GeoLocation of Wireless Access Points & "Wireless GeoCaching"

Presented By: Rick Hill

The Problem: 802.11b Geo-Location

- Researchers have documented at least 4 Techniques for Geo-Location of Wireless Access Points (APs)[1]
- Netstumbler doesn't Geo-Locate –> It simply gives the Driver's GPS Position.

- Netstumbling & GeoCaching Compared:

  Wardrivers don't locate AP's with the same intent that GeoCachers find Caches; they're content to simply find New Networks. GeoCaching, in contrast, is all about Precise Location…

- What if we could combine the two?

  Consider a New Sport: "Wireless GeoCaching"

What's GeoCaching?

- Wikipedia:
  - **GeoCaching** is an outdoor treasure-hunting game in which the participants use a Global Positioning System (GPS) receiver or other navigational techniques to hide and seek containers (called "GeoCaches" or "caches").
  - Typical Cache - a small waterproof container containing a logbook & "treasure," usually toys or trinkets of little monetary value.

Project Goals

- Our Goals:
  - Build an Automated 802.11b Tracking Device using OTS Components
  - Test Device in a Controlled Environment (the Lake)
  - Participate in “Wireless GeoCaching” Game: Geo-Locate hidden AP’s & Caches using Netstumbler and Radio Direction Finding (RDF) techniques.

Project Concept

- Of the 4 DF Methods ->
  - Received Signal Strength Indication (RSSI) + Angle of Arrival (AOA) + Triangulation is easiest to Implement
- Our Platform: Sea Ray Boat
- Location: Lake Anna, VA
- Equipment:
  - Hardware - 15 Db YAGI Antenna, Stepping Motor & Controller, Digital Compass, GPS, Dell Laptop
  - Software – XP, Netstumbler 0.4.0, Visual Basic 5.0

Agenda

- Background – Why is Wireless Tracking so Hard???
- 4 Techniques – Advantages / Disadvantages
- Building the Tracker (HW/ SW)
- Static Test with a Known AP
- Wireless GeoCaching
- Accuracy compared to other Techniques

Why So Difficult?

- Spread Spectrum Technology - DSSS hops many x/sec. and covers a 22 Mhz Bandwidth
- Spread Spectrum designed by the Military to look like Background Noise (Very Low Power)
- Must wait on Beacon Frames & Probe Frames
- 2.4 Ghz Radio Propagation Subject to:
  - Multipath Inteference
  - Scattering Interference, (Trees & Buildings)

4 DF Techniques

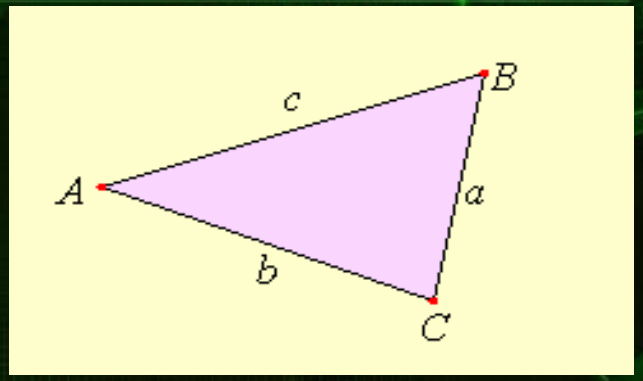
- Radio Direction Finding (RDF)
- Received Signal Strength Indication (RSSI) + Angle of Arrival (AOA) + Triangulation
- Doppler Direction Finding
- Time of Arrival (TOA) & Time Difference of Arrival (TDOA)

Radio Direction Finding (RDF)

- Very Simple – Point a directional antenna in the proper direction & Maximize Signal
- Advantages:
  - Low Cost
  - Can be done Manually (aim the Cantenna.) Duh!
- Disadvantages:
  - Accuracy limited to Antenna Beamwidth & Rotor System Mechanics
  - Can't Geo-Locate –> Simply guides you in the Right Direction (Sort of)

RSSI + AOA + Triangulation

- A step up from simple RDF: Given >= 2 locations (fixes), target position follows by Triangulation:



$$\frac{\sin A}{a} = \frac{\sin B}{b} = \frac{\sin C}{c}$$

Law of Sines

- AP Target located @ A.
- Boat takes 2 Fixes, giving angles B & C.
- Side a = GPS distance B -> C.
- Distance to Target follows from the Law of Sines.

Doppler Direction Finding (DDF)

- DDF systems employ 4 + Antennas & use the Doppler effect to derive AOA & Distance



Advantages:

Better for moving Targets

More accurate Speed Calculation

Disadvantage:

Equipment is very expensive: Professional 2.4 Ghz RDF rig costs approx. $3,000

Time of Arrival (TOA) & Time Difference of Arrival (TDOA)

- Similar to Doppler: Electronically calculated from Multiple Antennas
- Examples:
  - Cellular Tower Signal Location
  - People Tracking via RFID & WiFi (**AeroScout.com**)
  - CISCO 2710 Wireless Location Appliance
- Advantage:
  - Excellent with known Cell Towers or AP's
- Disadvantages:
  - May not be as Accurate
  - Requires Existing Infrastructure

Building the Wireless Tracker

- Our Tracking Device will look a lot like the Radar Antennas seen on Navy Ships
- It Consists of:
  - Stepper Motor for 360 deg. Rotation (1)
  - Stepping Motor Controller (1)
  - Laser Pointer (1)
  - Miniature 15 Db. YAGI Antenna (1)
  - Mounting Pole and Plate - For mounting 7’ above the Boat Deck (1)
  - Digital Compass and GPS (1 each)
- Hardware shown next slide…

Building the Tracker - Hardware





Building the Wireless Tracker cont'd

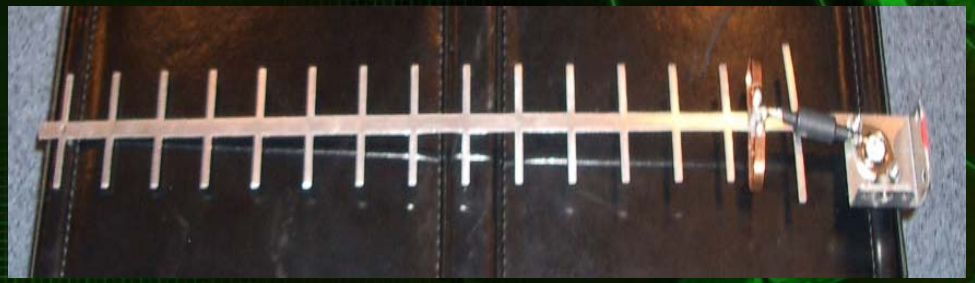
- First: The stepper motor must be mounted on a stable, flat surface. For our project this is a 7" x 7" square LEXAN sheet. LEXAN sheet is held 2.5" above the Boat table by 4 Hex Bolts
- Drill 4 holes for motor mount & 4 holes for the LEXAN stepper motor "tabletop"





Building the Wireless Tracker cont'd

- 2nd: Mount the Antenna with ½" aluminum strip to Stepping Motor shaft. Note Brass coupler w/ 2 set screws that mount directly to the motor

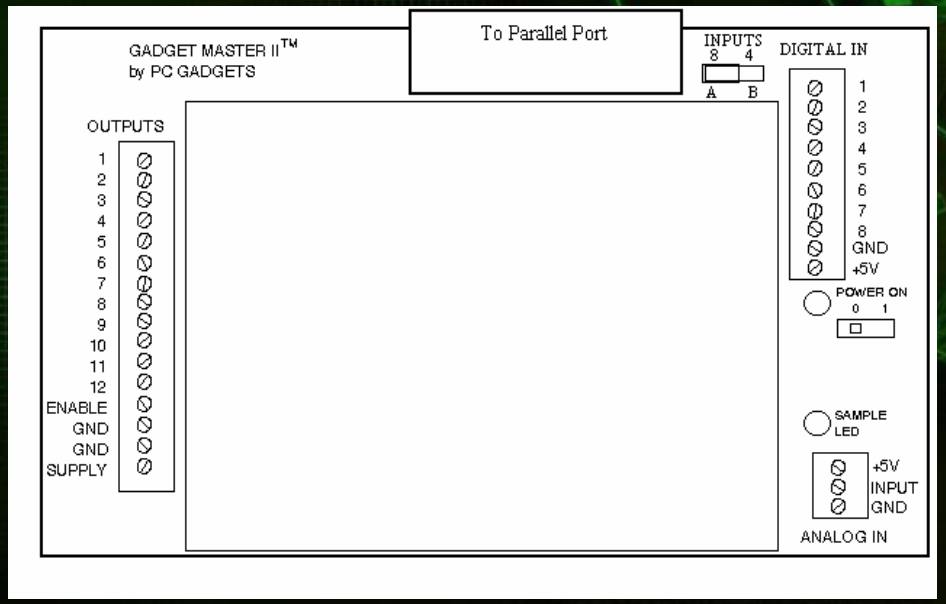


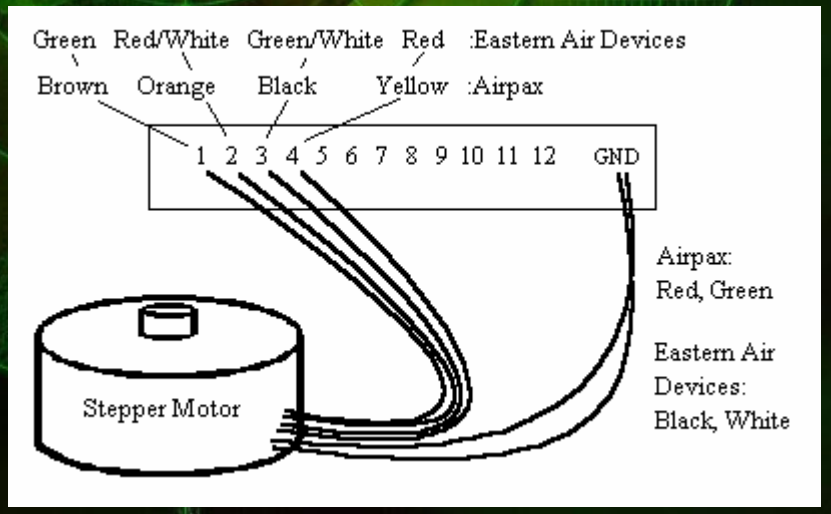




Building the Wireless Tracker cont'd

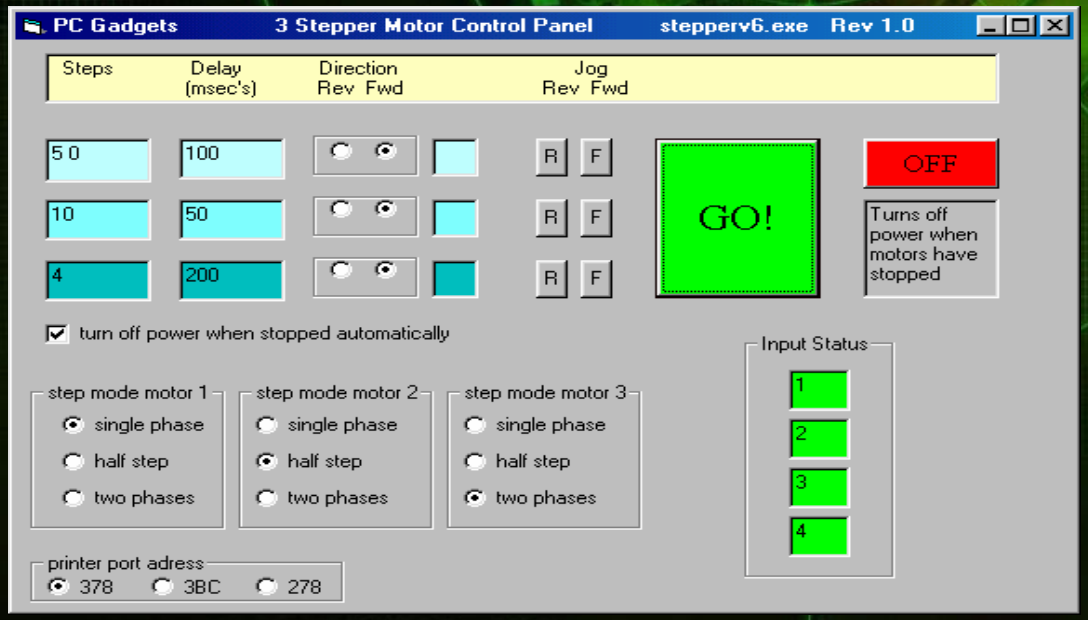
- Third: Hook up the parallel printer (control) cable to the Laptop. Carefully wire the Stepper motor to the Control Board as shown below. Use Outputs 1-4 for the 4 phases… Note there are a total of 6 wires on this UniPolar Motor (5 & 6 go to Ground)





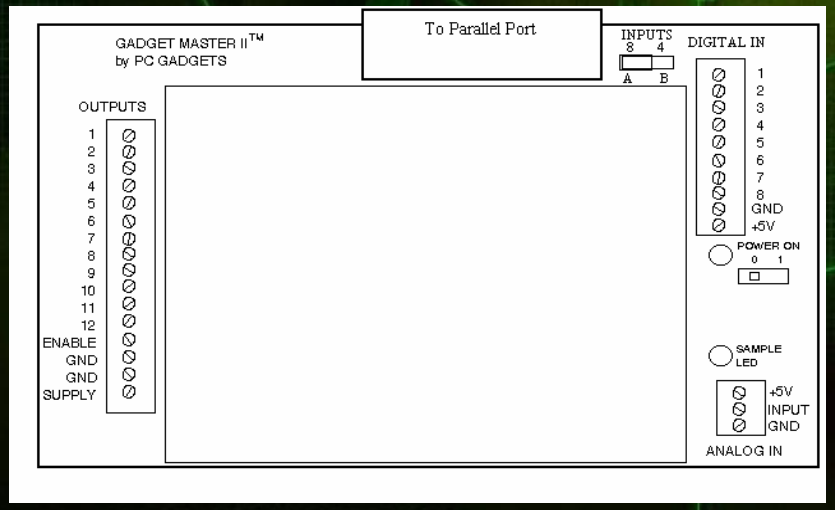
Building the Wireless Tracker cont'd

- Fourth: Test the stepping Motor & verify proper operation with the included Program StepperV6.EXE. Note: Our motor steps @ 7.5 degrees/ step. So, 48 steps = 1 Revolution = 1 Compass Rose. Screen Shot:



Building the Wireless Tracker cont'd

- Final Step: Mount the Compass & (optional) Laser Pointer just above and pointing in exactly the same direction as the YAGI antenna. Connect between Output 12 and GND of the Control Board.
- The Laser pointer can be used at night to Illuminate Target AP & Direction once Max Signal Strength found.



Building the Wireless Tracker cont'd

- Finished Tracker Mounted on Sea Ray Boat:



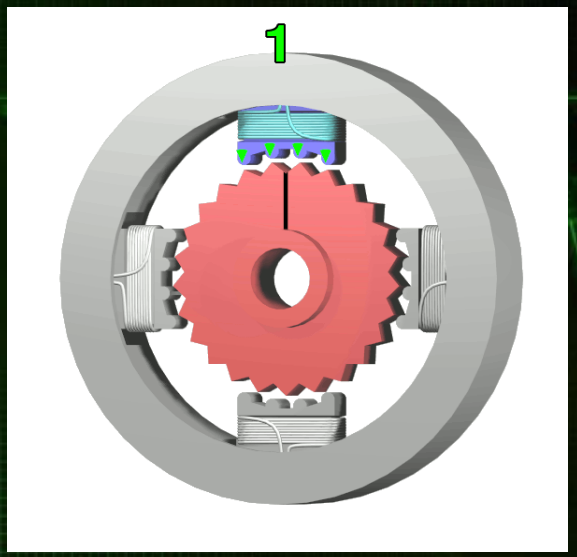
So, Why a Stepper Motor?

- Stepper Motors achieve very Precise Control of Angular Rotation
- No Feedback Loop Required
- Repeatable Control allows them to be used in floppy Disk Drives & Flatbed Scanners
- Can be salvaged from old Floppy drives & used in projects like this:

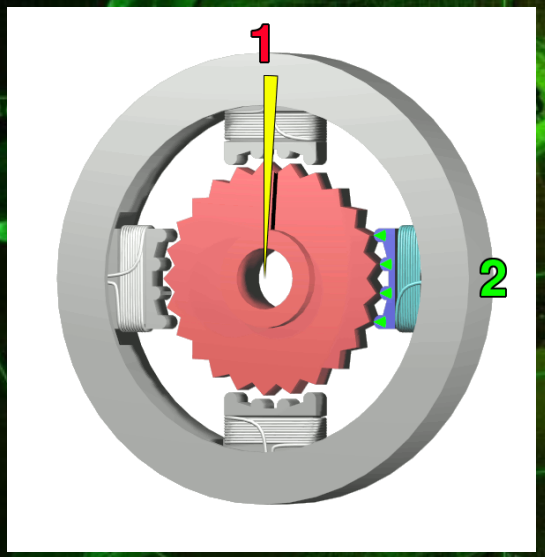
http://www.epanorama.net/circuits/diskstepper.html)

Stepper Motor Operation

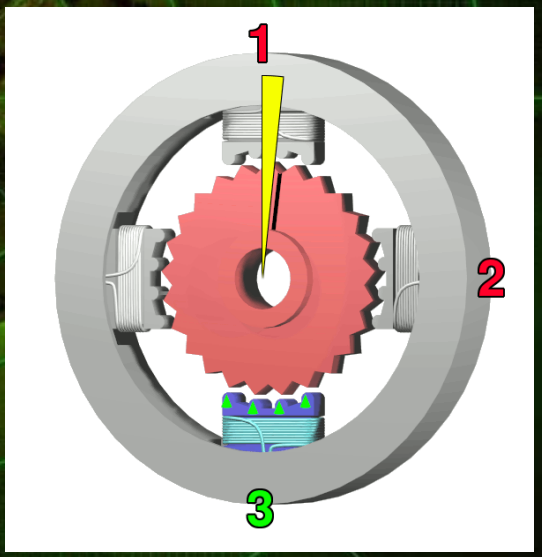
- Stepper Motors Rotate by Energizing Phases 1-4 in sequence. Source: Wikipedia



1- Magnet (1) is charged, attracting the topmost four teeth of sprocket.



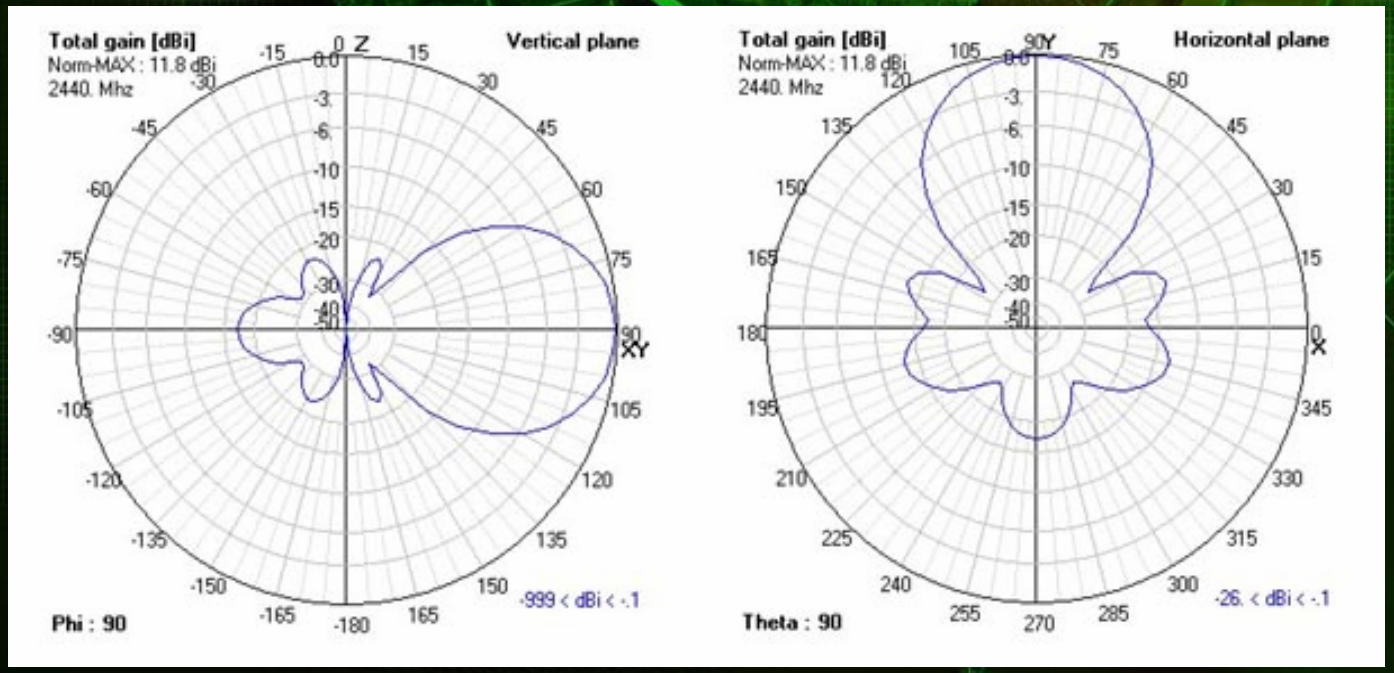
2- Magnet (1) turned off, Magnet (2) charged, pulling four teeth to the right. This results in a rotation of 3.6°



3- Magnet (2) off, (3) on, another 3.6 deg. rotation; Repeat for Phases 3-4…

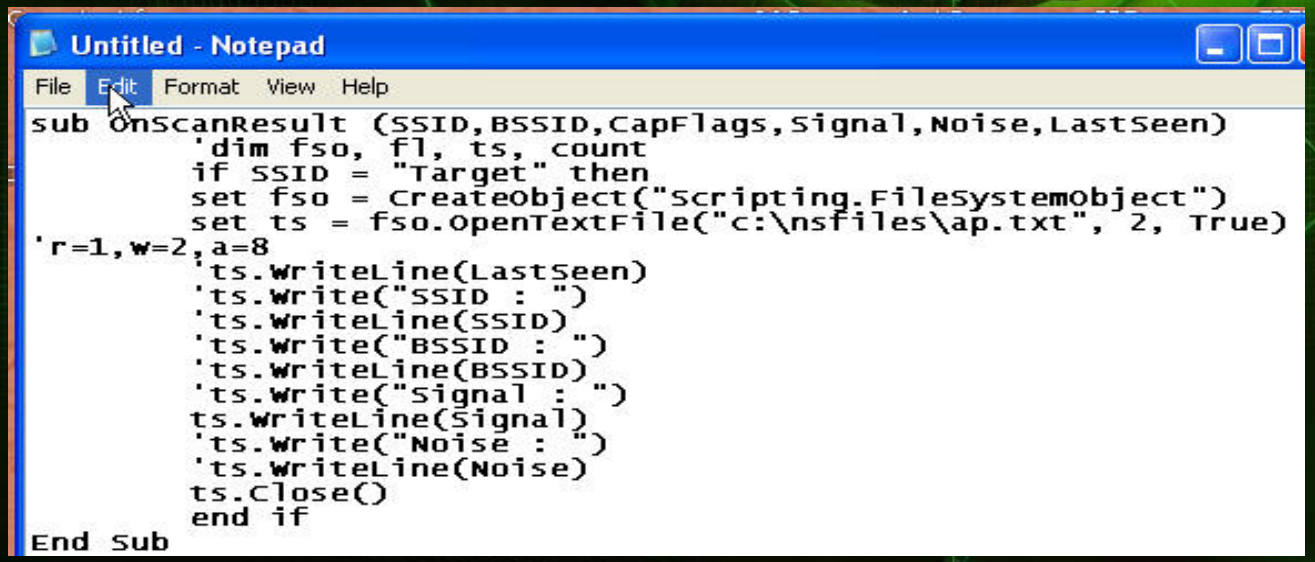
And the Antenna Selection?

- YAGI Antenna - Very Directional with High Front to Back ratio. Practically, this means no 180 deg. mistakes in Direction Finding (DF)
- Perfect Pattern for DF and weighs only 2.9 oz



Building the Tracker - Software

- PCMCIA Card – Senao 2511 with Prism Chipset
- Front-End Monitoring via Netstumbler 0.4.0
- Netstumbler Script: Given an AP SSID as the Target, Script captures the Signal Strength readings on Fast Scan & writes them to a file



Building the Tracker - Software

- Visual Basic: Back-end VB program controls both Stepper Motor rotation & getting Signal Strength from the NS Script file. (VB Code included as a separate file.)

```
FOR Step = 1 to 100                    ‘ 360 Degree Scan
If rev1.Value = False Then             ‘REVERSE OR FORWARD
    Call stepper_move(1, Val(steps1.Text))   ‘FORWARD
Else
    Call stepper_move(1, -Val(steps1.Text))   ‘REVERSE
End If
Next Step
```

Software – Programming Sequence

[1] Boat cruises looking for Target AP (Omni Antenna)

[2] VB Code displays Splash Screen "Target Acquired"

[3] Switch Input to Directional Antenna

[4] Scan 360 deg. in 7.5 deg. & 3.75 deg. Increments

[5] Average 3 RSSI readings / step

[6] Save MAX Reading & Angle

[7] Point Antenna @ Target, Illuminate Laser

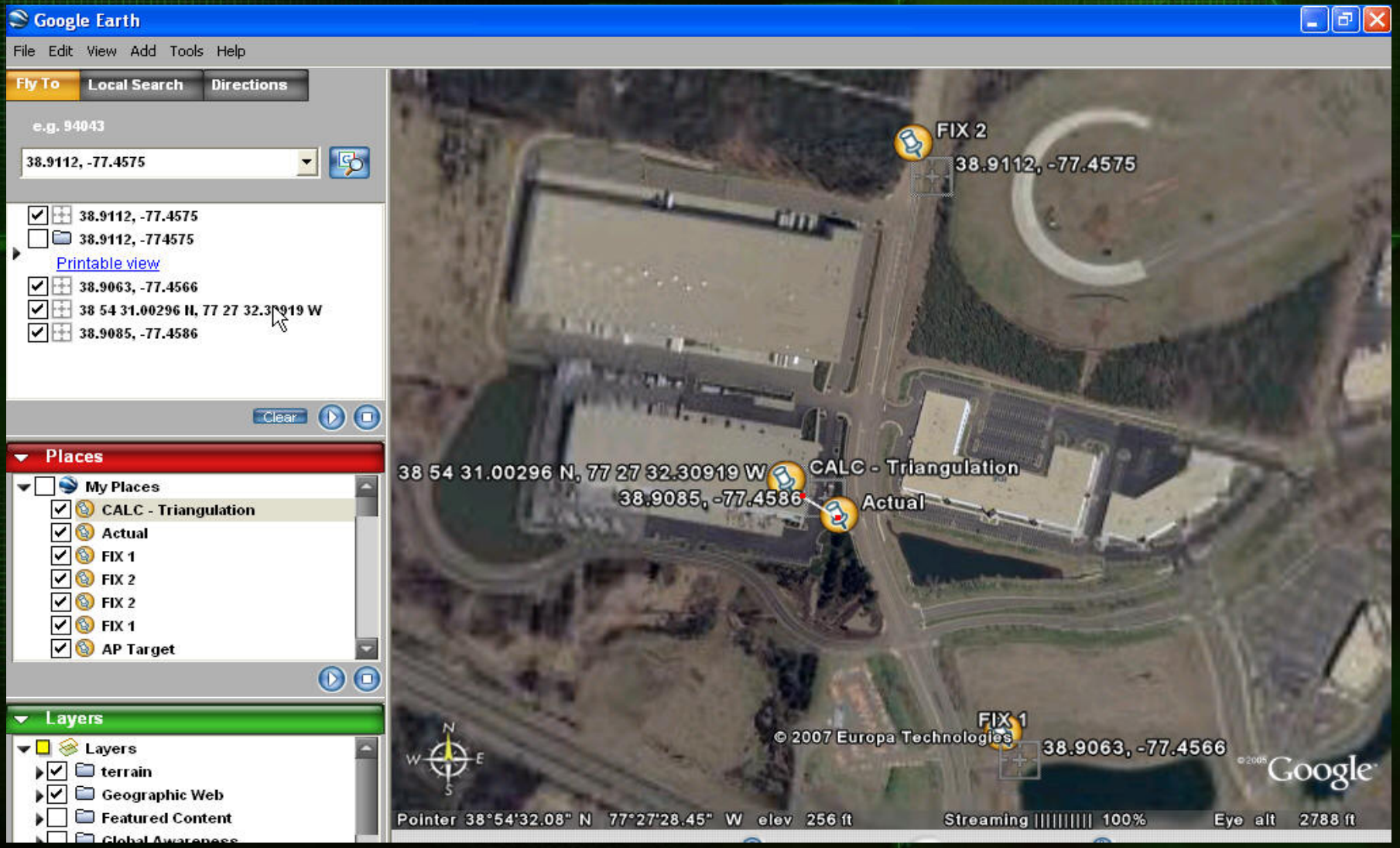
[8] Save GPS Coordinates, MAX Reading & Angle

[9] Calculate Target AP Position given 2 or more fixes

Sorties

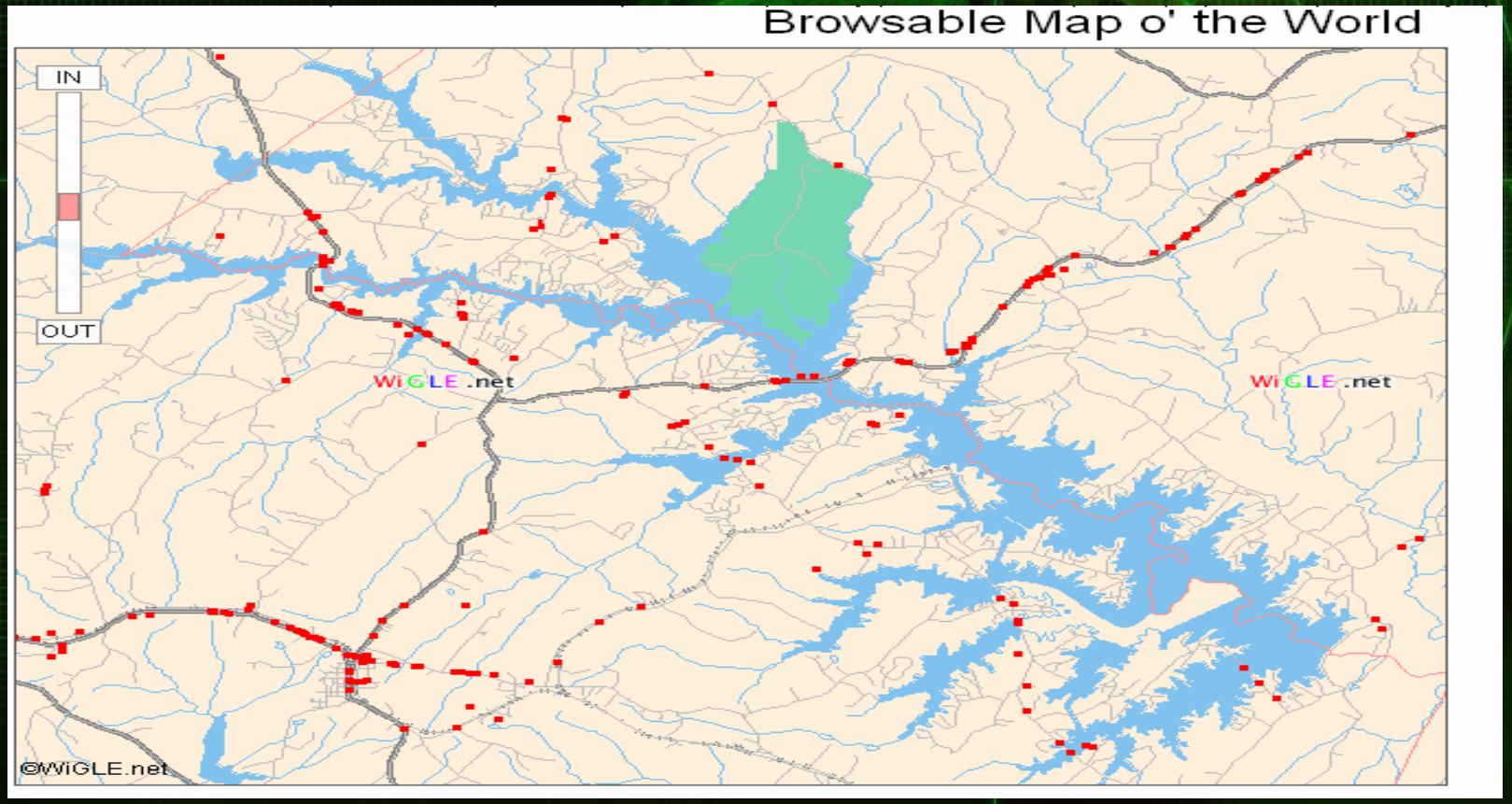
- 8 Sorties over 2 days:
  - 1 Static Test on Land
  - 4 against AP's with Known GPS Positions
  - 2 GeoCaching Games
  - 1 against an Unknown AP (Not visible LOS)

Static Test with a Land-Based AP



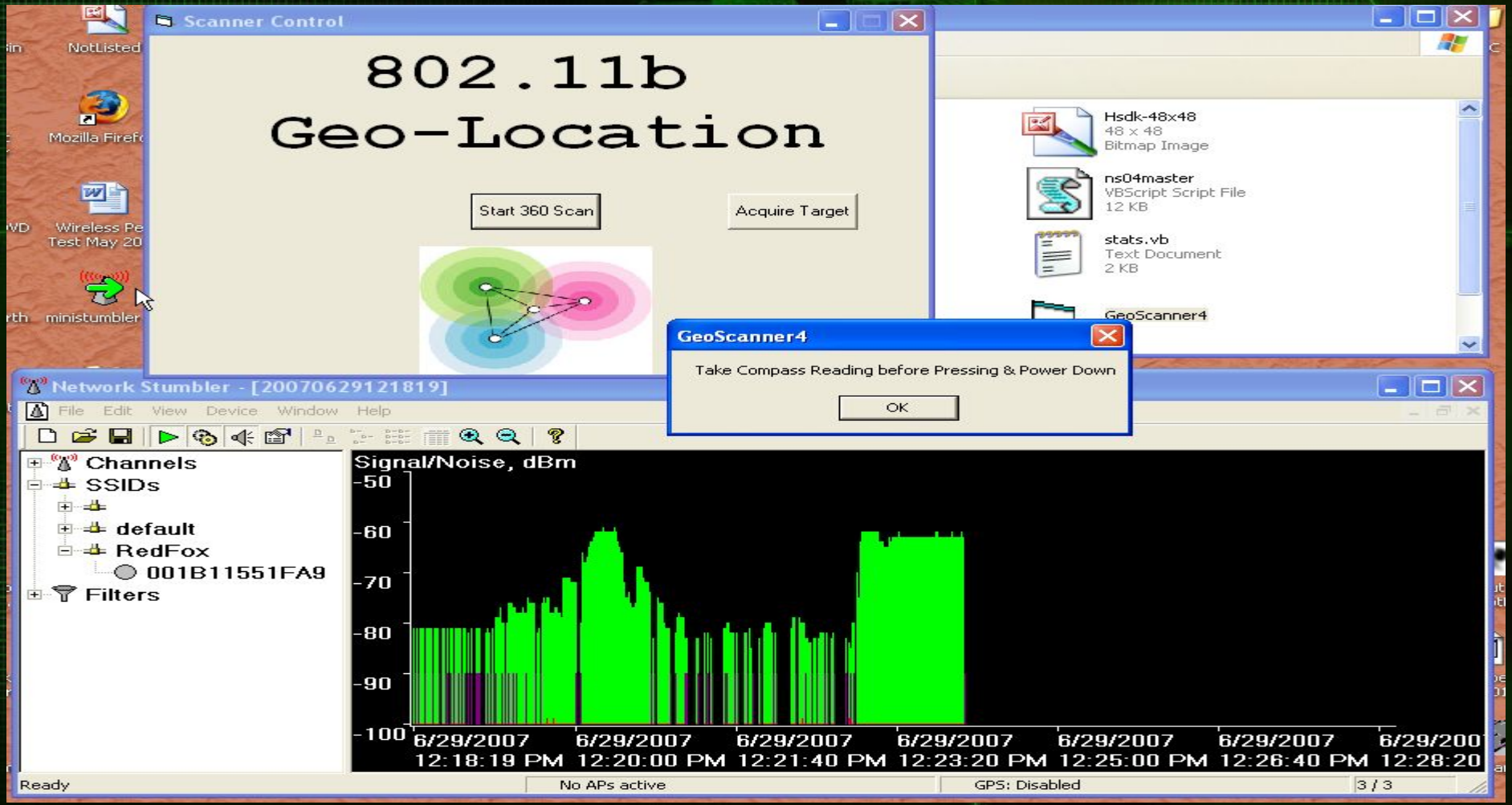
Lake Anna: WIGLE.Net

- AP's currently mapped @ Lake Anna, VA:



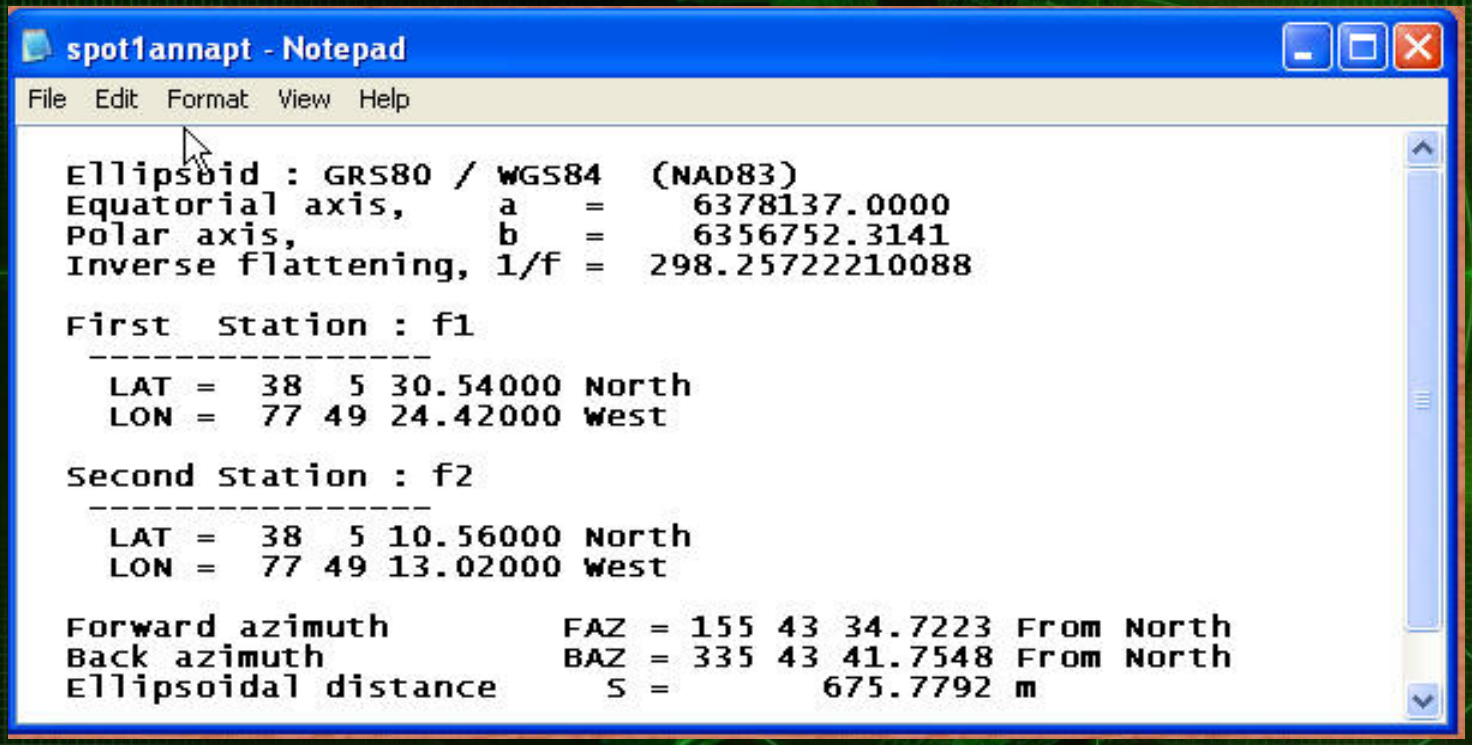
- Apparently, None of the Drivers own Boats, Go Figure?

Scan Result: Island1-F2



Note the Bell Curve & Signal Lock

Calculations – Inverse & Forward



INVERSE Program – Distance between 2 pts.
FORWARD Program – Distance & Angle to Target

http://www.ngs.noaa.gov/TOOLS/Inv_Fwd/Inv_Fwd.html

2nd Sortie – Anna Point Marina



Next: Wireless GeoCaching –> Searching for Hidden AP's

Wireless GeoCaching

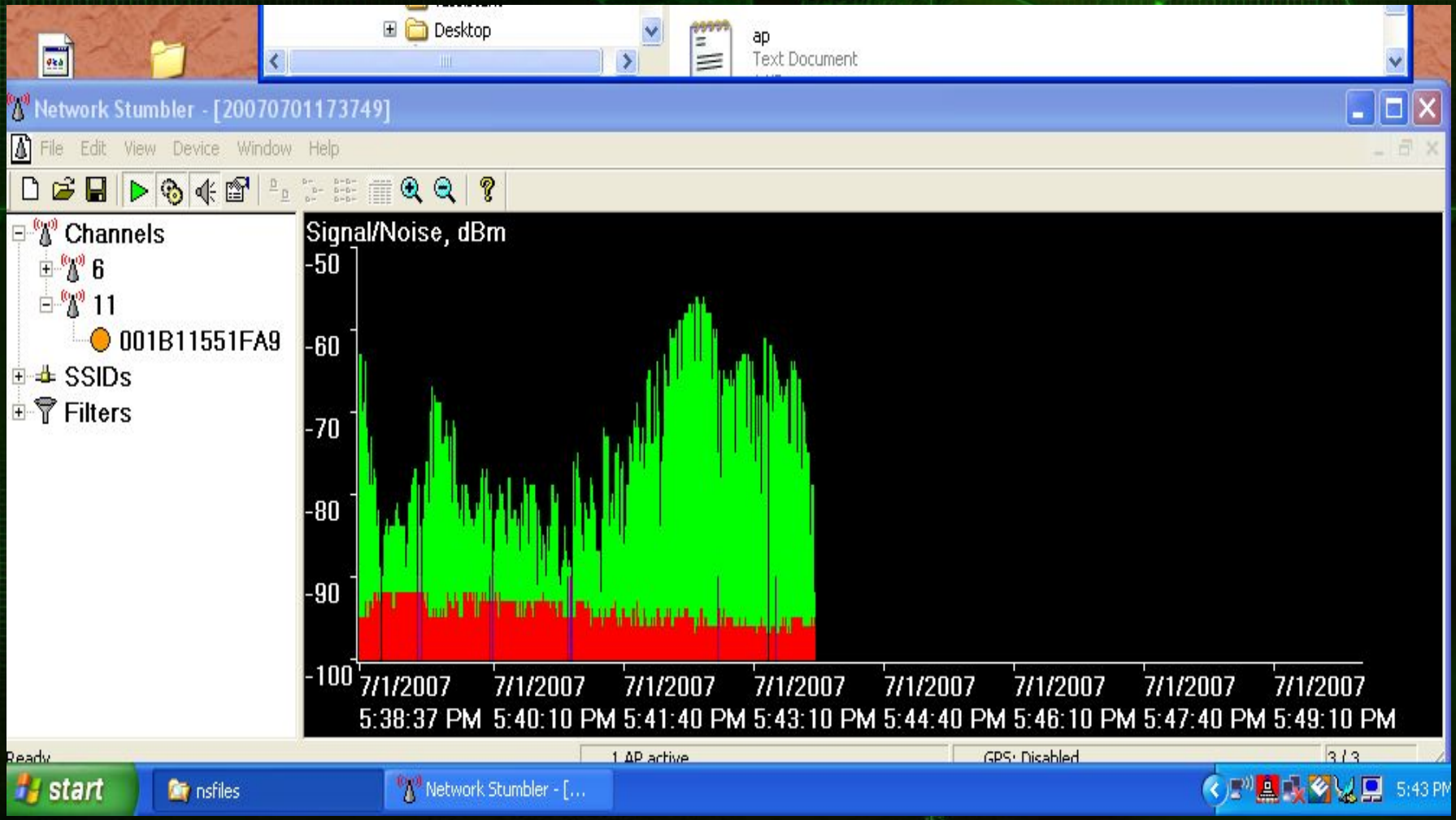
- Let the Games Begin!:
- Setup:
  - 2 teams of Two -
  - 1st Team drops a Black Bucket containing the AP & GeoCache Treasure on shore.
    - Rules: Within 100 ft. of shoreline & < 5 miles from the Marina
  - 2nd Team: Finds AP with the Scanner

Wireless GeoCaching

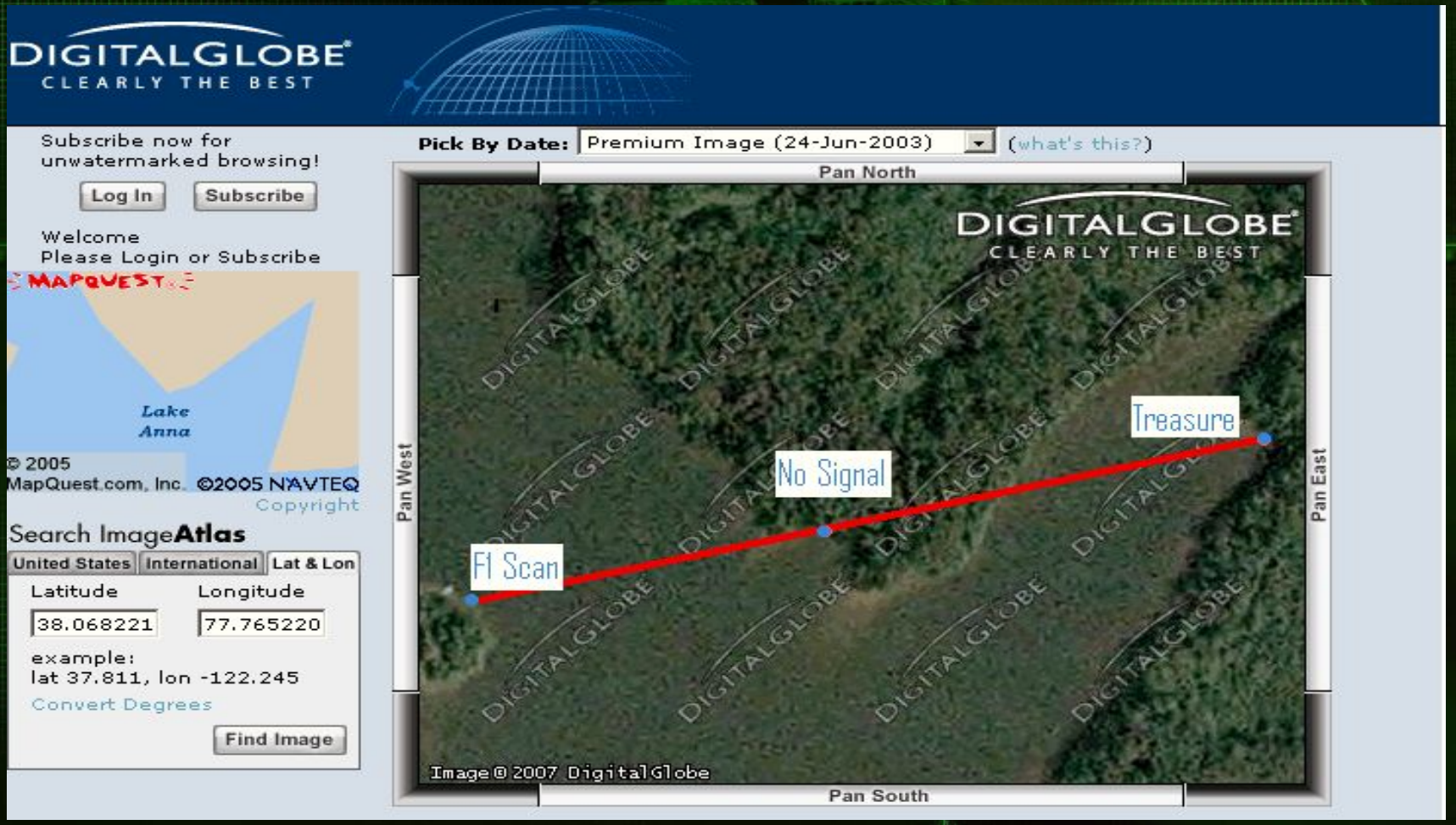
- Pictures / Video of Wireless GeoCaching
- Slide Show - ~ 5 min.

Picture Break

Sortie 7 - GeoCache Found: SilverFox

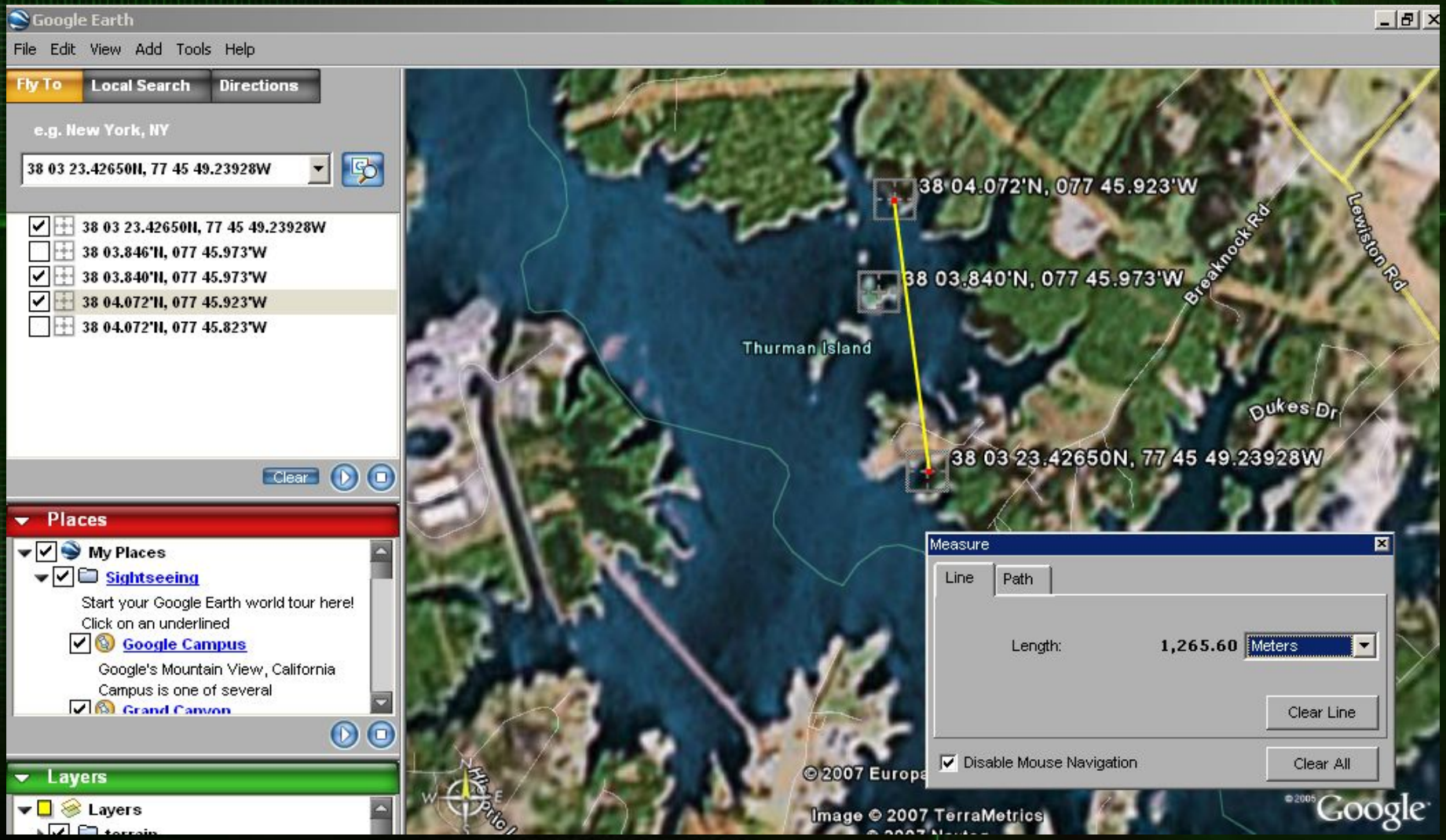


RDF Challenges - SilverFox

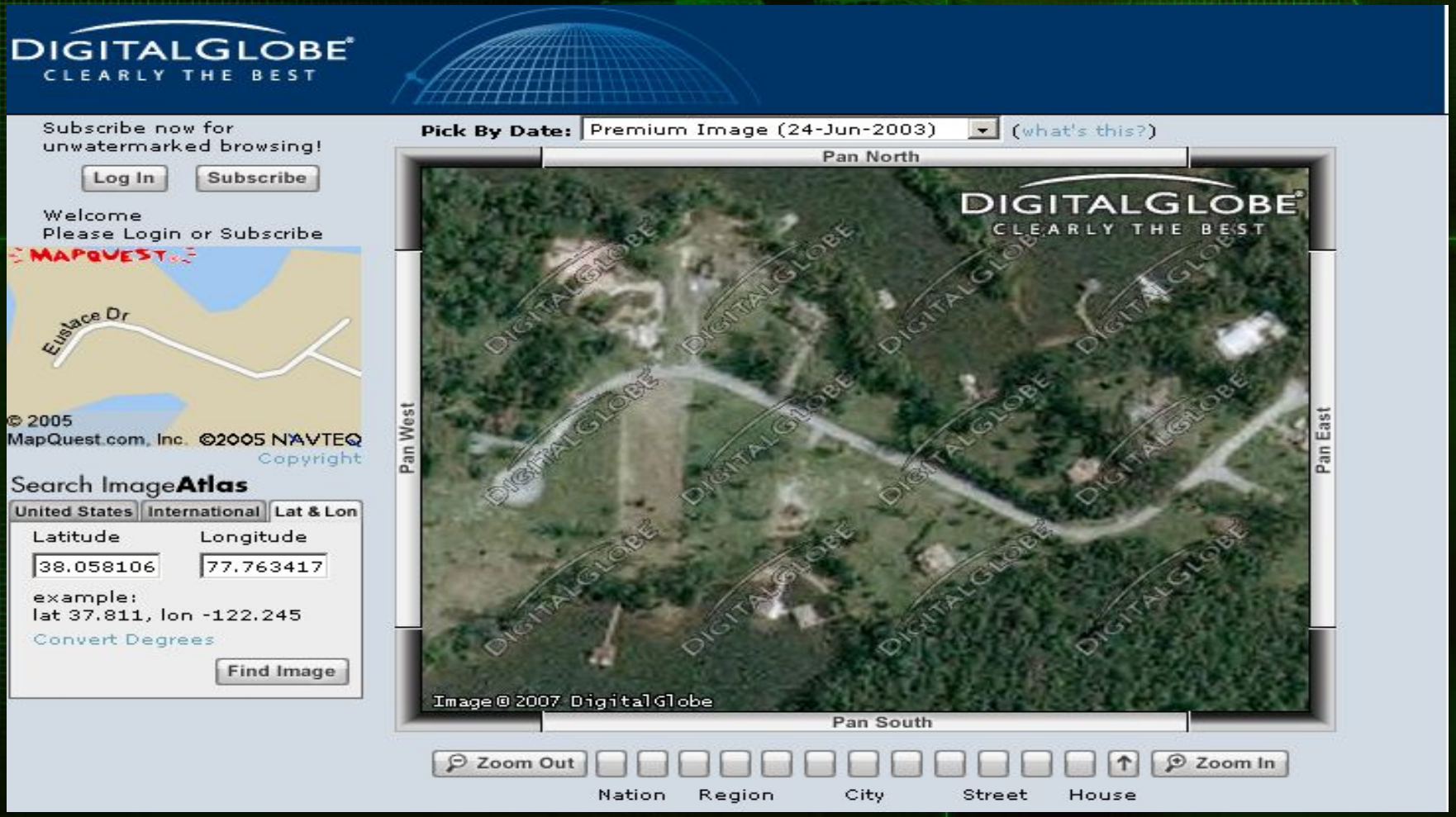


Required 3 Scans – Signal vanished @ F2

Sortie 8: AP Unknown Location SSID: default



Eustace Drive AP



Triangulation - Possible 3 houses on Eustace Drive

"The" House



Subsequent Scan finds the exact House, SSID (default)

GeoLocation – Result Summary

#/ Location	Error (m)	#/ Location	Error (m)
#1- Land Test	35	#5 – Anna Pt.	100
#2 – AP Bridge	234	#6- State Park (GeoCache)	110
#3 – Island 1	54	#7- SilverFox (GeoCache)	DR
#4 – Island1 LP	109	#8- Unknown AP	(See Picture)

Average Error: 107 m

AVG Distance - Target: 750 m

Accuracy Comparison

	Method	Accuracy (meters)	
GPS GeoCaching	GPS Standard	10	
GPS	WAAS	2	
Netstumbler	GPS Receiver Only	1000 (Vehicle Position)	
Wireless GeoCaching	GPS with RDF Triangulation	107	

Comparison to Other Methods

- 1st – Wireless GeoCaching Game was played under almost Ideal Conditions:
  - Clear Line of Sight
  - No traffic (other than 1 or 2 Boats).
  - Virtually No Multipath Interference
- GeoLocation in an Urban environment would not work as well.

RDF - More Art than Science

- Largely responsible for defeat of German U-Boats in the Atlantic WWII (Huff-Duff)
- Works best with Acute triangles
- With experience you get really good @ this! (Caches are a nice bonus)
- Recommend – 1st find target w/ trianglation. Then, simply scan closer & closer

Wireless GeoCaching -> Its all about the Hunt!

Safety Warning

- WARNING: The as-built version of the Scanner utilizing a Senao 200 mw high-power card produces an EIRP of 4 watts (the maximum legal limit)
- While within FCC limits, radiation exposure limits state you should stay at least **36 inches away** from ANY Beam antenna and operate the scanner such that it does not point at any vehicle occupants. (see ARRL on the web for more info.)
- Never operate a Laser such that it points directly at another person, (eyes).

Questions?

Device Demo

rhill@tenacitysolutions.net

References[1]

- "Database Correlation Method for Multi-System Location", Paul Kemppi, Helsinki University, 8/2005
- "Indoor Propogation Modeling @ 2.4 Ghz for IEEE 802.11 Networks", Dinesh Tummala, University of North Texas, 12/2005
- "Wireless Support Positioning using Support Vector Machines", Philipp Schloter, Stanford University, 7/2006
- "A Practical Approach to Identifying & Tracking Unauthorized 802.11 Cards & Access Points", Interlink Networks, 2002

Parts List & Suppliers

- MFJ Enterprises MFJ-1800 15db Antenna, mfjenterprises.com
- Brunton Nomad V2 Digital Compass, thecompassstore.com
- DigiKey 7.5 deg. Stepping Motor, #403-1010-ND, digikey.com
- Stepper Motor & Analog/ Digital Controller, gadgetmasterII, pcgadgets.com
- Laptop with Visual Basic 5.0 or later & Netstumbler 0.4.0 intstalled
- Magellan GPS 315
- Laser Pointer (generic)