YELLOWJACKET-TABLET

802.11b/a/n/g Wi-Fi Spectrum Analyzer

manual version 1.7

Yellowjacket®-TABLET Interface Hardware user's manual

Yellowjacket®-TABLET/Yellowjacket®-TABLET Interface Hardware

Yellowjacket®-TABLET Interface Software user's manual

Be sure to disable the Wireless LAN Radio and the Bluetooth Transmitter on the Tablet PC to minimize interference with the Yellowjacket® Receiver before you establish a connection.

Unpacking Your Yellowjacket®-TABLET

Opening your box reveals Yellowjacket®-TABLET protective case, documentation box and monopole.

Documentation includes software (some products use CD-ROM while others use SD card installers), user's manual and claibration certificate and USB communication cable.

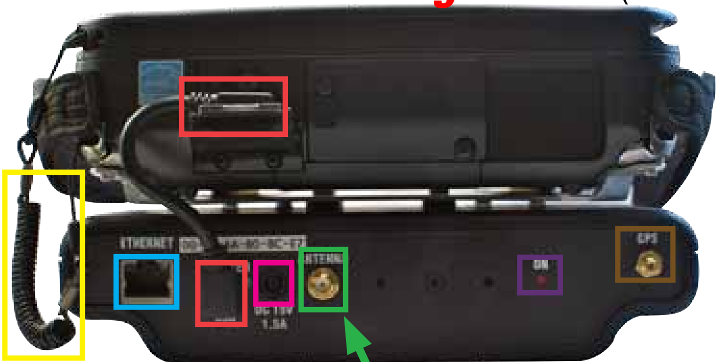
Unpack and assemble your Yellowjacket®-TABLET unit as shown. Your Yellowjacket®-TABLET is a self-contained spectrum analyzer. The user interface (Samsung Q1 UMPC Tablet), antenna and power connections are all accessible, but there is usually no need to open the protective, yellow and black hard rubber casing. The tablet should not be disconnected and removed nor batteries changed by users. Removing such components will void your hardware warranty. Please consult the included Samsung Q1 documentation for complete operating instructions, troubleshooting and tips of tablet PC. When you open your yellow, hard, protective case you will see the Yellowjacket®-TABLET unit with receiver hidden below it, included antennas, SD software loader card, receiver power/charging adapter, ethernet cable and GPS antenna. The required USB communication cable is located in the documentation box. After screwing the bottom plate onto the monopole, the Yellowjacket®-TABLET unit simply rests on the surface to alleviate the weight for the user.

BVS offers 2 different tablet models with your Yellowjacket system. The Panasonic Toughbook is a premium tablet option that includes a full 3 year warranty over the standard 1 year Samsung Q1 tablet warranty.

Yellowjacket Top View

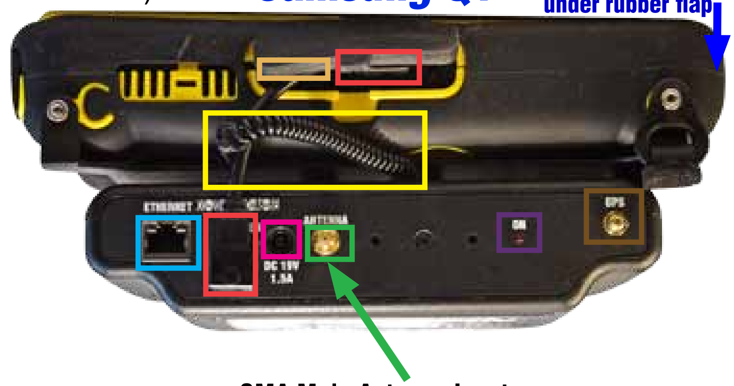
Panasonic Toughbook (both models shown) **Samsung Q1**

Power ON/OFF switch located under rubber flap



SMA Male Antenna Input

Warning: Maximum input 0 dBm NO DC Input



SMA Male Antenna Input

Warning: Maximum input 0 dBm NO DC Input

Center screw must be loosened fully (turn counterclockwise) before sliding tablet off of receiver.

About Yellowjacket®-TABLET

All basic ports and functions on the Samsung Q1 Tablet portion of your Yellowjacket-TABLET Wi-Fi Analzyer are explained in your Samsung Q1 user's manual included with your Yellowjacket unit. The Yellowjacket receiver contains all indicators and ports you need to communicate with the Q1 tablet. The receiver should not be removed from the tablet unless a BVS technical support expert has instructed you to do so. The ethernet 10/100 Mbit port is used to communicate with a PC. Be sure that the USB comm cable is securely connected between the Q1 tablet and Yellowjacket receiver. The SD card slot is located next to that for installing, removing or re-installing the Yellowjacket-TABLET software. The SMA male antenna connector is for use with the included omni directional antennas or the optional DF antenna systems. Please consult with Berkeley engineers before employing any antenna not supplied by BVS. The sylus can be found connected to the attached coil-cord which is attached to the bottom of the Q1 tablet. The unit also contains a GPS antenna input when GPS data is required for studies.

Powering Your Yellowjacket®-TABLET

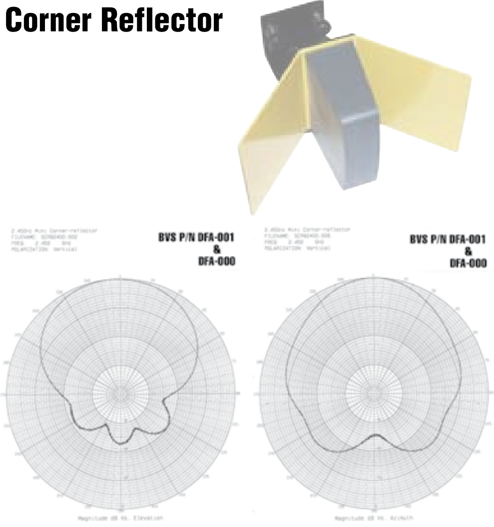
Powering up your Yellowjacket-TABLET begins by switching power on the Tablet PC. The **Power ON/OFF switch** is located on the side of the tablet PC under the rubber flap. Yellowjacket-TABLET Wi-Fi Analzyer contains an internal, rechargeable Li-Ion battery system in the receiver unit on the bottom. Users should not open the receiver unless a BVS technical support expert has instructed you to do so. The internal batteries are charged using the supplied DC power adapter connected to the power input. Consult the technical specifications sheet for common charging and running times for your unit. The red LED light next to this power input will blink while charging and go solid red when charging is complete. When your Yellowjacket-TABLET Wi-Fi Analzyer is charged, the Samsung Q1 tablet is powered on and the Yellowjacket-TABLET software is running, the red LED on the receiver (next to the GPS antenna input) will turn on. This indicates constant communication between the receiver and the tablet interface. NOTE: BVS recommends charging the unit every 2 weeks and at least once a month to avoid poor battery life.

Opening Your Yellowjacket®-TABLET

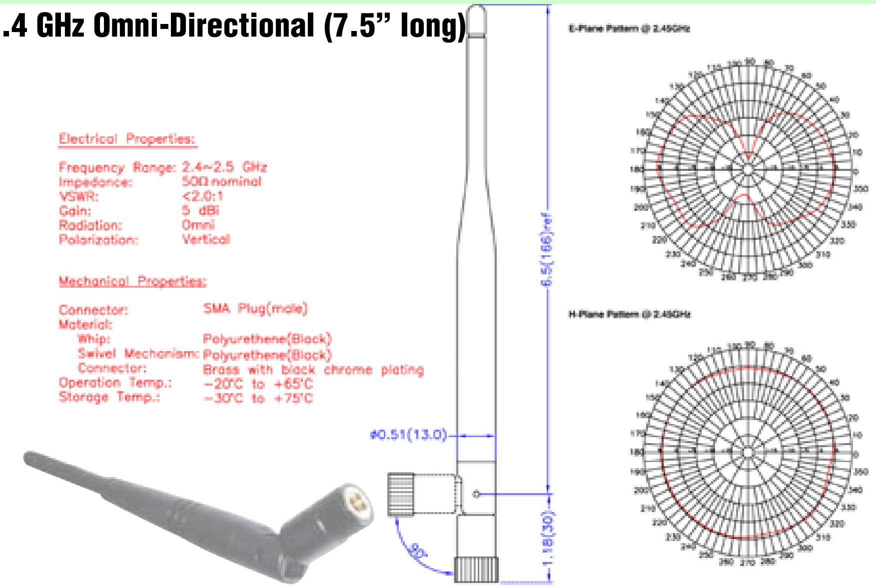
Always contact BVS technical support (1-888-737-4287 or +1 732-548-3737 8AM - 6PM EST or e-mail support@bvsystems.com) before attempting any modifications or repairs to your Yellowjacket-TABLET. In some cases, users may replace batteries or perform simple changes within the receiver module but failure to contact BVS technical support for procedural steps before proceeding will result in a VOIDED WARRANTY.

Optional Directional & Omni Antenna Specifications

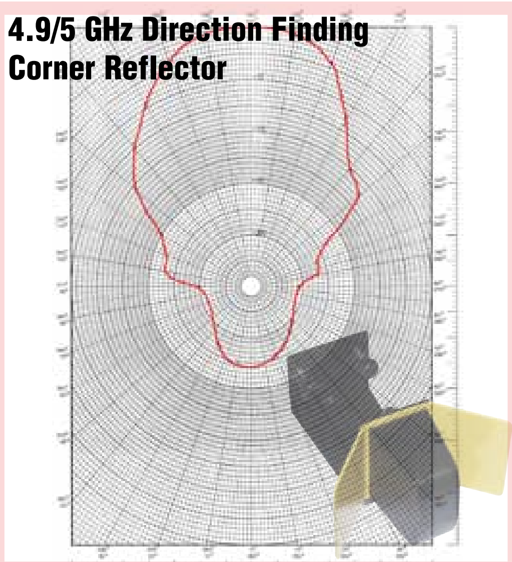
2.4 GHz Direction Finding Corner Reflector



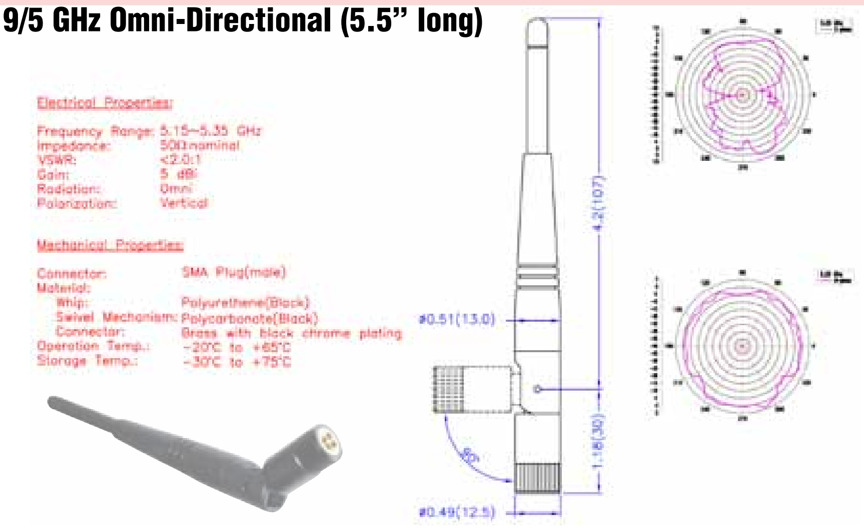
2.4 GHz Omni-Directional (7.5" long)



4.9/5 GHz Direction Finding Corner Reflector

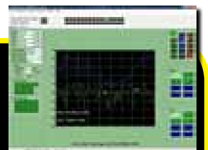


4.9/5 GHz Omni-Directional (5.5" long)



Accessories for your YELLOWJACKET-TABLET

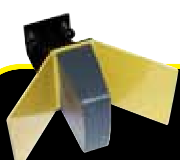
12VDC to 110VAC car cigarette lighter power inverter
75 Watts output
P/N YF-12V-USB
$ 75.00
OPTIONAL



Remote Manager
802.11b/a/n/g monitoring software
Ask for a Quote
OPTIONAL

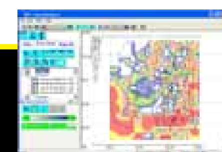
4.9/5 GHz Direction Finding Antenna with mounting bracket, cable & SMA male
9 dBi gain
P/N 5NE
$ 250.00
OPTIONAL

30 dB attenuator pad for use with directional antennas (between DF antenna & Yellowjacket®)
SMA male to female
P/N bbpad30
$ 30.00
OPTIONAL



2.4 GHz Direction Finding Antenna with mounting bracket, cable & SMA male
9 dBi gain
P/N 2ND
$ 250.00
OPTIONAL

Rugged Carrying Case
ABS Plastic
P/N P-CASE
$ 150.00
STANDARD



Swarm
802.11b/a/n/g mapping software
Ask for a Quote
OPTIONAL

2.4 GHz Omni Antenna
SMA male swivel
P/N S151AM-2450S
$ 25.00
STANDARD

3.5 GHz Omni Antenna
SMA male swivel
P/N 5NP
$ 25.00
STANDARD

4.9/5 GHz Omni Antenna
SMA male swivel
Co-Linear Dipole 5 dBi VSWR 1.8:1
P/N K181AM-5250S
$ 25.00
STANDARD

SWARM™

802.11b/a/n/g Wi-Fi Indoor/Outdoor Site Surveys

1 Create Survey Maps:
Swarm Projector (PC)

Import any bitmap for use in your Yellowjacket B/A/N/G

Create geo-coded site files for analysis

2 Constant Realtime Wi-Fi Surveys:
Swarm Collector (iPAQ)

Scan all 802.11 channels on BOTH 2.4 GHz and 5 GHz

JPEG snapshots of any survey screen

Collect survey data automatically via GPS

Collect data by manually tapping touch-screen

3 Coverage Reliability Analysis:
Swarm Analyzer (PC)

Plot surveys in multiple graphical and table views

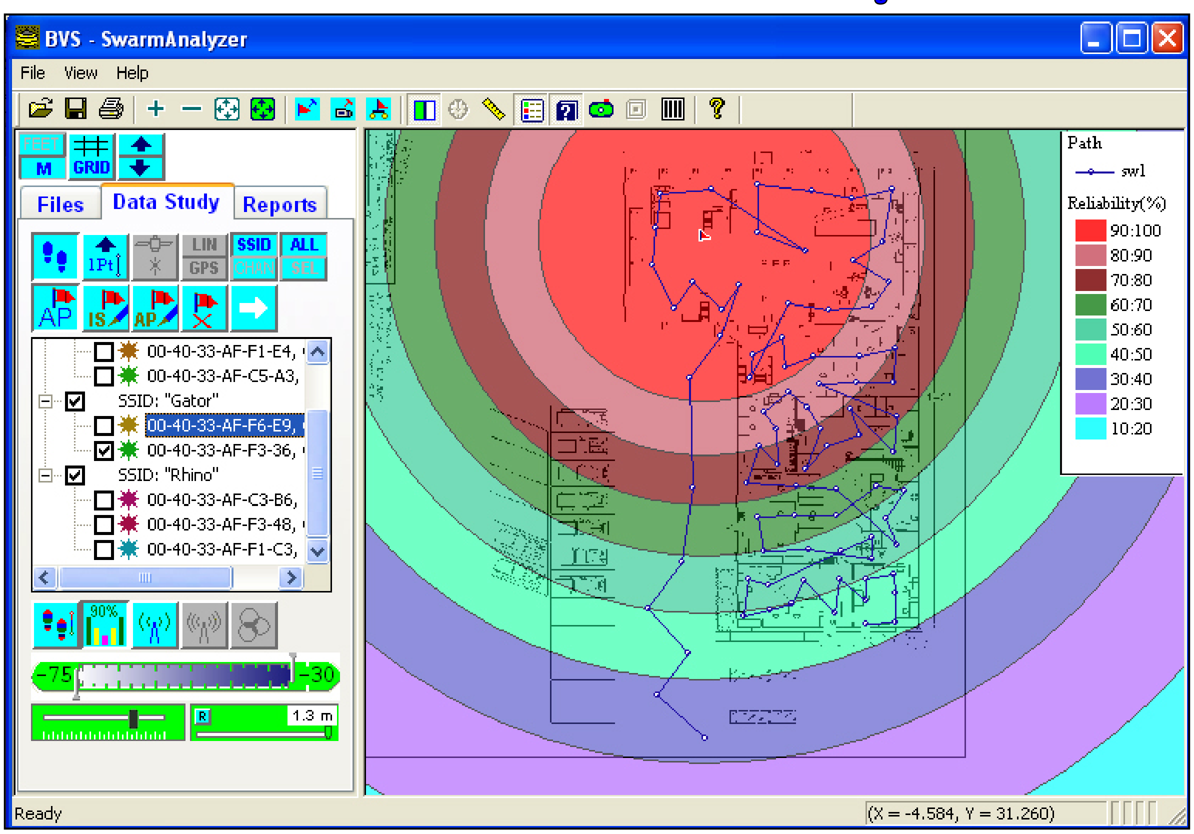
Plot coverage by APs or AP channels

Locate unknown APs' positions

Print and export plots into bmp files for spreadsheets

Create KML file for plotting coverage over Google Earth™

Swarm™ combines the power of realtime Yellowjacket® 802.11b/a/n/g Wi-Fi measurements with GPS geo-coding accuracy. First, create your survey bitmaps with both Linear and GPS **PROJECTOR** software. Next, simply walk or drive to any spot with GPS reception while ***Swarm™*** **COLLECTOR** scans all 802.11b/a/n/g channels and correlates them to your exact location automatically via GPS or manually by tapping on the touch-screen. GPS measurements provide both LAT and LON as well as time stamping for a complete Wi-Fi survey path anywhere in the world. ***Swarm™*** **COLLECTOR** allows JPEG screen snapshots to be taken at particular points of interest throughout the survey. Finally, survey data such as RSSI, MAC and SSID may be exported into ***Swarm's*** **ANALYZER** for further mapping coverage studies in multiple graphical and tabular layouts. In areas with little or no GPS reception, ***Swarm™*** **ANALYZER** only needs a few reference points to fill in the locations for the rest making it effective for quick outdoor studies. Surveys may be exported further into KML files for plotting in applications such as Google Earth™.



Features:

- Create survey bitmaps with BVS' Linear or GPS Projector software
- Collect data by using GPS position for outdoor surveys
- Collect data by manually tapping locations for indoor studies
- Choose any 802.11b/a/n/g Wi-Fi channels to scan
- JPEG screen snapshots may be taken throughout the survey
- Survey data such as RSSI, MAC and SSID is exported into Swarm Analyzer for further mapping cov erage studies in multiple graphical and spreadsheet layouts
- Surveys may be exported further into KML files for plotting in applications such as GoogleEarth™

Call us today for more information:
TOLL FREE 1-888-737-4287
Tel: +1 732-548-3737 Fax: (732) 548-3404
www.bvsystems.com email: sales@bvsystems.com

Berkeley Varitronics Systems®
Clarifying RF
Providing wireless solutions for over 35 years.

OPTIONAL SOFTWARE AVAILABLE FOR YOUR YELLOWJACKET-TABLET

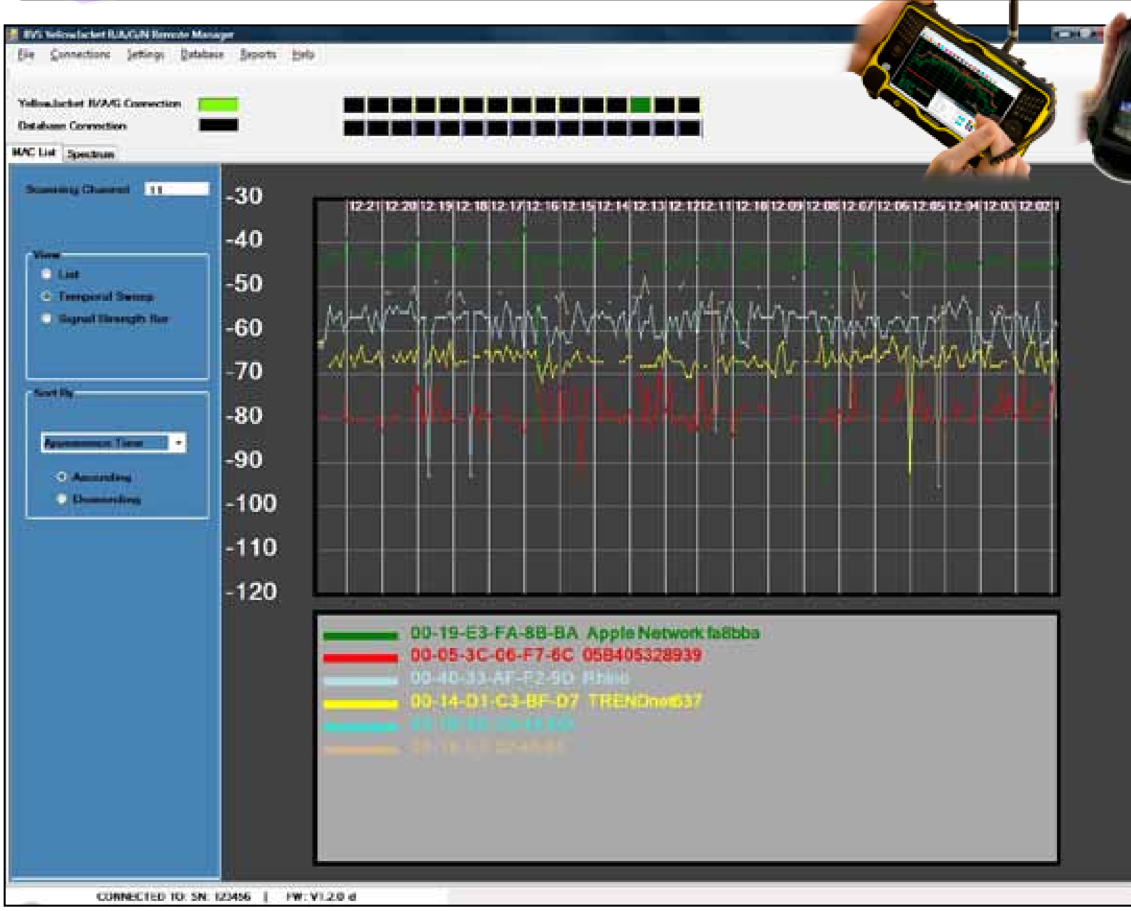
REMOTE MANAGER software

software for your

BEETLE-B/A/N/G
YELLOWJACKET® B/A/N/G

See EVERYTHING your Wi-Fi receiver sees...


802.11B/A/N/G REMOTE MONITORING SOFTWARE



MAC

SSID

Multipath

Power Triggers*

Waveform Traces*

Absolute Channel

Spectrum Analysis*

Peak Hold/Search*

Signal-to-Noise Ratios

*Yellowjacket support only

...from ANYWHERE

FEATURES

- Controls Yellowjacket B/A/N/G or Beetle-BANG remotely from any RJ-45 connection
- Monitor your network from anywhere - home and office.
- Data collected in real-time and stored in a relational database*
- Create comprehensive reports from your measured network data
- Export reports to PDF® and MS Excel® formats
- Collect spectrum data from the RF environment
- Collect packet data parameters such as MAC, SSID, Channel
- Data reports over various time periods for temporal overview of your network
- Software includes ethernet receiver dongle and cable

Remote Manager™ software is a data monitoring & reporting application that connects to any ***Yellowjacket® B/A/N/G or Beetle™-BANG*** through a standard 10/100 ethernet connection. With ***Remote Manager™***, users can control what wireless data is to be collected via the ***Yellowjacket®*** or ***Beetle™*** Wi-Fi receivers and store that data in a relational database* for future retrieval and analysis. ***Remote Manager™*** allows users to scan the RF spectrum (***Yellowjacket® B/A/N/G only)*** for packets and interference over time creating a network footprint of usage to find out who's in your network airspace with or without authorization. ***Remote Manager™*** even creates comprehensive PDF or MS Excel reports for an IT manager's overview. All of this can be accomplished from anywhere in the world; all you need is access to an ethernet connection to place your ***Yellowjacket®*** or ***Beetle™*** Wi-Fi receiver.

OPTIONAL SOFTWARE AVAILABLE FOR YOUR YELLOWJACKET-TABLET

After starting the program (double-click on the BVS Yellow Jacket BANG Tablet shortcut icon), the receiver unit Red LED will turn on, indicating the receiver is on, followed by the display of the main application window (Yellow Jacket TABLET B/A/N/G) and two other windows (Receiver Properties and Spectrum Analysis Options) as seen in Figure 1:

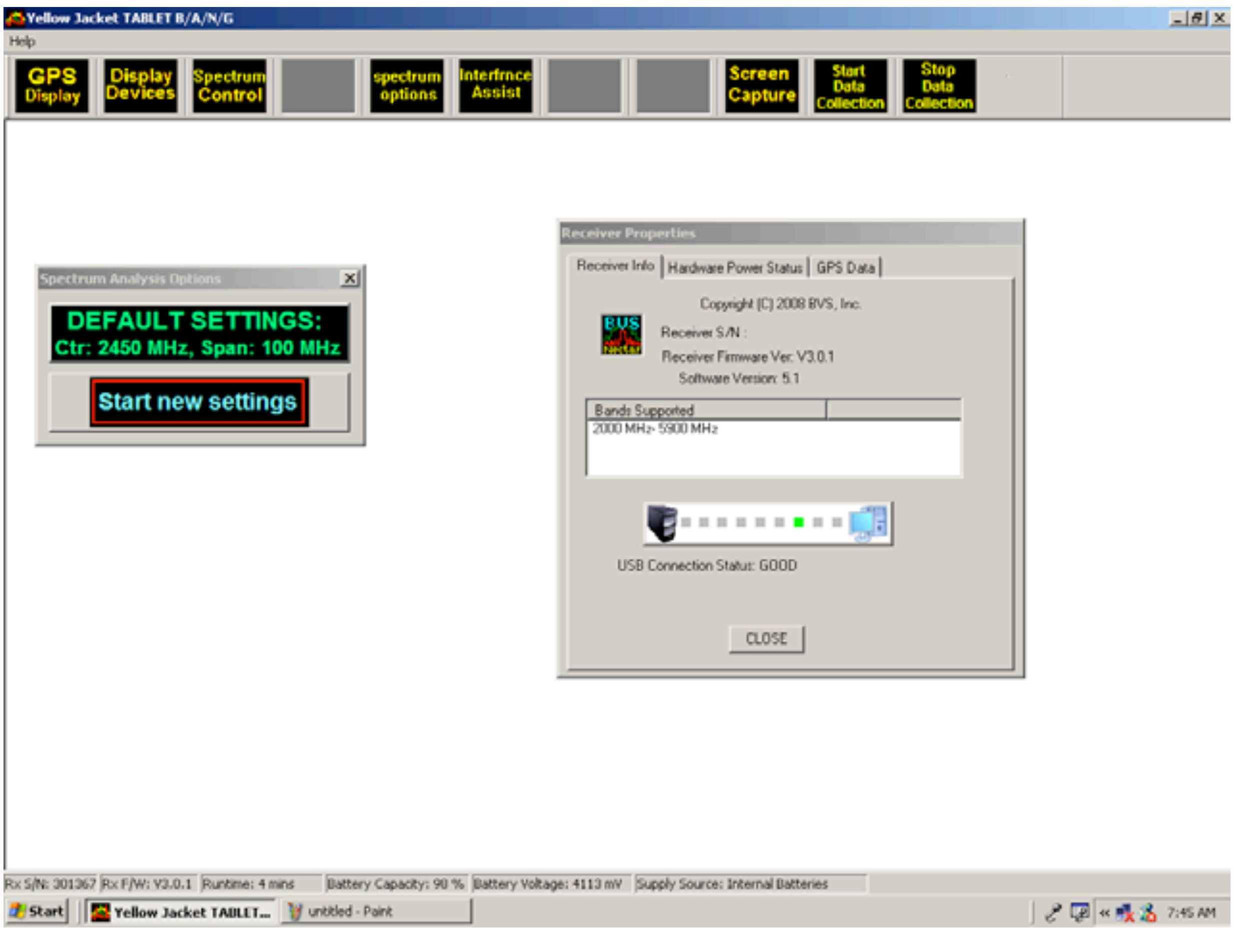


Figure 1. Main Application and Startup Windows

If the program is started without the USB jumper cable between the receiver unit and the tablet or the batteries in the receiver are discharged, an error message will be displayed upon starting the software (see item 7 under "Operating and Troubleshooting Notes" below).

The Receiver Properties window has three different tabs as follows:

Receiver Info

When this tab is pressed, receiver parameters such as Serial Number, firmware and software versions and Supported Bands are indicated as seen in Figure 2:

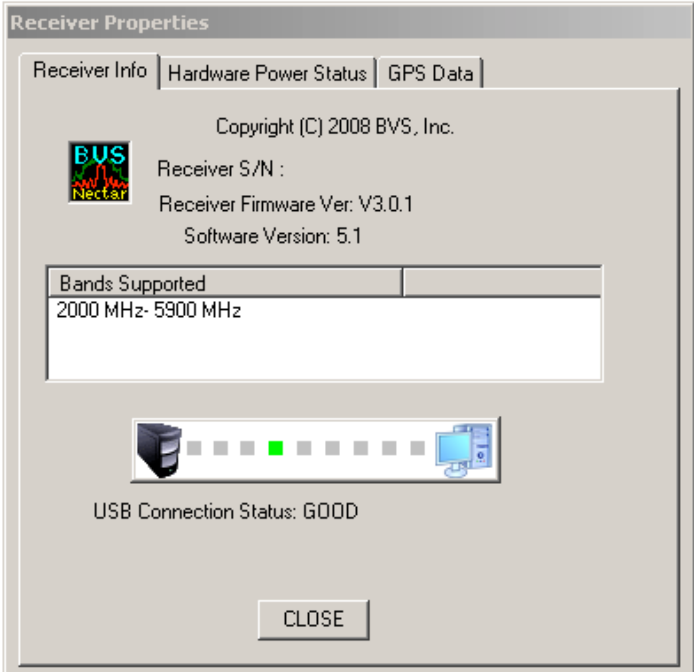


Figure 2. Receiver Info tab

Hardware Power Status

This tab will display the Power Supply status for the Yellow Jacket BANG receiver, as seen in Figure 3:

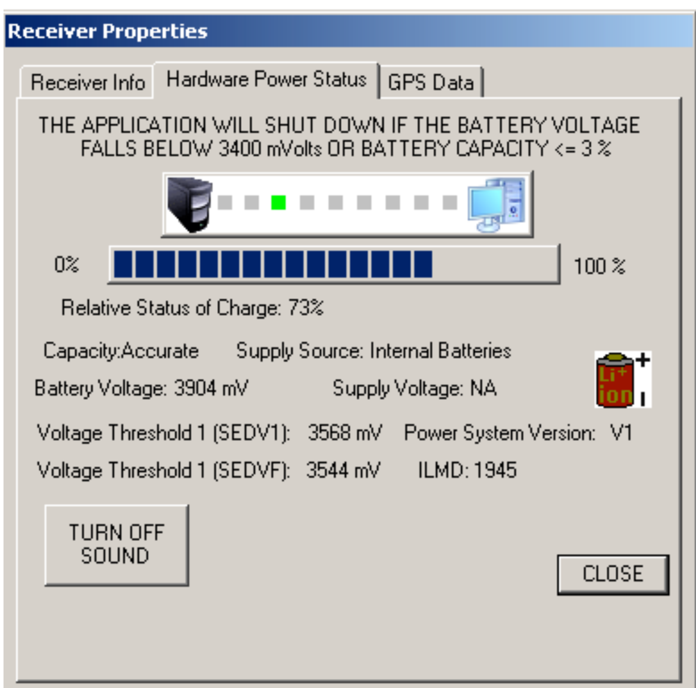


Figure 3. Hardware Power Status tab

IMPORTANT NOTE: If the Capacity field shows "Inaccurate", please contact BVS Technical Support: support@bvsystems.com OR 1-732-548-3737.

GPS Data
This tab will show relevant GPS information as seen in Figure 4:

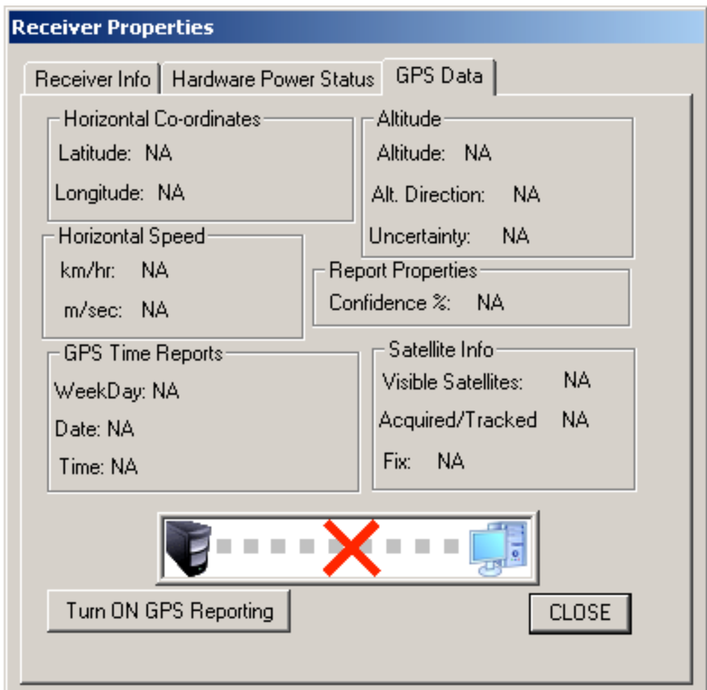


Figure 4. GPS Data tab

Closing the two windows (Receiver Properties and Spectrum Analysis Options) will allow the user to have full view of the main application window (Yellow Jacket TABLET B/A/N/G), as seen in Figure 5:

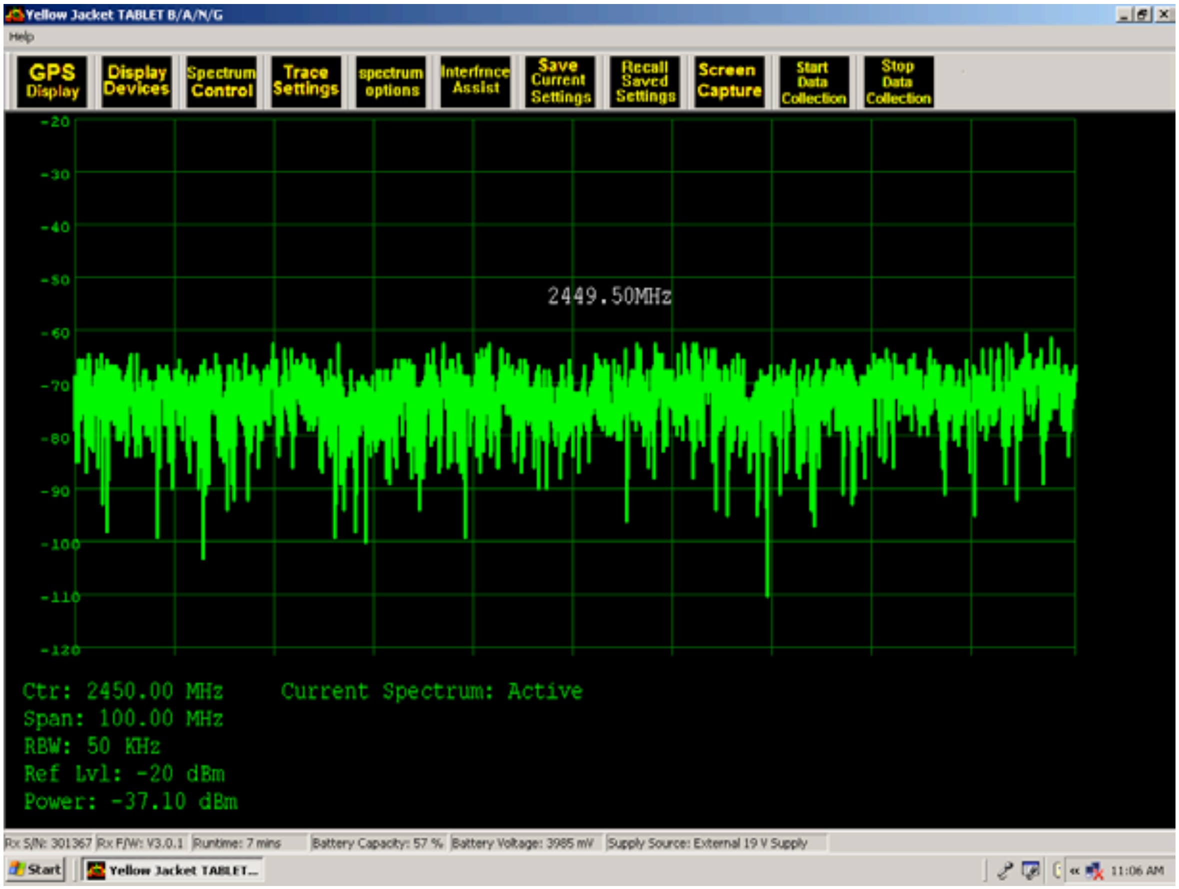


Figure 5. Spectrum Analysis window

This window will also be referred to as the "Spectrum Analysis" window throughout this manual.

Main Application Window Tool-Bar Button Functions:

The tool-bar in the main application window (see Figure 5) has eleven (11) soft-buttons. The functions of these buttons are as follows:

Clicking this button will display the GPS records as described above.

Pressing this button will result in a list of detected wireless devices as seen in Figure 6:

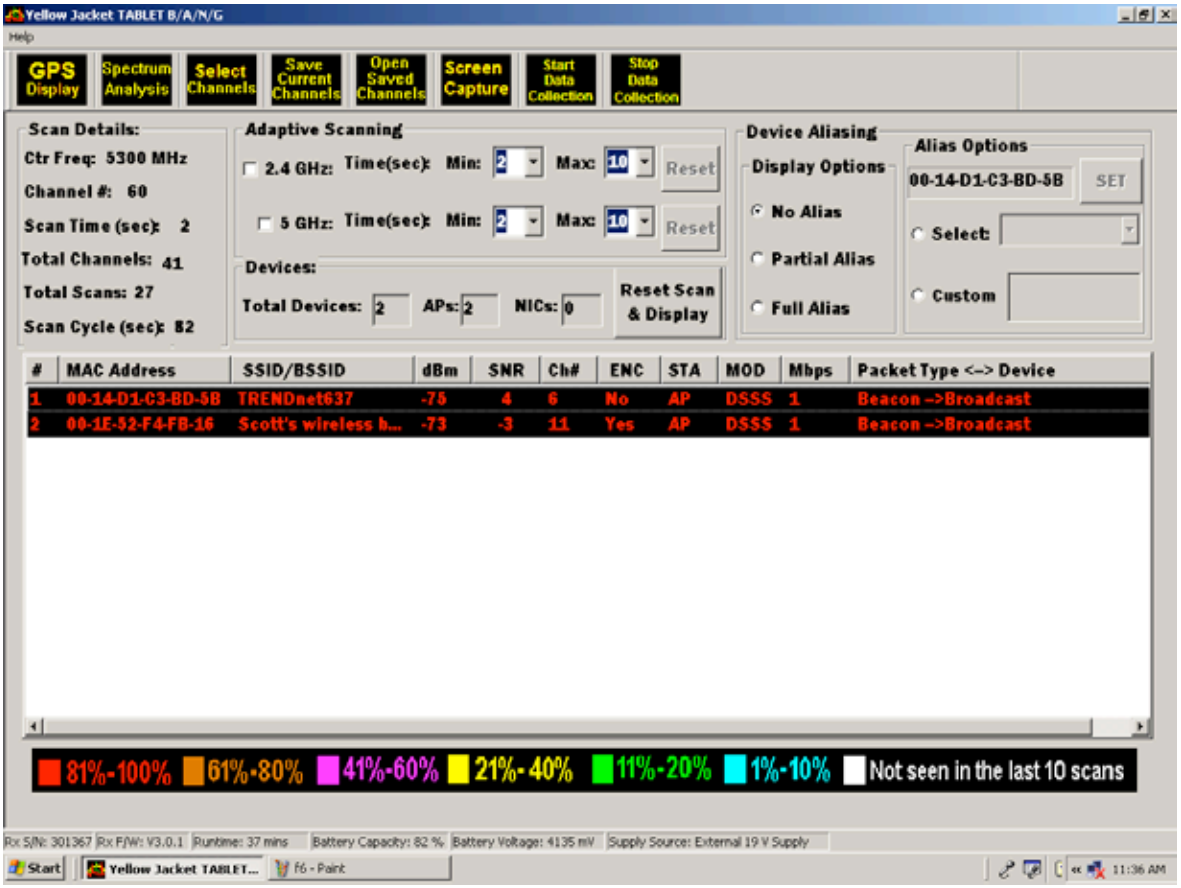


Figure 6. List of Detected Wireless Devices

The color of the wireless device entries in the list will change as a function of frequency of detection in time, according to the percentages seen at the bottom of Figure 6.

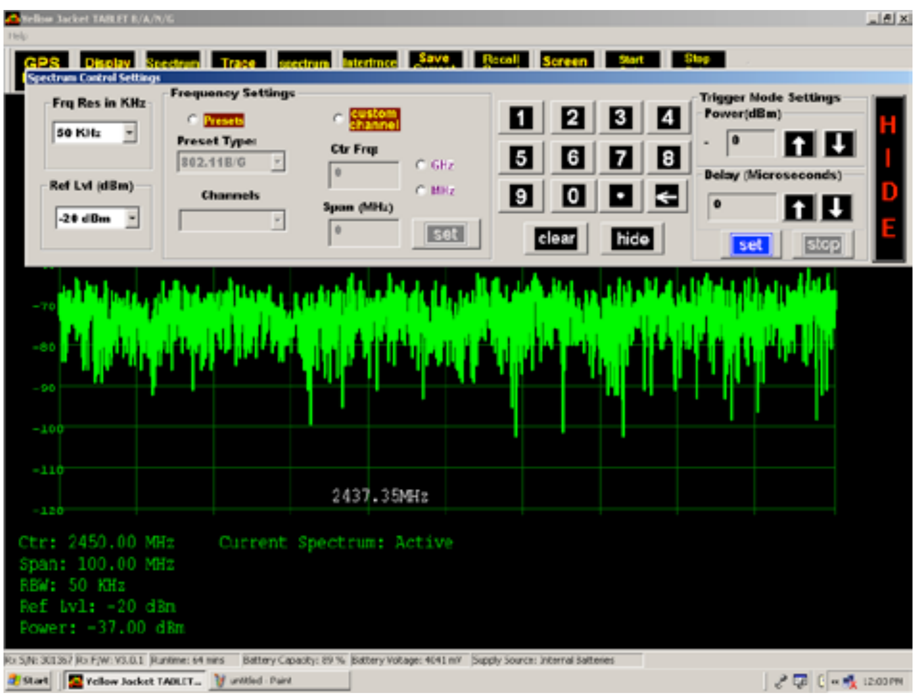


Figure 7. Spectrum Control Settings panel

In order to perform Spectrum Analysis on a specific wireless device, first select the device by a left-click, and then press the "Spectrum Analysis" button in Figure 6. This will return the user to the Spectrum Analysis application main window, with a "Spectrum Control Settings" panel as seen in Figure 7. To have full view of the main window tool-bar buttons left-click on the "HIDE" button in the spectrum control panel in Figure 7. More detailed discussions of the Detected Wireless Devices window will be given below in a section with the heading: "**MAC List View Detailed Discussion**".

Spectrum Control Settings: The frequency control panel pops up on clicking this button, as seen in Figure 7. This can be used to control spectrum settings in the Spectrum View. The Center Frequency, Span, Resolution Bandwidth, reference Level can be set using this panel. Trigger Mode settings can also be set using this panel. Left-click on "HIDE" to close the "Spectrum Control Settings" window.

Spectrum Trace Settings: This panel can be used for Peak-Hold, Setting Markers and Waveform Averaging in the Spectrum Analysis Mode.

Spectrum Options: The Spectrum Options allows the user to observe the Spectrogram or the Histogram of the current Spectrum. For in-depth discussions of these functions see the section entitled "Spectrogram Function" and "Histogram Function" below.

Interference Analyst: The Interference Analyst is very useful tool for users. Pressing this button displays an assortment of various waveforms of most commonly used digital modulation and transmission techniques in the 2.4 GHz and 5.8 GHz frequency bands, as seen in Figure 8 below.

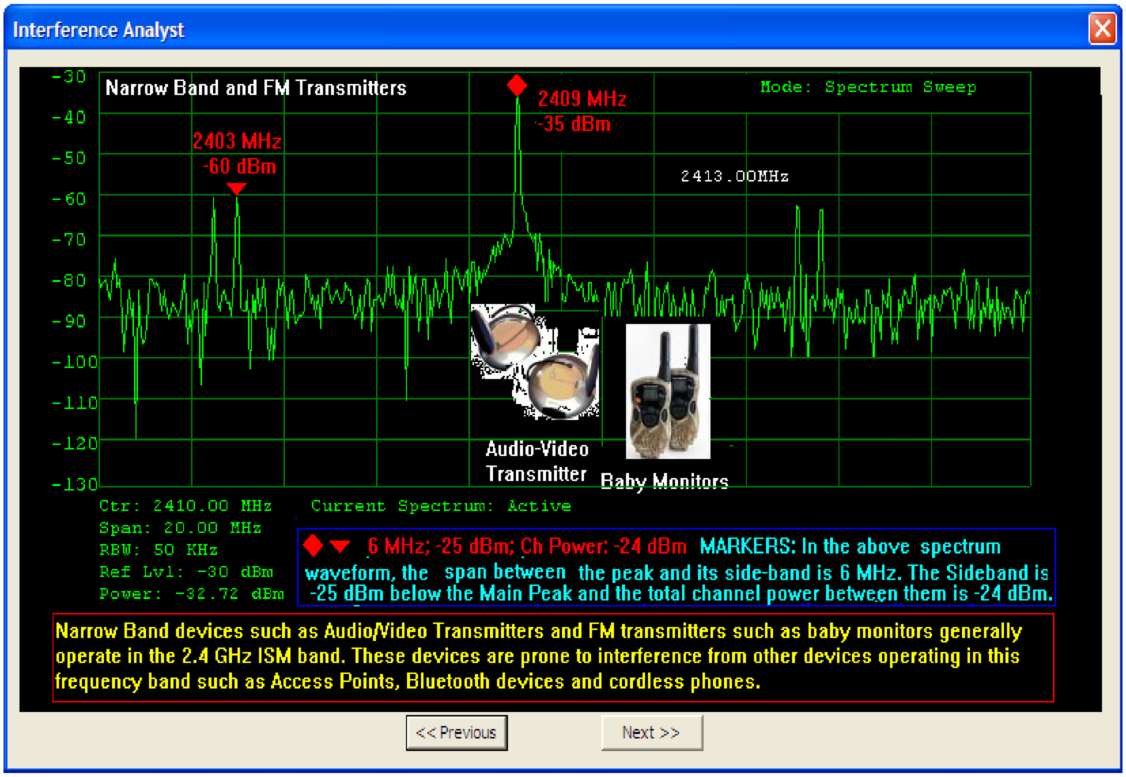
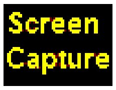


Figure 8. Interference Analyst Window

The Interference Analyst provides visual representation and description of waveforms of Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), and Microwave oven Power Leakage. It also provides visual images of what the Spectrum looks like when one transmission scheme interferes with another. The user can sequence by clicking the buttons "Previous" and "Next" as needed.

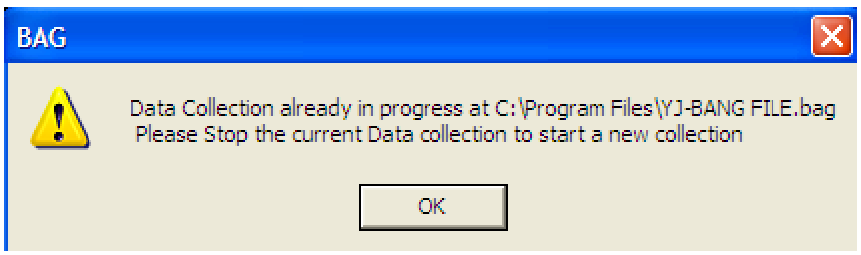
Create a User defined Spectrum Preset by saving a Spectrum Setting File: In the spectrum mode, the user can save the current spectrum settings to a file. Parameters such as Center Frequency, Span, Resolution Bandwidth, Reference Level, Trigger Power Threshold (If Trigger Mode is ON) are saved to a file location which can be invoked at a later instance by a single button click. The user is referred to the section entitled "Creating a User Defined Preset by Saving a Spectrum Context to a File" for further discussion.

Re-Open a saved Spectrum Setting File to trigger a User-defined Spectrum Preset: In the Spectrum Mode, Spectrum Settings previously saved can be invoked at this click on this button without making individual settings using the Frequency Control Dialog.



Snapshot: This button takes a snapshot of the current view within the application window. The snapshot can be saved either as a jpeg or a bmp at any location.

Data Collection: The raw data being obtained from the receiver and processed by the software can be collected to a binary file for further post processing using the Chameleon software which comes along with the product. If data collection is in progress, pressing this button will show the location of the file being collected currently, as follows:



Stop Data Collection: pressing this button will allow the user to start collecting new data.

Other Buttons

There are also other buttons which do not appear in the main application (or, Spectrum Analysis) window (Figure 5) but will appear only after the "**Display Devices**" button is pressed, as seen in Figure 6 above. These buttons are:

Spectrum Analysis: pressing this button will return the user to the main application window, i.e., Spectrum Analysis

This button is used to set the channels to be scanned in the Demodulation Mode to look for 802.11 a/b/g devices within the 2.4 GHz and 5 GHz bands. The scan time per channel can be set by the user for each channel. Alternately, scanning can be done adaptively to allow more scan time for a channel on which activity is detected and vice-versa. In the adaptive scanning mode, the receiver will vary the scan time per channel between a non-zero minimum and a maximum value. The channel scan time is incremented by one second every time any activity is detected on a channel and decremented by the same amount if no activity is seen during a particular scan. The minimum scan time is 2 sec and the maximum scan time is 10 seconds.

The current 2.4 GHz and 5 GHz channels being scanned can be saved to a file. These channels can then be selected for a future scan by just opening the same file.

This button will allow the user to point to the file where the channels are saved.

MAC List View Detailed Discussion

Clicking the "Display Devices" button will tabulate and show Wireless Device Information obtained as the receiver scans the selected channels, as seen in Figure 9:

#	MAC Address	SSID/BSSID	dBm	SNR	Ch#	ENC	STA	MOD	Mbps	Packet Type <-> Device
1	00-40-33-AF-F6-E9	Gator	-36	55	4	No	AP	DSSS	1	Beacon ->Broadcast
2	00-11-24-03-5B-D1	Apple Airport Expr...	-71	20	11	Yes	AP	DSSS	1	Beacon ->Broadcast
3	00-05-5D-26-12-8B	BVS802.11A	-42	49	64*	No	AP	OFD...	6	Beacon ->Broadcast
4	00-05-3C-06-F7-6C	05B405328939	-74	-6	7*		NIC	DSSS	11	Probe Rq ->Broadcast
5	00-1B-9E-83-11-E3	Gator	-33	42	11*		NIC	DSSS	1	Probe Rq ->Broadcast
6	00-14-D1-C3-BD-5B	TRENDnet637	-60	5	6	No	AP	DSSS	1	Beacon ->Broadcast
7	00-1B-9E-A7-3A-29	TRENDnet637	-57	38	9*		NIC	DSSS	1	Probe Rsp<-00-1E-52-F4-FB-16
8	00-1E-52-F4-FB-16	Scott's wireless b...	-58	-9	1	Yes	AP	DSSS	1	Beacon ->Broadcast

Figure 9. MAC List for Detected Devices

The entries in the device list are color-coded according to their frequency of detection. The last column in the list displays the 802.11 MAC packet being transmitted or received by the detected device and the transmitter/recipient of that packet.

MAC address Aliasing: The MAC address in the device list can be aliased to a more convenient name for the device for ease of identification. This helps to identify the device in the list without knowing the MAC addresses of all the devices in the list every time. In order to do so, left-click the MAC Address in the list once and observe entries under "Device Aliasing" in the upper right-hand quadrant of the Detected

Wireless Devices window in Figure 6 above, and either select a generic alias from "Select" field or enter a custom alias from the "Custom" field to name the device, as shown in Figures 10 and 11 below:

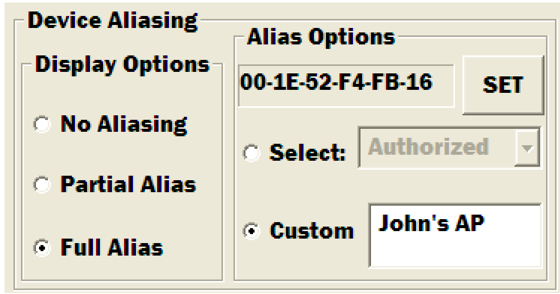


Figure 10. "Device Aliasing" panel in Detected Wireless Devices Window

Click the "Set" button to assign the alias name to the selected MAC address. Depending upon the Alias display settings, either a "Full" or a "Partial Alias" will be displayed in the list in place of the entire MAC address, as seen in the leftmost column in Figure 11:

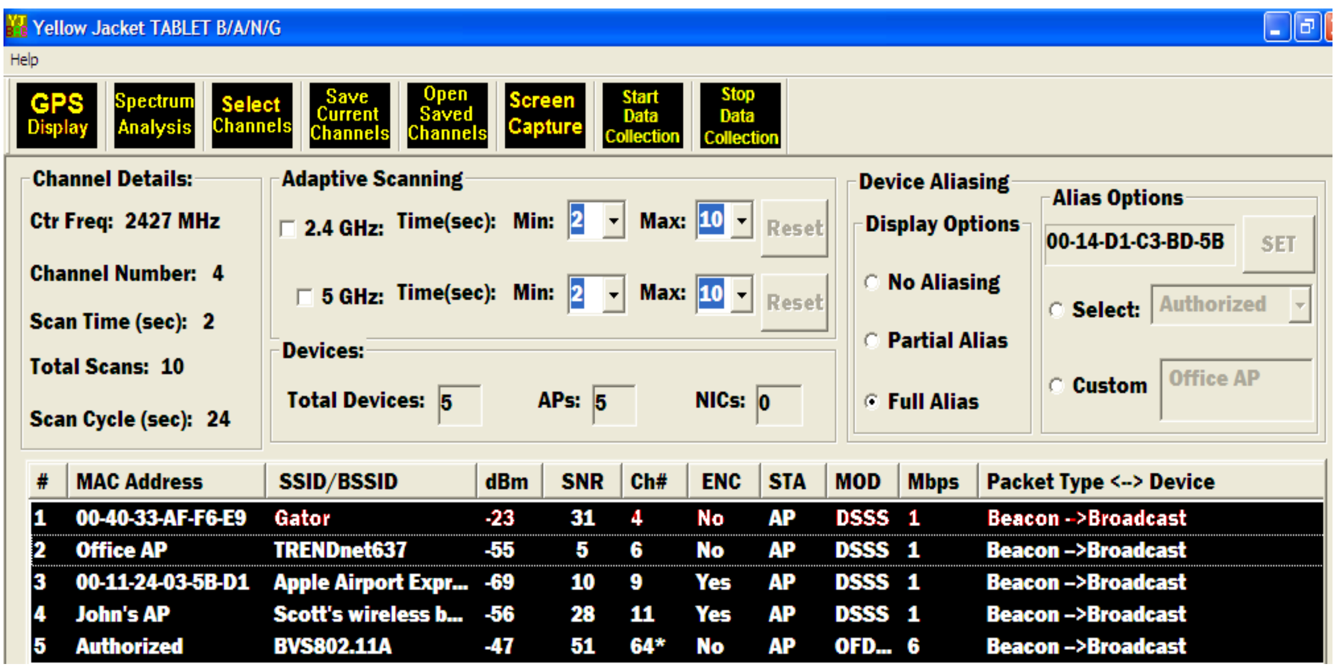


Figure 11. Custom Aliasing of Detected Devices

Full Alias will display the selected alias name in place of the entire MAC Address, as seen in Figure 11.

Partial Alias will display the selected alias name and the last six characters of the MAC address. For any MAC address, the first six characters generally indicate the manufacturer of the radio device (Access Point, Network interface card etc) and the last six characters are unique for every radio device. For example, given a MAC Address "00-40-33-AF-F6-E9", the first six characters "00-40-33" indicate the vendor which manufactured the radio device and the remaining characters "AF-F6-E9" is unique to every device.

Adaptive Scanning: This method of scanning allows for intelligent scanning of channels. See upper center panel entitled “Adaptive Scanning” in Figure 11 above. When Adaptive Scanning is enabled, the receiver will “dwell” on a channel with wireless activity for a longer period of time than a channel with lesser or no activity. The dwell time on a particular channel varies between a user settable minimum value and a maximum value. When the unit observes wireless traffic on a channel during a scan, the software will increase the receiver dwell time on that channel by a second if it is less than the maximum dwell time. If no traffic is detected, the dwell time is reduced by 1 second if it is greater than the minimum dwell time. This way, the receiver dwells on a channel with wireless traffic longer than a channel with no wireless traffic.

Single-Mac Mode of Operation

The receiver can be made to monitor a number of parameters and conditions associated with a single detected wireless device. Doing so will interrupt the dynamic scanning of all channels and the receiver will monitor only the channel of the device of interest. When operating in this mode, the receiver can be set to monitor any one of the following eight single-MAC functions:

1. MULTIPATH DISPLAY (multiple reflections)
2. DELAY SPREAD (due to multiple reflections)
3. ANTENNA ALIGNMENT
4. TRAFFIC ANALYSIS
5. RSSI vs. TIME
6. security information
7. Greenfield Capabilities
8. 802.11N PHY Capabilities

Pressing the “RETURN TO SCAN” button will return the user to the Display Devices window (Figure 6 or 11 above). The above Single-MAC functions are initiated by selecting the corresponding soft buttons seen in Figure 12:

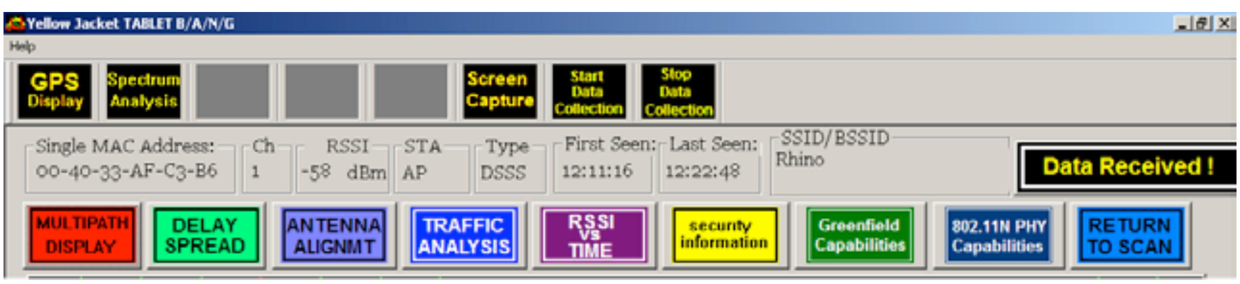
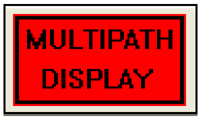


Figure 12. Single-MAC Function Window Initiated

Doing so will, by default, set the receiver to perform the first function, namely MULTIPATH DISPLAY for the selected wireless device (see Figure 12 below). Once the receiver enters this mode, any of the 8 functions (including MULTIPATH DISPLAY) may be initiated or re-set by left-clicking the corresponding button in the lower toolbar in the window seen in Figure 12. Each of the soft buttons (different colors); associated windows and functions are discussed next:



Multipath Display: Is initiated either by left-double clicking a device in the Display Wireless Devices window MAC Address list (from Figure 6 or 11) or by left-clicking the "MULTIPATH DISPLAY" button in Figure 12. Doing so will initiate this function for the previously selected device as seen in the window in Figure 13:

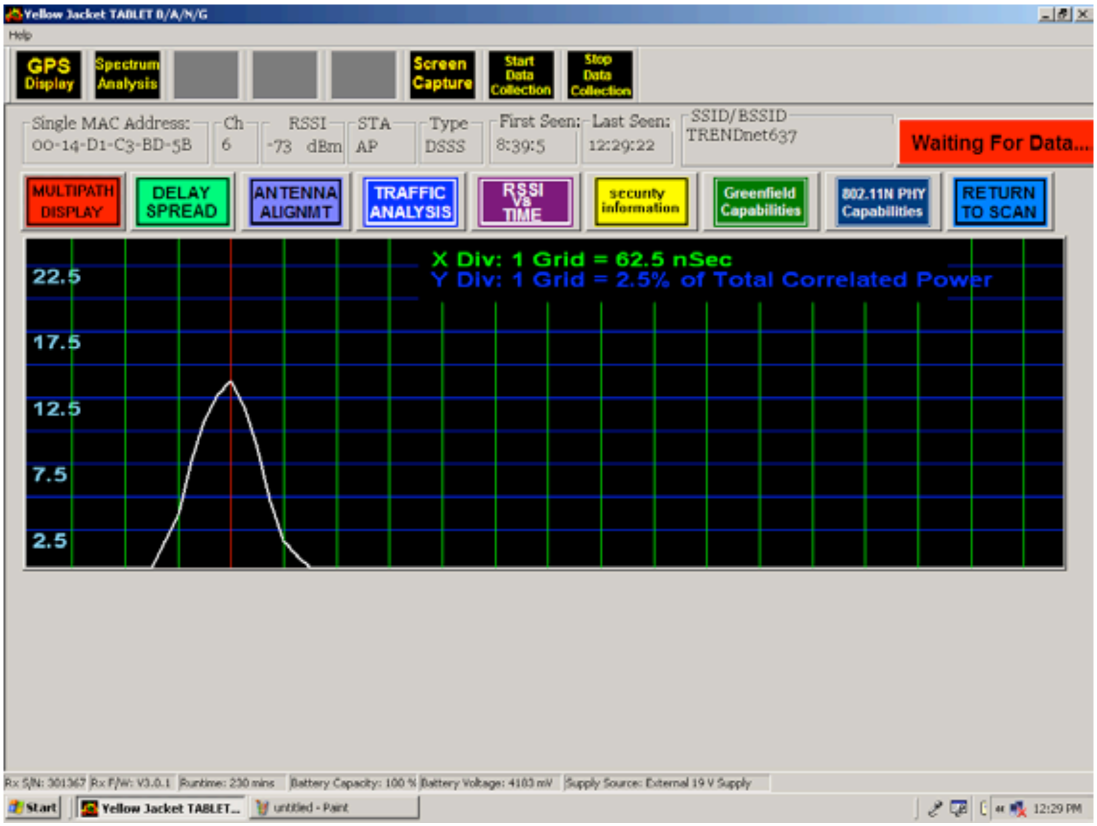
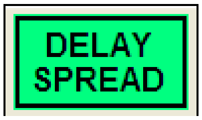


Figure 13. Multipath Display function window re-set

The Multipath Display shows the percentage correlation power of the different multipath components (multiple reflections of the same RF signal). Typically, if multipath interference is less, the received direct line of sight wave has the maximum power indicated by the peak (Figure 13 corresponds to no significant reflected paths). If most of the reflected power is in one reflection path only, the display would indicate two humps, namely line-of-sight and one reflected paths.



Delay Spread: This function shows the instantaneous Multipath Delay spread. The color of the instantaneous Multipath Delay Spread bar is displayed in terms of the color gradient shown. The display also shows the Peak (maximum) and Minimum Delay Spread due to Multipath, as seen in Figure 14:

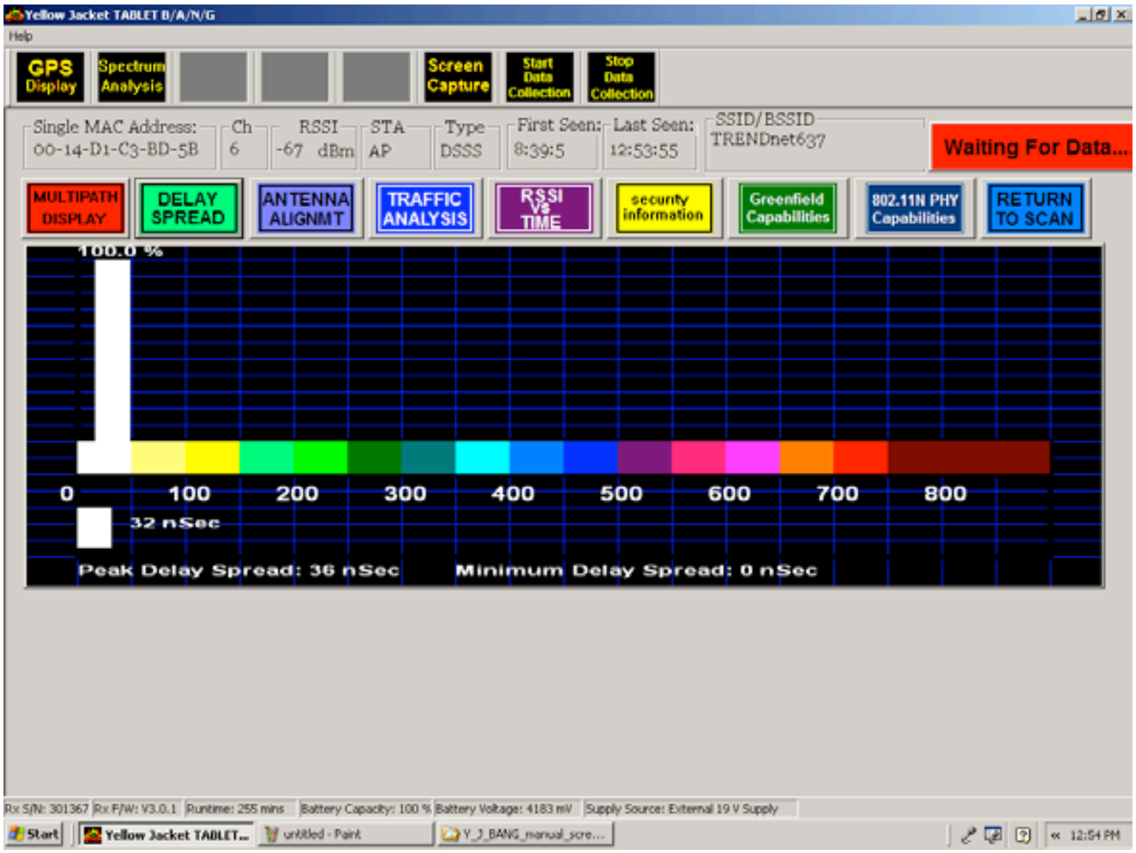
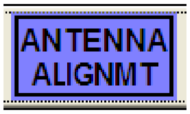


Figure 14. Delay Spread function window



Antenna Alignment: The antenna alignment screen displays the percent distribution of observed values of the Received Signal Strength Indicator (RSSI) as a function of signal strength in real time. The color of the RSSI distribution components indicate signal strength according to the color code seen in Figure 15. This function allows the user to identify and physically locate sources with a specific MAC address. More on this subject is discussed below in a section entitled "Direction Finding Antenna Use in Single-MAC Mode of Operation".

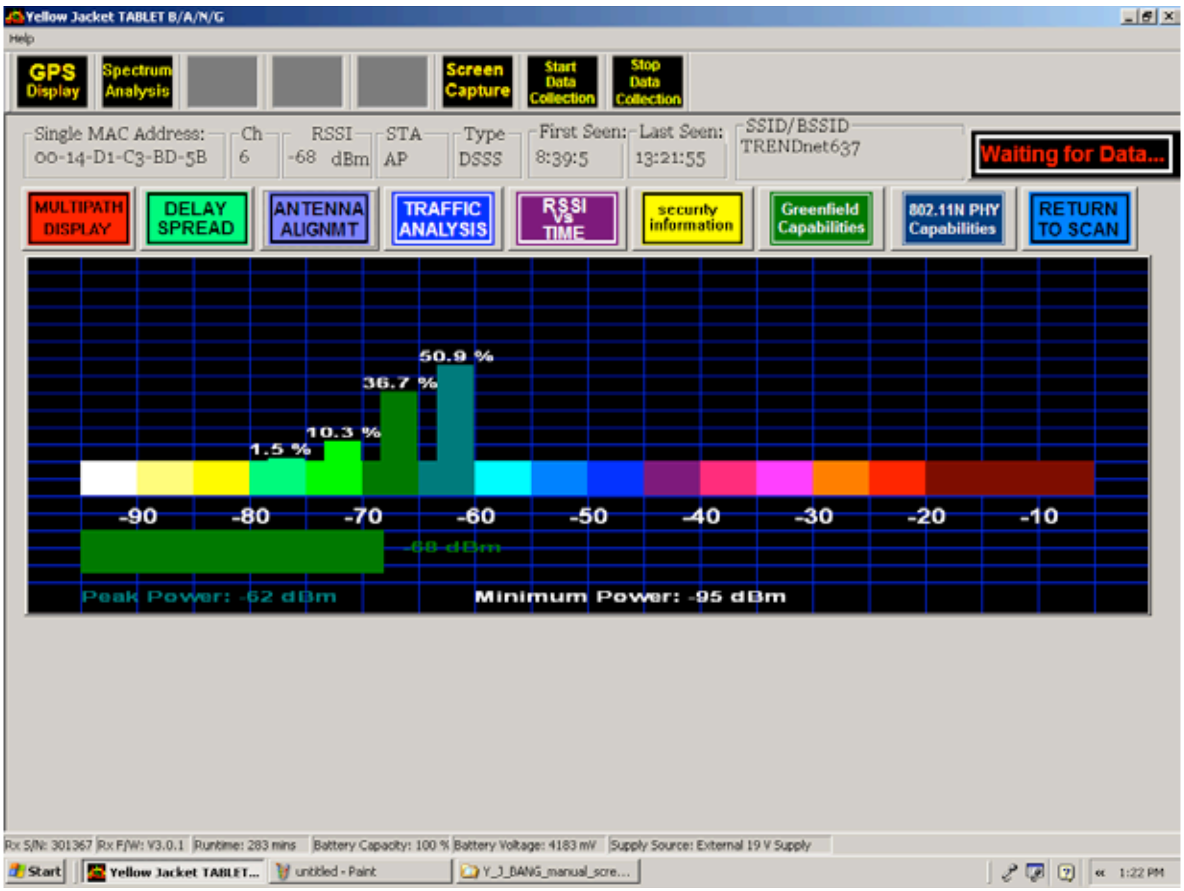
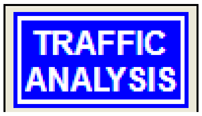


Figure 15. Antenna Alignment function window



Traffic Analysis: The Traffic Analysis Screen (see Figure 16 below) shows the relative distribution of the transmitted and received packets by the selected device in the MAC address list in the Detected Wireless Devices screen (see Figure 6 or 11 above).

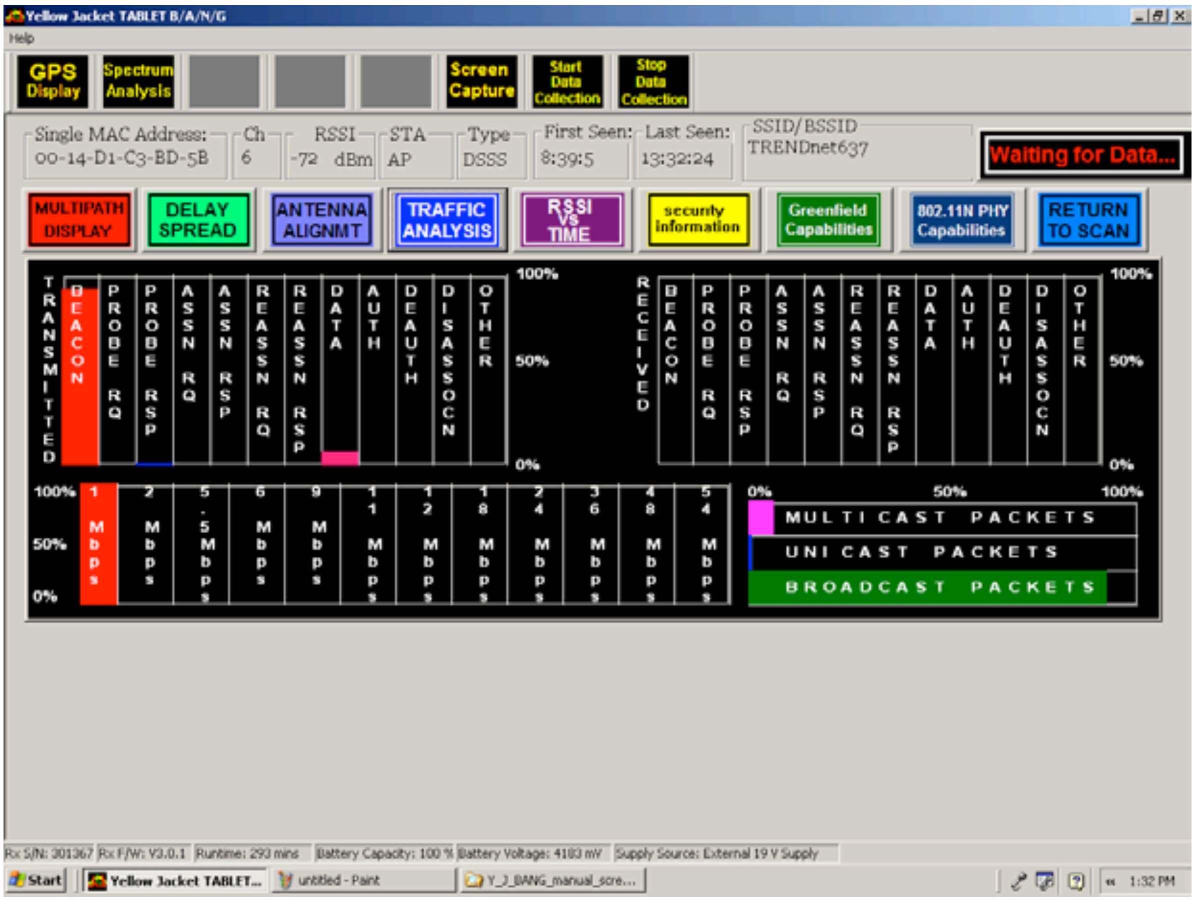


Figure 16. Traffic Analysis function window

Direction Finding: The Direction Finding screen (see Figure 17) displays the past instances, as a histogram, of the Received Signal Strength Indicator (RSSI) for the last 34 reports. With the help of a direction finding antenna, this can be helpful in identifying the location of a wireless transmitter in the 2.4 GHz and 5 GHz frequency bands by locking the Direction Finding antenna in the direction of the signal which is consistently strong over a period of time. The display can be reset by clicking the same button again.

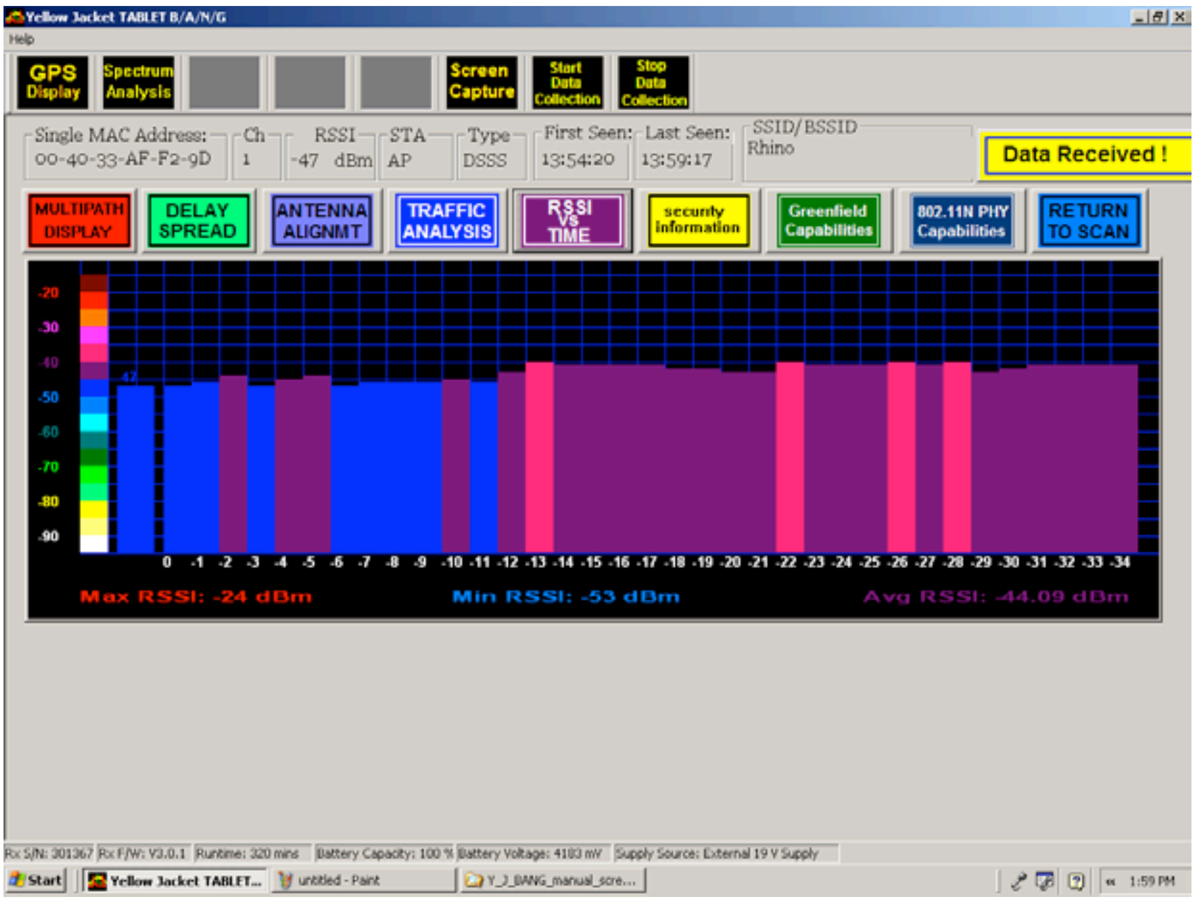
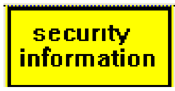


Figure 17. RSSI vs. TIME function window



Security information: Left clicking the corresponding button will display the security attributes of the selected wireless device, as seen in Figure 18:

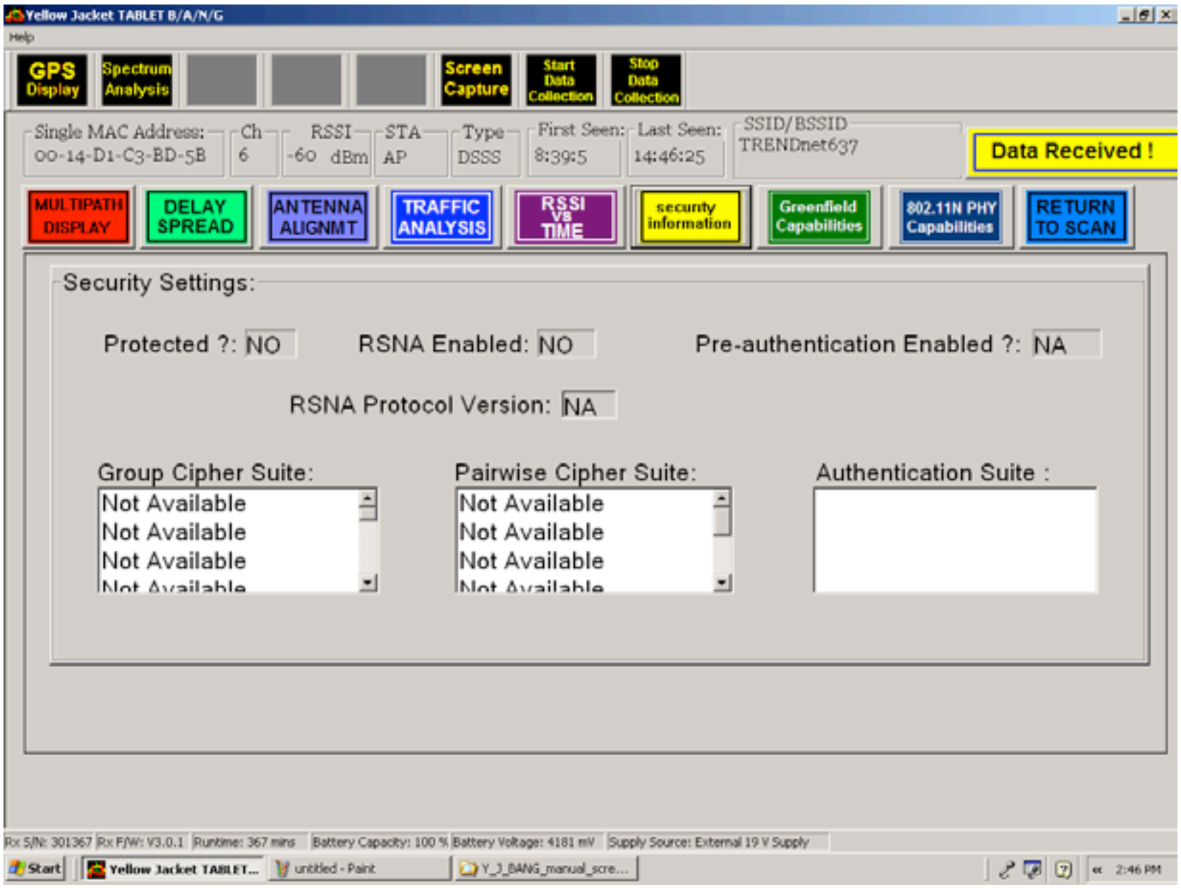


Figure 18. Security Information function window

As an example, consider the attribute settings displayed in Figure 19 below:

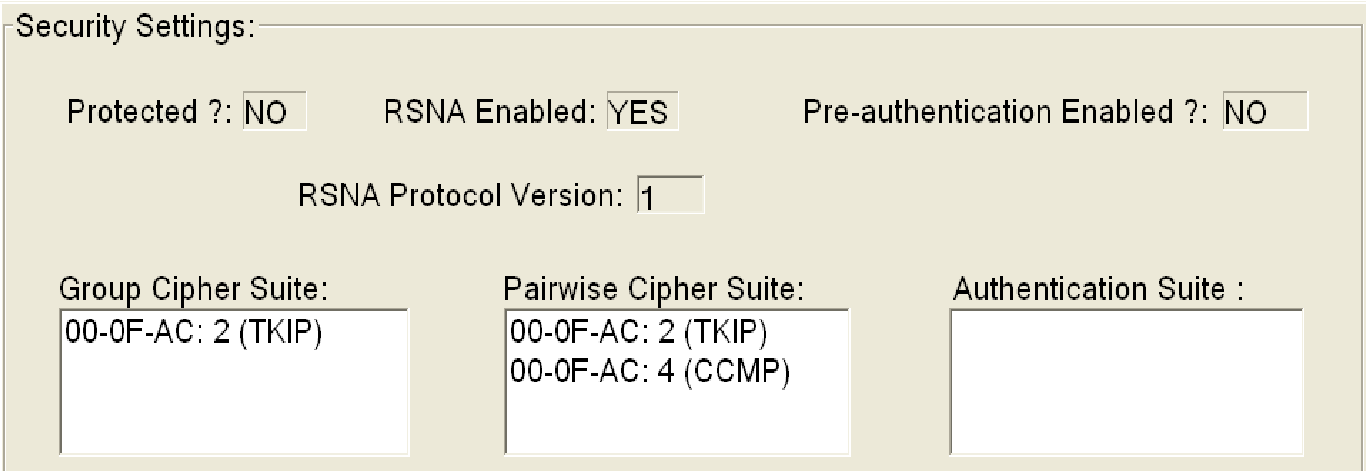


Figure 19. Security Settings

Protected ?: [YES/NO]: indicates if the transmissions from this device will be protected using some secure encryption scheme.

RSNA Enabled: [YES/NO]: indicates if RSNA has been enabled for this device.

Pre-authentication enabled: [YES/NO]: indicates if Preauthentication is enabled for this device.

RSNA Protocol version: indicates the RSNA protocol version currently being used by the device.

Group Cipher Suite: provides information of the Group Cipher suite being used.

Pairwise Cipher Suite: provides information of the Pairwise Cipher suite being used.

Authentication Suite: provides information of the Authentication suite being used.

Greenfield Capabilities: This screen analyzes and displays the Greenfield capabilities of an IEEE 802.11 N draft specification 2.0 compliant device. A sample of this window appears in Figure 20:

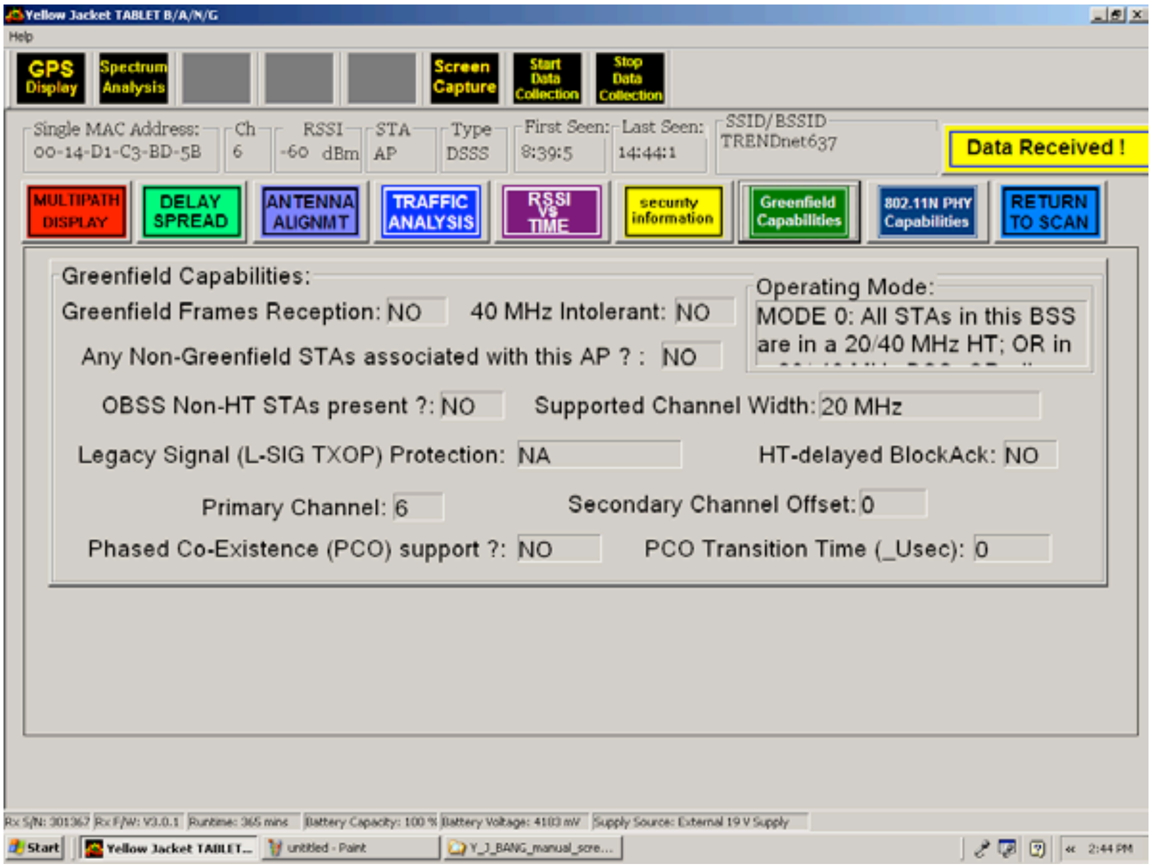


Figure 20. Greenfield Capabilities function window

A Greenfield device is one which supports all the high throughput (HT) capabilities such as the usage of a 40 MHz channel instead of a 20 MHz channel for the transmission of more information. To achieve this, the Greenfield device reserves two adjacent 20 MHz channels to form the 40 MHz wide channel. The above fields can be explained as follows:

Greenfield Frames Reception [YES/NO]: This field indicates if the device has been configured to receive Physical Layer Convergence Protocol (PLCP) protocol data units (PPDUs) with the HT Greenfield format.

40 MHz Intolerant [YES/NO]: if set to NO, indicates one of the following:
If the device is an AP, the AP allows the use of 40 MHz transmission in the neighboring Basic Service Sets (BSSs).
If the device is an STA (i.e. Station: typically a network interface card – NIC in a wireless device) indicates to an AP to which it is associated to inform the AP that it is not restricted in its use of 40 MHz transmissions within its BSS.

If set to YES, indicates one of the following:

- If the device is an AP, it does not allow the use of a 40 MHz channel for transmissions in the neighboring BSSs.
- If the device is an STA, it indicates that the AP to which it is associated is required to restrict its use of 40 MHz transmissions within its BSS.

Operating Mode: Indicates the operating mode of the BSS from which protection requirements of HT transmissions may be determined. HT transmissions shall be protected if there are other STAs (HT or non-HT) that cannot interpret HT transmissions correctly. The fields Operating Mode and Non-Greenfield STAs Present in the HT Information element within the Beacon and Probe Response frames are used to determine if protection is required for transmission.

When the **Operating Mode = 0 or 2** and **Any Non-Greenfield STAs associated with this AP ? = NO**, no protection is required since all associated HT stations in the BSS are capable of decoding HT mixed format and HT Greenfield format transmissions. No protection is required for 40 MHz transmissions since enough of the preamble is sent on both 20 MHz halves of the 40 MHz transmission to ensure that a 20 MHz STA is able to decode the preamble and infer the duration of the transmission.
When the **Operating Mode field is set to 0 or 2** and **Any Non-Greenfield STAs associated with this AP ? = YES**, HT transmissions that use the Greenfield preamble shall be protected.

NOTE 2—When the BSS is operating in the 2.4 GHz band and when the **Operating Mode = 0 or 2**, there are no non-HT STAs in the BSS.

When the **Operating Mode field = 3**, HT transmissions shall be protected. The type of protection that is required depends on the type of transmission as well as the type of the non-HT STAs that are present in the BSS. The specific mechanisms that are to be used for protection for Operating Mode set to 3 are described in the following Table: (Protection requirements for Operating Modes of 1 and 3)

Type of Transmission	**Operating Mode = 3**	**Operating Mode = 1 or 3**
20 MHz transmission	HT transmissions using the HT Greenfield format and/or using RIFS within the HT transmission bursts are protected.	All HT transmissions shall be protected using RTS/CTS or CTS-to-self prior to the HT transmissions.
40 MHz transmissions	HT transmissions using the HT Greenfield format and/or using RIFS within the HT transmission bursts are protected.	All HT transmissions shall be protected using RTS/CTS or CTS-to-self prior to the HT transmissions.

Mode 0 is also called the “pure mode”.
Mode 1 is called as HT non-member protection mode.
Mode 2 is called “pure mode” with at least one non-HT member present.
Mode 3 is the HT-mixed mode and is used if one or more non-HT stations are associated in the BSS.
Overlapping Basic Service Set (OBSS) non-HT STAs present ?[YES/NO]
= YES if the use of protection for non-HT STAs by overlapping BSSs is determined to be desirable.
Some examples when this may be YES, but not limited to:

- one or more non-HT STAs are associated.
- A non-HT BSS is overlapping.

– A management frame (excluding Probe Response) which includes higher supported rates.
= NO otherwise.

Supported Channel Width: indicates if a 20 MHz operation or a 20/40 MHz operation is supported.

Legacy Signal Transmit Opportunity (L-SIG TXOP) Protection[YES/NO]: An HT STA shall indicate whether it supports L-SIG TXOP Protection in its L-SIG TXOP Protection Support capability field in Association Requests and Probe Responses. The AP determines whether all HT STAs associated with its BSS support L-SIG TXOP Protection and indicates this in the L-SIG TXOP Protection Full Support field of its HT Information Element. This field shall be set to 1 only if the L-SIG TXOP Protection field is set to 1 by all HT STA in the BSS.

A STA shall not transmit a frame using L-SIG TXOP Protection directed to a recipient that does not support L-SIG TXOP Protection.

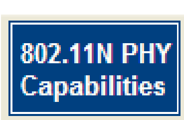
HT-Delayed Block-Ack [YES/NO]: indicates support for HT-delayed BlockAck operation.

Primary Channel: Indicates the channel number of the primary channel.

Secondary Channel: Indicates the offset of the secondary channel relative to the primary channel.
= 1 if the secondary channel is above the primary channel.
= 3 if the secondary channel is below the primary channel.
= 0 if no secondary channel is present.
The value 2 is reserved and is not used.

Phased Co-existence (PCO): Indicates support for Phased Co-existence (PCO).
When an AP supports PCO, it can operate its BSS as a PCO BSS.
A PCO capable non-AP STA will support PCO if it meets the requirements of the PCO capable AP.

PCO Transition Time: indicates that the STA can switch between 20 MHz channel width and 40 MHz channel width within the specified time. Standard transition times are: 400 **µ**sec, 1.5 msec and 5 msec.



802.11 N PHY Capabilities: The window associated with this function appears in Figure 21:

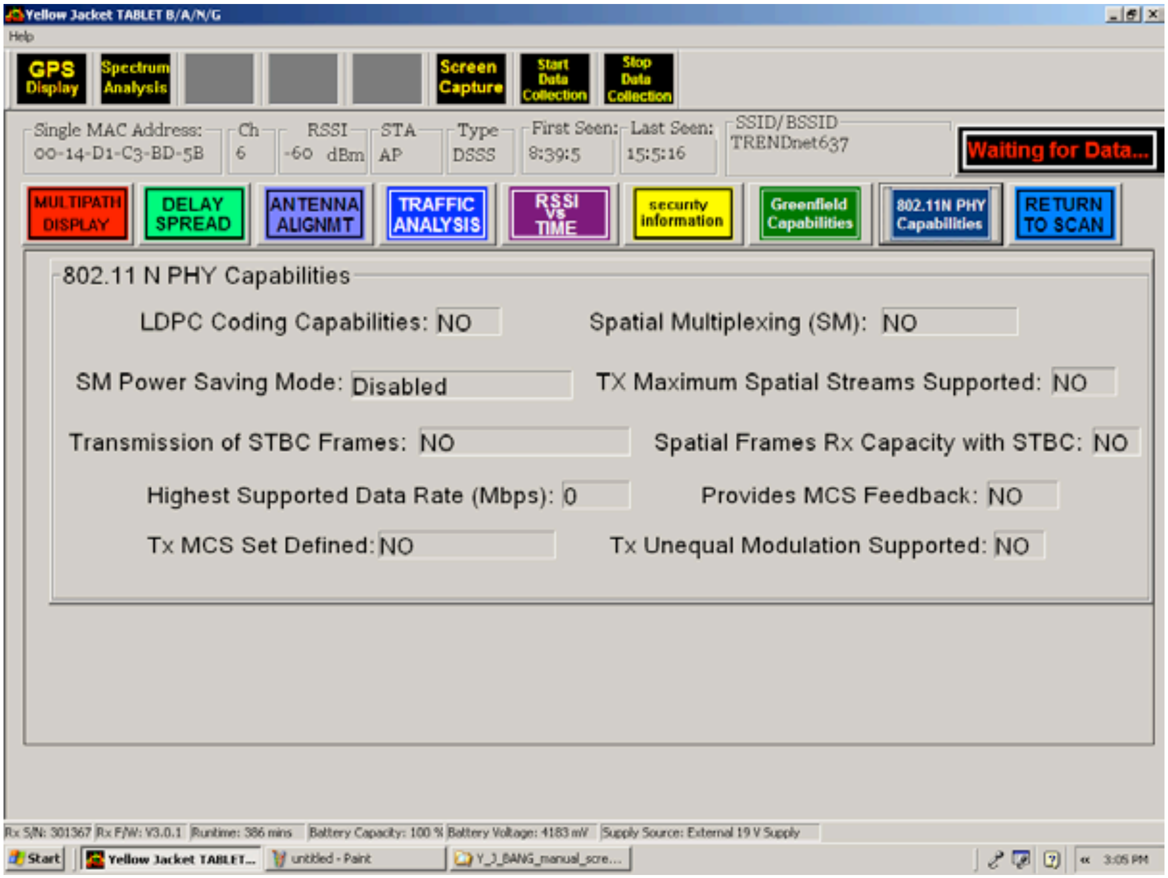


Figure 21. 802.11N PHY Capabilities function window

The attributes associated with this window are as follows:

Low Density Parity Check (LDPC) Coding Capabilities: [YES/NO]: indicates support for receiving LDPC coded packets.

Spatial Multiplexing (SM): [ENABLED/DISABLED]: Indicates if SM has been enabled or disabled.

SM Power Saving Mode: indicates if SM has been enabled; if yes, whether Static or Dynamic SM power save.

Transmission of Space Time Block Coded (STBC) frames is supported: [SUPPORTED/UNSUPPORTED]: indicates the transmission of packets using STBC.

Spatial Frames Rx Capacity using STBC:indicates support of the reception of frames using STBC
= 0 for no support.
= 1 for one spatial stream support.
= 2 for one and two spatial streams support.
= 3 for one, two and three spatial streams support.

Highest Supported Data Rates (Mbps): Indicates the highest data rate supported by this device.

Provides Modulation and coding scheme (MCS) Feedback: Indicates the capability of the STA to provide MCS feedback.
= 0 if the STA does not provide MCS feedback.
= 2 if the STA provides only unsolicited feedback.
= 3 if the STA can provide MCS feedback in response to MRQ as well as unsolicited MCS feedback.
The value of 1 is reserved and unused.

TX MCS Set defined: [YES/NO]: If the transmission modulation and coding scheme (MCS) has been defined.

Unequal Modulation Supported: [YES/NO]: indicates if the device supports unequal modulation.

Spectrum Analyzer Operating Modes and Options

This section demonstrates the following important features of the Yellow Jacket BANG Tablet Spectrum Analyzer:

1. Power Trigger Mode
2. Creating a User-Defined Preset by Saving a Spectrum Context to a File
3. Spectrogram Function
4. Histogram Function

Power Trigger Mode:

The Power Trigger Mode is initiated via the "Spectrum Control" button in the tool bar, which opens the "Spectrum Control Settings" window, allowing the user to enter in the "Trigger Mode Settings" panel in the same window (see Figure 7 above). This is a useful mode in which, the receiver triggers only when the channel power exceeds a certain threshold, which is set by the user. If the user has set a value for the measurement delay, the receiver will take measurements only after that delay time. The device will trigger when the detected channel power exceeds the set power threshold.

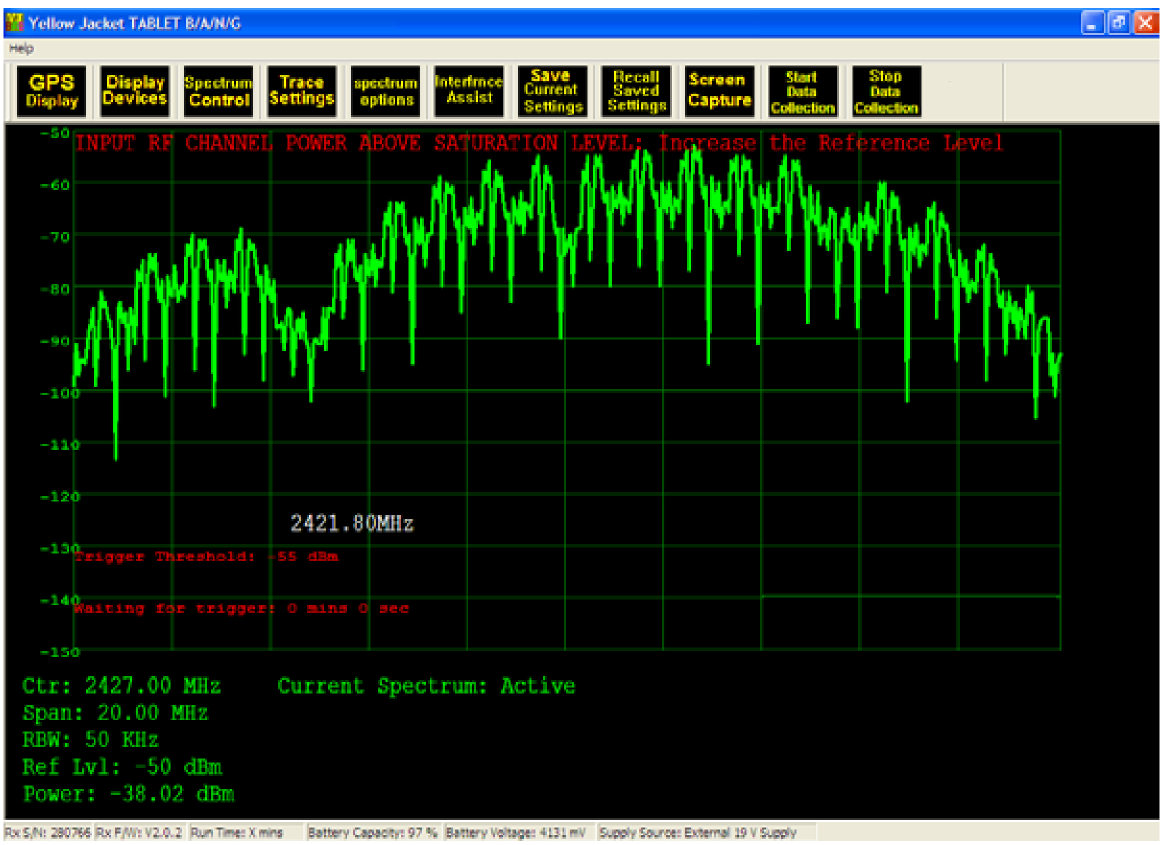


Figure 22. Power Trigger Mode Operation

This mode is useful in detecting activity from non-continuous transmission sources such as Beacon packets from an AP or Frequency Hopping Spread Spectrum (FHSS) Packets from a Bluetooth device or any other Narrow band or CW signal. Figure 22 shows the main application window in Power Trigger Mode

Operation.

IMPORTANT NOTES:

1. **The Trigger can only be set for a maximum Span of 20 MHz**. Set the Center Frequency to a suitable value and then set the Span to 20 MHz.
2. **The Trigger Threshold Power must be within 20 dB of the Reference Level.** If the Threshold value is below 20 dB of the Reference Level, the Yellow Jacket BANG Receiver will not trigger. To adjust the threshold level greater than 20 dB below the reference level, lower the reference level and then adjust the trigger threshold.
3. **Stop the Trigger by clicking "Stop Trigger" to exit the Trigger Mode and resume the normal Spectrum Mode.**

IMPORTANT TIPS WHILE USING THE TRIGGER MODE:

The trigger mode will trigger when the power in a 20 MHz channel exceeds the set power threshold. The presets can be very helpful in conjunction with the trigger mode.

- **Select a channel using the Preset tabs.**
- **Set the Reference Level and the Resolution Bandwidth.**
- **Set a threshold value to be within AT MOST 20 dB below the reference level.**
- **Start the trigger. The receiver will now trigger on the preset channel.**
- **Click "Stop Trigger" to stop the trigger.**

Reference Level:

Varying the Reference Level of the Receiver can change the Dynamic Range of Power measurement of the Yellow Jacket BANG. The Reference Level Settings for the Yellow Jacket BANG Receiver can be changed from –20 dBm to –70 dBm in steps of 10 dB. For measuring very strong signals the reference level can be set to a high value like –20 dBm while low power signals can be measured by setting the reference level to –70 dBm. Hence when the Reference level has been set to –20 dBm, the receiver can measure signals with a maximum value of –20 dBm. If the reference level is a low value compared to the value of the received signal, the signals will be clipped.

Creating a User-Defined Preset by Saving a Spectrum Context to a File

A particular spectral context of interest can be saved in a file at the click of the tool-bar button "**Save Current Settings**" (see Figure 22) for future access. This provides for user-defined presets for quick-access in situations when certain spectral settings need to be changed frequently. Upon clicking the **Save Spectrum Settings** button the software displays the current spectrum analyzer settings which can be saved in a file, in Figure 23:

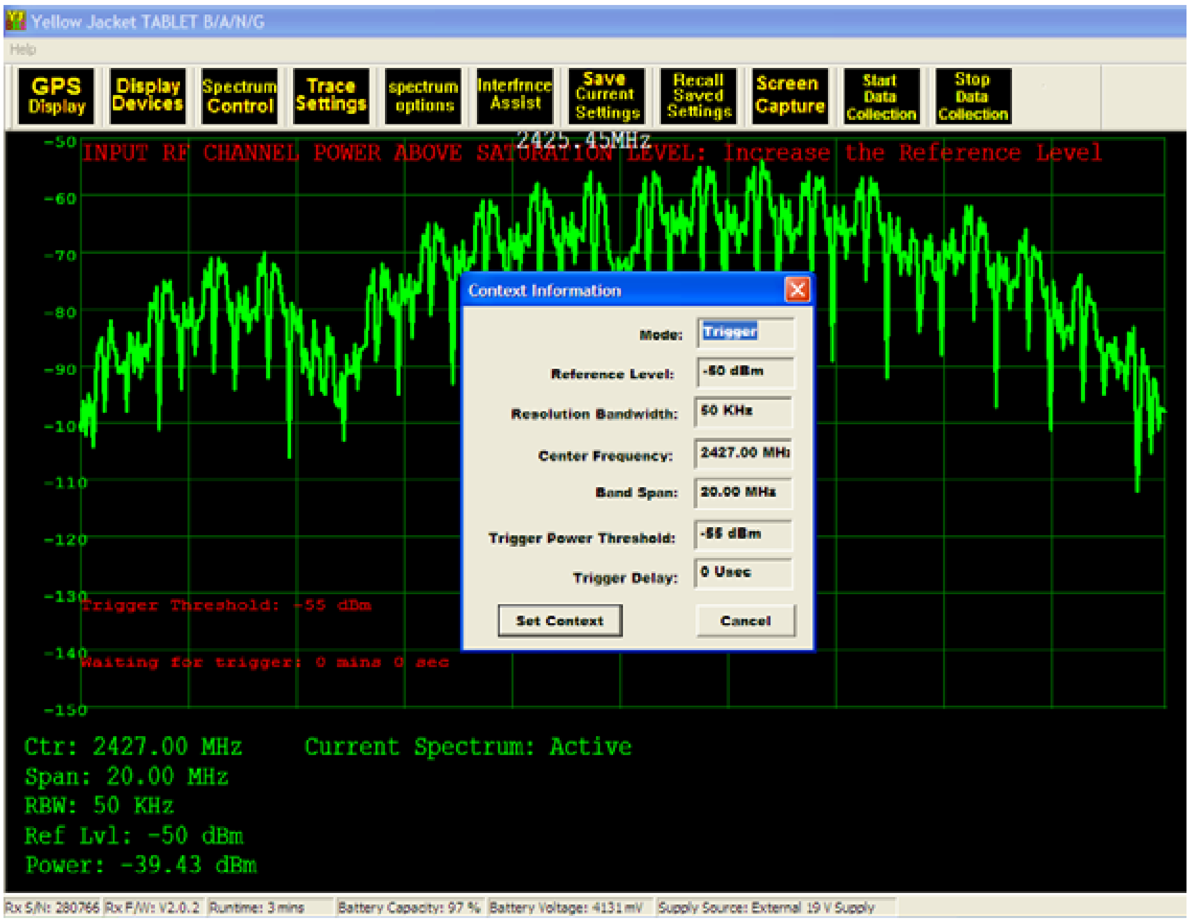


Figure 23. Saving Spectrum Context Information

Upon clicking the "Set Context" button on the settings display dialog window "**Context Information**", the settings can be saved to a file at a desired location. This saved context file can later be invoked by clicking the "**Recall Saved Settings**" button on the toolbar in Figure 23, to set the Yellow Jacket BANG spectrum analyzer to operate in that context. This allows the user to store frequently visited contexts and later revisit them conveniently without having to manually change the settings every time.

Spectrogram Function

To activate this function, click the “spectrum options” button in the main application window toolbar, then select the “TURN SPECTROGRAM DISPLAY ON” button seen in Figure 24:

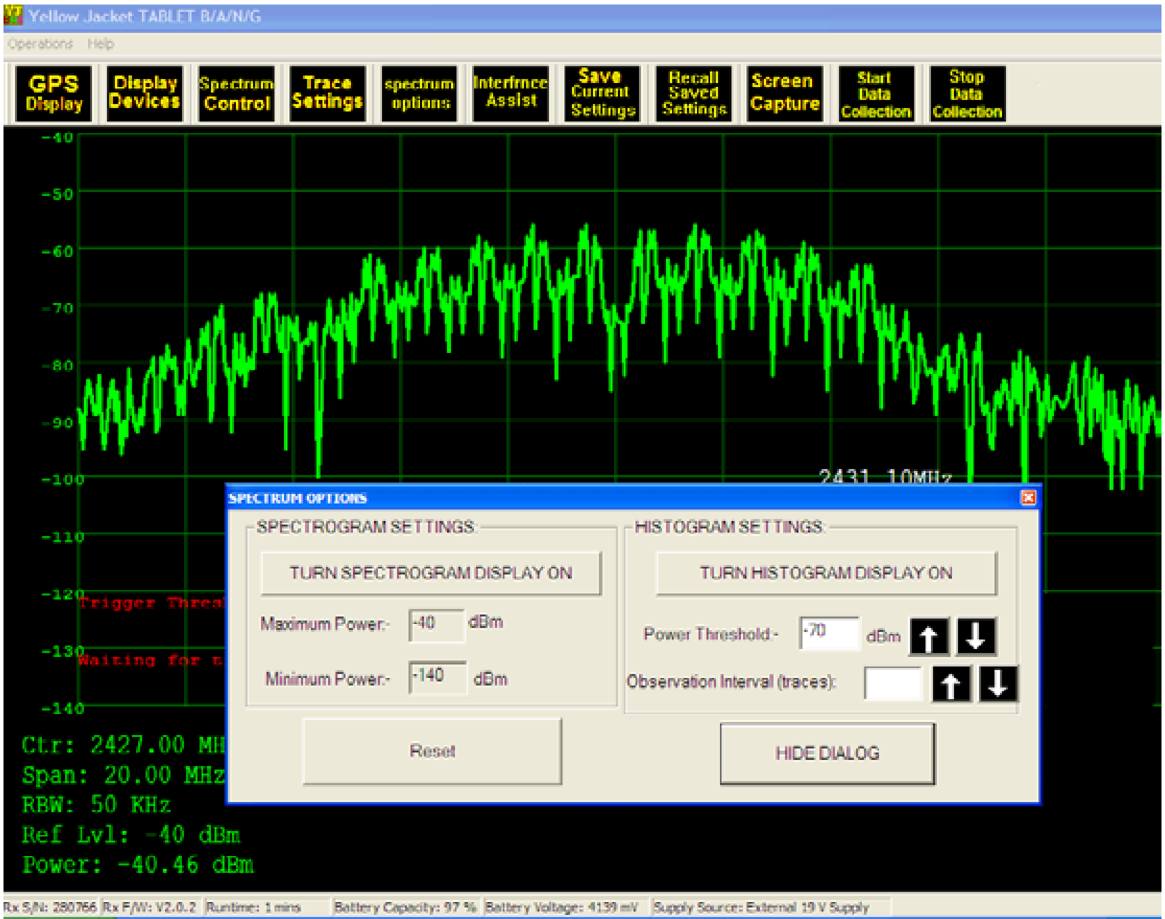


Figure 24. Spectrum Options

The resulting Spectrogram screen (see Figure 25 below) displays the last 100 spectrum traces with each trace point on the spectrograph color coded to reflect the appropriate RSSI level between a maximum value (current reference level) and a minimum value (100 dB below the reference level):

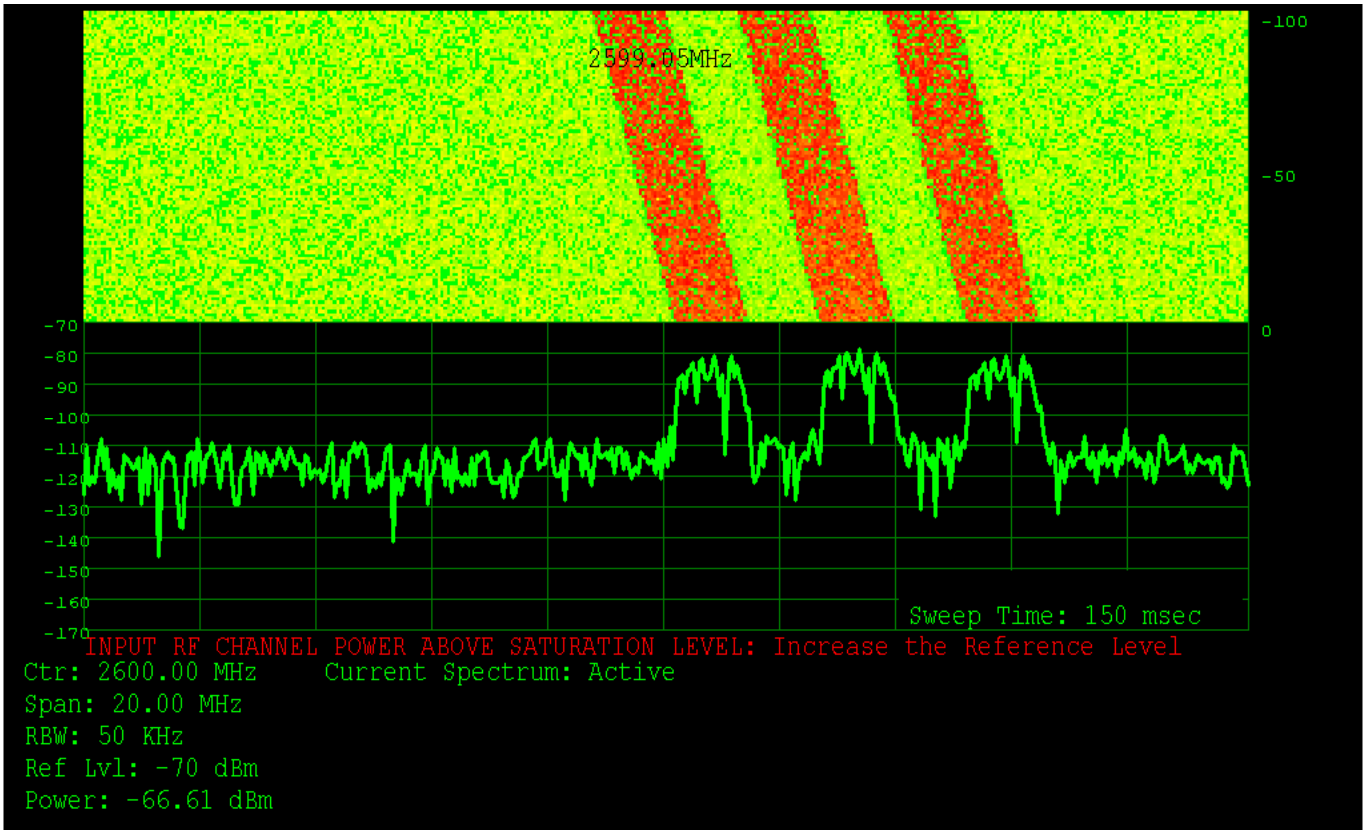


Figure 25. Spectrogram Function (toolbar not shown)

Histogram Function

This function is selectable from the "**Spectrum Options**" dialog window seen in Figure 24, by selecting "TURN HISTOGRAM ON". When activated, the Histogram screen displays the percentage of past triggers for which the RSSI at a frequency on the spectrum exceeds the current set threshold. The number of traces for which this observation is to be made as well as the Power Threshold can be user settable as seen in the dialog window in Figure 26:

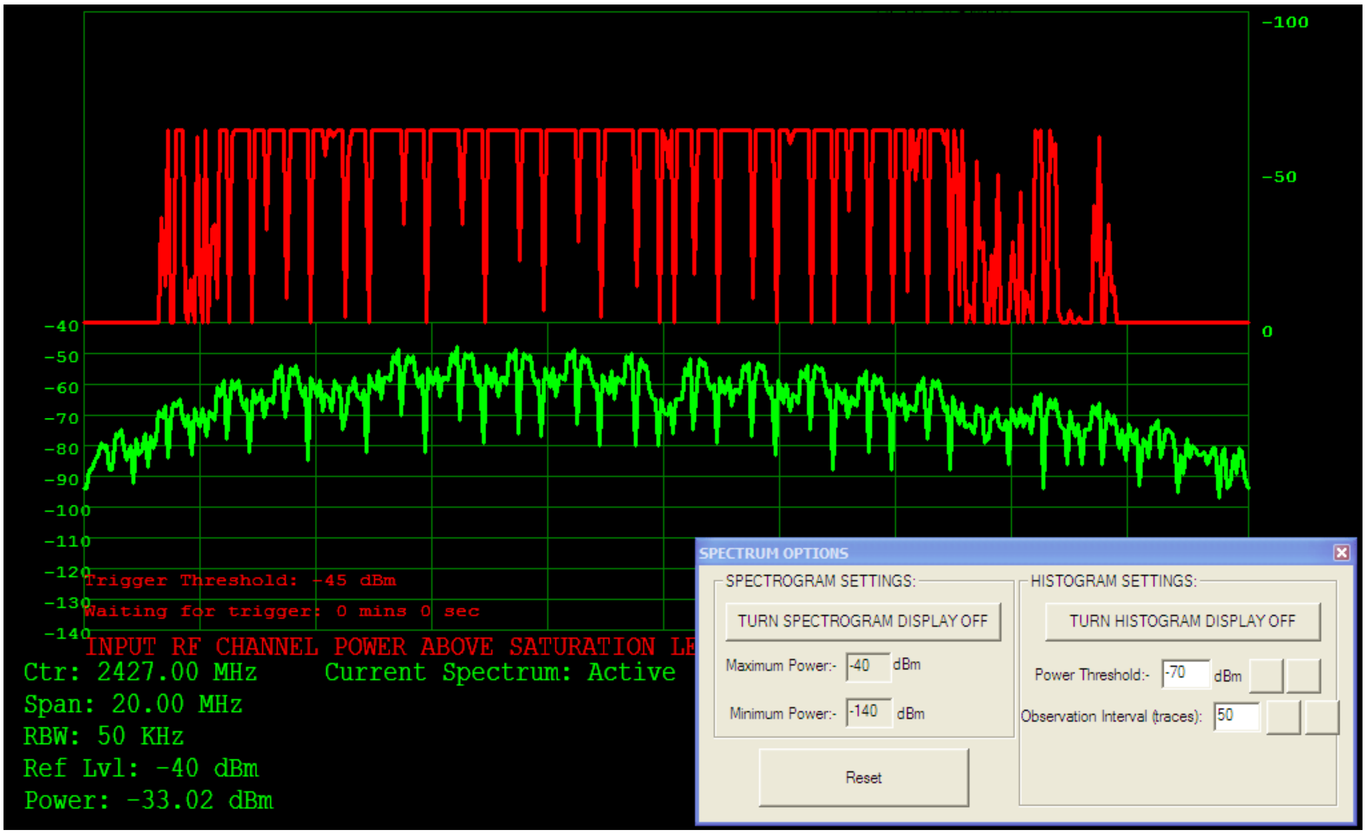


Figure 26. Histogram Function Settings (toolbar not shown)

Direction Finding Antenna Use in Single-MAC Mode of Operation

The “ANTENNA ALIGNMENT” function (see Figure 15 above) enables the user to physically locate a wireless device with a given MAC address. The Yellow Jacket BANG receiver builds the signal strength distribution as it accumulates records of observed signals in real time, while the orientation of the Direction Finding (DF) antenna is fixed. Since the unit needs a finite amount of time to capture and process two or more consecutive signals from the same device in real time, the user must allow the unit to function long enough for the ANTENNA ALIGNMENT distribution to stabilize in time, while the DF antenna is held fixed in the same direction. Devices transmitting consistently over relatively shorter period(s) will generally be located in a shorter time (and much easier) than devices transmitting intermittently, or randomly over relatively longer periods, for the same reasons.

Assuming the user has given enough time for the signal distributions to stabilize every time the DF antenna is pointing in a new direction over a 360 degree sweep range, he or she will soon be able to identify an initial Line Of Position (LOP) yielding the “sharpest” signal distribution (i.e., when almost all of observed signals have the same signal strength) over the 360 degree sweep range. The user can locate a source using one LOPs or “triangulate” using two (or more) LOPs:

Using One LOP

The user would try to confirm the initial LOP orientation as he/she is getting closer to the source slowly while sampling the signal distribution at relevant azimuth angles at points 1, 2, 3, etc as depicted in Figure 27. This process can be repeated while moving along the same LOP and/or making adjustments to the initial LOP till the user is within arm’s reach of the source.

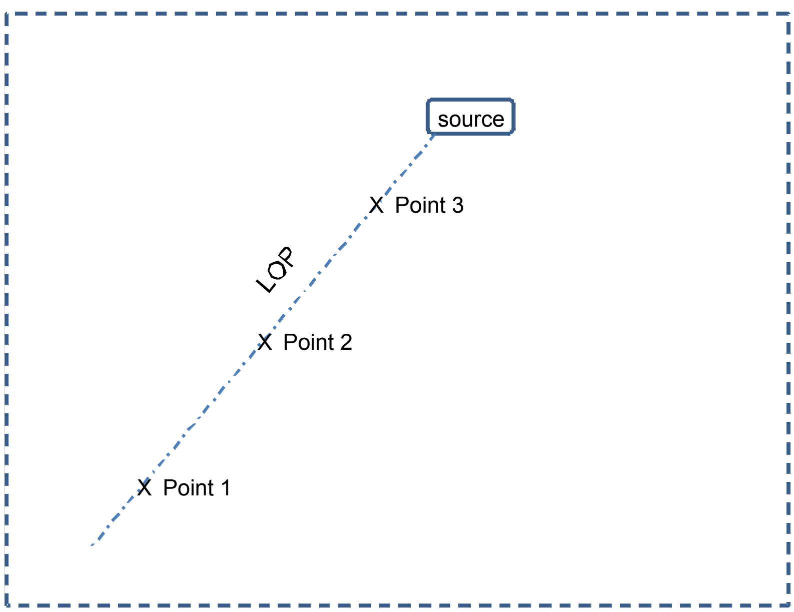


Figure 27. Method 1: Pursuing Source along the Same LOP

<u>"Triangulate" using Two (or more) LOPs</u>

This method helps the user "triangulate" the location of source by determining two (or more) LOPs of the source from two (or more) different positions on the floor (see Figure 28). The following sequence is used:

1. Choose Point 1 and determine LOP1

2. Move away from LOP 1 in the perpendicular direction to Point 2 without getting too close to obstructions and/or walls. At Point 2 determine LOP2.

3. Mentally determine approximate area of intersection for LOP1 and LOP2 within the space monitored.

4. Move to point of intersection and pin-point to source by finding new LOP if needed

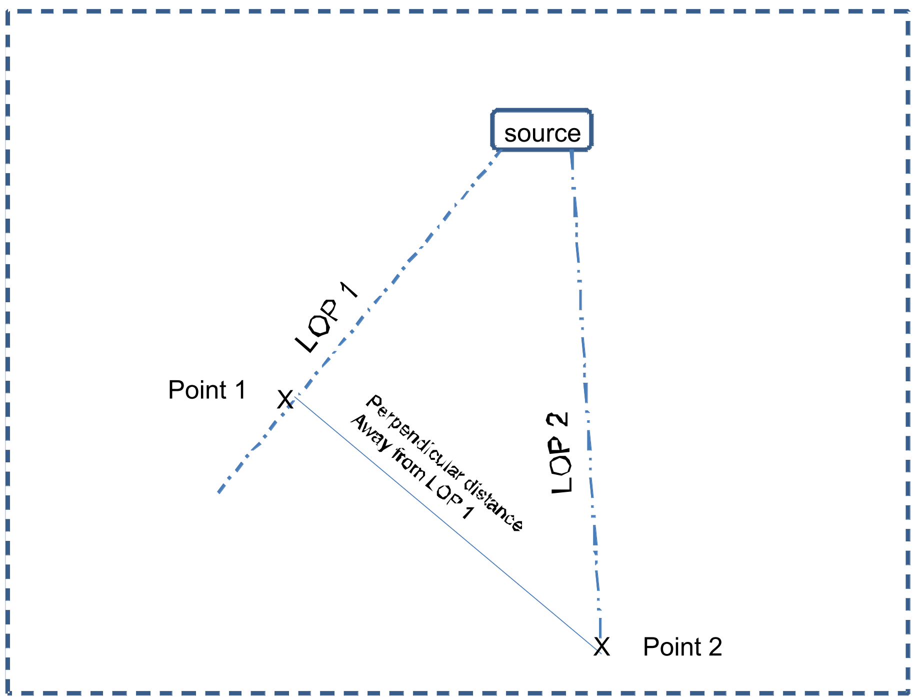


Figure 28. "Triangulating" the Source Using Two LOPs

Locating Rouge Access Point(s) with the Yellow Jacket Toughbook BAGN analyzer

A Rouge Access Point (RAP) is a WiFi access point connected to a Local Area Network (LAN), without authorization, with or without intent. Since such an Access Point (AP) is not managed by the appropriate network administrator, a RAP cannot be expected to conform to the security policies of the network it is connected to. When connected to a secure network, a RAP could allow any WiFi equipped Notebook or Laptop PC user to access the LAN, effectively bypassing several layers of security that legitimate users of the network have to go through. The Yellow Jacket Toughbook BAGN analyzer can be used to detect, monitor and locate RAPs using a directional antenna. The purpose of this section is to explain and demonstrate how the Yellow Jacket Toughbook BAGN analyzer should be set up to help the user detect and locate RAPs.

Currently the YJ BAGN Analyzer can be deployed with optional directional antennas for 2.4GHz and 4.9/5GHz frequency bands. The procedures described in this section are applicable to both of these antennas.

Setting Up the Analyzer

The Yellow Jacket Toughbook BAGN analyzer should be set up as follows:

4. Replace the Omnidirectional antenna with the (optional) Directional antenna [1]
5. Obtain the MAC List of all detected WiFi stations, by clicking the "Display Devices" button (see Figure 1):

#	MAC Address	SSID/BSSID	dBm	SNR	Ch#	ENC	STA	MOD	Mbps	Packet Type <-> Device
1	00-40-33-AF-F6-E9	Gator	-36	55	4	No	AP	DSSS	1	Beacon ->Broadcast
2	00-11-24-03-5B-D1	Apple Airport Expr...	-71	20	11	Yes	AP	DSSS	1	Beacon ->Broadcast
3	00-05-5D-26-12-8B	BVS802.11A	-42	49	64*	No	AP	OFD...	6	Beacon ->Broadcast
4	00-05-3C-06-F7-6C	05B405328939	-74	-6	7*		NIC	DSSS	11	Probe Rq ->Broadcast
5	00-1B-9E-83-11-E3	Gator	-33	42	11*		NIC	DSSS	1	Probe Rq ->Broadcast
6	00-14-D1-C3-BD-5B	TRENDnet637	-60	5	6	No	AP	DSSS	1	Beacon ->Broadcast
7	00-1B-9E-A7-3A-29	TRENDnet637	-57	38	9*		NIC	DSSS	1	Probe Rsp<--00-1E-52-F4-FB-16
8	00-1E-52-F4-FB-16	Scott's wireless b...	-58	-9	1	Yes	AP	DSSS	1	Beacon ->Broadcast

Figure 1. MAC List for Detected Devices (excerpt from main screen)

6. After a specific MAC address in the list has been identified to correspond to a RAP, select that device by clicking on the corresponding row (see Figure 1).

7. Enter the "Single MAC Mode of Operation" by double-clicking on the selected device/row in Figure 1, to initiate the Single-MAC Function Window seen in Figure 2:

1 The user may deploy either the 2.4GHz or the 4.9/5 GHz corner reflector directional anntenna.

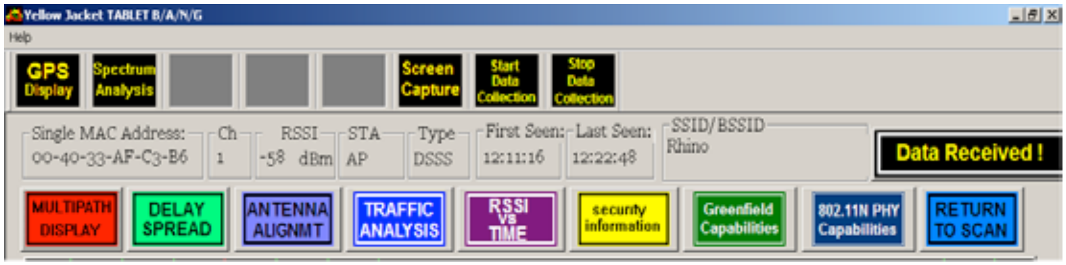


Figure 2. Single-MAC Function Window (excerpt from main screen)

8. Click the soft-button labeled "ANTENNA ALIGNMENT" :

this will initiate the Antenna Alignment screen seen in Figure 3:

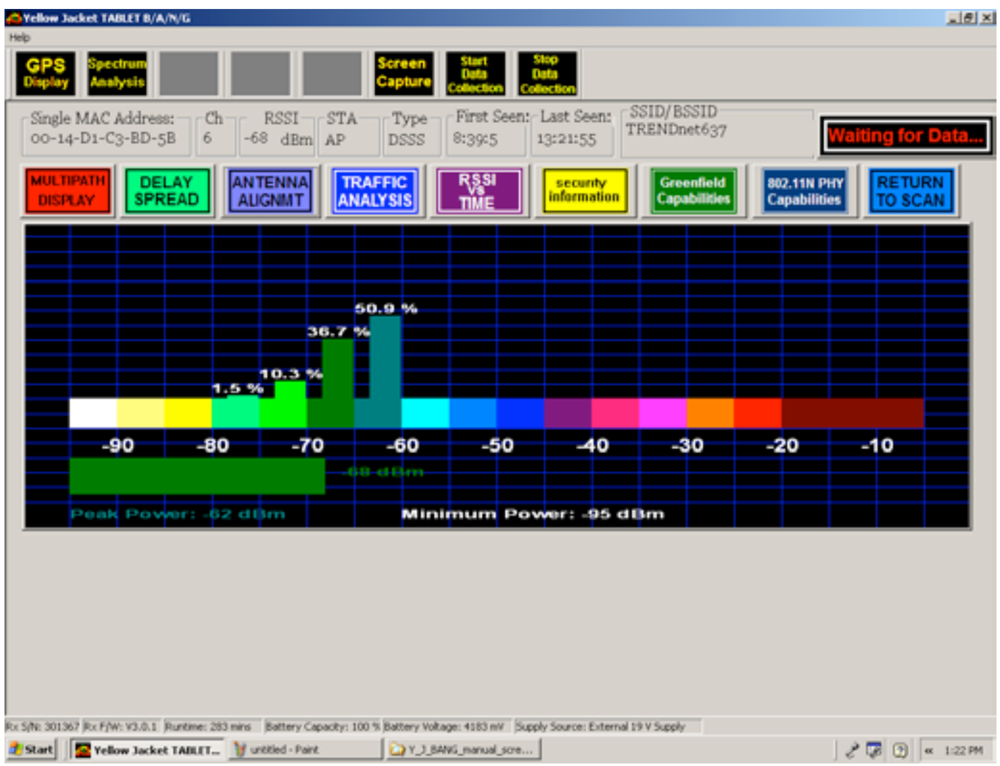


Figure 3. Antenna Alignment function screen

The horizontal axis of the bar-chart in Figure 3 corresponds to the detected signal peak power level in dBm scale; the vertical axis in Figure 3 corresponds to the percentage (%) of all detected signals in the same peak power group. Thus, 50.9 % of all signals observed had a peak power level of -62dBm, 36.7% of all observed signals had a peak power level of -67dBm, 10.3% had a peak power level of -72dBm, etc.. Therefore, it may be expected that when all incident signals to the receive antenna come directly from the same transmit antenna the great majority of signals will be in the same power group (or, the distribution of detected signals will become much narrower). Conversely, the farther away the Directional Antenna is pointing from the source of signals, the smaller will be the percentage of signals occupying the highest power levels (due to multiple-reflections), or, the broader the power distribution of the detected signals.

9. The Directional Antenna may be used for determining the azimuth direction of the RAP antenna. To do so, the user observes the shape of the detected signal power distribution (Antenna Alignment screen) as the Directional Antenna is "swept" from side to side in the horizontal plane. When the Directional Antenna is pointing directly at the source of transmitted signals, the shape of the observed distribution will be "narrowest" (or, majority of detected signals will be in one or two power groups). This orientation of the directional antenna corresponds to a "Line of Position" LOP, which defines the azimuth position of the RAP.

10. To locate a RAP, the user either needs to get closer to the RAP along the initial LOP or needs to move to a new location (move perpendicularly away from the first LOP) and determine at least one more LOP for triangulating the RAP source. These two methods (A and B) are discussed below.

Practical Methods for Locating a RAP Using One or more LOPs

After the first LOP is established by a 360 degree sweep, the user re-confirms the LOP orientation by sweeping the unit back and forth about the initial LOP (see Figure 4), while observing the "width" or the number of power ranges of the detected signal distribution in the Antenna Alignment screen in Figure 3.

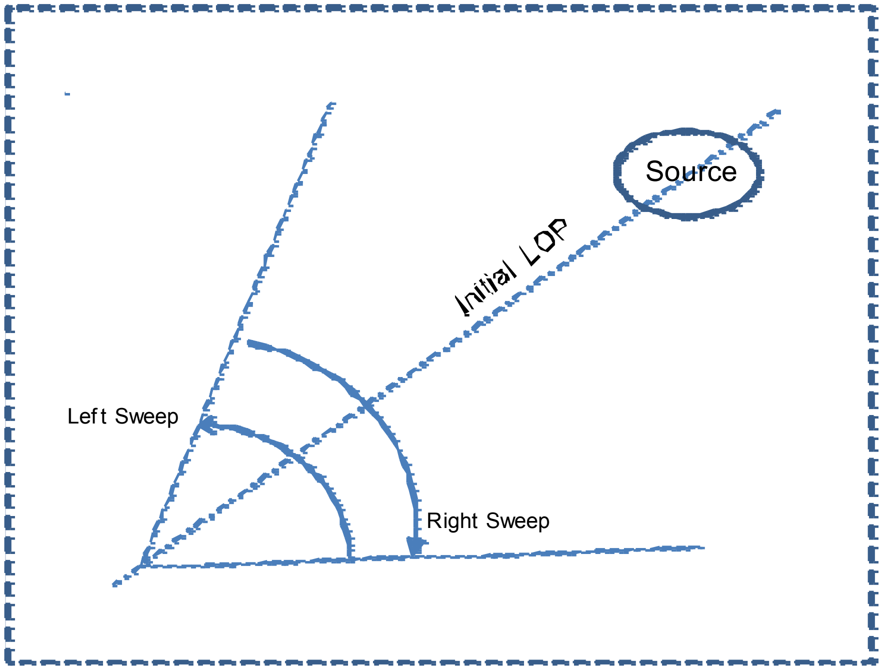


Figure 4. LOP Continually Re-Confirmed About Initial Orientation

Once the initial LOP is determined, the user may locate the source using one or both of the following two methods.

Method A: Maximizing Signal Along one LOP

This method is based on approaching the source along one LOP (see Figure 5), in order to increase the observed power levels of the detected signals.

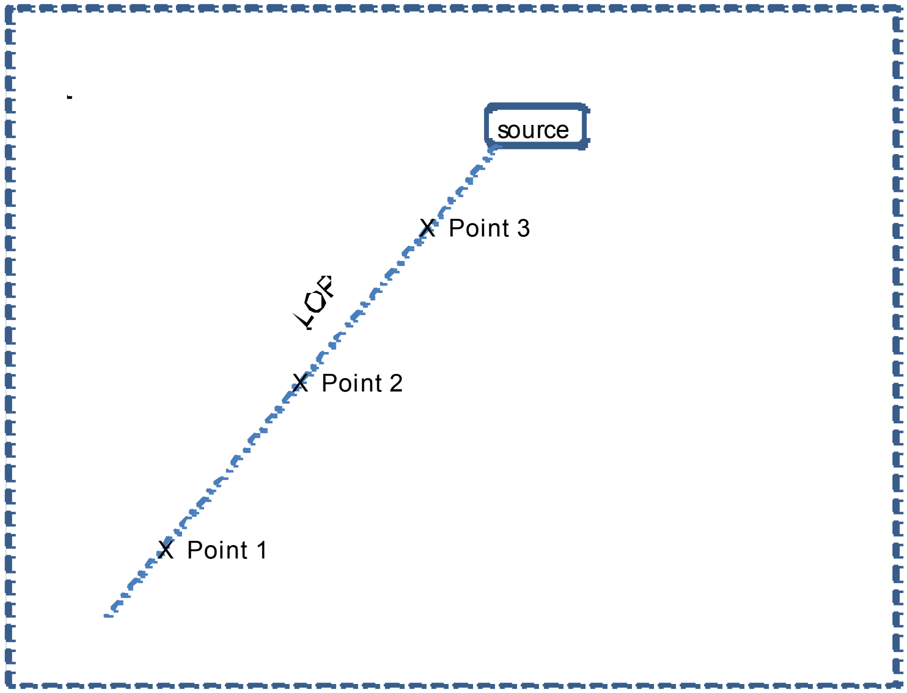


Figure 5. Method A: Pursuing Source Along the Same LOP

use the following sequence to accomplish this:

2. Level the DF antenna by pointing the flat surface of the DF antenna to the potential source.
3. Keeping it level (or at the angle of the potential source), scan the DF antenna azimouthally, from side to side within an arc of about 90 degrees (i.e., 45 degrees to right, then 45 degrees to left, and repeat …) to determine relative direction for maximum signal distribution.
4. Advancing slowly in the same heading, scan the unit side-to-side again while the signal level (in dBm scale) increases.
5. Keep walking in the same direction and repeat Steps 2 and 3 for increased signal till the source is within reach.

Method B: "Triangulate" with Two (or more) LOPs

This method helps the user to rapidly "triangulate" the approximate location of a RAP by determining two (or more) LOPs from two (or more) different positions on the floor (see Figure 6).

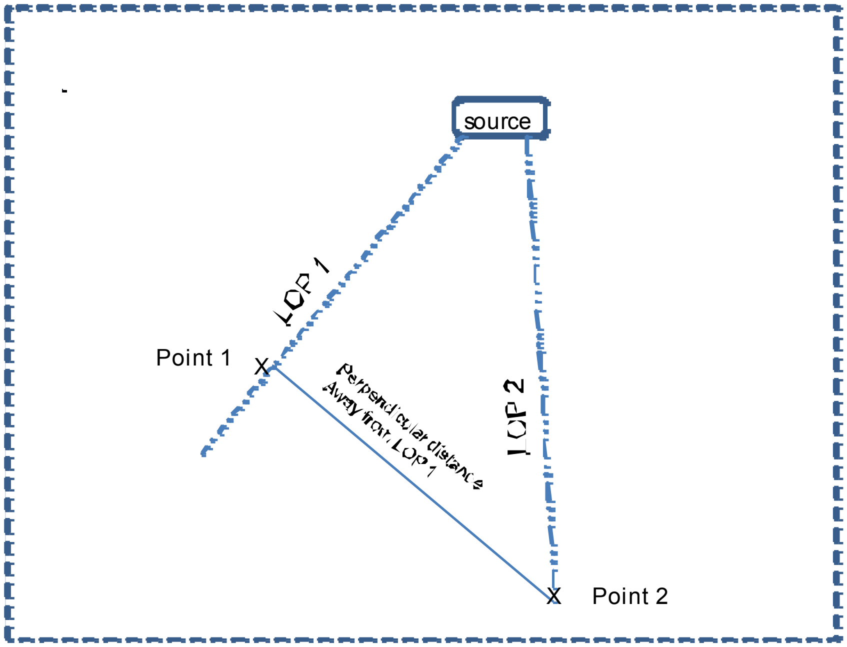


Figure 6. Method B: Triangulating the Source Using Two LOPs

To accomplish this, use the following sequence of steps:

Choose Point 1 and determine LOP1
Move away from LOP 1 in the perpendicular direction to Point 2 without getting too close to obstructions and/or walls. At Point 2 determine LOP2.
Mentally determine approximate area of intersection for LOP1 and LOP2 within the space monitored.
Move to the point of intersection of LOP1 and LOP2 to find the RAP.

If Method B reveals approximate location of the RAP but it still cannot be located, use Method A to move in closer on the source, till it is within arm's reach.

Operating and Troubleshooting Notes

1. In order to eliminate known sources of interference with the Yellow Jacket BANG Tablet Receiver, please ensure that the Wireless LAN Radio and the Bluetooth transmitter are disabled before using the software.

2. When the Yellow Jacket BANG receiver is being used with Batteries, the software will monitor the battery charge and will terminate the application if the batteries drop low on charge. A notification message will be displayed before the software terminates. This is done to protect the batteries from draining completely and causing subsequent damage to the receiver.

3. The Samsung Q1 UMPC must be securely connected to the cable and the cable must be securely connected to the Yellow Jacket BANG Receiver through the USB cable. Loose cable connection can be a major problem while using the Yellow Jacket BANG Tablet Software.

4. Please remove the USB Cable from the USB slot on the Yellow Jacket BANG Tablet before replacing the batteries on the Yellow Jacket BANG Receiver.

5. Use fully charged batteries in the Yellow Jacket BANG Receiver and charge the Yellow Jacket BANG Tablet before running the software for a longer duration of usage. When the batteries in the Yellow Jacket BANG Receiver fall low on charge and need to be recharged, the Yellow Jacket BANG Tablet software will shut down after a 30 second warning message.

6. The default power settings cause the Tablet PC to turn off and hibernate after 15 minutes. For better performance, set the Tablet PC power options to optimize performance. This can be done by: Start Menu>>Control Panel>>Power Options.

7. If the USB cable is incorrectly connected or the batteries in the receiver are completely discharged, then a message shown below will be displayed upon starting the software. On clicking "Try Again", the software will establish a connection with the Yellow Jacket BANG Receiver.