

Name : Tanmoy Sarkar
Roll No : 002010501020
Class : BCSE III
Assignment No : 5
Subject : Computer Network
Group : A1

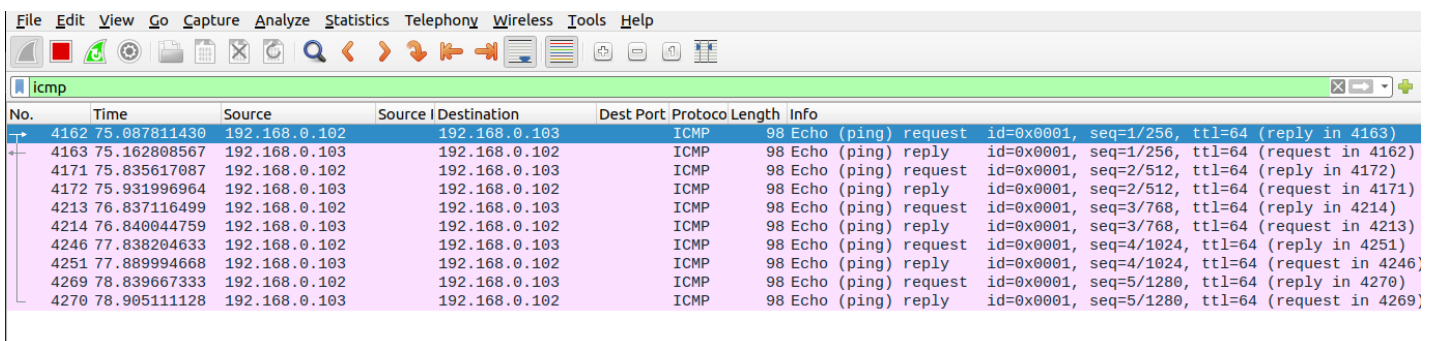
Overview

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, colourizing 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.

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.

```
(base) tanmoy@tanmoy-laptop:~$ ping 192.168.0.103 -c 5
PING 192.168.0.103 (192.168.0.103) 56(84) bytes of data.
64 bytes from 192.168.0.103: icmp_seq=1 ttl=64 time=329 ms
64 bytes from 192.168.0.103: icmp_seq=2 ttl=64 time=96.4 ms
64 bytes from 192.168.0.103: icmp_seq=3 ttl=64 time=2.95 ms
64 bytes from 192.168.0.103: icmp_seq=4 ttl=64 time=51.8 ms
64 bytes from 192.168.0.103: icmp_seq=5 ttl=64 time=65.5 ms

--- 192.168.0.103 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.949/109.085/328.769/113.900 ms
```



The image shows a screenshot of the Wireshark network protocol analyzer. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window displays a list of captured packets, with the 'icmp' filter applied. The packet list shows 10 packets, alternating between ICMP Echo (ping) requests and replies. The packet details pane on the right shows the selected packet (No. 4163) with its details: Ethernet II, Internet Protocol Version 4, and ICMP Echo (ping) reply. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Source Destination	Dest Port	Protocol	Length	Info
4162	75.087811430	192.168.0.102	192.168.0.103		ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 4163)
4163	75.162808567	192.168.0.103	192.168.0.102		ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 4162)
4171	75.835617087	192.168.0.102	192.168.0.103		ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 4172)
4172	75.931996964	192.168.0.103	192.168.0.102		ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 4171)
4213	76.837116499	192.168.0.102	192.168.0.103		ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 4214)
4214	76.840044759	192.168.0.103	192.168.0.102		ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 4213)
4246	77.838204633	192.168.0.102	192.168.0.103		ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 4251)
4251	77.889994668	192.168.0.103	192.168.0.102		ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 4246)
4269	78.839667333	192.168.0.102	192.168.0.103		ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 4270)
4270	78.905111128	192.168.0.103	192.168.0.102		ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 4269)

2. Generate some web traffic and
a. find the list of the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.

No.	Time	Source	Source Destination	Dest Port	Protocol	Length	Info
55	1.474542820	142.250.82.29	3478 192.168.0.102	47445	UDP	601	3478 → 47445 Len=559
56	1.487786777	192.168.0.102	47445 142.250.82.29	3478	UDP	90	47445 → 3478 Len=48
57	1.511728867	142.250.82.29	3478 192.168.0.102	47445	STUN	142	Binding Success Response user: nTTUSBf5kjlGuQoKAAiKAIaEEA:n7vi
58	1.550325558	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44
59	1.576358195	142.250.82.29	3478 192.168.0.102	47445	UDP	141	3478 → 47445 Len=99
60	1.595094295	142.250.82.29	3478 192.168.0.102	47445	UDP	91	3478 → 47445 Len=49
61	1.659609291	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44
62	1.669142717	142.250.82.29	3478 192.168.0.102	47445	UDP	604	3478 → 47445 Len=562
63	1.769186338	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44
64	1.816099518	192.168.0.102	47445 142.250.82.29	3478	UDP	138	47445 → 3478 Len=96
65	1.847236489	192.168.0.102	47445 142.250.82.29	3478	UDP	118	47445 → 3478 Len=76
66	1.883352686	142.250.82.29	3478 192.168.0.102	47445	UDP	622	3478 → 47445 Len=580
67	1.950627542	192.168.0.102	51674 142.250.183.197	443	TCP	66	51674 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1609249145 T
68	1.987854043	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44
69	1.995435039	142.250.82.29	3478 192.168.0.102	47445	UDP	142	3478 → 47445 Len=100
70	2.001342286	142.250.183.197	443 192.168.0.102	51674	TCP	66	[TCP ACKed unseen segment] 443 → 51674 [ACK] Seq=1 Ack=2 Win=2
71	2.015340734	142.250.82.29	3478 192.168.0.102	47445	UDP	91	3478 → 47445 Len=49
72	2.085900881	142.250.82.29	3478 192.168.0.102	47445	UDP	619	3478 → 47445 Len=577
73	2.097264045	192.168.0.102	47445 142.250.82.29	3478	UDP	90	47445 → 3478 Len=48
74	2.190861881	192.168.0.102	47445 142.250.82.29	3478	UDP	90	47445 → 3478 Len=48
75	2.355205311	142.250.82.29	3478 192.168.0.102	47445	UDP	604	3478 → 47445 Len=562
76	2.355205731	142.250.82.29	3478 192.168.0.102	47445	RTCP	234	Sender Report
77	2.417044430	142.250.82.29	3478 192.168.0.102	47445	UDP	154	3478 → 47445 Len=112
78	2.425423946	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44
79	2.437855849	142.250.82.29	3478 192.168.0.102	47445	UDP	91	3478 → 47445 Len=49
80	2.498209580	142.250.82.29	3478 192.168.0.102	47445	UDP	604	3478 → 47445 Len=562
81	2.534658528	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44
82	2.706667496	192.168.0.102	47445 142.250.82.29	3478	UDP	138	47445 → 3478 Len=96
83	2.710799282	142.250.82.29	3478 192.168.0.102	47445	UDP	604	3478 → 47445 Len=562
84	2.753471151	192.168.0.102	47445 142.250.82.29	3478	UDP	86	47445 → 3478 Len=44

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.)

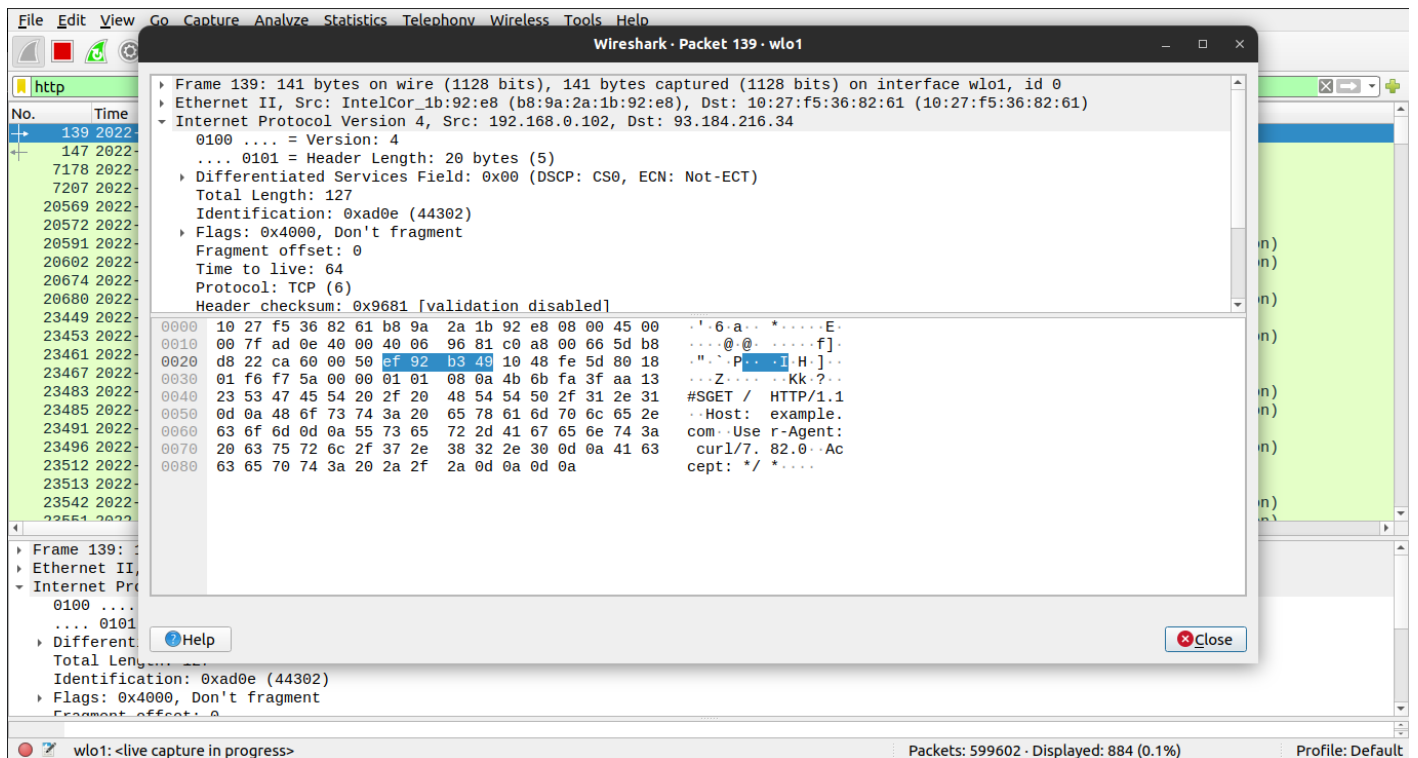
No.	Time	Source	Source Destination	Dest Port	Protocol	Length	Info
139	2022-10-27 23:41:03.014702709	192.168.0.102	51808 93.184.216.34	80	HTTP	141	GET / HTTP/1.1
147	2022-10-27 23:41:03.258817666	93.184.216.34	80 192.168.0.102	51808	HTTP	1657	HTTP/1.1 200 OK (text/html)

Request sent at 23:41:03.014702709 and received response at 23:41:03.258817666.
So, delay = 0.244114957 seconds

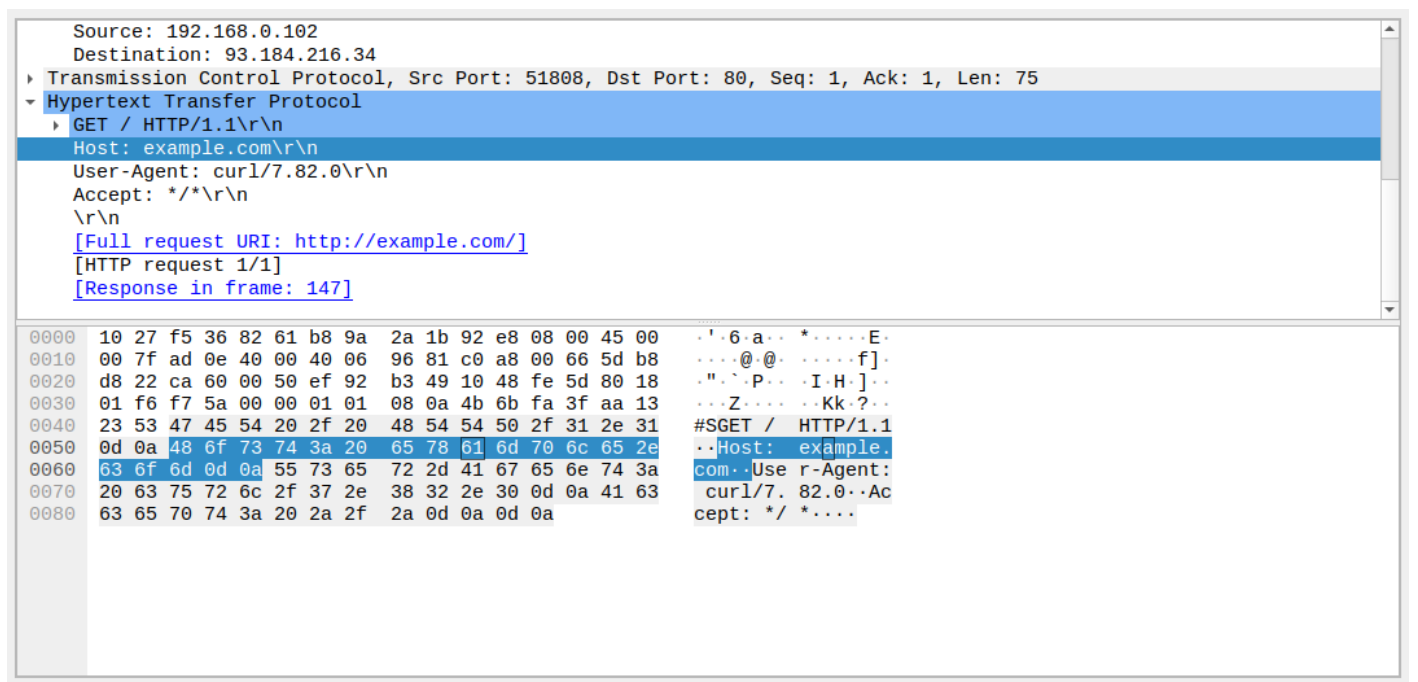
c. What is the Internet address of the website? What is the Internet address of your computer?

Internet address of website : 93.184.216.34
Internet address of computer : 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.

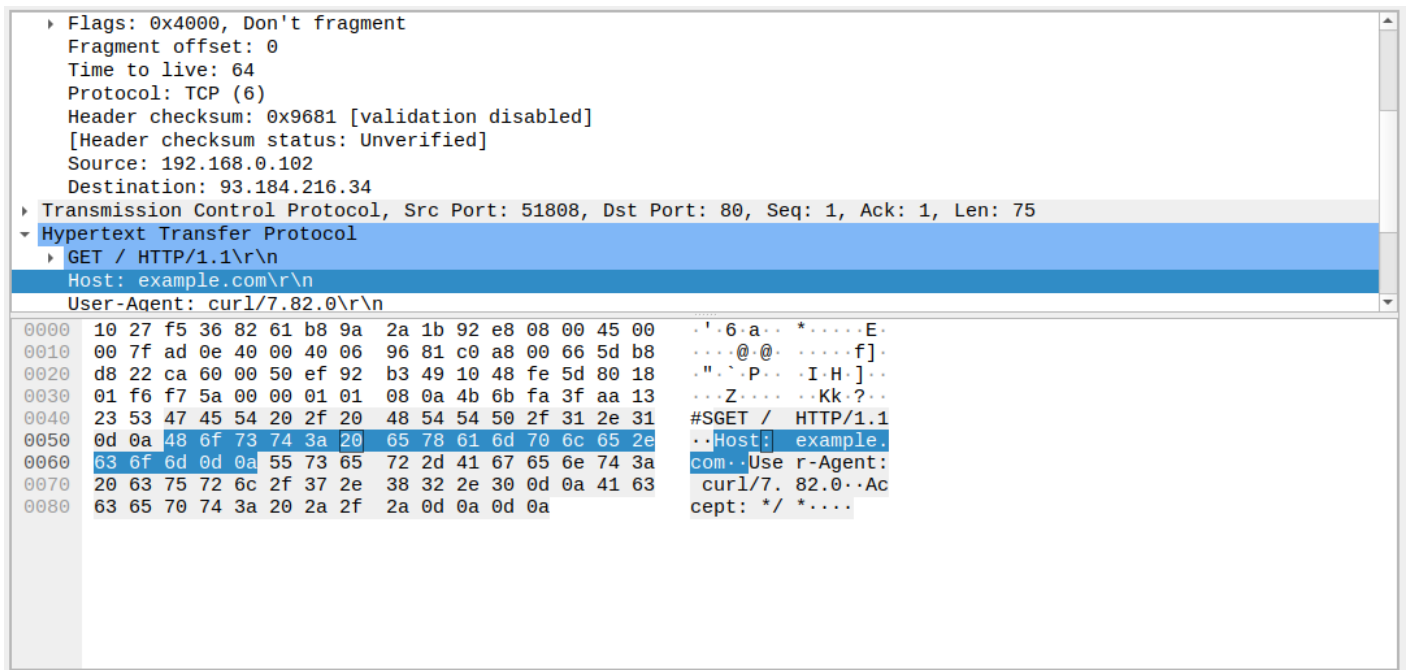


e. Find out the value of the Host from the Packet Details Panel, within the GET command.



Host : example.com

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



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

First 4 bytes are - 48 6f 73 74

5. Filter packets with http, TCP, DNS and other protocols. a. Find out what 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 :

No.	Time	Source	Source Destination	Dest Port	Protocol	Length	Info
139	2022-10-27 23:41:03.014702709	192.168.0.102	51808 93.184.216.34	80	HTTP	141	GET / HTTP/1.1
147	2022-10-27 23:41:03.258817666	93.184.216.34	80 192.168.0.102	51808	HTTP	1657	HTTP/1.1 200 OK (text/html)
7178	2022-10-27 23:43:24.512410642	192.168.0.102	35082 35.232.111.17	80	HTTP	153	GET / HTTP/1.1
7207	2022-10-27 23:43:24.814648403	35.232.111.17	80 192.168.0.102	35082	HTTP	214	HTTP/1.1 204 No Content
20569	2022-10-27 23:44:58.498855785	192.168.0.102	34994 43.205.231.38	5555	HTTP	658	POST /api HTTP/1.1 (text/plain)
20572	2022-10-27 23:44:58.499589794	192.168.0.102	35008 43.205.231.38	5555	HTTP	935	POST /api HTTP/1.1 (text/plain)
20591	2022-10-27 23:44:58.678238348	43.205.231.38	5555 192.168.0.102	34994	HTTP	417	HTTP/1.1 200 OK (application/json)
20602	2022-10-27 23:44:58.681594580	43.205.231.38	5555 192.168.0.102	35008	HTTP	363	HTTP/1.1 200 OK (application/json)
20674	2022-10-27 23:44:59.370996586	192.168.0.102	35008 43.205.231.38	5555	HTTP	652	POST /api HTTP/1.1 (text/plain)
20680	2022-10-27 23:44:59.411511248	43.205.231.38	5555 192.168.0.102	35008	HTTP	411	HTTP/1.1 200 OK (application/json)
23449	2022-10-27 23:45:20.754382143	192.168.0.102	43522 43.205.231.38	5555	HTTP	1056	POST /api HTTP/1.1 (text/plain)
23453	2022-10-27 23:45:20.897824553	43.205.231.38	5555 192.168.0.102	43522	HTTP	538	HTTP/1.1 200 OK (application/json)
23461	2022-10-27 23:45:21.015277143	192.168.0.102	43522 43.205.231.38	5555	HTTP	658	POST /api HTTP/1.1 (text/plain)
23467	2022-10-27 23:45:21.076804766	192.168.0.102	43534 43.205.231.38	5555	HTTP	935	POST /api HTTP/1.1 (text/plain)
23483	2022-10-27 23:45:21.211047943	43.205.231.38	5555 192.168.0.102	43534	HTTP	402	HTTP/1.1 200 OK (application/json)
23485	2022-10-27 23:45:21.211174419	43.205.231.38	5555 192.168.0.102	43522	HTTP	417	HTTP/1.1 200 OK (application/json)
23491	2022-10-27 23:45:21.347286297	192.168.0.102	43534 43.205.231.38	5555	HTTP	678	POST /api HTTP/1.1 (text/plain)
23496	2022-10-27 23:45:21.400962375	43.205.231.38	5555 192.168.0.102	43534	HTTP	412	HTTP/1.1 200 OK (application/json)
23512	2022-10-27 23:45:21.672231397	192.168.0.102	43534 43.205.231.38	5555	HTTP	658	POST /api HTTP/1.1 (text/plain)
23513	2022-10-27 23:45:21.672783075	192.168.0.102	43522 43.205.231.38	5555	HTTP	935	POST /api HTTP/1.1 (text/plain)
23542	2022-10-27 23:45:21.858434893	43.205.231.38	5555 192.168.0.102	43534	HTTP	417	HTTP/1.1 200 OK (application/json)
23551	2022-10-27 23:45:21.863741268	43.205.231.38	5555 192.168.0.102	43522	HTTP	402	HTTP/1.1 200 OK (application/json)
23571	2022-10-27 23:45:22.122402607	192.168.0.102	43522 43.205.231.38	5555	HTTP	673	POST /api HTTP/1.1 (text/plain)
23573	2022-10-27 23:45:22.127720872	192.168.0.102	43534 43.205.231.38	5555	HTTP	840	POST /api HTTP/1.1 (text/plain)
23629	2022-10-27 23:45:22.300380729	43.205.231.38	5555 192.168.0.102	43534	HTTP	1065	HTTP/1.1 200 OK (application/json)
23631	2022-10-27 23:45:22.303250549	43.205.231.38	5555 192.168.0.102	43522	HTTP	416	HTTP/1.1 200 OK (application/json)
23744	2022-10-27 23:45:23.239964179	192.168.0.102	43522 43.205.231.38	5555	HTTP	652	POST /api HTTP/1.1 (text/plain)
23752	2022-10-27 23:45:23.297484569	43.205.231.38	5555 192.168.0.102	43522	HTTP	412	HTTP/1.1 200 OK (application/json)

GET / HTTP/1.1
Host: example.com
User-Agent: curl/7.82.0
Accept: */*

HTTP/1.1 200 OK
Age: 202148
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Thu, 27 Oct 2022 18:11:03 GMT
Etag: "3147526947+ident"
Expires: Thu, 03 Nov 2022 18:11:03 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (dcb/7F18)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256

<!doctype html>
<html>
<head>
 <title>Example Domain</title>

 <meta charset="utf-8" />
 <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
 <meta name="viewport" content="width=device-width, initial-scale=1" />
 <style type="text/css">
 body {
 background-color: #f0f0f2;
 margin: 0;
 padding: 0;
 font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
 }
 div {
 width: 600px;
 margin: 5em auto;
 padding: 2em;
 background-color: #fdfdff;
 border-radius: 0.5em;
 box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
 }
 a:link, a:visited {
 color: #38488f;
 text-decoration: none;
 }
 @media (max-width: 700px) {

Packet 147. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1,666 bytes)

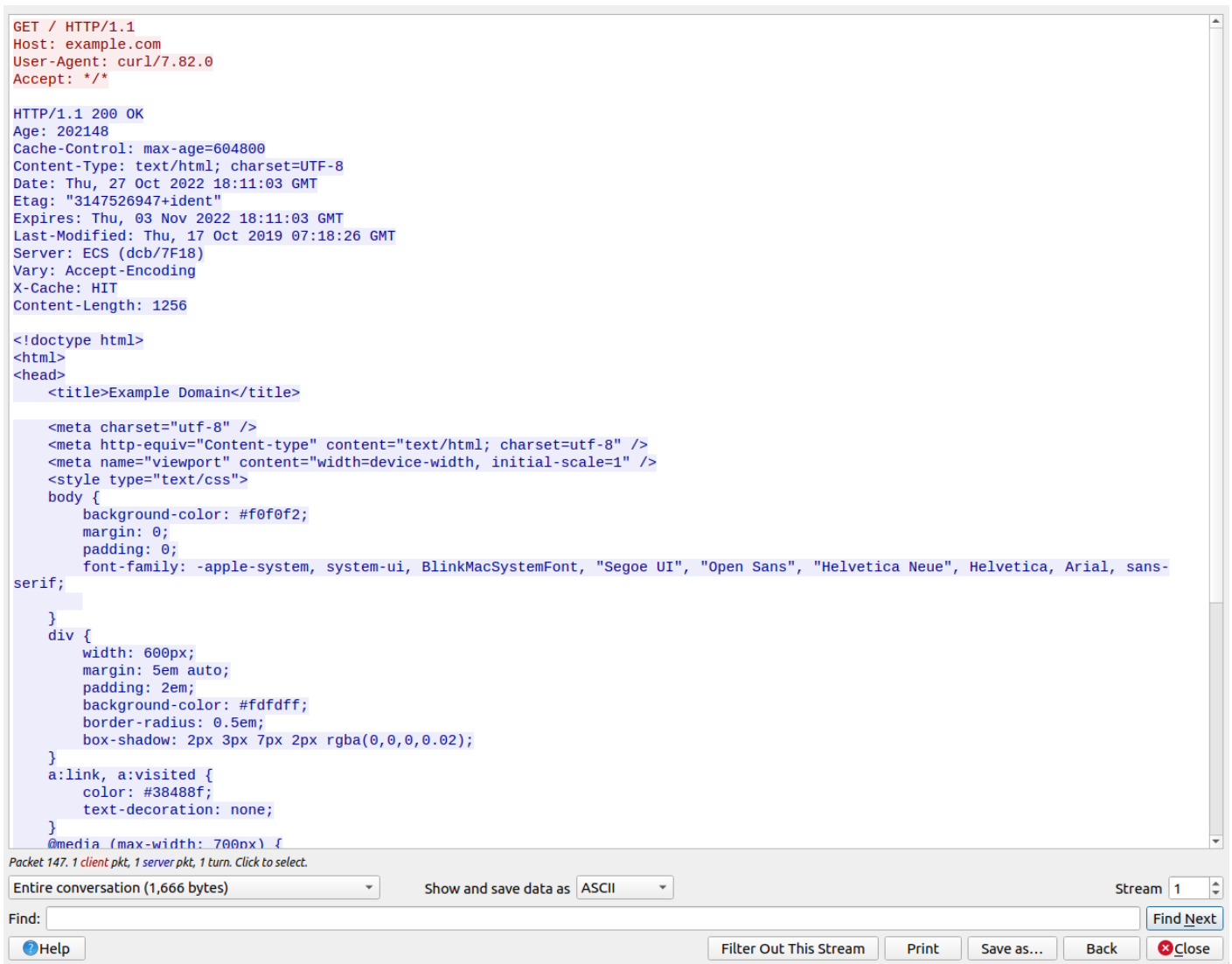
Show and save data as ASCII

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

TCP :

No.	Time	Source	Source Destination	Dest Port	Protocol	Length	Info
22	2022-10-27 23:41:00.849816541	192.168.0.102	55194 142.250.182.197	443	TCP	66	55194 → 443 [ACK] Seq=1 Ack=1 Win=1137 Len=0 TSval=366447919 TSecr=35892419...
28	2022-10-27 23:41:00.891936258	142.250.182.197	443 192.168.0.102	55194	TCP	66	[TCP ACKed unseen segment] 443 → 55194 [ACK] Seq=1 Ack=2 Win=612 Len=0 TSva...
121	2022-10-27 23:41:02.770713875	192.168.0.102	51808 93.184.216.34	80	TCP	74	51808 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=126536737...
137	2022-10-27 23:41:03.014513673	93.184.216.34	80 192.168.0.102	51808	TCP	74	80 → 51808 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva...
138	2022-10-27 23:41:03.014597416	192.168.0.102	51808 93.184.216.34	80	TCP	66	51808 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1265367615 TSecr=2853380...
139	2022-10-27 23:41:03.014702709	192.168.0.102	51808 93.184.216.34	80	HTTP	141	GET / HTTP/1.1
140	2022-10-27 23:41:03.028036721	93.184.216.34	80 192.168.0.102	51808	TCP	66	80 → 51808 [ACK] Seq=1 Ack=76 Win=29184 Len=0 TSval=2853380949 TSecr=126536...
147	2022-10-27 23:41:03.258817666	93.184.216.34	80 192.168.0.102	51808	HTTP	1657	HTTP/1.1 200 OK (text/html)
148	2022-10-27 23:41:03.258875588	192.168.0.102	51808 93.184.216.34	80	TCP	66	51808 → 80 [ACK] Seq=76 Ack=1592 Win=62720 Len=0 TSval=1265367859 TSecr=285...
149	2022-10-27 23:41:03.259450101	192.168.0.102	51808 93.184.216.34	80	TCP	66	51808 → 80 [FIN, ACK] Seq=76 Ack=1592 Win=64128 Len=0 TSval=1265367860 TSec...
153	2022-10-27 23:41:03.305529076	93.184.216.34	80 192.168.0.102	51808	TCP	66	80 → 51808 [ACK] Seq=1592 Ack=77 Win=29184 Len=0 TSval=2853380977 TSecr=126...
181	2022-10-27 23:41:03.502520568	93.184.216.34	80 192.168.0.102	51808	TCP	66	80 → 51808 [FIN, ACK] Seq=1592 Ack=77 Win=29184 Len=0 TSval=2853380996 TSec...
182	2022-10-27 23:41:03.502594810	192.168.0.102	51808 93.184.216.34	80	TCP	66	51808 → 80 [ACK] Seq=77 Ack=1593 Win=64128 Len=0 TSval=1265368193 TSecr=285...
187	2022-10-27 23:41:03.647092873	192.168.0.102	44478 52.52.240.208	443	TLSv...	121	Application Data
193	2022-10-27 23:41:03.912817867	52.52.240.208	443 192.168.0.102	44478	TCP	66	443 → 44478 [ACK] Seq=1 Ack=56 Win=184 Len=0 TSval=871935987 TSecr=14083159...
194	2022-10-27 23:41:03.913695957	52.52.240.208	443 192.168.0.102	44478	TLSv...	107	Application Data
196	2022-10-27 23:41:03.956760022	192.168.0.102	44478 52.52.240.208	443	TCP	66	44478 → 443 [ACK] Seq=56 Ack=42 Win=501 Len=0 TSval=1408316304 TSecr=871935...
224	2022-10-27 23:41:04.932765102	192.168.0.102	56792 138.199.14.86	443	TCP	66	56792 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1326545945 TSecr=16167448...
225	2022-10-27 23:41:05.135881568	138.199.14.86	443 192.168.0.102	56792	TCP	66	[TCP ACKed unseen segment] 443 → 56792 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSva...
377	2022-10-27 23:41:08.772750979	192.168.0.102	42266 18.155.107.121	443	TCP	66	42266 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4133718232 TSecr=19878184...
378	2022-10-27 23:41:08.786952181	18.155.107.121	443 192.168.0.102	42266	TCP	66	[TCP ACKed unseen segment] 443 → 42266 [ACK] Seq=1 Ack=2 Win=140 Len=0 TSva...
389	2022-10-27 23:41:09.052623033	52.52.240.208	443 192.168.0.102	44478	TLSv...	101	Application Data
390	2022-10-27 23:41:09.052675840	192.168.0.102	44478 52.52.240.208	443	TCP	66	44478 → 443 [ACK] Seq=56 Ack=77 Win=501 Len=0 TSval=1408321400 TSecr=871941...
391	2022-10-27 23:41:09.052820677	192.168.0.102	44478 52.52.240.208	443	TLSv...	105	Application Data
404	2022-10-27 23:41:09.306031571	443 192.168.0.102	443 192.168.0.102	44478	TCP	66	443 → 44478 [ACK] Seq=77 Ack=95 Win=184 Len=0 TSval=871941435 TSecr=1408321...
409	2022-10-27 23:41:09.433016375	138.199.14.86	443 192.168.0.102	56792	TCP	66	[TCP Keep-Alive] [TCP ACKed unseen segment] 443 → 56792 [ACK] Seq=0 Ack=2 W...
410	2022-10-27 23:41:09.433060949	192.168.0.102	56792 138.199.14.86	443	TCP	66	[TCP Previous segment not captured] 56792 → 443 [ACK] Seq=2 Ack=1 Win=501 L...
514	2022-10-27 23:41:12.612879048	192.168.0.102	41336 184.26.12.177	443	TCP	64	41336 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0



DNS :

As the local system has cached ip of example.com, it need no dns resolution , So DNS request has been tracked by Wireshark

UDP :

As there is no DNS query for this particular request and the application need no additional UDP request , So nothing tracked in Wireshark

ARP :

No.	Time	Source	Source Destination	Dest Port	Protocol	Length	Info
1659	2022-10-27 23:41:36.302046026	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
1660	2022-10-27 23:41:36.302065346	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
4122	2022-10-27 23:42:22.382523207	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
4123	2022-10-27 23:42:22.382544501	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
7505	2022-10-27 23:43:29.215336703	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
7506	2022-10-27 23:43:29.215388896	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
14063	2022-10-27 23:44:15.023737149	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
14064	2022-10-27 23:44:15.023750768	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
21260	2022-10-27 23:45:03.504256929	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
21261	2022-10-27 23:45:03.504267521	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
25471	2022-10-27 23:45:39.600639097	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
25472	2022-10-27 23:45:39.600657622	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
30371	2022-10-27 23:46:24.641135740	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
30372	2022-10-27 23:46:24.641159658	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
38893	2022-10-27 23:47:03.329616788	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
38894	2022-10-27 23:47:03.329634621	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
44813	2022-10-27 23:47:42.257944581	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
44814	2022-10-27 23:47:42.257968831	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
50026	2022-10-27 23:48:23.778404553	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
50027	2022-10-27 23:48:23.778436720	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
54681	2022-10-27 23:49:02.760005812	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
54682	2022-10-27 23:49:02.760031924	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
58983	2022-10-27 23:49:38.835183980	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
58984	2022-10-27 23:49:38.835195681	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
65598	2022-10-27 23:50:35.219742250	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1
65599	2022-10-27 23:50:35.219770288	IntelCor_1b:92:e8	10:27:f5:36:82:61		ARP	42	192.168.0.102 is at b8:9a:2a:1b:92:e8
78176	2022-10-27 23:50:57.171945354	10:27:f5:36:82:61	IntelCor_1b:92:e8		ARP	42	Who has 192.168.0.102? Tell 192.168.0.1

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.

Frame 147: 1657 bytes on wire (13256 bits), 1657 bytes captured (13256 bits) on interface wlo1, id 0

Ethernet II, Src: 10:27:f5:36:82:61 (10:27:f5:36:82:61), Dst: IntelCor_1b:92:e8 (b8:9a:2a:1b:92:e8)

- Destination: IntelCor_1b:92:e8 (b8:9a:2a:1b:92:e8)
 - Address: IntelCor_1b:92:e8 (b8:9a:2a:1b:92:e8)
 - 0. = LG bit: Globally unique address (factory default)
 - 0 = IG bit: Individual address (unicast)
- Source: 10:27:f5:36:82:61 (10:27:f5:36:82:61)
 - Address: 10:27:f5:36:82:61 (10:27:f5:36:82:61)
 - 0. = LG bit: Globally unique address (factory default)
 - 0 = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 93.184.216.34, Dst: 192.168.0.102
- Transmission Control Protocol, Src Port: 80, Dst Port: 51808, Seq: 1, Ack: 76, Len: 1591
- Hypertext Transfer Protocol
- Line-based text data: text/html (46 lines)

```

0000  b8 9a 2a 1b 92 e8 10 27 f5 36 82 61 08 00 45 00  ..*...'.6.a.E.
0010  06 6b dd 09 40 00 3b 06 65 9a 5d b8 d8 22 c0 a8  .k.@.;.e.]...
0020  00 66 00 50 ca 60 10 48 fe 5d ef 92 b3 94 80 18  .f.P.H.].....
0030  00 39 fd 46 00 00 01 01 08 0a aa 13 23 6c 4b 6b  .9.F....#lKk
0040  fa 3f 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f  .?HTTP/1.1 200 0
0050  4b 0d 0a 41 67 65 3a 20 32 30 32 31 34 38 0d 0a  K.Age: 202148.
0060  43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d  Cache-Control: m
0070  61 78 2d 61 67 65 3d 36 30 34 38 30 30 0d 0a 43  ax-age=6 04800.C
0080  6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78  ontent-Type: tex
0090  74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d  t/html; charset=
00a0  55 54 46 2d 38 0d 0a 44 61 74 65 3a 20 54 68 75  UTF-8.D ate: Thu

```

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

Manufacturer of my PC's NIC - Intel

Manufacturer of server's NIC - Can't be detected by Wireshark

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

Hex values of my PC's OUI - b8:9a:2a

Hex values of server's OUI - 10:27:f5

9. Find the following statistics:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	516	100.0	96628	33 k	0	0
Ethernet	100.0	516	7.5	7224	2,532	0	0
Internet Protocol Version 4	99.6	514	10.6	10280	3,604	0	0
User Datagram Protocol	39.7	205	1.7	1640	574	0	0
Domain Name System	2.7	14	1.2	1133	397	14	1133
Data	37.0	191	35.6	34424	12 k	191	34424
Transmission Control Protocol	59.9	309	43.3	41865	14 k	214	11012
Transport Layer Security	11.2	58	26.1	25191	8,832	56	15277
SSH Protocol	5.2	27	3.9	3808	1,335	27	3808
Hypertext Transfer Protocol	2.3	12	8.6	8302	2,910	6	2735
Portable Network Graphics	0.2	1	0.1	124	43	1	124
Line-based text data	1.0	5	7.1	6852	2,402	5	5164
Address Resolution Protocol	0.4	2	0.1	56	19	2	56

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

- 26.0 % of packets in the capture are TCP
- Higher level protocols using TCP - HTTP, FTP

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

- 73.6% packets are UDP
- Higher level protocols using UDP- SNMP

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

