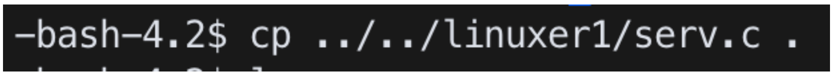
lect4, 5_homework

12141163

이욱진

5. Homework

1) Copy serv.c.



```
-bash-4.2$ cp ../../linuxer1/serv.c .
```

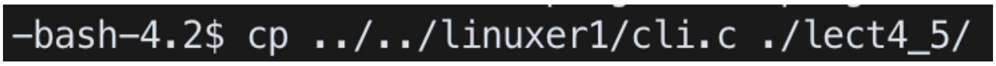
- Open putty terminal and connect to 165.246.38.151 or 165.246.38.157
- Copy serv.c

```
$ cp ../../linuxer1/serv.c . (or "cp  ../../linuxer3/serv.c  ." in 157)
$ ls
serv.c
```

- Compile

```
$ gcc -o serv serv.c
```

2) Copy cli.c



```
-bash-4.2$ cp ../../linuxer1/cli.c ./lect4_5/
```

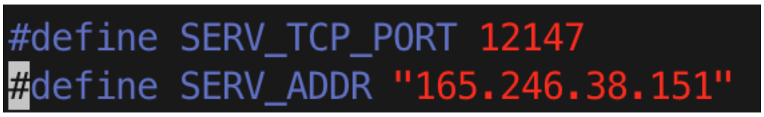
- Open another putty terminal and connect to 165.246.38.151 or 165.246.38.157
- Copy cli.c

```
$ cp ../../linuxer1/cli.c . (or "cp  ../../linuxer3/cli.c  ."  in 157)
$ ls
cli.c
```

- Compile

```
$ gcc -o cli cli.c
```

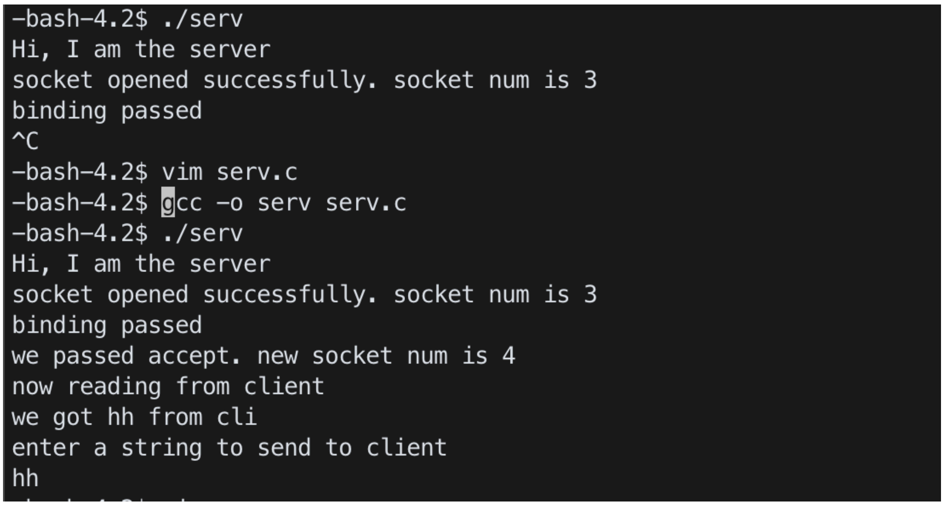
3) Adjust port number both server and client. Recompile both and run the server first and run the client next. The client should talk first and then the server.



```
#define SERV_TCP_PORT 12147
#define SERV_ADDR "165.246.38.151"
```

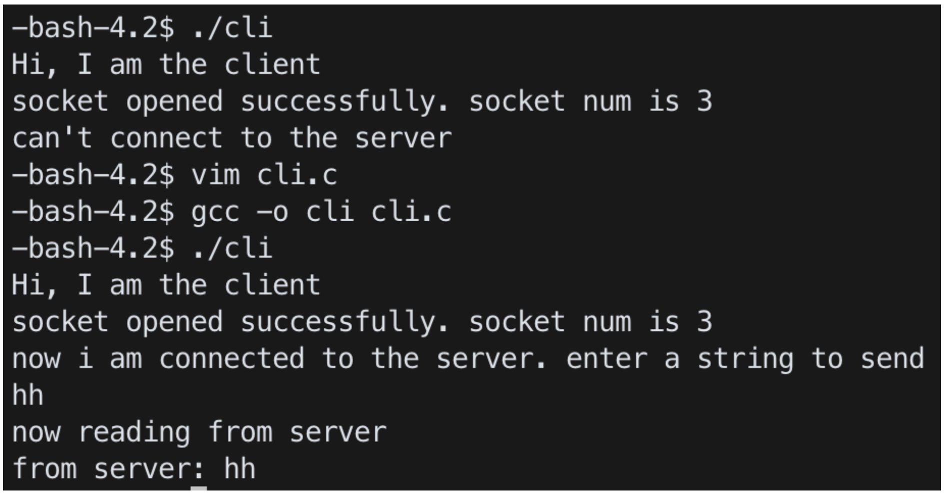
serv.c 와 cli.c 의 port number를 12147 로 동일하게 설정해주었습니다.
그리고 컴파일을 다시 한 후 서버를먼저 실행시킨 뒤 클라이언트를실행시켜 정상적으로 대화할 수 있는지 확인하였습니다.

serv



```
-bash-4.2$ ./serv
Hi, I am the server
socket opened successfully. socket num is 3
binding passed
^C
-bash-4.2$ vim serv.c
-bash-4.2$ gcc -o serv serv.c
-bash-4.2$ ./serv
Hi, I am the server
socket opened successfully. socket num is 3
binding passed
we passed accept. new socket num is 4
now reading from client
we got hh from cli
enter a string to send to client
hh
```

cli



```
-bash-4.2$ ./cli
Hi, I am the client
socket opened successfully. socket num is 3
can't connect to the server
-bash-4.2$ vim cli.c
-bash-4.2$ gcc -o cli cli.c
-bash-4.2$ ./cli
Hi, I am the client
socket opened successfully. socket num is 3
now i am connected to the server. enter a string to send
hh
now reading from server
from server: hh
```

1) Make a client in your PC as follows.
(For macOS, use sftp to download cli.c from lab server and use it to connect to the server.)

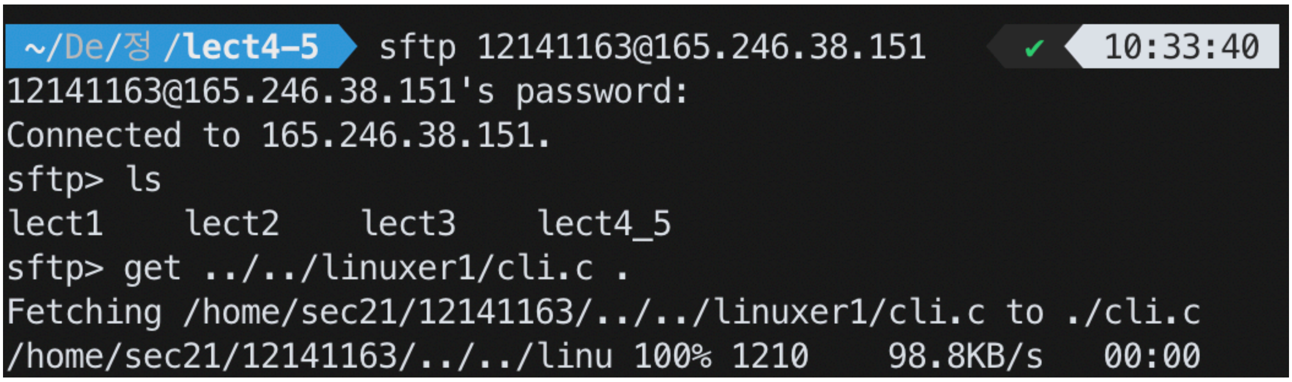
a) Run Microsoft Visual Studio.
b) Create an empty project:
- Select file->new->projects->win32 console application
- Adjust “Location” for the project directory and give a project name (e.g. “proj1”) and hit “Confirm” button
- Hit “Next” in the wizard window.
- Uncheck every box and check “Empty Project” box and hit “Finish” button.
c) Write a C++ source file
- Press the right mouse button on “proj1” symbol.
- Select Add->New Item->C++ file
- Give a file name (for example: main.cpp) and hit “Add” button.
- Copy and paste "wincli.cpp" code (given below). Adjust ip/port number.
d) Compile
- Select “project->proj1->manifest tools->input and output->include manifest” and set “No”
- add ws2_32.lib in project>properties>linker>input>additional dependencies>edit

- Select build->Solution Build
- You should see “Success 1” at the bottom of the compile window.

e) Run

- Run the server first.
- Run the client: select Debug->Execute without debugging

(* if you have LINK error even with ws2_32.lib included, add below at the top of your code:
    #pragma comment (lib, "ws2_32.lib")
*)



```
~/De/정 /lect4-5  sftp 12141163@165.246.38.151                    ✓  10:33:40
12141163@165.246.38.151's password:
Connected to 165.246.38.151.
sftp> ls
lect1     lect2     lect3     lect4_5
sftp> get ../../linuxer1/cli.c .
Fetching /home/sec21/12141163/../../linuxer1/cli.c to ./cli.c
/home/sec21/12141163/../../linu 100% 1210     98.8KB/s   00:00
```

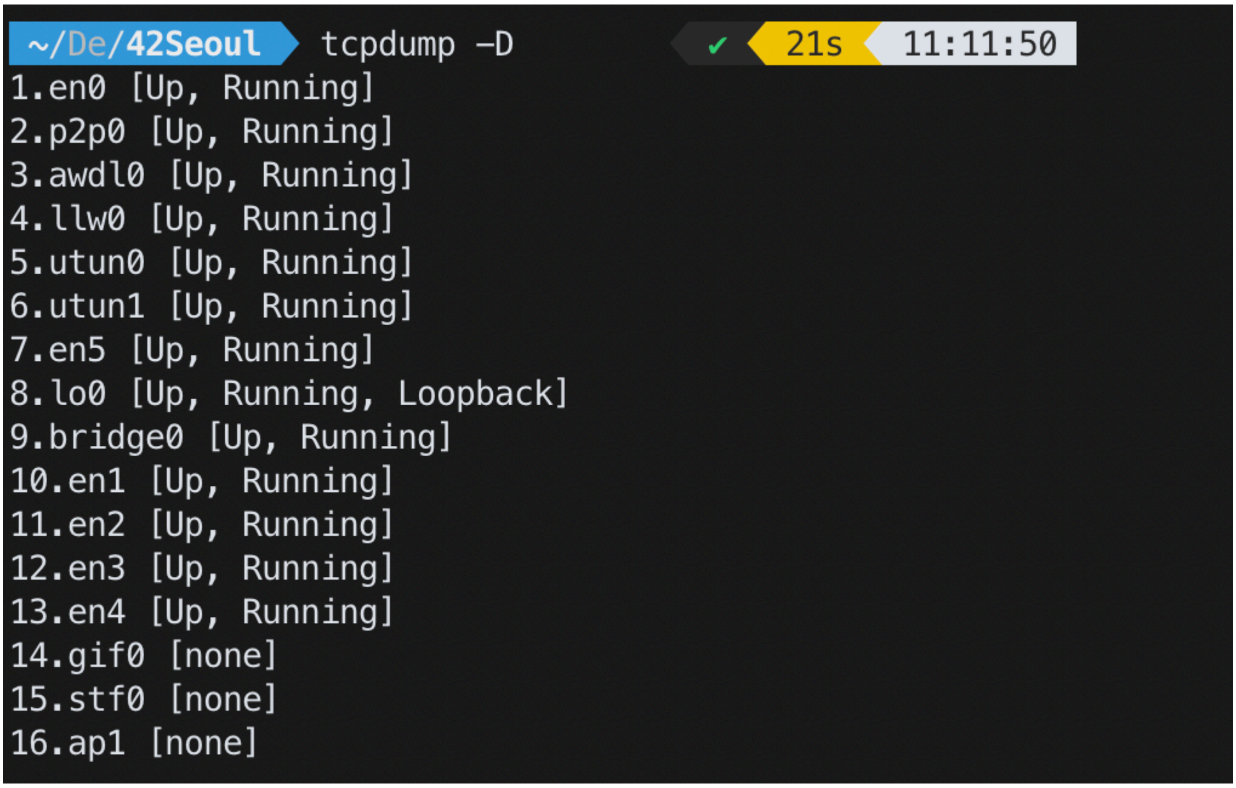
sftp를 이용하여 서버의 cli.c를 get명령어를 이용하여 제 개인컴퓨터로 가지고왔습니다.

2) Download win10pcap from iClass and install. Download windump.exe from iClass and run (in the command window; open command window as admin if needed) to monitor packets for specified port.

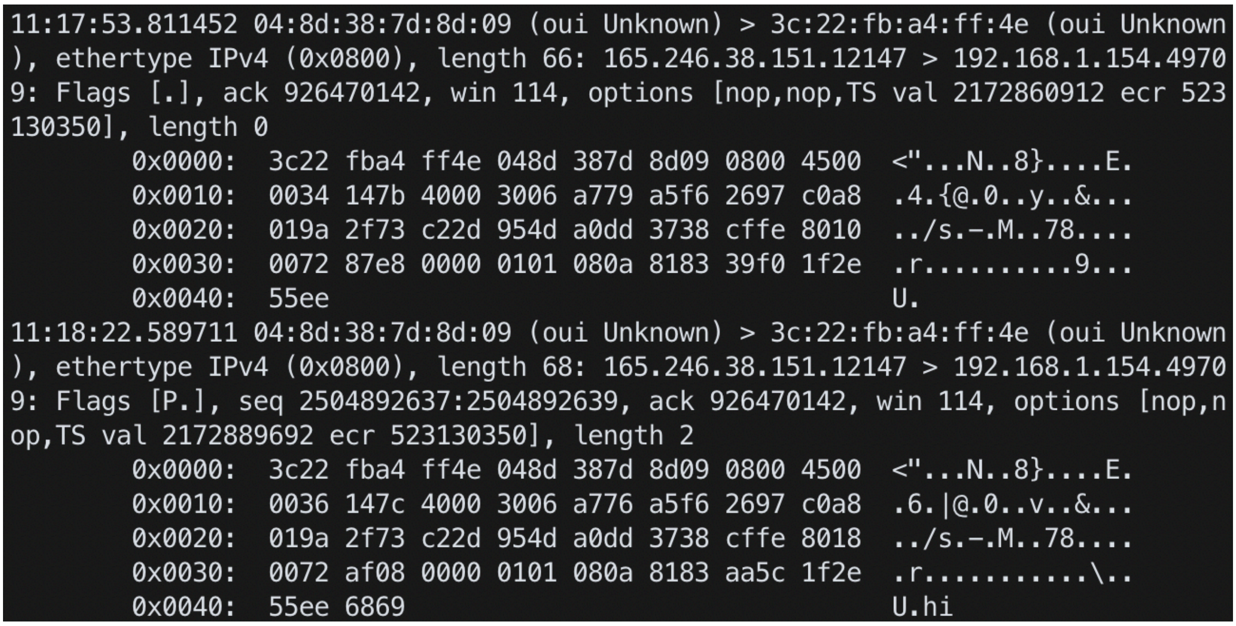
    windump -D   : check available network interfaces
    windump -eSXX -i 2 -s 80 port 9924   : monitor packets at device 2 whose src or dest ports are 9924

(for wireshark: right mouse button click, run as admin)
(for MacOS, use tcpdump)

tcpdump를 사용하기 전 -D옵션을통하여 사용가능한 인터페이스를 확인하였습니다.



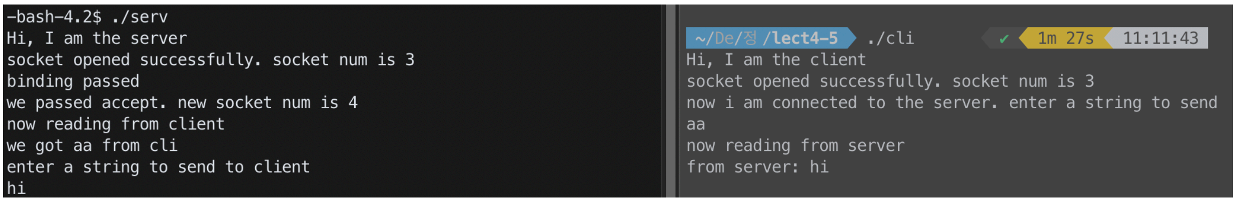
```
~/De/42Seoul  tcpdump -D              ✓  21s  11:11:50
1.en0 [Up, Running]
2.p2p0 [Up, Running]
3.awdl0 [Up, Running]
4.llw0 [Up, Running]
5.utun0 [Up, Running]
6.utun1 [Up, Running]
7.en5 [Up, Running]
8.lo0 [Up, Running, Loopback]
9.bridge0 [Up, Running]
10.en1 [Up, Running]
11.en2 [Up, Running]
12.en3 [Up, Running]
13.en4 [Up, Running]
14.gif0 [none]
15.stf0 [none]
16.ap1 [none]
```



```
11:17:53.811452 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown
), ethertype IPv4 (0x0800), length 66: 165.246.38.151.12147 > 192.168.1.154.4970
9: Flags [.], ack 926470142, win 114, options [nop,nop,TS val 2172860912 ecr 523
130350], length 0
	0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4500  <"...N..8}....E.
	0x0010:  0034 147b 4000 3006 a779 a5f6 2697 c0a8  .4.{@.0..y..&...
	0x0020:  019a 2f73 c22d 954d a0dd 3738 cffe 8010  ../s.-.M..78....
	0x0030:  0072 87e8 0000 0101 080a 8183 39f0 1f2e  .r.........9...
	0x0040:  55ee                                     U.
11:18:22.589711 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown
), ethertype IPv4 (0x0800), length 68: 165.246.38.151.12147 > 192.168.1.154.4970
9: Flags [P.], seq 2504892637:2504892639, ack 926470142, win 114, options [nop,n
op,TS val 2172889692 ecr 523130350], length 2
	0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4500  <"...N..8}....E.
	0x0010:  0036 147c 4000 3006 a776 a5f6 2697 c0a8  .6.|@.0..v..&...
	0x0020:  019a 2f73 c22d 954d a0dd 3738 cffe 8018  ../s.-.M..78....
	0x0030:  0072 af08 0000 0101 080a 8183 aa5c 1f2e  .r..........\..
	0x0040:  55ee 6869                                U.hi
```

sudo tcpdump 를 이용하여 en0인터페이스를 사용하여 패킷을 확인하였습니다.

3) Run your server again. Run the client in your PC.



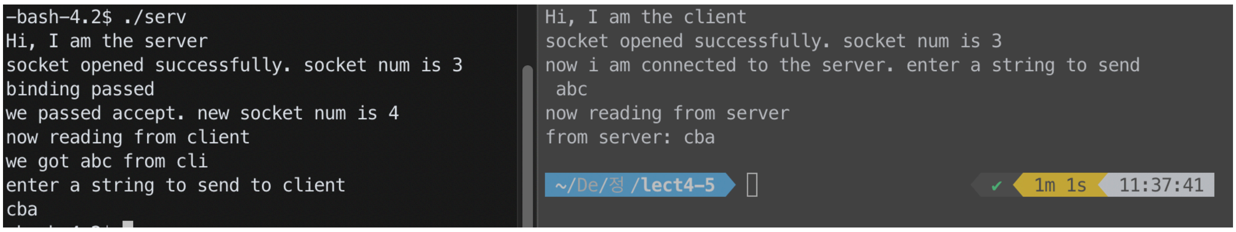
```
-bash-4.2$ ./serv
Hi, I am the server
socket opened successfully. socket num is 3
binding passed
we passed accept. new socket num is 4
now reading from client
we got aa from cli
enter a string to send to client
hi
```

```
~/De/정 /lect4-5  ./cli                    ✓  1m 27s  11:11:43
Hi, I am the client
socket opened successfully. socket num is 3
now i am connected to the server. enter a string to send
aa
now reading from server
from server: hi
```

각각의 터미널을 이용하여 151서버내부에서 server를 실행시키고 그 후 제 개인컴퓨터에서 cli를 실행하였습니다. 정상적으로 패킷을 주고받는것을 확인할 수 있었습니다.

4) Find the first packet which is a SYN packet sent by the client to the server in the windump window. Extract all packet header information. Refer TCP packet structure in Section 6 below.

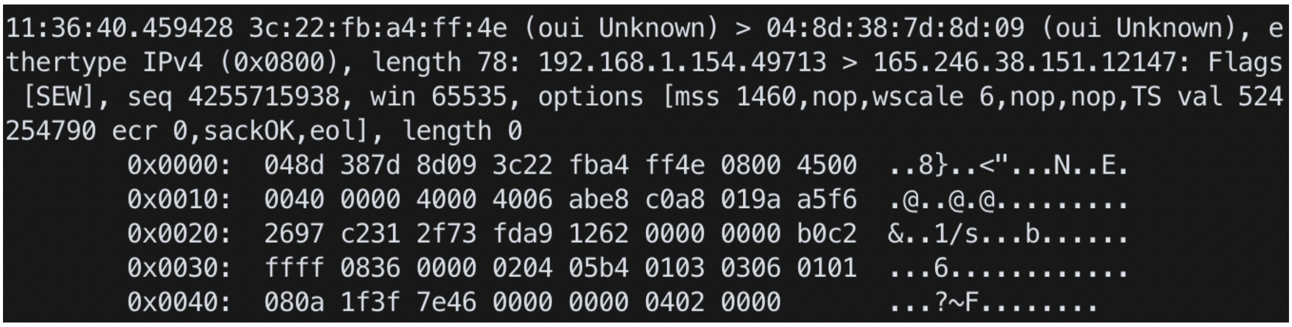
다시서버와 클리언트를 재실행시켜 abc와 cba라는 문자를 주고받게 하였습니다.



```
-bash-4.2$ ./serv
Hi, I am the server
socket opened successfully. socket num is 3
binding passed
we passed accept. new socket num is 4
now reading from client
we got abc from cli
enter a string to send to client
cba
```

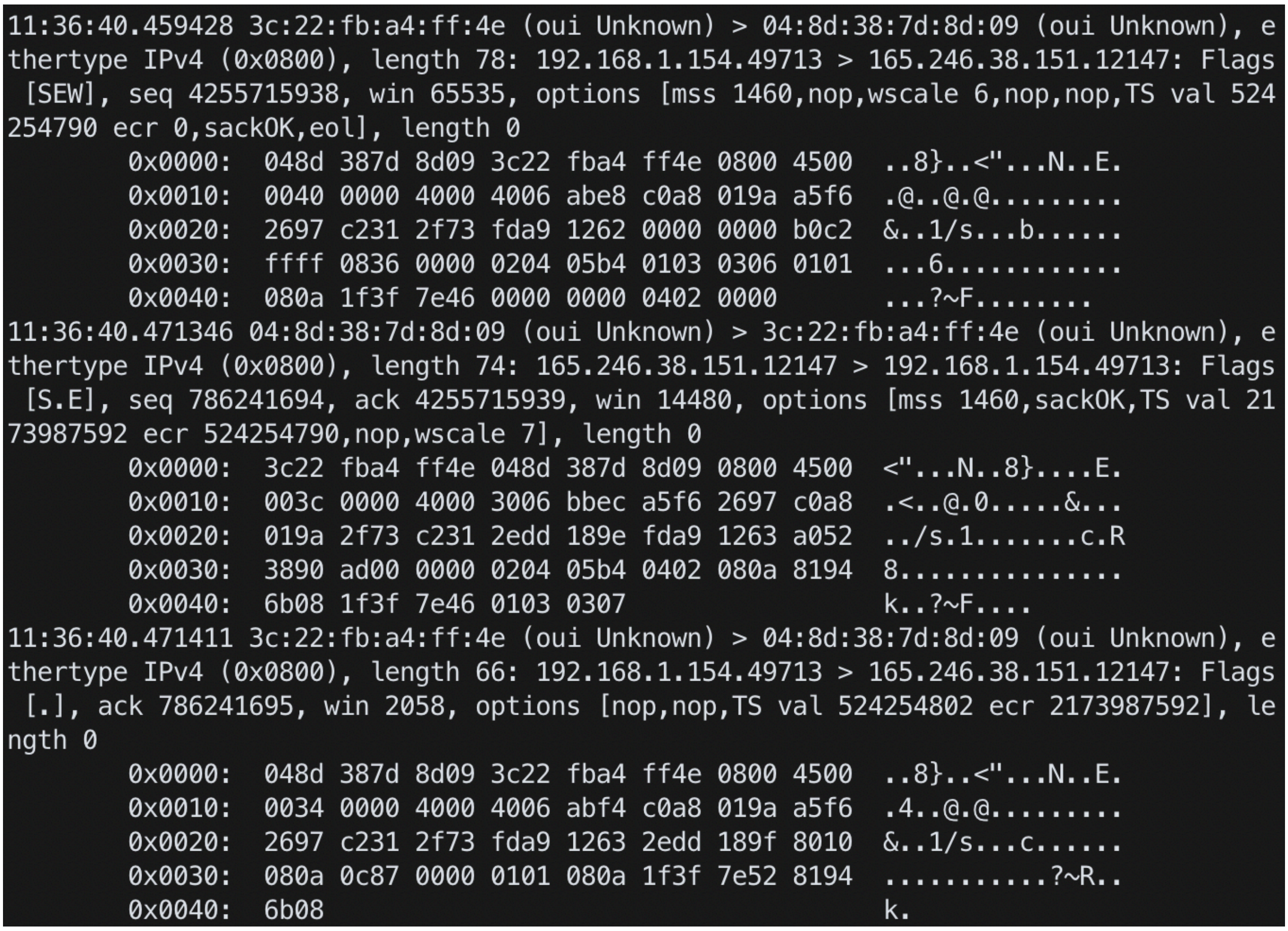
```
Hi, I am the client
socket opened successfully. socket num is 3
now i am connected to the server. enter a string to send
 abc
now reading from server
from server: cba

~/De/정 /lect4-5  ▯                        ✓  1m 1s  11:37:41
```

tcpdump를 사용하여 처음 정보를주고받기 전 syn packet을 찾을 수 있었습니다.

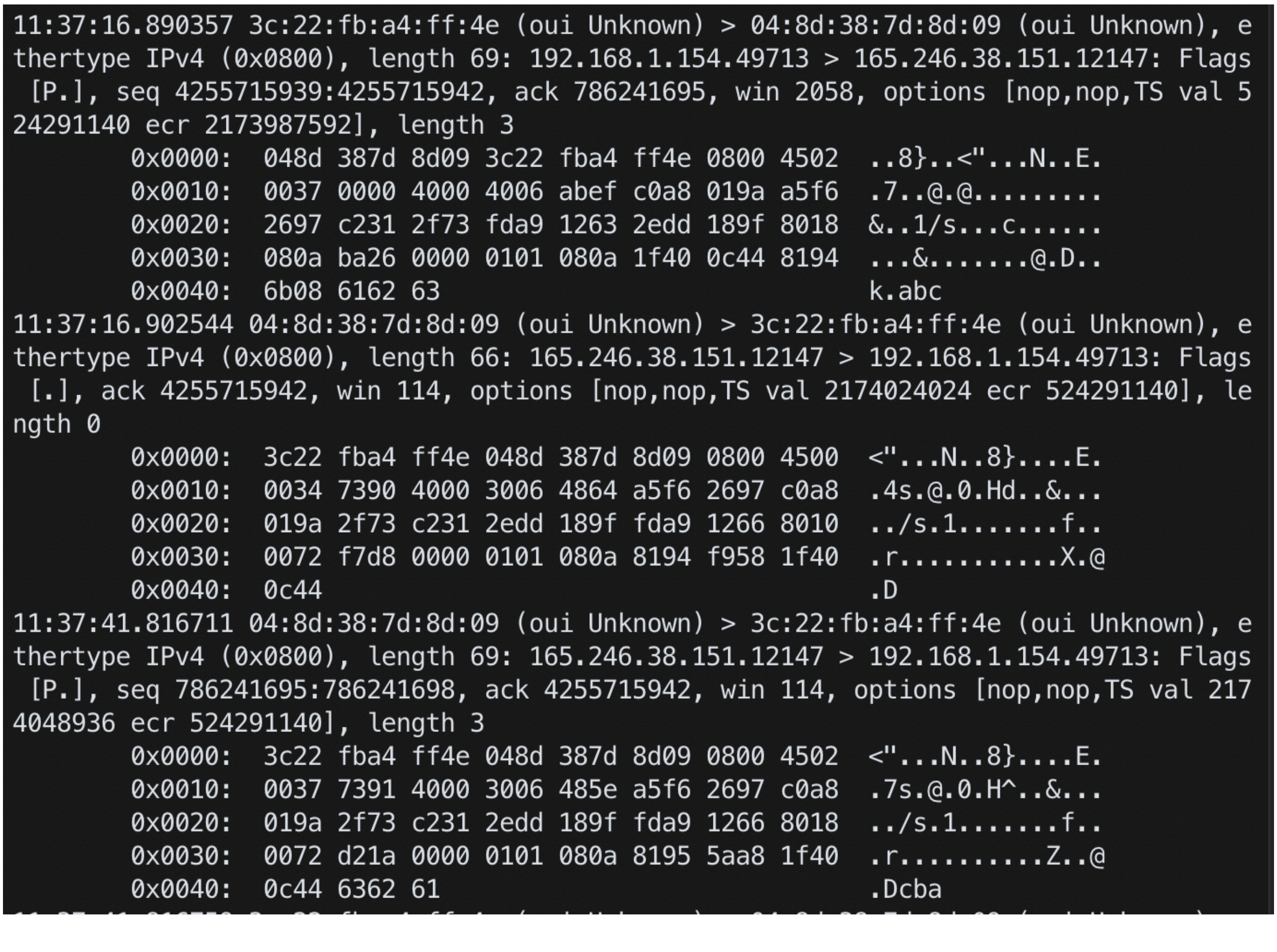


```
11:36:40.459428 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 78: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [SEW], seq 4255715938, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 524
254790 ecr 0,sackOK,eol], length 0
	0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4500  ..8}..<"...N..E.
	0x0010:  0040 0000 4000 4006 abe8 c0a8 019a a5f6  .@..@.@.........
	0x0020:  2697 c231 2f73 fda9 1262 0000 0000 b0c2  &..1/s...b......
	0x0030:  ffff 0836 0000 0204 05b4 0103 0306 0101  ...6............
	0x0040:  080a 1f3f 7e46 0000 0000 0402 0000       ...?~F........
```

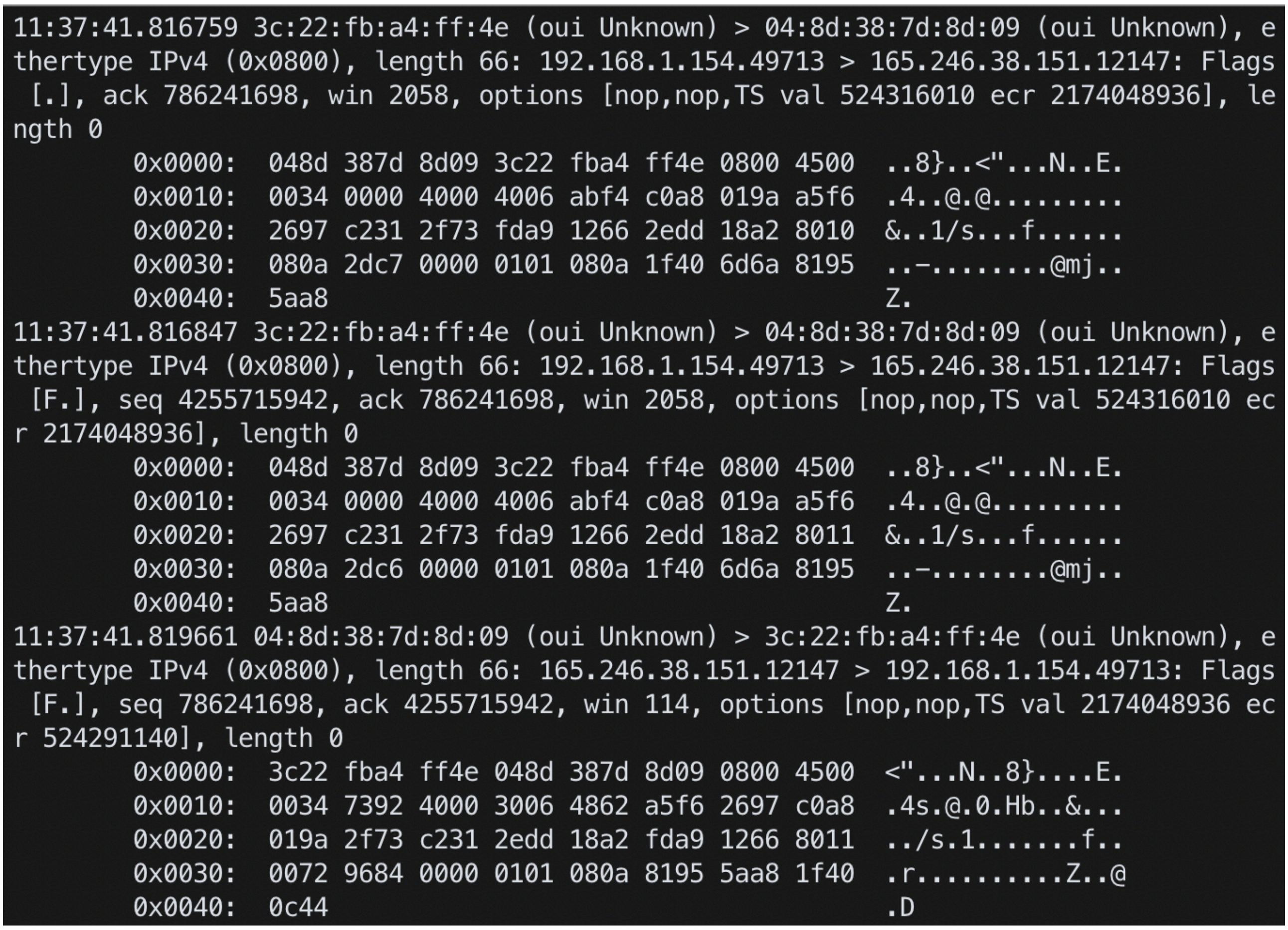
5) Analyze rest of the packets similarly.



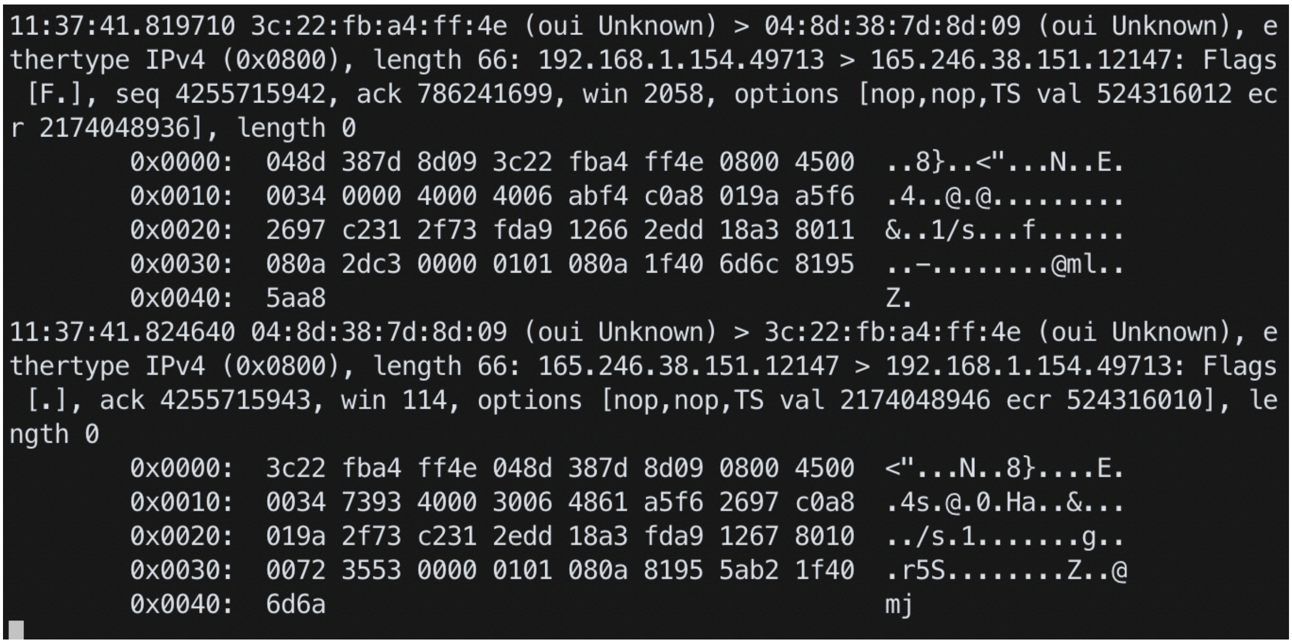
```
11:36:40.459428 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 78: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [SEW], seq 4255715938, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 524
254790 ecr 0,sackOK,eol], length 0
        0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4500  ..8}..<"...N..E.
        0x0010:  0040 0000 4000 4006 abe8 c0a8 019a a5f6  .@..@.@.........
        0x0020:  2697 c231 2f73 fda9 1262 0000 0000 b0c2  &..1/s...b......
        0x0030:  ffff 0836 0000 0204 05b4 0103 0306 0101  ...6............
        0x0040:  080a 1f3f 7e46 0000 0000 0402 0000       ...?~F........
11:36:40.471346 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown), e
thertype IPv4 (0x0800), length 74: 165.246.38.151.12147 > 192.168.1.154.49713: Flags
 [S.E], seq 786241694, ack 4255715939, win 14480, options [mss 1460,sackOK,TS val 21
73987592 ecr 524254790,nop,wscale 7], length 0
        0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4500  <"...N..8}....E.
        0x0010:  003c 0000 4000 3006 bbec a5f6 2697 c0a8  .<..@.0.....&...
        0x0020:  019a 2f73 c231 2edd 189e fda9 1263 a052  ../s.1.......c.R
        0x0030:  3890 ad00 0000 0204 05b4 0402 080a 8194  8...............
        0x0040:  6b08 1f3f 7e46 0103 0307                 k..?~F....
11:36:40.471411 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 66: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [.], ack 786241695, win 2058, options [nop,nop,TS val 524254802 ecr 2173987592], le
ngth 0
        0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4500  ..8}..<"...N..E.
        0x0010:  0034 0000 4000 4006 abf4 c0a8 019a a5f6  .4..@.@.........
        0x0020:  2697 c231 2f73 fda9 1263 2edd 189f 8010  &..1/s...c......
        0x0030:  080a 0c87 0000 0101 080a 1f3f 7e52 8194  ...........?~R..
        0x0040:  6b08                                     k.
```



```
11:37:16.890357 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 69: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [P.], seq 4255715939:4255715942, ack 786241695, win 2058, options [nop,nop,TS val 5
24291140 ecr 2173987592], length 3
        0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4502  ..8}..<"...N..E.
        0x0010:  0037 0000 4000 4006 abef c0a8 019a a5f6  .7..@.@.........
        0x0020:  2697 c231 2f73 fda9 1263 2edd 189f 8018  &..1/s...c......
        0x0030:  080a ba26 0000 0101 080a 1f40 0c44 8194  ...&.......@.D..
        0x0040:  6b08 6162 63                             k.abc
11:37:16.902544 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown), e
thertype IPv4 (0x0800), length 66: 165.246.38.151.12147 > 192.168.1.154.49713: Flags
 [.], ack 4255715942, win 114, options [nop,nop,TS val 2174024024 ecr 524291140], le
ngth 0
        0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4500  <"...N..8}....E.
        0x0010:  0034 7390 4000 3006 4864 a5f6 2697 c0a8  .4s.@.0.Hd..&...
        0x0020:  019a 2f73 c231 2edd 189f fda9 1266 8010  ../s.1.......f..
        0x0030:  0072 f7d8 0000 0101 080a 8194 f958 1f40  .r...........X.@
        0x0040:  0c44                                     .D
11:37:41.816711 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown), e
thertype IPv4 (0x0800), length 69: 165.246.38.151.12147 > 192.168.1.154.49713: Flags
 [P.], seq 786241695:786241698, ack 4255715942, win 114, options [nop,nop,TS val 217
4048936 ecr 524291140], length 3
        0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4502  <"...N..8}....E.
        0x0010:  0037 7391 4000 3006 485e a5f6 2697 c0a8  .7s.@.0.H^..&...
        0x0020:  019a 2f73 c231 2edd 189f fda9 1266 8018  ../s.1.......f..
        0x0030:  0072 d21a 0000 0101 080a 8195 5aa8 1f40  .r..........Z..@
        0x0040:  0c44 6362 61                             .Dcba
```



```
11:37:41.816759 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 66: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [.], ack 786241698, win 2058, options [nop,nop,TS val 524316010 ecr 2174048936], le
ngth 0
        0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4500  ..8}..<"...N..E.
        0x0010:  0034 0000 4000 4006 abf4 c0a8 019a a5f6  .4..@.@.........
        0x0020:  2697 c231 2f73 fda9 1266 2edd 18a2 8010  &..1/s...f......
        0x0030:  080a 2dc7 0000 0101 080a 1f40 6d6a 8195  ..-........@mj..
        0x0040:  5aa8                                     Z.
11:37:41.816847 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 66: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [F.], seq 4255715942, ack 786241698, win 2058, options [nop,nop,TS val 524316010 ec
r 2174048936], length 0
        0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4500  ..8}..<"...N..E.
        0x0010:  0034 0000 4000 4006 abf4 c0a8 019a a5f6  .4..@.@.........
        0x0020:  2697 c231 2f73 fda9 1266 2edd 18a2 8011  &..1/s...f......
        0x0030:  080a 2dc6 0000 0101 080a 1f40 6d6a 8195  ..-........@mj..
        0x0040:  5aa8                                     Z.
11:37:41.819661 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown), e
thertype IPv4 (0x0800), length 66: 165.246.38.151.12147 > 192.168.1.154.49713: Flags
 [F.], seq 786241698, ack 4255715942, win 114, options [nop,nop,TS val 2174048936 ec
r 524291140], length 0
        0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4500  <"...N..8}....E.
        0x0010:  0034 7392 4000 3006 4862 a5f6 2697 c0a8  .4s.@.0.Hb..&...
        0x0020:  019a 2f73 c231 2edd 18a2 fda9 1266 8011  ../s.1.......f..
        0x0030:  0072 9684 0000 0101 080a 8195 5aa8 1f40  .r..........Z..@
        0x0040:  0c44                                     .D
```



```
11:37:41.819710 3c:22:fb:a4:ff:4e (oui Unknown) > 04:8d:38:7d:8d:09 (oui Unknown), e
thertype IPv4 (0x0800), length 66: 192.168.1.154.49713 > 165.246.38.151.12147: Flags
 [F.], seq 4255715942, ack 786241699, win 2058, options [nop,nop,TS val 524316012 ec
r 2174048936], length 0
        0x0000:  048d 387d 8d09 3c22 fba4 ff4e 0800 4500  ..8}..<"...N..E.
        0x0010:  0034 0000 4000 4006 abf4 c0a8 019a a5f6  .4..@.@.........
        0x0020:  2697 c231 2f73 fda9 1266 2edd 18a3 8011  &..1/s...f......
        0x0030:  080a 2dc3 0000 0101 080a 1f40 6d6c 8195  ..-........@ml..
        0x0040:  5aa8                                     Z.
11:37:41.824640 04:8d:38:7d:8d:09 (oui Unknown) > 3c:22:fb:a4:ff:4e (oui Unknown), e
thertype IPv4 (0x0800), length 66: 165.246.38.151.12147 > 192.168.1.154.49713: Flags
 [.], ack 4255715943, win 114, options [nop,nop,TS val 2174048946 ecr 524316010], le
ngth 0
        0x0000:  3c22 fba4 ff4e 048d 387d 8d09 0800 4500  <"...N..8}....E.
        0x0010:  0034 7393 4000 3006 4861 a5f6 2697 c0a8  .4s.@.0.Ha..&...
        0x0020:  019a 2f73 c231 2edd 18a3 fda9 1267 8010  ../s.1.......g..
        0x0030:  0072 3553 0000 0101 080a 8195 5ab2 1f40  .r5S........Z..@
        0x0040:  6d6a                                     mj
```

6) Connect to www.inha.ac.kr and analyze SYN, S/ACK, ACK packets between the web browser and www.inha.ac.kr. You may need "-c num" option to capture the first num packets as below.

```
windump –eSXX –c 20 –i 2 –s 80 host www.inha.ac.kr
```

7) Click login menu(로그인) and enter id and password. Find the packet that contains your login ID and password. To capture login ID and password, make the capture size larger, e.g. 3000. Use –w option to save the result in a file (e.g. pktout) and use –r option to read packets from a file.

```
windump –eSXX –w pktout –i 2 –s 3000 host www.inha.ac.kr
windump –eSXX –r pktout > x
vi x
```

8) Connect to portal.inha.ac.kr and do the same thing as in Problem 6) and 7).