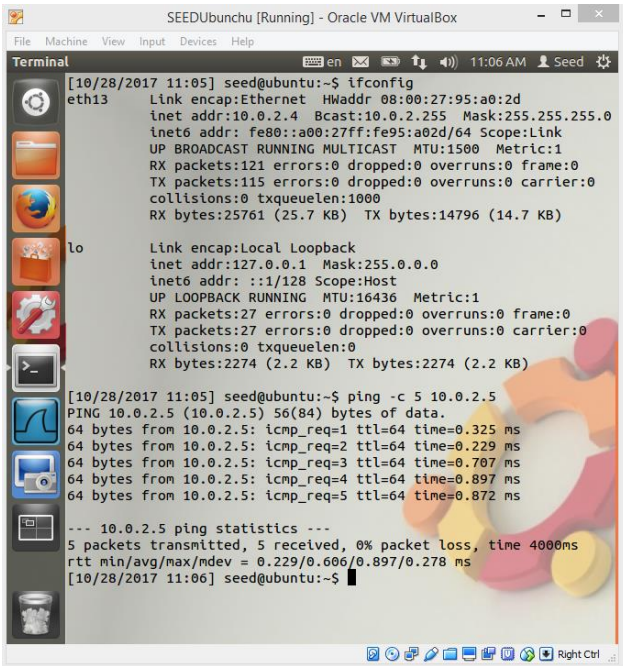
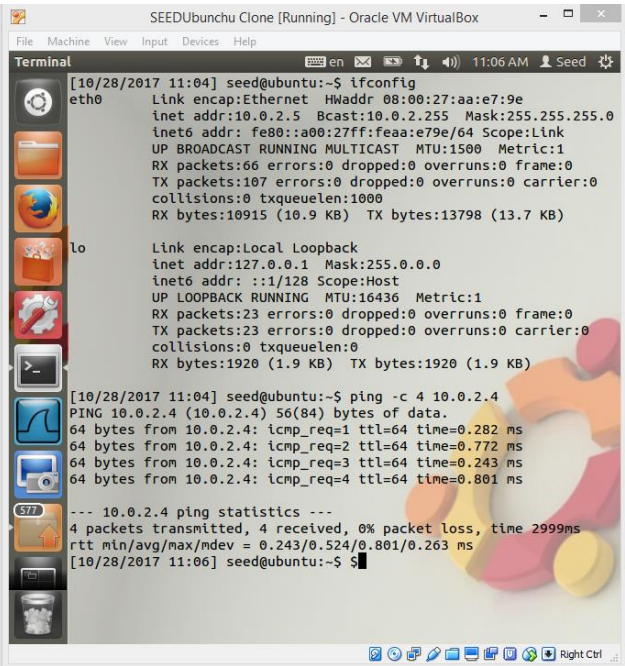
Caleb Chong
10/28/2017
CS380

EX5

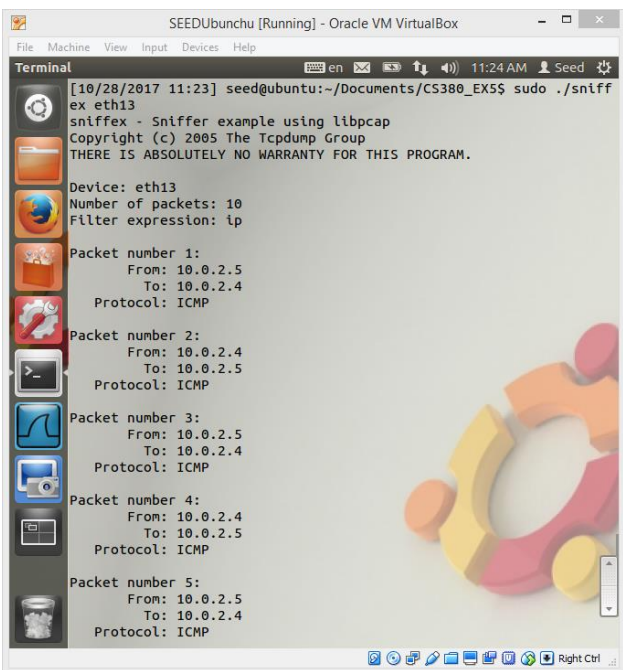
3.1 Problem 1: Verifying the Network

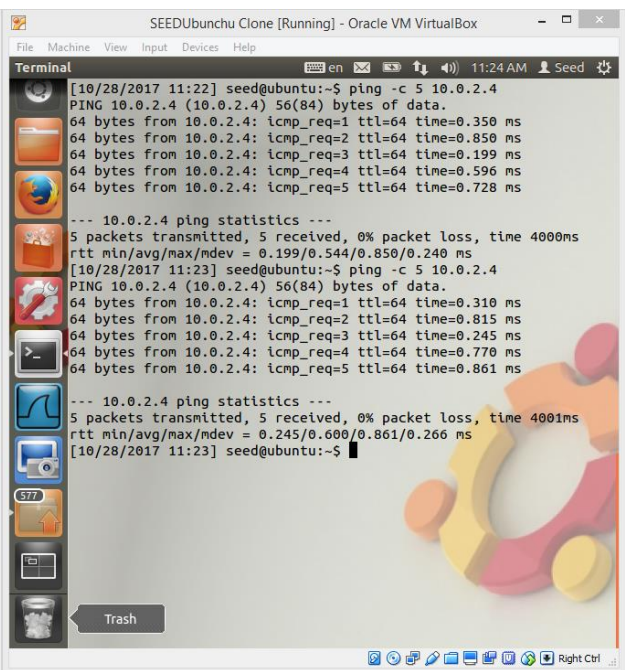




The virtual machines can ping each other successfully, indicating that the network is set up correctly.

3.2 Problem 2: Writing a Packet Sniffer





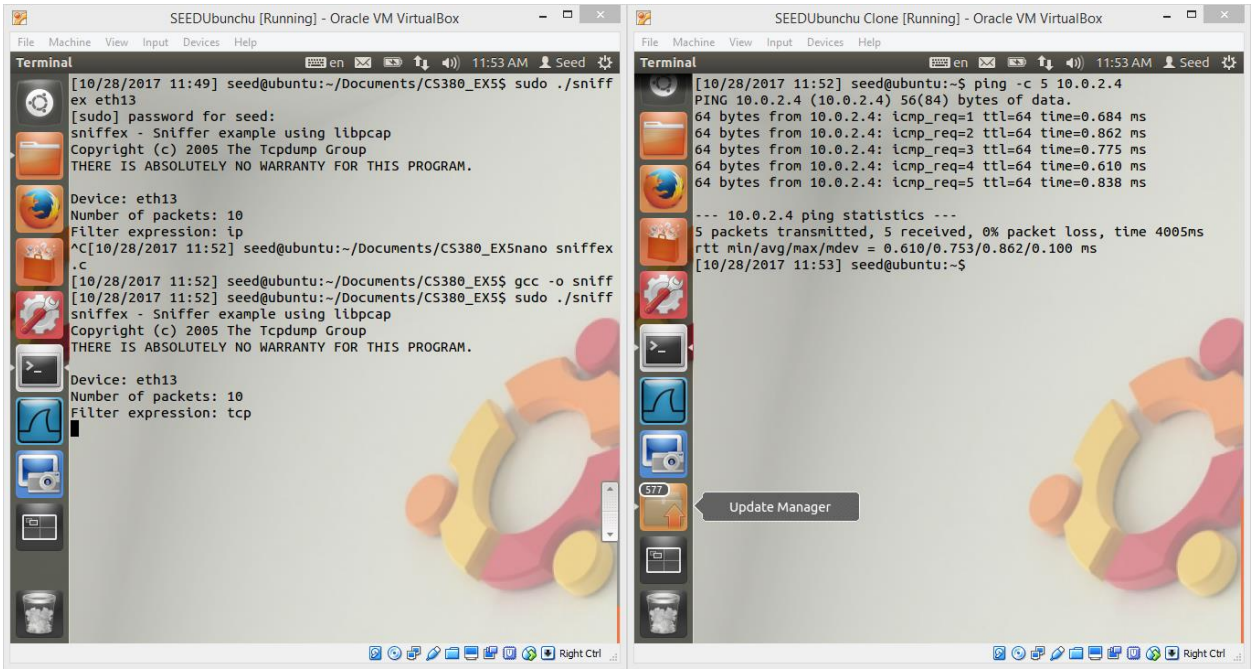
We successfully sniff the packets received and sent when pinging.

```
int main(int argc, char **argv)
{

        char *dev = NULL;
        char errbuf[PCAP_ERRBUF_SIZE];
        pcap_t *handle;

        char filter_exp[] = "tcp";
        struct bpf_program fp;
```

Edit the code to capture TCP packets only.



As expected, no packets are captured, because ping does not make TCP packets.

3.3 Problem 3: Password Sniffing

We can successfully sniff the username and password from Telnet. The following is relevant packets from the packet sniffer output, with the username and password.

```
Packet number 18:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   73                                                s

Packet number 19:
       From: 10.0.2.4
         To: 10.0.2.5
```

```
   Protocol: TCP
   Src port: 23
   Dst port: 37171
   Payload (1 bytes):
00000   73                                                  s

Packet number 20:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23

Packet number 21:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 22:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 23
   Dst port: 37171
   Payload (1 bytes):
00000   65                                                  e

Packet number 23:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23

Packet number 24:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 25:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 23
   Dst port: 37171
   Payload (1 bytes):
00000   65                                                  e

Packet number 26:
       From: 10.0.2.5
         To: 10.0.2.4
```

```
   Protocol: TCP
   Src port: 37171
   Dst port: 23

Packet number 27:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   64                                                  d

Packet number 28:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 23
   Dst port: 37171
   Payload (1 bytes):
00000   64                                                  d

.
.
.

Packet number 33:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   64                                                  d

Packet number 34:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 23
   Dst port: 37171

Packet number 35:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 36:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 23
   Dst port: 37171

Packet number 37:
```

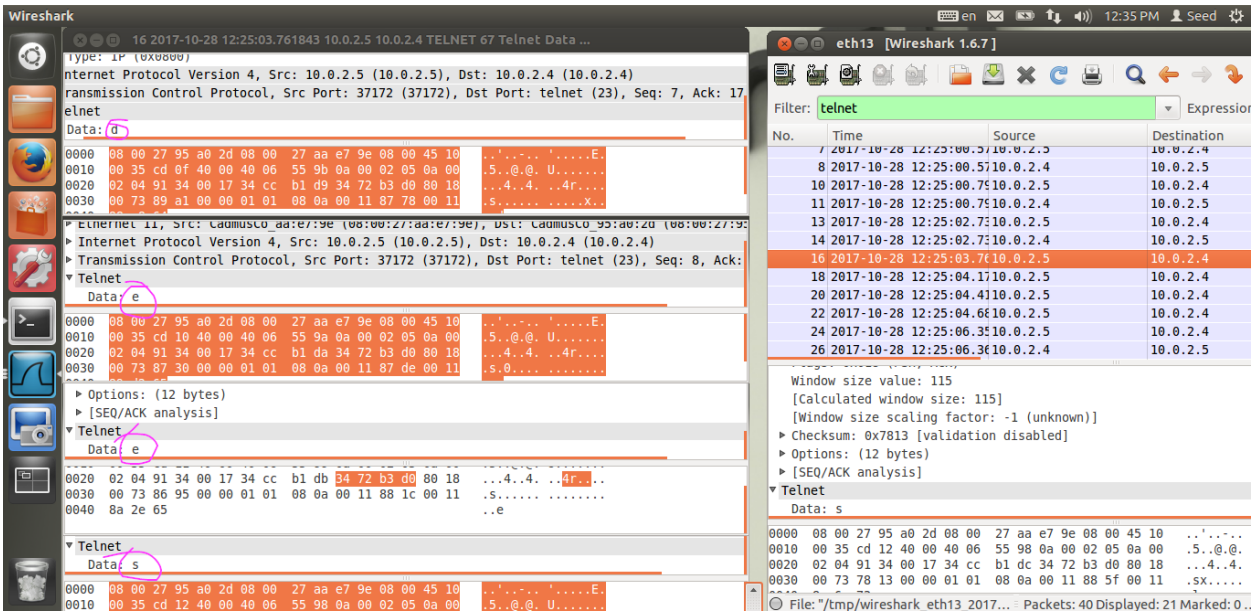
Caleb Chong
10/28/2017
CS380

```
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   65                                                e

Packet number 38:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 23
   Dst port: 37171

Packet number 39:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37171
   Dst port: 23
   Payload (1 bytes):
00000   73                                                s
```

We can do the same using Wireshark. This shows the password.



3.4 Problem 4: SSH

We cannot do the same technique against SSH, because the username and password are encrypted, rather than being transmitted in plaintext. Without any means to decrypt the data, we are unable to extract the username and password from the captured packets.

Caleb Chong
10/28/2017
CS380