

Pedro Ruelas

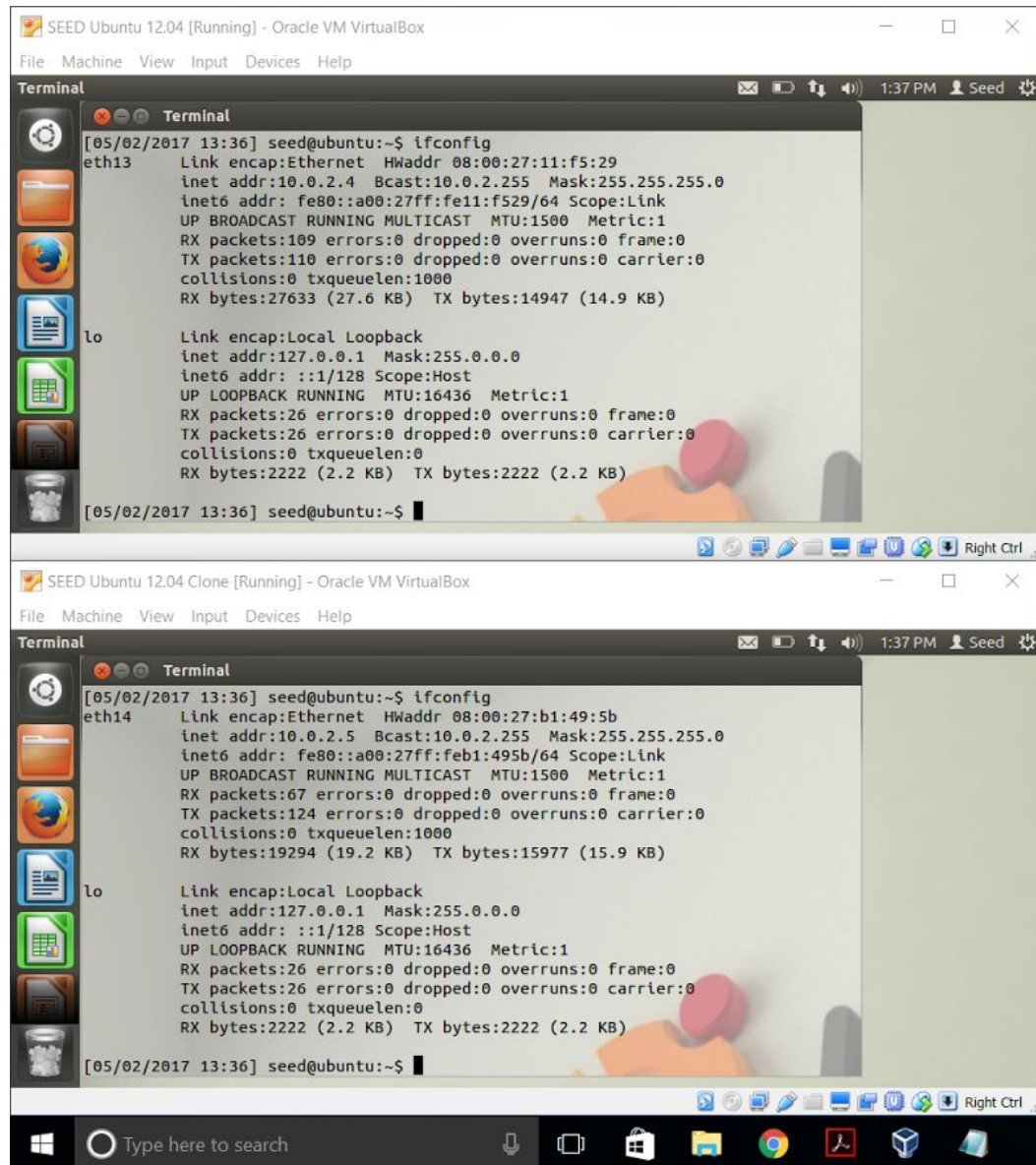
[https://github.com/pruelas/Exercise\\_5](https://github.com/pruelas/Exercise_5)

## Exercise 5

### 3.1 Problem 1: Verifying the Network

Output for terminal command:

\$ ifconfig



```
[05/02/2017 13:36] seed@ubuntu:~$ ifconfig
eth13      Link encap:Ethernet  HWaddr 08:00:27:11:f5:29
            inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe11:f529/64  Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:109 errors:0 dropped:0 overruns:0 frame:0
            TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:27633 (27.6 KB)  TX bytes:14947 (14.9 KB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128  Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:26 errors:0 dropped:0 overruns:0 frame:0
            TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:2222 (2.2 KB)  TX bytes:2222 (2.2 KB)

[05/02/2017 13:36] seed@ubuntu:~$
```

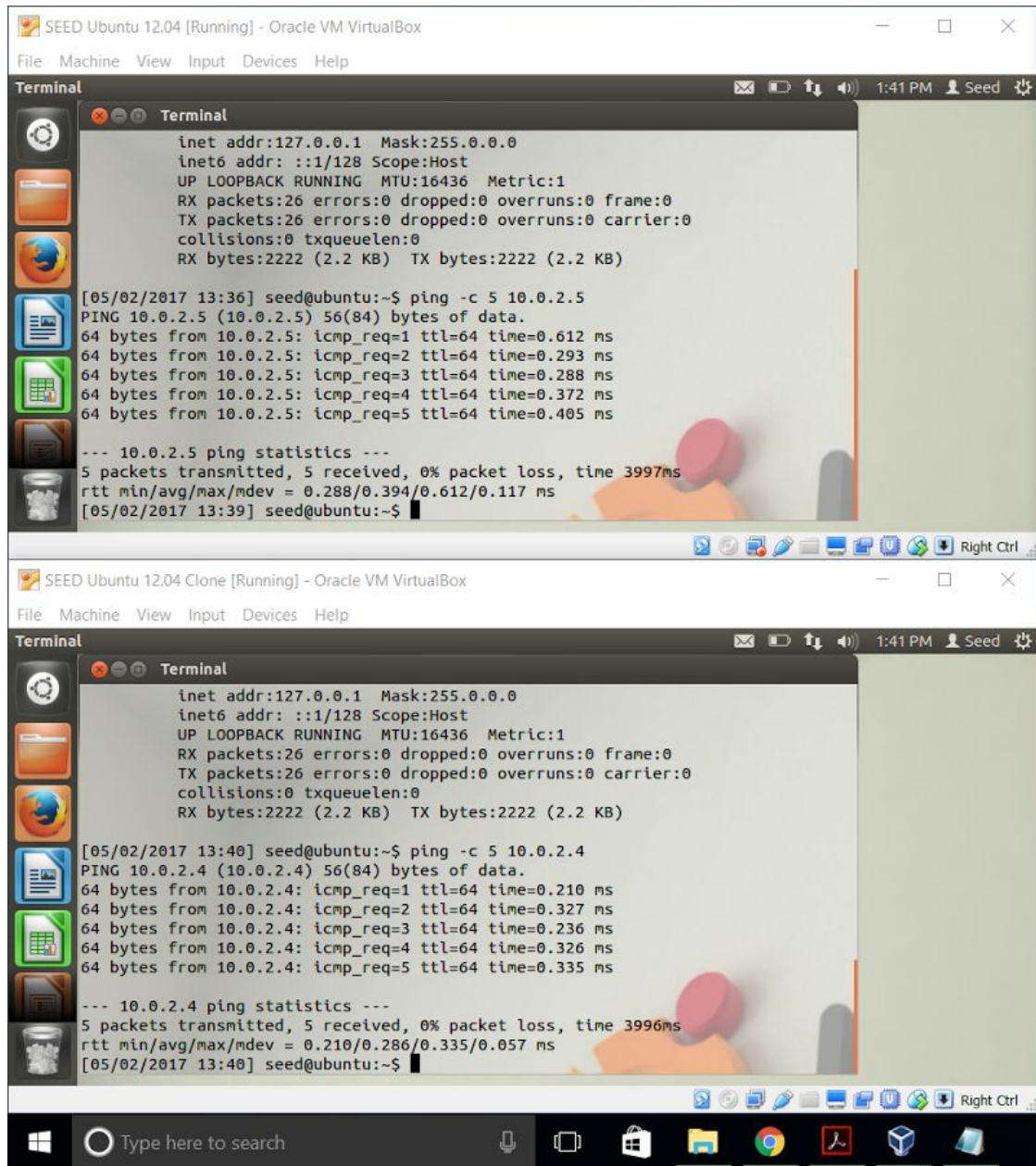
```
[05/02/2017 13:36] seed@ubuntu:~$ ifconfig
eth14      Link encap:Ethernet  HWaddr 08:00:27:b1:49:5b
            inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:feb1:495b/64  Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:67 errors:0 dropped:0 overruns:0 frame:0
            TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:19294 (19.2 KB)  TX bytes:15977 (15.9 KB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128  Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:26 errors:0 dropped:0 overruns:0 frame:0
            TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:2222 (2.2 KB)  TX bytes:2222 (2.2 KB)

[05/02/2017 13:36] seed@ubuntu:~$
```

Output for terminal command:

\$ ping -c 5 x.x.x.x



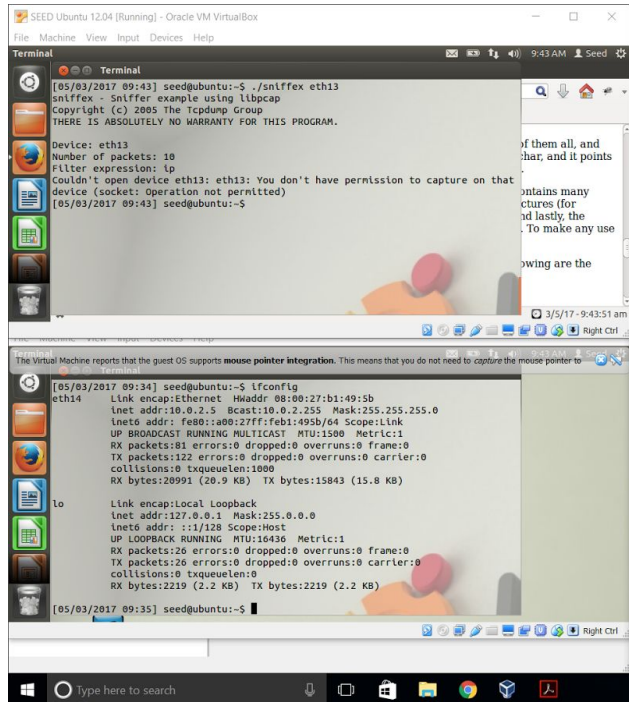
### 3.2 Problem 2: Writing a Packet Sniffer

#### Summary of the PCAP Library

- The pcap library is used to view the traffic that is passing on an interface. One must inform the pcap on which device it will be viewing the traffic and inform what types of traffic it will be viewing. After running the pcap, it will view the traffic until it has received a set amount of packets specified by the user.

After terminal command:

`$.sniffex eth13`



```
[05/03/2017 09:43] seed@ubuntu:~$ ./sniffex eth13
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth13
Number of packets: 10
Filter expression: ip
couldn't open device eth13: You don't have permission to capture on that
device (socket: Operation not permitted)
[05/03/2017 09:43] seed@ubuntu:~$

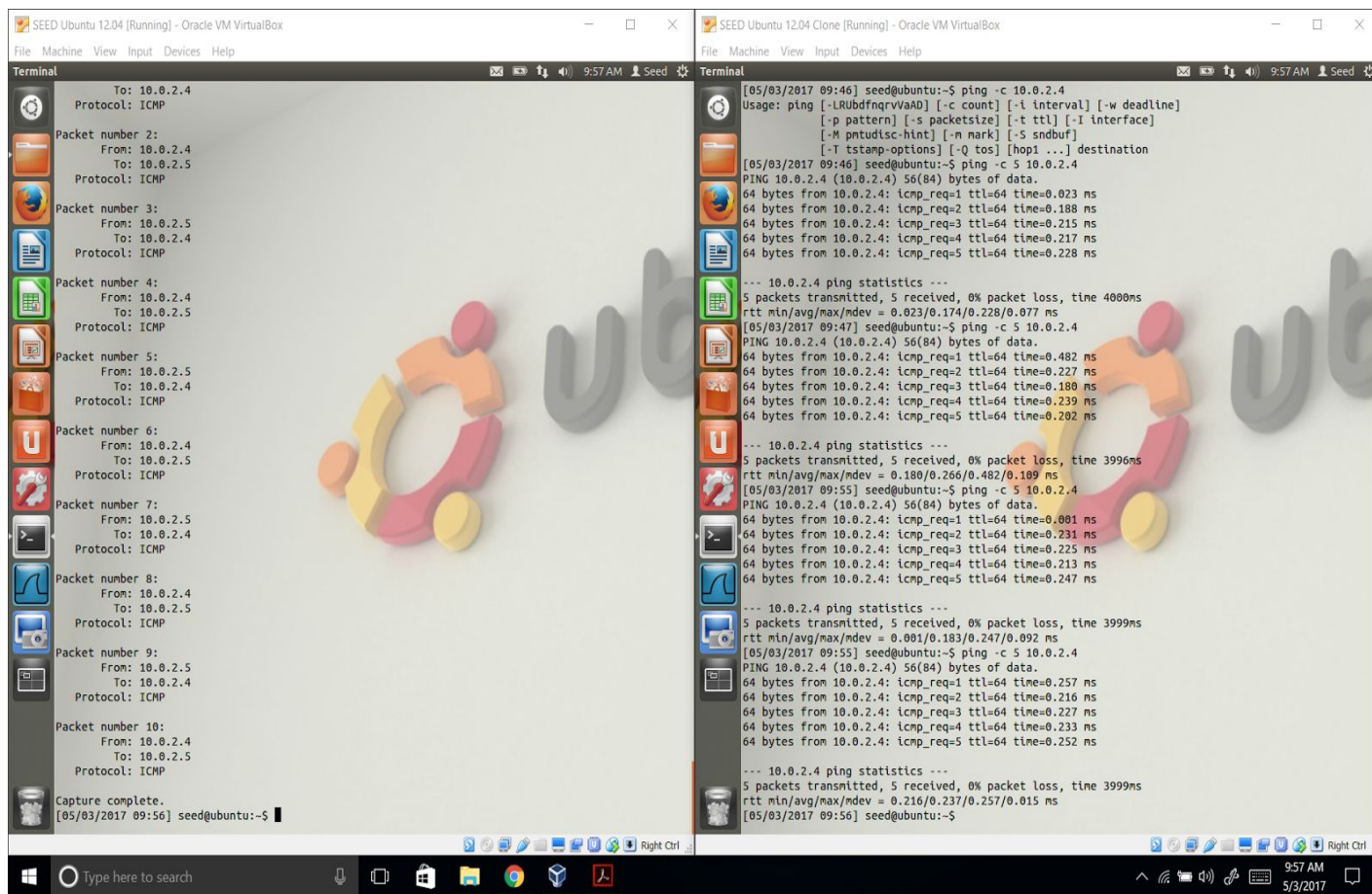
[05/03/2017 09:34] seed@ubuntu:~$ ifconfig
eth14
Link encap:Ethernet  HWaddr 08:00:27:b1:49:5b
inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:feb1:495b/64 Scope:link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:81 errors:0 dropped:0 overruns:0 frame:0
TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20991 (20.9 KB)  TX bytes:15043 (15.8 KB)

lo
Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:16436  Metric:1
RX packets:26 errors:0 dropped:0 overruns:0 frame:0
TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2219 (2.2 KB)  TX bytes:2219 (2.2 KB)

[05/03/2017 09:35] seed@ubuntu:~$
```



Results for running the sniffer program in the first machine and pinging from the second.



The image shows two side-by-side terminal windows from a VM. The left window displays a packet capture of ICMP ping requests from 10.0.2.4 to 10.0.2.5. The right window shows the execution of the 'sniffex' program, which captures and displays the same ICMP traffic, including packet details and ping statistics.

```
SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
To: 10.0.2.4
Protocol: ICMP
Packet number 2:
From: 10.0.2.4
To: 10.0.2.5
Protocol: ICMP
Packet number 3:
From: 10.0.2.5
To: 10.0.2.4
Protocol: ICMP
Packet number 4:
From: 10.0.2.4
To: 10.0.2.5
Protocol: ICMP
Packet number 5:
From: 10.0.2.5
To: 10.0.2.4
Protocol: ICMP
Packet number 6:
From: 10.0.2.4
To: 10.0.2.5
Protocol: ICMP
Packet number 7:
From: 10.0.2.5
To: 10.0.2.4
Protocol: ICMP
Packet number 8:
From: 10.0.2.4
To: 10.0.2.5
Protocol: ICMP
Packet number 9:
From: 10.0.2.5
To: 10.0.2.4
Protocol: ICMP
Packet number 10:
From: 10.0.2.4
To: 10.0.2.5
Protocol: ICMP
Capture complete.
[05/03/2017 09:56] seedubuntu:~$

SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[05/03/2017 09:46] seedubuntu:~$ ping -c 10 10.0.2.4
Usage: ping [-LrUbfqrvVaAD] [-c count] [-i interval] [-w deadline]
[-p pattern] [-s packetsize] [-t ttl] [-I interface]
[-M pmtudisc-hint] [-m mark] [-S sndbuf]
[-T tstamp-options] [-Q tos] [hop1 ...] destination
[05/03/2017 09:46] seedubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.023 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.188 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.215 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.217 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.228 ms

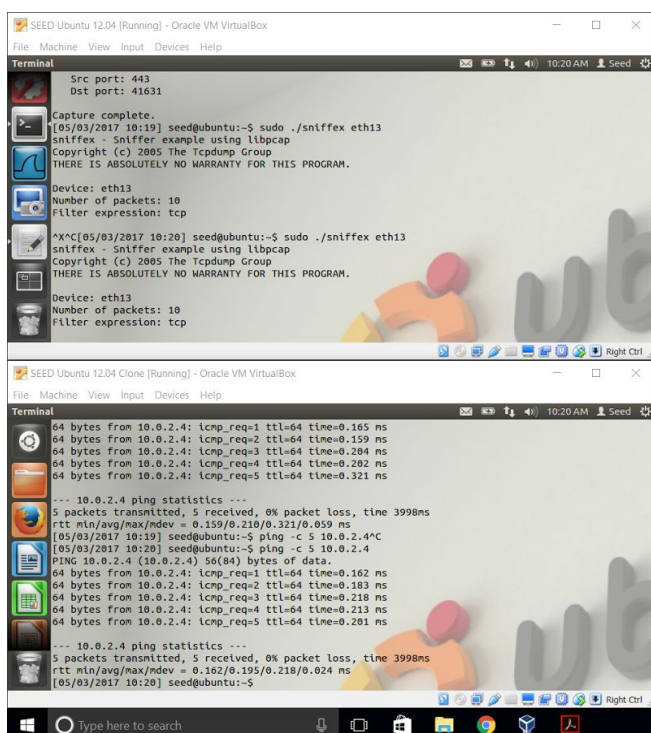
--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.023/0.174/0.228/0.077 ms
[05/03/2017 09:47] seedubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.482 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.227 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.180 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.239 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.202 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.180/0.266/0.482/0.109 ms
[05/03/2017 09:55] seedubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.001 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.231 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.225 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.213 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.247 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.001/0.183/0.247/0.092 ms
[05/03/2017 09:55] seedubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.257 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.216 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.227 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.233 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.252 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.216/0.237/0.257/0.015 ms
[05/03/2017 09:56] seedubuntu:~$
```

After modifying the filter in the packet sniffer source code so that it captures TCP packets, the pings from the second machined are not being captured by the machine running the sniffer.



The image shows two side-by-side terminal windows. The top window shows the execution of 'sniffex' with a filter expression of 'tcp'. The bottom window shows the execution of 'sniffex' with a filter expression of 'tcp' and the resulting capture of TCP traffic from 10.0.2.4 to 10.0.2.5.

```
SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Src port: 443
Dst port: 41631
Capture complete.
[05/03/2017 10:19] seedubuntu:~$ sudo ./sniffex eth13
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.
Device: eth13
Number of packets: 10
Filter expression: tcp
^X^C[05/03/2017 10:20] seedubuntu:~$ sudo ./sniffex eth13
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.
Device: eth13
Number of packets: 10
Filter expression: tcp

SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.165 ns
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.159 ns
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.183 ns
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.202 ns
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.321 ns

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.159/0.210/0.321/0.059 ns
[05/03/2017 10:19] seedubuntu:~$ ping -c 5 10.0.2.4
[05/03/2017 10:20] seedubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data:
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.162 ns
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.183 ns
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.218 ns
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.213 ns
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.201 ns

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.162/0.195/0.218/0.024 ns
[05/03/2017 10:20] seedubuntu:~$
```

### 3.3 Problem 3: Password Sniffing

After running the terminal command below on the first machine

```
$ sudo service openssh-sftp-server start
```

And using the terminal command below on the second machine

```
$ telnet 10.0.2.4
```

I logged from the second machine into the first and created a text file called "test.txt." After logging out, the text file was present on the first machine.

The image consists of two screenshots of a VirtualBox window showing two Ubuntu 12.04 VMs. The top window, titled 'SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox', shows a terminal session where the user 'seed' runs 'sudo service openssh-sftp-server start' and then 'ls' in the Desktop directory. The output of 'ls' shows various files including 'openssl-1.0.1', 'sniffex.c', and 'test.txt'. The bottom window, titled 'SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox', shows a terminal session where the user 'seed' runs 'cd Desktop', 'vi test.txt', 'ls', and 'exit'. The output of 'ls' shows the same files as the top window, including 'test.txt'. The bottom window also shows a Windows taskbar at the bottom with a search bar and several application icons.

```
SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox
Terminal
00336 ef 4b 60 5d fe c3 6c 7a 5f 0e ee 40 c5 35 1d 0b .K'..lz_..@.5..
00352 b5 39 89 de 85 06 f4 f3 9c a0 43 a6 31 f5 c3 03 .9.....C.1...
00368 6c 5d bf 0a af 3a e5 2a da d0 b2 0c d4 9a 75 d7 l]...*......u.
00384 68 fc 44 29 f1 8a 9d b8 2d f5 85 ac 6c 5b 9a 50 h.D).....l[P
00400 5a 30 cd b9 e9 4d ed 8d 26 4e 64 29 31 53 78 d5 Z0..M.&Nd)1Sx.
00416 1f 23 44 48 7b 34 ed df 5f bd 02 d4 33 e7 d5 b1 .#DH{4.....3...
00432 45 34 dd 08 64 4e c7 84 27 0a e9 e0 73 b2 20 8d E4.dN.....S.
00448 30 b4 c3 29 b1 8f ff 16 03 03 00 04 0e 00 00 00 0..).....

Capture complete.
[05/03/2017 10:20] seed@ubuntu:~$ sudo service openssh-sftp-server start
* Starting internet sftpserver inetd
[05/03/2017 10:23] seed@ubuntu:~$ ls
Desktop          Music             Pictures          sniffex.c-
Documents         openssl-1.0.1     Public            Templates
Downloads         openssl_1.0.1-4ubuntu5.11.debian.tar.gz  sniffex
elggData          openssl_1.0.1-4ubuntu5.11.dsc             sniffex
examples.desktop openssl_1.0.1.orig.tar.gz                 sniffex.c
[05/03/2017 10:27] seed@ubuntu:~$ cd Desktop
[05/03/2017 10:27] seed@ubuntu:~/Desktop$ ls
sniffex.desktop  sniffex.desktop  libcap2.22  Netwag.desktop  Pacgen-1.10  test.txt  WireShark.desktop
[05/03/2017 10:27] seed@ubuntu:~/Desktop$

SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox
Terminal
* Documentation: https://help.ubuntu.com/

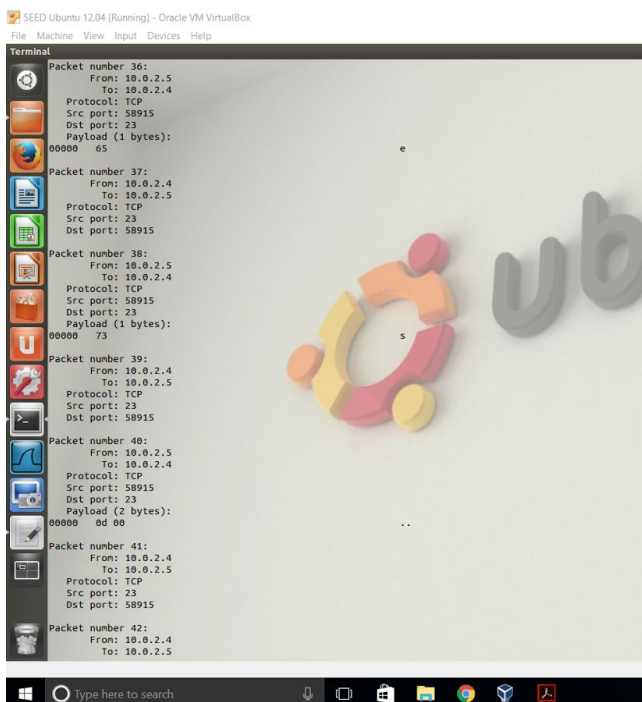
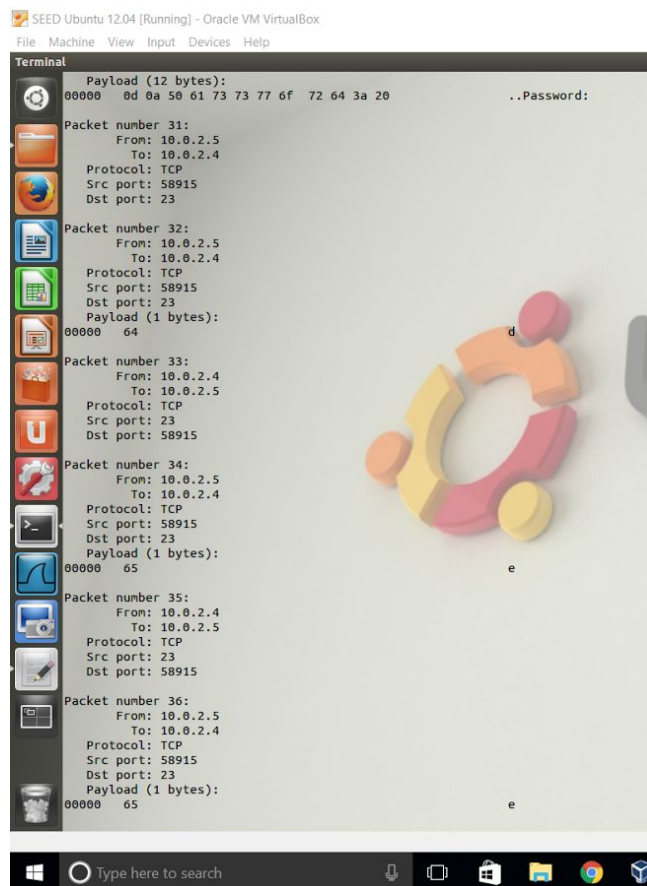
New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[05/03/2017 10:24] seed@ubuntu:~$ cd Desktop
[05/03/2017 10:24] seed@ubuntu:~/Desktop$ vi test.txt
[05/03/2017 10:26] seed@ubuntu:~/Desktop$ ls
sniffex.desktop  sniffex.desktop  libcap2.22  Netwag.desktop  Pacgen-1.10  test.txt  WireShark.desktop
[05/03/2017 10:26] seed@ubuntu:~/Desktop$ exit
logout
Connection closed by foreign host.
[05/03/2017 10:27] seed@ubuntu:~$
```

Trying to find the password of the user logging in.  
The password was visible.



### Using Wireshark

- When using wireshark instead of my own packet sniffer, I am still able to locate the user's password by looking at the telnet data segments present in wireshark.

After these experiments it appears that using telnet as a method of remotely accessing a system is not secure and should be avoided since the password of a user can be retrieved without much difficulty.

### 3.4 Problem 4: SSH

When using SSH to login to the first virtual machine, I am unable to find the password entered at the second virtual machine through wireshark. When one looks through the packets, it appears impossible to determine the password.