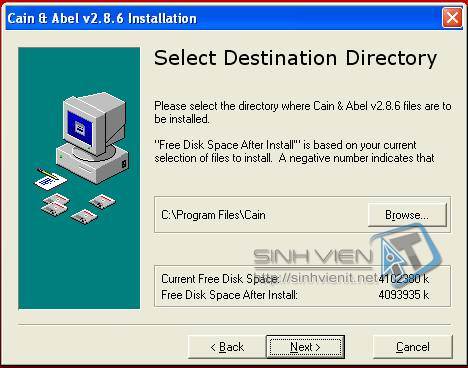
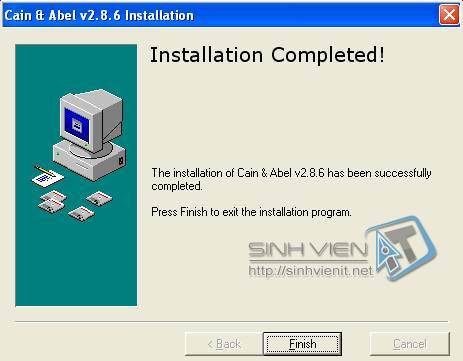
*Sơ Lược Quá trình hoạt động*  
  
Trên cùng một mạng, Host A và Host B muốn truyền tin cho nhau, các Packet sẽ được đưa xuống tầng Datalink để đóng gói, các Host phải đóng gói MAC nguồn, MAC đích vào Frame. Như vậy trước khi quá trình truyền Dữ liệu, các Host phải hỏi địa chỉ MAC của nhau.   
Nếu như Host A khởi động quá trình hỏi MAC trước, nó sẽ gởi broadcast gói tin ARP request cho tất cả các Host để hỏi MAC Host B, lúc đó Host B đã có MAC của Host A, sau đó Host B chỉ trả lời cho Host A MAC của Host B(ARP reply ).   
  
Có 1 Host C liên tục gởi ARP reply cho Host A và Host B địa chỉ MAC của Host C, nhưng lại đăt địa chỉ IP là Host A và Host B. Lúc này Host A cứ nghĩ máy B có MAC là C. Như vậy các gói tin mà Host A gởi cho Host B đều bị đưa đến Host C, gói tin Host B trả lời cho Host A cũng đưa đến Host C. Nếu Host C bật chức năng forwarding thì coi như Host A và Host B không hề hay biết rằng mình bị tấn công ARP 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Ví dụ :   
Ta có mô hình gồm các host   
  
Attacker : là máy hacker dùng để tấn công ARP   
IP : 10.0.0.11   
MAC : 0000.0000.1011   
  
Victim : là máy bị tấn công   
IP : 10.0.0.12   
MAC : 0000.0000.1012   
  
HostA   
IP : 10.0.0.13   
MAC : 0000.0000.1013   
  
- Đầu tiên, HostA muốn gởi dữ liệu cho Victim, cần phải biết địa chỉ MAC của Victim để liên lạc. HostA sẽ gởi broadcast ARP Request tới tất cả các máy trong cùng mạng LAN để hỏi xem IP 10.0.0.12 (IP của Victim) có địa chỉ MAC là bao nhiêu.   
  
- Attacker và Victim đều nhận được gói tin ARP Request, nhưng chỉ có Victim gởi trả lời gói tin ARP Reply lại cho HostA. ARP Reply chứa thông tin về IP 10.0.0.12 và MAC 0000.0000.1012 của Victim   
  
- HostA nhận được gói ARP Realy từ Victim, biết được địa chỉ MAC của Victim là 0000.0000.1012 sẽ bắt đầu thực hiện liên lạc truyền dữ liệu đến Victim. Attacker không thể xem nội dung dữ liệu được truyền giữa HostA và Victim   
  
Máy Attacker muốn thực hiện ARP attack đối với máy Victim. Attacker muốn mọi gói tin HostA gởi đến máy Victim đều có thể chụp lại được để xem trộm   
  
- Attacker thực hiện gởi liên tục ARP Reply chứa thông tin về IP của Victim 10.0.0.12, còn địa chỉ MAC là của Attacker 0000.0000.1011.   
  
- HostA nhận được ARP Reply nghĩ rằng IP Victim 10.0.0.12 có địa chỉ MAC là 0000.0000.1011. HostA lưu thông tin này vào bảng ARP Cache và thực hiện kết nối.   
  
- Lúc này mọi thông tin, dữ liệu HostA gởi tới máy có IP 10.0.0.12 (là máy Victim) sẽ gởi qua địa chỉ MAC 0000.0000.1011 của máy Attacker.   
  
  
**CAIN (Sử dụng phần mềm CAIN)**  
  
Phần mềm Cain là phần mềm sniffer khá hiệu quả hiện nay. Các tính năng của cain có thể cho phép sniffer được các thông tin bí mật trong hệ thống mạng LAN như passowrd e-mail, password dịch vụ ftp,telnet,….   
  
*1.Yêu cầu về phần cứng :*  
  
- ổ cứng cần trống 10 Mb   
- hệ điều hành Win 2000/2003/XP   
- cần phải có Winpcap   
  
*2. Cài đặt:*

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Chọn Next. 

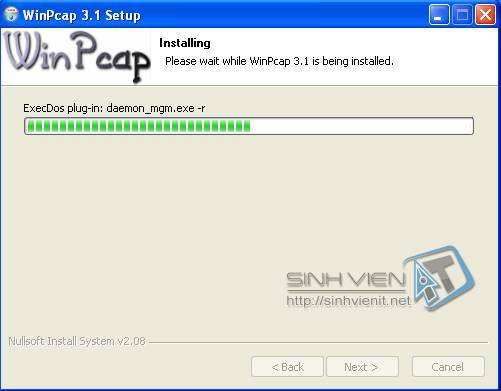
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

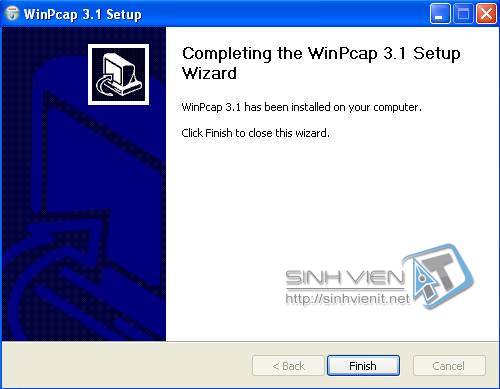
Chọn Next. 

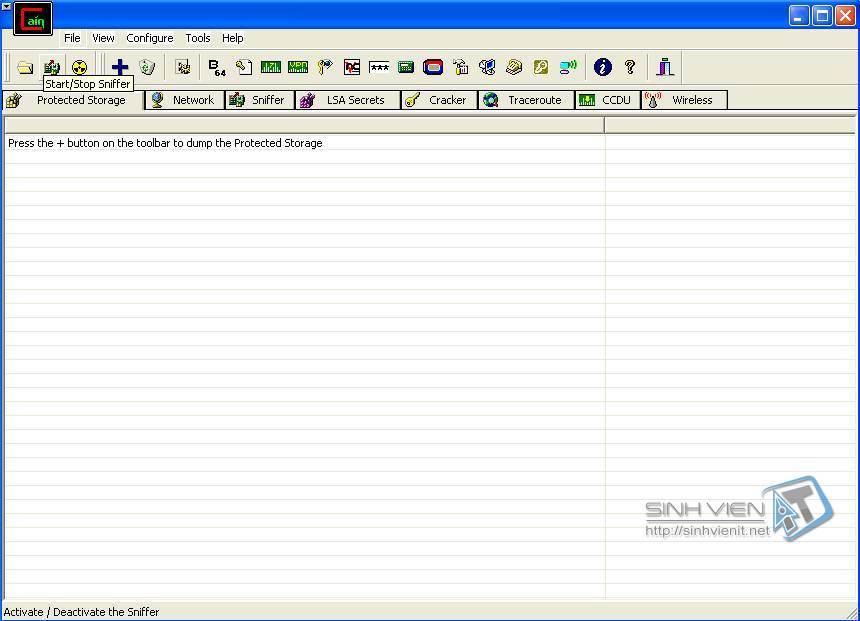
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Chọn Finish. 

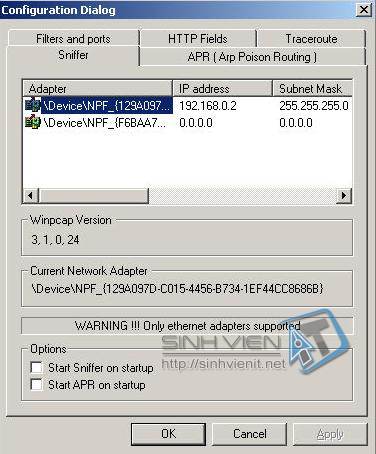
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

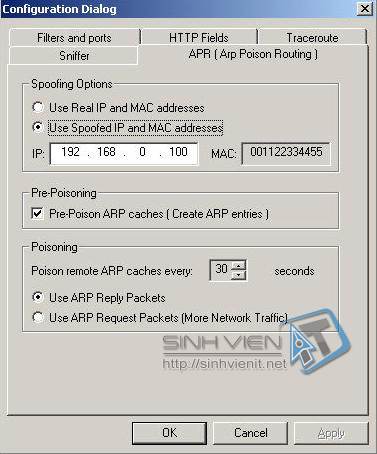
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

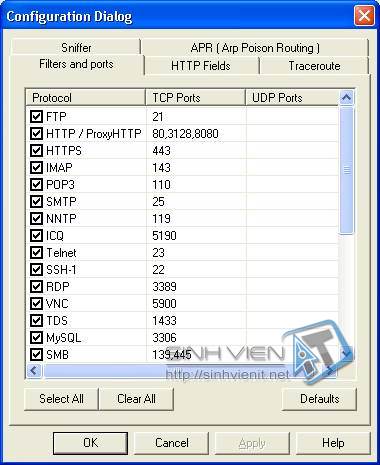
*3. Cấu hình*  
Cain & Abel cần cấu hình một vài thông số , mọi thứ có thể được điều chỉnh thông qua bảng Configuration dialog .   
Sniffer tab: 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

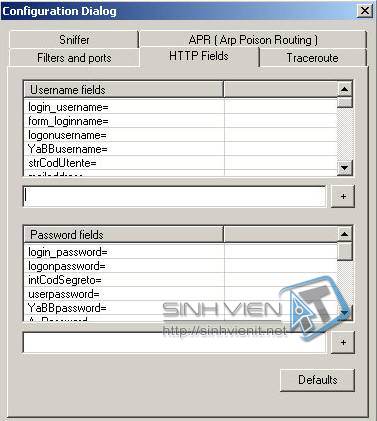
-Tại đây chúng ta chọn card mạng sử dụng để tiến hành sniffer và tính năng APR . Check vào ô Option để kích hoạt hay không kích hoạt tính năng.   
  
-Sniffer tương thích với Winpcap version 2.3 hay cao hơn . Version này hỗ trợ   
card mạng rất nhiều .   
**APR tab :**

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

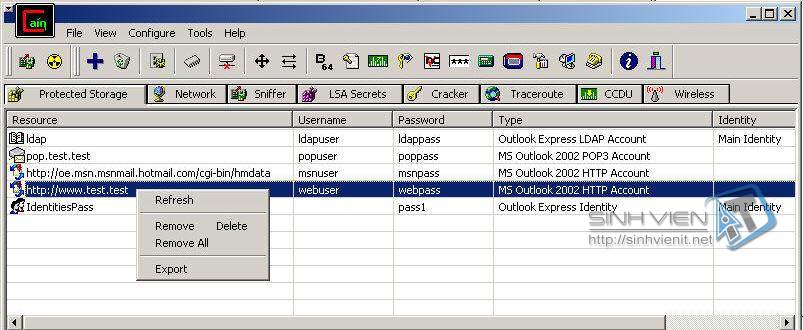
-Đây là nơi bạn có thể config ARP . Mặc định Cain ngăn cách 1 chuỗi gửi gói ARP từ nạn nhân trong vòng 30 giây . Đây thực sự là điều cần thiết bởi vì việc xâm nhập vào thiết bị có thể sẽ gây ra sự không lưu thông tính hiệu . Từ dialog này bạn có thể xác định thời gian giữa mỗi lần thực thi ARP, xác định thông số ít sẽ tạo cho ARP lưu thông nhiều ,ngược lại sẽ khó khăn hơn trong việc xâm nhập .   
  
*-Tại mục này, ta cần chú ý tới phần Spoofing Options:*  
+Mục đầu tiên cho phép ta sử dụng địa chỉ MAC và IP thực của máy mà mình dang sử dụng.   
+Mục thứ hai cho phép sử dụng một IP và địa chỉ MAC giả mạo. (Lưu ý địa chỉ ta chọn phải không trùng với IP của máy khác) Khi click vào tab filters and ports, ta sẽ thấy một số thông tin về giao thức và các con số port tương ứng với giao thức đó. 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

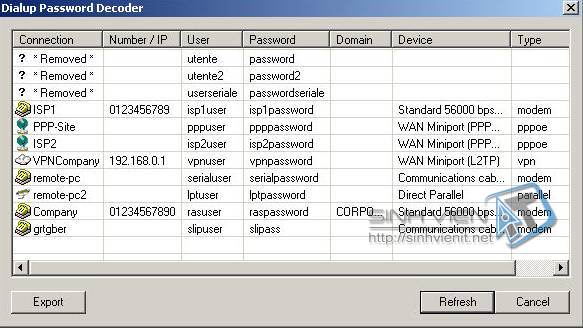
**Fliter and Ports Tab :**  
  
-Tại đây bạn có thể chọn kích hoạt hay không kích hoạt các port ứng dụng   
TCP/UDP .   
  
**HTTP fields tab :**

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

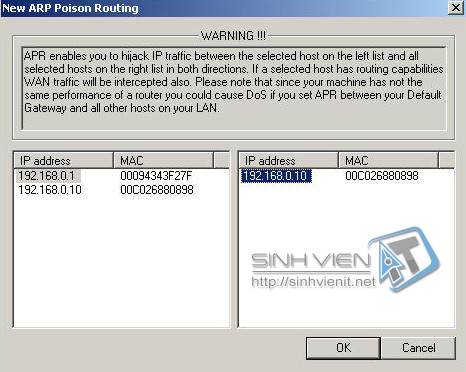
- Tại đây có 1 list danh sách username và password sử dụng được HTTP sniffer lọc lại.   
- Tại tab này cho phép ta biết dược chương trình này sẽ bắt 1 số thông tin về trang web như:   
+ Mục Username Fields: nó sẽ lấy thông tin những gì liên quan đến cái tên (user name, account, web name v.v..) .   
+ Mục Password Fields: lanh vực này sẽ đãm nhiệm vai trò lấy thông tin về password (login password, user pass, webpass v.v…)   
  
*4. Các ứng dụng của CAIN :*  
  
+ Bảo vệ password manager :   
  
Trước hết nó được sử dụng như 1 private key bảo mật một số vấn đề cho user . Hầu hết thông tin trong Protected Storage được mã hóa.Sử dụng như 1 key nhận được từ việc logon password của user.Cho phép điều hòa viêc truy cập thông tin để owner có thể an toàn truy xuất .   
  
Một vài ứng dụng của Windows có nét đặc trưng nên sử dụng dịch vụ này :   
Internet Explorer , Oulook , Oulook Express 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

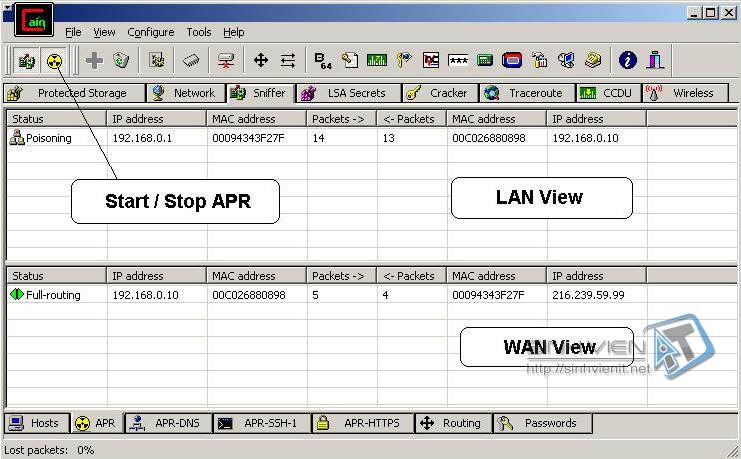
+ Giải mã password manager :   
Nó cho phép bạn đưa user names và passwords cho 1 tài nguyên mạng khác và 1 ứng dụng ,sau đó hệ thống tự động cung cấp thông tin về những sự viếng thăm thông tin mà bạn không can thiệp.   
  
+ LSA secrets dumper:   
LSA secrets thì sử dụng thông tin password cho accounts dùng để start một dịch vụ khác dữ liệu cục bộ. Dial Up và một số ứng dụng khác xác định password nằm ở đây .   
  
+ Giải mã password Dial-Up: 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

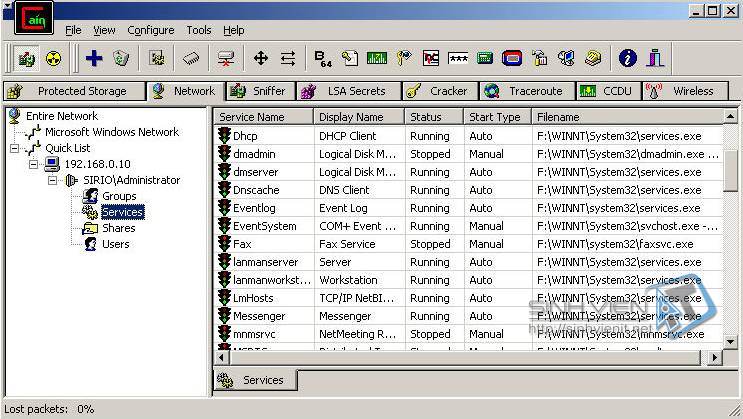
+APR:   
  
APR là nét đặc trưng chính của chương trình .Nó cho phép lắng nghe về các mạng chuyển mạch và sự tấn công lưu thông IP giữa các host . “APR poinsion routing” thực hiện : tấn công và định tuyến chính xác địa chỉ đích   
  
APR tấn công cơ bản thông qua thao tác của host ARP.Trên 1 địa chỉ IP hay Ethernet khi mà 2 host muốn truyền tin lẫn nhau thì phải biết địa chỉ MAC addresses của nhau. Host gốc thấy bảng ARP nếu mà ở đây có 1 MAC addresses tương ứng với địa chỉ IP addresses của nó. Nếu không, nó là địa chỉ broadcasts ,một lời yêu cầu ARP hỏi địa chỉ MAC của địa chỉ đích. Bởi vì gói thông tin này được gửi trong miền broadcasts, nó sẽ đi đến những cái host cùng subnet , tuy nhiên host với IP address trên lý thuyết khi nhận được yêu cầu sẽ trả lời lại địa chỉ MAC gốc của nó. Trái lại nếu ARP-IP tiếp cận địa chỉ   
đích của host thì nó sẵn sàng đưa ra soure host trên ARP cache. Điều này sẽ được dùng để phát sinh lưu thông ARP   
  
*Config :*  
Cần chỉnh 1 vài thông số, điều này có thể thực hiện được bằng việc chỉ rõ việc bắt chước MAC và IP addresses bằng việc sử dụng ARP poision packets .   
Điều này thật sự khó khăn khi không để lại vết tích của việc tấn công bởi vì người tấn công thực tế không bao giờ gửi địa chỉ qua lại trên mạng.Trên mạng người tấn công lúc nào cũng lén lúc ở giữa để quan sát 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

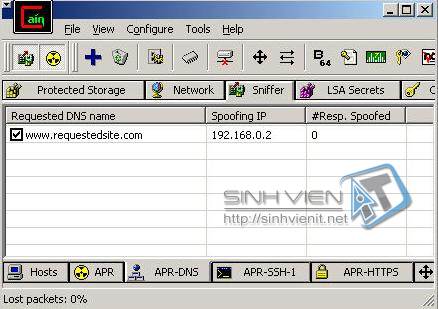
Hình ở trên là ta muốn tấn công ip từ 192.168.0.1 ? 192.168.0.10 .Công việc tiến hành theo cơ chế Người ở giữa , chương trình sẽ thực hiện 1 sự tấn công ARP poision , CAIN có thể phát triển sự tấn công bộ nhớ Của nhiều host trong khoảng thời gian như nhau, bạn cần chọn 1 địa chỉ ở ô bên trái 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

+ Service manager : ta có thể start/stop ,pause/continued hay remove bất cứ 1 dịch vụ nào có trên cửa sổ giao diện 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

+ Sniffer : 

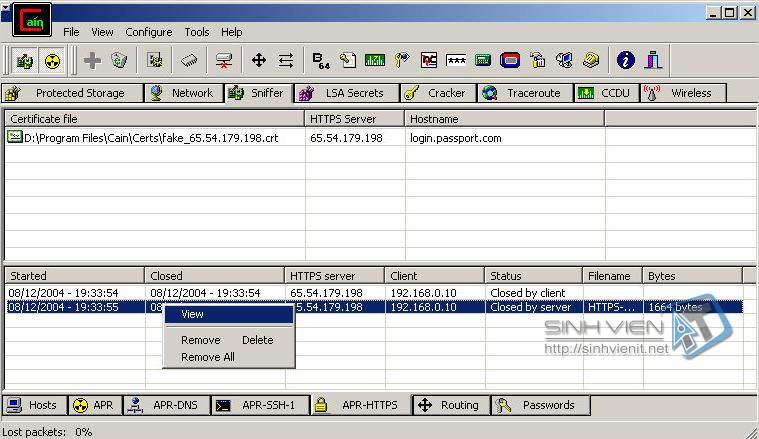
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

ARP-DNS :   
Nét đặc trưng ở đây là cho phép DNS tiến hành giả mạo thành 1 DNS-reply để có thể tấn công . 

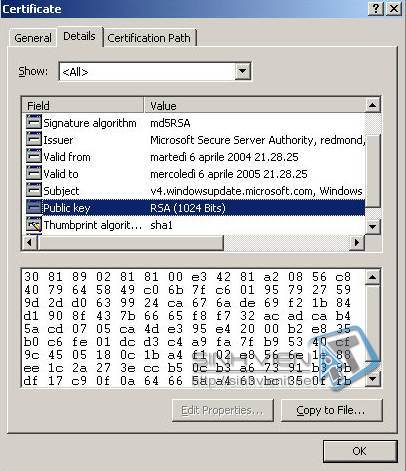
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

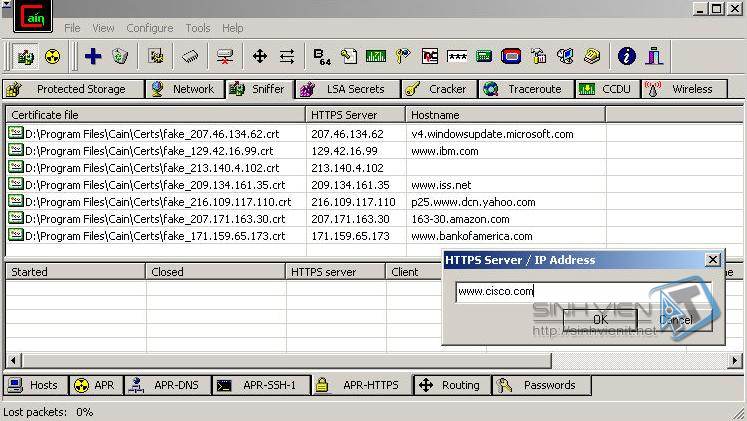
ARP-DNS dễ dàng tạo ra 1 ip address trên DNS-reply .Sniffer dễ dàng rút ra được tên yêu cầu từ gói dữ liệu kết hợp với việc thấy được địa chỉ trên bảng danh sách.Ở đây gói dữ liệu sẽ được chỉnh lại IP address để sau đó re-route đi .Lúc này client sẽ bị đánh lừa để ta dễ dàng biết được địa chỉ đích .   
  
ARP-HTTPS :   
ARP-HTTPS cho phép việc bắt gói và giải mã trong sự lưu thông của HTTPS giữa các host . Đây là công việc kết hợp với công cụ Certificate Collector . Khi mà nạn nhân Start HTTPS trình duyệt của anh ta sẽ hiện lên po-pup báo động . 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

+ Certificates Collector : 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

***Nguồn:*** Trung tâm đào tạo an ninh mạng ATHENA