Paper: <https://arxiv.org/pdf/1804.08598.pdf>

Code: <https://github.com/labsix/limited-blackbox-attacks>

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 8896:8896 --name nesattack -v /home/daryln/adversarial\_attacks/nes\_attack:/home --gpus=1 daryln/nesattack:latest**

The code can be accessed in the home directory (cd home/limited-blackbox-attacks)

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

1. Pip install requirements

tensorflow-gpu==1.15.0

Pillow

matplotlib

1. mkdir *data* in *tools* directory
2. curl -L -O <http://download.tensorflow.org/models/inception_v3_2016_08_28.tar.gz> in terminal and save it in *tools/data*
3. Create a new directory with a *val* directory inside. This val directory will contain the validation images of the ImageNet dataset. This new directory will contain the test images of the ImageNet dataset
4. curl -L -O <http://www.image-net.org/challenges/LSVRC/2012/dd31405981ef5f776aa17412e1f0c112/ILSVRC2012_img_test_v10102019.tar> to download test images (Extract the tar file and save the images)
5. curl -L -O <http://www.image-net.org/challenges/LSVRC/2012/dd31405981ef5f776aa17412e1f0c112/ILSVRC2012_img_val.tar> to download validation images (Extract the tar file and save the images in the val directory)
6. curl -L -O <https://github.com/labsix/limited-blackbox-attacks/files/5100014/val.txt> to save this labels file in the directory containing the test images
7. **Steps 3 to 9 has been done for you**

The test images and val folder containing the val images are in the directory **home/limited-blackbox-attacks/test**

1. Precompute using **python precompute.py test**
2. Run attack (3 variations)

**./query-limited.sh | ./partial-info.sh | ./label-only.sh**

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=8896 --allow-root**

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





