Design of Secure Computer Systems

Lab 04

Wireshark & Pcapanlysis

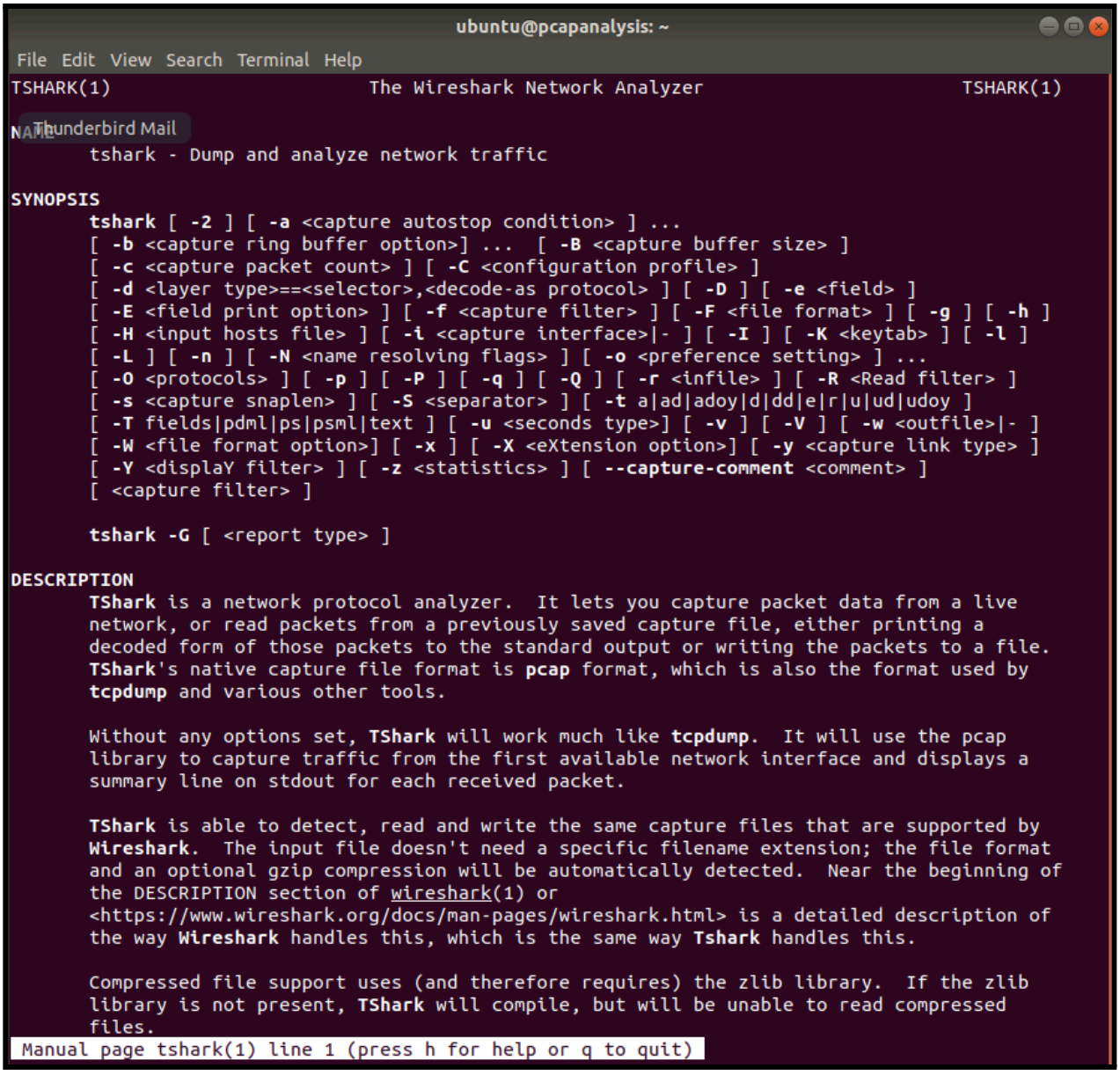
These LABS will demonstrate on capturing packet and analysis of captured packet to retrieve information.

Name: Rakshita Mathur

Pcapanalysis

1. Running tshark to perform PCAP Analysis

In the process of exploring tshark, to see the various options available for tshark, we used the command: **man tshark** as it will show the complete manual for tshark.



Tshark command to display specific fields like number time frame data etc command used: **tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap**

```
ubuntu@pcapanalysis:~$ tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap
1       Sep 15, 2017 16:50:54.565296000 UTC
2       Sep 15, 2017 16:50:55.565131000 UTC
3       Sep 15, 2017 16:50:55.565151000 UTC
4       Sep 15, 2017 16:50:55.581034000 UTC
5       Sep 15, 2017 16:50:55.581061000 UTC
6       Sep 15, 2017 16:50:56.565410000 UTC
7       Sep 15, 2017 16:50:56.565430000 UTC
8       Sep 15, 2017 16:50:57.565300000 UTC
9       Sep 15, 2017 16:50:57.565321000 UTC
10      Sep 15, 2017 16:50:58.565874000 UTC
11      Sep 15, 2017 16:50:58.565902000 UTC
12      Sep 15, 2017 16:50:59.565221000 UTC
13      Sep 15, 2017 16:50:59.565251000 UTC
14      Sep 15, 2017 16:51:06.857851000 UTC
15      Sep 15, 2017 16:51:06.857912000 UTC
16      Sep 15, 2017 16:51:06.857946000 UTC
17      Sep 15, 2017 16:51:06.861076000 UTC
18      Sep 15, 2017 16:51:06.861092000 UTC
19      Sep 15, 2017 16:51:06.922766000 UTC
20      Sep 15, 2017 16:51:06.922833000 UTC
21      Sep 15, 2017 16:51:06.930978000 UTC
22      Sep 15, 2017 16:51:06.930985000 UTC
23      Sep 15, 2017 16:51:06.936254000 UTC
24      Sep 15, 2017 16:51:06.940813000 UTC
25      Sep 15, 2017 16:51:06.950229000 UTC
26      Sep 15, 2017 16:51:06.955763000 UTC
27      Sep 15, 2017 16:51:06.993028000 UTC
28      Sep 15, 2017 16:51:06.993070000 UTC
29      Sep 15, 2017 16:51:06.993077000 UTC
30      Sep 15, 2017 16:51:06.993186000 UTC
31      Sep 15, 2017 16:51:06.993269000 UTC
32      Sep 15, 2017 16:51:06.994865000 UTC
33      Sep 15, 2017 16:51:07.033196000 UTC
34      Sep 15, 2017 16:51:09.627868000 UTC
35      Sep 15, 2017 16:51:09.657967000 UTC
36      Sep 15, 2017 16:51:09.658079000 UTC
37      Sep 15, 2017 16:51:09.658175000 UTC
38      Sep 15, 2017 16:51:09.701038000 UTC
39      Sep 15, 2017 16:51:09.776377000 UTC
40      Sep 15, 2017 16:51:09.813495000 UTC
41      Sep 15, 2017 16:51:09.813518000 UTC
42      Sep 15, 2017 16:51:09.813545000 UTC
```

```
43      Sep 15, 2017 16:51:09.813681000 UTC
44      Sep 15, 2017 16:51:09.813686000 UTC
45      Sep 15, 2017 16:51:09.818573000 UTC
46      Sep 15, 2017 16:51:09.819664000 UTC
47      Sep 15, 2017 16:51:09.819704000 UTC
48      Sep 15, 2017 16:51:09.962228000 UTC
49      Sep 15, 2017 16:51:10.000904000 UTC
50      Sep 15, 2017 16:51:16.016735000 UTC
51      Sep 15, 2017 16:51:16.052892000 UTC
52      Sep 15, 2017 16:51:18.946769000 UTC
53      Sep 15, 2017 16:51:18.946783000 UTC
54      Sep 15, 2017 16:51:18.946971000 UTC
55      Sep 15, 2017 16:51:18.946995000 UTC
56      Sep 15, 2017 16:51:18.947165000 UTC
57      Sep 15, 2017 16:51:18.947185000 UTC
58      Sep 15, 2017 16:51:20.959876000 UTC
59      Sep 15, 2017 16:51:20.969350000 UTC
60      Sep 15, 2017 16:51:20.974592000 UTC
61      Sep 15, 2017 16:51:20.974607000 UTC
62      Sep 15, 2017 16:51:23.512697000 UTC
63      Sep 15, 2017 16:51:23.512774000 UTC
64      Sep 15, 2017 16:51:23.512817000 UTC
65      Sep 15, 2017 16:51:23.515574000 UTC
66      Sep 15, 2017 16:51:23.515582000 UTC
67      Sep 15, 2017 16:51:23.538873000 UTC
68      Sep 15, 2017 16:51:23.538990000 UTC
69      Sep 15, 2017 16:51:23.539635000 UTC
70      Sep 15, 2017 16:51:23.544517000 UTC
71      Sep 15, 2017 16:51:23.549115000 UTC
72      Sep 15, 2017 16:51:23.558409000 UTC
73      Sep 15, 2017 16:51:23.564036000 UTC
74      Sep 15, 2017 16:51:23.601214000 UTC
75      Sep 15, 2017 16:51:23.601262000 UTC
76      Sep 15, 2017 16:51:23.601268000 UTC
77      Sep 15, 2017 16:51:23.601397000 UTC
78      Sep 15, 2017 16:51:23.601469000 UTC
79      Sep 15, 2017 16:51:23.602942000 UTC
80      Sep 15, 2017 16:51:23.640945000 UTC
81      Sep 15, 2017 16:51:26.071615000 UTC
82      Sep 15, 2017 16:51:26.082132000 UTC
83      Sep 15, 2017 16:51:26.082208000 UTC
84      Sep 15, 2017 16:51:26.082303000 UTC
85      Sep 15, 2017 16:51:26.121338000 UTC
86      Sep 15, 2017 16:51:26.172264000 UTC
87      Sep 15, 2017 16:51:26.208903000 UTC
```

```
88      Sep 15, 2017 16:51:26.208930000 UTC
89      Sep 15, 2017 16:51:26.208952000 UTC
90      Sep 15, 2017 16:51:26.209117000 UTC
91      Sep 15, 2017 16:51:26.209124000 UTC
92      Sep 15, 2017 16:51:26.215627000 UTC
93      Sep 15, 2017 16:51:26.216766000 UTC
94      Sep 15, 2017 16:51:26.216817000 UTC
95      Sep 15, 2017 16:51:26.216872000 UTC
96      Sep 15, 2017 16:51:26.257003000 UTC
97      Sep 15, 2017 16:51:26.343473000 UTC
98      Sep 15, 2017 16:51:26.343524000 UTC
99      Sep 15, 2017 16:51:28.151857000 UTC
100     Sep 15, 2017 16:51:28.188895000 UTC
101     Sep 15, 2017 16:51:28.263475000 UTC
102     Sep 15, 2017 16:51:28.263755000 UTC
103     Sep 15, 2017 16:51:28.269427000 UTC
104     Sep 15, 2017 16:51:28.269468000 UTC
105     Sep 15, 2017 16:51:30.109137000 UTC
106     Sep 15, 2017 16:51:30.109175000 UTC
107     Sep 15, 2017 16:51:30.250426000 UTC
108     Sep 15, 2017 16:51:30.250474000 UTC
109     Sep 15, 2017 16:51:30.253915000 UTC
110     Sep 15, 2017 16:51:30.253945000 UTC
111     Sep 15, 2017 16:51:33.173962000 UTC
112     Sep 15, 2017 16:51:33.174013000 UTC
113     Sep 15, 2017 16:51:33.293601000 UTC
114     Sep 15, 2017 16:51:33.293682000 UTC
115     Sep 15, 2017 16:51:33.293775000 UTC
116     Sep 15, 2017 16:51:33.293788000 UTC
117     Sep 15, 2017 16:51:33.293861000 UTC
118     Sep 15, 2017 16:51:33.293882000 UTC
119     Sep 15, 2017 16:51:33.293924000 UTC
120     Sep 15, 2017 16:51:33.293960000 UTC
121     Sep 15, 2017 16:51:33.295297000 UTC
122     Sep 15, 2017 16:51:33.295321000 UTC
123     Sep 15, 2017 16:51:33.295418000 UTC
124     Sep 15, 2017 16:51:33.295432000 UTC
125     Sep 15, 2017 16:51:33.295610000 UTC
126     Sep 15, 2017 16:51:33.295756000 UTC
127     Sep 15, 2017 16:51:33.295861000 UTC
128     Sep 15, 2017 16:51:33.295910000 UTC
129     Sep 15, 2017 16:51:33.296499000 UTC
130     Sep 15, 2017 16:51:33.296513000 UTC
131     Sep 15, 2017 16:51:33.300439000 UTC
132     Sep 15, 2017 16:51:33.300480000 UTC
```

```
135     Sep 15, 2017 16:51:33.300609000 UTC
136     Sep 15, 2017 16:51:33.300646000 UTC
137     Sep 15, 2017 16:51:33.300901000 UTC
138     Sep 15, 2017 16:51:33.300922000 UTC
139     Sep 15, 2017 16:51:33.305056000 UTC
140     Sep 15, 2017 16:51:33.305108000 UTC
141     Sep 15, 2017 16:51:36.114142000 UTC
142     Sep 15, 2017 16:51:36.114175000 UTC
143     Sep 15, 2017 16:51:36.185499000 UTC
144     Sep 15, 2017 16:51:36.185576000 UTC
145     Sep 15, 2017 16:51:36.185631000 UTC
146     Sep 15, 2017 16:51:36.185644000 UTC
147     Sep 15, 2017 16:51:36.188592000 UTC
148     Sep 15, 2017 16:51:36.188624000 UTC
149     Sep 15, 2017 16:51:36.189071000 UTC
150     Sep 15, 2017 16:51:36.189088000 UTC
151     Sep 15, 2017 16:51:36.190444000 UTC
152     Sep 15, 2017 16:51:36.190453000 UTC
153     Sep 15, 2017 16:51:36.190677000 UTC
154     Sep 15, 2017 16:51:36.190684000 UTC
155     Sep 15, 2017 16:51:36.190833000 UTC
156     Sep 15, 2017 16:51:36.213594000 UTC
157     Sep 15, 2017 16:51:36.213669000 UTC
158     Sep 15, 2017 16:51:58.131149000 UTC
159     Sep 15, 2017 16:51:58.131199000 UTC
160     Sep 15, 2017 16:51:58.131256000 UTC
161     Sep 15, 2017 16:51:58.131787000 UTC
162     Sep 15, 2017 16:51:58.131833000 UTC
163     Sep 15, 2017 16:51:58.149802000 UTC
164     Sep 15, 2017 16:51:58.149839000 UTC
165     Sep 15, 2017 16:51:58.149890000 UTC
166     Sep 15, 2017 16:51:58.149921000 UTC
167     Sep 15, 2017 16:51:58.149978000 UTC
168     Sep 15, 2017 16:51:58.152096000 UTC
169     Sep 15, 2017 16:51:58.152428000 UTC
170     Sep 15, 2017 16:51:58.152908000 UTC
171     Sep 15, 2017 16:51:58.152948000 UTC
172     Sep 15, 2017 16:51:58.152987000 UTC     Ubuntu 16.04.1 LTS

173     Sep 15, 2017 16:51:58.192950000 UTC
174     Sep 15, 2017 16:51:58.192976000 UTC     server login:
175     Sep 15, 2017 16:51:58.192995000 UTC
176     Sep 15, 2017 16:52:01.238745000 UTC     admin

177     Sep 15, 2017 16:52:01.239814000 UTC     admin
```

```
178     Sep 15, 2017 16:52:01.239861000 UTC
179     Sep 15, 2017 16:52:01.242365000 UTC     Password:
180     Sep 15, 2017 16:52:01.242401000 UTC
181     Sep 15, 2017 16:52:06.963166000 UTC     admin-password

182     Sep 15, 2017 16:52:06.963971000 UTC

183     Sep 15, 2017 16:52:06.963993000 UTC
184     Sep 15, 2017 16:52:09.820267000 UTC

185     Sep 15, 2017 16:52:09.820306000 UTC
186     Sep 15, 2017 16:52:09.820469000 UTC     Login incorrect

187     Sep 15, 2017 16:52:09.820484000 UTC
188     Sep 15, 2017 16:52:09.821778000 UTC     server login:
189     Sep 15, 2017 16:52:09.821797000 UTC
190     Sep 15, 2017 16:52:11.907777000 UTC     john

191     Sep 15, 2017 16:52:11.908174000 UTC     john

192     Sep 15, 2017 16:52:11.908196000 UTC
193     Sep 15, 2017 16:52:11.909525000 UTC     Password:
194     Sep 15, 2017 16:52:11.909542000 UTC
195     Sep 15, 2017 16:52:19.756176000 UTC     john-password

196     Sep 15, 2017 16:52:19.757236000 UTC

197     Sep 15, 2017 16:52:19.757286000 UTC
198     Sep 15, 2017 16:52:22.378455000 UTC
,Login incorrect

199     Sep 15, 2017 16:52:22.378503000 UTC
200     Sep 15, 2017 16:52:22.379319000 UTC     server login:
201     Sep 15, 2017 16:52:22.379359000 UTC
202     Sep 15, 2017 16:52:27.510911000 UTC
203     Sep 15, 2017 16:52:27.511804000 UTC
204     Sep 15, 2017 16:52:27.511923000 UTC
205     Sep 15, 2017 16:52:32.377326000 UTC
206     Sep 15, 2017 16:52:32.377401000 UTC
207     Sep 15, 2017 16:52:33.378691000 UTC
208     Sep 15, 2017 16:52:33.378732000 UTC
```

```
209     Sep 15, 2017 16:52:34.377664000 UTC
210     Sep 15, 2017 16:52:34.377685000 UTC
211     Sep 15, 2017 16:52:35.377160000 UTC
212     Sep 15, 2017 16:52:35.377217000 UTC
ubuntu@pcapanalysis:~$
```

2. Displaying the single packet containing invalid “admin” password

Used command: **tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap -Y frame.number==181**

```
ubuntu@pcapanalysis:~$ tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap -Y frame.number==181
181     Sep 15, 2017 16:52:06.963166000 UTC     admin-password

ubuntu@pcapanalysis:~$
```

Using Checkwork command and stoplab command to stop the lan and end it.

```
student@LabtainersVM:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/pcapanalysis
Labname pcapanalysis

Student              |      view_frame | view_telnet_dat |
==================== | =============== | =============== |
rmath049_at_uottawa. |               Y |               Y |
What is automatically assessed for this lab:
        view_telnet_data: did the student look at telnet data?
        view_frame: Viewed the intended frame
```

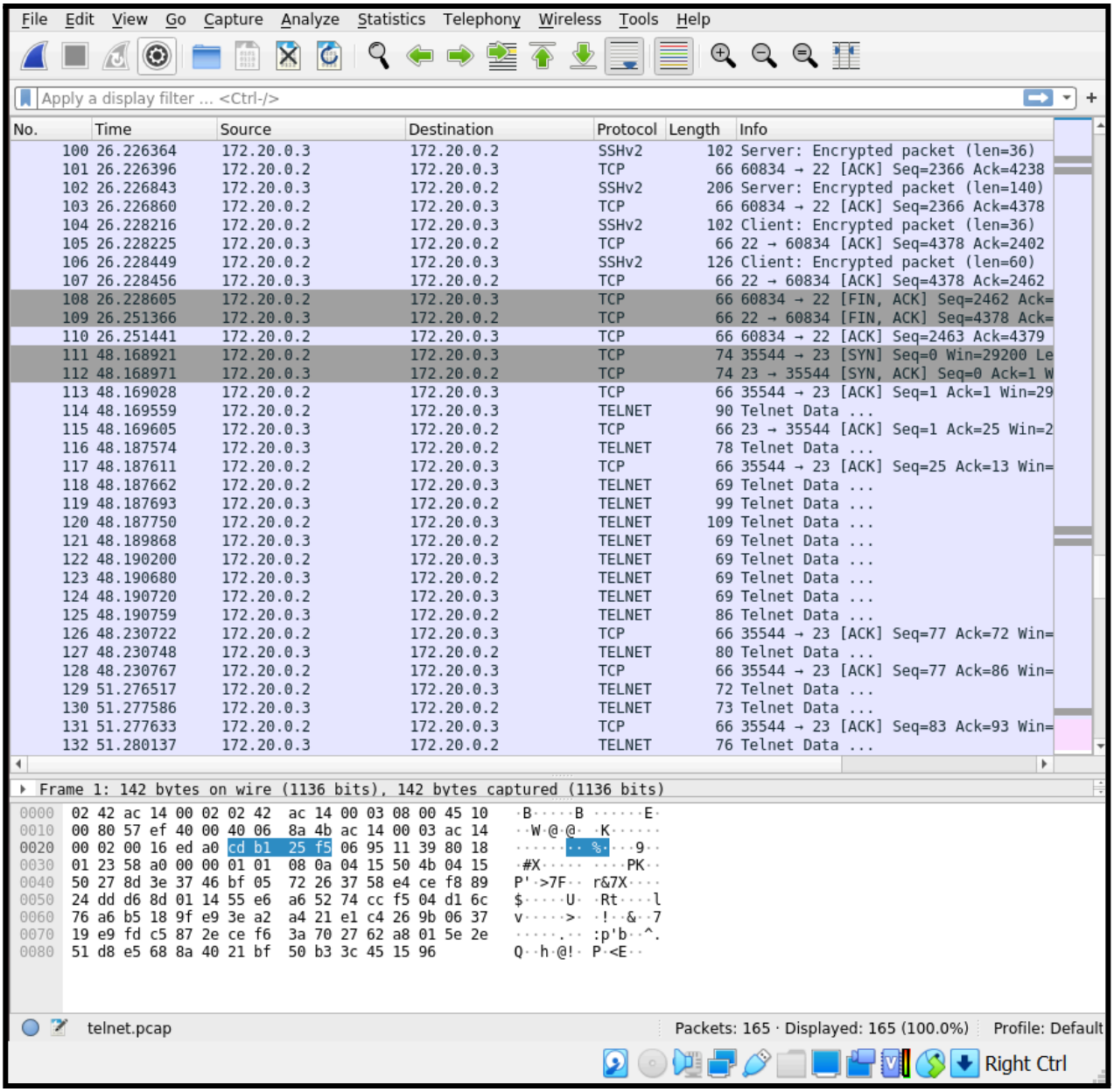
2. Wireshark Introduction

1. Explore

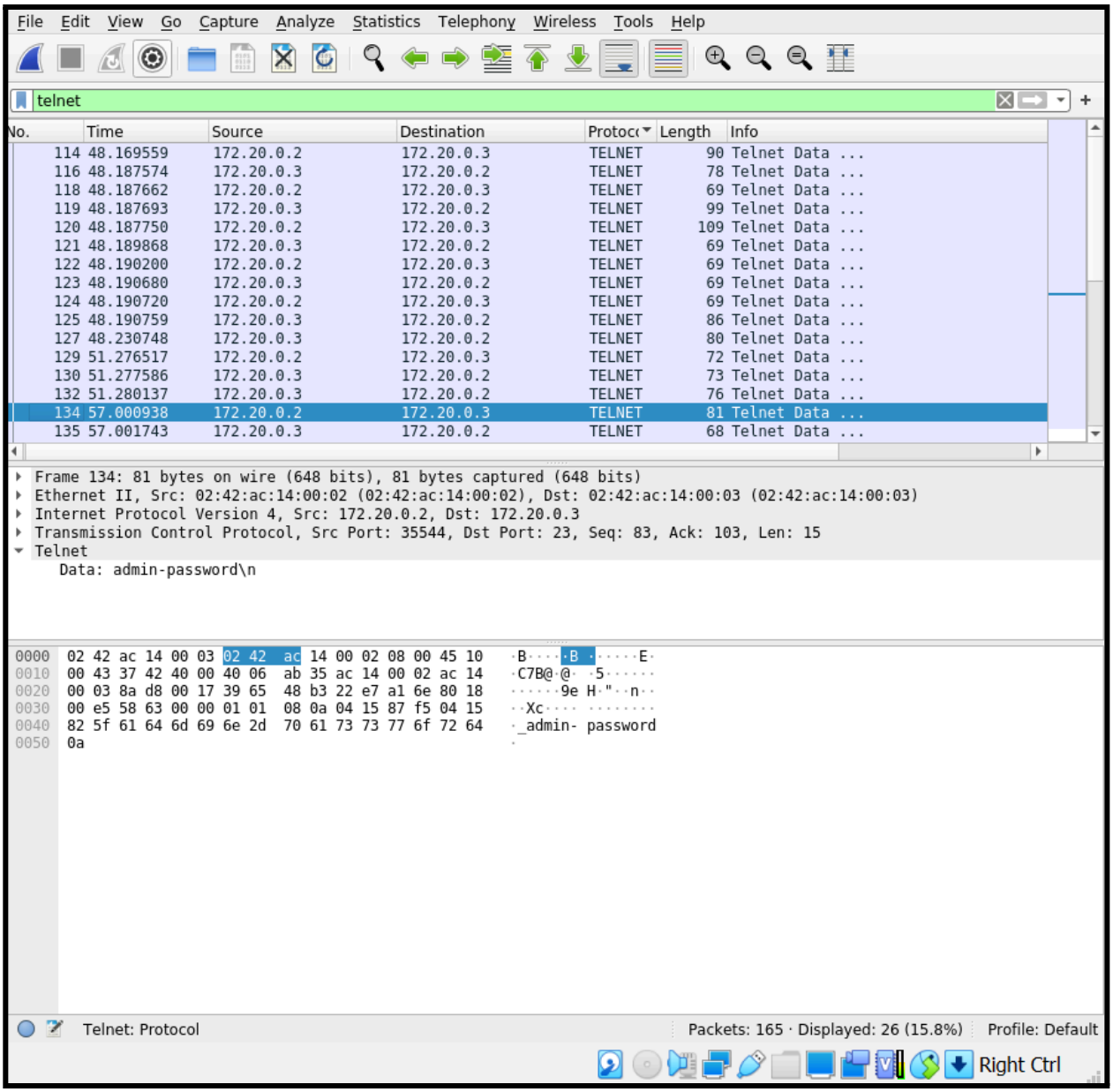
   Use the ls command to view the content of the directory in the terminal that opened when you started the lab. That telnet.pcap file contains the network traffic you will analyze. Use file **telnet.pcap**

```
                                                ubuntu@wireshark-intro: ~
File  Edit  View  Search  Terminal  Help
ubuntu@wireshark-intro:~$ ls
telnet.pcap
ubuntu@wireshark-intro:~$
```

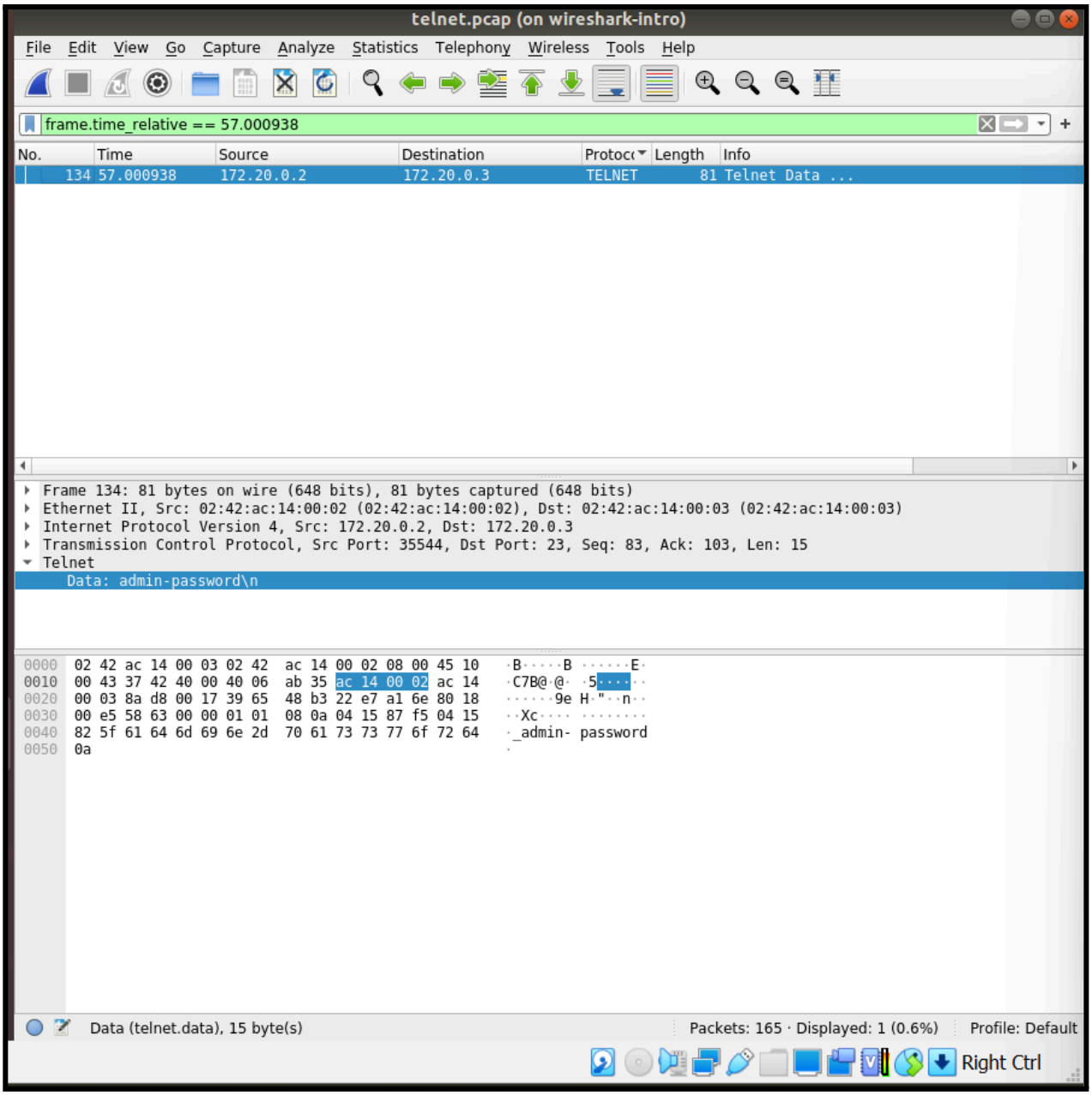
2. Running Wireshark to perform PCAP analysis



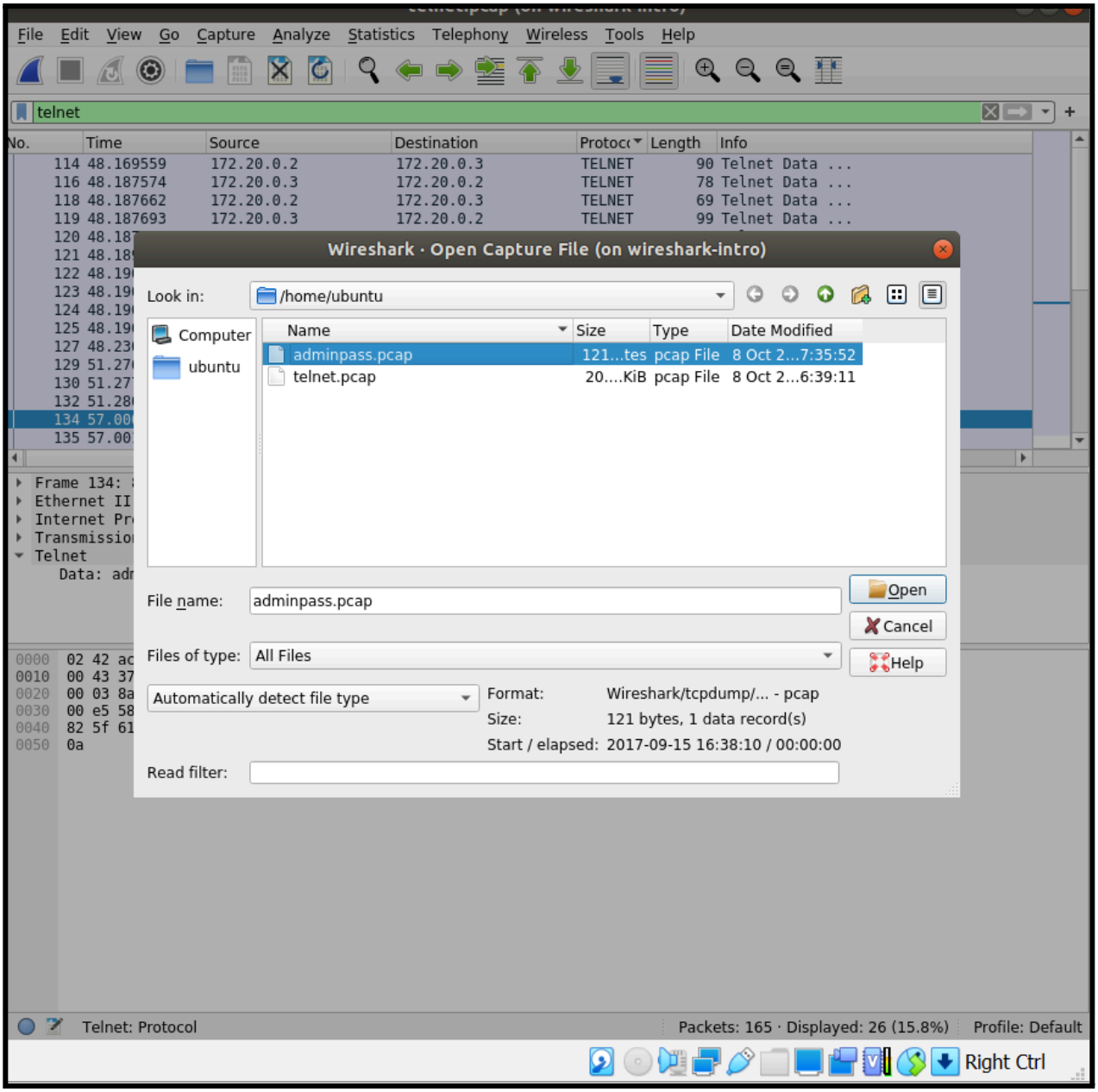
3. Finding a specific packet



Finding the right packet by looking at the telnet data.



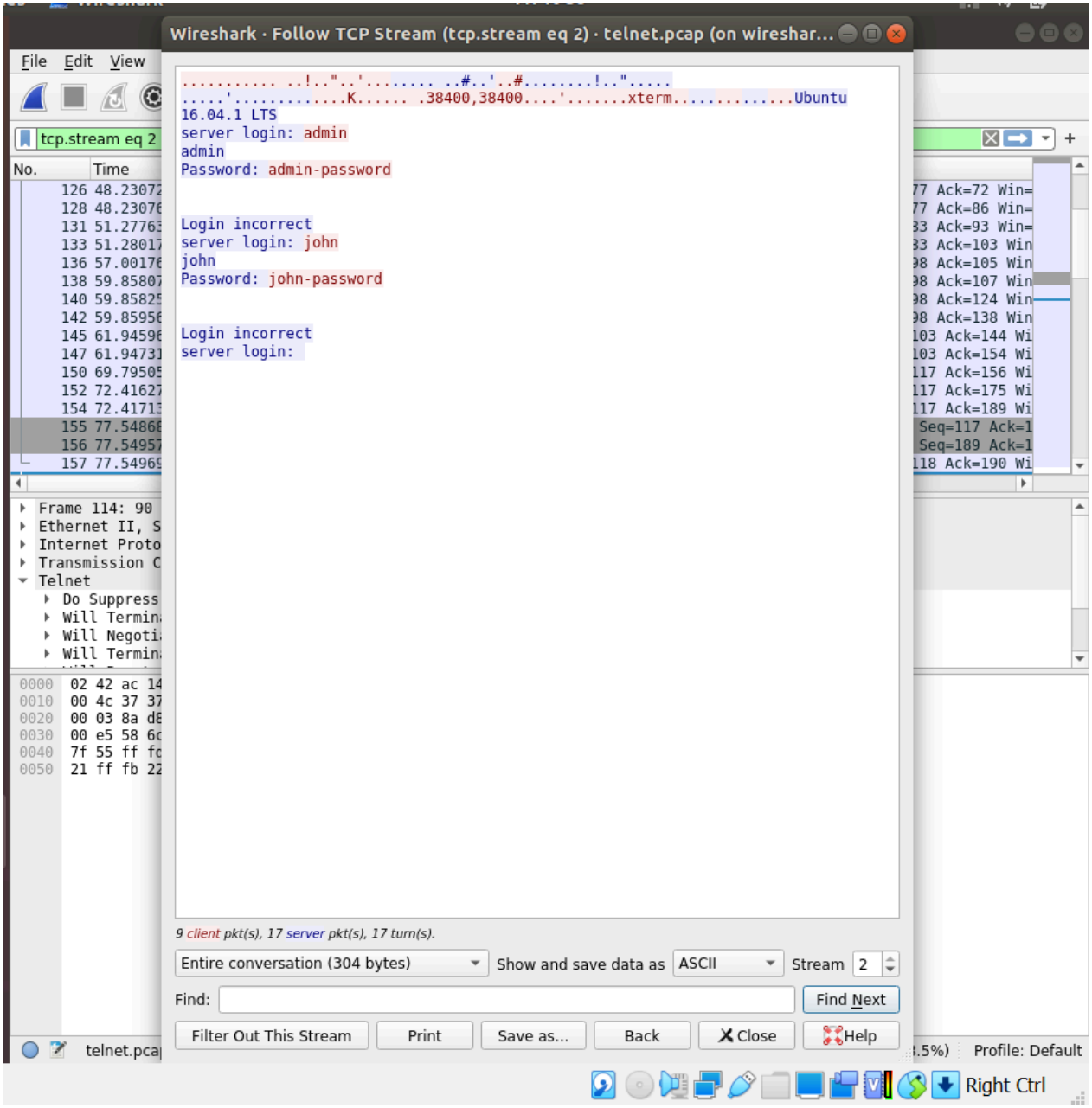
Selecting the packet and exporting it.



Saving the packet.

4. Explore some more

Using the follow command to see all the telnet data once.


Wireshark · Follow TCP Stream (tcp.stream eq 2) · telnet.pcap (on wireshar...
File Edit View
tcp.stream eq 2
No. Time
Frame 114: 90
Ethernet II, S
Internet Proto
Transmission C
Telnet
Do Suppress
Will Termin
Will Negoti
Will Termin
0000 02 42 ac 14
0010 00 4c 37 37
0020 00 03 8a d8
0030 00 e5 58 6c
0040 7f 55 ff fc
0050 21 ff fb 22
....!.."..'........ ..#..'..#........!.."..... .....'.............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:
9 client pkt(s), 17 server pkt(s), 17 turn(s).
Entire conversation (304 bytes)
Show and save data as ASCII
Stream 2
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
telnet.pcap
Profile: Default
Right Ctrl