





ADVERSARIAL MACHINE LEARNING

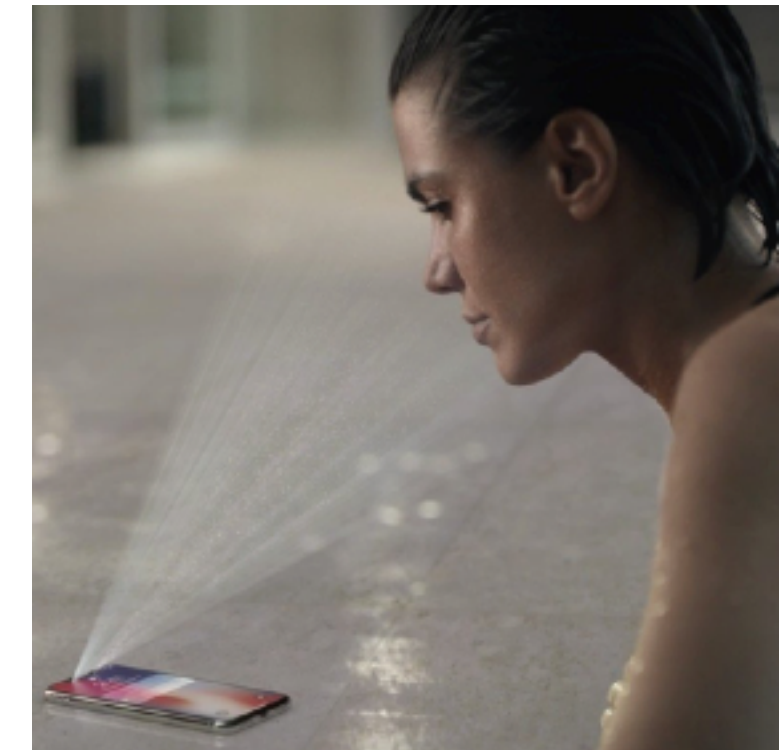
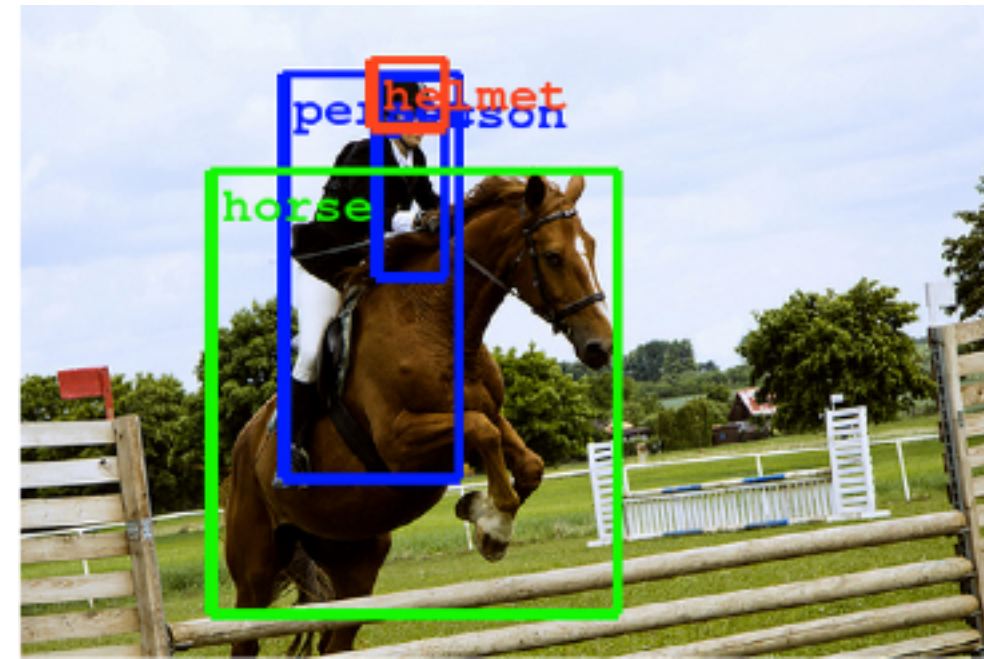
NILAY THAKOR & DR. DINESH GARG

IIT GANDHINAGAR



# SUCCESS OF DEEP NEURAL NETWORKS

- ▶ Computer Vision
  - ▶ Object Detection
  - ▶ Image Classification
  - ▶ Style Transfer
- ▶ Natural Language Processing
  - ▶ Machine Translation
  - ▶ Topic Modelling
  - ▶ Text Summary
- ▶ Decision Making
  - ▶ Self Driving Cars
  - ▶ Alpha Go



# ADVERSARIAL MACHINE LEARNING

---

NILAY THAKOR & DR. DINESH GARG  
IIT GANDHINAGAR