

MiniStumbler v0.4.0 Release Notes

Marius Milner <mariusm@pacbell.net>

Thank you for your interest in MiniStumbler. It is provided to you as a convenience, at no cost and without warranty. If you don't like it, or if you feel that it doesn't quite do what you want, you are free to delete it from your system. By installing or using it, you agree to be bound by the terms of the License Agreement.

MiniStumbler is "beggarware". This means that you do not have to pay for a license to use it. However if you use it and like it, please consider making a donation at <http://www.stumbler.net/donate> to support future development, web hosting and other costs that I incur as a result of making this software available to you. Please bear in mind that I do this as a hobby in my spare time, not as a full time job.

Commercial and Government users are strongly encouraged to donate. The suggested donation is US\$50 per copy. You may donate by visiting the web site <http://www.stumbler.net/donate>. You can pay in a variety of ways and may send a Purchase Order if needed.

What is MiniStumbler?

MiniStumbler is a tool for Windows CE that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses:

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for WarDriving.

Requirements

General Requirements

The requirements for MiniStumbler are somewhat complex and depend on hardware, firmware versions, driver versions and operating system. The best way to see if it works on your system is to try it.

Some configurations have been extensively tested and are known to work. These are detailed at <http://www.stumbler.net/compat>. If your configuration works but is not listed, or is listed but does not work, please follow the instructions on the web site to report it.

The following are rules of thumb that you can follow in case you cannot reach the web site for some reason.

- This version of MiniStumbler is known to work on HPC2000, PocketPC 3.0, PocketPC 2002 and Windows Mobile 2003.
- The Proxim models 8410-WD and 8420-WD are known to work. The 8410-WD has also been sold as the Dell TrueMobile 1150, Compaq WL110, Avaya Wireless 802.11b PC Card, and others. Some of these cards do not come with drivers for Windows CE; for these you can install the ORiNOCO driver, insert the card, and enter wlluc46 as the driver name to use. For these cards you must have driver version 7.X or better. The 6.X drivers cannot be used.
- The Dell Truemobile 1180 CF card works.
- Many cards based on the Intersil Prism/Prism2 chip set also work. This includes the Socket SDIO 802.11b card and the built-in wireless on the Toshiba e740, and others.
- I cannot help you figure out what chip set is in any given card.

Other Requirements and Compatibility Issues

- Your card must be configured in such a way that it can be seen by the management software that came with the card.

- If using a GPS receiver, please make sure that you are able to use other GPS-capable applications with it before reporting problems.
- When MiniStumbler is in "auto reconfigure" mode (the default), it will occasionally disconnect you from your network. This enables it to perform its scans accurately, and is not a bug.
- If you have the WLAN card configured to connect to a specific SSID, MiniStumbler may not report any access points other than those that have that SSID. Configure your card with a blank SSID or, if a blank one is not permitted, "ANY" (without quotes).

Legal Note

I am not a lawyer. However as a user of this software, you need to be aware of the following.

In most places, it is illegal to use a network without permission from the owner. The definition of "use" is not entirely clear, but it definitely includes using someone else's internet connection or gathering information about what is on the network. It may include getting an IP address via DHCP. It may even include associating with the network.

The IP address reporting functionality in MiniStumbler (only available on PocketPC and Windows Mobile 2003) is for you to check the settings of your own network, and for corporate users to identify rogue access points operating within their organization. If you are doing neither of these things, it is suggested that you disable TCP/IP on your wireless adapter. This will help you to avoid possible legal trouble.

Marius Milner, NetStumbler.com and stumbler.net accepts no liability for damages caused by use of this software. For further information please consult the License Agreement that can be found both in the installer and on the www.stumbler.net web site.

File Formats

MiniStumbler uses the same .NS1 file format as NetStumbler.

- The files that you create using MiniStumbler 0.4.0 can be read by NetStumbler 0.4.0 and above.
- MiniStumbler can read NS1 files created by NetStumbler 0.4.0 and below.
- MiniStumbler can read NS1 files created by MiniStumbler 0.3.23.
- NOTE: MiniStumbler cannot read any of the text formats exported by NetStumbler.

Mini-FAQ

Q1: MiniStumbler reports "No wireless card found". Why?

A1: Please check the compatibility lists above. Perhaps your adapter is not supported.

Q2: Why doesn't MiniStumbler see the access point right next to my device?

A2a: The access point is configured not to respond to broadcast probes. Most manufacturers call this "disable broadcast SSID" or "closed". MiniStumbler cannot see these networks unless you know the SSID and have your device configured to connect to it.

A2b: Your wireless card is configured to connect to a specific SSID. Try setting it to connect to a blank SSID or to "ANY" (without quotes).

Q3: What 802.11 frames does MiniStumbler send?

A3a: It sends out a probe request about once a second, and reports the responses. This is known as Active Scanning.

A3b: (ORiNOCO only and with "Query APs for names" enabled) When it is connected to a BSS network, it will attempt to get the name of the access point. When it is connected to an IBSS network, it will try to get the names of all locally visible peers. This is done via Proxim's proprietary WMP protocol.

A3c: (Only when connected to a Cisco access point and with "Query APs for names" enabled and with a valid IP address) It will attempt to use Cisco's IAPP protocol to get the name and IP address of the access point.

A3d: If you leave TCP/IP enabled, your adapter may attempt to get a DHCP lease or send other traffic. MiniStumbler will record the fact that you were issued an IP address.

Q4: Does MiniStumbler listen for beacons, or put my card into promiscuous or RFMON mode?

A4: This is called Passive Scanning and is not in this version.

Q5: I'm seeing access points appear briefly and then disappear for a long time. What's happening?

A5a: Some wireless networks can be configured not to respond to probes every time they hear a request.

A5b: If you see lots of networks that appear briefly and then disappear forever, you may have found a FakeAP installation.

Q6: Why does MiniStumbler disconnect me from the network?

A6: If you have "Options->Reconfigure card automatically" checked, it will configure your card with a profile that uses a null SSID and BSS mode (It will not change your WEP settings). Also, when it sees another network that has a better signal than the one you're connected to, it may disconnect the

current connection so that it can get the AP name on the other network.

Q7: Does MiniStumbler detect ROR and COR installations?

A7: Not usually. They are not always fully compliant with 802.11b and therefore may not be visible to NetStumbler.

Q8: When will you support wireless card / device X? When will you add new feature Y that I want?

A8: I work on this in my spare time. I can make no commitment to dates for new features or bug fixes. If you would like to help me support a particular piece of hardware, please consider sending me a sample rather than complaining that it isn't supported.

Q9: What does "Auto Reconfigure" actually do?

A9a: When using the ORiNOCO driver, it stops the Wireless Zero Configuration service and makes sure that the card is always set to a blank SSID and BSS mode.

A9b: When using the Prism driver, it stops the Wireless Zero Configuration service and checks for a blank or "ANY" SSID. If necessary, it makes changes to the card's registry settings and prompts you to reinsert the card.

Release History

Version 0.4.00 (April 21, 2004):

- Support for Atmel and Intersil Prism2 based wireless cards.
- Allow use of Serial Earthmate GPS.
- If you connect to a network that supports DHCP, the IP subnet is reported.

- If the access point is discovered in the ARP table, its IP address is reported.
- A whole lot of new Scripting features.
- Allow configuration of baud rate and other settings for GPS.
- Close connection to NIC when scanning is not happening.
- Support for HPC2000.
- Moved much of the configuration to a dialog box.
- Support for user-provided scripts to be invoked when various events occur. Note: you may not have scripting available on your system.
- Toolbar buttons now indicate state accurately.
- ORiNOCO errors reported properly.
- When you select an invalid COM port for GPS, it no longer locks up the system.

Version 0.3.23 (February 14, 2002):

- Count of filtered and all APs in bottom right corner.
- Handle "ASTRAL" on serial port so that Tripmate can be used.
- Autosave feature added.
- Popup menu allows deletion of APs from list.
- Complete rewrite of NIC access code in preparation for multiple chipset support.
- First public release. No tree or graph view.