HƯỚNG DẪN XÁC ĐỊNH KHOANH VÙNG

MÁY TÍNH NHIỄM MÃ ĐỘC

Trường hợp này áp dụng cho địa chỉ IP được dùng bởi nhiều máy con, ví dụ IP được dùng cho LAN truy cập Internet,…

Các trường hợp được hướng dẫn có sơ đồ mạng thuộc các trường hợp:

1. Tất cả máy con sử dụng IP đi qua máy cài đặt các dịch vụ DNS, ISA, IPTABLES,...

2. Tất cả máy con sử dụng IP đi qua ROUTER, SWITCH có cổng MONITOR, SPAN.

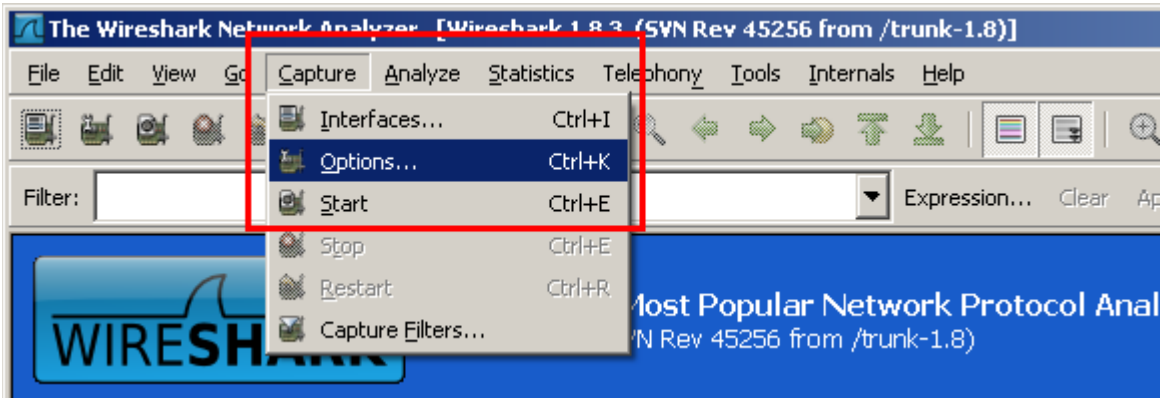
3. Trường hợp khác.

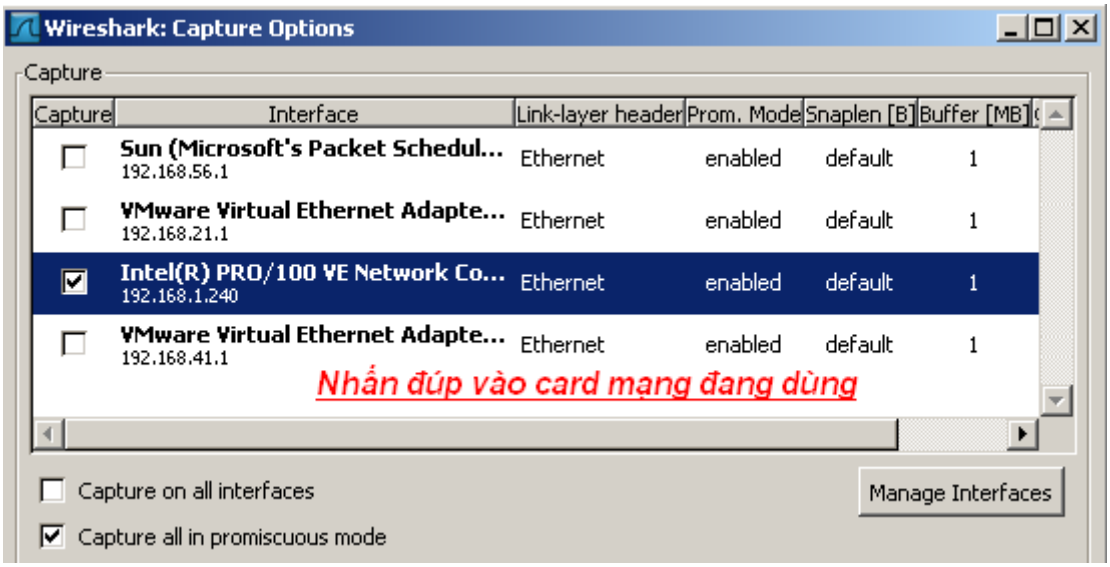
<u>TRƯỜNG HỢP 1</u>: Số lượng máy con lớn hơn 10 và tất cả máy con đi qua máy tính cài đặt dịch vụ nào đó. Ví dụ DNS, ISA, IPTABLES,…

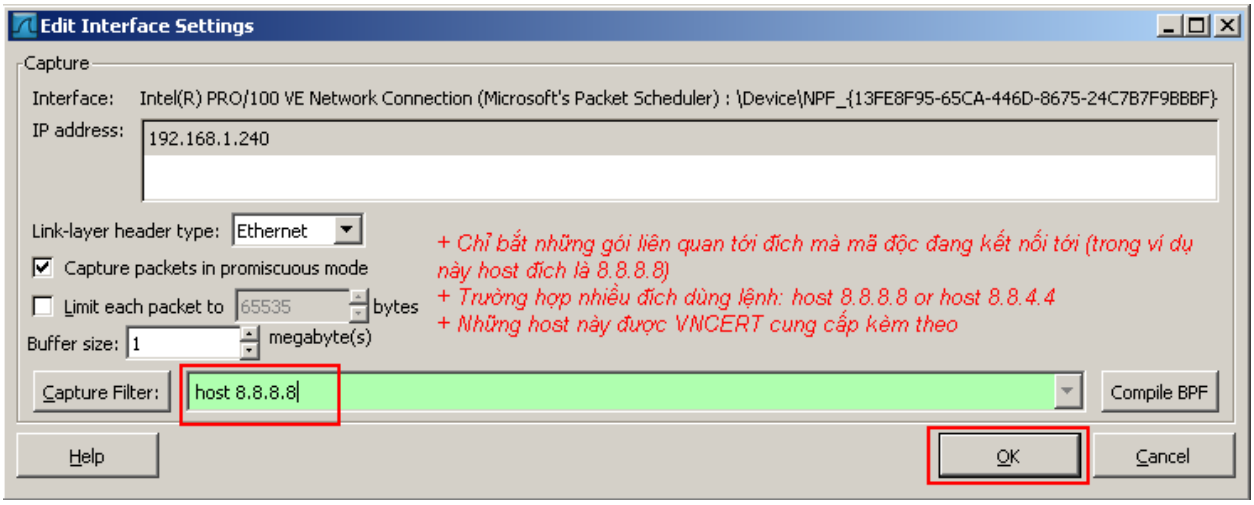
1. **Đối với Hệ điều hành Windows (ISA, DNS,…):**

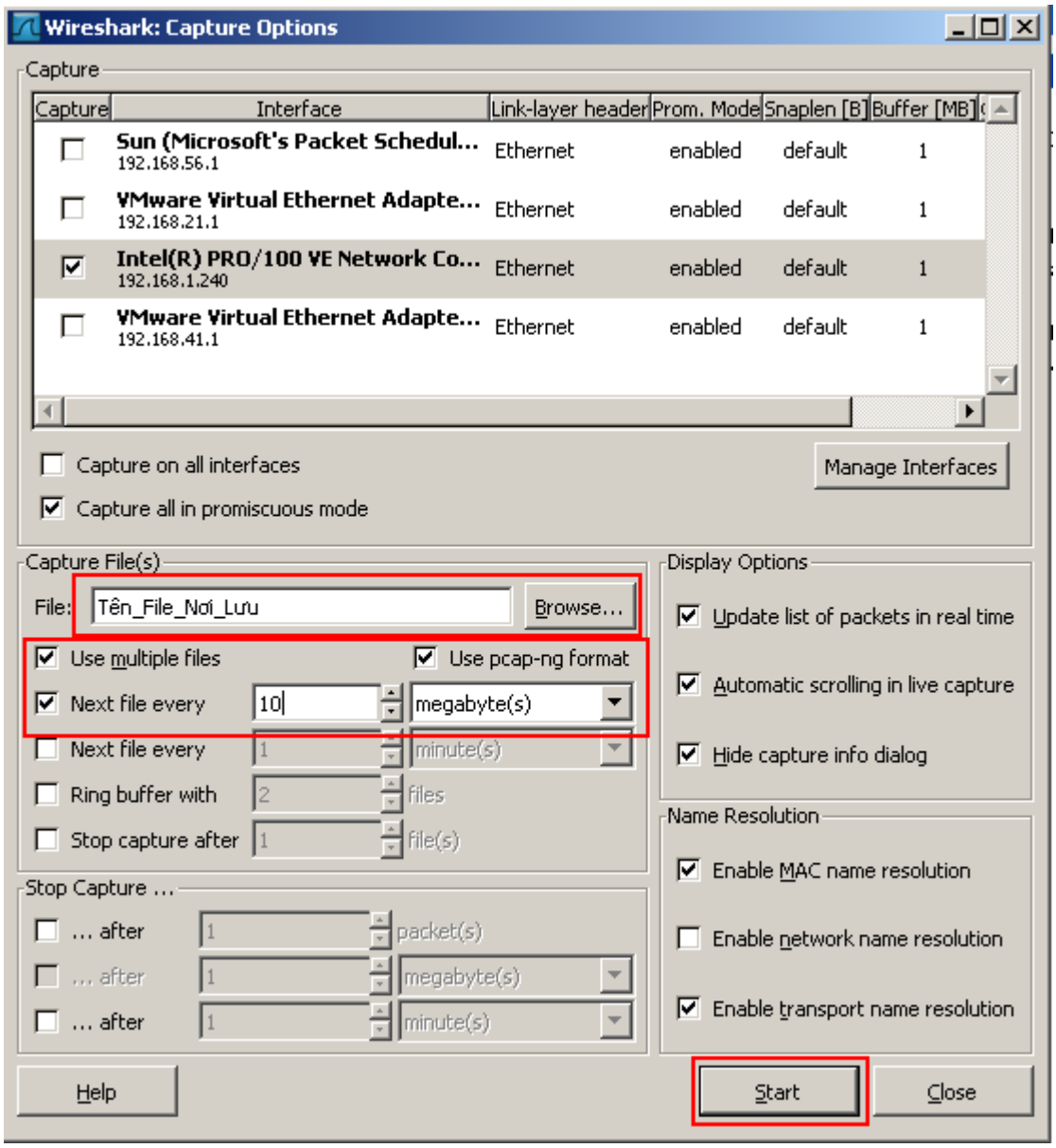
   + Cài đặt **Wireshark** được tải tại http://www.wireshark.org/download.html

   + Tiến hành bắt gói tin đi qua máy này. Xem hình dưới:




Wireshark: Capture Options
Capture
Capture
Interface
Link-layer header
Prom. Mode
Snaplen [B]
Buffer [MB]
Sun (Microsoft's Packet Schedul...
192.168.56.1
Ethernet
enabled
default
1
VMware Virtual Ethernet Adapte...
192.168.21.1
Ethernet
enabled
default
1
Intel(R) PRO/100 VE Network Co...
192.168.1.240
Ethernet
enabled
default
1
VMware Virtual Ethernet Adapte...
192.168.41.1
Ethernet
enabled
default
1
Nhấn đúp vào card mạng đang dùng
Capture on all interfaces
Manage Interfaces
Capture all in promiscuous mode


Edit Interface Settings
Capture
Interface:
Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : \Device\NPF_{13FE8F95-65CA-446D-8675-24C7B7F9BBBF}
IP address:
192.168.1.240
Link-layer header type:
Ethernet
Capture packets in promiscuous mode
Limit each packet to
65535
bytes
Buffer size:
1
megabyte(s)
+ Chỉ bắt những gói liên quan tới đích mà mã độc đang kết nối tới (trong ví dụ này host đích là 8.8.8.8)
+ Trường hợp nhiều đích dùng lệnh: host 8.8.8.8 or host 8.8.4.4
+ Những host này được VNCERT cung cấp kèm theo
Capture Filter:
host 8.8.8.8
Compile BPF
Help
OK
Cancel



+ Nhấn **Start** để bắt đầu quá trình bắt gói tin. Nên nhớ ở hình cuối cùng, nếu lưu lượng quá lớn thì nên **bỏ dấu check** ở ô có dòng "*Update list of packets in real time*".

+ Nếu **không có** gói tin nào thuộc lọc trên thì có thể cắm máy cho chạy trong vòng 12 tiếng.

+ Nếu **có gói tin** nào hiện lên thì chỉ cần bắt trong vòng 10 phút. Địa chỉ IP con đang thực hiện kết nối chính là IP nhiễm Botnet.

2. **Đối với Hệ điều hành Linux (IPTABLES, DNS,…):**

+ Kết nối vào SSH hoặc đăng nhập trực tiếp trên máy đó với quyền root.

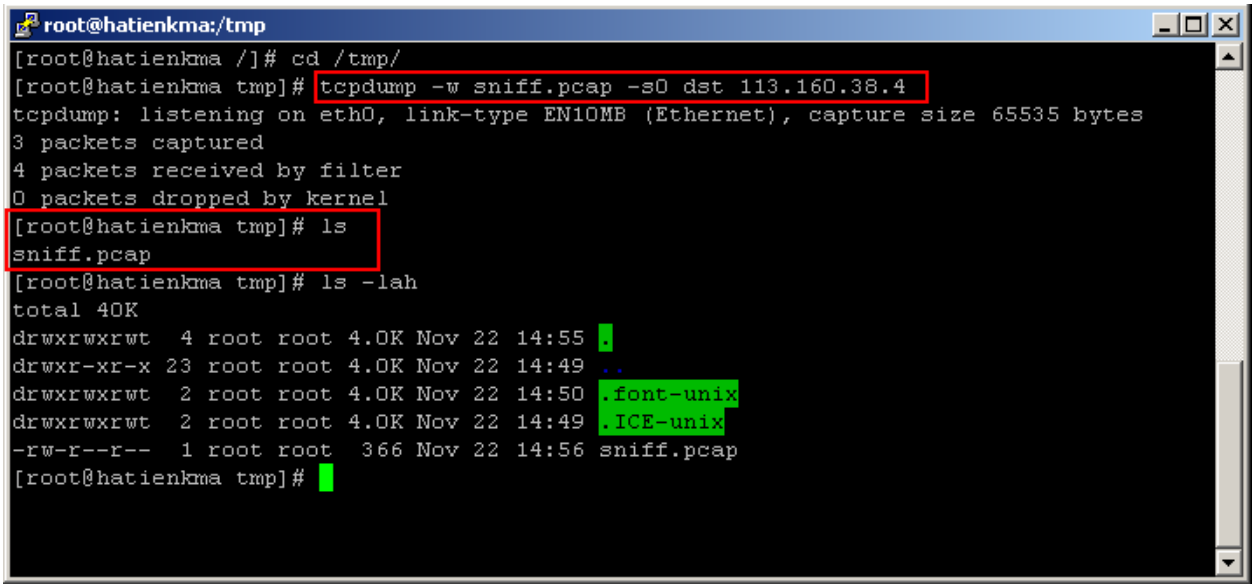
+ Nếu chưa cài đặt tcpdump thì dùng lệnh "*yum –y install tcpdump*" để cài.

+ Nếu đã cài (đa số đã cài) tcpdump thì dùng lệnh sau để bắt gói tin

"***tcpdump -w sniff.pcap -s0 dst 113.160.38.4***".

Trong đó *113.160.38.4* là host. Địa chỉ này VNCERT sẽ cung cấp trong quá trình cảnh báo.

Sau 15 phút nhấn ***Ctrl + C*** để thoát và tiến hành phân tích. Nếu có máy con kết nối tới địa chỉ đích đã cung cấp thì địa chỉ máy đó chính là địa chỉ máy tính bị nhiễm.

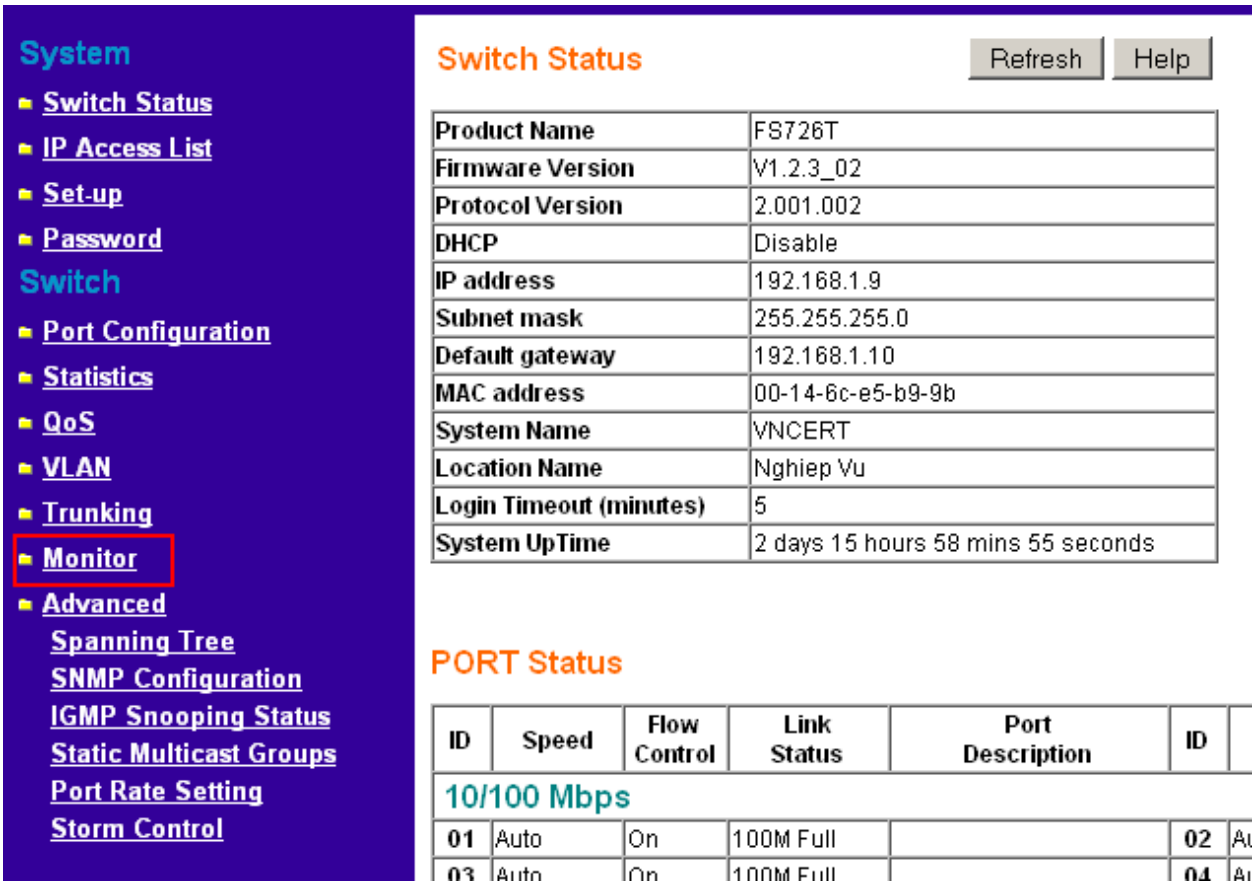


<u>TRƯỜNG HỢP 2</u>: Số lượng máy con lớn hơn 10 và tất cả máy con đi qua ROUTER hay SWITCH có cổng MONITOR hay SPAN.

Cổng MONITOR hay SPAN là cổng mà có nhiệm vụ giữ 1 bản copy của các gói tin đi ra vào trong Switch.

+ Trường hợp này là phổ biến. Cách cấu hình phải là người am hiểu về kỹ thuật. Ví dụ dưới đây hướng dẫn cấu hình Switch.

+ Login vào quản lý Switch có giao diện (các loại khác tương tự).



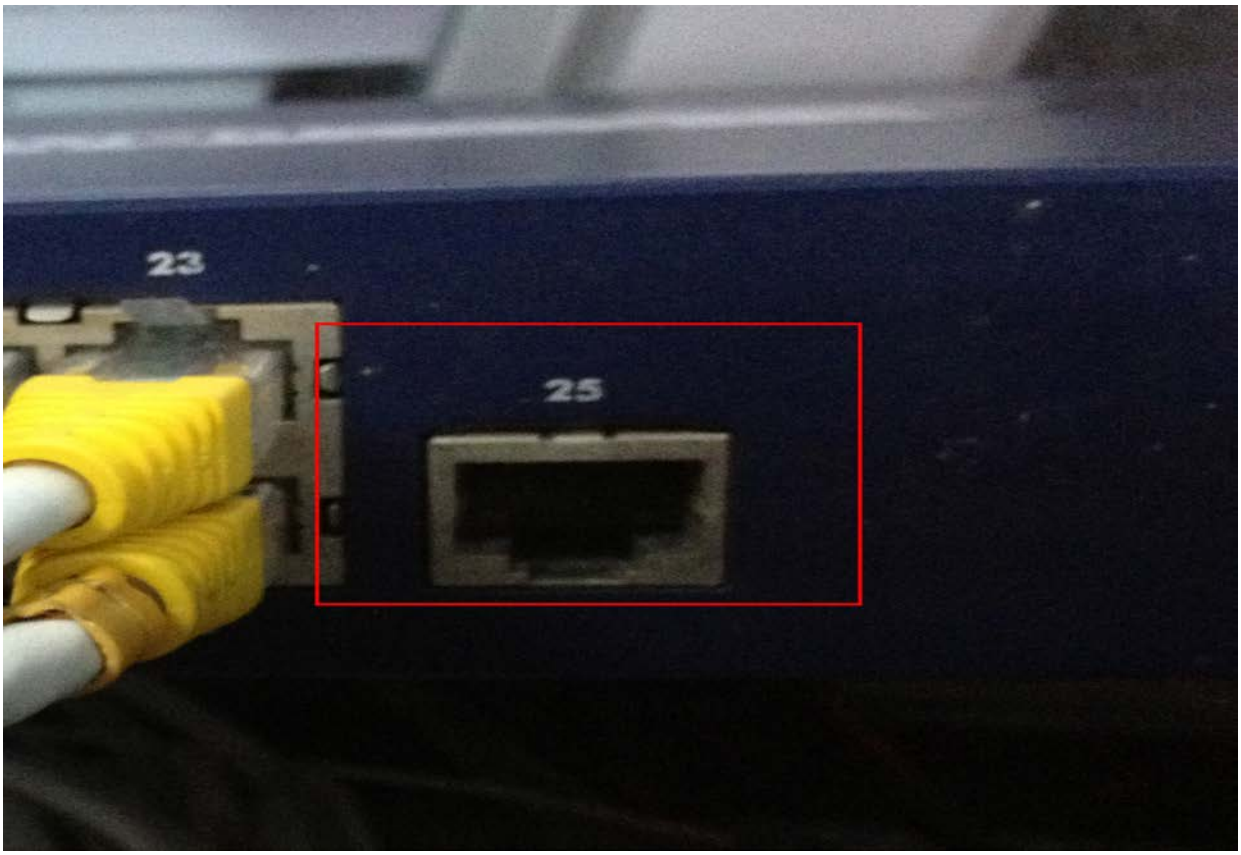
+ Ví dụ lấy cổng số 25 trên Switch làm cổng Monitor:

Monitor Setting

Group 1	Sniffer Mode	Both
	Sniffer Port	25
	Source Port	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

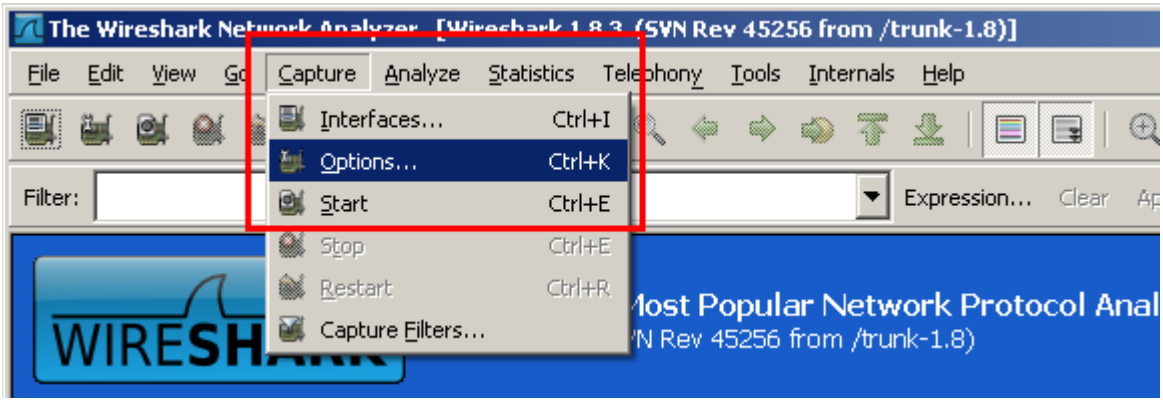
Apply Help

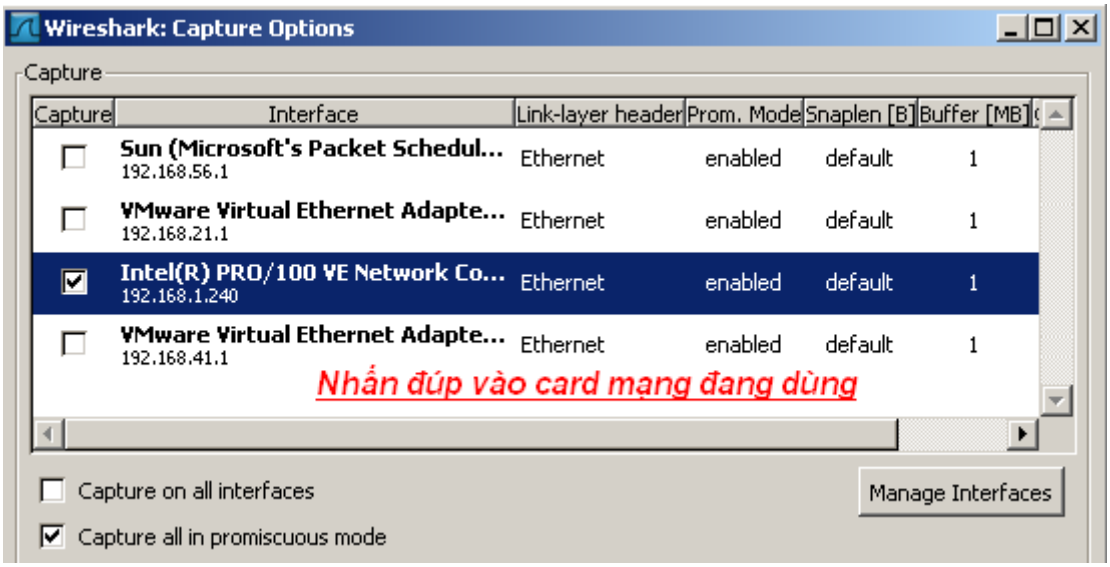
+ Sau khi cấu hình xong, nhìn vào Switch (hình dưới) chúng ta nối dây mạng vào cổng 25 và một máy tính có cài đặt Wireshark. Tiến hành bắt gói tin trên Wireshark theo hướng dẫn hình dưới.

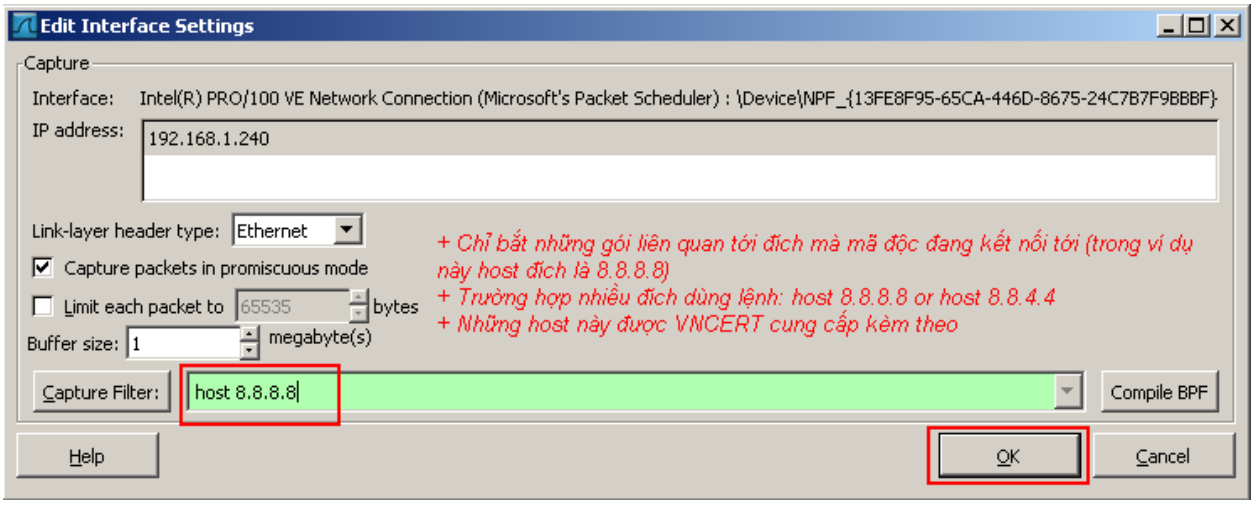


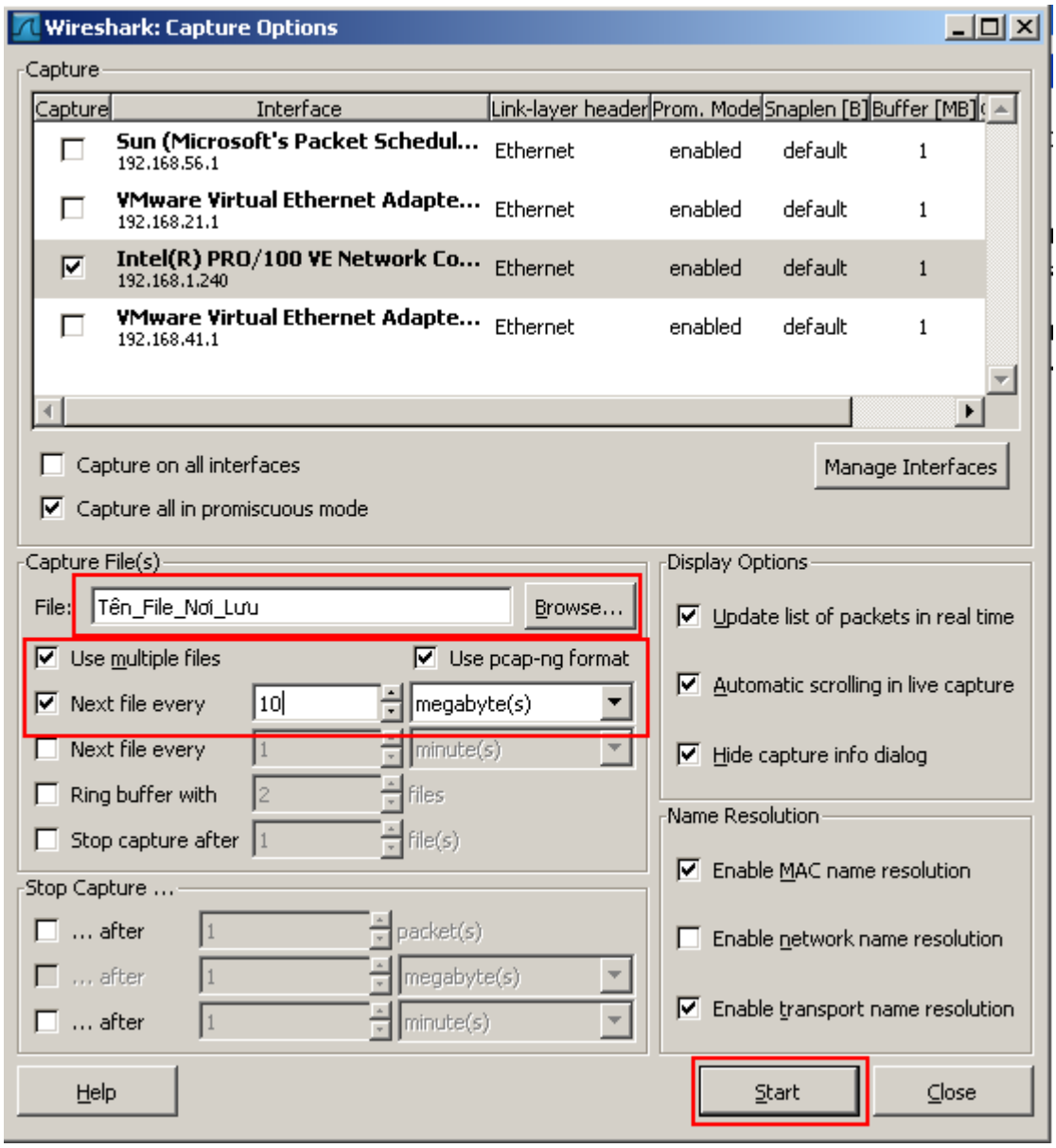
+ Cài đặt **Wireshark** được tải tại http://www.wireshark.org/download.html

+ Tiến hành bắt gói tin đi qua máy này. Xem hình dưới:









+ Nhấn **Start** để bắt đầu quá trình bắt gói tin. Nên nhớ ở hình cuối cùng, nếu lưu lượng quá lớn thì nên **bỏ dấu check** ở ô có dòng "*Update list of packets in real time*".

+ Nếu **không có** gói tin nào thuộc lọc trên thì có thể cắm máy cho chạy trong vòng 12 tiếng.

+ Nếu **có gói tin** nào hiện lên thì chỉ cần bắt trong vòng 10 phút. Địa chỉ IP con đang thực hiện kết nối chính là IP nhiễm Botnet.

<u>TRƯỜNG HỢP 3</u>: Trường hợp khác

Đối với trường hợp khác bao gồm không có các thiết bị trên hoặc cùng chung LAN, chúng ta sử dụng ARP Spoofing nhằm giả mạo địa chỉ IP gateway và điều hướng tất cả các máy trong LAN đi qua một địa chỉ máy đã giả mạo. Chi tiết xem tại video hướng dẫn: http://www.youtube.com/watch?v=4ZmYa_3UCVw

Notice: Thông tin hỗ trợ khác.

*

* * *

Trong quá trình lấy thông tin nếu chưa rõ hoặc cần hỗ trợ thì có thể:

a. *Support qua Yahoo ID**: hatienkma***

b. *Số điện thoại: **0986.334.358***

c. *Email: **hvtien@vncert.vn***