Reverse-Engineering WiFi

Diana Zhang
Recitation #1, 18-441/741
January 25th, 2019

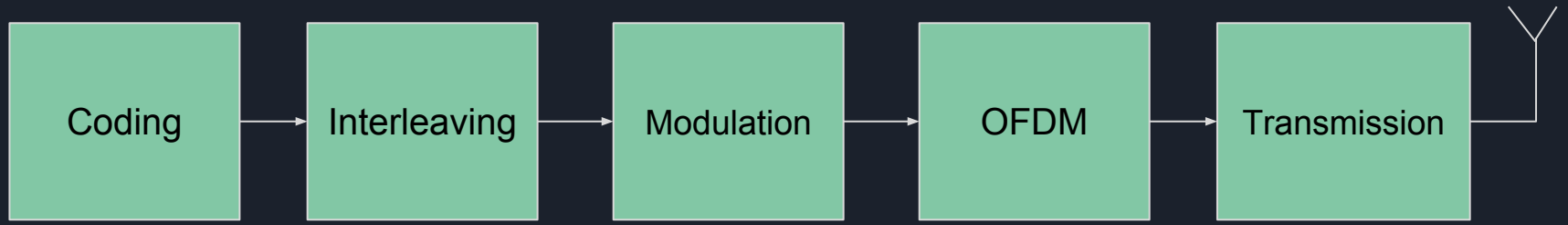
WiFi Overview

WiFi is a *Wireless* LAN(Local Area Network) defined by IEEE 802.11 standards, with interoperability ensured by the WiFi Alliance industry group.

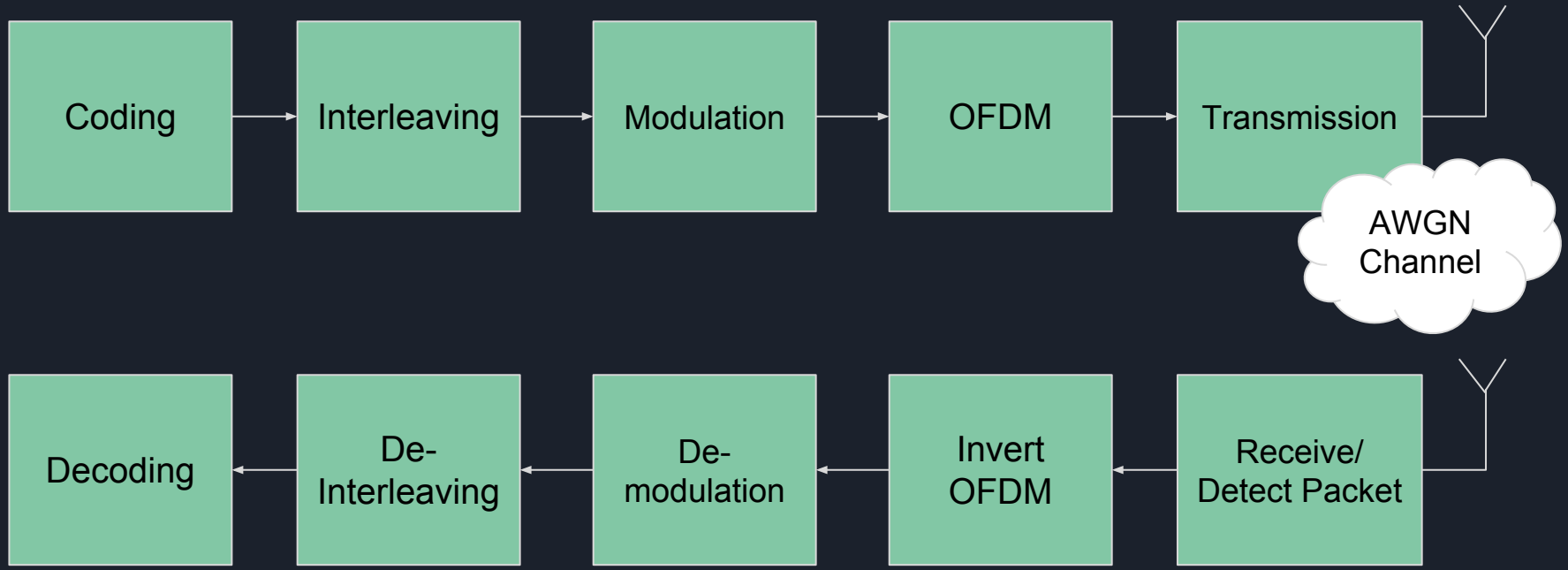
Defined by specific Data Link and Physical Layer protocols, a few of which you'll be interacting with on this project.

Being *wireless* results in the case where everyone in an area shares a medium -- imagine seven computers not coordinating with each other, on a faulty bus that drops bits sometimes.

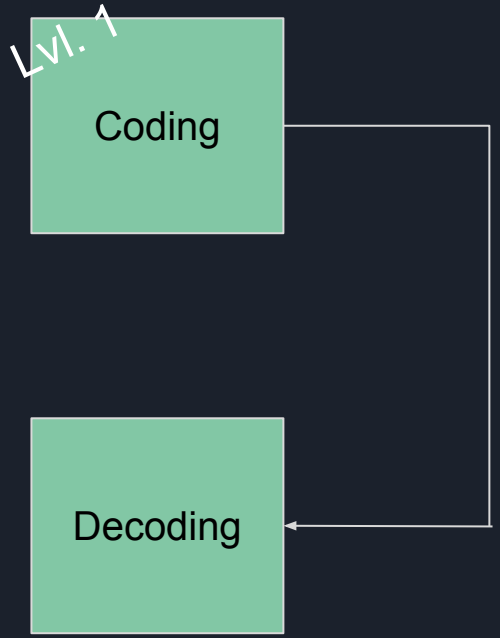
Project 1 Steps



Project 1 Steps



Where to Start?



What is Coding?

The wireless environment is challenging! People move. Dogs knock over routers. Seven people try to stream video on this shared spectrum at once.

Coding introduces *redundancy* into your bits, so a message can be recovered even if some bits are lost, at the cost of more bits to transmit for a message.

The most basic code is a repetition code:

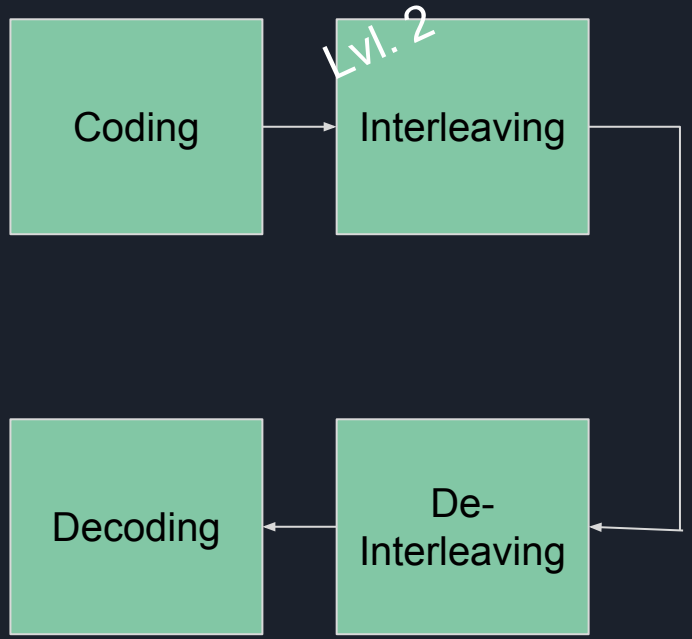
0 1 0 1 1 0 -> 000 111 000 111 111 000

Okay...so what's this Trellis encoding thing?

The turbo encoding scheme that WiFi uses is a type of trellis encoding, which is an encoding scheme that uses state machines to encode data. They are often paired with Viterbi Decoders.

Example on board...

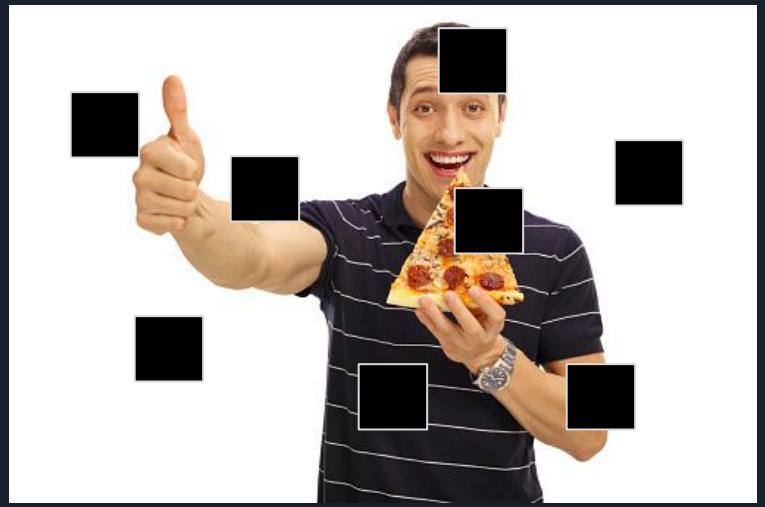
Project 1 Steps

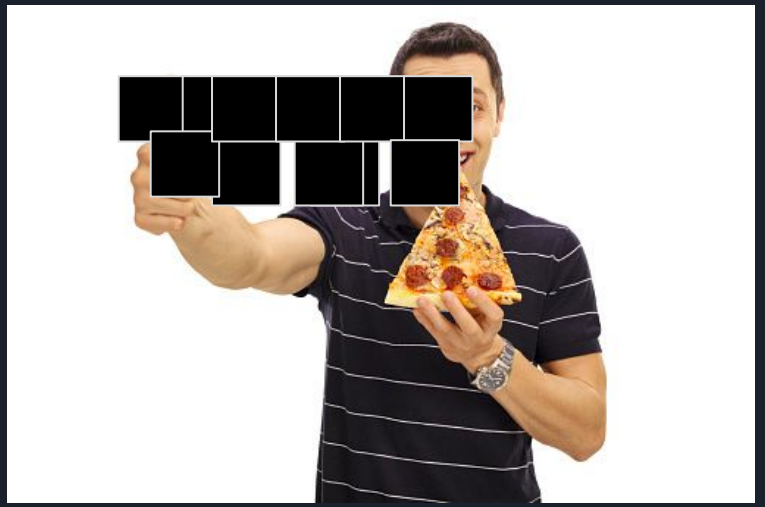


Symbols

A symbol is one or more bits transmitted in a “pulse.” WiFi uses multiple different *subcarriers*, which are small slices of frequency ranges, to send multiple bits per symbol. In this project, a symbol is defined as nfft=64 bits.

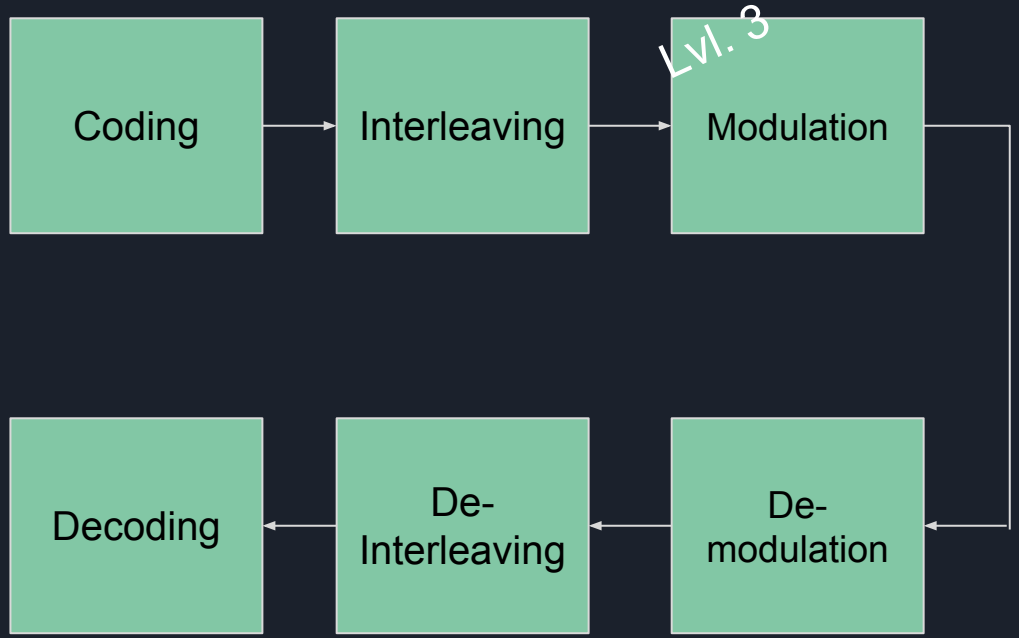
Interleaving shuffles bits to prevent large contiguous chunks of data being lost.





Check out the Interleave Variable in wifitransmitter.m!

Project 1 Steps



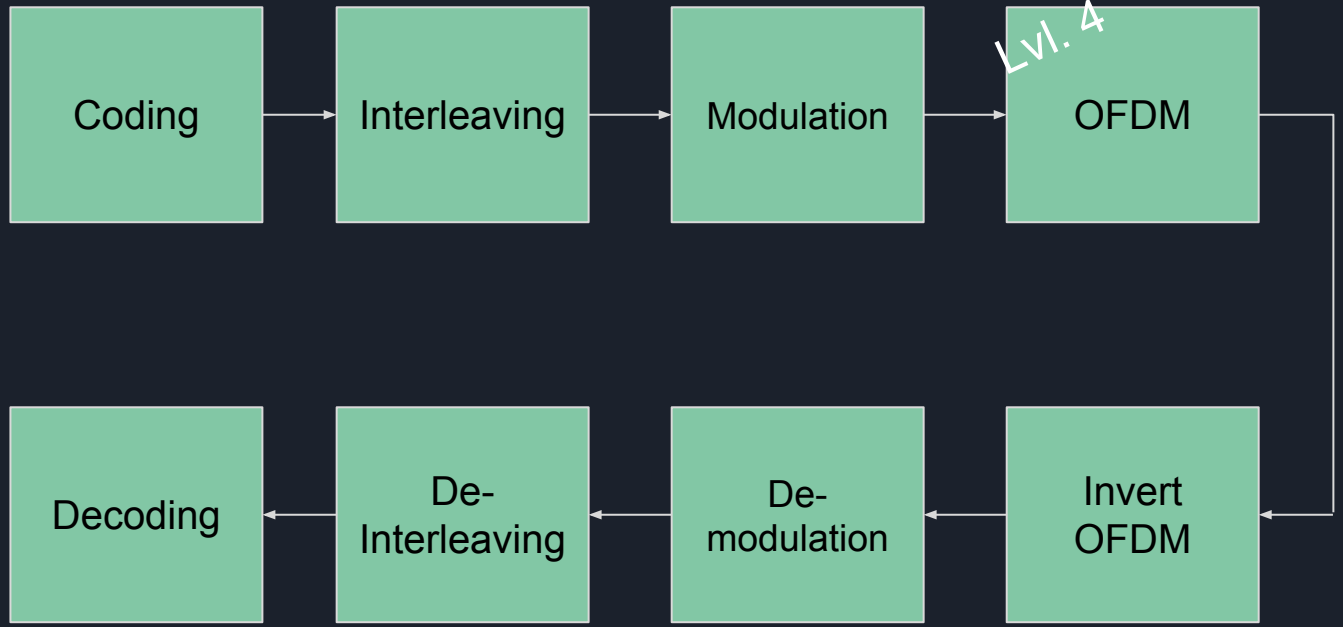
Modulation: What do bits look like in the air?

Modulation: What do bits look like in the air?

They don’t! In the air, signals are sent with some combination of phase and power offsets. This can be visualized in signal constellations. One of the most fundamental types of modulation is QAM (quadrature amplitude modulation), which is what you use in this project.

Drawings on board...

Project 1 Steps



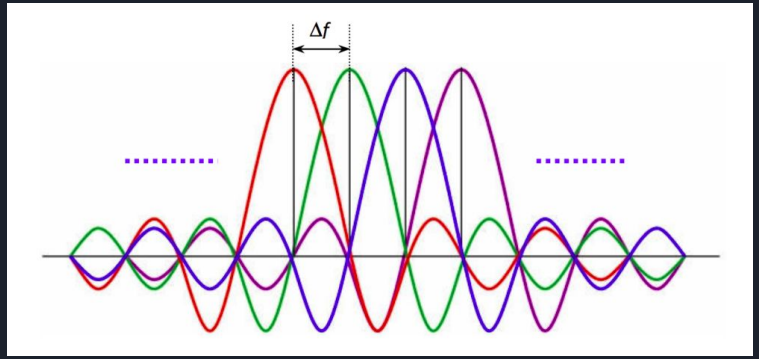
Orthogonal Frequency Domain Multiplexing (OFDM)

How do you increase throughput?

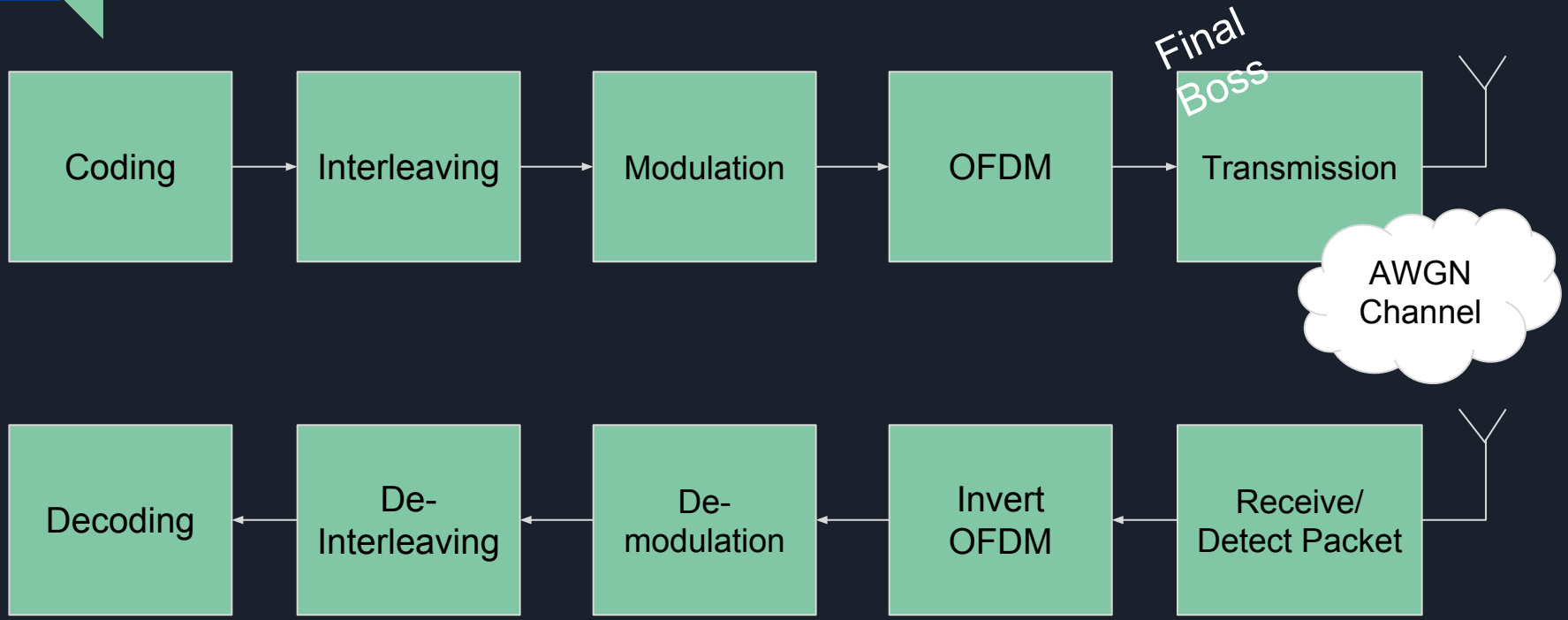
Goals: Increase Symbol Length for less Inter-Symbol Interference, handle frequency-selective fading.

Orthogonal Frequency Domain Multiplexing (OFDM)

Instead of square waves, you can layer sinc waves so the nulls align with the peak of the new signal. Convert from square waves to sinc using FFT!

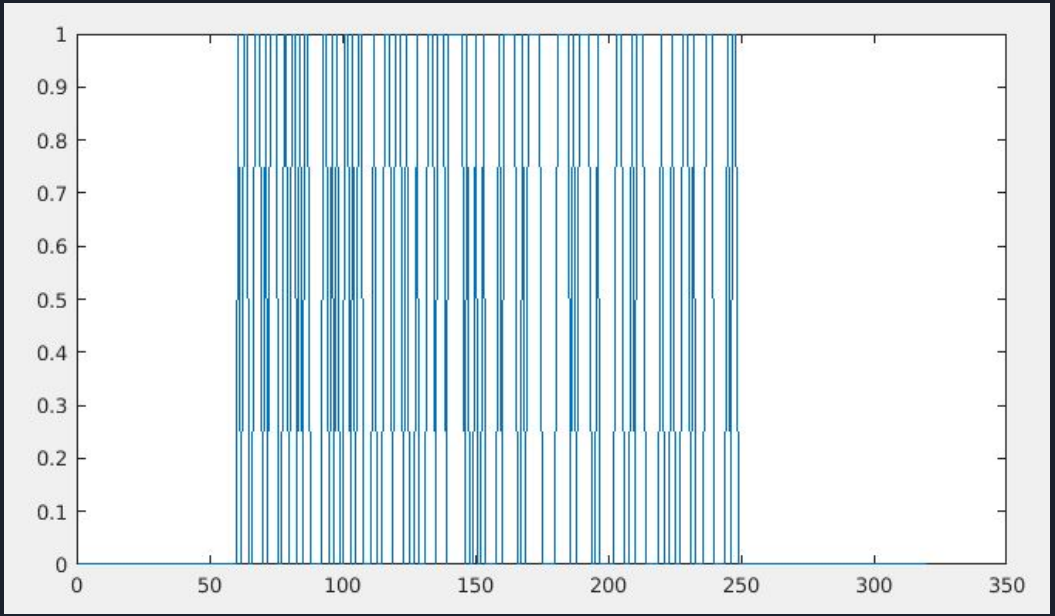


Project 1 Steps

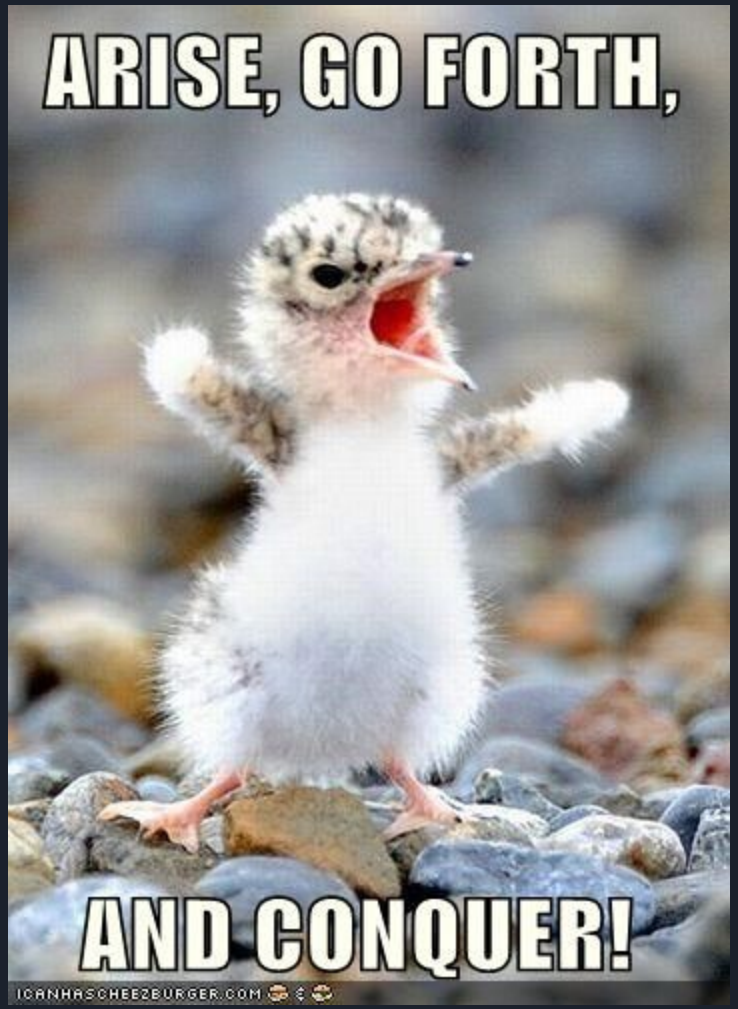


Receiving/Detecting a Packet

‘hello world’, plotted



Approach
Ideas?


ARISE, GO FORTH,
AND CONQUER!
ICANHASCHEEZBURGER.COM