

**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

1.	Bài thực hành số 1 .....	3
	Tên bài: Sử dụng Wireshark bắt các gói tin TCP và phân tích. ....	3
	a) Bắt lưu lượng TCP .....	3
	b) Sơ bộ về các gói tin đã bắt được .....	4
	3) Cơ bản về TCP .....	5
2.	Bài thực hành số 2 .....	8
	Tên bài: Lập trình TCP socket với java và bắt phân tích với Wireshark .....	8



## 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 <a href="http://gaia.cs.umass.edu/wiresharklabs/alice.txt">http://gaia.cs.umass.edu/wiresharklabs/alice.txt</a>
Bước 2: Vào trang web <a href="http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html">http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html</a>
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:



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.145	128.119.245.12	TCP	1250 > http [SYN] Seq=0 Len=0 MSS=1460
2	0.046402	128.119.245.12	192.168.2.145	TCP	http > 1250 [SYN, ACK] Seq=0 Ack=1 win=5840
3	0.046524	192.168.2.145	128.119.245.12	TCP	1250 > http [ACK] Seq=1 Ack=1 win=65535 [TS
4	0.046963	192.168.2.145	128.119.245.12	HTTP	POST /ethereal-labs/lab3-1-reply.htm HTTP/1
5	0.047339	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
6	0.128451	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=514 win=6432 Le
7	0.128619	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
8	0.128717	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
9	0.214161	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=1966 win=8712 L
10	0.214315	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
11	0.214415	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
12	0.298180	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=3418 win=11616
13	0.298326	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
14	0.381927	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=4870 win=14520
15	0.382241	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
16	0.382377	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
17	0.382459	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
18	0.421386	192.168.2.102	192.168.2.255	NBNS	Name query NB MSHOME<1b>
19	0.466467	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=6322 win=17424
20	0.552453	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=7774 win=20328
21	0.624375	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=8957 win=23232
22	0.624707	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
23	0.624857	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
24	0.624943	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
25	0.708403	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=10409 win=26136
26	0.794139	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=11861 win=29040
27	0.866343	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=13053 win=31944
28	0.868855	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
29	0.869431	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
30	0.869544	192.168.2.145	128.119.245.12	HTTP	Continuation or non-HTTP traffic
31	0.950346	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=14505 win=32767
32	1.036229	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=15957 win=32767
33	1.108269	128.119.245.12	192.168.2.145	TCP	http > 1250 [ACK] Seq=1 Ack=17149 win=32767

Frame 1 (62 bytes on wire, 62 bytes captured)

Ethernet II, Src: Netgear\_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG\_45:90:a8 (00:0c:41:45:90:a8)

Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 1250 (1250), Dst Port: http (80), Seq: 0, Len: 0

0000 00 0c 41 45 90 a8 00 09 5b 61 8e 6d 08 00 45 00 ..AE.... [a.m..E.  
0010 00 30 2b 6b 40 00 80 06 96 9f c0 a8 02 91 80 77 .0+k@... ..w  
0020 f5 0c 04 e2 00 50 c2 67 22 99 00 00 00 70 02 ....P.g ".....p.  
0030 ff ff 60 2f 00 00 02 04 05 b4 01 01 04 02 .../.....

File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXa03100" 165 KB 00:00:09 P: 214 D: 214 M: 0 Drops: 0

## b) Sơ bộ về các gói tin đã bắt được

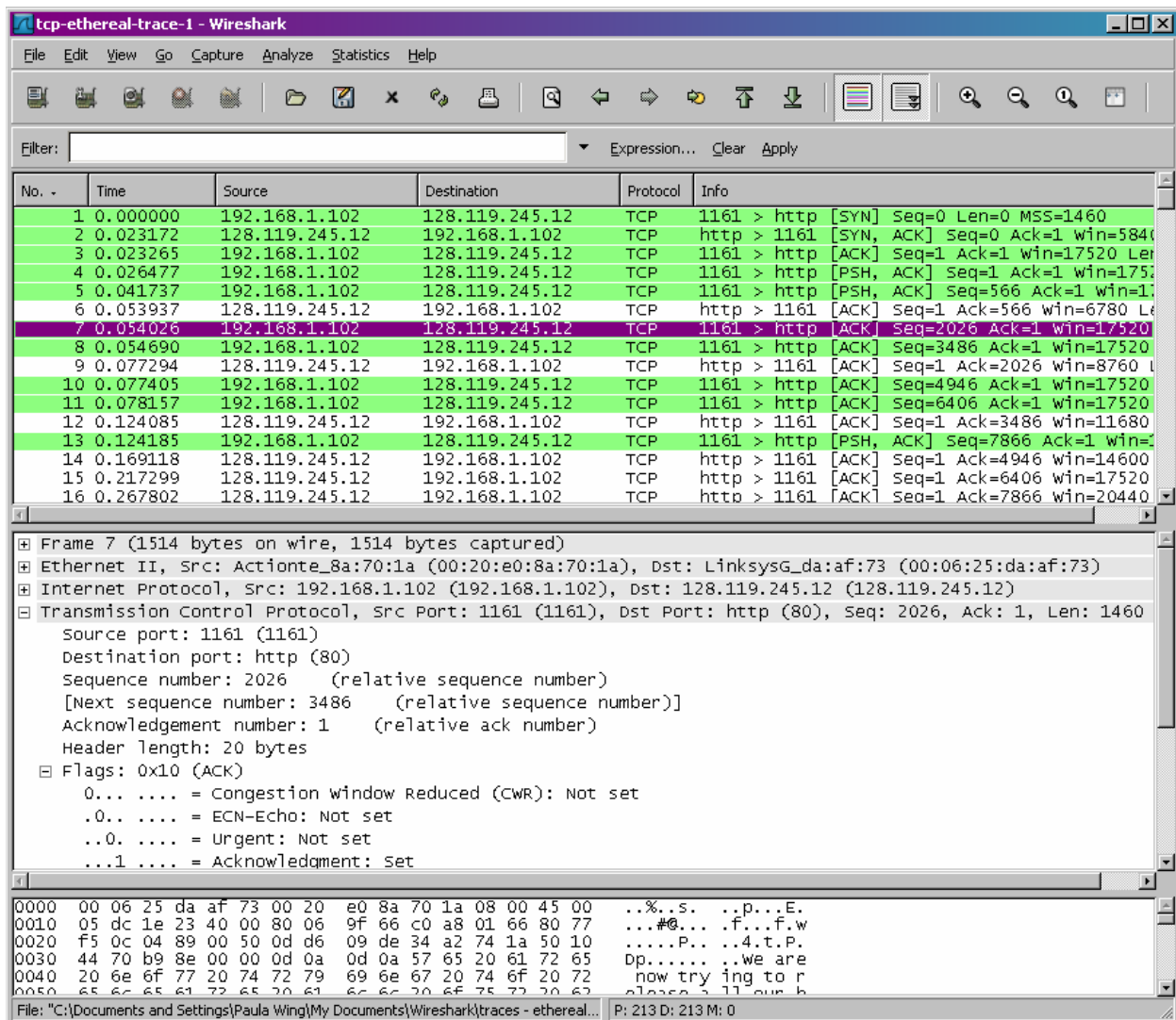
Trước tiên, gõ “tcp” trong thanh “Filter” ở Wireshark để xem các bản tin TCP và HTTP. Ta có thể thấy gói tin SYN trong giai đoạn bắt tay ba bước của TCP.

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:

The image shows a Wireshark packet capture window titled "tcp-ethereal-trace-1 - Wireshark". The filter is set to "tcp". The packet list shows five packets. The first packet is a SYN packet from 192.168.1.102 to 128.119.245.12 on port 80. The packet details pane shows the following information:

- Frame 1 (62 bytes on wire, 62 bytes captured)
- Ethernet II, Src: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG\_da:af:73 (00:06:25:da:af:73)
- Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: http (80), Seq: 0, Len: 0
  - Source port: 1161 (1161)
  - Destination port: http (80)
  - Sequence number: 0 (relative sequence number)
  - Header length: 28 bytes
  - Flags: 0x02 (SYN)
    - 0... .. = Congestion window Reduced (CWR): Not set
    - .0.. .. = ECN-Echo: Not set
    - ..0. .... = Urgent: Not set
    - ...0 .... = Acknowledgment: Not set
    - .... 0... = Push: Not set
    - .... .0.. = Reset: Not set
    - .... ..1. = Syn: Set
    - .... ...0 = Fin: Not set
  - Window size: 16384
  - Checksum: 0xf6e9 [correct]

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header. The TCP header shows the SYN flag is set.

- Độ dài của các gói tin từ 1-6:



tcp-ethereal-trace-1 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	1161 > http [SYN] Seq=0 Len=0 MSS=1460
2	0.023172	128.119.245.12	192.168.1.102	TCP	http > 1161 [SYN, ACK] Seq=0 Ack=1 win=5840
3	0.023265	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=1 Ack=1 win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	1161 > http [PSH, ACK] Seq=1 Ack=1 win=17520 Len=0
5	0.041737	192.168.1.102	128.119.245.12	TCP	1161 > http [PSH, ACK] Seq=566 Ack=1 win=17520 Len=0
6	0.053937	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=566 win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=2026 Ack=1 win=17520 Len=0
8	0.054690	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=3486 Ack=1 win=17520 Len=0
9	0.077294	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=2026 win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=4946 Ack=1 win=17520 Len=0
11	0.078157	192.168.1.102	128.119.245.12	TCP	1161 > http [ACK] Seq=6406 Ack=1 win=17520 Len=0
12	0.124085	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=3486 win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1161 > http [PSH, ACK] Seq=7866 Ack=1 win=17520 Len=0
14	0.169118	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=4946 win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=6406 win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	http > 1161 [ACK] Seq=1 Ack=7866 win=20440 Len=0

Frame 11 (1514 bytes on wire (1211 bytes captured) on interface 0)

Ethernet II, Src: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG\_da:af:73 (00:06:25:da:af:73)

Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)

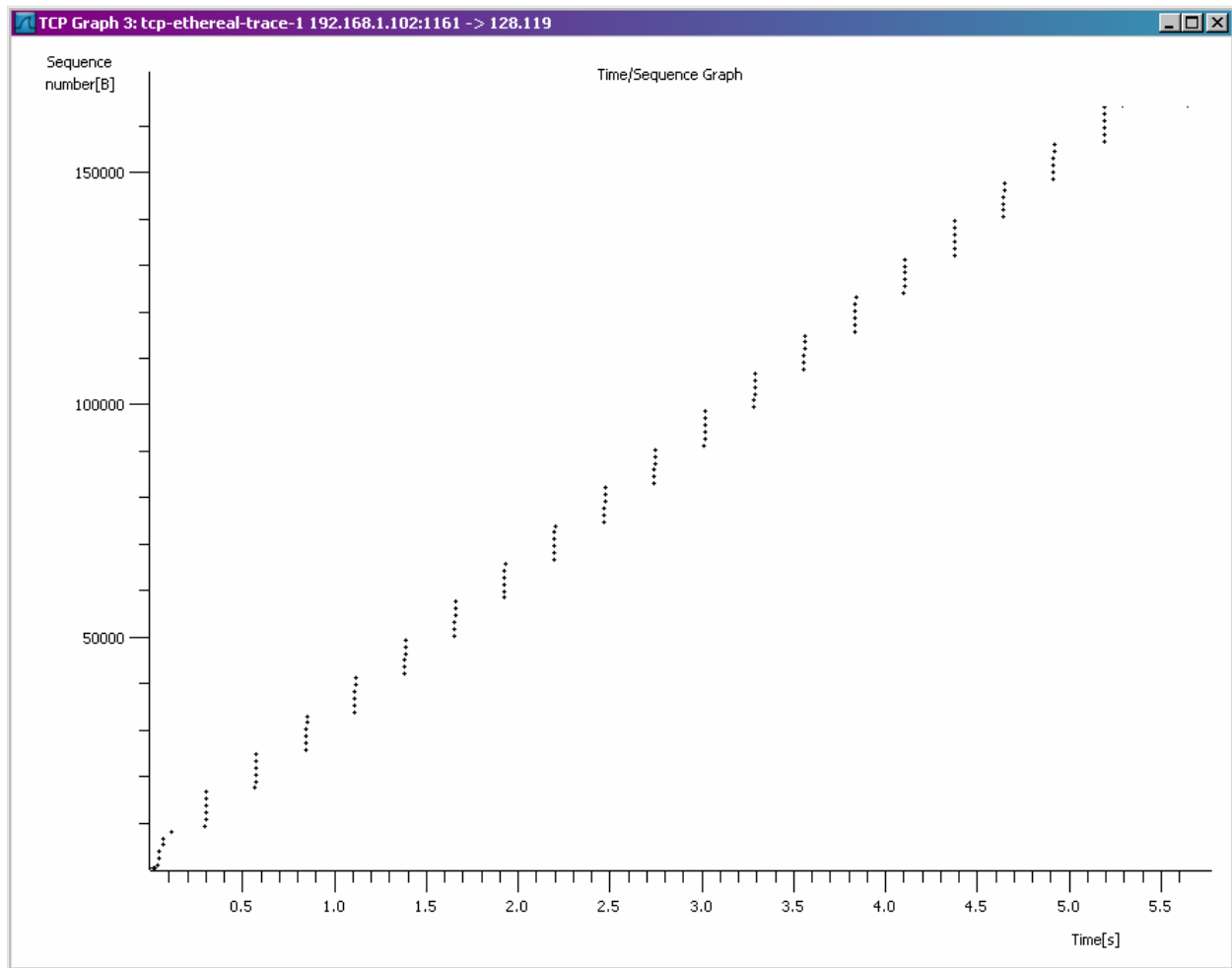
Transmission Control Protocol, Src Port: 1161 (1161), Dst Port: http (80), Seq: 6406, Ack: 1, Len: 1460

Source port: 1161 (1161)  
Destination port: http (80)  
Sequence number: 6406 (relative sequence number)  
[Next sequence number: 7866 (relative sequence number)]  
Acknowledgement number: 1 (relative ack number)  
Header length: 20 bytes  
Flags: 0x10 (ACK)  
0... .. = Congestion window Reduced (CWR): Not set  
0... .. = ECN-Echo: Not set  
..0. .... = Urgent: Not set  
...1 .... = Acknowledgment: Set

0020 f5 0c 04 89 00 50 0d d6 1a fa 34 a2 74 1a 50 10 ...P...4.t.P.  
0030 44 70 95 83 00 00 20 55 6e 69 74 65 64 20 53 74 Dp... United St  
0040 61 74 65 73 20 63 6f 70 79 72 69 67 68 74 0d 0a ates cop yright..  
0050 6f 6e 20 6f 72 20 66 6f 72 20 74 68 69 73 20 77 on or fo r this w  
0060 6f 72 6b 2c 20 73 6f 20 74 68 65 20 50 72 6f 6a ork, so the Proj  
0070 65 62 74 20 28 61 6a 64 20 70 6f 75 21 20 20 62 ect (and you) c

Transmission Control Protocol (tcp), 20 bytes P: 213 D: 213 M: 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?