S-Tools for Windows Help Contents

Select one from the following list to learn more about that subject:

Command Reference

This section explains the meaning of the menu options available within S-Tools. Choose one from the following list to learn more about the topic:

S-Tools File Menu

The S-Tools file menu contains options for saving and loading wave files, as well as options for hiding and revealing files. Choose one from the following list to learn more about the topic:

Open WAV file...
Save WAV file as...
Hide file...
Reveal file...
Exit

S-Tools Options Menu

The S-Tools options menu contains options for playing sound waves, both the original wave and the wave with a file hidden inside it. It also contains options that control the encryption and decryption of files that you are hiding. Choose one from the following list to learn more about the topic:

Open WAV file... (Ctrl+O)

This command is used to load a WAV file from disk. This is the option you need to use whether you are about to hide a file in the sound wave or you are about to reveal a hidden file from the wave. You should be familiar with the Windows standard file selection box that appears when you select this option.

Any currently loaded sound wave will be lost if you go through with this option and disregard the warnings that S-Tools will give you.

S-Tools understands a limited subset of the Windows WAV file format. That means that you may come across perfectly good WAV files that S-Tools does not recognise. S-Tools has been written to understand the most commonly used subset of the WAV file format. Registered users can send me the offending WAV file and I will do my best to update S-Tools to understand it.

S-Tools currently understands 8 and 16 bit samples, in mono or stereo. It does not understand extra information in the file, other than the sample data. It will complain if it comes across extraneous information such as cueing marks.

When the new sound wave has been loaded you will be shown a graphical representation of it in the main window, together with some information in the status bar at the bottom. This information will tell you the intended playback frequency of the sample, the number of bits per sample, whether it is a mono or stereo sample and also the maximum size file that you can hide within this sound wave. Do bear this number in mind when you come to choose a file that you want to hide !

Save WAV file as... (Ctrl+A)

This option is used to save a WAV file after you have hidden a file inside it. As such, this option will be disabled until you have successfully hidden a file in a wave that has been previously loaded using the Open WAV file... option.

If you really are trying to conceal information then it would make good sense to delete the original WAV file after saving the new one. You don't want a potential enemy finding two apparently identical WAV files with slightly different data do you ?

Hide File... (Ctrl+H)

This option is used to load in and hide a file within the current sound wave that you loaded using the Open WAV file... option. The Windows standard file selector will make another appearance for you to use to select the name of the file that you want to hide. The size of this file must be no greater than the maximum size indicated in the status bar. If you are unsure of the size of the file that you wish to hide then you can use the Windows File Manager program to find out.

If you are having trouble fitting the file that you want to hide inside a sound wave then you might like to try compressing it using one of the popular archiving programs such as PKZIP, ARJ or LHarc.

If you are using the registered version of S-Tools and have decided to encrypt the files that you hide then you will be required to enter a passphrase that will be used to encrypt the file. This passphrase must be greater than 6 characters long and must be entered identically twice in order to confirm it. The encryption systems offered by S-Tools are cryptographically strong. That means that if you forget your passphrase then neither you, or any organisation or government agency can retrieve the data for you.

If the file was successfully hidden then the wave displayed in the main window will change to a mixture of red and black lines. The red areas indicate where S-Tools modified the wave data to hold the hidden file. The black areas indicate where S-Tools, purely by chance, did not have to modify the original wave in order to store the hidden file. There will of course be a trailing black area at the end of the wave where the hidden file ends and the original wave continues.

Reveal file... (Ctrl+R)

This option is used to reveal a hidden file from within the current wave form that you loaded using the Open WAV file... option. Do note that S-Tools cannot mark the wave form in red and black after you retrieve a WAV file from disk since it has no idea that a hidden a file exists within the wave (only you know that), and even if it did it would have no way of knowing how the wave differs from the original.

If you are using the registered version of S-Tools and have decided to encrypt files that you are hiding then you will be required to enter the passphrase that you used to encrypt the file when you hid it. Be sure that the encryption options are set to the same as when you encrypted the file.

When you select this option S-Tools try's to figure out whether it is plausible that a file could have been hidden within the sound wave. It could get this wrong. It is possible that S-Tools can tell you that there is a hidden file when there is not. However, S-Tools will never deny that a hidden file exists when one does. This is of course no problem since you know which of your WAV files have hidden files within them, don't you ?

After confirming the likelihood of a hidden file, you will be presented with a small dialogue box that you can use to choose whether to extract the hidden file to the screen, where you can view it, or to a disk file. The former option is only suitable when the hidden file consists of text. Non-text files will show up as junk in the viewing window.

Do note that the hidden file remains within the wave form after being extracted. S-Tools has no idea what the original wave form looked like and so it cannot be re-constructed. This doesn't matter though, since you can't hear any difference between the long-forgotten original and the modified wave, can you ?

Exit (Alt+F4)

This option exits from S-Tools. If you have a WAV file loaded with something hidden in it, and this has not yet been saved then you will be prompted to save it before S-Tools exits.

Play (Ctrl+P)

This option plays the sound wave after you have hidden a file inside it. You can use this option to see if you can detect any difference between the original sound wave and the one with a file concealed within it.

You need to have installed a sound driver using the *Drivers* option of the Windows Control Panel to be able to play a sound wave.

Play Original (Ctrl+G)

After hiding a file within a sound wave you will doubtless want to compare the modified wave to the original. This option will play the original sound wave.

You need to have installed a sound driver using the *Drivers* option of the Windows Control Panel to be able to play a sound wave.

Encryption: Never

Selecting this option switches off the encryption options. Files that you hide will not be encrypted. Files that you reveal are assumed to be un-encrypted.

Encryption: Prompt

Selecting this option causes S-Tools to ask you whether you are using encryption whenever you hide or reveal a file. This option is only available in the registered version of S-Tools.

Encryption: Always

Selecting this option causes S-Tools to always encrypt files when you hide them inside sound waves. Files that you reveal are also considered to be encrypted. This option is only available in the registered version of S-Tools.

Encryption: Options

Firstly I should point out that this option is for users with an advanced knowledge of cryptography only. The default cryptography options selected by S-Tools provide an excellent level of security and should not need to be changed.

You can use this option to choose the cipher type and mode of operation that S-Tools will use when it encrypts and decrypts files that you hide.

The available ciphers are IDEA, DES, 3DES and MPJ2. The key lengths provided for MPJ2 are 128, 256, 384 and 512 bits.

The modes of operation supported by S-Tools are ECB, CBC, PCBC, CFB and OFB. S-Tools prepends 32 bits of pseudo-random time-dependent garbage to the front of every file that it hides so that two identical files encrypted in CBC mode will never encrypt to the same ciphertext. OFB and CFB have the interesting property of enciphering the first block identically. This means that you could encipher something in CFB mode and then attempt to decipher in OFB mode. S-Tools would report that there is a hidden file but will then decrypt absolute garbage.

I'm not going to say any more here about these options since the default is just right for those without a knowledge of cryptography, and those with a good enough knowledge won't need any further explanation :)

A step-by-step guide to hiding and revealing files

Choose one from the following list to learn more about the topic:

How to hide a file within a sound wave

In order to hide a file you need to be in possession of three pieces of information. These are:

The name of the file that you want to hide.
The name of the WAV file that you want to hide it in.
A name for the new WAV file that contains the hidden file.

If you are experimenting with S-Tools for the first time then you might like to try hiding something inside the ORIGINAL.WAV file that is supplied with S-Tools.

When you've figured out the above three pieces of information you need to follow the following steps.

Select the `Open WAV file' option from the `File' menu. Use the Windows file selection box to choose the name of the WAV file that you want to hide your file in. If the WAV file is one that S-Tools understands then you will see a representation of the sound wave in the main window area. In addition to this, you will see a few extra pieces of information about the file in the status bar at the bottom of the screen. This tells you some miscellaneous things like the playback frequency of the file, the number of bits per sample and, more importantly, the maximum size file that you hide within this WAV file.

Assuming the previous step went ahead without any trouble, you can now choose the file that you want to hide. Select the `Hide file' option from the `File' menu. Now use the Windows standard file selector to choose the name of the file that you want to hide. Assuming that the file is not too large to hide in the WAV file that you loaded, there will be a short delay and then the waveform display will change. The areas marked in red on the waveform are areas of the sound wave that were altered by the concealment process. The areas in black just happened to not have to be altered in order to conceal the file.

Naturally you will now want to save your modified wave file so that you can send it to the person that you are exchanging secret information with (!). To do this, simply select the `Save wave file as' option from the `File' menu. Use the Windows standard file selection box to choose the name of the new WAV file.

Well that's just about all there is to it. Except perhaps one thing. After you've hidden a file inside a wave, you might like to compare the sound of the original file to the sound of the modified one. The two `Play' options under the `Options' menu will do this for you. See if you can spot the difference between the original and the modified version ! Do you think you could spot a concealed file if you didn't have the original to compare to ? No way !

How to reveal a file hidden inside a sound wave

If you are experimenting with S-Tools for the first time then you might like to try extracting the hidden message within the file HIDDEN.WAV. The hidden file is comprised only of text, so you can use the `Screen' option to display the message.

Revealing a hidden file is even easier than hiding a file. All you need to do is to follow these steps.

Select the `Open WAV file' from the `File' menu. Use the Windows standard file selector to choose the name of the WAV file that contains the information that you want to extract. The main Window will change to display information about the WAV file, and a representation of its wave form.

Now choose the `Reveal file' option from the `File' menu. S-Tools will now try and guess whether the sound wave has a hidden file within it. It is quite possible that S-Tools will tell you that a there could be a hidden file in a wave when there isn't one, but never the other way around. It will never tell you there is no hidden file when there is one.

If it thinks the wave might have a concealed file then you will be shown a dialogue box with the length of the file in it, together with two buttons that allow you to either save the concealed file to disk or to show it in a window. Naturally, the latter option is only relevant if the file consists only of text. If you choose to save the concealed file to disk then you should use the Windows standard file selector to select a name for the extracted file. Please note that it is not possible to reconstruct the original sound wave, but then you couldn't hear the difference anyway could you ?

About S-Tools

Since the advent of computers there has been a vast dissemination of information, some of which needs to be kept private, some of which does not. S-Tools (Steganography Tools) brings you the capability of `hiding' files within Windows sound wave (.WAV) files. The modified .WAV file that contains your hidden file will not sound any different to the human ear than the original file. The modified file does not increase or decrease in size, it remains the same. I suppose you could look at this as a kind of infinite compressor for the file that you are hiding, since you can quite happily delete it after you've hidden it, extracting it from the WAV file whenever you need it.

See also:

Limitations
Information for the paranoid

Limitations

The WAV file format is quite complex and is extensible. S-Tools supports the most common subset of the WAV format, known as Microsoft PCM format. S-Tools supports 8 and 16 bit samples, in mono or stereo. It does not support files that contain extra information other than the wave data itself. Luckily nearly all WAV files (including those supplied with Windows 3.1) are of this limited form.

I have downloaded several hundred example WAV files from a popular archive site and S-Tools quite happily dealt with them all. It would seem that the most popular WAV format is 8-bit mono with a playback frequency of 11kHz.

You should never use any `lossy' compressor programs on WAV files that have files hidden within them, this will result in your hidden file being corrupted. I have not seen any such programs, but I don't doubt that they exist.

Information for the paranoid

If you intend to use S-Tools for hiding sensitive information then you should be aware of a few basic facts.

Firstly, you need to assume that any potential enemy has his own copy of S-Tools and is aware that you might be trying to hide information from him. You need to be able to say "I am not hiding anything, all my wave files are part of my extensive sound sample library". In order to be able to achieve this you should always use the encryption option provided by the registered version of S-Tools. If you are using the shareware unregistered version of S-Tools then you need to take a few extra measures:

You need to encrypt your files with an encryption package that uses a strong encryption algorithm. Such a package should be able to perform "raw" encryption of files, i.e. it should not tag any "magic numbers" on the front of encrypted files that are used to identify the file as being encrypted with that package. If it did then our aforementioned enemy would immediately know what kind of file he has just extracted. We want him to think that he's got junk, and not a hidden file at all.

The PGP package, originally by Phil Zimmerman satisfies the first requirement of strong encryption, but unfortunately it tags magic numbers on to the front of its encrypted files. There is a new development called Stealth-PGP that does away with the magic number identifiers, and this would appear to satisfy all our conditions. If you can get hold of this package then I would recommend that you do so.

I have not included encryption in the shareware version of S-Tools because it is illegal to export strong encryption packages from the U.S.A. and this would make distribution of the shareware version via U.S. based BBS's and ftp sites illegal. It is, however, perfectly legal to import such software into the U.S. so I would have no trouble sending you the registered version. Daft ? You bet, complain to your local politician !

Shareware information

S-Tools is shareware. That means that if you find it useful and would like to continue to use it after a reasonable trial period, which I consider to be about one calendar month, then you should register your copy of the program with me.

The registration fee for S-Tools is 15 UK pounds sterling. To register S-Tools, send a cheque drawn against a UK bank, International Money Order, International Postal Order or Sterling travellers cheques for 15 pounds to the address below:

Andy Brown
28 Ashburn Drive
Wetherby
West Yorkshire
LS22 5RD
United Kingdom

For your registration fee you will receive a printed manual, a personalised copy of the program, and a copy of the `C' source code.

I can be reached by e-mail at **asb@cs.nott.ac.uk** until June 1994.

Credits

The algorithm used in the derivation of cryptographic keys and variables is hereby identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm"

IDEA is registered as the international patent WO 91/18459 "Device for Converting a Digital Block and the Use thereof". For commercial use of IDEA, one should contact

> ASCOM TECH AG
> Freiburgstrasse 370
> CH-3018 Bern, Switzerland

The MPJ2 Encryption Algorithm may be used for any legal purpose without payment of royalties to the inventor or his employer. Some nations may restrict the use, publication, or export of strong encryption technology. Comments, questions, and reports of possible weaknesses should be sent to the author at:

Mike Johnson
PO BOX 1151
LONGMONT CO 80502-1151
USA

BBS: 303-938-9654
Internet: mpj@csn.org
CompuServe: 71331,2332

Steganography is the ancient art of hiding information in some otherwise inconspicuous information. Many years ago people used to use illustrations to conceal messages. The idea being that one party could send the illustration to the other in reasonable confidence that if the messenger was questioned then the illustration would not arouse any interest from his enemies.

Pretty Good Privacy, a free package for public key encryption and authentication of electronic mail messages. It can also perform strong conventional encryption on ordinary files. The U.S. authorities are not happy about PGP because they (probably) cannot break its encryption algorithms.

International Data Encryption Algorithm. The successor to the DEA, invented in Switzerland. The patent allows non-commercial use. This block cipher has a 128 bit key and operates on 64 bit blocks. Utilised by the ever-popular PGP package.

Data Encryption Standard. For 20 years the U.S. standard for non-classified information. Still safe from all but very large institutions and Governments. Operates on 64 bit blocks with a worryingly short 56 bit key. I do not recommend that you use ordinary DES unless you need cryptographic compatibility with some other package.

A variation on DES that increases its security by enciphering data 3 times using two encryptions and one decryption with a second key. The security of DES is considerably increased by this approach, although maybe not to the full 112 bits that one would expect.

A relatively recent cipher that has a variable key length and operates on 128 bit blocks. It's inventor, Mike Johnson, believes it to be at least as strong as IDEA. MPJ2 has not stood up to as much cryptanalysis as IDEA, and certainly not DES, but this cipher looks very promising.

Electronic Code Book. Blocks are enciphered "in place" with no additional obfuscation.

Cipher Block Chaining. Previous ciphertext blocks are combined with plaintext blocks before encipherment. Provides good obfuscation of repeating blocks in the plaintext.

Propagating Cipher Block Chaining. PCBC extends or propagates the effect of a single bit error in the cipherstream throughout the remainder of the decrypted text stream after the point of error.

Cipher Feedback mode. One of the four NBS standard modes. Each ciphertext character is functionally dependent on previous ciphertext characters.

Output Feedback mode. A feedback register is used as input to the block encryption algorithm. Has the property that encryption and decryption are the same. No separate decryption is required.