

WEP File Editor

User Handbook

Rev. 1

February, 2004 All Rights Reserved ©

Features :

- Loads huge WEP encrypted Files in a couple of seconds
- Import (load) trace files data in the following format : *.lfc; *.enc; *.snp
- Export (save) files in the following format : LibPCap file format *.cap, Microsoft Network Monitor Format (*.Cap), Network Associates Sniffer (DOS) Format (*.Enc), Network General's NetX'Ray Format (*.Cap), RFC 1761 Snoop Format (*.Snp)
- Advanced features for WinAirsnot Files
- Import and Export WinAirsnot Trace File data in the following format : *.Trc
- Import and Export WinAirsnot WEP File format in the following format : *.wep
- Easy to use HEX editor with standard cut/copy/paste functions
- Full Find functionality for many different data types with a powerful Find feature
- Data engine allows opening/copying/pasting huge WEP files instantly in most cases
- Easily loads files over 4Gb (if supported by the file system)
- GoTo (or jump) feature that allows you to move to any location in the file
- Full Undo and Redo support
- Expanding (inserting several parts) files, deleting parts of files etc.. with undo support
- Editor allows data to be edited in many different formats
- Computes Check Sum / Hash algorithms including CRC-16-CRC-32, MD2, MD4, MD5
- HEX calculator provided with the standard Editor program
- printing with full print preview, headers, footers and margins

Data Engine :

WEP File Editor uses a powerful data engine for all of its file operations. No other HEX editor works better with huge files than WEP File Editor. This system allows files over 4 GB to be opened instantly. The *Copy* and *Paste* commands can be used to copy huge blocks of encrypted data to the clipboard, and often these operations can be performed instantly. *Undo*

and *Redo* are also supported on all hex editing operations (even for large blocks of data). Depending upon what modifications were made, sometimes even huge files can be saved extremely quickly to disk. Structures are defined in a text file that closely resemble WEP style structure definitions.

With WEP File Editor, you can:

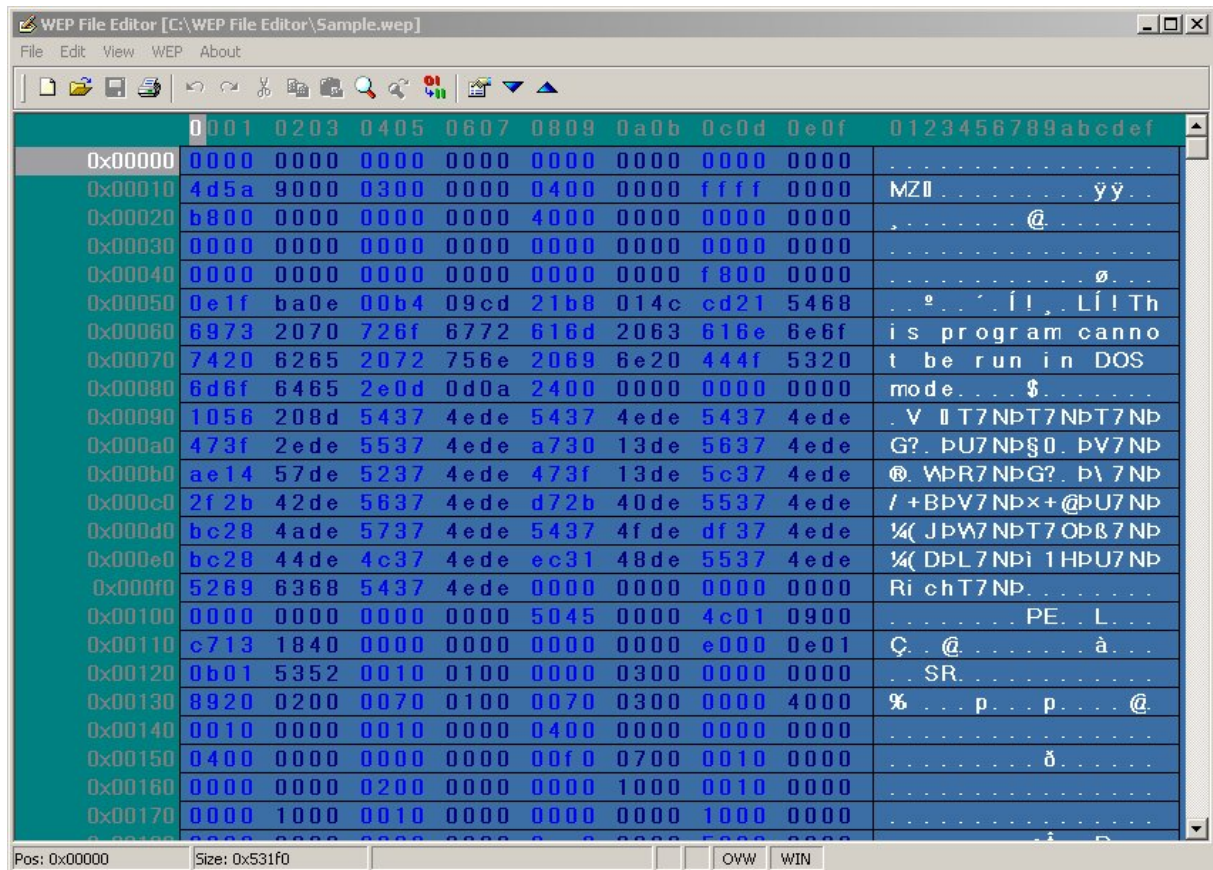
- Use a powerful, highly customizable, and easy to use editing environment.
- View and modify in its natural and native structured form through the Structure Viewer.
- Directly edit sectors of your floppies and hard disks.
- Hex Edit files WEP or other files
- Print high quality hex dumps with customized headers, footers, and fonts.
- Cut, Copy, Paste, Insert, Delete, Fill, Insert File, and multilevel Undo/Redo.
- View and Edit raw binary data as decimal values of the WEP files
- Interpret values in either Little Endian (e.g. Intel) or Big Endian (e.g. Motorola) byte ordering.
- Manipulate data (translate characters...)
- Insert external file contents or save a block of data as a new file.
- Visually see changes in your choice of color
- Import and Export WinAirsnot trace files
- Easily navigate around documents and sectors using the goto command.
- View text interpretations under ASCII, DOS, EBCDIC, Macintosh, Window, and Unicode character set filters.
- View Character Distributions and export results as Tabbed Text or Comma Separated Values.

Hex/ASCII Editing:

A WEP file can be edited from either the hex or ASCII display. The cursor can be toggled between hex and ASCII with the tab key or hex/ASCII can be chosen by clicking the mouse in the particular region.

You can tell what area you are editing by looking at the caret shape. A vertical blinking caret is displayed in the active area and a solid underline caret is displayed in the inactive area.

You can use the arrow keys to navigate around the document in either the hex or ASCII display. You will notice that the left and right arrow keys will move one byte (2 hex digits) at a time in the hex display.



Clipboard Functionality:

Cut, Copy, and Paste operate in a similar manner to other editors. Paste Special allows you choose from and paste any of the standard Windows Clipboard formats currently available into a file.

Undo & Redo

Undo and Redo allows you to reverse the most recent editing operation(s).



Inserting/Deleting:

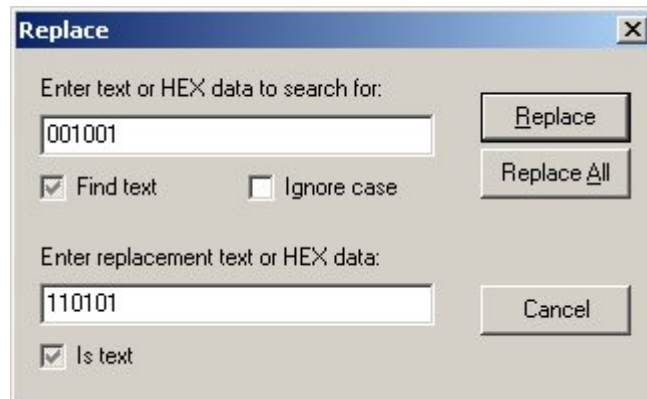
Automated Inserting allows a specified number of bytes to be inserted at the cursor position with any hex value. Deleting simply deletes the highlighted bytes. Normal editing can be done in either insert (INS) or overwrite (OVR) mode. Insert mode will automatically insert hex values entered at the cursor position, while overwrite mode will overwrite existing bytes at the cursor position with hex values entered. The current mode is shown in the far right pane of the status bar and is toggled with the insert (Ins) key.

Select Block/Select All:

A block of hex can be automatically selected at the cursor position using the Select Block feature and specifying either the size of the block or the ending position. In either case the block starts at the cursor position. Select All automatically selects the entire file.

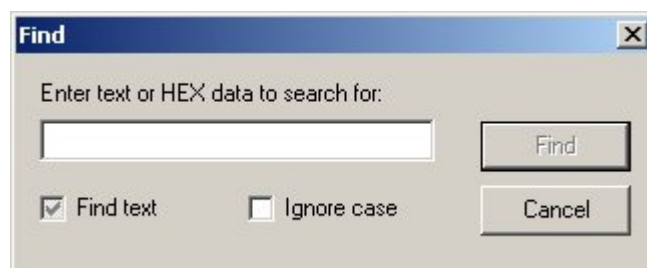
Replace

The Replace Utility, located under the Edit menu, works in the same manner as the Find. The Replace Utility allows for different sized search and replace strings, and has a Replace All option. In addition, the Replace Utility offers an option to "Pad String with Nulls" when replacing ASCII. This is useful if you are replacing a string with a shorter string and wish to leave the file size intact. The replace string will be padded with NULL chars until it is equal in size to the search string, before substituted.



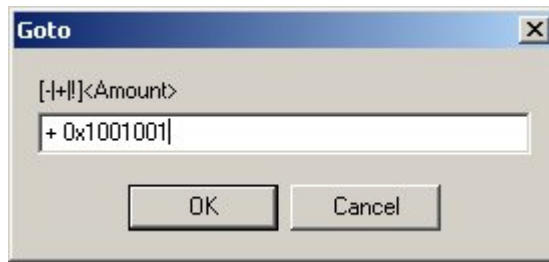
Find Utility

The Find Utility, located under the Edit menu, allows you to search for a hex, ASCII, decimal values, or bitmasks within a file or sector. If a hex value is the search type, it is assumed to be raw hex (no options are offered). If a decimal value is the search type, options are given for data type (byte, short, long, etc.) and byte ordering (Little Endian vs. Big Endian). If an ASCII value is the search type, the options given are for a case sensitive search and to search for a Unicode string. There are toolbar buttons that can be used as a shortcut for the Find Utility:



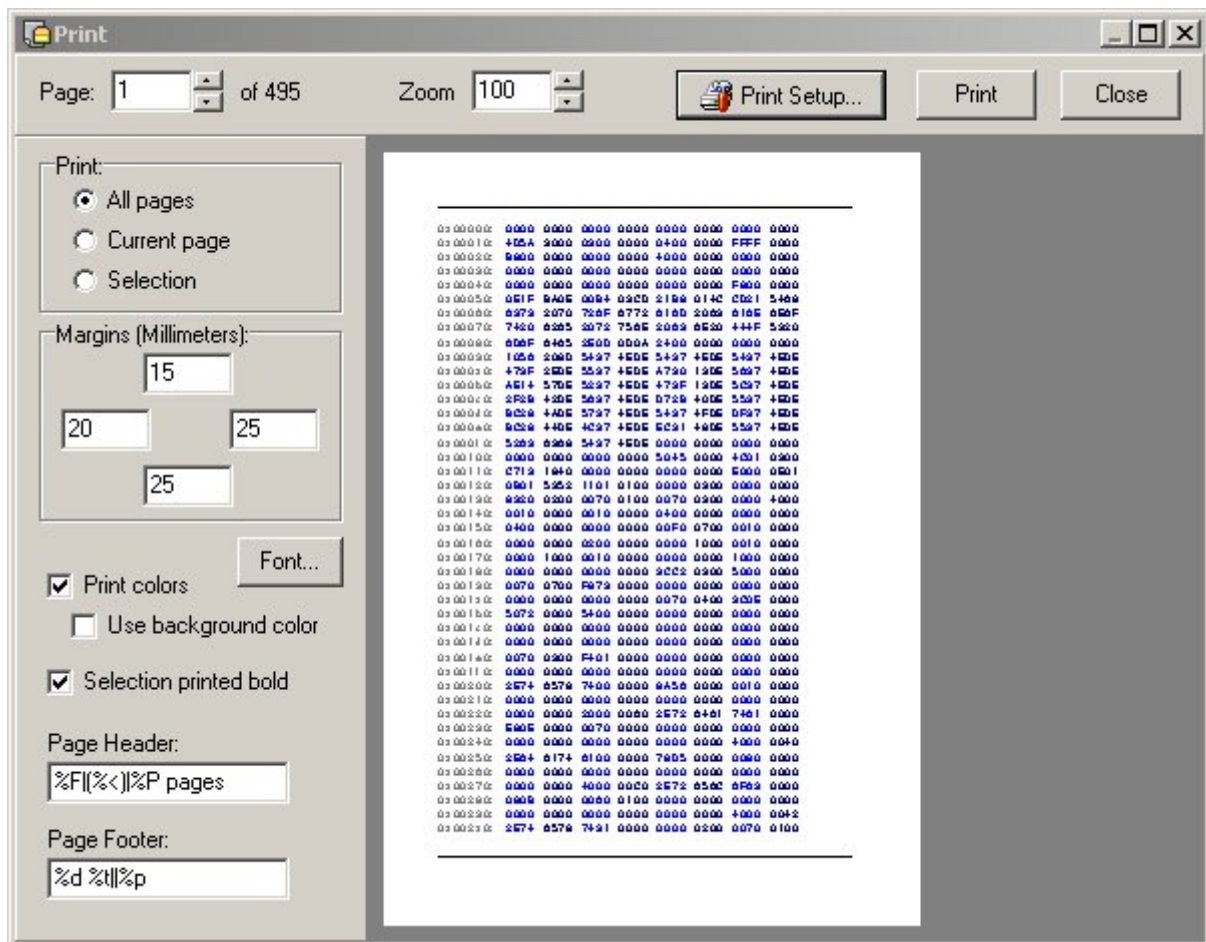
Goto Utility

The Goto Utility, located under the Edit menu, allows the user to logically move throughout the file. The Goto Utility can be used to move from the beginning of the file, the cursor position, or the end of the file. The number of bytes to move can be specified in either hex or decimal (with hex values always positive). When moving from the cursor position a negative decimal value may be entered to move backwards (This is the only time a negative value is allowed). In moving back from the end of the file, a positive number moves back into the file.



Print Setup

WEPEditor provides the ability to print customized printouts (hex dumps) with a Page Setup feature. Using the Page Setup users can use a custom header and/or footer, printer font, and margins.



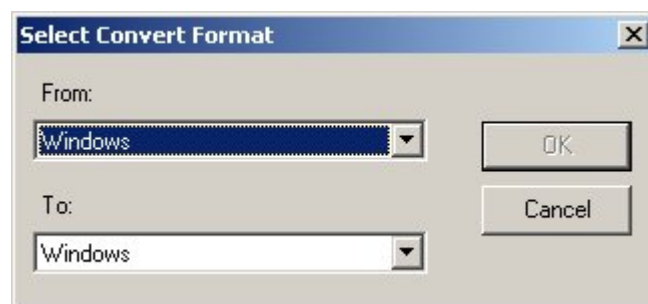
Header/Footer:

The header and footer can consist of any valid text. Using special codes, users can print the filename or full path, current page number, total pages, and time and date in a number of different formats. In addition, any portion or all of the headers and footers can be left, center, or right justified.

Convert Format

WEP File Editor is able to convert from and to these formats :

- WINDOWS
- DOS 8-bit
- ASCII 7-bit
- Macintosh
- EBCDIC Codepage 38
- Custom Translation

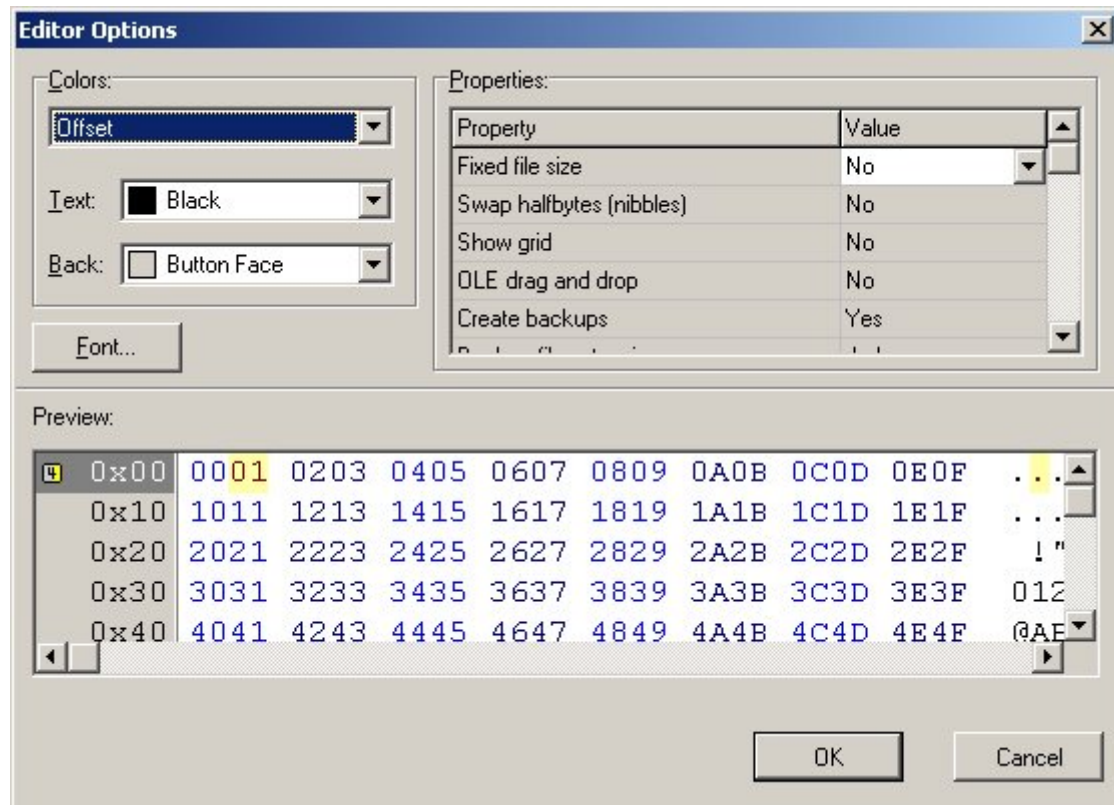


Options

Several options can be selected in the Editor Options. These options are listed hereafter :

- Fixed File Size
- Swap Halfbytes (nibbles)
- Show Grid
- OLE drag and drop
- Create Backups
- Backup file extension
- Clipboard text data has HEX format
- Preserve clipboard contents on close
- Support foreign clipboards format

- Use mouse wheel for zooming
- Substitute white spaces by
- Max Size of Undo buffer (bytes)
- HEX numbers in lower case
- 3D border
- Show Ruler



WEP File Analyzer

Additional Features WEP File Analyzer

February 2004, All Rights Reserved ©

Note to the "WEP File Editor" program users

Additional Features that follow in this User Handbook are not available in the WEP File Editor software !

A screenshot will remind you that you are using the Editor program, without enhanced WEP File Analyzer options.



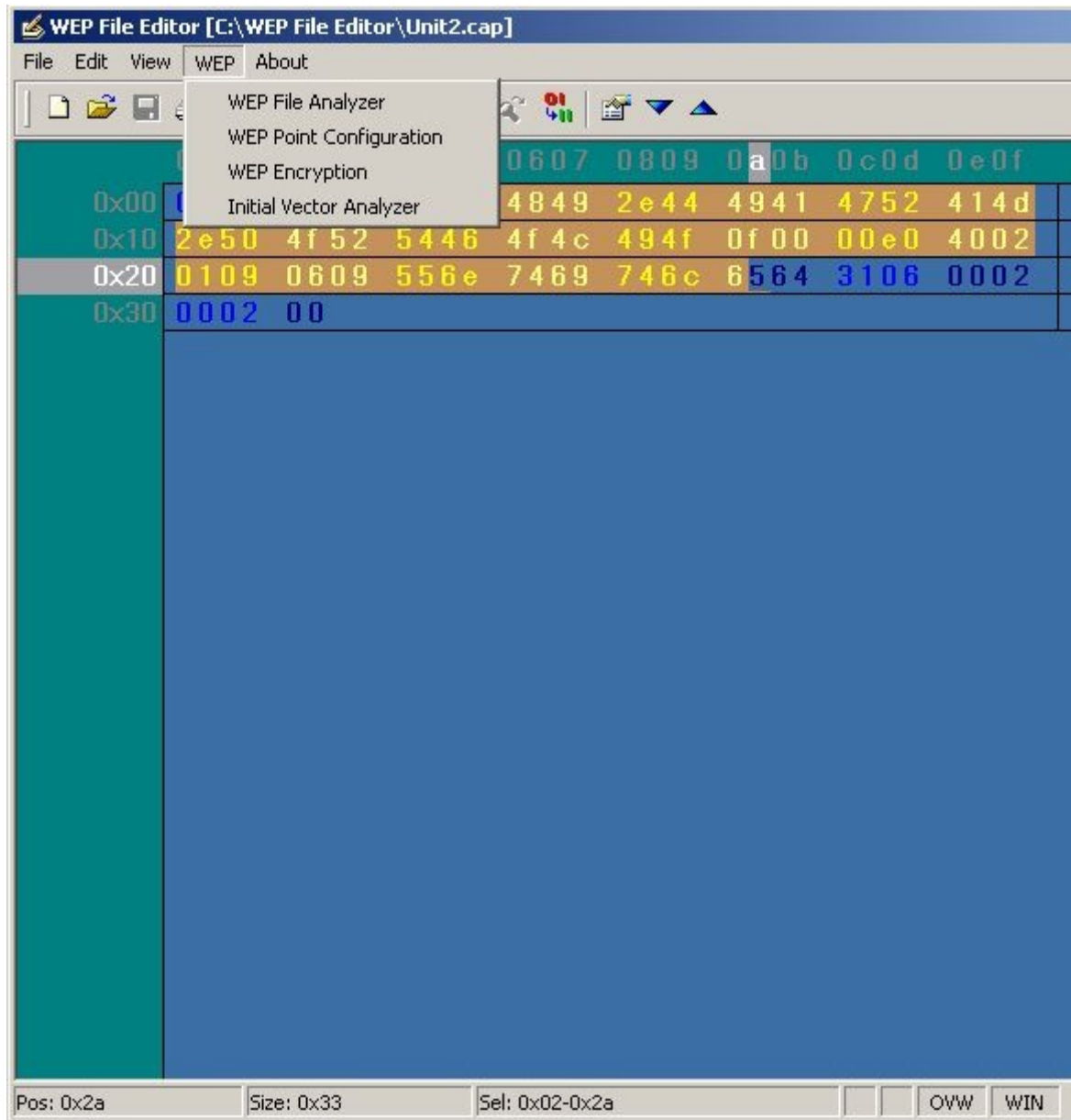
WEP Security Key Background

The Wired Equivalent Privacy protocol (WEP) is the standard for authentication and encryption used in the 802.11b wireless Ethernet protocol. For encryption, WEP uses the RC4 algorithm.

The WEP algorithm protects wireless communication from eavesdropping. WEP prevents unauthorized access to a wireless network. WEP relies on a secret key shared between a laptop with wireless Ethernet card (or mobile station) and an access point (the base station). The WEP secret key encrypts packages before they are transmitted. WEP uses an integrity check to prevent packets being modified in transit. Most installations use a single WEP key between the mobile stations and access points. Multi WEP key techniques in network management enhance the security.

WEP encryption is the translation of data into a secret code. The WEP encryption key is used to provide wireless clients with confidentiality and authentication in an IEEE 802.11 b environment. WEP encryption is the most effective way to achieve data security. To read a WEP encryption on file you need a secret key or password to decrypt it. Unencrypted data is called plain text, the cipher text refers to encrypted text. There are two main types of WEP encryption, asymmetric WEP encryption or public key WEP encryption and symmetric WEP encryption. To preserve confidentiality, WEP encryption uses RC4 encryption for the 802.11 frame with shared keys. WEP encryption uses the RC4 encryption method and the conversion of plain text, cipher text and the initialization vector (IV) that is used to turn the plain text into cipher text. This can in turn be decoded into the RC4 keystream. WEP encryption depends on a shared key, its distribution and the WEP encryption algorithm. The WEP encryption standard employs 40-bit encryption as well as a 128-bit WEP encryption option. Some WEP wireless vendors offer both WEP encryption options. By using the 128-bit keys, WEP encryption ensures that your data is as secure as unencrypted wired Ethernet.

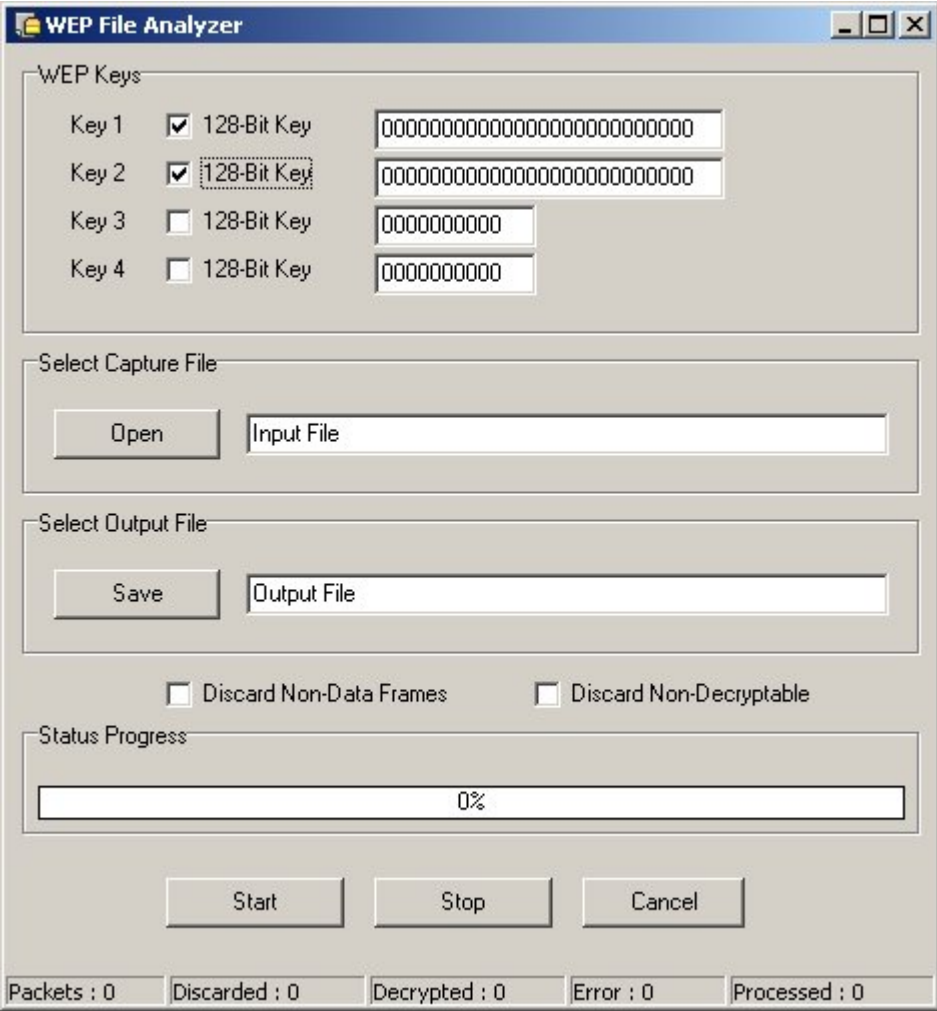
WEP File Analyzer Panel (screenshot)



The WEP File Analyzer is a Trace File Decrypter. This is a complex but very handy tool. It can be used to decrypt WEP'ed trace files off-line. This permits access to trace files that were captured via a tool that does not support WEP, and to data that was captured at a time when the WEP key(s) were not known. This WEP File Analyzer can be used in complement to WinAirsnot program for example.

IMPORTANT! This software performs WEP decryption and Analysis, not WEP key recovery. This is not a cracking tool ! The session keys must be known and input to the program before decryption can successfully occur.

The WEP File Analyzer panel (screenshot) can be viewed here below :



Enter the WEP Keys.

Enter the keys to be used to decrypt data frames contained in the file. You must know the keys in advance. The WEP File Analyzer will not recover keys automatically. The default is 64-bit encryption. To enable 128-bit operation, check the box labelled "128-Bit" next to the key entry field. The entry box will expand to permit the entry of the larger keys. WEP keys are made up of HEX digits. The characters "0123456789ABCDEF" are all valid HEX digits. 64-bit keys are comprised of 10 HEX digits. 128-bit keys are comprised of 26 HEX digits.

WEP Key setting is set to :

- Key1 : 64-bit or 128-bit Key
- Key2 : 64-bit or 128-bit Key
- Key3 : 64-bit or 128-bit Key
- Key4 : 64-bit or 128-bit Key

NOTE : The configuration possibilities make it clear that the WEP Key Analyzer program can support up to four different keys simultaneously. This is in accordance with the 802.11 standard, which defines four so-called "default keys". These keys can be used to smooth the transition from the usage of one key to usage of a next key. The general requirement for two cards to transmit encrypted between each other is that they share a common key value at the same key-index number in the 4-key area at the moment of transmission. The key-index of the key that was used for encryption is transmitted in clear-text in the header of the message, and will be used at the receiving side to determine which of the 4 keys to use for decryption.

So it is not mandatory that both sides have the same active set of 4 keys. As long as there is one key in common, they can communicate, provided they both use that common key.

Select the Capture (Encrypted) File.

Select the trace file containing WEP-encrypted frames that you want to render into plain-text. Several popular trace file formats are supported, including WinAirsnot File Format (WEP), LibPCap, Snoop, Sniffer-DOS, and NetXRay.

Import (load) trace files data in the following format : *.lfc; *.enc; *.snp
Import WinAirsnot Trace File data in the following format : *.Trc

Select the Output File.

Select the name of the file where the processed data will be stored. You can also select the file format. All of the trace file types mentioned above are supported. It is not required that the output file be the same type as the input file.

Export (save) files in the following format : LibPCap file format *.cap, Microsoft Network Monitor Format (*.Cap), Network Associates Sniffer (DOS) Format (*.Enc), Network General's NetX'Ray Format (*.Cap), RFC 1761 Snoop Format (*.Snp)

Export WinAirsnot WEP File format in the following format : *.wep

Select Options.

Select the options to be activated while decrypting :

- Discard non-data frames
- Discard non-decryptable frames

You can configure the option to pass only data frames through to the output file. This is useful if you are not interested in examining any of the 802.11 management or control functions, and would like to have a more compact output file. You can also specify how the WEP File Analyzer will handle frames that fail to decrypt correctly. They may either be discarded or passed transparently through to the output file. If they are passed through, then the output file may be reprocessed with another set of keys, thereby recovering more data.

Start Decryption.

Select the start button to begin the decryption process. WEP Decryption Steps are following :

- _ Use key number to get private key
- _ Use sent IV to generate keystream
- _ RC4(IV,Key)
- _ XOR received ciphertext with keystream
- _ Get ICV+Payload
- _ Compute ICV on Payload
- _ If new ICV then sent ICV, then packet good

Stop.

Select the stop button to stop the actual analysis process. The program records all data in the file. All data are stored in the saved File.

Status Progress.

This Status progress indicates the progress of the data analyzed. The program performs checks of file integrity, analyzes data-packet and then computes all data for decrypting.

IMPORTANT! This software performs WEP decryption and Analysis, not WEP key recovery. This program is able to decrypt very huge files, in other way such analysis could take few minutes to several hours ! Be aware that we are NOT responsible of any unsuccessful decrypting procedure due to the kind of file you want to decrypt, or any use you want to perform with this enhanced functions of WEP File Analyzer Program. WEP File Analyzer is not a cracking tool ! The session keys must be known and input to the program before decryption can successfully occur.

Decryption is Completed.

After the WEP File Analyzer has finished processing the trace file, the fields in the status bar at the bottom of the dialog will be updated with the tally of frames processed:

- Packets : Processing Packet number
- Discarded : Packets which are not analyzed or decrypted
- Decrypted : Packets which are currently analyzed or decrypted
- Error : Error occurred
- Processed : Total of analyzed packets

WEP Encryption Option Overview

An 802.11b frame is composed of a header which contains information specific to the 802.11b protocol (source/destination MAC address, type of frame, etc.) as well as a payload. The payload contains a IP header, a TCP header, and a data payload. When encrypting a frame, the first step is creating an Initial Chaining Vector (ICV), and appending this ICV to the end of the payload. The ICV is simply a 32-bit CRC of the payload contents. After the ICV is created, a 24-bit Initialization Vector (IV) is generated. The IV is used to initialize the RC4 algorithm prior to encryption. One of four encryption keys (40 bits each, stored on the client) is then selected and this key number (8 bits) is appended to the IV. In many implementations of WEP, the user can instead chose to use a single 104-bit key for better encryption. It is important to note that most keys are generated by software included with the 802.11b wireless card.

Often, client software will list a choice between 64 or 128 bit encryption. This simply refers to the size of the key plus the size of the IV – the key size remains 40 or 104 bits, respectively.

The WEP encryption feature offers encryption of data transmissions, using a method specified in the IEEE 802.11 standard.

WEP Encryption Steps

- _ ICV computed
- _ Checksum of payload (i.e., plaintext) using CRC
- _ Select encryption key
- _ One of four keys selected
- _ Generate IV
- _ Use RC4 to generate a keystream RC4(IV,Key)
- _ Note IV is prepended to key
- _ Concatenate ICV to payload, then XOR with the generated keystream to get ciphertext
- _ Send IV+keynumber+ciphertext over the air
- _ Key number is the key selected in the second step

WEP Encryption Panel :

Encryption WEP Key setting is set to :

- 64-bit shared Key
- 128-bit shared Key
- 256-bit shared Key

WEP Key Entry : Passphrase or Manual Entry

WEP File Analyzer asks the user to enter a phrase and generates a full 64 to 256-bit key based on this phrase, saving the user from manual key entry.

WEP Encryption

WEP Encryption Setting

Encryption (WEP) algorithm: 128-bit shared key

WEP Key Entry

Create with passphrase

Passphrase: This is my Passphrase

Manual Entry

Key 1	6a	3e	c4	9b	37
Key 2	7e	37	3a	c8	8f
Key 3	00	a8	4e	4a	b9
Key 4	78	09	ab	9b	7b

Choose Default to operate: Key 2

Status Progress: 0%

Output File: Save... Start Stop Cancel

Packets : 0 Discarded : 0 Decrypted : 0 Error : 0 Processed : 0

Manual Entry :

One to four encryption keys must be entered in the panel. These keys will be used to encrypt data file. The format of entering the key values is either in textual format or in hexadecimal format (an entry starting with "0x" will be interpreted as Hexadecimal). A text string is translated in the ASCII values associated with each character.

The user must assign one of the entered keys as the designated key for encrypting all packet transmission. This is done by selecting the appropriate number from the pull-down list "Choose Default to operate".

Choose Default (key) to operate :

WEP Key setting is set to :

Choose the default key to operate (Key1 to Key4).

NOTE : The configuration possibilities make it clear that the WEP Key Analyzer program can support up to four different keys simultaneously. This is in accordance with the 802.11 standard, which defines four so-called "default keys". These keys can be used to smooth the transition from the usage of one key to usage of a next key. The general requirement for two cards to transmit encrypted between each other is that they share a common key value at the same key-index number in the 4-key area at the moment of transmission. The key-index of the key that was used for encryption is transmitted in clear-text in the header of the message, and will be used at the receiving side to determine which of the 4 keys to use for decryption. So it is not mandatory that both sides have the same active set of 4 keys. As long as there is one key in common, they can communicate, provided they both use that common key.

Select the File to be saved.

Select the name of the file where the processed data will be stored. You can also select the file format. All of the trace file types mentioned above are supported.

Export (save) files in the following format : LibPCap file format *.cap, Microsoft Network Monitor Format (*.Cap), Network Associates Sniffer (DOS) Format (*.Enc), Network General's NetX'Ray Format (*.Cap), RFC 1761 Snoop Format (*.Snp)

Export WinAirsnot WEP File format in the following format : *.wep

Start Encryption.

Select the start button to begin the encryption process.

Stop.

Select the stop button to stop the actual analysis process. The program records all data in the file. All data are stored in the saved File.

Status Progress.

This Status progress indicates the progress of the data encrypted. The program performs checks of file integrity, analyzes data-packet and then computes all data for encrypting.

WEP Point Configuration Panel

WEP Point Configuration

Edit WEP Key Set

10 HEX digits (0-9, A-F) Check CRC

Key 1 CC1 Enable Encryption Key 1

Key 2 CC2 Enable Encryption Key 2

Key 3 CC3 Enable Encryption Key 3

Key 4 CC4 Enable Encryption Key 4

Encrypt Data

Deny non encrypted data XORing Data

Encrypt File using Key

Key 2

Status Progress

Checking File Integrity. Please Wait...

5%

Load... Save... Start Cancel

Packets : 0 Discarded : 0 Decrypted : 0 Error : 0 Processed : 0

Enter the WEP Keys.

Enter the keys into hexadecimal format (0-9 and A-F) to be used to decrypt data frames contained in the file. You must know the keys in advance. WEP keys are made up of HEX digits. The characters "0123456789ABCDEF" are all valid HEX digits. 64-bit keys are comprised of 10 HEX digits. 128-bit keys are comprised of 26 HEX digits.

WEP Key setting is set to :

- Key1 : Check CRC checksum for that key (CC1) – Enable or not the encryption Key.
- Key2 : Check CRC checksum for that key (CC2) – Enable or not the encryption Key.

- Key3 : Check CRC checksum for that key (CC3) – Enable or not the encryption Key.
- Key4 : Check CRC checksum for that key (CC4) – Enable or not the encryption Key.

Start Encryption.

Fill in the various fields as described in the above sections and when you are ready, select the "Start" button to begin the encryption process.

Stop.

Select the stop button to stop the actual analysis process. The program records all data in the file. All data are stored in the saved File.

Status Progress.

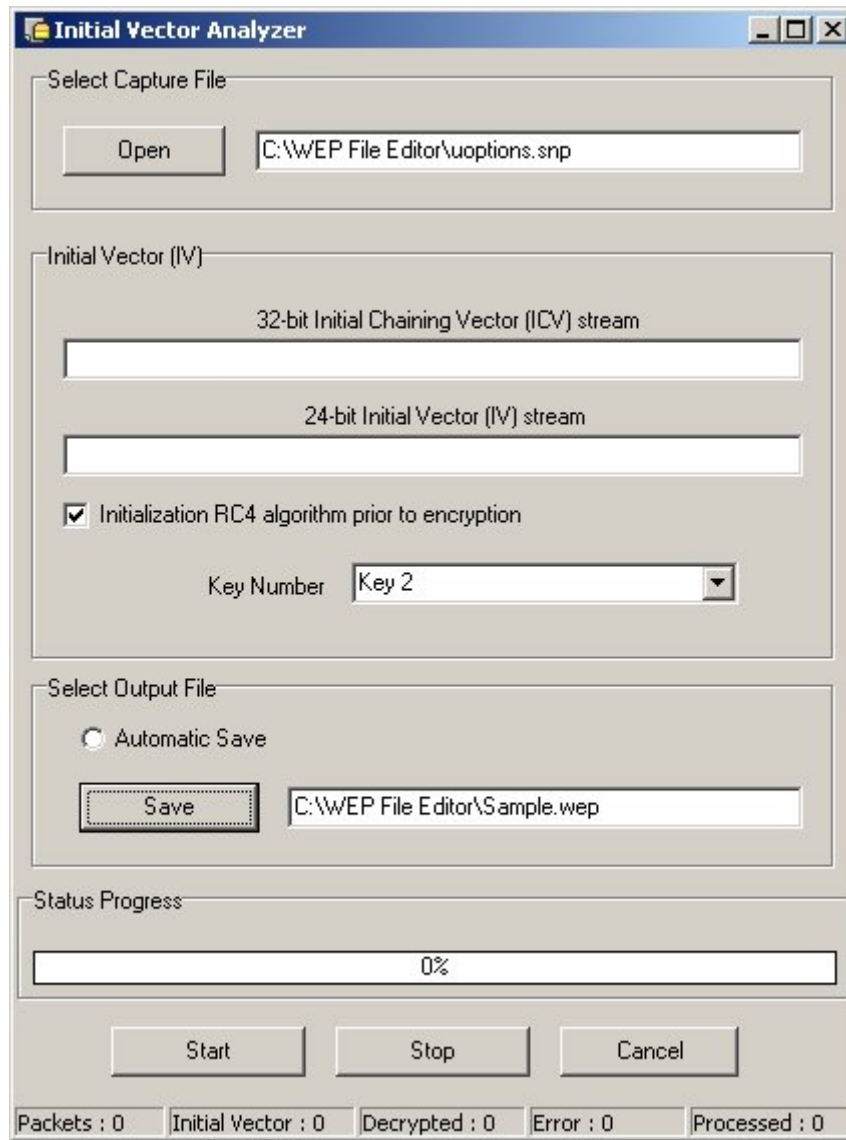
This Status progress indicates the progress of the data encrypted. The program performs checks of file integrity, analyzes data-packet and then computes all data for encrypting.

Initial Vector Analyzer (IV) Panel

An 802.11b frame is composed of a header which contains information specific to the 802.11b protocol (source/destination MAC address, type of frame, etc.) as well as a payload. The payload contains a IP header, a TCP header, and a data payload. When encrypting a frame, the first step is creating an Initial Chaining Vector (ICV), and appending this ICV to the end of the payload. The ICV is simply a 32-bit CRC of the payload contents. After the ICV is created, a 24-bit Initialization Vector (IV) is generated.

The IV is used to initialize the RC4 algorithm prior to encryption. One of four encryption keys (40 bits each, stored on the client) is then selected and this key number (8 bits) is appended to the IV. In many implementations of WEP, the user can instead chose to use a single 104-bit key for better encryption. It is important to note that most keys are generated by software included with the 802.11b card. The software asks the user to enter a phrase and generates a full 40 or 104 bit key based on this phrase, saving the user from manual key entry. Often, client software will list a choice between 64 or 128 bit encryption. This simply refers to the size of the key plus the size of the IV – the key size remains 40 or 104 bits, respectively.

Using the IV and key, the RC4 cipher is initialized and its output XOR-ed with the cipher text. A plaintext frame and ICV are the output. As a final check, the CRC of the plaintext payload is re-calculated and compared to the original CRC stored in the ICV.



Initial Vector Panel Screenshot

Select the Capture (Encrypted) File.

Select the trace file containing WEP-encrypted frames that you want to be analyzed. Several popular trace file formats are supported, including WinAirsnot File Format (WEP), LibPCap, Snoop, Sniffer-DOS, and NetXRay.

Import (load) trace files data in the following format : *.lfc; *.enc; *.snp
Import WinAirsnot Trace File data in the following format : *.Trc

Select The Initial Vector Stream

Select a 32-bit Initial Chaining Vector Stream and a 24-bit Initial Vector stream. Using the IV and key, the RC4 cipher is initialized and its output XOR-ed with the cipher text.

Select the File to be saved.

Select the name of the file where the processed data will be stored. You can also select the file format. All of the trace file types mentioned above are supported.

Export (save) files in the following format : LibPCap file format *.cap, Microsoft Network Monitor Format (*.Cap), Network Associates Sniffer (DOS) Format (*.Enc), Network General's NetX'Ray Format (*.Cap), RFC 1761 Snoop Format (*.Snp)

Export WinAirsnot WEP File format in the following format : *.wep

Start IV process stream.

Fill in the various fields as described in the above sections and when you are ready, select the "Start" button to begin the analysis process.

Stop.

Select the stop button to stop the actual analysis process. The program records all data in the file. All data are stored in the saved File.

Status Progress.

This Status progress indicates the progress of the data processed. The program performs checks of file integrity, analyzes data-packet and then computes all data.