



Practical Foxhunting 101

Adam Wirth - SimonJ



Overview

- ▶ About me
- ▶ About Foxhunting
- ▶ Equipment Overview & Selection
- ▶ Preparation
- ▶ Techniques

Who Am I?

- ▶ More than 15 years professional experience as a software & systems engineer
- ▶ Most of my career has been spent working on wireless communications & emitter geolocation systems
- ▶ Last year's winner of the Hide & Seek and Foxhunt events in the Wireless Pentathlon

What is Foxhunting?

- ▶ Finding the physical location of wireless emitters and/or their users, by measuring received power from different locations
- ▶ Foxhunting is between the "last mile" and the "last feet"; for greater or lesser distances, other techniques are more appropriate
 - ▶ Wet-work ninjas finding the correct bedroom in the house of the South American populist government official
 - ▶ Tracking the Corporate Exec whose iPhone you've trojaned into an access point, as part of a Red Team penetration test
 - ▶ **DEFCON 22 Wireless CTF**
- ▶ Techniques are applicable to all RF emitters, like mobiles phones, WiFi APs, heart monitors, etc.

What Equipment's Involved?

- ▶ Antennas
 - ▶ Omnidirectional and directional, for different purposes
- ▶ Radios
 - ▶ Capable of receiving the signal-of-interest
 - ▶ Software-defined radios are finally becoming affordable
- ▶ Visualization Software
 - ▶ Most important feature is viewing received power over time



Gear Selection:

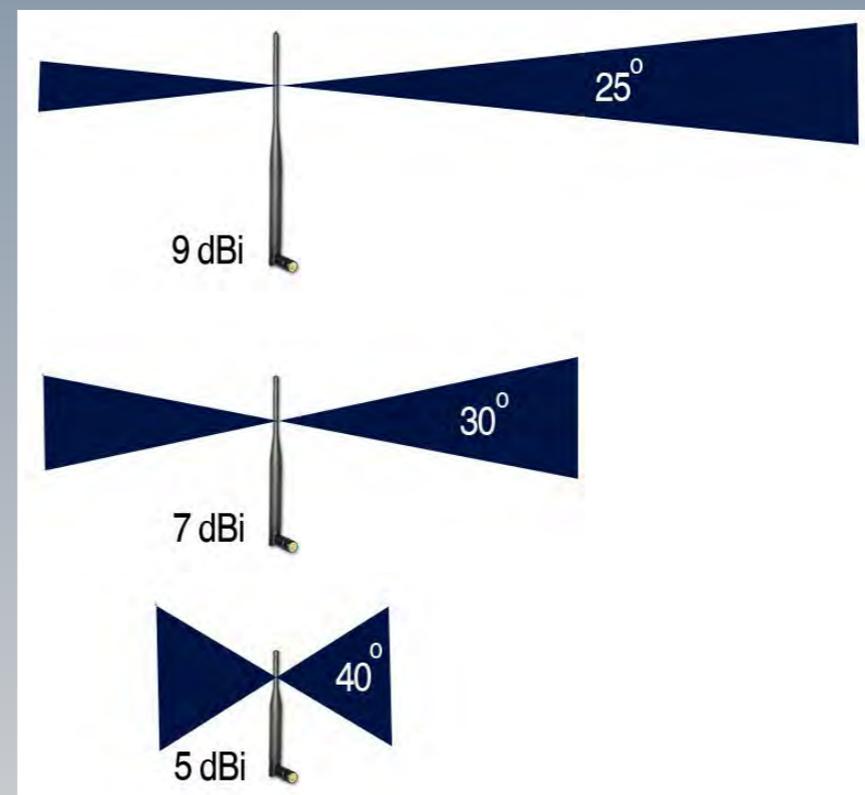
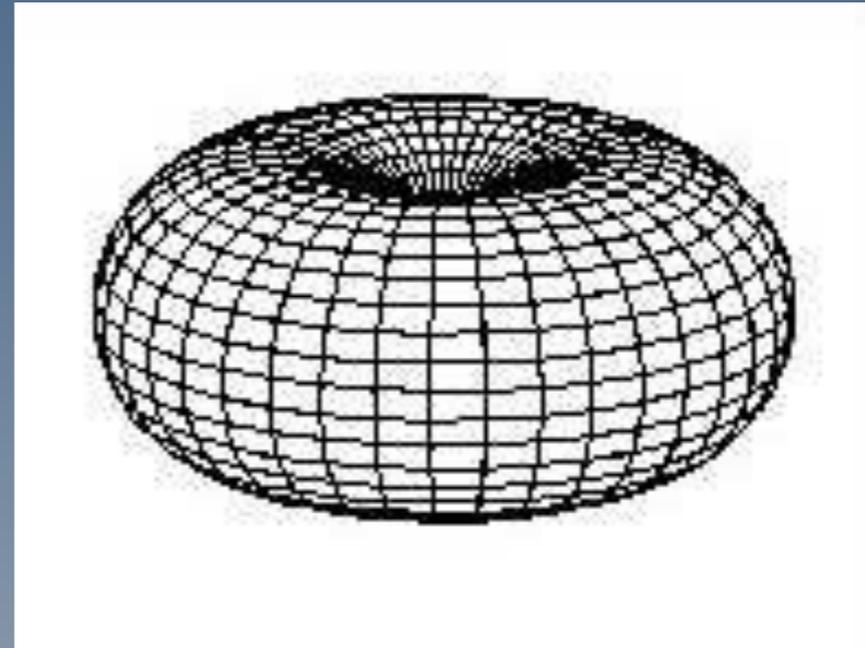
Antennas

Aperture Versus Gain

- ▶ As a rule, the more sensitive the antenna, the more focused (directional) its reception pattern
- ▶ Too much gain can be a bad thing
 - ▶ High gain requires accurate pointing
 - ▶ Power curve follows the Inverse-Square Law
 - ▶ Unless you can attenuate your gain, you lose range discrimination when you're close to an emitter

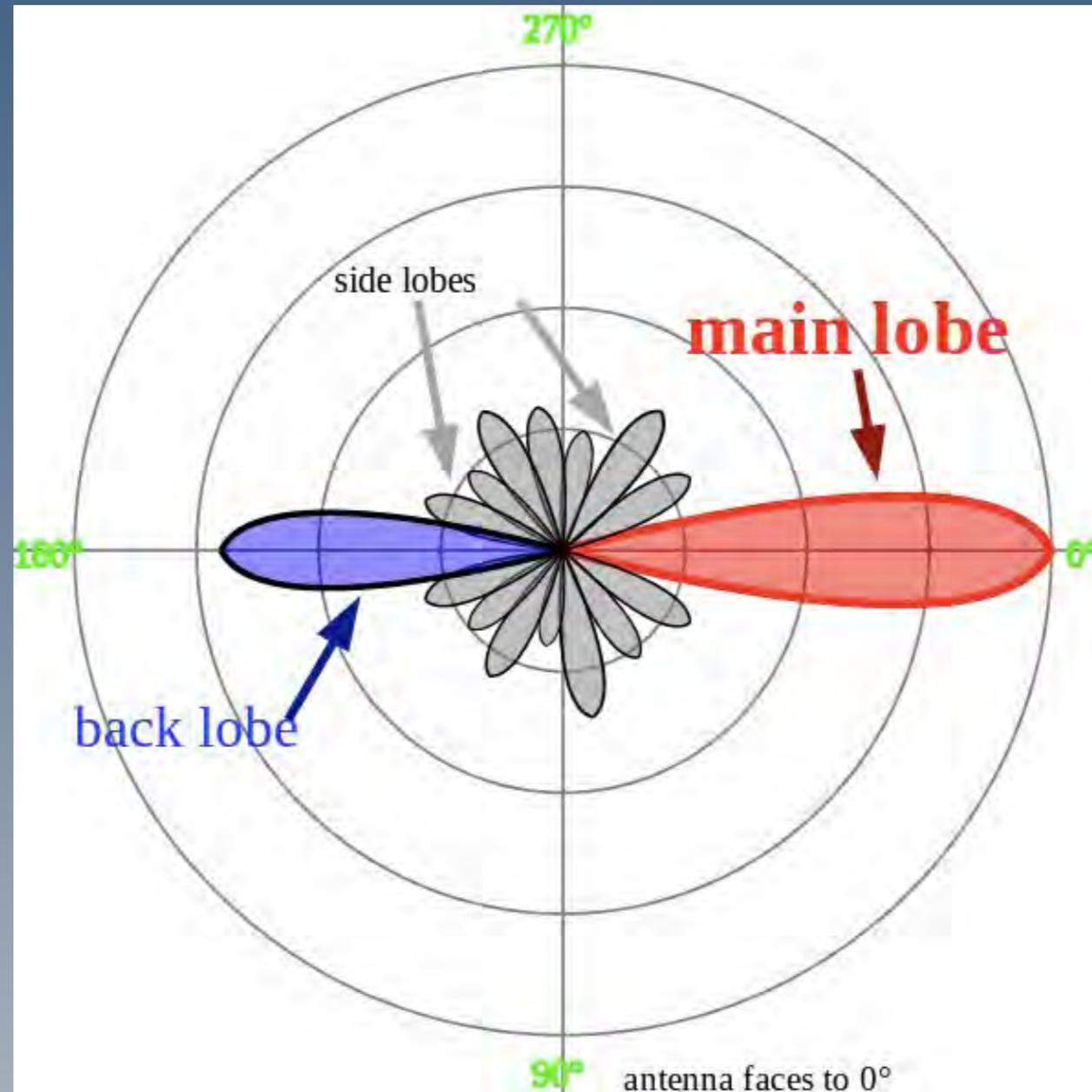
Omnidirectional Antennas

- ▶ Typically have a toroidal radiation pattern
- ▶ Gain varies inversely with z-axis directionality
- ▶ For foxhunting, high gain is good
 - ▶ Provides greater detection distance
 - ▶ Allows some degree of attenuation by varying orientation



Directional Antennas

- ▶ There are only two good choices, based on availability:
 - ▶ Yagi: High gain, narrow aperture, narrow bandwidth
 - ▶ Panel: Refers to several varieties of antennas that are flat perpendicular to their boresight, therefore performance varies
- ▶ Log-periodic antennas are also available, but are less common
- ▶ If you're on a budget, it's easy to make your own Cantenna or WokFi
- ▶ Choose your antenna based on performance and form factor



Directional Antenna Pattern

Beware of back lobes & side lobes when hunting

Multi-antenna Arrays

- ▶ Generally proprietary (Read: expensive)
- ▶ Require custom software
- ▶ Tricky to configure and use correctly
- ▶ But awesome when you have one!
- ▶ Challenge: Create a HackRF-based DF array



Gear Selection:

Radios

Cost Versus Performance

- ▶ RF equipment can get expensive quickly
- ▶ Broadband radios and software-defined radios are more expensive than their application-specific counterparts, but are more flexible
- ▶ Low-cost SDR is starting to become a reality
- ▶ WiFi radios are particularly inexpensive; perfect for beginners: Alfa 1 & Alfa N

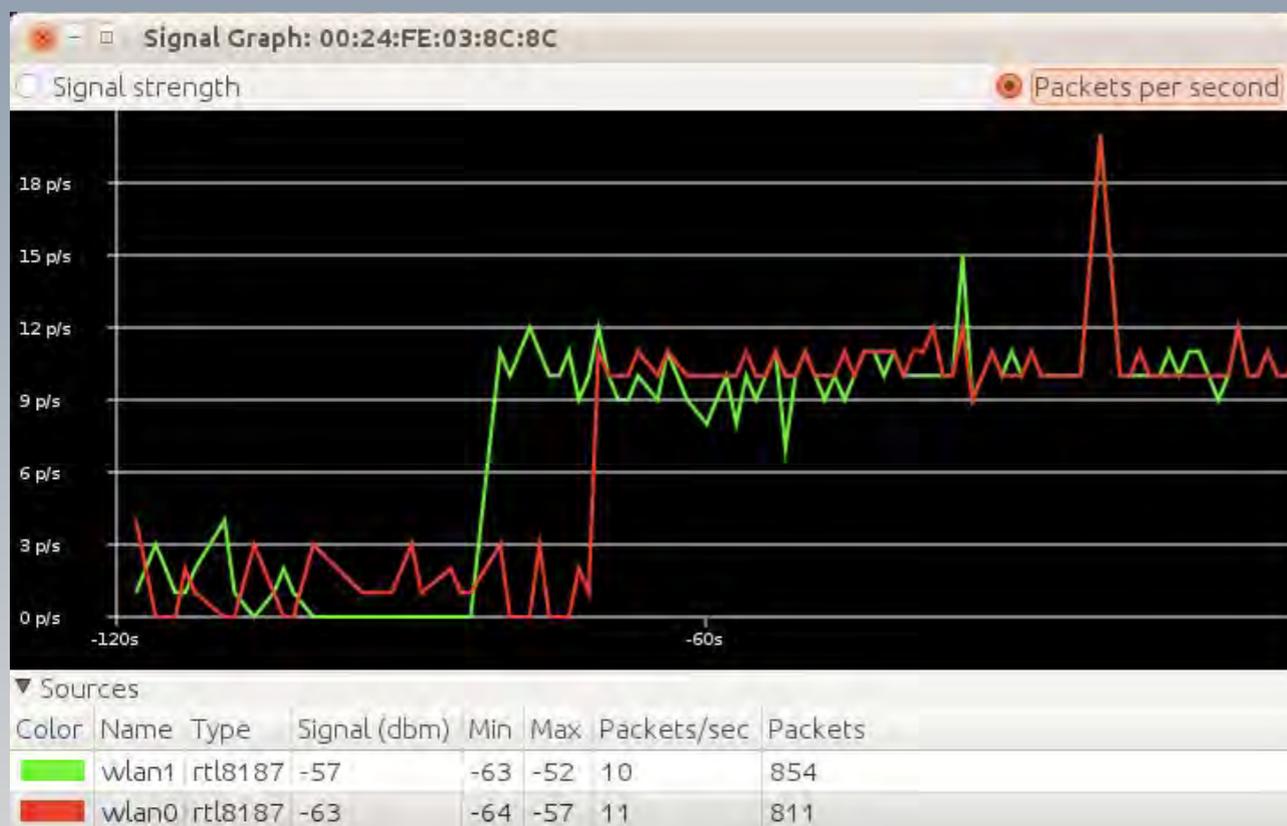
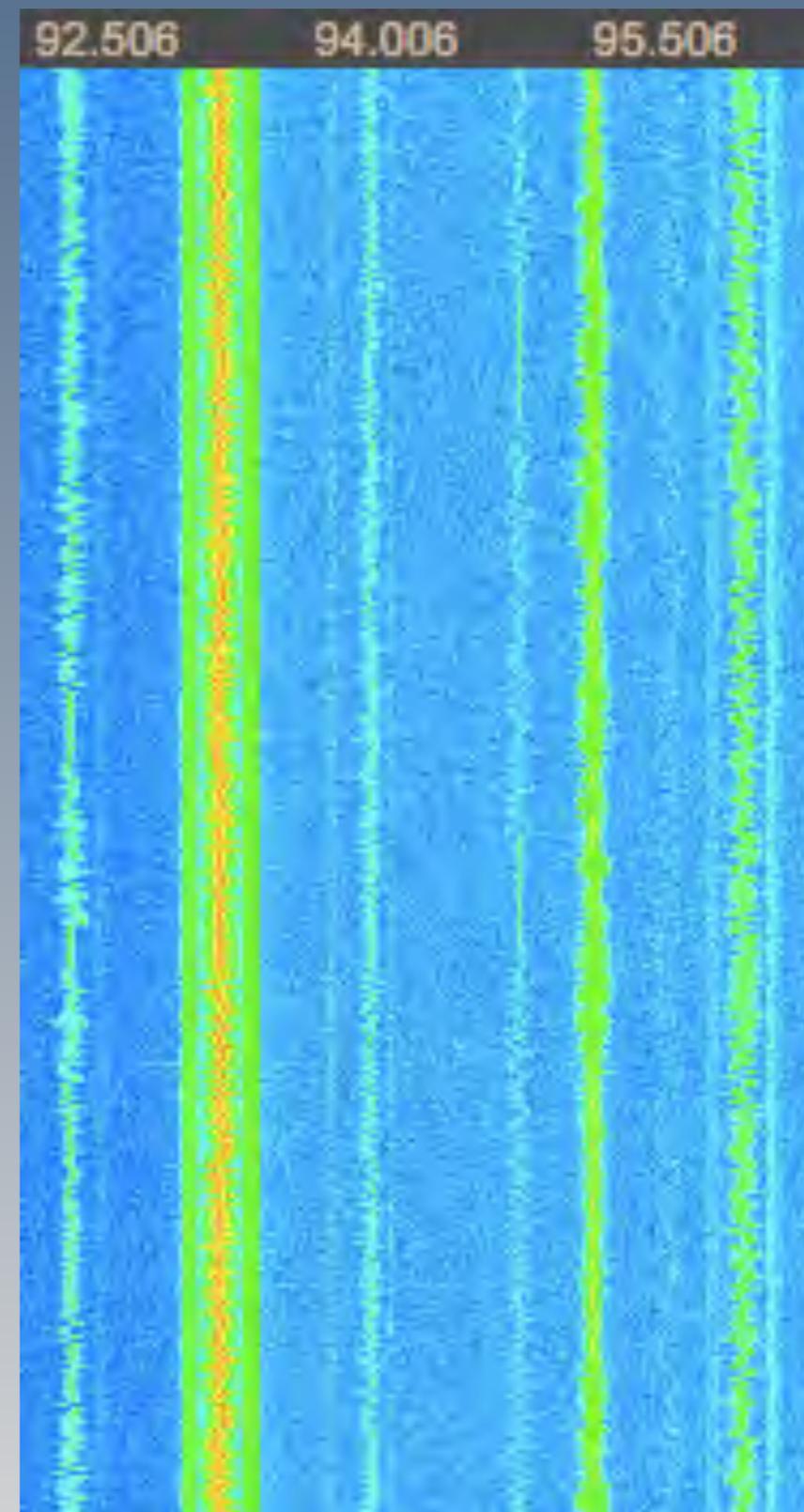
Variable Attenuators

- ▶ Used to reduce the strength of the received signal
- ▶ Allow you to use a very high-gain antenna, even at close ranges
- ▶ Not strictly necessary, but add versatility
- ▶ Many types are available, but they usually aren't cheap; check eBay
- ▶ Old-fashioned variable attenuator: rotate your antenna

Signal Displays

- ▶ Power Spectral Display
 - ▶ Helps locate your target in the RF spectrum
 - ▶ Not always needed, if you have other ways of tuning to an emitter
- ▶ Power/Time Domain
 - ▶ Used to track your target over time
 - ▶ Foxhunting tool of choice
- ▶ Cumulative Spectral Decay / Spectrogram / Waterfall
 - ▶ PSD & PTD combined; can be used to track multiple emitters over time: information overload for simple foxhunting

Signal Displays



Using Your Gear

Preparation

- ▶ Know and be comfortable with your equipment, especially how long your batteries will last
- ▶ Learn detection ranges for your particular setup; WiFi radios estimate signal strength inconsistently
- ▶ Know how sensitive your back/side lobes are
- ▶ Become fluent in the software you're using
- ▶ Practice



Inconspicuousness

- ▶ If you have a bunch of obvious equipment, people will be wary and avoid you
- ▶ Fly below the radar, or risk spooking your target

General Tips

- ▶ Be aggressive! Make an active effort to seek your target
- ▶ Be aware of your environment, and take an organized approach to your search area; don't just wander randomly
- ▶ Keep a mental map of where you've been, and the observed signal levels along the way, for mental triangulation
- ▶ Heads Up! Don't glue your nose to the screen, or you might miss a chance to find your target based on secondary indicators



Multipath

- ▶ RF emanations will reflect off structures and objects
- ▶ Same signal will be received from different directions at different times (Phase Shift)
- ▶ Changes the SNR of the received signal (Multipath Fading)
- ▶ To mitigate multipath interference during a foxhunt, keep moving!

Using An Omni

- ▶ Used for proximity detection (Am I getting closer to the emitter?)
- ▶ Possible to successfully hunt with just an omni
 - ▶ Easier when dealing with stationary targets
 - ▶ Move around a lot to determine emitter proximity from various locations
 - ▶ Keep a good mental map, to perform on-the-fly triangulation

Using A Directional

- ▶ Steers you in the right direction, once you've determined proximity using the omni
- ▶ Helpful to have a variable attenuator between your directional antenna and the radio
 - ▶ Reduces the antenna's lobes (enhancing directionality)
 - ▶ Reduces your effective gain when you're getting closer, to give you more headroom against your radio's maximum input gain

Basic Strategy

- ▶ Tune your radios to the target emitter
- ▶ Walk a search pattern, watching the signal strength on a PTD plot
 - ▶ Use the omni to determine if you're getting closer
 - ▶ Use the directional, and your historical direction of travel, to determine in which direction to continue
 - ▶ If you start to peak your signal, add attenuation
- ▶ Don't go too fast, because received power will fluctuate
- ▶ Look around: The emitter may become obvious once you relate RF power to what you see in the environment

My WiFi Setup

- ▶ 5db Omnidirectional rubber duck
- ▶ 8db simpleWiFi mini panel
- ▶ HP 8495A Manual Step Attenuator
- ▶ Alfa USB NICs - Alfa 1 & Alfa N
 - ▶ Alfa N on the omni - it holds connections better
 - ▶ Alfa 1 on the panel - it's more of a pure radio
- ▶ No good free software; Kismet/Kismon, WiFi Analyzer (Android), and NetSurveyor (Windows) are OK



1890

W. Kattner