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

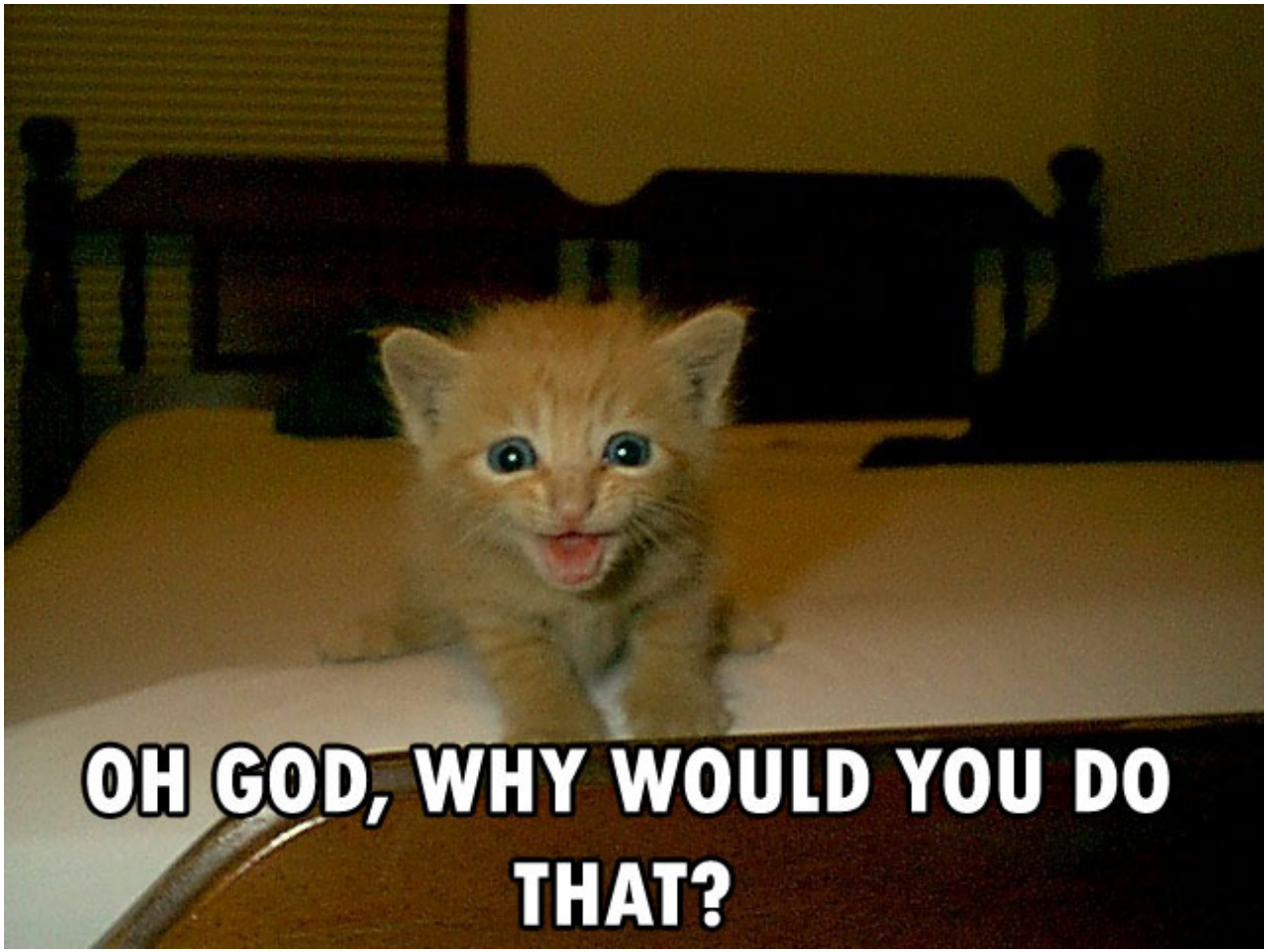
tenacity

What is This About?

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

tenacity

Weaponize your PETS!?!?!



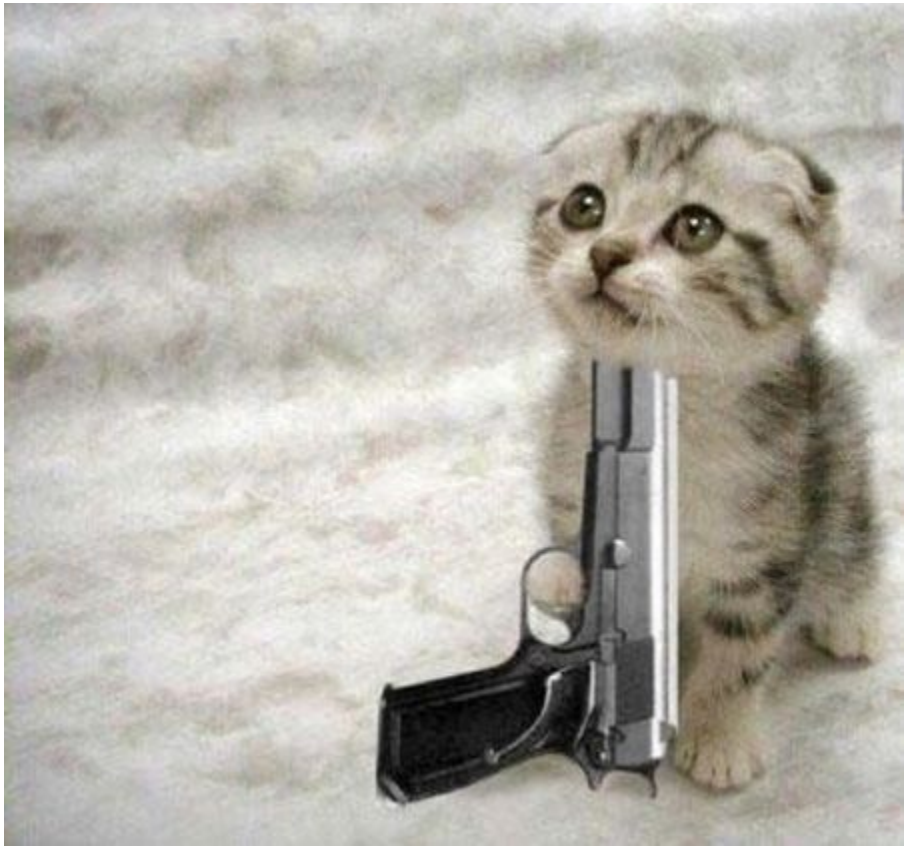
tenacity

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

tenacity

The pic that started it all:



tenacity

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!!!!

tenacity

What about the DoS Dog?

- AT Outerz0ne
- LadyMerlin walked in with a dog wearing a harness that said Denial of Service Dog
- I said “Is there a Pineapple in there?”
  - No, the dog is a pain, but that’s a geat idea!

tenacity

Working Animals

tenacity

Bad Ass Working Animals

tenacity

Badder Ass Working Animals

tenacity

Real Navy Seal

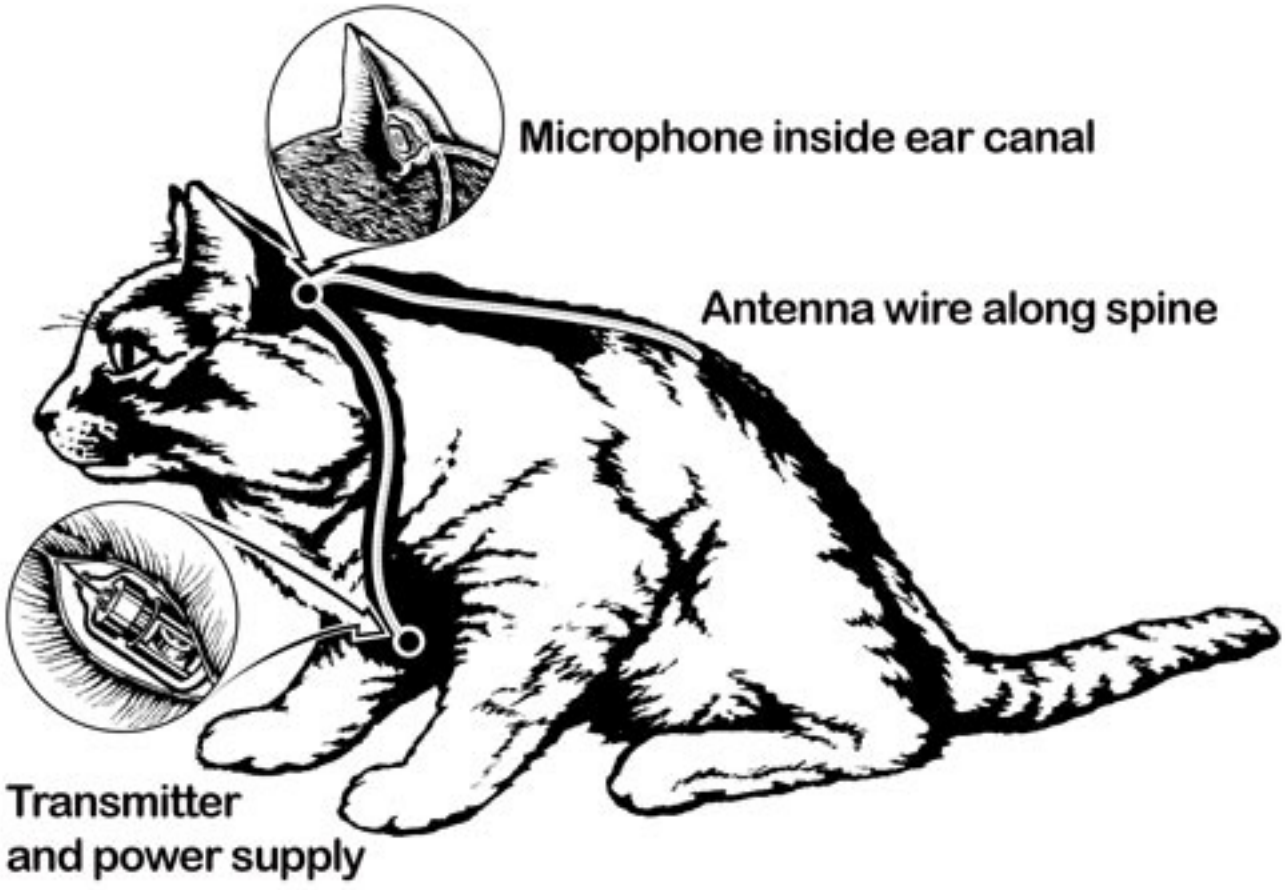
tenacity

Flipper Pic

tenacity

Other Research Efforts

- Accoustic Kitty



tenacity

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

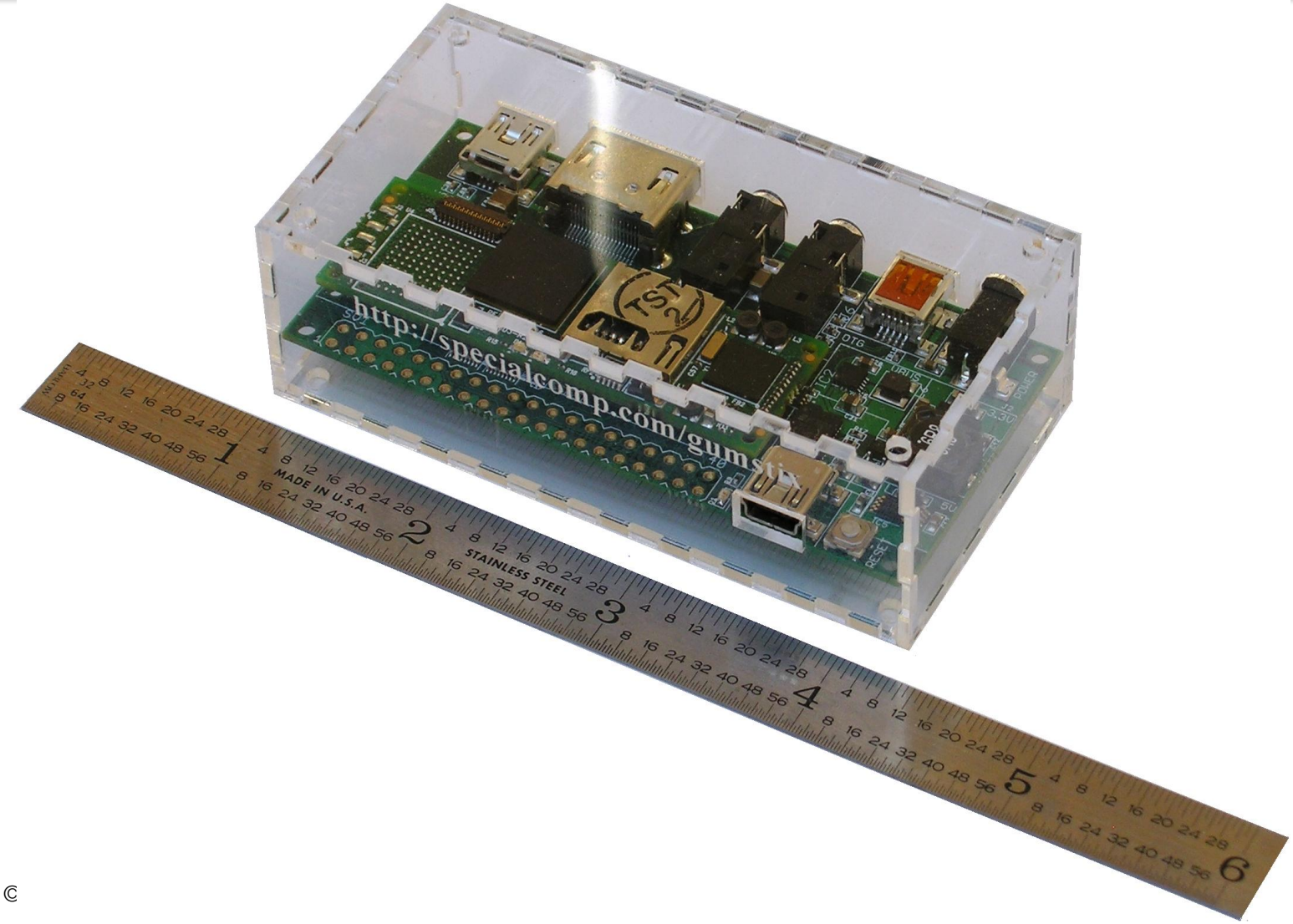
tenacity

Other Products

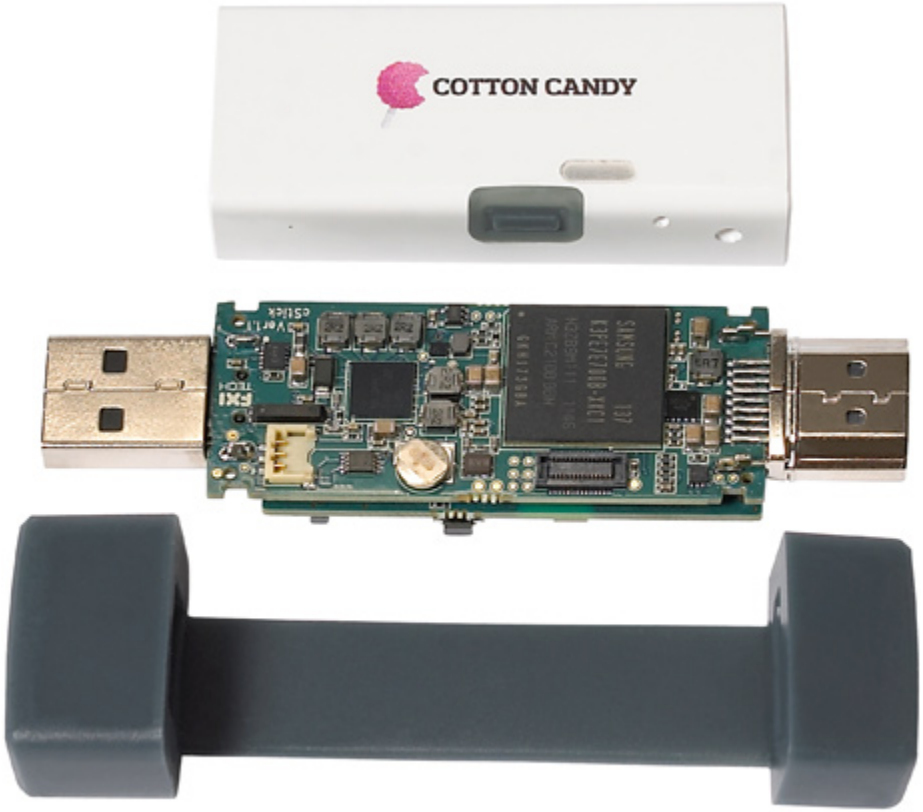
- Mr Lee Cat Cam
  - http://www.mr-lee-catcam.de
- Pet Tracker
  - http://www.pettracker.com
- Garmin
  - https://buy.garmin.com/

tenacity

GumStix



Cotton Candy



tenacity

RockChip 3066

tenacity

Thinking about it…

- Small form factor
- GPS
- Wifi
- Cellular

tenacity

How ‘bout a Cell Phone?

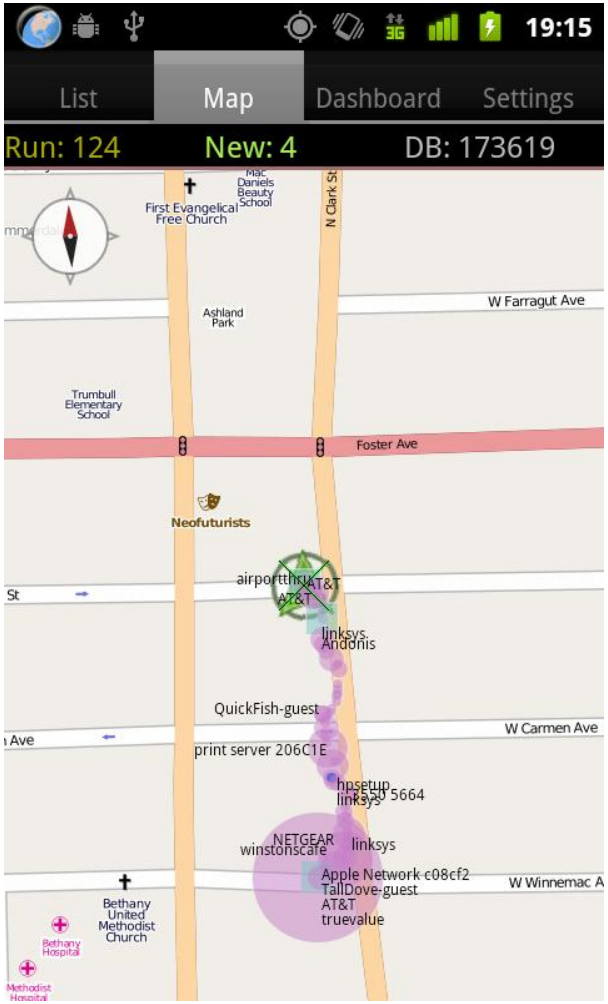
tenacity

Now make an APK!?!?

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

tenacity

WiGLE WiFi



tenacity

Volunteer Cat

tenacity

Cat Coat?

tenacity

“Cat” Coat

tenacity

Plan:

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

tenacity

Step 1

tenacity

Step 2

tenacity

Step 2 cont

tenacity

Step 3

tenacity

Step… 4?

tenacity

…yeah…

tenacity

Trying this again….

tenacity

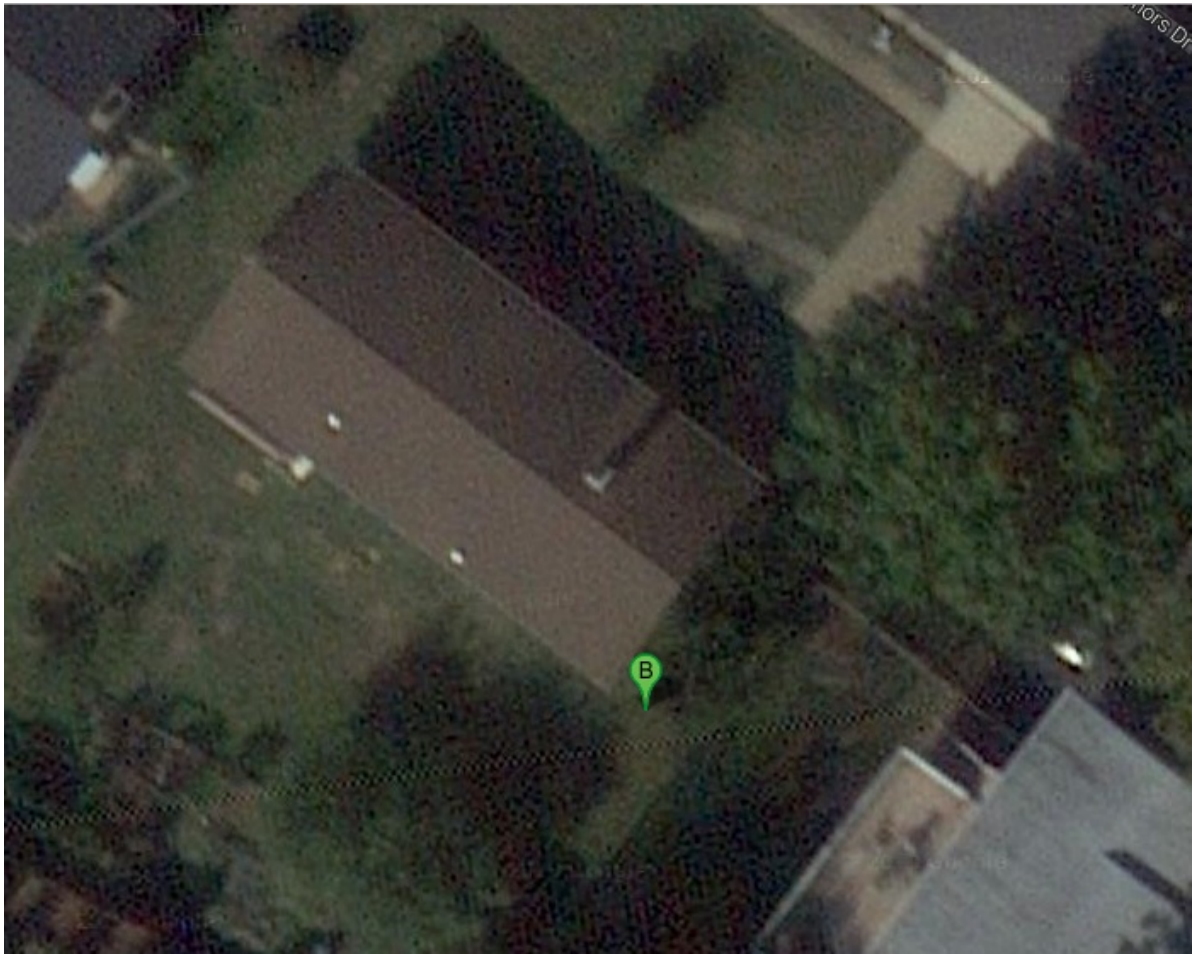
Ummm….

tenacity

FAIL!

tenacity

Last Known GPS…?



tenacity

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

tenacity

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

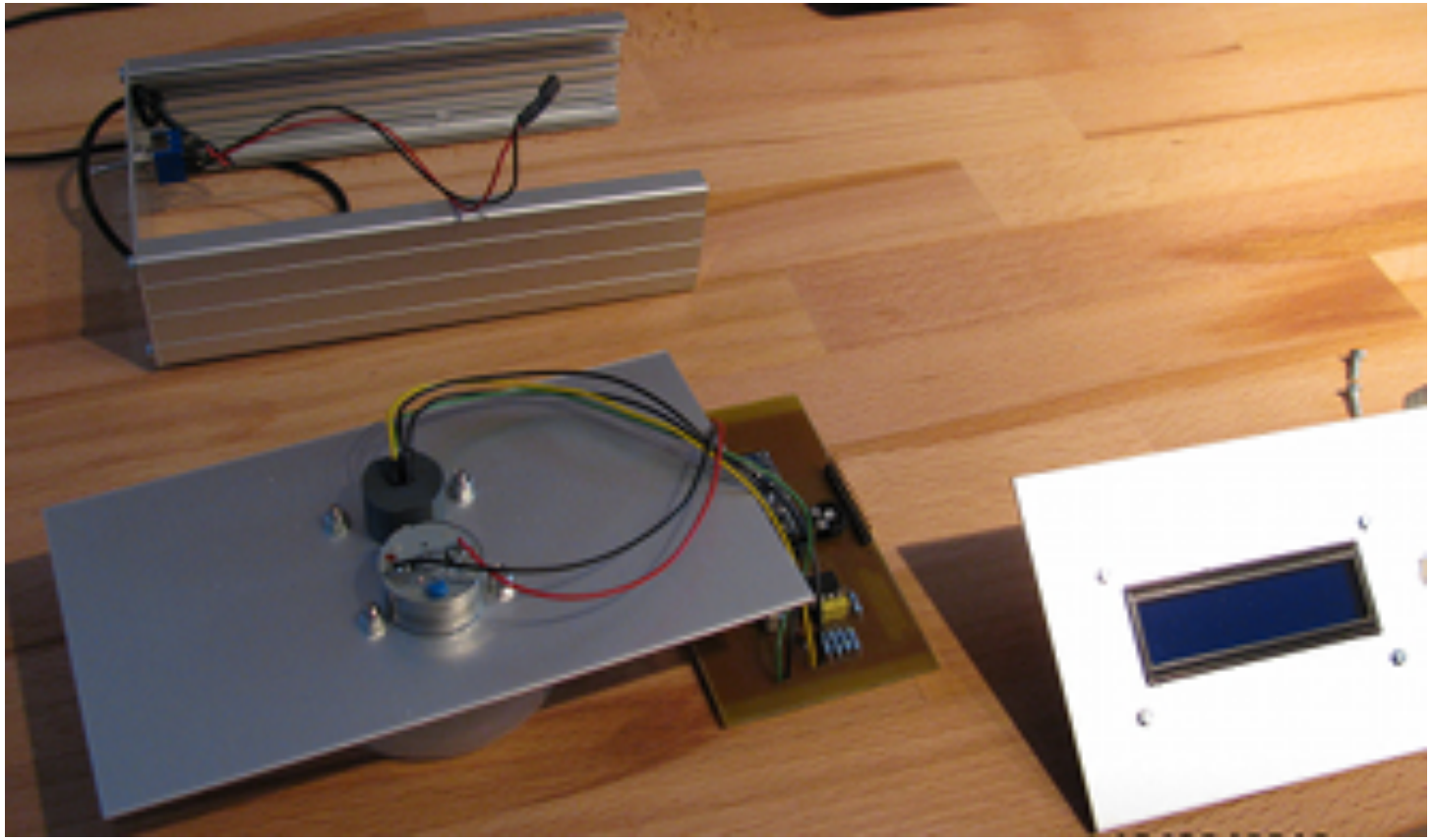
tenacity

What is Arduino?

- Arduino is an open-source electronics platform based on easy-to-use hardware and software. It's intended for anyone making interactive projects.
- Lots of expansion boards of “Shields”
- Make robots, remote control cars, home security products, etc.

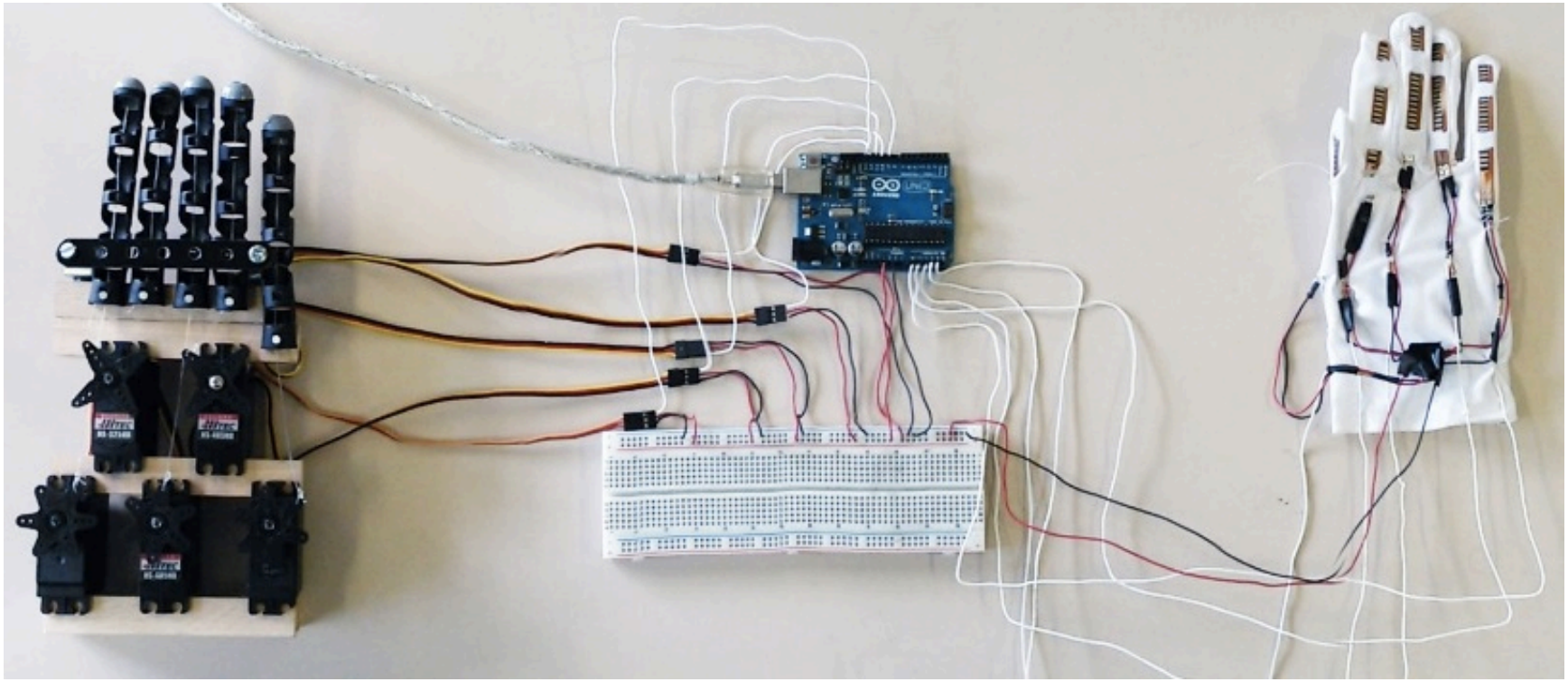
tenacity

Freezer check



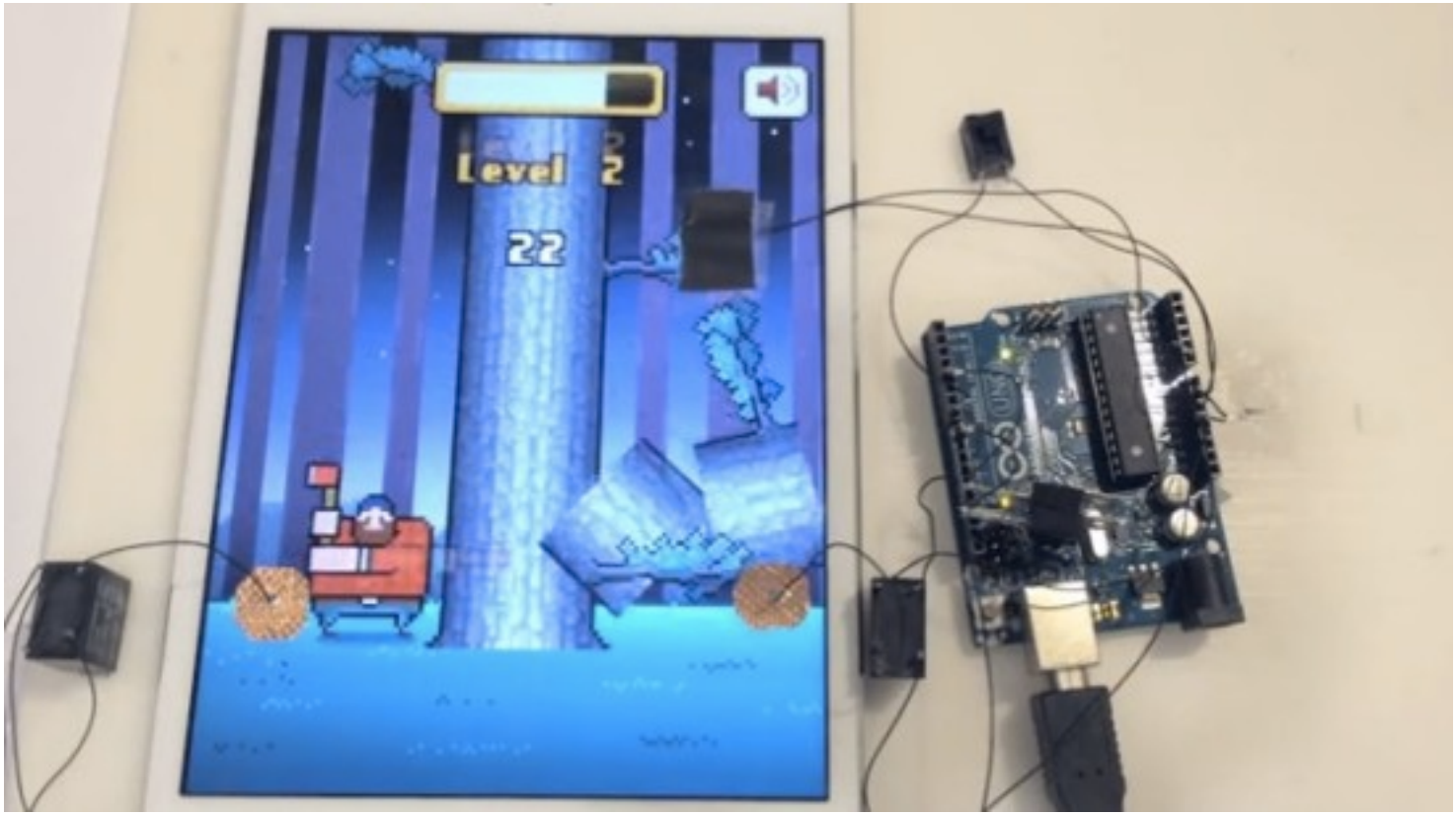
tenacity

Robotic Hand



tenacity

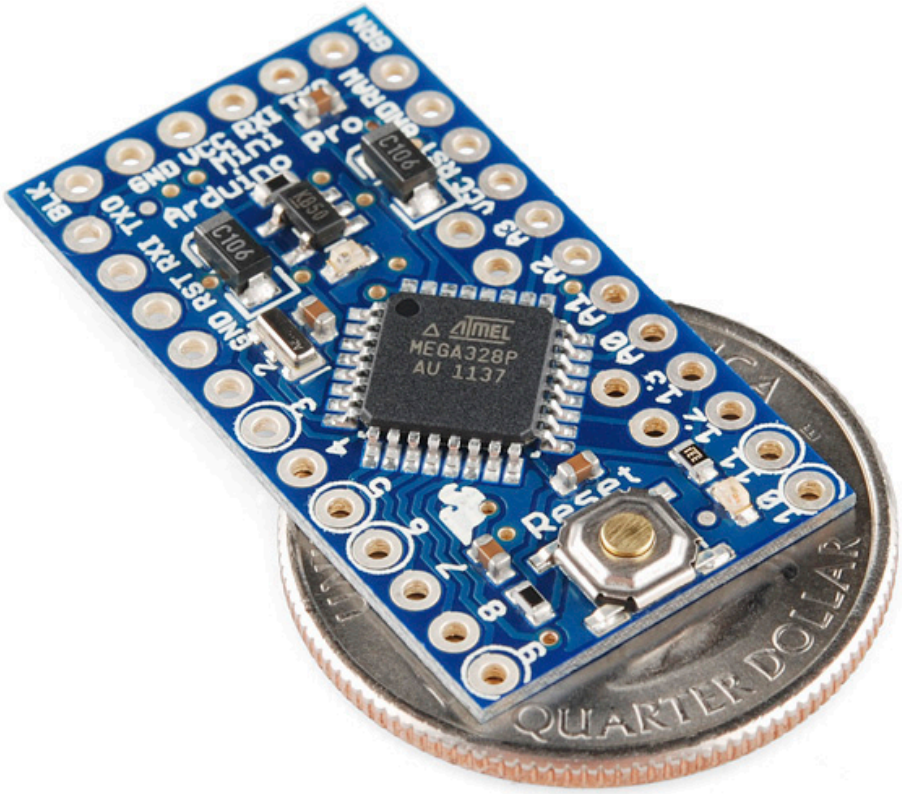
Video Games



tenacity

Small Form Factor…

- Arduino Mini…



tenacity

Good News… Bad News…

- Good News!
  - Open Source
  - Inexpensive
- Bad News!
  - Poorly Documented
  - Takes forever to get to you
  - Questionable performance…

tenacity

Well I Never…

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

tenacity

Don’t Worry

tenacity

Plan…

1.) Learn about Arduino

-- Get some basic stuff

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…

tenacity

Learning Arduino…

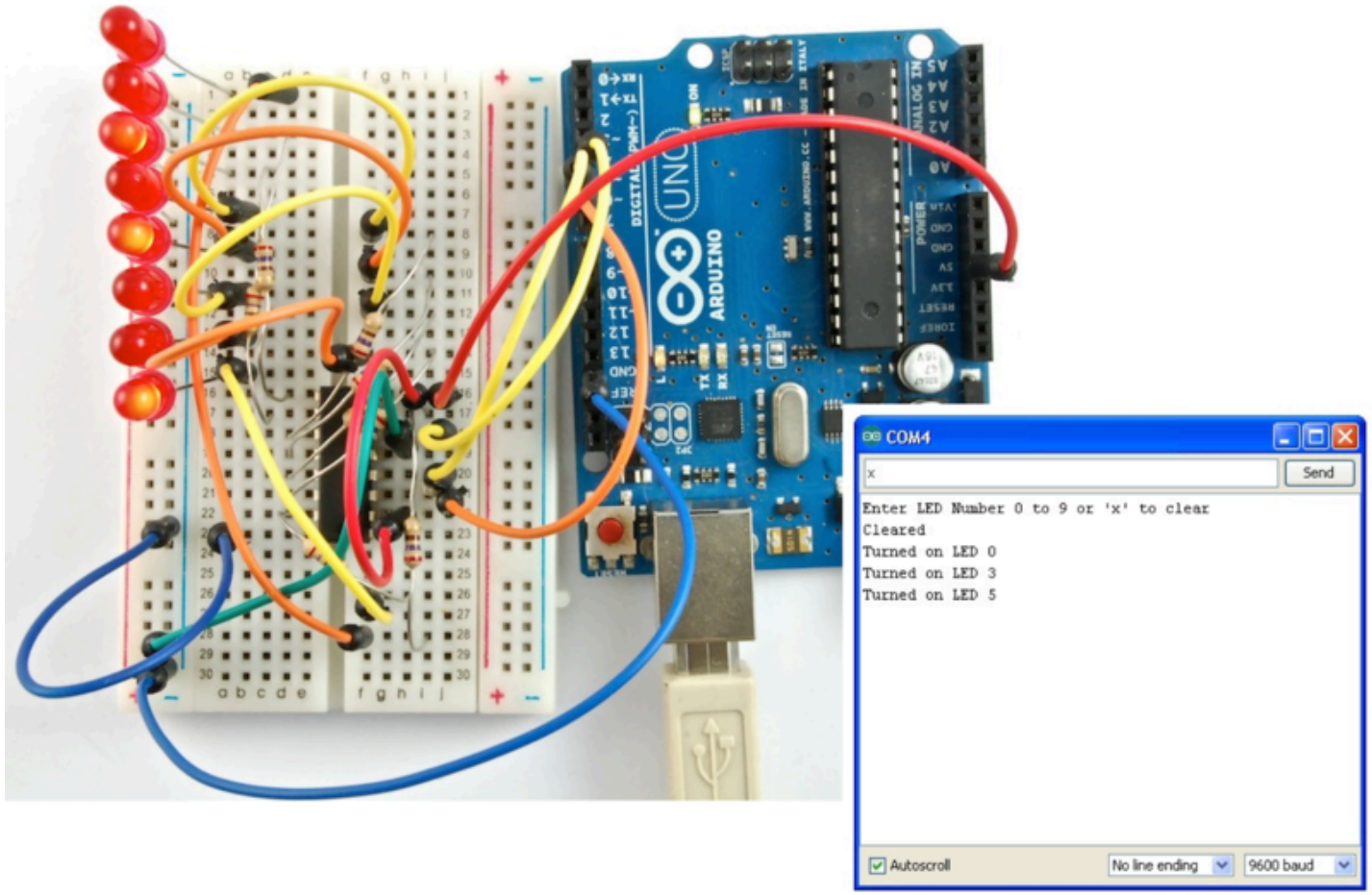
tenacity

Basic Stuff…

- Arduino Uno

tenacity

Flashy Things…



tenacity

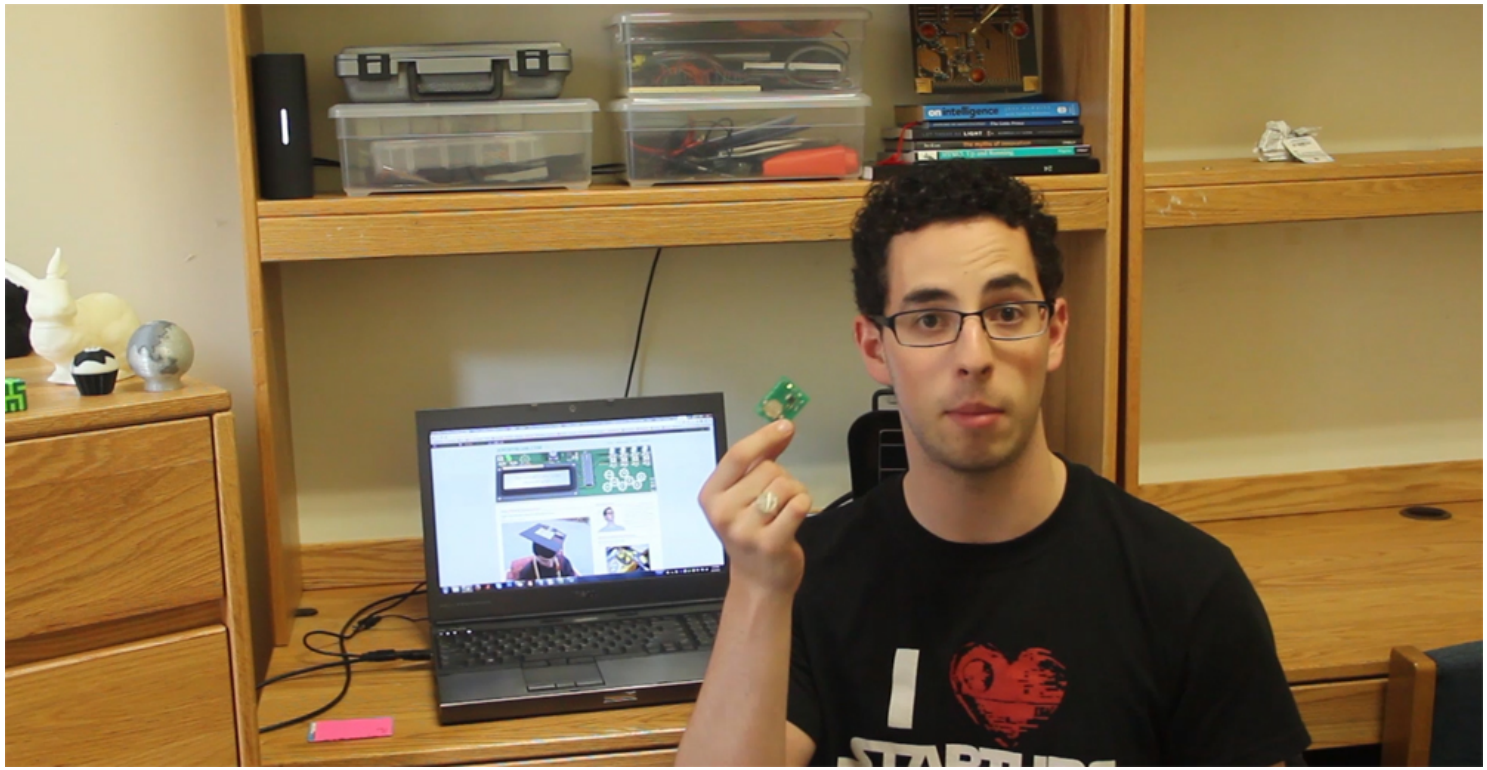
Cooler Stuff!

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

tenacity

Shout Out…

- Jeremy Blum Videos
  - Jeremyblum.com



tenacity

I r a Expert!

tenacity

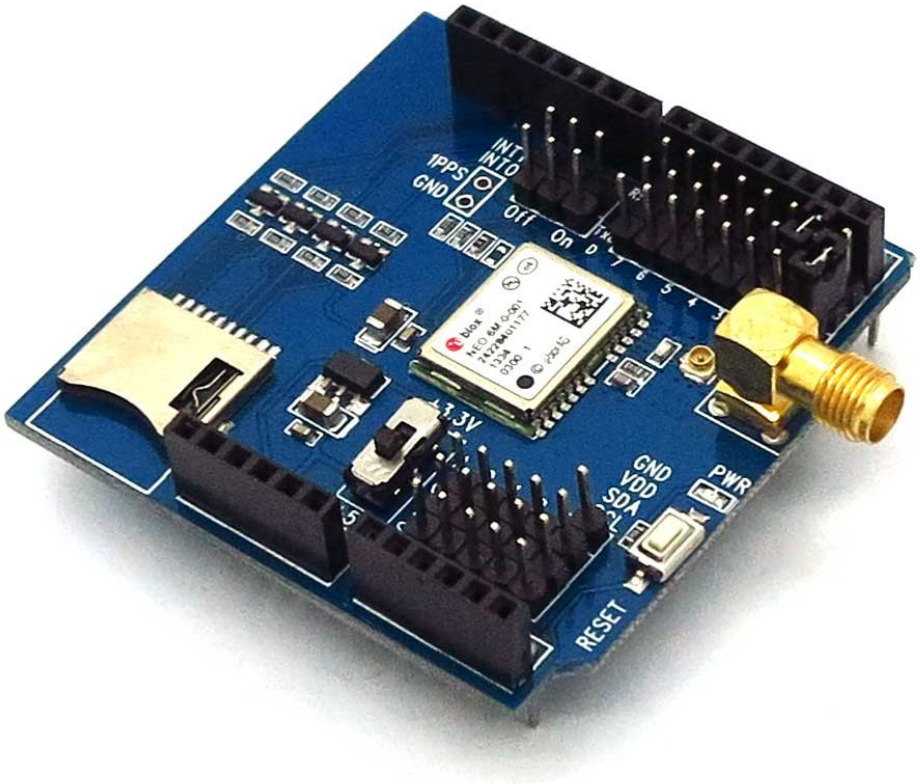
So I got…

- Arduino WiFi Shield

tenacity

And Finally…

- Itead Studio GPS Shield



tenacity

The plan…

- Get a WiFi collection function
  - Write to SD Card
- Get a GPS tracker
  - Write to SD card
- Combine

tenacity

WiFi Shield

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

tenacity

EASY!!!

tenacity

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)

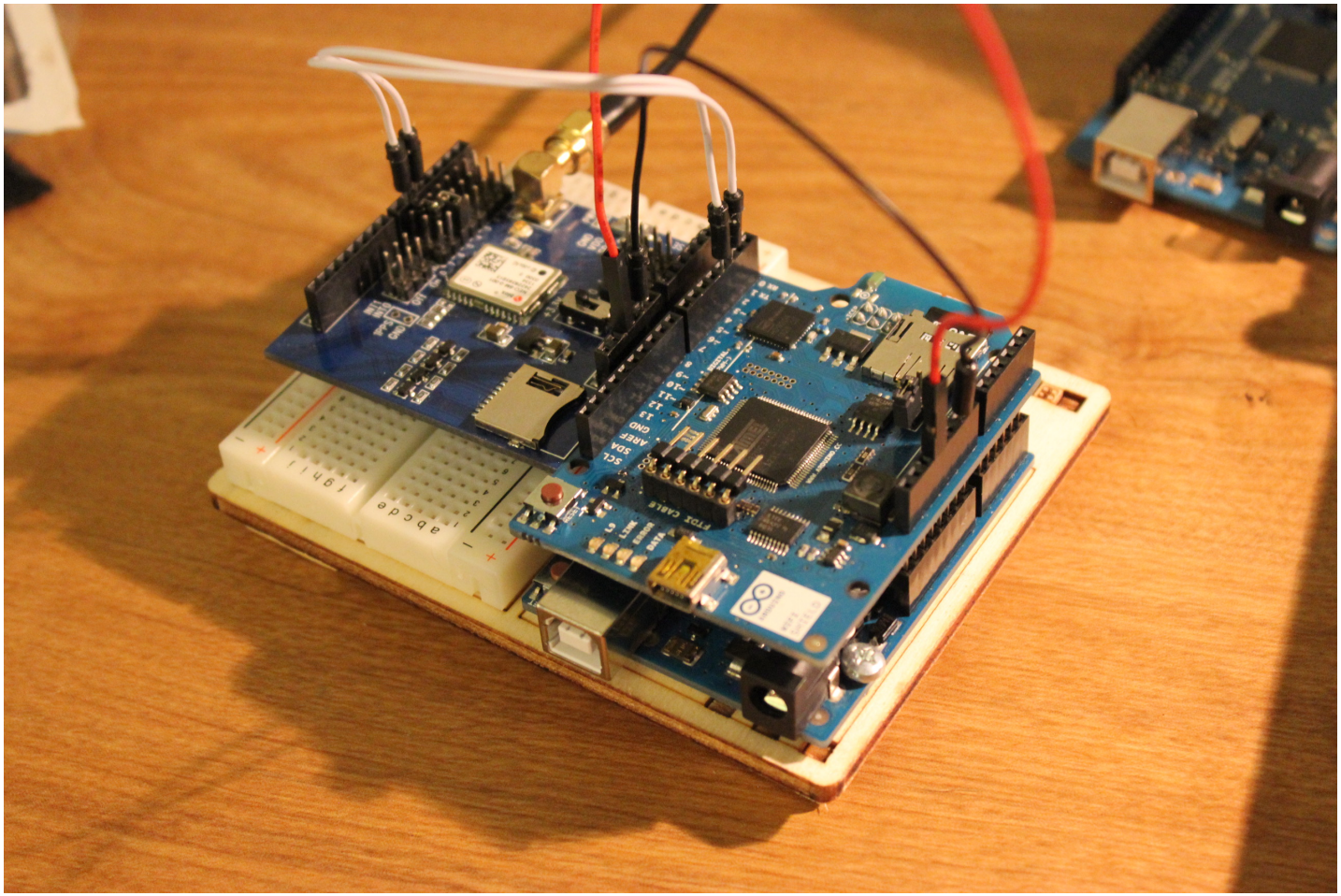
tenacity

GPS Shield

- Poorly Documented
- No docs in kit
- Searched forever to find baudrate of 34800
- Now I can’t NOT find it

tenacity

Put all the components together



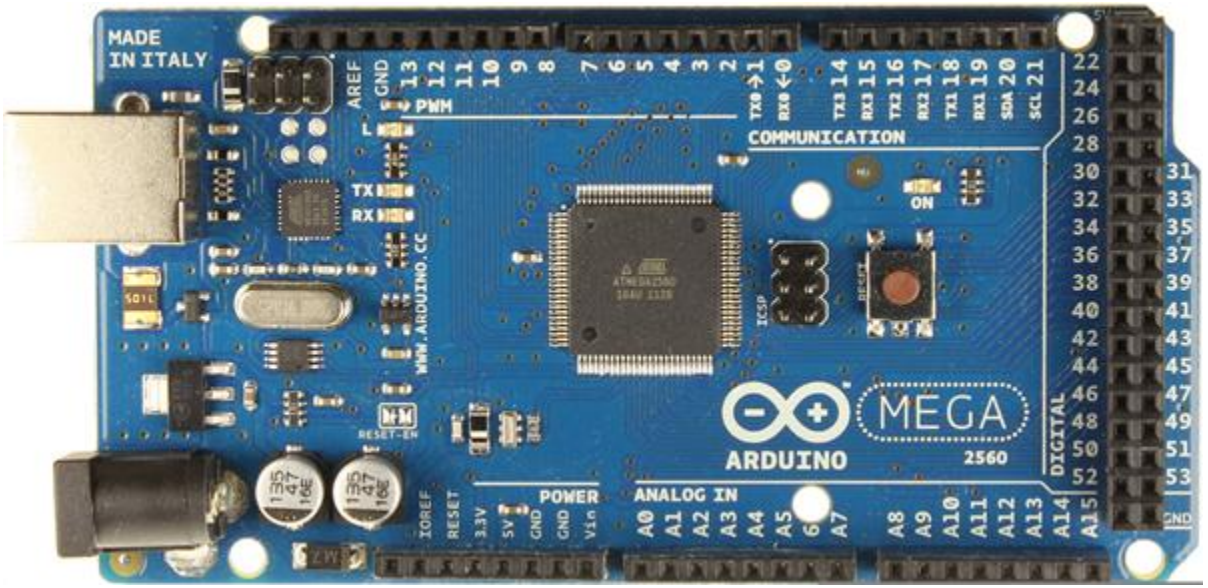
tenacity

So weird error…

- Something about 80% of memory utilized…
- Libraries and variables were too much…
- Arduino Uno – 32K
- Arduino Mega2560 – 256K

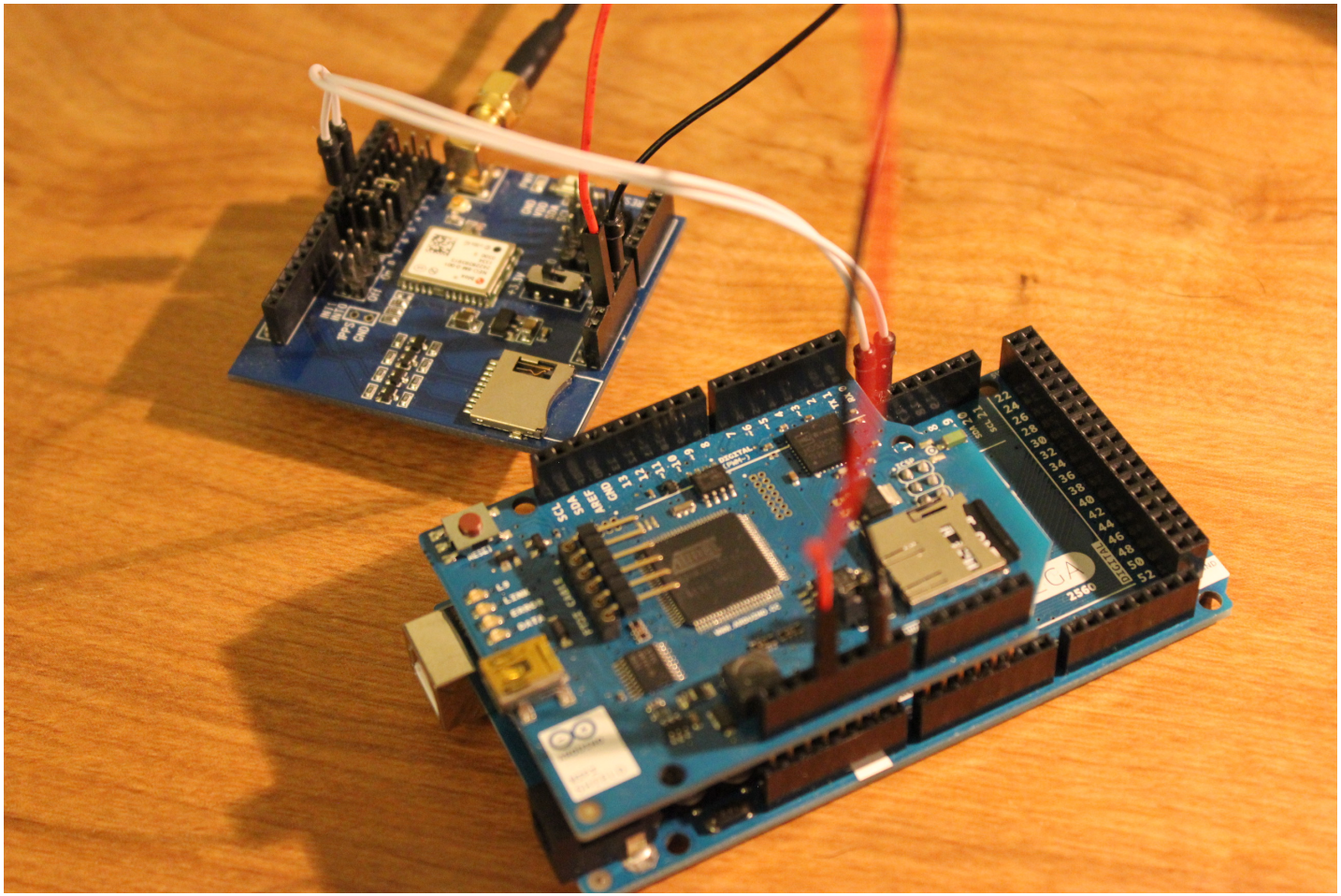
tenacity

Purchased the Mega…



tenacity

Put THAT all together



tenacity

It WORKS!!!

tenacity

Arduino Mega2560

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

tenacity

Tiny Arduino2560?

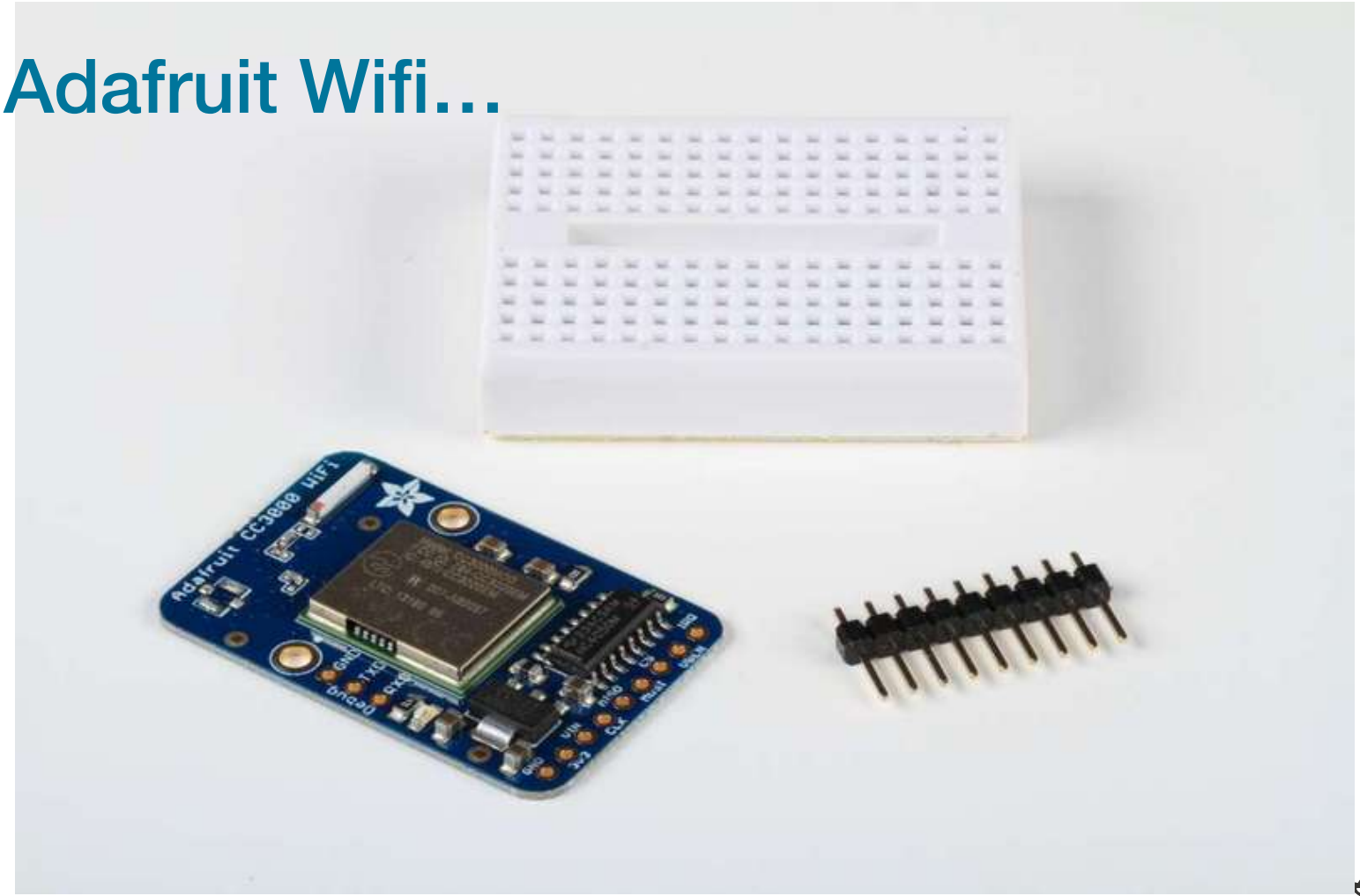
- Arduino MegaMini from JK Devices

- DON'T DO IT!!!!! more later…

tenacity

Small Form Factor

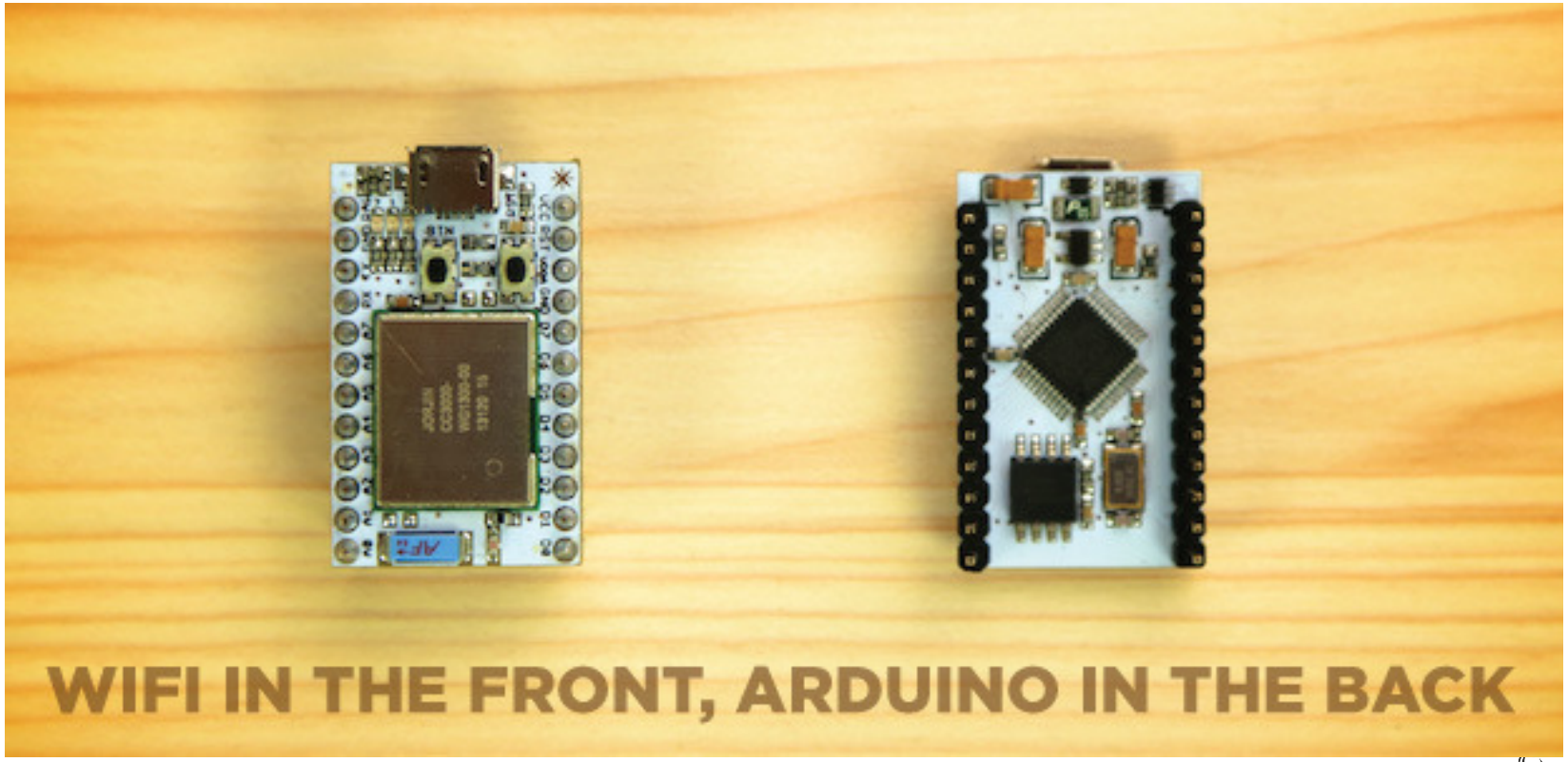
- Adafruit Wifi…



tenacity

Spark Core

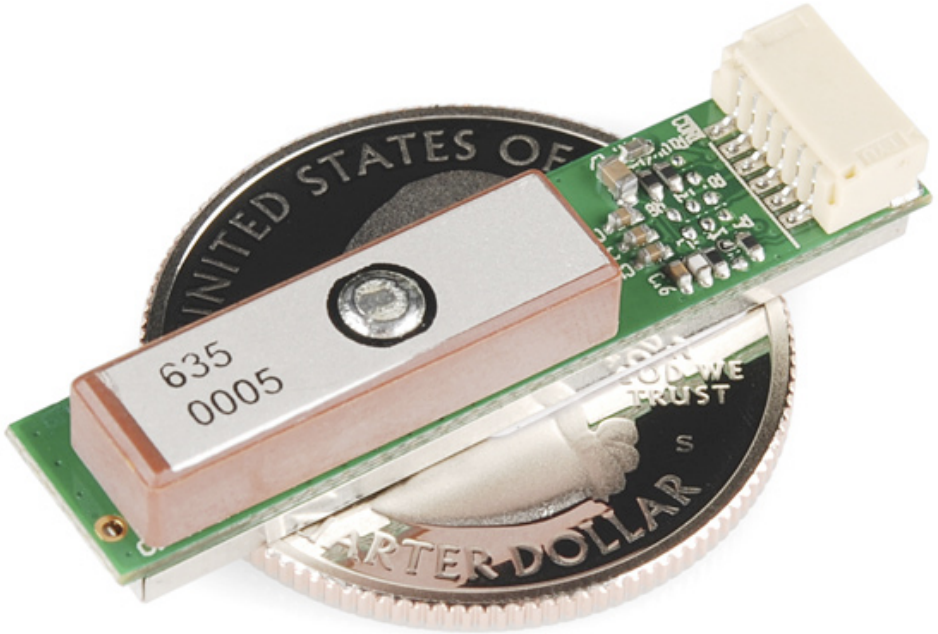
- Spark.io



tenacity

GPS chip

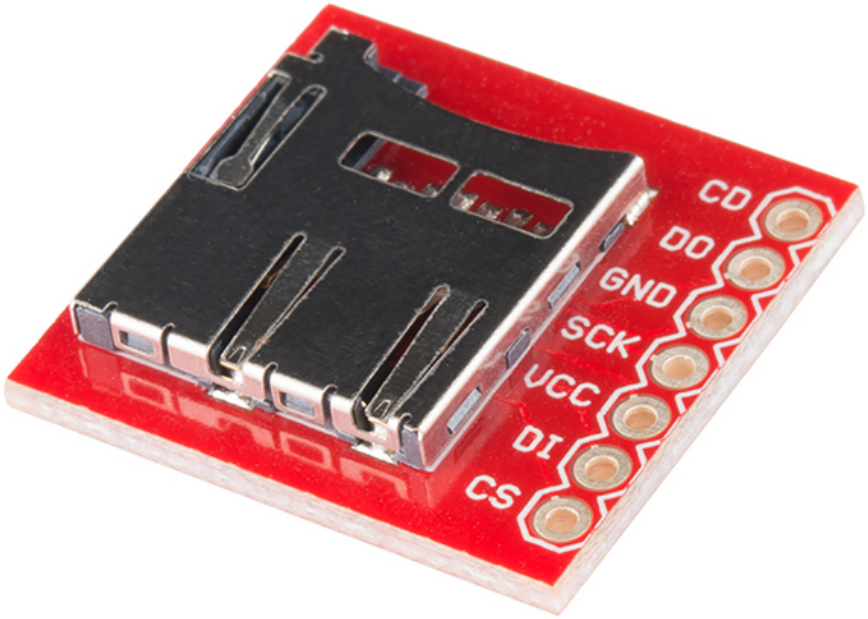
- GP-635T



tenacity

Micro SD Card

- SparkFun MicroSD Breakout Board



tenacity

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, had to borrow one

tenacity

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

tenacity

OMG

tenacity

Start-up Product

- Starting everything from scratch
  - Didn't have libraries for the stuff I needed
- To spite that, VERY COOL
- Dedicated core group of developers
  - Shout out to peekay123
- Lets see what happens…

tenacity

Libraries

- Someone Posted SD Card Libraries to the forums
  - They Compiled!
- Someone posted GPS libraries to the forums…
  - They Compiled & Worked with GPS Shield!

tenacity

WiFi Libraries

- …no readily available stuff for what I wanted to do
- Spark is an “Internet of Things” device
- WiFi as a service – not to mess with

tenacity

Adafruit FTW!

- Adafruit CC3000 Breakout board
- Libraries available on the Adafruit website for Download
- Messed with it earlier… let's see if it works!

tenacity

It WORKS!!!

tenacity

So now…

- Got GPS working on Spark
- Got SD compiled on Spark
- Got SSID collection working on Spark
- Now to work with tiny components

tenacity

Now, onto soldering

tenacity

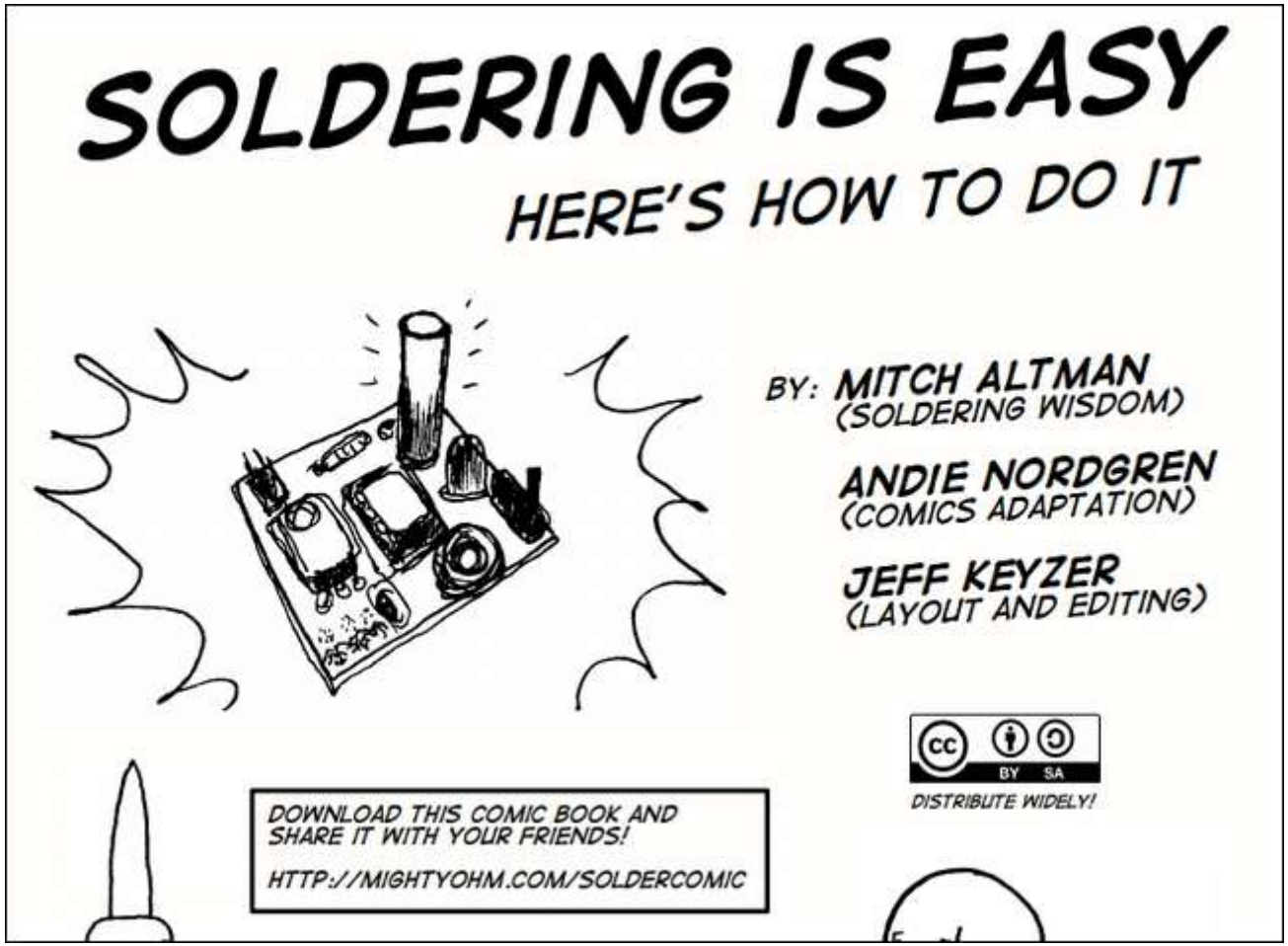
Rule 1

tenacity

Rule 2

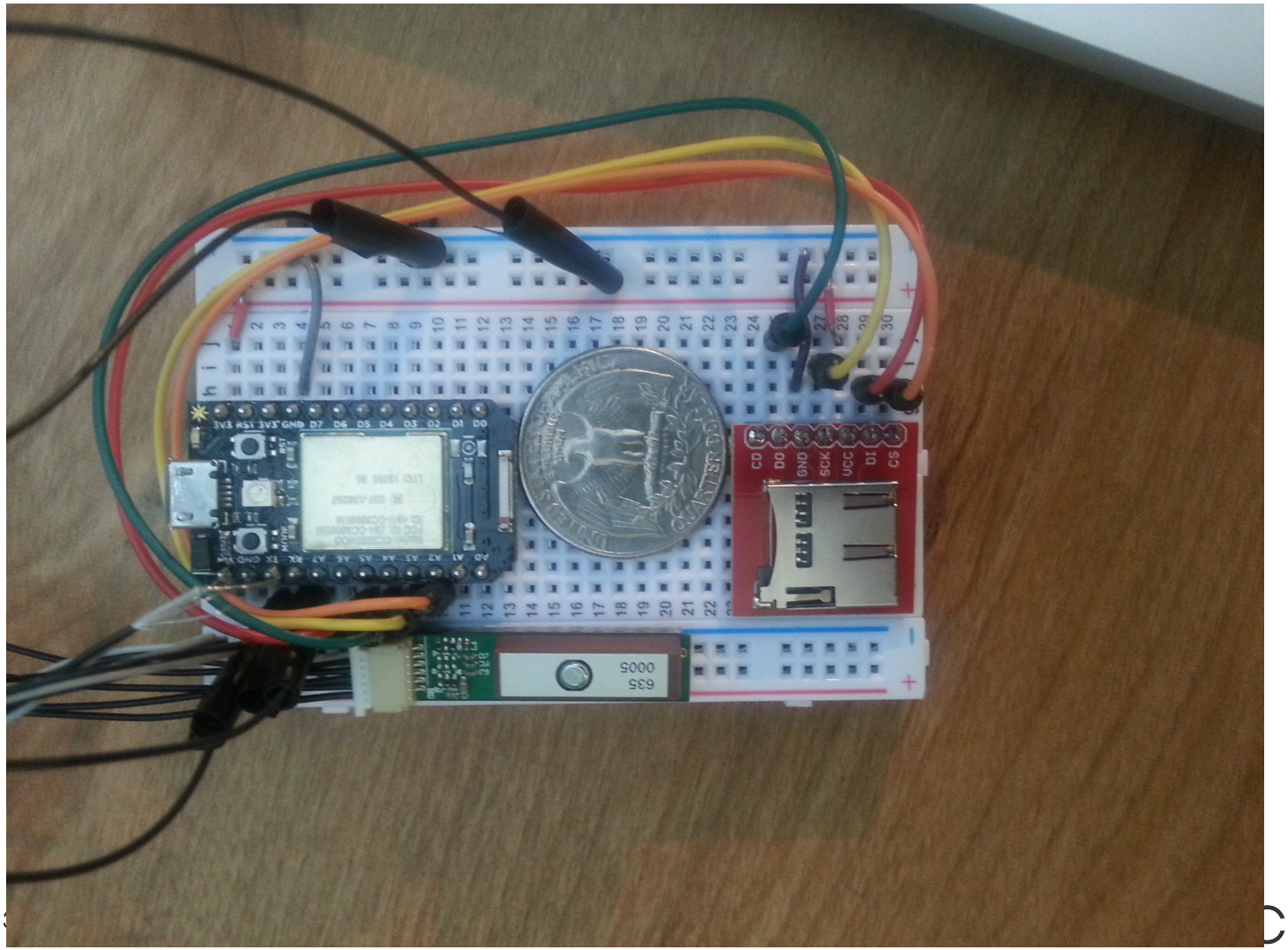
tenacity

Rule 3



tenacity

First attempts went very well…



city

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…?

tenacity

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

tenacity

What to do

- Noticed that I could scan SSID's before I associated with the AP
- Removed code from clause
- That's all I need anyway!

tenacity

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

tenacity

TinyGPS++

- LOVE to use TinyGPS++
  - Everything I need
  - Didn't work in Spark
- How to Port Libraries? Talk to Bill
- Rocket Science
  - Replace Arduino with Spark and fix what blows up

tenacity

It WORKS!!!

tenacity

Next Problem

- Power Consumption
  - How to do it best…?

- Eflite 3.7v 500mAh batteries

tenacity

Testing for Power Consumption

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

tenacity

Time to Make Collar

tenacity

Form Factor

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

tenacity

NOVALabs Shout Out

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

tenacity

Now… where my Maker's at?

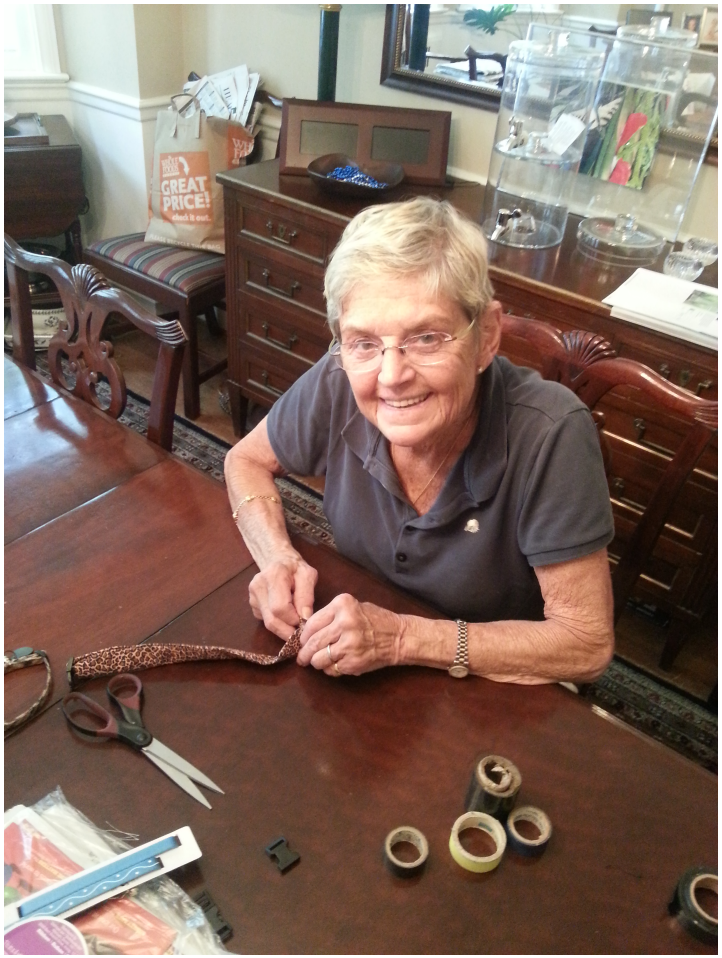
- Need to make a cat collar…
- How do I make a cat collar???
  - Lots of Ways
- Friend Joe suggested ribbons
  - Sew them together

tenacity

Ribbon

tenacity

Get a Grandma



tenacity

Collar Assembly

tenacity

Volunteer Cat

tenacity

So let's PRACTICE first..

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

tenacity

Old Way…

tenacity

New Collar

tenacity

Weight…

tenacity

So… New plan

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

tenacity

Initial results

- …Nothing….!?!?!?!?
- Put collar on cat
- Cat walked under a bush
- Hung out and licked himself for 20 minutes

tenacity

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…!?!?!?????

tenacity

SUCCESS!!!!

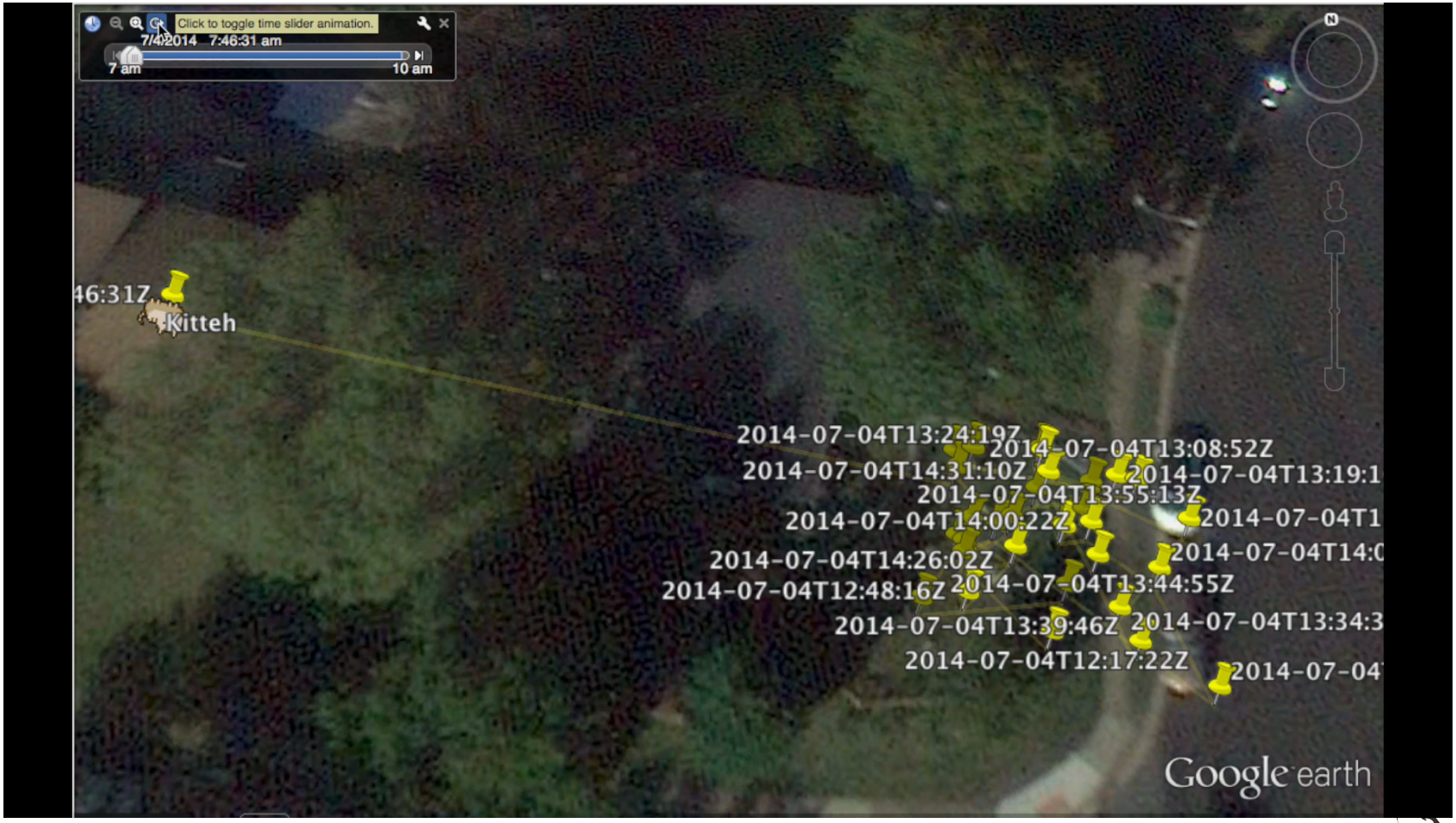
tenacity

Results

Date	Time	Lat	Lon	SSID	Signal	Encrypt
7/4/2014	11:46:31	39.09994	-76.******	walker2	-87	WPA2
7/4/2014	11:46:31	39.09994	-76.******	UDRK2	-92	WEP
7/4/2014	11:46:31	39.09994	-76.******	walker	-83	WPA
7/4/2014	11:46:31	39.09994	-76.******	KNPI1	-95	WEP
7/4/2014	11:46:31	39.09994	-76.******	HOME-BAC6	-93	WPA2
7/4/2014	11:46:31	39.09994	-76.******	8NBN8	-93	WPA2
7/4/2014	11:46:31	39.09994	-76.******	sportsfans	-96	WPA2
7/4/2014	11:46:31	39.09994	-76.******	6RZDB	-95	WPA2
7/4/2014	11:51:38	39.09986	-76.******	walker2	-88	WPA2
7/4/2014	11:51:38	39.09986	-76.******	8NBN8	-98	WPA2
7/4/2014	11:51:38	39.09986	-76.******	KNPI1	-95	WEP
7/4/2014	11:51:38	39.09986	-76.******	sportsfans	-96	WPA2
7/4/2014	11:51:38	39.09986	-76.******	HOME-BAC6	-94	WPA2
7/4/2014	11:51:38	39.09986	-76.******	walker	-83	WPA
7/4/2014	11:51:38	39.09986	-76.******	NOTyourWiFi	-94	WPA2
7/4/2014	11:56:46	39.09987	-76.******	walker2	-90	WPA2
7/4/2014	11:56:46	39.09987	-76.******	VCET0	-98	WEP
7/4/2014	11:56:46	39.09987	-76.******	UDRK2	-98	WEP
7/4/2014	11:56:46	39.09987	-76.******	8NBN8	-96	WPA2
7/4/2014	11:56:46	39.09987	-76.******	walker	-81	WPA
7/4/2014	11:56:46	39.09987	-76.******	P41R1	-95	WEP
7/4/2014	11:56:46	39.09987	-76.******	KNPI1	-94	WEP
7/4/2014	11:56:46	39.09987	-76.******	HOME-BAC6	-92	WPA2
7/4/2014	11:56:46	39.09987	-76.******	NOTyourWiFi	-96	WPA2
7/4/2014	11:56:46	39.09987	-76.******	6RZDB	-94	WPA2

tenacity

Video



tenacity

Coco

tenacity

Results

Date	Time	Lat	Lon	SSID	Signal	Encrypt
7/19/2014	16:59:07	38.94373	-77.******	6WWV8	-94	WPA2
7/19/2014	16:59:07	38.94373	-77.******	CROWLEY	-93	WEP
7/19/2014	16:59:07	38.94373	-77.******	DIRECT-roku-09C2C5	-88	WPA2
7/19/2014	16:59:07	38.94373	-77.******	xfinitywifi	-82	OPEN
7/19/2014	16:59:07	38.94373	-77.******	CoxWiFi	-80	OPEN
7/19/2014	16:59:07	38.94373	-77.******	CableWiFi	-80	OPEN
7/19/2014	17:04:16	38.94365	-77.******	Apple Network 6b7973	-89	WPA2
7/19/2014	17:04:16	38.94365	-77.******	6WWV8	-92	WPA2
7/19/2014	17:04:16	38.94365	-77.******	CQXPP	-76	WPA2
7/19/2014	17:04:16	38.94365	-77.******	P6829	-96	WPA2
7/19/2014	17:09:25	38.94386	-77.******	NETGEAR	-94	WPA2
7/19/2014	17:09:25	38.94386	-77.******	DIRECT-roku-409	-93	WPA2
7/19/2014	17:14:34	38.9435	-77.******	7LXJ3	-83	WEP
7/19/2014	17:14:34	38.9435	-77.******	peri	-93	WPA
7/19/2014	17:14:34	38.9435	-77.******	Ward3DC	-88	WPA2
7/19/2014	17:14:34	38.9435	-77.******	MYI14	-96	WEP
7/19/2014	17:19:43	38.94323	-77.******	7LXJ3	-94	WEP
7/19/2014	17:19:43	38.94323	-77.******	LuckyWhale_2GEXT	-93	WPA2
7/19/2014	17:24:52	38.94373	-77.******	LKMY4	-96	WPA2
7/19/2014	17:24:52	38.94373	-77.******	MYI14	-94	WEP
7/19/2014	17:40:19	38.94316	-77.******	LuckyWhale_2GEXT	-92	WPA2
7/19/2014	17:40:19	38.94316	-77.******	Motyka Wireless	-88	WPA
7/19/2014	17:40:19	38.94316	-77.******	Ward3DC	-90	WPA2
7/19/2014	17:40:19	38.94316	-77.******	SXJ32	-94	WPA2
7/19/2014	17:40:19	38.94316	-77.******	Q8ZS7	-96	WEP

tenacity

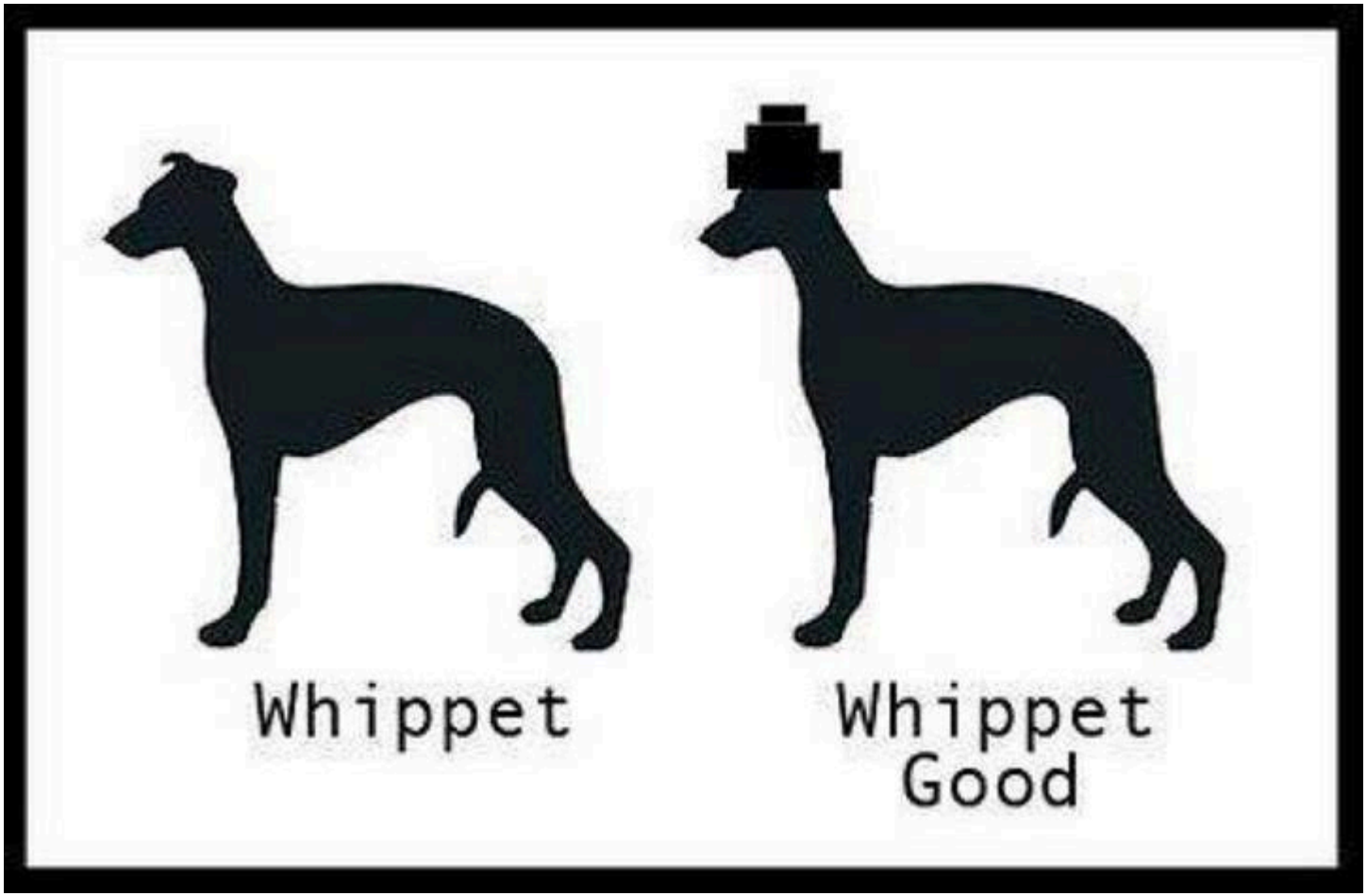
Video

tenacity

That's the WarKitteh!

tenacity

Denial of Service Dog



tenacity

DoS Dog

- So…. More trolling than anything
- WiFi Pineapple
  - Procured at ShmooCon
- TV B Gone
  - Adafruit/RadioShack
- Doggie Backpack with “Denial of Service Dog” patches

tenacity

WiFi Pineapple

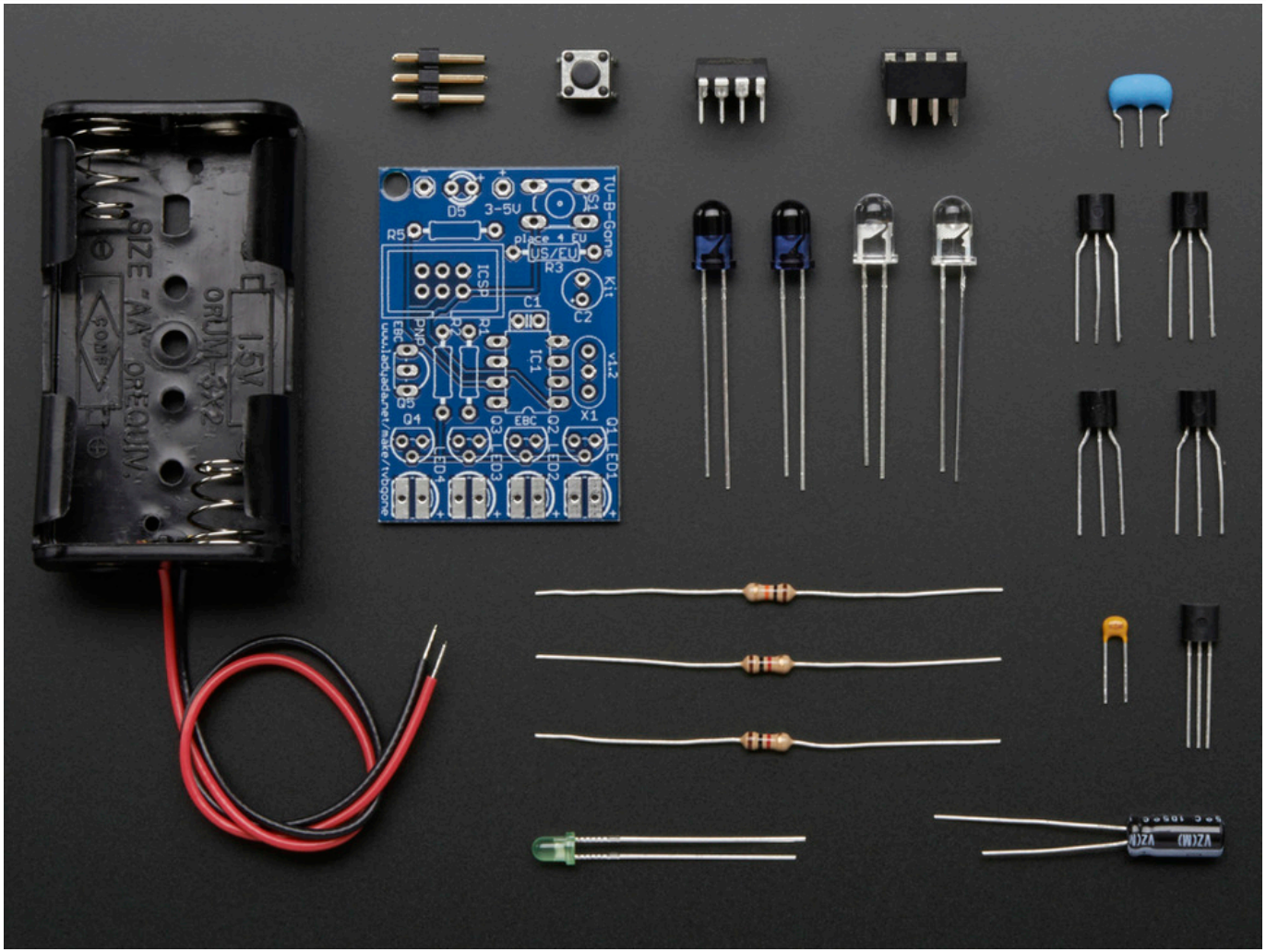
tenacity

What I'm gonna do is…

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

tenacity

TV B Gone ….in pieces.

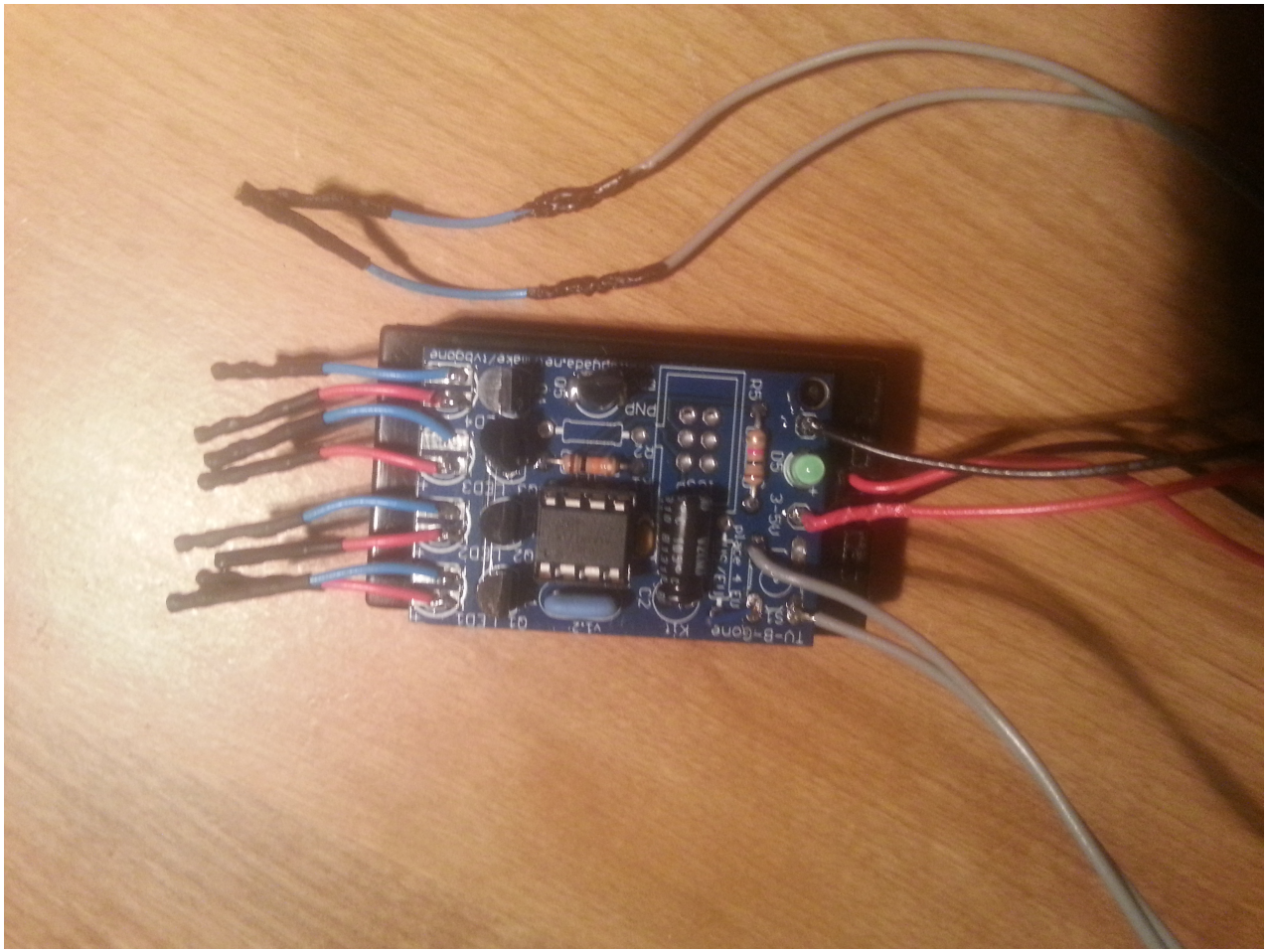


tenacity

TV B Gone

tenacity

Some minor modifications…



tenacity

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

tenacity

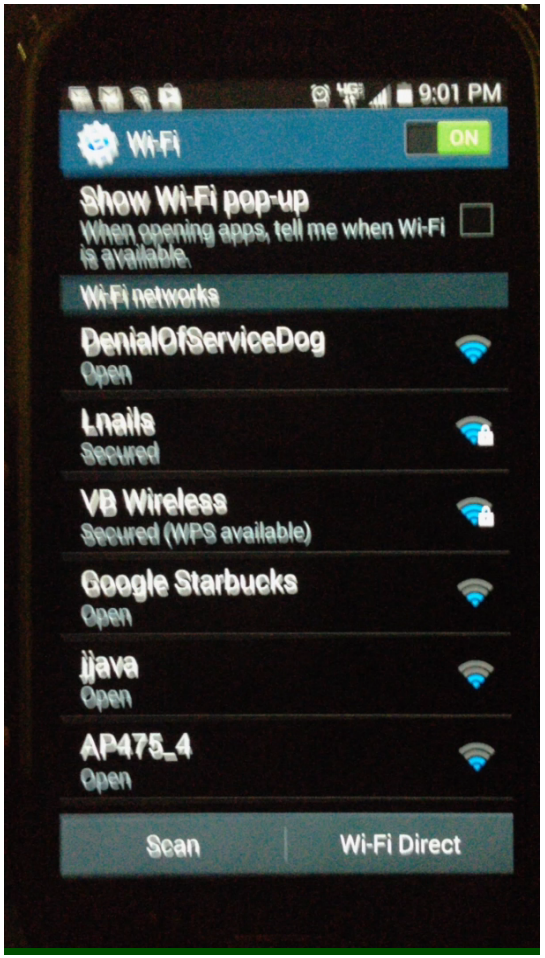
Victory!

tenacity

Demo Video

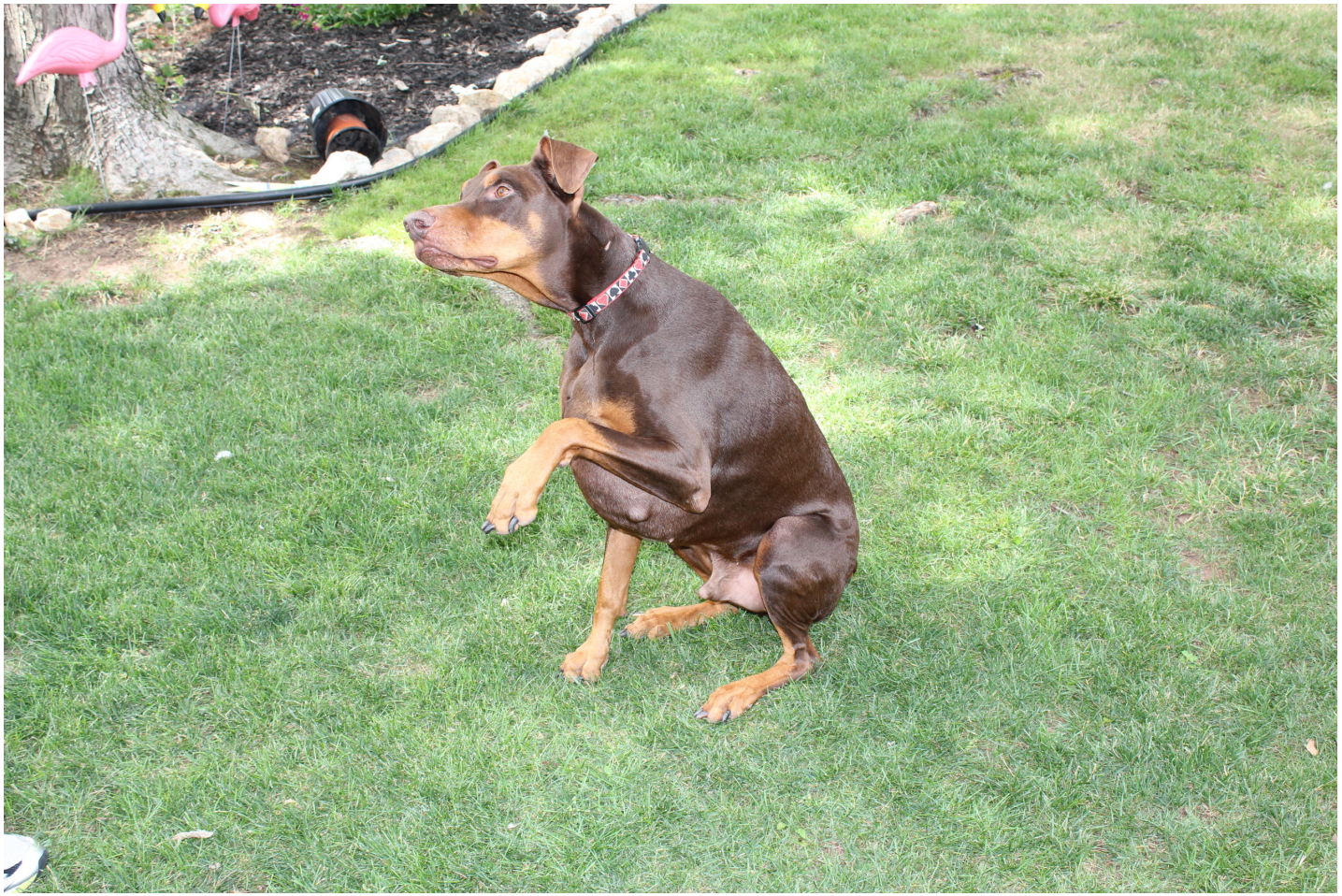
tenacity

Demo Video



tenacity

Volunteer Dog



tenacity

Volunteer Dog

tenacity

Volunteer Dog

tenacity

Volunteer Dog Ready to Go!

tenacity

Putting it on a Doggie Backpack

tenacity

Top View

tenacity

LEDs…

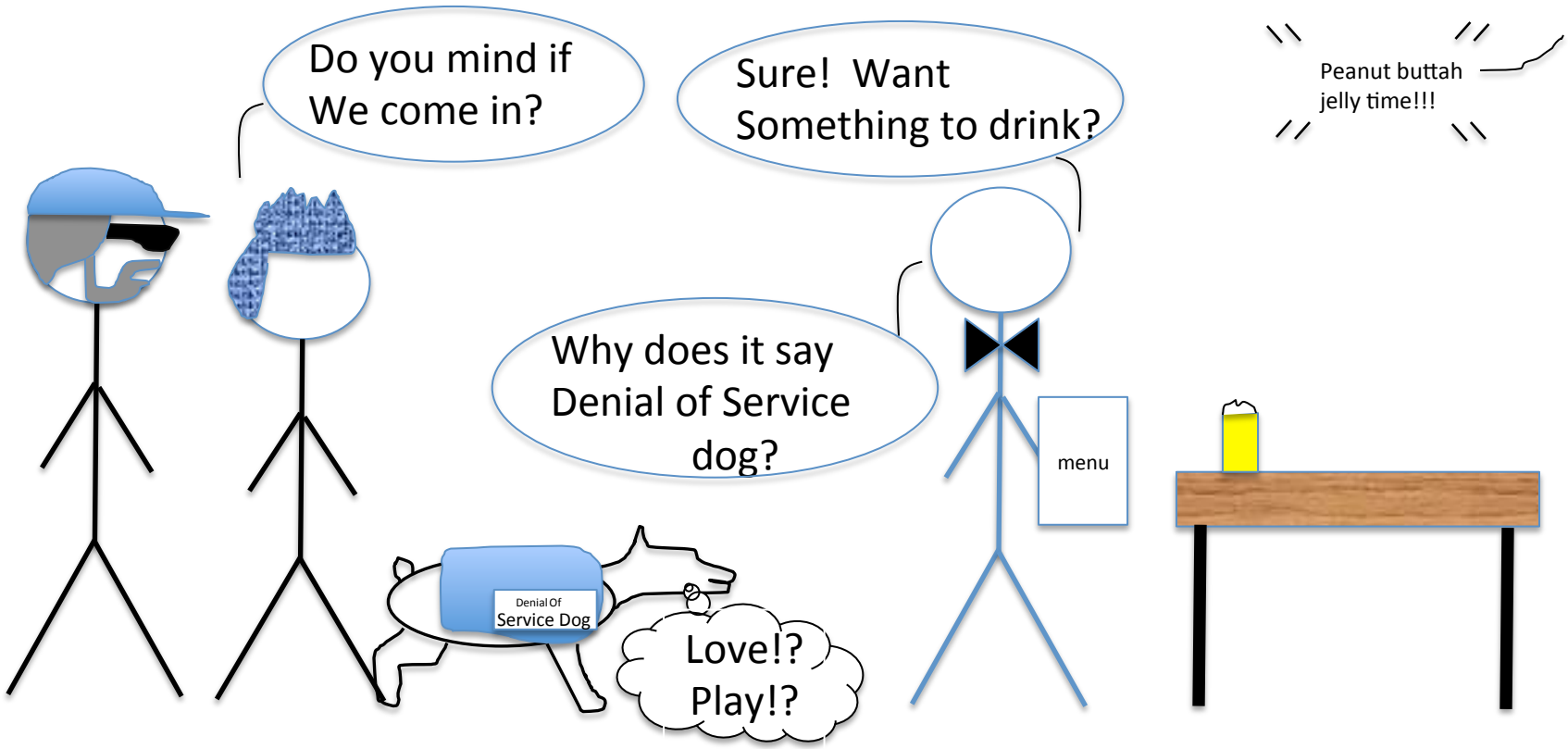
tenacity

Dog will Shake

- TV B Gone wasn't designed to be shaken in the manner in which V-dog was shaking..
- Also set off the TV-B-Gone

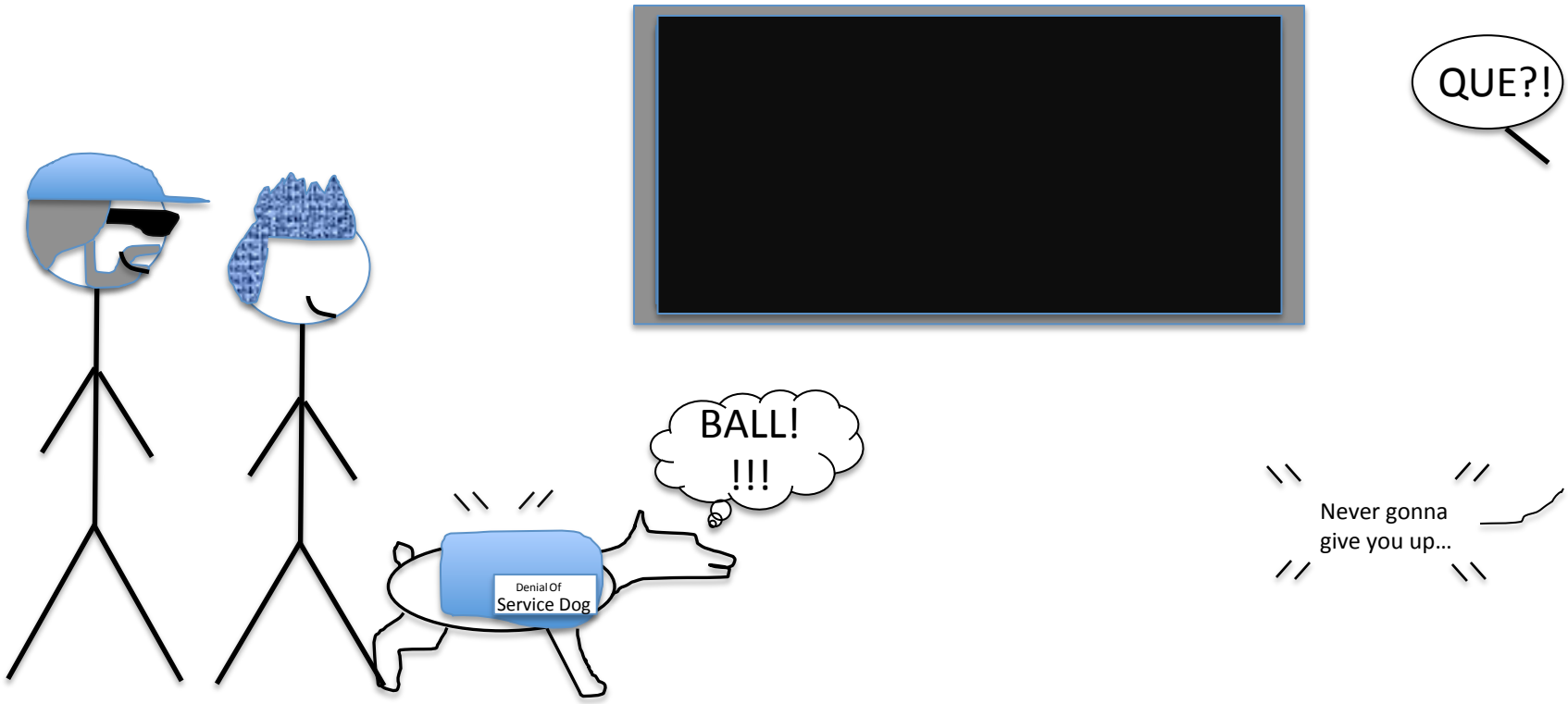
tenacity

Restaruant



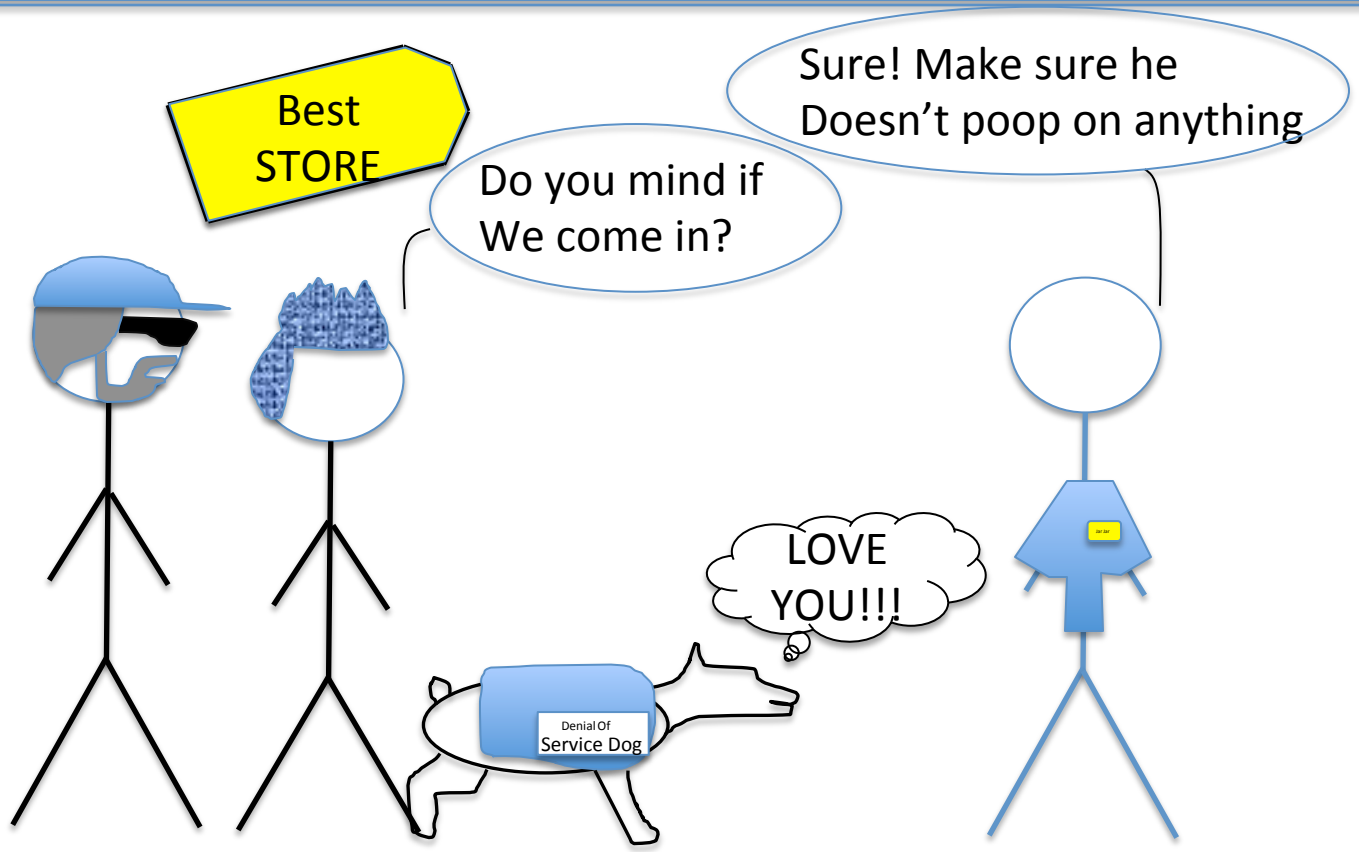
tenacity

Sports Bar



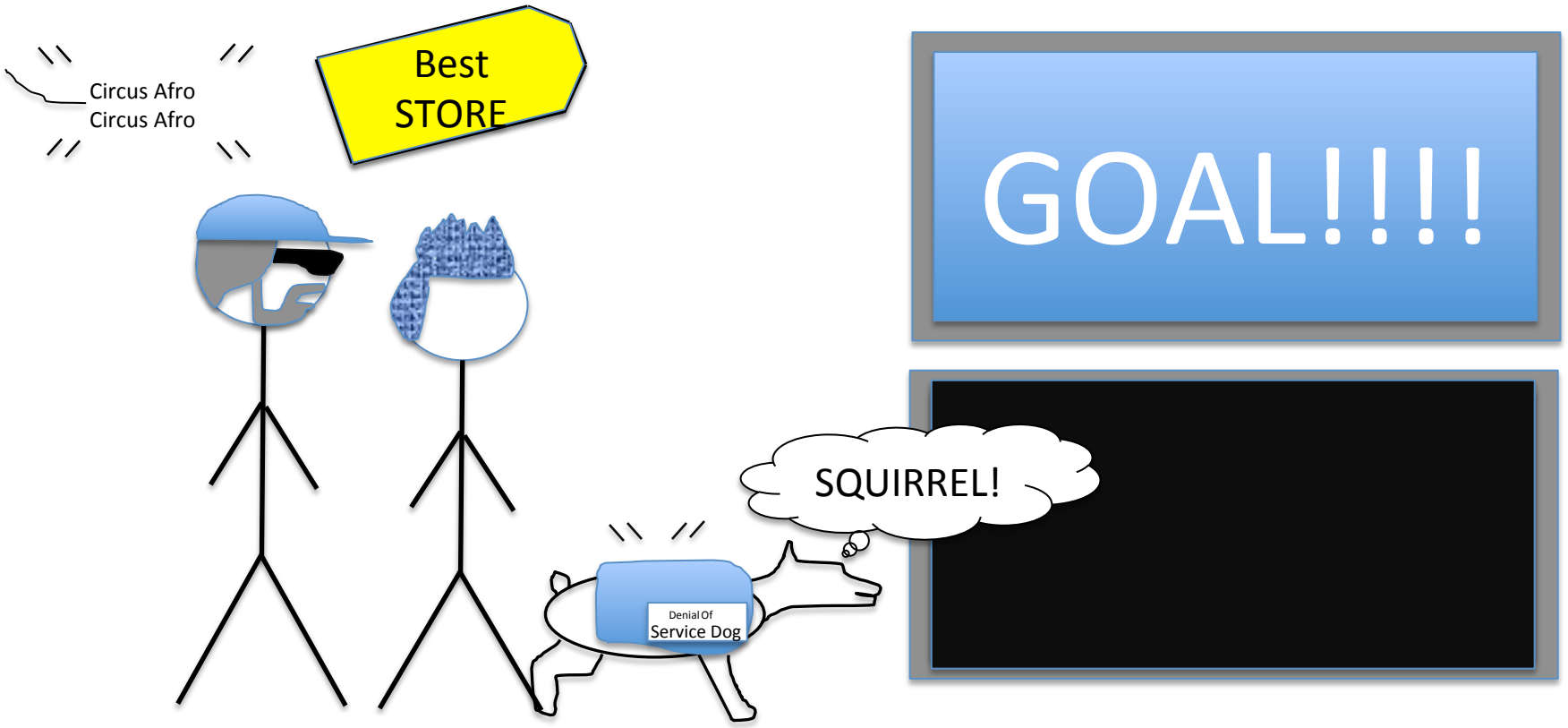
tenacity

Box Store



tenacity

Box Store Cont…



tenacity

Results…

- According to results, several hapless victims connected to Karma/Denial of Service dog
  - Logging Fail
- Only one person asked about “Denial Of” service dog
- Most people said “NICE DOGGY!”

tenacity

So What Have We Learned???

- A tech hobbyist with no prior firmware experience can create a functional WarKitteh Collar in a short amount of time.
- In 2014 there are STILL unsecured WiFi hotspots
- Lots of devices still probe
- Still no patch for human stupidity
- Cats – AND DOGS – are really hard to work with

tenacity

Shout out

- Jeremyblum.com
- Adafruit.com
- Sparkfun.com
- Spark.io
- Arduino.cc

tenacity

Oh BTW

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

tenacity

Thanks

- Reeves
- Bill
- Joe
- Joey
- Nancy
- Ricky
- V-dog.owners
- Spark.io Guys
- NoVaLabs Guys
- V-dog
- Skitzy
- Coco
- Tenacity
- DefCon

tenacity

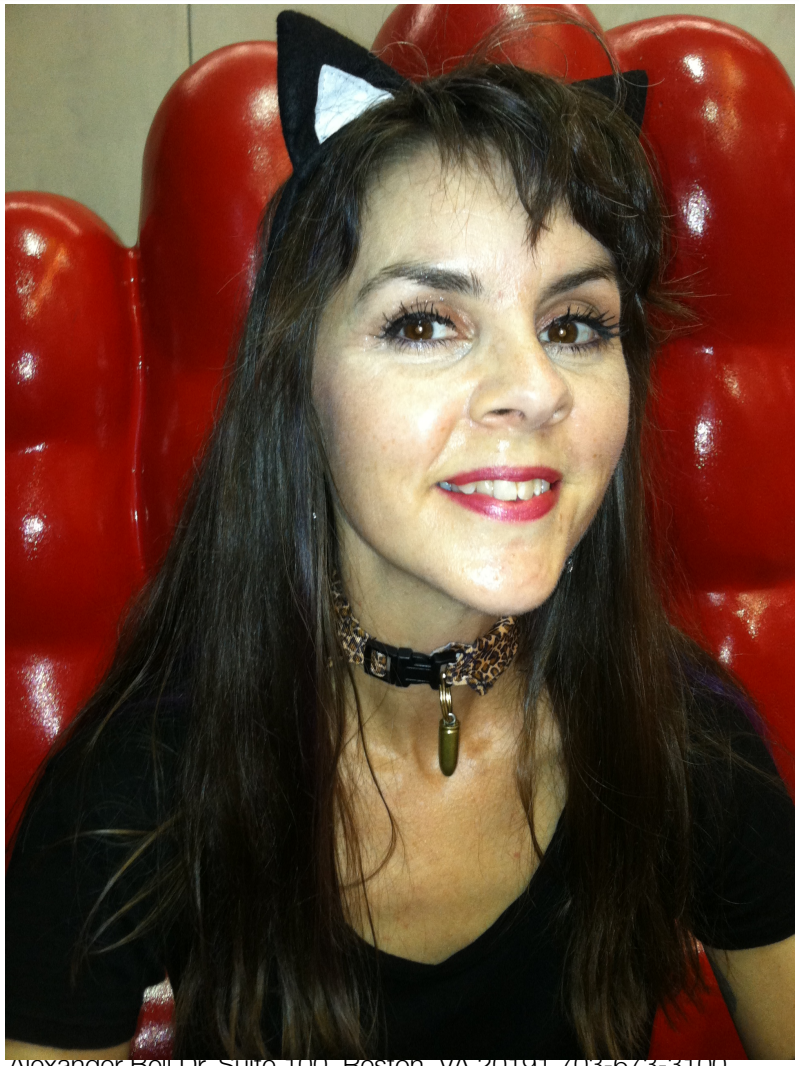
DefCon Activities

tenacity

DefCon WarKitteh

tenacity

BadKitty



tenacity

Walking The Strip

tenacity

All Kinds of People

tenacity

Street Performers

tenacity

Monuments

tenacity

Willing Participants

tenacity

Drunk Participants

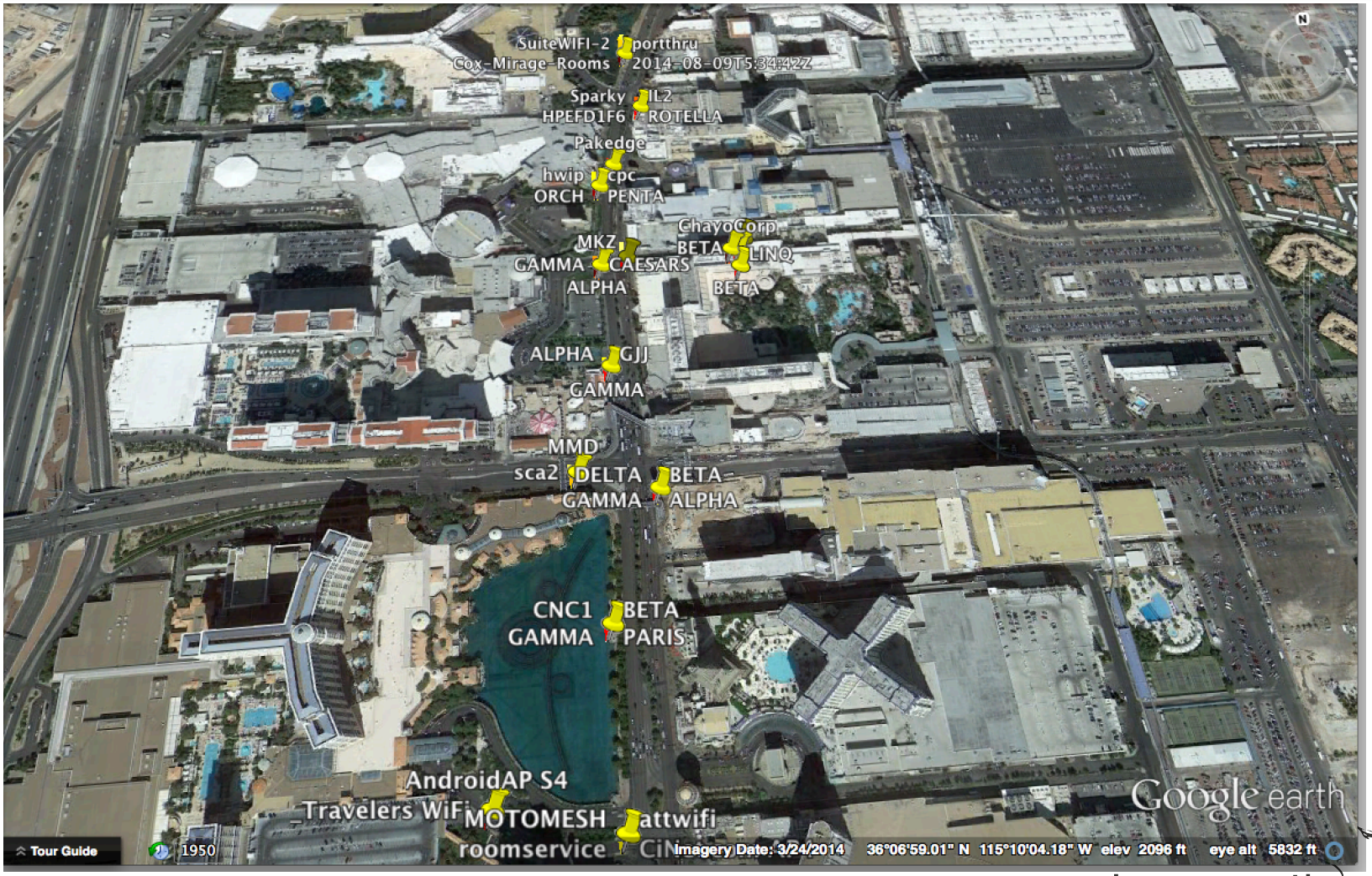
tenacity

Results

Date	Time	Lat	Lon	SSID	Signal	Encrypt
8/9/2014	5:34:42	36.12057	-115.173	Cox-Mirage-Rooms	-94	OPEN
8/9/2014	5:34:42	36.12057	-115.173	AirOne	-90	WPA2
8/9/2014	5:34:42	36.12057	-115.173	portthru	-90	OPEN
8/9/2014	5:39:52	36.11833	-115.173	attwifi	-71	OPEN
8/9/2014	5:39:52	36.11833	-115.173	hetwrls	-80	WPA2
8/9/2014	5:39:52	36.11833	-115.173	Gertrude	-80	WPA2
8/9/2014	5:39:52	36.11833	-115.173	i5875b	-86	WEP
8/9/2014	5:39:52	36.11833	-115.173	ALPHA	-96	WPA2
8/9/2014	5:39:52	36.11833	-115.173	GAMMA	-94	WPA2
8/9/2014	5:39:52	36.11833	-115.173	hwip	-89	OPEN
8/9/2014	5:39:52	36.11833	-115.173	MOTOMESH	-76	OPEN
8/9/2014	5:39:52	36.11833	-115.173	BETA	-94	WPA2
8/9/2014	5:39:52	36.11833	-115.173	PENTA Guest Access	-83	WPA2
8/9/2014	5:39:52	36.11833	-115.173	PENTA	-82	WPA2
8/9/2014	5:39:52	36.11833	-115.173	cpc	-96	WPA2
8/9/2014	5:39:52	36.11833	-115.173	ORCH	-94	WPA2
8/9/2014	5:39:52	36.11833	-115.173	LINQ	-90	OPEN
8/9/2014	5:45:01	36.11575	-115.173	Flamingo-Rooms-Cox	-89	OPEN
8/9/2014	5:45:01	36.11575	-115.173	MOTOMESH	-81	OPEN
8/9/2014	5:45:01	36.11575	-115.173	attwifi	-73	OPEN
8/9/2014	5:45:01	36.11575	-115.173	CROMWELL	-88	OPEN
8/9/2014	5:45:01	36.11575	-115.173	GJJ	-93	WPA2
8/9/2014	5:45:01	36.11575	-115.173	GAMMA	-86	WPA2
8/9/2014	5:45:01	36.11575	-115.173	ALPHA	-84	WPA2
8/9/2014	5:45:01	36.11575	-115.173	DELTA	-86	WPA2

tenacity

Video… er… PIC!!!



tenacity

DefCon DoS Dog

tenacity

SkyDog

tenacity

CNN Kitteh

tenacity

Questions?

tenacity

That's all Folks

tenacity