**Tasks:**

* **Presentation / Report**
  + Review research papers
  + Develop argument and reason for the work im doing
  + Devleop the plan
* **Deepspeech setup**
  + Setup deepspeech(end-to-end or MFCC???)
  + Select couple of phrases
  + Verification that it works
* **Signal Processing Attacks**
  + Implement signal processing attack algorithm
    - <https://hadiabdullah.github.io/>
    - In class I heard high pitch noise(probably from some technology component). It’s annoying but when listening to lecture its just noise. Now what if it was encoded with a ASR message that could be transcribed(This would be over-the-air which has limitations based on hardware and speakers. I’ll focus on over-the-line in simplified case)
  + If time permits implement audio adversarial examples
    - https://nicholas.carlini.com/code/audio\_adversarial\_examples
  + Make sure it works
* **Explainable AI**
  + Devleop algorithm and purpose
    - <https://christophm.github.io/interpretable-ml-book/counterfactual.html>
  + Can the algorithm be a counterfactual search from original message to noise. What is the minimum amount of a specific signal processing attack that prevents from human hearing
  + <https://ieeexplore.ieee.org/abstract/document/7498923>
  + Psychoacoustic algorithm to quantify how much algorithmic attack?
  + LIME Visualization of audio: “Let me explain!”: exploring the potential of virtual agents inexplainable AI interaction design, Katharina Weitz,Dominik Schiller,Ruben Schlagowski,Tobias Huber, Elisabeth Andre.
    - Could show visualization of spectrum of the attack one showing htat it works.

**Side Notes:**

* Mozilla DeepSpeech: Unlike other deepspeech, uses RNN and end-to-end feature engineering. Instead of MFCC to obtain features, it uses an NN for feature extraction instead.