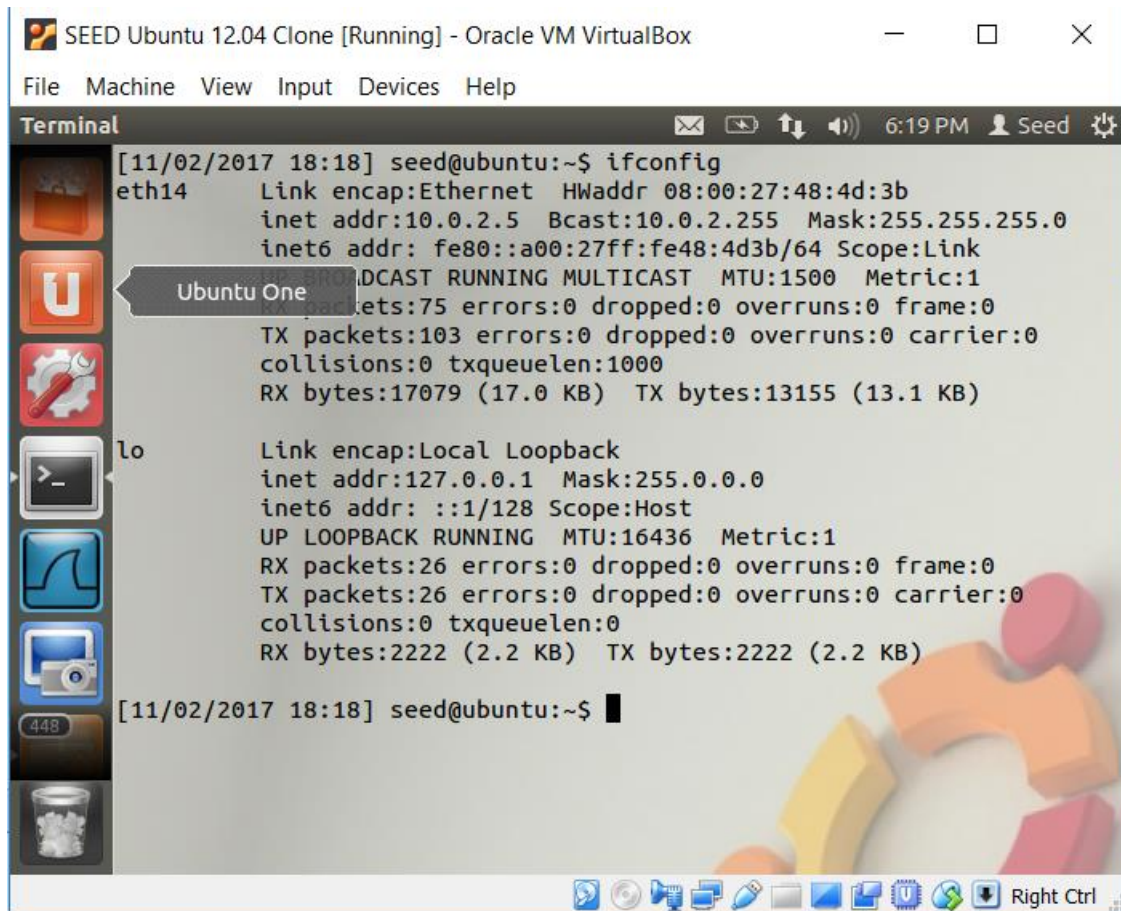


IfConfig of clone its eth14



```
[11/02/2017 18:18] seed@ubuntu:~$ ifconfig
eth14    Link encap:Ethernet  HWaddr 08:00:27:48:4d:3b
         inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe48:4d3b/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:75 errors:0 dropped:0 overruns:0 frame:0
         TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:17079 (17.0 KB)  TX bytes:13155 (13.1 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)

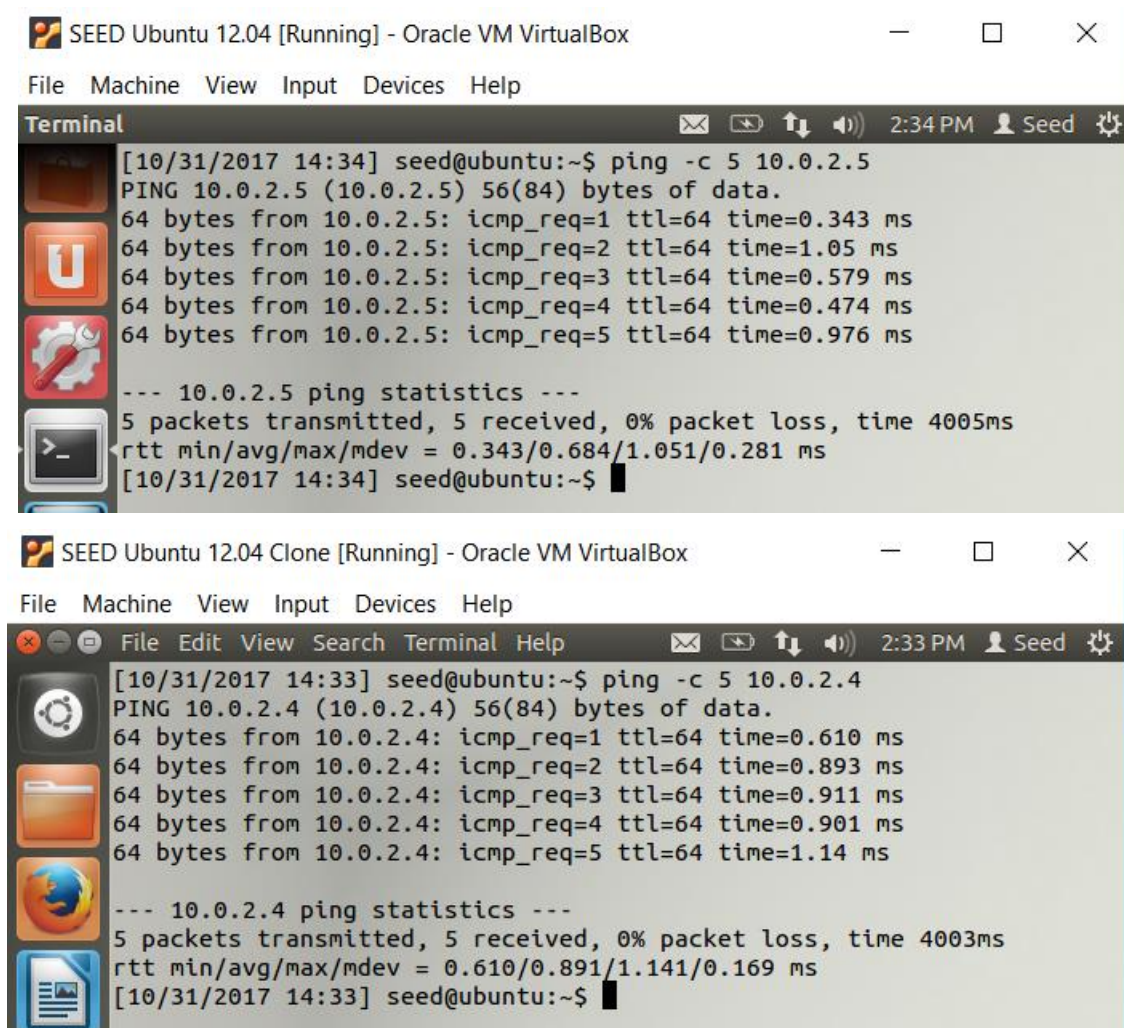
[11/02/2017 18:18] seed@ubuntu:~$
```

```
[11/02/2017 18:18] 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:255.255.25
          5.0
          inet6 addr: fe80::a00:27ff:fe11:f529/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21007 (21.0 KB)  TX bytes:12759 (12.7 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: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)

[11/02/2017 18:18] seed@ubuntu:~$ █
```

Ping



The image shows two screenshots of Oracle VM VirtualBox windows. The top window is titled 'SEED Ubuntu 12.04 [Running] - Oracle VM VirtualBox'. It shows a terminal window with the following output:

```
[10/31/2017 14:34] 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=0.343 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=1.05 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.579 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.474 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.976 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.343/0.684/1.051/0.281 ms
[10/31/2017 14:34] seed@ubuntu:~$
```

The bottom window is titled 'SEED Ubuntu 12.04 Clone [Running] - Oracle VM VirtualBox'. It shows a terminal window with the following output:

```
[10/31/2017 14:33] 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=0.610 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.893 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.911 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.901 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=1.14 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.610/0.891/1.141/0.169 ms
[10/31/2017 14:33] seed@ubuntu:~$
```

Problem 2 Sniffex

Needed to run sudo due to lack of permissions.

Terminal



Capture complete.

[11/01/2017 12:53] 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: 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



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



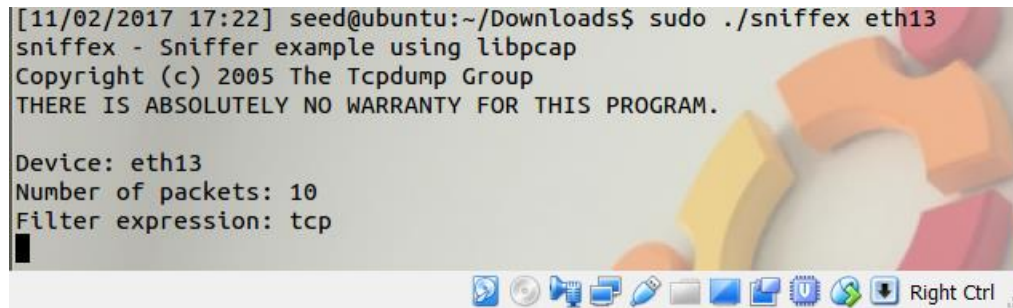
Capture complete.

[11/01/2017 12:53] seed@ubuntu:~/Downloads\$

Sniff tcp only

```
[11/02/2017 17:22] 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
█
```

The image shows a screenshot of an Ubuntu desktop environment. The background features large, colorful 3D letters spelling out 'Ubuntu' in shades of orange, yellow, and pink. A terminal window is open in the foreground, displaying the command 'sudo ./sniffex eth13' and its output. The terminal output includes the program name 'sniffex', copyright information for 'The Tcpdump Group' from 2005, a disclaimer, and configuration details: 'Device: eth13', 'Number of packets: 10', and 'Filter expression: tcp'. A cursor is visible on the line following the filter expression. The Ubuntu desktop icons are visible at the bottom, including a Dash icon, Home icon, and various application icons like a web browser, file manager, and terminal. The system clock shows 'Right Ctrl' and the date '11/02/2017'.

No tcp packets are being sent

Problem 3

```
Device: eth13
Number of packets: 10
Filter expression: tcp
^C[11/02/2017 17:34] 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.
```

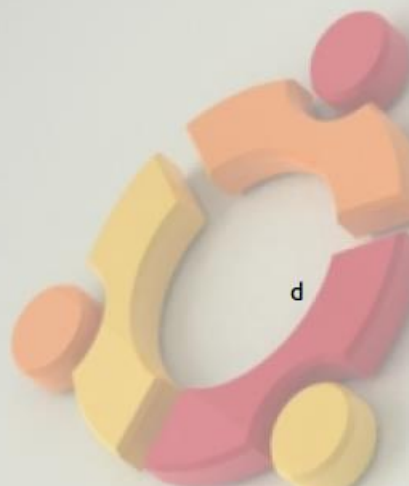
```
Device: eth13
Number of packets: 10
Filter expression: tcp
```

```
Packet number 1:
    From: 10.0.2.5
    To: 10.0.2.4
    Protocol: TCP
    Src port: 42173
    Dst port: 23
    Payload (1 bytes):
00000  64
```

```
Packet number 2:
    From: 10.0.2.4
    To: 10.0.2.5
    Protocol: TCP
    Src port: 23
    Dst port: 42173
```

```
Packet number 3:
    From: 10.0.2.5
    To: 10.0.2.4
    Protocol: TCP
    Src port: 42173
    Dst port: 23
    Payload (1 bytes):
00000  65
```

```
Packet number 4:
    From: 10.0.2.4
    To: 10.0.2.5
    Protocol: TCP
    Src port: 23
    Dst port: 42173
```



d

e

```
Packet number 5:
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: TCP
  Src port: 42173
  Dst port: 23
  Payload (1 bytes):
00000  65                                     e

Packet number 6:
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: TCP
  Src port: 23
  Dst port: 42173

Packet number 7:
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: TCP
  Src port: 42173
  Dst port: 23
  Payload (1 bytes):
00000  73                                     s

Packet number 8:
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: TCP
  Src port: 23
  Dst port: 42173

Packet number 9:
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: TCP
  Src port: 42173
  Dst port: 23
  Payload (2 bytes):
00000  0d 00                                ..

Packet number 10:
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: TCP
  Src port: 23
  Dst port: 42173

Capture complete.
[11/02/2017 17:36] seed@ubuntu:~/Downloads$
```

Easy to locate the users password when they log in.

Wire shark

1 2017-11-02 17:53:47.008959 10.0.2.5 10.0.2.4 TELNET 67 Telnet Data ...

- Frame 1: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
- Ethernet II, Src: CadmusCo_48:4d:3b (08:00:27:48:4d:3b), Dst: CadmusCo_11:f5:29 (08:00:27:11:f5:29)
- Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)
- Transmission Control Protocol, Src Port: 42173 (42173), Dst Port: telnet (23), Seq: 1, Ack: 1
- Telnet

0020 02 04 a4 bd 00 17 1c 58 b4 46 0f f8 08 1d 80 18X .F.....
0030 02 95 f4 d6 00 00 01 01 08 0a 00 15 c8 e3 00 15
0040 ac a9 64 ..d

3 2017-11-02 17:53:47.197692 10.0.2.5 10.0.2.4 TELNET 67 Telnet Data ...

- Frame 3: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
- Ethernet II, Src: CadmusCo_48:4d:3b (08:00:27:48:4d:3b), Dst: CadmusCo_11:f5:29 (08:00:27:11:f5:29)
- Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)
- Transmission Control Protocol, Src Port: 42173 (42173), Dst Port: telnet (23), Seq: 2, Ack: 1
- Telnet

0020 02 04 a4 bd 00 17 1c 58 b4 47 0f f8 08 1d 80 18X .G.....
0030 02 95 dd fc 00 00 01 01 08 0a 00 15 c9 12 00 15
0040 c2 53 65 .Se

5 2017-11-02 17:53:47.341361 10.0.2.5 10.0.2.4 TELNET 67 Telnet Data ...

- Frame 5: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
- Ethernet II, Src: CadmusCo_48:4d:3b (08:00:27:48:4d:3b), Dst: CadmusCo_11:f5:29 (08:00:27:11:f5:29)
- Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)
- Transmission Control Protocol, Src Port: 42173 (42173), Dst Port: telnet (23), Seq: 3, Ack: 1
- Telnet

0020 02 04 a4 bd 00 17 1c 58 b4 48 0f f8 08 1d 80 18X .H.....
0030 02 95 dd b2 00 00 01 01 08 0a 00 15 c9 36 00 156..
0040 c2 78 65 .xe

7 2017-11-02 17:53:47.519912 10.0.2.5 10.0.2.4 TELNET 67 Telnet Data ...

- Frame 7: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
- Ethernet II, Src: CadmusCo_48:4d:3b (08:00:27:48:4d:3b), Dst: CadmusCo_11:f5:29 (08:00:27:11:f5:29)
- Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)
- Transmission Control Protocol, Src Port: 42173 (42173), Dst Port: telnet (23), Seq: 4, Ack: 1
- Telnet

0020 02 04 a4 bd 00 17 1c 58 b4 49 0f f8 08 1d 80 18X .I.....
0030 02 95 cf 60 00 00 01 01 08 0a 00 15 c9 63 00 15C..
0040 c2 9c 73 ..S

Is able to get the password of the other computer.

SSH

D

```
5 2017-11-02 18:11:43.969814 10.0.2.5 10.0.2.4 SSH 194 Encrypted request packet len=128
Frame 5: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
Ethernet II, Src: CadmusCo_48:4d:3b (08:00:27:48:4d:3b), Dst: CadmusCo_11:f5:29 (08:00:27:11:f5:29)
Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)
Transmission Control Protocol, Src Port: 35112 (35112), Dst Port: ssh (22), Seq: 145, Ack: 3
SSH Protocol

0000 08 00 27 11 f5 29 08 00 27 48 4d 3b 08 00 45 00 ..'..)'.. 'HM;..E.
0010 00 b4 11 91 40 00 40 06 10 ab 0a 00 02 05 0a 00 ....@.@. ....
0020 02 04 89 28 00 16 6b 6f ca 00 6e 42 71 89 80 18 ....(..ko ..nBq...
0030 01 22 35 8f 00 00 01 01 08 0a 00 19 e4 9c 00 19 .."5.....
0040 de 01 50 f4 0b 81 29 99 8d a8 af 1d 57 bd 4a 4d ..P...). ....W.JM
0050 0a 93 e8 03 79 9d 52 8d 46 dc f7 be b7 83 73 11 ....y.R. F.....s.
0060 17 50 02 61 3b b3 49 c2 86 7f 8d ca 41 9a 85 fb .P.a;.I. ....A...
0070 b1 75 ad cc b1 af 0e a0 1a 2e 4a 9c 8b 99 67 11 .u..... ..J...g.
0080 3c 62 f0 01 2d 77 c0 fc 47 48 a6 66 fb 55 5b 1e <b...-w.. GH.f.U[.
0090 a9 75 1a a9 aa 3f c3 40 bf 3f 69 a9 8d 49 a9 af .u...?.@ .?i..I..
00a0 2c 30 58 5c 02 c1 5c 4c 23 fb c8 58 12 f5 06 26 ,0X\...\L #..X...&
00b0 d3 49 0f c2 a8 3e fc d0 df 62 7a ab 8d ab 99 68 .I...>.. .bz....h
00c0 64 8d d.
```

E

```
3 2017-11-02 18:11:43.969290 10.0.2.4 10.0.2.5 SSH 98 Encrypted response packet len=32
Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: CadmusCo_11:f5:29 (08:00:27:11:f5:29), Dst: CadmusCo_48:4d:3b (08:00:27:48:4d:3b)
Internet Protocol Version 4, Src: 10.0.2.4 (10.0.2.4), Dst: 10.0.2.5 (10.0.2.5)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: 35112 (35112), Seq: 1, Ack: 145
SSH Protocol

0000 08 00 27 48 4d 3b 08 00 27 11 f5 29 08 00 45 00 ..'HM;.. '..)'..E.
0010 00 54 a7 af 40 00 40 06 7a ec 0a 00 02 04 0a 00 .T..@.@. z.....
0020 02 05 00 16 89 28 6e 42 71 69 6b 6f ca 00 80 18 ....(nB qiko....
0030 01 38 18 4f 00 00 01 01 08 0a 00 19 de 01 00 19 .8.0....
0040 e4 96 19 5d e0 f7 7d 20 9a 97 1b 03 88 75 85 aa ...]} .....u..
0050 24 0e ba 17 d0 9e ac 33 b8 03 6e 48 40 ff e9 dd $......3 ..nH@...
0060 d8 dc ..
```

E

```

1 2017-11-02 18:11:43.944945 10.0.2.5 10.0.2.4 SSH 210 Encrypted request packet len=144
Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
Ethernet II, Src: CadmusCo_48:4d:3b (08:00:27:48:4d:3b), Dst: CadmusCo_11:f5:29 (08:00:27:11:f5:29)
Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 10.0.2.4 (10.0.2.4)
Transmission Control Protocol, Src Port: 35112 (35112), Dst Port: ssh (22), Seq: 1, Ack: 1,
SSH Protocol

0000  08 00 27 11 f5 29 08 00 27 48 4d 3b 08 00 45 00  ..'..).. 'HM;..E.
0010  00 c4 11 8f 40 00 40 06 10 9d 0a 00 02 05 0a 00  ....@.@. ....
0020  02 04 89 28 00 16 6b 6f c9 70 6e 42 71 69 80 18  ...(..ko .pnBqi..
0030  01 22 00 2e 00 00 01 01 08 0a 00 19 e4 96 00 19  .".....
0040  cf 41 e3 70 0c 39 95 42 e9 34 ba ca b3 b9 f4 a2  .A.p.9.B .4.....
0050  05 19 56 8e 16 54 f5 95 c0 49 6b 66 3d ea 15 65  ..V..T.. .Ikf=..e
0060  d0 e2 0b 51 57 5c 0c 90 b7 b3 a2 fd c2 00 d1 bb  ...QW\.. ....
0070  84 78 a4 0b 20 74 65 b4 08 fa 74 71 ad c7 e5 70  .x.. te. ..tq...p
0080  c0 5d e5 95 96 c1 ea f1 81 bc 83 02 c3 80 70 0c  .]..... ..p.
0090  f8 e2 c8 96 d4 3b fa 4c ..y.U.E. ....;..L
00a0  5c e6 a7 b8 a4 cd 56 bd ..=Dq..r7 \.....V.
00b0  2b 31 7c b2 2e 05 12 bc ca 78 2c 55 43 1b e1 29  +1|..... .x,UC..)
00c0  3c 4e 0f 9d 60 26 4c 5f 7d e6 5f 06 a8 57 07 98  <N...`&L }. ..W..
00d0  ad dc ..

```

S

```

7 2017-11-02 18:11:44.034194 10.0.2.4 10.0.2.5 SSH 114 Encrypted response packet len=48
114 bytes on wire (912 bits), 114 bytes captured (912 bits)
II, Src: CadmusCo_11:f5:29 (08:00:27:11:f5:29), Dst: CadmusCo_48:4d:3b (08:00:27:48:4d:3b)
Protocol Version 4, Src: 10.0.2.4 (10.0.2.4), Dst: 10.0.2.5 (10.0.2.5)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: 35112 (35112), Seq: 33, Ack: 273, Len: 48
col

0000  08 00 27 48 4d 3b 08 00 27 11 f5 29 08 00 45 00  ..'HM;.. '..)..E.
0010  00 64 a7 b1 40 00 40 06 7a da 0a 00 02 04 0a 00  .d..@.@. z.....
0020  02 05 00 16 89 28 6e 42 71 89 6b 6f ca 80 80 18  ....(nB q.ko....
0030  01 5f 18 5f 00 00 01 01 08 0a 00 19 de 12 00 19  .._.....
0040  e4 9c fe 92 5b 4b 2c d9 61 19 07 6c 4e 0d a7 be  ....[K,. a..lN...
0050  6b 89 c2 78 89 0d 95 60 f7 2d ef 56 81 b4 2e fd  k..x...` ..-V....
0060  fb 31 7b 56 a3 b8 34 d4 4b 16 41 8f 63 e2 be 5e  .1{V..4. K.A.c..^
0070  2b 4e +N

```

Can not find the password that is encoded by ssh.