Docker Containers for Malware Analysis

Lenny Zeltser

Senior Faculty Member, SANS Institute Product Management Director, NCR Corp

Get these slides now at https://zeltser.com/media/archive/docker.pdf

Lots of awesome malware analysis

tools run on Linux.

* Should you run them on your primary system?
* Use the REMnux distro for easier set up?
* Containers offer another convenient option.

2

Docker containers offer a nice app

packaging and distribution mechanism.

* Each application has its own runtime environment.
* More lightweight than full-fledged virtualization, but weaker isolation.
* Rich ecosystem for building, distributing and running apps as containers.

3



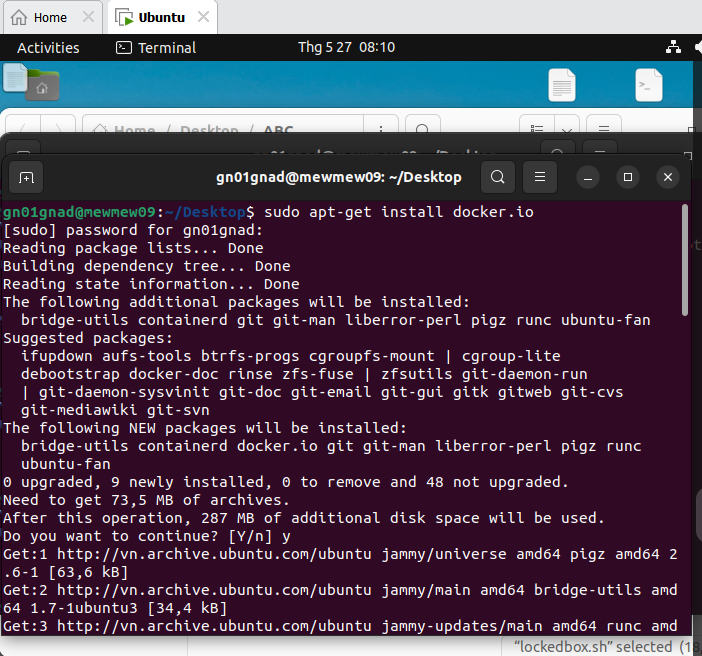
# What Are Docker Application Containers?

4

Docker is software and an ecosystem

for application containers.

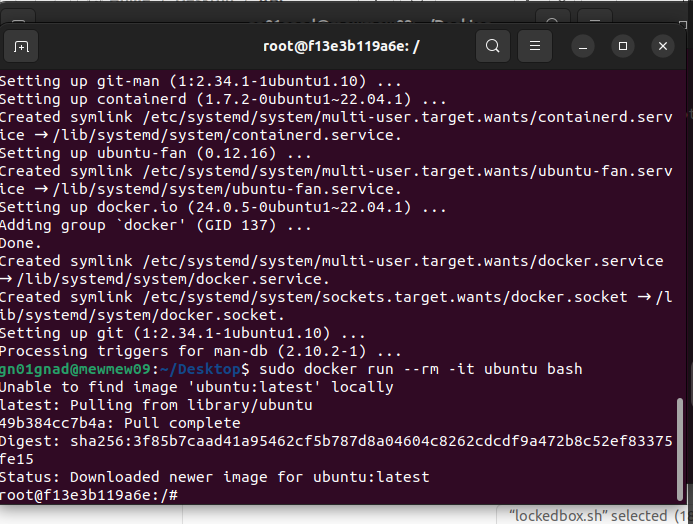
Docker software runs best on Linux, but also works fine on Windows and OS X.



Docker maintains the Docker Hub

Registry of public app images.

For instance, you can easily launch a transient instance of an Ubuntu container.



Remove container when done

Make container interactive

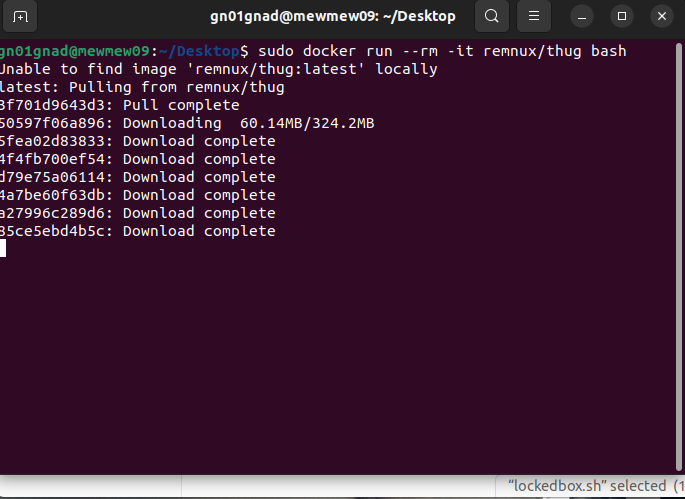
Run bash inside the container

ẽiA Docker image of an app contains

7

the software and its dependencies.

For example, you can easily launch the Thug honeyclient container. Docker automatically downloads the image.



clA container gets its own file system,

process listing and network stack.

However, containers share the OS kernel with each other and the underlying host.

Malware analysis apps as Docker

containers offer several benefits.

* Apps with conflicting dependencies can run on the same host.
* No unwanted files lying around after you’re done with the analysis.
* Some level of isolation around the analysis application container.

We Just Discussed



Docker

Application images Application containers Installing Docker

Launching an app container Advantages of containers



# Running and Interacting with Docker Containers

11

The REMnux project provides

several Docker images.

* Examine websites and scripts: remnux/thug, remnux/jsdetox, remnux/v8
* Process multiple samples: remnux/mastiff, remnux/maltrieve
* Research threats: remnux/viper, remnux/crits
* Examine memory: remnux/rekall, remnux/volatility
* Analyze code: remnux/radare2

https://remnux.org/docs/containers/run-apps

Use “-v” to map the host’s

directory into the container.

First create the directory on the underlying host and make it world-accessible.

A screenshot of a computer

Description automatically generatedcle

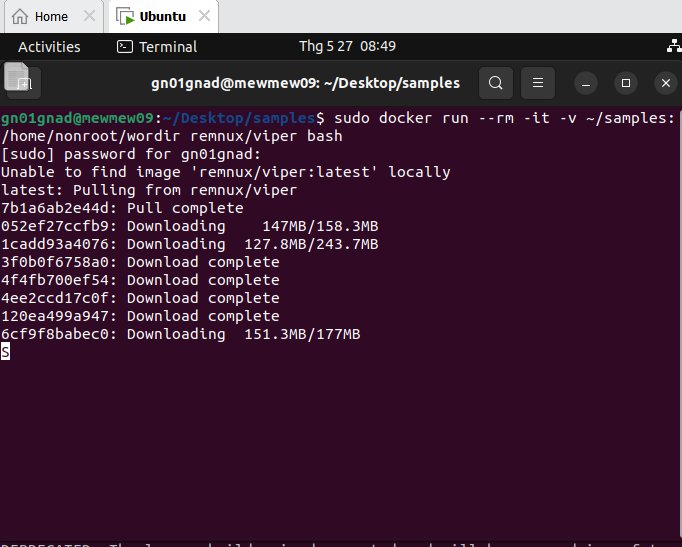
The use of containers encourages

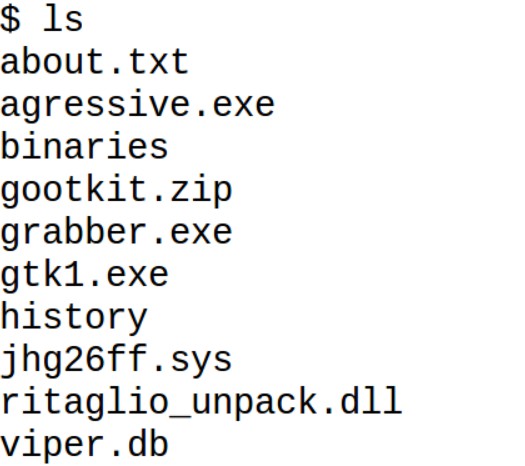
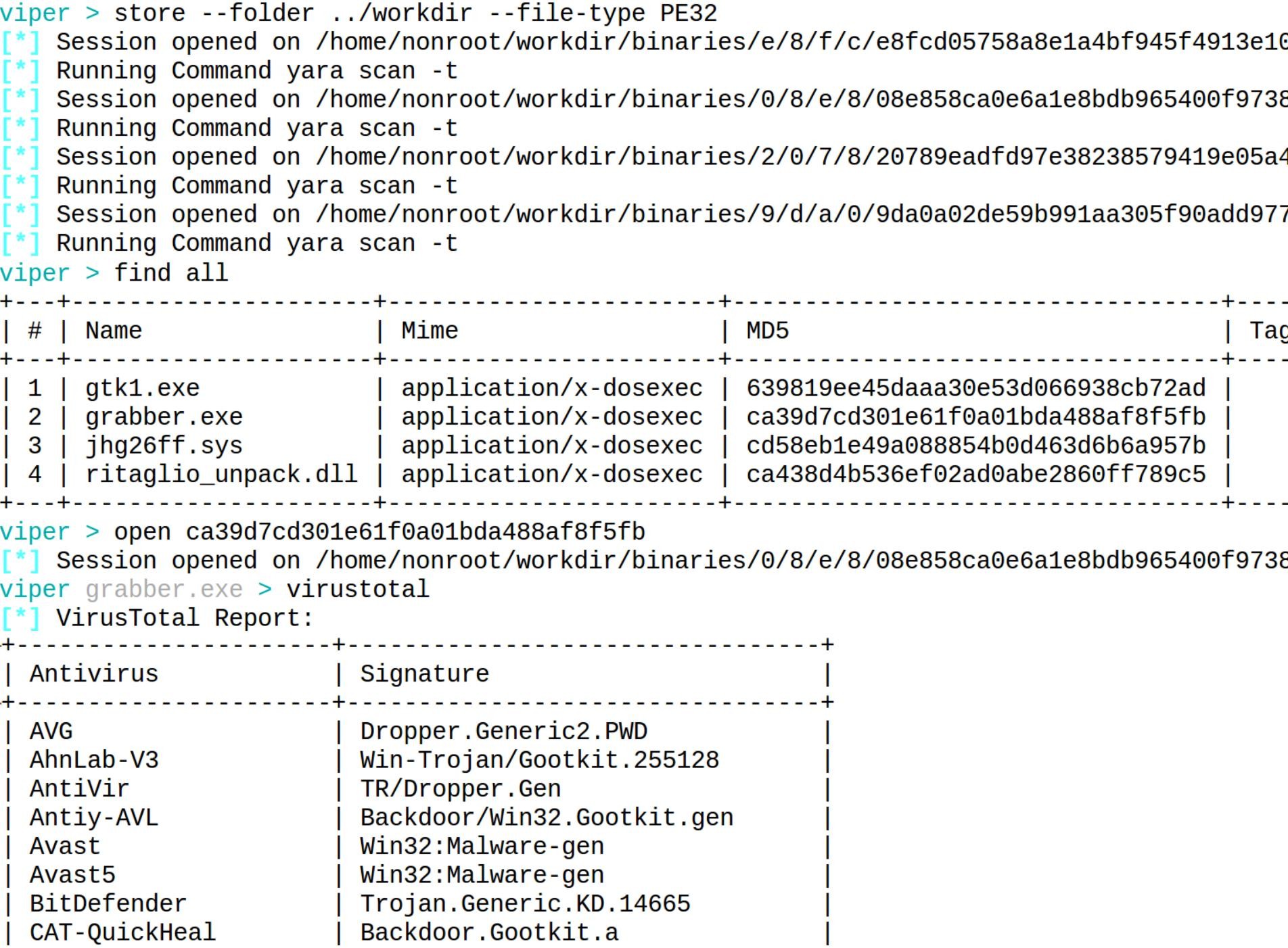
separating “code” from “data”.

Store data on your underlying host while running apps in transient environments.

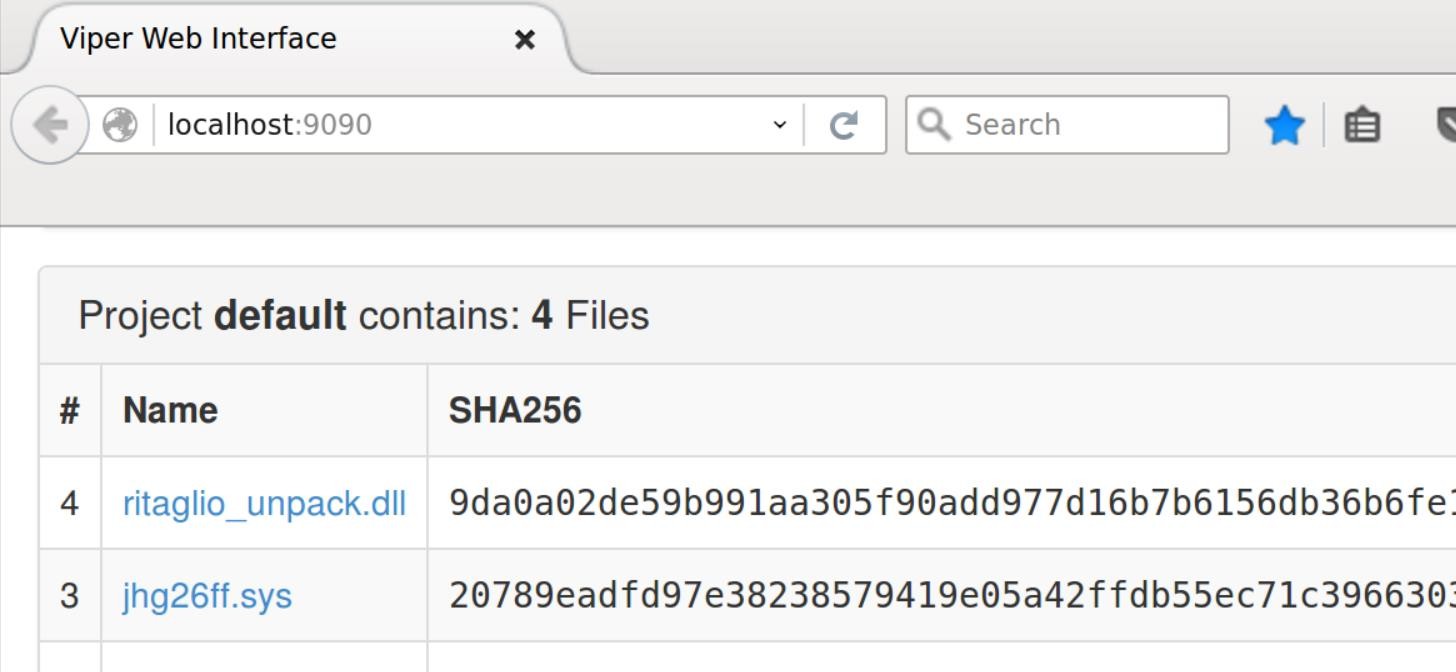
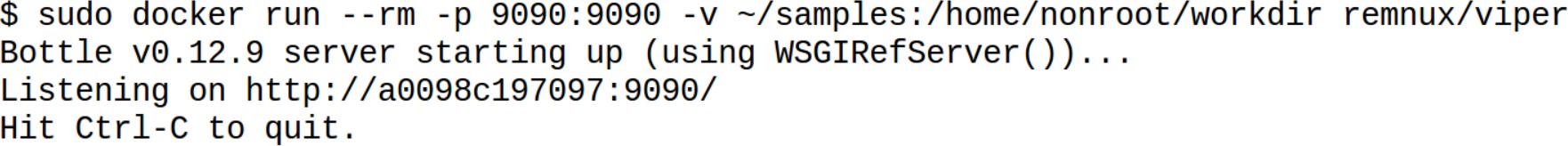
A screenshot of a computer

Description automatically generated





Use “-p” to access network ports



within a container.

Expose container’s TCP port 9090 to interact with the application from localhost.

Use “ps” to show running containers

and “stop” to stop them.

You can refer to the container using its ID or its easier-to-type name.

A screenshot of a computer

Description automatically generated

Docker automatically removes this container after it is stopped, because we launched it with the “--rm” parameter.

17

Docker containers aren’t isolated

as strongly as virtual machines.

* The OS kernel is shared among containers and with the underlying host.
* Containers don’t receive their own user namespaces, but Docker is working to fix this.
* Presently, root processes in containers interact with the kernel with root privileges.

We Just Discussed



REMnux collection of images Sharing directories with containers Separating “code” from “data” Mapping network ports Limitations of container isolation



# Building and Your Own Docker Images

20

A Dockerfile contains instructions

for building a new Docker image.

* Use an existing image as a starting point.
* Document instructions for downloading, compiling and configuring the application.
* Commands must work without user interaction.
* Look at other Dockerfiles to start learning.
* Test commands manually by running them in “sudo docker run --rm -it ubuntu:14.04 bash”.

https://registry.hub.docker.com/u/remnux/thug/dockerfile

21

Docker images in the REMnux

22

collection start from ubuntu:14.04.

Start with “apt-get update”, then install only the packages required by the software.

FROM ubuntu:14.04

MAINTAINER Lenny Zeltser (@lennyzeltser, [www.zeltser.com)](http://www.zeltser.com/)

USER root

RUN apt-get update && \

apt-get install -y --no-install-recommends \ python2.7 \

python2.7-dev \ python-html5lib \

…

Docker stacks read-only file system

images to form an image.

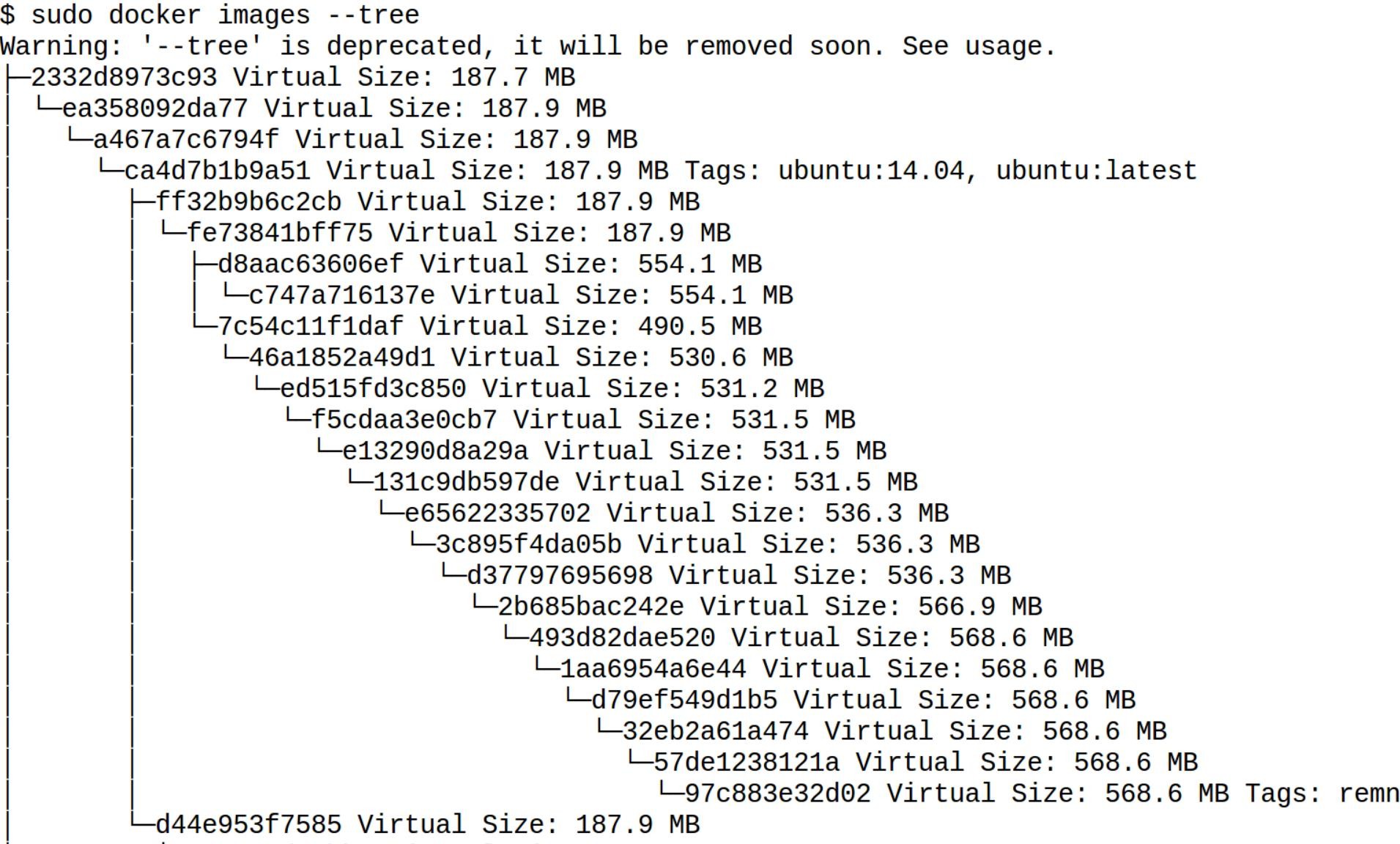
A union mount allows multiple file systems to be mounted and appear as a single file system.

Thug

V8, Python, libemu, ssdeep, etc.

Ubuntu 14.04

23

Images based on the same layers

occupy less disk space.

24

Balance efficiency and readability

25

when crafting the Dockerfile.

Chain commands into a single RUN instruction to remove files before a layer is committed.

…

rm -rf /var/lib/apt/lists/\* && \

pip install -q jsbeautifier \ rarfile \

beautifulsoup4 \ pefile \

six && \

groupadd -r thug && \

useradd -r -g thug -d /home/thug -s /sbin/nologin -c "Thug User" thug

Avoid saving files to the file system

to help minimize disk space.

Don’t bother removing files after the layer has been already committed (e.g., “apt-get clean”).

…

curl -SL http:// … /files/ssdeep-2.12/ssdeep-2.12.tar.gz/download | \

tar -xzC . && \

cd ssdeep-2.12 && \

./configure && \ make install && \ cd .. && \

rm -rf ssdeep-2.12 && \ BUILD\_LIB=1 pip install ssdeep && \ chown -R thug:thug /home/thug

Don’t run commands as “root”

unless you really need to.

* That’s why we created user “thug”.
* Use “USER” to specify which user account to use for subsequent commands.
* Understand “ENV”, “WORKDIR” and “CMD” Dockerfile directives.

USER thug

ENV HOME /home/thug

ENV USER thug

WORKDIR /home/thug/src CMD ["./thug.py"]

Use “docker build” to build the

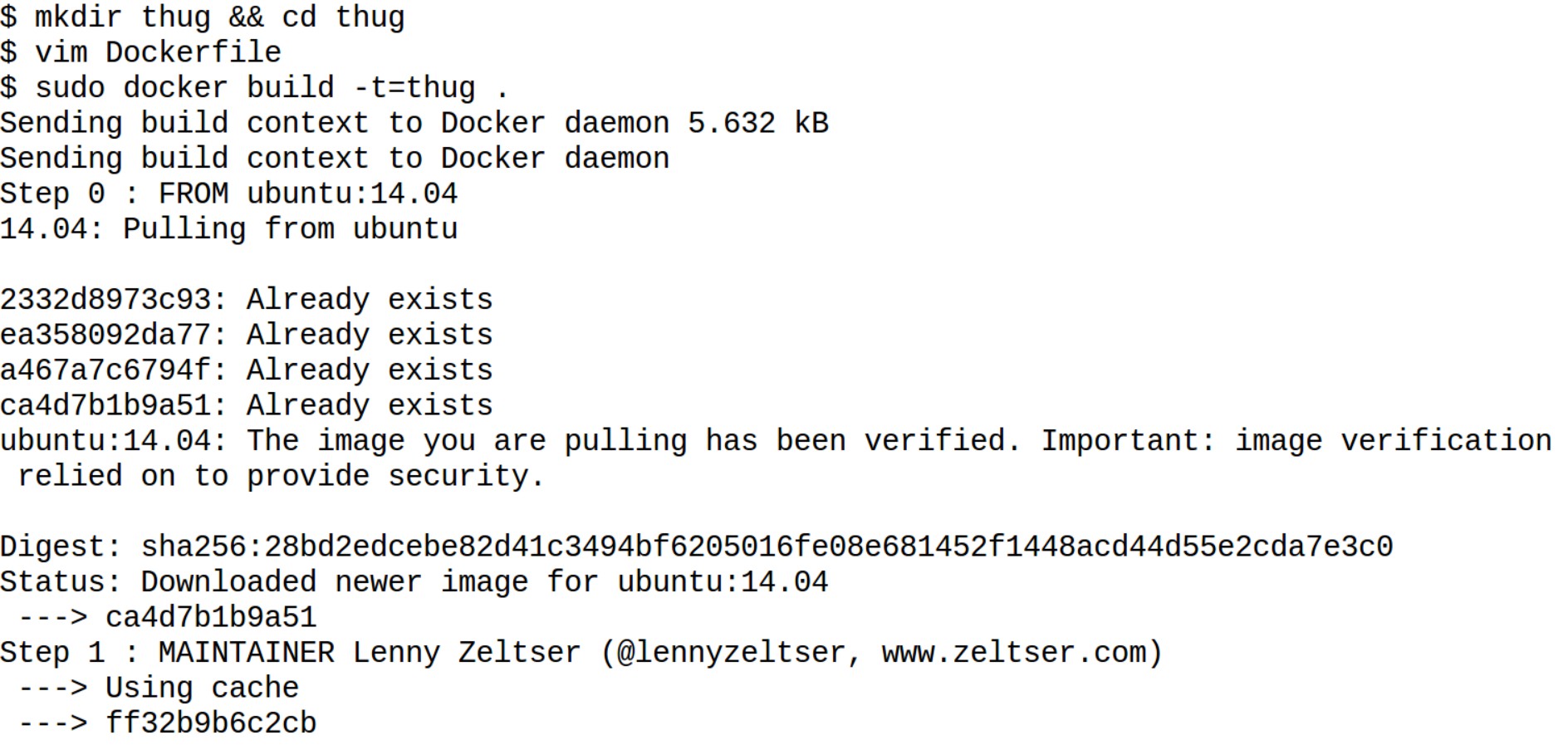


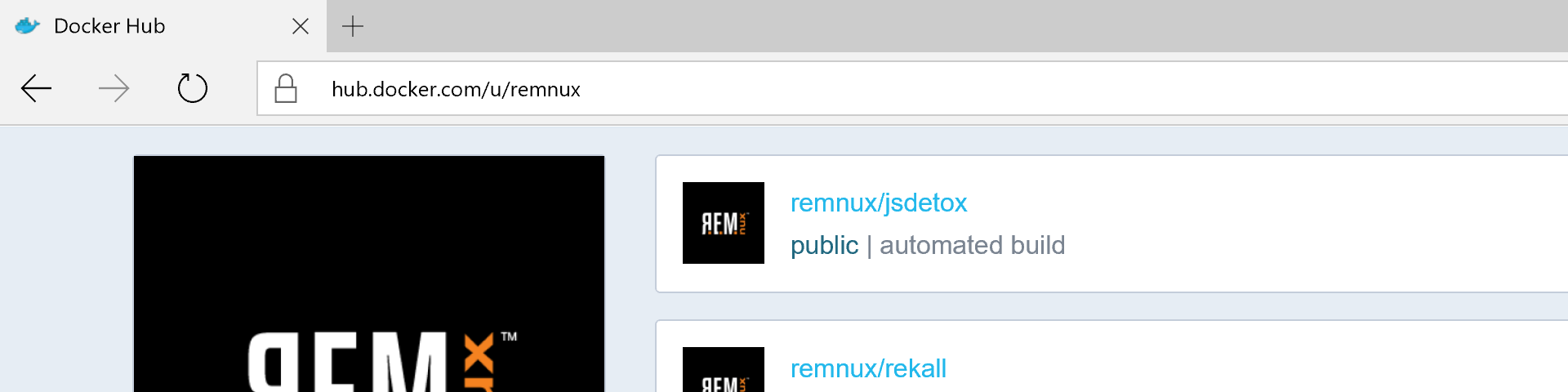
image out of the Dockerfile.

Assign it a name using “-t=*image-name* .”

Use “docker images” and “docker rmi”



to list and remove images.

Share your images via the public

Docker Hub registry.

* Create a repository on registry.hub.docker.com
* Save images to the repository using the “docker push” command.
* Better yet store your Dockerfile files on Github or BitBucket and create an Automated Build.

We Just Discussed



File system layers Dockerfile syntax Optimizing image size Building an app image

Listing and removing images Sharing your images



# Conclusions and Wrap-Up

32

Docker containers offer a convenient

app distribution mechanism.

* Containers are growing in popularity.
* They will follow an evolution path similar to that virtualization and VLANs.
* The REMnux collection provides several images useful for malware analysis.
* Experiment, learn, contribute.

https://remnux.org/docs/containers/malware-analysis

33

If interested in malware analysis, take

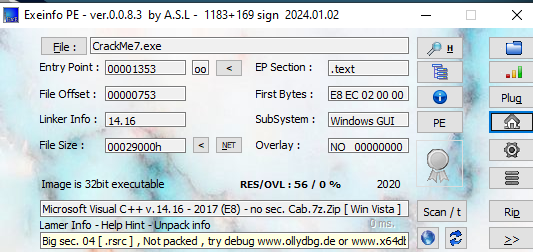
a look at the FOR610 course at SANS.

* + Visit LearnREM.com
  + Course offered at SANS conferences and on-line
  + 10% discount code “SANSLZ”
  + @lennyzeltser and zeltser.com

34

**CrackMe7**

Kiểm tra thông tin file bằng tool ExeInfo Pe. Ta thấy đây là file được viết bằng C++ và là file 32bit



Chương trình này khá đơn giản. Nó mov 2 vào eax và kiểm tra nó.

A screenshot of a computer

Description automatically generated

Em đã đổi lên lệnh jump từ jz thành jmp. Và ta có

A screenshot of a computer

Description automatically generated