

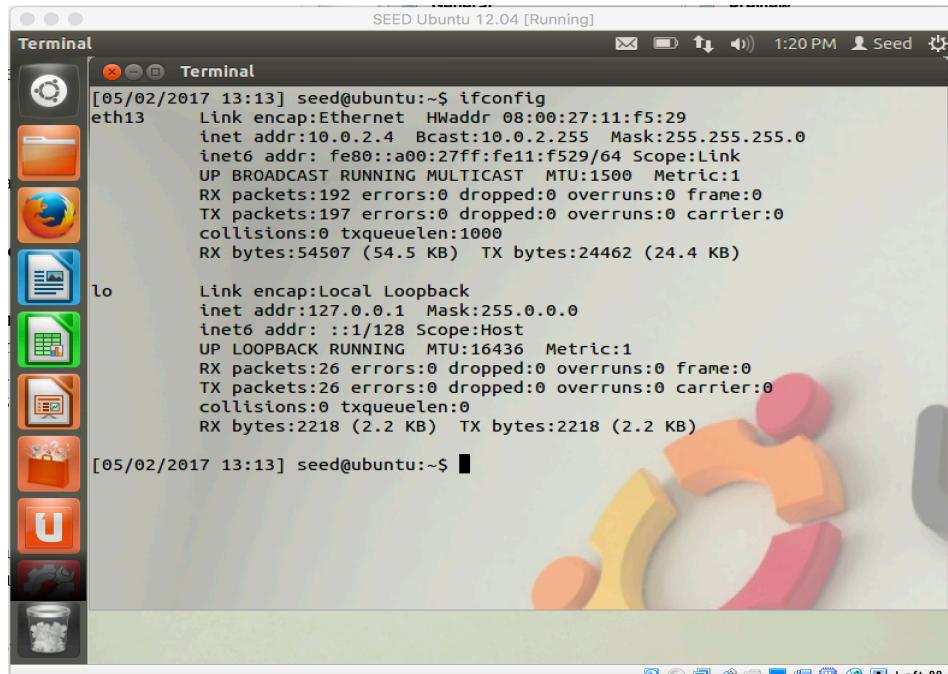
CS380-EX5

Christian Kim

Problem 1: Verifying the Network

Verified unique addresses

SEED – 10.0.2.4 (eth13) Clone – 10.0.2.5 (eth0)

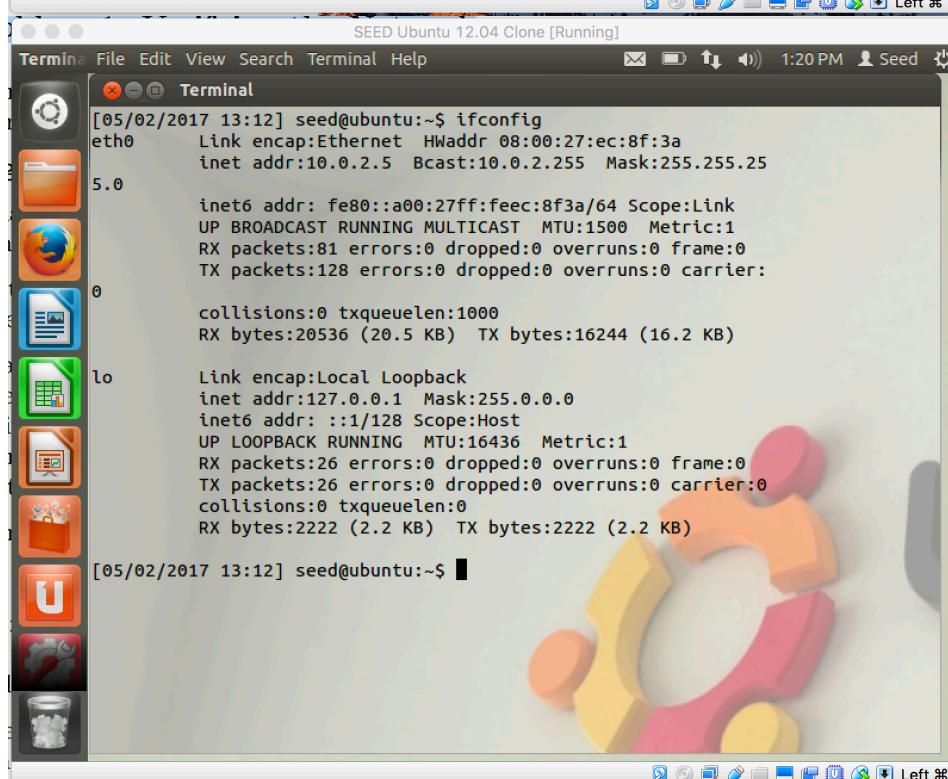


Terminal

```
[05/02/2017 13:13] 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:255.255.255.0
           inet6 addr: fe80::a00:27ff:fe11:f529/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:192 errors:0 dropped:0 overruns:0 frame:0
             TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:54507 (54.5 KB) TX bytes:24462 (24.4 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:2218 (2.2 KB) TX bytes:2218 (2.2 KB)

[05/02/2017 13:13] seed@ubuntu:~$
```



Terminal

```
[05/02/2017 13:12] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:ec:8f:3a
           inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:feec:8f3a/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:81 errors:0 dropped:0 overruns:0 frame:0
             TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:20536 (20.5 KB) TX bytes:16244 (16.2 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)

[05/02/2017 13:12] seed@ubuntu:~$
```

Verifying connection through pings. Working.

SEED Ubuntu 12.04 [Running]

Terminal

```
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:192 errors:0 dropped:0 overruns:0 frame:0
TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:54507 (54.5 KB) TX bytes:24462 (24.4 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:2218 (2.2 KB) TX bytes:2218 (2.2 KB)

[05/02/2017 13:13] 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=0.457 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.423 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.320 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.507 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.567 ms
```

SEED Ubuntu 12.04 Clone [Running]

Terminal

```
5.0      inet6 addr: fe80::a00:27ff:feec:8f3a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:81 errors:0 dropped:0 overruns:0 frame:0
TX packets:128 errors:0 dropped:0 overruns:0 carrier:

0      collisions:0 txqueuelen:1000
RX bytes:20536 (20.5 KB) TX bytes:16244 (16.2 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)

[05/02/2017 13:12] 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=0.019 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.334 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.353 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.386 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.346 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.019/0.287/0.386/0.136 ms
[05/02/2017 13:25] seed@ubuntu:~$
```

Problem 2: Writing a packet Sniffer

```
[05/02/2017 13:39] 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: 10.0.2.4
        To: 162.213.33.49
    Protocol: TCP
    Src port: 59060
    Dst port: 443

Packet number 2:
    From: 162.213.33.49
        To: 10.0.2.4
    Protocol: TCP
    Src port: 443
    Dst port: 59060

Packet number 3:
    From: 10.0.2.4
        To: 162.213.33.49
    Protocol: TCP
    Src port: 59060
    Dst port: 443

Packet number 4:
    From: 10.0.2.4
        To: 162.213.33.49
    Protocol: TCP
    Src port: 59060
    Dst port: 443
    Payload (148 bytes):
00000  16 03 00 00 8f 01 00 00  8b 03 03 59 08 ee c0 0f  ....Y....
00016  e0 3a c0 a6 0e 28 9e db  55 39 89 af 78 15 f8 c8  ..(.U9..x...
00032  83 7f 9f 3e d0 fc a9 81  ed 88 e7 00 00 30 00 33  ...>.....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
```

```

Packet number 5:
    From: 162.213.33.49
        To: 10.0.2.4
    Protocol: TCP
    Src port: 443
    Dst port: 59060

Packet number 6:
    From: 162.213.33.49
        To: 10.0.2.4
    Protocol: TCP
    Src port: 443
    Dst port: 59060
    Payload (1460 bytes):
00000  16 03 03 00 55 02 00 00  51 03 03 73 4c b2 b4 3b  ....U...Q..sL...;
00016  0d a7 48 3e c2 89 a4 b3  01 95 37 ed 24 bb b2 b9  ..H>.....7.$...
00032  e9 95 03 6c 02 99 5f e5  1c 05 d9 20 7c f2 7c d7  ...l..._....|.|.
00048  d6 7a 8b e8 c2 55 87 6f  73 98 69 a8 fc 60 6f a6  .z...U.os.i...`o.
00064  27 cd 56 de 4c a5 58 3a  8f 46 b1 a5 00 67 00 00  '.V.L.X:.F...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 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.ubuntu
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 c4y.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 30y.....0
00656	82 01 d9 30 1f 06 03 55	1d 23 04 18 30 16 80 140...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 cd0...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 16 300...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 620k..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 99mc7?..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 48T...>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 22w@..._h."
01312	96 9d ed 9f 0a 57 10 b1	51 d6 31 c7 a6 2e 41 44W..Q.1...AD
01328	8b 6b a7 9c 80 d2 19 ef	41 b8 78 e3 fe 83 11 a8	.k.....A.x.....
01344	6c d3 6e 90 37 c9 0a a3	5a bd ec 44 b2 8a 28 99	l.n.7...Z..D..(.
01360	3c 04 d8 8a 93 ea 5f b1	78 90 f1 df 11 6b 6b 9c	<....._x....kk.
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 cfn.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: 10.0.2.4
To: 162.213.33.49
Protocol: TCP
Src port: 59060
Dst port: 443

```

Packet number 8:

```

From: 162.213.33.49
To: 10.0.2.4
Protocol: TCP
Src port: 443
Dst port: 59060
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 01 000.....
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 92y.....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..
00416	da 73 8b 12 97 48 90 04	45 75 1a dd 37 31 97 92	.s...H..Eu..71..
00432	e8 cd 54 0d 3b e4 c1 3f	39 5e 2e b8 f3 5c 7e 10	..T.;..?9^....\\~.
00448	8e 86 41 00 8d 45 66 47	b0 a1 65 ce a0 aa 29 09	..A..EfG..e...).
00464	4e f3 97 eb e8 2e ab 0f	72 a7 30 0e fa c7 f4 fd	N.....r.0.....
00480	14 77 c3 a4 5b 28 57 c2	b3 f9 82 fd b7 45 58 9b	.w...[(W.....EX.
00496	02 03 01 00 01 a3 82 01	5a 30 82 01 56 30 12 06Z0..V0..
00512	03 55 1d 13 01 01 ff 04	08 30 06 01 01 ff 02 01	.U.....0.....
00528	00 30 0e 06 03 55 1d 0f	01 01 ff 04 04 03 02 01	.0....U.....
00544	86 30 34 06 08 2b 06 01	05 05 07 01 01 04 28 30	.04..+.....(0
00560	26 30 24 06 08 2b 06 01	05 05 07 30 01 86 18 68	&0\$..+.....0...h
00576	74 74 70 3a 2f 2f 6f 63	73 70 2e 64 69 67 69 63	http://ocsp.digic
00592	65 72 74 2e 63 6f 6d 30	7b 06 03 55 1d 1f 04 74	ert.com0{..U..t
00608	30 72 30 37 a0 35 a0 33	86 31 68 74 74 70 3a 2f	0r07.5.3.1http:/
00624	2f 63 72 6c 33 2e 64 69	67 69 63 65 72 74 2e 63	/crl3.digicert.c
00640	6f 6d 2f 44 69 67 69 43	65 72 74 47 6c 6f 62 61	om/DigiCertGloba
00656	6c 52 6f 6f 74 43 41 2e	63 72 6c 30 37 a0 35 a0	lRootCA.crl07.5.
00672	33 86 31 68 74 74 70 3a	2f 2f 63 72 6c 34 2e 64	3.1http://crl4.d
00688	69 67 69 63 65 72 74 2e	63 6f 6d 2f 44 69 67 69	igicert.com/Digi
00704	43 65 72 74 47 6c 6f 62	61 6c 52 6f 6f 74 43 41	CertGlobalRootCA
00720	2e 63 72 6c 30 3d 06 03	55 1d 20 04 36 30 34 30	.crl0=..U..6040
00736	32 06 04 55 1d 20 00 30	2a 30 28 06 08 2b 06 01	2..U..0*0(..+..
00752	05 05 07 02 01 16 1c 68	74 74 70 73 3a 2f 2f 77https://w
00768	77 77 2e 64 69 67 69 63	65 72 74 2e 63 6f 6d 2f	ww.digicert.com/
00784	43 50 53 30 1d 06 03 55	1d 0e 04 16 04 14 0f 80	CPS0...U.....
00800	61 1c 82 31 61 d5 2f 28	e7 8d 46 38 b4 2c e1 c6	a..1a./(..F8.,..
00816	d9 e2 30 1f 06 03 55 1d	23 04 18 30 16 80 14 03	..0...U.#..0....
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	90...n\..\$&.....
00928	c7 2e 02 c6 4d 4a bf b0	42 df 78 da b3 a8 f9 6dMJ..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 b8M'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 daq..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.....*.*
01216	e6 cc b1 04 1f fc 48 4c	1b 70 73 c1 13 0b ff 36HL.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 c72.....;/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 44	e8 29 de 5a c7 93 11 e9	,.....D.).Z....
01408	ba 93 22 5c 19 8d a7 0e	1d d9 b7 40 49 b5 4d 2b	." \.....@I.M+
01424	c8 dd 39 40 2d 06 8d f0	db f2 1a d8 e9 16 3b 10	.9@-.....;.
01440	93 62 9a 3b a3 b3 e5 19	93 25 3c 67 7c 39 4a 1e	.b.;.....%<g 9J.
01456	a5 e6 a8 df	

Packet number 9:

From: 10.0.2.4
 To: 162.213.33.49
 Protocol: TCP
 Src port: 59060
 Dst port: 443

Packet number 10:

From: 162.213.33.49
 To: 10.0.2.4
 Protocol: TCP
 Src port: 443
 Dst port: 59060
 Payload (464 bytes):

00000	4d 02 ad 0d 59 72 fc 00	83 86 ed d5 06 fc de 66	M...Yr.....f
00016	3d d0 a5 fd 38 d8 a1 48	4a f0 60 f3 5e 79 97 fe	=...8..HJ.`.^y..
00032	18 33 3b 2c 9e 3d 9c fc	7c 75 b2 ee ad e9 37 ad	.3;,.=.. u....7.
00048	b5 e2 47 79 58 ab f5 4d	25 2e 01 95 8b 5b 25 44	..GyX..M%....[%D
00064	31 2d 03 bc a2 5d 71 9c	02 e1 f2 9e 8e c9 ed e1	1-..]q.....

00080	cd 41 bb d1 85 00 7d 6e be e9 e5 b6 f4 6d 93 cd	.A.....}n.....m..
00096	06 fb 3c de 8f dd fb 22 b6 ca 15 da 22 16 22 3f	..<....."....."?"
00112	61 25 ca 54 ff 96 68 0e f6 ea 79 8e 5a 7d 9a 98	a%.T...h....y.Z}...
00128	32 34 85 dd e5 ae cd 6f 80 e0 cc 1e 1d 54 47 ba	24.....o.....TG.
00144	ea 6c 39 7f c6 0b 2f b0 80 38 35 84 84 58 6d f8	.l9....//.85..Xm.
00160	18 d4 1e fb bc 80 87 1c 9a 45 17 5f 4e 75 01 2aE._Nu.*
00176	dc 06 ef 90 ca 38 3a 43 b0 a7 2d 31 b9 db c7 ec8:C...-1....
00192	a2 df 3a 04 01 01 00 5e f8 6c fe dc 5a 6d 35 99	..:.....^l..Zm5.
00208	c4 98 61 b3 18 3e 90 c6 95 e5 17 86 ea 18 a9 55	..a..>.....U
00224	c0 34 b5 40 2e d5 4b d1 a4 95 1e 47 c9 df 21 cd	.4.@..K....G...!
00240	cd 8e af be 2c a5 3e 24 9d 96 d6 2f 3c 4b 47 17,>\$.../<KG.
00256	e3 9a 79 15 7d 35 19 e8 26 ba 6a f9 0e 74 87 b2	..y.}5...&.j...t..
00272	56 9d 7a cd 21 9d 5f c5 e9 1c d2 49 30 92 a7 cc	V.z.!_.....I0...
00288	9d e9 ed bd f2 0d 6a 84 17 53 a0 06 d2 f9 50 58j..S....PX
00304	cf a6 bb 4e c5 63 1e a9 c7 08 bc d5 5e 42 d2 01	...N.C.....^B..
00320	74 26 4a e3 a9 bf d0 17 d5 85 9b ce 4f d4 cb 01	t&J.....O...
00336	01 d3 08 a5 83 60 5c fa 2d d8 c8 f7 0a 01 fb f1`\\.....
00352	bb 09 e1 7a d9 c7 75 6b 94 e7 90 db 54 c9 5e 76	...z..uk....T.^v
00368	17 e3 68 f5 5c 53 04 c0 8e ce ee 3b bd f1 0d 29	..h.\\$.....;....)
00384	0c 30 9f dd f3 26 66 c4 e5 20 31 7b 5a ec c0 34	.0....&f... 1{Z..4
00400	16 75 71 85 bd 16 e1 00 ce 41 1e 20 e0 72 08 9b	.uq.....A. .r..
00416	a6 9b 3e e9 3e ab 89 29 67 f6 22 19 65 d8 0e 77	..>.>...)g.".e..w
00432	d2 5e 18 6a e6 ab ac 2d 8b f3 4b ed 01 af 8f c8	.^.j.....K.....
00448	37 fa a8 8b bd 99 8d 16 03 03 00 04 0e 00 00 00	7.....

Capture complete.

[05/02/2017 13:40] seed@ubuntu:~/Downloads\$

```
SEED Ubuntu 12.04 Clone [Running]
File Edit View Search Terminal Help
Terminal
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)

[05/02/2017 13:12] 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=0.019 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.334 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.353 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.386 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.346 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.019/0.287/0.386/0.136 ms
[05/02/2017 13:25] 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=0.566 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=0.364 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.504 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.435 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.315 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.315/0.436/0.566/0.094 ms
[05/02/2017 13:41] seed@ubuntu:~$
```

When looking at the sniffer program with TCP, it gives you the information of the packets whereas the others didn't.

Problem 3: Password Sniffing

```
Dst port: 60373
Payload (1 bytes):
00000  73          s

Packet number 3:
    From: 10.0.2.5
        To: 10.0.2.4
    Protocol: TCP
    Src port: 60373
    Dst port: 23

Packet number 4:
    From: 10.0.2.5
        To: 10.0.2.4
    Protocol: TCP
    Src port: 60373
    Dst port: 23
    Payload (1 bytes):
00000  65          e

Packet number 5:
    From: 10.0.2.4
        To: 10.0.2.5
    Protocol: TCP
05/02/2017 14:00] seed@ubuntu:~/Desktop$ exit
ogout
onnection closed by foreign host.
05/02/2017 14:00] seed@ubuntu:~$ telnet 10.0.2.4
ryng 10.0.2.4...
nnected to 10.0.2.4.
scape character is '^]'.
buntu 12.04.2 LTS
buntu login: seed
assword:
```

As you can see, when I typed in seed for the login, the sniffer program was able to log my key strokes and get what I was typing. In the above picture, you can see the s and the e of the username "seed". It successfully also logged the different letters of the username and password. Something interesting was that it logged multiple instances of only one keyboard stroke.

As for wireshark, you were still able to sniff out the username and password. For the username, it documented two of each keystroke, and the password came out exactly as I typed it.

Problem 4: SSH

Capturing from eth13 [Wireshark 1.6.7]

Filter List the available capture interfaces...

No.	Time	Source	Destination	Protocol	Length
61	2017-05-02 14:08:51.29	10.0.0.2.4	10.0.2.5	TCP	114
62	2017-05-02 14:08:51.29	10.0.0.2.5	10.0.2.4	TCP	66
63	2017-05-02 14:08:51.55	10.0.0.2.5	10.0.2.4	TCP	130
64	2017-05-02 14:08:51.56	10.0.0.2.4	209.18.47.62	DNS	81
65	2017-05-02 14:08:51.56	209.18.47.62	10.0.2.4	DNS	140
66	2017-05-02 14:08:51.59	10.0.0.2.4	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	10.0.0.2.4	224.0.0.251	MDNS	81
69	2017-05-02 14:08:51.68	10.0.0.2.5	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	10.0.0.2.4	224.0.0.251	MDNS	74
72	2017-05-02 14:08:51.78	10.0.0.2.5	224.0.0.251	MDNS	84
73	2017-05-02 14:08:51.78	10.0.0.2.4	10.0.2.5	TCP	130
74	2017-05-02 14:08:51.79	10.0.0.2.5	10.0.2.4	TCP	66
75	2017-05-02 14:08:52.66	10.0.0.2.4	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	10.0.0.2.5	10.0.2.4	TCP	210
78	2017-05-02 14:08:55.91	10.0.0.2.4	10.0.2.5	TCP	66
79	2017-05-02 14:08:55.94	10.0.0.2.4	10.0.2.5	TCP	98
80	2017-05-02 14:08:55.94	10.0.0.2.5	10.0.2.4	TCP	66
81	2017-05-02 14:08:55.94	10.0.0.2.5	10.0.2.4	TCP	194
82	2017-05-02 14:08:55.98	10.0.0.2.4	10.0.2.5	TCP	66

Invalid filter: "d" is neither a field nor a column

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:~$
```

When trying to sniff the password using ssh. I was not able to locate the letters to the password. I believe this is the reason ssh has gained a lot of popularity. It is secure and all the information is encrypted.