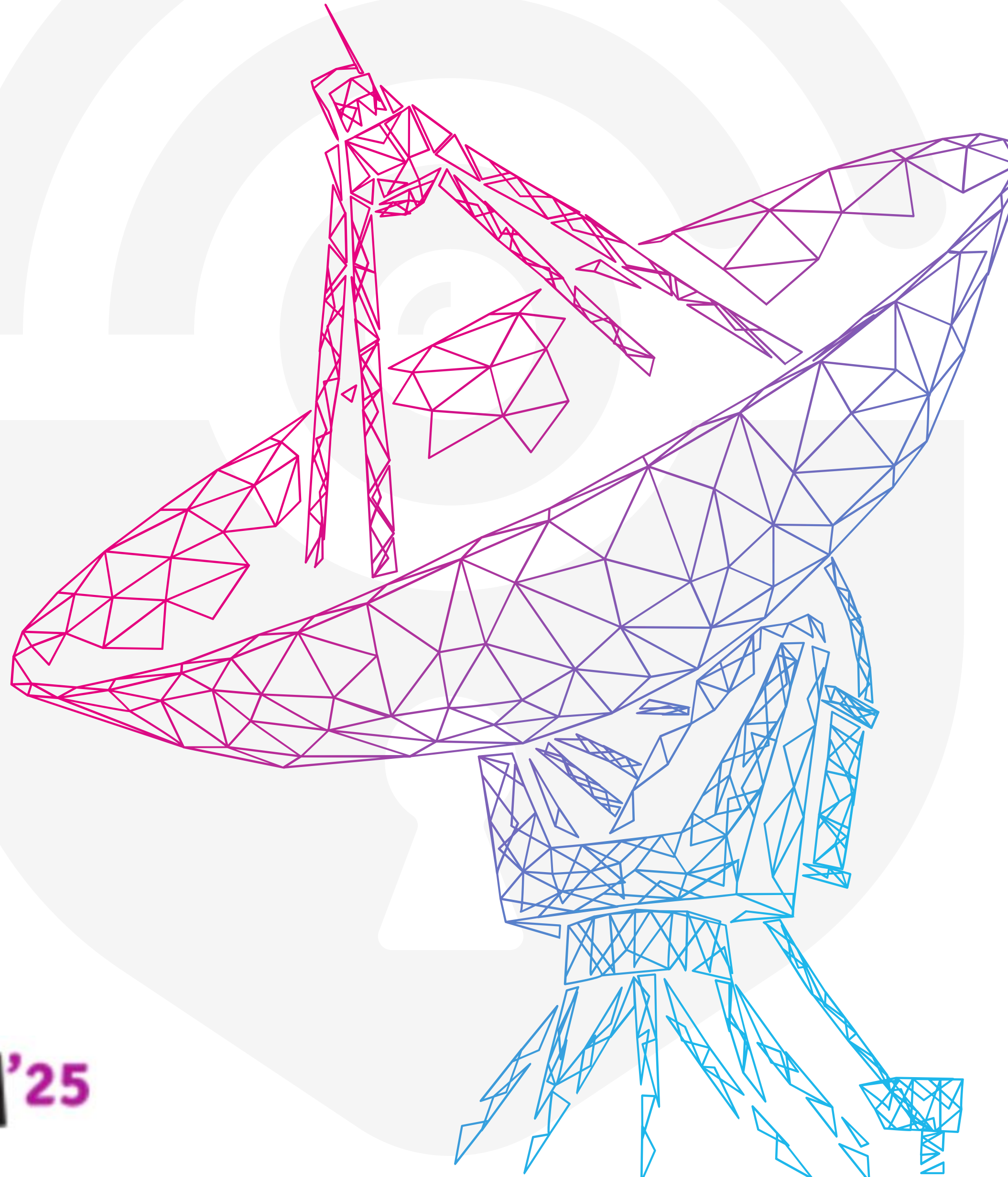
penthertz

RF Swift: a swifty toolbox for all wireless assessments

By Sébastien Dudek



FOSDEM'25

About myself

Founder of Penthertz

- Sébastien Dudek (@FlUxIuS)
- CEO of Penthertz
  - Founded during COVID in 2020
  - Specialized in Wireless communications security
- > 10 years of experience in Software & Hardware security
  - Security researcher
  - Pentester & Red Team
  - Vulnerability researcher

Perfect mix to make Penthertz!

Main activities

Security assessments

- Wireless communications (RFID, Wi-Fi, Mobile communications, Bluetooth, etc.)
- Embedded devices
- Backend servers
- Red Team

Trainings

- Software-Defined Radio Hacking
- Wi-Fi Red teaming
- RFID Hacking
- Mobile attacks (2G/3G/4G/5G), and more…

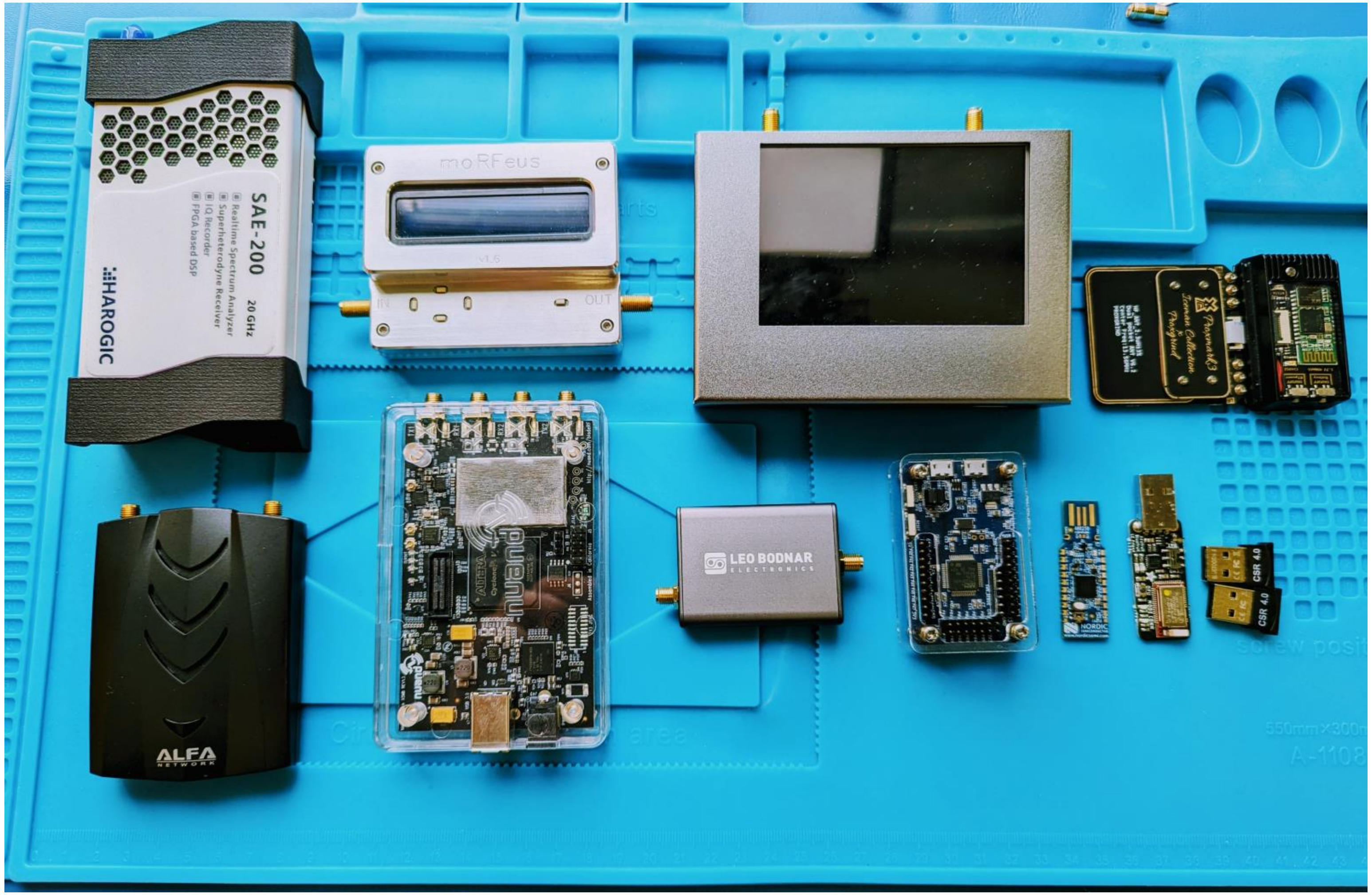
Hardware security

- Firmware extraction
- Chip off
- Secrets extraction
- Library's analysis
- Vulnerability hunting

RF Pentester 010:
Having a good setup

Setup

A minimum setup for assessments



Setup

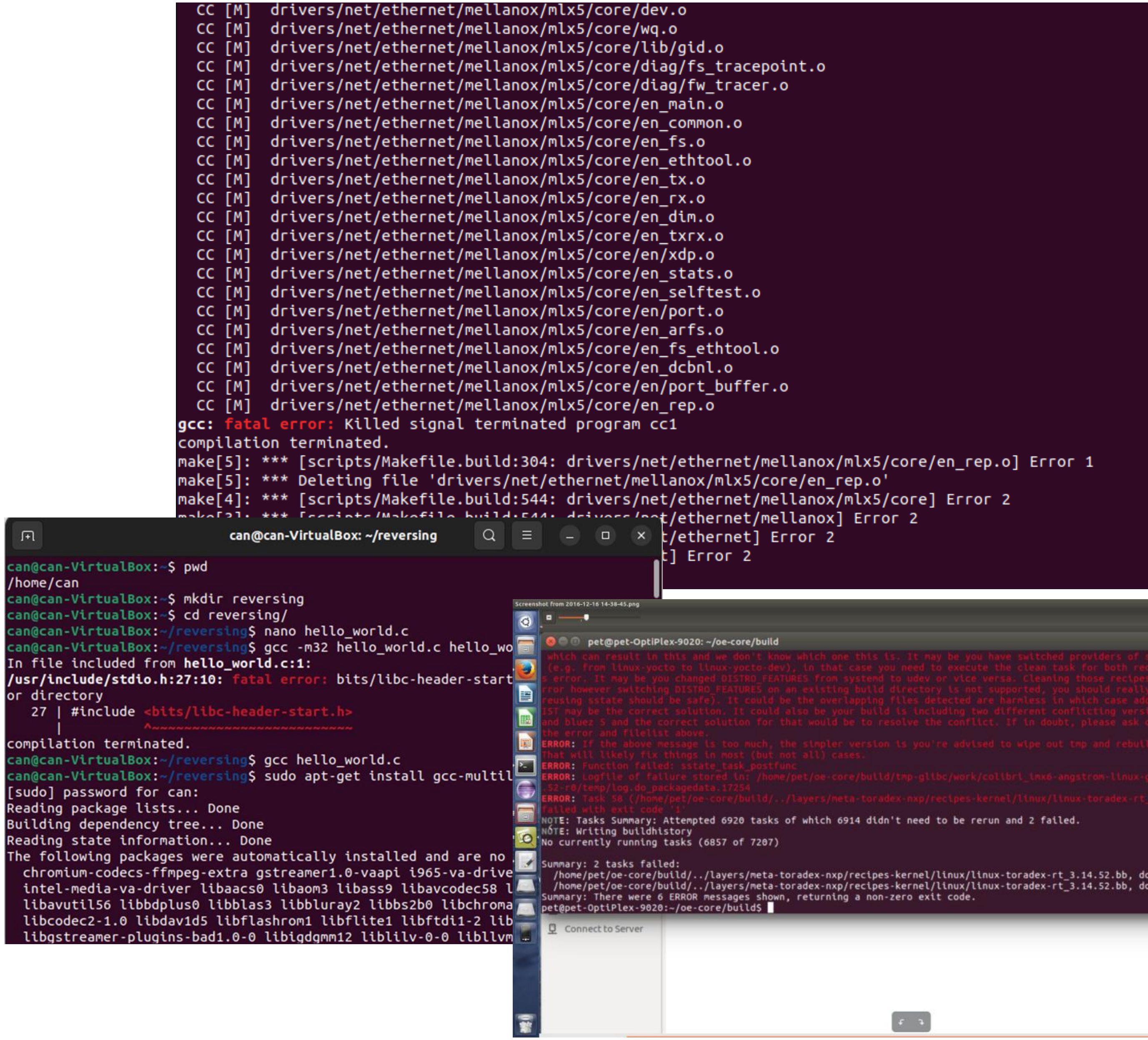
Software setup

- We need all required pentests tools for different context:
  - Wi-Fi
  - RFID
  - Bluetooth Classic & LE 4/5
  - Telecom
  - And even exotic communications
- In addition: report generator, common network tools, web tools, etc.
- But: takes at least 1-5 days to setup properly (depending on number of tools)

Setup

Compile your tools

- Need to deal with:
  - Compilation issues
  - Dependencies
  - Collisions/conflicts
- A good setup can take a day to a week depending on needed tools
- Time is running
- Not good when rushing on an assessment...



```
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/dev.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/wq.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/lib/gid.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/diag/fs_tracepoint.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/diag/fw_tracer.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_main.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_common.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_fs.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_ethtool.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_tx.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_rx.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_dim.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_txrx.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en/xdp.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_stats.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_selftest.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en/port.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_arfs.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_fs_ethtool.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_dcbnl.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en/port_buffer.o
  CC [M]  drivers/net/ethernet/mellanox/mlx5/core/en_rep.o
gcc: fatal error: Killed signal terminated program cc1
compilation terminated.
make[5]: *** [scripts/Makefile.build:304: drivers/net/ethernet/mellanox/mlx5/core/en_rep.o] Error 1
make[5]: *** Deleting file 'drivers/net/ethernet/mellanox/mlx5/core/en_rep.o'
make[4]: *** [scripts/Makefile.build:544: drivers/net/ethernet/mellanox/mlx5/core] Error 2
make[3]: *** [scripts/Makefile.build:544: drivers/net/ethernet/mellanox] Error 2
t/ethernet] Error 2
t] Error 2
```

can@can-VirtualBox: ~/reversing

```
can@can-VirtualBox:~$ pwd
/home/can
can@can-VirtualBox:~$ mkdir reversing
can@can-VirtualBox:~$ cd reversing/
can@can-VirtualBox:~/reversing$ nano hello_world.c
can@can-VirtualBox:~/reversing$ gcc -m32 hello_world.c hello_wo
In file included from hello_world.c:1:
/usr/include/stdio.h:27:10: fatal error: bits/libc-header-start
or directory
   27 | #include <bits/libc-header-start.h>
      |          ^~~~~~~~~~~~~~~~~~~~~~~~~~
compilation terminated.
can@can-VirtualBox:~/reversing$ gcc hello_world.c
can@can-VirtualBox:~/reversing$ sudo apt-get install gcc-multil
[sudo] password for can:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-drive
  intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 l
  libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchroma
  libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2 lib
  libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm
```

Screenshot from 2016-12-16 14-38-45.png

pet@pet-OptiPlex-9020: ~/oe-core/build

```
 which can result in this and we don't know which one this is. It may be you have switched providers of
 (e.g. from linux-yocto to linux-yocto-dev), in that case you need to execute the clean task for both re
s error. It may be you changed DISTRO_FEATURES from systemd to udev or vice versa. Cleaning those recipes
rror however switching DISTRO_FEATURES on an existing build directory is not supported, you should really
reusing sstate should be safe). It could be the overlapping files detected are harmless in which case add
IST may be the correct solution. It could also be your build is including two different conflicting versi
and bluez 5 and the correct solution for that would be to resolve the conflict. If in doubt, please ask o
the error and filelist above.
ERROR: If the above message is too much, the simpler version is you're advised to wipe out tmp and rebuil
That will likely fix things in most (but not all) cases.
ERROR: Function failed: sstate_task_postfunc
ERROR: Logfile of failure stored in: /home/pet/oe-core/build/tmp-glibc/work/colibri_imx6-angstrom-linux-g
.52-r0/temp/log.do_packagedata.17254
ERROR: Task 58 (/home/pet/oe-core/build/../layers/meta-toradex-nxp/recipes-kernel/linux/linux-toradex-rt_
failed with exit code '1'
NOTE: Tasks Summary: Attempted 6920 tasks of which 6914 didn't need to be rerun and 2 failed.
NOTE: Writing buildhistory
No currently running tasks (6857 of 7207)

Summary: 2 tasks failed:
  /home/pet/oe-core/build/../layers/meta-toradex-nxp/recipes-kernel/linux/linux-toradex-rt_3.14.52.bb, do
  /home/pet/oe-core/build/../layers/meta-toradex-nxp/recipes-kernel/linux/linux-toradex-rt_3.14.52.bb, do
Summary: There were 6 ERROR messages shown, returning a non-zero exit code.
pet@pet-OptiPlex-9020:~/oe-core/build$
```

Setup

Alternative distributions

- Existing alternative distributions:
  - Kali: packages for Wi-Fi, Bluetooth, RFID, SDR and many other pentest tools
  - Pentoo: Like Kali with extra GNU Radio tools and modules, SDR tools as well (https://github.com/pentoo/pentoo-overlay/tree/master/net-wireless)
  - Dragon OS: Really focusing on radio tools and much more complete that other distributions
  - Others

Alternative distributions (2)

- **Pros**:
  - Packages as much tools as possible --> reducing installation time
    - Tools not yet package can be installed after
  - Less troubleshooting during our setup --> tools are ready to be used
  - Perfect for less experienced people
- **Cons**:
  - Need to reinstall the computer with the specialized distribution
  - Dependencies issues with new installed tools --> breaking the setup

Setup

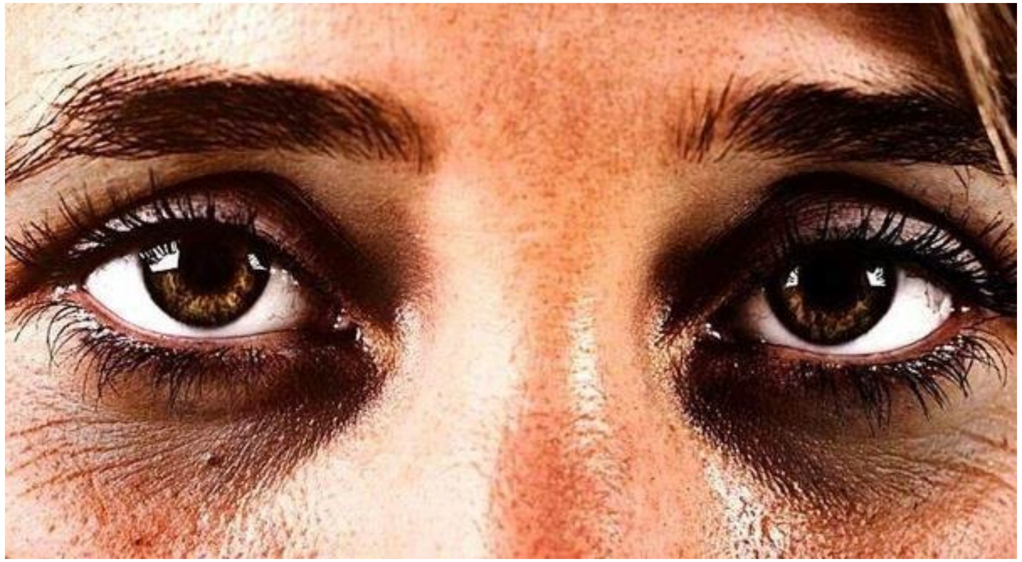
Alternative distributions

- Existing alternative
  - Kali: package ID, SD many other pente
  - Pentoo: Like Kali with ex modules, SDR tools as well ([https://github.com/pe overlay/tree/maste
  - Dragon OS: Re ools a more complete t tions
  - Others

PENTOO

Breaking the setup

- **Need to reinstall everything! Sometimes until 5am during a pentest...**



Breaking the setup (2)

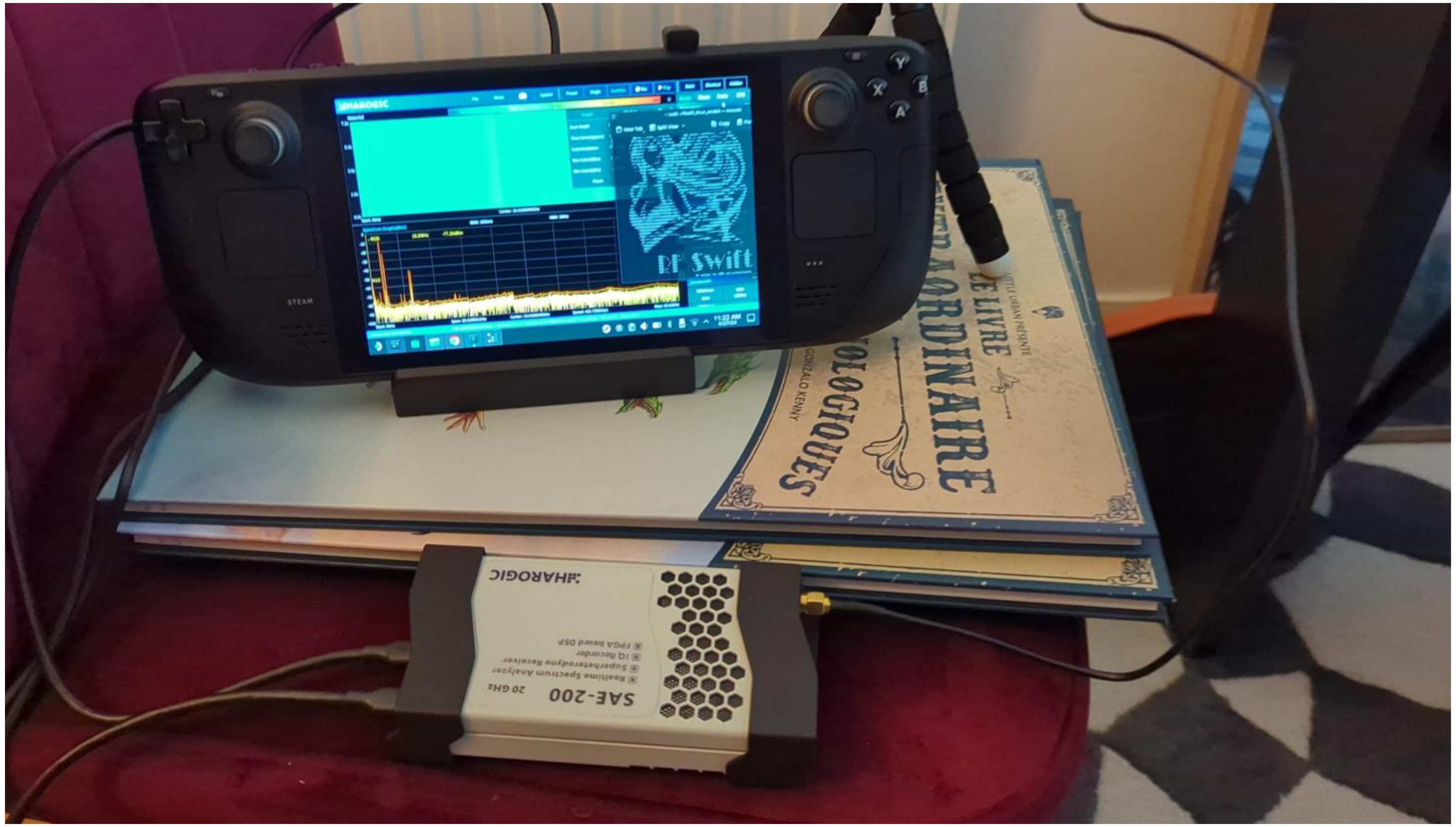
- **And doing that all the time, your turn like:**

Meet RF Swift!

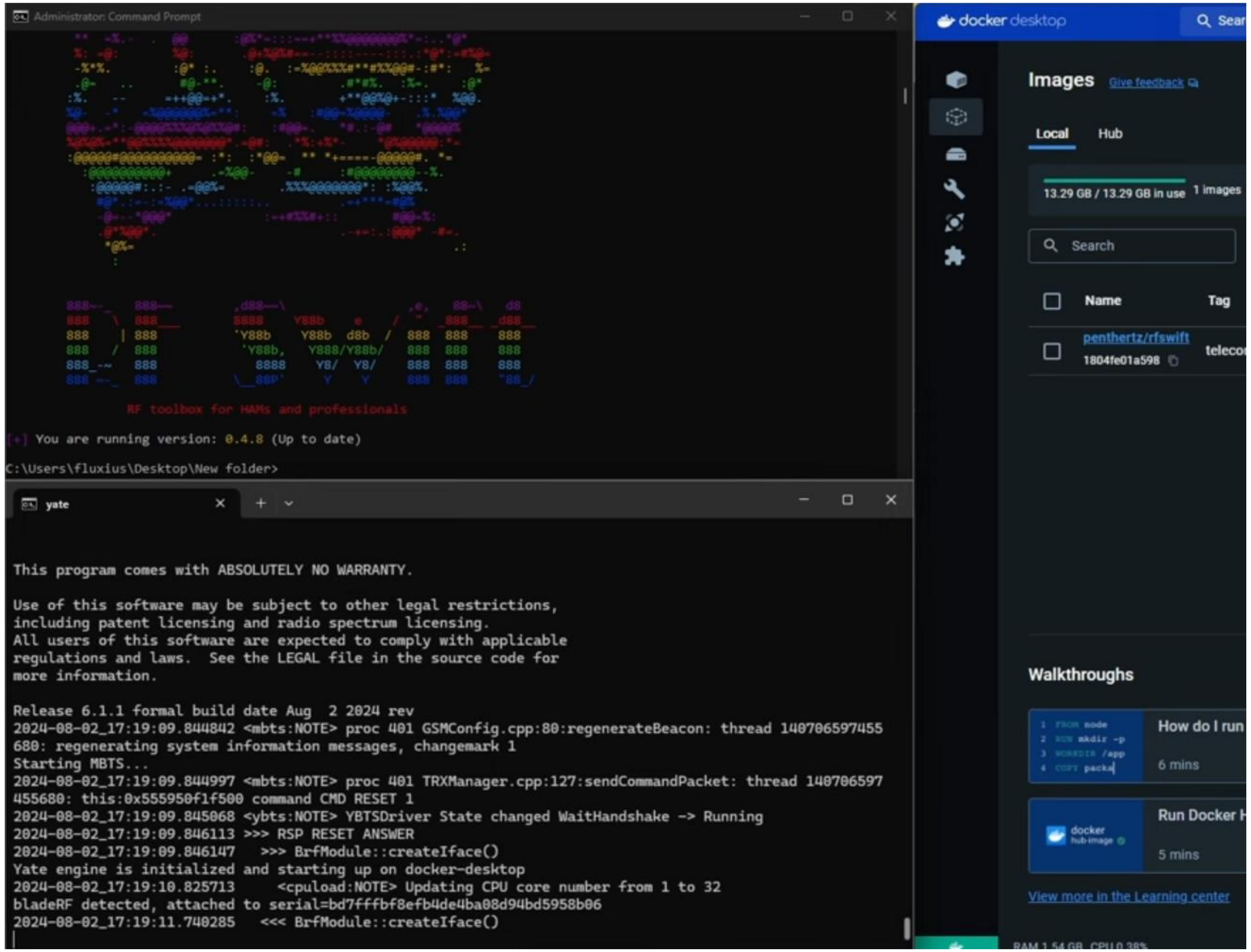
What is it?

- Tool made in Go --> Instrumenting Docker + host
    - Inspirated from Exegol project ;)
- Docker files "recipes"
- Registry with built images
- Scripts for automating installations of various tools
- Supported and tested architectures: x86_64, ARM64, and RISC-V 64
- Supported and tested OSes: Linux and Windows

Assessments on a Steam Deck



Windows GPRS stations (in few minutes)



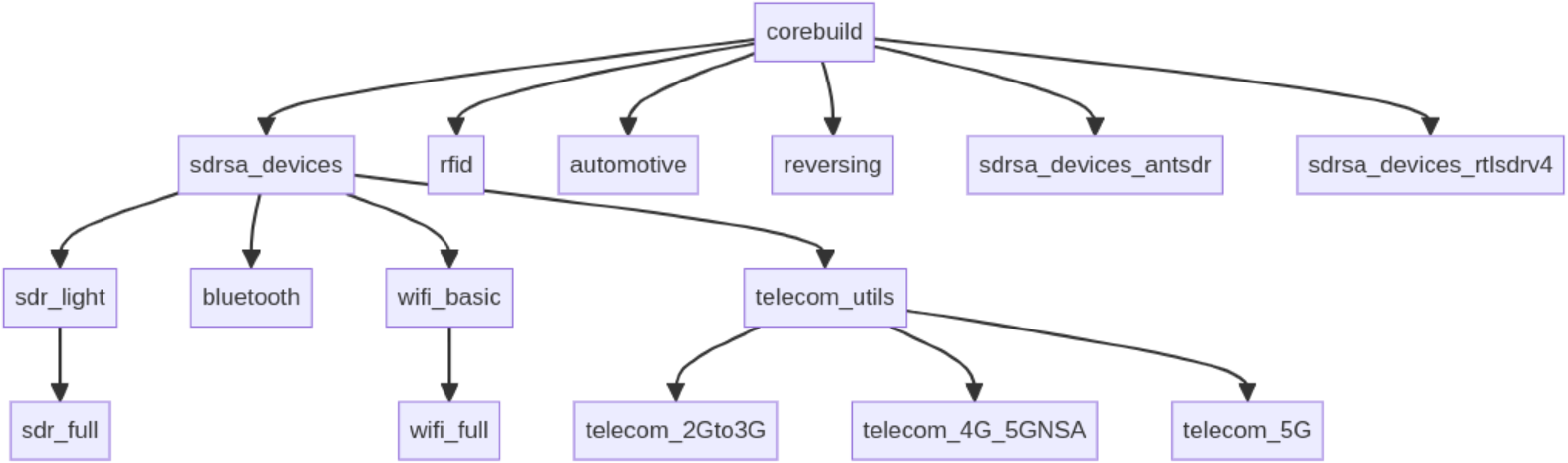
```
RF toolbox for HAMs and professionals

[+] You are running version: 0.4.8 (Up to date)

C:\Users\fluxius\Desktop\New folder>
```

```
This program comes with ABSOLUTELY NO WARRANTY.

Use of this software may be subject to other legal restrictions,
including patent licensing and radio spectrum licensing.
All users of this software are expected to comply with applicable
regulations and laws.  See the LEGAL file in the source code for
more information.

Release 6.1.1 formal build date Aug  2 2024 rev
2024-08-02_17:19:09.844842 <mbts:NOTE> proc 401 GSMConfig.cpp:80:regenerateBeacon: thread 140706597455
680: regenerating system information messages, changemark 1
Starting MBTS...
2024-08-02_17:19:09.844997 <mbts:NOTE> proc 401 TRXManager.cpp:127:sendCommandPacket: thread 140706597
455680: this:0x555950f1f500 command CMD RESET 1
2024-08-02_17:19:09.845068 <ybts:NOTE> YBTSDriver State changed WaitHandshake -> Running
2024-08-02_17:19:09.846113 >>> RSP RESET ANSWER
2024-08-02_17:19:09.846147   >>> BrfModule::createIface()
Yate engine is initialized and starting up on docker-desktop
2024-08-02_17:19:10.825713     <cpuload:NOTE> Updating CPU core number from 1 to 32
bladeRF detected, attached to serial=bd7fffbf8efb4de4ba08d94bd5958b06
2024-08-02_17:19:11.740285   <<< BrfModule::createIface()
```

RF Swift

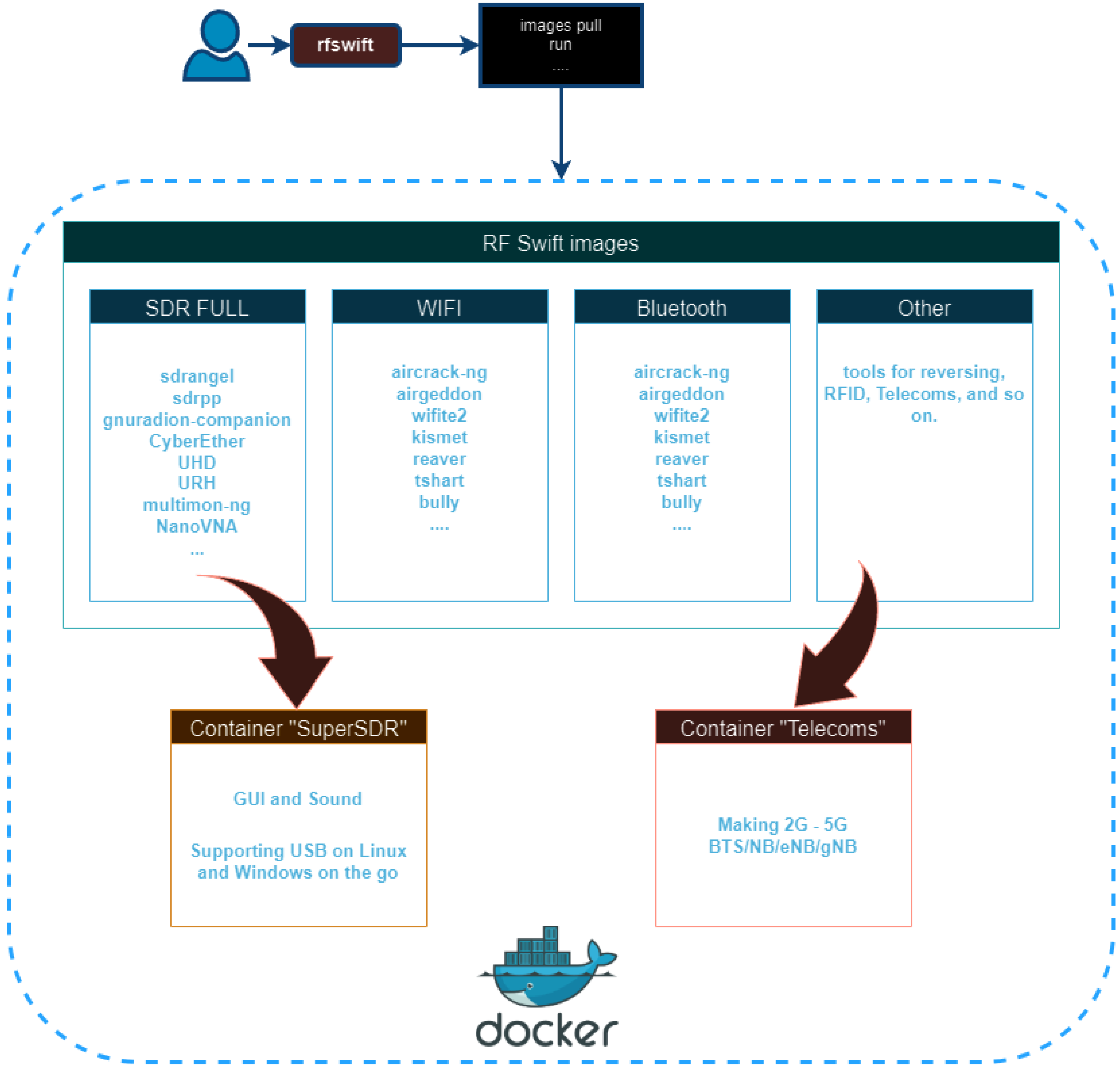
Images' hierarchy

- Following Docker images layers concept: reuse of layers -> speed and space saving



Architecture

- Each created container has tools included in dedicated images
- Each container represent a "mission"
  - ○ Perfect for assessments separation: client1 and client2 are not in the same space
  - ○ Messing with one container -> throw it and run a new container!



Demo time!

Conclusion

Going further

To conclude

- You can travel and assess devices safely with RF Swift
- Keep you setup light based on your own "recipes"
- RF Swift is 3 months old --> will grow with more tools
- Need also contributors:
  - Documentation: https://rfswift.io/
  - Go binary for instrumentation and user experience
- Our discord: https://discord.com/invite/NS3HayKrpA

penthertz

Thank You

Please contact us:

✉ contact@penthertz.com

☎ +33 1 73 13 82 77

🌐 penthertz.com

Watch us on YouTube