Government Engineering College, Thrissur

CS334 – Network Programming Lab

Documentation -

Exp 11 –

Wireshark to Observer TCP Packets

Date of Submission

3 July 2021

Submitted By

Kowsik Nandagopan D

Roll No 31

TCR18CS031

GECT CSE S6

Experiment 11

Using Wireshark observe Three Way Handshaking Connection Establishment, Data Transfer and Three Way Handshaking Connection Termination in client server communication using TCP.

Executing program

- Code is provided in the **Server.java** and **Client.java** (Tested and verified on Ubuntu 20.04)

```
javac Server.java
java Server
```

```
javac Client.java
java Client
```

- **Client - Server program is not mandatory. We can observer the TCP packets from internet to browser using wireshark. But here for the testing and for sake of simplicity we generate using the java program**
- Server.java program sends a message “ABCDE” to client every two seconds. To stop transmission use CTRL + C

PROCEDURE

- Open wireshark in super user mode using the command

```
sudo wireshark
```

- Open the Loopback mode. Since the transmission is between two processes in the same system between two ports.

P. T, O

Output / Screenshots

Running server and client

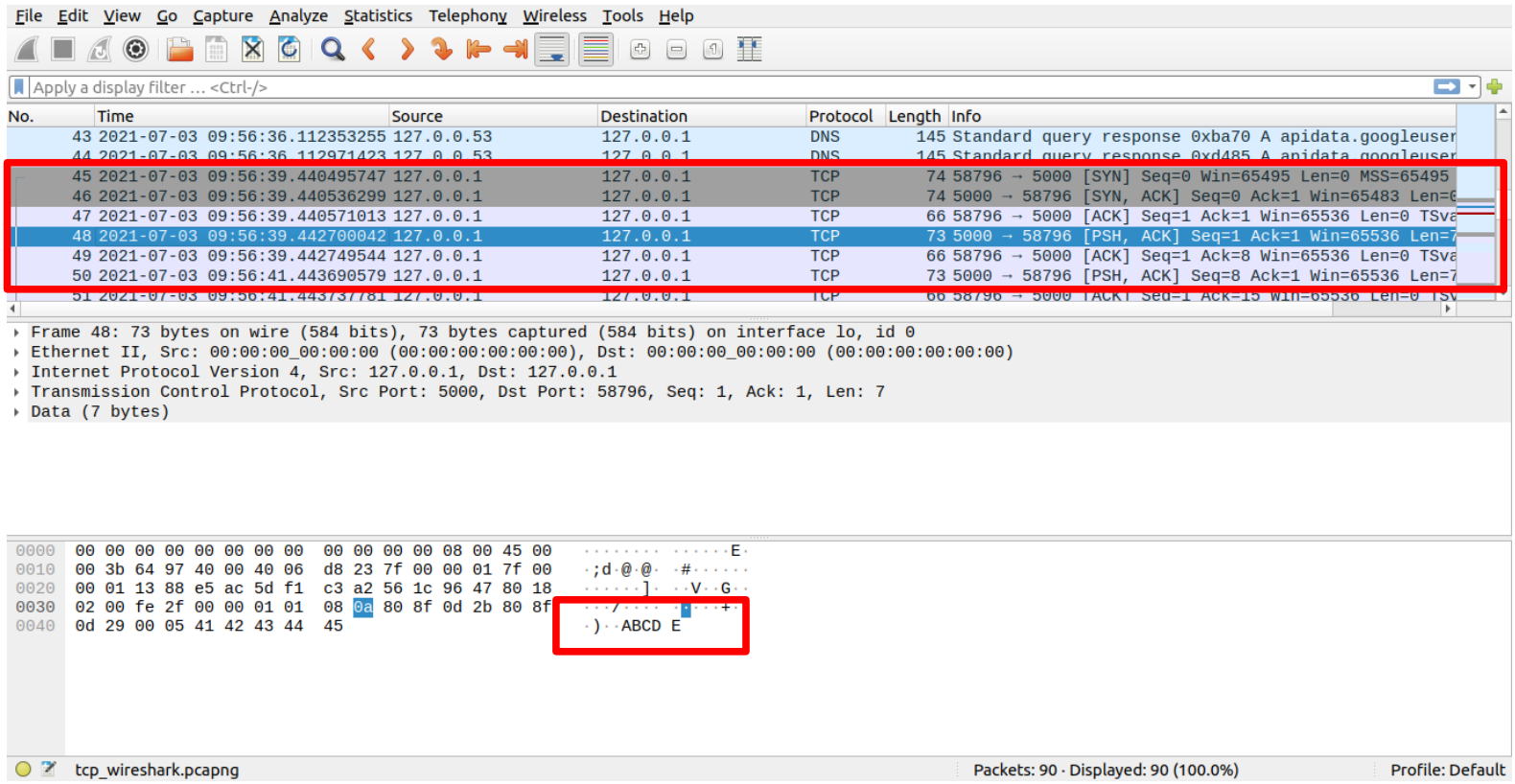
Server

```
hp@hp ~/Documents/S6/Network Lab/Exp11 ‹master*›
$ javac Server.java && java Server                                    130
Server socket created.
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
```

Client

```
hp@hp ~/Documents/S6/Network Lab/Exp11 ‹master*›
$ javac Client.java && java Client
Client socket created.
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
ABCDE
```

Wireshark



We can see TCP handshake in above image (highlighted in red) 45-47 serial number denotes Syn-Syn/Ack-Ack 49 -50 data transfer. For each message sent there will be an acknowledgment. Data inside each packet can be seen at the bottom of the application.