

DigiSecret

Help Documentation

Copyright © 2001-2007 TamoSoft

Introduction

About 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 and self-extracting EXE files and for 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.

DigiSecret makes the process of working with files and archives very simple. Its intuitive interface allows you to create or read secure archives in a matter of seconds. You can add or delete entire folders or individual files to/from your archives, modify them, or manage multiple archives.

You can also share sensitive information with your associates who don't even have to have DigiSecret installed—all one needs to know is the passphrase, which protects the self-extracting archive. After the correct passphrase is entered, the files or folders will be extracted from the archive automatically.

If the recipient of the information is online and you have previously agreed upon the passphrase, DigiSecret will help you transmit the information securely. The two computers will establish connection; the data will be encrypted and sent to the recipient and automatically decrypted. You no longer need to worry about your information being intercepted—it will take the most powerful computers millennia to retrieve the information without knowing the passphrase.

DigiSecret also takes care of permanently erasing files or folders that you wish to remove. The files are deleted and overwritten several times to eliminate every possibility of recovering the information.

DigiSecret was developed and compiled outside of the USA, has no back doors or escrow keys, and is not subject to US export restrictions. Files are encrypted using the most reliable [encryption algorithms](#) that have resisted any form of cryptanalysis by the best mathematicians in the world: CAST (128-bit key), Blowfish (448-bit key), Twofish (256-bit key), and Rijndael (also known as AES, 256-bit key).

The fast proliferation of information technology exposes private data to breaches of confidentiality. Unfortunately, most of the encryption tools for individual and commercial users available on the market today are unable to provide the level of encryption sufficient to protect us from eavesdropping due to weak, easily broken security or general unawareness of the problem. If you don't use strong encryption, sensitive information can be easily stolen from your computer, intercepted by your Internet Service Provider, hackers, government, or global surveillance networks.

What's New

Version 2.1

- Windows Vista support.
- Improved interface.

Version 2.0

- DigiSecret now comes in two versions: Lite and Pro. DigiSecret Pro has all the functionality of the Lite version, as well as the following additional features: Ability to send encrypted files to other users via TCP/IP; Message Encryption Center that allows the user to encrypt plain text messages and send them via e-mail; Ability to customize SFX archives, i.e. create a custom window caption and hyperlink that executes any command.
- Robust operation with large files (over 2 Gbytes).
- A new compression algorithm with a better performance and higher compression ratio. Compression ratio can now be adjusted, and compression can be optionally turned off.
- More compact SFX archives.
- DigiSecret now interacts with e-mail clients in two ways: via MAPI or by using EML files.
- Localized versions of the program are now available. Supported languages include French, German, Russian, and Spanish.
- Many interface improvements including a new, fast file list with adjustable columns, dual progress bars (current and total progress), and Windows XP themes support.

Version 1.1

- Added a virtual keyboard that allows you to enter passphrases using the mouse and protects you from key loggers
- Added highly customizable and useful hints
- You can now paste files from the clipboard to DigiSecret
- Customized title can be added to self-extracting archives
- Files in the archive are automatically updated if you modify them
- Send archives by e-mail as attachments with just one mouse click
- Process priority can be changed
- Program status indicator added
- Many interface improvements
- New options added
- A new Windows Explorer menu item has been added when you drag archives with the right mouse button pressed

Using DigiSecret

Quick Start

If you don't like reading long manuals, this is probably the only chapter you need to read to get started.

Step 1.

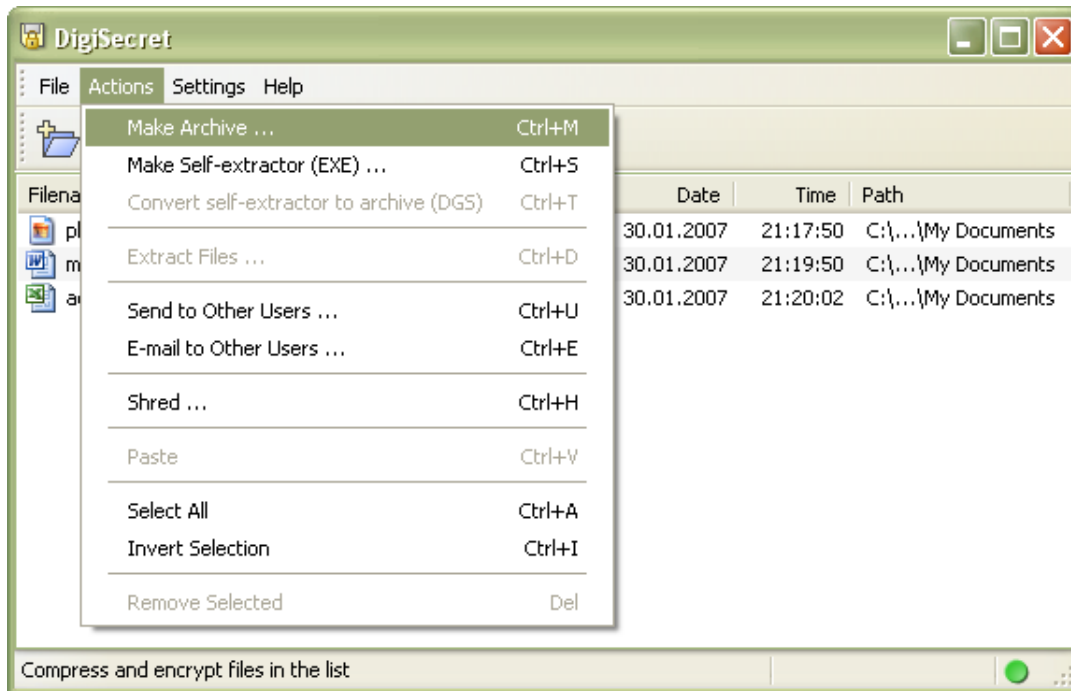
Launch the program.

Step 2.

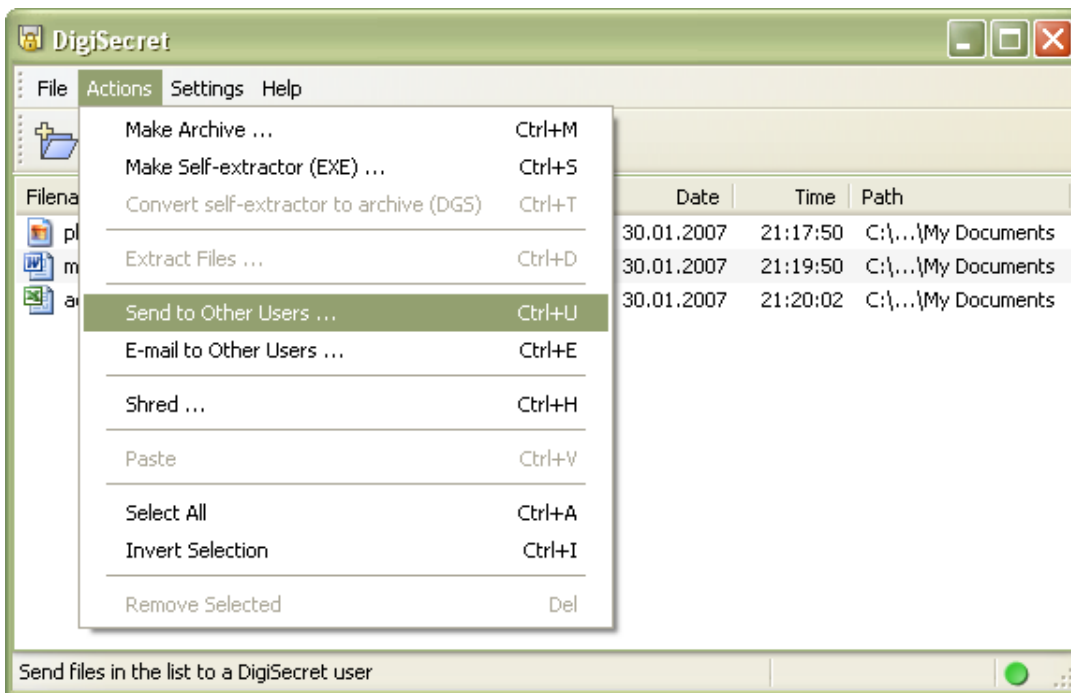
Drag & drop files or folders onto the program input area.

Step 3.

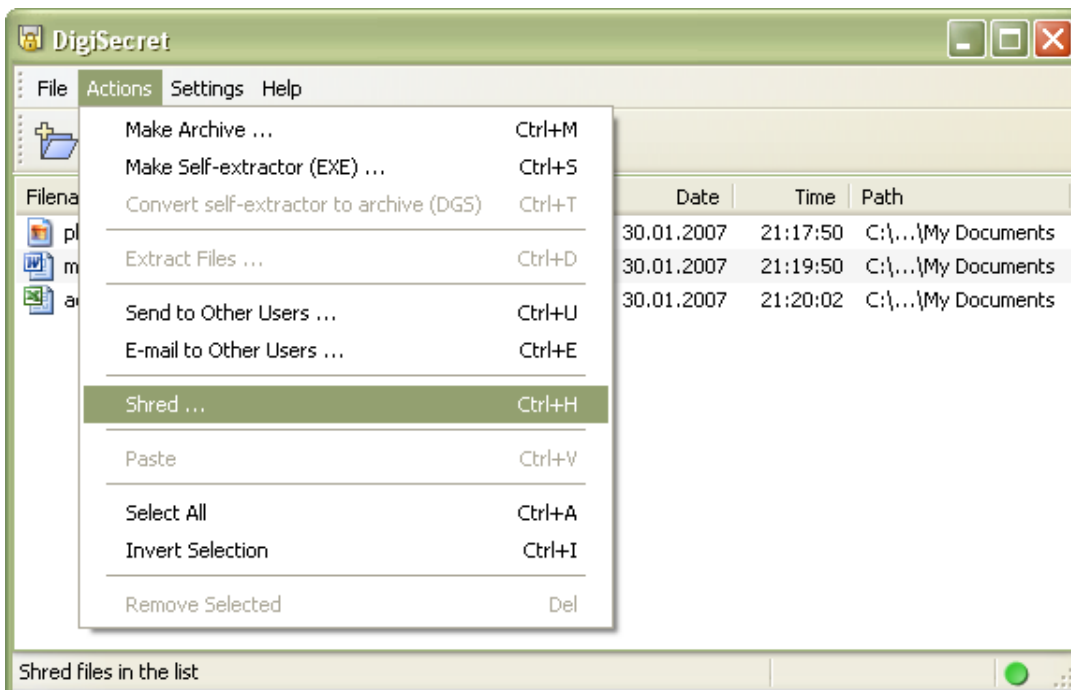
To create a DigiSecret encrypted archive, click **Actions => Make Archive ...** or **Make Self Extractor (EXE) ...**, type the passphrase into the **Passphrase** fields in the dialog window and click **Encrypt**.



To send files or folders to a recipient, click **Send** button on the toolbar, type the passphrase into the **Passphrase** fields, and click **Encrypt & Send**.



To remove selected files or folders from your disk without a possibility of recovering them, click **Shred** button on the toolbar.



DigiSecret is integrated into the Windows shell, which means that you can right-click on any file, select **DigiSecret** from the context menu, and perform any of the operations described above.

Overview

It is good to know what are [encrypted archives](#) before creating them. The files on your disks or the files that you send by e-mail have no protection from unauthorized access. They can be opened by whoever got hold of them. If you use DigiSecret to put your files into encrypted archives, the only way to view your files is to enter the correct passphrase. There are no backdoors in the program, so even if you forget your own passphrase the information cannot be recovered.

The program consists of the main window where the files and folders are displayed, the menu, and the toolbar for performing standard operations.

The color indicator in the right corner of the status bar shows the current status of the program. Normally it is green, but turns red when DigiSecret is busy.

DigiSecret is integrated into Windows Explorer and can be invoked by the file context menu. You do not have to launch DigiSecret to work with encrypted archives, encrypt files, send them by e-mail as attachments, or send them to other users securely. Right click on them and choose the action to perform; DigiSecret will be started automatically.

Additionally, when you drag DigiSecret archives using the right mouse button, you can extract files to the selected location with just a mouse click.

Main Menu

File

Add Files - adds new files to the list. If an archive is opened, the file selection dialog will allow you to add files to the current archive or open them in a new window.

Add Folder - adds the contents of folders (including subfolders) to the list. If an archive is opened, the folder selection dialog will allow you to add files to the current archive or open them in a new window.

Open Archive - opens an existing archive from the disk. A dialog window where you can select the archive to be opened will pop up.

Clear - clears the list of files. If an archive is open, the list of files is also cleared.

Message Encryption Center - launches [Message Encryption Center](#) window.

Exit - closes the program. All actions are interrupted.

Actions

Make Archive - compresses and encrypts all files from the list into one [archive](#).

Make Self-extractor (EXE) - compresses and encrypts all files from the list into one self-decrypting, [self-extracting archive](#) (EXE file).

Convert Archive to/from Self-extractor - [converts DigiSecret archive](#) to self-decrypting, self-extracting archive and vice versa.

Extract Files - decrypts and [unpacks](#) selected files from an open archive; if no files are selected, the entire archive is unpacked.

Send to Other Users - [sends](#) files from the list or an open archive to another DigiSecret user. Before the files are sent, DigiSecret puts them into an archive.

E-mail to Other Users - [sends](#) files from the list or an archive by e-mail using the default e-mail program. Before the files are sent, DigiSecret puts them into an archive.

Shred - removes files from disk without a possibility to recover them ([secure deletion](#)).

Paste - pastes files from the clipboard into the DigiSecret main window.

Select All - selects all files from the list.

Invert Selection - deselects the selected files and selects the ones that have not been selected.

Settings

Interface Font – allows you to select the font used by DigiSecret in all windows.

Options – displays the program settings.

Listen for Files – turns listening mode on or off. When listening is on, the program is able to [receive files](#) from other DigiSecret users.

Address Book – electronic notebook where the list of users and corresponding IP addresses/hostnames can be [stored](#).

Help

Contents – opens the help file.

Search For Help On – opens the DigiSecret help index

What's My IP Address – shows the IP address(es) assigned to your computer.

About – shows the About window.

Right-clicking on the program main window brings up the following menu:

Remove/Delete Selected - removes selected files from the list/deletes selected files from the archive.

Remove All - clears the list of files.

Select All - selects all files from the list.

Invert Selection - deselects the selected files and selects the ones that have not been selected

View with Associated Application - allows you to view selected files (up to 20) using applications associated with these files.

View with Default Viewer - allows you to view selected files (up to 20) with the default text editor.

View with ... - allows you to choose an application for viewing files.

Open Containing Folder - opens folders containing selected files (up to 20; does not apply to files from an open archive).

Paste - pastes the files from the clipboard into the program main window.

Creating DigiSecret Archives

To create DigiSecret archive, paste or drag files or folders to the program main window and click **Actions => Make Archive ...** menu, or simply click the **Encrypt** toolbar button. A dialog window will appear. The **Output File** field shows the location and the file name of the archive to be created. Click the **Browse** button to change the destination path of the archive. Type your passphrase in the **Enter Passphrase** field and confirm it in the **Re-enter** field. If you would like to see the passphrase as you type it, check the **Show typing** checkbox. If you would like to enter your passphrase without using the keyboard, click on the [Virtual Keyboard](#) button. To preserve folder structure in the archive (if it contains folders), check the **Preserve folder structure** checkbox. If this option is not selected, all files from all folders will be placed in one folder when decrypted. You can change the type of archive from DigiSecret (DGS) to [self-extracting](#) (EXE) archive by checking the **Self-extracting archive (EXE)** checkbox. When this checkbox is checked, additional tabs will appear that allow you to customize the caption and the hyperlink in the [SFX archive](#). **Encryption algorithm** menu allows you to select your favorite encryption algorithm from the list. For more information on encryption algorithms, please see the [Encryption](#) chapter. The **Compression** slider allows you to set the desired compression ratio for the archive. The compression varies from **None** (encryption only, very high speed of archiving) to **Maximum** (the data is compressed much better than if ZIP algorithm were used).

Shredding

You can choose what action you would like to perform with the original files in the **Shredding** tab, in the **What to do with original files** menu. The default option is to leave them as they are; alternatively you can simply delete the files or [delete](#) them without a possibility of recovery (shred options). If you choose any of the delete options, you can also check the **Delete empty folders** checkbox to remove the empty folders as well.

If you would like to use the current settings for all archives created in the future, check the **Use these settings as default** checkbox.

Click on the **Encrypt** button in the dialog window and the new archive will be created.

You can also create DigiSecret archive by right-clicking on a file in Windows Explorer and selecting **DigiSecret =>Archive ...** .

Creating Self-extracting Encrypted Archives

To create self-extracting archive paste or drag files or folders to the program main window and click **Actions => Make Self-extractor (EXE) ...** menu, or simply click the **Encrypt** toolbar button. A dialog window will appear. The **Output File** field shows the location and the file name of the archive to be created. Click the **Browse** button to change the destination path of the archive. Type your passphrase in the **Enter Passphrase** field and confirm it in the **Re-enter** field. If you would like to see the passphrase as you type it, check the **Show typing** checkbox. If you would like to enter your passphrase without using the keyboard, click on the [Virtual Keyboard](#) button. To preserve folder structure in the archive (if it contains folders) check the **Preserve folder structure** checkbox. If this option is not selected, all files from all folders will be placed in one folder when decrypted. You can change the type of archive from self-extracting (EXE) to DigiSecret (DGS) [archive](#) by un-checking the **Self-extracting archive (EXE)** checkbox. **Encryption algorithm** menu allows you to select your favorite encryption algorithm from the list. For more information on encryption algorithms, please see the [Encryption](#) chapter.

Shredding

You can choose what action you would like to perform on the original files in the **What to do with original files** drop-down box of the files in the **Shredding** tab. The default option is to leave them as they are; alternatively you can simply delete the files or [delete](#) them without a possibility of recovery (shred options). If you choose any of the options that involve deletion, you can also check the **Delete empty folders** checkbox to remove the empty folders as well.

EXE Caption

Text entered in the box will be displayed in the top part of the SFX archive window when the SFX file is launched. The text may be loaded from a text file by clicking the **Load** button and browsing for the file on the disk. The **Clear** button clears the text box. This functionality is available in *DigiSecret Pro* only.

EXE Hyperlink

SFX archives may display a hyperlink in the upper right corner of their windows. Clicking on the hyperlink executes any command that was specified by you (opens a specific web page, sends an e-mail using the MAILTO command, launches an application, opens a document, etc.) *This functionality is available in DigiSecret Pro only.*

Display hyperlink - check this checkbox if you would like the hyperlink displayed in the SFX archive window.

Visible caption - the text of the hyperlink that is visible to the user (does not have to correspond to the command that will be executed when the user clicks on the hyperlink).

Command to run - command line that will be executed when clicking on the hyperlink. Examples of such commands are:

```
Notepad.exe
http://www.tamos.com
mailto:myname@hotmail.com?subject=Notify
MyNotes.doc
```

The hyperlink in the upper right corner of the tab is for testing. It emulates the hyperlink that will be displayed in the SFX archive being created. When you click on it, the specified command will be executed.

If you would like to use the current settings for all archives created in the future, check the **Use these settings as default** checkbox.

Click on the **Encrypt** button in the dialog window and the new self-extracting archive will be created.

You can also create self-extracting archive by right-clicking on a file in Windows Explorer and selecting **DigiSecret => SFX Archive (EXE) ...**

Extracting from Archives

To extract files or folders from DigiSecret archive, double-click on it or click on the **Open** toolbar button and select the archive. You will then be prompted for the passphrase and if you enter it correctly, you will see the contents of the archive in the program main window. If you would like to enter your passphrase without using the keyboard, click on the [Virtual Keyboard](#) button. Click on the **Extract** toolbar button or **Actions => Extract Files ...** menu. A dialog window will appear. The **Output File** field shows the folder that the files are going to be extracted to. Click the **Browse** button to change the destination folder. Check the **Reconstruct folder structure** checkbox if your archive contains folders and you want to have their structure reconstructed; otherwise, all files will be extracted to the same folder. If you would like to extract only the files that you selected before clicking on the **Extract** toolbar button or **Actions => Extract Files** menu, check the **Extract selected files only** checkbox. Click **Decrypt & Extract** and the contents of the archive will be extracted into the selected folder. You can also drag files from an open archive to extract them.

If you view one or several files from an open DigiSecret archive with an associated application or default viewer, the program creates their temporary copies on the disk and will prompt you to have the files in the archive replaced by the newer versions if you modify these files. After that the temporary copies will be shredded.

You can also extract DigiSecret archive by right-clicking on an archive in Windows Explorer and selecting **DigiSecret => Extract to ...** or by dragging the archive to the target location holding the right mouse button.

Converting Archives

To convert DigiSecret archive to a self-extracting exe file or vice versa, click **File => Open** or click on the **Open** toolbar button and select the archive that you wish to have converted. Click **Actions => Convert Self-extractor to archive (DGS)** if you selected a self-extracting archive or **Actions => Convert archive to Self-extractor (EXE)**. The confirmation of the conversion will appear on the bottom pane.

Converting Old Format Archives

This dialog window appears when DigiSecret detects an old format archive that the user wishes to modify or convert to the new format. The contents of the archives in the old format can only be extracted; no alterations, such as adding to or deleting from those archives, can be performed. The major change in the new type of DigiSecret archive is the new compression algorithm that significantly increases the compression ratio and the data processing speed. This dialog window also includes an option to archive the files without compression, just encrypting them. This mode allows you to pack the data at the highest speed possible.

The conversion dialog window allows you to set the compression ratio for the new archive. The Fast (default) level approximately corresponds to the compression ratio of the old archives.

Secure File Transfer

DigiSecret can be used for sending files over the Internet or Local Area Network securely. Your data is automatically encrypted before it is sent and decrypted when it is received. In order for the recipient to successfully receive your files or folders, he/she must know the passphrase that you used to protect the files being sent. The passphrase must be agreed upon before the file transfer takes place, and it cannot be transmitted openly. If your passphrase is intercepted, the whole purpose of secure file transfer is defeated - whoever intercepted the passphrase may also intercept the files that you send and recover them. It is highly recommended to use a secure channel (e.g. PGP) for agreeing upon a secret passphrase.

To send files or folders, drop them on the program main window or click on the **Add** toolbar button and select the files/folders you want to send. Click on the **Send** toolbar button or **Actions => Send to Other Users ...**. A dialog window will appear. Enter the recipient's IP address or hostname in the **Remote IP address/hostname** field and select your preferred encryption algorithm from the Encryption algorithm menu. If you are sending an encrypted archive, the **Encryption algorithm** menu is disabled. The recipient's address may already be in the [address book](#); in this case you can select it by clicking the **Addr. Book** button and double-clicking on the address line, or, if the recipient is on the local network, you can find the recipient by clicking the **Browse** button. Type your passphrase in the **Enter Passphrase** field and confirm it in the **Re-enter** field. If you would like to see the passphrase as you type it, check the **Show typing** checkbox. If you would like to enter your passphrase without using the keyboard, click on the [Virtual Keyboard](#) button. Click the **Advanced** button if you would like to change the remote TCP port number for this session, or if your network connection is routed via a SOCKS5 firewall and you need to enter SOCKS5 server settings. When you are ready to send, click the **Encrypt & Send** button to initiate file transfer.

If you would like to receive files, you need to deploy [DigiSecret Agent](#). If it does not launch at Windows startup, you will need to start it manually by clicking Start => Programs => DigiSecret => DigiSecret Agent. When someone sends files to you, a dialog window will pop up that will show the sender's IP address and hostname, and prompt you for a passphrase. To start receiving files, enter the passphrase and click the **Accept & Receive** button.

You can also send files to other DigiSecret users by right-clicking on a them in the Windows Explorer and selecting **DigiSecret =>Send to DigiSecret User ...**. *The ability to send and receive files is available in DigiSecret Pro only.*

Sending Archives by E-mail

DigiSecret allows you to send files or DGS archives by e-mail using the default e-mail program. DigiSecret can send files by e-mail in two ways:

- By creating an EML file that contains the encrypted archive as attachment, and then launching this file. To use this mode, it is necessary that EML files be associated with the e-mail application and the application is able to open them correctly. This mode suits such e-mail clients as Microsoft Outlook and Outlook Express.
- By using the MAPI system e-mail interface. It suits virtually any e-mail client and should be used with such applications as Eudora and The Bat!.

During the first use of this function, DigiSecret will prompt you to select the method of sending files if it has not been explicitly specified in the program options. You can try both methods and choose the one that works best with your e-mail client.

If unencrypted files are being sent, they are put into an encrypted DigiSecret archive. To send files or DGS archive by e-mail, click **Actions => E-mail to Other Users ...**. A dialog window similar to [Encrypt](#) window will appear. Select your preferred encryption algorithm from the Encryption algorithm menu. Type your passphrase in the **Enter Passphrase** field and confirm it in the **Re-enter** field. If you would like to see the passphrase as you type it, check the **Show typing** checkbox. If you would like to enter your passphrase without using the keyboard, click on the [Virtual Keyboard](#) button. After you click the **Encrypt & Send** button, a new message window with the attached archive will open in your default e-mail program. If you are sending a DigiSecret archive, the new message window will open right after you select **E-mail to Other Users** menu item.

You can also send files or archives by e-mail by right-clicking on them in the Windows Explorer and selecting **DigiSecret =>E-mail to ...**.

Message Encryption Center

Message Encryption Center is a part of DigiSecret Agent that allows you to encrypt/decrypt plain text messages and send them via e-mail. The message is compressed and encrypted with a symmetric key. This process is the same as when creating encrypted archives; the same encryption and hashing [algorithms](#) are used.

The message text is ASCII-armored to prevent it from distortion during transmission (for example via E-mail). A typical encrypted message looks like this:

```
----- BEGIN DigiSecret Encrypted Message -----  
KJfmAE0AFBSOAAAUGK1pxNIODYD+gkBPPcv+Mxo6HTEKI / PU8N1RXEbeNanxnju  
nAE44PicAHfRQl7wyN8s+lcY6EEW0qVda7D/8AFnFnLQsSzHgOkwEn6F8pCoWPim  
mT2B3B6szA3RBHPQZavdqPgNbfd9ytYWbanx2xW5s1Vj+Af5QMZZ7AA5bQ8a9j0J  
rRojWdtxBfgvc/eXDaDGWrs561S5m7N/5Uihu2JW5SjuyDkL2JgPFE9za60zKzy5  
3gWzPCq6voicgeZa4sWSKOiCNLOAwHRqPGaix1OS+LWJeMiXE1f02tf1FAOE/L6Q  
rbtZNLw0cvNG  
----- END DigiSecret Encrypted Message -----
```

To launch Message Encryption Center, click **File => Message Encryption Center**, or right-click on the DigiSecret system tray icon and select **Message Encryption Center**.

Message Encryption Center has a toolbar with buttons for loading the text of the message, saving it to the disk, and clipboard operation. It also has a drop-down selection box for choosing an encryption algorithm to be used.

To create an encrypted message, please enter or paste your text in the Message Encryption Center window, and enter your password in the corresponding boxes below. When decrypting the message, you only need to enter the password once.

The **E-mail** button launches your default e-mail client and creates a new message with the encrypted message in its body.

Message Encryption Center is available in DigiSecret Pro only.

DigiSecret Agent

DigiSecret Agent's main function is to accept files sent by other DigiSecret users via TCP/IP. Besides, DigiSecret Agent includes [Message Encryption Center](#) that allows you encrypt/decrypt plain text messages.

Clicking on the tray icon will launch either a new DigiSecret window or Message Encryption Center, which can be set in the program options. The **Settings => Options** menu allows you to choose whether the Agent will start at Windows startup and enable/disable the listening mode, responsible for accepting files from other DigiSecret users.

Right-clicking on the tray icon brings up the following menu:

New DigiSecret Window - opens a new DigiSecret window.

Message Encryption Center - launches Message Encryption Center.

Settings - allows you to enable/disable listening mode, specify if you would like the Agent to launch at Windows startup, and open the program settings dialog.

Help - allows you to launch program manual, search the help index for keywords, see the information about the program, and view the IP address(es) of your computer.

Close All DigiSecret Instances - closes all active DigiSecret windows.

Exit - closes DigiSecret Agent and removes its icon from the system tray.

DigiSecret Agent is available in DigiSecret Pro only.

Shredder

DigiSecret can erase files or folders from your disks beyond recovery. When you delete a file using the standard methods, it is usually moved to the Recycle Bin, which makes it possible to restore the file later on. Even if you empty the Recycle Bin, your files can still be recovered using a special utility; the operating system just marks it so that it can be overwritten in the future, but doesn't wipe the information contained in the file. DigiSecret deletes files and overwrites them with random data multiple times, using special patterns, to eliminate any possibility to recover them. You can choose how many times the file is overwritten (1 to 35 times). To permanently delete the files or folders, drag them to the program main window and click **Actions => Shred ...** or the **Shred** toolbar button. A dialog window will appear where you can select the preferred shredding scheme. Check the **Delete empty folders** checkbox to remove the empty folders along with the files. Check the **Use these settings as default** checkbox if you would like to use the selected shredding scheme as the default one in the future.

The choice of the shredding scheme depends on the estimated resources and determination of the adversary that, you believe, may be trying to recover your files. If your opponent's only tool is a simple Undelete program, the **Basic** scheme is enough to make your files unrecoverable. If you are dealing with a powerful government agency that possesses the state-of-the-art technology to thoroughly examine your drives, even the **Full** scheme may be sometimes insufficient to provide 100 percent guarantee that all the information that you erased is gone forever, although the cost of data recovery would be prohibitively expensive.

You can also remove files permanently by right-clicking on them in Windows Explorer and selecting **DigiSecret => Shred ...** .

Address Book

You can save a list of DigiSecret users and their IP addresses in the address book by clicking **Settings =>Address book**.

Type in a name and an IP address or hostname and click the **Add/Modify** button. To edit an entry, click on it and edit the text in the **Name** or **IP address/hostname** fields. To delete an entry, right-click on it and choose **Clear Selected**, or **Clear All** if you want to remove all entries. You can protect your address book with a password by clicking **Settings =>Options =>Security** and checking the **Password-protected Address Book** checkbox.

Virtual Keyboard

Virtual Keyboard allows you to protect your passphrase from being logged by stealth keyboard logging programs that might be running on your computer. You can enter your passphrase using only the mouse.

The **Virtual Keyboard** button can be found in every DigiSecret dialog window that prompts you for a passphrase. The **Virtual Keyboard** window has a typical password input area where the entered password is replaced by asterisks or displayed as typed. The buttons with characters represent the real keyboard buttons. The characters' case can be changed by clicking the Shift button or holding the Shift button on the actual keyboard. The **Virtual Keyboard** automatically detects the language layout changes and displays the corresponding language characters on the key buttons. The name of the current language layout is displayed in the window title bar.

You can also enter characters using their ASCII codes, which allows you to enter any characters from the ASCII table, even the ones that are not present on your keyboard. The use of additional characters increases the passphrase strength and considerably complicates the task of breaking it by brute force attack.

Configuring DigiSecret

Security

Default encryption algorithm – the selected [algorithm](#) will be used by default in all corresponding dialog windows.

Default shredding scheme – the selected scheme will be used by default in all corresponding dialog windows, and also for removal of all temporary files that may be created by the program, as well as the results of unaccomplished actions.

Password protected Address Book – prompts for a password when accessing the address book. The address book is stored on the disk in encrypted format; the file has the name of the current user followed by the .DSB extension. It can be copied to another computer and renamed. If your address book is password-protected and you enter the incorrect password, you will be prompted to re-enter it or delete the address book. If you choose to delete it, the program will open a blank address book for you.

Enable passphrase caching – checking this box turns on password caching. DigiSecret can save entered passwords in a special memory area that is protected from swapping to disk. Note that such protection is only possible under Windows NT/2000/XP; if you are running Windows 95/98/ME, there is absolutely no guarantee that the cached information won't be swapped to disk. When you close DigiSecret, all cached passwords are erased from the computer memory.

Purge cache after – allows you to specify the time after which the entered passwords are erased from memory.

Interface & Settings

Main Window

This tab allows you to customize the program main window.

Reuse application window whenever possible – when checked, the program attempts to perform actions without opening new windows.

Explorer-like buttons – the toolbar buttons style resembles the Windows Explorer toolbar buttons when this option is checked.

Hide button captions - if this option is selected, the names of toolbar buttons will be removed, leaving only pictograms on the buttons.

Full row select – if this option is selected, the entire line in the file list will be highlighted.

Alternate colors – check this box to have the program display the file list in the two-color mode.

Grid lines – when checked, grid lines in the program main window are displayed.

Interface Language - allows you to select the language for the program interface (menus, hints, names of checkboxes, etc.) from the list. To use a language different from the default one, you need to have the appropriate .TLF file in the application folder. The language files that are currently available can be downloaded [here](#).

Hints

Show application hints – when checked, hints for buttons and other elements are displayed.

Show toolbar hints – if this option is checked, hints for the toolbar buttons are displayed.

Include shortcut information – if checked, the keyboard shortcut information is added to the text of the hint when applicable.

Actions

Confirmations Dialogs

Don't show shred confirmation dialog – if this option is selected, the dialog window that confirms the removal of files after they are added to the archive is not displayed.

Don't show shred warning dialog (for beginners only) – if this option is selected, the warning that all files from the current list will be deleted is not displayed.

Don't prompt for confirmation when deleting files from archives – if this option is selected, the confirmation dialog saying that the selected file(s) will be deleted is not displayed.

Don't prompt for confirmation when overwriting files in archives – if this option is selected, the confirmation dialog saying that the file(s) in the archive will be overwritten is not displayed.

DigiSecret Agent Tray Icon

Clicking on the tray icon invokes DigiSecret window/Message Encryption Center - allows you to select what program component you want to be launched by clicking on the DigiSecret Agent tray icon.

Miscellaneous

Default Viewer - allows you to specify the path to the default application for viewing files that are used by the “**View with Default Viewer**” command.

Temp Folder - allows you to select the folder where all DigiSecret temporary files are kept. You can schedule Windows to automatically purge or shred this folder.

E-mail sending

Using Files/ Using MAPI interface - allows you to select the method by which DigiSecret sends files by [e-mail](#).

Network

File transfers

Run DigiSecret Agent at Windows startup - makes DigiSecret agent launch automatically when Windows starts. DigiSecret Agent is responsible for accepting files from other users via TCP/IP. When it is launched, its icon is displayed in the system tray. Right-clicking on the icon brings up a menu with Agent options that also allows you to open a DigiSecret window or a Message Encryption Center window.

Listen for file transfers at Agent startup - as soon as the DigiSecret Agent is launched, it opens a TCP/IP port (by default 4012) for accepting files from other users. If you do not wish to accept file transfers, this option can be disabled and enabled when needed via system tray icon menu.

Listen on TCP port – the port number on which the program listens for files, as well as the default port number for outgoing connections.

Download folder (where received files will be stored) – the path to the folder where files received from other users will be stored.

Remember most recently used IP addresses - select this option if you would like to keep a list of most recently used IP addresses.

Number of IP addresses to remember - the number of recently used IP addresses which should be preserved for future use. The stored list of addresses is encrypted. If you do not wish to keep the list of IP addresses, enter 0 (zero) in this field.

Firewall

Use SOCKS5 firewall – check this box if your computer is behind a firewall and direct TCP connections are blocked. This option allows DigiSecret to work on client machines behind most of the popular firewalls/proxy servers.

Host – specify the hostname/IP address of the SOCKS firewall.

Port – specify the port number of the SOCKS firewall.

User authentication – allows you to enter your login and password if the firewall requires authentication. The supported authentication type is RFC 1929 (cleartext).

Important Security Information

Frequently Asked Questions

Q. Why do I need DigiSecret Agent? Can I do without it?

A. If you use DigiSecret just to create encrypted archives, store them locally, and/or e-mail them, you can do without DigiSecret Agent. If you also want to share files in a secure manner with your friends or colleagues using the encrypted file transfer feature, or encrypt some text and send it by e-mail, you would certainly need to use it. Once started, DigiSecret Agent listens on a TCP port and accepts connections when someone wants to securely transfer files to you; also, DigiSecret Agent includes Message Encryption Center, a component that allows you to type any plain text message, encrypt it, and send it via e-mail in a matter of seconds.

Q. I do not use Message Encryption Center and never send or receive files via TCP/IP. How do I prevent DigiSecret Agent from starting?

A. Click **Settings => Options**, select the **Network & Agent** tab and uncheck the **Run DigiSecret Agent at Windows Startup** checkbox to prevent DigiSecret Agent from starting at Windows startup.

Q. How do I configure DigiSecret to launch Message Encryption Center rather than a new DigiSecret Window when I click on the system tray icon.

A. Click **Settings => Options**, select the **Interface & Settings** tab, then the **Actions** tab and select the **Message Encryption Center** radio button. This will make DigiSecret launch Message Encryption Center when you click on the DigiSecret tray icon.

Q. When I click on the system tray icon, the program creates a new DigiSecret window, but I already have another window I'm working with. Is there a way to change this behavior?

A. You can activate the existing window by clicking on its task bar button rather than on the system tray icon. However, if you want to change this behavior, you can check the **Reuse application window whenever possible checkbox** in the **Interface & Settings** tab, **Settings => Options** menu.

Q. My firewall software tells me that DigiSecret tries to open a port. Why is it necessary? What can I do to prevent DigiSecret from opening it?

A. If you use DigiSecret to accept files from other DigiSecret users, DigiSecret Agent needs to open a TCP port to accept incoming file transfers. If you do not need to accept files, you can disable the listening mode. Click **Settings => Options**, select the **Network & Agent** tab, and uncheck the **Listen for file transfers at Agent startup** checkbox.

Q. When I open a file from my DigiSecret archive with an associated application (e.g. MS Word), does DigiSecret store them in non-encrypted form and if yes, where does it keep them?

A. To be accessed by an application, files have to be in non-encrypted form, otherwise the programs would not be able to open them. Therefore, DigiSecret decrypts them and places their copies into the system TEMP folder (typically C:\winnt\temp or C:\Documents and Settings\Username\Local Settings\Temp). If the files have been modified by the time you close the archive, DigiSecret will prompt you to update the files in the archive. If you click Yes, then the files in the archive will be updated. The decrypted copies in the TEMP folder are always shredded when the archive is closed.

How DigiSecret Works

1. General information.

When an archive is being created, the following actions are performed on the source files:

- Hash calculation to ensure data integrity;
- Compression;
- Encryption.

When files are being extracted from the encrypted archive, the following actions are performed on the archive:

- Decryption;
- Decompression;
- Hash calculation for checking data integrity.

In each case all three actions are performed in one pass. The processed data is written directly to the destination archive, so that the archiving/extraction process is carried out without creating any temporary files. Along with other mechanisms implemented in DigiSecret, this ensures high efficiency of all file operations.

The implemented data compression algorithm provides a better compression ratio than the ZIP algorithm for most of the files. The compression speed is comparable with the ZIP algorithm, and it is considerably higher than the speed of other popular archiving utilities on the market.

DigiSecret uses the following algorithms for data encryption:

Algorithm	Key length, bits
Blowfish	448
Twofish	256
Cast-128	128
Rijndael	256

The implementation of the algorithms was checked against the publicly available test vectors:

Blowfish	http://www.counterpane.com/vectors.txt
Twofish	http://www-08.nist.gov/encryption/aes/round1/testvals/twofish-vals.zip
Cast-128	http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2144.html
Rijndael	http://www-08.nist.gov/encryption/aes/round1/testvals/rijndael-vals.zip

The following hash calculation algorithms are used in the application:

Hash algorithm	Hash size, bits:
SHA-1	160
RipeMD-160	160

The implementation of the algorithms was checked against the publicly available test vectors:

SHA-1	http://www.itl.nist.gov/fipspubs/fip180-1.htm
RipeMD-160	http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html

2. Creating an archive.

DigiSecret can create two types of archives: DGS (a standard encrypted archive) and EXE (a self-extracting encrypted archive). The data storage format is completely identical for both types of the archives. Moreover, the EXE archive extraction code is based on the same engine as the one used in DigiSecret itself. This helps us maintain the same security and efficiency standards when extracting the data from both DGS and EXE files. At the same time, the size of the self-extracting archive is increased very insignificantly (by about 70 Kb) compared to DGS.

Data encryption is initialized with a user-defined passphrase and a random Initialization Vector (IV).

The passphrase entered by the user is not used as the encryption key directly. Rather, it is used as an input value for the functions that performs 1,000 SHA-1 hash iterations to produce the key that matches the maximum key space for the chosen cipher, which makes dictionary attacks more complicated.

The IV is created using a Pseudo-Random Number Generator (Mersenne Twister: A 623-Dimensionally Equidistributed Uniform Pseudo-Random Number Generator). The derived IV is saved with the archive and is later used for encryption algorithm initialization when extracting the data.

All the encryption algorithms used in DigiSecret operate in the Cipher Block Chaining (CBC) mode.

In order to ensure data integrity, DigiSecret calculates the SHA-1 hash value of the files included in the archive. This hash value is stored in the archive so that the program could detect possible data corruption when extracting the files. The name, real size, creation date and attributes of the archived files are also encrypted and stored in the archive.

3. Extracting data from an archive.

The decryption process is initialized the same way as the encryption, i.e. using the hashed passphrase and the IV stored in the archive. During data decryption and decompressing, the SHA-1 hash value of the extracted data is calculated. If the calculated hash value doesn't match the value stored in the archive, the unpacked file is immediately shredded with multiple passes even though the data contained in the file is incorrect. In case any errors occur while the data is extracted (e.g. lack of free space on the disk), the incorrect file is also shredded. If you open a DigiSecret archive and work with the files without explicitly extracting them, DigiSecret decrypts them and places their copies into the system TEMP folder (typically C:\winnt\temp or C:\Documents and Settings\Username\Local Settings\Temp). If the files have been modified by the time you close the archive, DigiSecret will prompt you to update the files in the archive. If you click Yes, then the files in the archive will be updated. The decrypted copies in the TEMP folder are always shredded when the archive is closed.

4. Sending and Receiving Files

When sending/receiving data via TCP/IP protocol, the files being sent are encrypted using the passphrase. Additionally, before sending the encrypted data to the recipient, the program verifies if the passphrases entered by the sender and recipient match (otherwise the decryption will fail). In order to perform such verification, the program calculates the passphrase checksum using many rounds of SHA-1 and finally one round of RipeMD-160 and uses the first 10 bytes of the resulting value as the checksum. The checksum is long enough to ensure with almost 100% probability that the passphrase is the same on both ends, and at the same time is useless for potential attempts to reconstruct the encryption key. If the entered passphrases don't match, the recipient is prompted to enter a different passphrase.

5. Shredding

The file deletion implemented in DigiSecret allows you to erase the files from the hard drive or a floppy disk and makes it virtually impossible to recover the data. Although it is believed that it is impossible to completely erase data from magnetic media, shredding the files using the **Full** scheme makes data recovery prohibitively expensive even for the most powerful and well-funded adversaries. If you believe that your opponents may have practically unlimited budget and the most advanced technical means; it is recommended that you physically destroy the media containing the sensitive information

The shredding process in the **Full** mode includes the following operations:

- The file is overwritten 35 times and the data is flushed to the disk after each pass;
- The file size is set to 1 byte;
- The File creation date, last access, last write attributes are set to random value;
- The file name is replaced with a randomly generated string;
- The file is deleted.

The table below lists the data patterns used to overwrite the file in the **Full** mode (35 passes). Other modes (Basic, Normal, Medium) use a smaller number of passes, starting from the beginning of the table.

Pass No.	Data Written
1	Random
2	Random
3	Random
4	Random
5	01010101 01010101 01010101 0x55
6	10101010 10101010 10101010 0xAA
7	10010010 01001001 00100100 0x92 0x49 0x24
8	01001001 00100100 10010010 0x49 0x24 0x92
9	00100100 10010010 01001001 0x24 0x92 0x49
10	00000000 00000000 00000000 0x00
11	00010001 00010001 00010001 0x11
12	00100010 00100010 00100010 0x22
13	00110011 00110011 00110011 0x33
14	01000100 01000100 01000100 0x44
15	01010101 01010101 01010101 0x55
16	01100110 01100110 01100110 0x66
17	01110111 01110111 01110111 0x77
18	10001000 10001000 10001000 0x88
19	10011001 10011001 10011001 0x99

20	10101010 10101010 10101010 0xAA
21	10111011 10111011 10111011 0xBB
22	11001100 11001100 11001100 0xCC
23	11011101 11011101 11011101 0xDD
24	11101110 11101110 11101110 0xEE
25	11111111 11111111 11111111 0xFF
26	10010010 01001001 00100100 0x92 0x49 0x24
27	01001001 00100100 10010010 0x49 0x24 0x92
28	00100100 10010010 01001001 0x24 0x92 0x49
29	01101101 10110110 11011011 0x6D 0xB6 0xDB
30	10110110 11011011 01101101 0xB6 0xDB 0x6D
31	11011011 01101101 10110110 0xDB 0x6D 0xB6
32	Random
33	Random
34	Random
35	Random

The deterministic patterns between the random writes are permuted before the write is performed, to make it more difficult for an opponent to use knowledge of the erasure data written to attempt to recover overwritten data. The patterns were obtained from the article "[Secure Deletion of Data from Magnetic and Solid-State Memory](#)" by Peter Gutmann.

Choosing the Passphrase and Algorithm

Choosing the right passphrase

Your passphrase is the most important factor influencing the security of your files. This means that it is absolutely unacceptable to use weak passphrases, i.e. short or easy-to-guess ones. If your passphrase is in the dictionary, you are definitely in jeopardy. It is highly recommended that you use a long and unusual passphrase containing upper and lower case letters, numbers, spaces, and punctuation marks, preferably something that you can easily remember but that others cannot guess. In other words "Hello" or "My computer" are bad passphrases, while something like "is 1t TiMe to ch00z someth!ng bet-ter 4 you&me?" is good (don't use this one though!). It's also a good idea to mix your native language with foreign words and use non-English characters.

Which encryption algorithm should I choose?

In fact it's a difficult question. Given today's understanding of cryptography, all the four algorithms used in DigiSecret are unbreakable in the foreseeable future. CAST-128 has been proven to be resistant to both linear and differential cryptanalysis and can be broken only by brute force. Twofish and Blowfish, developed by a famous security expert Bruce Schneier, are also good and fast ciphers with no known weaknesses. Rijndael is the winner of the AES (Advanced Encryption Standard) contest and will soon become the standard in the USA. If we assume that these algorithms can be broken only by brute force, 128-bit keys will be able to withstand attacks for many decades, while 448-bit keys make attacks against them impossible even in theory.

Information

How to Purchase DigiSecret

This program is a 30-day evaluation version. If you would like to continue using it after 30 days, you must purchase it. Below is the pricing for the fully functional unrestricted version of the program:

License type	Price, US
DigiSecret Pro, 1 user license	\$49.00
DigiSecret Lite, 1 user license	\$29.00

Contact us or visit our site for pricing on larger site licenses.

What's the difference between the Pro and Lite versions?

The following features are available in the Pro version only:

- Message Encryption Center that allows you to encrypt and e-mail text messages;
- Ability to send and receive files via TCP/IP to/from other DigiSecret users;
- Ability to customize SFX archives by adding a title and hyperlink that can execute a specified command.

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 cards orders, orders by phone and fax, checks, 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:

PO Box 1385
Christchurch 8015
New Zealand

Fax: +64 3 359 0392 (New Zealand)

Fax: +1 917 591 6567 (USA)

Other Products by TamoSoft

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 a 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](#)

CommView for WiFi

CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g networks. Loaded with many user-friendly features, CommView for WiFi combines performance and flexibility with an ease of use unmatched in the industry. CommView for WiFi captures every packet on the air to display important information such as a list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for WiFi can help you view and examine packets, pinpoint network problems, perform site surveys, and troubleshoot software and hardware.

[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](#)

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, or 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](#)

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. What makes CountryWhois different from similar tools is its very high accuracy (over 98%), unprecedented speed of processing (a 100 MB log file is processed within one second), regular updates that keep the ever-changing IP address database up-to-date, an array of supported import and export formats, command-line mode, and a convenient interface.

[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](#)

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](#)