PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641004
Department of Applied Mathematics and Computational Sciences

20XC46 COMPUTER NETWORKS LAB

&

20XW46 COMPUTER NETWORKS AND TCP/IP LAB

Wireshark Lab-ARP

Objective

To see how ARP (Address Resolution Protocol) works. ARP is an essential glue protocol that is used to join Ethernet and IP.

Requirements

Wireshark: This lab uses the Wireshark software tool to capture and examine a packet trace. A packet trace is a record of traffic at a location on the network, as if a snapshot was taken of all the bits that passed across a particular wire. The packet trace records a timestamp for each packet, along with the bits that make up the packet, from the lower-layer headers to the higher-layer contents. Wireshark runs on most operating systems, including Windows, Mac and Linux. It provides a graphical UI that shows the sequence of packets and the meaning of the bits when interpreted as protocol headers and data. It color-codes packets by their type, and has various ways to filter and analyze packets to let you investigate the behavior of network protocols. Wireshark is widely used to troubleshoot networks. You can download it from www.wireshark.org if it is not already installed on your computer.

arp: This lab uses the "`arp`" command-line utility to inspect and clear the cache used by the ARP protocol on your computer. `arp` is installed as part of the operating system on Windows, Linux, and Mac computers, but uses different arguments. It requires administrator privileges to clear the cache.

ifconfig / ipconfig: This lab uses the "`ipconfig`" (Windows) command-line utility to inspect the state of your computer's network interface. `ipconfig` is installed as part of the operating system on Windows computers.

route / netstat: This lab uses the "`route`" or "`netstat`" command-line utility to inspect the routes used by your computer. A key route is the default route (or route to prefix 0.0.0.0) that uses the default gateway to reach remote parts of the Internet. Both "`route`" and "`netstat`" are installed as part of the operating system across Windows and Mac/Linux, but there are many variations on the command-line parameters that must be used.

Browser: This lab uses a web browser to find or fetch pages as a workload. Any web browser will do.

Network Setup

We want to observe the ARP protocol in action. ARP is used to find the Ethernet address that corresponds to a local IP address to which your computer wants to send a packet. A typical example of a local IP address is that of the local router or default gateway that connects your computer to the rest of the Internet. Your computer caches these translations in an ARP cache so that the ARP protocol need only be used occasionally to do the translation. The setup from the viewpoint of your computer is as shown in the example below.

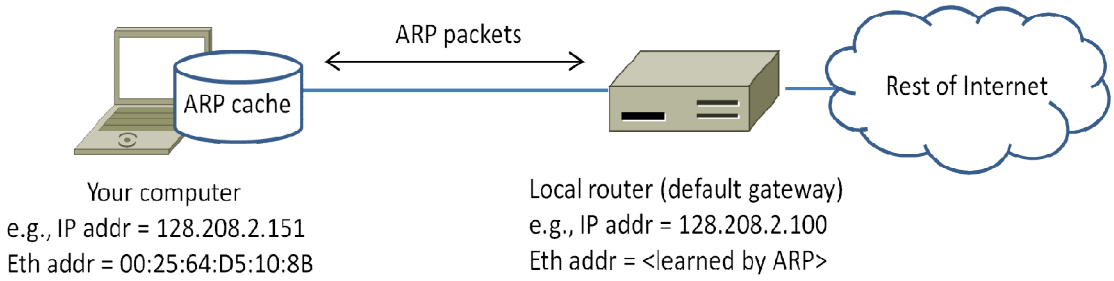


Figure 1: Network setup under which we will study ARP in second part

How ARP Works

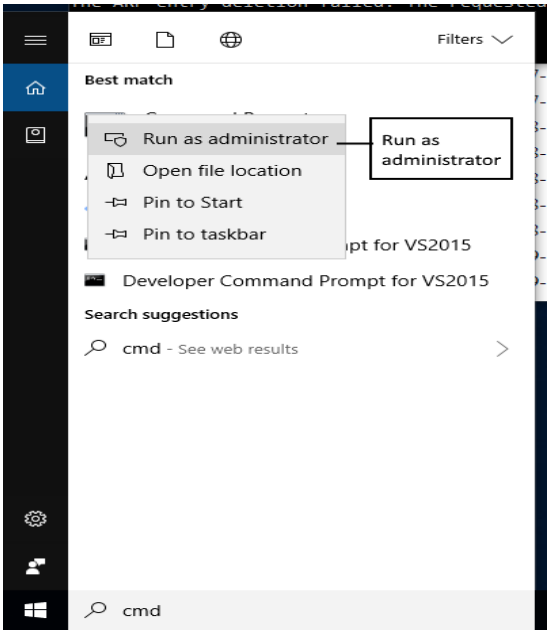
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

There is a Reverse ARP (RARP) for host machines that don't know their IP address. RARP enables them to request their IP address from the gateway's ARP cache.

Step 1: Finding your IP address and Gateway address

1. Open a command prompt as an administrator as follows:



2. *Find the **Ethernet** address of the main network interface OR the **wireless** address (see figure 3) of your computer with the* `ipconfig` *command*. You will want to know this address for later analysis. On Windows, bring up a command-line shell and type "`ipconfig /all`". Among the output will be a section for the main interface of the computer (likely an Ethernet interface) and its Ethernet address. Common names for the interface are "eth0" or "Ethernet adapter". An example is shown below in figure 2, with added highlighting.

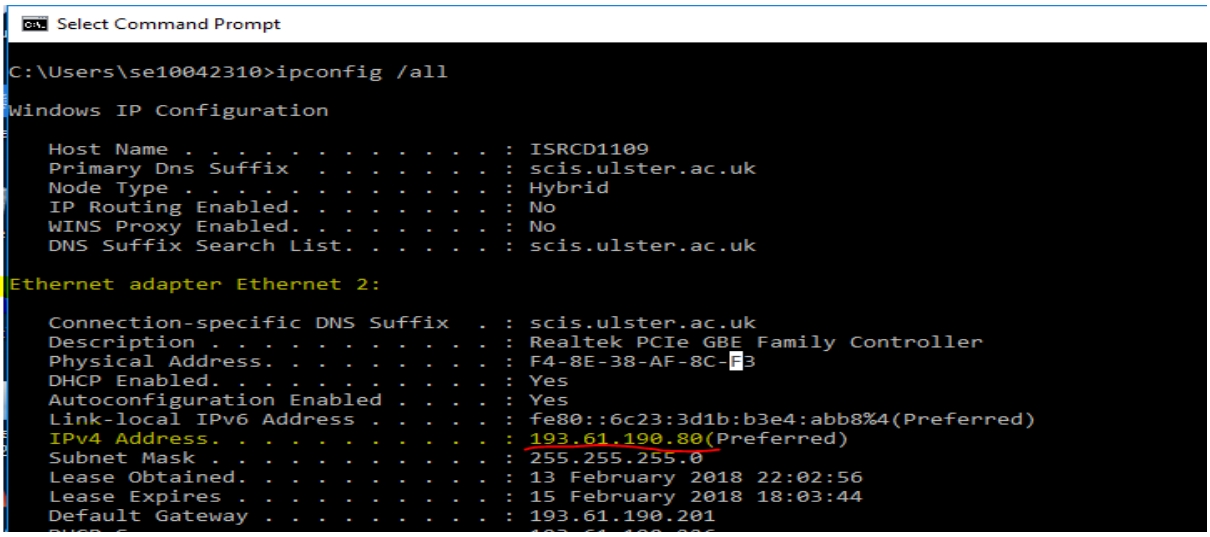


Figure 2: Finding the computer's Ethernet address with `ipconfig` (Windows)

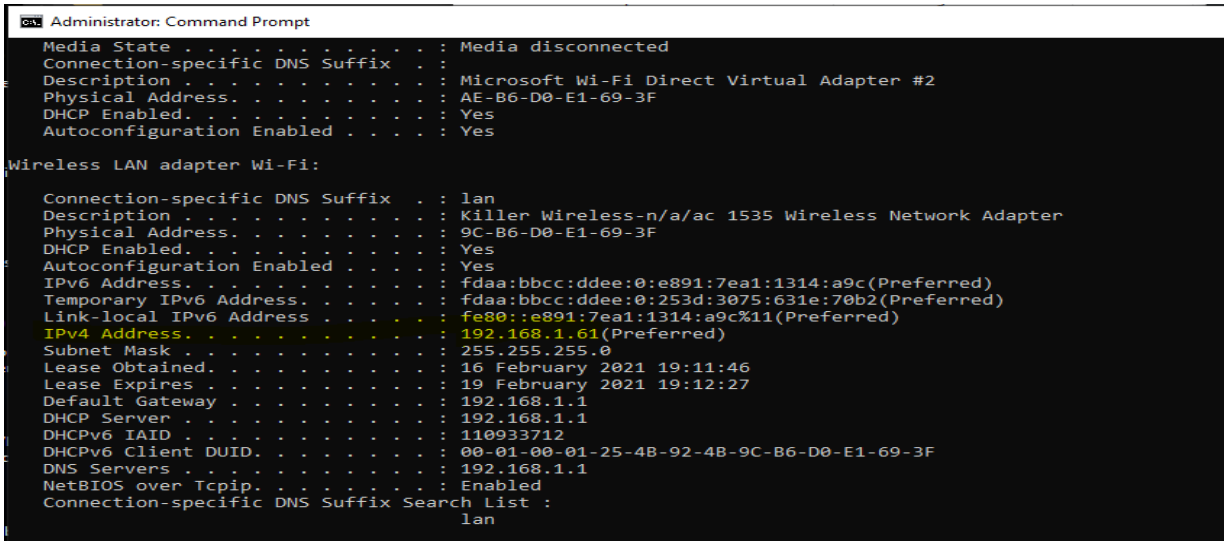


Figure 3: Finding the computer's WiFi IP address with ipconfig (Windows)

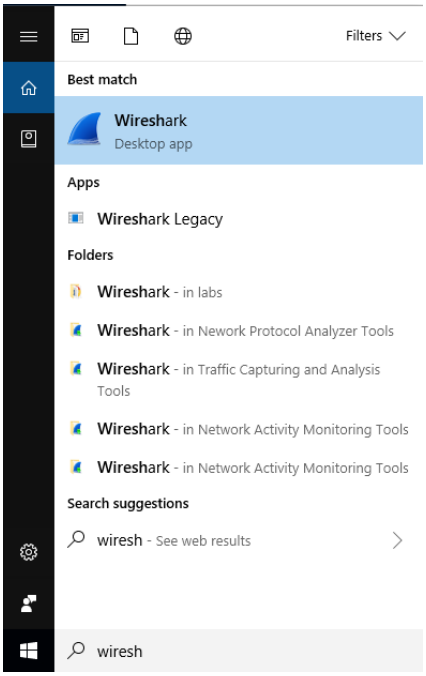
3. *Find the IP address of the local router or default gateway that your computer uses to reach the rest of the Internet using the* `netstat` / `route` *command.* You should be able to use the `netstat` -r command on Windows.

   Alternatively, you can use the route command ("`route print`" on Windows). In either case you are looking for the gateway IP address that corresponds to the destination of default or 0.0.0.0. An example is shown in figure 3 for `netstat`, with added highlighting.

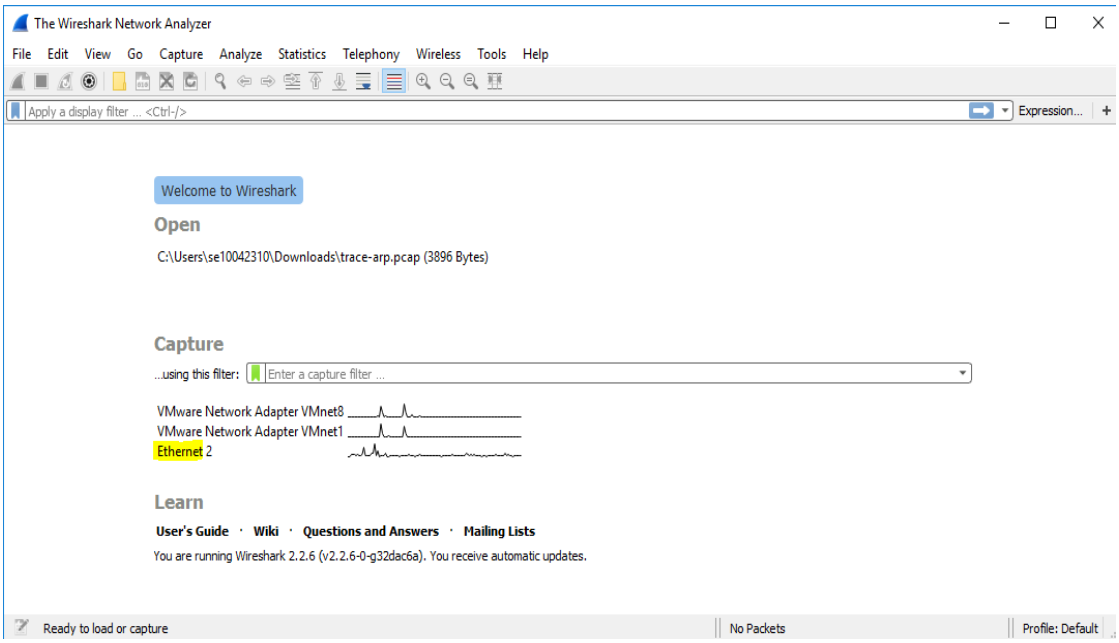
```
C:\Users\se10042310>netstat -r
===========================================================================
Interface List
  4...f4 8e 38 af 8c f3 ......Realtek PCIe GBE Family Controller
  3...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  6...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   193.61.190.201    193.61.190.80     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.139.0    255.255.255.0         On-link     192.168.139.1    291
    192.168.139.1  255.255.255.255         On-link     192.168.139.1    291
  192.168.139.255  255.255.255.255         On-link     192.168.139.1    291
    192.168.159.0    255.255.255.0         On-link     192.168.159.1    291
    192.168.159.1  255.255.255.255         On-link     192.168.159.1    291
  192.168.159.255  255.255.255.255         On-link     192.168.159.1    291
```

Figure 4: Finding the default gateway IP address with `netstat` (Windows)

4. Now **run Wireshark** by typing "*wireshark*" in the bottom left search box in Windows



5. You should see the main Wireshark interface. **Click on the Ethernet OR Wireless interface** to start traffic analysis on that interface.



6. *Add a filter of* "`arp`". Your capture window should be like the one pictured below.

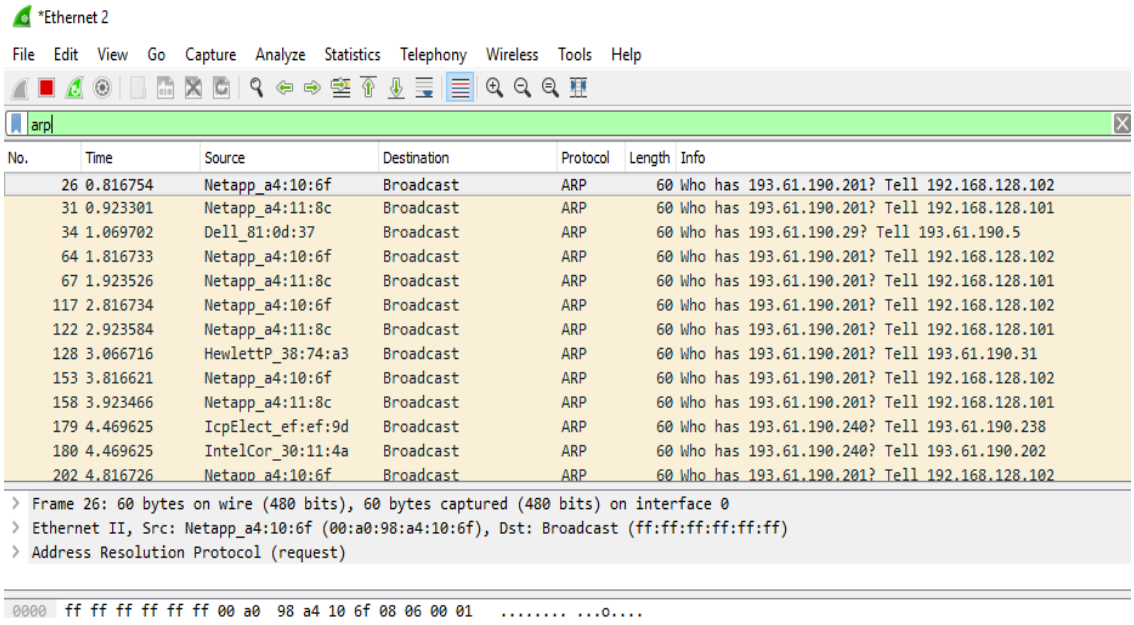
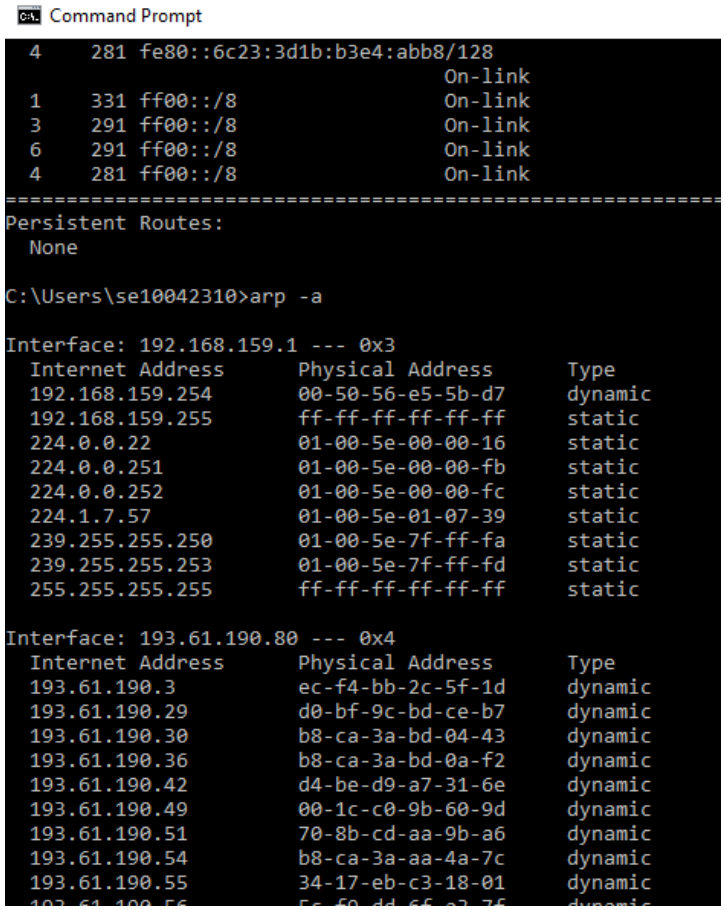


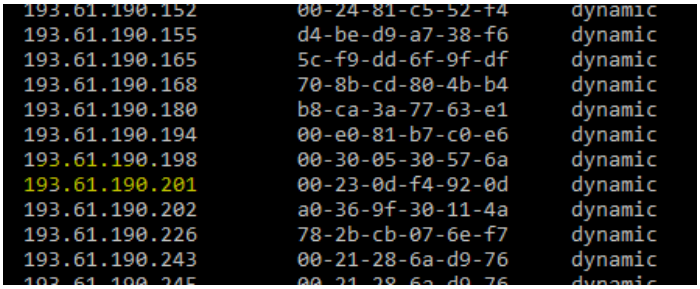
Figure 6: Setting up the capture options

7. *When the capture is started, use the "`arp`" command to clear the default gateway from the ARP cache.* Using the command "`arp -a`" will show you the contents of the ARP cache as a check that you can run "`arp`".

   Go to command prompt and type **arp -a** as shown below.



You should see an entry for the IP address of the default gateway as shown in image below. In this case it is 193.61.190.201 which is the default gateway on my office PC.



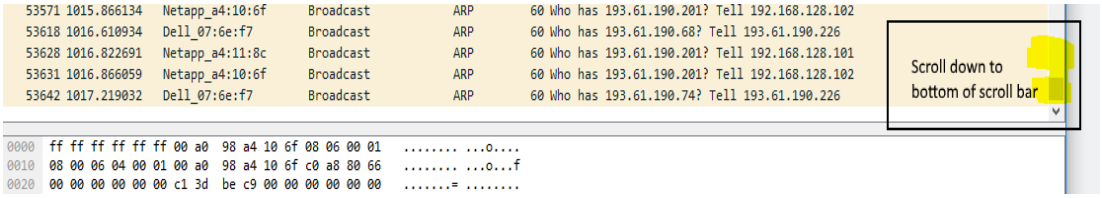
8. To clear this entry, use the arp command with different arguments ("`arp –d`" on Windows) as follows. Type **arp -d** in the command prompt.

```
C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>
```

Note: This usage of `arp` will need administrator privileges to run, so you have to run as a privileged user on Windows which is what you should have done in step 1. The command should run without error, but the ARP entry may not appear to be cleared if you check with "`arp –a`". This is because your computer will send ARP packets to repopulate this entry as soon as you need to send a packet to a remote IP address, and that can happen very quickly due to background activity on the computer.

9. *Now that you have cleared your ARP cache,* ***fetch a remote page with your Web browser***. This will cause ARP to find the Ethernet address of the default gateway so that the packets can be sent.

10. You will see these packets flowing through your computer by scrolling down in the Wireshark window to the bottom as shown below.



11. These ARP packets will be captured by Wireshark. You might clear the ARP cache and fetch a document a couple of times. Hopefully there will also be other ARP packets sent by other computers on the local network that will be captured. These packets are likely to be present if there are other computers on your local network. In fact, if you have a busy computer and extensive local network then you may capture many ARP packets. The ARP traffic of other computers will be captured when the ARP packets are sent to the broadcast address, since in this case they are destined for all computers including the one on which you are running Wireshark. Because ARP activity happens slowly, you may need to wait up to 30 seconds to observe some of this background ARP traffic.

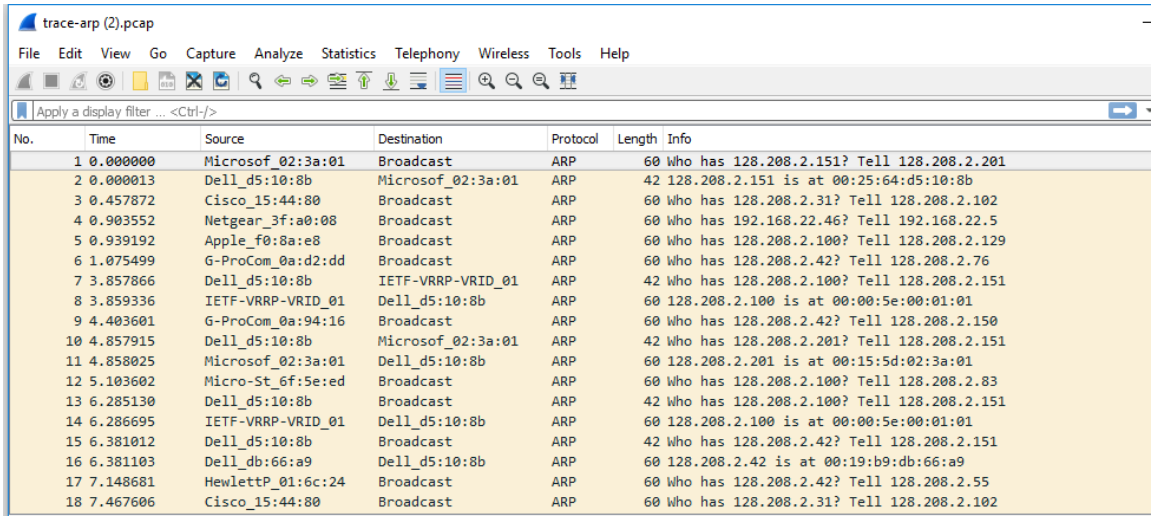
12. *Once you have captured some ARP traffic, stop the capture.* You will need the trace, plus the Ethernet address of your computer and the IP address of the default gateway for the next steps.

Step 2: Inspect the supplied ARP Trace

1. **Close** Wireshark.

2. Once Wireshark is closed, **open** the ARP trace here:

   You should see a screen as shown below.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Microsof_02:3a:01	Broadcast	ARP	60	Who has 128.208.2.151? Tell 128.208.2.201
2	0.000013	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	128.208.2.151 is at 00:25:64:d5:10:8b
3	0.457872	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102
4	0.903552	Netgear_3f:a0:08	Broadcast	ARP	60	Who has 192.168.22.46? Tell 192.168.22.5
5	0.939192	Apple_f0:8a:e8	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.129
6	1.075499	G-ProCom_0a:d2:dd	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.76
7	3.857866	Dell_d5:10:8b	IETF-VRRP-VRID_01	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
8	3.859336	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
9	4.403601	G-ProCom_0a:94:16	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.150
10	4.857915	Dell_d5:10:8b	Microsof_02:3a:01	ARP	42	Who has 128.208.2.201? Tell 128.208.2.151
11	4.858025	Microsof_02:3a:01	Dell_d5:10:8b	ARP	60	128.208.2.201 is at 00:15:5d:02:3a:01
12	5.103602	Micro-St_6f:5e:ed	Broadcast	ARP	60	Who has 128.208.2.100? Tell 128.208.2.83
13	6.285130	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.100? Tell 128.208.2.151
14	6.286695	IETF-VRRP-VRID_01	Dell_d5:10:8b	ARP	60	128.208.2.100 is at 00:00:5e:00:01:01
15	6.381012	Dell_d5:10:8b	Broadcast	ARP	42	Who has 128.208.2.42? Tell 128.208.2.151
16	6.381103	Dell_db:66:a9	Dell_d5:10:8b	ARP	60	128.208.2.42 is at 00:19:b9:db:66:a9
17	7.148681	HewlettP_01:6c:24	Broadcast	ARP	60	Who has 128.208.2.42? Tell 128.208.2.55
18	7.467606	Cisco_15:44:80	Broadcast	ARP	60	Who has 128.208.2.31? Tell 128.208.2.102

   The setup from the viewpoint of your computer from this trace is shown in the example below.

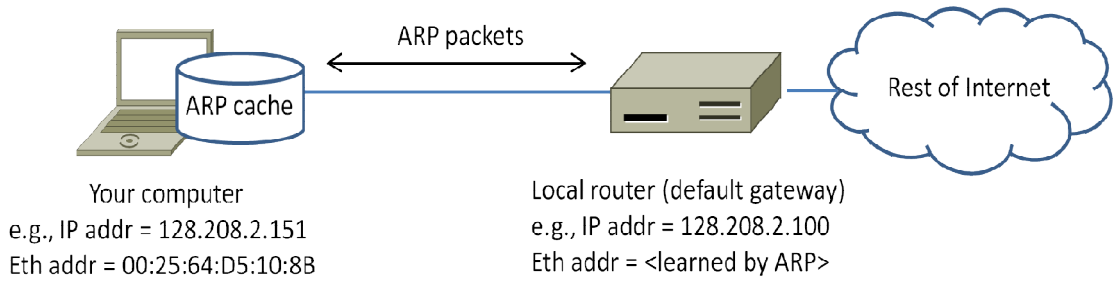


Figure 7: Network setup under which we will study ARP in this part

Note: **Ethernet address** of computer: 00:25:64:d5:10:8b and IP address of **gateway**: 128.208.2.100

3. Now we can look at an ARP exchange. Since there may be many ARP packets in your trace, we'll first narrow our view to only the ARP packets that are sent directly from or to your computer.

   Set a display filter for packets with the Ethernet address of your computer which is this case is ***00:25:64:d5:10:8b.***

You can do this by entering an expression in the blank "Filter:" box near the top of the Wireshark window and clicking "Apply" or Enter. After applying this filter your capture should look something like the figure below, in which we have expanded the ARP protocol details.

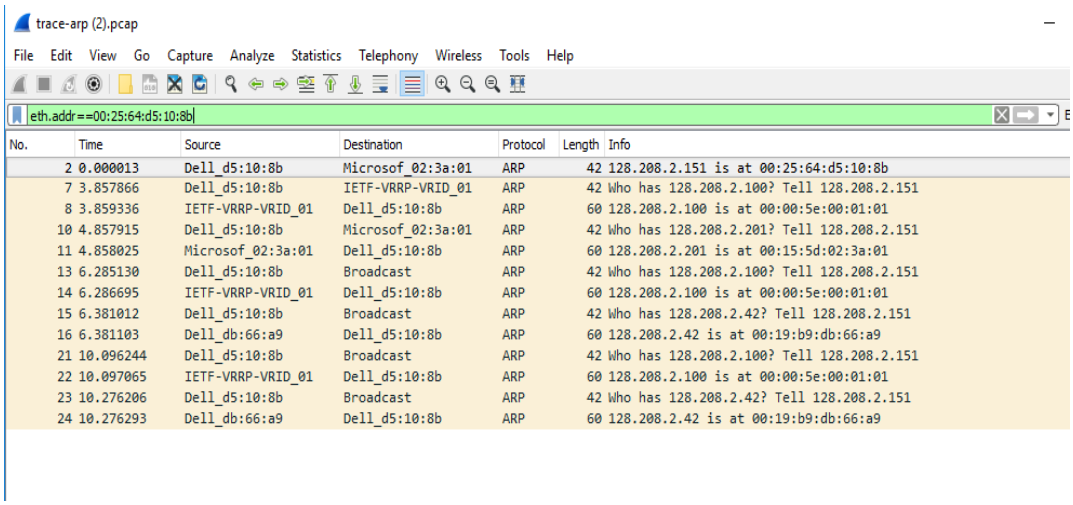


Figure 8: Capture of ARP packets, showing details of a request

Find and select an ARP request for the default gateway and examine its fields. There are two kinds of ARP packets, a request and a reply, and we will look at each one in turn. The Info line for the request will start with "Who has …". You want to look for one of these packets that asks for the MAC address of the default gateway, e.g., "Who has xx.xx.xx.xx …" where xx.xx.xx.xx is your default gateway. You can click on the + expander or icon for the Address Resolution Protocol block to view the fields:

- Hardware and Protocol type are set to constants that tell us the hardware is Ethernet and the protocol is IP. This matches the ARP translation from IP to Ethernet address.

- Hardware and Protocol size are set to 6 and 4, respectively. These are the sizes of Ethernet and IP addresses in bytes.

- The opcode field tells us that this is a request.

- Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP. These fields are filled in as much as possible. For a request, the sender knows their MAC and IP address and fills them in. The sender also knows the target IP address – it is the IP address for which an Ethernet address is wanted. But the sender does not know the target MAC address, so it does not fill it in.

Next, select an ARP reply and examine its fields. The reply will answer a request and have an Info line of the form "xx.xx.xx.xx is at yy:yy:yy:yy:yy:yy":

- The Hardware and Protocol type and sizes are as set as before.

- The opcode field has a different value that tells us that this is a reply.

- Next come the four key fields, the sender MAC (Ethernet) and IP and the target MAC (Ethernet) and IP just as before. These fields are reversed from the corresponding request, since the old target is the new sender (and vice versa). The fields should now be all filled in since both computers have supplied their addresses.

Step 3: Details of ARP over Ethernet

ARP packets are carried in Ethernet frames, and the values of the Ethernet header fields are chosen to support ARP. For instance, you may wonder how an ARP request packet is delivered to the target computer so that it can reply and tell the requestor its MAC address. The answer is that the ARP request is (normally) broadcast at the Ethernet layer so that it is received by all computers on the local network including the target. Look specifically at the destination Ethernet address of a request: it is set to ff:ff:ff:ff:ff:ff, the broadcast address. So, the target receives the request and recognizes that it is the intended recipient of the message; other computers that receive the request know that it is not meant for them. Only the target responds with a reply. However, anyone who receives an ARP packet can learn a mapping from it: the sender MAC and sender IP pair. The ARP header for a request and a reply is 28 bytes for both the request and reply for IPv4.

(Please note that answers on next page to following 5 questions)

To look at further details of ARP, examine an ARP request and ARP reply to answer these questions:

1. *What opcode is used to indicate a request? What about a reply?*
2. *What value is carried on a request for the unknown target MAC address?*
3. *What Ethernet Type value which indicates that ARP is the higher layer protocol?*
4. *Is the ARP reply broadcast (like the ARP request) or not?*

Answers to Step 3: ARP request and reply

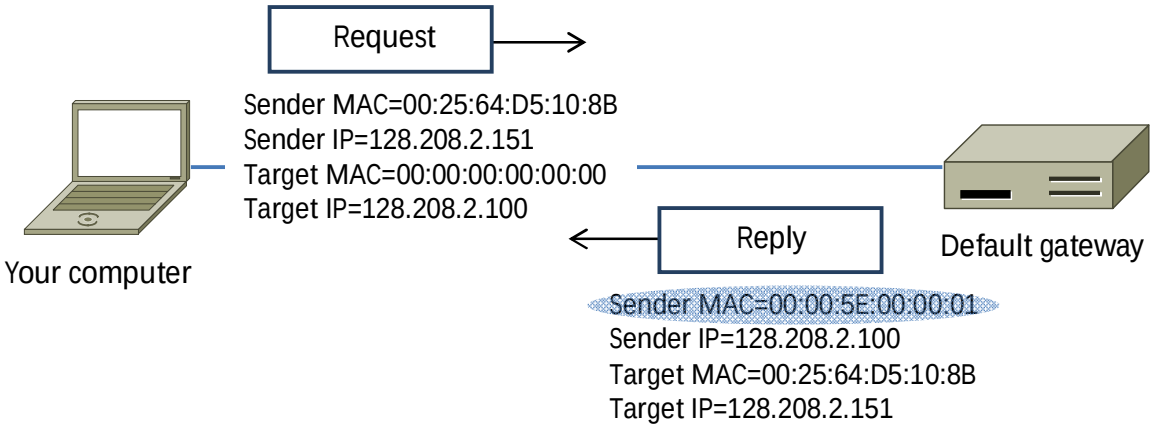


Figure 9: Details of the ARP request and reply to resolve the default gateway

There are several features to note:

- On the request, the target MAC is not known so it is usually filled in as 00:00:00:00:00:00.
- On the reply, the request target becomes the reply sender and vice versa.
- On the reply, the sender MAC returns the answer that is sought; it is highlighted.
- All of the fields that are shown are ARP header fields

Lab Exercise – Snooping on other trafficin

Lab through ARP Poison Attack

Objective - To demonstrate a Man in the middle (MITM) hack with the Ettercap tool. Ettercap is a multipurpose sniffer/interceptor/logger for switched LAN, and pretty much the Swiss army knife of ARP poisoning. Every security researcher should include it in his toolbox. It is included in Backtrack

– the popular Linux distribution. Ettercap features a GUI and a command line *text mode* tool.

1. Download Ettercap
2. Follow the instructions to install it. See figure below.

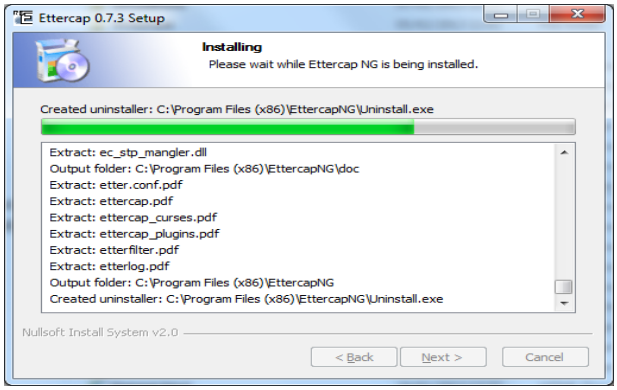


Figure 1: Ettercap installation in progress

3. Go to “Ask me anything” search box in bottom left of Windows Desktop and type "ettercap". You should see it appear as in the following figure.

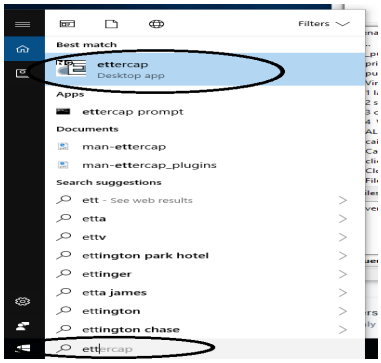


Figure 2: Running Ettercap in Lab

4. Next select *Unified Sniffing* from the *Sniff* menu option as show in figure 3.

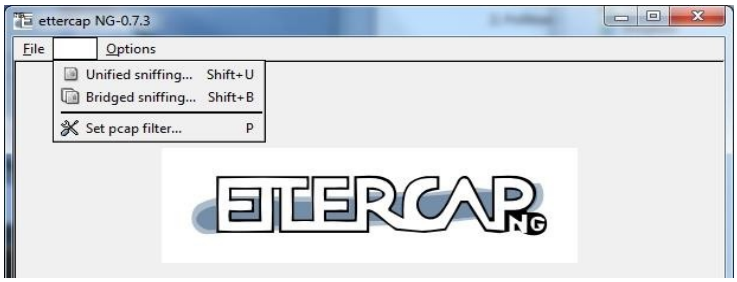


Figure 3: Step 1 in process of snooping

5. Select the *Ethernet Connection* network interface (see figure 4).

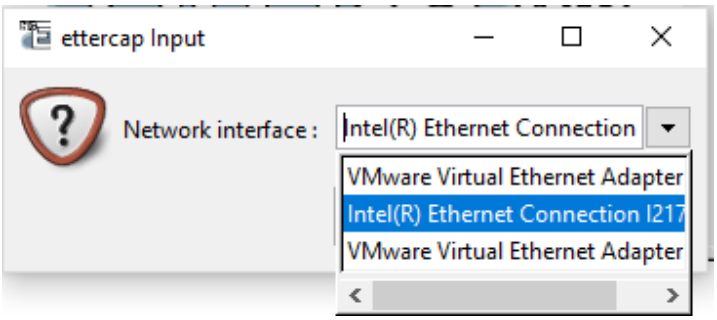


Figure 4: Selection of network interface

1. Next you should be presented with a series of menu options including Start, Targets, Hosts, View Mitm, Filters, Logging and Plugins. You should select the *Hosts* option and choose *Scan for Hosts.* See figure 5.

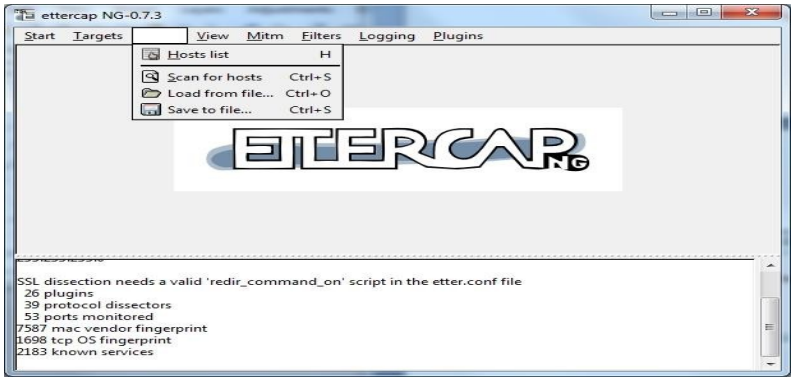


Figure 5: Selection of hosts to scan on LAN

2. Once you select *Scan for hosts*, you should see a pop up window displaying the progress when all 255 hosts on the local network are scanned. See figure 6.

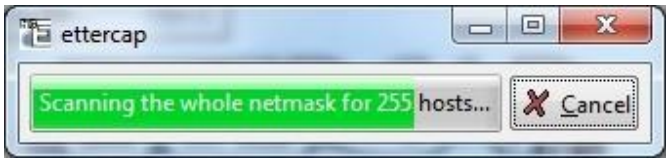


Figure 6: Hosts being scanned locally

3. Next you should select *Hosts List* from the Hosts menu. You should then see a screen similar to figure 7 with a list of hosts that have been found.

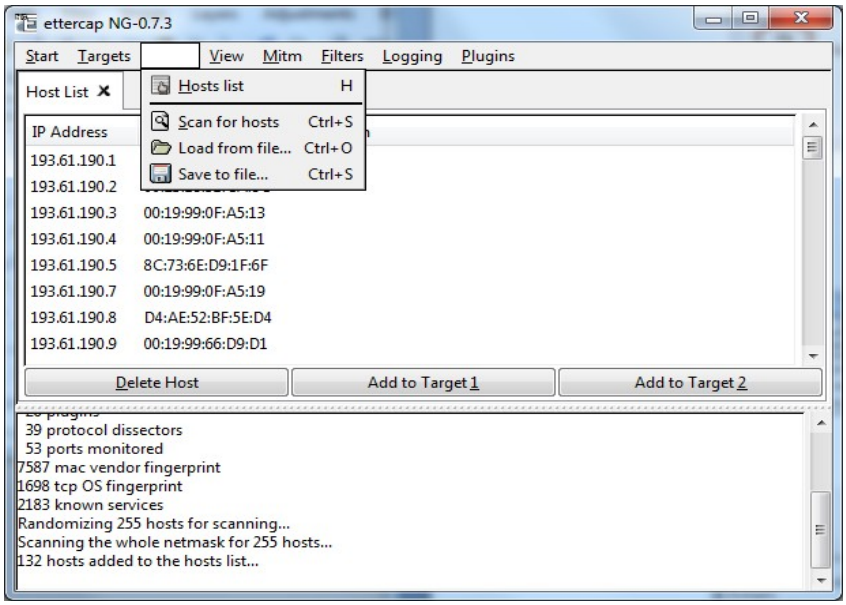


Figure 7: Hosts that were scanned locally

4. ***Please ask permission from a colleague to allow you to select their computer to be scanned. They should confirm their IP address to you.*** That can be found as in previous weeks by typing *cmd* in the windows start menu and opening a command prompt. Then in the command prompt, type *ipconfig* and note the ipv4 address displayed. You may need to scroll up to see it in the command prompt window. Here in figure 8, host 193.61.190.73 is being selected for scanning.

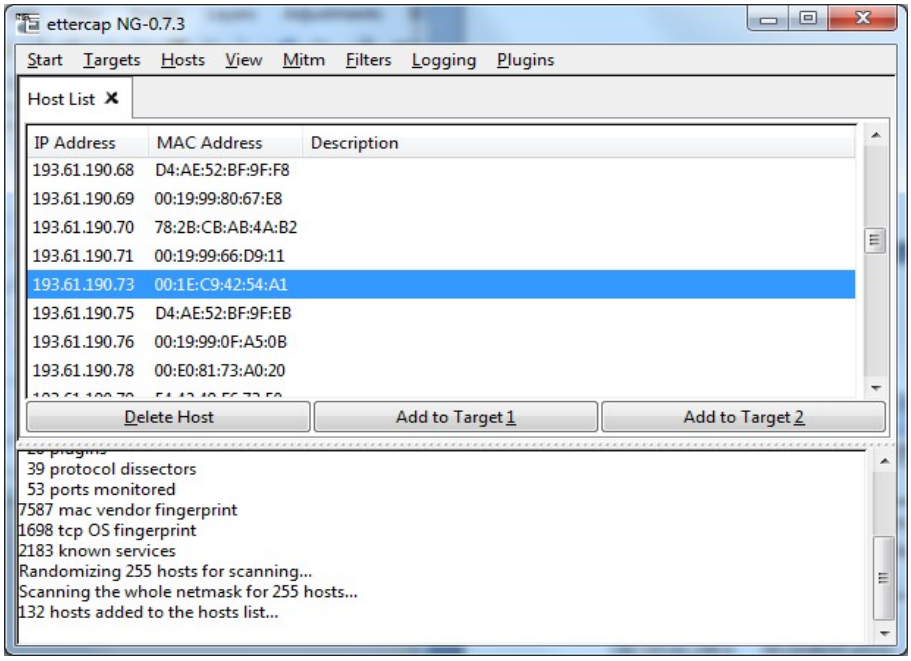


Figure 8: host 193.61.190.73 is being selected for scanning

5. Once you have the target selected with your mouse, then select the *Add to Target 1* button. See figure 9.

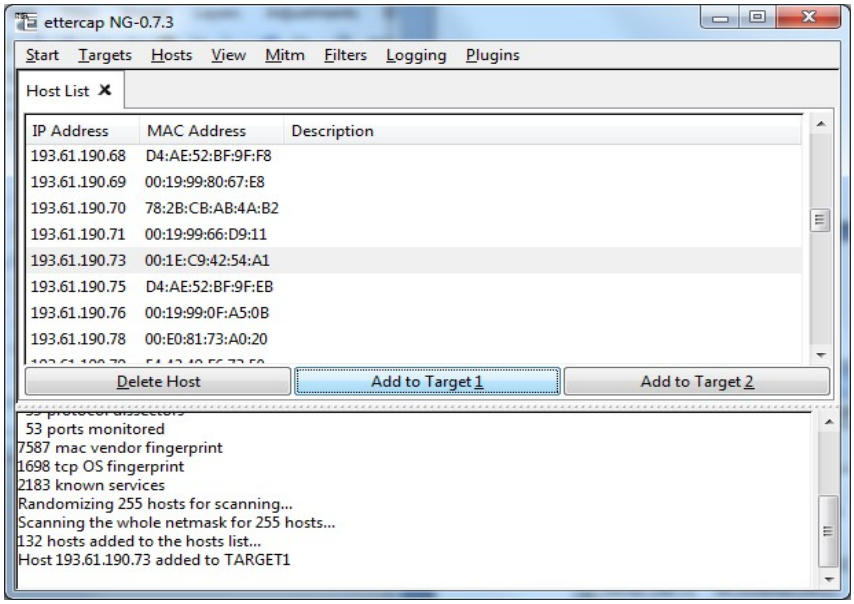


Figure 9: host 193.61.190.73 is being added to Target 1.

6. Select the *Targets* menu option and then select C*urrent Targets* as shown in figure 10.

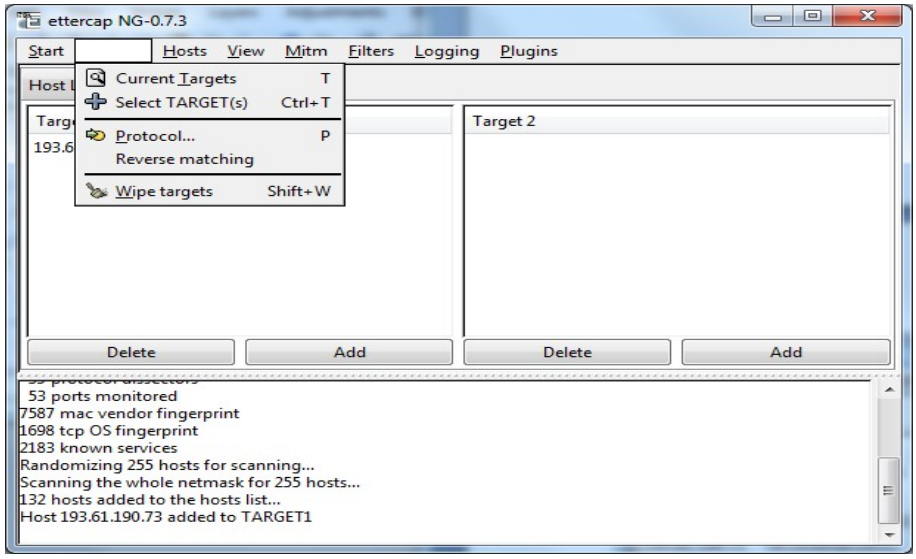


Figure 10: Targets being selected

7. Now you should only see your class mates computer shown as in figure 11.

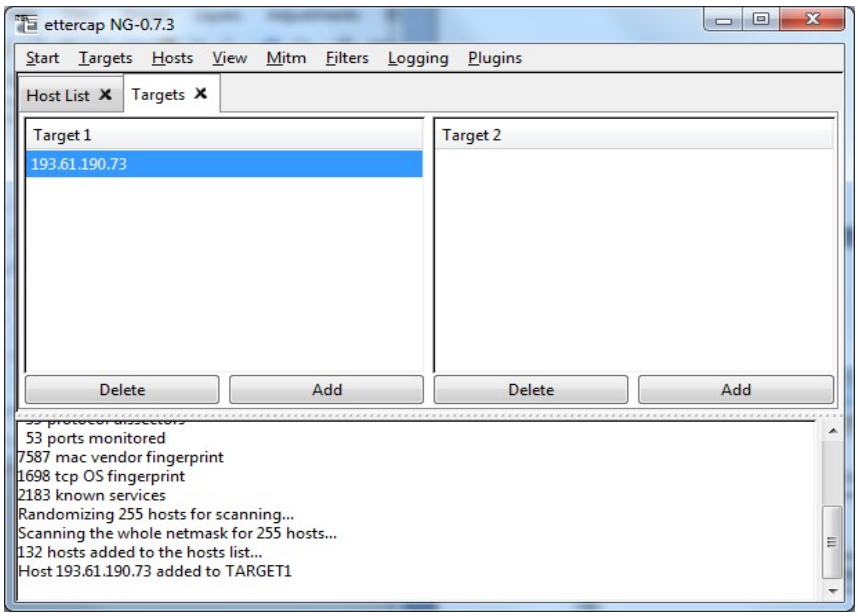


Figure 11: host selected for attack

8. Now go to the *mitm* option as show in figure 12. Select *Arp poisoning.*

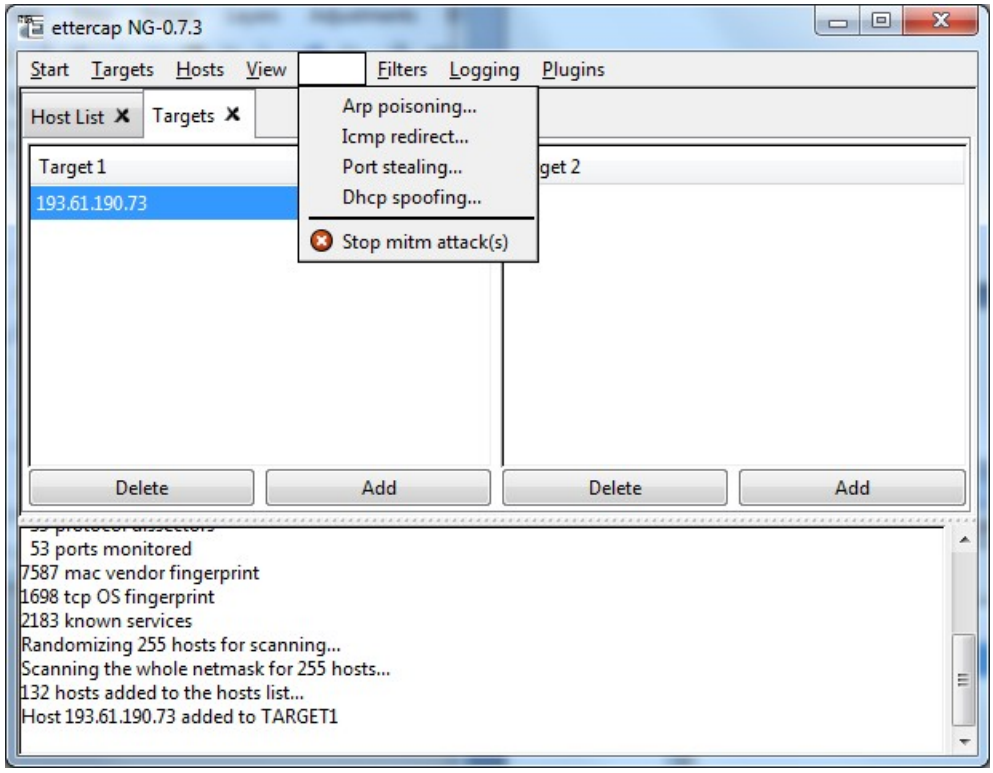


Figure 12: ARP Poisoning selection

9. Once *Arp poisoning* is selected, you will be presented with the dialogue window as shown in figure 13. Simply click *OK.*

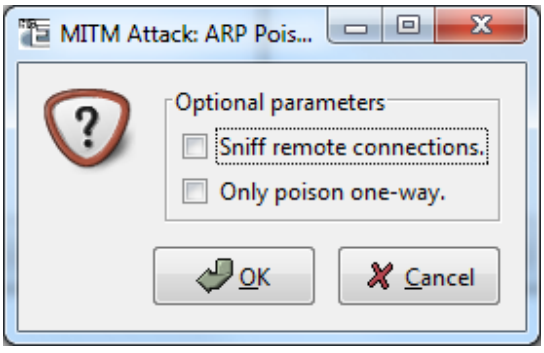


Figure 13: Options for ARP poison attack

10. You will then be presented with a window once again which is similar to figure 14. The ARP poison attack however is happening underneath. You now have access to all the traffic which is being routed to the IP address which you have entered earlier. We will now move to Wireshark to see the power of an ARP poison mitm attack.

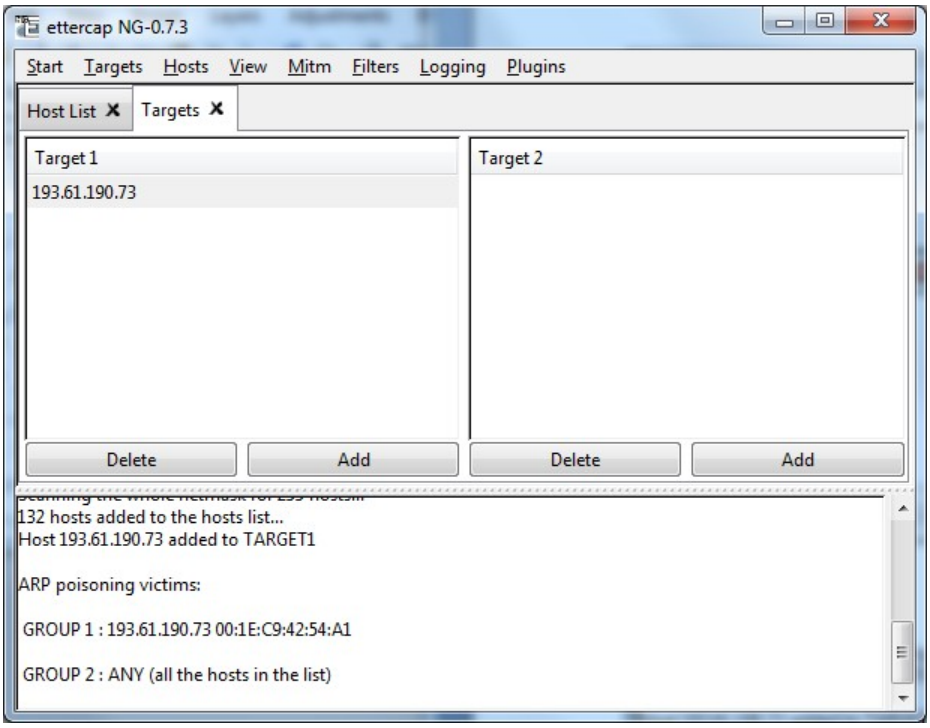


Figure 14: Main window after attack has been started

11. Open Wireshark by typing wireshark at the run programs option. You will then select the usual Xtreme Gigabit Interface and *Start* a capture. In the display filter, type the following: *ip.src==yourfriendsipaddress && tcp.port==80 e.g. ip.src==193.61.191.88 && tcp.port==80.* See figure 15.

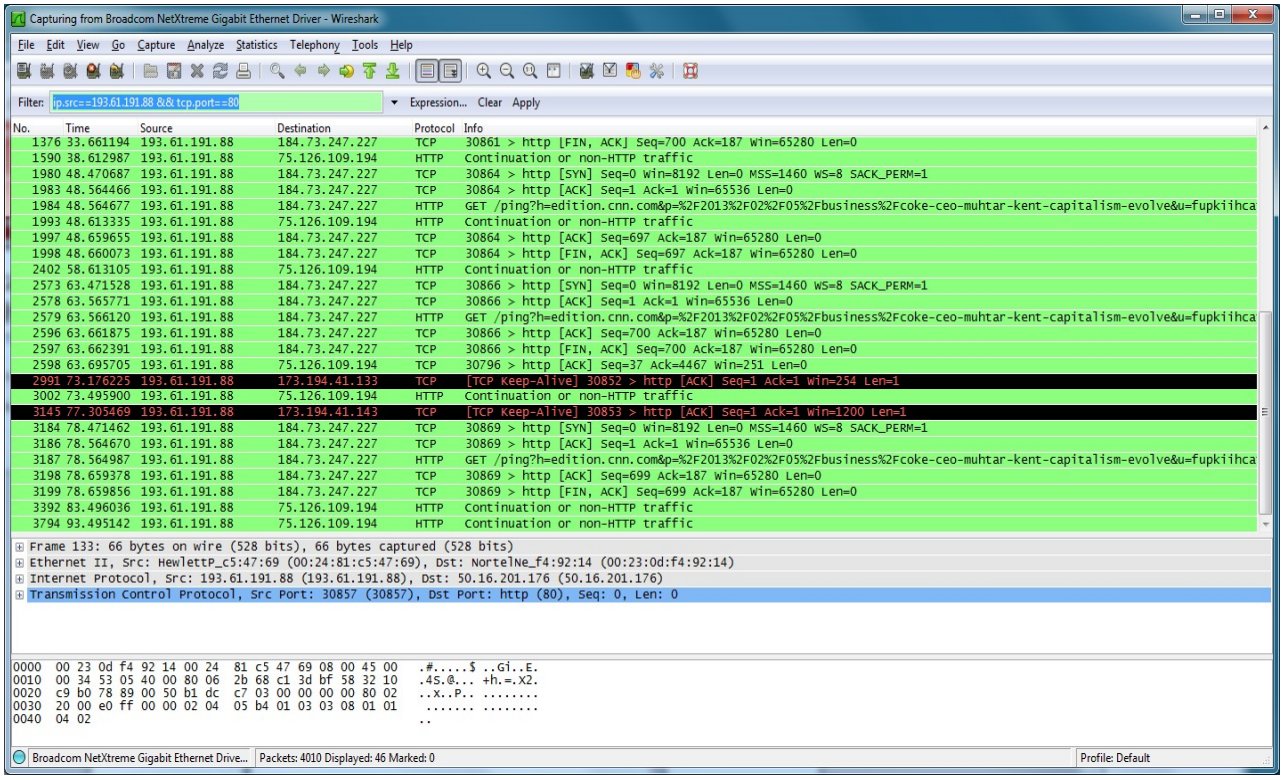


Figure 15: Sample scan of web traffic on IP address 193.61.191.88

12. Get your friend to browse to any site. In this example below, I have gone to a CNN page which discusses Coca-Cola remarks from the CEO. It is at http://edition.cnn.com/2013/02/05/business/coke-ceo-muhtar-kent-capitalism-evolve/

Figure 16: Sample page surfed.

13. Once your friend has started to surf, you should start to see a lot of HTTP and TCP packets appear in your packet list window. After some time you can stop the capture. You may also choose to stop the mitm attack. You can always resume the attack to see 'fresh' traffic remotely. You should then select the page that he surfed through e.g. CNN and right click on it as displayed below and select *Follow TCP Stream.*

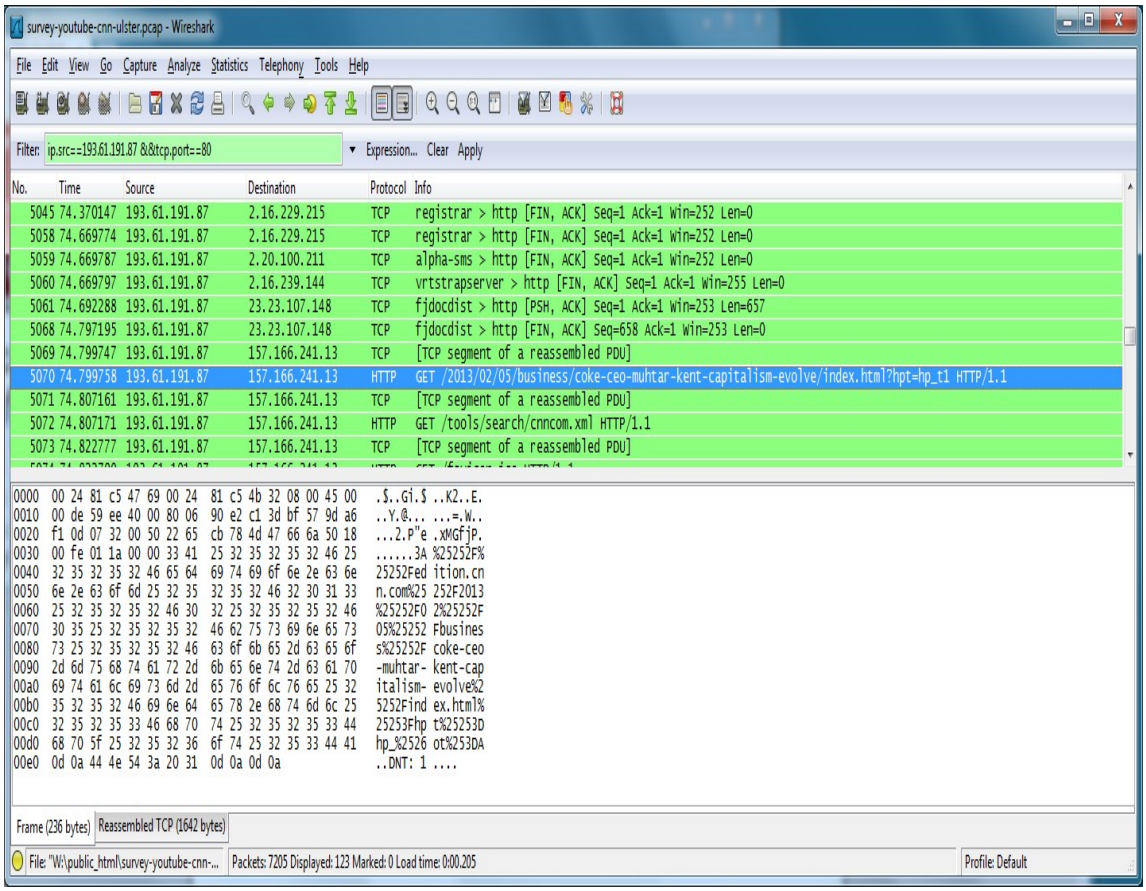


Figure 17: Sample page from CNN being selected in the Wireshark interface. Note the ip address and port filtering

14. The TCP Follow Stream should lead you to a window such as displayed below. Note the contents of the GET and HOST on the first two lines. When we put them together we get the location of the site visited which is edition.cnn.com/2013/02/05/business/coke-ceo-muhtar-kent- capital-ism-evolve/. This should now show you that all surfing can be snooped on a LAN.

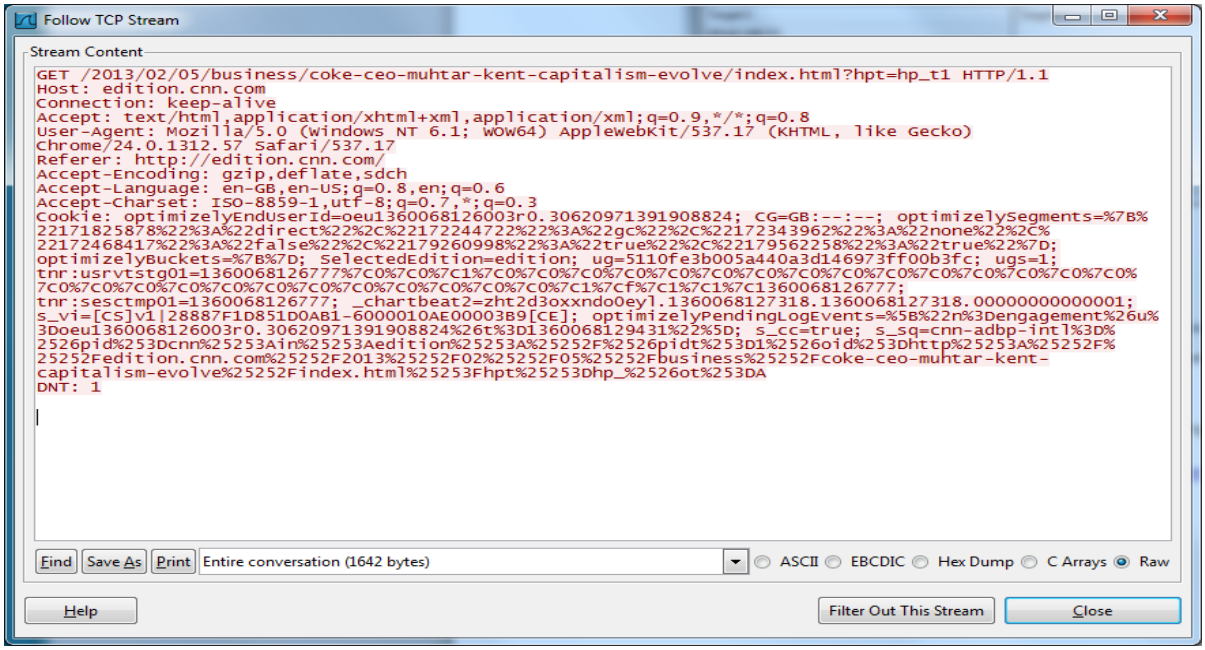


Figure 18: CNN page after selecting *Follow TCP Stream*

20. Now get your friend to go to a site which requires a login. Try for instance signing up for a free account on Survey Monkey at https://www.surveymonkey.com/MyAccount Join.aspx

21. Repeat the steps above. Look for a post and then in examining the stream, you should find the username and password sent to the remote site.

22. Finally, please return to the ettercap program and select *Mitm* and click on *Stop mitm attack(s).*
    This will ensure that the ARP tables return to normal and no unnecessary snooping of a new-comer to your friend's machine takes place. See figure 19.

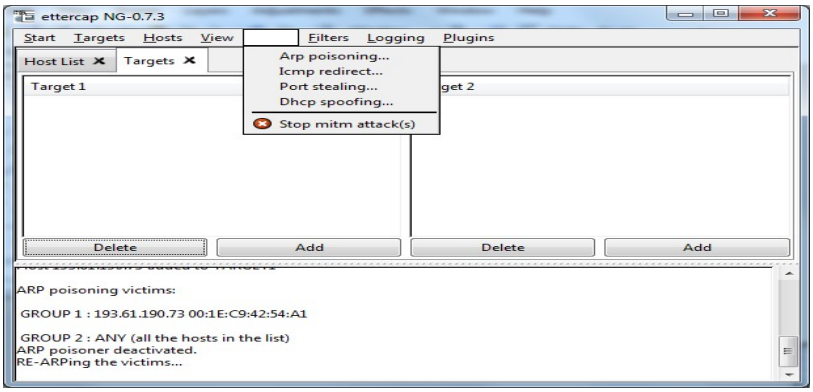


Figure 19: Stopping the man in the middle ARP attack

23. The following popup windows should confirm that all man in the middle attacks have stopped.People are now safe again in the lab.

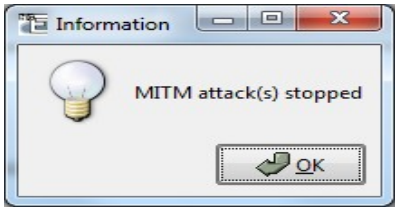


Figure 20: Confirmation of mitm attack being stopped.

24. Finally, you can exit the program.

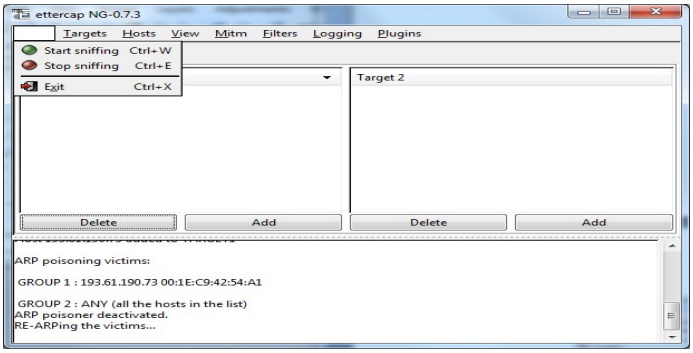


Figure 21: Ensuring you exit the attack vector program