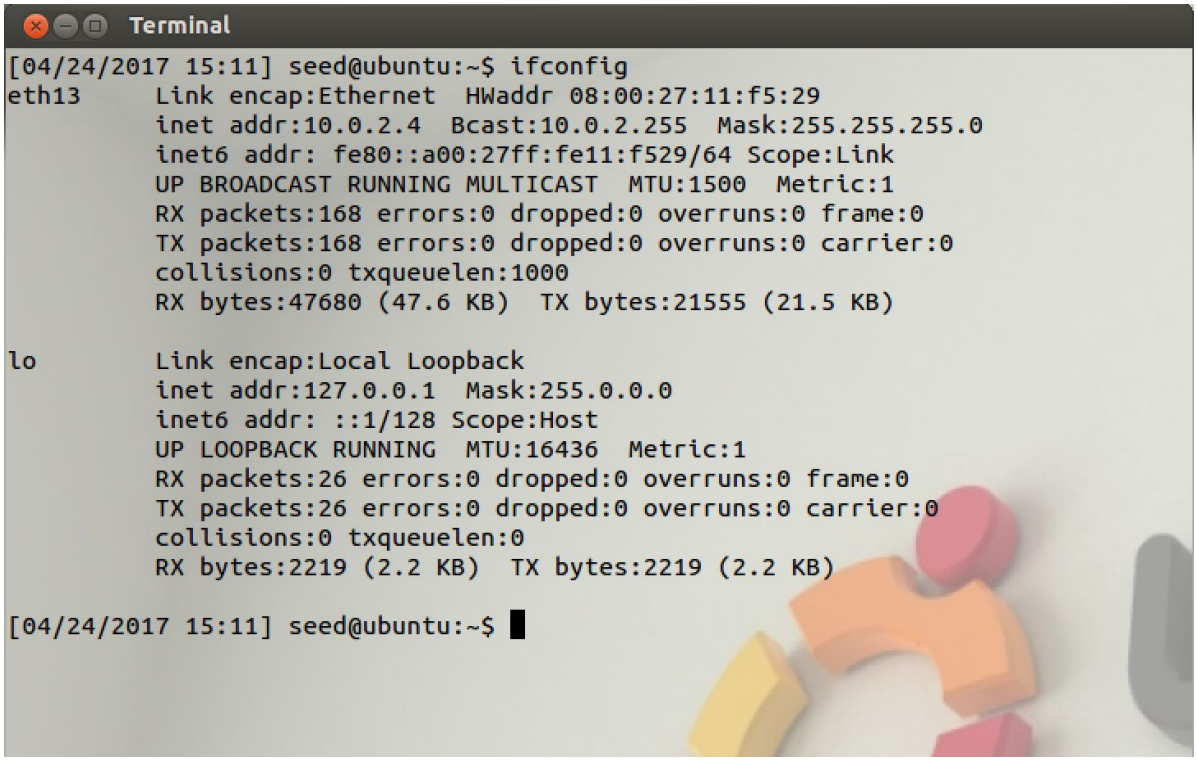
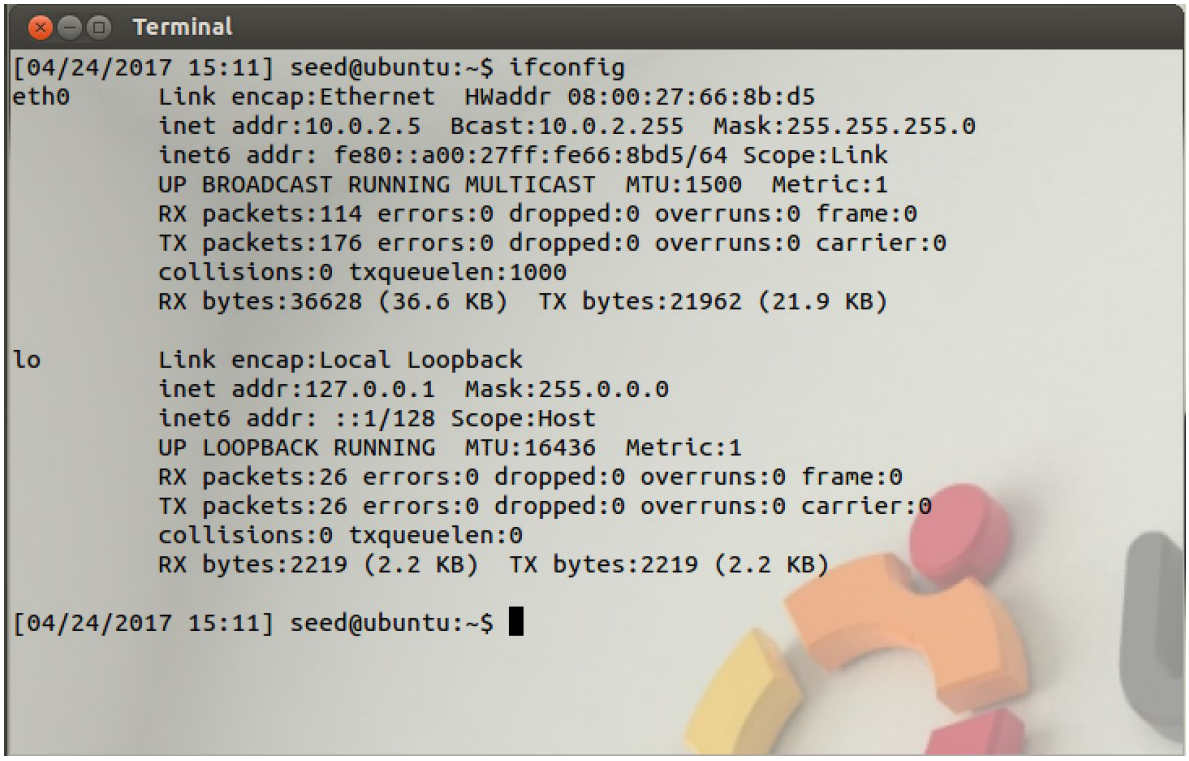
CS380 - EX5

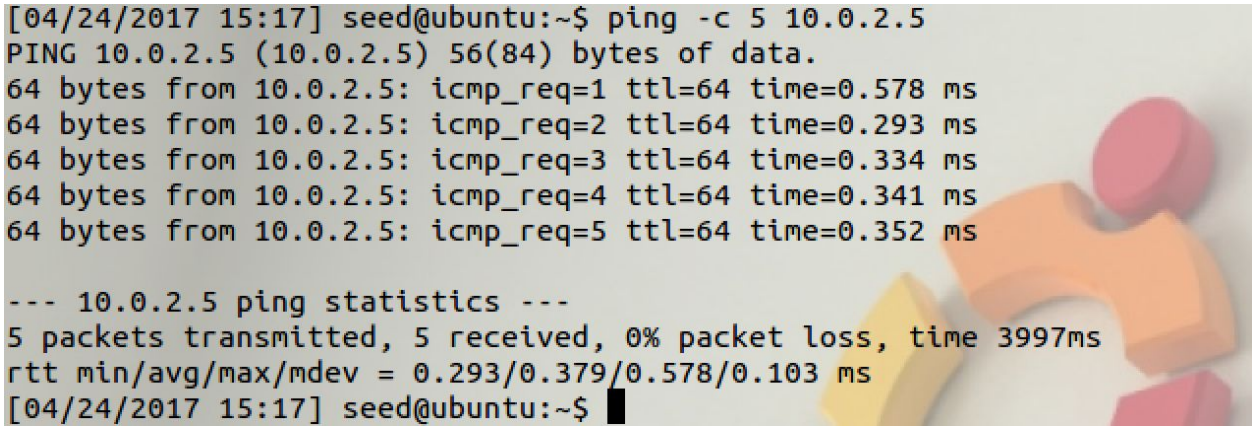
Bradley Gulli & Brian Sandoval

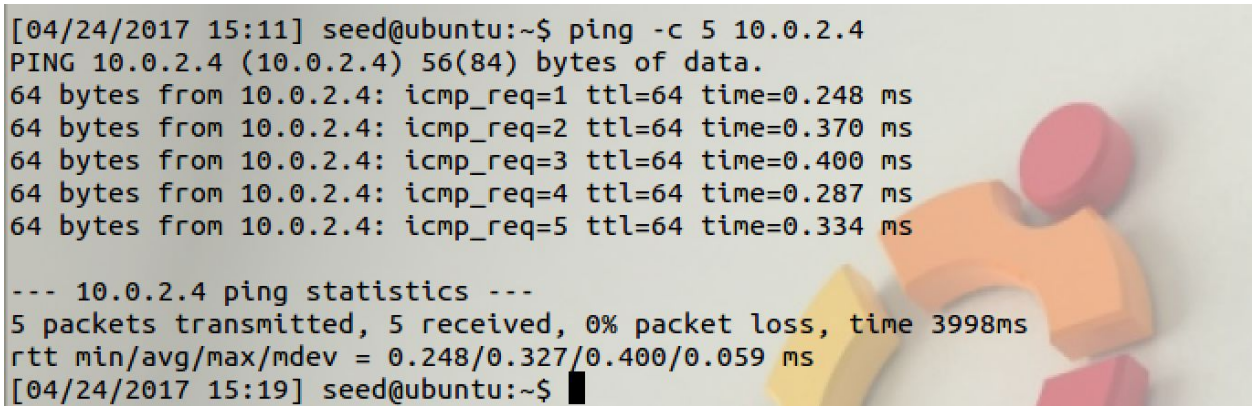
Problem #1: Verify The Network - VM1 - 10.0.2.4 VM2 - 10.0.2.5





Verify communication through pings: Both worked





Problem #2: Writing a Packet Sniffer

Explanation on how to write packet sniffer:

In order to have the pcap application work, we must do a series of steps which we will outline in the following sections to set it up and then execute it.

Setting the Device

The first thing we must do is to set up our device which can be done in two different ways. The first of these two, is to have the user pass in an argument into the program which will specify the device. The second way to set the device is to have the pcap set it on its own. What happens in this case is that a device is preset in the code and the code includes variables that will hold information on these devices when they succeed or fail. For example, if a command fails, a string will populate which will give a description of the error and be stored in one of said variables.

Opening the device for sniffing

To open the device that we set, an integer is passed as an argument which defines the maximum number of bytes to be captured by the pcap. This essentially opens the device and tells it how many bytes to read. When it comes to this, we can sniff the data in both promiscuous and non- promiscuous methods. What we find is that promiscuous sniffing allows for us to collect more packets, however the host machine can detect whether another host is doing promiscuous sniffing. Finally, in this section, you must provide the Ethernet headers, as not all devices provide the same type of link-layer headers. If the program does not support the link-header provided by the device, the program will terminate.

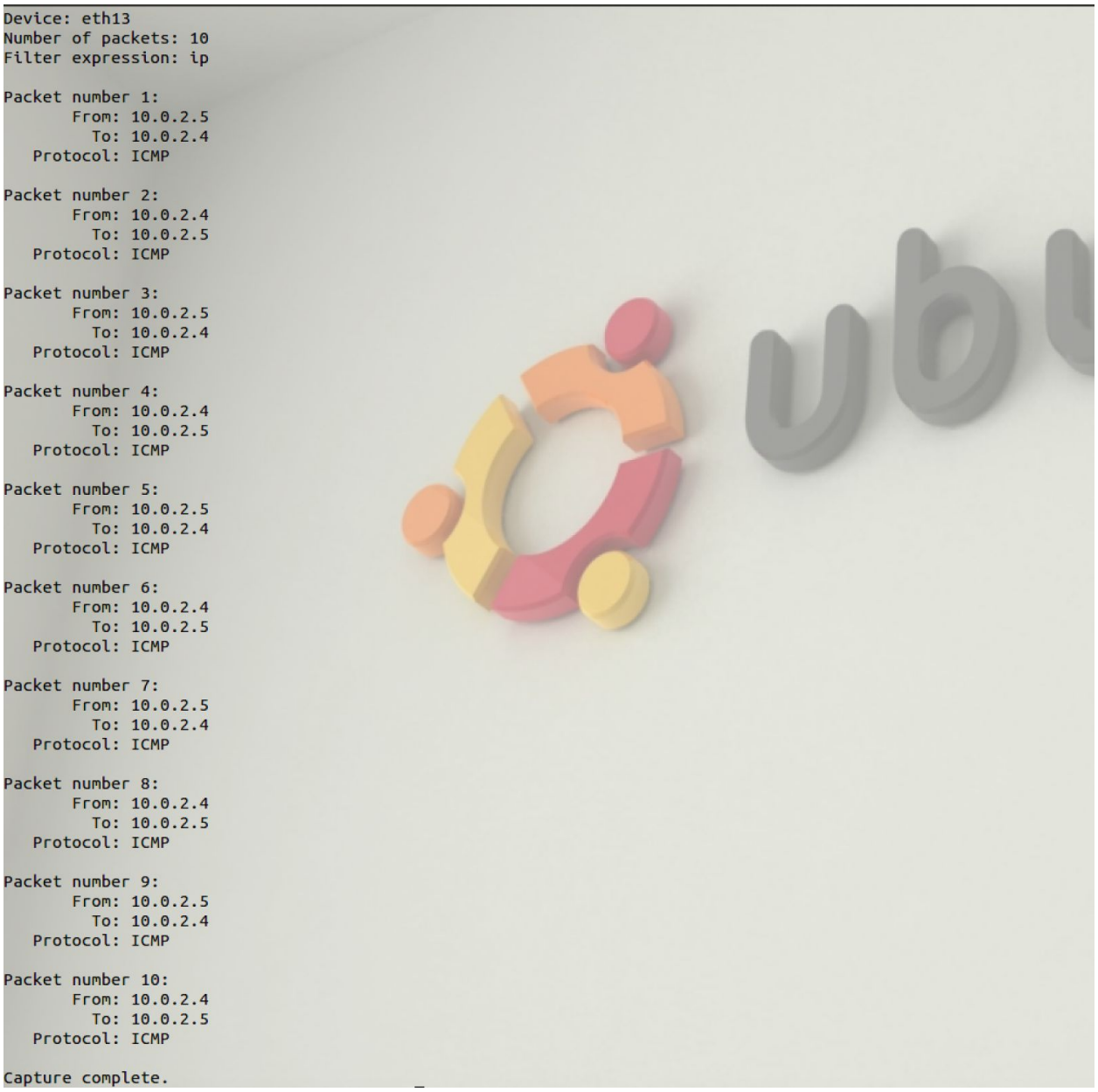
Filtering Traffic

In order to filter we can call the pcap filter as it is much easier and does it "directly with the BPF filter…." Before applying the filter, we must first compile it, as it is kept in a regular character array. To do this we use the method, pcap_compile(). The first argument for this method is a pointer to the session handle, with the second argument being a reference to the location we will store the location of the compiled version of the filter. Following this we also pass in an integer that determines whether it is optimized or not, and finally we must specify the network mask of the network which we are applying the filter to. The process in this section prepares the sniffer to sniff data being sent through a specific port.

The Actual Sniffing

There are two main ways to capture packets being sent. This comes to capturing a single packet at a time or capturing single packets until N number of packets have been caught. Once again, we use a method from the pcap library which has the first argument be a pointer to the session handler. The second argument however, is a pointer to "a structure that holds general information about the packet, specifically the time in which it was sniffed, the length of the packet, and the length of the specific portion." During this process, whatever device was set is sniffed by putting it in promiscuous mode.

Running the sniffex program:



Sniffex program for TCP: When we do this we see the bytes of information in the packets

```
Packet number 5:
       From: 162.213.33.49
         To: 10.0.2.4
   Protocol: TCP
   Src port: 443
   Dst port: 35932

Packet number 6:
       From: 162.213.33.49
         To: 10.0.2.4
   Protocol: TCP
   Src port: 443
   Dst port: 35932
   Payload (1288 bytes):
00000   16 03 03 00 55 02 00 00  51 03 03 e3 88 64 cd 73    ....U...Q....d.s
00016   42 6e 77 54 a0 a2 cd 14  e9 f7 44 5b 99 9f 24 61    BnwT......D[..$a
00032   31 1e 44 87 8b e0 45 29  a4 70 3e 20 1f 6f 69 3f    1.D...E).p> .oi?
00048   4f 7f e5 de d7 a5 be 3f  ac 18 00 57 5c 04 10 b3    O......?...W\...
00064   0e e9 88 81 03 11 0a 8b  83 cd bc 97 00 67 00 00    .............g..
00080   09 00 00 00 00 ff 01 00  01 00 16 03 03 09 bc 0b    ................
00096   00 09 b8 00 09 b5 00 05  17 30 82 05 13 30 82 03    .........0...0..
00112   fb a0 03 02 01 02 02 10  0d e1 47 7e 3f 3e b2 22    ..........G~?>."
00128   53 6f 57 30 63 d0 91 aa  30 0d 06 09 2a 86 48 86    SoW0c...0...*.H.
00144   f7 0d 01 01 0b 05 00 30  4d 31 0b 30 09 06 03 55    .......0M1.0...U
00160   04 06 13 02 55 53 31 15  30 13 06 03 55 04 0a 13    ....US1.0...U...
00176   0c 44 69 67 69 43 65 72  74 20 49 6e 63 31 27 30    .DigiCert Inc1'0
00192   25 06 03 55 04 03 13 1e  44 69 67 69 43 65 72 74    %..U....DigiCert
00208   20 53 48 41 32 20 53 65  63 75 72 65 20 53 65 72     SHA2 Secure Ser
00224   76 65 72 20 43 41 30 1e  17 0d 31 36 30 36 30 36    ver CA0...160606
00240   30 30 30 30 30 30 5a 17  0d 31 37 30 36 32 38 31    000000Z..1706281
00256   32 30 30 30 30 5a 30 5d  31 0b 30 09 06 03 55 04    20000Z0]1.0...U.
00272   06 13 02 47 42 31 0f 30  0d 06 03 55 04 07 13 06    ...GB1.0...U....
00288   4c 6f 6e 64 6f 6e 31 1c  30 1a 06 03 55 04 0a 13    London1.0...U...
00304   13 43 61 6e 6f 6e 69 63  61 6c 20 47 72 6f 75 70    .Canonical Group
00320   20 4c 74 64 31 1f 30 1d  06 03 55 04 03 13 16 76     Ltd1.0...U....v
00336   69 64 65 6f 73 65 61 72  63 68 2e 75 62 75 6e 74    ideosearch.ubunt
00352   75 2e 63 6f 6d 30 82 01  22 30 0d 06 09 2a 86 48    u.com0.."0...*.H
00368   86 f7 0d 01 01 01 05 00  03 82 01 0f 00 30 82 01    .............0..
00384   0a 02 82 01 01 00 b9 45  e9 20 a8 da a6 34 11 ad    .......E. ...4..
00400   f1 64 da 87 18 90 ec b5  6a f8 f6 6c 39 0f b5 31    .d......j..l9..1
00416   7b 1c 22 4a 65 2c 61 8f  07 cf 25 ff e1 e9 f1 ba    {."Je,a...%.....
00432   4c fe 91 c6 f4 aa 1d 68  e0 3c 5e a5 35 a1 7c 4c    L......h.<^.5.|L
00448   2b d8 72 3d ab 3d 44 f9  93 89 01 ed a0 c7 43 80    +.r=.=D.......C.
00464   d7 d8 97 e4 58 d0 33 4e  11 1d 2b 24 00 d9 f0 3d    ....X.3N..+$...=
00480   de a9 ee be 79 f4 36 3f  20 14 dc 7a 1c ee 69 c4    ....y.6? ..z..i.
00496   22 02 a4 89 25 6e dd bd  6b bd 4b 45 99 a1 81 ac    "...%n..k.KE....
00512   54 28 5c 72 6e e4 97 14  da f1 13 d2 5c 96 61 56    T(\rn.......\.aV
00528   5c ad ac 43 66 46 ae 6a  bc 91 0a 12 90 96 08 a5    \..CfF.j........
00544   1d 56 c2 e9 4c 84 f9 9e  eb 85 94 a1 11 c1 ce 10    .V..L...........
00560   32 82 b2 c9 81 e8 68 d1  f3 a2 a9 e9 63 8b f8 92    2.....h.....c...
00576   15 df 27 69 7c 1f fb f7  15 e0 cc 19 d6 aa e2 e4    ..'i|...........
00592   6c 3b 71 bb 67 26 ce 7a  92 f7 c2 bc e2 50 cb 48    l;q.g&.z.....P.H
00608   54 2a 56 a7 57 18 58 3e  da fc 9a 2c 02 c9 f3 52    T*V.W.X>...,...R
00624   73 02 d8 8d f0 e1 fd 76  43 c9 bd 77 b3 32 f1 d6    s......vC..w.2..
00640   cd ff 18 bf 03 79 02 03  01 00 01 a3 82 01 dd 30    .....y.........0
00656   82 01 d9 30 1f 06 03 55  1d 23 04 18 30 16 80 14    ...0...U.#..0...
```

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

Packet number 1:
       From: 10.0.2.4
         To: 162.213.33.49
   Protocol: TCP
   Src port: 35932
   Dst port: 443

Packet number 2:
       From: 162.213.33.49
         To: 10.0.2.4
   Protocol: TCP
   Src port: 443
   Dst port: 35932

Packet number 3:
       From: 10.0.2.4
         To: 162.213.33.49
   Protocol: TCP
   Src port: 35932
   Dst port: 443

Packet number 4:
       From: 10.0.2.4
         To: 162.213.33.49
   Protocol: TCP
   Src port: 35932
   Dst port: 443
   Payload (148 bytes):
00000   16 03 00 00 8f 01 00 00  8b 03 03 58 ff 8a fb 93    ...........X....
00016   b8 ca b2 20 3c 54 52 92  8c f9 5b 98 44 ad 65 6d    ... <TR...[.D.em
00032   24 8a 9c 6b 80 eb c8 05  72 c1 90 00 00 30 00 33    $..k....r....0.3
00048   00 67 00 45 00 39 00 6b  00 88 00 16 00 32 00 40    .g.E.9.k.....2.@
00064   00 44 00 38 00 6a 00 87  00 13 00 66 00 2f 00 3c    .D.8.j.....f./.<
00080   00 41 00 35 00 3d 00 84  00 0a 00 05 00 04 01 00    .A.5.=..........
00096   00 32 00 00 00 1b 00 19  00 00 16 76 69 64 65 6f    .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 00 0d  00 0a 00 08 04 02 04 01    m...............
00144   02 01 02 02                                        ....
```

```
00672   0f 80 61 1c 82 31 61 d5  2f 28 e7 8d 46 38 b4 2c    ..a..1a./(..F8.,
00688   e1 c6 d9 e2 30 1d 06 03  55 1d 0e 04 16 04 14 cd    ....0...U.......
00704   c8 5c c5 26 d3 bf 4b 30  52 b0 aa 3b 3a 82 d1 4d    .\.&..K0R..;:..M
00720   9a 76 3f 30 21 06 03 55  1d 11 04 1a 30 18 82 16    .v?0!..U....0...
00736   76 69 64 65 6f 73 65 61  72 63 68 2e 75 62 75 6e    videosearch.ubun
00752   74 75 2e 63 6f 6d 30 0e  06 03 55 1d 0f 01 01 ff    tu.com0...U.....
00768   04 04 03 02 05 a0 30 1d  06 03 55 1d 25 04 16 30    ......0...U.%..0
00784   14 06 08 2b 06 01 05 05  07 03 01 06 08 2b 06 01    ...+.........+..
00800   05 05 07 03 02 30 6b 06  03 55 1d 1f 04 64 30 62    .....0k..U...d0b
00816   30 2f a0 2d a0 2b 86 29  68 74 74 70 3a 2f 2f 63    0/.-.+.)http://c
00832   72 6c 33 2e 64 69 67 69  63 65 72 74 2e 63 6f 6d    rl3.digicert.com
00848   2f 73 73 63 61 2d 73 68  61 32 2d 67 35 2e 63 72    /ssca-sha2-g5.cr
00864   6c 30 2f a0 2d a0 2b 86  29 68 74 74 70 3a 2f 2f    l0/.-.+.)http://
00880   63 72 6c 34 2e 64 69 67  69 63 65 72 74 2e 63 6f    crl4.digicert.co
00896   6d 2f 73 73 63 61 2d 73  68 61 32 2d 67 35 2e 63    m/ssca-sha2-g5.c
00912   72 6c 30 4c 06 03 55 1d  20 04 45 30 43 30 37 06    rl0L..U. .E0C07.
00928   09 60 86 48 01 86 fd 6c  01 01 30 2a 30 28 06 08    .`.H...l..0*0(..
00944   2b 06 01 05 05 07 02 01  16 1c 68 74 74 70 73 3a    +.........https:
00960   2f 2f 77 77 77 2e 64 69  67 69 63 65 72 74 2e 63    //www.digicert.c
00976   6f 6d 2f 43 50 53 30 08  06 06 67 81 0c 01 02 02    om/CPS0...g.....
00992   30 7c 06 08 2b 06 01 05  05 07 01 01 04 70 30 6e    0|..+........p0n
01008   30 24 06 08 2b 06 01 05  05 07 30 01 86 18 68 74    0$..+.....0...ht
01024   74 70 3a 2f 2f 6f 63 73  70 2e 64 69 67 69 63 65    tp://ocsp.digice
01040   72 74 2e 63 6f 6d 30 46  06 08 2b 06 01 05 05 07    rt.com0F..+.....
01056   30 02 86 3a 68 74 74 70  3a 2f 2f 63 61 63 65 72    0..:http://cacer
01072   74 73 2e 64 69 67 69 63  65 72 74 2e 63 6f 6d 2f    ts.digicert.com/
01088   44 69 67 69 43 65 72 74  53 48 41 32 53 65 63 75    DigiCertSHA2Secu
01104   72 65 53 65 72 76 65 72  43 41 2e 63 72 74 30 0c    reServerCA.crt0.
01120   06 03 55 1d 13 01 01 ff  04 02 30 00 30 0d 06 09    ..U.......0.0...
01136   2a 86 48 86 f7 0d 01 01  0b 05 00 03 82 01 01 00    *.H.............
01152   c9 62 f6 30 f3 48 f6 f1  6a 14 c5 3a 04 18 2a 9f    .b.0.H..j..:..*.
01168   89 71 f9 10 a4 03 d5 03  6b e3 bb 97 69 b2 29 aa    .q......k...i.).
01184   d9 a9 08 12 91 6d 43 37  3f 98 87 64 83 3a 60 99    .....mC7?..d.:`.
01200   d4 4e d1 c0 b5 94 54 d8  6f 14 42 1d 7d 83 38 96    .N....T.o.B.}.8.
01216   f9 97 81 9c dd c8 e7 d8  17 54 b6 f5 d8 3e e8 48    .........T...>.H
01232   13 35 c5 1c 5b 80 0c e1  3b 18 19 2c 23 40 a4 c7    .5..[...;..,#@..
01248   66 66 ce 7d cc ce 40 4b  84 65 2c 1f 8c 6e ee fd    ff.}..@K.e,..n..
01264   13 5f aa 3a 84 87 2c fd  7b 53 ca ce fd ce 7f a8    ._.:..,.{S......
01280   33 d1 08 39 be d3 7c 0b                            3..9..|.

Packet number 7:
       From: 10.0.2.4
         To: 162.213.33.49
   Protocol: TCP
   Src port: 35932
   Dst port: 443

Packet number 8:
       From: 162.213.33.49
         To: 10.0.2.4
   Protocol: TCP
   Src port: 443
   Dst port: 35932
   Payload (1460 bytes):
```

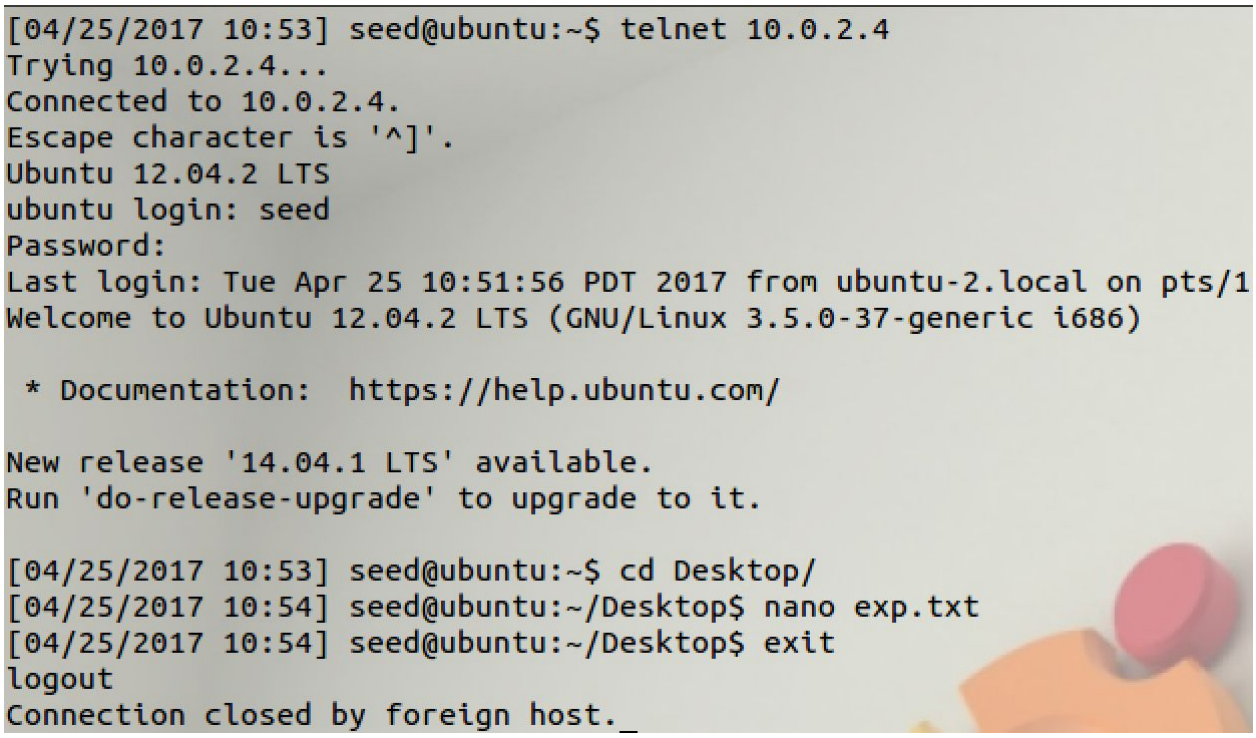
```
00064   5a bd ec 44 b2 8a 28 99  3c 04 d8 8a 93 ea 5f b1    Z..D..(.<....._.
00080   78 90 f1 df 11 6b 6b 9c  45 f6 db 03 3e 8a b7 a4    x....kk.E...>...
00096   51 9d dc 13 91 b3 90 eb  a3 58 ba b3 4c 8d d2 97    Q........X..L...
00112   67 b8 89 56 e8 cf 32 0d  00 04 98 30 82 04 94 30    g..V..2....0...0
00128   82 03 7c a0 03 02 01 02  02 10 01 fd a3 eb 6e ca    ..|...........n.
00144   75 c8 88 43 8b 72 4b cf  bc 91 30 0d 06 09 2a 86    u..C.rK...0...*.
00160   48 86 f7 0d 01 01 0b 05  00 30 61 31 0b 30 09 06    H........0a1.0..
00176   03 55 04 06 13 02 55 53  31 15 30 13 06 03 55 04    .U....US1.0...U.
00192   0a 13 0c 44 69 67 69 43  65 72 74 20 49 6e 63 31    ...DigiCert Inc1
00208   19 30 17 06 03 55 04 0b  13 10 77 77 77 2e 64 69    .0...U....www.di
00224   67 69 63 65 72 74 2e 63  6f 6d 31 20 30 1e 06 03    gicert.com1 0...
00240   55 04 03 13 17 44 69 67  69 43 65 72 74 20 47 6c    U....DigiCert Gl
00256   6f 62 61 6c 20 52 6f 6f  74 20 43 41 30 1e 17 0d    obal Root CA0...
00272   31 33 30 33 30 38 31 32  30 30 30 30 5a 17 0d 32    130308120000Z..2
00288   33 30 33 30 38 31 32 30  30 30 30 5a 30 4d 31 0b    3030812000 0Z0M1.
00304   30 09 06 03 55 04 06 13  02 55 53 31 15 30 13 06    0...U....US1.0..
00320   03 55 04 0a 13 0c 44 69  67 69 43 65 72 74 20 49    .U....DigiCert I
00336   6e 63 31 27 30 25 06 03  55 04 03 13 1e 44 69 67    nc1'0%..U....Dig
00352   69 43 65 72 74 20 53 48  41 32 20 53 65 63 75 72    iCert SHA2 Secur
00368   65 20 53 65 72 76 65 72  20 43 41 30 82 01 22 30    e Server CA0.."0
00384   0d 06 09 2a 86 48 86 f7  0d 01 01 01 05 00 03 82    ...*.H..........
00400   01 0f 00 30 82 01 0a 02  82 01 01 00 dc ae 58 90    ...0..........X.
00416   4d c1 c4 30 15 90 35 5b  6e 3c 82 15 f5 2c 5c bd    M..0..5[n<...,\.
00432   e3 db ff 71 43 fa 64 25  80 d4 ee 18 a2 4d f0 66    ...qC.d%.....M.f
00448   d0 0a 73 6e 11 98 36 17  64 af 37 9d fd fa 41 84    ..sn..6.d.7...A.
00464   af c7 af 8c fe 1a 73 4d  cf 33 97 90 a2 96 87 53    ......sM.3.....S
00480   83 2b b9 a6 75 48 2d 1d  56 37 7b da 31 32 1a d7    .+..uH-.V7{.12..
00496   ac ab 0a f4 aa 5d 4b b7  47 46 dd 2a 93 c3 90 2e    .....]K.GF.*....
00512   79 80 80 ef 13 04 6a 14  3b b5 9b 92 be c2 07 65    y.....j.;......e
00528   4e fc da fc ff 7a ae dc  5c 7e 55 31 0c e8 39 07    N....z..\~U1..9.
00544   a4 d7 be 2f d3 0b 6a d2  b1 df 5f fe 57 74 53 3b    .../..j..._.WtS;
00560   35 80 dd ae 8e 44 98 b3  9f 0e d3 da e0 d7 f4 6b    5....D.........k
00576   29 ab 44 a7 4b 58 84 6d  92 4b 81 c3 da 73 8b 12    ).D.KX.m.K...s..
00592   97 48 90 04 45 75 1a dd  37 31 97 92 e8 cd 54 0d    .H..Eu..71....T.
00608   3b e4 c1 3f 39 5e 2e b8  f3 5c 7e 10 8e 86 41 00    ;..?9^...\~...A.
00624   8d 45 66 47 b0 a1 65 ce  a0 aa 29 09 4e f3 97 eb    .EfG..e...).N...
00640   e8 2e ab 0f 72 a7 30 0e  fa c7 f4 fd 14 77 c3 a4    ....r.0......w..
00656   5b 28 57 c2 b3 f9 82 fd  b7 45 58 9b 02 03 01 00    [(W......EX.....
00672   01 a3 82 01 5a 30 82 01  56 30 12 06 03 55 1d 13    ....Z0..V0...U..
00688   01 01 ff 04 08 30 06 01  01 ff 02 01 00 30 0e 06    .....0.......0..
00704   03 55 1d 0f 01 01 ff 04  04 03 02 01 86 30 34 06    .U...........04.
00720   08 2b 06 01 05 05 07 01  01 04 28 30 26 30 24 06    .+........(0&0$.
00736   08 2b 06 01 05 05 07 30  01 86 18 68 74 74 70 3a    .+.....0...http:
00752   2f 2f 6f 63 73 70 2e 64  69 67 69 63 65 72 74 2e    //ocsp.digicert.
00768   63 6f 6d 30 7b 06 03 55  1d 1f 04 74 30 72 30 37    com0{..U...t0r07
00784   a0 35 a0 33 86 31 68 74  74 70 3a 2f 2f 63 72 6c    .5.3.1http://crl
00800   33 2e 64 69 67 69 63 65  72 74 2e 63 6f 6d 2f 44    3.digicert.com/D
00816   69 67 69 43 65 72 74 47  6c 6f 62 61 6c 52 6f 6f    igiCertGlobalRoo
00832   74 43 41 2e 63 72 6c 30  37 a0 35 a0 33 86 31 68    tCA.crl07.5.3.1h
00848   74 74 70 3a 2f 2f 63 72  6c 34 2e 64 69 67 69 63    ttp://crl4.digic
00864   65 72 74 2e 63 6f 6d 2f  44 69 67 69 43 65 72 74    ert.com/DigiCert
00880   47 6c 6f 62 61 6c 52 6f  6f 74 43 41 2e 63 72 6c    GlobalRootCA.crl
00896   30 3d 06 03 55 1d 20 04  36 30 34 30 32 06 04 55    0=..U. .60402..U
00912   1d 20 00 30 2a 30 28 06  08 2b 06 01 05 05 07 02    . .0*0(..+......
00928   01 16 1c 68 74 74 70 73  3a 2f 2f 77 77 77 2e 64    ...https://www.d
00944   69 67 69 63 65 72 74 2e  63 6f 6d 2f 43 50 53 30    igicert.com/CPS0
```

```
00928   01 16 1c 68 74 74 70 73  3a 2f 2f 77 77 77 2e 64    ...https://www.d
00944   69 67 69 63 65 72 74 2e  63 6f 6d 2f 43 50 53 30    igicert.com/CPS0
00960   1d 06 03 55 1d 0e 04 16  04 14 0f 80 61 1c 82 31    ...U........a..1
00976   61 d5 2f 28 e7 8d 46 38  b4 2c e1 c6 d9 e2 30 1f    a./(..F8.,....0.
00992   06 03 55 1d 23 04 18 30  16 80 14 03 de 50 35 56    ..U.#..0.....P5V
01008   d1 4c bb 66 f0 a3 e2 1b  1b c3 97 b2 3d d1 55 30    .L.f........=.U0
01024   0d 06 09 2a 86 48 86 f7  0d 01 01 0b 05 00 03 82    ...*.H..........
01040   01 01 00 23 3e df 4b d2  31 42 a5 b6 7e 42 5c 1a    ...#>.K.1B..~B\.
01056   44 cc 69 d1 68 b4 5d 4b  e0 04 21 6c 4b e2 6d cc    D.i.h.]K..!lK.m.
01072   b1 e0 97 8f a6 53 09 cd  aa 2a 65 e5 39 4f 1e 83    .....S...*e.9O..
01088   a5 6e 5c 98 a2 24 26 e6  fb a1 ed 93 c7 2e 02 c6    .n\..$&.........
01104   4d 4a bf b0 42 df 78 da  b3 a8 f9 6d ff 21 85 53    MJ..B.x....m.!.S
01120   36 60 4c 76 ce ec 38 dc  d6 51 80 f0 c5 d6 e5 d4    6`Lv..8..Q......
01136   4d 27 64 ab 9b c7 3e 71  fb 48 97 b8 33 6d c9 13    M'd...>q.H..3m..
01152   07 ee 96 a2 1b 18 15 f6  5c 4c 40 ed b3 c2 ec ff    ........\L@.....
01168   71 c1 e3 47 ff d4 b9 00  b4 37 42 da 20 c9 ea 6e    q..G.....7B. ..n
01184   8a ee 14 06 ae 7d a2 59  98 88 a8 1b 6f 2d f4 f2    .....}.Y....o-..
01200   c9 14 5f 26 cf 2c 8d 7e  ed 37 c0 a9 d5 39 b9 82    .._&.,.~.7...9..
01216   bf 19 0c ea 34 af 00 21  68 f8 ad 73 e2 c9 32 da    ....4..!h..s..2.
01232   38 25 0b 55 d3 9a 1d f0  68 86 ed 2e 41 34 ef 7c    8%.U....h...A4.|
01248   a5 50 1d bf 3a f9 d3 c1  08 0c e6 ed 1e 8a 58 25    .P..:.........X%
01264   e4 b8 77 ad 2d 6e f5 52  dd b4 74 8f ab 49 2e 9d    ..w.-n.R..t..I..
01280   3b 93 34 28 1f 78 ce 94  ea c7 bd d3 c9 6d 1c de    ;.4(.x.......m..
01296   5c 32 f3 16 03 03 03 0f  0c 00 03 0b 01 00 b8 12    \2..............
01312   23 3c 57 7e c8 d5 03 9e  ad e6 4a b6 08 60 88 57    #<W~......J..`.W
01328   97 e3 5f 39 06 92 f0 ee  1f f7 b2 21 98 15 c3 ef    .._9.......!....
01344   e5 29 cc 66 c6 23 4b eb  d4 88 0b 0e 35 7e 8a 38    .).f.#K.....5~.8
01360   0f 8e 90 3f 11 ac 03 56  1c 40 1a 7a 34 82 1c a6    ...?...V.@.z4...
01376   ce d9 48 db 9b a1 1c cb  2a 88 31 2a e6 cc b1 04    ..H.....*.1*....
01392   1f fc 48 4c 1b 70 73 c1  13 0b ff 36 06 ae 0c 5f    ..HL.ps....6...._
01408   02 b0 84 32 fc b7 e3 76  a0 37 76 ff 23 46 81 b1    ...2...v.7v.#F..
01424   23 20 95 82 39 e2 0e 58  d1 e9 b0 0b ab 03 07 5f    # ..9..X........_
01440   20 3f 03 55 ae fd 92 44  7e 00 30 58 04 de d8 e4     ?.U...D~.0X....
01456   a6 32 82 d4                                        .2..

Packet number 9:
       From: 10.0.2.4
         To: 162.213.33.49
   Protocol: TCP
   Src port: 35932
   Dst port: 443

Packet number 10:
       From: 162.213.33.49
         To: 10.0.2.4
   Protocol: TCP
   Src port: 443
   Dst port: 35932
   Payload (636 bytes):
00000   ce cb b2 3b 2f 45 38 c7  13 26 e2 99 e9 7e fb 9d    ...;/E8..&...~..
00016   74 6c 39 ef c4 45 95 e1  65 85 fd fc b3 55 e5 d1    tl9..E..e....U..
00032   54 a8 d5 43 33 44 b2 7a  36 be 6f db 0b 1d f3 05    T..C3D.z6.o.....
00048   33 ff 0c f1 34 5d f7 e1  23 34 02 f2 da ea 12 d5    3...4]..#4......
00064   58 a5 4a af 11 42 fc fc  e6 64 34 a4 e4 ef 56 30    X.J..B...d4...V0
00080   fd a6 81 35 5c 88 2b 0b  b1 e4 ff fc ac 22 61 ed    ...5\.+......"a.
00096   ec f3 92 37 97 a1 48 64  2c a3 00 01 02 01 00 21    ...7..Hd,......!
```

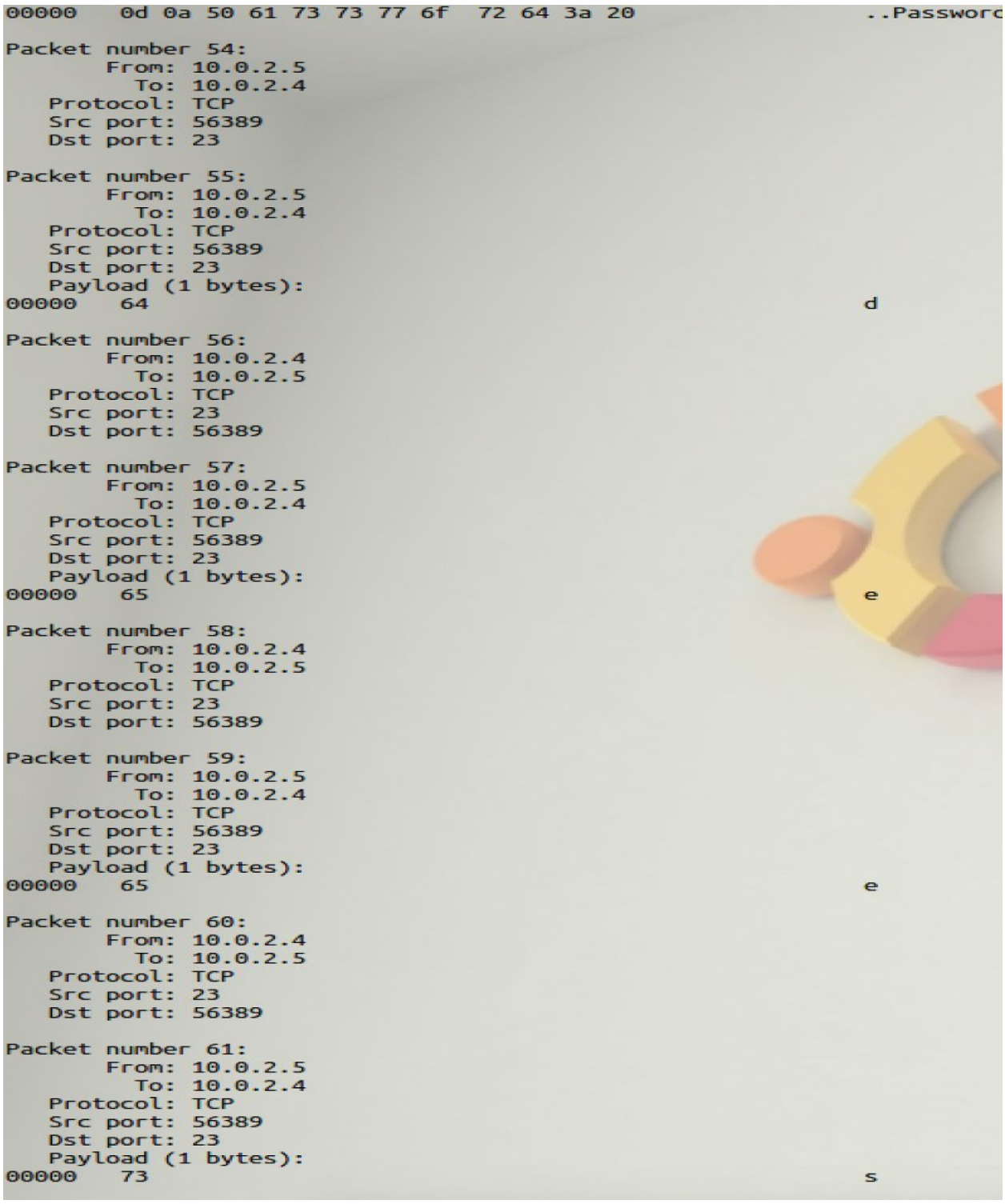
```
00320   4f b9 b2 6d 79 8f ae ef  dc a0 97 42 90 de 53 7f    O..my......B..S.
00336   00 7d 64 b8 84 50 92 83  25 fd 7a 86 0a 33 0e af    .}d..P..%.z..3..
00352   00 dc bd 5a bf 39 2f 69  c5 9a 25 df 43 76 84 04    ...Z.9/i..%.Cv..
00368   01 01 00 9b 33 b8 af c5  b3 dd 09 8c 5c 57 cd 3c    ....3.......\W.<
00384   32 d4 f6 f6 dc 3b 2a 9b  0b 63 4d 87 7d 3f 1d ce    2....;*..cM.}?..
00400   7b e2 72 c0 4b cb d7 57  6e ee 97 f6 84 0b ec 62    {.r.K..Wn......b
00416   ae 16 18 5b 3a 64 8c 3b  9a 98 49 df c9 52 e0 7b    ...[:d.;..I..R.{
00432   51 15 09 12 3a 57 b4 2c  7c 43 de 8f a6 56 0c 81    Q...:W.,|C...V..
00448   3e b2 1e 88 f9 05 d7 81  51 11 0e 24 5f d9 42 76    >.......Q..$_.Bv
00464   f7 1e 66 26 35 46 7e 14  ec e5 9b 9e ee 58 99 04    ..f&5F~......X..
00480   5c 5d 50 53 c0 ce 49 fc  5e 14 79 db 94 01 bd f3    \]PS..I.^.y.....
00496   45 32 9e 28 5a 67 13 e8  f2 08 b1 f3 a3 3c 67 a8    E2.(Zg.......<g.
00512   58 d7 11 f3 b7 08 75 1b  0d 45 90 f5 fa 9d 55 e2    X.....u..E....U.
00528   14 13 8d c6 a2 84 05 22  46 4a e9 82 d9 76 1c 18    .......FJ...v..
00544   16 17 e2 75 5a 67 5b 13  54 93 02 d4 52 32 39 4d    ...uZg[.T...R29M
00560   78 38 aa 43 06 14 b4 23  7a 2d a9 40 58 c2 7c 28    x8.C...#z-.@X.|(
00576   4c d4 be e8 90 ea 12 dd  1b cd 40 9b 3f 04 e0 39    L.........@.?..9
00592   bf 87 de 89 fb 21 d8 17  f8 1a f3 7c 0f 90 02 d4    .....!.....|....
00608   28 e0 2f 26 64 de 72 84  dd 04 ab b1 6c 28 4c 7e    (./&d.r.....l(L~
00624   53 97 ae 16 03 03 00 04  0e 00 00 00                S...........

Capture complete.
```

Problem #3: Password Sniffing

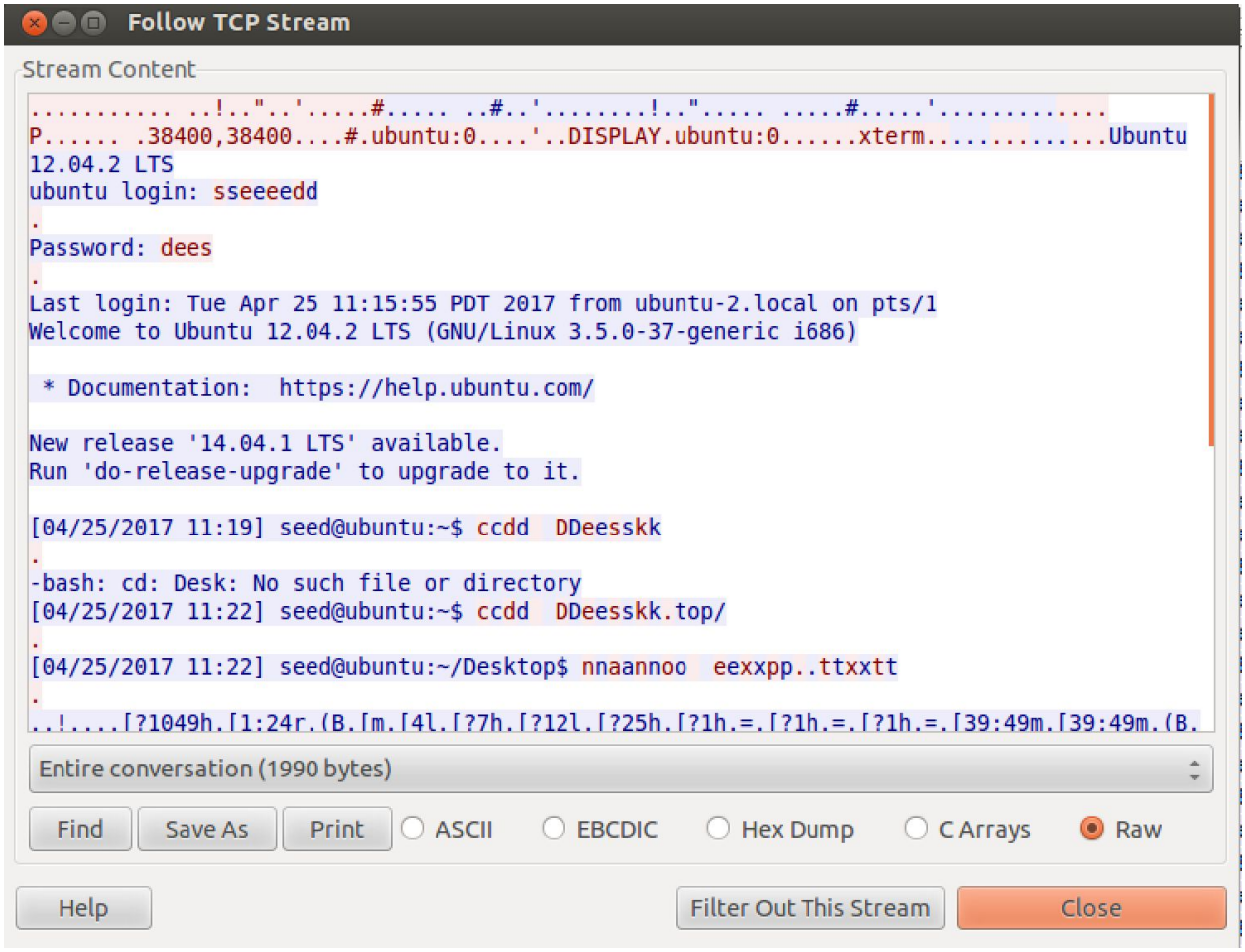
First we used Telnet to remotely access one VM from the other and create a text file on its desktop.



Then we repeated the above process while running our packet sniffer, and we were able to see the password “dees”:



This experiment was run again, but this time using Wireshark instead of our own packet sniffer:



And we can see all of the commands typed into the terminal which we were using to access the VM remotely, including the password.

The above experiment would lead us to the conclusion that Telnet is not a very secure method of communication, since it is very easy to monitor the traffic on the connection, which can be used to obtain sensitive information, like login information.

Problem #4: SSH

We tried again to use wireshark to see the communication that was occurring between the two VMs. But, since this time we were using SSH instead of telnet, the information was encrypted, so we could not find the password. This is why SSH is used today to remotely access systems, and not Telnet.