Introduction to Wireshark

By

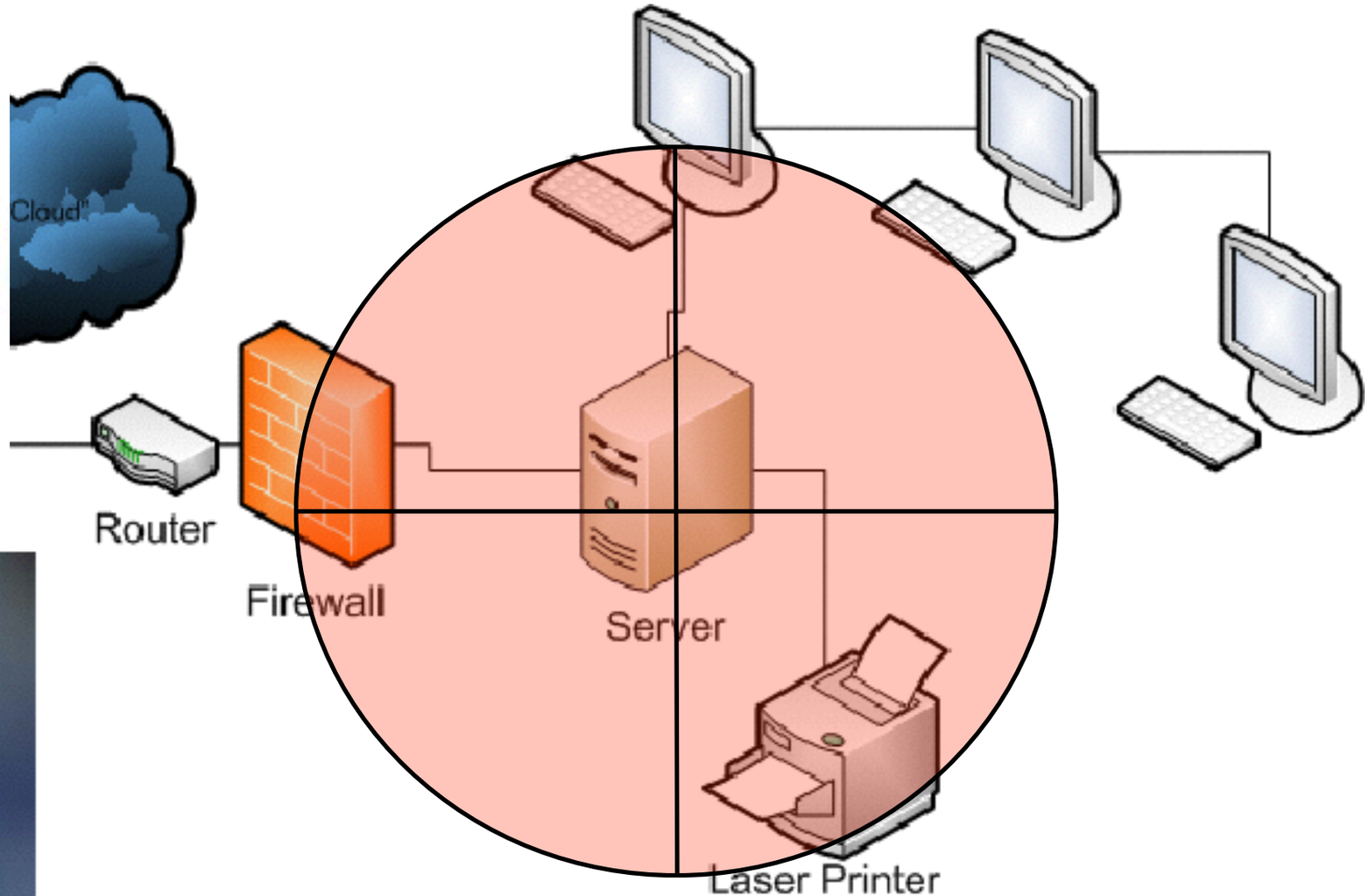
Kitisak Jirawannakool

E-Government Agency (Public Organization)

Agenda

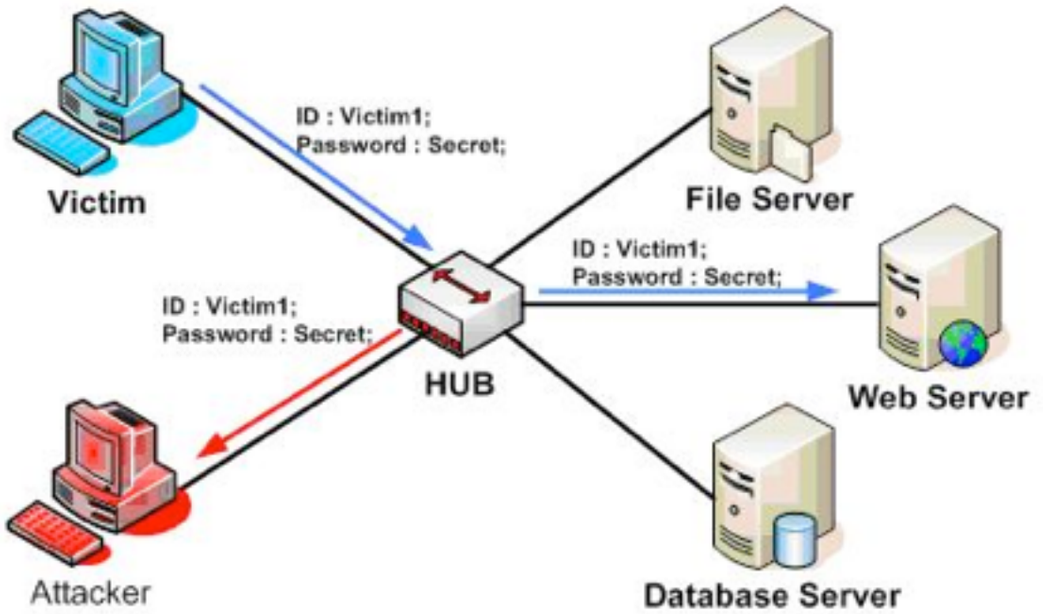
- What is Network monitoring?
- Why we need?
- About wireshark?
- Demo
- Exercises

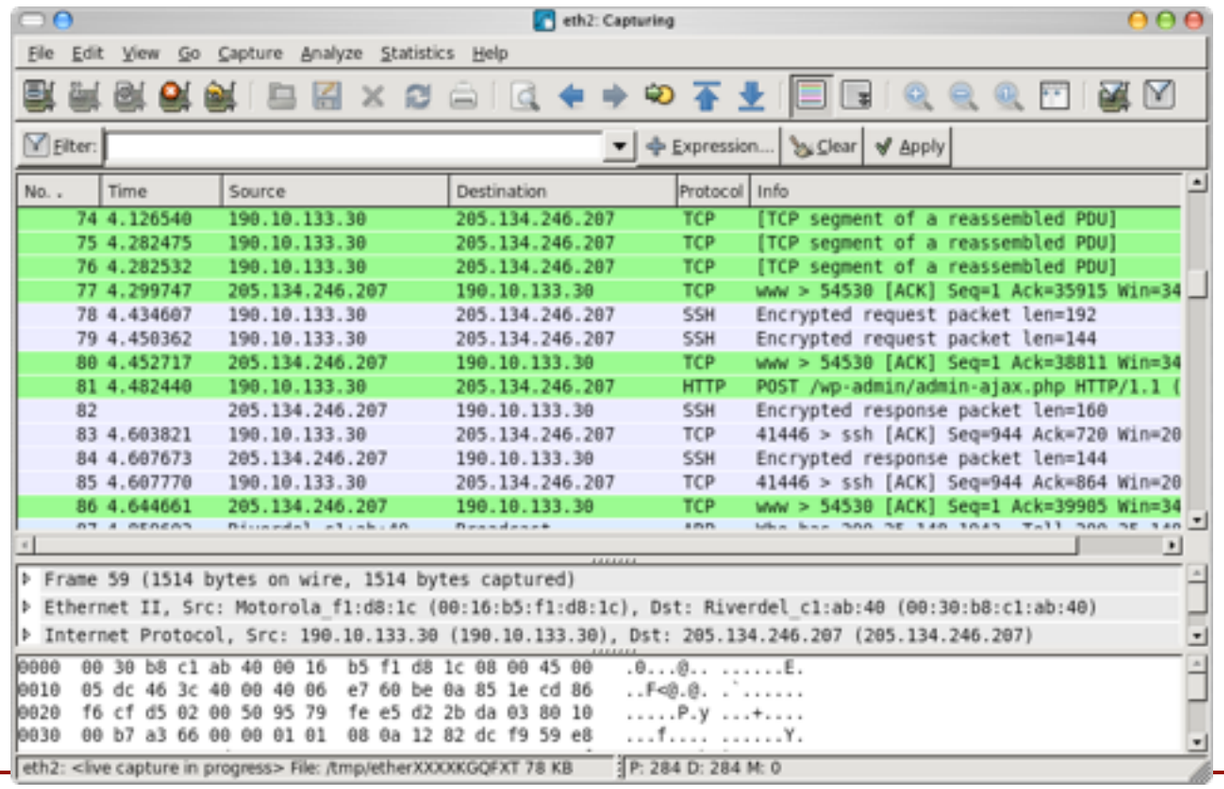
What is Network Monitoring?



Eavesdropping

Network Eavesdropping





Why we monitor?

- Network Capacity Design
  - Do we have to purchase ADSL or Lease line?
- Performance Monitoring
  - Fast enough? Too Slow?
  - Packet losses?
- Maintain Security
  - Malware (Bot, Key logger)
  - Insider threat (Policy violation)

EGA
e-Government Agency

G-CERT by EGA

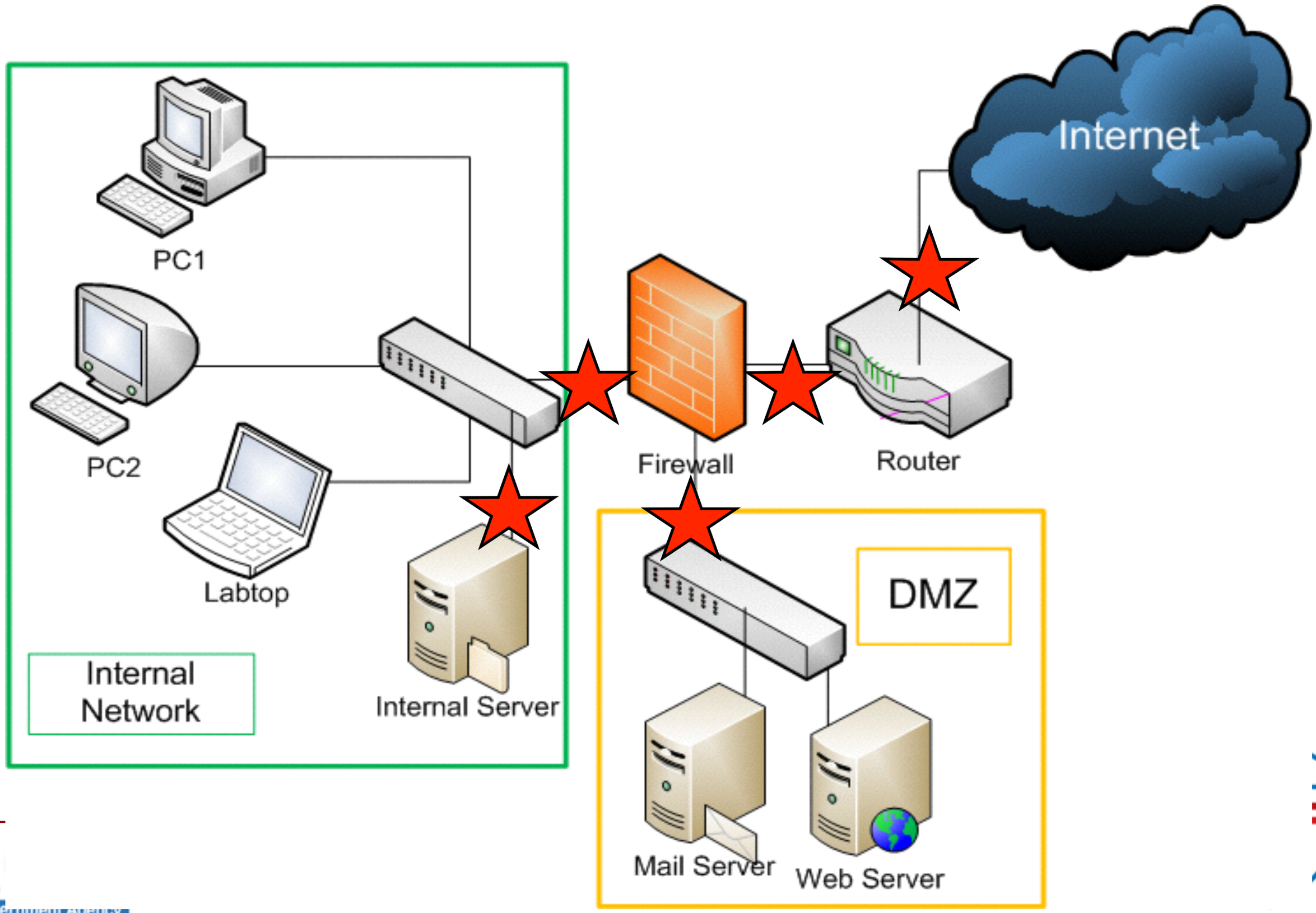
What kind of information we need?

Purpose	Tech	Tool ex)	Note
Traffic accounting	SNMP	MRTG	
Intrusion Detection	IDS	snort	False positive/netgative issue
Full content	Packet capture	tcpdump libpcap	Be aware, it may contains private data
Sessions statistics	netflow	Nfdump, nfsen	
Log	Files on Firewalls servers	Many	Log level configuration is a KEY.

How to monitor the network?

- Using monitoring agent
  - software/tools
  - port mirroring on network switch or router
    - aggregate all traffic that are processed by a network switch into one single port.
  - use shared hub
    - Shared hub is more expensive than a switching hub!!!
  - network tap
    - Can be installed without modifying your network design.

Where to monitor?



Where to monitor?

- Out side of Firewall
  - To understand what is going on the side of "THE INTERNET".
  - Research purpose.
  - Since it's a chaotic world, you will see too many suspicious flow.
- DMZ
  - To understand threat by external attack
- Local network
  - Monitor traffic within your corporate network
  - Prevent information leakage

What we can't do with network monitor?

- Monitor Encrypted traffic SSL, IPSec, SSH, HTTPS, and other
- Active protection
  - Network monitoring is Not for protect, not for filter, just watching what's in and out
  - Network monitoring system may not send any packet
- Monitor Huge traffic
  - Difficult to monitor everything because of tons of traffic
- Finding Targeted Attacks

Legal and Privacy

- We should be sure if network monitoring is clear to do by aspect of
  - Legal
    - Checking only in your country is enough ?
    - Any branches in other countries…
  - Privacy
    - Full traffic monitoring may contain privacy data
      - E-mail contents
      - Web history
      - Password

Legal and Privacy

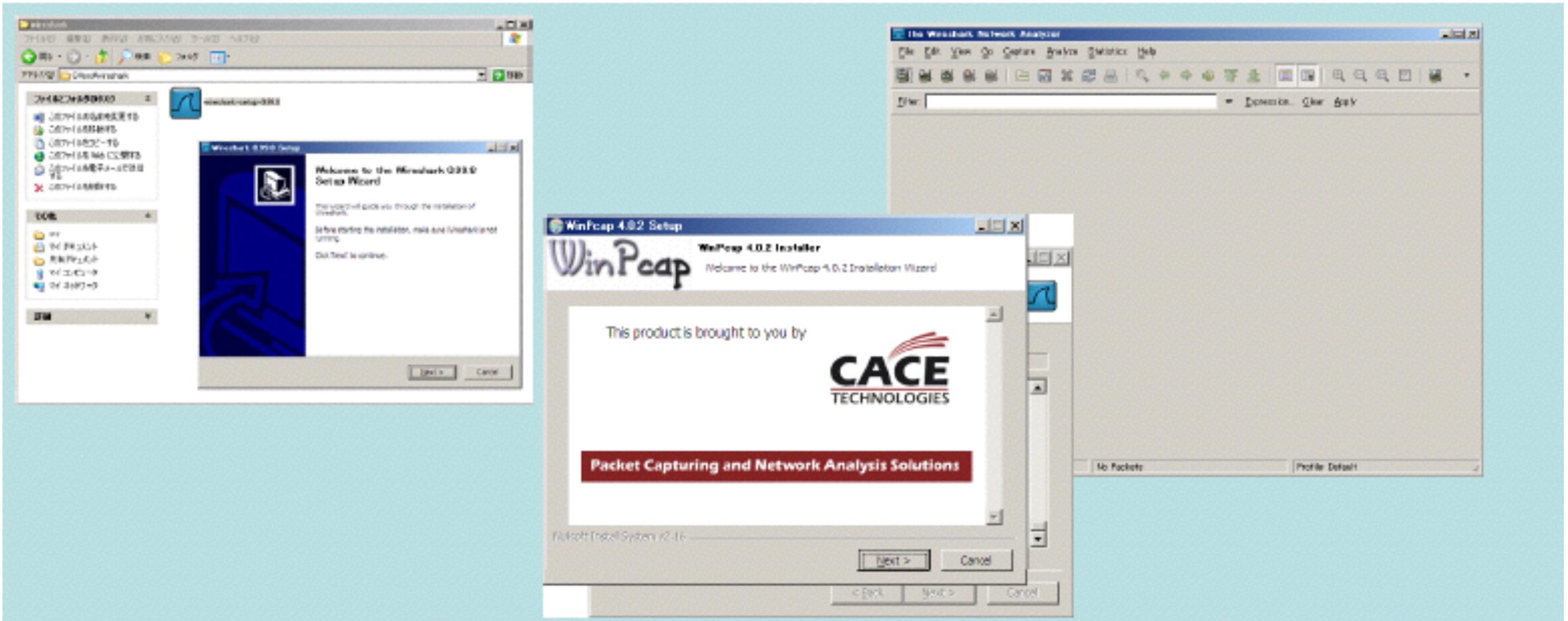
- Organizational Policy
  - Advertise that you are monitoring network
  - For users
- Ethic
  - Some cases, we can monitor neighborhood wireless traffic…
  - Is hotel wireless/network

About WireShark

- Formerly known as “Ethereal”
- Free
- Official website :http://www.wireshark.org
- Requirement
  - Need to install winpcap
  - Some Windows Need Administrator privilege to capture
- GUI - AHA!!!!!!!!!!!

How to Install

- Very straight forward
- Just double-click and follow the instructions



How to capture

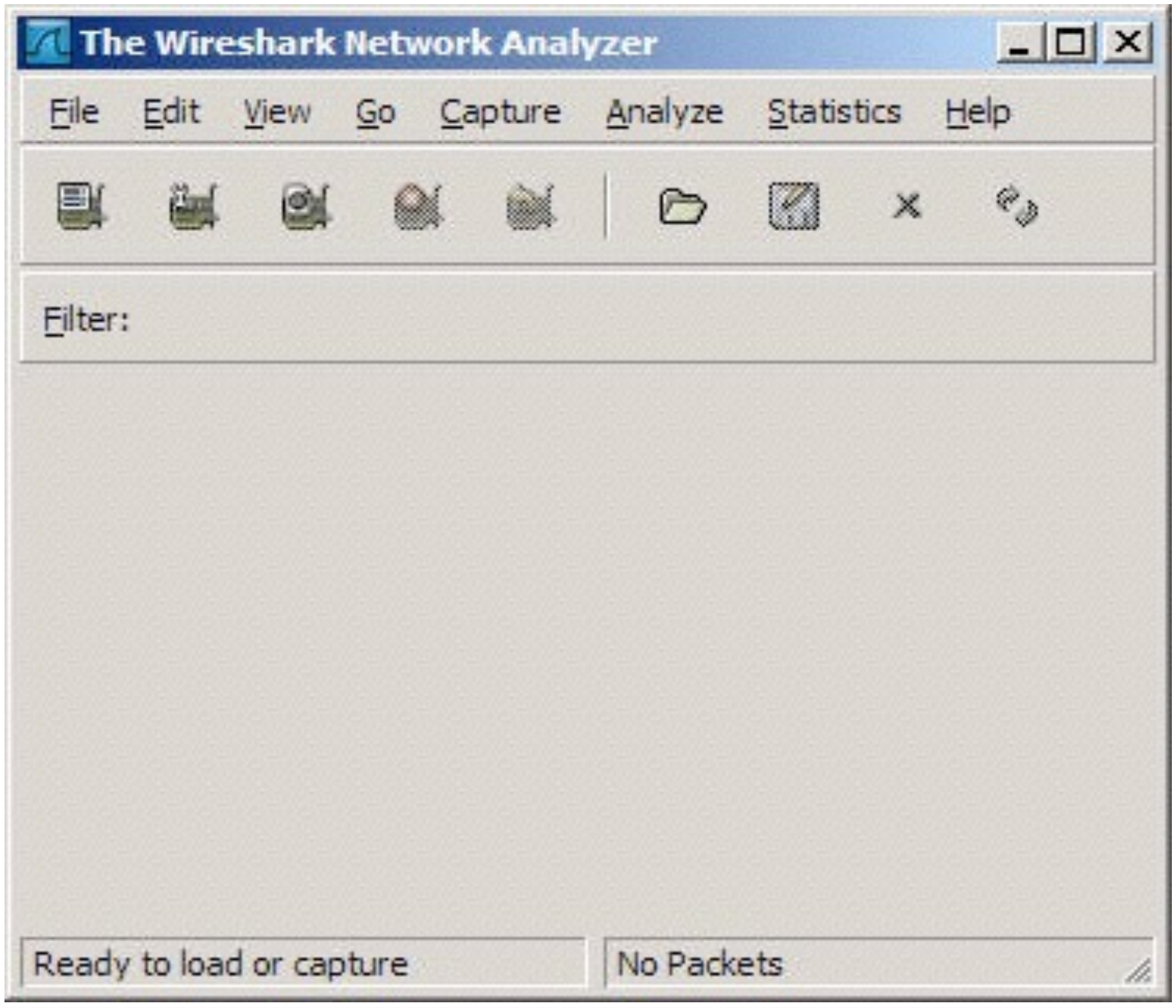
- What is Promiscuous mode?
- Capture filters
- Display option
- Name resolution

Filters

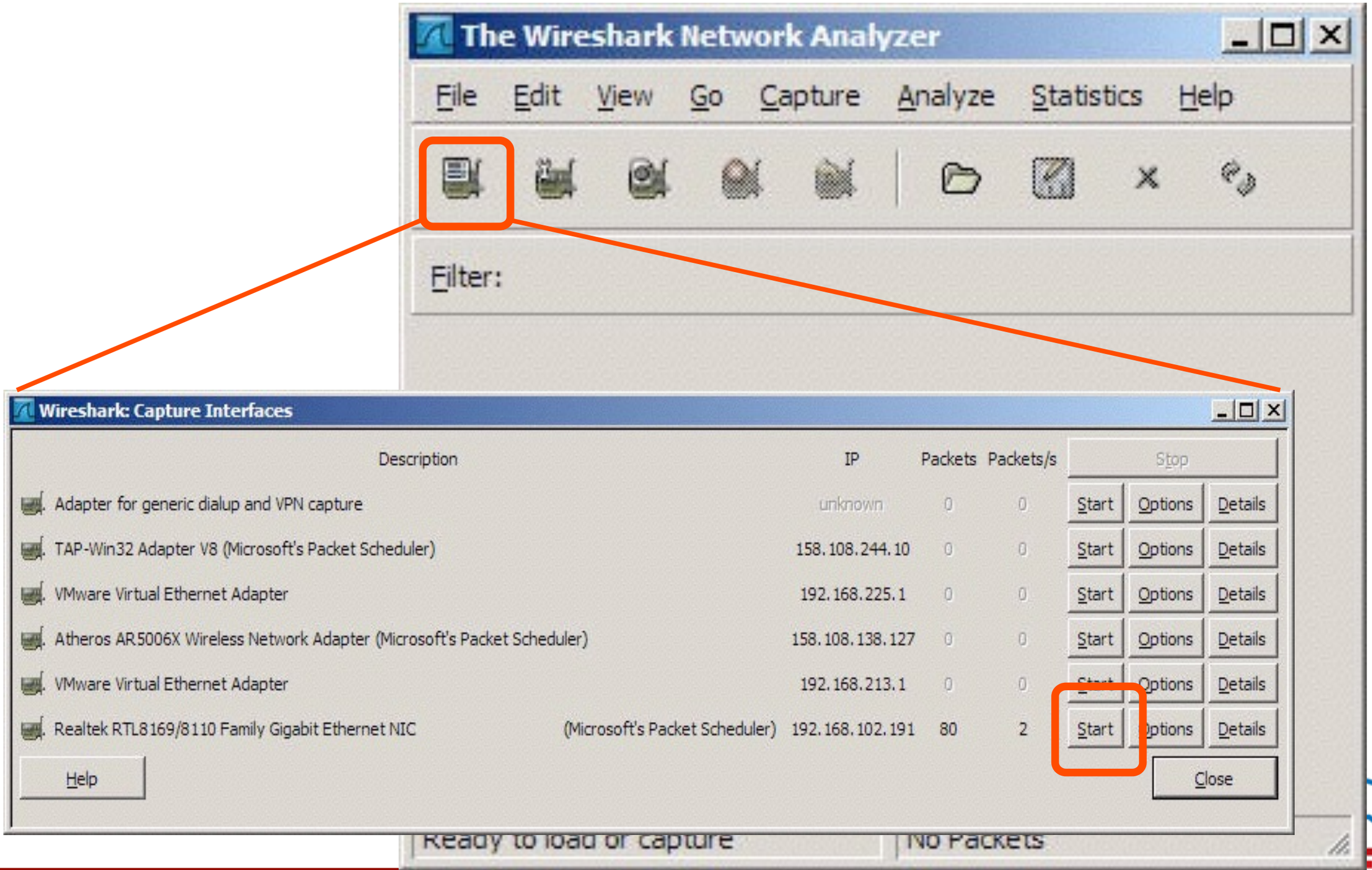
- Capture filter
  - Capture traffic that match capture filter rules
  - Save disk space
  - Prevent packet loss
- Display filter ← we will focus today
  - Display packet that match display filter rules
  - Easy to read and analyze
  - Can focus on some behavior
- In a broadband network, you should set the capture filter carefully

How to use wireshark?

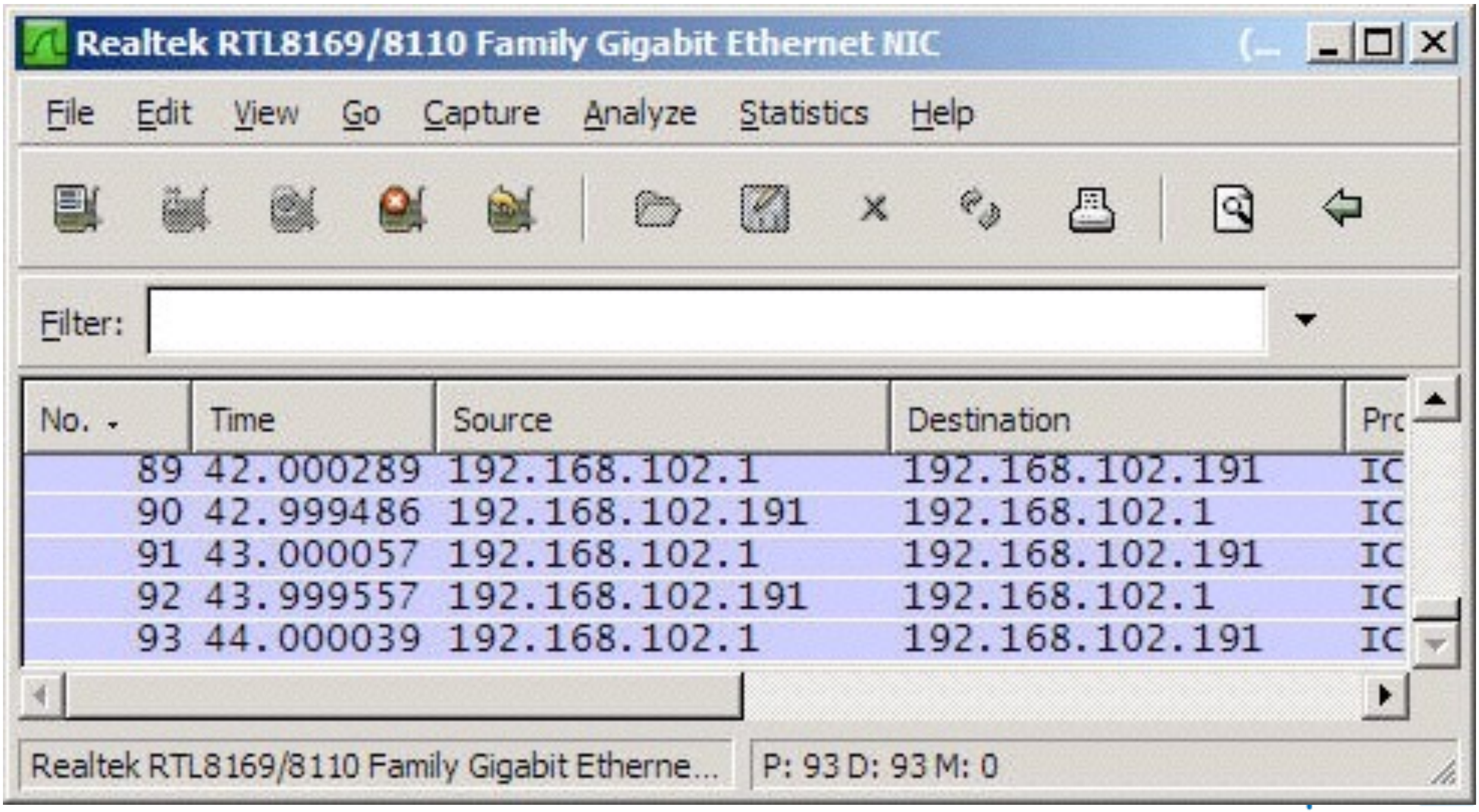
- Main program



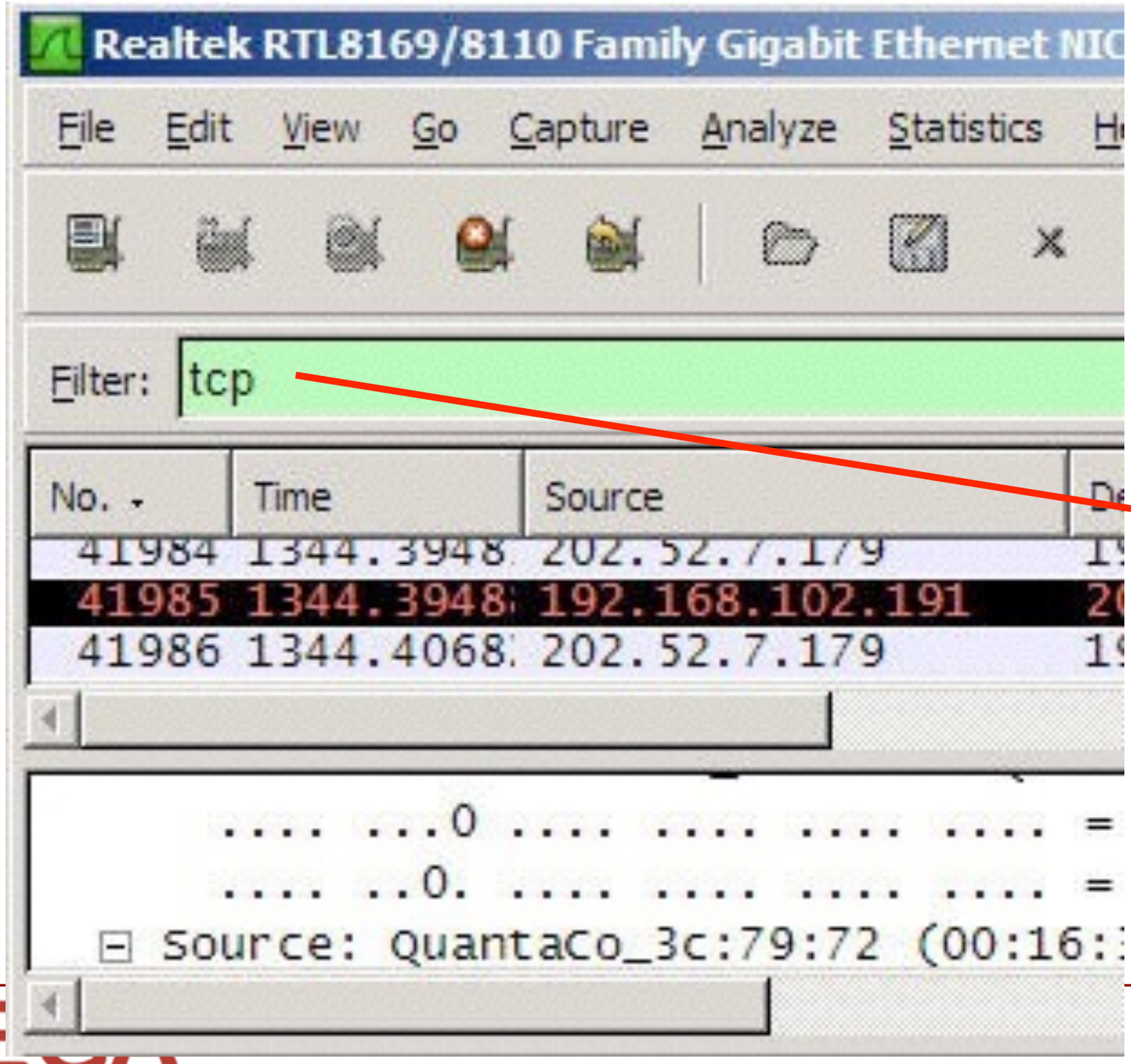
Start Capturing

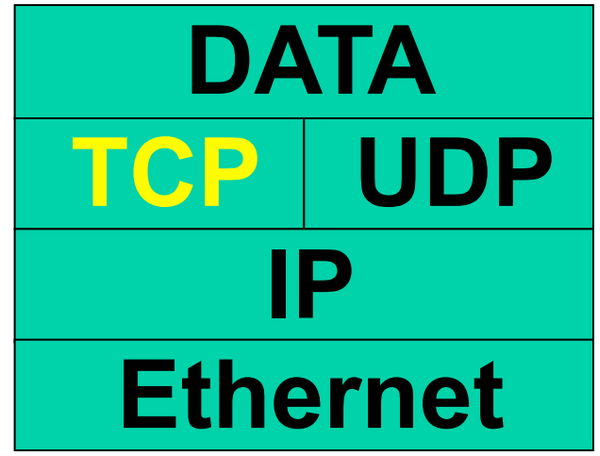


The capture result



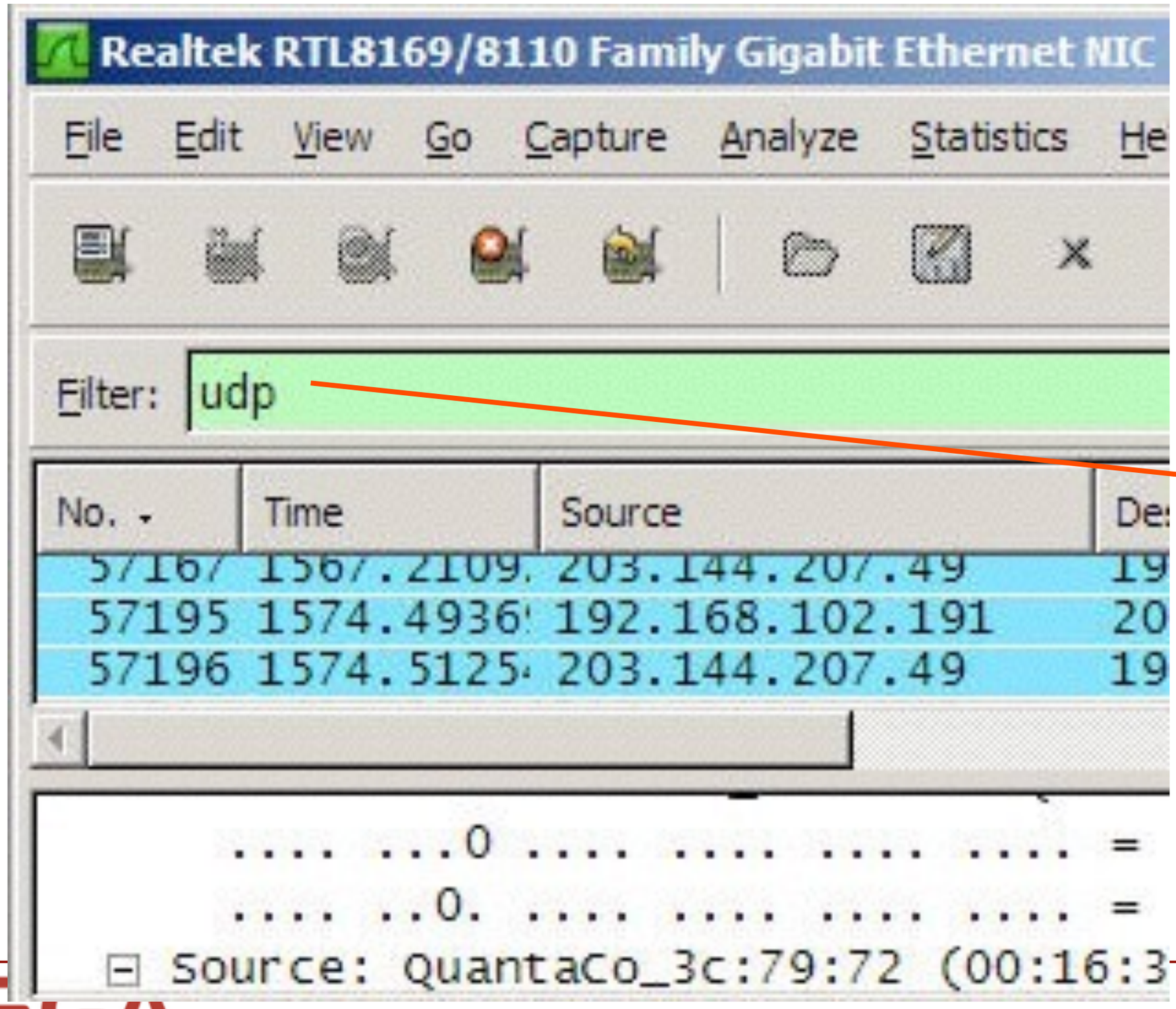
Display filters – Only TCP





tcp.port==23

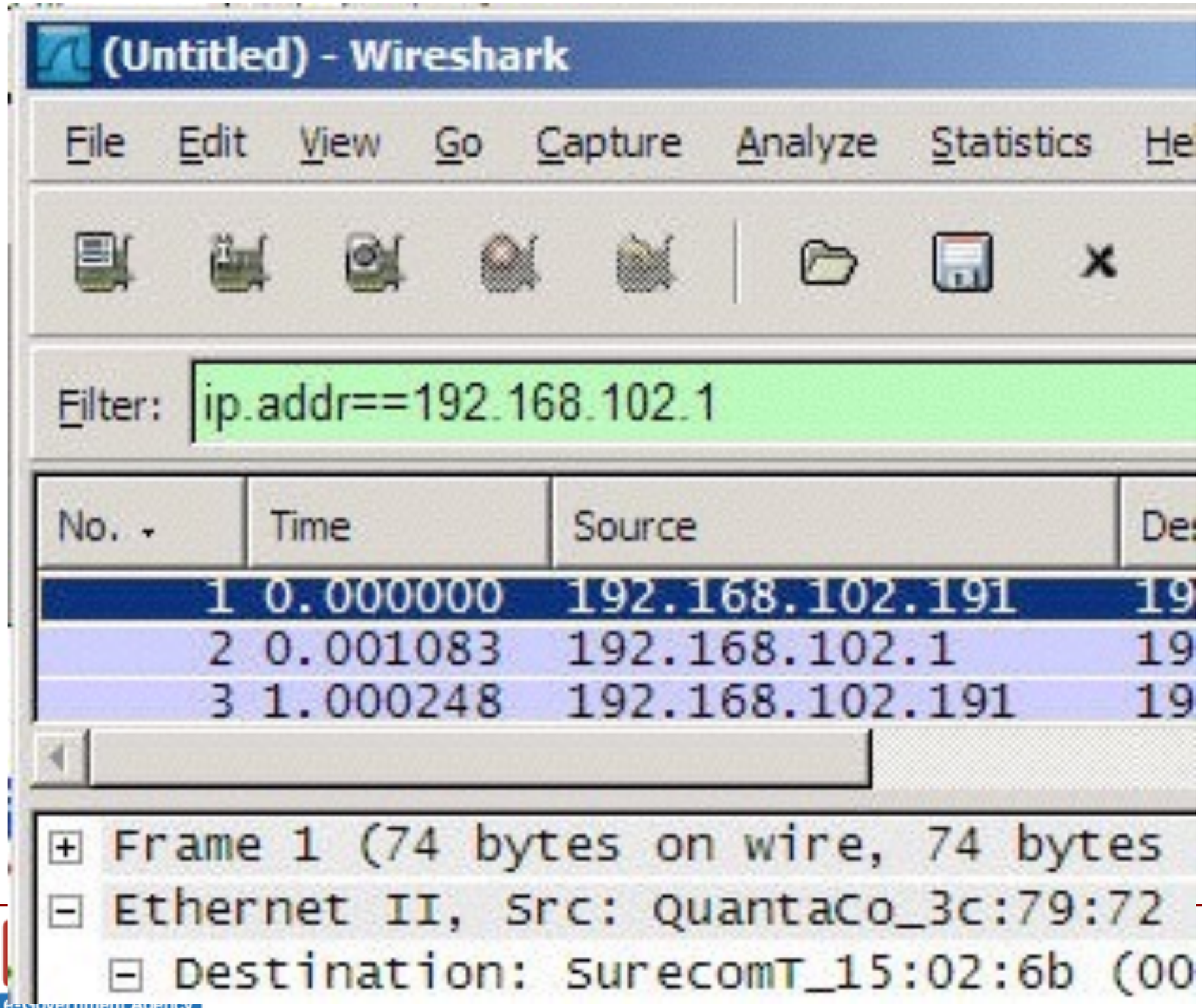
Display filter – Only UDP

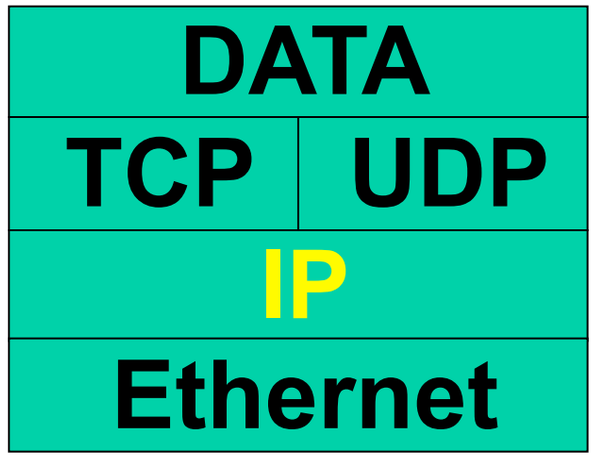


DATA	
TCP	UDP
IP	
Ethernet	

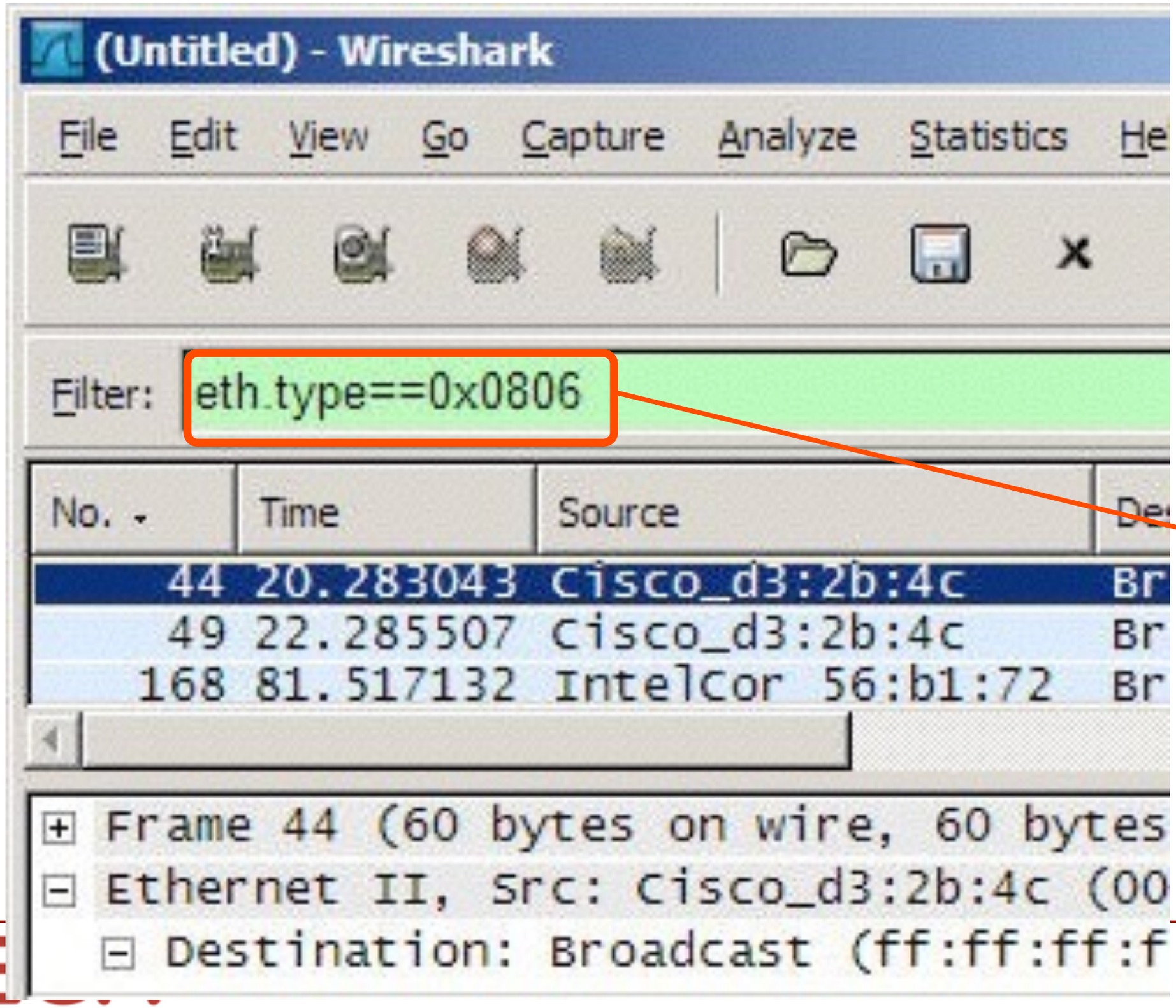
udp.port==xx

Display filter - IP

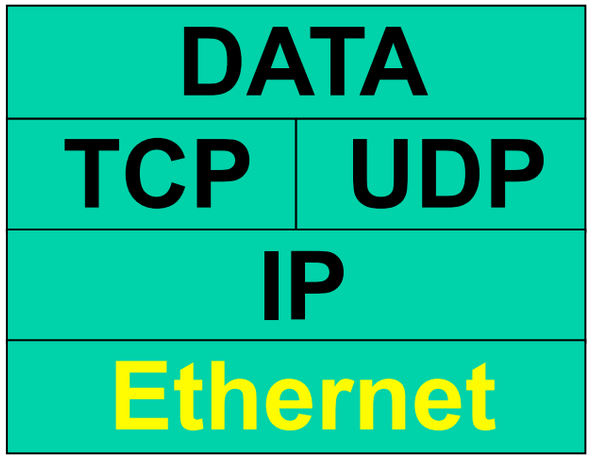




Display filter – Ethernet (LAN)

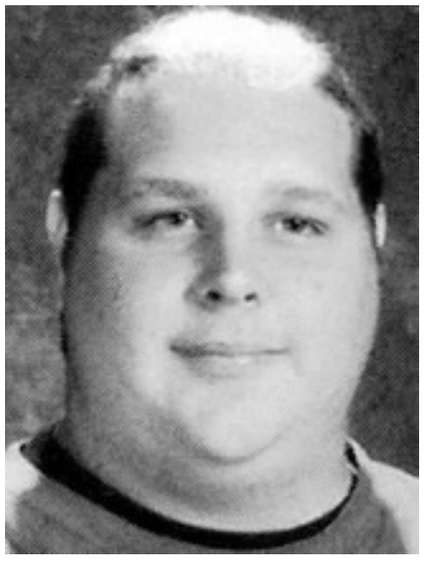


arp



Applying filter to detect Blaster worm

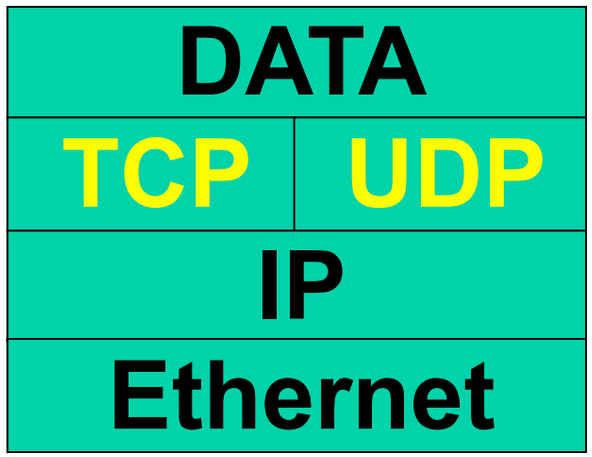
- Attack DCOM RPC by using 135/TCP and 137/UDP (MS03-026 vulnerability)
- Effect for Windows NT, 2000, XP and 2003
- Countdown 30 seconds and automatically restart



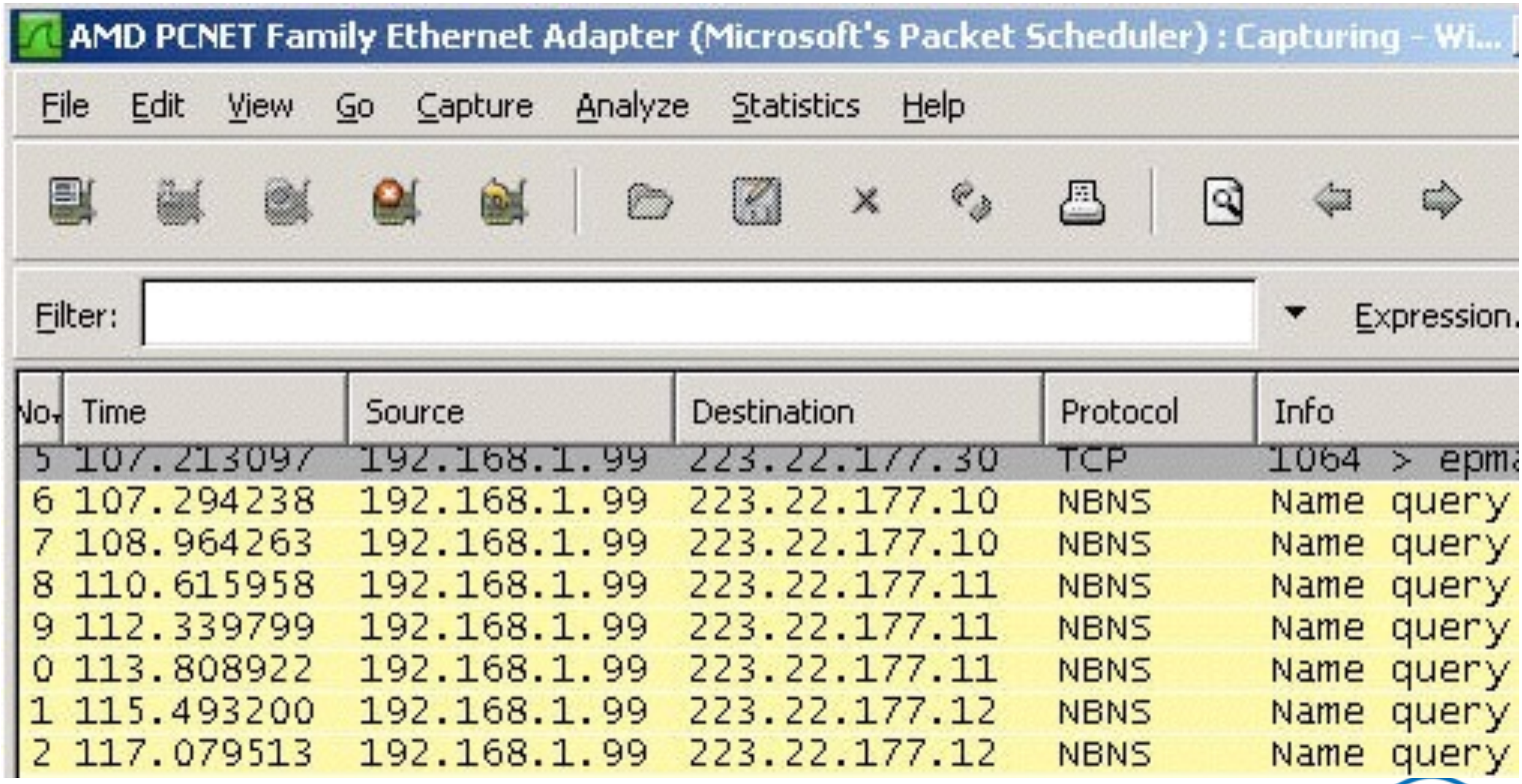
Jeffrey Lee Parson, 19
Blaster worm writer

Example for filtering

- Analyze the Blaster's behavior
  - Target on 135/TCP
  - Target on 137/UDP



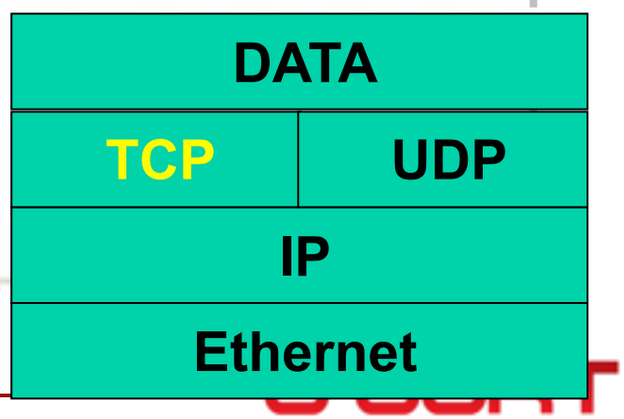
Blaster's traffic



Blaster's traffic

```
⊞ Frame 286 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Vmware_85:4f:6c (00:0c:29:85:4f:6c)
⊞ Internet Protocol, Src: 192.168.1.99 (192.168.1.99),
⊞ Transmission Control Protocol, Src Port: 1104 (1104),
```

```
   Source port: 1104 (1104)
   Destination port: epmap (135)
   Sequence number: 0    (relative sequence number)
   Header length: 28 bytes
⊞  Flags: 0x02 (SYN)
   Window size: 64240
⊞  Checksum: 0x35da [correct]
⊞  Options: (8 bytes)
```



Infected machine's IP

```
⊞ Frame 286 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Vmware_85:4f:6c (00:0c:29:85:4f:6c)
⊞ Internet Protocol, Src: 192.168.1.99 (192.168.1.99),
⊞ Transmission Control Protocol, Src Port: 1104 (1104),
```

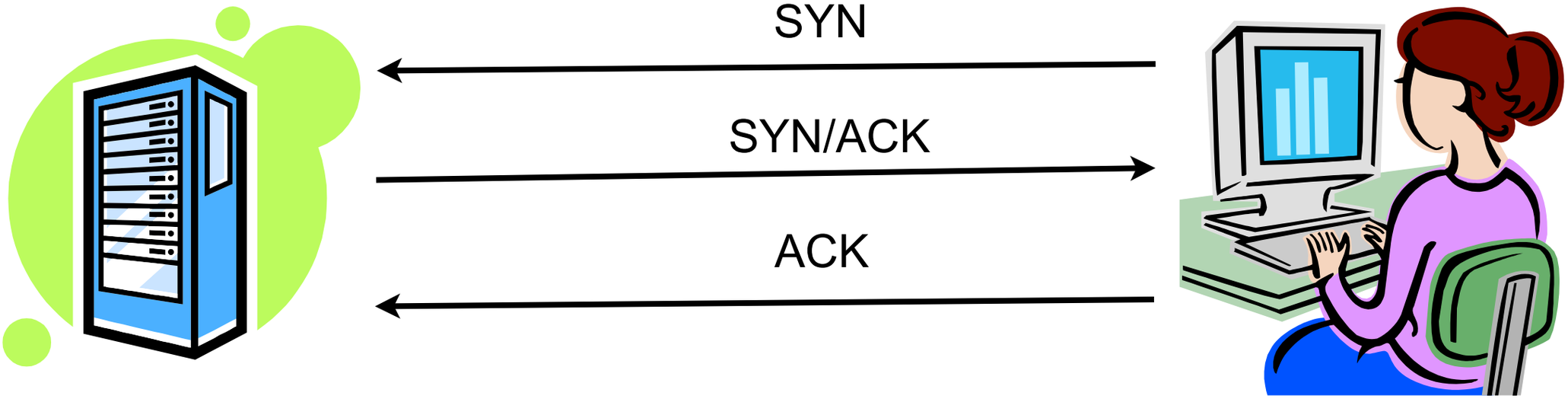
```
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0xa709 [correct]
    Source: 192.168.1.99 (192.168.1.99)
    Destination: 223.22.177.70 (223.22.177.70)
⊞ Transmission Control Protocol, Src Port: 1104 (1104),
```

DATA	
TCP	UDP
IP	
Ethernet	

The TCP Three Way Handshake

1. The Sending Host sends a SYN packet to the Receiving host. (Phone Rings)
2. The Receiving host response with a SYN-ACK. (Hello?)
3. The Sending Host then responds with an ACK. (HI!!)
4. The Connection is now up.

The TCP Three Way Handshake



Simple HTTP

- File – 01_http.pcap
- Questions
  - What is IP of the web server?
  - What is the URL of the web server?
  - Can you guess what is the user doing?

- Tip
  - 3 ways hand-shake

Login through HTTP

- File – 02_http_login.pcap
- Questions
  - What is the method for submitting info to web server?
  - Who login to this web site?

    Username _____,Password _____.

- Tips
  - 3 ways hand-shake
  - HTTP traffic is not secure

Good Old Telnet

- File – 03_telnet.pcap
- Questions
  - What is port number of Telnet service?
  - Who logged into 10.0.1.10 Username _____,Password _____.
    - (Optional) After logged in what did the user do?
      - Answer for 3 commands
- Tip
  - Telnet traffic is not secure

????

- File – 05.pcap
- Questions
  - What is this activity?
  - What is attacker's IP?
  - What port that opens on the server?

- Tip
  - 3 ways hand-shake

Follow me @.....

Name : Kitisak Jirawannakool

Facebook : http://www.facebook.com/kitisak.note

Email : kitisak.jirawannakool@ega.or.th

jkitisak@gmail.com

Weblog : http://foh9.blogspot.com

Twitter : @kitisak

Thank you

Contact me

helpdesk@ega.or.th

http://www.ega.or.th