

WEP Key Recovery

Help Documentation

Copyright © 2005-2007 TamoSoft

About WEP Key Recovery

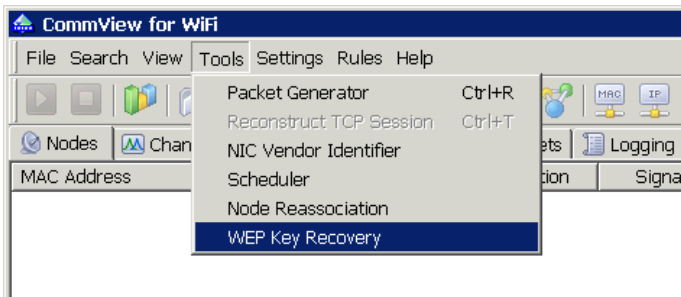
WEP Key Recovery (WEPKR) is an add-on for CommView for WiFi designed for recovering WEP encryption keys for WEP-protected 802.11 a/b/g wireless networks. This application takes advantage of a number of weaknesses found in the WEP encryption algorithm. By analyzing a few hundred thousand data packets captured by CommView for WiFi, WEPKR can obtain a 64-, 128-, 152-, or 256-bit key.

Installation & Requirements

To install WEPKR, simply launch the setup file. WEPKR requires CommView for WiFi 5.2 Build 482 or later and will be installed to the CommView for WiFi application folder. You can also install WEPKR on a computer without CommView for WiFi if you would like to use WEPKR in offline mode, for processing capture files copied from the computer running CommView for WiFi. If you install WEPKR on a computer without CommView for WiFi, you can launch it by double-clicking the program's executable file located in the folder to which you installed it.

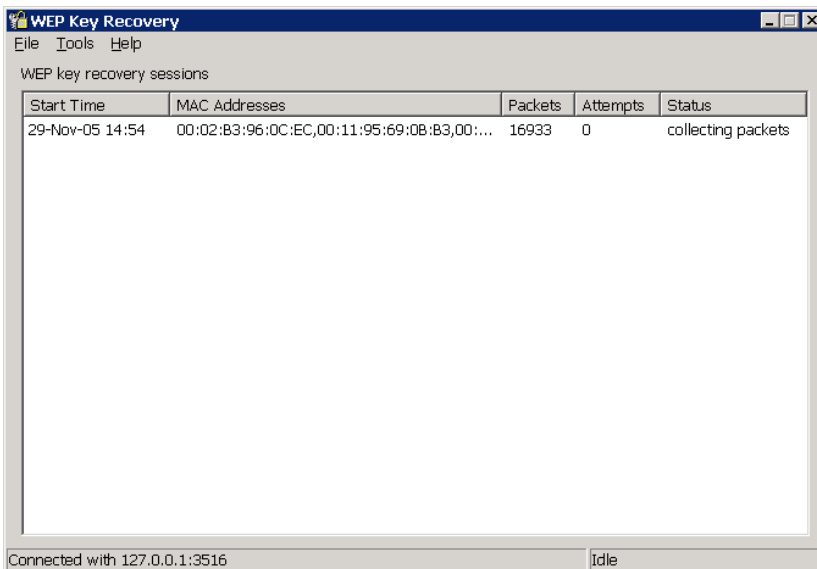
Usage

Once WEPKR has been installed, you can launch it by clicking **Tools => WEP Key Recovery** in the CommView for WiFi menu, as shown below:

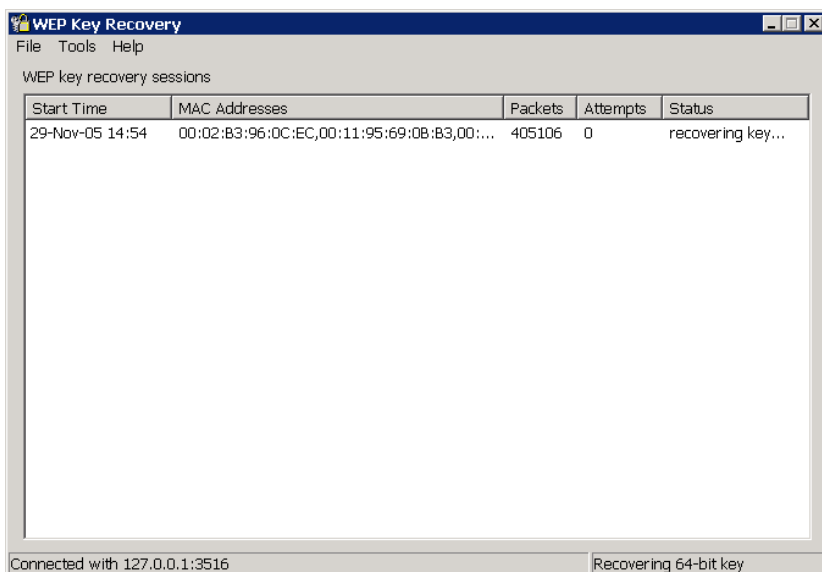


Note that this menu item becomes available only after you've installed WEPKR. When WEPKR is launched, CommView for WiFi establishes a TCP/IP connection with WEPKR so CommView for WiFi can send captured packets to WEPKR for analysis.

The WEP key recovery process starts with collecting the necessary number of data packets. The number of packets required for key recovery depends on the key length and is discussed in detail in the next chapter. To collect the packets, you should capture them using CommView for WiFi, as you normally do. When WEPKR collects a minimum number of packets (10,000 by default) to initiate a new key recovery session, it will display a new line in the main window, as shown below.



The **Start Time** column indicates the time at which a new session was started. The **MAC Addresses** column lists the hardware addresses of the access points and stations involved in the session. The **Packets** column displays the number of usable packets collected during the given session. Please bear in mind that not all captured packets are useable for key recovery; only Data packets are usable, Management and Control packets are not. Additionally, to be usable, the Data packets must have the correct CRC value (i.e. must not be broken), must not have the Retry flag set, and of course, must be WEP-encrypted. Therefore, the number of packets shown in the column will be lower than the number of captured packets as reported by CommView for WiFi. The **Attempts** column shows the number of attempts made to recover the key so far. This value remains zero until the necessary number of packets has been collected by WEPKR. The **Status** column displays the current application status.

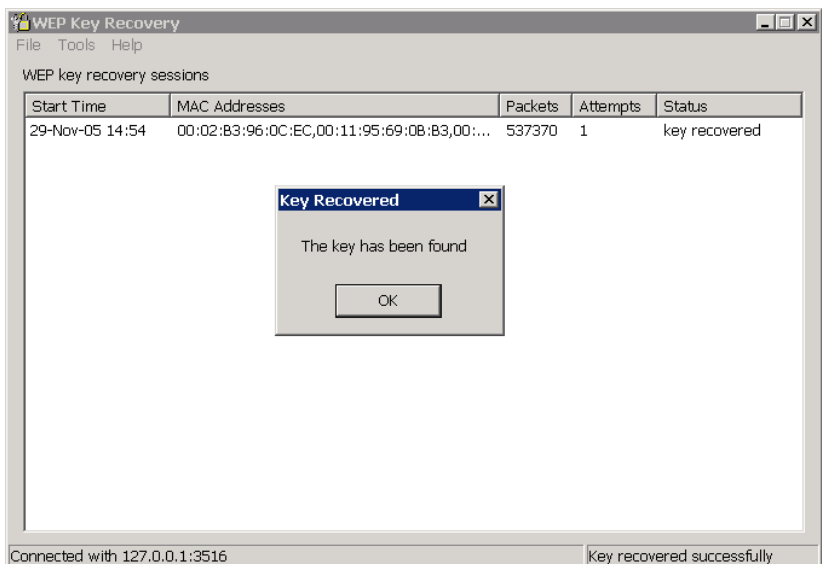


Please note that the collected packets are buffered to a temporary file in a subfolder located in the WEPKR folder. Since you may need over a million packets, make sure that you have sufficient disk space. A million packets occupy about 500 Mbytes.

The key recovery process starts when WEPKR has received the minimum necessary number of usable packets from CommView for WiFi. The packet collection process may take significant time. The time taken is fully dependent on the utilization of the WLAN being monitored. You can, however, artificially increase the WLAN utilization by using the method described in the [Traffic Generation](#) chapter.

After the packets have been collected, the time needed for key recovery varies depending on the number of collected packets (the more packets have been collected the faster the key will be recovered), expected key length, CPU speed, and current CPU utilization. (You may want to stop capturing in CommView for WiFi to decrease CPU utilization.)

The key recovery process on a P4-2800 computer may take anywhere from 2 seconds for a 64-bit key to several hours for 128-, 152-, and 256-bit keys. This largely depends on the particular packets and cannot be predicted. On the average, a 64-bit key is recovered within a few minutes, and a 128-bit key is recovered within half an hour.



The **Action** menu can be used for manually controlling the key recovery process. For example, you may want to start key recovery before the minimum number of packets has been collected, or you may want to stop key recovery and collect more packets for increasing the success probability.

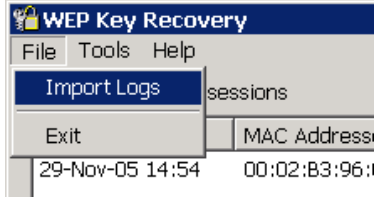
When the WEP key is recovered, the corresponding message will be displayed. Depending on the application configuration (see the [Configuration](#) chapter), WEPKR may decrypt and then "inject" the decrypted packets back to CommView for WiFi. The obtained WEP key can be seen by clicking **Tools => WEP Keys** in the application menu. In evaluation mode, some bytes of the key are replaced by XX. The licensed version displays all the key bytes.

The recovered key can be entered into CommView for WiFi by clicking **Settings => WEP/WPA Keys** in the main menu, after which WEPKR can be closed. Alternatively, you can leave WEPKR running and let it perform the decryption itself. (See the [Configuration](#) chapter for information on how to make WEPKR send packets back to CommView for WiFi.)

WEPKR memorizes recovered keys between launches and tries them first, before attempting to recover them.

Working with Log Files

CommView for WiFi allows you to log captured packets automatically to NCF log files. Using WEPKR, you can process these log files in offline mode. To load NCF files, click **File => Import Logs** in WEPKR, and browse for the logging directory. You can then select one or several NCF files for import.



If the number of packets in these log files is sufficient, the key recovery process will start immediately.

Configuration

To configure WEPKR, click **Tools => Options:**

The screenshot shows the 'Options' dialog box for WEPKR. It is divided into several sections:

- WEP key sizes:** Four checkboxes are present. '64-bit' and '128-bit' are checked, while '152-bit' and '256-bit' are unchecked.
- Session settings:** Two input fields. The first is 'packets needed to start a new session' with the value '10000'. The second is 'session start timeout (mins)' with the value '180'.
- Packets needed to start key recovery:** Four input fields. '64-bit key' is '400000', '128-bit key' is '800000', '152-bit key' is '1000000', and '256-bit key' is '1800000'.
- Port to listen on:** An input field containing '11333'.
- Send decrypted packets back to the application:** An unchecked checkbox.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

WEP key sizes – allows you to specify the expected key size. For every key size, the recovery process must be performed separately. That's why limiting the number of possible key sizes can noticeably reduce the time needed to find the key. If the key size is unknown, you may want to try the most popular key sizes first, 64 and 128 bits. Also, if the AP vendor is known, you can base your assumption on that information, as some vendors don't support all four WEP key sizes. For example, D-Link access points don't support 256-bit keys.

Session settings – allows you to configure WEP recovery session parameters. Use **packets needed to start a new session** to set the minimum number of packets required for initiating packet collection for a new WEP key recovery session. The **session start timeout** field sets a time period for inactivity; if the number of collected packets during that period for the given session is below the number set in the **Packets needed to start key recovery** field, the session is deleted. For WLANs with low utilization, collecting a few hundred thousand packets may take a long time, so you may want to increase the default value.

Packets needed to start key recovery – sets the number of packets required for starting a key recovery process. WEP key recovery is a probabilistic process the result of which largely depends on the number of collected packets; the higher the number, the higher the probability of successful key recovery. The default values ensure about 60% probability of successful key recovery. If you cannot collect the required number of packets, you may want to decrease the default values, but this will also diminish the success probability. If you can easily collect many packets, you may want to increase the default values, as this will speed up key recovery.

Port to listen on – allows you to specify the TCP port that will be used for communicating locally with CommView for WiFi. If the default port (11333) is occupied by another application, you can change the port number.

Send decrypted packets back to the application – if this box is checked, WEPKR will "inject" the packets it has collected so far into CommView for WiFi once the key is recovered. The application uses the following mode of operation:

1. Encrypted WEP packets are captured by CommView for WiFi and passed to WEPKR in real time.
2. When enough packets are collected, WEPKR starts key recovery.
3. When the key is recovered, WEPKR decrypts the packets accumulated in the buffer and passes them back to CommView for WiFi, where they are displayed.
4. All subsequent encrypted packets captured by CommView for WiFi and passed to WEPKR are immediately decrypted and passed back.

This option may be a good choice if you don't log packets in CommView for WiFi, or if you are monitoring several WLANs at the same time. Since CommView for WiFi can use only one WEP key set at any given time, you can use WEPKR for automatic decryption of the data collected from several WLANs that use different WEP keys. Please note that broadcast and multicast packets will NOT be decrypted and sent back to CommView for WiFi, as WEPKR ignores such packets.

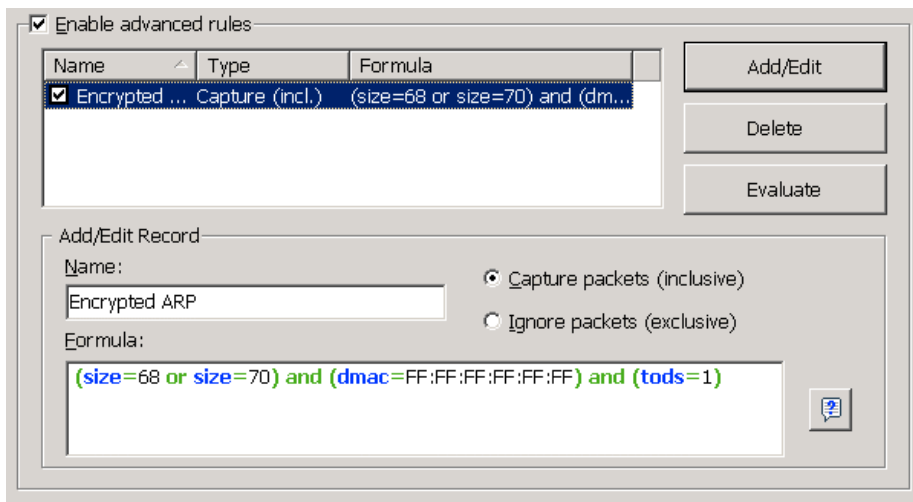
Traffic Generation

In WLANs with low network traffic levels, collecting a few hundred thousand unique packets necessary for key recovery (at least 400,000 for a 56-bit key) takes a long time. Using CommView for WiFi, one can induce a higher traffic level by sending encrypted ARP Request packets. The WLAN would then reply with ARP Response packets, thus generating additional traffic. While the original ARP Request packets being replayed cannot contribute to the pool of the packets needed for key recovery (they all have exactly the same contents, while key recovery requires unique packets), the ARP Response packets are different from each other, as a new Initialization Vector (IV) is used for every new packet.

The following steps should be taken for desired traffic generation:

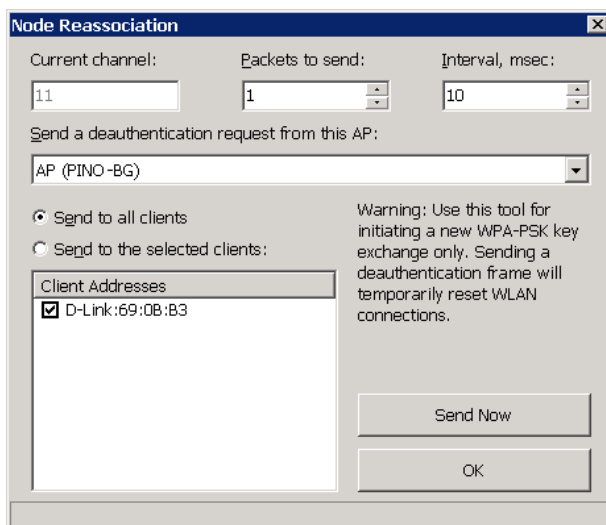
Step 1

Since the WLAN traffic is encrypted, we can't see which of the captured packets are ARP Request packets. However, we can make a guess. An ARP Request packet is typically 68 bytes long (or 70 bytes long, if the WLAN is QoS-enabled), has the broadcast destination address, and has the ToDS flag set. Configure CommView for WiFi to capture such packets by creating a new capturing rule, as shown below:



Step 2

ARP Request packets are usually sent immediately after the station performs the association. To force reassociation, use the Node Reassociation tool in CommView for WiFi (**Tools => Node Reassociation**):

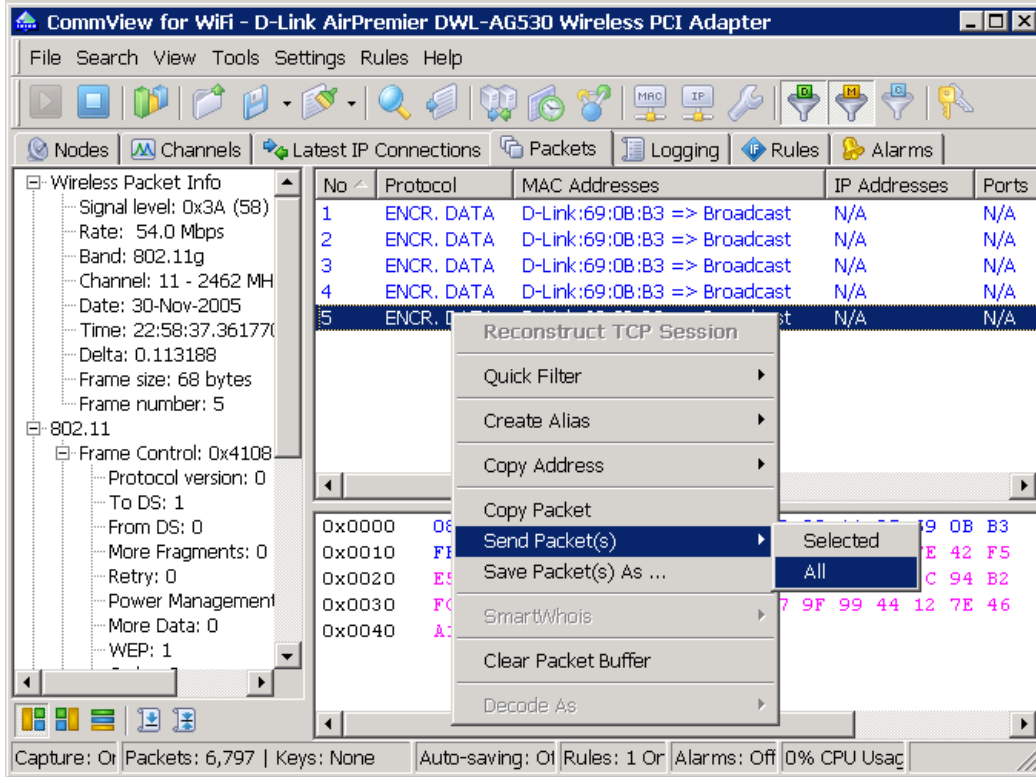


Capturing should be turned on prior to using this tool.

Step 3

Following the reassociation, stations would normally send ARP Request packets. Because we created a rule that discards all packets except ARP Requests, CommView for WiFi would display only encrypted ARP Request packets. You may need to go back to Step 2 if you can't capture these packets and click **Send Now** multiple times.

Once these packets are displayed as shown below, select **Send Packet(s) => All** to load these packets into **Packet Generator**:

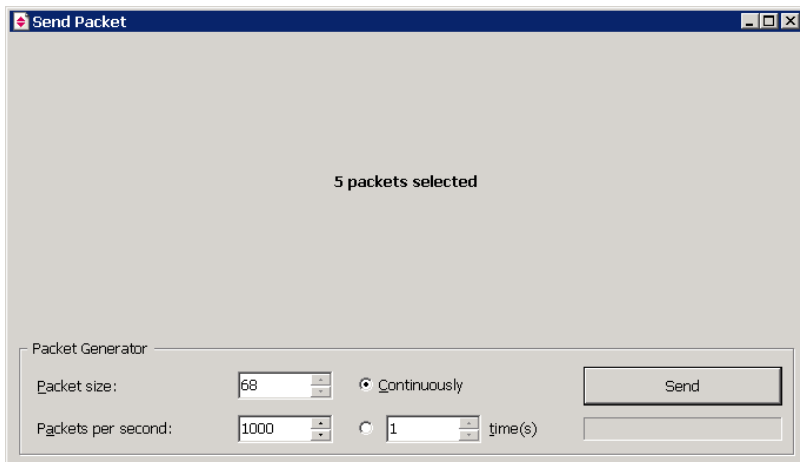


Step 4

Go back to the **Rules** tab (shown in Step 1) and disable the rule you created. This is very important, because if you don't do that, CommView for WiFi will filter out virtually all traffic, so no packets will be passed to WEPKR.

Step 5

The **Packet Generator** (shown below) allows you to send the selected packets with an arbitrary speed on the wireless channel currently being monitored. Set the desired packets per second rate, select the continuous mode, and click **Send** to start sending. You should normally see a hike on the traffic graph in CommView for WiFi, as well as the packet counter moving faster in WEPKR.



Frequently Asked Questions

Q. I'm trying to recover a 128-bit key. I've collected 800,000 packets, but WEPKR failed to recover the key. What should I do?

A. Recovering a WEP key is about probability. 800,000 packets are not sufficient in many cases. One of the most important factors is the number of unique initialization vectors (IVs) in the collected packets. 800,000 packets may contain 100% unique IVs or 50% unique IVs. This cannot be predicted. Also, even 800,000 unique IVs cannot guarantee success. So the best thing to do is to collect more packets by monitoring the WLAN for a longer period of time or by using the method described in the [Traffic Generation](#) chapter. Collect 1,600,000 packets and click **Action => Start key recovery now** to initiate a new key recovery session. If this doesn't work, collect 2 million packets.

Q. I'm trying to recover a key, one hour has passed, but the key has not been recovered yet.

A. First, make sure that you have a fast CPU. Recovering a WEP key on something like Pentium II-400 may take days. You must have at least Pentium 4. Second, the fewer packets you've collected, the slower the recovery process will be. If you have 800,000 packets for a 128-bit key and it's taking too long to recover it, collect another 800,000, in which case there is a very good chance that the key will be recovered within 15 minutes.

How to Purchase WEP Key Recovery

This program is a 30-day evaluation version.

A fully functional, unrestricted version of the program can be purchased for US\$499. Call us for pricing on larger site licenses. As a registered customer, you are entitled to:

- 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 phone and fax, checks, and wire transfers. Prices, terms, and conditions are subject to change without notice.

Contacting Us

Questions? Comments? Suggestions? Bug reports? Don't hesitate to contact us.

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

When describing your problem, please be as specific as possible. A detailed description of the problem will help us solve it much faster. Please don't forget to mention your OS version, the program version and build (Help => About), adapter type (e.g. Dial-Up Adapter), and any other details that you think may be relevant.

Other Products

CommView

CommView is a program for monitoring Internet and Local Area Network (LAN) activity and is 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](#)

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](#)

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 the 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](#)

NetResident

NetResident is an advanced network content monitoring program that captures, stores, analyzes, and reconstructs network events such as e-mail messages, Web pages, downloaded files and instant messages. NetResident uses advanced monitoring technology to capture the required data from the network, saves it to a database, reconstructs it, and displays this content in an easy-to-understand format. While NetResident is similar to network analyzers in many respects, it focuses on high-level protocols that are used to transfer content over the Internet or LAN. With NetResident, you don't need a profound understanding of networking technologies, have to use complex packet capturing and analysis software, or dig through network packets in order to reconstruct the actual data; NetResident does all the work for you and presents only the Web pages, e-mails, instant messages, or downloaded files as requested. NetResident is used by network administrators to enforce IT policy, parents to monitor their children's communication on the Internet, and by forensic experts to gain crucial information.

[More information](#)