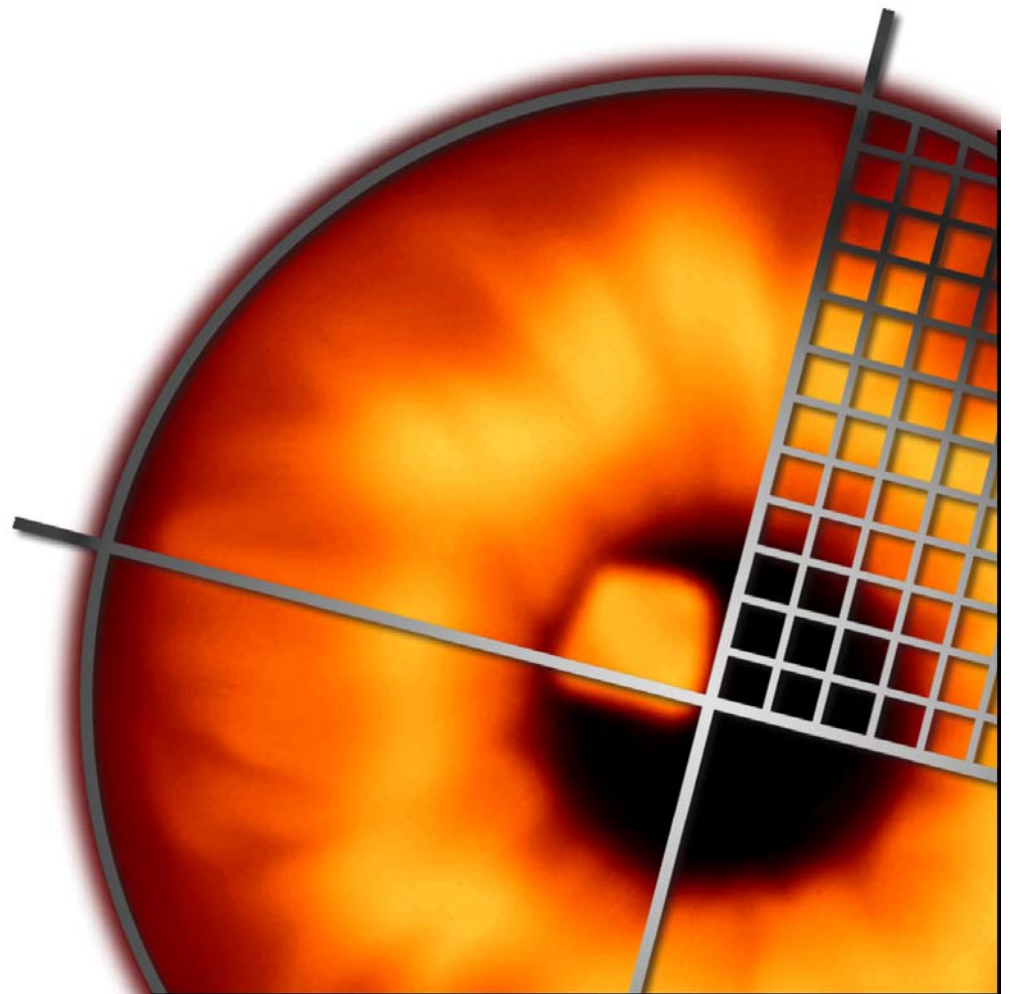




Users Manual

Retina[®] WiFi Scanner

Windows and Pocket PC



Warranty

This document is supplied on an "as is" basis with no warranty and no support.

Limitations of Liability

In no event shall eEye Digital Security be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained in this document is subject to change without notice.

No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this manual.

Disclaimer

All brand names and product names used in this document are trademarks, registered trademarks, or trade names of their respective holders. eEye Digital Security is not associated with any other vendors or products mentioned in this document.

Retina® WiFi Users Manual

© 2004-2005 eEye Digital Security. All rights reserved. | RWIFI-M-033105

This document contains information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of eEye Digital Security.

Collateral Information

For the latest updates to this document, please visit:

<http://www.eeye.com/partners>

Revision: 1-5

Table of Contents

- Overview2
- Operation3
 - Discover Tab3
 - List of detected wireless devices4
 - Detailed Information5
 - WiFi Options6
 - IP Options7
 - Report8
 - Report Summary8
 - Detailed Information9
- Menu9
 - File9
 - Tools10

Overview

Retina WiFi Scanner is a tool to be used to detect IEEE 802.11 (WiFi) based devices. It has following features.

- Detect IEEE 802.11 based access points and AdHoc devices, displaying detailed configuration information.
- If a detected device is an access point, the scanner will attempt to get the IP-related information from inside the network. That information that the scanner can detect includes the IP addresses of DHCP and DNS services, default gateways and access point, as well as domain names and other host and network information.
- Send events to a REM Management Server if unauthorized wireless devices are detected.
- Brute-force WEP keys.
- Generate HTML, XML, and text reports.
- Supports a wide range of NDIS 5.1 compatible wireless cards.

Operation

Discover Tab

Retina Network Security Scanner

File View Tools Help

Help and Support

- Help Topics
- eEye Web Site
- Technical Support
- About Retina

Discover Report

Actions

WiFi Options

- Wep Key Brute forcing attack
- Sound
- Debug
- Dump

Probing interval: 1000 msec

RSSI threshold for IP discovery: -65 msec

Scan

Detected Devices

Status	SSID	RSSI	AP MAC	AP IP	Standard
📶	linksys	-36 (dBm)	00:0C:41:FA:2B:42	192.168.10.1	IEEE 802.11g
📶	xyzyz	-45 (dBm)	00:06:25:00:06:25	10.100.25.43	IEEE 802.11b
📶	puwireless	-61 (dBm)	02:0E:35:00:01:D2	N/A	IEEE 802.11b
📶	regret	-61 (dBm)	02:0E:35:04:21:DC	N/A	IEEE 802.11b
📶	default	-69 (dBm)	00:05:5D:D9:9D:F8	N/A	IEEE 802.11b
📶	eereap	-75 (dBm)	00:40:05:B1:E2:5B	192.168.15.4	IEEE 802.11b
📶	Penguin	no signal	00:06:25:F3:4B:3F	N/A	IEEE 802.11b
✖	NETGEAR	no signal	00:09:5B:52:1F:80	192.168.0.1	IEEE 802.11b
✖	rx101	no signal	00:0C:41:A8:6D:94	192.168.0.254	IEEE 802.11b
✖	Wafaos	no signal	00:09:5B:3F:3D:33	N/A	IEEE 802.11b
✖	Homenet	no signal	00:0A:95:F1:9C:75	N/A	IEEE 802.11b
✖	HACKME	no signal	00:09:5B:9C:CE:46	N/A	IEEE 802.11b
✖	mouthbreathers	no signal	00:06:25:E5:FC:E1	N/A	IEEE 802.11b

Parameter Value

- SSID: xyzyz
- AP MAC: 00:06:25:00:06:25
- Vendor: The Linksys Group, Inc.
- WEP: OFF
- Rates: 1,2,5,11
- Standard: IEEE 802.11b
- RSSI: -45/-36 (dBm)
- Channel: 6
- Network Type: Direct Sequencing
- Mode: Infrastructure
- Beacon Period: 100 (Kusec)
- ATIM Window: 0 (Kusec)
- DHCP: 10.100.25.2
- DHCP MAC: 04:01:D3:C1:6B:42
- DNS: 10.100.60.60
- Gateway: 10.100.60.1
- Applied IP: 10.100.60.21
- AP IP: 10.100.60.43
- Domain: main.gov

Copyright © 2004 eEye Digital Security All right Reserved.

eEye Digital Security

Ready NUM

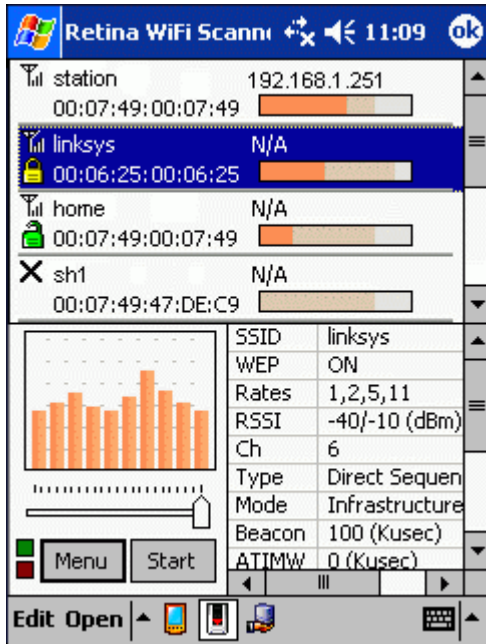
The Discover tab is used to setup and scan devices. The controls on the Discover tab are divided between the **Actions** and the **Detected Devices** panes. **Actions** selections are used to control scanning and **Detected Devices** is used to display information.

Actions:

- **Scan**—Used to start and stop scans.
- **WiFi Options**—Sub-tab used for setting wireless scanning options. These are discussed in the **WiFi Options** section of the manual.
- **IP Options**—Sub-tab used to setting options related to TCP/IP.

Detected Devices

- A list of detected wireless devices and a summary of the discovered information. These are discussed in detail in the next section.
- A graph of signal history
- A list box, to the right of the graph, containing detailed information about the selected wireless device.



Instead of Discover and Report tabs, the Pocket PC has a main screen as shown in Figure 1. This screen has a **Menu** button that will bring up the screens listed later in this document and a **Start** button that starts scanning.



Figure 1: Pocket PC

List of detected wireless devices

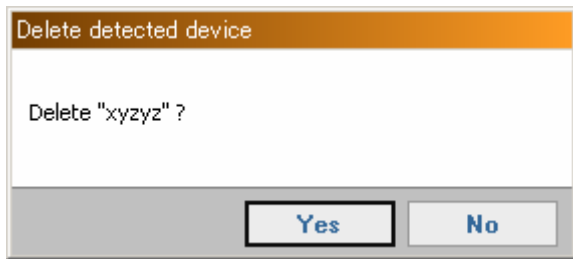
Status	SSID	RSSI	AP MAC	AP IP	Standard
📶 (🔒)	linksys	-36 (dBm)	00:0C:41:00:0C:41	192.168.10.1	IEEE 802.11g

Columns

- **Status**
 - 📶 Signal is alive
 - ✕ Signal is dead
 - 📶(🔒) Detected device is in infrastructure mode (access point)
 - 📶(📶) Detected device is AdHoc mode
 - 📶(🔒) Detected device is WEP enabled

- **SSID**—The Service Set Identifier of the device
- **RSSI**—The current and maximum received signal strength level.
 -  Current signal strength. The number at the right is the current signal strength in decibels per milliwatt (dBm)
 -  Maximum signal strength
- **AP MAC**—The MAC address the device
- **AP IP**—The IP address of the device.
- **Standard**—Which standard the device is using (IEEE 802.11b, IEEE 802.11a, IEEE 802.11g)

If you double click the detected device, you can delete it from the list



Detailed Information

The detailed information list box contains the following information for the currently selected device.

Parameter	Value
SSID	xyzzyz
AP MAC	00:06:25:00:06:25
Vendor	The Linksys Group, Inc.
WEP	OFF
Rates	1,2,5,11
Standard	IEEE 802.11b
RSSI	-45/-36 (dBm)
Channel	6
Network Type	Direct Sequencing
Mode	Infrastructure
Beacon Period	100 (Kusec)
ATIM Window	0 (Kusec)
DHCP	10.0.0.2
DHCP MAC	C1:6B:42:C1:6B:42
DNS	10.0.0.6
Gateway	10.0.0.1
Applied IP	10.0.0.5
AP IP	10.0.0.3
Domain	main.gov

- **SSID**—The Service Set Identifier of the device
- **AP MAC**—The MAC address the device
- **Vendor**—The manufacturer name of the device. This name is based on the MAC address.
- **WEP**—Wireless Encryption Protocol (WEP) setting (ON/OFF).
- **Rates**—Supported transmission speeds in megabytes.
- **Standard**—Standard of detected wireless network (IEEE 802.11b/IEEE 802.11a/IEEE 802.11g)
- **RSSI**—Received Signal Strength Indicator. This is shown as "current RSSI/maximum RSSI".
- **Channel**—Channel which is specified on the detected device.
- **Network Type**—The network type in use, "Direct Sequencing" or "Frequency Hopping".
- **Mode**—Infrastructure mode. "Infrastructure" or "IBSS".
- **Beacon Period**—Scanner is sending beacon (IEEE 802.11 beacon frame) to identify the wireless device. This value is the period (Kusec) for sending beacon frame.
- **ATIM Window Period**—ATIM window value (Kusec)
- **DHCP**—IP address of DHCP server, if detected.
- **DHCP MAC**—MAC address of DHCP server, if detected.
- **DNS**—IP address of DNS server (if DHCP server is detected, and DNS server is set in DHCP configuration)
- **Gateway**—IP address of default gateway (if DHCP server is detected, and default gateway is set in DHCP configuration)
- **Applied IP**—The IP address assigned by the DHCP server.

- **AP IP**—The IP address of the access point (if DHCP server and AP IP are both detected)
- **Domain**—Domain name (if DHCP server is detected)

WiFi Options

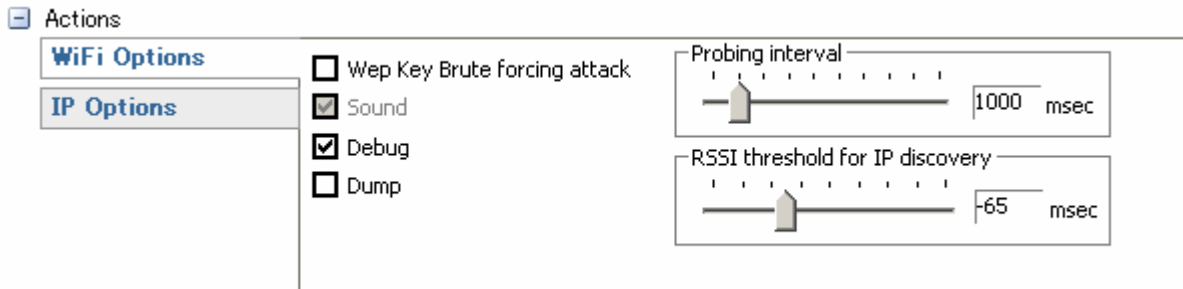


Figure 2: Windows version

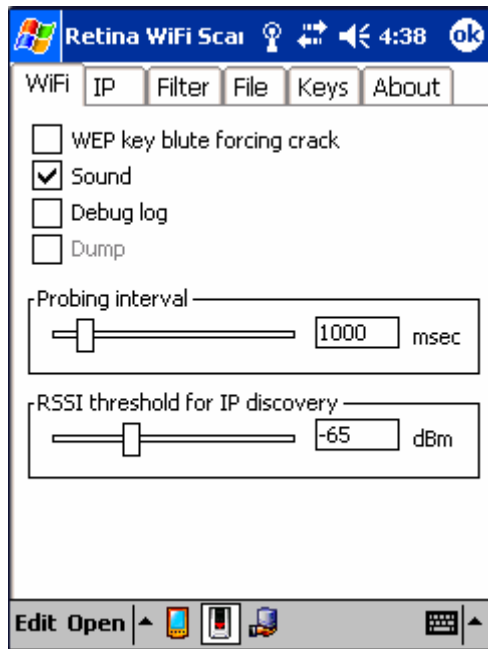


Figure 3: Pocket PC version

- **WEP key brute forcing attack**—Enable/disable WEP brute forcing. If you enable this option, the scanner will try to crack the WEP key based on the dictionary (See, Dictionary) if the WEP is enabled on the detected access points. If the WEP key can be determined, the scanner will attempt to get the IP parameters (See, IP Options).
- **Sound**—Enable/disable the scanner beep that is based on the signal power of the selected wireless device. If the signal power is strong, it makes a rapid high-pitched beep.
- **Debug**—Enable/Disable the debug log. The scanner generates a debug log in "c:\wifidbg.txt" if this option is checked. The log file contains debug information as well as scan results.
- **Dump**—Enable/Disable sending packet dumps to the debug log.
- **Probing interval**—Interval period for sending beacons to detect wireless devices.
- **RSSI threshold for IP discovery**—If the signal strength is low, gathering IP related information might fail. This is the threshold for discovery of IP related information.

IP Options

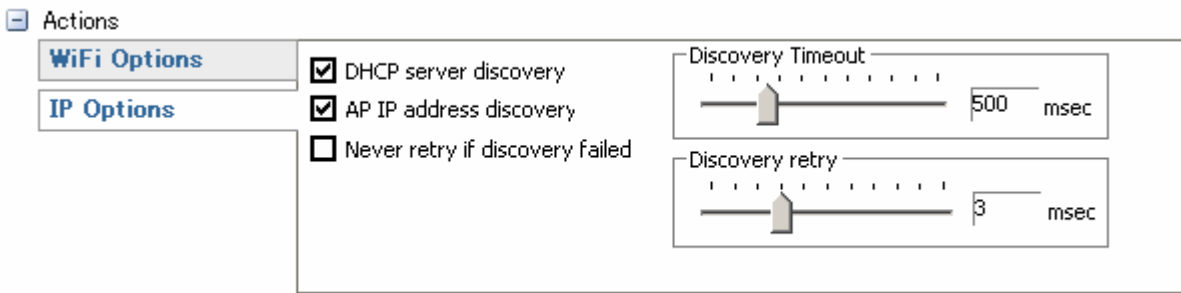


Figure 4: Windows version

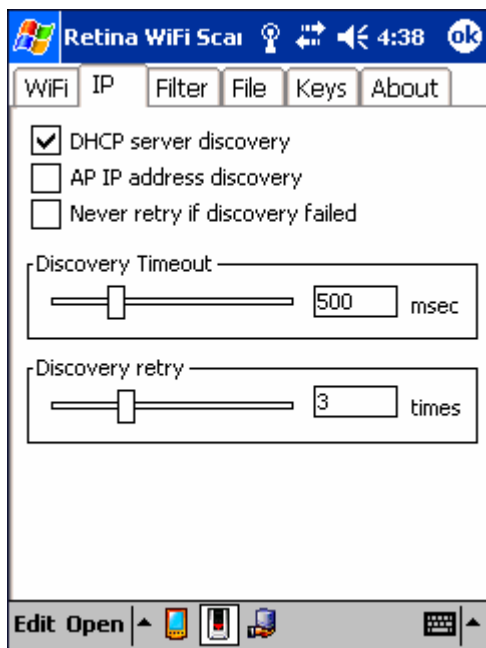
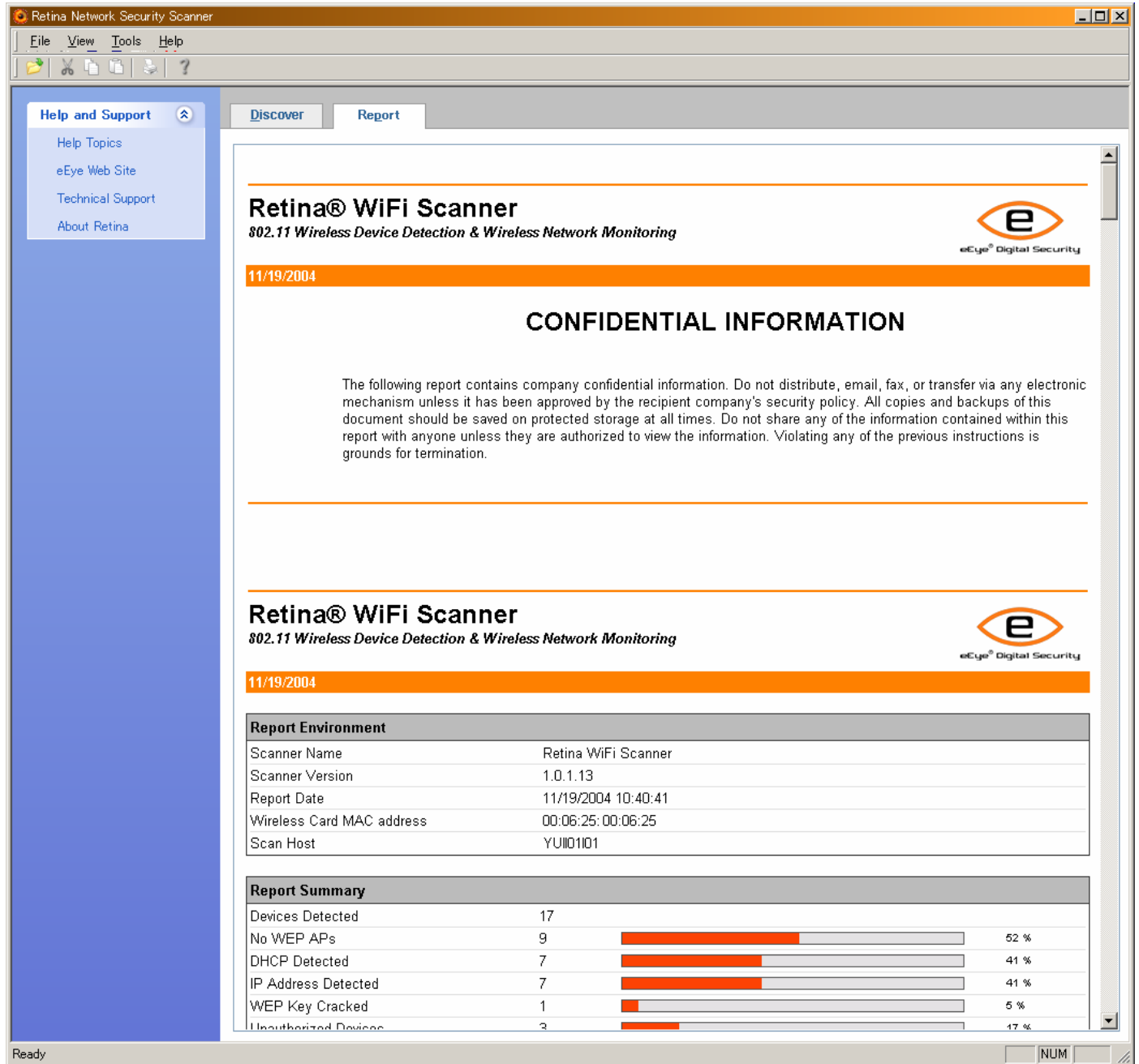


Figure 5: Pocket PC version

- **DHCP server discovery**—Enable/Disable DHCP server discovery. If you enable this option and the scanner can access the DHCP server through the access point, it will collect the following information about the DHCP server:
 - IP address
 - MAC address
 - DNS server (if set in DHCP)
 - Default gateway (if set in DHCP)
 - Domain name (if set in DHCP)
 - Address assigned by the DHCP server.
- **AP IP address discovery**—Enable/Disable the detection of the access point's IP address. The scanner will identify the IP address of the access point using ICMP and ARP. This only works if the DHCP server discovery is also enabled.
- **Never retry if discovery failed**—If **AP IP address discovery** fails, then retries could extend scan times greatly. If you disable the retry, the scan will be much faster.
- **Discovery Timeout**—Timeout value for DHCP and access point IP address detection.

- **Discovery retry**—Number of retries for DHCP and access point IP address detection.

Report



Selecting the **Report** tab generates an HTML-based report on the information gathered. There is no report tab on the Pocket PC version.

Report Summary

Devices Detected—Total number of detected devices

No WEP APs—Number of APs that do not have WEP enabled.

DHCP Detected—Number of networks the scanner was able to detect via the DHCP server.

IP Address Detected—Number of APs on which the scanner could detect the IP address.

WEP Key Cracked—Number of devices on which the scanner was able to determine the WEP key in use.

Unauthorized Devices—Number of devices that are not in the authorized.

Detailed Information

Security Information—Security warning

The following warnings will be shown if detected.

- **WEP Encryption**—WEP Key is not set.
- **DHCP Access**—DHCP Access is available. MAC address filtering is not set.
- **AP IP Access**—IP address of access point is detected.
- **WEP Key Cracking**—The WEP Key is too weak; it can be discovered by a dictionary attack.
- **Unauthorized Device Check**—Unauthorized wireless device.

802.11 Wireless Parameters—IEEE 802.11 related Information gathered from the AP: Vendor, WEP, Rates, Standard, RSSI, Channel, Network Type, Mode, Beacon Period, ATIM Window

IP Parameters—IP information gathered from the DHCP server. Such as: DHCP, DHCP MAC, DNS, Gateway, Applied IP, AP IP, Domain

Menu

File

New—Clear all detected devices.

Open—Open an RWS file. An RWS file contains all information about detected devices.

Save—Save detected devices into an RWS file.

Save As—Save detected devices into an RWS file with a different filename.

Report

- **Text Style**—Save report as text.
- **HTML Style**—Generate report in HTML format and show it using Internet Explorer.
- **XML Style**—Save report as XML format.

Exit—Exit wireless scanner

View—Display or hide the status and explorer bars.

The Pocket PC version has a **File** tab instead of a menu. You can save and load files as well as generate Text, HTML and XML reports.

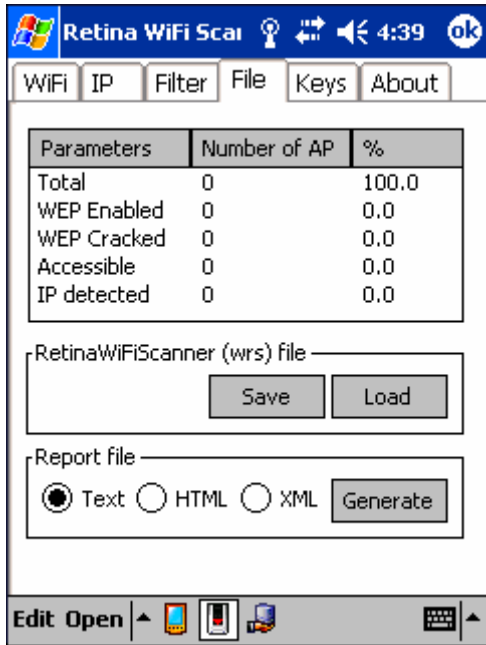


Figure 6: Pocket PC

Tools

Filter—Display the filter configuration dialog box.

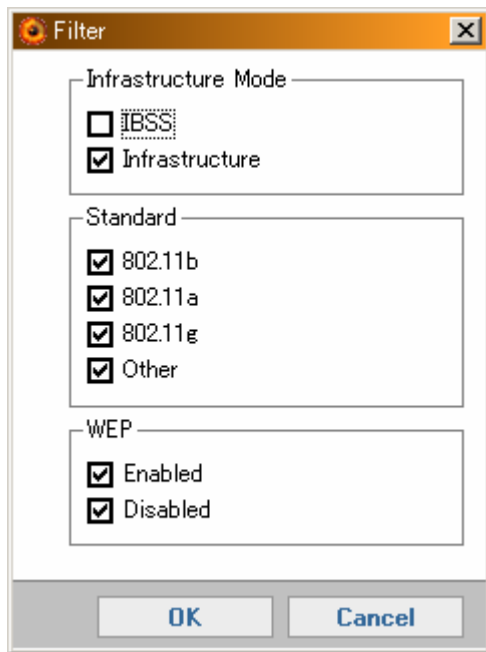


Figure 7: Windows

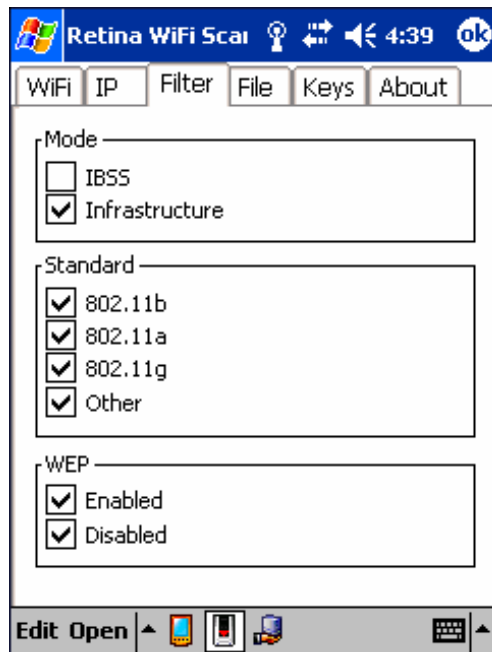


Figure 8: Pocket PC

WEP Dictionary—Display the dictionary editor for WEP brute-forcing attack.

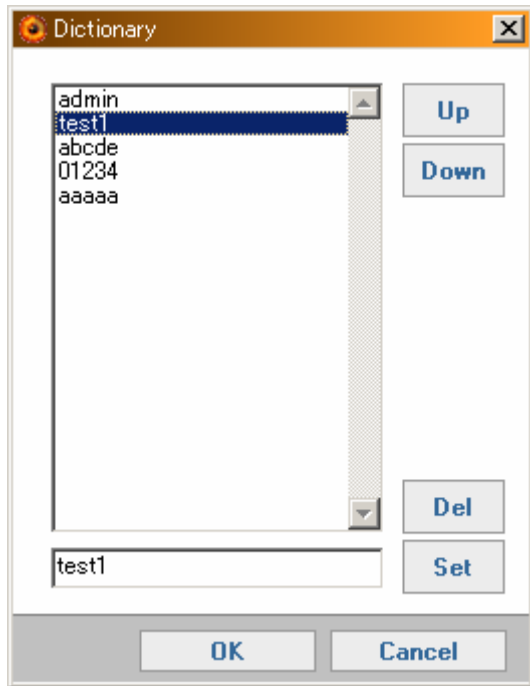
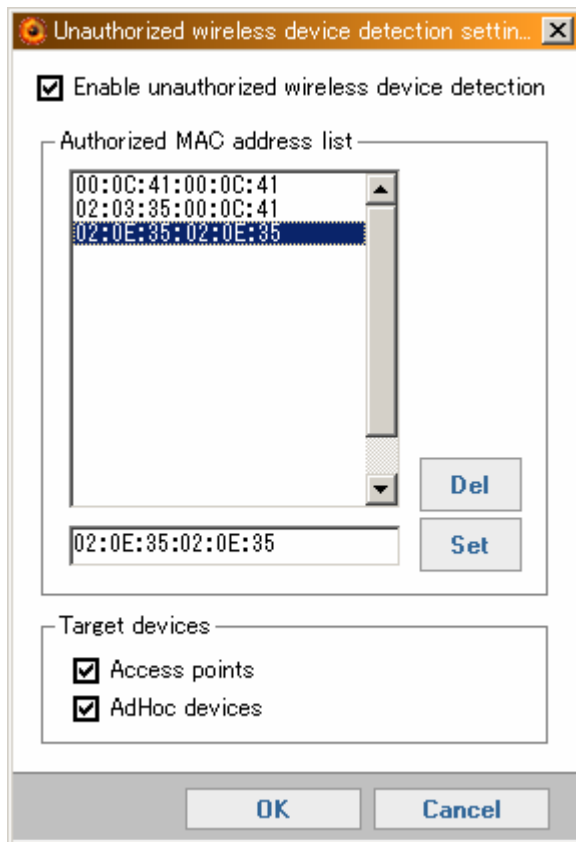


Figure 9: Windows





Figure 10: Pocket PC

Unauthorized wireless device detection—Display the **Authorized MAC address list** dialog box.



You must check the "Enable unauthorized wireless device detection" to enable this feature. You can append the AUTHORIZED devices in "Authorized MAC address list" area. You also can choose what types of devices will be included in the unauthorized wireless detection in the "Target devices" area.

If scanner detects unauthorized devices, the device icons in the status field of detected device list will be following icons.

-  : Unauthorized AP
-  : Unauthorized AdHoc device

If you have Retina and REM is set correctly, this scanner will send the event to REM when unauthorized device is detected.

Figure 11: Windows version