COMPUTING SUBJECT:	Packet sniffer
TYPE:	Assignment
IDENTIFICATION:	PACKET SNIFFER
COPYRIGHT:	*Michael Claudius*
LEVEL:	Easy
TIME CONSUMPTION:	1-2 hours
EXTENT:	50 lines
OBJECTIVE:	Packet sniffer in theory and practice
PRECONDITIONS:	Computer Networking Ch. 2.2, 2.7
COMMANDS:	

IDENTIFICATION: PACKETSNIFFER/MC

The Mission
First step to overlook/analyze network traffic and/or sniff packets is to set up a packet sniffer, which can capture all the ingoing, outgoing and ongoing traffic.
We are going to explore the basic concepts behind packet sniffers and have a look at some providers.

Useful links for this assignment

http://en.wikipedia.org/wiki/Packet_sniffer
http://en.wikipedia.org/wiki/Wireshark
http://www.wireshark.org
http://www.winpcap.org

1. Use of packet sniffers
Give examples of what packet sniffers can be used for by good guys and bad girls....

2. Packet sniffer providers
There are many well known and massively tested packet sniffers:

- dSniff
- Ettercap
- Network General Sniffer
- Network Instruments Observer
- PRTG
- snoop (Solaris)
- tcpdump
- Wireshark (formerly known as Ethereal[1])
- WPE (Winsock packet editor)
- dSniff

We shall focus on Wireshark. Take a look at Wikipedia-link Wireshark.

3. Download and install
Wireshark is using a packet capture program WinPcap (*http://www.winpcap.org*). Wireshark normally comes with the winpcap program and can be downloaded from the provider:

http://www.wireshark.org

Download and install WinPcap first if you choose separate download **(DON'T DO THAT).**

4. Packet sniffing
Start up Wireshark and try to perform an analysis. No filter just try to capture all packets.
Try to visit some home pages or let another student visit homepages while you are sniffing..
Later take a look at the captured http-packets.