Homework Part 1A

Richard Voragen - 917981018
Jonathan Yeung - 918630041
Files submitted: Reader.py, GetIpAddresses.py,
ChatGPT\Reader.py, ChatGPT\GetIpAddresses.py,
Part1.pcap, Part2.pcap, Part3.pcap, Part4.pcap, Part5.pcap

October 28, 2023

1 Part 1A - Monitoring live network traffic

1.1 Part 1: Displaying Different Application Layer Protocols (*Reader.py*)

In order to see the protocol for each of the activities we used dpkt.ethernet.Ethernet to get the ethernet data for the packet and then we used eth.data.get_proto(eth.data.p) to get the number correlating to the protocol. Finally we added .__name__ to get the written out name. We added this information to a dictionary to store and print it out. The table below displays the information.

Table 1: Different Application Layer Protocols

Activity	Protocols	Count
Ping Google.com x20	UDP	10
	ICMP	40
	TCP	18
Visit https://example.com	TCP	14
	UDP	9
Visit http://httpforever.com	UDP	19
	TCP	10
Access FTP Server	TCP	8
ssh into UNIX shell provider	TCP	20

1.2 Part 2: Showing http and https packets (*Reader.py*)

We keep track of the http and https packets by checking the dport and sport. If they are 80 then it is a http packet, if they are 443 then they are https. The table below shows the http requests, http responses, https requests, and https responses for activities 2 and 3.

Table 2: HTTP and HTTPS packets

Activity	Protocols	Count
Visit https://example.com	HTTP Requests	0
	HTTP Responses	0
	HTTPS Requests	7
	HTTPS Responses	7
Visit http://httpforever.com	HTTP Requests	2
	HTTP Responses	0
	HTTPS Requests	4
	HTTPS Responses	4

1.3 Part 3: Listing different Destination IP Addresses and Timestamps (*GetIpAddresses.py*)

Activity	Destination IP Addresses	Timestamps
Ping Google.com x20	224.0.0.251	1698607082.05484, 1698607083.067362, 1698607083.146384, 1698607083.147653, 1698607083.149346, 1698607084.073334, 1698607084.154283, 1698607084.158962, 1698607084.164516,
	142.250.189.238	1698607082.922974, 1698607083.941352, 1698607084.954933, 1698607085.978389, 1698607087.002982, 1698607088.02678, 1698607089.050615, 1698607090.0761, 1698607091.099726
	10.20.8.248	1698607082.951819, 1698607083.9673, 1698607084.462703, 1698607084.981508, 1698607086.004145, 1698607087.028784, 1698607087.595221, 1698607088.052545, 1698607089.075036
	10.20.8.242	1698607084.348002, 1698607084.50295, 1698607089.470557, 1698607089.625395, 1698607094.592781, 1698607094.746657, 1698607099.710085, 1698607099.862877,
	104.18.41.238	1698607087.579143, 1698607089.361183, 1698607102.607097,
	255.255.255.255	1698607094.12013
Visit https://example.com	142.251.46.195	1698965696.259656
	168.150.97.117	1698965696.267282, 1698965696.886144, 1698965696.945689, 1698965696.945689, 1698965696.945794, 1698965696.955425, 1698965697.201146, 1698965697.201146, 1698965697.201146, 1698965697.203241, 1698965697.673777, 1698965702.274859,
	142.251.46.164	1698965696.87763, 1698965696.895576, 1698965696.946101, 1698965696.94854
	93.184.216.34	1698965697.187045, 1698965697.187167, 1698965697.203296, 1698965697.658895
	142.251.46.238	1698965702.265013
	142.251.46.205	1698965702.455746
Visit http://httpforever.com	142.251.46.164	1698965105.580689, 1698965105.619147, 1698965105.625301, 1698965105.696935, 1698965105.697035, 1698965105.697084,
	168.150.97.117	1698965105.59232, 1698965105.624623, 1698965105.696615, 1698965105.696615, 1698965105.696615, 1698965105.730669, 1698965106.22268, 1698965106.780814, 1698965106.865714, 1698965107.869768, 1698965107.869768, 1698965107.890338,
	146.190.62.39	1698965106.211688, 1698965106.277615,
	172.64.134.11	1698965106.771429, 1698965106.771599, 1698965106.771674, 1698965106.771757, 1698965106.901093,
	23.39.1.24	1698965107.860301, 1698965107.869873,
	20.125.63.4	1698965107.860624, 1698965107.890471,
Access FTP Server	209.51.188.20	1698611532.662533, 1698611532.755697, 1698611533.016441, 1698611533.15229
	10.20.8.248	1698611532.755647, 1698611533.013283, 1698611533.10709, 1698611533.10709
ssh into UNIX shell provider	205.166.94.16	1698611611.211233, 1698611611.256237, 1698611611.26258, 1698611611.343346, 1698611611.398194, 1698611611.470638, 1698611611.710941, 1698611611.75699, 1698611611.942882, 1698611612.016813, 1698611612.117578,
	10.20.8.248	1698611611.256135, 1698611611.341222, 1698611611.391616, 1698611611.455516, 1698611611.710889, 1698611611.75677, 1698611611.942693, 1698611612.016416, 1698611612.072039,

1.4 Part 4: Can you tell which browser was used?

Yes, it is easy to tell what browser was used. If we look under the http headers, we can see that the user agent is ('user-agent', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64). This is because I use Google

Chrome for my web browser which is recognized as Mozilla/5.0 in the user agent field.

1.5 Part 5: ChatGPT Implementation ($ChatGPT\backslash Reader.py, ChatGPT\backslash GetIpAddresses.py$)

Reader.py: https://chat.openai.com/share/bed6e656-688b-4e5c-b822-4d4a158aa5e4
GetIpAddresses.py: https://chat.openai.com/share/fe542857-fa4a-4541-a075-a890f1b53d15