

# ***Intrusion Detection, Packet Sniffing***

**By : Eng. Ayman Amaireh  
Supervisor :Dr. Lo'ai Tawalbeh**

**New York Institute of Technology (NYIT)-  
Jordan's campus-2006**



# What is a "packet sniffer"?

---

- A **packet sniffer** is a wire-tap devices \SW that plugs into computer networks and eavesdrops on the network traffic. Like a telephone wiretap. allows us to listen in on other people's conversations
- a "sniffing" program lets someone listen in on computer conversations.



# Introduction

---

- Terminology: A **packet sniffer** also known as a **network analyzer** or **protocol analyzer**, for particular types of networks, an **Ethernet sniffer** or **wireless sniffer**
- Packet sniffer can intercept and log traffic passing over a digital network or part of a network. As data streams travel back and forth over the network, the sniffer captures each packet and eventually decodes and analyzes its content according with any specifications



# Introduction

---

- However, computer conversations consist of apparently random binary data. Therefore, network wiretap programs also come with a feature known as "protocol analysis", which allow them to "decode" the computer traffic and make sense of it.



# shared media

---

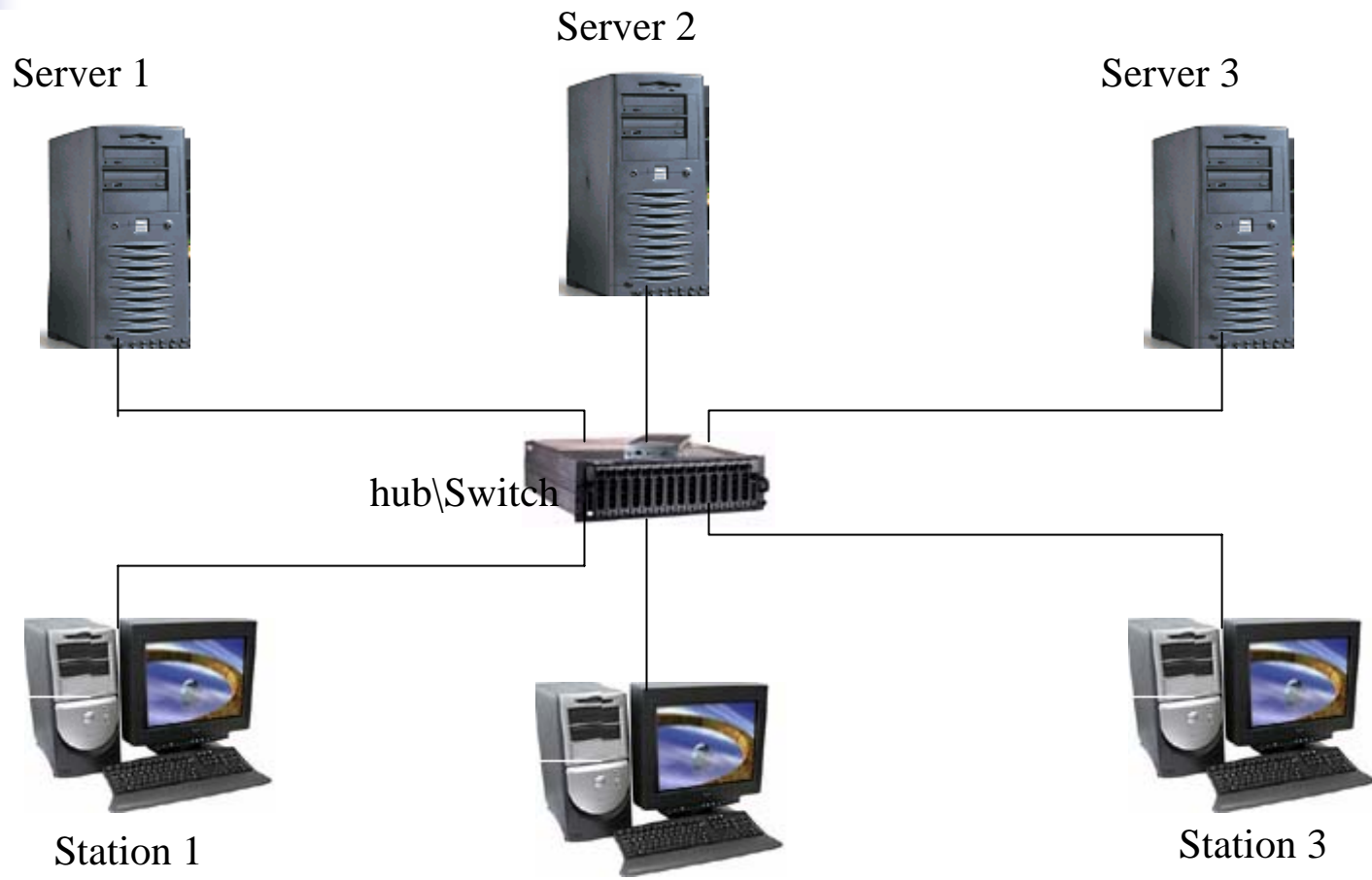
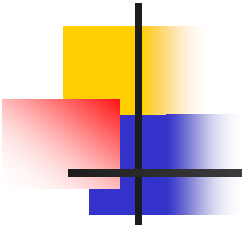
- Sniffing also has one advantage over telephone wiretaps: many networks use "shared media". This means that you don't need to break into a wiring closet to install your wiretap, you can do it from almost any network connection to eavesdrop on your neighbors. This is called a "promiscuous mode" sniffer. However, this "shared" technology is moving quickly toward "switched" technology where this will no longer be possible, which means you will have to actually tap into the wire.



# Shared media

---

- On wired broadcast LANs, depending on the network structure (hub or switch), one can capture traffic on all or just parts of the traffic from a single machine within the network; however, there are some methods to avoid traffic narrowing by switches to gain access to traffic from other systems on the network (e.g. ARP spoofing).
- For network monitoring purposes it may also be desirable to monitor all data packets in a LAN by using a network switch with a so-called monitoring port, whose purpose is to mirror all packets passing through all ports of the switch





# avoid traffic narrowing by switches

---

1. **ARP Spoofing:** We have explained earlier how ARP is used to obtain the MAC address of the destination machine with which we wish to communicate. The ARP is stateless, you can send an ARP reply even if one has not been asked for and such a reply will be accepted. Ideally when you want to sniff the traffic originating from machine Venus, you can ARP Spoof the gateway of the network. The ARP cache of Venus will now have a wrong entry for the gateway and is said to be poisoned. This way all the traffic destined for the gateway will pass through your machine. Another trick that can be used is to poison a hosts ARP cache by setting the gateway's MAC address to FF:FF:FF:FF:FF:FF (also known as the broadcast MAC). An excellent tool for this is the **arp spoof** utility that comes with the dsniff



# avoid traffic narrowing by switches



---

2. **MAC Flooding:** Switches keep a translation table that maps various MAC addresses to the physical ports on the switch. As a result of this it can intelligently route packets from one host to another. The switch has a limited memory for this work. MAC flooding makes use of this limitation to bombard the switch with fake MAC addresses till the switch can't keep up. The switch then enters into what is known as a "failopen mode" wherein it starts acting as a hub by broadcasting packets to all the machines on the network. Once that happens sniffing can be performed easily. MAC flooding can be performed by using **macof**, a utility that comes with dsniff suite.



# How does sniffing work?

---

- Ethernet was built around a "shared" principle: all machines on a local network share the same wire.
- This implies that all machines are able to "see" all the traffic on the same wire.
- Thus, Ethernet hardware is built with a "filter" that ignores all traffic that doesn't belong to it. It does this by ignoring all frames whose MAC address doesn't match.



# How does sniffing work?

---

- A sniffer program turns off this filter, putting the Ethernet hardware into "promiscuous mode". Thus, Mark can see all the traffic among all machines, as long as they are on the same Ethernet wire.



# What is it used for?

---

- Sniffing programs have been around for a long time in two forms. Commercial packet sniffers are used to help maintain networks.
- Underground packet sniffers are used to break into computers



# Why we use packet sniffing?

---

- The versatility of packet sniffers means they can be used to:
  - Analyse network problems.
  - Detect network intrusion attempts.
  - Gain information for effecting a network intrusion.
  - Gather and report network statistics.



# Why we use packet sniffing?

---

- Filter suspect content from network traffic.
- Debug client/server communications
- Milicious use:
  - Spy on other network users and collect sensitive information such as passwords (depending on any content encryption methods which may be in use)
  - Reverse engineer protocols used over the network.



## *Example uses*

---

- A packet sniffer for a token ring network could detect that the token has been lost or the presence of too many tokens (verifying the protocol).
- A packet sniffer could detect that messages are being sent to a network adapter; if the network adapter did not report receiving the messages then this would localize the failure to the adapter.



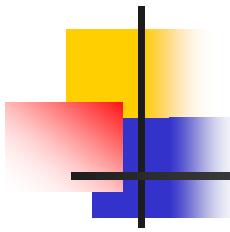
## *Example uses*

---

- A packet sniffer could detect excessive messages being sent by a port, detecting an error in the implementation.
- A packet sniffer could collect statistics on the amount of traffic (number of messages) from a process detecting the need for more bandwidth or a better method.

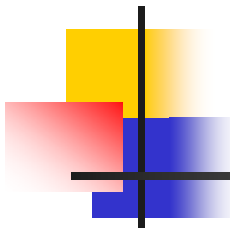


# What are the components of a packet sniffer?



---

- The hardware: Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth.



# What are the components of a packet sniffer?

---

- Capture driver :This is the most important part. It captures the network traffic from the wire, filters it for the particular traffic you want, then stores the data in a buffer.
- Buffer :Once the frames are captured from the network, they are stored in a buffer.



# What are the components of a packet sniffer?

---

- Decode :this displays the contents of network traffic with descriptive text so that an analyst can figure out what is going on.
- Packet editing/transmission :Some products contain features that allow you to edit your own network packets and transmit them onto the network.



# Sniffing Detection

---

- **Ping Method:** The trick used here is to send a ping request with the IP address of the suspect machine but not its MAC address. Ideally nobody should see this packet as each Ethernet Adapter will reject it as it does not match its MAC address. But if the suspect machine is running a sniffer it will respond, as it does not bother rejecting packets with a different Destination MAC address. This is an old method and not reliable any longer.
- **ARP Method:** A machine caches ARPs. So what we do is send a non-broadcast ARP. A machine in promiscuous mode will cache your ARP address. Next we send a broadcast ping packet with our IP, but a different MAC address. Only a machine that has our correct MAC address from the sniffed ARP frame will be able to respond to our broadcast ping request. Voila!



# Sniffing Detection

- **On Local Host:** Often after your machine has been compromised, hackers will leave sniffers, to compromise other machines. On a local machine run ifconfig. On a clean machine the output will be:

```
[root@ringwraith root]# /sbin/ifconfig
eth0  Link encap:Ethernet HWaddr 52:54:05:F3:95:01
inet addr:203.199.66.243 Bcast:203.199. ...
UP BROADCAST RUNNING MULTICAST MTU:1500 ...
```

But on a machine running a sniffer the output will be slightly different. Specifically check the last line wherein it mentions “**RUNNING PROMISC**”. That means the machine is in promiscuous mode and probably a sniffer is running on it.

```
[root@ringwraith root]# /sbin/ifconfig
eth0  Link encap:Ethernet HWaddr 52:54:05:F3:95:01
inet addr:203.199.66.243 Bcast:203.199. ...
UP BROADCAST RUNNING PROMISC MULTICAST ...
```

The output of the ifconfig command has been slightly modified to fit screen



# Sniffing Detection programs

---

- Anti Sniff: From the L0pht Heavy Industries comes the new program Anti Sniff. It has the ability to monitor a network and detect if a computer is in promiscuous mode. Available at: <http://www.securitysoftwaretech.com/antisniff/download.html>
- Neped: It detects network cards on the network that are in promiscuous mode by exploiting a flaw in the ARP protocol as implemented on Linux machines. Outdated. Available at: <ftp://apostols.org/AposTools/snapshots/neped/neped.c>
- ARP Watch: ARPWatch keeps track of Ethernet/IP address pairings. This is useful when you suspect you are being arp-spoofed. Available at: <ftp://ftp.ee.lbl.gov/arpwatch.tar.Z>
- Snort: Snort is an excellent Intrusion Detection System and its arp-spoof preprocessor can be used to detect instances of ARP Spoofing, which might be an indication that someone on the network is Sniffing. Available at: <http://www.snort.org/>



# Finally how to protect my self or packet ?

---

We can protect my packet through

- ❑ SSL :secure socket layer to encrypted packet with different way 40 bit -128 bit to get secure channel for database communication or SMTP
- ❑ Also we use some thing call SSL over http in e-Commerce & E-mail "HTTPS"

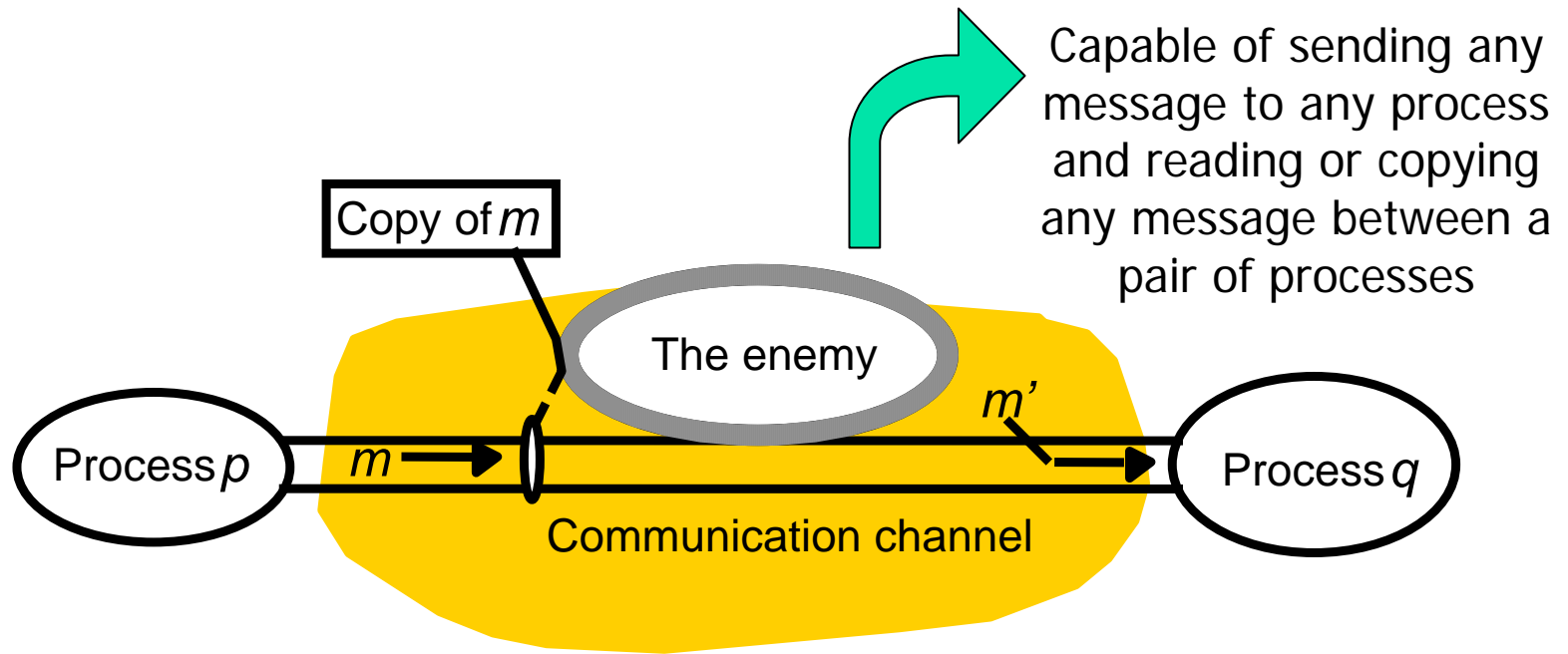
# Finally how to protect my self or packet ?

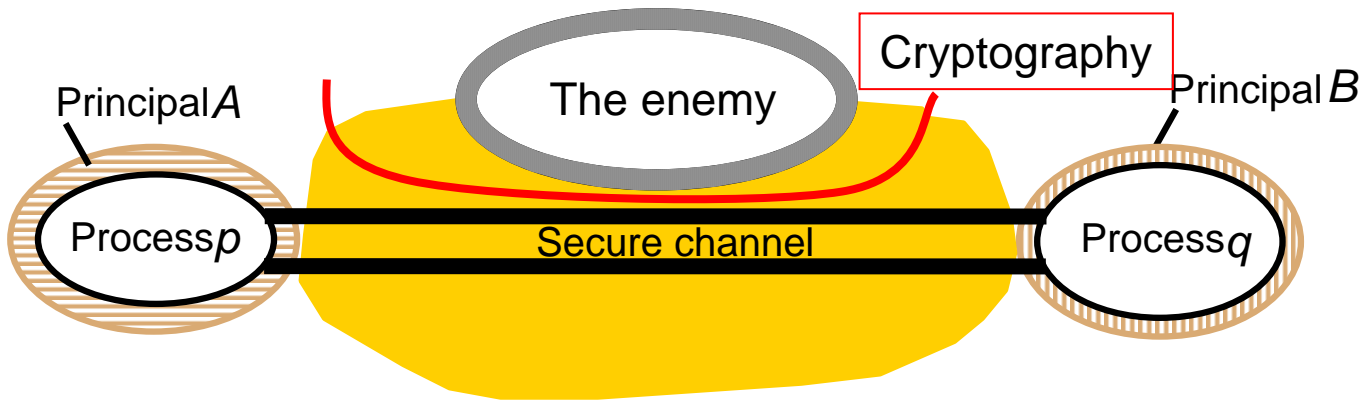
- ❑ TLS :Transport layer security which is based on SSL that need to use the certificates which now days called web-based certificates
- ❑ IPSec Protocol: it's worked in IP layer in N.W layer in OSI model it's encrypted all send packet .

<b>IP header</b>	<b>AH</b>	<b>TCP/UDP Header</b>	<b>application data</b>
------------------	-----------	-----------------------	-------------------------



# Security Model (1)







# Resources

---

- [http://en.wikipedia.org/wiki/Packet\\_sniffing](http://en.wikipedia.org/wiki/Packet_sniffing)
- <http://www.robertgraham.com/pubs/sniffing-faq.html>
- [http://www.securiteam.com/unixfocus/Detecting\\_sniffers\\_on\\_your\\_network.html](http://www.securiteam.com/unixfocus/Detecting_sniffers_on_your_network.html)



# Ultra Network Sniffer

---



# Sniffing SW

---

- Ultra Network Sniffer is a powerfully network visibility tools. It consists of a well-integrated set of functions that you can use to resolve network problem.
- Ultra Network Sniffer will list all of network packets in real-time from multi network card (Include Modem ,ISDN,ADSL) and also support capturing packet base on the application.
- Ultra Network Sniffer will capture the evidence of network intrusions
- Ultra Network Sniffer allows the network administrator to capture and retrace the steps of any network user



# Features

---

- Monitor network activity in real time.
- Dynamic network statistics and chart.
- Expert HTML Export.
- Get Permanent, Lifetime free software updates for register user.
- Capture network traffic for detailed analysis.
- Capture network traffic base on application (TDI,SOCKET).
- Probe the network with active tools to simulate traffic, measure response times, and troubleshoot problems
- Powerful packet generator in order to analyze network status and resolve troubleshoot.
- Supports all of windows version (Windows XP/2000/NT/ME/98/95);



# How to use it

---

- After installing Ultra Network Sniffer, Choose network adapter that you want to monitor, and click on Start Capture button in main toolbar.
- The Capture menu offers the following commands:



ID	Source Address	Destination Address	Length	Summary	Protocol	Time
141	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32792 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
142	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32792 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
143	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32792 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
144	10.0.0.2:138	10.0.0.255:138	216	UDP: src = 138, dst = 138, len = 182(0x00B6)	UDP	2006-11
145	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32795 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
146	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32795 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
147	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32795 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
148	10.0.0.2:138	10.0.0.255:138	243	UDP: src = 138, dst = 138, len = 209(0x00D1)	UDP	2006-11
149	10.0.0.2:138	10.0.0.255:138	216	UDP: src = 138, dst = 138, len = 182(0x00B6)	UDP	2006-11
150	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32800 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
151	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32800 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
152	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32800 OP = QUERY Name = WORKGROUP <1B>	WINS	2006-11
153	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32802 OP = QUERY Name = WORKGROUP <1E>	WINS	2006-11
154	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32802 OP = QUERY Name = WORKGROUP <1E>	WINS	2006-11
155	10.0.0.2:137	10.0.0.255:137	92	WINS: REQ. ID = 32802 OP = QUERY Name = WORKGROUP <1E>	WINS	2006-11
156	10.0.0.138:3626	239.255.255.250:1900	313	UDP: src = 3626, dst = 1900, len = 278(0x0117)	UDP	2006-11

```

ETHERNET: 00:14:38:08:BE:7D --> 00:90:D0:F5:4C:3D ETYPE = 0x0800, Protocol = Internet Protocol
  * ETHERNET: Destination Address = 00:90:D0:F5:4C:3D
  * ETHERNET: Source Address = 00:14:38:08:BE:7D
  * ETHERNET: Protocol = Internet Protocol
+ IP: 10.0.0.2 --> 64.236.22.112 ID = 0x00A4, Protocol = TCP, Length = 40(0x0028)
+ TCP: src = 1045, dst = 80, ack = 0x24573141, ACK
    
```

```

0x00: 00 90 D0 F5 4C 3D 00 14 38 08 BE 7D 08 00 45 00  L=..8.%}..E.
0x10: 00 28 00 A4 40 00 80 06 98 CE 0A 00 00 02 40 EC  .(.%@.ف.`خ....@ى
0x20: 16 70 04 15 00 50 1F 50 F2 81 41 31 57 24 50 10  .p...P.P`A1W$P.
0x30: FF FF 9F EA 00 00  ```è..
    
```





# SW interface

---

- This window displays packets as they arrive from the wire. The packet display window allows you to select specific packets to be shown in the Decoder Window, It also allows you to right click a specific packet and perform certain functions on it.
- User can drag packet to packet generator windows for send the packet to network.



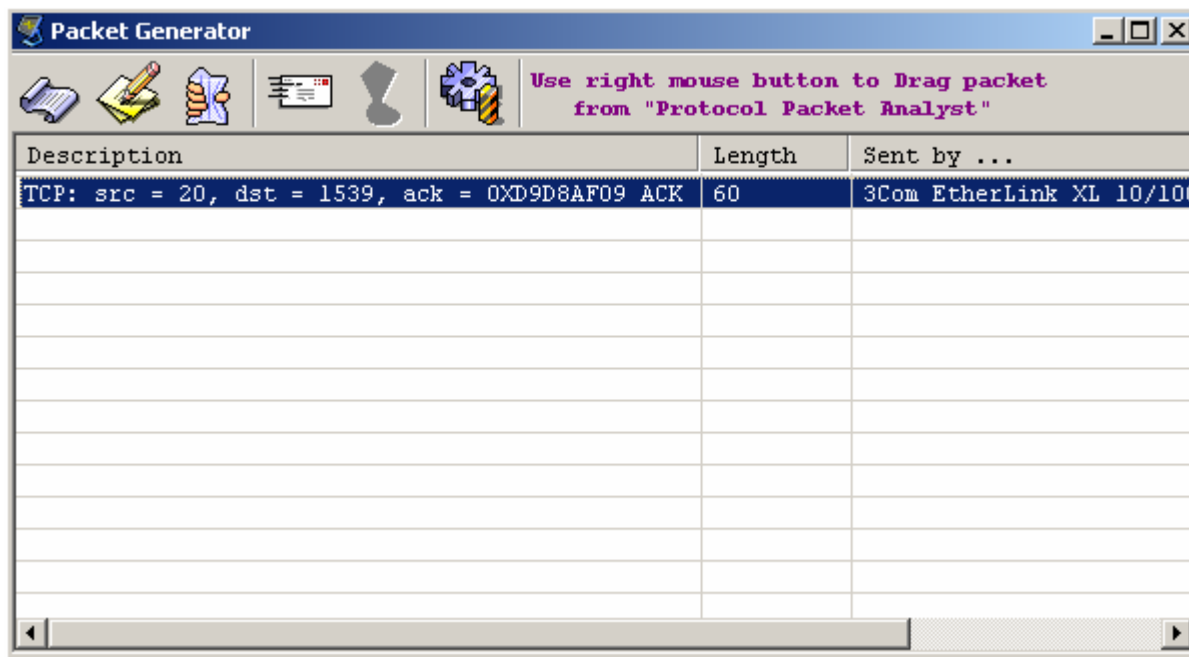
# Packet Decoder

---

- This window is used to display information about the structure of the packet from Packet List window, in an easy to understand tree form.
- This provides a simpler way of displaying the various aspects of the packet.
- Each header it finds (MAC Header, IP Header, ICMP Header, TCP Header, and UDP Header) will be broken down, displaying each part of the packet and the data it contains within.

# Packet Generator

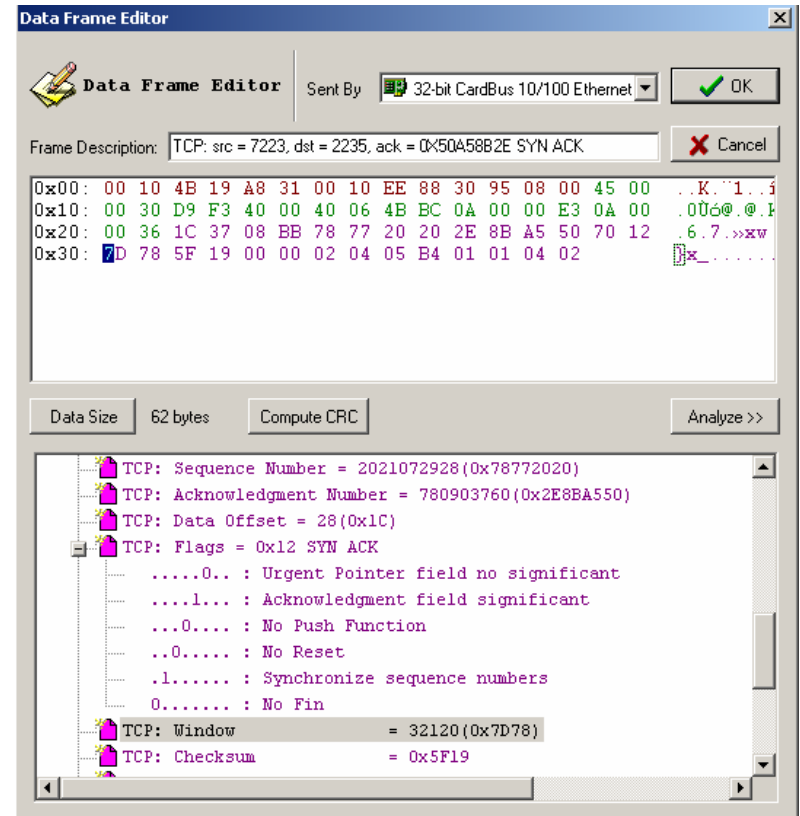
- Packet Generator allows you to edit and send packets via your network card



# Packet editor



- The Data Frame Editor allows user to change the packet contents and have the packet decode displayed in the bottom window as you edit it.
- You can create packets of any kind; you can choose which network adapter to send this packet. User can use compute CRC to automatically correct checksum.





# How to filter packet

---

- Examples: only capture data from 10.0.0.2 and "ip" protocol.
  1. Select main menu "monitor-->option"
  2. select page named "Protocol Filter"
  3. Uncheck all protocol and Only check protocol "IP" and its parent protocol and child protocol.
  4. Select page named "Advance filter".
  5. Check IP method in list box,you will see a list in right part of page.
  6. There are thee button on right of list,buttion "+" is used for adding one IP Filter,"-" is used for deleting one IP filter . "." is used for modifying.
  7. Click button "+" to add ip filter.IP filter dialog will show.
  8. Fill 10.0.0.2 ip into station1 and fill "any ip address" to staton2 fields on dialog.
  9. Fill the interested protocol into Protocol Type.
  10. Fill direction between stations into dir.
  11. Mode: Include is used for discarding all of matching packet.  
Exclude is used for only capturing all of matching packet.

thank's for all