A brief tutorial for coursework

UG3 Computer Communications & Networks (COMN)

Coursework Overview

- Goal
 - Implementation and evaluation of three end-to-end reliable data transfer protocols
 - Stop-and-Wait, Go-back-N, and Selective Repeat

• Assessment: 40% of course mark

- Part 1 (30%)
 - Part 1a (10%): rdt1.0
 - Part 1b (20%): rdt 3.0 (Stop-and-Wait)
- Part 2 (70%)
 - Part 2a (30%): Go-back-N
 - Part 2b (40%): Selective Repeat + iperf experiment

Virtual Machine (VM) Setup

- Need Oracle's VirtualBox virtualization software
- VirtualBox exists by default on all DICE machines
- List of DICE machines can be found at

- The VM image for the assignment
 - Can be accessed on DICE machines
 - Has dummynet link emulator and other relevant software

Creating VM

- 1. Log into a DICE machine
- 2. Open a terminal
- 3. Create a directory (e.g., comn-cwk) and 'cd' into it

mkdir comn-cwk

cd comn-cwk

openair@openair-1:~\$ ssh -X s1474946@student.ssh.inf.ed.ac.uk Password:

Last login: Sun Jan 26 15:15:23 2020 from 2001:630:3c1:90:ee3b:6300:6cf9:6e7f This is student.ssh.inf.ed.ac.uk running Scientific Linux 7 (sl7) DICE. It is just a gateway from the internet to our systems, so please now 'ssh student.login' before doing anything else, and remember to run any heavy/demanding programs on the compute server student.compute [bruegel]s1474946: ssh jackson.inf.ed.ac.uk Last login: Sun Jan 26 15:15:30 2020 from bruegel.inf.ed.ac.uk [jackson]s1474946:

Creating VM

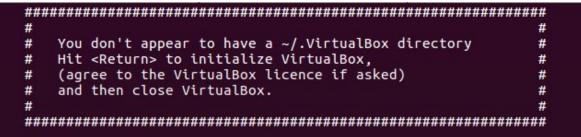
- 1. Log into a DICE machine
- 2. Open a terminal
- 3. Create a directory (e.g., comn-cwk) and 'cd' into it

mkdir comn-cwk

cd comn-cwk

4. Issue the following command:

/disk/scratch/dummynet/createdummynetvm



```
Hit <Return>...
```

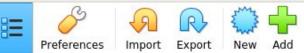
😑 🗈 🛛 Oracle VM VirtualBox Manager

File Machine Help

114

Tools





Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit <u>www.virtualbox.org</u> for more information and latest news.



```
#
      You don't appear to have a ~/.VirtualBox directory
   #
                                                   #
      Hit <Return> to initialize VirtualBox.
   #
      (agree to the VirtualBox licence if asked)
   #
      and then close VirtualBox.
   #
   Hit <Return>...

    Registering the Virtual Machine ...

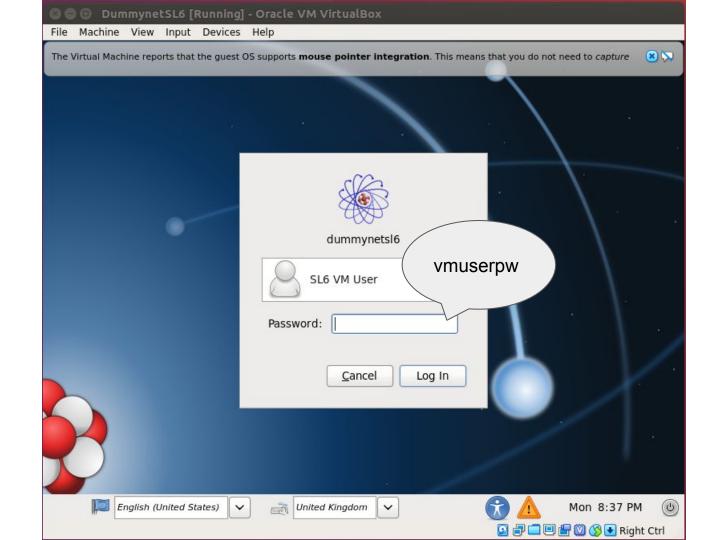
                                                           OK
Setting-up the Virtual Machine ...
                                                          OK
Downloading the disk image...
                                                          OK
4. Registering hard disks...
                                                          OK
Setting-up shared folder (dummynetshared)...
                                                           OK
   Your virtual machine 'DummynetSL6' is now ready.
   You can start the VM with './startvm.sh' or 'VirtualBox'.
   As root, use "mount -t vboxsf dummynetshared /mnt/shared"
   to mount the folder "/afs/inf.ed.ac.uk/user/s14/s1474946/comn cwk 2020/dummynetshared" on the VM.
   Your shared folder is '/mnt/shared' on the VM.
   #
      Put your data in '/work' or in '/mnt/shared' -
   #
      otherwise data will be lost when you close the VM.
   #
```

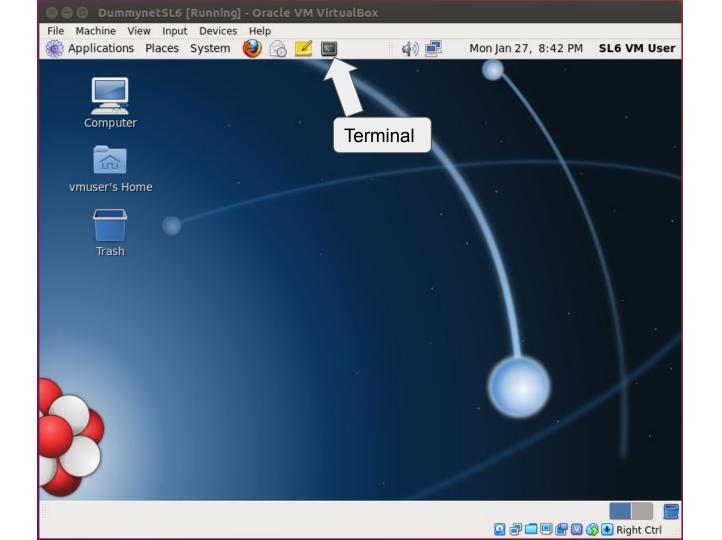
[jackson]s1474946:

[jackson]s1474946: pwd /afs/inf.ed.ac.uk/user/s14/s1474946/comn_cwk_2020 [jackson]s1474946: ls dummynetshared DummynetSL6 dummynetwork.vdi startvm.sh [jackson]s1474946:

Creating and Starting VM

- 5. Run the following command:
 - ./startvm.sh





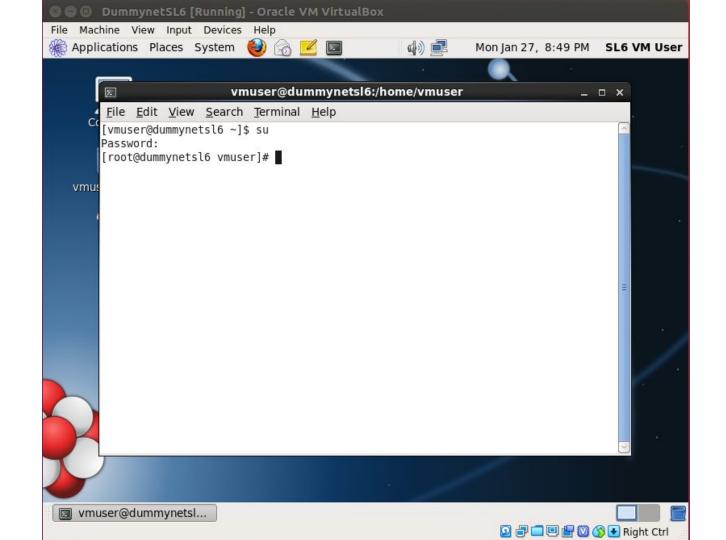
How to shut down VM

- Become a root using 'su'
 - Root password: vmrootpw

su

• Run the following command:

shutdown -h now

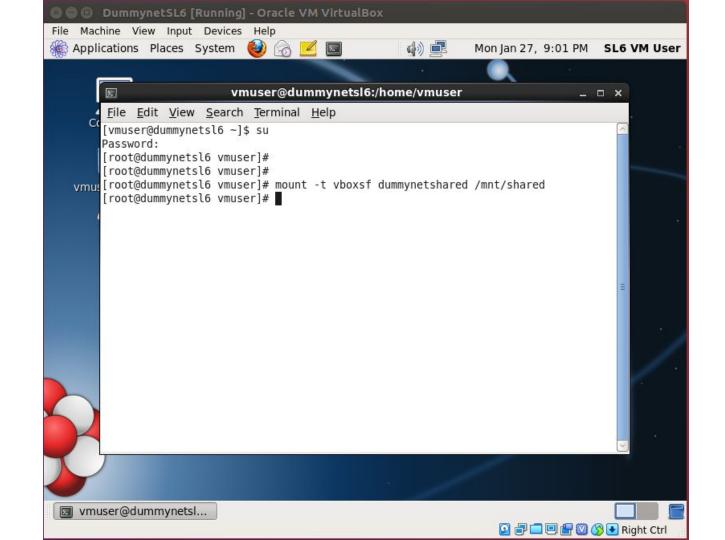


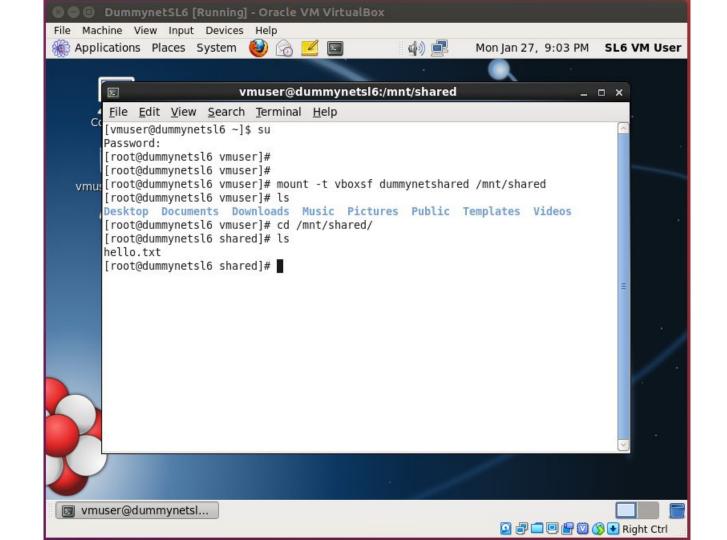
Shared Folder

 When the VM is set up for you, a directory called "dummynetshared" gets created in your assignment directory

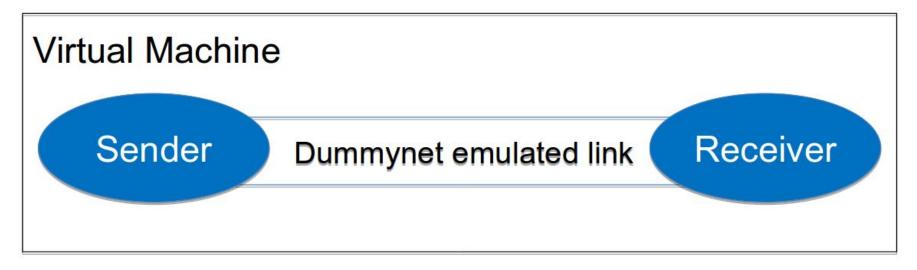
• You can mount this in the VM by (as root):

mount -t vboxsf dummynetshared /mnt/shared



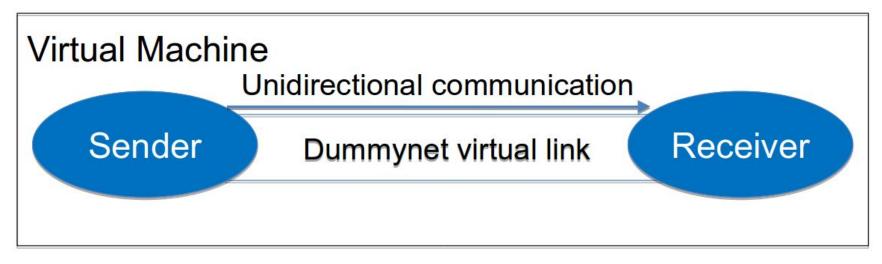


Conceptual Structure



- Dummynet
 - Creates emulated network link(s)
 - Configuration of link characteristics (BW, delay, loss)
 - Command-line program: ipfw

Conceptual Structure

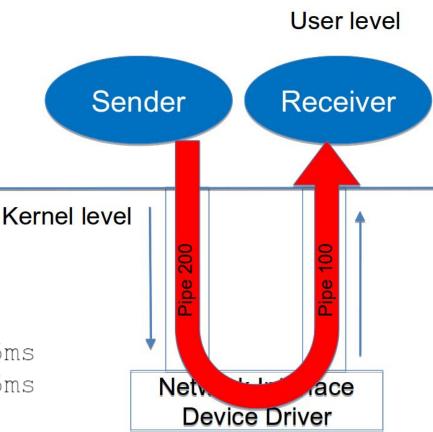


- Sender
 - Reads a file and breaks it into a number of packets
 - Sends the packets to a receiver over a simulated network link
- Receiver
 - Receives the packets; extracts data in the packets; and saves the data in a file

Effect of Dummynet

 When processes within the same host (or virtual machine) communicate with each other

% ipfw add pipe 100 in % ipfw add pipe 200 out % ipfw pipe 100 config delay 5ms % ipfw pipe 200 config delay 5ms

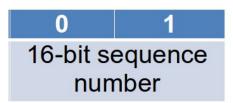


Header format

- The following formats should be used for both parts
 - Exception: no ACK packets for part1a
- Data packet
 - (Sender to Receiver)

0	1	2	3 ~ up to 1026
	equence nber	8-bit EoF flag	Data

- ACK packet
 - (Receiver to Sender)



iPerf

• iPerf is a tool used to measure network performance measurement in terms of throughput and latency.

openair@openair-1:~\$ iperf -s

Server listening on TCP port 5001 TCP window size: 85.3 KByte (default)

openair@openair-1:~\$ iperf -c 192.168.4.5 -i1 -t10	
Client connecting to 192.168.4.5, TCP port 5001 TCP window size: 85.0 KByte (default)	
[3] local 192.168.4.10 port 34562 connected with 192.168.4.5	port 5001
[ID] Interval Transfer Bandwidth	
[3] 0.0- 1.0 sec 11.2 MBytes 94.4 Mbits/sec	
[3] 1.0- 2.0 sec 11.2 MBytes 94.4 Mbits/sec	
[3] 2.0- 3.0 sec 11.1 MBytes 93.3 Mbits/sec	
[3] 3.0- 4.0 sec 11.2 MBytes 94.4 Mbits/sec	
[3] 4.0- 5.0 sec 11.2 MBytes 94.4 Mbits/sec	
[3] 5.0- 6.0 sec 11.1 MBytes 93.3 Mbits/sec	
[3] 6.0- 7.0 sec 11.2 MBytes 94.4 Mbits/sec	
[3] 7.0- 8.0 sec 11.1 MBytes 93.3 Mbits/sec	
[3] 8.0- 9.0 sec 11.2 MBytes 94.4 Mbits/sec	
[3] 9.0-10.0 sec 11.1 MBytes 93.3 Mbits/sec	
[3] 0.0-10.0 sec 112 MBytes 93.9 Mbits/sec	



iperf -c 192.168.4.5 -i1 -t10

iperf -c 192.168.4.5 -i1 -n 30MB

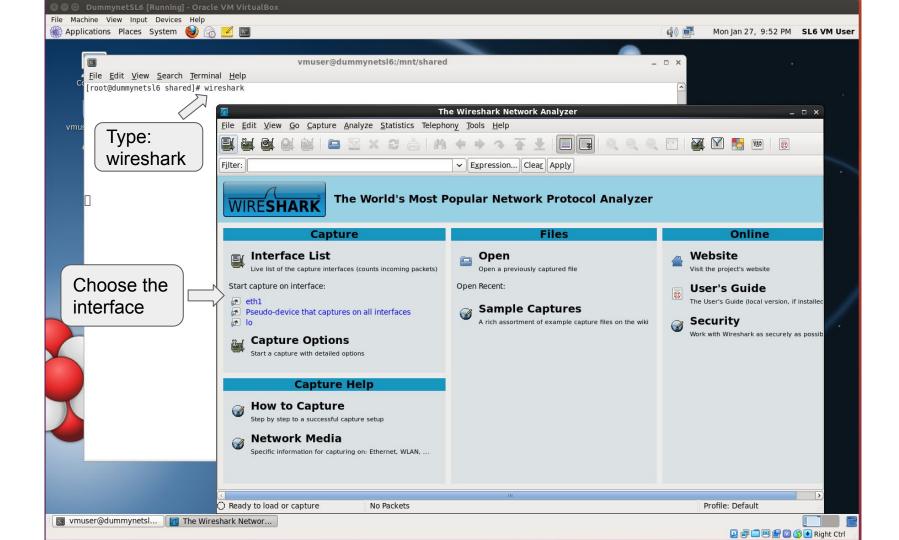
iperf -c 192.168.4.5 -i1 -F test.jpg -M 1KB

- $-c \rightarrow \text{Receiver IP address}$
- $-i \rightarrow$ Interval, seconds between periodic bandwidth reports
- -t \rightarrow time in seconds to transmit for (default 10 secs)
- $-n \rightarrow$ number of bytes to transmit (instead of -t)
- $-F \rightarrow$ input the data to be transmitted from a file
- $-M \rightarrow set TCP maximum segment size$

Wireshark

• Wireshark is an open-source packet analyzer tool that used to capture network packets to understand and troubleshoot network behavior.

- 1. Type in terminal \rightarrow wireshark
- 2. Choose the interface to capture the packets from.
- 3. Stop recording and save the file.



	a ci	apturing from eth1 - Wireshark	_ = X					
	ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp							
Stop								
	Expression Clear Apply							
recordir	g Time Source Destination	Protocol Info						
	Now it starts recording and will							
	display the packets here							
	display the packets here							
	athly clive conture in programs to ¹⁰ No Deckets	⁸ Draffa	: Default					
C C	eth1: vertice capture in progress> to No Packets vertice vertice of the second se	Profile						
			🗏 🔚 💟 🔇 💽 Right Ctrl					

	🕲 🗇 💷 DummynetSL6 [Running] - Oracle VM VirtualBox			
	File Machine View Input Devices Help		Man Ing 27, 10,02 PM	CI C 1/14 11
	🋞 Applications Places System 🍪 💮 🗹 🔤 1. jh.pcap - Wireshark	4) 🚅	Mon Jan 27, 10:02 PM	
(pture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp			_ ¤ ×
l				
1. Packet	Filter:			
	No. Time Source Destination Protocol . Info			<u>^</u>
Number	647 8.251971 10.10.0.133 10.10.0.107 TCP ssh > 33048 [ACK] Seq=15325 Ack=4949 Win=2140 Len=6			
	649 8.252113 10.10.0.133 10.10.0.107 TCP ssh > 33048 [ACK] Seq=15325 Ack=5033 Win=2140 Len=60 652 8.262918 10.10.0.107 10.10.0.133 TCP 33048 > ssh [ACK] Seq=5033 Ack=15861 Win=93 Len=60			
	655 5.264548 192.168.0.9 192.168.0.7 TCP 41040 > ssh [ACK] Seq=1 Ack=1381 Win=181 Len=0 TSV=			
	$\begin{array}{c} 660 \ 8.264780 \\ 661 \ 8.264842 \end{array} \begin{array}{c} 192.168.0.7 \\ 661 \ 8.264842 \end{array} \begin{array}{c} 192.168.0.7 \\ 192.$	1909242313	TSER=3374410398	
			3 TSER=2004771573	
	666 8.302089 Address 10 0.0.107 TCP ssh > 33048 0. SOULCE and	TSV=36914	3 TSER=2004771611	
	676 8.644636 (7) (1001 COS 19) 19 168.0.7 TCP 40038 > ssh Destination Ports		TSER=3374410778 TSER=3374411014	
	693 9.000390 1 4. Destination			=
	698 9.012641 1 600 / TCP 33048 > ssh [ACK] Seg=5273 Ack=16573 Win=93 Len=0 T			
	705 9.051970 1 IP Address / TCP ssh > 33048 [ACK] Seq=16765 Ack=5413 Win=2140 Len=6 707 9.052131 > 33048 [ACK] Seq=16765 Ack=5497 Win=2140 Len=6			~
	Frame 664 (68 bytes on wire, 68 bytes captured) Linux cooked capture Internet Protocol, Src: 10.10.0.133 (10.10.0.133), Dst: 10.10. Transmission Control Protocol, Src Port: ssh (22), Dst Port: 33-re (sec.or), seq. 2000, Ack: 5069, Len: 0			
	00000 00		Profile: Default	₹

le <u>E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp W W W W W W W W W W		ning] - Oracle VM VirtualBox									
Image: product											
Edit View Go Capture Analyze Statistics Telephony Tools Help Expression	🎆 Applications Places Syst	tem 👹 👩 🗾 国							d) 🛃	Mon Jan 27, 10:09 PM	SL6 VM Us
Image:	1			jh.pcap	- Wireshark						
Image:	File Edit View Go Capture	Analyze Statistics Telephon	y Tools Help								
Imme Source Destination Protocol. Info 647 8.231971 10.10.0.133 10.10.0.137 10.10.0.133 10.10.0.137 647 8.231971 10.10.0.133 10.10.0.137 10.10.0.137 10.10.0.137 658 8.24042 10.10.0.133 10.10.0.137 10.10.0.137 10.10.0.137 658 8.24042 102.10.0.107 10.10.0.137 10.10.0.137 10.10.0.137 658 8.24042 102.10.0.0.133 10.10.0.137 10.10.0.137 10.10.0.137 658 8.24042 102.10.0.133 10.10.0.107 10.10.0.137 10.10.0.107 658 8.24042 102.10.0.133 10.10.0.107 10.10.0.107 10.10.0.107 658 8.24042 102.10.0.133 10.10.0.107 10.10.0.107 10.10.0.107 658 8.24043 102.10.0.133 10.10.0.107 10.10.0.107 10.10.0.107 658 8.24042 102.10.0.133 10.10.0.107 10.10.0.107 10.10.0.107 658 8.24042 102.10.0.133 10.10.0.107 10.10.0.107 10.10.0.107 658 8.20050 10.10.0.133 10.10.0.107 10.10.0.107 10.10.0.107 658 9.20041 10.10.0.10						ER COL					
O Time Destination Protocol. Info 647 521971 10.18.0.133 10.10.0.137 10.10.0.137 1			♥ ♥ ֏ ★ ⊻			++		0			
647 2.23171 10.10.0.133 10.10.0.107 10.10.0.103 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.107 10.10.0.103 10.10.0.107 10	F <u>i</u> lter:		✓ Expression Clear	Apply							
649 622 10 10 0.10 0.10 10 10 10	No. Time	Source	Destination	Protocol .	Info						
649 622 10 10 0.10 0.10 10 10 10	647 8.251971	10.10.0.133	10.10.0.107	TCP	ssh > 33048	ACK1 S	eg=15325 Ack=4949	Win=2140 Le	en=0 TSV=3691	38 TSER=2004771523	
652 2.20218 10.10.0.107 10.10.0.133 TCP 33040 > 551 1ACK) Seq=3633 Ack=13801 Min=30 Lene TSV=2004771571 TSFE-305188 658 2.524780 192.166.0.6 192.166.0.7 TCP 41040 > 551 1ACK) Seq=1 Ack-1380 Win=30 Lene TSV=2004771571 TSFE-307410398 668 3.201064 192.166.0.7 TCP 41040 > 551 1ACK) Seq=1 Ack-7361 Win=30 Lene TSV=200472137 TSFE-307410398 668 3.201064 10.10.0.133 10.10.0.107 TCP 550 > 33048 IACK) Seq=1 Ack-7361 Win=181 Lene TSV=190924231 TSFE-304710570 668 3.201064 10.10.0.133 10.10.0.107 TCP 550 > 33048 IACK) Seq=16001 Ack-501 Win=131 Lene TSV=190924203 TSFE-304710511 678 5.04036 192.166.0.7 TCP 40033 > 551 IACK) Seq=16001 Ack-5751 Win=131 Lene TSV=190924203 TSFE-30471051 698 5.026140 10.10.0.133 10.10.0.137 TCP 550 > 33048 IACK) Seq=16061 Ack-5751 Win=31 Lene TSV=30924203 TSFE-30471051 698 5.05170 10.10.0.133 10.10.0.137 TCP 550 > 33048 IACK) Seq=1605 Ack-5413 Win=2140 Lene TSV-309212 TSFE-8204772320 7079 5.05170 16.0 4.0331 (10.10.0.137) TCP											
658 2.204348 192.106.0.9 192.106.0.7 TCP 41040 > shi (AcK) Seq=1.Ack+1381 Win=181 Lene TSV=1099242313 TSER-3374410398 668 2.67478 192.106.0.9 192.106.0.9 192.106.0.7 TCP 41040 > shi (AcK) Seq=1.Ack+1341 Win=181 Lene TSV=1099242313 TSER-3374410398 6618 2.644.3 192.106.0.9 192.106.0.107 TCP sho > 33048 (AcK) Seq=1.0ck+2608 Win=2140 Lene TSV=109924231 TSER-3374410398 6648 3.010.0.107 TCP sho > 33048 (AcK) Seq=1.0ck+2608 Win=2140 Lene TSV=109924233 TSER-3374410378 6668.8.012 192.106.0.9 192.108.0.7 TCP 40038 > shi (AcK) Seq=1.0ck+2618 Win=181 Lene TSV=109924293 TSER-3374410778 6688.8.012 192.108.0.9 192.108.0.7 TCP sho > 33048 (AcK) Seq=1.0ck+261 Win=181 Lene TSV=109924293 TSER-3374410778 693.000390 10.10.0.107 TCP sho > 33048 (AcK) Seq=1.0ck+261 Win=181 Lene TSV=109924293 TSER-3374410778 693.002108 10.0.0.107 TCP sho > 33048 (AcK) Seq=1.0ck+261 Win=181 Lene TSV=109924293 TSER-3374410778 693.002108 10.0.0.107 TCP sho > 33048 (AcK) Seq=1.0ck+261 Win=181 Lene TSV=109924293 TSER-3374410778 707.9.052131 10.10.0.133 10.10.0.133 10.10.0.137 TCP Sho > 33048 (AcK) Seq=1.0ck+261 Win=181 Len											
666 8: 264780 192, 168.0.9 192, 168.0.7 TCP 41040 > ssh [Ack] Seq=1 Ack=1449 Win=31 Len=0 TSV=199924231 TSER=3374410398 666 8: 264642 192, 168.0.9 192, 168.0.9 TCP ssh > 33484 [Ack] Seq=1 Ack=1249 Win=31 Len=0 TSV=199924231 TSER=3374410398 666 8: 26099 10.10.0.33 10.10.0.107 TCP ssh > 33484 [Ack] Seq=1 Ack=7561 Win=31 Len=0 TSV=199924231 TSER=3374410398 676 8: 26099 10.10.0.133 10.10.0.107 TCP ssh > 33484 [Ack] Seq=1 Ack=7561 Win=31 Len=0 TSV=199924293 TSER=3374410778 688 8: 88102 192, 168.0.9 192, 168.0.7 TCP 40038 > ssh [Ack] Seq=1 Ack=7561 Win=131 Len=0 TSV=199924293 TSER=3374410778 698 9.02541 10.8.0.617 10.10.0.133 TCP ssh > 33484 [Ack] Seq=1 Ack=7561 Win=131 Len=0 TSV=199924297 TSER=3374410778 698 9.02541 10.8.0.617 TCP ssh > 33484 [Ack] Seq=12675 Ack=517 Win=2140 Len=0 TSV=369212 TSER=2084772321 TSER=2084772321 TSER=2084772321 TSER=2084772321 TSER=2084772321 TSER=2084772323 TSER=2084772321											
6618 2.2.168.0.9 192.168.0.7 TCP 40038 > ssh [AcK] Seq=10A (AcK) (A											
666 8.301964 10.10.0.0.133 10.10.0.0.107 TCP ssh > 33048 (ACK) Seq=10601 Ack=3060 Min=2140 Len=0 TSV=309143 TSV=2094771573 666 8.30209 10.10.0.0107 TCP ssh > 33048 (ACK) Seq=10601 Ack=3500 Min=2140 Len=0 TSV=309413 TSV=2094771573 668 8.80102 192.168.0.7 TCP 40038 > ssh [ACK] Seq=10601 Ack=7561 Win=101 Len=0 TSV=309413 TSV=20947721573 698 9.002309 10.10.0.133 10.10.0.107 TCP ssh 33048<[ACK] Seq=16061											
6666 3.92089 10.10.0.133 10.10.0.107 TCP ssh 33448 [AcK] Seq=1.601 Ack=7505 Win=2140 Len=0 TSV=3092143 TSER=204771611 676 8.446366 132.166.0.7 TCP 40038 > ssh [AcK] Seq=1.Ack=7561 Win=2141 Len=0 TSV=10924203 TSER=204772301 688 8.881012 192.166.0.7 TCP 40038 > ssh [AcK] Seq=1.Ack=7361 Win=2140 Len=0 TSV=10924203 TSER=204772309 693 9.00390 10.10.0.133 10.10.0.107 TCP ssh 39484 [AcK] Seq=1.6075 Ack=7361 Win=111 Len=0 TSV=309213 TSER=204772309 787 9.052131 10.10.0.133 10.10.0.107 TCP ssh 39484 [AcK] Seq=16755 Ack=7361 Win=2140 Len=0 TSV=309213 TSER=204772321 787 9.052131 10.10.0.133 10.10.0.107 TCP ssh 39484 [AcK] Seq=16755 Ack=7361 Win=2140 Len=0 TSV=309213 TSER=204772321 11nx code capture Internet Protocol, Src Port: ssh (22), Dst Port: 3048 (33046), Seq: 1601, Ack: 5069, Len: 0 Source port: ssh (22) Dst Port: 3048 (Savefa) Source port: ssh (22) Dst Port: 3048 (Savefa) Source port: ssh (22) Source port: ssh (22) D											
676 8.644636 192.168.6.9 192.168.6.7 TCP 40083 > sh [AKK] seq=1 Ack=7501 win=181 Lene= TSV-1909242693 TSER-3374410778 688 8.81012 192.168.6.9 192.168.6.7 TCP 40083 > sh [AKK] seq=1601 Ack=7501 win=181 Lene= TSV-1909242693 TSER-3374410778 698 9.000390 10.10.6.133 10.10.0.107 TCP sh 33448 [AKK] seq=1601 Ack=5173 win=2140 Len=0 TSV-19092420321 TSER-3204772309 698 9.025131 10.10.6.133 10.10.0.107 TCP sh > 3348 [AKK] seq=16765 Ack=5413 win=2140 Len=0 TSV-3692121 TSER-2004772323 707 9.052131 10.10.0.133 10.10.0.107 TCP sh > 3348 [AKK] seq=16765 Ack=5437 win=2140 Len=0 TSV-369218 TSER-2004772323 Trame 664 (68 bytes on wire, 68 bytes captured) Internet Protocol, Src Port: sh (22), Dst Port: 33048 (33048), Seq: 16001, Ack: 5069, Len: 0 Source port: sh (22) Dst Ination port: sh (22) Dst Ination port: sh (22) Dst Ination port: sh (22) Destination port: sh (22) Dst Ination port: sh (22) TCP windowy Sizee Vindow size: 2140 Vindow size: 2140 Vindow size: 2140 Vindow size: 2140 0 of 00 00 01 00 06 02 15 6d c5 c3 c7 09 09 08 00 Exception to the too too too too too too too too too to											
668 8.81012 192.168.0.9 192.168.0.7 TCP 40083 > sth [AKK] Seq=1 Ack=7601 Win=181 Len=0 TSV=30924229 TSER=3374411014 693 9.003909 10.10.0.133 10.10.0.133 TCP 33048 > sth [AKK] Seq=16001 Ack=713 Win=214 Len=0 TSV=309242929 TSER=3374411014 10.10.0.133 10.10.0.133 TCP 33048 > sth [AKK] Seq=16765 Ack=5413 Win=2140 Len=0 TSV=309218 TSER=2004772323 705 9.051370 10.10.0.133 10.10.0.107 TCP sth > 33048 [AKK] Seq=16765 Ack=5413 Win=2140 Len=0 TSV=309218 TSER=2004772323 Transet 664 (68 bytes on wire, 68 bytes captured) Linux cooked capture Internet Protocol, 5rc: 10.10.0.133 (10.10.0.133), 0st: 10.10.0.107 TCP sth > 33048 [AKK] Seq=16765 Ack=543 Win=2140 Len=0 TSV=309218 TSER=2004772323 Transet for the capture of the transet of the tr											
693 9.000390 10.10.0.133 10.10.0.107 TCP ssh > 33048 [Ack] Seq=16001 Ack=05173 Min=2140 Len=0 TSV=36212 TSE=2004772309 608 9.012641 10.10.0.133 10.10.0.137 TCP ssh > 33048 [Ack] Seq=16755 Ack=16573 Min=2140 Len=0 TSV=369218 TSE=2004772301 TSE TSE TSE TSE TSE TSE											
698 9.012641 10.10.0.107 10.10.0.133 10.10.0.133 10.10.0.133 10.10.0.107 TCP ssh > 33048 > ssh [Ack] Seq=3573 Ack=16573 Win=93 Lene 0 TSV=2004772321 TSER=309213 707 9.052131 10.10.0.133 10.10.0.107 TCP ssh > 33048 [Ack] Seq=1676 Ack=5413 Win=93 Lene 0 TSV=369218 TSER=2004772361 Inux cooked capture Inux cooked capture Inux cooked capture Inux cooked capture Intract Protocol, Src: 10.10.0.133 (10.10.0.133), Dst: 10.10.0.107 (10.10.0.167) Transnission Control Protocol, Src: Port: ssh (22), Dst Port: 33048 (33048), Seq: 16001, Ack: 5069, Len: 0 Source port: ssh (22) Destination port: ssh (23) Destination port: ssh (23) Destination port: 33048 (33048) [stream index: 1] Sequence number: S669 (relative sequence number) 7. TCP sequence number: Number P Flags: GN (Ack) Window size: 2140 Stream Source port: Ssh (22) Streem Source port: Ssh (22) 9 0 0 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0											
705 9.451570 10.10.0.133 10.10.0.107 TCP ssh > 33048 fAck[Seq=16765 Ack=5413 Win=2140 Len=0 TSV=369218 TSER=2004772323 707 9.052131 10.10.0.133 10.10.0.107 TCP ssh > 33048 fAck[Seq=16765 Ack=5413 Win=2140 Len=0 TSV=369218 TSER=2004772323 Internet Protocol, Src: 10.10.0.133 (10.10.0.107 TCP ssh > 33048 fAck[Seq=16765 Ack=5413 Win=2140 Len=0 TSV=369218 TSER=2004772361 Internet Protocol, Src: 10.10.0.133 (10.10.0.107 TCP ssh > 33048 fAck[Seq=16765 Ack=5413 Win=2140 Len=0 TSV=369218 TSER=2004772361 Internet Protocol, Src: 10.10.0.107 TSER Source port: Sh (22) Dst Port: Sloge16 Ack: Source port: Source po											
707 10.10.0.133 10.10.017 TCP ssh > 33048 [ACK] Seq=16765 Ack=5497 Win=2140 Len=0 TSV=369218 TSER=2004772361 Frame 664 (68 bytes on wire, 68 bytes captured) Internet Protocol, Src: 10.10.0.133 (10.10.0.133), Dst: 10.10.0.107) Transmission Control Protocol, Src Port: ssh (22), Dst Port: 33048 (33048), Seq: 16001, Ack: 5069, Len: 0 Source port: ssh (22) Destination port: 3048 (33048) [Stream index: 1] Sequence number: 5069 (relative sequence number) Vindow Size 7. TCP sequence number Note that the sequence number is the sequence number) Vindow Size 116.0.0.000 (relative ack number) 7. TCP sequence number: 5069 (relative ack number) Vindow Size 116.0.0.000 (relative ack number) 8. TCP windOwy Size 8. TCP windOwy Size Vindow Size 10.40.0.000 (relative ack number) F.4.(0.0.0.000 (relative ack number)) Vindow Size 10.40.000 (relative ack number) F.4.(0.0.0.000 (relative ack number)) Vindow Size 10.40.000 (relative ack number) F.4.(0.0.000 (relative ack number)) Vindow Size 10.40.000 (relative ack number) F.4.(0.0.000 (relative ack number) Vindow Size 10.40.000 (relative ack number) F.4.(0.0.000 (relative ack number) Vindow Size 10.40.000 (re											
Frane 664 (68 bytes on vire, 68 bytes captured) Linux cooked capture Internet Protocol, Src: 10.10.0.133 (10.10.0.133), Dst: 10.10.0.107 (10.10.0.107) Transmission Control Protocol, Src: 20.10.0.133 (10.10.0.133), Dst: 10.10.0.107 (10.10.0.107) Source port: ssh (22) Destination port: 33048 (33048) [Stream index: 1] Sequence number: 16001 (relative sequence number) Header length: 32 bytes > Flags: 0x10 (ACK) Window size: 2140 • Checksum: 0x49dd [Unov 0 potions: (12 bytes) > [St0/ACK analysis] • [St0/ACK analysis] • [St0/ACK analysis] • [St0 0 0 0 0 1 00 06 62 215 6d c5 c3 c7 00 0 08 06] • [A + 0.0 0 0 0 1 00 06 62 215 6d c5 c3 c7 00 0 08 06] • [St0/ACK analysis]											
Internet Protocol, Src: 10.10.0.133 (10.10.0.133), Dst: 10.10.0.107 (10.10.0.107) Transmission Control Protocol, Src Port: ssh (22), Dst Port: 33048 (33048), Seq: 16001, Ack: 5069, Len: 0 Source port: ssh (22) Destination port: 33048 (33048) [Stream index: 1] Sequence number: 16001 (relative sequence number) Header lengt: 32 bytes Plags: 8x10 (AcK) Window size: 2140 O checksum: 0x49dd [V- 0 potions: [12 bytes] [SEQ/ACK analysis] 0 0 00 00 01 00 06 02 15 6d c5 c3 c7 00 00 08 06 0 45 08 00 34 e2 cb 40 00 40 06 42 ed 08 80 08 65 0 60 00 00 10 08 06 02 15 6d c5 c3 c7 00 00 08 06 0 45 08 00 34 e2 cb 40 00 40 06 42 ed 08 80 08 65 0 9 00 00 10 80 06 00 10 80 06 09 10 81 80 70 e8 09 58 11 		The, of bytes captured)									
Transmission Control Protocol, Src Port: ssh (22) Dst Port: 33048 (33048), Seq: 16001, Ack: 5069, Len: 0 Source port: ssh (22) Destination port: 33048 (33048) [Stream index: 1] Sequence number: 16001 (relative sequence number) Sequence number: 16001 (relative sequence number) Image: Control Protocol, Src Port: Source port: ssh (22) P Flags: 0x10 (AcK) (relative sequence number) Image: Control Protocol, Src Port: Source		10 10 0 122 (10 10 0 122)	Det. 10 10 0 107 (10	10 0 107)							
Source port: ssh (22) Destination port: 33048 (33048) [Stream index: 1] Sequence number: 16001 (relative sequence number) Header length: 32 bytes > Flags: 0x10 (ACK) Window size: 2140 • Options: (12 bytes) > [SEQ/ACK analysis] 00 00 00 00 01 00 06 02 15 6d C5 C3 C7 00 00 08 06 ISEQ/ACK analysis] 00 00 00 00 01 00 06 02 15 6d C5 C3 C7 00 00 08 06 ISEQ/ACK analysis] 01 45 88 60 34 e2 cb 40 00 48 66 42 ed 68 40 885 20 8a 9a 06 66 90 16 81 18 7e 26 fd d6 47 34 87 11 					01 Ack, 5060	l en ·	0				
Destination port: 33048 (33048) [Stream index: 1] Sequence number: 5069 (relative sequence number) Acknowledgement number: 5069 (relative ack number) Header length: 32 bytes > Flags: 0x10 (ACK) Window size: 2140 > Checksum: 0x49dd [V- > C		totot, sit Port: SSH (22),	USC PUIL: 33040 (3304	-0), Sed: 100	01, ACK: 3009	, Len:	U				
[Stream index: 1] Sequence number: 16001 (relative sequence number) Acknowledgement number: 5069 (relative ack number) Header length: 32 bytes > Flags: 8x10 (ACK) Window size: 2140 > Checksum: 6x49dd [Wr > Checksum: 6x49dd [Wr > Size		(22048)	_								
Acknowledgement number: 5069 (relative ack number) Header length: 32 bytes (relative ack number) > Flags: 0x10 (ACK) (ACK) Window size: 2140 (is		10 (JJU40)		TOD							
Acknowledgement number: 5069 (relative ack number) Header length: 32 bytes (relative ack number) > Flags: 0x10 (ACK) (ACK) Window size: 2140 (is				ICP se	equence	Э					
Header Length: 32 bytes Flags: 0x10 (ACK) Window size: 2140 disating O Options: (12 bytes) 8. TCP window Size Size 000 00 00 00 01 00 06 02 15 6d c5 c3 c7 00 00 08 00 02 0a 00 60 00 168 118 72 c6 fd d6 4d 73 48 71 03 80 10 08 5c 49 dd 00 00 01 01 08 0a 00 5a 1 f7											
Flags: 0x10 (ACK) Vindow size: 2140 Checksum: 0x49dd [Vr Options: (12 bytes) B. TCP window Size 00 00 00 00 01 00 06 02 15 6d c5 c3 c7 90 00 88 00 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 0a 08 05 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 0a 00 85 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 0a 00 85 10 45 08 00 36 e2 cb 40 00 40 06 42 ed 0a 0a 00 85 10			nui nui	mber							
Window size: 2140 Viradow size: 2140 Checksum: 0x49dd [Vr Viradow size: 2140 0 options: (12 bytes) 8. TCP window Size Size 00 00 00 00 01 00 66 02 15 6d c5 c3 c7 90 00 88 00 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a ao a0 85 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a ao a0 85 10 45 08 00 36 e2 15 6d c5 c3 c7 90 00 88 00 10 45 08 00 36 e2 cb 40 00 40 06 42 ed 0a ao a0 85 11		25									
Checksum: 0x49dd [v, dis 12 bytes] Checksum: 0x49dd [v, dis 12 bytes] 8. TCP window size 00 00 00 00 01 00 06 02 15 6d c5 c3 c7 00 00 08 00] 10 45 08 00 34 e2 cb 40 00 40 66 42 ed 0a 00 85 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 00 85 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 00 85 10 45 08 00 36 e2 15 6d c5 c3 c7 00 00 08 00] 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 00 85 10 40 85 c49 dd 00 00 01 01 08 0a 00 05 a1 f7 11											
Options: (12 bytes) [SEQ/ACK analysis] S. TCP window Size Si											
P [SE0/ACK analysis] Size 00 00 00 00 01 00 06 02 15 6d c5 c3 c7 00 00 08 00] 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 00 85 20 0a 0a 00 6b 00 16 81 18 72 c6 fd d6 44 73 48 71	▷ Checksum: 0x49dd [Vr-	disa									
P [SE0/ACK analysis] Size 00 00 00 00 01 00 06 02 15 6d c5 c3 c7 00 00 08 00 10 45 08 00 34 e2 cb 40 00 40 06 42 ed 0a 00 85 20 0a 0a 00 6b 00 16 81 18 72 26 fd d6 44 73 48 71	▷ Options: (12 bytes)		window								
Size 30 00		0.101	WINGOW								
00 00 00 00 01 00 60 02 15 6d c5 c3 c7 00 00 00 01 01 06 02 15 6d c5 c3 c7 00 00 00 01 01 00 00 01 01 00 00 01 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 00 00 01 01 <td< td=""><td>,</td><td>oizo</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	,	oizo									
0 45 08 03 42 cb 40 06 42 ed 00 00 00 01 01 08 06 03 00 05 00 16 81 18 72 26 fd 64 73 48 71 k ~6 MsHq 10 08 10 08 56 49 dd 00 01 10 80 00 53 1 ~6 MsHq ~6 MsHq		SIZE		J							
10 45 08 03 42 cb 40 06 42 ed 0a 0a <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>											
20 0a 0a <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>											
10 80 10 08 5 49 dd 00 01 01 08 02 01 01 01 02 01											
Frame (frame), 68 bytes Packets: 2169 Displayed: 2169 Marked: 0 Profile: Default Image: wide wide wide wide wide wide wide wide			k ~&MsHq								
👿 vmuser@dummynetsl 🔟 jh.pcap - Wireshark	30 80 10 08 5c 49 dd 00	00 01 01 08 0a 00 05 a1 f7	\I								
	Frame (frame), 68 bytes	Packets: 2169 Displaye	d: 2169 Marked: 0							Profile: Default	
	🔄 vmuser@dummynetsl	📶 jh.pcap - Wireshark									
											🔊 💽 Right Ct

Miscellaneous

- Some essential Java packages for the assignment:
 - o java.io.File
 - o java.io.FileInputStream
 - o java.io.FileOutputStream
 - java.net.DatagramPacket
 - java.net.DatagramSocket
 - java.net.InetAddress

Q&A