What Can Docker Do For Me?

What Can Docker Do For Me?

Overview

- Concepts
- Common Use Cases
  - Linux Distros
  - Databases (or really any kind of service)
  - Tools
- Larger Projects

Reasons to Use Docker

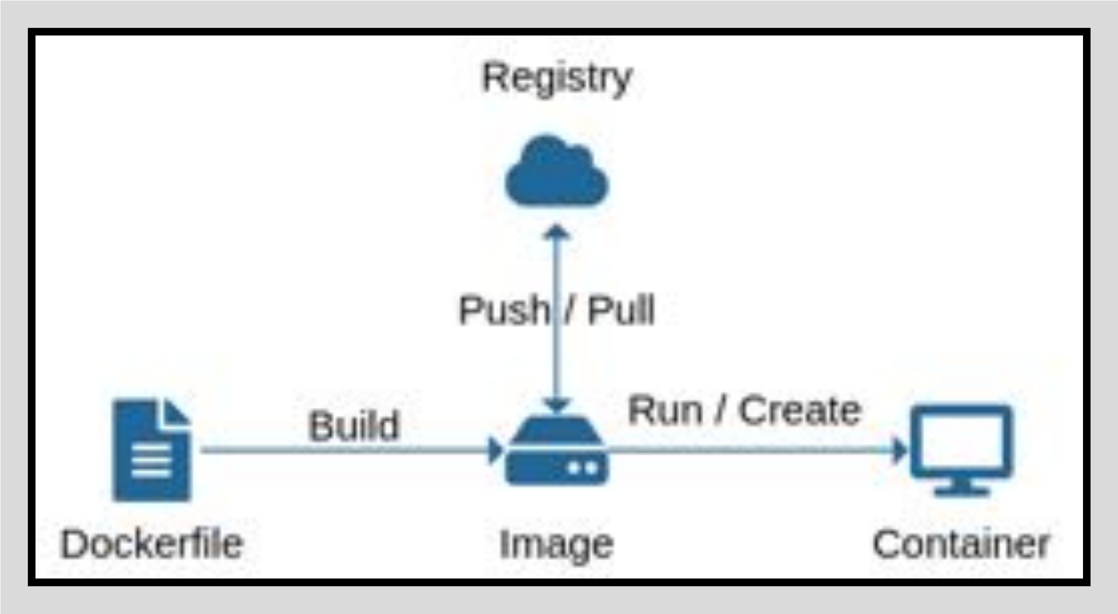
- Better than VMs
- Plays well with others
- Escape dependency hell

Installing

- Windows / Mac - Docker Desktop
  - Bundled with docker-compose and kubernetes
- Linux - instructions per distro
  - or… easy mode (aka non-production):

```
curl -fsSL https://get.docker.com | sh -
```

Concepts


Registry
Push / Pull
Build
Run / Create
Dockerfile
Image
Container

Image

Analogies:

- Golden disk image
- VM snapshot

Dockerfile

Instructions on how to create an image

```
FROM debian

RUN echo "Hello, World!" >> message.txt

ENTRYPOINT cat message.txt
```

Registry

Server that stores pre-built images

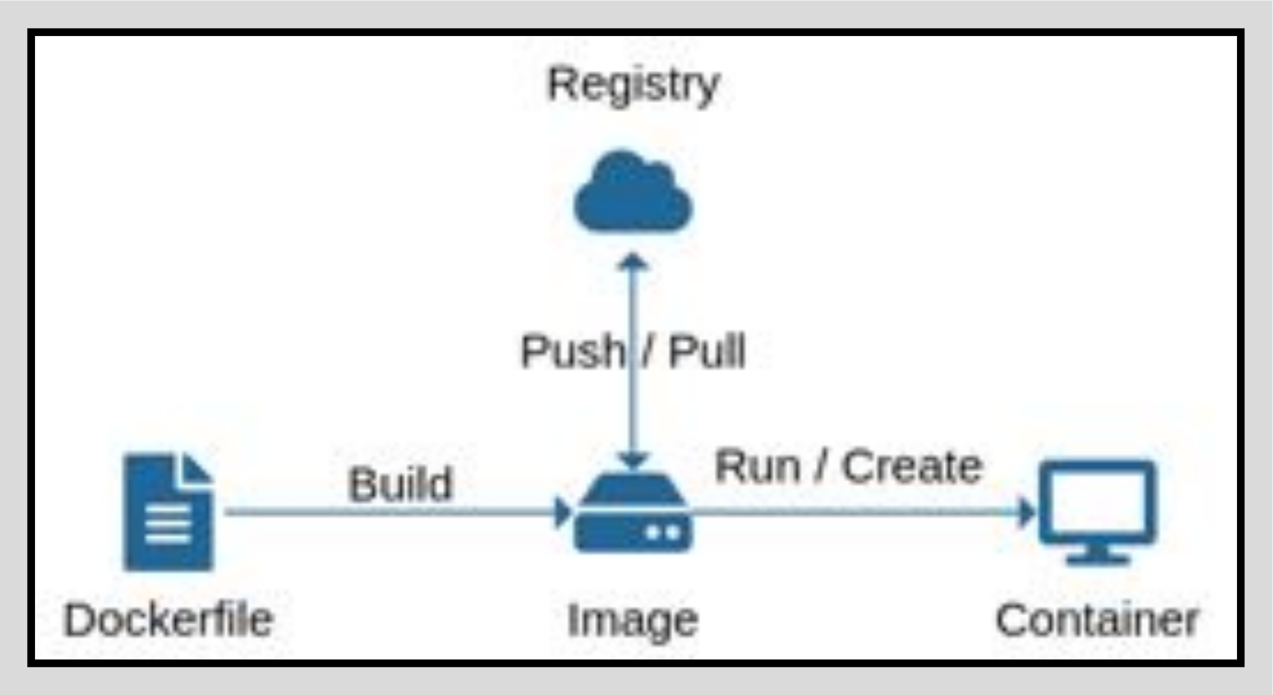
Similar to Linux package repository

- DockerHub.com
- Quay.io

Container

Analogies:

- Provisioned server / VM (powered on or not)
- Initially contains golden image but can change


Registry
Push / Pull
Build
Run / Create
Dockerfile
Image
Container

Volumes

- Data persistence
- Can be shared between containers
- Shared data between host and containers

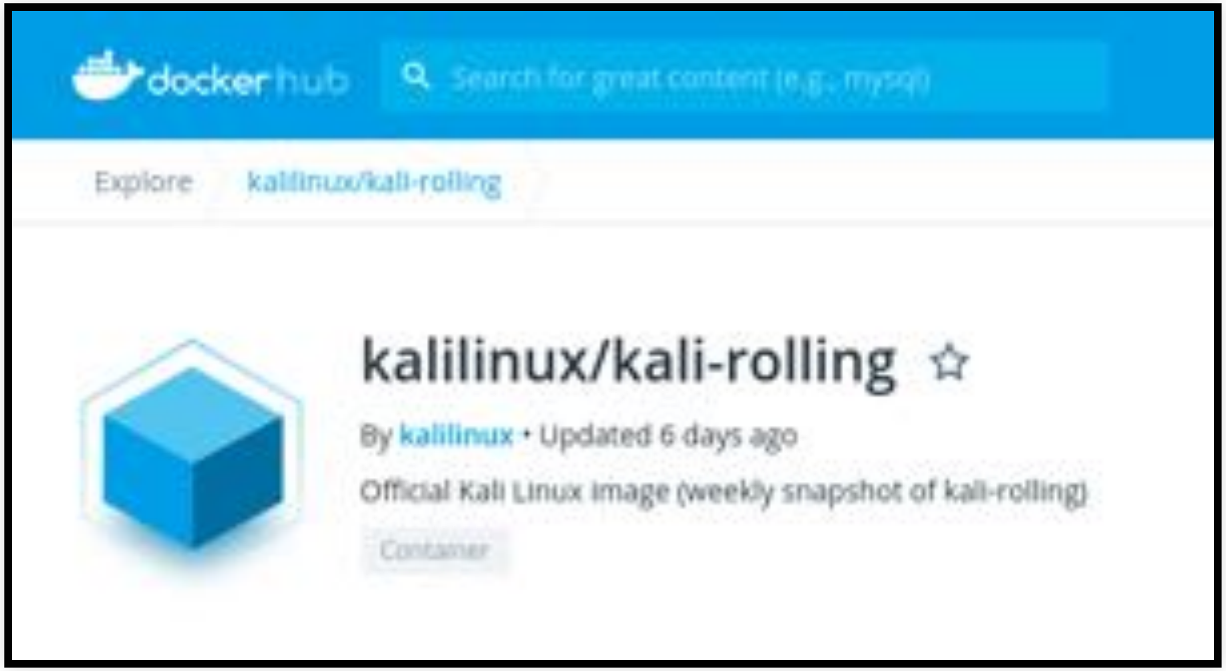
Use Cases

- Distros
- Databases
- Tools

Distros

Can your VMs do this?

Kali



kalilinux/kali-rolling ☆

By kalilinux • Updated 6 days ago

Official Kali Linux image (weekly snapshot of kali-rolling)

Container

```
docker container run --interactive --tty kalilinux/kali-rolling
```

is equivalent to

```
docker run -it kalilinux/kali-rolling
```

Size Comparison

Type	Size
Full Live ISO	2,900 MB
Minimal Netinstall ISO	420 MB
Docker Image	113MB (47.36 MB compressed)

Docker Hub

- Debian
- Ubuntu
- CentOS
- Fedora
- Windows

Tags

What if you need an older version?

```
docker run -it debian:6
```

```
docker run -it ubuntu:12.04
```

Databases

Postgres

```
docker container run \
     --publish 5432:5432 \
     --detach \
     --env POSTGRES_USER=docker \
     --env POSTGRES_PASSWORD=SuperSecretAwesomePassword \
     postgres
```

is equivalent to

```
docker run -p 5432:5432 -d \
     -e POSTGRES_USER=docker \
     -e POSTGRES_PASSWORD=SuperSecretAwesomePassword \
     postgres
```

Postgres Client

CLI

```
docker run --rm -it postgres psql -h 172.29.52.68 -U docker
```

Web UI

```
docker run --rm -p 8080:80 \
    -e PGADMIN_DEFAULT_EMAIL=user@example.com \
    -e PGADMIN_DEFAULT_PASSWORD=password \
    dpage/pgadmin4
```

All the versions!

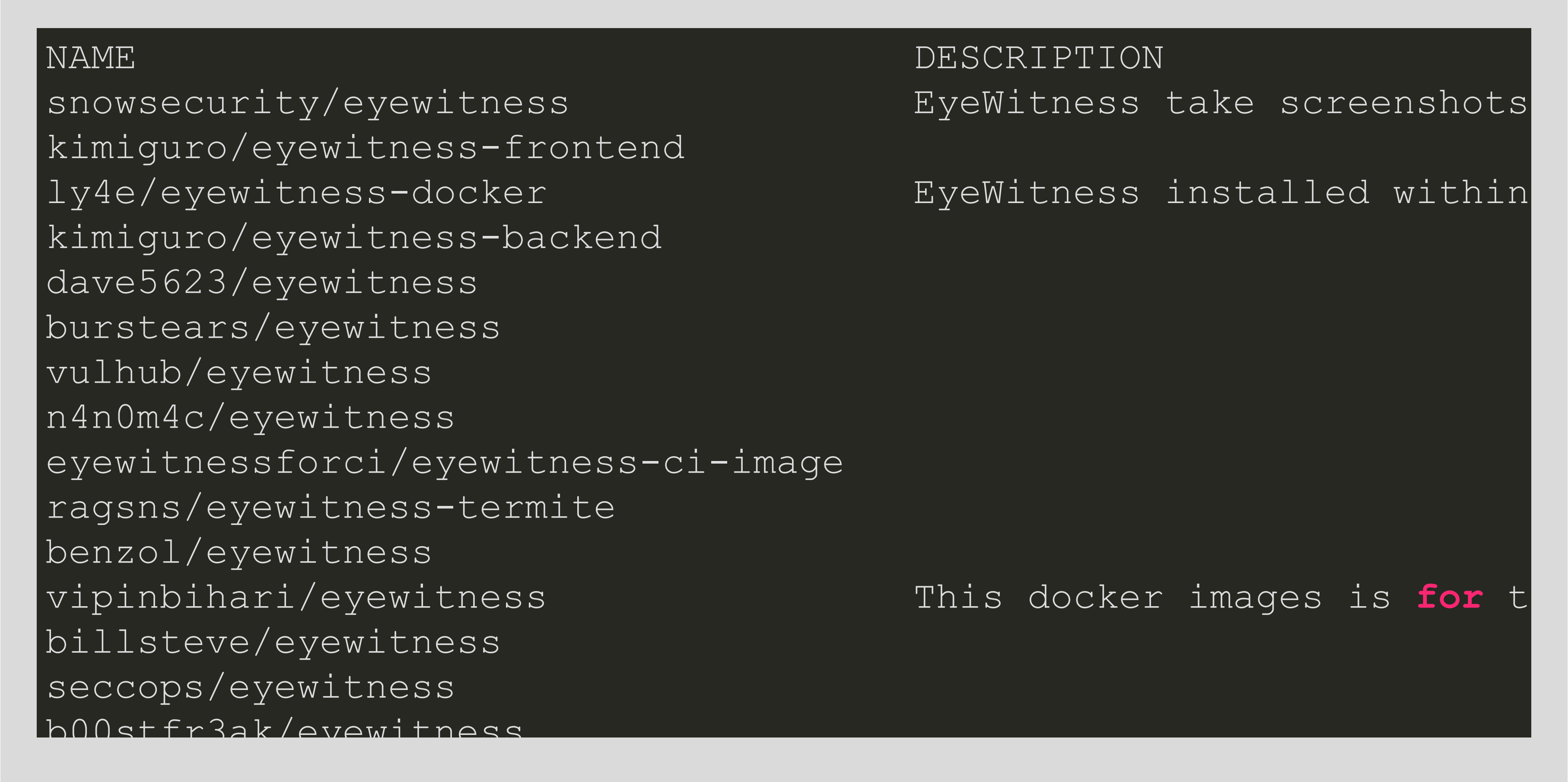
```
docker run -p 5433:5432 -d postgres:9.6.18
docker run -p 5434:5432 -d postgres:10.13
docker run -p 5435:5432 -d postgres:11
```

Tools

EyeWitness

```
docker search eyewitness
```

So many options...



```
NAME                                  DESCRIPTION
snowsecurity/eyewitness               EyeWitness take screenshots
kimiguro/eyewitness-frontend
ly4e/eyewitness-docker                EyeWitness installed within
kimiguro/eyewitness-backend
dave5623/eyewitness
burstears/eyewitness
vulhub/eyewitness
n4n0m4c/eyewitness
eyewitnessforci/eyewitness-ci-image
ragsns/eyewitness-termite
benzol/eyewitness
vipinbihari/eyewitness                This docker images is for t
billsteve/eyewitness
seccops/eyewitness
b00stfr3ak/eyewitness
```

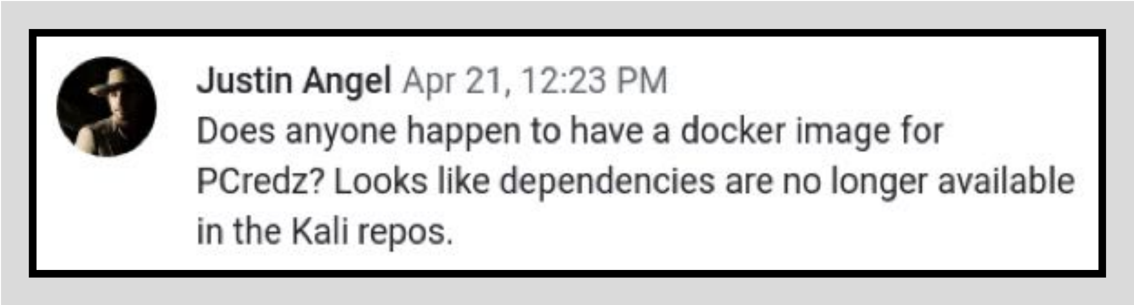
Let’s Get Building

```
git clone https://github.com/FortyNorthSecurity/EyeWitness
docker image build \
    --build-arg user=$USER \
    --tag eyewitness \
    --file EyeWitness/Python/Dockerfile \
    EyeWitness
# or
docker build --build-arg user=$USER \
    -t eyewitness \
    -f EyeWitness/Python/Dockerfile \
    EyeWitness
```

Now let's run

```
mkdir output
docker run --rm -it \
    -v `pwd`/output:/eye \
    eyewitness -d /eye/out --web --single http://www.google.com
```

PCredz



Justin Angel Apr 21, 12:23 PM

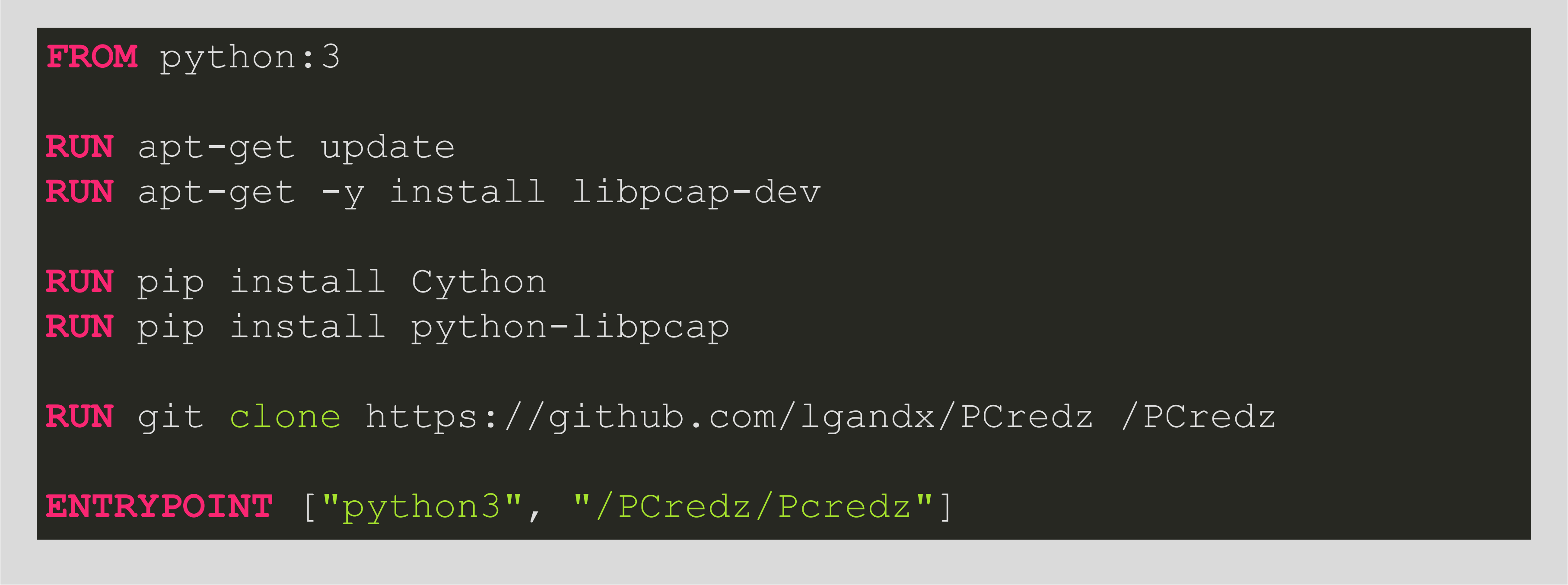
Does anyone happen to have a docker image for PCredz? Looks like dependencies are no longer available in the Kali repos.

Interactive Install

```
docker run -it python:3 bash
```

Or skip for the answer

Dockerfile



```dockerfile
FROM python:3

RUN apt-get update
RUN apt-get -y install libpcap-dev

RUN pip install Cython
RUN pip install python-libpcap

RUN git clone https://github.com/lgandx/PCredz /PCredz

ENTRYPOINT ["python3", "/PCredz/Pcredz"]
```

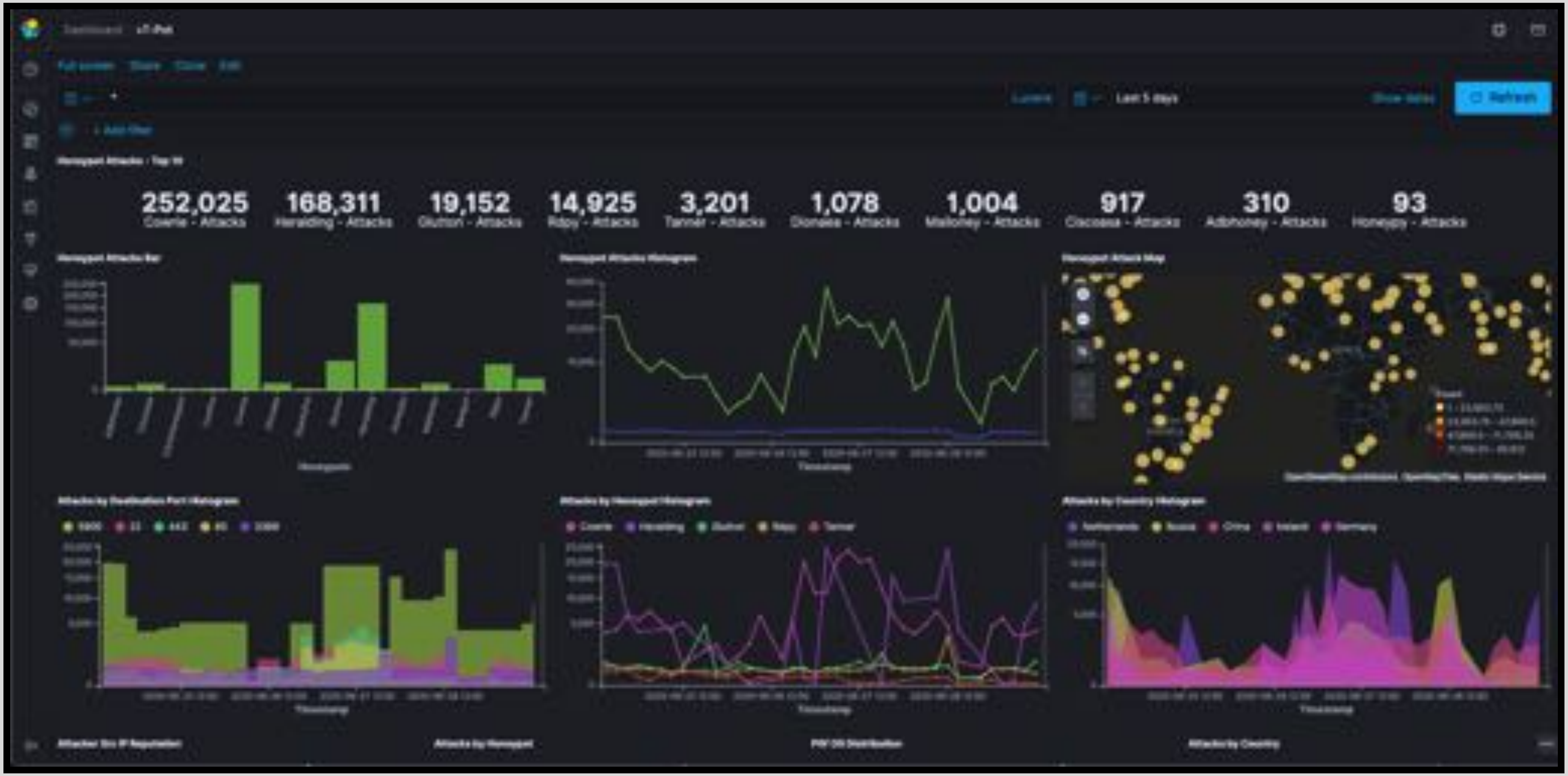
More Complex

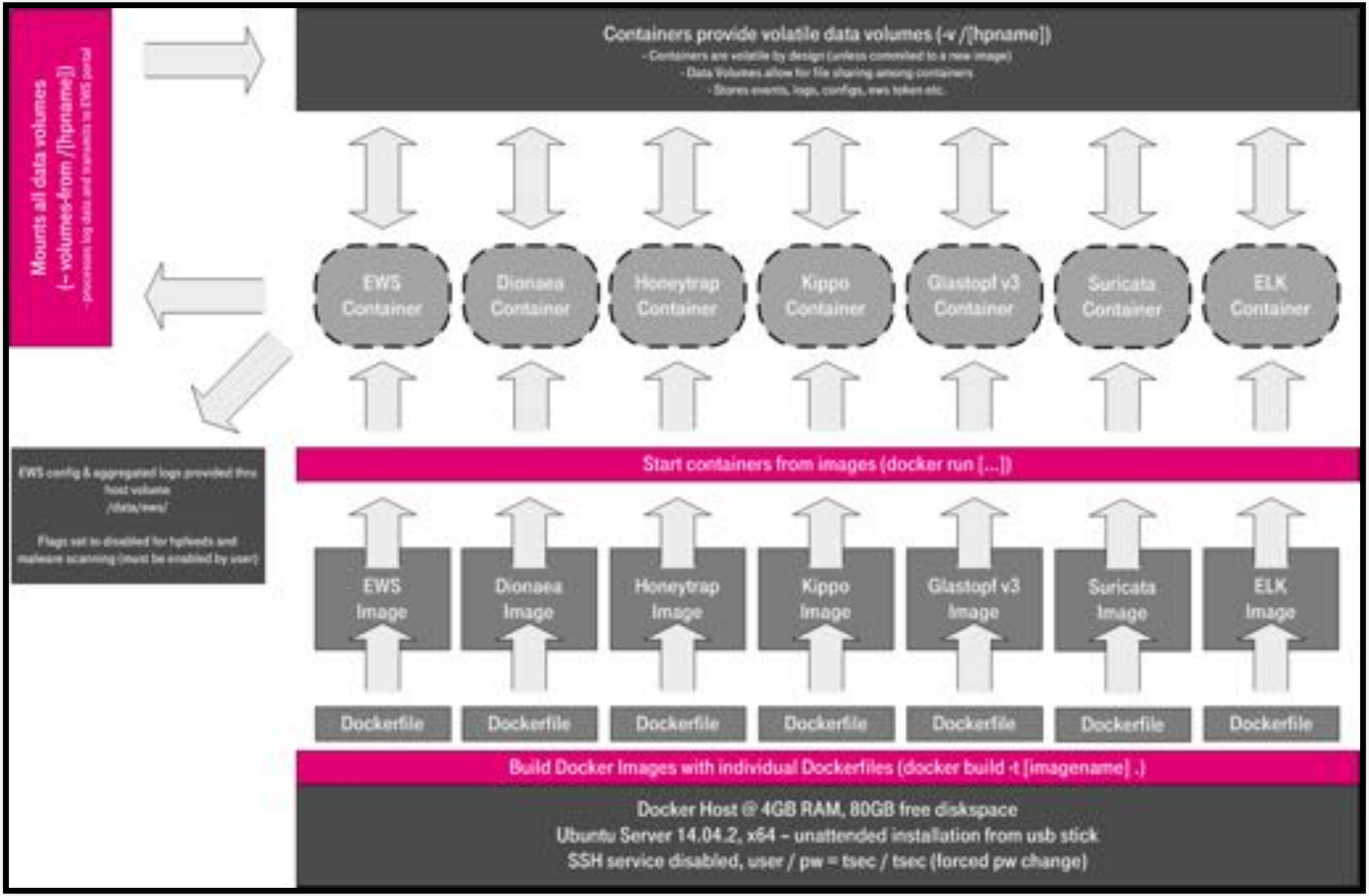
Feature	**Examples**
Networking	ELK, Web Apps
GUI (X11 / VNC / RDP)	Wireshark, WINE, Rdesktop
Kernel capabilities	Zeek, OpenVPN
All-in-one	ML-Toolbox, ELK

Larger Projects Built with Docker

T-Pot

Honeypots in containers





Mounts all data volumes
(--volumes-from /[hpname])
- processes log data and transmits to EWS portal

Containers provide volatile data volumes (-v /[hpname])
- Containers are volatile by design (unless committed to a new image)
- Data Volumes allow for file sharing among containers
- Stores events, logs, configs, ews token etc.

EWS Container
Dionaea Container
Honeytrap Container
Kippo Container
Glastopf v3 Container
Suricata Container
ELK Container

EWS config & aggregated logs provided thru host volume
/data/ews/

Flags set to disabled for hpfeeds and malware scanning (must be enabled by user)

Start containers from images (docker run [...])

EWS Image
Dionaea Image
Honeytrap Image
Kippo Image
Glastopf v3 Image
Suricata Image
ELK Image

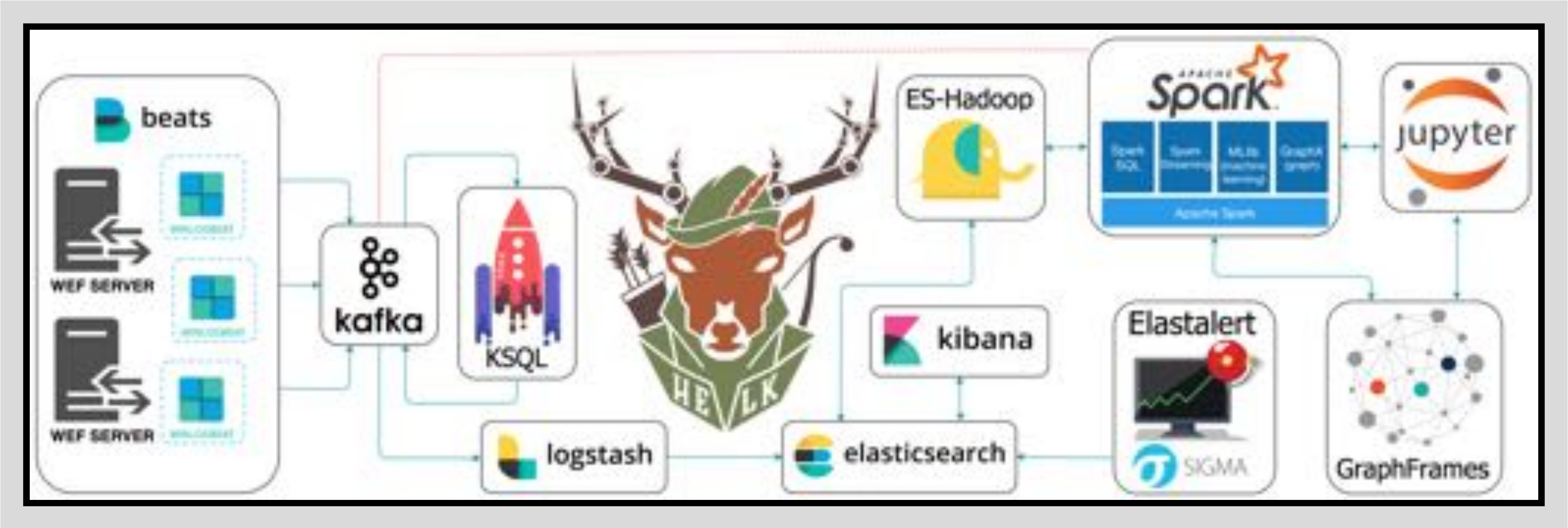
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile

Build Docker Images with individual Dockerfiles (docker build -t [imagename] .)

Docker Host @ 4GB RAM, 80GB free diskspace
Ubuntu Server 14.04.2, x64 – unattended installation from usb stick
SSH service disabled, user / pw = tsec / tsec (forced pw change)

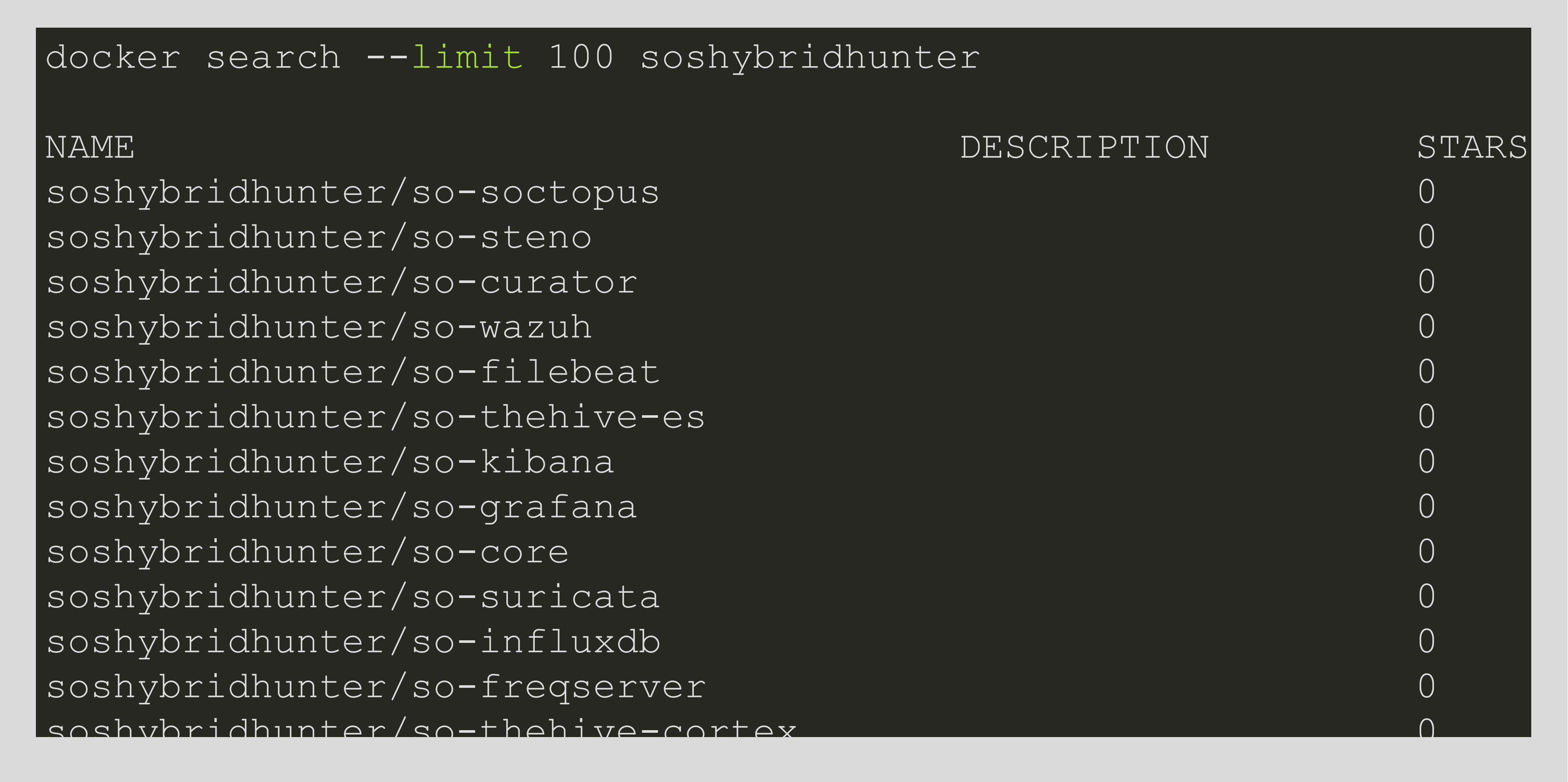
HELK

The Hunting ELK


beats
WEF SERVER
WINLOGBEAT
WEF SERVER
kafka
KSQL
HELK
ES-Hadoop
Spark
Spark SQL
Spark Streaming
MLlib (machine learning)
GraphX (graph)
Apache Spark
jupyter
kibana
Elastalert
SIGMA
GraphFrames
logstash
elasticsearch

Security Onion

Hybrid Hunter



```
docker search --limit 100 soshybridhunter

NAME                                    DESCRIPTION         STARS
soshybridhunter/so-soctopus                                 0
soshybridhunter/so-steno                                    0
soshybridhunter/so-curator                                  0
soshybridhunter/so-wazuh                                    0
soshybridhunter/so-filebeat                                 0
soshybridhunter/so-thehive-es                               0
soshybridhunter/so-kibana                                   0
soshybridhunter/so-grafana                                  0
soshybridhunter/so-core                                     0
soshybridhunter/so-suricata                                 0
soshybridhunter/so-influxdb                                 0
soshybridhunter/so-freqserver                               0
soshybridhunter/so-thehive-cortex                           0
```

Resources

- Play with Docker
- Jess Frazelle - Docker Containers on the Desktop