

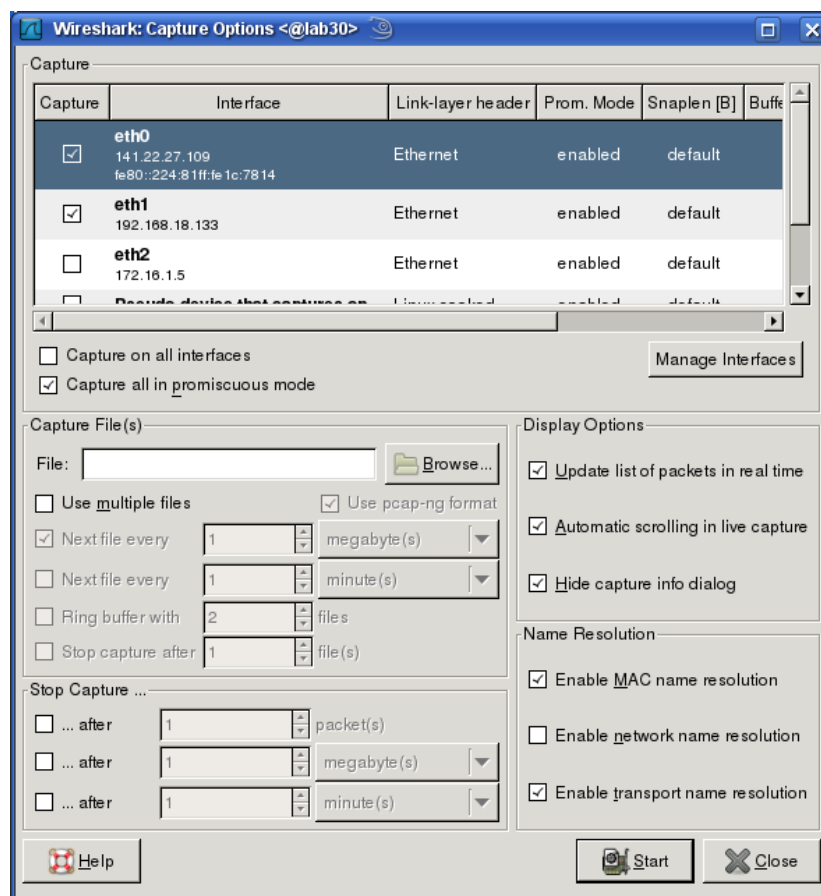
Network sniffer (*wireshark*)

Help texts on functionalities and options are available by moving the mouse cursor over the desired item.

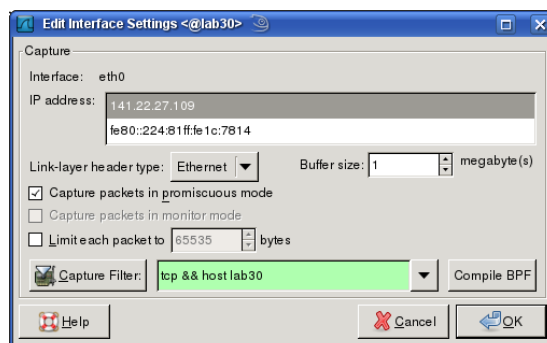
Before first use access to the display must be granted by issuing the **xhost +** command.

1. Step: Set up '*Capture - Options*':

Click  in the main window or in the Capture menu.



- Select *Interface(s)* according to desired network(s).
- *Capture Filters* can be set up by double-clicking the desired interface:



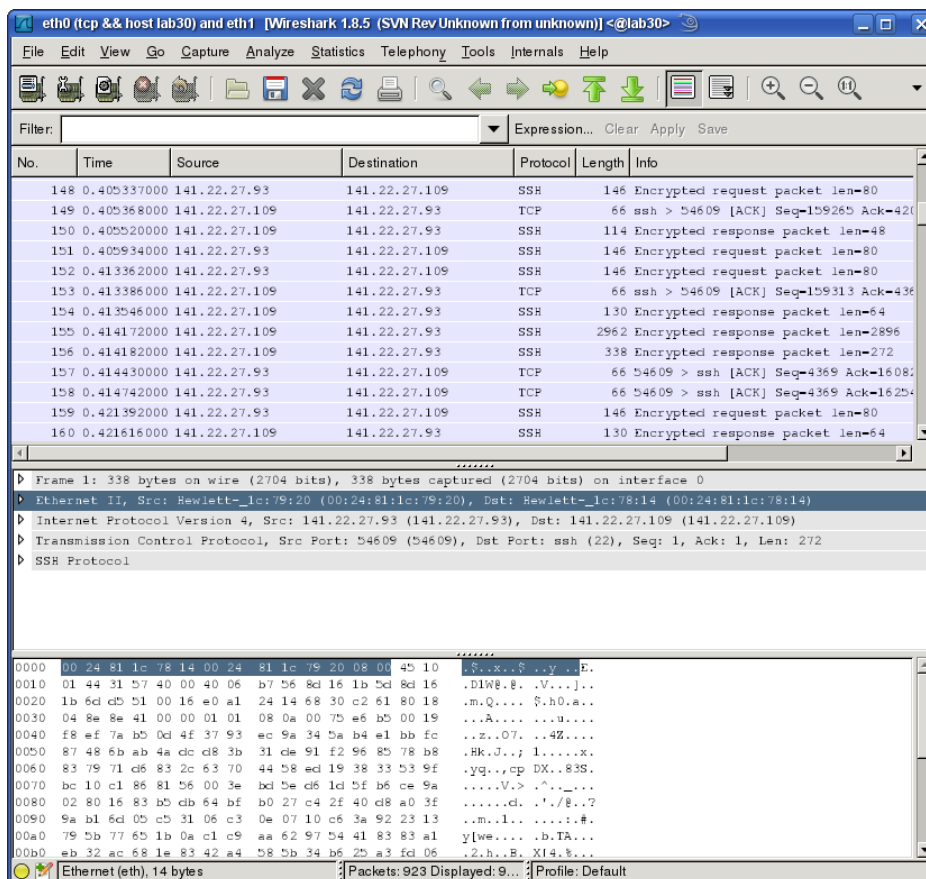
(This example: TCP protocol, host name lab30). Boolean operators (&&, ||,...) can be used to combine multiple conditions. Predefined filters are available by clicking the "Capture Filter" button.

Refer to the Wireshark Documentation or the man pages for further details on filtering.

2. Step: Start the sniffer ('*Capture – Start*')

The capture can be stopped by clicking the *Stop*-Button  or through *Capture – Stop*.

3. Step: Evaluation



- upper third of the window: chronological list of captured packets
- mid third of the window: details of the currently selected packet
- lower third of the window: native data of the selected packet (left: hex, right: ASCII)

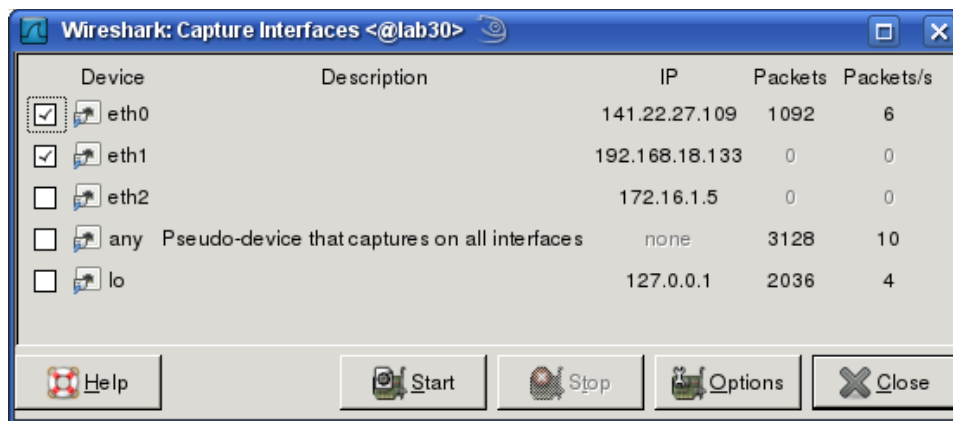
NB: Information displayed may be based on Wireshark's interpretation of native data.

4. Step: Saving a snapshot can be done:

- as text: Menu **File – Print** – choose **Plain text** and **Output to file**.
The packet range and format can be set individually. Choosing "Packet summary line" and deselecting "Packet details" will produce an output similar to the contents of the upper third of Wireshark's window.
- for viewing the snapshot off-line or further processing with analysing tools choose **File – Save** or **File – Save As...**

Further functionalities and settings:

1. Choosing **Capture – Interfaces** gives an overview of the network traffic on all interfaces.



Clicking **Options** the options for the selected card can be set. Clicking **Start** will start a new capture on the selected interfaces.

2. **Display filter** ("Filter" button): This filter merely suppresses displaying of all packets that do not match the given criteria. Unlike the *Capture*-filter all packets are still available in the buffer, so they can be made visible by clicking **Clear** at any time.
3. The meaning of colours can be looked up through **View – Coloring Rules** or the equivalent button. Enabling and disabling can be done in the **View – Colorize Packet List** Menu.
4. **Sequence numbers** (TCP): Relative numbering is used by default. This can be changed through **Edit – Preferences** under **Protocols – TCP**.
5. **Follow TCP Stream**: If you select a packet from the list in the upper third of the window that is part of a TCP session, you can choose "Follow TCP Stream" from the context menu to view the data exchange of this session in a separate window. In connection with this a **display filter** will be set automatically.
6. **Man pages** can be viewed from the Help menu:

