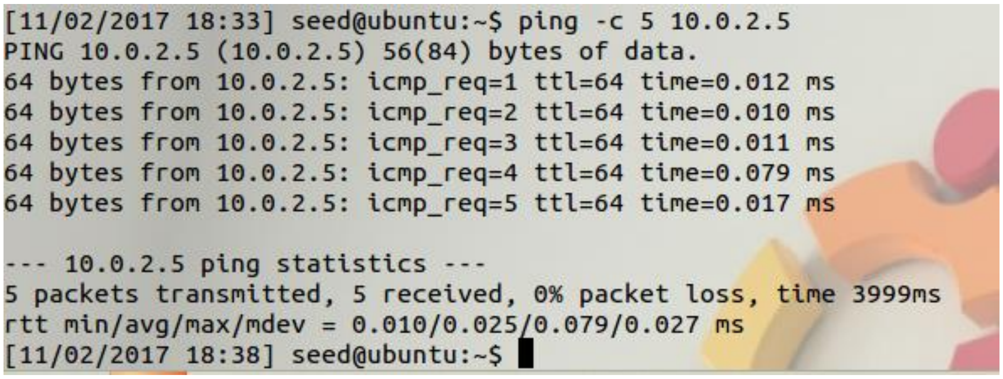
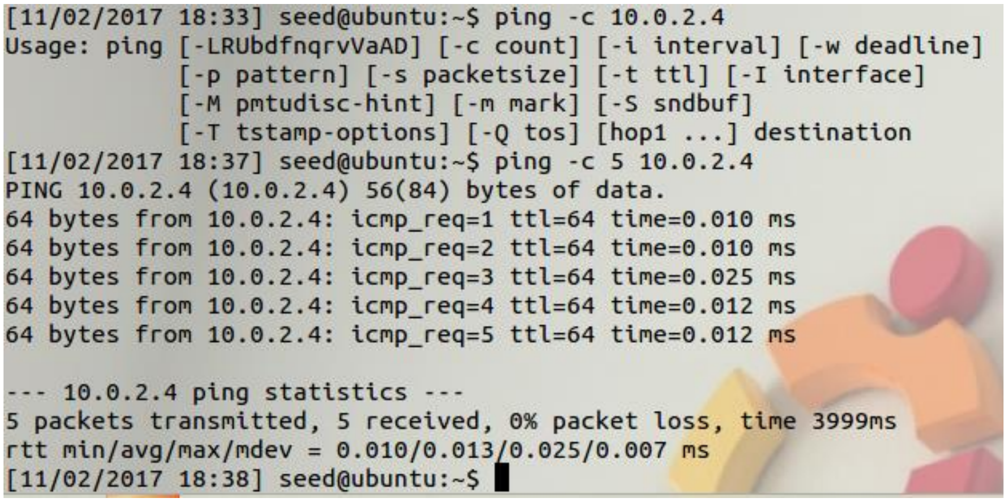
Daniel Spencer

https://github.com/dmspencer87/cs380-ex5 - screenshots taken

Pings to test connection:

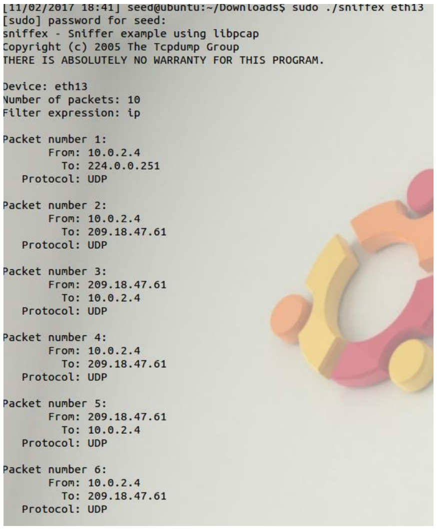


```
[11/02/2017 18:33] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.012 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.010 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.011 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.079 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.017 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.010/0.025/0.079/0.027 ms
[11/02/2017 18:38] seed@ubuntu:~$ 
```



```
[11/02/2017 18:33] seed@ubuntu:~$ ping -c 10.0.2.4
Usage: ping [-LRUbdfnqrvVaAD] [-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
[11/02/2017 18:37] 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=0.010 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.010 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.025 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.012 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.012 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.010/0.013/0.025/0.007 ms
[11/02/2017 18:38] seed@ubuntu:~$ 
```

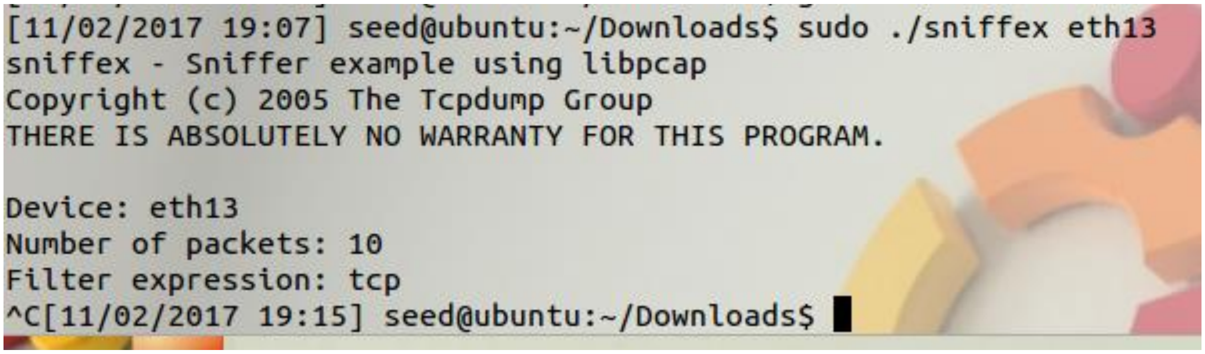
Tested IPSNIFF: PCAP libraries are used to connect to device and monitor the devices UDP and TCP traffic. Changing the protocol from ip to tcp by modifying the filter expression and also Increase the amount of packets.



```
[11/02/2017 18:41] seed@ubuntu:~/Downloads$ sudo ./sniffex eth13
[sudo] password for seed:
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

Packet number 1:
       From: 10.0.2.4
         To: 224.0.0.251
   Protocol: UDP

Packet number 2:
       From: 10.0.2.4
         To: 209.18.47.61
   Protocol: UDP

Packet number 3:
       From: 209.18.47.61
         To: 10.0.2.4
   Protocol: UDP

Packet number 4:
       From: 10.0.2.4
         To: 209.18.47.61
   Protocol: UDP

Packet number 5:
       From: 209.18.47.61
         To: 10.0.2.4
   Protocol: UDP

Packet number 6:
       From: 10.0.2.4
         To: 209.18.47.61
   Protocol: UDP
```

Recorded DataGram packets between port 209.58.47.01

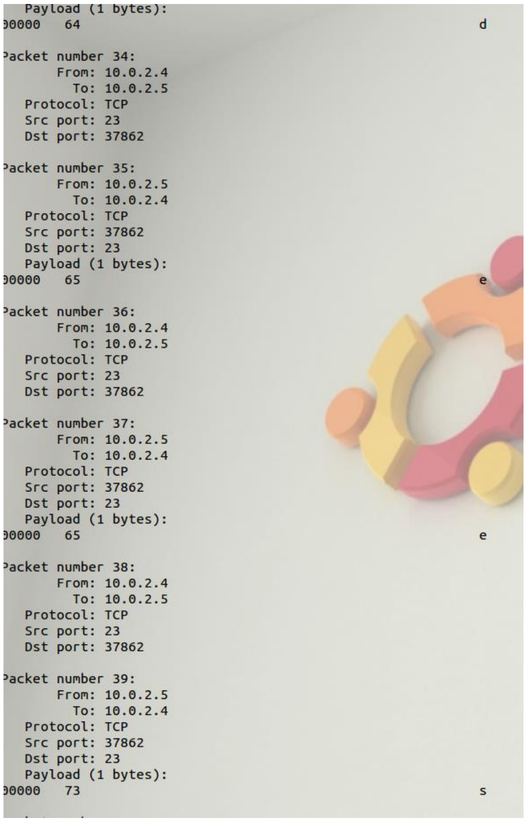
Tested TCP Sniff:



```
[11/02/2017 19:07] seed@ubuntu:~/Downloads$ 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
^C[11/02/2017 19:15] seed@ubuntu:~/Downloads$
```

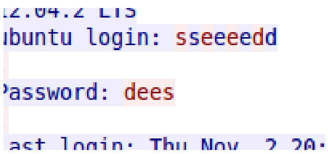
No Tcp packets were being sent.

TCP Sniff with telnet:



```
   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: 37862

Packet number 35:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37862
   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: 37862

Packet number 37:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37862
   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: 37862

Packet number 39:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 37862
   Dst port: 23
   Payload (1 bytes):
00000   73                                                  s
```

WireSHark



```
12.04.2 LTS
ubuntu login: sseeeedd

Password: dees

Last login: Thu Nov  2 20:
```

Looking at the right-hand side you will noticed I found the password via TCP sniff and the password is very clear using wireshark. It seems there is a security concern using telenet.

SSH: connecting via SSH(secure shell) I was unable to retrieve the password information.