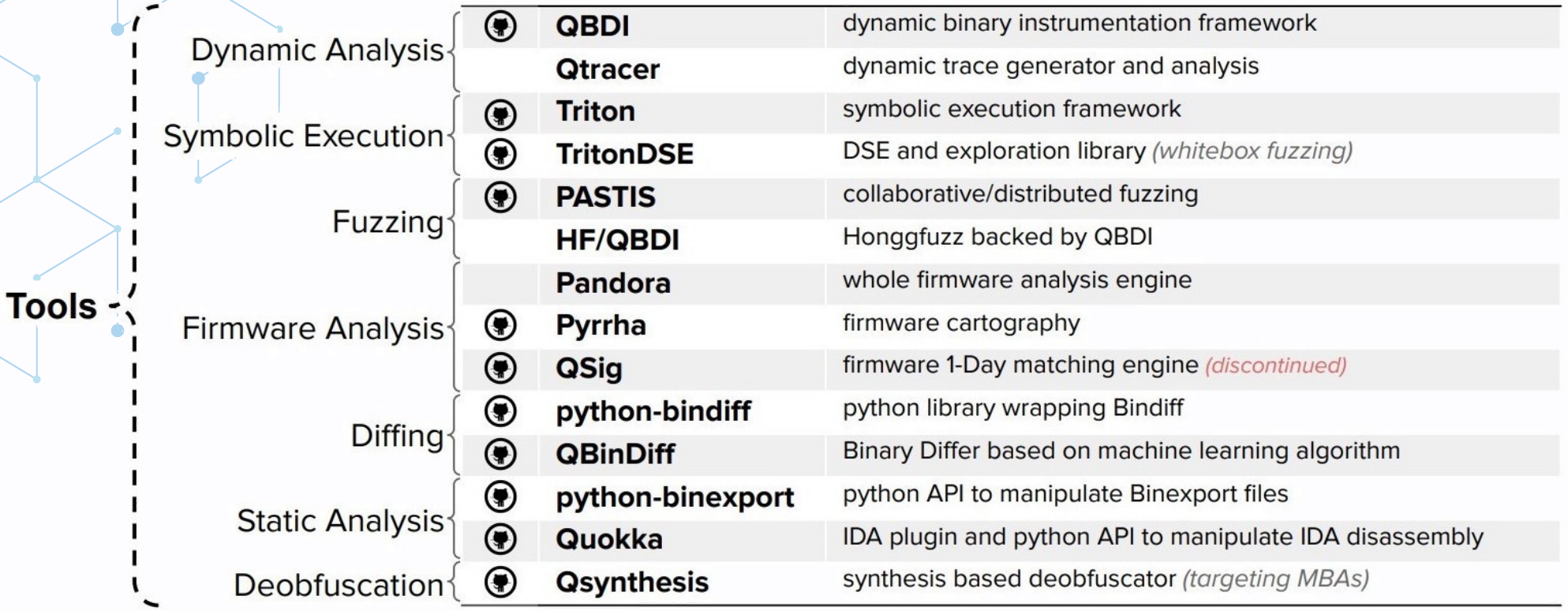
Quarkslab

Pyrrha: navigate easily into your system binaries

Eloïse Brocas | CTI-summit 2023

Whoami

- Security R&D Engineer @ Quarkslab
  - Vulnerability research and reverse-engineering



✓	**QBDI**	dynamic binary instrumentation framework
	Qtracer	dynamic trace generator and analysis
✓	**Triton**	symbolic execution framework
✓	**TritonDSE**	DSE and exploration library *(whitebox fuzzing)*
✓	**PASTIS**	collaborative/distributed fuzzing
	HF/QBDI	Honggfuzz backed by QBDI
	Pandora	whole firmware analysis engine
✓	**Pyrrha**	firmware cartography
✓	**QSig**	firmware 1-Day matching engine *(discontinued)*
✓	**python-bindiff**	python library wrapping Bindiff
✓	**QBinDiff**	Binary Differ based on machine learning algorithm
✓	**python-binexport**	python API to manipulate Binexport files
✓	**Quokka**	IDA plugin and python API to manipulate IDA disassembly
✓	**Qsynthesis**	synthesis based deobfuscator *(targeting MBAs)*

Tools developed by the Quarkslab Automated Analysis Team.

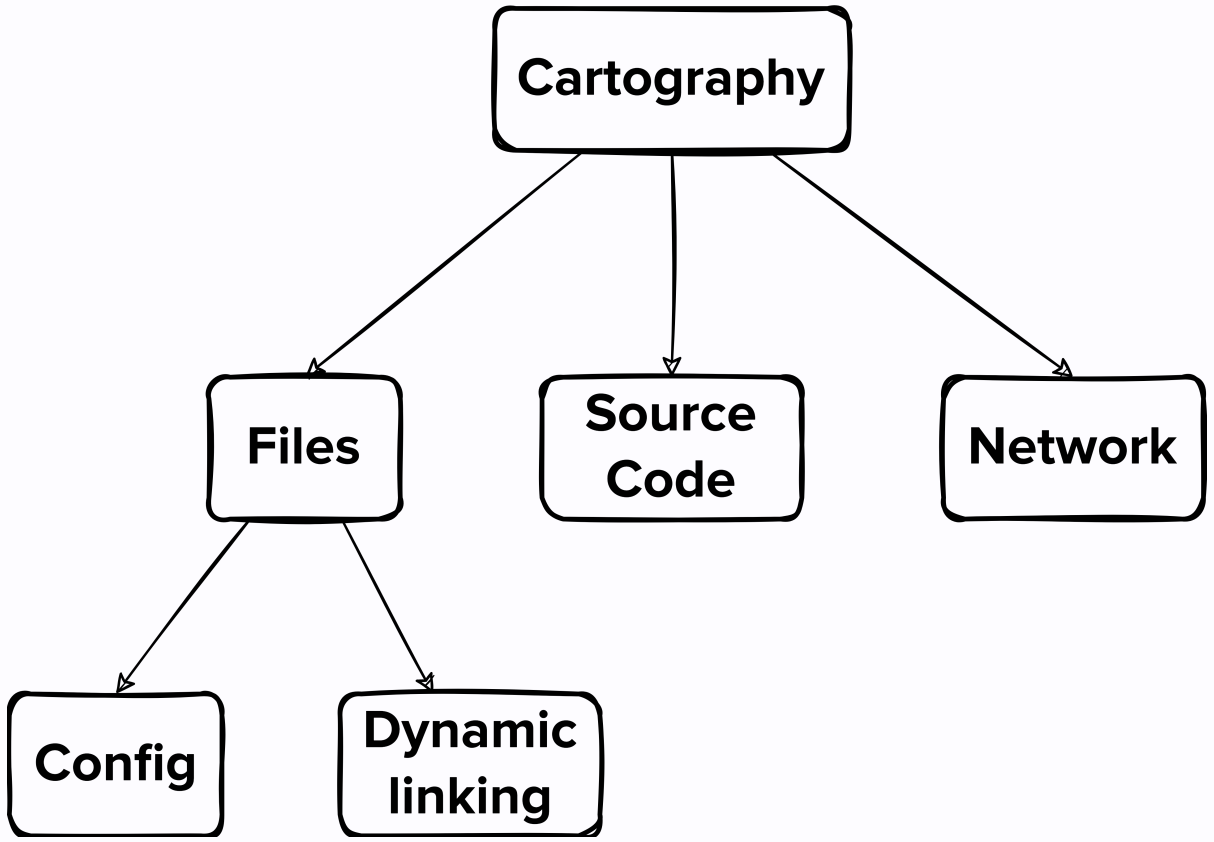
Problematics

Firmwares

- embedded into IoT objects
  - routers
  - smartphones
  - automotive
- complete OS (Android, Linux, OpenWRT, ...)
- *structured firmwares*
  - filesystem
  - thousands of files

Cartography

Goal: understand interactions between components



Visualization is the key

Pyrrha, J.-P. A. Tassaert. Source: Musée du Louvre.

Sisyphus, Titian. Source: Wikimedia.

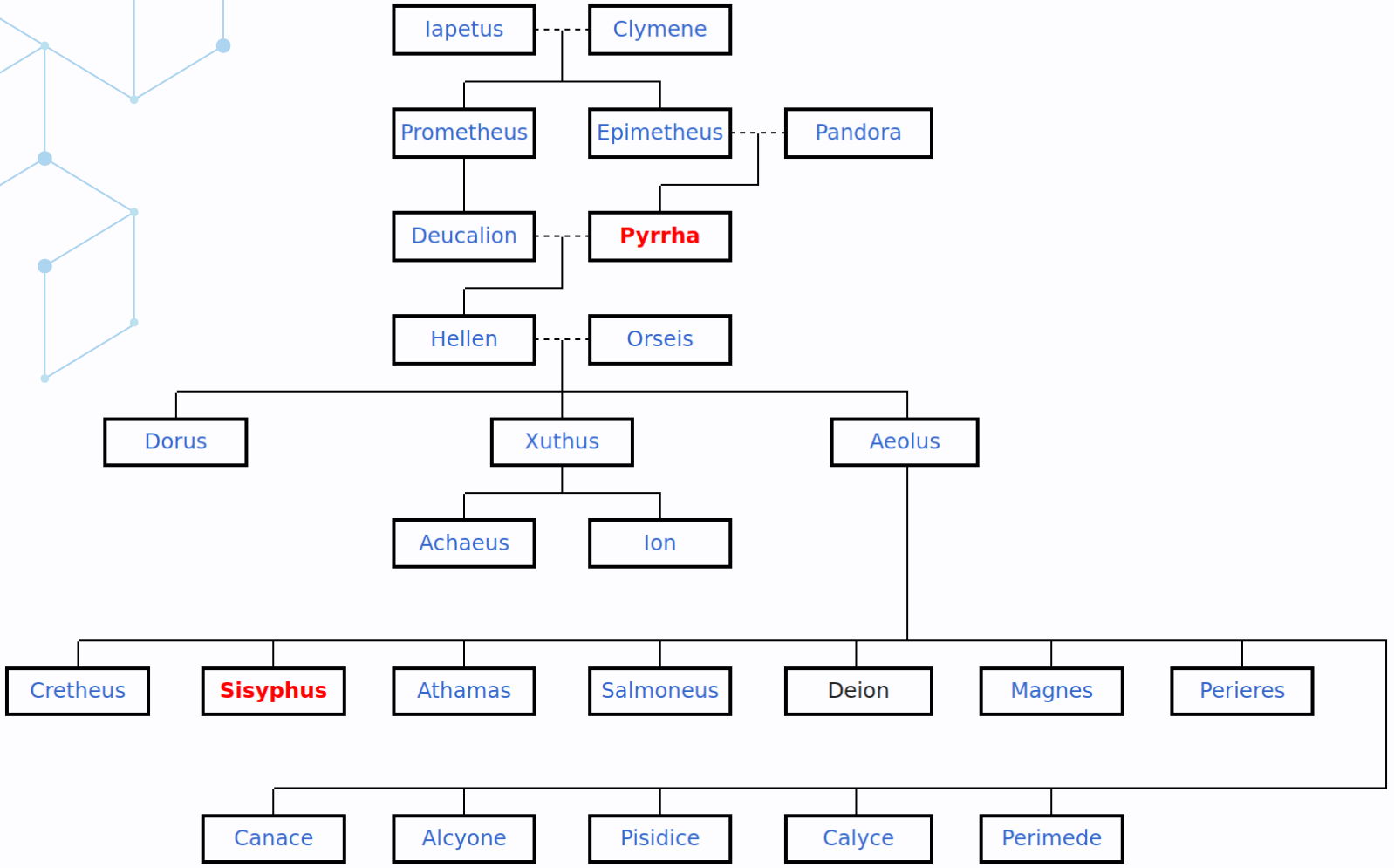
Visualization is the key

«[1.7.2] And Prometheus had a son Deucalion. He reigning in the regions about Phthia, married Pyrrha, the daughter of Epimetheus and Pandora, the first woman fashioned by the gods. And when Zeus would destroy the men of the Bronze Age, Deucalion by the advice of Prometheus constructed a chest, and having stored it with provisions he embarked in it with Pyrrha. But Zeus by pouring heavy rain from heaven flooded the greater part of Greece, so that all men were destroyed, except a few who fled to the high mountains in the neighborhood. It was then that the mountains in Thessaly parted, and that all the world outside the Isthmus and Peloponnese was overwhelmed. But Deucalion, floating in the chest over the sea for nine days and as many nights, drifted to Parnassus, and there, when the rain ceased, he landed and sacrificed to Zeus, the god of Escape. And Zeus sent Hermes to him and allowed him to choose what he would, and he chose to get men. And at the bidding of Zeus he took up stones and threw them over his head, and the stones which Deucalion threw became men, and the stones which Pyrrha threw became women. Hence people were called metaphorically people (laos) from laas, “a stone.” And Deucalion had children by Pyrrha, first Hellen, whose father some say was Zeus, and second Amphictyon, who reigned over Attica after Cranaus; and third a daughter Protogenia, who became the mother of Aethlius by Zeus

[1.7.3] Hellen had Dorus, Xuthus, and Aeolus by a nymph Orseis. Those who were called Greeks he named Hellenes after himself, and divided the country among his sons. Xuthus received Peloponnese and begat Achaeus and Ion by Creusa, daughter of Erechtheus, and from Achaeus and Ion the Achaeans and Ionians derive their names. Dorus received the country over against Peloponnese and called the settlers Dorians after himself. Aeolus reigned over the regions about Thessaly and named the inhabitants Aeolians. He married Enarete, daughter of Deimachus, and begat seven sons, Cretheus, Sisyphus, Athamas, Salmoneus, Deion, Magnes, Perieres, and five daughters, Canace, Alcyone, Pisidice, Calyce, Perimede.»

Apollodorus, 1.7.[2-3].

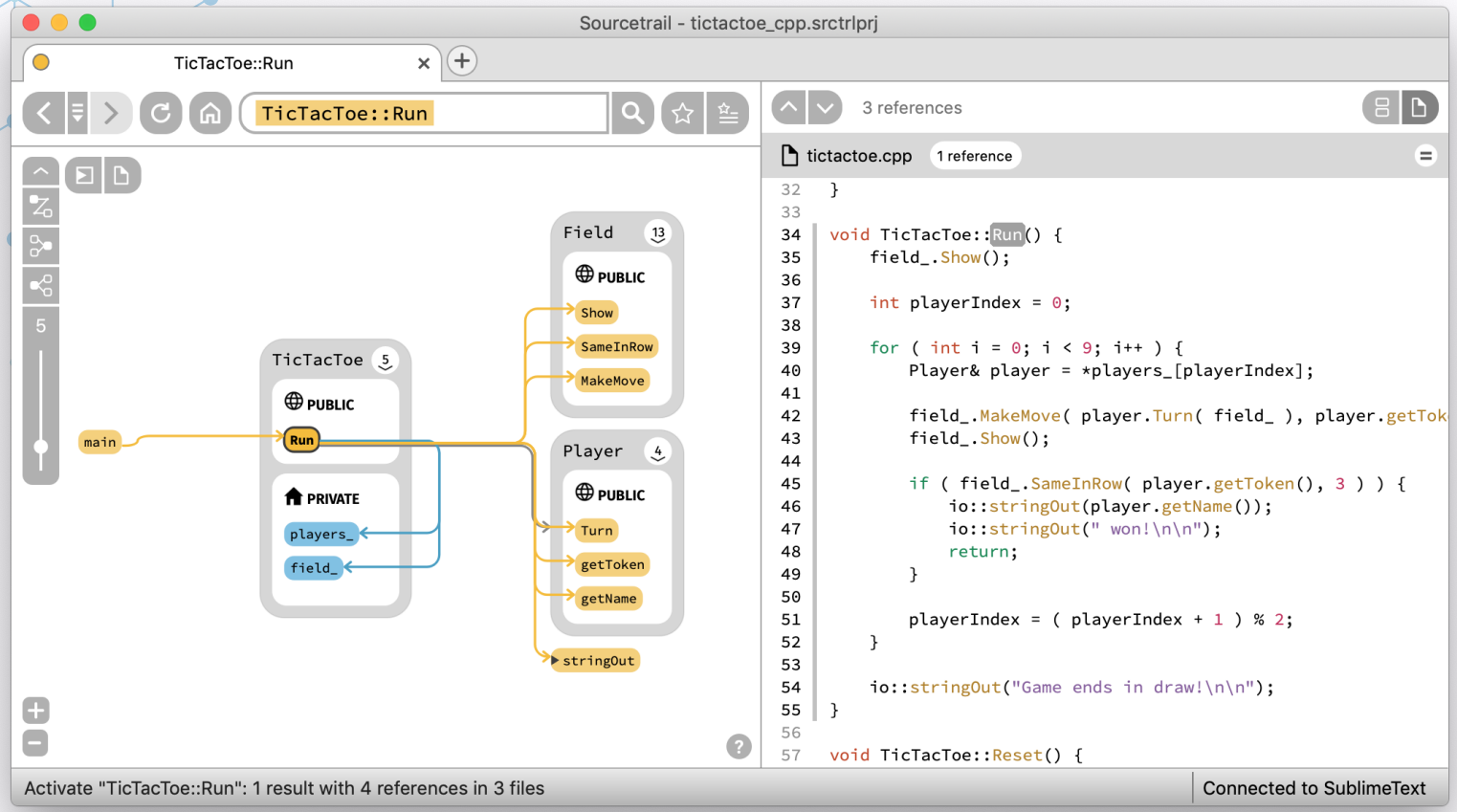
Visualization is the key



Genealogy of Hellenes. Source: Wikipedia.

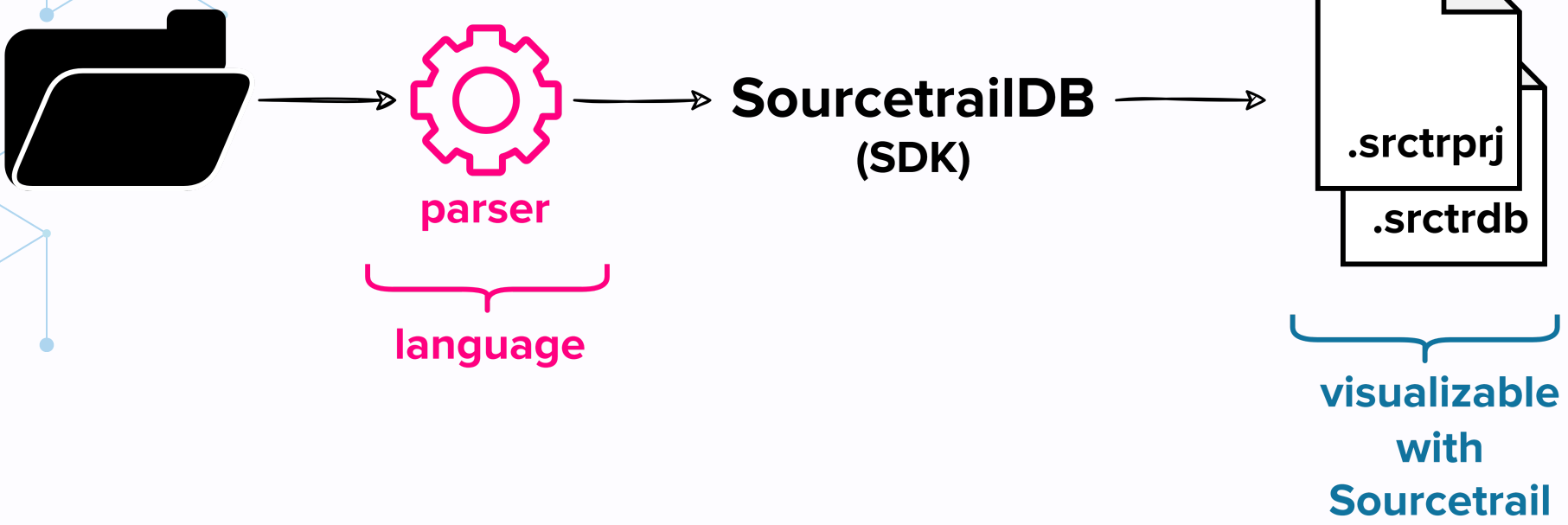
Let's try not to reinvent the wheel!

Sourcetrail



Source: Sourcetrail README.

Extend Sourcetrail



Pyrrha

Filesystem as a language

Binaries	Symlinks
`Class`	`TypeDef`

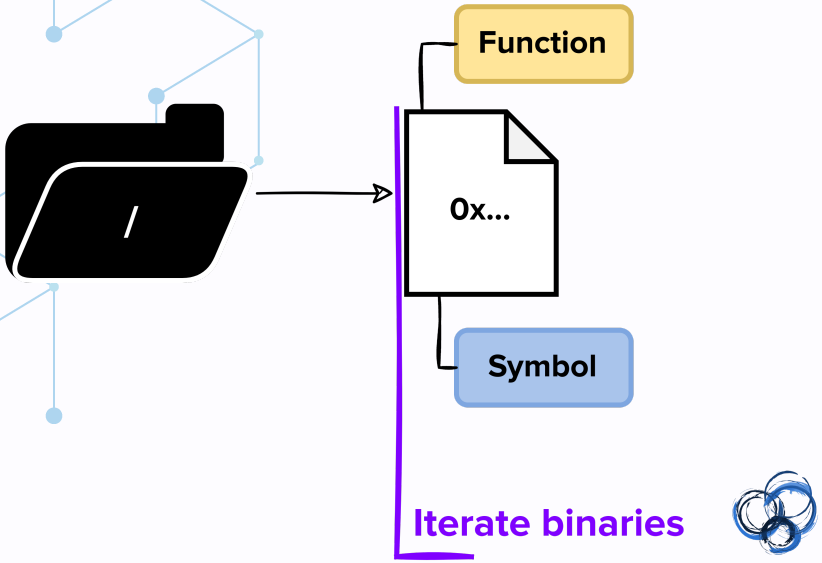
Exported functions	Exported symbols
`function`	`variable`

Pyrrha workflow

Filesystem to map

- already extracted
- entry: root directory

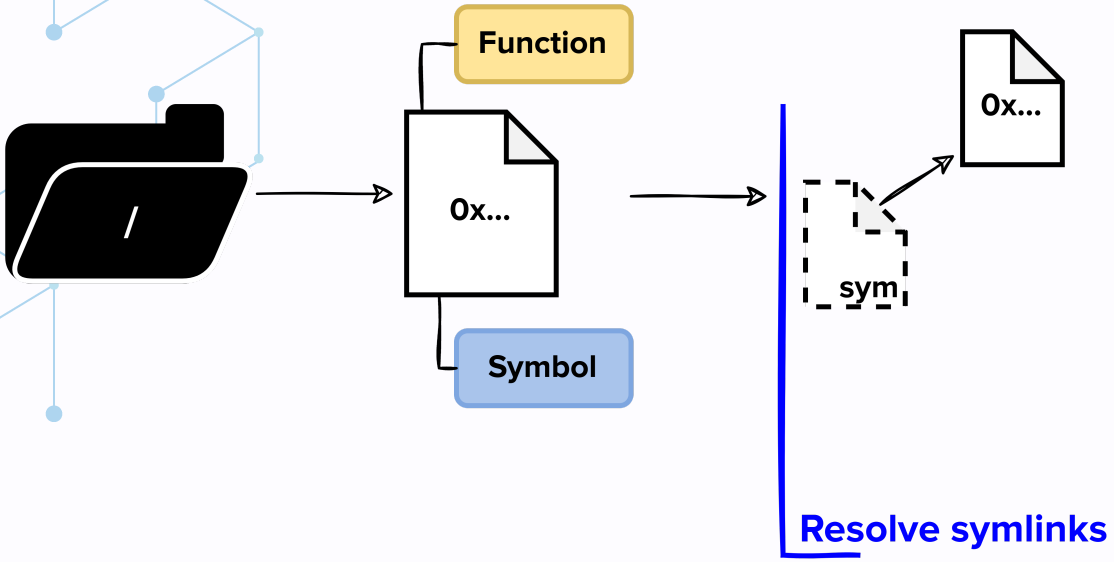
Pyrrha workflow



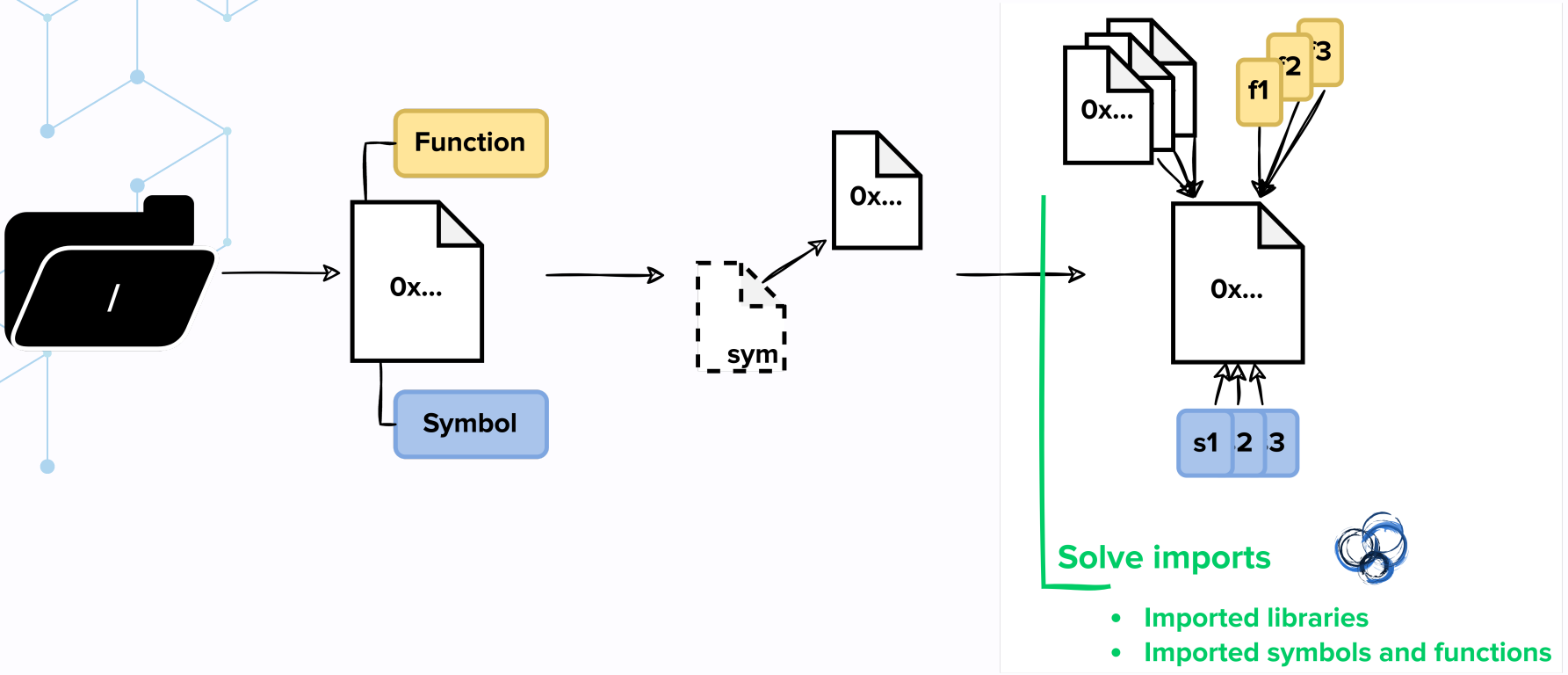
Iterate binaries

- Exported symbols
- Exported functions

Pyrrha workflow



Pyrrha workflow



2 steps

```
Usage: pyrrha fs [OPTIONS] ROOT_DIRECTORY

  Map a filesystem into a sourcetrail-compatible db.

Options:
  --db PATH   Sourcetrail DB file path (.srctrldb).  [default: pyrrha.srctrldb]
  -j, --json  Create a JSON export of the resulting mapping.
  -H, --help  Show this message and exit.
```

```
$ pyrrha --db test.srctrldb root-fs
$ sourcetrail test.srctrlprj
```

Demo Time

Result Export for intercompatibility

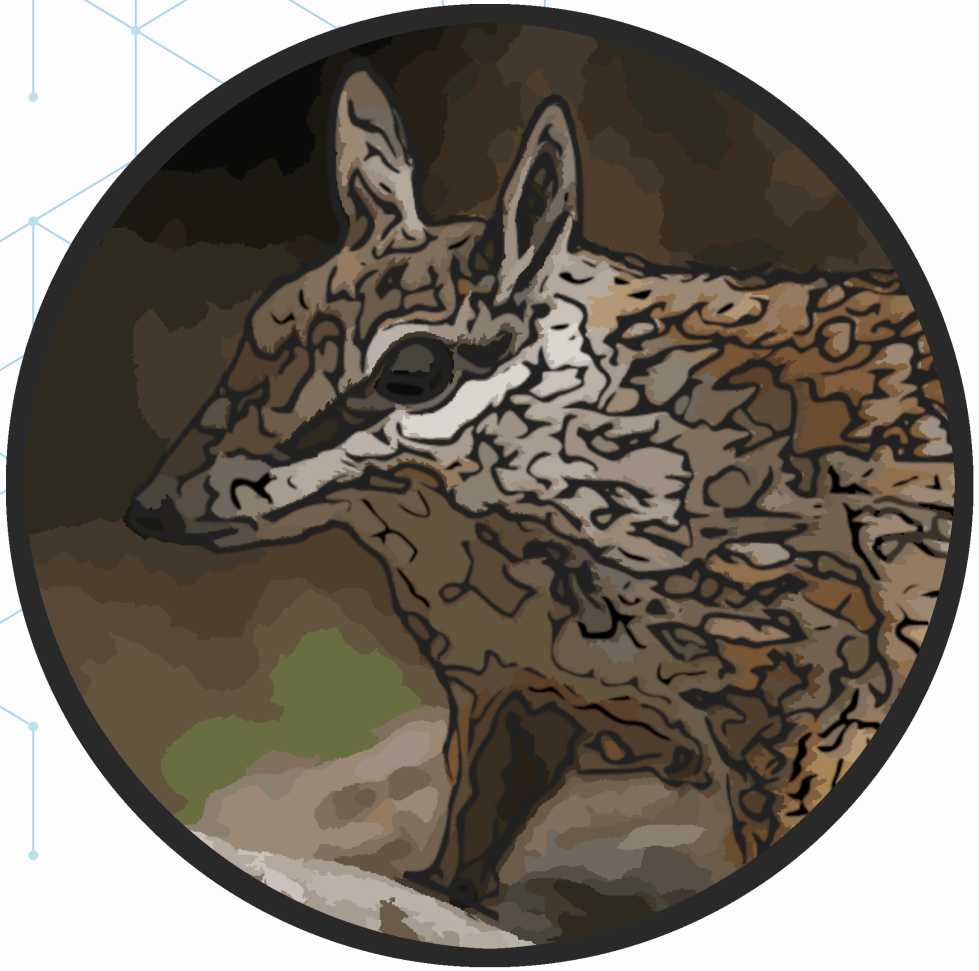
```
Binaries no longer in RAX30-V1.0.9.90_3.json:
  - /lib/libcurl.so.4.6.0
  - /bin/pppoe-relay
  - /bin/websockd

Binaries added in RAX30-V1.0.9.90_3.json:
  - /[KERNEL_VERSION]/kernel/net/netfilter/xt_connlimit.ko
  - /lib/libcurl.so.4.7.0
[...]

Common binaries that have changed:
pudil have changed:
  - symbols removed: {'sprintf'}
  - symbols added: {'sleep', 'snprintf'}
fing_dil have changed:
  - lib removed: {'libcurl.so.4.6.0'}
  - lib added: {'libcurl.so.4.7.0'}
[..]

Total having changed: 108
```

Diffing use case example.

Known limitations

- LIEF limitations
  - no support for MIPS
- Sourcetrail is an archived project
  - OpenSourceTrail
  - Numbat

Numbat



- Quarkslab implementation of Sourcetrail API
- fully Pythonic
- release soon

Conclusion

Pyrrha

- Python Package / Docker
- available on Quarkslab's Github: https://github.com/quarkslab/pyrrha

Future

- add new Sourcetrail capabilities
- add features (diffing, metadata)
- publish it on pypi

Quarkslab

Thank you!

ebrocas@quarkslab.com
@_cryptocorn_