|  |  |
| --- | --- |
|  | **2015** |
|  | The Company  Martien Huijsmans |

|  |
| --- |
| **[wireshark]** |
| Installation and usage |

Inhoud

[Home page 1](#_Toc417152021)

[Linux Installation 1](#_Toc417152022)

# Home page

todo

# Linux Installation

Sudo yum install wireshark-gnome

Wireshark is a big program with many plugin. It is split into a small program that runs as root and an application that runs in user space. After default installation steps are needed to be able to start wireshark in user space and see the interfaces, that only root component(dumpcap) can see.

For user USERXYZ execute following commands to be able to start wireshark in user mode.

*$ ls -ls /usr/sbin/dumpcap*92 -rwxr-x---. 1 root wireshark 87720 Mar 5 15:44 /usr/sbin/dumpcap

List the groups that I am part of  
*$ groups USERXYZ*

Asd existing user USERXYZ to existing group wireshark  
*$ sudo usermod -a -G wireshark USERXYZ*

Now reboot, because permission are read at startup.  
*$ sudo reboot*

Enter following command to start wireshark  
$ wireshark&