



RF Swift: a swift toolbox for all wireless assessments

By Sébastien Dudek



About myself

Founder of Penthertz

- Sébastien Dudek ([@FlUxluS](https://twitter.com/FlUxluS))
- 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!

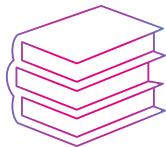


Main activities



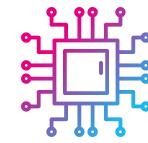
Security assessments

- 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...



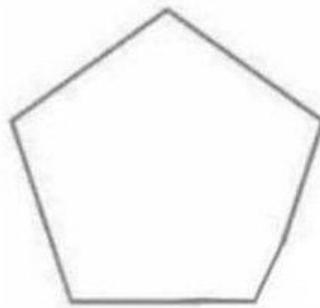
Hardware security

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

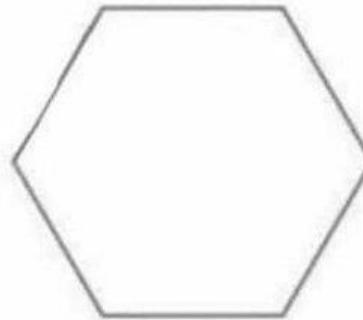
RF Pentester 010: Having a good setup



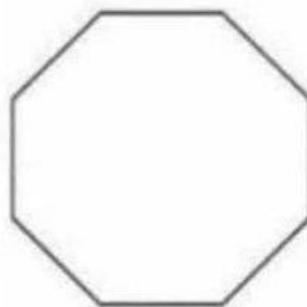
A real lab -> follow the geometry...



Pentagon



Hexagon



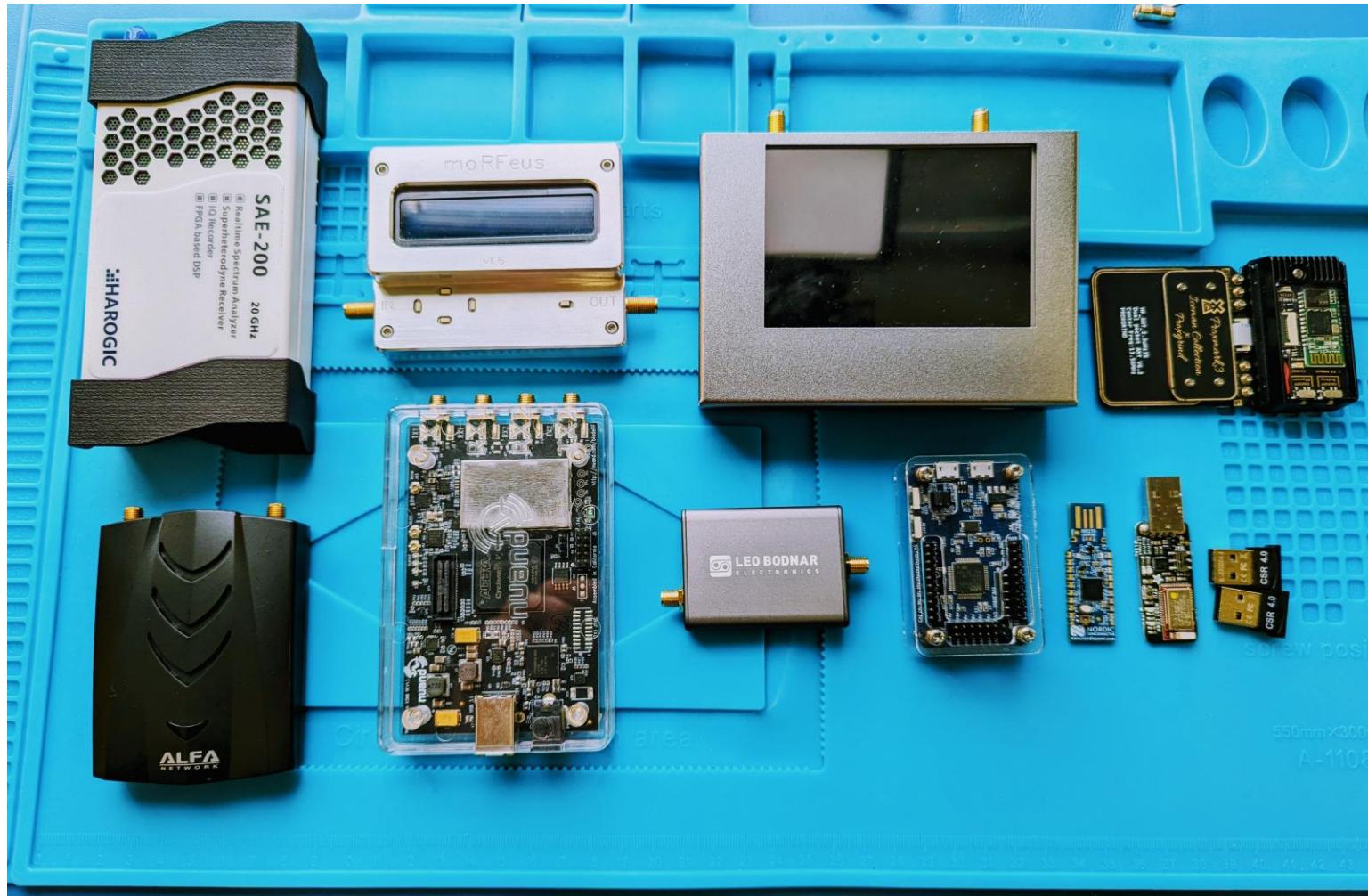
Octagon



Moneygone

Setup

A minimum setup for RF assessments: ~3-4k€

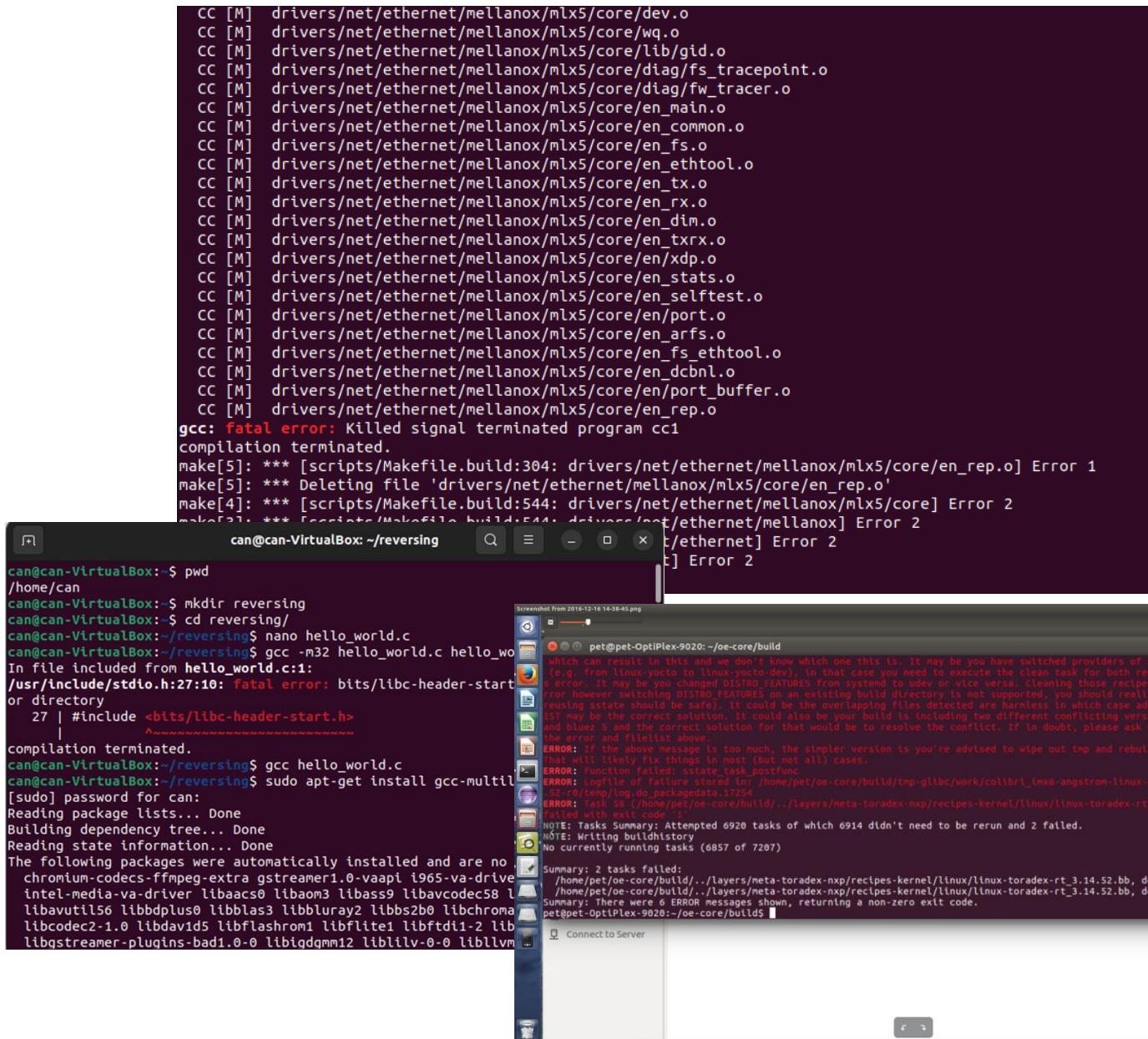


Software setup

- 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)**

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[2]: *** [scripts/Makefile.build:511: drivers/net/ethernet/mellanox] Error 2
make: *** [ethernet] 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_world
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-multilib
[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-driver
intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 lib
libavutil56 libbdplus0 libblas3 libbluray2 libbs2b0 libchroma
libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libfdt1-2 lib
libgstreamer-plugins-bad1.0-0 libigdmm12 liblilv-0-0 liblilv

```

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

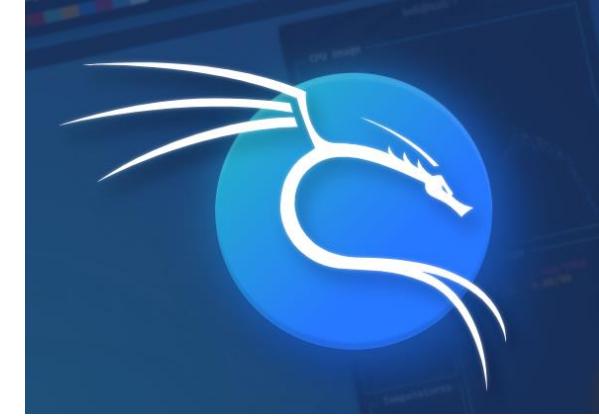
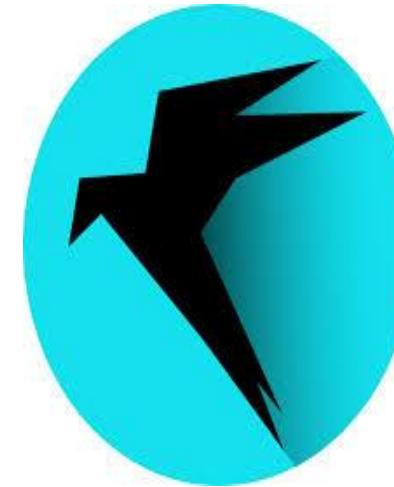
```

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 a
(e.g. from linux-yocto to linux-yocto-dev). In that case you need to execute the clean task for both re
error. It may be you changed DISTRO_FEATURES from sysroot to udev or vice versa. Cleaning those recip
error however switching DISTRO_FEATURES on an existing build directory is not supported, you should real
reusing sstate should be safe). It could be the overlapping files detected are harmless in which case ad
ist may be the correct solution. It could also be your build is including two different conflicting vers
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 rebu
that will likely fix things in most (but not all) cases.
ERROR: Function with state is not positive.
ERROR: Logfile of failure is located in: /home/pet/oe-core/build/tmp-glibc/work/collbr_imx6-angstrom-linux-g
ERROR: Task 58 (/home/pet/oe-core/build/../.layers/meta-toradex-nxp/recipes-kernel/linux/linux-toradex-rt
ERROR: Task 58 (/home/pet/oe-core/build/../.layers/meta-toradex-nxp/recipes-kernel/linux/linux-toradex-rt
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/builds

```

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 than other distributions
 - Others
- **But nothing specific to RF & Hardware security with hardware accesses (USB, mPCIe, GPU, sound, etc.)**



PENTOO



Alternative distributions (2)

- **Pros:**

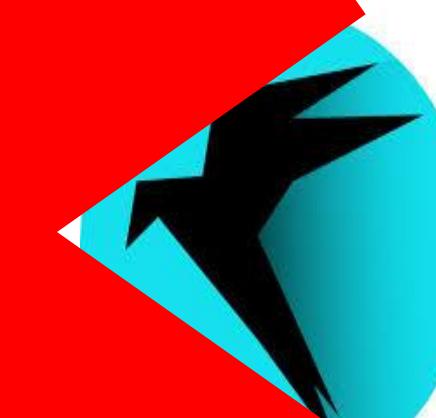
- Packages as much tools as possible --> reducing installation time
 - Tools not yet package can be installed after
- Less troubleshooting during our setup --> tools are ready to be used
- Perfect for less experienced people

- **Cons:**

- Need to reinstall the computer with the specialized distribution
 - And also to complete it with missing tools
- Dependencies issues with new installed tools --> breaking the setup
- No scalability

Alternative distributions

- Existing alternative
 - Kali: packages for penetration testing, including WiFi, SDR, and many other pentesting tools
 - Pentoo: Like Kali with extensive WiFi and SDR modules, SDR tools as well (<https://github.com/pentoo-project/pentoo-overlay/tree/master>)
 - Dragon OS: Recently released, includes WiFi tools and more complete toolset and applications
 - Others
 - **But nothing specific to RF & Hardware security with hardware accesses (USB, mPCIe, GPU, sound, etc.)**



PENTOO



Breaking the setup

- **Need to reinstall everything! Sometimes until 5am right before a pentest...**
- **You morning starts like that:**



Breaking the setup (2)

- **How the client sees you during the assessment:**



Each mission is different

- A mission needs a dedicated container:
 - More reproducibility + scalability
 - Avoid mixing "client 1" traces with "client 2"
 - You can mess inside a container -> destruct it there after



Let me introduce you RF Swift!

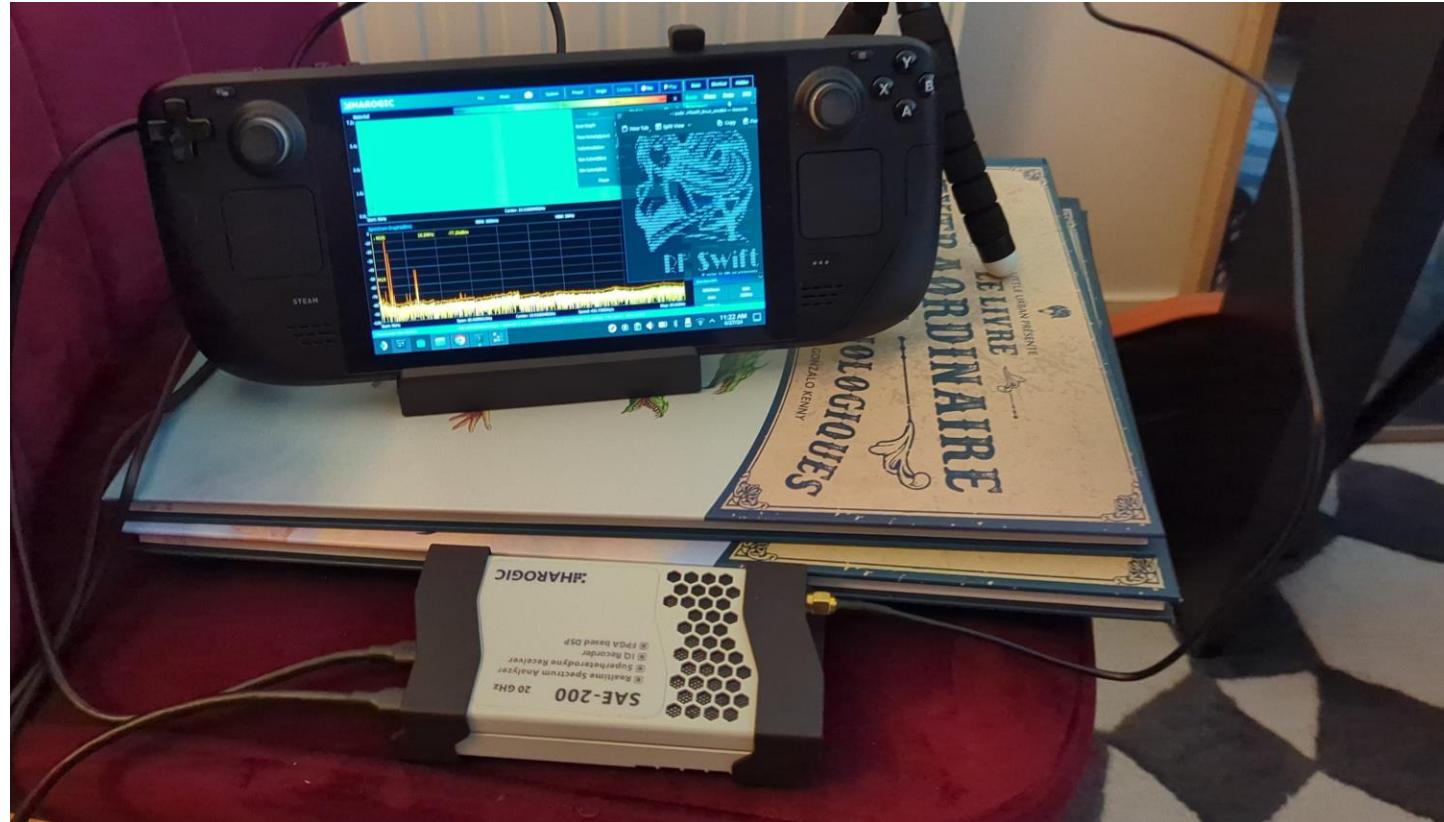


What is it?

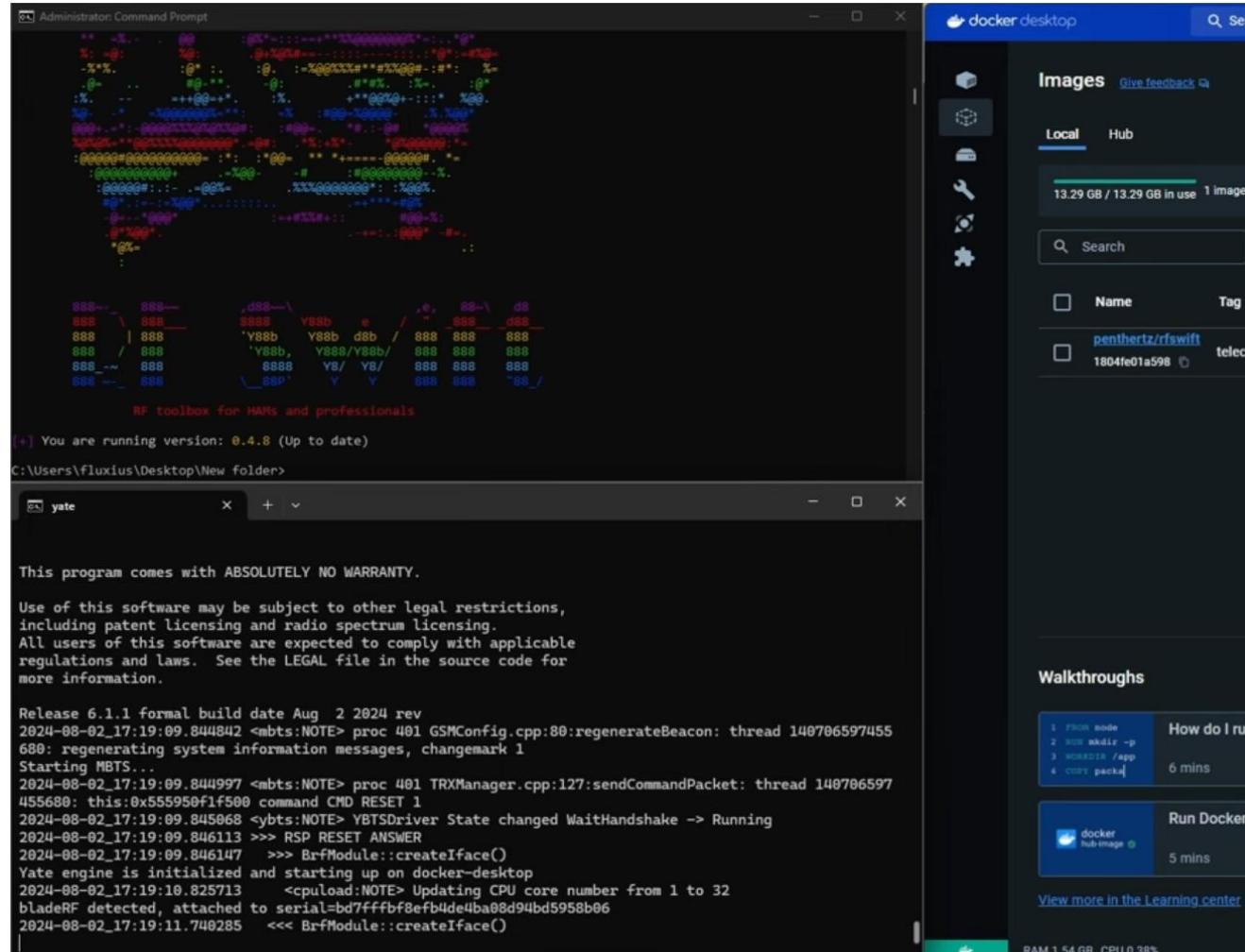
- Tool made in Go --> Instrumenting Docker + host
 - Inspired from Exegol project ;)
- Docker files "recipes"
- Registry with built images
- Scripts for automating installations of various tools
- Supported and tested architectures: x86_64, ARM64, and RISC-V 64
- Supported and tested OSes: Linux and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



Assessments on a Steam Deck

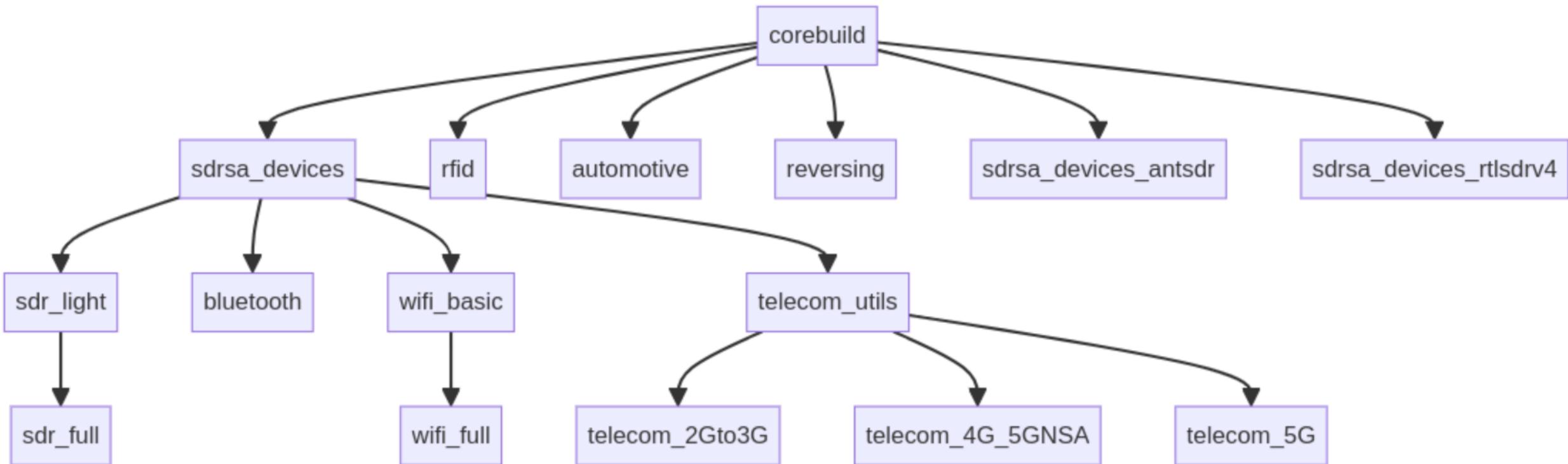


Windows GPRS stations (in few minutes)



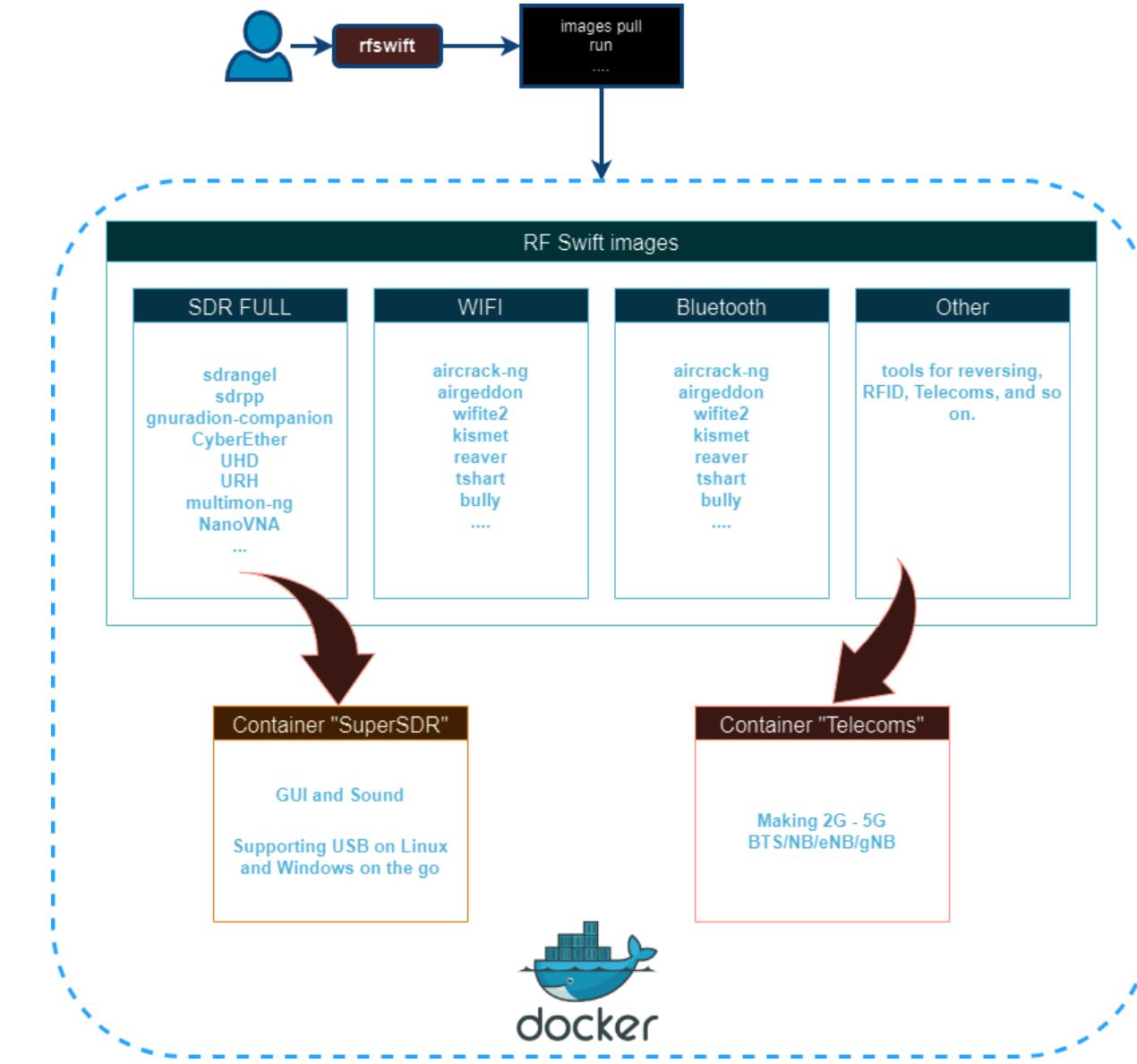
Images' hierarchy

- 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!



Key commands

- Impatient to make your images? Pull one from our registry:

```
$ sudo ./rfswift images pull -i <reference> -t <tag name to apply>
```

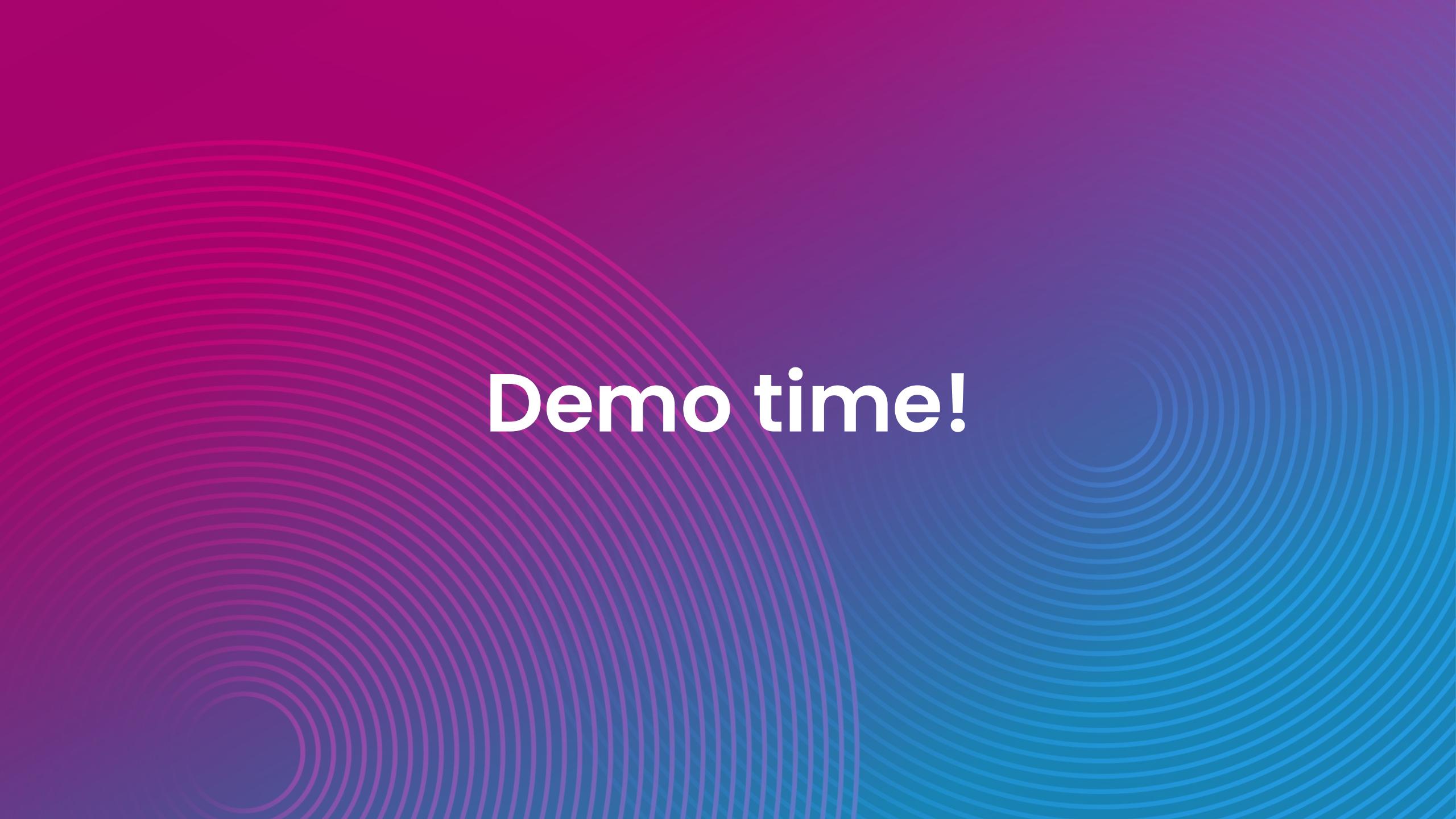
- Run a container:

```
$ sudo ./rfswift run -i <image name> -n <container name> [-e <command>]  
[-b <extra volumes>]
```

- Shoot! I kill my terminal!! shhNOO problem:

```
$ sudo ./rfswift exec [-c <container name>] -e <command>
```

- Let's discover what's inside!

The background features a series of concentric, slightly curved lines that create a sense of depth and motion. The lines are primarily red on the left side and transition to blue on the right side, with a central area of purple. The overall effect is reminiscent of a colorful, abstract sunburst or a high-energy particle field.

Demo time!

Conclusion

To conclude

- You can travel and assess devices safely with RF Swift
 - e.g. -> my computer that was just erased and used for traveling
- Keep your setup light based on your own "recipes"
- RF Swift is 1y old -> still a lot to do!
- 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

