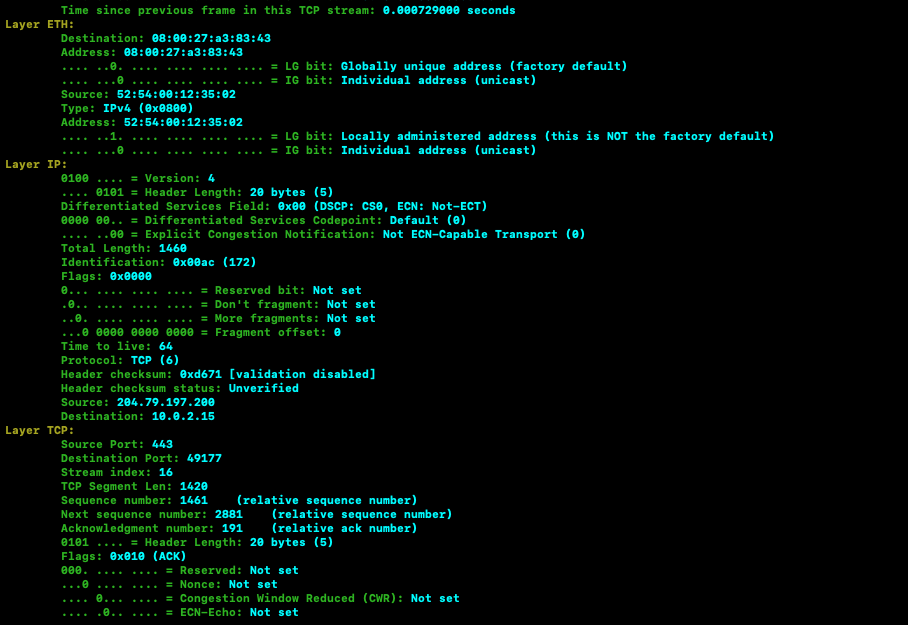
Pyshark and Scapy Lab

You will scraping and manipulating packets with pyshark and scapy. Please make sure that these two libraries are installed as well as Python 3.x

Using pyshark

Task 1

* Download cap.pcap from Blackboard
* Using pyshark, write a function in python that takes in a string file path to read the file pcap file. Save your file as pysahrk .pcap. Pretty print your results and post a screenshot of the output.



Task 2

* Filter your results to contain only traffic on tcp port 80 and 443. Use a Wireshark filter.

1. What was your filter? tcp.port==80 or tcp.port==443

Task 3

* Modify your output to keep track of tcp streams. (Hint: tcp streams are in pkt.tcp.stream)

1. How many packets are in the 2nd stream (pkt.tcp.stream =2) ? 2
2. What’s the largest tcp stream number? 9

Task 4

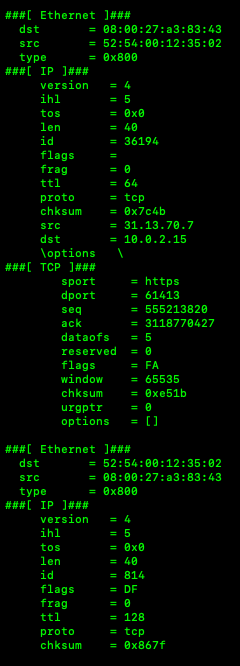
* Create a live capture. Save the capture as shark.pcap
* Use a BPF filter to show only tcp port 443 and port 80

1. What BPF filter did you use? ‘tcp port 443 or tcp port 80’

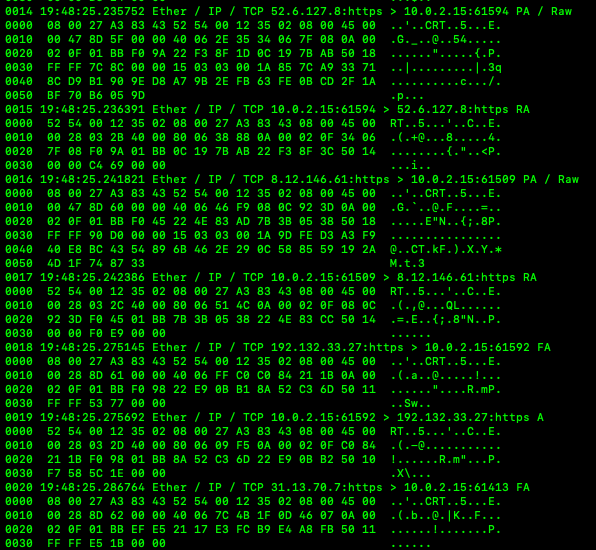
Using Scapy

Task 1

* Create a new script called scap.py
* Read the pcap file using scapy. Pretty print the output and paste a screenshot of the results.



* Hexdump the entire packet list and screenshot



* Save the fifth packet as a pdf report and attach it. Name it five.pdf. You will need the PyX library

Task 2

* Traceroute to ‘8.8.8.8’
* Create a graph of the traceroute using the graph() function. You will need the graphviz library. Use the target= ‘<filename>’ option

1. How many hops were there? Will vary

Task 3

* Create 100 IP packets to be sent to ‘8.8.8.8’. Fuzz the rest of the IP and TCP layers.

Task 4

* Prepare another 10 packets to be sent and received ‘192.168.1.1’. Make sure the packets have an IP and TCP field.
* Use .conversations() function to generate an .svg of the network conversation. Save the file as conversations.svg. Again use the target=’<filename>’ option.

1. How many answers did you receive? Will vary but should be greater than 0
2. Name three fields in the response packet’s TCP layer.

* sport
* dport
* seq
* ack
* dataofs
* reserved
* flags
* window
* chksum
* urgptr
* options

1. Name three fields in the response packet’s IP layer.

* version
* ihl
* tos
* len
* id
* flags
* frag
* ttl
* proto
* chksum
* src
* dst