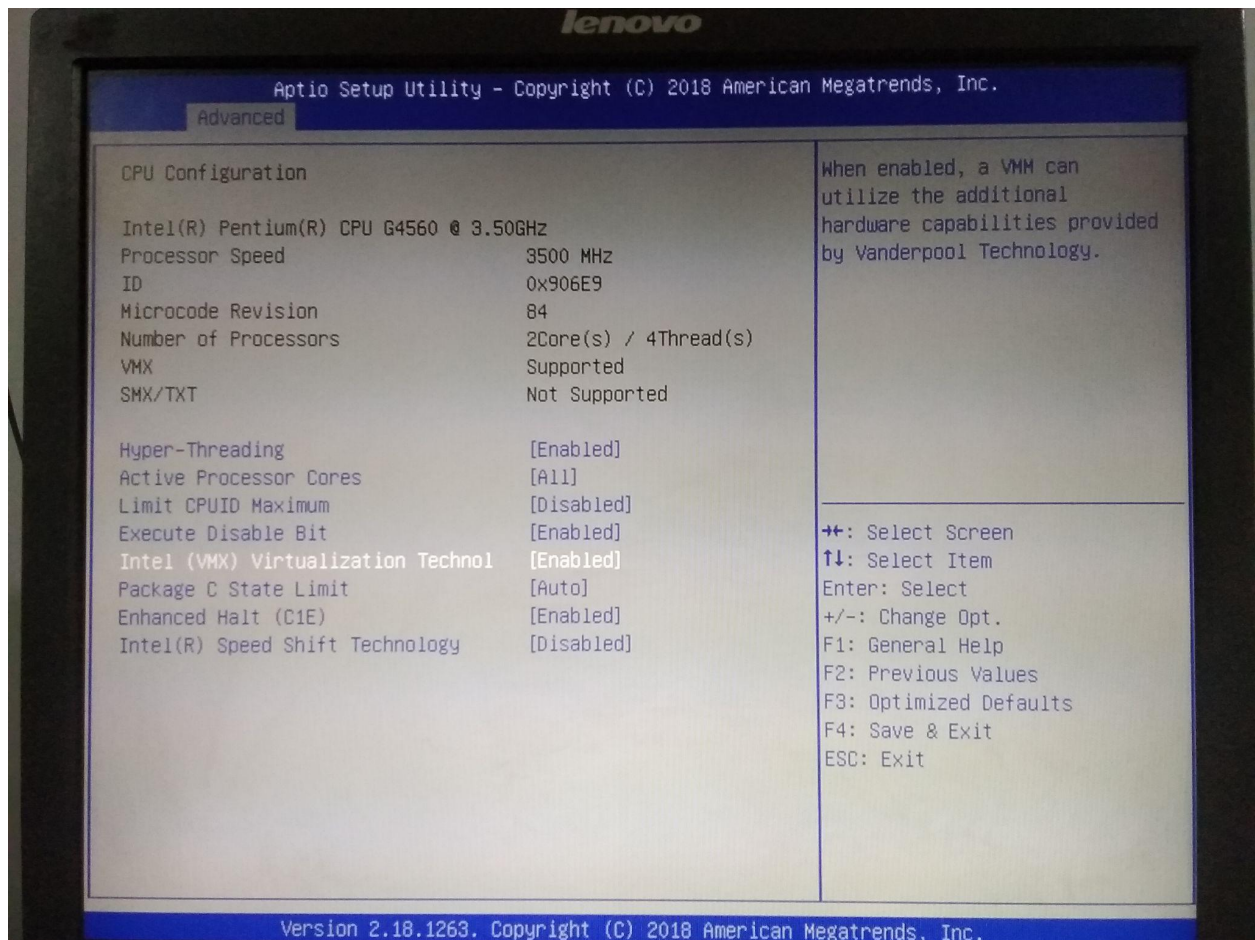# Introduction to Zeek

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.
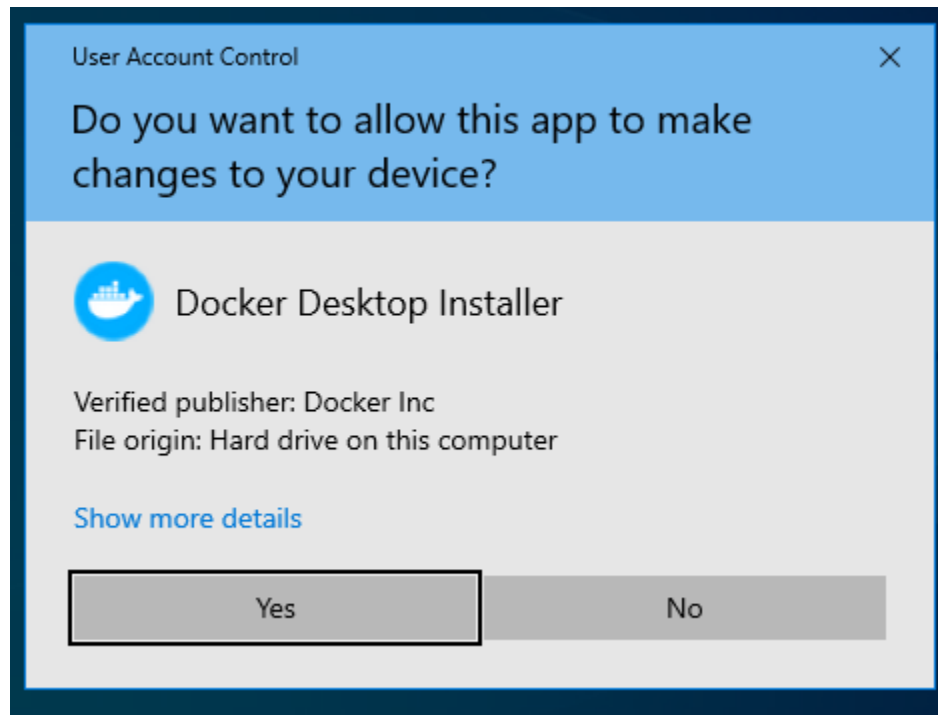

Step2: Download the docker setup for Windows 10 - https://docs.docker.com/docker-for-windows/install/

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.

User Account Control ✕

Do you want to allow this app to make changes to your device?

Docker Desktop Installer

Verified publisher: Docker Inc
File origin: Hard drive on this computer

Show more details

| Yes | No |

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."
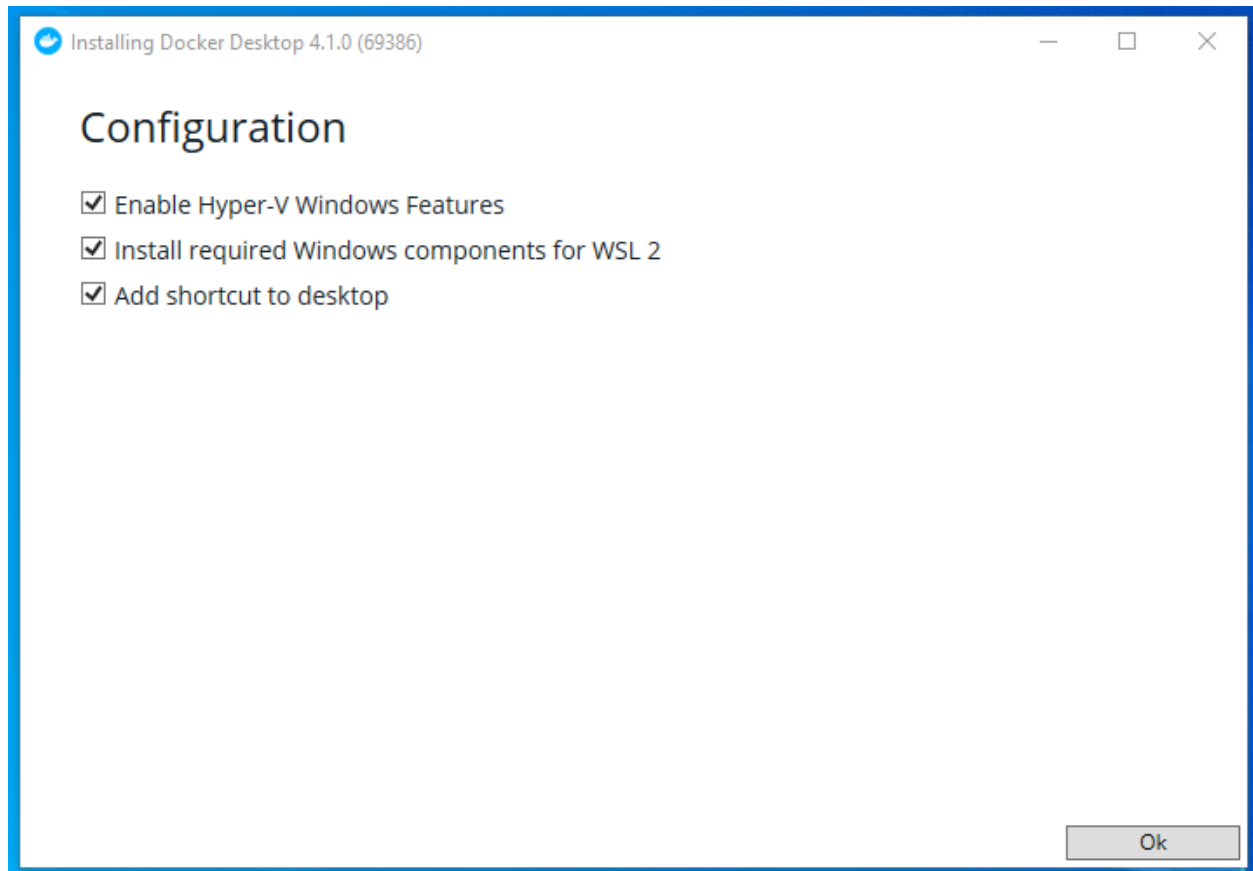
Step 6: Then, follow the installation process to allow the installer and wait till the process completes.
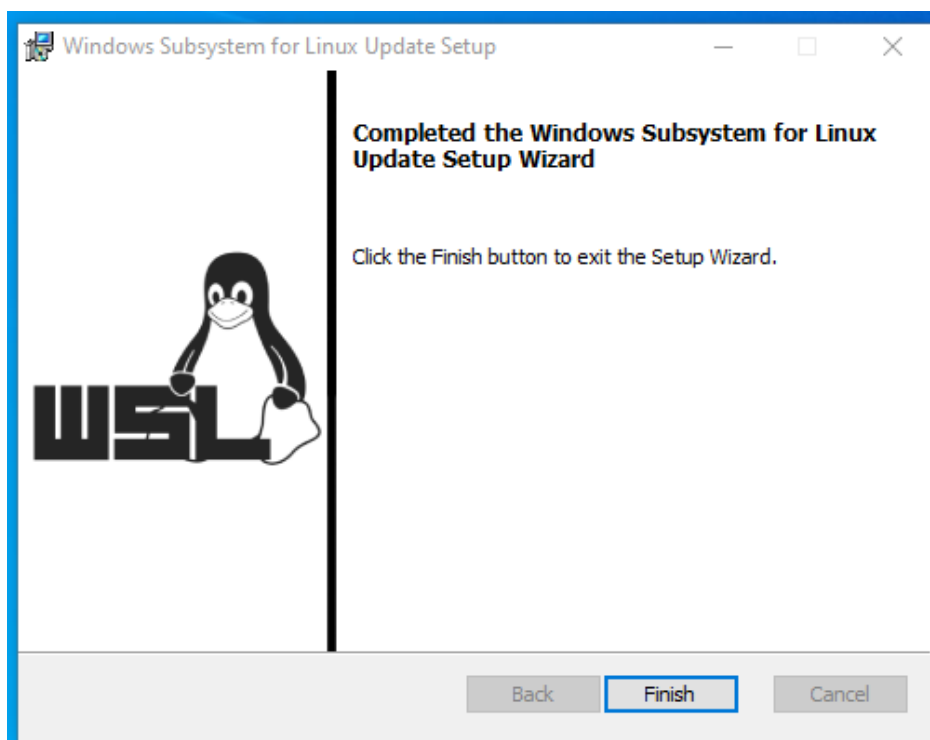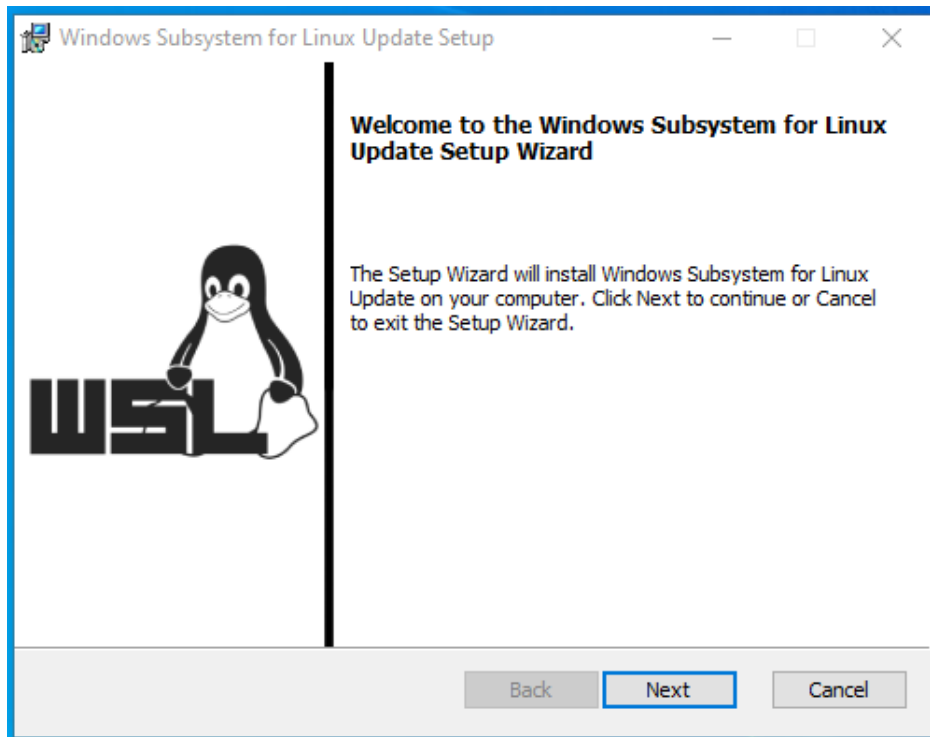
Step 7: After completion of the installation process, click Close and restart.
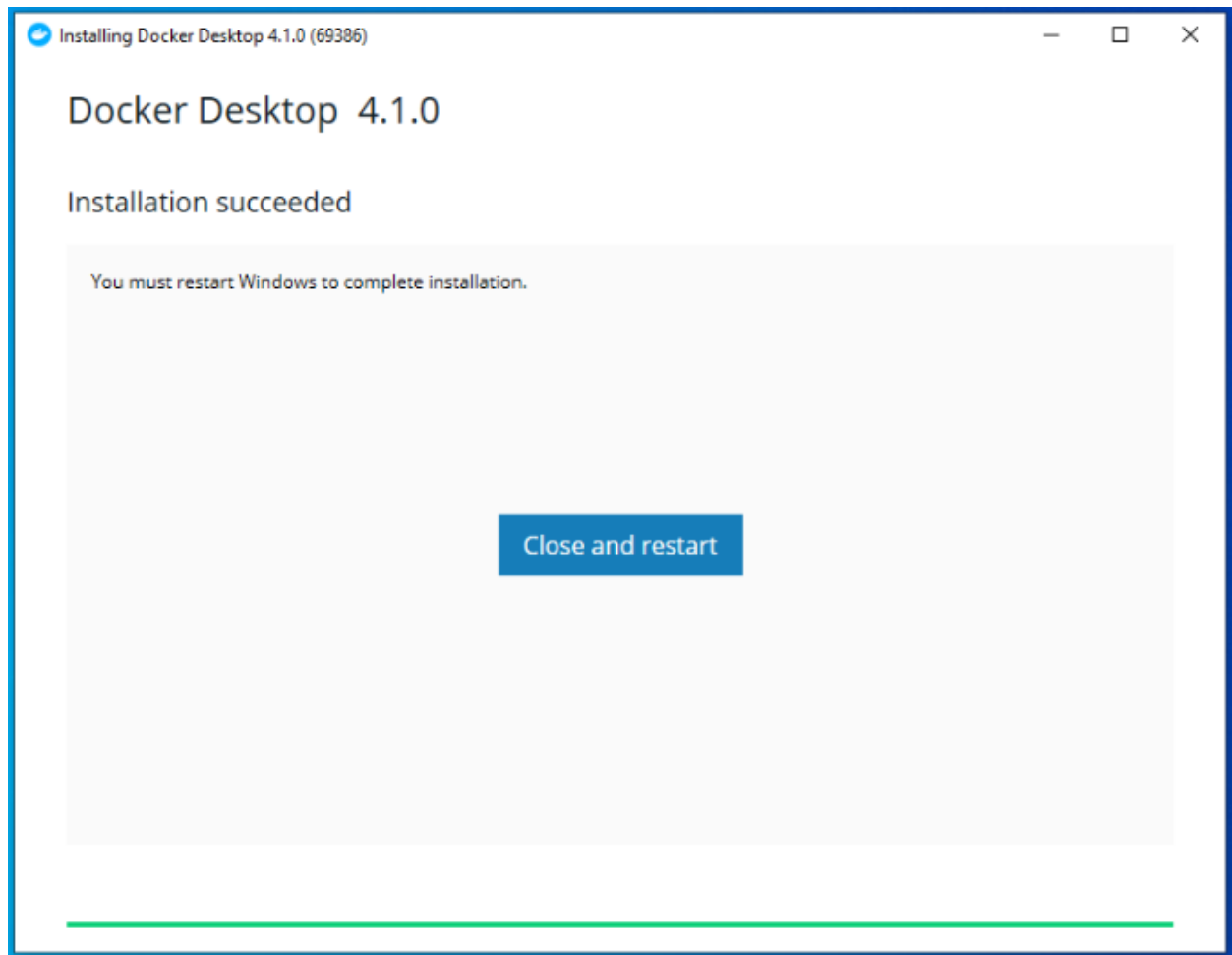

Step 8: If Docker fails to open/start, then update the Windows subsystem for Linux(WSL) i.e. Download the updates of WSL by using the below link

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:

Windows Subsystem for Linux Update Setup

Welcome to the Windows Subsystem for Linux Update Setup Wizard

The Setup Wizard will install Windows Subsystem for Linux Update on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Back   Next   Cancel

Windows Subsystem for Linux Update Setup

Completed the Windows Subsystem for Linux Update Setup Wizard

Click the Finish button to exit the Setup Wizard.

Back   Finish   Cancel

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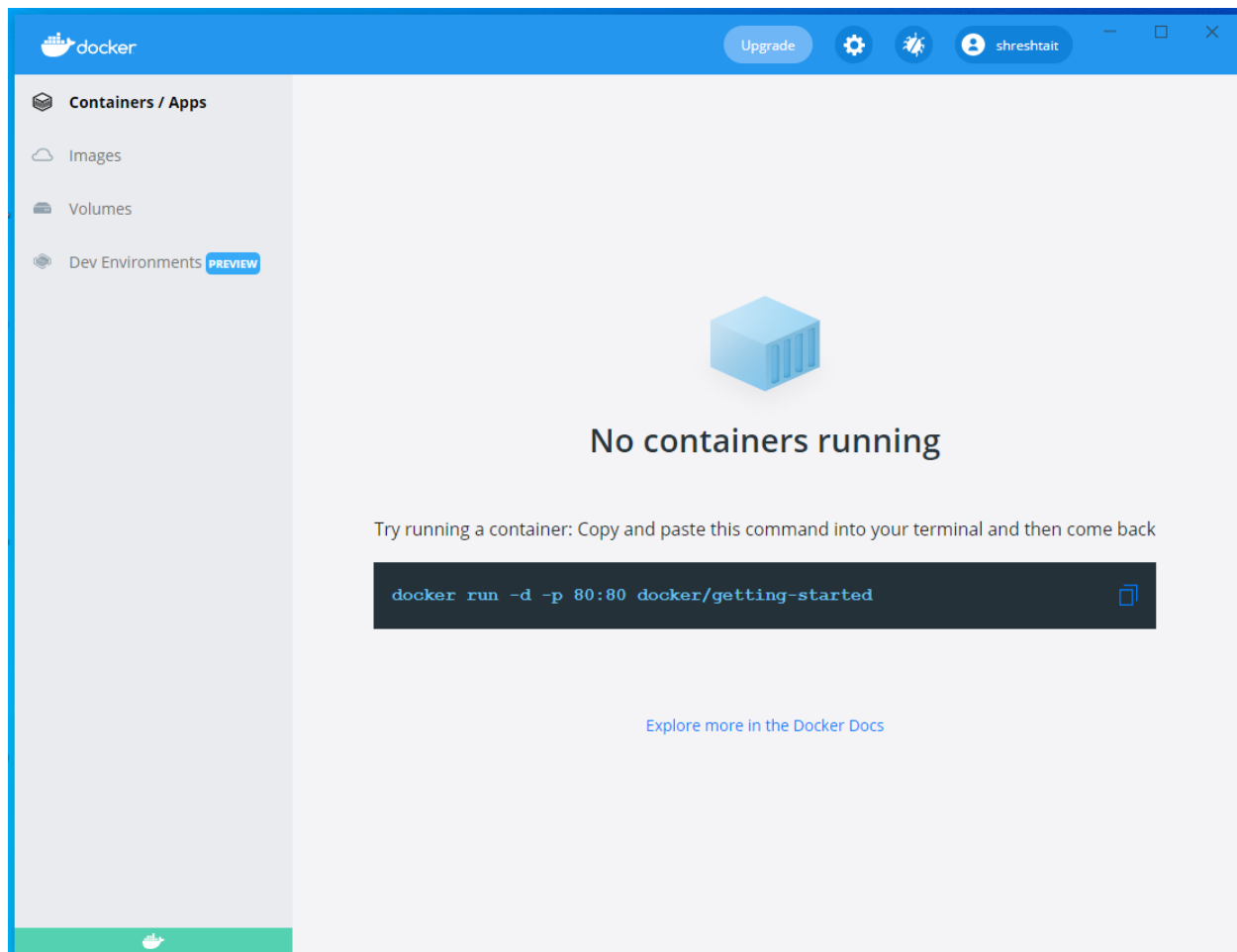
# Steps to pull the Zeek Docker Image and start the container in Docker

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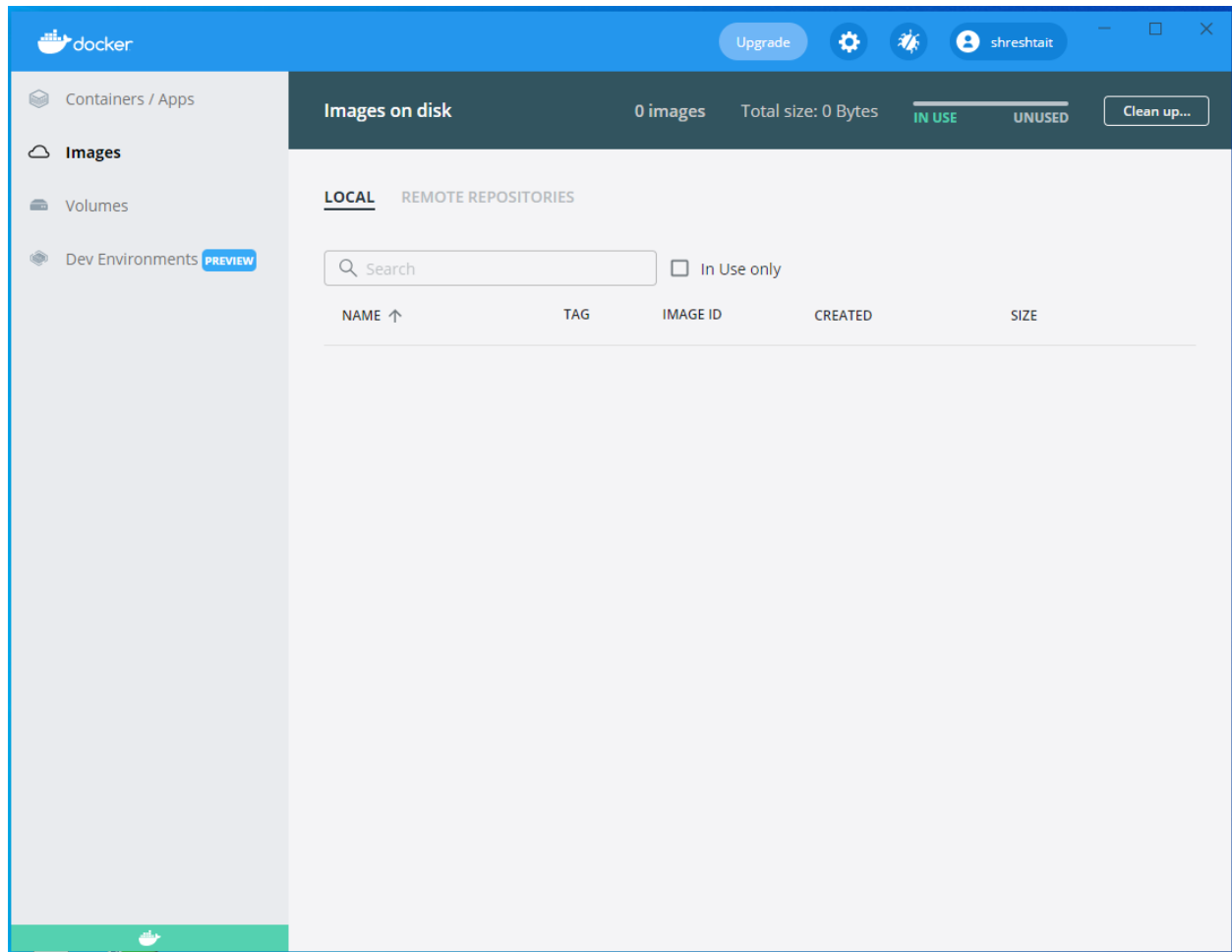

Step 2: Now, open the command prompt and enter the below command and press "Enter."
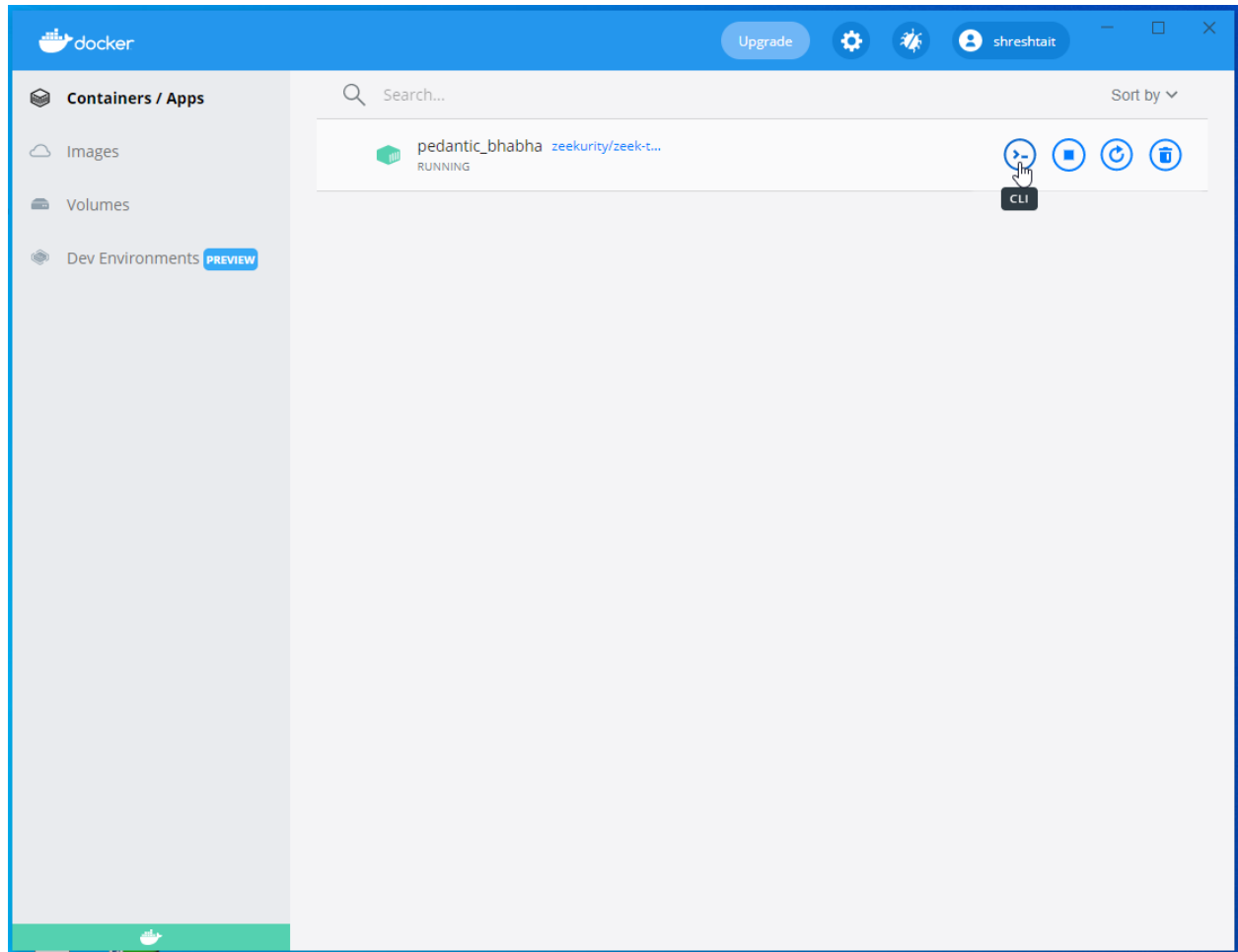
docker pull zeekurity/zeek-training-2022

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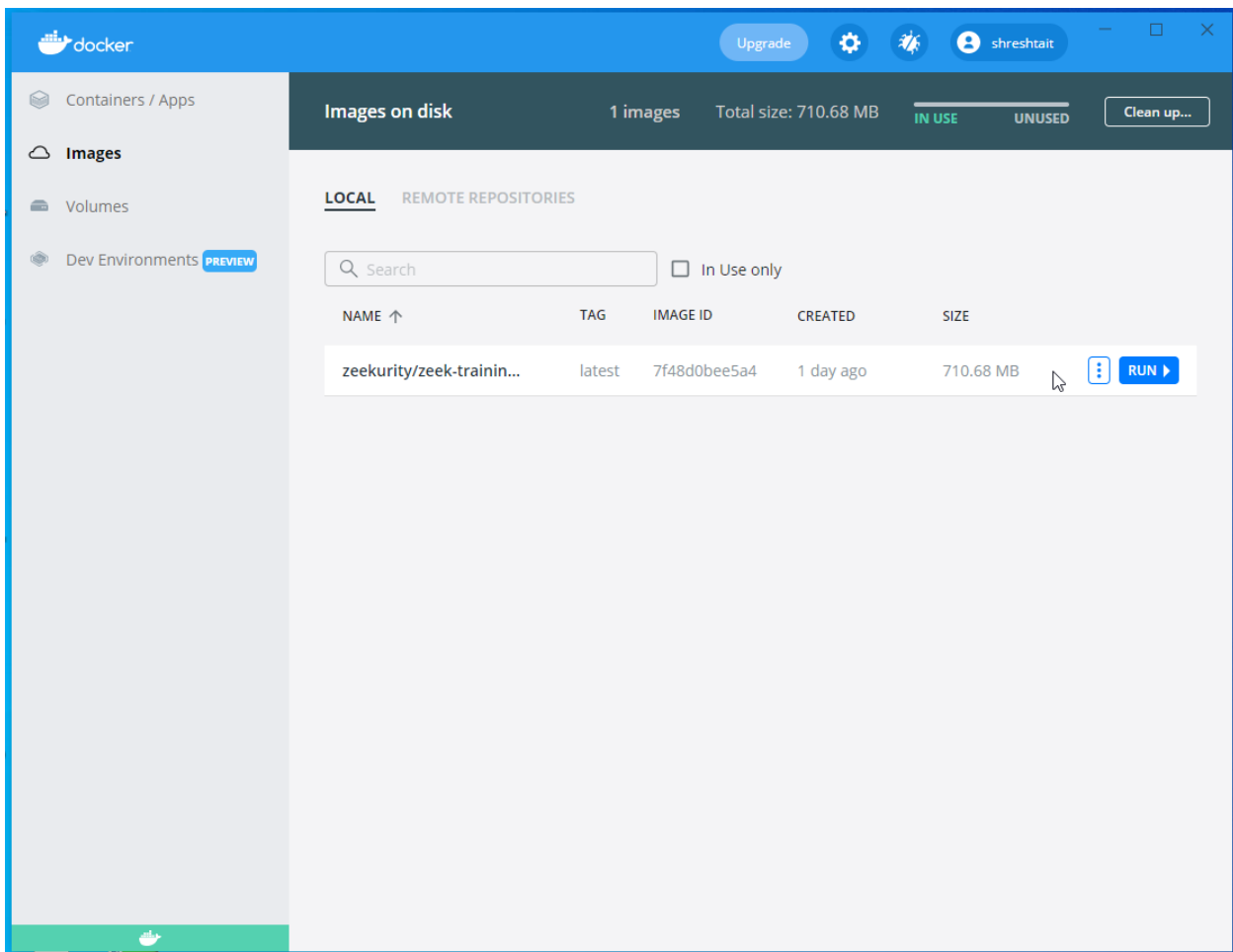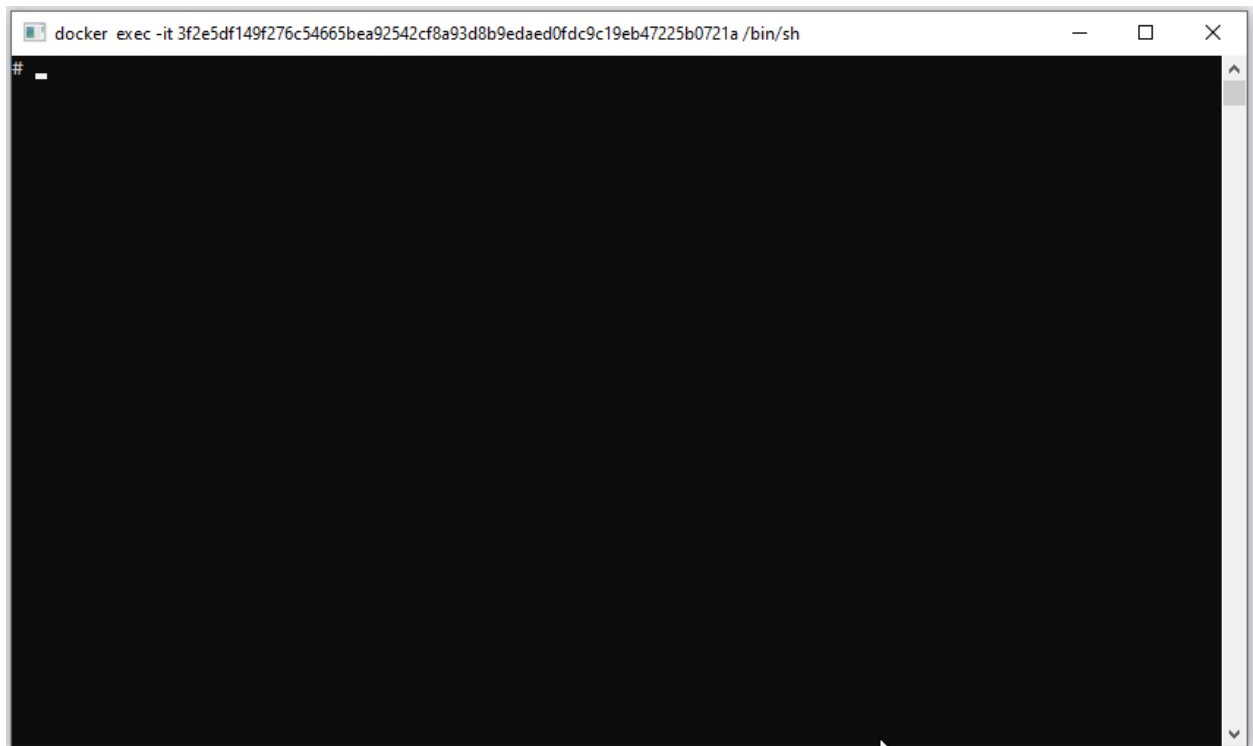

Step 4: Click on "Run" to start a docker container using the image. You can verify the container has started by accessing the "Containers" menu option.
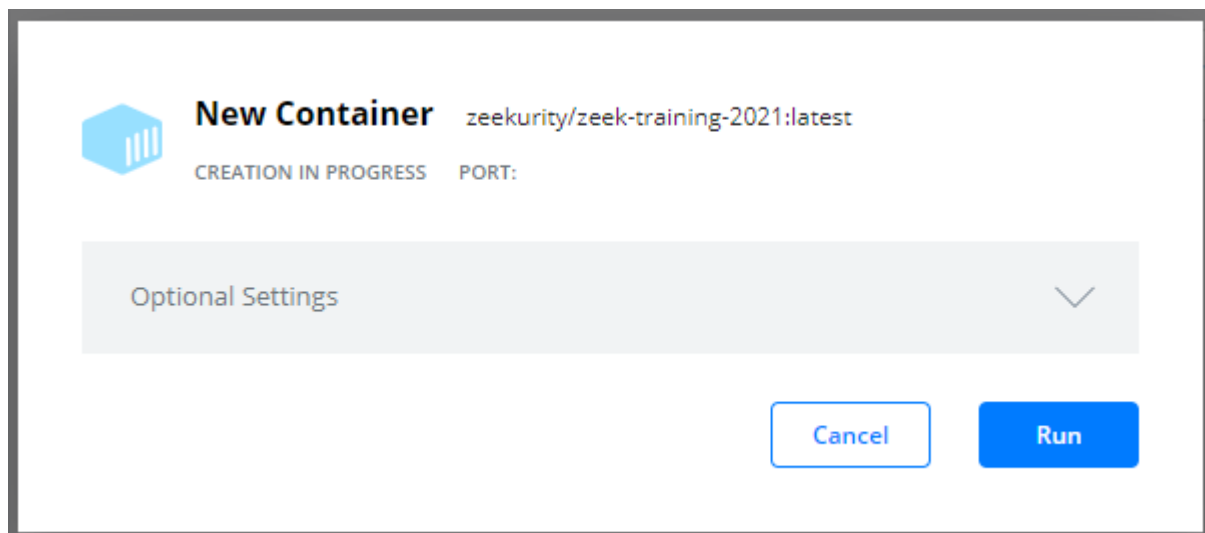
Step 5: Access the "Containers" menu option and click on the "CLI" button. It will open a command prompt and give us access to the live container running Zeek.

```
docker  exec -it 3f2e5df149f276c54665bea92542cf8a93d8b9edaed0fdc9c19eb47225b0721a /bin/sh
#
```

Step 6: Verify Zeek command is accessible.

       # **/opt/zeek/bin/zeek --version**