



USERGUIDE

2003 © Max Moser (mmo@remote-exploit.org)
English translation Gürkan Sengün (gurkan@linuks.mine.nu)
and Nils Brünggel (neo@cyber-hacking.com)

1 Preface

Meanwhile wireless 802.11 networks are common in companies and in home use too. No matter if you comfortably surf the Internet while in the garden or to simplify the data processing in shops.

Unfortunately this flexibility also has disadvantages.

Wellenreiter was developed to analyze wrongly configured networks. This is simple and possible transparently and without interfering the network. The collected information helps to optimize the environment.

With the actual version of Wellenreiter everybody can optimize and secure it's wireless network and verify it's state.

Table of content

1 Preface	2	6.2.5 Reset.....	11
2 Wireless LAN basics.....	4	6.2.6 Close.....	11
2.1 The objects in a wireless LAN.....	4	6.3 Statusbar.....	12
2.2 IBSS / ESS.....	4	6.4 Treeview.....	12
2.2.1 IBSS (AD-HOC mode).....	4	6.5 Clist.....	13
2.2.2 ESS (INFRASTRUCTURE mode).....	5	6.5.1 State.....	13
2.3 ESSID / SSID.....	6	6.5.2 Chan	13
2.4 Channel / Frequency	6	6.5.3 Network ESSID.....	13
2.5 MAC Filter.....	6	6.5.4 MAC-Address.....	13
2.6 WEP (Wired Equivalent Privacy).....	6	6.5.5 WEP.....	14
2.7 GPS / GPSD.....	6	6.5.6 Manufactor.....	14
3 Installation of Wellenreiter.....	7	6.5.7 Networktype.....	14
4 Hardware Requirements.....	7	6.5.8 Packet indicator.....	14
5 Starting Wellenreiter.....	8	7 The event window.....	15
5.1 Inserting the wireless card.....	8	8 The log window.....	15
5.2 Getting superuser / root privileges.....	8	9 The Active Traffic window.....	16
5.3 Running Wellenreiter.pl.....	8	10 The about window.....	16
6 The main window.....	9	11 The Detail window.....	17
6.1 Menulist.....	9	12 Scanning with Wellenreiter.....	18
6.1.1 File.....	9	12.1 Scan – Start.....	18
6.1.2 Scan.....	9	12.2 Examine the logwindow.....	18
6.1.3 View.....	9	12.3 New object found	19
6.1.3.1 Toggle Log Window.....	9	12.3.1 Treeview.....	19
6.1.3.2 Toggle Traffic Window.....	9	12.3.2 Clist.....	19
6.1.3.3 Toggle Toolbar.....	9	12.3.3 Logwindow.....	19
6.1.3.4 Reset.....	9	12.4 Viewing the details of a discovered object..	20
6.1.4 Options.....	10	13 Resetting Wellenreiter	21
6.1.4.1 Accoustic beacon indicator...	10	14 Aborting the scan.....	21
6.1.4.2 Accoustic events.....	10	15 Saving the data of Wellenreiter	21
6.1.4.3 Configure soundevents.....	10	15.1 Automatic Save.....	21
6.1.5 Help.....	10	15.2 Manual Save.....	21
6.2 Toolbar.....	11	16 Exporting to other formats.....	21
6.2.1 Start	11	17 Quit Wellenreiter.....	21
6.2.2 Stop.....	11		
6.2.3 Save.....	11		
6.2.4 Load.....	11		

2 Wireless LAN basics

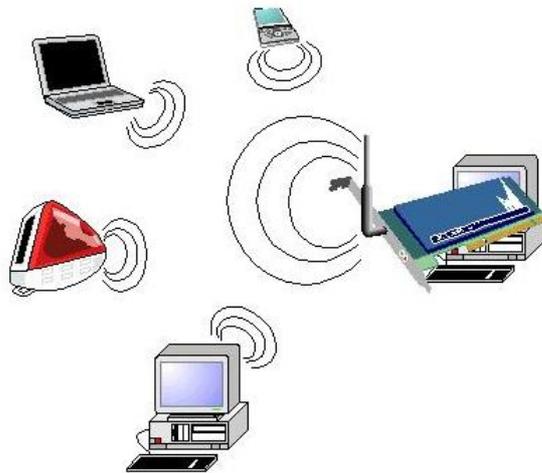
2.1 The objects in a wireless LAN

A wireless network consists of at least two devices. There needs to be one accesspoint and one or multiple clients with the appropriate hardware. The accesspoint is the connecting part between the clients and the usual cabled network.

2.2 IBSS / ESS

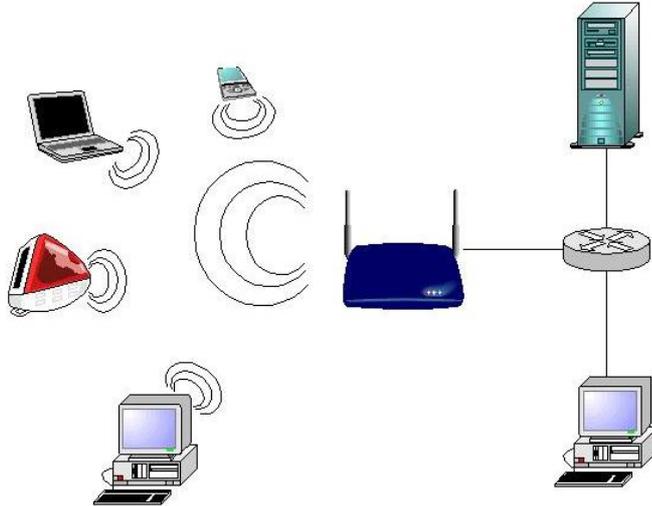
2.2.1 IBSS (AD-HOC mode)

A client can be configured to act as an accesspoint. That pseudo accesspoint has some limitations for encryption, transmitting range, the roamings and controlling. This operating mode is known as IBSS or AD-HOC mode. This is much like a classic peer to peer network. Everybody is talking to everybody, the pseudo accesspoint takes care about the timing.



2.2.2 ESS (INFRASTRUCTURE mode)

If you use a real hardware accesspoint, that mode is called ESS or Infrastructure Mode. You do not have the mentioned limitationed above, the transmitting range often is multiple times bigger too. Each station is communicating with the accesspoint, which itself is sending it further to other networks.



2.3 ESSID / SSID

The (E)SSID (Extended Service Set Identifier) is the name of the wireless network and can be compared with VLAN labels. That name enables you to enter the network and to define what is part of it.

2.4 Channel / Frequency

Each network can be run in one or multiple frequencies. The available channels vary because of the permitted frequencies allowed for communication. Most countries in Europe have 13 channels. The USA has 11 and Japan only has one due to military restrictions. There are several recommendations in what channels accesspoints shall be overlaid for data transmission. Generally one can say overlaid frequencies should be avoided. If every accesspoint would use the same frequency data would be lost and there would be a performance problem.

2.5 MAC Filter

Each networkcard has a unique address, the MAC address. This identifier can be used to control access. The use is called MAC filtering and is only available to real ESS accesspoints. The MAC filter is limited in efficiency because the MAC address can be changed by software on nearly all cards. A MAC-filter is not able to protect your network traffic from being sniffed by somebody, because everybody gets the radio beams.

2.6 WEP (Wired Equivalent Privacy)

The 802.11b standard integrates that fast but not perfect encryption. WEP is not secure. About 2.000.000 packets are required to calculate the key. It is possible to break the encryption faster if the authentication is done by WEP. A text is sent plain text first and then encrypted. That way known plaintext attacks can be used to find out the key.

2.7 GPS / GPSD

Global Positioning System, short GPS, is a satellite based system to define the exact position. With a GPS daemon you can connect GPS devices to the computer by the serial port. Wellenreiter detects if a gpsd is active. If GPS information is available, the positions of found objects is logged automatically. The GPS daemon gpsd is started manually before Wellenreiter.

3 Installation of Wellenreiter

Please refer to the install document shipped with the software.

4 Hardware Requirements

Wellenreiter needs at least one wireless card.

The following are supported:

- Lucent/Orinocco based cards with patched drivers (Firmware 6.16 is recommended)

- Cisco Aironet 350 cards with RFMON activated drivers (Version 5.x firmware and higher are not supported)

- Prism2/Prism2.5 chip based cards with WLAN-NG drivers

The HOSTAP driver as well as PCMCIA cards are not supported in the actual version of Wellenreiter. A gpsd compatible GPS device with the required cabling is recommended to use the GPS functionality. A Machine comparable to a Pentium with 500 mhz is recommended.

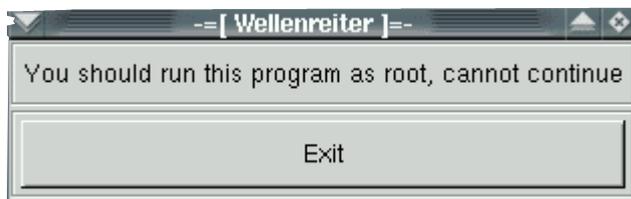
5 Starting Wellenreiter

5.1 Inserting the wireless card



Before you start Wellenreiter, you must insert a wireless card into the PCMCIA slot.

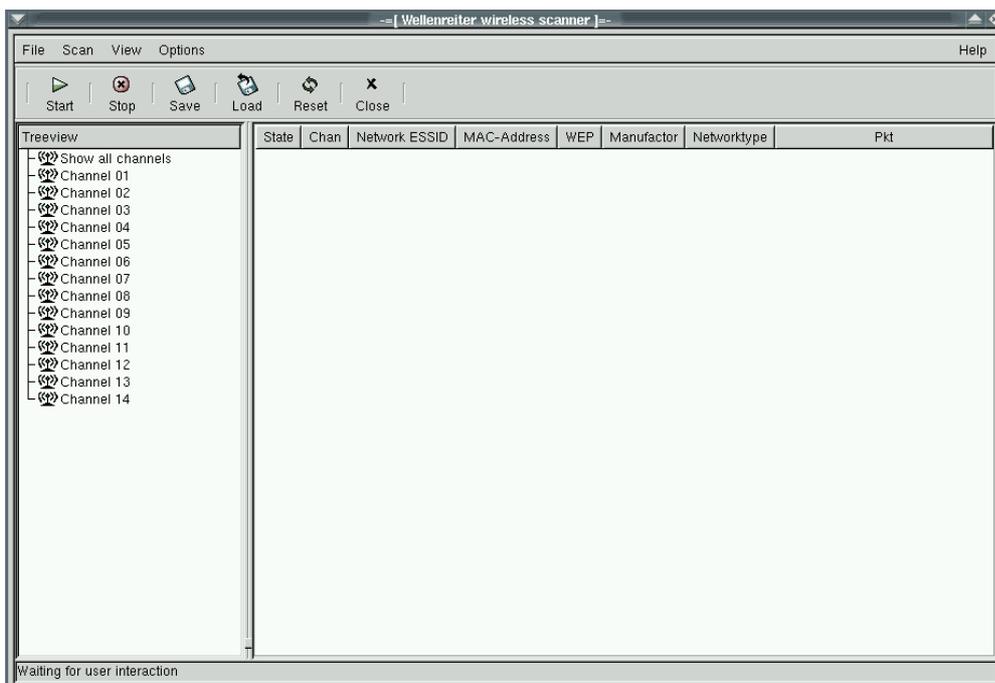
5.2 Getting superuser / root privileges



To use Wellenreiter successfully you will need root or superuser access. Login as root or use SUDO to run Wellenreiter as root. It's required that Wellenreiter has root privileges, Wellenreiter checks that on startup, if you don't have root privileges, Wellenreiter will tell you that and quit itself, because it cannot work without.

5.3 Running Wellenreiter.pl

When Wellenreiter is installed you can start it with the command 'Wellenreiter.pl'. Of course you can also create an icon or a menu entry on your desktop. (Please read the documentation of your desktop environment) After a short time Wellenreiter's main window will pop up.

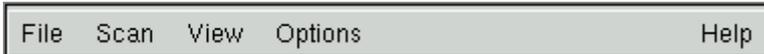


6 The main window

The main window is divided in several parts, which are shortly explained here.

6.1 Menulist

The menulist is used to control Wellenreiter with classical menus.



6.1.1 File

The file menu includes the commands “Open” and “Save”. Save is used to save collected data and to export it in different formats. With the entry “Exit” you can quit Wellenreiter.

6.1.2 Scan

Scan includes the two commands “Start” and “Stop” to start or stop a Scan.

6.1.3 View

In the View menu you find entries to display additional windows or change the view in the main window.

6.1.3.1 Toggle Log Window

With this menu entry you can display the log window. In which are all important informations, concerning wellenreiter, logged.

6.1.3.2 Toggle Traffic Window

This menu entry opens or closes the “Active Traffic” window, in which is displayed what types packets are received from which station.

6.1.3.3 Toggle Toolbar

Here you can show or hide the toolbar.

6.1.3.4 Reset

This menu entry resets the main window and clears all received objects.

6.1.4 Options

The menu options includes all configurations and optional activatable parameters.

6.1.4.1 Accoustic beacon indicator

With this menu entry it is possible to activate an acustic signal for received Beacon frames. This Beacon indicator is used to track the exact location of an accesspoint. Every received Beacon frame procuces a pertinent acustic signal.

6.1.4.2 Accoustic events

This menu entry activates or deacitvates the events which are played when an event happens.

6.1.4.3 Configure soundevents

When this menu point is activated, the “Event configuration” window will pop up. Here you can entry commands which are executed when the appropriate event happens.

6.1.5 Help

Here you will find the about screen which is including the version number.

6.2 Toolbar

The toolbar has got the most important buttons.



6.2.1 Start



Use this button to start the scanning.

6.2.2 Stop



Stop the scan process by clicking this button.

6.2.3 Save



Save collected information additionally to the automatic saves.

6.2.4 Load



With the Load button you can load information you saved before.

6.2.5 Reset



Resets the main window to the defaults. This is the same as if you would restart the program.

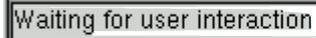
6.2.6 Close



This button is used to quit Wellenreiter.

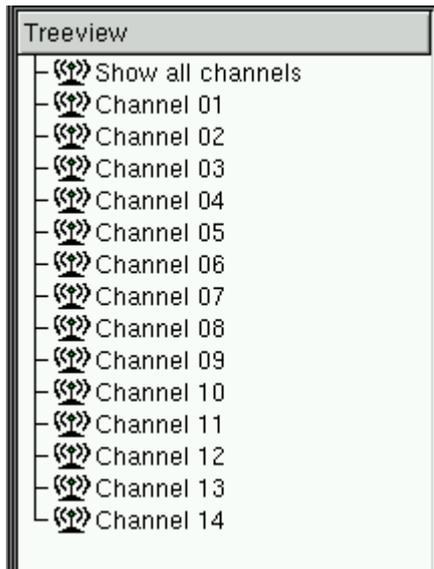
6.3 Statusbar

The status line, at the bottom left, shows some information about what Wellenreiter is actually doing.



Waiting for user interaction

6.4 Treeview



The treeview shows all supported radio frequencies. When an objects are found the are added under the appropriate frequency. The color of a Channel is changed too, after a new object was added. The color can be nomalized by doubleclicking the appropriate Channel. When you select an object the detail window will open.

6.5 Clist

The Clist is the main view of Wellenreiter. Inside the Clist, you can see which objects were found and which parameters they have. If only one channel is selected in the treeview, the Clist will show the associated and newly found objects. If "Show all channels" is activated in the treeview, filtering will be disabled.

State	Chan	Network ESSID	MAC-Address	WEP	Manufacturer	Networktype	Pkt
-------	------	---------------	-------------	-----	--------------	-------------	-----

6.5.1 State

State	This column shows if a network reveals its ESSID or not. If the icon is red, the network will not reveal its name, otherwise the icon is green.
	
	

6.5.2 Chan

Chan	This column shows the channel number, in which the object was found.
11	
7	

6.5.3 Network ESSID

Network ESSID	Here are the found network names displayed. If a network does not reveal its name, Wellenreiter will display "Non-broadcasting". When Wellenreiter could figure out the ESSID, because of the network traffic, "Non-broadcasting" will be replaced with the discovered name.
Non-broadcasting	
wlan	

6.5.4 MAC-Address

MAC-Address	This column displays the MAC-address of the object.
00409657c3b6	
000393e9e67c	

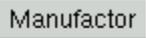
6.5.5 WEP



Here is shown, if an object chiffers it's data with WEP or not.



6.5.6 Manufacturer



AIRONET
APPLE

With the MAC-Adress, the manufactur of the card can be analyzed. Of course this indication does not have to match with the "Label" of the device, because most device manufacturers buy their chips and do not factor themselves.

6.5.7 Networktype



This icon symbolizes, if it's a real accesspoint or a WLAN-card in AD-HOC Mode.

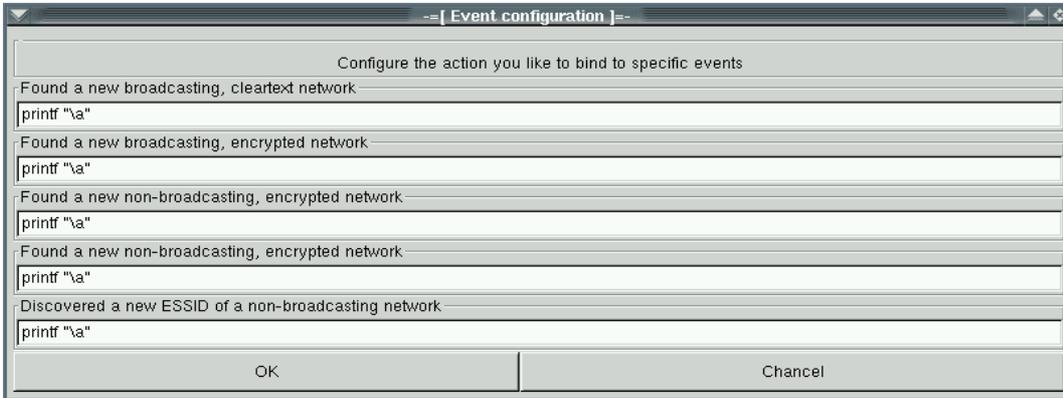


6.5.8 Packet indicator

This column displays alternating the sign "*" and "+", if the appropriate objects sends packts. So it's possible to also find the acctually sending object in overlaying networks.

7 The event window

The event window is used to assign commands to certain events. By default, an acoustic signal will be played, although it's possible to execute all kinds of commands. For example it's possible to play a .wav file, if the name of an unknown network has been found. You can do that by entering the command "play filename.wav". By pressing the OK button, the settings will be saved.



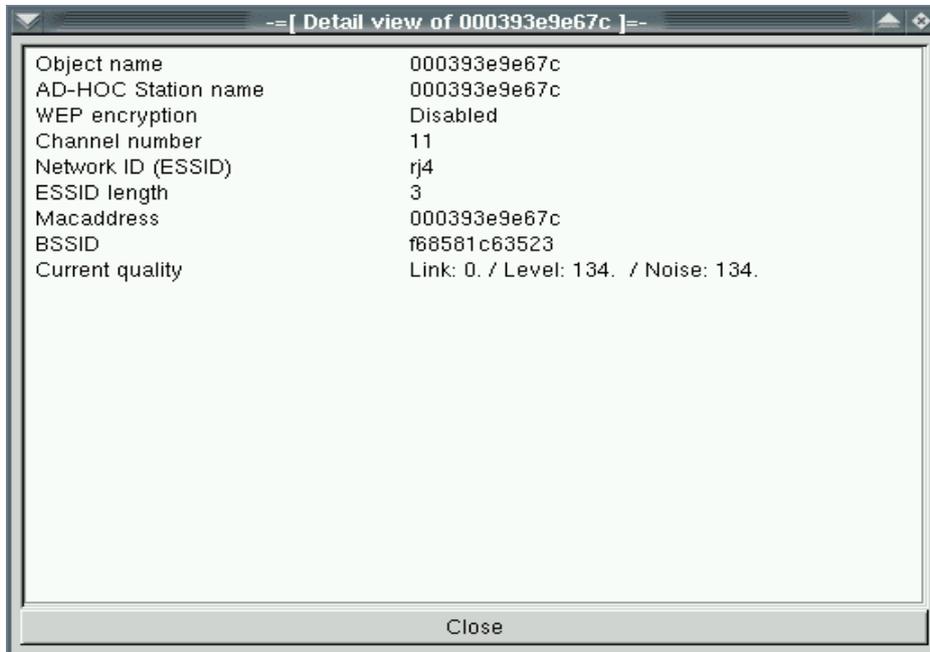
8 The log window

The log window displays the most important information. No information is saved.



11 The Detail window

This window updates its content regularly, so that the most actual informations are displayed. If an object in the treeview of the main window was chosen, a detail window will open. Important: On the first opening it's possible, that the content appears only after a short time.

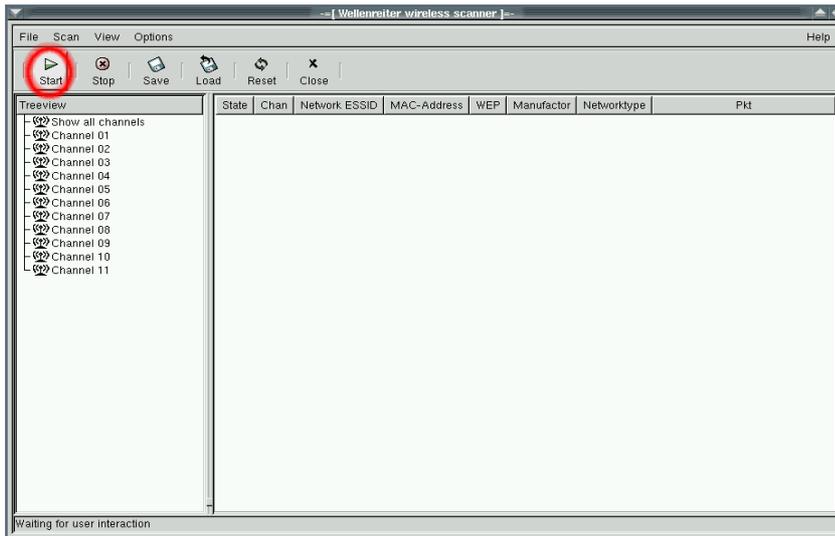


12 Scanning with Wellenreiter

This Chapter is a short introduction about analyzing a wireless network with Wellenreiter.

12.1 Scan – Start

After Wellenreiter was started successfully and the main window is visible, scanning can be started by pressing the scan button or chose “Scan” from the menu “Start”. The statusbar changes it's content from “Waiting for user interaction” to “Waiting for packtes...”



12.2 Examine the logwindow

You should open the logwindow by choosing “Toggle Log Window” in the menu “View”. The last line shows that Wellenreiter is jumping through frequencies. Further the logwindow shows, that two files are created. One with the ending “.save” and a second with the ending “.dump”. The “.save” file includes the found objects in Wellenreiter savefile formate. The “.dump” file is a tcpdump / Ethereal compatible dumpfile. The dumpfile can be used for further Evaluation of the data with a sniffer like Ethereal.



12.3 New object found

When Wellenreiter finds a new object, it will add the object to the Clist, the treeview and the logfile.

12.3.1 Treeview



The frequencies channel will be, by finding a new object, become red. The color will be normal again, if the appropriate channel has been chosen by mouse-click.

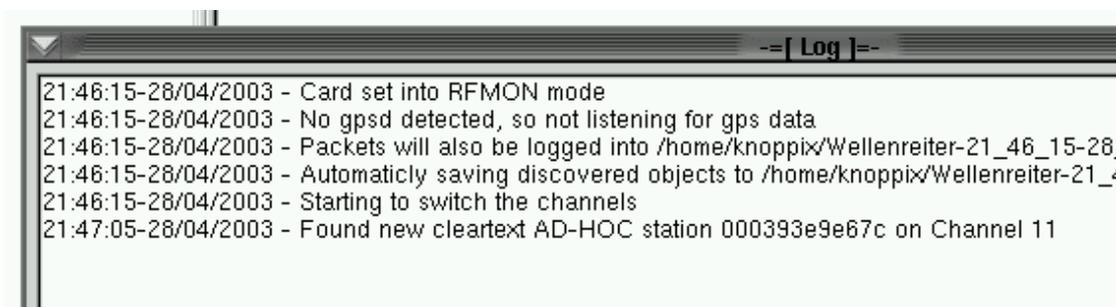
12.3.2 Clist

The Clist gets a new entry with the data to the actual found object. With the "Pkt" Column it's possible to see how often the object transmits data.

State	Chan	Network ESSID	MAC-Address	WEP	Manufactor	Networktype	Pkt
	11	rj4	000393e9e67c	 Off	APPLE	 BSS	*

12.3.3 Logwindow

In the logwindow an entry appears, which describes the found object.



12.4 Viewing the details of a discovered object



To view the details of an object, it must be selected with a mouse-click in the treeview.

After that, the detailwindow with the informationen to the object is shown. Important: It can take a while until the detail informations are shown in the window. This is due to the refresh interval.



13 Resetting Wellenreiter

If you want to reset the Wellenreiter data, simply select the button or select Reset from the View menu.



14 Aborting the scan

To abort the Scan press the button or select Scan and Stop from the toolbar menu.



15 Saving the data of Wellenreiter

15.1 Automatic Save

Wellenreiter saves its data automatically in the “.save” file. The name of this file is created dynamically, as soon as you start a scan.

15.2 Manual Save

If you want to save to specific file select File and then Save.

16 Exporting to other formats

Wellenreiter can export the data to Microsoft compatible mappoints or the much more used CSV format. To do this you select the submenu Export as. Now you need to select the place where you want the new file to be saved.

17 Quit Wellenreiter

You can quit Wellenreiter by clicking the button in the menu File, Exit.

