ARP Spoofing Tutorial

(the hard way)

The idea behind ARP spoofing is to trick a target computers ARP cache causing it to send all the traffic through an attacking machine before returning back to the target computer. Sniffing the network activity with wireshark while the attack is in progress allows you to view all the information and content that the target computer is viewing. (i.e. passwords, account information, visited sites, etc.) I suggest you read up on ARP spoofing more before continuing on with this manual method of ARP spoofing.

This link gives a nice explanation on ARP, what it is and what it is used for.

http://www.oxid.it/downloads/apr-intro.swf

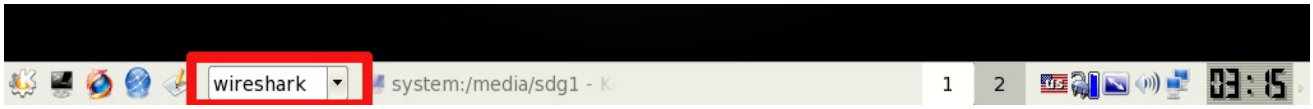
This entire tutorial is ran in Backtrack2 stable release. It is available for download for free from following link.

http://www.remote-exploit.org/backtrack_download_old.html

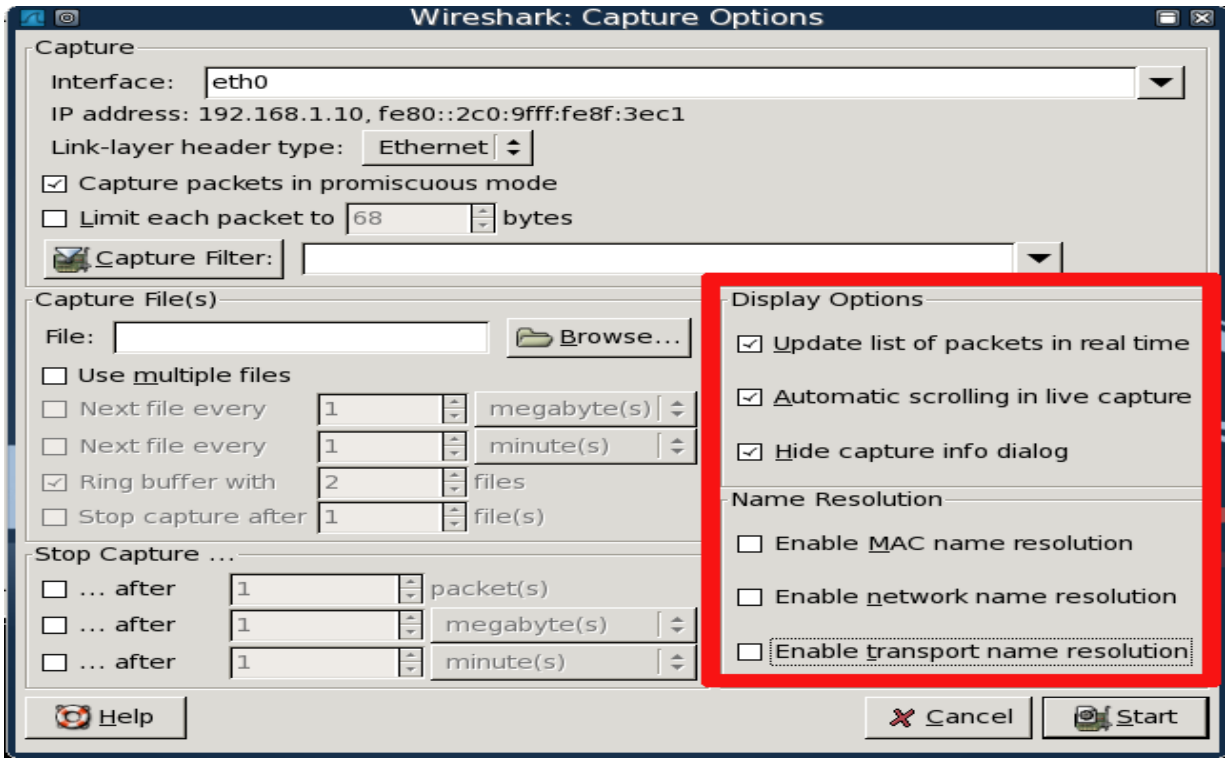
Getting an ARP reply packet:

The first step would be to capture a simple ARP reply packet to use as a template in creating a spoofed ARP reply packet that we will be sending to the target computer.

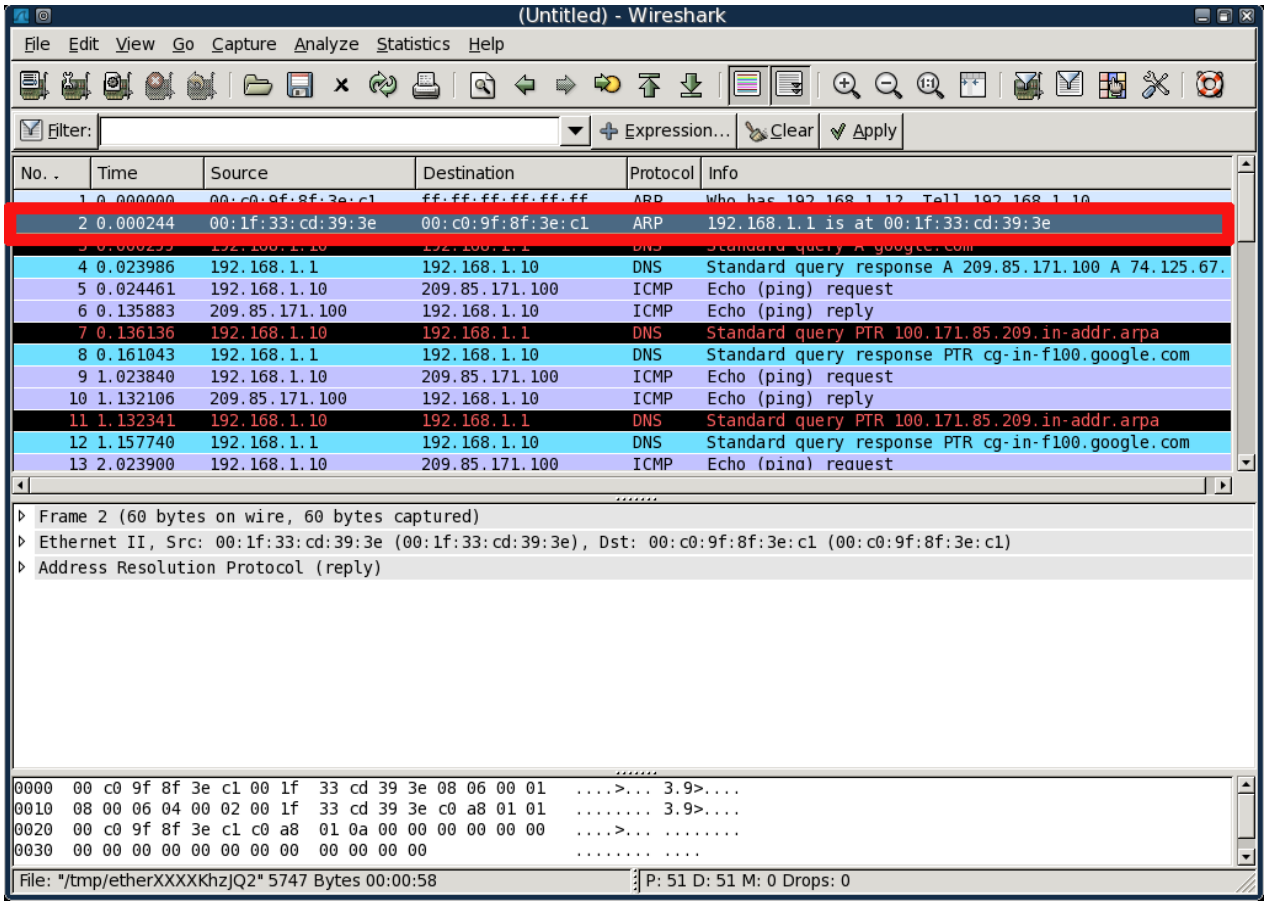
1- **A-** Open wireshark and start sniffing. To do this in Backtrack2 simply type "wireshark," into the run box.



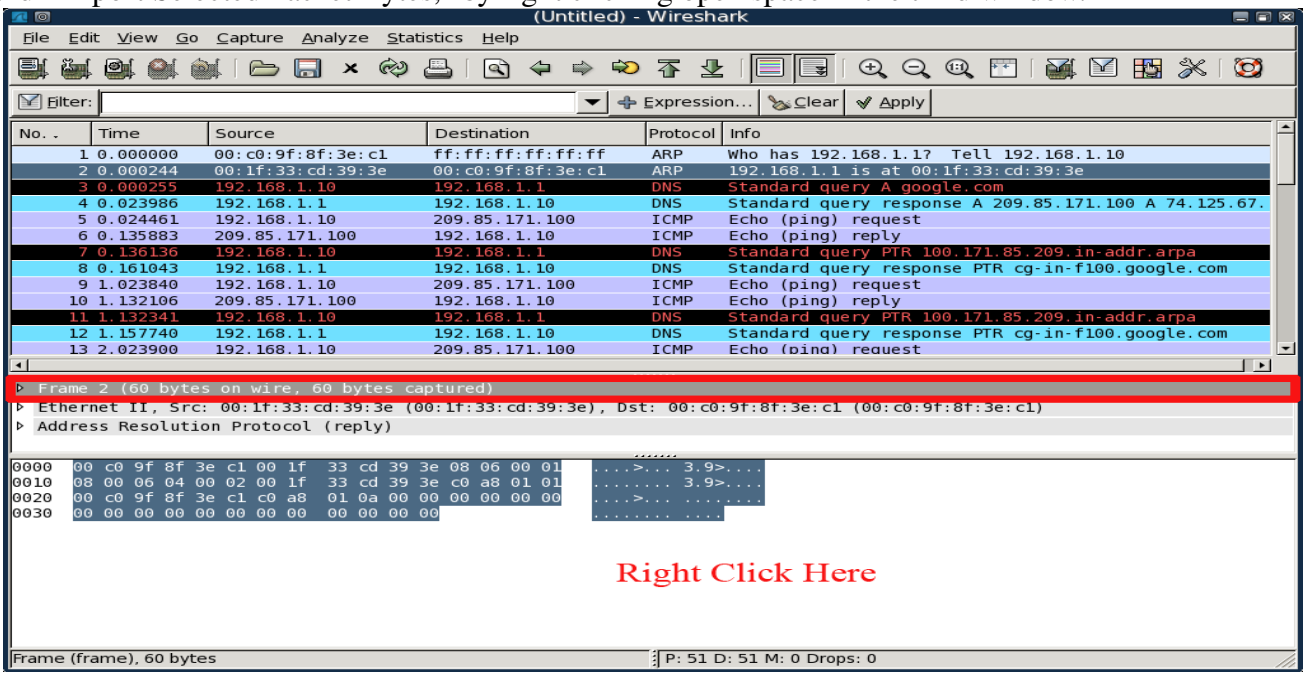
B- I suggest using the following settings for your network card while capturing to avoid confusion.



2- Ping a site, i.e. google.com, and wait for wireshark to capture an ARP reply. You should see the packet that is highlighted in the picture below in wiresharks capture.



3- With the packet shown above highlighted in wireshark, select “Frame 2,” from the second window and “Export Selected Packet Bytes,” by right clicking open space in the third window.



Editing the packet:

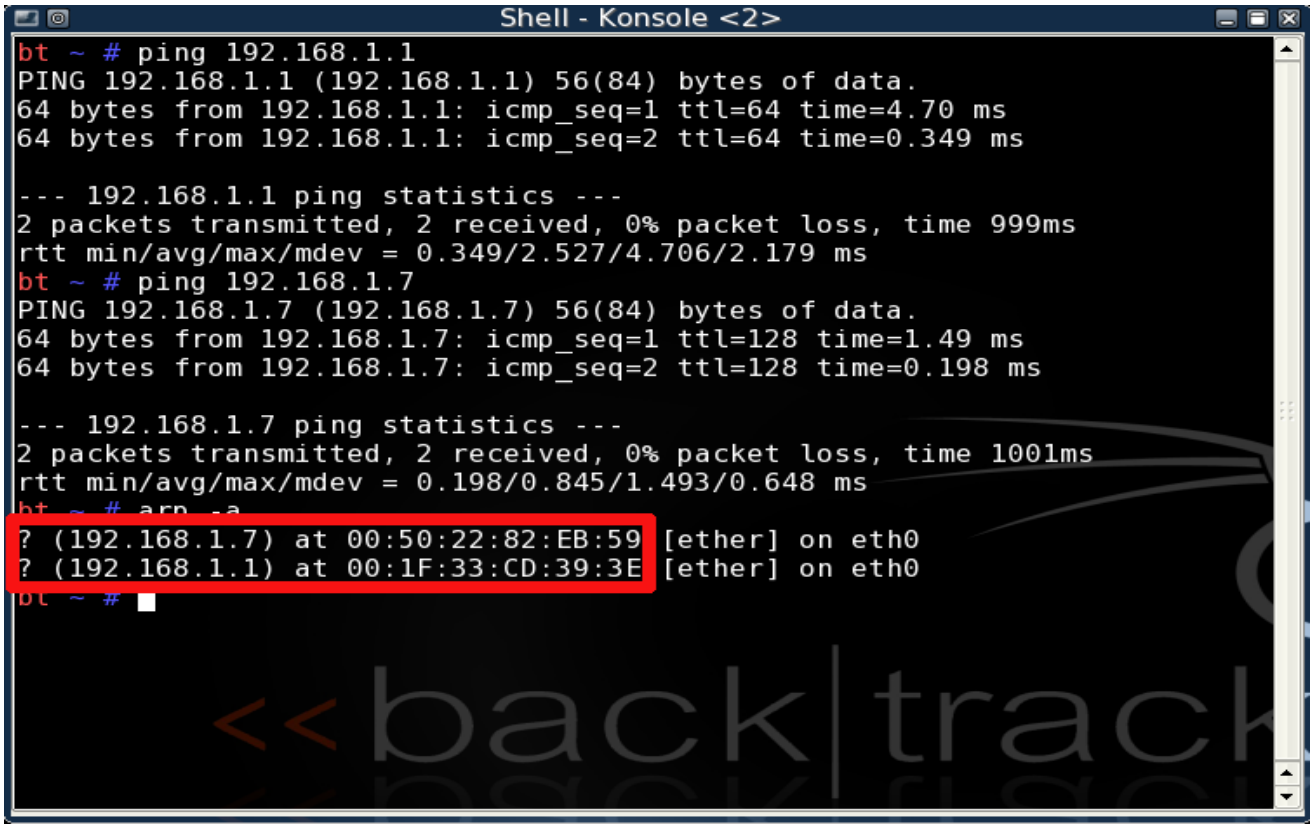
Now that we have a ARP reply packet to use as a template we can edit it in a hex editor to specify the needs for our attack.

4- Open the saved ARP reply packet with the hex editor by typing the following command into the terminal.

hexedit -b 'name of the ARP reply packet you saved'

-b = buffers the entire file in memory, much faster, enables inserting and deleting

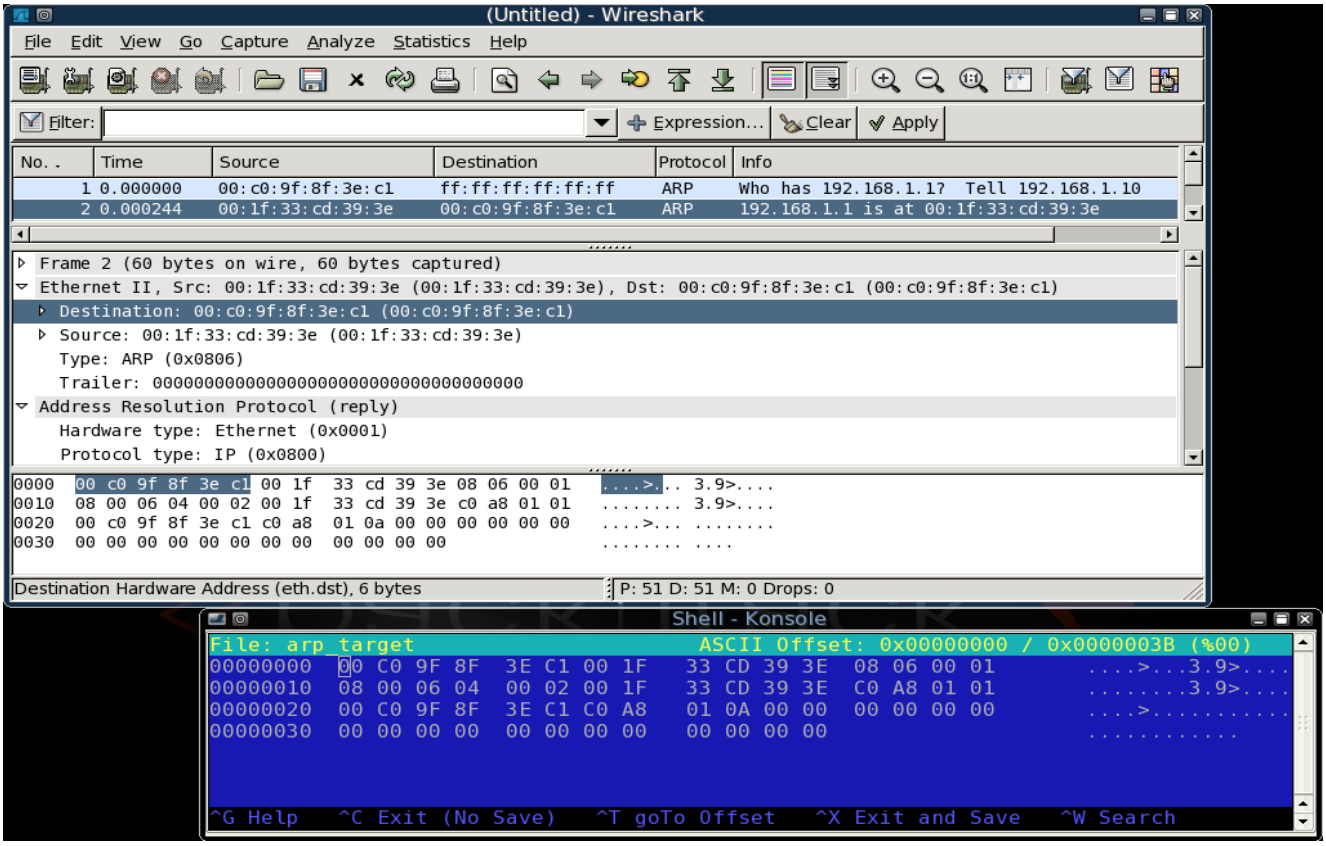
5- Before editing the packet we must obtain the target computer, attacking computer, and the gateway's IP's and MAC address. In order to find this information we ping the target computer and gateway. Observe the screen shot below and open up a text editor or the old fashion piece of paper to write down the highlighted information for easy access later on.



To find your attacking computer's IP and MAC address simply type the following command into the terminal and record the IP and MAC address.

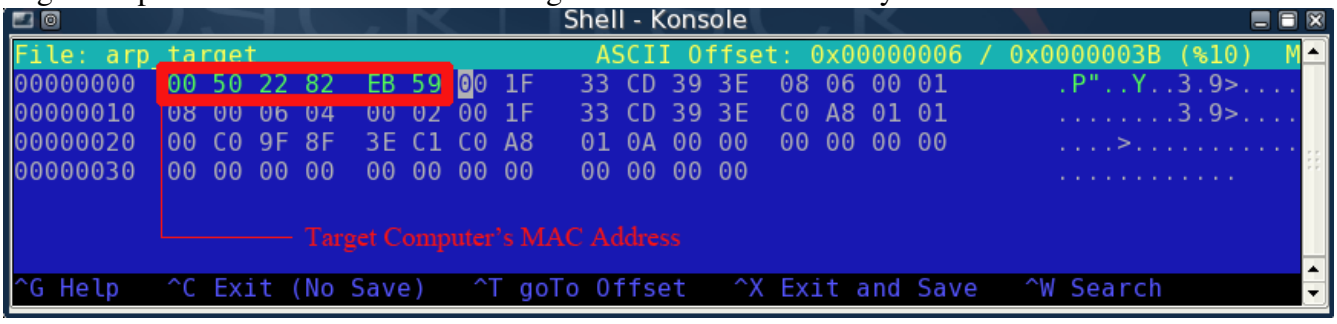
ifconfig

6- Now that we have the needed information we can edit our ARP reply packet. Go back to the hex editor and wireshark and open them to where you can see the needed information comfortably like pictured below. Also be sure to have the information recorded from step 5 handy and at the ready.

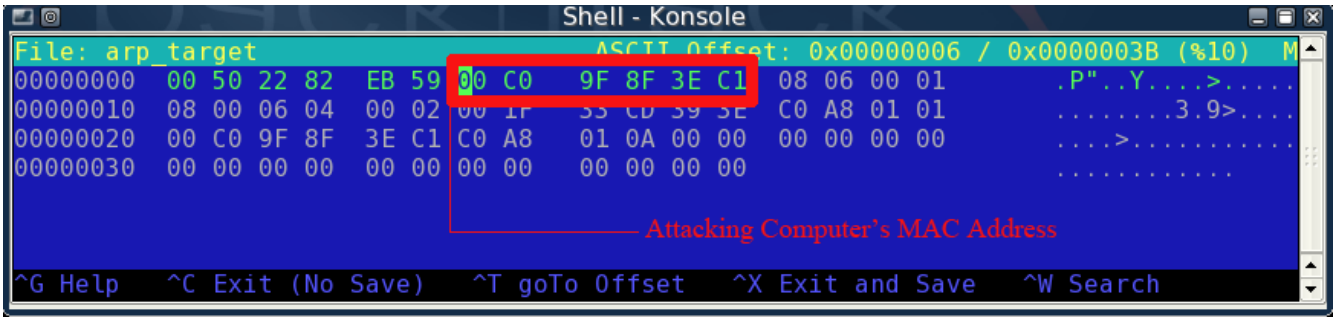


7- The first fields that need to be edited are the “Destination” and “Source” MAC address's. This information is displayed in the second window in wireshark under the “Ethernet II,” drop down while the ARP reply packet is highlighted from the first window. For our attack the destination will be the target computer's MAC address and the source will be our attacking computer's MAC address. Clicking on the fields in wireshark will highlight the corresponding information given in hex by the packet in the third window. All of this information is also shown in the picture above.

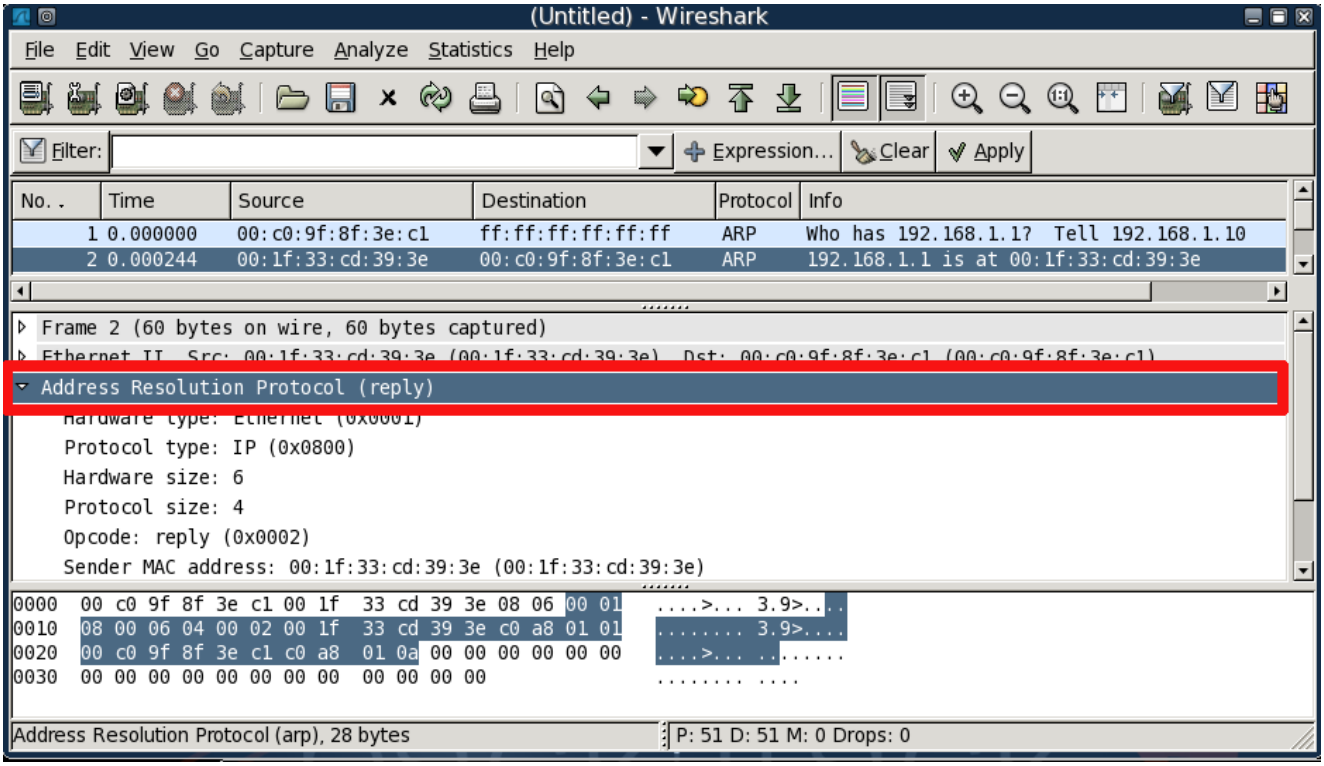
8- Now that you can see where the destination MAC address is in the hex editor you change it to the target computer's MAC address. The changes will be colored in a sky blue color.



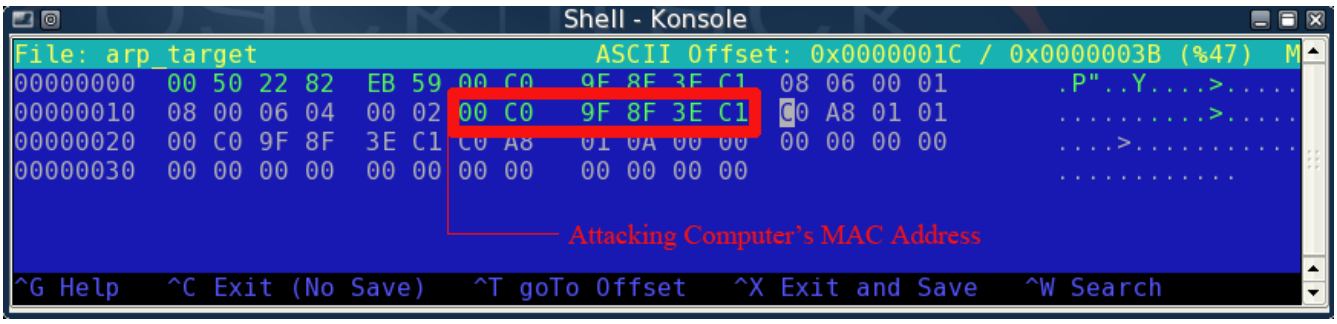
9- Select the “Source,” field in wireshark to see where it is located in your hex editor. Change that to your attacking computer's MAC address.



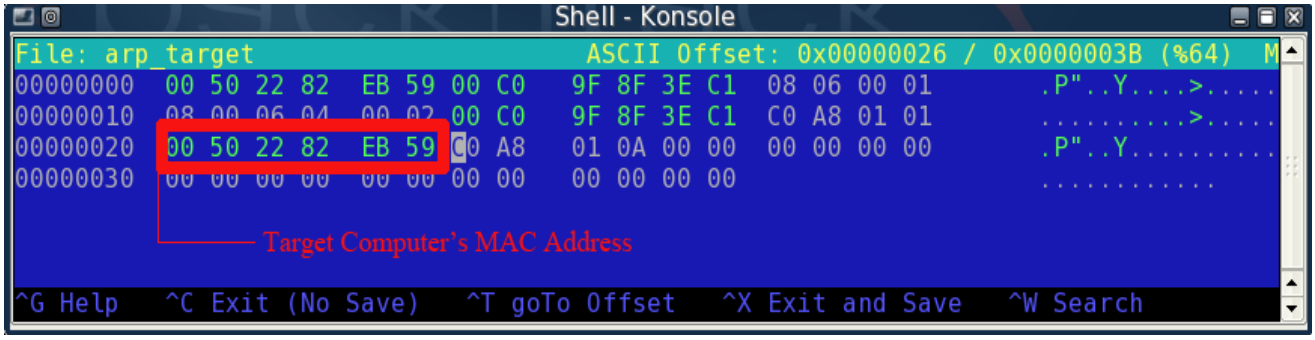
10- The next fields that we need to edit are located in the "Address Resolution Protocol (reply)," drop down in the second window of wireshark.



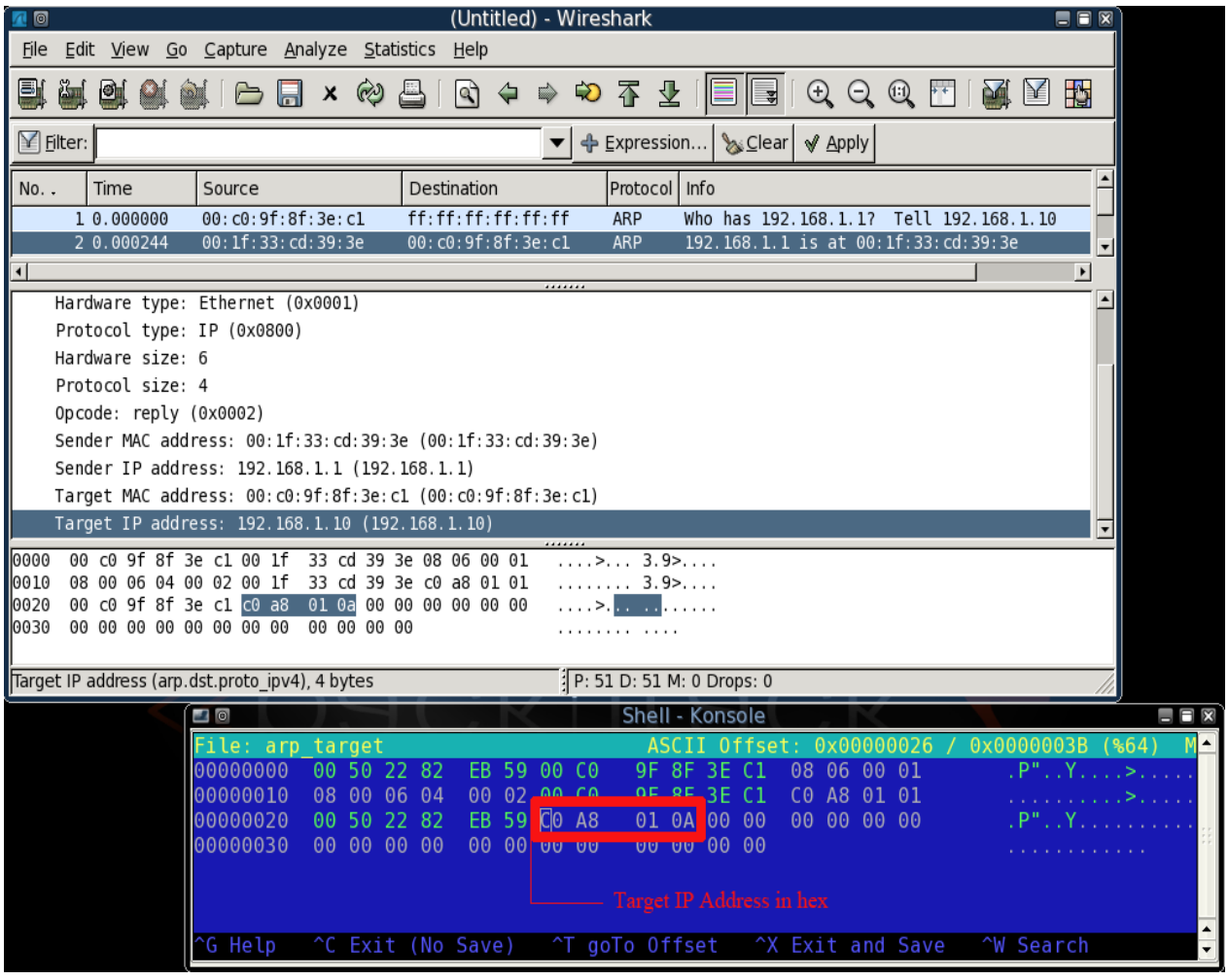
11- We need to change the "Sender MAC address," to our attacking computer's MAC address in the hex editor.



12- We now need to change the "Target MAC address," to our target computer's MAC address.

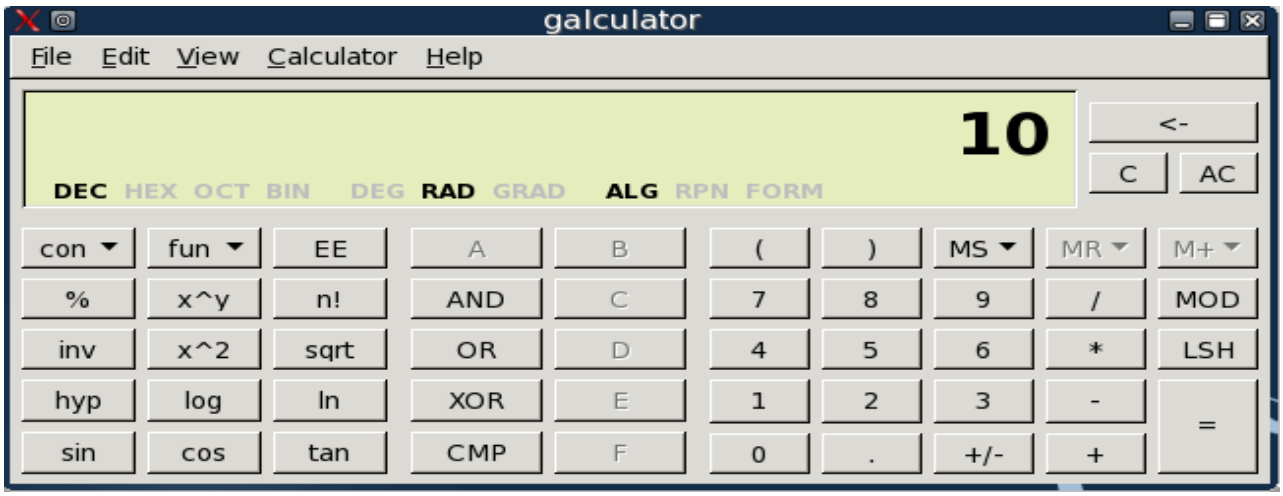


13- We now need to change the "Target IP address," to the target computer's IP address. However we are now dealing with numeric values of the IP instead of the hex code of the MAC address's. You can see that the target IP address of the packet is directly after the target MAC address field in the hex editor.

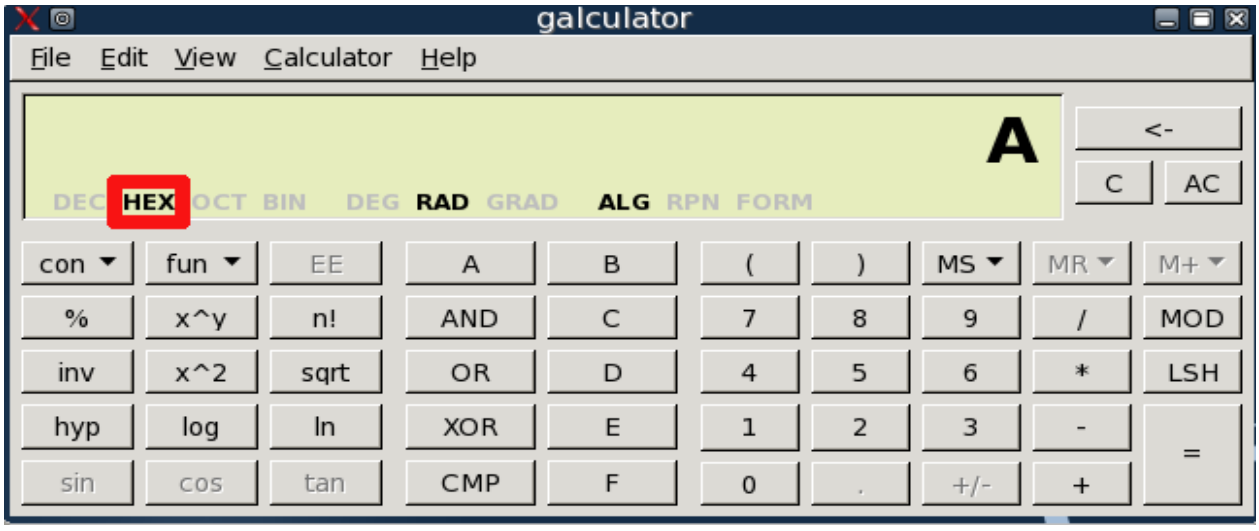


Observing the highlighted field in the above picture you can see that "C0 A8 01 0A" is hex for

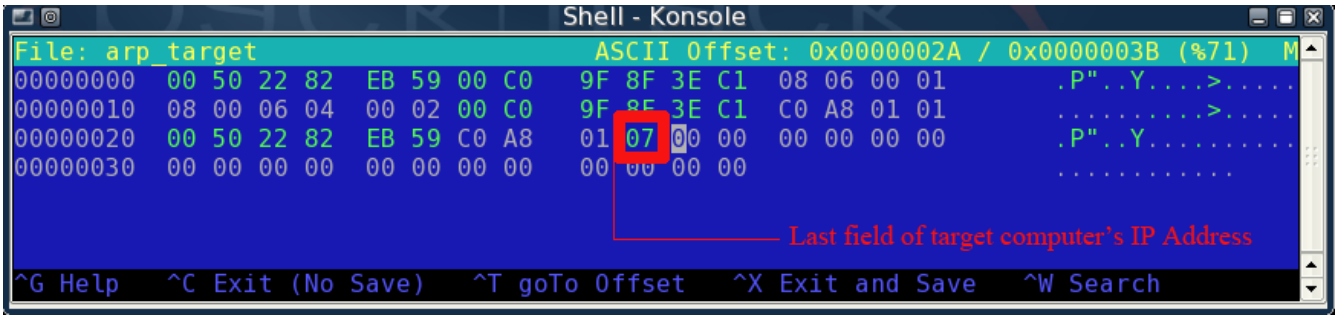
“192.168.1.10.” Now knowing this the only value we must change is the last field of the IP address. In order to find the hex value of the target computer's IP you can use the built in “Galculator,” to convert it. It is located in the “Utilities,” tab of the KDE start menu. Change the view to scientific and input the last field of the target computer's IP address.



Now all you need to do is click the greyed “HEX” area in the Galculator. This will convert your numeric value to hex.



Now that you have the last field of the target computer's IP address in hex you can input it into the hex editor.

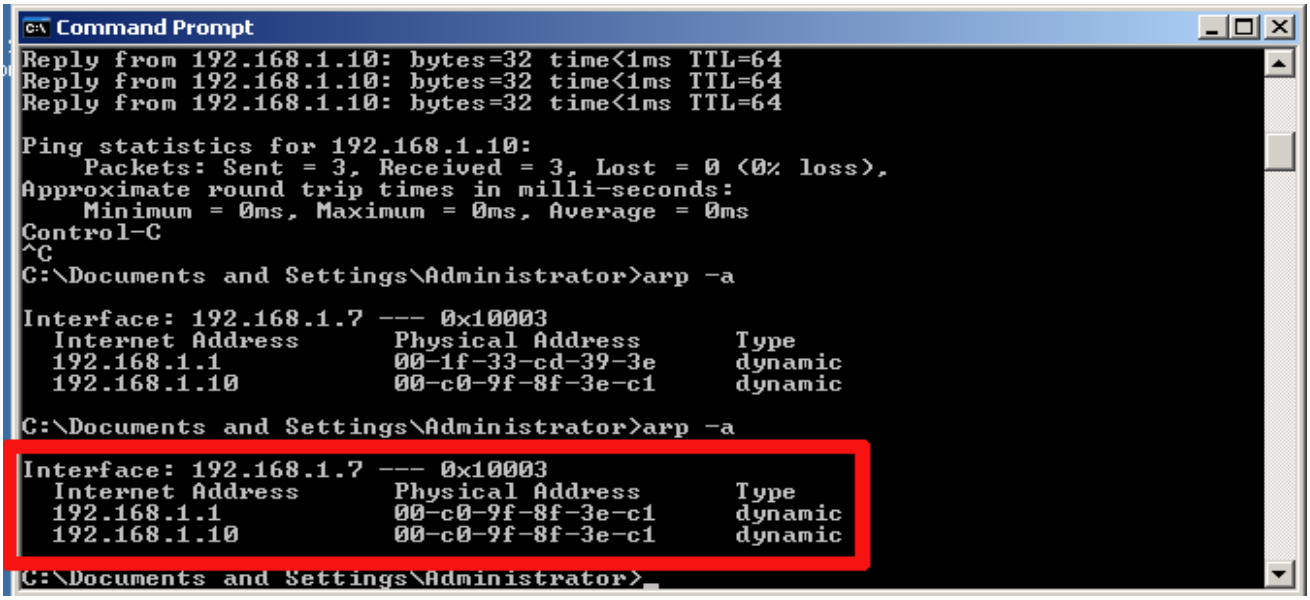


14- We can now save this packet and test it. Save the packet and in the terminal type the following command.

file2cable -i eth0 -f arp_target

-i = network card interface
-f = file of packet (in this case arp_target)

Execute the command twice for safe measure. If you now go into the target computer and view its ARP cache you will see that the gateway and the attacking computer have the same physical address. If you constructed the packet correctly you should see something similar to the picture below on the target computer.



15- The next step will be to create our spoofed gateway packet. We can copy our packet we made for the target computer and use it as a template for building this gateway packet by typing the following command into the terminal.

cp arp_target arp_gateway

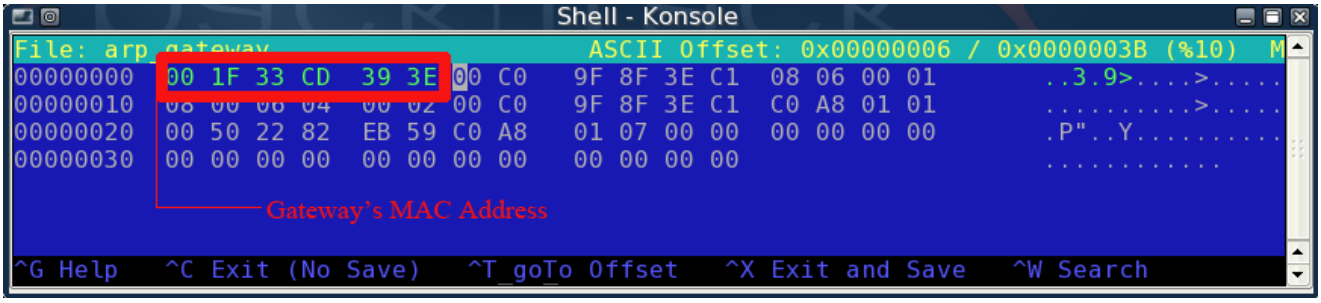
arp_target was the name of the packet we first created and we copied it to a new file with the name arp_gateway

16- Open the newly created arp_gateway packet with the hex editor.

hexedit -b arp_gateway

-b = buffers the entire file in memory, much faster, enables inserting and deleting

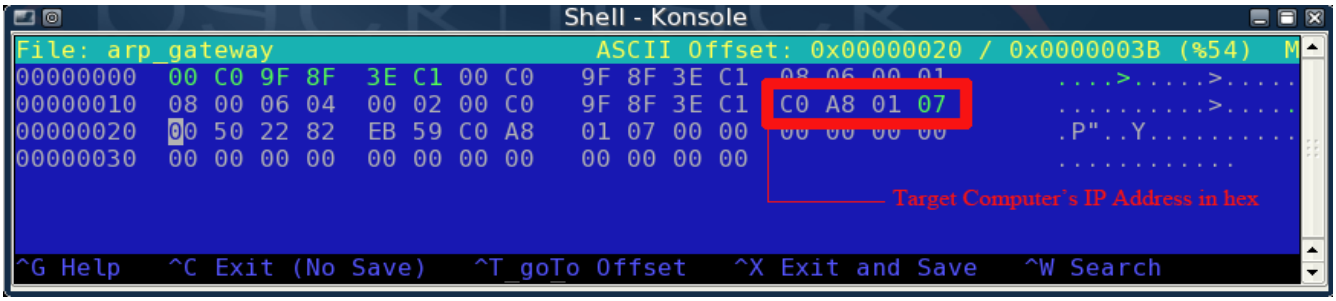
17- First we will change the destination field to the gateway's MAC address.



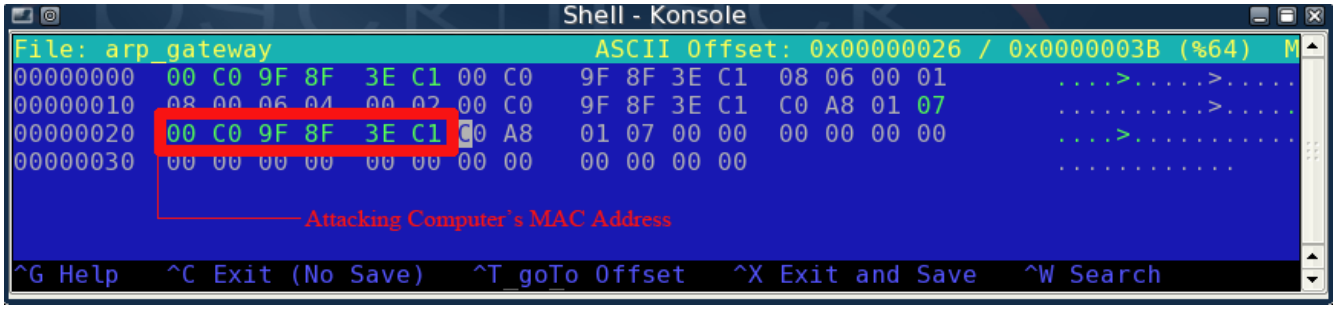
18- Next we change the source field to our attacking computer's MAC address, but luckily for us it is already filed in correctly from inputing it in our arp_target packet.

19- We will now edit the sender MAC address field to be our attacking computer's MAC address, once again lucky for us it is already filled in correctly from our previous packet.

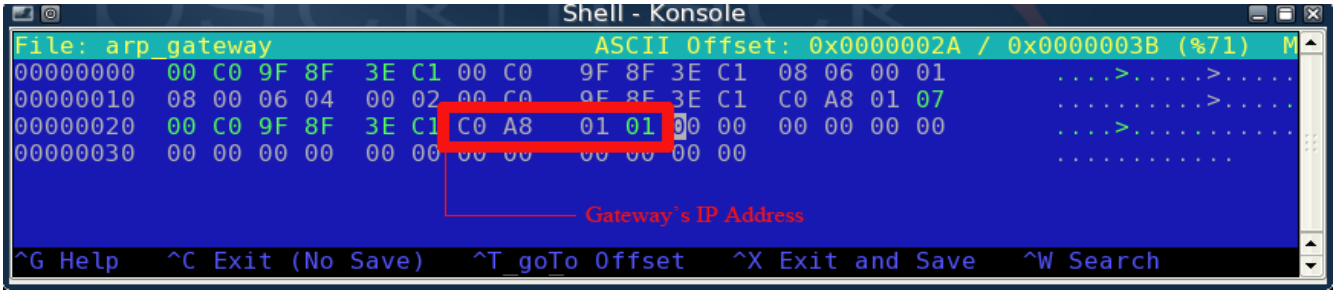
20- The sender IP address if the field we want to spoof, so we enter in the IP of the target computer in this field.



21- We now want to change the target MAC address field to the attacking computer's MAC address.



22- Next we want to change the target IP address field to the gateway's IP address.



23- Now that we finally have our packets constructed we can almost commence our attack. However for the spoof to be executed correctly IP forwarding must be enabled on our attacking machine. Not doing so will result in a Denial of Service attack on the target computer. We do this by typing the following command into the terminal.

echo>1/proc/sys/net/ipv4/ip_forward

Placing the value 1 in the above file enables IP forwarding, allowing our computer to... forward IPs :P

24- Since the method used in step 14 is only temporary we will create a script that sends our created packets over the network every two seconds. Create a new file called attack.sh and open it in nano. We can do this by typing the following command into the terminal.

nano attack.sh

creates a new file named attack.sh and opens it in nano

25- Enter in the following code in this file in order to create our looping script.

```
#!/bin/bash

while [1];do

file2cable -i eth0 -f arp_target
file2cable -i eth0 -f arp_gateway
sleep 2
done
```
this loops the file2cable commands every 2 seconds until it is stopped

26- Save the the attack.sh script and give it executable permissions by typing the following command into the terminal.

```
chmod 755 attack.sh
```
gives the file attack.sh executable permissions

By creating this script and giving it executable permissions, when ran it will keep sending our packets through the network every two seconds not allowing the target computer's ARP cache to recover.

27- SO! we have successfully created our packets and a script to loop those packets. If we run this script by entering the following command into the terminal our attack will commence.

```
./attack.sh
```
executes the attack.sh script

28- If all of the above steps went smoothly we should be able to launch our attack script, start up our sniffer, and watch as we capture the traffic that our target computer is receiving. :) You should see something similar to the image below in wiresharks capture.