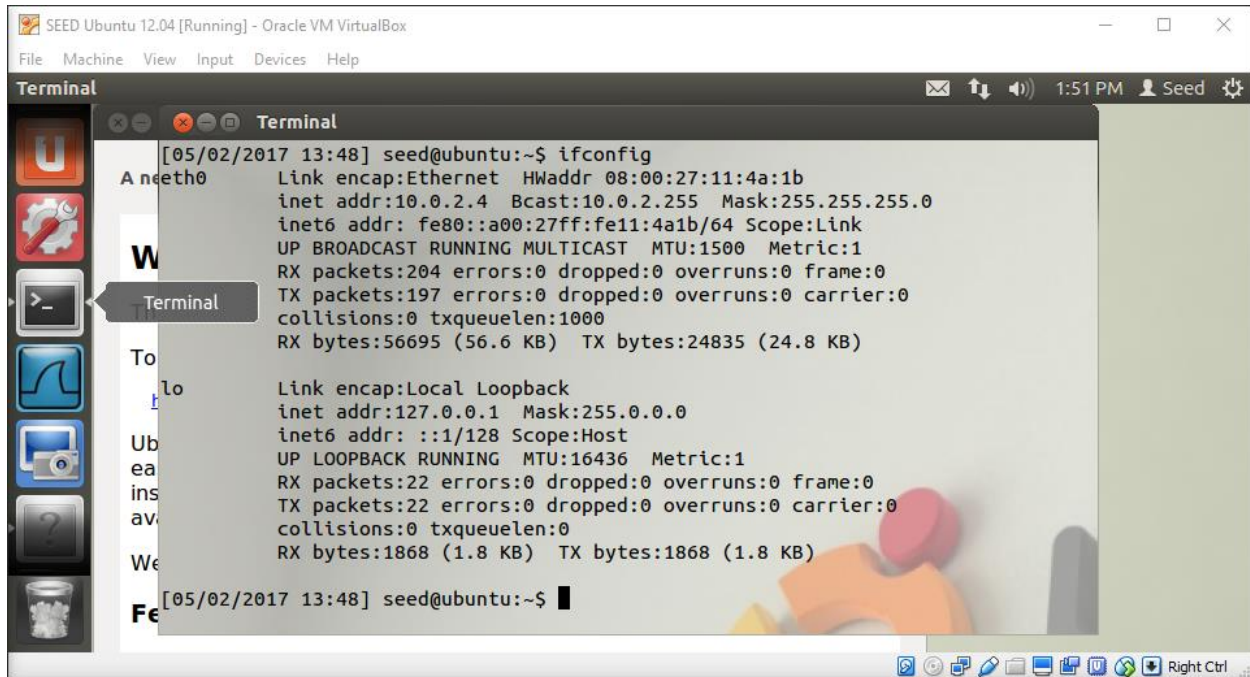


Michael Acosta

<https://github.com/m-acosta/cs380-exercise5>

Problem 1



SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

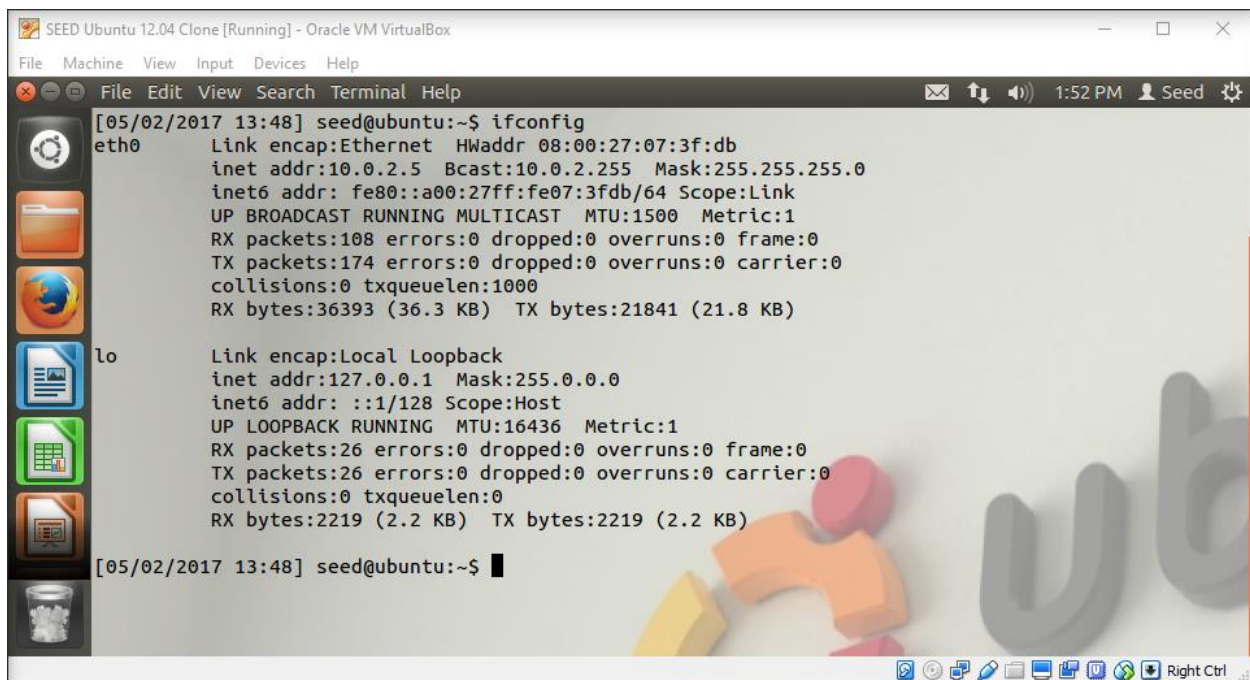
Terminal

1:51 PM Seed

```
[05/02/2017 13:48] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:4a:1b
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:4a1b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:204 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:56695 (56.6 KB)  TX bytes:24835 (24.8 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:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1868 (1.8 KB)  TX bytes:1868 (1.8 KB)

[05/02/2017 13:48] seed@ubuntu:~$
```



SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox

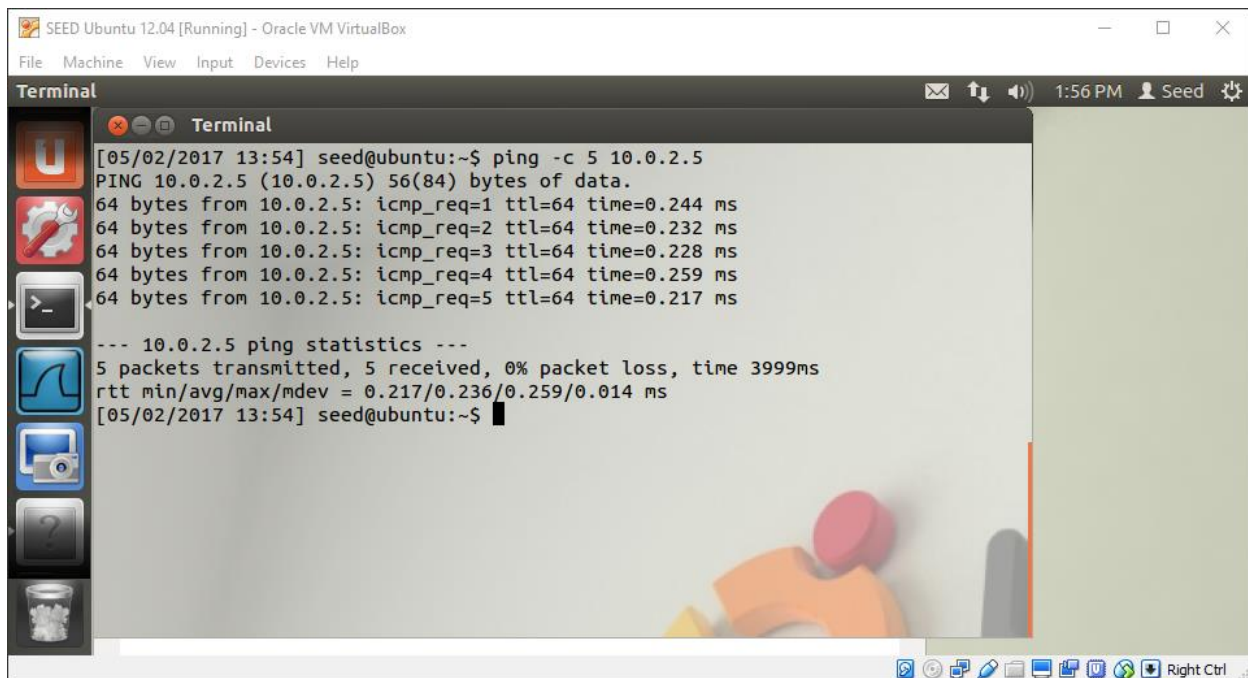
File Edit View Search Terminal Help

1:52 PM Seed

```
[05/02/2017 13:48] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:07:3f:db
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe07:3fdb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:174 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36393 (36.3 KB)  TX bytes:21841 (21.8 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)

[05/02/2017 13:48] seed@ubuntu:~$
```



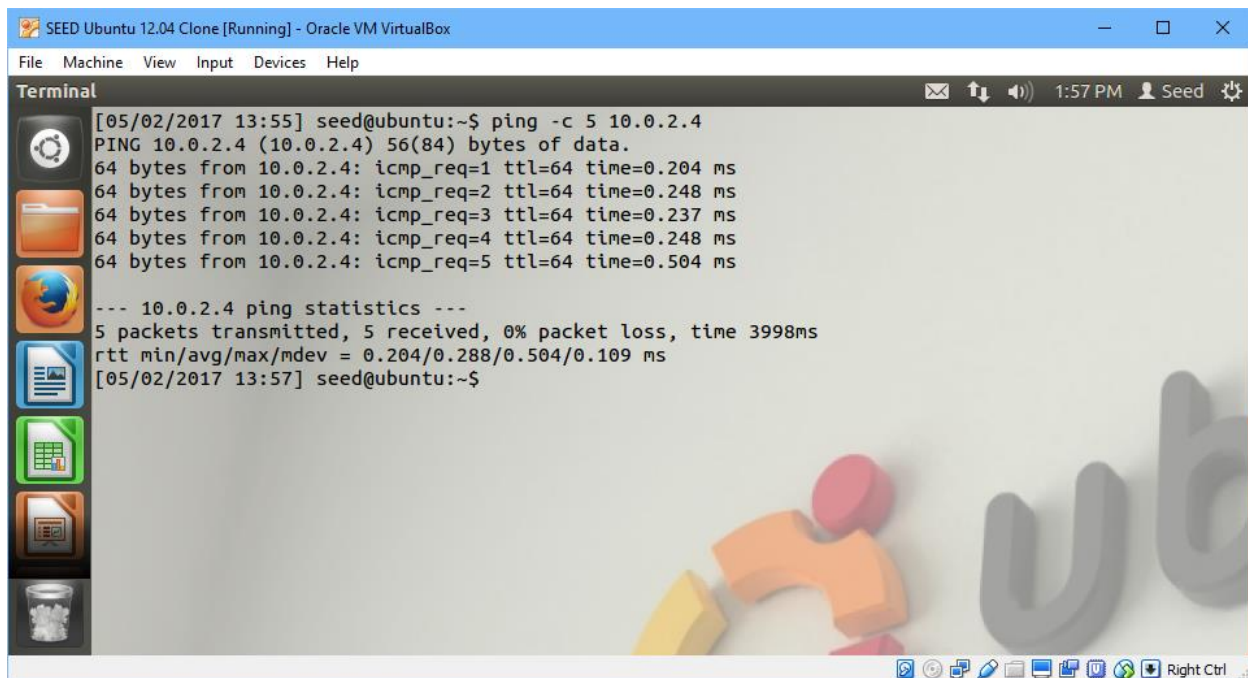
SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[05/02/2017 13:54] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.244 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.232 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.228 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.259 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.217 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.217/0.236/0.259/0.014 ms
[05/02/2017 13:54] seed@ubuntu:~$
```



SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[05/02/2017 13:55] seed@ubuntu:~$ 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=0.204 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.248 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.237 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.248 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.504 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.204/0.288/0.504/0.109 ms
[05/02/2017 13:57] seed@ubuntu:~$
```

Problem 2

The interface on which to sniff is specified by the string in the command line, and that is initialized with pcap. Each time the sniffer is run, it has a different file handle to differentiate between devices and runs. The type of traffic can be set with a filter, and then handled with the

pcap compiler. In the main execution loop, pcap will wait for packets (specified by the filter) and that packet is printed to the user in a manner they can see.

When running the `./sniffex ethX` command, it fails because it does not have permission to capture on that socket. The operation is not permitted.

```
SEED Ubuntu 12.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[05/02/2017 14:11] seed@ubuntu:~/Downloads$ sudo ./sniffex eth0
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth0
Number of packets: 10
Filter expression: ip

Packet number 1:
  From: 10.0.2.5
  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: 10.0.2.4
  To: 162.213.33.50
  Protocol: TCP
  Src port: 52013
  Dst port: 443

Packet number 4:
  From: 162.213.33.50
  To: 10.0.2.4
  Protocol: TCP
  Src port: 443
  Dst port: 52013

Packet number 5:
  From: 10.0.2.4
  To: 162.213.33.50
  Protocol: TCP
  Src port: 52013
  Dst port: 443

Packet number 6:
  From: 10.0.2.4
  To: 162.213.33.50
  Protocol: TCP
  Src port: 52013
  Dst port: 443

Payload (148 bytes):
0000  16 03 00 00 8f 01 00 00 8b 03 03 59 08 f6 64 d7  ....Y..d.
00016  bf d6 df ed e8 84 e7 05 8a 7f c9 d6 90 f6 46 ea  ....F...F.
00032  c0 2e dd fe c5 e2 cf e4 e9 46 c1 00 30 00 33     ....F...0.3
00048  00 87 00 45 00 39 00 0b 00 88 00 16 00 32 00 40  .g.f.9.k....2.@
00064  00 44 00 38 00 6a 00 87 00 13 00 66 00 2f 00 3c  .D.B.j....f./.<
```

```
SEED Ubuntu 12.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[05/02/2017 14:40] seed@ubuntu:~/Downloads$ sudo ./sniffex eth0
[sudo] password for seed:
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth0
Number of packets: 10
Filter expression: tcp

Packet number 1:
  From: 10.0.2.4
  To: 162.213.33.50
  Protocol: TCP
  Src port: 52070
  Dst port: 443

Packet number 2:
  From: 162.213.33.50
  To: 10.0.2.4
  Protocol: TCP
  Src port: 443
  Dst port: 52070

Packet number 3:
  From: 10.0.2.4
  To: 162.213.33.50
  Protocol: TCP
  Src port: 52070
  Dst port: 443

Packet number 4:
  From: 10.0.2.4
  To: 162.213.33.50
  Protocol: TCP
  Src port: 52070
  Dst port: 443

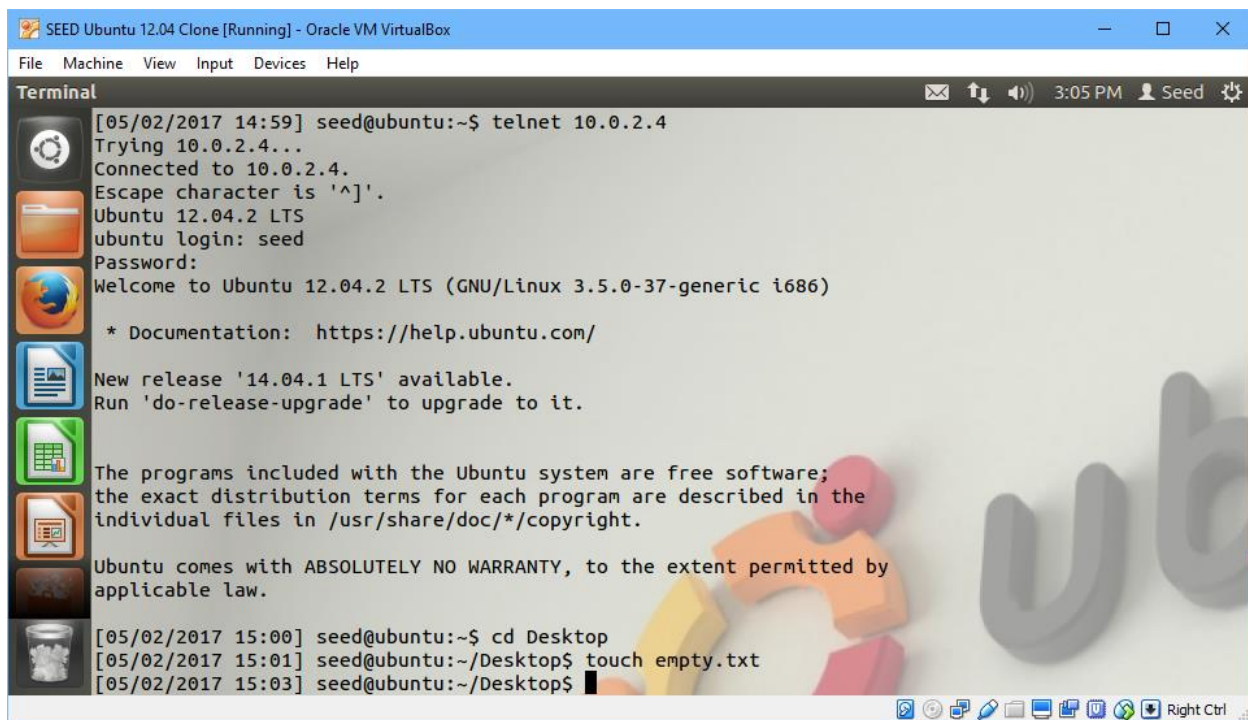
Payload (148 bytes):
00000  16 03 00 00 8f 01 00 00 8b 03 03 59 08 fc f6 d8  ....Y....
00016  ac 8b eb 4f 4c e3 4f 9c f5 27 36 13 44 4f cb 24  ...OL.O..6.DD.$
00032  ce a7 9b b3 af a2 e2 4e a4 08 94 00 00 30 00 33  ....N.....0.3
00048  00 87 00 45 00 39 00 0b 00 88 00 16 00 32 00 40  .g.f.9.k....2.@
00064  00 44 00 38 00 6a 00 87 00 13 00 66 00 2f 00 3c  .D.B.j....f./.<
00080  00 41 00 35 00 3d 00 84 00 0a 00 05 00 04 01 00  .A.S.=.....
00096  00 32 00 00 0b 00 19 00 00 16 76 69 64 05 0f     .2.....video
00112  73 65 61 72 63 68 2e 75 62 75 6e 74 75 2e 63 6f  search.ubuntu.co
00128  6d ff 01 00 01 00 0d 00 0a 00 08 04 02 04 01     .....
00144  02 01 02 02  ....

Packet number 5:
  From: 162.213.33.50
  To: 10.0.2.4
```


With the ip filter expression, a packet is received of type ICMP from 10.0.2.5 which is the clone machine. A packet is then sent back to that address as a confirmation. Then there are more packets (TCP) to and from the address 162.213.33.50.

With the tcp filter, the packets from the clone machine don't get reported by the sniffer. Only the packets from the 162.213.33.50 are shown. This is because the packets aren't sent by the TCP protocol from the other machine.

Problem 3



```
SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[05/02/2017 14:59] seed@ubuntu:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

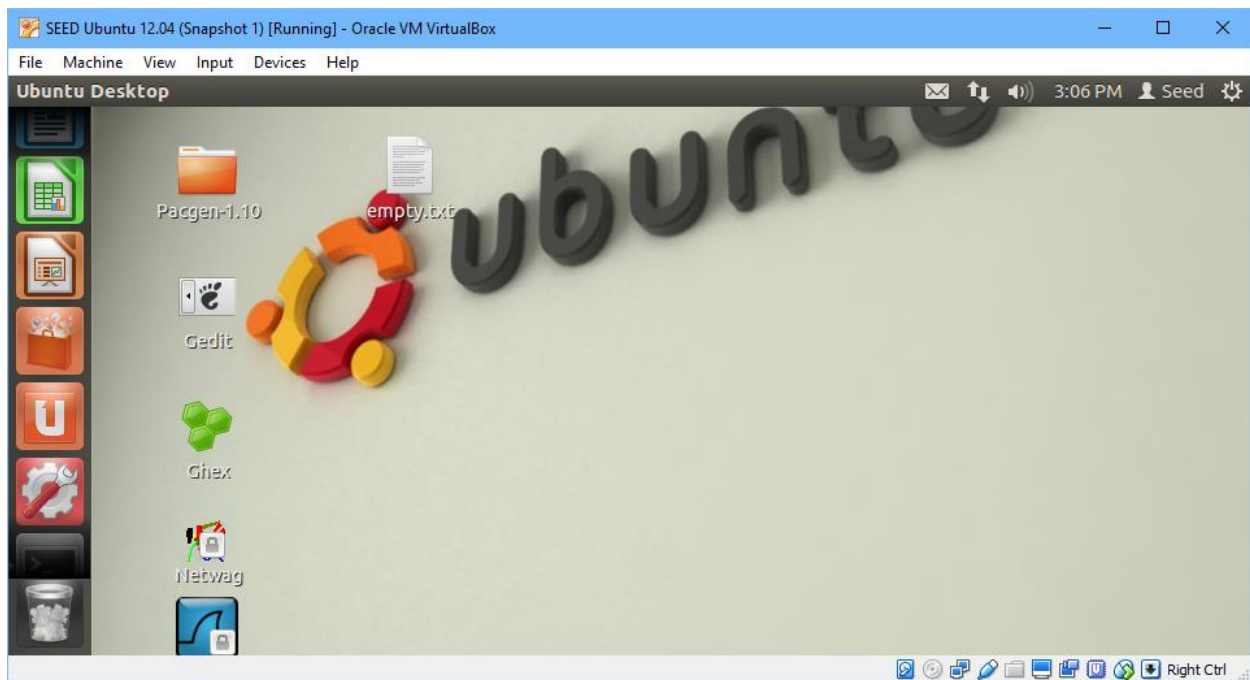
 * Documentation:  https://help.ubuntu.com/

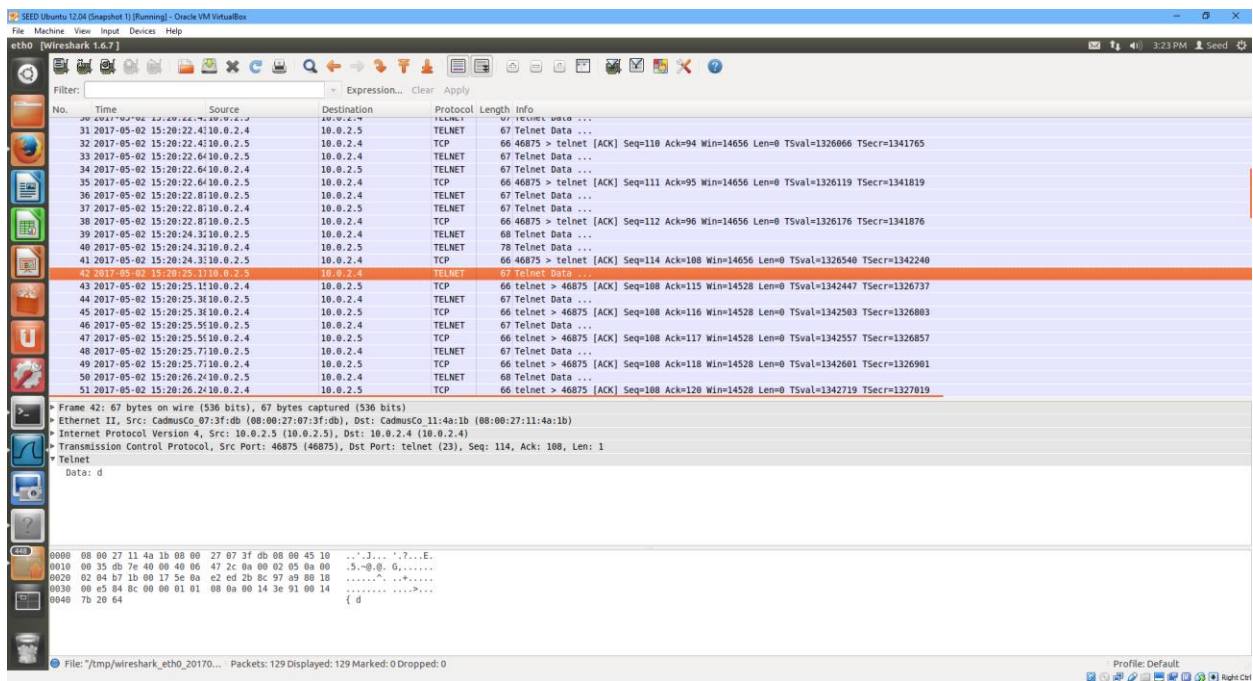
New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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.

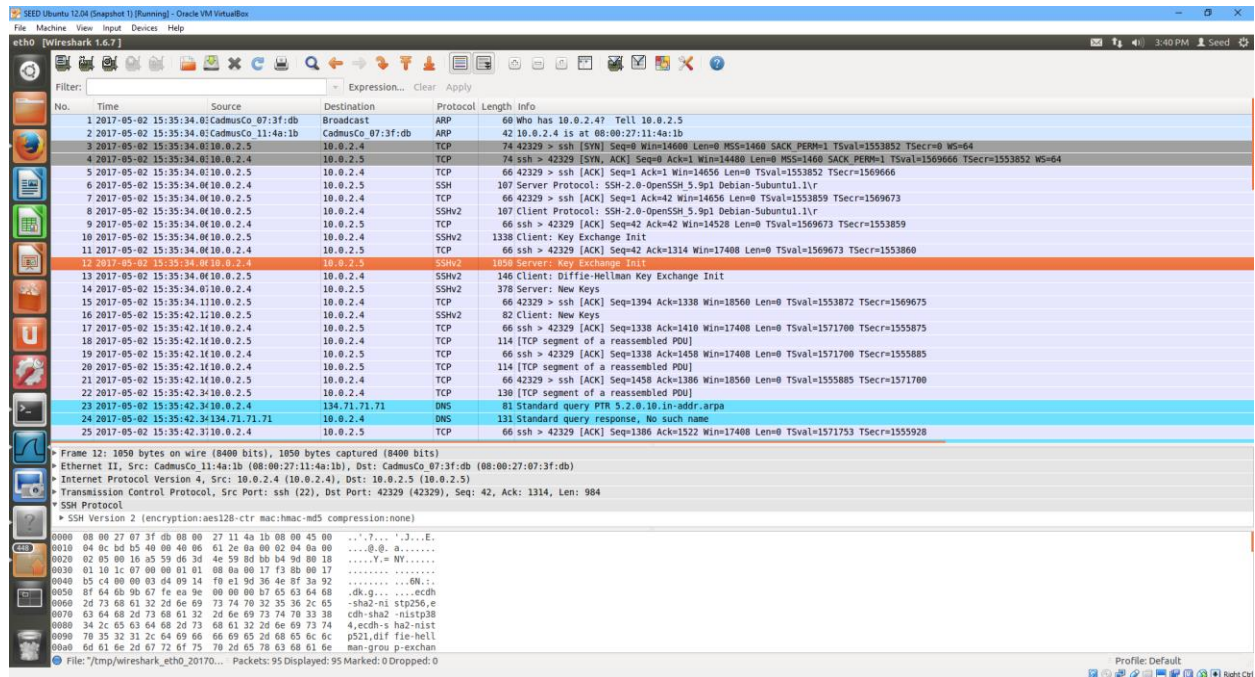
[05/02/2017 15:00] seed@ubuntu:~$ cd Desktop
[05/02/2017 15:01] seed@ubuntu:~/Desktop$ touch empty.txt
[05/02/2017 15:03] seed@ubuntu:~/Desktop$
```





The password, dees, shows up with both packet sniffers. In the Wireshark window, the three telnet packets below the selected one are the remaining: ees. Telnet does not encrypt this password data at all, the packets are sent as is. So a sniffer set up on a telnet server can capture every user's password which is very unsafe.

Problem 4



Wireshark shows the SSH and SSHv2 traffic, and then the following TCP packets but none of them show the password information at all. The packets are all encrypted, even past the header.