

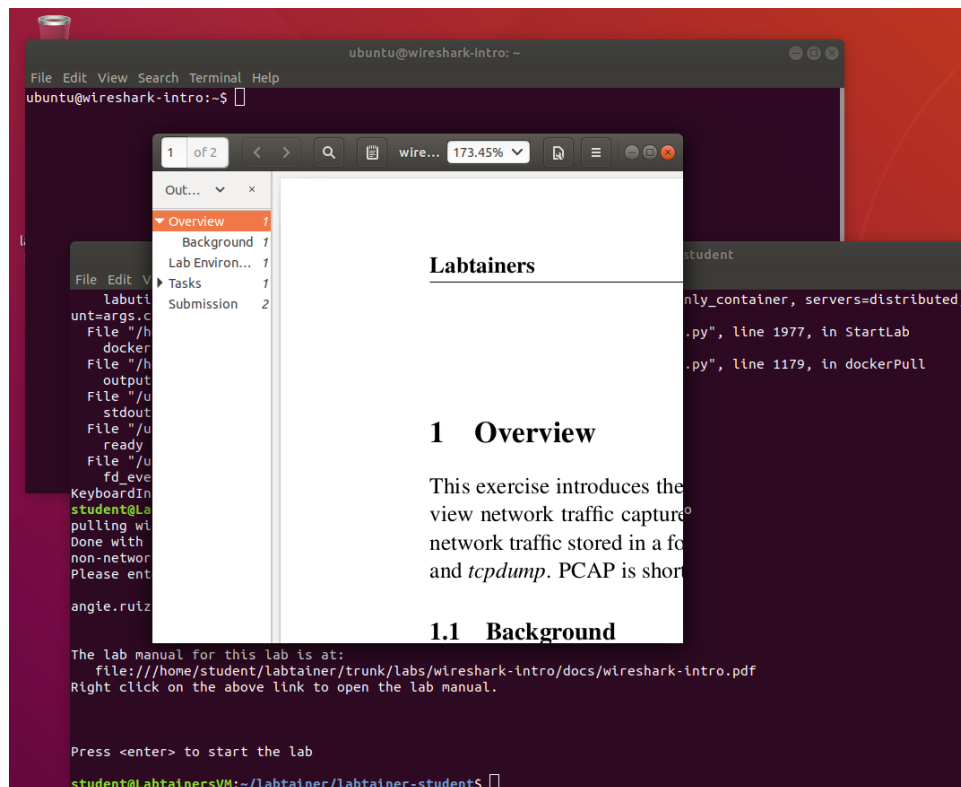
Wireshark Introduction and PCAP Analysis Labs:

1. Objetivos Generales:

- Entender el funcionamiento del tráfico de red Telnet usando la herramienta Wireshark.
- Entender el análisis de archivos PCAP de Tshark.
- Aprender a usar la herramienta Wireshark para capturar archivos PCAP (interfaz de una aplicación de programación para captura de paquetes) y para localizar un paquete específico.
- Aprender a usar la herramienta Tshark para analizar archivos PCAP y para localizar un paquete específico.
- Aprender a analizar los inicios de sesión inválidos en los PCAP.

2. Pasos de realización del laboratorio "Wireshark Introduction":

Ingresaremos al ambiente con "labtainer wireshark-intro", luego digitamos nuestro correo electrónico y posteriormente abriremos el archivo correspondiente al laboratorio:

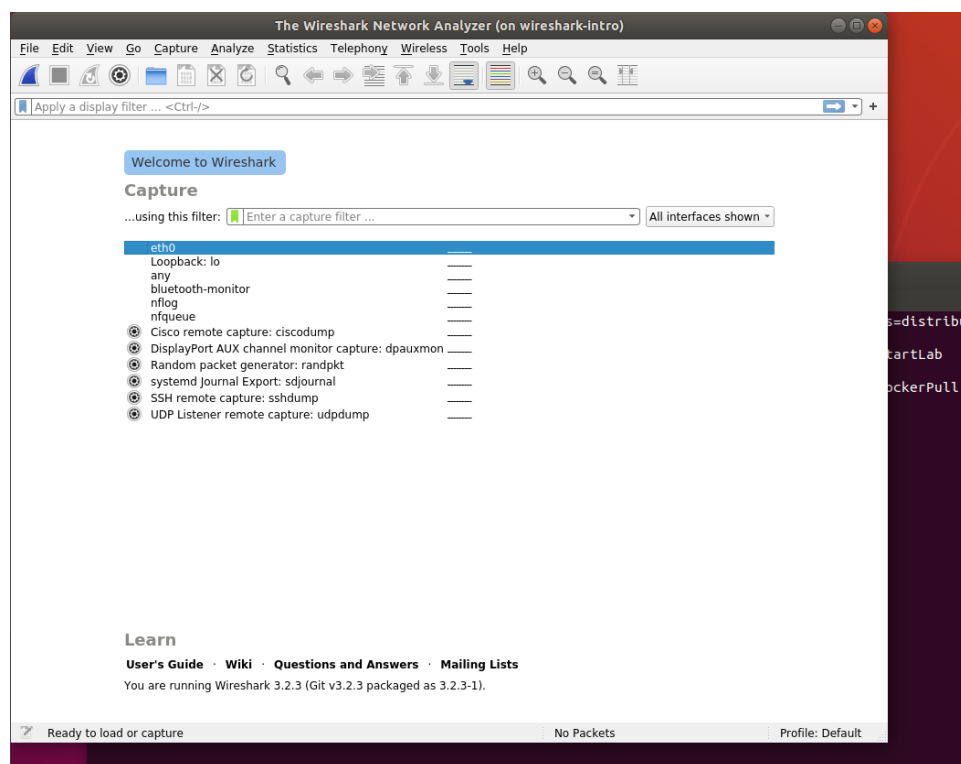


Tarea 1: Utilizaremos el comando "ls -l" para ver el contenido del directorio en la terminal del ambiente del laboratorio, en el contenido vemos el archivo telnet.pcap, el

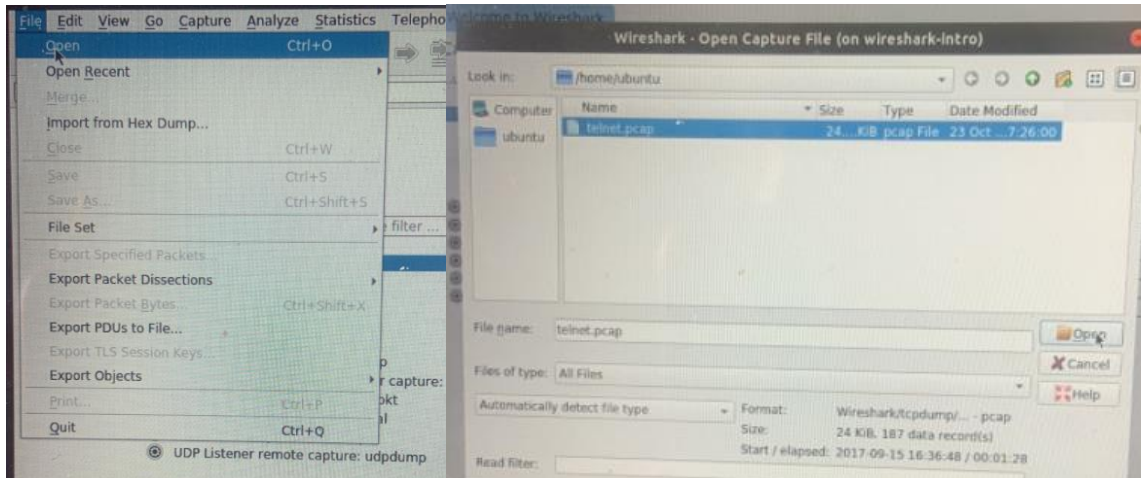
cual contiene el tráfico de red que se usará para analizar, por ende, para comenzar usaremos el comando “file telnet.pcap” para ver la información acerca del archivo:

```
ubuntu@wireshark-intro: ~  
File Edit View Search Terminal Help  
ubuntu@wireshark-intro:~$ ls -l  
ls: cannot access '$'\342\200\223'\302\240': No such file or directory  
ubuntu@wireshark-intro:~$ ls -l  
total 28  
-rw-rw-r-- 1 ubuntu ubuntu 25364 Oct 23 17:26 telnet.pcap  
ubuntu@wireshark-intro:~$ file telnet.pcap  
telnet.pcap: pcap capture file, microsecond ts (little-endian) - version 2.4 (Ethernet, capture length 262144)  
ubuntu@wireshark-intro:~$
```

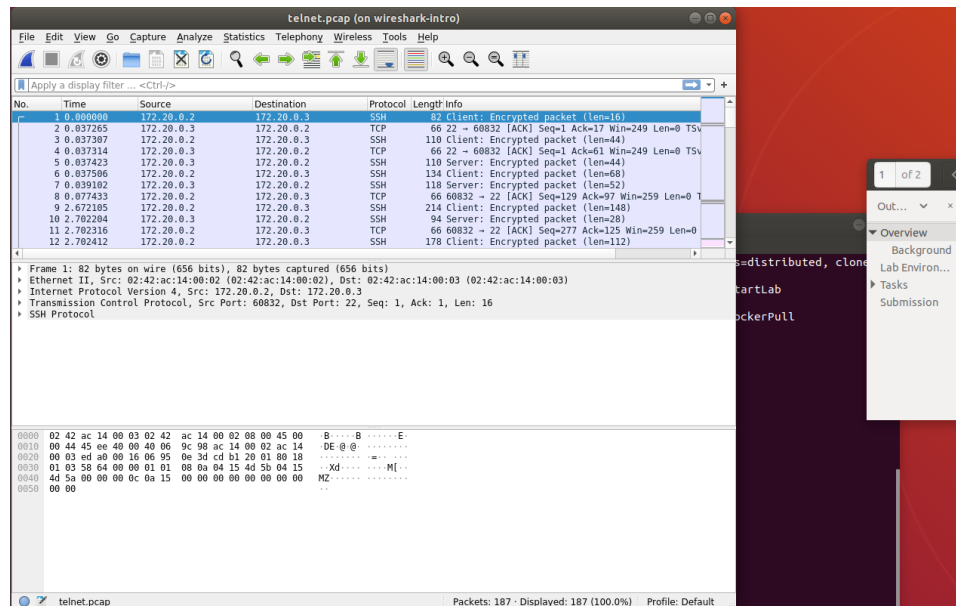
Tarea 2: Ahora utilizaremos el comando "wireshark" y se nos abrirá la siguiente ventana:



Ahora abriremos el archivo que mencionaban en la anterior tarea de la siguiente manera:

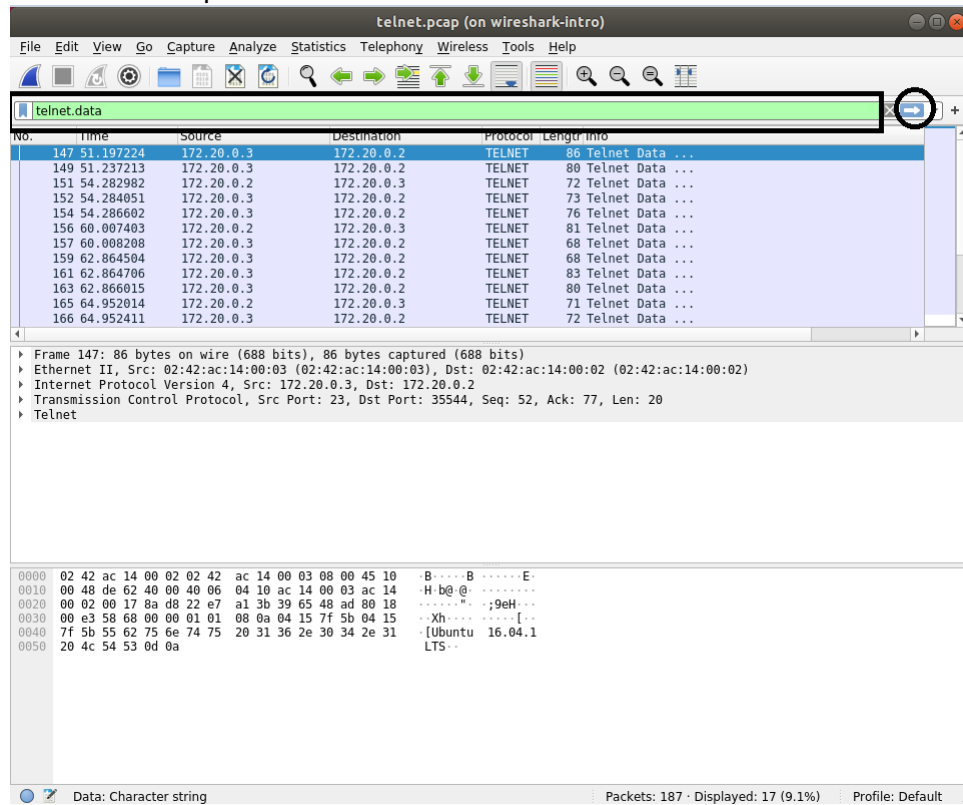


Para ver finalmente el archivo abierto en la pantalla:



Tarea3: Ahora buscaremos un archivo específico, el cual contiene la contraseña proporcionada cuando el usuario intentó utilizar Telnet para iniciar sesión como usuario "john", entonces primero en el espacio donde nos dice que podemos aplicar filtros (rectángulo) ingresaremos "telnet.data" y en la flechita (círculo) haremos clic para aplicar

el filtro de búsqueda



telnet.pcap (on wireshark-intro)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet.data

No.	Time	Source	Destination	Protocol	Length	Info
147	51.197224	172.20.0.3	172.20.0.2	TELNET	86	Telnet Data ...
149	51.237213	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
151	54.282982	172.20.0.2	172.20.0.3	TELNET	72	Telnet Data ...
152	54.284951	172.20.0.3	172.20.0.2	TELNET	73	Telnet Data ...
154	54.286602	172.20.0.3	172.20.0.2	TELNET	76	Telnet Data ...
156	60.007403	172.20.0.2	172.20.0.3	TELNET	81	Telnet Data ...
157	60.008208	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
159	62.864504	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
161	62.864706	172.20.0.3	172.20.0.2	TELNET	83	Telnet Data ...
163	62.866015	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
165	64.952014	172.20.0.2	172.20.0.3	TELNET	71	Telnet Data ...
166	64.952411	172.20.0.3	172.20.0.2	TELNET	72	Telnet Data ...

Frame 147: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
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)
Internet Protocol Version 4, Src: 172.20.0.3, Dst: 172.20.0.2
Transmission Control Protocol, Src Port: 23, Dst Port: 35544, Seq: 52, Ack: 77, Len: 20
Telnet

0000 02 42 ac 14 00 02 02 42 ac 14 00 03 08 00 45 10 -B-...B-...E-
0010 00 48 de 62 40 00 40 06 04 10 ac 14 00 03 ac 14 -H-b@-...-
0020 00 02 00 17 8a d8 22 e7 a1 3b 39 65 48 ad 80 18 -...-;9eH-...
0030 00 e3 58 68 00 00 01 01 08 0a 04 15 7f 5b 04 15 -Xh-...-...
0040 7f 5b 55 62 75 6e 74 75 20 31 36 2e 30 34 2e 31 -[Ubuntu 16.04.1
0050 20 4c 54 53 0d 0a LTS-...

Data: Character string

Packets: 187 · Displayed: 17 (9.1%) Profile: Default

Acá como vemos tenemos el único paquete con la contraseña no válida:

Wireshark

telnet.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet.data

No.	Time	Source	Destination	Protocol	Length	Info
147	51.197224	172.20.0.3	172.20.0.2	TELNET	86	Telnet Data ...
149	51.237213	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
151	54.282982	172.20.0.2	172.20.0.3	TELNET	72	Telnet Data ...
152	54.284051	172.20.0.3	172.20.0.2	TELNET	73	Telnet Data ...
154	54.286602	172.20.0.3	172.20.0.2	TELNET	76	Telnet Data ...
156	60.007403	172.20.0.2	172.20.0.3	TELNET	81	Telnet Data ...
157	60.008208	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
159	62.064504	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
161	62.064706	172.20.0.3	172.20.0.2	TELNET	83	Telnet Data ...
163	62.066015	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...
165	64.952014	172.20.0.2	172.20.0.3	TELNET	71	Telnet Data ...
166	64.952411	172.20.0.3	172.20.0.2	TELNET	72	Telnet Data ...
168	64.953762	172.20.0.3	172.20.0.2	TELNET	76	Telnet Data ...
170	72.000413	172.20.0.2	172.20.0.3	TELNET	80	Telnet Data ...
171	75.001123	172.20.0.3	172.20.0.2	TELNET	68	Telnet Data ...
173	75.422692	172.20.0.3	172.20.0.2	TELNET	85	Telnet Data ...
175	75.423556	172.20.0.3	172.20.0.2	TELNET	80	Telnet Data ...

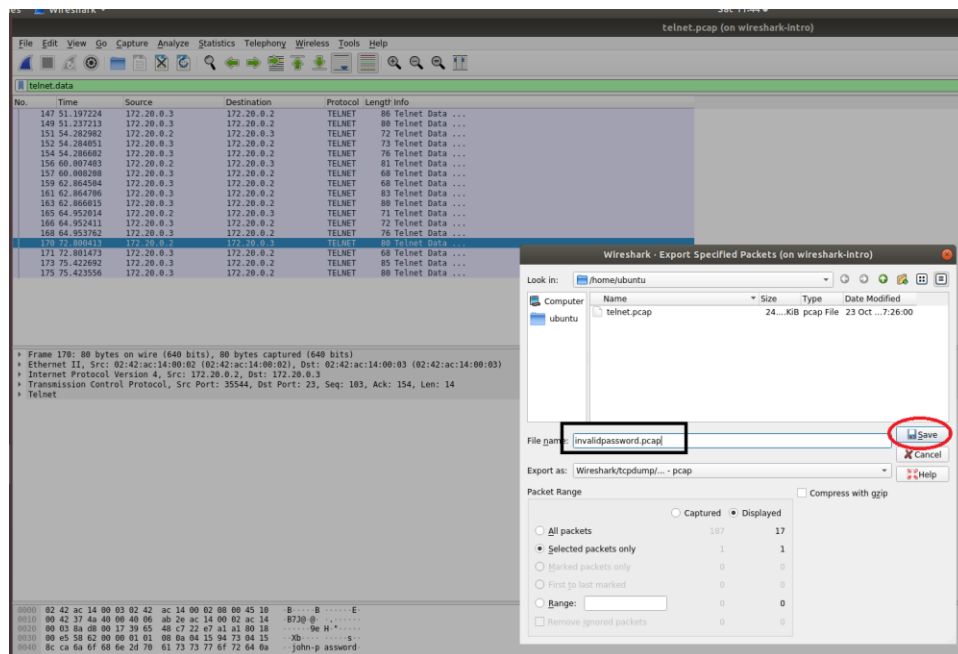
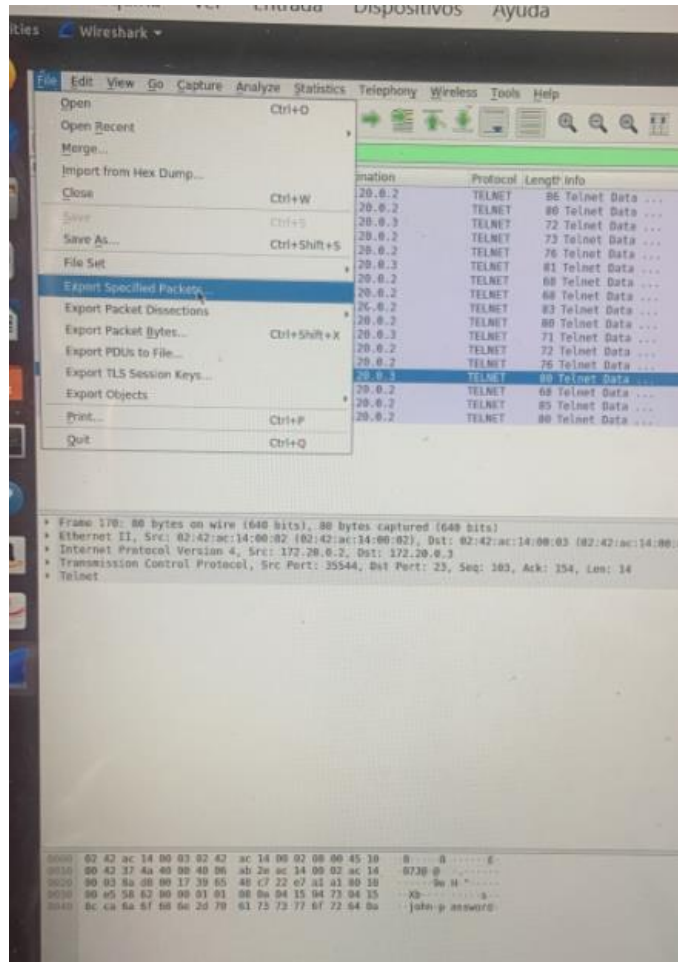
Frame 170: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)

- Ethernet II, Src: 02:42:ac:14:00:02 (02:42:ac:14:00:02), Dst: 02:42:ac:14:00:03 (02:42:ac:14:00:03)
- Internet Protocol Version 4, Src: 172.20.0.2, Dst: 172.20.0.3
- Transmission Control Protocol, Src Port: 35544, Dst Port: 23, Seq: 103, Ack: 154, Len: 14
- Telnet

```

0000  02 42 ac 14 00 03 02 42 ac 14 00 02 08 00 45 10  -B-----E-
0010  00 42 37 4a 40 00 40 06 ab 2e ac 14 00 02 ac 14  -B73@.@-
0020  00 03 8a d8 00 17 39 65 48 c7 22 e7 a1 80 18  -.....9eH*
0030  00 e5 58 62 00 00 01 01 08 0a 04 15 94 73 04 15  -..Xb.....S-
0040  8c ca 6a 6f 68 6e 2d 70 61 73 73 77 6f 72 64 0a  -..john-p assword
  
```

Por ende, ahora lo vamos a exportar y guardar de la siguiente manera:



LabtainerVM-2-baseline [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Wireshark Sat 11:4 invalidpassword.pcap (or

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

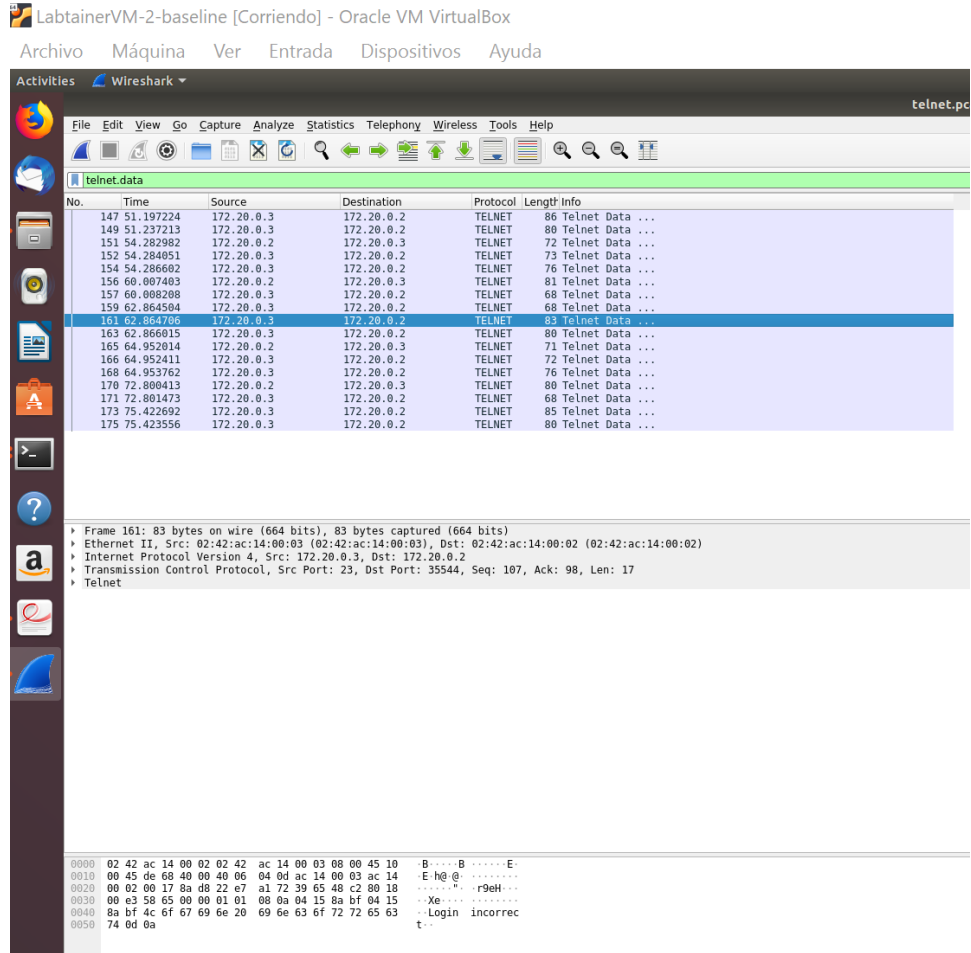
telnet.data

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.0.2	172.20.0.3	TELNET	80	Telnet Data ...

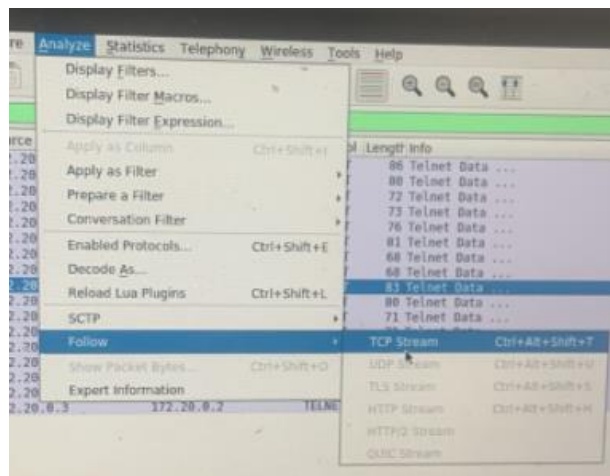
▶ Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
 ▶ Ethernet II, Src: 02:42:ac:14:00:02 (02:42:ac:14:00:02), Dst: 02:42:ac:14:00:03 (02:42:ac:14:00:03)
 ▶ Internet Protocol Version 4, Src: 172.20.0.2, Dst: 172.20.0.3
 ▶ Transmission Control Protocol, Src Port: 35544, Dst Port: 23, Seq: 1, Ack: 1, Len: 14
 ▶ Telnet

```

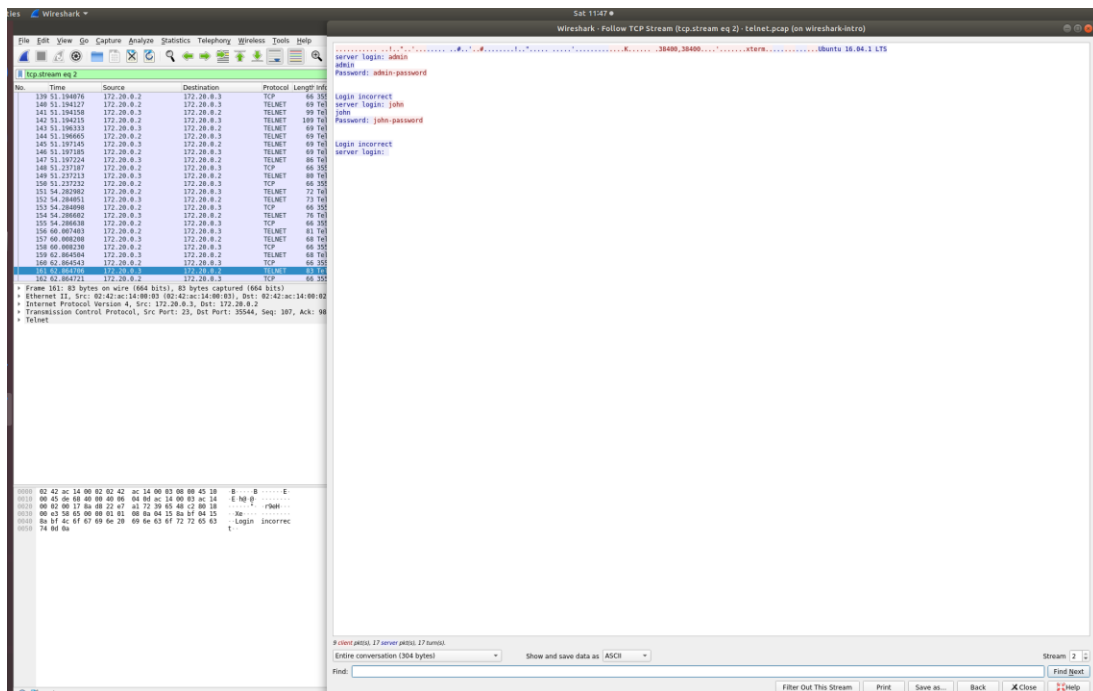
0000  02 42 ac 14 00 03 02 42  ac 14 00 02 08 00 45 10  -B---B-----E-
0010  00 42 37 4a 40 00 40 06  ab 2e ac 14 00 02 ac 14  -B730000000000
0020  00 03 8a 08 00 17 39 65  48 c7 22 e7 a1 a1 80 18  -...9eH*.....
0030  00 e5 58 62 00 00 01 01  08 0a 04 15 94 73 04 15  -Xb.....5...
0040  8c ca 6a 6f 68 6e 2d 70  61 73 73 77 6f 72 64 0a  -..john-p assword
  
```



Y usaré esta función para seguir el flujo TCP:

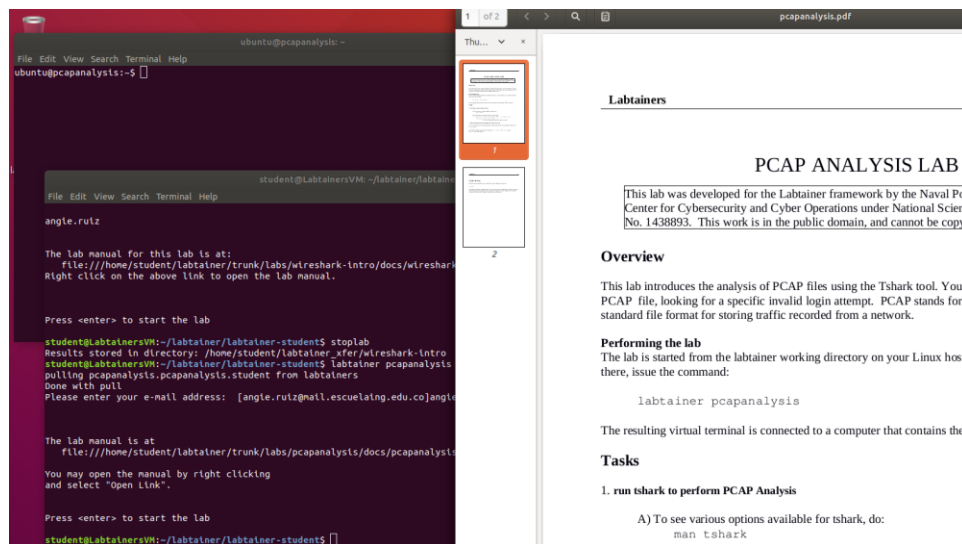


Y veremos finalmente la pantalla de la conversación TELNET completa:



3. Pasos de realización del laboratorio “PCAP Analysis”:

Ingresaremos al ambiente con "labtainer pcapanalysis", luego digitamos nuestro correo electrónico y posteriormente abriremos el archivo correspondiente al laboratorio:



Tarea 1: En la terminal del ambiente del laboratorio colocaremos el comando "man tshark" para ver las opciones disponibles a realizar.

```
ubuntu@pcapanalysis: ~  
File Edit View Search Terminal Help  
TSHARK(1) The Wireshark Network Analyzer TSHARK(1)  
  
NAME  
tshark - Dump and analyze network traffic  
  
SYNOPSIS  
tshark [ -2 ] [ -a <capture autopstop 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|adod|d|dd|e|r|u|ud|udod ]  
[ -T fields|pdm|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  
Manual page tshark(1) line 1 (press h for help or q to quit)
```

Ahora, por ejemplo, para mostrar campos específicos como lo son el número del fotograma, la fecha, la hora, los datos telnet y el paquete telnet; usaremos “tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap” y veremos lo siguiente:

```
LabtainerVM-2-baseline [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
Activities Terminal  
File Edit View Search Terminal Help  
95 Sep 15, 2017 17:33:43.131199000 UTC  
96 Sep 15, 2017 17:33:43.131256000 UTC  
97 Sep 15, 2017 17:33:43.131787000 UTC  
98 Sep 15, 2017 17:33:43.131833000 UTC  
99 Sep 15, 2017 17:33:43.149802000 UTC  
100 Sep 15, 2017 17:33:43.149839000 UTC  
101 Sep 15, 2017 17:33:43.149890000 UTC  
102 Sep 15, 2017 17:33:43.149921000 UTC  
103 Sep 15, 2017 17:33:43.149978000 UTC  
104 Sep 15, 2017 17:33:43.152096000 UTC  
105 Sep 15, 2017 17:33:43.152428000 UTC  
106 Sep 15, 2017 17:33:43.152908000 UTC  
107 Sep 15, 2017 17:33:43.152948000 UTC  
108 Sep 15, 2017 17:33:43.152987000 UTC Ubuntu 16.04.1 LTS  
  
109 Sep 15, 2017 17:33:43.192950000 UTC  
110 Sep 15, 2017 17:33:43.192976000 UTC server login:  
111 Sep 15, 2017 17:33:43.192995000 UTC  
112 Sep 15, 2017 17:33:46.238745000 UTC admin  
  
113 Sep 15, 2017 17:33:46.239814000 UTC admin  
  
114 Sep 15, 2017 17:33:46.239861000 UTC  
115 Sep 15, 2017 17:33:46.242365000 UTC Password:  
116 Sep 15, 2017 17:33:46.242401000 UTC  
117 Sep 15, 2017 17:33:51.963166000 UTC admin-password  
  
118 Sep 15, 2017 17:33:51.963971000 UTC  
  
119 Sep 15, 2017 17:33:51.963993000 UTC  
120 Sep 15, 2017 17:33:54.820267000 UTC  
  
121 Sep 15, 2017 17:33:54.820306000 UTC  
122 Sep 15, 2017 17:33:54.820469000 UTC Login incorrect  
  
123 Sep 15, 2017 17:33:54.820484000 UTC  
124 Sep 15, 2017 17:33:54.821778000 UTC server login:  
125 Sep 15, 2017 17:33:54.821997000 UTC  
126 Sep 15, 2017 17:33:56.907777000 UTC john  
  
127 Sep 15, 2017 17:33:56.908174000 UTC john  
  
128 Sep 15, 2017 17:33:56.908196000 UTC  
129 Sep 15, 2017 17:33:56.909525000 UTC Password:  
130 Sep 15, 2017 17:33:56.909542000 UTC  
131 Sep 15, 2017 17:34:04.756176000 UTC john-password  
  
132 Sep 15, 2017 17:34:04.757236000 UTC  
  
133 Sep 15, 2017 17:34:04.757286000 UTC  
134 Sep 15, 2017 17:34:07.378455000 UTC  
Login incorrect  
  
135 Sep 15, 2017 17:34:07.378503000 UTC  
136 Sep 15, 2017 17:34:07.379319000 UTC server login:  
137 Sep 15, 2017 17:34:07.379359000 UTC  
138 Sep 15, 2017 17:34:12.510911000 UTC  
139 Sep 15, 2017 17:34:12.511804000 UTC  
140 Sep 15, 2017 17:34:12.511923000 UTC  
141 Sep 15, 2017 17:34:17.377326000 UTC  
142 Sep 15, 2017 17:34:17.377401000 UTC  
143 Sep 15, 2017 17:34:18.378691000 UTC  
144 Sep 15, 2017 17:34:18.378732000 UTC  
145 Sep 15, 2017 17:34:19.377644000 UTC  
146 Sep 15, 2017 17:34:19.377685000 UTC  
147 Sep 15, 2017 17:34:20.377160000 UTC  
148 Sep 15, 2017 17:34:20.377217000 UTC
```

Tarea 2: Finalmente intentaremos localizar el paquete único que contiene la clave “admin” que no es válida. Buscaremos al usuario admin, para ello utilizaremos la opción “-Y frame.number == N”. 117 en este caso, es el número del fotograma por el cual reemplazaremos N, de la siguiente manera:

```
ubuntu@pcapanalysis:~$ tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap -Y frame.number==117
117   Sep 15, 2017 17:33:51.963166000 UTC      admin-password
```

4. Conclusiones:

- Wireshark es un analizador de protocolos, sobre el cual se realizan análisis y se solucionan problemas en redes de comunicaciones. En este laboratorio como vimos el protocolo usado fue Telnet, y este es un protocolo de comunicaciones (es inseguro debido a que no es cifrado) el cual permite a un usuario emitir comandos de shell a un host remoto.
- Con wireshak podemos aplicar filtros sobre el análisis que hace la aplicación sobre la red, y además nos permite inspeccionar cada elemento encontrado y si queremos, podemos crear un solo archivo pcap por separado de unos elementos específicos que nos interesen.
- Con el filtro telnetn.data podemos analizar los inicios de sesión inválidos en los PCAP desde wireshark, tiene la opción de seguir el flujo TCP permitiéndonos así ver la conversación TELNET completa.
- TShark es una versión de Wireshark (admite sus mismas opciones) orientada a terminales, usada para capturar y mostrar paquetes cuando una interfaz de usuario interactiva no es necesaria o no está disponible.
- Tshark nos permite desde consola digitar comandos que nos permiten ver los campos que deseamos de la información TELNET, y en caso de requerirlo, también nos permite localizar un paquete específico dado el número del fotograma para cuando veamos algo de interés, como en estos casos, inicios de sesión no válidos.