

---

# Introduction to Wireshark

By

Kitisak Jirawannakool

E-Government Agency (Public Organization)

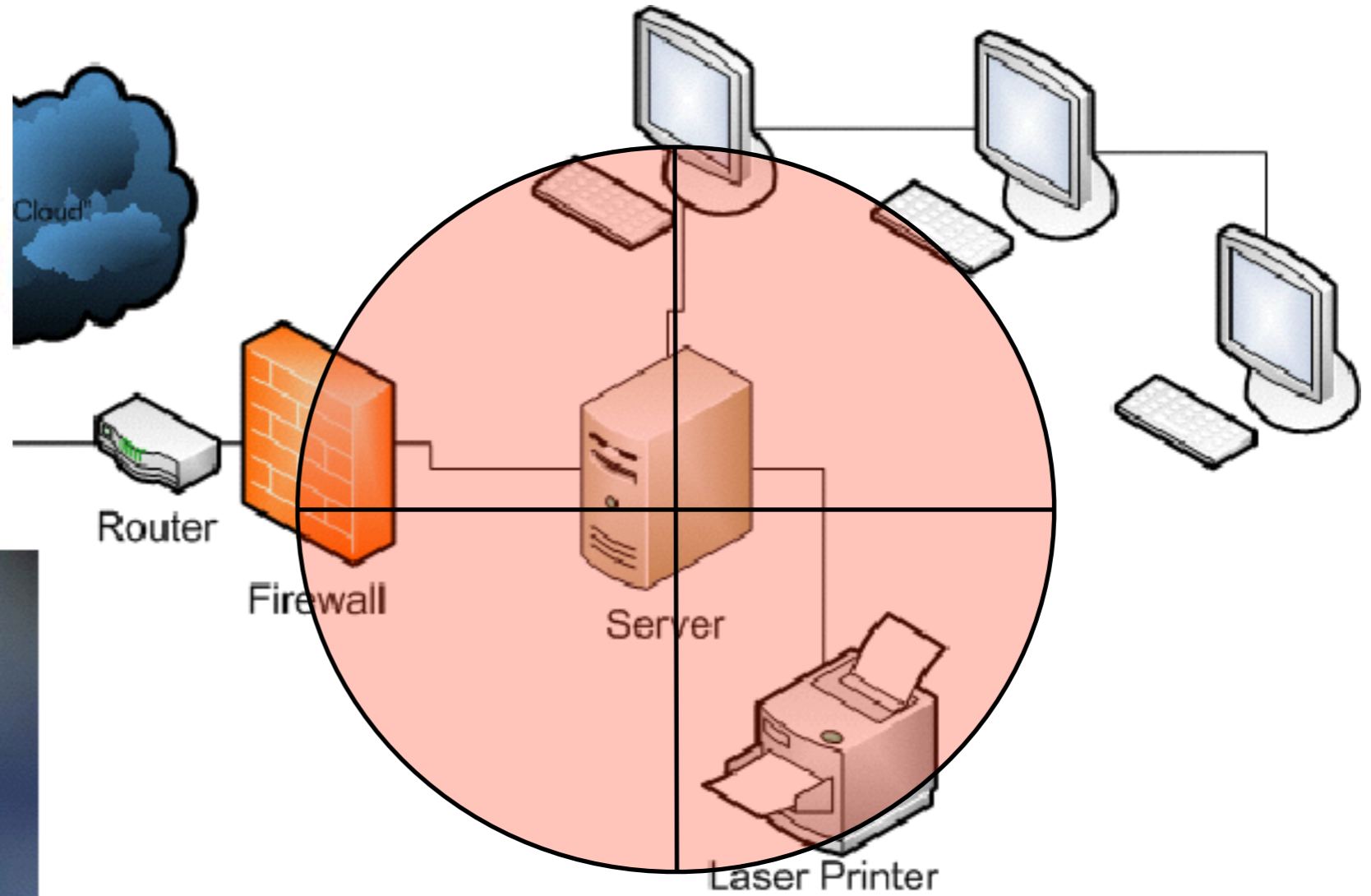


# Agenda

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



# What is Network Monitoring?



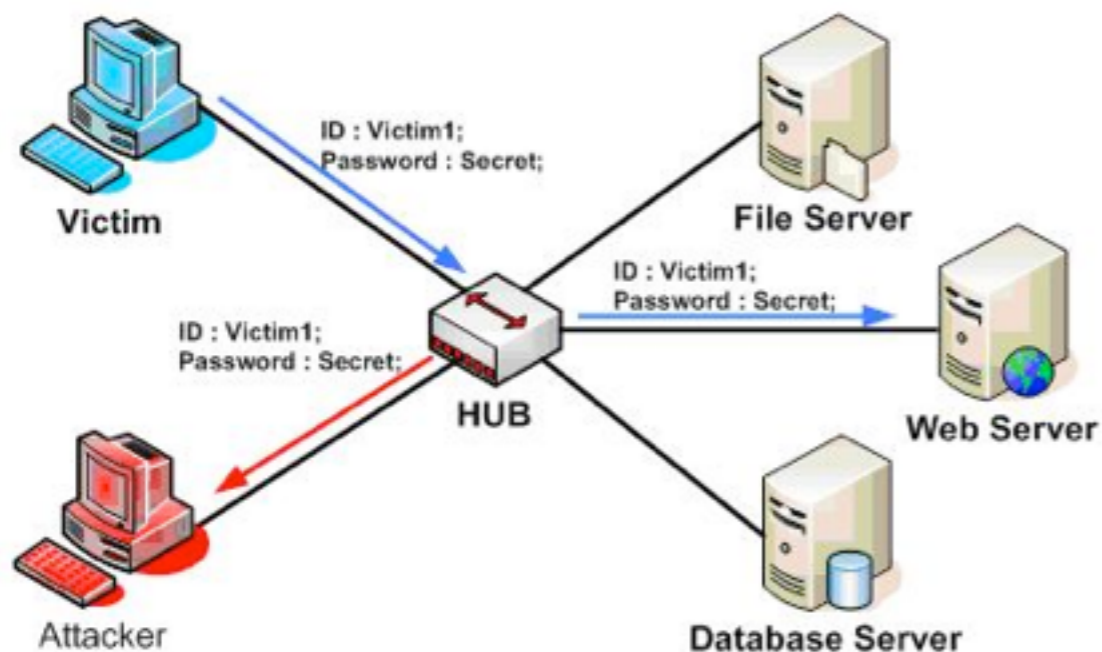
# Eavesdropping



FreakingNews.com



# Network Eavesdropping



The screenshot shows a network capture tool window titled 'eth2: Capturing'. It displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets are filtered to show traffic between 190.10.133.30 and 205.134.246.207. The details for Frame 59 are expanded, showing Ethernet II and Internet Protocol headers.

No.	Time	Source	Destination	Protocol	Info
74	4.126540	190.10.133.30	205.134.246.207	TCP	[TCP segment of a reassembled PDU]
75	4.282475	190.10.133.30	205.134.246.207	TCP	[TCP segment of a reassembled PDU]
76	4.282532	190.10.133.30	205.134.246.207	TCP	[TCP segment of a reassembled PDU]
77	4.299747	205.134.246.207	190.10.133.30	TCP	www > 54530 [ACK] Seq=1 Ack=35915 Win=34
78	4.434607	190.10.133.30	205.134.246.207	SSH	Encrypted request packet len=192
79	4.450362	190.10.133.30	205.134.246.207	SSH	Encrypted request packet len=144
80	4.452717	205.134.246.207	190.10.133.30	TCP	www > 54530 [ACK] Seq=1 Ack=38811 Win=34
81	4.482440	190.10.133.30	205.134.246.207	HTTP	POST /wp-admin/admin-ajax.php HTTP/1.1 [
82		205.134.246.207	190.10.133.30	SSH	Encrypted response packet len=160
83	4.603821	190.10.133.30	205.134.246.207	TCP	41446 > ssh [ACK] Seq=944 Ack=720 Win=20
84	4.607673	205.134.246.207	190.10.133.30	SSH	Encrypted response packet len=144
85	4.607770	190.10.133.30	205.134.246.207	TCP	41446 > ssh [ACK] Seq=944 Ack=864 Win=20
86	4.644661	205.134.246.207	190.10.133.30	TCP	www > 54530 [ACK] Seq=1 Ack=39985 Win=34

Frame 59 (1514 bytes on wire, 1514 bytes captured)  
Ethernet II, Src: Motorola\_f1:d8:1c (00:16:b5:f1:d8:1c), Dst: Riverdel\_c1:ab:40 (00:30:b8:c1:ab:40)  
Internet Protocol, Src: 190.10.133.30 (190.10.133.30), Dst: 205.134.246.207 (205.134.246.207)

```
0000 00 30 b8 c1 ab 40 00 16 b5 f1 d8 1c 00 00 45 00  .0...@.. ..E.  
0010 05 dc 46 3c 40 00 40 06 e7 60 be 0a 85 1e cd 86  ..F<@. ....  
0020 f6 cf d5 02 00 50 95 79 fe e5 d2 2b da 03 80 10  ....P.y ..+...  
0030 00 b7 a3 66 00 00 01 01 08 0a 12 82 dc f9 59 e8  ...f.... ..Y.
```

# 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)



# What kind of information we need?

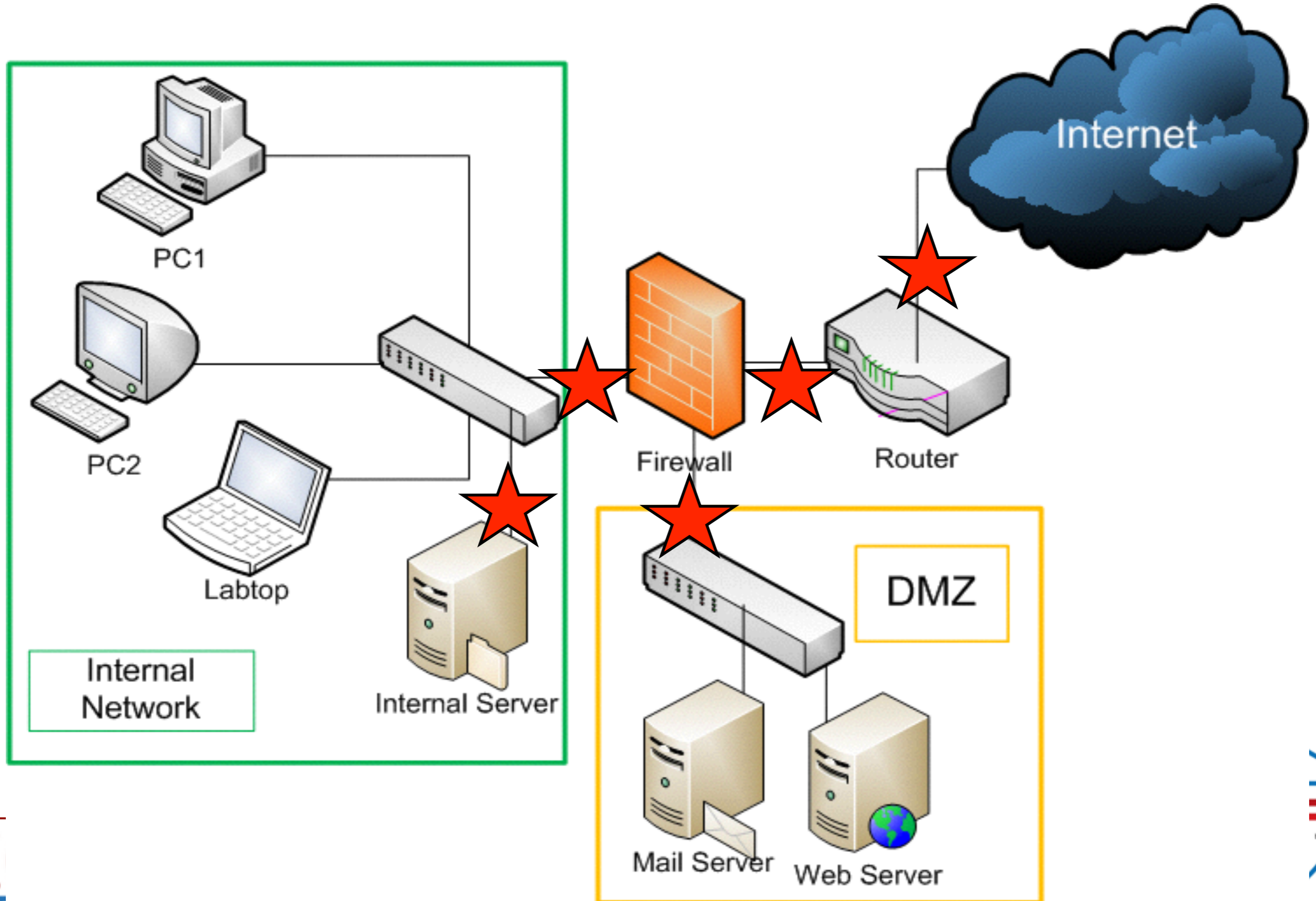
Purpose	Tech	Tool ex)	Note
Traffic accounting	SNMP	MRTG	
Intrusion Detection	IDS	snort	False positive/netgative issue
Full content	Packet capture	tcpdump libpcap	Be aware, it may contains private data
Sessions statistics	netflow	Nfdump, nfsen	
Log	Files on Firewalls servers	Many	Log level configuration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

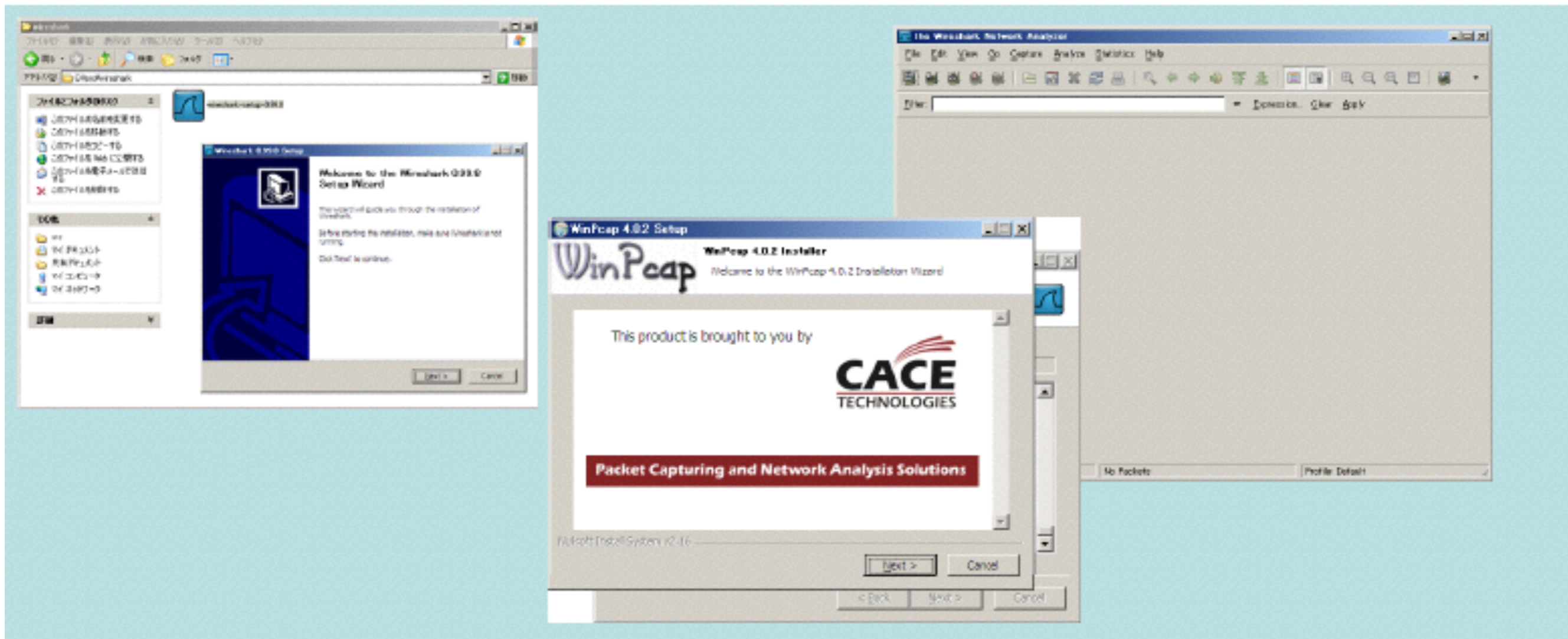
# About WireShark

- ❖ 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

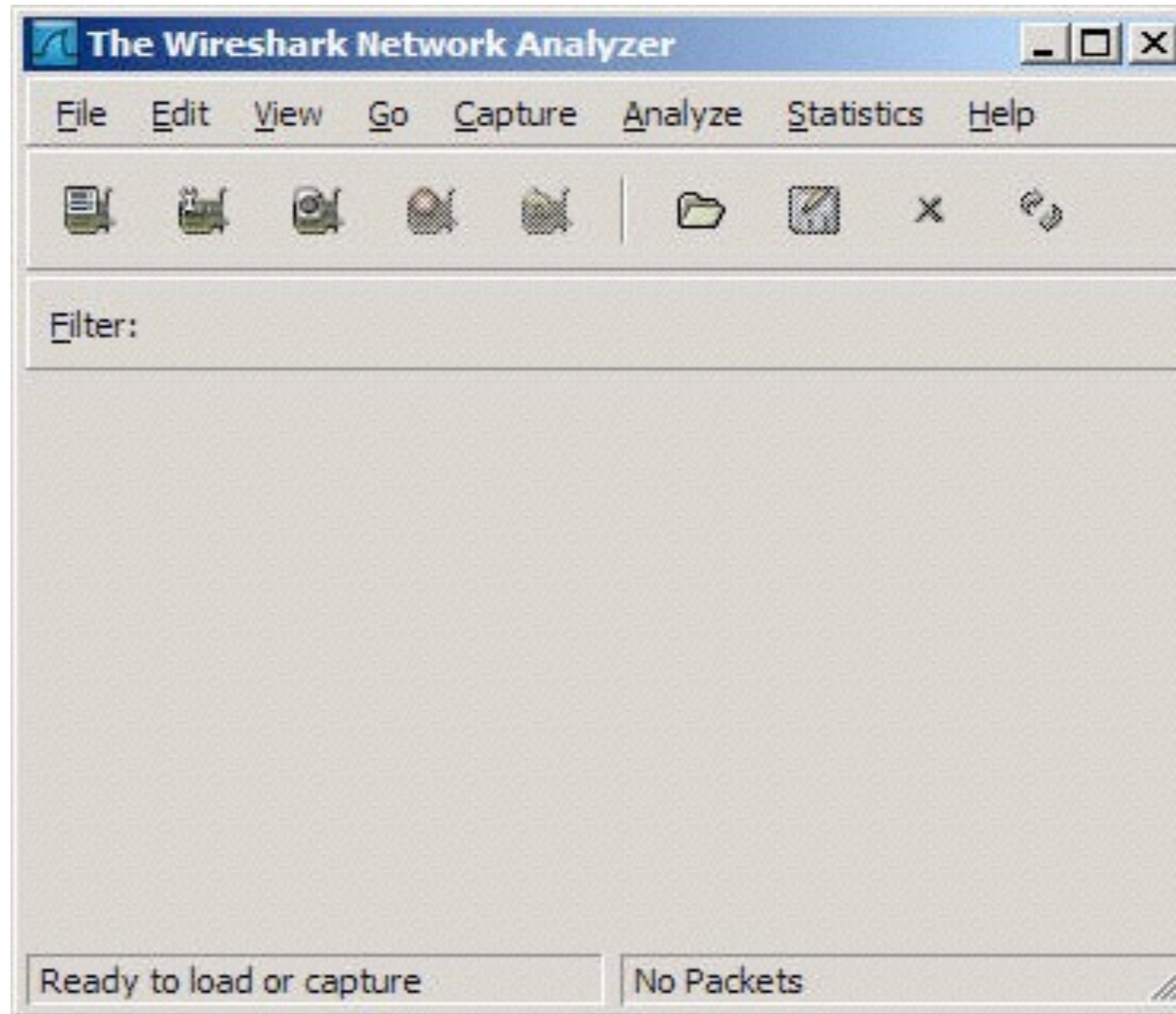


# Filters

- ❖ 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 screenshot shows the Wireshark Network Analyzer interface. The main window has a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help) and a toolbar. The 'Capture' button in the toolbar is highlighted with an orange box. Below the toolbar is a 'Filter:' field. A dialog box titled 'Wireshark: Capture Interfaces' is open, showing a list of network interfaces. The 'Start' button for the 'Realtek RTL8169/8110 Family Gigabit Ethernet NIC' is highlighted with an orange box. The status bar at the bottom of the dialog box shows 'Ready to load or capture' and 'No Packets'.

Description	IP	Packets	Packets/s	Start	Options	Details
Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
TAP-Win32 Adapter V8 (Microsoft's Packet Scheduler)	158.108.244.10	0	0	Start	Options	Details
VMware Virtual Ethernet Adapter	192.168.225.1	0	0	Start	Options	Details
Atheros AR5006X Wireless Network Adapter (Microsoft's Packet Scheduler)	158.108.138.127	0	0	Start	Options	Details
VMware Virtual Ethernet Adapter	192.168.213.1	0	0	Start	Options	Details
Realtek RTL8169/8110 Family Gigabit Ethernet NIC (Microsoft's Packet Scheduler)	192.168.102.191	80	2	Start	Options	Details

# The capture result

No. ▾	Time	Source	Destination	Proc
89	42.000289	192.168.102.1	192.168.102.191	IC
90	42.999486	192.168.102.191	192.168.102.1	IC
91	43.000057	192.168.102.1	192.168.102.191	IC
92	43.999557	192.168.102.191	192.168.102.1	IC
93	44.000039	192.168.102.1	192.168.102.191	IC

Realtek RTL8169/8110 Family Gigabit Etherne... P: 93 D: 93 M: 0

# Display filters – Only TCP

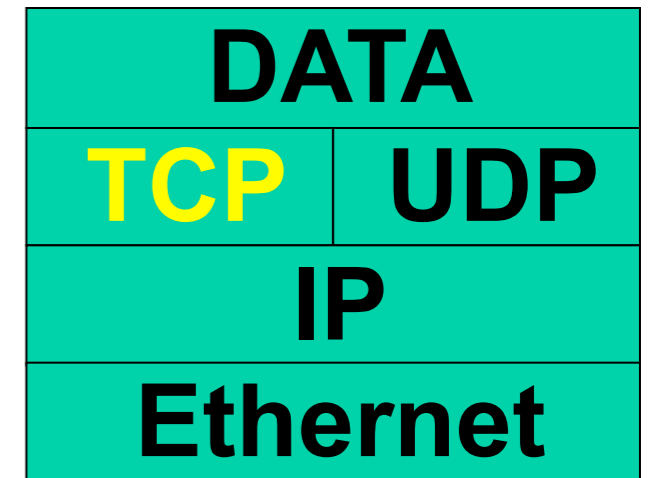
Realtek RTL8169/8110 Family Gigabit Ethernet NIC

File Edit View Go Capture Analyze Statistics Help

Filter: tcp

No.	Time	Source	Destination
41984	1344.3948	202.52.7.179	192.168.102.191
41985	1344.3948	192.168.102.191	202.52.7.179
41986	1344.4068	202.52.7.179	192.168.102.191

Source: QuantaCo\_3c:79:72 (00:16:8d:00:00:00)



tcp.port==23

# Display filter – Only UDP

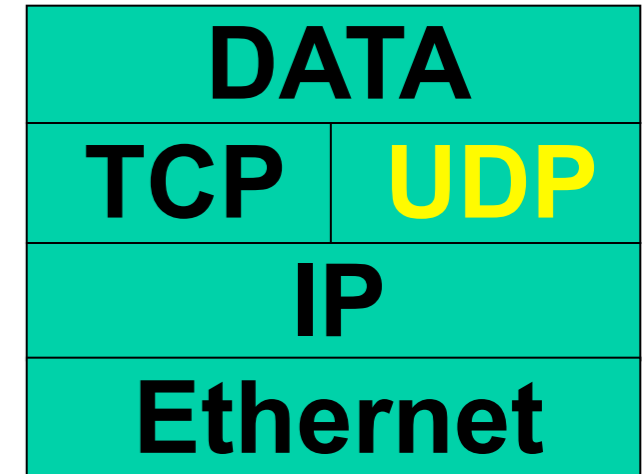
Realtek RTL8169/8110 Family Gigabit Ethernet NIC

File Edit View Go Capture Analyze Statistics Help

Filter: `udp`

No.	Time	Source	Destination
57167	1567.2109	203.144.207.49	192.168.1.1
57195	1574.4936	192.168.102.191	203.144.207.49
57196	1574.5125	203.144.207.49	192.168.1.1

Source: QuantaCo\_3c:79:72 (00:16:3c:79:72:00)



`udp.port==xx`

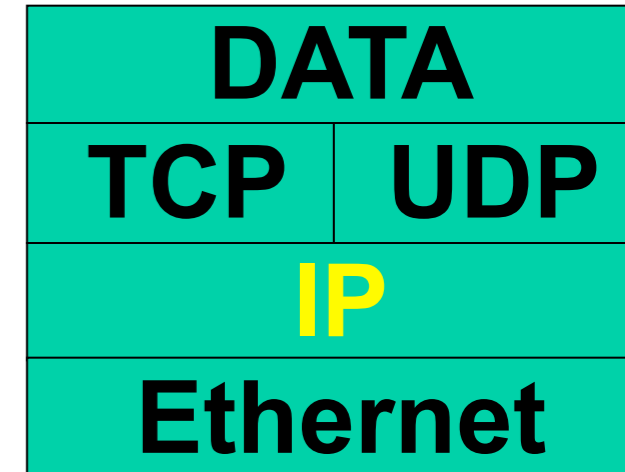
# Display filter - IP

The image shows the Wireshark network protocol analyzer interface. The title bar reads "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains icons for opening files, saving, and other functions. The filter field is set to "ip.addr==192.168.102.1". Below the filter is a table of captured packets:

No.	Time	Source	Destination
1	0.000000	192.168.102.191	192.168.102.1
2	0.001083	192.168.102.1	192.168.102.191
3	1.000248	192.168.102.191	192.168.102.1

The packet details pane shows the following information for the selected packet:

- Frame 1 (74 bytes on wire, 74 bytes captured)
- Ethernet II, Src: QuantaCo\_3c:79:72
- Destination: SurecomT\_15:02:6b (00:0c:29:15:02:6b)



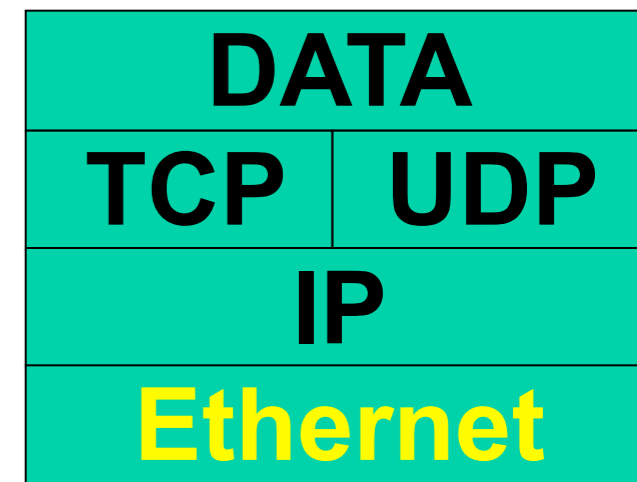
# Display filter – Ethernet (LAN)

The image shows the Wireshark network protocol analyzer interface. The title bar reads "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu is a toolbar with various icons. The filter field contains the text "eth.type==0x0806", which is highlighted with a red box. Below the filter is a table of captured packets:

No.	Time	Source	Destination
44	20.283043	Cisco_d3:2b:4c	Broadcast
49	22.285507	Cisco_d3:2b:4c	Broadcast
168	81.517132	IntelCor 56:b1:72	Broadcast

Below the table, the details pane shows the structure of the selected packet (Frame 44):

- Frame 44 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: Cisco\_d3:2b:4c (00:0c:29:2b:4c:00)
- Destination: Broadcast (ff:ff:ff:ff:ff:ff)



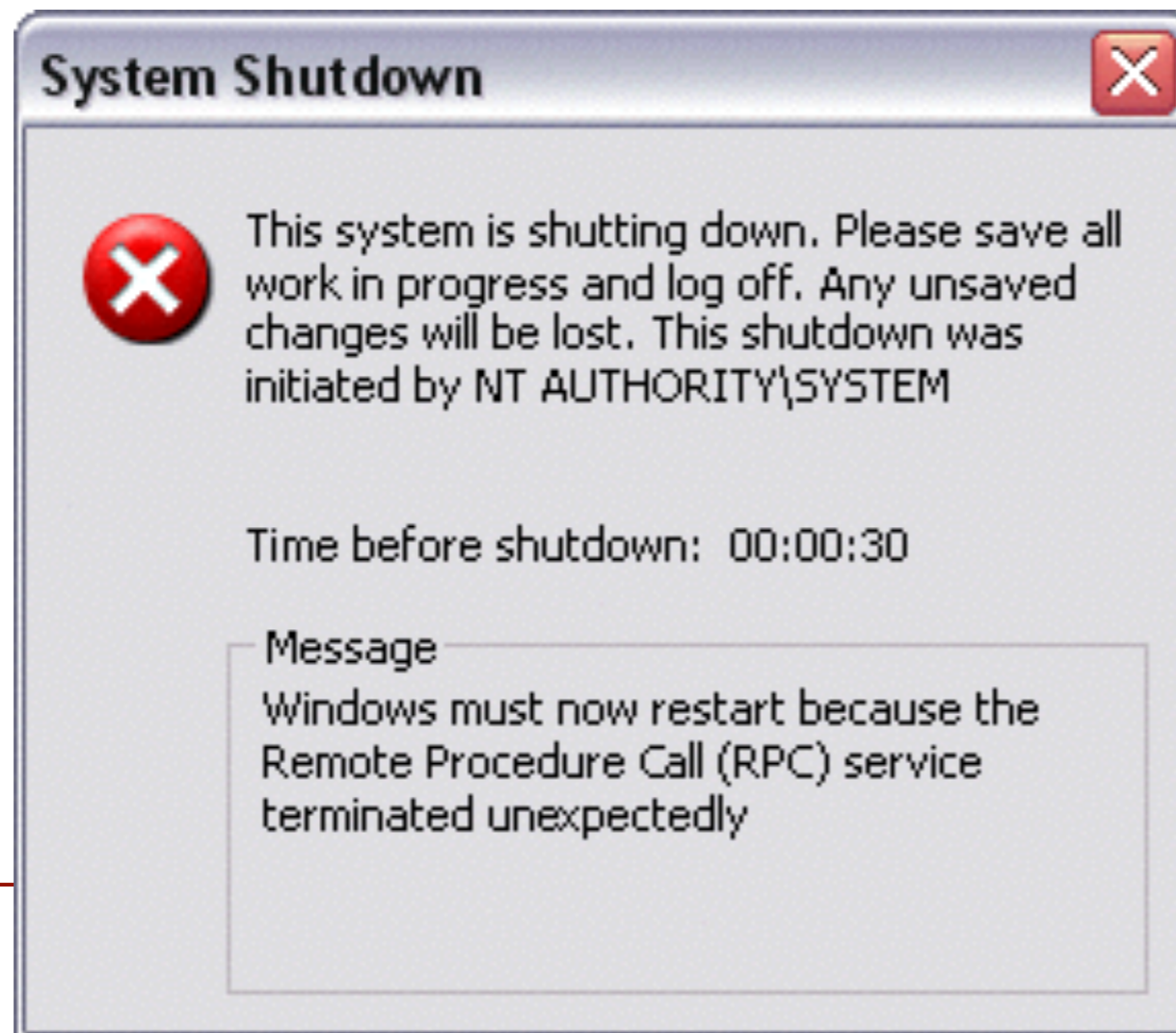
arp





# 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

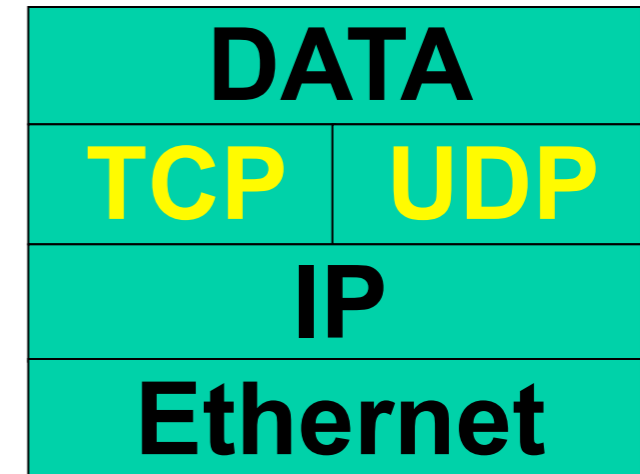


Jeffrey Lee Parson, 19  
Blaster worm writer



# Example for filtering

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



# Blaster's traffic

No.	Time	Source	Destination	Protocol	Info
5	107.213097	192.168.1.99	223.22.177.30	TCP	1064 > epma
6	107.294238	192.168.1.99	223.22.177.10	NBNS	Name query
7	108.964263	192.168.1.99	223.22.177.10	NBNS	Name query
8	110.615958	192.168.1.99	223.22.177.11	NBNS	Name query
9	112.339799	192.168.1.99	223.22.177.11	NBNS	Name query
0	113.808922	192.168.1.99	223.22.177.11	NBNS	Name query
1	115.493200	192.168.1.99	223.22.177.12	NBNS	Name query
2	117.079513	192.168.1.99	223.22.177.12	NBNS	Name query

# 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)
```

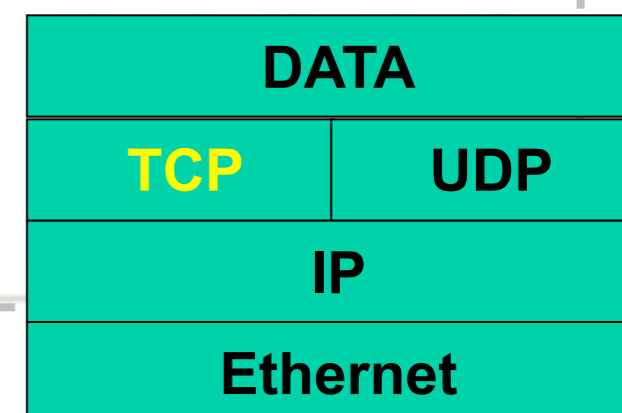
```
Header length: 28 bytes
```

```
+ 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)
```

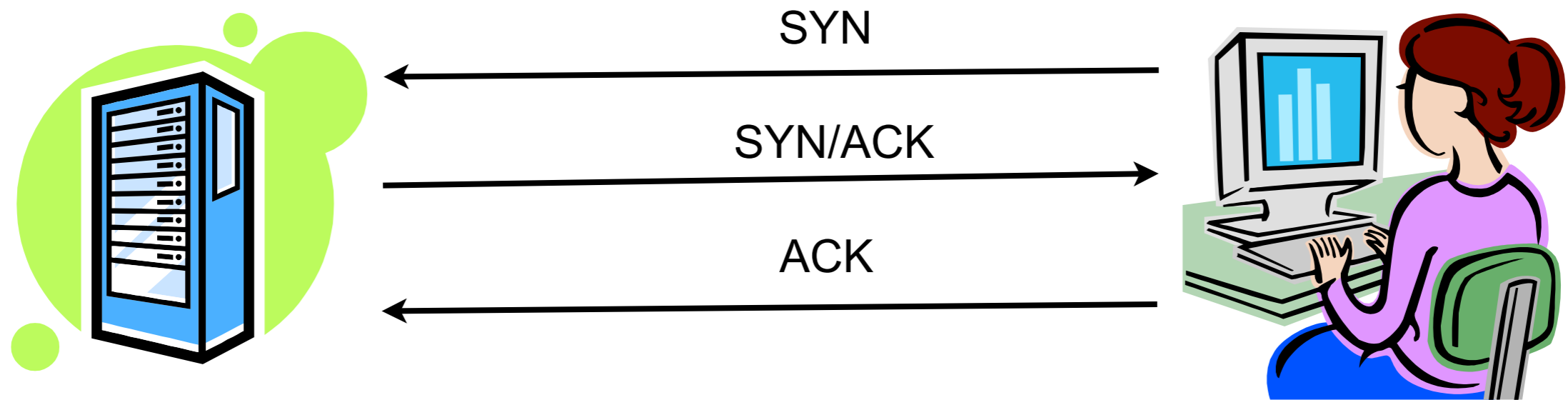
```
+ Transmission Control Protocol, Src Port: 1104 (1104),
```

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](mailto:kitisak.jirawannakool@ega.or.th)  
[jkitisak@gmail.com](mailto:jkitisak@gmail.com)

Weblog : <http://foh9.blogspot.com>

Twitter : @kitisak



# Thank you

---



Contact me

[helpdesk@ega.or.th](mailto:helpdesk@ega.or.th)

<http://www.ega.or.th>