Weaponizing your Pets

The War Kitteh and the Denial of Service Dog

DefCon

10 August 2014

tenacity

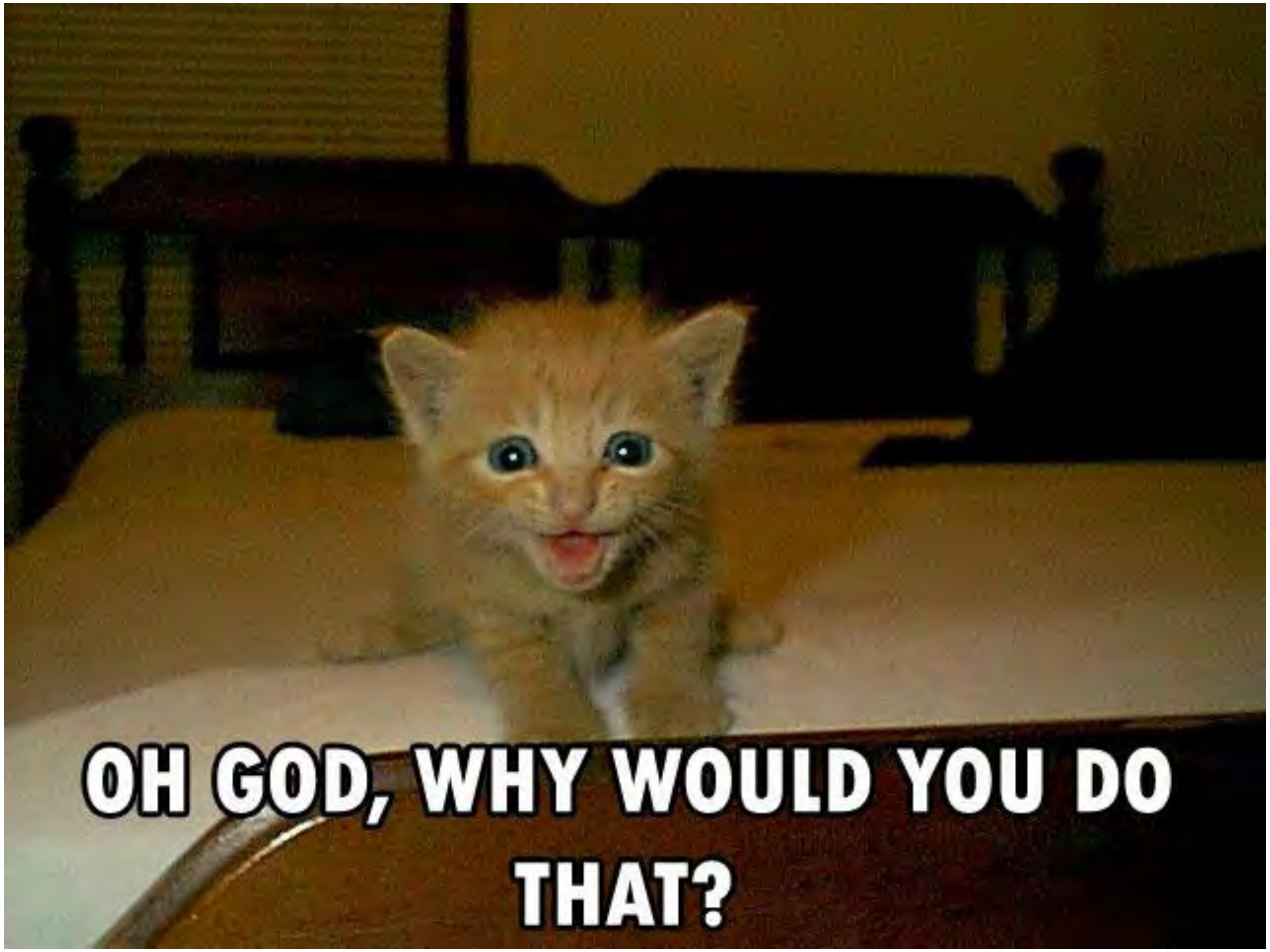
Introductions

- Gene Bransfield @gbransfield
- Principle Security Engineer @ Tenacity
- I Love My Job
- They want my job
- They can't have it

What is This About?

- Having a humorous idea
- Bringing Ideas to Fruition
- Stories of Triumph and Woe
- Valuable Lessons Learned

Weaponize your PETS!?!?!



Background:

- 15% of the world's Internet traffic is dedicated to Cats
- I find most tech briefings boring, so I use pics of cats to help keep people awake

The pic that started it all:

Just Finished a Presentation…

- Someone told me they were going to give me this tracking collar that they won
  - GPS
  - Cellular
  - Told you where the Kitteh was at all times

- …add a little wifi sniffer and we'd have a WAR KITTEH!!!!

What about the DoS Dog?

- AT Outerz0ne
- LadyMerlin walked in with a dog all tricked out with saddlebags and WiFi Gear
  - – Called it a WiFi Service Dog
- I said “Should have put a Pineapple in there and call it a Denial of Service Dog”

Working Animals

Bad Ass Working Animals

Badder Ass Working Animals

Real Navy Seal

Flipper Pic

More Flipper

Monkeys

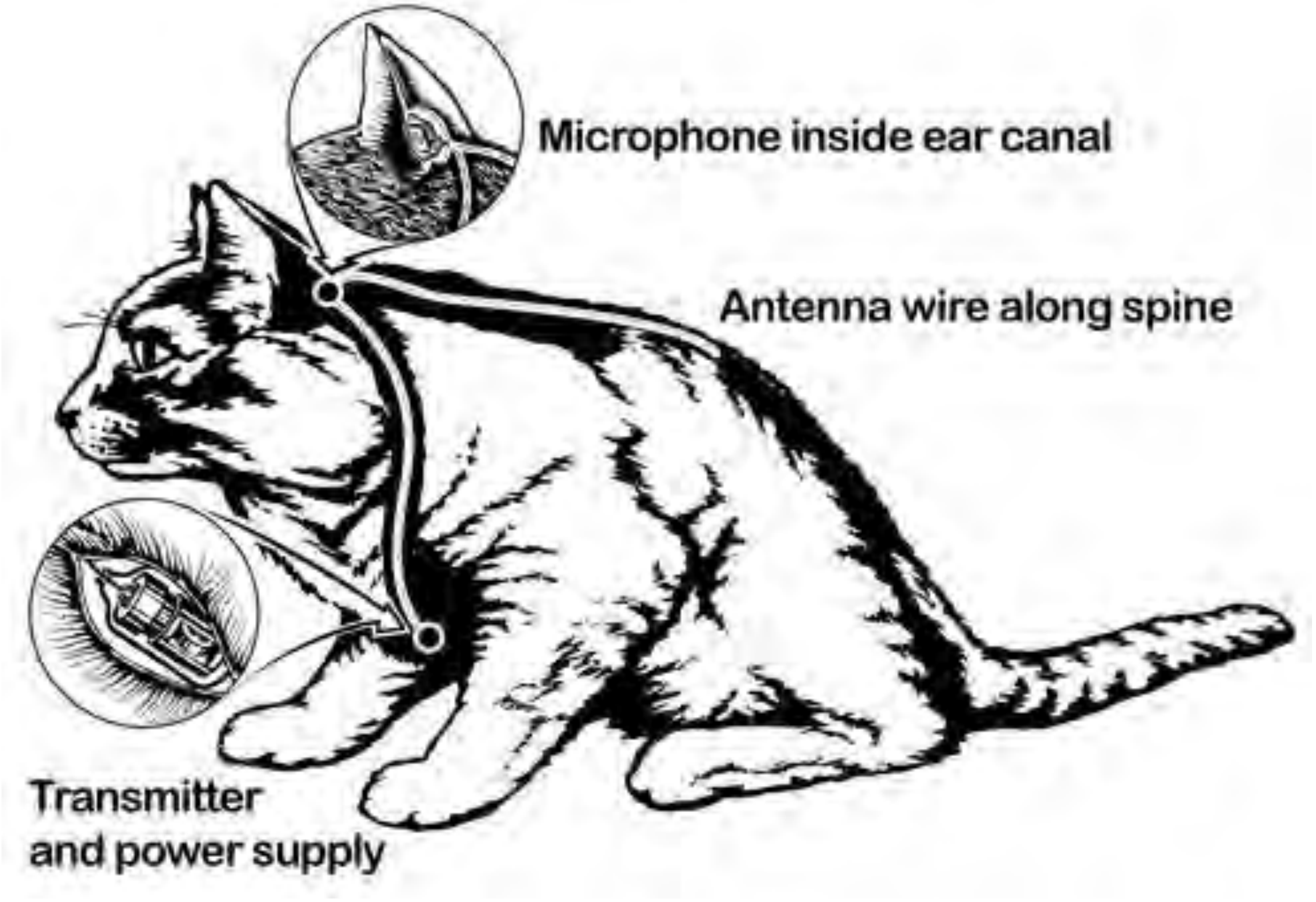
PLA DAILY/ CHINESE AIR FORCE NETWORK/MINISTRY OF NATIONAL DEFENSE

More Monkeys

PLA DAILY/CHINESE AIR FORCE NETWORK/MINISTRY OF NATIONAL DEFENSE

Other Research Efforts

- Accoustic Kitty



MY STUFF -- Requirements

- War Kitteh Requirements:
- CONOP: Put a collar/harness on a cat and allow said feline to roam the neighborhood normally. The collar/harness shall contain a GPS tracking device and a wireless sniffer/scanner. We'll be looking to map WiFi Access points similar to war driving.
  - 0.) CAT SHALL NOT BE HARMED
  - 1.) Cat shall be able to comfortably wear stuff and should not be harmed by said stuff or by wearing said stuff
  - 2.) GPS shall record waypoints with associated date/time stamp for collection post-walkabout (e.g. when the cat returns).
    - a.) optionally, solution to provide on-demand locational data as well so we can find a lost kitteh or kitteh harness
  - 3.) WiFi sniffer scanner shall sync time with GPS device and collect wifi SSIDs and other WiFi-related signals for later Analysis

Other Products

- Mr Lee Cat Cam
  - http://www.mr-lee-catcam.de
- Pet Tracker
  - http://www.pettracker.com
- Garmin
  - https://buy.garmin.com/

GumStix

http://specialcomp.com/gums
MADE IN U.S.A.
STAINLESS STEEL
1
2
3
4
5
6

©

Cotton Candy

RockChip 3066

Thinking about it…

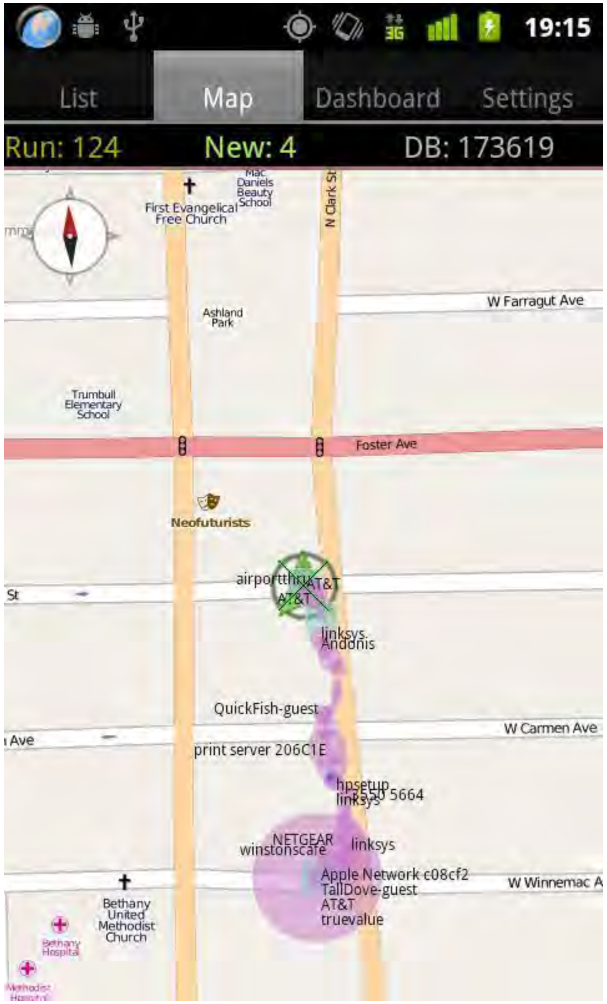
- Small form factor
- GPS
- Wifi
- Cellular

How ‘bout a Cell Phone?

Now make an APK!?!?

- Need to code a wifi war driving
- Let’s do some android coding…?
- They already thought of that…

WiGLE WiFi

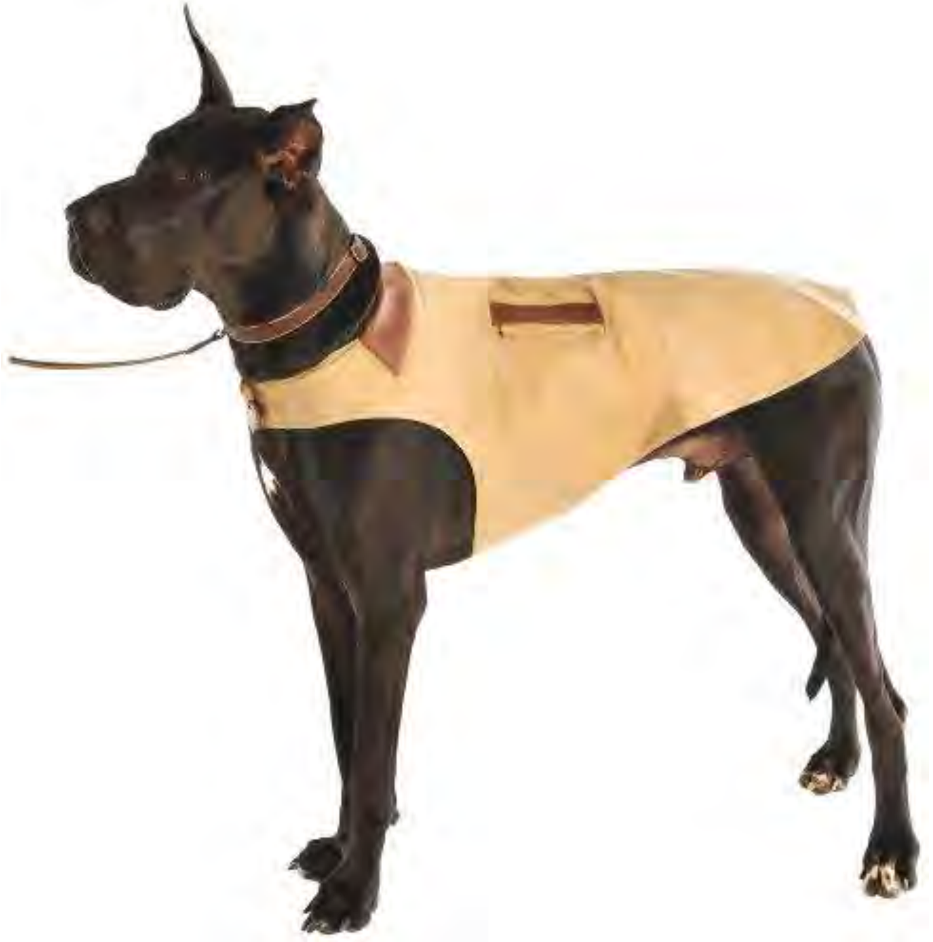


19:15
List
Map
Dashboard
Settings
Run: 124
New: 4
DB: 173619
First Evangelical Free Church
Mac Daniels Beauty School
N Clark St
W Farragut Ave
Ashland Park
Trumbull Elementary School
Foster Ave
Neofuturists
airportthru
AT&T
AT&T
linksys
Andonis
QuickFish-guest
W Carmen Ave
print server 206C1E
hpsetup
linksys
5664
NETGEAR
winstonscafe
linksys
Apple Network c08cf2
TallDove-guest
AT&T
truevalue
W Winnemac A
Bethany United Methodist Church
Bethany Hospital

Volunteer Cat

Cat Coat?

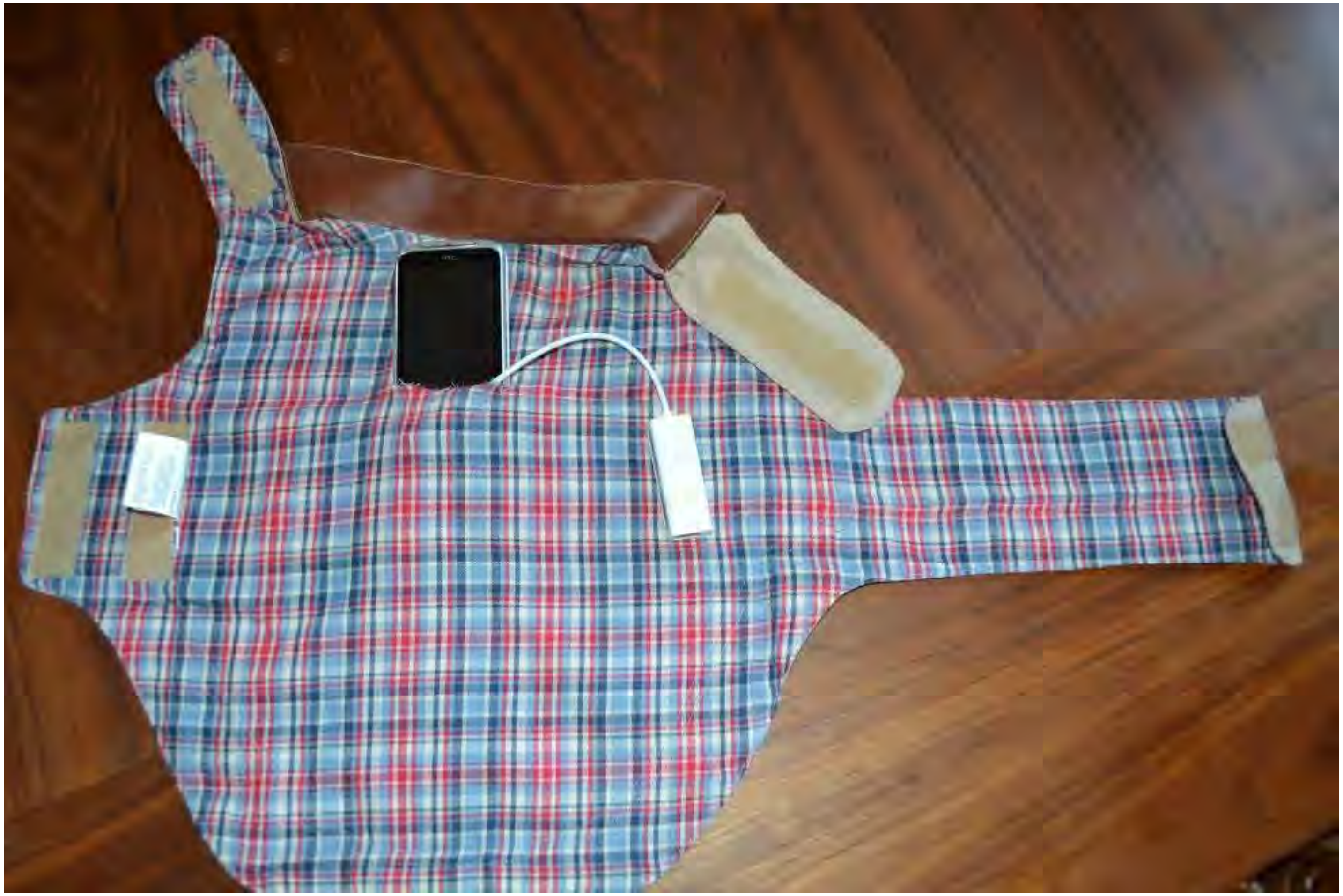
“Cat” Coat



Plan:

- Put Tech in Coat
- Put Coat on Cat
- Send cat on walkabout
- Recover data when cat returns
- Profit!

Step 1



Step 2

Step 2 cont

Step 3

Step… 4?

…yeah…

Trying this again….

Ummm….

FAIL!

Last Known GPS…?

Lessons Learned

- Cats are damn hard to work with
- Always test before you send out ‘spensive stuff
- Amazon Prime account
- Worried about cat, so no more coat
- Smaller form factor with same capability

Talked to my Friend Bill…

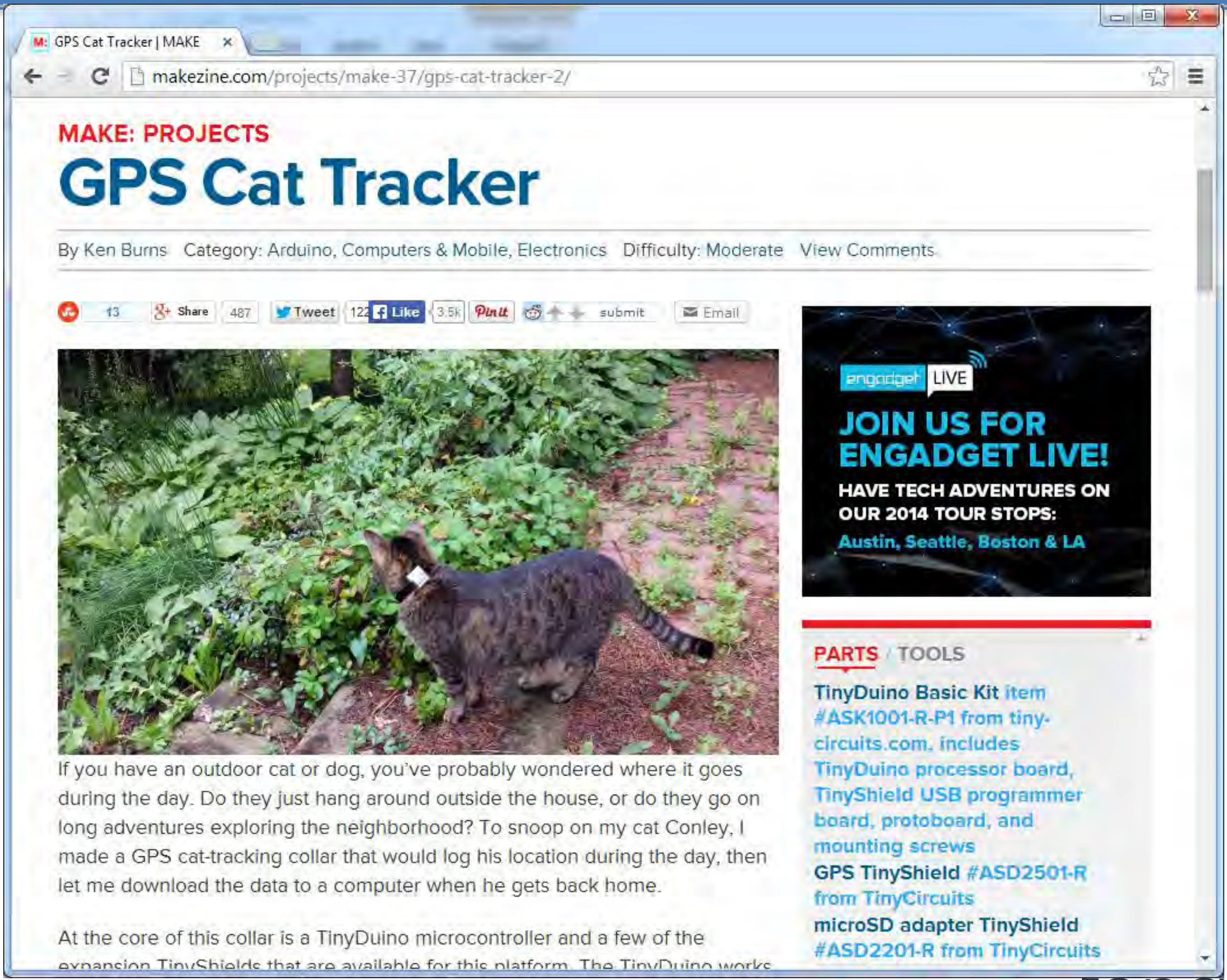
- Hobbiest & Technologist
- What about Arduino
  - Small form factor
  - Low power consumption
  - Does what you need it to do and no more
  - Many chips, variety of solutions

Well I Never…

- Done Anything with Arduino
- Worked with firmware/small chip sets
- Not a professional coder…
- Soldered

Don’t Worry

Arduino Kitteh Collar



MAKE: PROJECTS

GPS Cat Tracker

By Ken Burns Category: Arduino, Computers & Mobile, Electronics Difficulty: Moderate View Comments

If you have an outdoor cat or dog, you've probably wondered where it goes during the day. Do they just hang around outside the house, or do they go on long adventures exploring the neighborhood? To snoop on my cat Conley, I made a GPS cat-tracking collar that would log his location during the day, then let me download the data to a computer when he gets back home.

At the core of this collar is a TinyDuino microcontroller and a few of the expansion TinyShields that are available for this platform. The TinyDuino works

PARTS / TOOLS

TinyDuino Basic Kit item #ASK1001-R-P1 from tiny-circuits.com, includes TinyDuino processor board, TinyShield USB programmer board, protoboard, and mounting screws

GPS TinyShield #ASD2501-R from TinyCircuits

microSD adapter TinyShield #ASD2201-R from TinyCircuits

Plan…

1.) Learn about Arduino

-- Get some basic chips

2.) Decide on most accommodating form factor for WarKitteh

3.) Put it all together in a collar FTW

4.) Do some stuff with DoS Dog…

Learning Arduino…

WELCOME
ARDUINO.CC/STARTERKIT
THE ORIGINAL ARDUINO STARTER KIT
FEATURES 15 SIMPLE PROJECTS
THAT SHOW YOU HOW TO USE ARDUINO
TO TURN AN IDEA INTO REALITY
MORE IMPORTANTLY
IT PROVIDES THE BASIC KNOWLEDGE AND TOOLS
THAT CAN BRING OUT YOUR INNER GENIUS
AND FUEL YOUR CREATIVITY FOREVER
– what's your invention going to be?
ARDUINO PROJECTS BOOK
ARDUINO
UNO

Basic Stuff…

- Arduino Uno

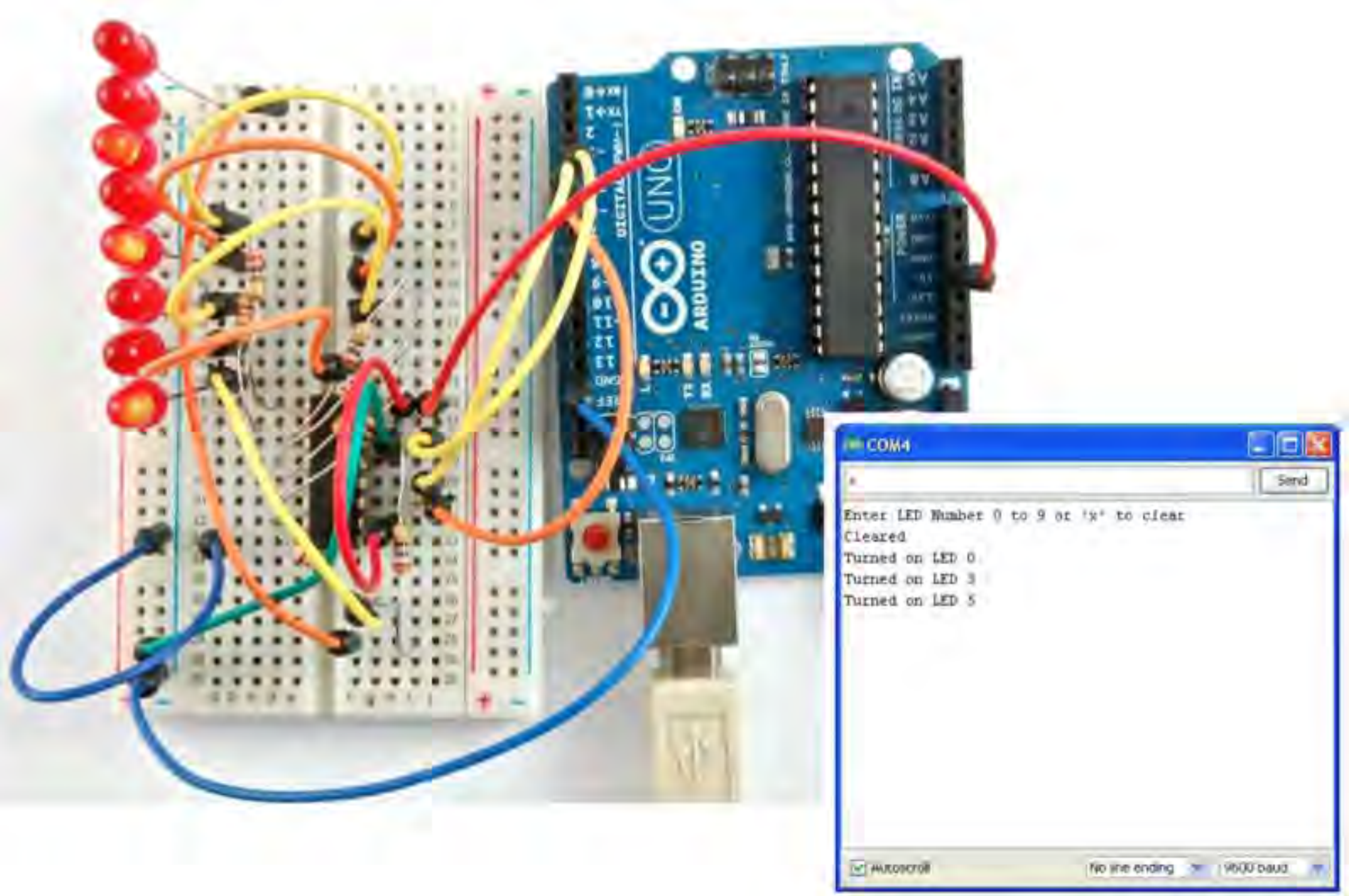
New learnin’

- Volts, amps, current, ohms
- Ohm’s Law
- Milliamps
- Science/Engineering

Cool Stuff

- SPI
  - – Very cool for inter “thing” communication
- I2C
  - – Very cool for inter-chip communication
- Serial Communications
  - – Rx goes to Tx, Tx goes to Rx

Flashy Things…



```
Enter LED Number 0 to 9 or 'x' to clear
Cleared
Turned on LED 0
Turned on LED 3
Turned on LED 5
```

Cooler Stuff!

- I need libraries for WiFi
  - – They got it!
- I need libraries for GPS
  - – They got it!
- I need libraries for SD card stuff
  - – They got it!!

Shout Out…

- Jeremy Blum Videos
  - Jeremyblum.com

I r a Expert!

Small Form Factor…

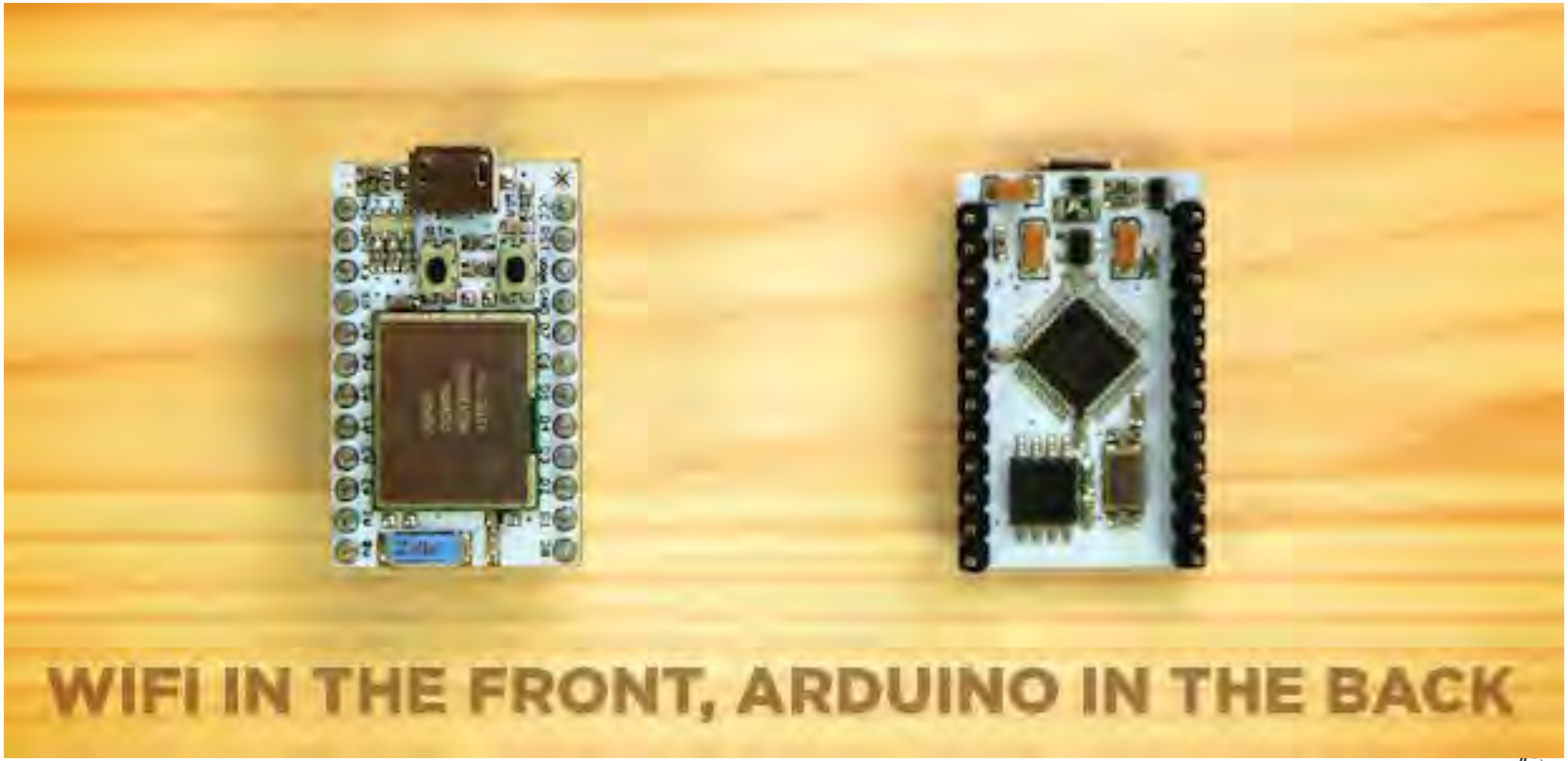
- Arduino Mini…

Small Form Factor

- Adafruit Wifi…

Spark Core

- Spark.io

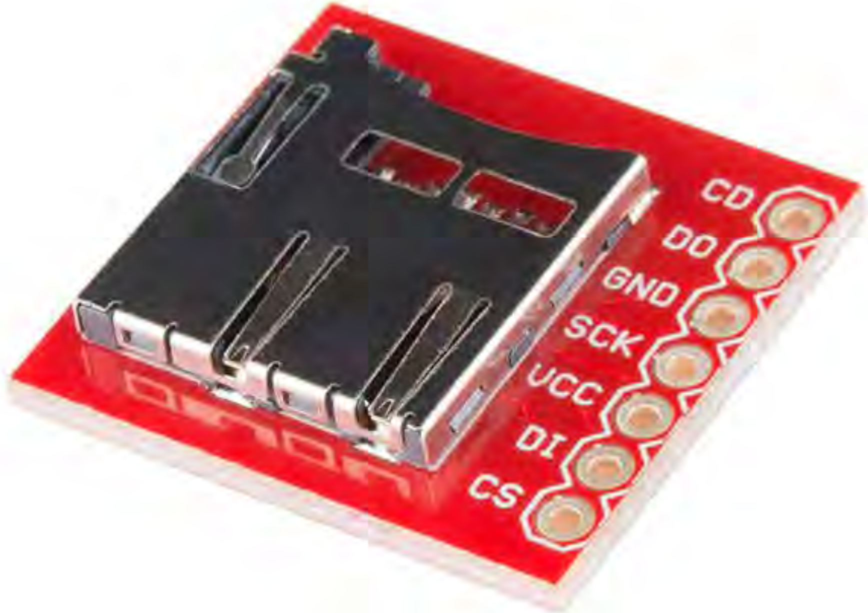


GPS chip

- GP-635T

Micro SD Card

- SparkFun MicroSD Breakout Board



So…

- I ordered all of that stuff…
- But I need to get some demo stuff going before I get the real stuff in…

So I got…

- Arduino WiFi Shield

And Finally…

- Itead Studio GPS Shield

Good News… Bad News…

- Good News!
  - – Open Source
  - – Inexpensive

- Bad News!
  - – Poorly Documented
  - – Takes forever to get to you
  - – Questionable performance…

WiFi Shield

- Set up was easy
- Drivers worked
- Messing around with parameters and variables and
- PROFIT!!!

EASY!!!

GPS Shield

- Serial connection…
  - Set rate at both sides
  - Standard rate is 9600

- Not working
- Not working
- Not working

A bit about GPS

- NMEA string
  - National Maratime Electronics Association

```
$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47
```

- Boot process
  - Start up
    - Where am I…?
  - Listen to SPACE
  - Get a lock (at least 3 satellites)
    - 2-15 minutes!!! (depending on conditions)

So….

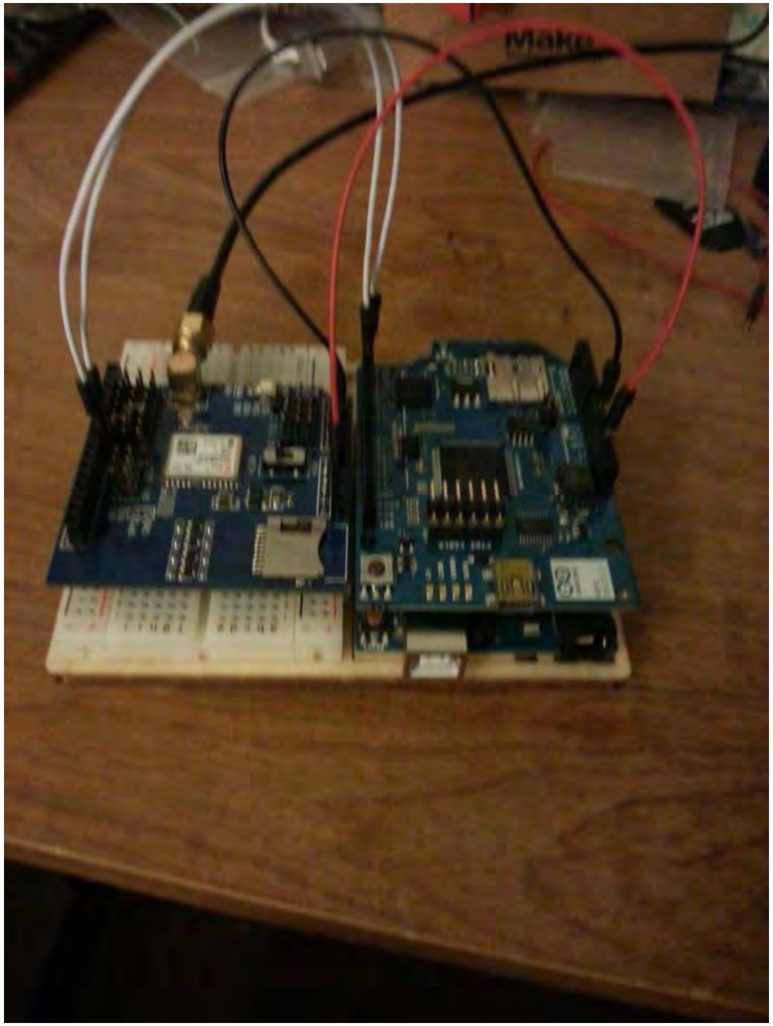
- After an hour, still no lock

- Internet searches and searches
  - Documentation I received said baud 9600
  - Typical baud rates 2400, 4800, 9600, 14400

- End of endless searches
  - 34800

It WORKS!!!

Put all the components together



So now…

- Got a GPS tracker
  - Writes to SD card
- Got a WiFi collection function
  - Writes to SD Card
- Combine
- Profit!

So weird error…

- Something about 80% of memory utilized…

- Ignore that – It'll be fine

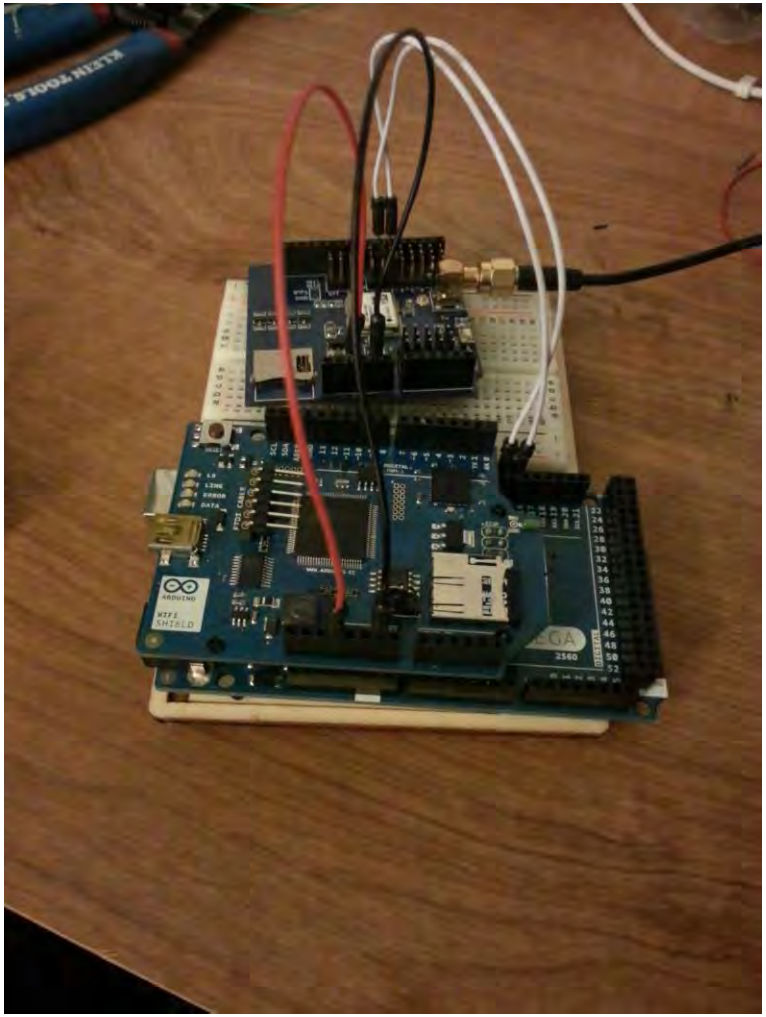
- Boot up and… strange characters showing up in output…

So…

- When the chip tells you it’s low on memory… BELIEVE IT!
- Headers and variables were too much…
- Arduino Uno – 32K
- Arduino Mega2560 – 256K

Purchased the Mega…

Put THAT all together



It WORKS!!!

Arduino Mega2560

- Mo Memory
  - Mo betta
- Mo Ports
  - Mo betta
- Mo Size
  - Not Mo betta

Tiny Arduino2560?

- Arduino MegaMini from JK Devices

- DON’T DO IT!!!!! more later…

So it works, but…

- MegaMini says it's going to be 4 weeks to ship at least…
- Other solutions are too big (size) or too small (memory)
- Spark.io Spark Core
  - Shipping problem delayed by 2 months…

Tech on the Spark

- ARM 32-bit M3 CPU
- 128KB Memory (wooHOO!!!)
- SPI and I2C compliant
- TI CC3000 WiFi chip
- “Arduino Compatible”

- So I borrowed one… From Bill

Real Tech on Spark

- ARM 32-bit M3 CPU √
- 128KB Memory (wooHOO!!!) √
- SPI and I2C compliant √
- TI CC3000 WiFi chip √
- "Arduino Compatible" X
  - – Worked with external components
  - – Coding wouldn't work
  - – Completely different development environment

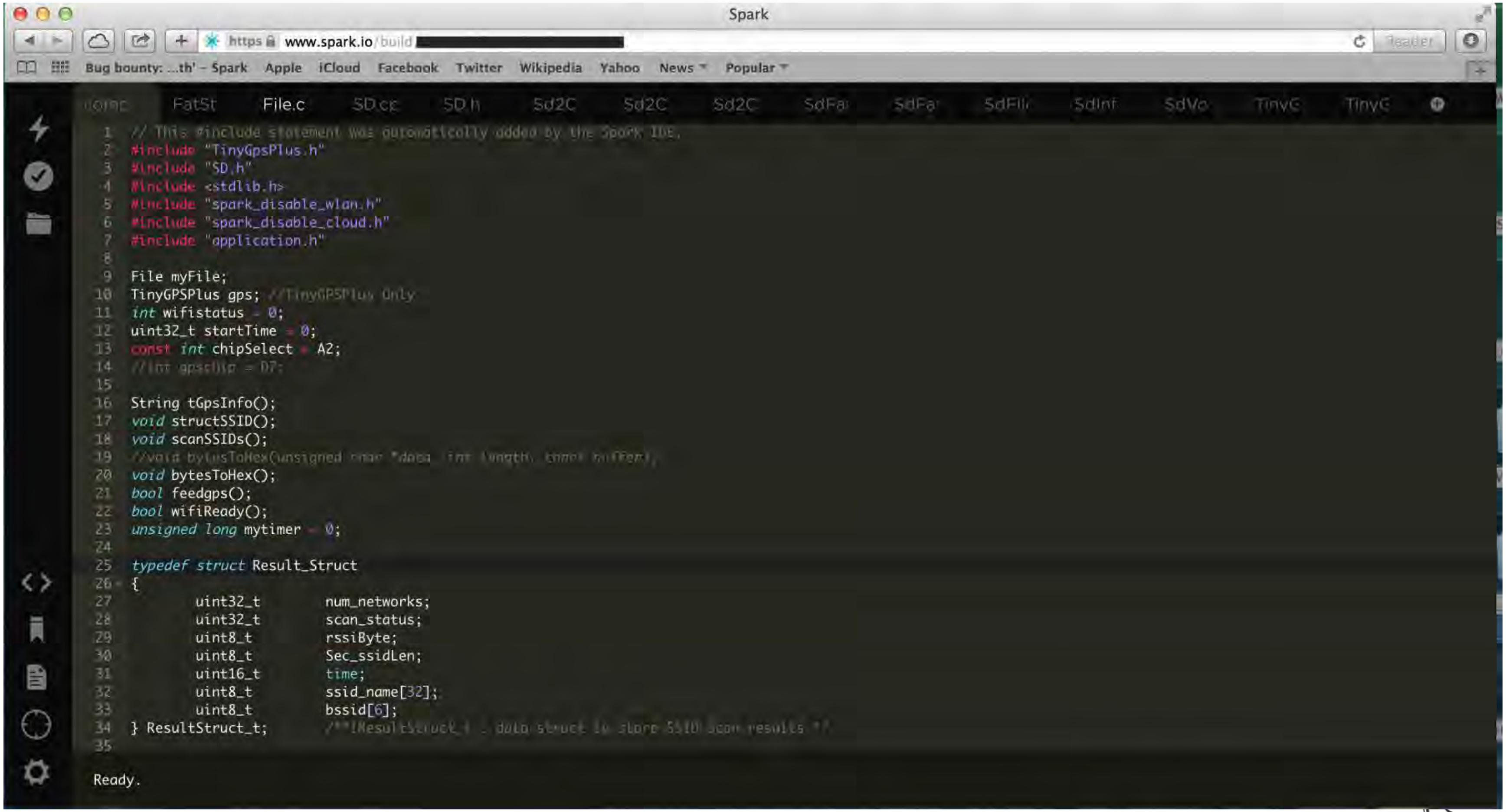
OMG

Start-up Product

- Starting everything from scratch
  - WiFi Drivers were included, but no overt way to interact with them
  - No SD Libraries
  - No GPS Libraries

- VERY COOL

Online IDE



```
// This #include statement was automatically added by the Spark IDE.
#include "TinyGpsPlus.h"
#include "SD.h"
#include <stdlib.h>
#include "spark_disable_wlan.h"
#include "spark_disable_cloud.h"
#include "application.h"

File myFile;
TinyGPSPlus gps; //TinyGPSPlus Only
int wifistatus = 0;
uint32_t startTime = 0;
const int chipSelect = A2;
//int gpsclip = D7;

String tGpsInfo();
void structSSID();
void scanSSIDs();
//void bytesToHex(unsigned char *data, int length, char* buffer);
void bytesToHex();
bool feedgps();
bool wifiReady();
unsigned long mytimer = 0;

typedef struct Result_Struct
{
        uint32_t        num_networks;
        uint32_t        scan_status;
        uint8_t         rssiByte;
        uint8_t         Sec_ssidLen;
        uint16_t        time;
        uint8_t         ssid_name[32];
        uint8_t         bssid[6];
} ResultStruct_t;       /**!ResultStruct_t : data struct to store SSID scan results */

```

```
Ready.
```

Very Robust Community

- Dedicated core group of developers
  - Shout out to peekay123
- Very cool product, with changes constantly happening
- Let’s do what we can and see what happens

GPS Libraries

- Someone posted GPS libraries to the forums…

- They worked!
  - Good for me!

SD Card Libraries

- Someone Posted SD Card Libraries to the forums
- They Worked!

WiFi Libraries

- …no readily available stuff for what I wanted to do
- Spark is an "Internet of Things" device
- Internet connectivity is part of the set-up process

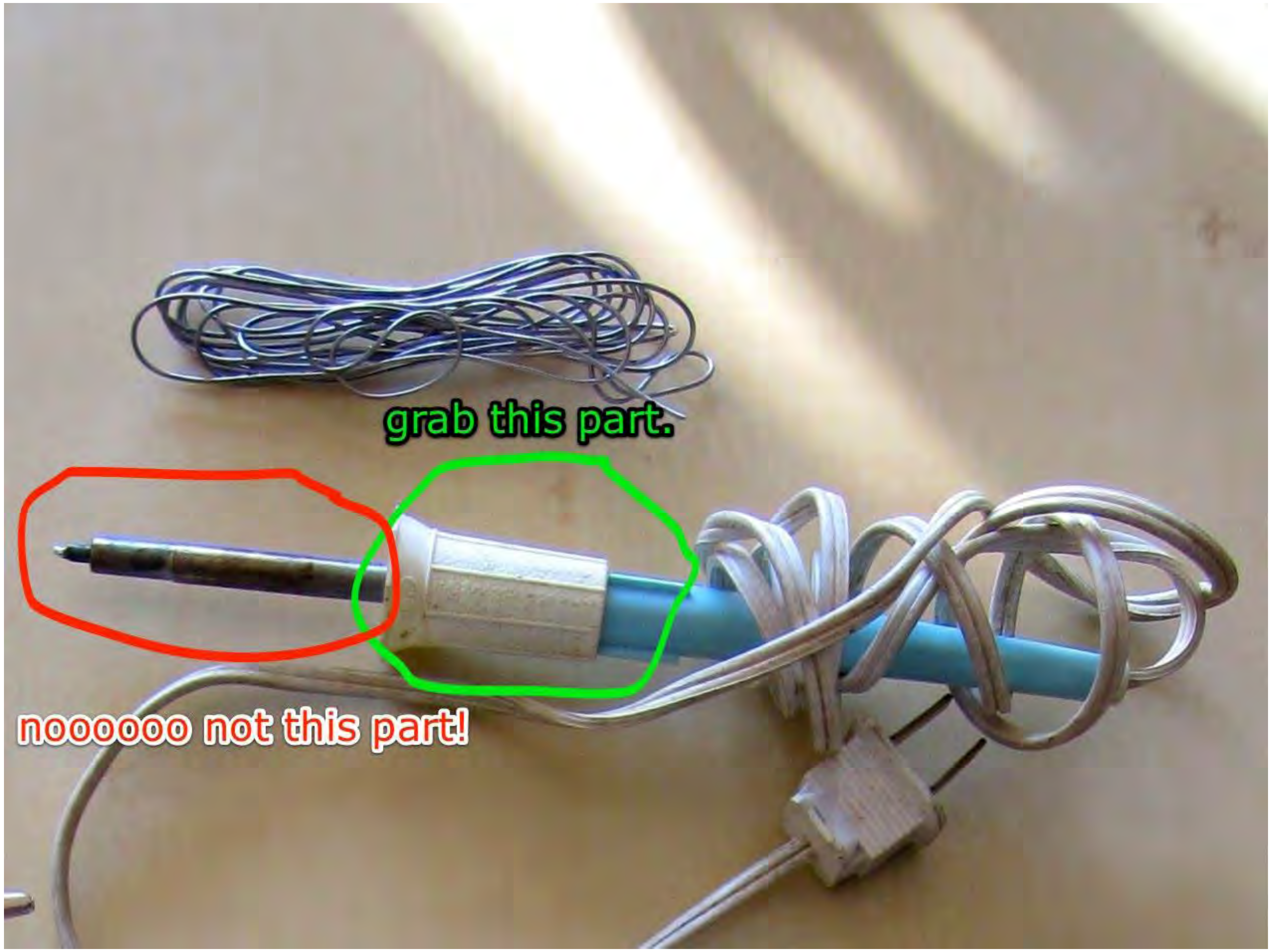
Adafruit FTW!

- Adafruit CC3000 Breakout borad
- Supporting code on the Adafruit website for Download
- Messed with it earlier… let's see if it works!

It WORKS!!!

Now, onto soldering

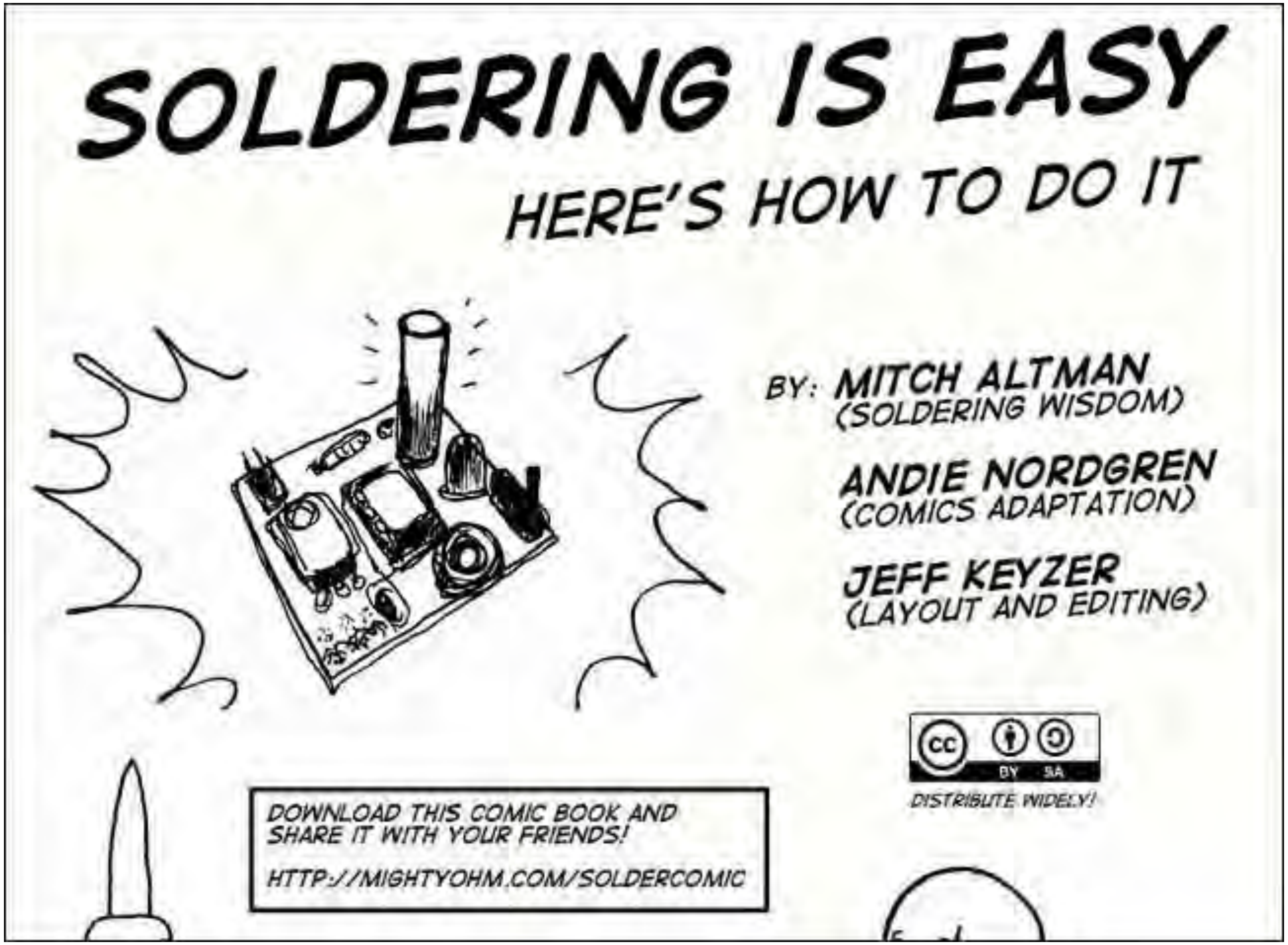
Rule 1



Rule 2

Rule 3

Rule 4



SOLDERING IS EASY

HERE'S HOW TO DO IT

BY: MITCH ALTMAN (SOLDERING WISDOM)

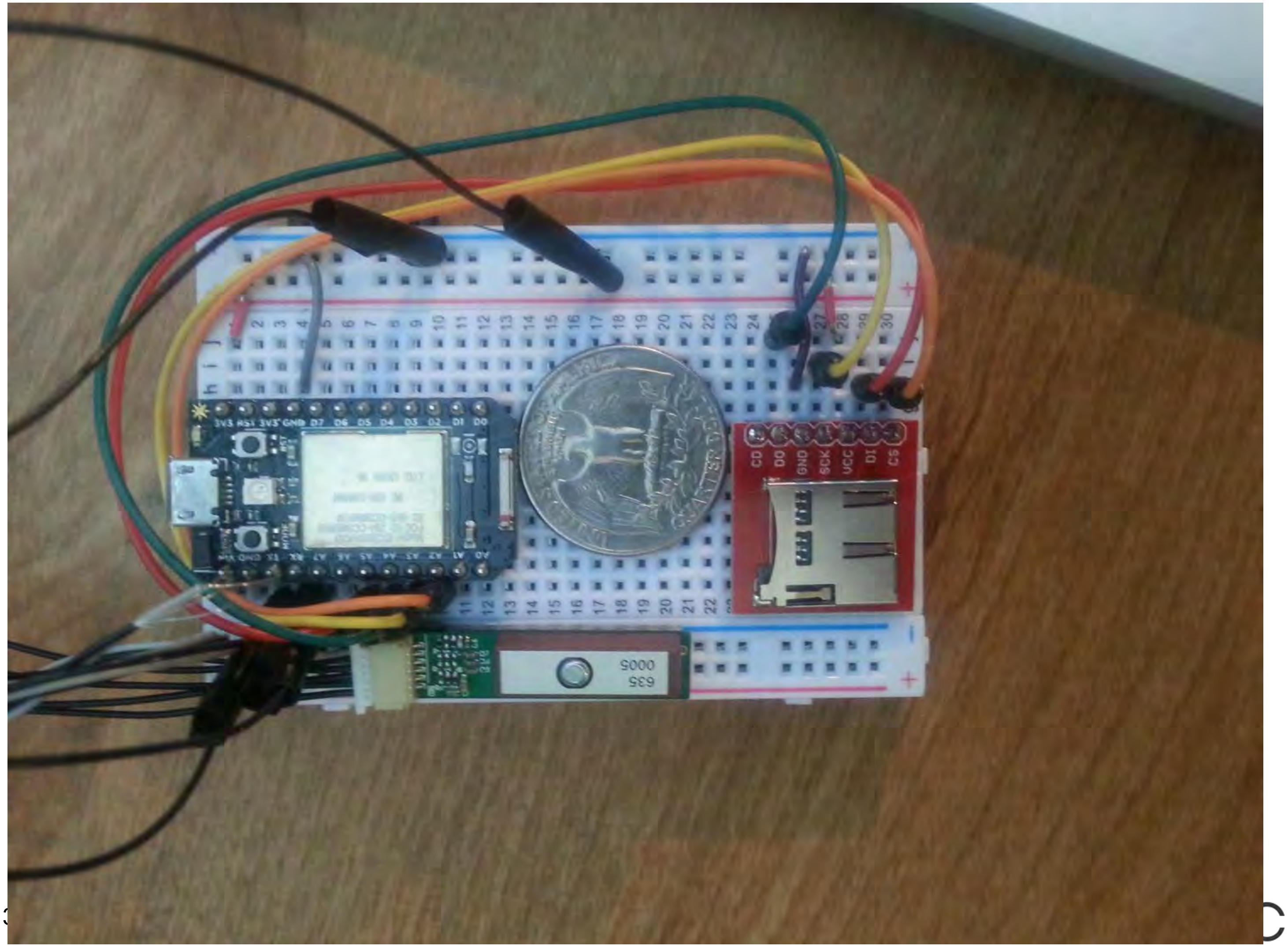
ANDIE NORDGREN (COMICS ADAPTATION)

JEFF KEYZER (LAYOUT AND EDITING)

DOWNLOAD THIS COMIC BOOK AND SHARE IT WITH YOUR FRIENDS!

HTTP://MIGHTYOHM.COM/SOLDERCOMIC

First attempts went very well…



Testing…

- At home everything went Great!
- Took it out for a walk around the yard and it was great!
- Took it for a ride in the car and FAIL!!!
- What happened…?

Spark Concept

- Internet of Things device
- Never meant to be disconnected from the Internet
- Encased in a “If status == WIFI_ON” clause
  - Must be connected to a known WAP to return true

What to do

- Noticed that I could scan SSID's before I got an IP address
- Removed code from clause
- PROFIT!

More testing…

- Took it for a drive
- Got Data back!!!!
- Looked at the GPS cords… they were off by about half a mile…
- GPS Libraries were wrong

TinyGPSPlus

- LOVE to use TinyGPSPlus
  - Everything I need
  - Didn't work in Spark
- How to Port Libraries? Talk to Bill
  - Rocket Science
- Replace Ardruino.h with application.h and test
  - Fix what blows up

It WORKS!!!

Next Problem

- Power Consumption
  - How to do it best…?

- Eflite 3.7v 500mAh batteries

tenacity

Testing

- Originally tried cycling WiFi on and off
  - That really didn't work well
- Put main chip in Deep sleep to save juice
  - Keep GPS chip on
- Hits every 30 sec lasted 4 hours
- Hits every 10 minutes lasted 8 hours

Time to Make Collar

Form Factor

- DeSoldering is TWICE as much fun as soldering
  - NOT
- Internet again NOT helpful
- YouTube makes it look TOO easy

NOVALabs Shout Out

- Reston, VA
- Ted
  - Mad Scientist/Evil Genius
  - Helped me learn EAGLE
- Brian
  - Soldering Tutor
  - Right Iron, Right Solder

Now… where my Maker's at?

- Need to make a cat collar…
- How do I make a cat collar???
  - Lots of Ways
- Friend Joe suggested ribbons
  - Sew them together
- Who knows how to Sew?

Get a Grandma

Volunteer Cat

So let’s PRACTICE first..

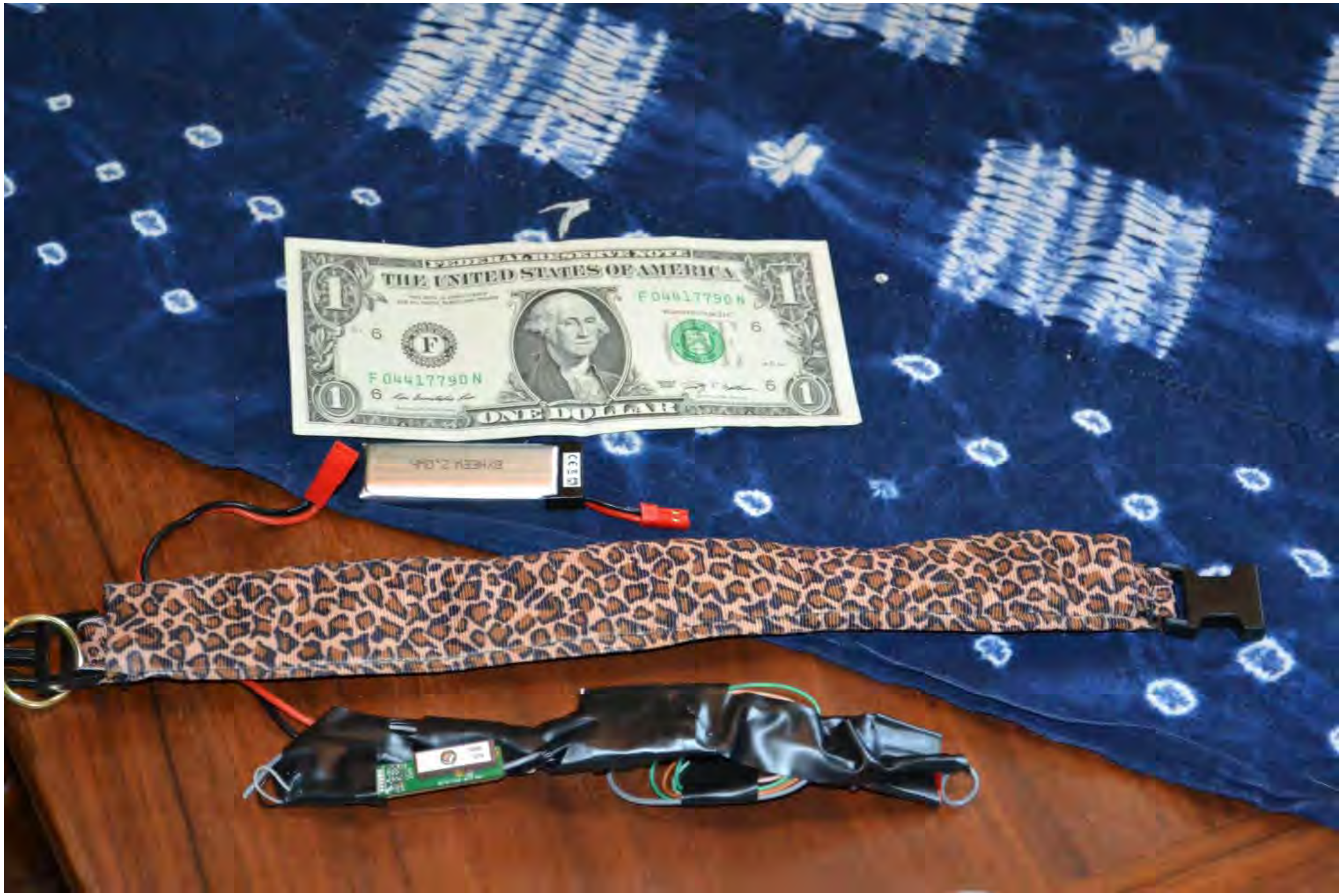
- Let cat out with no-tech collar and see if he tolerated it…
- HE DID!

Old Way…

New Collar

tenacity

Collar Assembly



So… New plan

- Tech goes in the Collar
- Collar goes on the cat…
- Cat goes on a walk about…
- Profit

Initial results

- …Nothing….!?!?!?!?
- W
- T
- *********
- !?!!??!?!?
- Investigation

What had happened was…

- Put collar on cat
- Cat walked under a bush
- Hung out and licked himself for 20 minutes

New Deployment procedures

- Let collar sit outside for 5-10 min
- Bring cat to collar, put it on cat
- Let cat go for a walk about…
- …profit…!?!?!?????

Results

- SUCCESS!!!!!

Denial of Service Dog

On the Internet,
Nobody Knows You're a Dog

"On the Internet, nobody knows you're a dog."

DoS Dog

- So…. More trolling than anything
- WiFi Pineapple
  - Pineapple Juice
- TV B Gone

Things I Need…

- WiFi Pineapple
  - – Picked one up at ShmooCon
- TV B Gone
  - – Adafruit kit
- "Denial of Service Dog" patches
- Doggie Back Pack

Volunteer Dog

WiFi Pineapple

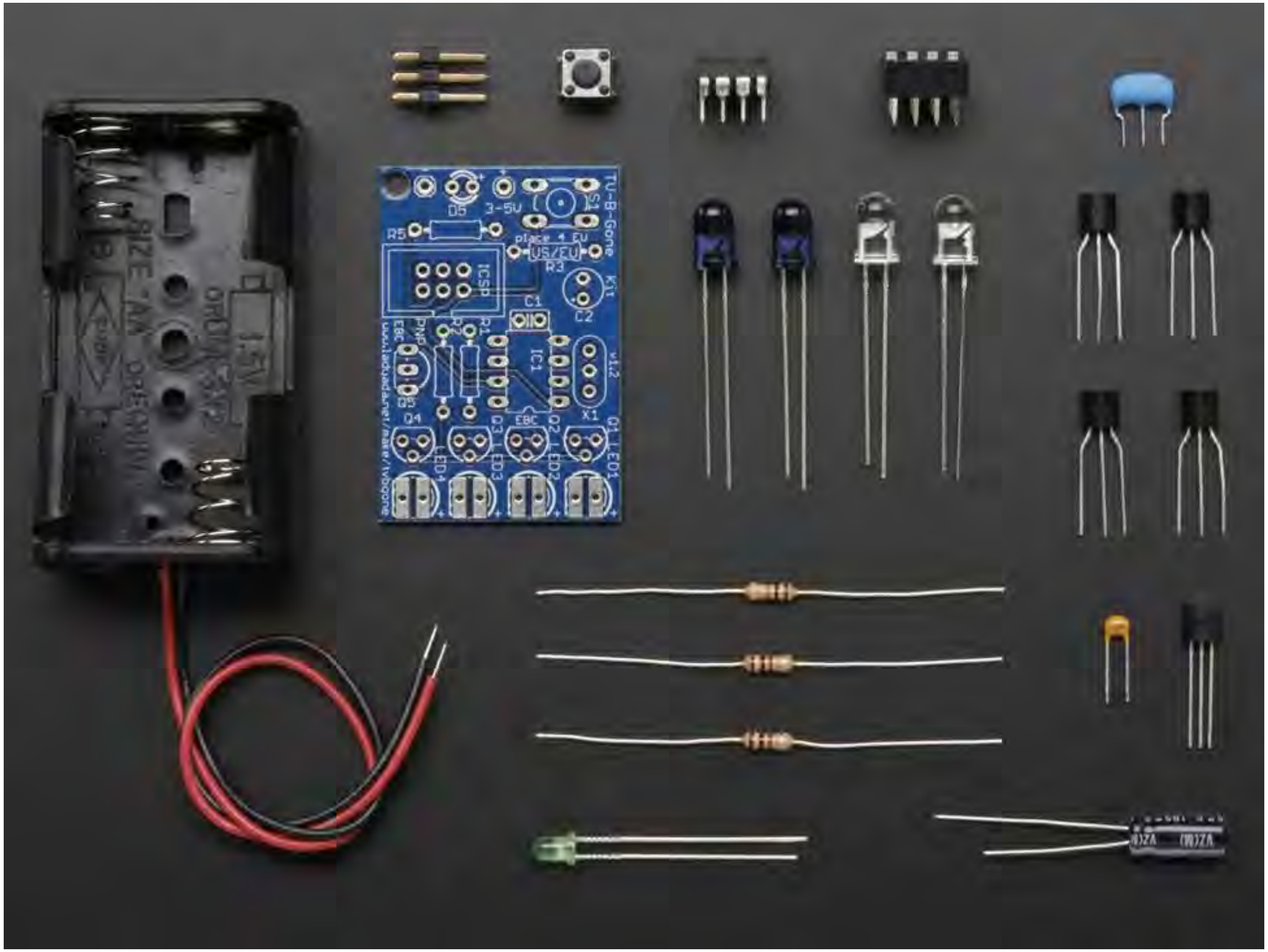
What I’m gonna do is…

- Karma
  - Answers Probes
- DNS Spoof
  - Redirects all things to Pineapple
- randomroll…
  - ‘cause RickRoll makes trolling better

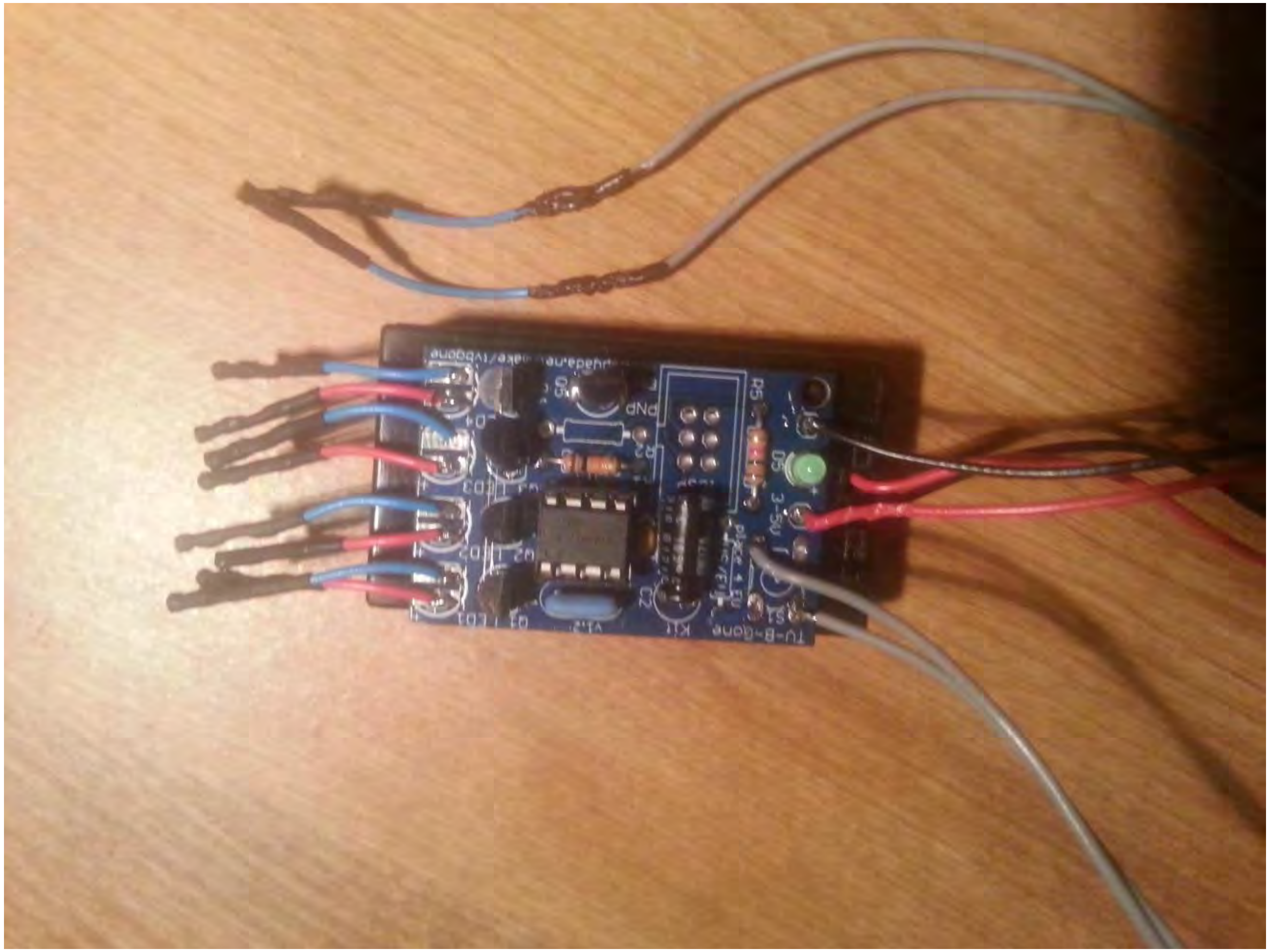
TV B Gone

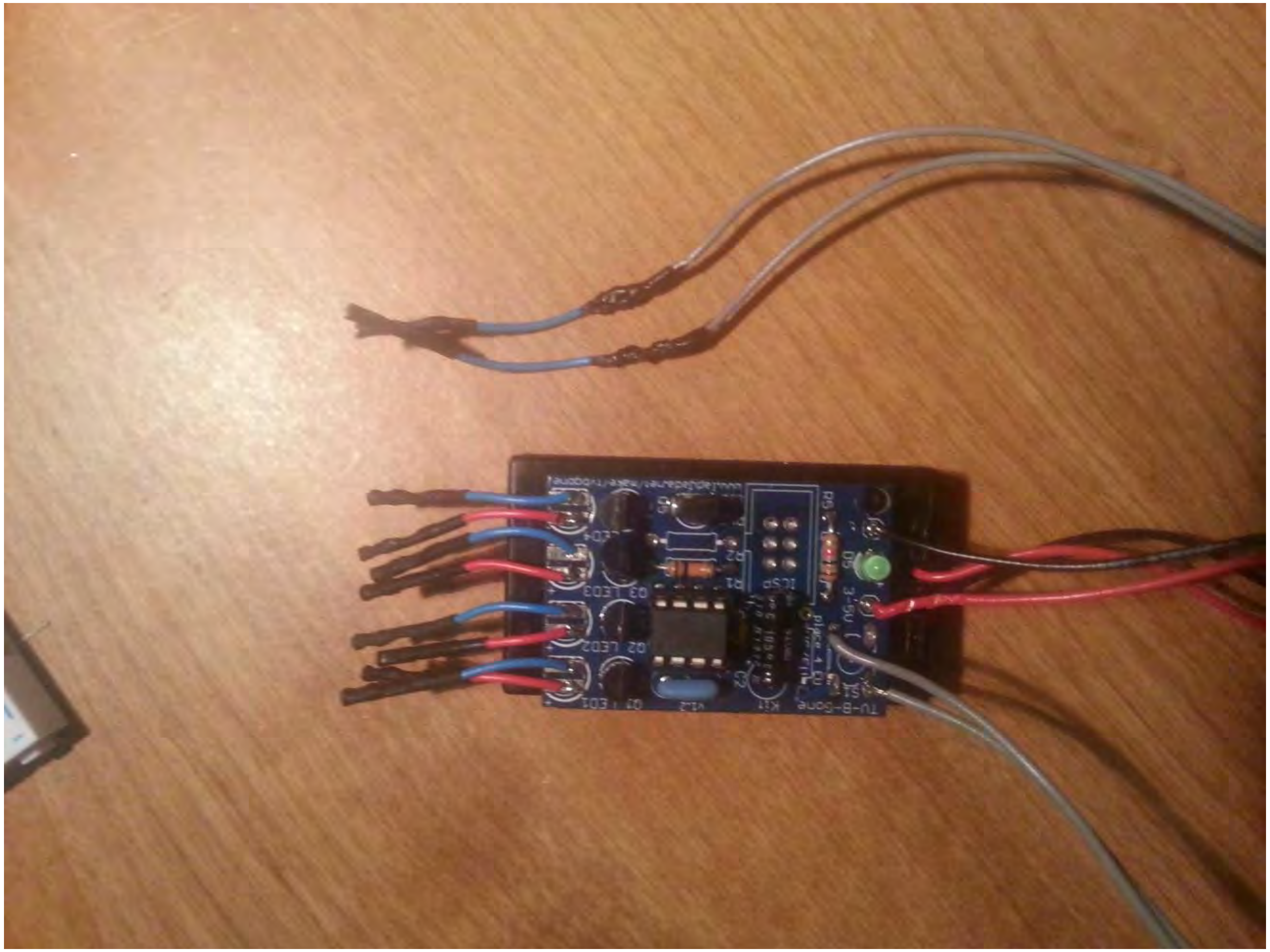
tenacity

…in pieces.



Some minor modifications…



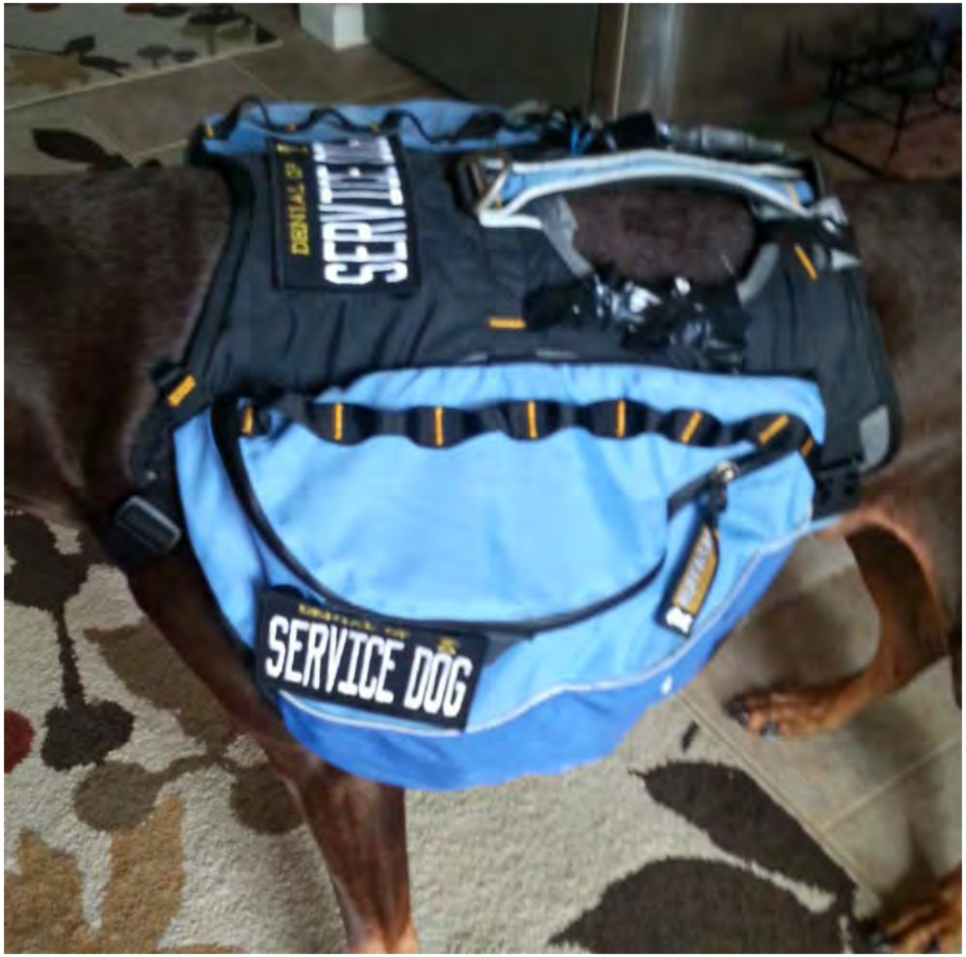


Patches

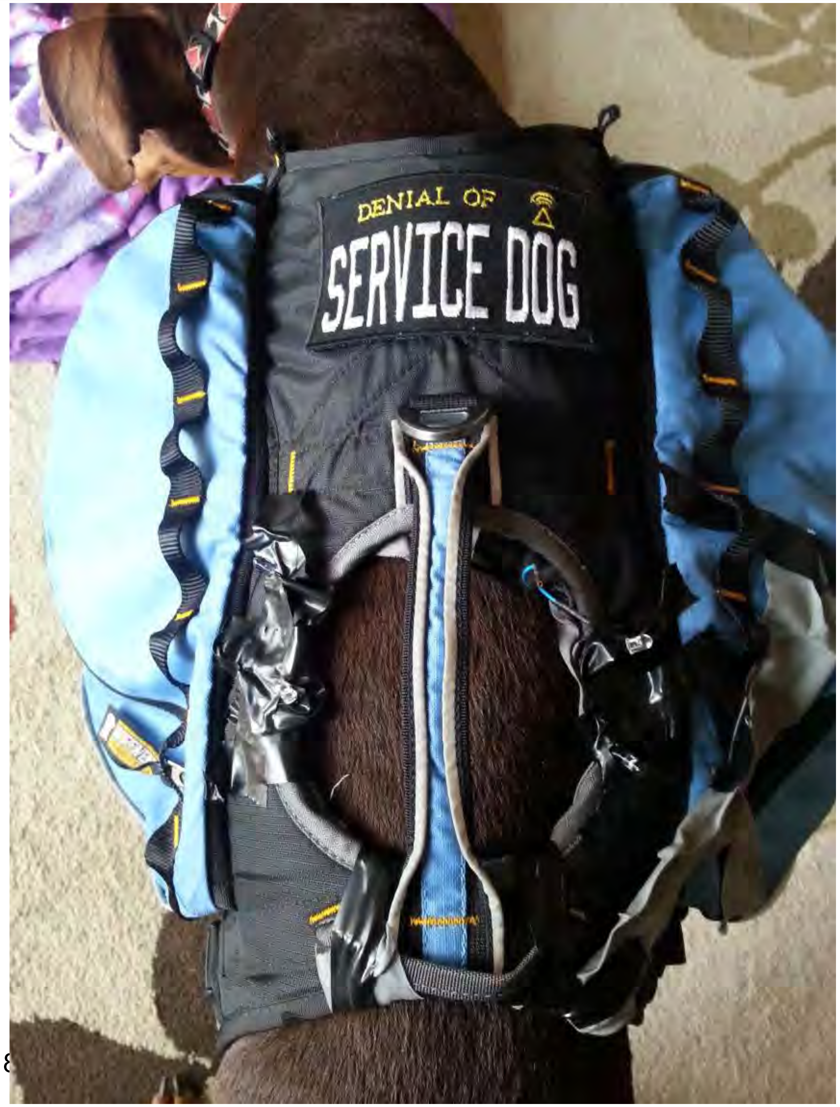
- WHOLLY Crap! What a pain in the butt!
- Nobody does it anymore
- ‘Cept Irina & Friends at JoAnn’s Fabrics in Sterling, VA
  - Thank Jesus

Victory!

Putting it on a Doggie Backpack



Top View



LEDs…

Volunteer Dog Ready to Go!

tenacity

Dog will Shake

- TV B Gone wasn't designed to be shaken in the manner in which V-dog was shaking..
- Minor Soldering repairs…
- Trying things again…

Demo Video

- Proof that it works
- Restaurant…?
- Box Store…?
- Etc…

So What Have We Learned???

- Trolling is fun
- Set your mind to it, Makers, Hackers, and normal people will be glad to help
- Don’t give up, you will eventually beat the tech
- Trolling is fun – even for cats and dogs

Oh BTW

- JK Devices (jkdevices.com)
  - Complete Scam
  - Don’t waste your money
- No emails
- No contact
- No Product

Questions?

That’s all Folks

- Thanks!

EXTRA SLIDES

- Nothing further… move along…

Further Research

- Spark https://www.spark.io/

- Wifi Redback http://www.cutedigi.com/
- Tons of Arduino sites out there

War Kitteh!

STAY TUNED!!!!

Denial of Service Dog

- ……yeah, nothing yet
- Plans:

  Pineapple

  TV-B-Gone

  WiFi War Mushing?

  OsmocomBB – 22nd USENIX

    “Let me Answer that for You”

And THEN…..!?