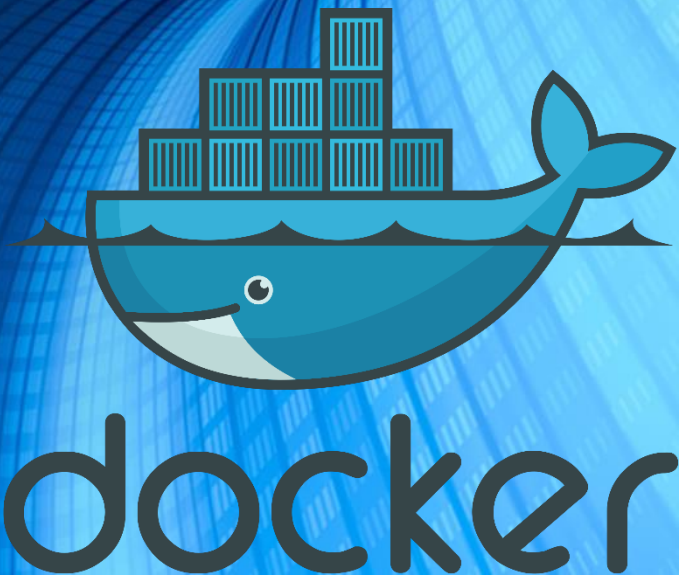
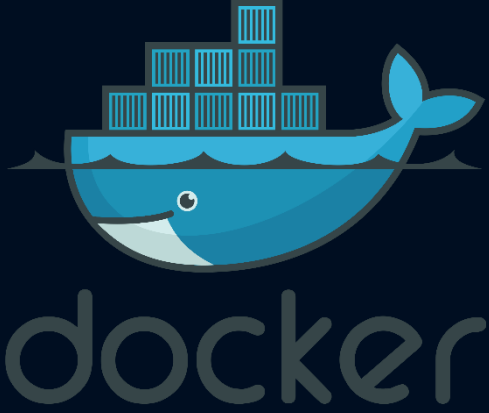
FORENSICS BASIC OF DOCKERS & MALWARE

HARSHITA C. JADHAV
D4N6 INTERN



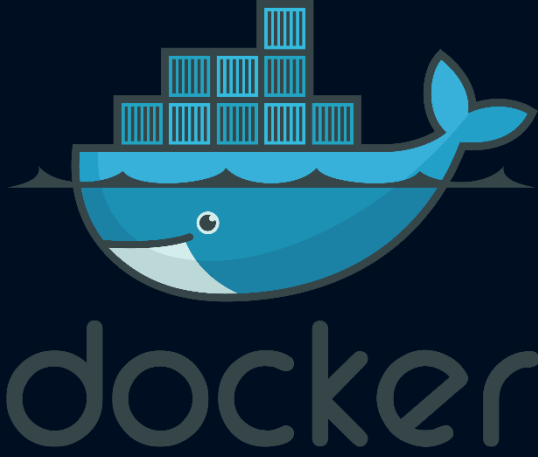


DOCKER

Docker is a popular open-source project based on Linux containers. Docker is written in go and developed by Dot cloud (A PaaS Company). It is basically a container engine that uses the Linux Kernel features like namespaces and control groups to create containers on top of an operating system.

Docker as an open-source project that automates the deployment of software applications inside containers by providing an additional layer of abstraction and automation of OS-level virtualization on Linux.

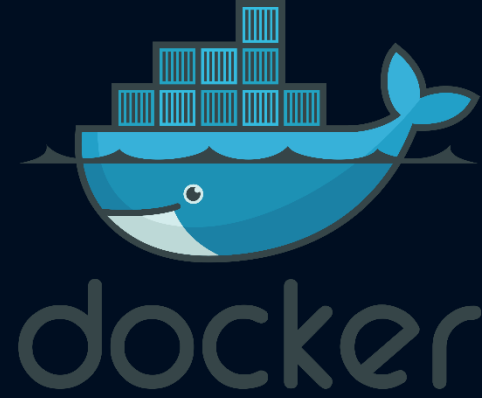
HOW DOES DOCKER WORKS?



Lets looks at the key Docker components.

Docker is composed of the following four components

1. Docker Daemon
2. Docker Client
3. Docker Images
4. Docker Registries
5. Docker Containers



DOCKER DAEMON

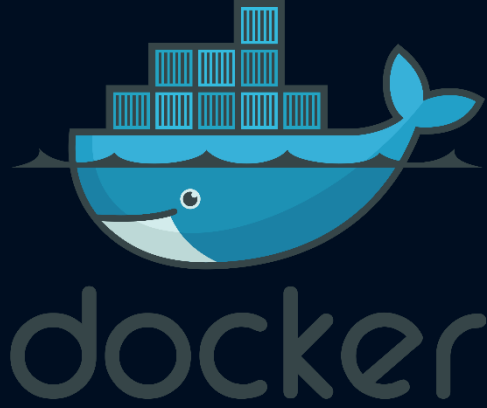
Docker has a client-server architecture. Docker Daemon or server is responsible for all the actions that are related to containers.

The daemon receives the commands from the Docker client through CLI or REST API. Docker client can be on the same host as a daemon or it can be present on any other host.

DOCKER IMAGES

Images are the basic building blocks of Docker.

Containers are built from images. Images can be configured with applications and used as a template for creating containers. It is organized in a layered fashion. Every change in an image is added as a layer on top of it.



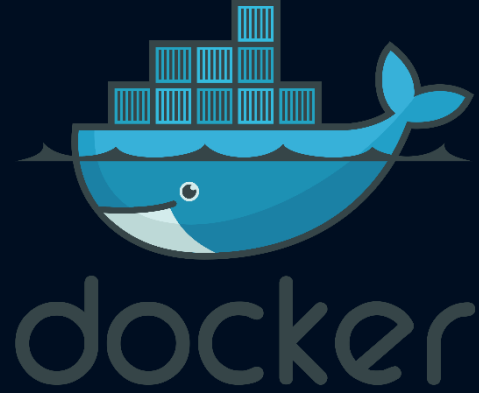
DOCKER REGISTRY

It is a repository for Docker images. Using the Docker registry, you can build and share images with your team.

A registry can be public or private. Docker Inc provides a hosted registry service called Docker Hub. It allows you to upload and download images from a central location.

If your repository is public, all your images can be accessed by other Docker hub users. You can also create a private registry in Docker Hub.

Docker hub acts like git, where you can build your images locally on your laptop, commit it and then can be pushed to the Docker hub.



DOCKER CONTAINER

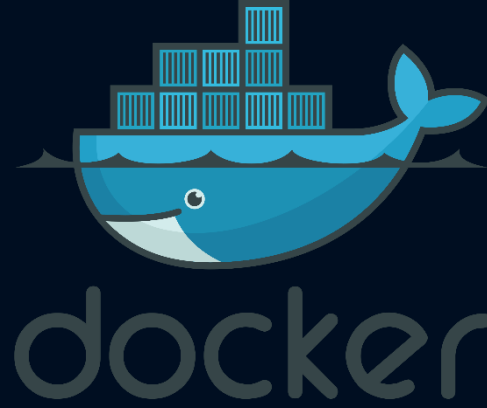
It is the execution environment for Docker. Containers are created from images. It is a writable layer of the image.

You can package your applications in a container, commit it and make it a golden image to build more containers from it.

Two or more containers can be linked together to form tiered application architecture. Containers can be started, stopped, committed and terminated. If you terminate a container without committing it, all the changes made to the container will be lost.

WHY CONTAINERS ARE BETTER THAN VM'S?

- Resource Utilisation & Cost
- Provisioning & Deployment
- Drift Management



CONCLUSION

The best feature of Docker is collaboration.

Docker images can be pushed to a repository and can be pulled down to any other host to run containers from that image.

Moreover, Docker hub has thousands of images created by users and you can pull those images down to your hosts based on your application requirements. Also, it is primarily used in container orchestration tools like Kubernetes .

If you want to run Docker for production workloads, make sure you follow the recommended practices of using Docker images.

You can get started by installing Docker and run the basic operations.

MALWARE

The term malware is a contraction of malicious software. Put simply, malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing a mess. Viruses, Trojans, spyware, and ransomware are among the different kinds of malware.

Malware is often created by teams of hackers: usually, they're just looking to make money, either by spreading the malware themselves or selling it to the highest bidder on the Dark Web. However, there can be other reasons for creating malware too — it can be used as a tool for protest, a way to test security, or even as weapons of war between governments.

WHAT DOES MALWARE DO?

All kinds of things. It's a very broad category, and what malware does or how malware works changes from file to file. The following is a list of common types of malware, but it's hardly exhaustive:

- Virus: Like their biological namesakes, viruses attach themselves to clean files and infect other clean files. They can spread uncontrollably, damaging a system's core functionality and deleting or corrupting files. They usually appear as an executable file (.exe).
- Trojans: This kind of malware disguises itself as legitimate software, or is hidden in legitimate software that has been tampered with. It tends to act discreetly and create backdoors in your security to let other malware in.
- Spyware: No surprise here spyware is malware designed to spy on you. It hides in the background and takes notes on what you do online, including your passwords, credit card numbers, surfing habits, and more.

WHAT DOES MALWARE DO?

- Worms: Worms infect entire networks of devices, either local or across the internet, by using network interfaces. It uses each consecutively infected machine to infect others.
- Ransomware: This kind of malware typically locks down your computer and your files, and threatens to erase everything unless you pay a ransom.
- Adware: Though not always malicious in nature, aggressive advertising software can undermine your security just to serve you ads which can give other malware an easy way in. Plus, let's face it: pop-ups are *really* annoying.
- Botnets: Botnets are networks of infected computers that are made to work together under the control of an attacker.

HOW TO PROTECT AGAINST MALWARE

- When it comes to malware, prevention is better than a cure. Fortunately, there are some common sense, easy behaviors that minimize your chances of running into any nasty software.
- Don't trust strangers online! "Social engineering", which can include strange emails, abrupt alerts, fake profiles, and curiosity-tickling offers, are the #1 method of delivering malware. If you don't know exactly what it is, don't click on it.
- Double-check your downloads! From pirating sites to official storefronts, malware is often lurking just around the corner. So before downloading, always double-check that the provider is trustworthy by carefully reading reviews and comments.
- Get an ad-blocker! Malvertising – where hackers use infected banners or pop-up ads to infect your device – is on the rise. You can't know which ads are bad: so it's safer to just block them all with a reliable ad-blocker.
- Careful where you browse! Malware can be found anywhere, but it's most common in websites with poor backend security, like small, local websites. If you stick to large, reputable sites, you severely reduce your risk of encountering malware.

HOW TO DETECT MALWARE

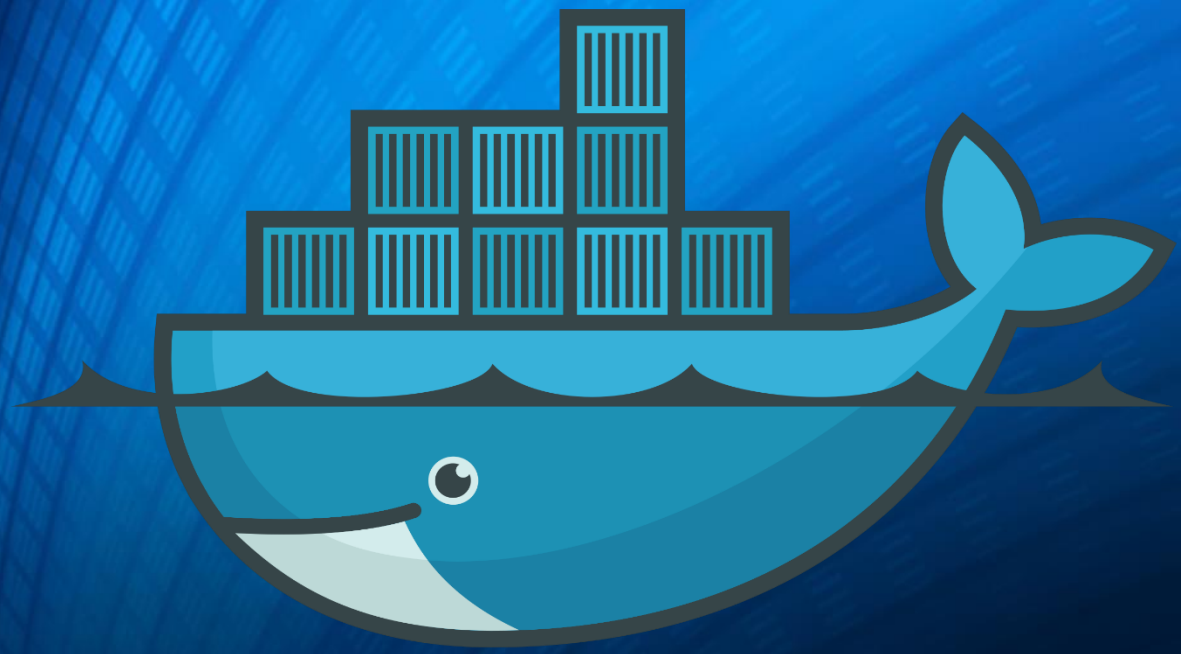
Certain strains of malware are easier to detect than others. Some, like ransomware and adware, make their presence known immediately, either by encrypting your files or by streaming endless ads at you. Others, like Trojans and spyware, go out of their way to hide from you as long as possible, meaning they could be on your system a long time before you realize that they're present. And then there are others, like viruses and worms, that might operate in secret for a time, before the symptoms of their infection start to appear, such as freezing, deleted or replaced files, sudden shutdowns, or a hyperactive processor.

The only surefire way to detect all malware before it infects your PC, Mac, or mobile is to install anti-malware software, which will come packaged with detection tools and scans that can catch malware currently on your device, as well as block malware trying to infect it.

HOW TO REMOVE MALWARE

- Physically Disconnect Your System From Internet
- Boot your PC into Safe Mode
- Check Installed Programs
- Clear temporary files from your system
- Police Your Online Behavior
- Scan Your Device Using a Reputed Antivirus
- Run Malware Detector Tool

  Example - Malwarebytes



docker

THANK YOU

HARSHITA C. JADHAV
D4N6 INTERN