**Wireshark**

Download latest Wireshark source code (stable release wireshark-2.4.4.tar.xz) from this link <https://www.wireshark.org/download.html>. After downloaded successfully untar it by using tar command as mentioned below. Install some supporting packages to make run Wireshark.

tar –xvf wireshark-2.4.4.tar.xz

**Follow the below version details**

|  |  |
| --- | --- |
| Linux OS | Ubuntu v16.04 LTS |
| Kernel | V4.4.0-109 |
| Wireshark | V2.4.4 |

**Pre-requisites to install supporting packages before build Wireshark source**

1. sudo apt-get install bison
2. sudo apt-get install flex
3. sudo apt-get install g++
4. sudo apt-get install libpcap-dev
5. sudo apt-get install autotools-dev
6. sudo apt-get install automake
7. sudo apt-get build-dep wireshark
8. sudo apt-get install qt5-default
9. sudo apt-get install libssl-dev
10. sudo apt-get install libgtk-3-dev

**Steps to be followed for building Wireshark source code**

1. Goto Wireshark top directory i.e., wireshark-2.4.4 and run ./configure command in command prompt.
2. If all the required packages for Wireshark are not installed on your system then the ./configure command will fail. Install the packages mentioned below and try the same command again.
   1. sudo apt-get install libgcrypt11-dev
   2. sudo apt-get install libglib2.0-dev
   3. sudo apt-get install qtools5-dev-tools
   4. sudo apt-get install libminiupnpc-dev
   5. sudo apt-get install libtool-bin
3. Run sudo make command to build the Wireshark source code in command prompt.
4. After build completed successfully, then run ./wireshark command to launch the Wireshark.

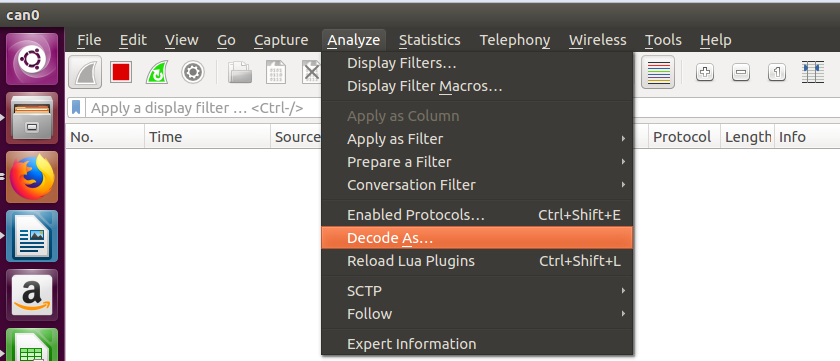
---------------------------------------------------------------------------------------------------------------------

**Steps to add sub dissector code changes into Wireshark source**

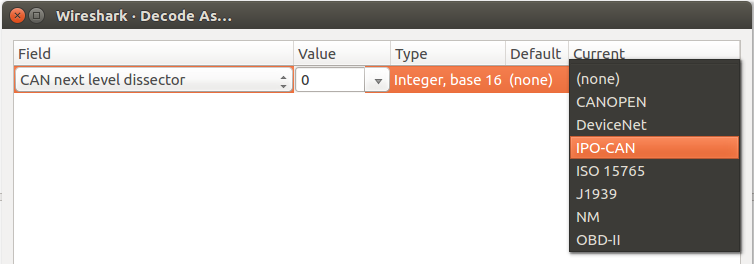
1. There are 4 files modified and added a new file as well.
2. Replace modified proto.c file into appropriate path “Wireshark-2.4.4/epan/”.
3. Replace modified CMakeLists.txt file into appropriate path “Wireshark-2.4.4/epan/dissectors/”.
4. Replace modified Makefile.am file into appropriate path “Wireshark-2.4.4/epan/dissectors/”.
5. Replace modified packet-socketcan.c file into appropriate path “Wireshark-2.4.4/epan/dissectors/”.
6. Add new file packet-ipocan.c into appropriate path “Wireshark-2.4.4/epan/dissectors”.
7. Do make clean and goto Wireshark source top directory (Wireshark-2.4.4) and run this command “./configure –-prefix=${HOME}/build/root” in command prompt. Here, ${HOME}/build/root path denotes that where you want to load the binaries after built.
8. Then, run this command “make install” to install the updated Wireshark with new changes.

**Steps to use sub-dissector in a Wireshark**

1. Open Wireshark by run this command “./wireshark”.
2. Go to Analyze menu and select an option “Decode As”.



1. Select + symbol to add subdissector which you have created newly and select “field” tab which has “CAN next level dissector” option to choose.
2. Select the option “None” from “current” tab which lists the number of available subdissectors for CAN. Then, select your subdissector which needs to be used.



1. Run appropriate command and to view the details of dissected packet displayed in Wireshark which is triggered from your subdissector.

---------------------------------------------------------------------------------------------------------------------