## **Networking Lab Assignment**

Name : SP Harish

Roll No: IIT2013134

Compiling and Running the file:

a) There are two projects:

SingleClientServer\_ChatApplication ,

MultipleClientChatting

- b)To run a project, copy the entire project into Netbeans Projects Application or import the project;
- c)For each of the projects, run the Server class first to set up the server. Then run the Client class. In Case of multiple chat clients, run the Client class again multiple number of times.

Run Command for a class: Open the class in Netbeans and press 'Shift+F6'

1)A simple chat application in which a single client communicates with the server.

Wireshark screenshot:

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help										
•	<b>1</b>			<b>→ → ★ ★</b>		<b>+</b> - 1	**		I ங 🖭 🍪	
Filte	r:		_	Expression Clea	r Apply	/ Save				
No.	Time	Source	Destination	Protoco	Lengti	Info				
	1 0.00000000	0 127.0.0.1	127.0.0.1	TCP	79	34372 > persona	al-agent	[PSH,	, ACK] Seq=1 Ack=1 Win=342 Len=13 TSval=14362648 TSecr=	:14343
	2 0.00005200	0 127.0.0.1	127.0.0.1	TCP	66	personal-agent	> 34372	[ACK]	] Seq=1 Ack=14 Win=342 Len=0 TSval=14362648 TSecr=14362	2648
	3 11.8164780	0 127.0.0.1	127.0.0.1	TCP					, ACK] Seq=1 Ack=14 Win=342 Len=26 TSval=14365602 TSec	
	4 11.8165260			TCP					] Seq=14 Ack=27 Win=342 Len=0 TSval=14365602 TSecr=1436	
	5 148.688062	0 127.0.0.1	127.0.0.1	TCP					, ACK] Seq=27 Ack=14 Win=342 Len=0 TSval=14399820 TSec	
	6 148.725220			TCP					] Seq=14 Ack=28 Win=342 Len=0 TSval=14399830 TSecr=1439	
	7 149.857173	0 127.0.0.1	127.0.0.1	TCP					, ACK] Seq=14 Ack=28 Win=342 Len=0 TSval=14400112 TSeci	
	8 149.857224	0 127.0.0.1	127.0.0.1	TCP	66	personal-agent	> 34372	[ACK]	] Seq=28 Ack=15 Win=342 Len=0 TSval=14400113 TSecr=1440	0112
	9 154.932963	0 127.0.0.1	127.0.0.1	TCP					] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=144	
	10 154.932981	0 127.0.0.1	127.0.0.1	TCP					, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=	
	11 154.932999	0 127.0.0.1	127.0.0.1	TCP					] Seq=1 Ack=1 Win=43776 Len=0 TSval=14401381 TSecr=1440	
	12 159.511897	0 127.0.0.1		TCP					, ACK] Seq=1 Ack=1 Win=43776 Len=13 TSval=14402526 TSec	
	13 159.511941	0 127.0.0.1		TCP					] Seq=1 Ack=14 Win=43776 Len=0 TSval=14402526 TSecr=144	
	14 182.919855	0 127.0.0.1	127.0.0.1	TCP	91	personal-agent	> 34373	[PSH,	, ACK] Seq=1 Ack=14 Win=43776 Len=25 TSval=14408378 TSe	cr=14
	15 182.919916	0 127.0.0.1	127.0.0.1	TCP	66	34373 > persona	al-agent	[ACK]	] Seq=14 Ack=26 Win=43776 Len=0 TSval=14408378 TSecr=14	140837
[Length: 26]										
0010	00 4e fb 3a 4	10 00 40 06	41 6d 7f 00 00 01 7f 00	.N.:@.@. Am		*******				
0020			4a 72 82 ce 81 c5 80 18	D Jr						
			08 0a 00 db 33 a2 00 db	.V.B3						
0040 0050	28 18 00 18 6 65 2e 2e 20 6		69 20 61 6d 20 66 69 6e 72 20 75 3f	<pre>(hi! i am fin e how r u?</pre>						
***	Data (data.dat	a). 26 bytes	Packets: 15 · Displaye	ed: 15 (100.0%)					Profile: Default	

### Data Sent from client :

### Reply from Server :

# Chatting Screenshot : Client :

```
Connecting to server
Hi how r u?
Server: I am fine. How are you?
I am great
Just graduated with flying colors
Server: that is so great
Server: i am happy for u
```

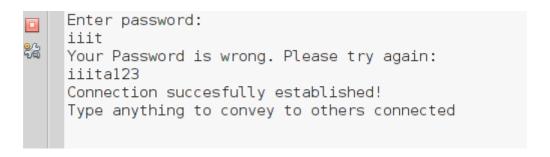
#### Server:

```
Waiting for client....
Client: Hi how r u?
I am fine. How are you?
Client: I am great
Client: Just graduated with flying colors
that is so great
i am happy for u
```

2) Supporting Multiple clients using thread programming wiht authentication. Server Log:



## Password Checking:



### Screenshot of 3 clients:

```
Enter password:
iiita123
Connection succesfully established!
Type anything to convey to others connected
Client 3: hi there
hello guys
Client 1: hello all
```

Enter password:
iiita123
Connection successfully established!
Type anything to convey to others connected
hi there
Client 2: hello guys
Client 1: hello all



3) I Encrypt messages while sending through the server and decrypt it again back. Encrypted message captured in wireshark:

4) For security reasons, we encrypt the message and send it via the server using AES Algorithm.

For encryption we must use a secret key along with the algorithm. We use an algorithm called **AES 128.** AES algorithm can use a key of 128 bits (16 bytes

\* 8);

Actual message : helloall

EnCrypted message: njmBzJz9MMjPV0ucb1IQog== by algorithm which is same as captured in the wireshark.