# DNS Cache poising

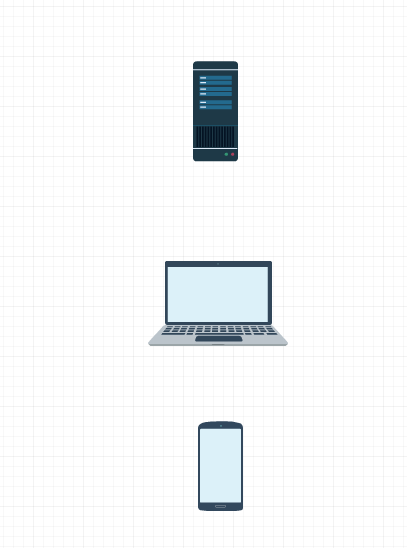
For this Cain and Abel software was used to perform DNS poising or man in the middle attack.

To install Cain and Able software run the ca\_setup and follows the instructions.

For this attack you will also need either a virtual box or another device that can connect to the internet.

One is going to be the attacker this has the Cain installed the other is the victim all it needs to be is on the same network as the hacker.

Look at Fig1 for a set up:



Server DNS CACHE

Hacker

Target

Sends back the hackers request to Hackersite.com

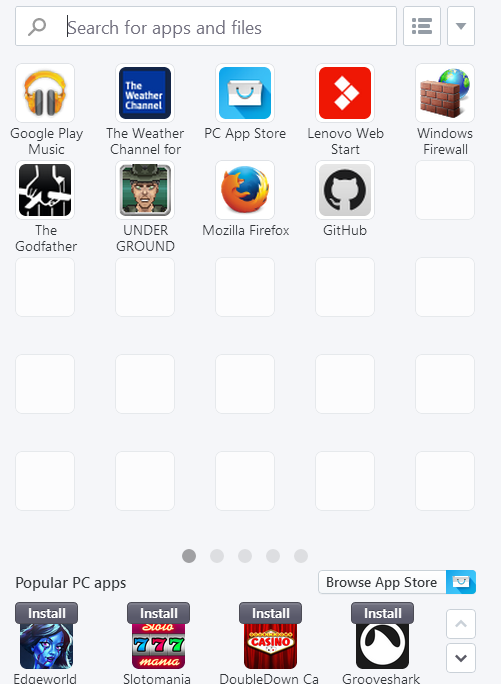
Request for bing.com

Intercept the request

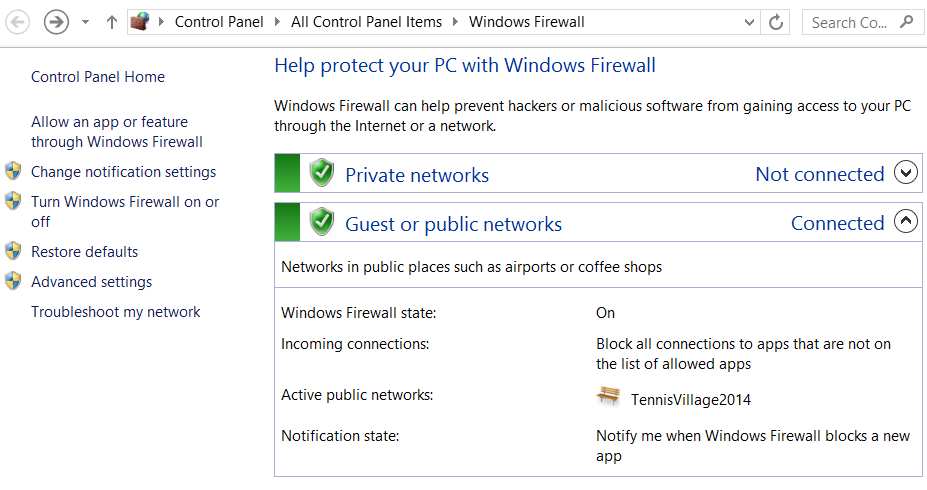


In this example I used a phone as the victim. The original request being sent up to the server is [www.bing.com](http://www.bing.com) but it will return [www.goole.ie](http://www.goole.ie)

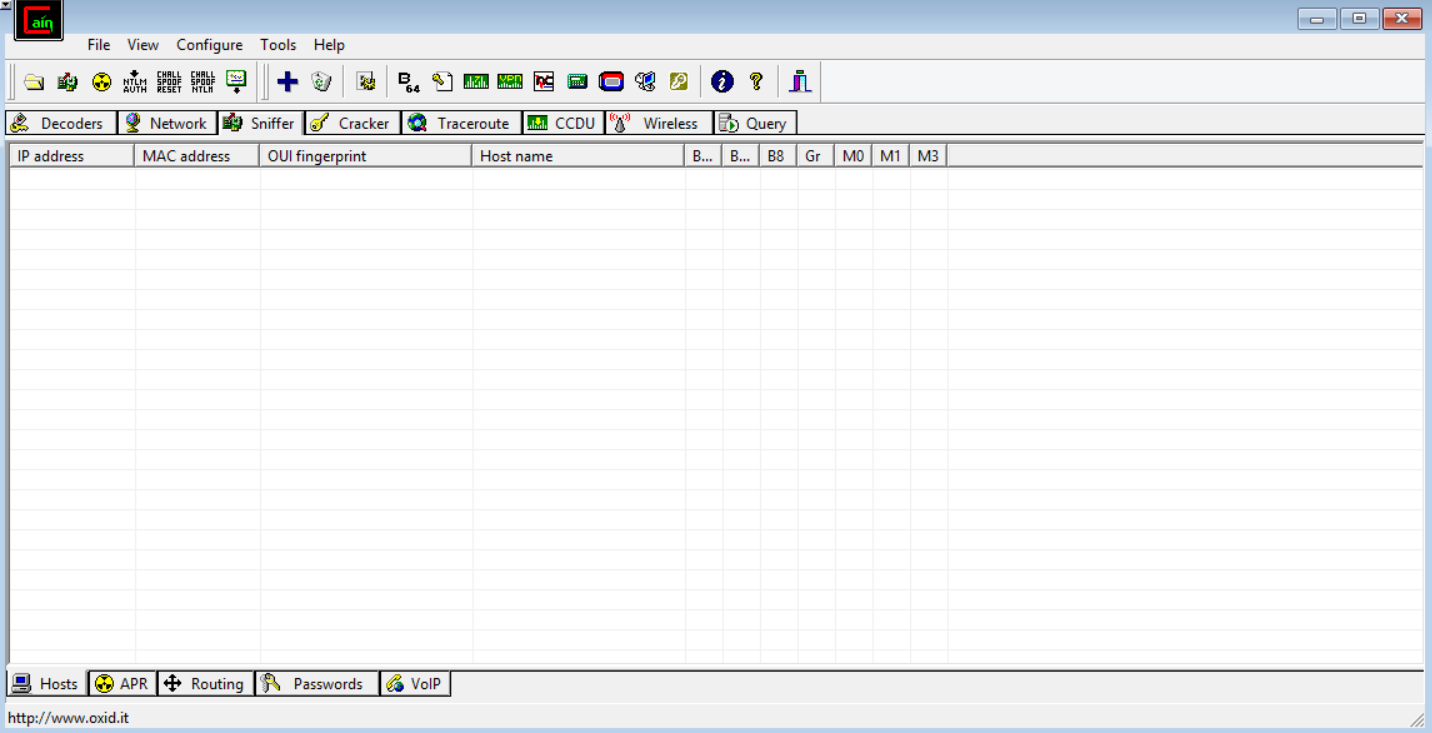
Open up Cain and Able you may get a prompt to turn off ypu firewall to do that go **to start – search Firewall and turn on/ off firewall**

****



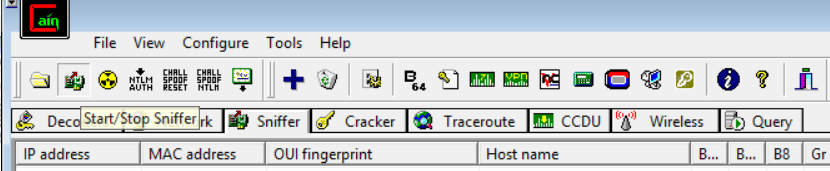
****

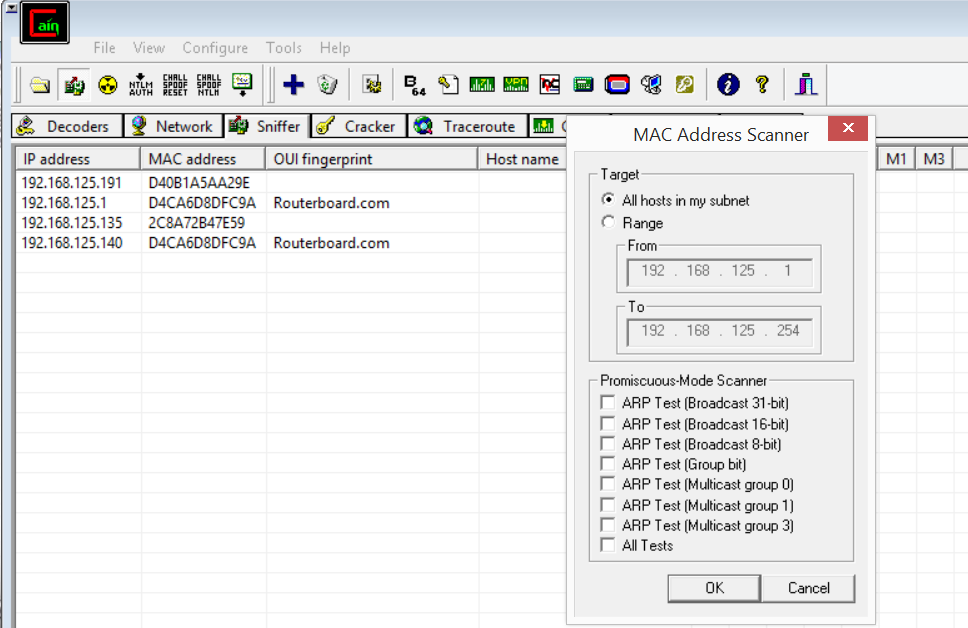
Once that is done go back to Cain and navigate to the Sniffer tab. In the bottom left corner are two tabs Hosts and APR these are the two tabs we will be using by default we are in the hosts tab here we can get all the ip addresses that are on the network.



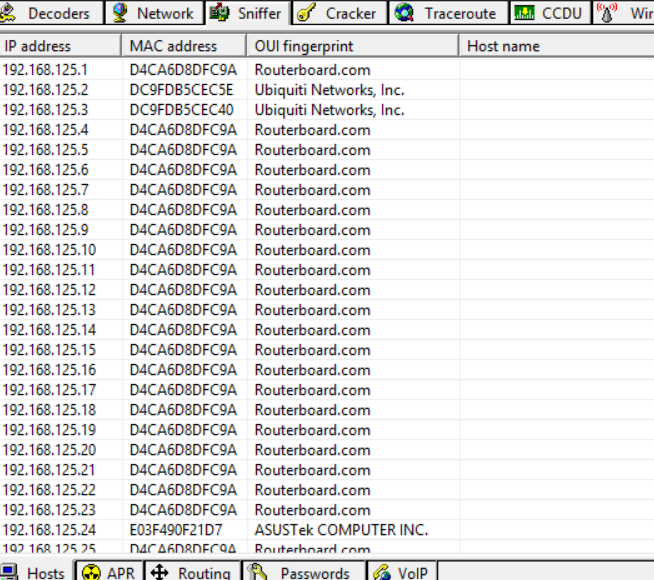


To populate the ip’s click on a white cell than **Start/ Sniffer** button followed by **ADD list.**

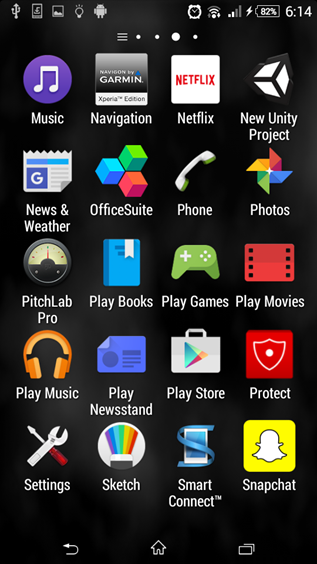
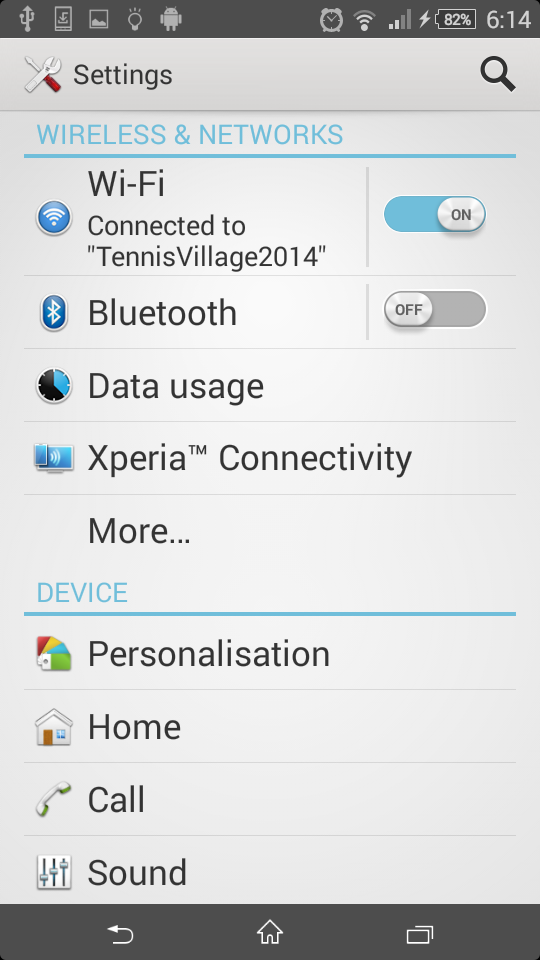




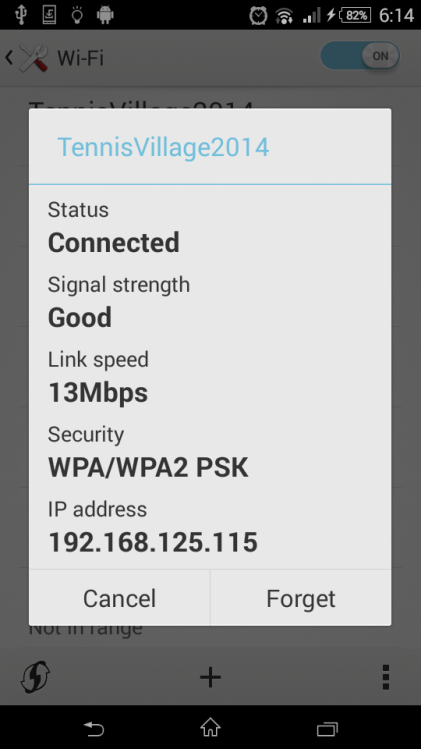




Here we can see a list of all the IP that are on the network, if we now go to our phone and go to **settings**. Click on **WI-FI**



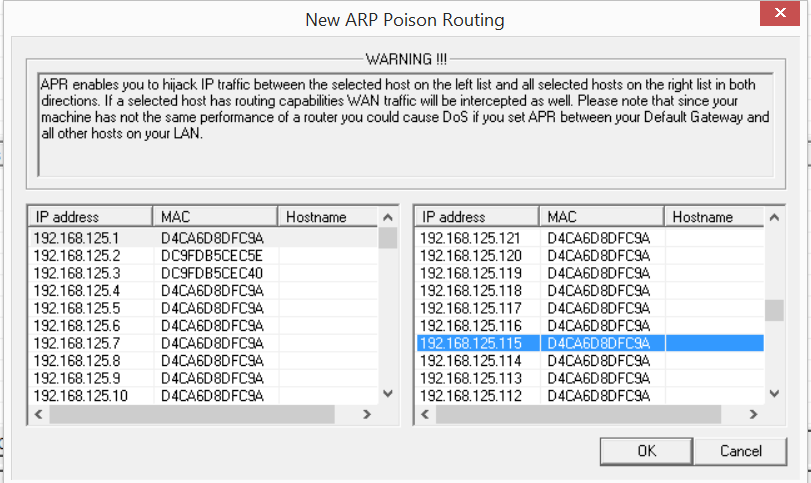
We can the phones ip address that is now our target.



You should now go back to Cain and click on the **APR** tab. Here we set up for our attack back intercepting communication between 192.168.125.115 and the default gateway 192.168.125.1.

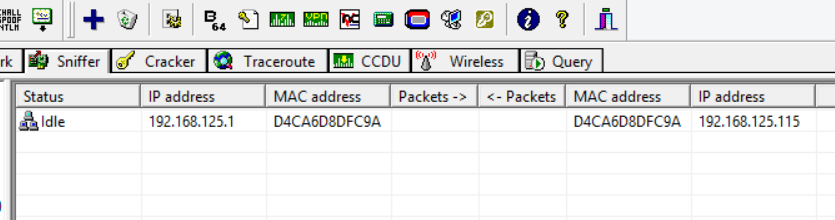
While in the APR menu click on the **ADD to List** button to bring up the list of available IP addresses,

On the right click on the default gateway and on right select our target.

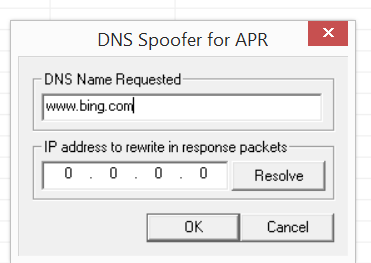




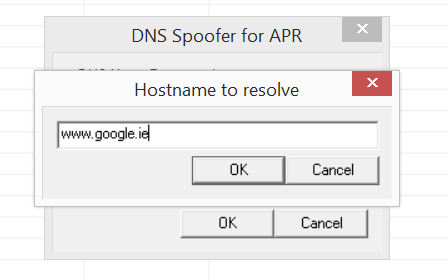
After hitting ok we have the following.



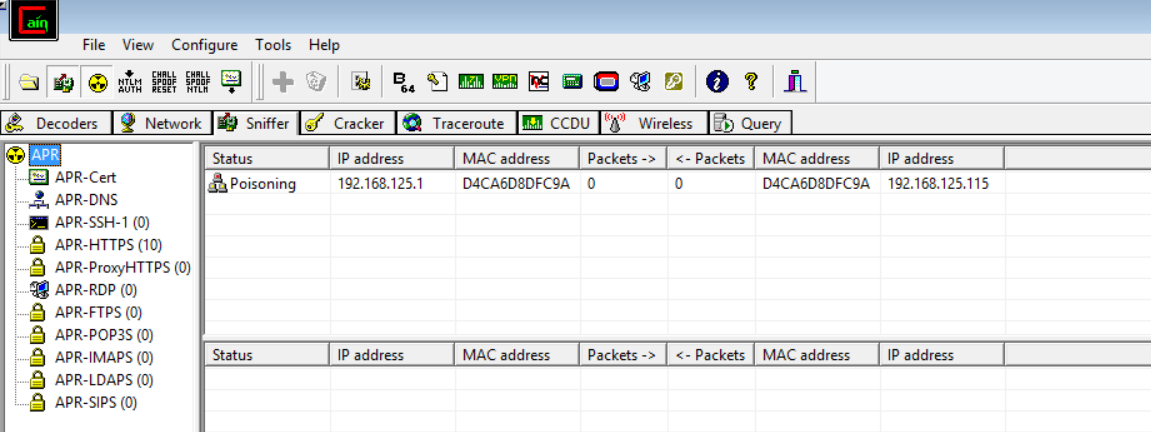
Next is to divert the request on the left panel select **APR-DNS** again select a white cell and click **Add to list.**

****

Enter the target site and hit Resolve.

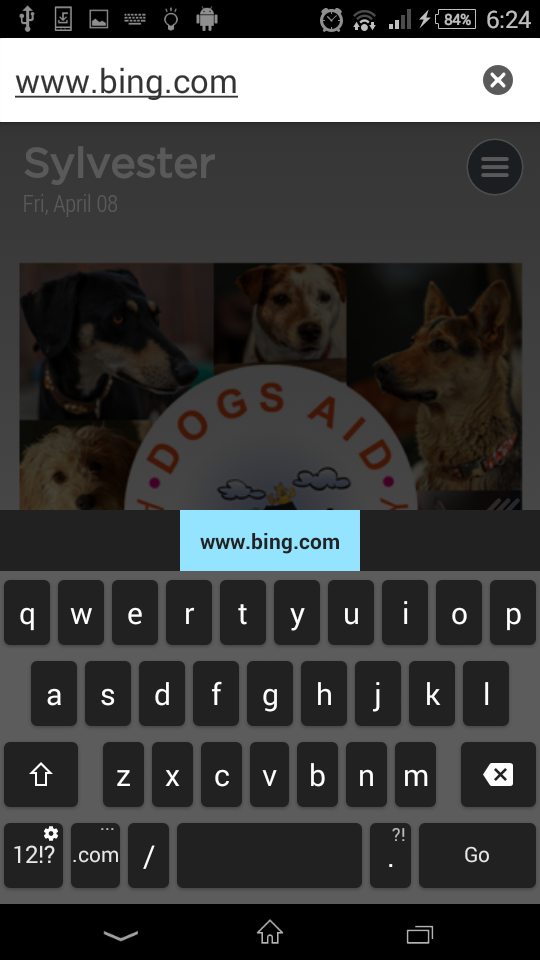
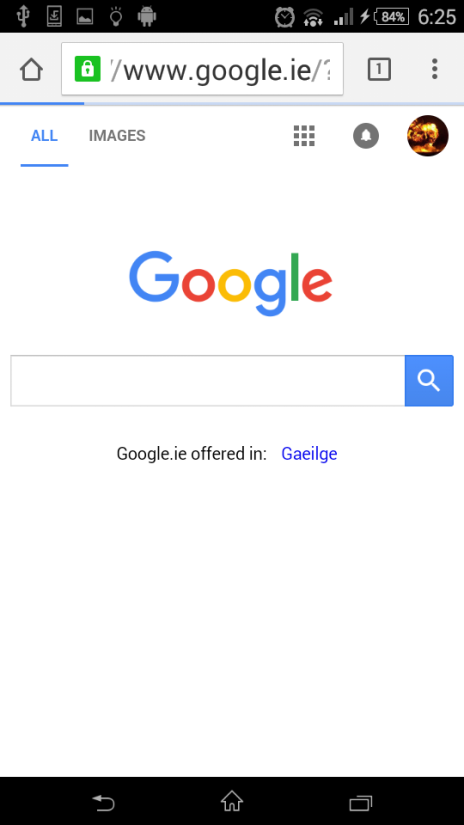


You end up with the following; you are now all set to hack press the **start/stop APR** and it will begin poisoning.





If we now go to our victims device and enter Bing .com into the search bar we get Google.ie instead.



### Conclusion

This only show a positive test the actual outcome was that not easy to prove from this test the conclusions gather is that google has its own set of security protocol that prevent this type of attack from happening. When a retest was tried using a laptop and internet explorer this still did fix the problem this was also proven by using Firefox. In Conclusion most browsers have set protocols in place that prevent this attack.