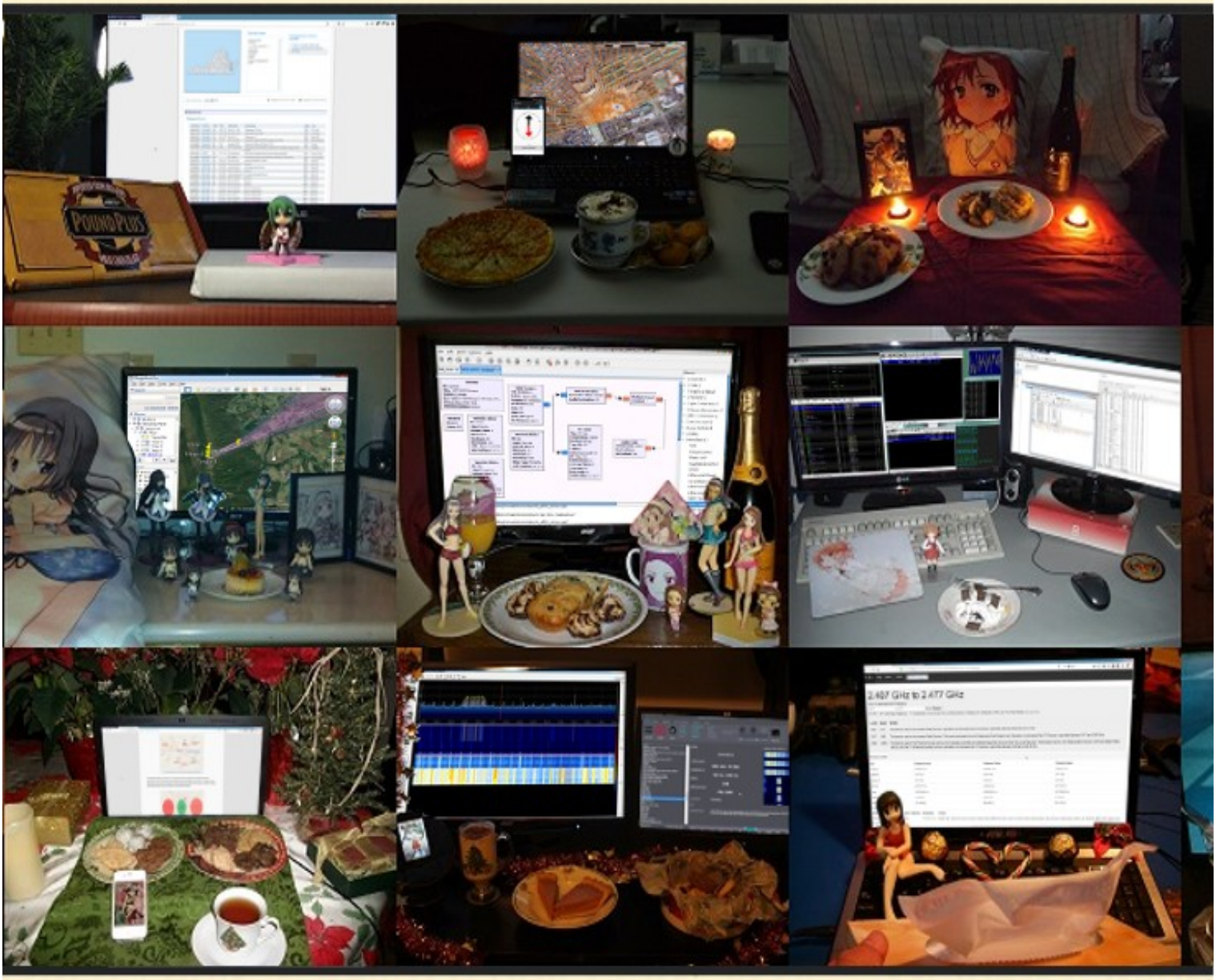
Strelok's Amateur Intelligence Manual

Signals Intelligence



/k/

A NEET's guide to cheap homemade SIGINT, including listening methods, research tools, direction finding, and software suggestions, for hobby analysts, radio amateurs, and budget militias.

V 0.5 Initial release finished up to “Metasignals”
V 0.6 Finished Metasignals intro, added Direction Finding and Sources sections.
V 1.0 Final update pending requests for topics / annual review

WARNING: UNTILL SHIT HITS THE FAN, THE FCC REQUIRES THAT YOU OWN A HAM RADIO LICENSE (Technician Class and up) BEFORE OPERATING A HAM BAND RADIO SUCH AS THE BAOFENG UV-5RA. IF YOU GET YOUR ASS HANDED TO YOU BY THE FCC BECAUSE YOU WERE CARELESS AND STARTED BROADCASTING FART NOISES THROUGH YOUR LOCAL REPEATERS, THAT'S ON YOU. JUST REMEMBER, EVERY TIME YOU KEY THE MIC WITHOUT A LICENSE, YOU'RE PLAYING RUSSIAN ROULET WITH A SWAT TEAM AND A 5 FIGURE FINE, SO GET A LICENSE AND HAVE YOUR CALL SIGN MEMORIZED!!!

ADDITIONALLY, SOME EUROPEAN COUNTRIES MAY HAVE LAWS PROHIBITING SOME SIGNAL MONITORING TECHNIQUES DEMONSTRATED IN THIS GUIDE. IN THE UNITED STATES IT IS LEGAL TO MONITOR UNENCRYPTED SIGNALS, BUT POSSESSION OF DECRYPTION KEYS FOR GOVERNMENT RADIO NETWORKS WILL GET YOU V&’D. REGARDLESS OF LEGALITY, BE SMART: DON’T TEST OUT YOUR RADAR AT THE END OF A MILITARY RUNWAY AND READ KACZYNSKI WHILE YOU WAIT.

ALSO, THIS GUIDE IS ONLY TO HELP SPARK YOUR INTEREST IN RADIO TECH AND TO HELP DURING A SHTF SENARIO. MUCH OF WHAT IS SAID HERE IS OPEN TO CORRECTION, AND SHOULD BE TREATED AS SUCH. I EXPECT YOU ALL TO DO YOUR OWN FUCKING RESEARCH BEFORE COMMITING TO THIS GUIDE. BECAUSE SHTF OR NOT, HAM RADIO IS JUST FUCKING FUN. IF DRAGON DILDO FUCKING FURRIES CAN DO IT, SO CAN YOU!!!

NEET Signals Agency: The HAM Strelok's Guide to Cheap Signals Intelligence

Congratulations, Strelok! You read the Beginner's Guide, got your license, got your Baofeng, practiced by listening to old men, and now you and your friends are all ready for SHTF! As soon as you hear the news, you and your friends grab your guns, grab your radios, grab your packs, get your mission briefing from your intel gu-
Ah, you don't have an intel guy, do you? Well, I guess you guys can wait at the park and hope some ZANU fighters show up. Alternatively, YOU (Yes YOU!) can become the intel guy!

There are plenty of declassified manuals, amateur tradecraft, and government studies detailing other disciplines, but there's one thing you'll be hard-pressed to find in any government intelligence manual: SIGINT equipment you can afford. The aim of this guide is to show you how to pluck knowledge out of the sky without having to spend exorbitant amounts of cash on an industry-grade 50W TX/RX 500MSPS SDR when you just need to listen to a strong WBFM transmission on 90.3MHZ.

Define to Achieve: The Fuck is Intelligence?

A lot of jokes can be made at your expense with that question, but I'll call you a faggot and move on. The details of intelligence, from disciplines, to counter-intelligence, to management, are all critical in making sure a well-trained Strelok is in the right place at the right time. You don't need to be an expert in all of these topics (though there are Master's degrees available if you wish to be,) but the more familiar you are with the principles the better you can identify your needs and capabilities.

Good intelligence must be relevant, timely, and actionable. Relevant and timely is obvious: It is not helpful if you catch word over the radio that there's a lot of fighting in the Donbass while you're in Delaware, and likewise it doesn't help to report "intel documents" you found from the War of 1812. Actionable is a bit harder, and typically affects larger organizations more than small units. Let's say you're trying to get to your family in Cleveland, and you're in Nashville. It is actionable to find out that Cincinnati has large scale unrest and is unsafe to travel through; you can take Hwy64 through Lexington instead. On the other hand, let's say you find out that there are currently 11,730 cars traveling on Hwy71, while there are 9,884 cars traveling on Hwy64. It's relevant; both roads are good options for getting to Cleveland, and it's certainly timely, but can you really act on that information? This is important to keep in mind with SIGINT and is why familiarity with SQL, C, or Python are great assets for any analyst working with such data. For instance, while it is not actionable to say how many cars are traveling down a road, graphing the number of cars per hour over 3 days may help you plan when to start driving in the morning. When performing signals analysis (or any analysis) always work with goal of relevant, timely, and actionable.

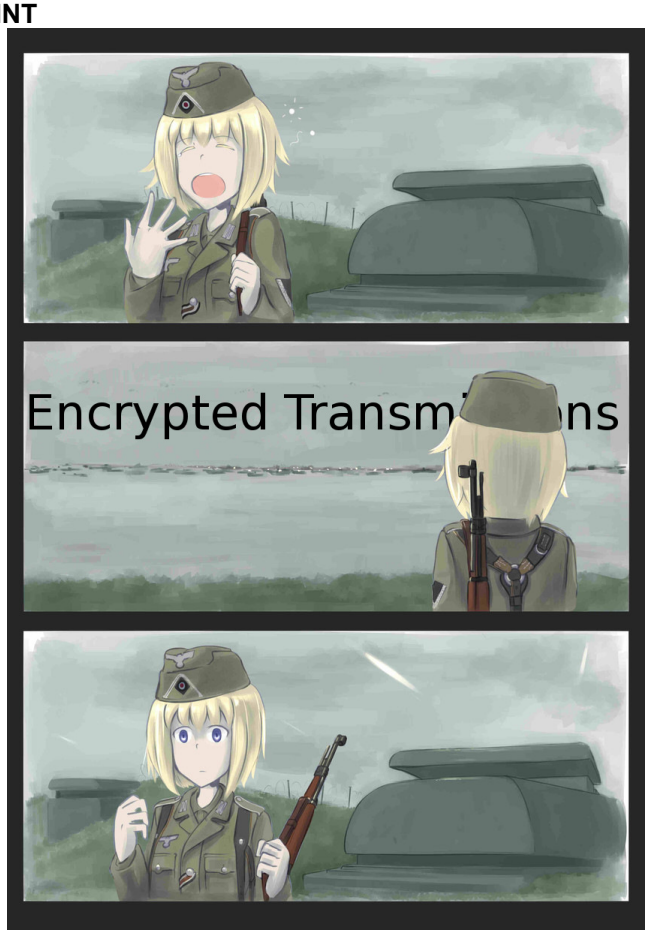
Which Button on the Baofeng does the SIGINT?

Hold the orange button the side. In seriousness, SIGINT comes in too many forms to mention in this guide, even-- or especially-- affordable SIGINT collection is only limited by your imagination. For the purposes of this guide, I'll break SIGINT collection out into 4 categories: Direct COMINT, Obfuscated COMINT, Metasignals, and a few misc capabilities. ELINT will only be mentioned in passing due to my personal lack of knowledge. We will be going more in depth later in this guide.

Direct COMINT

Listening to your fucking radio, plain and simple. No tricks here, but in many cases it's the most useful.

Obfuscated COMINT



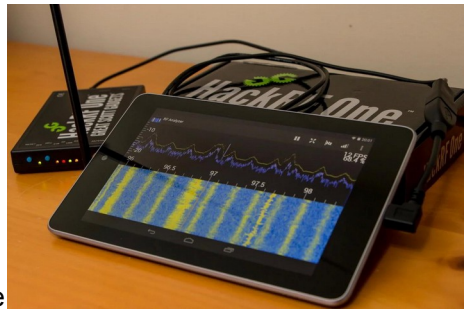
Metasignals

If you aren't lying about having read the Beginner's Guide, then you know that radio signals are transmitted energy modulated to send information. If you have any cyber knowhow then you know that even if you don't have access to data, the packaging can still be useful. Metasignal analysis (made up word) uses characteristics of a signal to derive usable information.

Misc

SIGINT is nice because it lets you operate with your waifu without getting her daki dirty.

Strelok Directed Retardity: The Hardware Foundation



Think back to the first day you got your Baofeng. "Oh wow, 2m AND 70cm bands? AND I can listen to radio? How do they do it!?" Well, get ready to bully your dumb past-self, because we're going to talk about Software Defined Radios (SDRs). An SDR is basically a radio+USB stick that converts the super magic analog radio signals into equally super magic digital radio signals that can be processed by your computer. The benefits are obvious: digital mode demodulation, band monitoring, trunked radio listening, and logging just to list the basics. But wait, there's more! If you thought the Baofeng was wide-band, a typical SDR's bandwidth is contiguous and measured in GHz. Not only that, but SDRs can commonly receive 2-3MHz at once (see

picture), with higher end models reaching 20MHz bandwidth. Holy shit! “But hold on”, you say, “Why spend hundreds of dollars on one SDR when I can buy hundreds of Baofengs and monitor hundreds of freqs?” Well, first of all, unless you’re divorced or funding South American militias you don’t need more than 10 radios. Secondly, you can (and should) pick up an RTL-SDR dongle that fits the aforementioned specs for 20 fucking USD. That’s right asshole, bet you feel dumb with your crates of Baofengs now. If you want to getserious about learning about your local radio environment beyond whatever’s in 2m/70cm amateur, an SDR is a requirement. In fact, every SIGINT category listed above besides Direct COMINT requires an SDR to perform. “Well damn,” you say, embarrassed and indignant, “if the SDR is so great why do people still buy $700 Yaesu transceivers?” The answer to that is simple: Until you break the $250 range, SDRs are incapable of transmitting, and even the ones that do are too shit to even replace your $20 Baofeng. Don’t get me wrong, the HackRF can do a ton of super cool shit, like unlocking car doors, spoofing GSM, or killing diabetic people, but it can only do those things at 0.3W. We’re concerned here with SIGINT over electrical engineering regardless.*

じゃ、聞くましょう！

Now that we got the boring foundational info out of the way, let’s get into the applications and software! For the first two sections I will be speaking from a Windows perspective. Many of these programs work with Wine, or have alternatives available for Linux. Linux users also have much more freedom in the form of Gnuradio Companion (Shown on the center of the cover page)- a GUI for building Python scripts using the Gnuradio library. GRC is an incredibly powerful SIGINT tool that I am too stupid to use. Tutorials are available from GreatScottGadgets.

Direct COMINT

Sure you Baofeng can do it, but your SDR can do it better! The bottom-center picture on the cover page shows how simple it is to listen to a (relatively) large section of the spectrum using your SDR. To listen to transmissions, you’ll need:

Analog	SDR#, RadioReference(OPTional)
Digital	SDR#, DSD+, RadioReference(OPT), Artemis (OPT)
Trunked	2x SDRs, Unitrunker, DSD+, RadioReference(OPT)
Encrypted Digital/Trunked	Decryption keys, a large-diameter asshole for the prison you’ll go to.(OPT)

SDR# (SDRuno & HDSDR also work)

SDR# is my program-of-choice for basic SDR RX. It is highly user-friendly, supports most SDRs, and has a feature allowing you to overlay the band plan over the spectrum. You will be using this to listen to FM, AM, SSB, and CW transmissions, as well as to scan the spectrum for signals of interest.

RadioReference.com

Shown in the top-left of the cover page. *The* go-to for finding active channels, amateur or otherwise. RadioReference features a county-by-county breakdown of municipal, state, federal, amateur, and private frequencies as well as which mode they are broadcast in. Think of this website as part of your radio JIPOE, to be used as a baseline for active frequencies in the area. You can also find Amateur callsigns in a given county on this site.

DSD+

The most user-friendly version of DSD, a program for decoding most digital modes you will encounter in the HF-UHF bands. Simply run the exe, use a virtual audio cable to set the output from SDR# or Unitrunker as the input for DSD+, and set your speakers as the output for DSD+.

Artemis

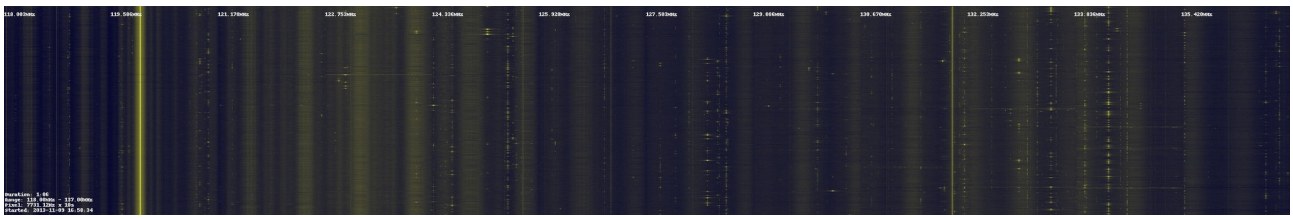
The other program running on the bottom-center on the cover page. This is the offline executable version of the sigidwiki database. If you find a weird waveform while scanning around in SDR# you can search Artemis by signal-width and frequency and compare images of identified signals to determine if it’s something you can decode and listen in on. Also extremely useful for Obfuscated COMINT.

*I will encourage any Strelok interested in low-cost TX SDRs to keep an eye on Nexmon SDR, osmo-fl2k, and related projects. There have been lots of developments in this area, and I would not be surprised if a viable <$50 5W SDR transceiver is released within the next couple years.

Unitrunker

Oh boy, trunked radio. This one is a bit more of a doozy, as shown on the center-right of the cover page. Most government radio networks have transitioned away from simple analog/digital transmissions on a set frequency and have upgraded to trunked systems. Basically, trunked systems have a control station that listen for networked users. When somebody tries to send a message, they transmit to the control station saying “This is Radio #048, I want to broadcast to Group #3”, then the control station assigns one of ~8-10 freqs and broadcasts out to all the users “Any radios on Group #3, listen on 421.111MHz.” I’m retarded, so that might not be exactly how it works, but I’ve been listening to trunked radio for a while with that understanding, so it’s good enough. What you need to know is that you need two SDRs to fully utilize trunked radio: one to listen to the control station telling who is broadcasting and where, and another SDR to actually listen to that broadcast. Keep in mind also that all broadcasts are going to be digital, and a good percentage of them might be encrypted, depending on where you are, so you’ll also need DSD+ running. Now, there’s a fuck of a lot of information just being broadcast by the control station, especially if you can figure out which department is assigned to which group, so if you aren’t interested in listening to a souped-up police scanner then you can get by with a single SDR logging all the data from the control station, but you might want to brush up on your Excel & SQL skills to really turn that data into actionable intelligence.

Obfuscated COMINT



Obfuscated COMINT is less dependent on monitoring individual transmissions and more dependent on volumetric analysis; seeing how activity changes hour-to-hour or day-to-day across the band. For this reason you want to have a good idea of what “normal” looks like in your area. A good tool for this is RTLPower (Pictured), a Linux script for taking snapshots of a given portion of the spectrum over a given time. The nice thing about RTLPower is that it is not limited by your SDR’s bandwidth; even though this picture is only across a couple MHz, RTLPower is capable of logging the entire 1.7GHz band receivable by an RTL-SDR. RadioReference is again useful for finding a baseline of activity, helping you determine when and where on the bands businesses, government agencies, and amateurs are active, so in an emergency situation you can assess, for instance, if emergency services are still organized, as well as notice frequencies not previously associated with any service.

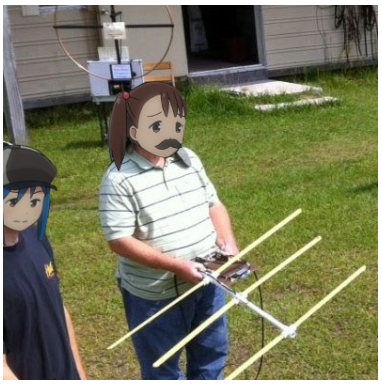
Amateur ELINT: FCCIDs and You

As you’ve studied HAM radios, you’ve probably developed a healthy suspicion of those damn neighborhood kids and their relation to your lawn. Specifically, you might been concerned about what they might be up to with their newfangled drones, but how can you tell when they’re flying that damned thing around? The answer is found somewhere on the product, usually by the serial number: the FCC ID number. Wireless devices sold in the US have to file with the FCC, and the FCC provides them with a manufacturer ID “VK6” for example, and a product ID “IRU600V4” for example. Using this information, you can visit fccid.io and search that ID in order to find everything you could ever need to find that device with your SDR: frequencies used, power output, even manuals, photographs of the products, and schematics in some cases. Fccid.io can also be used to search frequency ranges. Unfortunately with the number of items in the database you’re unlikely to find the exact product emitting on a given frequency of interest, but the site gives you enough information that you can often make educated guesses.

Metasignals

Metasignals analysis dips its toes heavily into the previous category, and the previous category into Metasignals. “Metasignals” for the purposes of this guide is any use of the physical properties of a transmission to get useful data. For instance, comparing reception of two transmissions to figure which one is closer.

Direction Finding:



Oh shit nigger, we FBI now. Well honestly, we've been FBI; now we just FCC. Direction finding has as many techniques as applications: from foxhunting yagis to doppler dishes, and radionavigation to geolocation, with a general trend of more $$$ = higher accuracy. Consider use-cases for all these methods, specifically keeping in mind what information could be gained from locating various types of signals, including BLUFOR signals.

Pic related shows the cheapness and simplicity of our first method: **Foxhunting**. Even a loli can afford PVC piping and a tape measure! In foxhunting, you buy or build a highly directional antenna, and wave the thing around to figure out in which direction the signal is strongest. You can do this on foot or in an open area to approach the signal as-the-crow-flies, or you can get log bearings periodically and map the general source if you're in an urban area and can't go climbing through people's backyard. Another bonus is the ability to listen to analog signals as you track them, what-since the antenna is plugged straight into your Baofeng. A complete Foxhunting kit, Baofeng included, will run you somewhere in the neighborhood of $50, $25 if you have a HT.

Another low-cost method you can attempt is the Multilateration (**Time Difference of Arrival**). This method allows you to triangulate a transmission to within a few hundred meters within 60-120 seconds of transmission, even if the transmission itself only lasts a couple seconds. This is done by using >=3 SDRs with omnidirectional antennae tuned to a given frequency, and transmitting raw signal data to a central computer, which compares when certain portions of the signal were received to estimate each SDRs distance from the transmitter, thus triangulating the signal. The downside of this method is that the triangulation effect occurs best when the SDRs surround the area of interest, have clear reception of the signal, and are not affected by multi-path propagation; triangulation will still be possible, but may produce lower confidence location, take longer, and in cases of multi-pathing, return a false location. A complete TDoA kit will run you ~$25 per SDR, totaling $75. If you don't have 3 computers available to plug the SDRs into, add an additional $105 for 3 Raspberry Pi's. The RaspPis also have the added benefit of portability, making them easy to move and conceal; pictured is a complete TDOA station.

The final method we will be talking about has many names, but we will settle for **Direction of Arrival**. DoA is like Foxhunting in effect, in that it producing a general bearing for a signal, and like TDoA in infrastructure, in that it is a semi-static system connected to a computer. The idea is to connect two SDRs to a single clock (known as a coherent SDR) and use this perfect synchronicity to compare, bit-for-bit, the strength and TDoA of signals on two side-by-side omnidirectional antennae and produce a bearing. You can imagine it as being similar to the way your brain compares the strength of noise between your left and right ear to figure generally where a sound is coming from. Currently a coherent SDR will cost you ~$150 if you buy one online, but during the writing of this guide the folks over at RTL-SDR have announced the KerberosSDR, a coherent SDR featuring four SDRs and featuring software built to just werk, even on a Raspberry Pi (they hope). Current price is $150, which makes this the go-to for coherence, assuming similar performance. This makes me happy, as my current SIGINT project utilizes this method; if all goes well this section will be much longer in the near future.

Sources / Additional Reading

Sources & Additional Reading are not differentiated because I stole things from all these sites.

https://www.rtl-sdr.com/ - Aside from developing SDRs, this site features a regularly updated blog which will help you stay up-to-date on new software and interesting projects, both of which crop up at amazing speed these days.

https://brushbeater.wordpress.com/ - The /k/ component of this /Ω/k/ guide. Lots of focus on working with mobile/handheld transceivers, improvisation, and organizing a signals unit; some articles are even good reads for Streloks without interest in SIGINT. This guy posts on /hamradio/ and gets asshurt about comment sections.

https://www.youtube.com/user/TheChemlife – Videos on Biology / Telecommunications, the former being neat gee-whiz stuff, and the latter serving as a source of ideas. Not the only channel like this on YT, but a start.

Sam Whiting DoA – Not to be recreated in light of KerberosSDR, but a good visulization and general explanation of DoA Direction Finding.

Osmocom – Open-Source cell phone networks, something not touched on in the guide itself for legal reasons (and because I'm too retarded to explain it properly). Relatively advanced, but if you know what you're doing it can be more powerful than anything else in this guide during large-scale unrest. Again, read the warning at the start of this guide 5 times before going into this, because this will get you v& if you're dumb with it.