HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

*****

BÀI THỰC HÀNH CHƯƠNG 3

HỌC PHẦN:
MẠNG MÁY TÍNH

Hà Nội - 2017

MỤC LỤC

BÀI THỰC HÀNH CHƯƠNG 2

1. Bài thực hành số 1

Tên bài: Sử dụng Wireshark bắt các gói tin TCP và phân tích.

❖ Chuẩn bị:

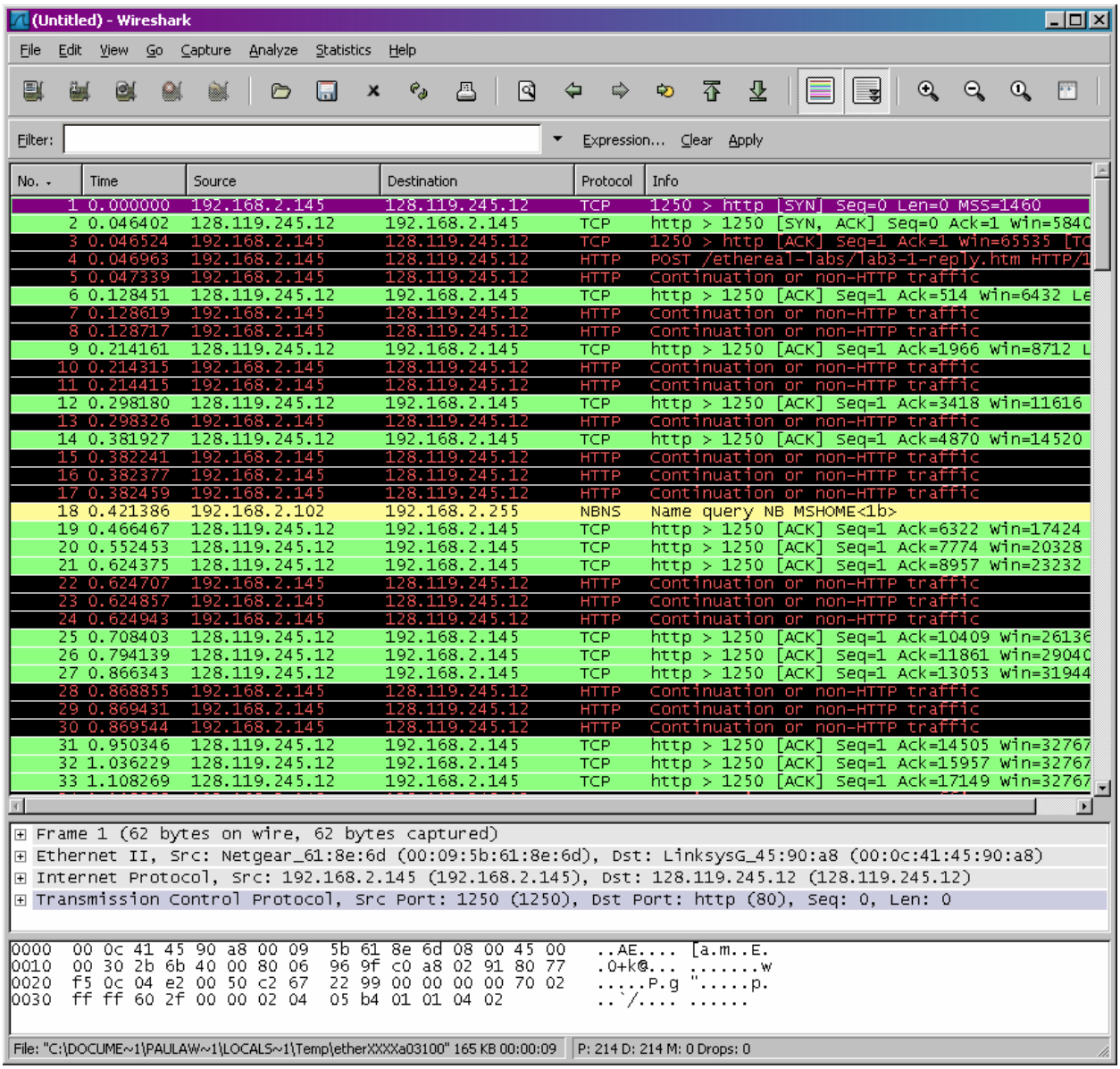
Sử dụng một máy tính chạy hệ điều hành Windows có kết nối mạng internet hoặc LAN làm môi trường thực hành. Cài đặt Wireshark.

❖ Các bước thực hiện:

a) Bắt lưu lượng TCP

Bước 1: Chạy trình duyệt và download file http://gaia.cs.umass.edu/wiresharklabs/ alice.txt
Bước 2: Vào trang web http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
Bước 3: Nhấn nút "Browse" và chọn file vừa download, chưa bấm nút "Upload alice txt file "
Bước 4: Chạy Wireshark để bắt đầu bắt gói tin
Bước 5: Vào trình duyệt bấm nút "Upload alice txt file "
Bước 6: Dừng bắt gói tin trong Wireshark

Ta được kết quả như sau:



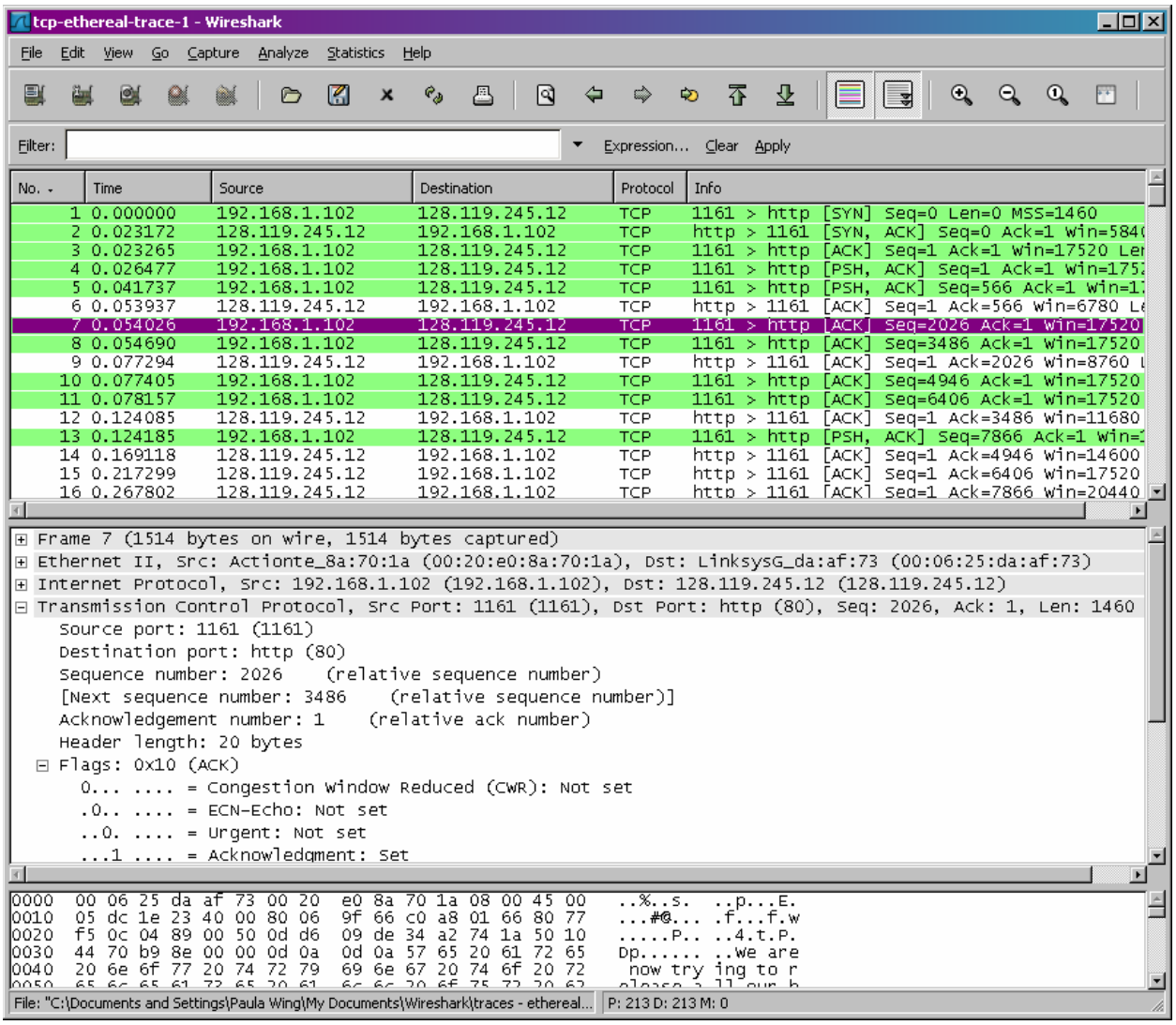
b) Sơ bộ về các gói tin đã bắt được

Trước tiên, gõ "tcp" trong thanh "Filter" ở Wireshark để xem các bản tin TCP và HTTP. Ta có thể thấy gói tin SYN trong giai đoạn bắt tay ba bước của TCP.

Trả lời câu hỏi sau:

1. Địa chỉ IP của client và server, và port tương ứng

Do ta chỉ phân tích TCP chứ không phân tích HTTP nên cần lọc TCP riêng bằng cách chọn: *Analyze -> Enabled Protocols* . Sau đó bỏ đánh dấu ô HTTP, nhấn OK. Khi đó màn hình sẽ thành:



3) Cơ bản về TCP

Trả lời các câu hỏi sau về TCP segment:

2. “sequence number” của gói TCP SYN bắt đầu kết nối TCP giữa client và server là gì?

3. “sequence number” của gói SYN ACK gửi từ server về client, trả lời cho SYN?

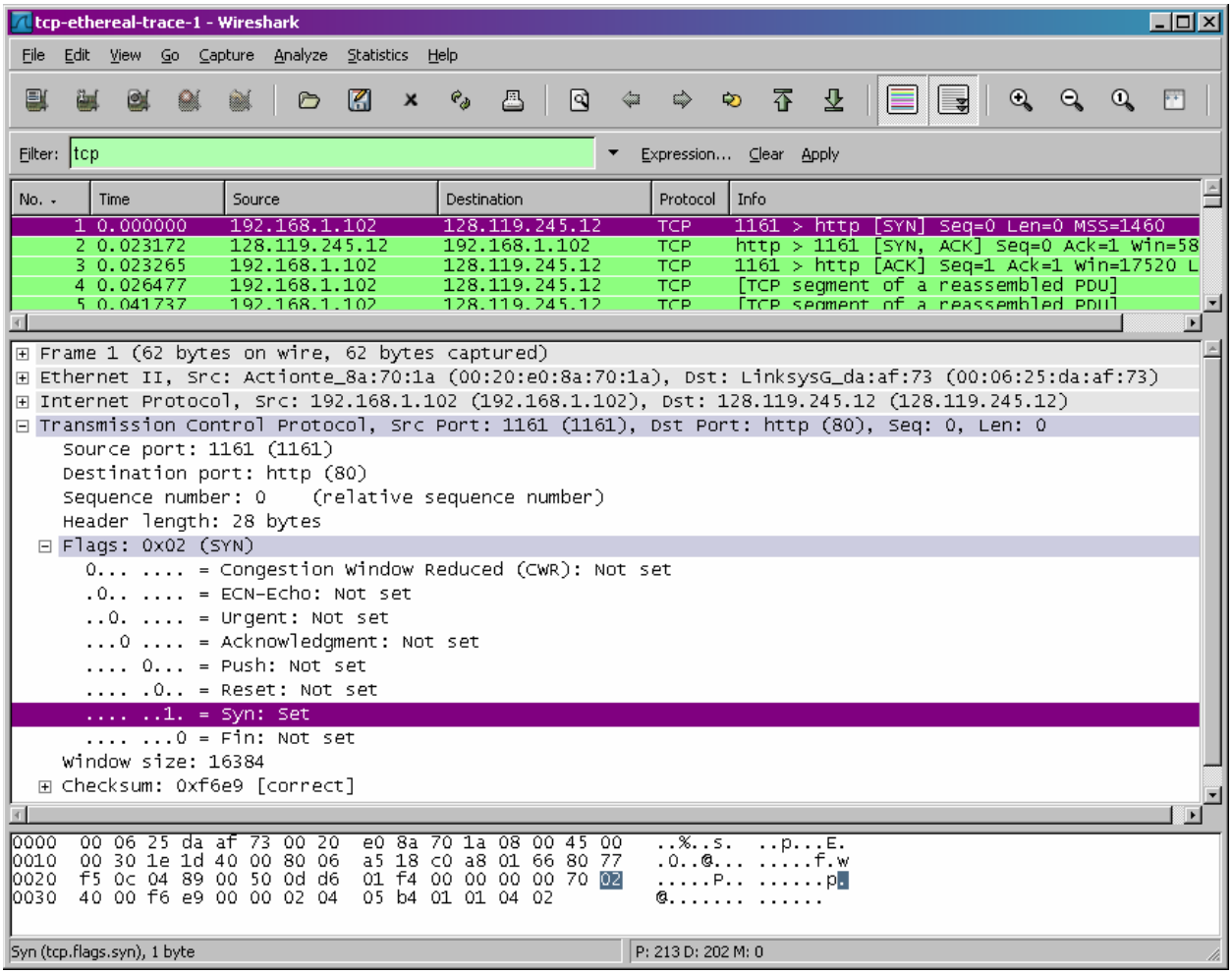
4. Round Trip Time của các gói TCP đã gửi? Có thể xem bằng "*Statistics -> TCP Stream Graph -> Round Trip Time Graph*"

5. Độ dài của mỗi gói TCP đầu tiên?

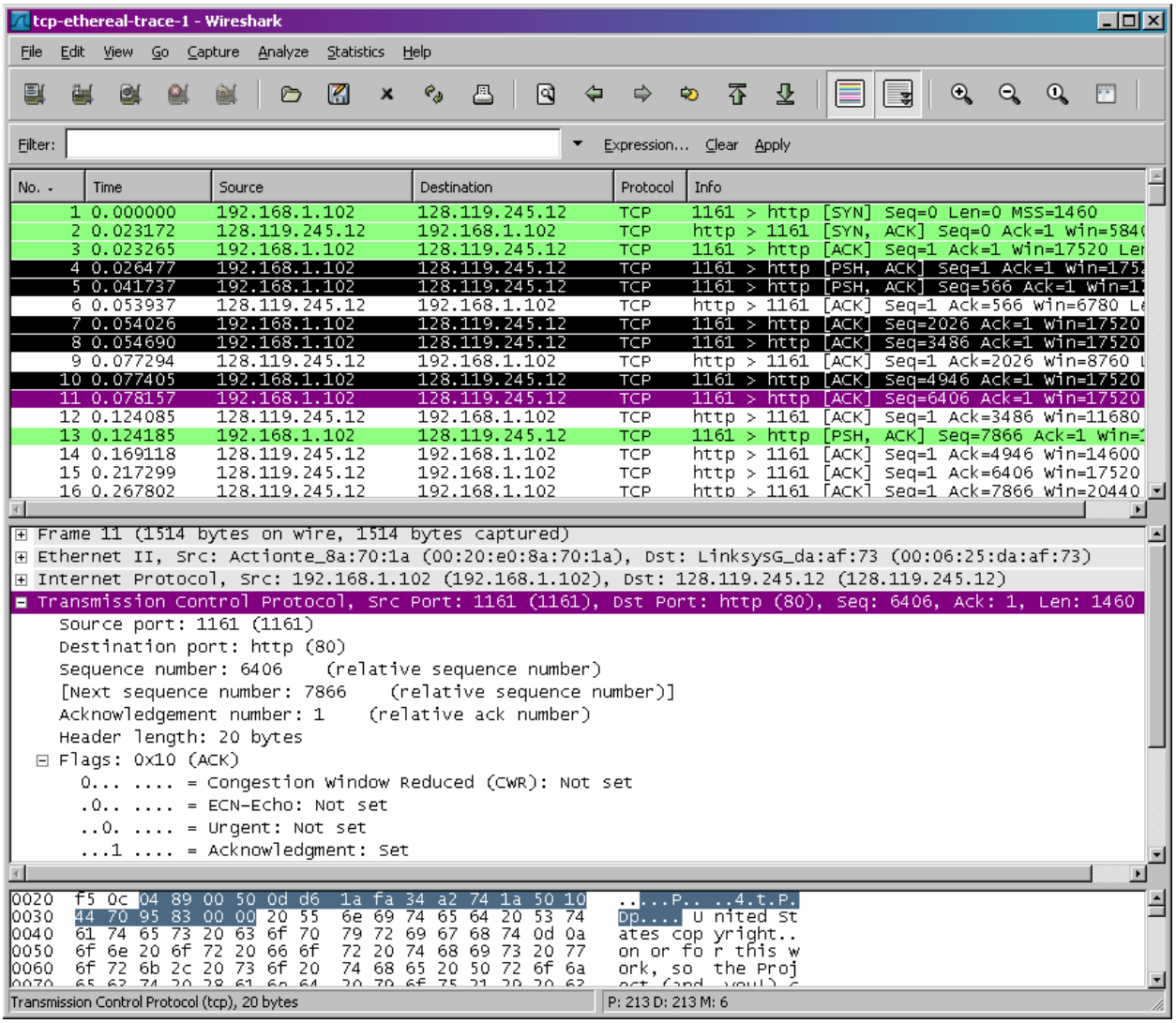
6. Có gói tin nào cần truyền lại không? (retransmitted)

Gợi ý:

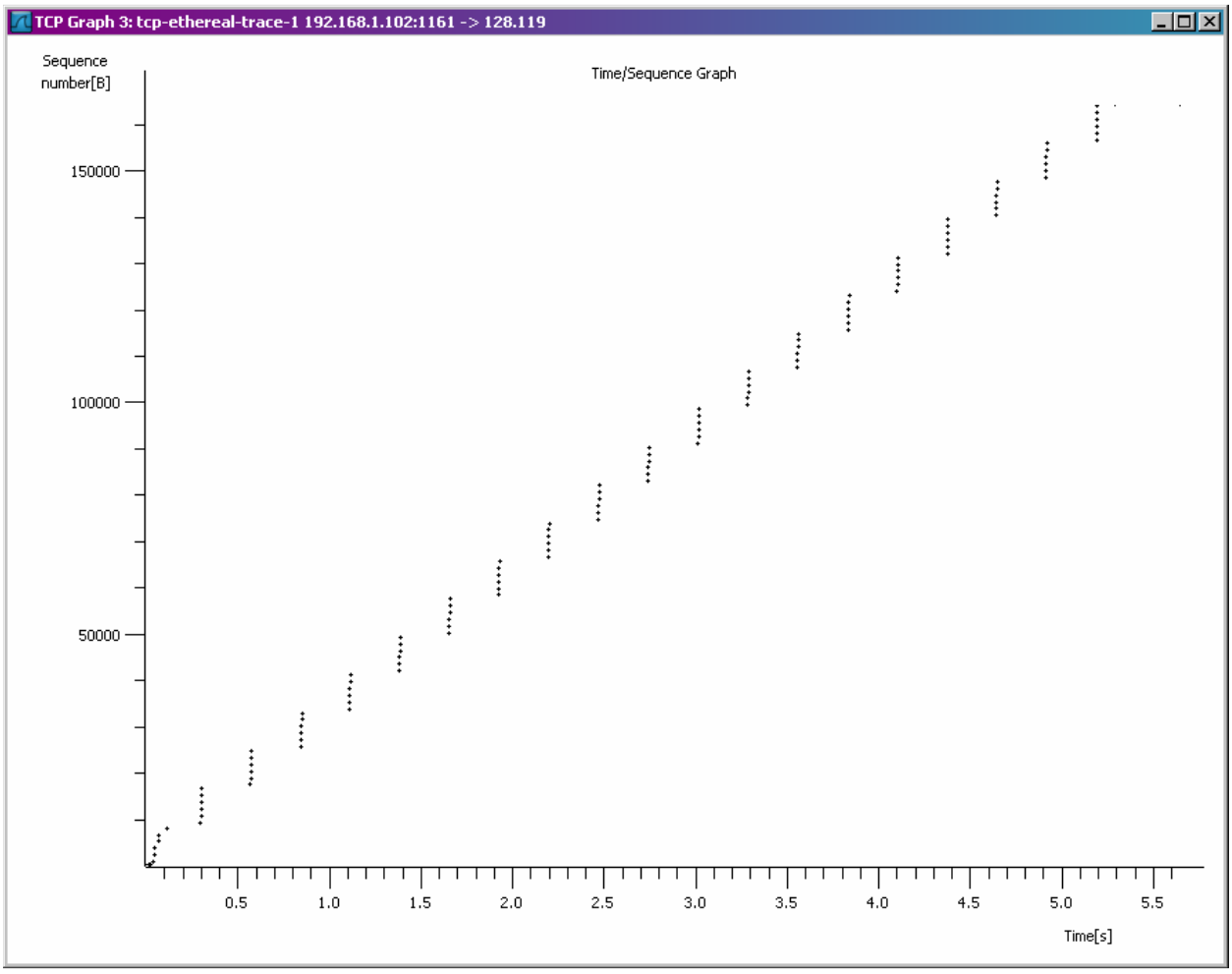
- Xem cờ SYN:



- Độ dài của các gói tin từ 1-6:



- Kiểm tra xem có retransmit không bằng cách xem sequence numbers của các gói TCP bằng cách vào *Time-Sequence-Graph.* Nếu tăng liên tục không giảm thì không bị truyền lại.



2. Bài thực hành số 2

Tên bài: Lập trình TCP socket với java và bắt phân tích với Wireshark

❖ Chuẩn bị:

Sử dụng một máy tính có kết nối mạng internet hoặc LAN để tiến hành bắt gói tin trên máy tính cài đặt hệ điều hành Windows. Cài đặt Netbeans để lập trình java socket. Sau đó cài đặt client và server ở 2 máy riêng biệt để dùng Wireshark bắt, phân tích. Sinh viên tùy chọn chạy client hoặc server, 2 người 1 nhóm.

❖ Các bước thực hiện:

Vào trang web https://www.javatpoint.com/socket-programming để xem giới thiệu sơ bộ về đối tượng socket trong Java.

Trong Netbeans, lập trình một trong 2 chương trình client/server dưới đây:

TCPServer.java

```
import java.io.*;
import java.net.*;

class TCPServer {
 public static void main(String argv[]) throws Exception {
  String clientSentence;
  String capitalizedSentence;
  ServerSocket welcomeSocket = new ServerSocket(6789);

  while (true) {
            Socket connectionSocket = welcomeSocket.accept();
            BufferedReader inFromClient =
            new BufferedReader(new InputStreamReader(connectionSocket.getInputStream()));
            DataOutputStream outToClient = new DataOutputStream(connectionSocket.getOutputStream());
            clientSentence = inFromClient.readLine();
            System.out.println("Received: " + clientSentence);
            capitalizedSentence = clientSentence.toUpperCase() + '\n';
            outToClient.writeBytes(capitalizedSentence);
  }
 }
}
```

Và TCPClient.java

```
import java.io.*;
import java.net.*;

class TCPClient {
 public static void main(String argv[]) throws Exception {
  String sentence;
  String modifiedSentence;
  BufferedReader inFromUser = new BufferedReader(new InputStreamReader(System.in));
  Socket clientSocket = new Socket("127.0.0.1", 6789);
  DataOutputStream outToServer = new DataOutputStream(clientSocket.getOutputStream());
  BufferedReader inFromServer = new BufferedReader(new InputStreamReader(clientSocket.getInputStream()));
  sentence = inFromUser.readLine();
  outToServer.writeBytes(sentence + '\n');
  modifiedSentence = inFromServer.readLine();
  System.out.println("FROM SERVER: " + modifiedSentence);
  clientSocket.close();
```

Chú ý: địa chỉ ip và port trong chương trình client phải thay bằng địa chỉ ip và port của máy tính server đang chạy. Nếu muốn chạy cả 2 chương trình trên cùng máy tính thì thay địa chỉ IP thành *127.0.0.1* hoặc *localhost* .

Thực hiện các bước sau:

- Một sinh viên chạy client, một sinh viên chạy server và thử nghiệm, sau đó đổi lại.

Nếu không có Netbeans thì chạy chương trình bằng 1 trong 2 câu lệnh (tùy theo chương trình client hay server):

javac TCPServer.java

javac TCPClient.java

- Tại client, nhập chuỗi bất kỳ, server sẽ đổi thành chuỗi viết hoa và trả lại client. Quan sát các kết quả có đúng không?

- Tại máy tính chạy server và client, chạy Wireshark để bắt gói tin TCP như bài 1 trên, tìm gói tin chứa nội dung của chuỗi đã nhập và chuỗi viết hoa đã chuyển đổi.

- Chỉ ra gói tin SYN trong giai đoạn bắt tay 3 bước.

- Có bao nhiêu gói TCP được truyền?