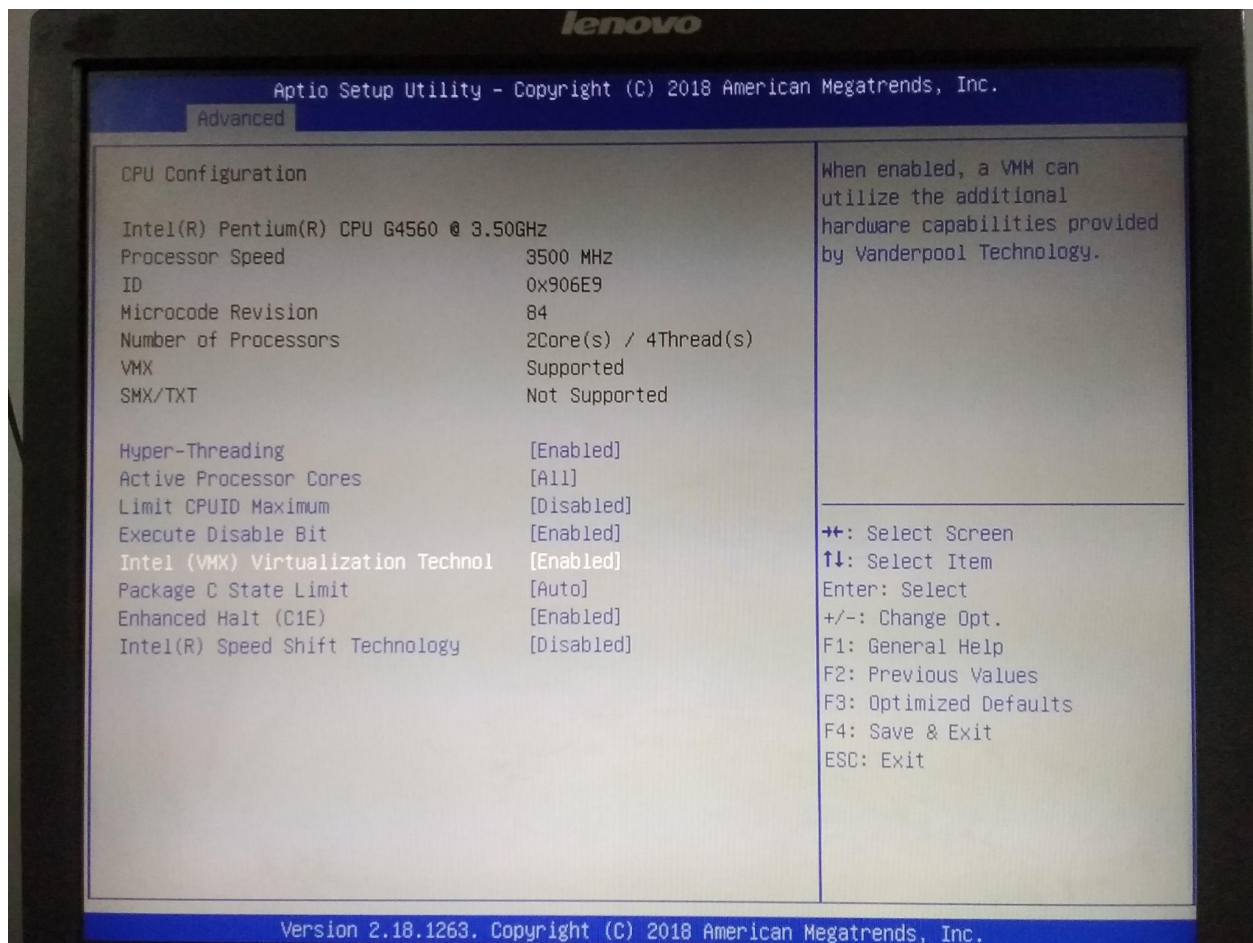


# Introduction to Zeek

## Instructions for installation of Zeek in Ubuntu 20.04

**Step 1:** We will be installing Zeek using docker. To install docker, first, we have to enable Virtualization in the BIOS. On most systems, the BIOS is accessible by pressing the F2 key or Del key on boot.

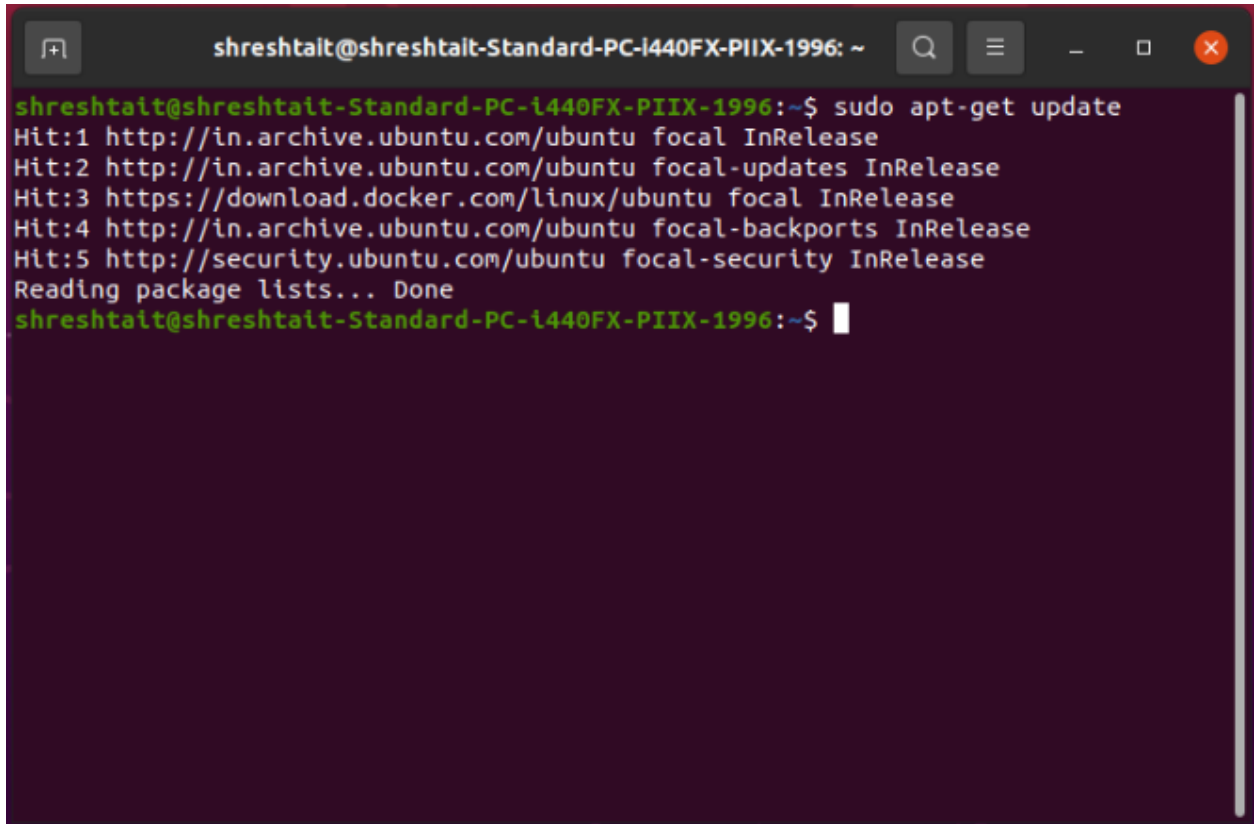


**Step 2:** Access <https://docs.docker.com/engine/install/ubuntu/> and follow the steps to install docker or follow along,

## Install docker using the official repository

**Step 1:** Open a terminal and update the repositories

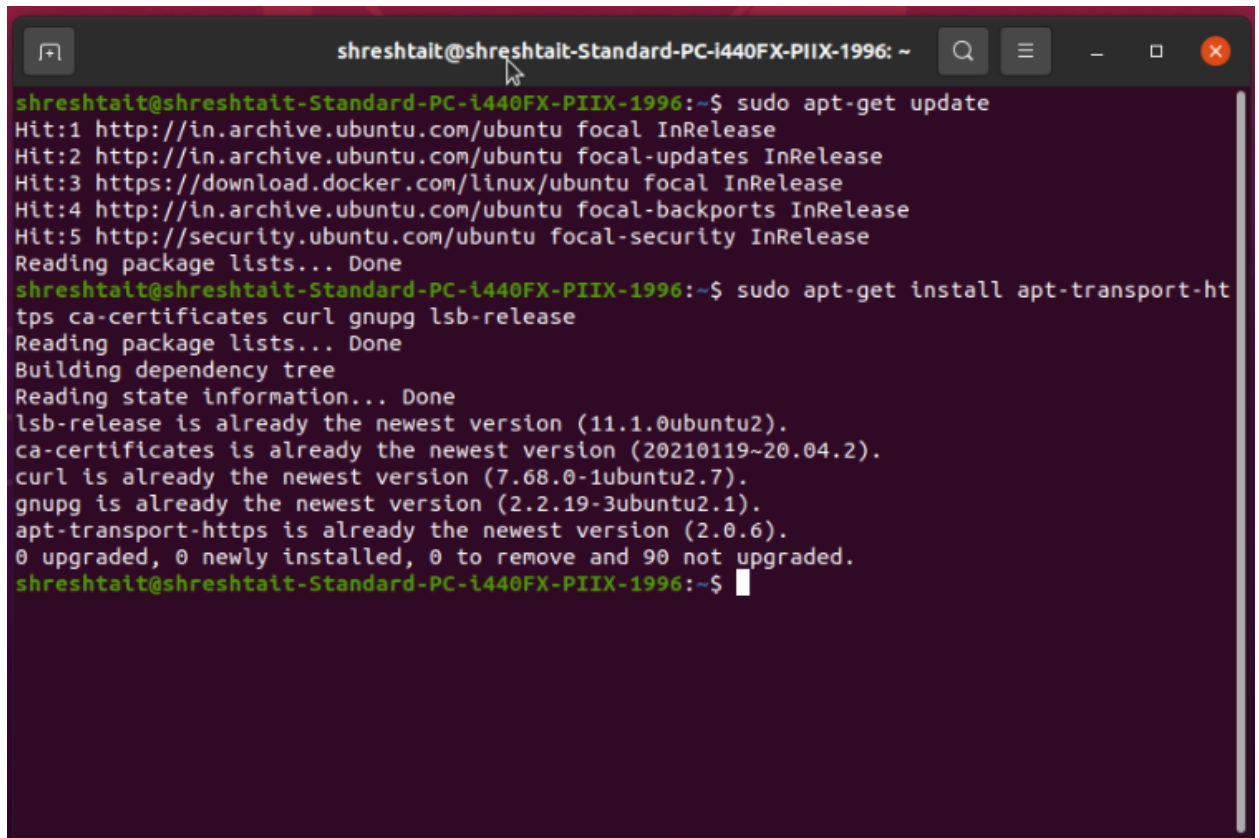
`sudo apt-get update`

A terminal window with a dark purple background. The title bar shows the user 'shreshtait' and the machine name 'shreshtait-Standard-PC-i440FX-PIIX-1996'. The terminal displays the command 'sudo apt-get update' and its output: 'Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease', 'Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease', 'Hit:3 https://download.docker.com/linux/ubuntu focal InRelease', 'Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease', 'Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease', and 'Reading package lists... Done'. The prompt returns to 'shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~\$'.

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get update  
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease  
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:3 https://download.docker.com/linux/ubuntu focal InRelease  
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease  
Reading package lists... Done  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$
```

**Step 2:** Install the dependency packages required by docker,

`sudo apt-get install apt-transport-https ca-certificates curl gnupg lsb-release`

A terminal window with a dark purple background and light green text. The window title is 'shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~'. The user has entered two commands: 'sudo apt-get update' and 'sudo apt-get install apt-transport-https ca-certificates curl gnupg lsb-release'. The output shows that several packages are already up-to-date and no new packages were installed. The terminal window has standard Ubuntu window controls at the top.

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~$ sudo apt-get update
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 https://download.docker.com/linux/ubuntu focal InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get install apt-transport-ht
tps ca-certificates curl gnupg lsb-release
Reading package lists... Done
Building dependency tree
Reading state information... Done
lsb-release is already the newest version (11.1.0ubuntu2).
ca-certificates is already the newest version (20210119~20.04.2).
curl is already the newest version (7.68.0-1ubuntu2.7).
gnupg is already the newest version (2.2.19-3ubuntu2.1).
apt-transport-https is already the newest version (2.0.6).
0 upgraded, 0 newly installed, 0 to remove and 90 not upgraded.
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$
```

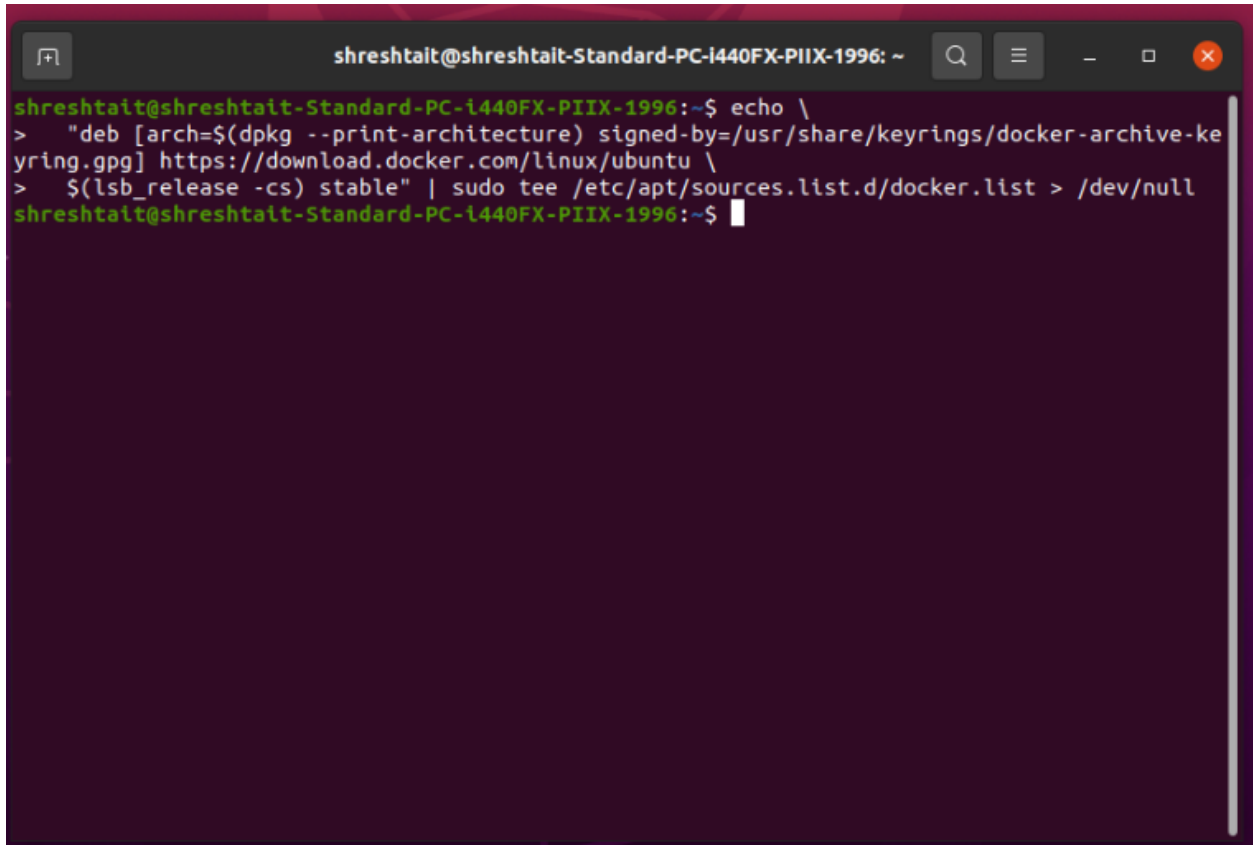
**Step 3:** Add Docker's official GPG key as follows,

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/docker-archive-keyring.gpg
```

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get update  
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease  
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:3 https://download.docker.com/linux/ubuntu focal InRelease  
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease  
Reading package lists... Done  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get install apt-transport-ht  
tps ca-certificates curl gnupg lsb-release  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
lsb-release is already the newest version (11.1.0ubuntu2).  
ca-certificates is already the newest version (20210119-20.04.2).  
curl is already the newest version (7.68.0-1ubuntu2.7).  
gnupg is already the newest version (2.2.19-3ubuntu2.1).  
apt-transport-https is already the newest version (2.0.6).  
0 upgraded, 0 newly installed, 0 to remove and 90 not upgraded.  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ curl -fsSL https://download.docker.co  
m/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg  
File '/usr/share/keyrings/docker-archive-keyring.gpg' exists. Overwrite? (y/N) y  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$
```

**Step 5:** Use the following command to add the docker repository in apt,

```
echo "deb [arch=$(dpkg --print-architecture)  
signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]  
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee  
/etc/apt/sources.list.d/docker.list > /dev/null
```

A terminal window with a dark background and light green text. The window title is 'shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~'. The terminal shows a multi-line command being entered: 'echo \' followed by a multi-line string for a Docker repository entry, and finally '\$(lsb\_release -cs) stable' | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null'. The prompt returns to the shell after the command is executed.

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ echo \  
> "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-ke  
yring.gpg] https://download.docker.com/linux/ubuntu \  
> $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$
```

**Step 6:** Update the apt package index, and install the latest version of Docker Engine and containerd,

```
sudo apt-get update
```

```
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ echo \  
> "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-ke  
yring.gpg] https://download.docker.com/linux/ubuntu \  
> $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get update  
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease  
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:3 https://download.docker.com/linux/ubuntu focal InRelease  
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease  
Reading package lists... Done  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$
```

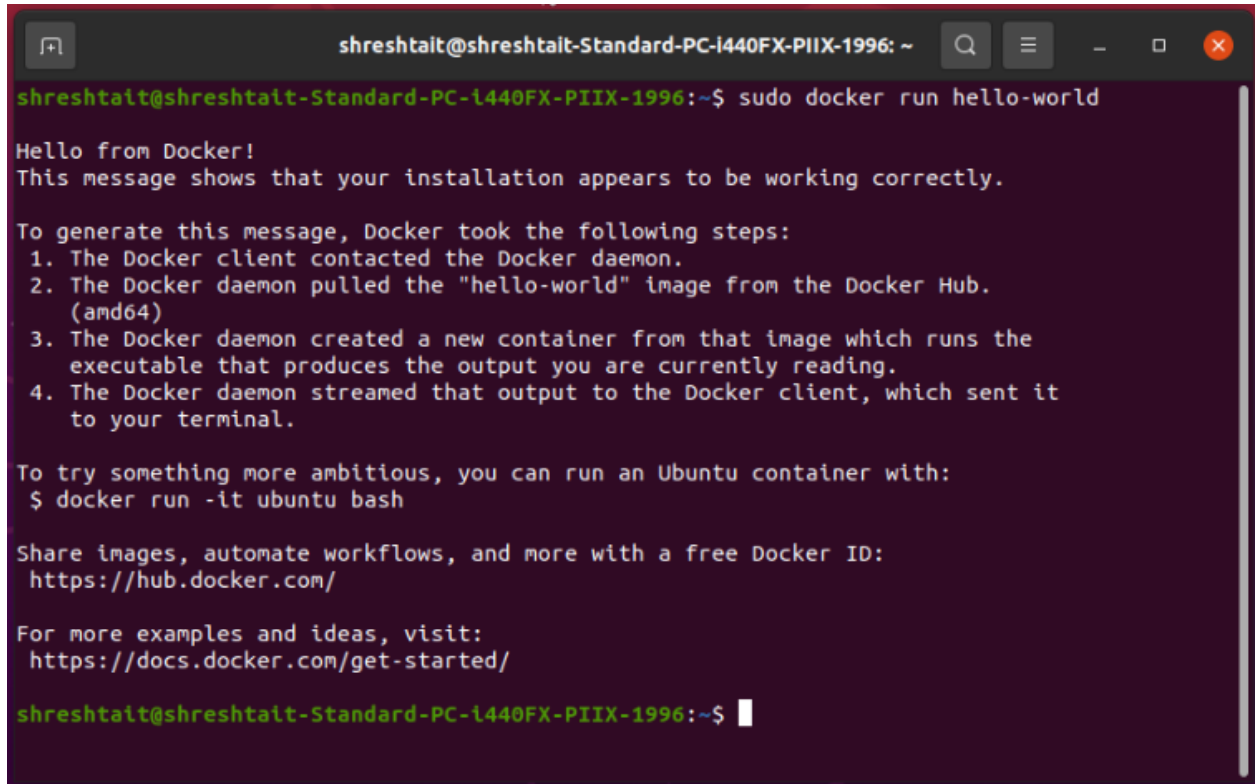


```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ echo \  
> "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-ke  
yring.gpg] https://download.docker.com/linux/ubuntu \  
> $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get update  
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease  
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:3 https://download.docker.com/linux/ubuntu focal InRelease  
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease  
Reading package lists... Done  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get install docker-ce docker  
-ce-cli containerd.io  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  docker-ce-rootless-extras docker-scan-plugin pigz slirp4netns  
Suggested packages:  
  aufs-tools cgroupfs-mount | cgroup-lite  
The following NEW packages will be installed:  
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras docker-scan-plugin pigz  
  slirp4netns  
0 upgraded, 7 newly installed, 0 to remove and 90 not upgraded.  
Need to get 0 B/95.6 MB of archives.  
After this operation, 403 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~  
Reading package lists... Done  
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo apt-get install docker-ce docker  
-ce-cli containerd.io  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  docker-ce-rootless-extras docker-scan-plugin pigz slirp4netns  
Suggested packages:  
  aufs-tools cgroupfs-mount | cgroup-lite  
The following NEW packages will be installed:  
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras docker-scan-plugin pigz  
  slirp4netns  
0 upgraded, 7 newly installed, 0 to remove and 90 not upgraded.  
Need to get 0 B/95.6 MB of archives.  
After this operation, 403 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Selecting previously unselected package pigz.  
(Reading database ... 184693 files and directories currently installed.)  
Preparing to unpack .../0-pigz_2.4-1_amd64.deb ...  
Unpacking pigz (2.4-1) ...  
Selecting previously unselected package containerd.io.  
Preparing to unpack .../1-containerd.io_1.4.11-1_amd64.deb ...  
Unpacking containerd.io (1.4.11-1) ...  
Selecting previously unselected package docker-ce-cli.  
Preparing to unpack .../2-docker-ce-cli_5%3a20.10.9~3-0~ubuntu-focal_amd64.deb ...  
Unpacking docker-ce-cli (5:20.10.9~3-0~ubuntu-focal) ...
```

**Step 7:** Verify that the Docker engine is installed correctly by running the hello-world image.

**sudo docker run hello-world**

A terminal window with a dark purple background and light green text. The window title is 'shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996: ~'. The command 'sudo docker run hello-world' has been entered and executed. The output is a multi-line message from Docker, explaining the steps taken to run the 'hello-world' image and providing links to Docker Hub and documentation. The prompt 'shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~\$' is visible at the bottom.

```
shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$ sudo docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
   (amd64)
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

shreshtait@shreshtait-Standard-PC-i440FX-PIIX-1996:~$
```

The above command downloads a test image and runs it in a container. When the container runs, it prints a message and exits.



# Steps to pull the Zeek Docker Image and start a docker container

**Step 1:** Open a terminal and pull the Zeek image,

```
#sudo docker pull zeekurity/zeek-training-2022
```

**Step 2:**After pulling the zeek image, verify the image is available

```
#sudo docker images
```

**Step 3:** Start a docker container using the Zeek image

```
#sudo docker run -it zeekurity/zeek-training-2022 /bin/bash
```

**Step 4:** Once the container starts successfully, it will drop us into a shell. Verify Zeek command is accessible

```
#!/opt/zeek/bin/zeek --version
```