

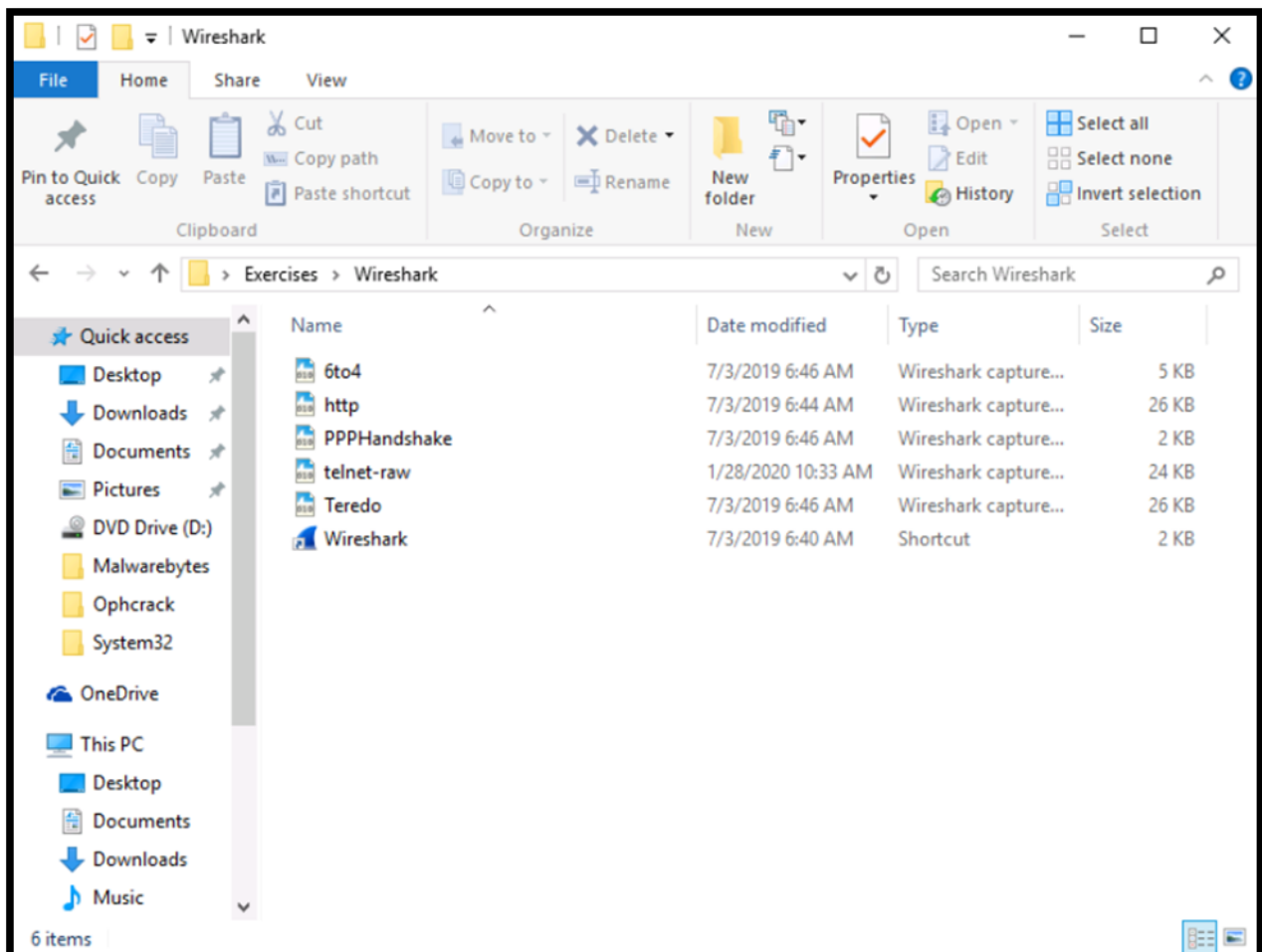
# 1.3 Guided Exercise: Analysing Telnet Network Traffic

## Resources

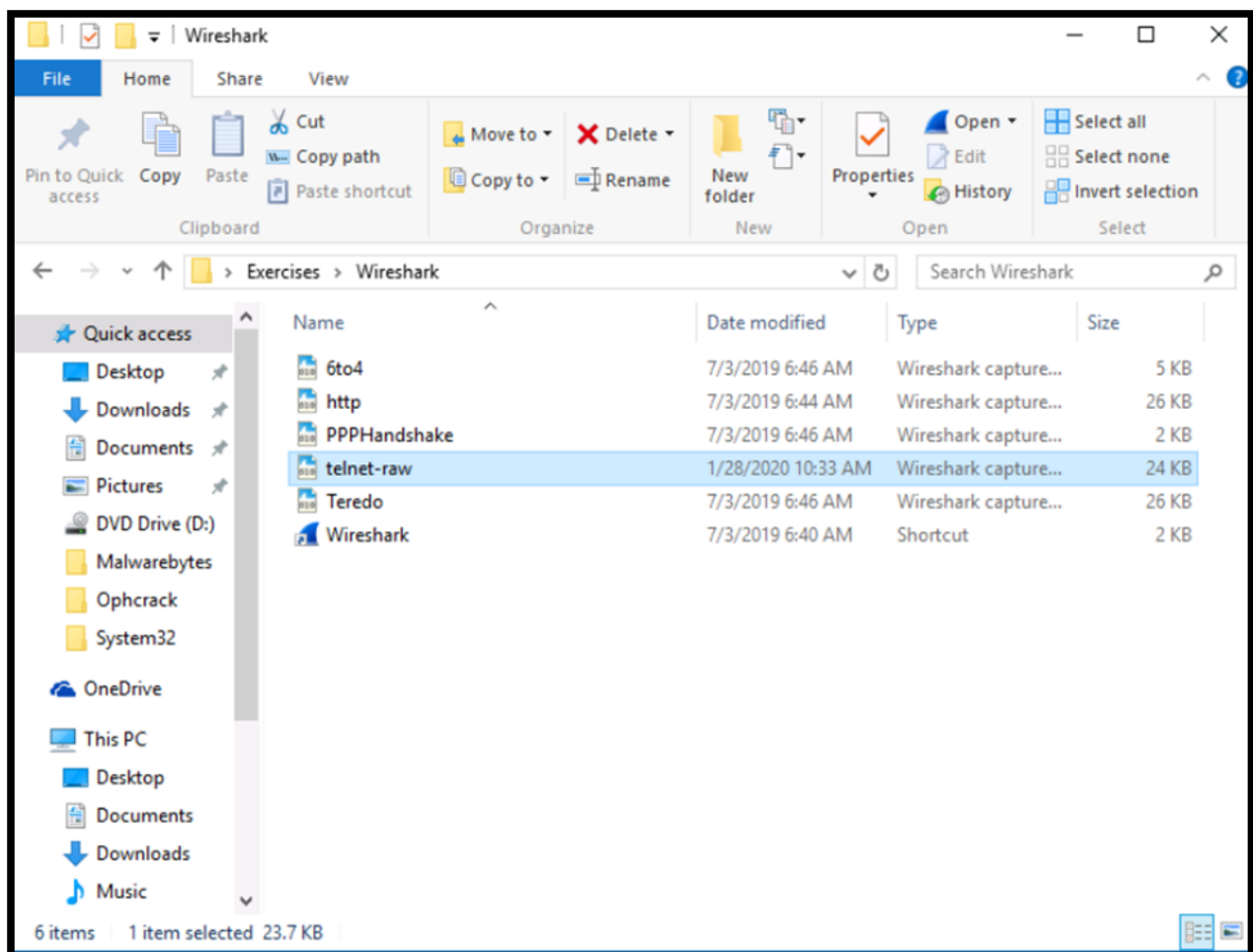
Files	None
Machines	Windows 10

In this exercise you will use Wireshark to analyse network traffic.

Wireshark is already installed and you may start it by opening the Desktop folder called Exercises and then Wireshark. Double click Wireshark to open it.



Once Wireshark starts go to File -> Open and select the file called telnet-raw from the folder Exercises -> Wireshark.



Once the file opens locate the Source and Destination IPv4 addresses. These should be 192.168.0.2 and 192.168.0.1 respectively.

telnet-raw.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1254 → 23 [SYN] Seq=0
2	0.001690	192.168.0.1	192.168.0.2	TCP	74	23 → 1254 [SYN, ACK]
3	0.001741	192.168.0.2	192.168.0.1	TCP	66	1254 → 23 [ACK] Seq=1
4	0.013173	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150283	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150351	192.168.0.2	192.168.0.1	TCP	66	1254 → 23 [ACK] Seq=2

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: Lite-OnU\_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD\_9f:a0:97 (00:00:c0:9f:a0:97)

> Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1

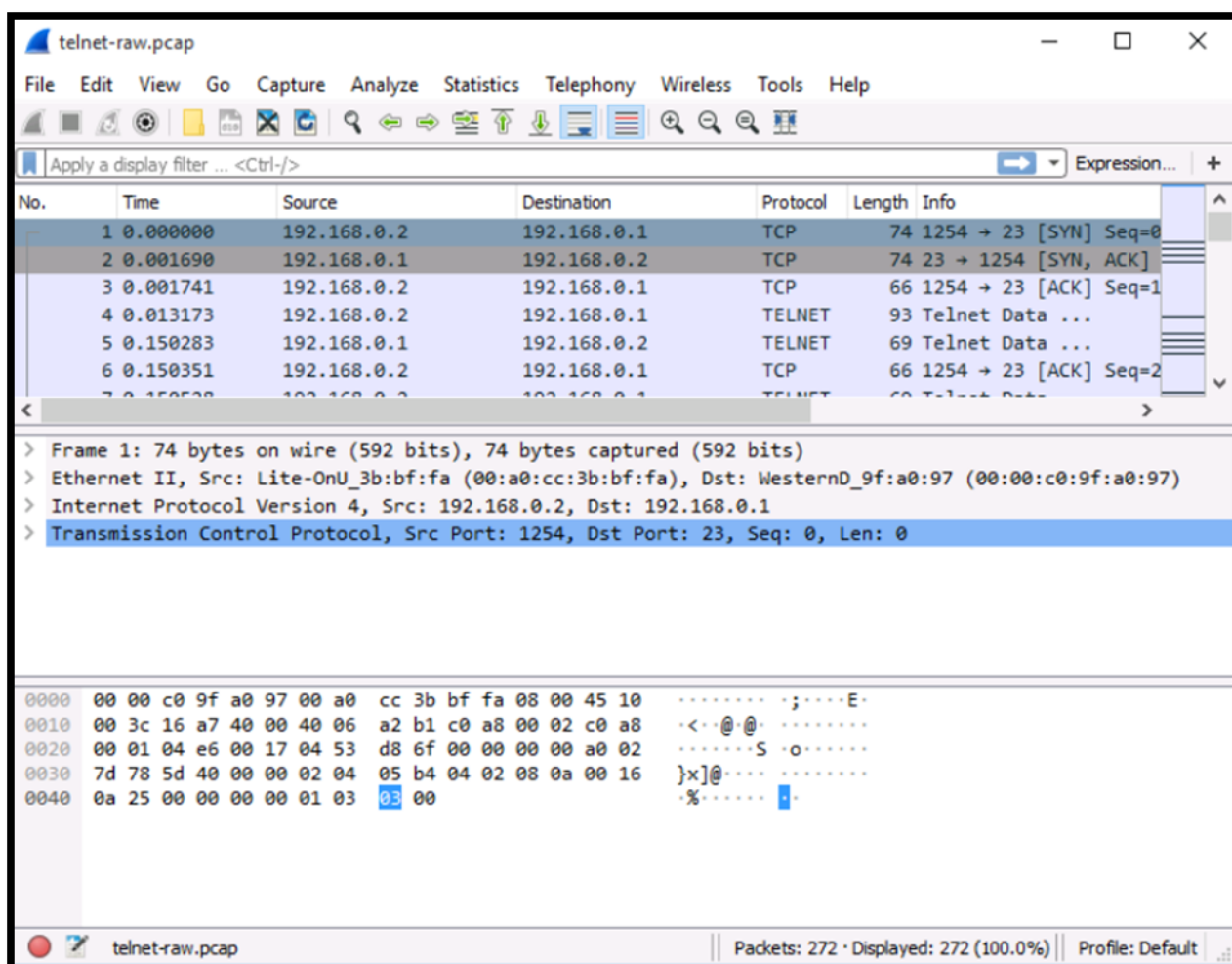
> Transmission Control Protocol, Src Port: 1254, Dst Port: 23, Seq: 0, Len: 0

```

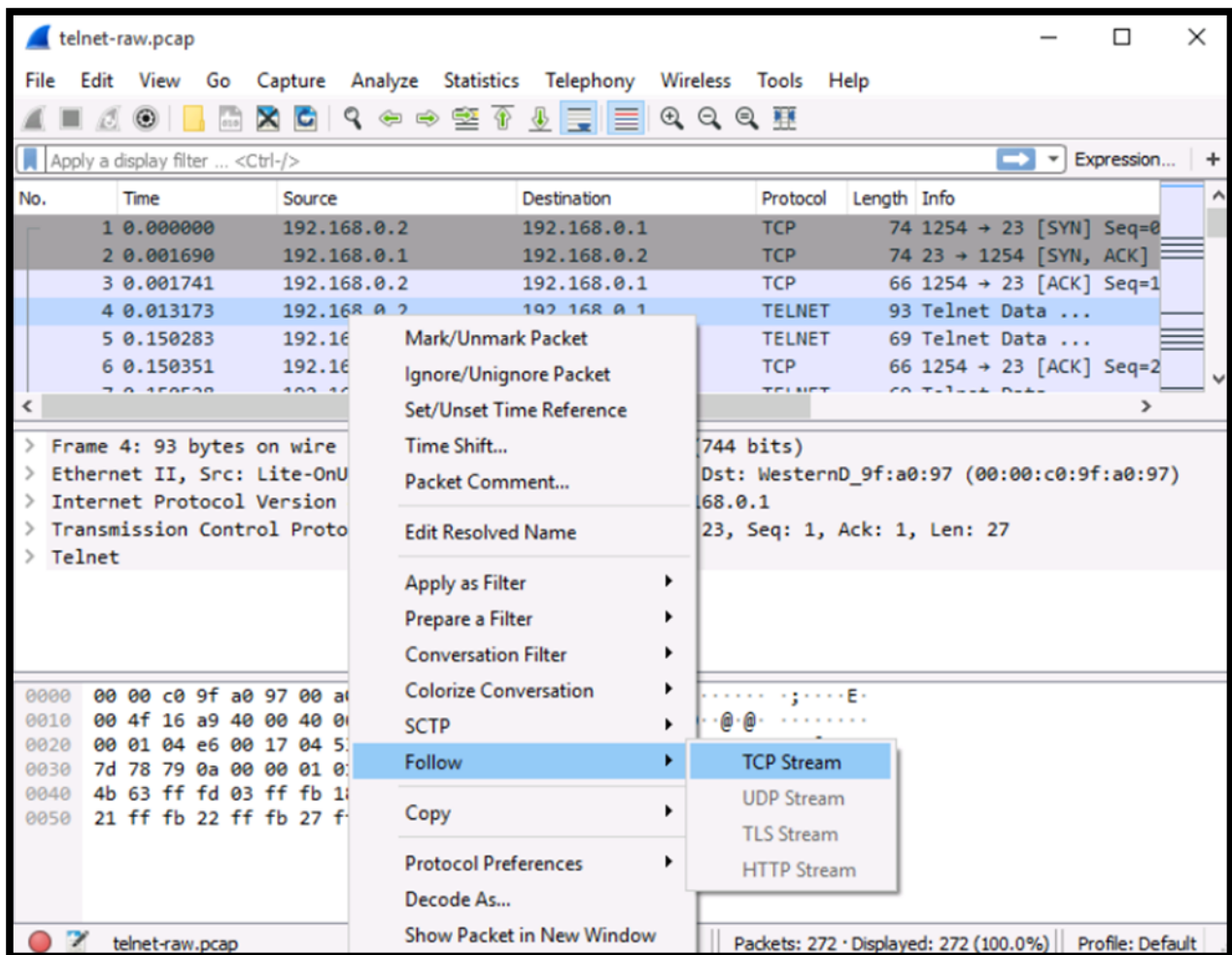
0000  00 00 c0 9f a0 97 00 a0 cc 3b bf fa 08 00 45 10  .....;....E.
0010  00 3c 16 a7 40 00 40 06 a2 b1 c0 a8 00 02 c0 a8  .<...@: @ .....
0020  00 01 04 e6 00 17 04 53 d8 6f 00 00 00 00 a0 02  .....S.o.....
0030  7d 78 5d 40 00 00 02 04 05 b4 04 02 08 0a 00 16  }x]@ .....
0040  0a 25 00 00 00 00 01 03 03 00  .....%.
  
```

telnet-raw.pcap | Packets: 272 · Displayed: 272 (100.0%) | Profile: Default

Determine the Source Port and Destination Port. These should be 1254 and 23 respectively.



Select packet number 4 and then right click on it. Go to Follow and then click on TCP Stream.



On the new window that opens you will notice the username and password that the user used to login to the telnet server. The username is “fake” and the password is “user”.

