Wireshark PCAP Analysis Lab Exercise

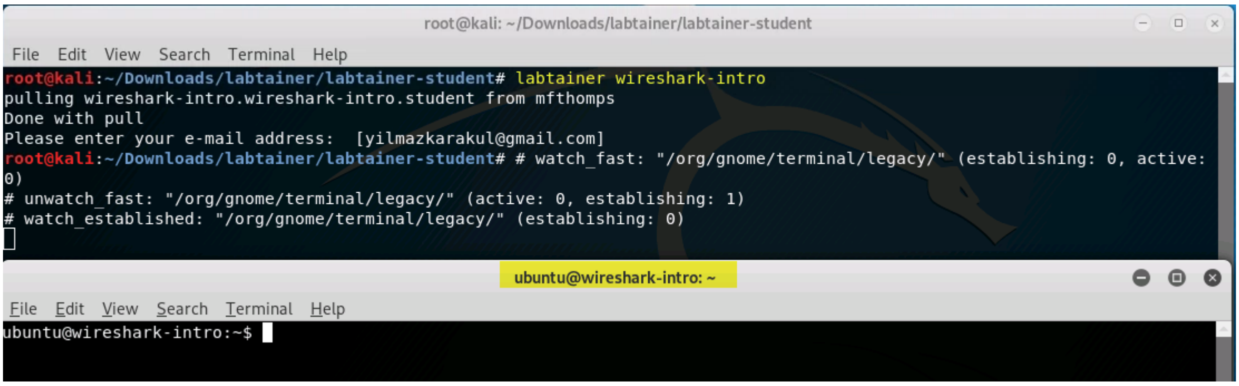
1. Background

This lab introduces analysis of PCAP files using the wireshark tool. You will analyze an existing PCAP, looking for a specific invalid login attempt. PCAP files contain copies of network traffic stored in a format that can be processed by various network analysis tools such as Wireshark and tcpdump. "PCAP" is short for "packet capture".

2. Performing the lab

The lab is started from the Labtainer working directory (labtainer-student) on your Linux host. From there, issue the command:

```
  labtainer wireshark-intro
```


root@kali: ~/Downloads/labtainer/labtainer-student
File Edit View Search Terminal Help
ubuntu@wireshark-intro: ~
File Edit View Search Terminal Help

```
root@kali:~/Downloads/labtainer/labtainer-student# labtainer wireshark-intro
pulling wireshark-intro.wireshark-intro.student from mfthomps
Done with pull
Please enter your e-mail address:  [yilmazkarakul@gmail.com]
root@kali:~/Downloads/labtainer/labtainer-student# # watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active:
0)
# unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
# watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
```

```
ubuntu@wireshark-intro:~$
```

The resulting virtual terminals include a display of these instructions and a terminal connected to a computer that contains the PCAP of interest.

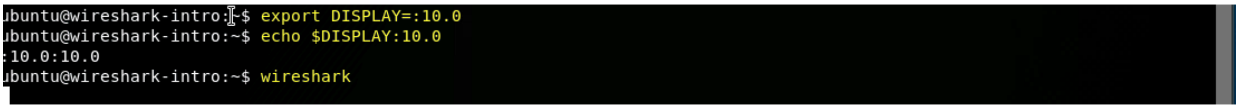
To navigate this instruction, the arrow keys along with with the Space/Home/End/Page-Up/Page-Down keys are usable. To exit navigation of this instruction, type 'q'.

3. Tasks

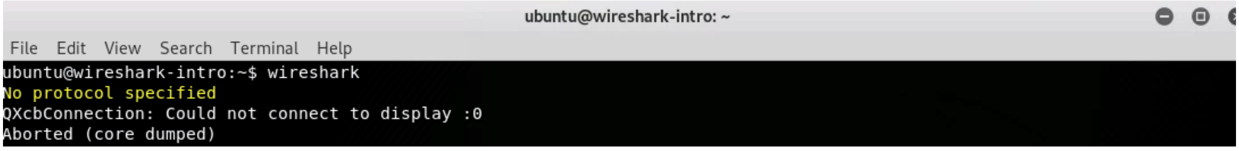
3.1. Run wireshark to perform PCAP Analysis

a. Start a wireshark:

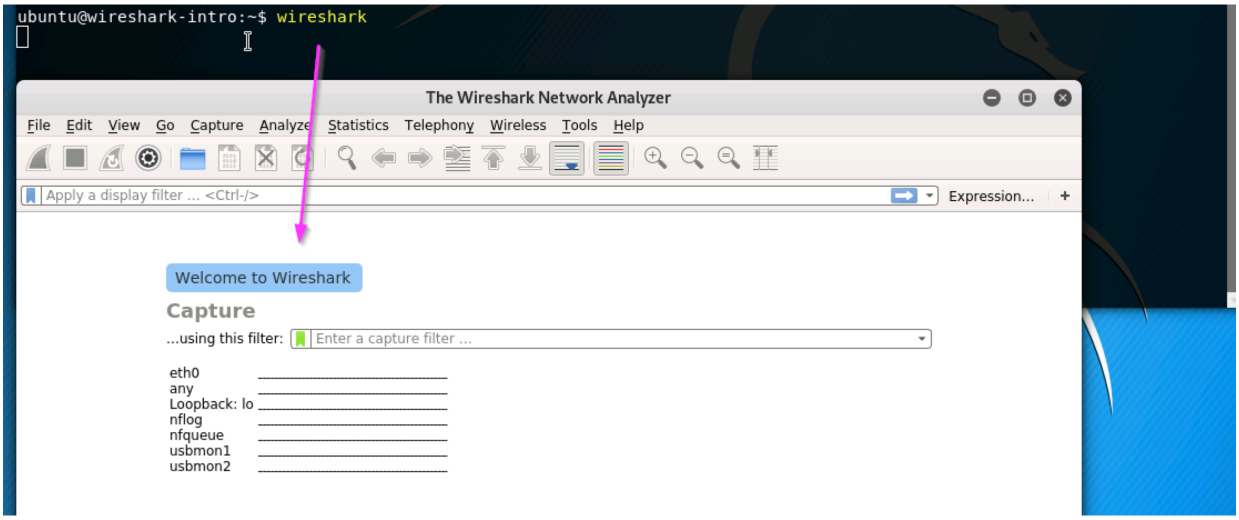
```
Wireshark
```



```
ubuntu@wireshark-intro:~$ export DISPLAY=:10.0
ubuntu@wireshark-intro:~$ echo $DISPLAY:10.0
:10.0:10.0
ubuntu@wireshark-intro:~$ wireshark
```


ubuntu@wireshark-intro: ~
File Edit View Search Terminal Help

```
ubuntu@wireshark-intro:~$ wireshark
No protocol specified
QXcbConnection: Could not connect to display :0
Aborted (core dumped)
```

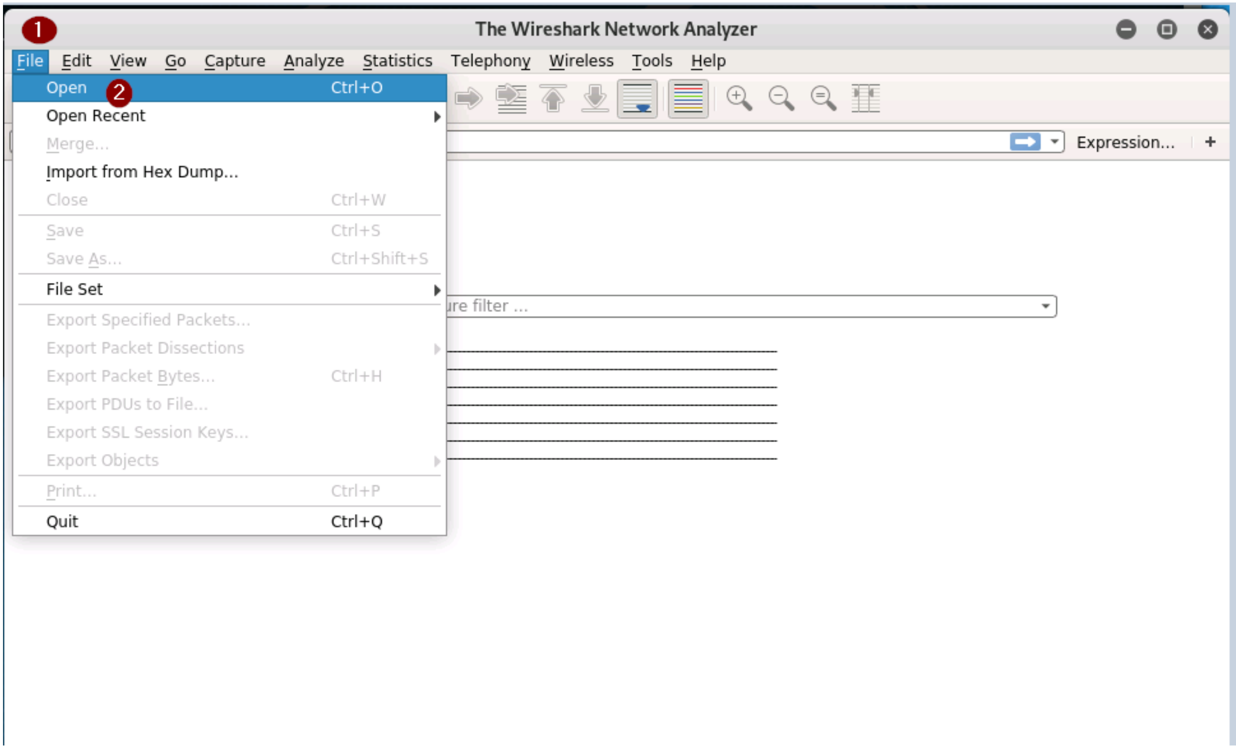


```
ubuntu@wireshark-intro:~$ wireshark
```

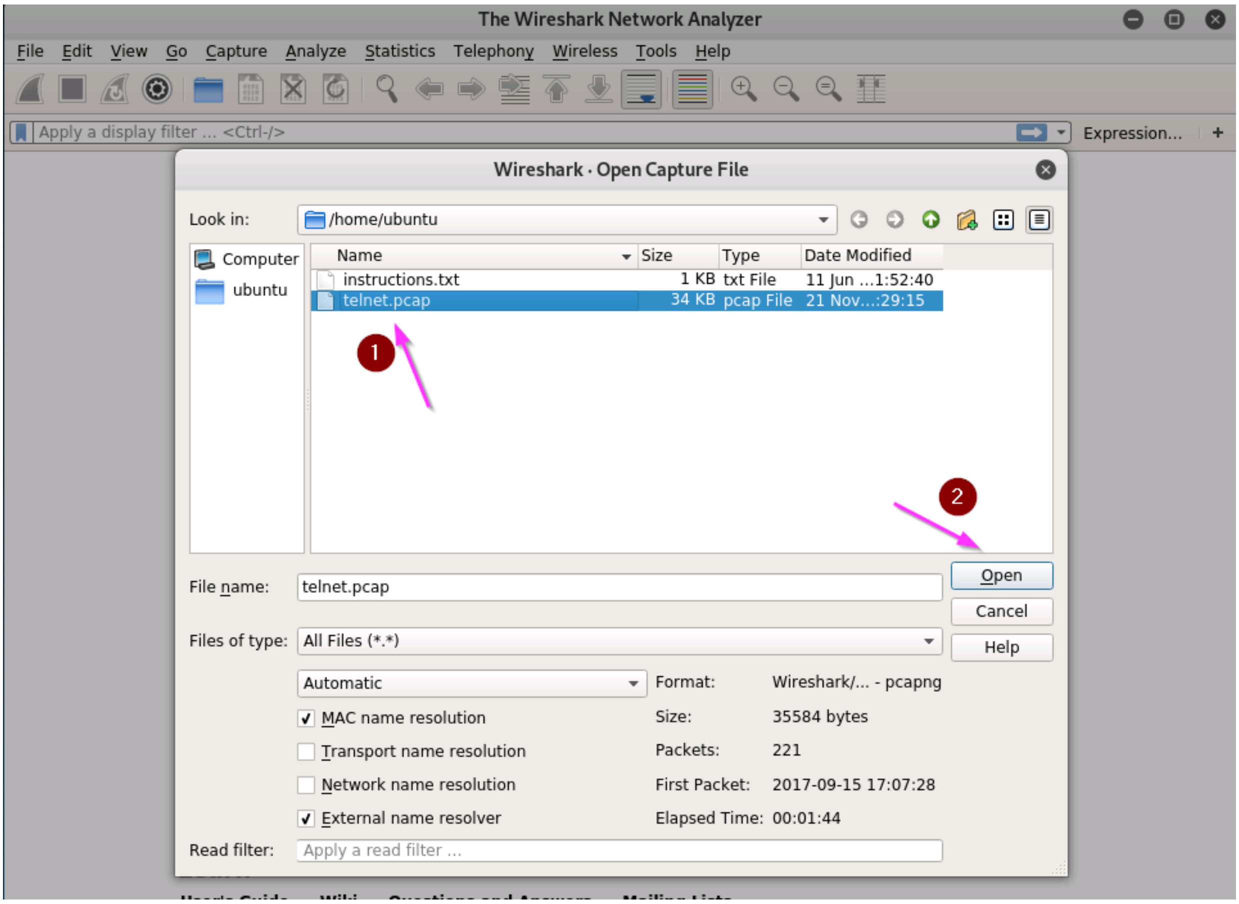
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2

b. Open ’telnet.pcap’ file:

File->Open



select the ’telnet.pcap’ file then click Open


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Wireshark · Open Capture File
Look in:
/home/ubuntu
Computer
ubuntu
Name
Size
Type
Date Modified
1
2
Open
Cancel
Help

Name	Size	Type	Date Modified
instructions.txt	1 KB	txt File	11 Jun ...1:52:40
telnet.pcap	34 KB	pcap File	21 Nov...:29:15

File name: telnet.pcap

Files of type: All Files (*.*)

Automatic

☑ MAC name resolution

□ Transport name resolution

□ Network name resolution

☑ External name resolver

Format: Wireshark/... - pcapng

Size: 35584 bytes

Packets: 221

First Packet: 2017-09-15 17:07:28

Elapsed Time: 00:01:44

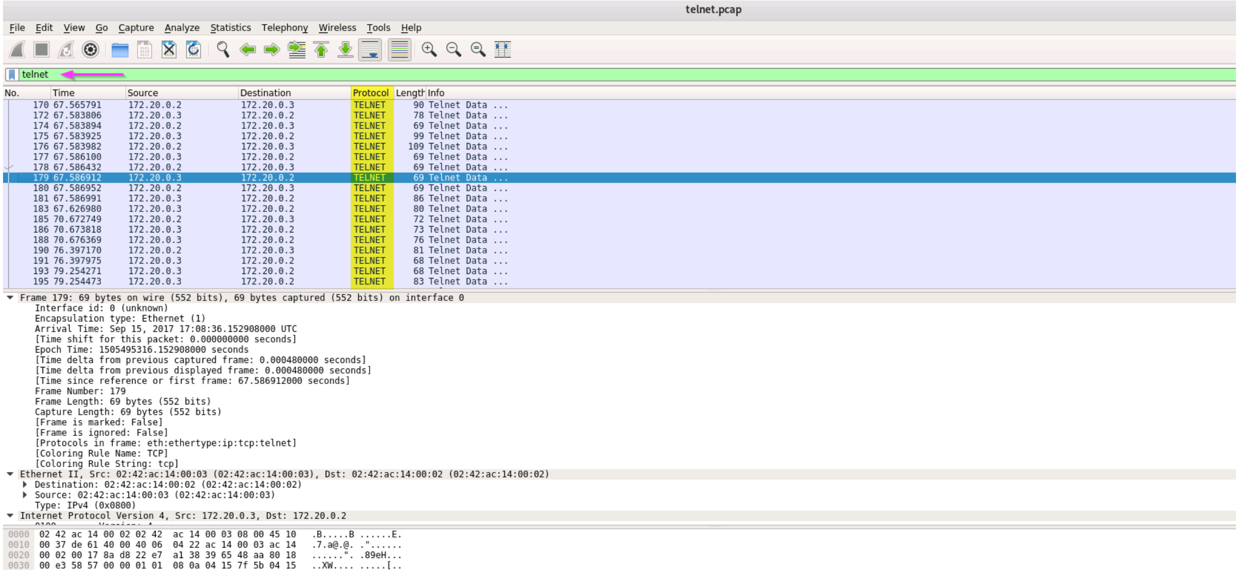
Read filter: Apply a read filter ...

Telnet is a communications protocol that allows a user to issue shell commands to a remote host. Telnet network traffic is not encrypted. Refer to the telnet lab for further background.

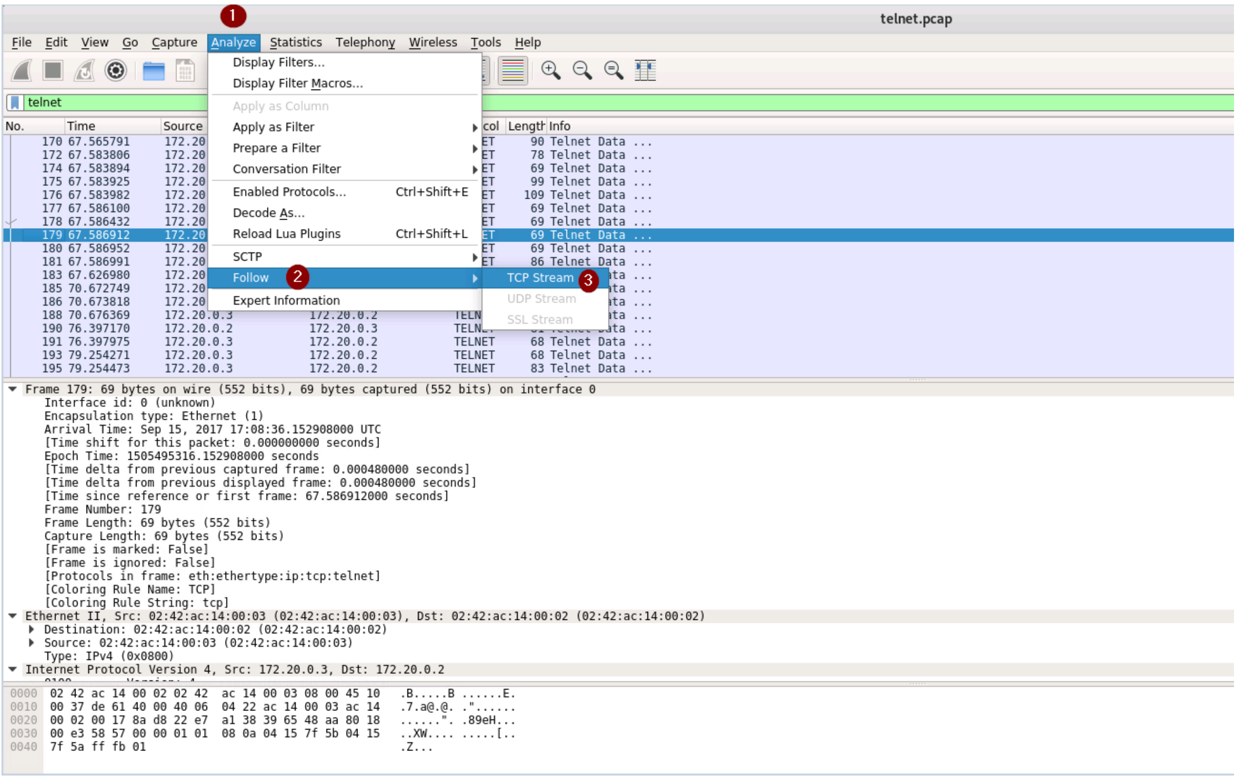
3.2. Search for the packet containing the invalid user "john" password inside a telnet data

Locate the single frame which contains the password provided when the user attempted to login as the "john" user.

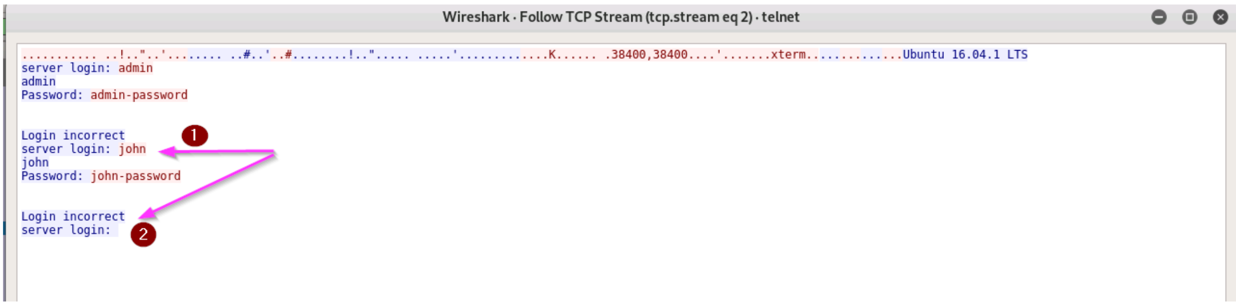
Note: one way is to apply a telnet.data filter


telnet.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet

```
No.   Time        Source       Destination  Protocol Length Info
  170 67.565791   172.20.0.2   172.20.0.3   TELNET     90 Telnet Data ...
  172 67.583806   172.20.0.3   172.20.0.2   TELNET     78 Telnet Data ...
  174 67.583894   172.20.0.2   172.20.0.3   TELNET     69 Telnet Data ...
  175 67.583925   172.20.0.3   172.20.0.2   TELNET     99 Telnet Data ...
  176 67.583982   172.20.0.2   172.20.0.3   TELNET    109 Telnet Data ...
  177 67.586100   172.20.0.3   172.20.0.2   TELNET     69 Telnet Data ...
  178 67.586432   172.20.0.2   172.20.0.3   TELNET     69 Telnet Data ...
  179 67.586912   172.20.0.3   172.20.0.2   TELNET     69 Telnet Data ...
  180 67.586952   172.20.0.2   172.20.0.3   TELNET     69 Telnet Data ...
  181 67.586991   172.20.0.3   172.20.0.2   TELNET     86 Telnet Data ...
  183 67.626980   172.20.0.3   172.20.0.2   TELNET     80 Telnet Data ...
  185 70.672749   172.20.0.2   172.20.0.3   TELNET     72 Telnet Data ...
  186 70.673818   172.20.0.3   172.20.0.2   TELNET     73 Telnet Data ...
  188 70.676369   172.20.0.3   172.20.0.2   TELNET     76 Telnet Data ...
  190 76.397170   172.20.0.2   172.20.0.3   TELNET     81 Telnet Data ...
  191 76.397975   172.20.0.3   172.20.0.2   TELNET     68 Telnet Data ...
  193 79.254271   172.20.0.3   172.20.0.2   TELNET     68 Telnet Data ...
  195 79.254473   172.20.0.3   172.20.0.2   TELNET     83 Telnet Data ...

▼ Frame 179: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
    Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 15, 2017 17:08:36.152908000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1505495316.152908000 seconds
    [Time delta from previous captured frame: 0.000480000 seconds]
    [Time delta from previous displayed frame: 0.000480000 seconds]
    [Time since reference or first frame: 67.586912000 seconds]
    Frame Number: 179
    Frame Length: 69 bytes (552 bits)
    Capture Length: 69 bytes (552 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:telnet]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
▼ Ethernet II, Src: 02:42:ac:14:00:03 (02:42:ac:14:00:03), Dst: 02:42:ac:14:00:02 (02:42:ac:14:00:02)
  ▶ Destination: 02:42:ac:14:00:02 (02:42:ac:14:00:02)
  ▶ Source: 02:42:ac:14:00:03 (02:42:ac:14:00:03)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 172.20.0.3, Dst: 172.20.0.2

0000  02 42 ac 14 00 02 02 42  ac 14 00 03 08 00 45 10   .B.....B ......E.
0010  00 37 de 61 40 00 40 06  04 22 ac 14 00 03 ac 14   .7.a@.@. .".....
0020  00 02 00 17 8a d8 22 e7  a1 38 39 65 48 aa 80 18   ......". .89eH...
0030  00 e3 58 57 00 00 01 01  08 0a 04 15 7f 5b 04 15   ..XW.... .....[..
```

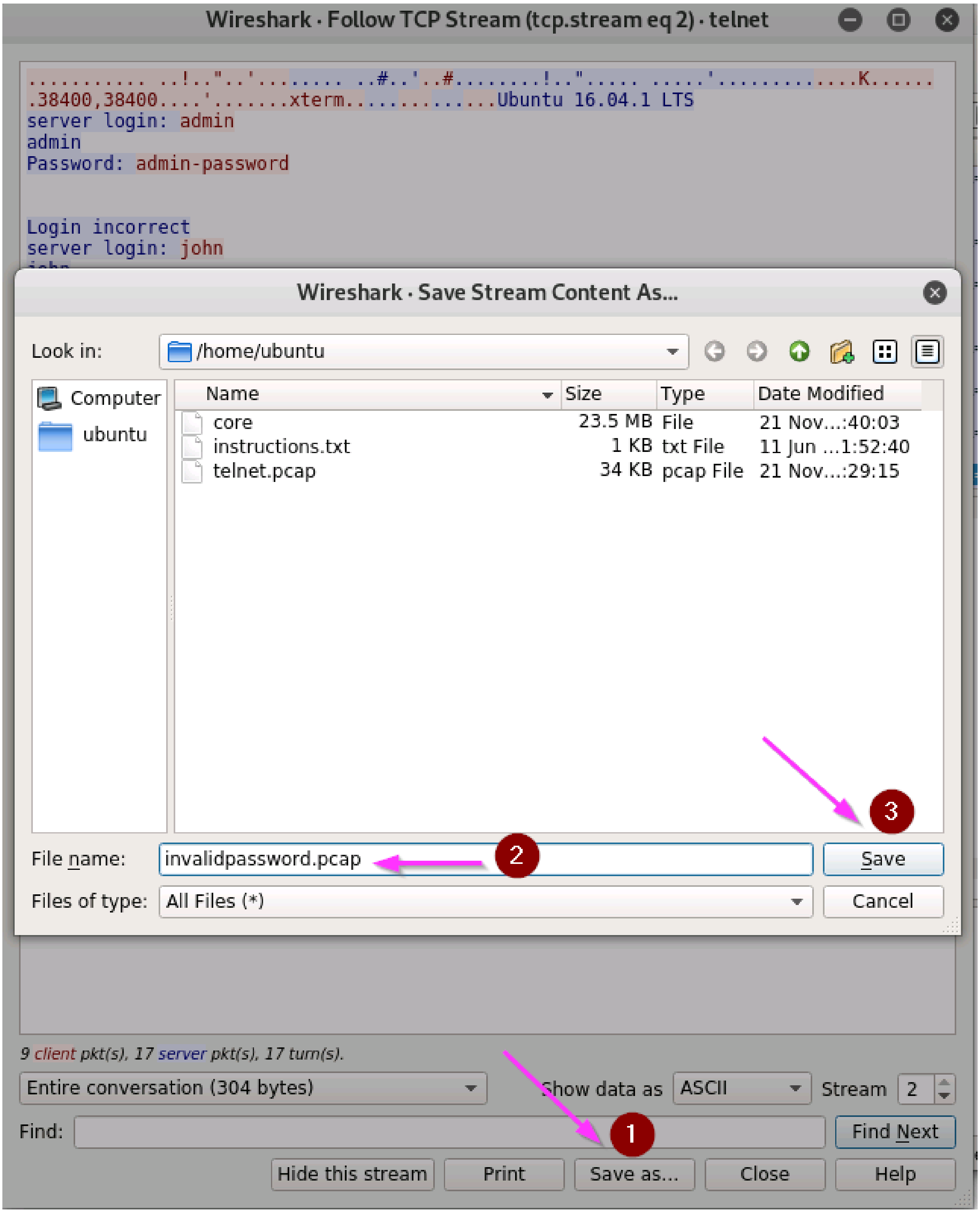


```
▼ Frame 179: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
    Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 15, 2017 17:08:36.152908000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1505495316.152908000 seconds
    [Time delta from previous captured frame: 0.000480000 seconds]
    [Time delta from previous displayed frame: 0.000480000 seconds]
    [Time since reference or first frame: 67.586912000 seconds]
    Frame Number: 179
    Frame Length: 69 bytes (552 bits)
    Capture Length: 69 bytes (552 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:telnet]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
▼ Ethernet II, Src: 02:42:ac:14:00:03 (02:42:ac:14:00:03), Dst: 02:42:ac:14:00:02 (02:42:ac:14:00:02)
  ▶ Destination: 02:42:ac:14:00:02 (02:42:ac:14:00:02)
  ▶ Source: 02:42:ac:14:00:03 (02:42:ac:14:00:03)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 172.20.0.3, Dst: 172.20.0.2

0000  02 42 ac 14 00 02 02 42  ac 14 00 03 08 00 45 10   .B.....B ......E.
0010  00 37 de 61 40 00 40 06  04 22 ac 14 00 03 ac 14   .7.a@.@. .".....
0020  00 02 00 17 8a d8 22 e7  a1 38 39 65 48 aa 80 18   ......". .89eH...
0030  00 e3 58 57 00 00 01 01  08 0a 04 15 7f 5b 04 15   ..XW.... .....[..
0040  7f 5a ff fb 01                                     .Z...
```



```
........... ..!..".."...... ..#..'..#........!.."..... .....'.............K...... .38400,38400....'.......xterm..............Ubuntu 16.04.1 LTS
server login: admin
admin
Password: admin-password


Login incorrect
server login: john
john
Password: john-password


Login incorrect
server login: 
```

Save the specified packet/frame as 'invalidpassword.pcap'.



Wireshark · Follow TCP Stream (tcp.stream eq 2) · telnet

```
........... ..!..."..'.........  ..#..'..#........!.."..... .....'.............K......
.38400,38400....'.......xterm..............Ubuntu 16.04.1 LTS
server login: admin
admin
Password: admin-password


Login incorrect
server login: john
```

Wireshark · Save Stream Content As...

Look in: /home/ubuntu

Name	Size	Type	Date Modified
core	23.5 MB	File	21 Nov...:40:03
instructions.txt	1 KB	txt File	11 Jun ...1:52:40
telnet.pcap	34 KB	pcap File	21 Nov...:29:15

File name: invalidpassword.pcap

Files of type: All Files (*)

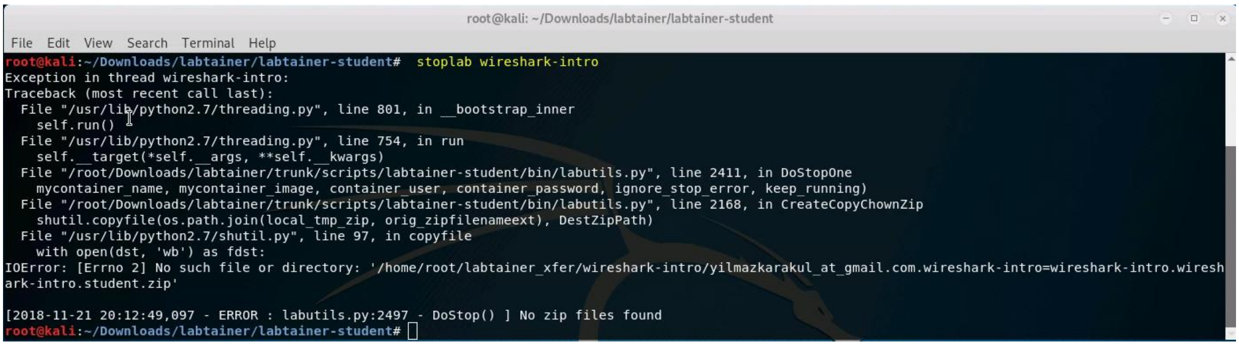
9 client pkt(s), 17 server pkt(s), 17 turn(s).

Entire conversation (304 bytes) | Show data as ASCII | Stream 2

4. Stop the Labtainer

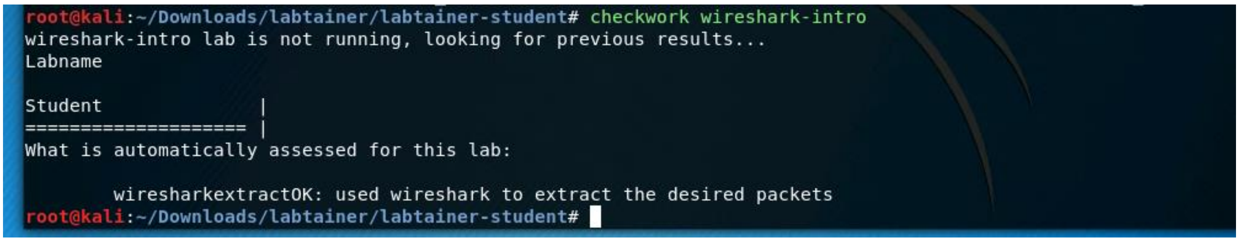
When the lab is completed, or you'd like to stop working for a while, run

```
stoplab wireshark-intro
```



root@kali: ~/Downloads/labtainer/labtainer-student
File Edit View Search Terminal Help

```
root@kali:~/Downloads/labtainer/labtainer-student#  stoplab wireshark-intro
Exception in thread wireshark-intro:
Traceback (most recent call last):
  File "/usr/lib/python2.7/threading.py", line 801, in __bootstrap_inner
    self.run()
  File "/usr/lib/python2.7/threading.py", line 754, in run
    self.__target(*self.__args, **self.__kwargs)
  File "/root/Downloads/labtainer/trunk/scripts/labtainer-student/bin/labutils.py", line 2411, in DoStopOne
    mycontainer_name, mycontainer_image, container_user, container_password, ignore_stop_error, keep_running)
  File "/root/Downloads/labtainer/trunk/scripts/labtainer-student/bin/labutils.py", line 2168, in CreateCopyChownZip
    shutil.copyfile(os.path.join(local_tmp_zip, orig_zipfilenameext), DestZipPath)
  File "/usr/lib/python2.7/shutil.py", line 97, in copyfile
    with open(dst, 'wb') as fdst:
IOError: [Errno 2] No such file or directory: '/home/root/labtainer_xfer/wireshark-intro/yilmazkarakul_at_gmail.com.wireshark-intro=wireshark-intro.wiresh
ark-intro.student.zip'

[2018-11-21 20:12:49,097 - ERROR : labutils.py:2497 - DoStop() ] No zip files found
root@kali:~/Downloads/labtainer/labtainer-student# 
```



```
root@kali:~/Downloads/labtainer/labtainer-student# checkwork wireshark-intro
wireshark-intro lab is not running, looking for previous results...
Labname

Student              |
==================== |
What is automatically assessed for this lab:

        wiresharkextractOK: used wireshark to extract the desired packets
root@kali:~/Downloads/labtainer/labtainer-student# 
```

from the host Labtainer working directory. You can always restart the Labtainer to continue your work. When the Labtainer is stopped, a zip file is created and copied to a location displayed by the stoplab command. When the lab is completed, send that zip file to the instructor.