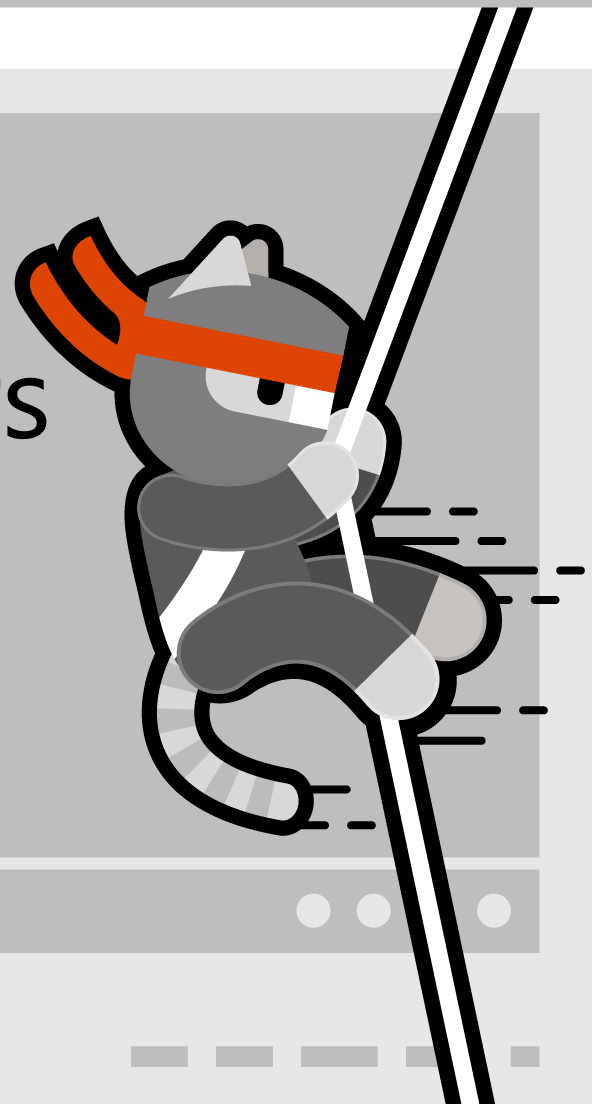
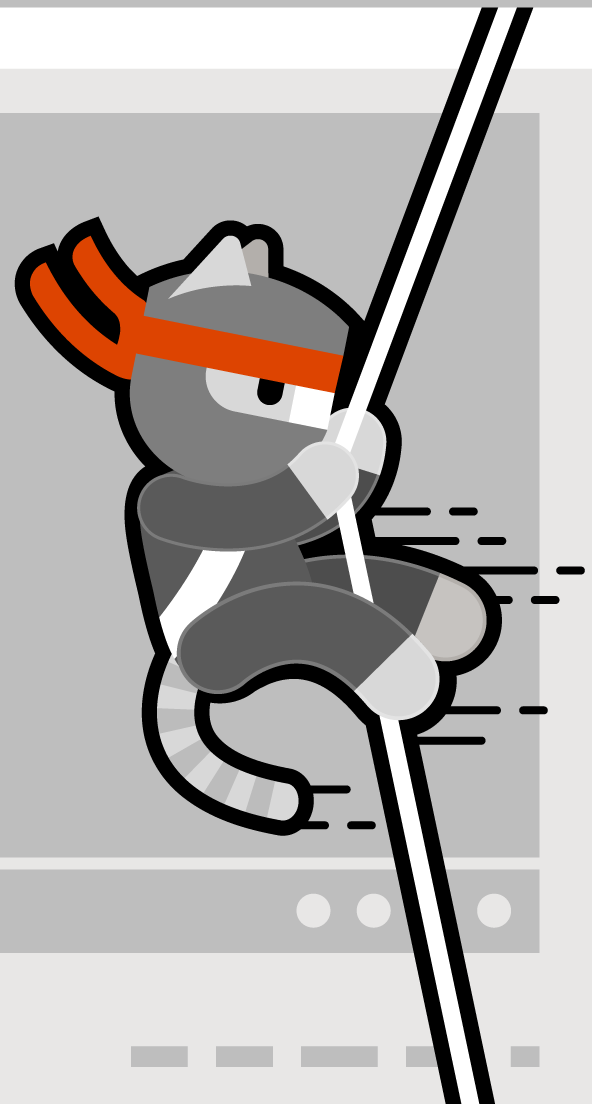
Hacking Containers

Container Storage



Eng Teong Cheah

Microsoft MVP



Storage

The mechanism that Docker and several other container runtimes use is know as a ***union file system (UnionFS)***.

To best understand a union file system, consider a set of clear pieces of transparent paper.

One paper at the bottom has a single line; let's call this the lower layer.

The next piece of paper placed on top of it, also translucent, has a line connecting to the first, and the picture that's formed shows two lines making a 90 degree angle.

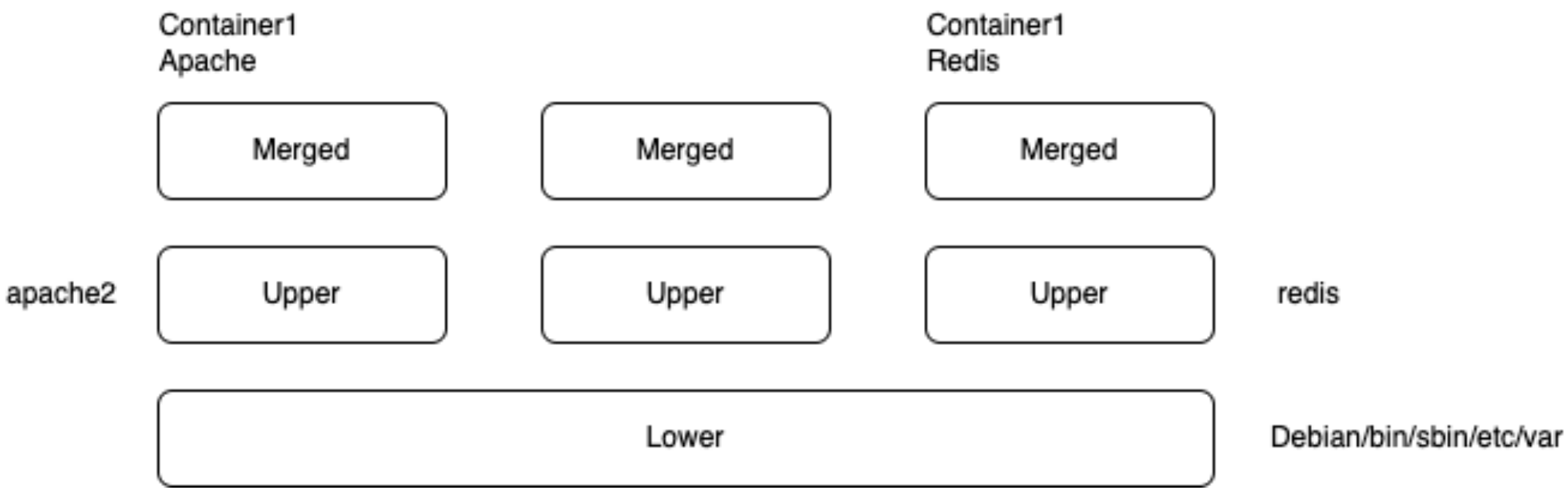
The next piece of paper is overlayed on top, and that paper has a third line connecting to the first two lines; this picture forms a square U. We'll call this the layer upper.

Storage

The final sheet of paper on top we'll call the workdir; it completes the picture, and we see a square.

The layering represents how the overlay file system, which is in use in Docker, uses layers that include diffs between each layer on our disk.

Storage


Container1
Apache
Container1
Redis
Merged
Merged
Merged
apache2
Upper
Upper
Upper
redis
Lower
Debian/bin/sbin/etc/var

Storage

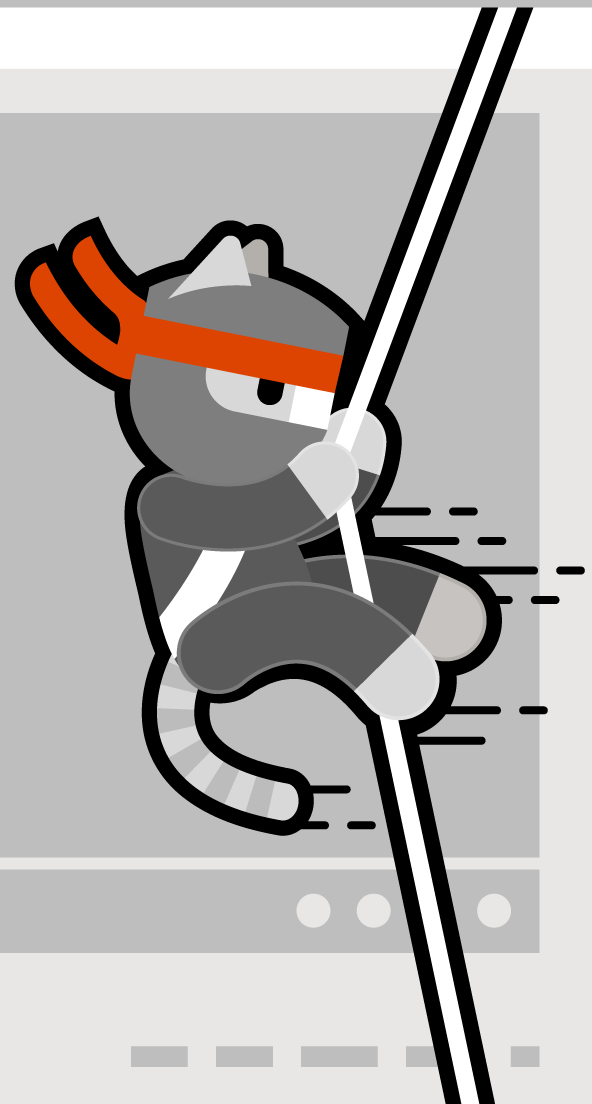
We can inspect these changes using the **docker inspect** and **docker volume** commands.

We can also traverse the file system to the areas that correspond to the file system layers.

Each file system layer is SHA-256 hashed and checked for integrity, as these file systems are supposed to be read-only.

The mechanism used to create each layer is actually in the Dockerfile.

Demo
Container Storage



References

Gray Hat Hacking, Sixth Edition