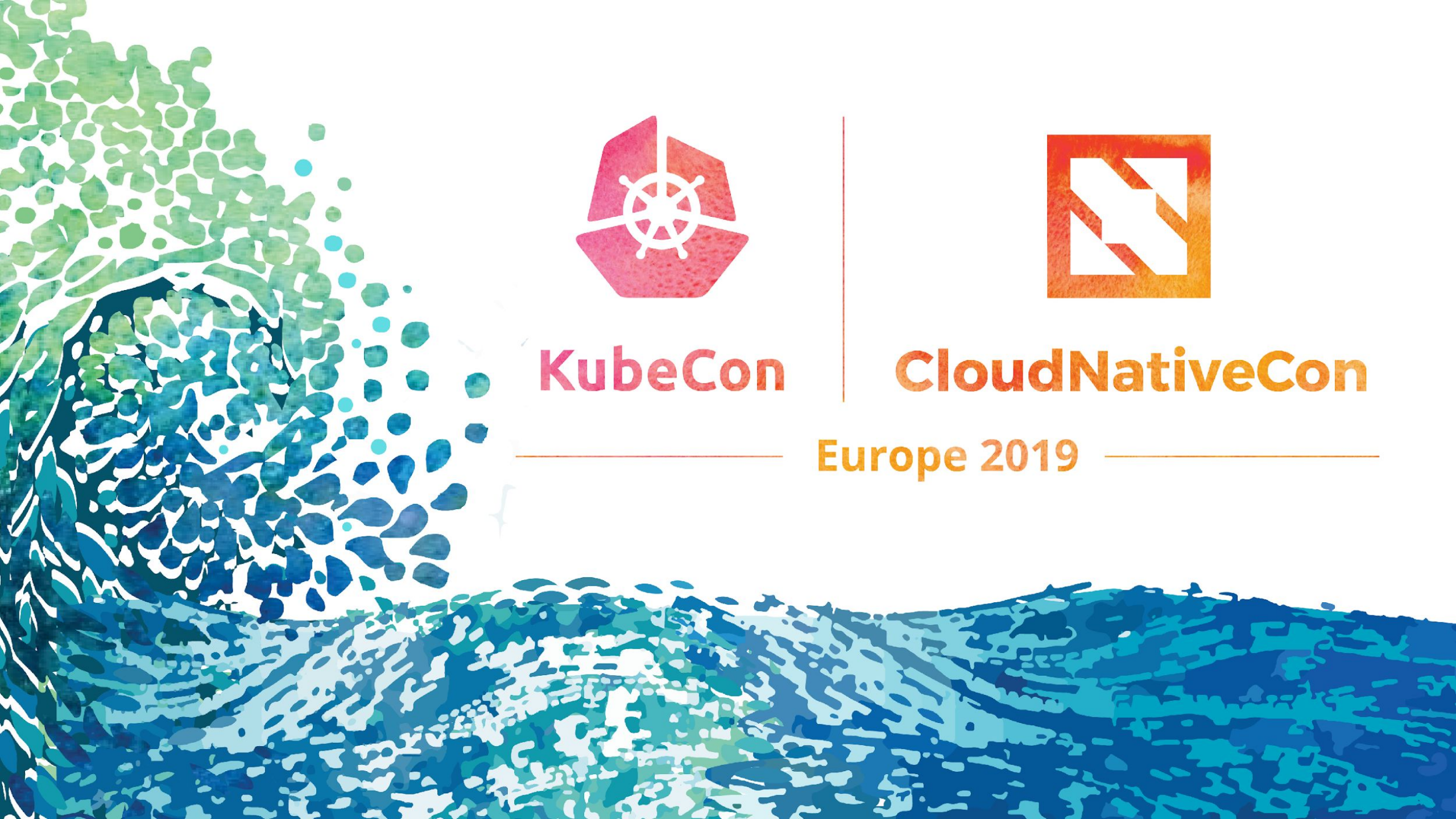
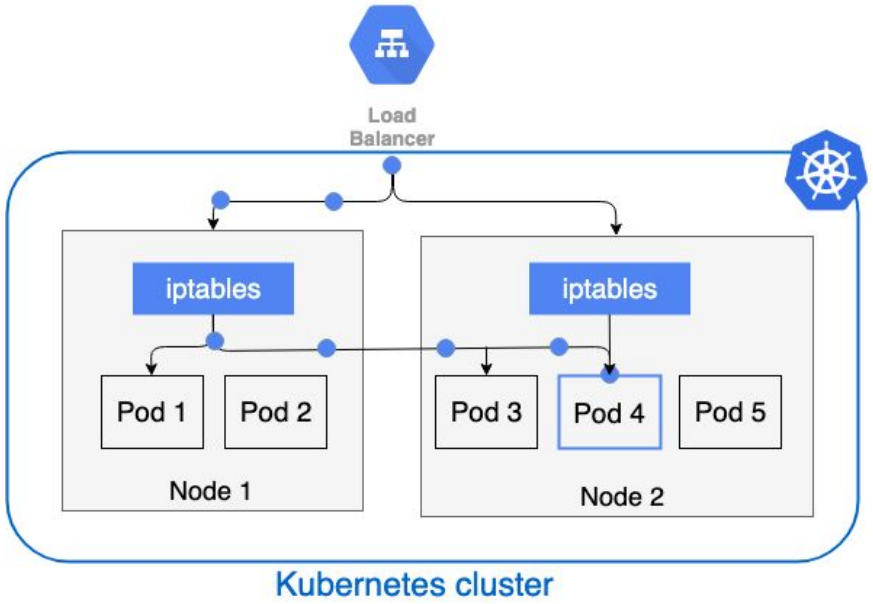

KubeCon
CloudNativeCon
Europe 2019

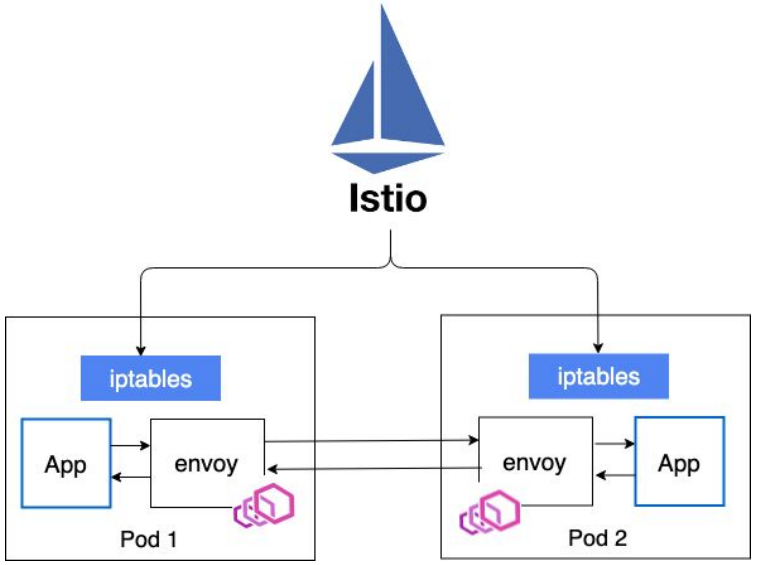
KubeCon | CloudNativeCon Europe 2019

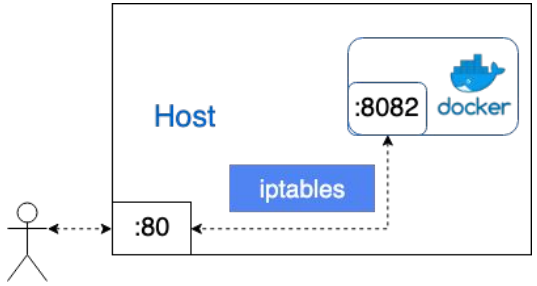
Back to the future with eBPF

@beatrizmrg, Beatriz Martínez Rubio

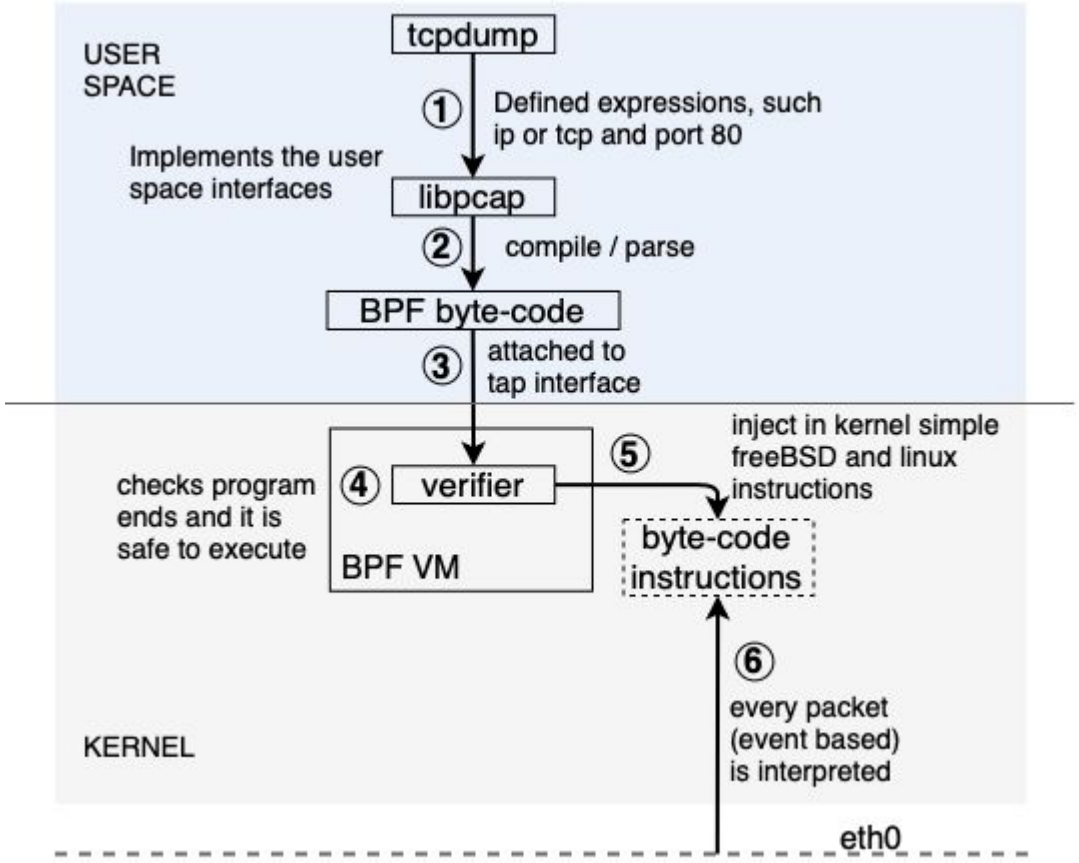
Supporting the Cloud Native World





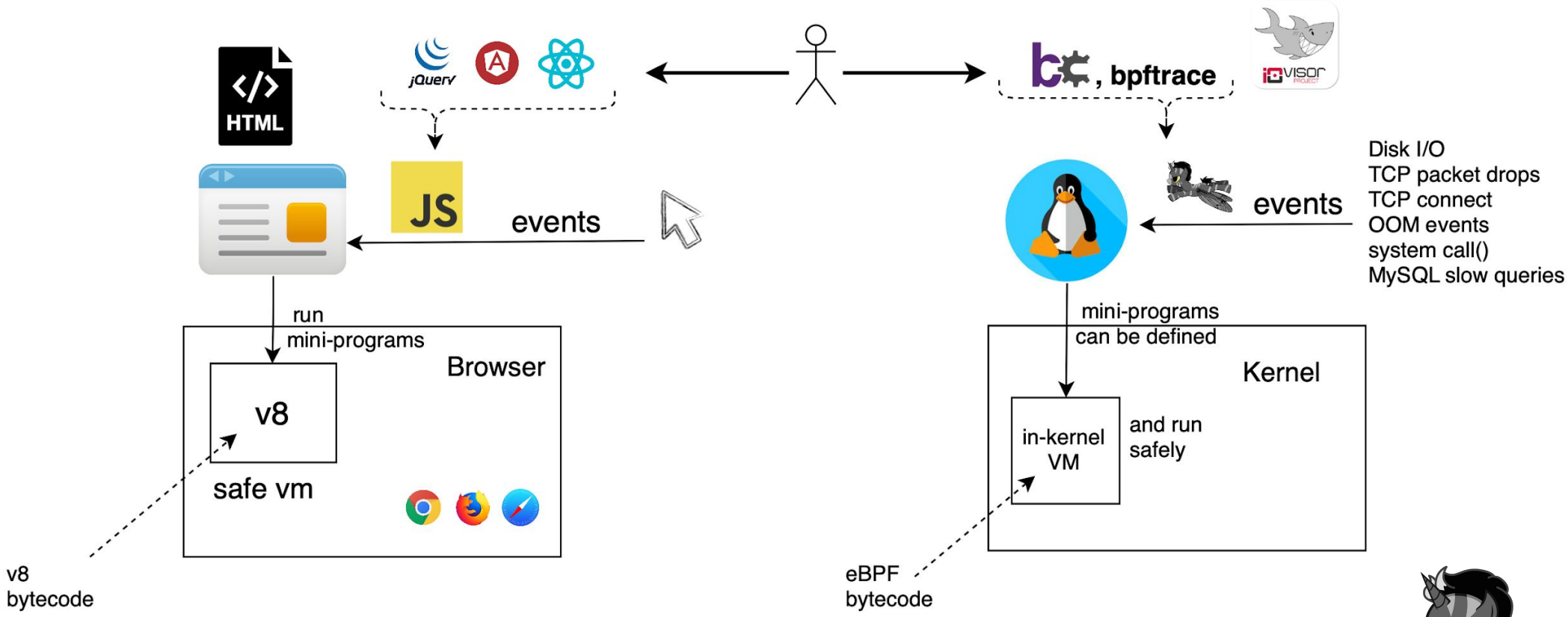


BPF (1992)




```
$ 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;
```

```
(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
```

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

Used in prod:
Netflix, Facebook

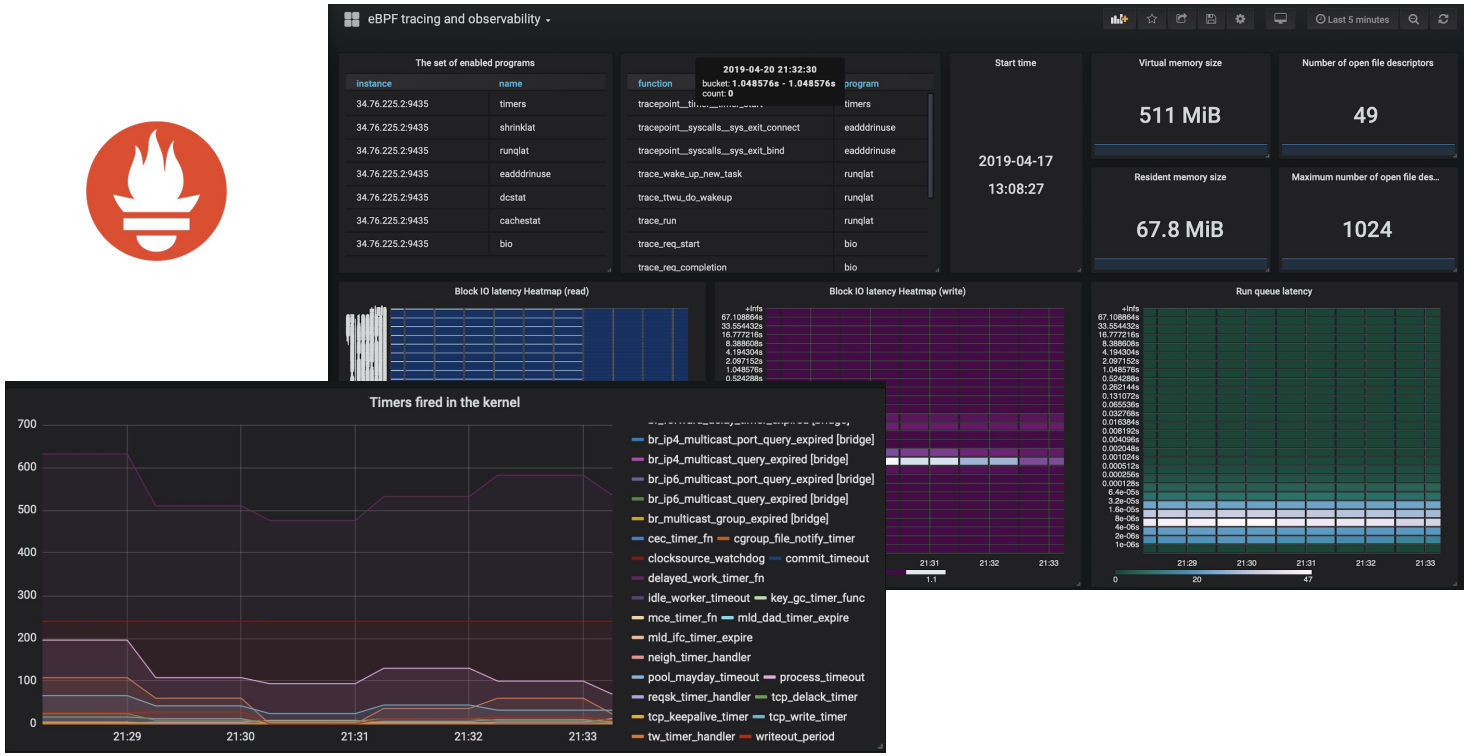
one-liners

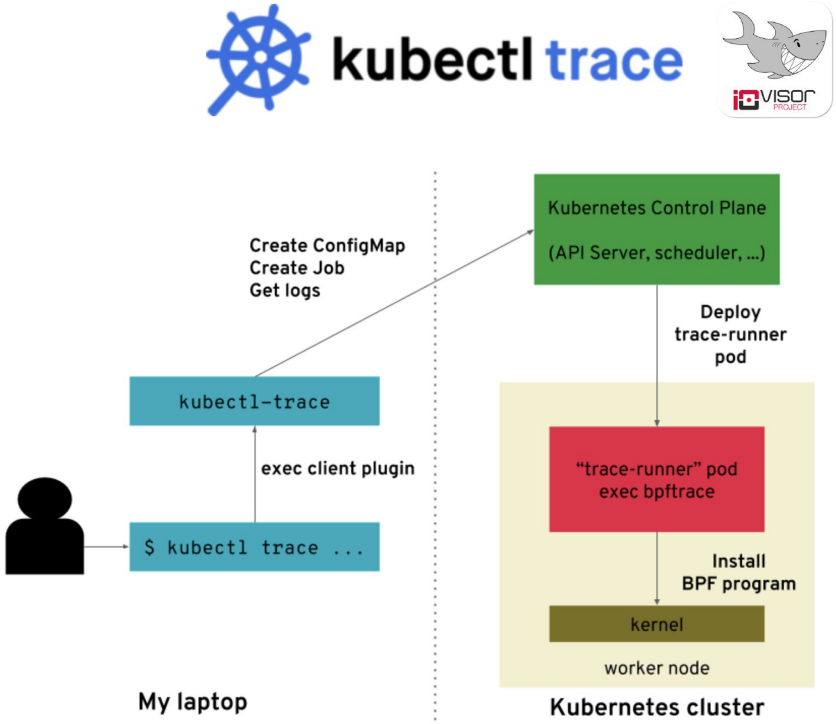
Syscall counts by process

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

Testing eBPF

ebpf-exporter (bcc)





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

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

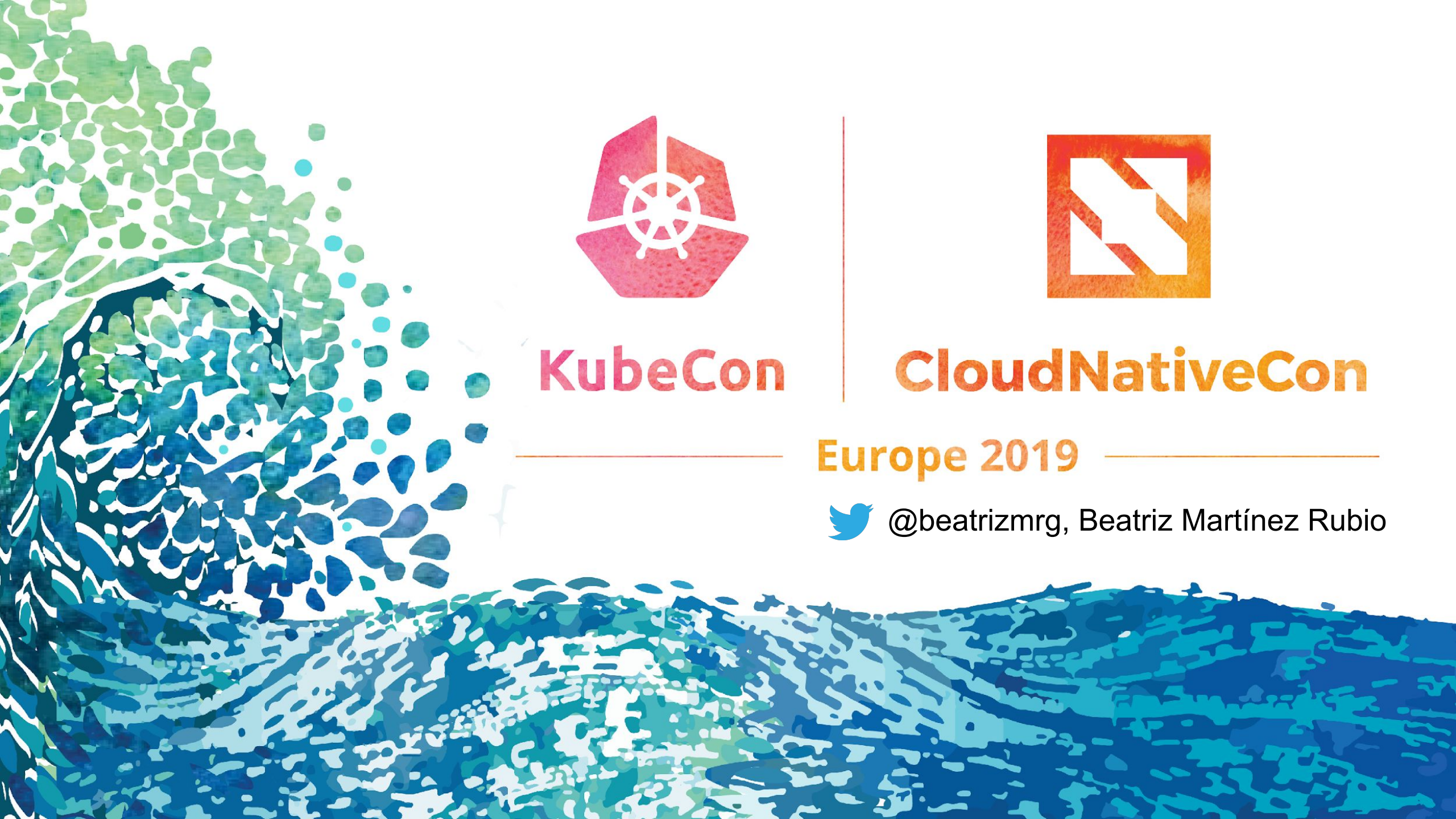
Cloudflare
DDoS and Observability

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



@beatrizmrg, Beatriz Martínez Rubio