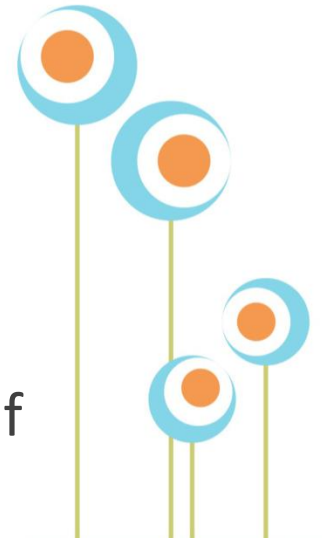
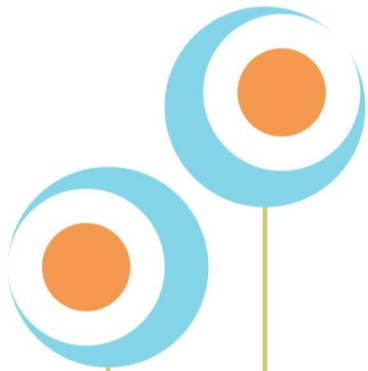


# Docker Containers for Malware Analysis

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.



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.

# What Are Docker Application Containers?

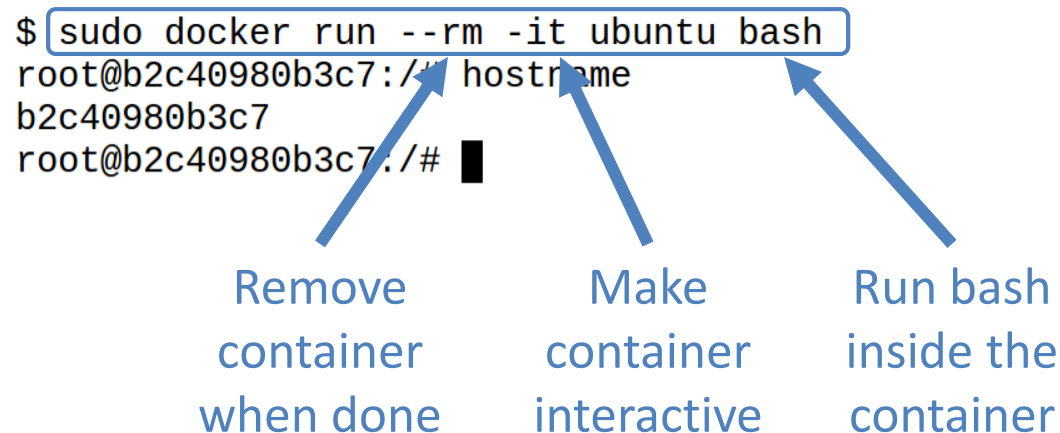
# Docker is software and an ecosystem for application containers.

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

```
$ sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  btrfs-tools debootstrap lxc rinse
The following NEW packages will be installed:
  docker.io
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.
Need to get 4,749 kB of archives.
After this operation, 29.1 MB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/ trusty-updates/universe docker.io amd64 1.6.2~c
Fetched 4,749 kB in 7s (676 kB/s)
Selecting previously unselected package docker.io.
(Reading database ... 133218 files and directories currently installed.)
Preparing to unpack .../docker.io_1.6.2~dfsg1-1ubuntu4~14.04.1_amd64.deb ...
```

# Docker maintains the Docker Hub Registry of public app images.

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



# A Docker image of an app contains the software and its dependencies.

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

```
$ sudo docker run --rm -it remnux/thug bash
Unable to find image 'remnux/thug:latest' locally
latest: Pulling from remnux/thug
```

```
428b411c28f0: Downloading [> ] 539.6 kB/
435050075b3f: Download complete
9fd3c8c9af32: Download complete
6d4946999d4f: Download complete
8a9ba9ab6104: Download complete
ee16d7fd9ce9: Download complete
8b738260758d: Downloading [> ] 1.068 MB/
73b4a72be805: Download complete
3375c26d52c1: Downloading [====> ] 1.327 MB/
```



A container gets its own file system, process listing and network stack.

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

```
$ sudo docker run --rm -it remnux/thug bash
thug@3d01bd39c553:~/src$ ./thug.py -F http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0jYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
[2015-12-01 16:24:02] [WARNING] Androguard not found - APK analysis disabled
[2015-12-01 16:24:03] [window open redirection] about:blank -> http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0jYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
Dwvc3Bhbj48YnI/ZDZkZjI2M2M3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
[2015-12-01 16:24:04] [HTTP] URL: http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0jYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/ (Status: 403, Referer: None)
[2015-12-01 16:24:04] [HTTP] URL: http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0jYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/ (Content-type: text/html; charset=iso-8859-1,
[2015-12-01 16:24:04] Thug analysis logs saved at ../logs/2314c49469105f6ccfa308aafdfb5628
thug@3d01bd39c553:~/src$
```



# 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

# 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.

```
$ mkdir logs && chmod a+xwr logs
$ sudo docker run --rm -it -v ~/logs:/home/thug/logs remnux/thug bash
thug@f06f5d87e727:~/src$ ./thug.py -F http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
[2015-12-01 17:11:47] [WARNING] Androguard not found - APK analysis disabled
[2015-12-01 17:11:48] [window open redirection] about:blank -> http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
Dwvc3Bhbj48YnI/ZDZkZjI2M2M3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
[2015-12-01 17:11:49] [HTTP] URL: http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/ (Status: 403, Referer: None)
[2015-12-01 17:11:49] [HTTP] URL: http://lnx.iwa3a.it/c2l6ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFjMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/ (Content-type: text/html; charset=iso-8859-1,
[2015-12-01 17:11:49] Thug analysis logs saved at ../logs/2314c49469105f6ccfa308aafdfb5628
thug@f06f5d87e727:~/src$ exit
exit
$ ls logs
2314c49469105f6ccfa308aafdfb5628  thug.csv
$ █
```





```
viper > store --folder ../workdir --file-type PE32
[*] Session opened on /home/nonroot/workdir/binaries/e/8/f/c/e8fcd05758a8e1a4bf945f4913e10
[*] Running Command yara scan -t
[*] Session opened on /home/nonroot/workdir/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738
[*] Running Command yara scan -t
[*] Session opened on /home/nonroot/workdir/binaries/2/0/7/8/20789eadfd97e38238579419e05a4
[*] Running Command yara scan -t
[*] Session opened on /home/nonroot/workdir/binaries/9/d/a/0/9da0a02de59b991aa305f90add977
[*] Running Command yara scan -t
```

```
viper > find all
```

#	Name	Mime	MD5	Tag
1	gtk1.exe	application/x-dosexec	639819ee45daaa30e53d066938cb72ad	
2	grabber.exe	application/x-dosexec	ca39d7cd301e61f0a01bda488af8f5fb	
3	jhg26ff.sys	application/x-dosexec	cd58eb1e49a088854b0d463d6b6a957b	
4	ritaglio_unpack.dll	application/x-dosexec	ca438d4b536ef02ad0abe2860ff789c5	

```
viper > open ca39d7cd301e61f0a01bda488af8f5fb
```

```
[*] Session opened on /home/nonroot/workdir/binaries/0/8/e/8/08e858ca0e6a1e8bdb965400f9738
```

```
viper grabber.exe > virustotal
```

```
[*] VirusTotal Report:
```

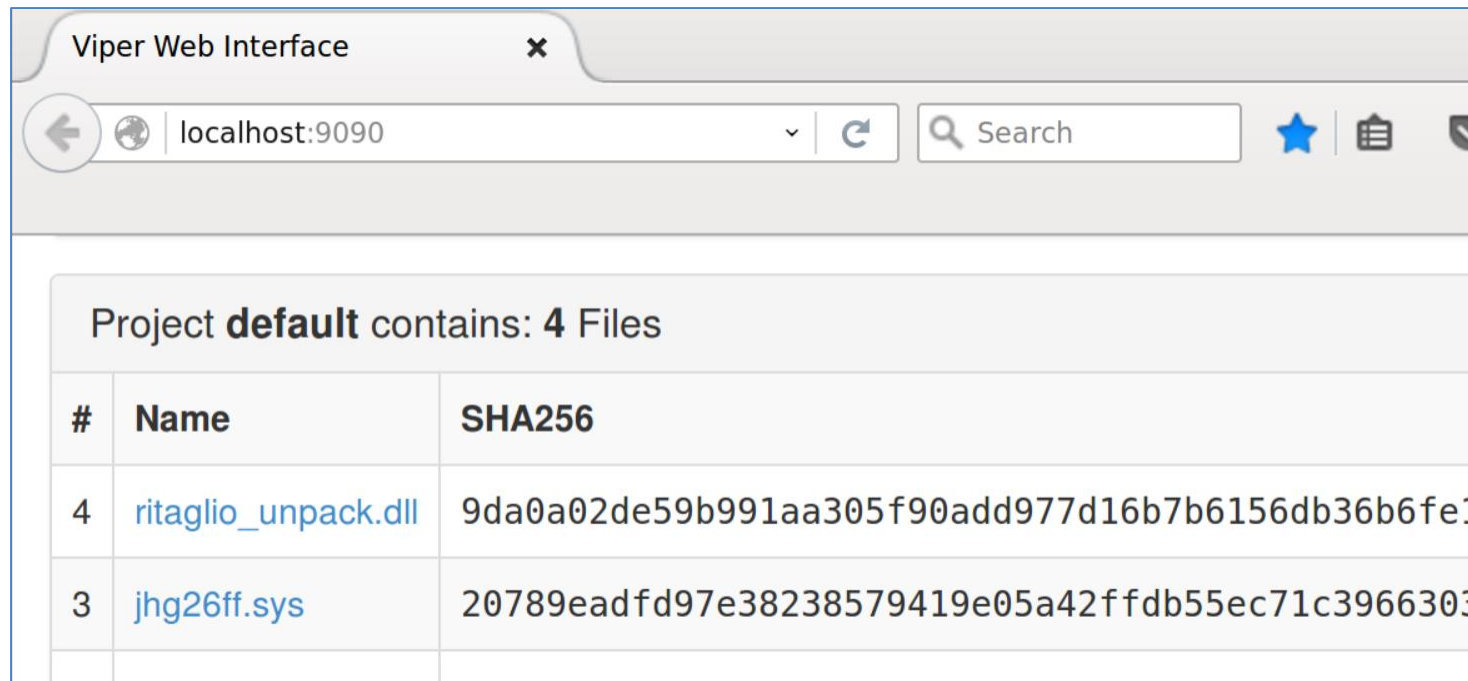
Antivirus	Signature
AVG	Dropper.Generic2.PWD
AhnLab-V3	Win-Trojan/Gootkit.255128
AntiVir	TR/Dropper.Gen
Antiy-AVL	Backdoor/Win32.Gootkit.gen
Avast	Win32:Malware-gen
Avast5	Win32:Malware-gen
BitDefender	Trojan.Generic.KD.14665
CAT-QuickHeal	Backdoor.Gootkit.a

```
$ ls
about.txt
agressive.exe
binaries
gootkit.zip
grabber.exe
gtk1.exe
history
jhg26ff.sys
ritaglio_unpack.dll
viper.db
```

# Use “-p” to access network ports within a container.

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

```
$ sudo docker run --rm -p 9090:9090 -v ~/samples:/home/nonroot/workdir remnux/viper
Bottle v0.12.9 server starting up (using WSGIRefServer())...
Listening on http://a0098c197097:9090/
Hit Ctrl-C to quit.
```



Viper Web Interface

localhost:9090

Project **default** contains: 4 Files

#	Name	SHA256
4	<a href="#">ritaglio_unpack.dll</a>	9da0a02de59b991aa305f90add977d16b7b6156db36b6fe1
3	<a href="#">jhg26ff.sys</a>	20789eadfd97e38238579419e05a42ffdb55ec71c3966303

# 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.

```
$ sudo docker ps
CONTAINER ID   IMAGE                                COMMAND                                CREATED
STATUS        PORTS                                NAMES
a0098c197097  remnux/viper:latest                "/bin/sh -c './web.p                 5 minutes ago
Up 5 minutes   0.0.0.0:9090->9090/tcp              cranky_bartik
$ sudo docker stop cranky_bartik
cranky_bartik
$ █
```

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

# 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.

```
$ ls -l
total 1372
-rw-rw-r-- 1 remnux remnux    99 Jan  4  2015 about.txt
-rw-rw-r-- 1 remnux remnux 159264 Jun 20  2010 aggressive.exe
drwxr-x--- 6    999    999   4096 Dec  1 12:51 binaries
-rw-rw-r-- 1 remnux remnux 518842 Jun 12 12:36 gootkit.zip
-rw-rw-r-- 1 remnux remnux 258048 Jun  2  2010 grabber.exe
-rw-rw-r-- 1 remnux remnux 117760 Jun  8  2010 gtk1.exe
-rw----- 1    999    999   101 Dec  1 12:59 history
```

# 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



# 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>

# Docker images in the REMnux 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)

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

# Images based on the same layers occupy less disk space.

```
$ sudo docker images --tree
```

```
Warning: '--tree' is deprecated, it will be removed soon. See usage.
```

```
├─2332d8973c93 Virtual Size: 187.7 MB
  └─ea358092da77 Virtual Size: 187.9 MB
    └─a467a7c6794f Virtual Size: 187.9 MB
      └─ca4d7b1b9a51 Virtual Size: 187.9 MB Tags: ubuntu:14.04, ubuntu:latest
        └─ff32b9b6c2cb Virtual Size: 187.9 MB
          └─fe73841bff75 Virtual Size: 187.9 MB
            └─d8aac63606ef Virtual Size: 554.1 MB
              └─c747a716137e Virtual Size: 554.1 MB
            └─7c54c11f1daf Virtual Size: 490.5 MB
              └─46a1852a49d1 Virtual Size: 530.6 MB
                └─ed515fd3c850 Virtual Size: 531.2 MB
                  └─f5cdaa3e0cb7 Virtual Size: 531.5 MB
                    └─e13290d8a29a Virtual Size: 531.5 MB
                      └─131c9db597de Virtual Size: 531.5 MB
                        └─e65622335702 Virtual Size: 536.3 MB
                          └─3c895f4da05b Virtual Size: 536.3 MB
                            └─d37797695698 Virtual Size: 536.3 MB
                              └─2b685bac242e Virtual Size: 566.9 MB
                                └─493d82dae520 Virtual Size: 568.6 MB
                                  └─1aa6954a6e44 Virtual Size: 568.6 MB
                                    └─d79ef549d1b5 Virtual Size: 568.6 MB
                                      └─32eb2a61a474 Virtual Size: 568.6 MB
                                        └─57de1238121a Virtual Size: 568.6 MB
                                          └─97c883e32d02 Virtual Size: 568.6 MB Tags: remn
└─d44e953f7585 Virtual Size: 187.9 MB
```

# Balance efficiency and readability 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* .”

```
$ mkdir thug && cd thug
$ vim Dockerfile
$ sudo docker build -t=thug .
Sending build context to Docker daemon 5.632 kB
Sending build context to Docker daemon
Step 0 : FROM ubuntu:14.04
14.04: Pulling from ubuntu
2332d8973c93: Already exists
ea358092da77: Already exists
a467a7c6794f: Already exists
ca4d7b1b9a51: Already exists
ubuntu:14.04: The image you are pulling has been verified. Important: image verification
relied on to provide security.

Digest: sha256:28bd2edcebe82d41c3494bf6205016fe08e681452f1448acd44d55e2cda7e3c0
Status: Downloaded newer image for ubuntu:14.04
---> ca4d7b1b9a51
Step 1 : MAINTAINER Lenny Zeltser (@lennyzeltser, www.zeltser.com)
---> Using cache
---> ff32b9b6c2cb
```

# Use “docker images” and “docker rmi” to list and remove images.

```
remnux@remnux:~/thug$ sudo docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	VIRTUAL SI
thug	latest	a7bf7eadb188	16 minutes ago	595.2 MB
remnux/viper	latest	97c883e32d02	6 hours ago	568.6 MB
ubuntu	14.04	ca4d7b1b9a51	3 weeks ago	187.9 MB
ubuntu	latest	ca4d7b1b9a51	3 weeks ago	187.9 MB
remnux/thug	latest	e93f932d121b	5 months ago	584.7 MB

```
remnux@remnux:~/thug$ sudo docker rmi thug
```

```
Untagged: thug:latest
```

```
Deleted: a7bf7eadb188e807c7d6ec99b93bc2f0d3691446982ecffa5444255fc84018ee
```

```
Deleted: 62d7cdc5740d7ef17b7725a38917aa0a45d2b9a22fb3875b225bde7927e0e294
```

```
Deleted: 67641b1b8c226384c21ef094bbd75cf6e535d15d93b9ab1337ba0bfbf3b12000
```

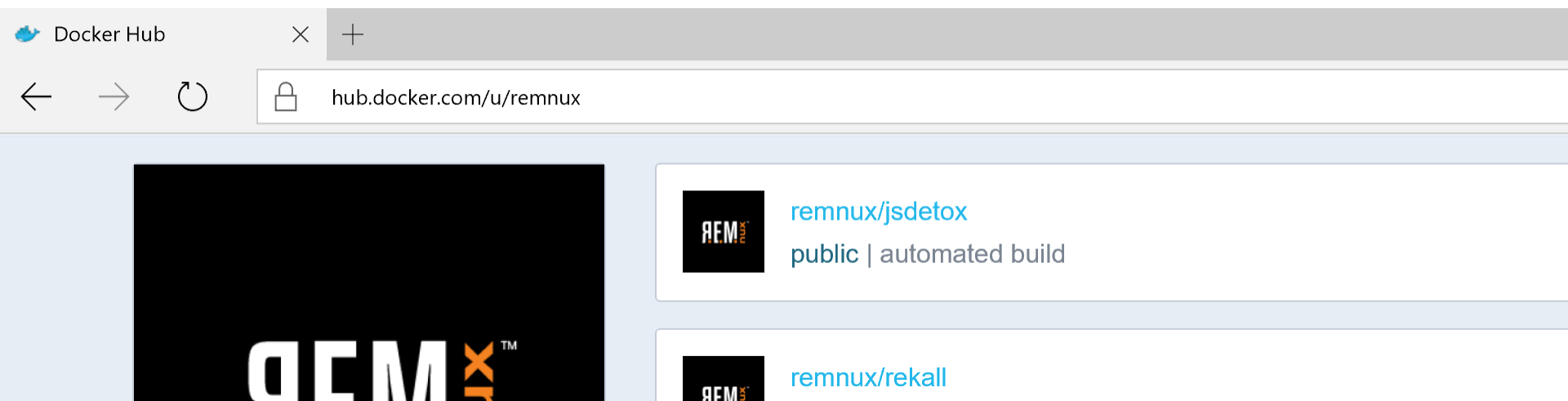
```
Deleted: 8b3444dbc594d1d8840231323ec486aef366a2fca5439b008a179b3c9277621d
```

```
Deleted: d93bf03fb482f97af3724964f8dab6c3d15dc878a8719c941aab1bb2faca139d
```

```
remnux@remnux:~/thug$ █
```

# 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

# 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>



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

Download and these slides from  
<https://zeltser.com/media/archive/docker.pdf>