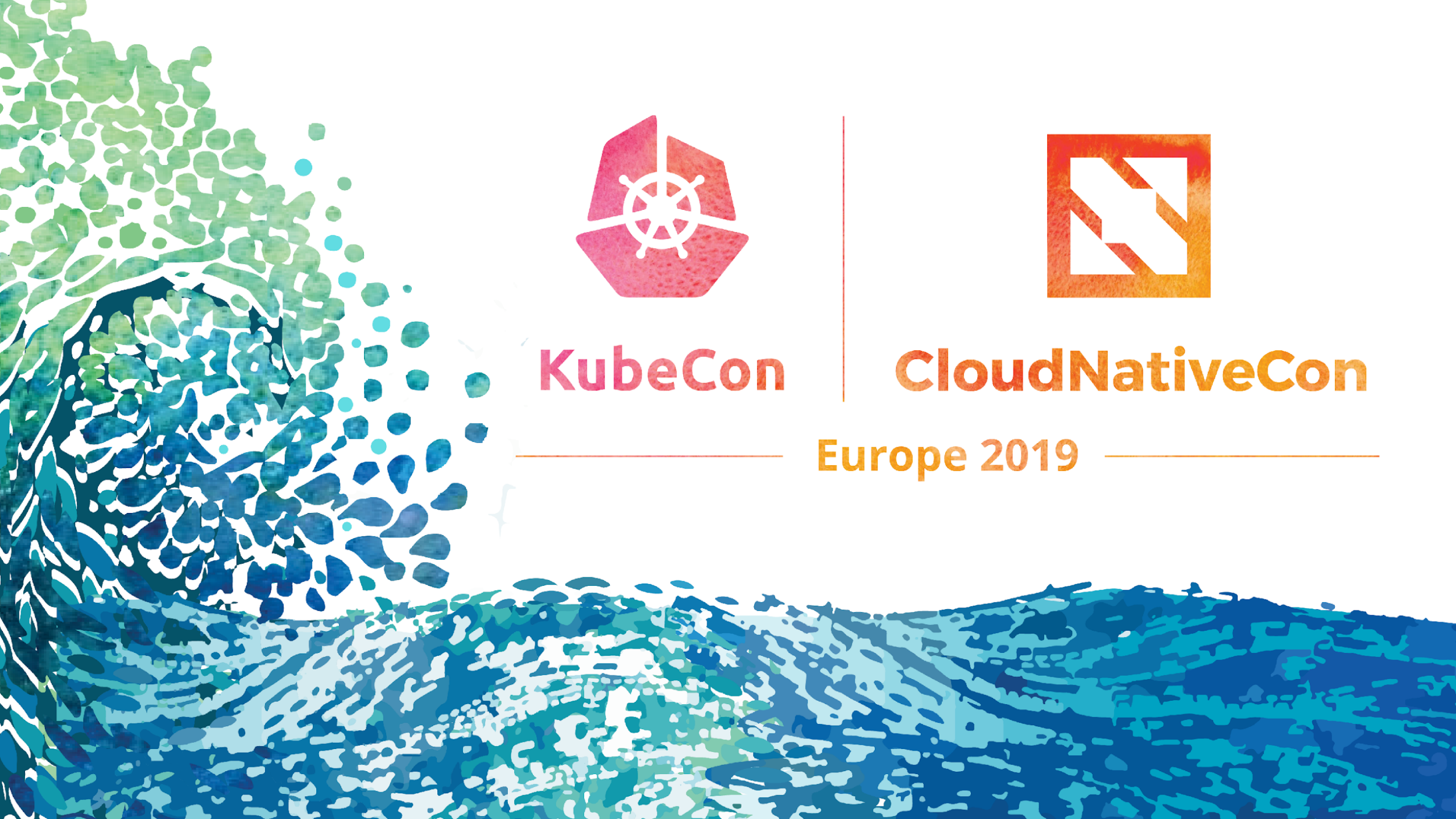
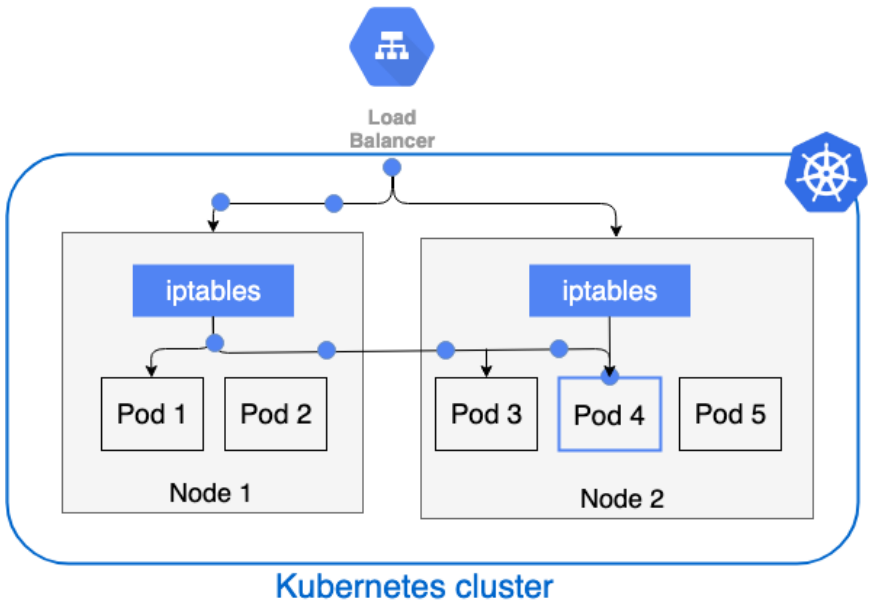
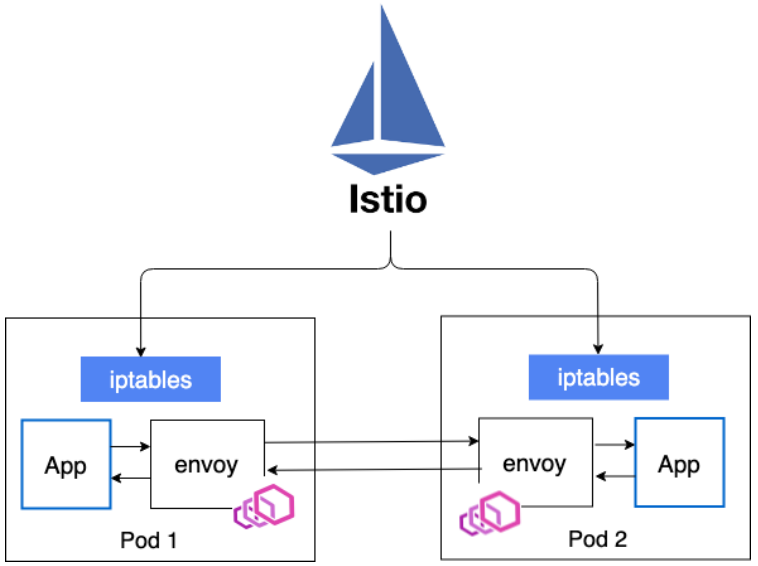

KubeCon
CloudNativeCon
Europe 2019

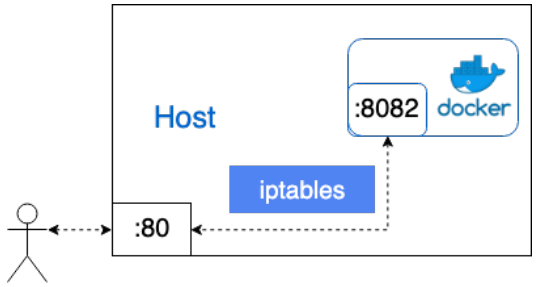
Back to the future with eBPF

@beatrizmrg, Beatriz Martínez Rubio

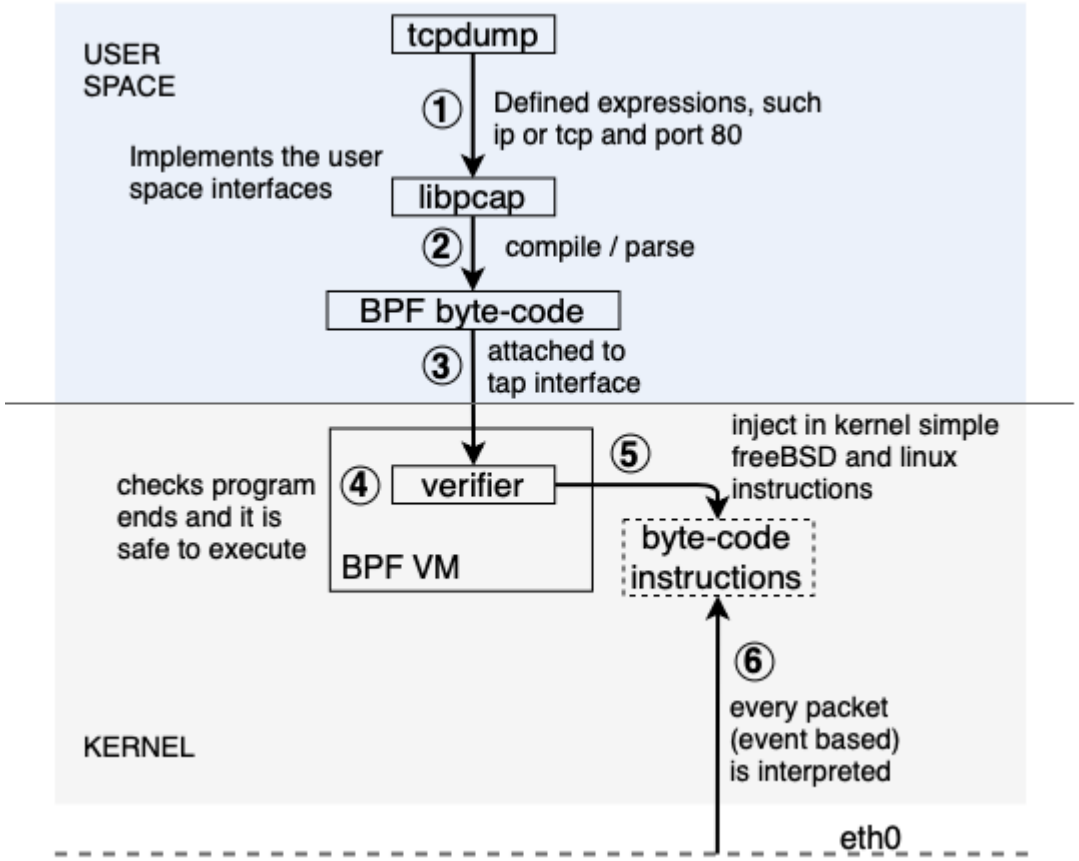
Supporting the Cloud Native World





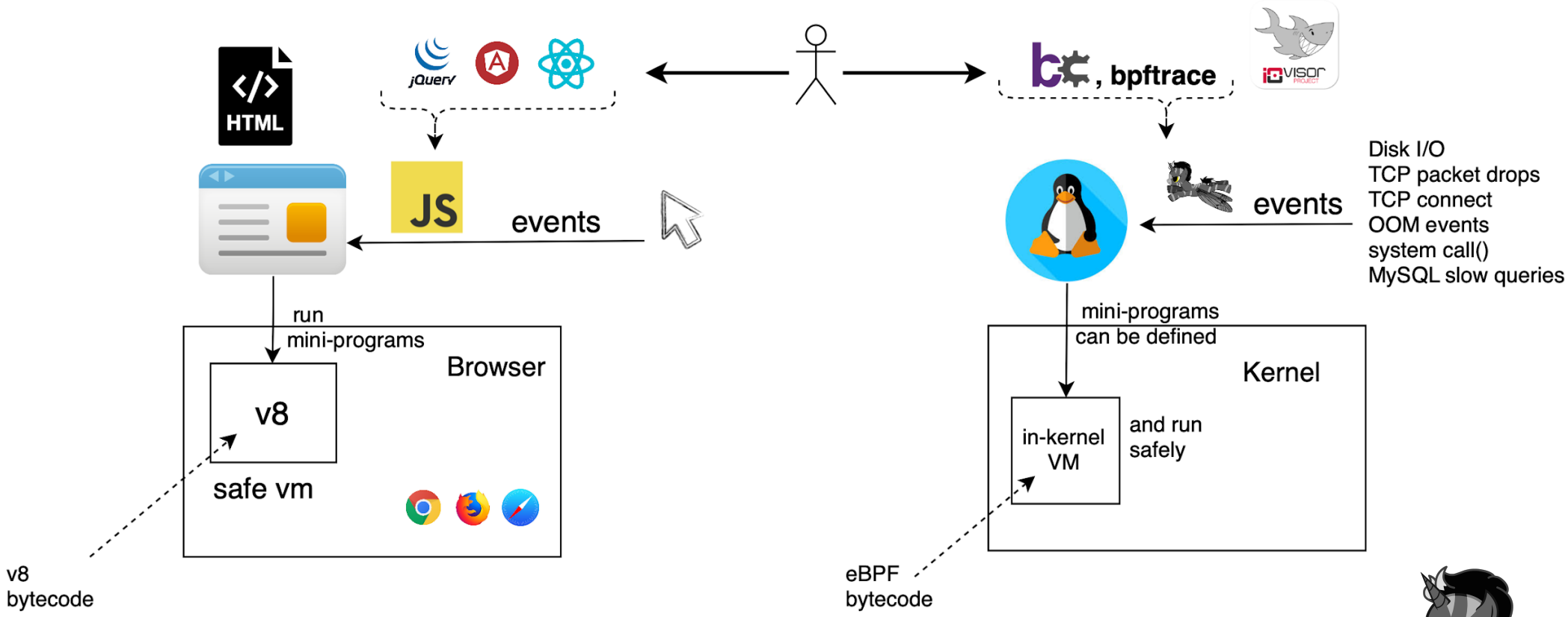


BPF (1992)




```
$ tcpdump -p -ni en0 -d "ip or tcp and port 80"
(000) ldh      [12]
(001) jeq      #0x800           jt 2    jf 12
(002) ldb      [23]
(003) jeq      #0x6             jt 4    jf 12
(004) ldh      [20]
(005) jset     #0x1fff          jt 12   jf 6
(006) ldxb     4*([14]&0xf)
(007) ldh      [x + 14]
(008) jeq      #0x50            jt 11   jf 9
(009) ldh      [x + 16]
(010) jeq      #0x50            jt 11   jf 12
(011) ret      #262144
(012) ret      #0
```

eBPF: dynamic Linux kernel



Inspired on Brendan Gregg's Blog example

Writing eBPF programs


```
#define ETH_LEN 14


struct dns_hdr_t
{
   uint16_t id;
   uint16_t flags;
   uint16_t qdcount;
   uint16_t ancount;
   uint16_t nscount;
   uint16_t arcount;
} BPF_PACKET_HEADER;


struct dns_query_flags_t
{
 uint16_t qtype;
 uint16_t qclass;
} BPF_PACKET_HEADER;
```

BPF bytecode	Brutal
C	Hard
perf	Hard
bcc	Moderate
bpftrace	Easy
ply	Easy

```
(000) ldh      [12]
(001) jeq      #0x800
jt 2    jf 5
(002) ldb      [23]
(003) jeq      #0x11
jt 4    jf 5
(004) ret      #65535
(005) ret      #0
```

Used in prod:
Netflix, Facebook

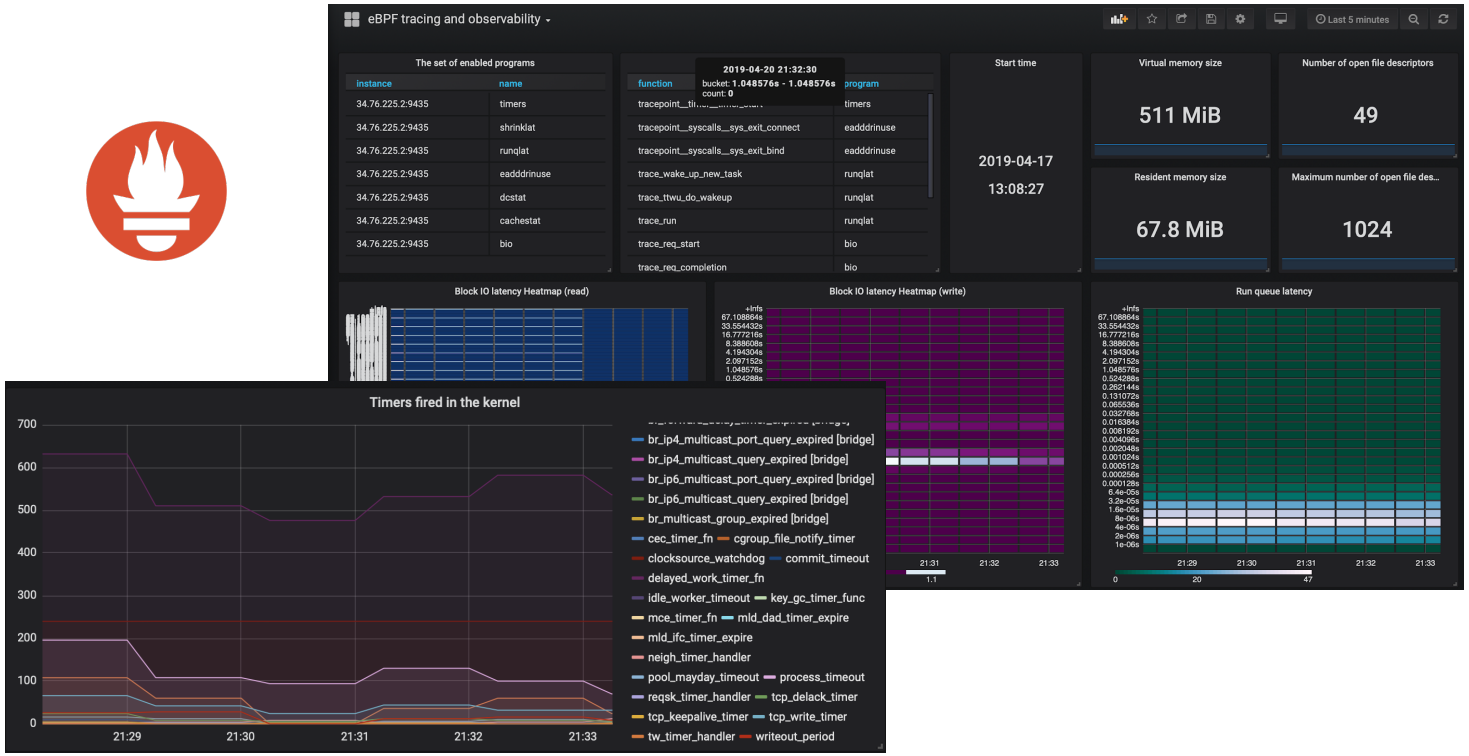
one-liners

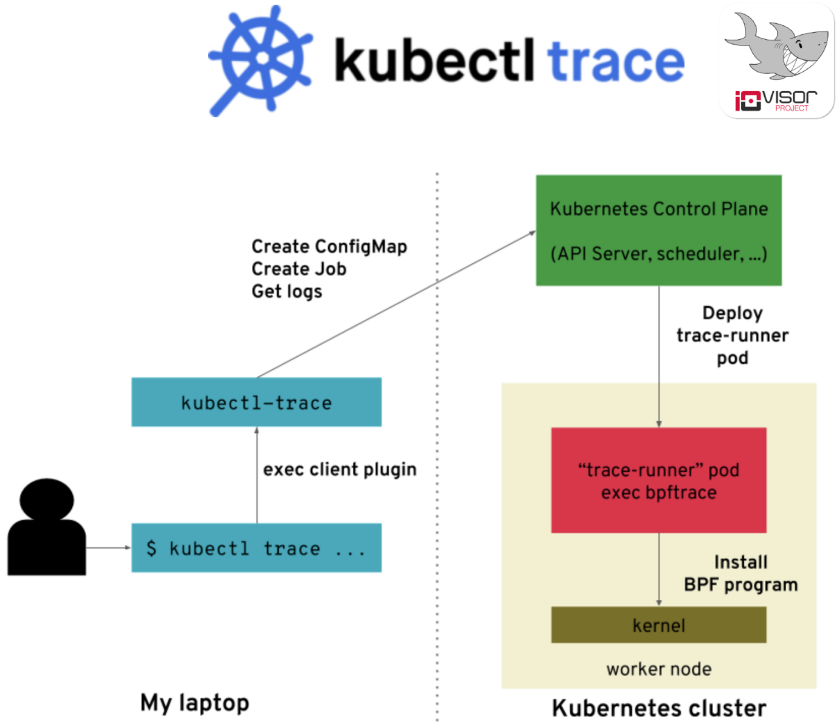
Syscall counts by process

```
bpftrace -e 'tracepoint:raw_syscalls:sys_enter { @[comm] = count(); }'
```

Testing eBPF

ebpf-exporter (bcc)





https://github.com/zoidbergwill/awesome-ebpf

Work in progress

Cilium
@ciliumproject
Following

Great photo from @brendangregg during the eBPF conference

Engineers from Cilium, Cloudflare, Google (Project Zero), Facebook, Netflix, Netronome and Redhat are discussing the future of eBPF.

12:48 PM - 2 May 2019

Linux Kernel Developers' bpfconf 2019

bpfconf is an invitation-only technical workshop run by the Linux community in order to bring BPF core developers together, to discuss new ideas and to work out improvements to the Linux BPF subsystem that will make their way into future mainline kernels and into the LLVM BPF backend.

Andrii Nakryiko
@anakryiko
Seguir

Future of BPF application development: no more 10s of MBs of LLVM/Clang deployed w/ application, no more kernel headers, no more compiling BPF program on production servers. Just "Compile Once and Run Everywhere" (BPF CO-RE): vger.kernel.org/bpfconf2019.ht…

Real world examples

Use cases:

- Networking
- Firewalls
- Security
- Tracing
- Device Drivers

Netflix
Performance profiling and tracing

Facebook
eBPF-based load balancer with DDoS

Sysdig
eBPF instrumentation for high performance system calls tracing

Cloudflare
DDoS and Observability

Weaveworks
Trace TCP events

Cilium
Powerful and efficient networking, security and load-balancing at L3-L7.

AWS Firecracker
Using Seccomp BPF to restrict system calls.

Redhat
RHEL 7.6 enables extended eBPF in-kernel VM

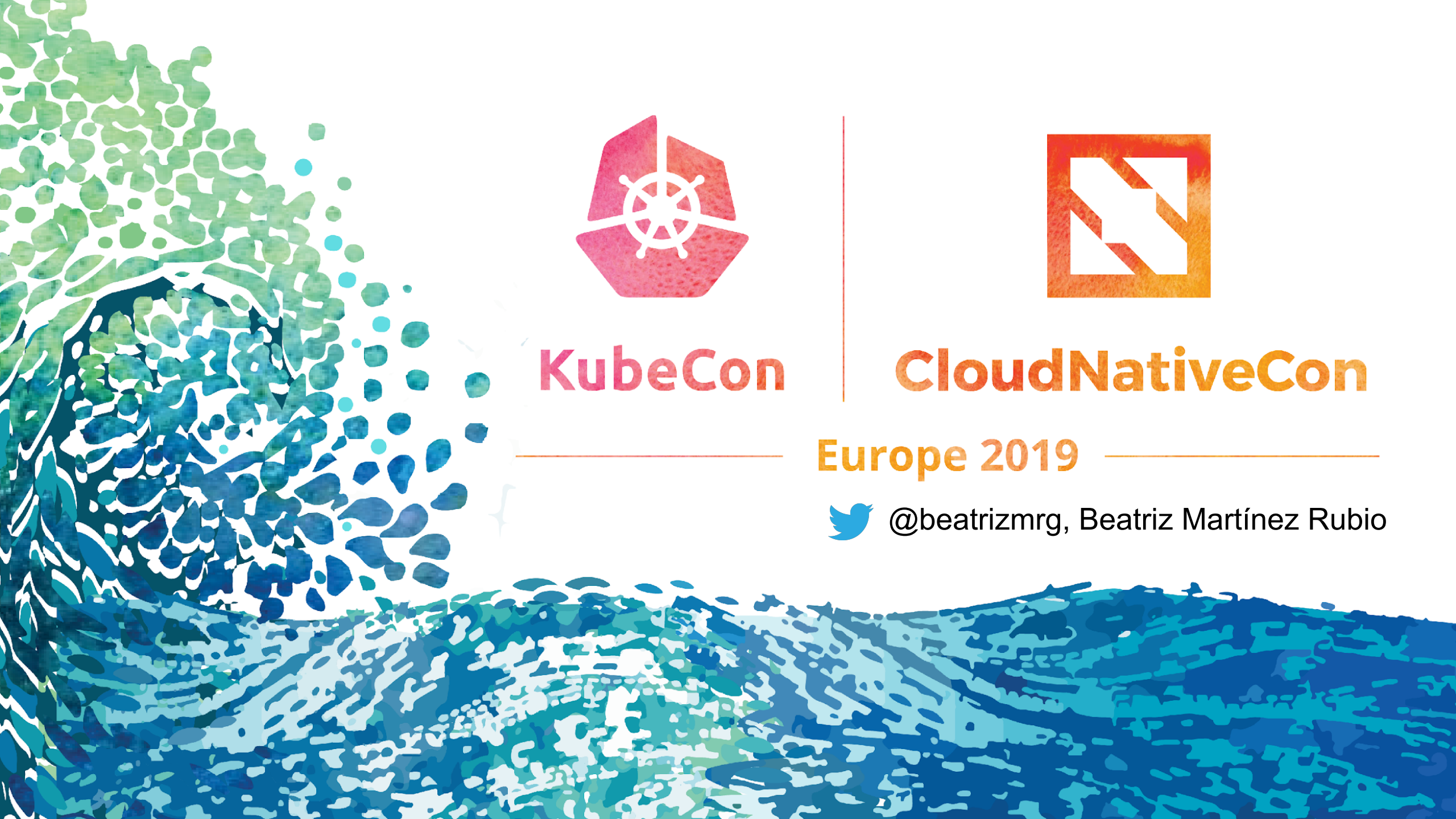
Thank you!

https://github.com/iovisor

@beatrizmrg

@beatrizmrg

Network Security for microservices with ebpf


KubeCon
CloudNativeCon
Europe 2019
@beatrizmrg, Beatriz Martínez Rubio