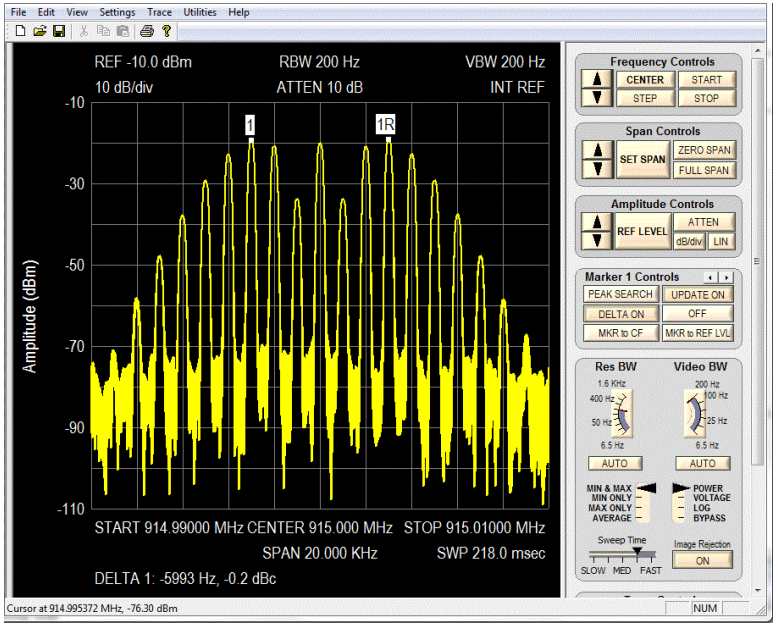
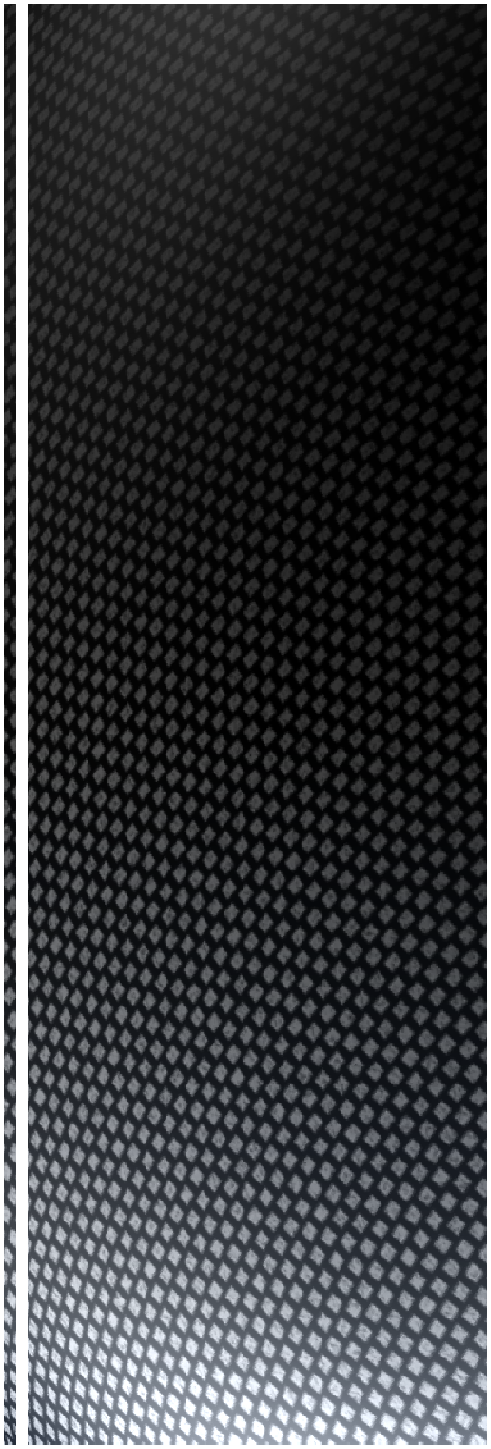
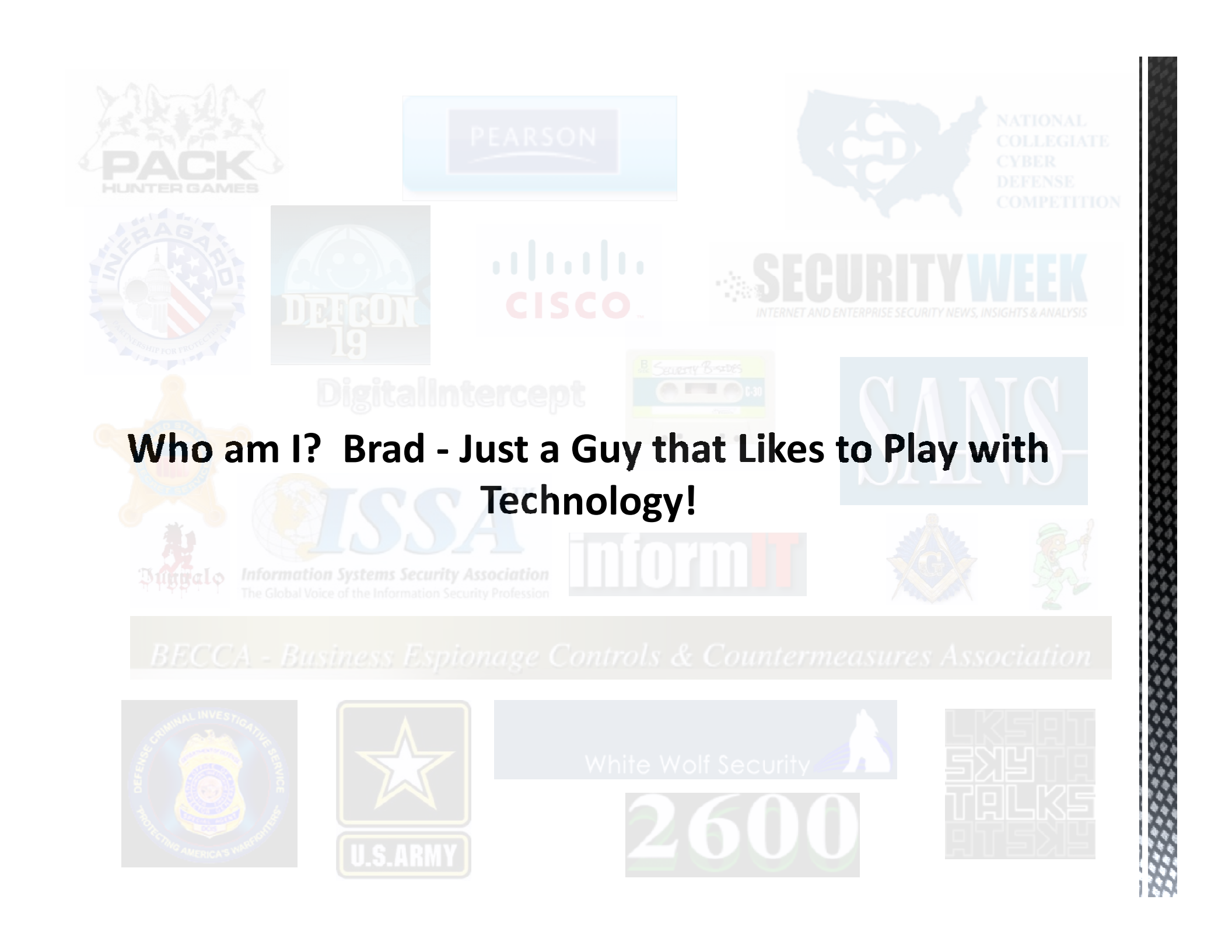
Building Measurement & Signal Intelligence (MA**S**INT) on a Hackers Budget:
Tracking & Fingerprinting RF Devices

WarezJoe







Who am I? Brad - Just a Guy that Likes to Play with Technology!

Disclaimer

Everything I say is my personal opinion and not those of my employer!

Education and Entertainment purposes only!

This is a work in progress!

Some equipment or functionality may be considered “Dual-use munitions” and controlled under ITAR 121.1. Be sure to follow appropriate laws!

Never go full tard!
Above all do no harm!

Goodbye SOPA…. Goodbye PIPA…. Thank you for playing!

Agenda

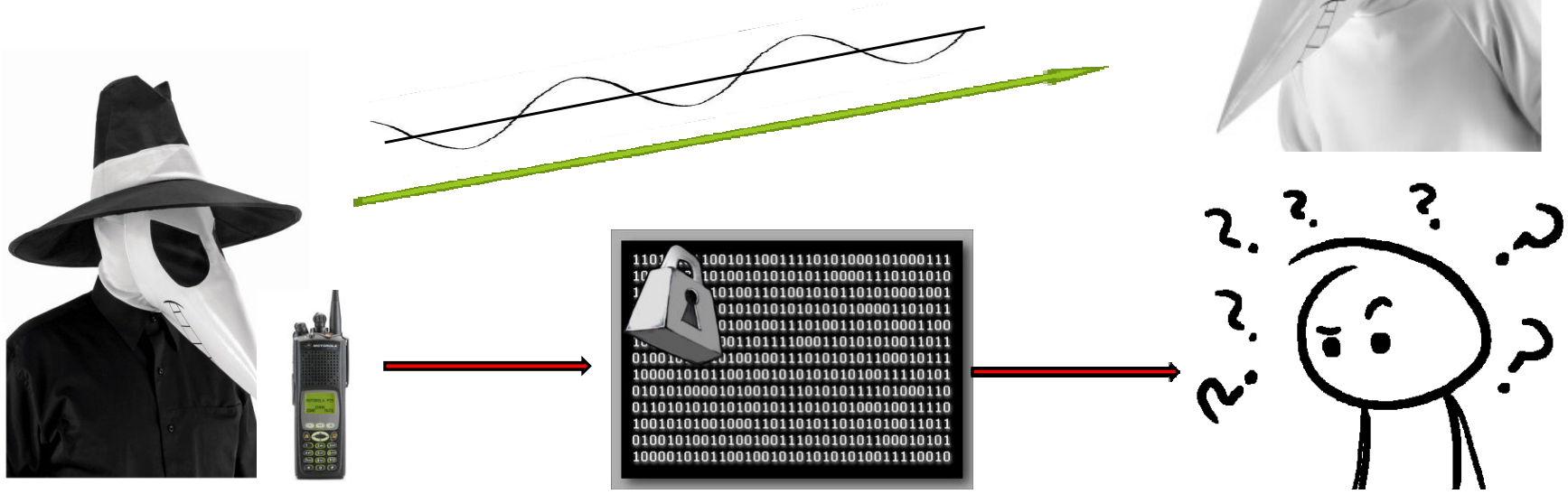
- What is MASINT/(TSCM)
- How is it used & why should you care
- MASINT on a Hacker's budget
  - Equipment
  - Testing / Process / Methodology
  - Creating / Analyzing Signatures
- Making things do what they were not intended!
- What's next
- Q&A

Let's get our terms right

- What is MASINT ?
- Measurement & Signature Intelligence
- Collection of unintended emissions or byproducts of devices
- All devices generate unique undesirable trans. artifacts
- Discrete intelligence gathering process
- DoD - Officially adopted as a Intelligence discipline in the 80s
- Often aggregated with other intelligence sources
  - (ELINT, SIGINT, HUMINT, ETC.)
- MASINT – (Tactical and Strategic Sensors)
  - Electro / Electronic
  - Nuclear / Explosives
  - Geospatial / Materials
  - Radio Frequency / Electromagnetic fields*

Who uses it? – What does it do?

- DoD and Intel Community
- Identify / tags “enemy” equipment
- For RF MASINT - Identifies types of comm.
- Frequency, Origin and strength – (SOI)
- Signal Intelligence Support System – (SIGINT)
- Gather Actionable Intelligence



RF MASINT – What does it do? Cont…

- Lots of passive Intelligence to be had!
- Unique hardware / radio frequency signature
- Characteristics of the signal
- Track user movements and habits via RDF
- Other useful intelligence
- Hardware capabilities / Transmission range / Frequencies
- Identify patterns & Weakness
- Naturally occurring / Very difficult to spoof*


Why should i care?

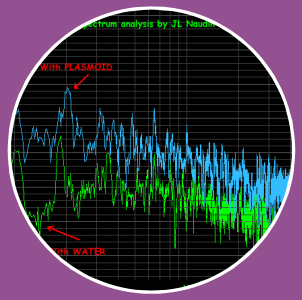
MASINT - Why Should you Care?

- Make some Info. Sec. friendly tools
- Add MASINT components to you pen testing capabilities
- Uniquely identify equipment by its RF signature
- Track people by the electronic devices they carry
- Develop Technical Surveillance & Counter Measures Capabilities
- Identify spurious transmissions / jamming
- Battlefield RF MASINT capabilities are being adapted for:
  - Law Enforcement – tracking transmissions / illegal devices, etc.
  - Commercial use (Industrial & Corporate Espionage) – Law offices
  - Information on competitor's products
- Cost and complexity for MASINT technology is decreasing
- Legalities of LE using MASINT for intel gather remains unchallenged

RF MASINT – Lets Build It!

Spectrum Analyzer

(SDR) Search Receiver & Antenna System



Signal Collection Analysis & Signature Generation

Signature Analysis, Tracking, Intel

Let's build it!!! – Equipment

- Spectrum Analyzers – Lots of Choices but…..
  - Generally very expensive! ($10K-$60K)
  - Typically not designed to provide MASINT or TSCM functionality
  - Limited frequency range
  - Difficult to get data out of in raw form
  - Restrictive antenna capabilities
- Some hacker friendly models exist (SpecTran, Anritsu, TekTronix, etc.)
- Device of choice – Signal Hound (USB-SA44B)
  - Software defined / USB connected / easily interfaced
  - Decoding Capabilities (FM,WFM, NFM, CW, SSB, Video, FSK, ASK, etc.)
  - API available / scripting friendly
  - Low cost $300 - $400 used
  - 1Hz to 4.4GHz / fast sweep times*
  - Good Sensitivity / built-in Preamp / Attenuators*
  - Calibration capabilities

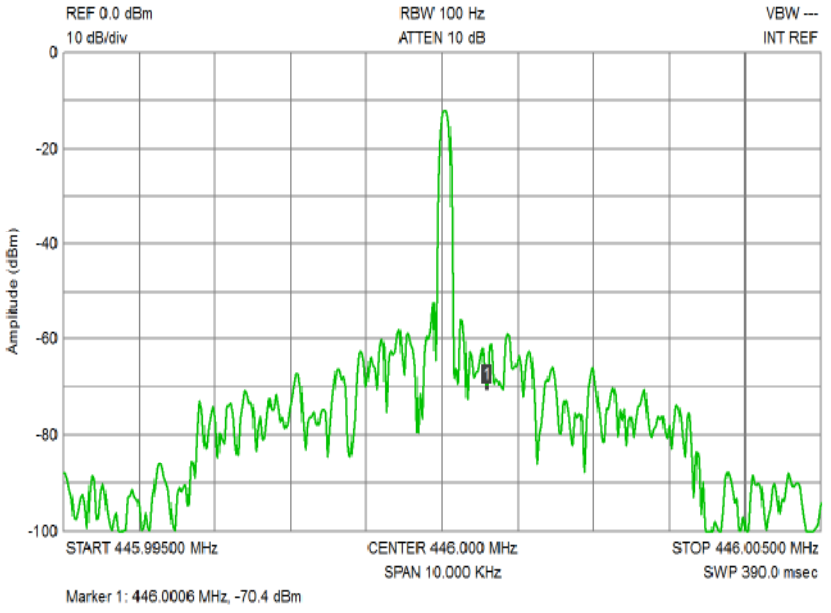
Let's build it!!! – Spectral collection

- Premise – low power RF equipment can be uniquely identified
- Signatures structure
  - Signature taken a set frequency (446MHz, 220MHz, 146MHz, 900MHz)
  - RF Signature recorded over (3) secs with a Span of 10Khz
  - Unique Signature created using Amplitude (Max & Min) per/Hz
  - Aprox. Distance 10ft – no faraday enclosure used

Motorola XTS3000 model3

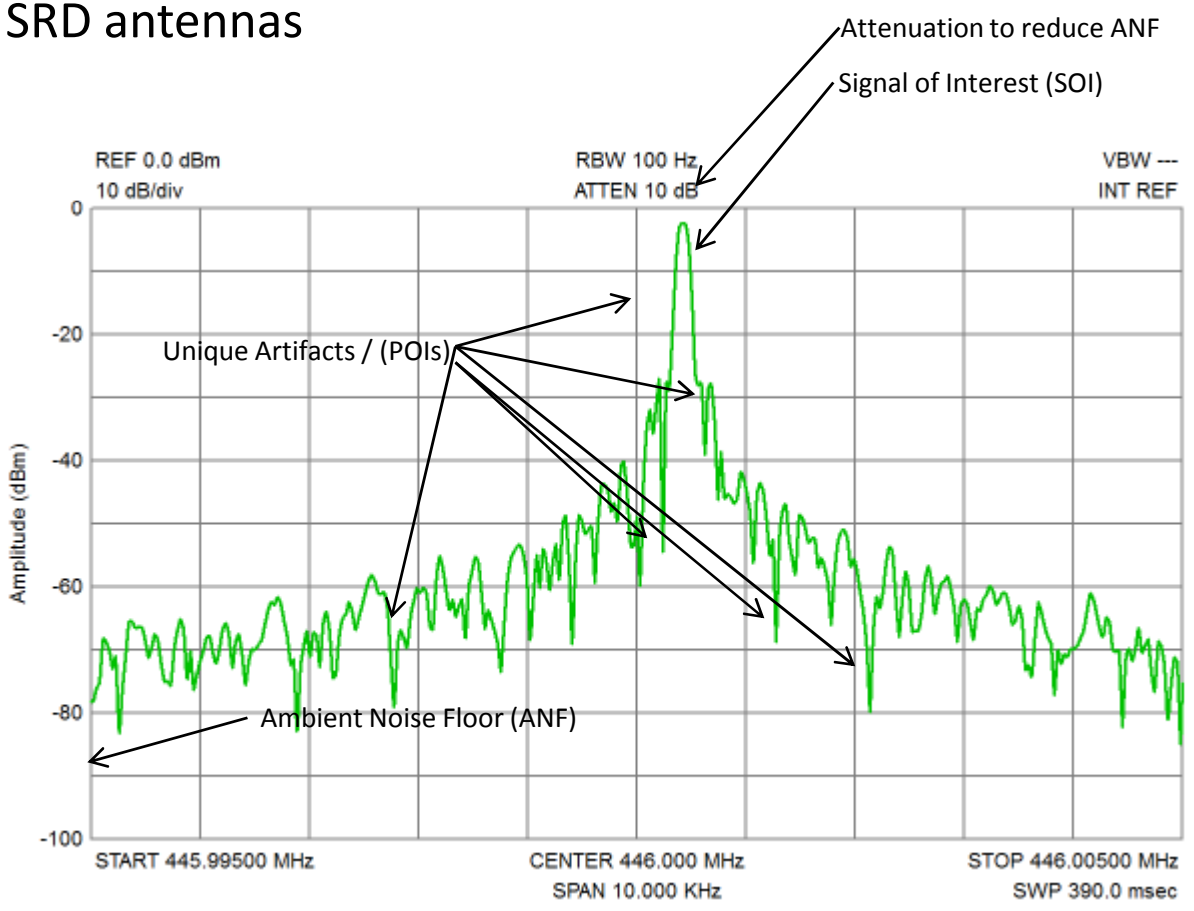
Frequency (MHz)	Amplitude Min(mW)	Amplitude Max(mW)
445.994986	1.51E-09	1.51E-09
445.995015	1.53E-09	1.53E-09
445.995045	1.17E-09	1.17E-09
445.995075	7.27E-10	7.27E-10
445.995104	4.87E-10	4.87E-10
445.995134	1.91E-10	1.91E-10
445.995164	1.66E-10	1.66E-10
445.995193	2.63E-10	2.63E-10
445.995223	4.61E-10	4.61E-10
445.995253	5.80E-10	5.80E-10
445.995282	3.29E-10	3.29E-10
445.995312	1.12E-10	1.12E-10
445.995342	6.12E-10	6.12E-10

Motorola XTS3000 model3



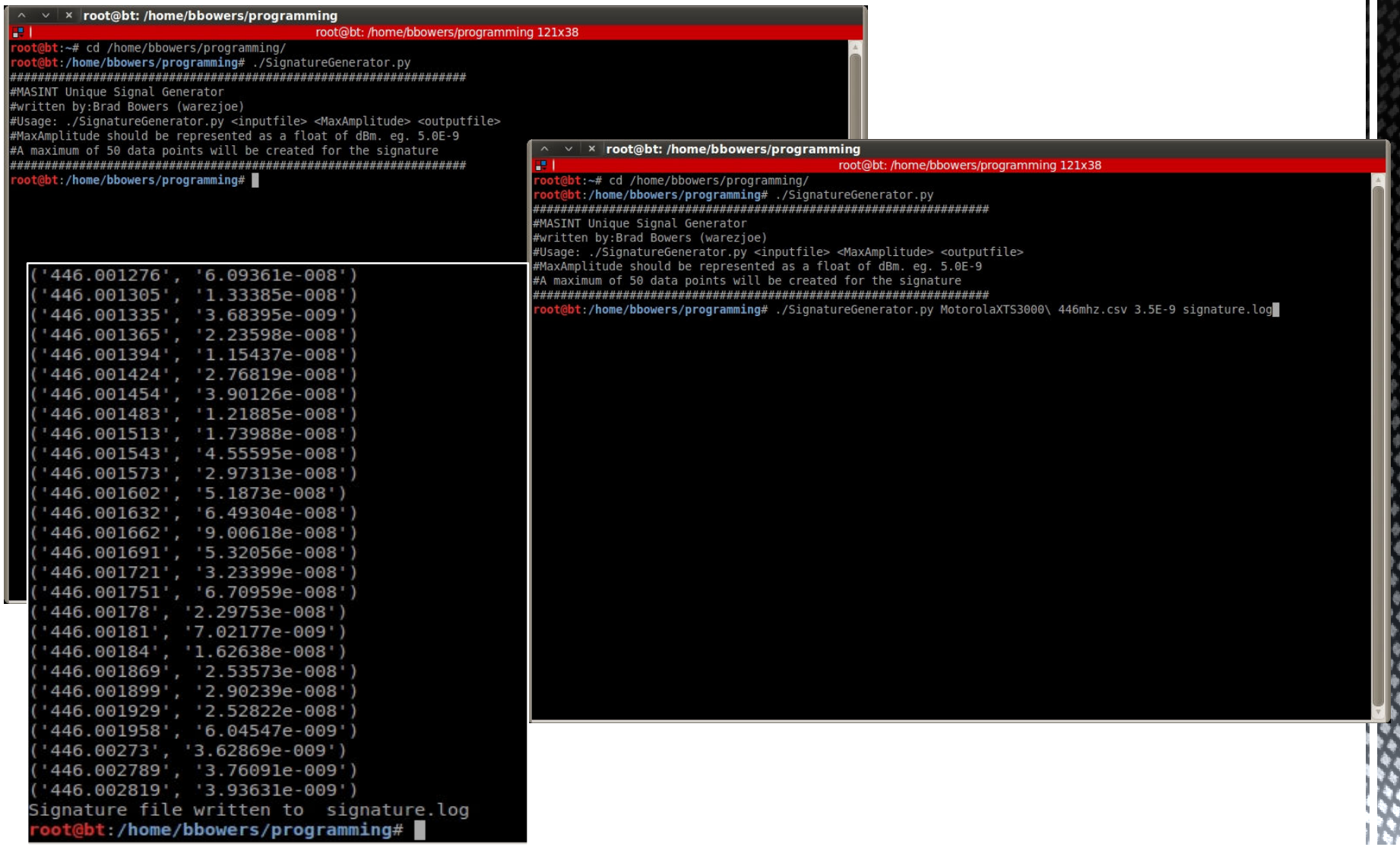
Let's build it!!! – SOI Signature Collection

- Finding unique RF characteristics
  - All electronic devices will generate unique "Artifacts" in near-field
  - Filtering Ambient noise with 10db attenuation
  - Measuring mW at the SRD antennas
  - Collecting Amplitude Max/Mins
  - RF span 10Khz
  - 3+ sec measurement
  - 340 Points of Interest
  - 0.e-14 sensitivity
  - .CSV file output
  - User defined Max Amplitude



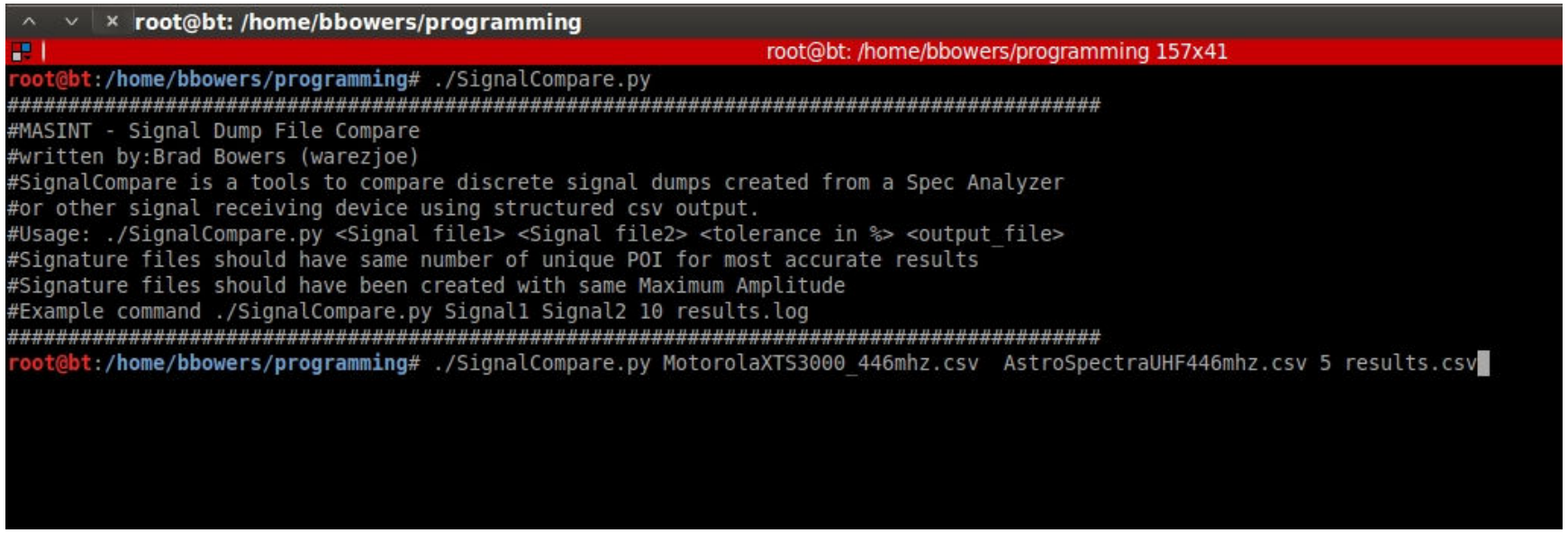
Let's build it!!! – SOI Signature Creation

- Signature Creation Scripts – Python
  - Signature Generator & Signature Compare

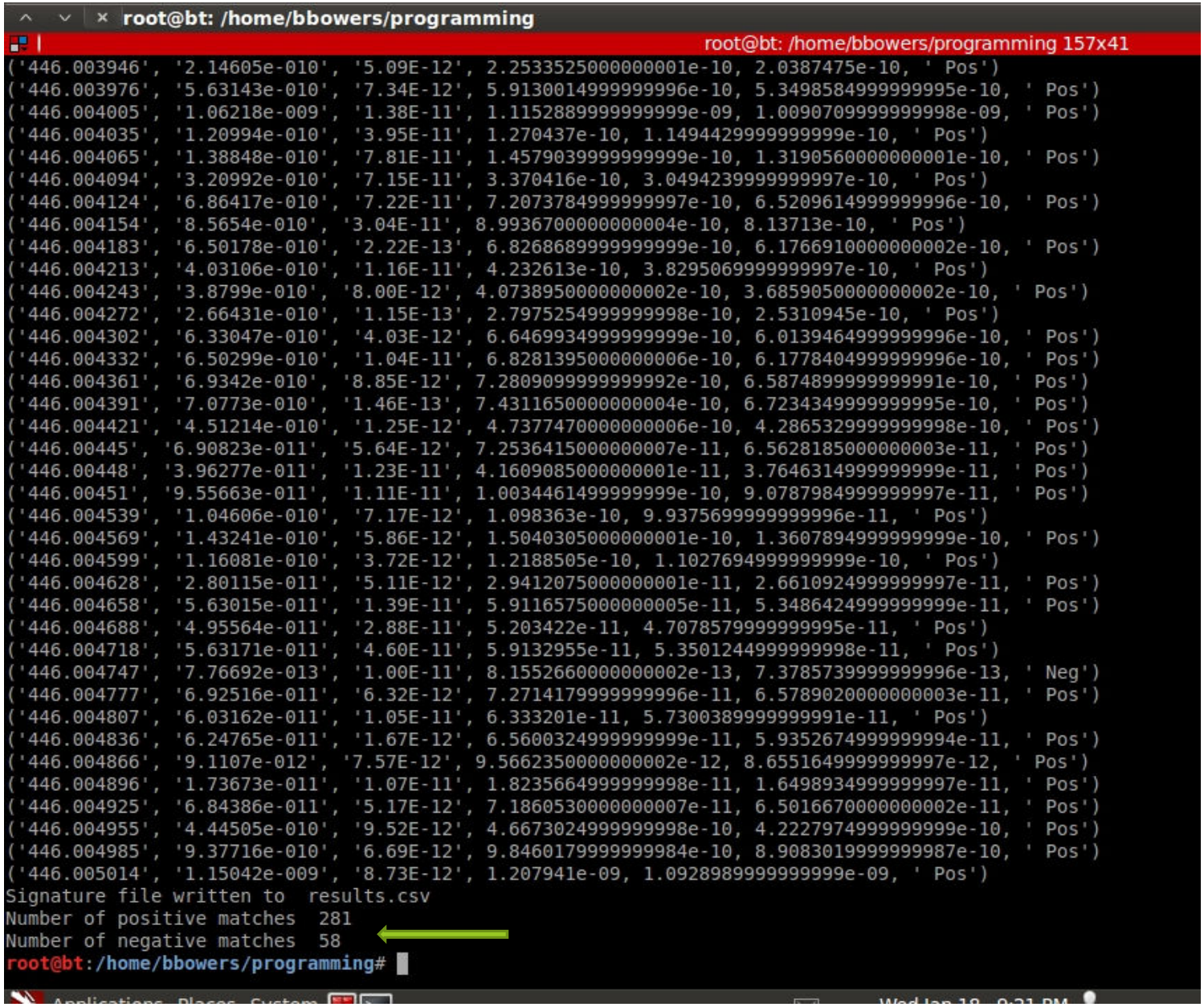


Let's build it!!! – SOI Signature Compare

- Signature Comparing
  - No two signatures will come back 100% same
  - Script provides a configurable tolerance
  - Tolerance does not sway results significantly because of the ranges
  - Negative hits increase as you move away from center



Let's build it!!! – Signature Compare Contin…



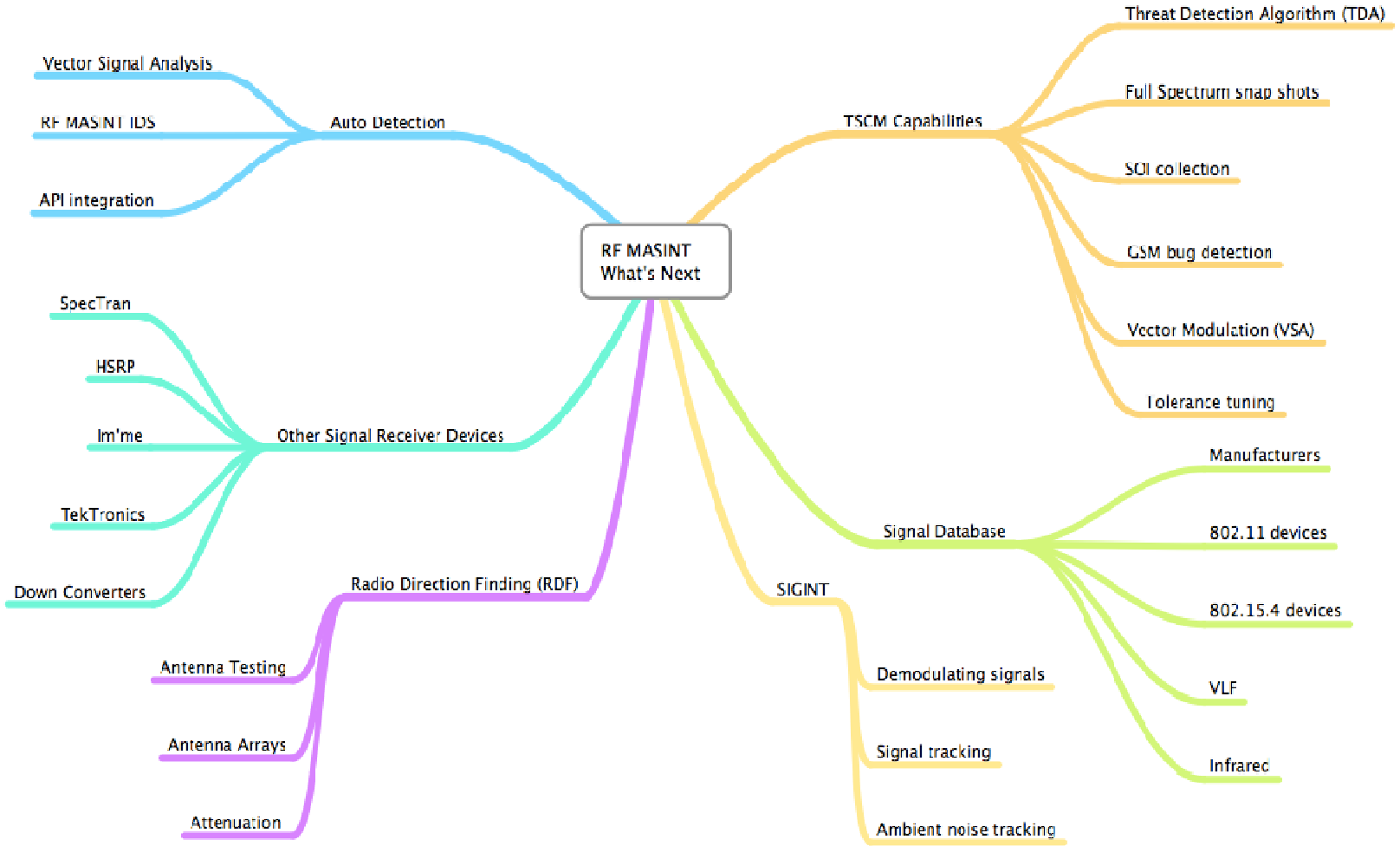
Caveats…..

- Lots of things can throw off your Signals of Interest (SOI)
  - Changing antennas, RF noise, Physical structures, atmospheric, etc.
  - Spread spectrum signals can be missed in a simple full spectrum sweep
- Lower output devices require a closer (near field) range
  - Some devices have too low of output in standby mode to detect cleanly
- Antennas are extremely important
  - RDF – requires both attenuators and directional antennas (Yagi)
  - 96” Discone and a collection of whip antenna worked well (YMMV)
- Sweep speeds become really important when looking at TSCM
  - 20secs is very fast for low cost units. OSCAR devices are probably better

To Surmise…..

- Lots of interesting intelligence can be derived from the unintended emission or artifacts.
- All electronics put off some form of near field RF artifacts
- RF MASINT / TSCM capabilities can be developed using relatively low cost SDR Spec. Analyzers and a bit of code
- MASINT technology is slowly being incorporated in the commercial Sector.
- RF MASINT / TSCM capabilities may add a new “value add” to pen testing engagements.

What's Next? Where's this going….?



THANK YOU!!!

Contact information : Warezjoe
Warezjoe@digitalintercept.com
Special Thanks to Mike M. (Megalos) & David P. (Yeti)