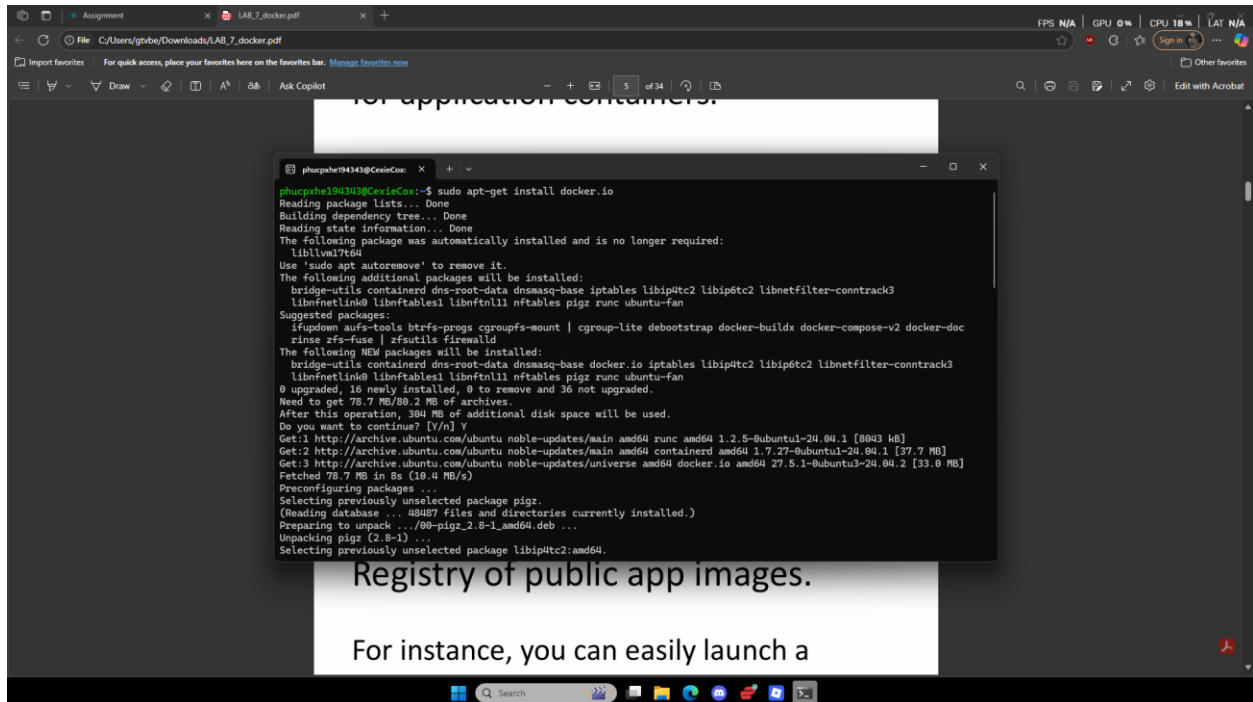


Lab 7

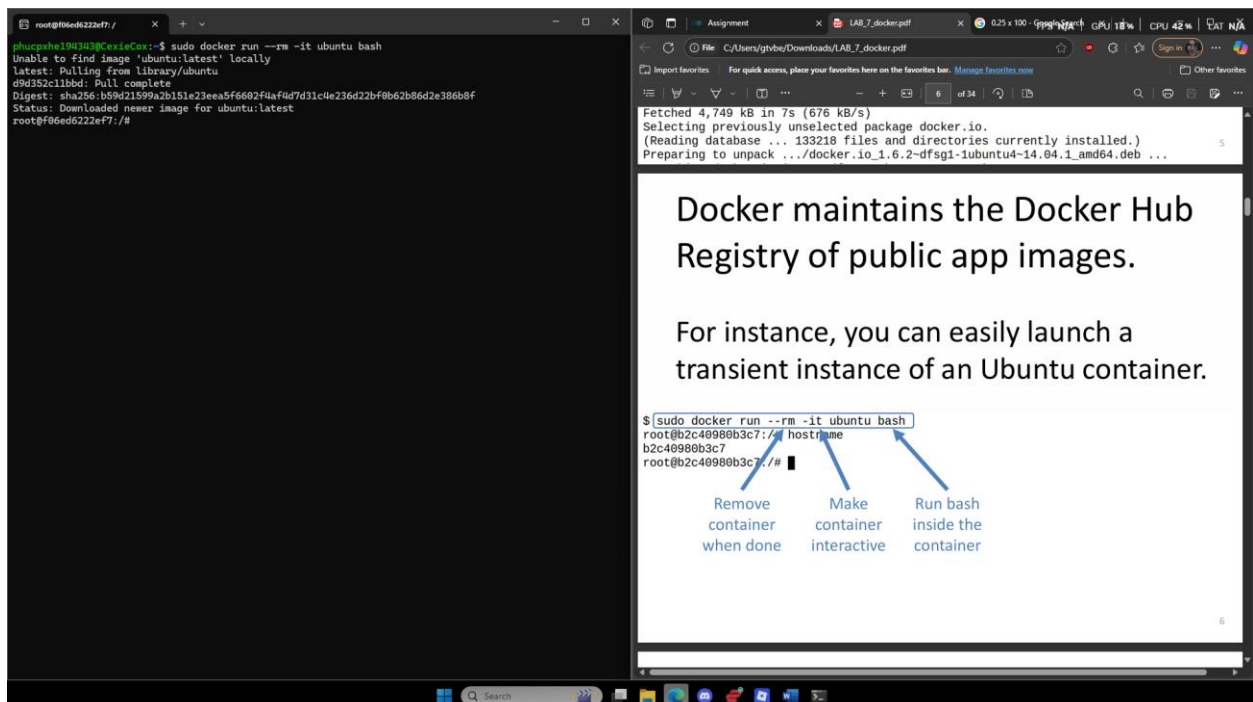


For application containers.

```
phucp@ph194343@CecileCox:~$ sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  liblvm2t64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base iptables libip6tc2 libip6tc2 libnetfilter-contrack3
  libnetfilter-nftables libnftnl1 nftables pigz runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools btrfs-progs cgroupfs-mount | cgroup-lite debstrap docker-buildx docker-compose-v2 docker-doc
  zfs-zfs-utils | zfsutils firewall
The following NEW packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base docker.io iptables libip6tc2 libip6tc2 libnetfilter-contrack3
  libnetfilter-nftables libnftnl1 nftables pigz runc ubuntu-fan
0 upgraded, 16 newly installed, 0 to remove and 36 not upgraded.
Need to get 78.7 MB/88.2 MB of archives.
After this operation, 384 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 runc amd64 1.2.5-0ubuntu1-24.04.1 [8043 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 containerd amd64 1.7.27-0ubuntu1-24.04.1 [37.7 MB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 docker.io amd64 27.5.1-0ubuntu3-24.04.2 [33.0 MB]
Fetched 78.7 MB in 8s (10.4 MB/s)
Preconfiguring packages ...
Selecting previously unselected package pigz.
(Reading database ... 48487 files and directories currently installed.)
Preparing to unpack .../00-pigz_2.8-1_amd64.deb ...
Unpacking pigz (2.8-1) ...
Selecting previously unselected package libip6tc2:amd64.
```

Registry of public app images.

For instance, you can easily launch a



```
root@f06e6222ef7:/$ sudo docker run --rm -it ubuntu bash
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
d9d352c11bbd: Pull complete
Digest: sha256:b59d21599a2b151e23ee5f6682f4cf4d7d31cde236d22bf9b62b86d2e386b8f
Status: Downloaded newer image for ubuntu:latest
root@f06e6222ef7:/#
```

Docker maintains the Docker Hub Registry of public app images.

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

```
$ sudo docker run --rm -it ubuntu bash
root@b2c40980b3c7:/# hostname
b2c40980b3c7
root@b2c40980b3c7:/#
```

Remove container when done

Make container interactive

Run bash inside the container

```
thug@6210e831f72:~$ docker run --rm -it --entrypoint /bin/bash remnux/thug
phucpsh1943d3@CecieCox:~$ sudo docker run --rm -it --entrypoint /bin/bash remnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
thug@6210e831f72:~$
```

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/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODg4ZjUxMjFiZTU=/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/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/
[2015-12-01 16:24:04] [HTTP] URL: http://lnx.iwa3a.it/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/ (Status: 403, Referer: None)
[2015-12-01 16:24:04] [HTTP] URL: http://lnx.iwa3a.it/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODg4ZjUxMjFiZTU=/Redirection/ (Content-type: text/html; charset=iso-8859-1)
[2015-12-01 16:24:04] Thug analysis logs saved at ../logs/2314c49469195f6ccfa308aafdfb5
thug@3d01bd39c553:~/src$
```

Malware analysis apps as Docker containers offer several benefits.

- Apps with conflicting dependencies can

```
phucpsh1943d3@CecieCox:~$ sudo docker run --rm -it remnux/thug bash
Unable to find image 'remnux/thug:latest' locally
latest: Pulling from remnux/thug
3f701d9643d3: Pull complete
58597f06a896: Downloading [148.5MB/324.2MB]
5fea02d83833: Download complete
4f4fb700ef54: Download complete
d79e75a06114: Download complete
4a7be68f63db: Download complete
a27996c209d6: Downloading [19.25MB/33.72MB]
85ce9ebd4b5c: Download complete
```

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

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

However, containers share the OS kernel

```
thug@4f609f418fe9:~$ docker run --rm -it --entrypoint /bin/bash remnux/thug
phucpkhe194343@CexieCox:~$ docker run --rm -it --entrypoint /bin/bash remnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

thug@6210e8311f72:~$ exit
exit
phucpkhe194343@CexieCox:~$ sudo docker run --rm -it -v ~/logs:/home/thug/logs \ --entrypoint /bin/bash
h \ remnux/thug
docker: invalid reference format.
See 'docker run --help'.
phucpkhe194343@CexieCox:~$ sudo docker run --rm -it -v ~/logs:/home/thug/logs --entrypoint /bin/bash r
emnux/thug
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

thug@4f609f418fe9:~$
```

Use “-v” to map the host’s directory into the container.

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

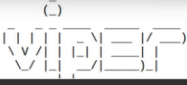
```
$ mkdir logs && chmod a+wxr logs
$ sudo docker run --rm -it -v ~/logs:/home/thug/logs remnux/thug bash
thug@f06f5d87e727:~/src$ ./thug.py -F http://lnx.iwa3a.it/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODQ4ZjUxMjFiZTU=/Redirection/
[2015-12-01 17:11:47] [WARNING] Androguard not found - APK analysis disabled
[2015-12-01 17:11:48] [window open redirection] about:blank -> http://lnx.iwa3a.it/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODQ4ZjUxMjFiZTU=/Redirection/
[2015-12-01 17:11:49] [HTTP] URL: http://lnx.iwa3a.it/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODQ4ZjUxMjFiZTU=/Redirection/ (Status: 403, Referer: None)
[2015-12-01 17:11:49] [HTTP] URL: http://lnx.iwa3a.it/c216ZToxMHB402ZvbnQtd2VpZ2h0OjYwM3MTQ0NWFiMTg4ZmMxODQ4ZjUxMjFiZTU=/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
$
```

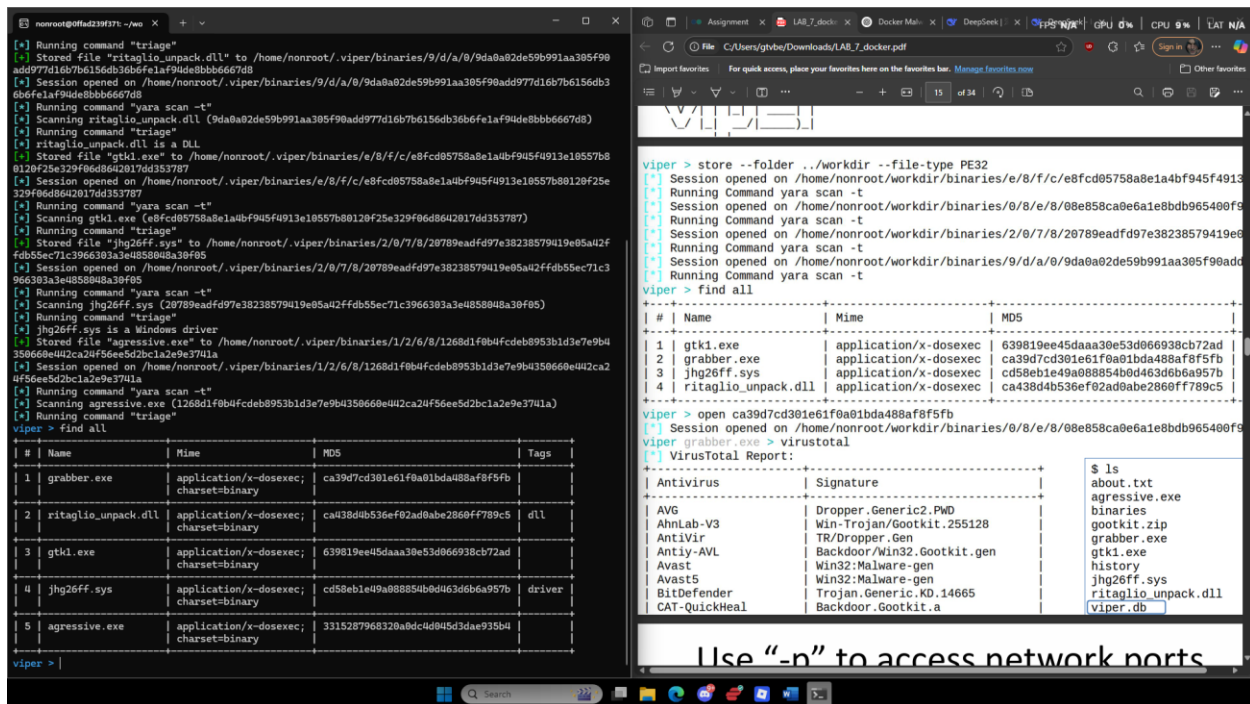
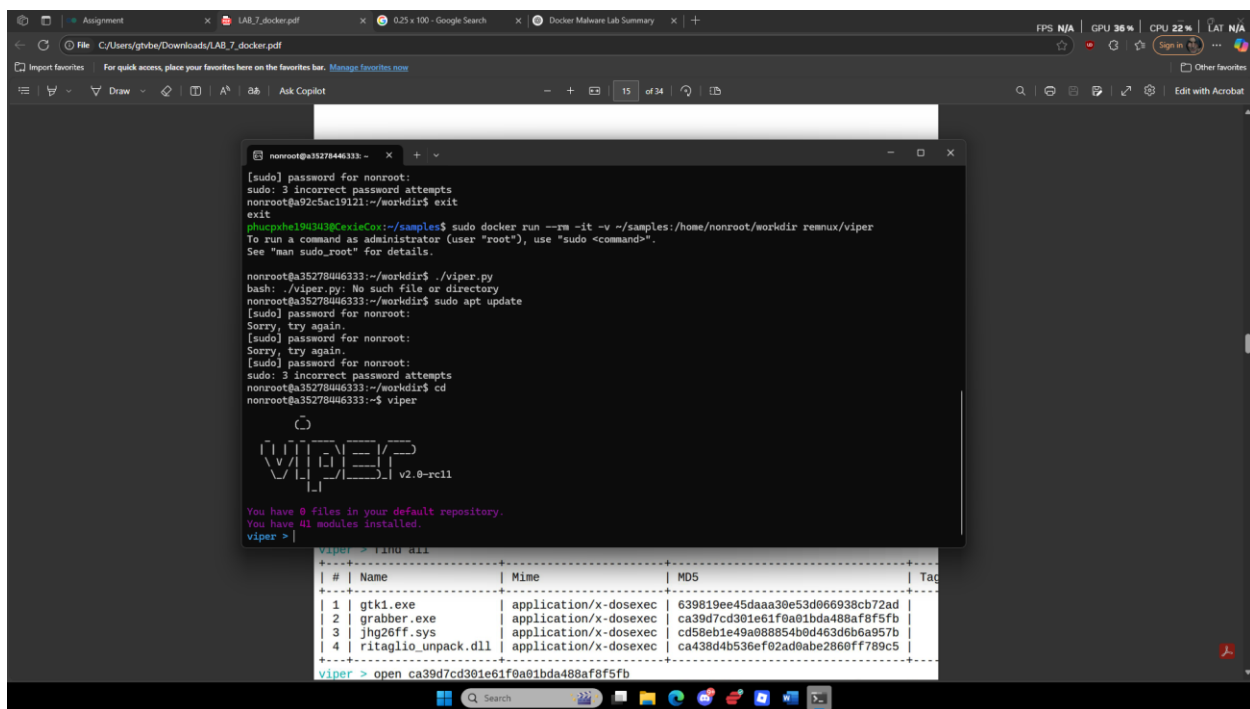
The use of containers encourages separating “code” from “data”

```
$ ls logs
2314c49469105f6ccfa308aafdfb5628 thug.csv
```

```
phucpkhe194343@CexieCox:~$ mkdir ~/samples && chmod a+rx ~/samples && cd ~/samples
phucpkhe194343@CexieCox:~/samples$ wget -q https://zeltser.com/media/archive/gootkit.zip
phucpkhe194343@CexieCox:~/samples$ unzip gootkit.zip
Archive: gootkit.zip
[gootkit.zip] about.txt password:
  inflating: about.txt
  inflating: aggressive.exe
  inflating: grabber.exe
  inflating: gtk1.exe
  inflating: jhg26ff.sys
  inflating: ritaglio_unpack.dll
phucpkhe194343@CexieCox:~/samples$ sudo docker run --rm -it \
> -v ~/samples:/home/nonroot/workdir \
> -c
phucpkhe194343@CexieCox:~/samples$ sudo docker run --rm -it \
-v ~/samples:/home/nonroot/workdir \
--entrypoint /bin/bash \
remnux/viper
Unable to find image 'remnux/viper:latest' locally
latest: Pulling from remnux/viper
7b1a6ab2e44d: Pull complete
052ef27ccfb9: Extracting [=====] 145.9MB/158.3MB
1cad993a4076: Download complete
3f8b9f6758a0: Download complete
4f4fb708ef54: Download complete
4ee2ccd17c9f: Download complete
128ea499a907: Download complete
6cf9f8abec6: Downloading [====] 2.153MB/177MB
```

```
nonroot@d5e475e8c597:~/viper$ ./viper.py
```





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

```
phucpsh194343@CexieCox:~/thug_project/thug$ cat Dockerfile
FROM ubuntu:20.04

LABEL maintainer="OpenAI / based on original by Lenny Zeltser"

ENV DEBIAN_FRONTEND=noninteractive

# Cài các gói hệ thống và Python 2.7
RUN apt-get update && \
    apt-get install -y --no-install-recommends \
        python2 \
        python2-dev \
        curl \
        build-essential \
        libfuzzy-dev \
        automake \
        autoconf \
        wget \
        ca-certificates \
        git && \
    apt-get clean && \
    rm -rf /var/lib/apt/lists/*

# Cài pip cho Python 2.7
RUN curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o get-pip.py && \
    python2 get-pip.py && \
    rm get-pip.py

# Cài các thư viện Python cần cho Thug
RUN pip install --trusted-host pypi.org --trusted-host files.pythonhosted.org \
```

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

occupy less disk space.

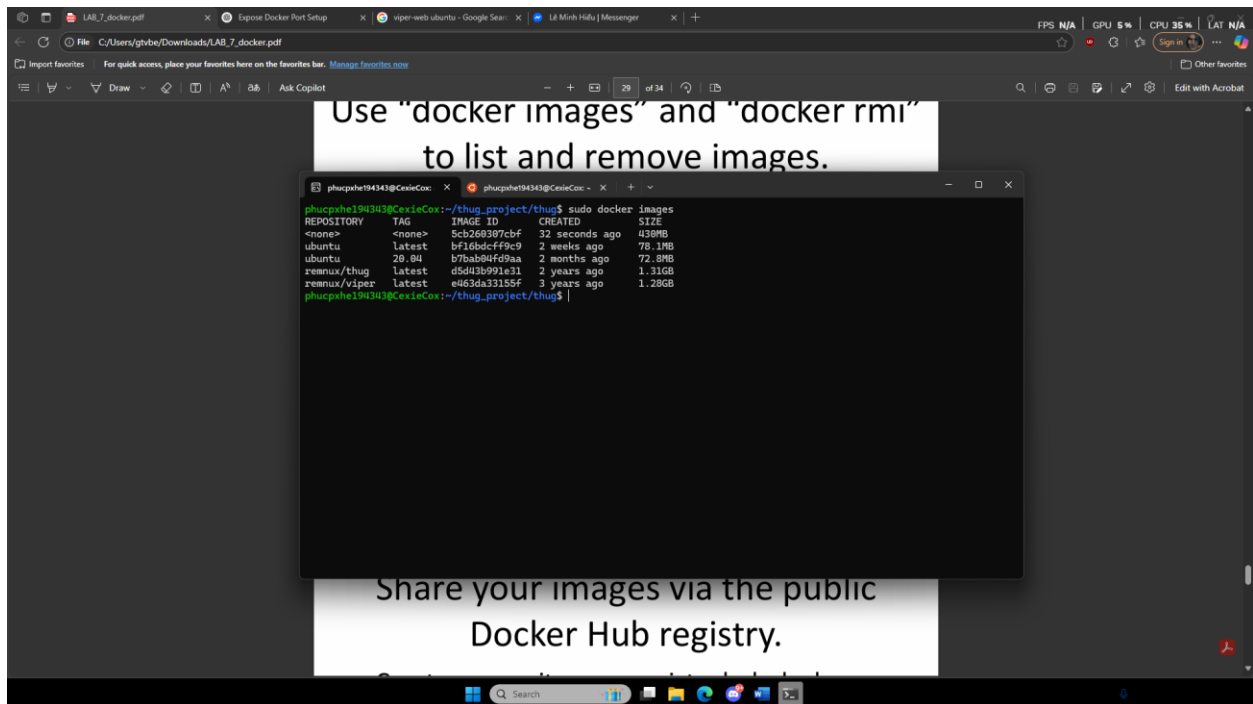
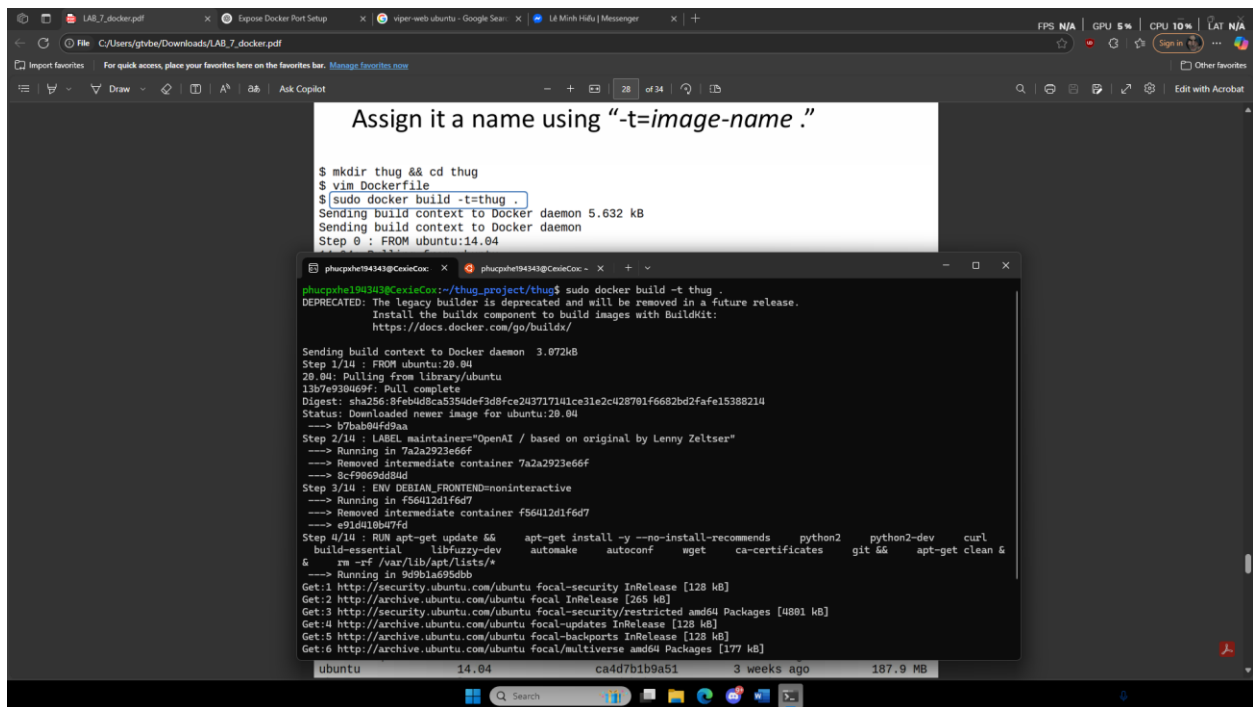
```
$ sudo docker images --tree
Warning: '--tree' is deprecated, it will be removed soon. See usage.
--232d8973c93 Virtual Size: 187.7 MB

phucpsh194343@CexieCox:~/thug_project/thug$ sudo docker images --tree
WARNING: This is an experimental feature. The output may change and shouldn't be depended on.

IMAGE          ID              DISK USAGE  CONTENT SIZE  IN USE
ubuntu:latest   bf16bdcff9c9    78.1MB      0B            0B
remnux/thug:latest d5d43b991e31    1.31GB      0B            0B
remnux/viper:latest e463da33155f    1.28GB      0B            0B
phucpsh194343@CexieCox:~/thug_project/thug$
```

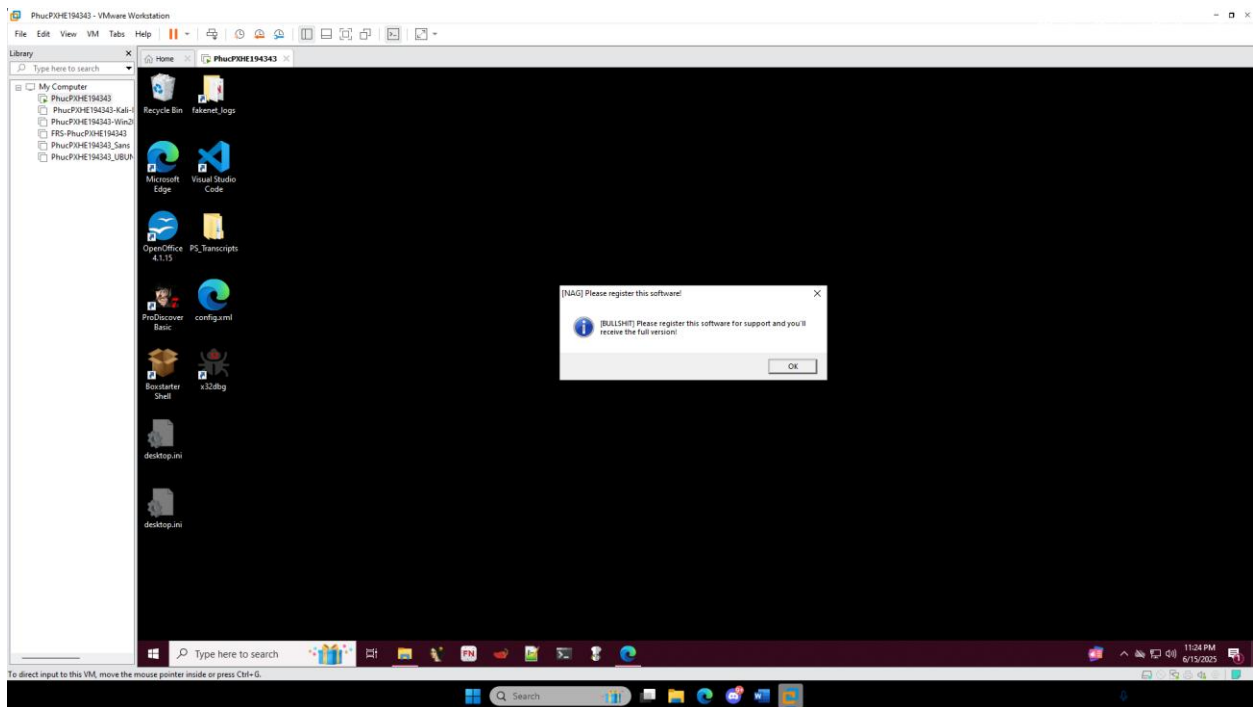
when crafting the Dockerfile.

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

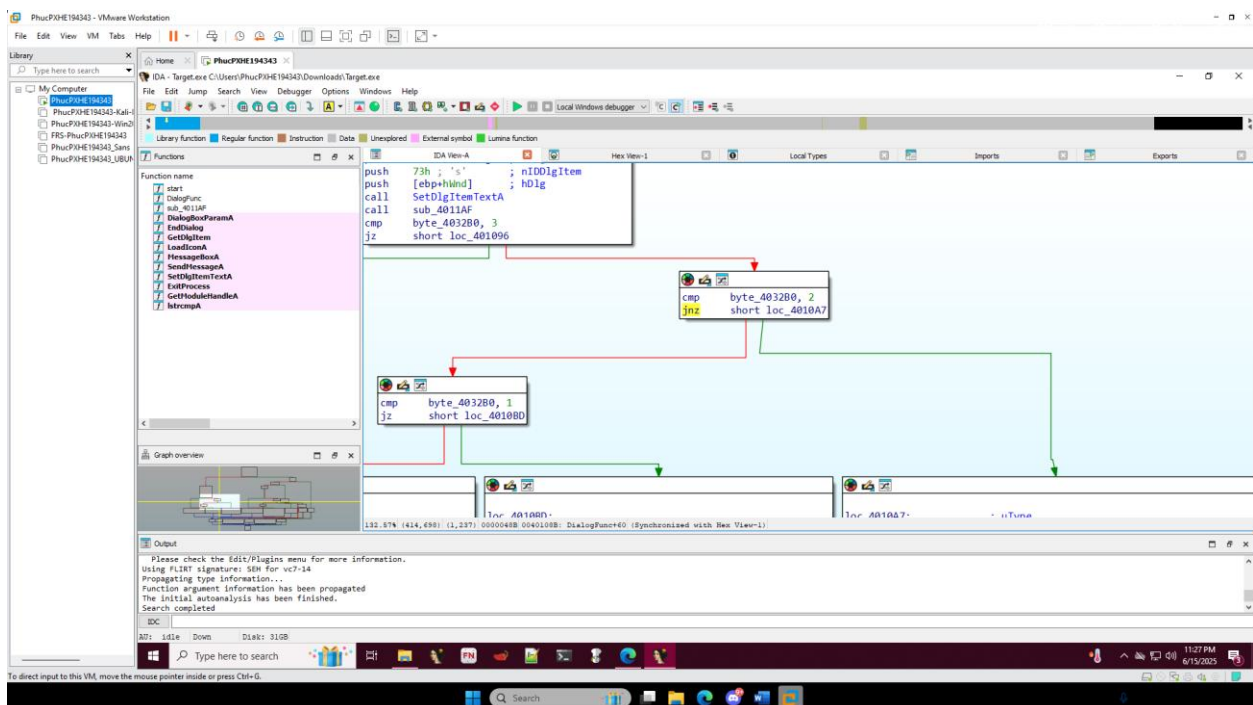


Crack me 6

Step 1: Open the exe file to check for the program



Step 2: Search for the string “BULLSHIT” and found the diagram, as we can see that the program compare the byte_4032B0 to 1, 2, 3 and the result is in the first run of the program, all we need to do to reverse the compare condition then it will run to the next case which is remove nag but dirty and clean remove nag. Reverse the condition again and we get clean remove nag



Step 3: Apply patch to the program and we see the result that we want

