



Signal Hunting and Classification



The importance of quickly tracking down signals that may be used for disruptive or illegal purposes has grown significantly in recent years. Wireless bugs, malicious remote control RF links, illicit activities using wireless devices or simply unintentional emissions hampering infrastructure operation, are often of interest. Finding, identifying and physically locating RF emitters that are misusing the crowded radio spectrum can be a challenging process. In the past this endeavor has required expensive specialty equipment, often adapted from intelligence gathering systems that were not originally intended for highly portable signal hunting. Tektronix' **RFHawk** now offers a modern, portable design that is ideal for searching the spectrum, identifying rogue signals and hunting down their transmitters. Rapid scan rate, sophisticated signal identification capability, integrated GPS mapping and a long battery life, set this signal hunter apart from general purpose test equipment and costly collection systems.

Introduction

Finding specific or unauthorized transmitters in the radio spectrum requires a variety of capabilities rarely found in a single instrument. Complicating matters, the proliferation of consumer wireless devices is changing the very nature of many signal hunting applications, requiring a truly man-portable solution for use inside buildings or in dense urban environments.

The need for a variety of specialized instrument capabilities in a highly portable design is rendering traditional approaches to signal hunting obsolete.

In this application note we look at the challenges of scanning the RF spectrum, identifying/classifying each signal, and then physically tracking down the rogue transmitter. A particular emphasis is placed on the signal identification and classification tools that help sort out undesirable use of the RF spectrum.

Let us now explore how the **RFHawk** analyzer is pioneering a new class of signal hunting instruments.

The Need to Find Emitters

The reasons for finding a rogue signal emitter are very diverse. Searching for wireless bugs in an embassy, conducting a roadside sweep for Improvised Explosive Devices (IEDs), locating the source of interference in a licensed radio channel, tracking wildlife migration patterns, finding illicit activity from secure areas, or simply responding to regulatory complaints – the need to find rogue RF transmissions and locate their source of emissions is an essential part of the mission of many institutions, agencies and military organizations.

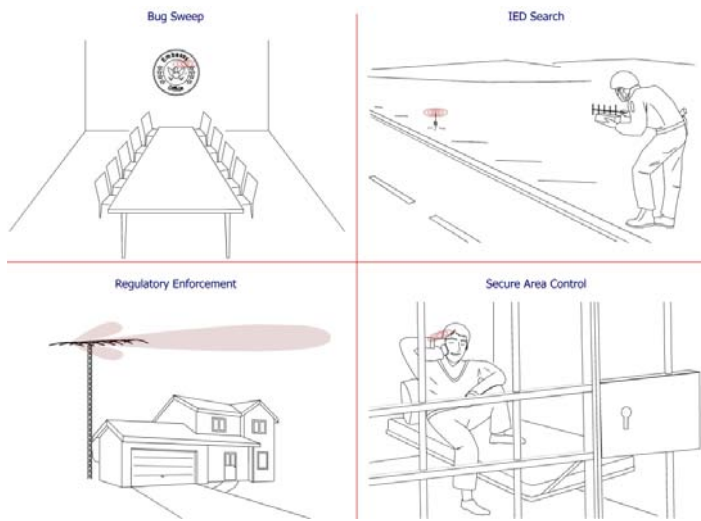


Figure 1. The need to locate the source of wireless signals arises from many situations, including bug sweeps, IED detection, prison searches and tracking illicit activity.

With the recent explosion of wireless devices, now more than ever, signal hunting is garnering more attention from a diverse set of intelligence agencies and law enforcement groups.

When faced with such a mission, what is the best solution to quickly finding the source of wireless transmissions? To understand what makes an effective solution, let's review the basics of how RF signals are found, identified and tracked down.

Signal Hunting Basics

The process of hunting down an RF signal takes on three distinct steps.

Finding RF Signals

First, the radio spectrum must be scanned to survey what signals are being transmitted. As we change our location,

the radio spectrum also varies, as some signals fade out of range and new ones come within range. So each new location necessitates a scan of the radio spectrum to see what RF energy is present.

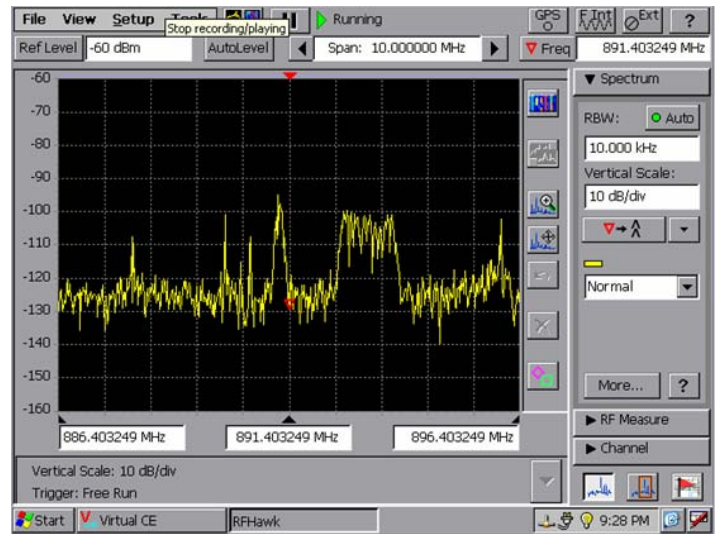


Figure 2. A simple spectrum plot reveals a variety of transmitters in the local vicinity.

Scanning the radio spectrum is usually done with the traditional spectrum plot or the spectrogram. The traditional spectrum plot tends to be best for Continuous Wave (CW) transmissions that are always on, whereas the spectrogram is better suited for finding intermittent signals.

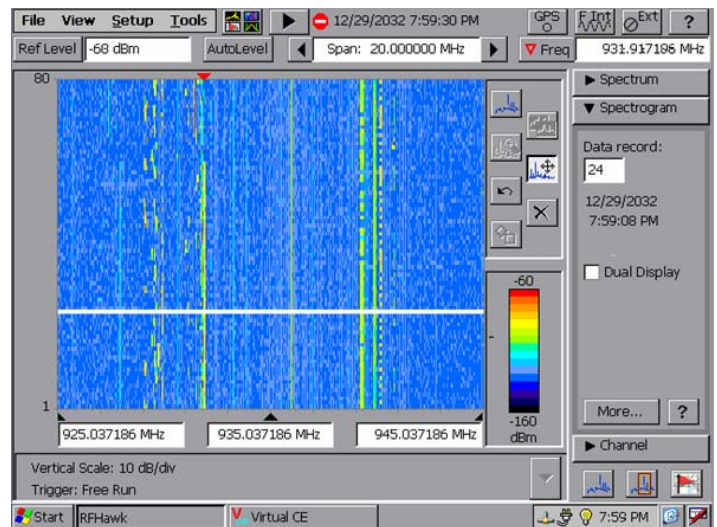
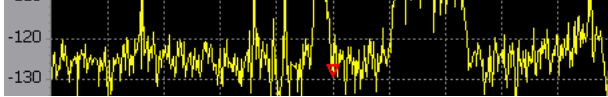


Figure 3. The spectrogram shows frequency versus time, with color representing signal level, and is often preferred for surveying intermittent signal transmitters.

Once the signals in the spectrum are found, it is then necessary to identify them and classify their use.



Sorting Out Signals of Interest

As the nature of each signal is revealed, its use of the radio spectrum can be classified. Is the transmission an authorized or permitted legal emission of RF energy, or is the signal illegitimate, illegal, malicious, and unauthorized?

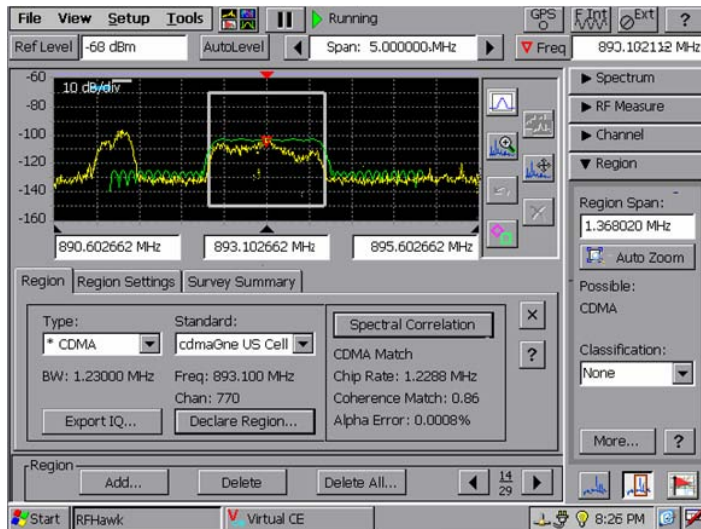


Figure 4. RFHawk offers both simple and sophisticated signal Identification (ID) capabilities. The green reference signal profile of cdmaOne's spectrum allows us to compare its shape with the yellow received spectrum.

Identifying and classifying a transmission poses a particular challenge to the signal hunter, requiring extensive knowledge of the modulation characteristics that make up a signal's spectrum.

The modern portable signal-hunting tool offers expert systems that guide the user in identifying and correctly classifying signals. This is important because illicit signals can blend in with a background of hundreds of legitimate users and occasionally attempt to mimic known signals.

The specialty signal identification features are a key element that separates the true signal-hunting instrument from most general-purpose test equipment.

Visiting the Source

After identifying a suspect signal in the radio spectrum, the next challenge is to locate the transmitter and ultimately its owner.

Automatic GPS navigation combined with a directional antenna and signal strength readings, enables users to plot the direction from which a signal is emanating at a variety of precisely located points on the map. Using the direction of strongest signal arrival from a few points, one can rapidly narrow the search area, homing in on the target. Thus RF signal emitters can be found, identified and physically visited.

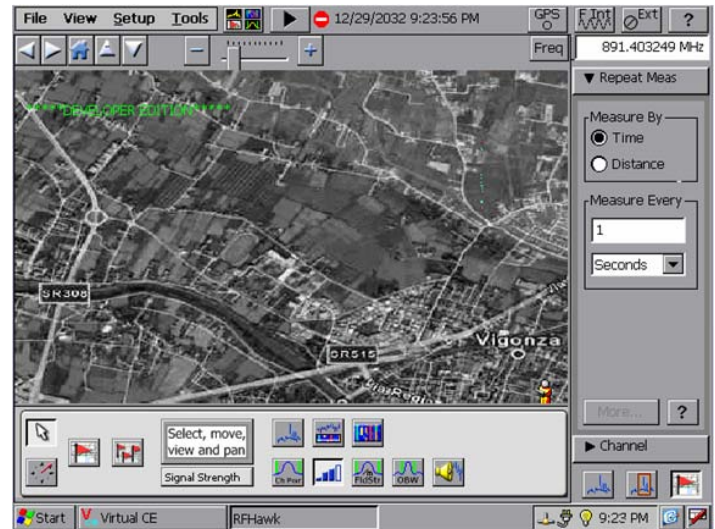


Figure 5. GPS mapping technology and DF capability guides users to the physical location of signal emitters. RFHawk can display a wide variety of map types by converting them to its native format.

Historical Solutions

Signal Direction Finding (DF) systems have been around for many years. Most of these systems, however, are special purpose machines that don't incorporate all the functions of a true signal hunter – namely, scan, identify/classify and locate (DF). Many of these DF systems were also composed of a variety of special purpose instruments, making such solutions less than ideal.

On the less expensive end of equipment options, the general-purpose spectrum analyzer has been a popular tool. Unfortunately, few were designed for efficient, portable, battery-powered field operation, making these a clumsy choice. The spectrum analyzer designed for test and measurement also lacks important signal identification capability and GPS mapping ability.

Furthermore, those spectrum analyzers that were portable had dismally slow spectrum scanning performance, resulting in poor Probability Of Intercept (POI) for elusive burst signals. The general purpose spectrum analyzer also typically has a very high noise figure, offering little for intercepting weak signals.

Many of these limitations are surmountable by cobbling together additional instruments, but the low cost spectrum analyzer approach rapidly becomes a high-end custom system.

On the high end of equipment cost, many well-funded agencies opted for expensive vans filled with specialized equipment primarily designed for signal monitoring and collection applications. These high-end, budget-breaking systems usually feature extensive intelligence gathering capabilities, of little value to the signal hunter. Such systems

offer good receiver noise figure and improved POI with faster scan rates, but sophisticated data collection and recording features are simply impractical when trying to chase down a host of small portable wireless devices in buildings or densely populated areas.

Until now, the technology to provide an effective field-portable signal hunting solution with sophisticated classification capability has been elusive.

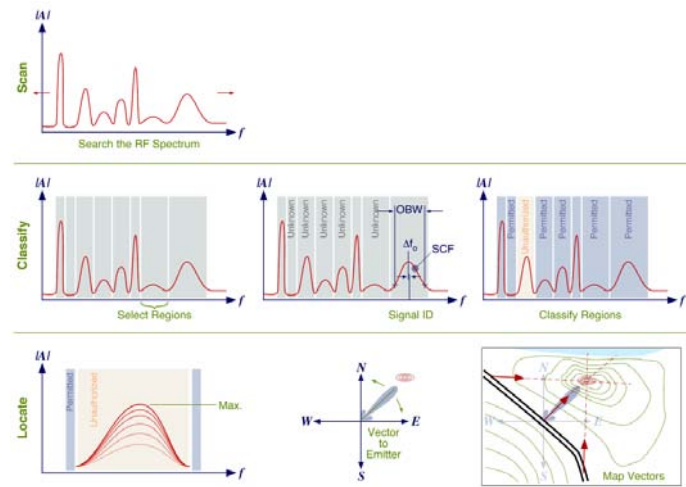


Figure 6. The signal hunting process involves three distinct steps. The RF spectrum is scanned, regions of interest are selected, and signals are identified by their spectral characteristics enabling classification. Finally when suspicious signals are found, using a directional antenna, vectors to the emitter can be mapped to locate the source of emissions. Signal identification and classification technologies are critical capabilities for signal hunting.

A Modern Approach

What is needed is a lightweight, rugged, portable analyzer with outstanding battery performance. To go beyond conventional test equipment solutions a true signal-hunting device should incorporate the key features unique to signal hunting. Spectrum survey regions, received signal strength displays, integrated GPS mapping capability, and expert signal ID analysis tools like profile overlays and advanced spectral correlation function analysis, would be a great help in sorting out exactly what lies in the spectrum.

Tektronix, a leader in real-time spectrum analysis for over two decades, has now applied advanced spectral correlation density algorithms and integrated mapping

technologies to the real-time spectrum analyzer. Some of the most difficult challenges of signal hunting can now be addressed with a highly portable, light-weight unit, at a price point that fits much better than larger and poorly integrated systems. RFHawk truly represents a new class of dedicated signal hunter.

In many ways this new class of signal hunter rivals the sophisticated and expensive high-end surveillance system historically applied to signal hunting, at a fraction of the price. RFHawk is the first all-purpose signal hunter to provide the portability demanded by today's highly mobile pocket sized wireless devices.

Key among the features that elevate RFHawk to the head of the class is the sophistication of its signal identification and classification. Let's review why signal ID and classification is critical and why it separates spectrum analyzers from true stand-alone signal hunters.

Signal Classification

Signal ID is an important element to understanding the nature of a transmitting device. After scanning the frequency band, it is necessary to sort out what signals belong there and which might be tied to suspicious activity. For example, a Frequency Modulated (FM) signal found in the middle of a cellular band that uses Gaussian Minimum Shift Keying (GMSK) probably indicates an unauthorized and covert use of the frequency spectrum. Depending on what is found, one of several possible signal classifications may be appropriate.

The challenges of looking at a signal's spectrum and identifying the type of modulation contained within it can vary from easy to extremely difficult. Thus to hunt down rogue transmitters, signal ID features are an essential capability beyond simply viewing the spectrum and direction finding to the transmitter's location.

RFHawk provides different signal ID technologies for different levels of assurance that the ID and classification will be correct. Rapid and robust ID capabilities protect against spoofed, fake or imitation signals that are designed to go unnoticed.

Another common problem is that signal observations may occur under poor transmission reception conditions. Covert operations or merely the need to avoid public scrutiny can dictate suboptimal antenna positioning, weakening the received signal and making identification more difficult.

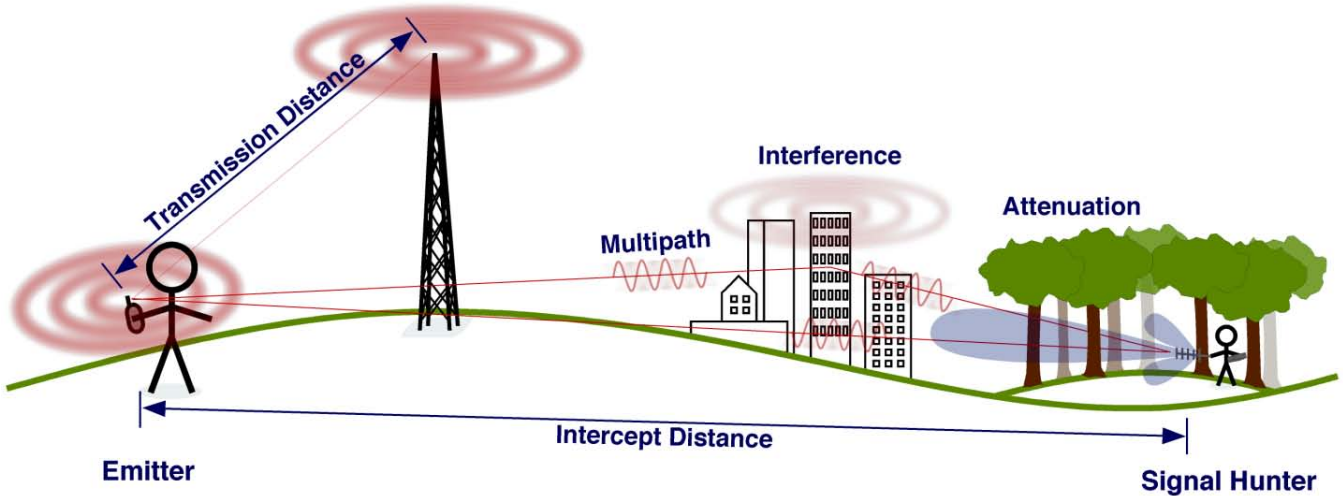


Figure 7. The signal hunter is often at a disadvantage when it comes to receive signal strength. Multi-path, interference or greater distances to the emitter give rise to the need for good receiver performance and advanced signal ID features.

Such situations call for advanced signal identification algorithms that are capable of sorting out signal types without sufficient energy to demodulate the signal.

Before exploring the details of identifying signals with insufficient signal to noise ratio to demodulate them, let us review the process of searching the spectrum for signals.

Scan

Often, the starting point in searching for rogue signals is looking for new energy.

Finding New Energy

RFHawk's auto mask feature enables the user to rapidly create a mask around current spectral activity. When new transmitter energy appears above the mask, triggered alarms can alert the operator of its presence. This provides a first line defense against short duration burst signals that may be attempting to flash by unnoticed.

Once the mask is triggered, the user can tap over to it and begin identifying the new signal.

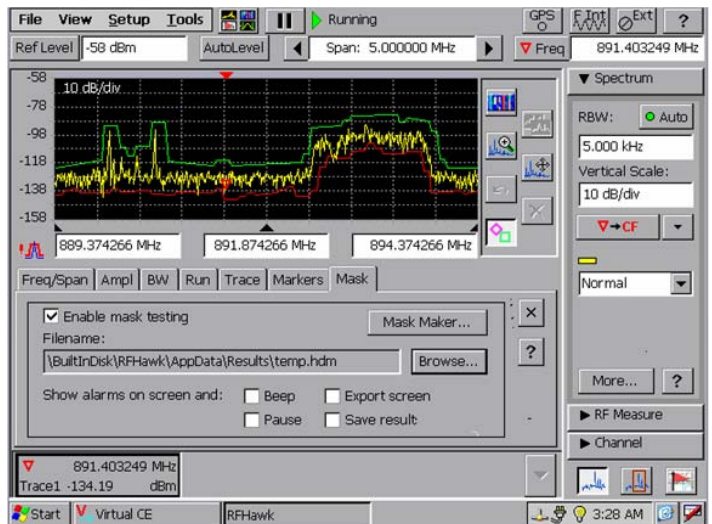


Figure 8. RFHawk's Auto-Mask feature helps find new energy by building a spectral mask around the current signal. When the mask is broken, operator alarms can be triggered.

Unique Fast User Display Interface

Searching the spectrum and identifying signals requires a considerable amount of spectrum analyzer display manipulation. Intermittent signals, buried signals and the sheer number of signals in the spectrum all demand rapid display manipulation.

On conventional spectrum analyzers the continuous panning up and down in frequency, then zooming in and out on individual signals is a time consuming process. Popularized in the 1970s, the classic single digital adjustment knob for dialing in frequency, span and marker measurements is by today's technology cumbersome at best.

To be more responsive to the signal hunter's dynamically changing signal environment, Tektronix reengineered the user interface for RFHawk to allow a much faster approach to viewing key events in the spectrum.

RFHawk uses a touch screen display that is sensitive to commands drawn on the screen. At the same time, the improved signal cursor performs more rapid signal observations, adding up to a giant leap forward over the conventional single input knob on most analyzers today.

Either a finger or a stylus depressed on the screen can slide right or left to move the center tuning frequency. This produces the effect of 'grabbing' the spectrum and pushing it right or left through the display window. Similarly, amplitude can be adjusted up or down by simply grabbing and sliding the trace up or down.

Also, unlike conventional displays, the span function operates around the cursor. This takes advantage of the ability to move the cursor to any point on the display by tapping on that point. To zoom in on a particular signal, one can simply tap on it and reduce the span by drawing a diagonal line from the top left to the bottom right. These two simple motions on the display replace a half dozen key strokes and turns of the knob on conventional analyzers.

A tap of the stylus can also select the demodulator frequency and spectrum region. Dozens of signals across the display can be quickly evaluated by tapping on them. The touch screen also has a variety of sounds to provide input pressure and operation feedback, along with a mute capability of all sounds for covert or sensitive applications.

To better understand the operation of the touch screen, the reader may wish to refer to the videos on Tektronix.com or request a demonstration.

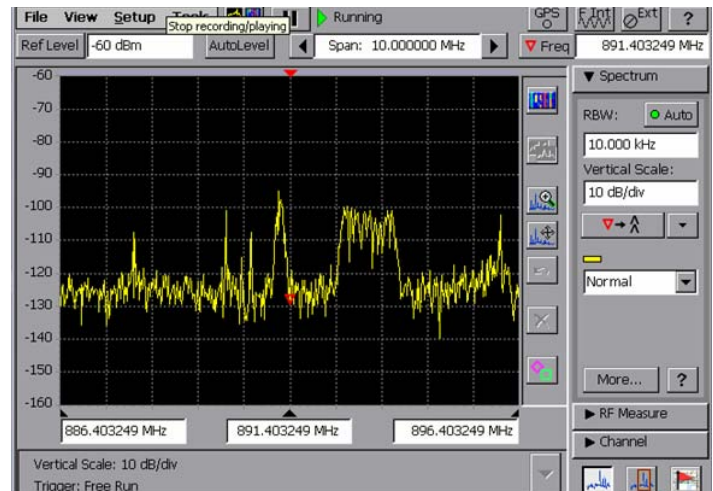


Figure 9. RFHawk features a touch sensitive screen that accelerates searching the spectrum by simply tapping on signals or sliding the spectrum for optimal viewing.

Designed for Challenging Signals

As mentioned earlier, most spectrum analyzer products are designed for laboratory environments and lack key surveillance and signal hunting performance traits that are important when classifying signals under less than ideal conditions. Let us explore some of these technical issues.

Unlike most general-purpose spectrum analyzers, RFHawk offers a low system noise figure of 10 dB. This is a key advantage under poor signal level conditions where weak signals can easily be buried in noise added by the measurement instrument. When compared to the typical 30-to-40 dB noise figure of most general-purpose spectrum analyzers, RFHawk can effectively operate under weak signal conditions without bulky add-on preamplifiers or a larger antenna.

Bandwidth is another important feature for a signal hunter. RFHawk's 20 MHz of real-time BW is sufficient for most common wireless devices. By today's bench-top spectrum analyzer standards for very wide IF bandwidth, like the RSA 6000 with over 110 MHz of bandwidth, RFHawk is considerably narrower. However, amongst battery-powered field-portable instrumentation, RFHawk is superior.

Spectrum scan rate has long been a key differentiator for signal surveillance applications, as the faster the scan-rate, the better the POI for certain burst signals trying to avoid detection. RFHawk also offers an ultra-fast scan rate by virtue of its FFT based hardware. Again, amongst the portable battery-powered equipment available, it is currently the best in class.



Experienced users often notice the outstanding spectrogram characteristics of **RFHawk** relative to competitive products. The uniquely clear spectrograms arise from its rapid FFT spectral update rate. With improved time resolution and elimination of tremendous amounts of dead time between spectral samples, a clearer signal view is presented. Again, the reader may wish to refer to video comparisons available on Tektronix.com.

I-Q export capabilities for offline analysis are also possible with **RFHawk**, so events of particular interest can be brought back to the laboratory for more detailed analysis.

Finally, another important capability for the signal hunter or surveillance operation is remote LAN control for leave-it-in place applications. An integrated LAN port allows operation of the instrument from virtually anywhere in the world for monitoring situations at a safer distance.

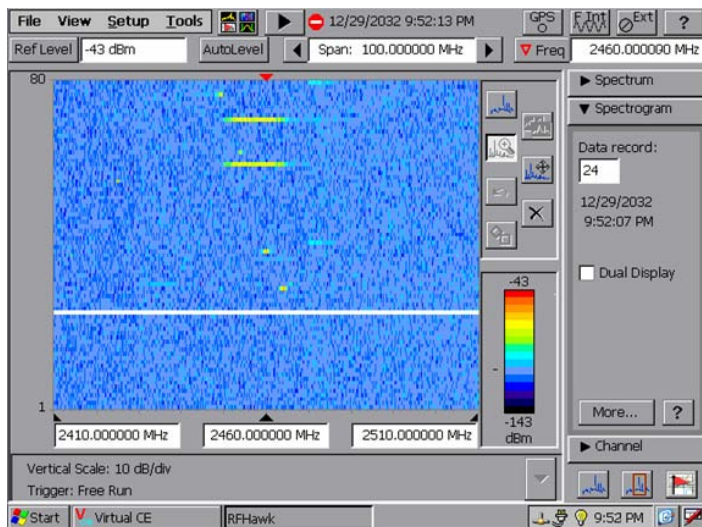


Figure 10. *RFHawk's spectrograms offer a uniquely clear representation of the spectral energy present compared to conventional analyzers. This is due to the very high update rate of the FFT based spectrum analyzer.*

Classify

Finding improper use of the radio spectrum is often a tedious and slow process of elimination. One by one, authorized or permitted signals are found and eliminated from the search until only questionable signals remain.

Spectral Regions of Interest

We begin by breaking up the spectrum into regions of interest, wherever a signal is being transmitted. **RFHawk** allows users either to snap regions of interest to the channel raster grid or place them randomly over the spectrum.

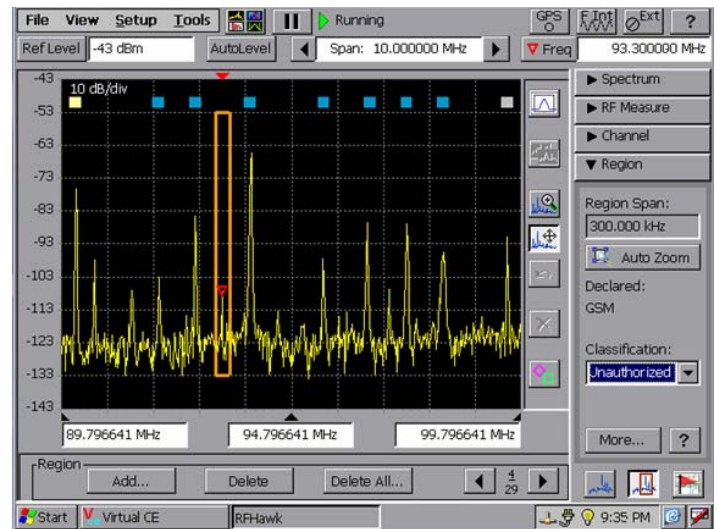


Figure 11. *RFHawk allows the user to select regions of the spectrum and assign a classification to each region. Permitted signals on the FM broadcast band channel raster are shaded blue, unknown signals are shaded yellow, and not permitted spurious is shaded orange.*

Automatic comparisons of popular channel raster plans or user-definable raster patterns aid in determining if the signals found belong to a regulated group. Popular cellular bands, WLAN and other common channel rasters come preprogrammed into **RFHawk**.

Once signals are found, a box is then drawn around the signal, allowing basic signal comparisons for ID purposes. Does the signal fall on the regulated raster plan or is it somewhere a signal doesn't belong, such as in the middle of a stop band?

If the signals do fall on the correct channel frequencies, the next step is to verify that the bandwidth and shape of the signal are correct for the authorized modulations used in the band.

Categorizing Signals

RFHawk provides spectral profiles to aid in identifying signals. Received signals are often distorted by multi-path and dispersion in the channel. Turning on a spectral profile of what the signal theoretically looked like as it left the transmitter can be invaluable in identifying its modulation type from its spectrum, and ultimately whether the signal belongs in the band. Many modulation spectral profiles are preprogrammed in RFHawk for popular wireless standards. The user can also define a profile for a new modulation or a less common signal shape.

If a signal fits or appears to fit on the channel raster and has a modulation shape similar to the spectral profile, some simple RF measurements can help to confirm the signal is a permitted use that meets the regulatory requirements. Occupied BandWidth (OBW) measurements can provide additional confidence that the signal's bandwidth fits the regulatory agency's requirements.

Analog Amplitude Modulated (AM) and Frequency Modulated (FM) signals have a less distinct modulation profile and bandwidth. RFHawk offers both AM/FM demodulation capabilities to listen in on analog signals and identify them where legally appropriate. With an 8 kHz AM demodulator and FM demodulators ranging from 8 kHz to 200 kHz, RFHawk handles a wide variety of two way radio services used for private businesses, aircraft and emergency services.

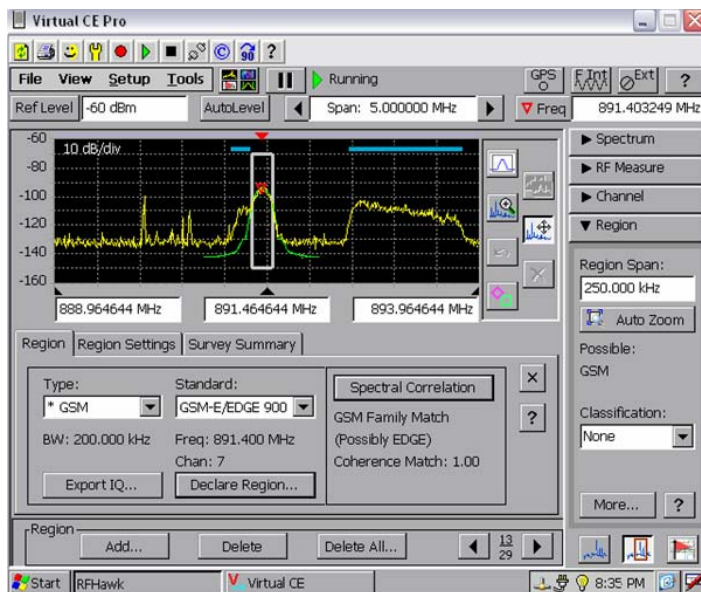


Figure 12. Spectral profiles can be very helpful in signal identification. RFHawk allows users to select either common preprogrammed profiles or custom entered profiles.

Sophisticated Tools Aid in Classification

RFHawk allows the user to classify the signal in one of four ways:

- None (Un-analyzed)
- Unknown (Not Identified)
- Unauthorized (Identified & Not Allowed)
- Permitted (Identified & Allowed)

Initially all signals start out with no classification, then progress to identified and classified as each is examined. As each emitter is classified, signals of interest can be sorted out from those properly using the radio spectrum.

First level ID tools are great for easy signal types at strong signal levels, but what of imposter signals or those mostly buried in the noise?

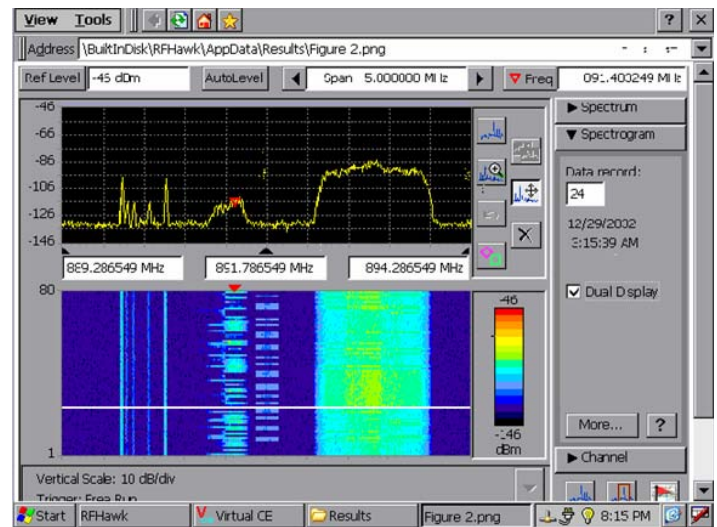


Figure 13. An illegal FM signal sits next to a legitimate GSM signal. Subtle differences in spectrogram 'splatter' indicate something might be wrong with the signal, but expert analysis is needed. RFHawk offers sophisticated spectral correlation density analysis to determine if the signal is an imposter.

In many cases expert analysis is needed to rapidly characterize or identify signals that are either badly distorted by the channel or are imposter signals designed to avoid detection.

Demodulation and eavesdropping is often considered an efficient approach to determining what a signal is used for, but it may not be the best option. Insufficient Signal to Noise Ratio (SNR) from a suboptimal signal intercept position or limited antenna size may prevent successful demodulation. Listening in may also be illegal or require time consuming legal hurdles. Even when authorized, listening in can be a slow process, as voice traffic might not immediately reveal what the data link is being used for.



RFHawk, like many other spectrum analyzers, does offer basic AM and FM demodulation, useful for listening in on many industrial and emergency service bands. More complicated signal modulations or difficult reception conditions demand a better solution for identifying the nature of the transmission.

Expert signal ID capability that doesn't require signal demodulation separates true signal hunters like **RFHawk** from less sophisticated general-purpose test instruments. **RFHawk** has a unique spectral correlation density signal ID analysis function that surpasses the basic first level tools of frequency and bandwidth measurements.

Spectral Correlation Function

Spectral Correlation Function (SCF) analysis uses statistical techniques to provide an expert opinion on the probability that a particular signal type matches a known modulation standard. It is important to note that **RFHawk's** expert signal identification provides an analysis result, but leaves the final signal classification selection up to the user. This gives the user both the benefit of extensive ID capability and the flexibility to classify a signal in any way deemed appropriate.

The process by which SCF analysis is able to identify signal types in specific regions may seem mysterious, but is fundamentally based on advanced statistics.

Spectral Correlation Function

SCF technology can be understood in terms of an extension of RF spectral analysis to a more generalized case.

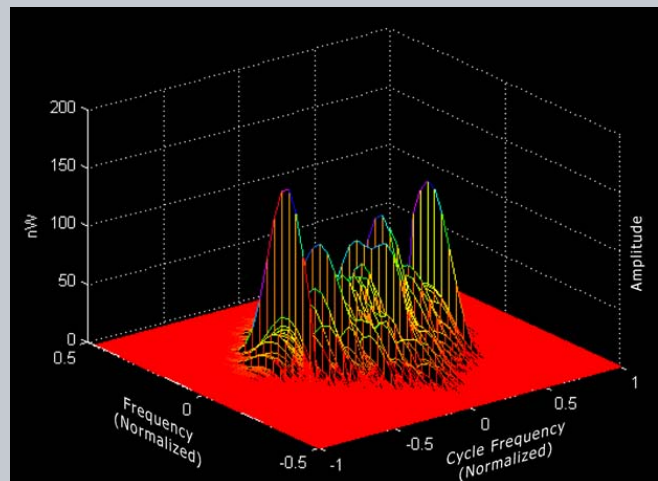
In RF spectral analysis, a time varying voltage is passed through a narrow bandwidth filter, the Resolution BandWidth (RBW) filter. The signal emerging from the filter represents a narrow slice of the spectrum at a given frequency. The detected voltage signal coming from the filter is squared making it proportional power. The RBW filter is then swept or stepped in frequency to piece together the RF spectrum.

The Spectral Correlation Function (SCF) uses a similar process but with a few important differences.

Instead of using a single narrowband RBW filter, two filters of equal bandwidth and equal spacing from the center frequency are employed. The spectral correlation function shows how pairs of filter outputs at different center frequency offsets (cycle frequencies) are related over time. The outputs of the two filters are multiplied together, down-converting them to base-band where their correlation is measured. By correlating the two filters at different center frequencies and offset spacings, the spectral correlation function emerges.

The resulting plane of data (power correlation, center frequency and filter offset spacing or cycle frequency) contains a variety of quantifiable elements that are modulation specific.

Modulated signals produce significant spectral correlation only at particular filter pair cycle frequency separations. This is because, digital modulations are composed of a variety of symbol rates, chip rates, hop frequencies, slot rates, frame rates, and events that give rise to correlation peaks at specific cycle frequencies. The SCF provides a unique signature for many modulation types. This information can be used to verify whether a transmission is of a particular modulation standard or a fake for an unauthorized purpose.



*The spectral correlation function of a signal reveals a complex pattern of peaks and valleys unique to a given signal type. **RFHawk** uses this intermediate SCF data for identifying unknown signals.*

SCF technology can sort out internal signal patterns to determine the probability that the signal is of a given type.

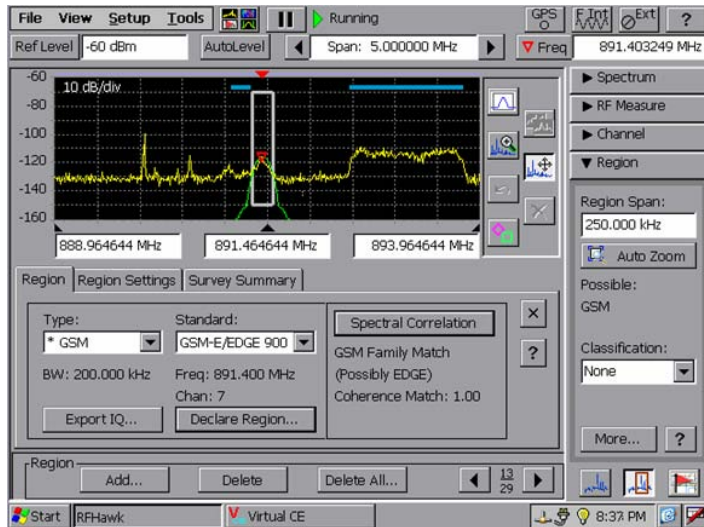


Figure 14. Spectral correlation density analysis of a signal sorts out the nature of a GSM signal, determining a high probability of a match, even though the signal is too weak to demodulate effectively.

Spectral correlation is generally much more effective than actually demodulating the signal, particularly in low signal to noise conditions. Not only can the signal type be identified without ever demodulating it, thereby avoiding potential legal issues, in many cases the SCF analysis will work at a SNR below where the signal can be successfully demodulated.

RFHawk's SCF capability helps operators quickly understand the received signal and whether further investigation is needed.

Location

Once signals of interest are found, physically visiting the transmitter that produced them is usually desirable, requiring some means of direction finding or homing in on the signal. Viewing a map of the surrounding area significantly enhances DF capability, as transmitters are often located in such settings as hilltops. Mapping capability also provides a convenient means to document where signal measurements were made and under what transmission surroundings. With knowledge of terrain and other geographical features, even relatively simple DF capability can rapidly lead to the location of a desired transmitter.

RFHawk features integral GPS mapping capability that physically locates the instrument on a map anywhere in the world. A fast drawing bit map approach allows a wide variety of map standards to be converted for use on the instrument. This makes street maps, topographic maps and even large building floor plans suitable for display on RFHawk.

Special mapping tools are provided to capture user-drawn vectors that point to the strongest direction of signal reception. Annotating a few measurement points directly on top of the map can quickly point the way to a rogue emitter.



Figure 15. GPS mapping capability significantly helps narrow DF information to home in on transmitter locations.

Built-in audio and visual aids assist in finding the direction to the emitter by providing rapid signal strength feedback. A handheld directional antenna can scan the horizon for strongest signal level. Either a bar graph display or an audio tone that changes frequency with increasing Received Signal Strength (RSS) allows the operator to select the appropriate azimuth to the target.

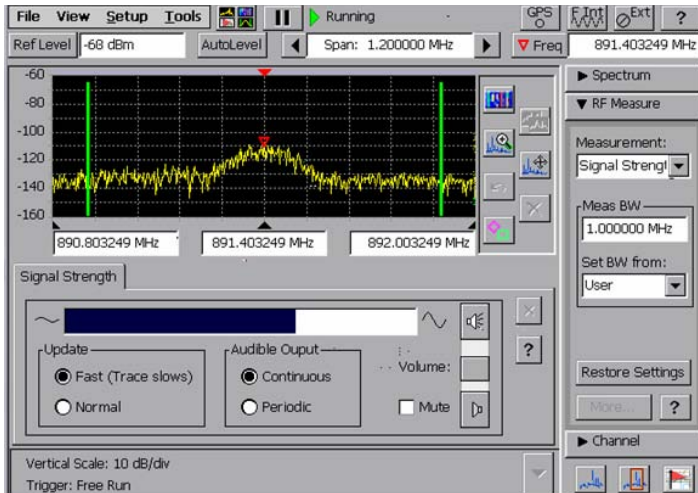


Figure 16. RFHawk's signal level meter with audio signal strength tones and a directional antenna allow rapid determination of the emitter's direction.

Selection of the appropriate antenna can minimize sidebands and provide a distinct peak signal strength point for an optimal vector to the target. Of course multi-path can affect the bearing angle to the target, however by knowing the terrain and taking a few data points, one can usually spot and discard the erroneous vectors.

Mapping and geo-location rounds out RFHawk's capability, offering the complete set of functions needed by the signal hunter in one compact, portable unit.

Conclusion

RFHawk meets the demands of an important and growing group of signal hunting applications used by a variety of agencies.

Beyond its hardware designed for surveillance, the fastest scan time in the industry for a portable instrument and outstanding noise figure, it possesses the sophisticated tools needed to rapidly classify signal types.

Sorting through the permitted signals to find the offending illegal emitter is often the most difficult aspect of hunting for inappropriate use of the RF spectrum. RFHawk has both the first level signal identification tools for easily recognized RF modulations, and the higher level tools that permit positive identification at signal to noise ratios that simply would not permit demodulation. Using spectral regions to classify identified signals is a simple process, and with its innovative touch screen display interface, RFHawk is remarkably fast at zooming in on spectral regions of interest.

RFHawk solves the signal hunter's problems in a truly compact field-portable box that can quickly and unobtrusively find and locate unauthorized emitters. While RFHawk is not a high-end and costly surveillance-monitoring tool, it is a very effective signal hunter – ideal for field use at a fraction of the price.

To learn more about how RFHawk can solve your signal hunting applications, arrange for a demonstration today through your Tektronix representative.

About Tektronix:

Tektronix has more than 60 years of experience in providing network operators and equipment manufacturers a comprehensive and unparalleled suite of network diagnostics and management solutions for fixed, mobile, IP and converged multi-service networks.

These solutions support such architectures and applications as fixed mobile convergence, IMS, broadband wireless access, WiMAX, VoIP and triple play, including IPTV.

Learn more about Tektronix' communications test, measurement and network monitoring solutions by visiting:
www.tektronix.com/communications

For Further Information:

Tektronix maintains a comprehensive, constantly expanding collection of application notes, technical briefs and other resources to help engineers working on the cutting edge of technology.

Please visit www.tektronix.com/communications

Contact Tektronix:

Please visit www.tektronix.com/communications

Phone:
1-800-833-9200 option 1
+1-469-330-4000

Locate your nearest Tektronix representative at:
www.tektronix.com/contactus