Paper: <https://arxiv.org/pdf/1805.00089.pdf> Code: <https://github.com/TrustAI/DeepConcolic>

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 deepconcolic -v /home/daryln/adversarial\_attacks:/home --gpus=1 daryln/deepconcolic:latest**

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

1. DeepConcolic attack directory is under /home as DeepConcolic
2. Install Anaconda and activate its virtual environment and follow the requirements in the paper
   1. tensorflow-gpu==2.0.0
3. Run attack using

**python deepconcolic.py --model ../saved\_models/mnist\_complicated.h5 --mnist-data --outputs outs/**

1. The adversarial images will be generated as .png files under the “outs” directory as specified above (I have renamed my folder to be “first\_run”).

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=8889 --allow-root**

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

 

