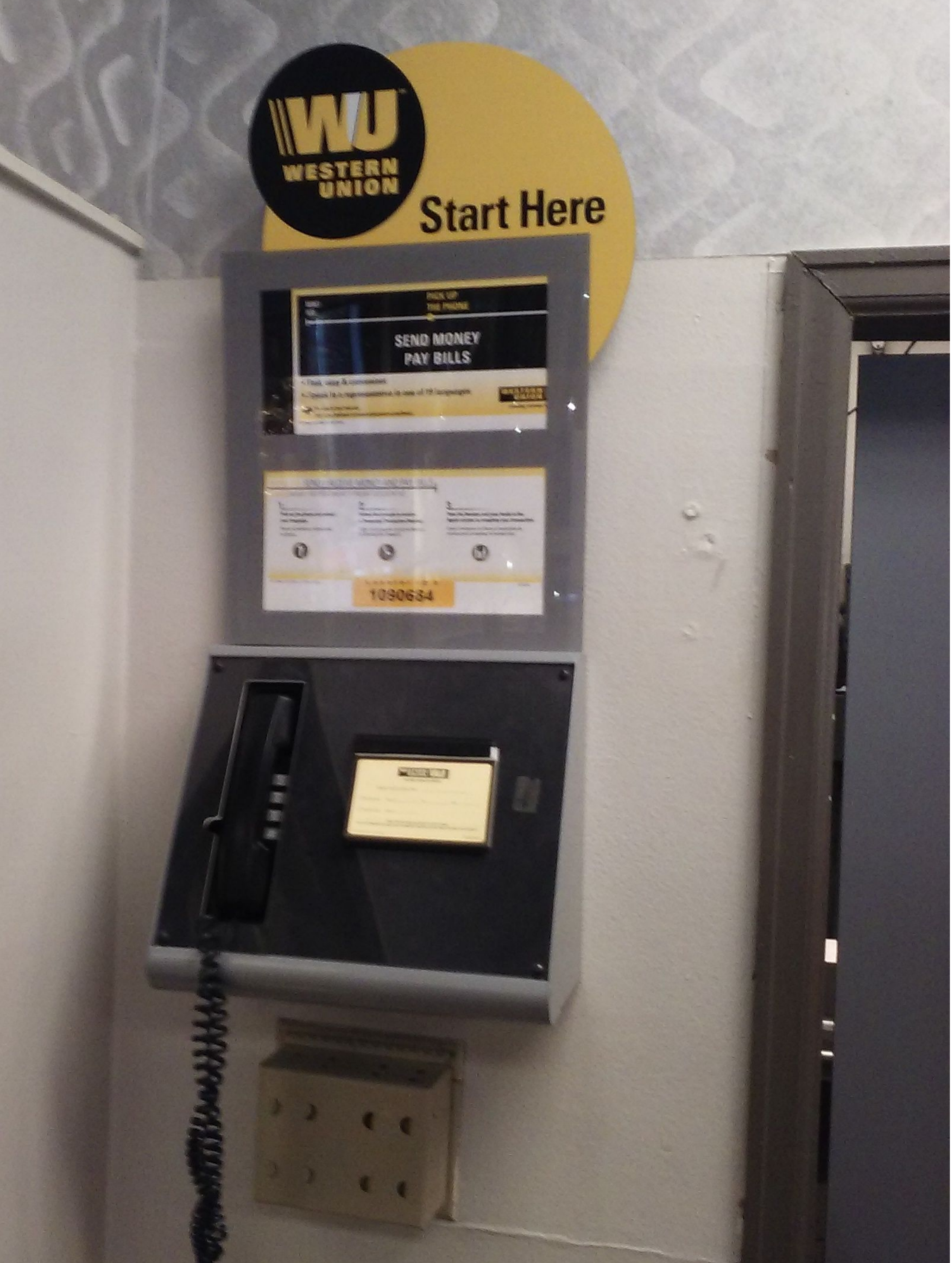
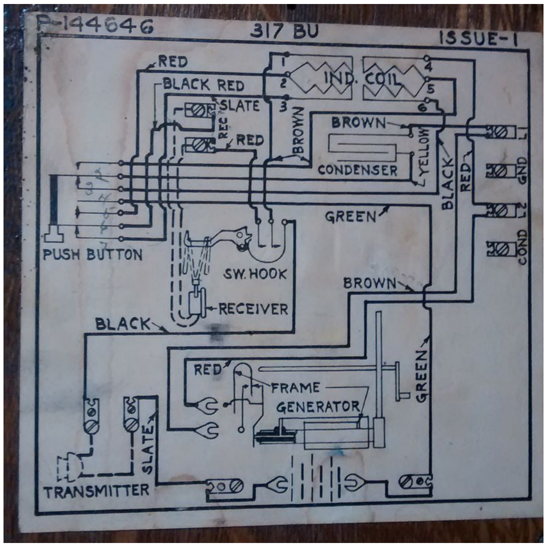
(Cyber)Tek Journal

Issue #29
Edited by Ticom.
est. 1990


WU
WESTERN UNION
Start Here
PICK UP THE PHONE
SEND MONEY
PAY BILLS
1090684



(Cyber)Tek Journal

Issue #29 – Samhain, 2019
Edited by Ticom <ticom.new.england@gmail.com>
http://ticom.livejournal.com/

Please reproduce this fine publication, and spread the gift of самиздат to all who might like to read it.

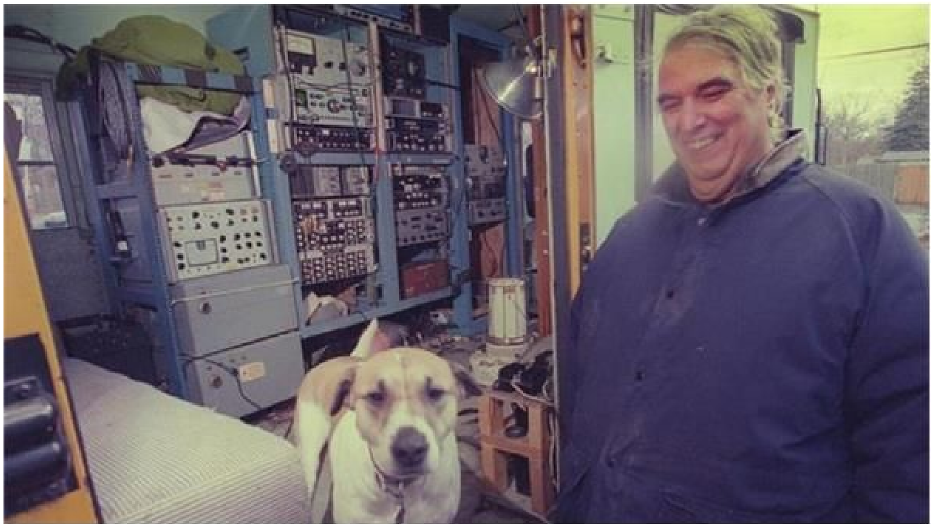
Table of Contents

- (Cyber)Tek Journal is having its 30th Anniversary in 2020, which happens to coincide with the release of our next issue, #30. We're looking for authors, artists, researchers, and fellow travelers to contribute articles, pictures, and what-not. At present the issue scheduled for release sometime around Imbolic, 2020. Please send contributions to <ticom.new.england@gmail.com> sometime before then. Thank you!
- (Cyber)Tek Journal was established in 1990 by Ticom. It was also known as "Cybertek: The Cyberpunk Technical Journal". It is published on a sporadic basis. It traditionally covers a wide range of subject matter revolving around hacking/technology, and self-reliance/preparedness.
- That means you can copy, adapt, spin, fold, mutilate, et cetera, et cetera as long as you give proper attribution to the publication and author. In fact, we'd be much obliged if you did. Please reproduce this fine publication, and spread the gift of самиздат to all who might like to read it.
- In the meantime, my email is <ticom.new.england@gmail.com>, and you can find me at my Livejournal blog that's now old enough to drive: http://ticom.livejournal.com/. That's where you'll find announcements of new (Cyber)Tek Journal issues, and not much else.
- If you're a friend or acquaintance from back in the day, please use this new issue release as an excuse to send me an email and say "Hi!"
- HOPE 2020 is next year. Being back East, and having lost something for way too long, I'm planning on attending.
- This issue is dedicated to absent friends.

R.I.P. Preston Nichols, 1946-2018

About a year ago, I received a message from one of the two surviving Lone Gunmen that Preston Nichols of Montauk Project fame had passed away. (He died on October 5th, 2018.) Preston was an electronics hobbyist and retired engineer from a northeastern defense contractor. After his retirement, he became well known in paranormal circles as the author of a series of books detailing high strangeness on Long Island, NY, in particular the decommissioned radar station at Montauk Point, involving time travel and space aliens. What was not well known is that Preston was also a skilled communications monitoring hobbyist. He had outfitted a small surplus school bus with a load of ex-government Watkins Johnson receiving equipment, and was a frequent anonymous contributor to the New York City Metro area scanner net in the 1990s. This was detailed in my short story, “Preston and the Magic School Bus.”

I attended a few presentations and meetings Preston held in New York for the metaphysical “woo” crowd, and talked with him on the phone numerous times when doing research on my Hacking Invisible Worlds project. I put Preston in the same category as John Titor. The surface premise may have been total fiction, but upon doing research, there was enough factual background data to warrant an investigation. His talk about time travel, space aliens, and esoteric brainwashing aside, Preston possessed a high level of technical skill, and test equipment to match. Like other technological professionals who may have delved in classified areas, he used fiction as a hook to intrigue others into investigating high strangeness and discovering the facts. In the same vein, when I was experimenting with “radio research” in the Hudson Valley, NY region during the “Black Triangle UFO” sightings of the mid 1980s. I detected some interesting radio signals that led me to suspect that the UFOs were actually experimental aircraft. Many, many years later my suspicions were confirmed. This was all done with regular hobbyist gear and consumer electronics equipment, and anyone with the right skills and mindset can do the same today. I managed to see and hear history being made with the test flights of some of the early stealth aircraft platforms, and I hope that you might be able to do something as cool in your future.

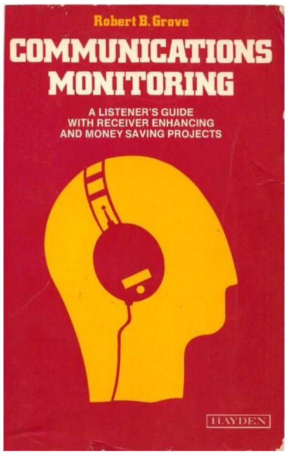


Preston, a friend, and his school bus full of WJ SIGINT Gear.

Setting Up The Lab: Advice For Novice Techies

The novice techie should start small. Don’t go any bigger than a single table-sized workbench in a 10 ft x 10 ft space. That’s plenty to start with. Get some basic tools and test equipment. Start with hand tools: screwdrivers, pliers, wire cutters/strippers, nut-drivers, and wrenches. Basic test equipment you should get right away are a multimeter/VOM, SWR/watt meter good to at least 150 MHz, and dummy load good to at least 150 MHz. After that get a frequency counter, and antenna analyzer or GDO/grid-dip meter good to at least 150 MHz. Then get a signal generator, LCR meter, and spectrum analyzer. At some time later one you’ll want to extend your upper frequency limit to at least 1300 MHz, preferably 3000 MHz. If you can, try to start with an upper frequency limit as high as possible.

When I started, it was with a shortwave receiver, tag sale multiband radio, 20 channel police scanner, and a copy of a book titled **Communications Monitoring**[1], by Bob Grove. Biggest changes over the decades are a wide-SDRs that plug into your computer, and the use of digital modulation versus analog FM, which also can be decoded with software. I’m going to say it now and get it over with. Police scanners are lame and overrated. Get yourself some nice wideband communications receivers instead. The initial frequency range should be 60 KHz. to 2 GHz. or as close as possible to it. I like old school analog tunables with a dial, but SDRs are the current receiver du jour. The HackRF One from Great Scott Gadgets[2] goes from 1 MHz. to 6 GHz. and costs $300. Buy it from Adafruit[3] and tell them I sent you. That takes care of most of the frequency range you want, and it’s easy enough to get coverage down to 60 KHz.


Robert B. Grove
COMMUNICATIONS MONITORING
A LISTENER'S GUIDE WITH RECEIVER ENHANCING AND MONEY SAVING PROJECTS
HAYDEN

As I just mentioned, I like analog tunable receivers, preferably with a dial for manual frequency changes. The nicest ones I’ve owned so far were mil-spec surveillance receivers made by CEI/Watkins Johnson, and a Wavetek SAM (Signal Analysis Meter)[4] I bought for $20 at a hamfest. It covers 4-300 MHz, and was used for testing CATV systems before TV went digital. It has outputs for an oscilloscope so you can look at waveforms and it is as a spectrum analyzer. I started with a couple analog multiband portable and shortwave receivers, and while the big thing now is SDRs, they don’t work well for old-school dial spinning to see what’s out there in the aether. They do have good spectrum display capabilities, and for around $20 the RTL-SDR is a good deal. It’s something I wish I had 30 years ago.

Antennas are what will make or break your receiver set up. Fortunately antennas are easy and cheap enough when you roll your own. You can start by taking your web browser and visiting WA5VJB’s Reference Page[5]. There’s a bunch of good info on that page for cheap homebrew DIY antennas. Another good source of information are books from the late Joseph Carr. His Receiving Antenna Handbook[6] is a good start for the lower frequencies, and the Practical Antenna Handbook[7] has good info for the higher frequencies. The Folkscanomy Ham and Amateur Radio Collection[8] at archive.org has many more useful books for your perusal, but they don’t yet have my favorite Joe Carr title, the two-volume **Radio Science Observing** series.

[1] https://archive.org/details/CommunicationsMonitoring
[2] https://greatscottgadgets.com/hackrf/one/
[3] https://www.adafruit.com/product/3583
[4] http://ham-radio.com/k6sti/sam.htm
[5] http://wa5vjb.com/references.html
[6] https://archive.org/details/JoeCarrReceivingAntennaHandbook
[7] https://archive.org/details/PracticalAntennaHandbook
[8] https://archive.org/details/folkscanomy_hamradio

Wal-Mart Warrior

Numerous times I have mentioned kitting out with common retail sources and consumer electronics equipment. My favored retail department store chain for general shopping is actually Target as they cater to a higher class of lowlife, but Wal-Mart has a better magazine rack, sporting goods and hardware departments, and is more prolific. Common disposables are found cheaper at odd lot and job lot stores such as Big Lots and Ocean State Job Lot, and at the increasing number of “dollar store” chains. When shopping I always take a look in the various clearance sections to see what bargains I can find. I’ve found 12→110 Volt inverters, rechargeable lantern batteries, camouflage clothing (including Frogg Toggs), and Case knives, in addition to more mundane, but still useful items.

vtech
Enhanced Range Digital Audio Monitor
$15.00
Clearance
Hear your baby's every sound
6.0

I was shopping a few days ago, and found the pictured item on the clearance shelf for less than half of its original price. Some of you may look at the picture and only see a baby monitor, and it is one. It is important to see beyond the obvious and look at alternative uses of items, especially if they can be modified/hacked. In this instance we have a source for wirelessly transmitting room audio a distance of 1,500 feet, 500 yards, the distance of five football fields, or a little more than a quarter mile. That’s not all. It has two-way capability, and runs DECT 6.0 technology.

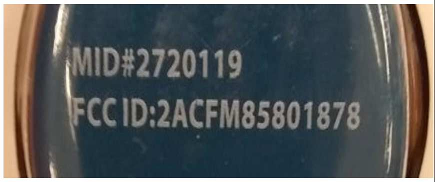
When you see something like “DECT 6.0,” and you don’t know what it is, you should be taking a break from Breitbart and Barnhardt, and doing a Google search. In this instance you would learn that DECT 6.0 is the Digital Enhanced Cordless Telecommunications standard for the United States. You would also learn that it’s a digital FDMA/TDMA system, operates in the 1920–1930 MHz. range, and can support encryption. The big take away on all that is that a common police scanner won’t be able to receive it. That’s pretty good for something that costs all of 15 bucks! You could use this as an inexpensive opportunity to study DECT 6.0 devices. You could also use this to secure and monitor an approach to your camp, or a section of your property such as an outbuilding. Not only would you hear what’s going on, but also be able to project audio to that location if you wanted to communicate with someone approaching or attempt to distract/scare off an intruder. I’m sure you can think of a few ideas.

All department stores have a selection of baby monitors in their infants department that can be used for security/surveillance purposes. Prices start at about $30 or so and go up from there. Some are audio only. Some have low-light video. Many operate on DECT 6.0, but there are other bands that are used as well. Some of them, especially older and low-tier models, can be heard on a police scanner. This particular unit, a Vtech DM1211, was notable because of the really good clearance price and the fact that a police scanner **won’t** hear it. All it takes to find gems like this is to take a quick look around the clearance aisles of your local retail stops during your normal shopping routine. Who knows? You might find some nice 6 Volt rechargeable lantern batteries for $5 each, or a $10 camo Frogg Togg jacket that you can toss in the trunk of your car for when you need something rain proof or earth-toned.

Even cheaper than Wal Mart?!

Once or twice a month I make the rounds of the local thrift stores (Salvation Army, Goodwill, and Savers) looking for interesting electronics devices. Of the three, Savers usually has the best finds. Thrift stores are great because you can find stuff cheap and pay with anonymous cash. On my recent run, I found these two items for less than $10 for the pair. The item on the right was a basic 49 MHz. baby monitor, but with the added capability for intercom operation. Still not bad for $4, considering what we learned from the FMLA stories. The item on the left cost the princely sum of $5, and was more interesting.

At first glance, I knew the second item was a video baby monitor with low-visibility LED illumination for operating in the dark. A quick check of the FCC ID[9], BMWTFY7500C, showed that it runs digital frequency-hopping spread spectrum on the 2.4 GHz. Band. The heart of the unit is an A7125 2.4 GHz. FSK transceiver chip, controlled by what appears to be a variant of an ARM9 microprocessor. Interestingly enough, the A7125 is somewhat older tek, being around since 2007, and has been sold as the heart of an RF module that it used with hobbyist microcontrollers such as the Arduino[10]. Cost for the module is $1.50 in small quantities. Funny what you can find when you stop listening to Alex Jones, go visit a thrift store, and do a simple Google search. You might find a digital video surveillance system with the range of a football field usable for watching your front door, back yard or outbuilding lab.



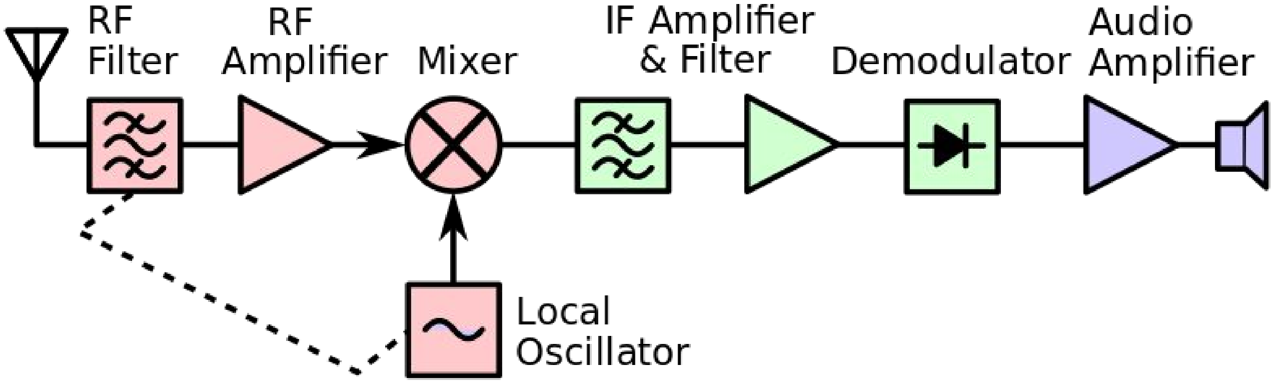
Here's one more for you. I found these in the seasonal section of my local Target department store. They are obviously a pair of radio transceivers marketed at kids playing in the outdoors (radios and the outdoors: two good things for kids in my opinion), and cost all of $7 for the pair. Now at $7 you might as well just buy the things if you're curious (you should be) and have the disposable money. Some of us however, want to learn all we can before parting with our hard-earned cash. What can we determine about these radios before buying them and using test equipment? In this instance, it was a simple matter of looking at the back of the package. On the back of the radios was an FCC ID number. Looking it up, you will discover that these radios operate on 27.145 MHz. under FCC Part 15. That frequency is known as "Channel 15A," and is an R/C toy frequency stuck between CB Channels 15 and 16.

How Does He Do This?! You start by finding sources. Find every junk store and thrift shop within comfortable driving distance. Out here the big two are Savers and Goodwill (in that order), with Salvation Army coming in a distant third. Also keep an eye open for tag sales and flea markets during the warmer seasons. The next thing you do is bookmark the FCC ID lookup website on your (not-so) Smart Phone. Once a month/week/whenever do a run of your used sources. When you find something, find the FCC ID on the item, and run it through the database. You'll at least find the frequency of operation and possibly modulation modes. Sometimes the grantee will have not requested confidentiality of their data, and you'll find schematics with chip numbers. Run the chip numbers through Google and you'll learn what they do. It's that simple.

[9] https://www.fcc.gov/oet/ea/fccid
[10] https://www.elecfreaks.com/estore/2-4ghz-easy-radio-de-a7125-module-rfm06.html

Receiver Local Oscillator (LO) Detection: An Experiment

This article came about as a result of a radio communications discussion on a fairly well-known (among followers of that genre) “threeper/patriot” blog. In the comments section a commentators expressed that he/she (you can’t really tell on the Internet) would be safer than other readers because he/she would only be listening. One of the things about these blogs is that when one makes such a comment, it will be replied to by other readers who believe (correctly or not), or would like others to believe, that they know something the other person doesn’t, and have the irresistible urge to share it publicly. In this case, commentator #2 said commentator #1 was wrong, but didn’t go into any particular detail about it. Incidentally, commentators #2 was correct, but only in theory.



Most modern analog receivers are of a variant of a superhetrodyne design, in which a local oscillator (LO) generates an RF signal which then mixes with the received signal to produce a lower intermediate frequency (IF) that is more easily processed for demodulation. A block diagram is shown above.

Being that the LO is in essence a small emitter, it is indeed possible to not only detect an operating receiver at a distance, but also, if the IF is known, know what frequency the receiver was tuned to. This is nothing new. In World War II and the Cold War, LO detection was used to detect clandestine receivers used by intelligence agents. The BBC is reported to use such technology to detect un-licensed television receivers (TV watching is taxed in the UK). American states in which radar detectors are illegal are known to use a similar device to detect the contraband devices in motor vehicle. Finally, marketing companies have used this technique in shopping centers to produce advertising analytics for radio stations. Better quality (mil-spec) receiving gear is designed to reduce LO emissions, but most consumer grade gear generates enough signal to be heard at a distance. Just how far is the subject of this article.

For the first experiments, I used a Uniden model BC760 Police Scanner. It is a single-conversion design typical of low-tier VHF/UHF receivers. The radio was attached to a stock telescoping whip antenna and tuned to 460 MHz. Using a spectrum analyzer, the LO was easily detected at 10.85 MHz. below the tuned frequency. This is a typical IF for this design. By attaching the Spectrum Analyzer to the antenna port of the scanner, it was determined that the LO was generating an output of -39 dBm or about .0001 milliwatt. Using another scanner receiver with a “rubber duck” antenna, I was able to hear the LO from inside an urban industrial building out to 100 feet. That translates to the parking lot and street in front of the building in an electronically noisy environment. In fact, other emitters from various electronic devices were also heard during the experiment. The setup was then moved to a more rural environment, and the whip antenna was swapped out for a VHF/UHF ham radio unity-gain mag-mount antenna placed on the roof of a car. Using the same detection/receiving gear, in a rural low-noise environment the detection distance went up to 250 feet. That’s almost the length of a football field.

While 250 feet is a respectable distance for such a micro flea-power signal, there are several factors that need to be taken into consideration. The first is that during this experiment, the target receiver tuned to a single known frequency, with a known IF. This made the task of locating the target's LO emission significantly easier than if the target was scanning 100 channels per second on random unknown frequencies from 25-1300 MHZ. At 100 channels per second all a spectrum analyzer user would see is a quick 10 millisecond blip on their screen, which can be very easily missed, especially when the signal is almost down in the noise floor, the bandwidth being searched is high, and you have to hunt for it among all the other intentional and unintentional emitters in the aether. In closing, while this is a thing, it's field practicality in light of modern spectrum conditions is very minimal to non-existent. With that said, there are better things to spend your time worrying about.

How To Experiment, and What To Do, With This

Find an older dual-conversion superhet design scanner. Ther first IF will be somewhere between 10.7 and 10.9 MHz. Radio Shack/GRE is usually 10.7 MHz., and Uniden/Bearcat is usually 10.85 MHz. Sometimes the first IF will be listed in the specifications, if not you'll have to find it. Take the scanner and program in a frequency, say 460.00 MHz. Now take that frequency and subtract the value of the IF. If the IF is 10.85 MHz, then 460.00-10.85=449.150 MHz. With a second receiver, tune to that result frequency, and you should hear a continuous unmodulated carrier. When you tune the target receiver to another frequency, the signal should go away.

The LO output power of the Uniden was -39 dBm, and is a pretty respectable level for receiver testing. That means you can use the LO output of a receiver to test the functionality of other receivers. Using easily-built RF attenuators (I believe the plans are in **Experimental Methods of RF Design**[11]), you drop that signal level down to the noise floor. A good receiver will have a threshold sensitivity of somewhere around -117 to -120 dBm. So, that old police scanner can now double as a piece of test equipment.

For those of who who want to experiment with spread spectrum (which is where you should be going if you want more secure comms), consider that your average police scanner runs at 20-100 channels per second over a spectrum range of 25-1300 MHz. That means the frequency synthesizer is capable of doing 20-100 frequency changes per second over a spectrum range comparable to that of some military commo gear. Let the implications of that sink in for a bit. It is entirely possible, subject to further experimentation, that old police scanners can be used as the starting point for the VFO of a spread spectrum radio. Considering how cheap they are at hamfests, it would be well within the average experimenter's means to play with this, learn something, and maybe develop something interesting.

[11] http://www.arrl.org/shop/Experimental-Methods-in-RF-Design-Classic-Reprint-Edition/

Implementing a Short-Range RF Activity Detector With a Whistler WS1040 Police Scanner (and Maybe Other Models)

Radio Shack released the Signal Stalker radios about 10-15 years ago. They were an improvement from the handheld frequency counters we used for on-scene frequency sleuthing. With a Signal Stalker, you knew the radio activity was close by, up to 1000 feet for a handheld radio, and a mile for a high-powered base station. This was important as nearby signals were of greater concern and interest than distant ones. Unlike a frequency counter, you were able to hear the signal instead of just getting the frequency. Optoelectronics did make a "Scout" frequency counter that would automatically tune an Icom or AOR receiver, but this system cost about $700 compared to the $100 for the handheld Radio Shack frequency counter, or the entry-level PRO-83 Signal Stalker scanner. Many of us relegated the frequency counter to the test bench, and bought a Signal Stalker. Uniden/Bearcat sold one too under the name of "Close Call." You could buy the Uniden model at Wal-Mart. Uniden still offers this feature in certain scanners, and Whistler markets it as "Spectrum Sweeper."

It is well know that hobbyist databases of VHF/UHF LMR frequencies are incomplete, and do not accurately represent the RF activity of a given area. By using Spectrum Sweeper over a period of time you will get an accurate picture of VHF/UHF communications activity in your neighborhood. Driving down the highway you will hear nearby mobiles, and know when truckers go off Channel 19 to have a "private" conversation elsewhere on the 40 legal CB channels or one of the multiple "freeband" channels above and below the standard CB band.

The Whistler WS1040 is a mid-tier handheld VHF/UHF "police scanner" receiver with Spectrum Sweeper, P25, Motorola, EDACS, and LTR trunking reception capability, and Object Oriented memories. It is that last capability that led me to decide that this model, and similar Whistler models with Object Oriented Programming, could be used effectively for detecting short-range RF activity on common low-power simplex frequencies and bands. According to the WS1040 manual:

> *"What is Object Oriented Scanning?*
> *Programming scanning receivers can be challenging, but object-oriented programming simplifies the process by using common conventions for scanning concepts that have common characteristics. A Scannable Object is any defined item that can be scanned or monitored, including:*
> *• Conventional, non-trunkedadio frequencies,*
> *• Talkgroups used on a trunked radio system,*
> *• Radio services,*
> *• Defined searches."*

Previously, non-Object Oriented receivers were programmed for either point searches or sector searches, and not both at the same time. Also, point searches for common services such as CB and FRS/GMRS/MURS required the specific service frequencies to be entered as individual memories. Object Oriented programming allows for all these searches: point, sector, and service, to be combined in a single memory bank.

The Current Primary Target

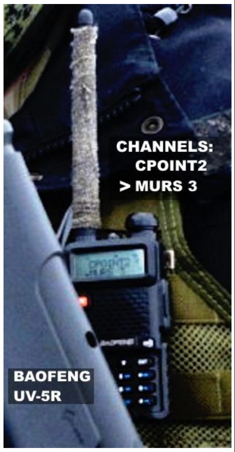
The current primary target is best represented by inexpensive frequency-agile handhelds such as the Baofeng UV-5R. This is a ~$20 VHF/UHF handheld radio with frequency coverage of 136-174 MHz. and

400-520 MHz. They are often, but not always, used on license-free VHF/UHF Part 95 services (FRS, GMRS, MURS), VHF Marine Band, and the Amateur Radio service. However being frequency agile and front panel programmable, users of these radios, and similar models, are capable of appearing anywhere in the radio’s frequency coverage range.

In addition to possible monitoring targets on the VHF-High and UHF bands, there also exists a modicum of activity in, above, and below the HF 27 MHz. Part 95 CB band. Many groups of interest have adopted this frequency range when looking for license-free communications that exceed the range of low-power VHF/UHF handheld radios. Indeed, the communications range of a stock CB radio can reach 20 miles under most conditions, and achieve transcontinental ranges during band openings. The Part 95 CB band consists of 40 channels in the 26.965-27.405 MHz. range, but frequency-agile equipment exists that enable communications from 25 – 30+ MHz.

Observations and Analysis

Most potential targets are known to stay in their safe places when it comes to communications. MURS, FRS, GMRS, and CB see the most use. Nominally smarter groups may operate on common low-power and itinerant business band channels. Amateur Radio sees little overt use due to licensing requirements which are perceived as a threat to privacy and/or OPSEC, and a reputation among the ham community for self-policing their bands. Particularly slick groups may bootleg on any frequency on the coverage range of their communications gear, using short transmissions and changing frequencies on a regular basis. Based on these observations, the following sector search ranges and radio services are of interest:



- CB
- MURS
- FRS
- GMRS
- VHF Marine Band
- 25-30 MHz.
- 136-174 MHz.
- 400-520 MHz.

In addition to these frequency ranges and services, the following frequencies should also be monitored for nearby activity. Some of these are common low-power business and industrial pool LMR frequencies that are found pre-programmed into low-tier and mid-tier handhelds from Land Mobile Radio manufacturers. Others are Part 15 frequencies used for communications, such as the 49 MHz. hands-free radios used before FRS came into existence. Others are common wireless microphone frequencies which see use in low-tier audio surveillance equipment.

35.04 – Itinerant	43.04 – Itinerant	49.830 - Part 15
49.845 - Part 15	49.860 - Part 15	49.875 - Part 15
49.890 - Part 15	151.505 – Itinerant	151.625 - Itinerant, Red Dot
151.955 - Purple Dot	158.400 – Itinerant	169.445 - Wireless Mics

169.505 -Wireless Mics	170.245 - Wireless Mics	170.305 -Wireless Mics
171.045 - Wireless Mics	171.105 -Wireless Mics	171.845 - Wireless Mics
171.905 -Wireless Mics	451.800 – Itinerant	464.500 -Itinerant/Brown Dot
464.550 –Itinerant/Yellow Dot	467.7625 - J Dot	467.8125 - K Dot
467.850 - Silver Star	467.875 - Gold Star	467.900 - Red Star
467.925 - Blue Star		

Implementation

When programming the WS1040 and other Whistler models, a memory object can be a conventional frequency, talkgroup on a trunked system (including a “wildcard” which receives any talkgroup on the system), or a search range. All of these objects are treated the same way, which means you can program the scanner to first scan a range of conventional channels, then monitor a trunked system, and then do a sector search before cycling back to the beginning. Given the capabilities of the WS1040 and the threat profile detailed earlier, the recommended programming of the radio would be as follows:

- The previous 28 frequencies programmed as conventional objects.
- CB Service Search
- MURS/FRS/GMRS Service Search
- VHF Marine Band Service Search
- Spectrum Sweep Search of the following bands:
  - VHF-Low Band (25-30 MHz.)
  - VHF-High Band (136-174 MHz.)
  - UHF Band (400-470 MHz.)
  - UHF-T Band (470-512 MHz.)

This arrangement will enable the monitor to detect communications on common low-power, portable, and license-free services/frequencies out to 1-2 miles, and detect activity on commonly-used frequency bands to a range of 1000 feet for portable radio operations or a mile for higher-powered base stations.

The WS1040 is an FM, AM, and P25 Phase 1 mode VHF/UHF receiver. It will not receive signals below 25 MHz. It also will not receive single sideband signals which are encountered on the CB bands. Finally, the WS1040 will not detect 900 MHz. frequency hopping speread spectrum communications such as those from the Motorola DTR series of radios. This is not earth-shattering news, as previous Signal Stalker and Close Call scanners also lacked HF and SSB reception capability. Nor is there any non-panadapter equipped receiver that will detect FHSS signals. The WS1040 will not demodulate DMR or NXDN signals, although there are higher-tier Whistler Scanners with Spectrum Sweeper such as the TRX-1 that will do so. Should DMR or NXDN be a common mode in your area it would be worthwhile to spend the extra money on a TRX-1.

Previous implementations for short-range RF activity identification using radios such as the Icom IC-R6 or Uniden BC-92XLT required the user to program in upwards of 200 channels to cover common frequencies and bands, or featured a nearby signal detection mode (Signal Stalker) that operated exclusively. The ability of the WS1040 to combine search modes as regular memory objects provides the best of both worlds. Nearby “Spectrum Sweeper” detection will become more important as potential threat elements leave their safe space frequencies and find other places in the spectrum coverage of their Baofengs to operate.

Some Crypto Thoughts

This is a work in progress.

Ah yes, fucking crypto. The thing that is verboten and not talked about on the ham bands, and the same thing that every prepper and paranoid wants to have the perfect form of without the expending any effort to get there. Fucking crypto… I use it regularly with parties I care enough about to use it with. Otherwise, as a high-profile writer in a controversial field who has experienced his fair share of verehrt und angespien, I run everything in the clear with the exception of some ROT13 and ROT47 to protect spoilers and see who's paying attention. Memetic weapons don't work well with crypto, which dilutes the effects of things that once seen cannot be unseen.

"Hört von den sieben vaganten
die ihr glück in der hölle fanden
behangen mit fetzen und schellen
die so laut wie hunde bellen
ihr lachen ist sturm und gewitter
feiern und zechen bis kommt der tödliche schnitter
verehrt und angespien"
-In Extremo

Go visit https://gnupg.org/. This is the website for GNU Privacy Guard. Download the software. Generate a key pair. Convince your "friends" to do the same. Exchange public keys. Set up a private email daisy-chain list. Discuss things. Share Janet Reno jokes. Forget that last one, de mortuis nihil nisi bonum, and you have better things to do with your time. The problem with crypto is that most people don't want to spend the time and effort to do it right, and that its obvious use leads to increased scrutiny from certain sectors. It is general knowledge in certain circles that if certain entities are interested in your comms, and you use secure crypto, then other, more tradecraft-esque techniques will be used to monitor your traffic.

If you overheard someone talking about "yumblatz," you would have no idea what they were talking about unless your kid or grandkid was a fan of a certain children's show. If they talked about getting yumblatz and you observed them walking into a diner and ordering a hot dog, then you might reasonably guess that a yumblatz is another word for a hot dog. If you are of a certain preferable mindset, you might Google it, and would find out it's from a Mickey Mouse cartoon show. If you were monitoring a RTTY circuit and saw the text "XUSYS OISKY ODIRL SIERT TIRES" you likewise would have no idea what was being transmitted, but if you were listening to a police dispatch channel and the dispatcher told a unit to "33 the station," then you could guess that means the dispatcher would like the officer to call the station via telephone. Most of you are familiar with terms such as "QRZ," "QTH," "10-4," and "10-20." Those are codes that are known as "brevity codes which are used to shorten a transmission time by substituting a simple word or designation for a longer sentence. Brevity codes are not used for cryptographic purposes, but instead as a shortcut to make communications quicker. "Q-Signals" used in amateur and commercial shortwave radio, and "10-codes" used in public safety and CB are good examples of brevity codes. In addition to brevity purposes, codes can also be used for cryptographic purposes. The difference is that unlike brevity codes, cryptographic code meanings are not distributed outside an organization, and treated as classified information.

Cryptographic codes are unbreakable when used properly. There is no way that one, for example, would know that “THUNDERBIRD[12]” is a codeword for whatever. However, if a monitor is paying attention to other activity and indicators in additon to communications monitoring, and codes are not changed regularly, then it is only a matter of time that the monitor will figure out that THUNDERBIRD means XXXXXXXX when that codeword is used and XXXXXXXX happens. Likewise, if codewords for particular meanings are not chosen randomly, and in particular if the codeword has some relation to the meaning, then the meaning of the codeword can often be inferred and cracked. For example, if I heard a group of individuals on MURS Channel 3 talk about meeting at “Checkpoint Delta”, and five minutes later a group of vehicles sporting “Oathkeeper” and “III%” bumper stickers show up at the local diner, I might guess that “Checkpoint Delta” is the local diner, especially if I hear and see the same communication → action more than once. If they acted in a rude and boorish manner, or otherwise became worthy of attention for whatever reason, further intelligence information could be collected. At the very least they would be worth watching simply because they’d probably make excellent coalmine canaries, and subjects for my next “Don’t Be That Guy” article.

The best crypto systems don’t look or sound like crypto systems. Back in the pre-cellphone days, I knew a group of good old boys who where allegedly involved in all sorts of interesting business, and they used CBs for all their communications. If you listened to their communications, it sounded like legit, everyday conversation. They eventually switched to cellphones, but their crypto system would have transitioned over nicely. One of the hallmarks of a good crypto system is that it can easily transition from one medium to the other, like the old Chuck U. Farley Pirate Paging Network.

Everytime I listen to the “nonsense” on “Superbowl” CB Channel 6, I wonder just how nonsensical it really is. Let’s take another look at the “nonsense” sentence: “Renfield, it’s time to walk the monkey.” Let’s break this sentence down to see what is actually being communicated.

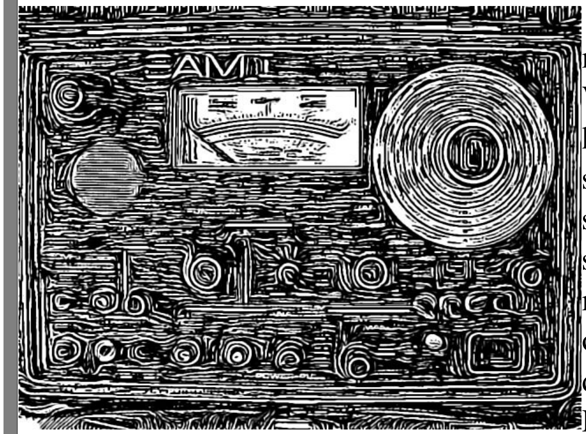
- Renfield – The transmitting party is specifically addressing a particular party, or maybe a group, identified as “Renfield.”
- It’s time – The transmitting party is conveying that a specific condition exists.
- To walk – The transmitting party is conveying a specific action that needs to occur as a result of the condition.
- The monkey – The transmitting party is conveying the recipient or subject of said action.

A similar message can be conveyed with the sentence, “Honey, please feed the dog tomorrow morning.” If I took that second sentence and encrypted it with ROT47, as a simple example, it would come out as “w@? 6J[A=62D6 7665 E96 5@8 E@>@CC@H >@C?:?8]” and be pretty obvious as an encrypted message. One might even be tempted to run some quick simple cryptoanalysis techniques on it to see if it’s something simple and easily cracked. Since ROT47 is a simple and very common mono-alphabetic substitution cipher, its plaintext will be sussed out in short order.

Let’s go back to the original sentence. “Renfield, it’s time to walk the monkey.” This is written in plain English, but apparently would mean nothing unless your name is Renfield and you are tasked with taking care of a monkey. But the reality is that the receiver doesn’t have to be named Renfield, and doesn’t have to walk his monkey, if you catch my drift.

[12] What’s the word?

Sector Search Thoughts



I like analog tunable receivers, and police scanners with a dial for manual frequency changes. The nicest one I've owned so far was a Wavetek SAM (Signal Analysis Meter) I bought for $20 at a hamfest. It covers 3-300 MHz. and was used for testing CATV systems before TV went digital. It has outputs for an oscilloscope so you can look at waveforms, and use it as a spectrum analyzer of sorts. I started with a couple analog multiband and shortwave receivers. The big thing now is SDRs, but they don't work well for old-skool dial spinning to see what's out there in the aether. They do have good spectrum display capabilities, and for ~$20 the RTL-SDR is a good deal. It's something I wish I had 30 years ago.

You really should periodically tune through the coverage bands of your receiver every once in a while, and especially when you are new to all this, or have moved to a new area. Downloading lists from Radioreference is all fine and dandy, but as I have previously pointed out those lists are inadequate when it comes to finding out just what you are able to hear from your QTH, with the system (antenna in particular) you have. Most receivers have frequency coverage of 148-174 and 450-470 MHz. The frequency ranges of 148-174 and 450-470 are known as the VHF-High and UHF Land Mobile Radio (LMR) bands respectively. They are adjacent to the 2 meter (144-148 MHz.) and 70 centimeter (420-450 MHz.) Amateur Radio bands. Being the two most popular local-coverage ham bands, you may wish to also include them in your band search. Start with those two ranges as they are the most active in any given area. Start at one end of each band, and search your way to the other.

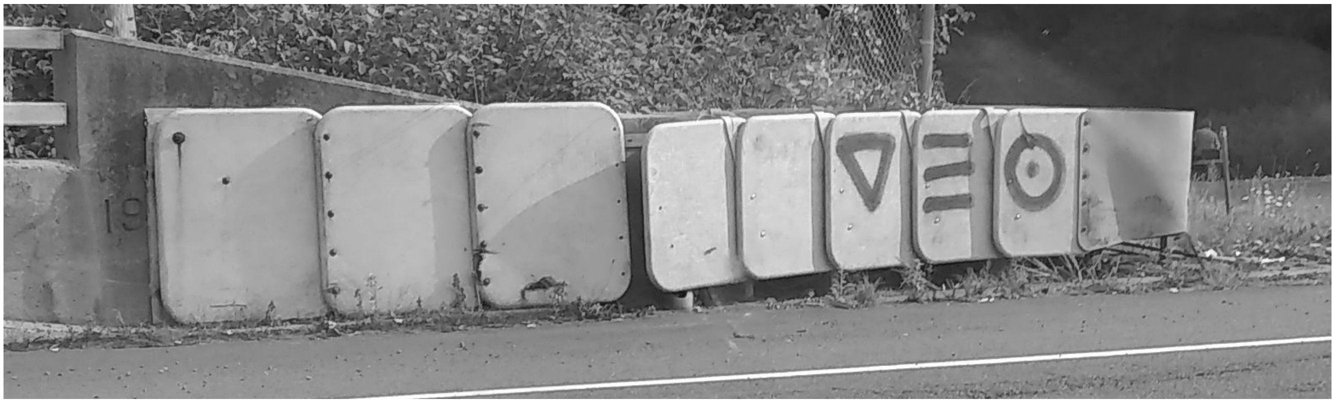
What's the frequency, Kenneth? Note down every signal you find, and include a few notes on what you heard. You should copy down the PL/DPL/NAC code as well, if there is any, and what type of modulation the signal used, whether it's AM, FM, P25, DMR, NXDN, data, or something else. You should always keep a notebook and pen at your monitoring post, and make frequent use of it. After a monitoring session, you can then visit the FCC and radio hobbyist sites to research what frequencies you've found.

What will you hear? Generally speaking, with the receiver's stock antenna you will be limited to a 10-15 mile radius depending on the terrain. If you are situated above average terrain, and have an antenna on your roof, you can expect upwards of 50-60 miles reception distance on the VHF-High band, and shorter distances on UHF. Here is where noting PL/DPL/NAC codes come in handy. If you have a reception range of more than 20 miles, you will probably hear multiple users on the same frequency. PL/DPL/NAC codes, along with careful listening, will help you distinguish between the different users. Take a common frequency in the public safety pool, 155.205 MHz. for example. This was previously allocated to the "Special Emergency" service which included ambulance and school bus services. In any given area, you can expect to hear at least 2-3 different users on that frequency, and each will have their own PL/DPL/NAC code.

Once you have spent some time searching VHF-High and UHF bands, you should then see what signals you can hear on the 30-50 MHz. VHF-Low band. This band offers longer reception range than the other two bands, especially in rural and mountainous areas, but a properly resonant antenna will be required to maximize your reception capability. During the occasional band openings, however, expect to hear signals across the country. This is where writing down PL/DPL information is necessary, as you can and will hear signals from across the country.

Signs

I was driving to work one day, and saw these symbols spray-painted on a guardrail:



At first I thought it was some graffiti artist's tag, but then I saw the same set of symbols painted on highway bridge spans in spots that would require some form of assistance to reach. Based on that observation, I concluded that this is a survey or inspection mark placed by the contractor working on the particular piece of highway infrastructure. I don't know what it might mean exactly, but regardless it serves a purpose in communicating something to those in the know, who work in that particular field. It, however, made me think a little. Around the same time I was reading the news feeds and read a story about the U.S. Navy practicing with the use of air-dropped bean bags for communications between aircraft and ships. This old-skool technique was being re-adopted to help defeat the SIGINT resources of potential opposing forces, and shows all the appliance operators that the lo-tek stuff is still being used. Let's just say that it may not be a coincidence that the later Sparks31 classes put a little more emphasis on lo-tek commo techniques.

When the Sparks31 classes were being conducted in the Rockies, a simple cardboard sign was placed at the last intersections leading to FTX sites. It simply had "S31→" written on it, with the instructor's handwriting being what it is, some people may have interpreted it as "531→." Regardless, all the students attending knew, from being told previously, that following the "S31→" signs would get them to the FTX location. Most other people seeing these signs would have ignored them as being of no relevance, or dismiss them as directions to a private party or other event. If the sign said "YARD SALE →," then we would have had a few more visitors show up looking for cheap stuff to maybe buy. The author has previously written about The Wander Society, created by author Keri Smith. Ms. Smith's books, in particularly **How To Be An Explorer Of The World**, have been noted as recommendations for the budding dystonaut, and mentioned in Sparks31 classes, as they very nicely teach observation and recording skills. The Wander Society's symbol could be described variously as either a lightning bolt or the letter "Z." It serves as a recognition symbol among those who have read the book and embraced the philosophy written therein.

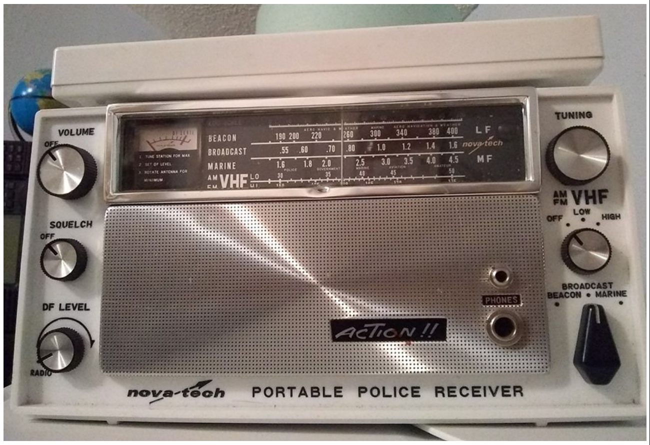
When you are out and about, look for signs that others may have posted along the road. Think about them, and think about how much thought you, or maybe someone else, would normally give to a tag sale sign dated last weekend that someone may have left stapled to a telephone pole, or what *appears to be* some graffiti artist's tag. Think about how can you leverage the average person's lack of attention to their surroundings with mundane-appearing communications to securely and discretely send a status report or initiate a plan of action.

Communications Monitoring: Putting It All Together and Making It Work

Start with a NOAA All-Hazards radio. Program in your SAME code and let it sit. When a hazardous weather warning or other situation becomes worthy of official notice, you'll find out about it. You can also get current weather conditions and forecasts by listening to the NOAA Radio Service. These units are pretty much plug and play, so there isn't much else that needs to be said about them.

The second item you shuld be getting at the same time is a decent AM/FM/Shortwave portable. It should have feature a BFO (Beat Frequency Oscillator) so you can receive SSB and CW signals, but if you can't find one right away, don't worry about it for now. You'll upgrade later eventually. It would also be nice if the radio has an external antenna connector so you can attach a proper antenna. Again, not necessary for your first radio, but nice to have.

My current portable is an early 1990s vintage Radio Shack DX-375. I bought it on clearance to serve as a source of entertainment when working night shift doing security after I came off active duty. As it turned out, the DX-375 is a top AM BCB performer which is what I mostly use it for. It's paired with a Grundig AN-200 Medium Wave Loop Antenna. This combination will receive AM broadcasts out to 500 miles most nights. The current popular entry-tier portable AM/FM/Shortwave radios are Tecsun and CountyComm. Those monitors wanting a slightly higher-tier unit can choose between Sony, Sangean, and Grundig. Then there is always the vintage equipment route. I visited a hamfest last October, and searching among the tailgaters I found this late 1960s/early 70s vintage Nova-Tech receiver for $20! The first station I heard tuning through the bands with it later that evening was Zoomer Radio, CFZM AM 740 KHz. out of Toronto, Ontario, Canada. The second station I heard for a Low Frequency navigation beacon in Quebec. The bar on top is actually a directional ferrite loopstick antenna that you can take bearings with for radio direction finding on the AM and longwave bands. It also covers VHF high & low bands, and shortwave to 5 MHz. The front end on this receiver is ***hawt,*** and the antenna helps null out noise sources and co-channel stations so you can hear some decent DX. I'd even hazard the opinion that it picks up a little better than the DX-375. This is one of the reasons I visit hamfests,



Once you get your AM/FM/SW portable, you should spend every night for a week or so surfing the bands to see what stations you can hear. For FM, concentrate on the frequency range of 88-92 MHz. because that's where all the good stuff will be. Once you get a station ID (its callsign) you can then Google it and you will probably find a station schedule online. NPR is good. College stations are better. You're not looking for an echo chamber. You're not looking for someone on "your side" to give you a distorted and watered-down version of bad it is. You want news and beginning trends straight from the horse's mouth.

AM Broadcast Band is best scanned through twice: once during the day and once at night. You'll get your local stations during the day, and at night the band goes long and you'll hear stations 500+ miles away. The more interesting shows are on at night. AM is the undisputed home of "conservative" talk radio shows. They will be the inverse of what you'll generally hear on the low-end of the FM band, and the two will balance each other out if you pay attention. **That** is how you properly collect information.

I wish I could say nicer things about US domestic shortwave broadcasters, but there are way too many perverts and con-men masquerading as religious pundits occupying the aether. The overseas stations are better. Personal favorites are Radio Havana Cuba and their opposition, Radio Miami International (Se habla Español is a bonus here), WBCQ, and WTWW. All of these stations have their schedules posted online. Of the four, I'd say the best is WBCQ on weekend evenings. When tuning the shortwave spectrum, 1.7-7.0 MHz. works best at night, 15-30 MHz. is better during the day, and 7-15 MHz. offers good performance 24/7.

With that said and done, go visit http://wa5vjb.com/references.html and build up a Yagi antenna for the TV/HDMI monitor you're using for your Raspberry Pi. Then visit the FCC DTV Map site at: https://www.fcc.gov/media/engineering/dtvmaps. Find your nearest PBS/public television station and aim your antenna at it, or install a rotor on your antenna so you can aim at different stations in case you have PBS and another non-commercial public television station in opposite directions. Put your TV into scan mode and see what stations you can receive. Just like with radio, the stations will have an online presence where you can find a schedule.

If you are a smart parent, you will only let your kids watch PBS. I have evaluated and analyzed both PBS and commercial broadcash television for the past 15 years with the help of a like-minded psychologist, and made an interesting discovery. All the "brainwashing" that is alleged to occur with television programming happens on the commercial broadcash stations, and is all about marketing. PBS actually has educational programs that teach critical thought, problem solving, and personal interaction. You know, things that will be needed in the future.

Now that your broadcast and shortwave reception needs are taken care of, examine your VHF/UHF Land Mobile Radio (LMR) monitoring needs. If you visit http://www.interceptradio.com/ (where all the cool kids hang out) and http://www.radioreference.com/ (run by fellow cool kid and author Lindsay Blanton) you will be able to find out what type of police scanner you'll need to monitor your local public safety an business/industrial LMR users. In most places this will mean trunked system tracking with P25 and DMR demodulating capability. When it comes to scanner brands currently in production, you have a choice between Uniden and Whistler. I prefer Whistler. Your mileage may vary.

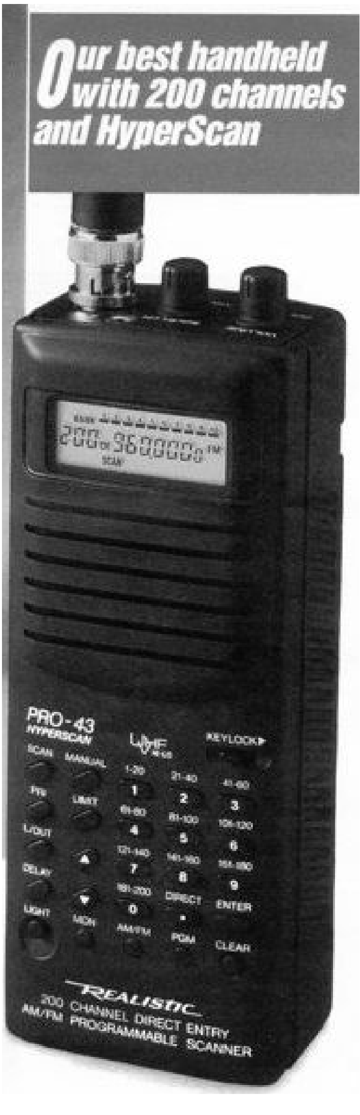
While scanner programming software is all the rage, you should learn how to program your scanner manually. If you are even moderately active with VHF/UHF communciations monitoring, you will be changing around your programming frequently until you get it a way you like. Start with your local police, fire, and EMS departments, local state police/highway patrol barracks, and county sheriff. From there you might add local critical infrastructure (utility companies and transportation), and the public safety agencies from neighboring juristictions.

The easiest scanner to get up and running for the complete beginner is the Uniden Home Patrol. I used to recommend it, and don't anymore. The reason is that they require frequent programming updates via an online database, and you will be at the mercy of the users who contributed the information for your area. You are far better off buying a scanner you have more programming control over, learning how to use it, doing the necessary frequency research for your area, and programming it yourself.

The most important VHF/UHF LMR frequency or talkgroup (TG) you will need to monitor is your local Fire Department's dispatch channel. Those of you in less urban locales will be more fortunate in that it will be a single frequency using unencrypted analog FM. It may also be a countywide or regional frequency as well. The local fire department is the designated first-responder for most disasters you actually have to worry about. After the local FD dispatch, program in any local public safety car-to-car, “on scene” and “tactical” frequencies/TGs you might have. These are especially useful if they are conventional simplex frequencies because then you will know that something is going on in your immediate area, which may be worthy of your attention and interest. The third thing you should add are all regional interoperability and mutual-aid frequencies and TGs because they will let you know about major situations that require a multi-jurisdictional response. They will enable you, if you wish, to ignore minor problems occuring locally and save your attention for major ones. This is especially useful if you are lone-wolfing it. Now add the dispatch and operations channels for your police department, county sheriff, and state police/highway patrol. These are more useful for long-term strategic monitoring, which is something you are probably not starting out with. Finally, add the frequencies/TGs of things like transportation infrastructure, forestry, DEP/EnCon, public works, EMS, et. al. There is a lot of mundane traffic on these frequencies, but they help complete the picture for long-term strategic monitoring goals. If this looks like a lot to do, it is. Start out basic and small at first. Concentrate on short term tactical monitoring goals and work your way up to long-term strategic monitoring. Hopefully along the way you can find a few like-minded individuals and out together a monitoring group with each member concentrating on a certain aspect, and then pooling the information for a more complete collection and analysis effort than what just an individual would be able to do.

If you live in an area with a significant conventional analog LMR presence, go look for cheap late-model scanners at hamfests, tag sales, flea markets, pawn shops, et al. Even basic 8-Channel early 1980s vintage units can be used to priority monitor things like the local county fire dispatch channel, or mutual-aid channel. These units enjoy little demand from the majority of less-experienced monitors, and are usually only of interest to collectors of vintage gear. As such most can be purchased for a minimal amount of money. One of the primo units, shown here, is the famous Radio Shack PRO-43 handheld scanner from the early 1990s. The same hamfest where I just visited and bought the Nova-Tech also had a Radio Shack PRO-2042 scanner for sale at one from the tailgaters. It was equipped with the Optoelectronics OS-535 computer interface board, and also came with a laptop that had the appropriate scanner software on it. The dude selling it only wanted $100 for it. I passed it up in favor of a late-model Hammurland SP-600 variant that likely resided for a while at Vint Hill. At the end of the hamfest, despite the dude willing to part with it for less than $100, the whole setup remain unsold.

In the big rush to hear “everything,” novice monitors miss a lot by starting with a quantity of communications systems that is way beyond their ability to keep track of and extract useful information from. By starting small and keeping it local, one is able to more easily keep track of activities in an area that is most relevant to their needs and concerns. Don’t be afraid to minimize your scope of monitoring activity all the way down to one or two channels or talkgroups. By concentrating on your local fire department’s dispatch channel, and/or the primary operations channel of your local police department, you will gain immense insight on the happenings in your community, and be very well informed of local affairs.



Analytics

I recently was asked how one “determines the truth of a narrative.” That falls into the realm of analytics, taking information collected from various sources and turning it into useful intelligence. Basic investigative procedure 101 teaches how to collaborate statements and testimony to see if a party is telling the truth or not. SIGINT, HUMINT, IMGINT, MASINT, and all the other intelligence disciplines work together to show one the big picture and produce good intelligence product. Worried about concentration camps? If it were to happen, you’ll start noticing things. Additional personnel will be deployed into an area. Locations large enough to house large quantities of people will be commandeered and obvious modifications will be made to them. The state PSYOP apparatus will be operating in full force. Increased logistics activity to feed people on both sides of the fence will be apparent. Cordon and search activities in targeted neighborhoods will commence. You will see an increase in radio traffic. In the early 1990s, it took a whole brigade combat team along with local and state police forces to pacify a one square mile area in Los Angeles, and all the government wanted was for the locals to stop rioting. Now just think what it would take to detain a whole country of 3,000,000+ heavily-armed, pissed-off people, many with outdoor, hunting, and military experience. From a military standpoint, it would be (almost) impossible. From a social or psychological standpoint? I’ll let you decide. What if the latter was successful, would the former be easier? Listed below are the URLs to some manuals and papers in PDF format. All contain educational information that you will find useful in the future.

US Army Field Manual FM 19-20, Law Enforcement Investigations
https://www.bits.de/NRANEU/others/amd-us-archive/FM19-20%2885%29.pdf

US Army Field Manual FM 34-3, Intelligence Analysis
https://archive.org/download/milmanual-fm-34-3-intelligence-analysis/fm_34-3_intelligence_analysis.pdf

US Army Field Manual FM 34-60, Counterintelligence
https://archive.org/download/milmanual-fm-34-60-counterintelligence/fm_34-60_counterintelligence.pdf

DEA Intelligence Collection and Analytical Methods
https://archive.org/download/intelligencecoll020331mbp/intelligencecoll020331mbp.pdf

TM 32-250 Fundamentals Of Traffic Analysis
https://cryptome.org/2015/04/nsa-traffic-analysis-1948.pdf

A Collection of Writings On Traffic Analysis
https://www.governmentattic.org/8docs/NSA-TrafficAnalysisMonograph_1993.pdf

Basic Communications Information
http://militarynewbie.com/wp-content/uploads/2013/11/US-Army-electronics-course-Basic-Communications-Information-IT0301.pdf

So to go back to the truth of a narrative. The “truth” in this instance may be whether or not an event occurred, but more important would be how relevant it is to one’s situation, and what the result/consequences might be regardless of whether it happened or not. Let me end with a caveat on Open Source Intelligence. Make sure you go straight to the source, and check for supporting indicators. I have noticed that politicians on both sides of the fence like to say one thing and do another. Recent example being “pro-RKBA” Donald Trump’s bump-stock ban, more than one statist Republican politician suddenly finding religion and becoming a libertarian, and a few rural Democrats who talk about being pro-gun control and yet vote the other way when the time comes. My advice in that instance is to look at the person and not necessarily their party.

A Renaissance Person’s Bookshelf

This list was started about 10m years ago. It is not complete, but it is a good start. There is a wide range of stuff in it from all over the spectrum. The list also acts as a filter. When some ass-clown says “You shouldn’t read such-and-such because of blah-blah, and blah,” you know something about them. You don’t have to agree with everything in the Philosophy, Religion, & Politics section. You simply should read all of it so you know first-hand who some of the major players are in the land where faith often substitutes for reason.

Once you have gone through this list, add to it with titles you discovered on your own. You have previously been given instructions on how to randomly select books for exploration at your local library. A similar system can be devised for use at bookstores. Use it when you are feeling lost, or just want to add some interesting randomness to your journey. Don’t be surprised or upset ~~if~~ when some of your preconceived notions are shattered. Evolution, besides being scientific fact, is a good thing. You wouldn’t be here otherwise. This is a lot of books, and will take you a really long time to finish this list. Where you start is not important, but I’d first pick a book on a topic you know nothing about.

D.I.Y. & Science

- Boy Scientist, by Popular Mechanics
- Caveman Chemistry, by Kevin M. Dunn
- Complete Metalsmith, by Tim McCreight
- Machinerys Handbook
- Makeshift Workshop Skills for Survival and Self-Reliance, by James Ballou
- Reflections on the Motive Power of Fire, by Sadi Carnot
  ISBN 978-0486446417
- Shelters, Shacks, and Shanties, by D.C. Beard
  ISBN 978-1616081348

Electronics

- ARRL Handbook
- Boy Electrician, by Alfred Powell Morgan
- Electronic Sensors For the Evil Genius, by Tom Petruzzellis
- Engineer’s Mini Notebook, Electronic Sensor Circuits and Projects, by Forrest M. Mims III
- Engineer’s Mini Notebook, Science and Communication Circuits and Projects, by Forrest M. Mims III
- Experimental Methods in RF Design
- NEETS (Navy Electricity and Electronics Training Series) volumes
  Download from http://www.phy.davidson.edu/instrumentation/NEETS.htm
- Pirate Radio and Video Experimental Transmitter Projects, by Newton C. Braga
  ISBN 0-7506-7331-1. Complements of HD

- Electrical Engineering 101, by Ashby
- Sourcebook of Electronic Circuits, by Markus

Computers

- The UNIX Operating System, by Kaare Christensen
- The Art of Unix Programming, by Eric S. Raymond
- Software Tools, by Brian W. Kernighan and P.J. Plauger
  ISBN-10: 020103669X, ISBN-13: 978-0201036695
- C Programming Language (2nd Edition), by Brian W. Kernighan and Dennis Ritchie,|
  ISBN-10: 0131103628, ISBN-13: 978-0131103627
- Lions' Commentary on Unix, by John Lions, ISBN-10: 1573980137, ISBN-13: 978-1573980135
- The Unix Programming Environment, by Brian W. Kernighan and Rop Pike,
  ISBN-10: 013937681X, ISBN-13: 978-0139376818
- Practical Cryptography, by Niels Ferguson and Bruce Schneier,
  ISBN-10: 0471223573, ISBN-13: 978-0471223573

Spook Territory

- The Big Brother Game, by Scott French
- The Craft of Intelligence, by Allen W. Dulles
- Cryptanalysis: a study of ciphers and their solution, by Helen Fouché Gaines
- U.S. Army Field Manual FM 34-40-2, Basic Cryptanalysis
  Download from http://www.umich.edu/~umich/fm-34-40-2/.

Fiction

- Atlas Shrugged, by Ayn Rand
- The Fountainhead, by Ayn Rand
- Naked Lunch, by William S. Burroughs
  ISBN 978-0802140180
- To Kill A Mockingbird, by Harper Lee
- 1984, by George Orwell
- Fahrenheit 451, by Ray Bradberry
- Animal Farm, by George Orwell
- Brave New World
- Flow My Tears, The Policeman Said, by Phillip K. Dick
- A Scanner Darkly, by Phillip K. Dick

- Pattern Recognition, by William Gibson
- Spook Country, by William Gibson
- Zero History, by William Gibson
- Catch-22, by Joseph Heller
- Revolt in 2100, by Robert A. Heinlein
- The Moon Is a Harsh Mistress, by Robert A. Heinlein
- Stranger In a Strange Land, by Robert A. Heinlein
- A Clockwork Orange.

Homesteading and Self-Reliance

- Basic Butchering Of Livestock & Game, by John J. Mettler, Jr. D.V.M.
- Boy Scout Fieldbook
- The Chernobyl Syndrome, by Dean Ing
- Down Home Ways, by Jerry Mack Johnson
- Earthwise American Indian Traditional Uses of Native Northeast Trees, by E. Barrie Kavasch
- Edible Wild Plants, A North American Field Guide, by Thomas S. Elias & Peter A. Dykeman
- Five Acres & Independence, by M.G. Kains
  ISBN 978-0486209746
- Foxfire series
- Live Off the Land In the City and Country, by Ragnar Benson
- Long-Term Survival In the Coming Dark Age, by James Ballou
- Native American Crafts & Skills, by David Montgomery
- Nuclear War Survival Skills, by Cresson Kearny
  ISBN 978-0942487015
  Download from http://www.nukepills.com/docs/nuclear_war_survival_skills.pdf
- One Acre and Security, by Bradford Angier
  ISBN 978-1572233942
- Starving The Monkeys, by Tom Baugh
  ISBN 978-0982543108
- Woodcraft and Camping, by “Nessmuk”
  ISBN 978-1486149896
- Storey’s Basic Country Skills, by John Storey
  ISBN 978-1580172028
- Ball Complete Book of Home Preserving, by Kingry and Divine
  ISBN 978-0778801313

- Dirr's Encyclopedia of Trees and Shrubs, by Michael Dirr
  ISBN 978-0881929010
- Square Foot Gardening
- Green Beret's Guide to Outdoor Survival, by Don Paul
- Great Living in Grubby Times, by Don Paul

Medical

- A Modern Herbal, by Mrs. M. Grieve F.R.H.S.
  ISBN 978-0880299213
- Emergency War Surgery
- Medicine for Mountaineering
- Merck Index
- Merck Manual
- Peterson Field Guides, Eastern/Central Medicinal Plants and Herbs, by Steven Foster & James A. Duke
  ISBN 978-0395988145
- Physicians Desk Reference
- Special Forces Medic Handbook
- The Merck Veterinary Manual, by Kahn and Line
  ISBN 978-0911910933
- Where There Is No Doctor
- Where There Is No Dentist

Non-Fiction

- Walden
- The Black Swan
- Brave New War, by John Robb

Philosophy, Religion, & Politics

- Cyberpunks Cyberfreedom: Change Reality Screens (Reboot Your Brain), by Timothy Leary
- The Fugitive Philosopher, By Timothy Leary
- Holy Bible
- Torah
- Q' Uran
- Bhagavad Gita

- The Kama Sutra
- Satan Speaks, by Anton LeVay
- Federalist Papers
  Download from http://www2.hn.psu.edu/faculty/jmanis/poldocs/fed-papers.pdf.
- Anti-Federalist Papers
  Download from http://www.wepin.com/articles/afp/.
- Communist Manifesto, by Marx & Engels
  Download from http://www.gutenberg.org/ebooks/61.

Firearms

- Sixguns, by Elmer Keith
- Fast and Fancy Revolver Shooting, by Ed. McGivern
- The Deer Rifle, by L.R. Wallack
- Gunsmithing Pistols & Revolvers, by Patrick Sweeney
  ISBN 978-1-4402-0389-3
- All the Gun Digest “Gunsmithing” series are good.
- Lyman Reloading Handbook
- Pistolsmithing, by George C. Nonte Jr.

Military Science

- A Rifleman Went to War, by Herbert W. McBride
  ISBN 978-1614271673
- The Art of War, by Sun Tzu
- The Book of Five Rings, by Miyamoto Musashi
- On Combat, by Lt. Col Dave Grossman
  ISBN 978-0964920545
- The Poor Man’s James Bond Series, by Kurt Saxon
- U.S. Army Field Manual FM 7-8, Infantry Rifle Platoon & Squad
  Download from http://www.marines.mil/news/.../FM%207-8%20W%20CH%201.pdf

This list is only the beginning, and could use some additions. When you find something worthy of inclusion, please send me an email at <ticom.new.england@gmail.com>, and when I get enough contributions, a few issues down the road, I’ll print an update with everyone’s submissions.

PUSH TO TALK
RELEASE TO L

Phone
1 STOP
2
3
COIN RELEASE
5-10-25
U.S. COINS ONLY
Lowest Rates Worldwide... All Day... Everyday!
CALL COLLECT
1-866-866-CALL (2255)
SAVE UP TO 50%!!
¡HASTA AHORRA
CALL WITH COINS
Call the World! ¡Llama a Tu País!
AT&T OPERATOR CALLS Dial 00
COLLECT CALLS
SAVE! UP TO 50% OVER AT&T
Dial 1-866-866-CALL
TELEPHONE