RF Trace Analysis Primer

By Thomas H. Jones, REI General Manager
June 21, 2005

Abstract

REI has developed a new detection technology called Trace Analysis for identifying and locating RF signals associated with espionage related surveillance devices. These analysis techniques have been developed and optimized primarily in the firmware and software associated with the OSCOR 5000E (Omni-Spectral Correlator) and the OSCOR PC software. This document is intended to be non-technical for quick understanding of the basic principles, but some limited technical points are included for completeness. The main goal is to explain the basic concepts using a real world example and screen shots taken from the OPC software.

Background: Understanding of RF Propagation Loss

RF propagation loss refers to the RF energy loss associated with distance; as the distance from a transmitter increases, the RF energy decreases. The reverse is also true: as you get closer to a transmitter, the RF energy increases.

The most basic and simplest theory is often called Inverse Square law theory. Additional information on the Inverse Squares Law can be found in Appendix A of this report.

In mathematical terms, as the distance from the transmitter is increased, the received power decreases with the square of the distance. More importantly, in the most useful terms for TSCM, if you half the distance to a transmitter, the signal level increase is quadrupled.

Therefore, getting close to a transmitter provides tremendous advantage to detecting threatening transmitters; this is a fundamental principle in Trace Analysis Methodology.

Note: The Inverse Square law theory works well in large open fields or ideal laboratory settings. However, in practice (particularly indoors) RF propagation loss is affected by many factors as the RF energy may be absorbed, scattered, or attenuated as it comes in contact with surfaces such as metal, masonry and brick, wood, glass, etc. (see Appendix A). However, the relationship between RF energy and distance to the transmitter still provides a tremendous advantage for TSCM purposes.

Introduction to Trace Analysis

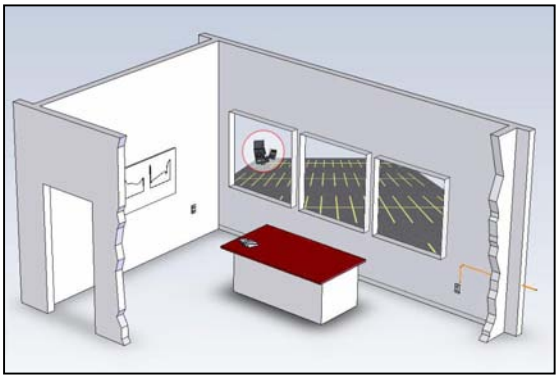
Before discussing the methodology of trace analysis, it is important to understand the OSCOR concept of capturing a peak trace. The peak trace function is very similar to the Max Hold function in most Spectrum Analyzers. However, there is a very important difference in how the data is stored: in most Spectrum Analyzers, the Max Hold function is a memory buffer that is tied to the Spectrum Analyzer display, and therefore, as long as the frequency range of the spectrum analyzer is not changed, then the function will display the cumulative maximum graph of each individual pass through the current frequency spectrum. This Max Hold data may be stored and recalled later, but it is tied specifically to the current displayed frequency range, and is typically lost when the frequency range or sweeping parameters are changed. However, the OSCOR Peak Trace mode is tied to a memory buffer that covers the entire OSCOR frequency spectrum. Therefore, regardless of the displayed frequency span, the Peak Trace Memory is always being updated in the background. In other words, the OSCOR Peak Trace Mode is on all the time and cannot be turned off with the exception that the memory buffer can be cleared (erased manually) when entering a new environment. This functionality is a great improvement over basic Max Hold concepts because it provides the ability to investigate and analyze suspicious portions of the spectrum while maintaining and updating a single data file of the complete spectrum.

Hence the basic methodology of trace analysis relies on the process of capturing Peak Trace data from different locations or from different times and performing spectrum comparisons to look for anomalies.

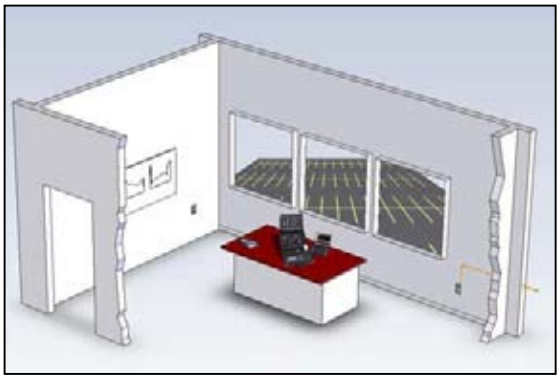
Peak versus Friendly

The most basic method of trace analysis is a basic 2-step process:

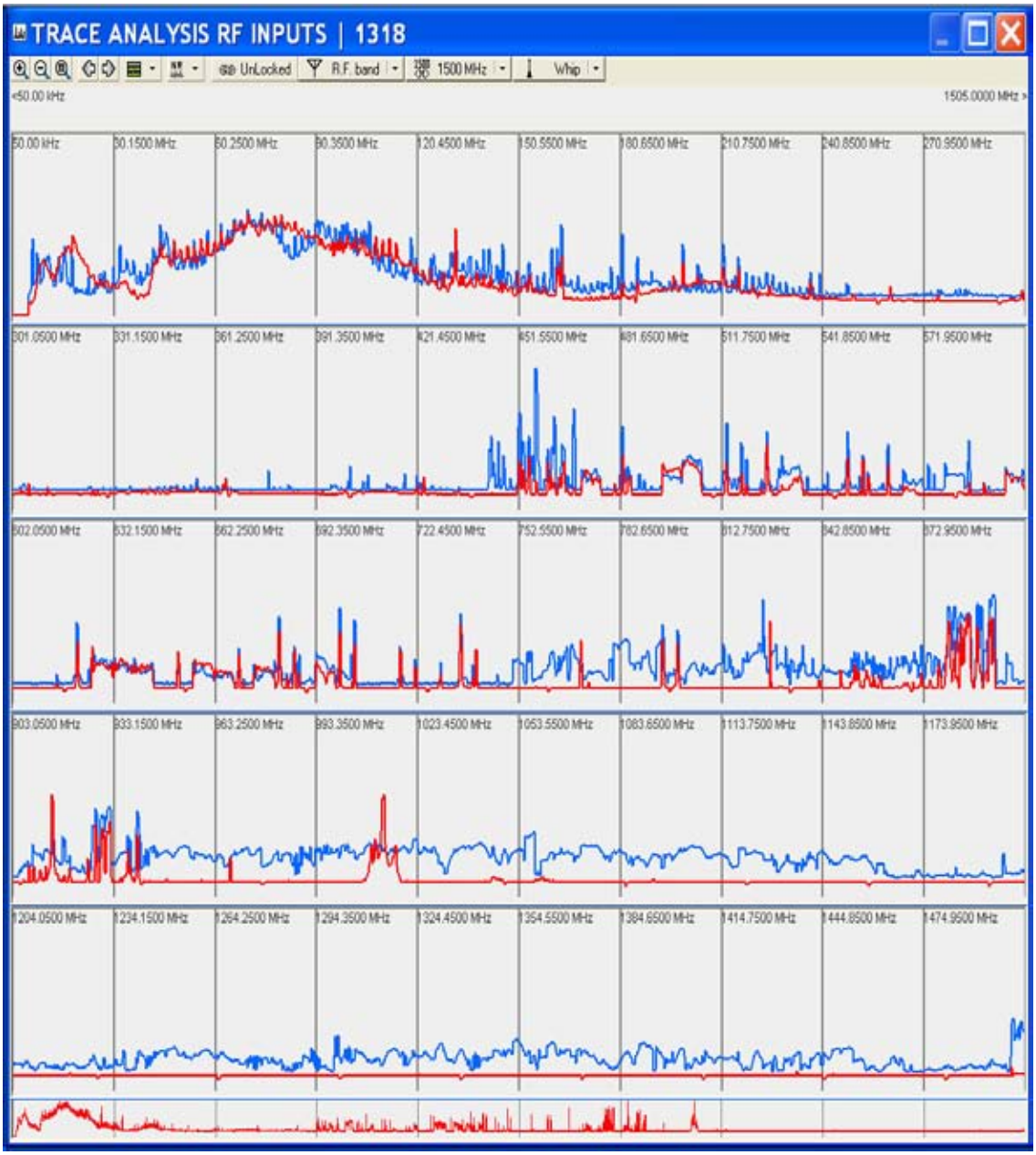
1. **Capture a *Friendly* Trace** at a safe distance from the target environment. Typically this can be done in the parking lot of the building at a reasonable distance from the Target Room. This Peak Trace is called the Friendly Trace. This data should be captured for at least 5 minutes, but better performance will be achieved by increasing the Friendly Capture time.



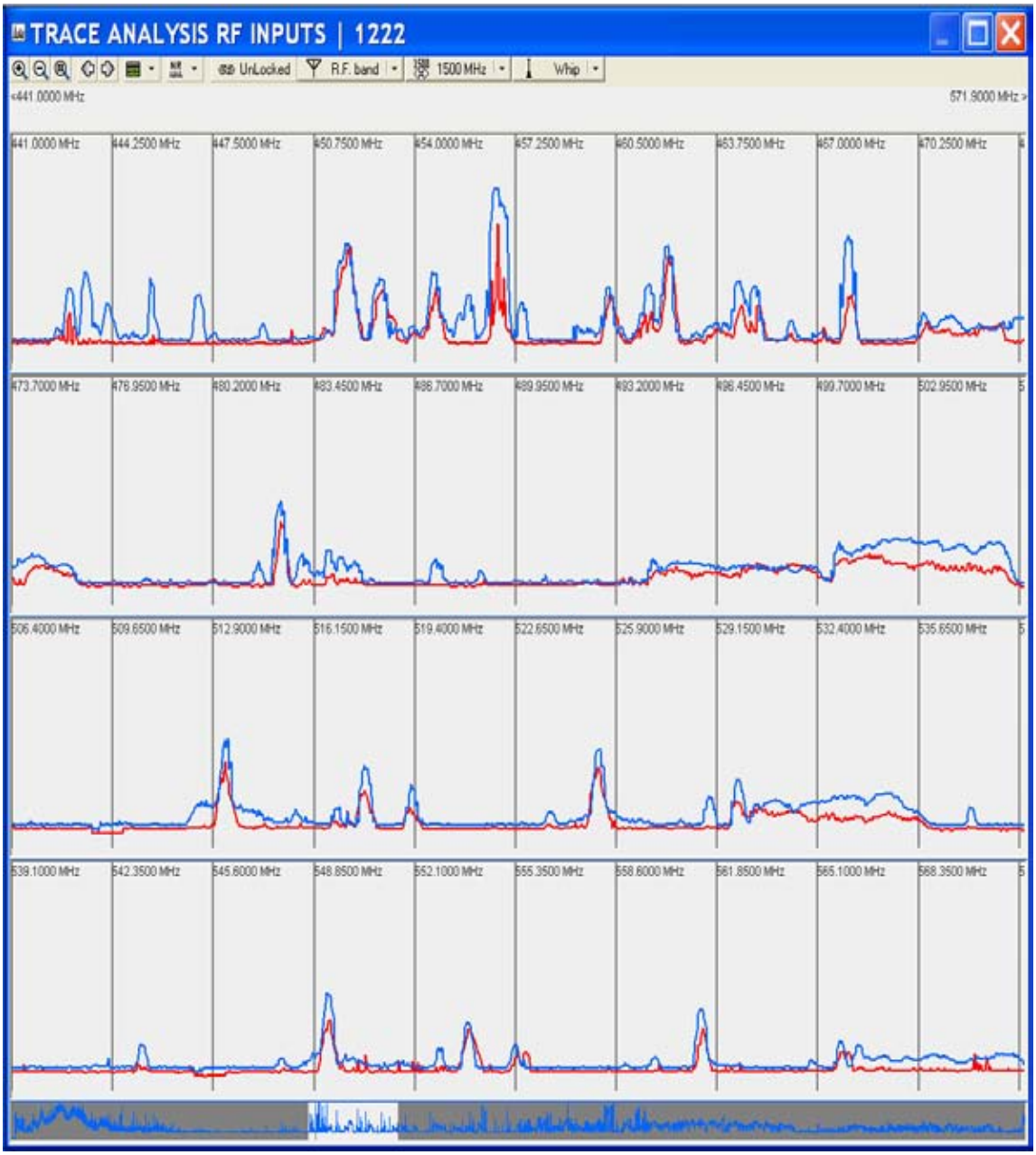
2. **Capture Peak Trace** Data from the Target Environment, and then compare the differences between this trace data and the Friendly Trace. Again, this trace data should be captured for at least 5 minutes, but allowing the Peak capture to run for longer times will increase reliability against intermittent signals such as burst or frequency hopping threats.



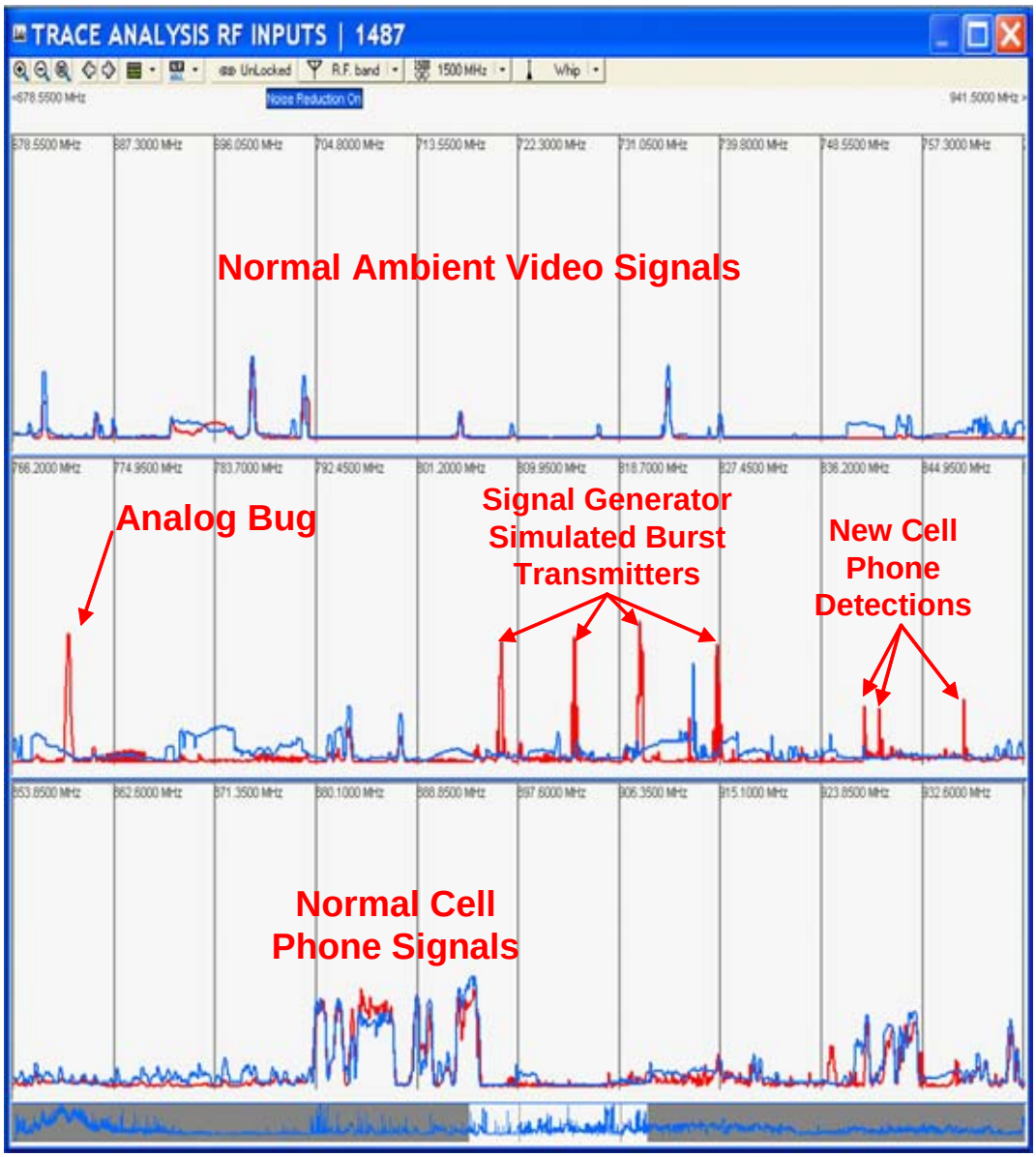
The figure below shows actual Friendly and Peak Trace data that was taken from a building in Dallas Texas. The **Blue** Color shows the **Friendly Trace** captured outside of the target sweep area, and the **Red** shows the **Peak Trace** taken from inside the target building. In General, the **Friendly Trace** should be larger or very close to the **Peak Trace** data.



The figure below shows a zoomed in portion of the previous data to show some **Friendly** signals. From this figure, it is easy to realize that the ambient RF signals are stronger outside the building, and therefore, whenever the **Friendly** is greater than the **Peak**, there should be no cause for concern.



However, the figure below shows a different zoomed in portion of the spectrum. In this section of the spectrum, there are several signals where the **Peak** is larger than the **Friendly** indicating a larger signal strength inside the building (meaning these transmitters are likely emitting from inside the building). Some of these signals are of no concern because they are expected in the ambient environment due to the intermittent nature of the signals (such as mobile phones or pagers), but others are actual threats. In this figure, these signals are readily identified and labeled.

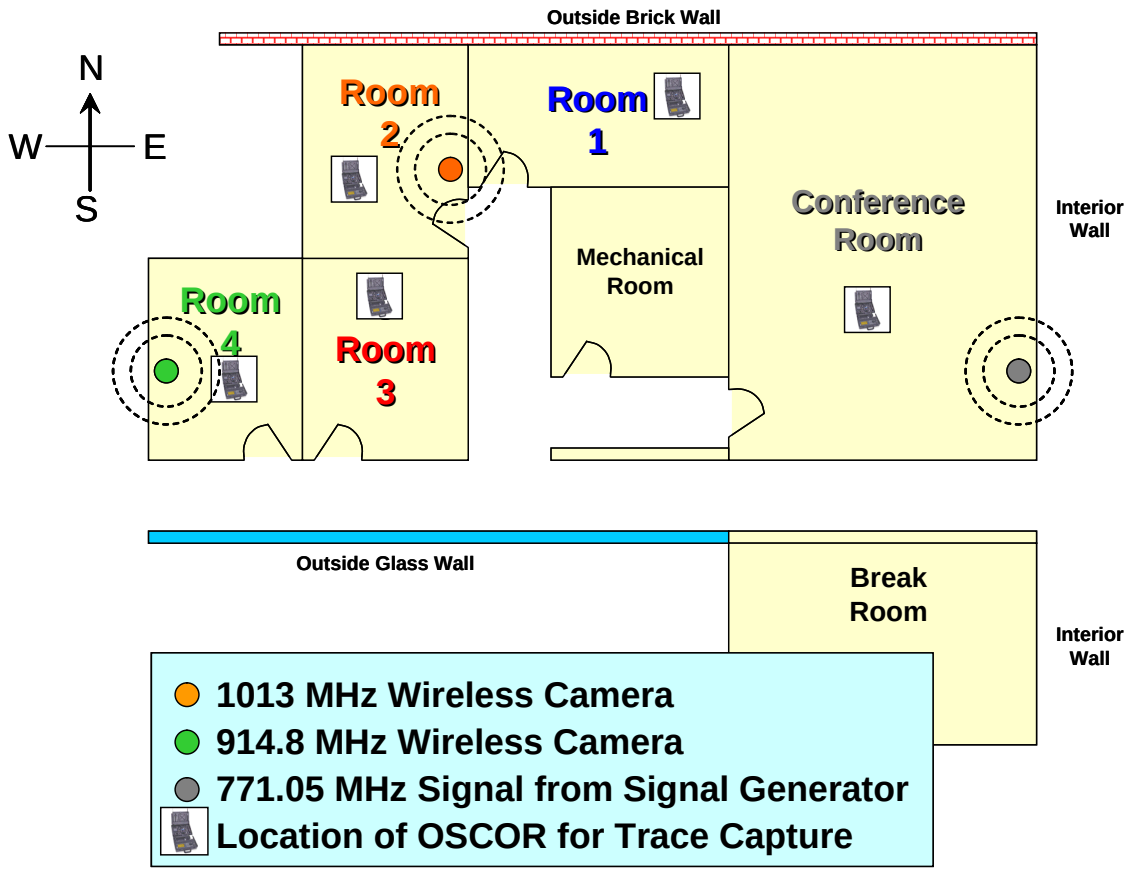


RF Mapping Concepts

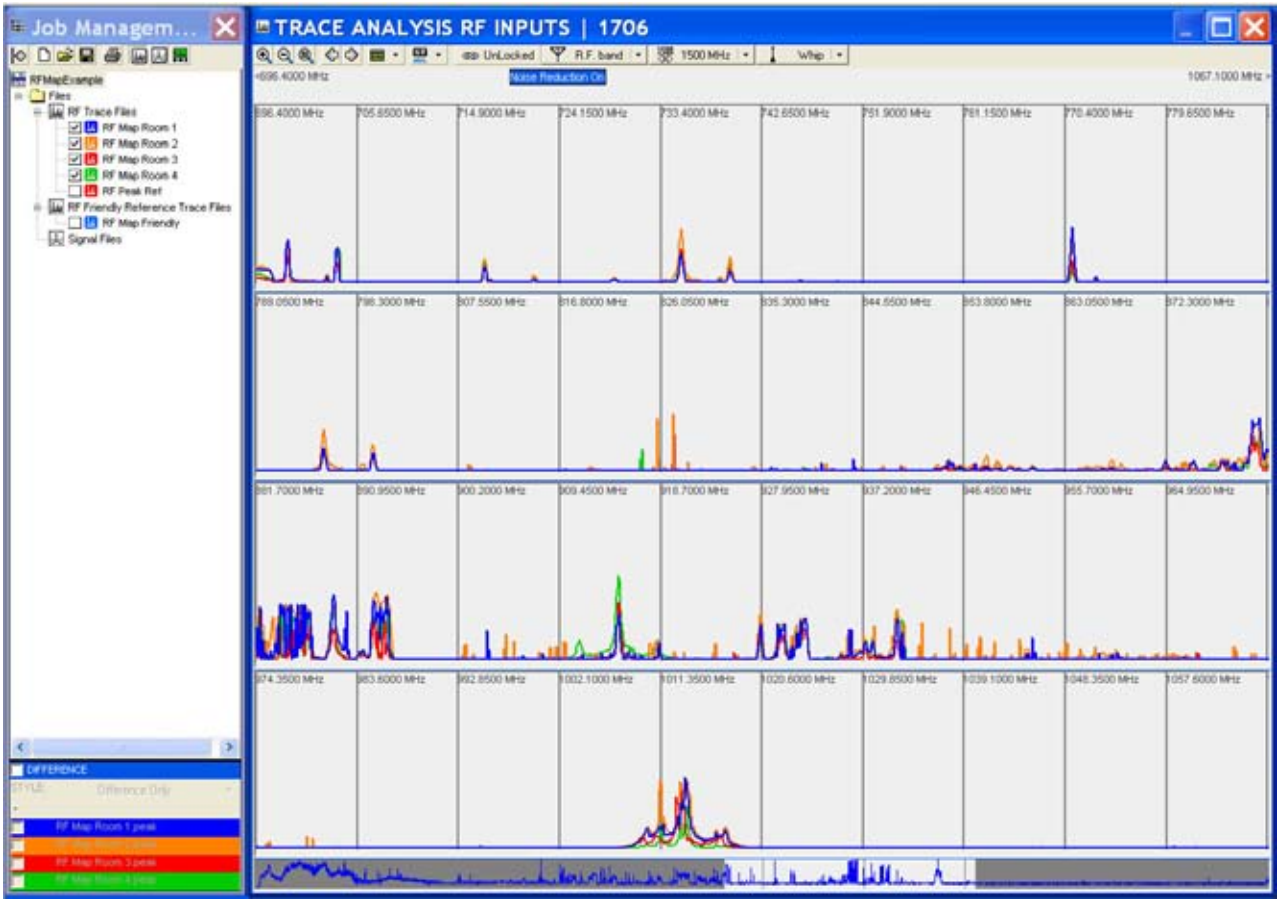
By collecting and storing Peak traces from multiple locations, the concept of trace analysis can be extended to a method of RF mapping. RF mapping refers to the process of taking Peak trace analysis data from different locations within a building and outside of a building and comparing the trace data. In this approach, it is beneficial to have Friendly trace data, but it is not absolutely necessary. This process may be more useful in high-rise buildings where it is not practical or reliable to compare Friendly Traces at the street level to Peak Traces that are 3 or 4 stories up. Furthermore, this process is extremely useful in getting a general idea about the direction from which a signal is being transmitted.

In the example below, trace data was captured during a training exercise in Dallas Texas in 4 different rooms. This data was taken by simply moving the OSCOR to each room, clearing the Peak Trace data, allowing the OSCOR to capture trace data for a few minutes, and storing the Peak trace data to a computer using the OPC software before leaving each room. The entire data collection process for this exercise took less than 1 hour and covered the frequency spectrum from 5 MHz to 3 GHz. However, in a real situation, it is recommended that data be collected in each room for at least 1 hour.

The map of this exercise (below) includes the locations of the OSCOR test points, 2 wireless video/audio “bugs” hidden in the offices for training purposes, and one signal generator. These video/audio signals contain FM modulated video with sub-carrier audio.



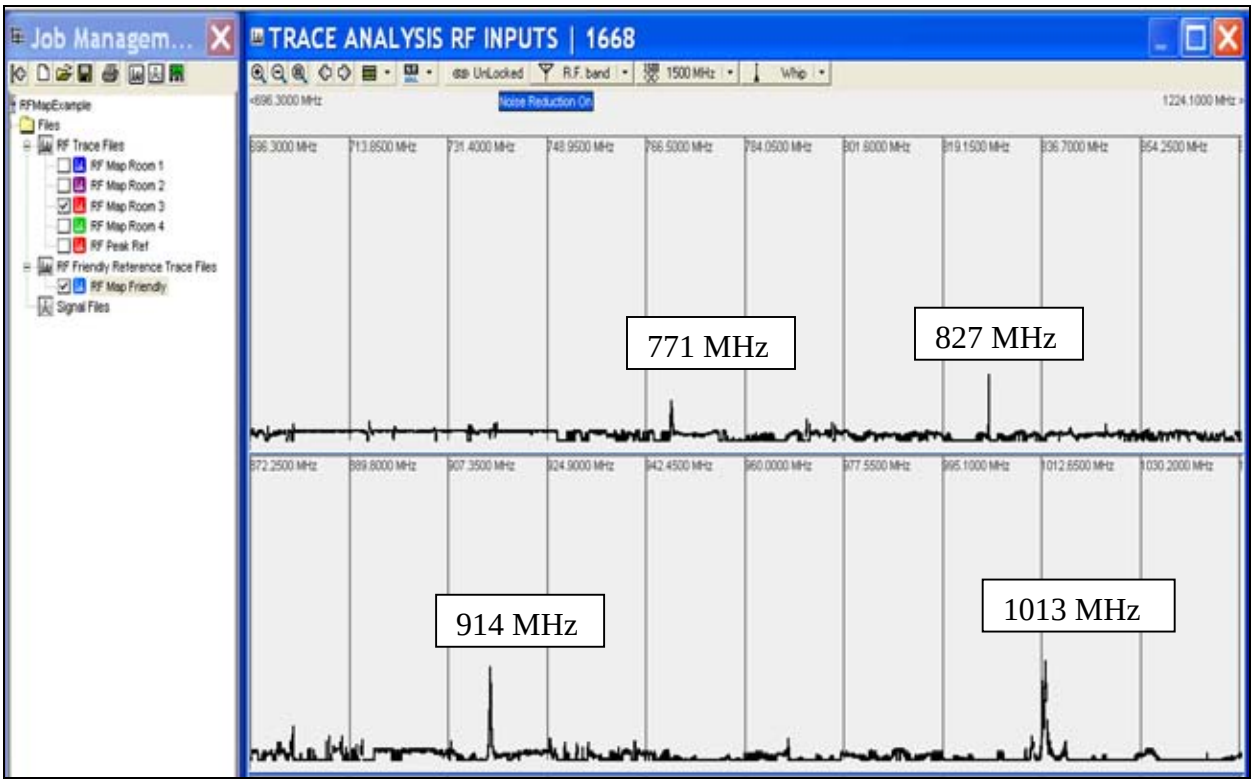
In order to keep this document brief and address the example threats, this document will only address a small portion of this spectrum from 700 MHz to 1100 MHz. A screen shot of the OPC software is shown below with the trace data from the 4 rooms (not including the Conference Room). This screen shot was taken using the OPC software and previously captured traces (no OSCOR is connected at time of the screen shot), and with the analysis display set to 4 display bands provide a detailed view of the spectrum.



In a normal analysis, the process would be the following:

1. If Friendly Trace data is available, inspect the difference between the target sweep area Peak Trace Data and the Friendly Data to identify immediate signals/frequencies of concern.
2. Inspect the frequencies of concern by zooming in on these signals and comparing the signal levels in the different rooms.

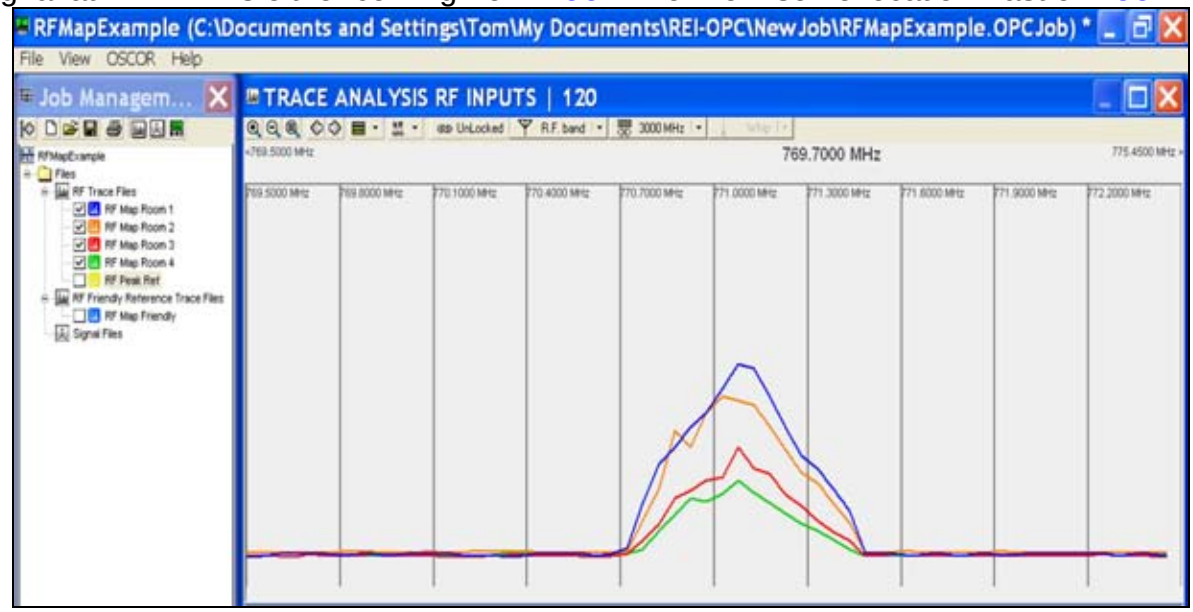
The figure below is a Difference Only graph generated from the **Room 3** data and the Friendly spectrum. **Room 3** was chosen as a starting point simply because it was the most centrally located test point. It is very easy to see 4 distinct signals of concern. Using the pointer on the OPC software, it is easy to quickly mark the signal frequencies as: 770, 827, 914, and 1013 MHz.



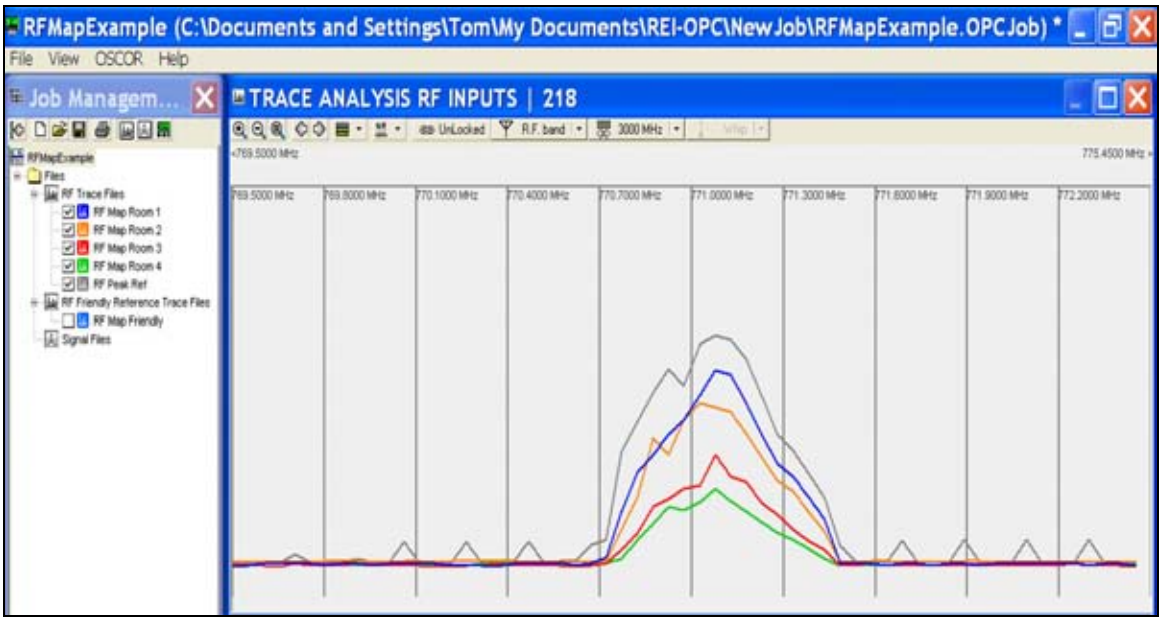
To further analyze these 4 signals, we would zoom in on these signals and examine the additional trace data for each signal. The following sections examine each of these four signals of concern.

Signal 771 MHz

Zooming in on the first signal, we can compare the levels between the other rooms, and see that **Room 1** has the strongest level followed by **Room 2**, **Room 3**, and **Room 4**. Therefore, referring back to the room diagram on page 6, it is easy to predict that the signal at 771MHz is either coming from **Room 1** or from some location East of **Room 1**.



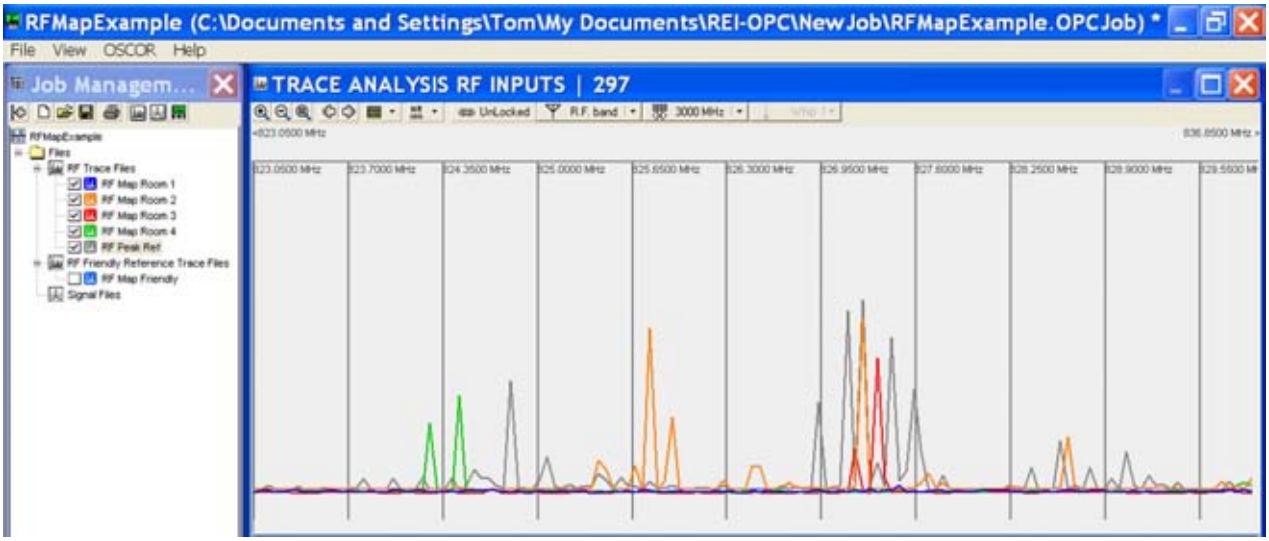
In this case, the signal is actually coming from the **Conference Room** East of **Room 1**. In order to determine the true location of the transmitter, it is necessary to use the OSCOR locator probe. Since the signal was not detected in **Room 1**, additional trace data was taken directly east of **Room 1** in the **Conference Room** resulting in the data shown below:



Since the Peak data was stronger in the **Conference Room**, the signal was then easily found using the RF locator probe. Next we will move on to investigate the remaining 3 potentially threatening signals.

Signal 827 MHz

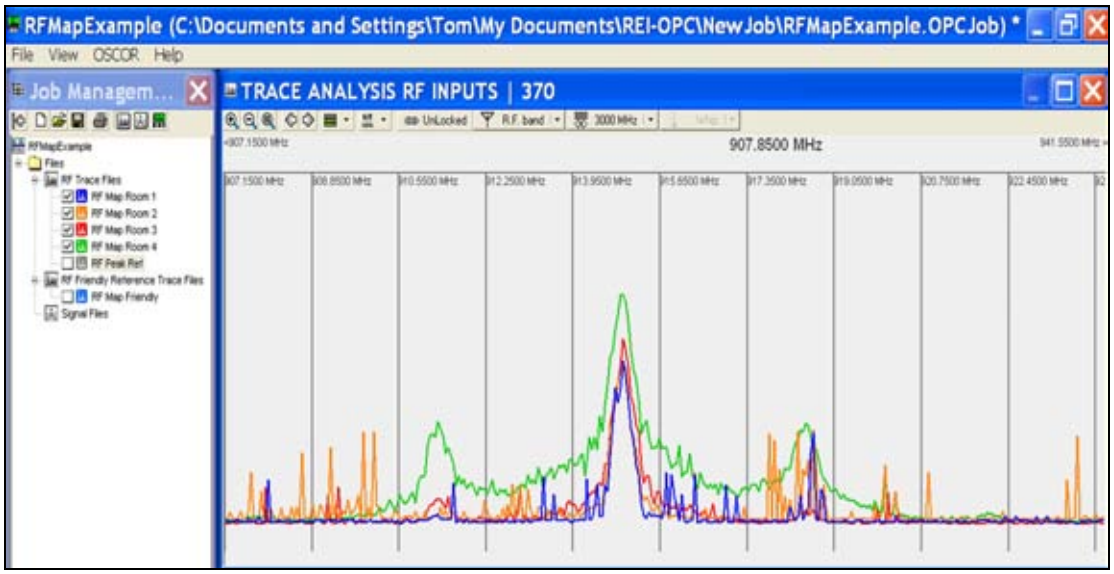
The next signal to investigate had a frequency of 827 MHz. This signal is in the 850 MHz band for US cell phones, and was inspected and discarded as a cell phone transmission. The screen shot below shows several of these signals. The reason that these signals only appear in certain rooms is that that transmissions only occurred while the OSCOR was located in those specific rooms at that specific time.



Next we will move on to investigate the remaining 2 potentially threatening signals.

Signal 914 MHz

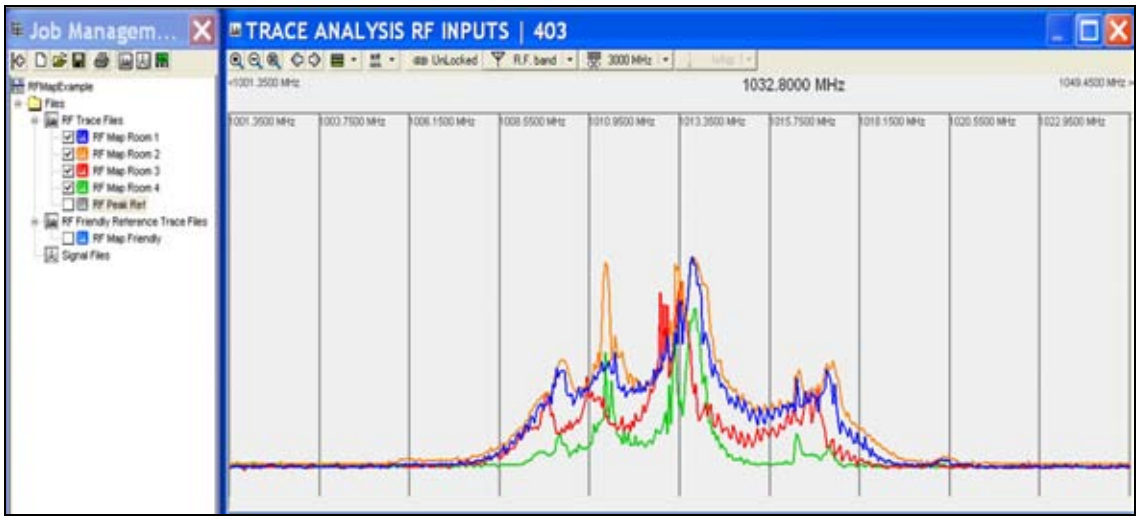
The signal at 914 MHz is clearly a video signal with sub-carrier audio. This can be identified by the characteristic shape of the signal having a wide bandwidth center and side lobes resulting from the audio sub-carrier. The shape of the signal may vary from room to room depending on the changing video and audio near the device during the capture of each scan, but it is very clear that this signal is much stronger in **Room 4**, followed by **Room 3**, compared to the other rooms. And, looking closely at the graph, **Room 1** has the lowest signal levels as expected.



Since the Peak data was stronger in the **Room 4**, the signal was then easily found by turning on the OSCOR video monitor, demodulating the signal and studying the video image to locate the camera. Additionally, the OSCOR RF locator probe could be used to locate the source of the RF transmitter. Next we will move on to investigate the remaining potentially threatening signal.

Signal 1013 MHz

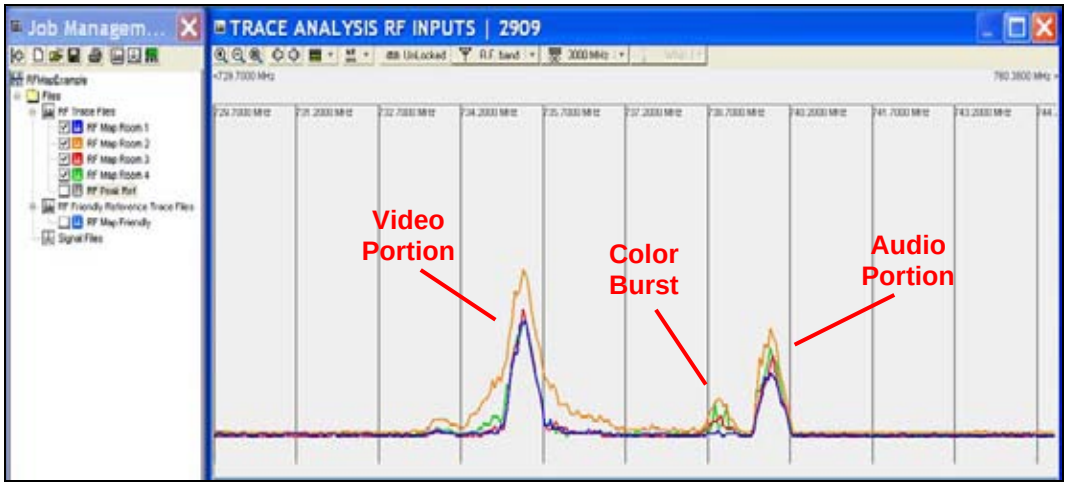
The signal at 1013 MHz also appears to be a video signal based on its shape (wide bandwidth center and side lobes resulting from the audio sub-carrier). The strongest trace level for this signal indicates that the transmitter is located in **Room 2**; it is important to note that **Room 1** has the second highest level for this room, even though **Room 3** is basically the same distance from the transmitter. This results from the location of the doors. **Room 1** and **Room 2** have doors that are in close proximity and the doors were open during the sweep so that there was little attenuation (signal loss) between **Room 1** & **Room 2**, and there would be greater attenuation (signal loss) through the wall between **Room 2** & **Room 3**.

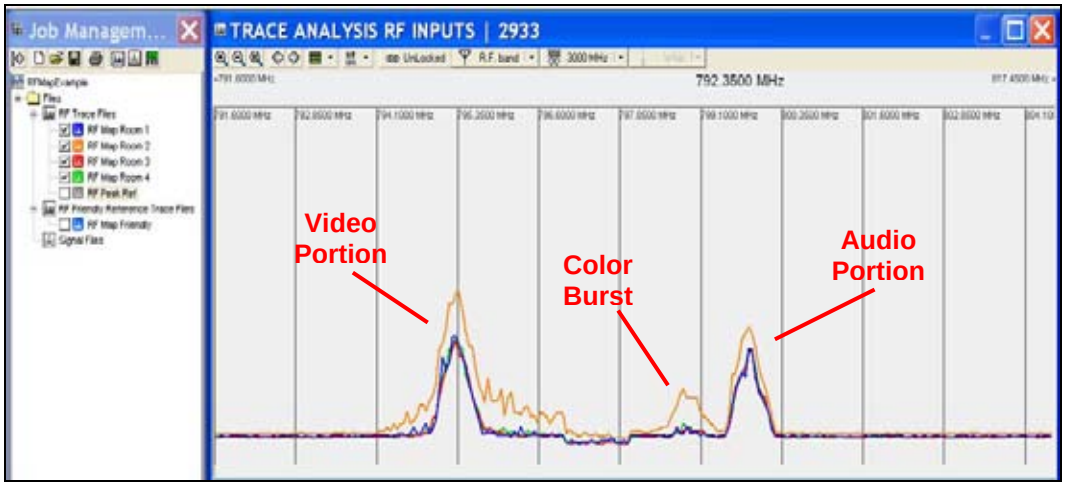


Since the Peak data was stronger in the **Room 2**, the signal was then easily found using the RF locator probe.

Additional Signals Discussed for learning purposes

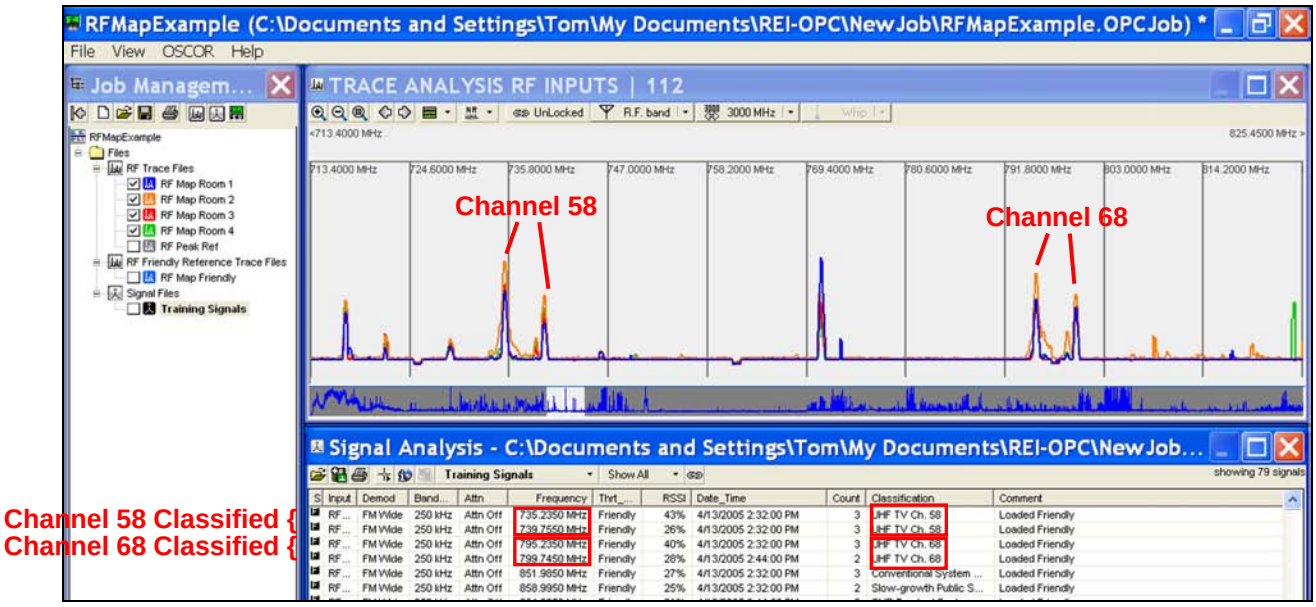
The previous discussion covers all of the signals that were identified as potential threats based on the difference mode. However, within this band there were additional signals that merit discussion. One example is the signals associated with television broadcasts as shown below.



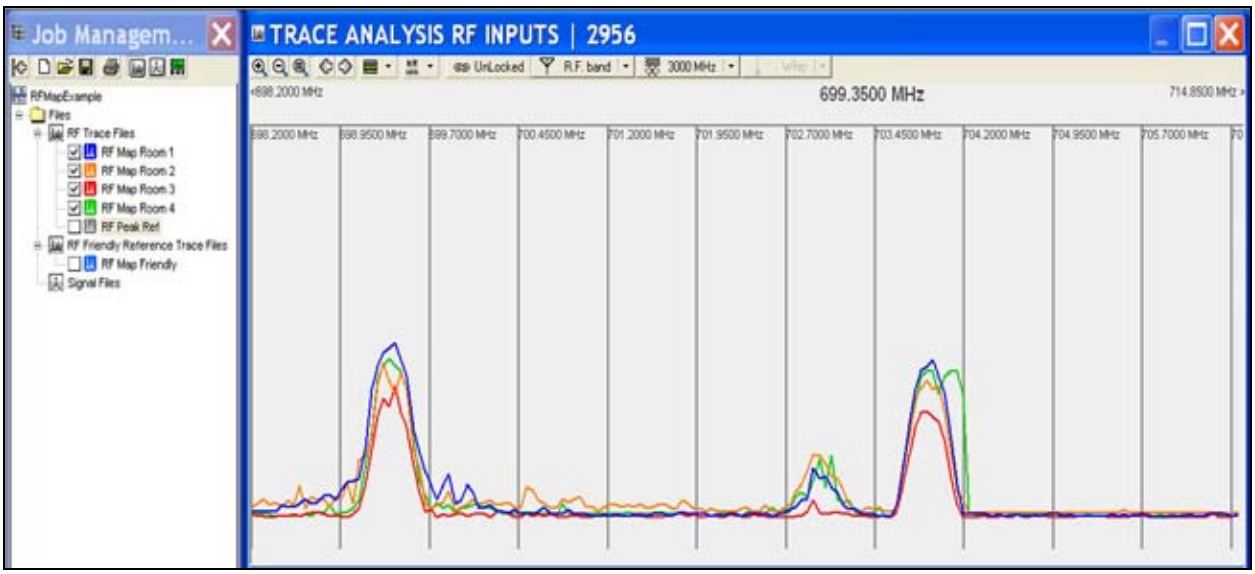


The two screen shots above each show two examples of different television signals, each signal is comprised of 3 portions (labeled in each screenshot): the video portion, the audio portion (standard NTSC television format has the audio signal 4.5 MHz above the video signal), and the color burst portion which contains color information for the video. This characteristic shape should be easily identified. But what is especially interesting about these two plots is that these two stations are coming from the same TV tower because the relative signal strengths for each room are the same for both signals. Based on the map of the facility and the strong signal strength in **Room 2**, it most probable that the direction of the TV transmission tower is North-West of the target sweep building. These TV channels are easily classified by using the Frequency database built into the OPC software.

These two television signals are from TV channels number 58 and 68 as shown below:



The next figure is a different TV station (channel 52) that has the strongest trace level in **Room 1** and the weakest in **Room 3**. This indicates that this TV station is definitely from a different tower and the tower is probably in the North-East direction.



Conclusion

As the distance to a transmitter is decreased, the received RF energy will increase, providing a tremendous advantage for locating eavesdropping transmitters with the proper methodology.

With the proper equipment and methodology, RF Mapping and the OSCOR/OPC System described in this document provides a procedure for quickly gathering important information regarding potentially threatening RF signals, including information about localizing the source and direction of both threatening and non-threatening transmissions.

Furthermore, this detection methodology is not dependant on demodulating the RF signal to determine whether it is a threatening signal, making Trace Analysis and RF Mapping equally useful for analog and sophisticated digital signals.

The OSCOR RF trace analysis methodology is a new approach that further advances the state-of-the-art in RF sweep analysis.

Appendix A

The general form of the equation that describes RF propagation path loss is:

$$P_r = \frac{P_{tx}\lambda^2}{(4\pi R)^2 La}$$

Where:

- **P_{tx}= Transmit Power**
- **P_r = Power at Receiver**
- **R = Range (distance)**
- **λ = Wavelength of Transmission**
- **La = Atmospheric Loss (Propagation Medium)**

The theory of Inverse Square law basically comes from the mathematical model of taking a single point source radiator that radiates in a perfect sphere and calculating the change in energy density of the surface area of the sphere as the radius of the sphere is increased.

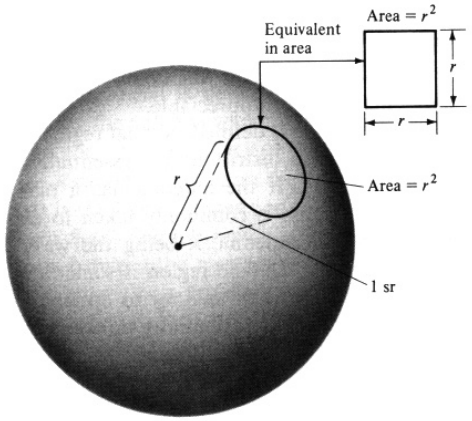


Figure: *Antenna Theory, Analysis and Design*, Constantine A. Balanis, 1982 Harper & Row.

As the distance from the transmitter is increased, the received power decreases with the square of the distance. For example, if the distance from the transmitter is doubled, the power decrease is quadrupled.

More importantly, in the most useful terms for TSCM, if you half the distance to a transmitter, the signal level increase is quadrupled.

In a large open area (for example an open field of several acres, or a ideal laboratory environment), this theory works fairly well. However, in the TSCM world, which deals with indoor office spaces, the Inverse Square Law is affected by other complicating factors, some of which include:

1. Propagation through building material causes energy loss. As a general rule, ranking building material from most attenuation to least is: Metal, Masonry, Wood, and Glass.
    a. Metal acts as an RF shield and will greatly reduce RF energy inside a building.

   b. Concrete, Brick, and Mortar will also cause RF attenuation but it depends on the thickness of the material, structural metal, and the grounding of the structure.
   c. Wood will also provide some attenuation but not as much as Brick and Mortar.
   d. Glass provides very little attenuation.
2. Metal structures such as filing cabinets, steel beams, door frames, drop ceiling grids, furniture, heating and cooling systems create reflections, diffractions, and scattering, which do not adhere to the basic Inverse Square Law principle. Therefore, when taking trace data in a room, the OSCOR should be placed in the center of the room, as far from metal structures as possible.