Section 2

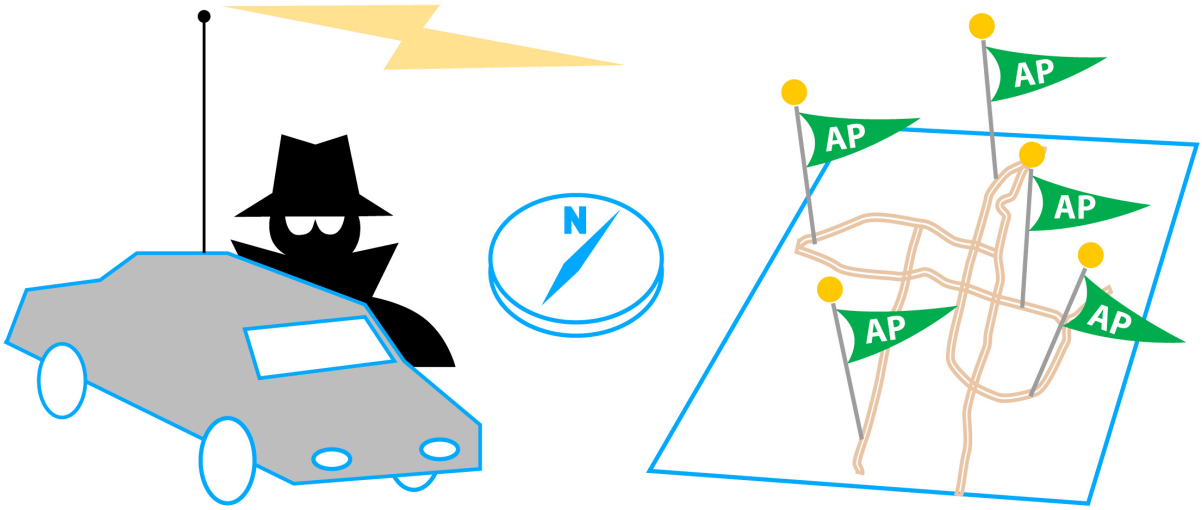
Discovering, Locating, & Accessing WiFi Networks

The first part of scanning will be the RF environment – using the WiSpy Spectrum Analysis tool, we'll show what different 'RF Signatures' look like and what you should be looking for in your networks.

Then we'll move on to using different tools- WiFi Hopper, Network Stumbler, and AirDefense Mobile to scan, document and finally find rogue devices on your 802.11 network.

Next, a quick stop with a Bluetooth scanner then on to the fun labs configuring and using GPS to document how your wireless networks 'leak' into the surrounding area. We'll have you WarDriving with some pretty cool kit in no time.

Finally, on to use some internet tools to document and present your WarDriving findings.



Lab 2.1: RF Scanning- with WiSpy &RF Signatures

The purpose of this lab is to learn how to identify and locate Wi-Fi Networks. You will learn how to locate an Access Point or The following tools will be used to discover wireless networks: Netstumbler, Zyxel, WI-Fi Hopper, Wi-Spy Spectrum Analyzer.

Additionally, this lab will explain how to find Access Points and stations. This is critical in quickly finding and removing rogue Access Points. Rogue Access Points are the # 1 biggest security risk to a wireless LAN implementation.

The Nokia N800 will be used to connect to the open Wi-Fi networks.

Product Information

Source

Netstumbler

Free

www.netstumbler.org

Wi-Fi Hopper

$34.95

www.wifihopper.com

Wi-Spy Spectrum Analyzer

$199.00

www.metageek.net

Where, When, Why

The tools Airdefense Mobile, WiFi Hopper, and Wi-Spy Spectrum Analyzer will all be used to identify wireless networks and find the approximate location of a rogue access point. A GPS device will be used to find a more precise estimate of the devices location. During a wireless security assessment, a pen tester can use all these tools in concert to locate the exact position of a rogue access point, essential information for quickly removing the Rogue from the network.

Usage and Features

- Locate the position of an Access Point
- Locate a wireless station
- Identify and locate rogue AP's

Requirements / Dependencies

- Zyxel
- WiFi Hopper
- Wi-Spy Spectrum Analyzer
- Garmin GPS

What you will do in this lab:

- Scan for RF signatures of wireless devices
- Identify wireless LAN's by RF signature

Lab Part 1 - Using WiSpy to identify 802.11 Access Point RF signatures

Step 1. Plug the Wi-Spy USB adapter into your WLSAT Laptop.

Step 2. Open ***chanalyzer*** – `Start → Wireless Tools → Chanalyzer`.

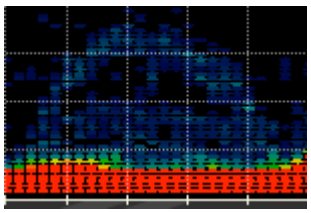
Step 3. Click the `View` menu and choose `All Three Views`; Spectral, Topographic, and Planar view.

Step 4. Identify the RF signature of your Access Point – it might be just a bit 'crowded' here in the classroom with all these APs on the same channel.

Step 5. Change the `channel of your Access Point` and see if you can identify the RF signature on the Spectrum Analyzer.

Step 6. What does the RF signature of a DSSS device look like on a Spectrum Analyzer?

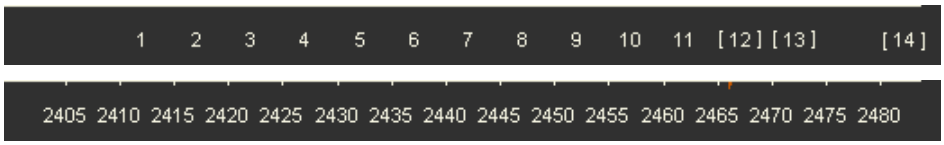
_____



Step 7. What frequencies are affected by an Access Point on Channel 1?

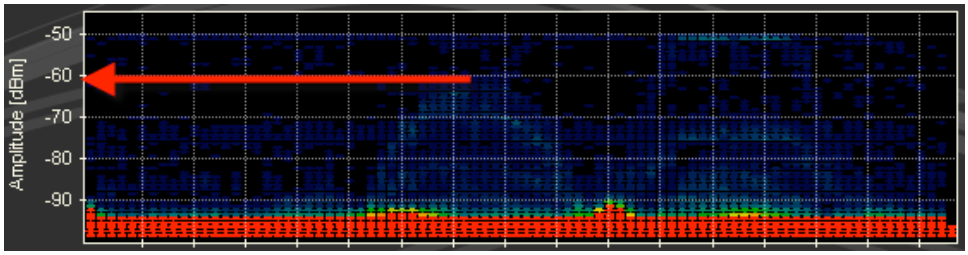
_____

(change view of Frequencies vs Channels)



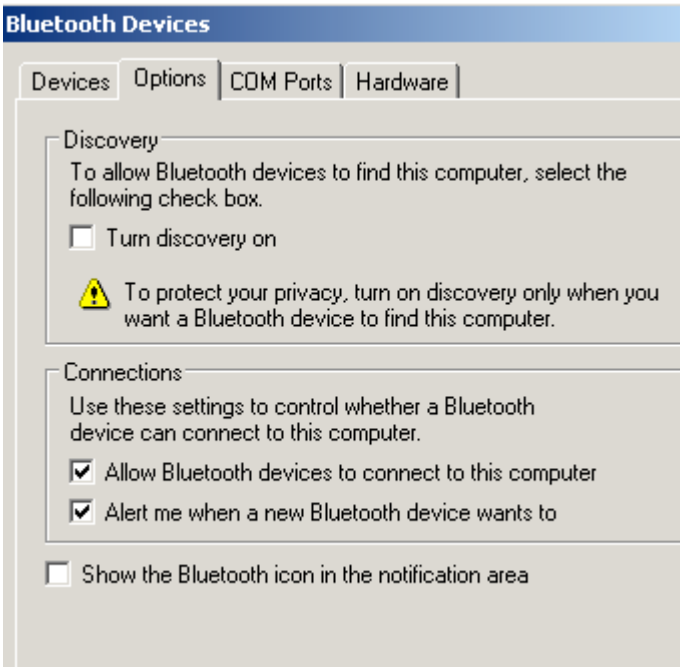
Step 8. What is the amplitude of the signal?

_____



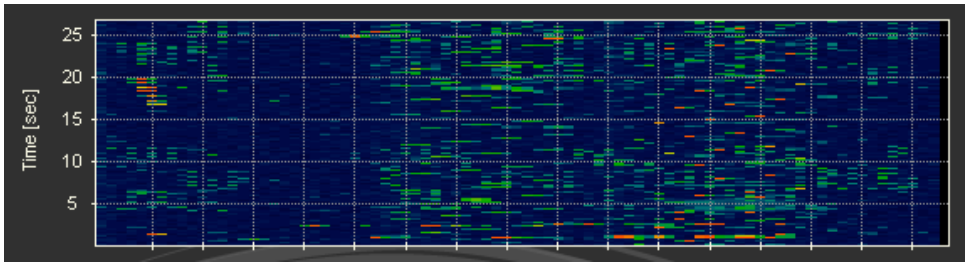
Lab Part 2 - Using WiSpy to identify Bluetooth RF signatures

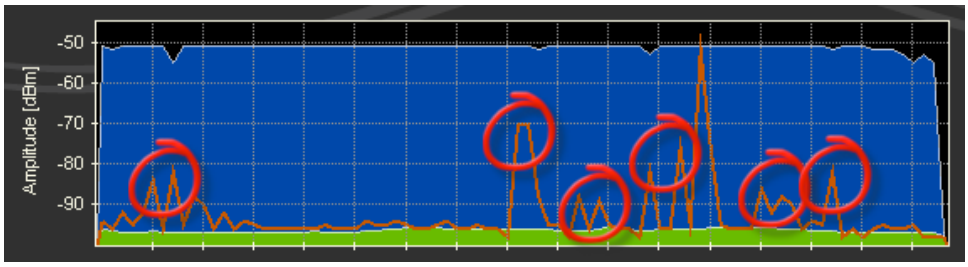
Step 1. Enable the Bluetooth radio on your WLSAT laptop and/or Nokia N800 and see if you can identify the RF signature.



Step 2. What does the RF signature of a FHSS device (like Bluetooth) look like on a Spectrum Analyzer?

_____





Step 3. What frequencies are affected by bluetooth?

_____

Step 4. What is the amplitude of the signal?

_____

Step 5. How does that compare with the Access Point's signal strength?

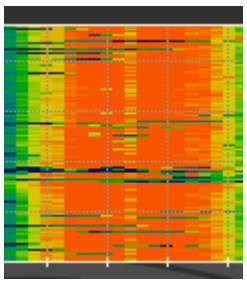
_____

Lab Part 3 - Using WiSpy to identify RF jammer signatures

Step 1. Turn on your 2.4 Ghz Jammer (Wireless Camera) and see if you can identify the RF signature.

Step 2. What does the RF signature of a Jammer device look like on a Spectrum Analyzer?

_____



Step 3. What frequencies are affected by the jammer transmitting?

_____

Step 4. What is the amplitude of the signal?

_____

Step 5. How does that compare with the Access Point's signal strength?

_____

Lab Part 4 - Using WiSpy to create a baseline recording of the RF environment

During a wireless security assessment it is usually a good idea to take an RF baseline of the network. This baseline can be referenced in the WLAN assessment report document and used for later analysis. This RF baseline can be especially useful when trying the troubleshoot RF interference or noise.

Step 1. Click the `File Menu`.

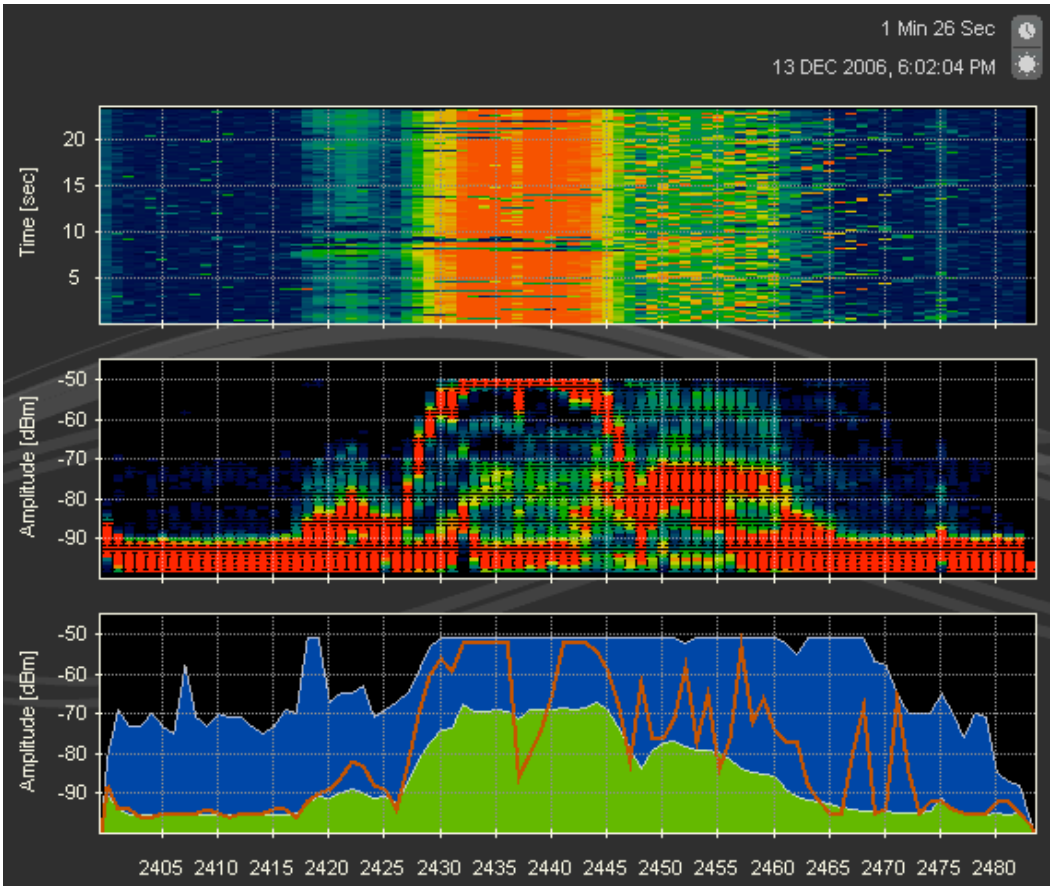
Step 2. Click `Create New Recording`.

Step 3. Type a *`name for the recording`* and document it here.

_____

Step 4. Click `Save`.

Step 5. Let Wispy run for a period of time and then click `end recording`.



Lab 2.2: Scanning for networks: directional & high gain antennas

What you will do in this lab:

- Scan for available wireless networks with a low gain omni antenna
- Scan for available wireless networks with a directional high gain antenna

Lab Part 1 - Using the Zyxel AG-225H utility to scan for wireless networks

Step 1. Plug in the Zyxel AG-225H USB adapter.

Step 2. Launch the *Zyxel* utility. `Start → Wireless Tools → Zyxel AG-225H(v2) Utility`

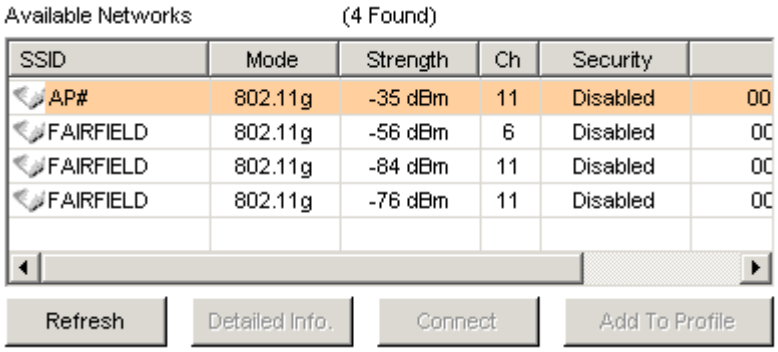
> Note: You'll need to choose the version of the Zyxel utility that matches the revision of your AG-225H USB Adapter –

Step 3. Click the `Site Survey button`.

Step 4. Scroll through the list of available networks.

How many networks were visible?

_____



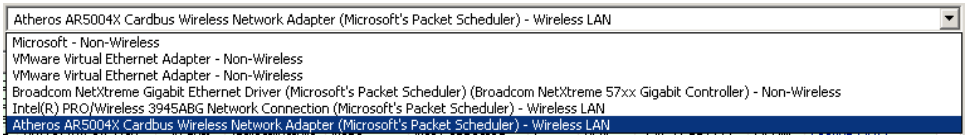
> You can also use the Zxyel without a computer. Just turn it on with the switch on top – and wait while it scans and shows the available WiFi Networks.

Lab Part 2 - Using WiFi Hopper to scan for wireless networks

Step 1. Plug the Ubiquiti card into you wireless pen testing laptop and connect the low gain (small 2.2dBi) Omni antenna.

Step 2. Open ***WiFi Hopper***. *Start → Wireless Tools → WiFi Hopper*

Step 3. And select the Ubiquiti Card's driver.



Step 4. Do you see any additional AP's that were not displayed in the ***Zyxel*** utility?

_____

Ssid	Type	MAC Address	Signal	Mode	Encryption	Status	Hits	Score	Frequency	PHY	Vendor
FAIRFIELD	802.11g	00:90:96:ff:4b:e8	-82 dBm	Infrastructure	None	Not Connected	251	63%	2.437 Ghz (6)	OFDM	ASKEY COMPUT...
FAIRFIELD	802.11g	00:90:96:ff:4c:19	-58 dBm	Infrastructure	None	Not Connected	251	75%	2.437 Ghz (6)	OFDM	ASKEY COMPUT...
FAIRFIELD	802.11a	00:90:96:ff:4c:3b	-88 dBm	Infrastructure	None	Not Connected	251	59%	5.300 Ghz (60)	OFD...	ASKEY COMPUT...
AP#	802.11g	00:1a:70:5a:61:c9	-39 dBm	Infrastructure	None	Not Connected	251	86%	2.462 Ghz (11)	OFDM	Lookup OUI?
FAIRFIELD	802.11g	00:90:96:ff:4c:4f	-82 dBm	Infrastructure	None	Not Connected	251	63%	2.462 Ghz (11)	OFDM	ASKEY COMPUT...
mole	802.11g	00:17:3f:54:4c:dc	-92 dBm	Infrastructure	WPA	Not Connected	251	0%	2.442 Ghz (7)	OFDM	Lookup OUI?
FAIRFIELD	802.11g	00:90:96:ff:4c:68	-79 dBm	Infrastructure	None	Not Connected	251	65%	2.462 Ghz (11)	OFDM	ASKEY COMPUT...
FAIRFIELD	802.11g	00:90:96:ce:c1:c1	-91 dBm	Infrastructure	None	Not Connected	251	58%	2.412 Ghz (1)	OFDM	ASKEY COMPUT...
FAIRFIELD	802.11g	00:90:96:ce:c2:01	-93 dBm	Infrastructure	None	Not Connected	251	57%	2.412 Ghz (1)	OFDM	ASKEY COMPUT...
Motorola	802.11g	00:14:a5:86:00:e2	-93 dBm	Infrastructure	WEP	Not Connected	251	0%	2.412 Ghz (1)	OFDM	Lookup OUI?

Lab Part 3 - Using Network Stumbler and a high gain directional antenna to scan for wireless networks

What you will do in this lab…

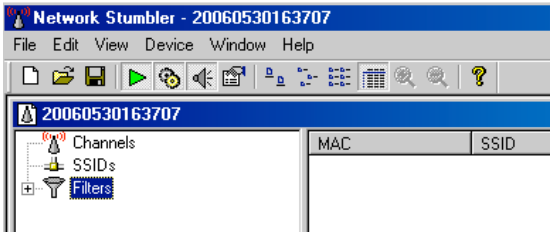
- Configure Network Stumbler
- Use Network Stumbler's AP scanner
- Use Network Stumbler to displays AP's by channel
- Use Network Stumbler to display signal strength of an AP

Introduction: In this Lab, you will first configure Network Stumbler to use the Windows built-in Wi-Fi card and select the NDIS driver for it. Then you will use it to scan and gain information on the Access Points it detects in and around the classroom.

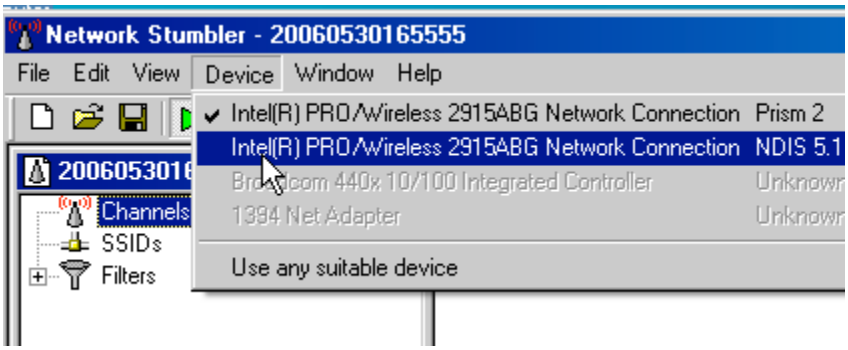
Assuming you have re-booted your notebook into the Windows OS and assuming that your wireless Ethernet card is active but not connected with an AP or AdHoc network, you have met the prerequisites for starting Network Stumbler.

Step 1. Start ***Network Stumbler***. *Start → Wireless Tools → Network Stumbler*

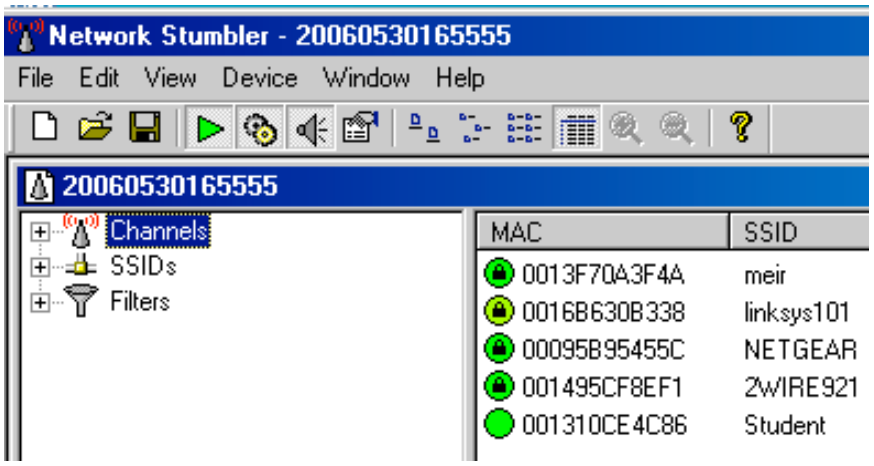
Step 2. When Network Stumbler starts, it typically does not detect any AP's or activity:



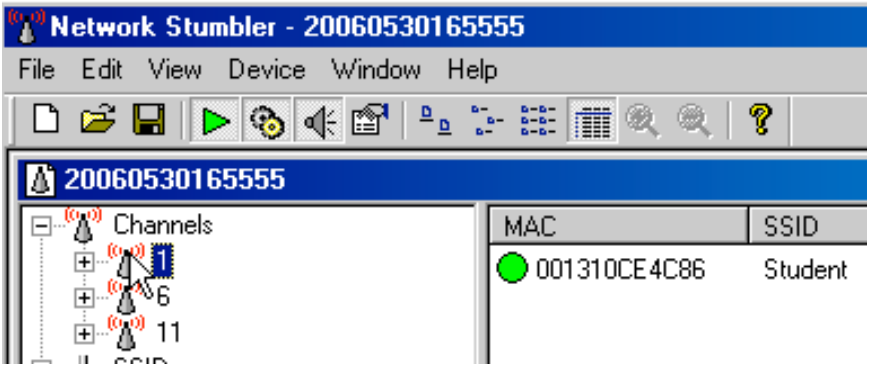
Step 3. This is because you must enable an NDIS driver for your Wi-Fi card. In the Network Stumbler menu, click on **Device**, and select the ***Intel PRO/Wireless 2915ABG Network Connection NDIS 5.1*** driver.:



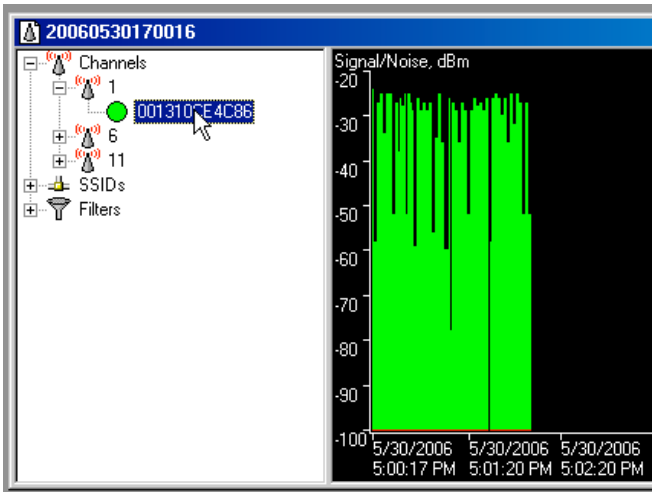
Step 4. Classroom and nearby AP traffic should begin to appear in Network Stumbler:



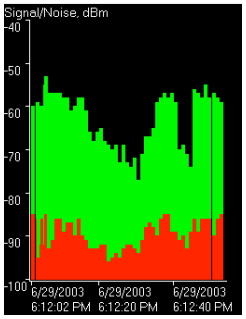
Step 5. **Left click no the + sign** next to Channels and select **channel 1** for classroom AP's (assuming all are on channel 1):



Step 6. To display the signal strength of the selected AP, double-click the MAC address of that AP:

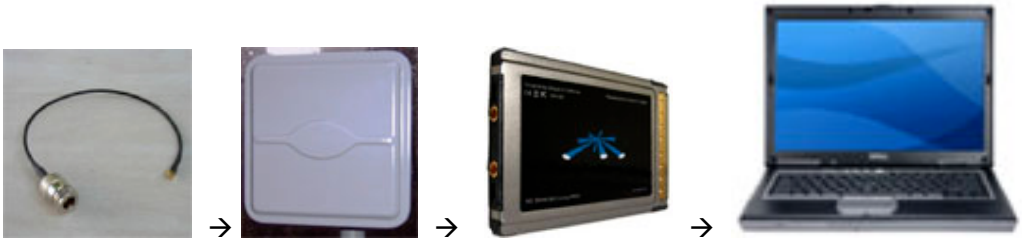


Step 7. Note that the red line along the bottom of the screen is the noise level. If your AP is very near, this line will be very low and will increase as a function of distance from the AP:



Step 8. Network Stumbler's Help menu provides additional information on how to view speed, encryption, IP, and other information about the detected AP's.

Step 9. Plug the high gain directional antenna into the Ubiquiti card.



Step 10. Change the **Device** to ***Atheros AR5004X Cardbus Wireless Network Adapter NDIS 5.1***.

Step 11. Point the directional antenna toward the outside of the building or if possible go outside and point it towards another building.

Step 12. You should see many other wireless networks that are farther away and could not be see with the lower gain antenna.

Do you see any more Access Points with the larger antenna?

_____

You can also try changing to WiFi Hopper and see if it sees any more Access Points when compared to NetStumbler.

What you learned in this Lab:

In this Lab you learned to configure and launch Network Stumbler for Wi-Fi scanning and detection.

1. Configuring Network Stumbler's to use an NDIS driver for the wireless LAN card
2. Selecting AP's by channel or SSID.
3. Obtaining and analyzing signal strength data from AP's.
4. Viewing data organized by channel.
5. Displaying signal to noise ratio from an AP.
6. Obtaining additional information about data available within Network Stumbler.

Lab 2.3: Physically locating an Access Point based on signal strength using WiFiHopper, Zyxel, and AirDefense Mobile

What you will do in this lab:

- Using the raw signal strength identify the location of the Access Point

Lab Part 1 - Open WiFi Hopper and scan for available wireless networks

Step 1. Connect the Ubiquiti wireless LAN card and antenna to the WLSAT laptop.

Step 2. Launch the ***WiFi Hopper*** utility. `Start → Wireless Tools → WiFi Hopper`

Step 3. How many wireless networks are available?

_____

Step 4. How many networks have no security?

_____

Lab Part 2 - Open ZyXEL and scan for available wireless networks

Step 1. Open the ***ZyXel*** utility. `Start → Wireless Tools → Zyxel Utility`

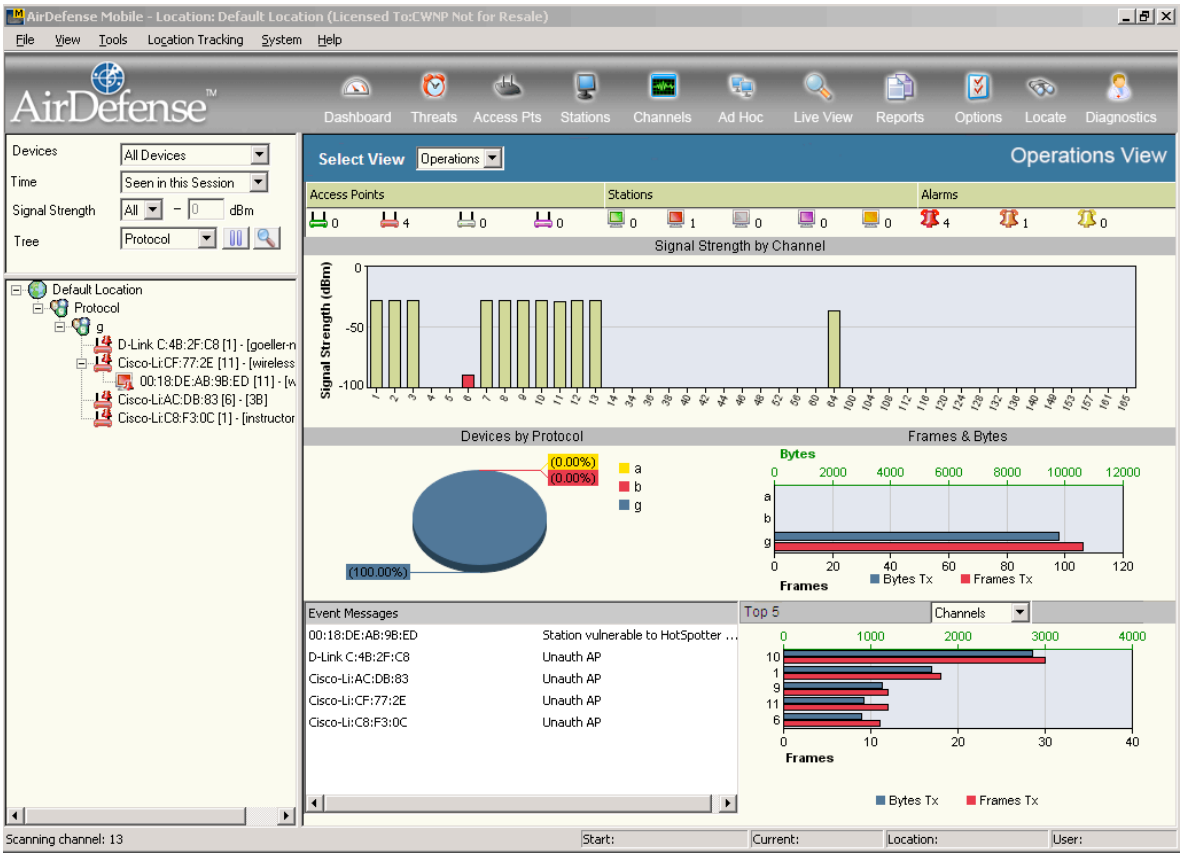
Step 2. While monitoring the signal strength of the AP, walk around the room and locate the AP. Remember the closer to 0 (meaning the higher the negative value) the higher the signal strength.

> A signal strength of -30 indicates you are within 5-10 feet of the AP. Try to see what different type Access Points report – from different distances.

Lab Part 3 - Open AirDefense Mobile and locate wireless networks

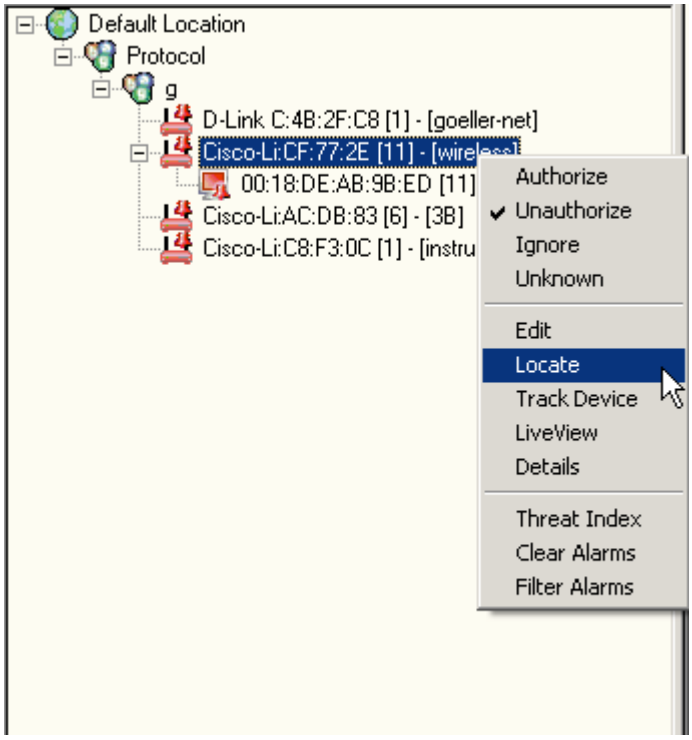
Step 1. Go to **Start → 'Switch to AirDefense Mobile Driver'**

Step 2. Open ***AirDefense Mobile***.

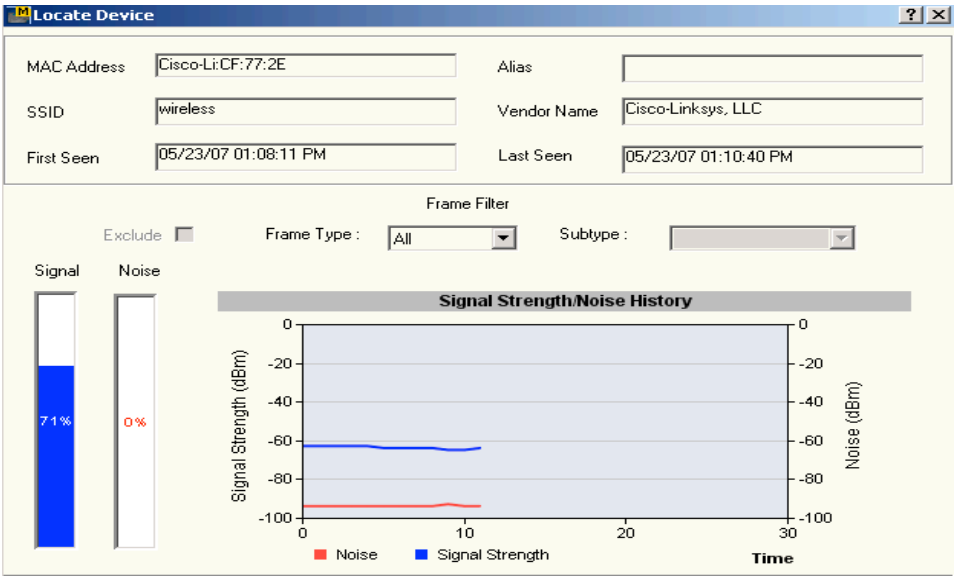


Step 3. **Right click** the ***MAC address*** of the classroom AP.

Step 4. Click **Locate**.



Step 5. While monitoring the signal strength of the AP, walk around the room and locate the AP. The higher the graph the closer you are to the AP.



Step 6. Where is the classroom AP located?

_____

Step 7. Now have someone 'hide' and access point and use these same tools for locating.

What you learned in this Lab:

In this Lab you learned use wireless scanning tools to:

- Identify F signatures

- Scan for AP's using high gain directional antennas
- Locate an AP using a directional antenna and GPS
- Locate an AP using signal strength

Variable

Wispy recording name _____

Lab 2.4: Bluetooth scanning- AirMagnet Bluesweep

AirMagnet Bluetooth Analyzer is a simple, easy-to-use Bluetooth detection and monitoring utility for the Windows platform. It can discover and track any Bluetooth device within its range and display key information about each and every detected Bluetooth device as well as the service or services it provides. With the growing popularity of Bluetooth technology, AirMagnet Bluetooth Analyzer will enable WLAN administrators to effectively guard their networks against security vulnerabilities associated with Bluetooth devices.

Product Information

Source

AirMagnet

Free

www.AirMagnet.com

Where, When, Why

This tool allows you to check the 2.4GHz space for Bluetooth encoded signals. As part of your reconnaissance efforts – this allows one to 'see' the various Bluetooth devices operating in a given area.

Bluetooth is normally a very short-range solution, so to get a throughout view of a client site's Bluetooth activity, you'll need to scan by walking around.

Usage and Features

Device/Service View—allows you to toggle the screen display between device data and service data. The former shows key information about the Bluetooth devices the program discovered within range; the latter displays the service or services each of the devices support.

Tree/List View—enables you to fine-tune the data display by toggling between the list view and the tree view. The former displays the data (i.e., devices or services) in the form of a list; the latter groups the same data by category and displays them in an structured fashion (i.e., tree structure).

Ability to detect and track Bluetooth devices — AirMagnet Bluetooth Analyzer can allows network administrator to easily and effortlessly discover and track Bluetooth devices that are active in the working place so that they act proactively to guard their corporate network against the potential vulnerabilities posed by those Bluetooth devices.

Ability to discover Bluetooth services— AirMagnet Bluetooth Analyzer enables network administrators to quickly and easily find out the service or services any detected Bluetooth device is providing or is able to provide so that they know exactly what is going on in the airspace over the network.

Requirements / Dependencies

- A compatible Bluetooth device

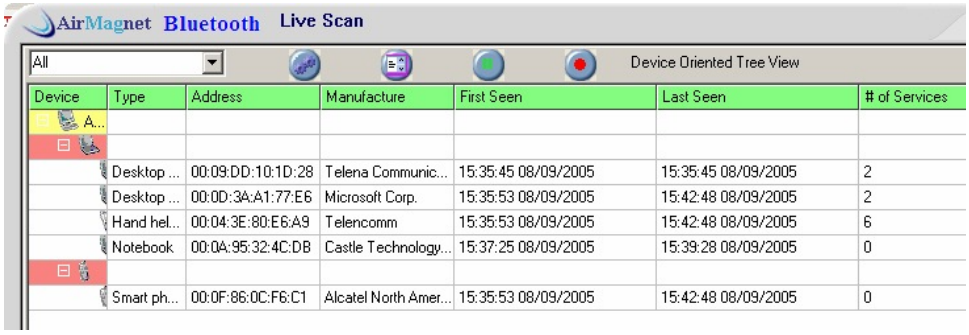
What you will do in this lab:

- Scan your 2.4GHz RF environment for Bluetooth encoded packets

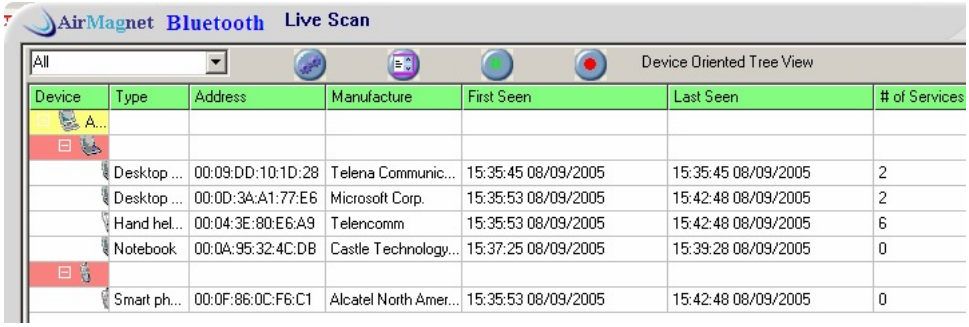
Step 1. Start ***AirMagnet Bluetooth Analyzer***.

The program interface appears on the screen once you have double-clicked the program icon.

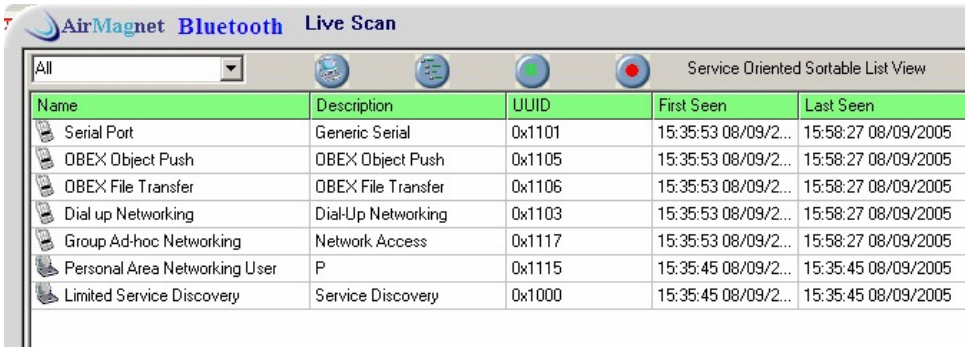
The screen is blank on the start because no data has been captured yet, or because no Bluetooth device is active within range, or because the Bluetooth devices are set in the 'non-discoverable' mode. However, the screen will be populated with data in a few seconds if the program has detected Bluetooth devices.



By default, AirMagnet Bluetooth Analyzer's screen lists all the devices it has detected in Device View, as shown.

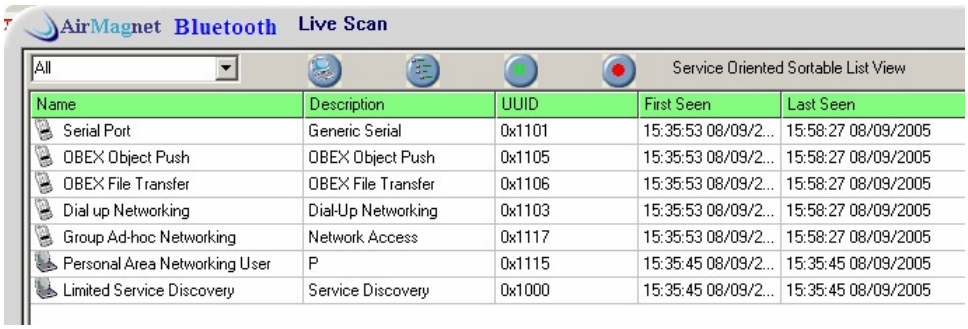


Step 2. You can display the devices by service category by clicking **Service Oriented button**.



This shows all the data in the form of a tree structure, which groups the detected Bluetooth devices into different categories.

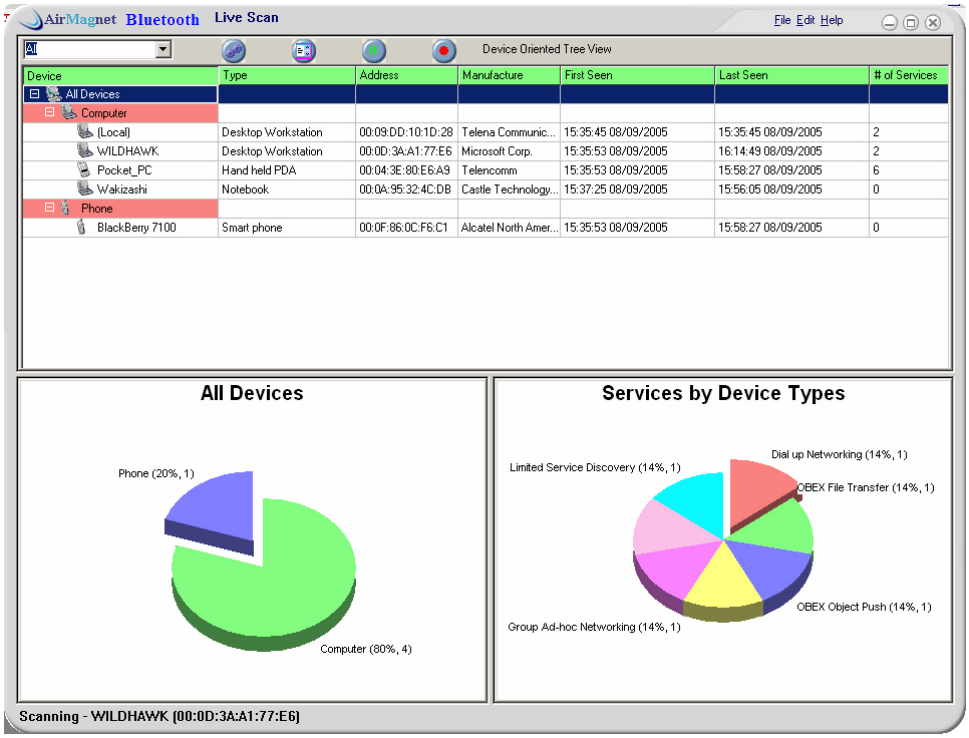
Step 3. You can also display the data in the form of a list by clicking the **List View button**.



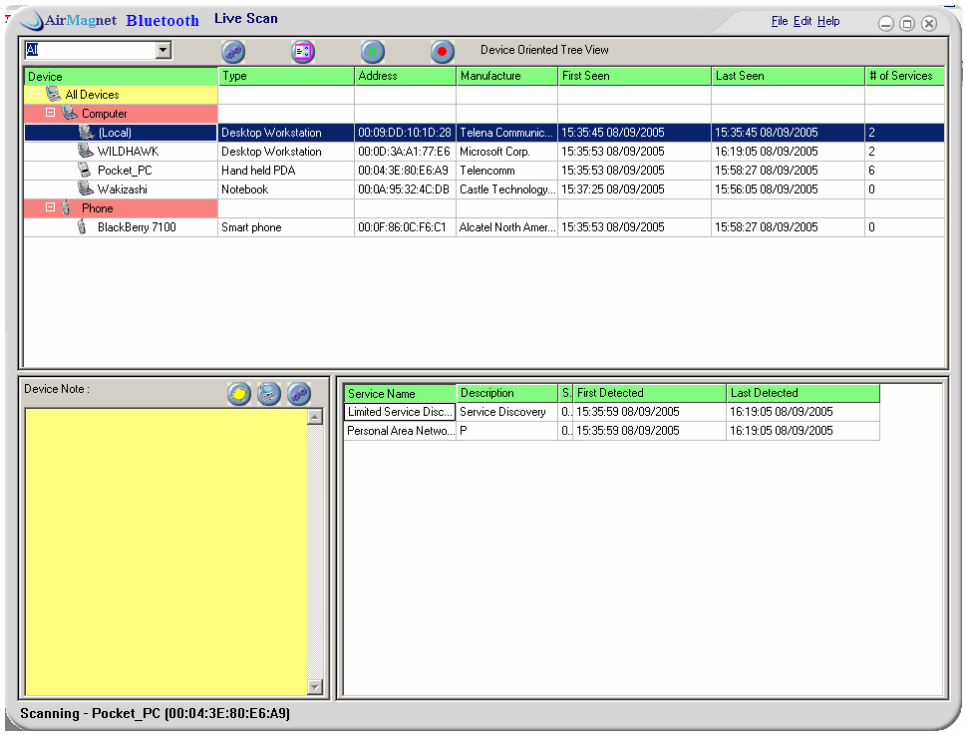
Step 4. The four buttons across the top of the screen are used to navigate through the program:

- Device Oriented/Service Oriented—toggles between Device and Service Views
- Tree View/List View—toggles between Tree View and List View.
- Pause/Resume—Pause or resume the scanning.
- Reset/Start—Clear the data on the current screen and start scanning all over again.

Step 5. Click **All Devices** from the upper part of the screen. The data of the selected entry will show in the lower section of the screen.



Step 6. Click a **Specific Device**. The lower part of the screen will show detailed data about that device.



Lab 2.5: Installing and Using a GPS device

With the eTrex Legend, Garmin has loaded a full basemap of North America into one small unit. The Legend is also designed to provide precise GPS positioning using correction data obtained from the Wide Area Augmentation System (WAAS). This product will provide position accuracy to less than three meters when receiving WAAS corrections.

Additionally – this GPS system comes with a simple easy-to-use RS-232 Serial connection. This way you can add GPS coordinates to many WLAN software tools.

Product Information

Source

Garmin

$149.00

www.garmin.com

Where, When, Why

By adding GPS information to your security assessments, you can build and show 'outside' leakage of WLAN RF signals, as well as plot external Access Points and how then might influence your target location.

Requirements / Dependencies

- Garmin eTrex Legend handheld GPS Receiver
- Owners' Manual, Lanyard, Quick-Start Guide
- Garmin custom connector to 9-pin RS-232 Serial cable
- Requires either a 9-pin serial port or an external 9-pin serial to USB adapter. (your Dell D620 already has a 9-pin serial port)

Where to Go for More Information

- Google GPS Tutorial for more information on GPS in general
- View Introduction to GPS video on your Student DVD

What you will do in this lab:

- Initial Setup of your Garmin eTrex GPS
- Review all five main pages of the GPS Screens
- Configure your Garmin eTrex GPS to speak 'NEMA' and Serial connection so you can use your GPS with your WLAN software packages
- Test connectivity between GPS and your Dell D620 laptop

Lab Part 1 - Initial Setup of Garmin eTrex Legend GPS

To configure your GPS, go through the following steps.

Step 1. Review the features and buttons on your Garmin eTrex Legend GPS by reading Page 2 of the Users Manual.

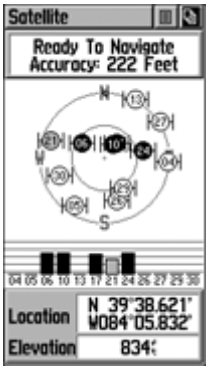
Step 2. Open the back of your GPS by twisting the small metal ring. Insert two AA batteries, following the printed icons for battery polarity, and close the back.

Step 3. Turn on the GPS by pressing the lower button the right side.

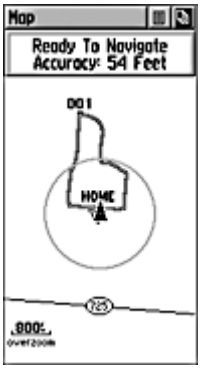
Step 4. Take the GPS outside, or very close to a window, where it can see the sky. It will take up to 10 minutes to do the initial setup and finding of GPS satellites. It will be *much* faster in the future after it figures out where in the world it is.

> **NOTE:** If the unit is off and you change your location drastically, it will take an extended period of time to 're-lock' onto the new locations configuration of GPS satellites.

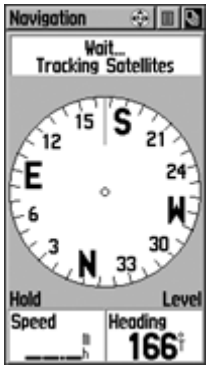
All of the information you need to operate the eTrex Legend can be found on five main pages (or display screens). You can press and release the Page button to cycle through the Satellite Page, Map Page, Navigation Page, Trip Computer, and Main Menu Page.



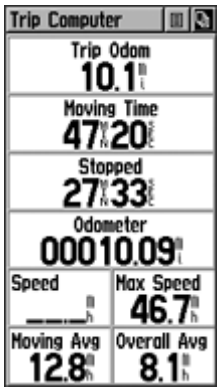
The Satellite Page shows satellite signal strength, displays when the unit is able to navigate, and tells the location by latitude/longitude. There is a "Skyview" graphic that shows the relative position of each satellite as if you were looking up at the sky. This display has each satellite's assigned number labeled. Also shown here are bars indicating signal strength for each satellite. The strength of the signal is represented by the height of the bar.



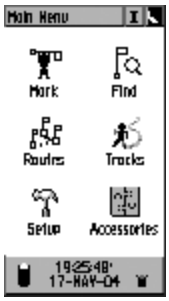
The Map Page displays your present position and direction of movement using a triangular 'Position Icon' that is centered on the map. As you travel, the map display leaves a "trail" (track log) of your movements. The map also displays geographic details such as major rivers, lakes, highways, and towns. A higher level of detail can be obtained by downloading maps from a CD ROM mapping program. The map scale can be changed from 20 feet to 500 miles.



The Navigation Page provides active guidance, with a rotating compass ring that shows your course over ground (track) while you're moving and a bearing pointer to indicate the current direction to your destination (bearing) relative to the course over ground. The Status Window at the top of the page shows you the name of your destination, the distance, and the time to go.



The Trip Computer Page displays up to eight different types of navigation data and are user programmable. Each data field is selectable and can contain one of many data information options. By selecting the information options that you prefer and arranging them in a desired order on the page, you can customize the Trip Computer Page to meet your navigation needs.



The Main Menu provides access to additional eTrex Legend feature pages. From the Main Menu Page you can mark and create new waypoints; find map items such as cities, interstate exits, addresses, points of interest, etc.; create routes; save tracks; setup system operating features; or access and use unit accessories.

Lab Part 2 - Configure your GPS to communicate with Laptop

To configure your GPS, go through the following steps.

Step 1. Turn on GPS with the **Power button** (right side lower button).

Step 2. Press the **'Thumb Stick' twice** to bring up the Main Menu.

Step 3. **Navigate** with the 'Thumb Stick' to the **Setup icon** and press the 'Thumb Stick' to get to the ***Setup Screen***.

Step 4. **Navigate** with the 'Thumb Stick' to the **Interface icon** and press the 'Thumb Stick' to get to the ***Interface Screen***.

Step 5. Press Down on the 'Thumb Stick' to select ***Garmin*** and then press the 'Thumb Stick'.

Step 6. Scroll down to ***NMEA In/NMEA Out*** and then press the 'Thumb Stick' to Select.

Step 7. Note the Baud Rate is set to ***4800***.

Step 8. Navigate to the '**X**' in the upper right hand corner of the screen to exit.

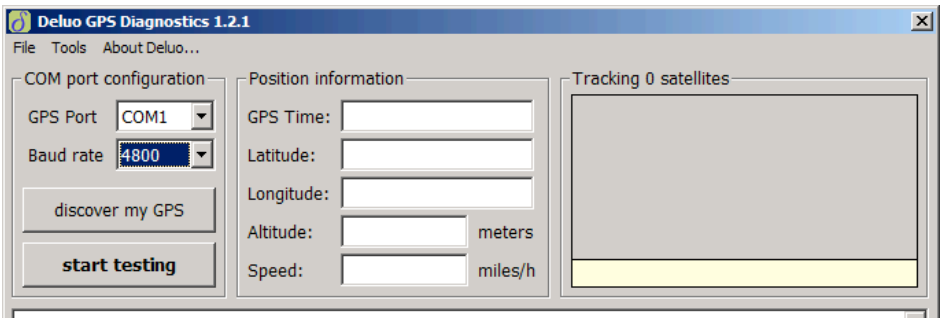
Step 9. You have now configured your GPS to work with WLAN software on your laptop.

Lab Part 3 - Test connectivity between GPS and Laptop

To test the connectivity between your GPS and Laptop, complete the following steps.

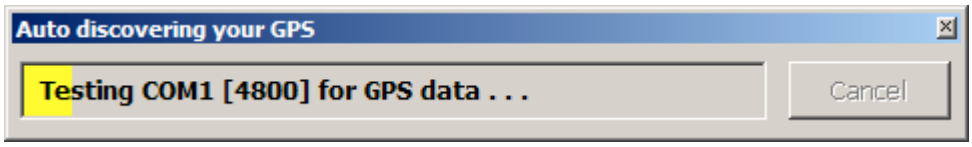
Step 1. Connect the Serial cable to the GPS and to the 9-pin RS-232 port on your Dell D620. (You have to open the little rubber gasket on the top back of the GPS)

Step 2. Start the Deluo GPS Diagnostics software from the Start Menu.

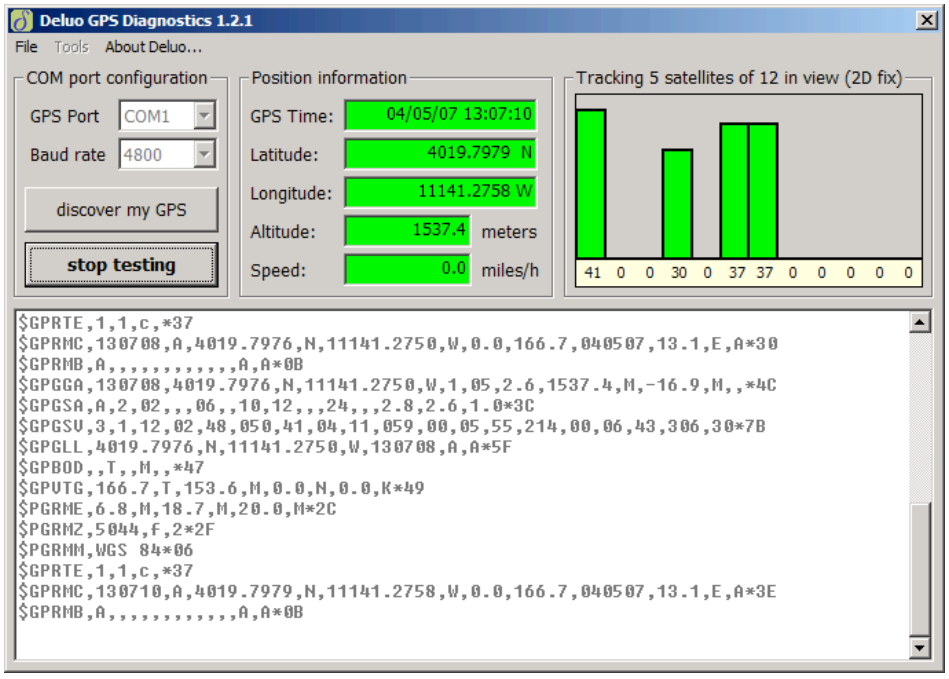


Step 3. Set the GPS Port to *COM1* and the Baud Rate to *4800* then

Step 4. Click on the *Discover my GPS*.



Step 5. To test your connection, click the Stop Testing button.



Step 6. You have now tested your GPS's connection to your laptop.

What you learned in this Lab:

In this Lab you learned to use your Garmin eTrex GPS to:

- Set your initial GPS Location information
- Reviewed all Garmin eTrex Screen
- Configured your GPS to communicate with your Laptop using NMEA Protocol
- Tested the GPS connectivity

Lab 2.6: WarDriving, WiGLE, & Google Earth

NETSTUMBLER.COM

In this lab exercise we'll be using the configured GPS along with the software NetStumbler to do a 'War Drive' to gather information on Access Points. Then process that data into a file supported by Google Earth to plot our War Drive.

Product Information

Where, When, Why

Part of any Wireless LAN Security Assessment is the mapping of external 'leakage' of Access Point signals outside of the target location. In addition, our Wardriving will give us a visual image of not only the client Access Points, but all the neighbors as well.

Using Google Earth, we can make a very professional presentation of this GPS data.

Usage and Features

NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows 98 and above. A trimmed-down version called MiniStumbler is available for Windows CE.

NetStumbler is commonly used for:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in one's WLAN
- Detecting causes of wireless interference
- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links

Google Earth combines the power of Google Search with satellite imagery, maps, terrain and 3D buildings to put the world's geographic information at your fingertips.

- Fly to your house. Just type in an address, press Search, and you'll zoom right in.
- Search for schools, parks, restaurants, and hotels. Get driving directions.
- Tilt and rotate the view to see 3D terrain and buildings.
- Save and share your searches and favorites.

Requirements / Dependencies

- GPS Device communicating with NMEA format
- Wireless NIC Card
- Google Earth Software

Where to Go for More Information

- www.netstumbler.com
- Earth.google.com
- http://www.gpsvisualizer.com/map?form=wifi

What you will do in this lab:

- Configure NetStumbler to use the Garmin eTrex Legend GPS
- Perform a War Drive – Wireless LAN External Site Survey
- Convert the NetStumbler information into Google Earth Format
- View and Analyze War Driving Data with Google Earth
- Use WiGLE Data to show what is available on the Net for your client's site

Lab Part 1 – Configure NetStumber and Perform War Drive

Wardriving is driving around searching for the existence of Wireless LAN (802.11) Networks. It's locating and logging wireless access points while in motion. Often, this task is automated using dedicated wardriving software and a GPS unit.

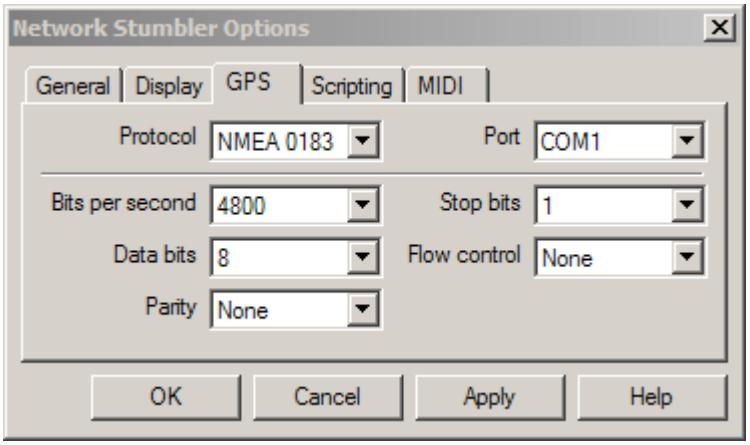
Wardriving was named after wardialing (popularized in the Matthew Broderick movie WarGames) because it also involves searching for computer systems with software that would use a phone modem to dial numbers sequentially and see which ones were connected to a fax machine or computer, or similar device.

The legality of wardriving in the United States is not clearly defined. There has never been any conviction for wardriving, and there is the untested argument that the 802.11 and DHCP protocols operate on behalf of the owner giving consent to use the network, but not if the user has other reason to know that there is no consent.

Step 1. Launch ***NetStumbler***.

Step 2. Go to **View > Options > GPS Tab**.

Step 3.



Step 4. Make sure the **Port is set** to ***COM1*** and the **Bits per second is set** to ***4800 Baud***. Then **click OK**.

Step 5. You can change which Wireless NIC card will be used by NetStumbler by **clicking on the Device menu option** at the top of the program's interface.

> **NOTE:** There are two types of drivers NetStumbler can use. Either the default NDIS driver, or a driver specific for your card. The card's specific driver will give better results

Step 6. For this lab we'll be using the 7dBi external antenna, mounted on the Magnetic Mount platform. Screw the antenna into the mag mount, then in turn screw in the mag mount's other cable end into the short 1' pigtail cable. Then finally put the pigtail's other end into the MMCX port on the Ubiquiti card.

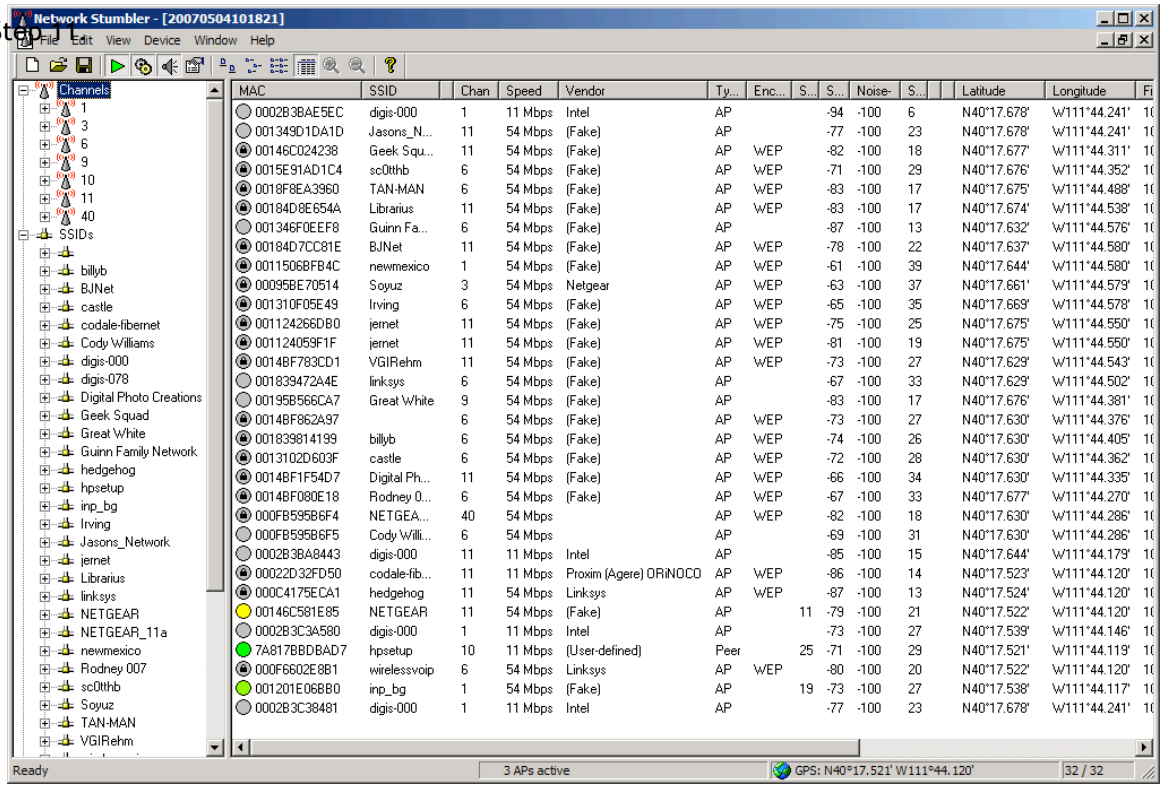
Step 7. You can run the Mag Mount antenna cable through the window of your card. By using the Mag Mount antenna we get the antenna element outside of the metal box of your car for better RF results.

Step 8. NetStumbler will constantly be saving the GPS location along with each Access Point or Ad Hoc network it can see. NetStumbler sends out Probe Requests and tracks the Probe Response results.

Step 9. To start a new capture click on `File New`.

Step 10. Now as you drive around you'll both see and hear as NetStumbler finds new Access Points.

Step 11.



NOTE: NetStumbler will save the GPS coordinate for each Access Point where the signal strength is strongest.

Step 12. Save the file when you are complete. Default location is your My Documents with a unique date/time based file name.

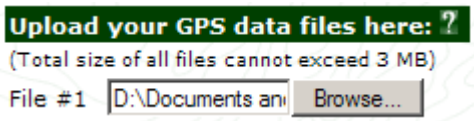
Step 13. Write down your filename here _____.

Lab Part 2 – Convert War Driving Data and Review in Google Earth

NetStumbler saves its data in a unique NS1 file format. We'll need to convert this into a standard file format that can be read and displayed in Google Earth.

Step 1. Open a browser and go to **http://www.gpsvisualizer.com/map?form=wifi**.

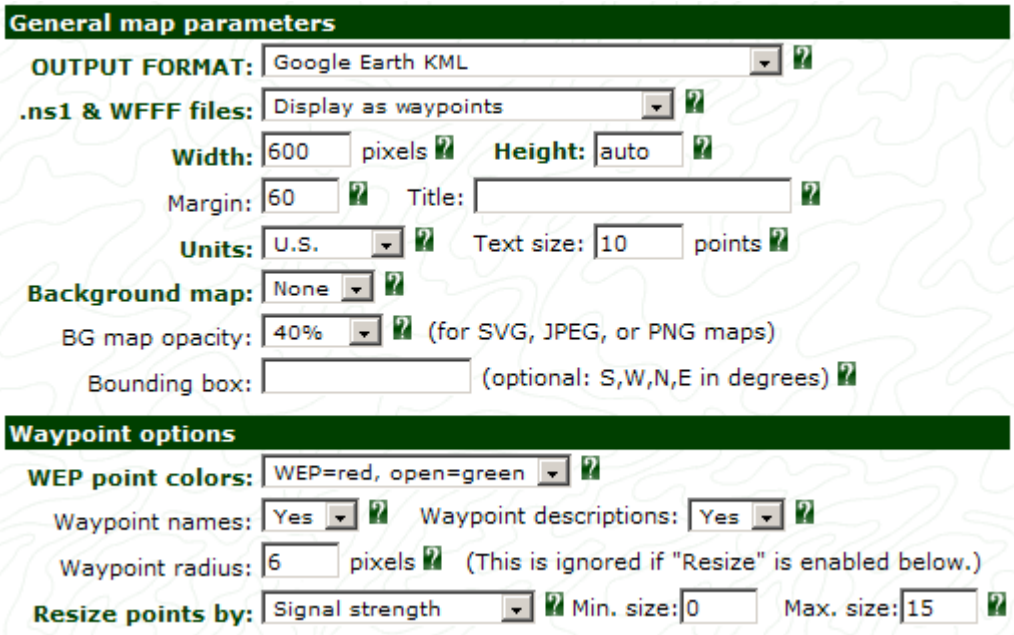
Step 2. Browse to your ***NetStumber*** file with the tools on this web page.



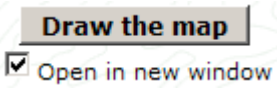
Step 3. Change the Output Format to ***Google Earth KLM***.

Step 4. Change the Waypoint Names and Waypoint Descriptions to ***Yes***.

Step 5. Set the Max Size to ***15***.



Step 6. Then Click **Draw Map**.



Step 7. Your converted file is now ready. Since we have already installed Google Earth on your Dell D620, just click on the file and it will open Google Earth with the new WarDriving Data already included.

Google Earth output

Your GPS data has been processed. Here's your KML or KMZ file:

1178298951-31107-76.164.26.38.kmz

Step 8. You can now use all the Google Earth tools to Zoom In, Move Around, and add different Road or other elements to your Graphic.

NOTE: During the data conversion we had the Encrypted Access Points come in Red and the Open Access Points in Green. Also – The stronger the AP's signal strength the larger the AP circle

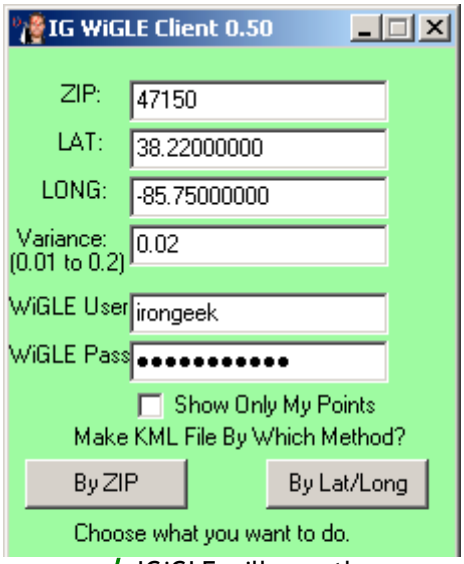
Lab Part 3 – Using WiGLE Data as part of Security Assessment

If you don't have time to do a 'live' WarDrive of your client area, you can take a 'short-cut' and go to a national repository of wardriving data instead. Please note, your actual WarDrive will be current and totally under your control. If you use the WiGLE database information you might be getting outdated plots.

Step 1. Open a browser and go to ***http://www.wigle.net/gps/gps/main/register*** to setup a Wigle account.

Step 2. Open **IGiGLE**.

There are two ways to query data with IGiGLE, by ZIP or by latitude and longitude. Which input boxes are used depend on which button you click, "By ZIP" or "By Lat/Long".



Step 3. Enter the ***ZIP Code*** of your client site.

Step 4. **Leave Variance** at ***0.02***.

The number of degrees to vary the map from it's center point. Don't make it to big, it will take a lot longer, bog down the WiGLE server, and may never return results.

Step 5. Enter your ***WiGLE Username*** and ***Password***. IGiGLE will pass these on when requesting your data from the WiGLE database. If you get an error on the Username/Password. Just try it a second time.

Show Only My Points - Check this box if you only want WiGLE to return Wireless Access Points you found and uploaded to the database yourself.

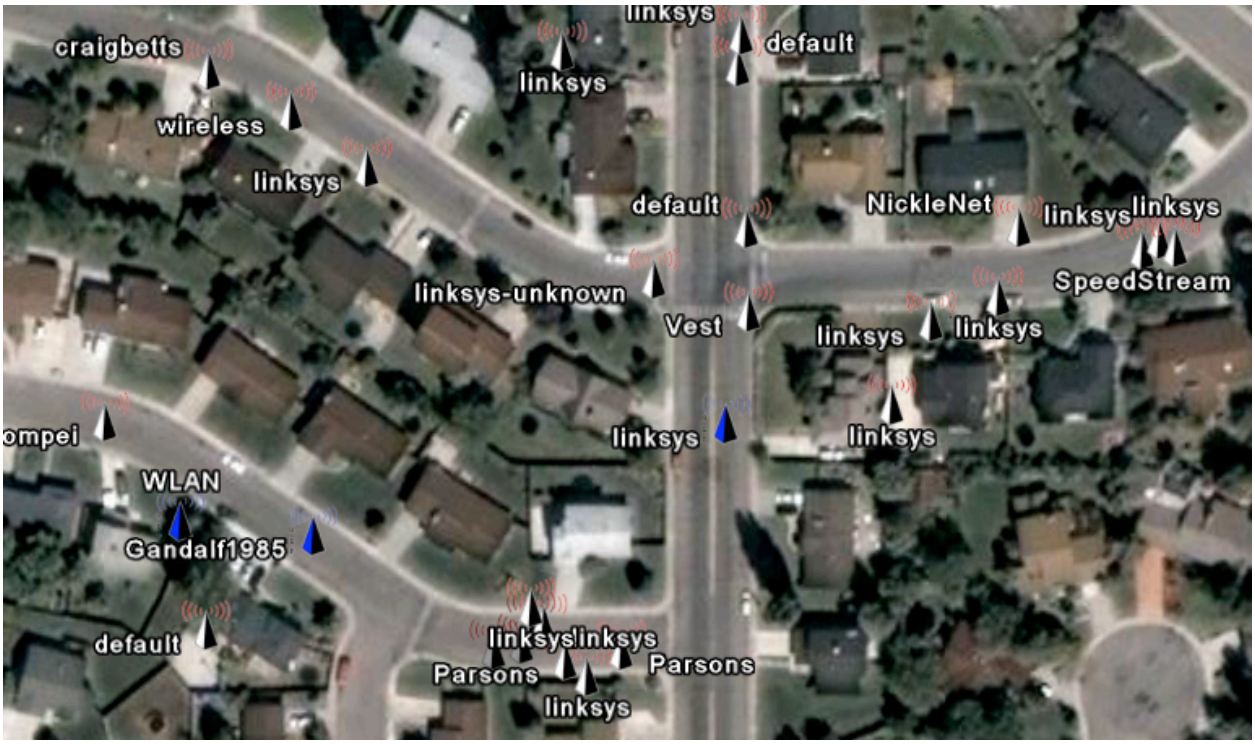
Step 6. Click the **By ZIP button** to generate your KML file based on the United States ZIP code. The LAT and LONG text boxes will be ignored.

By Lat/Long - Click this button to generate your KML file based on a given latitude and longitude. The ZIP text box will be ignored.

> **NOTE:** You may get some errors if your query is too big (a large variance or a place with a lot of WAPs close together). If you have problems getting a result try modifying your variance to be smaller, double check you user name and password, or try again later. Depending on the kind of load WiGLE is under at the time of your query, your results may vary.

When IGiGLE runs its query it first downloads the data to a tilde delimited text file in the same directory as the EXE, called either "<ZIP>.txt" or "<LAT-LONG>.txt" depending on which button you used. After the raw data is downloaded, IGlGLE will make a KML file with all of the wireless network SSIDS in it, called either "<ZIP>.kml" or "<LAT-LONG>.kml".

Step 7. **Double click** on the ***saved KLM file*** and it should open up in Google Earth.



You will notice when you open the KML file that there are two different icons for WAPs:

The one on the left is for Access Points without WEP/WPA and the one on the right is for ones with WEP/WPA enabled. Also you'll notice that the WEP and Non-WEP 802.11 access points are split into two folders, this is so you can easily choose to view only open or closed WAPs if you want to. By clicking on a WAPs icon you can find more details about it, such as its BSSID.

Step 8. Review your new WarDriving Map in Google Earth.

Step 9. Each individual Access Point has detail information – SSID, and MAC Address of the AP.

Note: If your client's wireless networks are available on WiGLE, anyone with network access can learn and use their WLANs. This is a great first pass for WLAN reconnaissance.

Lab 2.7: Using Kismet

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

Product Information

Source

Kismet

Free / Open Source

www.kismetwireless.net

Where, When, Why

Using the CACE Technologies USB AirPcap, Kismet can also run on a Windows Platform.

Use this tool to find 'Cloaked' Access Points. NetStumbler uses active scanning to find APs, Kismet is Passive and can even find 'Cloaked' APs who have turned off their Broadcast SSID.

Usage and Features

Kismet detects the presence of wireless networks, including those with hidden SSIDs. It can discover and report the IP range used for a particular wireless network, as well as its signal and noise levels. Kismet can also capture or "sniff" all network management data packets for an available wireless network. You can use Kismet to locate available wireless networks, troubleshoot wireless networks, optimize signal strength for access points and clients, and detect network intrusions.

Requirements / Dependencies

- For Windows platforms you must use AirPcap as the capture source
- Under Linux, many Wireless NIC cards can be used

Where to Go for More Information

- http://www.kismetwireless.net/index.shtml

What you will do in this lab:

- Load AirPcap Drivers (in previous lab)
- Start Kismet
- Analyze local Wireless Traffic

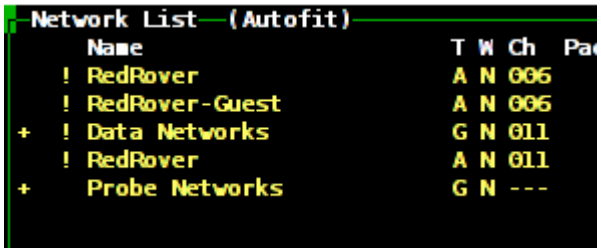
Lab Part 1 - Using Kismet for Windows with AirPcap

Kismet is a passive sniffer. Unlike NetStumbler, which broadcasts a request for access points responding to the SSID name "ANY," Kismet does not send any packets at all. Instead, Kismet works by putting the wireless client adapter into RF monitor mode. While in so-called "rfmon" mode, the wireless client is not (and cannot be) associated with any access point. Instead, it listens to all wireless traffic. Consequently, your wireless card cannot maintain a functional network connection while under Kismet control.

Users often report that Kismet finds more APs than NetStumbler. This is because NetStumbler only knows about access points that respond to its "ANY" SSID probe request. Some network administrators configure their APs not to broadcast, or to "hide" their SSID. These do not respond to NetStumbler's probe. Because the AP blanks out its SSID, Kismet will detect its presence, but without a network name. However, when a legitimate client associates with that AP, its real SSID is included in the initial handshake. Because Kismet sees all network management traffic, it will pick up these packets and discover the SSID which was supposedly "hidden."

Step 1. Confirm ***AirPcap*** drivers are loaded by inserting the AirPcap USB NIC in USB port.

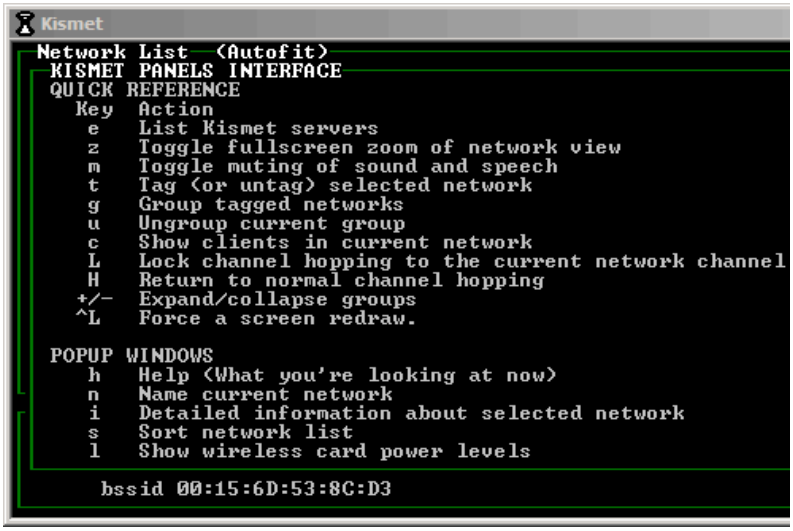
Step 2. Start **Kismet**.



Kismet shows the list of detected wireless networks. They are initially sorted in "Autofit" mode, which does not present the networks in a specific order.

Step 3. Press **"s"** to bring up the sort menu, where you can order the SSID's by name, chronology, and other criteria.

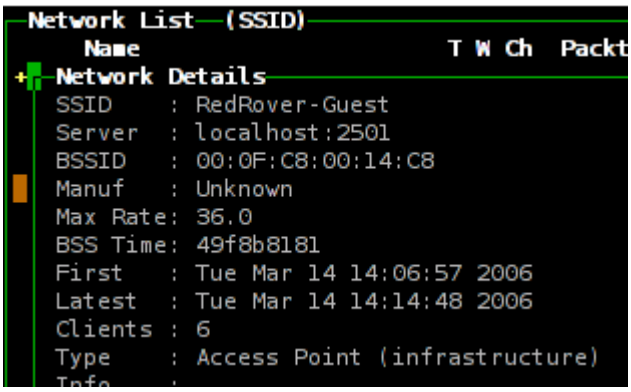
Step 4. You can press "h" in Kismet to pop a chart of key commands.



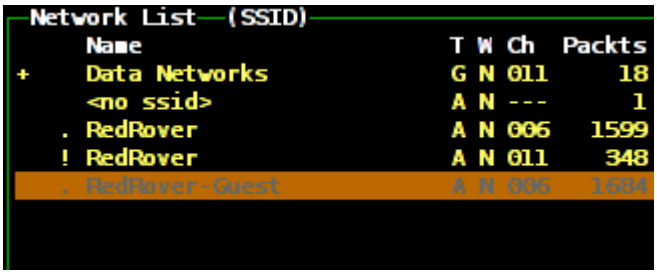
With the network names sorted, you can use the up/down arrow keys to navigate through the list.

Step 5. Press "i" on a network to see a detailed view of that particular network.

> **NOTE:** This doesn't work in the 'Autofit' default sort. You have to change to a different sort with 's' then one of the choices in order for detail view to work.



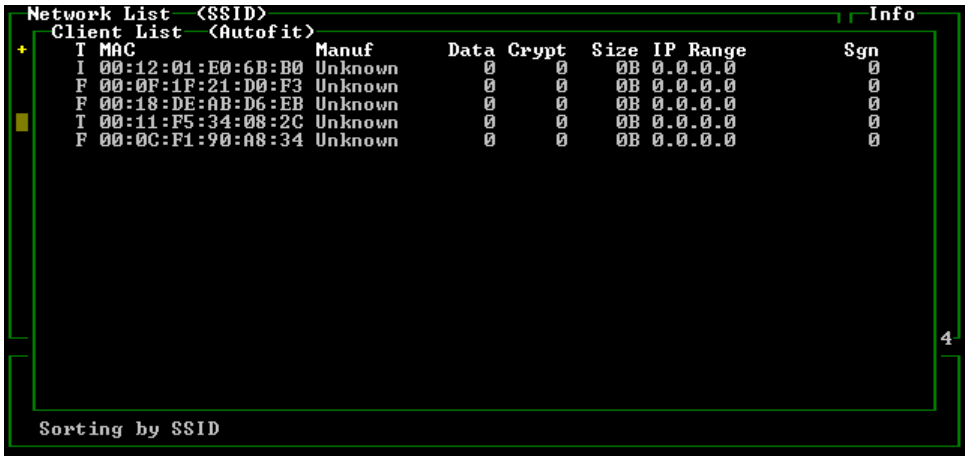
Step 6. Press the "l" key in Kismet to pop up signal strength data.



The wireless card power window is especially useful in troubleshooting wireless connections for source of noise, or optimizing locations of access points for maximizing signal strength within a space.

> **NOTE:** We've found this isn't the most stable of Kismet environments – but it should do in a 'pinch' if you don't want to run a Linux version.

Step 7. Selecting a **network**, then clicking on **'c'** will give you a list of clients associated with an Access Point.

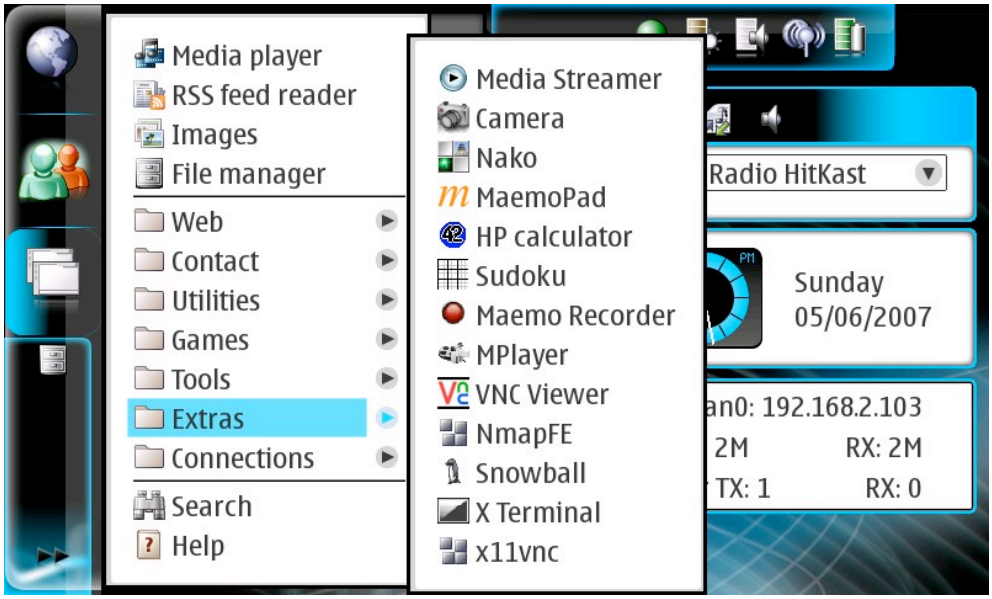


Type 'q' to return to the previous screen.

Lab Part 2 - Using Kismet on the Nokia N800

Use kismet on the Nokia N800 as a very portable discovery tool for 802.11 networks.

Step 1. Since ***Kismet*** is run from the command line we need to open up a terminal window by choosing the **main menu** (the twin windows icon), then **Extras**, then X Terminal.



Step 2. Now that a terminal window has appeared we can properly setup our environment for using kismet.

Step 3. We need root privileges in order to use kismet. There are dirtier ways to gain access to root on the N800 but we are going to use a less problematic method; use ssh to login to ourselves.

Type **`ssh root@127.0.0.1`**

Then you will be asked to supply the root password which is '***`rootme`***' by default.

```
~ $ ssh root@127.0.0.1
root@127.0.0.1's password:
```

You might have to type 'Y' to continue since 127.0.0.1 is an untrusted (though local) address.

You will know that you are properly logged in as 'root' because the prompt will change the display Nokia-N800-10:~#

Step 4. Now simply type **`kismet`** at the prompt. Keep in mind that this will enter your network card into monitor mode which means that you will lose any active connection or will not be able to establish any connection until your card is properly placed back into managed mode. Most of the time kismet will properly place your card into this mode upon a proper exit (using 'Q'). If not you will have to reboot.

```
BusyBox v1.1.3 (Debian 3:1.1.3-3.sdk3) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $
```

NOTE: There are known problems with the stock drivers for the wireless interface when in monitor mode. Symptoms include wireless interface not ever being able to exit monitor mode without rebooting the device, network features freeze, applications hang, etc. The temporary fix for this is to simply reboot your machine until better drivers are coded.

Step 5. Everything from this point on is the same as the tutorial from a previous lab. Keep in mind that due to the nature of the drivers some functionality may cause your device to lock up but basic functionality should not case any harm. **Just make sure you exit kismet with 'Q'!**

What you learned in this Lab:

In this Lab you learned to configure and launch Kismet for Wi-Fi scanning and detection.

1. Setting up Kismet's data collection directory
2. Obtaining and analyzing data from your own Linksys AP
3. Obtaining and analyzing data from other AP's