

ZeekWeek21 - Introduction to Zeek

Instructions for installation of Zeek in OS X

Step 1: We will be installing Zeek using docker. Download docker for Mac OS X using the link <https://docs.docker.com/desktop/mac/install/>

Step2: After docker has been successfully installed, open the Terminal app and docker command is working.

docker --version

A screenshot of a macOS Terminal window. The title bar shows the user 'swapneel@swapneel-2' and the window icon. The terminal content shows the last login time as 'Wed Oct 6 15:06:38 on ttys005'. The prompt is '~'. The user enters the command '\$ docker --version' and the output is 'Docker version 20.10.8, build 3967b7d'. The prompt is '\$'. The user enters the command '\$' and the prompt is '\$'.

```
swapneel@swapneel-2: ~
Last login: Wed Oct 6 15:06:38 on ttys005

~ 15:16:56
$ docker --version
Docker version 20.10.8, build 3967b7d

~ 15:17:22
$
```

Step 3: Pull the Zeek docker image using the docker command,

docker pull zeekurity/zeek-training-2021

```
swapneel@swapneel-2: ~  
~ 15:17:37  
$ docker pull zeekurity/zeek-training-2021  
Using default tag: latest  
latest: Pulling from zeekurity/zeek-training-2021  
0bc3020d05f1: Already exists  
b6ff8465a448: Already exists  
c913c300a426: Already exists  
867d566cf235: Already exists  
88beb3443fea: Already exists  
ae067c5a0603: Already exists  
9c9e72090c75: Already exists  
b368d7a9f8da: Already exists  
24beeea174d0: Already exists  
1de46056b28d: Already exists  
2a6d25c6421f: Already exists  
63ee5ddae99d: Already exists  
c6e21c2e8b6b: Already exists  
Digest: sha256:ae9f6a1e65b51bfbf72fd4d6f3cbfb7724abf95929e5580e80f2204ce6b1f953  
Status: Downloaded newer image for zeekurity/zeek-training-2021:latest  
docker.io/zeekurity/zeek-training-2021:latest  
~ 15:17:51  
$
```

Step 4: Start the container using the Zeek docker image and verify the zeek command,

`docker run -it zeekurity/zeek-training-2021 /bin/bash`

Inside the container run,

`zeek --version`

A terminal window with a dark title bar containing the text "docker run -it zeekurify/zeek-training-2021 /bin/bash". The terminal content shows a timestamp "15:18:04", a Docker command being executed, and the output of the "zeek --version" command.

```
~ 15:18:04
$ docker run -it zeekurify/zeek-training-2021 /bin/bash
root@7e9c17ac2295:/# zeek --version
zeek version 4.0.3
root@7e9c17ac2295:/#
```

Happy ZeekWeek21!