WhirlWind

Table of Contents

Table of figures

Table of tables

WhirlWind

The proliferation of wireless networks and mobile devices has untapped enormous new productivity potential for organizations that rely on corporate communications and rapid decision making. However, an increased level of security risks has been created as well. The widespread use and continuing expansion of wireless and mobile technologies is forcing government and commercial organizations and their IT security departments to seek tools to help them assess the risks of wireless networks and monitor them for potential attacks. Attacks of the wireless environment and employee misuse threaten to erase the gains in productivity realized through wireless and mobile devices. Organizations need to protect proprietary data and assets, not only within their corporate boundaries, but across the physical walls of their facilities into the outside wireless environment as well. Rarely are any such security policies in place to provide guidance on the use of wireless technologies or enumerate responsibilities.

Part of the problem of securing wireless technology is the low cost and ease with which these devices can be purchased. Wireless access points bought through the local computer/electronics stores generally are cheap and easy to install. Users take these products out of the box and deploy them without thought of configuration or security. The relative ease with which these products can be deployed is evidenced by the large number of wireless networks left with their factory default names, such as “linksys” and “dlink,” which remain unchanged by the user. Activation and implementation of the associated encryption modules more-often-than-not, are not utilized. Or if used, the minimal protection of Wired Equivalent Privacy (WEP), which can be easily cracked by hacker tools, is employed. Another threat is present when mobile users connect to public wireless networks with common names such as “tmobile” or “attwifi.” Mobile users connecting to these public networks offer unscrupulous individuals an opportunity to steal personal information or sensitive corporate information if they have not taken prior security precautions to protect their information from interception. Thus, the wireless and mobile environment is “prime” for a variety of standard hacker attacks such as sniffing, spoofing, man-in-the-middle, and wardriving.

It is this final item, wardriving, with which WhirlWind is concerned. Wardriving is the undertaking of surveying the wireless networks in a given area (usually by driving) and cataloguing the wireless access points detected based on their network name, security features, and other relevant characteristics. Hackers perform wardriving to find vulnerable networks to attack. Security professionals can perform wardriving against their own wireless networks using WhirlWind to find their own vulnerable networks before the hackers do and to correct the security problems before costly data breaches occur. WhirlWind organizes and displays the collected information about wireless networks in the easy-to-use Google Earth™ mapping application.

Introduction

Futures Inc. is a network security company headquartered in the Baltimore/ Washington, D.C. metropolitan area. The company has, and continues to provide leading-edge Information Assurance/Security products and services to commercial and government customers since 1996. In line with that vision, the security engineers and network analysts of Futures Inc. have developed another product for use in the security community – **WhirlWind**. This document serves as the users' manual for WhirlWind versions: Bronze, Silver, Gold and Platinum. All versions DO NOT have all capabilities. Each version is described in detail within the WhirlWind Features section.

Background

DDST stands for: *"Deployable, Disposable, Security Technology."*
DDST packages tools to create your deployable network solution, configurable to your unique requirements, creating bootable CD media to perform network monitoring, and intrusion detection and information collection at a low cost in materiel and user training. WhirlWind is built on DDST. It was created to allow someone to perform a wireless survey without knowing how to install tools, setup configuration files, etc. Simply place the CD-ROM in a computer system with a WiFi card (listings provided at Table 1) and a USB GPS device (listings provided at Table 3) and you can wardrive (survey) an area as well as collect GPS coordinates for points at which a network can be accessed. From system startup, WhirlWind can be ready to wardrive within 2 minutes.

Once the wardriving is completed, the resulting data set is automatically sent to an application called DustDevil for conversion into a Google Earth™ mapping file. Examples of mapped data sets can be found in the "Data Sets Mapping Display" section.

Scope

The design of WhirlWind is to catalog wireless network activity in a targeted environment to glean insight into that environment. Some of the benefits of this survey would be to determine access point identification and level of encryption (if any). This document describes capabilities and operation of WhirlWind at a high level. WhirlWind runs on most computer systems, may be (depends upon user options selected) non-invasive to operating system or data already loaded onto the hard disk drive(s), and is easily portable and disposable.

WhirlWind Overview

The purpose of WhirlWind is to be a rapidly deployable wireless network monitoring/collection product that is small, simple, inexpensive, disposable, and all the time remaining invisible to the wireless networking environment. WhirlWind catalogues activity on a wireless environment to glean insight into the types and volumes of activity. The product runs entirely within the RAM (Random Access Memory) of the host and has no interaction with the system or data "loaded" onto the storage media of the system unless the user directs it to do so. Upon a re-boot (with the CD removed), the host system reverts back to the state it was in prior to using the WhirlWind CD.

System Requirements

- Intel x86 or equivalent system.
- Adequate Memory – 256MB is recommended, if not using system memory for storage of data. If system memory is being used to store data, (which will be lost upon shutdown of the system) then 512MB of memory is recommended.
- For WiFi use: PCMCIA slot, USB port, or built-in miniPCI slot.
- Compatible WiFi device. A list of compatible devices is provided (See Appendix A, Table 1 – Tested WiFi Cards), but is not all inclusive.
- For Storage: System memory, USB device, Firewire device, internal hard drive (resulting in host modification), PCMCIA storage device, etc.
- For GPS (for collecting GPS coordinates): USB GPS device or USB-to-serial converter for serial GPS device. See Appendix C, Table 3 – Tested GPS Devices.
- System capable of booting from CD-ROM drive.

WhirlWind Features

Currently, there are four versions of WhirlWind (Bronze, Silver, Gold, and Platinum). The Bronze version is a build with a session limit of one (1) hour. Otherwise, Silver will be the initial production version. The following highlights the features of WhirlWind. Additional features are in testing as this document goes to print.

General Features

- Stealth WiFi Survey builds.
- Able to utilize just about any PC/Laptop with use of PCMCIA, USB, internal and mini PCI WiFi card. Use of GPS is optional, but recommended for DustDevil output file.
- Able to store data on USB/Firewire or internal storage device for analyzing data at a later time.
- DustDevil created specifically for converting WhirlWind datasets to mapping data sets, e.g., Google Earth™.
- Utilizes Kismet within build.
- Kiosk like environment.

WhirlWind - Bronze

- Evaluation version, only.
- System is limited to 1 hour of functional use per boot.
- Same functionality as WhirlWind Silver.

WhirlWind – Silver

- Strictly a WiFi survey tool.
- No WiFi traffic collection.
- All Kismet output (GPS, CSV, etc.) will be stored to the selected storage device.
- Futures' modified Kismet for BSSID locking.
- 1 WiFi device, users choice, if multiple are found.
- DustDevil breakdown of information for Google Earth™ Mapping of network locations.
    - After quitting kismet, or shutting down the system and prior to "umount"ing the storage device, run DustDevil against the data in the storage directory. Put the output from DustDevil into the same storage directory. This will allow user to immediately look at data on another system when completed.

WhirlWind – Gold

- All the features of WhirlWind Silver.
- WiFi traffic collection system.
- PCAP compliant dump files.

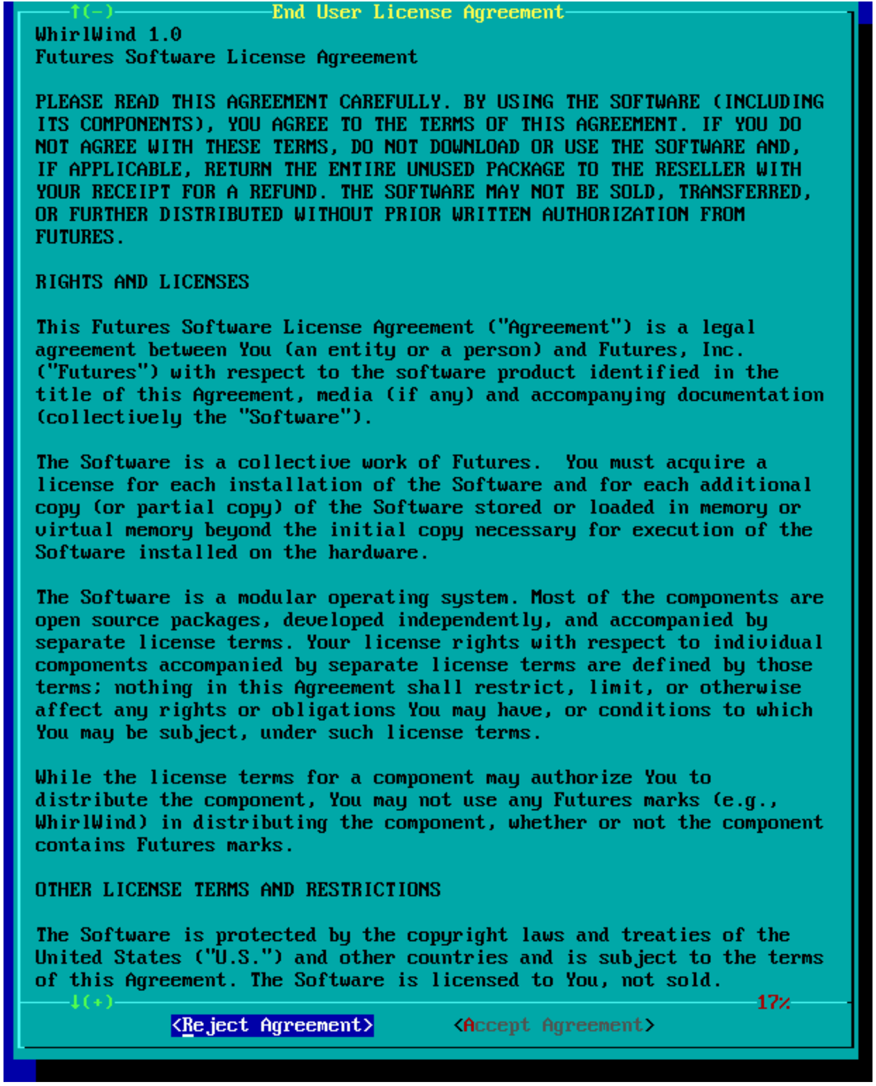
WhirlWind – Platinum

- All the features of WhirlWind Gold.
- Ability to enable/disable GPS use for mapping.
- Ability to enable/disable collection of network traffic.
- Capability to utilize more than 1 WiFi device.
- The user has the ability to assign specific channels to cards, or assign channel hopping to cards.
- Testing has proven 14+ cards usable by the system at one time.

Booting the system

To boot the WhirlWind system, insert the WhirlWind CD-ROM and power on the system. Some systems may require you to reconfigure the BIOS to enable booting from CD-ROM. Upon booting the system with WhirlWind, there will be a user license agreement that the user must accept before WhirlWind continues the boot process. Please use the <Tab> key to move from [Reject Agreement] to [Accept Agreement] and press <Enter> or <Return> to continue. The <up arrow> and <down arrow> keys may be used to scroll through the agreement. Failure to agree to the terms will result in WhirlWind aborting the boot sequence. Please see Appendix D of this manual for a copy of the complete license agreement.

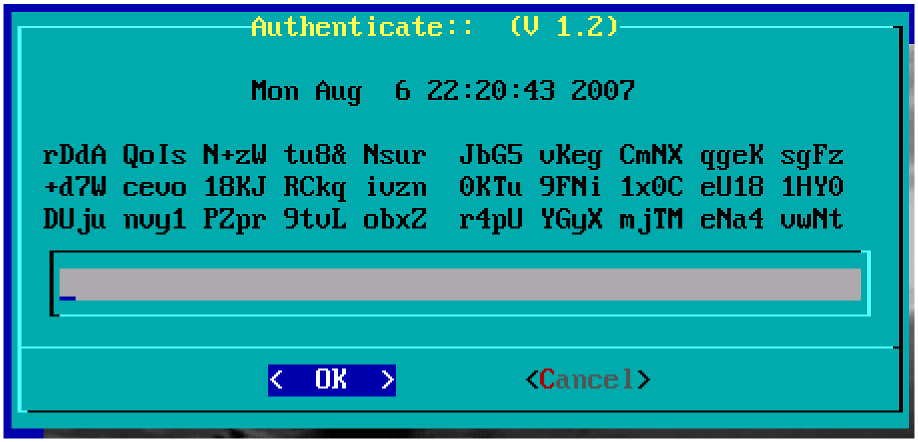
Figure 1



```
WhirlWind 1.0
Futures Software License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY. BY USING THE SOFTWARE (INCLUDING
ITS COMPONENTS), YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO
NOT AGREE WITH THESE TERMS, DO NOT DOWNLOAD OR USE THE SOFTWARE AND,
IF APPLICABLE, RETURN THE ENTIRE UNUSED PACKAGE TO THE RESELLER WITH
YOUR RECEIPT FOR A REFUND. THE SOFTWARE MAY NOT BE SOLD, TRANSFERRED,
OR FURTHER DISTRIBUTED WITHOUT PRIOR WRITTEN AUTHORIZATION FROM
FUTURES.

RIGHTS AND LICENSES

This Futures Software License Agreement ("Agreement") is a legal
agreement between You (an entity or a person) and Futures, Inc.
("Futures") with respect to the software product identified in the
title of this Agreement, media (if any) and accompanying documentation
(collectively the "Software").

The Software is a collective work of Futures.  You must acquire a
license for each installation of the Software and for each additional
copy (or partial copy) of the Software stored or loaded in memory or
virtual memory beyond the initial copy necessary for execution of the
Software installed on the hardware.

The Software is a modular operating system. Most of the components are
open source packages, developed independently, and accompanied by
separate license terms. Your license rights with respect to individual
components accompanied by separate license terms are defined by those
terms; nothing in this Agreement shall restrict, limit, or otherwise
affect any rights or obligations You may have, or conditions to which
You may be subject, under such license terms.

While the license terms for a component may authorize You to
distribute the component, You may not use any Futures marks (e.g.,
WhirlWind) in distributing the component, whether or not the component
contains Futures marks.

OTHER LICENSE TERMS AND RESTRICTIONS

The Software is protected by the copyright laws and treaties of the
United States ("U.S.") and other countries and is subject to the terms
of this Agreement. The Software is licensed to You, not sold.
```

Figure - 1 User Agreement

Immediately after the User License Agreement is the authentication challenge. It will look like the following figure.



```
Authenticate::  (V 1.2)

Mon Aug  6 22:20:43 2007

rDdA QoIs N+zW tu8& Nsur  JbG5 vKeg CmNX qgeK sgFz
+d7W cevo 18KJ RCkq ivzn  0KTu 9FNi 1x0C eU18 1HY0
DUju nvy1 PZpr 9tvL obxZ  r4pU YGyX mjTM eNa4 vwNt
```

Figure - 2 Authentication Challenge

The first line contains the host system's internal hardware clock date/time setting. The next 3 lines contain 10 groups of 4 characters each. These values have different content each time the authentication is presented.

The bottom box is for the user to enter a response to the challenge. Asterisks (*) will be echoed in the place of characters entered. The authentication phrase is dependent upon the specific contents of the CD, which are customer specific. A supplemental instruction sheet is provided to each customer giving specific instructions for authentication.

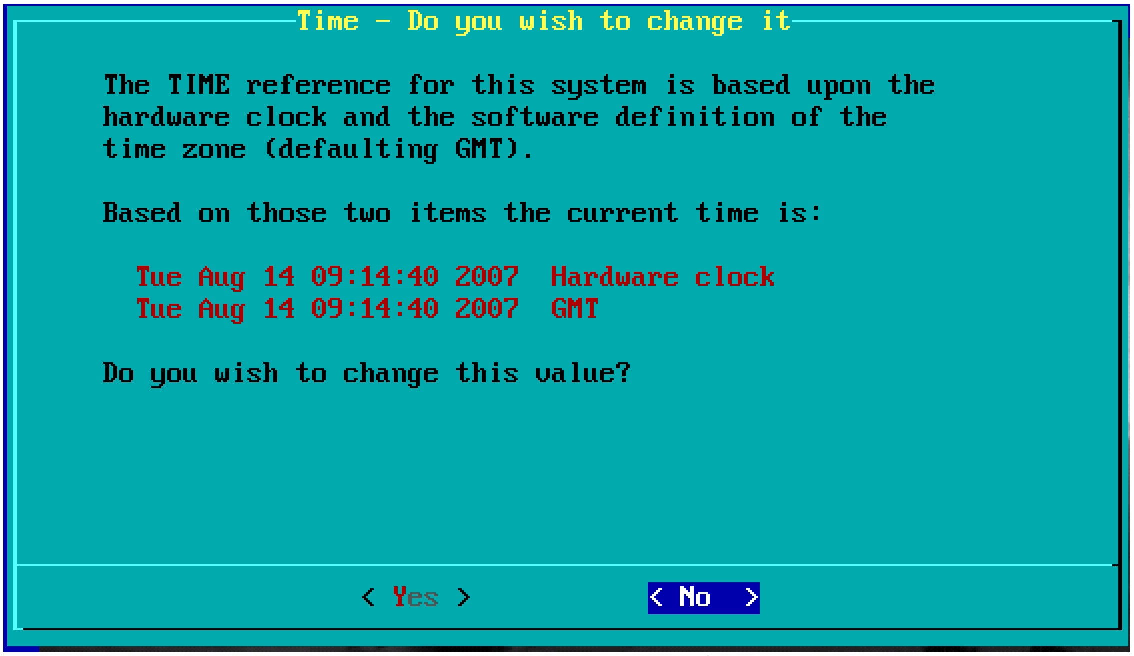
After typing the authentication phrase, press <**Enter**> or use the **<Tab>** key (if needed) to ensure the **[OK]** button is highlighted (as in the image). Then press the **<Enter>** key.

After the system receives the authentication phrase, the screen will then clear. If the authentication phrase was correct, the user will be asked to wait a moment ("One moment…please") and then the boot process will proceed.

If the authentication fails, (incorrect authentication phrase, pressing the **<Esc>** key or the **<Cancel>** button), the system will not start. To re-attempt system startup, **the user must re-cycle power to the computer**.

After authentication, the next screen is the Time Reference screen. This screen will time out and proceed with the current time in 30 seconds if there is no user interaction. This step allows setting WhirlWind's system time. The time is obtained from the RTC (Real Time Clock) chip on the machine. There is no way for the product to know what time zone or locality it represents. The software is set to UTC (Zulu) time zone.

The user is shown the following dialog and given the option to change the time value within the WhirlWind OS (Operating System). Altering the time on WhirlWind **will not** change the RTC chip value or the time on the underlying native OS.

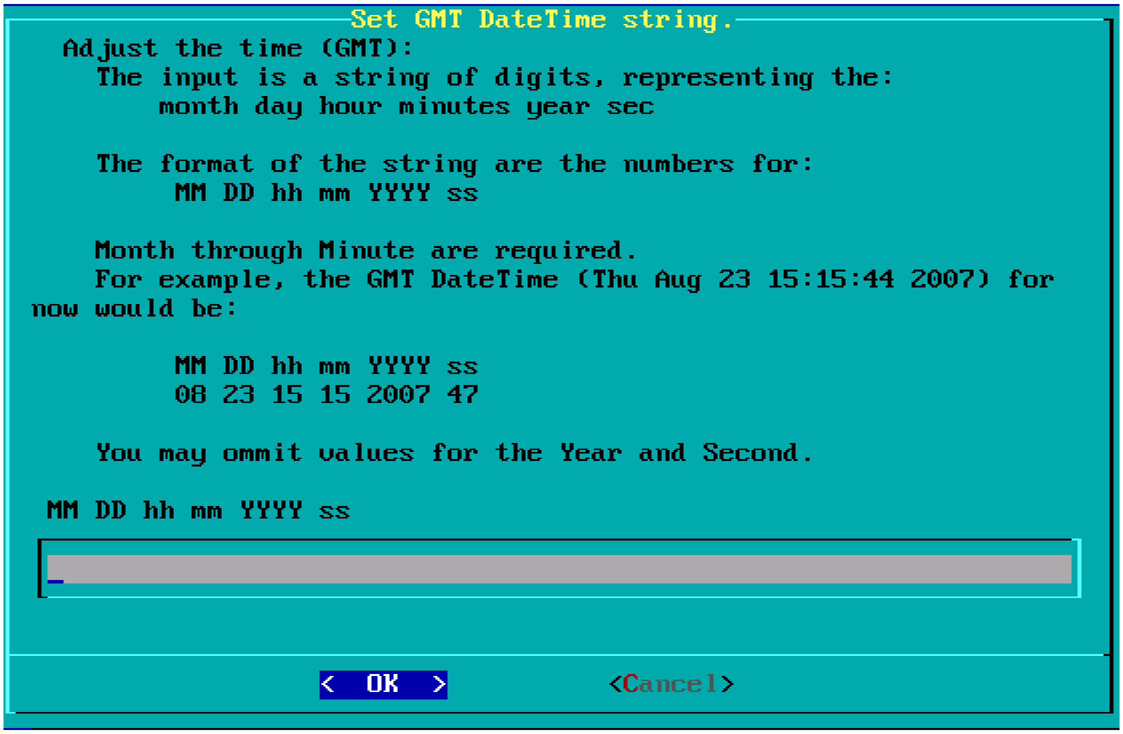


```
Time - Do you wish to change it

The TIME reference for this system is based upon the
hardware clock and the software definition of the
time zone (defaulting GMT).

Based on those two items the current time is:

  Tue Aug 14 09:14:40 2007  Hardware clock
  Tue Aug 14 09:14:40 2007  GMT

Do you wish to change this value?
```

Figure - 3 Time Reference Choices

The default answer is **[No]**. Press **<Enter>** to proceed. If a change is needed, use the **<Tab>** key to highlight the **[Yes]** button and press **<Enter>**.

The following screen illustrates setting of the OS time.

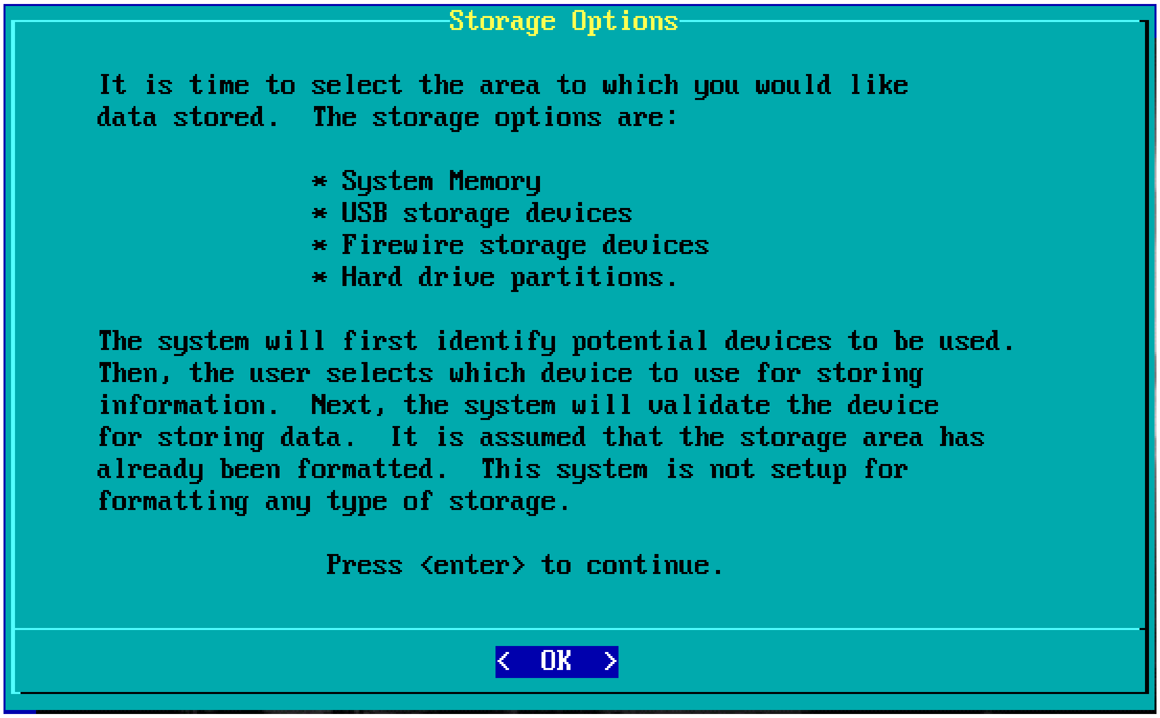


```
                              Set GMT DateTime string.
   Adjust the time (GMT):
     The input is a string of digits, representing the:
         month day hour minutes year sec

     The format of the string are the numbers for:
          MM DD hh mm YYYY ss

     Month through Minute are required.
     For example, the GMT DateTime (Thu Aug 23 15:15:44 2007) for
 now would be:

          MM DD hh mm YYYY ss
          08 23 15 15 2007 47

     You may ommit values for the Year and Second.

  MM DD hh mm YYYY ss
```

Figure - 4 Date / Time Set Instructions

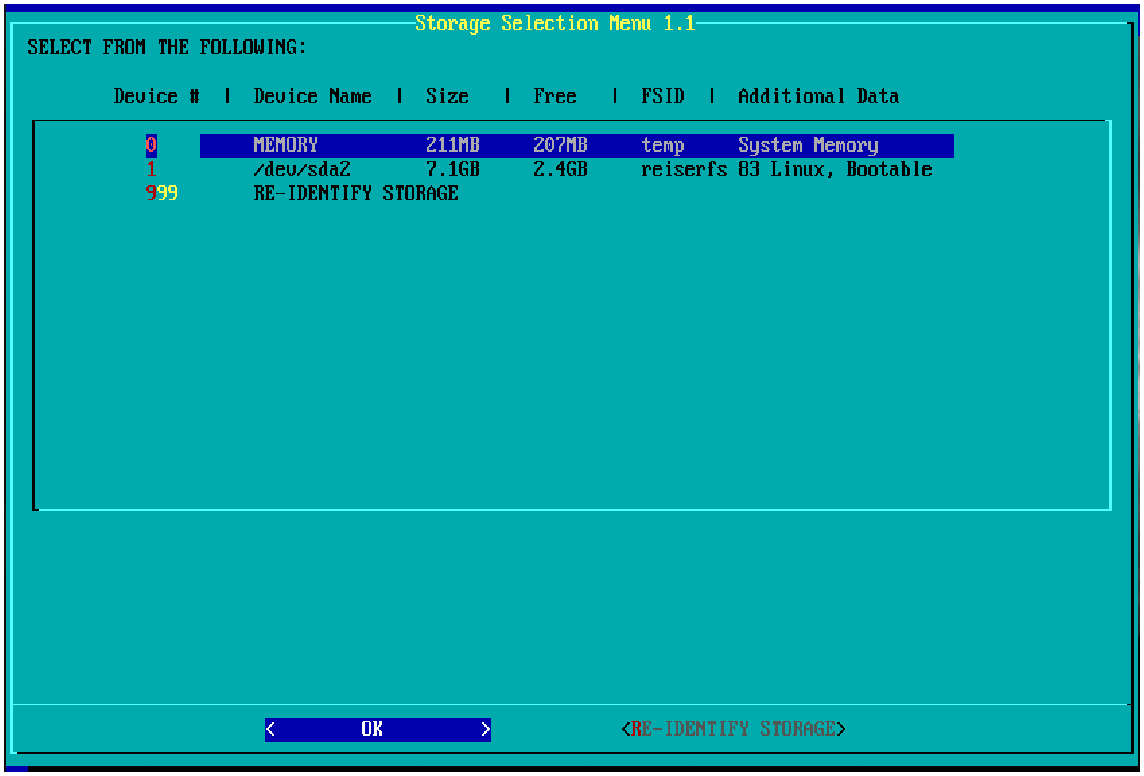
The screen is self-explanatory. The input string will be processed when the [**OK**] button is selected.

The next screen instructs the user to select a storage option, and the screen after that provides a menu for the user to select a storage device. Figure 5 indicates choices for selection: system memory, USB storage devices, firewire storage devices, and hard drive partitions. Testing has proven that PCMCIA storage devices are functional as long as the devices are recognized by the operating system. Figure 6 provides the illustration of the selection menu. Should the user wish to make a change to the storage selection or accidentally hit the wrong key, hitting the numeral nine key will allow for re-selection of storage area.



```
Storage Options

It is time to select the area to which you would like
data stored.  The storage options are:

             * System Memory
             * USB storage devices
             * Firewire storage devices
             * Hard drive partitions.

The system will first identify potential devices to be used.
Then, the user selects which device to use for storing
information.  Next, the system will validate the device
for storing data.  It is assumed that the storage area has
already been formatted.  This system is not setup for
formatting any type of storage.

              Press <enter> to continue.
```

Figure - 5 Storage Options

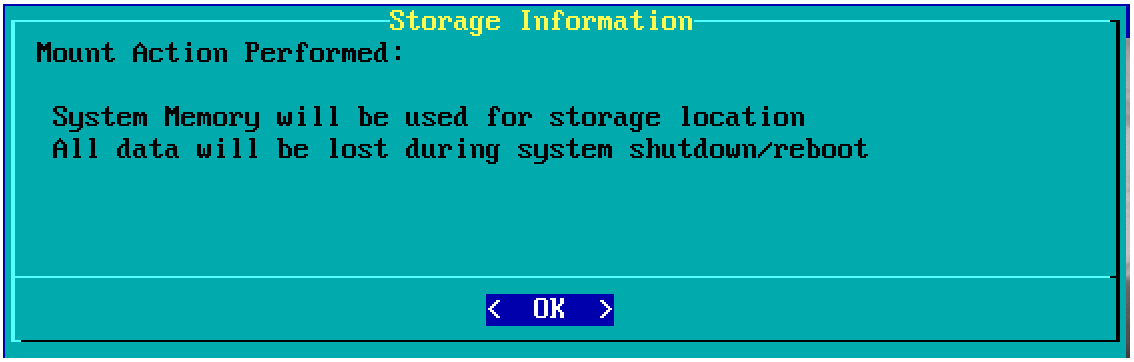


```
Storage Selection Menu 1.1
SELECT FROM THE FOLLOWING:

      Device #  |  Device Name  |  Size    |  Free    |  FSID   |  Additional Data

         0         MEMORY          211MB      207MB      temp       System Memory
         1         /dev/sda2       7.1GB      2.4GB      reiserfs 83 Linux, Bootable
         999       RE-IDENTIFY STORAGE
```

Figure - 6 Storage Selection Menu

For the purposes of this example, RAMDISK (system memory) is selected as the storage medium. Selecting other storage options will bring up other screens similar to Figure 7 except that the data will be non-volatile **(Note: If a USB or**

other external storage device is chosen, it is recommended that the user NOT remove the device during WhirlWind operation; removal of the storage device without shutting down WhirlWind could result in the loss of collected data and/or cause damage to the filesystem of the device). The next screen shot confirms the storage area selection of RAMDISK.



```
Storage Information
Mount Action Performed:

 System Memory will be used for storage location
 All data will be lost during system shutdown/reboot
```

Figure - 7 Storage Mount Action

From this point forward, there are two avenues for final setup with WhirlWhind depending on the version of WhirlWind being used. Please refer to the directed section for continuing with the configuration process:

- Bronze – Gold versions: Follow-on Configuration for Bronze – Gold
- Platinum version: Follow-on Configuration for Platinum only

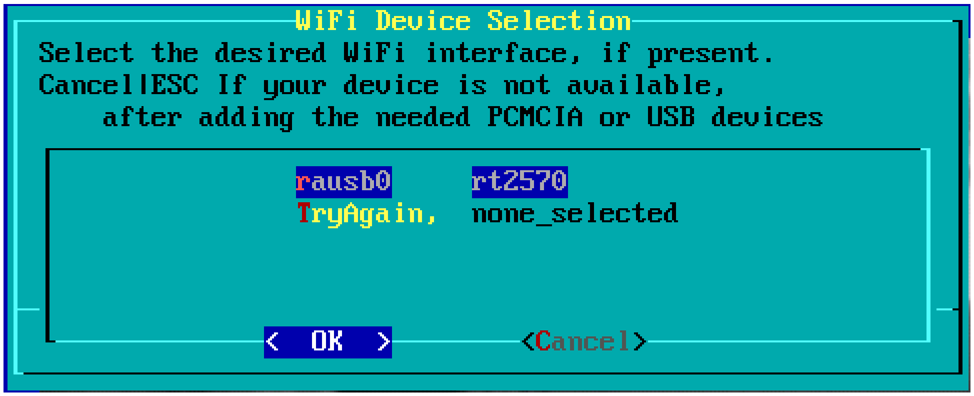
Follow-on Configuration for Bronze – Gold:

The next screen, WiFi Device Selection, requires the user to select the interface. (Removal or insertion of a WiFi network adapter during the boot and authentication process is not recommended and may cause WhirlWind to reboot).

There are multiple, possible presentations from “WiFi Device Selection”:

- Your device is not shown – because it is not attached to the system. Attach/Insert the device and select **[TryAgain]** and **[OK]**.
- Your device is not shown – but is attached/inserted. Your device is simply not identifiable by the system. It cannot be used. Remove the device, and supply another one. Then select **[TryAgain]** and **[OK]**.
- Multiple devices may be displayed. Internal WiFi along with PCMCIA/USB WiFi devices are probably present. Make your selection and select **[OK]** or press **<Enter>**.

Upon device selection, the WiFi device is placed into Monitor mode prior to Kismet starting. If the device can not be placed in Monitor mode, then Kismet will fail to start.



```
WiFi Device Selection
Select the desired WiFi interface, if present.
Cancel|ESC If your device is not available,
    after adding the needed PCMCIA or USB devices

            rausb0      rt2570
            TryAgain,   none_selected
```

Figure - 8 WiFi Device Selection (Bronze - Gold Versions)

The recommended way to terminate a Kismet session is with “Q” = <shift>+<q> in the main Kismet screen. Kismet will shutdown cleanly. Removal of a WiFi network adapter during collection will also cause Kismet to exit and return to the WiFi Device Selection screen.

Also, it has been observed that some WiFi network adapters may cause the system to freeze/lock if removed, depending on the system hardware and WiFi device combination.

Once device selection is completed, the system will start a local system Kismet server and connect to it, using a local Kismet client, which will display the information to the F10 screen.

For Bronze – Gold versions, please continue by going to the section:

- After General Configuration

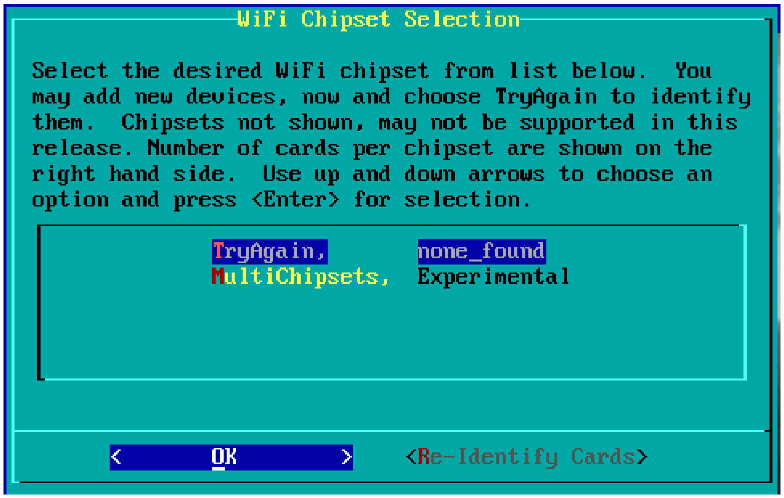
Follow-on Configuration for Platinum only:

The next screen, “WiFi Chipset Selection”, requires the user to select the WiFi chipset(s) for which the wireless cards connected to the system contain. Only chipsets from the cards connected to the system and recognized will be shown. A WiFi chipset refers to the specific wireless radio microchips utilized within a wireless card. It is recommended that wireless devices be placed in the system at this time and **[TryAgain]** or **[Re-Identify Cards]** may be selected to update all chipsets and wireless card count. The screen will show all identified chipsets as well as the number of cards for each (see the following WiFi Chipset Selection example figures 9-11); chipset name(s) on the left and the corresponding number of cards on the right. If the user selects a single chipset, they will only have access to the WiFi cards that contain the matching chipset. This is a good option if the system has a built in wireless card that the user does not wish to use. This screen will provide several options to the user:

- **[TryAgain]** or **[Re-Identify Cards]**: these options allow the user to place wireless cards in the system and have this screen refresh itself with new chipset or card count information
- **[MultiChipset]**: allows the user to utilize more than one chipset of cards at the same time. **This is experimental** because certain chipset combinations may cause the system to lock-up or freeze when multi-chipset configuration is performed. At this time a complete list of known combinations which may cause system lock-up is not completed. Please use this feature with caution. If the system happens to lock-up, please write-down the chipsets being combined and email that information to Futures, Inc. During a system lock-up the only way to help the situation is to reboot the system and not try the specific chipset combination at this time.
- Multiple chipsets may be displayed; in this case an internal WiFi card along with PCMCIA/USB WiFi devices may be present. Make your selection and choose **[OK]**.

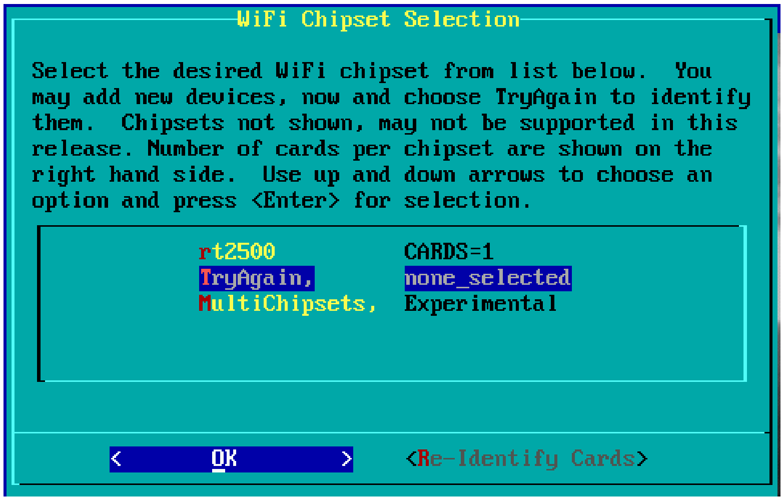
Other possibilities from “WiFi Chipset Selection”:

- A chipset for a given device is not shown – because it is not attached to the system. Attach/insert the device and select **[TryAgain]** and press **<Enter>**.
- A chipset for a device is not shown – but is attached/inserted. The device is not identified by the system and cannot be used at this time. Remove the device, and supply another one. Then select **[TryAgain]** and press **<Enter>**. A future version of WhirlWind may identify the unknown device.
- A WiFi card with a recognized chipset has been connected to the system, but upon a “refresh” the number of cards does not increase for the given chipset – it is possible the system has reached the maximum number of devices for the given chipset. More research in this area is being conducted by the development team.



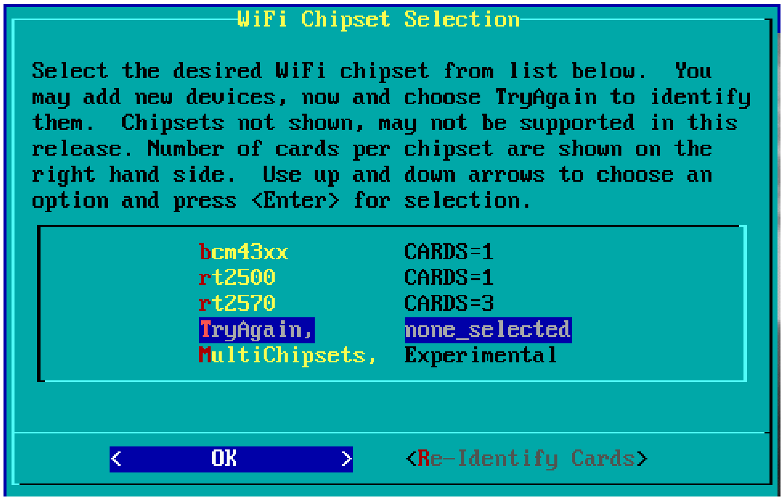
```
                 WiFi Chipset Selection

 Select the desired WiFi chipset from list below.  You
 may add new devices, now and choose TryAgain to identify
 them.  Chipsets not shown, may not be supported in this
 release. Number of cards per chipset are shown on the
 right hand side.  Use up and down arrows to choose an
 option and press <Enter> for selection.

              TryAgain,        none_found
              MultiChipsets,   Experimental

        <     OK      >    <Re-Identify Cards>
```

Figure - 9 WiFi Chipset Selection Example #1 (Platinum Version)



```
                 WiFi Chipset Selection

 Select the desired WiFi chipset from list below.  You
 may add new devices, now and choose TryAgain to identify
 them.  Chipsets not shown, may not be supported in this
 release. Number of cards per chipset are shown on the
 right hand side.  Use up and down arrows to choose an
 option and press <Enter> for selection.

             rt2500           CARDS=1
             TryAgain,        none_selected
             MultiChipsets,   Experimental

        <     OK      >    <Re-Identify Cards>
```

Figure - 10 WiFi Chipset Selection Example #2 (Platinum Version)



```
                 WiFi Chipset Selection

 Select the desired WiFi chipset from list below.  You
 may add new devices, now and choose TryAgain to identify
 them.  Chipsets not shown, may not be supported in this
 release. Number of cards per chipset are shown on the
 right hand side.  Use up and down arrows to choose an
 option and press <Enter> for selection.

             bcm43xx          CARDS=1
             rt2500           CARDS=1
             rt2570           CARDS=3
             TryAgain,        none_selected
             MultiChipsets,   Experimental

        <     OK      >    <Re-Identify Cards>
```

Figure - 11 WiFi Chipset Selection Example #3 (Platinum Version)

After completing the “WiFi Chipset Selection” screen, there are one of two paths the user will follow towards completing the WhirlWind Platinum setup process:

- Selection of a single chipset to be used:
    - **See section “WiFi Device Selection (Platinum Version)”**
- Selection of MultiChipsets (experimental):
    - **See section “WiFi MultiChipset Selection (Platinum Version)”**
    - This section is introduced first due to the “WiFi Device Selection” being part of both paths.

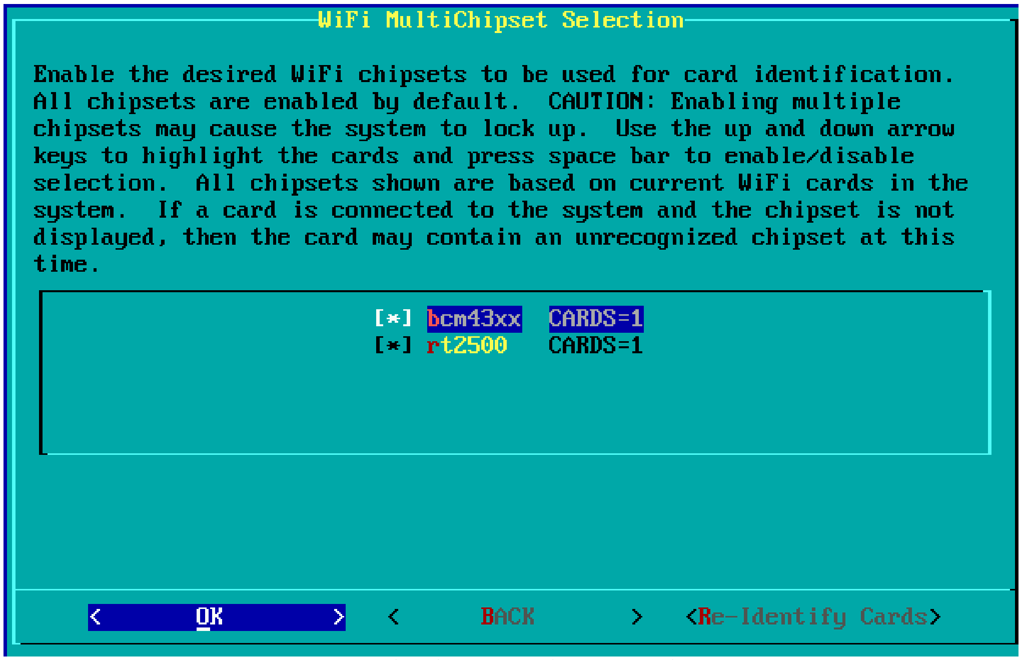
WiFi MultiChipset Selection (Platinum Version):

CAUTION: This is an experimental area of WhirlWind. It has been added to allow users to try various cards/chipsets at the same time. It has been observed that the system may lock-up during configuration of the cards, though rarely, depending on the system used and the chipsets within the wireless cards. If WhirlWind locks-up, please reboot the system, contact Futures with the chipset combination being attempted, and stop use of the chipset combination at this time.

This section discusses the screen presented to the user after selection of “MultiChipsets” has been made. See Figure 12. This screen shows a list of wireless chipsets on the left side and the number of respective cards attached to the system on the right side. Each chipset may be enabled/disabled by the user. All chipsets are enabled by default. Chipsets may be selected by the user pressing the <up arrow> and <down arrow> keys to highlight the chipset and enabling/disabling by pressing the <space bar>.

The following options are presented to the user:

- Toggling the use of WiFi chipsets on/off. * (Asterick) means the chipset is enabled for use
- **[OK]**: Utilize the selected chipsets for use by the system.
- **[BACK]**: Return to the previous screen.
- **[Re-Identify Cards]**: Have the system re-identify all the cards in the system and refresh the current display with the updated information. This option should be used if a new card has been placed in the system that needs to be identified.



```
WiFi MultiChipset Selection

Enable the desired WiFi chipsets to be used for card identification.
All chipsets are enabled by default.  CAUTION: Enabling multiple
chipsets may cause the system to lock up.  Use the up and down arrow
keys to highlight the cards and press space bar to enable/disable
selection.  All chipsets shown are based on current WiFi cards in the
system.  If a card is connected to the system and the chipset is not
displayed, then the card may contain an unrecognized chipset at this
time.

                        [*] bcm43xx   CARDS=1
                        [*] rt2500    CARDS=1
```

Figure - 12 WiFi MultiChipset Selection (Platinum Version)

Once the user selects **[OK]**, the system will display:

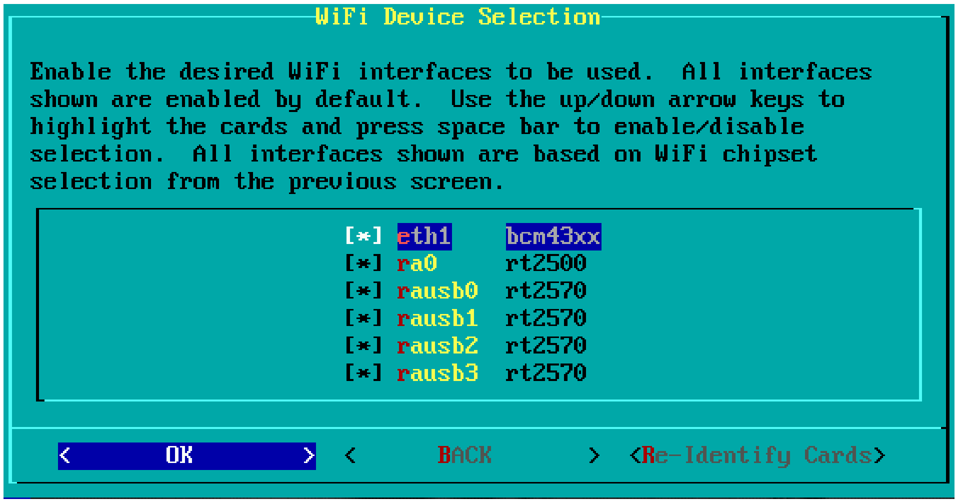
“WiFi Device Selection” screen.

WiFi Device Selection (Platinum Version)

This section discusses the screen presented to the user after selection of single Chipset or MultiChipset configuration. See Figure 13. This screen shows a list of wireless cards on the left side with their respective chipsets on the right. Each card may be enabled/disabled by the user. All cards are enabled by default. Cards may be selected by the user pressing the up and down arrow keys to highlight the card and enabled/disabled by pressing the space bar.

The following options are presented to the user:

- Toggling the use of WiFi cards on/off. * (Asterick) means the card is enabled for use.
- **[OK]**: Utilize the enabled cards for use by the system.
- **[BACK]**: Return to the previous screen.
- **[Re-Identify Cards]**: Have the system re-identify all the cards in the system and refresh the current display with the updated information. This should be used if a new card has been placed in the system that needs to be identified.



```
WiFi Device Selection

Enable the desired WiFi interfaces to be used.  All interfaces
shown are enabled by default.  Use the up/down arrow keys to
highlight the cards and press space bar to enable/disable
selection.  All interfaces shown are based on WiFi chipset
selection from the previous screen.

                  [*] eth1    bcm43xx
                  [*] ra0     rt2500
                  [*] rausb0  rt2570
                  [*] rausb1  rt2570
                  [*] rausb2  rt2570
                  [*] rausb3  rt2570

<      OK      >  <      BACK      >  <Re-Identify Cards>
```

Figure - 13 WiFi Device Selection (Platinum Version)

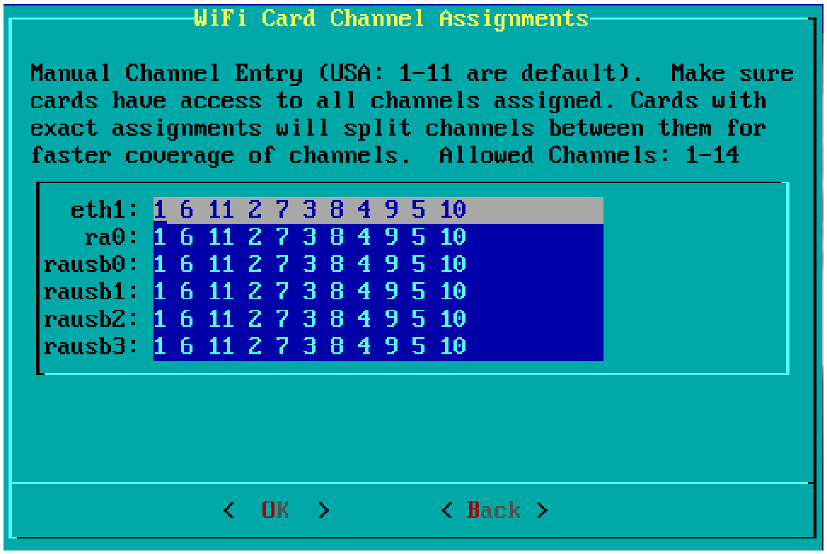
There are multiple, possible presentations from “WiFi Device Selection”:

- Your device is not shown – because it is not attached to the system. Attach/insert the device and select **[Re-Identify Cards]** and press **<Enter>**.
- Your device is not shown – but is attached/inserted. Your device is simply not identifiable by the system. It cannot be used. Remove the device, and supply another one. Then select **[Re-Identify Cards]** and press **<Enter>**.
- Multiple devices may be displayed. Internal WiFi along with PCMCIA/USB WiFi devices are probably present. Adjust the enabled/disabled card list and select **[OK]**.

Once the user selects **[OK]**, the system will display a WiFi card to channel assignment form: WiFi Card Channel Assignments.

WiFi Card Channel Assignments (Platinum Version)

All U.S. channels are assigned to every card in an order to provide best coverage of channels during channel hopping. The user is free to change the channel assignments as they see fit. Allowed channels are 1-14 (complete world channels). Any cards given the exact same channel assignments (order included) will be used for channel splitting across cards to provide a faster coverage of channels. This is done automatically by the system. A user may highlight the different card/channel assignments by using the up and down arrow keys. The user may enter any information they want into this window, but anything outside of bounds will be removed by the system prior to final assignment. Each channel assignment line is limited to 33 characters. This includes the channels being assigned and spaces between the assigned channels. A user may assign each card to a single channel in order to have cards locked onto a specific channel once kismet is started. If all cards are assigned all channels, a user may lock a given card on a specific channel once kismet is started and a network exists on the given channel. Once the assignment of channels is completed, the user can press **<Enter>** to continue or use the tab key to select the **[OK]** button.



WiFi Card Channel Assignments

Manual Channel Entry (USA: 1-11 are default). Make sure cards have access to all channels assigned. Cards with exact assignments will split channels between them for faster coverage of channels. Allowed Channels: 1-14

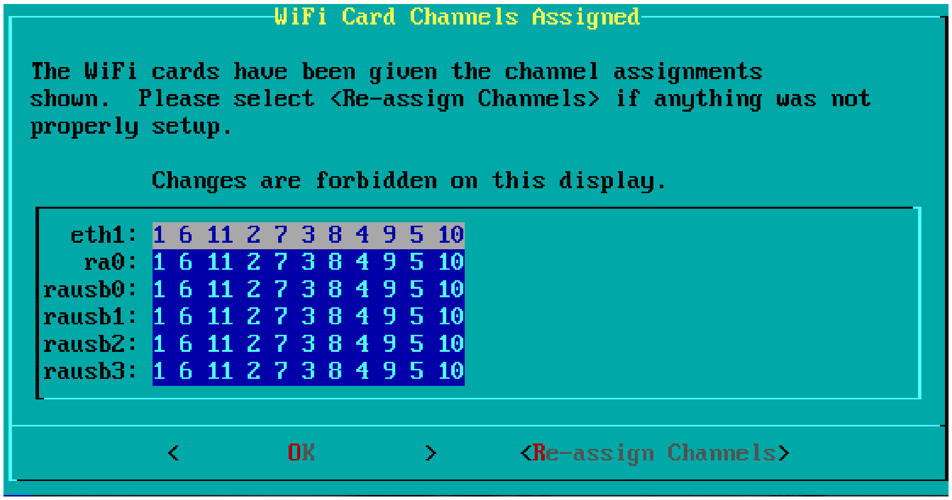
```
  eth1: 1 6 11 2 7 3 8 4 9 5 10
   ra0: 1 6 11 2 7 3 8 4 9 5 10
rausb0: 1 6 11 2 7 3 8 4 9 5 10
rausb1: 1 6 11 2 7 3 8 4 9 5 10
rausb2: 1 6 11 2 7 3 8 4 9 5 10
rausb3: 1 6 11 2 7 3 8 4 9 5 10
```

Figure - 14 WiFi Card Channel Assignments (Platinum Version)

Following this screen, the user will be provided the “WiFi Card Channels Assigned” screen.

WiFi Card Channels Assigned (Platinum Version)

This will allow the user to see what the exact card-to-channel configuration of the system is going to be. If the user has any changes that need to be made, please select **[Re-assign Channels]** button in order to go back to the “WiFi Card Channel Assignments” screen. The screen should look similar to the following:



```
WiFi Card Channels Assigned

The WiFi cards have been given the channel assignments
shown.  Please select <Re-assign Channels> if anything was not
properly setup.

          Changes are forbidden on this display.

   eth1: 1 6 11 2 7 3 8 4 9 5 10
    ra0: 1 6 11 2 7 3 8 4 9 5 10
 rausb0: 1 6 11 2 7 3 8 4 9 5 10
 rausb1: 1 6 11 2 7 3 8 4 9 5 10
 rausb2: 1 6 11 2 7 3 8 4 9 5 10
 rausb3: 1 6 11 2 7 3 8 4 9 5 10

        <       OK       >      <Re-assign Channels>
```

Figure - 15 WiFi Card Channels Assigned (Platinum Version)

After selecting **[OK]** or **[Return]**, all enabled WiFi devices are placed into Monitor mode prior to “Other Options Selection”. If any device can not be placed in Monitor mode, then Kismet will fail to start.

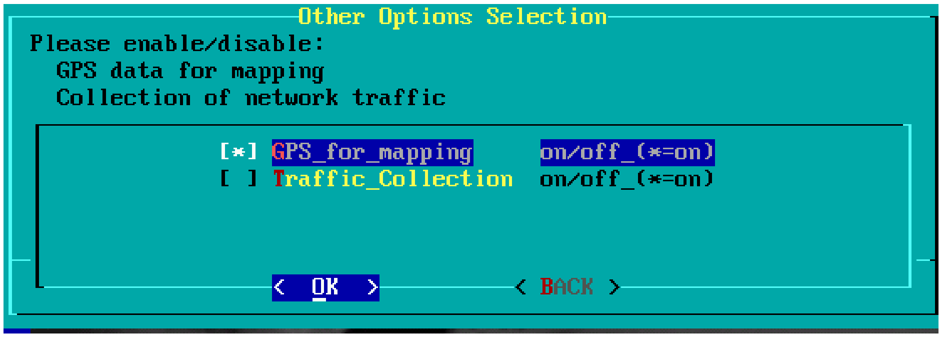
Other Options Selection (Platinum Version)

This section discusses other options provided to the user to enhance their control of the system. The window viewed should be something similar to that in Figure 16.

The following options are presented to the user:

- GPS for mapping: enabled by default. This instructs the system to utilize a GPS device while identifying wireless networks. This enables the system to perform mapping of networks to proximity of location while performing wardriving, warboating, etc. If you are only trying to identify networks in an area without locating them on the map, it is OK to disable this feature. With this feature disabled Kismet will not create a .gps output file. If this feature is enabled without using a compatible GPS device, Kismet will produce a .gps file full of “0” (zeroes) information.

- Traffic Collection: This feature, when enabled, instructs the system to collect wireless network traffic. It is essential for the user to know that this feature may be illegal in their local jurisdiction. Please be aware of the local laws for the area you are enabling this feature. This feature was created to allow a system administrator to collect traffic against their own wireless network and test the security of the network. Futures takes no responsibility for the user violating the law. This feature essentially turns the system into a wireless network sniffer. If the user is locked-on a given channel or a given BSSID, then traffic from that channel or network will be collected. If the system is in channel hopping mode, then packets from various channels will be collected over a period of time.
- **[OK]**: Implement the settings from this screen
- **[BACK]**: Return to the previous screen

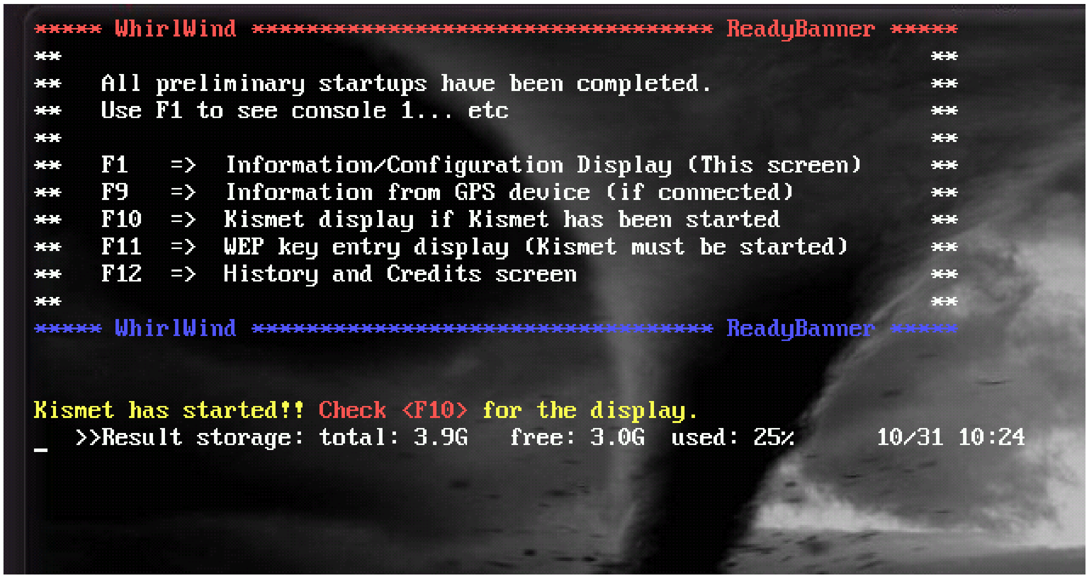


```
                    Other Options Selection
Please enable/disable:
  GPS data for mapping
  Collection of network traffic

             [*] GPS_for_mapping      on/off_(*=on)
             [ ] Traffic_Collection   on/off_(*=on)

                  <  OK  >            < BACK >
```

Figure - 16 Other Options Selection (Platinum Version)

After General Configuration (All Versions):

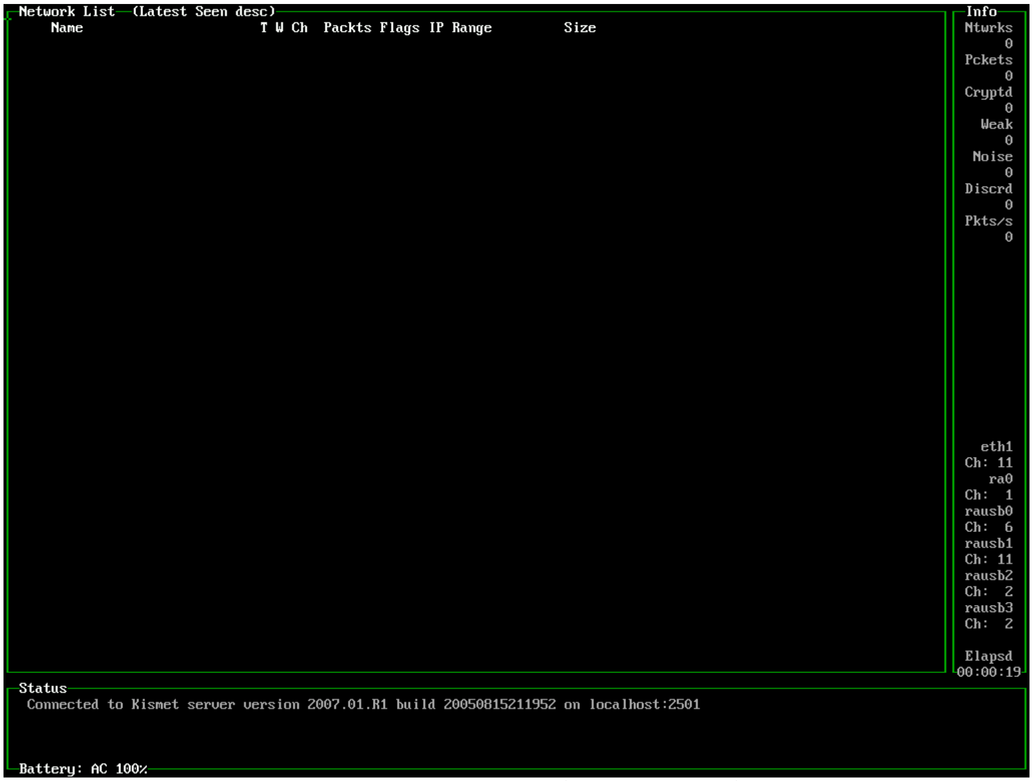
After the user selects **[OK]** from the above screen, the system will adjust all configuration settings of the system as defined by the user and start Kismet. If Kismet fails to start, more than likely a given card failed to enter monitor mode for the system. If the WiFi card(s) entered monitor mode correctly, the user will see a screen similar to the following, followed by a Kismet screen similar to that shown.



```
***** WhirlWind ********************************** ReadyBanner *****
**                                                                **
**   All preliminary startups have been completed.                **
**   Use F1 to see console 1... etc                               **
**                                                                **
**   F1   =>  Information/Configuration Display (This screen)     **
**   F9   =>  Information from GPS device (if connected)          **
**   F10  =>  Kismet display if Kismet has been started           **
**   F11  =>  WEP key entry display (Kismet must be started)      **
**   F12  =>  History and Credits screen                          **
**                                                                **
***** WhirlWind ********************************** ReadyBanner *****


Kismet has started!! Check <F10> for the display.
_  >>Result storage: total: 3.9G   free: 3.0G  used: 25%      10/31 10:24
```

Figure - 17 Ready Banner with Kismet Started

And immediately following this screen, the system will take the user to the Kismet screen (F10), which will initially look something like the following:



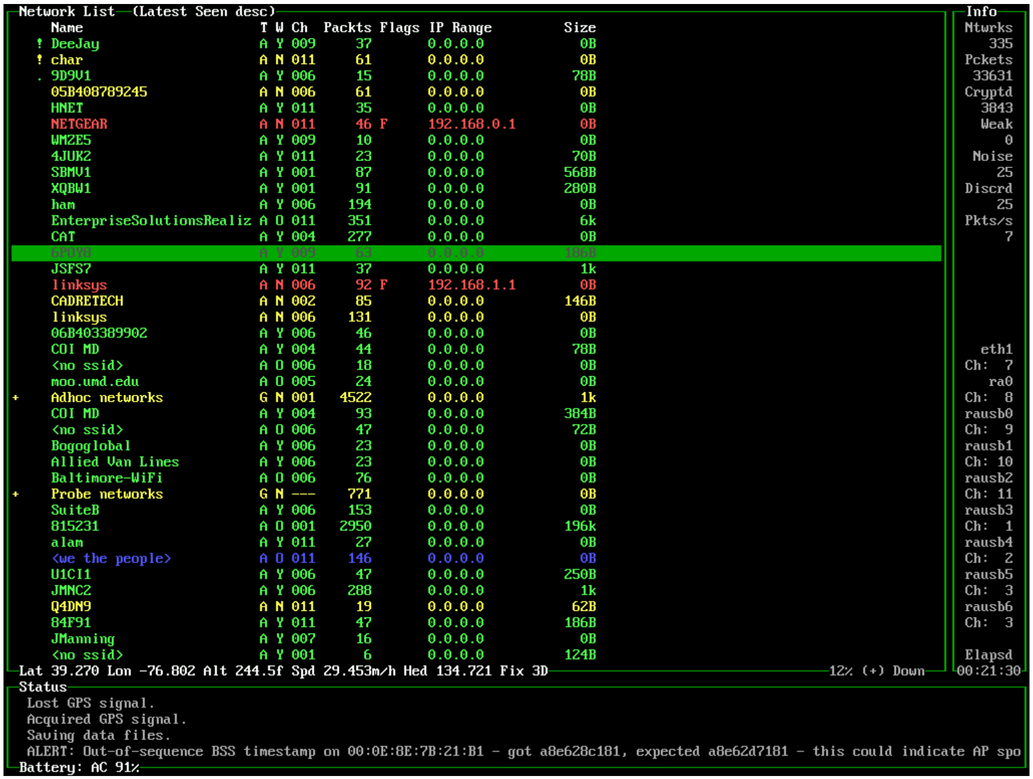
```
Network List—(Latest Seen desc)
    Name                        T W Ch  Packts Flags IP Range         Size
```

```
Info
Ntwrks
     0
Pckets
     0
Cryptd
     0
  Weak
     0
 Noise
     0
Discrd
     0
Pkts/s
     0

  eth1
Ch: 11
   ra0
Ch:  1
rausb0
Ch:  6
rausb1
Ch: 11
rausb2
Ch:  2
rausb3
Ch:  2

Elapsd
00:00:19
```

```
Status
 Connected to Kismet server version 2007.01.R1 build 20050815211952 on localhost:2501


Battery: AC 100%
```

Figure - 18 Kismet Start Screen Sample (No GPS - Platinum Version)

Over the course of time, the Kismet screen may resemble something closer to:



```
Network List—(Latest Seen desc)
    Name                        T W Ch  Packts Flags IP Range         Size
  ! DeeJay                      A Y 009     37       0.0.0.0            0B
  ! char                        A N 011     61       0.0.0.0            0B
  . 9D9V1                       A Y 006     15       0.0.0.0           78B
    05B408789245                A N 006     61       0.0.0.0            0B
    HNET                        A Y 011     35       0.0.0.0            0B
    NETGEAR                     A N 011     46 F     192.168.0.1        0B
    WMZE5                       A Y 009     10       0.0.0.0            0B
    4JUK2                       A Y 011     23       0.0.0.0           70B
    SBMV1                       A Y 001     87       0.0.0.0          568B
    XQBW1                       A Y 001     91       0.0.0.0          280B
    ham                         A Y 006    194       0.0.0.0            0B
    EnterpriseSolutionsRealiz A O 011    351       0.0.0.0            6k
    CAT                         A Y 004    277       0.0.0.0            0B
    6P0Y8                       A Y 009     63       0.0.0.0          186B
    JSFS7                       A Y 011     37       0.0.0.0            1k
    linksys                     A N 006     92 F     192.168.1.1        0B
    CADRETECH                   A N 002     85       0.0.0.0          146B
    linksys                     A N 006    131       0.0.0.0            0B
    06B403389902                A Y 006     46       0.0.0.0            0B
    COI MD                      A Y 004     44       0.0.0.0           78B
    <no ssid>                   A O 006     18       0.0.0.0            0B
    moo.umd.edu                 A O 005     24       0.0.0.0            0B
+   Adhoc networks              G N 001   4522       0.0.0.0            1k
    COI MD                      A Y 004     93       0.0.0.0          384B
    <no ssid>                   A O 006     47       0.0.0.0           72B
    Bogoglobal                  A Y 006     23       0.0.0.0            0B
    Allied Van Lines            A Y 006     23       0.0.0.0            0B
    Baltimore-WiFi              A O 006     76       0.0.0.0            0B
+   Probe networks              G N ---    771       0.0.0.0            0B
    SuiteB                      A Y 006    153       0.0.0.0            0B
    815231                      A O 001   2950       0.0.0.0          196k
    alam                        A Y 011     27       0.0.0.0            0B
    <we the people>             A O 011    146       0.0.0.0            0B
    U1CI1                       A Y 006     47       0.0.0.0          250B
    JMNC2                       A Y 006    288       0.0.0.0            1k
    Q4DN9                       A N 011     19       0.0.0.0           62B
    84F91                       A Y 011     47       0.0.0.0          186B
    JManning                    A Y 007     16       0.0.0.0            0B
    <no ssid>                   A Y 001      6       0.0.0.0          124B
Lat 39.270 Lon -76.802 Alt 244.5f Spd 29.453m/h Hed 134.721 Fix 3D———12% (+) Down
```

```
Info
Ntwrks
   335
Pckets
 33631
Cryptd
  3843
  Weak
     0
 Noise
    25
Discrd
    25
Pkts/s
     7

  eth1
Ch:  7
   ra0
Ch:  8
rausb0
Ch:  9
rausb1
Ch: 10
rausb2
Ch: 11
rausb3
Ch:  1
rausb4
Ch:  2
rausb5
Ch:  3
rausb6
Ch:  3

Elapsd
00:21:30
```

```
Status
 Lost GPS signal.
 Acquired GPS signal.
 Saving data files.
 ALERT: Out-of-sequence BSS timestamp on 00:0E:8E:7B:21:B1 - got a8e628c181, expected a8e62d7181 - this could indicate AP spo
Battery: AC 91%
```

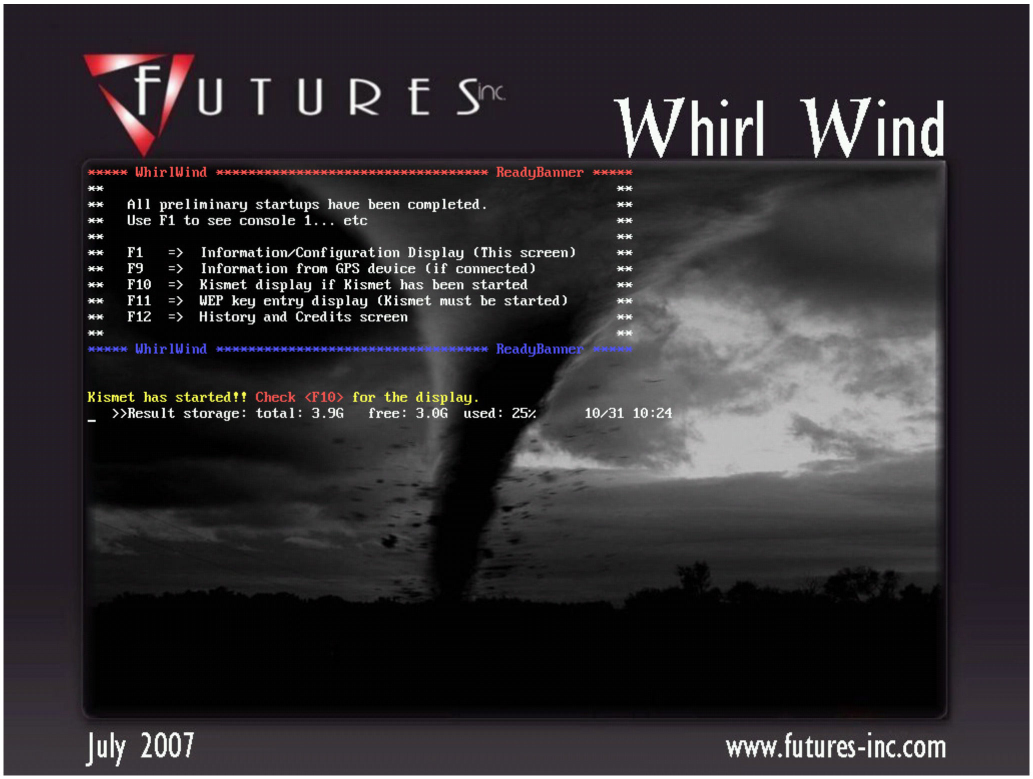
Figure - 19 Kismet Screen Sample Over Time (with GPS - Platinum Version)

The recommended way to terminate a Kismet session is with “Q” = **<shift>+<q>** in the main Kismet screen. Kismet will shutdown cleanly. Removal of a WiFi network adapter during collection will also cause Kismet to exit and return to the WiFi Device Selection screen.

It has been observed that some WiFi network adapters may cause the system to freeze/lock-up if removed, depending on the system hardware and WiFi device combination.

Console Displays

Once the boot sequence has completed, the user will be able to access different screens via the console keys. The console screens provide additional data on the health of WhirlWind in its operations.

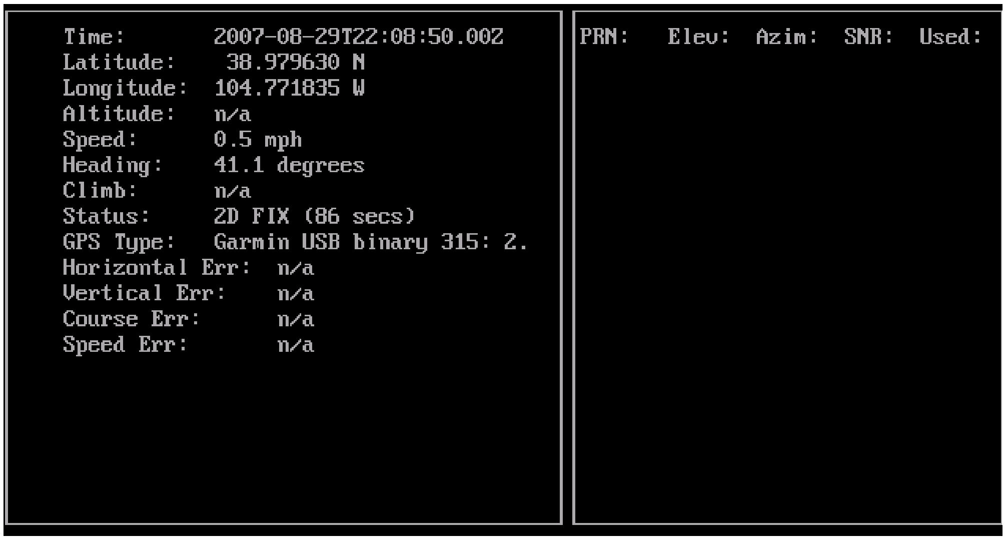


```
***** WhirlWind *********************************** ReadyBanner *****
**                                                                 **
**   All preliminary startups have been completed.                 **
**   Use F1 to see console 1... etc                                **
**                                                                 **
**   F1   =>  Information/Configuration Display (This screen)      **
**   F9   =>  Information from GPS device (if connected)           **
**   F10  =>  Kismet display if Kismet has been started            **
**   F11  =>  WEP key entry display (Kismet must be started)       **
**   F12  =>  History and Credits screen                           **
**                                                                 **
***** WhirlWind *********************************** ReadyBanner *****


Kismet has started!! Check <F10> for the display.
_  >>Result storage: total: 3.9G   free: 3.0G  used: 25%      10/31 10:24
```

Figure - 20 <F1> Console

The next console (located with <F9>) screenshot provides critical data on the GPS device that is being used. It is the application "cgps" which shows the state of the data coming from the GPS daemon ("gpsd"). This application is provided to simply check on the GPS data being provided from gpsd.

If, on this console (<F9>), you press the key "s" you toggle the "silent" attribute on and off. The actual data lines from the gpsd will be scrolled below this display when "on". Another "s" will toggle the on/off to the other state.



```
Time:        2007-08-29T22:08:50.00Z         PRN:   Elev:  Azim:  SNR:  Used:
Latitude:     38.979630 N
Longitude:   104.771835 W
Altitude:    n/a
Speed:       0.5 mph
Heading:     41.1 degrees
Climb:       n/a
Status:      2D FIX (86 secs)
GPS Type:    Garmin USB binary 315: 2.
Horizontal Err:  n/a
Vertical Err:    n/a
Course Err:      n/a
Speed Err:       n/a
```

Figure - 21 <F9> CGPS display

The “GPS Type” effectively identifies the receiver / protocol / firmware being used. This information is the primary way to identify differences between devices that appear similar, but whose performance is radically different.

By pressing the <F10> key the user will be taken to the main data screen for Kismet (reference Figure 23 in the following Kismet section). This will happen automatically when Kismet starts.

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.

Many Internet web sites are devoted to tutorials on how to install and properly configure Kismet—in many cases, complex modifications to the Linux kernel are required to get Kismet to work. WhirlWind comes ***preconfigured and ready to use*** Kismet, provided one of the supported wireless network adapters is used.

Kismet is a completely passive tool. It collects packets, detects standard named networks, and (given time) detects hidden networks through network traffic analysis (called decloaking).

One of the most convenient features of Kismet is the "Help" menu system. By pressing the "h" key from any screen a help menu will pop-up displaying the command keys that are available for that particular screen.

The following table illustrates what the user will see on the Kismet Panels Interface upon pressing the "h" key.

QUICK REFERENCE

Key	Action
e	List Kismet servers
z	Toggle fullscreen zoom of network view
m	Toggle muting of sound and speech
t	Tag (or untag) selected network
g	Group tagged networks
u	Ungroup current group
c	Show clients in current network
L	Lock channel hopping to the current network channel
l	Lock channel hopping to the current network channel & bssid
H	Return to normal channel hopping
+/-	Expand/collapse groups
^L	Force a screen redraw.

POPUP WINDOWS

h	Help (What you’re looking at now)
n	Name current network
i	Detailed information about selected network
s	Sort network list
d	Dump printable strings
r	Packet rate graph
a	Statistics
p	Dump packet type
f	Follow network center
w	Track alerts
x	Close popup window
Q	Quit/Exit Kismet

The panels interface supports displaying networks and clients detected by Kismet grouping of multiple networks, sorting of networks and clients, reporting the signal and noise levels of the wireless card, displaying printable strings, packet types, and many other features.

The panels interface is divided into three primary views:

1. Network display – This where the networks are listed.
2. Statistics – This lists the number of networks, packets, etc.
3. Status – This scrolls recent events which may be noteworthy.

Several types of network and client types are tracked:
Network/Group types:

P	Probe request – no associated connection yet
A	Access point – standard wireless network
H	Ad-hoc – point-to-point wireless network
T	Turbocell – Turbocell (aka Karlnet or Lucent Outdoor Router) network
G	Group – Group of wireless networks
D	Data – Data only network with no control packets.

Status Flags give a brief overview about information discovered on the network.

F Vulnerable factory configuration. Many people don’t bother to ever change the configuration on their WAP. This is bad.
T# Address range of # octets found via TCP traffic
U# Address range of # octets found via UDP traffic
A# Address range of # octets found via ARP traffic
D Address range found via observed DHCP traffic
W WEPed network decrypted with user-supplied key

WEP (W) flags show the type of encryption detected on the network.

N No encryption detected

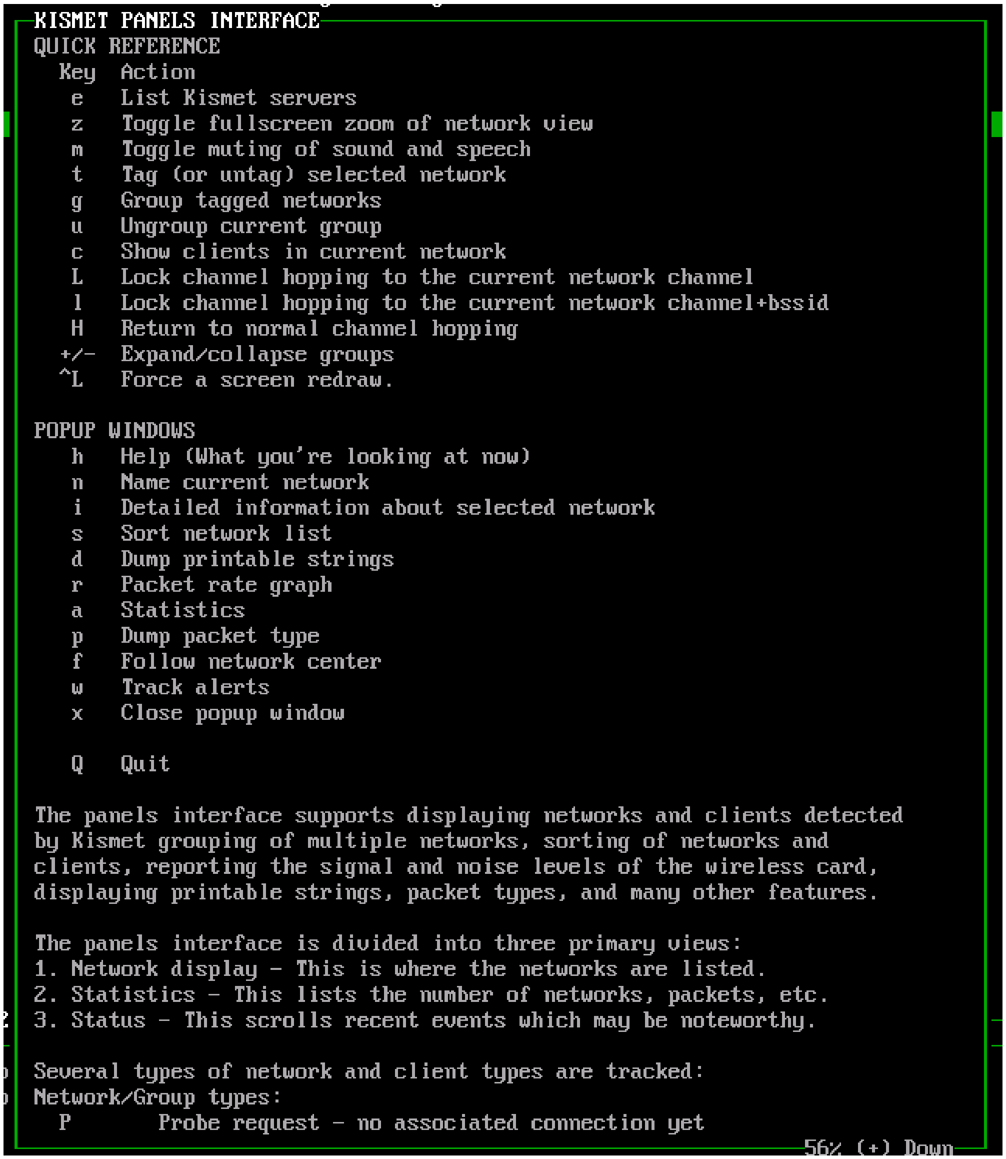
Y Standard WEP encryption

O Other encryption methods detected. See the network details for more information.

SELECTING NETWORKS:

The default sorting method is “Last Heard Descending”. This keeps the most recently active networks on the top of the display. Sort the network display by one of the other methods to select and group networks. Autofit mode changes the location of networks to frequently make selecting a single network realistic.

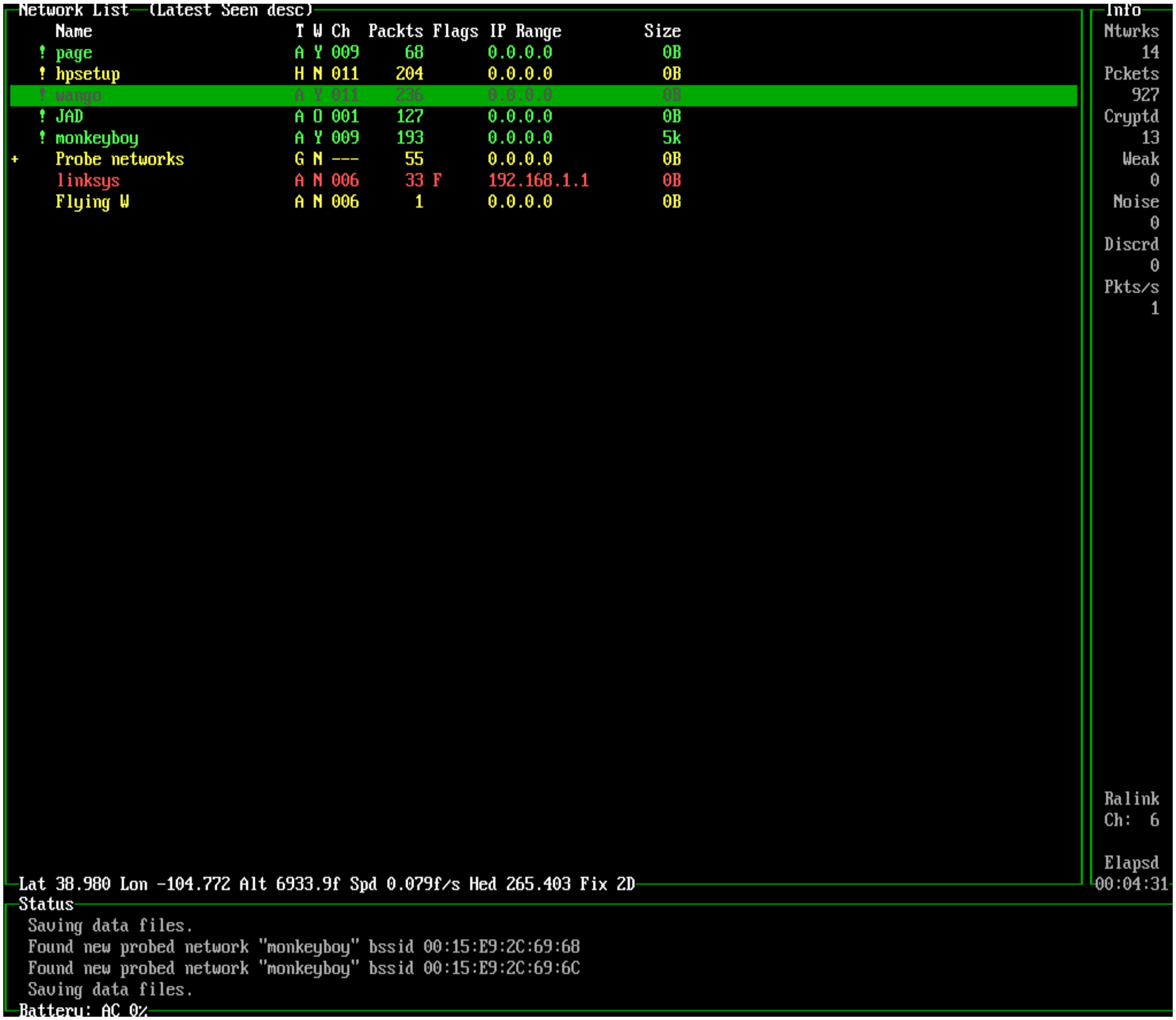
If all of the requested columns can not be fit on the screen, the left and right keys can be used to scroll the column display. The actual help menu screen will look similar to the one below.



```
KISMET PANELS INTERFACE
QUICK REFERENCE
  Key  Action
   e   List Kismet servers
   z   Toggle fullscreen zoom of network view
   m   Toggle muting of sound and speech
   t   Tag (or untag) selected network
   g   Group tagged networks
   u   Ungroup current group
   c   Show clients in current network
   L   Lock channel hopping to the current network channel
   l   Lock channel hopping to the current network channel+bssid
   H   Return to normal channel hopping
  +/-  Expand/collapse groups
  ^L   Force a screen redraw.

POPUP WINDOWS
   h   Help (What you're looking at now)
   n   Name current network
   i   Detailed information about selected network
   s   Sort network list
   d   Dump printable strings
   r   Packet rate graph
   a   Statistics
   p   Dump packet type
   f   Follow network center
   w   Track alerts
   x   Close popup window

   Q   Quit

The panels interface supports displaying networks and clients detected
by Kismet grouping of multiple networks, sorting of networks and
clients, reporting the signal and noise levels of the wireless card,
displaying printable strings, packet types, and many other features.

The panels interface is divided into three primary views:
1. Network display - This is where the networks are listed.
2. Statistics - This lists the number of networks, packets, etc.
3. Status - This scrolls recent events which may be noteworthy.

Several types of network and client types are tracked:
Network/Group types:
  P       Probe request - no associated connection yet
                                                          56% (+) Down
```

Figure - 22 Kismet Help Menu

During the boot-up process, the user will select a WiFi device(s) for Kismet to utilize. Once the WiFi source(s) is identified and the card is placed in Monitor mode, Kismet launches. The opening screen of Kismet looks similar (colors may vary) to this:

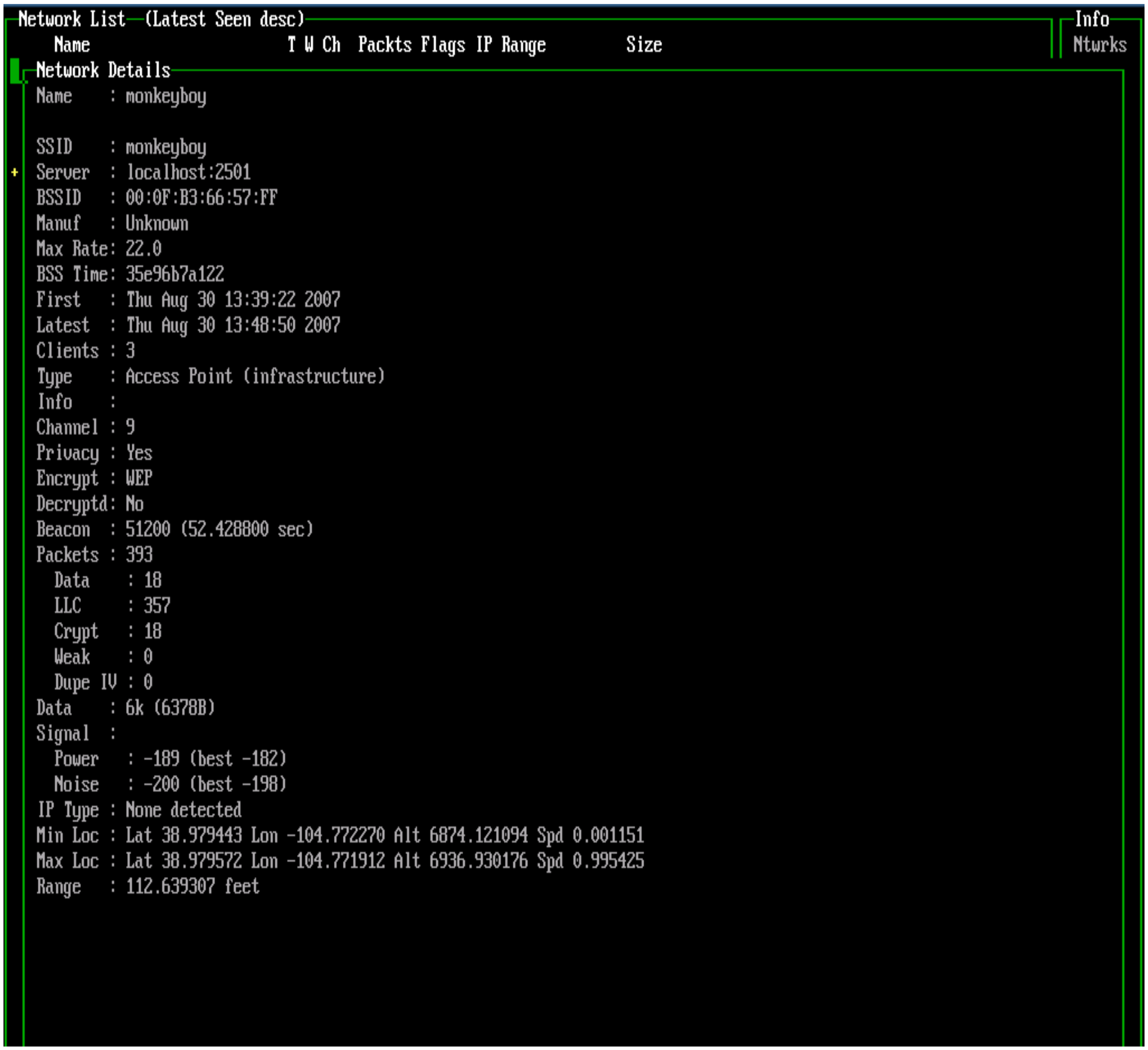


```
Network List (Latest Seen desc)                                      Info
   Name                     T W Ch  Packts Flags IP Range      Size  Ntwrks
 ! page                     A Y 009     68       0.0.0.0         0B      14
 ! hpsetup                  H N 011    204       0.0.0.0         0B  Pckets
 ! wango                    A Y 011    236       0.0.0.0         0B     927
 ! JAD                      A O 001    127       0.0.0.0         0B  Cryptd
 ! monkeyboy                A Y 009    193       0.0.0.0         5k      13
+  Probe networks           G N ---     55       0.0.0.0         0B    Weak
   linksys                  A N 006     33 F     192.168.1.1     0B       0
   Flying W                 A N 006      1       0.0.0.0         0B   Noise
                                                                          0
                                                                     Discrd
                                                                          0
                                                                     Pkts/s
                                                                          1

                                                                     Ralink
                                                                     Ch:  6

                                                                     Elapsd
Lat 38.980 Lon -104.772 Alt 6933.9f Spd 0.079f/s Hed 265.403 Fix 2D  00:04:31
Status
 Saving data files.
 Found new probed network "monkeyboy" bssid 00:15:E9:2C:69:68
 Found new probed network "monkeyboy" bssid 00:15:E9:2C:69:6C
 Saving data files.
Battery: AC 0%
```

Figure - 23 Illustration of WiFi Sources Detected

As Kismet starts, it begins to compile a list of all wireless networks within range of its wireless adapter. The first column displays the name of the wireless access point whose traffic is being collected (common names include “linksys,” “default,” or “<no ssid>”). Another particularly relevant column is the third column, labeled “W.” This column tells whether or not Kismet detects that the access point is using encryption. In Figure 23, only 4 of 8 wireless access points are using encryption.

A wireless access point can be selected by moving the cursor up or down and hitting “ENTER.” Hitting “ENTER” brings up detailed information about the selected access point:



```
Network List—(Latest Seen desc)                                              Info
    Name                     T W Ch  Packts Flags IP Range        Size       Ntwrks
 Network Details
 Name    : monkeyboy

 SSID    : monkeyboy
+Server  : localhost:2501
 BSSID   : 00:0F:B3:66:57:FF
 Manuf   : Unknown
 Max Rate: 22.0
 BSS Time: 35e96b7a122
 First   : Thu Aug 30 13:39:22 2007
 Latest  : Thu Aug 30 13:48:50 2007
 Clients : 3
 Type    : Access Point (infrastructure)
 Info    :
 Channel : 9
 Privacy : Yes
 Encrypt : WEP
 Decryptd: No
 Beacon  : 51200 (52.428800 sec)
 Packets : 393
   Data    : 18
   LLC     : 357
   Crypt   : 18
   Weak    : 0
   Dupe IV : 0
 Data    : 6k (6378B)
 Signal  :
   Power   : -189 (best -182)
   Noise   : -200 (best -198)
 IP Type : None detected
 Min Loc : Lat 38.979443 Lon -104.772270 Alt 6874.121094 Spd 0.001151
 Max Loc : Lat 38.979572 Lon -104.771912 Alt 6936.930176 Spd 0.995425
 Range   : 112.639307 feet
```

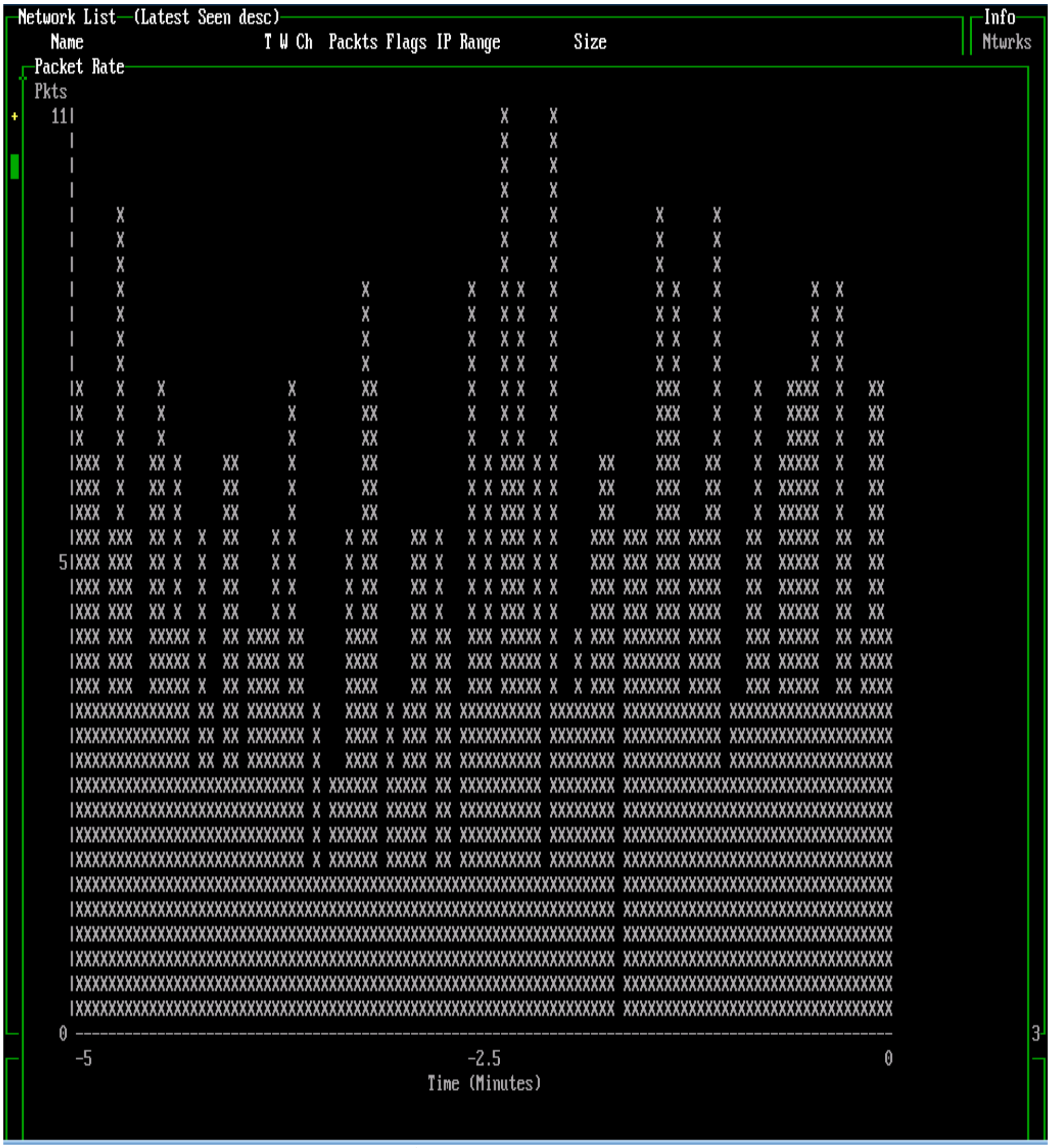
Figure - 24 Access Point (AP) Information

To escape this detailed view, press the “q” key (note the “q” will close out any pop-up windows in Kismet and return the user to the previous view). Some of the interesting information displayed on the Network Details screen includes:

- MAC address
- Manufacturer of access point (based on MAC address)
- Factory configuration alert
- Signal

Should a “factory configuration” alert message be shown, it indicates that the wireless access point has been installed with an “out of the box” configuration—no changes made to the default settings. Kismet alerts to factory configurations because they are extremely dangerous if deployed on an enterprise network—these configurations are typically very insecure (designed to help users get the product running with as little difficulty as possible).

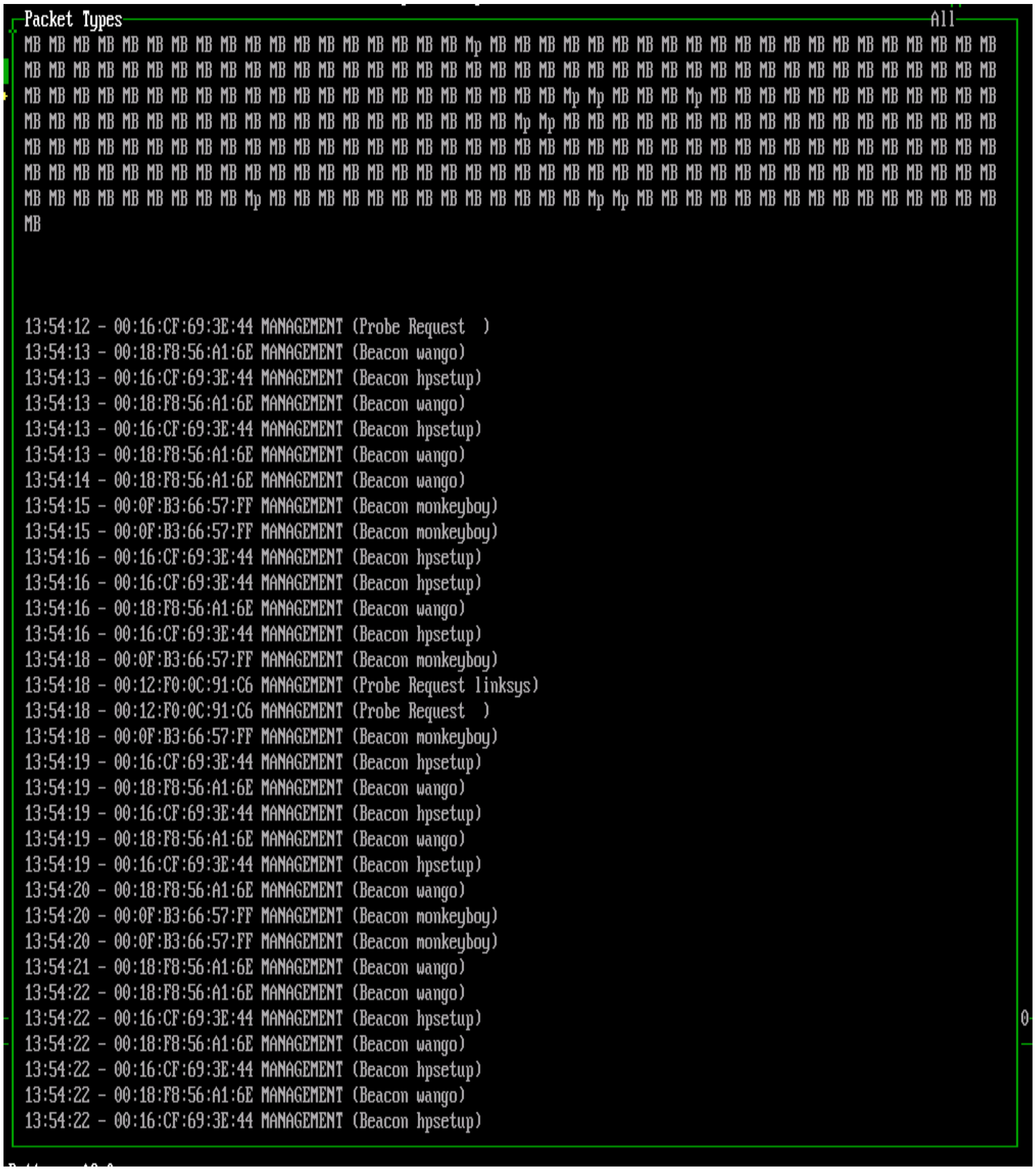
To see the rate of wireless packets traveling the wireless environment, press the “r” key.



```
Network List (Latest Seen desc)                                                                                       Info
    Name                      T W Ch  Packts Flags IP Range         Size                                              Nturks
  Packet Rate
  Pkts
    11|                                                    X     X
      |                                                    X     X
      |                                                    X     X
      |                                                    X     X
      |     X                                              X     X            X      X
      |     X                                              X     X            X      X
      |     X                                              X     X            X      X
      |     X                             X            X   X X   X            X X    X           X  X
      |     X                             X            X   X X   X            X X    X           X  X
      |     X                             X            X   X X   X            X X    X           X  X
      |     X                             X            X   X X   X            X X    X           X  X
      |X    X    X               X        XX           X   X X   X            XXX    X    X   XXXX  X   XX
      |X    X    X               X        XX           X   X X   X            XXX    X    X   XXXX  X   XX
      |X    X    X               X        XX           X   X X   X            XXX    X    X   XXXX  X   XX
      |XXX  X   XX X     XX      X        XX           X X XXX X X     XX     XXX   XX    X  XXXXX  X   XX
      |XXX  X   XX X     XX      X        XX           X X XXX X X     XX     XXX   XX    X  XXXXX  X   XX
      |XXX  X   XX X     XX      X        XX           X X XXX X X     XX     XXX   XX    X  XXXXX  X   XX
      |XXX XXX  XX X  X  XX    X X      X XX    XX X   X X XXX X X    XXX XXX XXX XXXX   XX  XXXXX  XX  XX
     5|XXX XXX  XX X  X  XX    X X      X XX    XX X   X X XXX X X    XXX XXX XXX XXXX   XX  XXXXX  XX  XX
      |XXX XXX  XX X  X  XX    X X      X XX    XX X   X X XXX X X    XXX XXX XXX XXXX   XX  XXXXX  XX  XX
      |XXX XXX  XX X  X  XX    X X      X XX    XX X   X X XXX X X    XXX XXX XXX XXXX   XX  XXXXX  XX  XX
      |XXX XXX  XXXXX X  XX XXXX XX     XXXX    XX XX  XXX XXXXX X  X XXX XXXXXXX XXXX   XXX XXXXX  XX XXXX
      |XXX XXX  XXXXX X  XX XXXX XX     XXXX    XX XX  XXX XXXXX X  X XXX XXXXXXX XXXX   XXX XXXXX  XX XXXX
      |XXX XXX  XXXXX X  XX XXXX XX     XXXX    XX XX  XXX XXXXX X  X XXX XXXXXXX XXXX   XXX XXXXX  XX XXXX
      |XXXXXXXXXXXXXX XX XX XXXXXXX X   XXXX X XXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXX XX XX XXXXXXX X   XXXX X XXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXX XX XX XXXXXXX X   XXXX X XXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXX X XXXXXX XXXXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXX X XXXXXX XXXXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXX X XXXXXX XXXXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXX X XXXXXX XXXXX XX XXXXXXXXXX XXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
      |XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
     0 ----------------------------------------------------------------------------------------------------
       -5                                              -2.5                                           0
                                                  Time (Minutes)
```

Figure - 25 Packets Traversing WiFi Environment

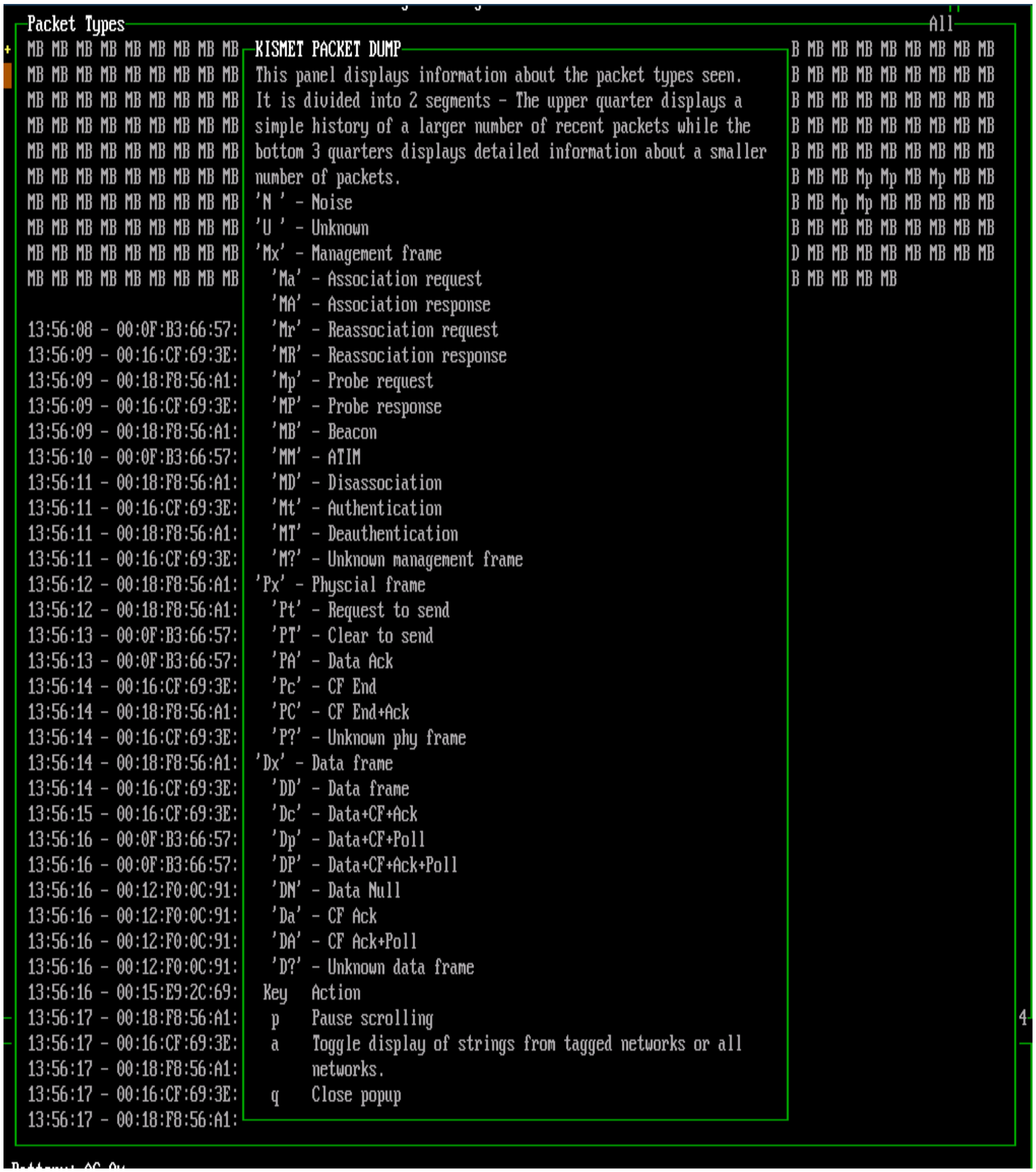
To view a live display of the types of packets (whether data frames, router management frames, etc.), press the “p” key.



```
Packet Types                                                                                    All
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB Mp MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB Mp Mp MB MB MB Mp MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB Mp Mp MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB Mp MB MB MB MB MB MB MB MB MB MB MB MB MB Mp Mp MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB



13:54:12 - 00:16:CF:69:3E:44 MANAGEMENT (Probe Request  )
13:54:13 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:13 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:13 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:13 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:13 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:14 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:15 - 00:0F:B3:66:57:FF MANAGEMENT (Beacon monkeyboy)
13:54:15 - 00:0F:B3:66:57:FF MANAGEMENT (Beacon monkeyboy)
13:54:16 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:16 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:16 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:16 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:18 - 00:0F:B3:66:57:FF MANAGEMENT (Beacon monkeyboy)
13:54:18 - 00:12:F0:0C:91:C6 MANAGEMENT (Probe Request linksys)
13:54:18 - 00:12:F0:0C:91:C6 MANAGEMENT (Probe Request  )
13:54:18 - 00:0F:B3:66:57:FF MANAGEMENT (Beacon monkeyboy)
13:54:19 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:19 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:19 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:19 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:19 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:20 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:20 - 00:0F:B3:66:57:FF MANAGEMENT (Beacon monkeyboy)
13:54:20 - 00:0F:B3:66:57:FF MANAGEMENT (Beacon monkeyboy)
13:54:21 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:22 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:22 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:22 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:22 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
13:54:22 - 00:18:F8:56:A1:6E MANAGEMENT (Beacon wango)
13:54:22 - 00:16:CF:69:3E:44 MANAGEMENT (Beacon hpsetup)
```

Figure - 26 Packet Information

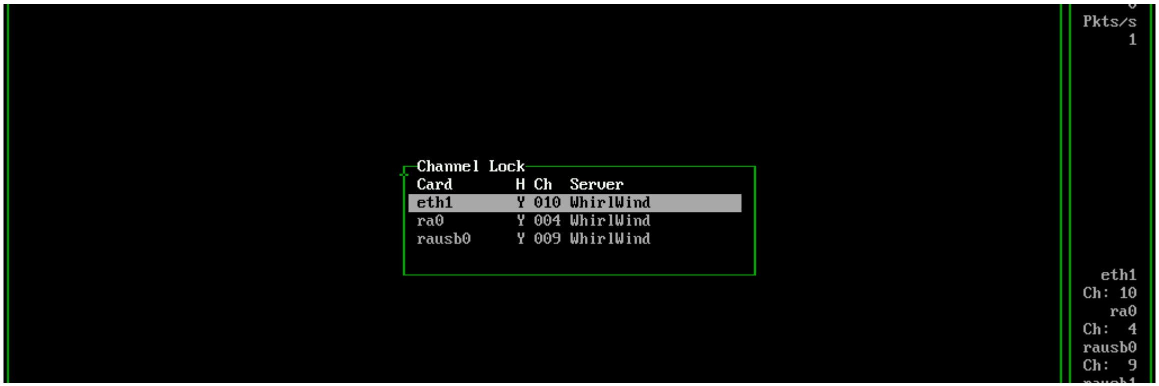
The display of the "Packet Type" information may be difficult to decipher. Recall, however, that every Kismet screen has "help." To display a legend for the packet type information press the "h" key.



```
Packet Types                                                                                         All
MB MB MB MB MB MB MB MB MB KISMET PACKET DUMP                                                   B MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB This panel displays information about the packet types seen.         B MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB It is divided into 2 segments - The upper quarter displays a         B MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB simple history of a larger number of recent packets while the        B MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB bottom 3 quarters displays detailed information about a smaller      B MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB number of packets.                                                   B MB MB Mp Mp MB Mp MB MB
MB MB MB MB MB MB MB MB MB 'N ' - Noise                                                         B MB Mp Mp MB MB MB MB MB
MB MB MB MB MB MB MB MB MB 'U ' - Unknown                                                       B MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB 'Mx' - Management frame                                              D MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB   'Ma' - Association request                                         B MB MB MB MB
                             'MA' - Association response
13:56:08 - 00:0F:B3:66:57:   'Mr' - Reassociation request
13:56:09 - 00:16:CF:69:3E:   'MR' - Reassociation response
13:56:09 - 00:18:F8:56:A1:   'Mp' - Probe request
13:56:09 - 00:16:CF:69:3E:   'MP' - Probe response
13:56:09 - 00:18:F8:56:A1:   'MB' - Beacon
13:56:10 - 00:0F:B3:66:57:   'MM' - ATIM
13:56:11 - 00:18:F8:56:A1:   'MD' - Disassociation
13:56:11 - 00:16:CF:69:3E:   'Mt' - Authentication
13:56:11 - 00:18:F8:56:A1:   'MT' - Deauthentication
13:56:11 - 00:16:CF:69:3E:   'M?' - Unknown management frame
13:56:12 - 00:18:F8:56:A1: 'Px' - Physcial frame
13:56:12 - 00:18:F8:56:A1:   'Pt' - Request to send
13:56:13 - 00:0F:B3:66:57:   'PT' - Clear to send
13:56:13 - 00:0F:B3:66:57:   'PA' - Data Ack
13:56:14 - 00:16:CF:69:3E:   'Pc' - CF End
13:56:14 - 00:18:F8:56:A1:   'PC' - CF End+Ack
13:56:14 - 00:16:CF:69:3E:   'P?' - Unknown phy frame
13:56:14 - 00:18:F8:56:A1: 'Dx' - Data frame
13:56:14 - 00:16:CF:69:3E:   'DD' - Data frame
13:56:15 - 00:16:CF:69:3E:   'Dc' - Data+CF+Ack
13:56:16 - 00:0F:B3:66:57:   'Dp' - Data+CF+Poll
13:56:16 - 00:0F:B3:66:57:   'DP' - Data+CF+Ack+Poll
13:56:16 - 00:12:F0:0C:91:   'DN' - Data Null
13:56:16 - 00:12:F0:0C:91:   'Da' - CF Ack
13:56:16 - 00:12:F0:0C:91:   'DA' - CF Ack+Poll
13:56:16 - 00:12:F0:0C:91:   'D?' - Unknown data frame
13:56:16 - 00:15:E9:2C:69:  Key   Action
13:56:17 - 00:18:F8:56:A1:   p    Pause scrolling                                                                              4
13:56:17 - 00:16:CF:69:3E:   a    Toggle display of strings from tagged networks or all
13:56:17 - 00:18:F8:56:A1:        networks.
13:56:17 - 00:16:CF:69:3E:   q    Close popup
13:56:17 - 00:18:F8:56:A1:
```

Figure - 27 Sniffer Data

In addition to cataloguing wireless network information, Kismet can also be used as a sniffer to intercept wireless network traffic. First select the wireless network of interest from the Kismet main screen, then press the “L” key to lock on the channel (note: this command is case sensitive, it must be an upper case “L” to lock the channel). The version of Kismet included in WhirlWind has been modified to not only lock onto a channel (the default behavior of Kismet), but to lock onto a single network operating on that channel. A lowercase “l” locks the channel and the BSSID. This behavior avoids collecting traffic from other access points that happen to be configured to use the same channel – a useful feature in a noisy environment. When operating a system with multiple WiFi cards, please note that a pop-up window similar to the follow will appear when requesting a channel lock or BSSID lock from Kismet. Kismet is requesting the user to select a card to utilize for performing the channel/BSSID lock. This menu is scrollable by using the up and down arrow keys. Please note that the window only shows 3 of the cards at a time, and scrolling through the list is necessary to see all possible selections in the list

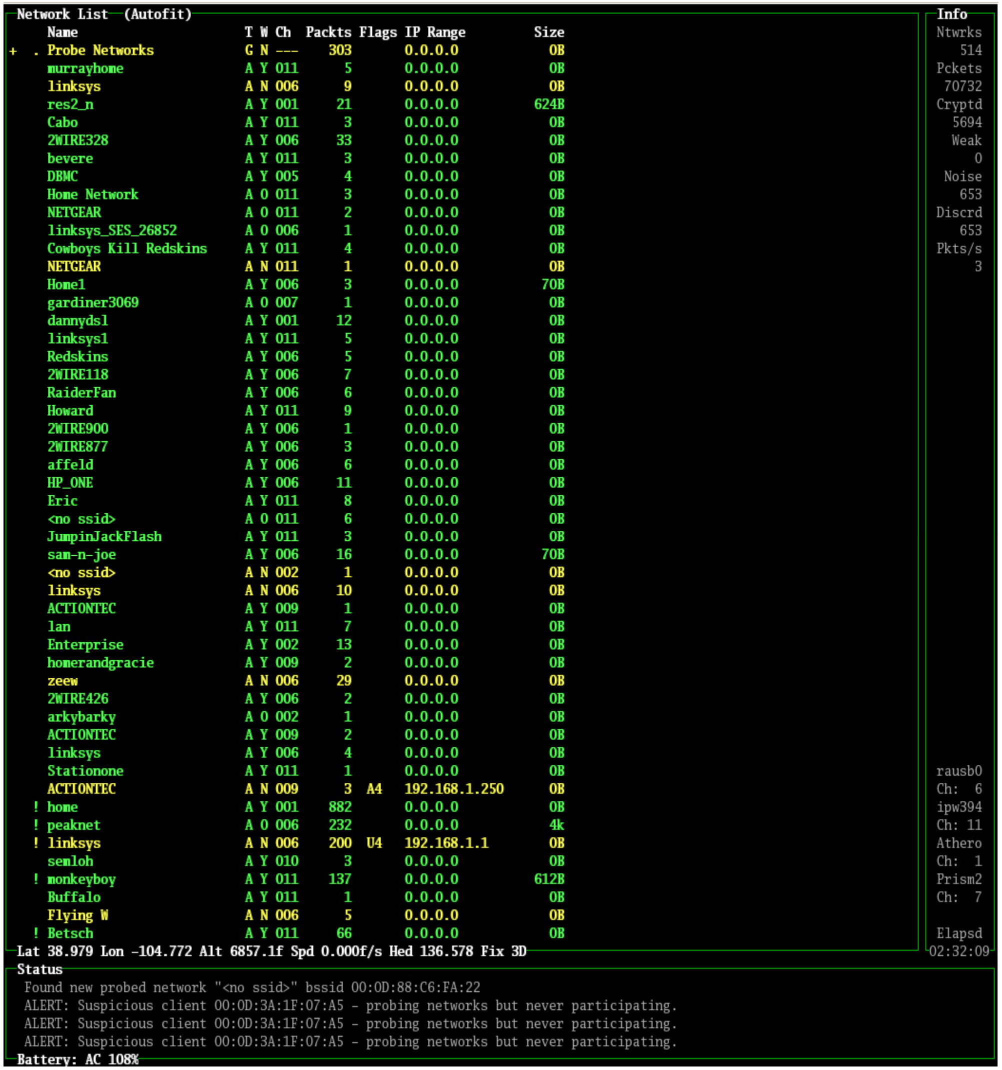


```
Channel Lock
Card         H Ch  Server
eth1         Y 010 WhirlWind
ra0          Y 004 WhirlWind
rausb0       Y 009 WhirlWind
```

```
Pkts/s
     1

  eth1
Ch: 10
   ra0
Ch:  4
rausb0
Ch:  9
```

Figure - 28 Kismet Selection Window Perform Locking (Multiple Card System - Platinum)

Next, press the “d” key to begin to “dump” the contents of data packets to the screen. The following screenshot depicts an actual wireless environment.

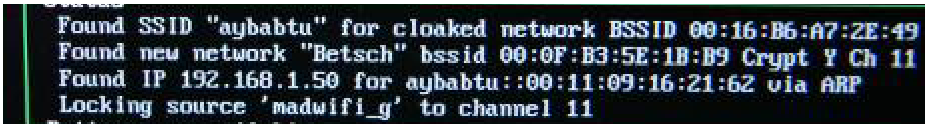


```
-Network List-(Autofit)------------------------------------------------  -Info-
    Name                      T W Ch  Packts Flags IP Range        Size   Ntwrks
+ . Probe Networks            G N ---    303       0.0.0.0           0B      514
    murrayhome                A Y 011      5       0.0.0.0           0B   Pckets
    linksys                   A N 006      9       0.0.0.0           0B    70732
    res2_n                    A Y 001     21       0.0.0.0         624B   Cryptd
    Cabo                      A Y 011      3       0.0.0.0           0B     5694
    2WIRE328                  A Y 006     33       0.0.0.0           0B     Weak
    bevere                    A Y 011      3       0.0.0.0           0B        0
    DBMC                      A Y 005      4       0.0.0.0           0B    Noise
    Home Network              A 0 011      3       0.0.0.0           0B      653
    NETGEAR                   A 0 011      2       0.0.0.0           0B   Discrd
    linksys_SES_26852         A 0 006      1       0.0.0.0           0B      653
    Cowboys Kill Redskins     A Y 011      4       0.0.0.0           0B   Pkts/s
    NETGEAR                   A N 011      1       0.0.0.0           0B        3
    Home1                     A Y 006      3       0.0.0.0          70B
    gardiner3069              A 0 007      1       0.0.0.0           0B
    dannyds1                  A Y 001     12       0.0.0.0           0B
    linksys1                  A Y 011      5       0.0.0.0           0B
    Redskins                  A Y 006      5       0.0.0.0           0B
    2WIRE118                  A Y 006      7       0.0.0.0           0B
    RaiderFan                 A Y 006      6       0.0.0.0           0B
    Howard                    A Y 011      9       0.0.0.0           0B
    2WIRE900                  A Y 006      1       0.0.0.0           0B
    2WIRE877                  A Y 006      3       0.0.0.0           0B
    affeld                    A Y 006      6       0.0.0.0           0B
    HP_ONE                    A Y 006     11       0.0.0.0           0B
    Eric                      A Y 011      8       0.0.0.0           0B
    <no ssid>                 A 0 011      6       0.0.0.0           0B
    JumpinJackFlash           A Y 011      3       0.0.0.0           0B
    sam-n-joe                 A Y 006     16       0.0.0.0          70B
    <no ssid>                 A N 002      1       0.0.0.0           0B
    linksys                   A N 006     10       0.0.0.0           0B
    ACTIONTEC                 A Y 009      1       0.0.0.0           0B
    lan                       A Y 011      7       0.0.0.0           0B
    Enterprise                A Y 002     13       0.0.0.0           0B
    homerandgracie            A Y 009      2       0.0.0.0           0B
    zeew                      A N 006     29       0.0.0.0           0B
    2WIRE426                  A Y 006      2       0.0.0.0           0B
    arkybarky                 A 0 002      1       0.0.0.0           0B
    ACTIONTEC                 A Y 009      2       0.0.0.0           0B
    linksys                   A Y 006      4       0.0.0.0           0B
    Stationone                A Y 011      1       0.0.0.0           0B   rausb0
    ACTIONTEC                 A N 009      3 A4    192.168.1.250     0B   Ch:  6
  ! home                      A Y 001    882       0.0.0.0           0B   ipw394
  ! peaknet                   A 0 006    232       0.0.0.0           4k   Ch: 11
  ! linksys                   A N 006    200 U4    192.168.1.1       0B   Athero
    semloh                    A Y 010      3       0.0.0.0           0B   Ch:  1
  ! monkeyboy                 A Y 011    137       0.0.0.0         612B   Prism2
    Buffalo                   A Y 011      1       0.0.0.0           0B   Ch:  7
    Flying W                  A N 006      5       0.0.0.0           0B
  ! Betsch                    A Y 011     66       0.0.0.0           0B   Elapsd
-Lat 38.979 Lon -104.772 Alt 6857.1f Spd 0.000f/s Hed 136.578 Fix 3D-   -02:32:09-
-Status-------------------------------------------------------------------------
 Found new probed network "<no ssid>" bssid 00:0D:88:C6:FA:22
 ALERT: Suspicious client 00:0D:3A:1F:07:A5 - probing networks but never participating.
 ALERT: Suspicious client 00:0D:3A:1F:07:A5 - probing networks but never participating.
 ALERT: Suspicious client 00:0D:3A:1F:07:A5 - probing networks but never participating.
-Battery: AC 108%---------------------------------------------------------------
```

Figure - 29 WarDrive data (Platinum Version displayed)

Sniffing a wireless network is a particularly useful way to identify who is using a network or for what purposes the network is being used (important steps if you've detected an unauthorized wireless network within the organization).

Finally, one of the unique features of Kismet is the ability to detect a wireless access point's SSID even if the access point is not broadcasting its name. This feature is called "decloaking" and is accomplished automatically through analysis of the wireless traffic. As soon as Kismet detects the name of an access point that is labeled <no SSID>, an alert will be displayed in the bottom area of the main Kismet window within the Status area informing the user. In Figure 30, an access point previously labeled <no SSID> has been decloaked and will now appear in the main screen network list as <aybabtu>:



```
 Found SSID "aybabtu" for cloaked network BSSID 00:16:B6:A7:2E:49
 Found new network "Betsch" bssid 00:0F:B3:5E:1B:B9 Crypt Y Ch 11
 Found IP 192.168.1.50 for aybabtu::00:11:09:16:21:62 via ARP
 Locking source 'madwifi_g' to channel 11
```

Figure - 30 SSID Dection

Figure 30 displays what is shown in the information panel of Kismet. Figure 19 on page 24 displays (in blue) a decloaked network named “<we the people>”.

Kismet has many other features that are not covered in this document and will doubtless add more as the author has time. For further documentation on Kismet and its use, consult http://www.kismetwireless.net/documentation.shtml .

The WhirlWind integration team would like to thank the author of Kismet for the dedication and hard work in developing such an application.

GPS Data Mapping

The following display examples are produced by WhirlWind utilizing Futures' DustDevil tool which extracts pertinent information to make .KML (Keyhole Markup Language). The resulting .KML file can be opened using the Google Earth™ application available at http://earth.google.com/download-earth.html. The viewing of WhirlWind output data is accomplished on a separate system with an Internet connection.

A typical wardrive, when displayed in Google Earth™, might look like the following from Google Earth™ version 4.0.2416. This screen may vary due to Google Earth™ API being updated from time-to-time.

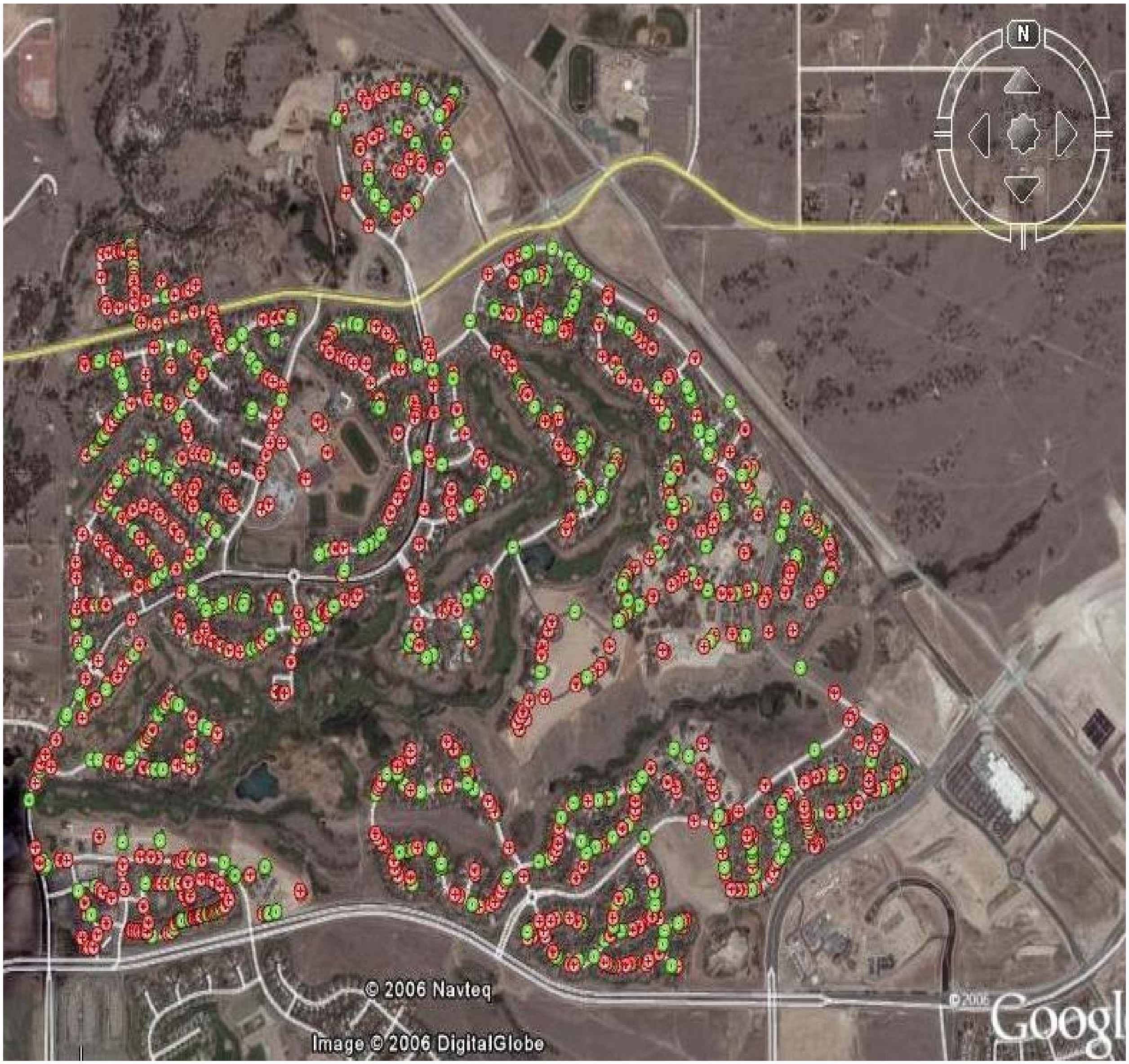


Figure - 31 GoogleEarth™ Wardrive results

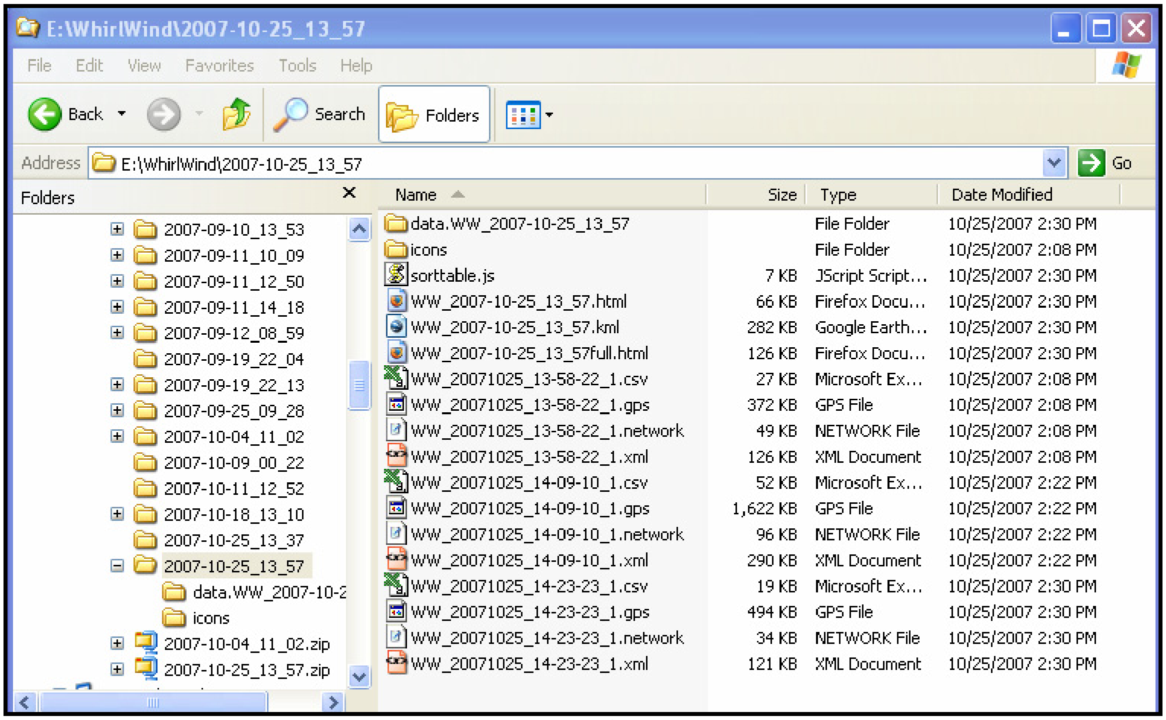
Storage and Operations

Storage

Early in the setup process, a selection was made as to where to store data being produced by Kismet. On that storage device, all the data produced during that boot is stored in a directory named with the date and time (Date-Time-Group (DTG)) of the system boot.

E:\WhirlWind\2007-10-25_13_17 = Oct 25 2007 1:17 PM

Below is the content of that directory from a single boot, which involved starting and stopping Kismet 3 times (voluntarily) during the run.



- 2007-09-10_13_53
- 2007-09-11_10_09
- 2007-09-11_12_50
- 2007-09-11_14_18
- 2007-09-12_08_59
- 2007-09-19_22_04
- 2007-09-19_22_13
- 2007-09-25_09_28
- 2007-10-04_11_02
- 2007-10-09_00_22
- 2007-10-11_12_52
- 2007-10-18_13_10
- 2007-10-25_13_37
- 2007-10-25_13_57
  - data.WW_2007-10-2
  - icons
- 2007-10-04_11_02.zip
- 2007-10-25_13_57.zip

Name	Size	Type	Date Modified
data.WW_2007-10-25_13_57		File Folder	10/25/2007 2:30 PM
icons		File Folder	10/25/2007 2:08 PM
sortable.js	7 KB	JScript Script...	10/25/2007 2:30 PM
WW_2007-10-25_13_57.html	66 KB	Firefox Docu...	10/25/2007 2:30 PM
WW_2007-10-25_13_57.kml	282 KB	Google Earth...	10/25/2007 2:30 PM
WW_2007-10-25_13_57full.html	126 KB	Firefox Docu...	10/25/2007 2:30 PM
WW_20071025_13-58-22_1.csv	27 KB	Microsoft Ex...	10/25/2007 2:08 PM
WW_20071025_13-58-22_1.gps	372 KB	GPS File	10/25/2007 2:08 PM
WW_20071025_13-58-22_1.network	49 KB	NETWORK File	10/25/2007 2:08 PM
WW_20071025_13-58-22_1.xml	126 KB	XML Document	10/25/2007 2:08 PM
WW_20071025_14-09-10_1.csv	52 KB	Microsoft Ex...	10/25/2007 2:22 PM
WW_20071025_14-09-10_1.gps	1,622 KB	GPS File	10/25/2007 2:22 PM
WW_20071025_14-09-10_1.network	96 KB	NETWORK File	10/25/2007 2:22 PM
WW_20071025_14-09-10_1.xml	290 KB	XML Document	10/25/2007 2:22 PM
WW_20071025_14-23-23_1.csv	19 KB	Microsoft Ex...	10/25/2007 2:30 PM
WW_20071025_14-23-23_1.gps	494 KB	GPS File	10/25/2007 2:30 PM
WW_20071025_14-23-23_1.network	34 KB	NETWORK File	10/25/2007 2:30 PM
WW_20071025_14-23-23_1.xml	121 KB	XML Document	10/25/2007 2:30 PM

Figure - 32 Storage directory Layout

There are 3 types of entities found in this directory.

1. Other sub-directories
2. Files created with each Kismet run:
    a. .csv, .xml, .network – default files
    b. .gps:
        i. Enabled by default on Bronze – Gold versions
        ii. if enabled by the user - Platinum version
    c. .dump:
        i. Not enabled on Bronze and Silver versions
        ii. Enabled by default on Gold version
        iii. If enabled by the user – Platinum version
3. Files created by WhirlWind processes (.js, .html, .kml)

File names created by Kismet are:

- “WW_”
- the DTG when Kismet run started
- a sequence number for uniqueness (generally “_1”)
- file extension associated with the file type
    - “.csv” – network data in a “comma separated values”, text format
    - “.gps” – detailed GPS data in an XML format
    - “.network” – network list in a textual “paragraph” format
    - “.xml” – network list in an XML format
    - “.dump” – raw traffic dump in a “pcap” format

Files created by WhirlWind are:

- “.js” – javascript to sort the .html display
- “.html” – network data in a browser file
- “.kml” – Google Earth™ displayable script in “keyhole markup language”

Directories are:

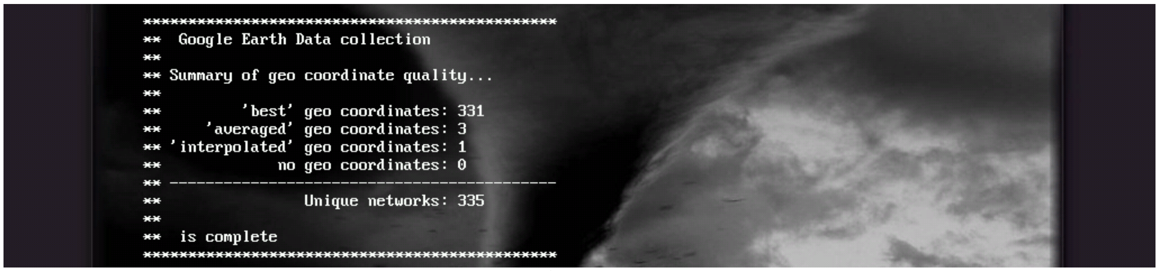
- “icons” – due to fluctuations in the GE API, local pushpin images are included
- “data.”BootDTG – individual .html files, 1 per network

During a Kismet run, data is written to storage every 60 seconds. It is also written a final time when Kismet is shutdown with a ‘Q’ keypress.

Operations

After Kismet has terminated, a WhirlWind process called “DustDevil” (DD) runs. DustDevil processes all of the .csv files found in the storage directory. See the figure below for an example screenshot for DD data processing.

- The contents of all of the .csv files are merged together and analyzed.
- The “best” geolocation data for each unique BSSID is processed into the Dustdevil .kml, and .html files.
- A summary count is displayed on Console #1
    - Total networks (BSSIDs) for the aggregate .kml
    - Count of “BEST” geolocation as identified by Kismet
    - Count of “Averaged” geolocation. These networks did not have a “Best” identified by Kismet; but did have Max/Min geolocation; the center of which will be plotted.
    - Count of “Interpolated” geolocation. These BSSIDs did not have valid location data, and are positioned midway between prior and next networks. Invalid location data are floating point multiples of 90.0° (0.0, 90.0,180.0)
- The WiFi card selection process starts again.



```
***********************************************
**  Google Earth Data collection
**
** Summary of geo coordinate quality...
**
**        'best' geo coordinates: 331
**    'averaged' geo coordinates: 3
** 'interpolated' geo coordinates: 1
**            no geo coordinates: 0
** --------------------------------------------
**               Unique networks: 335
**
**  is complete
***********************************************
```

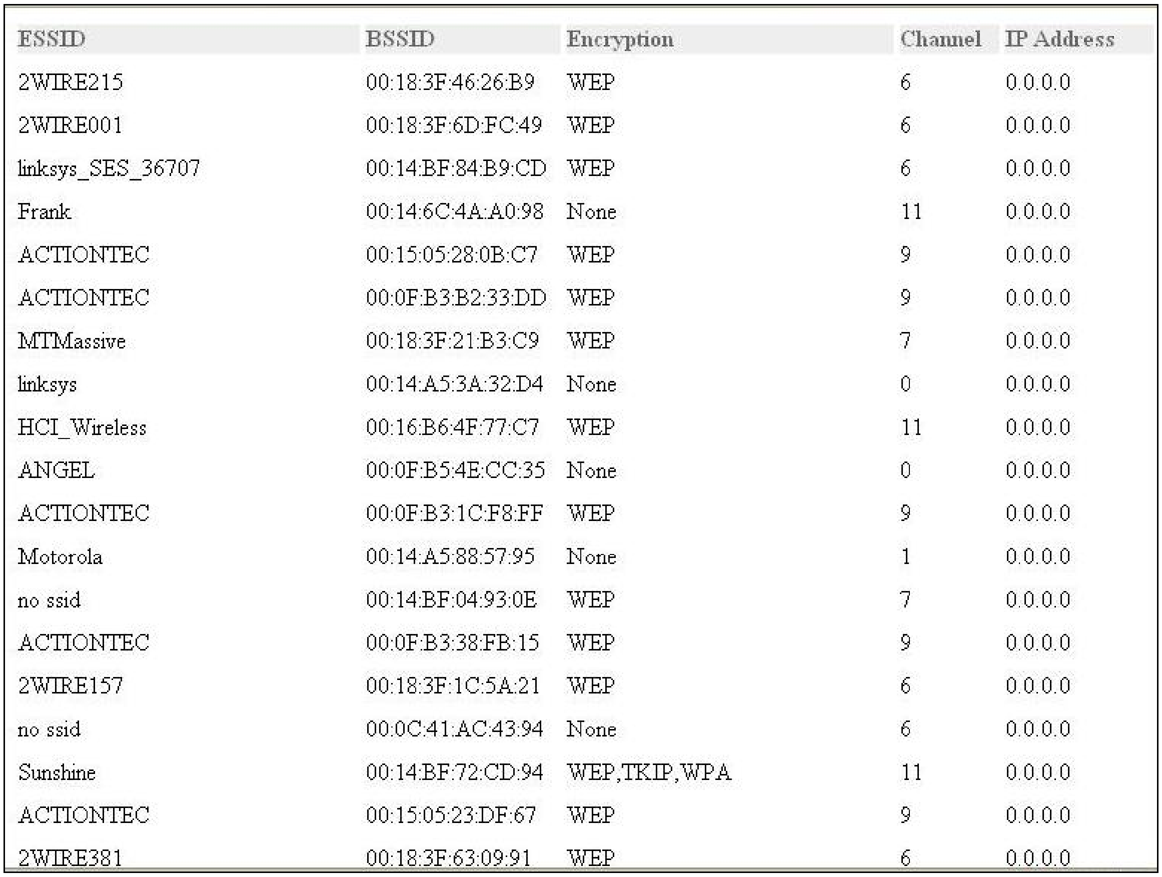
Figure - 33 DustDevil Processing Mapping Data

NOTE:

If operations of WhirlWind are terminated by a summary “power-off” or Ctl-Alt-Del while Kismet is running; DustDevil will not be given the opportunity to process the final (only) .csv file. This will result in either no .kml will be present or, in the case of multiple Kismet runs, the .kml will not include the final .csv file’s data.

Resulting Product

An HTML summary of the wireless networks shown in the prior image looks like the following:

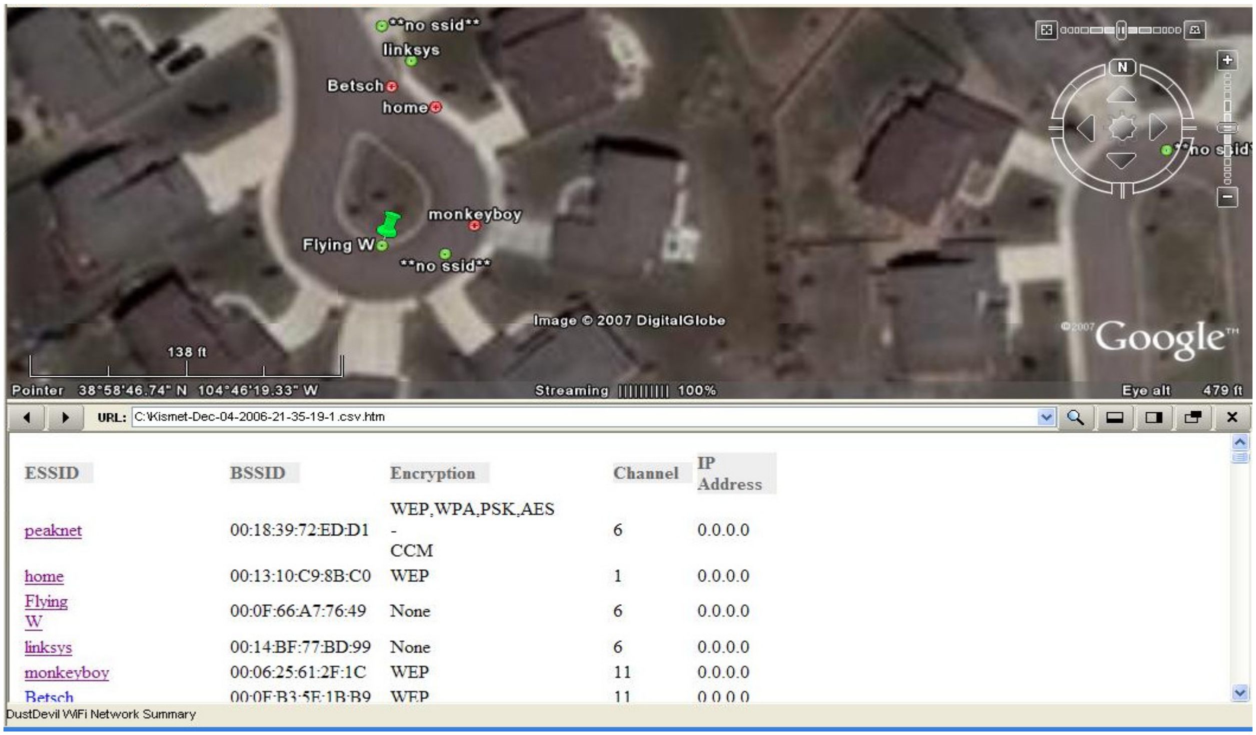


ESSID	BSSID	Encryption	Channel	IP Address
2WIRE215	00:18:3F:46:26:B9	WEP	6	0.0.0.0
2WIRE001	00:18:3F:6D:FC:49	WEP	6	0.0.0.0
linksys_SES_36707	00:14:BF:84:B9:CD	WEP	6	0.0.0.0
Frank	00:14:6C:4A:A0:98	None	11	0.0.0.0
ACTIONTEC	00:15:05:28:0B:C7	WEP	9	0.0.0.0
ACTIONTEC	00:0F:B3:B2:33:DD	WEP	9	0.0.0.0
MTMassive	00:18:3F:21:B3:C9	WEP	7	0.0.0.0
linksys	00:14:A5:3A:32:D4	None	0	0.0.0.0
HCI_Wireless	00:16:B6:4F:77:C7	WEP	11	0.0.0.0
ANGEL	00:0F:B5:4E:CC:35	None	0	0.0.0.0
ACTIONTEC	00:0F:B3:1C:F8:FF	WEP	9	0.0.0.0
Motorola	00:14:A5:88:57:95	None	1	0.0.0.0
no ssid	00:14:BF:04:93:0E	WEP	7	0.0.0.0
ACTIONTEC	00:0F:B3:38:FB:15	WEP	9	0.0.0.0
2WIRE157	00:18:3F:1C:5A:21	WEP	6	0.0.0.0
no ssid	00:0C:41:AC:43:94	None	6	0.0.0.0
Sunshine	00:14:BF:72:CD:94	WEP,TKIP,WPA	11	0.0.0.0
ACTIONTEC	00:15:05:23:DF:67	WEP	9	0.0.0.0
2WIRE381	00:18:3F:63:09:91	WEP	6	0.0.0.0

Figure - 34 HTML Summary

Additionally, when you select a network in the HTML summary, Google Earth™ will pan to the spot on the map where the network is shown and it will place a “pushpin” on the map to show you where the network is located (see Figure 34). This was done for two purposes – first, at times it was somewhat difficult to find the network of interest due to congestion or duplicate network names (like *No SSID*). Second, placing a pushpin on the map prevents Google Earth™ from creating a duplicate poker chip (the green or red icon) in the same place as the existing icon for the selected network.

Finally, it should be noted that all icons/pushpins are pulled down directly from Google Maps rather than a specific path on the hard drive. This will help avoid problems if a user has installed Google Earth™ to a non-standard directory or if they're running Google Earth™ on a Linux platform. These icons/pushpins get cached so the user does not have to be connected to the Internet each time they try to access them. It should be pointed out that only networks that have hyperlinks have had enough information to place a “pushpin” location for the network on Google Earth™.



URL: C:\Kismet-Dec-04-2006-21-35-19-1.csv.htm

ESSID	BSSID	Encryption	Channel	IP Address
peaknet	00:18:39:72:ED:D1	WEP,WPA,PSK,AES - CCM	6	0.0.0.0
home	00:13:10:C9:8B:C0	WEP	1	0.0.0.0
Flying W	00:0F:66:A7:76:49	None	6	0.0.0.0
linksys	00:14:BF:77:BD:99	None	6	0.0.0.0
monkeyboy	00:06:25:61:2F:1C	WEP	11	0.0.0.0
Betsch	00:0F:B3:5E:1B:B9	WEP	11	0.0.0.0

Figure - 35 HTML Summary w/ PushPin

Using the Google Earth™ application, it is also possible to zoom in for a close up of the WiFi environment. Individual networks might look like this:

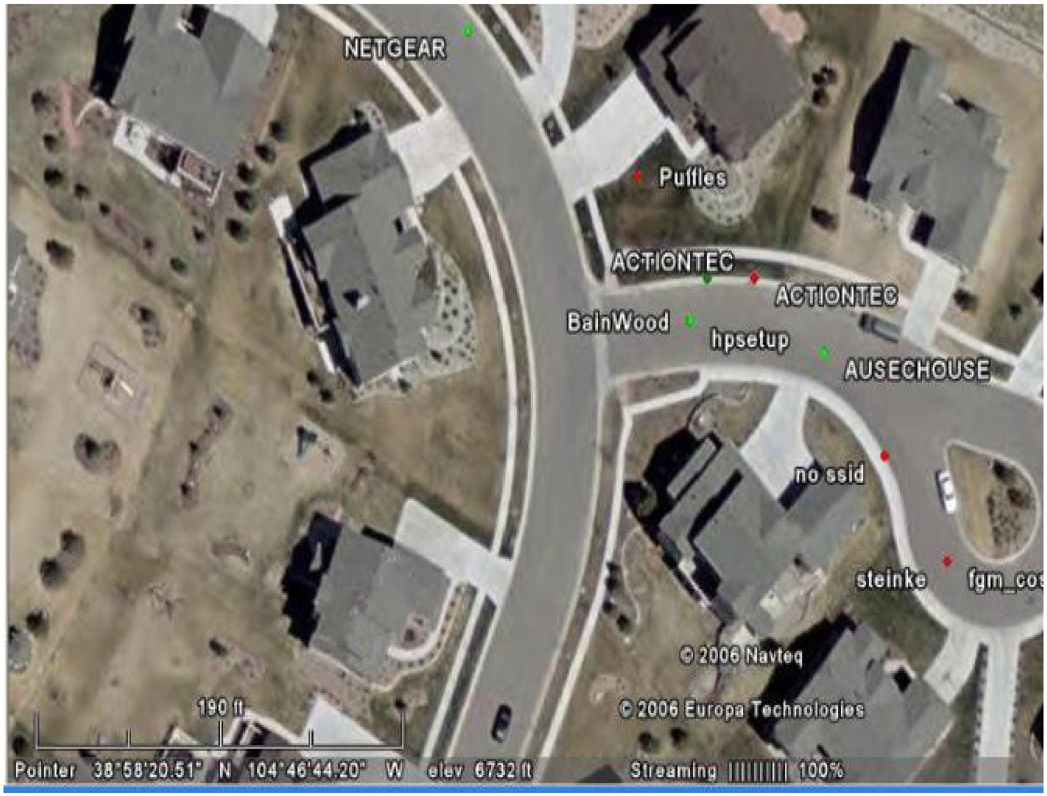
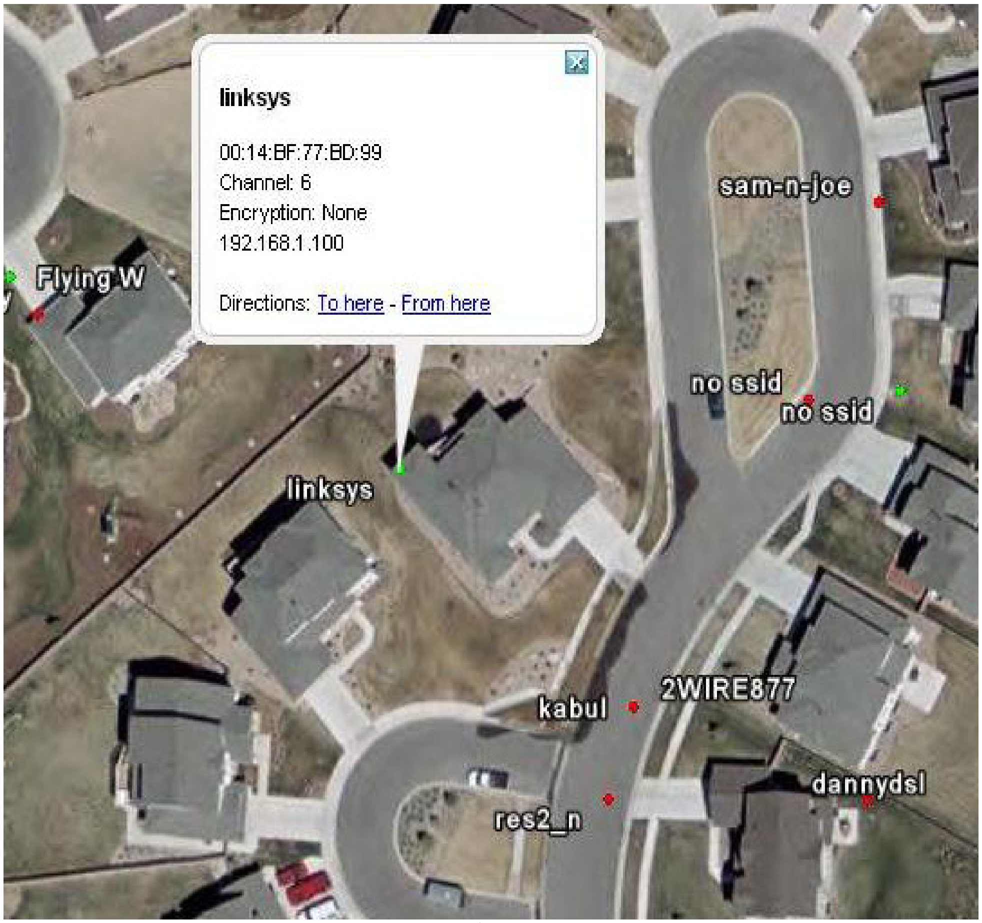


Figure - 36 Google Earth™ Mapping Close-up

By selecting a specific point (WiFi network) on the map, metadata concerning the wireless network is displayed in a pop-up box:



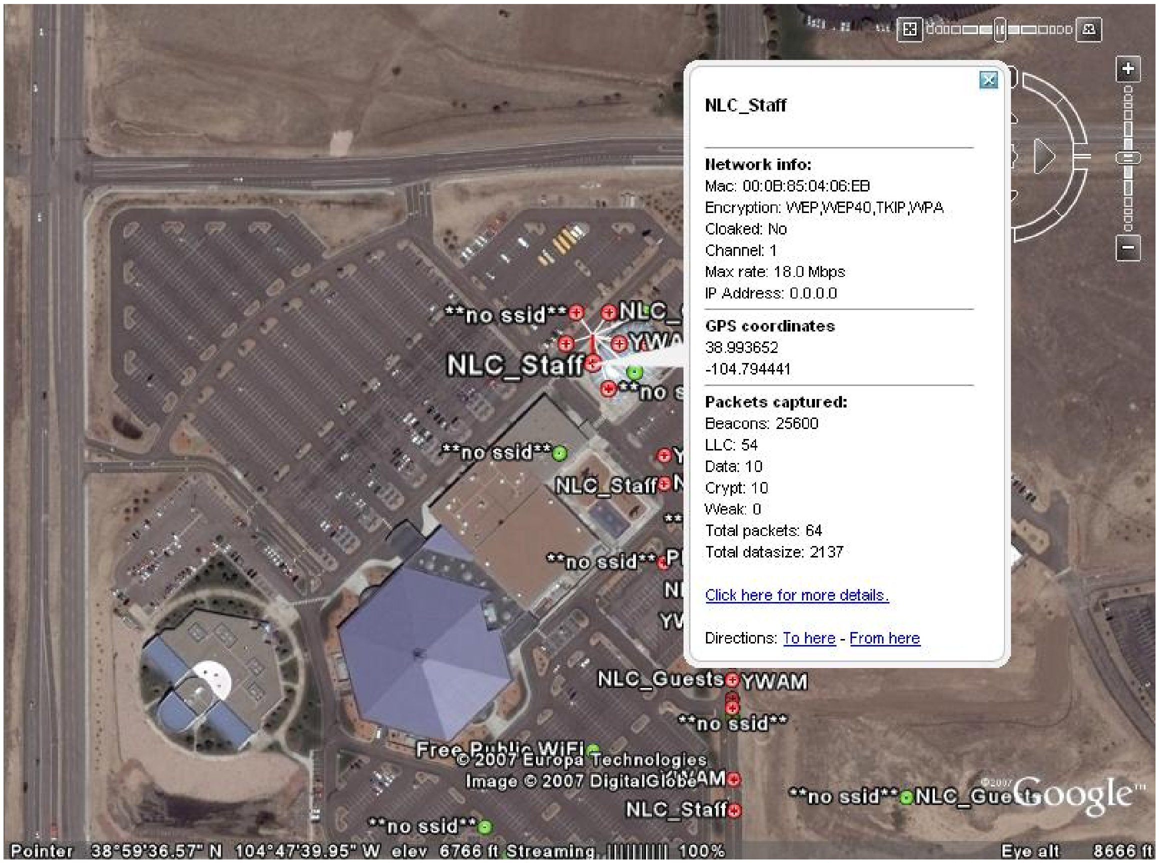
linksys

00:14:BF:77:BD:99
Channel: 6
Encryption: None
192.168.1.100

Directions: To here - From here

Figure - 37 Network Information Pop-Up

The following figure illustrates the robust relationship that DustDevil has with Kismet output data. There are increased data field displays within the bubble. For example – data rate displays and GPS coordinates. In addition, the bubble provides enhanced packet capture definition.



NLC_Staff

Network info:
Mac: 00:0B:85:04:06:EB
Encryption: WEP,WEP40,TKIP,WPA
Cloaked: No
Channel: 1
Max rate: 18.0 Mbps
IP Address: 0.0.0.0

GPS coordinates
38.993652
-104.794441

Packets captured:
Beacons: 25600
LLC: 54
Data: 10
Crypt: 10
Weak: 0
Total packets: 64
Total datasize: 2137

Click here for more details.

Directions: To here - From here

Figure - 38 Detailed Network Information Popup with Data Fields

Living Document

This user manual is written as a living document to provide the most current information, and subject to change as new capabilities are included in WhirlWind and as new devices for WhirlWind are tested.

Appendix A – Tested WiFi Cards

The following table illustrates some of the WiFi cards tested by the WhirlWind developers and whether or not the card was identified by the OS (Worked). As of this printing it is highly recommended that cards with the Atheros chip set NOT be used with the Whirl Wind product. Although recognized by the operating system testing has determined there are driver faults, at this time which may cause the card to stop working at an undetermined time period from start.

Manufacturer	Model	Chipset	Technology	Results
3Com	3CRPAG175B Rev:AA	Atheros (Atheros Communications, Inc. AR5006X 802.11abg NIC (rev 01)	PCMCIA	PASS* *not advised
3Com	3CRXJK10075 Rev:AB	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01)	PCMCIA	PASS*
Aerielink	AWPC3101	PrismGT (Intersil Corporation ISL3890 [Prism GT/Prism Duette]/ISL3886 [Prism Javelin/Prism Xbow] (rev 01))	PCMCIA	PASS
Airnet	AWN108	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Aries Dual Band	NL-5354CB	Atheros	PCMCIA	PASS*
Asus	WL-107G	Ralink b/g (RaLink RT2500 802.11g Cardbus/mini-PCI (rev 01))	PCMCIA	PASS
Asus	WL-167G	Ralink (Ralink USB)	USB	PASS
Belkin	F5D7010 v3001	Ralink b/g	PCMCIA	PASS
Belkin	F5D7011	Broadcom (Broadcom Corporation BCM4306 802.11b/g Wireless LAN Controller (rev 03))	PCMCIA	PASS
Buffalo	WLI-CB-G54HP	Broadcom	PCMCIA	PASS
Buffalo	WLI-CB-G54S	Broadcom	PCMCIA	PASS
Cisco	AIR-CB21AG-A-K9 Rev:A0	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
D-Link	DWL-G122	Ralink (rt2500)	USB	PASS
D-Link	DWL-G650 v2.54	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
D-Link	DWL-AG660 v1.29	Atheros (Atheros Communications, Inc. AR5212	PCMCIA	PASS*

		802.11abg NIC (rev 01))		
D-Link	DWL-G680 v1.00	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
D-Link	DWL-G630 v3.00	Atheros (Atheros Communications, Inc. AR5005G 802.11abg Wireless NIC (rev 01))	PCMCIA	PASS*
D-Link	DWL-G630 v3.01	Atheros (Atheros Communications, Inc. AR5005G 802.11abg Wireless NIC (rev 01))	PCMCIA	PASS*
D-Link	DWL-G650 v2.54	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
EDIMAX	EW-7108PCg	Ralink b/g (RaLink RT2500 802.11g Cardbus/mini-PCI (rev 01))	PCMCIA	PASS
Encore Electronics	ENPWI-SG	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Gigabyte Technology	GN-WBKG	Ralink (Ralink USB)	USB	PASS
Hawking Technologies	HWC54D	Ralink b/g (RaLink RT2500 802.11g Cardbus/mini-PCI (rev 01))	PCMCIA	PASS
Hawking Technologies	HWC54G	Ralink b/g (RaLink RT2500 802.11g Cardbus/mini-PCI (rev 01))	PCMCIA	PASS
Intel	IPW-2200	IPW-2200	MiniPCI	PASS
JAHT	WN-5054P	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Level 1	WPC-0300	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Linksys	WPC11 v3	Orinoco	PCMCIA	PASS
Linksys	WPC11 v4	RTL8180 (RealTek Semiconductor Co., Ltd. RTL8180L 802.11b MAC (rev 20))	PCMCIA	PASS
Linksys	WPC54G v1	Broadcom	PCMCIA	PASS
Linksys	WPC54G v3	Broadcom (Broadcom Corporation BCM4318 [AirForce One 54g] 802.11g Wireless LAN Controller (rev 02))	PCMCIA	PASS
Linksys	WPC54GS v1.1	Broadcom (Broadcom Corporation BCM4306 802.11b/g Wireless LAN Controller (rev 03))	PCMCIA	PASS
Linksys	WPC54GS v2	Broadcom (Broadcom Corporation BCM4318 [AirForce One 54g] 802.11g Wireless LAN Controller	PCMCIA	PASS

		(rev 02))		
Linksys	WPC55AG v1.1	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Linksys	WUSB54G v4	Ralink (Ralink USB)	USB	PASS
Linksys	WUSB54GP	Ralink (Ralink USB)	USB	PASS
Lucent Technologies	PC24E-H-FC (Orinoco Gold)	HERMES I (orinoco_cs)	PCMCIA	PASS
MSI	MS-6861	Ralink (Ralink USB)	USB	PASS
Netgear	WG511 (Not V3)	PrismGT 802.11g	PCMCIA	PASS
Netgear	WG511T	Atheros	PCMCIA	PASS*
Netgear	WG511U	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Netgear	WPN511	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Nova Tech	NV914	Ralink b/g (RaLink RT2500 802.11g Cardbus/mini-PCI (rev 01))	PCMCIA	PASS
SMC	SMC2336W-AG	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
SMC	SMC2532W-B	HERMES I	PCMCIA	PASS
SMC	SMCWCB-G	Atheros (Atheros Communications, Inc. AR5005G 802.11abg NIC (rev 01))	PCMCIA	PASS*
SMC	SMCWCT-G	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
TRENDnet	TEW-441PC	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
TRENDnet	TEW-501PC	Atheros (Atheros Communications, Inc. AR5006X 802.11abg NIC (rev 01))	PCMCIA	PASS*
Zonet	ZEW2500P	Ralink (Ralink USB)	Mini USB end cable	PASS
Zyxel	G-102 v2	Atheros (Atheros Communications, Inc. AR5212 802.11abg NIC (rev 01))	PCMCIA	PASS*
Zyxel	G-110	PrismGT 802.11g Card Bus w/Ext. Antenna Connector	PCMCIA	PASS
Zyxel	G-162	Texas Instruments ACX 111 54Mbps Wireless Interface	PCMCIA	PASS

Table - 1 Tested WiFi Cards

Appendix B – Tested WiFi Chip sets

The following table illustrates chipset compatibility as it applies to Kismet server recognition.

WiFi Chipset	Identified	Form Factor	Kismet Server Starts	Functional	Notes
Atheros	Yes	PCMCIA	Yes	Yes*	*Current drivers do not provide long term support for card use. *
Broadcom	Yes	miniPCI	Yes	Yes	No known issues as of 7/23/07
Broadcom	Yes	PCMCIA	Yes	Yes	No know issues as of 8/24/07
Centrino b/g	Yes	PCMCIA	Yes	Yes	No known issues as of 7/23/07
Centrino b/g	Yes	miniPCI	Yes	Yes	No known issues as of 7/23/07
Hermes I	Yes	PCMCIA	Yes	Yes	No known issues as of 7/23/07
PrismGT	Yes	PCMCIA	Yes	Yes	No known issues as of 9/07/07
Ralink b/g	Yes	PCMCIA	Yes	Yes	No known issues as of 7/23/07
Ralink USB	Yes	USB	Yes	Yes	No known issues as of 7/23/07
RTL8180 (RealTek)?	Yes	PCMCIA	Yes	Yes	No known issues as of 7/23/07

Table - 2 Tested WiFi Chip sets

Appendix C – Tested GPS Devices

Within the WhirlWind build, developers have wrapped within the open-source software “gpsd”. Gpsd is a daemon that monitors one or more GPS devices attached to the computer through the USB or serial ports. Multiple GPS client applications can share access to GPSes without contention or loss of data. As of this printing, gpsd version 2.34 is being used.

Developers and other contributors of gpsd have put together an extensive listing of GPS devices and their chipsets that have worked with various versions of GPSD. This listing may be found at *http://gpsd.berlios.de/hardware.html*.

The following table illustrates the GPS Devices that have been tested by WhirlWind developers.

Manufacturer	Model	Connection Type	Readable GPS Information	Notes
DeLORME	Earthmate LT-20	USB	No	No detection or response
Garmin	eMap	Serial to USB	Yes	Generic NMEA 4899 8N1
Garmin	GPSmap 76S	USB to Serial	Yes	4800 Baud GPS Device over serial line
GlobalSat	BU-353	USB	Yes	Sporadic misreads And Solid performer See Below
Pharos	GPS-360	USB	Yes	

Table - 3 Tested GPS Devices

During testing of USB GPS devices, it was found that devices that looked to be identical, performed radically differently. The key difference was in the firmware present in the device.

This value, among others, can be seen in the display of the “cgps” program running on Console #9. This display is present to simply display activity of the GPS. This program receives the very same data as Kismet.

The specific device was labeled “BU-353”. It is a black disc, just over 2 in. in diameter with beveled edges, with a grey label on the top.

One of these devices had a serial number “BUW19603” and a “cold fix” at startup would take 1.5-2 minutes.

The other was serial number “BU26903” and it took only 20 seconds to make a cold fix in the same location. The fundamental difference between the two was the SiRF firmware.

The firmware versions, were:

- GSW3.0.2-GS_3.0.00.03-C5P1.02b == 90 second cold fix
- GSW3.2.2_3.1.00.12_SDK C-03P1.01a == 20 second cold fix

The 3.2.2 firmware was the current firmware at the time of the testing. Obviously, improvements had been made since 3.0.2. Unfortunately, the firmware is not a value published in catalog specification.

Appendix D – End User License Agreement (EULA)

WhirlWind 1.0
Futures Software License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY. BY USING THE SOFTWARE (INCLUDING ITS COMPONENTS), YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT DOWNLOAD OR USE THE SOFTWARE AND, IF APPLICABLE, RETURN THE ENTIRE UNUSED PACKAGE TO THE RESELLER WITH YOUR RECEIPT FOR A REFUND. THE SOFTWARE MAY NOT BE SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED WITHOUT PRIOR WRITTEN AUTHORIZATION FROM FUTURES.

RIGHTS AND LICENSES

This Futures Software License Agreement ("Agreement") is a legal agreement between You (an entity or a person) and Futures, Inc. ("Futures") with respect to the software product identified in the title of this Agreement, media (if any) and accompanying documentation (collectively the "Software").

The Software is a collective work of Futures. You must acquire a license for each installation of the Software and for each additional copy (or partial copy) of the Software stored or loaded in memory or virtual memory beyond the initial copy necessary for execution of the Software installed on the hardware.

The Software is a modular operating system. Most of the components are open source packages, developed independently, and accompanied by separate license terms. Your license rights with respect to individual components accompanied by separate license terms are defined by those terms; nothing in this Agreement shall restrict, limit, or otherwise affect any rights or obligations You may have, or conditions to which You may be subject, under such license terms.

While the license terms for a component may authorize You to distribute the component, You may not use any Futures marks (e.g., WhirlWind) in distributing the component, whether or not the component contains Futures marks.

OTHER LICENSE TERMS AND RESTRICTIONS

The Software is protected by the copyright laws and treaties of the United States ("U.S.") and other countries and is subject to the terms of this Agreement. The Software is licensed to You, not sold.

The Software may be bundled with other software programs ("Bundled Programs"). Your license rights with respect to Bundled Programs accompanied by separate license terms are defined by those terms;nothing in this Agreement shall restrict, limit, or otherwise affect any rights or obligations You may have, or conditions to which You may be subject, under such license terms.

Futures reserves all rights not expressly granted to You. You may not: (1) reverse engineer, decompile, or disassemble the Software except and only to the extent it is expressly permitted by applicable law or the license terms accompanying a component of the Software; or (2) transfer the Software or Your license rights under this Agreement, in whole or in part.

MAINTENANCE AND SUPPORT

Your rights with respect to updates, patches, or other materials received under a subscription to a Futures maintenance program for the Software are defined by the relevant maintenance program terms.

Futures has no obligation under this Agreement to provide maintenance or support for the Software. Depending on how You acquired the Software, You may have also acquired a maintenance subscription for the Software. For more information on Futures' current maintenance and support offerings, see http://www.futures-inc.com/.

OWNERSHIP RIGHTS

No title to or ownership of the Software is transferred to You. Futures and/or its licensors owns and retains all title and ownership of all intellectual property rights in the Software, including any adaptations or copies. You acquire only a license to use the Software.

LIMITED WARRANTY

For ninety (90) days from Your date of purchase, Futures warrants that (1) any media on which the Software is delivered is free from physical defects; and (2) the Software will substantially conform to the documentation accompanying the Software. If the defective items are returned to Futures or if You report the nonconformity to Futures within ninety (90) days from the date of purchase, Futures will at its sole discretion either resolve the nonconformity or refund the license fees You paid for the Software. Any misuse or unauthorized modification of the Software voids this warranty. THE FOREGOING WARRANTY IS YOUR SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. (The foregoing warranty does not apply to Software provided free of charge. SUCH SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND.)

THE SOFTWARE IS NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR DISTRIBUTION WITH ON-LINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, COMMUNICATION, OR CONTROL SYSTEMS, DIRECT LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR OTHER USES IN WHICH FAILURE OF THE SOFTWARE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE.

THE SOFTWARE IS ONLY COMPATIBLE WITH CERTAIN COMPUTERS AND OPERATING SYSTEMS. THE SOFTWARE IS NOT WARRANTED FOR NON-COMPATIBLE SYSTEMS. Call Futures for information about compatibility.

Non-Futures Products. The Software may include or be bundled with hardware or other software programs licensed or sold by a licensor other than Futures. FUTURES DOES NOT WARRANT NON-FUTURES PRODUCTS. ANY SUCH PRODUCTS ARE PROVIDED ON AN "AS IS" BASIS. ANY WARRANTY SERVICE FOR NON-FUTURES PRODUCTS IS PROVIDED BY THE PRODUCT LICENSOR IN ACCORDANCE WITH THE APPLICABLE LICENSOR WARRANTY.

EXCEPT AS OTHERWISE RESTRICTED BY LAW, FUTURES DISCLAIMS AND EXCLUDES ANY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. FUTURES MAKES NO WARRANTY, REPRESENTATION OR PROMISE NOT EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY. FUTURES DOES NOT WARRANT THAT THE SOFTWARE WILL SATISFY YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED. Some jurisdictions do not allow certain disclaimers and limitations of warranties, so portions of the above limitations may not apply to You. This limited warranty gives You specific rights and You may also have other rights which vary from state to state.

LIMITATION OF LIABILITY

(a) Consequential Losses. NEITHER FUTURES NOR ANY OF ITS LICENSORS, SUBSIDIARIES, OR EMPLOYEES WILL IN ANY CASE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT, TORT, ECONOMIC OR PUNITIVE DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS OR DATA, EVEN IF ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.

(b) Direct Damages. IN NO EVENT WILL FUTURES' AGGREGATE LIABILITY FOR DIRECT DAMAGES TO PROPERTY OR PERSON (WHETHER IN ONE INSTANCE OR A SERIES OF INSTANCES) EXCEED 1.25 TIMES THE AMOUNT PAID BY YOU FOR THE SOFTWARE OUT OF WHICH SUCH CLAIM AROSE [OR $50 (U.S.) IF YOU RECEIVED THE SOFTWARE FREE OF CHARGE]. The above exclusions and limitations will not apply to claims relating to death or personal injury. In those jurisdictions that do not allow the exclusion or limitation of damages, Futures' liability shall be limited or excluded to the maximum extent allowed within those jurisdictions.

GENERAL TERMS

Term. This Agreement becomes effective on the date You legally acquire the Software and will automatically terminate if You breach any of its terms. Upon termination of this Agreement, You must destroy the original and all copies of the Software or return them to Futures and delete the Software from Your systems.

Benchmark Testing. This benchmark testing restriction applies to You if You are a software vendor or if You are performing testing on the Software at the direction of or on behalf of a software vendor. You may not, without Futures' prior written consent not to be unreasonably withheld, publish or disclose to any third party the results of any benchmark test of the Software. If You are a vendor of products that are functionally similar to or compete with the Software ("Similar Products"), or are acting on behalf of such a vendor, and You publish or disclose benchmark information on the Software in violation of this restriction, then notwithstanding anything to the contrary in the Similar Product's end user license agreement, and in addition to any other remedies Futures may have, Futures shall have the right to perform benchmark testing on Similar Products and to disclose and publish that benchmark information and You hereby represent that You have authority to grant such right to Futures.

Transfer. This Agreement may not be transferred or assigned without the prior written approval of Futures.

Law and Jurisdiction. This Agreement is governed by the laws of the State of Maryland, U.S. Any action at law relating to this Agreement may only be brought before the courts of competent jurisdiction of the State of Maryland. If, however, Your country of principal residence is a member state of the European Union or the European Free Trade Association, this Agreement is governed by the laws of that country, and any action at law may only be brought before a court of competent jurisdiction of that country.

Entire Agreement. This Agreement and the Upgrade/Additive Agreement (if applicable) sets forth the entire understanding and agreement between You and Futures and may be amended only in a writing signed by both parties. NO LICENSOR, DISTRIBUTOR, DEALER, RETAILER, RESELLER, SALES PERSON, OR EMPLOYEE IS AUTHORIZED TO MODIFY THIS AGREEMENT OR TO MAKE ANY REPRESENTATION OR PROMISE THAT IS DIFFERENT FROM, OR IN ADDITION TO, THE TERMS OF THIS AGREEMENT.

Waiver. No waiver of any right under this Agreement will be effective unless in writing, signed by a duly authorized representative of the party to be bound. No waiver of any past or present right arising from any breach or failure to perform will be deemed to be a waiver of any future right arising under this Agreement.

Severability. If any provision in this Agreement is invalid or unenforceable, that provision will be construed, limited, modified or, if necessary, severed, to the extent necessary, to eliminate its invalidity or unenforceability, and the other provisions of this Agreement will remain unaffected.

Export Compliance. Any person or entity exporting or re-exporting Futures products directly or indirectly and via any means, including electronic transfer, is wholly responsible for doing so in accordance with the U.S. Export Administration Regulations and the laws of host countries. Futures assumes no responsibility or liability for your failure to obtain any necessary export approvals. Approvals are dependent upon an item's technical characteristics, the destination, end-use and end-user, as well as other activities of the end user. Specifically, no Futures product may be exported to embargoed or otherwise restricted countries or end users. Please consult the Bureau of Industry and Security web page and other sources before exporting Futures products from the U.S. and familiarize yourself with the laws of destination countries before re-exporting Futures products. This provision shall survive the expiration or earlier termination of this Agreement.

U.S. Government Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions in FAR 52.227-14 (June 1987) Alternate III (June 1987), FAR 52.227-19 (June 1987), or DFARS 252.227-7013 (b)(3) (Nov 1995), or applicable successor clauses. Contractor/Manufacturer is Futures, Inc., 1225 Crows Foot Road, Marriottsville, Maryland 21104.

Other. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

Linux is a registered trademark of Linus Torvalds.

Acronyms and Glossary

ACCESS POINT – The hub of a wireless network

AES – Advanced Encryption Standard is a fast, secure symmetric algorithm.

API – Application Programming Interface. A code interface that a computer application, operating system, or library provides to support requests for services by the computer program.

BSSID – Basic Service Set Identifier. The MAC address of a station in a wireless access point.

GPS – Geo Positioning System

IEEE 802.11 – A family of Wireless Local Area Network (WLAN) specifications developed by the IEEE standards committee in the 5 GHz and 2.4 GHz public spectrum bands.

KML – Keyhole Markup Language

MIC – Message Integrity Check is a component of TKIP and is used to check the key values. If the key value has been tampered with WPA stops using those keys and re-keys.

PCMCIA – Personal Computer Memory Card International Association. The standards organization responsible for the form factors for the PC card.

PSK – Pre Shared Key is a type of WPA whereby the user can configure their own key.

SSID – Service Set Identifier, the network name that identifies a particular WiFi access point.

TKIP – Temporal Key Integrity Protocol is a stronger encryption algorithm than the one used by WEP and is used with WPA.

USB – Universal Serial Bus

WAP – Wireless Access Point

WiFi – Wireless Fidelity

WEP – Wired Equivalent Privacy aims to provide security by encrypting data over radio waves as defined in the 802.11b standard. WEP is not difficult to crack.

WPA – WiFi Protected Access is an improved encryption standard with a higher level of security than WEP. It bridges the gap between WEP and 802.11i (WPA2) networks. WPA uses TKIP.

WPA2 – The latest implementation of WPA providing stronger data protection and network access control. There are two versions of WPA2 – Personal and Enterprise. WPA2 Personal protects network access by using a setup password. WPA2 Enterprise verifies network users through a server. A feature of WPA2 is that it uses the AES algorithm.