Dissect

The open-source framework for large-scale host investigations

Paul Möller — Senior Security Researcher

Jan Willem Brandenburg — Lead Developer

2023-05-11 COMMERCIAL.RESTRICTED.NLUUG

Paul Möller

Senior Security Researcher

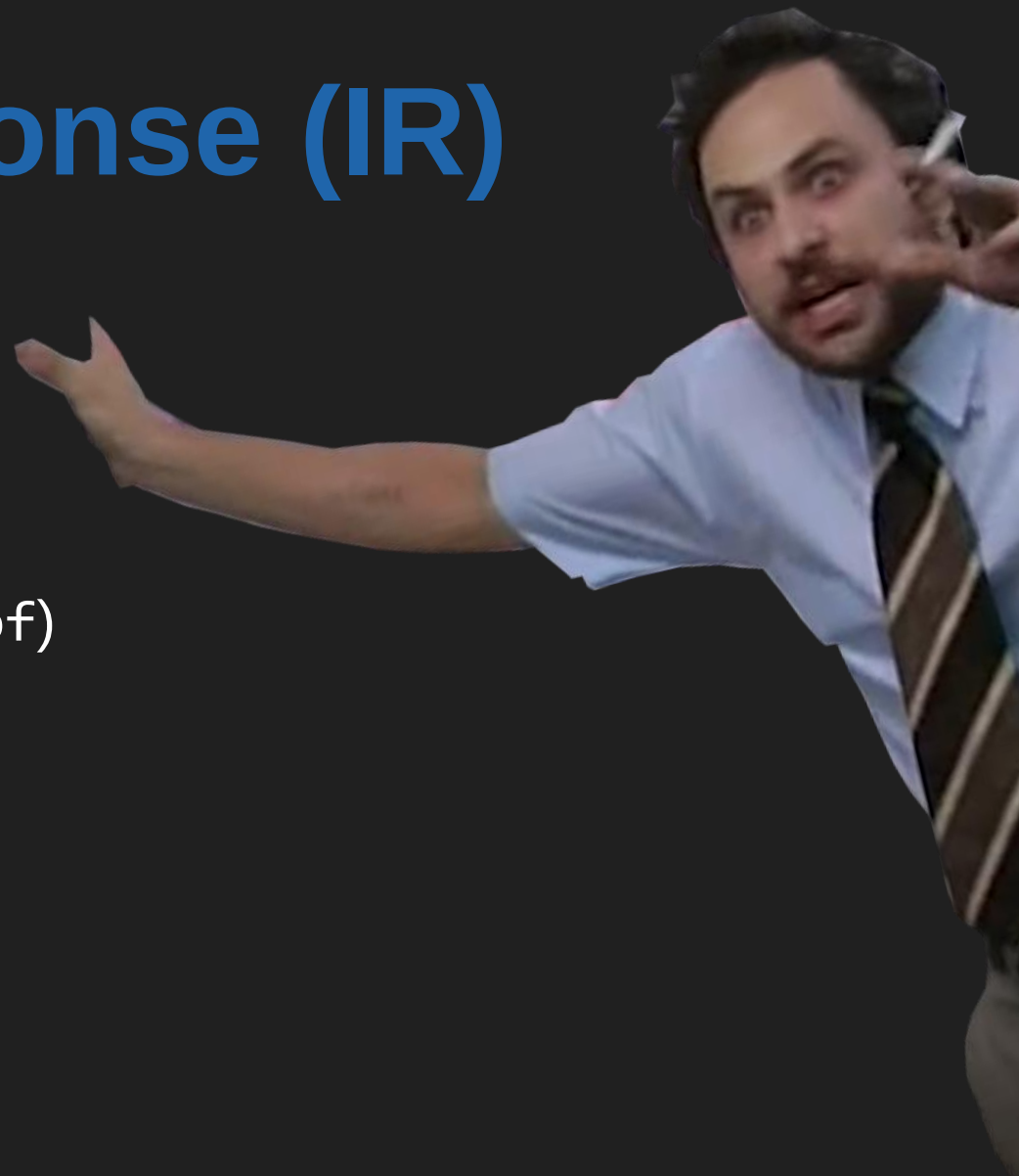
FOX IT
part of nccgroup

Jan Willem Brandenburg

Lead Developer

FOX IT
part of nccgroup

Incident Response (IR)



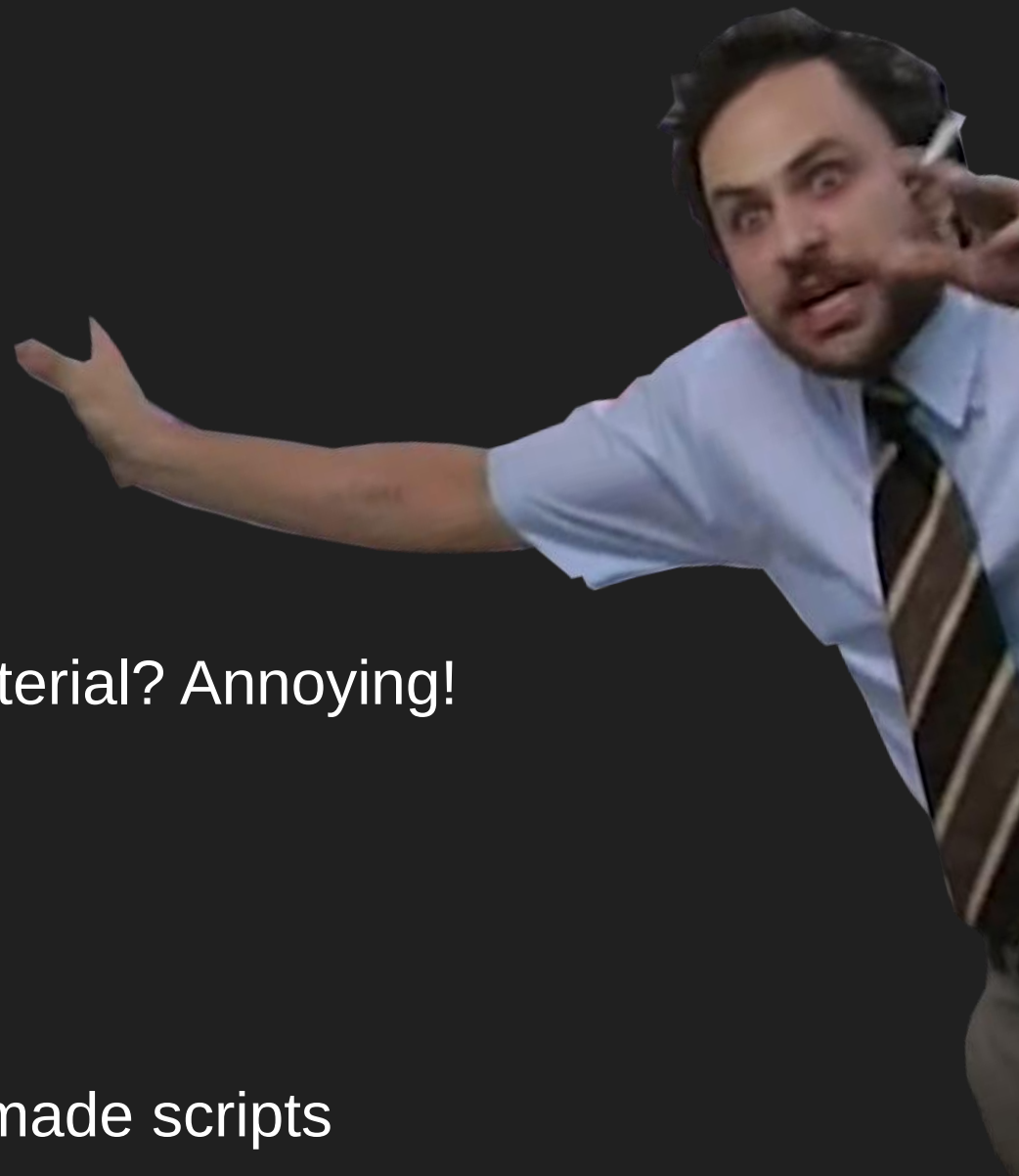
You're hacked, now what?

Year 2000:

- Look at processes (`ps`, `lsof`)
  - IRC bot (using BitchX)!
- `cron` jobs!
- `.bash_history`
- `auth.log` / `syslog` / `wtmp`

FOX IT
part of nccgroup

10 years ago



Investigating at scale? Hard!

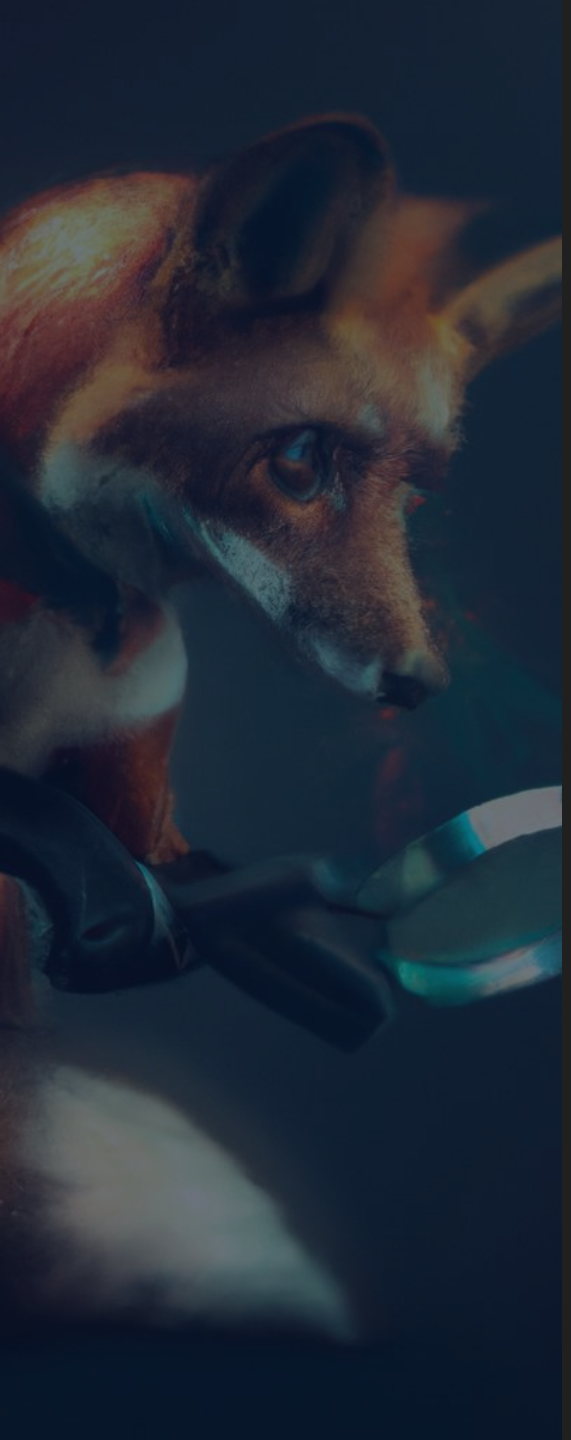
Sophisticated IOCs? Difficult!

Non-standard investigative material? Annoying!

Large teams? Chaos!

Result: home dirs full of tailor-made scripts

FOX IT
part of nccgroup



Our goal

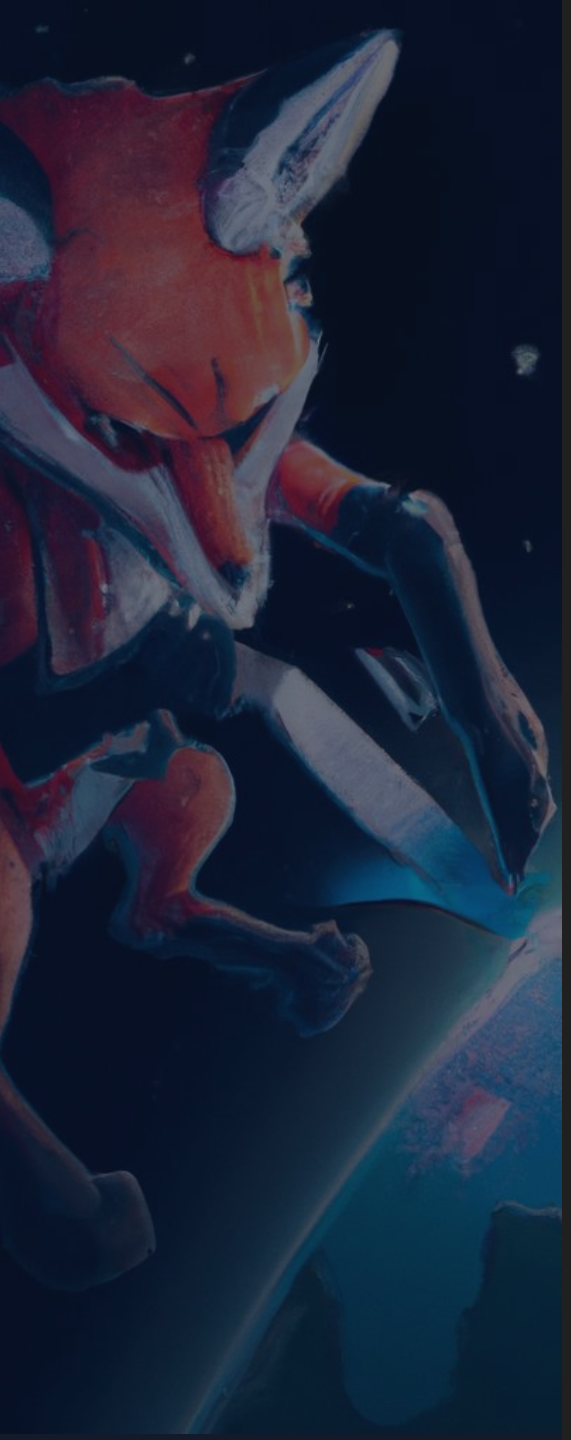
Size doesn’t matter

No data beyond our reach

No actor beyond our reach

Team distribution doesn’t matter

FOX IT
part of nccgroup



Introducing Dissect

A decade of development and IR

Modular Python framework with libraries and analyst tooling

Complex IR with ease and efficiency

We love it, we hope you do too!

FOX IT
part of nccgroup

Size doesn’t matter

Shotgun approach in data collection

Streamlined data ingestion

Collect instead of interpret

FOX IT
part of nccgroup

No data beyond our reach

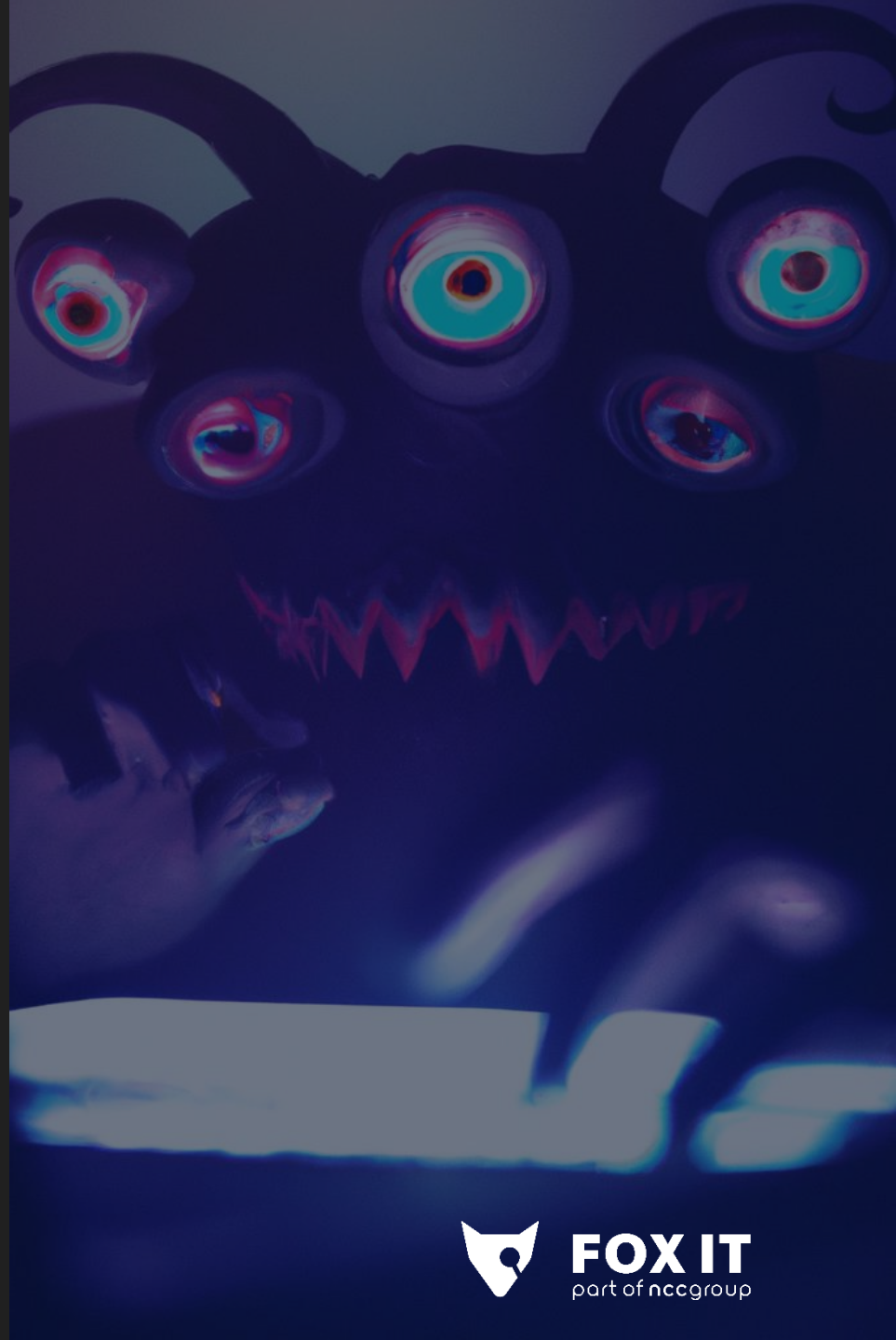
Analyse any type of data a case throws at us

Easily extendable for new data sources

- No change required to existing artefact parsers

Flexibility creates opportunities

- E.g. hypervisor data acquisition



No actor beyond our reach

Detect any technique an advanced threat actor throws at us

- Equation group, Turla, Lambert
- NTFS ACE persistence, post partition data, hidden filesystems

Possible without Dissect, but now effortlessly at scale from any source

FOX IT
part of nccgroup

Team distribution doesn’t matter

Uniform tooling, usage and output

Use different workflows, whatever suits your style

Easily allow different skill levels to work together

FOX IT
part of nccgroup

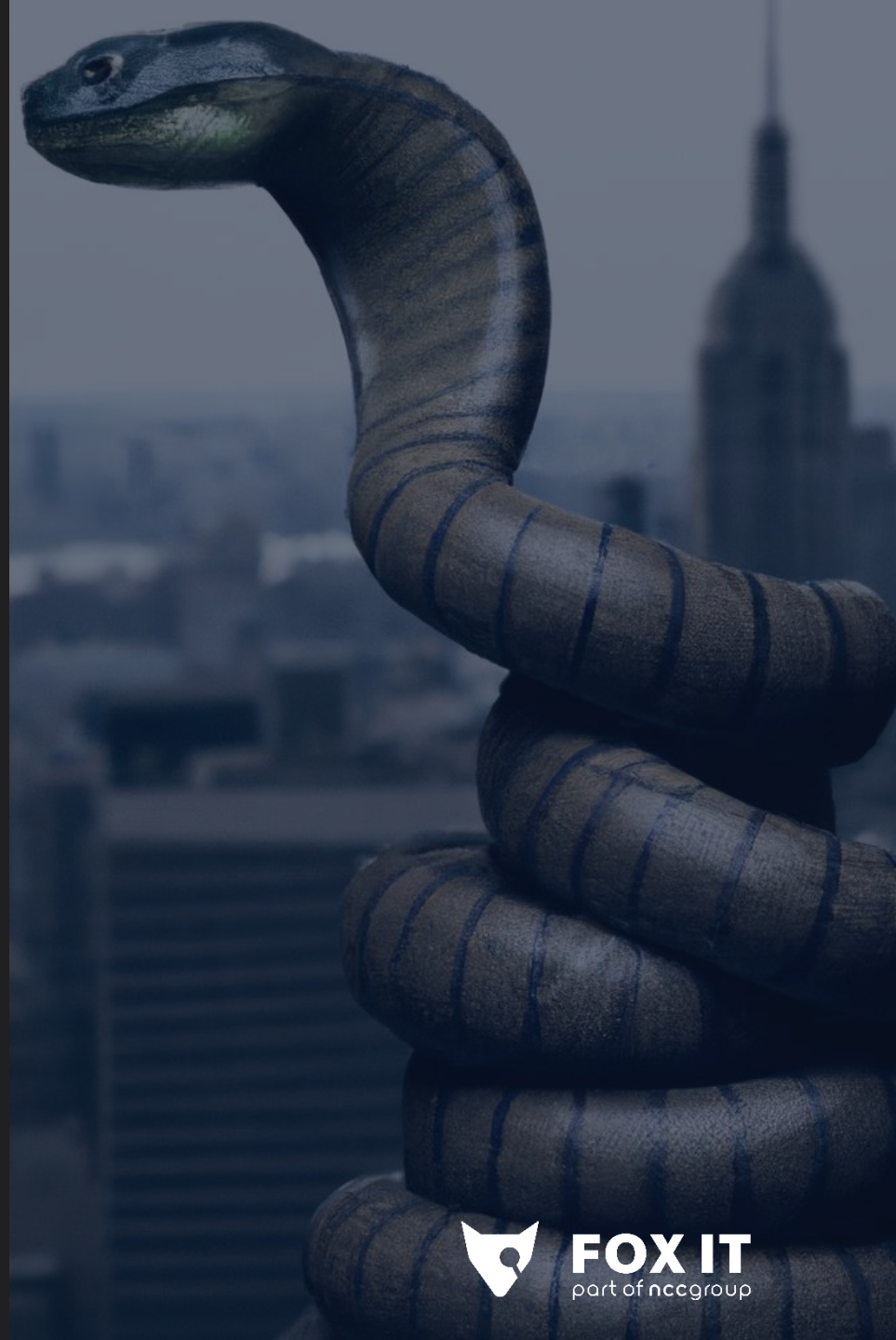
The details: What makes it tick?

Multiple abstraction layers

- Loader => Target
  - container/volume/fs implementation
    - abstract fs layer

Python `pathlib.Path` compatible implementation

- `TargetPath`



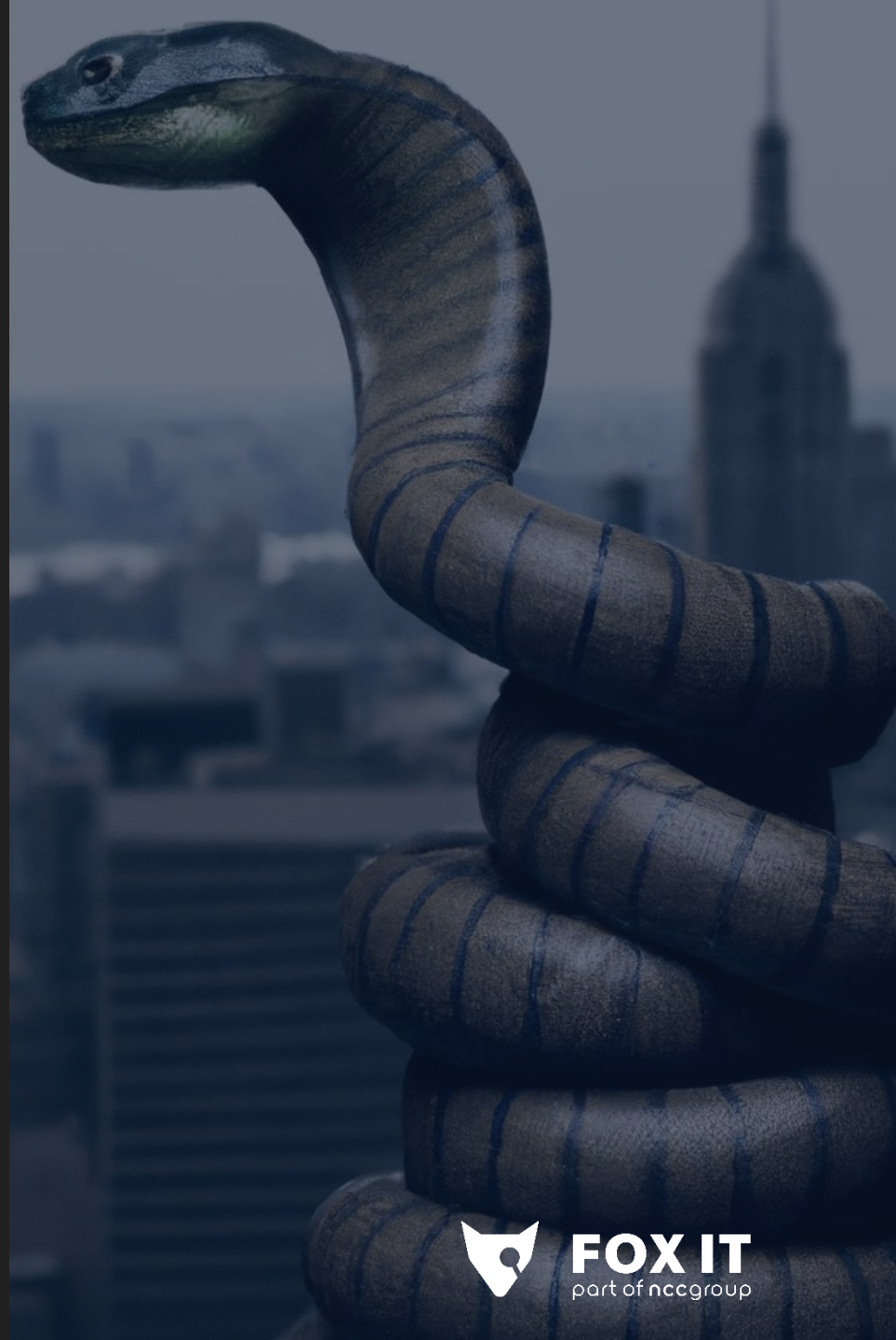
The details: What makes it tick?

Multiple abstraction layers

- Loader => Target
  - container/volume/fs implementation
    - abstract fs layer

Useful tool:

- `target-shell`



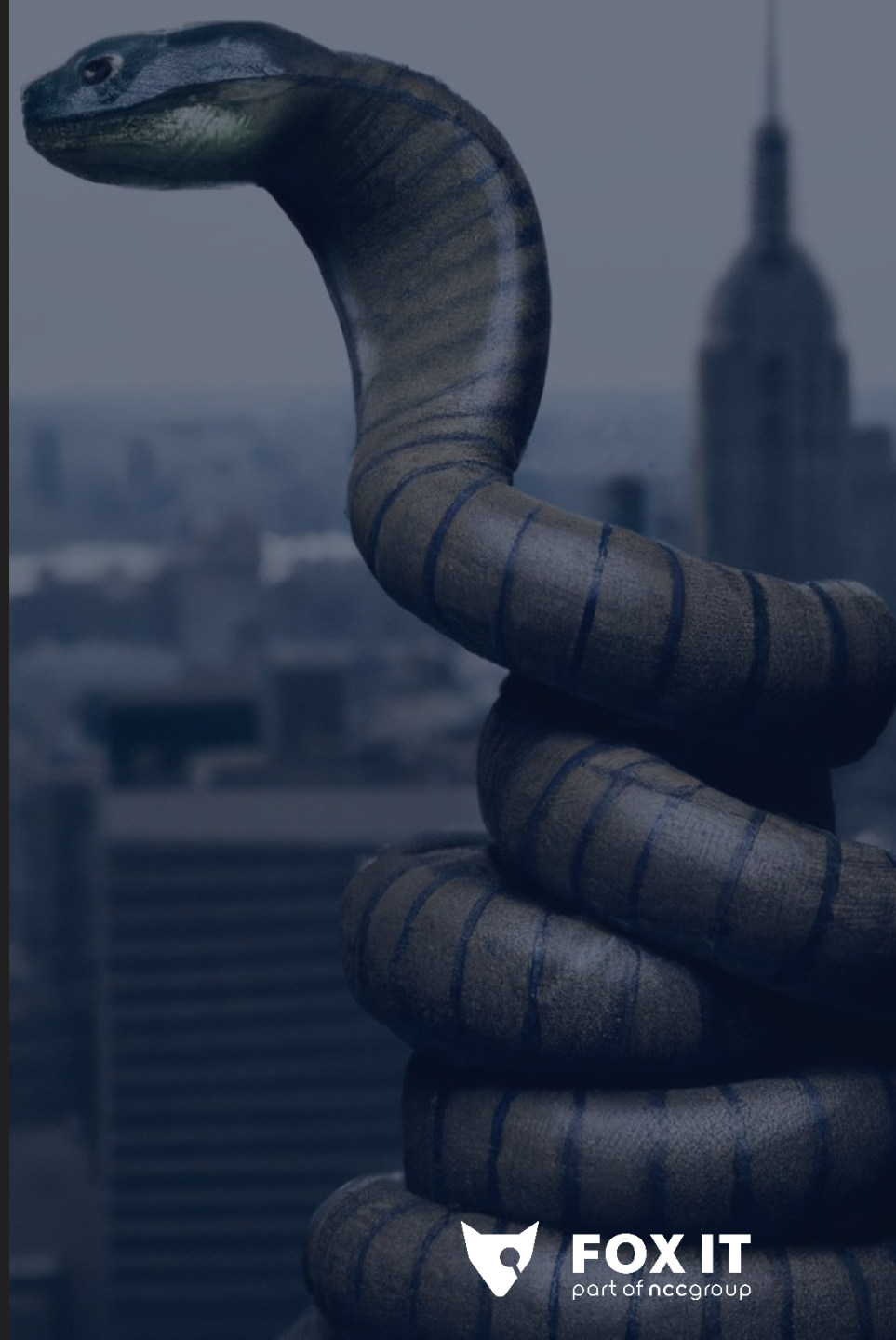
The details: What makes it tick?

Multiple abstraction layers

- Loader => Target
  - container/volume/fs implementation
    - abstract fs layer
      - OS detection (plugin)

bsd
bsd/ios
bsd/openbsd
bsd/osx
bsd/freebsd

linux
linux/fortigate
linux/redhat
linux/esxi
linux/android
linux/suse
linux/debian
linux/debian/vyos



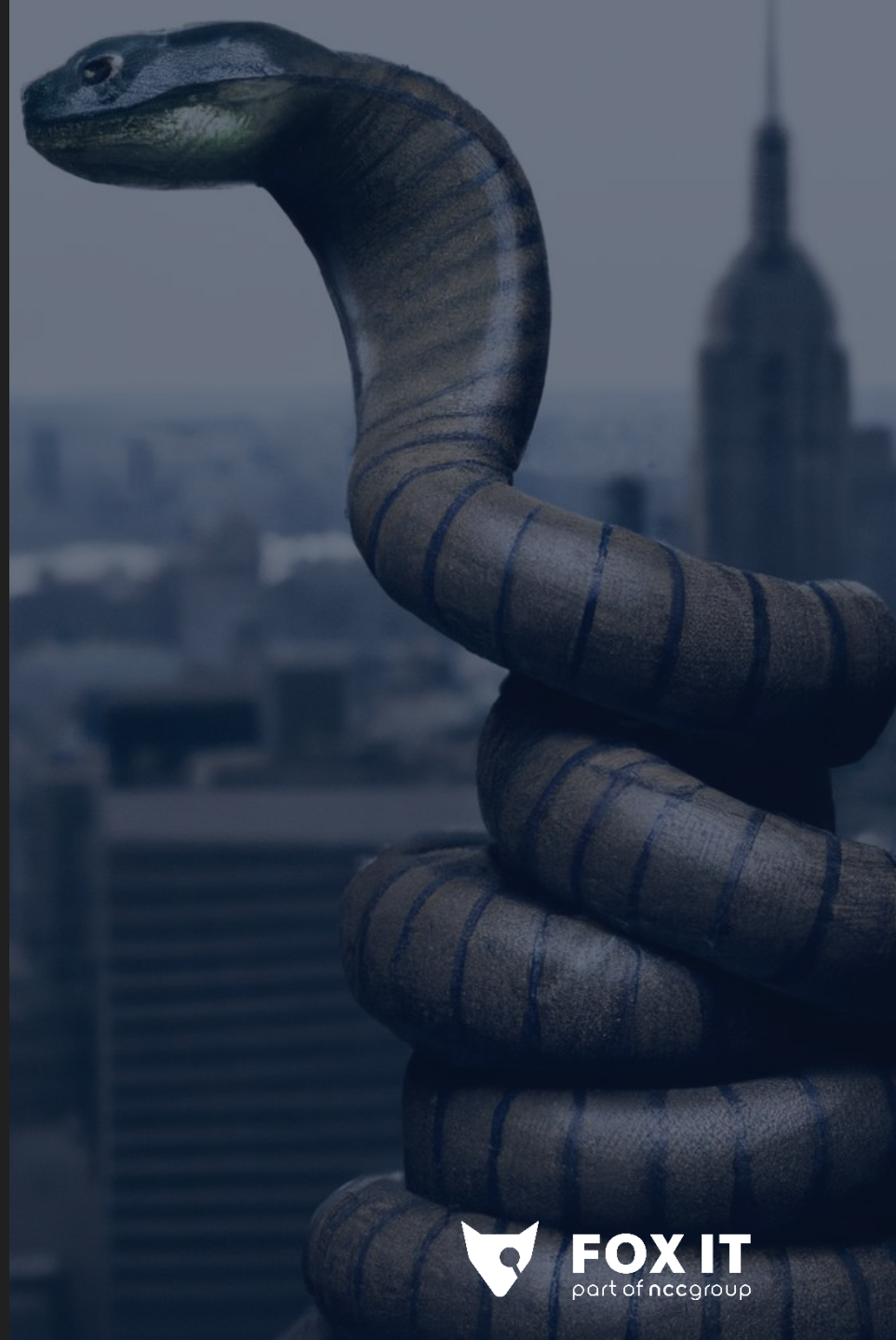
The details: What makes it tick?

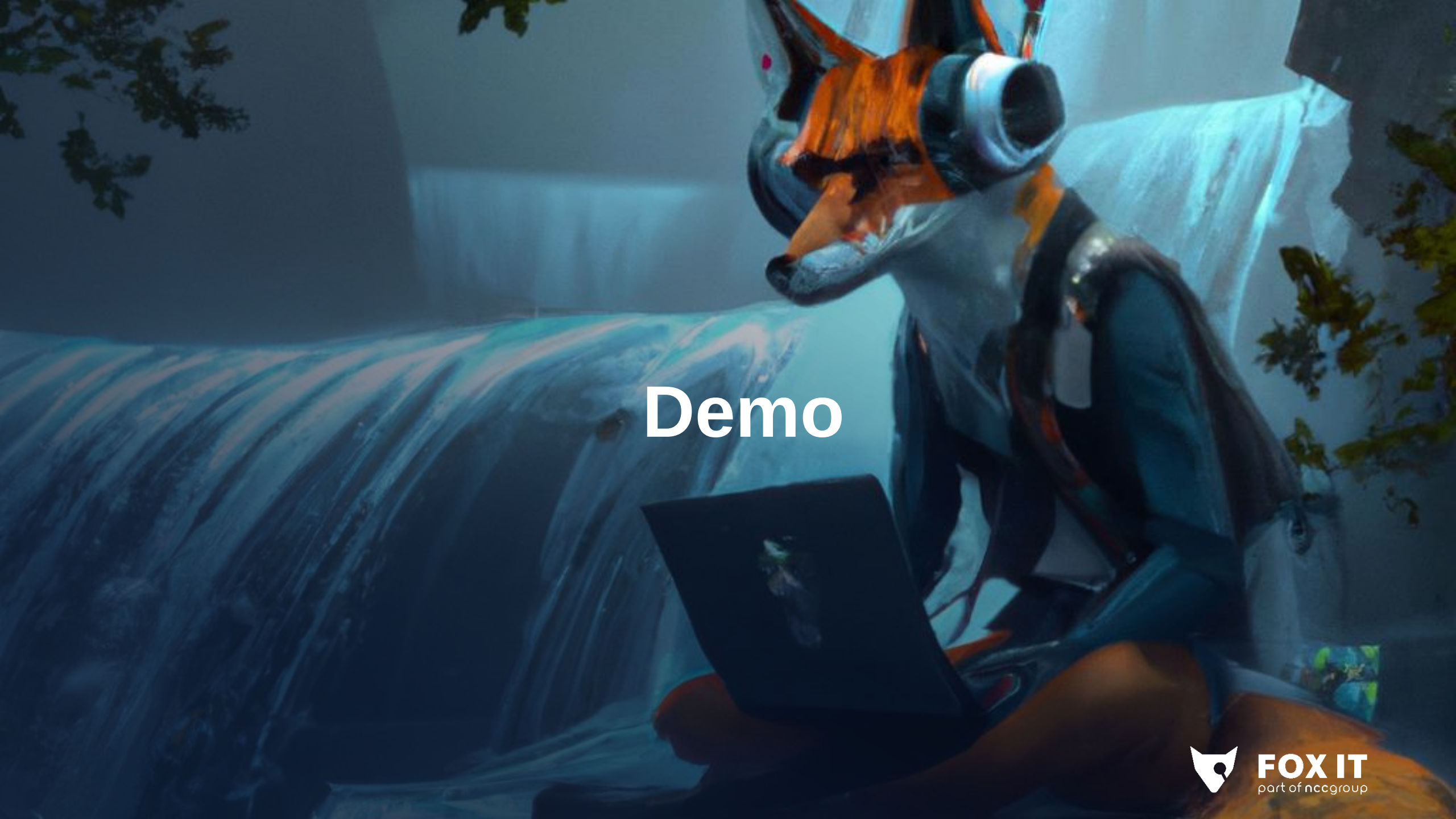
Multiple abstraction layers

- Loader => Target
  - container/volume/fs implementation
    - abstract fs layer
      - OS detection (plugin)
        - Plugins

Analysis plugins written on top

- Write once, run anywhere
- Internal: e.g. registry hive abstraction
- External: extract useful data to a structured format



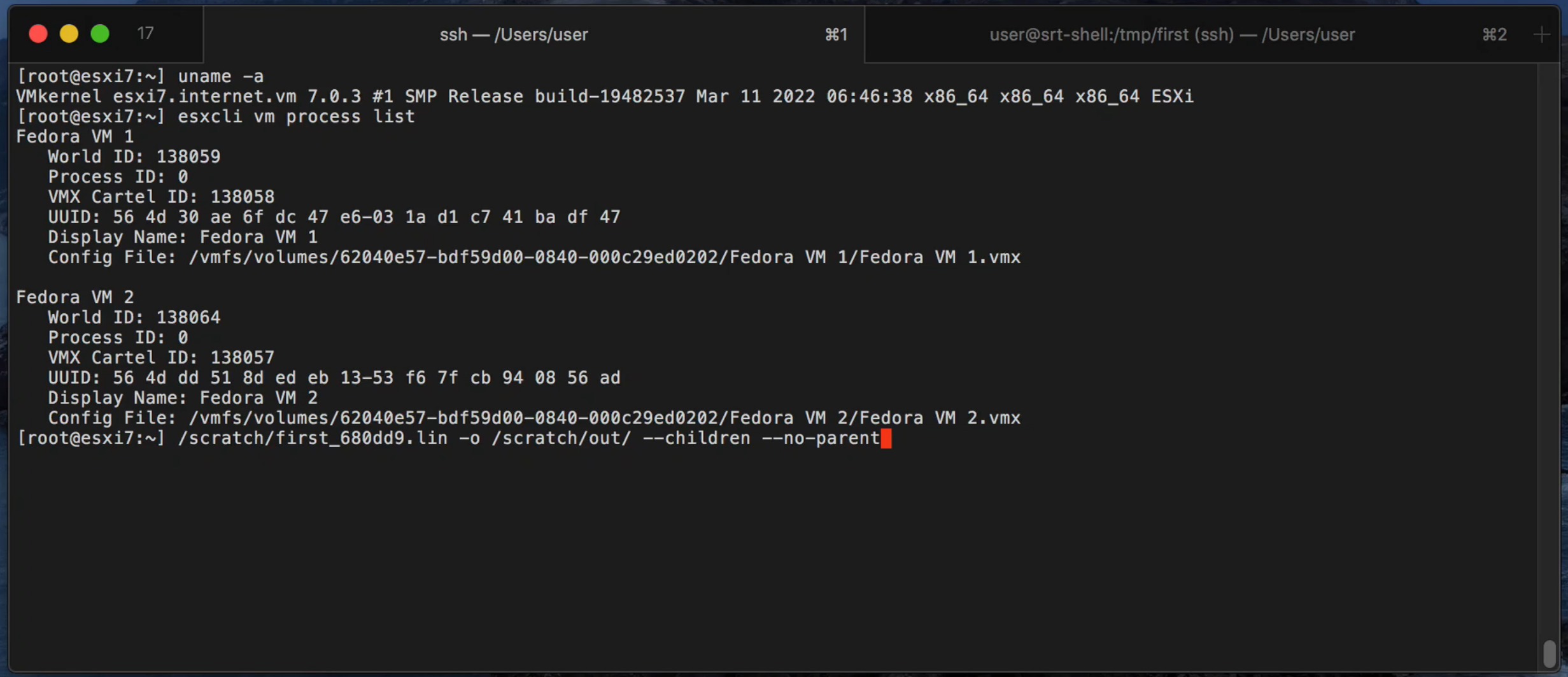


FOX IT
part of nccgroup

```
(v3.1) stefan.dereuver@lwp5 ~/fef/t $
```

```
(v3.1) stefan.dereuver@lwp5 ~/fef $
```

```
[fef] 1:bash*                                                    02 Dec 22 -- 10:44
```



FOX IT
part of nccgroup

Why open-source?

For a more secure society

We’ve depended on great open-source tools

Time to give back to the community

Encouraging contributions

FOX IT
part of nccgroup

Summary

Size doesn’t matter

No data beyond our reach

No actor beyond our reach

Faster and easier investigations benefits both analysts and clients

FOX IT
part of nccgroup

$ pip install dissect

Want to contribute?
Submit a PR at https://github.com/fox-it

FOX IT
part of nccgroup

```
$ pip install dissect
```

Documentation

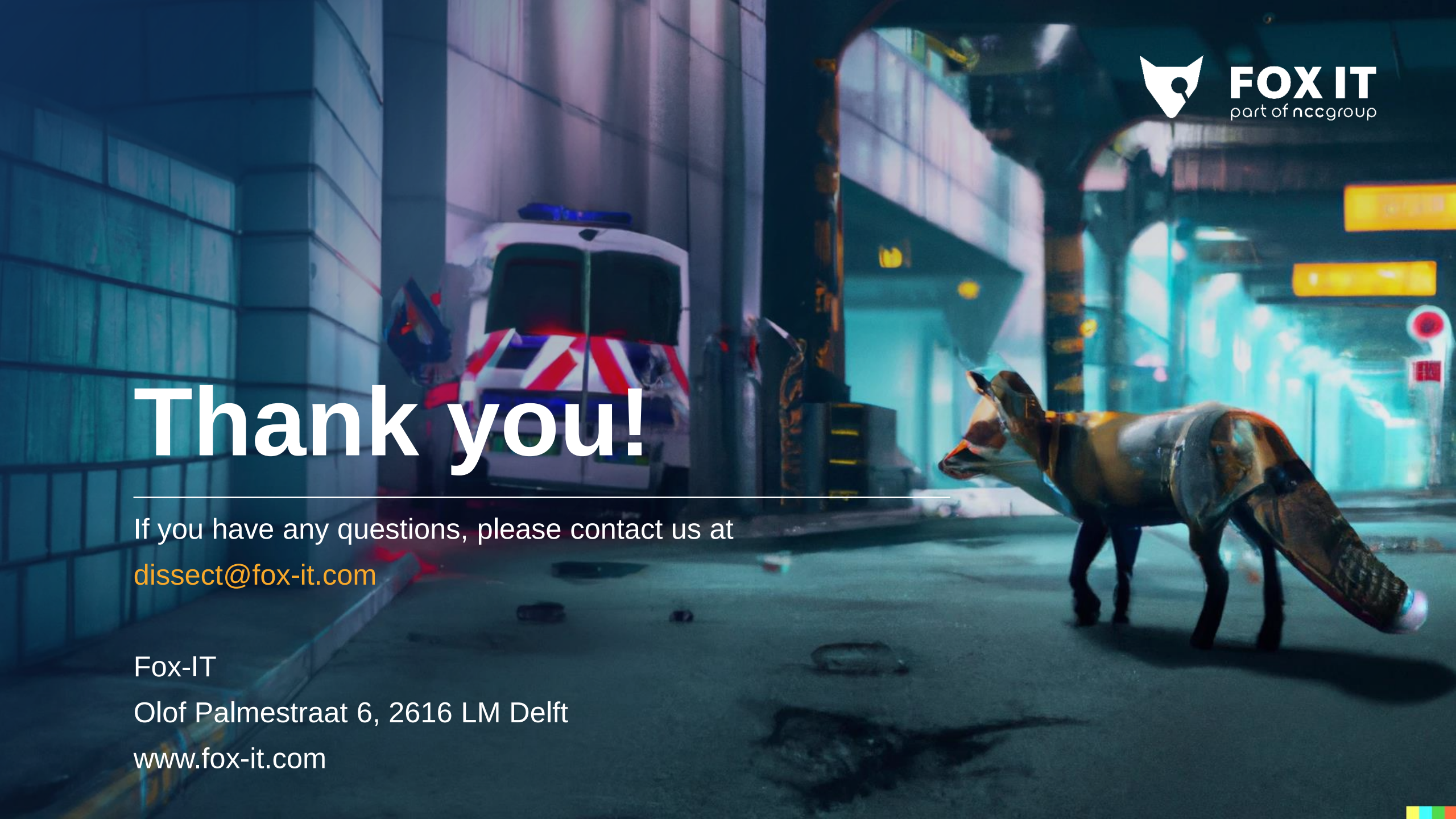
https://docs.dissect.tools/

Try for yourself

https://try.dissect.tools/

Want to contribute?
Submit a PR at https://github.com/fox-it

FOX IT
part of nccgroup



Thank you!

If you have any questions, please contact us at
dissect@fox-it.com

Fox-IT
Olof Palmestraat 6, 2616 LM Delft
www.fox-it.com