Wireshark - Tutorial

by Johannes Klick
Install Wireshark

- For installing Wireshark under Windows or MacOS please visit: http://www.wireshark.org.

- Wireshark is usually available on common Linux-Distributions.
  - **Attention**: You will need Root-Access to install and run Wireshark!
Wireshark – Default screen

Default screen on start.
For capturing packets you need to select a device by pushing "Start".
Now you can see some captured packets and also their type of protocol, source / destination address, payload etc.
Getting details

Just click on a packet to get more details about it.
See inside the packet

If you want to get more information about a special header of the packet, open the protocol you are interested in.

Click here to get more Information about the Ethernet header.

MAC addresses
By clicking on the destination MAC address you will see the used bytes in the data window in hexadecimal representation.
If you are interested in specific packets only you can use the display filter. In this example, only packets with the IP Source Address 87.77.156.23 appear.
The display filter also supports complex Boolean expressions.
If you need more information than provided in this small tutorial please visit:

http://www.wireshark.org/docs/wsug_html_chunked/

Thank you.