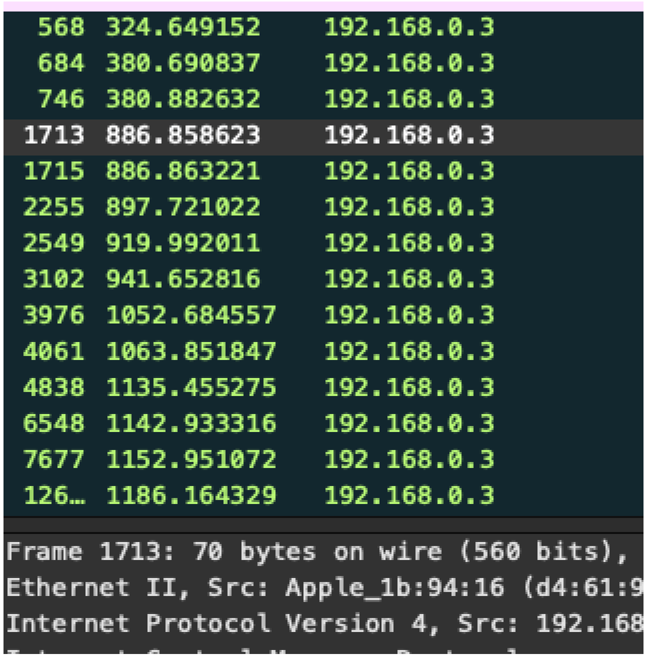
Assignment 4: Wireshark

GOOGLE DRIVE LINK FOR PCAP FILE

https://drive.google.com/file/d/1uB_wpkKT7t-Te2_RP9XyGLL_coQitK36/view?usp=share_link

Student number 22203536

1. So to find my IP address I typed in filters that were relevant to the network activities I performed such as icmp or http and then found which source address was consistent across the activities. The ip address was found to be 192.168.0.3. An example image is shown below

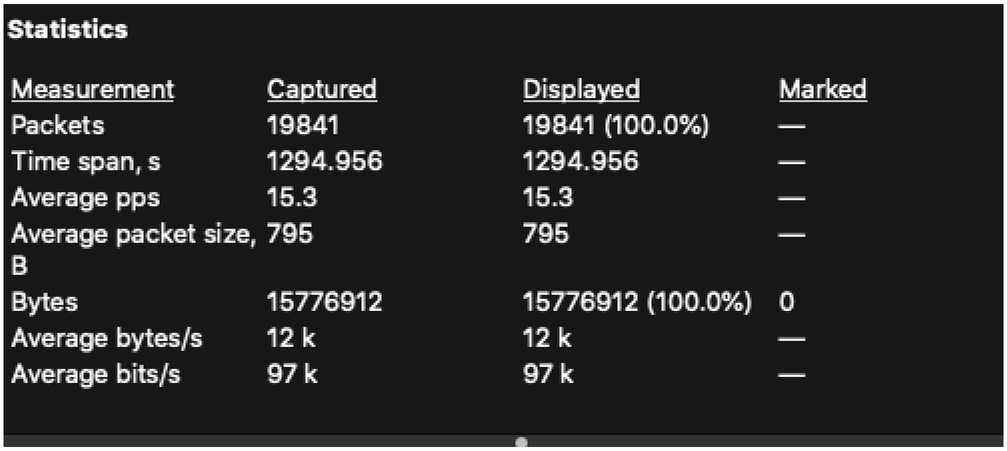


```
  568  324.649152    192.168.0.3
  684  380.690837    192.168.0.3
  746  380.882632    192.168.0.3
 1713  886.858623    192.168.0.3
 1715  886.863221    192.168.0.3
 2255  897.721022    192.168.0.3
 2549  919.992011    192.168.0.3
 3102  941.652816    192.168.0.3
 3976  1052.684557   192.168.0.3
 4061  1063.851847   192.168.0.3
 4838  1135.455275   192.168.0.3
 6548  1142.933316   192.168.0.3
 7677  1152.951072   192.168.0.3
 126…  1186.164329   192.168.0.3

Frame 1713: 70 bytes on wire (560 bits),
Ethernet II, Src: Apple_1b:94:16 (d4:61:9
Internet Protocol Version 4, Src: 192.168
```

Question 2

In the wire shark capture file properties I am able to view the relevant statistics from the image below



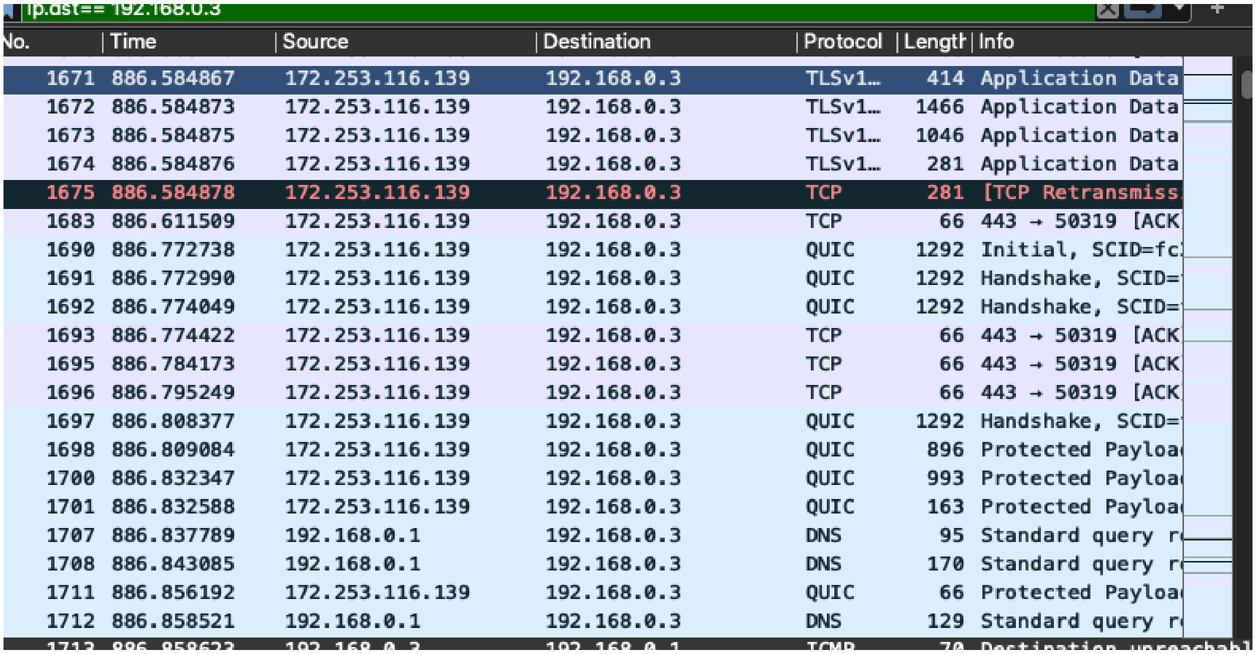
Statistics

Measurement	Captured	Displayed	Marked
Packets	19841	19841 (100.0%)	—
Time span, s	1294.956	1294.956	—
Average pps	15.3	15.3	—
Average packet size, B	795	795	—
Bytes	15776912	15776912 (100.0%)	0
Average bytes/s	12 k	12 k	—
Average bits/s	97 k	97 k	—

So filling out the table
Time span , s = 1295 seconds (to nearest second)
Total packets= 19841 packets
Bytes MiB = 15776912 / 1048576 = 15.05 MiB
Average packet size, B = 795 bytes
Average packets per second, pps = 15.3 pps
Average bits/second = 97000 bits per second

3.

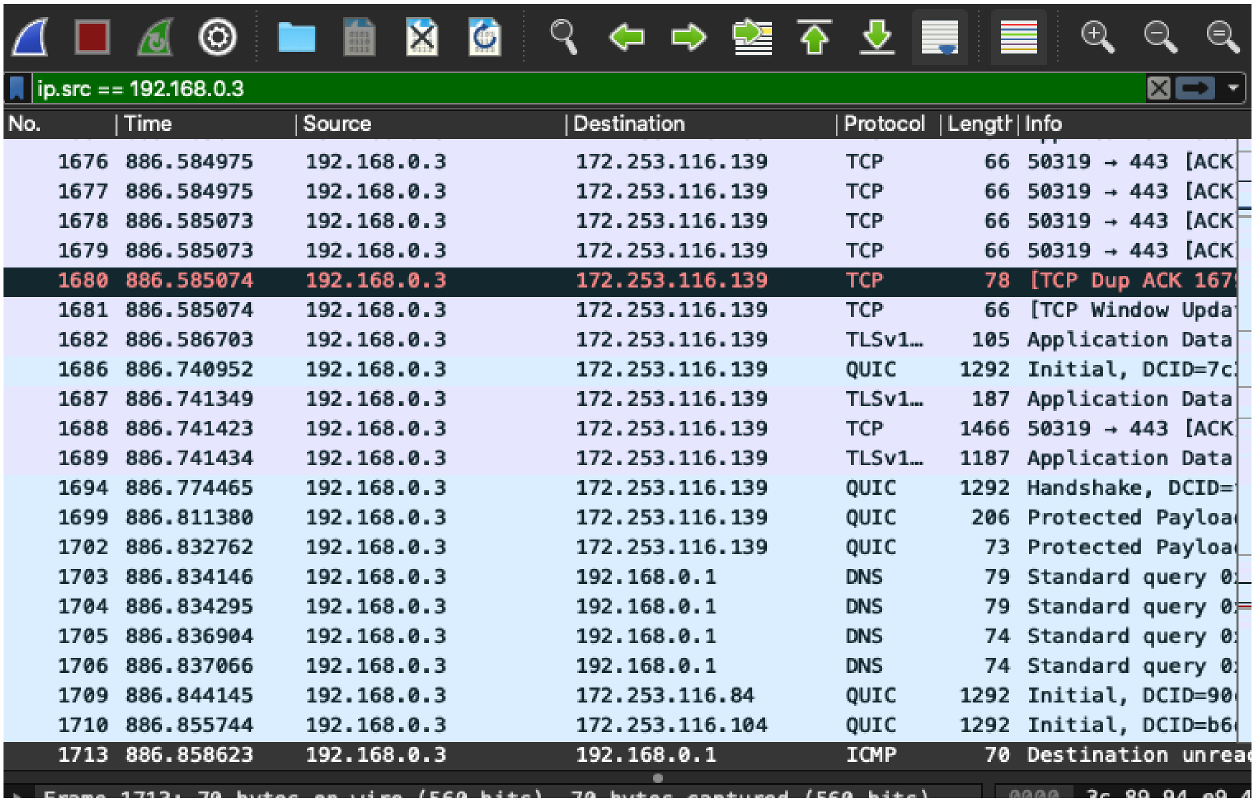
a) ip.dst == 192.168.0.3
(image below)



ip.dst== 192.168.0.3

No.	Time	Source	Destination	Protocol	Length	Info
1671	886.584867	172.253.116.139	192.168.0.3	TLSv1…	414	Application Data
1672	886.584873	172.253.116.139	192.168.0.3	TLSv1…	1466	Application Data
1673	886.584875	172.253.116.139	192.168.0.3	TLSv1…	1046	Application Data
1674	886.584876	172.253.116.139	192.168.0.3	TLSv1…	281	Application Data
1675	886.584878	172.253.116.139	192.168.0.3	TCP	281	[TCP Retransmiss
1683	886.611509	172.253.116.139	192.168.0.3	TCP	66	443 → 50319 [ACK
1690	886.772738	172.253.116.139	192.168.0.3	QUIC	1292	Initial, SCID=fc
1691	886.772990	172.253.116.139	192.168.0.3	QUIC	1292	Handshake, SCID=
1692	886.774049	172.253.116.139	192.168.0.3	QUIC	1292	Handshake, SCID=
1693	886.774422	172.253.116.139	192.168.0.3	TCP	66	443 → 50319 [ACK
1695	886.784173	172.253.116.139	192.168.0.3	TCP	66	443 → 50319 [ACK
1696	886.795249	172.253.116.139	192.168.0.3	TCP	66	443 → 50319 [ACK
1697	886.808377	172.253.116.139	192.168.0.3	QUIC	1292	Handshake, SCID=
1698	886.809084	172.253.116.139	192.168.0.3	QUIC	896	Protected Payloa
1700	886.832347	172.253.116.139	192.168.0.3	QUIC	993	Protected Payloa
1701	886.832588	172.253.116.139	192.168.0.3	QUIC	163	Protected Payloa
1707	886.837789	192.168.0.1	192.168.0.3	DNS	95	Standard query r
1708	886.843085	192.168.0.1	192.168.0.3	DNS	170	Standard query r
1711	886.856192	172.253.116.139	192.168.0.3	QUIC	66	Protected Payloa
1712	886.858521	192.168.0.1	192.168.0.3	DNS	129	Standard query r
1713	886.858623	192.168.0.3	192.168.0.1	ICMP	70	Destination unreachabl

b) ip.src == 192.168.0.3
(image is shown below)



```
ip.src == 192.168.0.3

No.    |Time        |Source          |Destination       |Protocol |Length|Info
  1676 886.584975   192.168.0.3      172.253.116.139    TCP          66  50319 → 443 [ACK
  1677 886.584975   192.168.0.3      172.253.116.139    TCP          66  50319 → 443 [ACK
  1678 886.585073   192.168.0.3      172.253.116.139    TCP          66  50319 → 443 [ACK
  1679 886.585073   192.168.0.3      172.253.116.139    TCP          66  50319 → 443 [ACK
  1680 886.585074   192.168.0.3      172.253.116.139    TCP          78  [TCP Dup ACK 167
  1681 886.585074   192.168.0.3      172.253.116.139    TCP          66  [TCP Window Upda
  1682 886.586703   192.168.0.3      172.253.116.139    TLSv1…      105  Application Data
  1686 886.740952   192.168.0.3      172.253.116.139    QUIC       1292  Initial, DCID=7c
  1687 886.741349   192.168.0.3      172.253.116.139    TLSv1…      187  Application Data
  1688 886.741423   192.168.0.3      172.253.116.139    TCP        1466  50319 → 443 [ACK
  1689 886.741434   192.168.0.3      172.253.116.139    TLSv1…     1187  Application Data
  1694 886.774465   192.168.0.3      172.253.116.139    QUIC       1292  Handshake, DCID=
  1699 886.811380   192.168.0.3      172.253.116.139    QUIC        206  Protected Payloa
  1702 886.832762   192.168.0.3      172.253.116.139    QUIC         73  Protected Payloa
  1703 886.834146   192.168.0.3      192.168.0.1        DNS          79  Standard query 0
  1704 886.834295   192.168.0.3      192.168.0.1        DNS          79  Standard query 0
  1705 886.836904   192.168.0.3      192.168.0.1        DNS          74  Standard query 0
  1706 886.837066   192.168.0.3      192.168.0.1        DNS          74  Standard query 0
  1709 886.844145   192.168.0.3      172.253.116.84     QUIC       1292  Initial, DCID=90
  1710 886.855744   192.168.0.3      172.253.116.104    QUIC       1292  Initial, DCID=b6
  1713 886.858623   192.168.0.3      192.168.0.1        ICMP         70  Destination unrea

Frame 1713: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)     0000  3c 89 94 e9 4
```

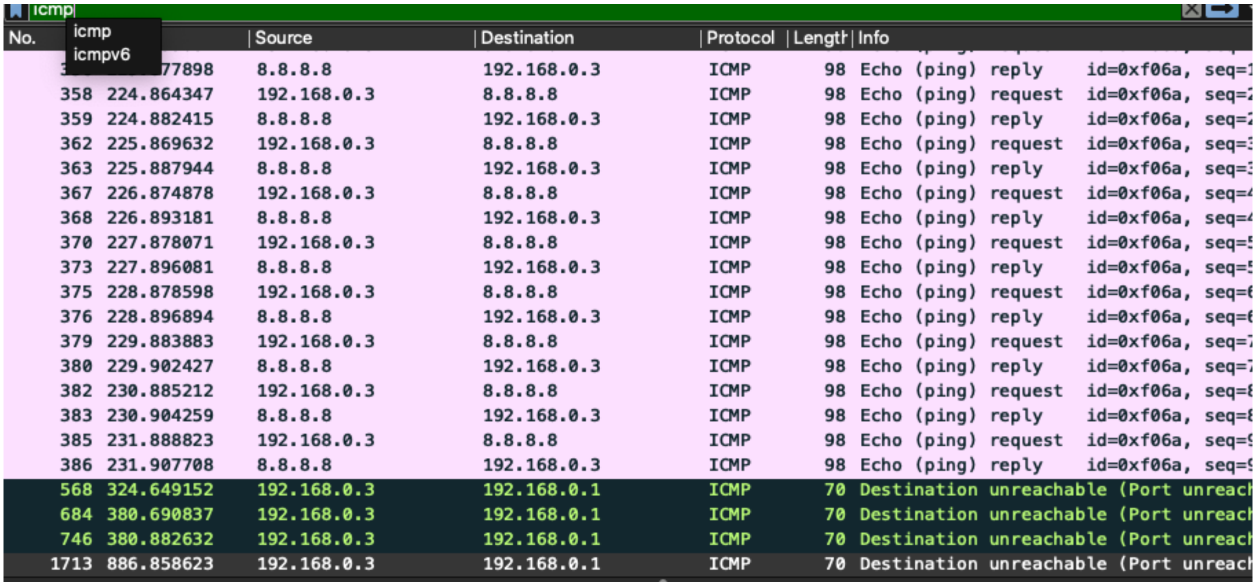
4.

a) Ping command is used to test if host is reachable on IP network and it also measures the packets round trip time

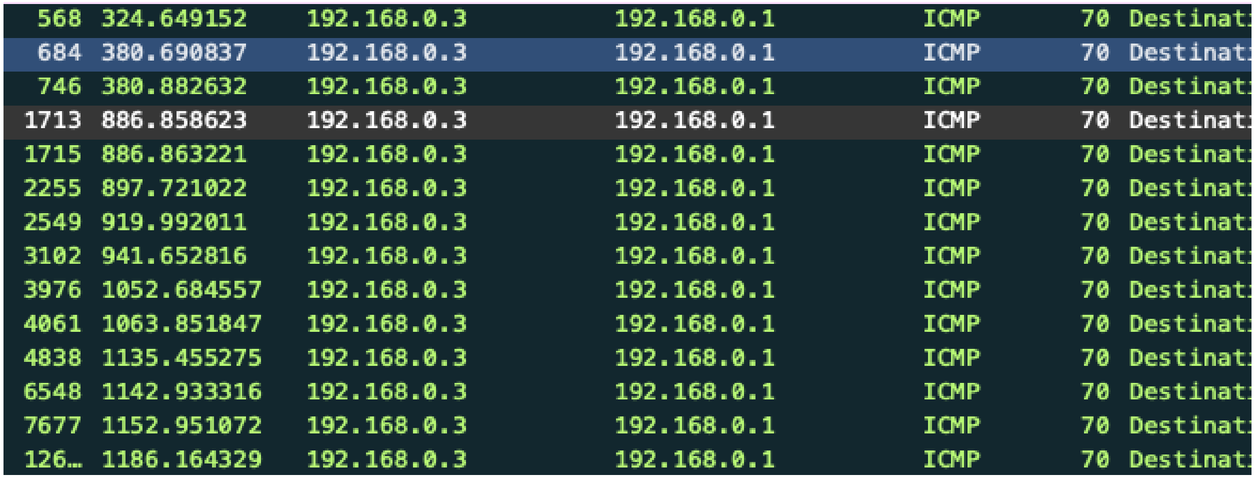
b) ICMP

c) icmp

d) I can see 31 packets total (note that these 2 images below overlap somewhat but there are in fact 31 total)



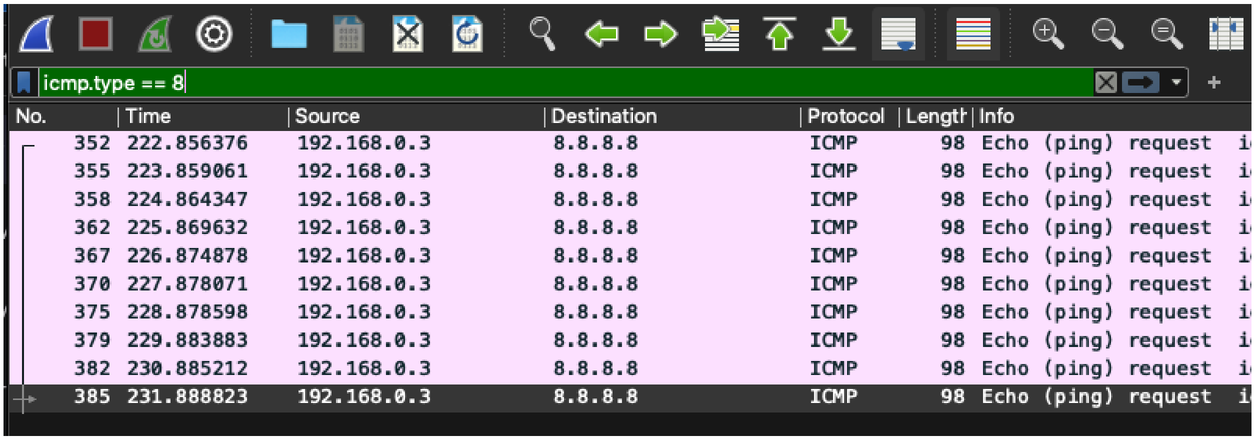
```
No.                 |Source          |Destination     |Protocol |Length|Info
 3     77898         8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=1
 358  224.864347     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=2
 359  224.882415     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=2
 362  225.869632     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=3
 363  225.887944     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=3
 367  226.874878     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=4
 368  226.893181     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=4
 370  227.878071     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=5
 373  227.896081     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=5
 375  228.878598     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=6
 376  228.896894     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=6
 379  229.883883     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=7
 380  229.902427     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=7
 382  230.885212     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=8
 383  230.904259     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=8
 385  231.888823     192.168.0.3      8.8.8.8          ICMP       98 Echo (ping) request  id=0xf06a, seq=9
 386  231.907708     8.8.8.8          192.168.0.3      ICMP       98 Echo (ping) reply    id=0xf06a, seq=9
 568  324.649152     192.168.0.3      192.168.0.1      ICMP       70 Destination unreachable (Port unreach
 684  380.690837     192.168.0.3      192.168.0.1      ICMP       70 Destination unreachable (Port unreach
 746  380.882632     192.168.0.3      192.168.0.1      ICMP       70 Destination unreachable (Port unreach
1713  886.858623     192.168.0.3      192.168.0.1      ICMP       70 Destination unreachable (Port unreach
```



```
 568  324.649152    192.168.0.3    192.168.0.1    ICMP    70  Destinat
 684  380.690837    192.168.0.3    192.168.0.1    ICMP    70  Destinat
 746  380.882632    192.168.0.3    192.168.0.1    ICMP    70  Destinat
1713  886.858623    192.168.0.3    192.168.0.1    ICMP    70  Destinat
1715  886.863221    192.168.0.3    192.168.0.1    ICMP    70  Destinat
2255  897.721022    192.168.0.3    192.168.0.1    ICMP    70  Destinat
2549  919.992011    192.168.0.3    192.168.0.1    ICMP    70  Destinat
3102  941.652816    192.168.0.3    192.168.0.1    ICMP    70  Destinat
3976  1052.684557   192.168.0.3    192.168.0.1    ICMP    70  Destinat
4061  1063.851847   192.168.0.3    192.168.0.1    ICMP    70  Destinat
4838  1135.455275   192.168.0.3    192.168.0.1    ICMP    70  Destinat
6548  1142.933316   192.168.0.3    192.168.0.1    ICMP    70  Destinat
7677  1152.951072   192.168.0.3    192.168.0.1    ICMP    70  Destinat
126…  1186.164329   192.168.0.3    192.168.0.1    ICMP    70  Destinat
```

e) Because you also see ICMP replies in addition to ICMP requests and destination unreached

f) You can filter by using icmp.type == 8
(image shown below)



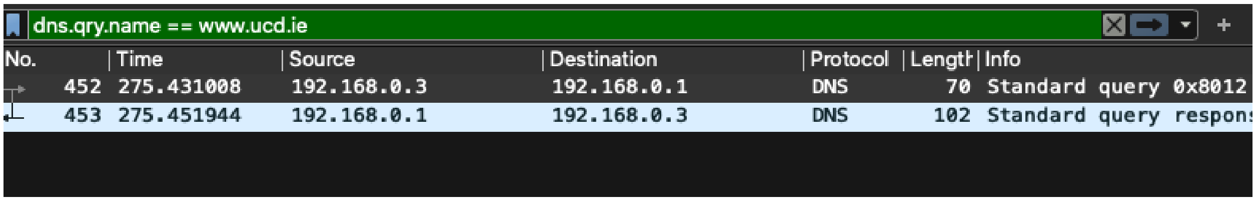
icmp.type == 8

No.	Time	Source	Destination	Protocol	Length	Info
352	222.856376	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
355	223.859061	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
358	224.864347	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
362	225.869632	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
367	226.874878	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
370	227.878071	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
375	228.878598	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
379	229.883883	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
382	230.885212	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i
385	231.888823	192.168.0.3	8.8.8.8	ICMP	98	Echo (ping) request i

Question 5

a) nslookup is used to query the DNS servers for in order to get info about domain names and IP addresses

b) dns.qry.name == www.ucd.ie



dns.qry.name == www.ucd.ie

No.	Time	Source	Destination	Protocol	Length	Info
452	275.431008	192.168.0.3	192.168.0.1	DNS	70	Standard query 0x8012
453	275.451944	192.168.0.1	192.168.0.3	DNS	102	Standard query respons

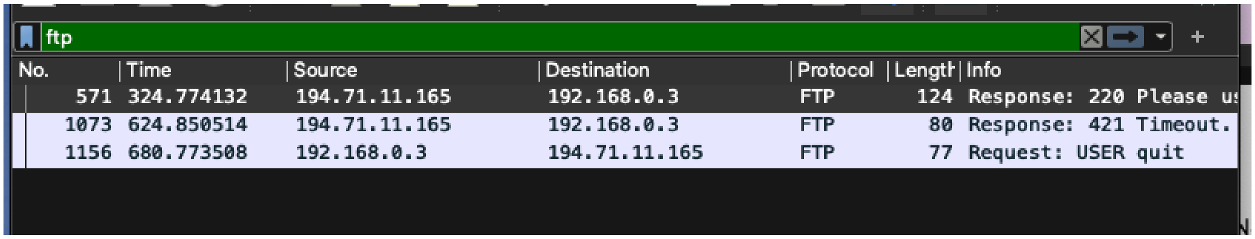
Question 6.

a) Ftp command transfers files between a client and a server using the FTP protocol.

b) Ftp

c)

From the image I can see 3 packets.

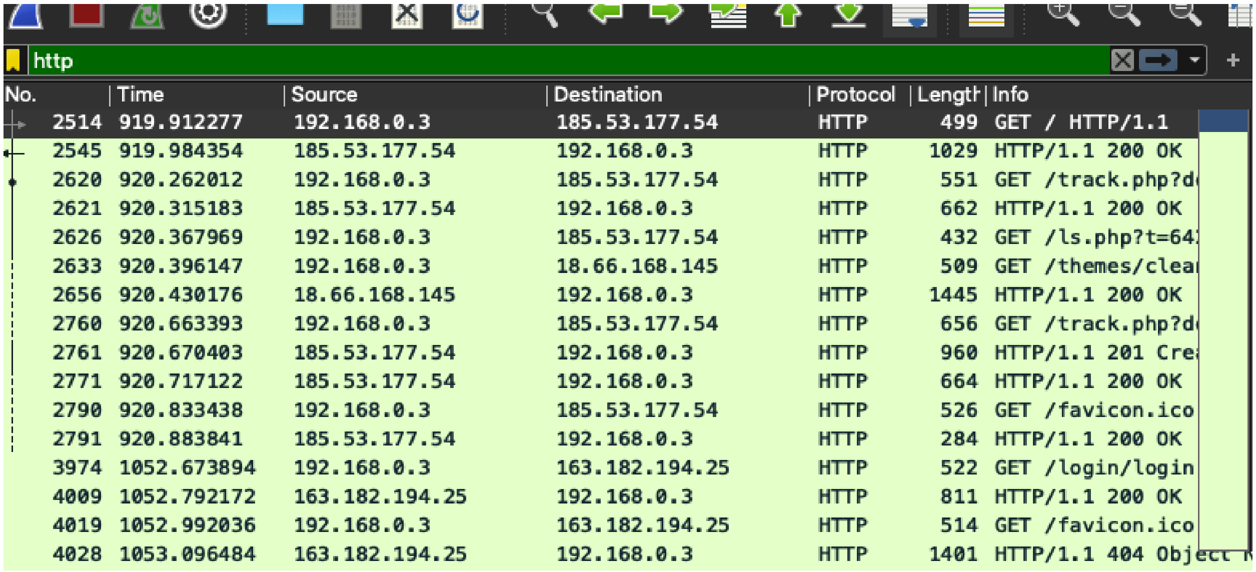


ftp

No.	Time	Source	Destination	Protocol	Length	Info
571	324.774132	194.71.11.165	192.168.0.3	FTP	124	Response: 220 Please u
1073	624.850514	194.71.11.165	192.168.0.3	FTP	80	Response: 421 Timeout.
1156	680.773508	192.168.0.3	194.71.11.165	FTP	77	Request: USER quit

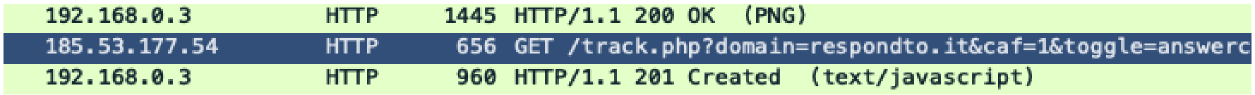
Question 7.

a) You filter using http as shown in the image below



```
http
No.   Time         Source           Destination      Protocol Length Info
 2514 919.912277   192.168.0.3      185.53.177.54    HTTP      499  GET / HTTP/1.1
 2545 919.984354   185.53.177.54    192.168.0.3      HTTP     1029  HTTP/1.1 200 OK
 2620 920.262012   192.168.0.3      185.53.177.54    HTTP      551  GET /track.php?d
 2621 920.315183   185.53.177.54    192.168.0.3      HTTP      662  HTTP/1.1 200 OK
 2626 920.367969   192.168.0.3      185.53.177.54    HTTP      432  GET /ls.php?t=64
 2633 920.396147   192.168.0.3      18.66.168.145    HTTP      509  GET /themes/clea
 2656 920.430176   18.66.168.145    192.168.0.3      HTTP     1445  HTTP/1.1 200 OK
 2760 920.663393   192.168.0.3      185.53.177.54    HTTP      656  GET /track.php?d
 2761 920.670403   185.53.177.54    192.168.0.3      HTTP      960  HTTP/1.1 201 Cre
 2771 920.717122   185.53.177.54    192.168.0.3      HTTP      664  HTTP/1.1 200 OK
 2790 920.833438   192.168.0.3      185.53.177.54    HTTP      526  GET /favicon.ico
 2791 920.883841   185.53.177.54    192.168.0.3      HTTP      284  HTTP/1.1 200 OK
 3974 1052.673894  192.168.0.3      163.182.194.25   HTTP      522  GET /login/login
 4009 1052.792172  163.182.194.25   192.168.0.3      HTTP      811  HTTP/1.1 200 OK
 4019 1052.992036  192.168.0.3      163.182.194.25   HTTP      514  GET /favicon.ico
 4028 1053.096484  163.182.194.25   192.168.0.3      HTTP     1401  HTTP/1.1 404 Object
```

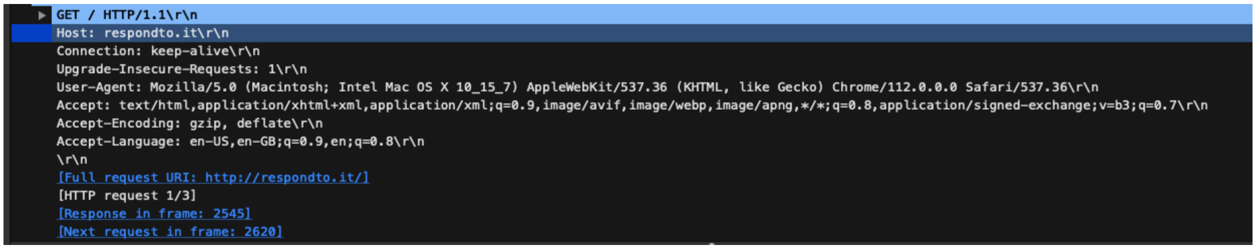
b)



```
192.168.0.3      HTTP   1445 HTTP/1.1 200 OK  (PNG)
185.53.177.54    HTTP    656 GET /track.php?domain=respondto.it&caf=1&toggle=answerc
192.168.0.3      HTTP    960 HTTP/1.1 201 Created  (text/javascript)
```

From the image the ip address of the respondto.it is 185.53.177.54

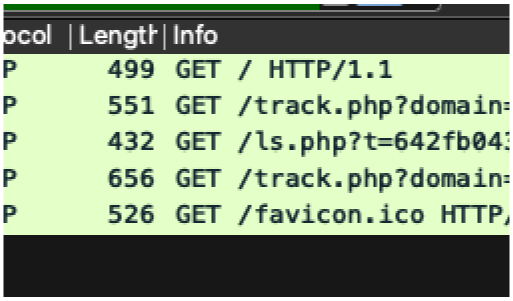
c) from the following image



```
GET / HTTP/1.1\r\n
Host: respondto.it\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://respondto.it/]
[HTTP request 1/3]
[Response in frame: 2545]
[Next request in frame: 2620]
```

I can see the url in the HTTP header

d) the methods are GET requests based on the image below

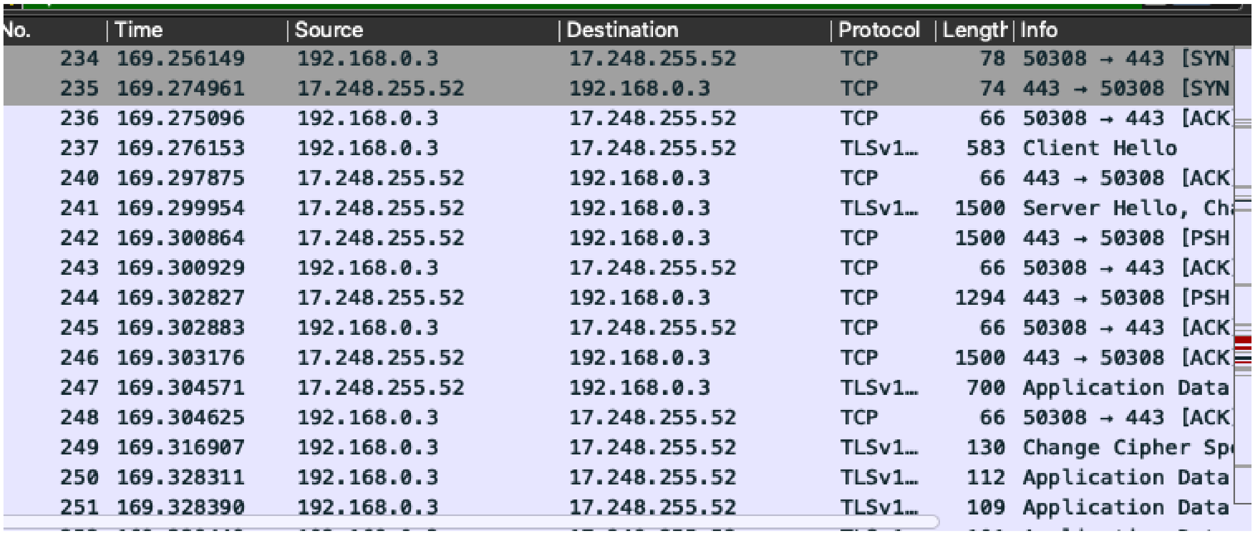


ocol	Lengt	Info
P	499	GET / HTTP/1.1
P	551	GET /track.php?domain=
P	432	GET /ls.php?t=642fb04
P	656	GET /track.php?domain=
P	526	GET /favicon.ico HTTP/

e) DNS protocol

Question 8.

a) Yes I can see TCP frames when I apply the tcp filter shown in the image below.



lo.	Time	Source	Destination	Protocol	Lengt	Info
234	169.256149	192.168.0.3	17.248.255.52	TCP	78	50308 → 443 [SYN
235	169.274961	17.248.255.52	192.168.0.3	TCP	74	443 → 50308 [SYN
236	169.275096	192.168.0.3	17.248.255.52	TCP	66	50308 → 443 [ACK
237	169.276153	192.168.0.3	17.248.255.52	TLSv1…	583	Client Hello
240	169.297875	17.248.255.52	192.168.0.3	TCP	66	443 → 50308 [ACK
241	169.299954	17.248.255.52	192.168.0.3	TLSv1…	1500	Server Hello, Ch
242	169.300864	17.248.255.52	192.168.0.3	TCP	1500	443 → 50308 [PSH
243	169.300929	192.168.0.3	17.248.255.52	TCP	66	50308 → 443 [ACK
244	169.302827	17.248.255.52	192.168.0.3	TCP	1294	443 → 50308 [PSH
245	169.302883	192.168.0.3	17.248.255.52	TCP	66	50308 → 443 [ACK
246	169.303176	17.248.255.52	192.168.0.3	TCP	1500	443 → 50308 [ACK
247	169.304571	17.248.255.52	192.168.0.3	TLSv1…	700	Application Data
248	169.304625	192.168.0.3	17.248.255.52	TCP	66	50308 → 443 [ACK
249	169.316907	192.168.0.3	17.248.255.52	TLSv1…	130	Change Cipher Sp
250	169.328311	192.168.0.3	17.248.255.52	TLSv1…	112	Application Data
251	169.328390	192.168.0.3	17.248.255.52	TLSv1…	109	Application Data

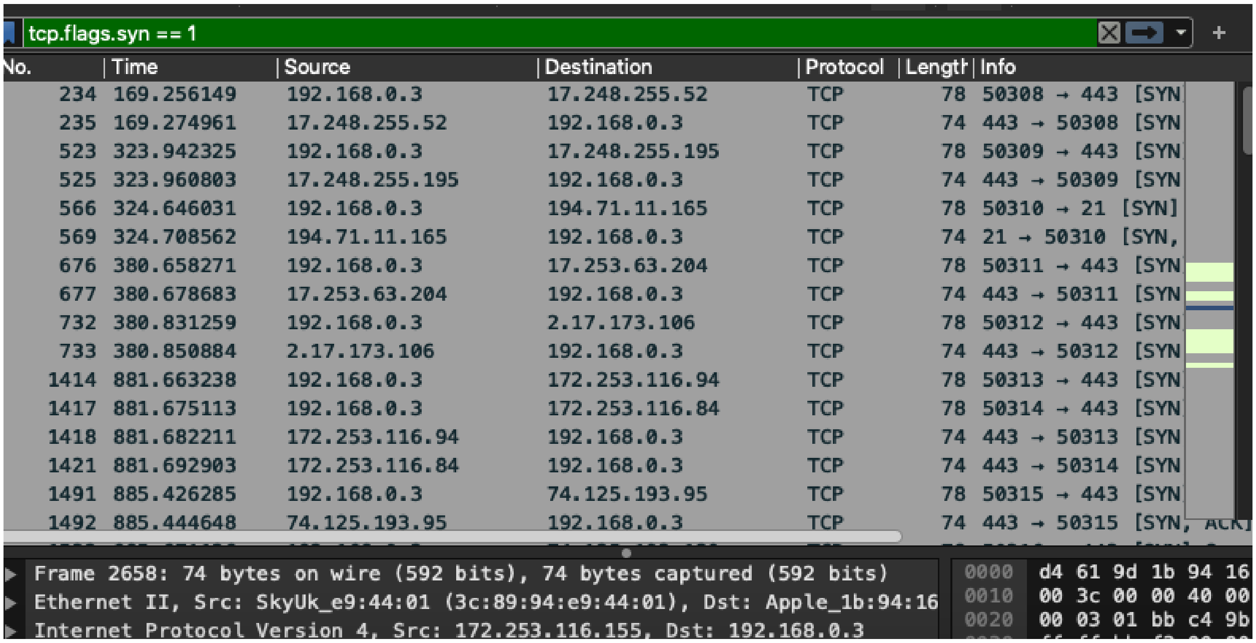
b) A 3 way handshake is a process that is used to create a connection between a client and a server. It consists of an ACK packet from the client side, a SYN packet from the client side and a SYN-ACK packet from the server.

c) The filter required is tcp.flags.syn == 1

d) data-text-lines contains "vbsca"

e) In the packet details pane go to the HTTP section then the form data subsection to see username and password.

An image of the implementation is shown below on the next page



```
tcp.flags.syn == 1

No.    Time         Source           Destination      Protocol  Length Info
   234 169.256149   192.168.0.3      17.248.255.52    TCP       78 50308 → 443 [SYN
   235 169.274961   17.248.255.52    192.168.0.3      TCP       74 443 → 50308 [SYN
   523 323.942325   192.168.0.3      17.248.255.195   TCP       78 50309 → 443 [SYN
   525 323.960803   17.248.255.195   192.168.0.3      TCP       74 443 → 50309 [SYN
   566 324.646031   192.168.0.3      194.71.11.165    TCP       78 50310 → 21 [SYN]
   569 324.708562   194.71.11.165    192.168.0.3      TCP       74 21 → 50310 [SYN,
   676 380.658271   192.168.0.3      17.253.63.204    TCP       78 50311 → 443 [SYN
   677 380.678683   17.253.63.204    192.168.0.3      TCP       74 443 → 50311 [SYN
   732 380.831259   192.168.0.3      2.17.173.106     TCP       78 50312 → 443 [SYN
   733 380.850884   2.17.173.106     192.168.0.3      TCP       74 443 → 50312 [SYN
  1414 881.663238   192.168.0.3      172.253.116.94   TCP       78 50313 → 443 [SYN
  1417 881.675113   192.168.0.3      172.253.116.84   TCP       78 50314 → 443 [SYN
  1418 881.682211   172.253.116.94   192.168.0.3      TCP       74 443 → 50313 [SYN
  1421 881.692903   172.253.116.84   192.168.0.3      TCP       74 443 → 50314 [SYN
  1491 885.426285   192.168.0.3      74.125.193.95    TCP       78 50315 → 443 [SYN
  1492 885.444648   74.125.193.95    192.168.0.3      TCP       74 443 → 50315 [SYN, ACK]

▶ Frame 2658: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)       0000  d4 61 9d 1b 94 16
▶ Ethernet II, Src: SkyUk_e9:44:01 (3c:89:94:e9:44:01), Dst: Apple_1b:94:16   0010  00 3c 00 00 40 00
▶ Internet Protocol Version 4, Src: 172.253.116.155, Dst: 192.168.0.3         0020  00 03 01 bb c4 9b
```

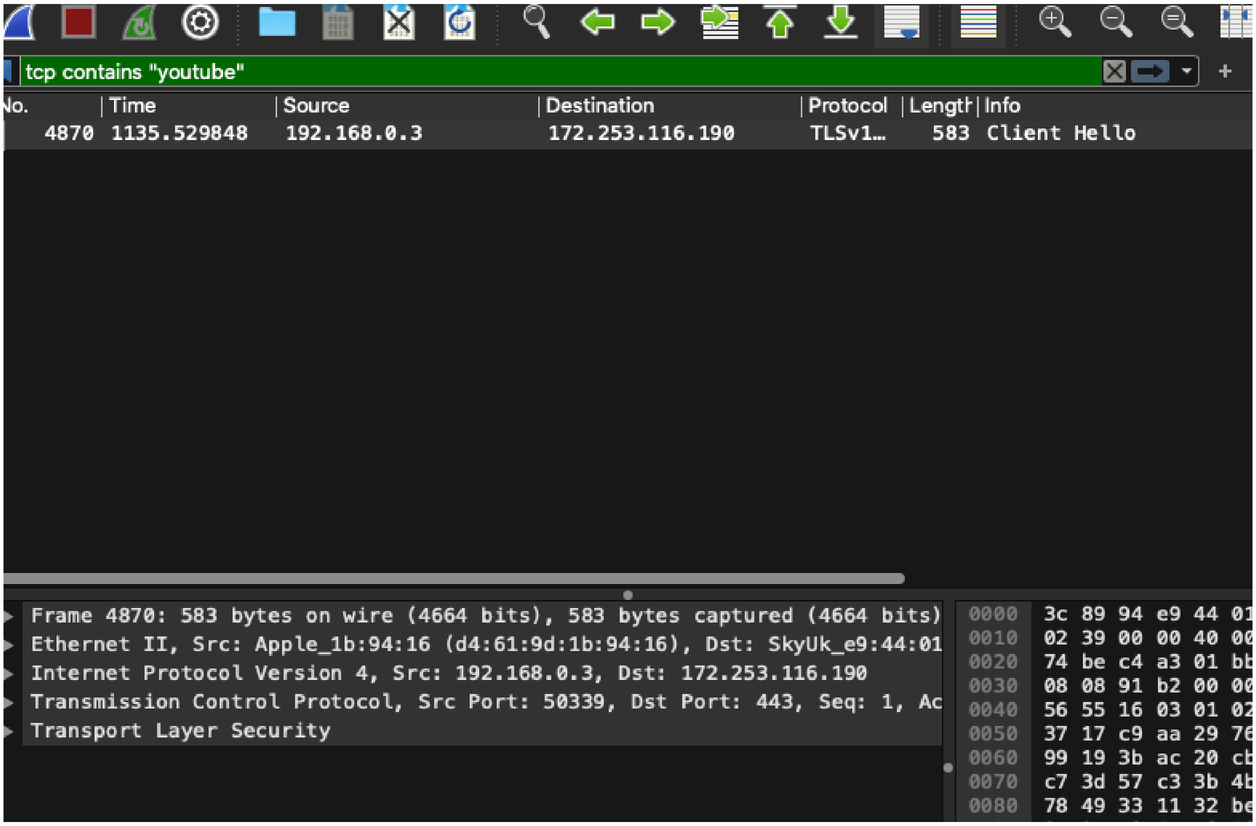
9.

a)

Use filter tcp contains “youtube”

Image below

Continued on next page



tcp contains "youtube"

```
No.   Time          Source          Destination       Protocol  Length Info
 4870 1135.529848   192.168.0.3     172.253.116.190   TLSv1…    583 Client Hello
```

```
Frame 4870: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
Ethernet II, Src: Apple_1b:94:16 (d4:61:9d:1b:94:16), Dst: SkyUk_e9:44:01
Internet Protocol Version 4, Src: 192.168.0.3, Dst: 172.253.116.190
Transmission Control Protocol, Src Port: 50339, Dst Port: 443, Seq: 1, Ac
Transport Layer Security
```

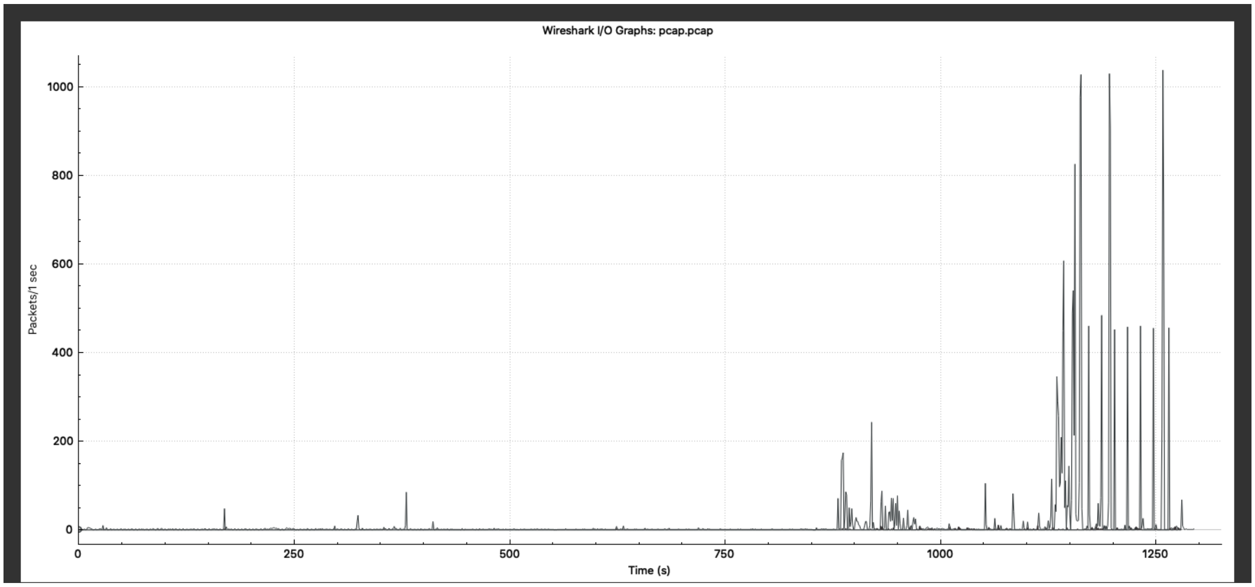
```
0000  3c 89 94 e9 44 01
0010  02 39 00 00 40 00
0020  74 be c4 a3 01 bb
0030  08 08 91 b2 00 00
0040  56 55 16 03 01 02
0050  37 17 c9 aa 29 76
0060  99 19 3b ac 20 cb
0070  c7 3d 57 c3 3b 4b
0080  78 49 33 11 32 be
```

b) the protocol shown in the image above for that packet is TLSv1.3
c) one way SSL is a security process where the client verifies the servers identity using the servers public key certificate.

Two way SSL both the client and the server verify each others identity via their public key certificates. Authentication is “2 way “ and mutual so this will give a higher level of security than one way SSL.

Continued on next page

10)



Wireshark I/O Graphs: pcap.pcap
Packets/1 sec
1000
800
600
400
200
0
0
250
500
750
1000
1250
Time (s)