

Equipment used in this Tutorial

Nokia N810



Bekin F5D7050 - Wireless G USB Network Adapter
Version 3 FCC ID: K7SF5D7050B



Realtek RTL8187L 1500mW Wireless Adapter Card Antenna



Micro USB Host Cable for Nokia N810 OTG



Lenmar PowerPort Mini Charger & Battery



Cable Style Dual-Power 1000mA USB 2.0 4-Port Hub



USB 2.0 Female to Dual USB A Male Power Y Cable



Tomtom MKII Bluetooth GPS receiver



Getting Started

First thing you should do is visit the Nokia Support website (<http://www.nokia.com/us-en/support/user-guide>) to learn all about your device (i.e. buttons, specifications, how-tos, guides, etc). You will have to search for the N810 in the archive section.

Direct Link to the User Guide http://nds1.nokia.com/files/support/nam/phones/guides/N810_US_en.PDF

User Guide Mirror http://www.jedge.com/n810/N810_US_en.pdf

After you get to know the device you will want to upgrade it to the latest version. The easiest way is with the Windows Nokia Internet Tablet Update Wizard (http://nds1.nokia.com/files/support/global/phones/software/Nokia_Internet_Tablet_Software_Update_Wizard.exe). Just follow the instructions to have the latest version of OS2008.

Update Wizard Mirror http://www.jedge.com/n810/Nokia_Internet_Tablet_Software_Update_Wizard.exe

Beware that flashing a new image on your tablet will reset the device back to factory defaults and remove all data not on the memory cards—preferences, bookmarks, installed applications, with a single exception that any previously-set lock code will be kept and not reset to the factory-default of "12345".
(Updating the firmware, 2009)

Once you boot your device for the first time there will be a couple wizards having you establish the device language and time. You can go ahead and cancel the wizards asking you to setup a connection to a mobile device. The following instructions below will go into quick and direct detail on how to configure the Nokia N810 as a wireless auditing device.

For Advanced Users: Flashing your Nokia N810 with Linux

The command line flasher tool can be downloaded from Nokia's developer site (<http://tablets-dev.nokia.com/maemo-dev-env-downloads.php>). The current version is 3.5. See the wiki for Flasher to understand all the options that exist for the tool (<http://wiki.maemo.org/Flasher>).

You can get the latest N810 image from http://tablets-dev.nokia.com/nokia_N810.php. You will need the device ID (MAC address) of your Nokia device. The information is located behind the battery.

My OS for testing the tool is Ubuntu 10.4 LTS so I downloaded the Debian (deb) package and installed it via the command line.

```
#dpkg -i maemo_flasher-2.5_2.5.2.2_i386.deb
```

Select Ok for the pop-up prompts and Yes to accept the license. Once flasher is installed you can run the following command to flash your device.

```
#flasher-3.5 -F RX-44_DIABLO_5.2008.43-7_PR_COMBINED_MR0_ARM.bin -f -R
```

Run this command and then plug in your N810 via the USB cable. Power on the device while holding the Swap (looks like two overlapping boxes on left side) button. Once the device starts flashing you can release both buttons. When flashing is complete you can cycle the device's power.

For Advanced Users: Flashing your Nokia N810 with Windows Command Line

These instructions exist because some day Nokia will stop providing the update wizard.

Download and install maemo_flasher-3.5_2.5.2.2.exe from the Nokia Maemo Development site (<http://tablets-dev.nokia.com/maemo-dev-env-downloads.php>). Download the latest N810 image from http://tablets-dev.nokia.com/nokia_N810.php. You will need the device ID (MAC address) of your Nokia device. The information is located behind the battery.

Flasher Mirror Link http://www.jedge.com/n810/flasher/maemo_flasher-3.5_2.5.2.2.exe

My OS for testing this tool was Windows 7 64-bit so I encounter, and solve, all the issues there is running this tool on this version of Windows. You will need to see this post <http://talk.maemo.org/showpost.php?p=849980&postcount=20> in order to get it to work properly. See [Appendix D](#) for the same post but modified for the N810 with mirrored links.

Once flasher is installed search for “flasher” in the Windows 7 search box. Click “Maemo Flasher 3.5”. You can run the following command to flash your device. This assumes that the image file is in your default Windows Downloads folder.

```
C:\Program Files (x86)\maemo\flasher-3.5>flasher-3.5.exe -F c:\Users\jedge\Downloads\RX-44_DIABLO_5.2008.43-7_PR_COMBINED_MR0_ARM.bin -f -R
```

Connect to an Access Point

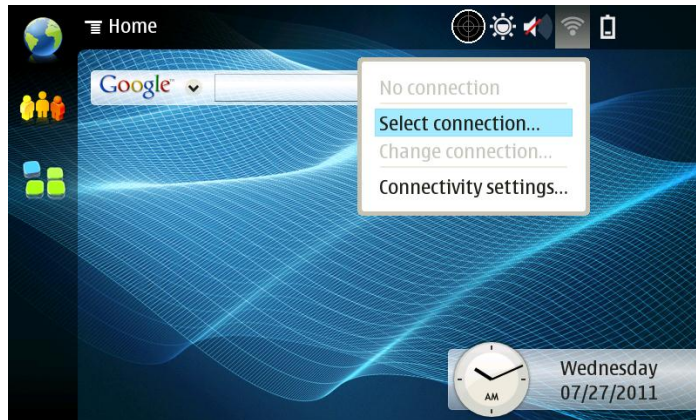


Figure 1: Select the Wireless Icon and choose Select Connection



Figure 2: Select your Access Point from the pop-up

Go to Application Manager

Enable Red Pill mode (this is so you can install software that needs access to the device libraries). See [Appendix B](#).

While in Application Manager (after following the Red Pill tutorial) enable the Maemo extras repository. Select maemo Extras, click Edit, uncheck the Disabled box, and click OK.

Using the Application Manager install the following software: rootsh, minigps, a-gps, telnet, vim, and dropbear (client and server).

Add Additional Application Repositories

Open your browser and go to the site <http://www.gronmayer.com/it/index.php>. This page cataloges all of the repositories that exist for the Nokie tablets. Scroll down the site and select the following repositories:



Figure 3: <http://www.gronmayer.com/it/>

Select

- maemo Extras
- Nokia certified
- Nokia non-certified
- Nokia System-update
- Maemo Chinook
- MULLINER.ORG Maemo Software
- tuomas.kulve.fi
- Mapper
- Diablo maemo extras
- Maemo diablo/tools
- Ricky Brent's Maemo Packages
- mg.pov.it(Diablo)
- Maemo Extras-Devel
- Qole

You are going to want to open the file (pop box) in Application Manager. This will load the application manager. Be patient if it looks like isn't doing anything for the first few seconds. It will begin asking you if you want to install each repository one by one. Then it will go to check updates (just a graphical apt-get update after you update the sources.list file) which will take a couple minutes.

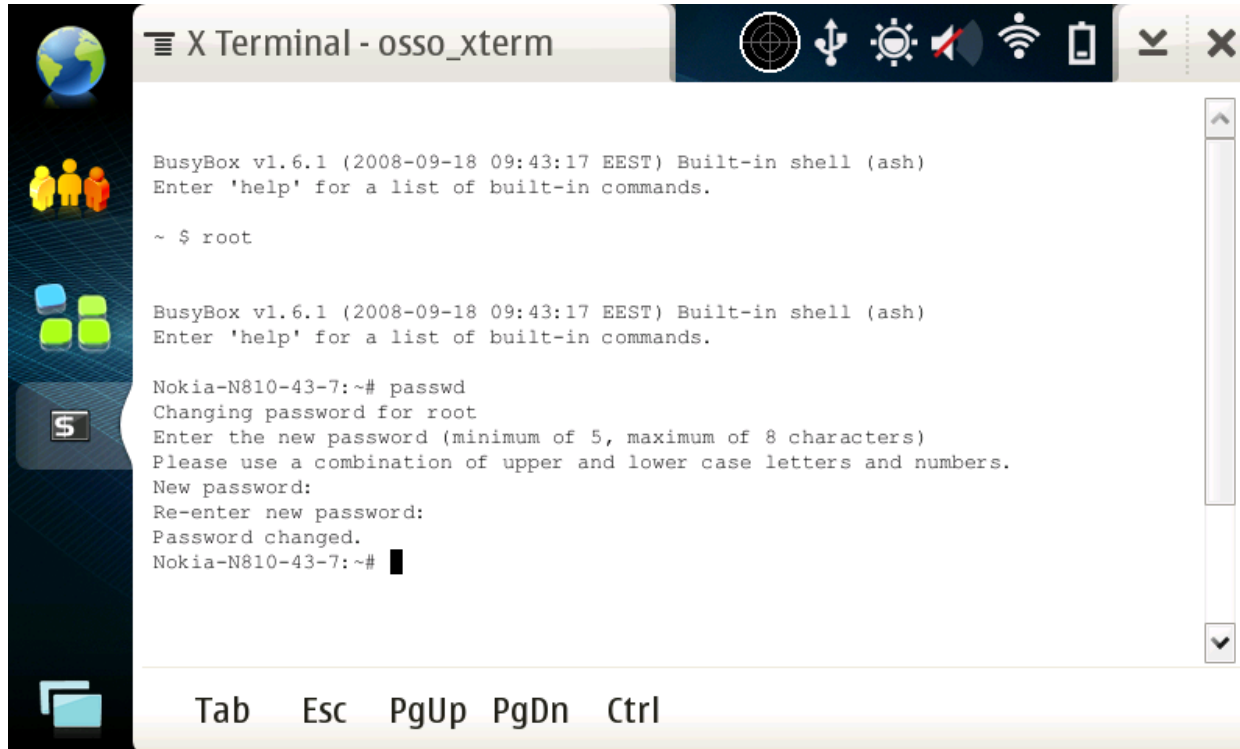
For Advanced Users: Adding Repositories

Modify the file `/etc/apt/sources.list.d/hildon-application-manager.list` and add the following repositories.

```
deb http://catalogue.tableteer.nokia.com/updates/diablo-2/ ./
deb http://repository.maemo.org/extras/ chinook free non-free
deb http://catalogue.tableteer.nokia.com/certified/ chinook user
deb http://catalogue.tableteer.nokia.com/non-certified/ chinook user
deb http://catalogue.tableteer.nokia.com/updates/chinook/ ./
deb http://repository.maemo.org/ chinook free non-free
deb http://www.mulliner.org/nokia770/repository/ chinook free
deb http://tuomas.kulve.fi/debian chinook maemo
deb http://download.talinux.tal.org/pub/maemo chinook free
deb http://repository.maemo.org/extras/ diablo free non-free
deb http://repository.maemo.org/ diablo/tools free
deb http://rickybrent.com/maemo/debs chinook free nonfree
deb http://mg.pov.lt/770 diablo user other
deb http://repository.maemo.org/extras-devel diablo free non-free
deb http://qole.org/repository maemo main
```


Set a Root Password

Open a terminal window on the device Utilities->X Terminal.



```
BusyBox v1.6.1 (2008-09-18 09:43:17 EEST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ root

BusyBox v1.6.1 (2008-09-18 09:43:17 EEST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

Nokia-N810-43-7:~# passwd
Changing password for root
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
Password changed.
Nokia-N810-43-7:~#
```

Figure 4: Setting Root Password

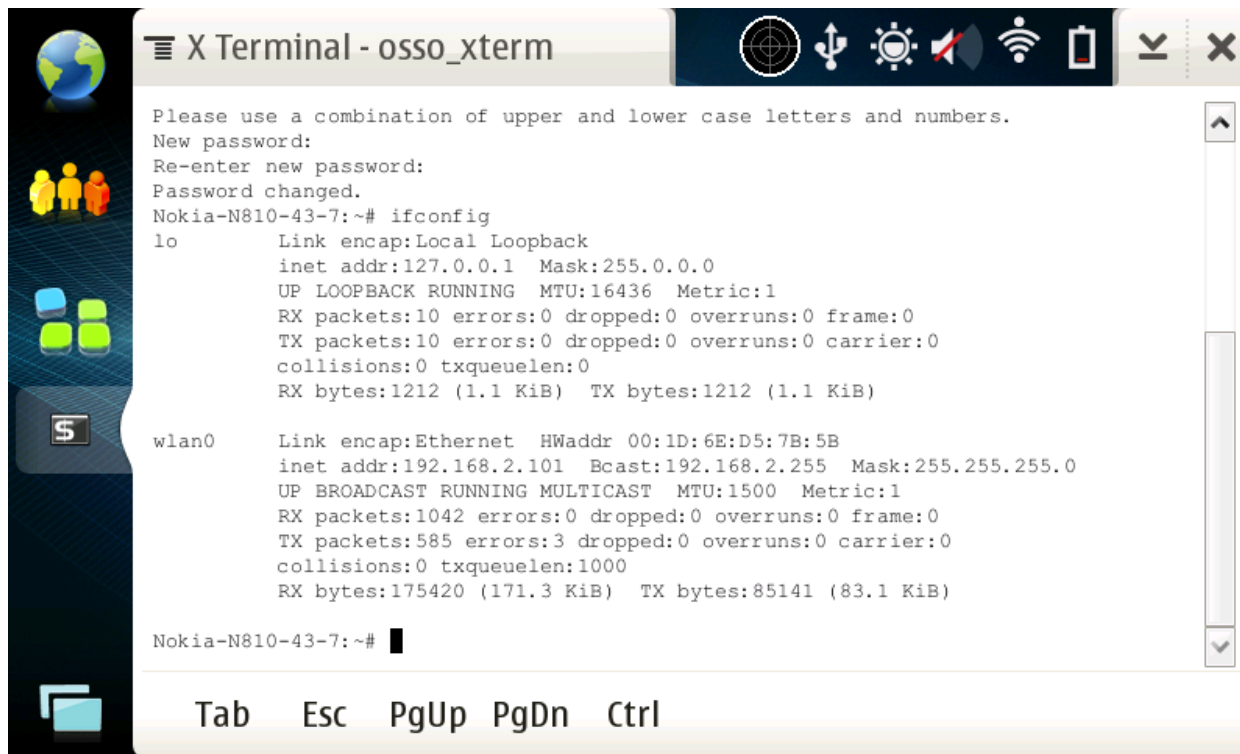
The screenshot above shows the commands entered to change the root password.

Become root	→	~ \$root
Run passwd	→	Nokia-N810-43-7:~#passwd

Nokia N810: Wireless Auditing Tool - Configuration Tutorial

Enter your password → New PASSWORD:
Re-enter your password → Re-enter new password:

Now you are able to access the device using the SSH (Secure Shell) protocol, the root account, and the new password you set. For Windows you can use the application Putty (www.chiark.greenend.org.uk/~sgtatham/putty/) to establish an SSH session with your device. You will need the IP address of your N810. From the terminal window run the command `ifconfig`.



```
X Terminal - osso_xterm

Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
Password changed.
Nokia-N810-43-7:~# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1212 (1.1 KiB)  TX bytes:1212 (1.1 KiB)

wlan0     Link encap:Ethernet  HWaddr 00:1D:6E:D5:7B:5B
          inet addr:192.168.2.101  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1042 errors:0 dropped:0 overruns:0 frame:0
          TX packets:585 errors:3 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:175420 (171.3 KiB)  TX bytes:85141 (83.1 KiB)

Nokia-N810-43-7:~#
```

Figure 5: Identify IP Address

You will see for device wlan0 the “inet addr” is 192.168.2.101. This IP address will be used to access the N810 using Putty. Once you have accessed the device

through Putty we will use the SSH connection to install and configure all wireless auditing tools.

Installing and Configuring Wireless Tools

Basic Tools

Useful tools and utilities that are important for all tutorials below.

```
Nokia-N810-43-7:~#apt-get install bash
```

```
Nokia-N810-43-7:~#bash-setup
```

```
Do you want to use bash as your default
login shell?
```

```
Enter Y to change shell to bash, or
Enter N to leave the current shell setting.
> y
```

```
B
```

```
It seems there is a leftover ~/.bashrc in your home
directory. It will override the prompt set by the
/etc/profile.d/prompt.sh script. Do you want to comment
out the line that sets the prompt in ~/.bashrc?
```

```
Enter Y to comment out the line, or
Enter N to leave ~/.bashrc intact.
> y
```

```
Nokia-N810-43-7:~#apt-get install wget unzip wireless-tools usbmode subversion
```

When installing usbmode this tool you will have to select an option on the N810 screen.

GPS Configuration

Start GPSD using MiniGPSD. Select the target icon at the top of the screen and choose Configure... In the options pane select Internal GPS Use n810 and click OK. Then click the target icon again and select Start GPSD.



Figure 6: Click Target Icon and Choose Configure



Figure 7: Check Box Use n810

The GPS chip in the N810 is the Texas Instruments GPS5300. This is a “low cost” chip made for mobile phones. It uses cellular communication to assist in obtaining your location. However, the N810 is not cellular!!!! Personally I feel this was a major design flaw and shows they were throwing in GPS as an afterthought. A-GPS to the rescue! This application pulls up a map of the world and allows you to point to where you are located to assist the GPS in obtaining a lock. Pull up the menu and go to Extras->A-GPS Beta. When the application opens just click on the area of the world that you are located.

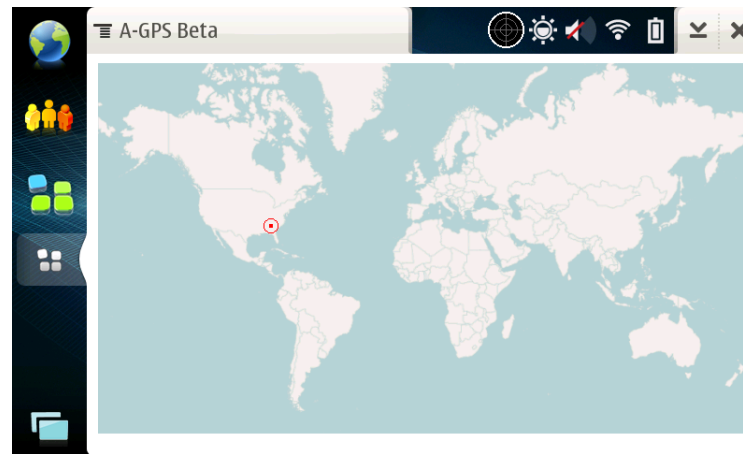


Figure 8: Click where you are in the World

Point the N810 toward the southern sky and allow a *few minutes* for it to obtain a lock. Once a lock is obtained the device is able to maintain it without

optimum visibility. A neat way to find which direction is south is to download a compass app onto your smartphone. Works like a charm. Or you can look around for any satellite dishes and point in the same direction.

When a lock is obtained the MiniGPS target icon will look like this.



Bluetooth GPS Receiver

The inexpensive Tomtom MkII Bluetooth GPS receiver can be obtained from Ebay or Amazon and works well with the Nokia N810. Following these steps will get the Bluetooth GPS working with MiniGPSd.

1. Pair the GPS device with the N810. Control Panel → Connectivity → Bluetooth
2. Turn Bluetooth on and click Devices to search for the TomTom MkII
3. Pair with the device with the code '0000'
4. Select the MiniGPSd icon and choose configure
5. Select External GPS, deselect Internal GPS, and select BT Scan
6. Bluetooth Scan and Set will scan/search for devices. When it is done you will be able to select the MKII
7. With the MkII selected you then select Set GPS, Set OBD, and Set V1 to assign the device MAC address for MiniGPSd
8. After clicking OK everything is all set. The Bluetooth icon will turn blue and MiniGPSd will start tracking satellites.

For screenshots to help with the steps above see [Appendix F](#).

Kismet Original (Oldcore)

```
Nokia-N810-43-7:~#apt-get install ncurses-base libpcrc3
Nokia-N810-43-7:~# wget http://www.jedge.com/n810/debs/kismet_2008-05-R1_armel.deb
Nokia-N810-43-7:~# dpkg -i kismet_2008-05-R1_armel.deb
```

Installing this package will “pause” in the Putty window. It is looking for you to select where you want the GUI icon for Kismet to be installed on the device. Go to the N810 and select where you want it installed.

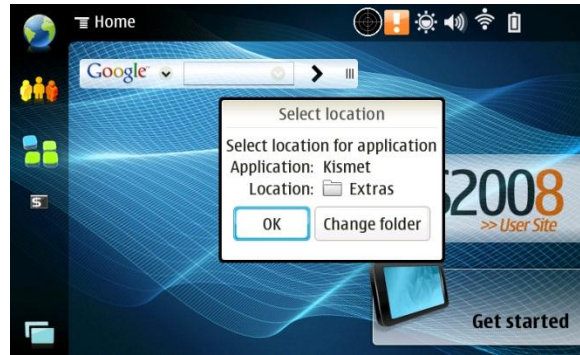


Figure 9: Finalizing Kismet Install

The Kismet configuration files are found in the `/etc/kismet` directory if you want to make modifications. However, the package you installed is already configured to work with the internal wireless interface of the N810. By default the log files are placed in folder that kismet is run from. You can modify `/etc/kismet/kismet.conf` to change the default or move to the folder where you want to files to be written to.

The default `kismet.conf` file does not come configured to utilize the N810 internal GPS. Line #119 of `kismet.conf` needs to be changed from `gps=false` to `gps=true`. This can be done from the Putty session and vim. An already modified `kismet.conf` file can be found at <http://www.jedge.com/n810/oldcore/kismet.conf>. While you are at it, download `kismet_ui.conf` file where I modified it to show the signal strength of the access points.

```
Nokia-N810-43-7:~#cd /etc/kismet
Nokia-N810-43-7:~#wget http://www.jedge.com/n810/oldcore/kismet.conf
Nokia-N810-43-7:~#wget http://www.jedge.com/n810/oldcore/kismet_ui.conf
Nokia-N810-43-7:~#mkdir /media/mmc1/kismet
```

If you want to utilize GPS with Kismet Oldcore you have to start the Kismet Server (`kismet_server`) and Kismet Client (`kismet_client`) in separate windows. There is a bug when you start Kismet from the menu item or from the command `kismet` when you have GPS enabled.

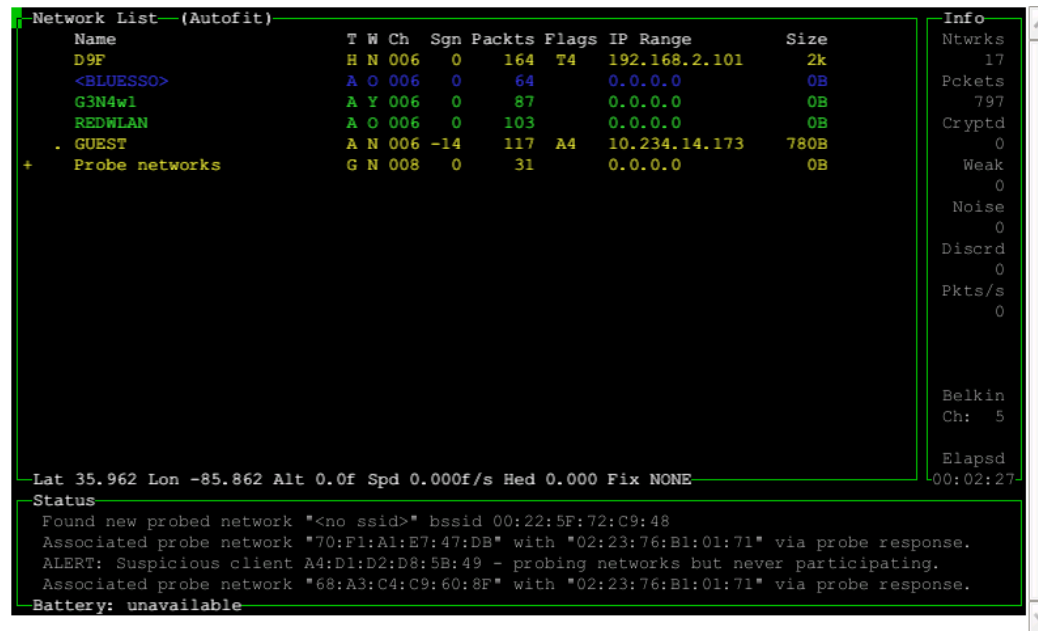
Open up the Terminal on the N810. Then select menu -> Windows -> New Window. You will now have two Terminal sessions. In the first window start `kismet_server` then start `kismet_client` in the second window.

```
BusyBox v1.6.1 (2008-09-18 09:43:17 EEST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ $ kismet_server
Will drop privs to user (29999) gid 29999
Waiting for Hildon gps to enable...
Hildon BT failed: GPS API should be called as "user" and not as root
No specific sources given to be enabled, all will be enabled.
Non-RFMon VAPs will be destroyed on multi-vap interfaces (ie, madwifi-ng)
Enabling channel hopping.
Enabling channel splitting.
NOTICE: Disabling channel hopping, no enabled sources are able to change channel.
Source 0 (Belkin): Enabling monitor mode for rt73 source interface wlan1 channel 6..
.
Source 0 (Belkin): Opening rt73 source interface wlan1...
Spawned channel control process 1586
Dropped privs to user (29999) gid 29999
Will attempt to put networkmanager to sleep...
Allowing clients to fetch WEP keys.
Logging networks to Kismet-Jul-28-2011-2.network
Logging networks in CSV format to Kismet-Jul-28-2011-2.csv
Logging networks in XML format to Kismet-Jul-28-2011-2.xml
Logging cryptographically weak packets to Kismet-Jul-28-2011-2.weak
Logging cisco product information to Kismet-Jul-28-2011-2.cisco
Logging gps coordinates to Kismet-Jul-28-2011-2.gps
Logging data to Kismet-Jul-28-2011-2.dump
Writing data files to disk every 300 seconds.
```

Figure 10: Starting Kismet Server





The screenshot displays the Kismet Client interface. It features a main window titled 'Network List (Autofit)' with a table of detected networks. To the right, there is an 'Info' panel showing various statistics. At the bottom, a 'Status' panel provides detailed information about the current network activity and battery status.

Name	T	W	Ch	Sgn	Pkts	Flags	IP Range	Size
D9F	H	N	006	0	164	T4	192.168.2.101	2k
<BLUESSO>	A	O	006	0	64		0.0.0.0	0B
G3N4w1	A	Y	006	0	87		0.0.0.0	0B
REDWLAN	A	O	006	0	103		0.0.0.0	0B
. GUEST	A	N	006	-14	117	A4	10.234.14.173	780B
+ Probe networks	G	N	008	0	31		0.0.0.0	0B

Info
Ntwrks 17
Pkts 797
Cryptd 0
Weak 0
Noise 0
Discrd 0
Pkts/s 0
Belkin Ch: 5
Elapsd 00:02:27

Lat 35.962 Lon -85.862 Alt 0.0f Spd 0.000f/s Hed 0.000 Fix NONE

Status

Found new probed network "<no ssid>" bssid 00:22:5F:72:C9:48
Associated probe network "70:F1:A1:E7:47:DB" with "02:23:76:B1:01:71" via probe response.
ALERT: Suspicious client A4:D1:D2:D8:5B:49 - probing networks but never participating.
Associated probe network "68:A3:C4:C9:60:8F" with "02:23:76:B1:01:71" via probe response.

Battery: unavailable

Figure 11: Kismet Client

Kismet Newcore

I've compiled the latest version of Kismet Newcore (7.28.2011 - Kismet-2011-03-R2) and packaged it. If you previously installed the Oldcore version of Kismet you need to remove it.

```
Nokia-N810-43-7:~#dpkg -r kismet
Nokia-N810-43-7:~# rm -rf /etc/kismet /usr/share/kismet
```

If you are starting the installation from scratch.

```
Nokia-N810-43-7:~#apt-get install ncurses-base libpcrc3 libcap1 libpcap1
```


Nokia N810: Wireless Auditing Tool - Configuration Tutorial

```
Nokia-N810-43-7:~# wget http://www.jedge.com/n810/debs/kismet-2011_03-R2-1_armel.deb
Nokia-N810-43-7:~#dpkg -i --force all kismet-2011_03-R2-1_armel.deb
Nokia-N810-43-7:~#mkdir ~/.kismet
Nokia-N810-43-7:~#cd ~/.kismet
Nokia-N810-43-7:~#wget http://www.jedge.com/n810/newcore/kismet_ui.conf
```

By default Kismet is configured to place all log files in /media/mmc1 and work with the internal wireless and gps. Client configuration is now done once kismet starts with the file found in /home/user/.kismet saving all options selected. For all new features with Kismet see <http://www.kismetwireless.net>. Moving around the application is best with the Tab key but it can also be done using the touchscreen. The N810 keyboard does not have the Tab key. Instead it is a button on the screen you have to tap or you have to click Ctrl-i which is on the same side of the keyboard and uncomfortable to reach. See the section of this document called Remapping Keys ([Appendix C](#)) to learn how to fix this as well as map other important keys.

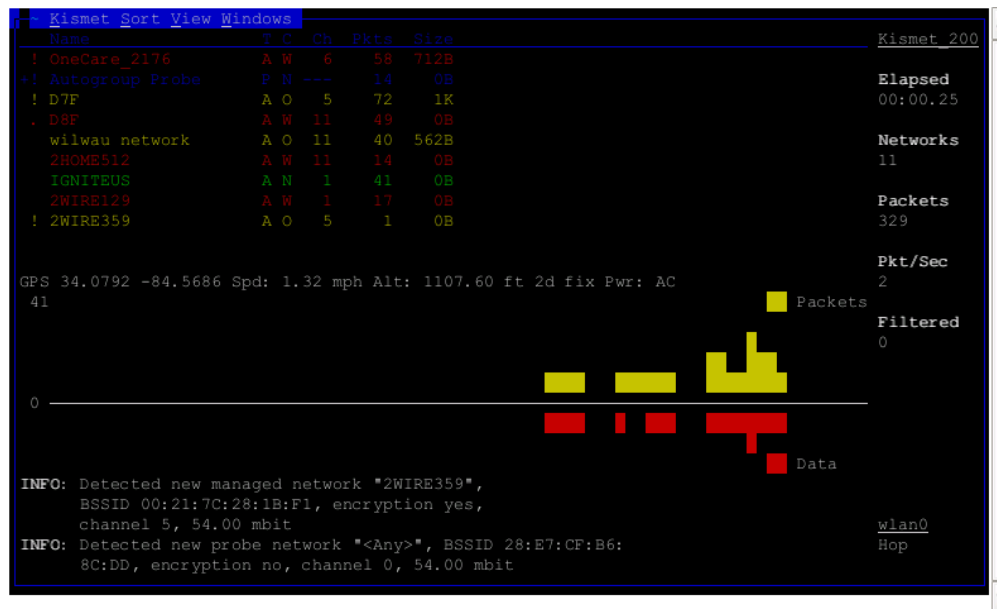


Figure 12: Kismet Newcore Client

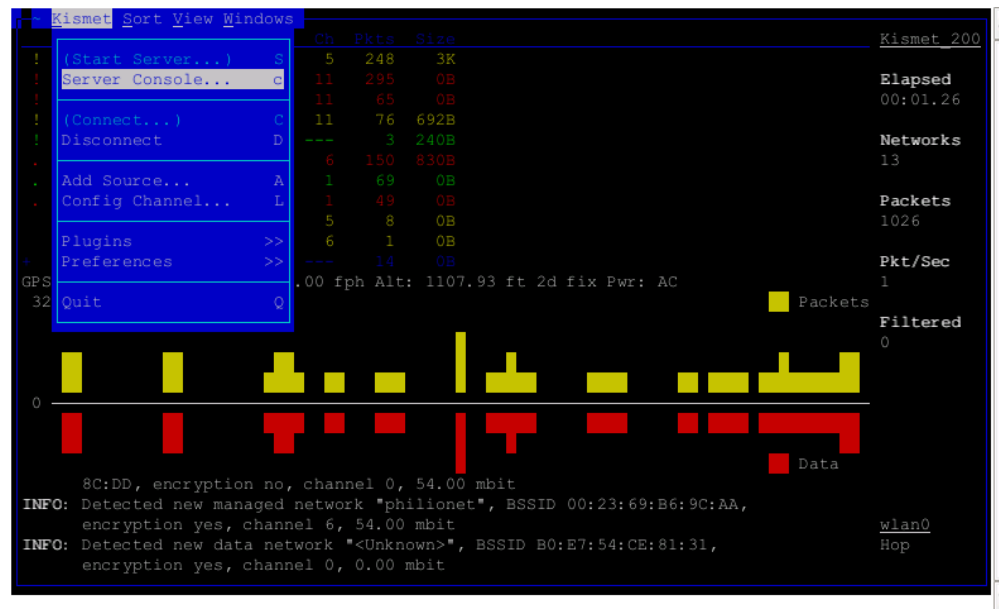


Figure 13: Kismet Client Menu

Configure USB Wireless Networking

These steps are going to detail how to install and configure USB Wireless Adapters from two different chipset manufactures.

Chipset: Ralink R73

Device: Belkin 802.11g 54Mbps USB wireless adapter v3 (FCC ID: K7SF5D7050B)

(http://en-us-support.belkin.com/app/answers/detail/a_id/297/~f5d7050-wireless-g-usb-network-adapter---drivers).

Chipset: Realtek RTL8187L

Devices: No-name 1500mW Wireless Adapter Card Antenna

Both of these devices can be found on Ebay or www.DealExtreme.com

Attach external adapter to N810 device

Three items are required to attach an external usb network adapter (Ethernet or 802.11) to the N810:

- OTG Micro USB Host Cable
- Dual-Power USB Hub **[OR]** USB Female to Dual USB A Male Power Y Cable
- 5V power source (the N810 offers minimal voltage when a device is attached. Only flash drives and keyboards will work without an external power source).

For testing purposes you can plug the other USB Male connector to a laptop or use a wall-wart USB power adapter to help power the USB 802.11 adapter. For my personal testing I plug the other usb connector right into the side of the laptop I used to create this tutorial. For use in the field I recommend a 5V rechargeable lithium battery from Lenmar (Google Search).



USB Hub: Front



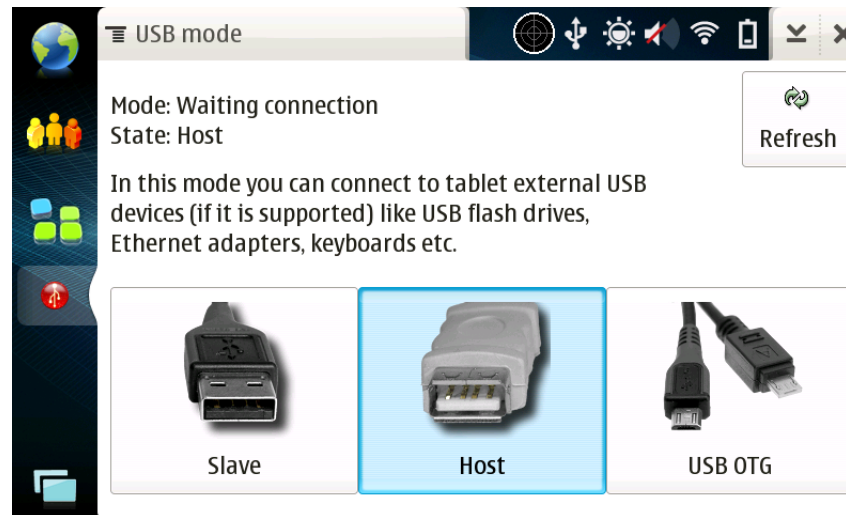
USB Hub: Rear



USB Y Cable: Rear

Enable USB Host Mode

Open the application Usbmode installed under the Settings menu and select Host for the mode we want enabled. This will allow us to connect the USB Wireless Adapter as well as USB Flash Drives.



Or from a Putty SSH session or an Xterm window as root:

```
Nokia-N810-43-7:~# echo host > /sys/devices/platform/musb_hdrc/mode
```

For the Y-cable (not the hub) you will also need to enter the command shown below. It tells the OS to ignore line power “issues” that are taken care of automatically by the circuit in the hub. It needs to be plugged into the device before running the command or it will error out.

```
Nokia-N810-43-7:~# echo -n 1 > /sys/bus/usb/devices/1-1/bConfigurationValue
```

Obtain and Install N810 drivers for RT73 and RT8187L

Download the following zip files, extract them, move the files to their proper location, and ensure they are loaded with the device starts:

```
Nokia-N810-43-7:~#wget http://www.jedge.com/n810/ rtl8187.zip
Nokia-N810-43-7:~#wget http://www.jedge.com/n810/rt73.zip
Nokia-N810-43-7:~#unzip rtl8187.zip
Nokia-N810-43-7:~#unzip rt73.zip
Nokia-N810-43-7:~#mv rt73.bin /usr/lib/hotplug/firmware/
Nokia-N810-43-7:~#mkdir /lib/modules
Nokia-N810-43-7:~#mv rt73.ko /lib/modules/
Nokia-N810-43-7:~#mv rtl8187/*.ko /lib/modules/
```

The script, netup, included in the zip file will load the drivers when you run it. It also has the commands detailed above for putting the usb port into host mode and allowing for a y-cable instead of the hub.

```
Nokia-N810-43-7:~#chmod 777 netup
Nokia-N810-43-7:~# ./netup
```

As a side note, the guy who created this awesome tutorial (<http://talk.maemo.org/showthread.php?t=30838>) called his script netup and I kept the name.

What I do when in the field is run netup, plug the device in, then run netup again if I'm using the Y-cable. Running netup, or more specifically echo command to the bConfigurationValue detailed previously will give the following error message.

```
netup: line 7: cannot create /sys/bus/usb/devices/1-1/bConfigurationValue: nonexistent directory
```

The directory isn't created until the usb is plugged into the N810. With the Y-cable, every time you unplug the usb device you need to run netup again (or just that one command on line 7 of the script). Note that the Y-cable is finicky so unplugging and plugging it back in works to get the n810 to recognize the wireless device.

When you plug in the USB Wireless Adapter error messages will pop up on the N810 screen. These can safely be ignored. Depending on which wireless adapter you are using you will see the following information when you run iwconfig at the terminal.

```
wlan1      802.11b/g  Mode:Managed  Access Point: Not-Associated
           Bit Rate:11 Mb/s   Tx-Power=7 dBm
           Retry:on    Fragment thr:off
           Encryption key:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
```

```
Tx excessive retries:0   Invalid misc:0   Missed beacon:0

wlan2    RT73 WLAN
Link Quality:0   Signal level:0   Noise level:113
Rx invalid nwid:0   invalid crypt:0   invalid misc:0
```

These devices support packet injection and provide signal strength readings for Kismet to help track down a rogue wireless device.

Aircrack-ng

The package of aircrack-ng that is downloaded and installed supports packet injection. This will be used with the external usb wireless adapter configured above.

```
Nokia-N810-43-7:~# wget http://www.jedge.com/n810/debs/aircrack-ng_1.0_rc3-2_armel.deb
Nokia-N810-43-7:~# wget http://www.jedge.com/n810/debs/libnl1_1.1-5_armel.deb
Nokia-N810-43-7:~# dpkg -i aircrack-ng_1.0_rc3-2_armel.deb
Nokia-N810-43-7:~# dpkg -i libnl1_1.1-5_armel.deb
```

Client Security Assessment

If you like entering the commands yourself then follow the instructions below. At the end I'll provide a link to a script you can download and run.

Update Iptables modules. We will need this for network address translation (nat).

```
Nokia-N810-43-7:~#apt-get install iptables-nat iptables-ext
```

Start Airbase-ng (part of the aircrack-ng suite) to listen for all probe requests and response with the corresponding ESSID, also offer the ESSID "Free WiFi". You can change this to whatever you would like that would help trick users to connecting to it.

```
Nokia-N810-43-7:~#ifconfig wlan1 down
Nokia-N810-43-7:~#ifconfig wlan1 up
Nokia-N810-43-7:~#airmon-ng start wlan1
Nokia-N810-43-7:~#airbase-ng -P -C 20 -e "Free WiFi" -v wlan1
```

In another terminal (xterm) window

Airbase-ng will create the access point interface at0 that the clients will be able to connect to. We need to set an IP address for at0 and run dnsmasq (DNS/DHCP server) so the client can get an IP address and any additional networking information.

```
Nokia-N810-43-7:~# ifconfig at0 up 192.168.5.254 netmask 255.255.255.0
Nokia-N810-43-7:~# dnsmasq -i at0 -a 192.168.5.254 -K -I lo -z -d --pid-file=/var/run/dnsmasq.at0.pid --dhcp-range=192.168.5.50,192.168.5.100,12h --address=/google.com/192.168.5.254
```

Dnsmasq options explained (for help on all available options see manpage here <http://thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html>)

- i : set the interface it will listen on
- a : set the IP address it will listen on
- K : run as an authoritative DHCP server that will respond to all address requests immediately even if the address requested from the client is not in the range. This is to prevent timeouts and Windows 7 clients choking saying "Windows unable to connect to" messages.
- I : ignore listening on an interface, in this case the local (lo) interface
- z : allows dnsmasq to discard requests that it shouldn't reply to. Helpful as dnsmasq runs as a service when the n810 boots.

-d : do not run in the background, good for troubleshooting and monitoring if dnsmasq is working. OPTIONAL
--pid-file= : set the pid file instead of the default. Good so we can still run the dnsmasq service that n810 starts when the device boots.
--dhcp-range=: self explanatory
--address : great option for a pentester. You can set a domain between the forward slashes that will be directed to the ip address given. This is so you can provide your own spoofed page for credential captures. OPTIONAL

```
Nokia-N810-43-7:~#
```

```
Nokia-N810-43-7:~#apt-get install php5-common php5-cgi lighttpd
Nokia-N810-43-7:~#mkdir /media/mmc1/www
Nokia-N810-43-7:~#mkdir /var/log/lighttpd
Nokia-N810-43-7:~#touch /var/log/lighttpd/error.log
Nokia-N810-43-7:~#chmod 777 /var/log/lighttpd
Nokia-N810-43-7:~#chmod 777 /var/log/lighttpd/error.log
Nokia-N810-43-7:~#vim /etc/lighttpd.conf
```

Make the following changes to lighttpd.conf. To help find the line numbers enter the command :set number

```
Line 25:  server.document-root = "/media/mmc1/www/"
Line 28:  server.errorlog = "/var/log/lighttpd/error.log"
Line 73:  server.port = 80
Line 76:  server.bind = "192.168.5.254"
Line 150: cgi.assign = ( ".pl" => "/usr/bin/perl", ".cgi" => "/usr/bin/perl", ".php" => "/usr/bin/php-cgi"
)
```

In the web document root we will place our scripts to assist in intercepting any form of web authentication that the client we are auditing uses. For example: create a web proxy page and ask for their domain username and password.

```
Nokia-N810-43-7:~#
```

Metasploit

```
Nokia-N810-43-7:~# wget http://www.jedge.com/n810/ruby.zip
Nokia-N810-43-7:~# unzip ruby.zip
Nokia-N810-43-7:~# cd ruby
Nokia-N810-43-7:~# dpkg -i ruby_1.8.5-p35_armel.deb
Nokia-N810-43-7:~# dpkg -i rubygems_0.9.2_armel.deb
Nokia-N810-43-7:~# gem install activesupport-1.4.1.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# gem install activerecord-1.15.2.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# gem install actionpack-1.13.2.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# gem install actionmailer-1.3.2.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# gem install actionwebservice-1.2.2.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# gem install rake-0.7.1.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# gem install rails-1.2.2.gem --no-rdoc --no-ri
Nokia-N810-43-7:~# dpkg -i sqlite3-ruby_1.2.1_armel.deb
Nokia-N810-43-7:~# dpkg -i nmap_4.20_armel.deb
```

On a separate Linux machine download one of the older versions of Metasploit 3 (version 3.2) and strip all .svn information.

```
#wget http://updates.metasploit.com/data/releases/framework-3.2.tar.gz
#tar zxvf framework-3.2.tar.gz
#cd framework-3.2
#find . -name .svn -exec rm -rf {} \;
#cd ..
#tar zcf framework-3.2.tar.gz framework-3.2
```

Copy the TAR ball to the Nokia device using scp

```
#scp framework3.tar.gz root@192.168.2.101:/
```

Note: Use your Nokia device's IP address

Back on the Nokia device

```
Nokia-N810-43-7:~# cd /
Nokia-N810-43-7:~# tar zxvf framework-3.2.tar.gz
Nokia-N810-43-7:~# rm framework-3.2.tar.gz
```

```
Nokia-N810-43-7:~# cd framework-3.2
Nokia-N810-43-7:~# ./msfconsole
```

Enjoy Metasploit!

```
BusyBox v1.6.1 (2008-09-18 09:43:17 EEST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
~ $ root
[1|root@Nokia-N810-43-7|~]cd /
[1|root@Nokia-N810-43-7|/]cd framework-3.2/
[1|root@Nokia-N810-43-7|/framework-3.2|]./msfconsole

      o               8      o  o
      8               8      8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8
8 8 8 8.      8 8      8 'Yb. 8 8 8 8 8 8 8
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....:8.....:
:8:
:8:
:8:
=====

      =[ msf v3.2-release
+ -- --=[ 320 exploits - 217 payloads
+ -- --=[ 20 encoders - 6 nops
      =[ 99 aux

msf > █
```


Bluetooth Scanning

Btscanner

Download and install the btscanner utility to scan and log Bluetooth devices in your environment.

```
Nokia-N810-43-7:~# wget http://www.jedge.com/n810/debs/btscanner_2.1-1_armel.deb
Nokia-N810-43-7:~# dpkg -i btscanner_2.1-1_armel.deb
```

To run btscanner open up the terminal application, become root, and run the command btscanner.

Time	Address	Clk off	Class	Name	RSSI: +0 LQ: 000 TXPWR: Cur +0
2011/08/01 15:27:23	1C:65:9D:F4:0D:D5	0x4930	0x00010c	(unknown)	Address: 3C:74:37:7B:93:55
2011/08/01 15:27:02	70:1A:04:5A:1A:ED	0x1ef0	0x000000	(unknown)	Found by: 00:1D:6E:D9:4B:EB
2011/08/01 15:26:56	70:1A:04:59:F0:97	0x462c	0x000000	Dell Wireless 3	OUI owner:
2011/08/01 15:26:50	00:25:56:D6:F7:3E	0x2563	0x000000	Dell Wireless 3	First seen: 2011/08/01 15:24:13
2011/08/01 15:26:42	00:22:5F:4B:A8:8D	0x2c7f	0x000000	Dell Wireless 3	Last seen: 2011/08/01 15:24:13
2011/08/01 15:26:17	90:4C:E5:F9:8D:84	0x1a89	0x000000	(unknown)	Name: BlackBerry 9800
2011/08/01 15:25:56	00:26:5E:96:46:43	0x42c7	0x7e010c	(unknown)	Vulnerable to:
2011/08/01 15:25:25	90:00:4E:DF:5E:0E	0x6824	0x000000	(unknown)	Clk off: 0x5f1d
2011/08/01 15:25:10	0C:60:76:85:B6:8D	0x5a88	0x7e010c	CBSL212035	Class: 0x7a020c
2011/08/01 15:24:17	6C:0E:0D:04:8A:EE	0x0cf0	0x5a0204	(unknown)	Phone/Smart phone
2011/08/01 15:24:13	3C:74:37:7B:93:55	0x5f1d	0x7a020c	BlackBerry 9800	Services: Networking,Capturing,Object Transfer,Audio,Telephony
2011/08/01 15:23:32	00:22:5F:4D:95:16	0x6bde	0x000000	(unknown)	HCI Version
2011/08/01 15:28:17	00:13:46:C8:E2:08	0x680a	0x02010c	J-LAPTOP	-----
2011/08/01 15:25:22	00:16:B8:E7:7C:CC	0x44a6	0x520204	W300i	LMP Version: 2.1 (0x4) LMP Subversion: 0x1dif
2011/08/01 15:28:14	00:25:56:D4:4E:8C	0x73e2	0x000000	Dell Wireless 3	Manufacturer: Texas Instruments Inc. (13)
2011/08/01 15:24:09	00:25:56:D2:76:DD	0x72a6	0x000000	Dell Wireless 3	
2011/08/01 15:22:48	00:24:2B:FC:49:D8	0x28c7	0x000000	Dell Wireless 3	
Found device 00:24:2B:FB:6C:E5					Found device 00:16:B8:E7:7C:CC
Found device 00:13:46:C8:E2:08					Found device 70:1A:04:58:8C:9E
Found device 00:24:2B:FB:6C:E5					Found device 00:25:56:D4:4E:8C
Found device 70:1A:04:58:8C:7F					Found device 00:13:46:C8:E2:08

Appendix A: All the Links I used to create this tutorial and then some

Setup Nokia Tablet Repositories

<http://www.gronmayer.com/it/index.php>

Mulliner Repository (has nmap, aircrack, socat)

<http://www.mulliner.org/nokia770/>

2008 Nokia Blog with A LOT of information

<http://andrew.daviel.org/n810-blog.html>

n810 Serial Port

<http://bu3sch.de/cms/index.php/nokia-n810-serial-console>

Cross-Compile Software for Nokia N810

<http://talk.maemo.org/archive/index.php/t-6191.html>

<http://maemo-sdk.garage.maemo.org/>

<http://www.scratchbox.org/documentation/docbook/installdoc.html>

Libpcap1 (version 1)

http://maintenance.maemo.org/packages/package_instance/view/diablo_extras-devel_free_armel/libpcap1/1.0.0-1/

Hackathon 2008 (nokismet guide(old))

<http://www.p16blog.com/p16/2008/05/hackathon-pics.html>

Newcore Kismet DEB and source

<http://matt.ucc.asn.au/kismet-maemo/>

Using Kismet and GPS on n810

<http://nile.cise.ufl.edu/pages/experiments-amp-testbeds/nokia-8x0-tips-and-tricks.php>

Latest oldcore version of Kismet DEB

<http://www.cise.ufl.edu/~agv/n800/index.php>

Old Nokia n810 page, how to update OS in Linux, a lot of information

<http://www.arachnoid.com/linux/nokia/>

Forum post with how to enable Red Pill mode

<http://forum.brighthand.com/nokia-maemo-os/258012-nokia-n800-n810-safe-mode.html>

Full Aircrack tools, need usb adapter

<http://talk.maemo.org/archive/index.php/t-20888.html>

<http://talk.maemo.org/showthread.php?t=20888&highlight=aircrack-ng+full+set>

GPS lock posts

<http://www.gossamer-threads.com/lists/maemo/users/31158>

<http://forums.internettablettalk.com/showthread.php?t=17229>

Nokia FAQ. Very helpful!

<http://andrew.daviel.org/N810-FAQ.html>

Compiled Aireplay-ng and info on what usb wireless card to get

<http://talk.maemo.org/showthread.php?t=13458>

External USB wireless

<http://talk.maemo.org/showthread.php?p=379915>

http://wiki.maemo.org/Networking_%28Diablo%29

<http://talk.maemo.org/showthread.php?t=31117>

rt73.ko driver

http://wiki.maemo.org/USB_to_ethernet_networking

RTL8187 (r8187 driver)

<http://talk.maemo.org/showthread.php?t=30838>

make your own usb power injector

<http://tabletblog.com/2006/01/usb-power-injector-2.html>

or

5V Battery

Google Lenmar PowerPort Mini 5V lithium battery

Screen Rotation

<http://wiki.maemo.org/Rotation>

Bluetooth (btscanner)

<http://forums.internettablettalk.com/showthread.php?p=281048>

Screenshots

<http://beans.seartipy.com/2007/10/03/different-ways-of-taking-screenshots-in-nokia-n800/>

Scratchbox Documentation

<http://www.scratchbox.org/documentation/docbook/tutorial.html>

<http://www.scratchbox.org/documentation/docbook/installdoc.html>

How to build packages

<http://wiki.maemo.org/Packaging>

<https://wiki.ubuntu.com/PackagingGuide/Complete>

USB Wireless Adapters

Belkin Wireless G USB (version 3xxx – F5D7050B)

http://en-us-support.belkin.com/app/answers/detail/a_id/297/~/f5d7050-wireless-g-usb-network-adapter---drivers

http://desc.shop.ebay.com/i.html?_nk=F5D7050B&_sacat=0&_odkw=F5D7050B&_osacat=0&_trksid=p3286.c0.m270.l1313&LH_TitleDesc=1

With external antenna

Hawking hwug1a

<http://www.hawkingtech.com/products/productlist.php?CatID=35&FamID=111&ProdID=362>

http://shop.ebay.com/i.html?_from=R40&_trksid=p5197.m570.l1313&_nkw=hwug1a&_sacat=See-All-Categories

Edimax EW-7318USg

<http://www.newegg.com/Product/Product.aspx?Item=N82E16833315075>

USB Host Mode

<http://talk.maemo.org/showthread.php?t=14092>

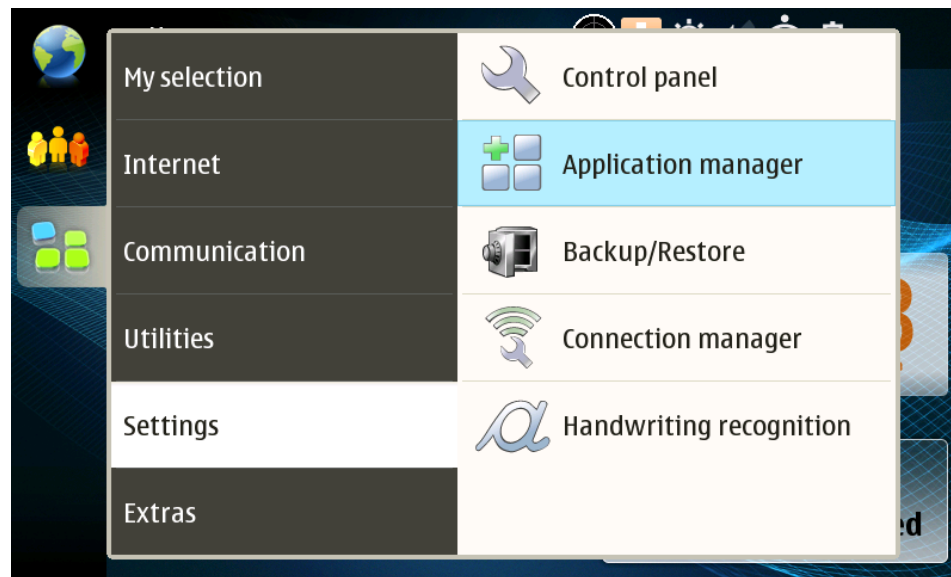
Metasploit 3 on N800 (probably works on N810)

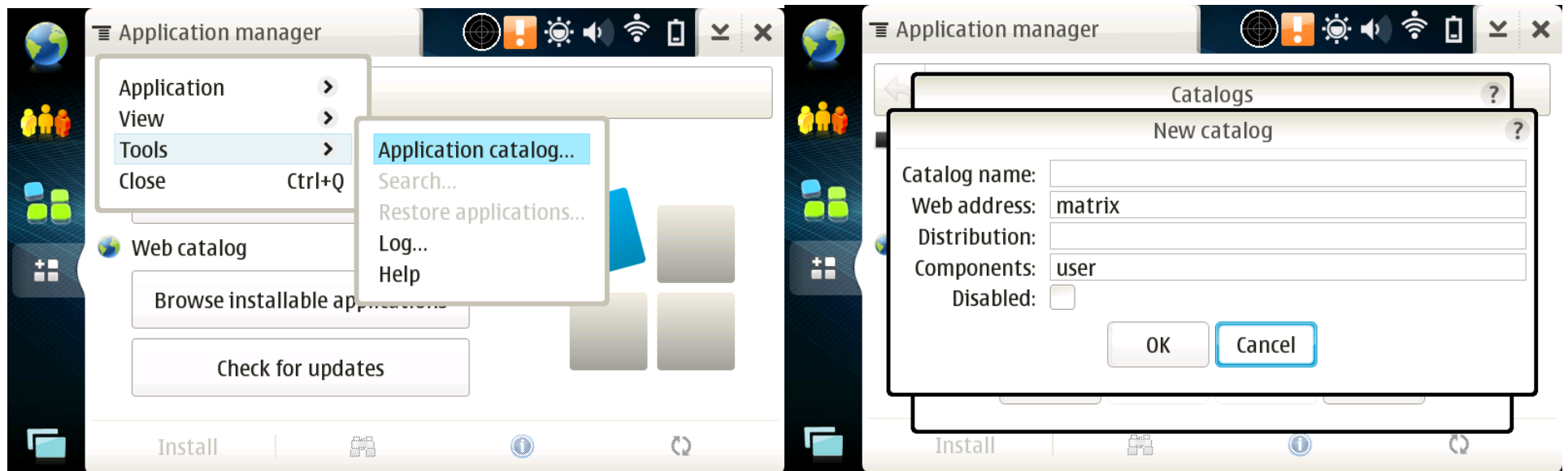
<http://mfresh-n800.blogspot.com/2007/07/installing-metasploit-framework-3-on.html>

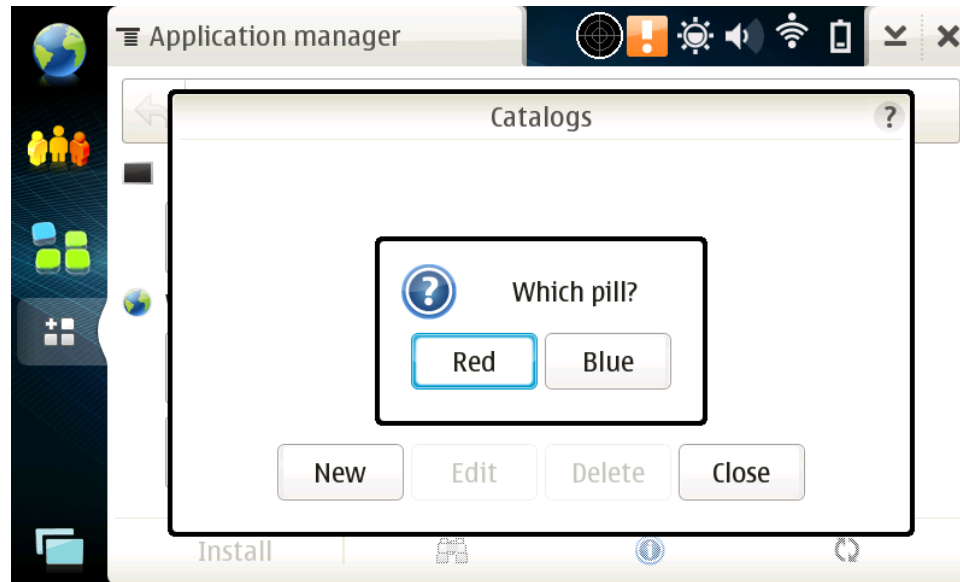
Appendix B: Enable Red Pill Mode

Enable Libraries through Application Manager for Nokia N810 – Red Pill Mode

Follow the screenshots to enable the ability to access the libraries on your Nokia N810. Note you are doing this at your own risk and you could brick your device. I have no idea if that is true but you have been warned.







Open the Application Manager and click the menu button in the top left corner of the window. You can also hit the menu button on the bottom left of the keyboard.

Select Tools → Application Catalog...

Select New and enter the word “matrix” (without the quotes) in the web address field. Delete the default http:// that you will find in the field. It must be all lowercase.

Click **Cancel**

When asked Which pill? Choose Red. Unlike Neo, you can always return by going through the same steps and picking the Blue pill.

Appendix C: Remapping Keys

Remapping Keys

The file that controls the key mappings is `/usr/share/X11/xkb/symbols/nokia_vndr/rx-44`. Modifying this file to change the Yen, British Pound, and Euro keys to more functional keys like Tab, Pipe `|`, and Esc.

For changing the mappings the words are case sensitive. Tab = Tab, the Pipe = bar, and Esc = Escape

The Euro symbol looks like an “E” so I made that the Escape key. The Yen is right next to the function key so I made that the Tab (easy to press both at once with your thumb). I made the pipe the British Pound. Below is what the changes look like.

```
partial_alphanumeric_keys
xkb_symbols "us" {
    name[Group1] = "U.S. English";

    include "nokia_vndr/rx-44(base)"

    key <AC01> { [ a, A, exclam, exclam ] };
    key <AC02> { [ s, S, quotedbl, quotedbl ] };
    key <AC03> { [ d, D, at, at ] };
    key <AC04> { [ f, F, numbersign, numbersign ] };
    key <AC05> { [ g, G, backslash, backslash ] };
    key <AC06> { [ h, H, slash, slash ] };
    key <AC07> { [ j, J, parenleft, parenleft ] };
    key <AC08> { [ k, K, parenright, parenright ] };
    key <AC09> { [ l, L, asterisk, asterisk ] };
    key <AC11> { [ apostrophe, question, question, question ] };

    key <AB01> { [ z, Z, Tab, Tab ] };
    key <AB02> { [ x, X, asciicircum, asciicircum ] };
    key <AB03> { [ c, C, asciitilde, asciitilde ] };
    key <AB04> { [ v, V, percent, percent ] };
    key <AB05> { [ b, B, ampersand, ampersand ] };
    key <AB06> { [ n, N, dollar, dollar ] };
    key <AB07> { [ m, M, Escape, Escape ] };
    key <AC10> { [ semicolon, colon, bar, bar ] };
```

```
key <AE11> {      [      minus,      underscore,      underscore,      underscore      ]      };
key <AE12> {      [      plus,      equal,      equal,      equal      ]      };

key <AB08> {      [      comma,      less,      comma,      less      ]      };
key <AB09> {      [      period,      greater,      period,      greater      ]      };
};
```

Appendix D – Getting flasher exe to work on Windows 7 64-bit.

How to get N810 flasher to work in Windows 7 64-bit (x64).

- Install Flasher 3.5 - <http://tablets-dev.nokia.com/maemo-d...-downloads.php>
- Download libusb-win32-bin-1.2.2.0.zip - <http://sourceforge.net/projects/libusb-win32/> and extract the contents of the zip file.
- With the USB plugged in power on the device while holding the Swap (looks like two overlapping boxes on left side) button.
- Wait for the original driver to install.
- Run inf-wizard.exe (bin folder in libusb folder you extracted from the zip file) - Run as Administrator
 1. Press "Next"
 2. Search in list and select "0x0421 - 0x0105 - Nokia N810 (Update Mode)"
 3. Press "Next"
 4. Press "Next"
 5. Save .inf file
 6. Press "Install Now"
 7. Press "Install this driver software anyway" on warning message.
 8. You should get "Installation successful." and press OK.
- Check Windows Device Manager for "libusb-win32 devices", expand and verify "Nokia N810 (Update Mode)" can be found.
- Now you are ready to run Flasher 3.5 with your parameters.

Appendix E – Windows Flasher Sample Output

```
flasher v2.5.2 (Sep 24 2009)

SW version in image: RX-44_DIABLO_5.2008.43-7_PR_MR0
Image 'kernel', size 1500 kB
    Version 2.6.21-200842maemo1
Image 'initfs', size 2273 kB
    Version 0.95.22-200842maemo1w38b3
Image 'rootfs', size 122496 kB
    Version RX-34+RX-44+RX-48_DIABLO_5.2008.43-7_PR_MR0
Image '2nd', size 8192 bytes
    Valid for RX-44: 0808
    Version 1.1.16-200844maemo2
Image 'xloader', size 9216 bytes
    Valid for RX-44: 0808
    Version 1.1.16-200844maemo2
Image 'secondary', size 100736 bytes
    Valid for RX-44: 0808
    Version 1.1.16-200844maemo2
Image '2nd', size 8192 bytes
    Valid for RX-44: 0801, 0802, 0803, 0804, 0805, 0806, 0901, 0902
    Version 1.1.16-200844maemo2
Image 'xloader', size 9216 bytes
    Valid for RX-44: 0801, 0802, 0803, 0804, 0805, 0806, 0901, 0902
    Version 1.1.16-200844maemo2
Image 'secondary', size 100736 bytes
    Valid for RX-44: 0801, 0802, 0803, 0804, 0805, 0806, 0901, 0902
    Version 1.1.16-200844maemo2
USB device found found at bus bus-0, device address \\.\libusb0-0001--0x0421-0x0
105.
Found device RX-44, hardware revision 0801
NOLO version 1.1.16
Version of 'sw-release': RX-44_DIABLO_5.2008.43-7_PR_MR0
```

```
Sending xloader image (9 kB)...  
100% (9 of 9 kB, avg. 2250 kB/s)  
Sending secondary image (98 kB)...  
100% (98 of 98 kB, avg. 10930 kB/s)  
Flashing bootloader... done.  
Sending kernel image (1500 kB)...  
100% (1500 of 1500 kB, avg. 14429 kB/s)  
Flashing kernel... done.  
Sending initfs image (2273 kB)...  
100% (2273 of 2273 kB, avg. 18943 kB/s)  
Flashing initfs... done.  
Sending and flashing rootfs image (122496 kB)...  
100% (122496 of 122496 kB, avg. 6690 kB/s)  
Finishing flashing... done
```

Appendix F – Screenshots to configure an external Bluetooth GPS

