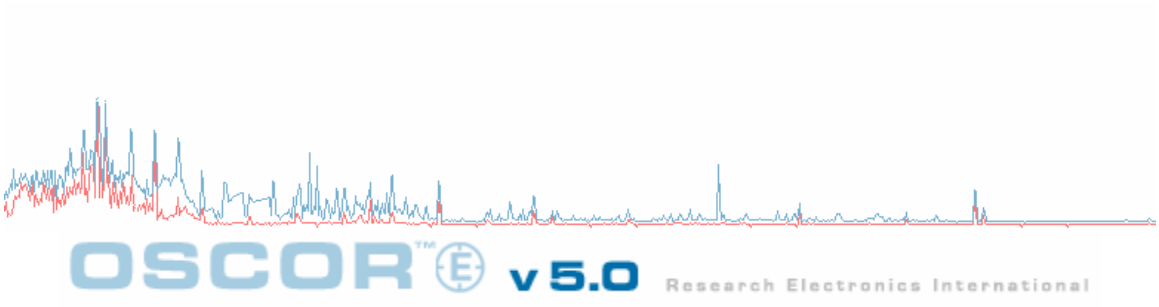


Build 5.02.xx documentation, Updated August 18, 2005

Contents subject to change

Table of Contents

Overview of OSCOR 5.0

The newly released version 5.0 of the OSCOR firmware has been designated as the OSCOR 5000 "E" (Enhanced) and brings significant updates including a high-speed USB port for PC connection, faster spectrum analyzer sweeping speed, a backlit display, and improved functionality.

The new OPC 5.0 software combined with the USB port provides the ability to store and compare multiple Peak Traces from previous sweeps, adjacent rooms, and real-time OSCOR data. This high-resolution data is easily manipulated for analysis.

OPC 5.0 Information > www.reiusa.net/opc5

See our website at www.reiusa.net

Introduction to Trace Analysis

The new OPC OSCOR 5.0 software was specifically designed for sophisticated RF trace analysis and RF mapping. The ambient frequency spectrum continues to be a dynamically changing environment. From small towns to big cities, new signals are appearing almost daily. These signals include intermittent analog signals such as police and taxi radios, digital pagers and mobile phones such as GSM, CDMA, PCS, etc. Wi-Fi wireless LANs, blue tooth, and new technologies such as Ultra-Wide Band (UWB) are on the way.

In order to address this changing RF spectrum, REI has developed a new methodology and new software. The new OPC OSCOR 5.0 Software and USB Interface provides real-time download of all frequency step data from the OSCOR TSCM Spectrum Analyzer. This means that as the OSCOR sweeps across the Whip Hi, Discone, and MDC antennas (5MHz to 21GHz) the spectrum comprising of 120,000 data points is transferred to the PC for high-resolution display and storage.

This provides the capability to store spectrum trace analysis data from multiple locations or from different times in order to perform detailed high-resolution trace analysis comparisons. In other words, you can capture RF spectrum trace data from a friendly location such as the parking lot or outside of the target sweep area, and from multiple locations from within the target building. Then, these trace spectrums can be compared to determine if transmissions are emanating from certain locations within a building, and thus provide an accurate RF map of a facility. Furthermore, the OPC software provides the ability to capture trace data in the same location at different times. For example, you can compare the Peak Trace data that was captured last month with a current Peak capture to see if any new signals have been brought into the environment.

Trace analysis is done primarily using Peak Trace data, which ensures that if energy has been encountered from an intermittent transmitter such as a Frequency Hopper or a Burst (packet) transmitter, then the evidence and signal level of these transmissions is easily captured and compared using a difference spectrum.

The new trace analysis functionality built into the OSCOR and OPC 5.0 Software provides a new level of comparability to rapidly identify very sophisticated transmissions, and provides an accurate indication of whether a transmission is emanating from within an area of concern.

Installation

Installing your OPC is a simple, two-step process: installing the application and USB drivers.

Installation from supplied CDROM or DOWNLOAD

1. If the CDROM does not start automatically, run the file **OPCSETUP.exe.**
   If installing from a download, run **OPCSETUP_06.exe** (the filename may not match exactly)
   a. Answer all installation questions, choosing the default or typical when available. Click IGNORE if Setup indicates a file not found or is in use.
   b. Read any instructions offered during the installation. You may be required to update your USB drivers.
2. Upon completion, connect your OSCOR and install the USB drivers
   a. Unless otherwise noted, you are not required to install the USB drivers when reinstalling

Recommended PC System

Pentium II Processor or higher

Processor speed of at least 500 MHz

64 MB of RAM

Sound Card with stereo "line in" input for audio

Windows 98, 2000, or XP (NT is not supported)

Installation of USB drivers for OSCOR

These instructions are for Windows XP.
Installation under Windows 98/ME/2000 is similar, but not necessarily identical.

OSCOR USB drivers are made up of two (2) parts.

The procedure below may have to be duplicated for each device found. (REI USB Device & REI UART to USB Controller)

1. Connect the OSCOR USB cable to an available port on your PC
   OSCOR does not need to be turned on for USB installation
2. The New Hardware Found Wizard should appear
3. Select "**Install from a list or specific location (Advanced)**"
   then click the [**Next >**] button.
4. Select "**Search for the best driver in these locations**"
   Check "**Include this location in the search**:"
   Use the [**Browse**] button to find the USB folder
   (Usually **C:\Program Files\REI\OSCOR\USB**,
   unless you chose a different folder when you installed the software)
   Click [**OK]**
5. Click the [**Next >**] button.
6. The wizard should have found the software….
   This dialog warns you that the driver has not been signed by Microsoft;
   You're going to have to click the [**Continue Anyway**] button.
7. Click the [**Finish]** button to complete the installation.

At this point, you may run the Application: **Program > OSCOR 5.0 > OSC5000E**

Your OSCOR should appear in the bottom of the application as shown in the 5.0 Layout.

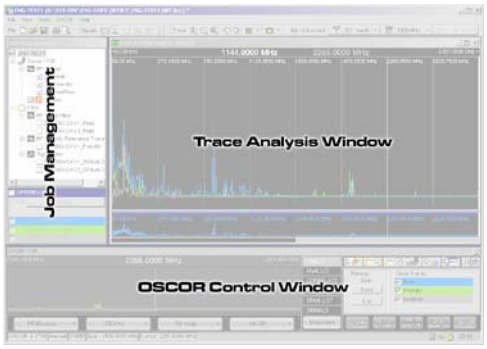
Application Layout

To the right is a screenshot of OPC 5.0. This is what you may expect to see when you first run the application.

Note: Your screen will look different if your OSCOR is not connected to your PC.
If this is the case, you may connect your OSCOR to an available USB port, and the select Scan for OSCORs from the main Menu. If you have not yet installed the USB drivers, please close the OPC5000E application and install them first.

The application is arranged in four (4) major zones (or windows).
The 4th window, Signal List may be open closed as needed.

When OSCOR is absent the OSCOR control window will be removed.

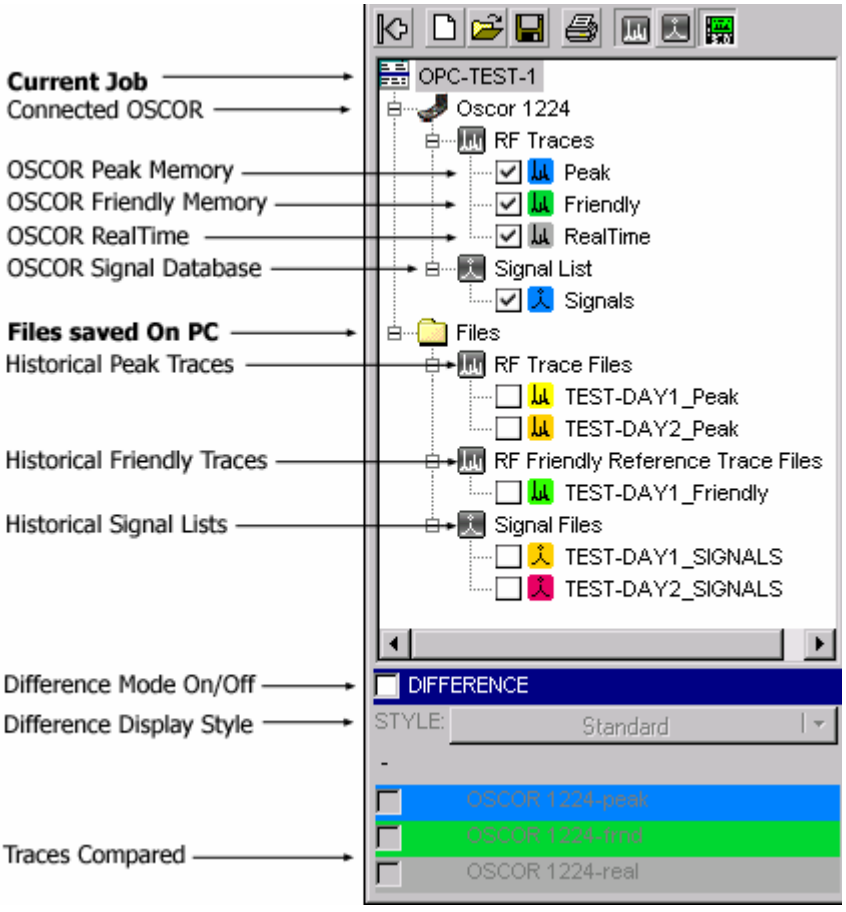


Job Management

OPC 5.0 is organized by Jobs. The Job is defined by *.OPCJob file which stores information about Traces, Signals & Spans as well as printer settings and colors chosen for items within the Job.

A job may contain Data from File, Live OSCOR Data or both, as well as data from multiple OSCORs simultaneously.

The Job file stores the relevant information about Trace sources, and all the settings of the Trace Analysis Window and application state.



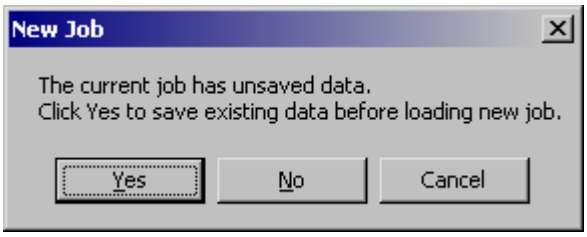
Starting OPC

When the OPC software is activated, you will be presented a screen where you have the options to start a new job, open an existing job or open the last job saved.

Click on the New Job Button on the splash screen.

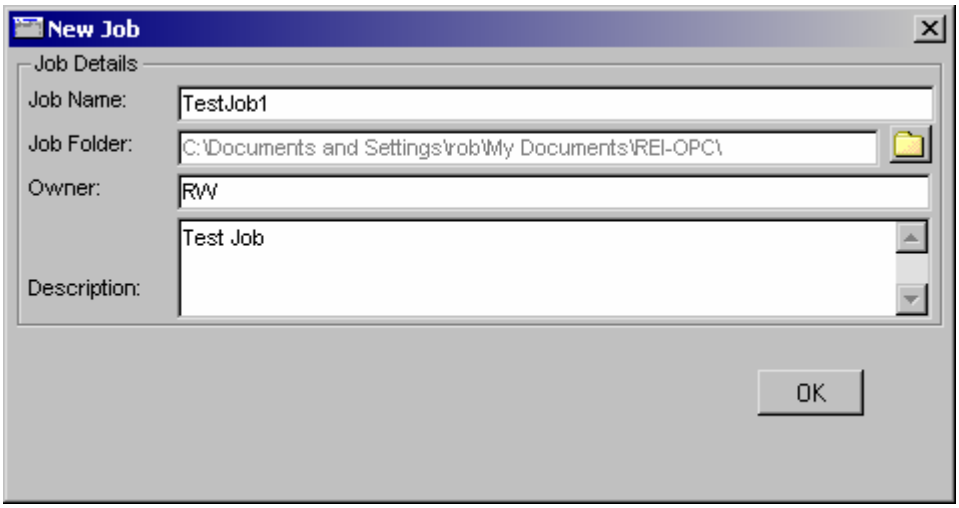
Creating a New Job

When creating a new job from within the application a
dialogue box will prompt you to save the current job and unsaved data.



Choosing No to discard all changes to current Job, and choosing Cancel will return you to the Current Job.

Choosing Yes will invoke the save job dialog.
Upon saving the current job you will then be prompted to enter information for the new job.



Enter your **Job Name.**

This will be saved in the folder specified. E.g. *TestJob1.OPCjob*
Select a **Folder.**

You may optionally record your name and a description of your job.

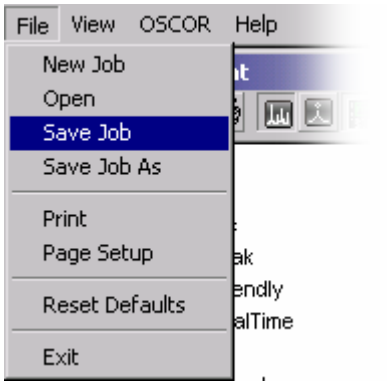
This information can be edited later when saving the job, or editing job properties.

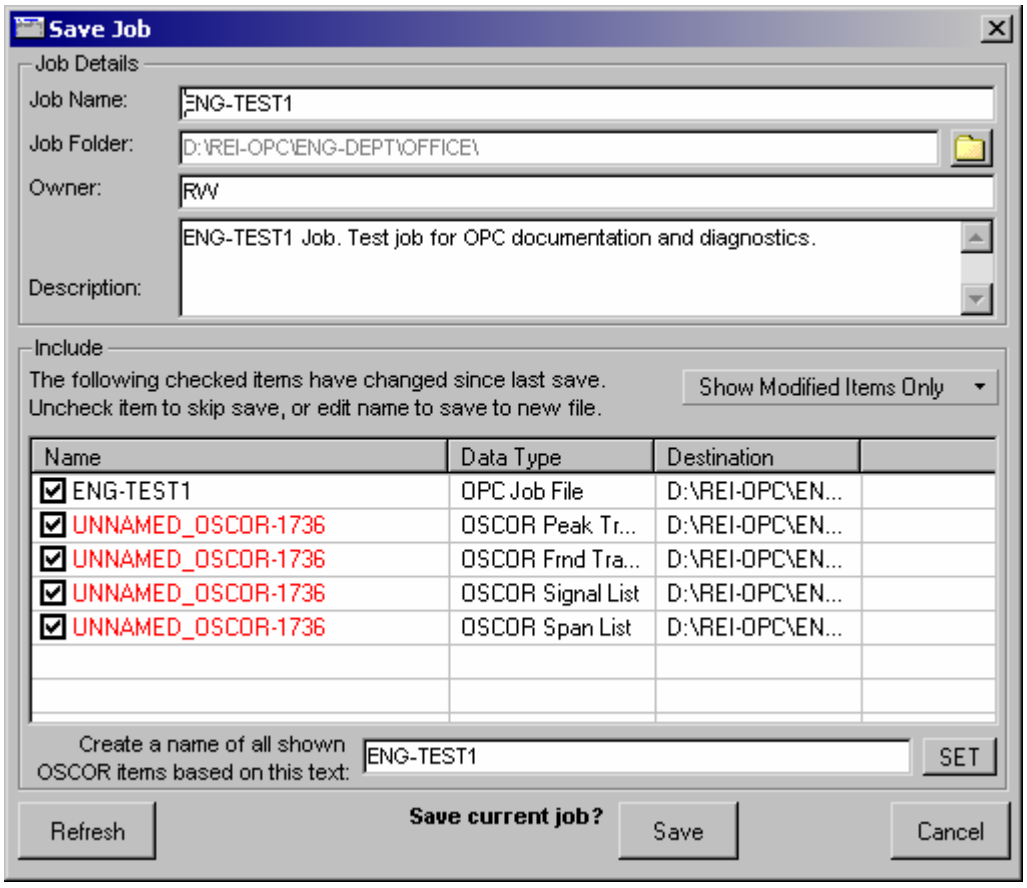
Click **OK** to continue

Saving a Job / Saving Data

To save a job:

Choose **File > Save** from the main menu**,** or Click the **Save Button** on the toolbar. 





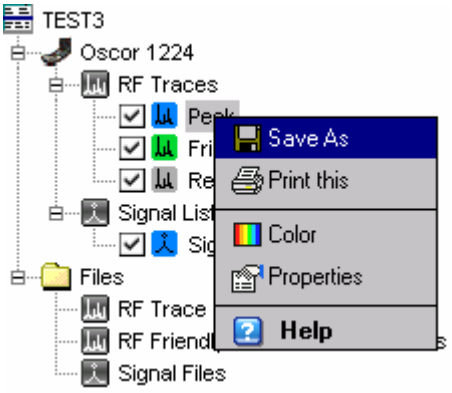
In the dialog above you have the option to automatically save associated data from the OSCOR to your PC. This process will add selected data to the job under the **File** node. You may set a prefix to all files to ensure unique identification of the data for later historical purposes.

If you do not wish to save updated OSCOR data to the job, simply uncheck the items to exclude. Files save automatically are placed in the job folder with the names set above.

Saving Trace and Signal Data From OSCOR

To manually Save **Traces** and **Signal Databases** from OSCOR to your PC,

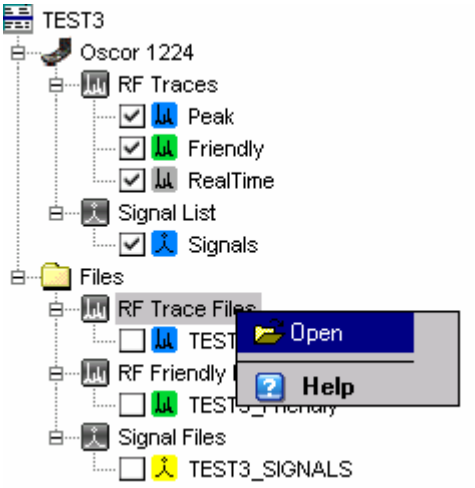
Right-click on the item under the OSCOR node in the Job Management window and click **Save**.



Importing Historical Data

In the Job Management window, historical data (any data saved on the PC), can be added for analysis & printing.

Right-Click on **RF Traces, RF Friendly Reference Trace Files** or **Signal Files** and click **Open.**

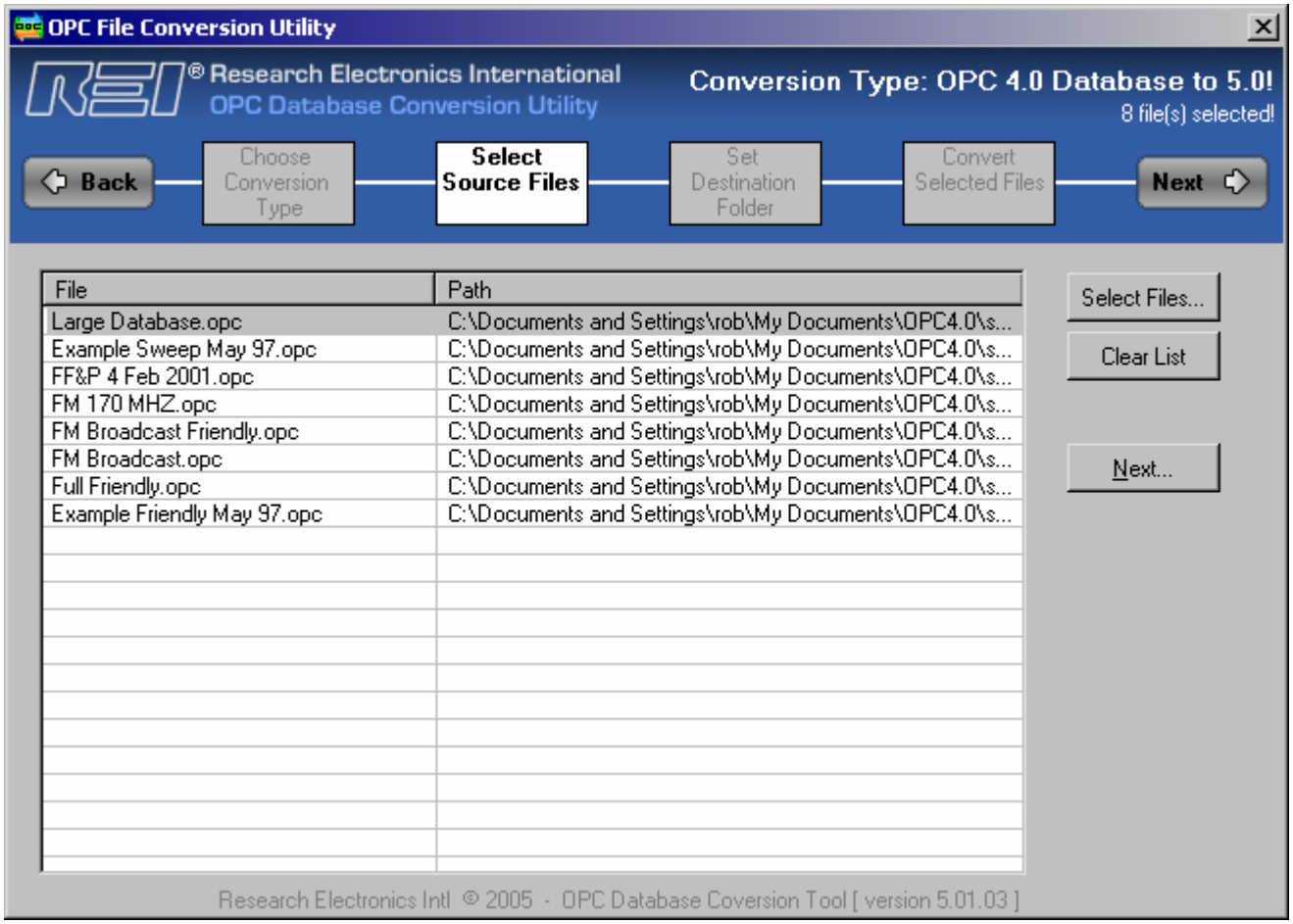


This will launch the File Open dialog where you can browse for the type and location of the file.
When opening and external File, OPC will use the color last set for that file. If no color information is found, a color will be sequentially assigned from the internal palette.

Converting 4.0 Database to 5.0

OPC includes a Batch file conversion tool capable of batch converting multiple OPC 4.0 Signal Lists to version 5.0.
To access the application, go to your start menu under **Program Files/OSCOR 5.0/Tools.**

» Click on **OPC 5.0 Batch Converter**.



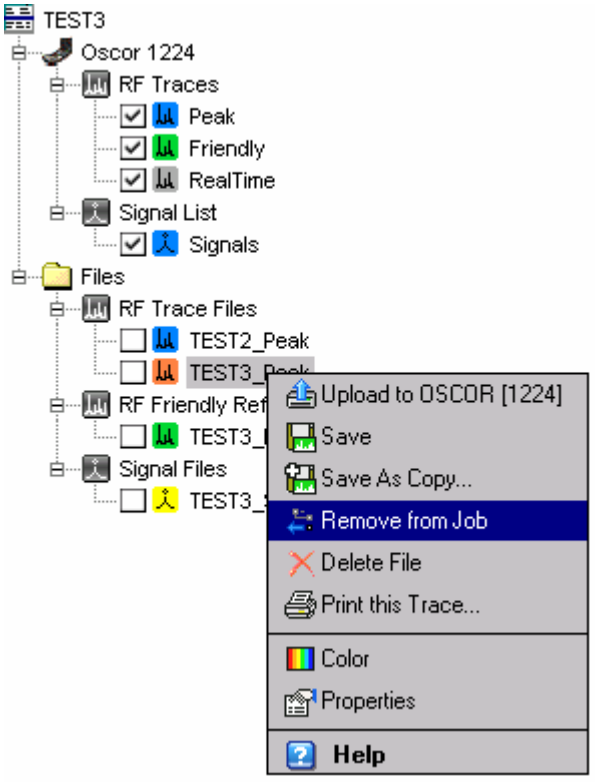
» Select Files to convert then click next.

» Choose a destination directory.

» Click Convert.

Removing Historical Data From a Job

Historical data that has been added to the Files section can be removed or deleted by right clicking on the file.



» Click **Remove**;

This does not permanently delete a file from your computer, it only removes from the current job.

To delete a file permanently:

» Click **Delete** from the context menu.

Trace Analysis

The TRACE ANALYSIS window is where the high-resolution sweep data obtained from OSCOR is displayed and compared.

Multiple Traces can be visible here at one time not including the difference Trace. These sources will be chosen from live connected OSCOR's and Historical Traces that are added from File.

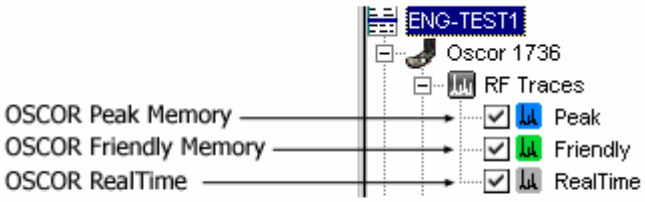
The Trace Analysis Window allows you to navigate any combination of sweep data and show differences between selected Traces as well as displaying overlaid markers indicating frequencies identified in the active Signal Database.

You may also split the Trace into multiple bands to aid in view large spans on one screen. Any arrangement of Trace data and difference Traces can be printed in very high resolution.

Working with Traces

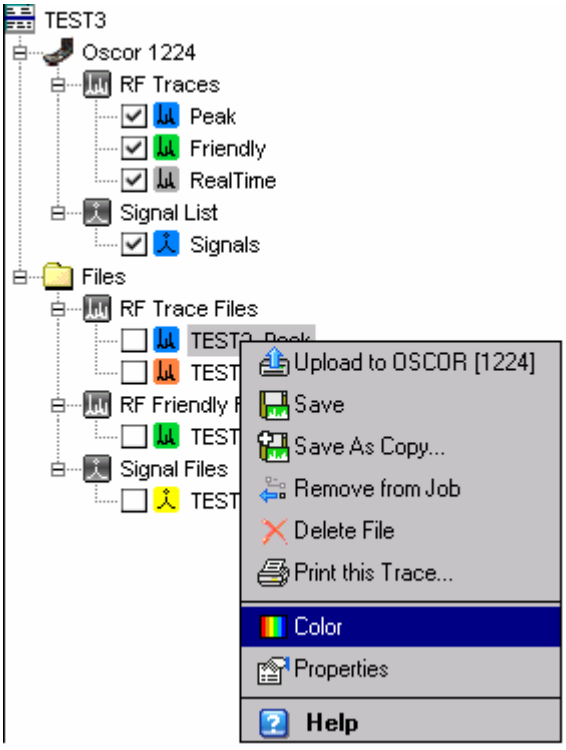
Viewing Traces

When the check box next to a signal is selected it becomes visible and is then added to the list of valid difference sources.



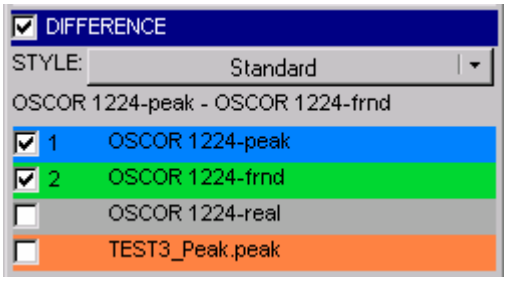
Changing Trace Colors

Right-Click the item in the Job Management Window and choose **Change Color.**



Comparing Data With Difference Mode

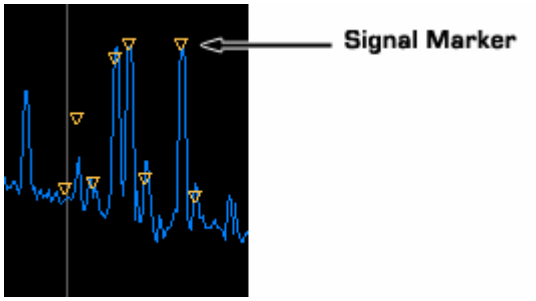
- As Trace files are loaded into OPC, the also appear below the Difference mode selector.
  A Trace must be selected in order to be available for comparison.
- If **Difference mode** is selected, the OPC software will display the difference between two of the available trace files. This can be displayed in one of four different methods: Standard, Centerline, Top Down, or Difference Only.
- The display of the difference mode will depend on the order of comparison. The OSCOR only allows a certain method of comparison, Peak minus Realtime, for example. The OPC software will allow you to compare data in any order that you prefer. You can choose the order the files will be compared in by clicking on the file and changing its' order from **1st** to **2nd**. By doing this, it is possible to invert the magnitude of difference and in some cases the difference trace may not be properly displayed. If it appears that the difference trace is out of view you should change the polarity of the selected traces.



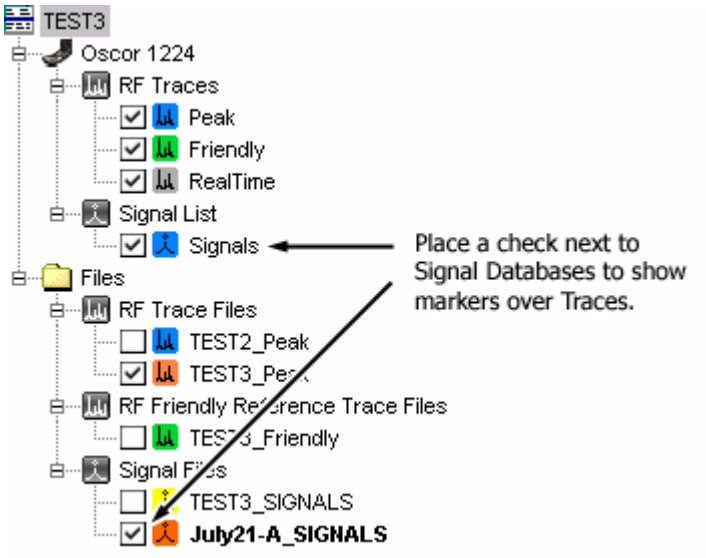
- The **Standard** method is comparable to what is built into the OSCOR. The two trace files are superimposed on the screen, with the difference between the two offset slightly to the bottom.
- The **Centerline** method will move the difference display up to the center of the trace display.
- The **Top Down** method will move the difference display up to the top of the display, which is useful when the difference is inverted and not properly displayed as mentioned above.
- The **Difference Only** method will display only the difference and not the original two trace files.

Displaying Signal Markers

- The OPC software will now display a symbol wherever a signal has been stored.
- This symbol is at the peak of the stored RSSI value.

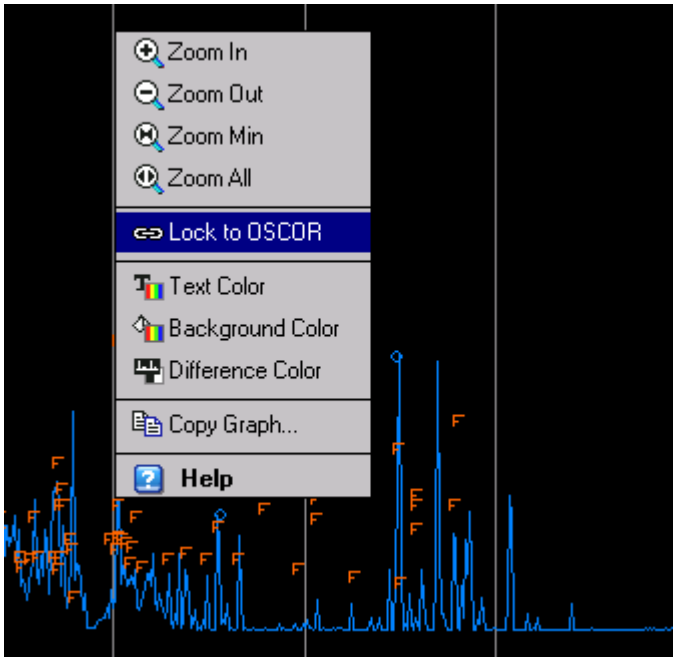


- **Right clicking** on a signal node in the tree and selecting change color can change the color of the signal marker.



Synchronizing Trace Window to an OSCOR

- The trace data window is a static display of traces collected by the OSCOR unless the OPC software and the OSCOR are synchronized.
- By 'right clicking' on the trace display widow and selecting "Lock to OSCOR", you are synchronizing the trace display window and the OSCOR. The Trace display window will now continuously update in near real-time.



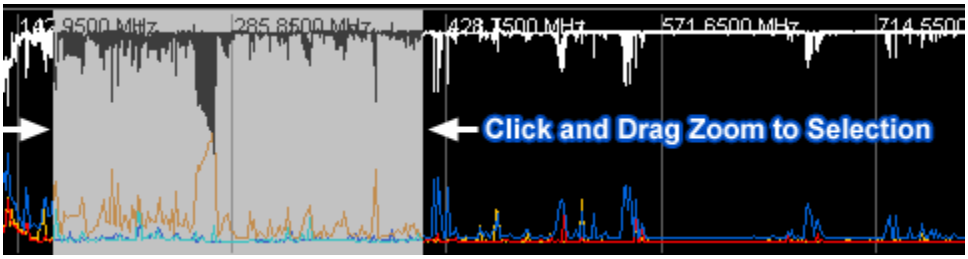
- This can also be selected on the main menu by toggling the button at the top of the trace data window.

Changing Frequency Range of a Graph

The frequency range displayed in the trace data window can be changed by one of four methods.

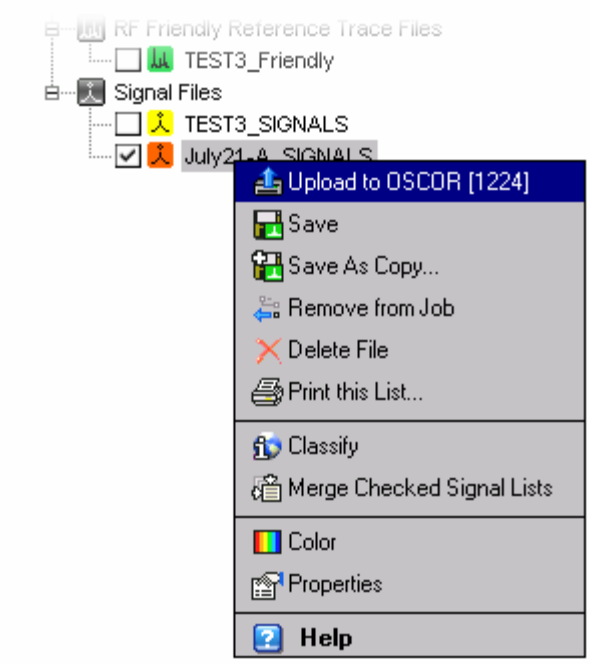
- In the upper menu, under Zoom, you can select to zoom in or out.
- The magnifying glass buttons will also allow control of zoom.

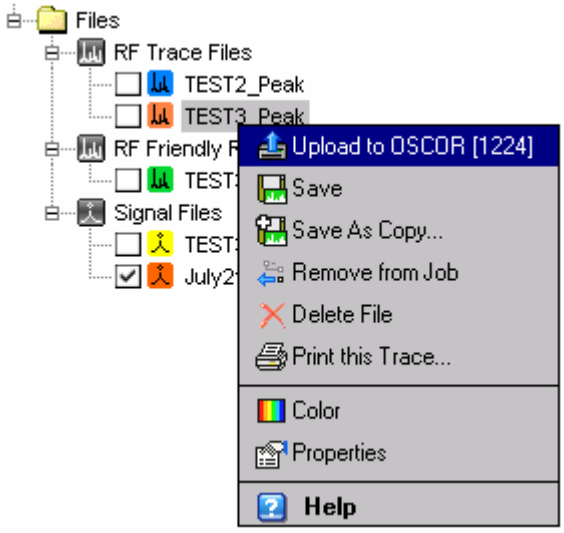
- You can also 'right-click' and select whether to zoom in or out.
- You may also click & drag your mouse to control the zoom.
    - Position the cursor over one end of the frequency span you wish to view, hold down the left mouse button and drag the cursor to the other end of your span, and release. You will now zoom in to the selected frequency range.



Uploading Data to OSCOR Memory

Data may be sent to the OSCOR from the OPC by either selecting OSCOR from the top text toolbar and choosing between Send signals, spans or all.





» You can also use the Load Items From Disk function in the OSCOR Data Command Toolbar.

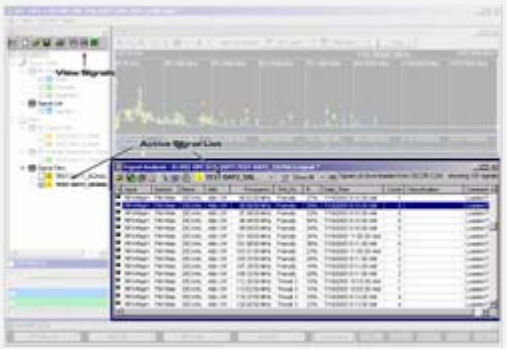
» If you have opened a signal list from a PC file, you can also ‘right click’ on the file and select "Upload" and it will send signals to the OSCOR.

Signal Lists

The Signal List Window allows viewing and recall of Frequencies through the connected OSCOR as well editing Signal Data.

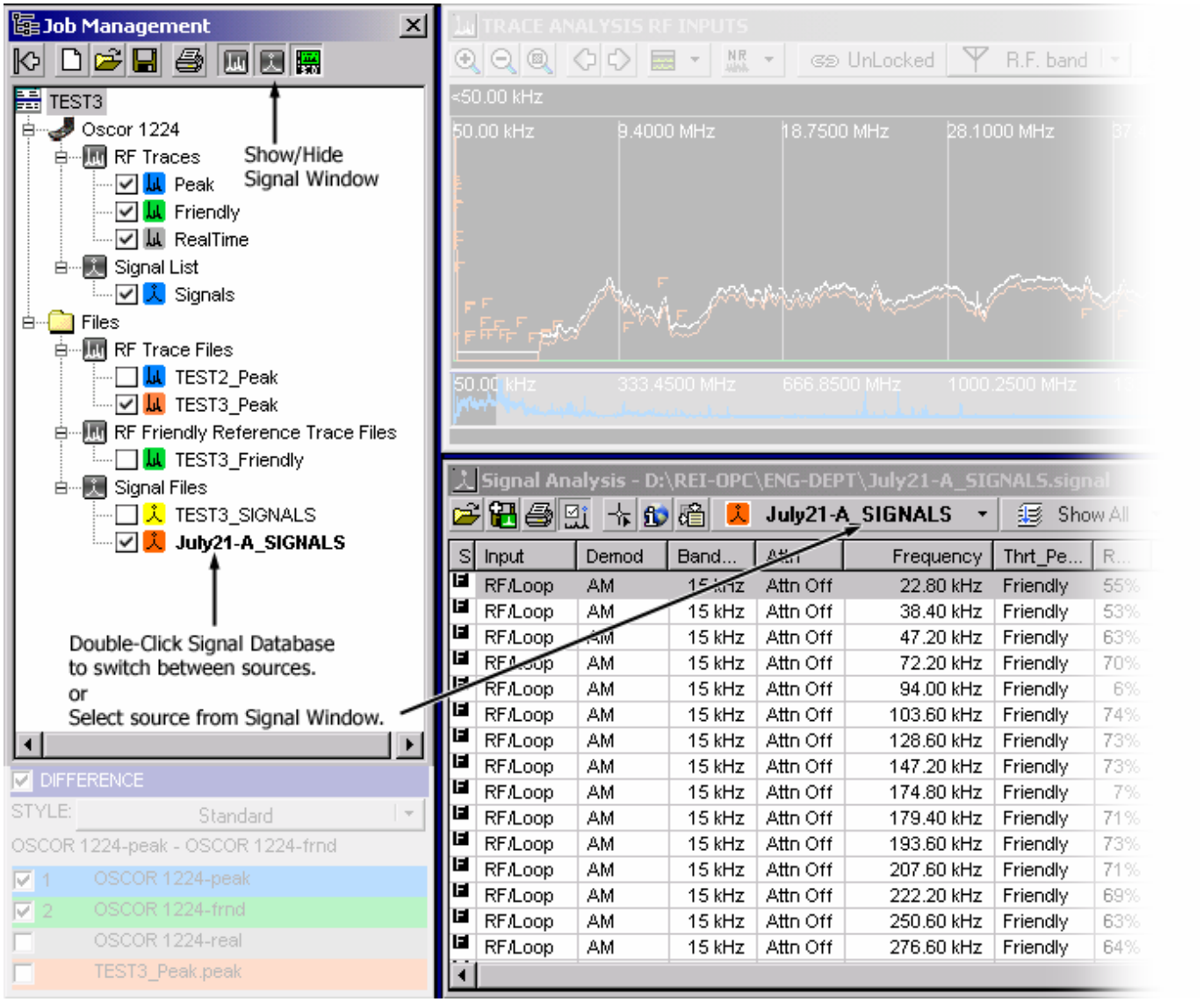
Like OPC 4.0 you may edit the Threat Level, add Comments and Classify frequencies using the ITU & FCC frequency band plans.

In addition OPC 5.0 allows you to merge signals from multiple databases and save it as a new database. It can then be uploaded back to OSCOR, or referenced by other Jobs.



Viewing Signals

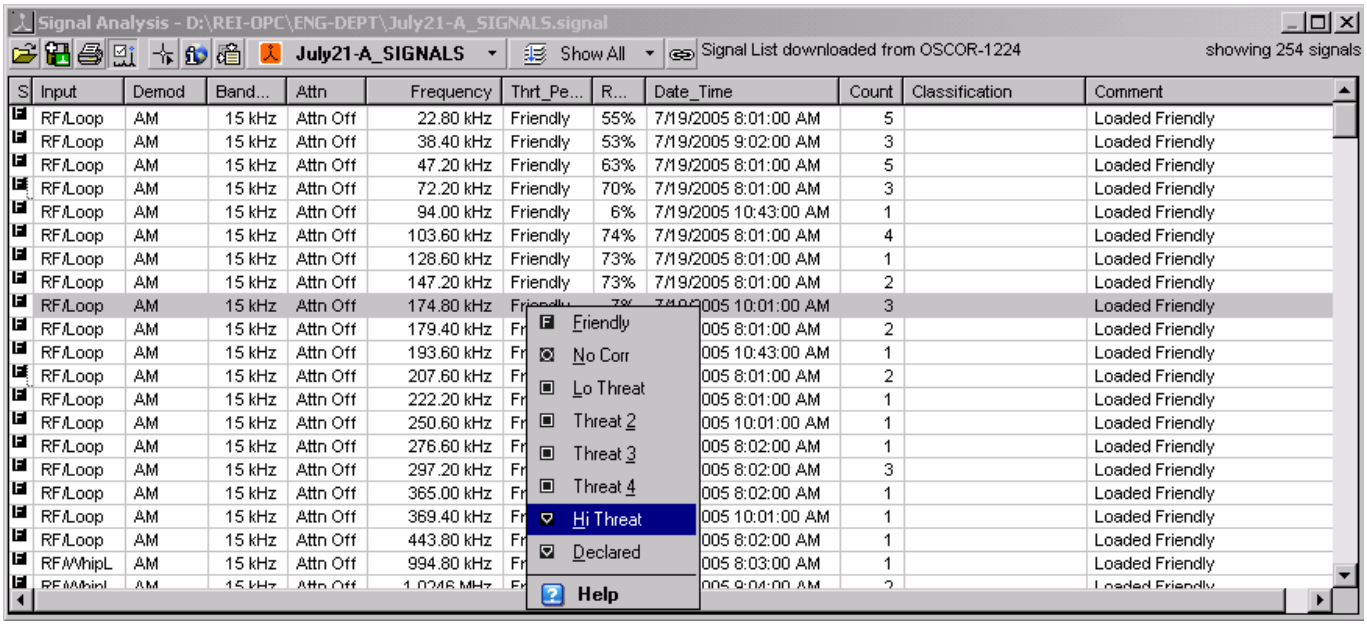
- The Signal Database Window can be shown or hidden by clicking the Signal Button in the Job Management Toolbar. Double-Clicking on a Signal Database Node in the Tree will have the same effect.
- Once the Window is open, you can switch between different databases by clicking on the Signal Node in the Tree, or by selecting the source in from within the Signal Window.



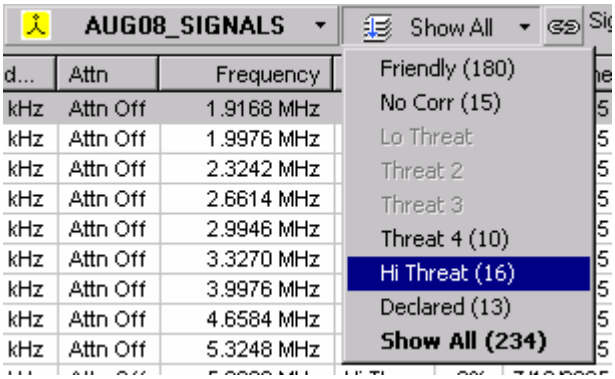
Editing Signals

- Signals may be sorted by any of the categories of collected data.
- The Threat status may be edited and you may enter custom comments for any of the signals listed.
- To edit the Threat status or Comments, Right Click or Double Click the row you wish to modify.
- If you wish to edit multiple rows simultaneously, you must right click to access the edit menu.

If you are editing OSCOR's signal list, the changes are sent in real time to OSCOR.



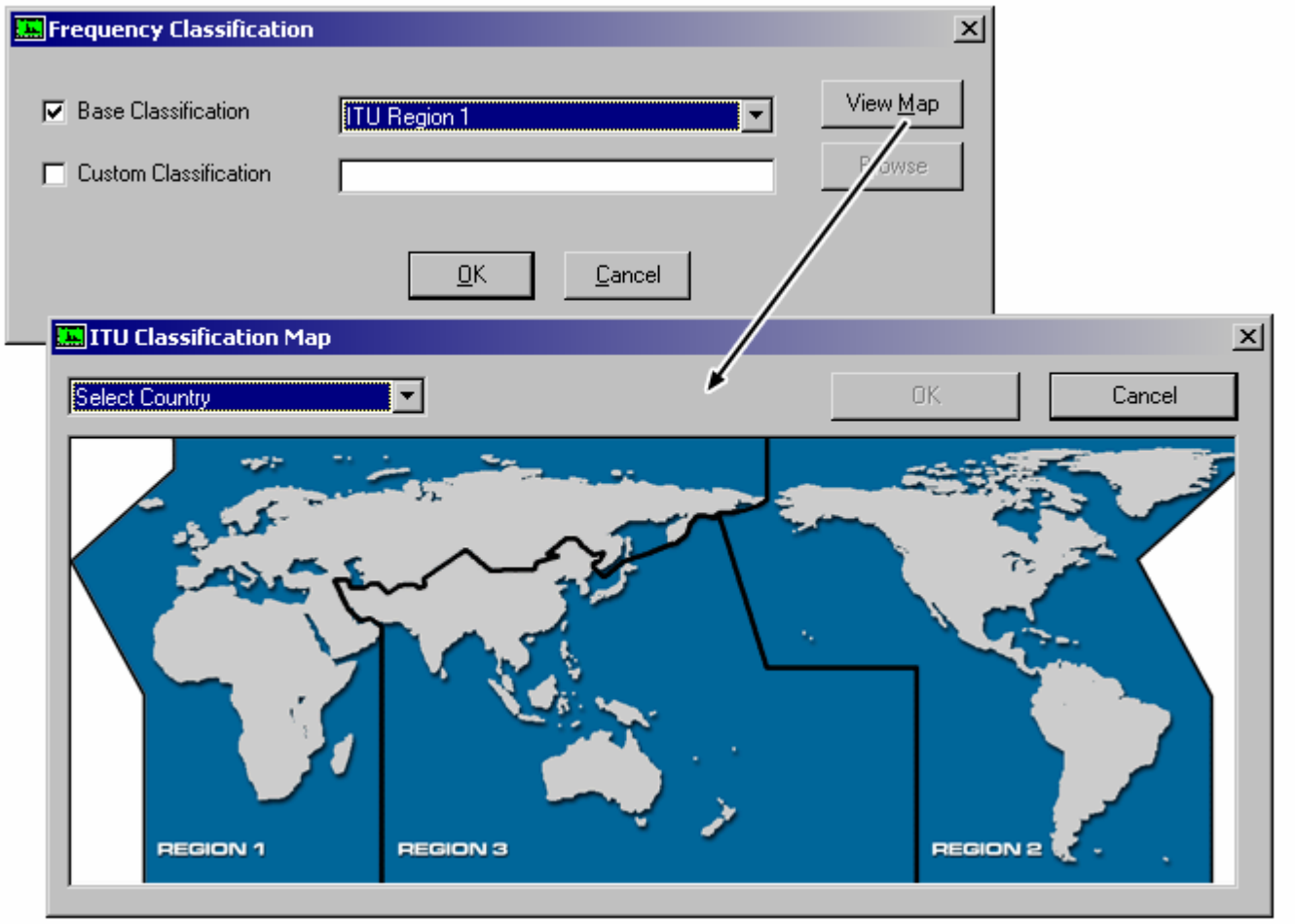
You may filter the list to show only specific categories using the filter button in the toolbar.



Frequency Classification

- You can apply the Frequency Classification by right clicking on the Signal List or on the Signal list in the Job Tree.
- OPC 5.0 also supports the use of custom classification files, which you can select in the Classify dialog.

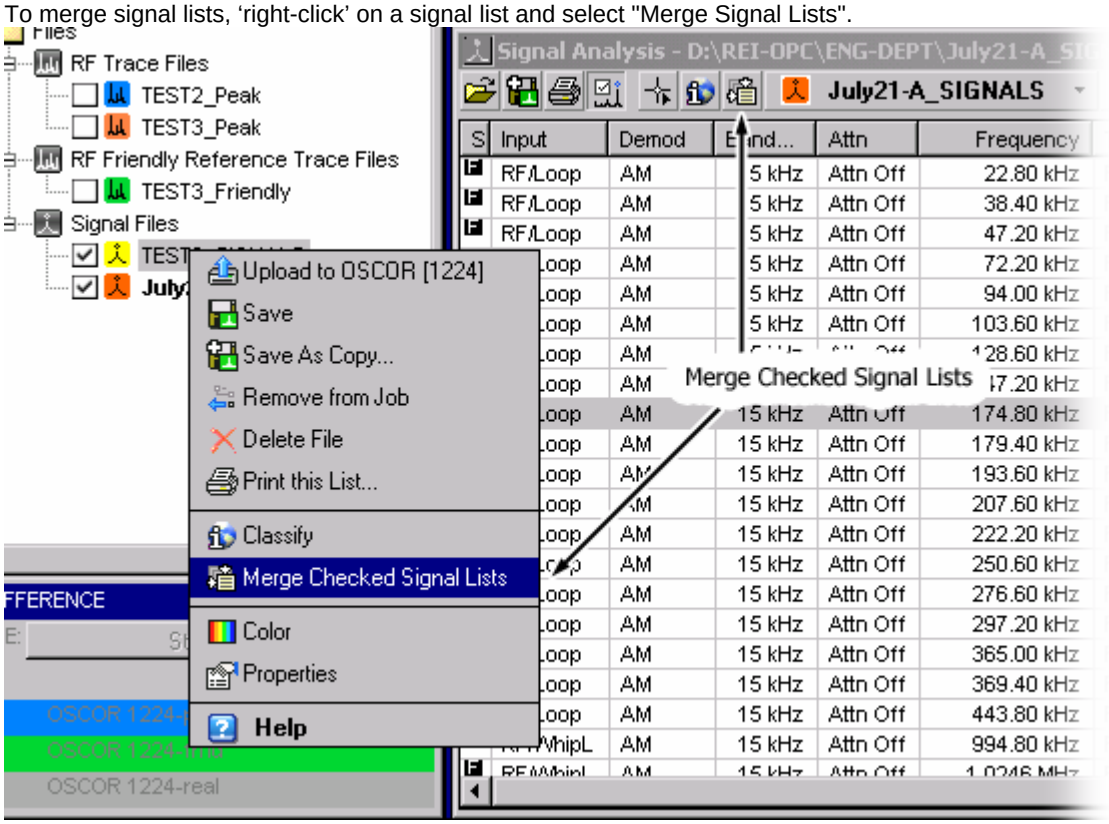
Right-Click on the signal File in the **Job Navigation Window** or the **Signal Window**, choose Classify.



Merging Signals

Multiple signal lists can be combined into one list by using the merge function.

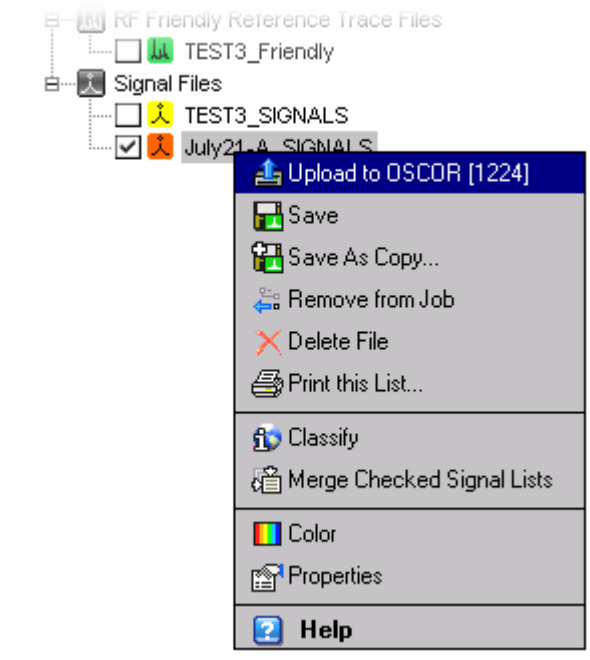
- To merge signal lists, ‘right-click’ on a signal list and select "Merge Signal Lists".



- If the same signal exists in each database, the signal with the strongest RSSI value will be kept.
- Signals that are Checked In the Job Tree are included in the merge function.

Uploading Signals

Right-Click on the Signal File that you wish to upload to OSCOR and click **Upload**.

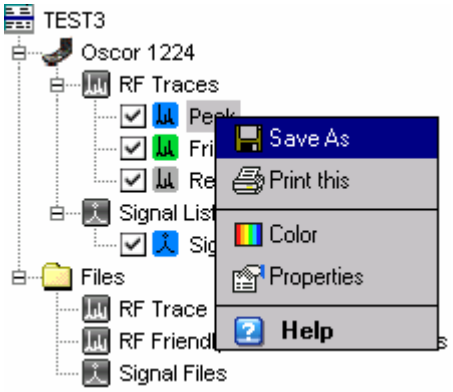


Saving Signals

Signals may be saved in one of three methods: When a Job is saved, the signal list is also saved, under the Job Management section, if you 'right click' on a signal list, you may save, and in the OSCOR Data Command Toolbar using the "Save Items to Disk" icon. Signals are saved as a *.signal file.

To manually Save **Signal Databases** from OSCOR to your PC,

Right-click on the signal file node in the Job Management window and click **Save**.



OSCOR Control

The OSCOR Control window provides nearly all the functionality available within the OSCOR itself. The layout contains familiar buttons and commands to communicate with the OSCOR.

The main part of the display (to the left) mimics most of the OSCOR screens. The Traces are color coded to match colors set in the job.

The right panel contains options available within each method (sweep, analyze, etc)

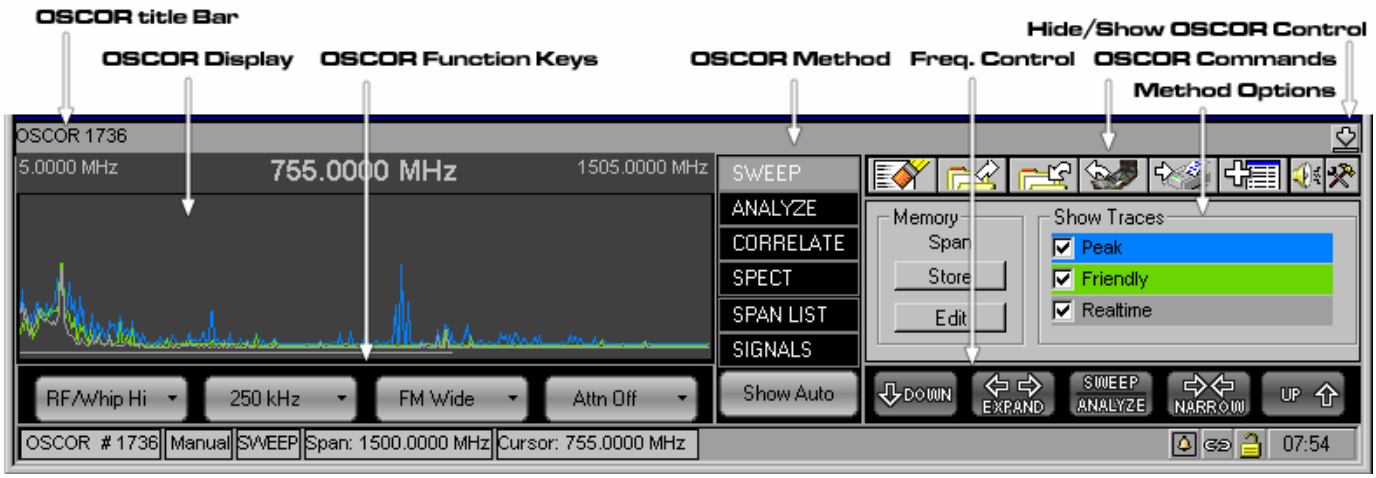
Connecting to an OSCOR

If the OSCOR has been connected to the PC prior to activating the software, the software will automatically detect the OSCOR when it starts up. When the software has been started before the OSCOR has been connected, you will need to tell the OPC software to look for the OSCOR.

Click **OSCOR > Scan USB Ports For OSCOR's.**

Controlling OSCOR

Most of the OSCOR's functions can be controlled with the OPC software. The main functions are: SWEEP, ANALYZE, CORRELATE, SPECT (spectral analysis), SPAN LIST, SIGNALS, and the AUTO / MANUAL selector.



When the OSCOR is initially connected to the OPC software, it will automatically synchronize its' data with the PC. All signals, traces and spans will be transferred to the PC. Using the OSCOR Command Toolbar and Pressing the "Retrieve Items From OSCOR" button can also retrieve data by selecting the type of data you would like to receive.

Data may be sent to the OSCOR from the OPC by either selecting OSCOR from the top text toolbar and choosing between Send signals, spans or all.

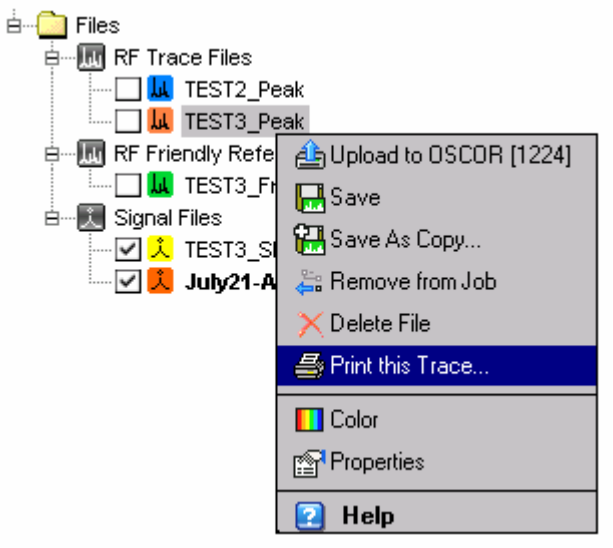
You can also use the Load Items From Disk function in the OSCOR Data Command Toolbar. If you have opened a signal list from a PC file, you can 'right click' on the file and select "Upload" and it will send signals to the OSCOR.

To erase individual signals from the OSCOR using the OPC software, you can select a signal or group of signals and press the delete key on your keyboard.

You may use the "Erase Items in OSCOR" button from the OSCOR Data Command Toolbar to delete an entire Signals Database.

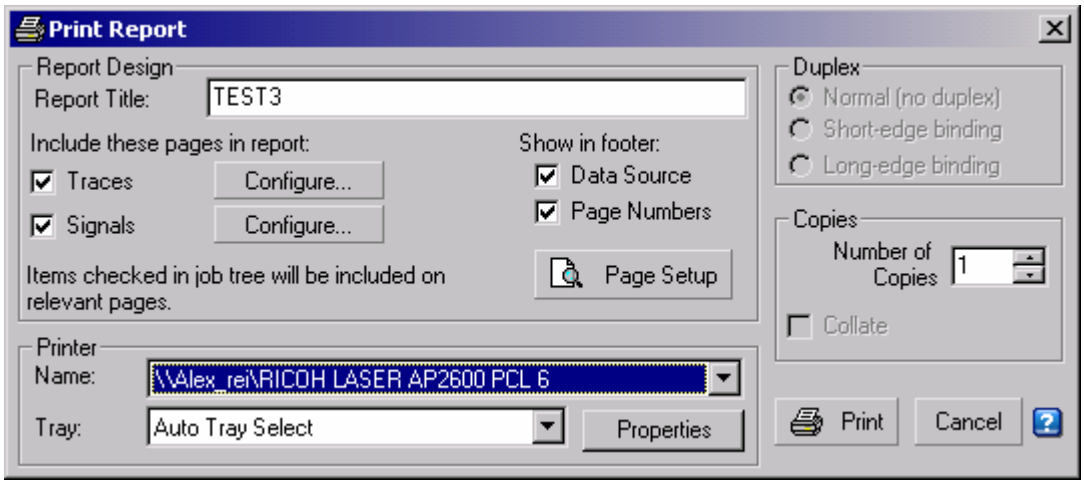
Printing Traces

Once you have setup your print options, you can 'right-click' on the traces listed in the Job Management section and select "print". This will print a graphic image of the Trace Display Window showing the trace file you have selected.



Page Setup

All print options are controlled in the Page Setup option in the OSCOR Data Command Toolbar under the "Print Item" icon or under the "File" text menu at the top of the page.



- From the Page Setup, you can select whether to print Signals (and which information you want to include in the print) and/or Traces and whether or not you want to include signal points over the Traces, as well as other standard print options.
- When "Print" is selected it will print the "Job" which is all data that you have selected in the "Page Setup" menu.

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

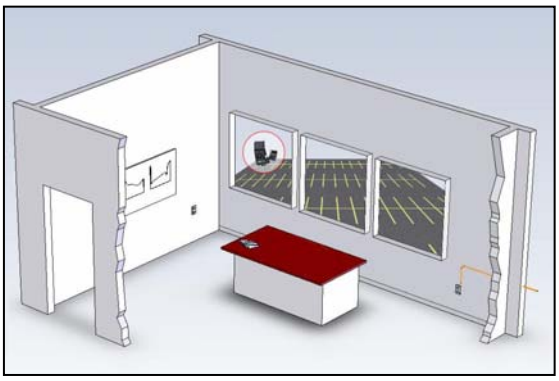
Before discussing the methodology of trace analysis, it is important to understand the OSCOR concept of capturing a peak trace. The peak trace function is very similar to the Max Hold function in most Spectrum Analyzers. However, there is a very important difference in how the data is stored: in most 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.

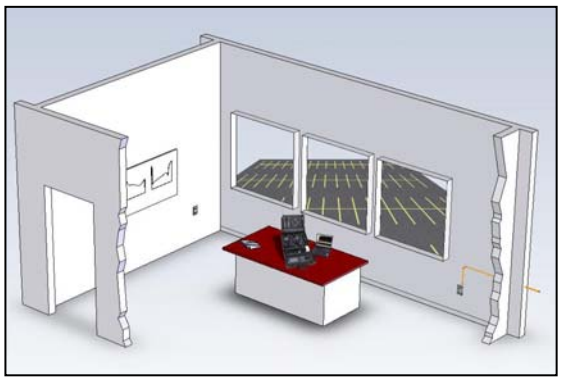
Peak versus Friendly

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

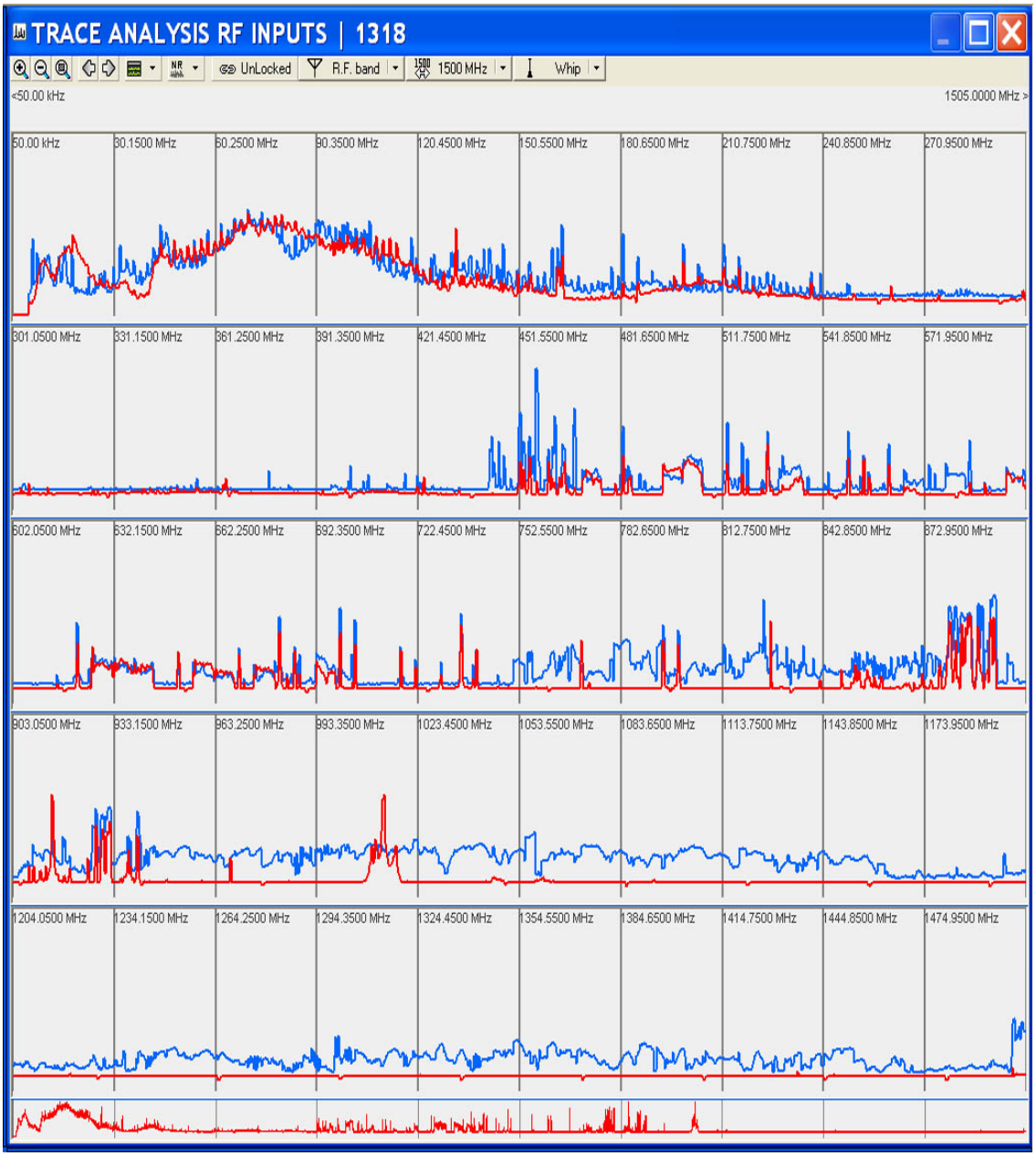
1. **Capture a *Friendly* Trace** at a safe distance from the target environment. Typically this can be done in the parking lot of the building at a reasonable distance from the Target Room. This Peak Trace is called the Friendly Trace. This data should be captured for at least 5 minutes, but better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



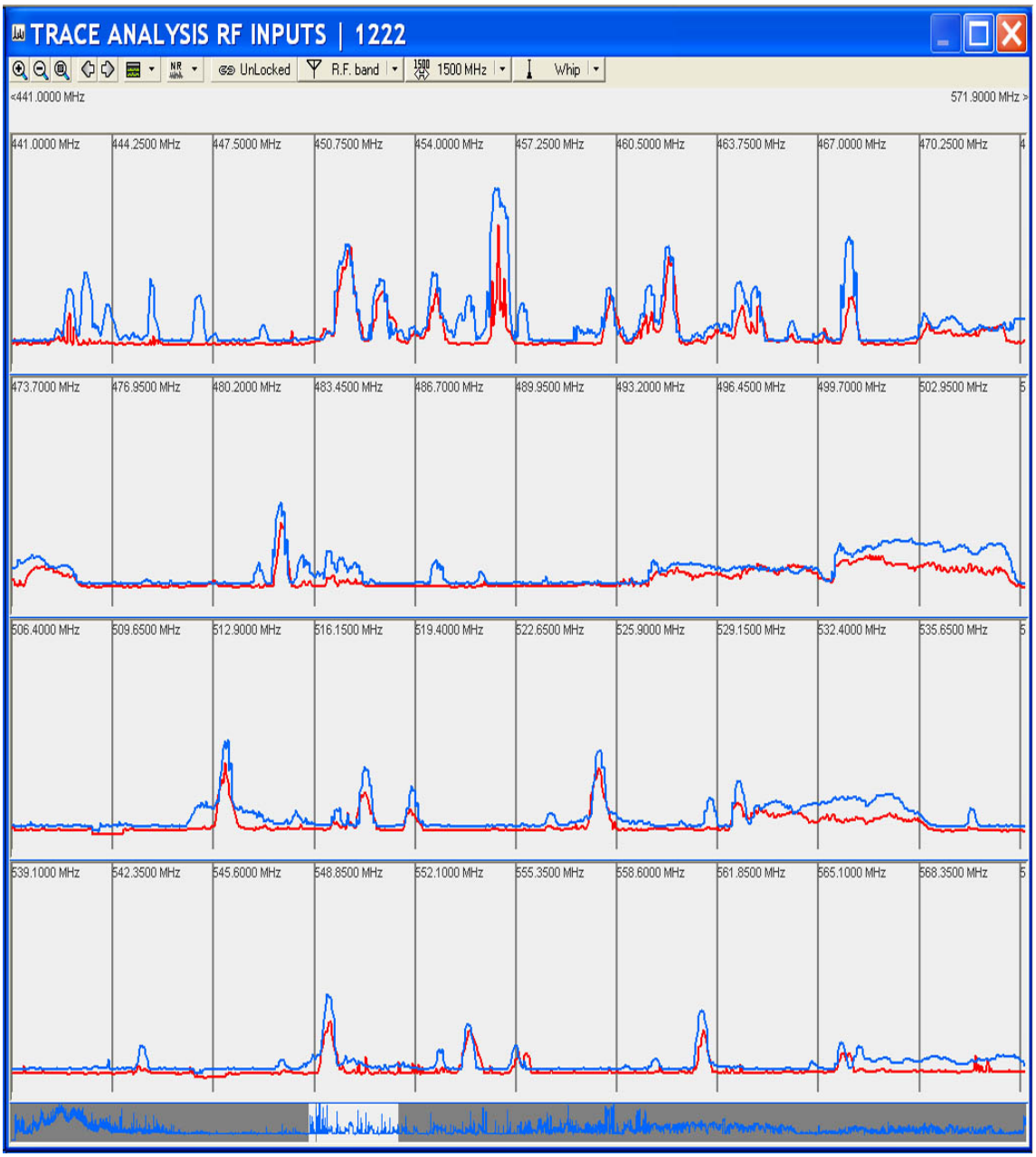
2. **Capture Peak Trace** Data from the Target Environment, and then compare the differences between this trace data and the Friendly Trace. Again, this trace data should be captured for at least 5 minutes, but allowing the Peak capture to run for longer times will increase reliability against intermittent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



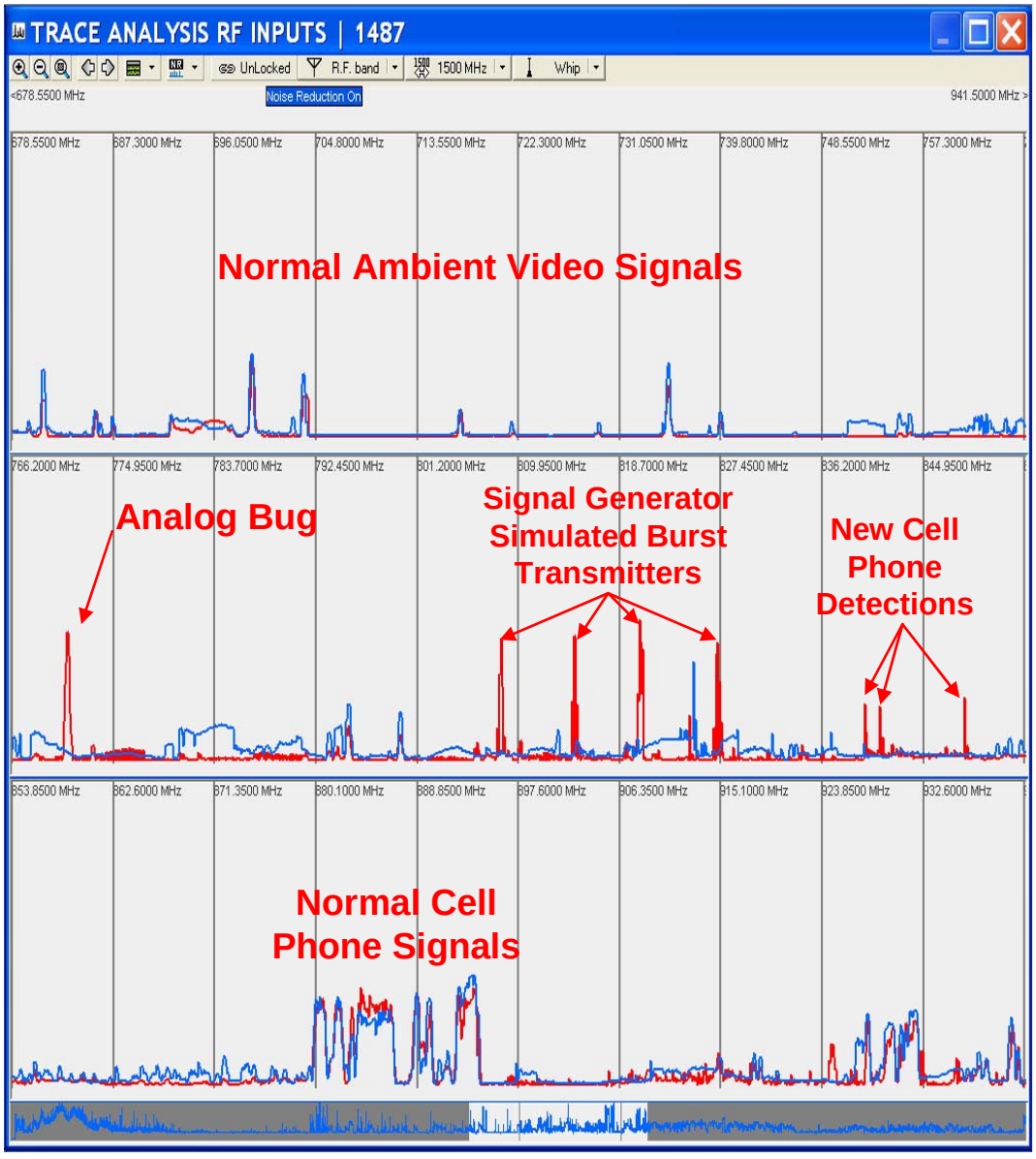
The figure below shows actual Friendly and Peak Trace data that was taken from a building in Dallas Texas. The **Blue** Color shows the **Friendly Trace** captured outside of the target sweep area, and the **Red** shows the **Peak Trace** taken from inside the target building. In General, the **Friendly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

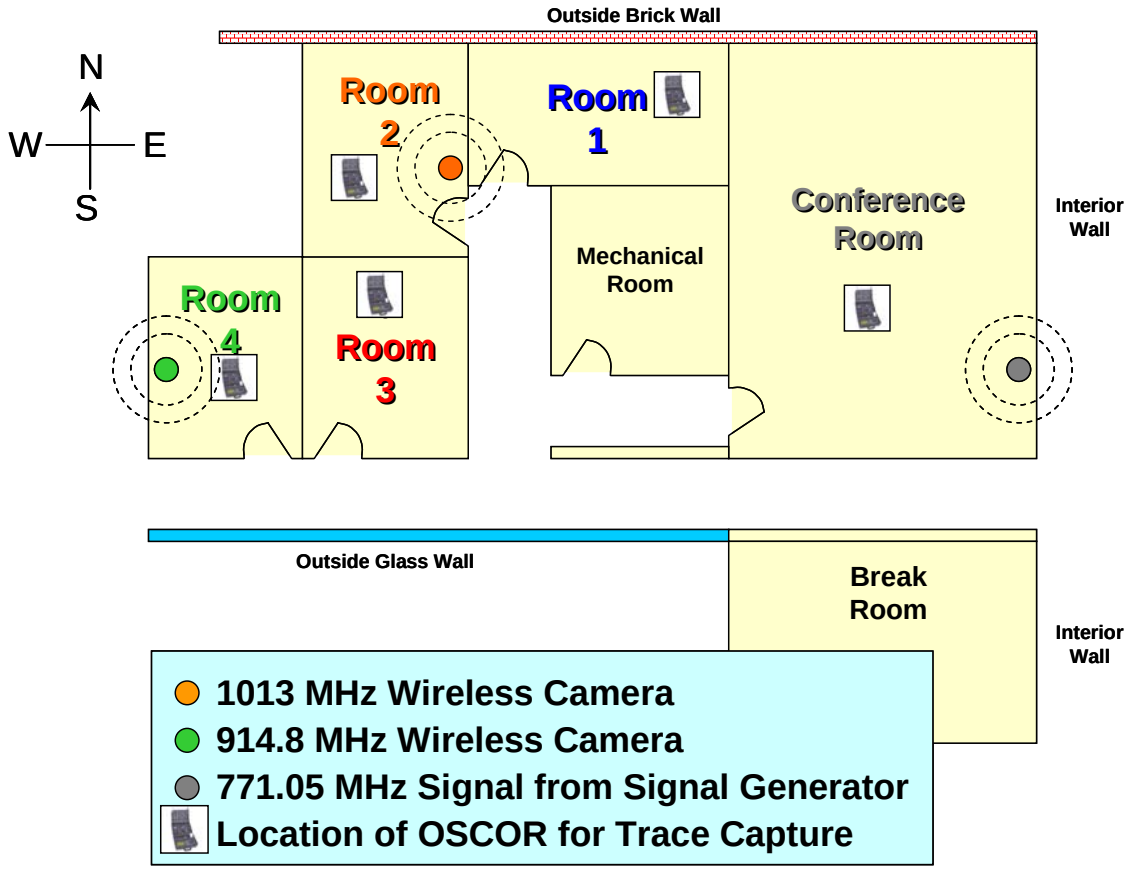


RF Mapping Concepts

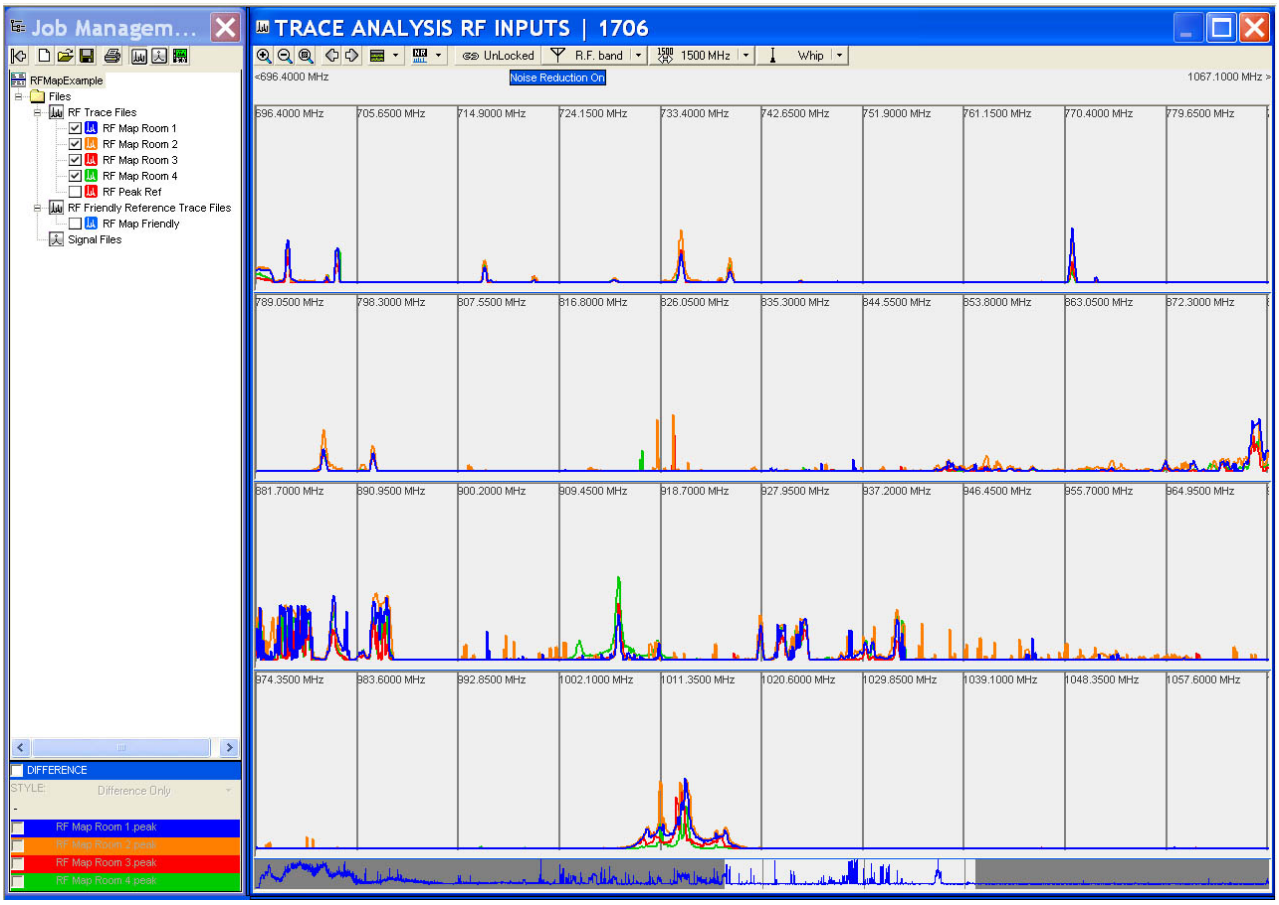
By collecting and storing Peak traces from multiple locations, the concept of trace analysis can be extended to a method of RF mapping. RF mapping refers to the process of taking Peak trace analysis data from different locations within a building and outside of a building and comparing the trace data. 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.



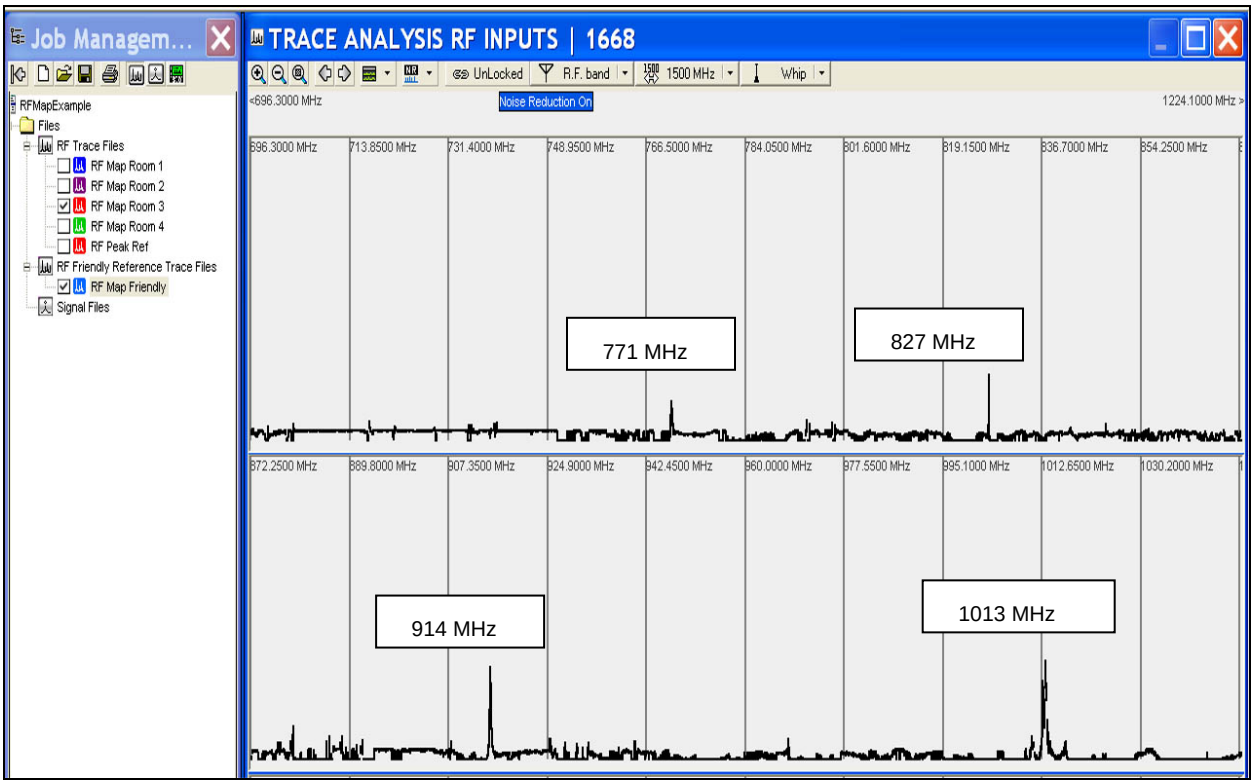
In order to keep this document brief and address the example threats, this document will only address a small portion of this spectrum from 700 MHz to 1100 MHz. A screen shot of the OPC software is shown below with the trace data from the 4 rooms (not including the Conference Room). This screen shot 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.

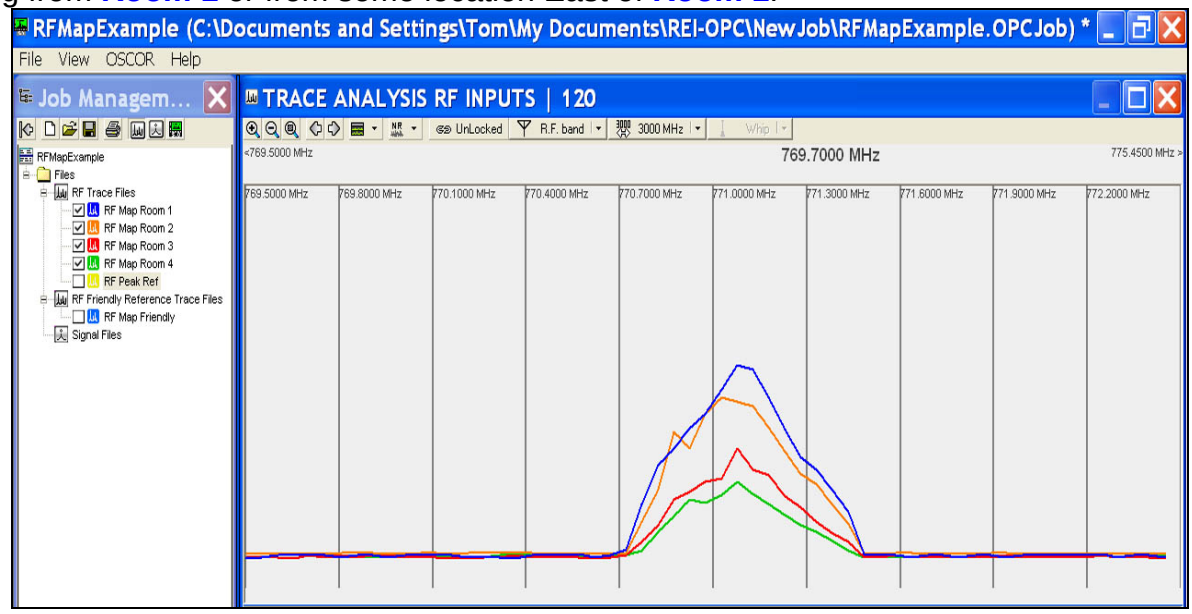
The figure below is a Difference Only graph generated from the **Room 3** data and the Friendly spectrum. **Room 3** was chosen as a starting point simply because it was the most centrally located test point. It is very easy to see 4 distinct signals of concern. Using the pointer on the OPC software,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



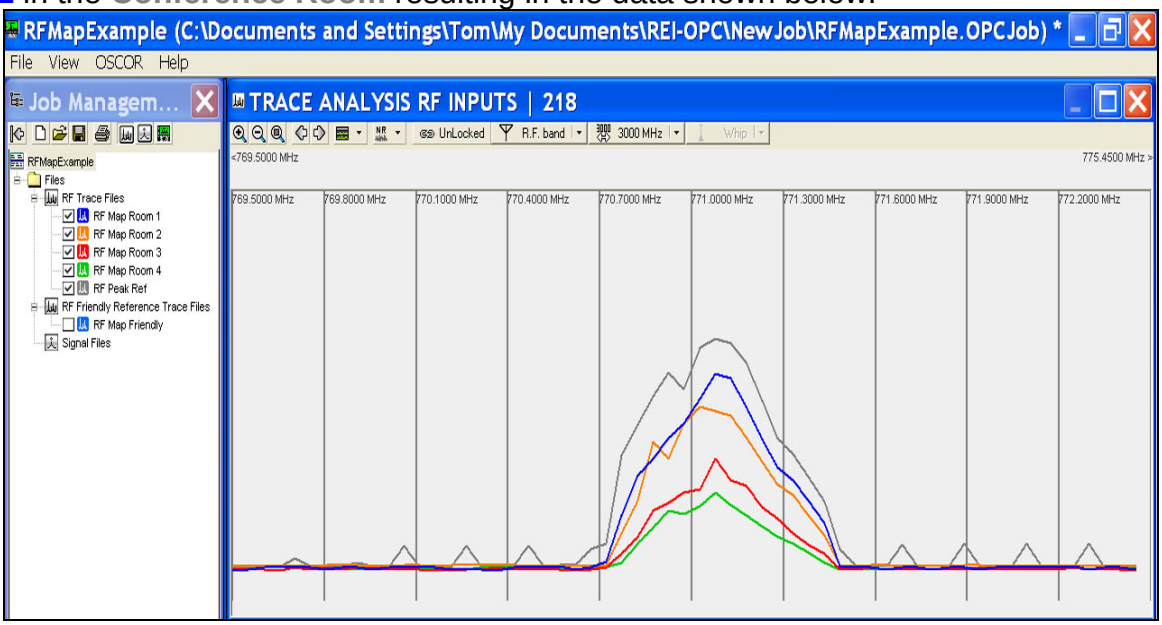
To further analyze these 4 signals, we would zoom in on these signals and examine the additional trace data for each signal. The following sections examine each of these four signals of concern.

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**.



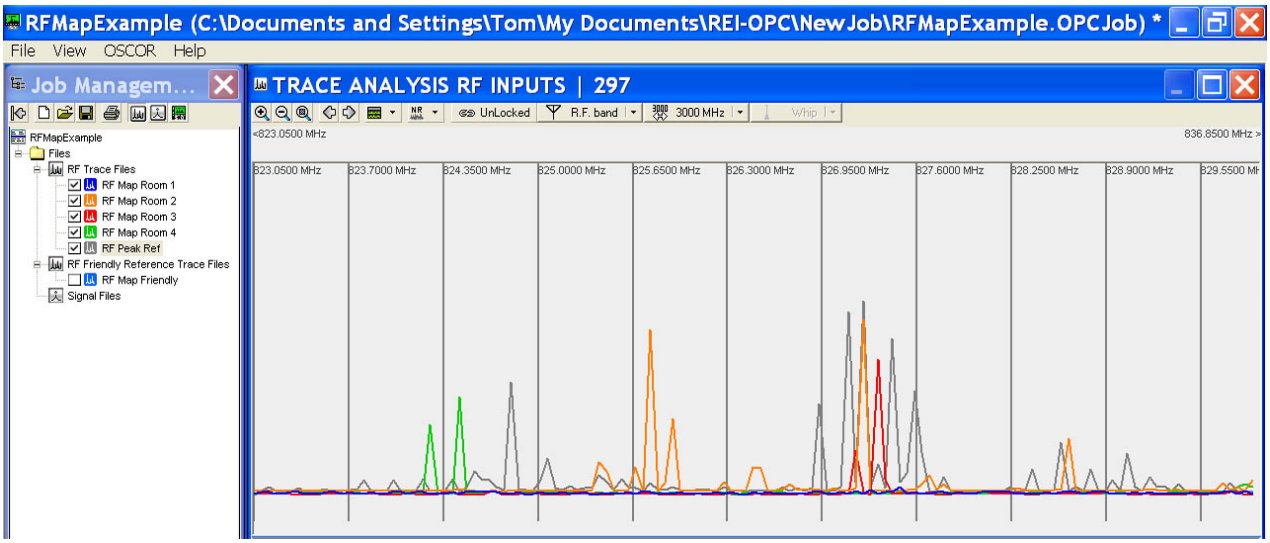
In this case, the signal is actually coming from the **Conference Room** East of **Room 1**. In order to determine the true location of the transmitter, it is necessary to use the OSCOR locator probe. Since the signal was not detected in **Room 1**, additional trace data was taken directly east of **Room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

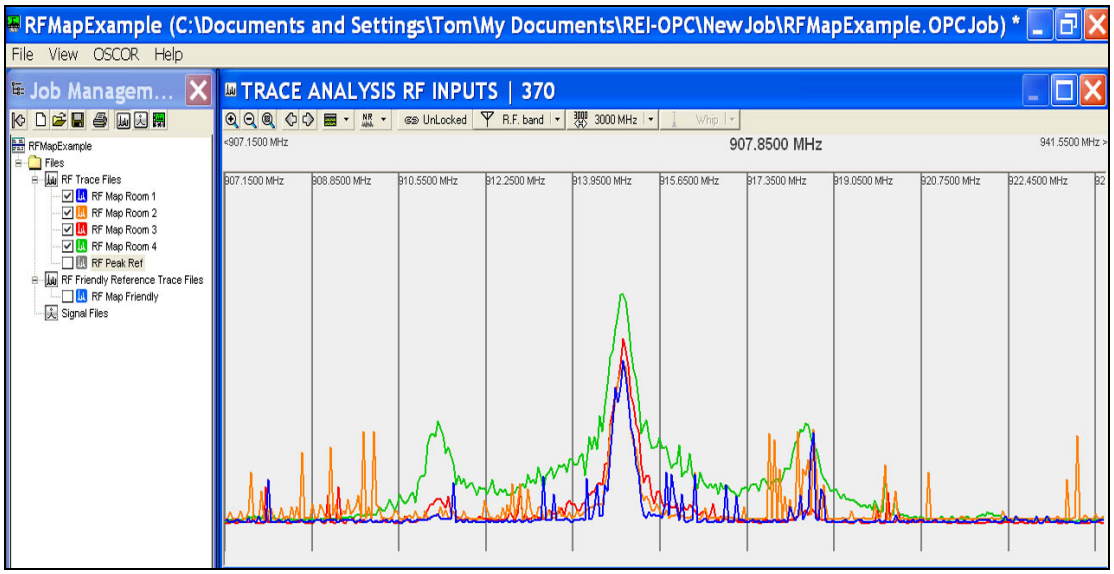
The next signal to investigate had a frequency of 827 MHz. This signal is in the 850 MHz band for US cell phones, and was inspected and discarded as a cell phone transmission. The screen shot below shows several of these signals. The reason that these signals only appear in certain rooms is that that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

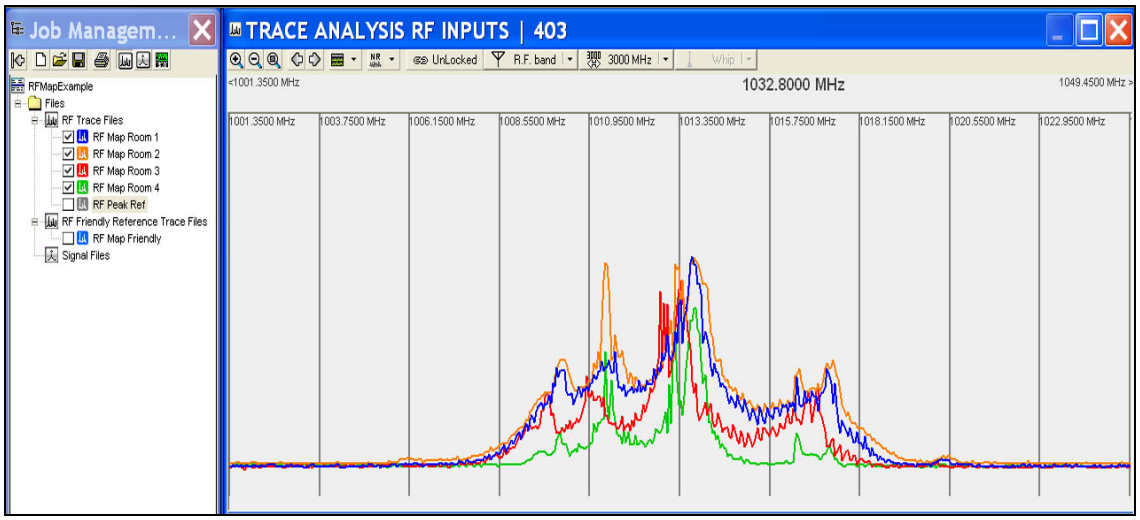
The signal at 914 MHz is clearly a video signal with sub-carrier audio. This can be identified by the characteristic shape of the signal having a wide bandwidth center and side lobes resulting from the audio sub-carrier. The shape of the signal may vary from room to room depending on the changing video 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

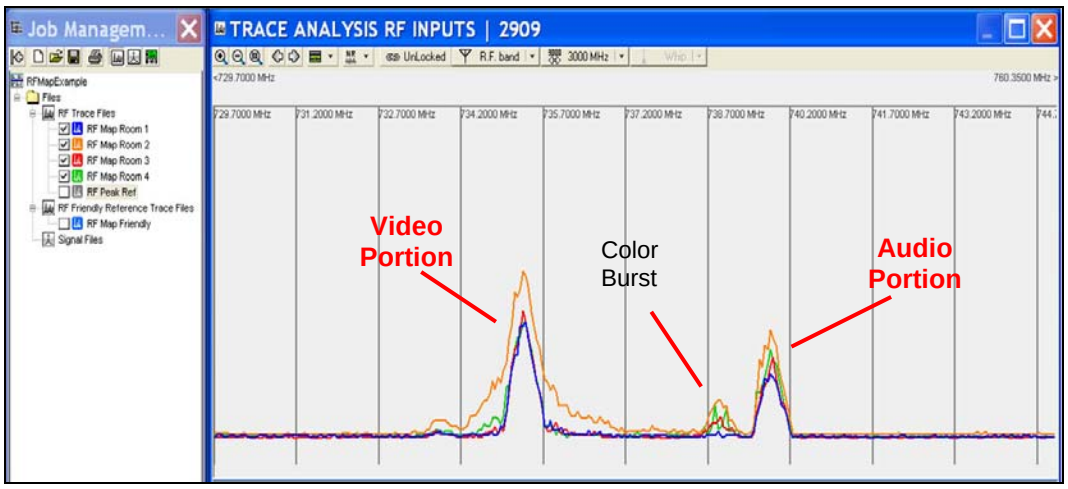
The signal at 1013 MHz also appears to be a video signal based on its shape (wide bandwidth center and side lobes resulting from the audio sub-carrier). The strongest trace level for this signal indicates that the transmitter is located in **Room 2**; it is important to note that **Room 1** has the second 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**.

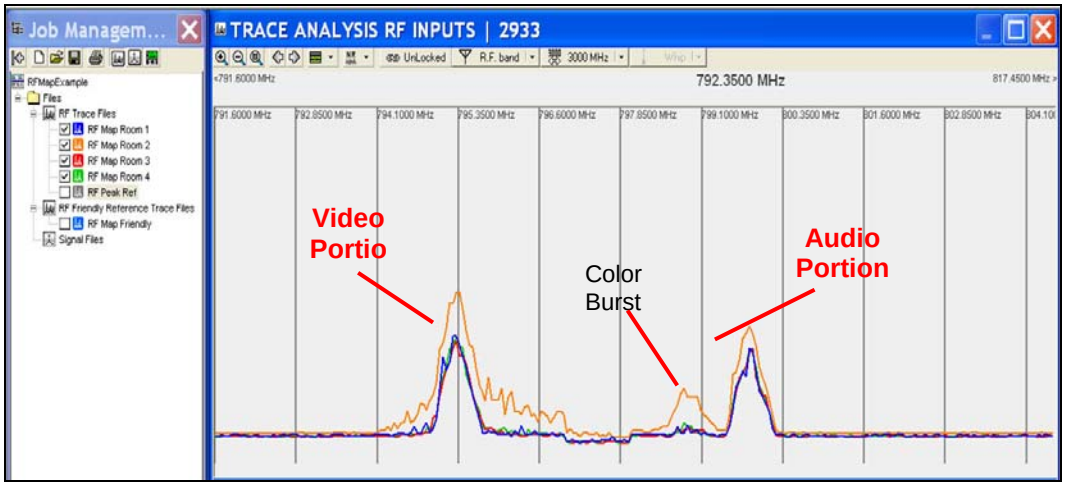


Since the Peak data was stronger in the **Room 2**, the signal was then easily found using the RF locator probe.

Additional Signals Discussed for learning purposes

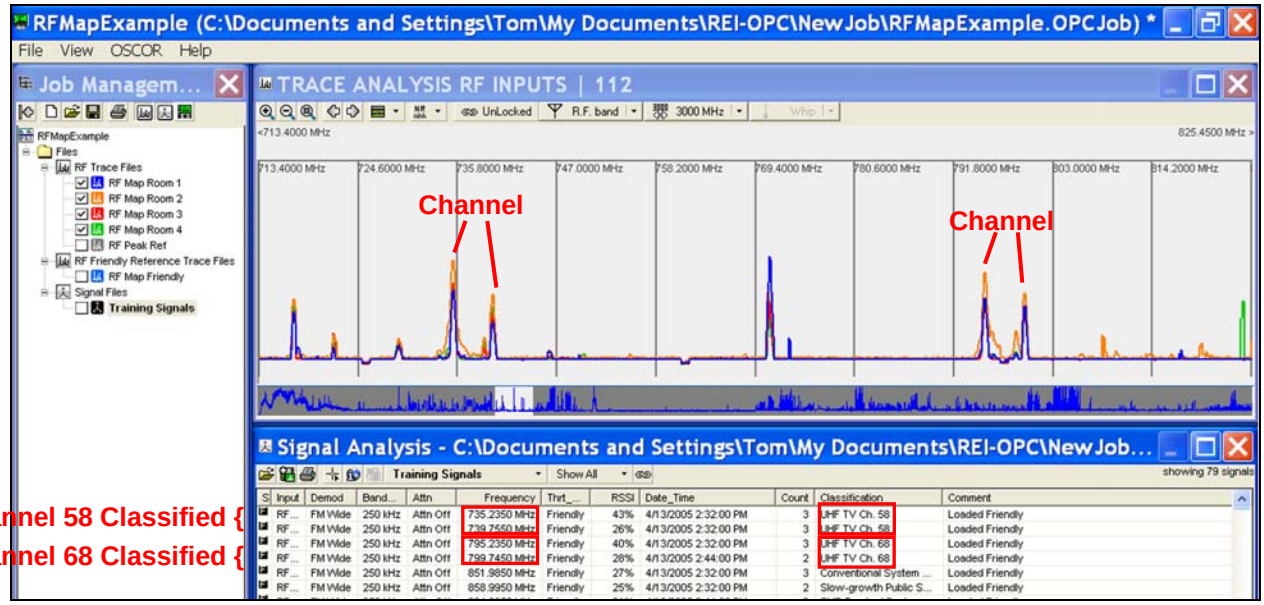
The previous discussion covers all of the signals that were identified as potential threats based on the difference mode. However, within this band there were additional signals that merit discussion. One example is the signals associated with television broadcasts as shown below.



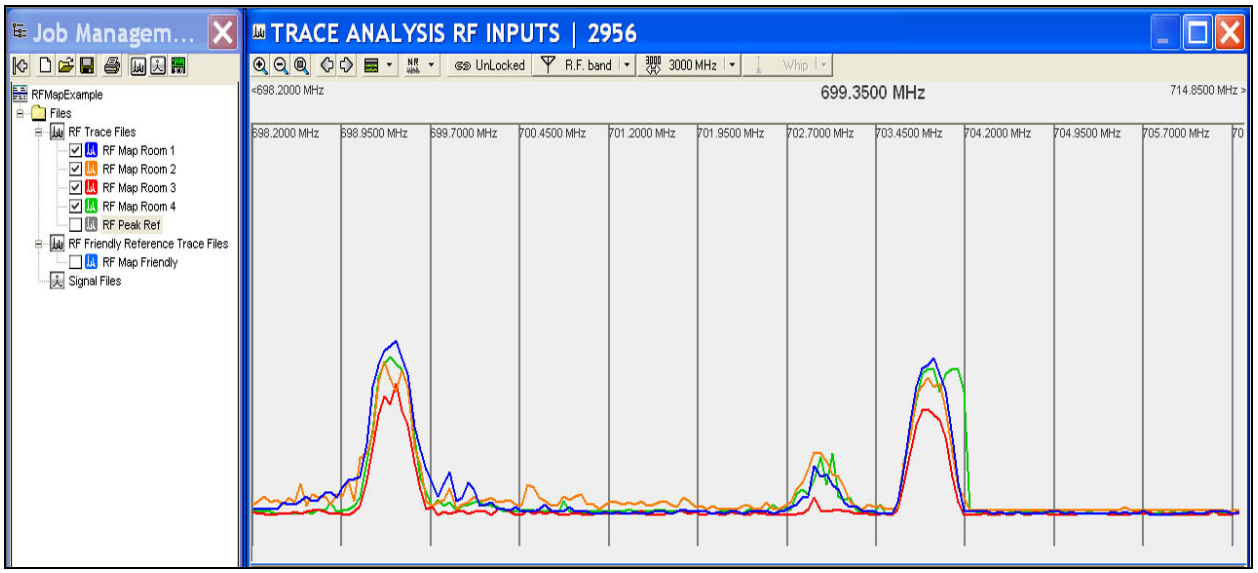


The two screen shots above each show two examples of different television signals, each signal is comprised of 3 portions (labeled in each screenshot): the video portion, the audio portion (standard NTSC television format has the audio signal 4.5 MHz above the video signal), and the color burst portion 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.

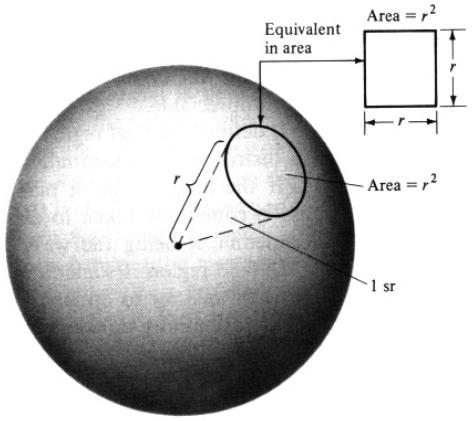


Figure: *Antenna Theory, Analysis and Design*, Constantine A. Balanis, 1982 Harper & Row.

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.

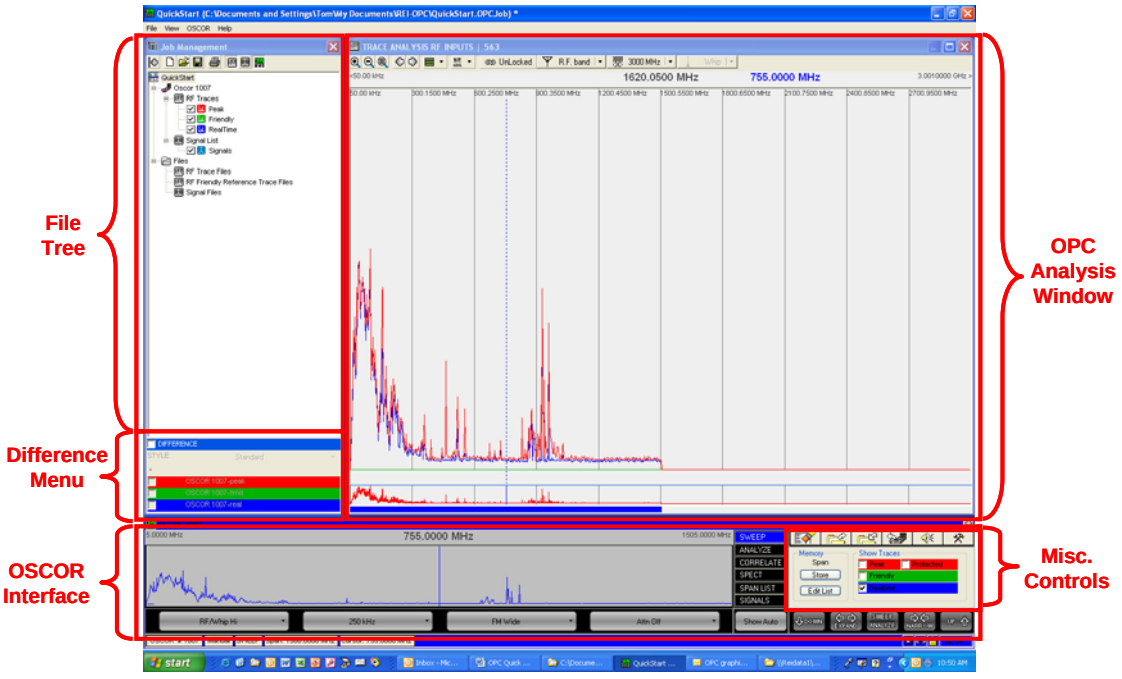
   c. Wood will also provide some attenuation but not as much as Brick and Mortar.
   d. Glass provides very little attenuation.
2. Metal structures such as filing cabinets, steel beams, door frames, drop ceiling grids, furniture, heating and cooling systems create reflections, diffractions, and scattering, 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.

OPC Quick Start Exercises

This section is intended to provide some very short exercises that will help the user quickly gain a working knowledge of some of the more basic functions and procedures. This section is not intended to provide complete explanation of either the suggested procedures or all of the OPC functions. In these exercises, a single transmitter is used simply for demonstration. The device used is a low power digital device at 420 MHz with a bandwidth of approximately 500 kHz. It is recommended that the user obtain some type of commercially available transmitter and duplicate these exercises understanding that the frequencies will be different and the spectrum displays will look different due to the nature of the different environment and different transmitter. Also, the OPC colors that were used in these exercises were altered from improved printing display. The default colors will not be the same as you do the exercises. Finally, these exercises assume that you have a basic knowledge of the OSCOR and its functions. The main emphasis of these exercises is to describe the basic concepts of trace analysis as they relate to comparing a Friendly Trace spectrum to a Peak Trace, and also to introduce the concept of RF mapping. If you do not have a working knowledge of OSCOR functions, it is recommended that your first review the Quick Start Exercises in the OSCOR manual.

Some Important observations regarding the OPC display.

- The Top Portion of the screen is the Analysis window for the PC and shows data that is stored in File or retrieved from the OSCOR.
- The bottom portion of the Screen is purely the direct OSCOR display and controls.



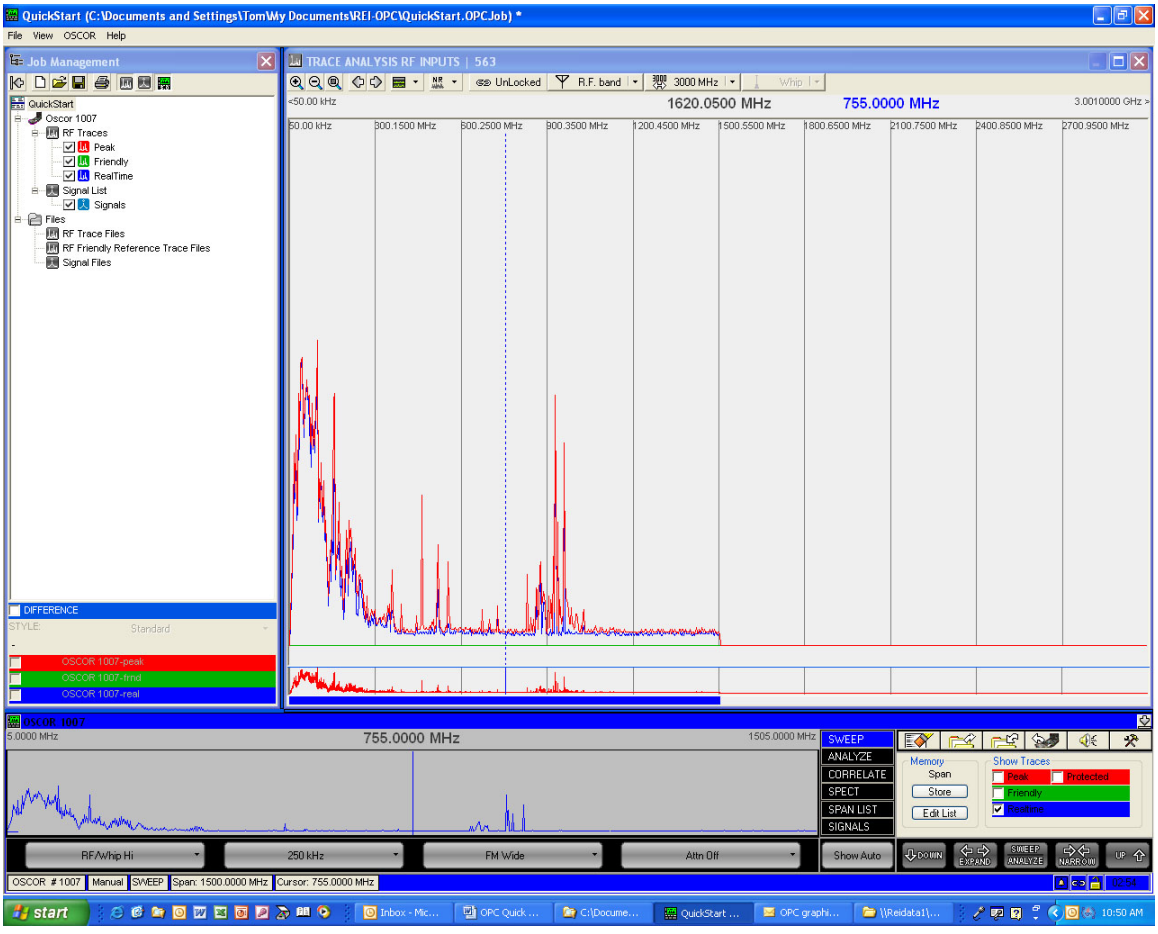
Exercise 1 – Peak Minus Friendly Trace Analysis .

The purpose of this example is to show the basic steps and OPC controls to

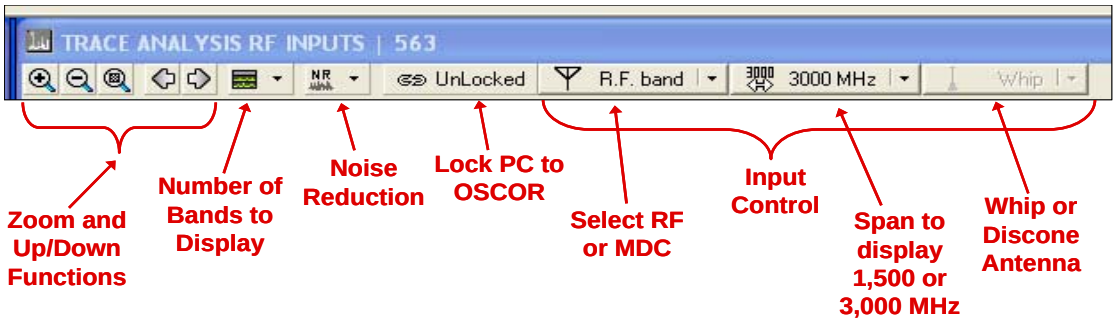
- Load a Friendly trace
- Capture a Peak trace
- View the difference mode
- Zoom in to a signal and analyze that signal.

Note: Before starting exercise, you will need a test transmitter, do not turn on yet. This exercise uses a device at 420MHz.

1. Turn on OSCOR and PC separately
2. Properly Connect cable to PC USB and then to OSCOR USB.
    a. Start OPC software
    b. Click on New Job
    c. Name Job as desired
3. Default span should be Whip Hi
    a. Have test transmitter ready to turn on later
    b. Color Scheme of screen shots will not match defaults. Color scheme was adopted to improve the printed view.

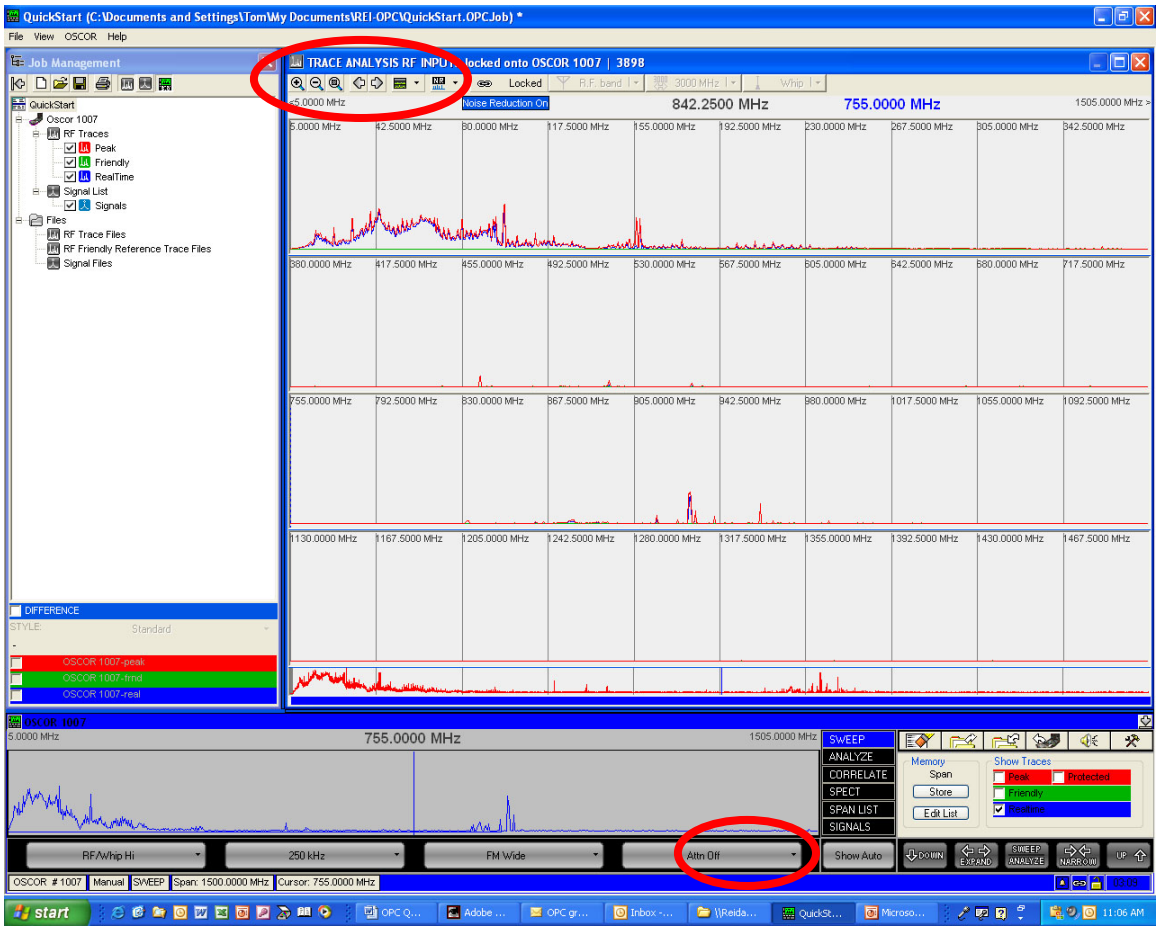


Note: the Control Buttons at the top of the Analysis window control the Analysis window. You can also, Right-Click on the screen to adjust the background color and access most of these same controls. It is suggested that you try these functions.



Note: the Analysis Window only shows data in 50KHz resolution. Therefore, the analysis window should only be used for higher frequency inputs such as Whip, Discone, and MDC.

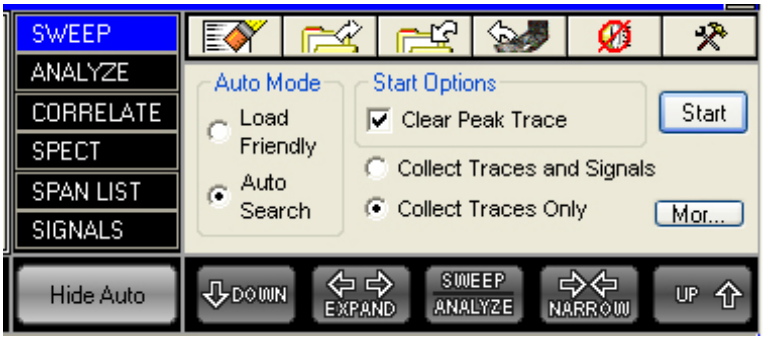
c. Click on "Number of Bands to Show" and select 3, 4, or 5. This makes it easier to see the spectrum.
d. Click on the Lock button to Lock the OPC to the OSCOR.



4. Click on “Show Auto” to open the Automatic Set-up
    a. Select Load Friendly
    b. Check Clean Start-Erase All
    c. Collect Traces Only
    d. Click “Start” then “Yes” to proceed.

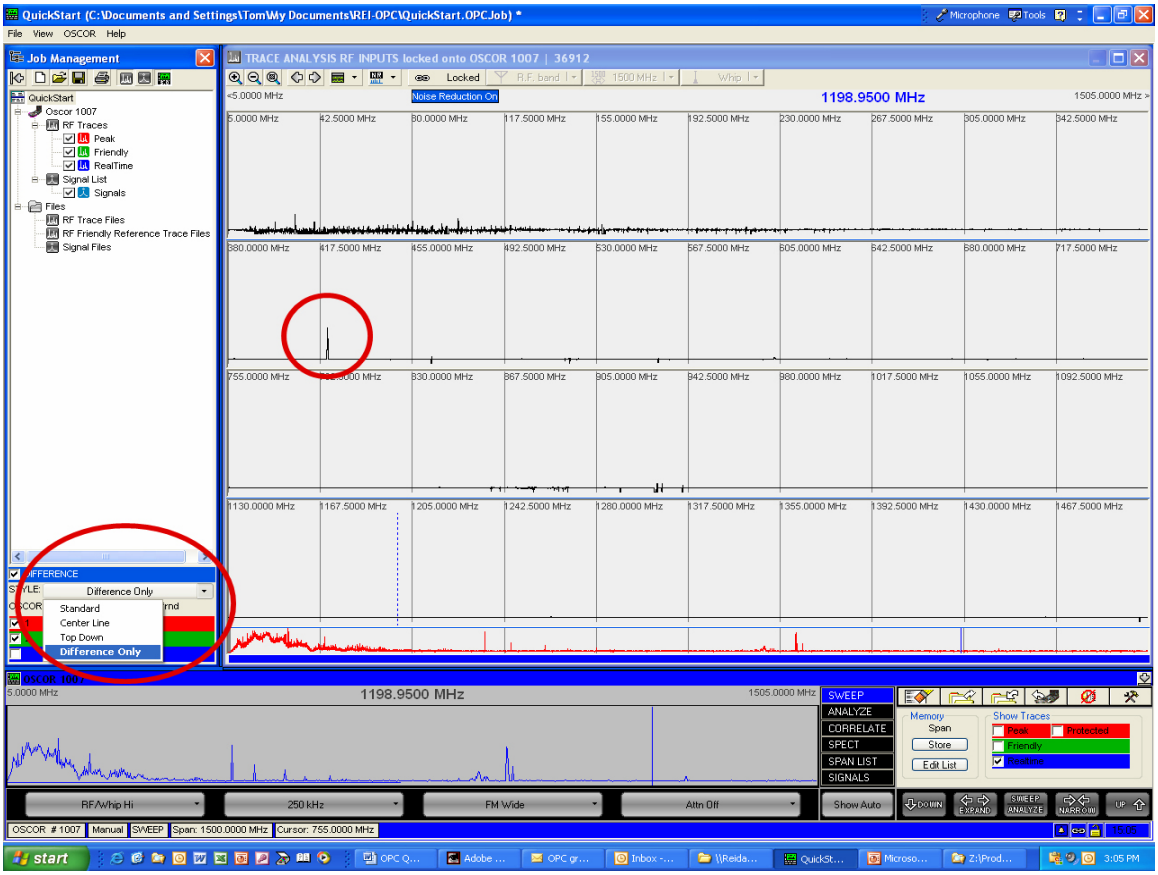
5. Allow the OSCOR to Capture Friendly trace data until at least 1 Cycle has been completed. This is indicated by the log and the Auto mode display as shown below. Click on “Stop Auto” and then “Hide Auto” (It is the same button that is relabeled).

6. Turn on a Test Transmitter. The Test transmitter used in this example was a low power digital transmitter at 420 MHz.
7. Click on “Show Auto” to open the Automatic Set-up
    a. Select “Auto Search
    b. Check “Clear Peak Trace”
    c. Collect Traces Only
    d. Click “Start” then “Yes” to proceed.

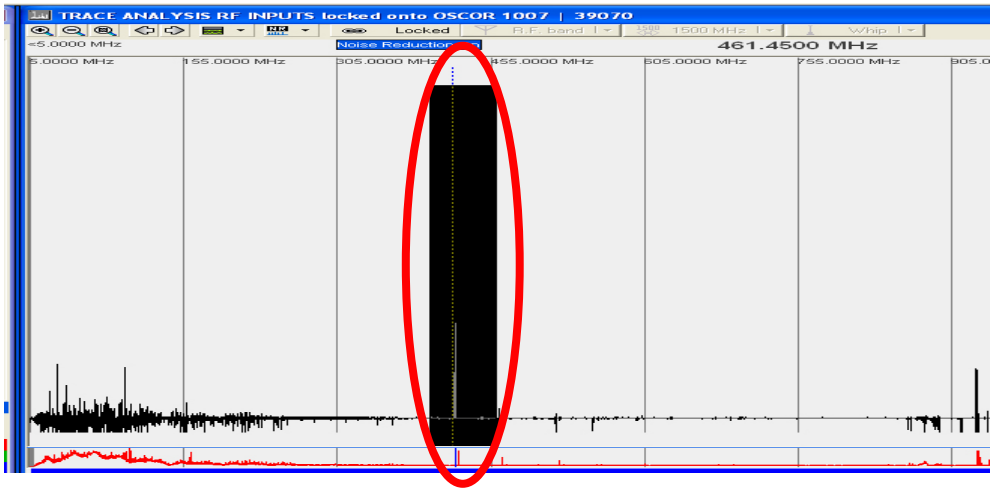


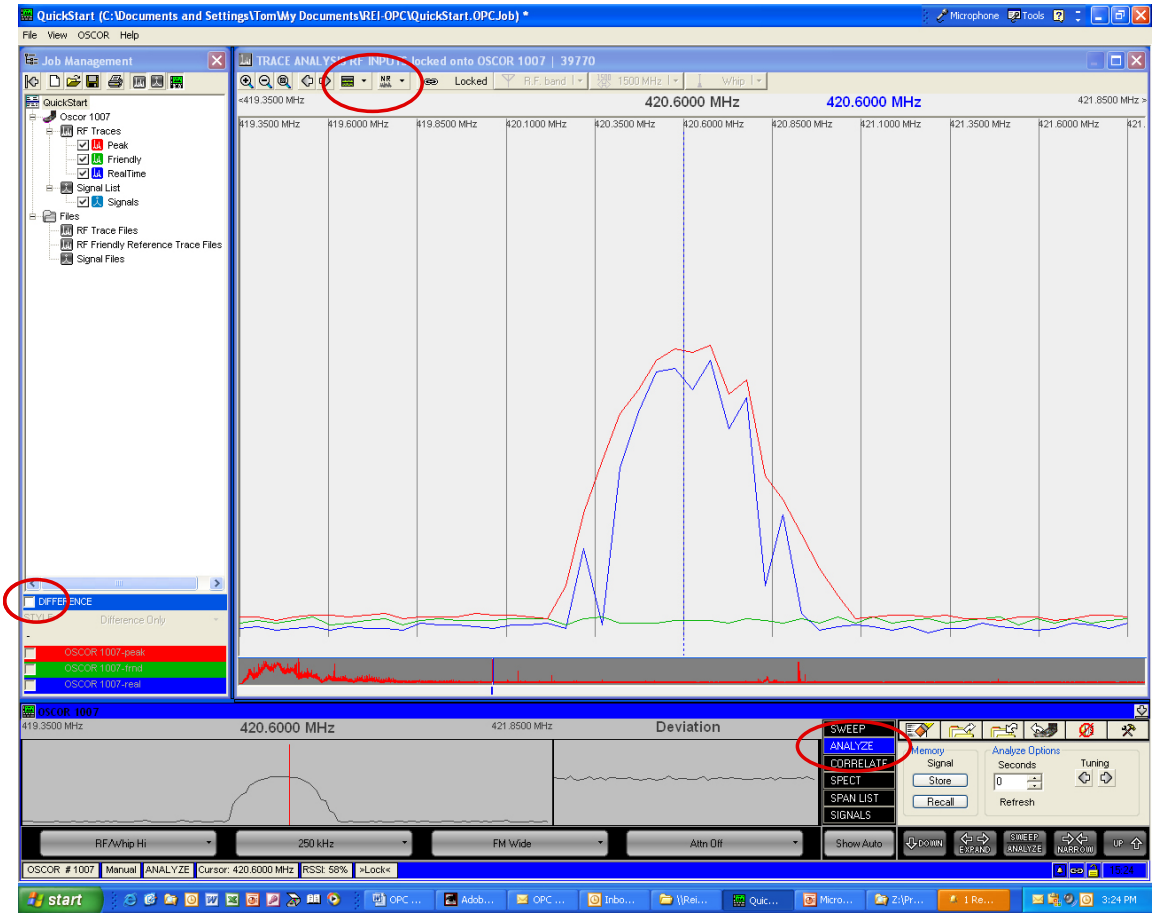
8. Allow the OSCOR to Capture data until at least 4 Cycles are complete. Click on “Stop Auto” and then “Hide Auto” (It is the same button. The “Hide Auto” but simply returns the original default menu. You should notices that under the Show traced menu, the Peak Protected box is now checked to ensure that this Peak data is not overwritten if the OSCOR is moved to another location).
9. Click on the Difference Display to turn on the difference mode. The Graphic display shows the result.

10. To enhance the view of the newly detect signal, click on the Difference Only Format under the File tree structure.



11. Now that a new signal has been identified, this signal can be quickly analyzed. The following steps should be taken to zoom in and evaluate the signal.
    a. Turn off the multiple bands and return to 1 band.
    b. Drag across the signal of interest to zoom in on that signal.
    c. Turn the Difference Mode off so that you can see the real-time display data from OSCOR.
    d. Click on the Analyze label and turn up the OSCOR volume if you wish to listen to this signal.

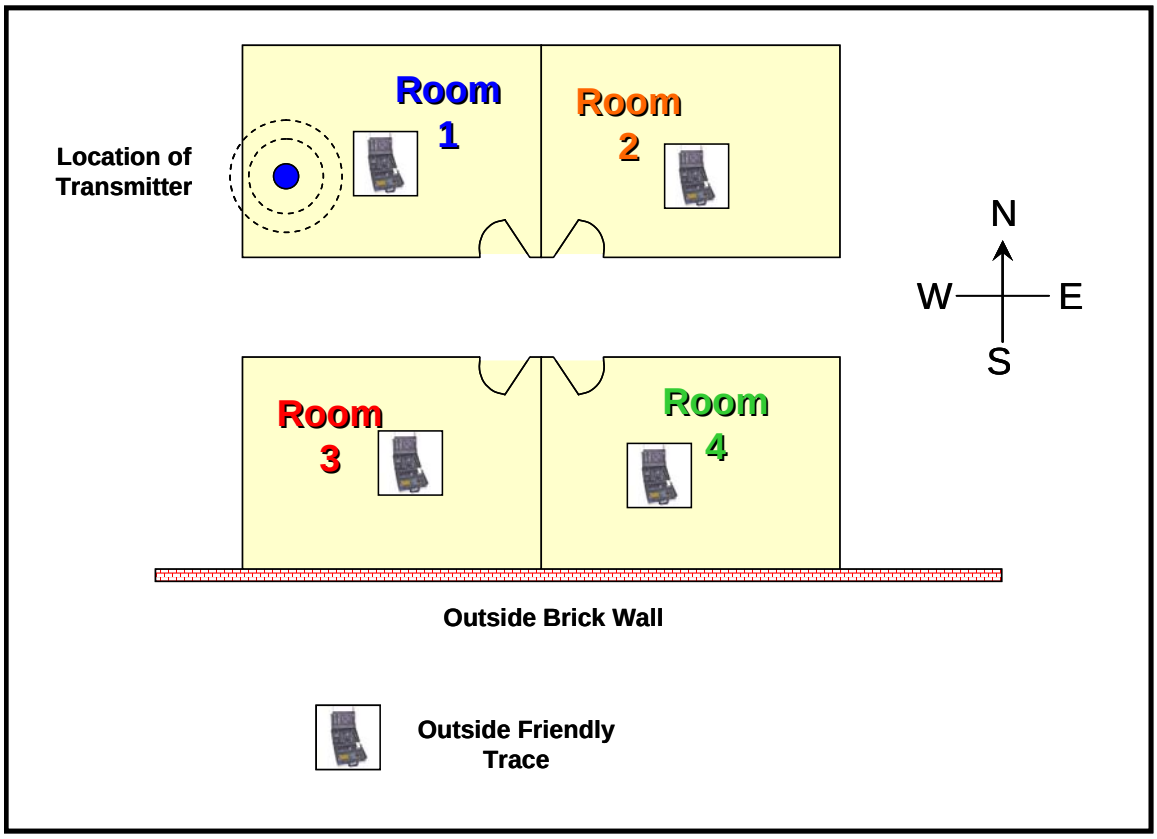




This particular signal was from a digital transmitter with approximately 500KHz bandwidth. It has no analog modulated audio and therefore you cannot use the OSCOR OTL device to locate the signal. At this point, the method to locate the transmitter is to remove the RF Locator probe from the OSCOR, and use the RF Locator method to locate the transmitter in the room.

Exercise 2 – RF Mapping Trace Analysis .

This exercise is designed to introduce the concept of RF mapping, and to provide a more realistic example procedure that may implemented in a sweep. It assumes that there are 4 rooms to sweep. In this example, the same transmitter from the previous exercise will be used, but the transmitter will be placed in an unknown room location. The problem is to identify that a threat exists and then identify the room location of the threat. It is recommended to read through this exercise completely, and then repeat the exercise adapting it to your environment and available transmitter by having a friend hide a transmitter in a nearby office, and attempt to locate the transmitter using the same method described herein.
For this example the following room layout was used.



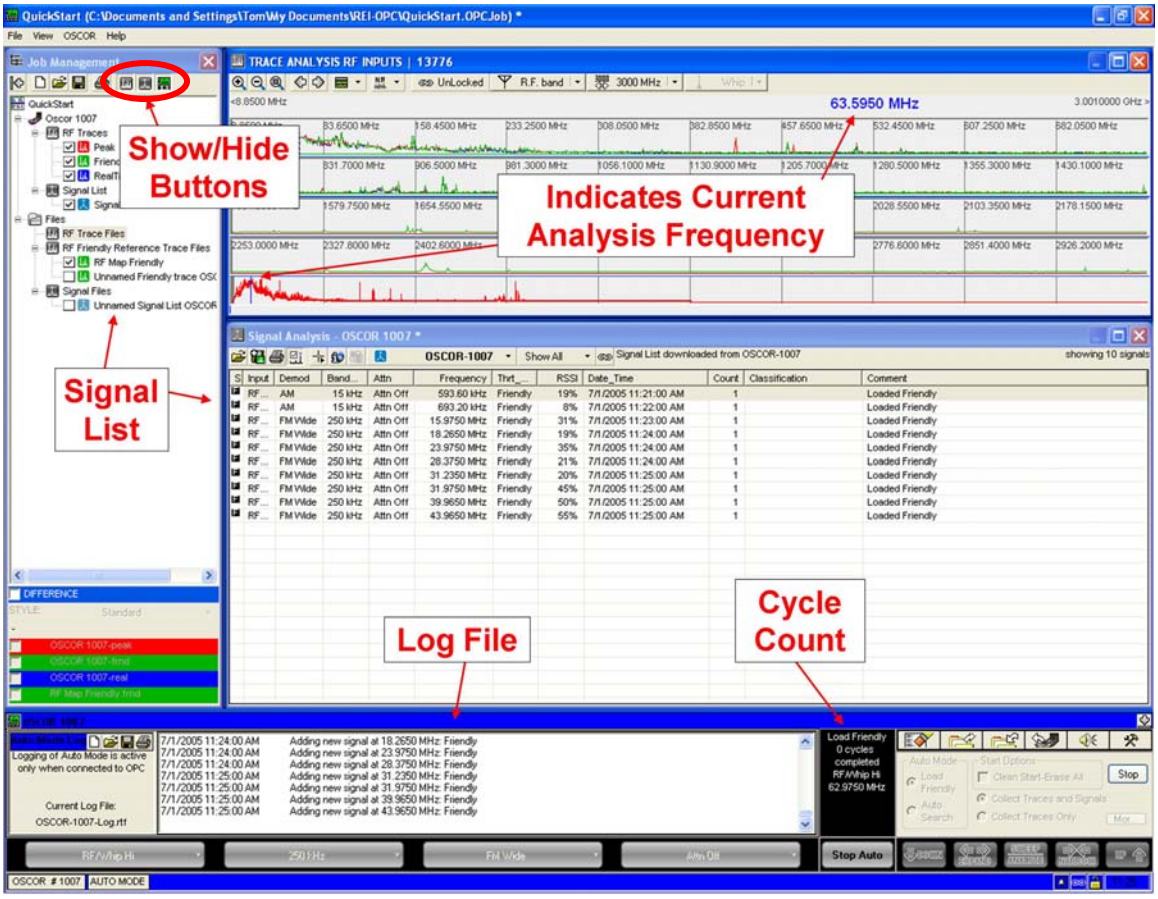
1. Setting up OPC to prepare for a sweep.
    a. Turn on OSCOR and PC separately
    b. Properly Connect cable to PC USB and then to OSCOR USB.
        i. Start OPC software
        ii. Click on New Job
        iii. Name Job as desired
    c. Default span should be Whip Hi
        i. Test transmitter should be available to use later, but turned off.
        ii. In this example, the color Scheme of screen shots will not match normal OPC defaults. This color scheme was adopted to improve the printed view.
    d. Click on “Number of Bands to Show” and select 3, 4, or 5. This makes it easier to see the spectrum.

e. Click on the Lock button to Lock the OPC to the OSCOR. This is not required, but recommended to minimize confusion between the OPC analysis screen and the OSCOR display screen.
f. Turn on the bug in one of the rooms. (Room 1 for this example).

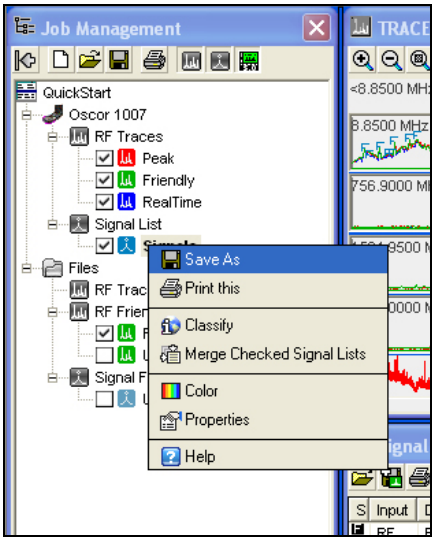
Note: In this exercise, we recommend to Load Friendly Signals as well as loading Friendly traces. This provides a good report data and reference signals for comparison and signal analysis if necessary.

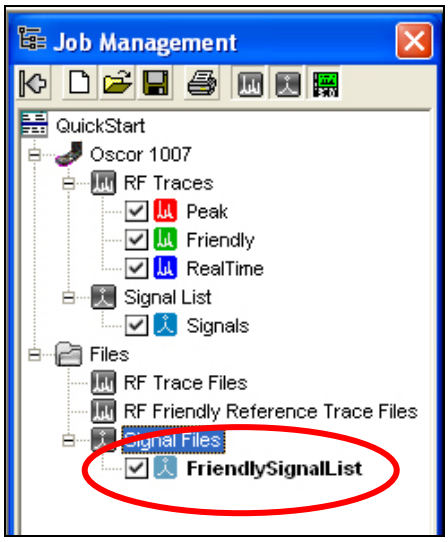
2. Loading and Saving Friendly Signals - Take the OSCOR outside of the building to Load Friendly.
   a. Start Load Friendly
      i. Click on "Show Auto" to open the Automatic Set-up
      ii. Select Load Friendly
      iii. Check Clean Start-Erase All
      iv. Collect Traces and Signals Only
      v. Click "Start" then "Yes" to proceed.

      vi. Stop Load Friendly - Allow the OSCOR to Capture Friendly Signal data until at least 1 Cycle has been completed. This typically takes between 15 and 40 minutes depending on the number of signals in the ambient environment. The number of cycles is indicated by the log and the Auto mode display as shown below. Click on "Stop Auto".
      vii. Show the Signal List – Click on the "Show/Hide Signal List" Button as indicated in the figure below. These buttons toggle the various display windows On and Off. You may wish to try then all to see the various screen options.

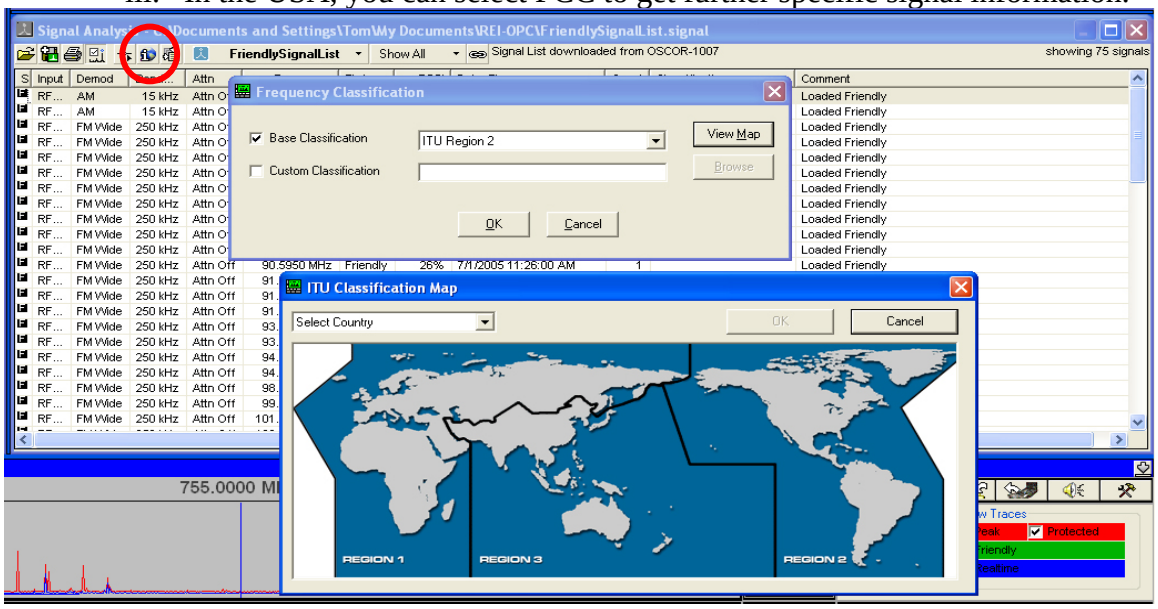


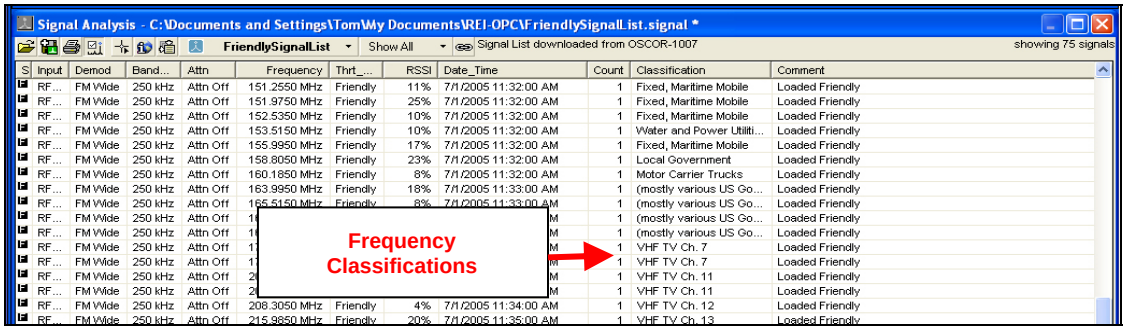
b. Save Load Friendly Signals to file - After Capturing the Friendly signals, it is important to save this Friendly Trace to the PC to keep as a reference. This is accomplished by putting the mouse on the Friendly Trace listed in the File tree and Right-Clicking to bring up the "Save As" menu. Type in a File name and enter OK.



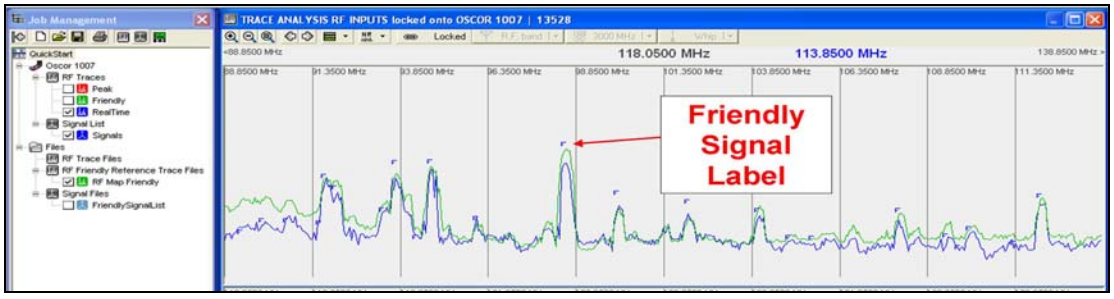


c. Classify Friendly Signals – The OPC software has a built-in database of the ITU (International Telecommunications Union) frequency bands and Regions.
   i. Click on the Frequency band information button.
   ii. Select the region of interest and select OK.
   iii. In the USA, you can select FCC to get further specific signal information.





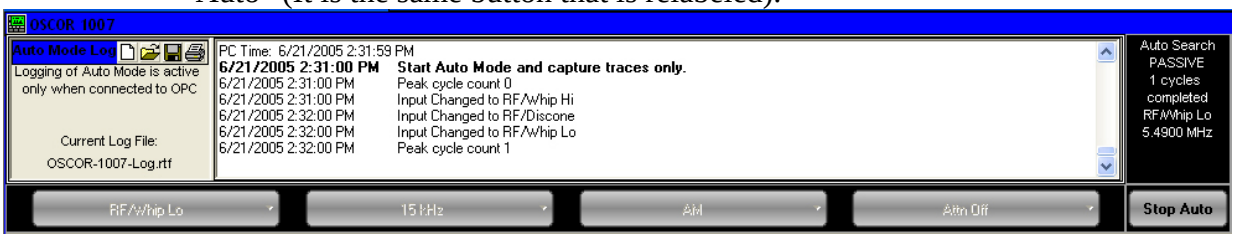
d. Hide Signal List – Click on the "Show/Hide Signal List button" as discussed above (or click on the X button in the window).
e. Note: If the signal list is checked in the file tree, then a small icon will be displayed in the trace analysis window above each signal to indicate that it is in the database. A friendly signal will be designated with an "F"



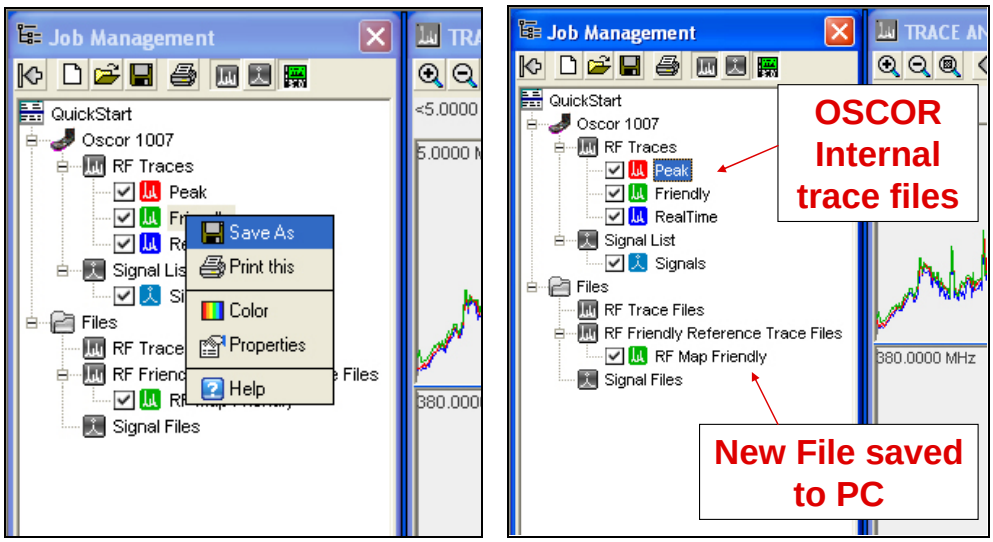
Note: The process of loading Friendly signals also produces Friendly trace data; however, the number of traces is only equal to the number of cycles. If you run a "Trace Only" Load Friendly, then logging signals is ignored and you can capture many traces at a much faster rate producing a more accurate Friendly Trace spectrum which will generate a better representation of intermittent signals such as pagers, mobile radios, mobile phones, etc..

3. Loading and Saving Friendly Traces
    a. Loading Friendly Traces
        i. Click on "Show Auto"
        ii. Select Load Friendly
        iii. **Un**-Check Clean Start (You do not want to erase the previously saved Signal data, however, even if you do, you have saved this signal data to the computer and it is not lost.)
        iv. Select "Collect Traces Only"
        v. Click "Start" then "Yes" to proceed.

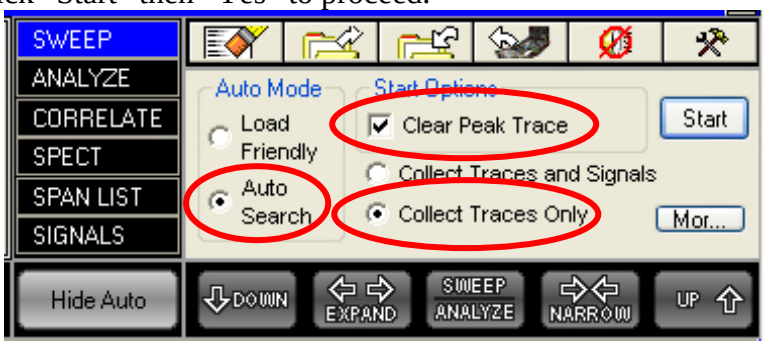
    b. Allow the OSCOR to Capture Friendly Trace Data for as long as possible. Since the traces data for the default inputs (Whip Lo, Whip Hi, and Discone) should only take about 50 seconds per cycle, it only takes a few minutes to gather several cycles. This is indicated by the log and the Auto mode display as shown below. Click on "Stop Auto" and then "Hide Auto" (It is the same button that is relabeled).



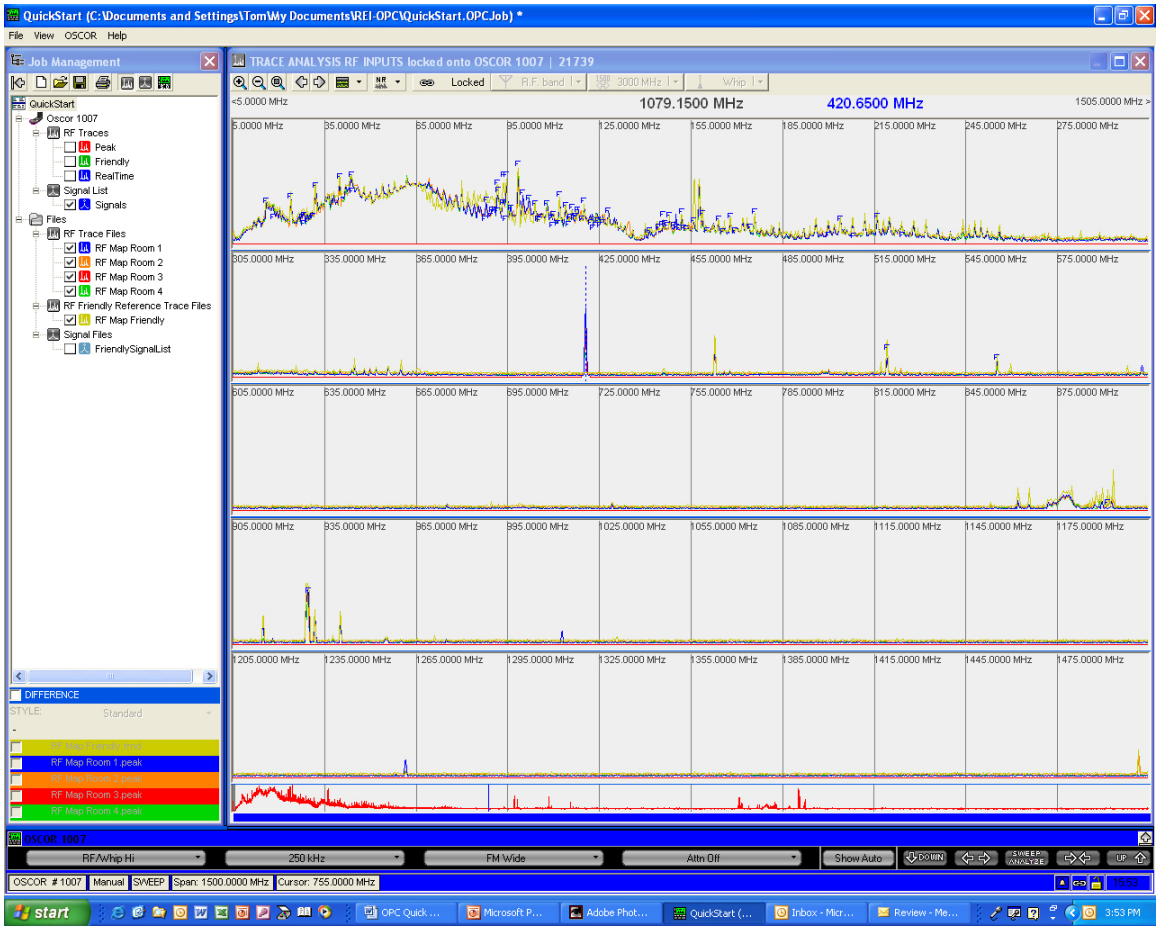
    c. Saving Trace Data to File
        i. Put the mouse on the Friendly Trace listed in the File tree and Right-Clicking to bring up the "Save As" menu.
        ii. Type in a File name and enter OK.



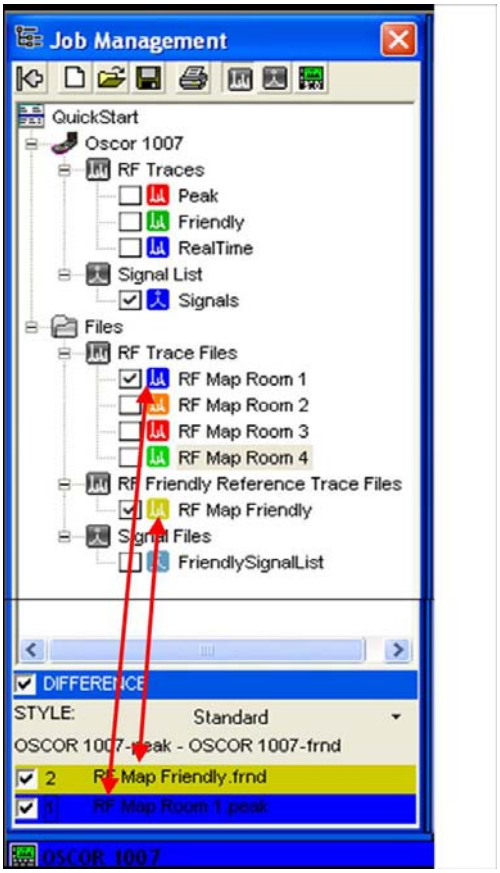
4. Capture Peak Trace Data in Rooms of Interest – Take OSCOR to each room of interest and repeat these steps:
    a. Capture Peak Trace Data of a Room
        i. Click on “Show Auto” to open the Automatic Set-up
        ii. Select “Auto Search
        iii. Check the “Clear Peak Trace”
        iv. Select “Collect Traces Only”
        v. Click “Start” then “Yes” to proceed.

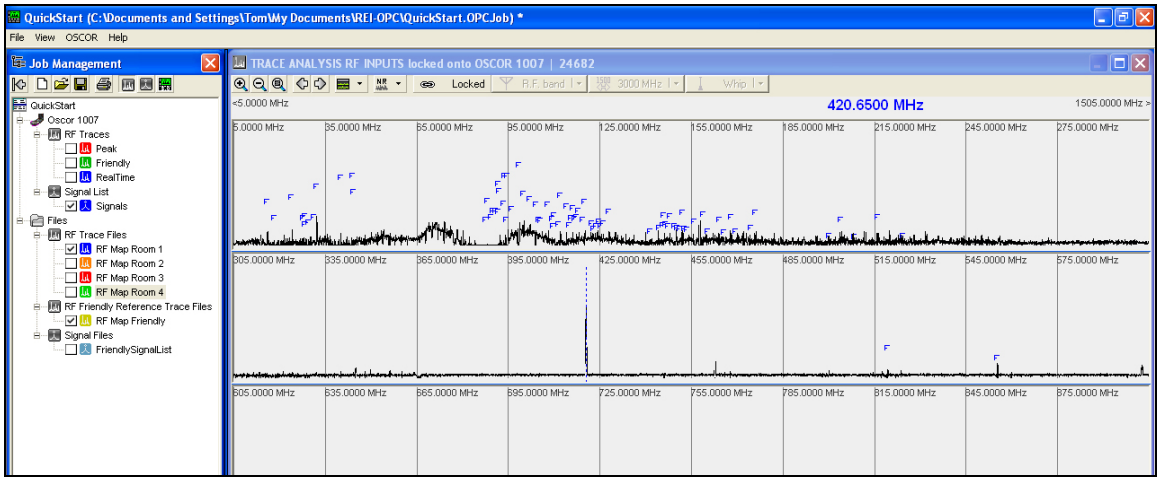


        vi. Allow the OSCOR to Capture Peak trace data for as long as possible or until at least 4 Cycles have been completed.
        vii. Click on “Stop Auto”.
    b. Save Peak Trace for Room - Right click on the Peak Trace File from OSCOR and select “Save As”. The filename that you enter should reflect specific room locations.
    c. Steps a and b, should be repeated in each of the 4 rooms so that Trace data is saved for each room of interest.
5. Analyze Trace Data
    a. Prepare Analysis Display
        i. Right Click on each saved trace to specify a trace color. For this exercise the colors of these traces were chosen to match the color code on the room map at the beginning of this exercise.
        ii. Hide the OSCOR display using the show/hide buttons (or click on the OSCOR window to hide it.)



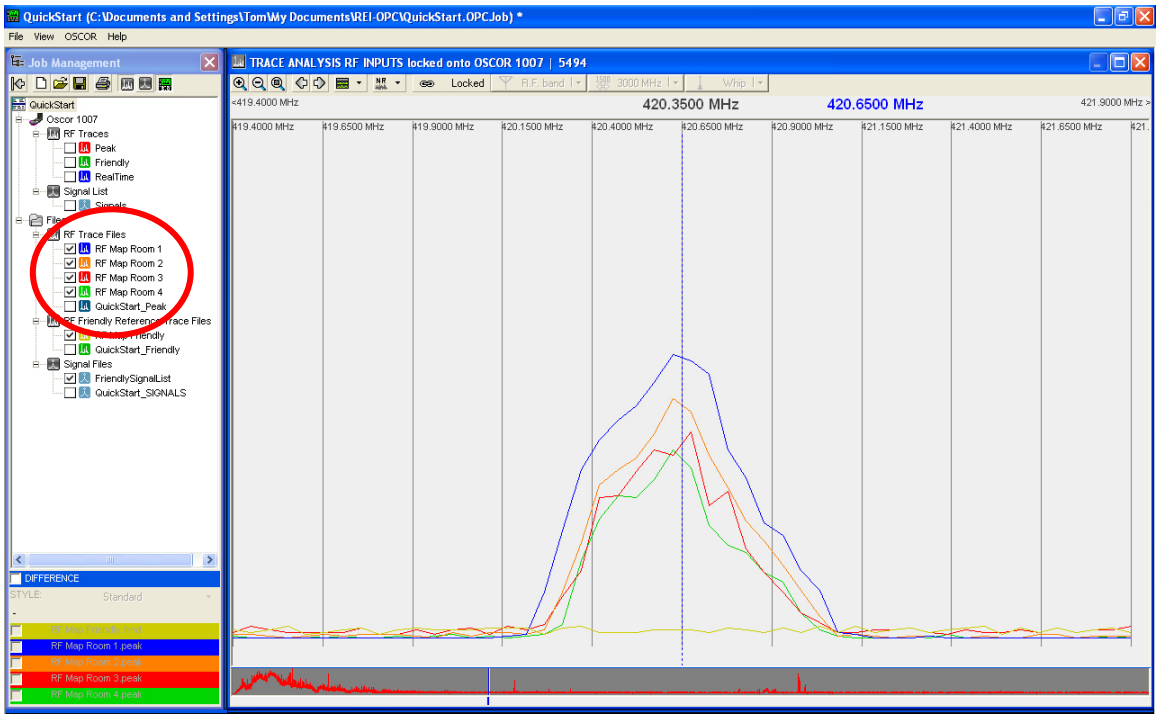
b. View Difference Spectrum of Peak minus Friendly
   i. Select a Room to use for first analysis (Room 1)
   ii. Un-select other rooms
   iii. Select Friendly trace to view
   iv. Select Difference Mode – You may need to click on Peak trace (Room 1) first and then the Friendly trace to ensure that it is Peak-Friendly and not Friendly-Peak.



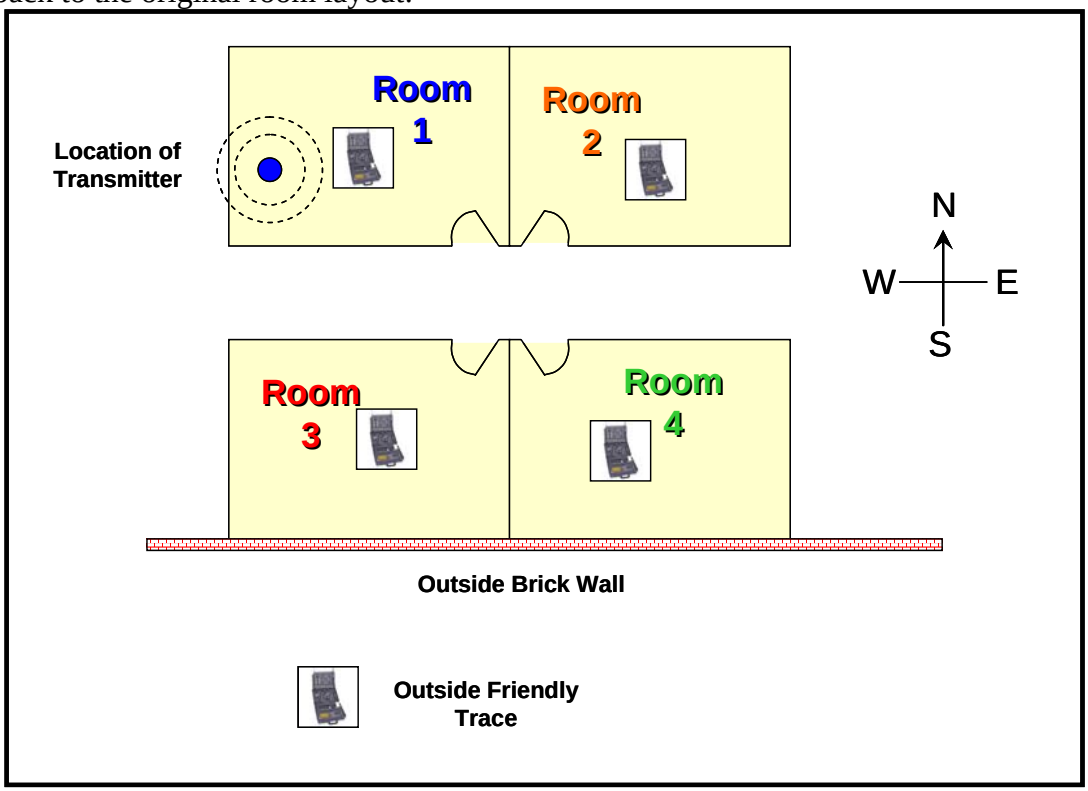


In this Difference view, it is easy to identify a Signal at 420MHz that indicates a large difference between the two traces. Also, this difference does not correspond to any stored friendly signals. Therefore, this signal should be analyzed.

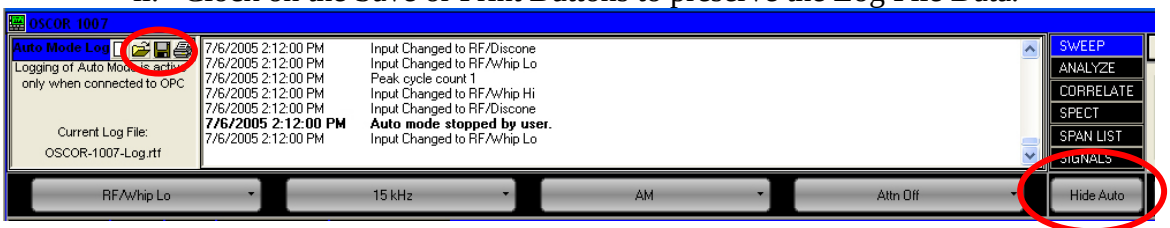
c. Zoom in to suspicious signals – Click and Drag across the signal of interest.
d. Change the number of display bands to a single band.
e. Turn off the Difference view.
f. Turn each of the Rooms View ON by clicking on the appropriate trace file box in the file tree.



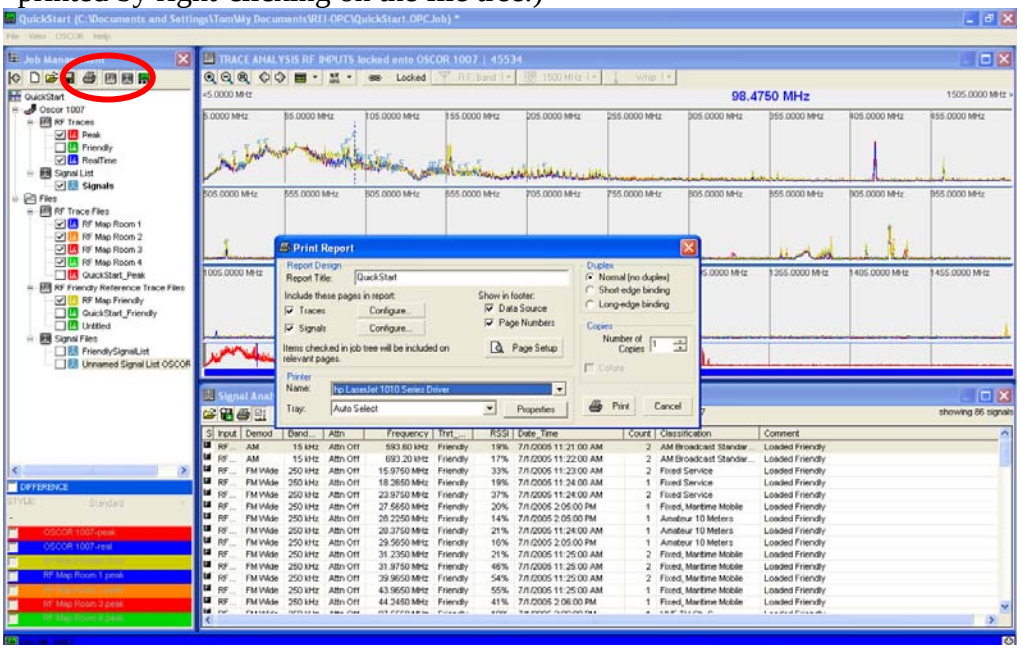
Referring back to the original room layout:



6. Analysis Observations:
   - This trace analysis clearly shows that the signal is strongest in Room 1 followed by Rooms 2, 3, & 4.
   - The transmitter is in Room 1 or is located in the North-West direction from Room 1. In this case, the transmitter could be found using the OSCOR RF locator probe in Room 1.
   - Room 2 appears to be about the same distance from the Transmitter as Room 3, but Room 2 only has 1 wall separating from the transmitter therefore, Room 2 has a stronger level than Room 3.
   - Room 4 is the furthest distance from the transmitter, however, the door alignment between the transmitter and the Room 4 OSCOR location is such that Room 4 signal level is almost as high as Room 3.
7. Print Reports
   a. Save the Log File
      i. Click on "Show Auto" (if the auto mode menus are hidden.)
      ii. Clock on the Save or Print Buttons to preserve the Log File Data.

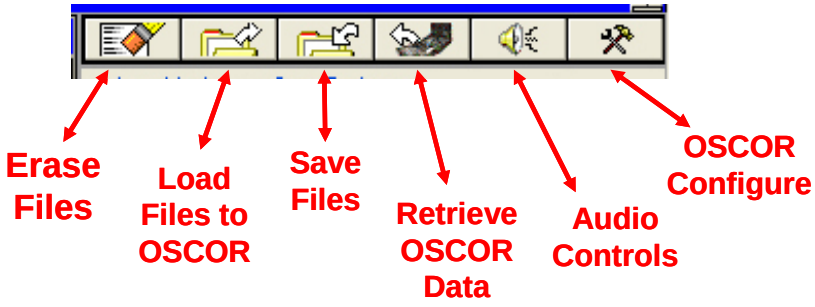


   b. Open the Signal Lists by pressing the Signal List Button (The signal lists must be displayed in the analysis window to be printed.
   c. Click on the Print Button to open the Print dialogue. (Note: Individual lists and files can be printed by right-clicking on the file tree.)



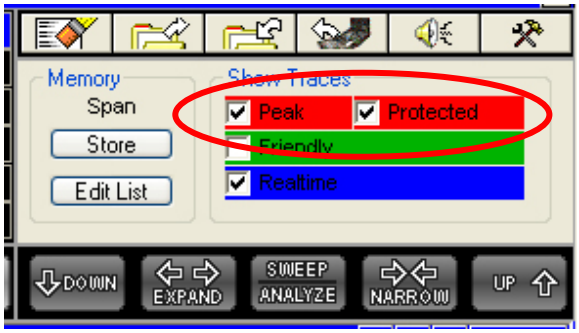
Some other useful OPC Functions

Data Control Functions – These buttons provide a quick method for controlling and transferring the data that is stored in the OSCOR or the PC as well as some additional controls.



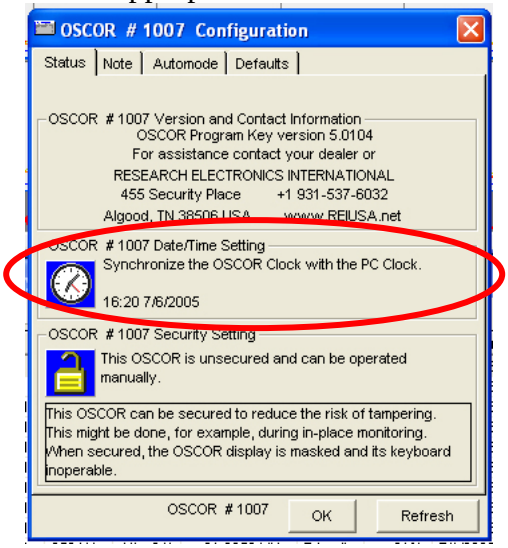
OSCOR Peak Protected Function

Whenever the "Peak Protected" is displayed in the OSCOR screen or checked in the OPC display as shown below, the Peak Trace mode is disabled. Whenever an Auto mode (Peak Trace Capture) is stopped, the Peak Data is automatically protected and not new data is added to Peak trace data. This function is built into the OPC/OSCOR normal operation to prevent the accident of moving the OSCOR to a new location before saving the peak data to file.



Update OSCOR Time Clock

Click on the Tool Button and click on the appropriate Functions of interest.



Recommended Consolidated RF Mapping Procedure

1. Setting up OPC to prepare for a sweep.
    a. Start OPC and Connect to OSCOR.
        i. Click on New Job
        ii. Label Job as desired
    b. Click on "Number of Bands to Show" and select 3, 4, or 5. This makes it easier to see the spectrum.
    c. Click on the Lock button to Lock the OPC to the OSCOR. This is not required, but recommended to minimize confusion between the OPC analysis screen and the OSCOR display screen.
    d. Turn on the bug in one of the rooms. (Room 1 for this example).
2. Loading and Saving Friendly Signals - Take the OSCOR outside of the building to Load Friendly.
    a. Start Load Friendly
        i. Click on "Show Auto" to open the Automatic Set-up
        ii. Select Load Friendly
        iii. Check Clean Start-Erase All
        iv. Collect Traces and Signals Only
        v. Click "Start" then "Yes" to proceed.
        vi. Stop Load Friendly after at least 1 Cycle has been completed.
        vii. Show the Signal List – Click on the "Show/Hide Signal List"
    b. Save Load Friendly Signals to file - Right-Click on OSCOR Signal List to "Save As".
    c. Classify Friendly Signals
        i. Click on the Frequency band information button.
        ii. Select the region of interest and select OK.
        iii. In the USA, you can select FCC to get further specific signal information.
    d. Hide Signal List
3. Loading and Saving Friendly Traces - Take the OSCOR outside of the building to Load Friendly.
    a. Loading Friendly Traces
        i. Click on "Show Auto"
        ii. Select Load Friendly
        iii. **Un**-Check Clean Start (You do not want to erase the previously saved Signal data, but if you have not previously loaded Friendly Signals you should Check Clean Start to make sure that you are not mixing data from another sweep.)
        iv. Select "Collect Traces Only"
        v. Click "Start" then "Yes" to proceed.
    b. Allow the OSCOR to Capture Data as long as possible. Click on "Stop Auto".
    c. Saving Trace Data to File – Right Click on OSCOR Friendly Trace to "Save As"
4. Capture Peak Trace Data in Rooms of Interest – Take OSCOR to each room and repeat steps:
    a. Capture Peak Trace Data of a Room
        i. Click on "Show Auto" to open the Automatic Set-up
        ii. Select "Auto Search
        iii. Check the "Clear Peak Trace"
        iv. Select "Collect Traces Only"
        v. Click "Start" then "Yes" to proceed.

vi. Allow the OSCOR to Capture Peak trace data for as long as possible or until at least 4 Cycles have been completed.
vii. Click on “Stop Auto”

b. Save Peak Trace for Room - Right click on the OSCOR Peak Trace File to “Save As”
c. Steps a and b, should be repeated in each room of interest.

5. Analyze Trace Data
    a. Prepare Analysis Display
        i. Right Click on each saved trace to specify a trace color if desired.
        ii. Hide the OSCOR display using the show/hide buttons if desired.
    b. View Difference Spectrum of Peak minus Friendly
        i. Select a Room to use for first analysis
        ii. Un-select other rooms
        iii. Select Friendly trace to view
        iv. Select Difference Mode – Select order of Difference Mode (Peak-Friendly)
    c. Zoom in to suspicious signals
    d. Change the number of display bands to a single band for single signal analysis
    e. Turn off the Difference view
    f. Turn each of the Rooms View ON
6. Analyze and Locate Signals of Interest
7. Print Reports
    a. Save the Log File
        i. Click on “Show Auto” (if the auto mode menus are hidden.)
        ii. Clock on the Save or Print Buttons to preserve the Log File Data.
    b. Open the Signal Lists by pressing the Signal List Button (Signal lists must be displayed in the analysis window to be printed.)
    c. Click on the Print Button to open the Print dialogue. (Note: Individual lists and files can be printed by right-clicking on the file tree.)