Paper: <https://arxiv.org/pdf/2003.01690.pdf> Code: <https://github.com/fra31/auto-attack>

1. From terminal/cmd:

**ssh** [**daryln@10.4.0.15**](mailto:daryln@10.4.0.15)**5 or ssh daryln@<server ip address>**

1. In server
   1. If container is not already running

command to run:

**docker run -it -p 8889:8889 --name autoattack -v /home/daryln/adversarial\_attacks/auto-attack:/workspace/auto-attack/ --gpus=1 mhilmiasyrofi/autoattack:latest**

* 1. If container is already running (should already be named)
     1. **docker start autoattack**
     2. **docker attach autoattack**

1. Auto attack directory is under /workspace as auto-attack
2. Run attack using

**python eval.py**

1. The adversarial images will be generated as .pth file under the results directory. A **log\_file.txt** will also be generated upon the completion of the above command. It contains results of the evaluation of the attack.

To view the imageset

To view them, it is recommended to open a Jupyter notebook for this. There is already one generated in the directory (**load images.ipynb)**.

To use Jupyter

Command to run: **jupyter lab --no-browser --ip=0.0.0.0 --port=8889 --allow-root**

Open the notebook and the code should already be written for you.

Using Pytorch to open

 

Using Numpy to open

 