

CommView[®] for WiFi PPC

Wireless Network Monitor and Analyzer for Pocket PC

Help Documentation

Copyright © 2005-2006 TamoSoft

Introduction

About CommView for WiFi PPC

CommView for WiFi PPC is a special lightweight edition of CommView for WiFi that runs on Pocket PC handheld computers. This product is a cost-effective WLAN diagnostic solution designed for express wireless site surveys, as well as capturing and analyzing network packets on wireless 802.11b/g networks. CommView for WiFi PPC gathers information from the wireless adapter and decodes the analyzed data.

With CommView for WiFi PPC, you can scan the air for WiFi signals, select channels for monitoring, detect access points and wireless stations, capture packets, measure signal strength, view the list of network connections, and examine and filter individual packets. If the packets are WEP-protected, you can decrypt them on-the-fly by entering the correct WEP key.

Wireless network administrators can use this portable solution as a source of important information on network parameters, radio interference, security holes, or rogue access points; all of which are necessary for the deployment and maintenance of WLANs. Although CommView for WiFi PPC is a full-fledged packet monitor and analyzer, it is often feasible to use it in conjunction with the [standard CommView for WiFi edition for Windows 2000/XP](#) for far more sophisticated tools for network traffic analysis. The most efficient way to use CommView for WiFi PPC is to perform express traffic monitoring and analysis, and then conduct in-depth research using CommView for WiFi on your Windows 2000/XP notebook computer.

This application requires a compatible wireless network adapter. For the list of supported adapters, please visit our [Web site](#).

License Agreement

Please read the following terms and conditions carefully before using this software. Your use of this software indicates your acceptance of this license agreement. If you do not agree with the terms of this license, you must remove this software from your storage devices and cease to use the product.

Copyright

This software is copyrighted 2005-2006 by TamoSoft. CommView is a registered trademark of TamoSoft. The use and copyright of this software are governed by international copyright treaties. TamoSoft retains full title and rights to this software and documentation, and in no way does the license granted diminish the intellectual property rights of TamoSoft. You must not redistribute the registration codes provided--on paper, electronically, or in any other form.

Evaluation Version

This is not free software. You are hereby licensed to use this software for evaluation purposes without charge for a period of 30 days. Using this software after the evaluation period violates copyright laws and may result in severe civil and criminal penalties.

Registered (Licensed) Version

One registered copy of this software may be used by a single person who uses the software personally on one or more computers, or it may be installed on a single workstation used non-simultaneously by more than one person, but not both. This software may be installed on a network server, provided that a separate, appropriate license to use this software has been granted by TamoSoft for each computer terminal having access to this software.

Upgrades

This Agreement does not grant you any right to any enhancement, updates, or upgrades for this software (collectively, "upgrades"). TamoSoft may or may not, at its sole discretion, offer such upgrades to licensed users. TamoSoft does not warrant that such upgrades will be available, or that such upgrades will offer any enhancements in compatibility with the latest industry standards, including, but not limited to, new hardware devices, network protocols, or encryption algorithms.

Disclaimer

TAMOSOFT DOES NOT WARRANT THAT THE PRODUCT IS ERROR FREE. THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL TAMOSOFT BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS.

Governing Law

This Agreement will be governed by the laws of New Zealand.

Distribution

This software may be distributed freely in its original unmodified and unregistered form. The distribution must include all files of its original distribution. Distributors may not charge any money for it. Anyone distributing this software for any kind of remuneration must first [contact us](#) for authorization.

Other Restrictions

You may not modify, reverse engineer, decompile or disassemble this software in any way, including changing or removing any messages or windows.

Using the Program

Installation

CommView for WiFi PPC Installation Instructions

Prior to installing CommView for WiFi PPC, please make sure that your wireless adapter is compatible with this product. Please read about the WiFi adapter compatibility in the Driver Installation Instructions section below.

Download the program installation file from our Web site to your PC.

Follow the process outlined below:

Step 1: Connect Your Handheld

Make sure your Pocket PC device is in its cradle and that a connection to your desktop computer has been established with ActiveSync.

Step 2: Run the Installer

On your desktop computer, locate the CommView for WiFi PPC installation file that you downloaded. Double-click the file to begin the installation.

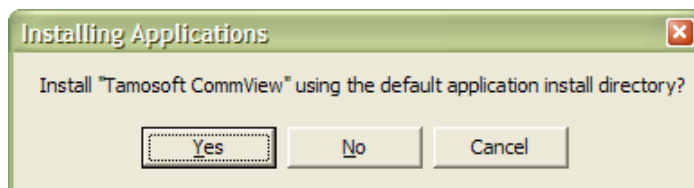
You will see a Welcome Screen. Click **Next** to continue.

You will be presented with a License Agreement Screen. Please read the CommView for WiFi PPC License, and then indicate that you accept the license, and click **Next** to continue.

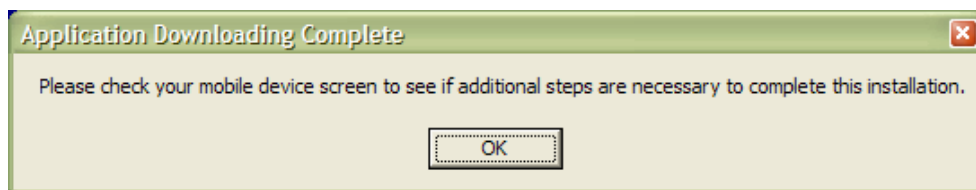
The installer will copy some files that are necessary to perform the installation of CommView for WiFi PPC to your Pocket PC device.

Step 3: Files Install to Your Device

While the CommView for WiFi PPC files are being copied to your device, you will see a dialog like this:



When this stage is complete you will see the following dialog:



Click OK and turn to your Pocket PC device. CommView for WiFi PPC installation is complete.

Step 4: Start CommView for WiFi PPC

To begin using CommView for WiFi PPC, look for its icon (a Pocket PC and antenna on yellow background) on your Start Menu, or under **Start => Programs** tap the icon to start CommView for WiFi PPC.

CommView for WiFi PPC is a tool for monitoring wireless 802.11b/g networks. To use this product, you **must** have a compatible wireless adapter. To enable the monitoring features of your wireless adapter, you will need to use the special driver that comes with this product. The instructions below will guide you through the driver installation process.

Please note that once the driver has been replaced, your adapter will no longer be able to communicate with other wireless hosts or access points, because the driver uses a passive monitoring mode. To restore the standard functions of your adapter, you would need to uninstall the CommView for WiFi driver (click **Uninstall** in **File=>Options=>Drivers**) and restart your Pocket PC. Please note that you must reset your Pocket PC by using the Reset button—turning it on and off is not sufficient.

Prior to installing the new driver for your wireless adapter, be sure that your adapter is compatible with this product. The list of compatible adapters can be found at the following URL:

<http://www.tamos.com/products/commwifippc/>

Driver Installation Instructions

Install the wireless adapter as per the manufacturer's instructions.

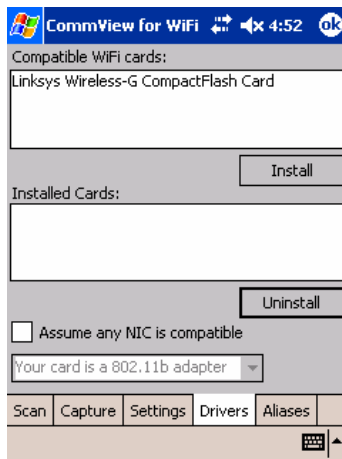
Insert the adapter and make sure that it provides network connectivity.

Launch CommView for WiFi PPC and choose **File=>Options=>Drivers**.

Select the desired wireless adapter from the list at the top of the screen (compatible WiFi cards section) and click on the Install button.

When you see the messages prompting you to restart the computer, do so. **Please note that you must reset your Pocket PC by using the Reset button, as turning it on and off is not sufficient.**

The program is ready for use. You can verify this by opening **File=>Options=>Drivers** and making sure that the correct adapter is listed in the Installed Cards section with the [CommView] prefix, and it is selected for monitoring in the **File=>Options=>Settings** screen.



If you would like to use a card that is not included in our list of compatible adapters, you can use the "**Assume any NIC is compatible**" option.

Important Note: Use this option at your own risk. We do not guarantee that your NIC will work after the driver is installed.

For better matching of the driver please specify your adapter band in the corresponding drop-down list. Use the arrow keys or scrolling wheel of your Pocket PC for item selection. The rest of the driver installation process is similar to the driver installation for a supported NIC.

Overview

The program interface allows you to view data and perform various actions with captured packets using the menu at the bottom of the screen. To start capturing packets, select the wireless adapter for monitoring in the **File=>Options=>Settings** screen and then click **File=>Start Capture** in the menu.

Main Menu

File

Scan channels - opens the Scanner screen and starts scanning WiFi channels

Capture - starts/stops capturing packets

Save packet - saves the selected packet

Save all packets - saves all packets in the buffer

Clear packets - clears the contents of the program's buffer and the packet list

Clear statistics - clears the IP statistics

Options - opens the program configuration menu

Exit - closes the program

Clicking **Stats** opens the IP Statistics screen that displays detailed information about WLAN connections.

Clicking **Packets** opens the Packets screen that lists all captured packets.

Clicking **Rules** opens the screen where you can configure traffic capturing rules.

Help

Contents - launches CommView for WiFi PPC help

Register - opens the program registration dialog

About - shows the information about the program

Many interface elements have context-sensitive menus that can be invoked by pressing the stylus against the interface element and holding it, and many commands are available only through these menus.

The **Stats** screen is used for displaying detailed information about WLAN network connections (IP protocol only). For more information see [Stats](#).

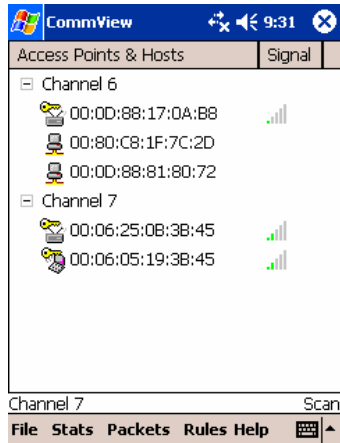
The **Packets** screen is used for viewing captured network packets and displaying detailed information about a selected packet. For more information see [Packets](#).

The **Rules** screen is for configuring rules that allow you to capture/ignore packets based on various criteria, such as IP address or port number. For more information see [Rules](#).

You can configure the scanning, capturing and other options by tapping **File=>Options**.

Scanner

The **Scanner** screen allows you to scan the air for WiFi signals and select a channel to monitor. To start scanning, choose **File=>Scan channels**. The scanning process is cyclic, i.e. the program will "listen" for signals on the first channel, then switch to the next channel and so forth, until it reaches the last channel, after which a new scanning cycle will begin. The scanning process will not stop until the **Scan channels** menu item is unchecked.

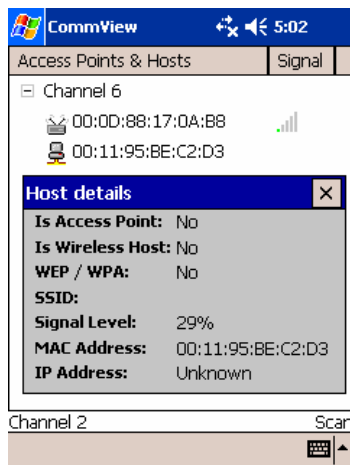


The meaning of the table columns is explained below:

Access Points & Hosts - MAC addresses of the access points and stations. The icon next to the MAC address represents the node type. A box with two antennas is an access point; a notebook represents a station in the infrastructure or the ad hoc mode. The golden key is shown when data encryption is being used.

Signal - signal level in graphical form. The more green bars that are in the picture, the stronger the signal.

When the **scanner** screen is populated, you can obtain brief information about a discovered wireless host by tapping on it.



To clear the data that has been collected, hold down the stylus on the word **Channel** and select **Reset** from the pop-up menu. When you are done with scanning and/or if you know the channel on which you want the program to capture packets, click **File=>Capture** and select the channel number from the drop-down list. You can also hold down the stylus on the desired channel from the list of channels in the **Scanner** screen and select **Capture** from the drop-down menu. Click **File=>Options=>Scan** to configure a number of scanning options:

Reset data after each cycle - check this box if you would like the program to clear all the data it has collected before beginning a new scanning cycle. This option has both drawbacks and advantages. The advantage is that resetting the data will give you the most up-to-date picture of the air. For example, if a certain station no longer sends data, it will not show up on the list again. However, the drawback is that if a certain station does not send data actively, e.g. it does so just a few times per minute, the scanner may not "notice" the station each time it scans a certain channel. Furthermore, this station will be removed from the list.

Capture data while scanning - check this box if you would like the program to display the packets being captured during scanning in the **Packets** and **Stats** screens. If this box is not checked, the packets that are captured while the scanner is working will not be displayed.

Hide wired hosts - check this box if you would like the program to show only wireless hosts and access points. If this box is not checked, the scanner will show both wireless and wired hosts in the segment being scanned. Note that enabling this option may sometimes hide wireless hosts, as the program needs to capture several data packets to determine if a host is wired or wireless.

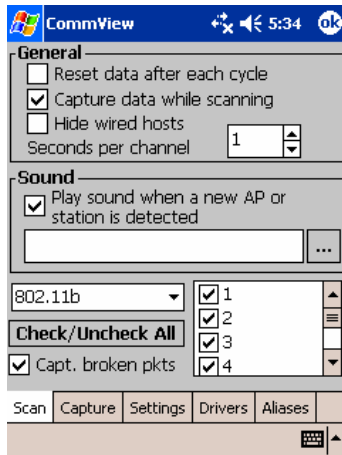
Seconds per channel - determines the time interval the scanner will listen for data on each scanned channel before moving to the next one.

Play sound when a new AP or station is detected - check this box and select a .WAV file if you want the program to notify you about access points or stations it has found.

Band – allows you to select the band (currently the 802.11b/g bands are supported).

Capt. broken pkts - check this box if you would like the program to capture and display packets that contain partly or fully invalid data.

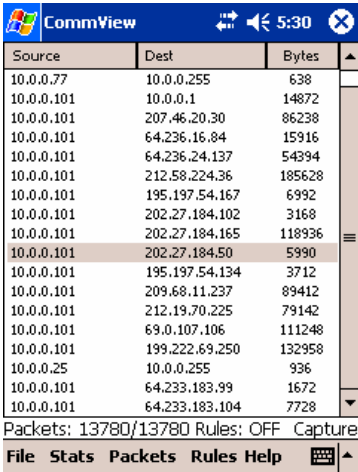
If you already know what channels you would like to monitor, leave the checkmarks only against those channels.



The radio used in a wireless adapter can receive data on only one channel at a time. When you have selected a certain channel for monitoring, the table will display the information on the nodes transmitting data on the selected channel only. You can, however, select a different channel and restart capturing at any time without resetting data in the table, or even let the Scanner sweep through the channels so that you can see active nodes on different channels (be sure to check the **Capture data while scanning** box in the Scanner options).

Stats

This screen is used for displaying detailed information about WLAN connections (IP protocol only). To start capturing packets, select **File=>Capture** in the menu. Please note that this page will **not** be populated unless the program is capable of decrypting WEP-encrypted WLAN traffic. WPA decryption is not supported in the current version; so WPA-encrypted connections will not be displayed. If your WLAN uses WEP encryption, all the data packets being sent are encrypted, and it is impossible to obtain information about their IP address unless you have entered the correct WEP key(s). To enter your WEP key(s), select **Settings=>Options**, go to the **Capture** page, check the **Decode WEP** checkbox, select the WEP key length (64 and 128 bit keys are supported) and enter it in the field below. The key should be entered as a hexadecimal string that is 10 or 26 characters long correspondingly. Check the **Ignore CRC err.** checkbox if you would like the program to ignore CRC errors while deciphering WEP.



Source	Dest	Bytes
10.0.0.77	10.0.0.255	638
10.0.0.101	10.0.0.1	14872
10.0.0.101	207.46.20.30	86238
10.0.0.101	64.236.16.84	15916
10.0.0.101	64.236.24.137	54394
10.0.0.101	212.58.224.36	185628
10.0.0.101	195.197.54.167	6992
10.0.0.101	202.27.184.102	3168
10.0.0.101	202.27.184.165	118936
10.0.0.101	202.27.184.50	5990
10.0.0.101	195.197.54.134	3712
10.0.0.101	209.68.11.237	89412
10.0.0.101	212.19.70.225	79142
10.0.0.101	69.0.107.106	111248
10.0.0.101	199.222.69.250	132958
10.0.0.25	10.0.0.255	936
10.0.0.101	64.233.183.99	1672
10.0.0.101	64.233.183.104	7728

Packets: 13780/13780 Rules: OFF Capture

File Stats Packets Rules Help

The meaning of the table columns is explained below:

Source, Dest – shows the pair of IP addresses between which the packets are being sent.

Bytes – shows the number of bytes transmitted during the session.

Menu Commands

Holding down the stylus on the Stats list brings up a menu with the following commands:

Add source IP alias – brings up a window where you can assign an easy-to-remember alias to the source IP address from the selected pair of addresses.

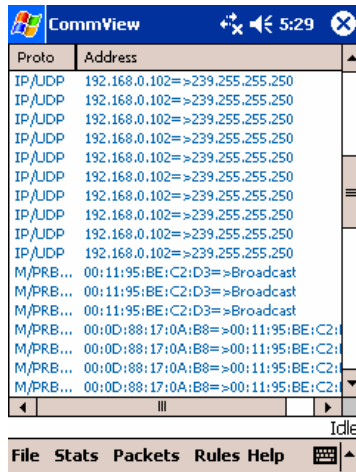
Add dest. IP alias – brings up a window where you can assign an easy-to-remember alias to the destination IP address from the selected pair of addresses.

Font – allows you to select the font size.

The **Stats** screen can be cleared by clicking **File=>Clear statistics**.

Packets

This tab is used for listing all captured network packets and displaying detailed information about a selected packet.



Proto	Address
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
IP/UDP	192.168.0.102=>239.255.255.250
M/PRB...	00:11:95:BE:C2:D3=>Broadcast
M/PRB...	00:11:95:BE:C2:D3=>Broadcast
M/PRB...	00:11:95:BE:C2:D3=>Broadcast
M/PRB...	00:0D:88:17:0A:B8=>00:11:95:BE:C2:D3
M/PRB...	00:0D:88:17:0A:B8=>00:11:95:BE:C2:D3
M/PRB...	00:0D:88:17:0A:B8=>00:11:95:BE:C2:D3
M/PRB...	00:0D:88:17:0A:B8=>00:11:95:BE:C2:D3
M/PRB...	00:0D:88:17:0A:B8=>00:11:95:BE:C2:D3

The table displays the list of captured packets. Use this list for selecting a packet that you want to have displayed and analyzed. When you select a packet by tapping on it, the information about the selected packet will be displayed.

The meaning of the table columns is explained below:

Proto – shows the packet's protocol.

Address – shows the source and destination IP addresses of the packet or the MAC addresses if the IP addresses are not available.

The packet output can be suspended by clicking **File=>Options** and checking the **Suspend packet output** checkbox in the **Capture** screen. In the Suspended mode, the packets are being captured, but not displayed, on the **Packets** screen. This mode is useful when you are interested only in the statistics rather than individual packets. To resume real-time packets display, uncheck the **Suspend packet output** checkbox.

Menu Commands

Holding down the stylus on a packet in the list brings up a menu with the following commands:

Decode – displays decoded packet information for the selected packet. This information includes vital data that can be used by network professionals. You can navigate between packets by clicking the **Previous** or **Next** buttons. Clicking on the **View as HEX** button will display the raw contents of the packet.

Hex dump – displays the raw contents of the packet, both in hexadecimal notation and as plain text. In the plain text, non-printable characters are replaced with dots. You can navigate between packets by clicking the **Previous** or **Next** buttons. Clicking on the **Decode** button will display the decoded packet information.

Aliases – brings up a window where you can assign an easy-to-remember alias to the selected MAC address.

Font – allows you to select the font size.

Copy Packet – copies the raw data of the selected packet to the clipboard.

Save – saves the contents of the selected packet to a file in .ncf (CommView native) format. NCF is an open format; please refer to the [CommView Log Files Format](#) chapter in the help file for CommView for WiFi (desktop version) for the detailed NCF format description.

Save all – saves the contents of all packets from the buffer to a file.

Delete – deletes the selected packet.

Delete all – deletes all packets from the buffer.

The **Packets** screen can be cleared by clicking **File=>Clear packets**. If you would like to save all captured packets, check the **Enable** checkbox in the **Auto save packets** section in the **File=>Options, Capture** screen. CommView for WiFi PPC will save all captured packets into the CommAuto.ncf file in the application folder. To remove all saved packets from this file, click on the **Clear** button.

Since CommView for WiFi PPC has restricted packet decoding and analysis capabilities due to the limited Pocket PC resources, it is recommended to save the log files on your Pocket PC and then transfer them to your notebook computer for detailed analysis with the standard version of CommView for WiFi. The standard version of CommView for WiFi decodes over 70 widespread protocols, decrypts WEP and WPA-encrypted packets, displays vital network statistics such as packets per second rate, bytes per second rate, Ethernet protocols, and IP protocols and sub-protocols distribution graphs. It is also capable of reconstructing TCP sessions if all packets required for the particular session reconstruction have been captured.

Rules

CommView allows you to set two types of rules.

The first type (**wireless rules**) allows you to filter packets based on the wireless packet type: **Data**, **Management**, and **Control** packets. You can turn the capturing of these packet types on or off in the **File=>Options, Capture** screen. Additionally, the **Allow capture Beacons** checkbox allows you to switch capturing of beacon packets on and off.

The second type (**conventional rules**) allows you to filter packets based on many criteria, such as port number or MAC address. To use this type of rule, switch to the **Rules** screen of the program's main window. If one or more rules are set, the program filters packets based on the set rules and displays only the packets that comply with these rules.

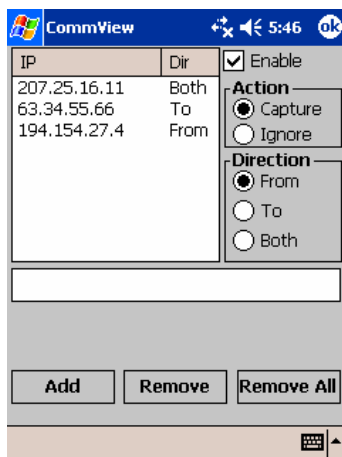
The program's status bar shows if any conventional rules are currently active. Note that it does **not** show if any wireless rules are active. Also note that wireless rules have precedence over conventional rules. Any captured packet must first pass the wireless rules before any further processing takes place. If, for example, none of the four wireless rules are enabled, the program will not display any packets.

You can save your rules configuration(s) to a file and load them by using the corresponding buttons in the **Rules** screen.

Since WLAN traffic can often generate a high number of packets, it is recommended that you use rules to filter out unnecessary packets. This can considerably reduce the amount of system resources consumed by the program. If you want to enable/disable a rule, click on the line with the desired rules type and check or uncheck the **Enable** box. There are five types of rules that can be used:

IP Addresses

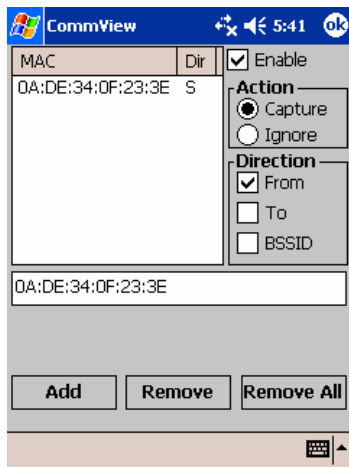
Allows you to ignore or capture packets based on IP addresses. Enter an IP address in the input field, select the direction (**From**, **To**, or **Both**), and click **Add**. The new rule will be displayed. Now you can select the action to be taken when a new packet is processed: the packet can be either captured or ignored.



This example shows how to make the program capture the packets that go to 63.34.55.66, go to and come from 207.25.16.11 and come from 194.154.27.4. All packets that come from other addresses or go to other addresses will be ignored. Since IP addresses are used in the IP protocol, such configuration will automatically make the program ignore all non-IP packets.

MAC Addresses

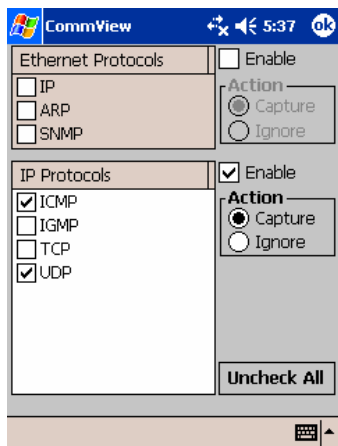
Allows you to ignore or capture packets based on MAC (hardware) addresses. Enter a MAC address in the input field, select the direction (**From, To**) or enter the **BSSID** of the network that you would like to monitor if more than one network is available on the channel, and select the action to be taken when a new packet is processed: capture or ignore, then click **Add**. The new rule will be displayed.



This example shows how to make the program capture packets that come from 0A:DE:34:0F:23:3E. All packets that come from other MAC addresses will be ignored.

Protocols

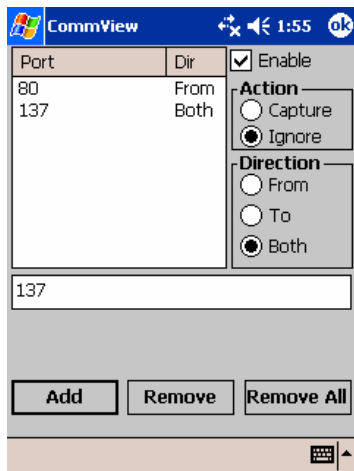
Allows you to ignore or capture packets based on Ethernet (Layer 2) and IP (Layer 3) protocols.



This example shows how to make the program capture only ICMP and UDP packets. All other packets in the IP family will be ignored.

IP Ports

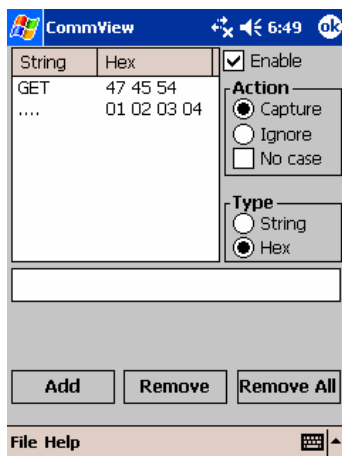
Allows you to ignore or capture packets based on IP (TCP and UDP) ports. Enter a port number in the input field, select the direction (**From**, **To**, or **Both**), and select the action to be taken when a new packet is processed: capture or ignore, and then click **Add**. The new rule will be displayed. Each port rule applies to both TCP and UDP ports.



This example shows how to make the program ignore packets that come from port 80 and go to and come from port 137. This rule will prevent CommView from displaying inbound HTTP traffic, as well as inbound and outbound NetBIOS Name Service traffic. All packets coming to and from other ports will be captured. Please note that the same rules will also apply to UDP ports 80 and 137.

Text

Allows you to capture packets that contain certain text. Enter a text string in the input field, select the type of entered information (String or Hex), select the action to be taken when a new packet is processed: capture or ignore, and click **Add**. The new rule will be displayed. You can enter text either as a string or as a hexadecimal value. The latter method should be used when you want to enter non-printable characters: just type hexadecimal character values separated by spaces.

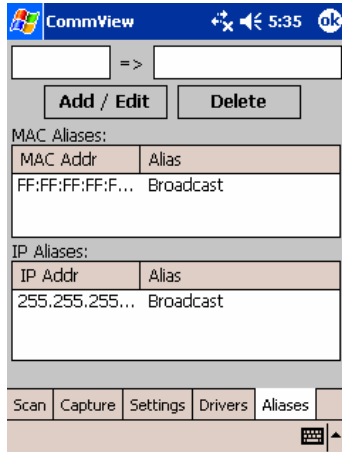


This example shows how to make the program capture only the packets that contain either "GET" or the 01 02 03 04 hex data. Uncheck the **No case** box if you want the rules to be case sensitive. All other packets that do not contain the text mentioned above will be ignored.

Using Aliases

Aliases are easy-to-remember, human-readable names that CommView will substitute for a MAC or IP address when showing the packets on the **Packets** and **Statistics** tabs. This can make packets easier to recognize and analyze. For example, 00:00:19:2D:0D:35 becomes GATEWAY2, and ns1.earthlink.com becomes MyDNS.

You can add aliases to MAC addresses by using the context menu in the **Packets** screen. IP address aliases may be added from the context menu in the **Stats** screen. Alternately, you can click **File=>Options=>Aliases** and enter the MAC or IP address and the alias in the input field manually. The program will determine if an IP address or MAC address alias is being entered. To delete an alias, select it and click **Delete**. To edit an alias, select it and click **Add/Edit**.



Information

How to Purchase CommView for WiFi PPC

This program is a 30-day evaluation version.

A fully functional, unrestricted version of the program can be purchased for US\$69.

Those customers who previously purchased the standard, non-wireless CommView edition or the desktop version of CommView for WiFi are eligible for a considerable discount; please visit our Web site for the details.

A single person who uses the software personally on one or more computers may use one licensed copy of CommView for WiFi PPC, or it may be installed on a single workstation used non-simultaneously by more than one person, but not both. Check our Web site for pricing on multi-user licenses if you need to purchase this product for more than one user.

As a registered user, you will receive:

- Fully functional, unrestricted copy of the software
- Free updates that will be released within 1 year from the date of purchase
- Information on updates and new products
- Free technical support

We accept credit card orders, orders by fax, checks, purchase orders, and wire transfers. Prices, terms, and conditions are subject to change without notice: please check our Web site for the latest product offerings and prices.

<http://www.tamos.com/order/>

Contacting Us

Web

<http://www.tamos.com>

E-mail

sales@tamos.com (Sales-related questions)
support@tamos.com (All other questions)

Mail and Fax

Mailing address:

TamoSoft
PO Box 1385
Christchurch 8140
New Zealand

Fax: +64 3 359 0392 (New Zealand)
Fax: +1 917 591-6567 (USA)

Other Products by TamoSoft

CommView for WiFi

CommView for WiFi is a special edition of CommView designed for capturing and analyzing network packets on wireless 802.11a/b/g networks. It gathers information from the wireless adapter and decodes the analyzed data. With CommView for WiFi, you can see the list of network connections and vital IP statistics and examine individual packets. Packets can be decrypted utilizing user-defined WEP or WPA-PSK keys and are decoded down to the lowest layer, with full analysis of the most widespread protocols. Full access to raw data is also provided. CommView is a helpful tool for network administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's wireless connection or WLAN segment.

[More information](#)

CommView

CommView is a program for monitoring Internet and Local Area Network (LAN) activity capable of capturing and analyzing network packets. It gathers information about data passing through your dial-up connection or Ethernet card and decodes the analyzed data. With CommView, you can see the list of network connections and vital IP statistics and examine individual packets. Packets are decoded down to the lowest layer with full analysis of the most widespread protocols. Full access to raw data is also provided in real time. CommView is a helpful tool for LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's PC or LAN segment.

[More information](#)

CommTraffic

CommTraffic is a network utility for collecting, processing, and displaying traffic and network utilization statistics for network connections, including LAN and dial-up. It shows traffic and network utilization statistics for each computer in the segment. The software provides a very attractive and customizable interface, with an optional tray icon menu that displays general network statistics. You can also generate reports that reflect the network traffic volume and Internet connection expenses (if any). CommTraffic supports virtually any rate plan your ISP might use, such as one based on connection time, traffic volume, time of the day, and other measures. You can set alarms that will inform you when certain criteria (e.g. amount of traffic, expenses) are reached. A configuration wizard will guide you through the setup and automatically detect your network or connection settings.

[More information](#)

SmartWhois

SmartWhois is a handy utility for obtaining information about any IP address, hostname, or domain in the world. Unlike standard whois utilities, it automatically delivers information associated with an IP address or domain no matter where it is registered geographically. In just a few seconds, you get all you want to know about a user: domain, network name, country, state or province, and city. Even if the IP address cannot be resolved to a hostname, SmartWhois won't fail!

[More information](#)

CountryWhois

CountryWhois is a utility for identifying the geographic location of an IP address. CountryWhois can be used to analyze server logs, check e-mail address headers, identify online credit card fraud, or in any other instance where you need to quickly and accurately determine the country of origin by IP address.

[More information](#)

Essential NetTools

Essential NetTools is a set of network tools useful in diagnosing networks and monitoring your computer's network connections. It's a Swiss Army knife for everyone interested in a set of powerful network tools for everyday use. The program includes a NetStat utility that shows your computer's network connections and open ports and maps them to the owning application. It also features a fast NetBIOS scanner, a NetBIOS Auditing Tool for checking LAN security, and a monitor of external connections to your computer's shared resources, as well as a process monitor that displays information about all the programs and services running on your computer. Other useful tools are included, such as Ping, TraceRoute, and NSLookup. Additional features include report generation in HTML, text, and comma delimited formats and a customizable interface. The program is an easy-to-use and powerful replacement for such Windows utilities as nbtstat, netstat, and NetWatcher. It incorporates many advanced features that standard Windows tools can't offer.

[More information](#)

DigiSecret

DigiSecret is an easy-to-use, secure, and powerful application for file encryption and sharing. It utilizes strong and time-proven encryption algorithms for creating encrypted archives, self-extracting EXE files, and sharing files with your associates and friends. DigiSecret also includes powerful and intelligent file compression; you no longer need .zip files when you can have encrypted and compressed DigiSecret files. The program is integrated with the Windows shell, and you can perform operations on files by right-clicking on them. It also fully supports drag-and-drop operations.

[More information](#)