Use sysdid to record a file capture.

- sysdig -w file.scap

Sysdig inspect

- https://github.com/draios/sysdig-inspect
- Once the container is installed run it:
- `docker run -it -v $(pwd):/captures -p8085:3000 sysdig/sysdig-inspect:latest`
- The above command assumes that you are in the same directory you saved your sysdig recording.

Recording

- If you record from the host VM.
  - You should have access to everything.
  - The k8s and docker containers are subprocess from the host (in this case the host is the VM)

Can filter based on:

- Username
  - `user.name=nobody`
- Process name
  - `proc.name=nginx`