README

How to run program:
In the directory where the program file is located, in the terminal type the following:

```
python analysis_pcap_arp.py pcap_filename.pcap
```

(python file name, pcap file name)

Program logic:
(i) Count the number of ARP messages. Code should be generic and run on other pcap files with ARP messages.

The program reads the pcap file and loops through each packet. It checks bytes 12-13 of the packet to check to see if it is of type ARP (0x0806). If it is, the count increases by one. This includes ARP broadcasts, requests and replies.
The code is generic and runs on other pcap files with ARP messages. When looping through each packet, it checks if the packet is of type ARP and then processes it. The ARP packets are stored in the global arp_packets array. When processing each ARP packet, it uses struct arp, and saves header element variables based on the packet's corresponding bytes. ARP requests are appended to array arp_requests and ARP replies are appended to arp_replies. To obtain the first ARP exchange, it starts to check at the beginning of arp_replies and then checks arp_requests for its corresponding request.

(ii) Print the entire ARP request and response for one ARP package exchange.
Printing the entire ARP request and response for the first ARP package exchange is done by obtaining the first exchange's reply and request. This request and reply of the first exchange has been appended to arp_exchange. When printing, it prints arp_exchange[0], the request and arp_exchange[1], the reply. Since struct arp has it's variables stored as bytes, printing is done through formatting. Printing the destination, source, sender MAC address, sender IP address, target MAC address, sender IP address is done with struct.unpack. Hardware and protocol type is printed with int.from_bytes.

(ii) Based on the ARP messages, tell us the IP address and MAC address of your router. Explain how you determined this.

(iii)
My router:
IP address: 192.168.1.1
MAC address: Netgear_41:1a:75 (4c:60:de:41:1a:75)

I determined this from the ARP packets. I know that my home router is used to connect to the internet, and that my family and I have devices connected to the router. My home network is a LAN. I also know that my home router's brand is Netgear. When inspecting the ARP packets, many packets have the source "Netgear_41:1a:75" and many of them have destination

“Broadcast”. On a LAN, computers can hear packets going to other computers on the network. On the Broadcast packet info, it says what IP address that the request is looking for. I can see that some requests are sent to IP addresses other than my computer - other computers on the network. I only see responses for exchanges for my computer - responses are unicast. With the requests that have my router as the source/sender, and that have the destination/target for my computer, I can see the following response packet.