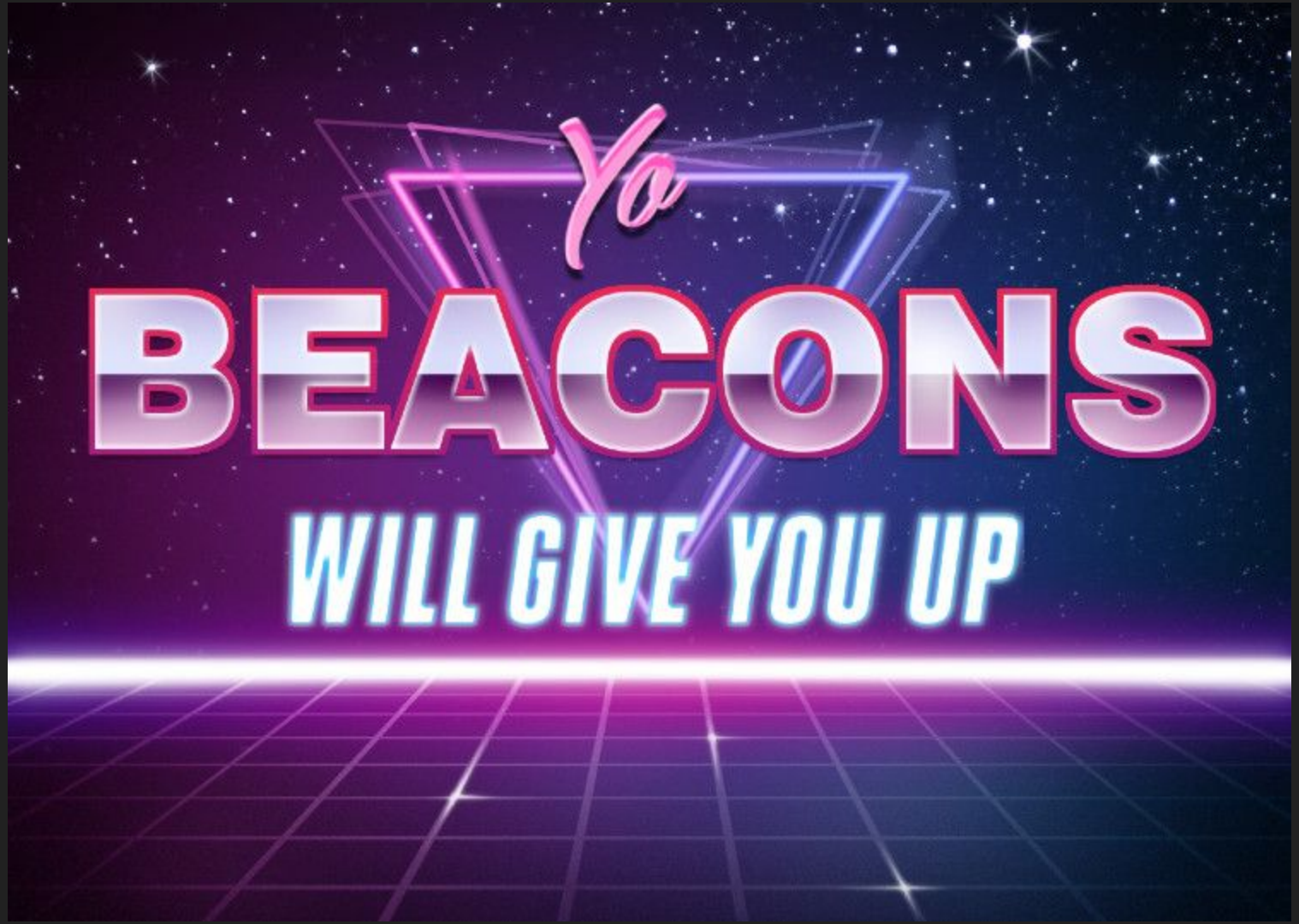

Yo
BEACONS
WILL GIVE YOU UP

Wi-Fi Beacons will give you up

By: John Aho
@dj_ir0ngruve

Who am I?

-John Aho @dj_ir0ngruve

Programmer who makes some useless things and occasionally accidentally useful ones.

-Made a gui wrapper years ago for a command line code auditing tool (scraping the barrel here)

-ported TryCatchHCF's cloakify to powershell (text based steganography)

-Rick Rolled a bunch of people last year over wifi ssid's with ESP8266's

-My Views / opinions are my own and not employers and all that.

Agenda

-Introduction

-Show the roll

-How to set them up the roll…

-About ESP8266’s

-Kinds of fun you can have with ESP8266’s

-Demo the Beacon8r

-Github info

-Code Show QA

Roll me!

-Check Wifi

-See for yourself

How to roll your own?

-You need an ESP8266 unit

-Code for the Roll - on github via me and many others

-Computer to run Arduino IDE

-A usb battery pack to be portable

-Google Fu if you run into problems

*Code for this will be gone over at end of session.

THEN YOU TOO CAN SET US UP THE ROLL!

More about ESP8266's

Showed up on the scene in 2014

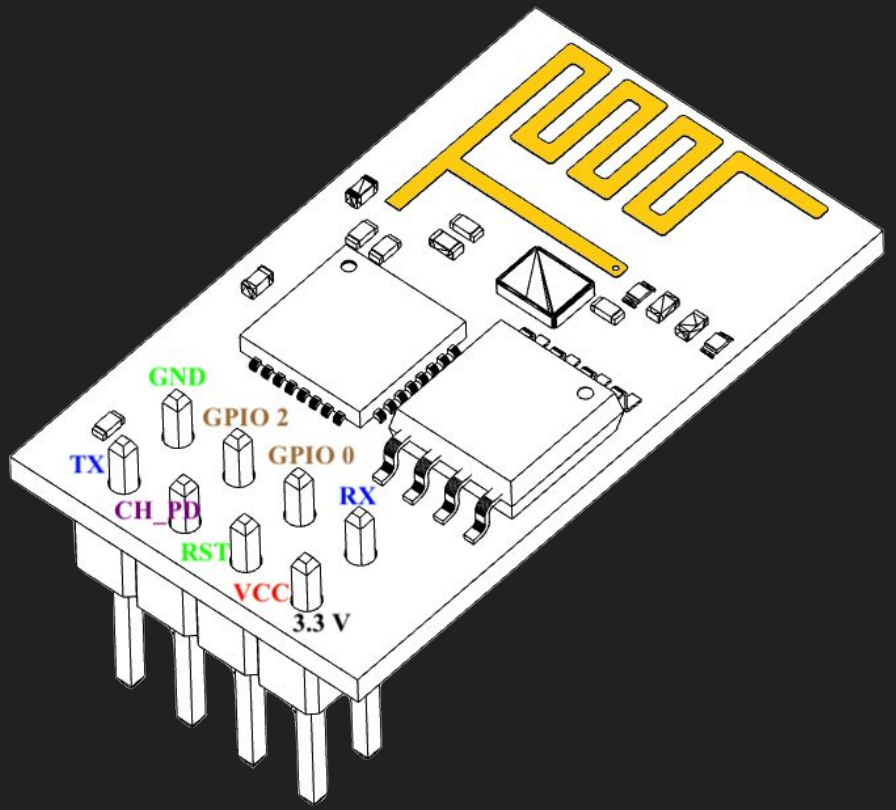
Low cost wifi board lots of possibilities

Loads of SDK's to program with

Many companies produced versions

-Big Info Dump

(vilian exposition)



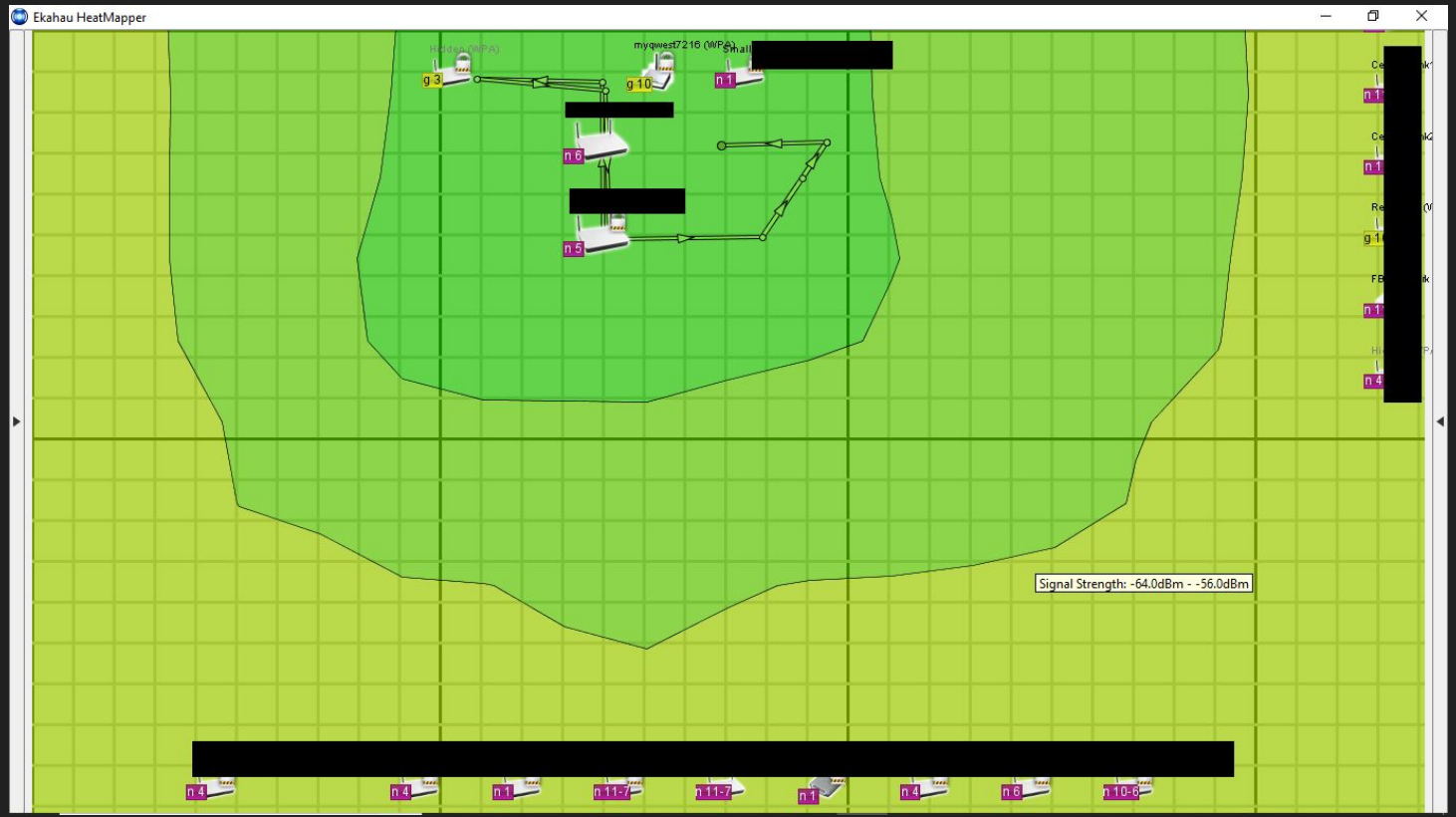
Ekahau’s Wifi mapper results…

-Laptop based wifi graphical mapper

-Produces spiffy results of base stations, signal strength and all that

-Most importantly it produces pretty graphics. We like pretty graphics.

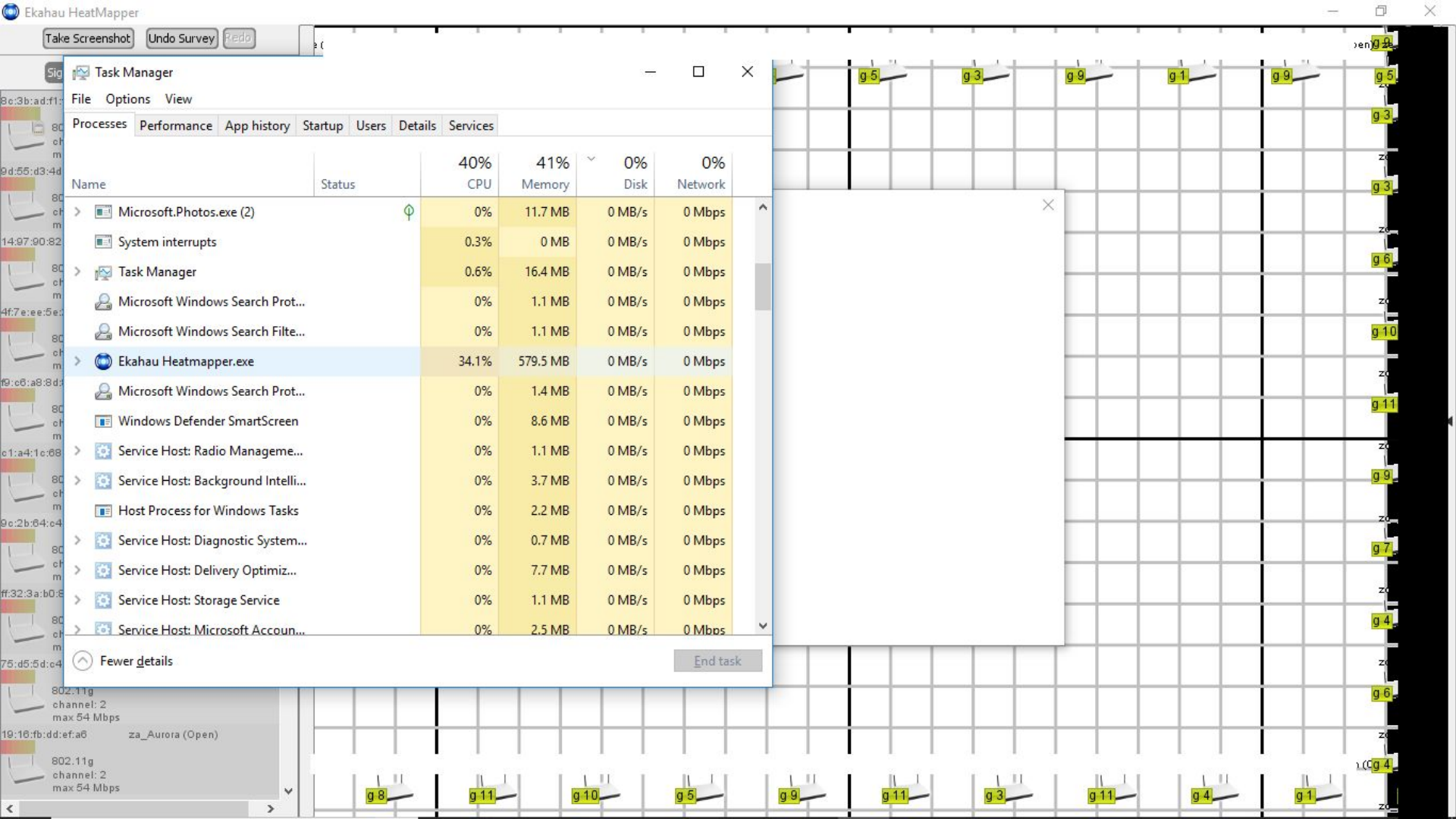
Baseline Scan with ambient WiFi



Turning on 14 early beacon8r’s

-WAIT FOR IT…

…….. LOADING>>>>


Ekahau HeatMapper
Take Screenshot
Undo Survey
Redo
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name Status 40% CPU 41% Memory 0% Disk 0% Network
Microsoft.Photos.exe (2) 0% 11.7 MB 0 MB/s 0 Mbps
System interrupts 0.3% 0 MB 0 MB/s 0 Mbps
Task Manager 0.6% 16.4 MB 0 MB/s 0 Mbps
Microsoft Windows Search Prot... 0% 1.1 MB 0 MB/s 0 Mbps
Microsoft Windows Search Filte... 0% 1.1 MB 0 MB/s 0 Mbps
Ekahau Heatmapper.exe 34.1% 579.5 MB 0 MB/s 0 Mbps
Microsoft Windows Search Prot... 0% 1.4 MB 0 MB/s 0 Mbps
Windows Defender SmartScreen 0% 8.6 MB 0 MB/s 0 Mbps
Service Host: Radio Manageme... 0% 1.1 MB 0 MB/s 0 Mbps
Service Host: Background Intelli... 0% 3.7 MB 0 MB/s 0 Mbps
Host Process for Windows Tasks 0% 2.2 MB 0 MB/s 0 Mbps
Service Host: Diagnostic System... 0% 0.7 MB 0 MB/s 0 Mbps
Service Host: Delivery Optimiz... 0% 7.7 MB 0 MB/s 0 Mbps
Service Host: Storage Service 0% 1.1 MB 0 MB/s 0 Mbps
Service Host: Microsoft Accoun... 0% 2.5 MB 0 MB/s 0 Mbps
Fewer details
End task
802.11g channel: 2 max 54 Mbps
19:16:fb:dd:ef:a6 za_Aurora (Open)
802.11g channel: 2 max 54 Mbps

Had an error before so not quite perfect test...

-RESTART and try again…..

Ekahau HeatMapper

Take Screenshot | Undo Survey | Redo

Signal | Channel | SSID | MAC | Security

802.11n
channel: 6
max 72 Mbps

802.11n
channel: 5
max 217 Mbps

802.11g
channel: 5
max 54 Mbps

802.11g
channel: 11
max 54 Mbps

802.11g
channel: 2
max 54 Mbps

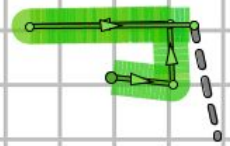
802.11g
channel: 2
max 54 Mbps

802.11g
channel: 6
max 54 Mbps

802.11g
channel: 1
max 54 Mbps

802.11g
channel: 1
max 54 Mbps

802.11g
channel: 3
max 54 Mbps



Results?

-Scan took a LOOOOONNNG time to process and display graph.

Many minutes

Machine was sluggish..

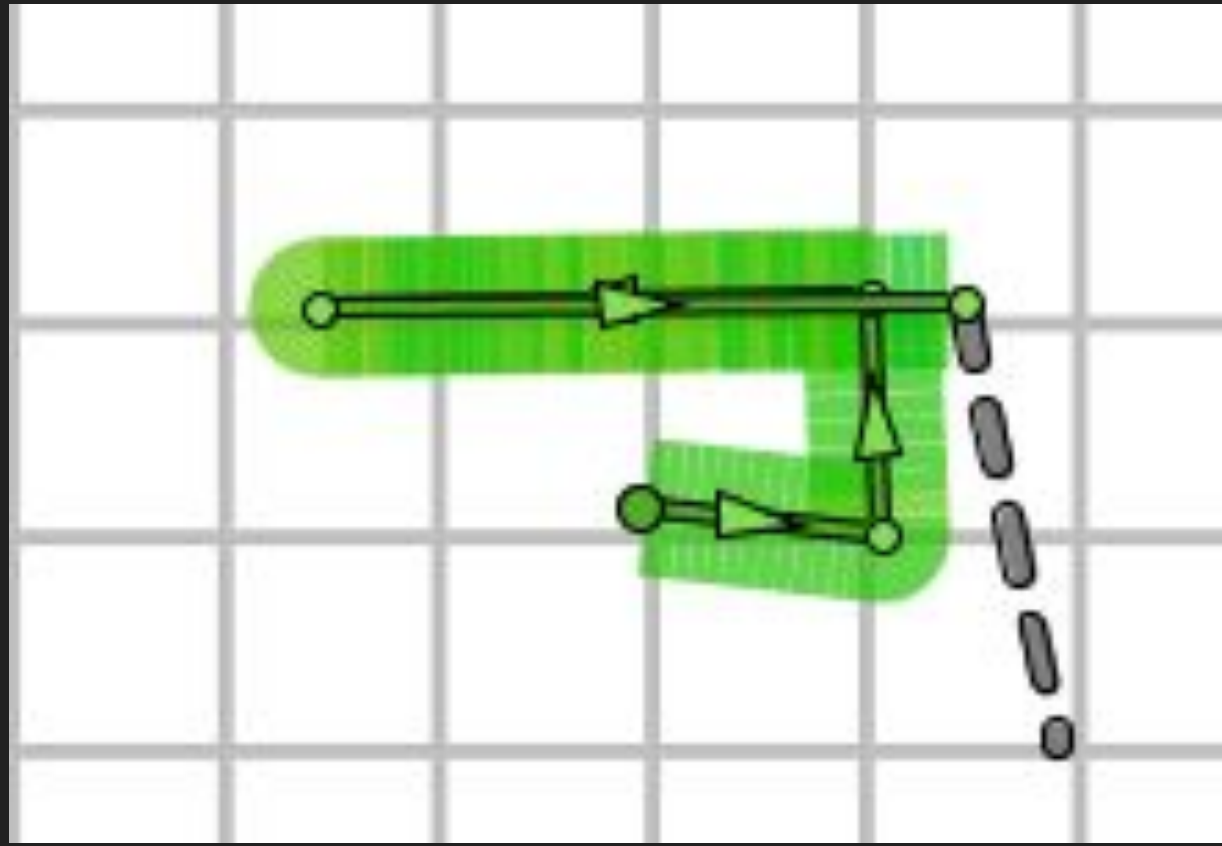
Results *may* not be typical - not a super fast laptop used for survey.

Zoom in, Enhance

-Enhance broken..

Notice all the lines?

-Unique Access points



Stuff you can do with ESP8266

-WiFi De-author - SpaceHun!!! -educational purposes only.. Probably not a good idea

-Lots of shields

-Button shields

Limitations of ESP8266

-Single threaded

-limited to 3.3v on most pins

-MicroSD card reading is SLOOOOWWWW.

--Literally watching words show up on screen as page loaded.

--Could be a PEBKAC issue with me though.

Somethings missing...

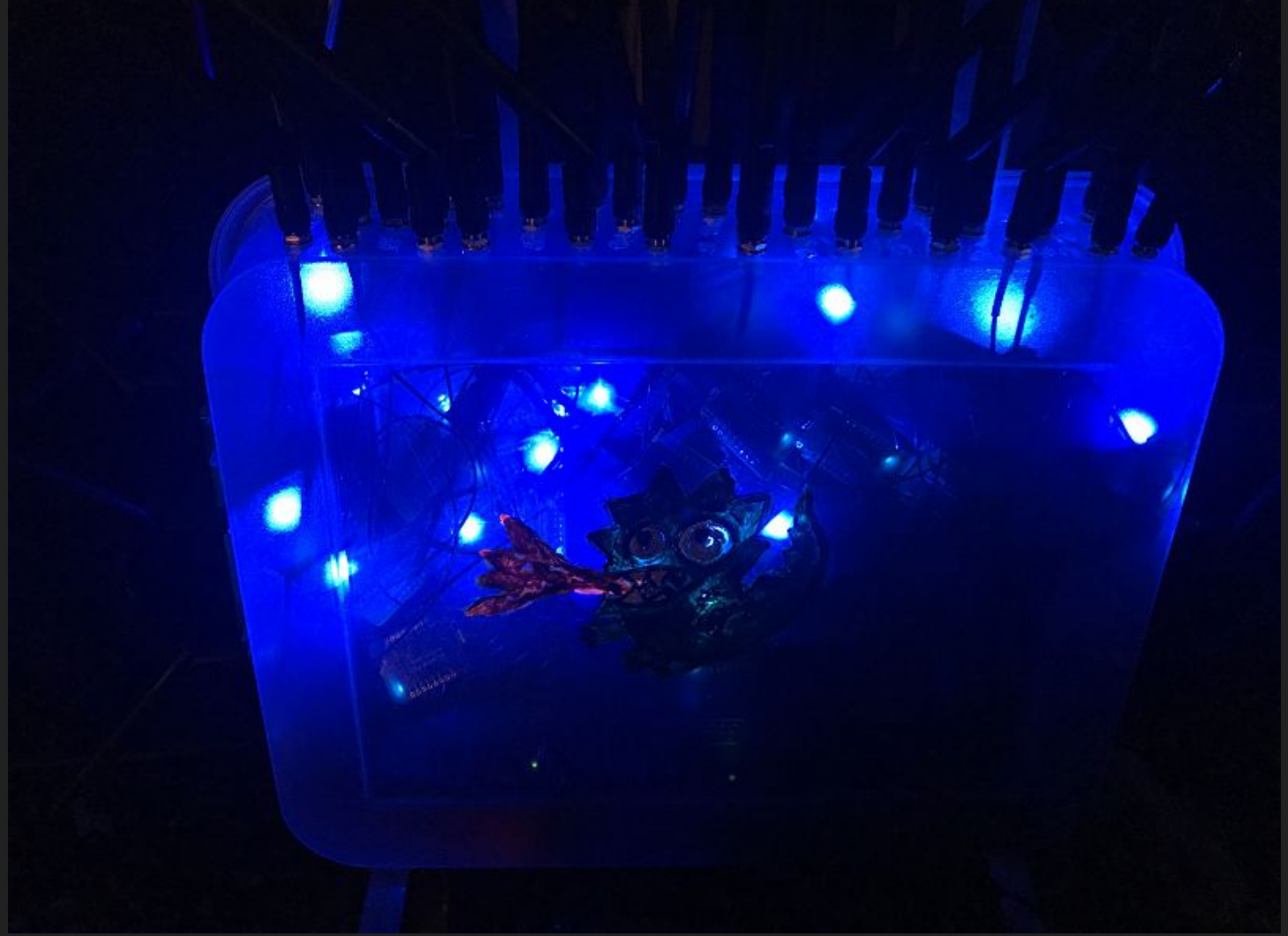
--At first beacons weren't showing up in wireshark…

--Turns out had to set the time of the beacon rame for my version of wireshark to capture it.

```
 currentTime = millis(); //gets current time
uint8_t packet[128] = ........


 // later on.....
 packet[24] = currentTime;
```

?



Beacon8r v1

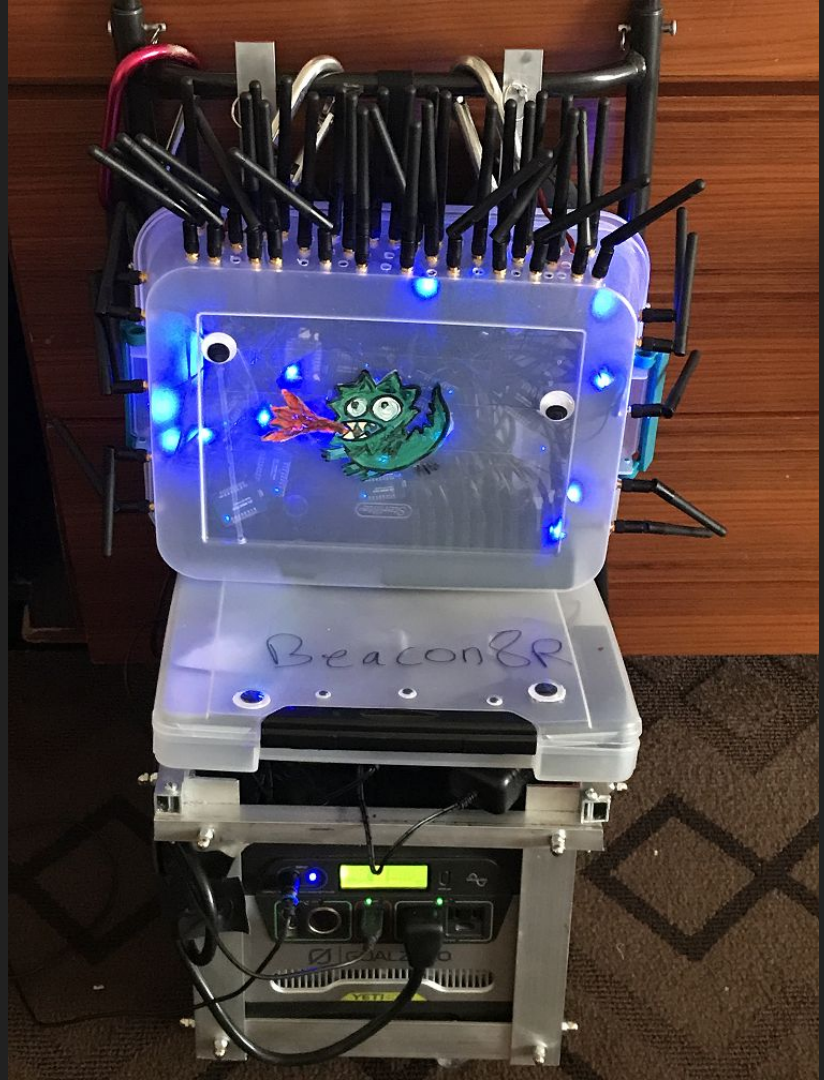
Potato build quality

Not that efficient

Makes up for it cool logo.

Can run for a few hours no big deal

Got lights no?



Beacon8r

-Aluminum Frame

    -Hardware store components

-Main section has 44 WeMos D1 Pro’s with Antennas

-Secondary has 13 NodeMCU’s broadcasting various stoofs.

-Big old tech battery

    -AGM lead acid baby!

-Coolest feature of all? Swivel WHEELS!

Frame shot

Mobile Book library...

-Sort of..

-Electronic only

-Set 4 ESP8266’s to act as web servers on port 80

-Every index request to it returns ENTIRE html book!

    -Thanks to Gutenberg Library for awesome online books.

-Each is programmed to auto-joins DefCon-Open on power up.

-Hopefully wifi sniffers will end up with lots of copies of books!

Book Choice #1 - Frankenstein

-Added image to each

-Shout out to @Foone

*Sierra Death Generator

Frankenstein;

or, the Modern Prometheus

by

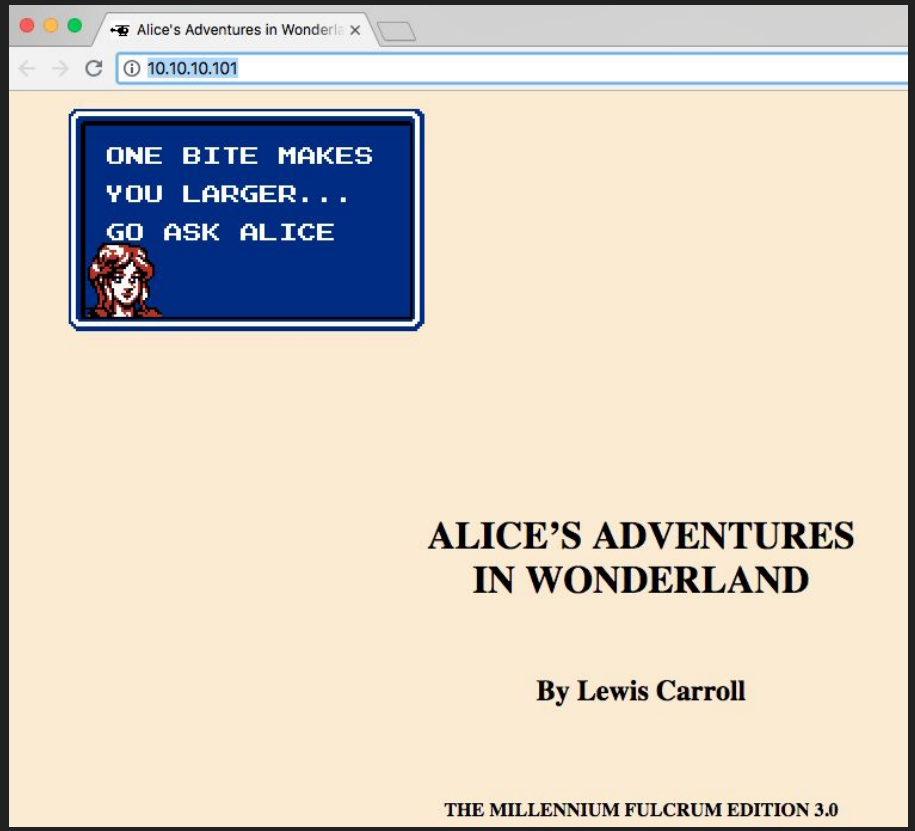
Mary Wollstonecraft (Godwin) Shelley

Book Choice #2 - Alice in Wonderland

-Added image to each

-Shout out to @Foone

*Sierra Death Generator

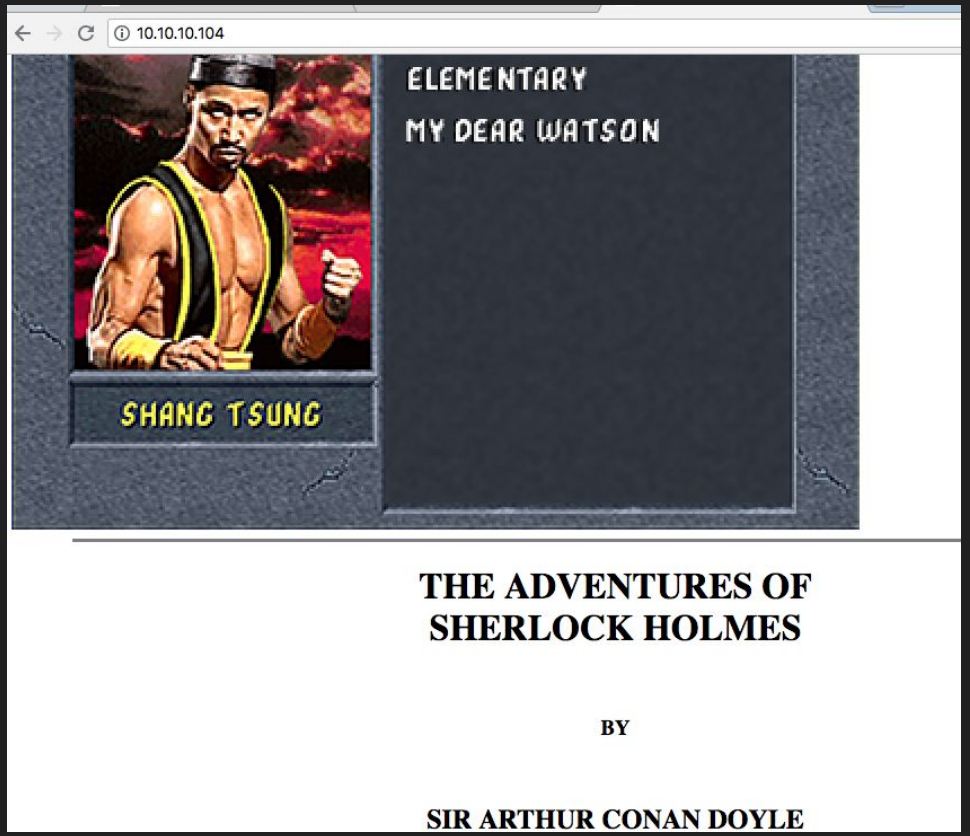


Book Choice #3 - Sherlock Holmes

-Added image to each

-Shout out to @Foone

*Sierra Death Generator



Book Choice #4 - Little Brother

-Thanks Cory Doctorow!

-Shout out to @Foone

*Sierra Death Generator

See the end of this file for the complete legalese.

INTRODUCTION

I wrote Little Brother in a white-hot fury between May 7, 2007 and July 2, 2007: exactly eight weeks from the day I tho
whom this book is dedicated, had to put up with me clacking out the final chapter at 5AM in our hotel in Rome, where
always dreamed of having a book just materialize, fully formed, and come pouring out of my fingertips, no sweat and fu
thought it would be. There were days when I wrote 10,000 words, hunching over my keyboard in airports, on subways,
was trying to get out of my head, no matter what, and I missed so much sleep and so many meals that friends started to

Possible future uses..

-Mobile library

-Make DIY Survival Beacons you can plug in to get access to survival info

    -Solar powered survival unit?

-Scavenged for parts for another project?

-Who knows?

"ESP8266's are a gateway drug to microcontrollers"
And possibly geekily bad decisions.

John Aho

Contact: @dj_ir0ngruve

Github: https://github.com/johnaho/Beacon8r

GitHub will be live in a few days.

GitHub then… CODE SHOW QA!

Me: John Aho

Contact: @dj_ir0ngruve

Github: https://github.com/johnaho/Beacon8r

GitHub will be live in a few days.

This is part where I open up arduino and load and explain the various uglicalities if there are questions.