The Dark Art of Container Monitoring

Gianluca Borello

Me

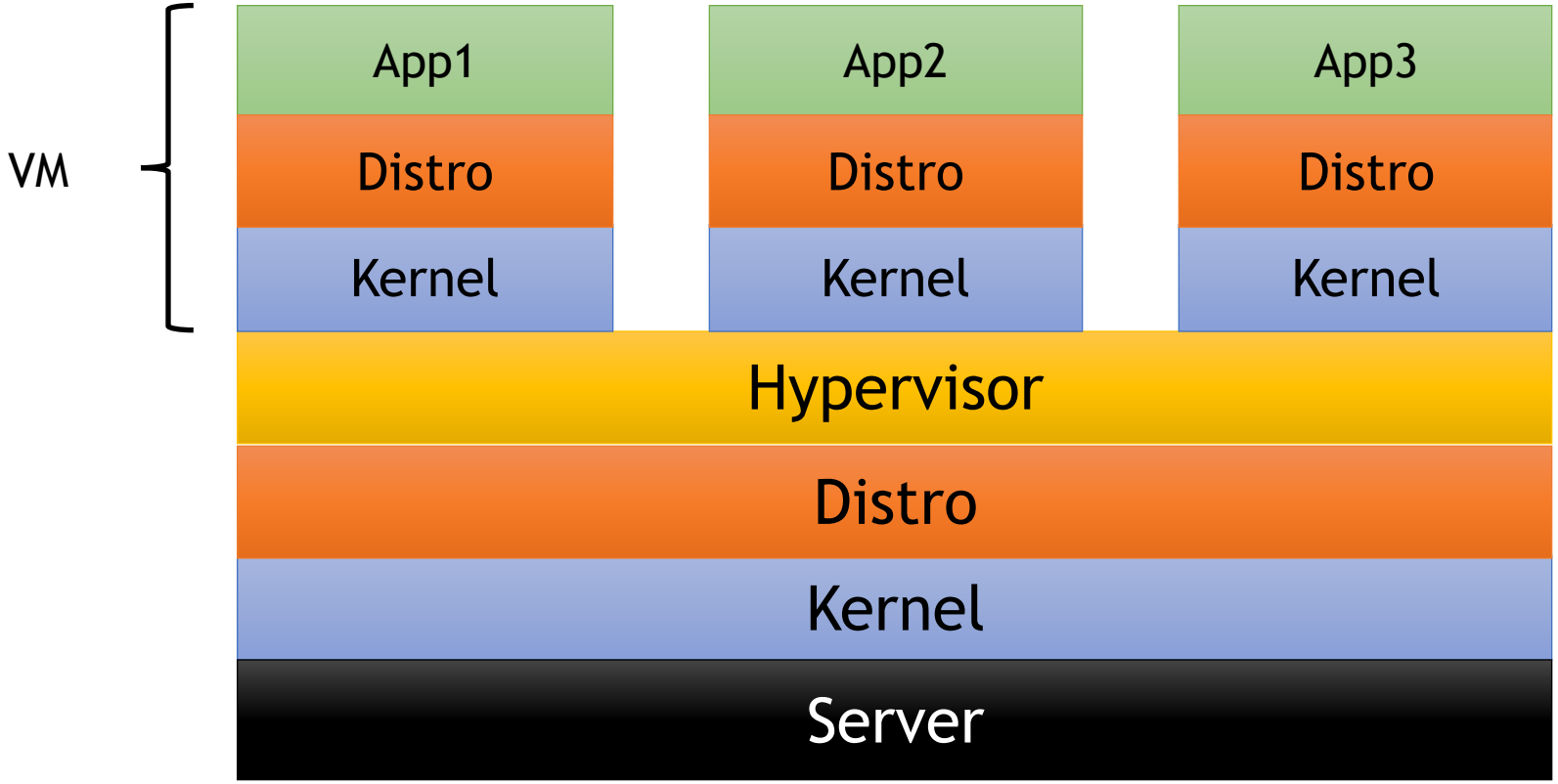
Gianluca Borello
- Software Engineer at Sysdig
- Core developer of sysdig
- Open source enthusiast

gianlucaborello

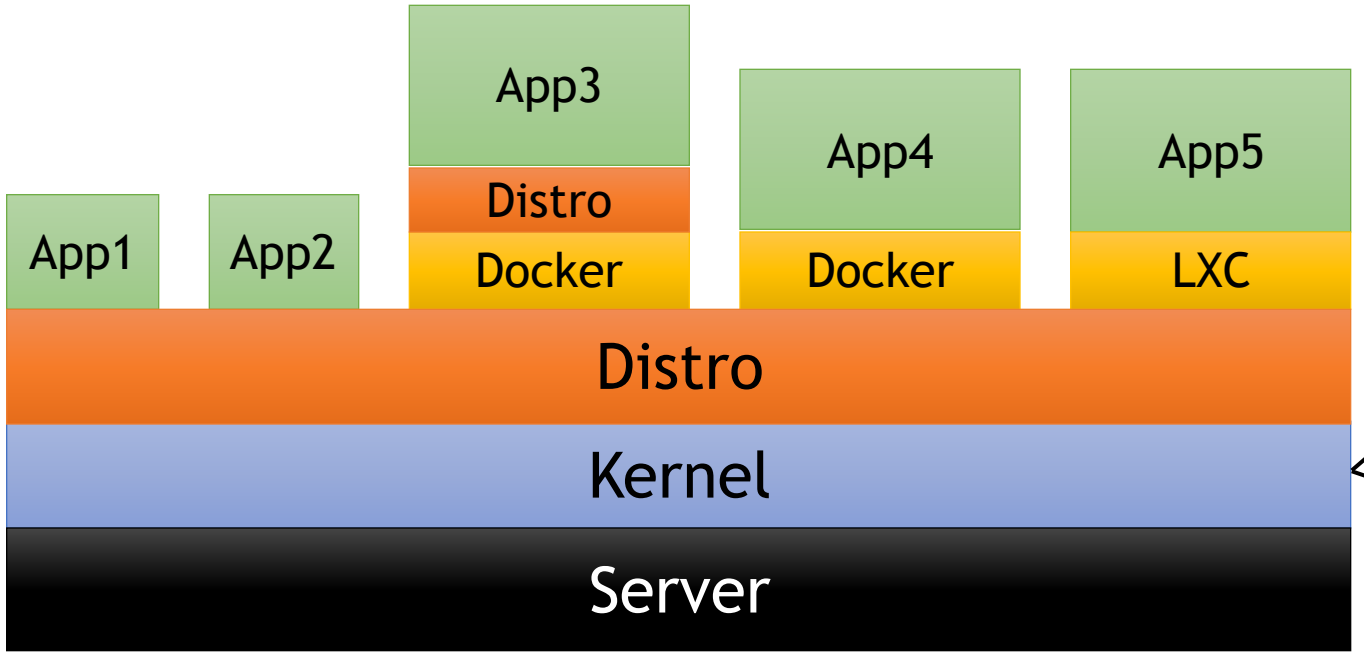
In This Talk

- Introduction to containers
- Monitoring containers with traditional open source tools
- Monitoring containers with sysdig
- Use cases

Containers vs VMs



Containers vs VMs



Cgroups
Cluster processes and constrain resource usage

Namespaces
Isolate resource identifiers

Containers Are Great…

- less overhead
- faster deployments
- reproducibility of environments
- cost optimizations
- Isolation
- flexibility

…But Seeing Inside Containers Is Not Easy

Containers are:

- Isolated
- Self-Contained
- Simple
- Lightweight

A slightly complicated containerized environment

- A “distributed” Wordpress web application
- Many containers

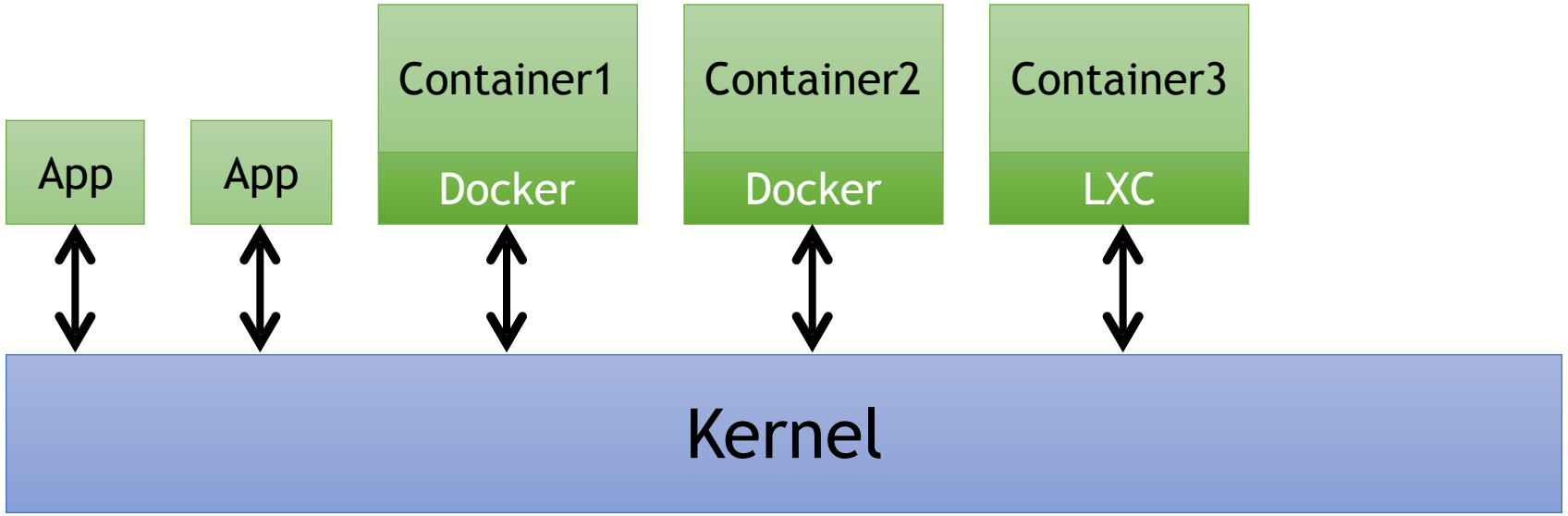
Some Things We Want to Monitor

- Resource usage (CPU/Memory/Disk)
- Network activity
- File I/O activity
- Errors/faults
- Application activity

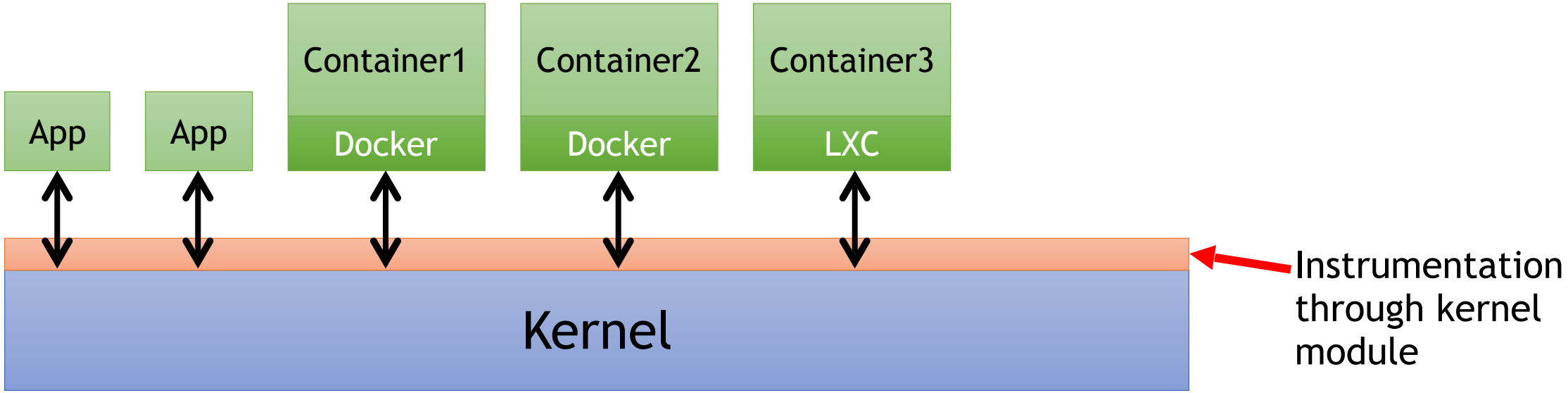
sysdig

- Capture system events, filter them, run useful scripts
- strace + tcpdump + lsof + htop + Lua
- Open Source
- Nice curses UI
- **Native support for containers!**

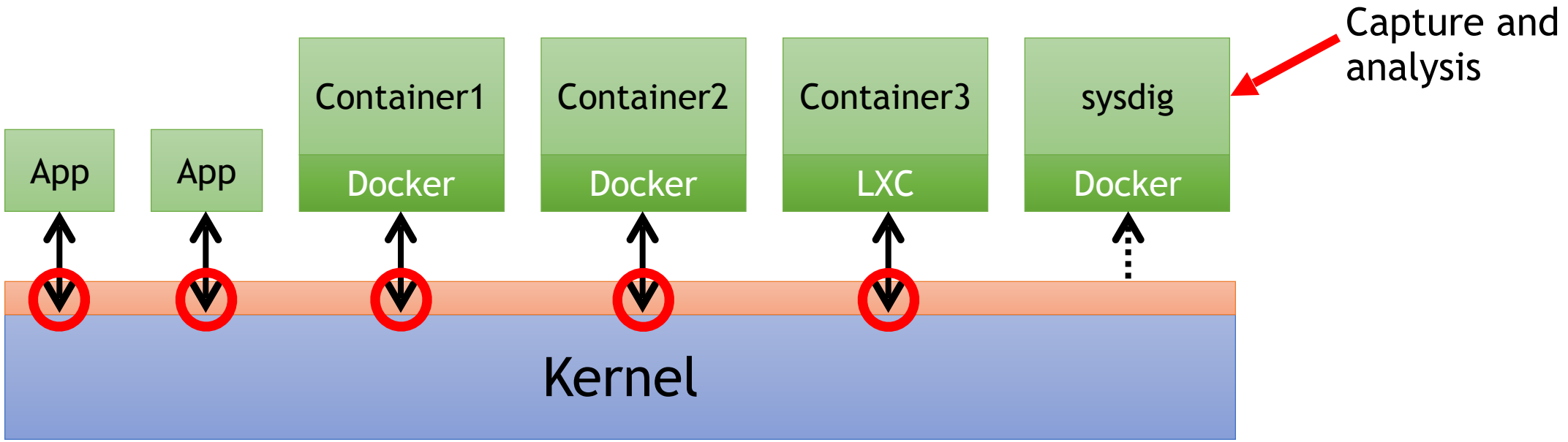
sysdig Architecture



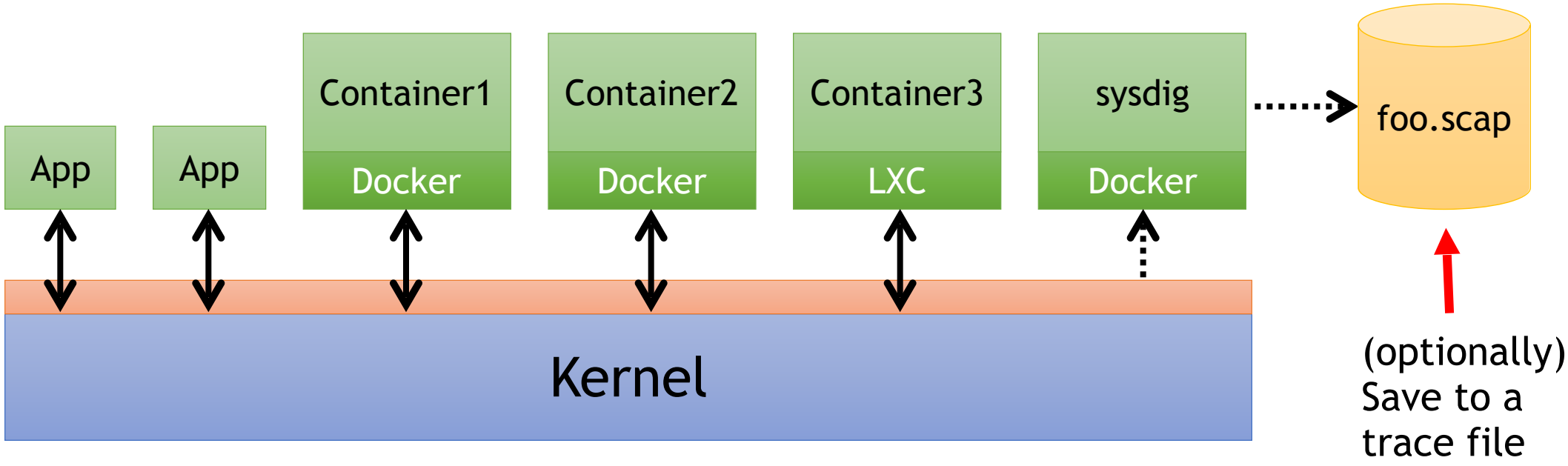
sysdig Architecture



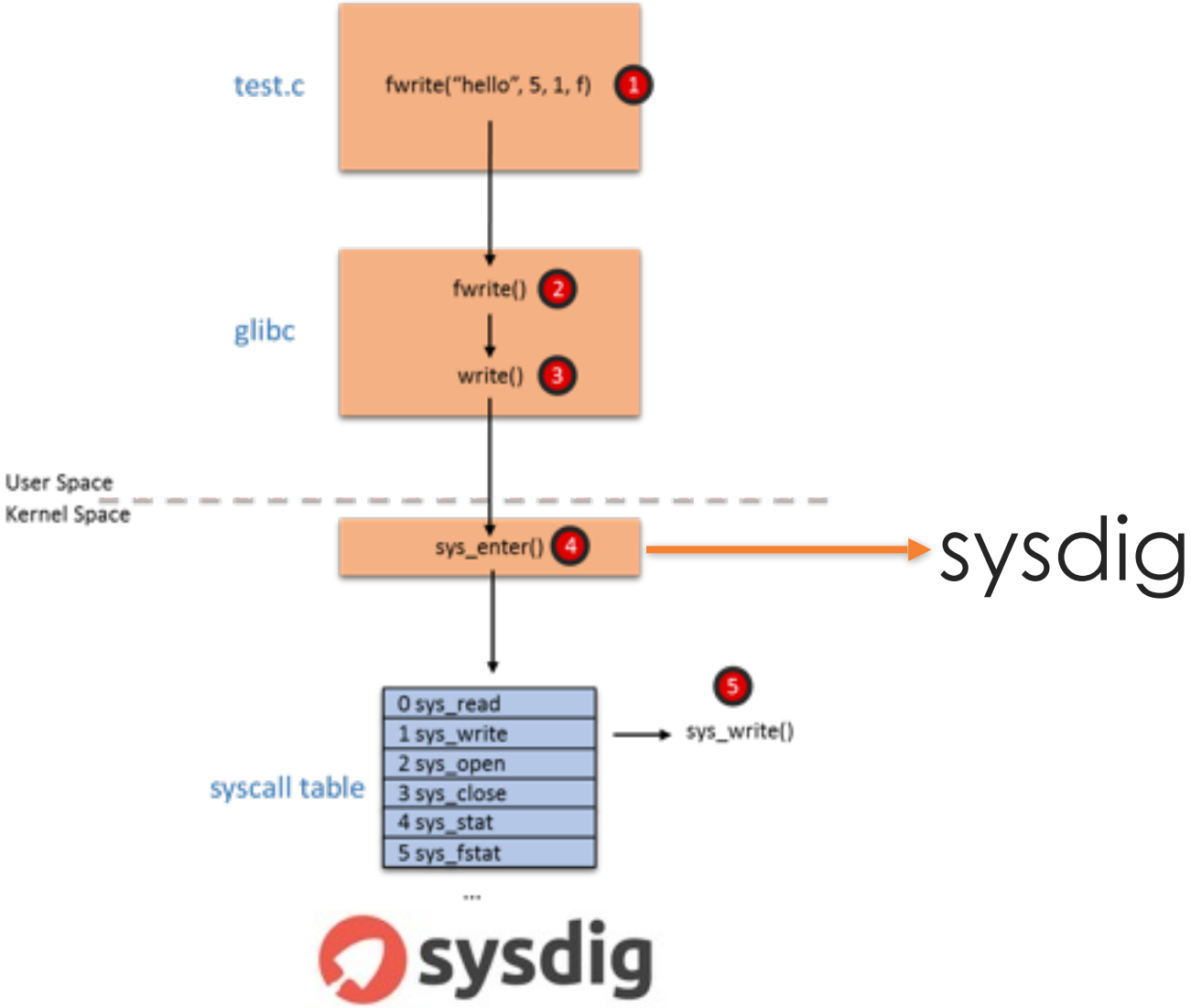
sysdig Architecture



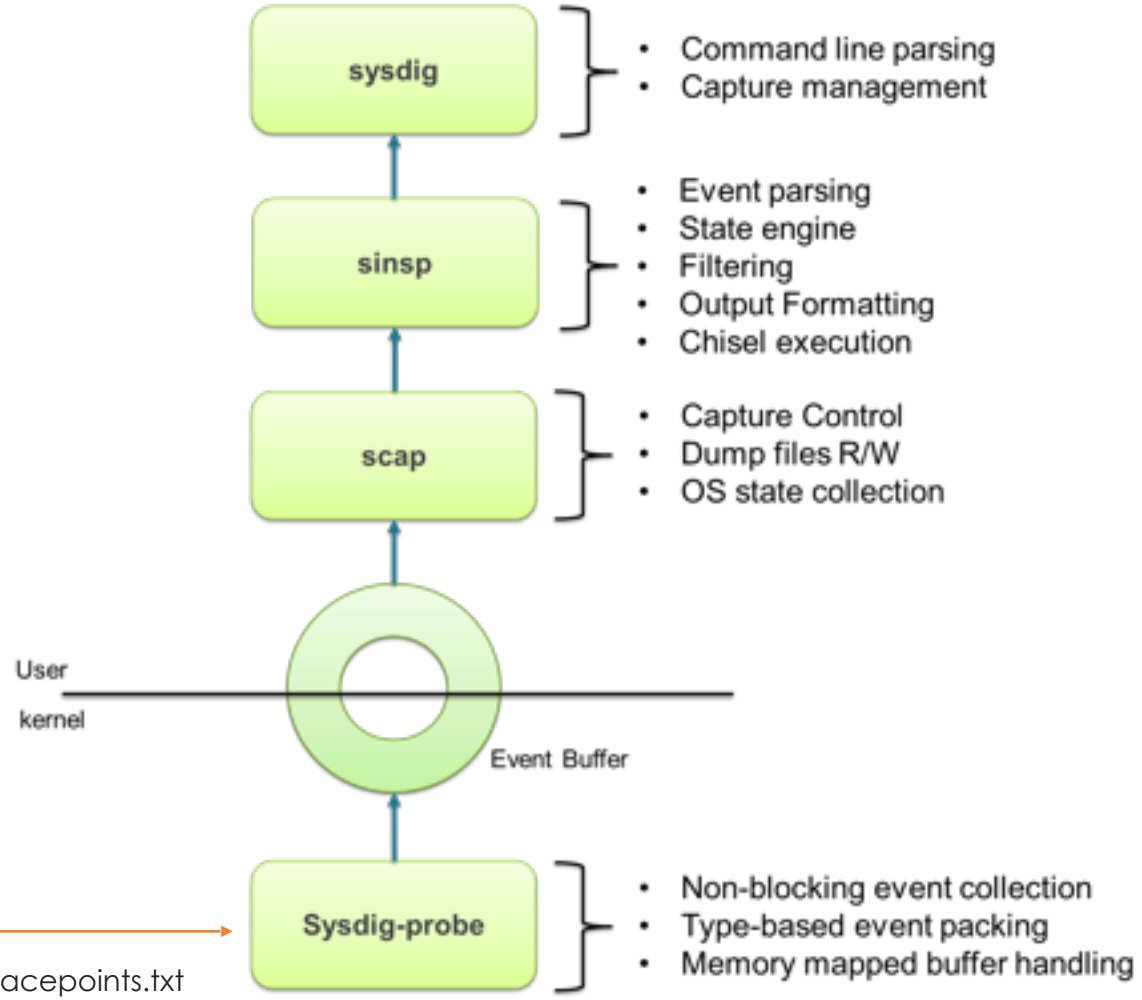
sysdig Architecture



What's a system call?



Sysdig's capture architecture



Tracepoints

/doc/Documentation/trace/tracepoints.txt

sysdig