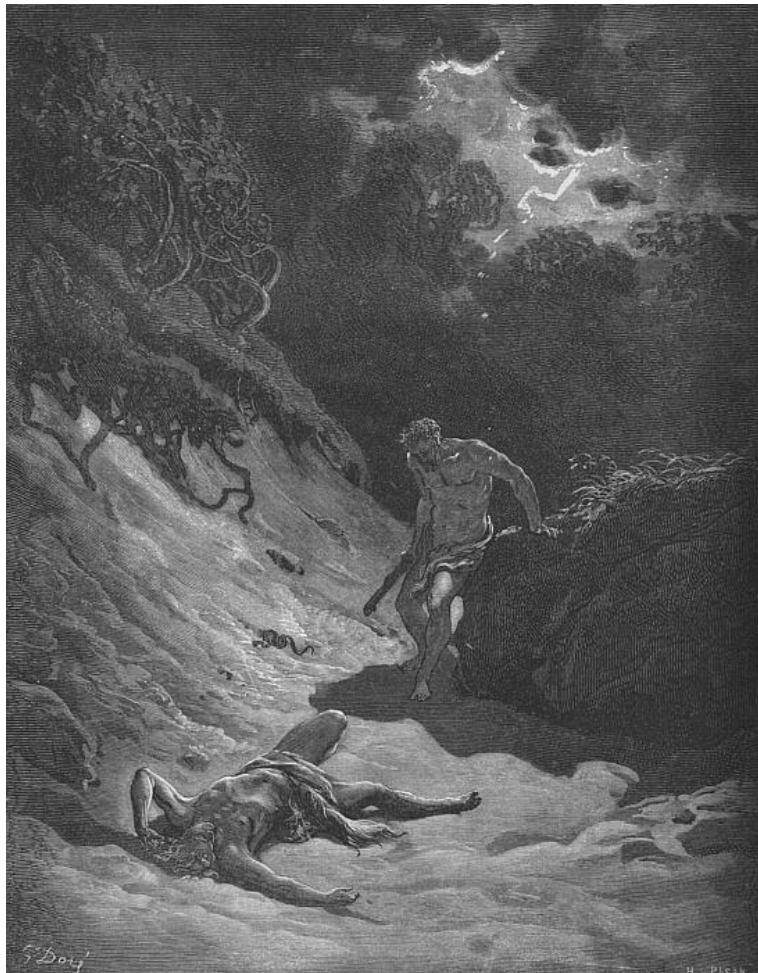


Cain and Able

A disturbing Tutorial



Questions? mutsonline.com

<http://mutsonline.com>

Cain and Able – The Terror begins

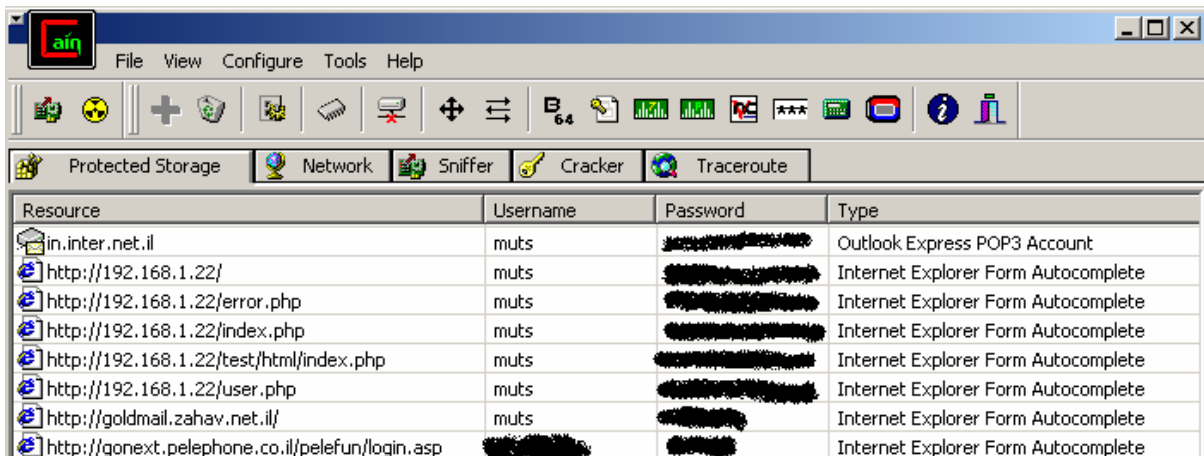
DESCRIPTION

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary & Brute-Force attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

It also has ARP poisoning and spoofing capabilities, making it into an extremely powerful hacking or auditing tool. The ARP spoofing feature works in a similar way as described in the "ARP Spoofing" tutorial. Indeed it would be wise to read that tutorial before attempting to use Cain.

Environment

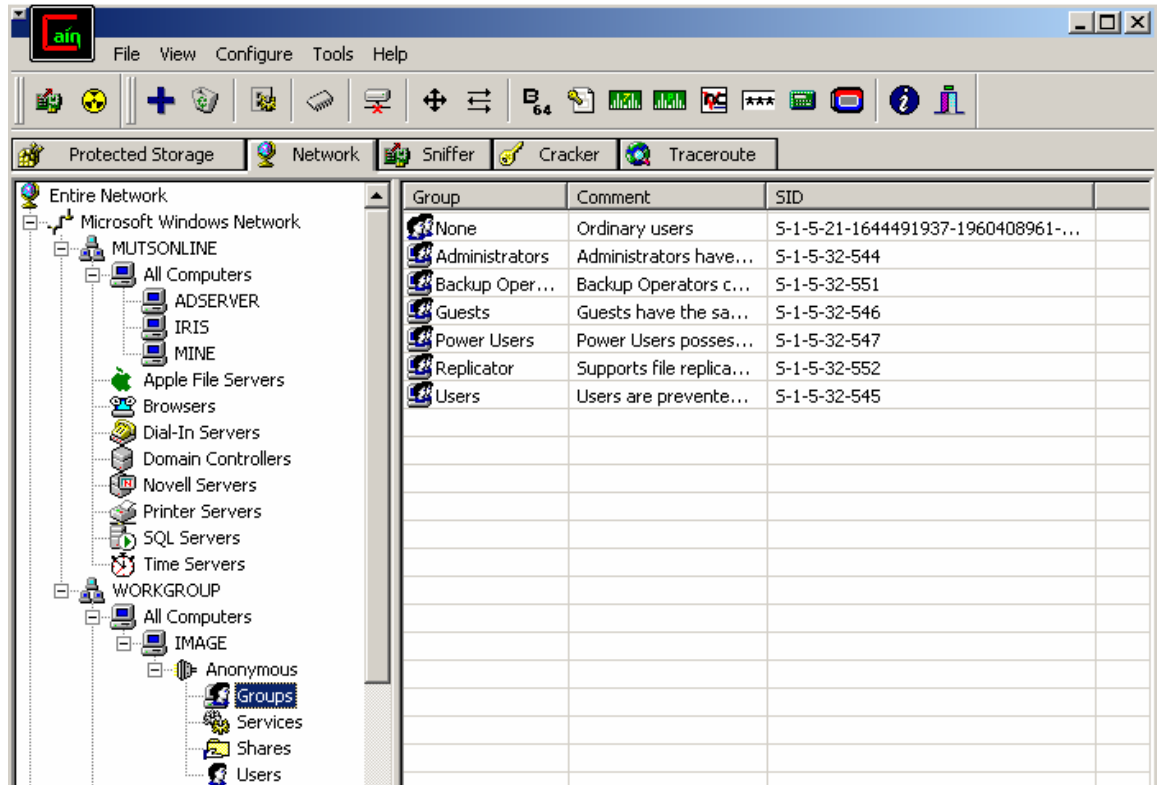
1. Install and run Cain. Immediately when it opens you can see the first disturbing scene. All the cached passwords are shown in the "Protected Storage" tab. These include passwords from IE, Outlook or other HTTP transactions.



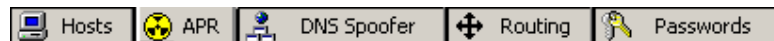
The screenshot shows the main window of Cain and Able. The 'Protected Storage' tab is active, displaying a table of recovered credentials. The table has four columns: Resource, Username, Password, and Type. The Password column contains several rows of blacked-out text, indicating that the passwords have been successfully recovered.

Resource	Username	Password	Type
in.inter.net.il	muts	[REDACTED]	Outlook Express POP3 Account
http://192.168.1.22/	muts	[REDACTED]	Internet Explorer Form Autocomplete
http://192.168.1.22/error.php	muts	[REDACTED]	Internet Explorer Form Autocomplete
http://192.168.1.22/index.php	muts	[REDACTED]	Internet Explorer Form Autocomplete
http://192.168.1.22/test/html/index.php	muts	[REDACTED]	Internet Explorer Form Autocomplete
http://192.168.1.22/user.php	muts	[REDACTED]	Internet Explorer Form Autocomplete
http://goldmail.zahav.net.il/	muts	[REDACTED]	Internet Explorer Form Autocomplete
http://gonext.pelephone.co.il/pelefun/login.asp	[REDACTED]	[REDACTED]	Internet Explorer Form Autocomplete

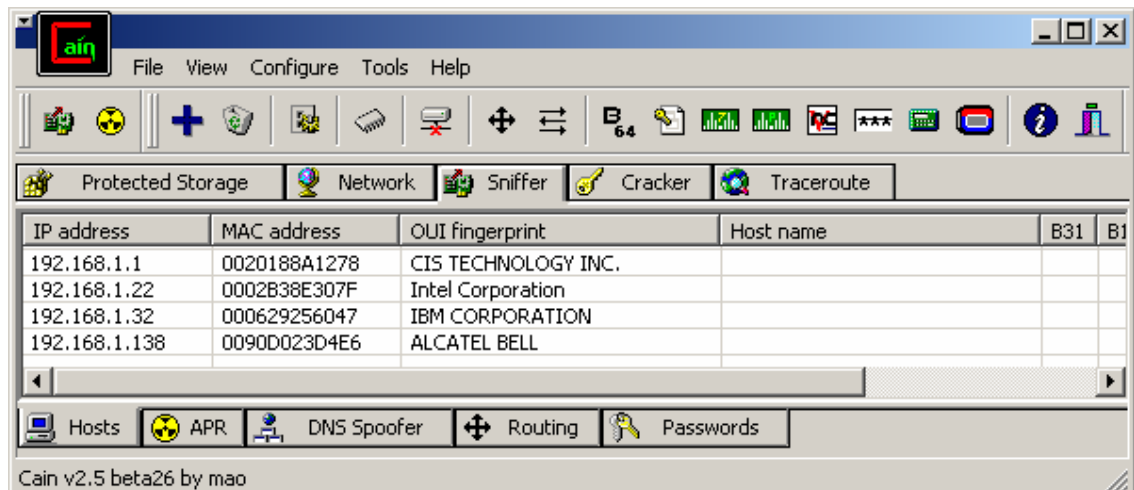
- The "Network" tab is a scaled enumeration system, able of enumerating all Windows computers it can find on the local network.





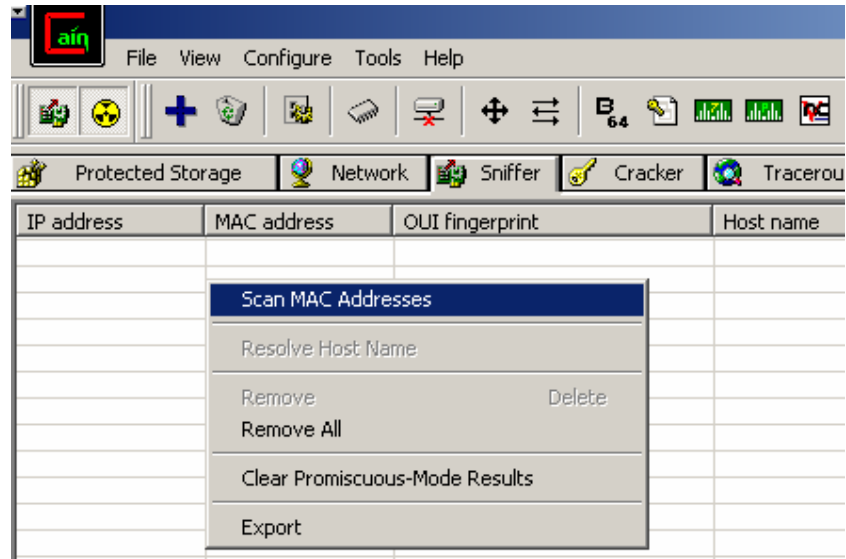
- The most interesting (IMHO) feature of Cain is in the "Sniffer" Tab. Cain allows you to ARPSpoof, Sniff and Brute force passwords all via one interface. Notice that the "Sniffer Tab" has 5 sub-tabs - **Hosts, APR, DNS Spoof, Routing and Passwords.**



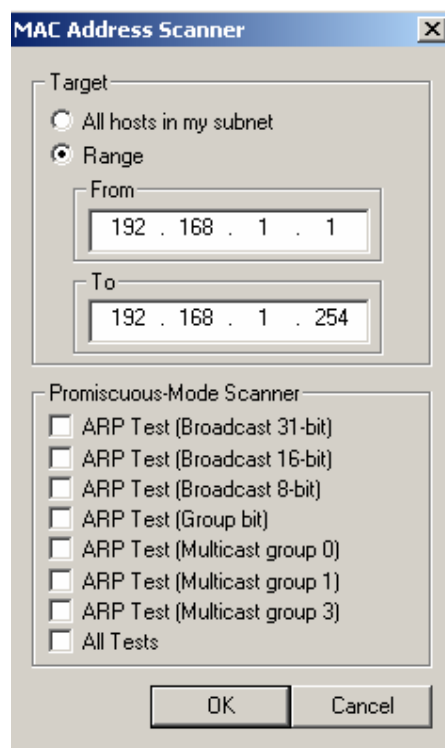
We will discuss Cain's functionality as an ARP-Spoof only.



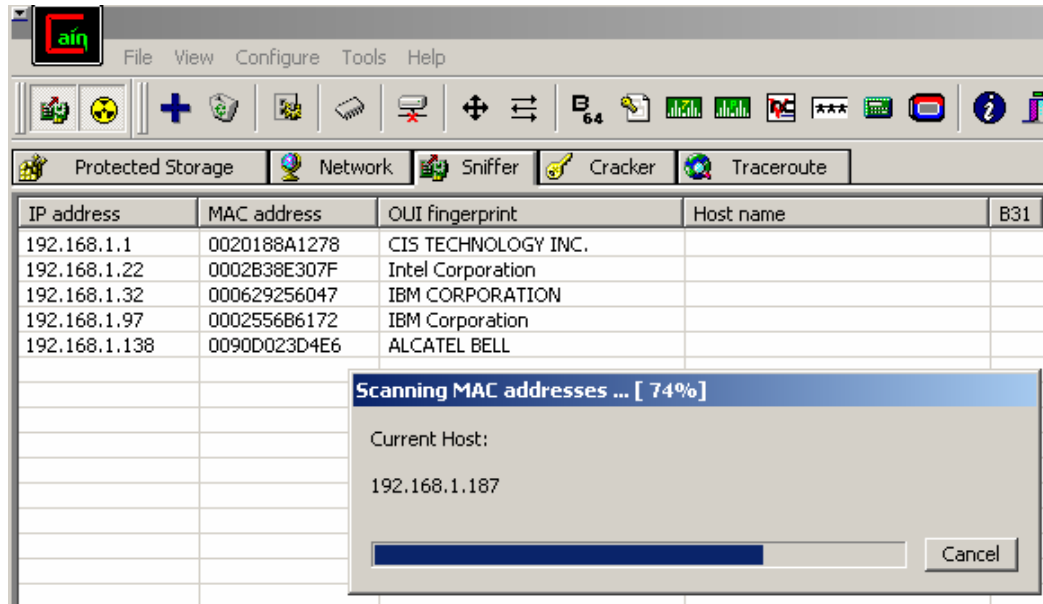
- To start ARP Spoofing, you need to activate the sniffing daemon and the APR daemon. You do this by clicking on both the "Sniff" and "APR" buttons at the top of the window ( ).
- Make sure you are in the "Sniffer" tab, and right click anywhere inside the tab. You should see a "Scan MAC addresses" option. Click it.




- Choose the appropriate IP range that suits your local network and click "Ok".

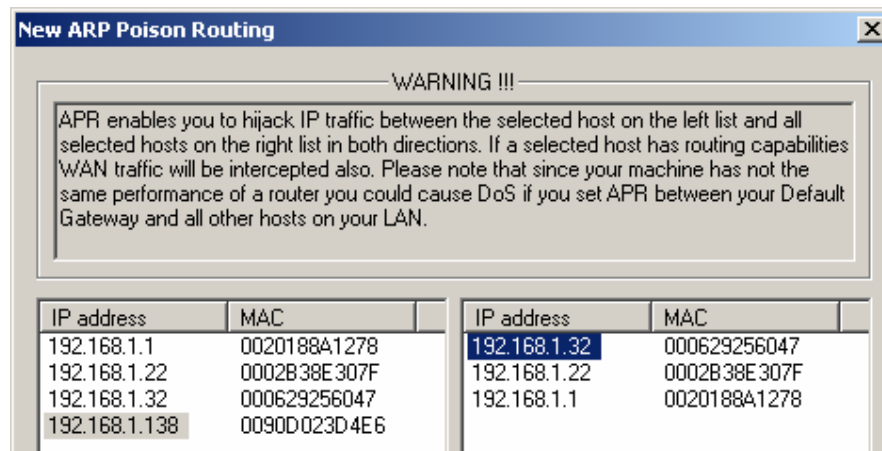


- A quick scan should occur, giving you all the MAC addresses present in that subnet.



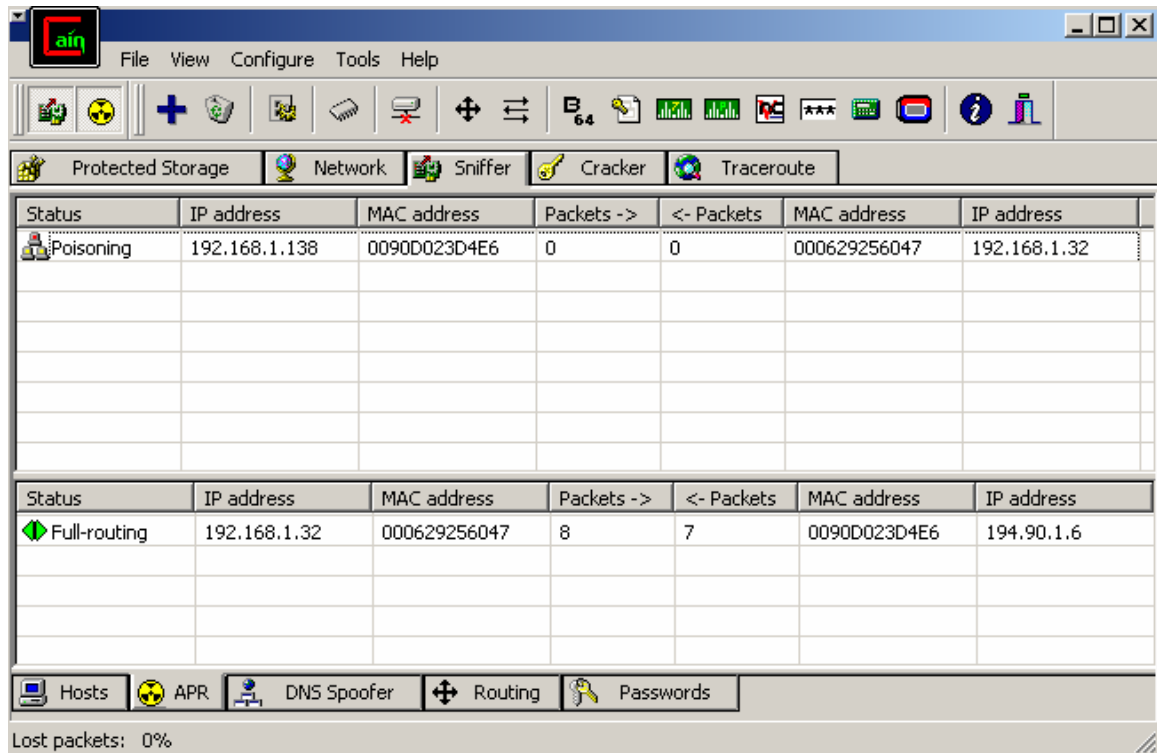
- Once the scan is complete, move to the APR sub-tab at the bottom of the window (). This is the window in which you choose the computers you want to attack. Now click on the blue "plus" sign at the top of the windows to add hosts to attack.

- You should get the following screen:

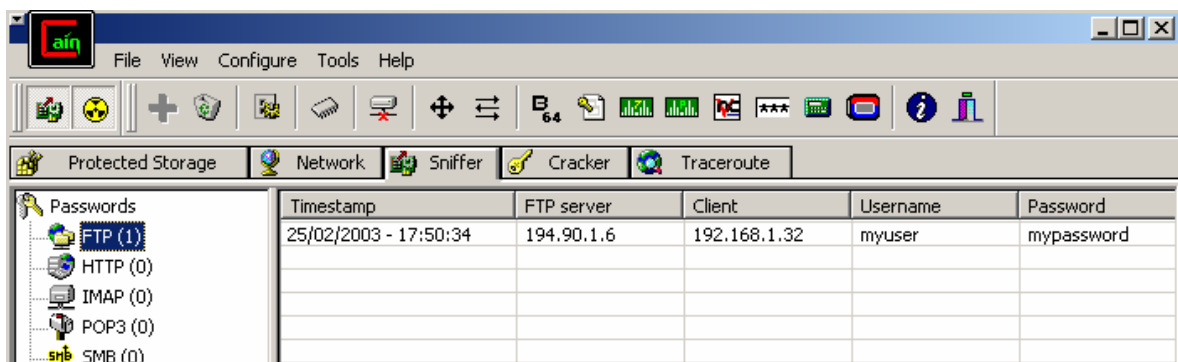


Here you choose the hosts which you want to route traffic through your computer. A default Gateway, or a Domain controller are good endpoints to choose between the attacked host.

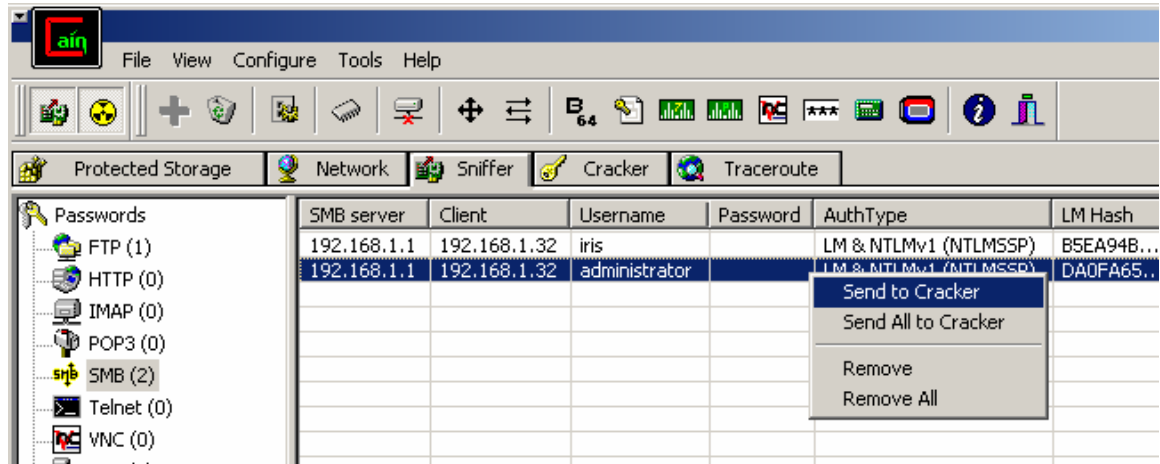
10. Now we wait for the attacked host to enter password data to services such as FTP, HTTP, POP3, IMAP, and lots of others. In the following screenshot, an FTP password was intercepted.



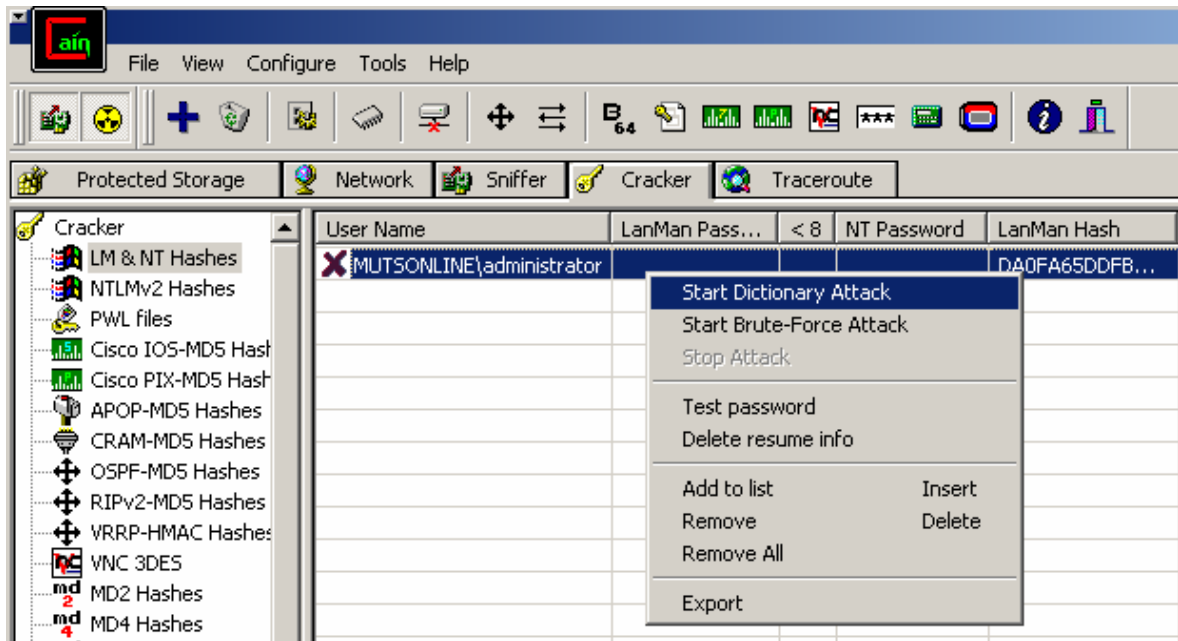
11. We can see that the FTP session between 192.168.1.32 (Attacked Computer) and 194.90.1.6 (Netvision's FTP server) was router via our computer. Now click on the "Passwords" (Passwords) and you will see the captured passwords.



12. For encrypted passwords such as SMB (NTLM in it's various flavours) you can send the password to a Brute Force session.



13. After sending the password to the cracker, click on the "Cracker" tab and start the required attack.



This was a quick tutorial about Cain's ARP Spoofing ability. Apart from ARP Spoofing Cain can do lots of other wonderful things, just take time to *carefully* learn the application.

Scary eh? ☺