Lab 6. TCP

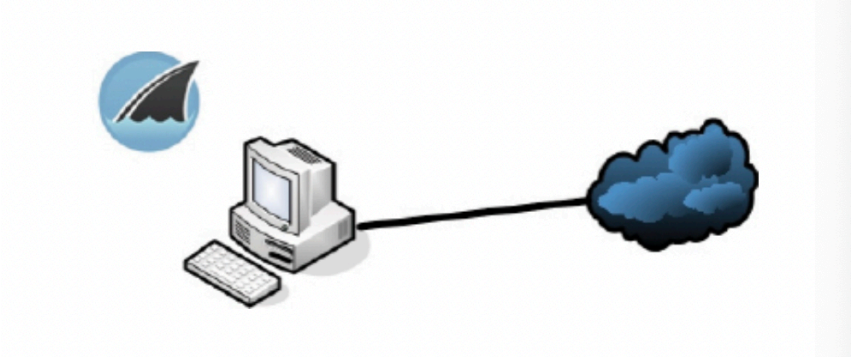
Lab Objective:
Learn how to recognize a TCP packet.

Lab Purpose:
TCP is the first part of the naming convention for the entire TCP/IP suite. It enables all connection-oriented services and protocols to run over networks such as Telnet, FTP, and some routing protocols, such as BGP.

Lab Tool:
Wireshark
Putty
Google

Lab Topology:
Run Wireshark.
Open Putty which is a Telnet/SSH client.
You can download Putty from https://putty.org.

It will make using Telnet much easier because most client software disables it by default.

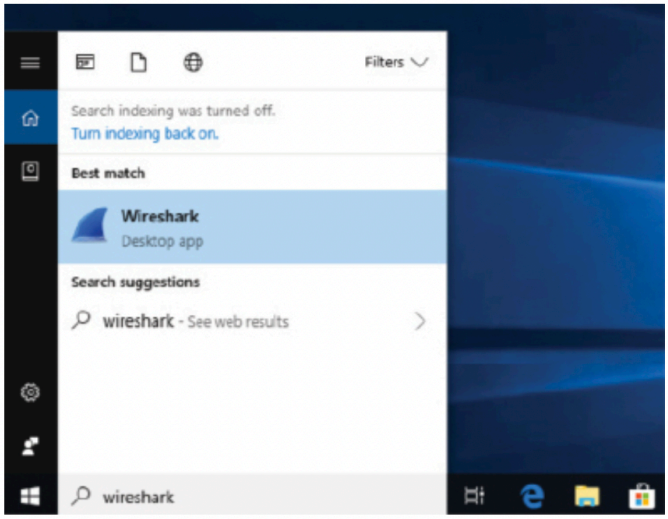


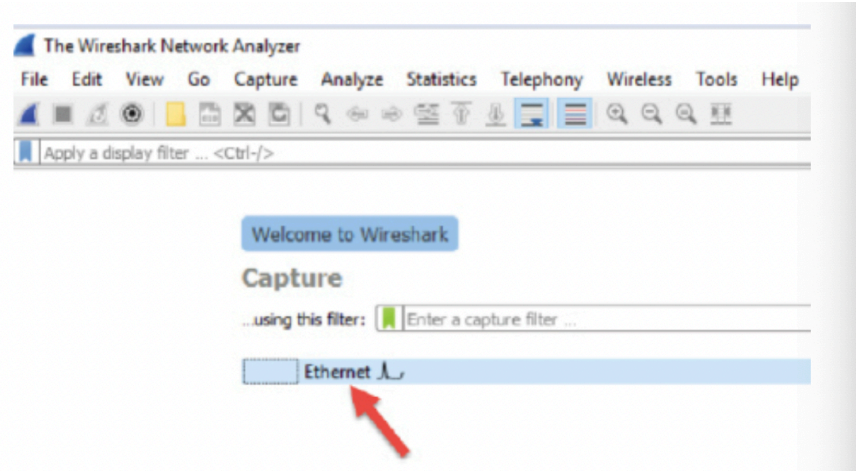
Lab Walkthrough::

Task 1:
Install Putty onto your device.

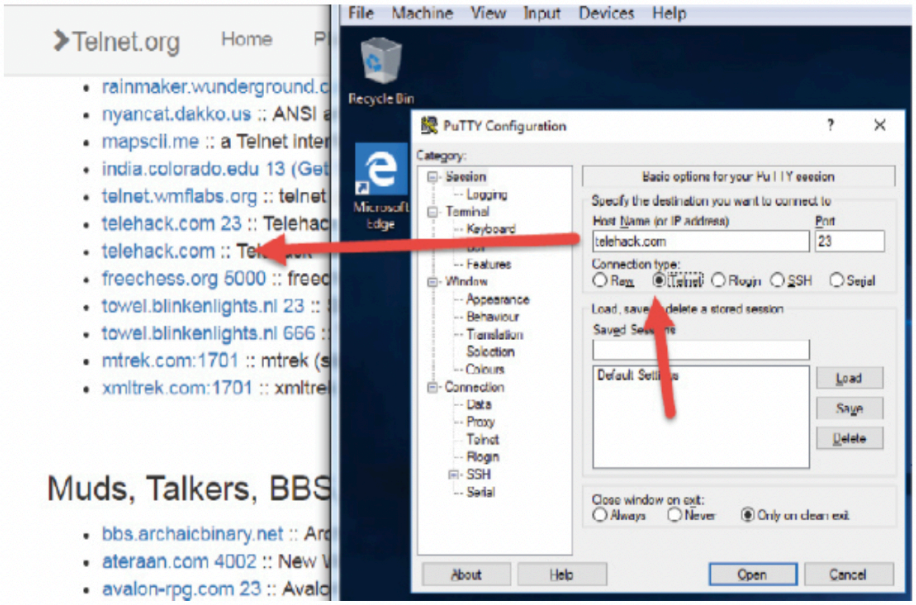
Task 2:
You may find using Telnet to access other devices on your network a bit tricky, so I checked on Google for hosts that permit Telnet. I found https://www.telnet.org/htm/places.htm and tried some of the suggestions there. The list may change, so your first attempt may fail.

Task 3:
Boot Wireshark on your PC and check the correct interface is the one being monitored. Click on the interface name to open the capture window.

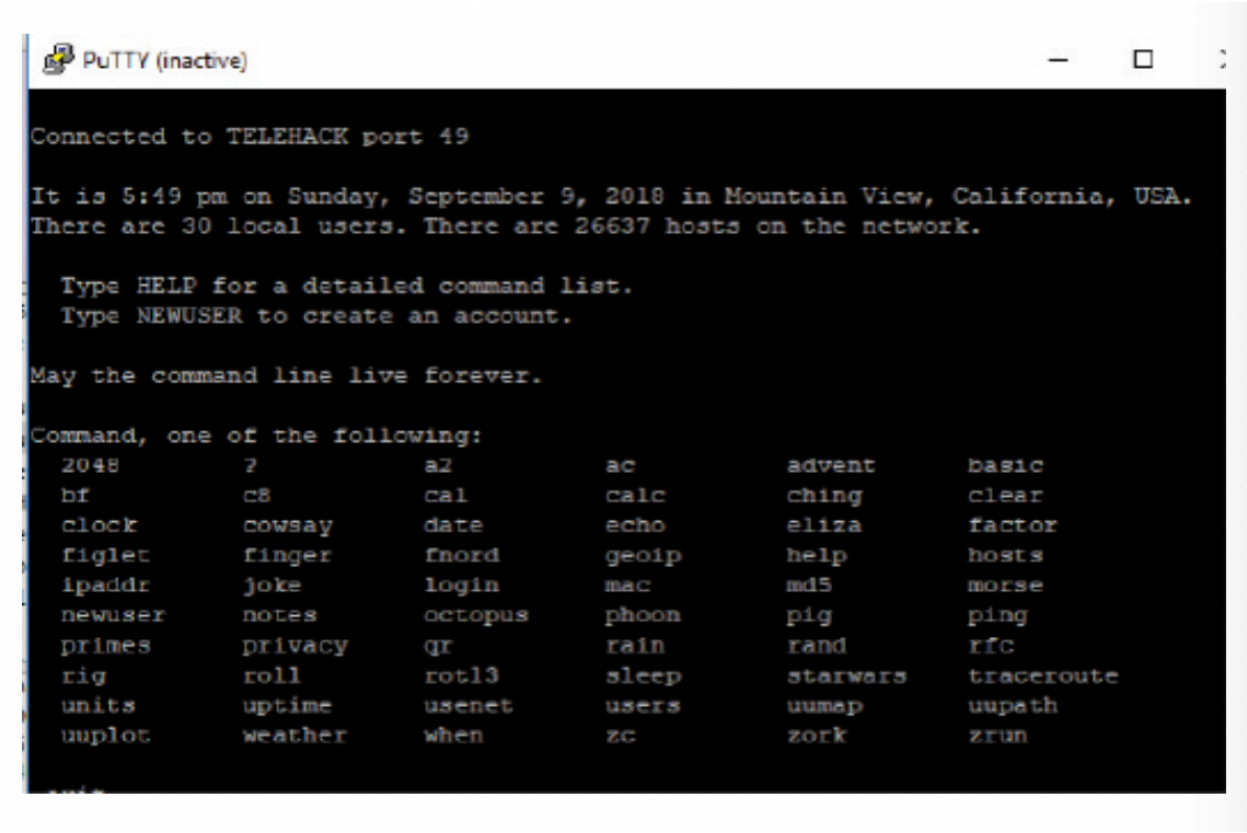




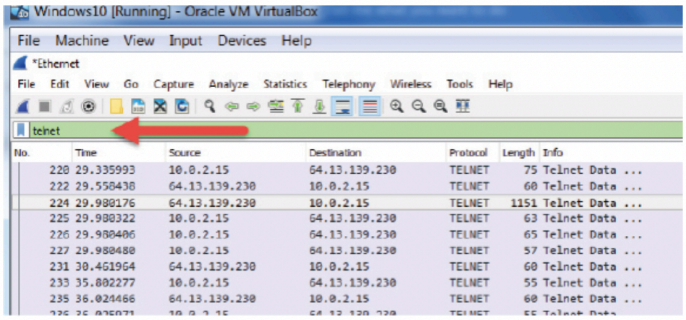
Task 4:
Open the Putty utility and enter the URL you wish to telnet to. I found that telehack.com worked well. You need to change from the default SSH to Telnet.



Task 5:
Your telnet session should work. Below is the window I was taken to for the Telehack website.

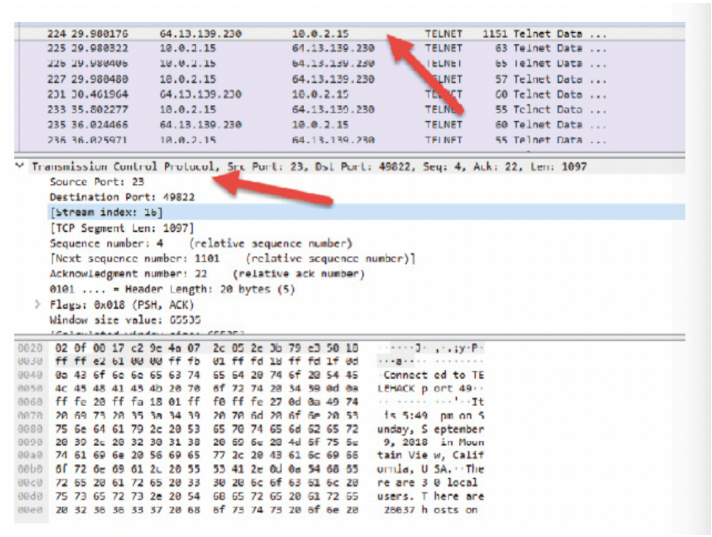


Task 6:
Go to Wireshark and in the filter box, type ‘telnet’ so you can see only the relevant traffic.

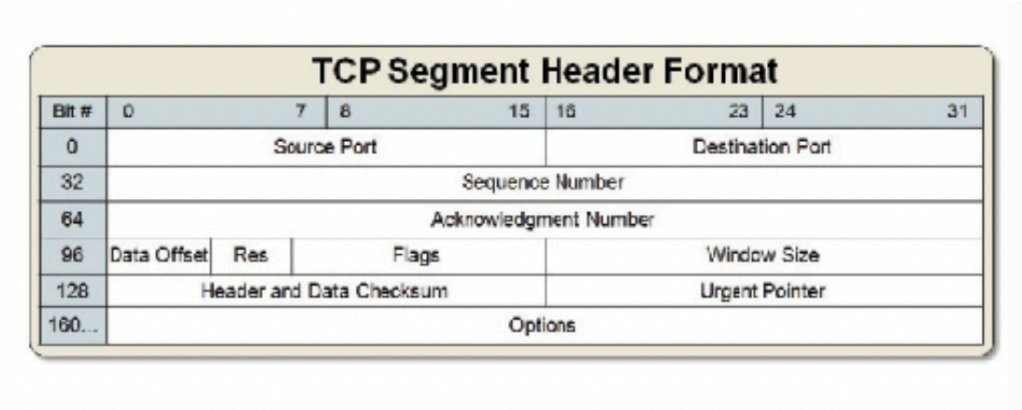


Task 7:

If you click on one of the packets, you can drill down to more detail. Please note that it says “TCP” which is what Telnet uses. Compare the fields to the image of the TCP packet below. See how many of the fields you can view.
You can see the source port is 23, which of course is Telnet. The bottom frame shows the actual text sent, which is in clear text, demonstrating the fact that there is no encryption involved.



Task 8:
You can use the below image as a reference to check the TCP fields



Task 9:

Lastly, note that Telnet does not encrypt the contents of the session, so you can easily see in the data stream what is being sent. This would include any passwords. You will find the actual data sent on the wire in the bottom windows of Wireshark.