Paper: <https://arxiv.org/pdf/1710.06081.pdf>

Code: **Non-Targeted Momentum Iterative attack** <https://github.com/dongyp13/Non-Targeted-Adversarial-Attacks>

**Targeted Momentum Iterative attack** <https://github.com/dongyp13/Targeted-Adversarial-Attack>

1. From terminal/cmd:

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

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

command to run:

**docker run -it -p 8891:8891 --name mi\_attack -v /home/daryln/adversarial\_attacks:/root --gpus=1 tensorflow/tensorflow:1.1.0-devel-gpu**

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

1. Momentum Iterative attack directory is under /root as Momentum-Iterative-Attack
2. Install required libraries: (pip install …)
   1. scipy==1.2.0
3. **cd Non-Targeted-Adversarial-Attacks**
4. Download dataset through: (It should already be downloaded and extracted in this container)

**curl -L -O** [**http://ml.cs.tsinghua.edu.cn/~yinpeng/adversarial/dataset.zip**](http://ml.cs.tsinghua.edu.cn/~yinpeng/adversarial/dataset.zip)

1. Download models through: (It should already be downloaded and extracted in this container)

**curl -L -O** [**http://ml.cs.tsinghua.edu.cn/~yinpeng/nips17/nontargeted/models.zip**](http://ml.cs.tsinghua.edu.cn/~yinpeng/nips17/nontargeted/models.zip)

1. **dataset/images** contains the subset of imagenet dataset
2. **mkdir adversarial\_output** to store the generated adversarial examples (Should already be created)
3. Run attack using

**./run\_attack.sh dataset/images adversarial\_output 70**

dataset/images -> the ImageNet images

adversarial\_output -> the directory that the adversarial images will be generated in

70 -> the intensity of perturbation to be applied to the images (MAX\_EPSILON)

1. The adversarial images will be generated as .png files under “adversarial\_output” directory.

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 (**Compare adversarial images.ipynb)**.

To use Jupyter

Command to run: **jupyter lab --no-browser --ip=0.0.0.0 --port=8891 --allow-root**

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

