CS380 — Exercise 5

Problem 1: Verifying the Network


```
[05/09/2017 21:11] seed@ubuntu:~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:11:f5:29
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:f529/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:56353 (56.3 KB)  TX bytes:24372 (24.3 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:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4965 (4.9 KB)  TX bytes:4965 (4.9 KB)

[05/09/2017 21:11] seed@ubuntu:~$
```
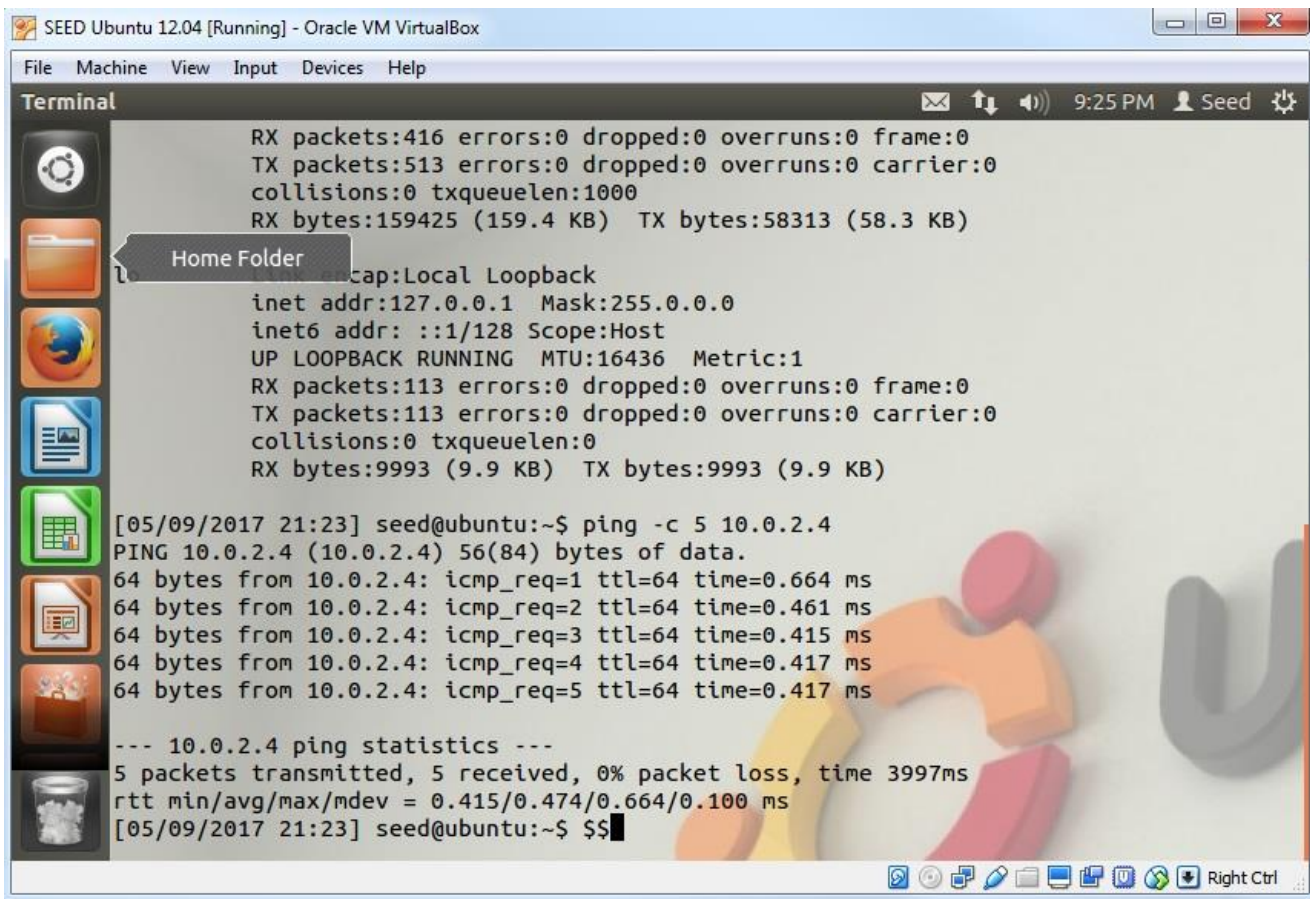


```
[05/09/2017 21:11] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:fc:aa:d2
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.25
5.0
          inet6 addr: fe80::a00:27ff:fefc:aad2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:177 errors:0 dropped:0 overruns:0 carrier:
0
          collisions:0 txqueuelen:1000
          RX bytes:43969 (43.9 KB)  TX bytes:22088 (22.0 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)

[05/09/2017 21:12] seed@ubuntu:~$
```

Verifying connection


```
             RX packets:416 errors:0 dropped:0 overruns:0 frame:0
             TX packets:513 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:159425 (159.4 KB)  TX bytes:58313 (58.3 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:113 errors:0 dropped:0 overruns:0 frame:0
             TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:9993 (9.9 KB)  TX bytes:9993 (9.9 KB)

[05/09/2017 21:23] 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=0.664 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.461 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.415 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.417 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.417 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.415/0.474/0.664/0.100 ms
[05/09/2017 21:23] seed@ubuntu:~$ $$
```
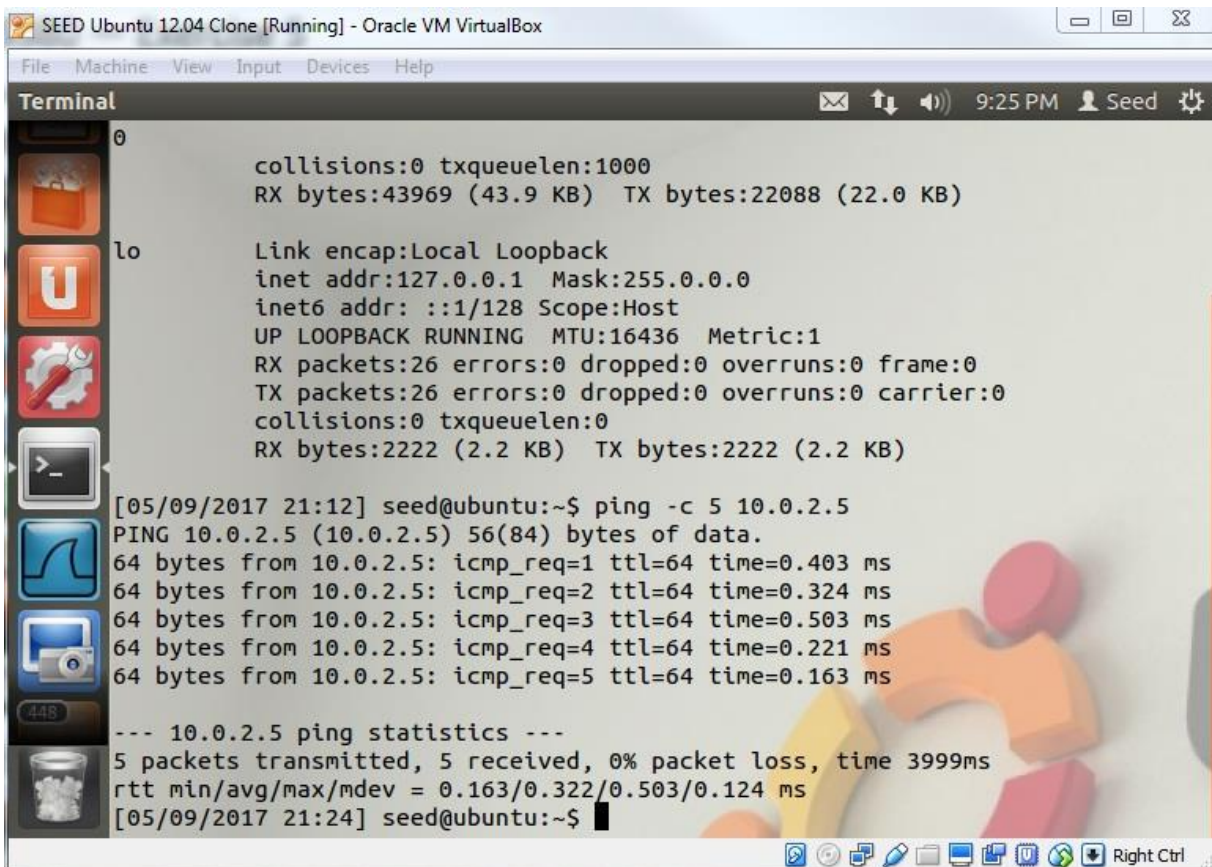


```
0
             collisions:0 txqueuelen:1000
             RX bytes:43969 (43.9 KB)  TX bytes:22088 (22.0 KB)

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)

[05/09/2017 21:12] 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=0.403 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.324 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.503 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.221 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.163 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.163/0.322/0.503/0.124 ms
[05/09/2017 21:24] seed@ubuntu:~$
```

Problem 2: Writing a Packet Sniffer

```
⊗ ⊖ ▢   Terminal
[05/09/2017 22:25] 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: 162.213.33.48
   Protocol: TCP
   Src port: 46322
   Dst port: 443

Packet number 2:
      From: 162.213.33.48
        To: 10.0.2.5
   Protocol: TCP
   Src port: 443
   Dst port: 46322

Packet number 3:
      From: 10.0.2.5
        To: 162.213.33.48
   Protocol: TCP
   Src port: 46322
   Dst port: 443

Packet number 4:
      From: 10.0.2.5
        To: 162.213.33.48
   Protocol: TCP
   Src port: 46322
   Dst port: 443
   Payload (148 bytes):
00000    16 03 00 00 8f 01 00 00   8b 03 03 59 12 a4 6b 81    ...........Y..k.
00016    47 74 a4 06 4a 16 8e 01   0f 7d b4 4e a0 f1 1a 7d    Gt..J....}.N...}
00032    61 0d 63 30 5e 1d f1 be   1a c1 98 00 00 30 00 33    a.c0^........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                                           ....
```

```
Terminal

Packet number 5:
        From: 162.213.33.48
          To: 10.0.2.5
   Protocol: TCP
   Src port: 443
   Dst port: 46322

Packet number 6:
        From: 162.213.33.48
          To: 10.0.2.5
   Protocol: TCP
   Src port: 443
   Dst port: 46322
   Payload (1460 bytes):
00000    16 03 03 00 55 02 00 00   51 03 03 5e e2 b8 ed 9d    ....U...Q..^....
00016    f4 57 6e c5 f2 39 32 10   cc 12 2e 67 f0 9a 6c 5d    .Wn..92....g..l]
00032    76 10 6d 58 60 7c ff 5b   24 46 63 20 e3 35 8d 45    v.mX`|.[$Fc .5.E
00048    eb 2d 74 fb 2c 80 64 c6   af d9 f7 9c c4 8b d0 62    .-t.,.d........b
00064    ce d8 7d 7b e0 c1 f8 8d   c1 38 63 31 00 67 00 00    ..}{.....8c1.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
```

```
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...
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   74 a5 67 c3 52 50 b1 4c    3..9..|.t.g.RP.L
01296    c7 19 c5 1e b9 af 01 77   40 9c 13 5f d2 68 15 22    .......w@.._.h."
01312    96 9d ed 9f 0a 57 10 b1   51 d6 31 c7 a6 2e 41 44    .....W..Q.1...AD
```

```
01376    45 f6 db 03 3e 8a b7 a4    51 9d dc 13 91 b3 90 eb    E...>...Q.......
01392    a3 58 ba b3 4c 8d d2 97    67 b8 89 56 e8 cf 32 0d    .X..L...g..V..2.
01408    00 04 98 30 82 04 94 30    82 03 7c a0 03 02 01 02    ...0...0..|.....
01424    02 10 01 fd a3 eb 6e ca    75 c8 88 43 8b 72 4b cf    ......n.u..C.rK.
01440    bc 91 30 0d 06 09 2a 86    48 86 f7 0d 01 01 0b 05    ..0...*.H.......
01456    00 30 61 31                                           .0a1


Packet number 7:
        From: 10.0.2.5
          To: 162.213.33.48
    Protocol: TCP
    Src port: 46322
    Dst port: 443


Packet number 8:
        From: 162.213.33.48
          To: 10.0.2.5
    Protocol: TCP
    Src port: 443
    Dst port: 46322
    Payload (1460 bytes):
00000    0b 30 09 06 03 55 04 06    13 02 55 53 31 15 30 13    .0...U....US1.0.
00016    06 03 55 04 0a 13 0c 44    69 67 69 43 65 72 74 20    ..U....DigiCert
00032    49 6e 63 31 19 30 17 06    03 55 04 0b 13 10 77 77    Inc1.0...U....ww
00048    77 2e 64 69 67 69 63 65    72 74 2e 63 6f 6d 31 20    w.digicert.com1
00064    30 1e 06 03 55 04 03 13    17 44 69 67 69 43 65 72    0...U....DigiCer
00080    74 20 47 6c 6f 62 61 6c    20 52 6f 6f 74 20 43 41    t Global Root CA
00096    30 1e 17 0d 31 33 30 33    30 38 31 32 30 30 30 30    0...130308120000
00112    5a 17 0d 32 33 30 33 30    38 31 32 30 30 30 30 5a    Z..230308120000Z
00128    30 4d 31 0b 30 09 06 03    55 04 06 13 02 55 53 31    0M1.0...U....US1
00144    15 30 13 06 03 55 04 0a    13 0c 44 69 67 69 43 65    .0...U....DigiCe
00160    72 74 20 49 6e 63 31 27    30 25 06 03 55 04 03 13    rt Inc1'0%..U...
00176    1e 44 69 67 69 43 65 72    74 20 53 48 41 32 20 53    .DigiCert SHA2 S
00192    65 63 75 72 65 20 53 65    72 76 65 72 20 43 41 30    ecure Server CA0
00208    82 01 22 30 0d 06 09 2a    86 48 86 f7 0d 01 01 01    .."0...*.H......
00224    05 00 03 82 01 0f 00 30    82 01 0a 02 82 01 01 00    .......0........
00240    dc ae 58 90 4d c1 c4 30    15 90 35 5b 6e 3c 82 15    ..X.M..0..5[n<..
00256    f5 2c 5c bd e3 db ff 71    43 fa 64 25 80 d4 ee 18    .,\....qC.d%....
00272    a2 4d f0 66 d0 0a 73 6e    11 98 36 17 64 af 37 9d    .M.f..sn..6.d.7.
00288    fd fa 41 84 af c7 af 8c    fe 1a 73 4d cf 33 97 90    ..A.......sM.3..
00304    a2 96 87 53 83 2b b9 a6    75 48 2d 1d 56 37 7b da    ...S.+..uH-.V7{.
00320    31 32 1a d7 ac ab 06 f4    aa 5d 4b b7 47 46 dd 2a    12.......]K.GF.*
00336    93 c3 90 2e 79 80 80 ef    13 04 6a 14 3b b5 9b 92    ....y.....j.;...
00352    be c2 07 65 4e fc da fc    ff 7a ae dc 5c 7e 55 31    ...eN....z..\~U1
00368    0c e8 39 07 a4 d7 be 2f    d3 0b 6a d2 b1 df 5f fe    ..9..../..j..._.
00384    57 74 53 3b 35 80 dd ae    8e 44 98 b3 9f 0e d3 da    WtS;5....D......
00400    e0 d7 f4 6b 29 ab 44 a7    4b 58 84 6d 92 4b 81 c3    ...k).D.KX.m.K..
```

```
00832    de 50 35 56 d1 4c bb 66   f0 a3 e2 1b 1b c3 97 b2    .P5V.L.f........
00848    3d d1 55 30 0d 06 09 2a   86 48 86 f7 0d 01 01 0b    =.U0...*.H......
00864    05 00 03 82 01 01 00 23   3e df 4b d2 31 42 a5 b6    .......#>.K.1B..
00880    7e 42 5c 1a 44 cc 69 d1   68 b4 5d 4b e0 04 21 6c    ~B\.D.i.h.]K..!l
00896    4b e2 6d cc b1 e0 97 8f   a6 53 09 cd aa 2a 65 e5    K.m......S...*e.
00912    39 4f 1e 83 a5 6e 5c 98   a2 24 26 e6 fb a1 ed 93    9O...n\..$&.....
00928    c7 2e 02 c6 4d 4a bf b0   42 df 78 da b3 a8 f9 6d    ....MJ..B.x....m
00944    ff 21 85 53 36 60 4c 76   ce ec 38 dc d6 51 80 f0    .!.S6`Lv..8..Q..
00960    c5 d6 e5 d4 4d 27 64 ab   9b c7 3e 71 fb 48 97 b8    ....M'd...>q.H..
00976    33 6d c9 13 07 ee 96 a2   1b 18 15 f6 5c 4c 40 ed    3m..........\L@.
00992    b3 c2 ec ff 71 c1 e3 47   ff d4 b9 00 b4 37 42 da    ....q..G.....7B.
01008    20 c9 ea 6e 8a ee 14 06   ae 7d a2 59 98 88 a8 1b     ..n......}.Y....
01024    6f 2d f4 f2 c9 14 5f 26   cf 2c 8d 7e ed 37 c0 a9    o-...._&.,.~.7..
01040    d5 39 b9 82 bf 19 0c ea   34 af 00 21 68 f8 ad 73    .9......4..!h..s
01056    e2 c9 32 da 38 25 0b 55   d3 9a 1d f0 68 86 ed 2e    ..2.8%.U....h...
01072    41 34 ef 7c a5 50 1d bf   3a f9 d3 c1 08 0c e6 ed    A4.|.P..:.......
01088    1e 8a 58 25 e4 b8 77 ad   2d 6e f5 52 dd b4 74 8f    ..X%..w.-n.R..t.
01104    ab 49 2e 9d 3b 93 34 28   1f 78 ce 94 ea c7 bd d3    .I..;.4(.x......
01120    c9 6d 1c de 5c 32 f3 16   03 03 03 0f 0c 00 03 0b    .m..\2..........
01136    01 00 b8 12 23 3c 57 7e   c8 d5 03 9e ad e6 4a b6    ....#<W~......J.
01152    08 60 88 57 97 e3 5f 39   06 92 f0 ee 1f f7 b2 21    .`.W.._9.......!
01168    98 15 c3 ef e5 29 cc 66   c6 23 4b eb d4 88 0b 0e    .....).f.#K.....
01184    35 7e 8a 38 0f 8e 90 3f   11 ac 03 56 1c 40 1a 7a    5~.8...?...V.@.z
01200    34 82 1c a6 ce d9 48 db   9b a1 1c cb 2a 88 31 2a    4.....H.....*.1*
01216    e6 cc b1 04 1f fc 48 4c   1b 70 73 c1 13 0b ff 36    ......HL.ps....6
01232    06 ae 0c 5f 02 b0 84 32   fc b7 e3 76 a0 37 76 ff    ..._...2...v.7v.
01248    23 46 81 b1 23 20 95 82   39 e2 0e 58 d1 e9 b0 0b    #F..# ..9..X....
01264    ab 03 07 5f 20 3f 03 55   ae fd 92 44 7e 00 30 58    ..._ ?.U...D~.0X
01280    04 de d8 e4 a6 32 82 d4   ce cb b2 3b 2f 45 38 c7    .....2.....;/E8.
01296    13 26 e2 99 e9 7e fb 9d   74 6c 39 ef c4 45 95 e1    .&...~..tl9..E..
01312    65 85 fd fc b3 55 e5 d1   54 a8 d5 43 33 44 b2 7a    e....U..T..C3D.z
01328    36 be 6f db 0b 1d f3 05   33 ff 0c f1 34 5d f7 e1    6.o.....3...4]..
01344    23 34 02 f2 da ea 12 d5   58 a5 4a af 11 42 fc fc    #4......X.J..B..
01360    e6 64 34 a4 e4 ef 56 30   fd a6 81 35 5c 88 2b 0b    .d4...V0...5\.+.
01376    b1 e4 ff fc ac 22 61 ed   ec f3 92 37 97 a1 48 64    ....."a....7..Hd
01392    2c a3 00 01 02 01 00 15   bc 4b b4 6b c5 f2 da a6    ,........K.k....
01408    7b 93 87 34 9a ba 41 3d   89 7e 5a 4b e5 f5 9f 80    {..4..A=.~ZK....
01424    36 0e 27 e9 2c 5f 69 4d   80 ba 76 01 1d 45 3c 9f    6.'.,_iM..v..E<.
01440    4d cc 59 4b 4e b0 ed c8   e2 0b 4a 4e 92 ae 69 c1    M.YKN.....JN..i.
01456    27 c6 38 8e                                          '.8.

Packet number 9:
        From: 10.0.2.5
          To: 162.213.33.48
   Protocol: TCP
   Src port: 46322
   Dst port: 443
```

```
Packet number 10:
        From: 162.213.33.48
          To: 10.0.2.5
    Protocol: TCP
    Src port: 443
    Dst port: 46322
    Payload (464 bytes):
00000    83 6d d6 45 9d 6a 6e 31    1d 08 d3 4a 3e 58 37 95    .m.E.jn1...J>X7.
00016    cf 6e 3d 08 e5 f4 b7 2d    1e c1 8d 67 da d7 65 54    .n=....-...g..eT
00032    dd 85 cf 3e 19 63 b1 0c    8a 2d 3a 44 f6 f7 f4 ef    ...>.c...-:D....
00048    e0 d3 c0 30 b5 e1 fb e1    d4 f3 54 ab 0c fb 63 d5    ...0......T...c.
00064    11 aa a8 b2 fc 26 22 a8    7a 50 b7 0f f2 56 9c dc    .....&".zP...V..
00080    46 03 7e ec f7 b0 b6 25    22 17 d2 bc 3e 5b 38 be    F.~....%"...>[8.
00096    f6 75 37 c5 c3 37 d4 10    68 cf 1c 52 a9 39 31 28    .u7..7..h..R.91(
00112    fa 11 ec 23 88 1a 49 c2    c1 c7 4f 37 55 bf 6a 83    ...#..I...O7U.j.
00128    78 98 48 d9 65 5b ed ab    1a be 73 e6 a6 0e b0 ed    x.H.e[....s.....
00144    eb 5d b1 6d 95 c8 9f 44    d7 01 d3 f4 4b c4 30 61    .].m...D....K.0a
00160    e9 4a 39 de f5 1c 96 0c    5f 4e e4 79 f5 e6 5c 42    .J9....._N.y..\B
00176    e2 cd b4 f7 d3 77 3a ec    d7 7a a0 cf 87 f9 5c e2    .....w:..z....\.
00192    cd ce a4 04 01 01 00 03    de 11 05 68 41 ee e9 71    ...........hA..q
00208    f6 6d 85 73 ed 1a 77 d6    50 cb 59 4e 64 de 7e 3a    .m.s..w.P.YNd.~:
00224    2e 45 03 fd 8b 5e a6 0e    da 50 e3 ae 91 d0 74 5b    .E...^...P....t[
00240    a3 5d e2 54 7b 30 5a d8    7e 53 13 55 82 b3 82 95    .].T{0Z.~S.U....
00256    23 09 c2 59 c5 0b b9 69    09 93 cd 53 54 67 59 49    #..Y...i...STgYI
00272    cd fb 7e 66 80 6d d6 da    c1 5f 25 67 fc 80 3e 28    ..~f.m..._%g..>(
00288    95 3a 74 03 c6 97 5e 9d    eb aa 97 11 65 7d 2f df    .:t...^.....e}/.
00304    8a 97 87 e2 3d f1 a4 f0    af d0 c6 b6 0b ac ff 80    ....=...........
00320    79 9e 37 23 be b8 48 7c    34 8e 36 79 a0 c0 9f a1    y.7#..H|4.6y....
00336    7a 0c b0 d1 6e f5 56 69    84 d2 dc b1 95 2e 44 66    z...n.Vi......Df
00352    ee 73 14 7f 75 96 bc fb    e9 28 ca d3 6d ab 44 aa    .s..u....(..m.D.
00368    68 9f 0f 2b 3c 8c 28 f4    0a ae f8 46 f1 c3 a2 07    h..+<.(....F....
00384    02 3f 90 0a 48 0b 1e 36    74 cf 90 fc ec 76 e5 82    .?..H..6t....v..
00400    d1 81 18 20 a7 38 db c5    23 6c 0b 62 70 c4 58 94    ... .8..#l.bp.X.
00416    0c b8 42 a6 b0 0e 03 79    c8 e0 b3 5d ab 95 8c 47    ..B....y...]...G
00432    77 a1 d3 75 96 20 0f 81    43 0a 1c 61 23 aa af 90    w..u. ..C..a#...
00448    e0 6f 69 70 eb 8f 87 16    03 03 00 04 0e 00 00 00    .oip...........

Capture complete.
[05/09/2017 22:26] seed@ubuntu:~/Downloads$ $
```

```
[05/09/2017 22:22] 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=0.699 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.412 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.396 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.418 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.361 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.361/0.457/0.699/0.123 ms
[05/09/2017 22:23] 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=0.385 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.399 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.413 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.404 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.428 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.385/0.405/0.428/0.029 ms
[05/09/2017 22:23] seed@ubuntu:~$
                                                    Right C
```

The sniffer Program with TCP gives information of the packets.

Problem 3: Password Sniffing

```
[05/09/2017 22:26] seed@ubuntu:~/Downloads$ sudo service openbsd-inetd start
 * Starting internet superserver inetd                                  [ OK ]
[05/09/2017 22:30] seed@ubuntu:~/Downloads$
```

```
[05/09/2017 22:33] seed@ubuntu:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
```

Problem 4: SSH

2:10 PM ⦿ Seed

Filter: List the available capture interfaces...   Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length
61	2017-05-02 14:08:51.29	10.0.2.4	10.0.2.5	TCP	114
62	2017-05-02 14:08:51.29	10.0.2.5	10.0.2.4	TCP	66
63	2017-05-02 14:08:51.55	10.0.2.5	10.0.2.4	TCP	130
64	2017-05-02 14:08:51.56	10.0.2.4	209.18.47.62	DNS	81
65	2017-05-02 14:08:51.58	209.18.47.62	10.0.2.4	DNS	140
66	2017-05-02 14:08:51.59	10.0.2.4	10.0.2.5	TCP	66
67	2017-05-02 14:08:51.68	fe80::a00:27ff:fe11:f!	ff02::fb	MDNS	101
68	2017-05-02 14:08:51.68	10.0.2.4	224.0.0.251	MDNS	81
69	2017-05-02 14:08:51.68	10.0.2.5	224.0.0.251	MDNS	103
70	2017-05-02 14:08:51.78	fe80::a00:27ff:fe11:f!	ff02::fb	MDNS	94
71	2017-05-02 14:08:51.78	10.0.2.4	224.0.0.251	MDNS	74
72	2017-05-02 14:08:51.78	10.0.2.5	224.0.0.251	MDNS	84
73	2017-05-02 14:08:51.78	10.0.2.4	10.0.2.5	TCP	130
74	2017-05-02 14:08:51.79	10.0.2.5	10.0.2.4	TCP	66
75	2017-05-02 14:08:52.68	10.0.2.4	209.18.47.62	DNS	76
76	2017-05-02 14:08:52.71	209.18.47.62	10.0.2.4	DNS	108
77	2017-05-02 14:08:55.91	10.0.2.5	10.0.2.4	TCP	210
78	2017-05-02 14:08:55.91	10.0.2.4	10.0.2.5	TCP	66
79	2017-05-02 14:08:55.94	10.0.2.4	10.0.2.5	TCP	98
80	2017-05-02 14:08:55.94	10.0.2.5	10.0.2.4	TCP	66
81	2017-05-02 14:08:55.94	10.0.2.5	10.0.2.4	TCP	194
82	2017-05-02 14:08:55.95	10.0.2.4	10.0.2.5	TCP	66

⬤ Invalid filter: "d" is neither a field nor   Packets: 189 Displayed: 189 Mar   Profile: Default

```
[05/02/2017 14:08] seed@ubuntu:~$ ssh seed@10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' can't be established.
ECDSA key fingerprint is 81:82:a9:af:bd:93:78:f9:1a:a7:ca:7f:e8:d6:6c:04.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.4' (ECDSA) to the list of known hosts.
seed@10.0.2.4's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue May  2 14:05:29 2017 from ubuntu-2.local
[05/02/2017 14:08] seed@ubuntu:~$
```