MAWLANA BHASHANI SCIENCE AND TECHNOLOGY UNIVERSITY

LAB-REPORT

Report no : 07

Report Name: Protocol analysis with Wireshark

Course code : ICT-3208

Course title : Network Planning and Designing Lab

Date of Submission : 05-August-2020

Submitted By

Name: Md. Nayan Ali
ID: IT-16062
3rd year 2nd semester
Session: 2015-2016
Dept. of ICT
MBSTU.

Submitted To

Mr. Nazrul Islam
Assistant Professor,
Dept. of ICT, MBSTU.

Objectives:

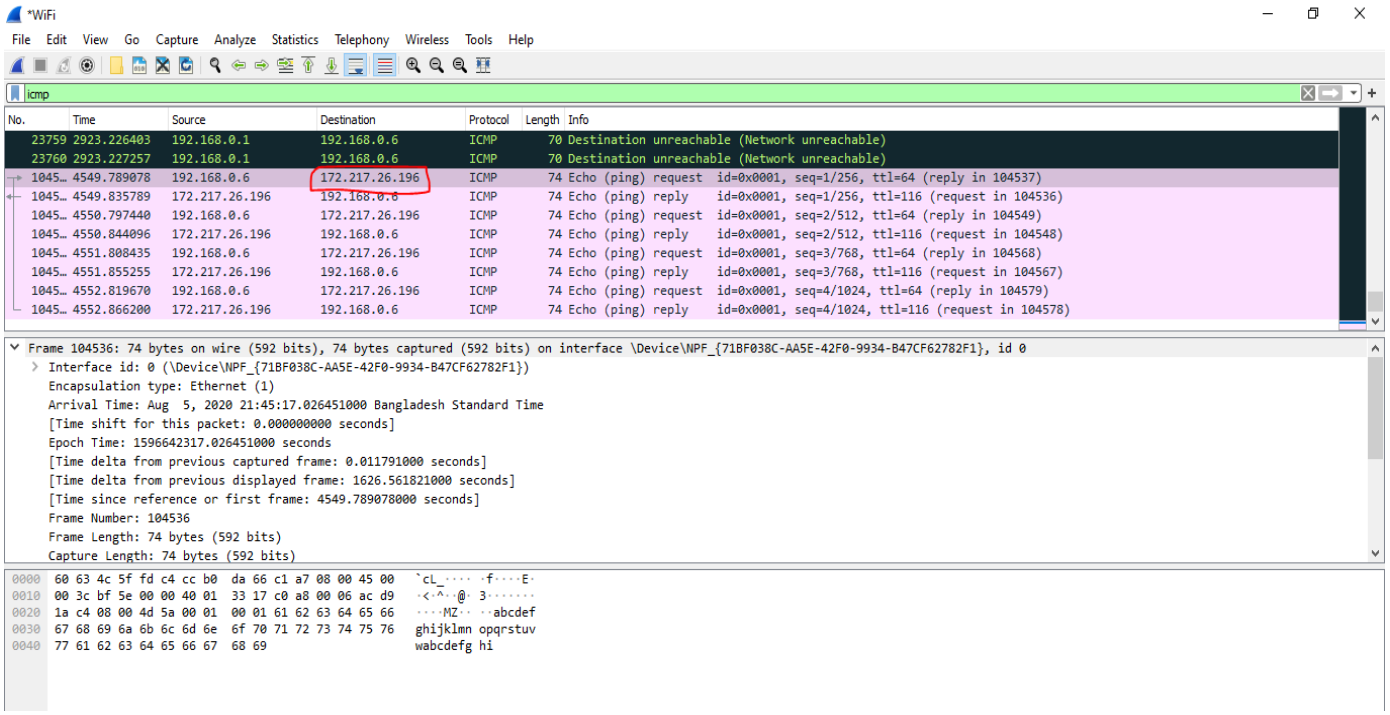
i) Packets and Protocols can be analyzed after capture.
ii) Individual fields and protocols can be easily seen.
iii) Graph and flow diagram can be helpful in analysis.

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.

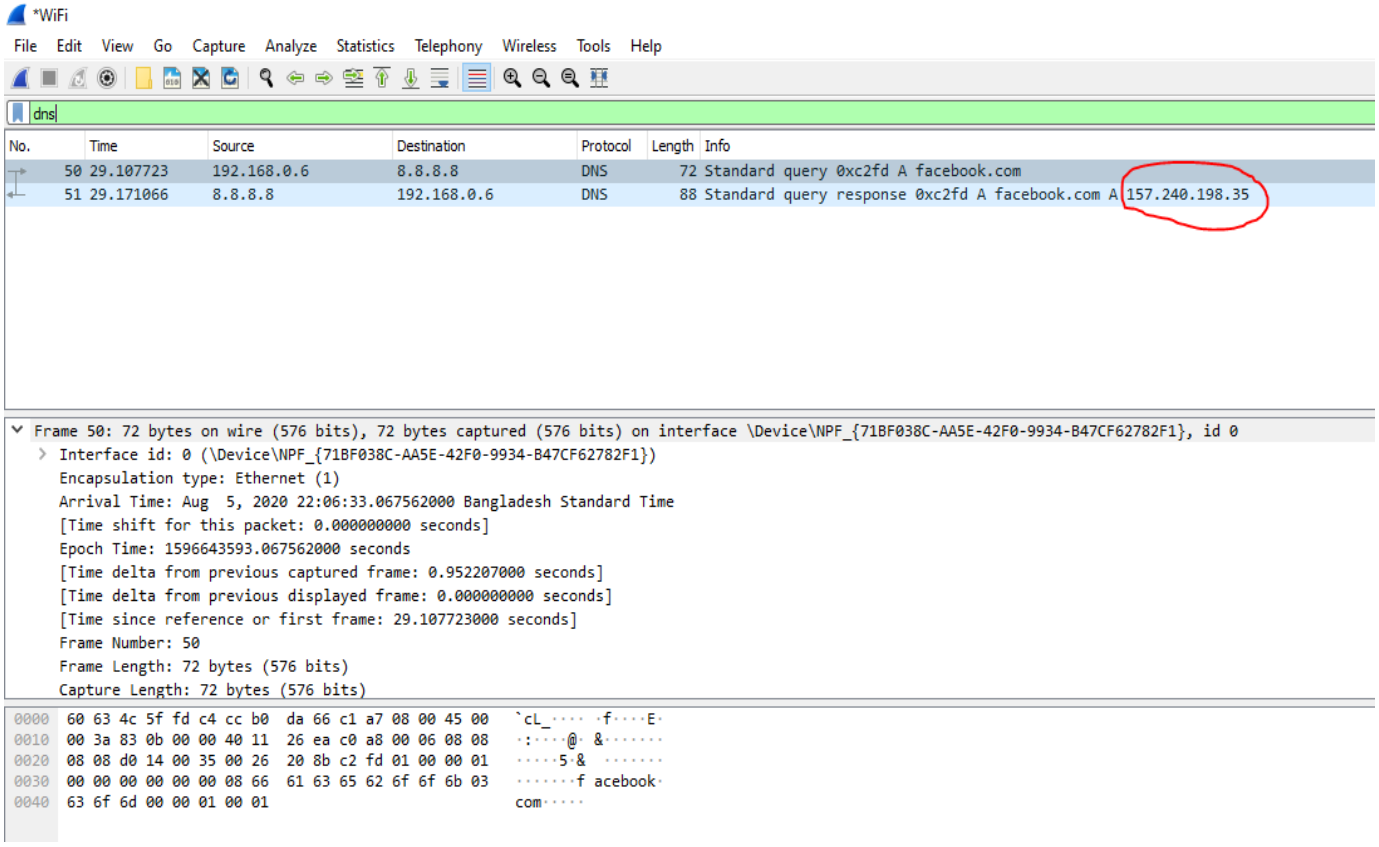
```
C:\Users\mnhru>ping www.google.com
Ping request could not find host www.google.com. Please check the name and try again.

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>
```



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.

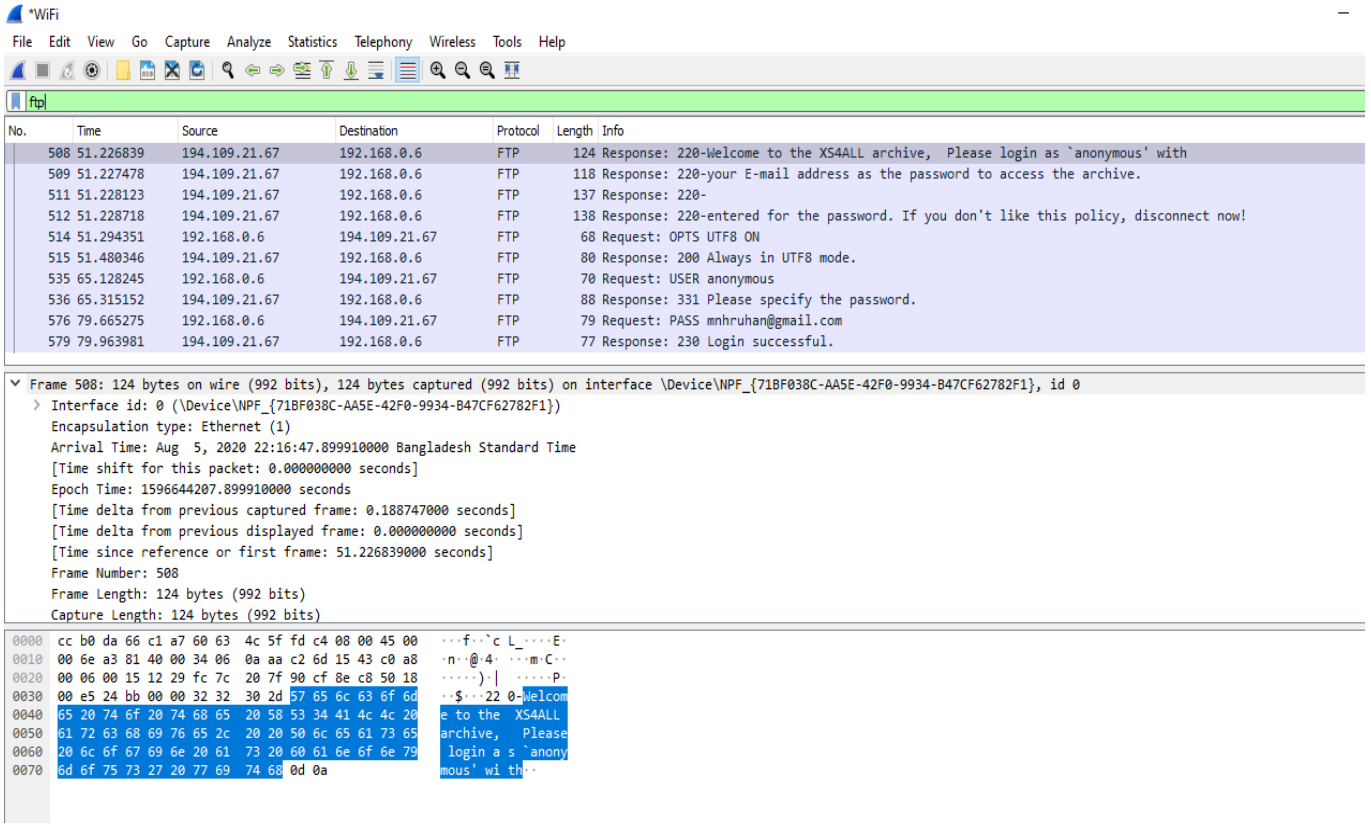
```
C:\Users\mnhru>ping facebook.com

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>
```



3. FTP: 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.

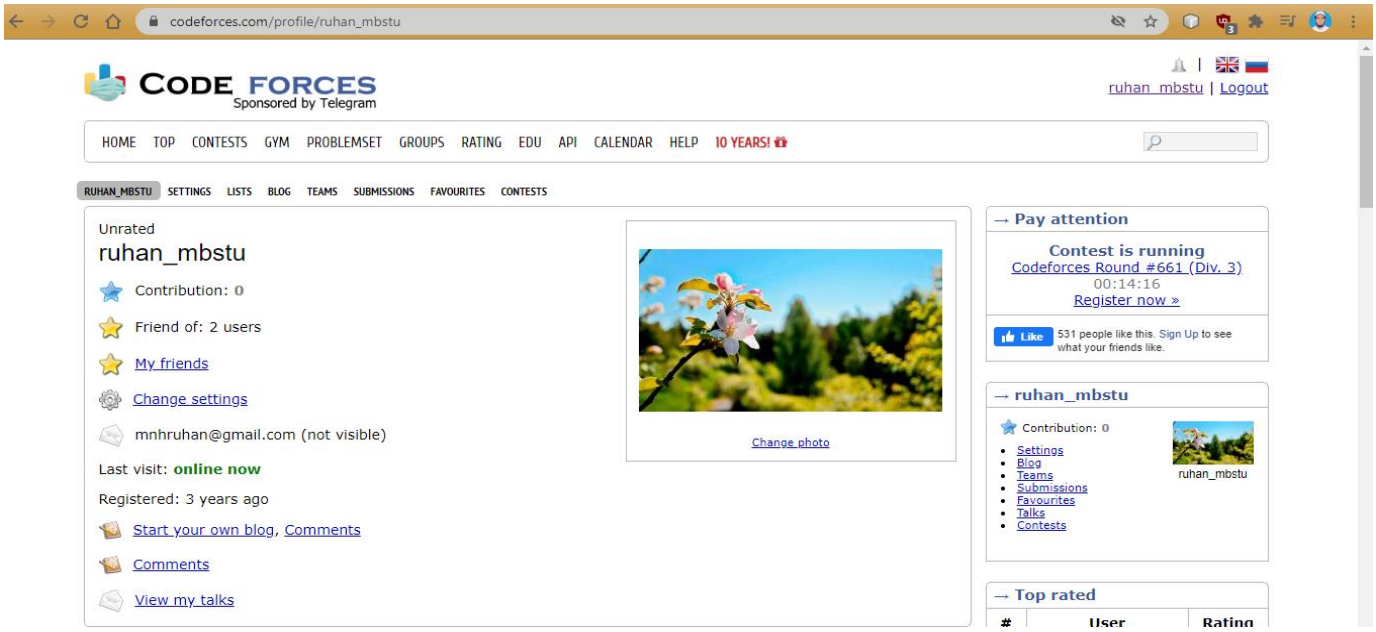
FTP is built on a client-server model architecture using separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is 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).

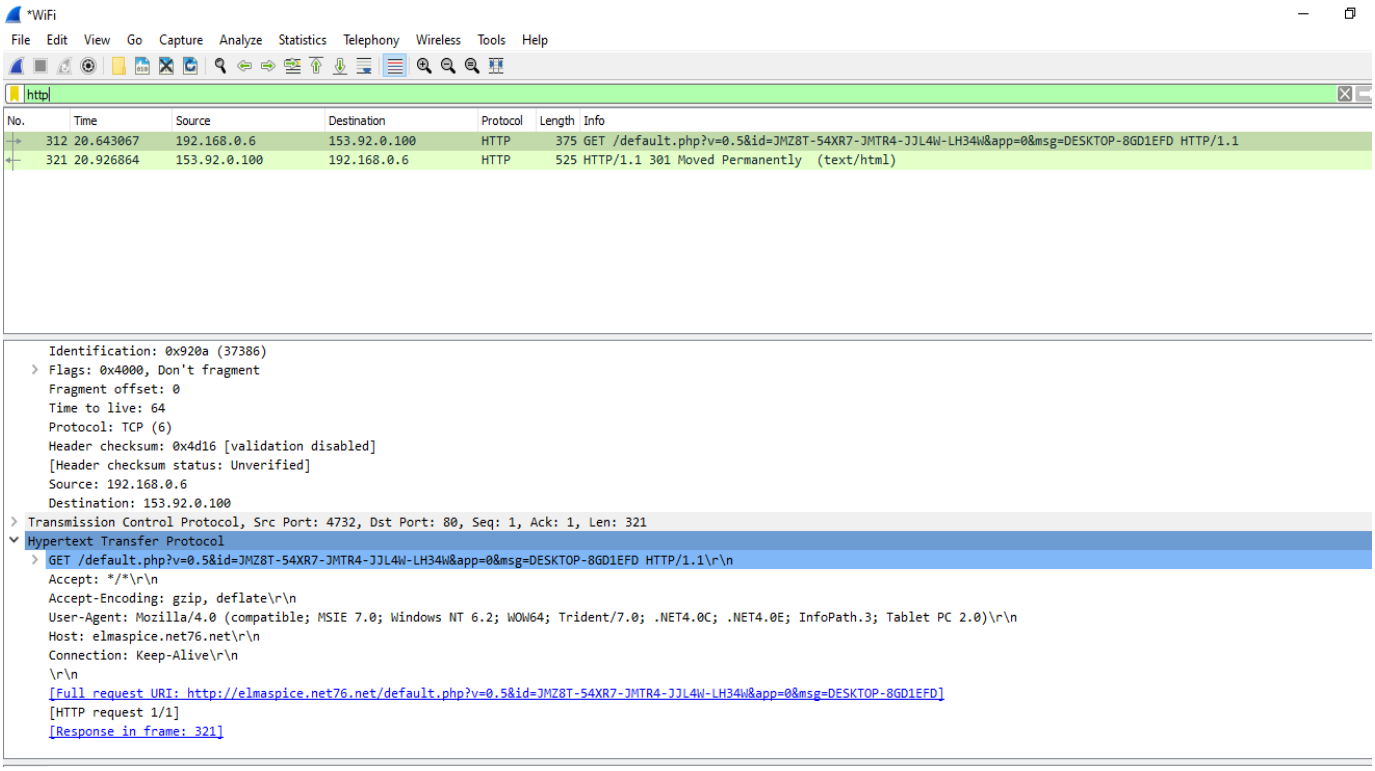
```
C:\Users\mnhru>ftp ftp.mirror.nl
Connected to dl.xs4all.nl.
220-Welcome to the XS4ALL archive,  Please login as `anonymous' with
220-your E-mail address as the password to access the archive.
220-
220-All anonymous transfers are logged with your host name and whatever you
220-entered for the password. 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>
```



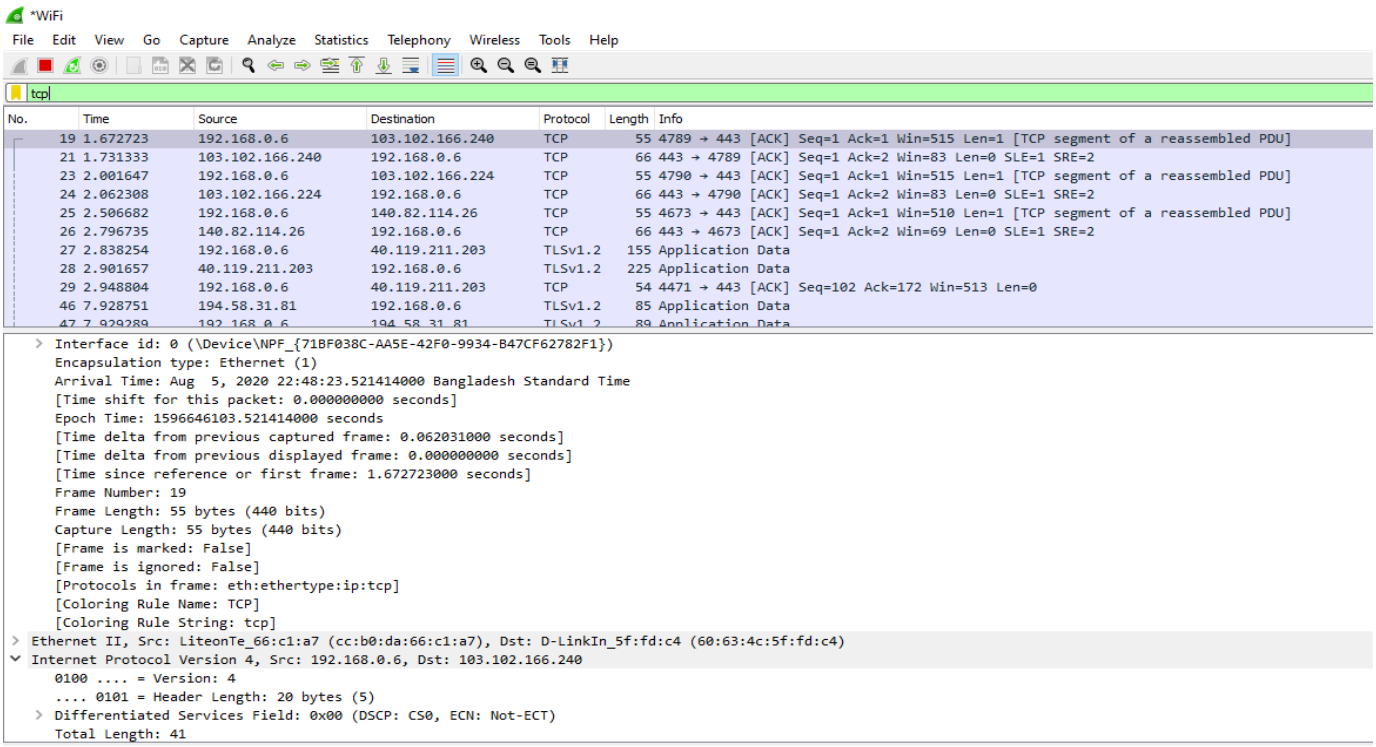
4. HTTP: HTTP is a client-server protocol: requests are sent by one entity, the user-agent (or a proxy on behalf of it). Most of the time the user-agent is a Web browser, but it can be anything, for example a robot that crawls the Web to populate and maintain a search engine index.

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.





5. TCP: 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.



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.