Introducing "Sherlock"—A Hi-Tech Fox Hunting Tool

Put your computer to work tracking down jammers and other unidentified signal sources.

By Malcolm C. Mallette, WA9BVS*

Jammers...you can't deny they're one of the great banes of ham radio. They disrupt repeater and simplex communications, and can make life generally miserable with unidentified, sometimes obscene, transmissions.

It's important that such behavior doesn't spread. If unidentified jamming of repeaters becomes common practice, 2 meters may someday resemble CB at its worst, making the band a lot less useful, especially when it comes to public service operations.

The easiest way to stop a jammer is to ignore him. NEVER, NEVER mention or threaten a jammer on the air. He wants to hear how much you hate him. KEEP YOUR MOUTH SHUT.

The Next Line of Defense

If silence doesn't work, there are several ways to determine the identity of operators who don't identify themselves. Jammers are generally unaware of it, but *their transmitters can identify them.*

For instance, a direction finding ("DF") team can locate the source of any signal on 2 meters by literally following the strength of the signal with their receivers. They generally use a method known as triangulation to track the offending signal. (See "Basics: Radio Direction Finding," elsewhere in this issue, to learn how triangulation works.)

Remember that you should *never say anything about the jammer on any ham frequency, and under no circumstances should you mention on the air any attempts being made to track down the jammer.* Coordinate your tracking operations on the telephone.

Malcolm Mallette, WA9BVS, is an attorney in Indianapolis. He holds an Advanced class amateur license.

Better Still...Let the Transmitter Identify Itself

But DFing is time-consuming and triangulation requires repeated or long-duration transmissions. An easier approach is to use the built-in tendency of transmitters to identify themselves, even if the operator doesn't give a callsign.

Modern 2-meter rigs have hundreds of channels available, with a microprocessor-controlled PLL (phase-locked loop) determining the transmit frequency. During the first 2/10ths of a second after the mic button is pressed, the transmitter moves in a unique pattern around the operating frequency, as the PLL locks up on the transmit frequency. This pattern is known as the transmitter's *turn-on characteristic.* A similar *turn-off characteristic* is generated when the mic key is released and the PLL unlocks.

For over 20 years, hams have used the turn-on characteristics of a transmitter to help identify a particular transmitter. In the old days of the tube radios on 6-meter FM, you could look at a scope or meter across the discriminator output to catch a glimpse of the turn-on characteristic of an unidentified transmission.

With modern computers and A/D (analog-to-digital) converters, it's easy to catch and store the turn-on and the turn-off characteristics of a transmitter. All you need is an FM receiver whose discriminator or other detector output is connected to an A/D converter and the proper software. The A/D converter will convert to a digital format the low-frequency audio that results from the turn-on or turn-off. The software will then display the turn-on or turn-off as a graph that the operator can compare to other turn-on and turn-off graphs. The comparison can identify, or help identify, the unknown transmitter.

In fact, there's even a microprocessor-controlled commercial unit (Motron's TxID-1) that can identify the station on its own by automatically comparing the signal it's hearing with data files of known transmitters! Well-funded repeater organizations may want to consider the purchase of that equipment. Its price, at around $700, is a bargain.

But if that's beyond the budget of *your* repeater group, you can build—for less than $100—a simple device that can capture the turn-on and turn-off, then interface with a computer to permanently store the data.†

Enter "Sherlock"

The Sherlock system is the modern equivalent of putting a scope across the discriminator. It consists of a simple A/D converter, an audio amplifier, and software, and it captures the turn-on and turn-off so that the operator himself can draw his own conclusions. While not a clone of the commercial unit, or intended for commercial use, Sherlock also enables the operator to identify a transmission if he has previously captured, or later catches, the turn-on and turn-off of the same transmitter when the operator gives his callsign. This must be done manually.

Sherlock's A/D converter is based on the Maxim MAX150 chip and is similar to a circuit that appeared in the January/

ftp.barc.org /pub/hamradio /log/ham-utils/sherlock.zip

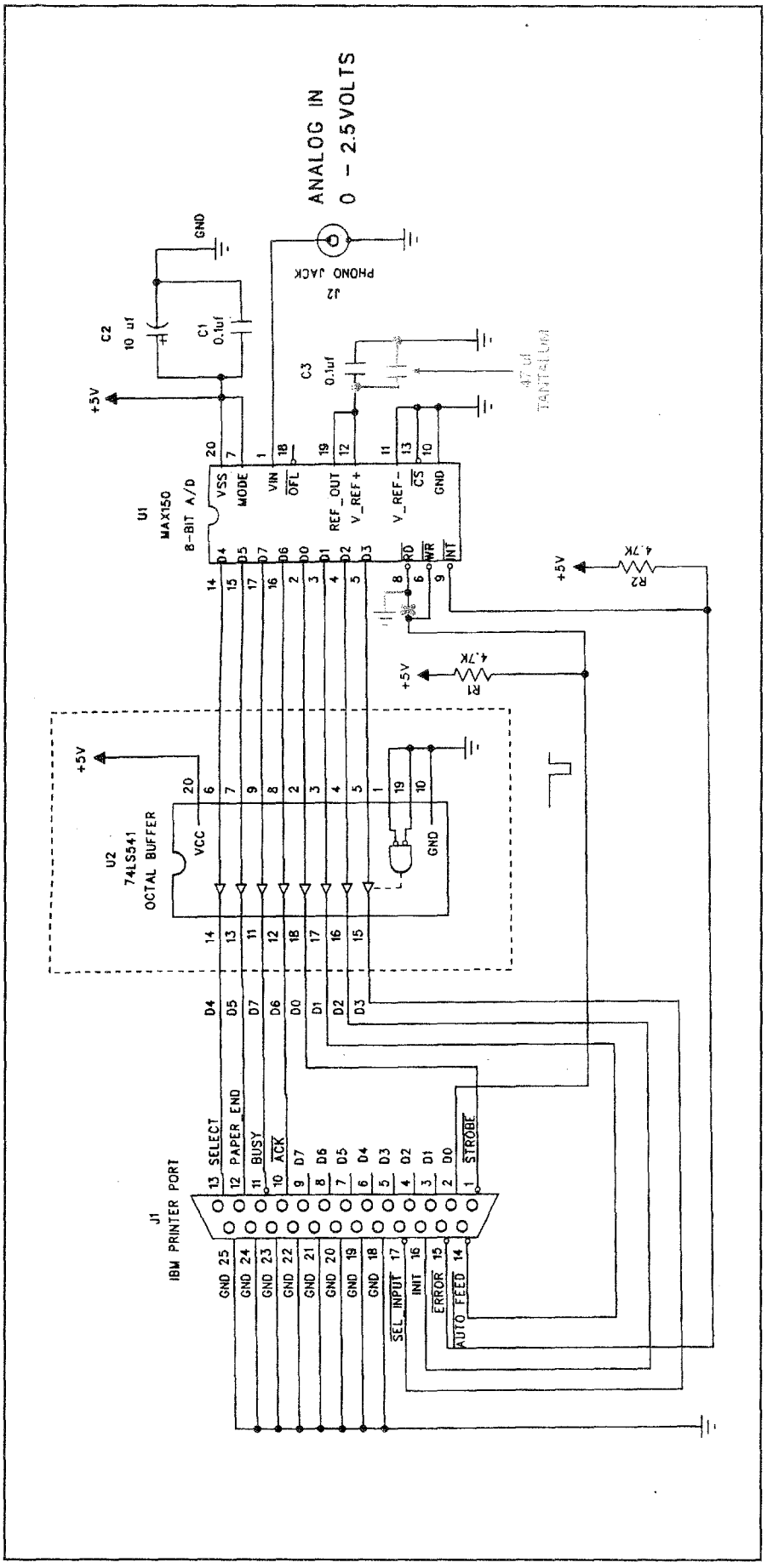

Figure 1. Schematic of the basic A/D converter circuit by Paul Bergsman, with modifications noted separately. (Original schematic reprinted with permission from the January/February, 1995, issue of MicroComputer Journal.)

February, 1995, issue of *MicroComputer Journal*. I've made two modifications to that circuit: Pin 8 of the MAX150 is now grounded, and there's a 47 µf tantalum capacitor from pins 12 and 19 of the MAX150 to ground (see Figure 1).

The audio amplifier is a Linear LT1077 (Figure 2), which provides the 0-2.5 volts output that the MAX150 needs to see as an input. (I'd like to thank Paul Bohrer, W9DUU, Jim Keeth, AF9A, and Bob Ulenski, N3FHI, for their help in designing these circuits.)

Building and Using Sherlock

The first requirement for using Sherlock is an FM receiver. It can be a scanner or a ham transceiver, but it must operate in FM. Even if you want to identify an AM transmitter, such as those used in the commercial aircraft service, you still

Parts List

A/D Converter
C1, C3 – 0.1 uf, 15-volt
C2 – 10 uf, 15-volt
Added capacitor – 47 uf Tantalum
J1 – Right-angle p-mount female subminiature D-shell connector (DigiKey catalog # 625F-ND)
J2 – Phono jack or BNC connector
R1, R2 – 4,700 ohms, 1/8-watt
U1 – MAX150BCPP 8-bit A/D converter
U2 – 74LS541 octal buffer

Audio Amplifier
C1 – 0.1 uf
C2 – .012 mf
C3 – 1 uf
R1 – 1 megohm
R2 – 1,000 ohm
U1 – LT 1077 IC
VR1 – 200K-ohm potentiometer
VR2 – 50K-ohm potentiometer

Power Supply
C1, C2 – 0.1 uf
U1 – LM7805 IC

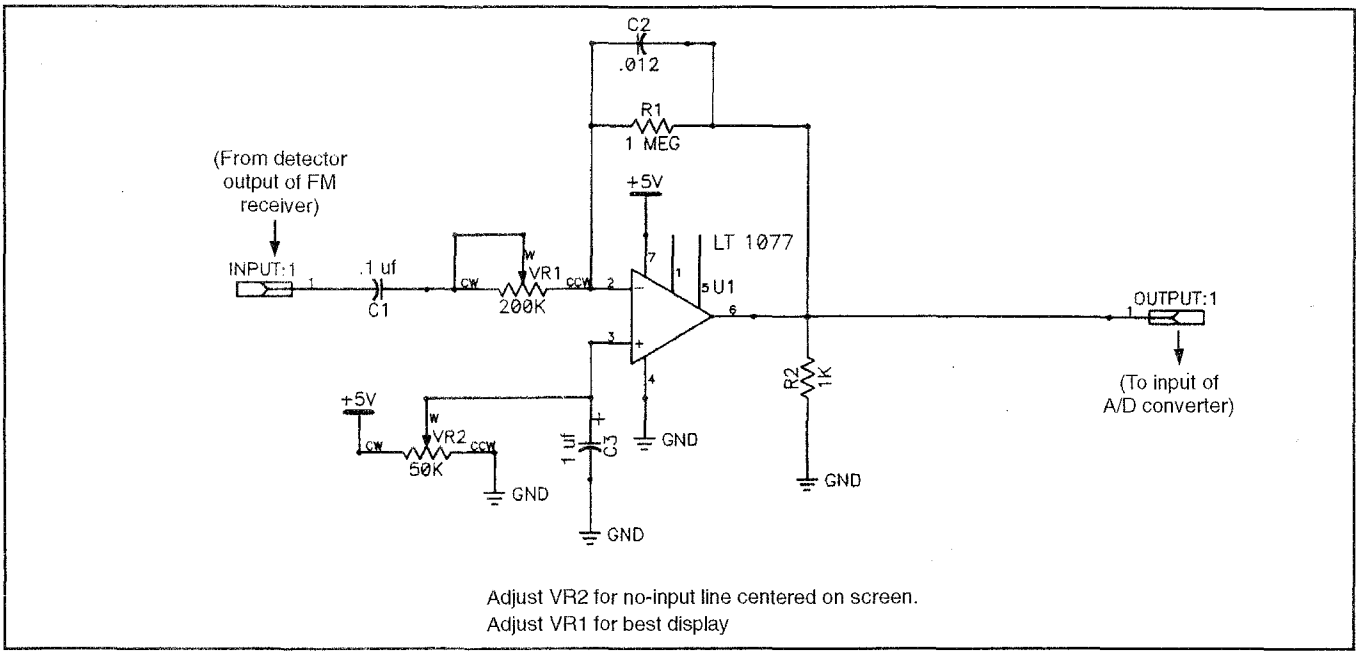

Figure 2. Schematic of the audio amplifier circuit. The audio amplifier must be connected directly to the A/D converter

need an FM receiver to capture the turn-on and turn-off information.

The second requirement is the A/D converter and the audio amplifier. The parts needed to build it are available from Digi-Key; the MAX150 may also be available from Maxim for about $25. You can build the A/D converter on a Radio Shack perforated PC board that has circles plated around the holes. Customized circuit boards are also available from FAR Circuits.

If you prefer, complete and tested A/D converters may be available from Paul Bergsman (write for his catalog). If you use his A/D converter, though, you'll have to change the board so pin 8 of the MAX150 is grounded and you'll have to add the 47 µf capacitor from pins 12 and 19 to ground. And, of course, you'll still have to build the audio amp yourself. (See "Resources" for contact information on all parts required.)

In any event, don't omit the octal buffer and do use sockets for the chips. Also, be sure to use a well regulated 5-volt power supply (see Figure 3).

Detector Detective

When the A/D converter is completed, connect the discriminator, ratio detector, or other detector output of your FM receiver to the input of the audio amp via a shielded cable.

You'll need a schematic of the FM receiver to determine where to connect the center conductor of the cable. *You must obtain the direct output of the detector; you cannot use the audio from the speaker or the headphone jack.* The receiver's audio circuits eliminate low tones, such as the sub-audible tones needed to use some repeaters. Those same circuits also eliminate the turn-off characteristics. (If you're unwilling to open the case of your receiver and make even the smallest modification, you should give up this project. In fact, you may even want to consider another hobby!)

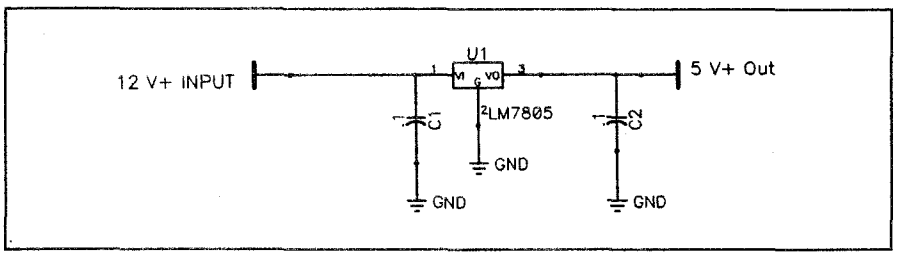

Figure 3. A simple power supply circuit to provide 5 volts DC to both the A/D converter and the audio amplifier. Note that it uses a 12-volt input.

Now, connect the digital end of the A/D converter to the parallel port (LPT-1) of your computer with a cable that has all 25 wires. If you have a printer on LPT-1, use a mechanical switch between the printer and the A/D converter. The computer must be an IBM or clone running DOS (not under Windows 3.1 or Windows 95, which I haven't tested yet) with at least a 486 DX 33 processor (an SX 33 may work) and a VGA monitor.

"Holmes": The Sherlock Software

"Holmes" is a compiled Quickbasic program that I've written to run with Sherlock. It's impossible to fully explain the program in this article, but here's a brief explanation of how it works. (Before attempting to run it, read the extensive instructions that come with it, and then read them again!)

First, after ensuring that the A/D converter is connected to parallel port LPT-1 and that the receiver is off, use the appropriate DOS commands to make a directory on your C: drive called "TI". Then make a subdirectory named "DTA", giving you "C:\TI\DTA". Copy the file "Holmes{x}" (x is the version, currently version 5) from the floppy into the C:\TI directory and the files "sample1" and "sample2" into the DTA subdirectory. Change the default directory to C:\TI and run the program by typing

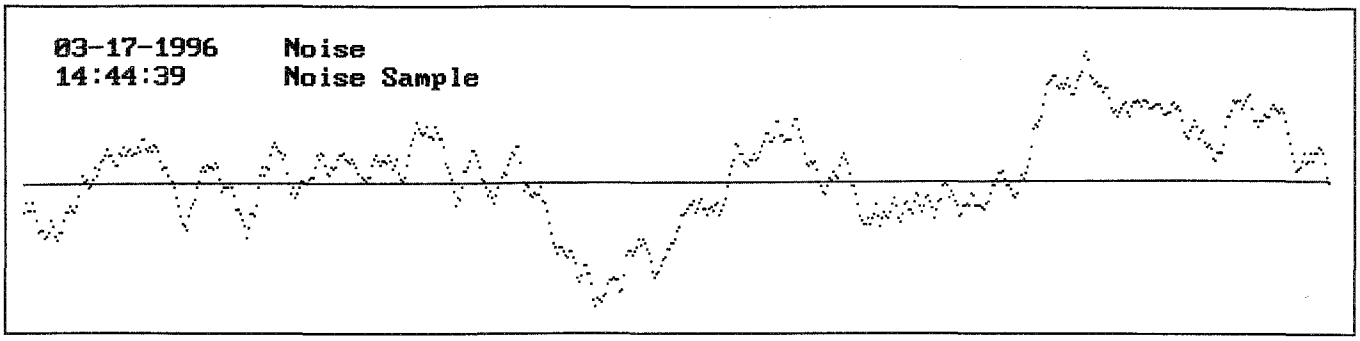

Figure 4. A noise sample as detected and displayed by Sherlock.

"Holmes{x}" <Enter>. So, for version 5, you'd type "Holmes5<Enter>".

The program will run and take you to the main menu from which you'll select "I". You'll see a blue screen with a white line strobing across it. There's also a very short violet line midway between the top and bottom of the screen on the left side. Adjust VR2 on the audio amplifier until the white line is over the short violet line.

Now turn on the receiver and adjust VR1 until you see noise displayed, as in Figure 4. Use an HT on low power with no antenna on the FM receiver for a test signal. You don't want to peg the receiver's S-meter or receive LED indicators.

Hit any key when you hear the noise from the receiver become an unmodulated signal. You'll very briefly see the HT's turn-on signature. You can save the data of any turn-on, or turn off, in a file, as detailed in the instructions. Simply enter the callsign and frequency; the date and time will be automatically entered from the clock in your computer (make sure the clock's accurately set!).

After entering the callsign and frequency information of the station whose turn-on you captured (your own in this test case), you'll be returned to the main menu. You can view the turn-on you got a brief glimpse of before by using the "V" selection from the menu. Select "V" and use the keys as explained in the instructions. If you press "B", the screens will scroll back and you'll see a carrier (a line across the screen at the mid-point) followed by the turn-on and then noise (prior to the turn-on.) Figure 5 is a printout of a turn-on; Figure 6 is a printout of the comparison feature, selection "C" from the main menu. This is the heart of the program, which enables you to compare a signal you're receiving with known transmitters stored in the database.

Once you become comfortable with the program, you normally won't use the main menu command "I" to capture a turn-on or turn-off. They simply occur too fast for you to see anything in this mode, and the data is broken up as the screen resets. Instead, you'll use the main menu command "D", which accomplishes the same thing but without displaying the incoming noise and signal.

Telling Transmitters Apart

I've been asked whether Sherlock can tell the difference between two transmitters of the same make and model. Well,

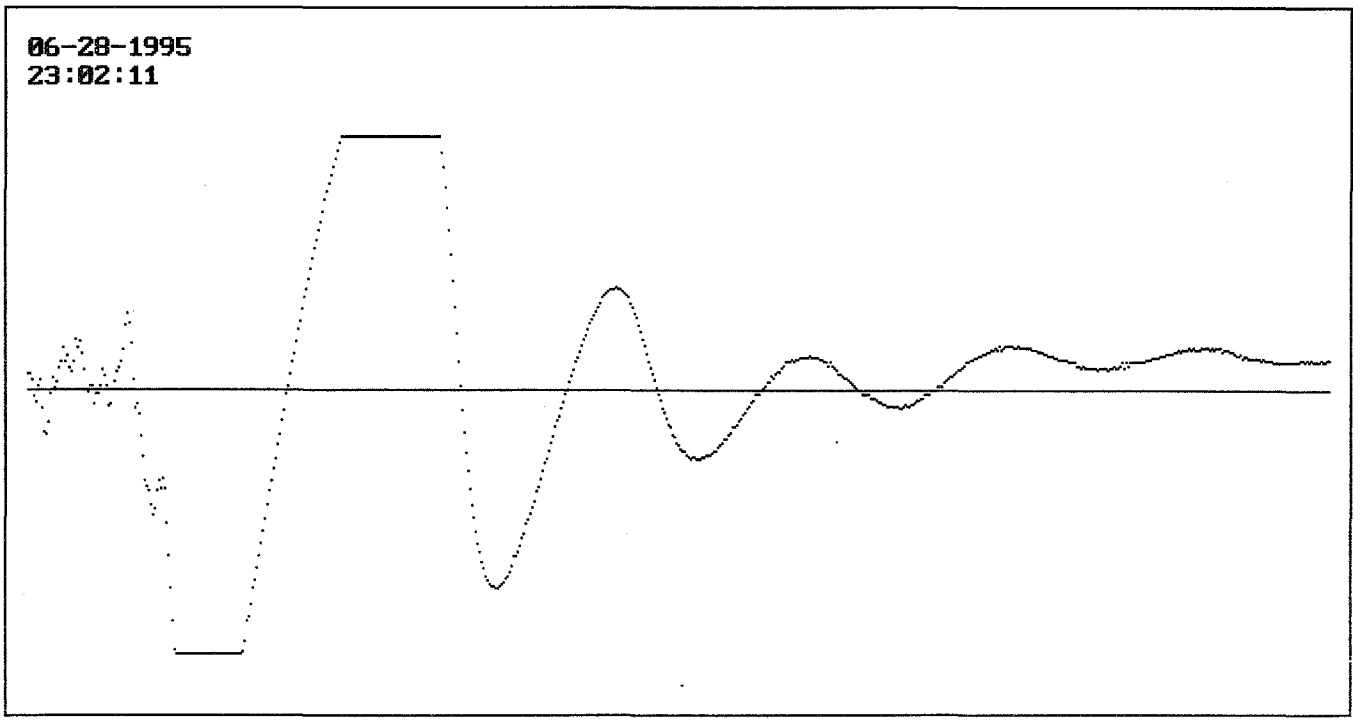

Figure 5. A sample of a transmitter "key-up." This unique pattern can be used to identify a transmitter.

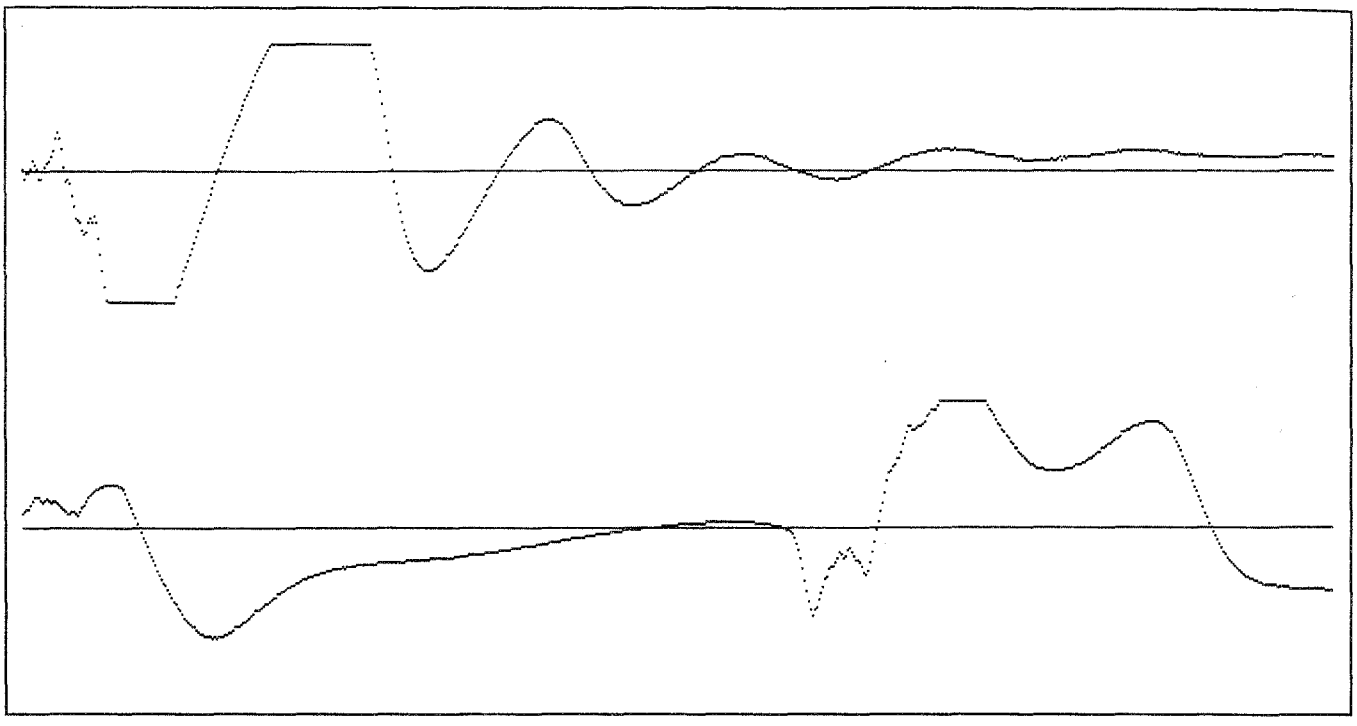

Figure 6. Comparing a signal from an unidentified transmitter with stored samples from known transmitters can help you identity a jammer.

at a demonstration of the system during a recent meeting of the Indiana ATV and UHF Club, two hams had the same make and model of HT. Sherlock could tell them apart. Two other hams had another pair of identical HTs (different from the first two) and Sherlock could tell them apart, too.

But more tests by many more users are necessary to be sure that all radios, of all makes and models, can be individually identified. It's possible that there are mobile transceivers with very short and limited turn-on characteristics so that two units of the same make and model can't be told apart. In such a case, the beam heading of the signal would become important, as would signal strength and other clues determined through more traditional DF methods.

Finally, as you've seen from the figures, the graphs of turn-ons and turn-offs can be printed out. You'll need a laser printer or ink-jet printer that's compatible with the DOS "graphics" command. This command must be issued *before* running Sherlock if you intend to print (see your DOS manual for further information.)

Let's Hear from You

If you build Sherlock, please drop me a QSL card or a note at my *Callbook* address, or via *CQ VHF*, and tell me how it works. You can also reach me by e-mail to the magazine (CQVHF@aol.com), and they'll forward it to me.

Good luck and happy hunting.

---

† *Motron's TxID-1 uses patented software (U.S. Patent # 5,005,210). My software is different. However, even though I am a lawyer, I do not practice patent law and I cannot advise you with certainty that manufacturing the equipment described in this article does not infringe on that patent or any other. If you plan to manufacture this device and are concerned about possible patent infringement, you should contact a patent attorney.*

Resources

Circuit boards for this project are available from:
FAR Circuits, 18N640 Field CT., Dundee, IL 60118-9269;
Phone/Fax: (847) 576-3540.

In addition, assembled and tested A/D converters may be available from:
Paul Bergsman, 521 E. Wynnewood Rd., Merion Station, PA 19066.

Parts for the project are available from:
DigiKey, (800) 344-4539.

The MAX150 may also be purchased for about $25 directly from:
Maxim Integrated Products, at (800) 998-8800.

The Holmes software is available without charge and may be downloaded by anonymous FTP to <ftp.hcares.gen.in.us> and is in the directory /pub/hamradio/sherlock. The software has two files, **sherlock.txt** and **holmes (x).exe**, where (x) is the version number. There are also two sample data files, **sample 1** and **sample 2**.

The Motron TxID-1 Transmitter Fingerprinting System is available for $699 from:
Motron Electronics, 310 Garfield St., Suite 4, P.O. Box 2748, Eugene, OR 97402;
Phone: (541) 687-2118; Fax: (541) 687-2492.