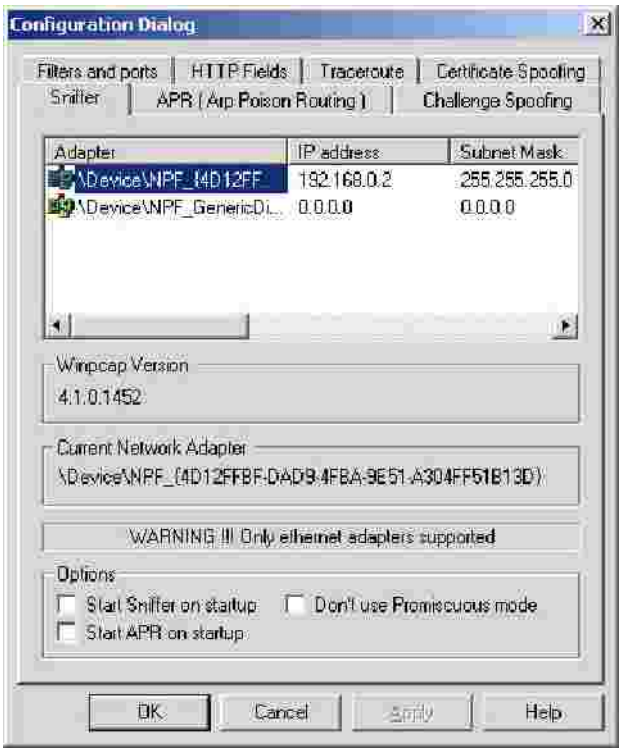
Configuration

Cain & Abel requires the configuration of some parameters; everything can be set from the main configuration dialog.

Sniffer Tab

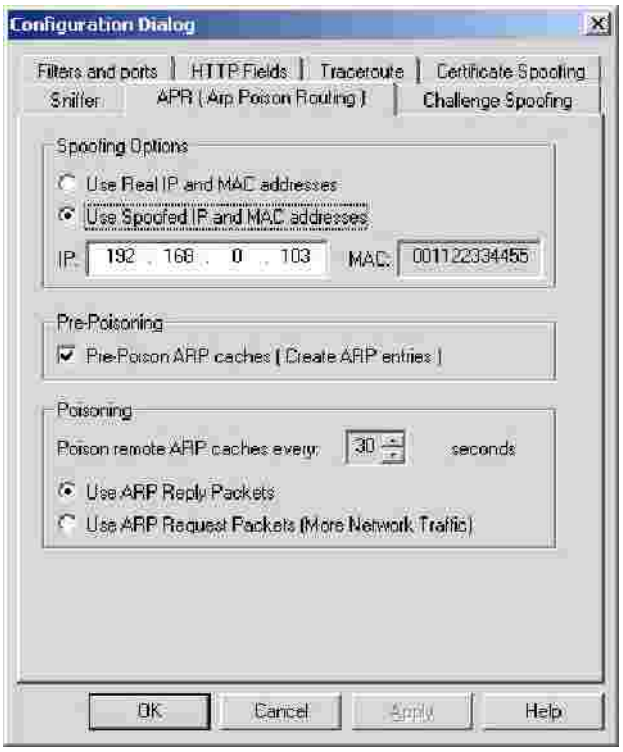
Here you can set the network card to be used by Cain's sniffer and APR features. The last two check boxes enable/disables these functions at the program's startup.
The sniffer is compatible with Winpcap drivers of version 2.3 or later and in this version only Ethernet adapters are supported by the program.



If enabled, the option "Don't use Promiscuous mode" en les APR Poisoning on wireless networks but please note that in this situation you cannot use the MAC spoofing feature below !

APR Tab

This is where you can configure APR (Arp Poison Routing). Cain uses a separate thread that sends ARP Poison packets to victim hosts every 30 seconds by default. This is necessary because entries present in the ARP cache of remote machines can be flushed out in case of no traffic. From this dialog you can set the time between each ARP Poison storm: setting this parameter to few seconds will cause a lot of ARP network traffic while setting it for long delays could not produce the desired traffic hijacking.



The spoofing options define the addresses that Cain wr s into the Ethernet, ARP headers of ARP Poison Packets and re-routed packets. In this case the ARP Poison attack will be completely anonymous because the attacker's real MAC an IP addresses are never sent on the network.

If you want to enable this option you must consider that:

- Ethernet address spoofing can be used only if the atta ker's workstation is connected to a HUB or to a network switch that does not use the "Port Security" feature. If "Port Security" is enabled on the switch, the source MAC address contained in every ethernet frame is checked against a list of allowed MAC addresses set on the switch. If the spoofing MAC address is not in this list the switch will disable the port and you will loose connectivity.

- The spoofing IP address must be a free address of your subnet. The ARP protocol does not cross routers or VLANs so you set a spoofing IP that is out of your subnet the remote host will reply to efault gateway and you will not see its responses. Also if you use a spoofing IP address that is already used in your subnet there will be an "IP ad flict" and the attack will be easily noticed. Here are some examples of valid spoofing addresses:

Real IP address	Subnet Mask	Valid range for the spoofing IP address
192.168.0.1	255.255.255.0	Must be an unused address in the range 192.168.0.2 - 192.168.0.254
10.0.0.1	255.255.0.0	Must be an unused address in the range 10.0.0.2 - 10.0.255.254
172.16.0.1	255.255.255.240	Must be an unused address in the range 172.16.0.2 - 172.16.0.14
200.200.200.1	255.255.255.252	Must be an unused address in the range 200.200.200.2 - 200.200.200.3

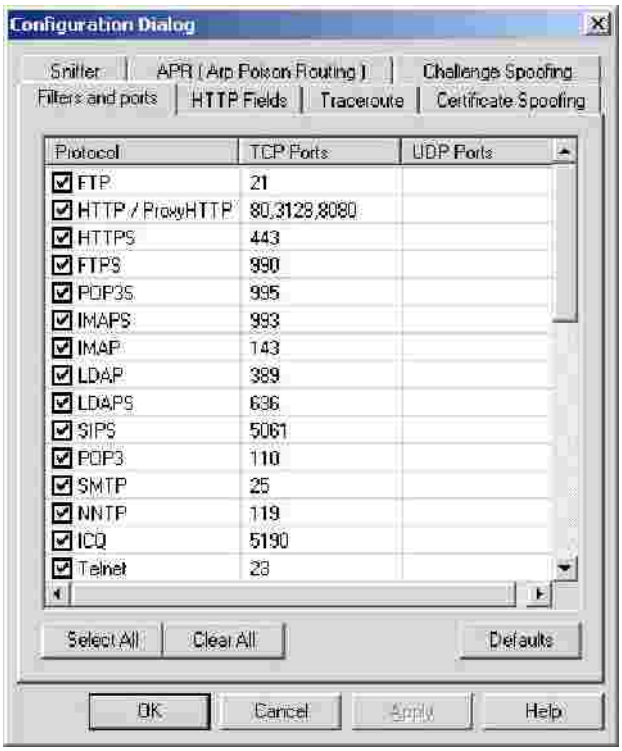
The spoofing IP address is automatically checked by the program when you press the "Apply" button, if the address is already in use in the subnet a message box will report the problem.

- The spoofing MAC address must not be present in your subnet. The presence of two identical MAC addresses on the same Layer-2 LAN can cause switches convergence problems; for this reason I decided to not let you easily set the spoofing MAC of your choice from the configuration dialog. The default value is set to 001122334455 which is an invalid address not supposed to exist in your network and that at the same time can be easily identified for troubleshooting. **IMPORTANT ! You cannot have, on the same Layer-2 network, two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address**. The spoofing MAC address can be changed modifying the registry value "SpoofMAC" at this location: "HKEY_CURRENT_USER\Software\Cain\Settings".

Filters and Ports Tab

Here you can enable/disable Cain's sniffer filters and application protocol TCP/UDP ports. Cain captures only authentication information not the entire content of each packet, however you can use the Telnet ter to dump, into a file, all the data present in a TCP session, modifying the relative filter port.

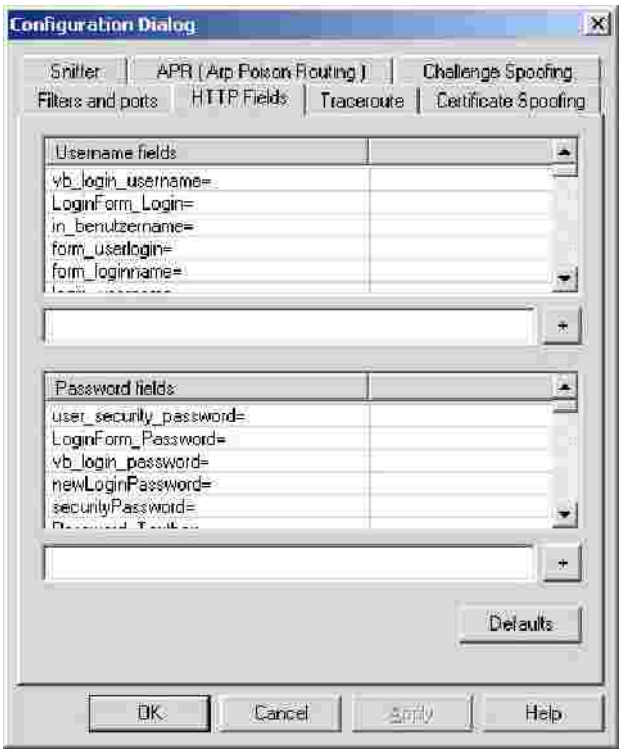
Cain's sniffer filters are internally designed to surv e in an unreliable world such as a network under ARP Poison attack; Cain uses different state machines to extract from network packets all the information needed to recover the plaintext form of a transmitted password. Some authentication protocols uses a challenge-response mechanism so it needs to collect parameters from Client->Server and Server->Client traffic; traffic interception in both directions is always possible if your Level-2 network is made by HUBs only or if you are connected o a mirror port on the switch but on switched networks in general, it can be achieved only using some kind of traffic hijacking technique such as Arp Poison Routing (APR). If you are sniffing with APR enabled, the sniffer will extract challenge-response authentications only if you reach a Full-Routing state between victim computers.



Under this tab you can also enable/disable the analysis of routing protocols (HSRP, VRRP, EIGRP, OSPF, RIPv1, RIPv2) and the APR-DNS feature that acts as a DNS Reply Rewriter.

HTTP Fields Tab

This tab contains a list of user name and password fields to be used by the HTTP sniffer filter. Cookies and HTML Forms that travel in HTTP packets are examined in this way: for each user name field all the password fields are checked and if these two parameters are found, the credentials will be captured and displayed on the screen.



The following cookie uses the fields "logonusername=" nd "userpassword=" for authentication purposes; if you don't include these two fields in the above list the sniffer will not extract relative crede ials.

GET /mail/Login?domain=xxxxxx.xx&style=default&plain=0 HTTP/1.1
*Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */**
Referer: http://xxx.xxxxxxx.xx/xxxxx/xxxx
Accept-Language: it
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5 SV1; (R1 1.3); .NET CLR 1.1.4322)

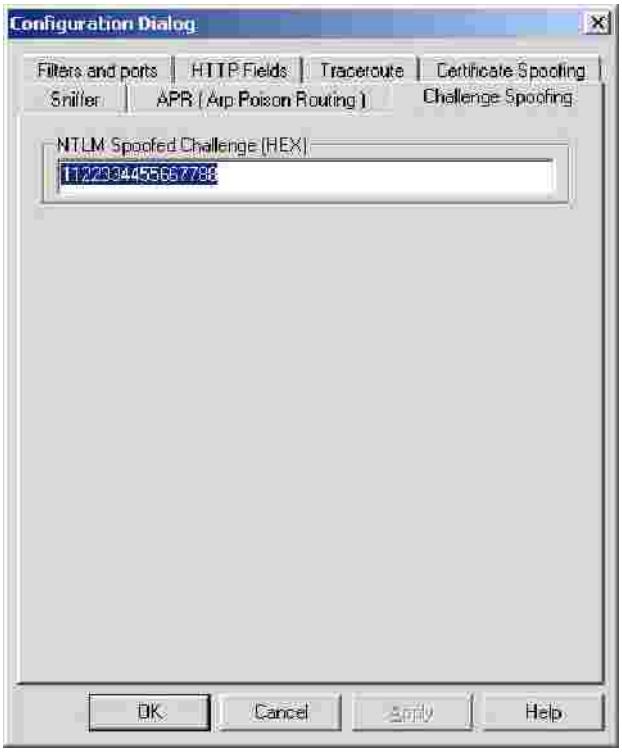
Host: xxx.xxxxxx.xx
Connection: Keep-Alive
Cookie: ss=1; logonusername=user@xxxxxx.xx; ss=1; srclng=it; srcdmn=it; srctrg=_blank; srcbld=y; to=on; srcclp=on; srcsct=web; userpassword=password; video=c1; TEMPLATE=default;

Traceroute Tab

This is used to configure Cain's ICMP/UDP/TCP traceroute. You can set to resolve host names, use ICMP Mask discovery and enable/disable WHOIS information extraction for each hop.

Challenge Spoofing Tab

Here you can set the custom challenge value to rewrite into NTLM authentications packets. This feature can be enabled quickly from Cain's toolbar and must be used with APR. A fixed challenge enables cracking of NTLM hashes captured on the network by mean of RainbowTables.



Certificate Spoofing Tab

This configuration page let you choose the type of fak certificates, created by Certificate Collector, to be used by APR-SSL based sniffer filters during MitM attacks.
You can choose to create self-signed or chained fake certificates signed by a truste root one. The "Certificate conversion" utility can be used to easily convert a certificate file from PKCS#12 (*.pfx or *.p12) format to PEM (*.crt).