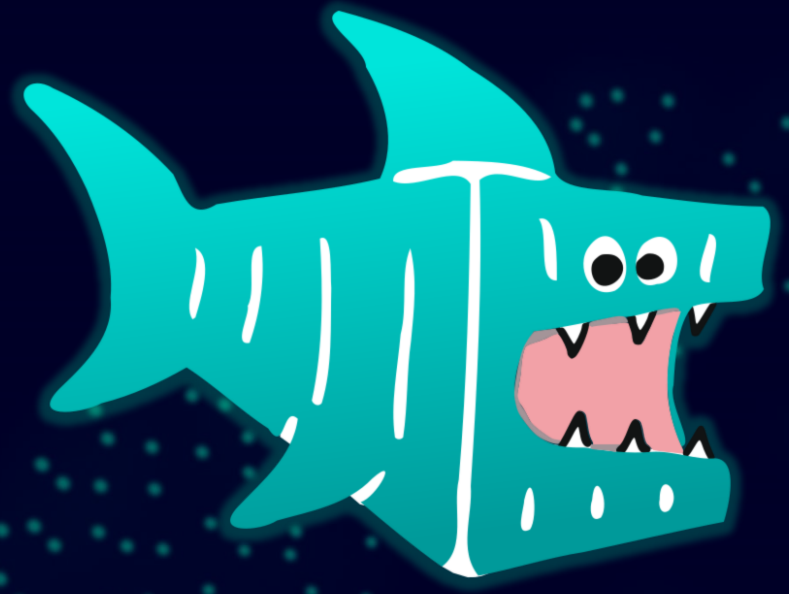
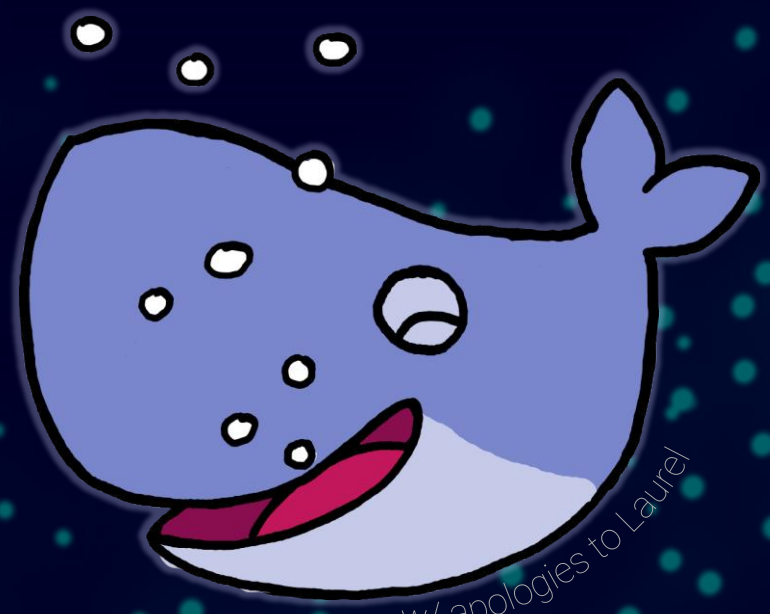
Edgeshark

Capture live container traffic from your comfy desktop Wireshark





SIEMENS

$ who am i

Principal Key Expert
in Siemens Digital Industries

- virtual (real-time) communication for containers and VMs
- container technology, especially some of its building blocks
- OT container security

Open Source (GitHub)

- @siemens/edgeshark – *this presentation*
- @onsi/gomega/gleak – *leak testing for Go routines*
- @google/nftables – *xtables match/target payload support*
- @thediveo/lxkns – *Linux kernel namespace discovery*
- @thediveo/morbid – *ephemeral containers in unit testing*
- ...

SIEMENS

Edgeshark?

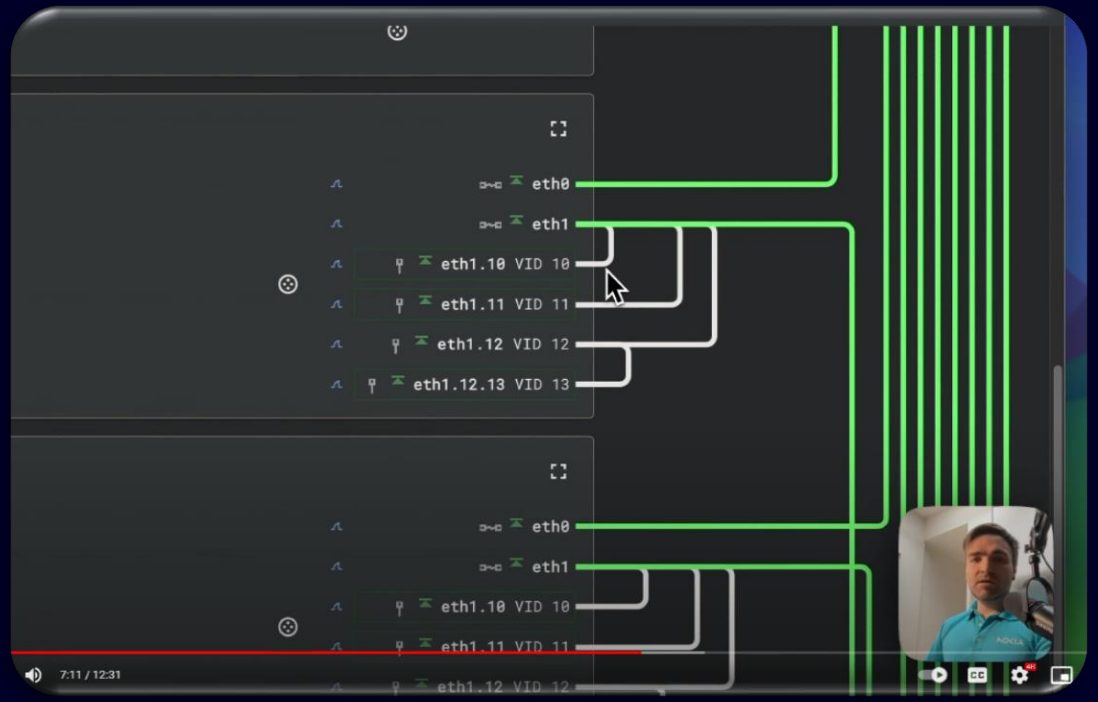
...erm, nooo!

SIEMENS

Edgeshark!

In the words of Roman Dodin,
Product Line Manager at Nokia, Github: @hellt

“ It allows to do magic ”



www.youtube.com/watch?v=iY90a_Gn5W0

SIEMENS

Do YOU Need Magic?

YOUR
container **communication**?

tap into container's and host's...

- "wiring"
- IP configuration
- DNS configuration
- open and forwarded ports
- traffic

...all put into context

HOWTO Magic?

Before: Shell Acrobatics

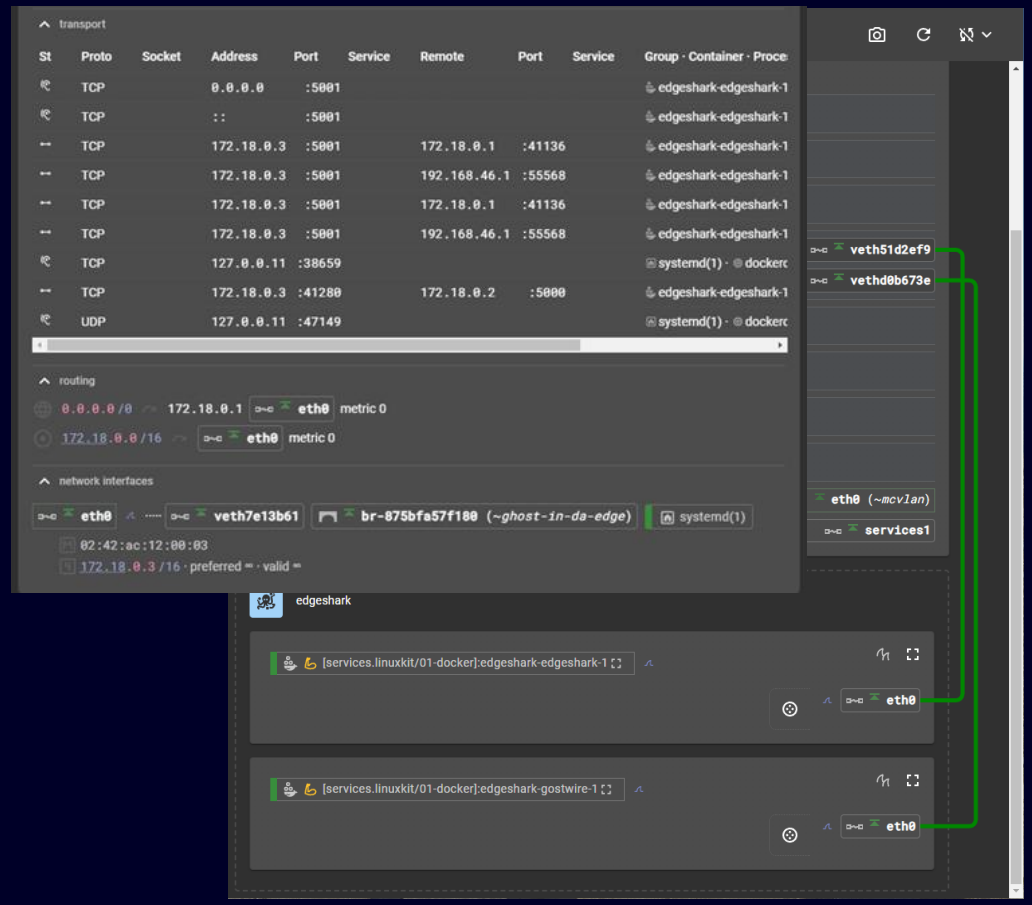
```
$ # capture remote container traffic
$ echo "YESIWANTMYSUDOPASSWORDINMYSHELLHISTORY" | \
    ssh me@containerhost 'sudo -S nsenter -t
      $(docker inspect --format "{{.State.Pid}}"
      edgeshark-gostwire-1)
      -n dumpcap -q -i eth0 -w -' | \
    wireshark -k -i -
```

```
$ # needs IP tooling inside cont
$ ssh me@containerhost \
    docker exec mycontainer ip route show
```

```
$ # needs cooperative shell inside container
$ ssh me@containerhost \
    docker exec mycontainer cat /etc/resolv.conf
```

SORRY!
no SSH for you

Edgeshark: All in a Single Place



SIEMENS

Instant Magic

`github.com/siemens/edgeshark` ➧ README ➧ Quick Start ➧ Docker Host

service

extcap

`wget … | docker compose -f – up`

(or App deployment in case of Industrial Edge)

`github.com/siemens/cshargextcap`

`wireshark.org`

Container Host
(Docker, …)

- vanilla Linux
- WSL2
- Docker Desktop (macos, Windows)
- Industrial Edge
- x86 64bit
- ARM 64bit

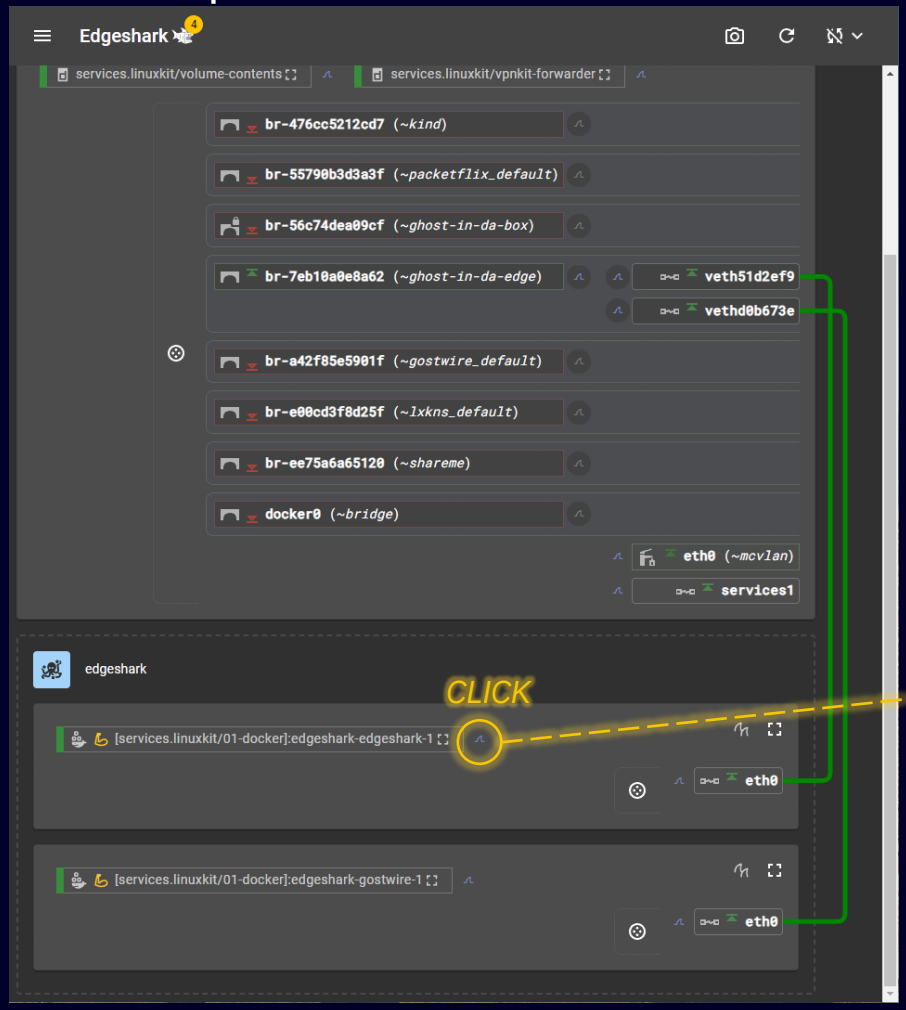
Desktop
(Browser, Wireshark)

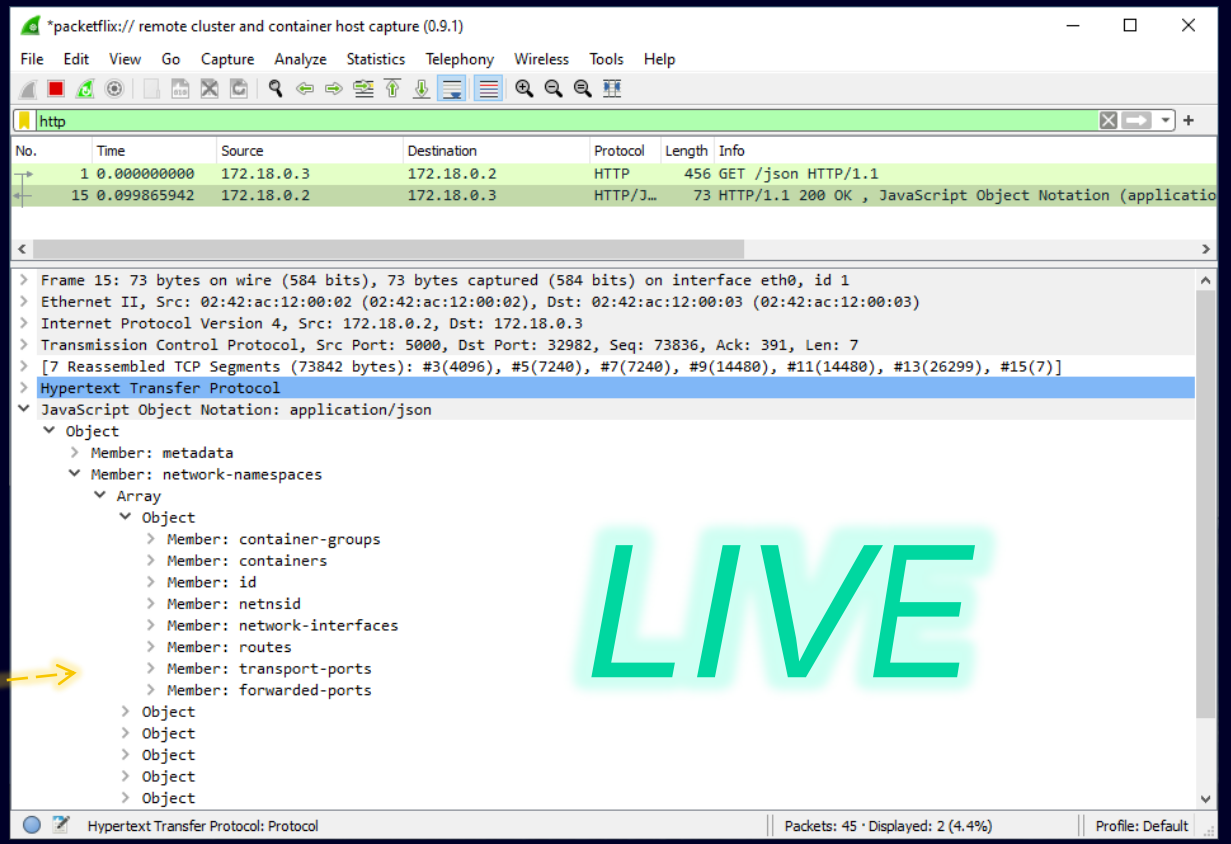
- Linux (x86 64bit, ARM 64bit)
  - .apk (Alpine)
  - .deb (Debian/Ubuntu)
  - .rpm (Fedora/…)
  - PKGBUILD (Arch)
- Windows (x86 64bit only)
- macos ARM64/x86 64bit (.zip)

SIEMENS

Tap into Virtual Networking Topology and Traffic

`http://localhost:5001`





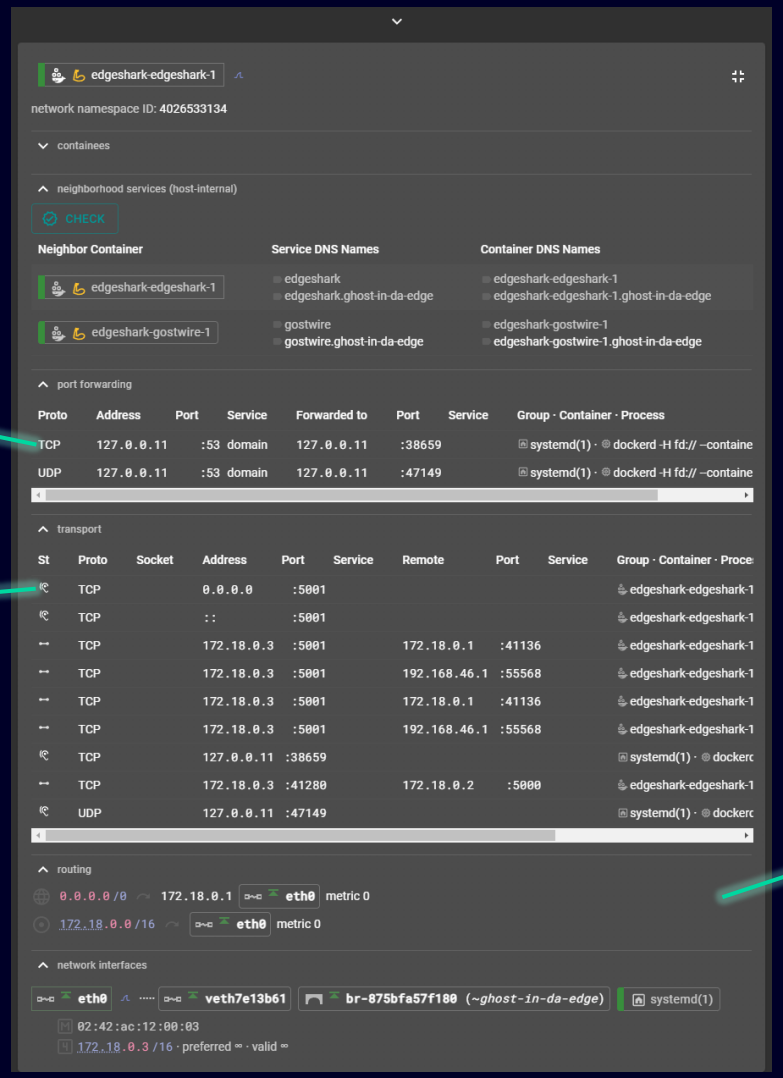
LIVE

SIEMENS

Tap into Container Communication Details

container-internal forwarded ports
(*here: Docker's embedded DNS*)

open or connected ports



IP routing and
address(es)

SIEMENS

Architect as a Service [Aaas]

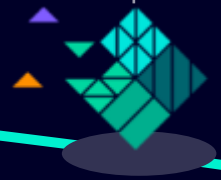
Spectre v1 full disclosure
Jan 2018

Ghostwire Discovery
Feb 2018: poc … proof-of-crash
May 2018: only terminal output yet

Packet Capture Streaming
and Wireshark plugin
Apr 2019

PACKETFLIX

Industrial Edge Support
Jan 2020
introduces the catchy “Edgeshark” name



OpenSource Github
Jun 2023

7 repositories;
15,000 LoC Go;
8,500 LoC React/TSX;
4,500 LoC Markdown

SIEMENS

Architecture of Magic

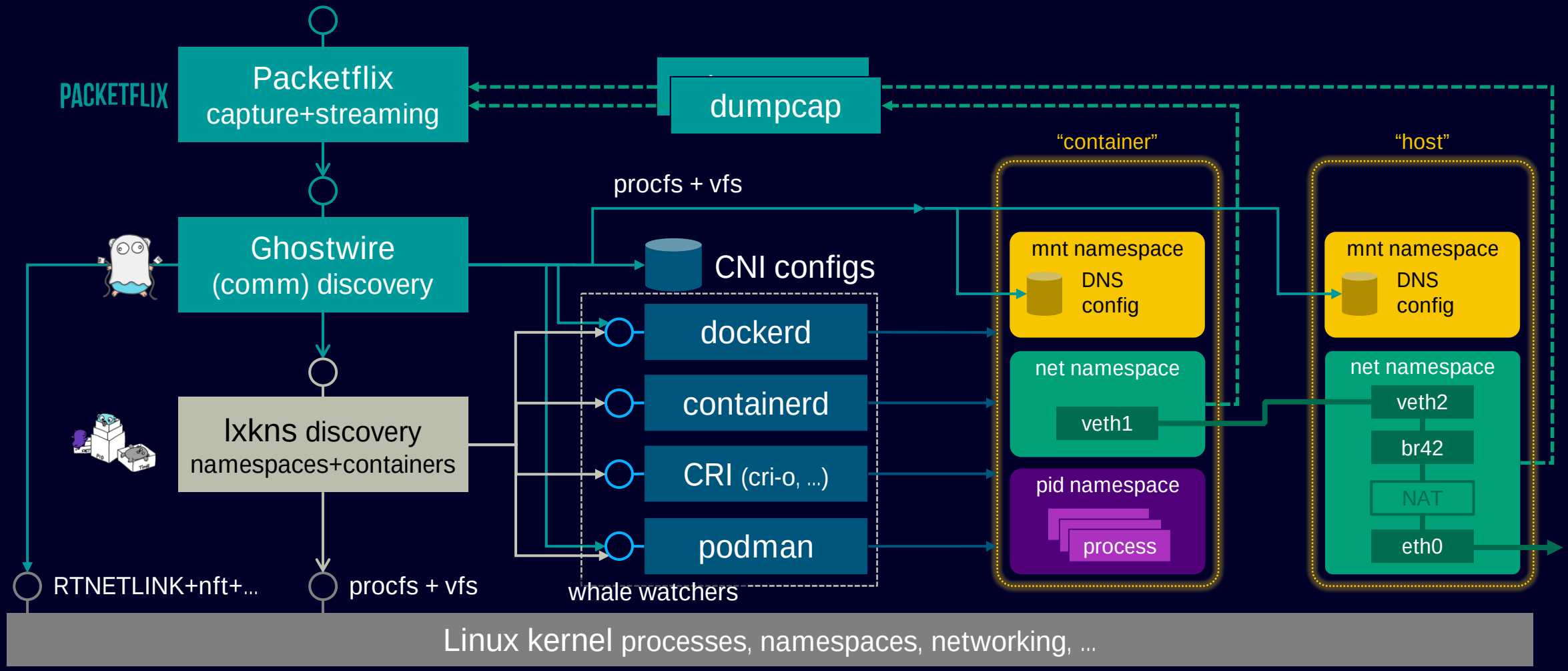
tap into container (host) traffic

tap into container/host configuration data: DNS resolver, CNI, ...

tap into container engine data: container workload, custom network names

tap into kernel networking communication state

Architecture of Magic



SIEMENS

(Where) Do You Mount the Docker Socket?

Any PSS-Os and -Es in the audience?

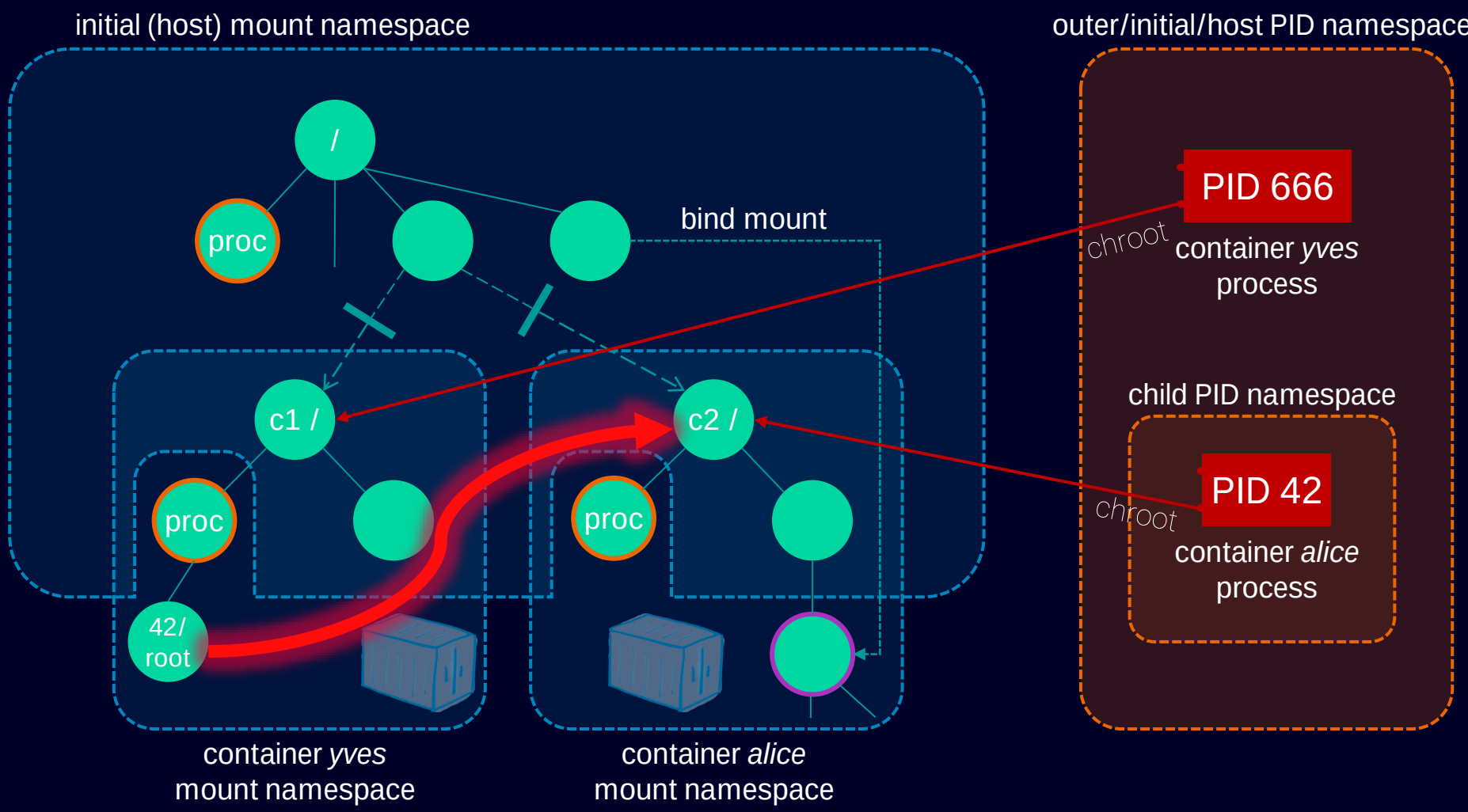
➔ *hand out the paper bags*

No, We Don't

[...*Magic*]

w/ apologies to Laurel

Tapping Into Engines/Containers [Mountineers … DON'T mount(2)]



mount namespaces

- separation of mount points
- NOT: ~~VFS separation.~~

proc fs

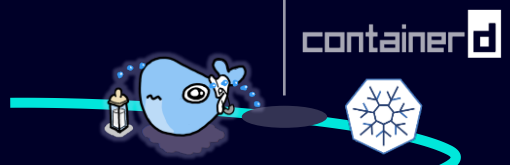
- `/proc/$PID/root`
- access mediation based on UID/GID *or* CAP_SYS_PTRACE
- used by cAdvisor, bcc(!), …

SIEMENS

Whale Whispering: Tapping Into Engines

detect container engine processes

dockerd, *containerd*, *cri-o*, ...



scan open file descriptors for listening unix sockets, get path(s)

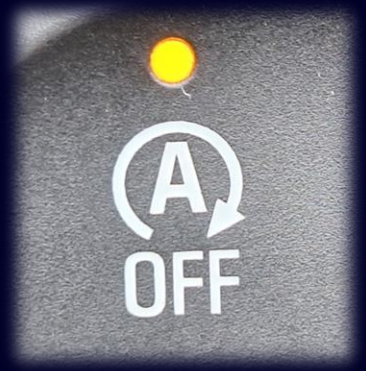
assemble full API path

`/proc/$ENGINEPID/root/$API`

access engine API “as usual”

SIEMENS

podman: Detecting the Undetectable



- podman exits when idle
- telemetry and diagnosis in prod/development cause *permanent* service operation – but we cannot rely on podman being active.

detect *socket activator* processes

…*anywhere*

scan open fd's for listening UDS with well-known suffix

`/…/…/podman.sock`

activate engine

…and wait for it to become responsive as we need its PID

access engine API "as usual"

SIEMENS

Edgeshark

[github.com/siemens/edgeshark]

- live tap into container network traffic directly from Wireshark
  - *downloading* [pcaps] *is so 90's*, everyone's *streaming*!

- ...much more than a "Wireshark Web UI", Edgeshark...
  - taps into virtual networks topology inside container hosts
  - taps into open and connected ports, forwarded ports (Docker, kube-proxy)
  - taps multiple container engines, *Docker*, *containerd*, *cri-o*, *podman*
  - has engine-in-container auto-detection
  - is KinD-aware ("Kubernetes-in-Docker")
  - comes with an integrated screenshot feature for documentation purposes
  - ...

Contact

Dr. Harald Albrecht
Principal Key Expert *Systems Communication and Control Networks*
harald.albrecht@siemens.com

github.com/siemens/edgeshark

SIEMENS