Jon Robison
Assignment 4

Part 1: Evading Detection

1. **Explain** the reason of why Alice and Bob are able to chat using this deceived arrangements?

Alice hosts three instances to which bob's three clients connect. The pipe redirects all standard output to the next item, until there is no pipe and printed to stdout. Any odd number of pipes would work, really.
Path from Alice: aliceServer1 -> bobClient1 |> bobClient2 -> aliceServer2 |> aliceServer3 -> bobClient3 |> stdout
Path from Bob: bobClient1 -> aliceServer1 |> aliceServer2 -> bobClient2 |> bobClient3 -> aliceServer3 |> stdout

2. Use ***lsof*** command to proof the communication paths between Alice and Bob.

```
something:~> lsof | grep jrobison | grep sock
...
sock    28966   jrobison        3u      IPv4 129700586       0t0      TCP
something.cs.odu.edu:43495->somethingelse.cs.odu.edu:11001 (ESTABLISHED)
…
sock    28967   jrobison        3u      IPv4 129701304       0t0      TCP
something.cs.odu.edu:38999->somethingelse.cs.odu.edu:11002 (ESTABLISHED)
…
sock    28968   jrobison        3u      IPv4 129700587       0t0      TCP
something.cs.odu.edu:37281->somethingelse.cs.odu.edu:11003 (ESTABLISHED)

somethingelse:~> lsof | grep jrobison | grep sock
…
sock    1469    jrobison3u      IPv4 2522150         0t0      TCP *:11001 (LISTEN)
sock    1469    jrobison4u      IPv4 2522151         0t0      TCP
somethingelse.cs.odu.edu:11001->something.cs.odu.edu:43495 (ESTABLISHED)
…
sock    1470    jrobison3u      IPv4 2521336         0t0      TCP *:11002 (LISTEN)
sock    1470    jrobison4u      IPv4 2521337         0t0      TCP
somethingelse.cs.odu.edu:11002->something.cs.odu.edu:38999 (ESTABLISHED)
…
sock    1471    jrobison3u      IPv4 2521338         0t0      TCP *:11003 (LISTEN)
sock    1471    jrobison4u      IPv4 2521339         0t0      TCP
somethingelse.cs.odu.edu:11003->something.cs.odu.edu:37281 (ESTABLISHED)
```

From this we see there are 3 communication paths between Alice and Bob.

3. Use ***tcpdump*** to capture all the SYN and FIN segments and the content of the chat messages. In this assignment: Type Alice in Host1. Then type Bob in Host2 followed by CTRL-D.

somethingelse:~> sudo tcpdump -tAN 'tcp[tcpflags] & (tcp-syn|tcp-ack) != 0 and portrange 11001-11003'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
IP something.37298 > somethingelse.11003: Flags [S], seq 3530317202, win 14600, options [mss 1460,sackOK,TS val 1038207013 ecr 0,nop,wscale 5], length 0
E..<..@.@....R...R.x..*..l].....9..X.....
=..%.....
IP somethingelse.11003 > something.37298: Flags [S.], seq 211576497, ack 3530317203, win 14480, options [mss 1460,sackOK,TS val 1036851945 ecr 1038207013,nop,wscale 5], length 0
E..<..@.@.0..R.x.R..*.....f..l]...8.
.....
=...=..%....
IP something.37298 > somethingelse.11003: Flags [.], ack 1, win 457, options [nop,nop,TS val 1038207014 ecr 1036851945], length 0
E..4..@.@....R...R.x..*..l]...f......K.....
=..&=...
IP something.39016 > somethingelse.11002: Flags [S], seq 1334541809, win 14600, options [mss 1460,sackOK,TS val 1038207014 ecr 0,nop,wscale 5], length 0
E..<..@.@.z..R...R.x.h*.O.}.....9.n$.....
=..&.....
IP somethingelse.11002 > something.39016: Flags [S.], seq 4084037814, ack 1334541810, win 14480, options [mss 1460,sackOK,TS val 1036851946 ecr 1038207014,nop,wscale 5], length 0
E..<..@.@.0..R.x.R..*..h.mx.O.}...8.
.....
=...=..&....
IP something.39016 > somethingelse.11002: Flags [.], ack 1, win 457, options [nop,nop,TS val 1038207014 ecr 1036851946], length 0
E..4..@.@.z..R...R.x.h*.O.}..mx......A.....
=..&=...
IP something.43515 > somethingelse.11001: Flags [S], seq 1617578094, win 14600, options [mss 1460,sackOK,TS val 1038207015 ecr 0,nop,wscale 5], length 0
E..<.I@.@....R...R.x..*.`jHn......9..5.....
=..'.....
IP somethingelse.11001 > something.43515: Flags [S.], seq 409434543, ack 1617578095, win 14480, options [mss 1460,sackOK,TS val 1036851947 ecr 1038207015,nop,wscale 5], length 0
E..<..@.@.0..R.x.R..*....gy.`jHo..8.
.....

=...=..'....
IP something.43515 > somethingelse.11001: Flags [.], ack 1, win 457, options [nop,nop,TS val 1038207015 ecr 1036851947], length 0
E..4.J@.@....R...R.x..*.`jHo.gy......^.....
=..'=...
IP somethingelse.11001 > something.43515: Flags [P.], seq 1:7, ack 1, win 453, options [nop,nop,TS val 1036856138 ecr 1038207015], length 6
E..:c[@.@..t.R.x.R..*....gy.`jHo....
......
=.+J=..'Alice

IP something.43515 > somethingelse.11001: Flags [.], ack 7, win 457, options [nop,nop,TS val 1038211206 ecr 1036856138], length 0
E..4.K@.@....R...R.x..*.`jHo.gy.....
=...=.+J
IP something.39016 > somethingelse.11002: Flags [P.], seq 1:7, ack 1, win 457, options [nop,nop,TS val 1038211206 ecr 1036851946], length 6
E..:..@.@.z..R...R.x.h*.O.}..mx.....
=...=...Alice

IP somethingelse.11002 > something.39016: Flags [.], ack 7, win 453, options [nop,nop,TS val 1036856138 ecr 1038211206], length 0
E..4b\@.@..y.R.x.R..*..h.mx.O.}.....
......
=.+J=...
IP somethingelse.11003 > something.37298: Flags [P.], seq 1:7, ack 1, win 453, options [nop,nop,TS val 1036856138 ecr 1038207014], length 6
E..:|X@.@..w.R.x.R..*.....f..l].....
......
=.+J=..&Alice

IP something.37298 > somethingelse.11003: Flags [.], ack 7, win 457, options [nop,nop,TS val 1038211206 ecr 1036856138], length 0
E..4..@.@....R...R.x..*..l]...f.....
=...=.+J
IP something.43515 > somethingelse.11001: Flags [P.], seq 1:5, ack 7, win 457, options [nop,nop,TS val 1038211699 ecr 1036856138], length 4
E..8.L@.@....R...R.x..*.`jHo.gy.....5(.....
=..s=.+JBob

IP somethingelse.11001 > something.43515: Flags [.], ack 5, win 453, options [nop,nop,TS val 1036856631 ecr 1038211699], length 0
E..4c\@.@..y.R.x.R..*....gy.`jHs....

.....
=.-7=..s
IP somethingelse.11002 > something.39016: Flags [P.], seq 1:5, ack 7, win 453, options [nop,nop,TS val 1036856631 ecr 1038211206], length 4
E..8b]@.@..t.R.x.R..*..h.mx.O.}.....
.....
=.-7=...Bob

IP something.39016 > somethingelse.11002: Flags [.], ack 5, win 457, options [nop,nop,TS val 1038211699 ecr 1036856631], length 0
E..4..@.@.z..R...R.x.h*.O.}..mx.....
=..s=.-7
IP something.37298 > somethingelse.11003: Flags [P.], seq 1:5, ack 7, win 457, options [nop,nop,TS val 1038211699 ecr 1036856138], length 4
E..8..@.@....R...R.x..*..l]...f.....
=..s=.+JBob

IP somethingelse.11003 > something.37298: Flags [.], ack 5, win 453, options [nop,nop,TS val 1036856632 ecr 1038211699], length 0
E..4|Y@.@..|.R.x.R..*.....f..l].....
.....
=.-8=..s
IP something.43515 > somethingelse.11001: Flags [F.], seq 5, ack 7, win 457, options [nop,nop,TS val 1038211887 ecr 1036856631], length 0
E..4.M@.@....R...R.x..*.`jHs.gy.....
=../=.-7
IP somethingelse.11001 > something.43515: Flags [F.], seq 7, ack 6, win 453, options [nop,nop,TS val 1036856819 ecr 1038211887], length 0
E..4c]@.@..x.R.x.R..*....gy.`jHt....
.....
=.-.=../
IP something.39016 > somethingelse.11002: Flags [F.], seq 7, ack 5, win 457, options [nop,nop,TS val 1038211887 ecr 1036856631], length 0
E..4..@.@.z..R...R.x.h*.O.}..mx.....
=../=.-7
IP something.43515 > somethingelse.11001: Flags [.], ack 8, win 457, options [nop,nop,TS val 1038211887 ecr 1036856819], length 0
E..4.N@.@....R...R.x..*.`jHt.gy.....B.....
=../=.-.
IP somethingelse.11002 > something.39016: Flags [F.], seq 5, ack 8, win 453, options [nop,nop,TS val 1036856819 ecr 1038211887], length 0
E..4b^@.@..w.R.x.R..*..h.mx.O.}.....
.....

=.-.=../
IP something.37298 > somethingelse.11003: Flags [F.], seq 5, ack 7, win 457, options [nop,nop,TS val 1038211887 ecr 1036856632], length 0
E..4..@.@....R...R.x..*..l]...f.....
=../=.-8
IP something.39016 > somethingelse.11002: Flags [.], ack 6, win 457, options [nop,nop,TS val 1038211887 ecr 1036856819], length 0
E..4..@.@.z..R...R.x.h*.O.}..mx.....".....
=../=.-.
IP somethingelse.11003 > something.37298: Flags [F.], seq 7, ack 6, win 453, options [nop,nop,TS val 1036856819 ecr 1038211887], length 0
E..4|Z@.@..{.R.x.R..*.....f..l].....
.....
=.-.=../
IP something.37298 > somethingelse.11003: Flags [.], ack 8, win 457, options [nop,nop,TS val 1038211888 ecr 1036856819], length 0
E..4..@.@....R...R.x..*..l]...f......+.....
=..0=.-.

Part 2: Simultaneous open & close
Use the **tcpdump** to capture:
1. The SYN segments of the **simultaneous** TCP connection **establishment** using:
SimulOpen_sh

somethingelse:~> sudo tcpdump -tAN 'tcp[tcpflags] & tcp-syn != 0 and portrange 11001-11002'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
<snip jrobison SOOO many repeated lines>
IP somethingelse.11002 > something.11001: Flags [S], seq 2887393658, win 14600, options [mss 1460,sackOK,TS val 1037222749 ecr 0,nop,wscale 5], length 0
E..<.'@.@.N..R.x.R..*.*...!z......9.
.....
=..].....
IP something.11001 > somethingelse.11002: Flags [S], seq 1256758207, win 14600, options [mss 1460,sackOK,TS val 1038577817 ecr 0,nop,wscale 5], length 0
E..<.&@.@.E..R...R.x*.*.J.....9.....
=.p.....
IP somethingelse.11002 > something.11001: Flags [S.], seq 2887393658, ack 1256758208, win 14600, options [mss 1460,sackOK,TS val 1037222749 ecr 1038577817,nop,wscale 5], length 0
E..<.(@.@.N..R.x.R..*.*...!zJ.....9.
.....
=..]=.p.....

IP something.11001 > somethingelse.11002: Flags [S.], seq 1256758207, ack 2887393659, win 14600, options [mss 1460,sackOK,TS val 1038577817 ecr 1037222749,nop,wscale 5], length 0
E..<.'@.@.E..R...R.x*.*.J.....!{..9.K.....
=.p.=..]....

2. The FIN segments of the **simultaneous** TCP connection **close** using:
SimulCloseClient.c & SimulCloseServer.c

Note: I got a couple 'Received signal: User defined signal 1' to which I responded "y" for the first and "n" to the second
somethingelse:~> sudo tcpdump -tN 'tcp[tcpflags] & tcp-fin != 0 and port 11002'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
IP something.39037 > somethingelse.11002: Flags [F.], seq 1715474245, ack 2530753293, win 457, options [nop,nop,TS val 1038827653 ecr 1037472585], length 0
IP somethingelse.11002 > something.39037: Flags [F.], seq 1, ack 1, win 453, options [nop,nop,TS val 1037472585 ecr 1038827653], length 0
IP something.39038 > somethingelse.11002: Flags [F.], seq 4280747361, ack 2210216936, win 457, options [nop,nop,TS val 1038829516 ecr 1037474448], length 0
IP somethingelse.11002 > something.39038: Flags [F.], seq 1, ack 1, win 453, options [nop,nop,TS val 1037474448 ecr 1038829516], length 0
IP somethingelse.11002 > something.39039: Flags [F.], seq 1417938034, ack 789634616, win 453, options [nop,nop,TS val 1037474703 ecr 1038829771], length 0
IP something.39039 > somethingelse.11002: Flags [F.], seq 1, ack 0, win 457, options [nop,nop,TS val 1038829771 ecr 1037474703], length 0