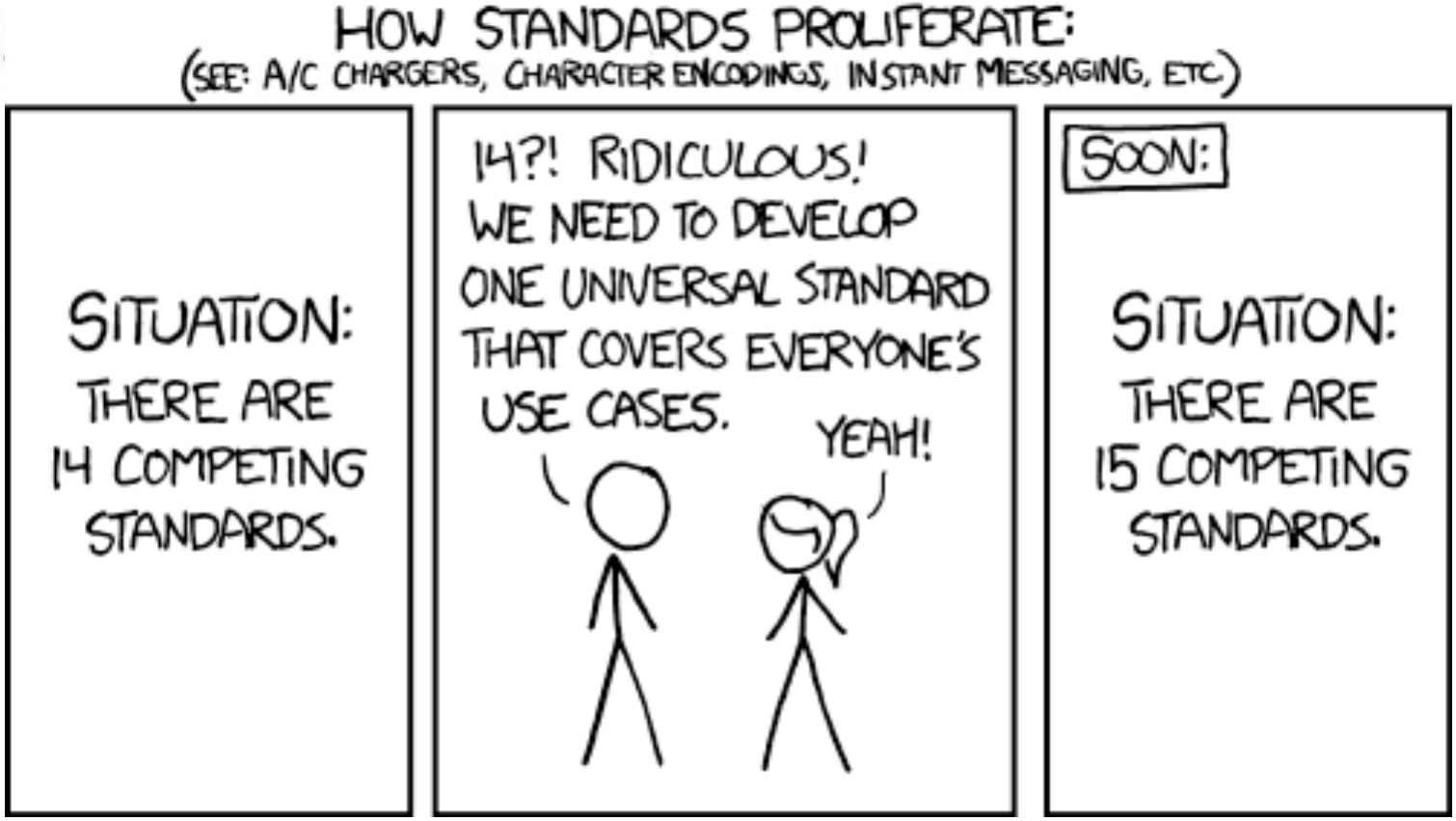
Blackhat Vegas, 2011

PPI-Geolocation: The next generation of 802.11 visualization and geo-location

Your presenter

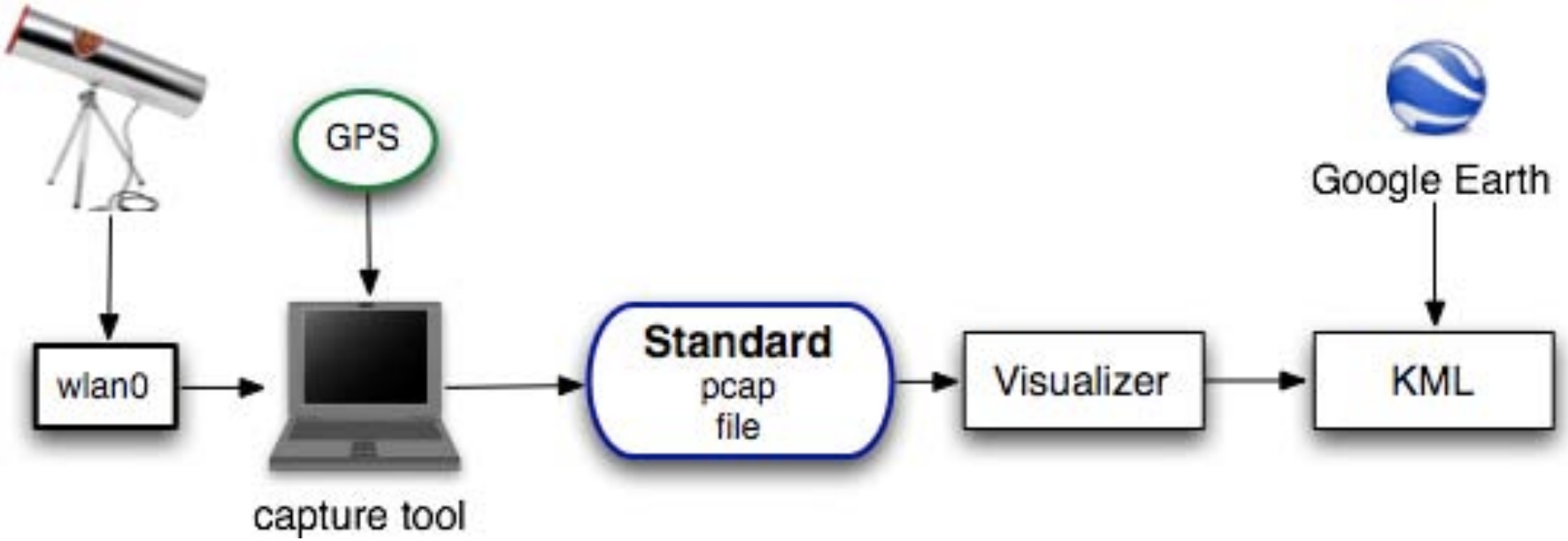
- Jon “Johnny Cache” Ellch
  - Co-Author: Hacking Exposed: Wireless
  - Many 802.11 cracking utilities
  - Aspiring Atari 2600 programmer
  - Wireless Engineer, Harris Corp.
  - Youngest obsolete guy around.

802.1 visualization now:



Motivation

HARRIS
Crucial Security Programs



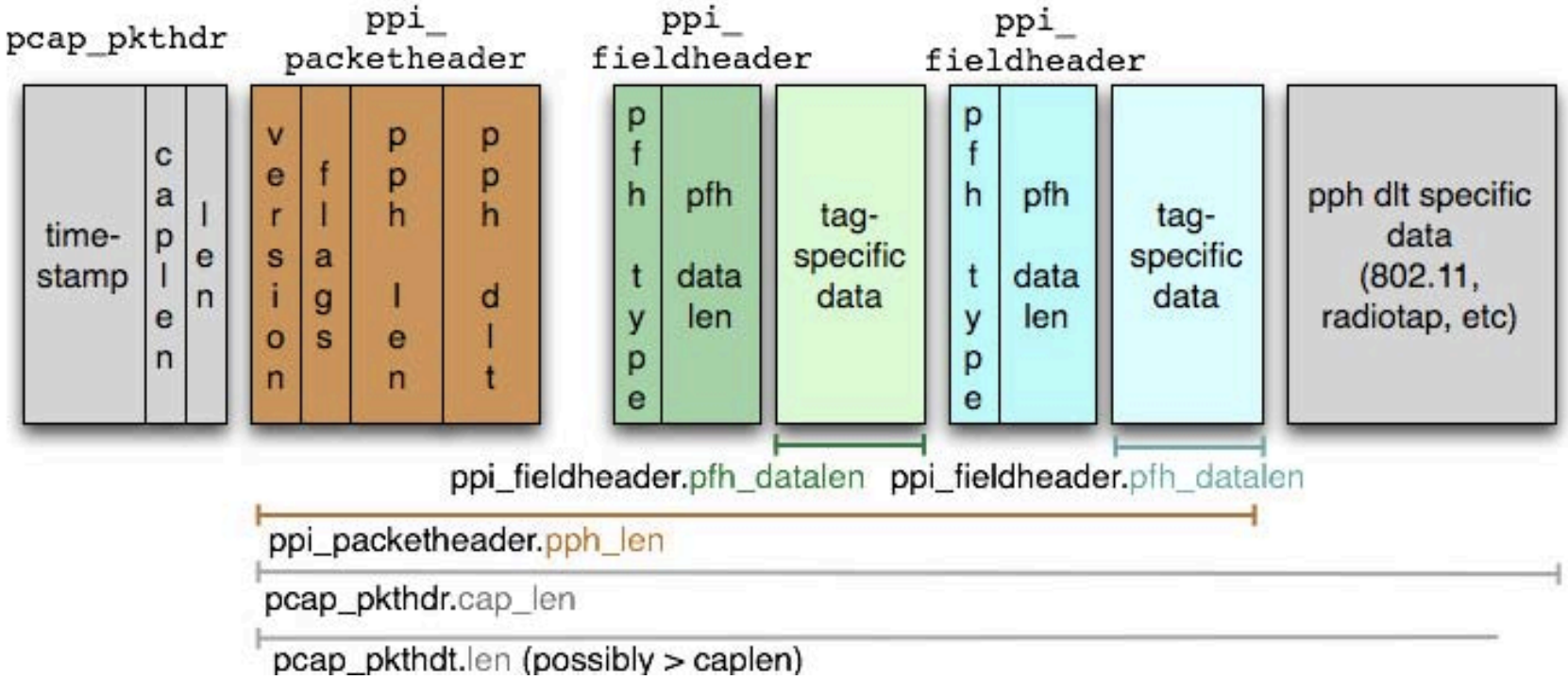
Per-Packet Information

- PPI for short.
- Developed by CACE in 2008
- Allows applications to store *Per-Packet Information* in standard pcap file **without** breaking compatibility with tools.

What PPI-GEOLOCATION gets us

- Ability to look at a single pcap file and tell when, where, and what captured a given wireless packet.
- Ability to create/modify this data across a wide variety of tools.
- Most obvious use: Universal visualizer

Per-Packet Information




© 2011 Google
Image © 2011 DigitalGlobe
7 m
Google

Well that's a start, but..

- What direction were we travelling?
- Where was the antenna pointed?
- Which way was the car pointing?
- We need a **Vector**

Vector details

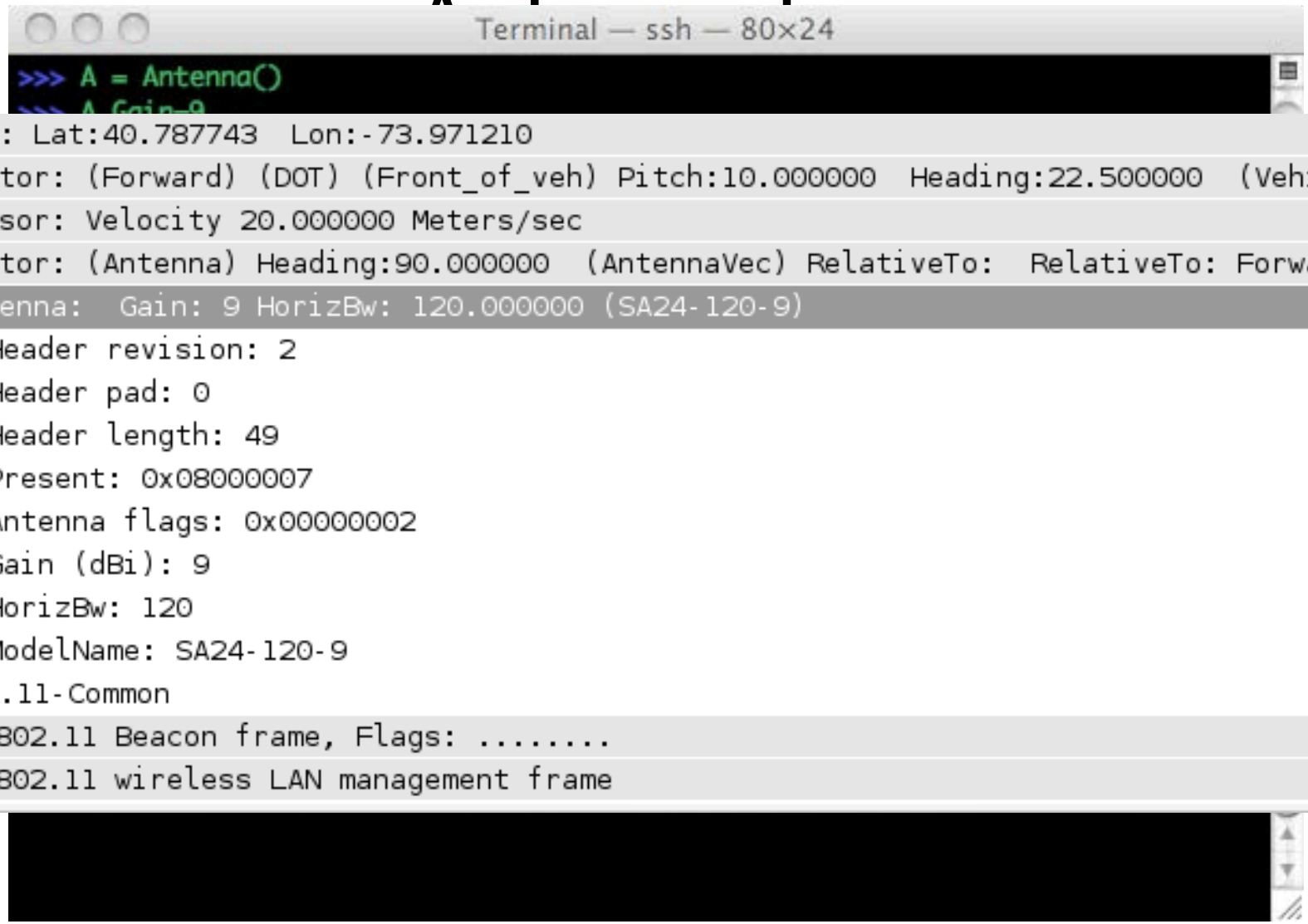
- Vectors specify arbitrary 3-dimensional orientation.
- Vectors can be relative to each other, or relative to earth.
- Vector Characteristic bitmask is used to denote what vector **represents**. Most likely uses are Direction of Travel, Front of Vehicle, and Antenna.


Direction of Travel
© 2011 Google
Image © 2011 DigitalGlobe
Google


Direction of Travel
Antenna Frame
© 2011 Google
Image © 2011 DigitalGlobe
5 m
Google

Okay, that was cool, But..

- What good is knowing the orientation if we don't know what sort of antenna is attached?


Terminal — ssh — 80×24
>>> A = Antenna()
GPS: Lat:40.787743 Lon:-73.971210
Vector: (Forward) (DOT) (Front_of_veh) Pitch:10.000000 Heading:22.500000 (VehicleVec)
Sensor: Velocity 20.000000 Meters/sec
Vector: (Antenna) Heading:90.000000 (AntennaVec) RelativeTo: RelativeTo: Forward
Antenna: Gain: 9 HorizBw: 120.000000 (SA24-120-9)
Header revision: 2
Header pad: 0
Header length: 49
Present: 0x08000007
Antenna flags: 0x00000002
Gain (dBi): 9
HorizBw: 120
ModelName: SA24-120-9
802.11-Common
IEEE 802.11 Beacon frame, Flags: ....
IEEE 802.11 wireless LAN management frame

Okay that was cool, But..

- What about how fast we were going?
- Did I say velocity? I meant Acceleration.
- And temperature.
- And Humidity (?)

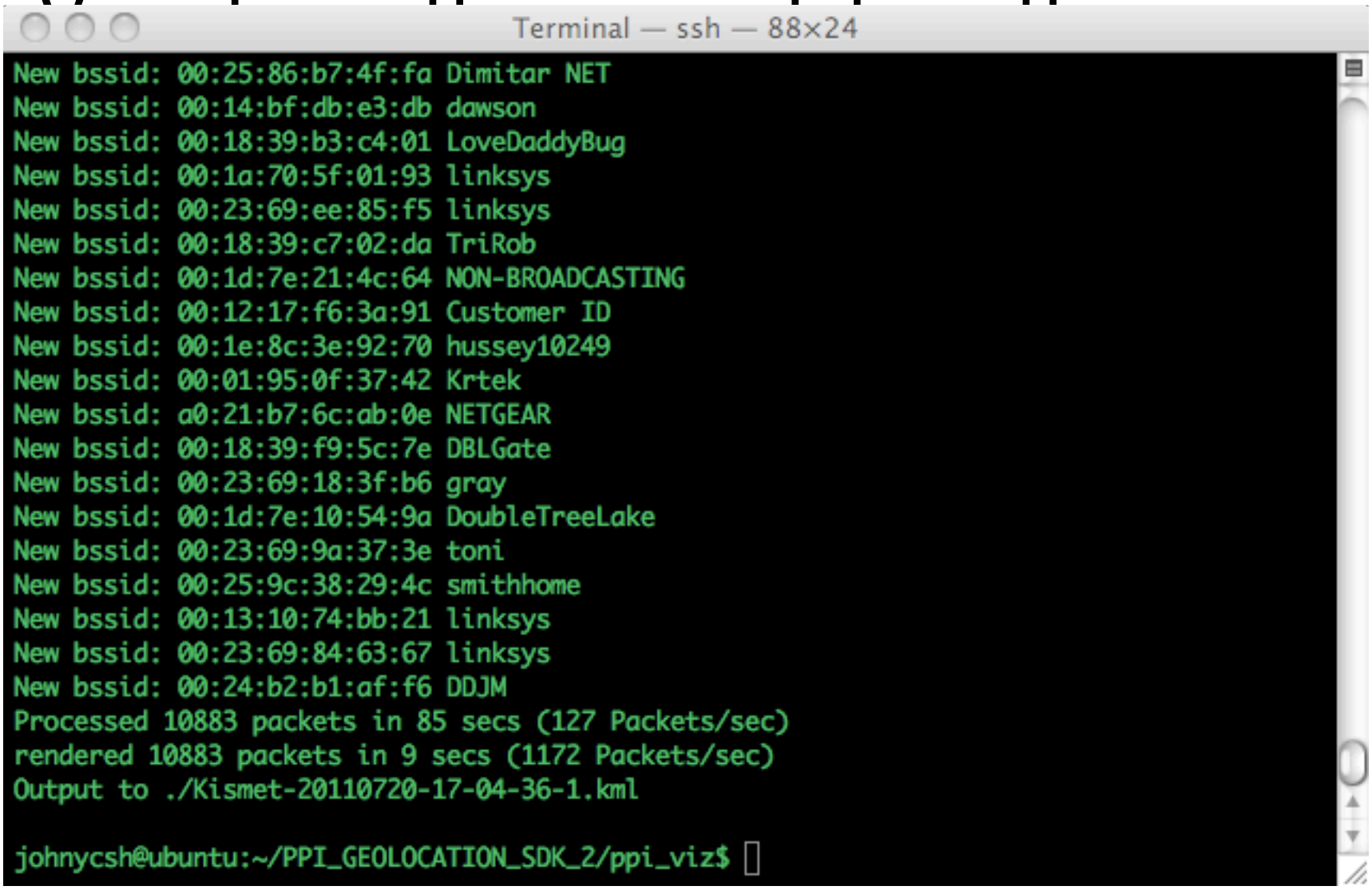
S = Sensor()

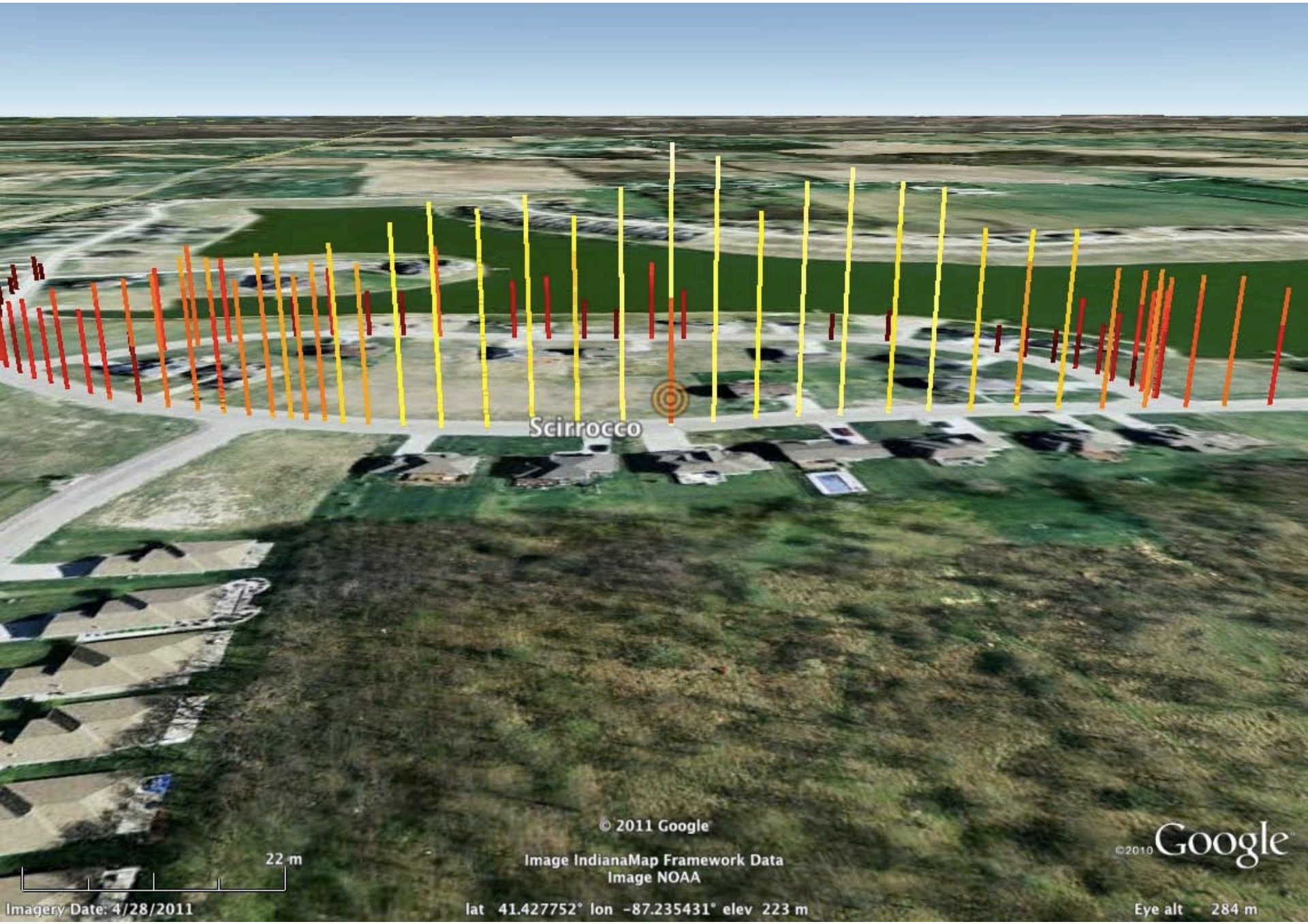

Terminal — ssh — 80×24
>>> S=Sensor()
>>> S.SensorType="Velocity"
>>> S.Val_T=20.0
PPI version 0, 239 bytes
Version: 0
Flags: 0x00
Header length: 239
DLT: 105
GPS: Lat:40.787743 Lon:-73.971210
Vector: (Forward) (DOT) (Front_of_veh) Pitch:10.000000 Heading:22.500000 (VehicleVec)
Sensor: Velocity 20.000000 Meters/sec
Header revision: 2
Header pad: 0
Header length: 14
Present: 0x00000021
SensorType: 1 Velocity
Val_T: 20 Meters/sec

Okay that was cool, But..

- I was told there would be pretty pictures!

Kismet-date.nettxt


Terminal — ssh — 88×24
New bssid: 00:25:86:b7:4f:fa Dimitar NET
New bssid: 00:14:bf:db:e3:db dawson
New bssid: 00:18:39:b3:c4:01 LoveDaddyBug
New bssid: 00:1a:70:5f:01:93 linksys
New bssid: 00:23:69:ee:85:f5 linksys
New bssid: 00:18:39:c7:02:da TriRob
New bssid: 00:1d:7e:21:4c:64 NON-BROADCASTING
New bssid: 00:12:17:f6:3a:91 Customer ID
New bssid: 00:1e:8c:3e:92:70 hussey10249
New bssid: 00:01:95:0f:37:42 Krtek
New bssid: a0:21:b7:6c:ab:0e NETGEAR
New bssid: 00:18:39:f9:5c:7e DBLGate
New bssid: 00:23:69:18:3f:b6 gray
New bssid: 00:1d:7e:10:54:9a DoubleTreeLake
New bssid: 00:23:69:9a:37:3e toni
New bssid: 00:25:9c:38:29:4c smithhome
New bssid: 00:13:10:74:bb:21 linksys
New bssid: 00:23:69:84:63:67 linksys
New bssid: 00:24:b2:b1:af:f6 DDJM
Processed 10883 packets in 85 secs (127 Packets/sec)
rendered 10883 packets in 9 secs (1172 Packets/sec)
Output to ./Kismet-20110720-17-04-36-1.kml
johnycsh@ubuntu:~/PPI_GEOLOCATION_SDK_2/ppi_viz$


Scirrocco
© 2011 Google
Image IndianaMap Framework Data
Image NOAA
©2010 Google
22 m
Imagery Date: 4/28/2011
lat 41.427752° lon -87.235431° elev 223 m
Eye alt 284 m

Okay that was cool, But..

- You've been working on this for a year and all you have are some bar graphs in GE?

Say hello to my little friend!

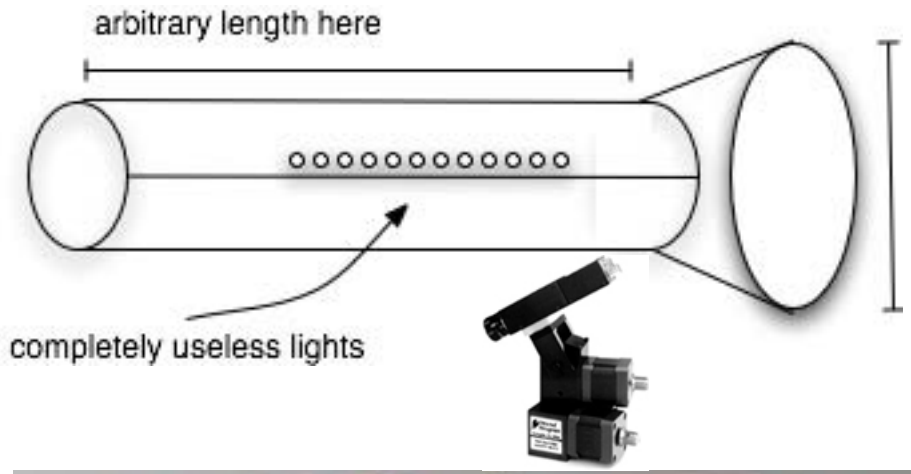
2008 Cobalt SS

- 260 HP Supercharged Ecotec Engine
- Ridiculous wing (+5 HP)
- Sunroof optional

Directed Perceptions Servo

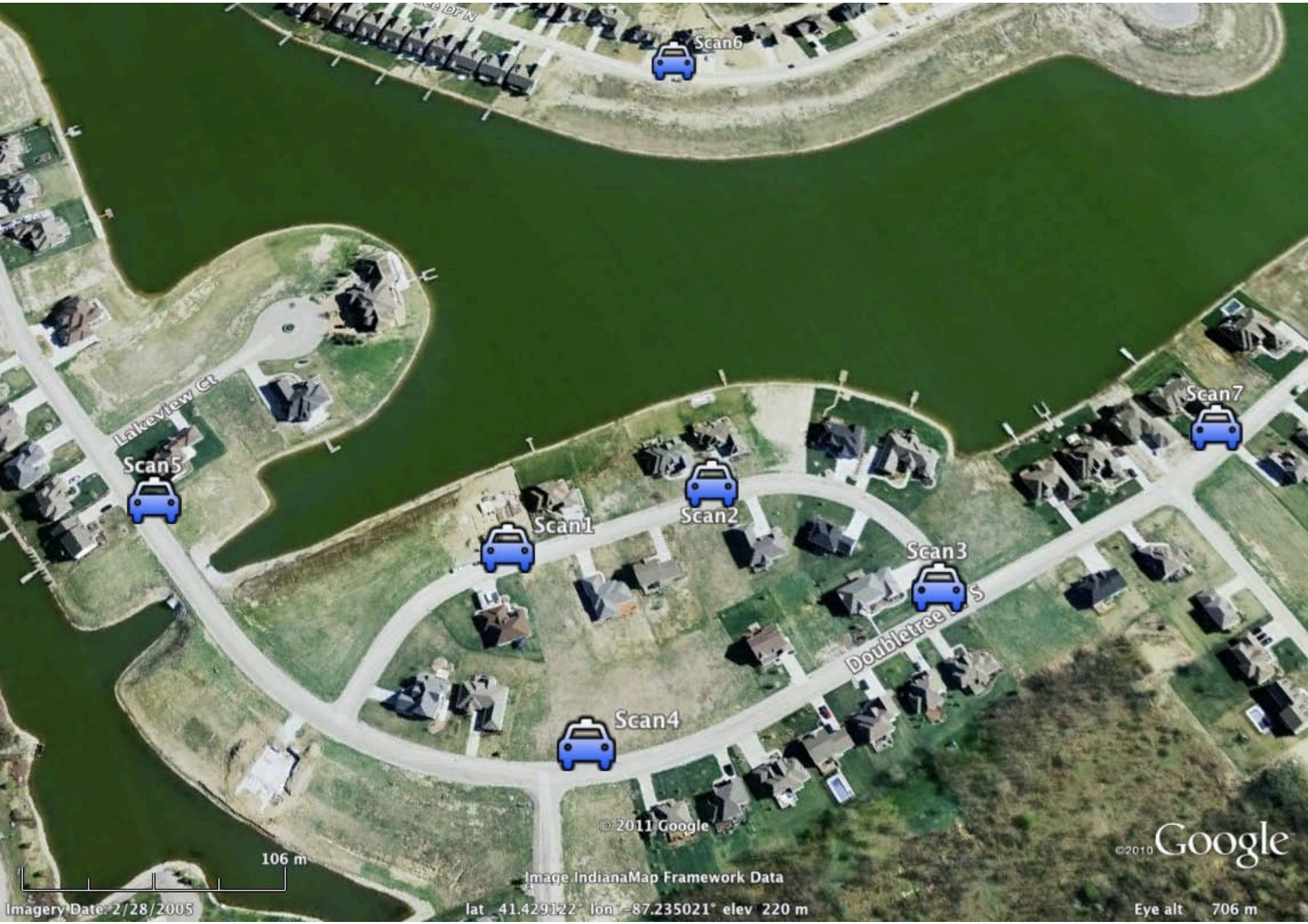
- 360° Pan
- +/- 30° Tilt
- 1 [illegible] software controlled

WiFi Cannon



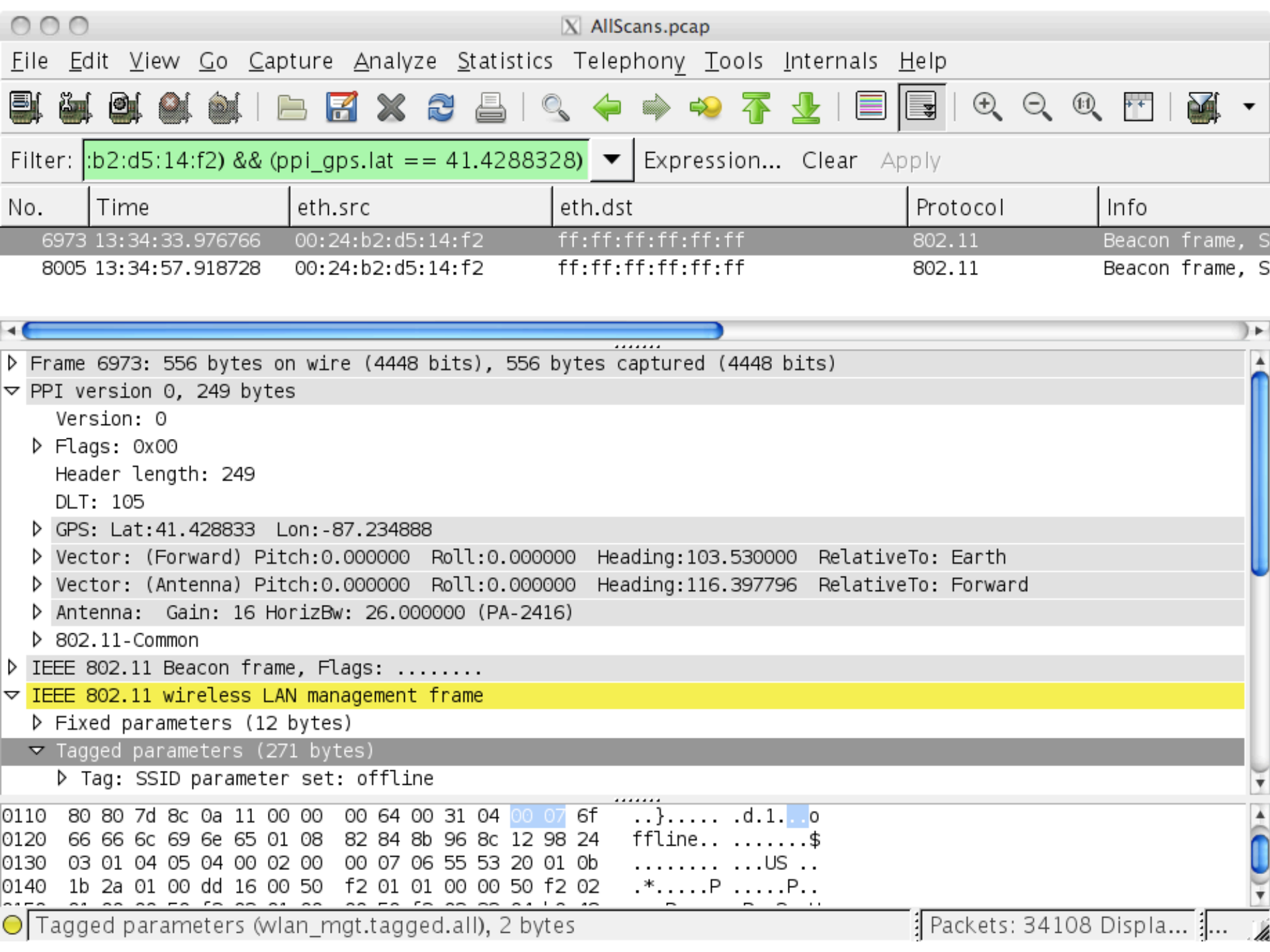
- 8 dBi antenna
- 30° horizbw

Servo Bot rollout!

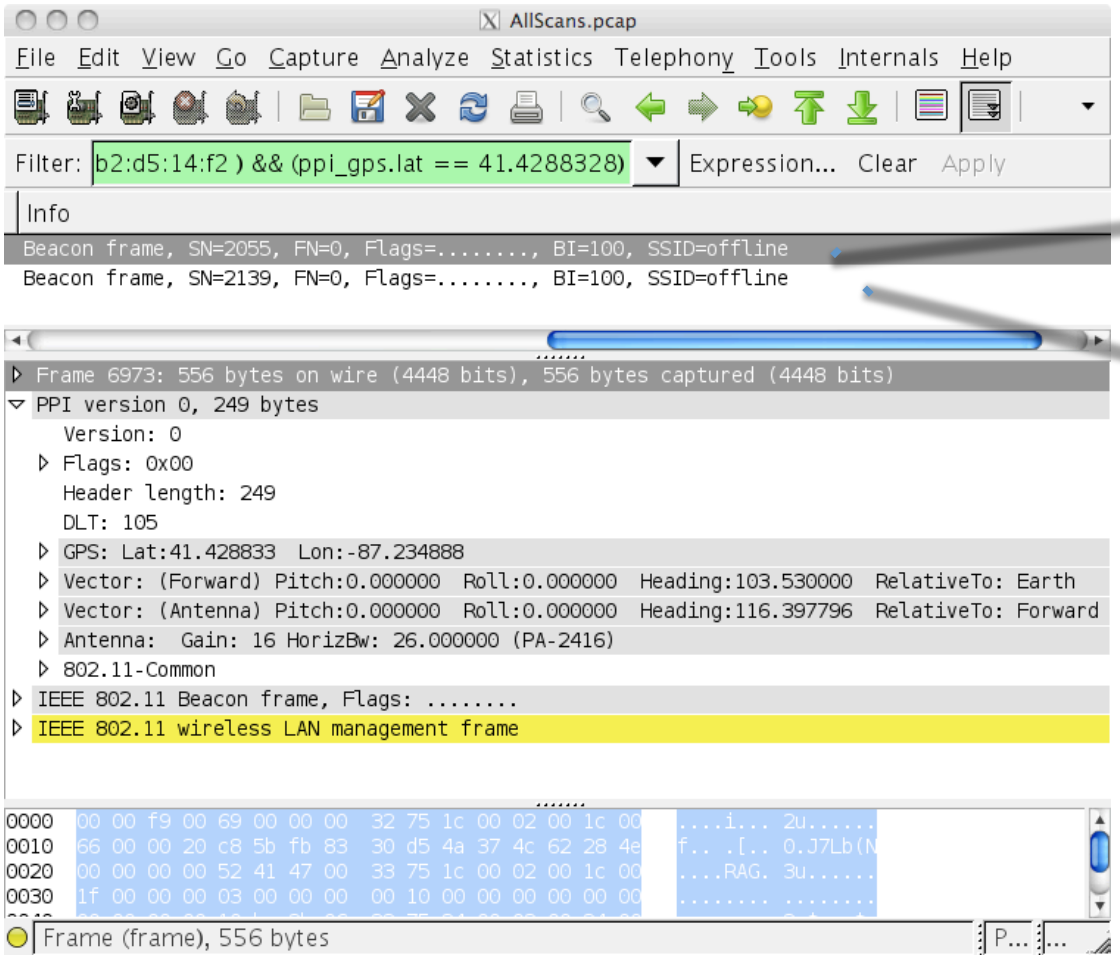

Scan6
Lakeview Ct
Scan5
Scan1
Scan2
Scan3
Scan4
Scan7
Doubletree
© 2011 Google
©2010 Google
106 m
Image IndianaMap Framework Data
Imagery Date: 2/28/2005
lat 41.429122° lon -87.235021° elev 220 m
Eye alt 706 m

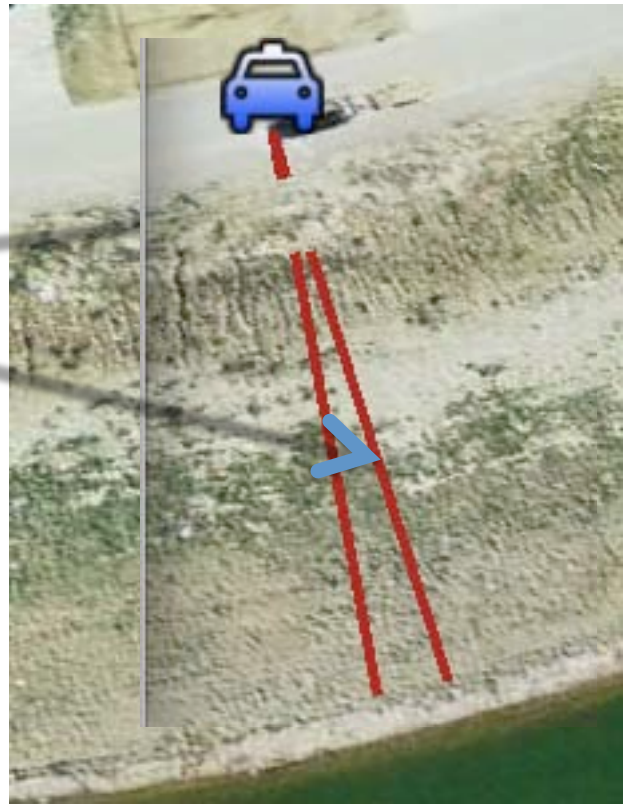

offline (triangulated)
Image IndianaMap Framework Data
© 2011 Google
55 m
Imagery Date: 2/28/2005
lat 41.429356° lon -87.234497° elev 218 m
Eye alt 450 m
Google

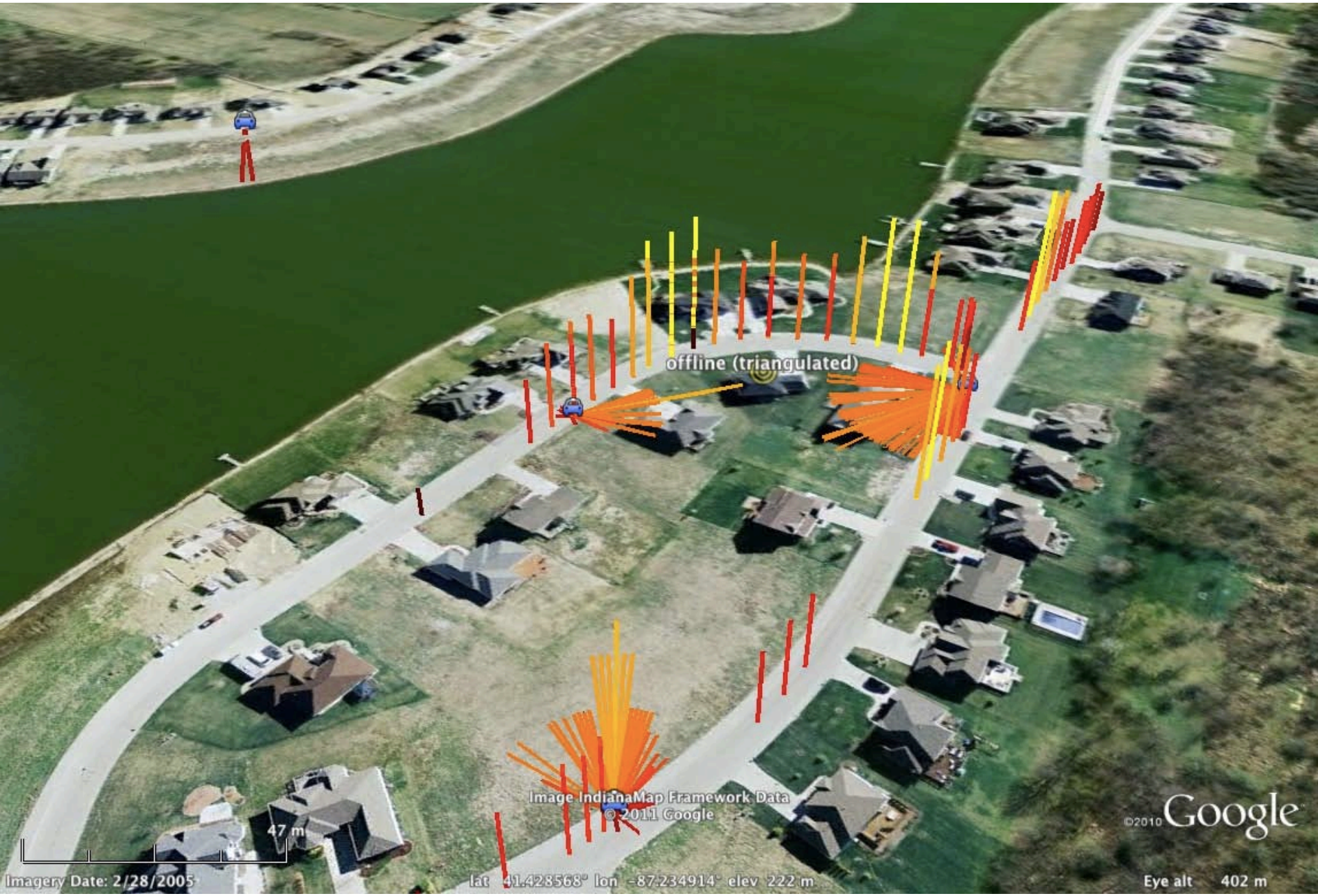

These two packets
Bounced off
this guys house.
offline (triangulated)
Image IndianaMap Framework Data
© 2011 Google
©2010 Google
44 m
Imagery Date: 2/28/2005
lat 41.429262° lon -87.234836° elev 218 m
Eye alt 398 m

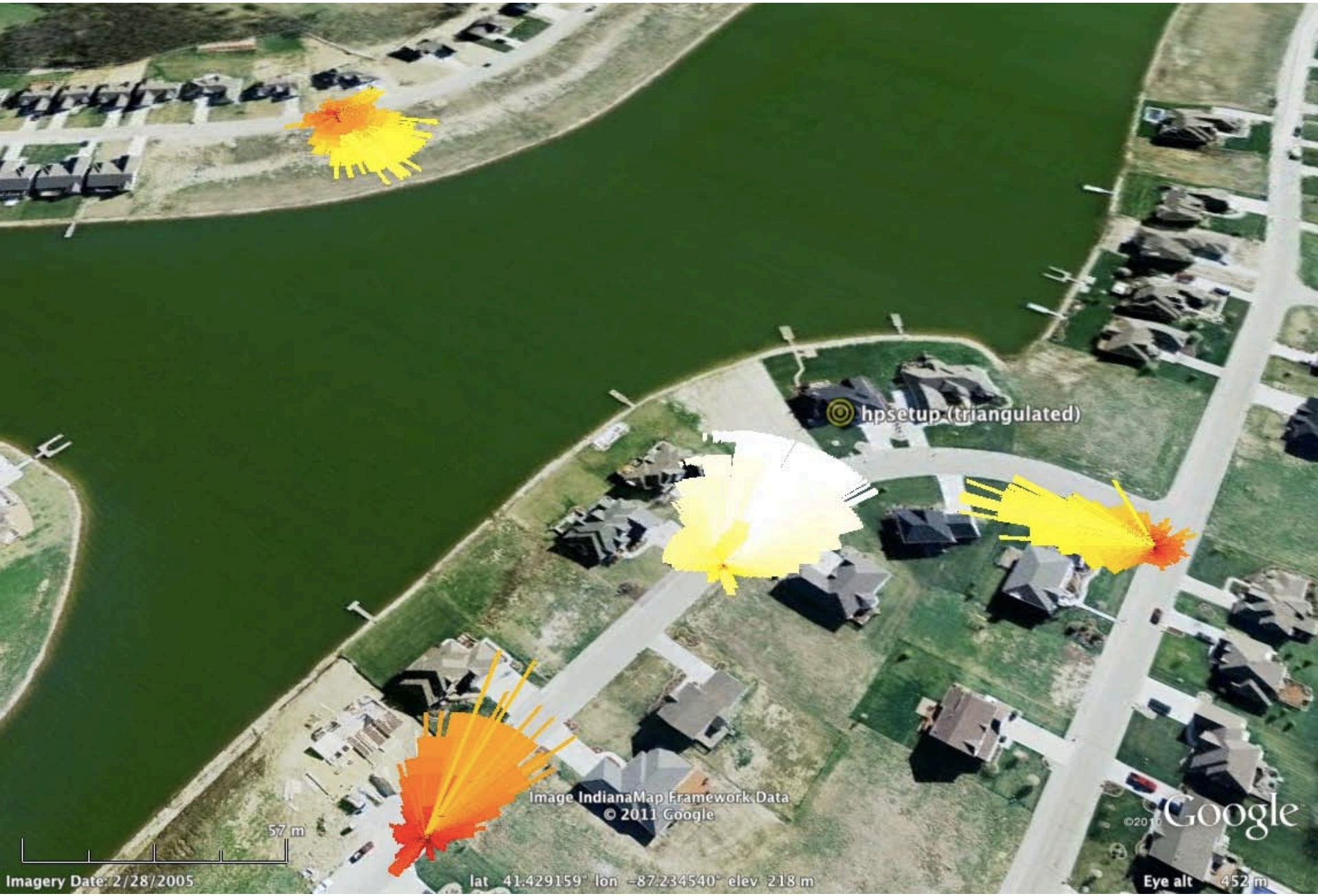

AllScans.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: :b2:d5:14:f2) && (ppi_gps.lat == 41.4288328) Expression... Clear Apply
No. Time eth.src eth.dst Protocol Info
6973 13:34:33.976766 00:24:b2:d5:14:f2 ff:ff:ff:ff:ff:ff 802.11 Beacon frame, S
8005 13:34:57.918728 00:24:b2:d5:14:f2 ff:ff:ff:ff:ff:ff 802.11 Beacon frame, S
Frame 6973: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits)
PPI version 0, 249 bytes
Version: 0
Flags: 0x00
Header length: 249
DLT: 105
GPS: Lat:41.428833 Lon:-87.234888
Vector: (Forward) Pitch:0.000000 Roll:0.000000 Heading:103.530000 RelativeTo: Earth
Vector: (Antenna) Pitch:0.000000 Roll:0.000000 Heading:116.397796 RelativeTo: Forward
Antenna: Gain: 16 HorizBw: 26.000000 (PA-2416)
802.11-Common
IEEE 802.11 Beacon frame, Flags: ....
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Tagged parameters (271 bytes)
Tag: SSID parameter set: offline
0110 80 80 7d 8c 0a 11 00 00 00 64 00 31 04 00 07 6f ..}..... .d.1...o
0120 66 66 6c 69 6e 65 01 08 82 84 8b 96 8c 12 98 24 ffline.. ....$
0130 03 01 04 05 04 00 02 00 00 07 06 55 53 20 01 0b ....US ..
0140 1b 2a 01 00 dd 16 00 50 f2 01 01 00 00 50 f2 02 .*.....P .....P..
Tagged parameters (wlan_mgt.tagged.all), 2 bytes
Packets: 34108 Displa...

These two packets

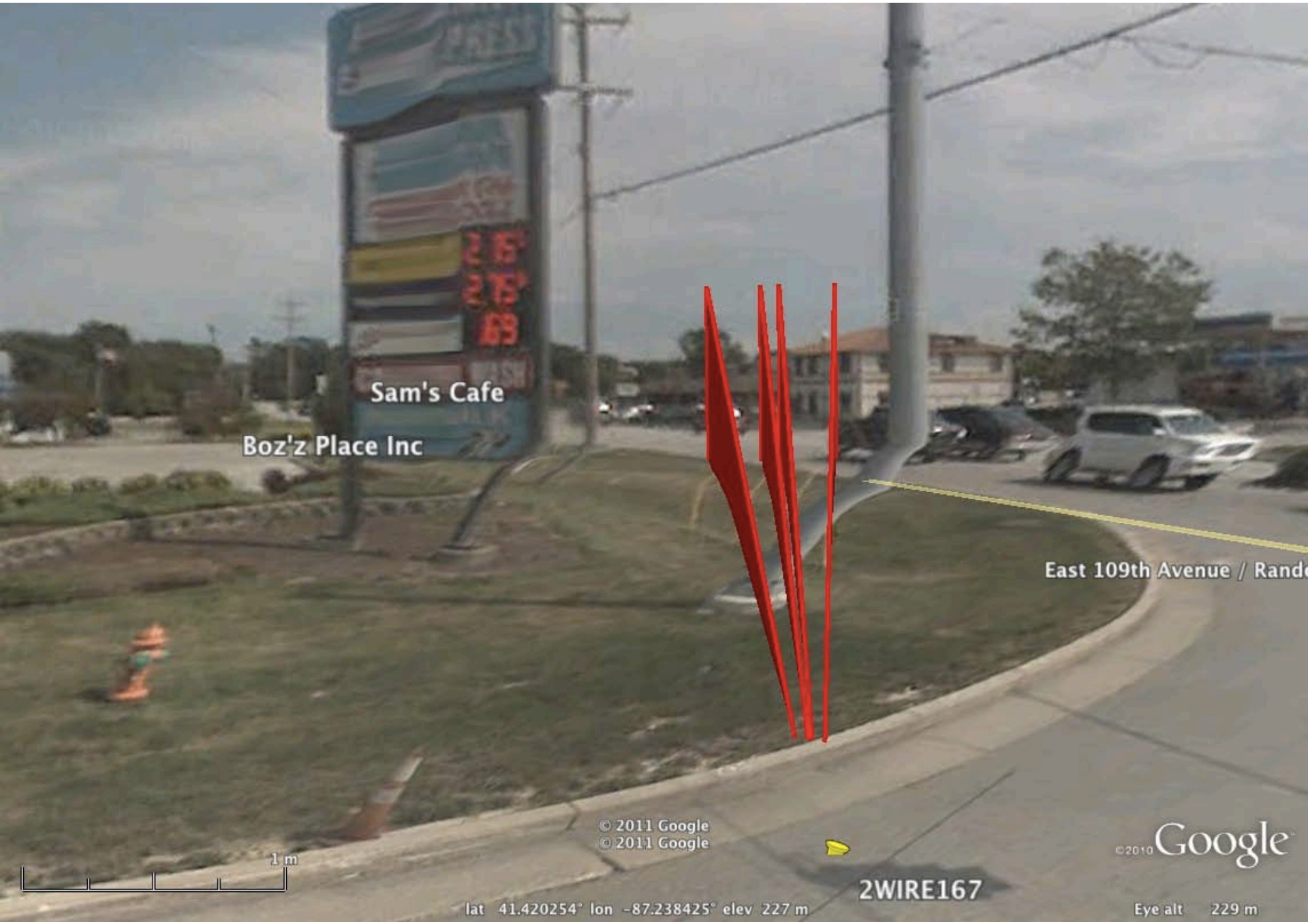





offline (triangulated)
Image IndianaMap Framework Data
© 2011 Google
©2010 Google
47 m
Imagery Date: 2/28/2005
lat 41.428568° lon -87.234914° elev 222 m
Eye alt 402 m


hpsetup (triangulated)
Image IndianaMap Framework Data
© 2011 Google
57 m
Google
Imagery Date: 2/28/2005
lat 41.429159° lon -87.234540° elev 218 m
Eye alt 452 m


Scirrocco (triangulated)
Image IndianaMap Framework Data
© 2011 Google
©2010 Google
40 m
Imagery Date: 2/28/2005
lat 41.428055° lon -87.234888° elev 223 m
Eye alt 388 m


Sam's Cafe
Boz'z Place Inc
East 109th Avenue / Rande
© 2011 Google
© 2011 Google
1 m
2WIRE167
©2010 Google
lat 41.420254° lon -87.238425° elev 227 m
Eye alt 229 m

Okay, That *was* cool

- But nothing! It was cool.
- But where is all this code?
  - Wireshark: merged.
  - Scapy: merged (/contrib)
  - Kismet: merged
  - SDK (http://www.govcomm.harris.com/solutions/products/csp-white-papers.asp)

Get The SDK:

- SDK Includes:
  - C++ Library for reading/writing tags (Linux/Windows)
  - Python state machine that illustrates proper interpretation
  - Ppi-viz-dev: Developer visualizer
  - Ppi-viz: Basic signal strength visualizer
  - http://www.govcomm.harris.com/solutions/products/csp-white-papers.asp

Supporting vendors

HARRIS

PRAXIS ENGINEERING

SRT Wireless

WIRESHARK

Scapy python

KISMET

You're Welcome.

Thanks to

- Charlie, Jody, Tyler, Megan, Manny ,Dragorn, Phillipe, Gerald, R15, Pandy, Craig, shegget, Kiersten, etc.
- Nick *kind-of-a-big-deal* Petrillo + Pusscat
- My (intentionally-vague) friend Josh.
- HD, skape, rjohnson + the rest of uninformed and 219.