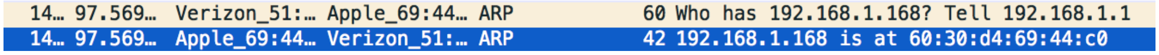
Programming Assignment 4: ARP Packet Capture and Analysis
CSE 310, Spring 2019
Instructor: Aruna Balasubramanian
Due date: April 29 2019, 9.00pm

The goal of this assignment is to learn how to perform packet capture and analysis on Wireshark. We are specifically going to look at ARP packets.

Part A Wireshark packet capture (15 points)

Your first task is to capture an ARP exchange from your computer. To do this, open Wireshark and start recording. It will be easier if you filter for the ``arp" packets. You should wait for some time, browse the Web etc and you will see an ARP message exchange. The message exchange includes a ARP request and a ARP response. Once you see the exchange, stop the capture and store the packet as ``assignment4_my_arp.pcap". Read a Wireshark tutorial on the Web if you are unsure how to do capture messages and store them.

Here is an example ARP message exchange I captured from my computer.



```
14… 97.569…  Verizon_51:… Apple_69:44… ARP          60 Who has 192.168.1.168? Tell 192.168.1.1
14… 97.569…  Apple_69:44… Verizon_51:… ARP          42 192.168.1.168 is at 60:30:d4:69:44:c0
```

Submit the assignment4_my_arp.pcap and the screenshot of your ARP message exchange (similar to the example above) for Part A.

Part B Analyze the ARP (85 points)

Your second task is to write a program ``analysis_pcap_arp" that analyzes the pcap trace for the ARP packet. This is similar to your previous assignment, but this time you are not allowed to use any structure. Perform a byte-level programming to read each byte and convert it to the ARP header element---for example, the sender MAC address, target MAC address, protocol type, etc. Refer to the ARP message structure in your book to determine the elements of the ARP message.

Your program does not need to process each packet. Instead, make sure for each packet you can determine if the packet is a ARP packet or not, and if it is an ARP packet then process it further. Based on your analysis, answer the following questions:

(i) Print the entire ARP request and response for **one** ARP packet exchange (preferably the one you show in the screenshot above).

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

Submit your well formatted program, answers to (i) and (ii) and a README that explains how to run your program including details of your program logic for Part B.

Bonus: Capture Gratuitous ARP (10%)

Because ARP packets are over the LAN, every host in the LAN receives the ARP packet. Your task here is to capture gratuitous ARP packets that are not meant for your computer. One easy way to capture this is the following: make sure your computer and a friend's computer is connected to the same LAN. Ask your friend to perform Web browsing and use Wireshark to capture traces on your computer. You should see the ARP packets meant for your friend's computer in your traces. Get a snapshot of these ARP messages (only the ARP request). Make sure you show us that these ARP messages were meant for a different IP address than your own.

For the bonus points, include the snapshot of the ARP messages as well as a short writeup of why you are seeing these messages meant for a different computer.

Submission instruction

As before, you may write your programs in the following languages: Python, Java, and C/C++. If you want to write in any other language, please talk to me.

You need to submit your homework in a single zip file as follows:

- The zip file and (the root folder inside) should be named using your last name, first name, and the assignment number, all separated by a dash ('-') e.g. lastname-firstname-assignment3.zip
- The zip file should contain all submissions for parts A and B and bonus if doing.