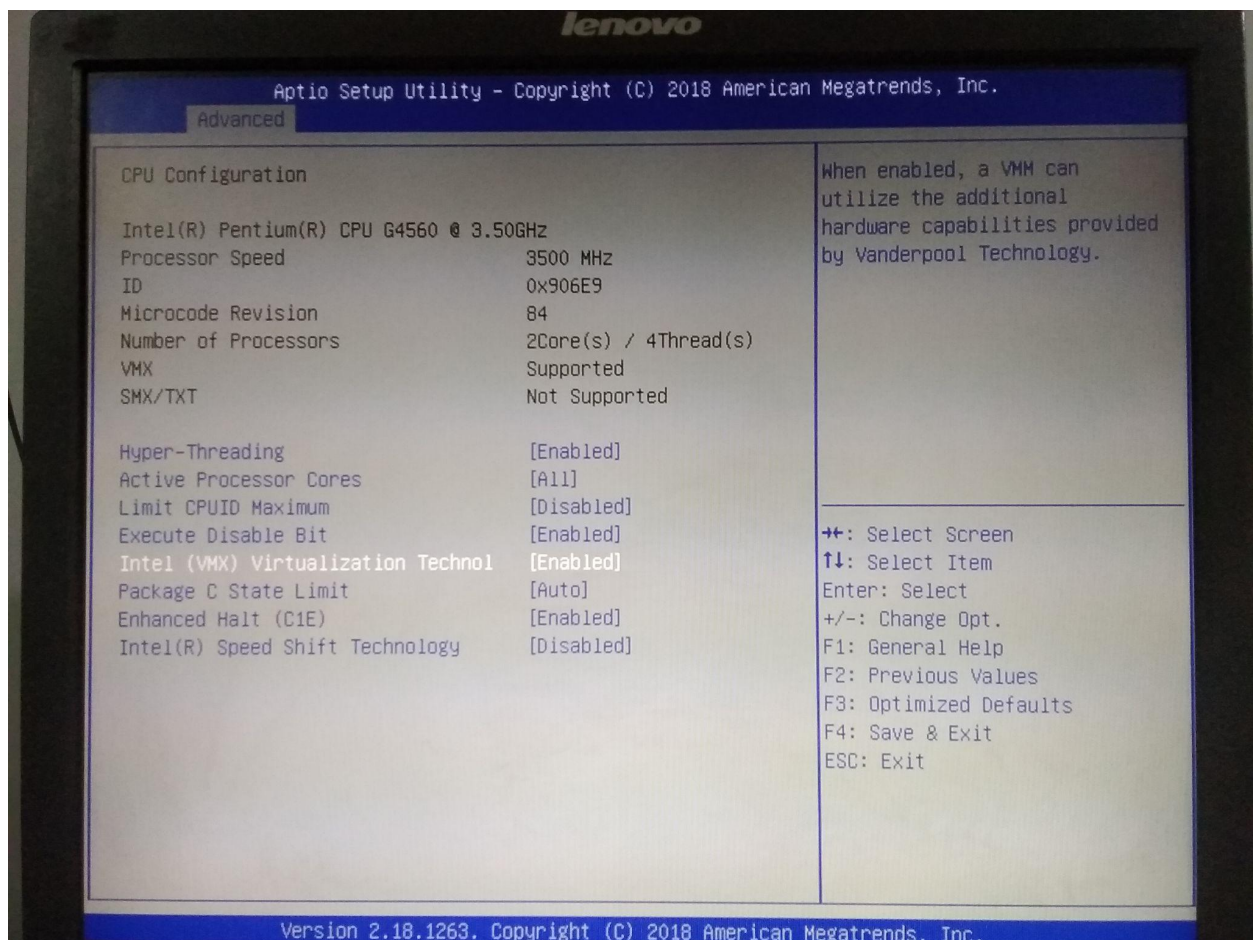


ZeekWeek21 - Introduction to Zeek

Instructions for installation of Zeek in Windows 10

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 F2 key or Del key on boot.

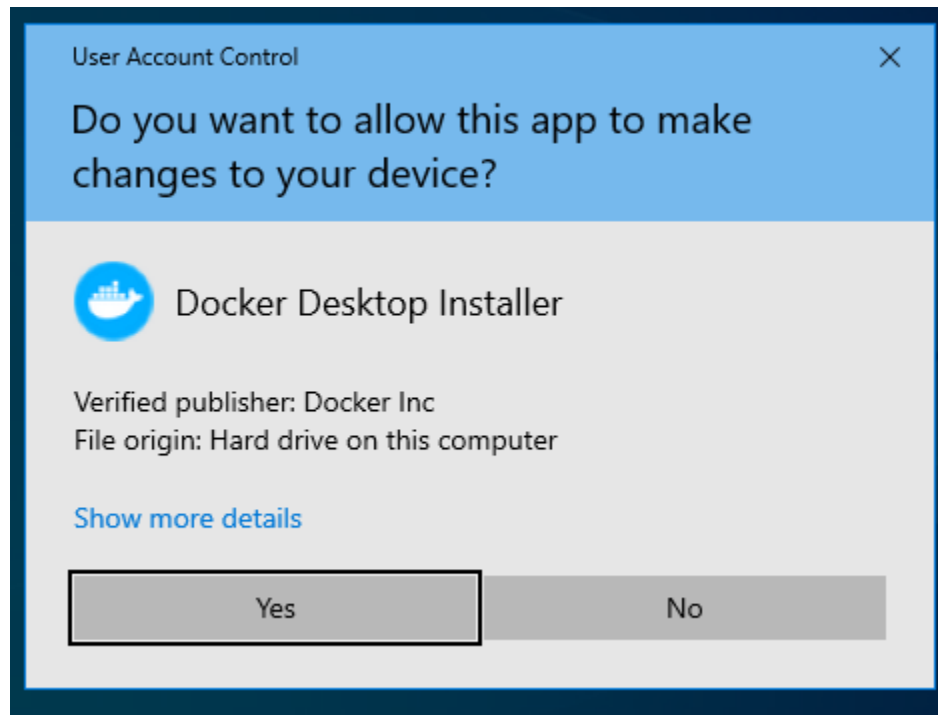


Step2: Download the docker setup for Windows 10 - <https://docs.docker.com/docker-for-windows/install/>

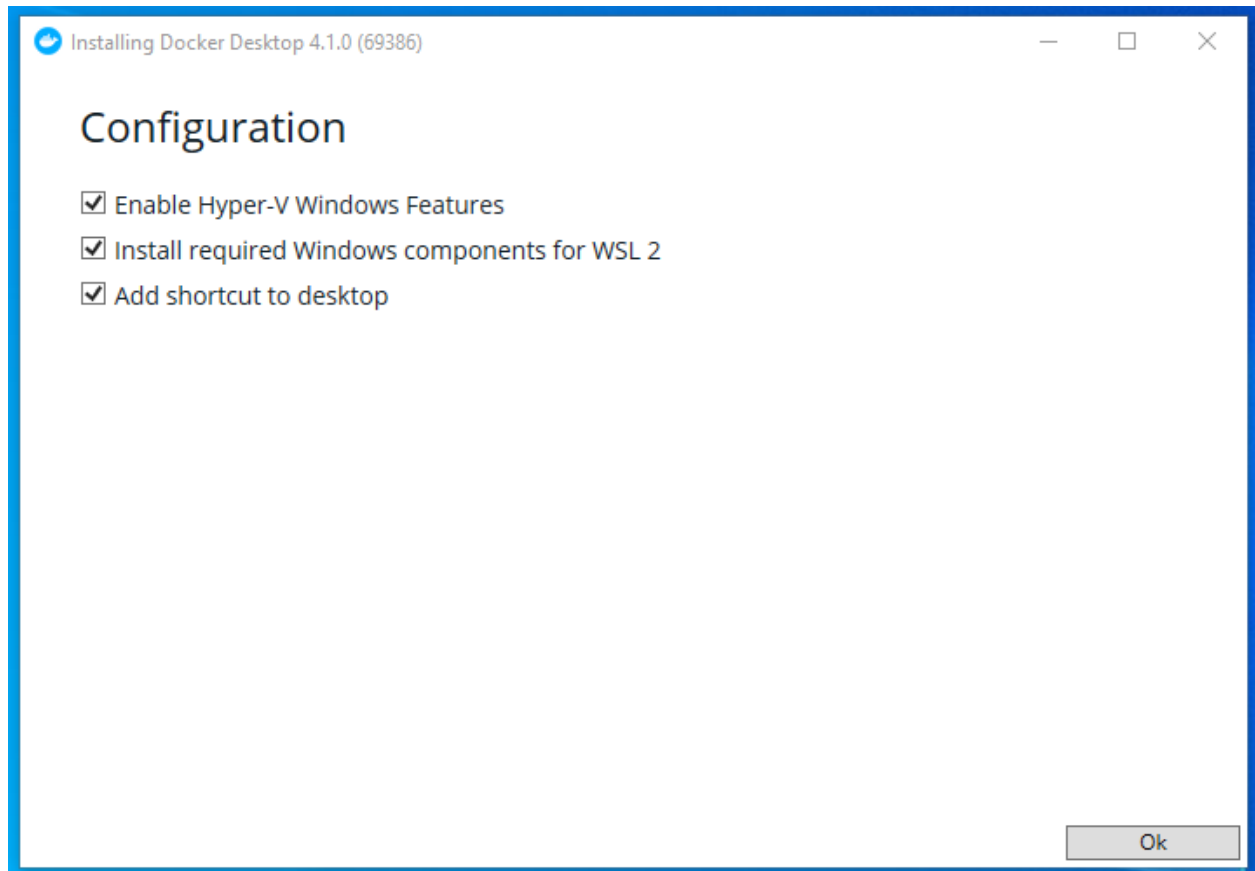
Note: A 64-bit processor and 4GB system RAM are the hardware prerequisites required.

Step 3: Then, double-click on the Docker Desktop Installer.exe to run the installer.

Step 4: Click "Yes" to start the installation.

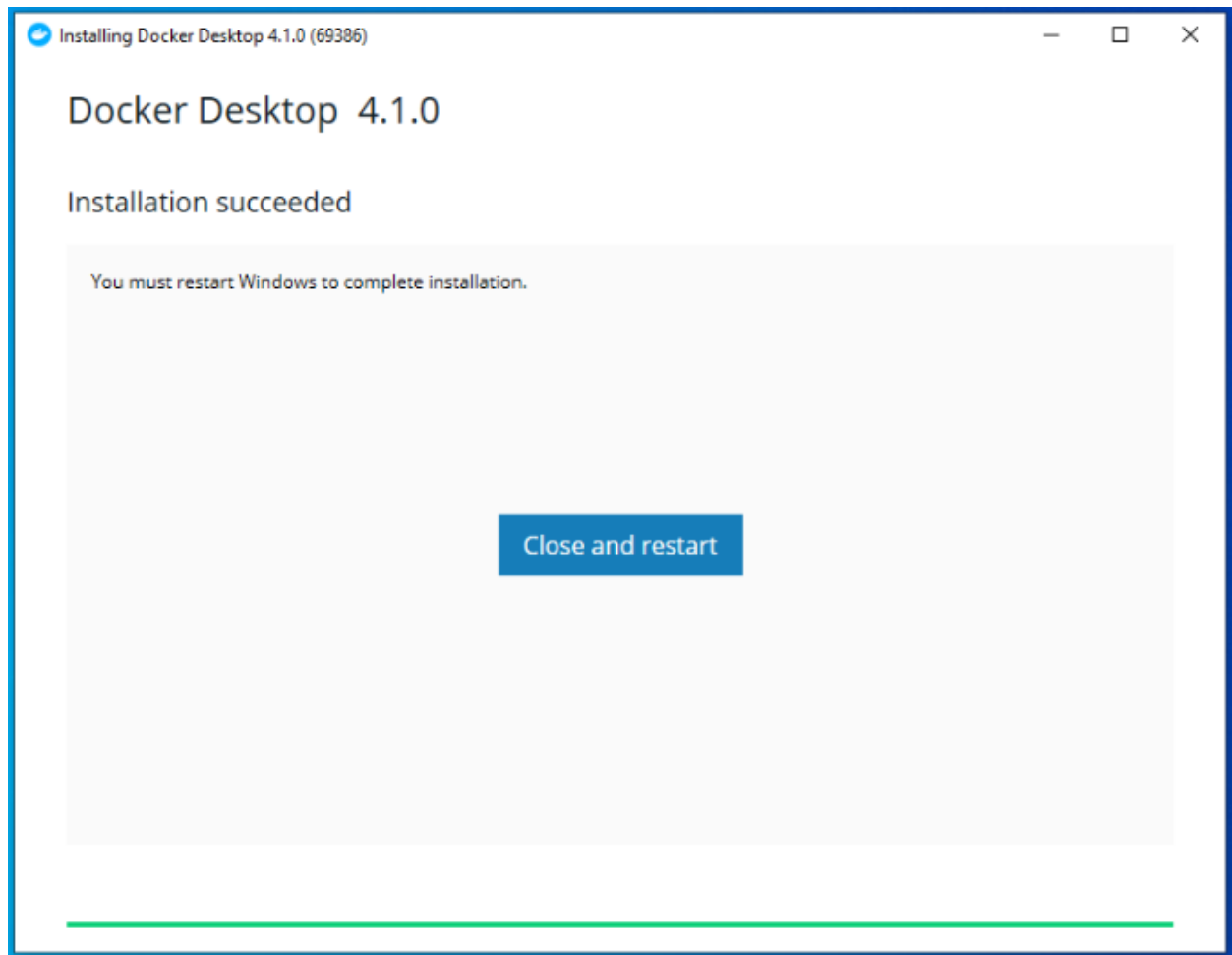


Step 5: Once you start the installation process, make sure to enable Hyper-V Windows Feature and Install required Windows components for WSL 2 on the Configuration page. Then, click, "ok."



Step 6: Then, follow the installation process to allow the installer and wait till the process completes.

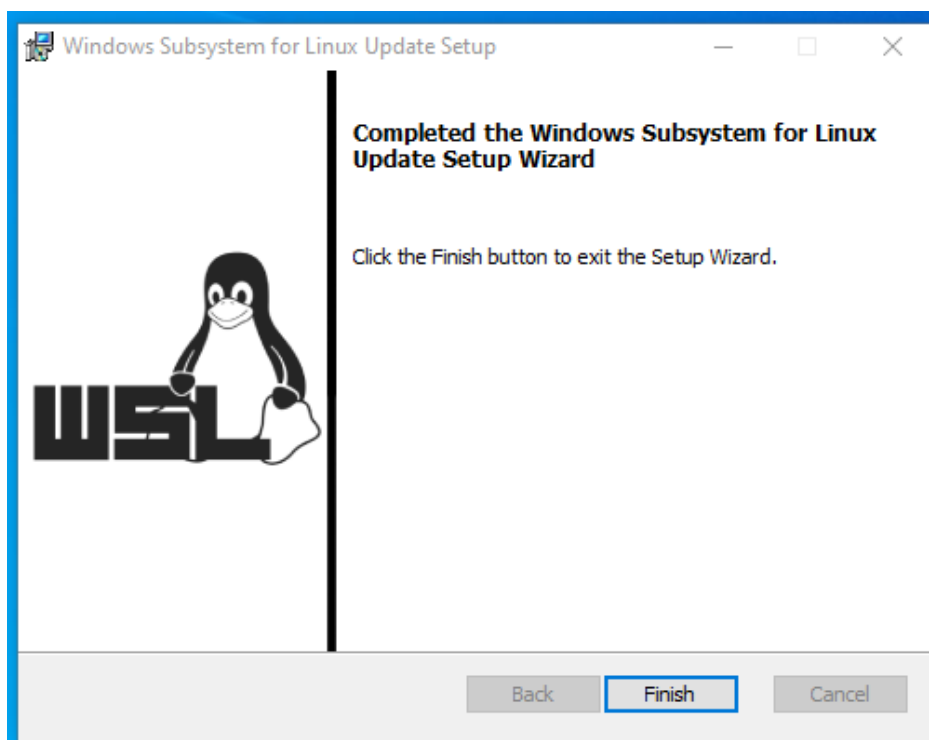
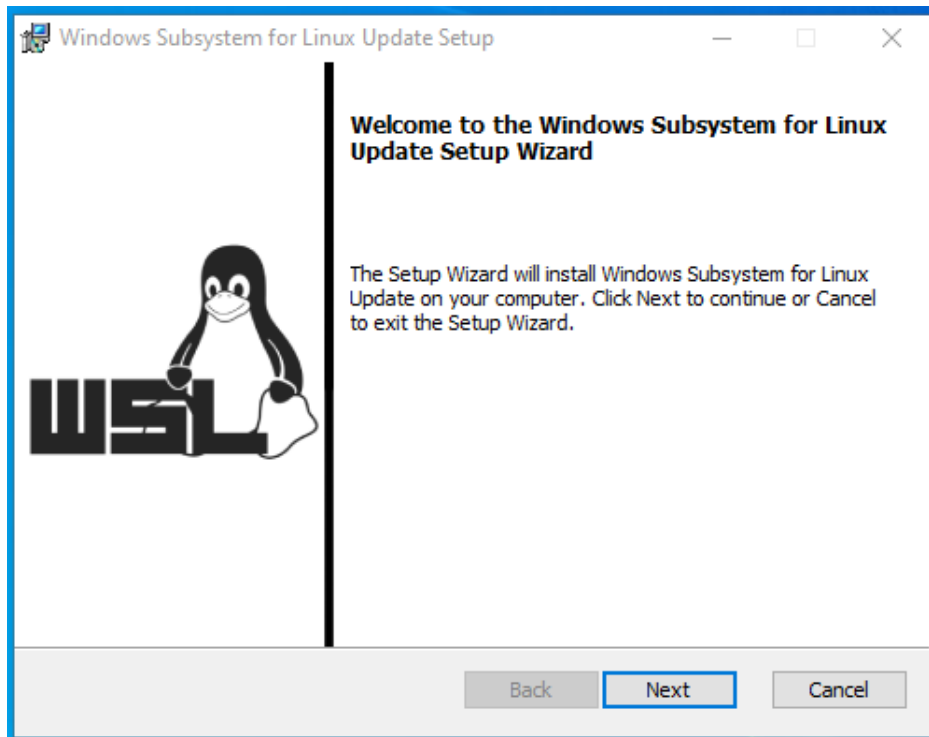
Step 7: After completion of the installation process, click Close and restart.



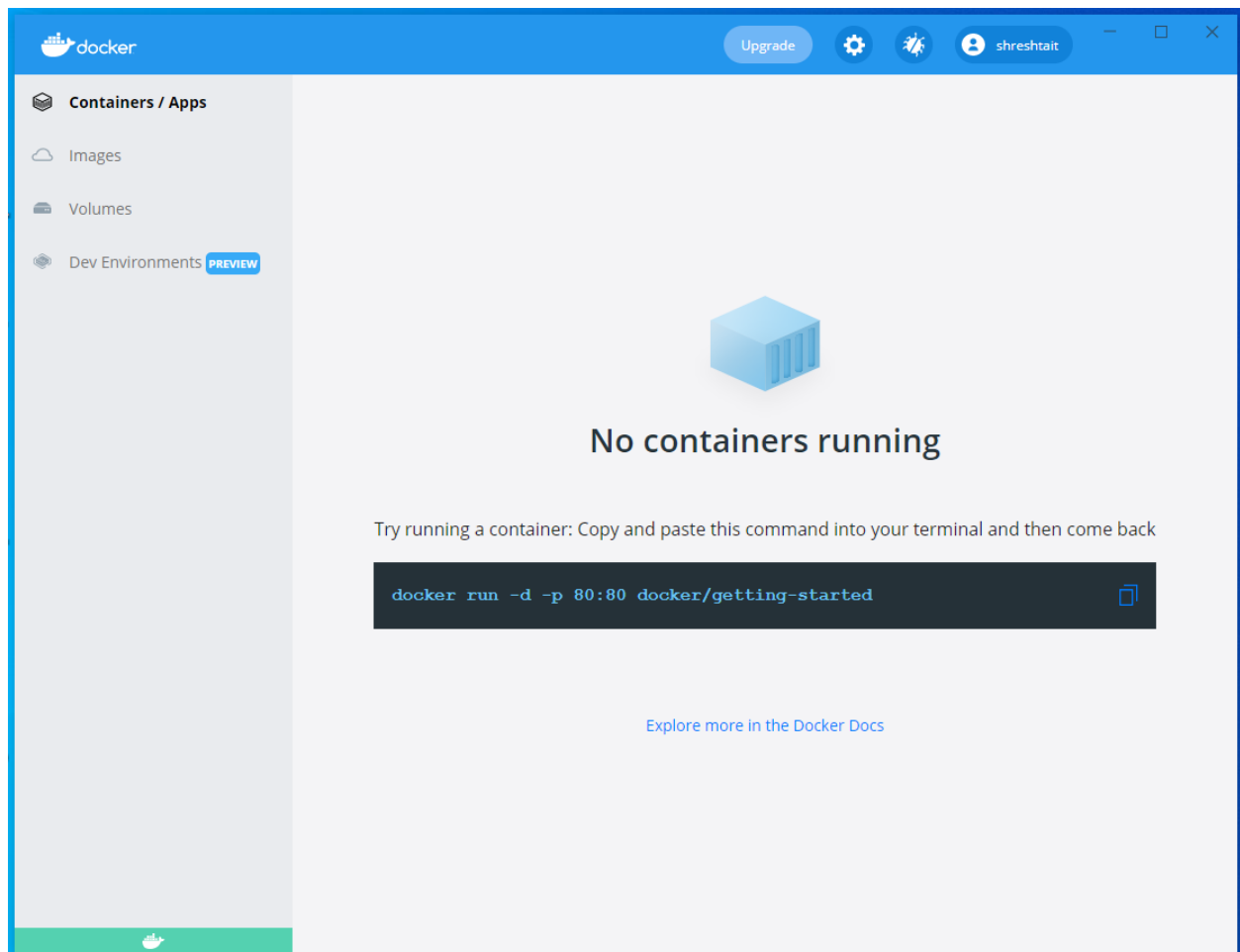
Step 8: If Docker fails to open/start, then update the Windows subsystem for Linux(WSL) i.e. Download the updates of WSL by using the below link

https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi

After downloading, double click on the .msi file, run it and complete the process as shown below:

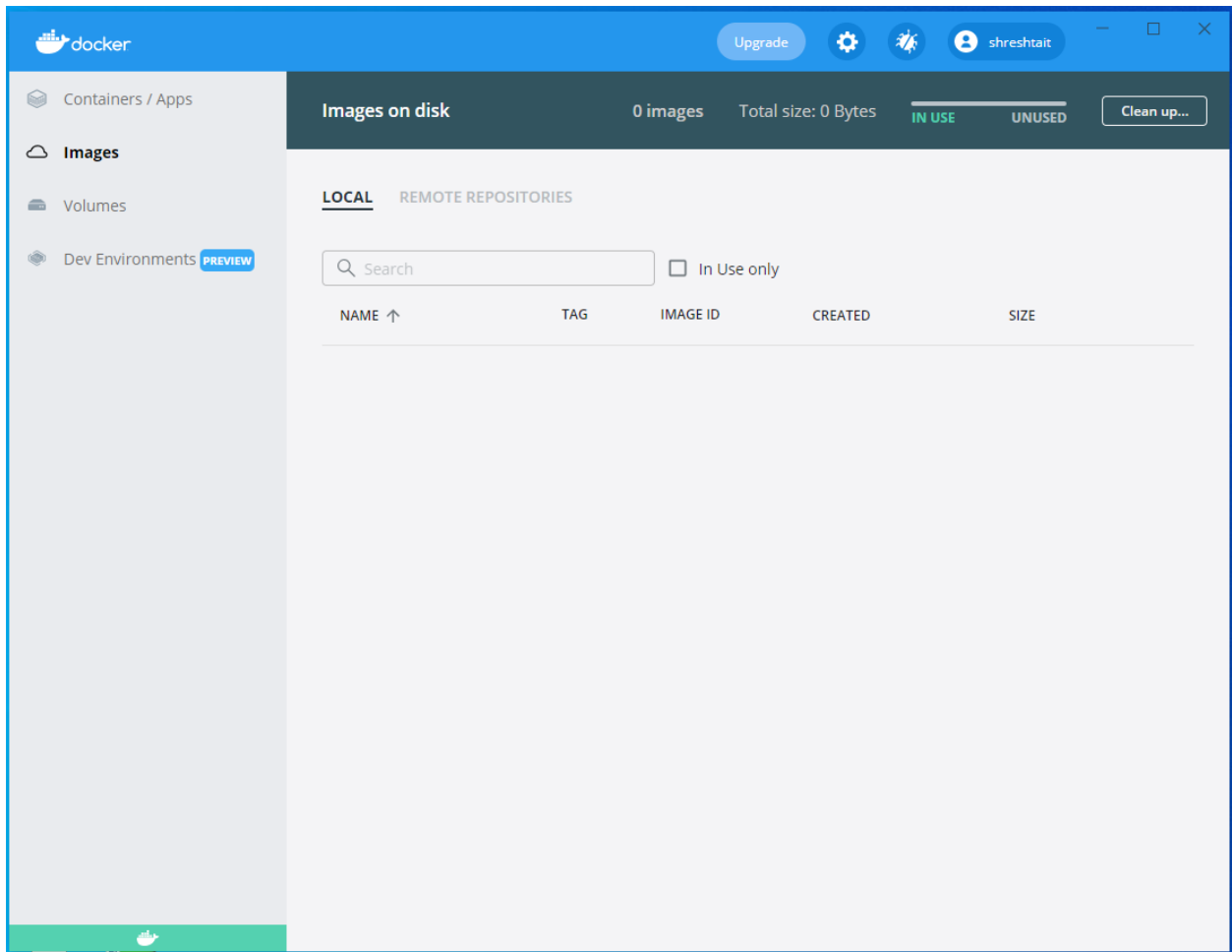


Step 9: Now, restart the system and open/run Docker by right-clicking → “Run as Administrator”. Now we can see the home page of Docker.



Steps to pull the Zeek Docker Image and start the container in Docker

Step 1 : Initially, there will be no images in docker. To pull the Zeek docker image, go to step 2.



Step 2: Now, open the command prompt and enter the below command and press “Enter.”

```
docker pull zeekurity/zeek-training-2021
```

```
C:\WINDOWS\system32\cmd.exe

C:\Users\shreshtait>docker pull zeekurity/zeek-training-2021
```

```
C:\WINDOWS\system32\cmd.exe - docker pull zeekurity/zeek-training-2021

C:\Users\shreshtait>docker pull zeekurity/zeek-training-2021
Using default tag: latest
latest: Pulling from zeekurity/zeek-training-2021
0bc3020d05f1: Pull complete
b6ff8465a448: Pull complete
c913c300a426: Pull complete
867d566cf235: Pull complete
88beb3443fea: Pull complete
ae067c5a0603: Pull complete
9c9e72090c75: Pull complete
b368d7a9f8da: Pull complete
24beeee174d0: Pull complete
1de46056b28d: Pull complete
2a6d25c6421f: Extracting 200MB/214.4MB
63ee5ddae99d: Download complete
c6e21c2e8b6b: Download complete
-
```

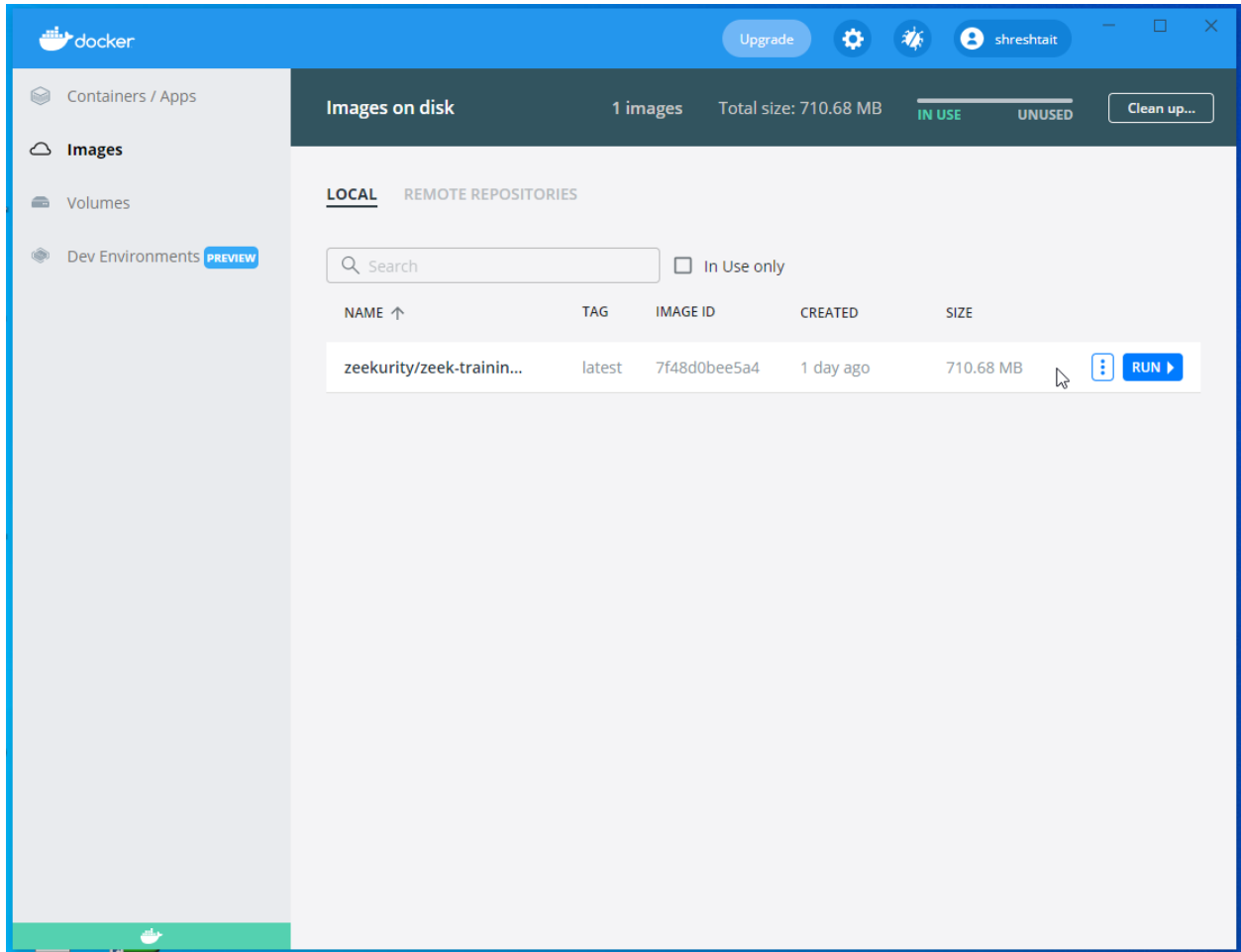


```
C:\WINDOWS\system32\cmd.exe

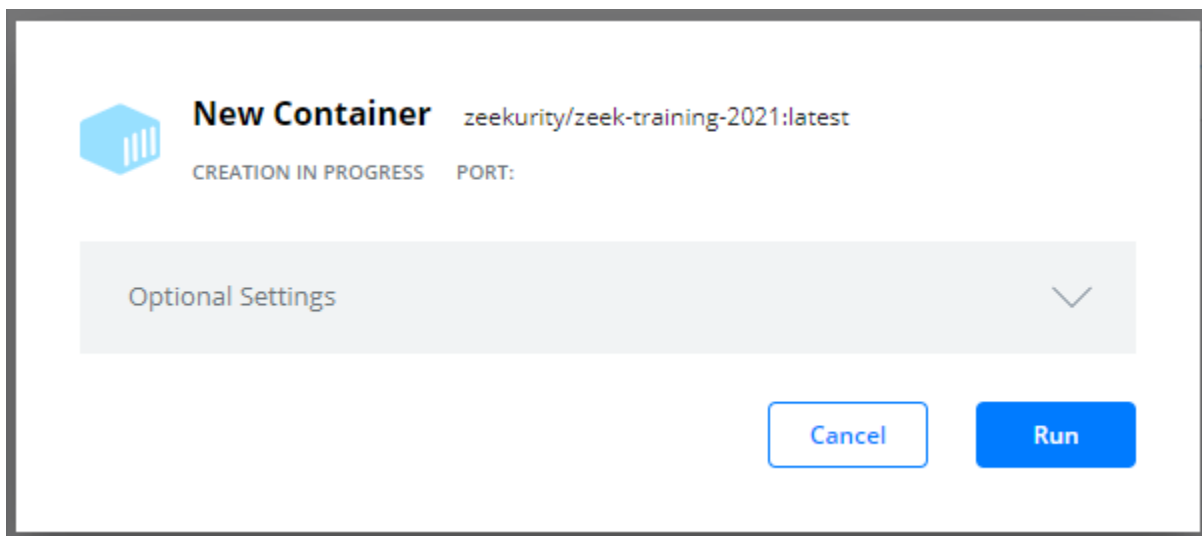
C:\Users\shreshtait>docker pull zeekurity/zeek-training-2021
Using default tag: latest
latest: Pulling from zeekurity/zeek-training-2021
0bc3020d05f1: Pull complete
b6ff8465a448: Pull complete
c913c300a426: Pull complete
867d566cf235: Pull complete
88beb3443fea: Pull complete
ae067c5a0603: Pull complete
9c9e72090c75: Pull complete
b368d7a9f8da: Pull complete
24beeea174d0: Pull complete
1de46056b28d: Pull complete
2a6d25c6421f: Pull complete
63ee5ddae99d: Pull complete
c6e21c2e8b6b: Pull complete
Digest: sha256:ae9f6a1e65b51bfbf72fd4d6f3cbfb7724abf95929e5580e80f2204ce6b1f953
Status: Downloaded newer image for zeekurity/zeek-training-2021:latest
docker.io/zeekurity/zeek-training-2021:latest

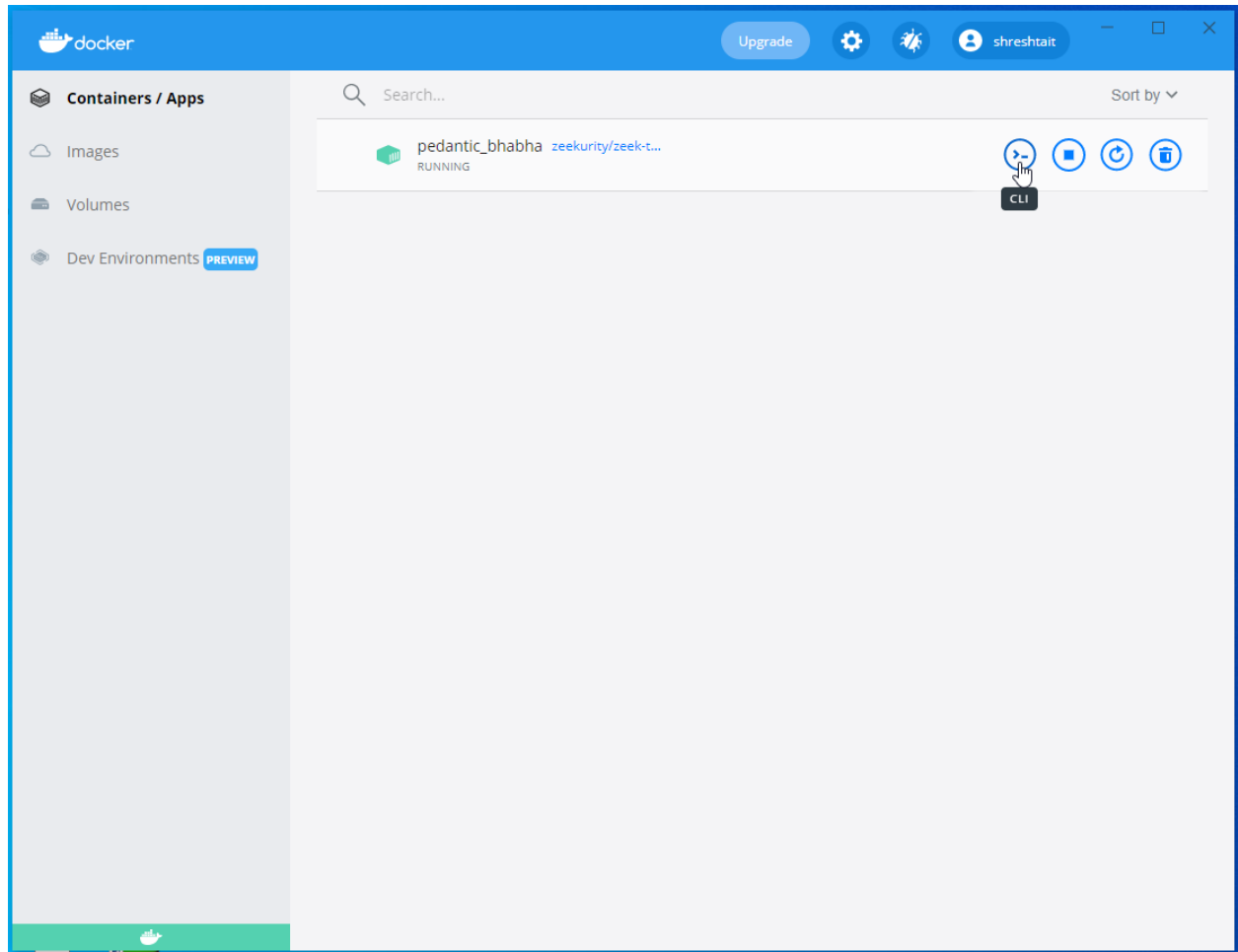
C:\Users\shreshtait>
```

Step 3: After the Zeek docker image download completes, we can run it by accessing the image from the “Images” menu option in docker.

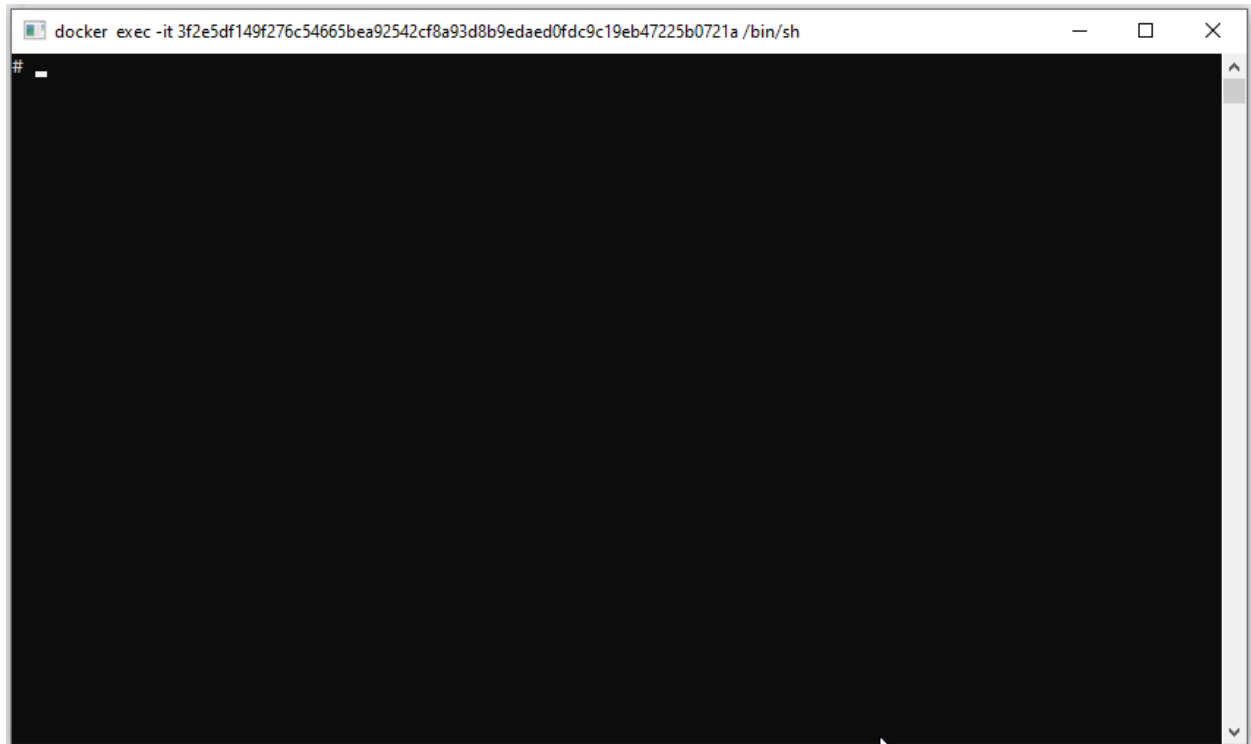


Step 4: Click on "Run" to start a docker container using the image. You can verify the container has started by accessing the "Containers" menu option.

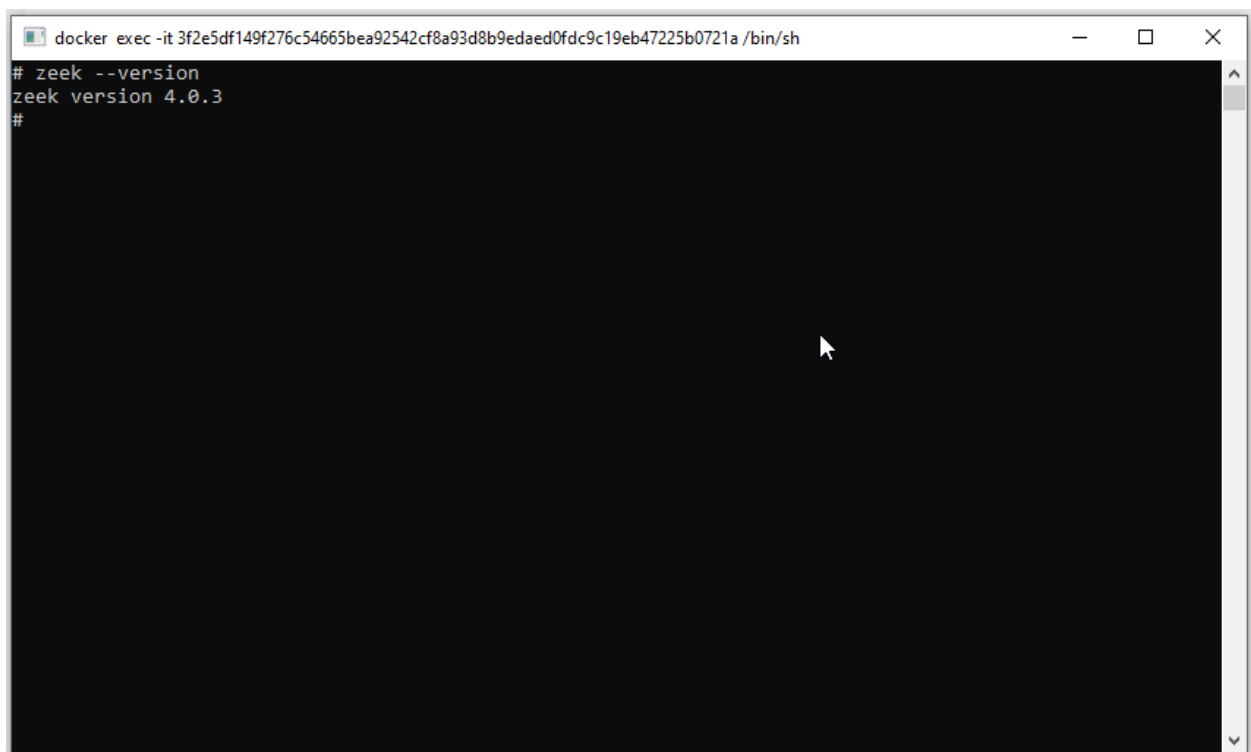




Step 5: Access the "Containers" menu option and click on the "CLI" button. It will open a command prompt and give us access to the live container running Zeek.



Step 6: Verify Zeek command is accessible.



Happy ZeekWeek21!