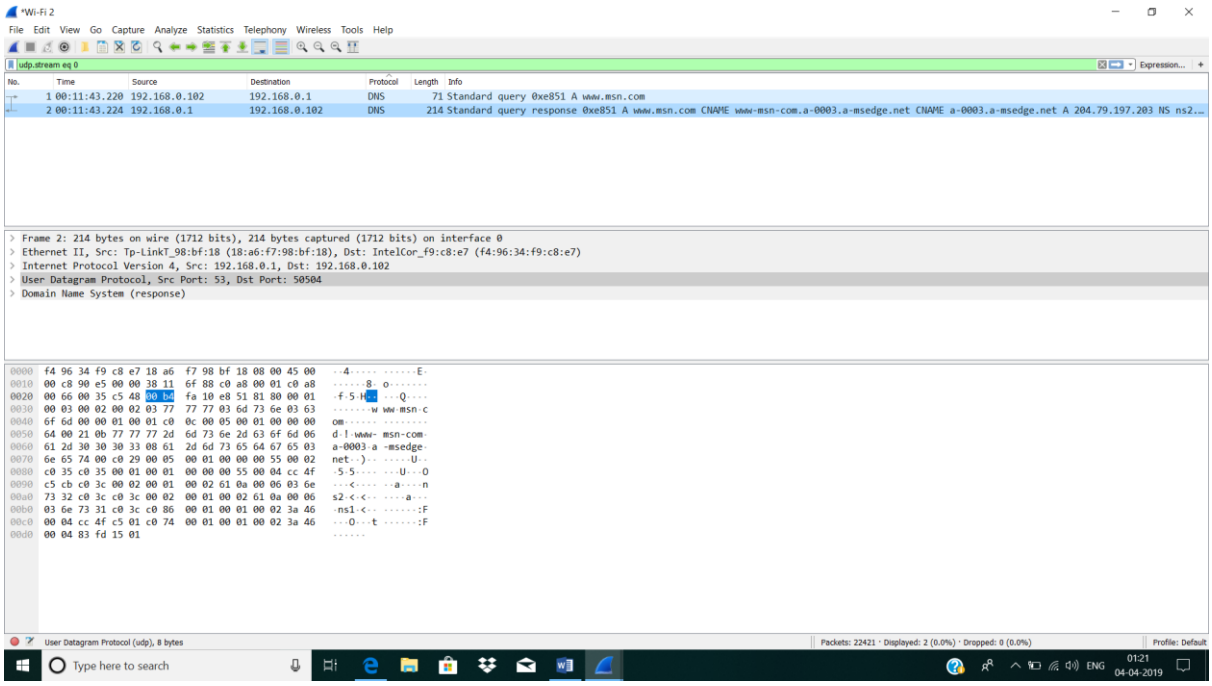


TLSv1.2:

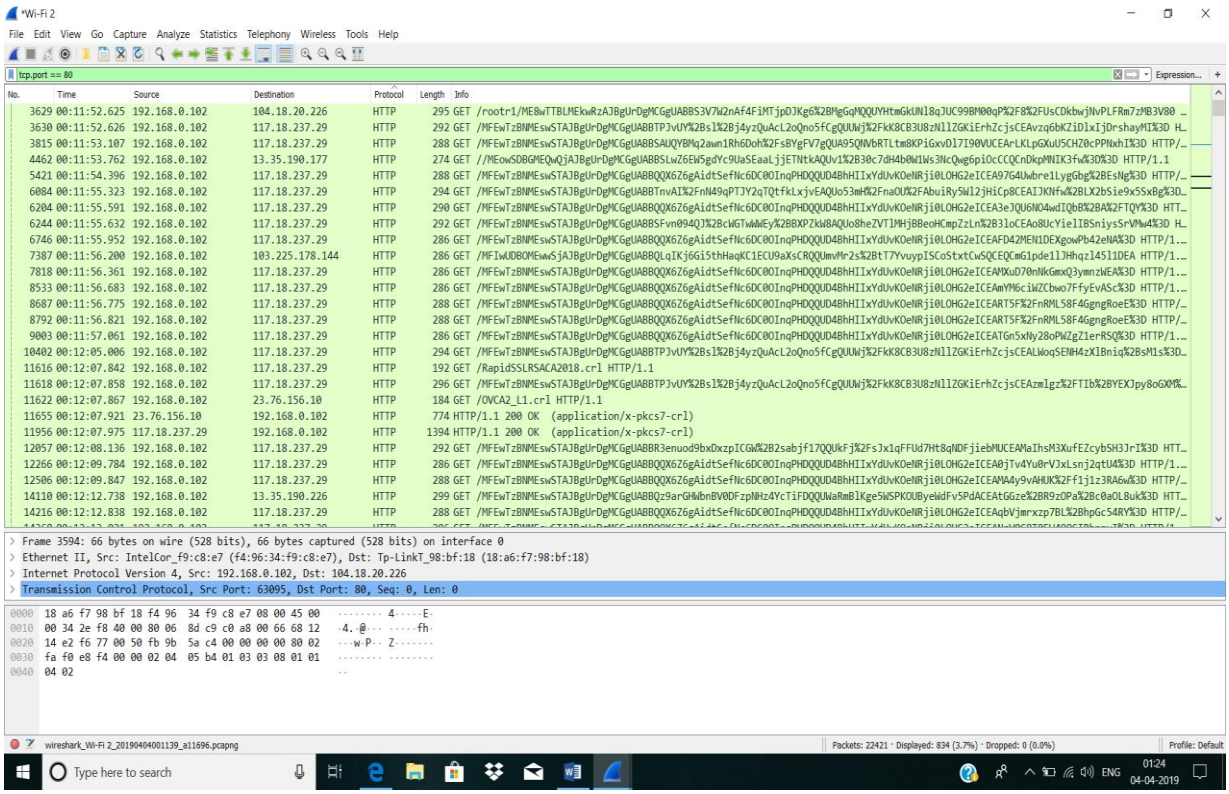


I'm selecting a packet having DNS protocol. On selecting follow (UDP stream) on this packet we get following result:

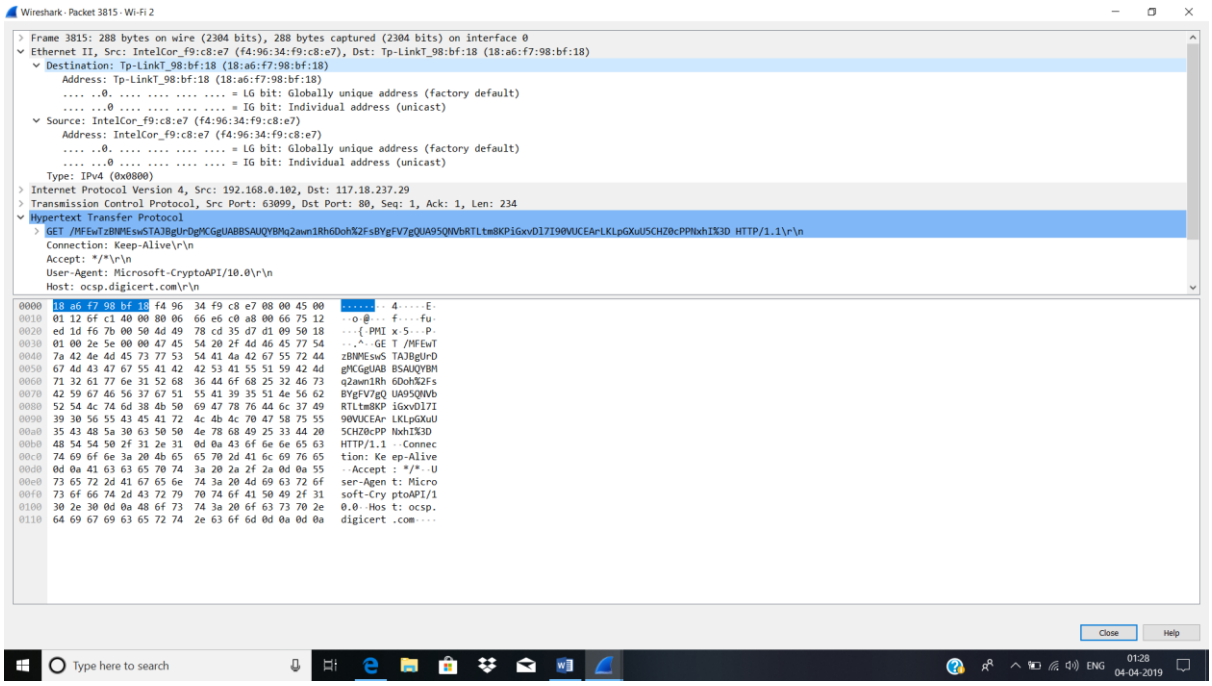




Q 6: Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.



On expanding Ethernet layer of a packet(3815) in Packet Details Panel following is the result:



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

Manufacturers of my PC's Network Interface Card (NIC) is:

IntelCor_f9:c8:e7 (f4:96:34:f9:c8:e7)

Manufacturers of myserver's Network Interface Card (NIC) is:

Tp-LinkT_98:bf:18 (18:a6:f7:98:bf:18)

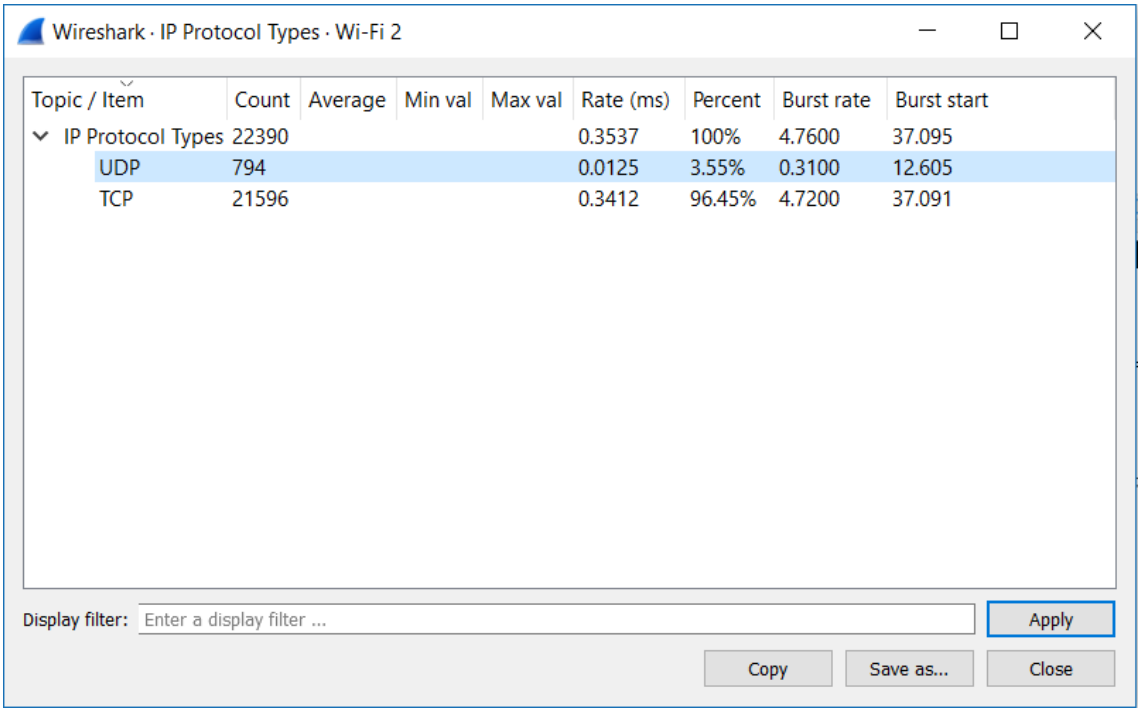
Q 8: What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?

For PC's manufacturers: **f4:96:34:f9:c8:e7**

For server's manufacturers: **18:a6:f7:98:bf:18**

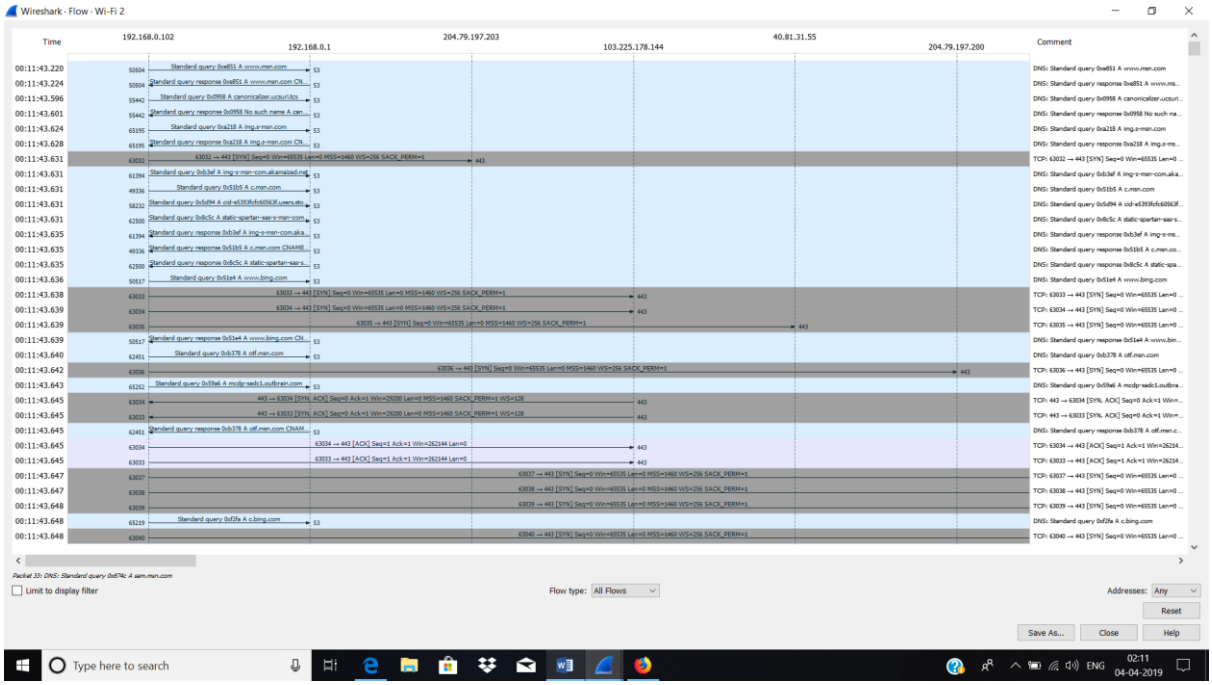
Q 9: Find the following statistics:

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?



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

For general flow:



For TCP flow: