Australian
National
University

Computer Lab 02

Wireshark (Why and How)

Networked Information Systems (COMP2410/ COMP6340), 2022 Semester 1

A/Prof Hanna Suominen, Dr Zakir Hossain, and Mr Arslan Khan

Research School of Computer Science,
College of Engineering and Computer Science (CECS)
The Australian National University
Canberra ACT 2601 Australia
www.anu.edu.au

CRICOS Provider No. 00120C

Contents

Wireshark

Summary

Wireshark is used for network troubleshooting, network analysis, software and communications protocol development, and general education about how networks work. It enables us to see all messages sent by a computer, as well as some or all of the messages sent by other computers on a local area network (LAN), depending on how the LAN is designed. This lab introduces a way to install Wireshark and to observe flow of packets using the Wireshark.

Learning Objectives

After completing this lab, students should

- be able to install Wireshark,
- be able to use Wireshark for inspecting network traffic, and
- be able to analyse flow of packets.

Seeing live packets

Requirements

a) Linux virtual machine (Ubuntu Xenial 64bit)
   - ✓ Creating a Virtual Machine in the lab

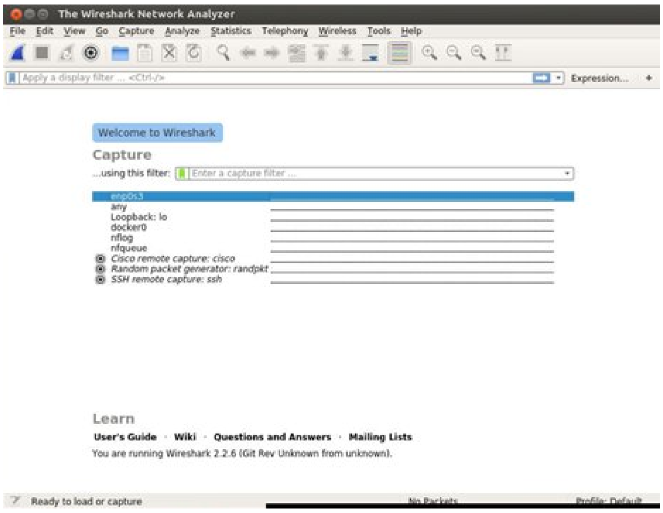
b) Wireshark (for Ubuntu)
   - ✓ How to Use Wireshark: A Complete Tutorial (https://bit.ly/36hyepq)
   - ✓ How To Use Wireshark To Inspect Network Traffic (https://bit.ly/2YsRVaQ)

Procedures

1. Install Wireshark (check before installing, it may already be installed in the lab). Open terminal in ubuntu and type following commands.

   $ sudo apt-get install wireshark

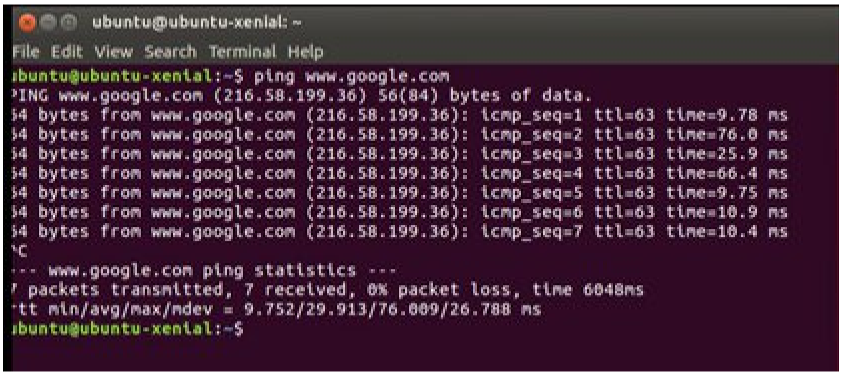
   $ sudo wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
enp0s3
any
Loopback: lo
docker0
nflog
nfqueue
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.6 (Git Rev Unknown from unknown).
Ready to load or capture
No Packets
Profile: Default

You can install wire shark in windows and mac as well. Just download and install them.

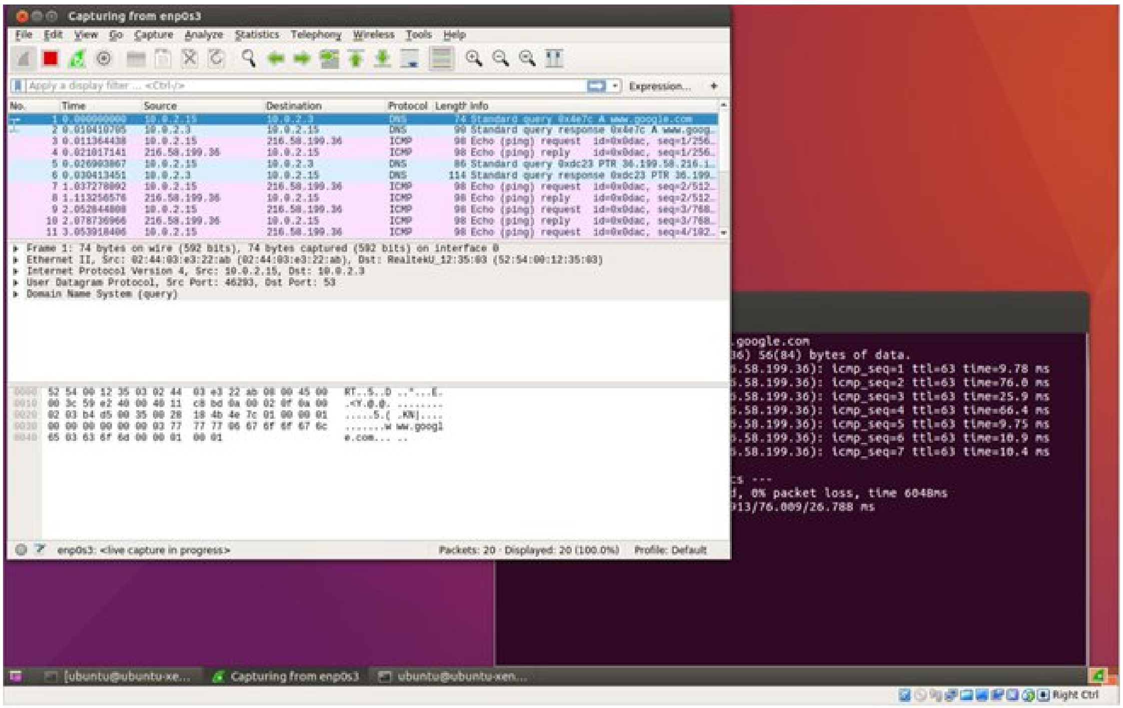
2. Capture packets

   Terminal session ($ ping www.google.com)



```
ubuntu@ubuntu-xenial: ~
ubuntu@ubuntu-xenial:~$ ping www.google.com
PING www.google.com (216.58.199.36) 56(84) bytes of data.
64 bytes from www.google.com (216.58.199.36): icmp_seq=1 ttl=63 time=9.78 ms
64 bytes from www.google.com (216.58.199.36): icmp_seq=2 ttl=63 time=76.0 ms
64 bytes from www.google.com (216.58.199.36): icmp_seq=3 ttl=63 time=25.9 ms
64 bytes from www.google.com (216.58.199.36): icmp_seq=4 ttl=63 time=66.4 ms
64 bytes from www.google.com (216.58.199.36): icmp_seq=5 ttl=63 time=9.75 ms
64 bytes from www.google.com (216.58.199.36): icmp_seq=6 ttl=63 time=10.9 ms
64 bytes from www.google.com (216.58.199.36): icmp_seq=7 ttl=63 time=10.4 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6048ms
rtt min/avg/max/mdev = 9.752/29.913/76.009/26.788 ms
ubuntu@ubuntu-xenial:~$
```

3. Capture packets with ping


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
[ubuntu@ubuntu-xe...
Capturing from enp0s3
ubuntu@ubuntu-xen...
Right Ctrl

```
No.   Time          Source           Destination      Protocol Length Info
   1 0.000000000   10.0.2.15        10.0.2.3         DNS       74 Standard query 0x4e7c A www.google.com
   2 0.010410705   10.0.2.3         10.0.2.15        DNS       90 Standard query response 0x4e7c A www.goog…
   3 0.011364438   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0dac, seq=1/256…
   4 0.021017141   216.58.199.36    10.0.2.15        ICMP      98 Echo (ping) reply    id=0x0dac, seq=1/256…
   5 0.026903867   10.0.2.15        10.0.2.3         DNS       86 Standard query 0xdc23 PTR 36.199.58.216.i…
   6 0.030413451   10.0.2.3         10.0.2.15        DNS      114 Standard query response 0xdc23 PTR 36.199…
   7 1.037278092   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0dac, seq=2/512…
   8 1.113256576   216.58.199.36    10.0.2.15        ICMP      98 Echo (ping) reply    id=0x0dac, seq=2/512…
   9 2.052844808   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0dac, seq=3/768…
  10 2.078736966   216.58.199.36    10.0.2.15        ICMP      98 Echo (ping) reply    id=0x0dac, seq=3/768…
  11 3.053918406   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0dac, seq=4/102…
```

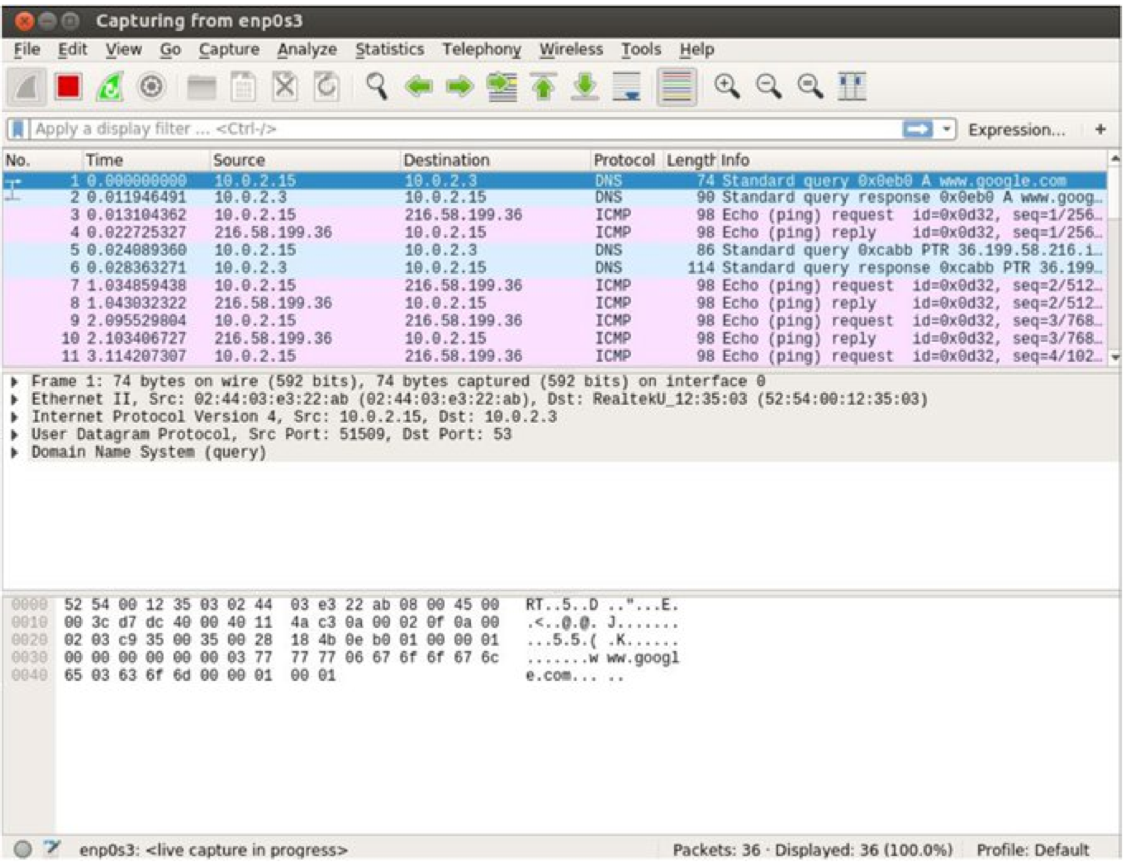
```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: 02:44:03:e3:22:ab (02:44:03:e3:22:ab), Dst: RealtekU_12:35:03 (52:54:00:12:35:03)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
▸ User Datagram Protocol, Src Port: 46293, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  52 54 00 12 35 03 02 44  03 e3 22 ab 08 00 45 00   RT..5..D ..."...E.
0010  00 3c 59 e2 40 00 40 11  c8 bd 0a 00 02 0f 0a 00   .<Y.@.@. ........
0020  02 03 b4 d5 00 35 00 28  18 4b 4e 7c 01 00 00 01   .....5.( .KN|....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e.com... ..
```

enp0s3: <live capture in progress>   Packets: 20 · Displayed: 20 (100.0%)   Profile: Default

```
.google.com
36) 56(84) bytes of data.
6.58.199.36): icmp_seq=1 ttl=63 time=9.78 ms
6.58.199.36): icmp_seq=2 ttl=63 time=76.0 ms
6.58.199.36): icmp_seq=3 ttl=63 time=25.9 ms
6.58.199.36): icmp_seq=4 ttl=63 time=66.4 ms
6.58.199.36): icmp_seq=5 ttl=63 time=9.75 ms
6.58.199.36): icmp_seq=6 ttl=63 time=10.9 ms
6.58.199.36): icmp_seq=7 ttl=63 time=10.4 ms

cs ---
d, 0% packet loss, time 6048ms
913/76.009/26.788 ms
```

4. Capture window
   - ➢ The packet list pane
   - ➢ The packet details pane
   - ➢ The packet bytes pane


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

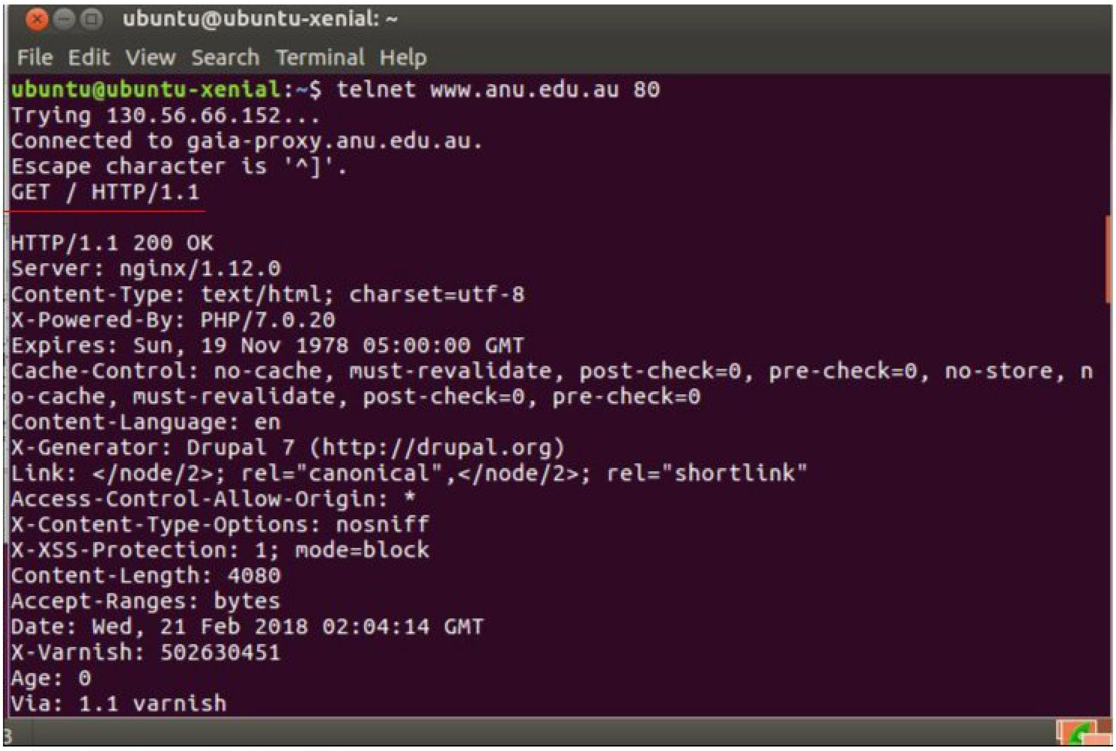
```
No.   Time          Source           Destination      Protocol Length Info
   1 0.000000000   10.0.2.15        10.0.2.3         DNS       74 Standard query 0x0eb0 A www.google.com
   2 0.011946491   10.0.2.3         10.0.2.15        DNS       90 Standard query response 0x0eb0 A www.goog…
   3 0.013104362   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0d32, seq=1/256…
   4 0.022725327   216.58.199.36    10.0.2.15        ICMP      98 Echo (ping) reply    id=0x0d32, seq=1/256…
   5 0.024089360   10.0.2.15        10.0.2.3         DNS       86 Standard query 0xcabb PTR 36.199.58.216.i…
   6 0.028363271   10.0.2.3         10.0.2.15        DNS      114 Standard query response 0xcabb PTR 36.199…
   7 1.034859438   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0d32, seq=2/512…
   8 1.043032322   216.58.199.36    10.0.2.15        ICMP      98 Echo (ping) reply    id=0x0d32, seq=2/512…
   9 2.095529804   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0d32, seq=3/768…
  10 2.103406727   216.58.199.36    10.0.2.15        ICMP      98 Echo (ping) reply    id=0x0d32, seq=3/768…
  11 3.114207307   10.0.2.15        216.58.199.36    ICMP      98 Echo (ping) request  id=0x0d32, seq=4/102…
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▸ Ethernet II, Src: 02:44:03:e3:22:ab (02:44:03:e3:22:ab), Dst: RealtekU_12:35:03 (52:54:00:12:35:03)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
▸ User Datagram Protocol, Src Port: 51509, Dst Port: 53
▸ Domain Name System (query)
```

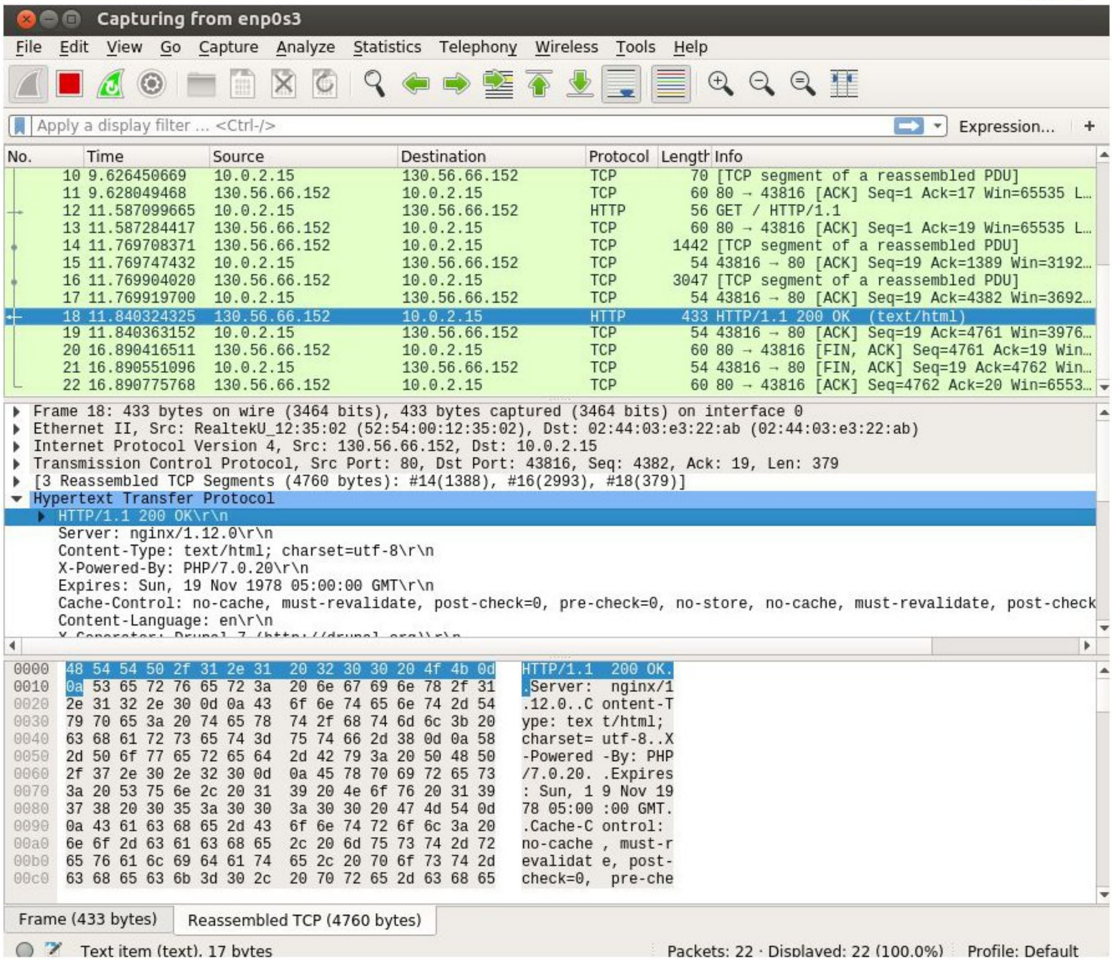
```
0000  52 54 00 12 35 03 02 44  03 e3 22 ab 08 00 45 00   RT..5..D ..."...E.
0010  00 3c d7 dc 40 00 40 11  4a c3 0a 00 02 0f 0a 00   .<..@.@. J.......
0020  02 03 c9 35 00 35 00 28  18 4b 0e b0 01 00 00 01   ...5.5.( .K......
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e.com... ..
```

enp0s3: <live capture in progress>   Packets: 36 · Displayed: 36 (100.0%)   Profile: Default

Try Telnet commands and look for packets in wireshark



```
ubuntu@ubuntu-xenial:~$ telnet www.anu.edu.au 80
Trying 130.56.66.152...
Connected to gaia-proxy.anu.edu.au.
Escape character is '^]'.
GET / HTTP/1.1

HTTP/1.1 200 OK
Server: nginx/1.12.0
Content-Type: text/html; charset=utf-8
X-Powered-By: PHP/7.0.20
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0, no-store, n
o-cache, must-revalidate, post-check=0, pre-check=0
Content-Language: en
X-Generator: Drupal 7 (http://drupal.org)
Link: </node/2>; rel="canonical",</node/2>; rel="shortlink"
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 4080
Accept-Ranges: bytes
Date: Wed, 21 Feb 2018 02:04:14 GMT
X-Varnish: 502630451
Age: 0
Via: 1.1 varnish
```

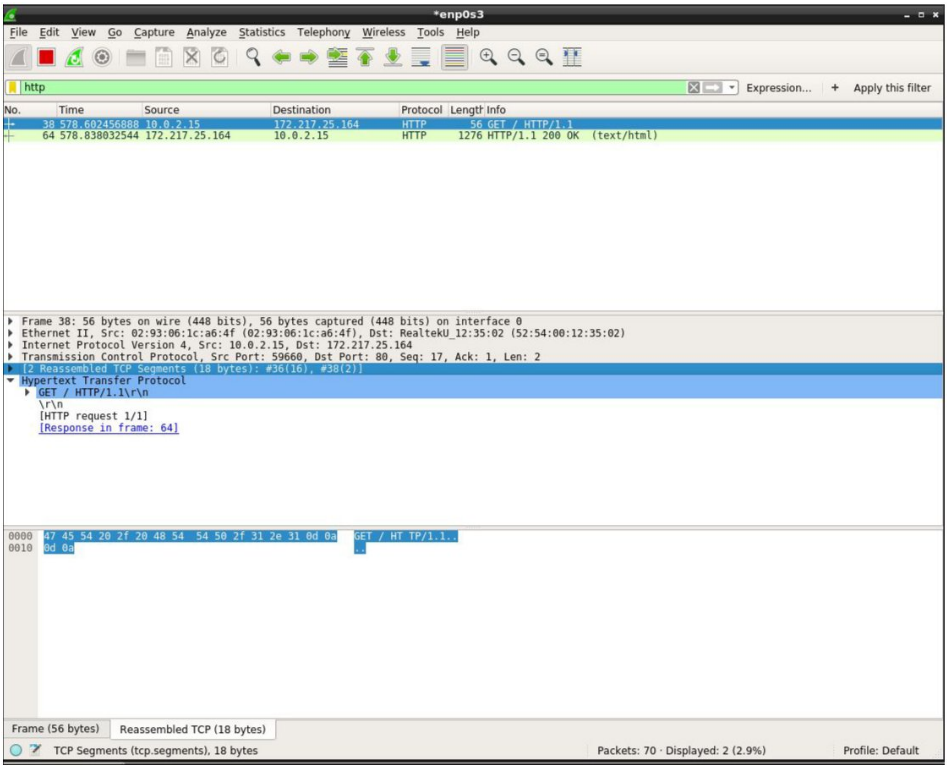

Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Frame (433 bytes)
Reassembled TCP (4760 bytes)

```
No.   Time          Source          Destination     Protocol Length Info
   10 9.626450669   10.0.2.15       130.56.66.152   TCP        70 [TCP segment of a reassembled PDU]
   11 9.628049468   130.56.66.152   10.0.2.15       TCP        60 80 → 43816 [ACK] Seq=1 Ack=17 Win=65535 L…
   12 11.587099665  10.0.2.15       130.56.66.152   HTTP       56 GET / HTTP/1.1
   13 11.587284417  130.56.66.152   10.0.2.15       TCP        60 80 → 43816 [ACK] Seq=1 Ack=19 Win=65535 L…
   14 11.769708371  130.56.66.152   10.0.2.15       TCP      1442 [TCP segment of a reassembled PDU]
   15 11.769747432  10.0.2.15       130.56.66.152   TCP        54 43816 → 80 [ACK] Seq=19 Ack=1389 Win=3192…
   16 11.769904020  130.56.66.152   10.0.2.15       TCP      3047 [TCP segment of a reassembled PDU]
   17 11.769919700  10.0.2.15       130.56.66.152   TCP        54 43816 → 80 [ACK] Seq=19 Ack=4382 Win=3692…
   18 11.840324325  130.56.66.152   10.0.2.15       HTTP      433 HTTP/1.1 200 OK  (text/html)
   19 11.840363152  10.0.2.15       130.56.66.152   TCP        54 43816 → 80 [ACK] Seq=19 Ack=4761 Win=3976…
   20 16.890416511  130.56.66.152   10.0.2.15       TCP        60 80 → 43816 [FIN, ACK] Seq=4761 Ack=19 Win…
   21 16.890551096  10.0.2.15       130.56.66.152   TCP        54 43816 → 80 [FIN, ACK] Seq=19 Ack=4762 Win…
   22 16.890775768  130.56.66.152   10.0.2.15       TCP        60 80 → 43816 [ACK] Seq=4762 Ack=20 Win=6553…
```

```
▶ Frame 18: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: 02:44:03:e3:22:ab (02:44:03:e3:22:ab)
▶ Internet Protocol Version 4, Src: 130.56.66.152, Dst: 10.0.2.15
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 43816, Seq: 4382, Ack: 19, Len: 379
▶ [3 Reassembled TCP Segments (4760 bytes): #14(1388), #16(2993), #18(379)]
▼ Hypertext Transfer Protocol
   ▶ HTTP/1.1 200 OK\r\n
     Server: nginx/1.12.0\r\n
     Content-Type: text/html; charset=utf-8\r\n
     X-Powered-By: PHP/7.0.20\r\n
     Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n
     Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0, no-store, no-cache, must-revalidate, post-check
     Content-Language: en\r\n
     X-Generator: Drupal 7 (http://drupal.org)\r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 53 65 72 76 65 72 3a  20 6e 67 69 6e 78 2f 31   .Server:  nginx/1
0020  2e 31 32 2e 30 0d 0a 43  6f 6e 74 65 6e 74 2d 54   .12.0..C ontent-T
0030  79 70 65 3a 20 74 65 78  74 2f 68 74 6d 6c 3b 20   ype: tex t/html;
0040  63 68 61 72 73 65 74 3d  75 74 66 2d 38 0d 0a 58   charset= utf-8..X
0050  2d 50 6f 77 65 72 65 64  2d 42 79 3a 20 50 48 50   -Powered -By: PHP
0060  2f 37 2e 30 2e 32 30 0d  0a 45 78 70 69 72 65 73   /7.0.20. .Expires
0070  3a 20 53 75 6e 2c 20 31  39 20 4e 6f 76 20 31 39   : Sun, 1 9 Nov 19
0080  37 38 20 30 35 3a 30 30  3a 30 30 20 47 4d 54 0d   78 05:00 :00 GMT.
0090  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20   .Cache-C ontrol:
00a0  6e 6f 2d 63 61 63 68 65  2c 20 6d 75 73 74 2d 72   no-cache , must-r
00b0  65 76 61 6c 69 64 61 74  65 2c 20 70 6f 73 74 2d   evalidat e, post-
00c0  63 68 65 63 6b 3d 30 2c  20 70 72 65 2d 63 68 65   check=0,  pre-che
```

```
Text item (text), 17 bytes        Packets: 22 · Displayed: 22 (100.0%)    Profile: Default
```



http

```
No.  Time            Source          Destination     Protocol Length Info
  38 578.602456888 10.0.2.15       172.217.25.164  HTTP       56 GET / HTTP/1.1
  64 578.838032544 172.217.25.164  10.0.2.15       HTTP     1276 HTTP/1.1 200 OK  (text/html)
```

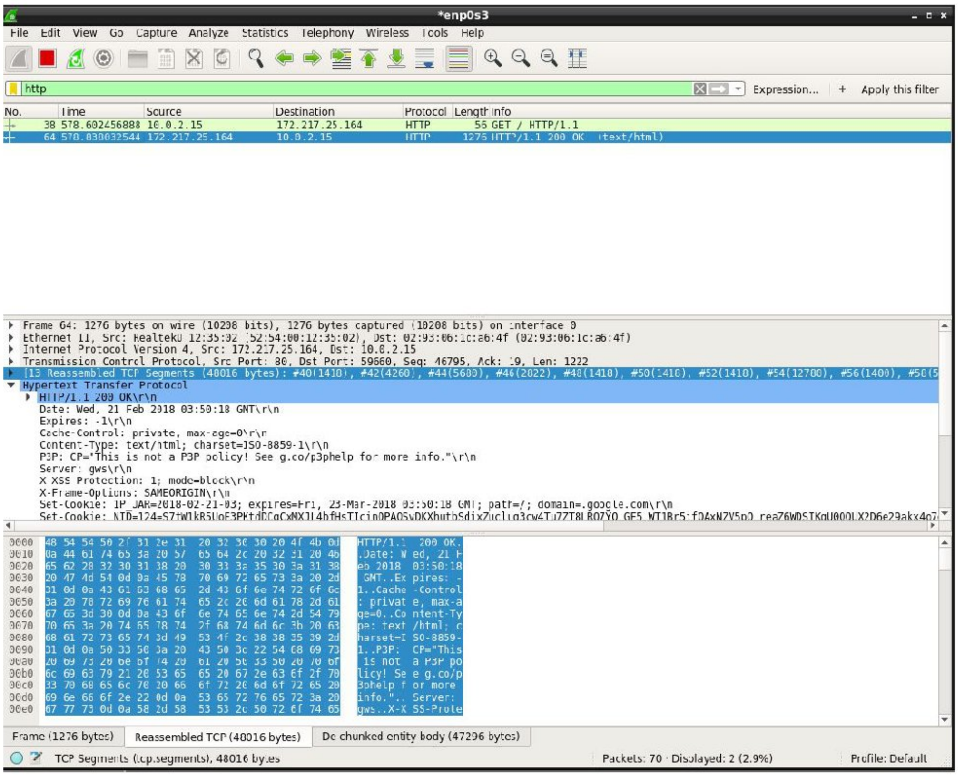
```
▸ Frame 38: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▸ Ethernet II, Src: 02:93:06:1c:a6:4f (02:93:06:1c:a6:4f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.25.164
▸ Transmission Control Protocol, Src Port: 59660, Dst Port: 80, Seq: 17, Ack: 1, Len: 2
▸ [2 Reassembled TCP Segments (18 bytes): #36(16), #38(2)]
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    \r\n
    [HTTP request 1/1]
    [Response in frame: 64]
```

```
0000  47 45 54 20 2f 20 48 54  54 50 2f 31 2e 31 0d 0a   GET / HT TP/1.1..
0010  0d 0a                                              ..
```

TCP Segments (tcp.segments), 18 bytes

Packets: 70 · Displayed: 2 (2.9%)

Profile: Default


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Apply this filter

```
http
```

```
No.  Time            Source          Destination     Protocol Length Info
  38 578.602456888   10.0.2.15       172.217.25.164  HTTP       56 GET / HTTP/1.1
  64 578.830032544   172.217.25.164  10.0.2.15       HTTP     1276 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 64: 1276 bytes on wire (10208 bits), 1276 bytes captured (10208 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: 02:93:06:1c:a6:4f (02:93:06:1c:a6:4f)
▸ Internet Protocol Version 4, Src: 172.217.25.164, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 59660, Seq: 46795, Ack: 19, Len: 1222
▸ [13 Reassembled TCP Segments (48016 bytes): #40(1410), #42(4260), #44(5680), #46(2022), #48(1410), #50(1410), #52(1410), #54(12700), #56(1400), #58(5
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 21 Feb 2018 03:50:18 GMT\r\n
    Expires: -1\r\n
    Cache-Control: private, max-age=0\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."\r\n
    Server: gws\r\n
    X-XSS-Protection: 1; mode=block\r\n
    X-Frame-Options: SAMEORIGIN\r\n
    Set-Cookie: 1P_JAR=2018-02-21-03; expires=Fri, 23-Mar-2018 03:50:18 GMT; path=/; domain=.google.com\r\n
    Set-Cookie: NID=124=S7tW1kR5UoE3PKtdDCqCxNXJL4bfHsTIcin0PAOSvDKXhutbSdixZuclin3cw4TuZ7T8LROZYQ_GE5_WT1Br5:fDAxNZV5pQ_reaZ6WDSIKqU000LX2D6e29akx4o7
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 32 31 20 46   .Date: W ed, 21 F
0020  65 62 20 32 30 31 38 20  30 33 3a 35 30 3a 31 38   eb 2018  03:50:18
0030  20 47 4d 54 0d 0a 45 78  70 69 72 65 73 3a 20 2d    GMT..Ex pires: -
0040  31 0d 0a 43 61 63 68 65  2d 43 6f 6e 74 72 6f 6c   1..Cache -Control
0050  3a 20 70 72 69 76 61 74  65 2c 20 6d 61 78 2d 61   : privat e, max-a
0060  67 65 3d 30 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   ge=0..Co ntent-Ty
0070  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 3b 20 63   pe: text /html; c
0080  68 61 72 73 65 74 3d 49  53 4f 2d 38 38 35 39 2d   harset=I SO-8859-
0090  31 0d 0a 50 33 50 3a 20  43 50 3d 22 54 68 69 73   1..P3P:  CP="This
00a0  20 69 73 20 6e 6f 74 20  61 20 50 33 50 20 70 6f    is not  a P3P po
00b0  6c 69 63 79 21 20 53 65  65 20 67 2e 63 6f 2f 70   licy! Se e g.co/p
00c0  33 70 68 65 6c 70 20 66  6f 72 20 6d 6f 72 65 20   3phelp f or more 
00d0  69 6e 66 6f 2e 22 0d 0a  53 65 72 76 65 72 3a 20   info.".. Server: 
00e0  67 77 73 0d 0a 58 2d 58  53 53 2d 50 72 6f 74 65   gws..X-X SS-Prote
```

Frame (1276 bytes)
Reassembled TCP (48016 bytes)
De chunked entity body (47296 bytes)
TCP Segments (tcp.segments), 48016 bytes
Packets: 70 · Displayed: 2 (2.9%)
Profile: Default

You may use the following commands in terminal to get Wireshark working in lab computers without making VMs.

xhost +si:localuser:root

sudo -i

sudo wireshark

A Client-Server in Action

Requirements

a) Linux virtual machine (Ubuntu Xenial 64bit). Try to run server on one ubuntu VM and client on another. For that you will have to specify server's IP when you run client from another machine. Screenshots below are from when both server and clients are running on the same VM.

b) JDK (Java Development Kit) for Ubuntu

Procedures

c) Install JDK (Java Development Kit); can be omitted if already installed.

$ sudo apt-get install default-jdk

$ java –version

openjdk version "1.8.0_151"

OpenJDK Runtime Environment (build 1.8.0_151-8u151-b12-0ubuntu0.16.04.2-b12)

OpenJDK 64-Bit Server VM (build 25.151-b12, mixed mode)

d) Download Client and Server code

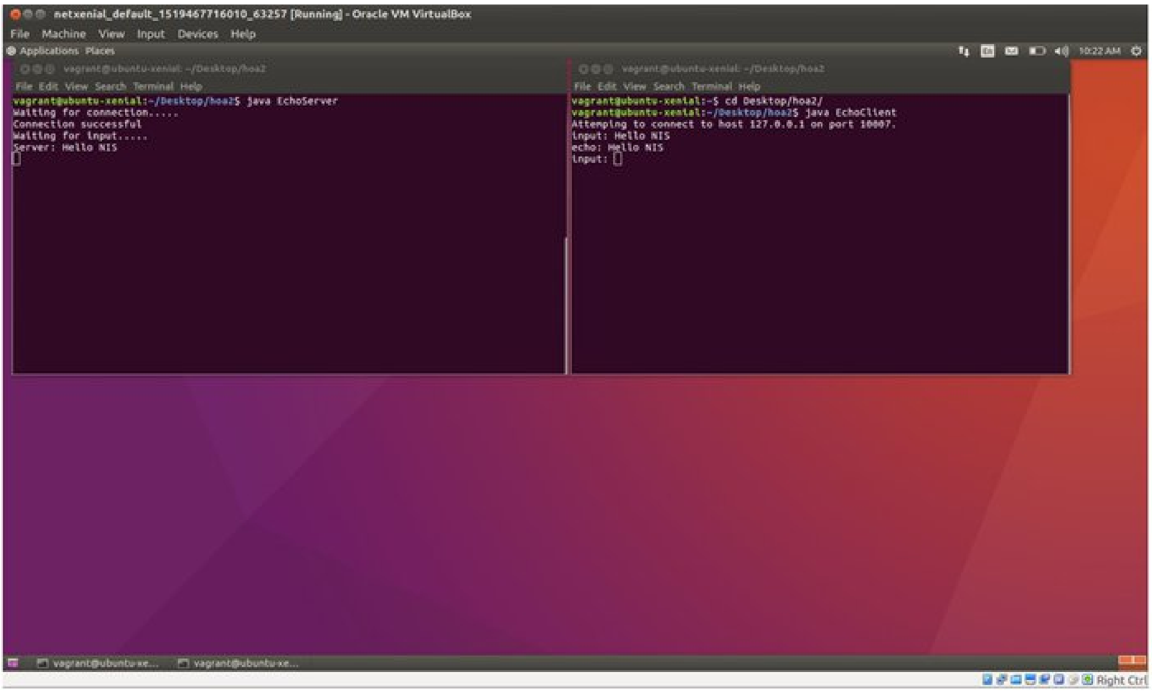
Link: https://www.cs.uic.edu/~troy/spring05/cs450/sockets/socket.html

e) Compile Client and Server

```
$ javac EchoClient.java
$ javac EchoServer.java
```

f) Run Server first and then Client, and look for the packets in Wireshark

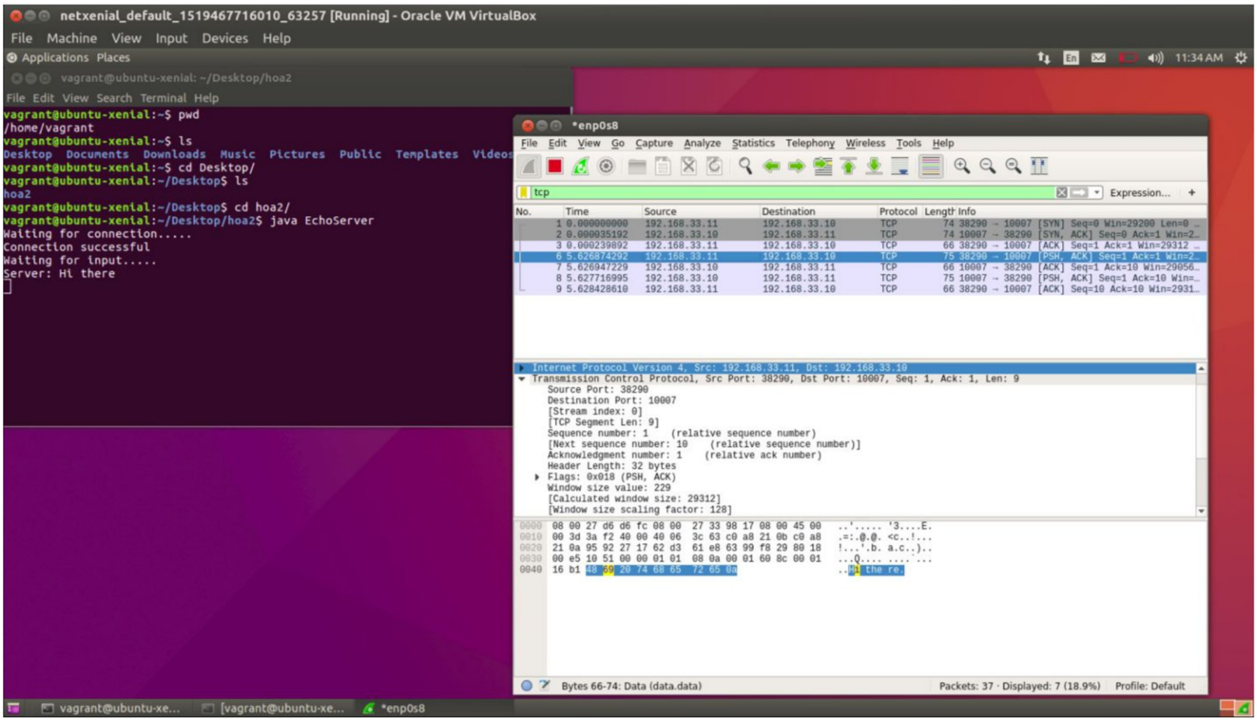
```
$ java EchoServer.java
$ java EchoClient.java
```


netxenial_default_1519467716010_63257 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
10:22 AM
vagrant@ubuntu-xenial: ~/Desktop/hoa2
File Edit View Search Terminal Help
vagrant@ubuntu-xenial: ~/Desktop/hoa2
File Edit View Search Terminal Help
vagrant@ubuntu-xe...
vagrant@ubuntu-xe...
Right Ctrl

```
vagrant@ubuntu-xenial:~/Desktop/hoa2$ java EchoServer
Waiting for connection.....
Connection successful
Waiting for input.....
Server: Hello NIS
```

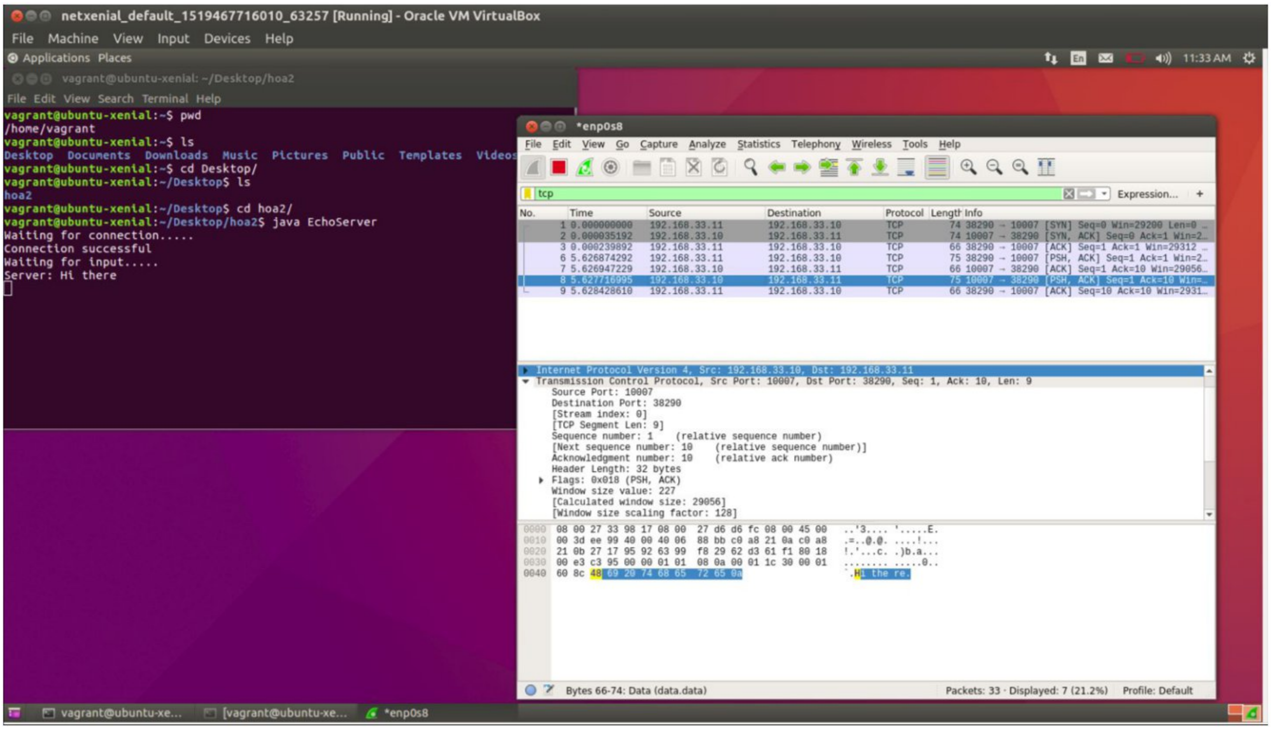
```
vagrant@ubuntu-xenial:~$ cd Desktop/hoa2/
vagrant@ubuntu-xenial:~/Desktop/hoa2$ java EchoClient
Attemping to connect to host 127.0.0.1 on port 10007.
input: Hello NIS
echo: Hello NIS
input:
```

- Client-Server on two IP addresses
  - ✓ A Client on 192.168.33.11
  - ✓ A Server on 192.168.33.10


netxenial_default_1519467716010_63257 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
11:34 AM
vagrant@ubuntu-xenial: ~/Desktop/hoa2
File Edit View Search Terminal Help
*enp0s8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
vagrant@ubuntu-xe...
[vagrant@ubuntu-xe...
*enp0s8

```
vagrant@ubuntu-xenial:~$ pwd
/home/vagrant
vagrant@ubuntu-xenial:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
vagrant@ubuntu-xenial:~$ cd Desktop/
vagrant@ubuntu-xenial:~/Desktop$ ls
hoa2
vagrant@ubuntu-xenial:~/Desktop$ cd hoa2/
vagrant@ubuntu-xenial:~/Desktop/hoa2$ java EchoServer
Waiting for connection.....
Connection successful
Waiting for input.....
Server: Hi there
```

```
tcp

No.  Time         Source         Destination    Protocol Length Info
   1 0.000000000  192.168.33.11  192.168.33.10  TCP      74 38290 → 10007 [SYN] Seq=0 Win=29200 Len=0 …
   2 0.000035192  192.168.33.10  192.168.33.11  TCP      74 10007 → 38290 [SYN, ACK] Seq=0 Ack=1 Win=2…
   3 0.000239892  192.168.33.11  192.168.33.10  TCP      66 38290 → 10007 [ACK] Seq=1 Ack=1 Win=29312 …
   6 5.626874292  192.168.33.11  192.168.33.10  TCP      75 38290 → 10007 [PSH, ACK] Seq=1 Ack=1 Win=2…
   7 5.626947229  192.168.33.10  192.168.33.11  TCP      66 10007 → 38290 [ACK] Seq=1 Ack=10 Win=29056…
   8 5.627716995  192.168.33.10  192.168.33.11  TCP      75 10007 → 38290 [PSH, ACK] Seq=1 Ack=10 Win=…
   9 5.628428610  192.168.33.11  192.168.33.10  TCP      66 38290 → 10007 [ACK] Seq=10 Ack=10 Win=2931…

▸ Internet Protocol Version 4, Src: 192.168.33.11, Dst: 192.168.33.10
▾ Transmission Control Protocol, Src Port: 38290, Dst Port: 10007, Seq: 1, Ack: 1, Len: 9
    Source Port: 38290
    Destination Port: 10007
    [Stream index: 0]
    [TCP Segment Len: 9]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 10    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 229
    [Calculated window size: 29312]
    [Window size scaling factor: 128]

0000  08 00 27 d6 d6 fc 08 00  27 33 98 17 08 00 45 00   ..'..... '3....E.
0010  00 3d 3a f2 40 00 40 06  3c 63 c0 a8 21 0b c0 a8   .=:.@.@. <c..!...
0020  21 0a 95 92 27 17 62 d3  61 e8 63 99 f8 29 80 18   !...'.b. a.c..)..
0030  00 e5 10 51 00 00 01 01  08 0a 00 01 60 8c 00 01   ...Q.... ....`...
0040  16 b1 48 69 20 74 68 65  72 65 0a                  ..Hi the re.

Bytes 66-74: Data (data.data)          Packets: 37 · Displayed: 7 (18.9%)     Profile: Default
```


netxenial_default_1519467716010_63257 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
11:33 AM
vagrant@ubuntu-xenial: ~/Desktop/hoa2
File Edit View Search Terminal Help
*enp0s8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
vagrant@ubuntu-xe...
[vagrant@ubuntu-xe...
*enp0s8

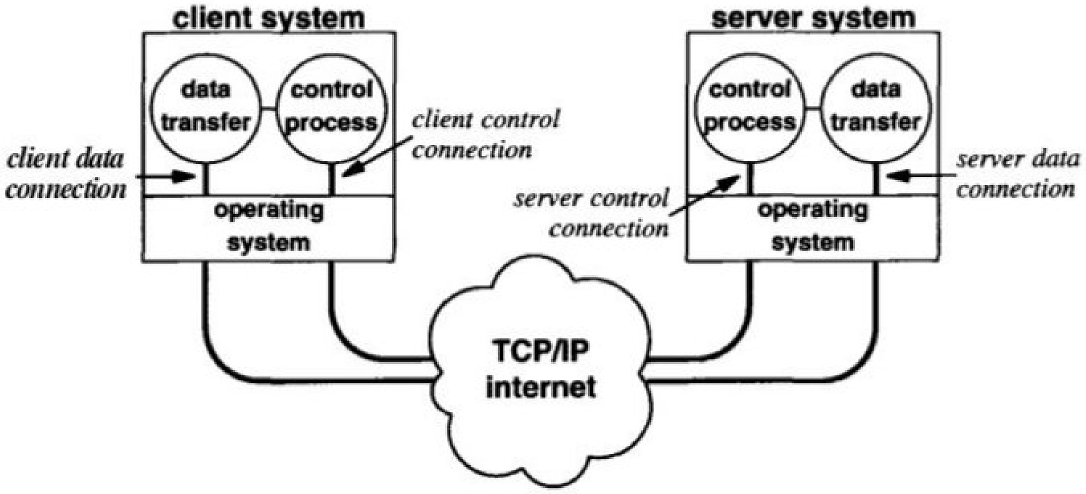
```
vagrant@ubuntu-xenial:~$ pwd
/home/vagrant
vagrant@ubuntu-xenial:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
vagrant@ubuntu-xenial:~$ cd Desktop/
vagrant@ubuntu-xenial:~/Desktop$ ls
hoa2
vagrant@ubuntu-xenial:~/Desktop$ cd hoa2/
vagrant@ubuntu-xenial:~/Desktop/hoa2$ java EchoServer
Waiting for connection.....
Connection successful
Waiting for input.....
Server: Hi there
```

```
tcp

No.  Time         Source         Destination    Protocol Length Info
   1 0.000000000  192.168.33.11  192.168.33.10  TCP      74 38290 → 10007 [SYN] Seq=0 Win=29200 Len=0 …
   2 0.000035192  192.168.33.10  192.168.33.11  TCP      74 10007 → 38290 [SYN, ACK] Seq=0 Ack=1 Win=2…
   3 0.000239892  192.168.33.11  192.168.33.10  TCP      66 38290 → 10007 [ACK] Seq=1 Ack=1 Win=29312 …
   6 5.626874292  192.168.33.11  192.168.33.10  TCP      75 38290 → 10007 [PSH, ACK] Seq=1 Ack=1 Win=2…
   7 5.626947229  192.168.33.10  192.168.33.11  TCP      66 10007 → 38290 [ACK] Seq=1 Ack=10 Win=29056…
   8 5.627716995  192.168.33.10  192.168.33.11  TCP      75 10007 → 38290 [PSH, ACK] Seq=1 Ack=10 Win=…
   9 5.628428610  192.168.33.11  192.168.33.10  TCP      66 38290 → 10007 [ACK] Seq=10 Ack=10 Win=2931…

▸ Internet Protocol Version 4, Src: 192.168.33.10, Dst: 192.168.33.11
▾ Transmission Control Protocol, Src Port: 10007, Dst Port: 38290, Seq: 1, Ack: 10, Len: 9
    Source Port: 10007
    Destination Port: 38290
    [Stream index: 0]
    [TCP Segment Len: 9]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 10    (relative sequence number)]
    Acknowledgment number: 10    (relative ack number)
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 227
    [Calculated window size: 29056]
    [Window size scaling factor: 128]

0000  08 00 27 33 98 17 08 00  27 d6 d6 fc 08 00 45 00   ..'3.... '.....E.
0010  00 3d ee 99 40 00 40 06  88 bb c0 a8 21 0a c0 a8   .=..@.@. ....!...
0020  21 0b 27 17 95 92 63 99  f8 29 62 d3 61 f1 80 18   !.'...c. .)b.a...
0030  00 e3 c3 95 00 00 01 01  08 0a 00 01 1c 30 00 01   ........ .....0..
0040  60 8c 48 69 20 74 68 65  72 65 0a                  `.Hi the re.

Bytes 66-74: Data (data.data)          Packets: 33 · Displayed: 7 (21.2%)     Profile: Default
```

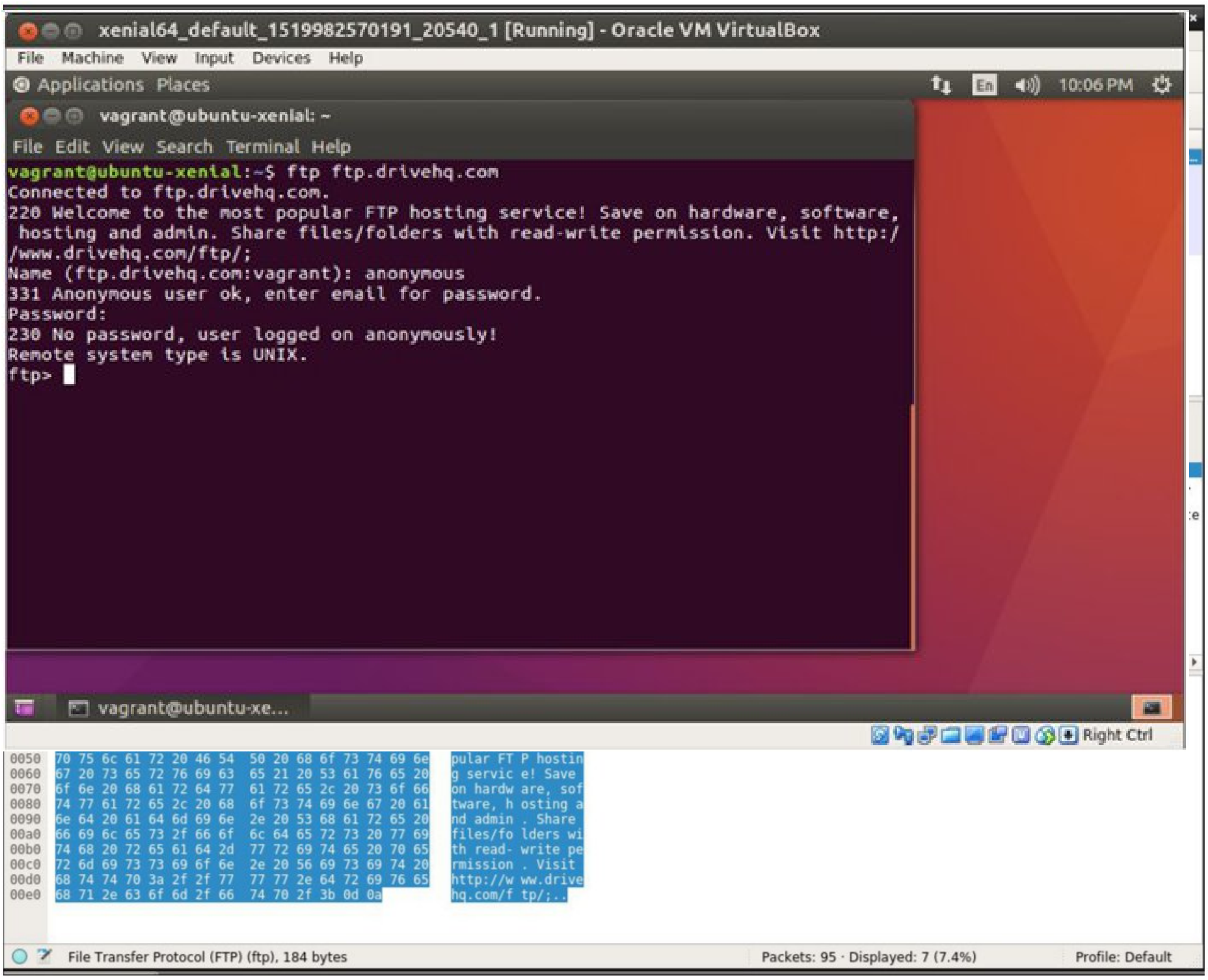
FTP at the Application Layer

Requirements

a) Linux virtual machine (Ubuntu Xenial 64bit)
b) Wireshark on Ubuntu
c) ftp client on Ubuntu



FTP client on Ubuntu VM



xenial64_default_1519982570191_20540_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
En
10:06 PM
vagrant@ubuntu-xenial: ~
File Edit View Search Terminal Help
vagrant@ubuntu-xe...
Right Ctrl

```
vagrant@ubuntu-xenial:~$ ftp ftp.drivehq.com
Connected to ftp.drivehq.com.
220 Welcome to the most popular FTP hosting service! Save on hardware, software,
 hosting and admin. Share files/folders with read-write permission. Visit http:/
/www.drivehq.com/ftp/;
Name (ftp.drivehq.com:vagrant): anonymous
331 Anonymous user ok, enter email for password.
Password:
230 No password, user logged on anonymously!
Remote system type is UNIX.
ftp> 
```

```
0050  70 75 6c 61 72 20 46 54  50 20 68 6f 73 74 69 6e   pular FT P hostin
0060  67 20 73 65 72 76 69 63  65 21 20 53 61 76 65 20   g servic e! Save 
0070  6f 6e 20 68 61 72 64 77  61 72 65 2c 20 73 6f 66   on hardw are, sof
0080  74 77 61 72 65 2c 20 68  6f 73 74 69 6e 67 20 61   tware, h osting a
0090  6e 64 20 61 64 6d 69 6e  2e 20 53 68 61 72 65 20   nd admin . Share 
00a0  66 69 6c 65 73 2f 66 6f  6c 64 65 72 73 20 77 69   files/fo lders wi
00b0  74 68 20 72 65 61 64 2d  77 72 69 74 65 20 70 65   th read- write pe
00c0  72 6d 69 73 73 69 6f 6e  2e 20 56 69 73 69 74 20   rmission . Visit 
00d0  68 74 74 70 3a 2f 2f 77  77 77 2e 64 72 69 76 65   http://w ww.drive
00e0  68 71 2e 63 6f 6d 2f 66  74 70 2f 3b 0d 0a         hq.com/f tp/;..
```

File Transfer Protocol (FTP) (ftp), 184 bytes

Packets: 95 · Displayed: 7 (7.4%)

Profile: Default

Reflective Questions

a) What are the insights of using Wireshark?
b) Please list and compare among 10 network packet analysers including Wireshark.
c) What are the reasons to pair between client and server?