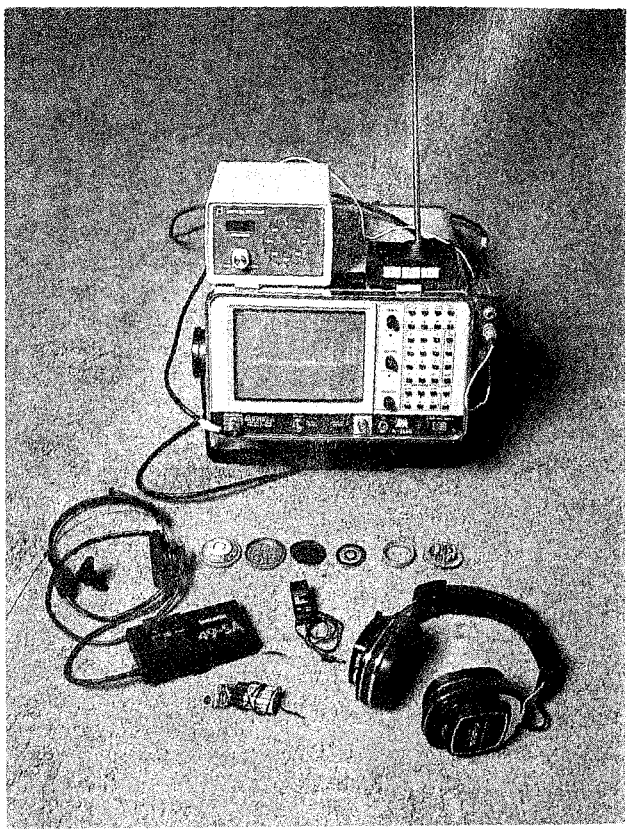


TRACKING DOWN BUGS USING A SPECTRUM ANALYZER

Are you being bugged? Here's how to find RF bugging devivces that are invading your privacy.

RICHARD A. BOWEN

BEING WIRETAPPED IS NO JOKE. TODAY'S micro-miniaturized electronics have made it easy for anyone with a little know-how and willful attitude to tap your phone and invade your privacy. Whether you call it eavesdropping, phone tapping, radio interception, or covert operations, we'll show you how to hunt down those tiny bugs.

Although there are many advertised gadgets that claim to locate clandestine transmitters, licensed private investigators, with few exceptions, have neither the technical expertise nor background to properly use them. Consequently, more and more investigators are turning to radio technicians who are knowledgeable in counter-surveillance technology.

That's why a competent radio technician with an inquisitive mind and the proper equipment can make a supplemental income (perhaps $100+ per hour) by availing himself, his equipment, and his expertise to investigators who are trying to locate clandestine transmitters.

Tools of the trade

The first order of business is to have the right tools. But what are the right tools for detecting bugs that are positioned by persons good at hiding them? Bar none, the most invaluable tool is a *spec*trum *an*alyzer (spec-an). The one used by the author is an IFR model *A7550*, which becomes portable when using its built-in Nickel Cadmium (Ni-Cd) battery—an essential convenience.

You'll also need a good receiver to scan the RF spectrum looking for the bug's frequency. Many spec-ans have radio-scanner options (receivers) that are designed to be hooked up without modification. Now admittedly, $500 dollars for that option might sound like a lot of money; but when you're talking about a $10,000 investment, if it's not really that much. After all, you're trying to discern what type of intelligence is contained in a detected signal, you need a good receiver. Of tremendous benefit would be some kind of mixer, down converter, or prescaler to extend the receiver's frequency range.

For obvious reasons, it's paramount to tape-record the bugged audio; also, a first-rate direction-finder is necessary so you can track down and locate clandestine, or spurious emissions.

Another option that is extremely useful is a *G*eneral *P*urpose *I*nterface *B*us (GPIB) interface with a plotter, which will allow you to make hard-copy two-color printouts of the suspect frequencies that you have discovered, or wish to document. The GPIB will interface the spec-an's output to the plotter.

There are a lot of gizmos that are advertised on the market as so-called "counter-intelligence devices." The author is compelled to warn you that most of the equipment will not perform as advertised, and the equipment that *will* perform is often unethically sold for 3 to 5 times the list price—*caveat emptor!*

If you think that you're being bugged, you may be desperate for anything that advertises to solve your problem quickly. The false promise of those gizmos seems like a good risk. But wait a minute: That's exactly what those unethical companies are depending on to motivate a sale! Don't fall into their trap. There's no short-cut gizmo that can replace the proper test equipment in the hands of a qualified radio technician.

Sleuthing

Technicians make some of the best detectives in the world—no kidding! They have to investigate why something doesn't work and trace down the fault; that takes an inquisitive mind. And if one has a good sense of business, there's plenty of work in counter-surveillance. That's because private citizens are being illegally bugged every day; not to mention all the industrial and foreign espionage that seems so prevalent in today's world. Yes, indeed, when word gets around that a technician knows how to ferret out phone-taps, that person's skills will be in demand.

Most people just aren't aware of all the inexpensive devices that can be legally purchased to invade their privacy. Figure 1 shows three tiny bugs that can hear everything you say. Although clandestine bugs can come in small packages, a willful intruder will use what's handy and what works. Bugs range from sugar-cube sized "wireless microphones" for $20, to candy-box sized "wireless intercoms," and handhelds, that will allow anyone within a half-mile radius to listen to every spoken word in your home. And you can bet that there are many more sophisticated and much more expensive devices, too! Let's face it; not just anyone can find one of those cleverly hidden bugs in your home or office. It takes someone like a technician with expert knowledge of radio transmissions, having the skills and equipment needed to track down tiny radio bugs.

Did you know that a perfectly legal

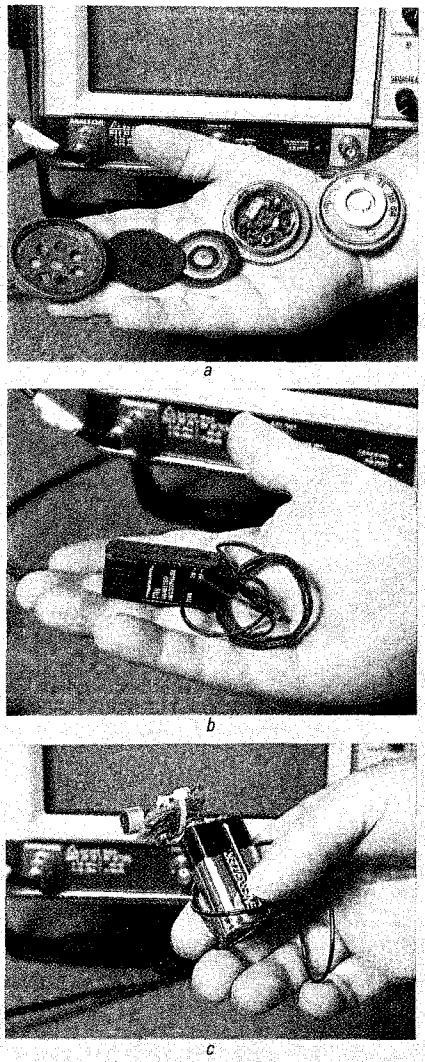


FIG. 1—THESE ARE CLANDESTINE radio bugs. In *(a)*, a parasitic phone-tap is shown disassembled. In *(b)*, a Radio Shack FM-transmitter (part No. 33-1076) can be conveniently dropped behind the cushion of a chair. In *(c)*, this tiny FM transmitter can be hidden in a kitchen cabinet.

(FCC registered) phone tap is available from many companies for only $25? That's because there's a big market for bugging *your own* phone. Just think for a moment: At one time or another haven't you called some big-time attorney, or doctor, or insurance company, only to hear strange beep-tones or clicks. That's right, you're being recorded—and it's all legal!

Most people are under the impression that intercepting *your own* telephone conversation, or recording the conversion without beep tones, is illegal. That simply isn't true! You don't have to notify anyone that you're tapping *your own* phone. How about that! And if you can buy a simple phone-tap, so can a criminal out to victimize the average Joe.

Bug frequency

Let's suppose a client suspects a radio bug has been planted in his telephone. However, the client might lack the know-how to either disassemble the phone, or even tell the difference between a wiretap and the normal telephone's circuitry. It's possible that the client has found a wiretap, but dosen't know what to do. A common wiretap is shown in Fig 1-*a*. It's a "parasitic telephone transmitter" (not to be confused with parasitic or spurious emissions from a legal RF transmitter).

The nomenclature "parasitic" was derived from the fact that the bug steals power (as a parasite feeds on others) from the telephone company and, consequently, needs no external battery or antenna. Those devices use the telephone's own headset coil-cord and associated wiring as the antenna, and the 48-volt central-station battery for power (which drops to about 10 volts when the handset is off hook).

Depending upon how the tiny phone-bug is designed and where it's located, it can be received on an FM radio, or other receiver, up to one-half mile away. The beauty of that bug is that it can't be detected unless it's actually operating, which means the phone must be off-hook. And although able to operate on virtually any frequency, it's common to sandwich the transmissions between high-powered FM-broadcast stations; that's so they won't create radio interference that would tip off the authorities. Besides, an FM transmission can be received by any inexpensive FM car radio—usually sitting in front of, or nearby, the victim's house or business.

Here's a step-by-step procedure using a spec-an to make any bug stand out like a sore thumb:

Step 1: Set scan-width for the 88 MHz to 108 MHz FM broadcast spectrum.

Step 2: Set bandwidth resolution to 3 kHz. You will now have a factual display of all electromagnetic radiations occurring in the 88 MHz to 108 MHz frequency range.

Step 3: Set the "peak hold" to capture and store all legitimate signals that are on the air (see Fig. 2-*a*).

Step 4: Digitally invert all stored information (see Fig. 2-*b*).

Step 5: Pick up the suspected telephone (off hook) and you'll notice that the signal previously not present is now displayed (see Fig. 2-*c*).

What we have accomplished is a digital cancellation of everything that

should be on the air against a brand new signal that was not there prior to our picking up the phone, but which now sticks out like a *sore thumb*.

Incidentally, for evidence in court (and customer records) the plots that are reproduced can be made at the actual scene of the crime with the GPIB option (also known as IEEE-488). One GPIB is available from IFR to connect their spec-an to a Hewlett Packard *7470A* Plotter. Whatever spectrum analyzer and plotter you're using, contact the manufacturer's representative for interfacing suggestions.

Bug locating

If you are sharp enough to find a bug, the last thing in the world that you want is the bug to hear itself! (If the bug is active, it is logical to assume that someone is listening.) If you have a receiver tuned to the bug with speaker audio, and you get too close, you'll get audio feedback, which will immediately tip off the spy that you're on to him! No good! Here's what to do.

Once the bug's frequency is found, use headphones with a long, long, extension cord (maybe 50-100 feet or so) to listen to the audio. Now walk around the house tapping the walls, rattling objects, or talking in a normal voice, while listening for an increase in volume level. Make your rattling sounds appear as natural as possible, so that the "bad guys" don't become suspicious. If the bug is in the kitchen, then as you move from the living room into the kitchen, the bug will pick up more audio thereby transmitting a higher-amplitude signal. You'll hear that over your headphones.

The receiver option of your spec-an will undoubtedly have a speaker output. Figure 3 shows how to convert the speaker output to a headphone output only. Although by no means any engineering marvel, the modification is extremely effective and retains the integrity of the receiver! The audio is re-directed (using shielded coaxial-cable) from the speaker to a set of headphones. Figure 4 shows the author's home-built adaptor box. Alternatively, a set of cordless infrared headphones, such as Maxon's model *49-SA* can be used, which would not only eliminate the possibility of tripping over a long headphone cord; but they are also useful in detecting infrared bugs—yes, those exist, too!

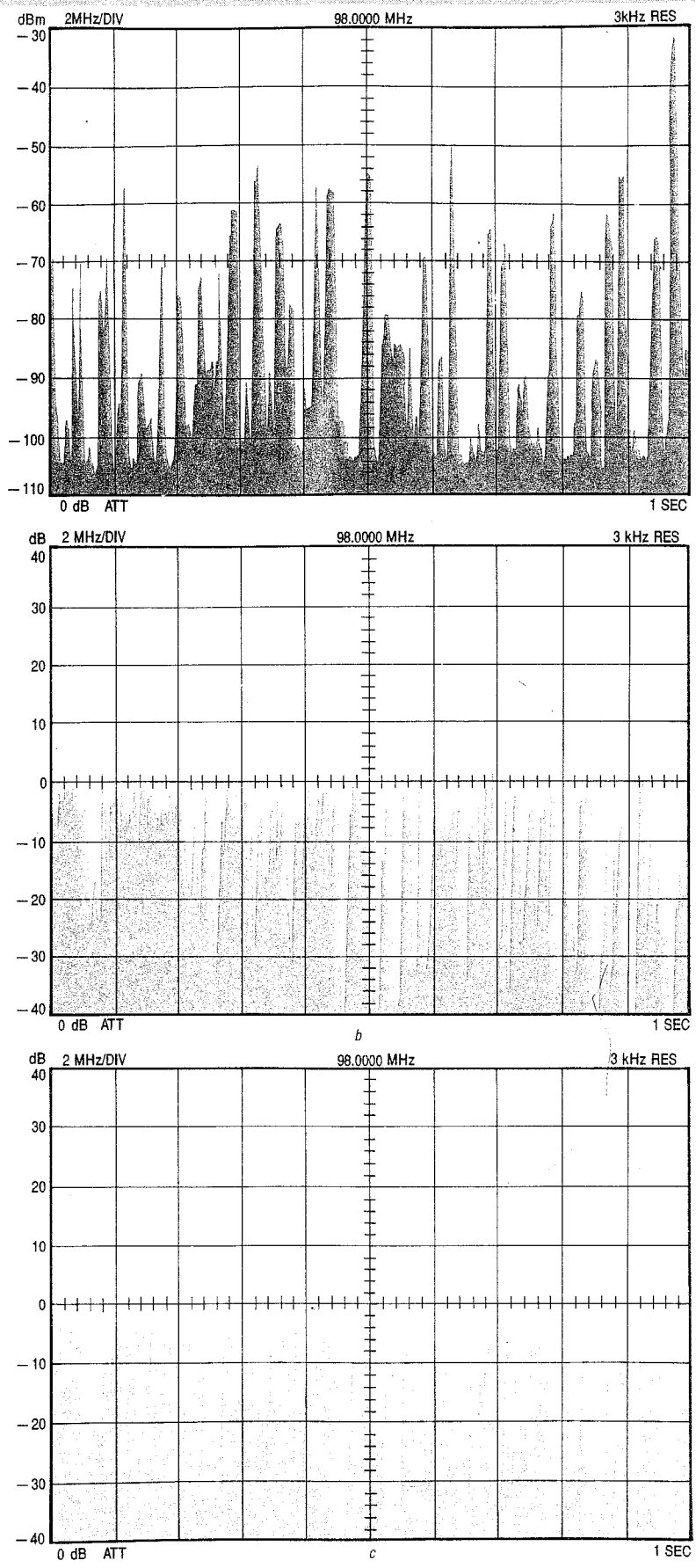


FIG. 2—A SPECTRUM ANALYZER WILL INTERCEPT THE BUGS FREQUENCY. In *(a)*, the broadcast (88-108MHz) FM spectrum is scanned and stored. In *(b)*, the stored spectrum is digitally inverted. In *(c)*, the bugs frequency sticks out like a sore thumb when the phone-tap begins transmitting.

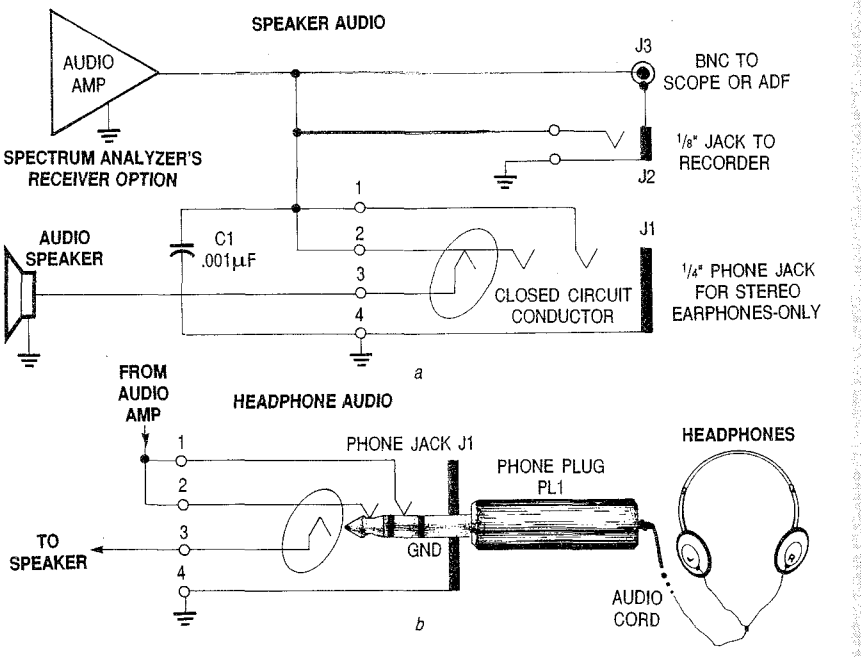


FIG. 3—USE HEADPHONES FOR LISTENING TO THE BUG'S TRANSMISSIONS. In *(a)*, this circuit will modify your receiver's speaker output for headphone use only. As shown in *(b)*, when the phone plug is inserted, the closed-circuit spring opens, thereby cutting off the speakers while re-directing the audio to the headphones.

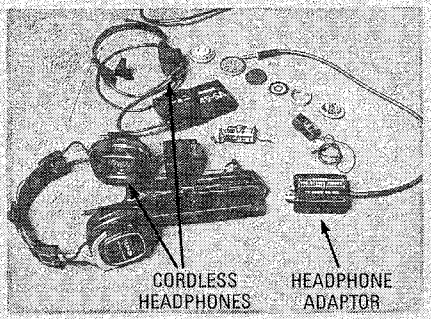


FIG. 4—USE THE AUTHOR'S home-built adaptor box with either a pair of stereo headphones, or a cordless infrared transmitter and receiver.

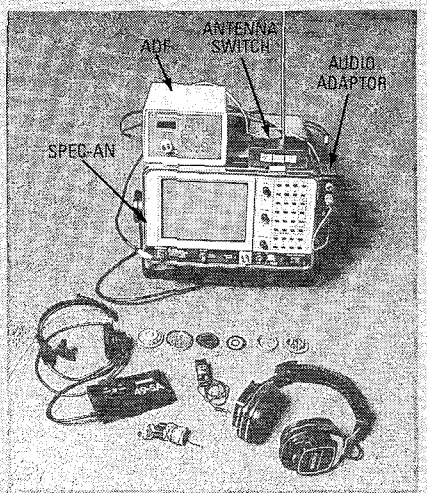


FIG. 5—HERE'S YOUR PERFECT sleuthing setup: a spectrum analyzer, automatic direction-finder, antenna switching box, and headphone audio-adaptor to listen privately to clandestine transmissions.

The headphone adaptor box can be attached with *Velcro* tape to the side of the spec-an. In addition to providing headphone-only audio, J2 can input to a *V*oice *O*perated *T*ransmit (VOX) actuated tape-recorder, J3 can input to an oscilloscope, *A*utomatic *D*irection *F*inder (ADF), or whatever else is required. Note: Use only a 1/4″ *stereo* phone-plug for audio-jack J1; that's because if a monophonic phone-plug is inserted, it will short-circuit the audio amplifier.

An actual bust

As a case in point, the author's services were requested by an out-of-state detective agency. They had a client who quite honestly thought she was losing her mind.

Separated from her husband and having their two children in her custody, the children stood to inherit close to three million dollars, which would be administered by their legal guardian as a trustee. (Not a bad situation for the legal guardian.) To her, it seemed that every single word she said inside her home, or over the phone, was somehow being overheard. No one could find any clandestine listening device, and her suspicions seemed to be getting the best of her. She thought, "Is my ex-husband trying to collect evidence to prove that I'm an unfit mother, and then use that as a tactic in court to remove my guardianship?" The husband would then stand to become the trustee to three-million smackers.

The author and out-of-state detective set up a spectrum analyzer, and proceeded to search for a radio signal that shouldn't be there. After an hour or so, an intermittent signal kept popping up in the middle of the FM-broadcast band that didn't correlate with any known or published local radio-stations in the area. Without going into detail, it was established that a *frequency-hopping transmitter* was operating, and was remotely controlled by an AC line-current carrier transmitter.

In other words, that was a bug that selectively transmitted information on numerous frequencies. The purpose was to make it much more difficult for someone, to locate the bug because it would continually "hop" to a new frequency. If such a signal is monitored on a single frequency, all that is heard is gibberish.

The control of that device was discovered to be an AC line-current carrier transmitter that could activate or disable the bug from a convenient location in the neighborhood. Now that you have found something as insidious as that, what do you do? Psychology is always the best weapon. If we were to rip the bug out, the "bad guys" would instantly know that it was found.

The author made a hand-written note, showed it to the parties involved, and instructed them to walk outside onto the patio where their conversation could not be overheard. There he informed the victim that she was neither paranoid nor insane, and she immediately fell into the author's arms, crying in relief. The author advised that if they tore apart the kitchen cabinets, (where the bug was located) that the perpetrator would be aware that the bug had been discovered.

So "what now?" The author suggested that she make a tape recording (at another residence) of the kids screaming and carrying on, as if something terrible was happening. The next step of the plan was to take the children and place them in someone else's custody, whose testimony and verification could not be disputed in a court of law.

Having done that, she should stay in her house alone, play back the tape as loud as possible, grab a few pots and pans and make as much noise as

possible (portraying a scene of total chaos and child abuse). The whole purpose of that action was to find out who would show up.

Well, it worked! It was the in-laws (outlaws) that showed up, and not the husband, much to the surprise of everyone. I can only presume that they cared more about the three-million dollar inheritance than they did about the welfare of their grandchildren.

Spec-an modifications

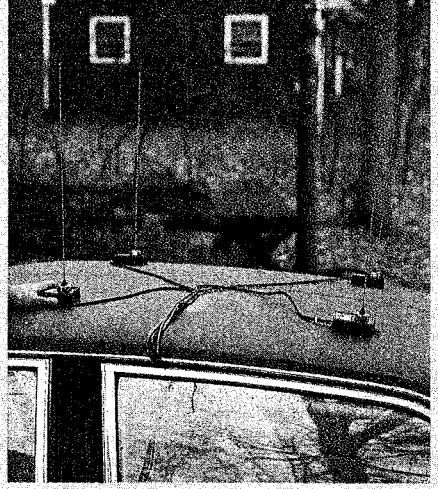
Unfortunately, the IFR *A7550*, along with other spectrum analyzers, has one fault in common: There is an unacceptable amount of leakage from the internal oscillators that cause alarming and inaccurate readings with an antenna placed as far as 20 to 30 feet away. The problem is caused by RF case leakage that can easily be corrected. But if you don't correct it, that leakage will ruin your day!

Spectrum analyzer RF leakage can be cured by making sure that the front and rear mounting bezels make good contact with the case. Dissimilar metals should not be used, because oxides caused by the bi-metallic contact will form a resistive film that isolates the bezel from the chassis. That turns the bezel and aluminum case into an antenna which, in turn, radiates all of the internal RF of the spec-an's circuitry. Also make sure that your plotter is line-filtered so that RF energy emitted by its microprocessor circuitry is not radiated into the power line.

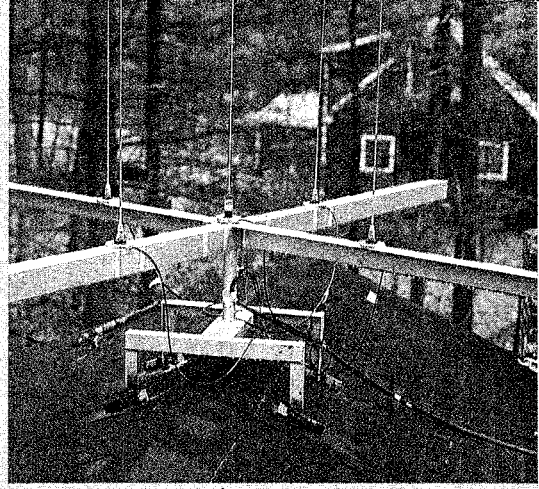
RF direction-finding

Sometimes clandestine, spurious or overbearing emissions can be so powerful that they cause problems many miles from their source. Enter the *automatic direction-finding system* manufactured by Doppler Systems Inc., PO Box 31819, Phoenix, AZ. 85046, (602) 488-9755. Figure 5 shows the Doppler direction-finder attached by *Velcro* to the right top of the spec-an. The circle of LEDs indicates the bearing to the RF source, while a 7-segment LED-display indicates the bearing in large numerals. The Doppler system has a frequency range of 27 MHz to 500 MHz, and can be connected to any standard VHF or UHF FM-receiver. No receiver modifications are required—simply plug the Doppler electronics into the receiver's antenna and external speaker jacks.

As shown in Fig. 6, four ¼-wave whip antennas can be mounted on a car's roof for mobile operation, or on the roof of a house. The antennas can electronically simulate a rotating directional-antenna. As the antenna moves toward the RF source, the apparent signal frequency increases; as the antenna moves away from the source, the apparent signal frequency decreases. That up-down (Doppler) frequency shift is detected by the FM receiver as a 300-Hz audio tone. The phase of the tone is related to the bearing angle and is used by the direction-finder electronics to compute and display the bearing.



a



b

FIG. 6—DIRECTION FINDING using Doppler System's four matched quarter-wave whips, shown in *(a)*, are supported on magnetically mounted bases for mobile operation. In *(b)*, four collapsible antennas are mounted on a sturdy platform, on top of the author's roof.

The purpose of the direction-finding platform is to get an initial bearing to the desired signal, and the relative signal strength. The ¼-wave whip antennas must be tuned to the exact frequency of the clandestine transmissions. You know the exact frequency by using the spectrum analyzer. The antennas are collapsible and will allow tuning by extension-retraction, and spacing the bases by sliding them along the platform. To work properly, the antennas must be spaced approximately ¼-wavelength apart.

One of the capabilities of a spectrum analyzer is the ability to identify the frequency of the offending radio-emission. That includes spurious emissions that are common in areas where multiple transmitters are placed in close proximity with each other. Besides the non-linear mixing that occurs in a transmitter's final-amplifier (called intermodulation) that create strong spurious signals, other far more exotic kinds of heterodyning also occur.

One time the author found a "difference" frequency coming from an oxidized dome of a town hall. There were two AM-broadcast stations less than a mile away; one was on 1590 kHz and the other on 900 kHz. Within a half mile of the town hall, everyone in town could hear one of the stations at 690 kHz! That was caused by rectification from the dome's copper-oxide layer.

When "DF-ing" a spurious signal in a moving vehicle, it is absolutely imperative that you have an assistant, or navigator to read a road map and give directions, or more important—to prevent you from kissing a telephone pole. Using Doppler System's *A*utomatic *D*irection *F*inder (ADF), the author has been able to track down signals to a specific section of a house—from the road out front!

Proximity signals

If you narrow down a suspected transmitter to within a given area, here's one method of determining its proximity. Place three identical antenna's having identical lengths (and types) of coaxial cable connected to a coaxial-switch box. Use the best coax, like RG 223-U coaxial cable, which is double-shielded (98% each) silver-plated (both shields and center-conductor) cable to ensure total integrity of the received signal. That may sound like overkill, but if you're going to do something, why not do it right?

Separate the three antennas by about 30 feet. A low-powered bug will show a marked change in signal strength on the spec-an, when antennas are independently selected. The stronger signal will indicate the relative bearing of the transmitter's location. Transmissions from far away will indicate almost identical signal strength. **R-E**