Chapter 4

Kismet Menus

Solutions in this chapter:

- Main display
- Popup windows
- Customizing the panels interface
- Third party front-ends

☑ Summary
☑ Solutions Fast Track
Introduction

Kismet is a text-based application that uses an ncurses/panels interface for its default front-end menus. Visually, the front ends are similar, although the ncurses interface is black and white, while the panels interface users color (see Figure 4.1). As we will see through this chapter, the value of color is immeasurable to Kismet’s panels interface in terms of the amount and value of the information it provides. In addition, the ncurses interface is a single, non-interactive display; the various secondary and popup menus specified within this chapter do not work.

Figure 4.1 Ncurses/Panels Interface

The choice of graphical user interface type to use is specified in the *kismet_ui.conf* file:

```
# Gui type to use
# Valid types: curses, panel
gui=panel
```

This file is typically located in */usr/local/etc*. The panel interface is the default, and is highly recommended. For the remainder of this chapter, all references and figures will use the panels interface.

An important feature of the Kismet panels interface is the integrated help screen. From the primary window, simply press `h` to bring up the help pop-up window (see Figure 4.2).
**Main Display**

The primary window or main display provides a general overview of Kismet’s operations (see Figure 4.3).
The display is divided into three panels: the network list panel, the information panel, and the status panel.

**Network List Panel**

The primary source of information on Kismet’s main display is the network list panel (see Figure 4.4). This panel consumes a considerable amount of screen space, and desires to strike a balance between displaying as many networks as possible, while still providing valuable information about each of those individual networks. In this section, we’ll discuss the various options to sort networks as well as the default columns and colors displayed by Kismet in the network list panel, and how they provide information to users.
Sorting
As you will note in Figure 4.4, Kismet’s default sorting mode is known as autofit. The goal of autofit is to display as many currently active networks as possible. While using autofit, network selection, tagging, grouping, scrolling, and so forth is disabled. To use any of these features, simply sort the network list by another method. To bring up the sort options, simply press s (see Figure 4.5).

Figure 4.5 Sort Options
The sort options displayed in Figure 4.5 are self-explanatory; although, as previously explained, you’ll need to choose something other than autofit to do anything useful. Service Sent Identifier (SSID) is common, and displayed in Figure 4.6:

**Figure 4.6 Networks Sorted by SSID**

Sorting also gives you a cursor-enabled selection bar that indicates which network is currently highlighted. Note in Figure 4.6, that the sort is ascending by default. In the case of first time seen, latest seen, Basic Service Sent Identifier (BSSID), SSID, and packet count, the capital letter equivalent (S rather than s) is a descending sort.

**Columns**

Kismet supports in excess of 20 column descriptions, although only the nine listed below are displayed by default (see “Customizing the Panels Interface” below for more information). Kismet will display as many columns as it can within the space provided.
Decay

The first column is *decay*, although it has no header and may not be immediately obvious. Decay is a measure of network activity and the amount of time passed, and is controlled by the decay variable in the *kismet_ui.conf* file. The default setting is three seconds:

- **Active**  If the network is active within the decay time, an exclamation point “!” is displayed prior to the network name.
- **Recent**  If the network was active within two periods of the decay time (i.e., six seconds), a period “.” is displayed prior to the network name. See the “WOPR” network in Figure 4.4 for an example.
- **Inactive** In all other cases (i.e., the network has not been active within six seconds), nothing is displayed.

Name

The network name is the most prominent column in the network list display. Typically, this lists the SSID, although you can change the name of any particular network with the “n” pop-up window. If a network is not broadcasting the SSID, Kismet can still infer its presence and will publish the network as `<no ssid>` until it can determine the name.

Type

The T column specifies the type of network:

- **A (Access Point)**  A wireless access point (AP) or wireless router; by far the most common network type
- **D (Data Network)**  Data packets have been seen, but Kismet has not captured any beacons or management frames and thus cannot yet tell what kind of network it is
Networks that have been manually grouped together by the user (t to tag networks, g to group tagged networks together)

Typically a wireless network set up between multiple laptops or clients without using an AP

A client probing for an AP that has not yet associated

Turbocell/Karlnet/Lucent router (uncommon)

The W column denotes whether or not encryption is being used on the network. However, it is more relevant to ask the question, “is WEP being used, or something else?”

e to tag networks, g to group tagged networks together

Wireless Encryption Protocol (WEP) is in use

The network is not encrypted

The network is encrypted with something other than WEP (for example, WPA)

The channel of the network is displayed in the C column:

For the more common 802.11b/g networks, the associated channels are 1–11 in the United States and 1–14 outside the United States.

For 802.11a, the following are allowable channels with the United States: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, and 165. Outside of the United States, particularly in Europe and Japan, more channels are available.

“Packts” is simply a cumulative total of packets captured for that particular network.

The bells should be going off in your head; this user has not changed anything from the original factory configuration
**W (WEP Decrypted)** This is a WEP-encrypted network that has been decrypted with a user-supplied key.

If Kismet can determine the address range and Internet Protocol (IP), it will display in the Flags column the method by which it obtained this information:

- **T (TCP)** The address range was determined via Transmission Control Protocol (TCP) traffic
- **U (UDP)** The address range was determined via User Datagram Protocol (UDP) traffic
- **A (ARP)** The address range was determined via Address Resolution Protocol (ARP) traffic
- **D (DHCP)** The address range was determined via Dynamic Host Configuration Protocol (DHCP) traffic

In addition, the T, U, and A flags may display a number (1–4), which indicates the number of octets discovered. For example, referring again to Figure 4.4, the **linksys** network displays the A4 flags, indicating that the address was discovered using ARP traffic, and all four octets have been discovered.

**IP**

By monitoring traffic, Kismet attempts to determine the IP address of the network, and this is displayed in the “IP Range” column. Kismet will display 0.0.0.0 until it finds some useful data via one of the methods described in the Flags section above. As you might suspect, more traffic collected from a particular network will provide a greater likelihood of finding the IP range, and more particularly, the exact IP address.

**Size**

The size column displays the total size of all the packets collected for that particular network.

**Colors**

While it is not accurately reproduced in a grayscale screenshot, the Kismet interface also displays to the shrewd observer, some valuable information by color-coding the networks:
Networks in yellow are not encrypted, meaning they are not using WEP or WPA. While these networks are coded as unencrypted, they still may be using a Virtual Private Network (VPN) or some other form of authentication after associating with the network. Yellow networks also indicate that at least some settings have been changed from their factory defaults.

The red color code is the signature of a network that is using the factory defaults. You may also see the F flag with this network. If the user hasn’t changed the factory configuration, you just might find that they haven’t changed the default password either!

Networks in green are using some form of encryption, usually either WEP or WPA. If Kismet cannot determine between the two, the Kismet .dump file can be imported into Wireshark, and the exact form of encryption determined there.

Blue networks are using SSID cloaking or are not broadcasting the SSID. An active scanner such as Network Stumbler (for Windows), which relies on the broadcast frame to determine the SSID, would not be able to locate this network.

GPS

When a supported Global Positioning System (GPS) is used together with Kismet, the applicable GPS data will be displayed along the bottom edge of the network list panel (see Figure 4.7).

Figure 4.7 GPS Status Information

As is typical of coordinates without north/south/east/west labels, positive latitudes indicate north, while negative latitudes indicate south. Likewise, positive longitudes indicate the eastern hemisphere, while negative longitudes indicate the western. In Figure 4.7, our coordinates are north of the equator, and in the western hemisphere (central Maryland to be more precise). Also included is a measure of altitude, speed, heading, and quality of fix.
Information Panel

The information panel labeled as “Info” is a small vertical panel to the right of the network list panel (see Figure 4.8).

- **Ntwrk** Total number of collected networks
- **Packets** Total number of collected packets
- **Cryptd** Total number of collected packets that were encrypted
- **Weak** Total number of weak packets collected
- **Noise** Worthless garbage packets
- **Discrd** Total number of discarded packets; includes noise and packets discarded from the use of filters
- **Pkts/s** Rate of packet collection (per second)
- **Elapsd** Total time (HH:MM:SS) since the Kismet was started

![Figure 4.8 Info Panel](image)

Status Panel

The status panel occupies the bottom section of the Kismet interface (see Figure 4.9). The status panel provides scrolling messages to the user:
Updates  Kismet will post a message to the status panel when it finds a new network, and provide additional information about networks when it becomes available.

Problems  Kismet will alert you to information regarding potential problems with Kismet’s connection to other services; for example, if Kismet cannot connect to gpds.

Alerts  These are primarily useful when using Kismet as an intrusion detection system (IDS); provides integration with third-party systems (i.e., Snort).

Battery Meter  Kismet will indicate if you are plugged into external power (AC), and display the percentage of battery life remaining; when using the battery Kismet will display an estimate of how much life is left. Keep in mind that you’ll need an APM-enabled kernel for battery life to report correct estimates.

Note

Even though Kismet places your wireless adapter in rfmon mode (meaning it does not transmit), simply having your wireless adapter radio on consumes more power from your battery. It is estimated that your battery life will be somewhere between 2–7 percent shorter. While this is not necessarily a hugely significant amount, it makes the battery meter all the more useful.

Figure 4.9 Status Panel

Pop-up Windows

All of Kismet’s windows beyond the main display are secondary displays or pop-up windows. These exist primarily as a means of displaying further information on a particular network, group, or client; providing statistics and useful information regarding packet rates and types; and other interesting data.
Network Details

The network details window displays the most comprehensive and detailed information collected about a particular network. When sorting by any mode other than autofit, simply scroll to the network of your choice and press enter or i (see Figure 4.10).

The network details window is useful if you need more information than is already provided in the network list. For example, the network list may show a particular network with the WEP flag “O,” which signifies the network is encrypted, but with something other than WEP. Under some circumstances, Kismet’s network details may be able to tell you specifically what type of encryption is being used. Be sure to scroll down as there is likely to be more than one screen of information.

Figure 4.10 Network Details Window

From the network details window, n will move you to the next network or group, while p will return you to the previous network or group. Alternatively, you can close the pop-up (q) and scroll to a different network. The network details window is one means of getting to the client list (c); you can also type (c) directly from the network list.
Client List

The client list window is very similar in both display and functionality to the network list panel. The default sort mode is also autofit, and the client list can be sorted in a similar manner.

The **n** and **p** keys display the client list of the next and previous network or group, respectively. Once a particular client is highlighted, the **i** key (or pressing **enter** ) changes to the client details display.

Columns

The following columns are displayed by default (again, as with the network list panel, see “Customizing the Panels Interface” later on in this chapter for changing the defaults):

**Decay**

The decay variable for a client is the same as it is for a network. As with the network list panel, the column is unlabeled and unseen unless a client is active or recent.
**Type**

The T column denotes the type of client. The client types are as follows:

- **F (From DS)** From a wireless distribution system (WDS) or AP to a wireless client; normally this means the client is wired
- **T (To DS)** To a WDS/AP from a wireless client; normally this means the client is wireless
- **I (Intra DS)** A node of the WDS/AP communicating to another node within the system
- **E (Established)** Most often a wireless client entering and leaving the WDS/AP
- **S (Sent To)** A client that has received data but not yet responded
- **(Unknown)** Self-explanatory

**Manufacturer**

The “Manuf” displays the manufacturer of the client based on the first three octets of the Media Access Control (MAC) address, which is known as the Organizationally Unique Identifier (OUI). As the name suggests, each manufacturer is assigned a specific block of octets that designate their equipment. Kismet attempts to match the client MAC with a list of OUIs in the `client_manuf` file. If a match is made, the manufacturer will be shown; otherwise *unknown* will be displayed.

---

**Note**

In some cases, Kismet may also be able to fingerprint the fourth octet of the MAC address, which is the first octet of the Network Interface Control (NIC)-specific portion of the MAC address. In this case, potentially more detailed information about a specific wireless adapter may be learned, such as the exact model of the particular device. In other cases, especially newer or rare equipment, Kismet may return *unknown* because it simply doesn’t know the MAC address. Likewise, a spoofed MAC address will fool Kismet as to the original manufacturer.
Tip
Kismet’s `ap_manuf` and `client_manuf` files are intentionally small to reduce memory use and Central Processing Unit (CPU) consumption. For those users that desire to use the full Institute of Electrical & Electronics Engineers, Inc. (IEEE) OUI list, Kismet provides a script (in the extras directory) called `ieee-manuf-tr.sh`, which will convert the OUI text file into a Kismet readable format. Of course, this will result in increased memory and CPU usage.

Data
This column displays the total number of data packets transferred by the client.

Crypt
The “Crypt” column displays the total number of encrypted packets transferred by the client.

Size
Size displays the total amount of data transferred by the client.

IP Range
“IP Range” displays the last known IP address of the client.

Sgn
The “Sgn” column displays the most recent signal strength of the client. As with all other issues related to signal strength, the accuracy of this data is entirely dependent upon the proper reporting of the data by the driver and/or firmware of the wireless adapter you’re using. To reiterate: if your card and/or driver does not support proper signal reporting, this value is useless.

Client Details
In the same way that the network details window shows the comprehensive collection of details about a particular network, the client details provides the same level of data for a particular client. Figure 4.12 provides an example of the level of client detail. Notice the client type is now a little clearer. This particular client is “From DS” or from the AP to a wireless client. As we know, these clients are typically wired. In fact, in this particular case, this client is the AP itself.
The `n` and `p` keys display the details of the next and previous client, respectively. Similarly to the network details display, scrolling down will provide you with more information.

### Packet rate

Kismet’s packet rate window will display a 5-minute history of the packet rate per second (see Figure 4.13).
Packet Types

Kismet will also dump the packet type information to the screen (see Figure 4.14).

Figure 4.14 Packet Type Display
The packet types panel is divided into two sections: the top displays a history of packet types by abbreviation (see the list below), while the bottom displays a scrolling list of the most recent packets with more detailed information. By default, Kismet will display packet types from all networks. However if you have tagged individual networks you can toggle between "all" and "tagged" with the a key. The following is a list of the applicable packet types:

‘N’ - Noise
‘U’ - Unknown
‘Mx’ - Management frame
  ‘Ma’ - Association request
  ‘MA’ - Association response
  ‘Mr’ - Reassociation request
  ‘MR’ - Reassociation response
  ‘Mp’ - Probe request
  ‘MF’ - Probe response
  ‘MB’ - Beacon
  ‘MM’ - ATIM
  ‘MD’ - Disassociation
  ‘Mt’ - Authentication
  ‘MT’ - Deauthentication
  ‘M?’ - Unknown management frame
‘Px’ - Physical frame
  ‘Pt’ - Request to send
  ‘PT’ - Clear to send
  ‘PA’ - Data Ack
  ‘Pc’ - CF End
  ‘PC’ - CF End+Ack
  ‘P?’ - Unknown phy frame
  ‘Dx’ - Data frame
  ‘DD’ - Data frame
  ‘Dc’ - Data+CF+Ack
  ‘Dp’ - Data+CF+Poll
  ‘DP’ - Data+CF+Ack+Poll
  ‘DN’ - Data Null
  ‘Da’ - CF Ack
  ‘DA’ - CF Ack+Poll
  ‘D?’ - Unknown data frame
Statistics

Kismet will display overall statistics that include the time you started the program, how many servers are currently running, the number of networks (broken down into encrypted and default), total number of packets seen, and maximum packet rate. In addition, Kismet provides both a graph and chart, which display channel usage information. See Figure 4.15 for the statistics window.

**Figure 4.15 Statistics Display**

Wireless Card Power

The 1 key will display signal power as well as report noise (see Figure 4.16). The name of this display is a bit of a misnomer, because it is not reporting the power of your wireless card; rather it is reporting the signal strength of the particular network or client. Remember that Kismet places your wireless card in rFmon mode, therefore your card is precluded from transmitting while Kismet is running.
Kismet has a nice (and not very well known) feature that will attempt to geo-locate a network. The accuracy of this information is wholly dependent upon GPS location data. Since estimating range based upon non-existent signal and noise standards is virtually impossible, this data is (unfortunately) not very useful in geo-location. Rather Kismet will guess location based upon a sample of GPS-logged locations.

Figure 4.16 Wireless Card Power Display

Network Location

Kismet has a nice (and not very well known) feature that will attempt to geo-locate a network. The accuracy of this information is wholly dependent upon GPS location data. Since estimating range based upon non-existent signal and noise standards is virtually impossible, this data is (unfortunately) not very useful in geo-location. Rather Kismet will guess location based upon a sample of GPS-logged locations.
Furthermore, Kismet does this on the fly; therefore it is advantageous to get sample data from a variety of locations to get a better guess. See Figure 4.17 for an example of the network location feature.

**Figure 4.17 Network Location Display**

Essentially, network location compares the location of where you were versus where you are now. This also assumes that your laptop is facing the direction of travel.

**Customizing the Panels Interface**

As has already been noted, Kismet can display a wealth of information about a network or client on the network and client lists (respectively), the only limitation being size. Should you find your work requires additional information to be available to you from one of these two displays, you can easily modify Kismet’s user interface configuration file to add or remove columns. Also, Kismet provides the ability to change colors to suit your needs.
Customizing the Network List Window

As we have seen, Kismet's main display contains a significant amount of useful information in the network list section. All of the information for a particular network is available in the network details window. Any or all of this information can be displayed in the main window by modifying the `kismet_ui.conf` file. The recognized columns, and their appropriate descriptions, are as follows (default columns are bold):

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bssid</td>
<td>BSSID (MAC address) of the network</td>
</tr>
<tr>
<td>channel</td>
<td>Last-advertised channel for network</td>
</tr>
<tr>
<td>clients</td>
<td>Number of clients (unique MACs) seen on network</td>
</tr>
<tr>
<td>crypt</td>
<td>Number of encrypted packets</td>
</tr>
<tr>
<td>data</td>
<td>Number of data packets</td>
</tr>
<tr>
<td>decay</td>
<td>Displays ‘!’ or ‘.’ or blank, based on network activity in the last ‘decay’ seconds (controlled by the ‘decay’ variable in the config file)</td>
</tr>
<tr>
<td>dupeiv</td>
<td>Number of packets with duplicate IVs seen</td>
</tr>
<tr>
<td>flags</td>
<td>Network status flags (Address size, decrypted, etc)</td>
</tr>
<tr>
<td>info</td>
<td>Extra AP info included by some manufacturers</td>
</tr>
<tr>
<td>ip</td>
<td>Detected/guessed IP of the network</td>
</tr>
<tr>
<td>llc</td>
<td>Number of LLC packets</td>
</tr>
<tr>
<td>manuf</td>
<td>Manufacturer, if matched</td>
</tr>
<tr>
<td>maxrate</td>
<td>Maximum supported rate as advertised by AP</td>
</tr>
<tr>
<td>name</td>
<td>Name of the network or group</td>
</tr>
<tr>
<td>noise</td>
<td>Last seen noise level</td>
</tr>
<tr>
<td>packets</td>
<td>Total number of packets</td>
</tr>
<tr>
<td>shortname</td>
<td>Shortened name of the network or group for small displays</td>
</tr>
<tr>
<td>shortssid</td>
<td>Shortened SSID for small displays</td>
</tr>
<tr>
<td>signal</td>
<td>Last seen signal level</td>
</tr>
<tr>
<td>signalbar</td>
<td>Graphical representation of signal strength</td>
</tr>
<tr>
<td>snrbar</td>
<td>Graphical representation of signal-to-noise ratio</td>
</tr>
<tr>
<td>size</td>
<td>Amount of data transferred on network</td>
</tr>
<tr>
<td>ssid</td>
<td>SSID/ESSID of the network or group</td>
</tr>
<tr>
<td>type</td>
<td>Network type (Probe, Adhoc, Infra, etc)</td>
</tr>
<tr>
<td>weak</td>
<td>Number of packets which appear to have weak IVs</td>
</tr>
<tr>
<td>wep</td>
<td>WEP status (does network indicate it uses WEP)</td>
</tr>
</tbody>
</table>

To modify the default columns in the main window, edit the `kismet_ui.conf` file at the following location:

```
# What columns do we display? Comma seperated. Read the documentation for what # columns are valid.
columns=decay,name,type,wep,channel,packets,flags,ip,size
```
Figure 4.18 shows a modified network list panel showing network name, manufacturer, total number of data packets by network, signal and noise information, and amount of data transferred per network.

**Figure 4.18 Modified Network List Window**

![Modified Network List Window]

**Customizing the Client List Window**

Similarly, the columns in the client window can be modified (all are on by default except “maxrate”):

- **crypt**: Number of encrypted data packets transferred by client
- **data**: Number of data packets transferred by client
- **decay**: Displays ‘!’, ‘.’, or ‘ ‘ based on network activity
- **ip**: Last seen IP used by client
- **mac**: MAC address of client
- **manuf**: Manufacturer of client (if known)
- **maxrate**: Maximum rate client seen transferring
noise        Last seen noise level of client
signal       Last seen signal level of client
size         Amount of data transferred by client
type         Type of client (Established, To-DS, From-DS, etc)
weak         Number of packets which appear to have weak IVs

To modify the default columns in the client window, edit the *kismet_ui.conf* file at
the following location:

```plaintext
# What columns do we display for clients? Comma seperated.
clientcolumns=decay,type,mac,manuf,data,crypt,size,ip,signal,quality,noise
```

## Customizing Colors

Kismet’s colors can be turned on or off, the background and border colors can be changed, and the default colors listed above can be changed by modifying the applicable portion of *kismet_ui.conf*:

```plaintext
# Colors (front, back) of text in the panel front. Valid colors are:
# black, red, yellow, green, blue, magenta, cyan, white
# optionally prefixed with “hi-” for bold/bright colors, ie
# hi-red, hi-yellow, hi-green, etc.
# Enable colors?
color=true
# Background
backgroundcolor=black
# Default text
textcolor=white
# Window borders
bordercolor=green
# Titles
titlecolor=hi-white
# GPS and APM info
monitorcolor=hi-white
# WEP network color
wepcolor=hi-green
# Factory network color
factorycolor=hi-red
# Open color
opencolor=hi-yellow
# Decloaked network color
cloakcolor=hi-blue
```
Third Party Front-ends

While the large majority of this chapter has focused on Kismet’s native panels interface, there are a number of third-party interfaces that have been developed over the years. These third-party front-ends are designed primarily as a way of enhancing the look or changing the interface from an ncurses/panel one to a truly graphical one. This section is not meant to be an exhaustive review of such graphical user interfaces (GUIs), but rather a brief survey of some of the options that are available.

**Note**

It is important to note that these third-party front-ends are simply replacements for the Kismet client (interface), and don’t actually do anything by themselves. They still require you to run Kismet in server mode and connect to it with the particular interface of your choice.

**gkismet**

One example of a popular Linux-based Kismet front end is *gkismet* (see Figure 4.19). The gkismet interface is designed to supplement or replace the native Kismet panels interface for those that prefer something more GUI-based. Many of the same features are available, and development is ongoing to remain compatible with the latest version of Kismet. For more information about gkismet, see http://gkismet.sourceforge.net/.
KisWin

*KisWin* (not to be confused with RenderMan’s Kismet for Windows package also known as KisWin, and located at http://www.renderlab.net/projects/wrt54g/) is a Windows-based GUI front-end for Kismet (see Figure 4.20). Whether you are running Kismet on Windows/Cygwin using a remote drone (such as a modified Linksys WRT54G), using CACE Technologies’ AirPcap adapter, or simply running Kismet
over a network to a Windows PC, *KisWin* provides you with a GUI interface. For more information about *KisWin*, see http://kiswin.taz00.com/

**Figure 4.20** *KisWin*

![Figure 4.20 KisWin](image)

**dumb kismet client**

The last interface we’ll mention is *dumb kismet client* for Win32. This particular client is lightweight, and should be able to run in front of any of the same Windows/Cygwin configurations as KisWin. While *dkc* is designed for Windows, it also worked fine under Linux using *wine*. For information about *dumb kismet client*, see http://www.d3tr.de/dkc/.
Further information

Once again, this section is not designed to be the end-all solution for third-party front-ends for Kismet, rather a sampling of some of the solutions that are available to users. See http://www.kismetwireless.net/links.shtml for more information on third-party tools for Kismet.
Summary

The Kismet client is the primary interface between the Kismet server and the user. The default display is the panels interface, which is a lightweight, interactive GUI display. The primary display provides the user with a general overview of Kismet’s collected data, and can be manipulated and modified to the user’s content. The remainder of the windows are secondary displays or pop-up windows that provide additional and amplifying information about selected networks, groups, or clients, as well as statistics and additional interesting information. Some of these displays can also be modified to the user’s liking. Lastly, there are a number of third-party front-ends to supplement or replace the default Kismet client.

What happens when you have a question? Your first source of information should be Kismet itself. Most if not all of the displays have integrated help screens (always the h key). Your second source should be the online documentation, found at www.kismetwireless.net/documentation.shtml. Of particular interest to this chapter are sections 10 (Ncurses/panel interface), 17 (Troubleshooting, and 18 (Frequently Asked Questions). You would benefit greatly from reading the documentation in its entirety (all the way to the end!). Once you exhaust those sources, move on to the Kismet forums (http://www.kismetwireless.net/forum.php), being sure to search before you post. Finally, consider using your best friend Google who, more often than not, can find something that will guide you in the right direction.

Solutions Fast Track

Main Display

- The Kismet panels display is the primary interface between the Kismet client and server and the user.
- The main display is divided into the network list panel, status panel, and information panel; and is designed to provide the user with an overview of Kismet’s collected information.
- Kismet’s integrated help feature is the gateway to more detailed information about a particular network.
Popup Windows

☑ All windows beyond the main display are secondary or pop-up windows, and provide additional and amplifying information about selected networks, groups, or clients, as well as statistics and additional interesting information.

☑ The information provided on the wireless card power and network location pop-up windows is wholly dependent upon the wireless card drivers and/or firmware. Kismet does not calculate signal or noise information, rather it simply reports it.

Customizing the Panels Interface

☑ Both the network list and client list can be modified to the user’s specifications by editing the *kismet_ui.conf* file.

☑ Kismet’s color scheme, including the background, borders, and default color-coding of networks, can be modified as well.

Third-Party Front-ends

☑ Third-party front-ends are GUIs designed to supplement or replace the Kismet client panels interface.

☑ Third-party clients are available to run on both Linux and Windows.
This page intentionally left blank