Name	: Md. Nazmul Hasan
ID	: IT-17005
Lab No	: 01
Name of the Lab	: Protocol analysis with Wireshark

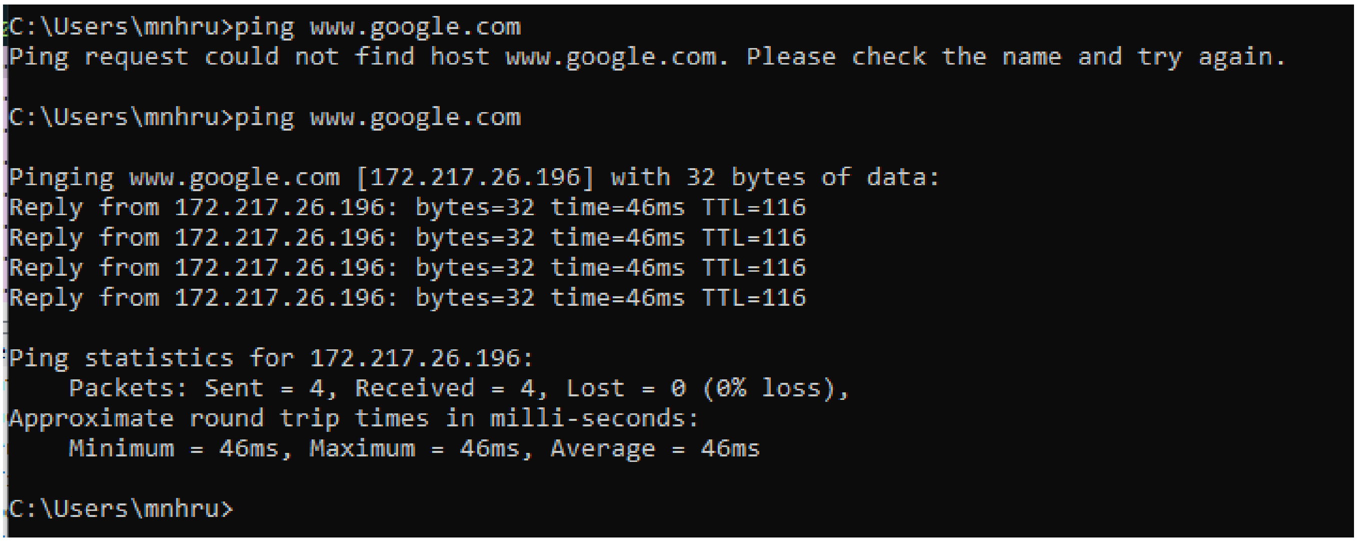
Objectives:

i) Packets and Protocols can be analyzed after capture.
ii) Individual fields and protocols can be easily seen.
iii) Graph and flow diagram can be helpful in analysis.

Protocol analysis with Wireshark

1. ICMP: The Internet Control Message Protocol is an internet layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers.

Ping is a utility which uses ICMP messages to report back information on network connectivity and the speed of data relay between a host and a destination computer. It's one of the few instances where a user can interact directly with ICMP, which typically only functions to allow networked computers to communicate with one another automatically.



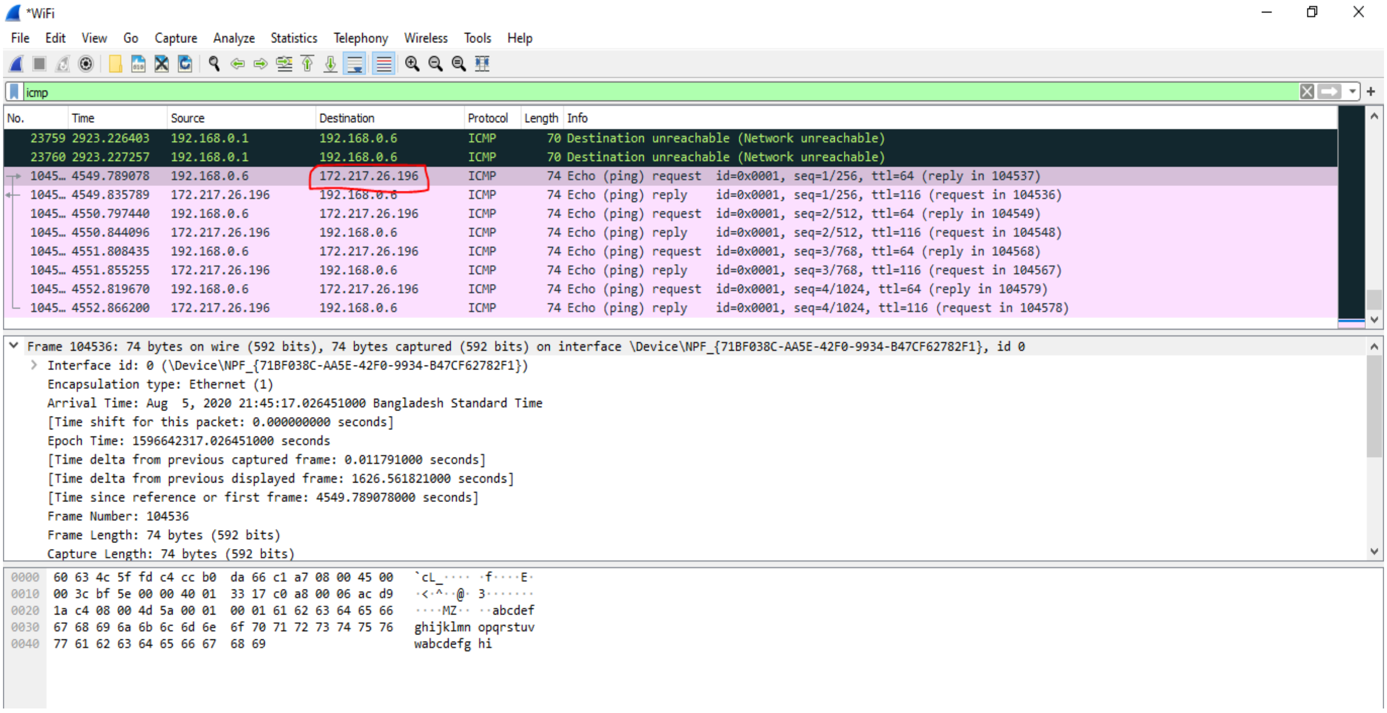
```
C:\Users\mnhru>ping www.google.com
Ping request could not find host www.google.com. Please check the name and try again.

C:\Users\mnhru>ping www.google.com

Pinging www.google.com [172.217.26.196] with 32 bytes of data:
Reply from 172.217.26.196: bytes=32 time=46ms TTL=116
Reply from 172.217.26.196: bytes=32 time=46ms TTL=116
Reply from 172.217.26.196: bytes=32 time=46ms TTL=116
Reply from 172.217.26.196: bytes=32 time=46ms TTL=116

Ping statistics for 172.217.26.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 46ms, Average = 46ms

C:\Users\mnhru>
```


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp
```

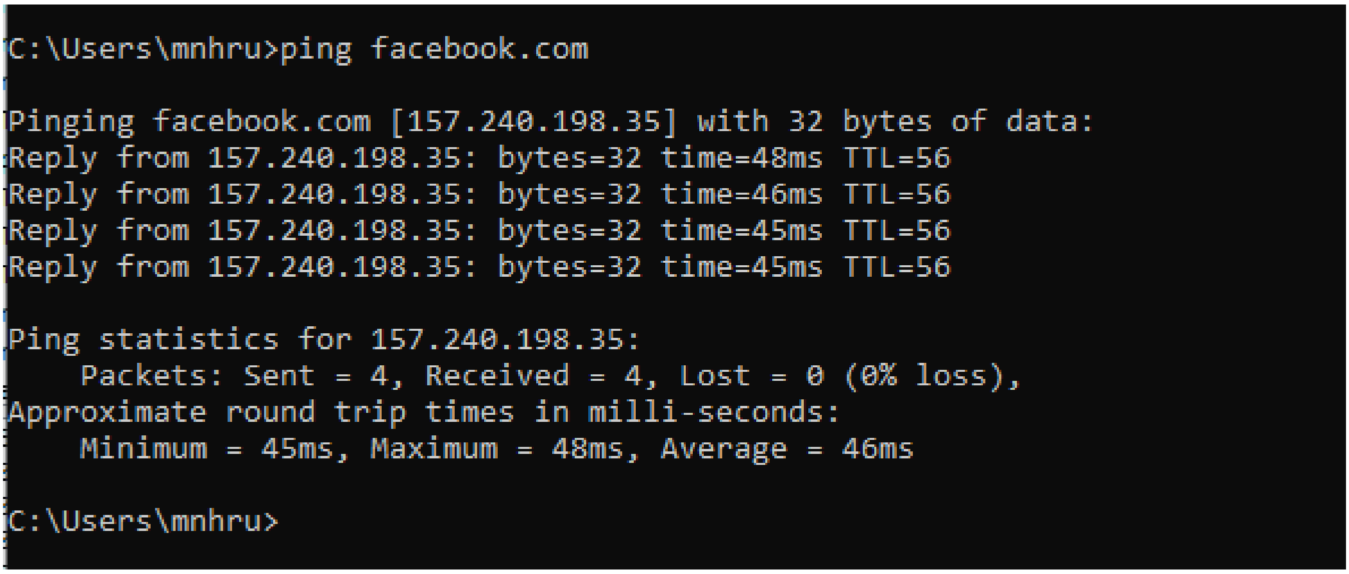
```
No.        Time          Source           Destination      Protocol  Length  Info
  23759 2923.226403   192.168.0.1      192.168.0.6      ICMP     70 Destination unreachable (Network unreachable)
  23760 2923.227257   192.168.0.1      192.168.0.6      ICMP     70 Destination unreachable (Network unreachable)
  1045… 4549.789078   192.168.0.6      172.217.26.196   ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (reply in 104537)
  1045… 4549.835789   172.217.26.196   192.168.0.6      ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=116 (request in 104536)
  1045… 4550.797440   192.168.0.6      172.217.26.196   ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=64 (reply in 104549)
  1045… 4550.844096   172.217.26.196   192.168.0.6      ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=116 (request in 104548)
  1045… 4551.808435   192.168.0.6      172.217.26.196   ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=64 (reply in 104568)
  1045… 4551.855255   172.217.26.196   192.168.0.6      ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=116 (request in 104567)
  1045… 4552.819670   192.168.0.6      172.217.26.196   ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=64 (reply in 104579)
  1045… 4552.866200   172.217.26.196   192.168.0.6      ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=116 (request in 104578)
```

```
Frame 104536: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1}, id 0
  Interface id: 0 (\Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1})
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug  5, 2020 21:45:17.026451000 Bangladesh Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1596642317.026451000 seconds
  [Time delta from previous captured frame: 0.011791000 seconds]
  [Time delta from previous displayed frame: 1626.561821000 seconds]
  [Time since reference or first frame: 4549.789078000 seconds]
  Frame Number: 104536
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
```

```
0000  60 63 4c 5f fd c4 cc b0  da 66 c1 a7 08 00 45 00   `cL_····  ·f····E·
0010  00 3c bf 5e 00 00 40 01  33 17 c0 a8 00 06 ac d9   ·<·^··@·  3·······
0020  1a c4 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ····MZ··  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn  opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg  hi
```

2. DNS: The Domain Network System (DNS) protocol helps Internet users and network devices discover websites using human-readable hostnames, instead of numeric IP addresses.

The process of DNS resolution involves converting a hostname (such as www.facebook.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (facebook.com) and the machine-friendly address necessary to locate the example.com webpage.

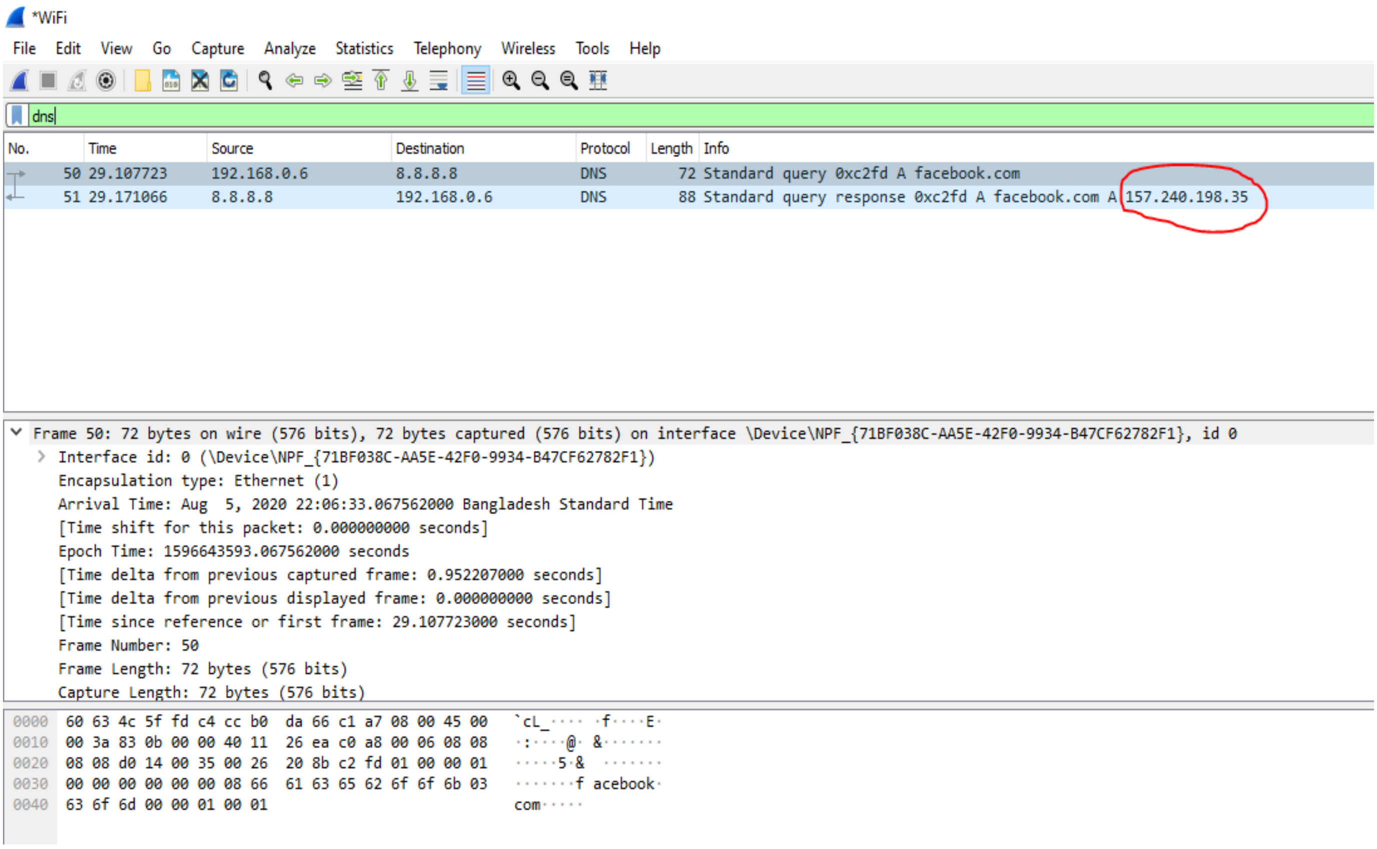


```
C:\Users\mnhru>ping facebook.com

Pinging facebook.com [157.240.198.35] with 32 bytes of data:
Reply from 157.240.198.35: bytes=32 time=48ms TTL=56
Reply from 157.240.198.35: bytes=32 time=46ms TTL=56
Reply from 157.240.198.35: bytes=32 time=45ms TTL=56
Reply from 157.240.198.35: bytes=32 time=45ms TTL=56

Ping statistics for 157.240.198.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 48ms, Average = 46ms

C:\Users\mnhru>
```



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

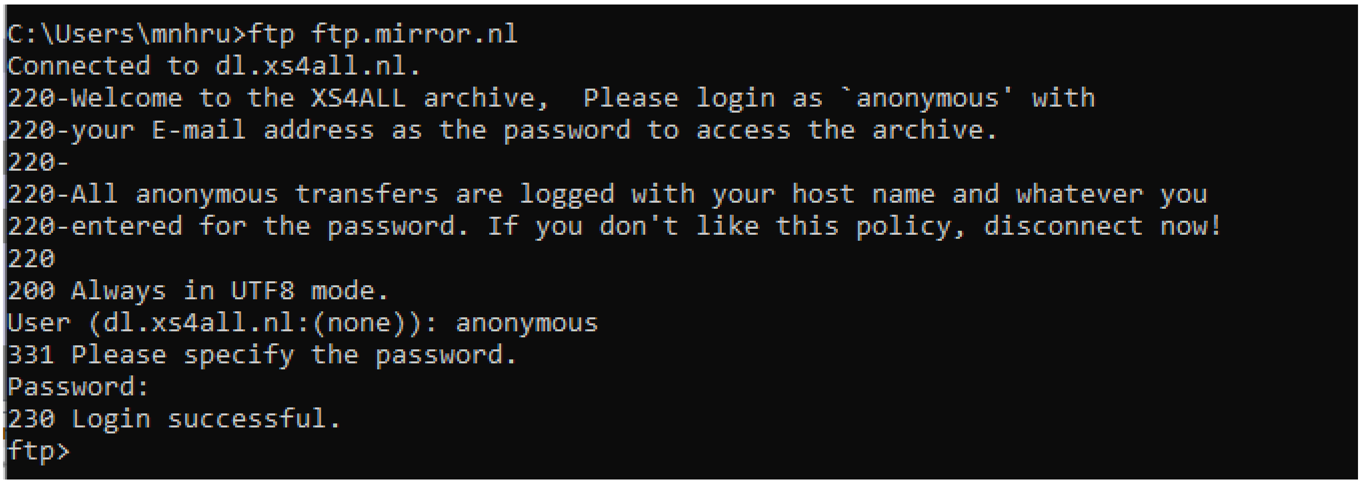
```
No.   Time        Source        Destination   Protocol  Length Info
   50 29.107723   192.168.0.6   8.8.8.8       DNS           72 Standard query 0xc2fd A facebook.com
   51 29.171066   8.8.8.8       192.168.0.6   DNS           88 Standard query response 0xc2fd A facebook.com A 157.240.198.35
```

```
Frame 50: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1}, id 0
  Interface id: 0 (\Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1})
  Encapsulation type: Ethernet (1)
  Arrival Time: Aug  5, 2020 22:06:33.067562000 Bangladesh Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1596643593.067562000 seconds
  [Time delta from previous captured frame: 0.952207000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 29.107723000 seconds]
  Frame Number: 50
  Frame Length: 72 bytes (576 bits)
  Capture Length: 72 bytes (576 bits)
```

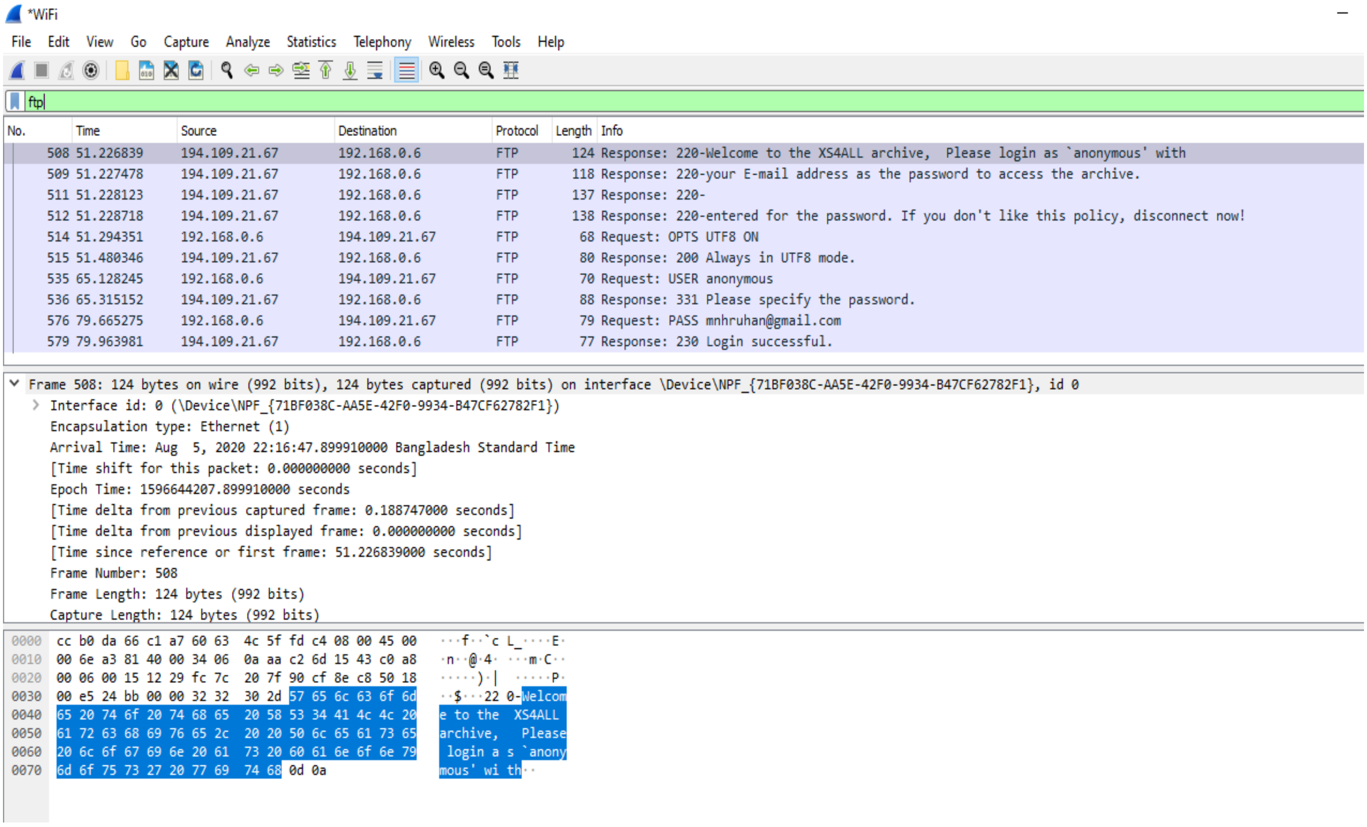
```
0000  60 63 4c 5f fd c4 cc b0  da 66 c1 a7 08 00 45 00   `cL_···· ·f····E·
0010  00 3a 83 0b 00 00 40 11  26 ea c0 a8 00 06 08 08   ·:····@· &·······
0020  08 08 d0 14 00 35 00 26  20 8b c2 fd 01 00 00 01   ·····5·&  ·······
0030  00 00 00 00 00 00 08 66  61 63 65 62 6f 6f 6b 03   ·······f acebook·
0040  63 6f 6d 00 00 01 00 01                            com·····
```

3. <u>FTP:</u> The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client-server model architecture using separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).



```
C:\Users\mnhru>ftp ftp.mirror.nl
Connected to dl.xs4all.nl.
220-Welcome to the XS4ALL archive,  Please login as `anonymous' with
220-your E-mail address as the password to access the archive.
220-
220-All anonymous transfers are logged with your host name and whatever you
220-entered for the password. If you don't like this policy, disconnect now!
220
200 Always in UTF8 mode.
User (dl.xs4all.nl:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp>
```


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Display filter: ftp

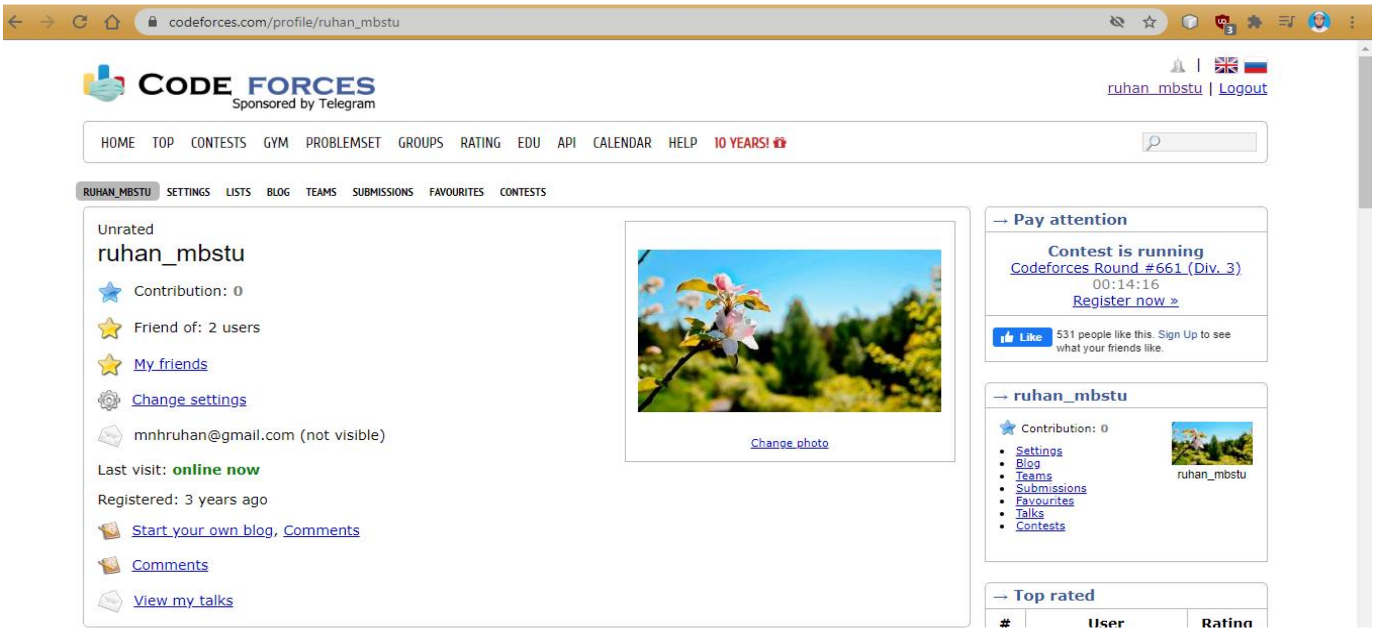
```
No.  Time        Source         Destination    Protocol Length Info
 508 51.226839   194.109.21.67  192.168.0.6    FTP      124 Response: 220-Welcome to the XS4ALL archive,  Please login as `anonymous' with
 509 51.227478   194.109.21.67  192.168.0.6    FTP      118 Response: 220-your E-mail address as the password to access the archive.
 511 51.228123   194.109.21.67  192.168.0.6    FTP      137 Response: 220-
 512 51.228718   194.109.21.67  192.168.0.6    FTP      138 Response: 220-entered for the password. If you don't like this policy, disconnect now!
 514 51.294351   192.168.0.6    194.109.21.67  FTP       68 Request: OPTS UTF8 ON
 515 51.480346   194.109.21.67  192.168.0.6    FTP       80 Response: 200 Always in UTF8 mode.
 535 65.128245   192.168.0.6    194.109.21.67  FTP       70 Request: USER anonymous
 536 65.315152   194.109.21.67  192.168.0.6    FTP       88 Response: 331 Please specify the password.
 576 79.665275   192.168.0.6    194.109.21.67  FTP       79 Request: PASS mnhruhan@gmail.com
 579 79.963981   194.109.21.67  192.168.0.6    FTP       77 Response: 230 Login successful.
```

```
v Frame 508: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1}, id 0
  > Interface id: 0 (\Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  5, 2020 22:16:47.899910000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1596644207.899910000 seconds
    [Time delta from previous captured frame: 0.188747000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 51.226839000 seconds]
    Frame Number: 508
    Frame Length: 124 bytes (992 bits)
    Capture Length: 124 bytes (992 bits)
```

```
0000  cc b0 da 66 c1 a7 60 63  4c 5f fd c4 08 00 45 00   ···f··`c L_····E·
0010  00 6e a3 81 40 00 34 06  0a aa c2 6d 15 43 c0 a8   ·n··@·4· ···m·C··
0020  00 06 00 15 12 29 fc 7c  20 7f 90 cf 8e c8 50 18   ·····)·|  ·····P·
0030  00 e5 24 bb 00 00 32 32  30 2d 57 65 6c 63 6f 6d   ··$···22 0-Welcom
0040  65 20 74 6f 20 74 68 65  20 58 53 34 41 4c 4c 20   e to the  XS4ALL 
0050  61 72 63 68 69 76 65 2c  20 20 50 6c 65 61 73 65   archive,   Please
0060  20 6c 6f 67 69 6e 20 61  73 20 60 61 6e 6f 6e 79    login a s `anony
0070  6d 6f 75 73 27 20 77 69  74 68 0d 0a               mous' wi th··
```

4. HTTP: HTTP is a client-server protocol: requests are sent by one entity, the user-agent (or a proxy on behalf of it). Most of the time the user-agent is a Web browser, but it can be anything, for example a robot that crawls the Web to populate and maintain a search engine index.

Each individual request is sent to a server, which handles it and provides an answer, called the response. Between the client and the server there are numerous entities, collectively called proxies, which perform different operations and act as gateways or caches.


codeforces.com/profile/ruhan_mbstu
CODE FORCES
Sponsored by Telegram
ruhan_mbstu | Logout
HOME TOP CONTESTS GYM PROBLEMSET GROUPS RATING EDU API CALENDAR HELP 10 YEARS!
RUHAN_MBSTU SETTINGS LISTS BLOG TEAMS SUBMISSIONS FAVOURITES CONTESTS

Unrated
ruhan_mbstu
Contribution: 0
Friend of: 2 users
My friends
Change settings
mnhruhan@gmail.com (not visible)
Last visit: online now
Registered: 3 years ago
Start your own blog, Comments
Comments
View my talks

Change photo

→ Pay attention
Contest is running
Codeforces Round #661 (Div. 3)
00:14:16
Register now »

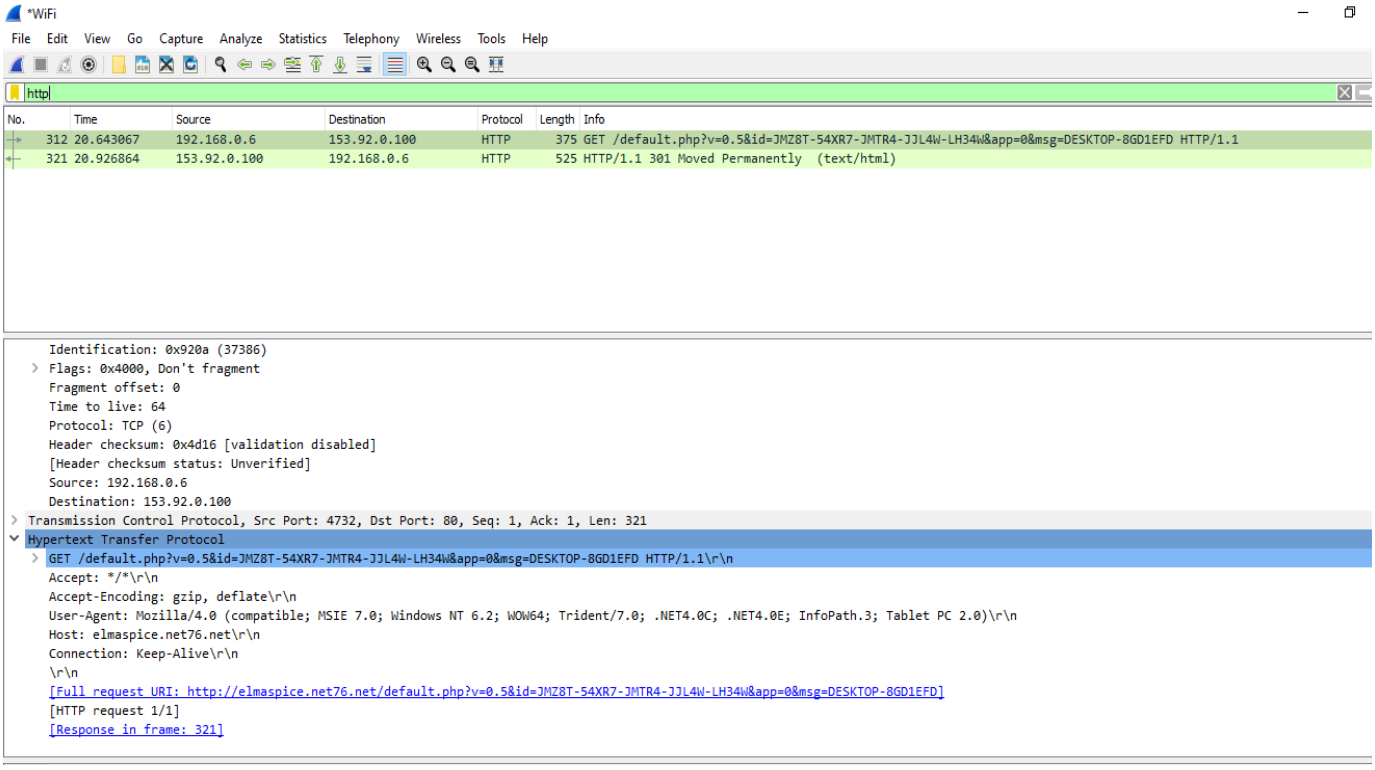
Like 531 people like this. Sign Up to see what your friends like.

→ ruhan_mbstu
Contribution: 0
- Settings
- Blog
- Teams
- Submissions
- Favourites
- Talks
- Contests

ruhan_mbstu

→ Top rated

#	User	Rating

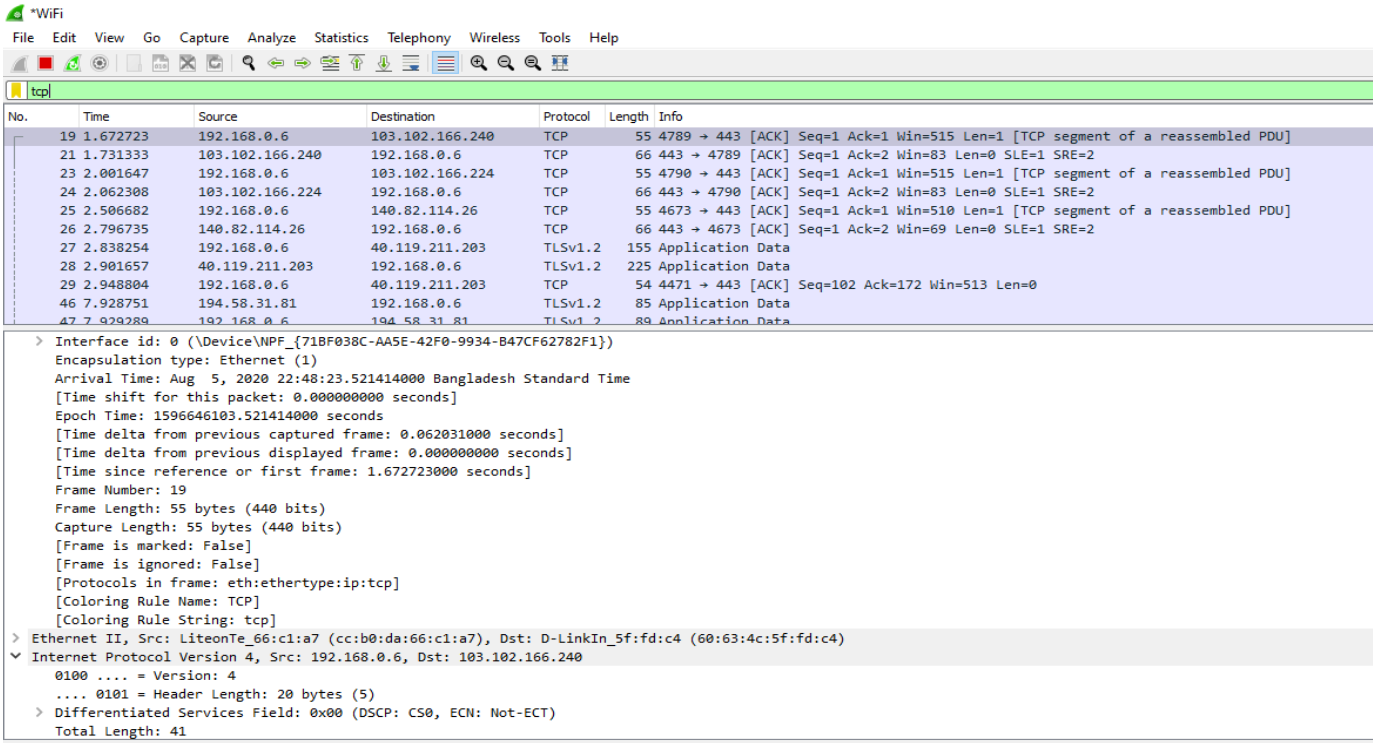

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.      Time       Source         Destination    Protocol  Length Info
   312 20.643067  192.168.0.6    153.92.0.100   HTTP       375 GET /default.php?v=0.5&id=JMZ8T-54XR7-JMTR4-JJL4W-LH34W&app=0&msg=DESKTOP-8GD1EFD HTTP/1.1
   321 20.926864  153.92.0.100   192.168.0.6    HTTP       525 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
    Identification: 0x920a (37386)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x4d16 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.6
    Destination: 153.92.0.100
> Transmission Control Protocol, Src Port: 4732, Dst Port: 80, Seq: 1, Ack: 1, Len: 321
v Hypertext Transfer Protocol
  > GET /default.php?v=0.5&id=JMZ8T-54XR7-JMTR4-JJL4W-LH34W&app=0&msg=DESKTOP-8GD1EFD HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; InfoPath.3; Tablet PC 2.0)\r\n
    Host: elmaspice.net76.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://elmaspice.net76.net/default.php?v=0.5&id=JMZ8T-54XR7-JMTR4-JJL4W-LH34W&app=0&msg=DESKTOP-8GD1EFD]
    [HTTP request 1/1]
    [Response in frame: 321]
```

5. <u>TCP:</u> The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

```
No.      Time       Source            Destination       Protocol  Length Info
     19 1.672723   192.168.0.6       103.102.166.240   TCP         55 4789 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
     21 1.731333   103.102.166.240   192.168.0.6       TCP         66 443 → 4789 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
     23 2.001647   192.168.0.6       103.102.166.224   TCP         55 4790 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
     24 2.062308   103.102.166.224   192.168.0.6       TCP         66 443 → 4790 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
     25 2.506682   192.168.0.6       140.82.114.26     TCP         55 4673 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
     26 2.796735   140.82.114.26     192.168.0.6       TCP         66 443 → 4673 [ACK] Seq=1 Ack=2 Win=69 Len=0 SLE=1 SRE=2
     27 2.838254   192.168.0.6       40.119.211.203    TLSv1.2    155 Application Data
     28 2.901657   40.119.211.203    192.168.0.6       TLSv1.2    225 Application Data
     29 2.948804   192.168.0.6       40.119.211.203    TCP         54 4471 → 443 [ACK] Seq=102 Ack=172 Win=513 Len=0
     46 7.928751   194.58.31.81      192.168.0.6       TLSv1.2     85 Application Data
     47 7.929289   192.168.0.6       194.58.31.81      TLSv1.2     89 Application Data
```

```
  > Interface id: 0 (\Device\NPF_{71BF038C-AA5E-42F0-9934-B47CF62782F1})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  5, 2020 22:48:23.521414000 Bangladesh Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1596646103.521414000 seconds
    [Time delta from previous captured frame: 0.062031000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.672723000 seconds]
    Frame Number: 19
    Frame Length: 55 bytes (440 bits)
    Capture Length: 55 bytes (440 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: LiteonTe_66:c1:a7 (cc:b0:da:66:c1:a7), Dst: D-LinkIn_5f:fd:c4 (60:63:4c:5f:fd:c4)
v Internet Protocol Version 4, Src: 192.168.0.6, Dst: 103.102.166.240
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 41
```

Conclusion: From this experiment we come to learn that protocol analysis with Wireshark using example. Protocol analysis is used to learn about the functionality of source and destination.