## Sample execution result

1. Run Adversarial_training.py

```
Successfully downloaded train-images-idx3-ubyte.gz 9912422 bytes.
Extracting /tmp/train-images-idx3-ubyte.gz
Successfully downloaded train-labels-idx1-ubyte.gz 28881 bytes.
Extracting /tmp/train-labels-idx1-ubyte.gz
Successfully downloaded t10k-images-idx3-ubyte.gz 1648877 bytes.
Extracting /tmp/t10k-images-idx3-ubyte.gz
Successfully downloaded t10k-labels-idx1-ubyte.gz 4542 bytes.
Extracting /tmp/t10k-labels-idx1-ubyte.gz
X_train shape: (60000, 28, 28, 1)
60000 train samples
10000 test samples
Defined TensorFlow model graph.
    Layer (type)                 Output Shape              Param #
    =================================================================
    conv2d_1 (Conv2D)            (None, 14, 14, 64)        4160
    _________________________________________________________________
    activation_1 (Activation)    (None, 14, 14, 64)        0
    _________________________________________________________________
    conv2d_2 (Conv2D)            (None, 5, 5, 128)         295040
    _________________________________________________________________
    activation_2 (Activation)    (None, 5, 5, 128)         0
    _________________________________________________________________
    conv2d_3 (Conv2D)            (None, 1, 1, 128)         409728
    _________________________________________________________________
    activation_3 (Activation)    (None, 1, 1, 128)         0
    _________________________________________________________________
    flatten_1 (Flatten)          (None, 128)               0
    _________________________________________________________________
```

```
dense_1 (Dense)              (None, 10)                1290
_________________________________________________________________
activation_4 (Activation)    (None, 10)                0
=================================================================
Total params: 710,218
Trainable params: 710,218
Non-trainable params: 0
Epoch 0
  Epoch took 125.58237195 seconds
Test accuracy on legitimate test examples: 0.9256
Epoch 1
  Epoch took 125.960160971 seconds
Test accuracy on legitimate test examples: 0.9518
Epoch 2
   Epoch took 126.341161966 seconds
Test accuracy on legitimate test examples: 0.9629
Epoch 3
   Epoch took 121.823987007 seconds
Test accuracy on legitimate test examples: 0.9710
Epoch 4
   Epoch took 124.107089043 seconds
Test accuracy on legitimate test examples: 0.9742
Epoch 5
   Epoch took 119.639467001 seconds
Test accuracy on legitimate test examples: 0.9764
Completed model training.
Test accuracy on adversarial examples: 0.0137

Repeating the process, using adversarial training
Epoch 0
   Epoch took 1937.52505207 seconds
```

```
Test accuracy on legitimate test examples: 0.9088
Test accuracy on adversarial examples: 0.2648
Epoch 1
    Epoch took 306.178752899 seconds
Test accuracy on legitimate test examples: 0.9472
Test accuracy on adversarial examples: 0.3639
Epoch 2
    Epoch took 281.781111956 seconds
Test accuracy on legitimate test examples: 0.9566
Test accuracy on adversarial examples: 0.3981
Epoch 3
    Epoch took 284.969310999 seconds
Test accuracy on legitimate test examples: 0.9638
Test accuracy on adversarial examples: 0.4533
Epoch 4
    Epoch took 294.823930979 seconds
Test accuracy on legitimate test examples: 0.9678
Test accuracy on adversarial examples: 0.4974
Epoch 5
    Epoch took 284.027938843 seconds
Test accuracy on legitimate test examples: 0.9704
Test accuracy on adversarial examples: 0.4985
Completed model training.

Process finished with exit code 0
```

2. Run CAE_training.py

| Layer (type) | Output Shape | Param # |
|---|---|---|
| input_1 (InputLayer) | (None, 1, 28, 28) | 0 |
| conv2d_1 (Conv2D) | (None, 16, 28, 28) | 160 |
| max_pooling2d_1 (MaxPooling2) | (None, 16, 14, 14) | 0 |
| conv2d_2 (Conv2D) | (None, 8, 14, 14) | 1160 |
| max_pooling2d_2 (MaxPooling2) | (None, 8, 7, 7) | 0 |
| conv2d_3 (Conv2D) | (None, 8, 7, 7) | 584 |
| max_pooling2d_3 (MaxPooling2) | (None, 8, 4, 4) | 0 |
| conv2d_4 (Conv2D) | (None, 8, 4, 4) | 584 |
| up_sampling2d_1 (UpSampling2) | (None, 8, 8, 8) | 0 |
| conv2d_5 (Conv2D) | (None, 8, 8, 8) | 584 |
| up_sampling2d_2 (UpSampling2) | (None, 8, 16, 16) | 0 |
| conv2d_6 (Conv2D) | (None, 16, 14, 14) | 1168 |
| up_sampling2d_3 (UpSampling2) | (None, 16, 28, 28) | 0 |
| conv2d_7 (Conv2D) | (None, 1, 28, 28) | 145 |

```
Total params: 4,385
Trainable params: 4,385
Non-trainable params: 0
Epoch 0
    Epoch took 380.548707008 seconds
Test accuracy on legitimate test examples: 0.9060
Test accuracy on adversarial examples: 0.1653
Epoch 1
    Epoch took 380.100882053 seconds
Test accuracy on legitimate test examples: 0.9364
Test accuracy on adversarial examples: 0.5875
Epoch 2
    Epoch took 379.717208147 seconds
Test accuracy on legitimate test examples: 0.9553
Test accuracy on adversarial examples: 0.8816
Epoch 3
    Epoch took 411.446470976 seconds
Test accuracy on legitimate test examples: 0.9647
Test accuracy on adversarial examples: 0.9303
Epoch 4
    Epoch took 421.051177025 seconds
Test accuracy on legitimate test examples: 0.9704
Test accuracy on adversarial examples: 0.9427
Epoch 5
    Epoch took 395.298976183 seconds
Test accuracy on legitimate test examples: 0.9735
Test accuracy on adversarial examples: 0.9465
Completed model training.
```