Paper: <https://arxiv.org/pdf/1802.00420.pdf>

Code: <https://github.com/anishathalye/obfuscated-gradients>

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 8894:8894 --name obfuscatedgradients -v /home/daryln/adversarial\_attacks/obfuscated-gradients:/home --gpus=1 tensorflow/tensorflow:1.15.0-gpu-py3**

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

1. Obfuscated Gradients attack directory is under /home
2. Install required libraries: (pip install …)
   1. Tensorflow-gpu==1.15
   2. keras==2.3.1
   3. scipy==1.1.0
3. Each directory contains a different variation of attack. Fetch models using **./setup.sh** (Models are already fetched)
4. Run the Jupyter notebook file in each directory to understand the attack. (**defensegan** is the only directory that does not seem to work)

To use Jupyter

**jupyter lab --no-browser --ip=0.0.0.0 --port=8894 --allow-root --NotebookApp.iopub\_data\_rate\_limit=1.0e10**

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