EECS 565
Qixiang Liu
04/06/2019

Packet sniffing

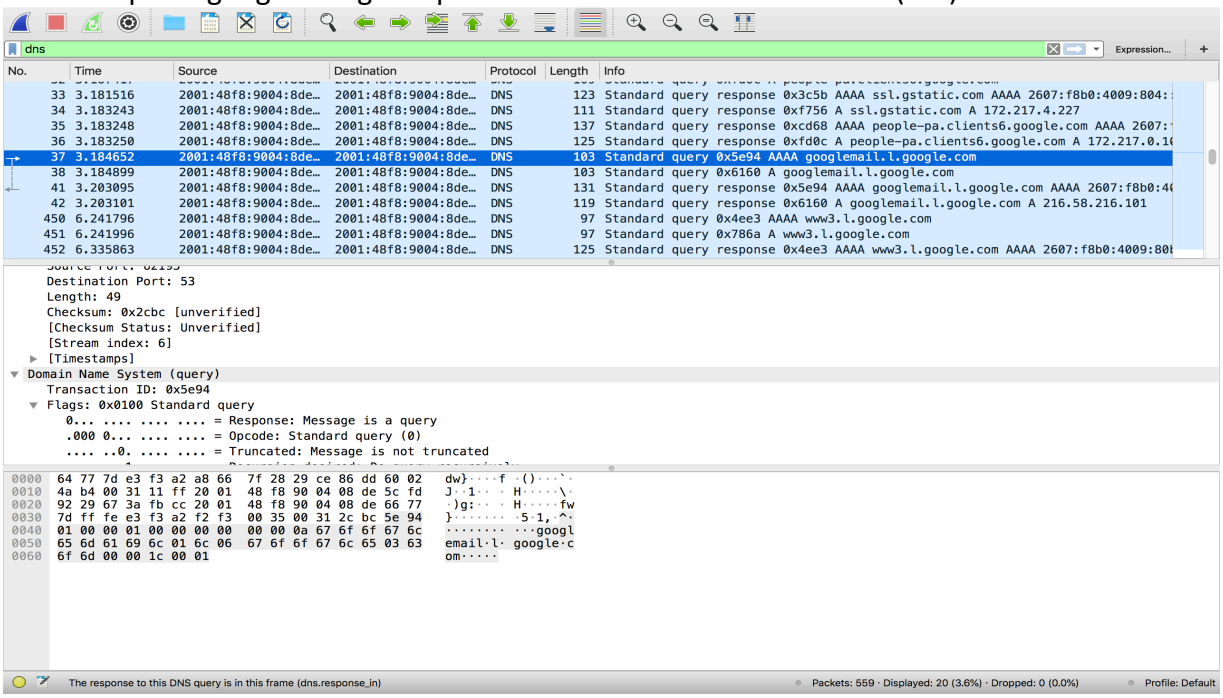
Introduction:

There are two tasks in the project 2. The project works on the wireshark. The goal is to analyze different sniffed packets and data. The first task is about DNS requests and HTTP traffic in my own ip address. The second task is about other devices that are connected to the same WIFI network, excluded my own ip address.

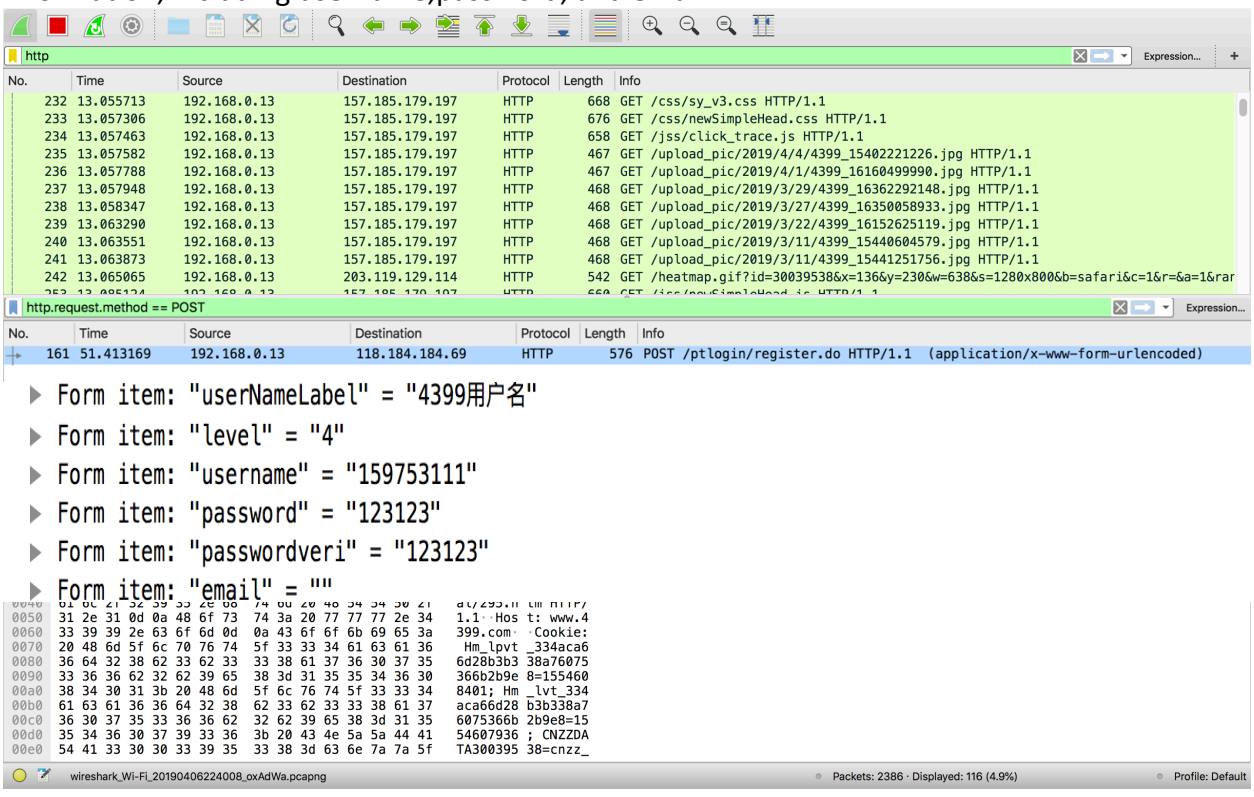
Background:

First, I should know some professional terms.
DNS: The domain name system; In other words, I check websites through domains name, like google.com(8.8.8.8) or youtube.com(199.223.232.0,etc). DNS translate ip addresses to domain names;
HTTP: HyperText Transfer Protocol. The protocol defines how messages are formatted and transmitted and how to deal with commands during response. HTTP is not safe, so communication is not protected between users and browser. HTTPS, 'S' is secure, and it is encoded by TLS and SSL.
TCP/IP: Transmission Control Protocol is complemented the IP. It is reliable to transmit data.
ARP: Address Resolution Protocol achieves physical address of TCP/IP address according to ip address. It can communicate with MAC address. ICMP: Internet Control Message Protocol.
DHCP: Dynamic Host Configuration Protocol is used on UDP/IP networks.
How to use wireshark:
Check local ip: "ipconfig"
Filter interface: "ip src host <ip address>" eg. ip src host 192.168.0.13. or choose WIFI/WLAN interface
Filter more: http.request.method == POST
Result:
192.168.0.13 is my own ipv4 address.
2001…8de… is my own ipv6 address.

Task 1: capture google and gmail packets. Protocol is DNS and HTTPS(TLS)

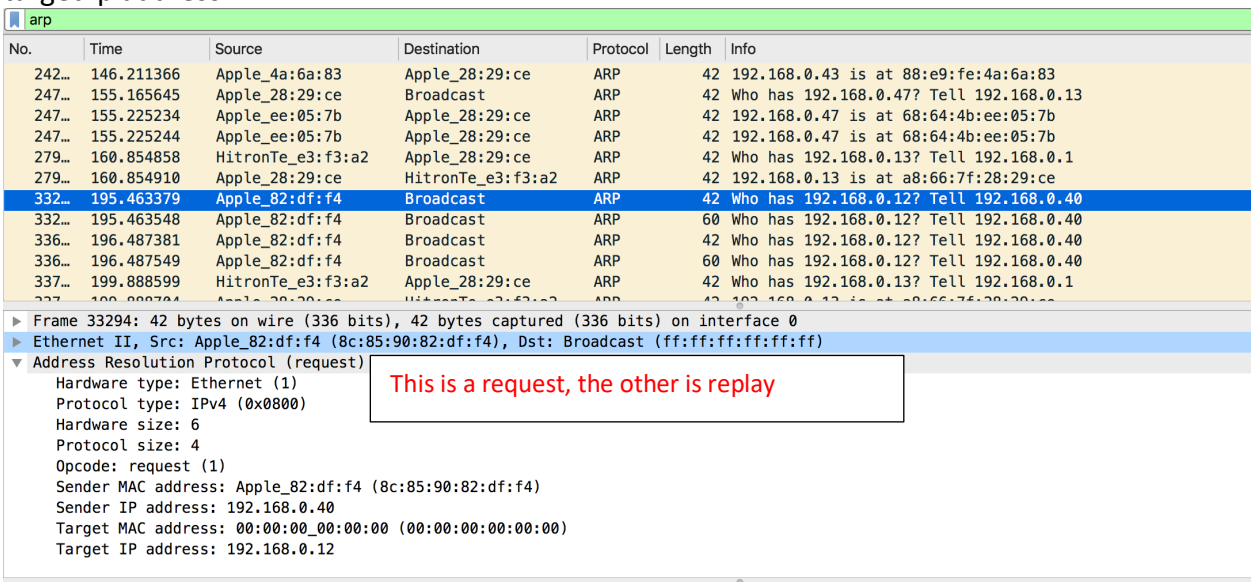


HTTP: www.4399.com is a Chinese game website. I think it is not safe website. The website has many advertisements. In the information tab, GET means get information from the website. When I login the website, I would get POST request from the website. In addition, I got my login information, including username,password, and email.

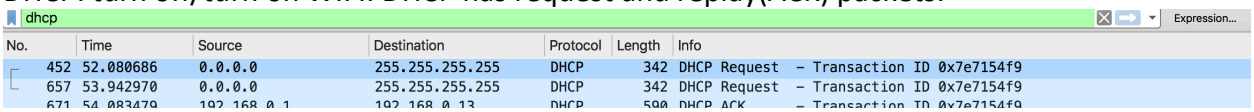


Task 2:

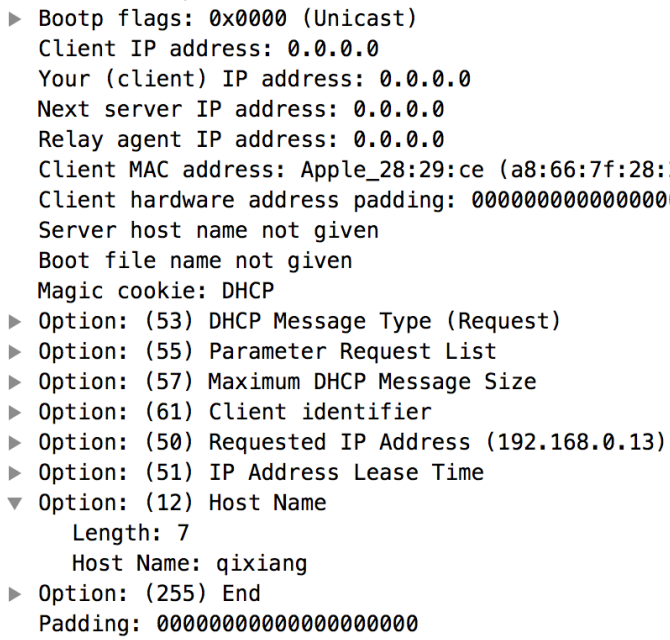
ARP: The host broadcasts the ARP request to all hosts on the network, and receives the return message, determines the physical address of the target IP address, and stores the IP address and hardware address in the local ARP cache, and directly queries the ARP cache on the next request. Although everyone can get the ARP protocol, the protocol can be ignored except target ip address.



DHCP: turn off/turn on WIFI. DHCP has request and replay(ACK) packets.

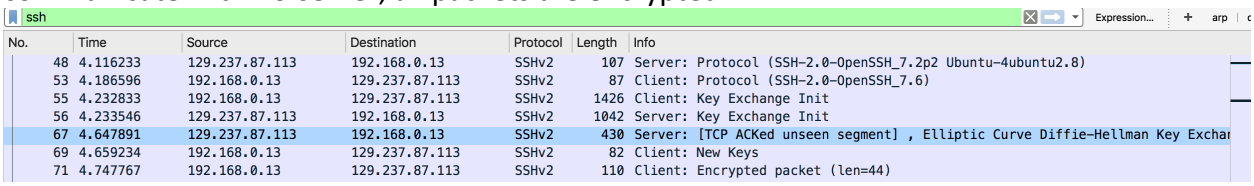


There are two types of DHCP. One is request, the other is ACK.



Host name: my computer's name
IP address: my own IP
MAC address:
There are lots of information about my private content.

SSH protocol: SSH server connection
First of all, I accept a response from KU cycle server to my IP address. The server needs a password to login server. Information displays key exchange and new keys. When I communicate with KU server, all packets are encrypted.



Discussion:

Communication needs to know MAC address on the Internet, so we need ARP translation. DHCP ensures that IP address can only be used by one DHCP client at a time, and it can assign a permanent fixed IP address to the user. DHCP has two other working stages that are DHCP discover and DHCP offer.

Conclusion:

If we are on the same network as others, when we log in to the http protocol website, others will get your account number and password through this method. Therefore, the outside WiFi should not be connected.

Worked Cited:

https://www.youtube.com/watch?v=pBj-7ez1RW0
https://blog.csdn.net/longwang155069/article/details/50107911