

Telive - Tetra live receiver v0.8

(c) 2014 Jacek Lipkowski <sq5bpf@lipkowski.org>

Description

Telive is a program which can be used to display information like signaling, calls etc from a Tetra network. It is also possible to log the signalling information, listen to the audio in realtime and to record the audio. Playing the audio and re-compressing it into ogg is done via external scripts. The software is based upon slightly modified osmocom-tetra software.

Prerequisites

Before installing please read all licenses, disclaimers, documentation for all installed packages, and about the Tetra protocol (i will not explain term like MNC, Colour Code, Usage identifier, SSI etc).

The software was tested on Debian GNU/Linux 6.0 and 7.0 64 bit versions (with the codec compiled in a 32-bit environment). Other linux distributions should work, but i have not tested them. It should probably be possible to run this software on other systems, but i haven't tried, and don't intend to (however if it works for you, please send me a detailed description so that i can add it to the docs).

Receiving is done using a RTL2832/R820T DVB-T USB dongle. Probably other receivers supported by gnuradio will work with minor modifications.

The following software needs to be installed:

Packages from your distribution

Install oggenc (package vorbis-tools under debian), sox (package sox), aplay (package alsa-utils), ncurses development libraries (package libncurses-dev). You will need all of the development packages, but that will be installed by build-gnuradio. If you have installed any gnuradio packages, then uninstall/purge them.

Gnuradio 3.6 (not 3.7!) with osmosdr support.

Probably the easiest way is to use the build-gnuradio script provided by SBRAC:

<http://www.sbrac.org/files/build-gnuradio>

Please run ./build-gnuradio -o (the -o parameter installs version 3.6).

Currently build-gnuradio doesn't support some newer versions of distributions, for example debian 7.4 is supported, but 7.7 is not. In case of debian this can be hacked around easily by modifying the line (around line 607):

```
*6.0*|*wheezy*|*sid*|*7.1*|*7.0*|*7.2*|*7.3*|*7.4*)
```

to read:

```
*6.0*|*wheezy*|*sid*|*7.1*|*7.0*|*7.2*|*7.3*|*7.4*|*7.5*|*7.6*|*7.7*|*7.8*|*7.9*)
```

Similar hacks should be possible for other distributions.

After building, test if the software works. There are many gnuradio-companion scripts on the internet, see if they work, and also use them to find the right ppm value for your rtl-sdr dongle.

libosmocom-sq5bpf

This is Osmocom libosmocom, the original software is here:

<http://bb.osmocom.org/trac/wiki/libosmocom>

Please read all documentation for this project.

The version in my repository is not patched in any way, but may be patched in the future.

To compile and install:

```
git clone https://github.com/sq5bpf/libosmocom-sq5bpf
cd libosmocom-sq5bpf
autoreconf -i
./configure
make
sudo make install
```

osmo-tetra-sq5bpf

This is a patched version of Osmocom osmo-tetra, the original software is here:

<http://tetra.osmocom.org/trac/wiki/osmo-tetra>

To compile:

```
git clone https://github.com/sq5bpf/osmo-tetra-sq5bpf
cd osmo-tetra-sq5bpf
cd src
make
```

The scripts receiver1 and receiver2 assume that you are in this directory (osmo-tetra-sq5bpf/src).

Tetra codecs

Please read the instructions in osmo-tetra-sq5bpf/etsi_codec-patches , including README_sq5bpf. This shows how to obtain and compile the codecs. Warning: the codecs won't run when compiled for 64-bits, please either use a compiler that produces 32-bit binaries, or set up a 32-bit build system in chroot(). See "Setting up a 32-bit build environment" on how to setup a 32-bit build environment under debian (might also work under other debian-derived distros like ubuntu or mint). Put the tetra codecs in /tetra/bin (created in the next step).

telive

To compile:

```
git clone https://github.com/sq5bpf/telive
cd telive
make
sudo mkdir /tetra
sudo chown YOURUSER.YOURGROUP /tetra
chmod 755 install.sh
./install.sh
```

The scripts rxx and rxx2 assume that you are in this directory.

Optional step

Get the latest wireshark from the repository. Wireshark can parse GSMTAP messages which are sent via tetra-rx and display the decoded Tetra frames.

Theory of operation

Please refer to Fig 2. The RF signal is received via a rtl-sdr dongle and gnuradio (the receiver is conveniently provided as an gnuradio-companion flow graph to aid easy modification). The received channel is passed via a named pipe /tmp/fifo1 to a CQPSK demodulator `simdemod2.py`. The demodulator output is fed to `float_to_bits` ("bit slicer"), and further to `tetra-rx` (which decodes the tetra protocol). `tetra-rx` sends some packets encapsulated in UDP to localhost. These packets are received with the `telive` program.

The `telive` program shows a list of possible usage identifiers (0-63, where 0-2 are reserved), and aggregates signaling information (SSI addresses etc) for each usage identifier. If there are any voice frames, then this information can be recorded or played back immediately. Later the recording is renamed to a filename containing the date, time and the last 3 SSI numbers seen for this usage identifier.

The `tetra-rx` program has been modified to receive SDS messages, and these messages can be logged by the `telive` program.

The `telive` program has these settings:

mutessi - allow recording and playback of data for a usage identifier with no SSI data (useful, because it suppressed the playback of encrypted data)

alldump - don't filter signaling information, show all in the log and in the message window

mute - mute playback audio (but not the recording)

record - record audio

log - log signalling information to file (default `telive.log`)

verbose – verbosity level (more shows more debug info)

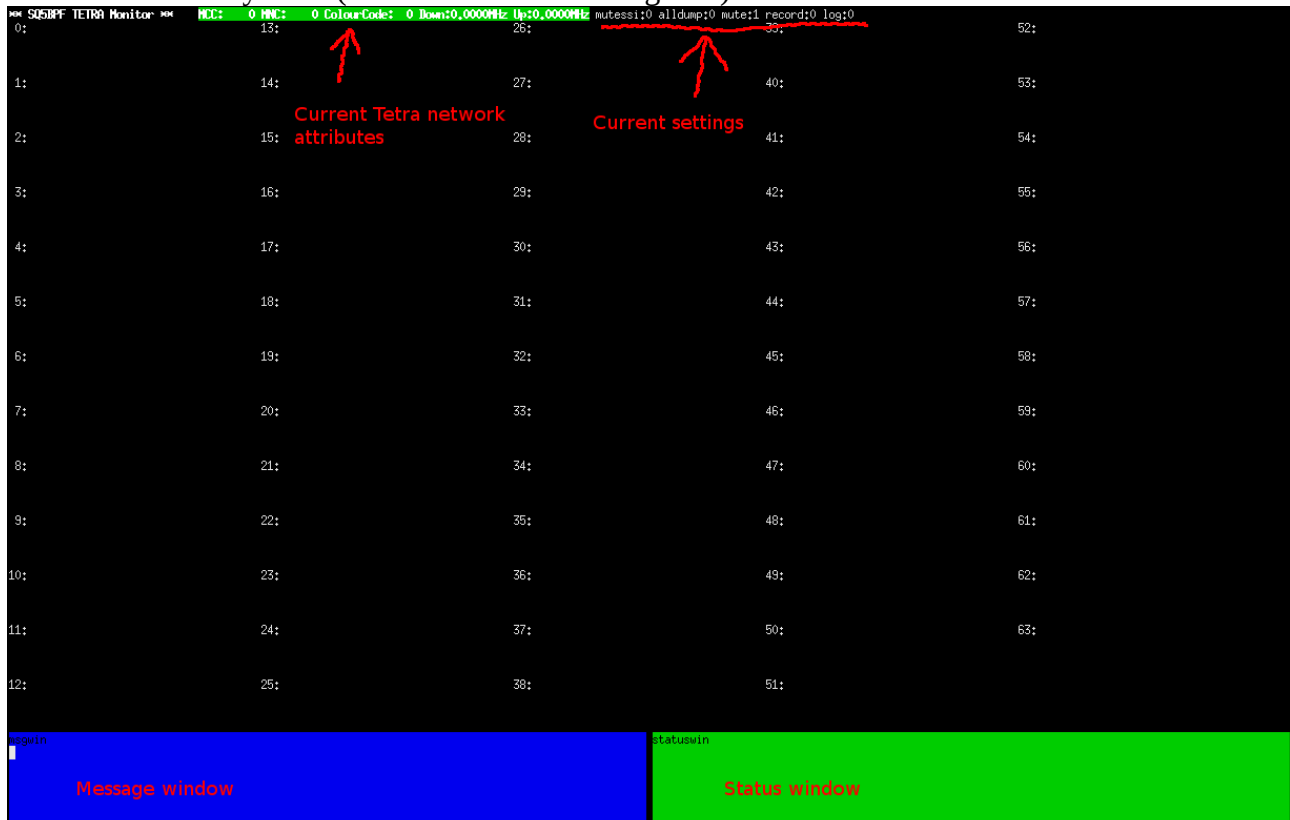


Fig 1. `telive` program screen

Keyboard commands:

? - show help in the status window

m - toggle *mutessi*

M - toggle *mute*

r - refresh screen (warning: segfaults sometimes, to be fixed)

R - toggle *record*

a - toggle *alldump*

l - toggle logging

s - stop play (if there are multiple channels active, this will end the active playback and search for another channel to play).

V/v – increase/decrease verbosity

The numbers 0-63 are the usage identifiers. If you see OK near the number then there is voice traffic present on it. If you see PLAY then this is the currently playing channel.

There can be multiple tetra-rx programs feeding data to one telive process, but be certain that they are on the same tetra network (same uplink/downlink, same colour code etc) - refer to Fig 3 for an example. It is also possible to feed totally different channels (from one or more gnuradio instance), each to its own named pipe, have many processes to decode them, and feed multiple telive processes from the receiver processes.

The message window shows tetra signaling messages (SETUP, RELEASE etc). The status window will show various information regarding program status (depending on the verbosity level), and text SDS messages.

Telive records the calls in in ACELP codec format. You can use the script tplay to play them, or tetrad to automatically encode them into OGG format.

Simple 1 channel setup example:

This is a simple receiver for one frequency only (it is best to use the control channel frequency, as it contains the most signaling information).

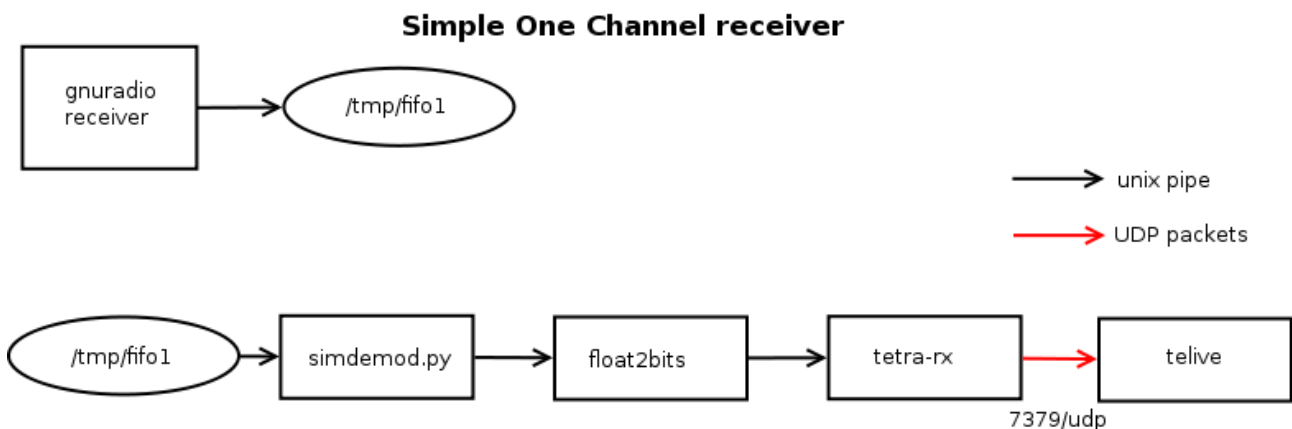


Fig 2. Simple one channel receiver

Open an xterm, change directory to the `osmo-tetra-sq5bpf/src` directory and execute

`./receiver1 1`

There should be no errors. This creates `/tmp/fifo1`, and listens for incoming data, piping it into `simdemod2.py`, `float_to_bits` and `tetra-rx`

Open another xterm with:

```
/usr/bin/xterm -font fixed -bg black -fg white -geometry 203x60
```

Change to the telive directory and execute:

```
./rxx
```

This launches the telive console. In the telive console pressing shift-R enables recording of voice calls, and pressing L enables logging. If you hear too much gibberish press m (enables mutessi).

In another xterm launch `/tetra/bin/tetrad` - this will recode voice in the ACELP format into OGG format, and put it into `/tetra/out`

Connect a rtl-sdr dongle and antenna. Open `telive_1ch.grc` (from the `telive/gnuradio-companion` directory) in `gnuradio-companion`, and run it. Currently `telive_1ch.grc` defaults to 435.500MHz and 56ppm. Please adjust the tuner main frequency, offset and ppm to receive a known strong tetra signal (preferably unencrypted). Correct the ppm value so that the spectrum looks "symmetrical".

If all is set up correctly, the xterm where `receiver1` is run should scroll a lot of text, while the telive console should display the MCC, MNC, Colour Code and uplink/downlink frequencies for the control channel. If there is any traffic you should see some SSI numbers on the console, and maybe hear some voice (voice is muted with the key command shift-M).

Two channel setup example

This is a receiver for two frequencies, preferably one signaling channel, and some other channel from the same network. The setup is similar to Fig. 2, but there are two `receiver1` processes, and `gnuradio` receives two channels simultaneously. Please refer to Fig 3

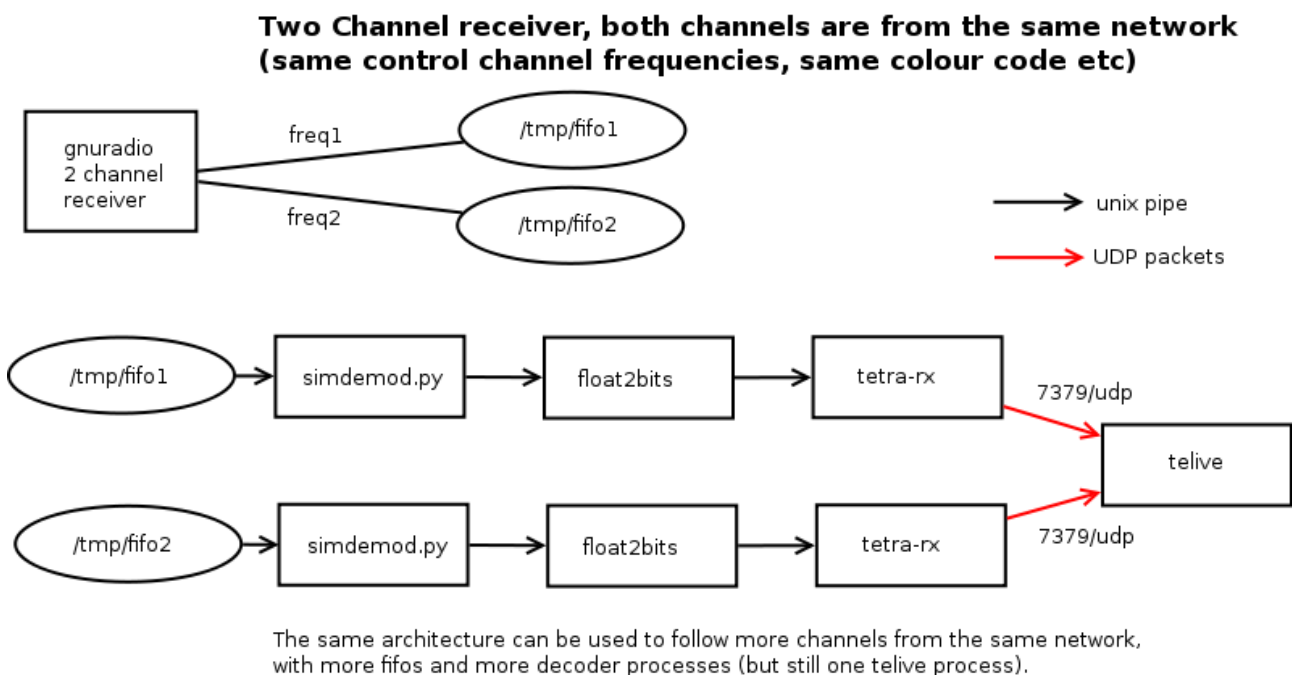


Fig 3. Two channel receiver setup

Open an xterm, change directory to the `osmo-tetra-sq5bpf/src` directory and execute

```
./receiver1 1
```

There should be no errors. This creates `/tmp/fifo1`, and listens for incoming data, piping it into `simdemod2.py`, `float_to_bits` and `tetra-rx`

Open an xterm, change directory to the `osmo-tetra-sq5bpf/src` directory and execute

```
./receiver1 2
```

There should be no errors. This creates /tmp/fifo2 , and listens for incoming data, piping it into simdemod2.py, float_to_bits and tetra-rx

Open another xterm with:

```
/usr/bin/xterm -font fixed -bg black -fg white -geometry 203x60
```

Change to the telive directory and execute:

```
./rx
```

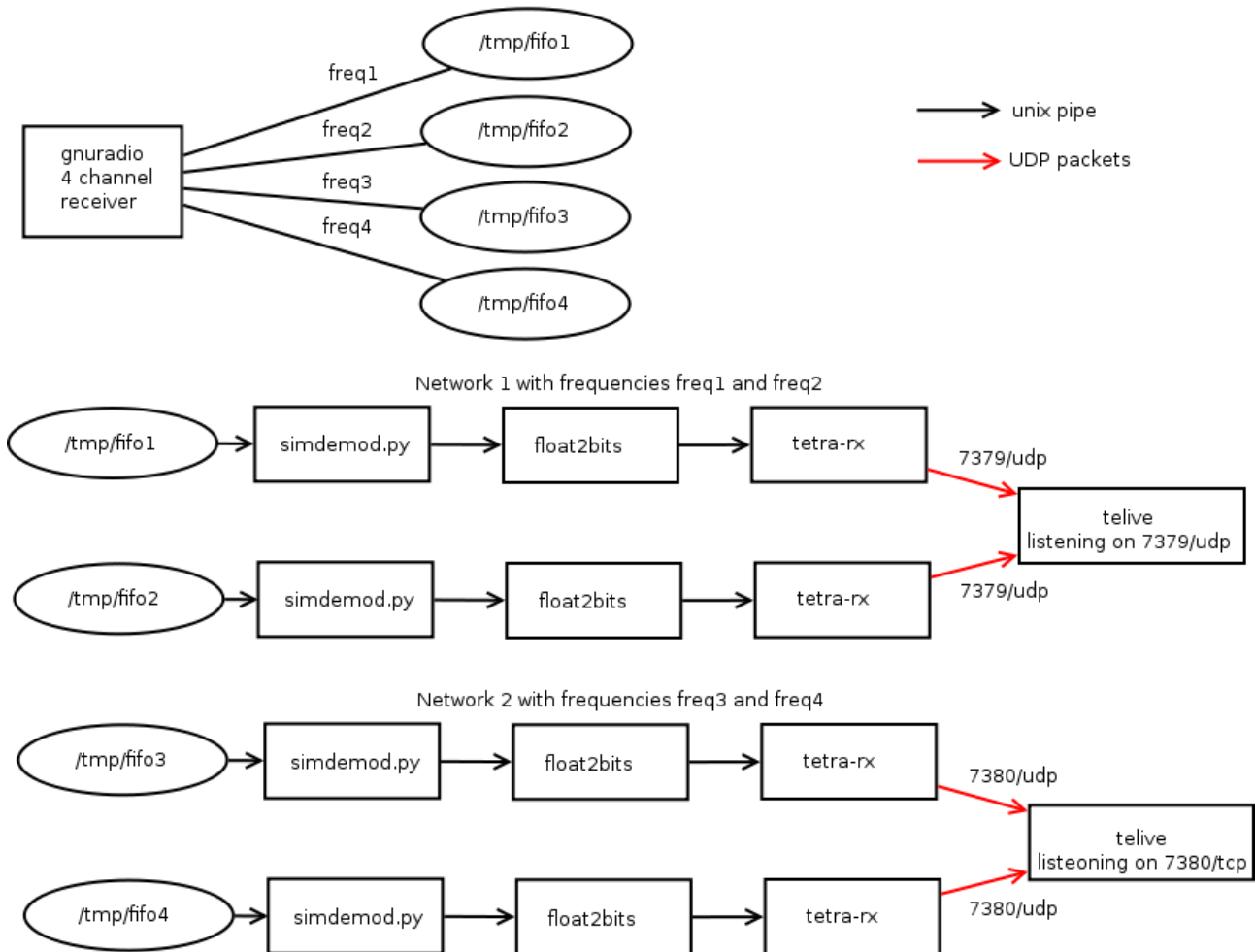
Connect a rtl-sdr dongle and antenna. Open telive_2ch.grc (from the telive/gnuradio-companion directory) in gnuradio-companion, and run it. Currently telive_2ch.grc defaults to 435.500MHz, 434.750MHz and 56ppm. Please adjust the tuner main frequency, offsets and ppm to receive a known strong tetra signal (preferably unencrypted). Correct the ppm value so that the spectrum looks "symmetrical"..

Please note that you will get more data then with the 1 channel receiver setup. If the tetra network attributes change in telive, then the two channels are not from the same network, and this won't work correctly.

Four channel, two networks setup

This is a receiver for four frequencies, to monitor two separate Tetra networks, each with two channels. This is basically the twice the Two channel setup from Fig. 3 .

**Four Channel receiver, 2 channels are from the same network,
and two channels from a different network**



The same architecture can be used to follow more channels from more networks, using many receivers and telive processes. You can also use multiple gnuradio receiver processes, each using its own usb dongle.

Fig 4. Four channel, two networks setup

Network 1:

Open an xterm, change directory to the `osmo-tetra-sq5bpf/src` directory and execute `./receiver1 1`

There should be no errors. This creates `/tmp/fifo1`, and listens for incoming data, piping it into `simdemod2.py`, `float_to_bits` and `tetra-rx`. This process will send data via UDP to `7379/udp`.

Open an xterm, change directory to the `osmo-tetra-sq5bpf/src` directory and execute `./receiver1 2`

There should be no errors. This creates `/tmp/fifo2`, and listens for incoming data, piping it into `simdemod2.py`, `float_to_bits` and `tetra-rx`. This process will send data via UDP to `7379/udp`.

Open another xterm with:

`/usr/bin/xterm -font fixed -bg black -fg white -geometry 203x60`

In the new xterm window that opened:

Check with `stty -a` that there are indeed 60 rows and 203 columns.

Change to the `telive` directory and execute:

`./rxx`

This `telive` process will listen to `7379/udp`

Network 2:

Create a directory /tetra2 analogous to /tetra. Setting up the various paths is left as an exercise to the reader.

Open an xterm, change directory to the osmo-tetra-sq5bpf/src directory and execute
./receiver2 3

There should be no errors. This creates /tmp/fifo3 , and listens for incoming data, piping it into simdemod2.py, float_to_bits and tetra-rx . . This process will send data via UDP to 7380/udp.

Open an xterm, change directory to the osmo-tetra-sq5bpf/src directory and execute
./receiver2 4

There should be no errors. This creates /tmp/fifo4 , and listens for incoming data, piping it into simdemod2.py, float_to_bits and tetra-rx . . This process will send data via UDP to 7380/udp.

Open another xterm with:

```
/usr/bin/xterm -font fixed -bg black -fg white -geometry 203x60
```

Change to the telive directory and execute:

```
./rxx2
```

This telive process will listen to 7380/udp

Connect a rtl-sdr dongle and antenna. Open telive_4ch.grc (from the telive/gnuradio-companion directory) in gnuradio-companion, and run it. Currently telive_4ch.grc defaults to 435.500MHz, 434.750MHz, 435.750MHz, 435.800MHz and 56ppm. Please adjust the tuner main frequency, offsets and ppm to receive a known strong tetra signal (preferably unencrypted). Correct the ppm value so that the spectrum looks "symmetrical".

Other setups

Please look at the scripts and the program sources. You can use multiple gnuradio receivers each with its own rtl-sdr dongle, and feed the results via named pipes to multiple receiver processes. The results can be displayed via multiple telive processes, each for one Tetra network.

End notes

This is code that i've written for my own pleasure. It is very ugly, but i've could either polish it so it looks nice, or "release early, release often" (per the open source methodology). Polishing it would take forever, and i believe that if one has a nice toy, he should share it with other children, rather than keep it to himself.

This code runs under linux, and was tested under Debian 6.0 and 7.0 64-bit versions. I will not answer questions how to make it work under opertating systems different than linux, however if you make it work, send me a description, so that i can put it into the documentation. Also i haven't really tried to make this user-friendly. The documentation is crap, despite my best efforts to write it. Basically read all of the documentation, the ETSI Tetra docs, and if you still don't understand something, then RTFS.

The architecture is modular, and you could probably use another receiver instead of gnuradio (like rtl_fm). This hasn't been tried, but should work, and should result in less CPU utilization.

The telive program uses the usage identifier as the key. This concept works, but is not correct. A more correct approach would be to use the notification id and receiver id. This will probably be implemented in some later version. The SDS decoding might not work in many cases. So far i've seen only type 0x82 (Text messaging), 8 bit encoding type SDS. 7-bit decoding might not work etc. I would also like to implement Location services, and data transfer services.

If you can provide samples of interesting traffic legally, then please do. It would be best if you have your own TMO Tetra network, that you could monitor, while changing various settings etc.

The core of this software: osmocom-tetra, libosmocore was written by Osmocom (i've only filled in some blanks, that others probably didn't want to fill in). As stated on their web page <http://tetra.osmocom.org/trac/wiki/FAQ> "Can I use OsmocomTETRA to listen to police radio? [...] Also, if this is your interest in this project: Please simply go away, we don't want to talk to you." - please respect this.

Disclaimer

I disclaim any liability because of the use of this software. If someone breaks something it's their fault. Also please observe the licenses. The telive software is licensed GPLv3. The osmosom-tetra software is licensed GNU Affero v3, and libosmocore is licensed GPLv2. The codecs are licensed by ETSI, and if i understand correctly, you can build binaries for yourself from the publically available source code, but might not be able to provide the binaries to others. IANAL, so don't take this as legal advice, if someone knows better, then please correct me on this.

TODO

Implement a better protocol to communicate with telive

Implement Location Information Protocol and Data Services

Don't use popen() for playback because of buffering.

Actually try to read the ETSI docs and not fall asleep after 20 pages.

Clean up the code, rewrite all comments in english (if there are any polish comments or variable names left).

Write proper documentation

FAQ

What does this software do?

It enables one to listen and record unencrypted TETRA calls, decode some SDS messages and log signalling information.

Where can I learn more about TETRA?

The TETRA standard is available from ETSI, go to <http://etsi.org> and search for TETRA. You will get more documents than you will ever want to read. Please note that TETRAPOL is something completely different (the only similarity being the first 5 letters :).

What operating systems does it run on?

It runs on linux. It was developed under Debian 6.0 64-bit and Debian 7.0 64-bit. Others have reported that it works under Kali linux, Mint and Ubuntu. Any Unix/Linux operating system should work with some tweaking, if you can get gnuradio working on it.

Does it work on Microsoft windows?

No. And i'm not interested in it. However you can run it in a virtual machine. Beware that a virtual machine doesn't run as fast as a normal installation, and might not be suitable for more advanced setups (monitoring multiple channels etc).

I don't understand all this, could you provide a nice description how to get it to work for people who don't know much about computers or radio?

Not really. Go away. And please don't send emails asking for this. Thanks!

If Linux is a problem, then go find some friendly linux user with at least basic skills (ie. one that can do something more then point the cursor at icons and press a button).

What is a usage identifier (also called usage marker)?

From the tetra docs: "A traffic usage marker is a 6-bit MAC label used during circuit mode calls for transmitter preemption, for prevention of crossed calls and for channel maintenance purposes. The BS shall assign a traffic usage marker before any traffic transmission takes place on an assigned channel."

This identifier is present during various call setup procedures, and also accompanies voice frames. This identifier is used by telive to bind voice traffic with signaling information. The identifiers 0-3 are reserved, and you should not see them in use in telive.

How can I record calls?

Press shift-R (the top line should read record:1). The calls are recorded in ACELP format in the directory /tetra/in. The script tetrad will recompress them into OGG files and put them in:

/tetra/out/YYYYMMDD/traffic_YYYYMMDD_HHMMSS_UU_SSI1_SSI2_SSI3.ogg

YYYYMMDD is year month date (like 20141127)

HHMMSS is hour minute second (like 230145)

UU is the usage identifier

SSI1, SSI2, SSI3 are the last 3 SSI numbers associated with this usage identifier

How can I log signalling?

Press L (the top line should read log:1). The log is in telive.log (this can be changed by setting the environment variable TETRA_LOGFILE). This log contains the signalling information in a readable form (not as long as the tetra-rx output), and SDS messages (the text messages should be decoded).

The most information is present in the tetra-rx output. To log it do:

```
./receiver1 1 2>&1 |tee -a /tmp/logfile
```

Beware that this will eat away many megabytes of disk space per minute.

I don't hear anything or something stutters, but the recordings are fine if I play them on another system

This has nothing to do with telive. Find some wave file and play it using aplay. Fiddle with the system until it's fixed (maybe change the mixer settings? See support forums for your distribution for possible fixes).

The telive program exits when it sees voice traffic. Why?

There is a problem running /tetra/bin/tplay , or a problem running sdecoder/cdecoder/aplay.

Something segfaults, how can I help debug it?

Please email me the result of these commands:

```
gdb program_that_segfaulted core
```

```
bt
```

The usage identifiers at the bottom are all on the same line, like 9:10:11:12: etc

This means that the xterm screen size is not 203x60 (maybe your window manager resized it). The software should still work, but the screen will be a bit unreadable.

I get fseek failed from receiver1

This means that something has closed /tmp/fifo... Most probably the gnuradio-companion receiver has died. Check for errors in the gnuradio-companion console.

I hear mostly unreadable audio

This is probably audio from encrypted calls, or some non-voice data. Enable mutessi – this will ignore usage identifiers which don't have at least one SSI number assigned.

Can I use a different receiver?

You can use any receiver that will be able to write baseband data to a pipe in the same format as gnuradio does.

How do I set up a 32-bit environment and compile the codecs?

Compiling the codecs needs a 32-bit environment for now, but most people have a 64-bit system installed. To compile under debian you can either set up a multi-arch environment, or install a separate build environment. Here i will describe how to set up a 32-bit build environment in chroot (i don't like to pollute my system with multiarch) under debian 7 64-bit (should work under other debian derived systems with minor modifications, please read the debootstrap manual). Please first read the full instructions is osmocode-tetra-sq5bpf/etsi_codec-patches. This is a "for dummies" version:

As root user do:

```
mkdir /build32
```

```
apt-get update
```

```
apt-get install debootstrap
```

```
debootstrap --variant=build --arch i386 wheezy /build32
```

```
mkdir /build32/root/codecs
```

```
#put the codec source and codec.diff in /build32/root/codec
cd /build32
#enter build environment
chroot /build32
apt-get install unzip
cd /root/codec
unzip -L en_30039502v010301p0.zip
patch -p1 -N -E < codec.diff
cd c-code
make
#exit build environment
exit
mkdir /tetra/bin
cd /build32/root/codec/c-code
cp cdecoder sdecoder /tetra/bin
```

tetra-rx reports Air Encryption:1, does this mean that all is encrypted?

No, this means that someone has paid money for the encryption license for their TETRA infrastructure. To use encryption each radio needs to have encryption enabled too, which also costs. So probably there will still be some radios (which are not used for secret communications), without encryption.

How do I find the ppm value quickly?

Although not recommended, this can be done also with this software. Set up everything up as in the “Simple 1 channel setup example”, and set the frequency to a known local strong transmitter. This doesn't have to be tetra, I usually use the VOLMET from the local airport for this. Now set the ppm slider so that the channel signal spectrum is symmetrical to 0kHz (in case of AM the carrier should be at 0kHz on the spectrum graph). The ppm value drifts with temperature, so determining the ppm should be done after the receiver has warmed up after at least 10 minutes.

The receiver doesn't work, no matter what frequency I tune it to. Gnuradio complains about PLL unock

You are probably not using the right format. Gnuradio expects to have frequency input in Hz. You can also use prefixes like k for kilo, M for mega etc. Quick example in the 1-channel demo: to listen to 435.2125MHz, you could use 435MHz baseband frequency and 212.5kHz offset (or for example 436MHz baseband and -787.5kHz offset). To tune enter 435M (not 435MHz!) for baseband frequency and press Enter, enter 212.5k for offset.

I get errors about the device being claimed by another driver

Probably the dvb_usb_rtl28xxu driver is loaded, this is the driver that can be used to watch TV using these dongles. To disable the module loading create a file /etc/modprobe.d/rtlsdr.conf containing the text:
blacklist dvb-usb-rtl28xxu
After this reboot

I get strange errors, I'm using Ubuntu

Some people report that a reboot solves these problems.

I have trouble when downloading software using the build-gnuradio script

Either the repository is not available at this time, or you have some Internet connectivity problems. Wait a few hours and try again.

OMG! Someone can listen to my secret tetra transmissions! The sky is falling!

Well, actually not. All these digital systems (Tetra, DMR, NXDN etc) have an option to either encrypt traffic or not. This is a major advantage over analog systems, where it was hard to encrypt. Now if a system doesn't have encryption enabled, than one can assume that it is a conscious choice of the system designer, and that the system is intended to be open to monitoring.

Of course the encryption algorithms are not public, so it is hard to tell if there are any flaws in them. Probably sooner or later someone will reverse engineer or leak them (as was with GSM A5/1 and other algorithms). And since there are not public, they were not subjected to public scrutiny, and may contain weaknesses (as was with GSM A5/1 and other algorithms). Please consider that all your encrypted traffic might be recorded today, and broken a few years from now. This is true of any technology, not just tetra.

But publishing this software makes it possible to monitor something that was not “monitorable” before. This changes everything

Well, actually not. The protocol specifications were publicly available for a long time and osmocom-tetra code has been available since 2011, patches to record audio have been floating around, and people had developed their own private versions. Also there is commercial software that enables TETRA monitoring like w-code from Wavecom. Publishing this code just makes the process less magical, and security hates magic.

Changelog:

20141207: added a bit to the FAQ --sq5bpf

20141206: Changed telive version to 0.8, added a bit to the FAQ --sq5bpf

20141127: Added the FAQ. Clarified a few things --sq5bpf