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

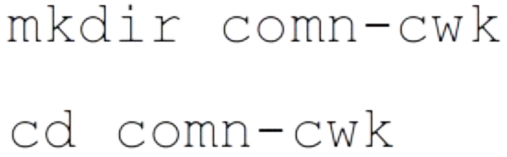
Virtual Machine (VM) Setup

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

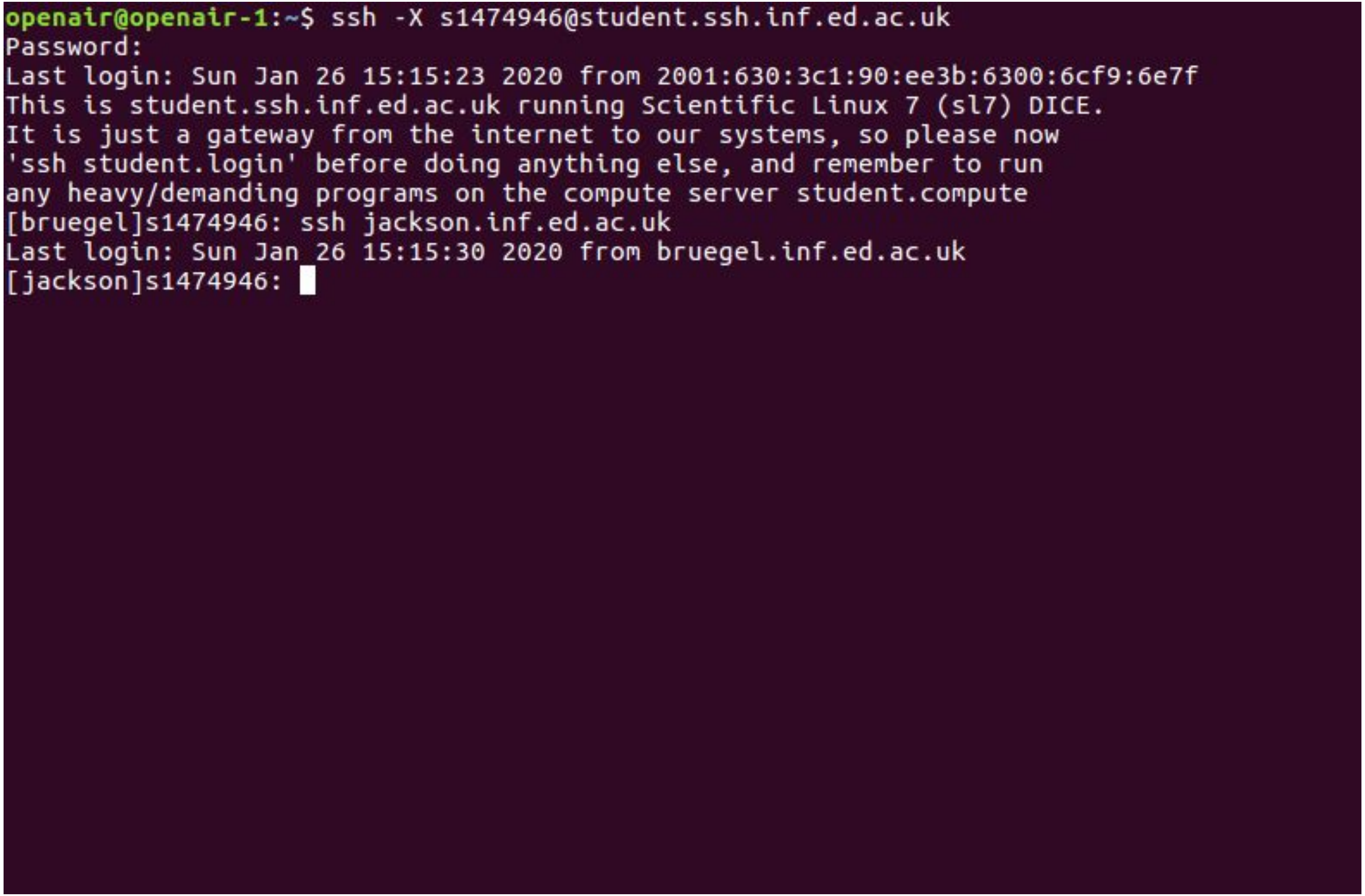
- The VM image for the assignment
  - Can be accessed on DICE machines
  - Has dummynet link emulator and other relevant software

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:
```

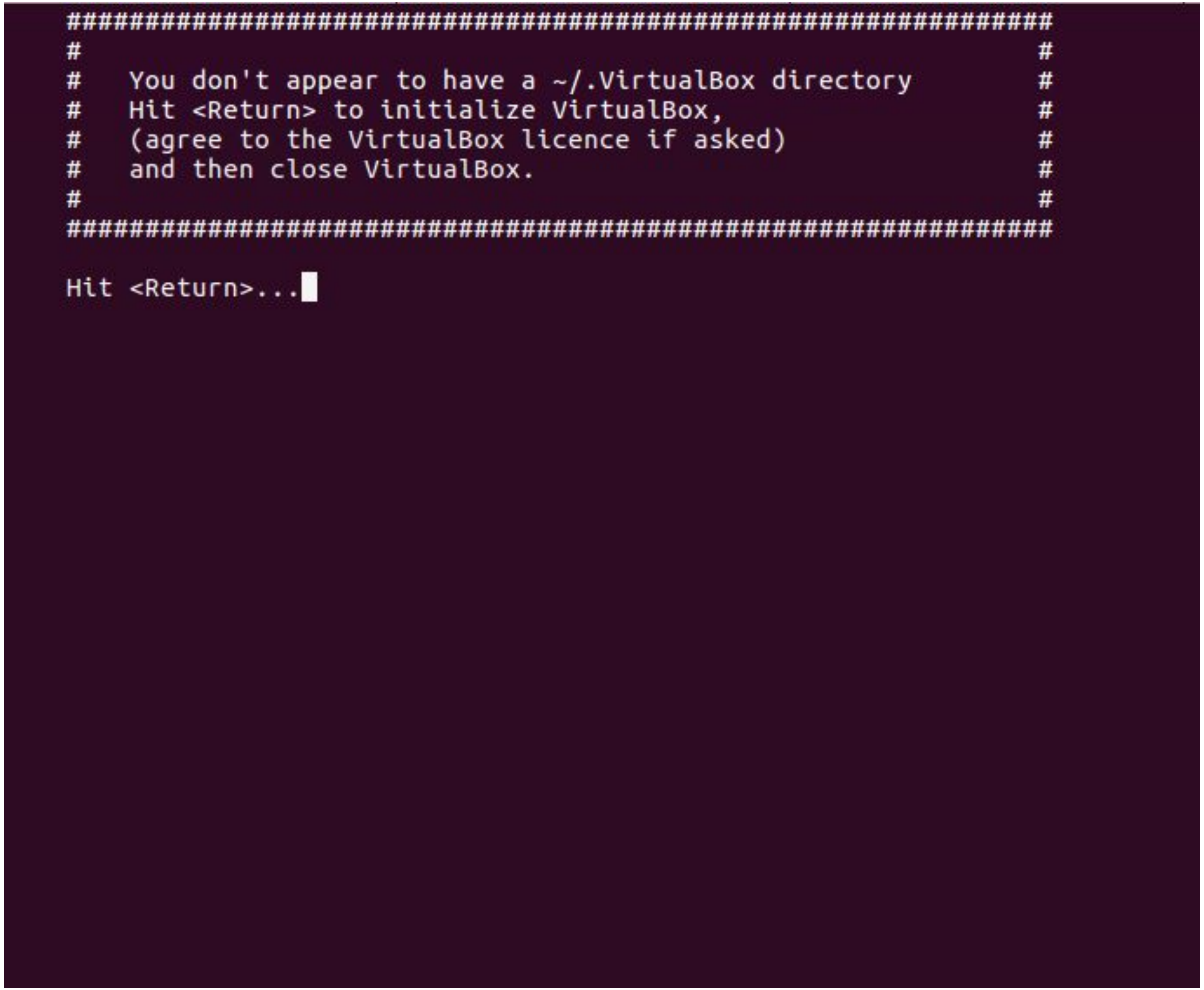
Creating VM

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

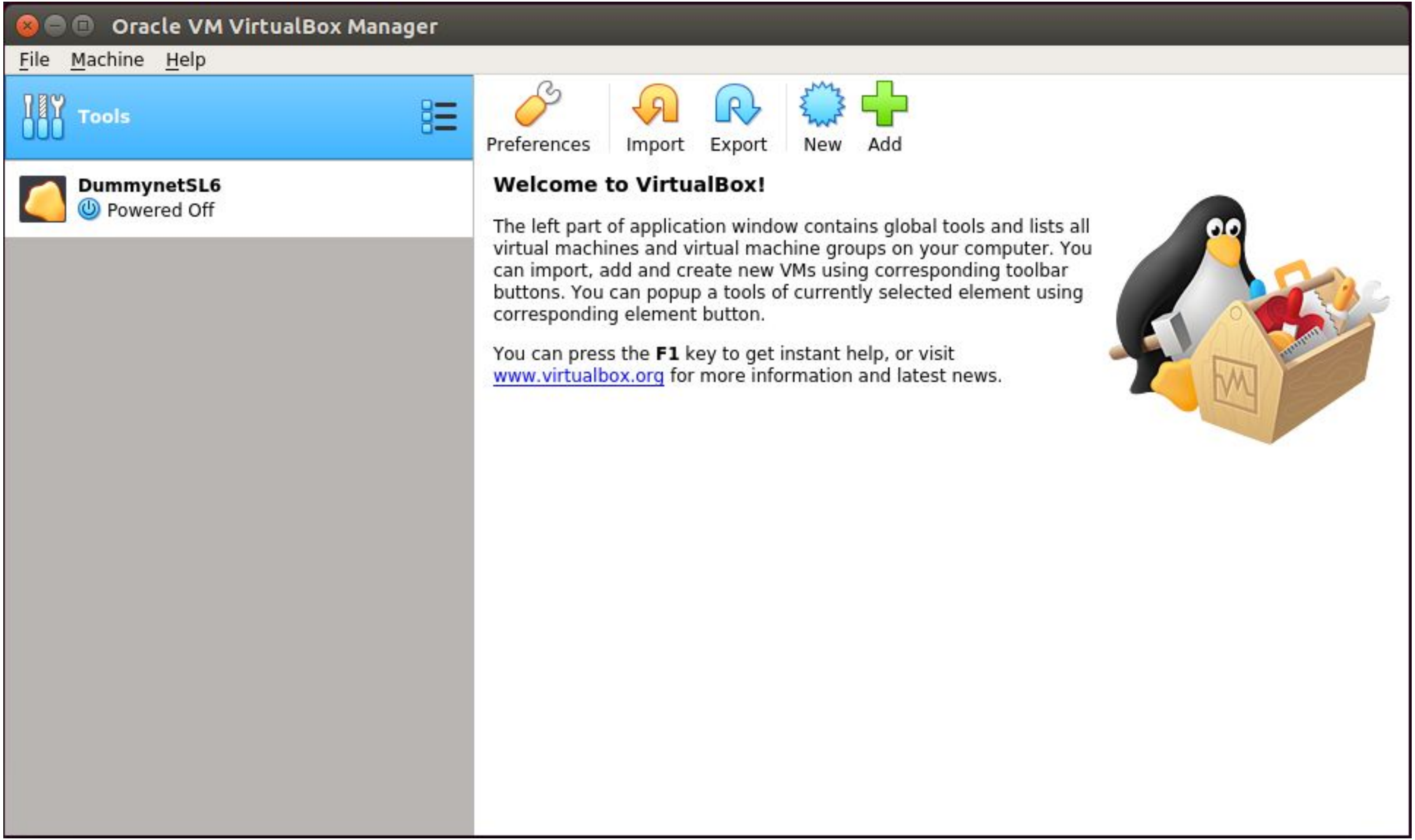
```
mkdir comn-cwk

cd comn-cwk
```

4. Issue the following command:

```
/disk/scratch/dummynet/createdummynetvm
```



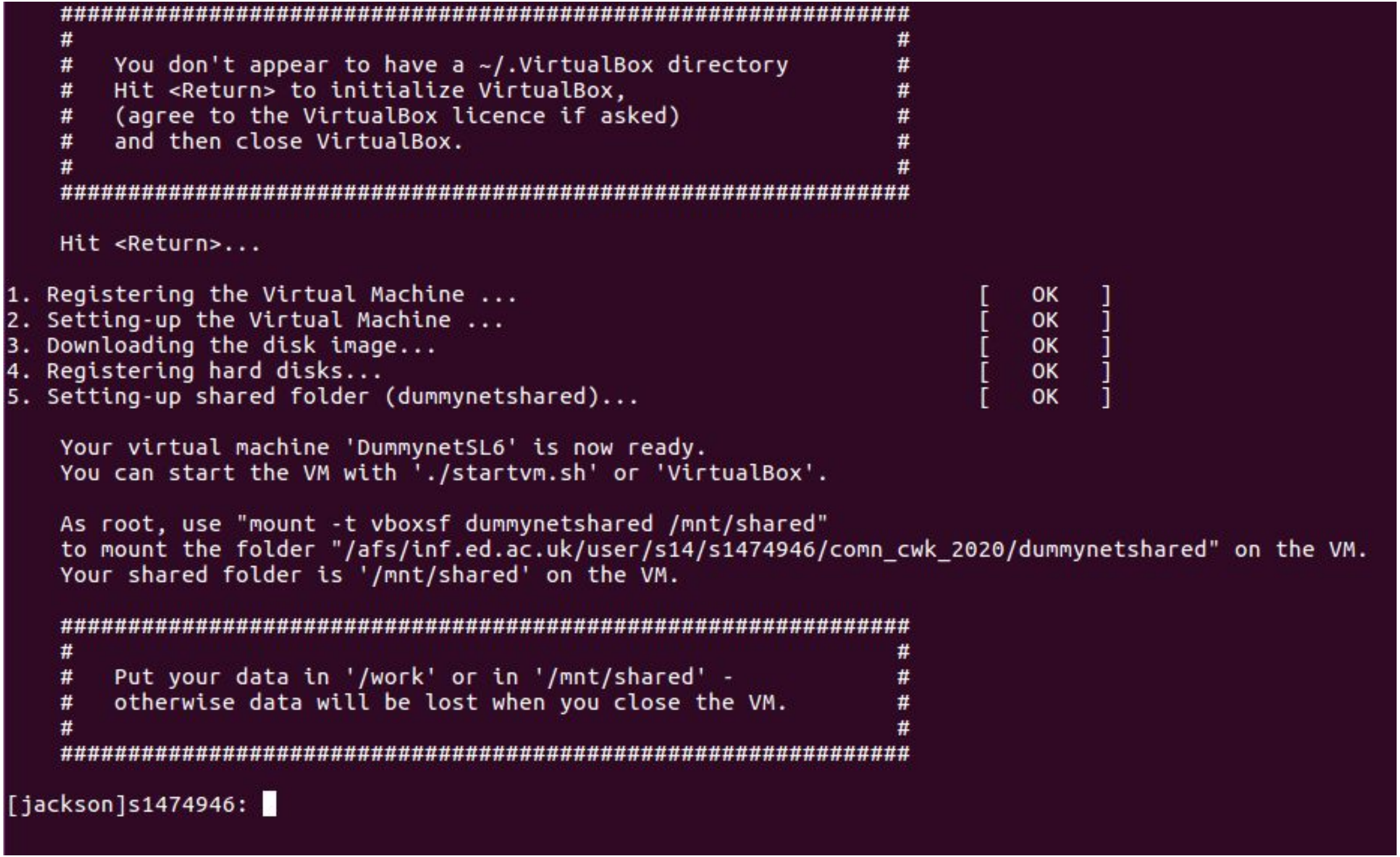
```
###############################################################
#                                                             #
#   You don't appear to have a ~/.VirtualBox directory        #
#   Hit <Return> to initialize VirtualBox,                    #
#   (agree to the VirtualBox licence if asked)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

Hit <Return>...
```



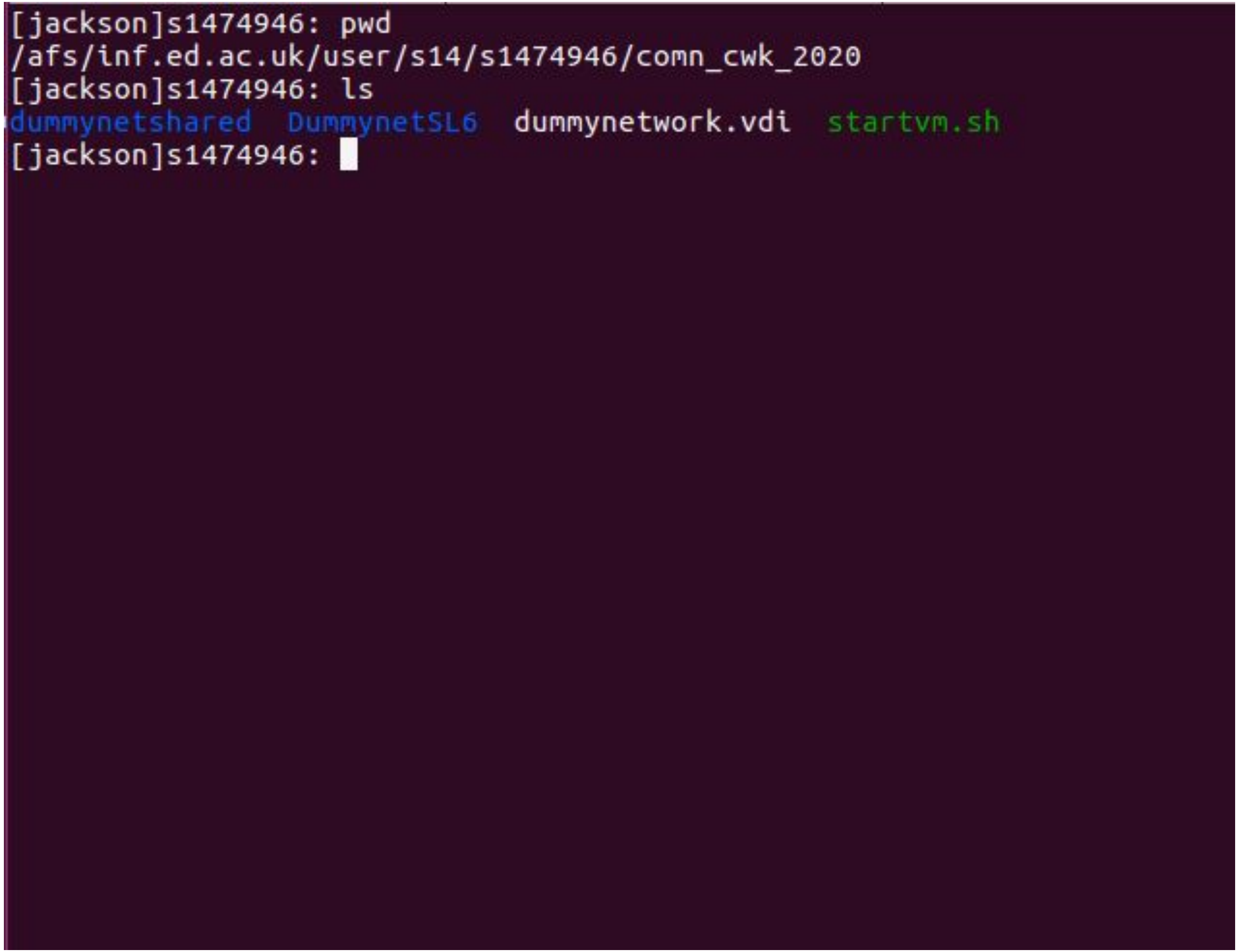
Welcome to VirtualBox!

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 www.virtualbox.org for more information and latest news.



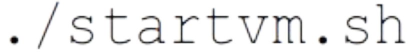
```
    ################################################################
    #                                                              #
    #   You don't appear to have a ~/.VirtualBox directory        #
    #   Hit <Return> to initialize VirtualBox,                     #
    #   (agree to the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

    Hit <Return>...

1. Registering the Virtual Machine ...                                   [   OK   ]
2. Setting-up the Virtual Machine ...                                    [   OK   ]
3. Downloading the disk image...                                         [   OK   ]
4. Registering hard disks...                                             [   OK   ]
5. 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: █
```



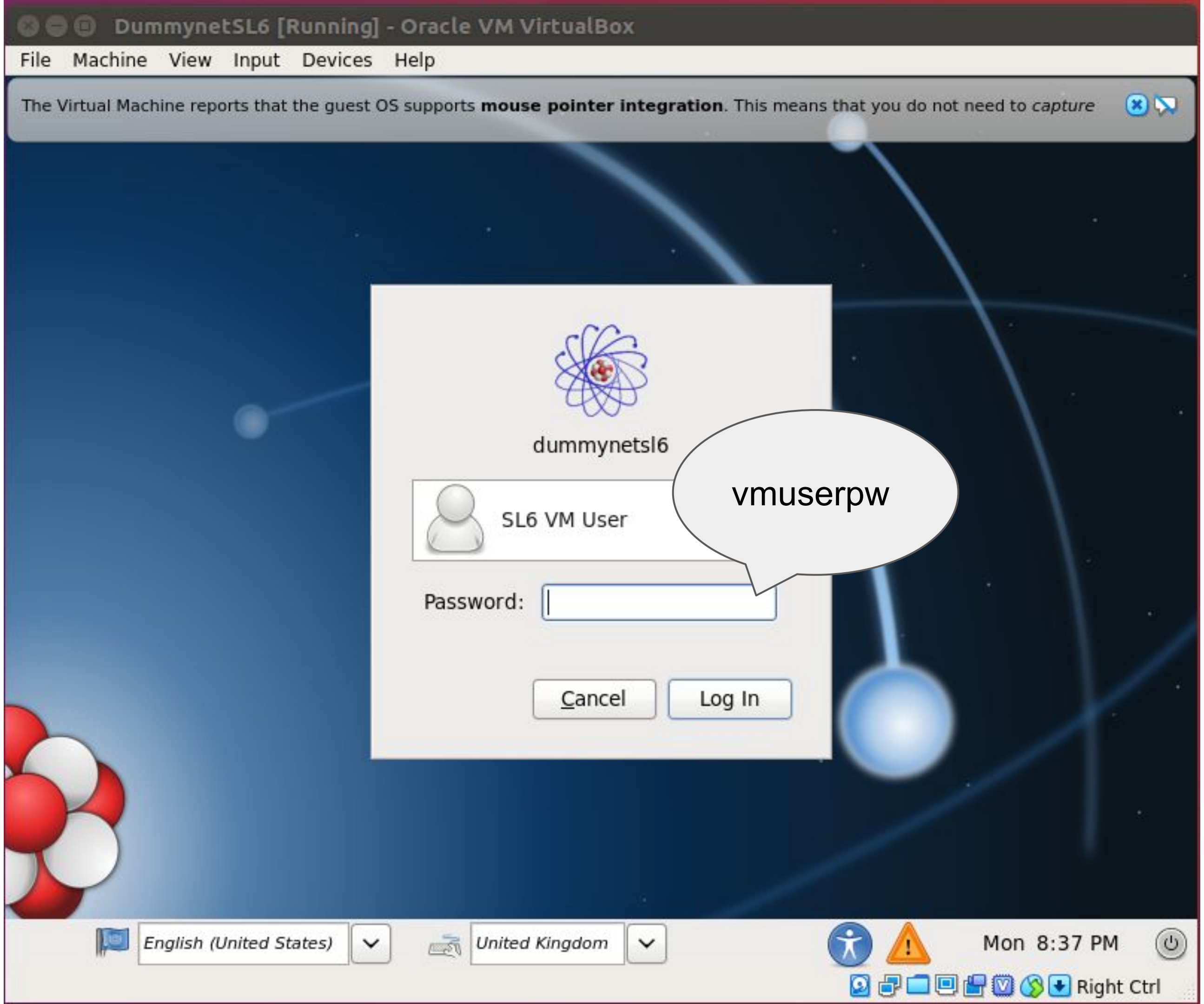
```
[jackson]s1474946: pwd
/afs/inf.ed.ac.uk/user/s14/s1474946/comn_cwk_2020
[jackson]s1474946: ls
dummynetshared  DummynetSL6  dummynetwork.vdi  startvm.sh
[jackson]s1474946: 
```

Creating and Starting VM

5. Run the following command:



```
./startvm.sh
```



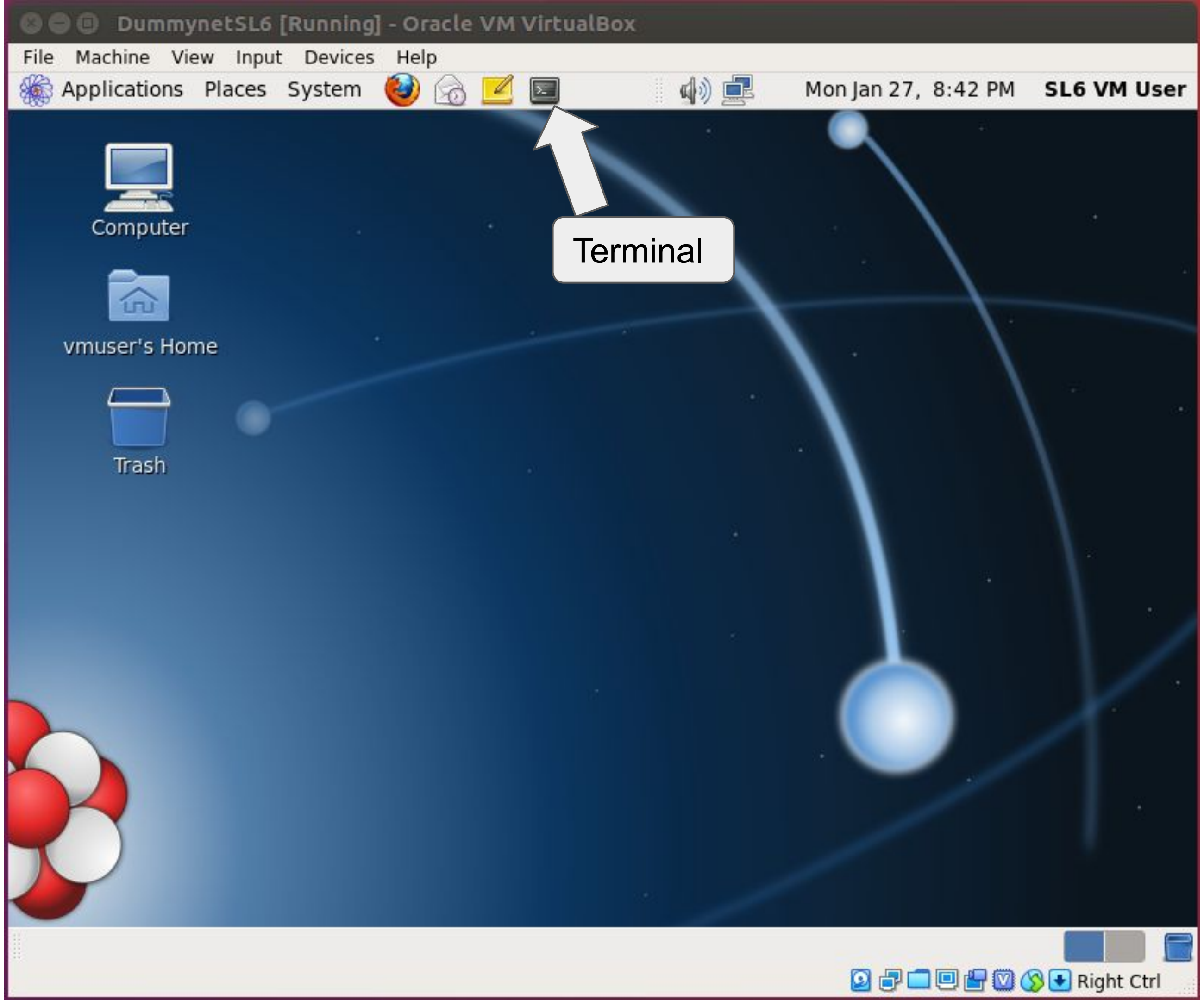
The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture*

Password:

English (United States)

United Kingdom

vmuserpw


DummynetSL6 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Applications
Places
System
Mon Jan 27, 8:42 PM
SL6 VM User
Computer
vmuser's Home
Trash
Right Ctrl

Terminal

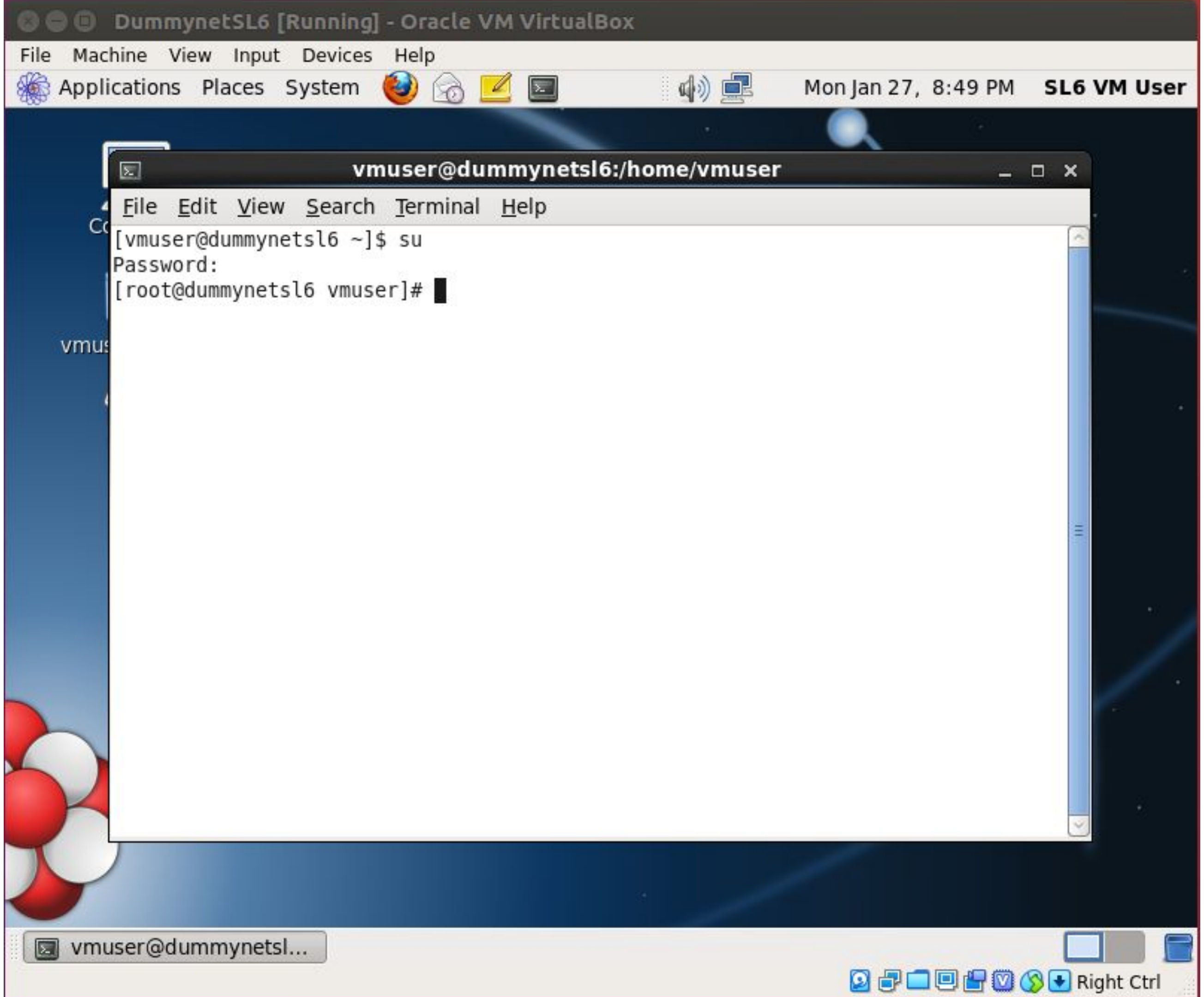
How to shut down VM

- Become a root using ‘su’
  - Root password: vmrootpw

```
su
```

- Run the following command:

```
shutdown -h now
```



DummynetSL6 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Jan 27, 8:49 PM
SL6 VM User
vmuser@dummynetsl6:/home/vmuser
File Edit View Search Terminal Help
vmuser@dummynetsl...
Right Ctrl

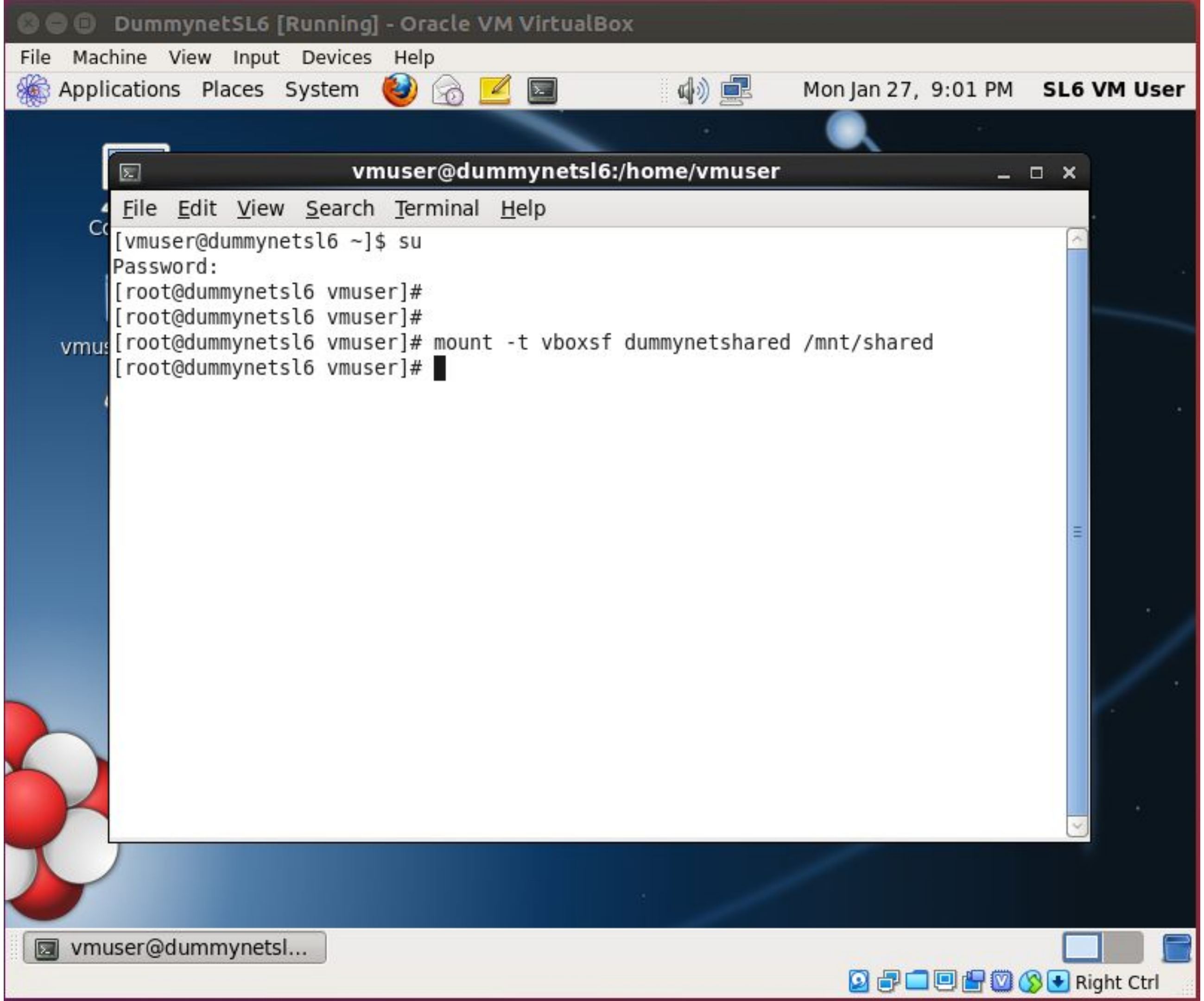
```
[vmuser@dummynetsl6 ~]$ su
Password:
[root@dummynetsl6 vmuser]#
```

Shared Folder

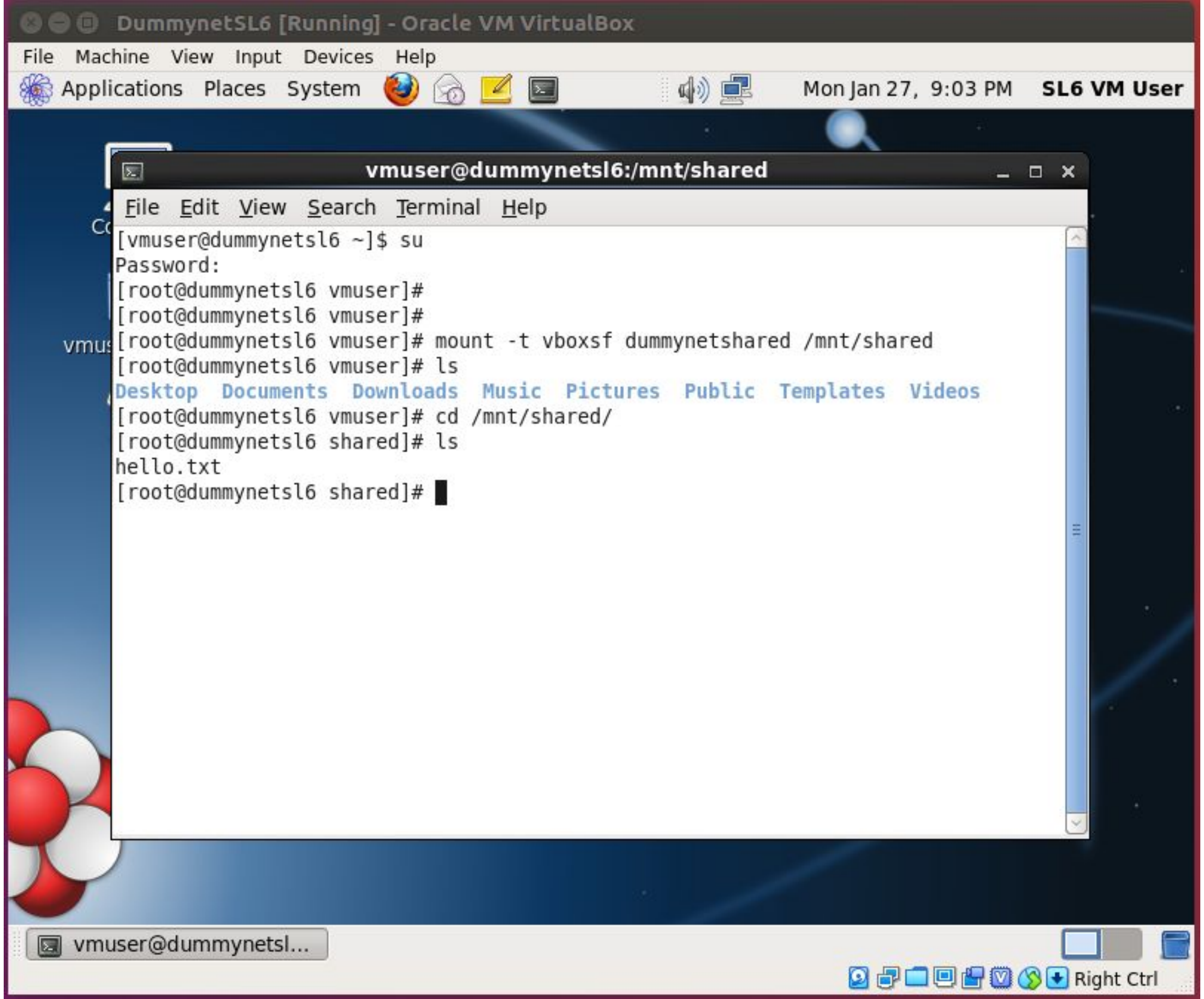
- When the VM is set up for you, a directory called "dummynetshared" gets created in your assignment directory

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

```
mount -t vboxsf dummynetshared /mnt/shared
```

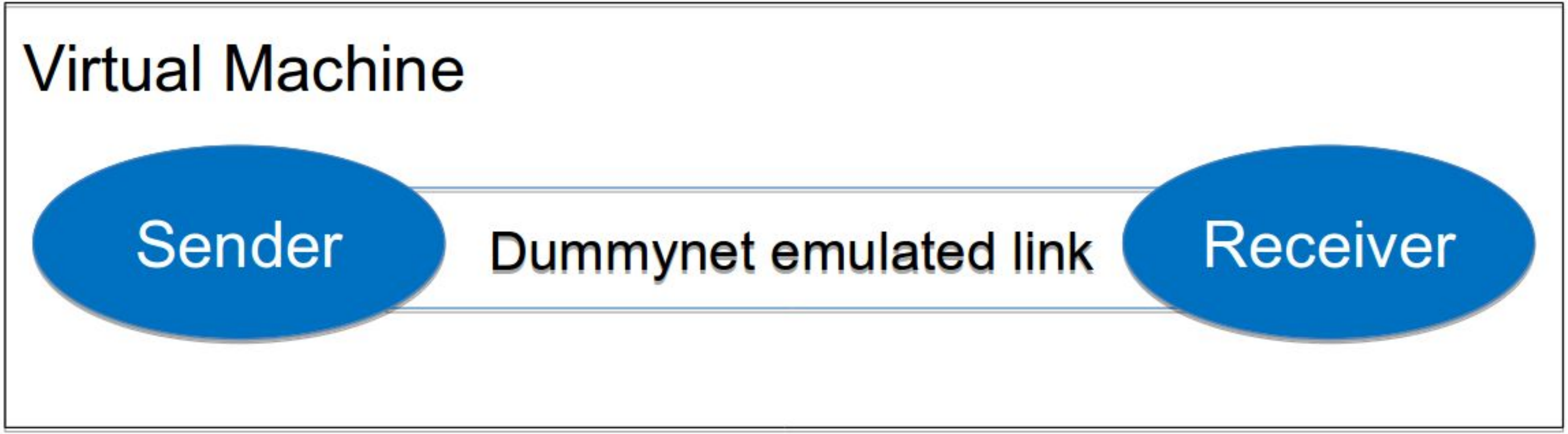


```
[vmuser@dummynetsl6 ~]$ su
Password:
[root@dummynetsl6 vmuser]#
[root@dummynetsl6 vmuser]#
[root@dummynetsl6 vmuser]# mount -t vboxsf dummynetshared /mnt/shared
[root@dummynetsl6 vmuser]# 
```


DummynetSL6 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Jan 27, 9:03 PM
SL6 VM User
vmuser@dummynetsl6:/mnt/shared
File Edit View Search Terminal Help
vmuser@dummynetsl...
Right Ctrl

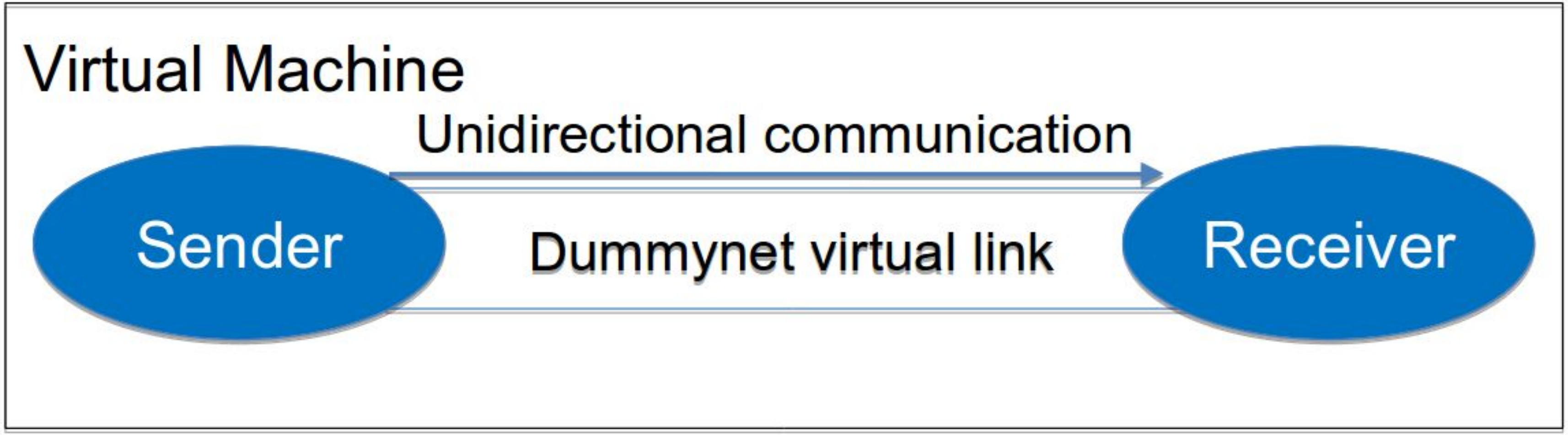
```
[vmuser@dummynetsl6 ~]$ su
Password:
[root@dummynetsl6 vmuser]#
[root@dummynetsl6 vmuser]#
[root@dummynetsl6 vmuser]# mount -t vboxsf dummynetshared /mnt/shared
[root@dummynetsl6 vmuser]# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[root@dummynetsl6 vmuser]# cd /mnt/shared/
[root@dummynetsl6 shared]# ls
hello.txt
[root@dummynetsl6 shared]# 
```

Conceptual Structure



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

Conceptual Structure

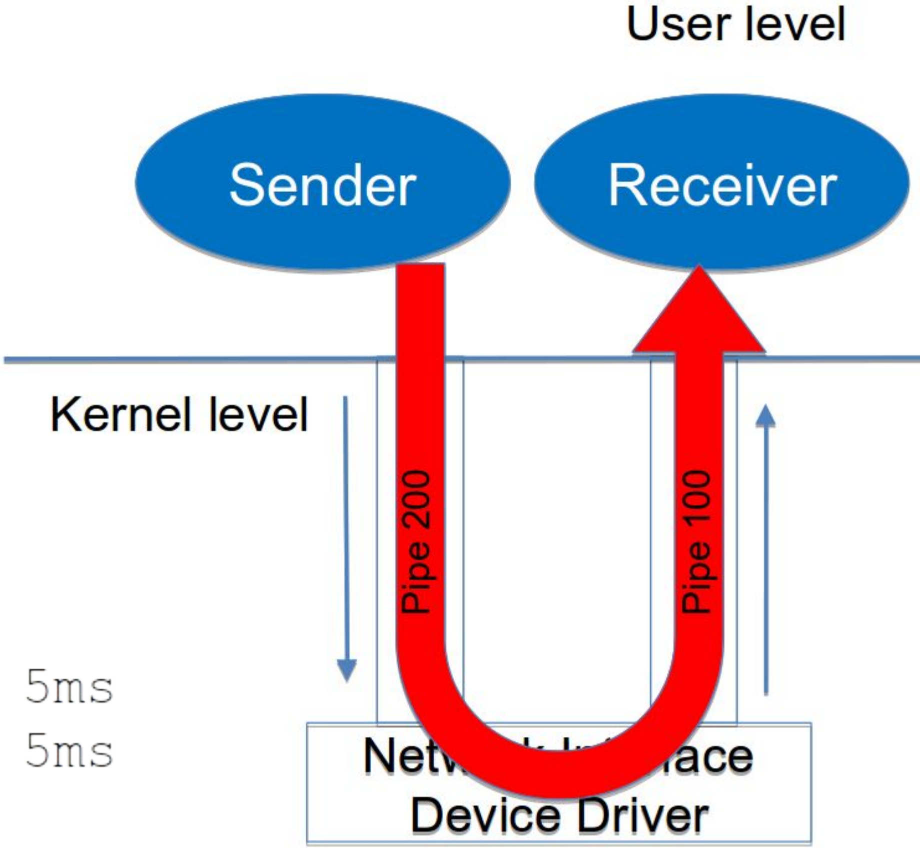


- Sender
    - Reads a file and breaks it into a number of packets
    - Sends the packets to a receiver over a simulated network link
- Receiver
    - Receives the packets; extracts data in the packets; and saves the data in a file

Effect of Dummynet

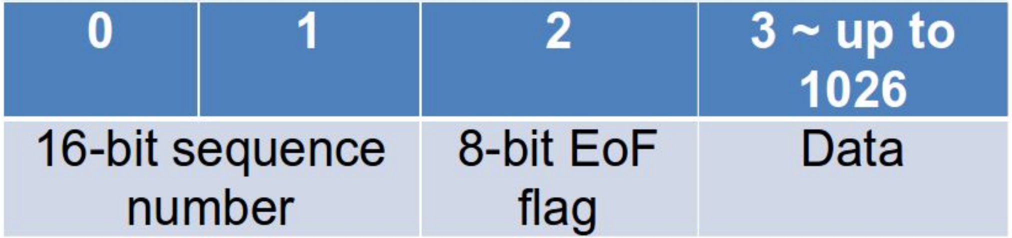
- When processes within the same host (or virtual machine) communicate with each other

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



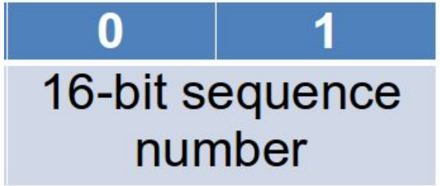
Header format

- 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
16-bit sequence number		8-bit EoF flag	Data

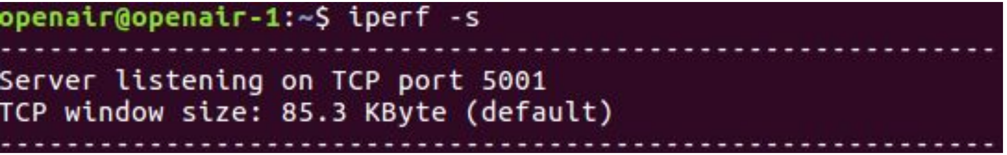
- ACK packet
  - (Receiver to Sender)



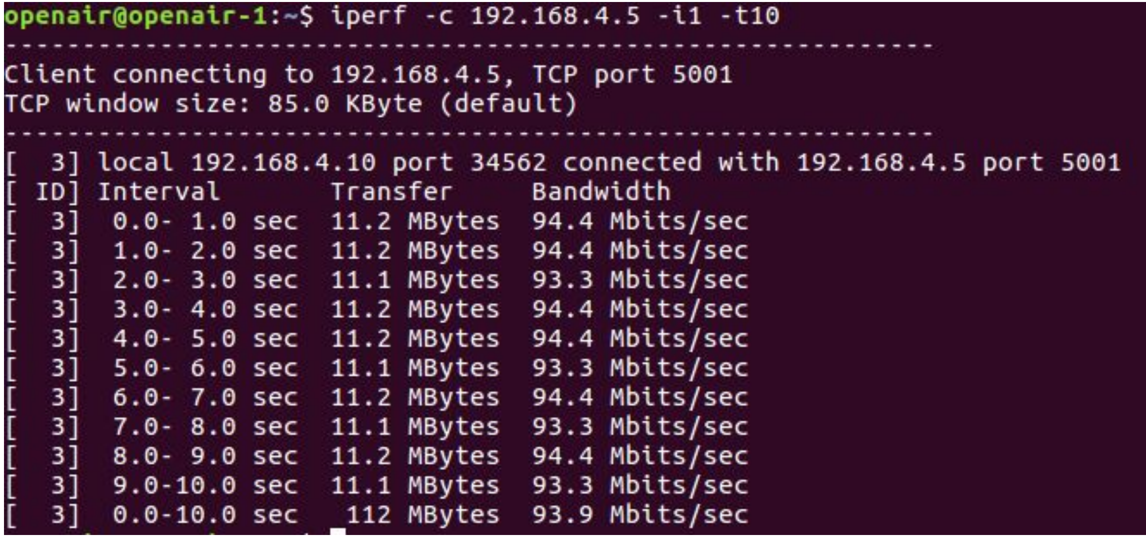
0	1
16-bit sequence number	

iPerf

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

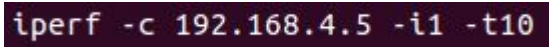


```
openair@openair-1:~$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
```

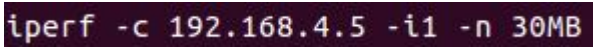


```
openair@openair-1:~$ iperf -c 192.168.4.5 -i1 -t10
------------------------------------------------------------
Client connecting to 192.168.4.5, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.4.10 port 34562 connected 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
```

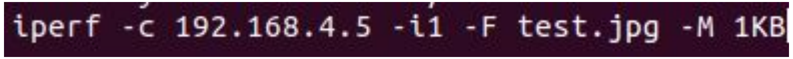
iPerf



```
iperf -c 192.168.4.5 -i1 -t10
```



```
iperf -c 192.168.4.5 -i1 -n 30MB
```



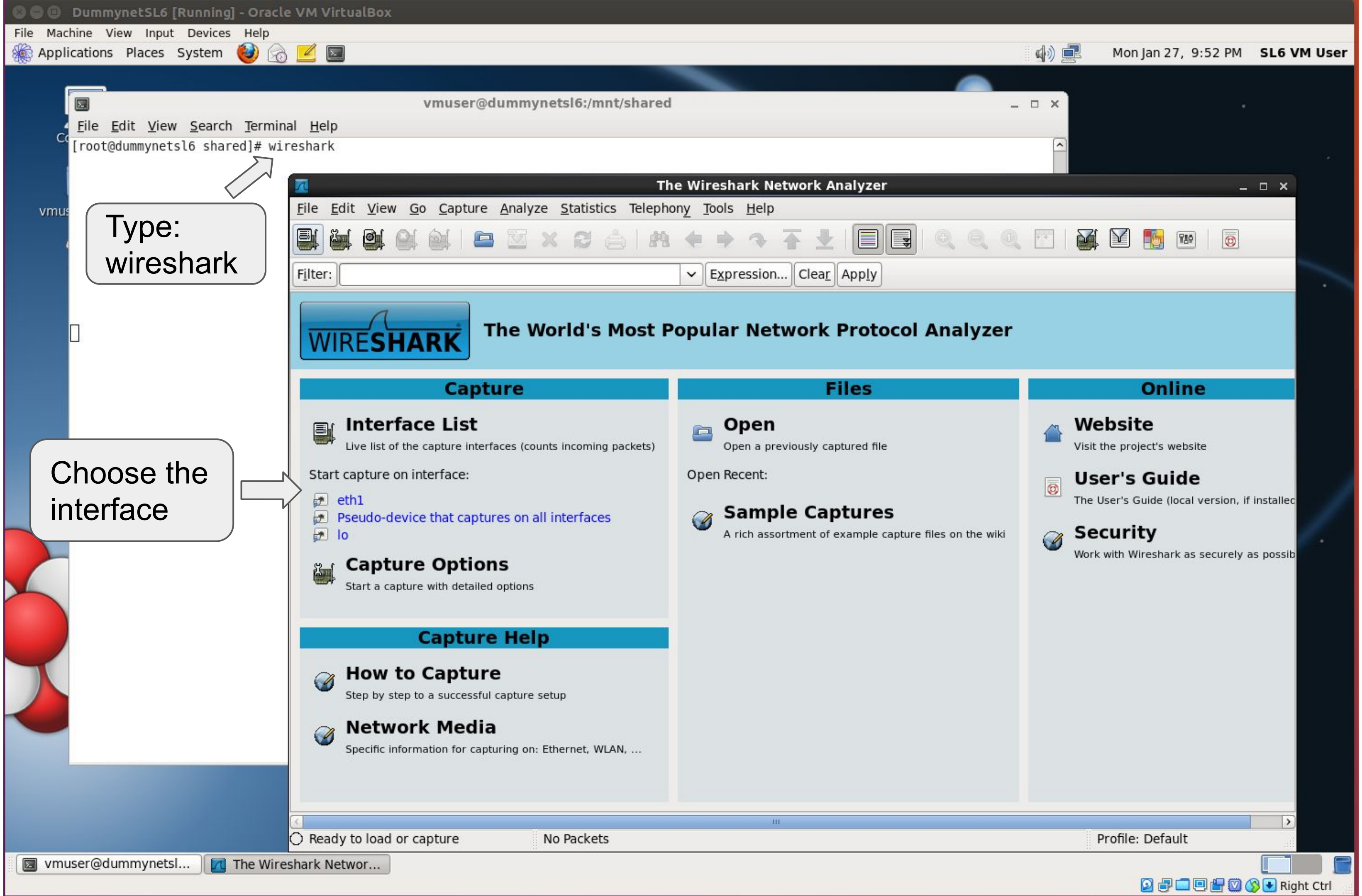
```
iperf -c 192.168.4.5 -i1 -F test.jpg -M 1KB
```

- -c → Receiver IP address
- -i → Interval, seconds between periodic bandwidth reports
- -t → time in seconds to transmit for (default 10 secs)
- -n → number of bytes to transmit (instead of -t)
- -F → input the data to be transmitted from a file
- -M → 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 → wireshark
2. Choose the interface to capture the packets from.
3. Stop recording and save the file.


DummynetSL6 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Jan 27, 9:52 PM SL6 VM User
vmuser@dummynetsl6:/mnt/shared
File Edit View Search Terminal Help
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply
WIRESHARK
vmuser@dummynetsl...
The Wireshark Networ...
Right Ctrl

```
[root@dummynetsl6 shared]# wireshark
```

Type: wireshark

Choose the interface

The World's Most Popular Network Protocol Analyzer

Capture

Interface List
Live list of the capture interfaces (counts incoming packets)

Start capture on interface:
- eth1
- Pseudo-device that captures on all interfaces
- lo

Capture Options
Start a capture with detailed options

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wiki

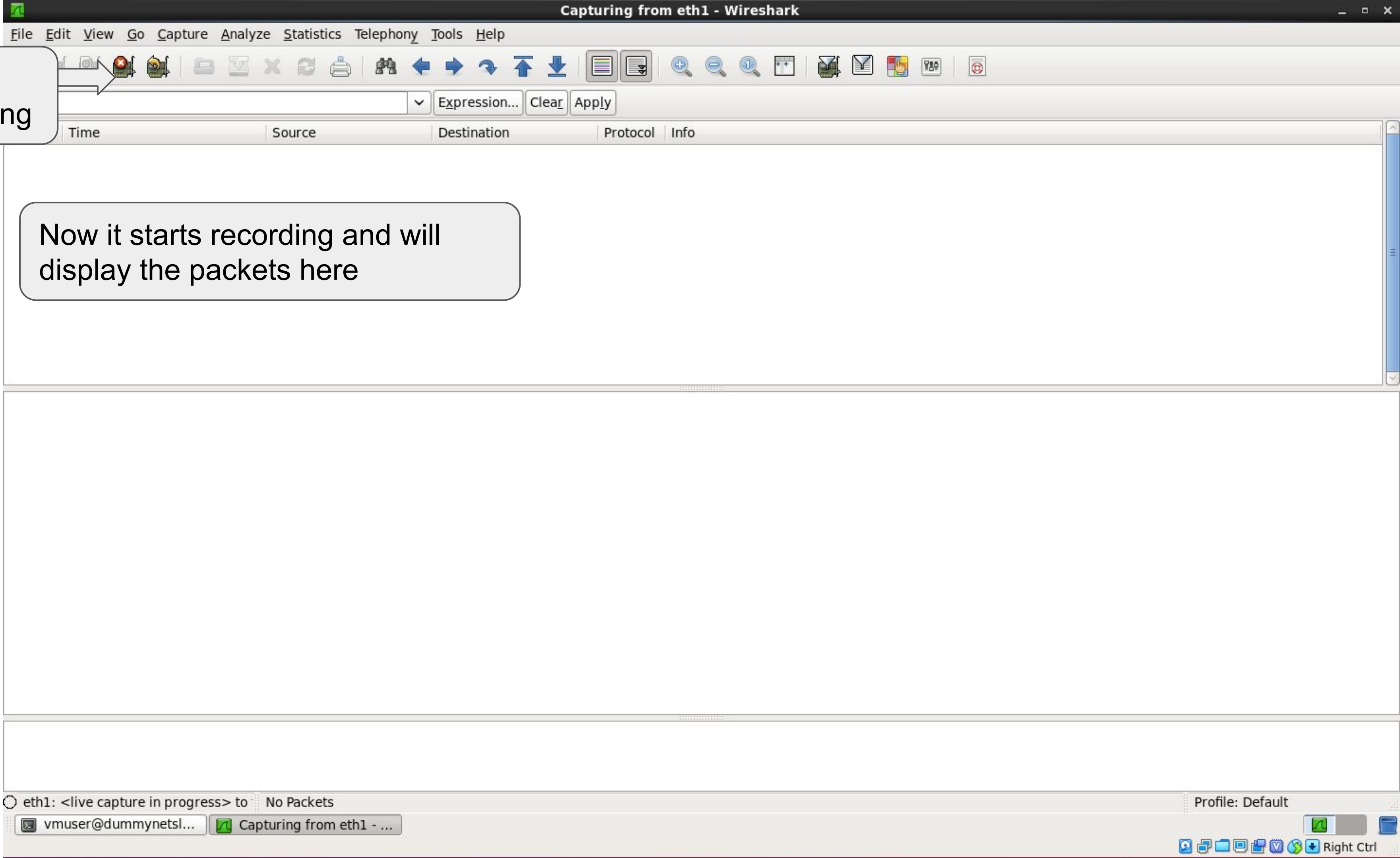
Online

Website
Visit the project's website

User's Guide
The User's Guide (local version, if installec

Security
Work with Wireshark as securely as possib

○ Ready to load or capture | No Packets | Profile: Default



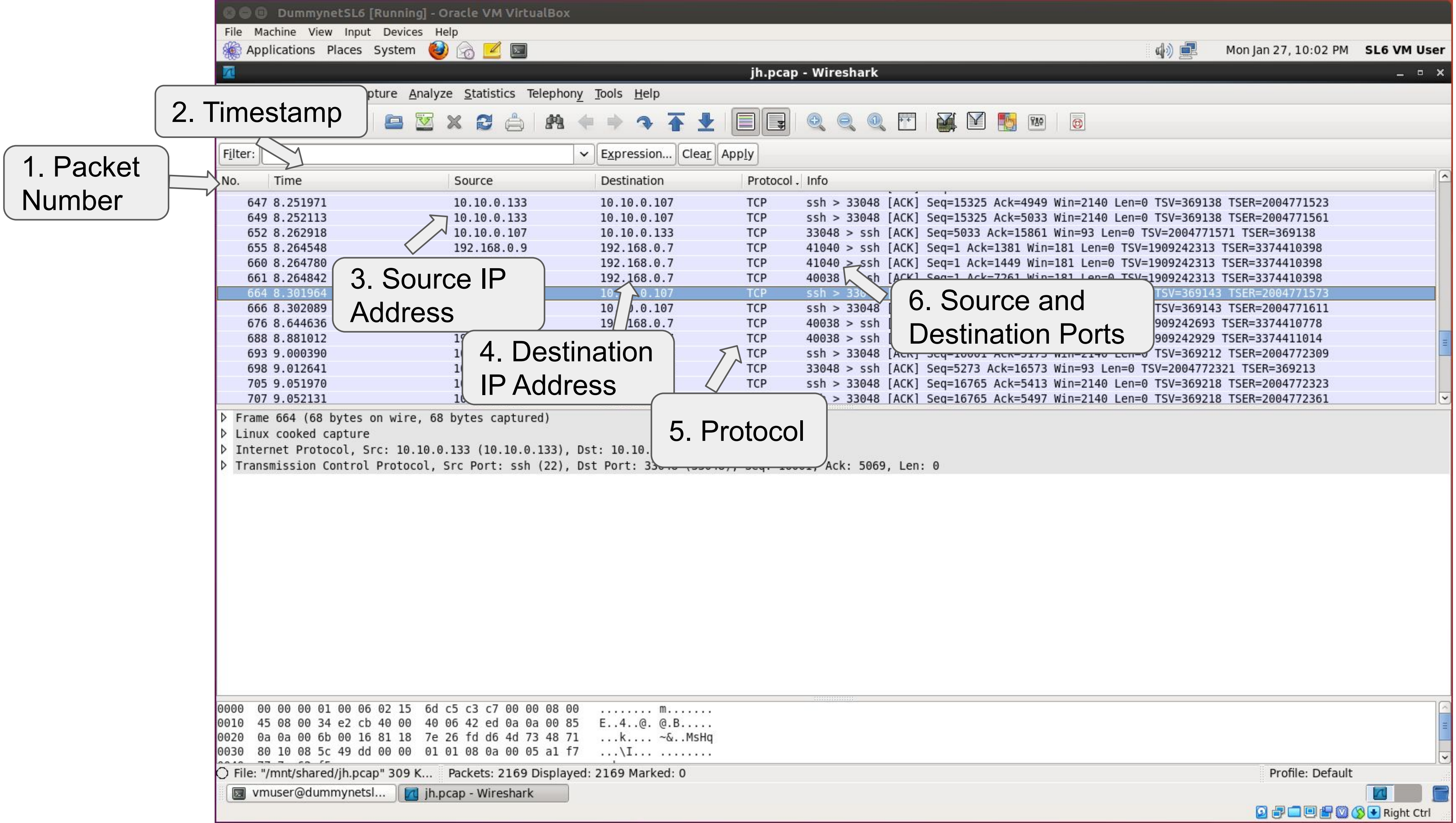
eth1: <live capture in progress> to

No Packets

Profile: Default

Stop recording

Now it starts recording and will display the packets here



DummynetSL6 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Jan 27, 10:02 PM SL6 VM User
jh.pcap - Wireshark
pture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

1. Packet Number

2. Timestamp

3. Source IP Address

4. Destination IP Address

5. Protocol

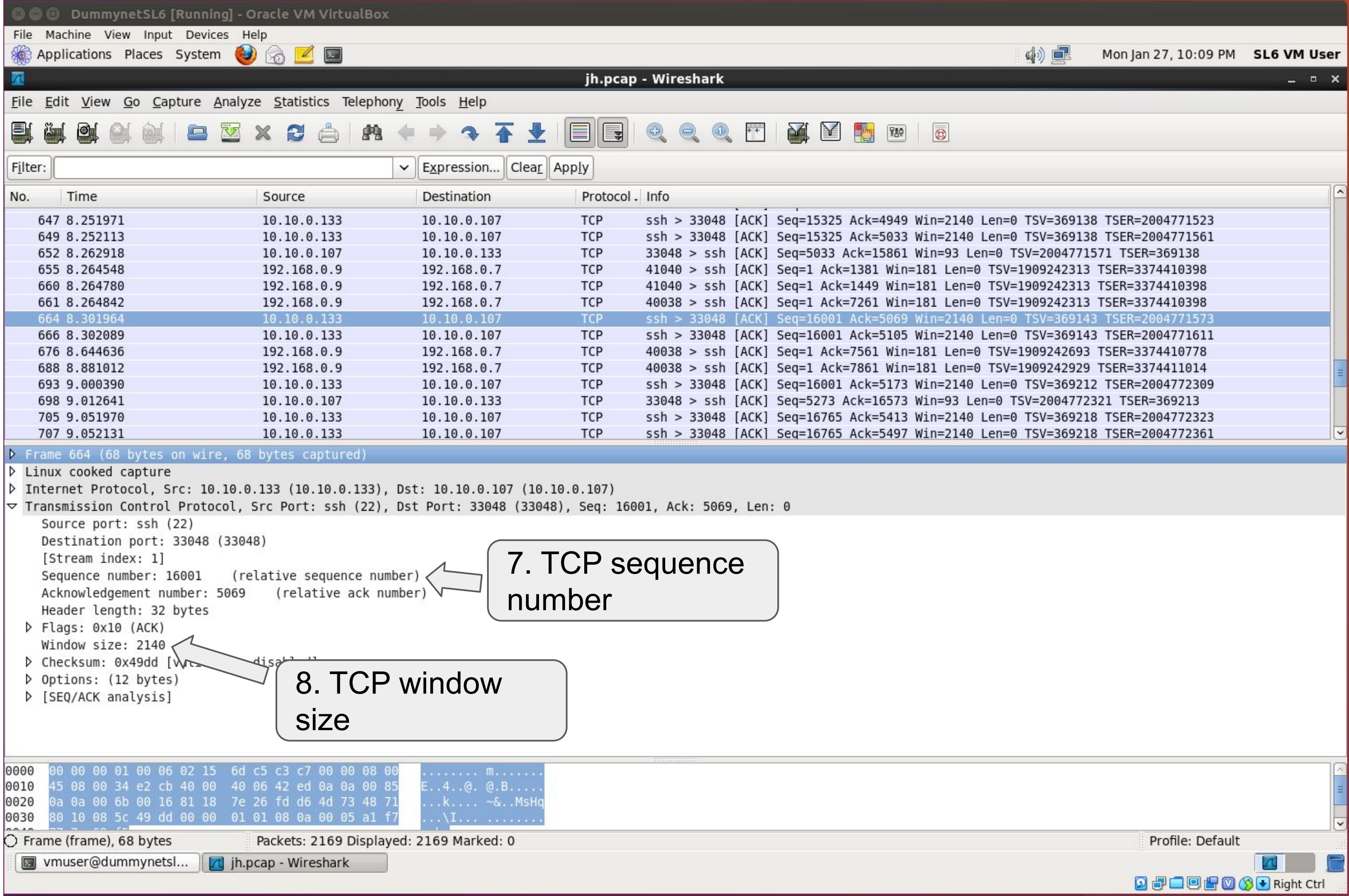
6. Source and Destination Ports

```
No.   Time        Source        Destination   Protocol  Info
  647 8.251971    10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=15325 Ack=4949 Win=2140 Len=0 TSV=369138 TSER=2004771523
  649 8.252113    10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=15325 Ack=5033 Win=2140 Len=0 TSV=369138 TSER=2004771561
  652 8.262918    10.10.0.107   10.10.0.133   TCP       33048 > ssh [ACK] Seq=5033 Ack=15861 Win=93 Len=0 TSV=2004771571 TSER=369138
  655 8.264548    192.168.0.9   192.168.0.7   TCP       41040 > ssh [ACK] Seq=1 Ack=1381 Win=181 Len=0 TSV=1909242313 TSER=3374410398
  660 8.264780                  192.168.0.7   TCP       41040 > ssh [ACK] Seq=1 Ack=1449 Win=181 Len=0 TSV=1909242313 TSER=3374410398
  661 8.264842                  192.168.0.7   TCP       40038 > ssh [ACK] Seq=1 Ack=7261 Win=181 Len=0 TSV=1909242313 TSER=3374410398
  664 8.301964                  10.  0.107    TCP       ssh > 330                                      TSV=369143 TSER=2004771573
  666 8.302089                  10  .0.107    TCP       ssh > 33048 [                                  TSV=369143 TSER=2004771611
  676 8.644636                  19  168.0.7   TCP       40038 > ssh [                                  909242693 TSER=3374410778
  688 8.881012    19                          TCP       40038 > ssh [                                  909242929 TSER=3374411014
  693 9.000390    1                           TCP       ssh > 33048 [ACK]                              TSV=369212 TSER=2004772309
  698 9.012641    1                           TCP       33048 > ssh [ACK] Seq=5273 Ack=16573 Win=93 Len=0 TSV=2004772321 TSER=369213
  705 9.051970    1                           TCP       ssh > 33048 [ACK] Seq=16765 Ack=5413 Win=2140 Len=0 TSV=369218 TSER=2004772323
  707 9.052131    1                                       > 33048 [ACK] Seq=16765 Ack=5497 Win=2140 Len=0 TSV=369218 TSER=2004772361
```

```
▷ 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                    Ack: 5069, Len: 0
```

```
0000  00 00 00 01 00 06 02 15  6d c5 c3 c7 00 00 08 00   ........ m.......
0010  45 08 00 34 e2 cb 40 00  40 06 42 ed 0a 0a 00 85   E..4..@. @.B.....
0020  0a 0a 00 6b 00 16 81 18  7e 26 fd d6 4d 73 48 71   ...k.... ~&..MsHq
0030  80 10 08 5c 49 dd 00 00  01 01 08 0a 00 05 a1 f7   ...\I... ........
```

File: "/mnt/shared/jh.pcap" 309 K...
Packets: 2169 Displayed: 2169 Marked: 0
Profile: Default
vmuser@dummynetsl...
jh.pcap - Wireshark
Right Ctrl


DummynetSL6 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Jan 27, 10:09 PM SL6 VM User
jh.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.   Time       Source        Destination   Protocol  Info
  647 8.251971   10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=15325 Ack=4949 Win=2140 Len=0 TSV=369138 TSER=2004771523
  649 8.252113   10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=15325 Ack=5033 Win=2140 Len=0 TSV=369138 TSER=2004771561
  652 8.262918   10.10.0.107   10.10.0.133   TCP       33048 > ssh [ACK] Seq=5033 Ack=15861 Win=93 Len=0 TSV=2004771571 TSER=369138
  655 8.264548   192.168.0.9   192.168.0.7   TCP       41040 > ssh [ACK] Seq=1 Ack=1381 Win=181 Len=0 TSV=1909242313 TSER=3374410398
  660 8.264780   192.168.0.9   192.168.0.7   TCP       41040 > ssh [ACK] Seq=1 Ack=1449 Win=181 Len=0 TSV=1909242313 TSER=3374410398
  661 8.264842   192.168.0.9   192.168.0.7   TCP       40038 > ssh [ACK] Seq=1 Ack=7261 Win=181 Len=0 TSV=1909242313 TSER=3374410398
  664 8.301964   10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=16001 Ack=5069 Win=2140 Len=0 TSV=369143 TSER=2004771573
  666 8.302089   10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=16001 Ack=5105 Win=2140 Len=0 TSV=369143 TSER=2004771611
  676 8.644636   192.168.0.9   192.168.0.7   TCP       40038 > ssh [ACK] Seq=1 Ack=7561 Win=181 Len=0 TSV=1909242693 TSER=3374410778
  688 8.881012   192.168.0.9   192.168.0.7   TCP       40038 > ssh [ACK] Seq=1 Ack=7861 Win=181 Len=0 TSV=1909242929 TSER=3374411014
  693 9.000390   10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] Seq=16001 Ack=5173 Win=2140 Len=0 TSV=369212 TSER=2004772309
  698 9.012641   10.10.0.107   10.10.0.133   TCP       33048 > ssh [ACK] Seq=5273 Ack=16573 Win=93 Len=0 TSV=2004772321 TSER=369213
  705 9.051970   10.10.0.133   10.10.0.107   TCP       ssh > 33048 [ACK] 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 [ACK] Seq=16765 Ack=5497 Win=2140 Len=0 TSV=369218 TSER=2004772361
```

```
▷ Frame 664 (68 bytes on wire, 68 bytes captured)
▷ Linux cooked capture
▷ Internet Protocol, Src: 10.10.0.133 (10.10.0.133), Dst: 10.10.0.107 (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)
    Acknowledgement number: 5069    (relative ack number)
    Header length: 32 bytes
  ▷ Flags: 0x10 (ACK)
    Window size: 2140
  ▷ Checksum: 0x49dd [validation disabled]
  ▷ Options: (12 bytes)
  ▷ [SEQ/ACK analysis]
```

7. TCP sequence number

8. TCP window size

```
0000  00 00 00 01 00 06 02 15  6d c5 c3 c7 00 00 08 00   ........ m.......
0010  45 08 00 34 e2 cb 40 00  40 06 42 ed 0a 0a 00 85   E..4..@. @.B.....
0020  0a 0a 00 6b 00 16 81 18  7e 26 fd d6 4d 73 48 71   ...k.... ~&..MsHq
0030  80 10 08 5c 49 dd 00 00  01 01 08 0a 00 05 a1 f7   ...\I... ........
```

Frame (frame), 68 bytes   Packets: 2169 Displayed: 2169 Marked: 0   Profile: Default

Miscellaneous

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

Q&A