# Debugging Kubernetes and Container Workloads with the Superpower of eBPF

Kubernetes Community Day, Islamabad, 2024

# Hello!

## Qasim Sarfraz

Software Engineer @ Microsoft

- I am from Lahore, Pakistan
- Currently, based in Hamburg, Germany
- I work with on OSS, Containers, Kubernetes
- I'm focused on Inspektor Gadget, kubectl aks and CoreDNS header plugin.
- I'm available at https://mqasimsarfraz.com

# Agenda

1. What is eBPF?
2. Debugging Containers using eBPF
3. Inspektor Gadget as a **tool**
4. Inspektor Gadget as a **framework**
5. Contributing

# What is eBPF?

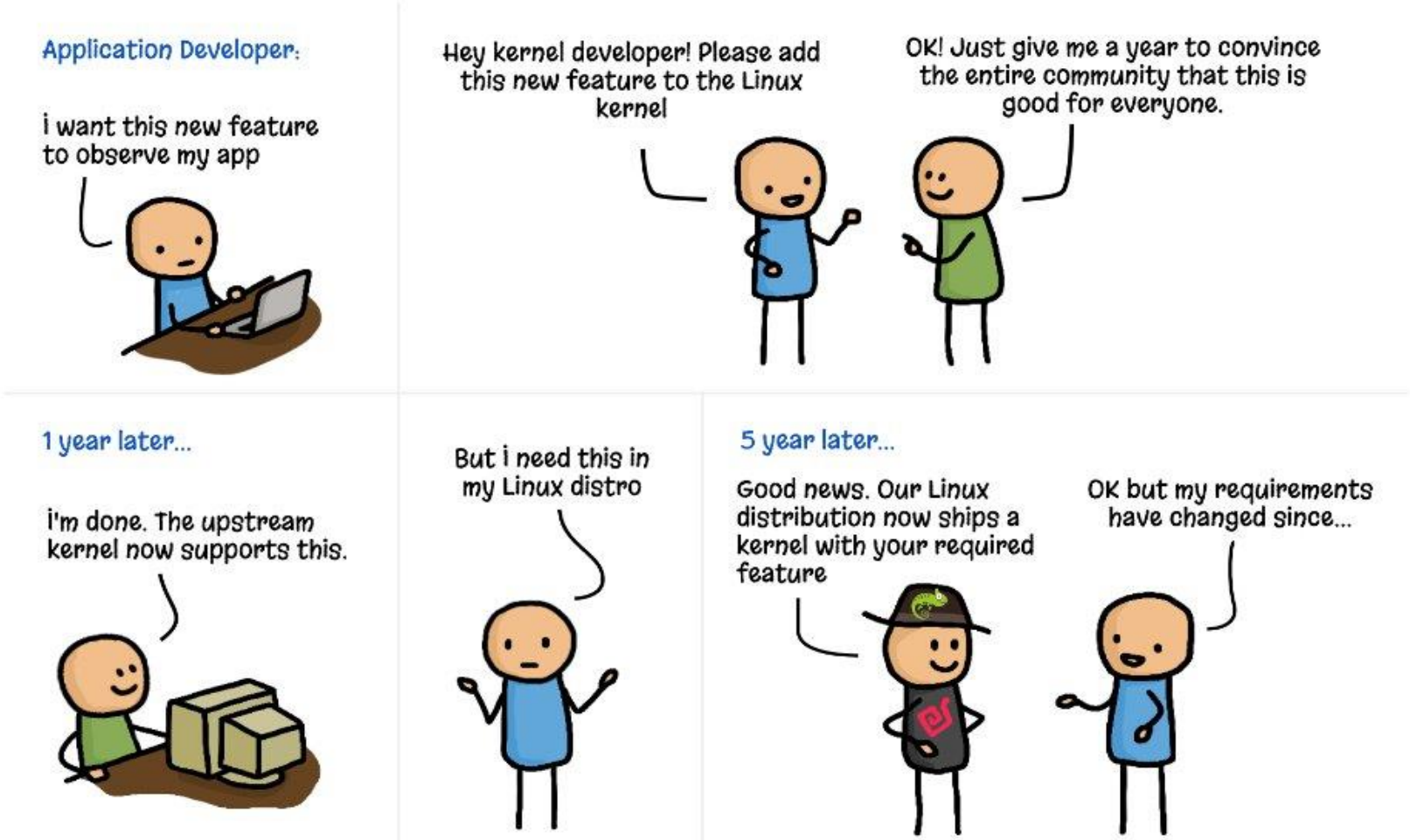
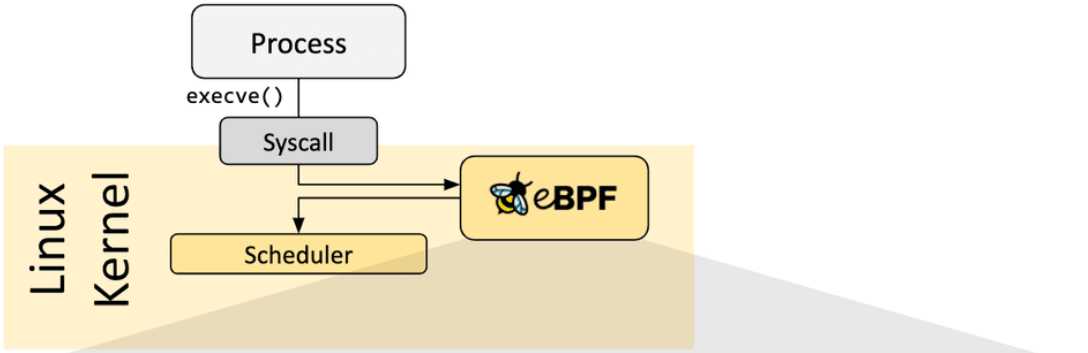



Image credit: Isovalent [blog]

# What is eBPF?

"eBPF does to Linux what JavaScript does to HTML. (Sort of.)" - Brendan Gregg, Netflix



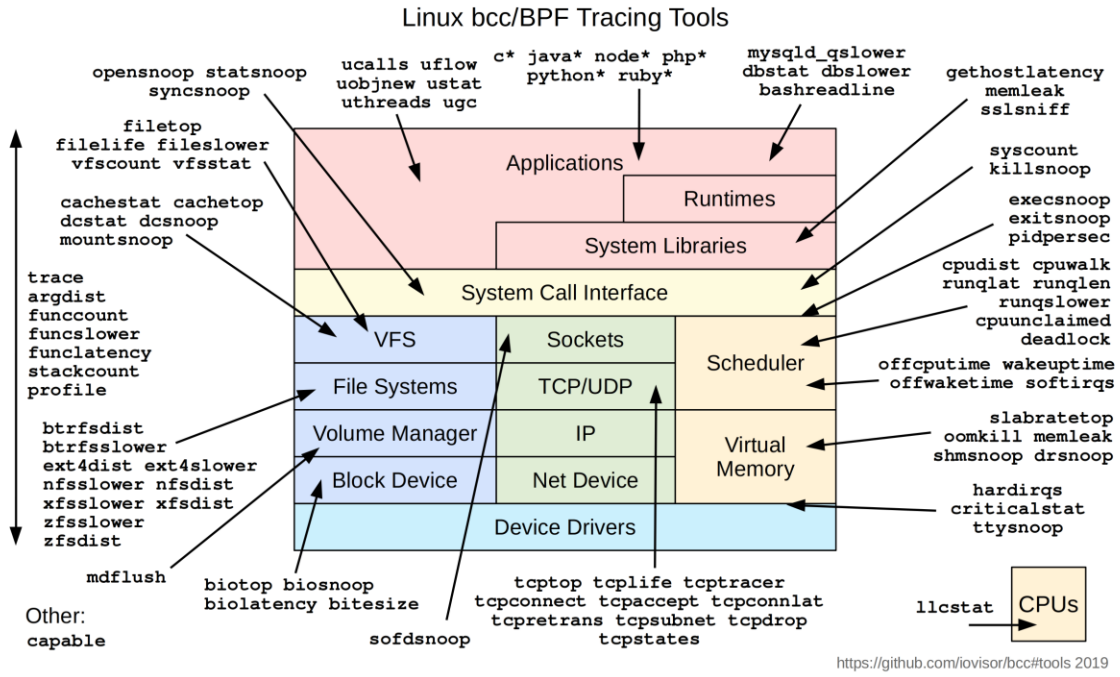

```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

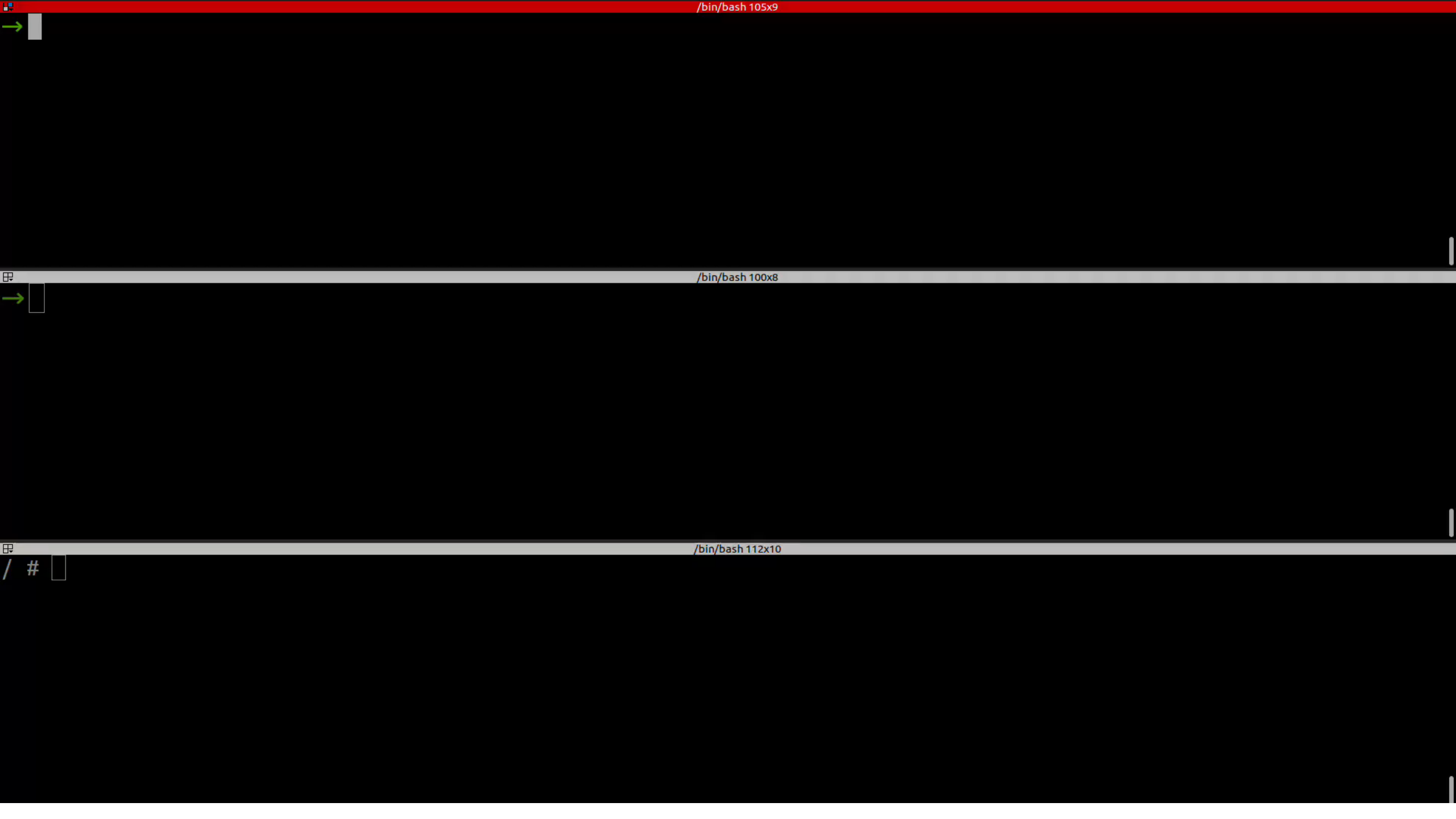
https://ebpf.io/what-is-ebpf/

# Debugging Containers using eBPF

# Debugging Containers using eBPF

- BPF Compiler Collection (BCC):
  - Special Filtering:
    - By cgroups
    - By mount namespace
  - For Example:
    - Create an an eBPF map
    - Start a BCC tool with the path to eBPF map
    - Update eBPF map by adding mount namespace of the container




/bin/bash 105x9
/bin/bash 100x8
/bin/bash 112x10
/ #

# Problems

INSPEKTOR GADGET

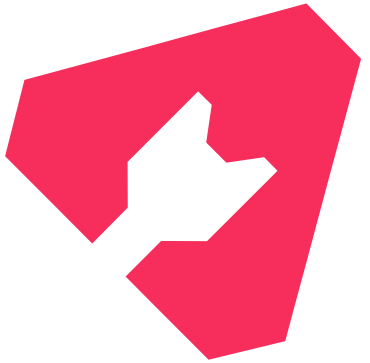
- Painful debugging experience.
- Lack of support of:
  - Container enrichment
  - Container filtering
- Distribution/Packaging Problem?

# Inspektor Gadget as a tool

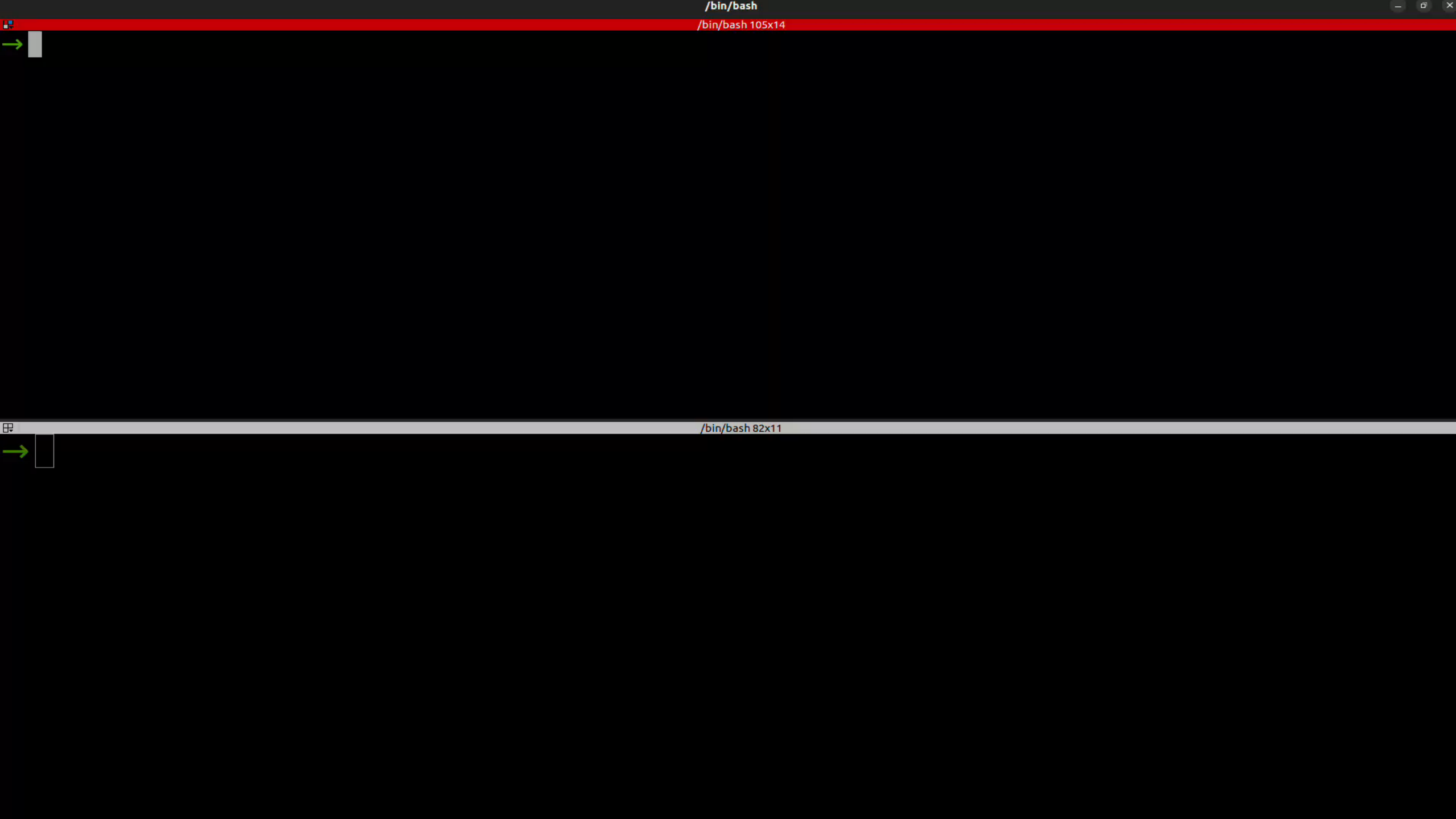
https://www.inspektor-gadget.io

# Inspektor Gadget as a tool

- A collection of **eBPF-based** gadgets to debug and inspect Kubernetes apps and resources
- It is a **CNCF** sandbox project
- Available as a krew plugin
  - **`kubectl krew install gadget`**
  - **`kubectl gadget deploy`**
- Also available as:
  - A CLI tool for Linux hosts called **ig**
  - A container image for **`kubectl debug`** ...



INSPEKTOR
GADGET


/bin/bash
/bin/bash 105x14
/bin/bash 82x11

# Can we improve it?

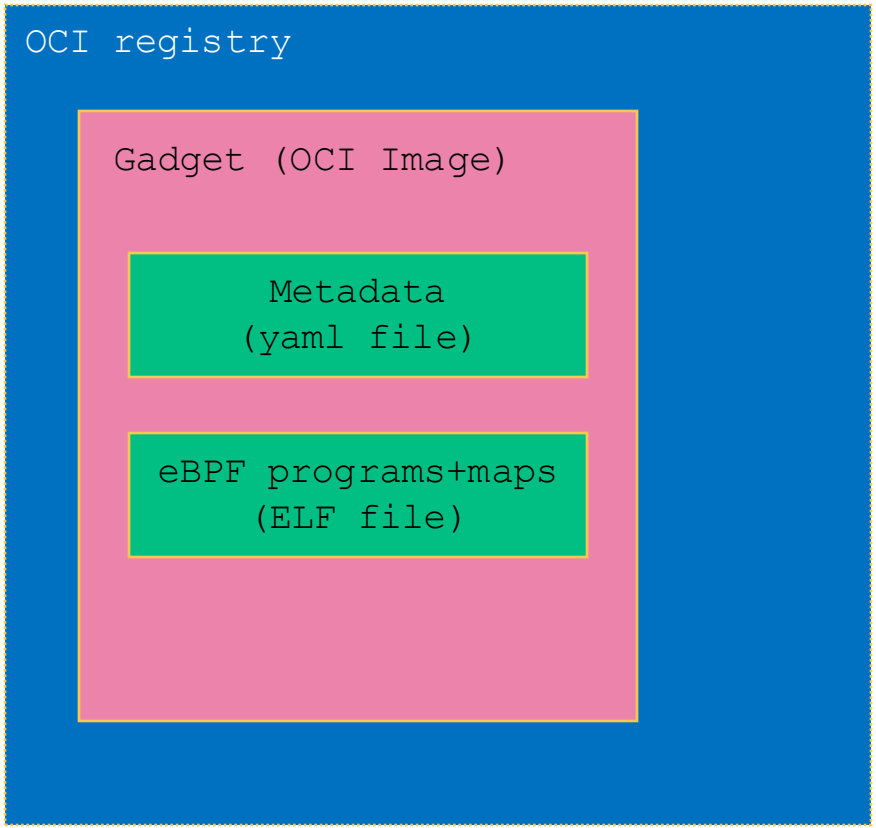
- Painful debugging experience. ✓
- Lack of support of:
  - Container enrichment ✓
  - Container filtering
- Distribution/Packaging Problem ?

# Inspektor Gadget as a framework

https://www.inspektor-gadget.io

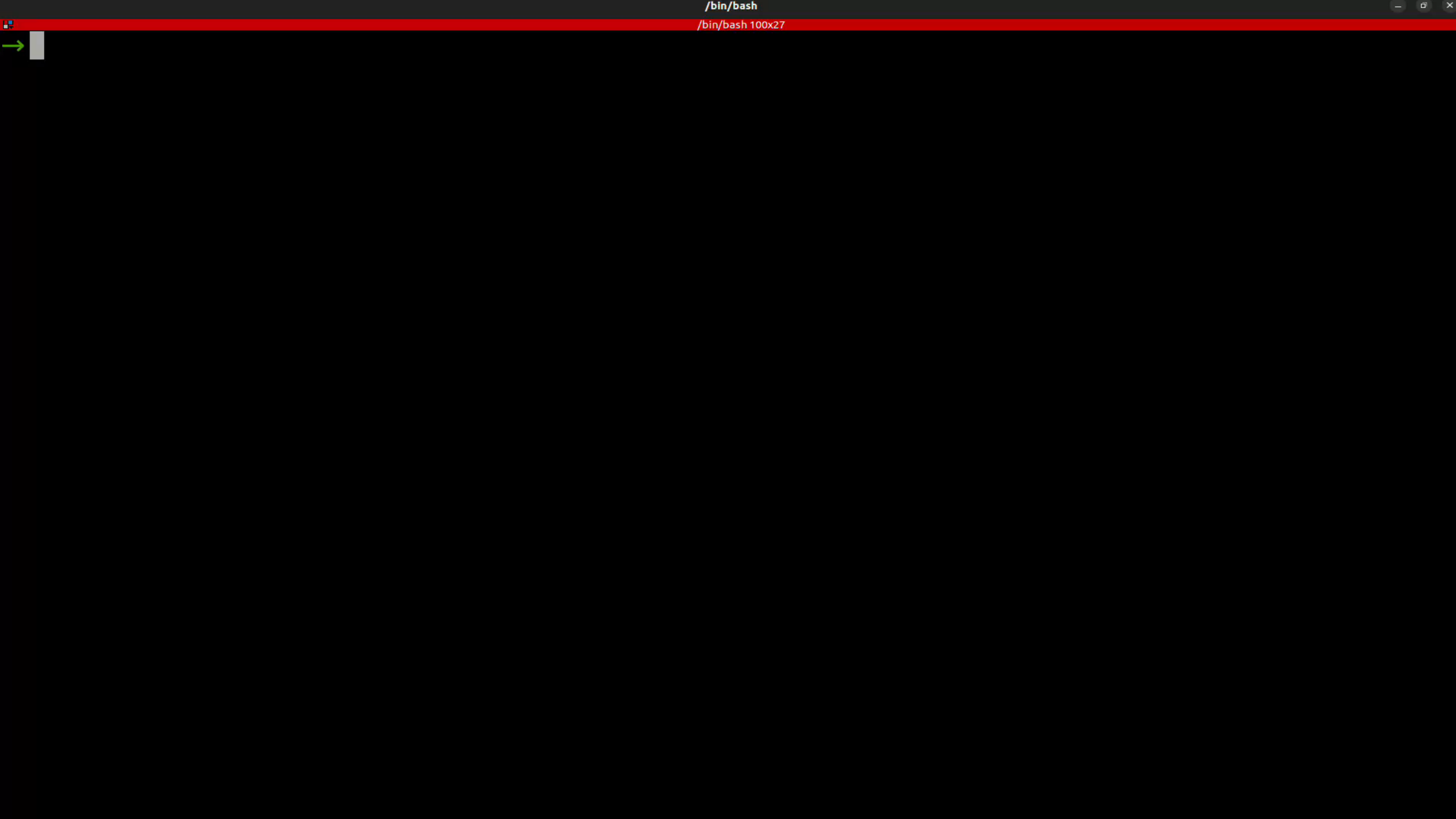
# Inspektor Gadget as a framework

- Decouple the idea of gadgets from Inspektor Gadget
- Use the idea of OCI artifacts e.g. SBOMS, Helm Charts etc.
- Gadgets packaged as OCI images and Published to OCI registries



# Inspektor Gadget as a framework

- A familiar UX to package your eBPF programs:
  - **build** – builds a gadget as an OCI image
  - **push** – pushes the gadget (OCI image) to a registry
  - **pull** – pulls the gadget from a registry
  - **run** – runs the specified gadget
- Discovery via Artifacthub
- The feature is under active development so looking for feedback from community! :)


/bin/bash
/bin/bash 100x27

# Interested in Contributing?

- We live on Github
- Use CONTRIBUTING.md as a starting point
- Look for issues with label: "good first issue"
- Reach us out at Kubernetes slack: #inspektor-gadget


# Thank you