**Hadaiq Ahmad**

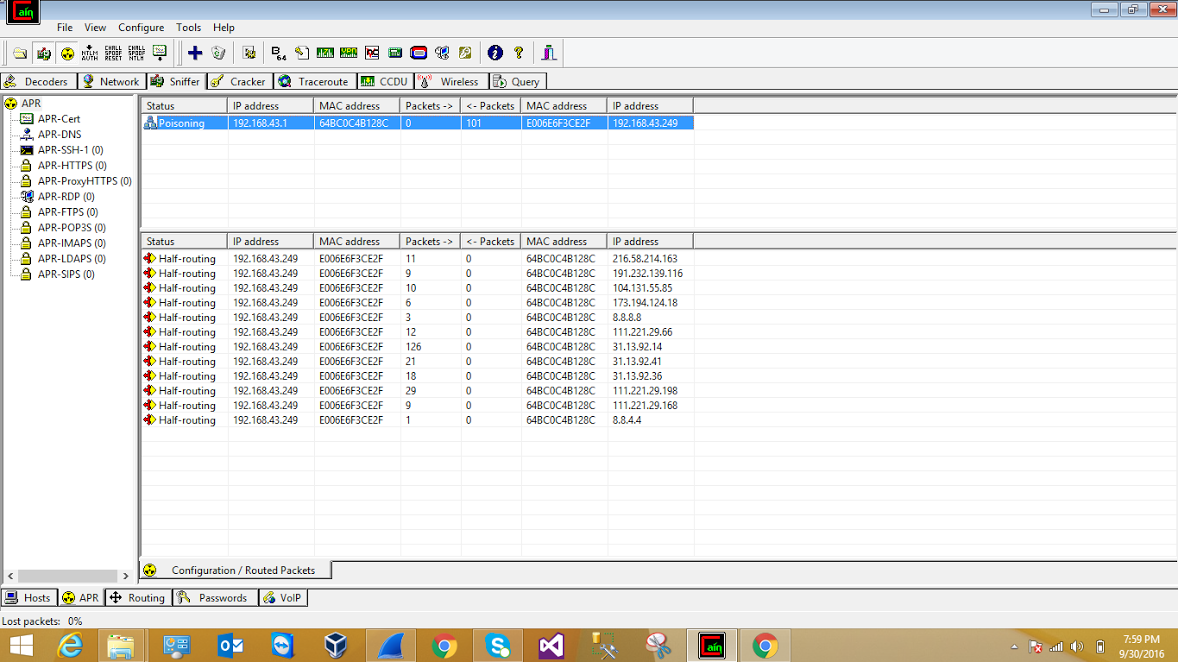
**Cmsid#112807**

**Lab Tasks**

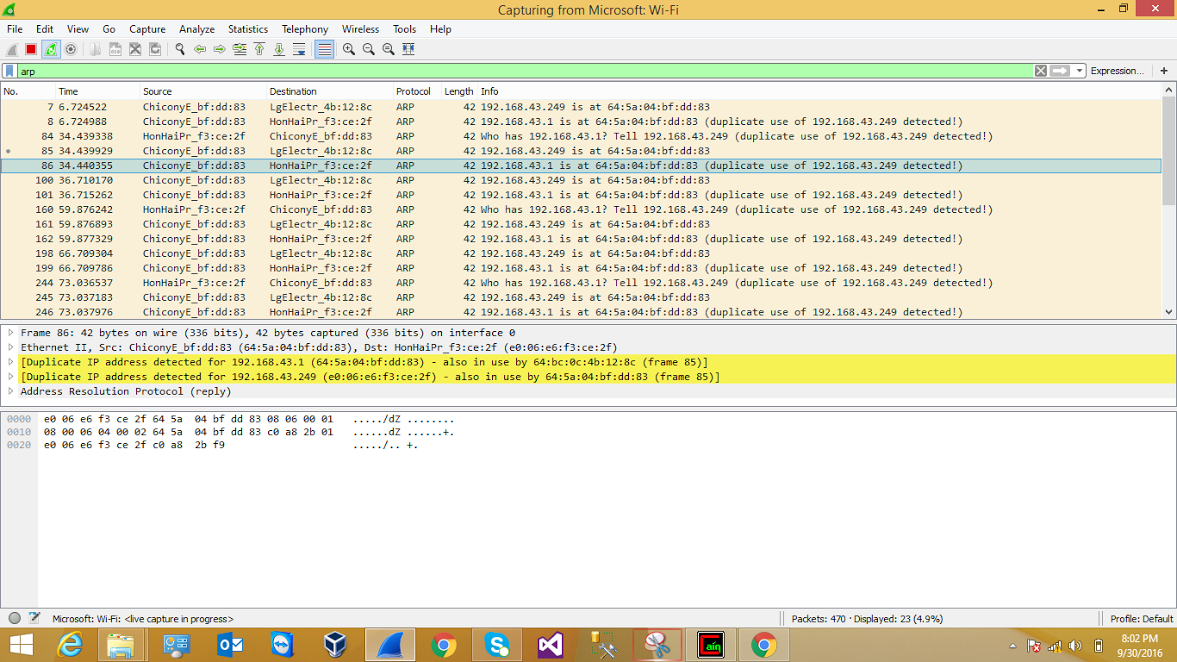
**Task 1:** In your report do three parts presented above:

1. Use **Cain & Abel** for ARP poisoning

In this task I performed ARP posining using a tool called Cain and abel. I downloaded the installation file first of all and installed the program. Then I looked for the ip addresses of communicating victims. Then I followed the given instructions in lab manual to completely accomplish the task. Screenshots of important steps are given below.



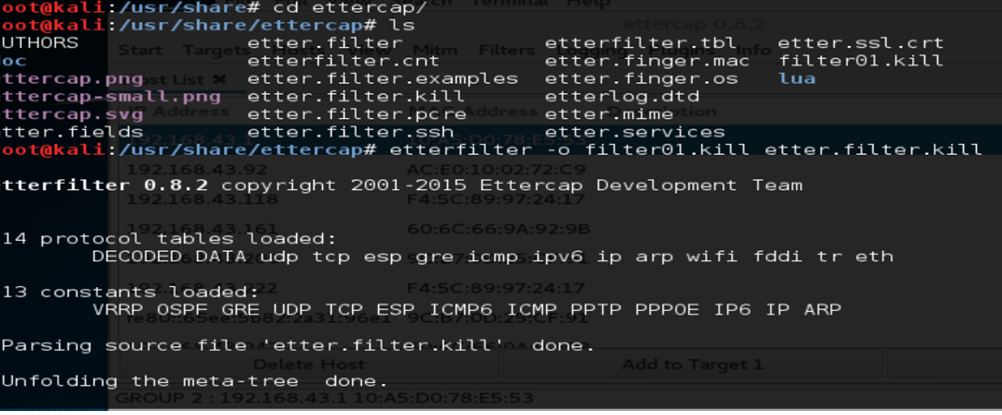
Wireshark step



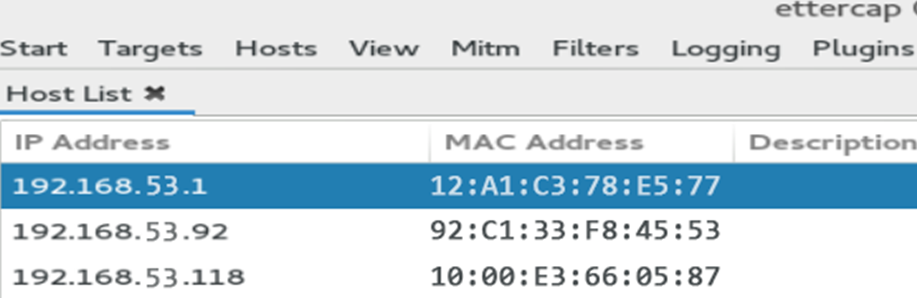
1. Use **Ettercap** to launch MITM with a filter that prevents sending any packet.

In part b I used Ettercap to launch MITM (man in the middle) attack. To use Ettercap I installed Kali linux using virtual machine. Then after installing Kali Linux I installed Ettercap through the tutorial shown in user manual. I also installed an Ettercap filter through shell that actually allowed me to accomplish the task. All these steps were shown in the tutorial. I used two computers to perform this task and a hotspot because I was unable to perform the task on NUST wifi connection. Screenshots are given below

1st step

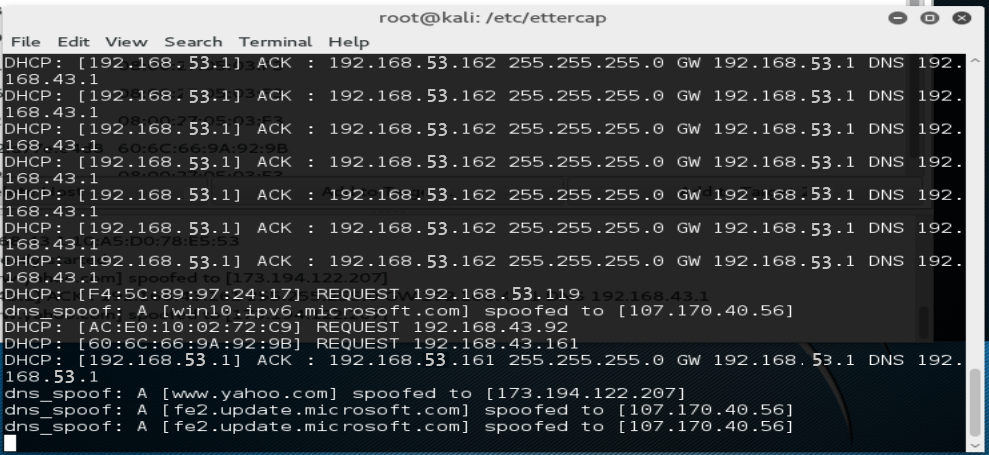


2nd step

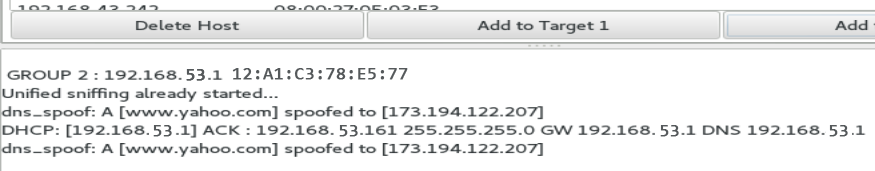


1. Use **Ettercap** for DNS-spoofing

In this task I again used Ettercap but this time for DNS spoofing. When the victim opens yahoo.com he/she will be redirected to google.com This is again done by using Ettercap filters. I modified etter.DNS file in this task which translated the host name of yahoo.com to google.com then again I followed few steps from the previous task and then finally used a plugin to that loaded the file we modified to launch the attack.



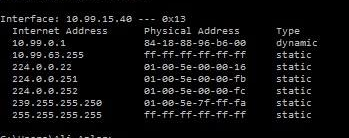
**Screesnhort2**



**Task 2:** As discussed in the report, “Hard Coding the ARP Cache” is an option in Windows-based-host to prevent against ARP Cache poisoning. Justify your answer how it affects ARP Poisoning, comparing both the results along with the screenshots (Dynamic and Static ARP Tables).

With ARP poisoning we can examine and monitor the network traffic of different hosts. We can do this in number of ways but commonly we use few different intrusion detection systems like Snort, it can also be done using xARP. But it has some limitations like this is easy for single host because there are less nodes in the network but for the complex networks it is difficult to manage the network because of more no. of nodes

**Screenshort**



**Deliverable:**

Students are required to upload the complete report on LMS before the deadline.