Docker Forensics Cheatsheet

Important Locations

Where Docker state is stored by default
(All paths in this sheet are relative to here)

```
/var/lib/docker
```

Listing of all images

```
image/*/repositories.json
```

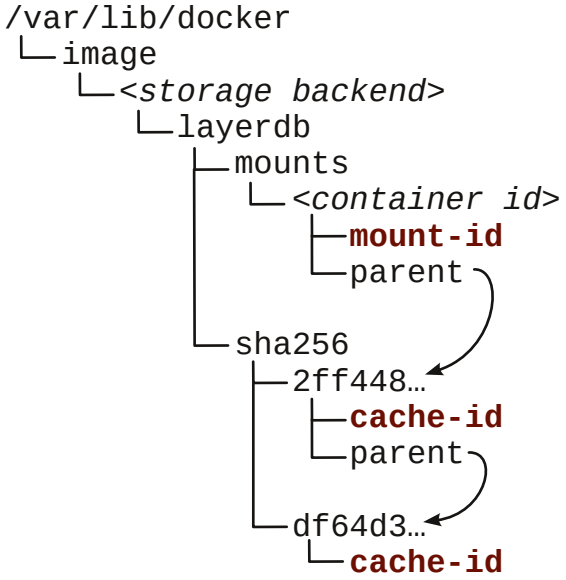
Image metadata (JSON)

```
image/*/imagedb/content/sha256/$IMAGE_ID
```

Container metadata

```
containers/$CONTAINER_ID/config.v2.json
```

Trace the Layer Chain



This directory tree illustrates how the layer chain of a container is linked.

The `parent` file in a layer DB directory points to the next lower layer.

The **id files** contain the storage ID for that layer.

Lookup a Storage ID

Lookup the storage ID of an image's top layer

```
$ cat image/*/layerdb/content/sha256/$IMAGE_ID/cache-id
d84279b377fbd9339694a1146f27a87f3d57a30877e55045026e7e3...
```

Lookup the storage ID of a container's R/W layer

```
$ cat image/*/layerdb/mounts/$CONTAINER_ID/mount-id
b5875928225a155715c6bd4866dd2d4fe480d9e0fe2d847745a...
```

Access an Overlay2 Layer

Mount the layer's filesystem, given its storage ID

```
$ cd overlay2
$ mount -t overlay overlay                          \
       -o ro,lowerdir=$ID/diff:$(cat $ID/lower) \
       /mnt/my-layer
```

Access a Devicemapper Layer

Display the device metadata for a layer, given its storage ID

```
$ jq . devicemapper/metadata/$ID
{
  "device_id": 17,
  "size": 10737418240,
  "transaction_id": 20,
  "initialized": false,
  "deleted": false
}
```

Create the layer block device using the device ID & size metadata *

```
$ dmsetup create dk-my-layer --table \
         "0 $((10737418240/512)) thin /dev/docker/thinpool 17"
```

Mount the layer's filesystem

```
$ mount -o ro,nouuid /dev/mapper/dk-my-layer /mnt/my-layer
```

Release the device when finished

```
$ dmsetup remove dk-my-layer
```

** For help loading the Docker LVM pool (/dev/docker/thinpool) first, see: https://www.forensicswiki.org/wiki/Linux_Logical_Volume_Manager_(LVM)*

Didactic Security
www.didactic-security.com