

Design of Secure Computer Systems

Lab 04

Wireshark & Pcapanalysis

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.

```

ubuntu@pcapanalysis: ~
File Edit View Search Terminal Help
TSHARK(1)                                The Wireshark Network Analyzer                                TSHARK(1)
tshark - Dump and analyze network traffic

SYNOPSIS
tshark [ -2 ] [ -a <capture autostop condition> ] ...
[ -b <capture ring buffer option> ] ... [ -B <capture buffer size> ]
[ -c <capture packet count> ] [ -C <configuration profile> ]
[ -d <layer type>==<selector>,<decode-as protocol> ] [ -D ] [ -e <field> ]
[ -E <field print option> ] [ -f <capture filter> ] [ -F <file format> ] [ -g ] [ -h ]
[ -H <input hosts file> ] [ -i <capture interface>|- ] [ -I ] [ -K <keytab> ] [ -l ]
[ -L ] [ -n ] [ -N <name resolving flags> ] [ -o <preference setting> ] ...
[ -O <protocols> ] [ -p ] [ -P ] [ -q ] [ -Q ] [ -r <infile> ] [ -R <Read filter> ]
[ -s <capture snaplen> ] [ -S <separator> ] [ -t a|ad|adoy|d|dd|e|r|u|ud|udoy ]
[ -T fields|pdl|ps|psml|text ] [ -u <seconds type> ] [ -v ] [ -V ] [ -w <outfile>|- ]
[ -W <file format option> ] [ -x ] [ -X <extension option> ] [ -y <capture link type> ]
[ -Y <display filter> ] [ -z <statistics> ] [ --capture-comment <comment> ]
[ <capture filter> ]

tshark -G [ <report type> ]

DESCRIPTION
TShark is a network protocol analyzer. It lets you capture packet data from a live
network, or read packets from a previously saved capture file, either printing a
decoded form of those packets to the standard output or writing the packets to a file.
TShark's native capture file format is pcap format, which is also the format used by
tcpdump and various other tools.

Without any options set, TShark will work much like tcpdump. It will use the pcap
library to capture traffic from the first available network interface and displays a
summary line on stdout for each received packet.

TShark is able to detect, read and write the same capture files that are supported by
Wireshark. The input file doesn't need a specific filename extension; the file format
and an optional gzip compression will be automatically detected. Near the beginning of
the DESCRIPTION section of wireshark(1) or
<https://www.wireshark.org/docs/man-pages/wireshark.html> is a detailed description of
the way Wireshark handles this, which is the same way Tshark handles this.

Compressed file support uses (and therefore requires) the zlib library. If the zlib
library is not present, TShark will compile, but will be unable to read compressed
files.

Manual page tshark(1) line 1 (press h for help or q to quit)

```

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 lab 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

Wireshark interface showing a packet capture of a Telnet session. The packet list displays 165 packets, with the selected packet (No. 132) being a Telnet data packet. The packet details pane shows the raw data and its hexadecimal representation.

No.	Time	Source	Destination	Protocol	Length	Info
100	26.226364	172.20.0.3	172.20.0.2	SSHv2	102	Server: Encrypted packet (len=36)
101	26.226396	172.20.0.2	172.20.0.3	TCP	66	60834 → 22 [ACK] Seq=2366 Ack=4238
102	26.226843	172.20.0.3	172.20.0.2	SSHv2	206	Server: Encrypted packet (len=140)
103	26.226860	172.20.0.2	172.20.0.3	TCP	66	60834 → 22 [ACK] Seq=2366 Ack=4378
104	26.228216	172.20.0.2	172.20.0.3	SSHv2	102	Client: Encrypted packet (len=36)
105	26.228225	172.20.0.3	172.20.0.2	TCP	66	22 → 60834 [ACK] Seq=4378 Ack=2402
106	26.228449	172.20.0.2	172.20.0.3	SSHv2	126	Client: Encrypted packet (len=60)
107	26.228456	172.20.0.3	172.20.0.2	TCP	66	22 → 60834 [ACK] Seq=4378 Ack=2462
108	26.228605	172.20.0.2	172.20.0.3	TCP	66	60834 → 22 [FIN, ACK] Seq=2462 Ack=
109	26.251366	172.20.0.3	172.20.0.2	TCP	66	22 → 60834 [FIN, ACK] Seq=4378 Ack=
110	26.251441	172.20.0.2	172.20.0.3	TCP	66	60834 → 22 [ACK] Seq=2463 Ack=4379
111	48.168921	172.20.0.2	172.20.0.3	TCP	74	35544 → 23 [SYN] Seq=0 Win=29200 Le
112	48.168971	172.20.0.3	172.20.0.2	TCP	74	23 → 35544 [SYN, ACK] Seq=0 Ack=1 W
113	48.169028	172.20.0.2	172.20.0.3	TCP	66	35544 → 23 [ACK] Seq=1 Ack=1 Win=29
114	48.169559	172.20.0.2	172.20.0.3	TELNET	90	Telnet Data ...
115	48.169605	172.20.0.3	172.20.0.2	TCP	66	23 → 35544 [ACK] Seq=1 Ack=25 Win=2
116	48.187574	172.20.0.3	172.20.0.2	TELNET	78	Telnet Data ...
117	48.187611	172.20.0.2	172.20.0.3	TCP	66	35544 → 23 [ACK] Seq=25 Ack=13 Win=
118	48.187662	172.20.0.2	172.20.0.3	TELNET	69	Telnet Data ...
119	48.187693	172.20.0.3	172.20.0.2	TELNET	99	Telnet Data ...
120	48.187750	172.20.0.2	172.20.0.3	TELNET	109	Telnet Data ...
121	48.189868	172.20.0.3	172.20.0.2	TELNET	69	Telnet Data ...
122	48.190200	172.20.0.2	172.20.0.3	TELNET	69	Telnet Data ...
123	48.190680	172.20.0.3	172.20.0.2	TELNET	69	Telnet Data ...
124	48.190720	172.20.0.2	172.20.0.3	TELNET	69	Telnet Data ...
125	48.190759	172.20.0.3	172.20.0.2	TELNET	86	Telnet Data ...
126	48.230722	172.20.0.2	172.20.0.3	TCP	66	35544 → 23 [ACK] Seq=77 Ack=72 Win=
127	48.230748	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
128	48.230767	172.20.0.2	172.20.0.3	TCP	66	35544 → 23 [ACK] Seq=77 Ack=86 Win=
129	51.276517	172.20.0.2	172.20.0.3	TELNET	72	Telnet Data ...
130	51.277586	172.20.0.3	172.20.0.2	TELNET	73	Telnet Data ...
131	51.277633	172.20.0.2	172.20.0.3	TCP	66	35544 → 23 [ACK] Seq=83 Ack=93 Win=
132	51.280137	172.20.0.3	172.20.0.2	TELNET	76	Telnet Data ...

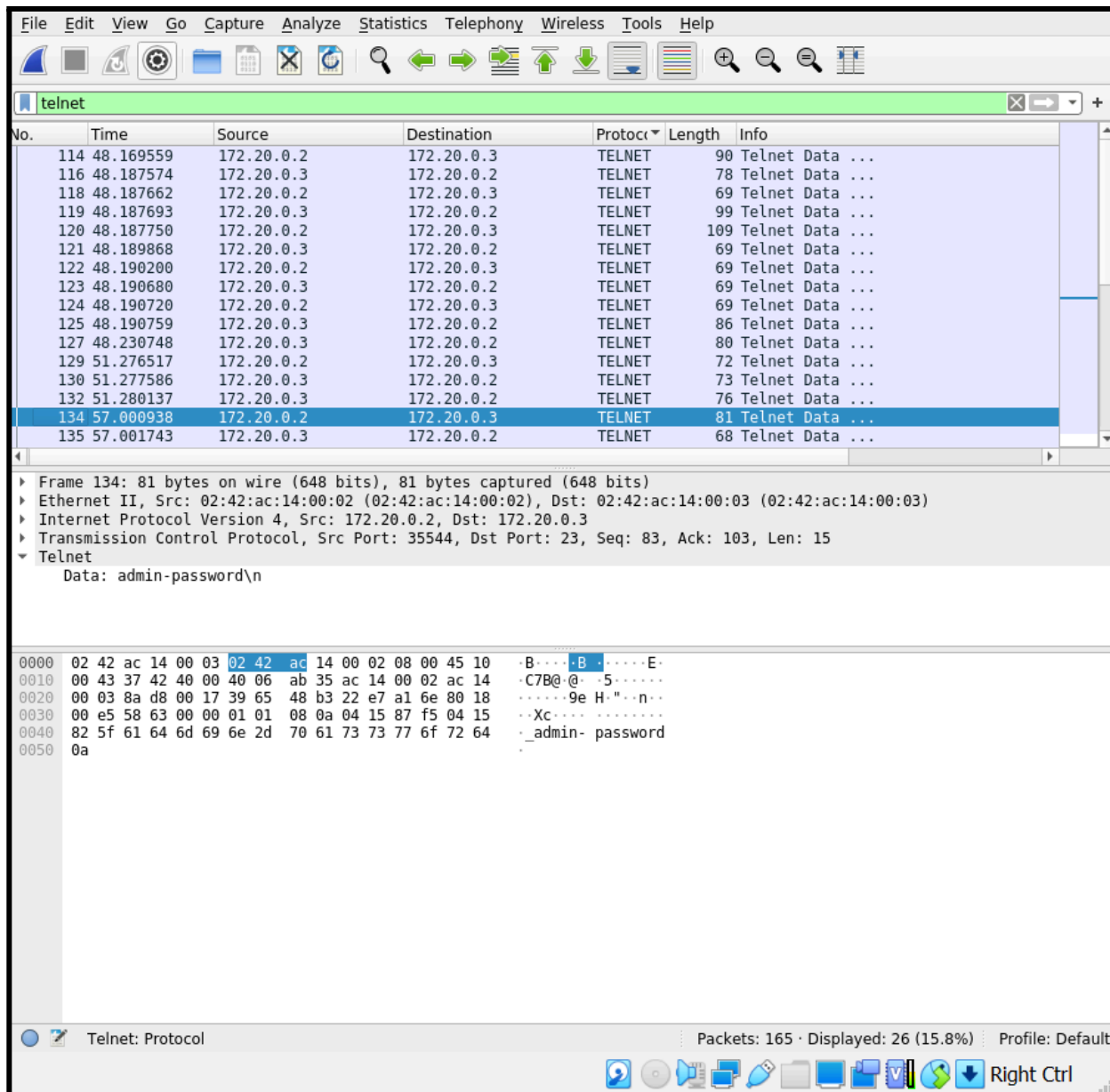
Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)

```

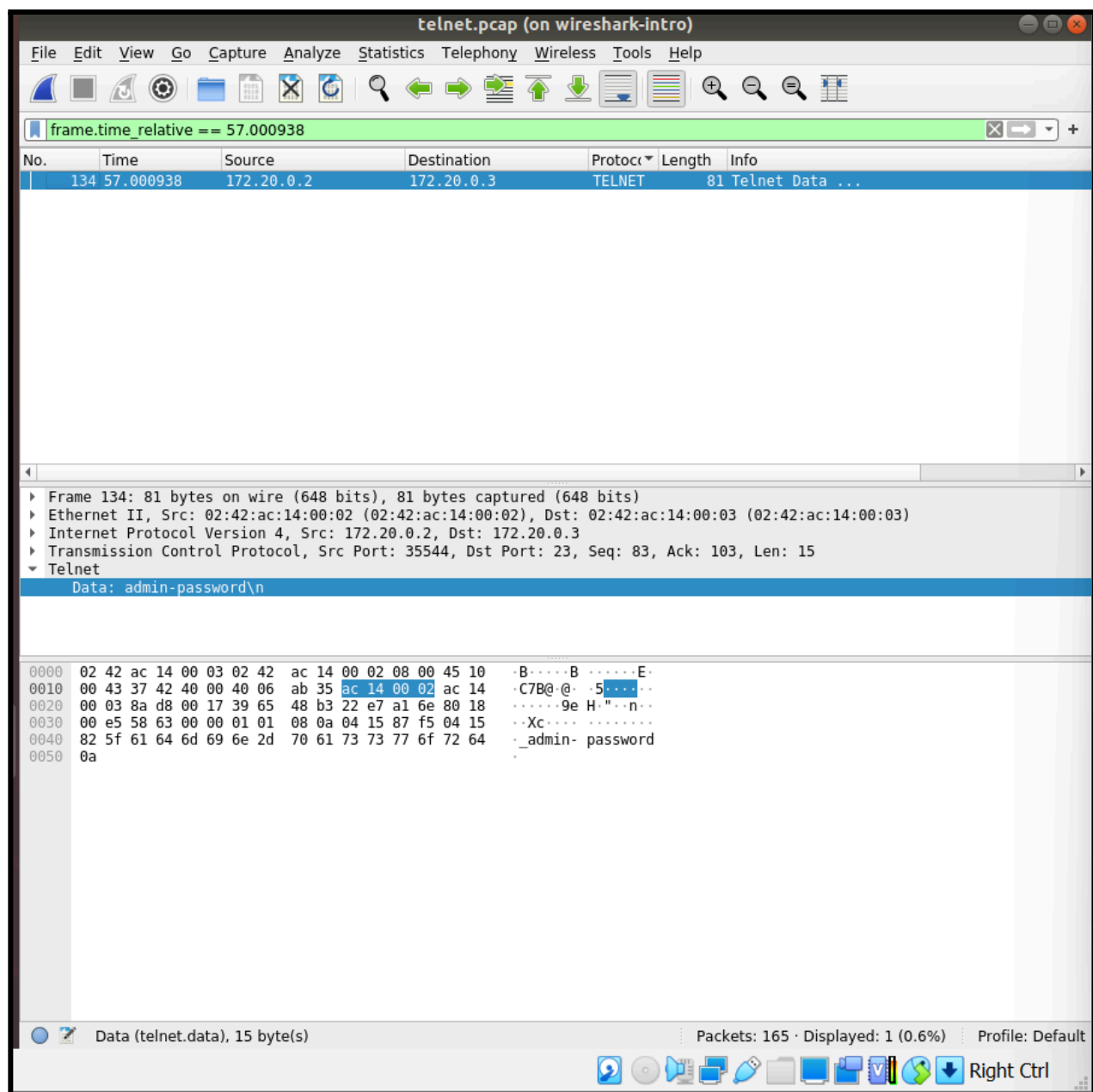
0000 02 42 ac 14 00 02 02 42 ac 14 00 03 08 00 45 10  .B.....B.....E
0010 00 80 57 ef 40 00 40 06 8a 4b ac 14 00 03 ac 14  ..W.@.@..K.....
0020 00 02 00 16 ed a0 cd b1 25 f5 06 95 11 39 80 18  .....%...9...
0030 01 23 58 a0 00 00 01 01 08 0a 04 15 50 4b 04 15  #X.....PK...
0040 50 27 8d 3e 37 46 bf 05 72 26 37 58 e4 ce f8 89  P'..>7F..r&7X...
0050 24 dd d6 8d 01 14 55 e6 a6 52 74 cc f5 04 d1 6c  $.....U..Rt....l
0060 76 a6 b5 18 9f e9 3e a2 a4 21 e1 c4 26 9b 06 37  v.....>..!..&..7
0070 19 e9 fd c5 87 2e ce f6 3a 70 27 62 a8 01 5e 2e  .....:p'b..^..
0080 51 d8 e5 68 8a 40 21 bf 50 b3 3c 45 15 96  Q..h.@!..P<E...
  
```

telnet.pcap Packets: 165 · Displayed: 165 (100.0%) Profile: Default

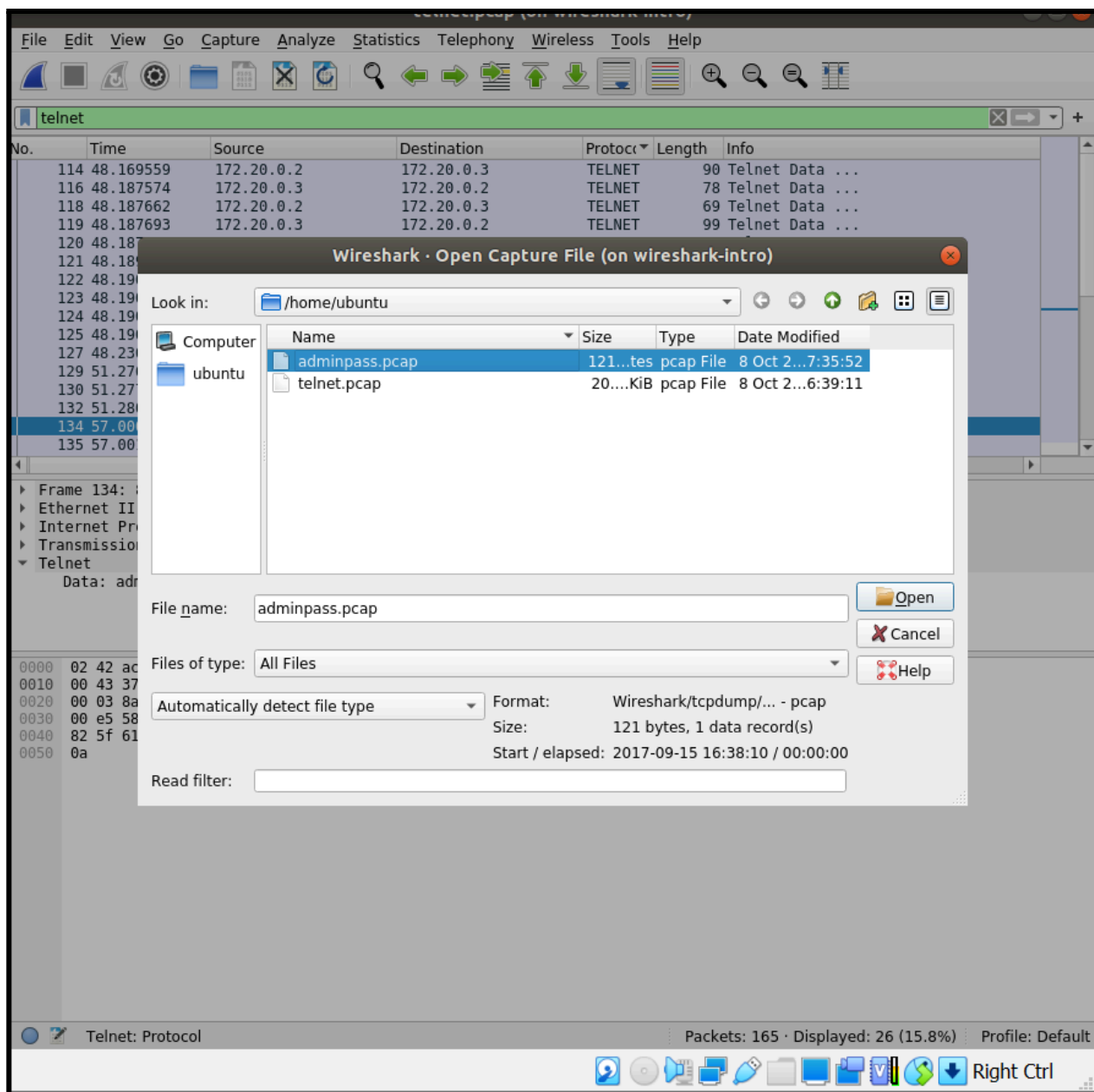
3. Finding a specific packet



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.

