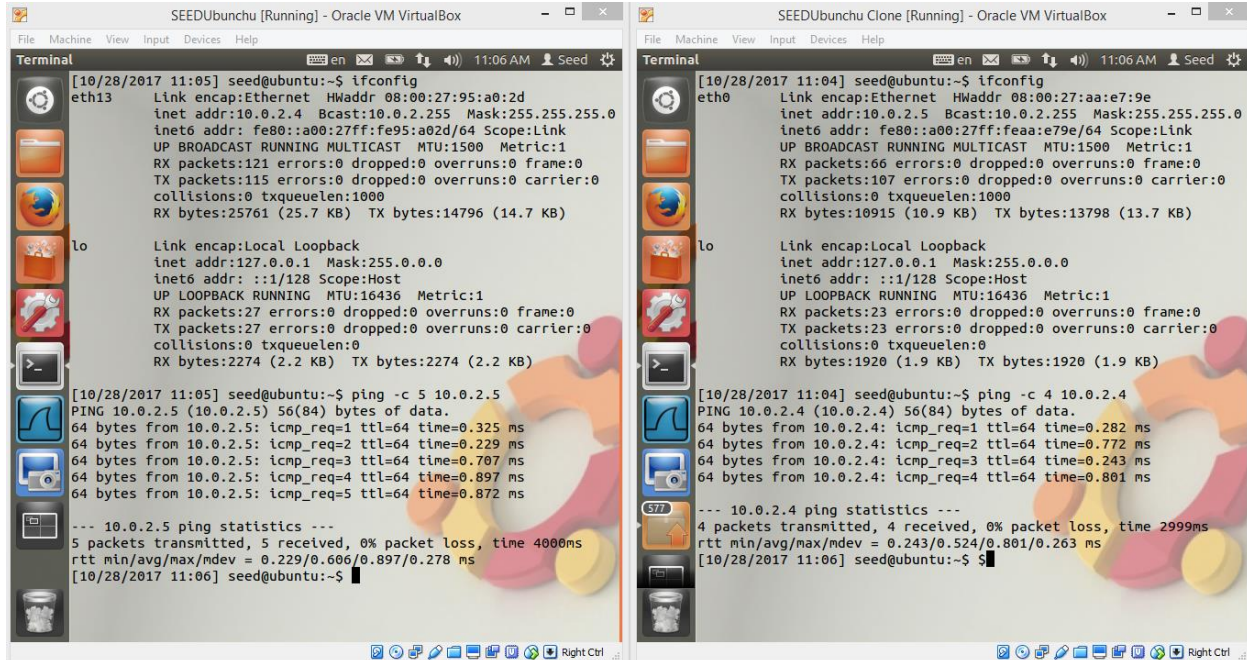


EX5

3.1 Problem 1: Verifying the Network



The image shows two terminal windows from Oracle VM VirtualBox. The left window is titled 'SEEDUubuntu [Running] - Oracle VM VirtualBox' and the right window is titled 'SEEDUubuntu Clone [Running] - Oracle VM VirtualBox'. Both windows show the output of the 'ifconfig' command for the 'eth13' interface, displaying IP address, netmask, and other network details. Below the 'ifconfig' output, both windows show the output of a 'ping -c 5 10.0.2.5' command, indicating successful connectivity with 0% packet loss and response times around 0.2-0.3 ms. The right window also shows a 'ping -c 4 10.0.2.4' command, also successful.

```
[10/28/2017 11:05] seed@ubuntu:~$ ifconfig
eth13    Link encap:Ethernet  HWaddr 08:00:27:95:a0:2d
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:fe95:a02d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25761 (25.7 KB)  TX bytes:14796 (14.7 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:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2274 (2.2 KB)  TX bytes:2274 (2.2 KB)

[10/28/2017 11:05] 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=0.325 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.229 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.707 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.897 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.872 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.229/0.606/0.897/0.278 ms
[10/28/2017 11:06] seed@ubuntu:~$
```

```
[10/28/2017 11:04] seed@ubuntu:~$ ifconfig
eth0     Link encap:Ethernet  HWaddr 08:00:27:aa:e7:9e
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:feaa:e79e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10915 (10.9 KB)  TX bytes:13798 (13.7 KB)

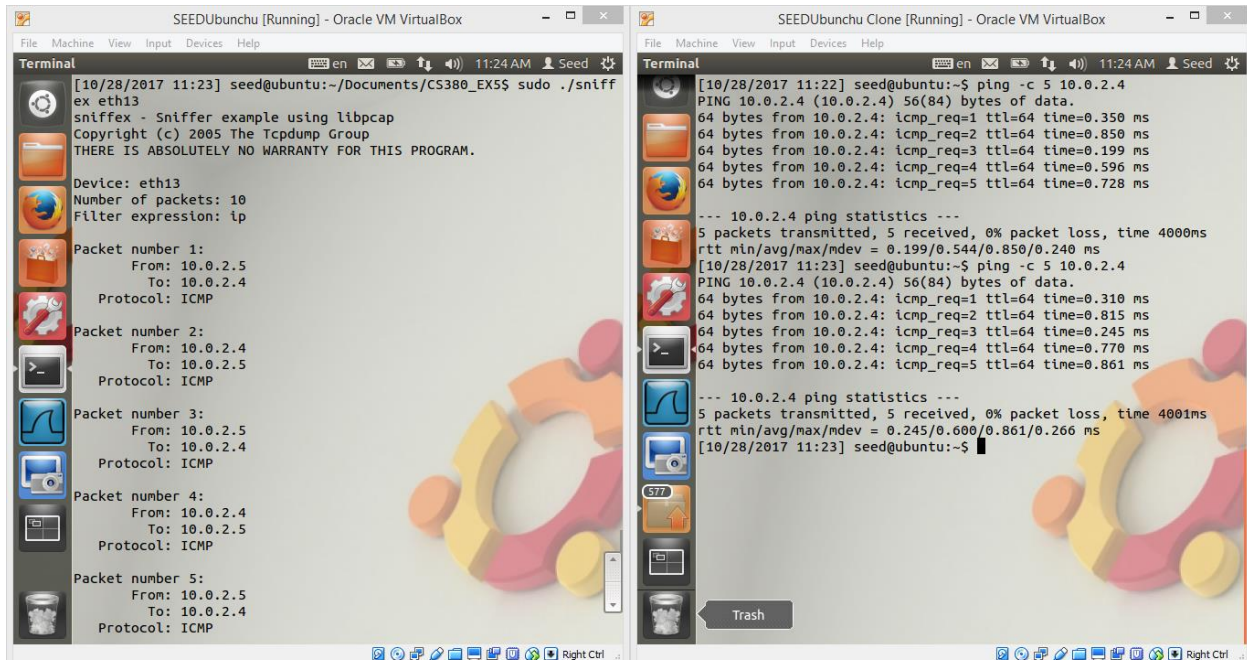
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1920 (1.9 KB)  TX bytes:1920 (1.9 KB)

[10/28/2017 11:04] seed@ubuntu:~$ ping -c 4 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=0.282 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.772 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.243 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.801 ms

--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.243/0.524/0.801/0.263 ms
[10/28/2017 11:06] seed@ubuntu:~$
```

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

3.2 Problem 2: Writing a Packet Sniffer



The image shows two terminal windows from Oracle VM VirtualBox. The left window is titled 'SEEDUubuntu [Running] - Oracle VM VirtualBox' and the right window is titled 'SEEDUubuntu Clone [Running] - Oracle VM VirtualBox'. Both windows show the output of the 'sniff' command, which is a packet sniffer. The left window shows the output of 'sniff -x eth13', displaying details for five captured packets, all of which are ICMP Echo (ping) requests from 10.0.2.5 to 10.0.2.4. The right window shows the output of 'ping -c 5 10.0.2.4' followed by 'sniff -x eth0', displaying details for five captured packets, all of which are ICMP Echo (ping) requests from 10.0.2.4 to 10.0.2.5. Both windows also show the output of a 'ping -c 5 10.0.2.5' command, indicating successful connectivity with 0% packet loss and response times around 0.2-0.3 ms.

```
[10/28/2017 11:23] seed@ubuntu:~/Documents/CS380_EX5$ sudo ./sniff
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: 10.0.2.5
  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: 10.0.2.5
  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
```

```
[10/28/2017 11:22] 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=0.350 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.850 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.199 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.596 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.728 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.199/0.544/0.850/0.240 ms
[10/28/2017 11:23] 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=0.310 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.815 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.245 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.770 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.861 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.245/0.600/0.861/0.266 ms
[10/28/2017 11:23] seed@ubuntu:~$
```

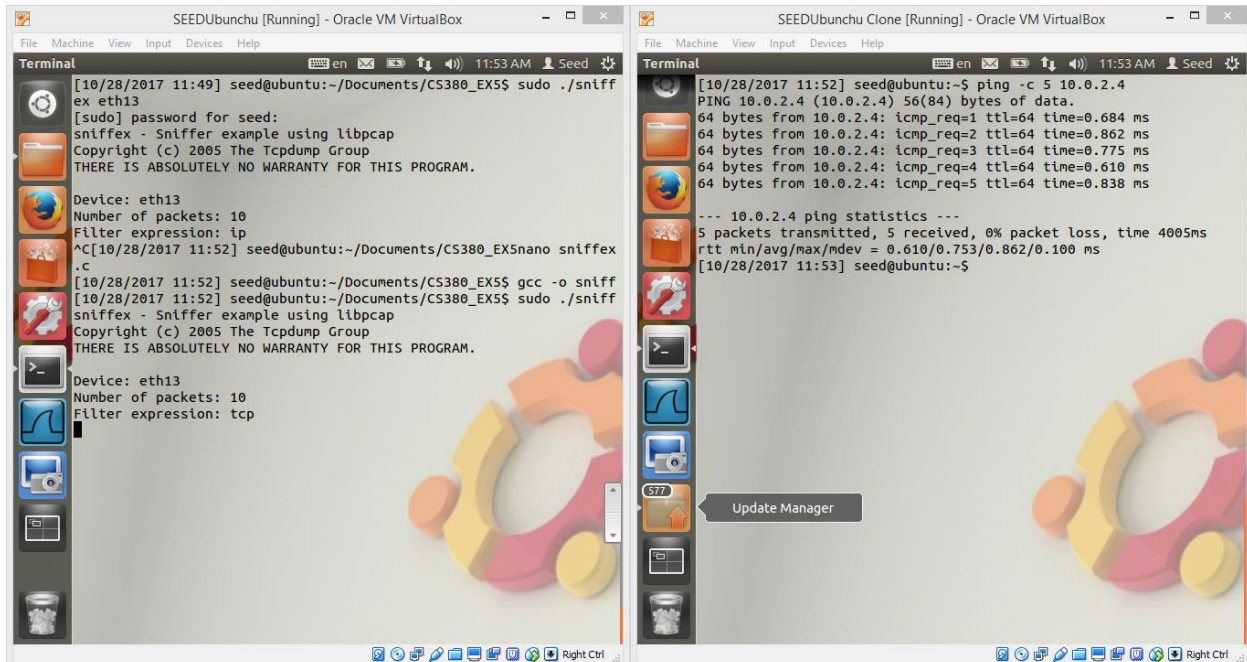
We successfully sniff the packets received and sent when pinging.

```
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):
000000  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

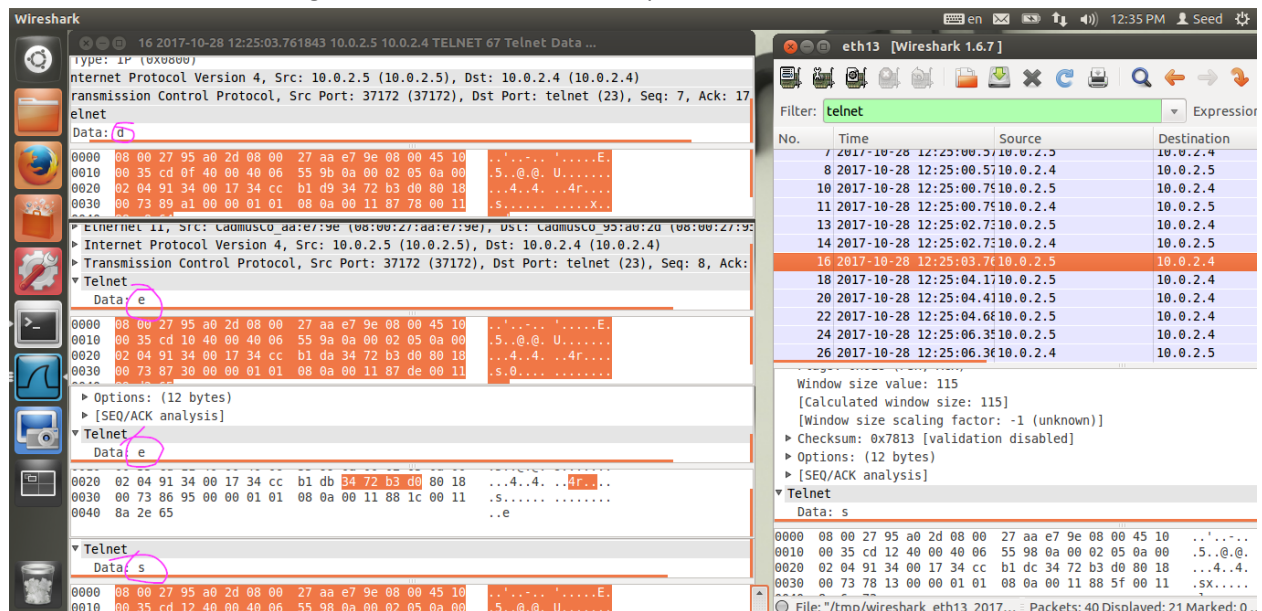
Packet number 37:

From: 10.0.2.5
To: 10.0.2.4
Protocol: TCP
Src port: 37171
Dst port: 23
Payload (1 bytes):
0000 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):
0000 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.

SEEDUbunchu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

eth13 [Wireshark 1.6.7] en 12:40 PM Seed

Filter: Expression...

| No. | Time | Source | Destination | P |
|-----|------------------------|-------------|-------------|---|
| 31 | 2017-10-28 12:38:12.55 | 10.0.2.5 | 10.0.2.4 | T |
| 32 | 2017-10-28 12:38:13.45 | 10.0.2.4 | 192.168.0.1 | D |
| 33 | 2017-10-28 12:38:13.48 | 192.168.0.1 | 10.0.2.4 | D |
| 34 | 2017-10-28 12:38:18.32 | 10.0.2.5 | 10.0.2.4 | T |
| 35 | 2017-10-28 12:38:18.32 | 10.0.2.4 | 10.0.2.5 | T |
| 36 | 2017-10-28 12:38:18.36 | 10.0.2.4 | 10.0.2.5 | T |
| 37 | 2017-10-28 12:38:18.36 | 10.0.2.5 | 10.0.2.4 | T |
| 38 | 2017-10-28 12:38:18.36 | 10.0.2.5 | 10.0.2.4 | T |
| 39 | 2017-10-28 12:38:18.46 | 10.0.2.4 | 10.0.2.5 | T |
| 40 | 2017-10-28 12:38:18.44 | 10.0.2.4 | 10.0.2.5 | T |
| 41 | 2017-10-28 12:38:18.44 | 10.0.2.5 | 10.0.2.4 | T |
| 42 | 2017-10-28 12:38:18.44 | 10.0.2.4 | 10.0.2.5 | T |

Frame 35: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: CadmusCo_95:a0:2d (08:00:27:95:a0:2d), Dst: CadmusCo_aa
Internet Protocol Version 4, Src: 10.0.2.4 (10.0.2.4), Dst: 10.0.2.5 (10.
Transmission Control Protocol, Src Port: ssh (22), Dst Port: 56159 (56159)
Source port: ssh (22)
Destination port: 56159 (56159)
[Stream index: 0]
Sequence number: 1450 (relative sequence number)
Acknowledgement number: 1666 (relative ack number)

0000 08 00 27 aa e7 9e 08 00 27 95 a0 2d 08 00 45 00 ..'.....'...E.
0010 00 34 5b e9 40 00 06 c6 d2 0a 00 02 04 0a 00 .4[.@.@.
0020 02 05 00 16 db 5f 13 2d e3 91 98 69 a1 c7 80 10-...i....
0030 00 9c 18 2f 00 00 01 01 08 0a 00 14 91 b9 00 14 .../....

File: "/tmp/wireshark_eth13_2017... Packets: 47 Click to change configuration profile

Right Ctrl