ECS 152A: HW1 Part 1b

Nghi Dao (921147615), Bian Lee (920763430)

November 2024

Link to ChatGPT conversation: Here. The GPT generated code can also be found in `1b_one_analysis_chatgpt.py`, and `1b_two_analysis_chatgpt.py` for the two parts. We referred to this generated code to polish our implementation and final code found in `1b_one_analysis.py` and `1b_two_analysis.py`.

- **Part 1:** The code reads the `ass1_1.pcap` file that lives in the same folder in binary mode, iterates over each packet and creates Ethernet object, to be able to check for IPv6 packets. It then checks if the data within the packet is of TCP or UDP, and if it's the case of either, it looks for occurences of string "secret" or "password" and prints the corresponding line.
- **Part 2:** The code reads the `ass1_2.pcap` and `ass1_3.pcap` makes external API call (https://ipinfo.io/) and checks if "city" is part of the returned response, and returns corresponding city if it is the case (if not, return "Unknown"). For each and every packet, it checks if it has IPv4 layer and also checks if it has ICMP protocol to then extract both the source and destination IP addresses. It extracts and prints out details like timestamp, protocol (ICMP), source and destination IPs, location, then the status based on ICMP packet type. If it's 11, it is "Time Exceeded", while if it's 3, it's Protocol Unreachable. The conclusion from the output is that the activity that both pcaps show is **Traceroute**, the second pcap shows greater delay in packet arrival, with greater number of geographic locations compared to first pcap which has fewer locations involved. The output of running the .py script is in `1b_two_results.txt`.