APT FILE PATH : /var/cache/apt/archives/

Ubuntu 20.04 LTS/22.04

REALISATION D’UN IMSI-CATCHER 4G HALF-MIDDLE MAN AVEC OPENLTE: Les attaques avancées possibles avec un half man in the middle (fake bts seulement mais sans fake ms)

Lecture : version de OpenLTE

* <https://openlte.sourceforge.net>
* <https://sourceforge.net/projects/openlte/files/>

Installation des dépendances de OpenLTE

# python3-pyqt4 python-qt4 libgsi-dev libssl1.0-dev libqt4-opengl-dev libssl1.0-dev

# libnicursesw5-dev libpython-dev python-pip

**apt-get install libboost-dev libpython3.8-dev cmake build-essential python3-qwt python3-guiqwt python3-pyqt5.qwt libgmp-dev libxi-dev libcppunit-dev libx11-6 libx11-dev flex libncurses5 libncurses5-dev libncursesw6 libpcsclite-dev libsdl1.2-dev zlib1g-dev libmpfr6 libmpc3 lemon aptitude libtinfo-dev libtool shtool autoconf git-core pkg-config make libmpfr-dev python-cheetah libmpc-dev libtalloc-dev libfftw3-dev libgnutls28-dev libtool-bin python-lxml libxml2-dev python-sip sofia-sip-bin libsofia-sip-ua-dev sofia-sip-bin bison libgmp3-dev alsa-oss asn1c libdbd-sqlite3 libboost-all-dev libusb-1.0-0-dev python-mako python3-mako doxygen python-docutils cmake build-essential g++ python-numpy python3-numpy swig libsqlite3-dev libi2c-dev libwxgtk3.0-gtk3-dev freeglut3-dev composer phpunit python3-pip libfontconfig1-dev libxrender-dev python-sip-dev python-sphinx\* libusb-dev libusb-1.0.0-dev libcomedi-dev libzmq3-dev**

# libpython-dev libncursesw5-dev

**apt-get install build-essential libgmp-dev libx11-6 libx11-dev flex libncurses5 libncurses5-dev libncursesw6 libpcsclite-dev zlib1g-dev libmpfr6 libmpc3 lemon aptitude libtinfo-dev libtool shtool autoconf git-core pkg-config make libmpfr-dev libmpc-dev libtalloc-dev libfftw3-dev libgnutls28-dev libtool-bin libxml2-dev sofia-sip-bin libsofia-sip-ua-dev sofia-sip-bin bison libgmp3-dev alsa-oss asn1c libdbd-sqlite3 libboost-all-dev libusb-1.0-0-dev python-mako python3-mako doxygen python-docutils cmake build-essential g++ python-numpy python3-numpy swig libsqlite3-dev libi2c-dev libwxgtk3.0-gtk3-dev freeglut3-dev composer phpunit python3-pip**

Pour plus de comprehension : <https://github.com/ImsicatcherBastienbaranoff/OpenLTE_RedirectionPatch/blob/main/all_patch.patch>

Remplacer par if((devs[idx-1]["type"] == "soapy")) par :

if((devs[idx-1]["type"] == "soapy")||(devs[idx-1]["type"] == "uhd"))

Pour limeSDR :

--- a/LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc2 2019-11-29 16:51:43.643623681 +0100

+++ b/LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc 2019-11-29 16:42:13.751607399 +0100

@@ -252,8 +252,6 @@

usrp->set\_rx\_freq((double)liblte\_interface\_ul\_earfcn\_to\_frequency(ul\_earfcn));

usrp->set\_tx\_gain(tx\_gain);

usrp->set\_rx\_gain(rx\_gain);

+ usrp->set\_tx\_antenna("BAND2");

+ usrp->set\_rx\_antenna("LNAH");

// Setup the TX and RX streams

tx\_stream = usrp->get\_tx\_stream(stream\_args);

rx\_stream = usrp->get\_rx\_stream(stream\_args);

**setxkbmap fr**

**git clone https://github.com/ettusresearch/uhd**

**git checkout aea0e2de34803d5ea8f25d7cf2fb08f4ab9d43f0**

**cd uhd/**

**cd host/**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**git clone https://github.com/pothosware/SoapySDR**

**cd SoapySDR/**

**git chekcout f722f9ce5b629c3c44401a9bf628b3f8e67a9695**

**mkdir build**

**cd build**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**git clone https://github.com/nuand/BladeRF**

**cd BladeRF/**

**git checkout 45521019c540392287eb6e03d52b8073b2fd0743**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**git clone https://github.com/pothosware/SoapyBladeRF**

**cd SoapyBladeRF/**

**git checkout 1c1e8aaba5e8ee154b34c6c3b17743d1c9b9a1ea**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**git clone https://github.com/pothosware/SoapyUHD**

**cd SoapyUHD/**

**git checkout 47972ba8b96beffb79915e300acea168bacd8d84**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**git clone https://github.com/myriadrf/LimeSuite**

**cd LimeSuite**

**git checkout c931854ead81307206bce750c17c230181065545**

**mkdir build**

**cd build**

**cmake ..**

**make**

**make install**

**ldconfig**

**git clone https://github.com/gnuradio/gnuradio**

**cd gnuradio/**

**git checkout 2d7f82342c1d63a1c4d7e18eb1289636ebcbb855**

**git submodule init && git submodule update**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**git clone https://github.com/osmocom/gr-osmosdr**

**cd gr-osmosdr/**

**git checkout 4d83c60**

**mkdir build**

**cmake ..**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

(commande en une seule ligne)

**wget https://src.fedoraproject.org/repo/pkgs/polarssl/polarssl-1.3.7-gpl.tgz/b656e4c83ee94f93d19eb0832fd7f976/polarssl-1.3.7-gpl.tgz**

ou

**git clone https://github.com/ImsicatcherBastienbaranoff/polarssl && cd polarssl**

**tar xvzf polarssl-1.3.7-gpl.tgz**

**cd polarssl-1.3.7**

**mkdir build**

**cd build**

**cmake ..**

**make**

**make install**

**ldconfig**

Compilez openlte avec redirection :

Pour plus de comprehension : <https://github.com/ImsicatcherBastienbaranoff/OpenLTE_RedirectionPatch/blob/main/all_patch.patch>

**git clone https://github.com/bbaranoff/openlte**

**cd openlte/**

**git checkout 4bd673b**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**LTE\_fdd\_enodeb**

**cd ..**

Compilez la dernière version de OpenLTE à savoir qu’il y a d’autres attaques en utilisant git checkout nom\_attaque

Some attacks implemented by [@onkarmumbrekar](https://github.com/onkarmumbrekar) can be found in the different branches:

* <https://github.com/ImsicatcherBastienbaranoff/Advanced_LTE_ATTACK>
* <https://drive.google.com/drive/folders/1u5bRMle3_iirDNfIEe8toGC4WDKfvkA5?usp=share_link>
* <https://github.com/mgp25/OpenLTE>
* akabypass
* attach\_reject
* dos\_tau\_reject\_dualcase
* dos\_tau\_reject
* malformed\_detach
* numb\_attack
* service\_reject\_on\_tau
* tau\_numb\_attack

Pour plus d’info veuillez lire l’article :

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE/**

**mkdir build**

**cd build && cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

Testons les autres cas, si jamais le checkout n’existe plus, il se trouve dans le drive du lien en haut

Fixing problem bladerf : <https://github.com/ImsicatcherBastienbaranoff/OpenLTE_Patch_AdvancedAttack>

gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**setxkbmap fr**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**git checkout akabypass**

**mkdir build/**

**cd build/**

**cmake ..**

**rm -rf \***

**cmake ..**

**make**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**cmake ..**

**make**

**make install**

**cd ..**

**cd ..**

**zip -r OpenLTE\_akabypass.zip OpenLTE/**

**rm -rf OpenLTE**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**git checkout attach\_reject**

**mkdir build/**

**cd build/**

**cmake ..**

**rm -rf \***

**cmake ..**

**make**

**cd ..**

**find -name LTE\_fdd\_enb\_radio.cc:**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**cmake ..**

**make**

**make install**

**cd ..**

**zip -r OpenLTE-attach\_reject.zip OpenLTE**

**rm -rf OpenLTE**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**checkout dos\_tau\_reject**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**cd ..**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**cmake ..**

**make**

**make install**

**cd ..**

**zip -r OpenLTE-dos\_tau\_reject.zip OpenLTE**

**rm -rf OpenLTE**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**git checkout malformed\_detach**

**cd build/**

**rm -rf \***

**ls**

**cmake ..**

**make**

**cd ..**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**cmake ..**

**make**

**make install**

**cd ..**

**zip -r OpenLTE-malformed\_detach.zip OpenLTE**

**rm -rf OpenLTE**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**mkdir build**

**cd build/**

**cd ..**

**git checkout numb\_attack**

**cd build/**

**cmake ..**

**rm -rf \***

**cmake ..**

**make**

**cd ..**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**cmake ..**

**make**

**make install**

**cd ..**

**zip -r OpenLTE-numb\_attack.zip OpenLTE**

**ls**

**rm -rf OpenLTE**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**git checkout service\_reject\_on\_tau**

**cd build/**

**ls**

**rm -rf \***

**cmake ..**

**make**

**cd ..**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

**zip -r OpenLTE-service\_reject\_on\_tau.zip OpenLTE**

**rm -rf OpenLTE**

**git clone https://github.com/mgp25/OpenLTE**

**cd OpenLTE**

**git checkout tau\_numb\_attack**

**cd build/**

**rm -rf \***

**cmake ..**

**make**

**cd ..**

**find -name LTE\_fdd\_enb\_radio.cc**

**gedit LTE\_fdd\_enodeb/src/LTE\_fdd\_enb\_radio.cc**

Regarder la fonction : bladerf\_get\_timestamp puis remplacer BLADERF\_MODULE\_RX par BLADERF\_RX

Remplacer tous : BLADERF\_MODULE\_TX par BLADERF\_TX\_X1

BLADERF\_MODULE\_RX par BLADERF\_RX\_X1

**cd build/**

**make ..**

**make**

**make install**

**cd ..**

**zip -r OpenLTE-tau\_numb\_attack.zip OpenLTE**

**rm -rf OpenLTE**

FUTUR CAS : AJOUTER PWS DANS OPEN\_LTE

liblte\_rrc.h

|  |
| --- |
| typedef struct{ |
|  | LIBLTE\_RRC\_PAGING\_RECORD\_STRUCT paging\_record\_list[LIBLTE\_RRC\_MAX\_PAGE\_REC]; |
|  | LIBLTE\_RRC\_PAGING\_V890\_IES\_STRUCT non\_crit\_ext; |
|  | LIBLTE\_RRC\_SYSTEM\_INFO\_MODIFICATION\_ENUM system\_info\_modification; |
|  | LIBLTE\_RRC\_ETWS\_INDICATION\_ENUM etws\_indication; |
|  | uint32 paging\_record\_list\_size; |
|  | bool system\_info\_modification\_present; |
|  | bool etws\_indication\_present; |
|  | bool non\_crit\_ext\_present; |
|  | }LIBLTE\_RRC\_PAGING\_STRUCT; |

Insertion de fonction SIB10,11,12

LIBLTE\_ERROR\_ENUM liblte\_rrc\_pack\_sys\_info\_msg(LIBLTE\_RRC\_SYS\_INFO\_MSG\_STRUCT \*sibs,

LIBLTE\_BIT\_MSG\_STRUCT \*msg)

….

case LIBLTE\_RRC\_SYS\_INFO\_BLOCK\_TYPE\_7:

case LIBLTE\_RRC\_SYS\_INFO\_BLOCK\_TYPE\_9:

case LIBLTE\_RRC\_SYS\_INFO\_BLOCK\_TYPE\_10:

case LIBLTE\_RRC\_SYS\_INFO\_BLOCK\_TYPE\_11:

gedit liblte/src/liblte\_rrc.cc

Recherchons : IE Name: System Information Block Type 10

(s’il n’arrive pas à faire de recherche enlever les espaces avant et derrières le texte à chercher)

Ajoutons le code proprement dit

Recherchons : IE Name: System Information Block Type 11

(s’il n’arrive pas à faire de recherche enlever les espaces avant et derrières le texte à chercher)

Ajoutons le code proprement dit

Recherchons : IE Name: System Information Block Type 12

(s’il n’arrive pas à faire de recherche enlever les espaces avant et derrières le texte à chercher)

Ajoutons le code proprement dit

**SRS\_LTE WITH CMAS**

sudo apt-get install cmake libfftw3-dev libmbedtls-dev libboost-program-options-dev libconfig++-dev libsctp-dev :

git clone <https://github.com/Risteel/srsLTE_cmas_etws>

mkdir build

cd build

cmake ..

make

make install

ldconfig

# [Installing HackRF Software — HackRF documentation](https://hackrf.readthedocs.io/en/latest/installing_hackrf_software.html)

# [How to install hackrf on Ubuntu 20.04 (Focal Fossa)? (devmanuals.net)](https://www.devmanuals.net/install/ubuntu/ubuntu-20-04-focal-fossa/installing-hackrf-on-ubuntu20-04.html)

git clone <https://github.com/mossmann/hackrf.git>

cd hackrf/host

mkdir build

cd build

cmake ..

make

sudo make install

sudo ldconfig

git clone https://github.com/pothosware/SoapyHackRF.git

cd SoapyHackRF/

mkdir build && cd build

cmake ..

make

sudo make install

SoapySDRUtil --info

Available factories...hackrf, null,

SoapySDRUtil --probe="driver=hackrf"

SoapySDRUtil --make="driver=hackrf"

# [Installing SoapySDR SoapyHackRF SoapyRTLSDR SoapyRemote CubicSDR (github.com)](https://gist.github.com/0x00-0xFF/c543b5b0ed8568f1c9e7)

NOTE : [HackRF – RTL-SDR – GNU RADIO Setup – F1ATB](https://f1atb.fr/index.php/2020/08/06/hackrf-orange-pi-gnuradio-setup/)

[GNU Radio first steps: a FM receiver (abclinuxu.cz)](https://www.abclinuxu.cz/blog/jenda/2019/11/gnu-radio-first-steps-a-fm-receiver)

INTERESSANT GFSK ET FM :

[ubuntu18 + gnuradio + gr-osmosdr + hackrf one GFSK文本音频传输接收\_osmosdr ubuntu\_平平无奇的小机灵的博客-CSDN博客](https://blog.csdn.net/whcyxx_begin/article/details/112364748)

GNURADIO 3.8 : [How to Install GNU Radio 3.8 in Ubuntu 20.04 & Fix Warning: failed to XInitThreads() - YouTube](https://www.youtube.com/watch?v=6gx9xfAC6Wk)

[www.youtube.com/watch?v=6gx9xfAC6Wk](http://www.youtube.com/watch?v=6gx9xfAC6Wk)

1. open terminal
2. do this command on terminal

sudo add-apt-repository ppa:gnuradio/gnuradio-releases-3.8

sudo apt-get update

sudo apt install gnuradio gnuradio-dev

3. Wait until finish

InstallWEB DEENDANCIES : <https://wiki.gnuradio.org/index.php?title=Old_Ubuntu_Deps>

apt-get install liblog4cplus-1.1-9 liblog4cplus-dbg liblog4cplus-dev liblog4cpp-doc

sudo apt install git cmake g++ libboost-all-dev libgmp-dev swig python3-numpy \

python3-mako python3-sphinx python3-lxml doxygen libfftw3-dev \

libsdl1.2-dev libgsl-dev libqwt-qt5-dev libqt5opengl5-dev python3-pyqt5 \

liblog4cpp5-dev libzmq3-dev python3-yaml python3-click python3-click-plugins \

python3-zmq python3-scipy python3-gi python3-gi-cairo gir1.2-gtk-3.0 \

libcodec2-dev libgsm1-dev libusb-1.0-0 libusb-1.0-0-dev libudev-dev

Desinstall gnuradio :

**git clone https://github.com/gnuradio/gnuradio**

**cd gnuradio/build**

**make uninstall**

**git submodule init && git submodule update**

**mkdir build**

**cd build/**

**cmake ..**

**make**

**make install**

**ldconfig**

**cd ..**

Desinstall puis reinstall gr-osmosdr pour checkout 3.8 :

**cd gr-osmosdr/**

*git checkout gr3.8*

**mkdir build**

**cmake ..**

**cd build/**

**cmake ../ -DENABLE\_DOXYGEN=1**

**make**

**make install**

**ldconfig**

**cd ..**

sudo apt-get install -y pkg-config swig liborc-0.4-dev

git clone https://gitlab.com/librespacefoundation/gr-soapy

cd gr-soapy

mkdir build

cd build

cmake .. -DCMAKE\_INSTALL\_PREFIX=/usr

make -j

sudo make install

sudo ldconfig

3.7 : [Linux Ubuntu 20.04安装UHD和GNU Radio\_linux安装gnuradio\_JingsenJiao的博客-CSDN博客](https://blog.csdn.net/ARQJohnson/article/details/123204594)

PYBOMBS :

<https://dsp-lab.net/2021/08/20/post-268/>

GIT [Ubuntu 20.04安装UHD 15.0.0和GNURadio 3.8.1.0 - 简书 (jianshu.com)](https://www.jianshu.com/p/5215e0a93c14)

git clone --recursive <https://github.com/gnuradio/gnuradio>

# [ModuleNotFoundError - GNU Radio](https://wiki.gnuradio.org/index.php/ModuleNotFoundError)

## E. Store the commands in a Bash start-up file[[edit](https://wiki.gnuradio.org/index.php?title=ModuleNotFoundError&action=edit&section=5)]

Once you have determined the correct two export commands to use, open your text editor and put them in your ~/.bash\_aliases or ~/.bashrc or ~/.profile file. Save the file. There are three ways for these changes to take effect.  
1. On your terminal enter exit. Then start a new terminal.  
2. Type source NAME\_OF\_FILE\_EDITED (e.g. source ~/.profile ).  
3. Reboot your computer.

As an example, your entries might be:

export PYTHONPATH=/usr/local/lib/python3/dist-packages:/usr/local/lib/python3.8/dist-packages:$PYTHONPATH

export LD\_LIBRARY\_PATH=/usr/local/lib:$LD\_LIBRARY\_PATH

## F. Starting GNU Radio from GUI[[edit](https://wiki.gnuradio.org/index.php?title=ModuleNotFoundError&action=edit&section=6)]

If you get the ModuleNotFoundError error while starting GNU Radio from GUI, but can start GNU Radio using the terminal, it is because the environment variables are set for the terminal, but not for your graphical environment. Try one of the listed solutions below.

1. Store the export commands stated in Part E in ~/.profile. Log out and back in for the changes to take effect.  
2. Store the export commands stated in Part E in a new shell script (with any name of your choice) in /etc/profile.d/. Restart your computer thereafter.