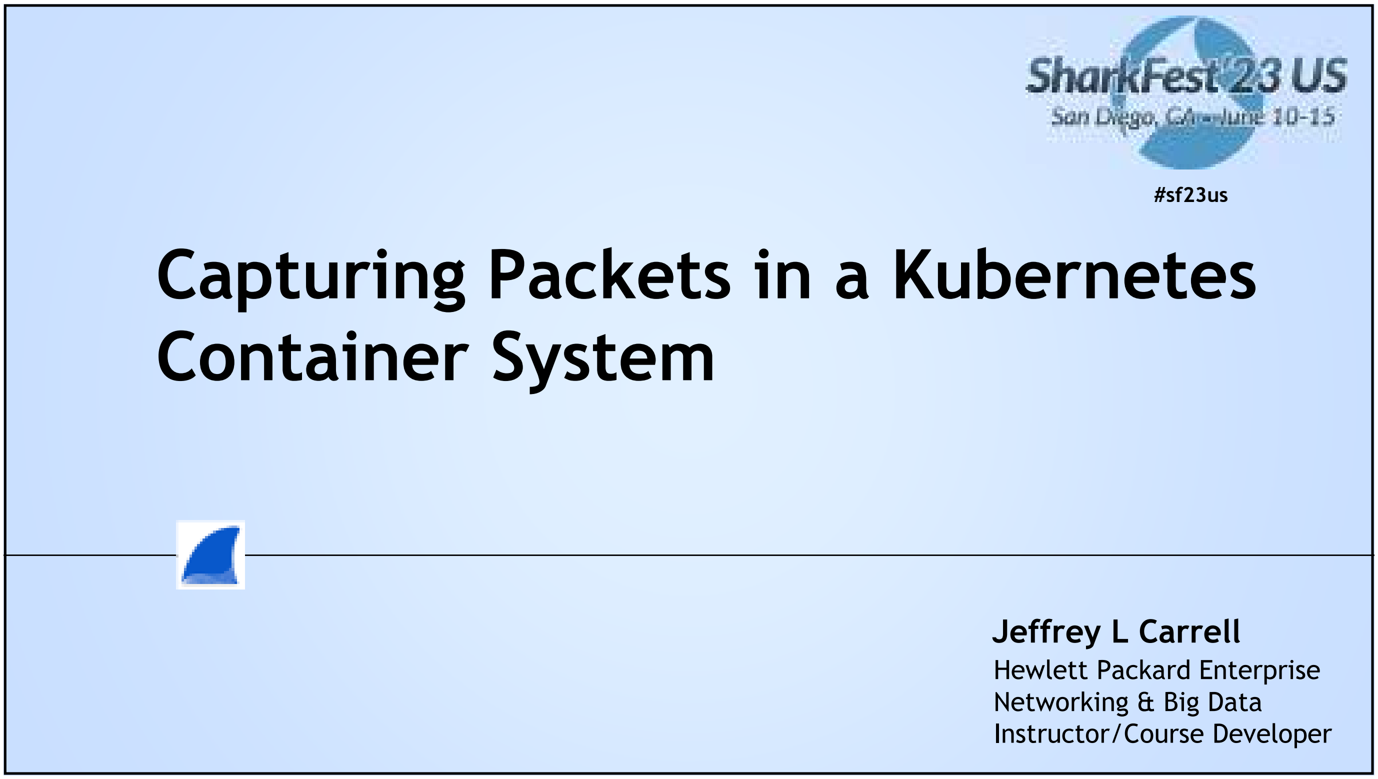
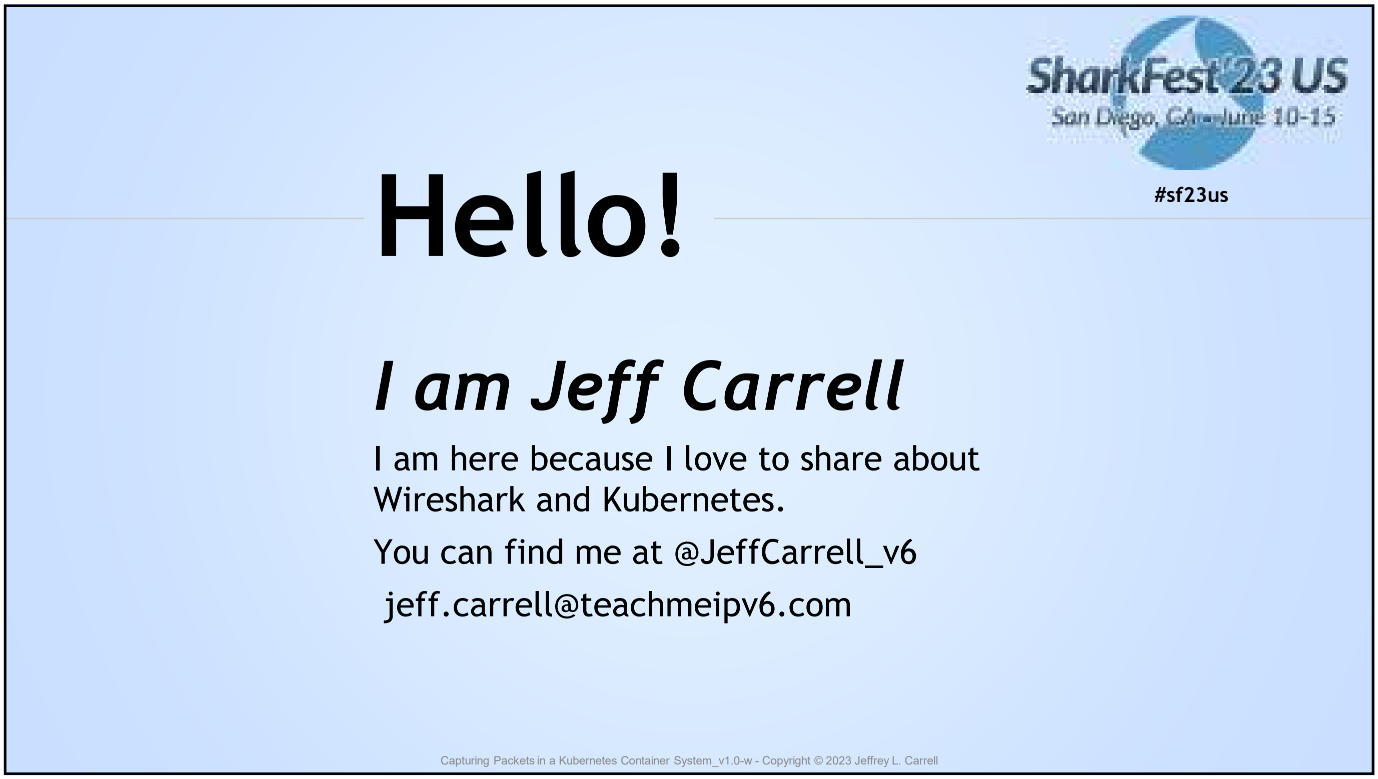


SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Capturing Packets in a Kubernetes Container System

Jeffrey L Carrell
Hewlett Packard Enterprise
Networking & Big Data
Instructor/Course Developer



SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

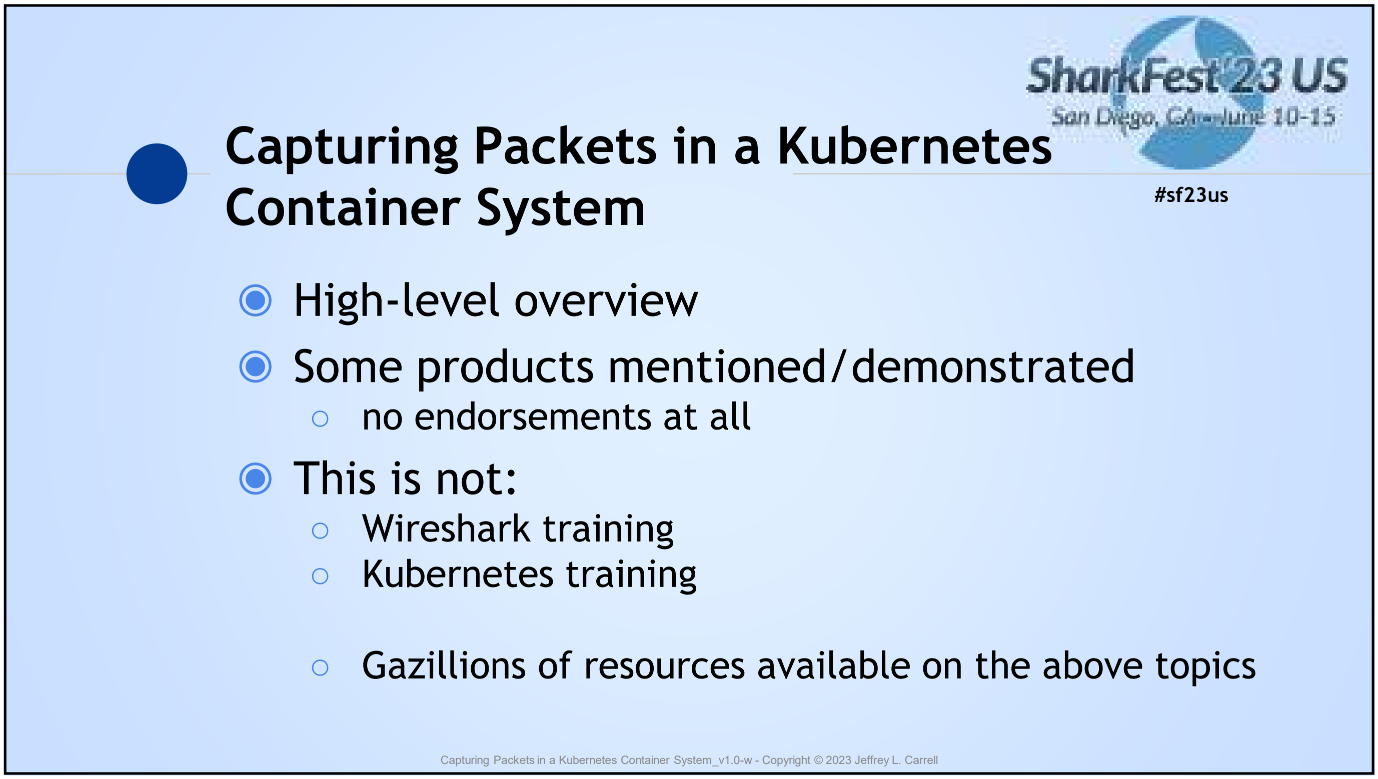
Hello!

I am Jeff Carrell

I am here because I love to share about Wireshark and Kubernetes.

You can find me at @JeffCarrell_v6

jeff.carrell@teachmeipv6.com

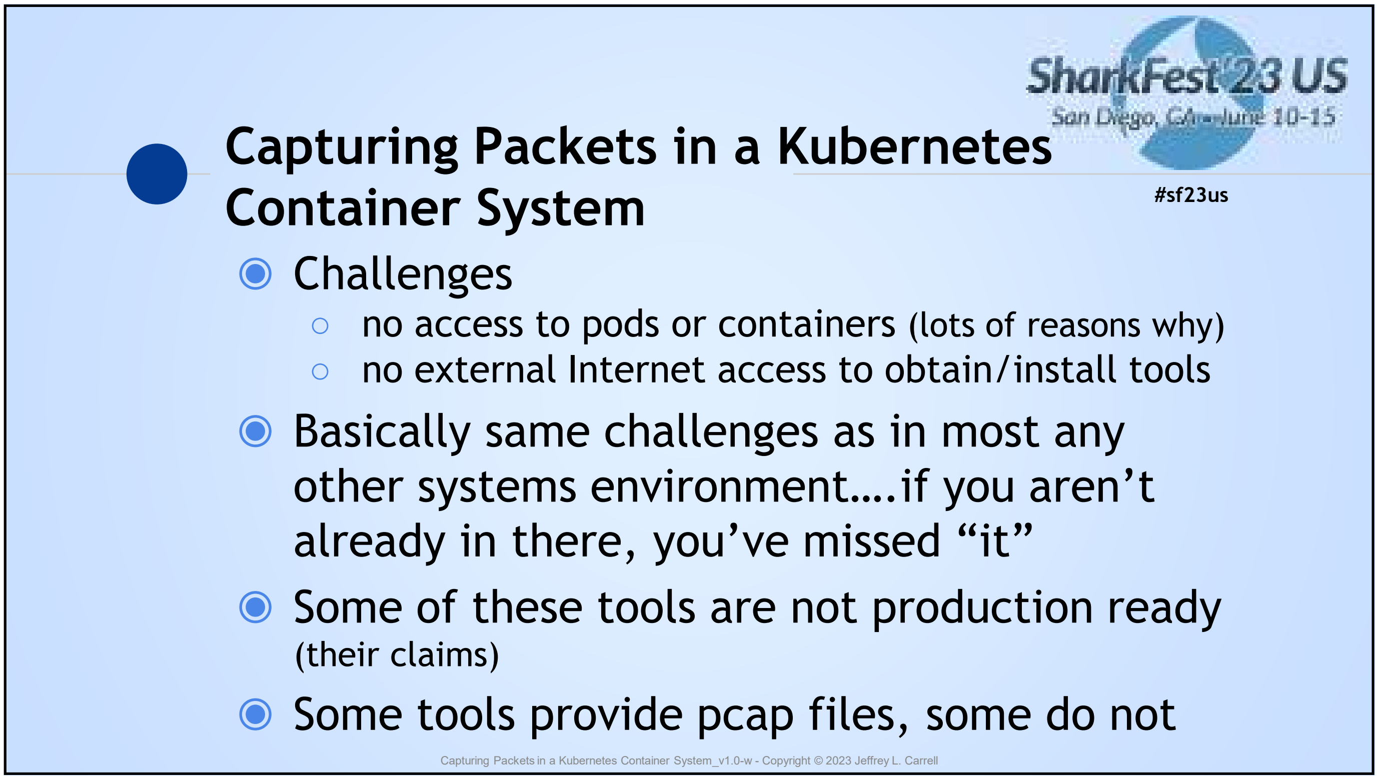


SharkFest'23 US
San Diego, CA - June 10-15

#sf23us

Capturing Packets in a Kubernetes Container System

- High-level overview
- Some products mentioned/demonstrated
  - no endorsements at all
- This is not:
  - Wireshark training
  - Kubernetes training
  - Gazillions of resources available on the above topics

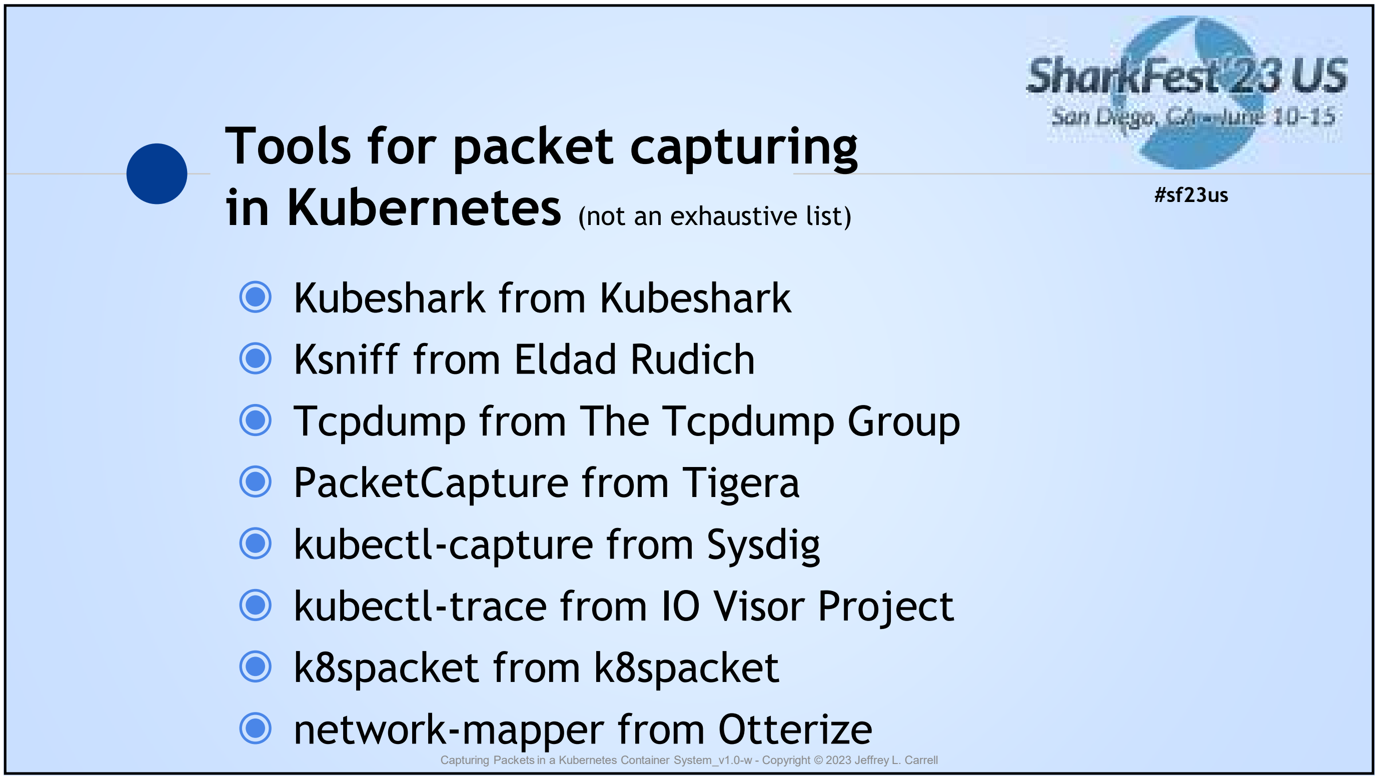


SharkFest'23 US
San Diego, CA - June 10-15

#sf23us

Capturing Packets in a Kubernetes Container System

- Challenges
  - no access to pods or containers (lots of reasons why)
  - no external Internet access to obtain/install tools
- Basically same challenges as in most any other systems environment….if you aren't already in there, you've missed "it"
- Some of these tools are not production ready (their claims)
- Some tools provide pcap files, some do not

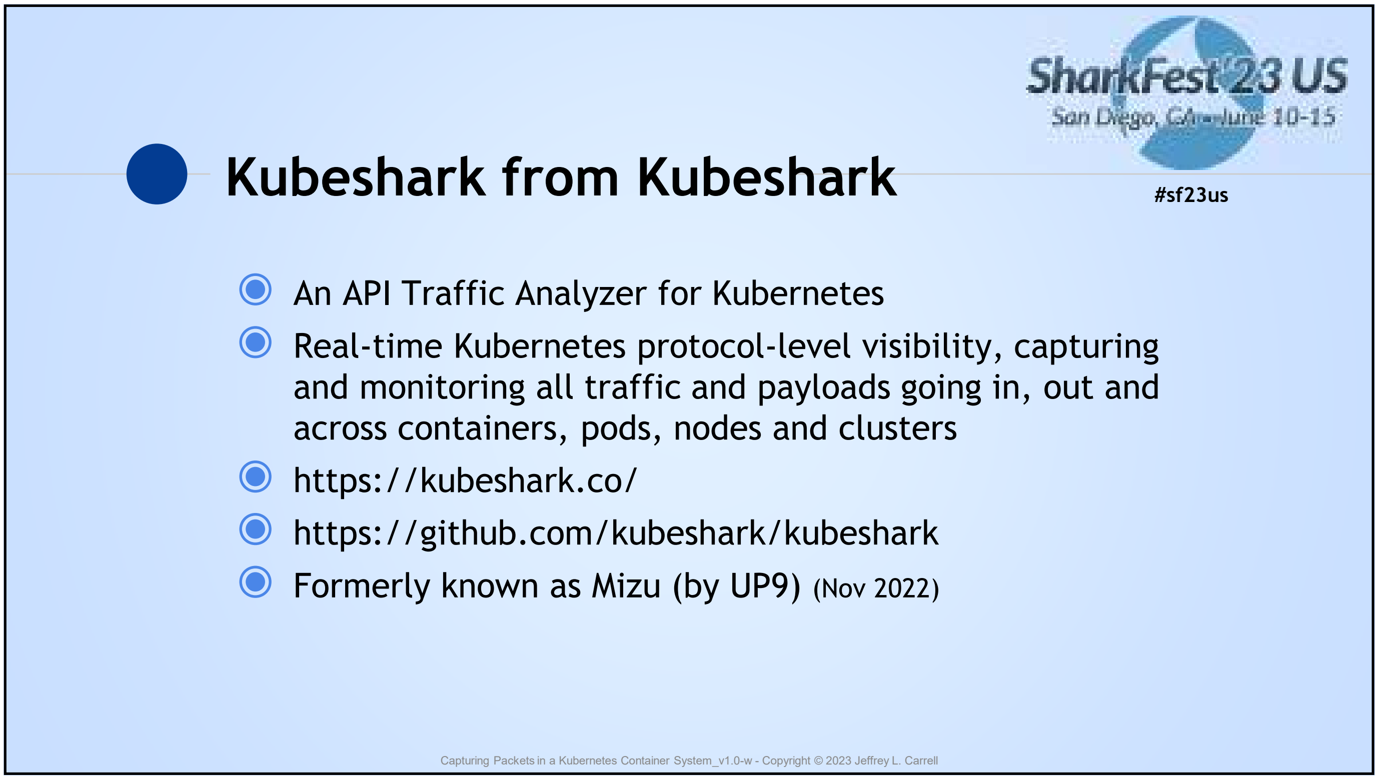


SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

Tools for packet capturing in Kubernetes (not an exhaustive list)

- Kubeshark from Kubeshark
- Ksniff from Eldad Rudich
- Tcpdump from The Tcpdump Group
- PacketCapture from Tigera
- kubectl-capture from Sysdig
- kubectl-trace from IO Visor Project
- k8spacket from k8spacket
- network-mapper from Otterize

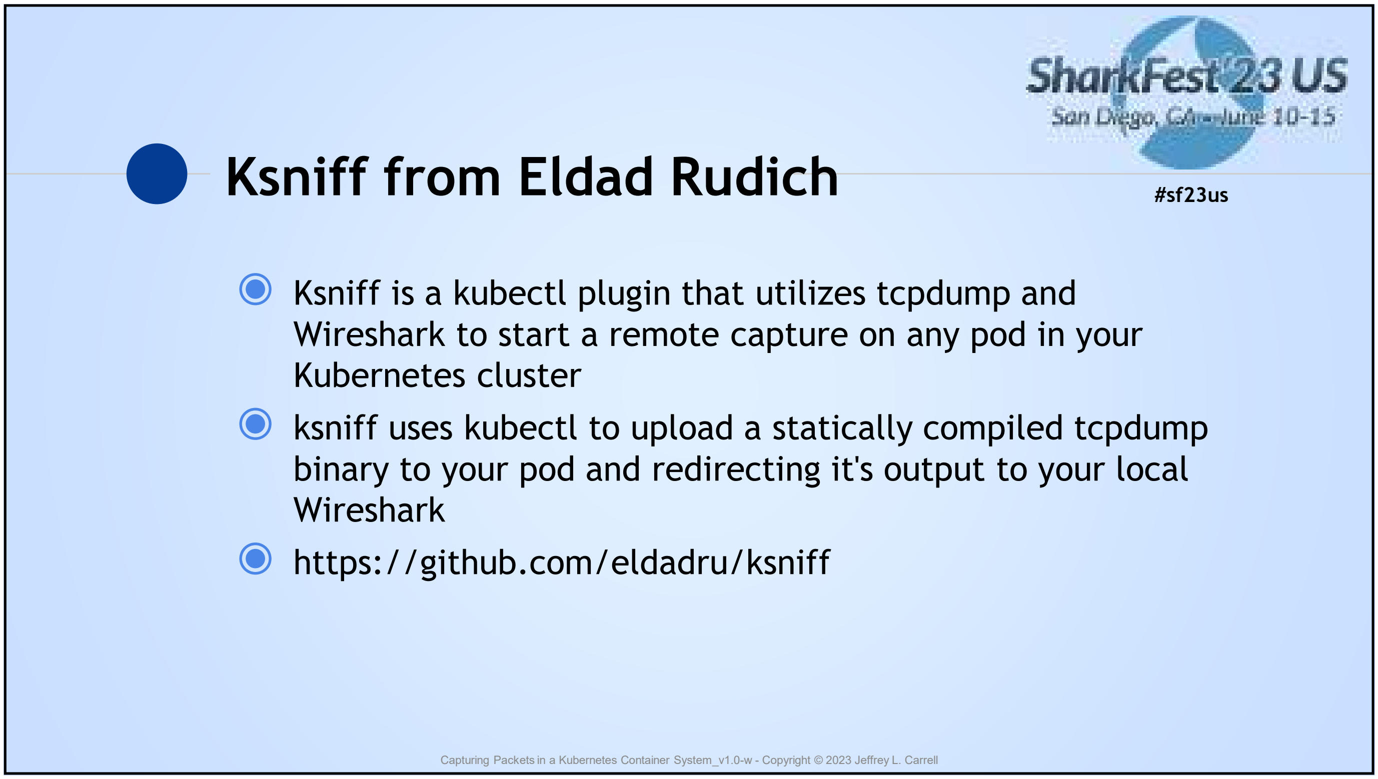


SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

Kubeshark from Kubeshark

- An API Traffic Analyzer for Kubernetes
- Real-time Kubernetes protocol-level visibility, capturing and monitoring all traffic and payloads going in, out and across containers, pods, nodes and clusters
- https://kubeshark.co/
- https://github.com/kubeshark/kubeshark
- Formerly known as Mizu (by UP9) (Nov 2022)

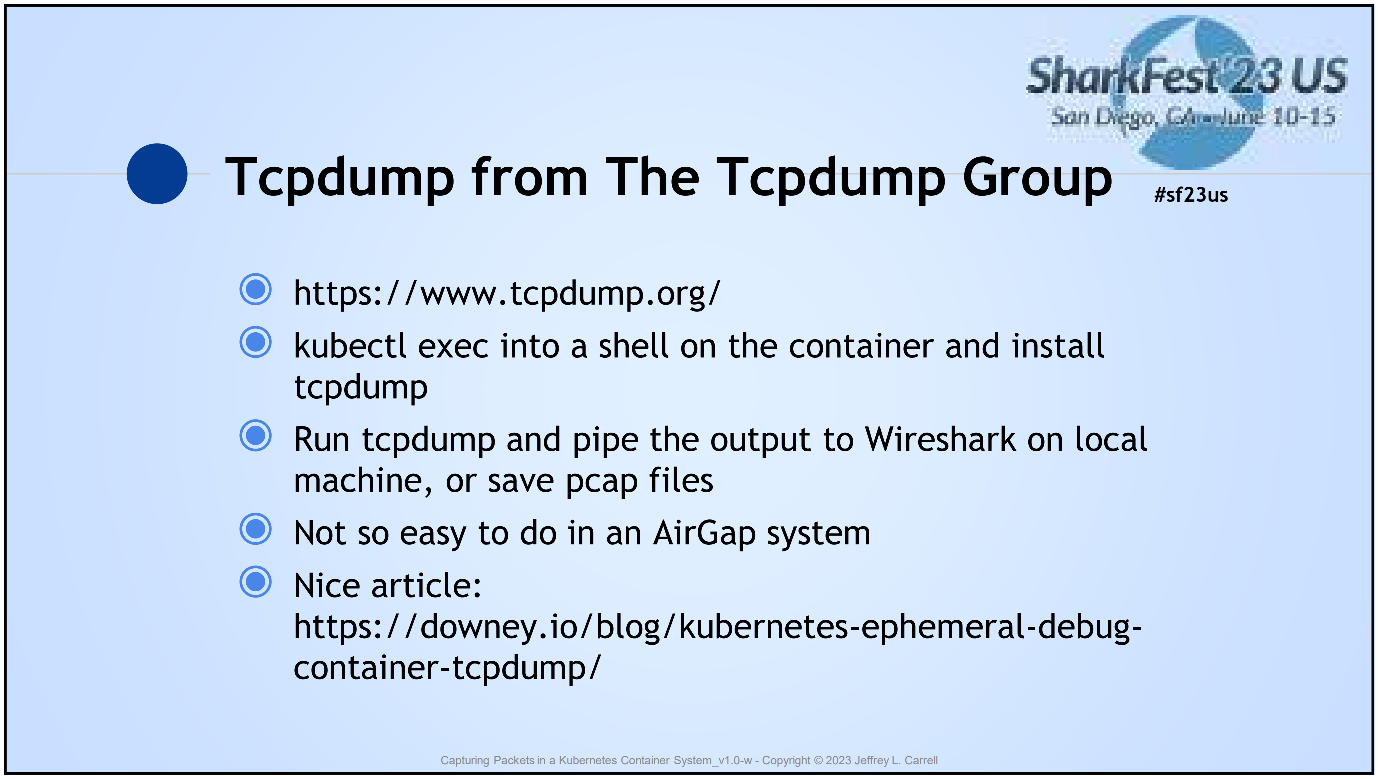


Ksniff from Eldad Rudich

#sf23us

- Ksniff is a kubectl plugin that utilizes tcpdump and Wireshark to start a remote capture on any pod in your Kubernetes cluster
- ksniff uses kubectl to upload a statically compiled tcpdump binary to your pod and redirecting it's output to your local Wireshark
- https://github.com/eldadru/ksniff

Capturing Packets in a Kubernetes Container System_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

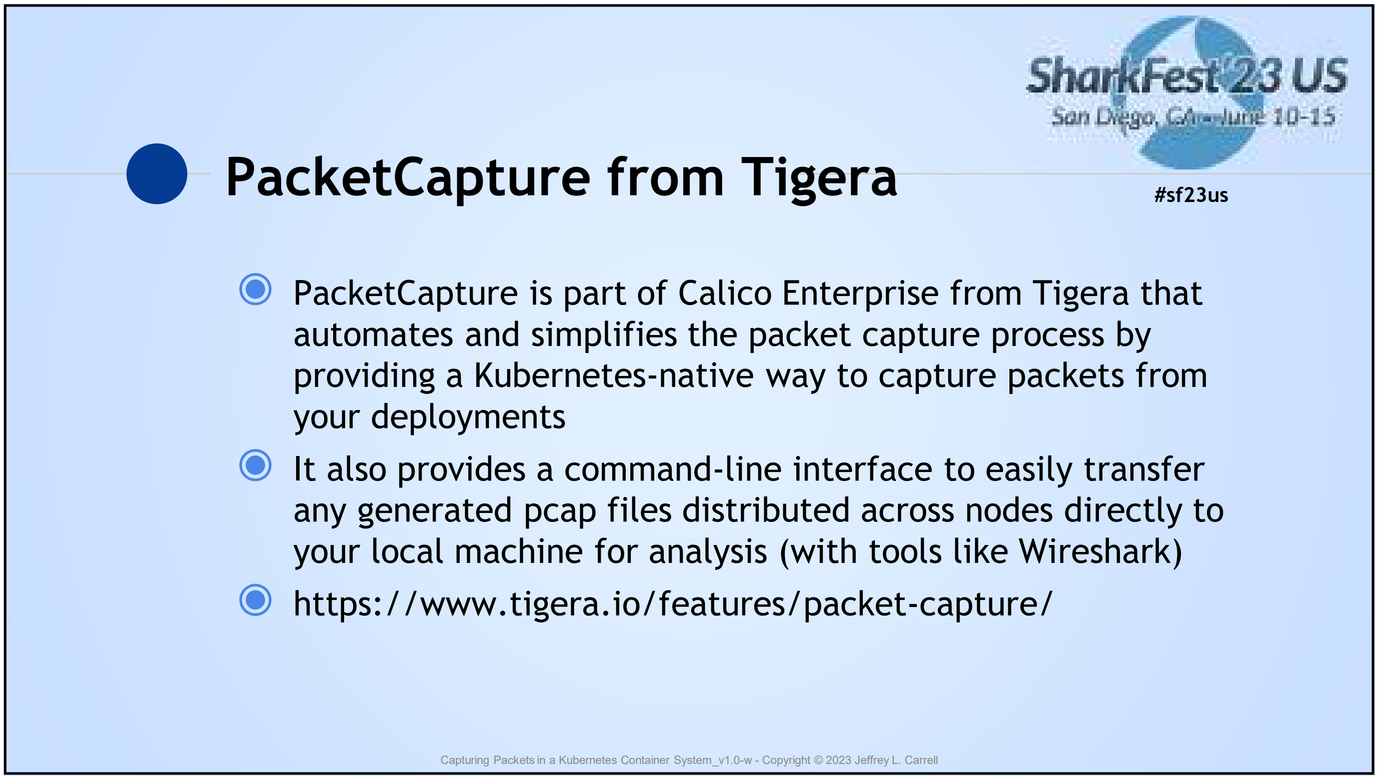


Tcpdump from The Tcpdump Group

#sf23us

- https://www.tcpdump.org/
- kubectl exec into a shell on the container and install tcpdump
- Run tcpdump and pipe the output to Wireshark on local machine, or save pcap files
- Not so easy to do in an AirGap system
- Nice article: https://downey.io/blog/kubernetes-ephemeral-debug-container-tcpdump/

Capturing Packets in a Kubernetes Container System_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

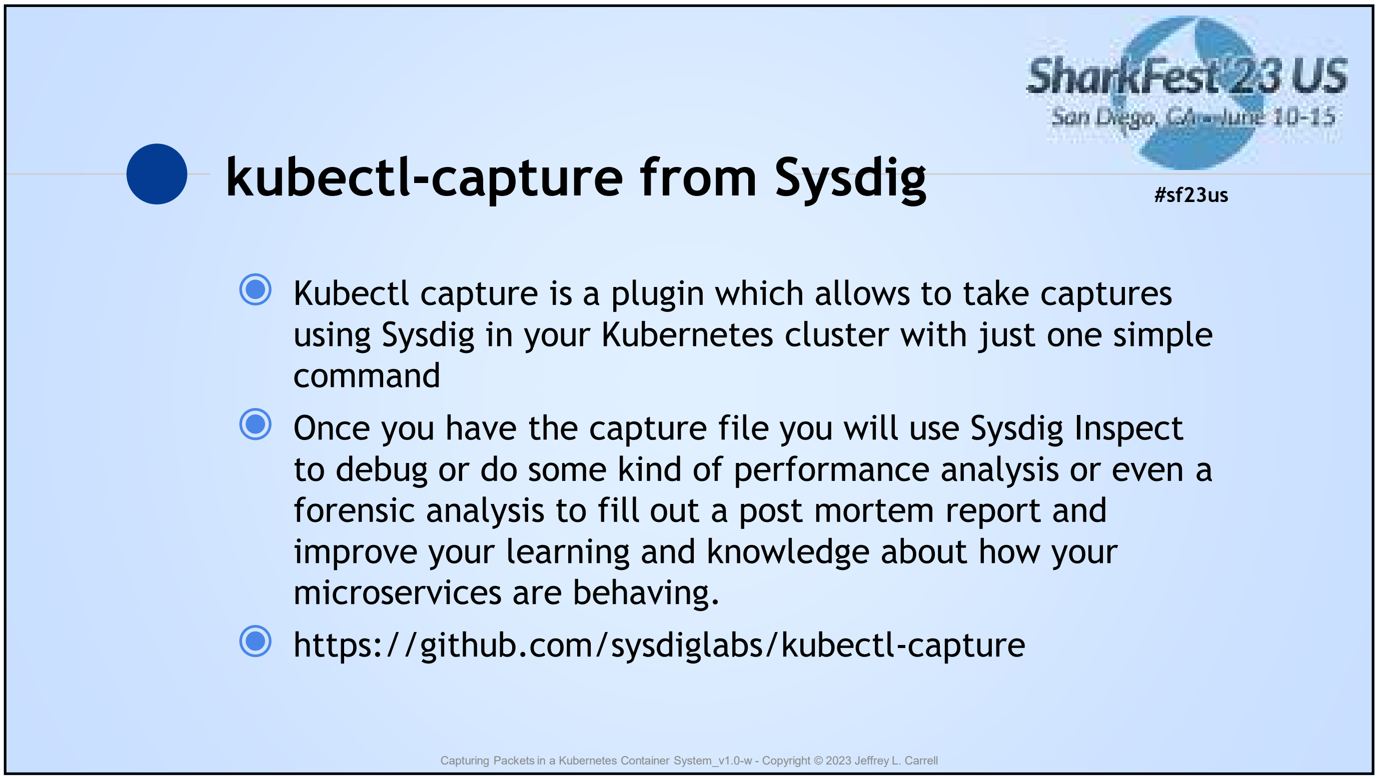


SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

PacketCapture from Tigera

- PacketCapture is part of Calico Enterprise from Tigera that automates and simplifies the packet capture process by providing a Kubernetes-native way to capture packets from your deployments
- It also provides a command-line interface to easily transfer any generated pcap files distributed across nodes directly to your local machine for analysis (with tools like Wireshark)
- https://www.tigera.io/features/packet-capture/

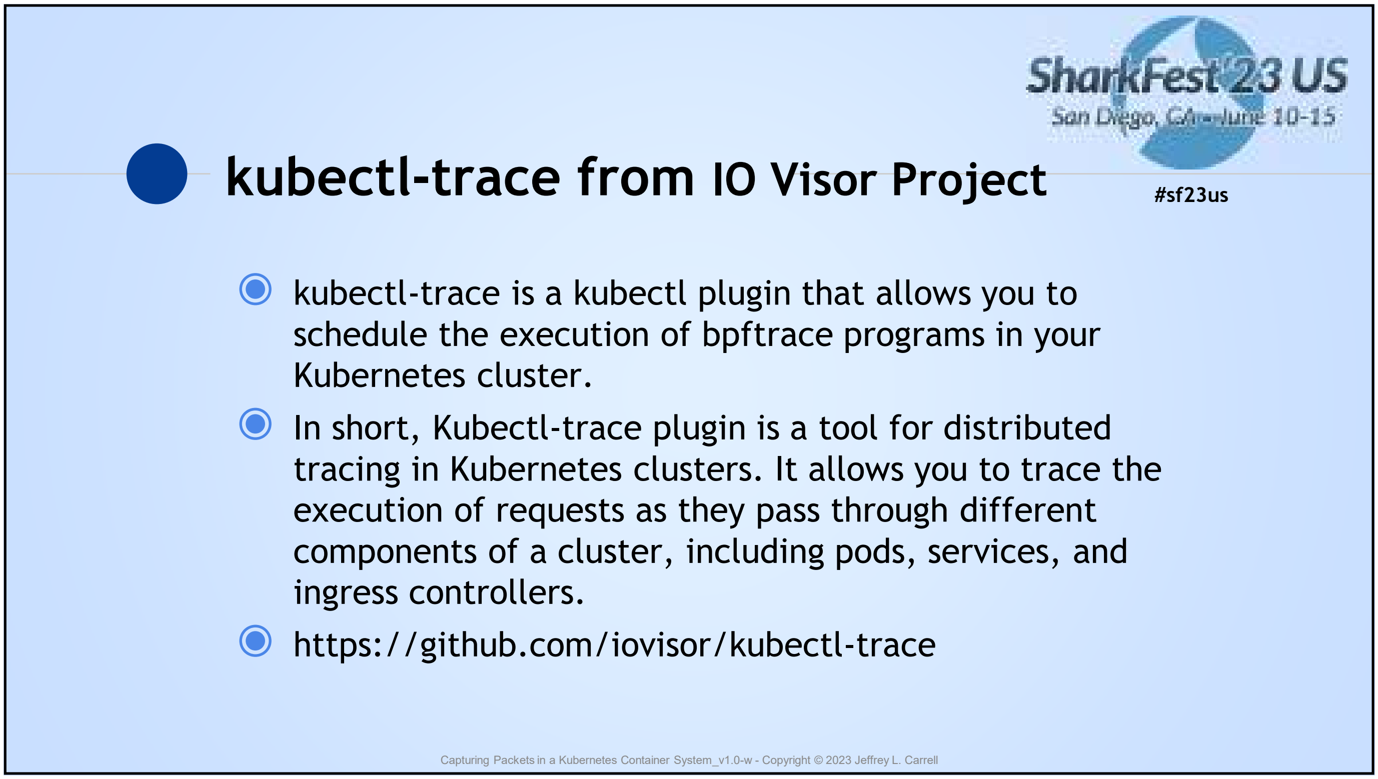


SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

kubectl-capture from Sysdig

- Kubectl capture is a plugin which allows to take captures using Sysdig in your Kubernetes cluster with just one simple command
- Once you have the capture file you will use Sysdig Inspect to debug or do some kind of performance analysis or even a forensic analysis to fill out a post mortem report and improve your learning and knowledge about how your microservices are behaving.
- https://github.com/sysdiglabs/kubectl-capture

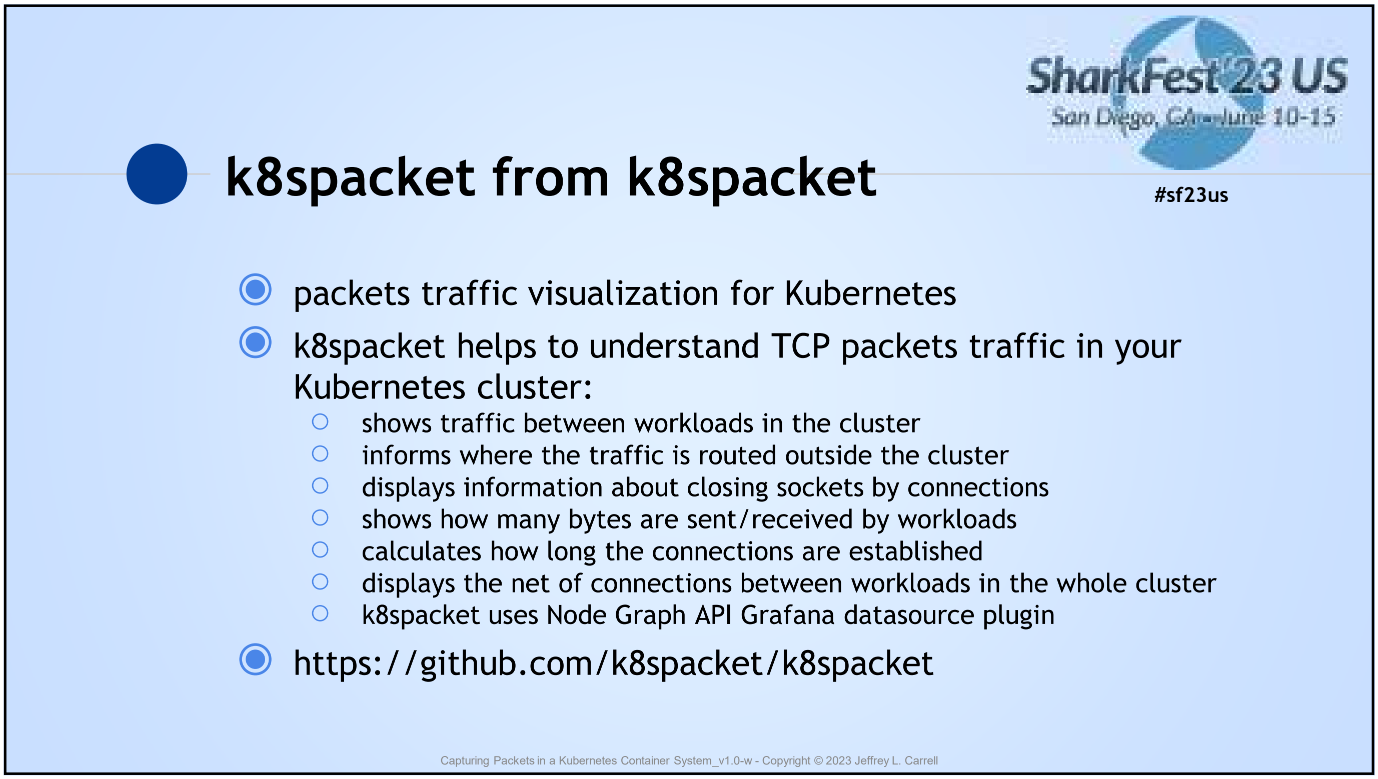


SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

kubectl-trace from IO Visor Project

- kubectl-trace is a kubectl plugin that allows you to schedule the execution of bpftrace programs in your Kubernetes cluster.
- In short, Kubectl-trace plugin is a tool for distributed tracing in Kubernetes clusters. It allows you to trace the execution of requests as they pass through different components of a cluster, including pods, services, and ingress controllers.
- https://github.com/iovisor/kubectl-trace

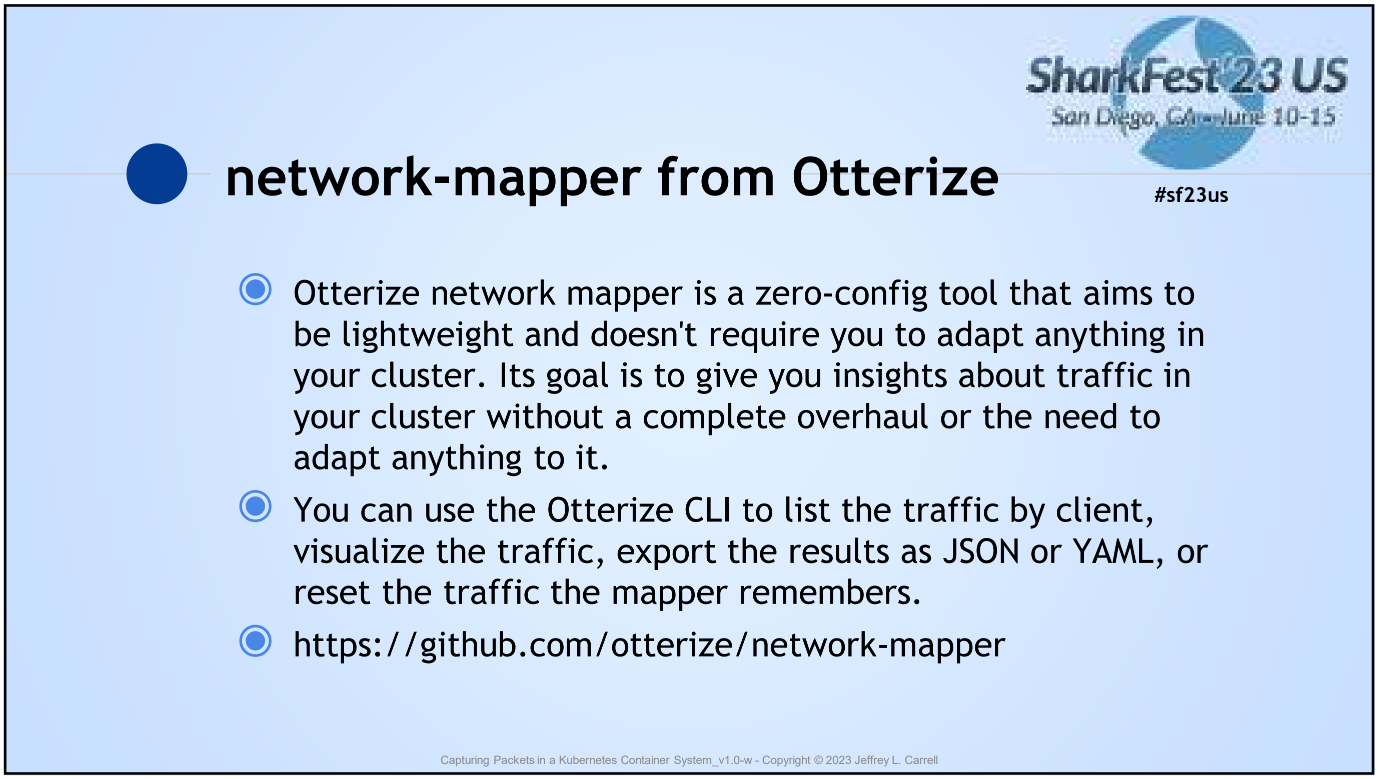


SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

k8spacket from k8spacket

- packets traffic visualization for Kubernetes
- k8spacket helps to understand TCP packets traffic in your Kubernetes cluster:
  - shows traffic between workloads in the cluster
  - informs where the traffic is routed outside the cluster
  - displays information about closing sockets by connections
  - shows how many bytes are sent/received by workloads
  - calculates how long the connections are established
  - displays the net of connections between workloads in the whole cluster
  - k8spacket uses Node Graph API Grafana datasource plugin
- https://github.com/k8spacket/k8spacket

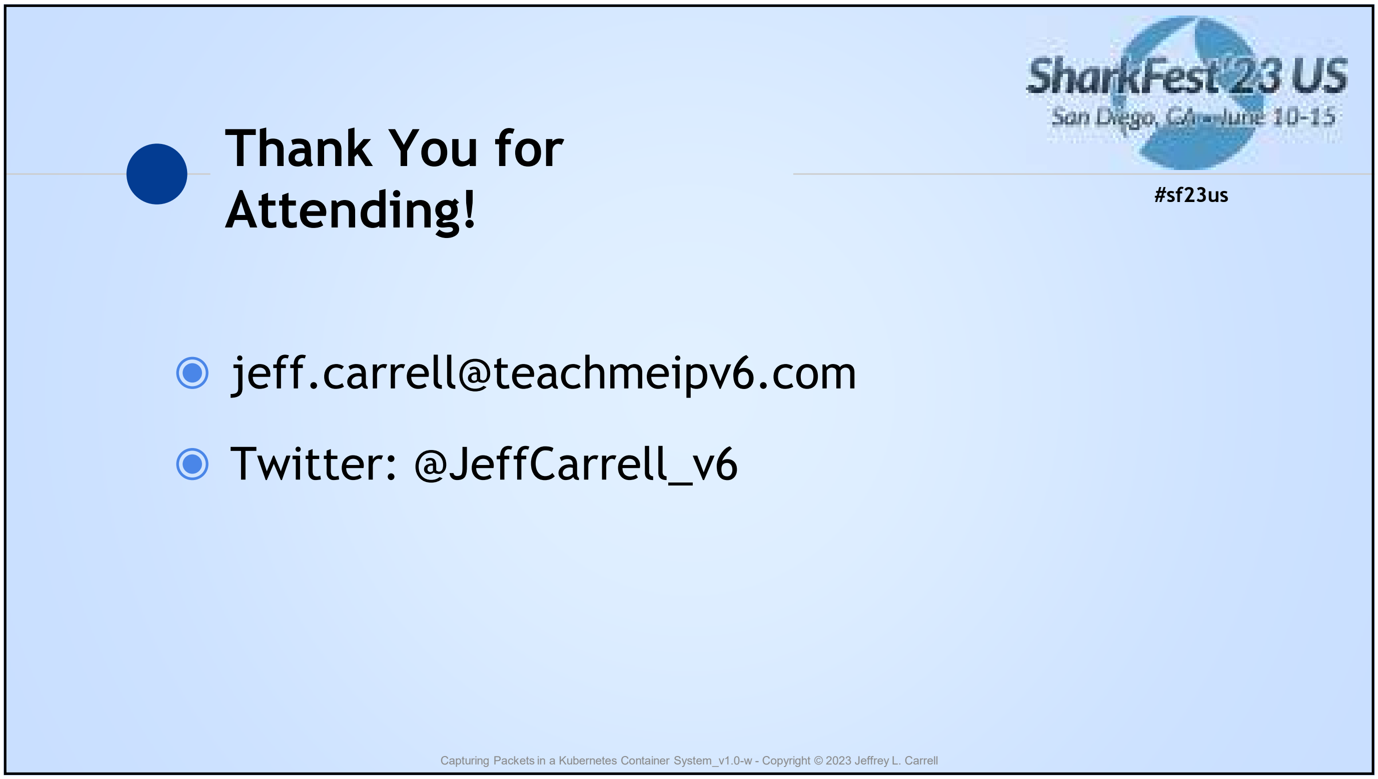


SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

network-mapper from Otterize

- Otterize network mapper is a zero-config tool that aims to be lightweight and doesn't require you to adapt anything in your cluster. Its goal is to give you insights about traffic in your cluster without a complete overhaul or the need to adapt anything to it.
- You can use the Otterize CLI to list the traffic by client, visualize the traffic, export the results as JSON or YAML, or reset the traffic the mapper remembers.
- https://github.com/otterize/network-mapper



SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Thank You for Attending!

- jeff.carrell@teachmeipv6.com
- Twitter: @JeffCarrell_v6