

```

*****
*****
**
**                               Hi ew Documentation
**                               =====
**                               (PDF Conversion by Thomas Antoni -- www.qbasic.de)
**
** Contents
** -----
** - Help File
**   . Edit searching string
**   . Edit string
**   . Text view
**   . Hex view
**   . Hex edit
**   . Bits edit
**   . Code view
**   . Code edit
**   . MZ-Header view
**   . MZ-Header edit
**   . NE-Header view
**   . NE Segment table flags
**   . LE/LX-Header view
**   . LX Object table flags
**   . PE-Header view
**   . PE Object table flags
**   . NLM-Header view
**   . Input/change base offset
**   . Crypt
**   . LE DDB Entry
**   . File list
**   . History files
**   . Get block from history files
**   . Last section
** - What's new in release 6.11
**   1. About HIEW
**   2. Assembler mode
**   3. Basing
**   4. Block operations
**   5. Video modes
**   6. Status bar
**   7. Keys
**   8. Bookmarks
**   9. Jumps (call/jmp) in the disassembler mode
**  10. Search/replace operations
**  11. Crypt operations
**  12. INI file
**  13. SAV file
**  14. XLT file structure
**  15. Command line
**  16. History
** - License Conditions
**
*****
*****

*
*
*                               [Hi ewHel p 5.01]
*
*****

```

[illegible]









```
; o MZ-Header view o
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE ¼
;
[HeaderMZ]
Escape - quit
AAAAAAAAAAAAAAAAAAAA Functions keys AAAAAAAAAAAAAAAAAAAAAA
F2 - Overl - goto overlay
F3 - Edit - edit header
F4 - Image - goto on top image of EXE-file
F5 - Entry - goto on entry point
F6 - NewExe - goto on new executable
F8 - NewHdr - show NewEXE header (if present)
;
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE »
; ° MZ-Header edit o
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE ¼
;
[HeaderMZEdit]
Escape - quit without saving
AAAAAAAAAAAAAAAAAAAA Functions keys AAAAAAAAAAAAAAAAAAAAAA
F2 - Pages - calculate pages value ( +2,+4 in header )
F3 - Undo - restore original value under cursor
F9 - Update - save changes
Enter - save changes
AAAAAAAAAAAAAAAAAAAA Cursors movement AAAAAAAAAAAAAAAAAAAAAA
Right - right on 1 byte
Left - left on 1 byte
Tab - Next field
Down - Next field
Backtab - previous field
Up - previous field
;
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE »
; ° NE-Header view o
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE ¼
;
[HeaderNE]
Escape - quit
AAAAAAAAAAAAAAAAAAAA Functions keys AAAAAAAAAAAAAAAAAAAAAA
F2 - Flags - show program flags
F4 - Go Hdr - goto on top NE-header
F5 - Entry - goto on entry point
F6 - SegTbl - show Segment table
F7 - ModRef - show Module Reference
F8 - OldHdr - show old EXE header
Ctrl F2 - SegTbl - goto offset of Segment table
Ctrl F3 - RsrTbl - goto offset of Resource table
Ctrl F4 - ResNam - goto offset of Resident name
Ctrl F5 - ModRef - goto offset of Module reference
Ctrl F6 - ImpNam - goto offset of Import name
Ctrl F7 - EntTab - goto offset of Entry table
Ctrl F8 - NonRes - goto offset of Non-resident name
;
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE »
; ° NE Segment table flags o
; EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE ¼
;
[NE Segment flags]
NEWEXE.H (C) Copyright Microsoft Corp 1984-1987
Unused
h Huge segment
C 32-bit code segment
d Discardable segment
```







**F10 - Servic - show DDB Service Table**

[FileList]

[illegible]

[HistoryFiles]

[illegible]

[BlockFromFile]

[illegible]

[End] \*\*\* End of helpfile \*\*\*

\*\*\*\*\*

\*\*\*\*\*

Page 12

#### \*\*\*\* Assembler mode \*\*\*\*

"Byte/word/dword/pword/qword/tbyte" may be abbreviated to "b,/w,/d,/p,/q,/t,". All numbers are hex, so the letter "h" is optional. You can use math operations (i.e. `mov bx, [123+23-46h] = mov bx, [100h]`). Error messages are very brief (invalid command, syntax error, invalid operand, missing/invalid size). Unconditional JMP will be translated to 0E9 XX XX, so if you want near jump (OEB), you have to type `jmp short xxxxx` (or `jumps xxxxx`).

There is 386 assembler in HIEW version 5.00 or later, so check all jumps carefully because you may get unwanted long jump in 8086 code.

WARNING! The same command can be assembled differently depending on the assembler you're using.

#### \*\*\*\* Basing \*\*\*\*

Base is a constant that will be added to offset and jump addresses. If current offset is YY and you need XX, you should type base `"*XX"` (asterisk is required!). You can use Ctrl-F5/Ctrl-F5 as `*0`.

#### \*\*\*\* Block operations \*\*\*\*

Block operations are working only in Hex and Decode modes. You can mark blocks without switching to Edit mode. Block can be written to file using PutBlk(F2).

If you want to append the block to the end of file, you should type "FFFFFFFF" offset. You can insert the block to the current file from another file using GetBlk (CtrlF2). Block will be inserted on the current offset.

With release 6.10 if no marked block in current file - call exist blocks from file history.

#### \*\*\*\* Video modes \*\*\*\*

HIEW supports video modes up to 132x75.

#### \*\*\*\* Status Bar \*\*\*\*

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
xxx% Filename.ext dFR      NE xxxxxxxx xxx - - - - - YYYYYYY° HIEW X.XX (c) SEN
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAÜ AAAAAAAAAAAÜ 333      3 AAAAAAAAAÜ AAÜ AAAAAAAAAÜ AAAAAAAAAÜ
percent          3 333      3 current      3 3          file length in bytes
indicator        3 333      3 offset       3 3
(only if BAR=P   3 333      V              3 3      1: status of the bookmarks:
in HIEW.INI)     3 333      NewExe type    3 3      '-' free
                V 333      ÅÄ> '1...8' respective position
                filename 333      3          is currently used
                333      3          '*' current
find direction <AAÜ33      3          2: "<Editor>" = Edit mode
                33      3
                V3      3
                area of search: 3      ÅÄ> 1: Text mode: number of the first
F - current file 3          column
B - block        3          2: Decode mode: measurement of
A - list argv** 3          operands and addresses
                3          (prefix 'a' show automatic
                V          defined size code)
                status of the file:
R - open in Read mode
W - open in Write mode

```

## U - modified

++++ Keys ++++++

All keys are described in HIEW.HLP (press Alt-H). HIEW.HLP may be modified. First line of HIEW.HLP must be "[HiewHelp 5.01]". Semicolon ';' is a comment prefix character. By pressing Alt-H the respective section (from [xxxx] till [yyyy]) will be displayed. HIEW.HLP must be terminated with [End].

++++ Bookmarks ++++++

Bookmarks is for saving/restoring of the current screen. Press '+' to save the state of current screen. You can save eight screens. To restore any saved screen, press Alt-1...Alt-8 respectively. There are different bookmarks for different modes (Text/ Hex/Decode).

++++ Jumps (call/jmp) in the disassembler mode ++++++

Now jumps is 100% configurable. Jumps can be specified in HIEW.INI in the jumpTable array. This line (C Language) consists of digits and letters. First character used to undo jump ('0' in HIEW 4, 'Z' in HIEW 5 day 28). After reading from keyboard the character will be converted to the upper case, then search in jumpTable will be performed. Default value of jumpTable is '1'-'9', then 'A'-'Z'.

++++ Search/replace operations ++++++

If search string was entered in ASCII field, case-insensitive search will be performed. If you want to perform case-sensitive search, move the cursor to the HEX field and press Enter.

You can search assembler commands (F7).

Now search/replace can be restricted to selected block (F4 during entering the search/replace string).

In the disassembler mode you can use wildcards in assembler commands for searching. The wildcard character is '?'.  
For example, DECODE <F7><F7> 'mov ax, ?' will look for 'mov ax, 1234h', 'mov ax, sp', etc.

With release 5.83 you can searched multiline assembler command, delimited sign is ';'.

For example: "push ?10; call ?; add ?"

find-it!	not find:
-----	-----
push 00010	push 00010
call 01234:05678	push 00011
add sp,00006	add ax,00006

With release 6.10 you can search/replace in all files from argv\*\* list - files from command line parameters. Enable for this - select area "filArg" with help F4 key in search/replace input.

++++ Crypt operations (F7/F8 in Edit) ++++++

Crypt operations are using for crypting/decrypting the code/data. Crypt

algorithm is very simple. Code/data will be crypted by the bytes/words (to change the size of the unit, press F2). Crypting routine must be terminated with "LOOP numberLine" operator.

Available commands:

```
Reg mode      : neg, mul, div
Reg-Reg mode:  mov, xor, add, sub, rol, ror, xchg
Reg-Imm mode:  mov, xor, add, sub, rol, ror
Imm mode      : loop
```

All 8/16 bit registers are available, except AL/AX that will be filled with (de)crypted byte/word.

The differences from standard assembler:

```
there are no jumps;
'loop' means 'jmp/stop'
the operands of 'rol/ror' commands must have the same size, i.e.
ROL AX, CL not allowed.
```

Example:

- a. XOR byte with 0AAh:
  1. XOR al, 0aah
  2. LOOP 1
- b. XOR word with mask increment
  1. MOV dx, 0
  2. XOR ax, dx
  3. ADD dx, 1
  4. LOOP 2

++++ INI file ++++++

INI file must be located in HIEW.EXE home directory. You can specify key "/INI=<inifile>" in the command line.

First line in HIEW.INI always "[HiewIni 5.03]" !

Blank line or line, beginners with ';' is ignored.

-----8<----- Example HIEW.INI -----8<-----

```
[HiewIni 5.03]
;
; Startup
;                                     ; legal values
; startup mode
;
; StartMode                = Text          ; Text | Hex      | Code
; beeper
; Beep                      = 0n           ; 0n   | Off
; percent indicator
; Bar                       = Left         ; Left | Right   | Percent
; warp/don't warp long lines
; Auto=Off for textfile, 0n for binary
; Wrap                     = Auto         ; Auto | 0n      | Off
; tabulation
; Auto=0n for textfile, Off for binary
; Tab                      = Auto         ; Auto | 0n      | Off
```

```

; step for Ctrl-Left, Ctrl-Right in textmode
StepCtrlRight      = 20                ; 1 - 128

; Show/Do not show mouse cursor
DisableMouse       = 0n                ; 0n | Off

; table symbols for branch call/jmp
JumpTable          = "0123456789ABCDEFGHIJKLMN0PQRSTUVWXYZ"

; Select symbol "linefeed": automatic      0x0a / 0x0d / 0x0d:0x0a
Linefeed           = Auto              ; LF | CR | LFCR      v5. 10

; Automatic define size of code for LX-executable
AutoCodeSize       = 0n                ; 0n | Off          v5. 41

; Flush keyboard buffer before read a key
KbdFlush           = 0n                ; 0n | Off          v5. 50

; View Offset for NE/LX/PE as local/global (toggle Alt-G)
ShowOffset         = Local              ; Local | Global      v5. 51

; Mask for showed offset in pattern search
RunningOffsetMask  = 0xFF              ; 0 - 0xFFFFFFFF      v5. 53

; Xlat table index in hiew.xlt ( 0 - As Is )
XlatTableIndex     = 0                  ; 0 - 15              v5. 85

; sort in filelist
FlistSort          = Name              ; none |Name |Ext |Time |Size v5. 90

; reverse sort in filelist
FlistSortReverse   = Off               ; 0n | Off            v5. 90

; show hidden files in filelist
FlistShowHidden    = Off               ; 0n | Off            v5. 90

; save current state( mode, offset, bookmarks, etc) for next file
NextFileSaveState  = Off               ; 0n | Off            v6. 00

; Scanning code step for search with pattern and find reference
;                               / by command / by one byte
ScanStep           = Command           ; Command | Byte      v6. 00

; Write savefile at exit
SaveFileAtExit     = Off               ; 0n | Off            v6. 00

; Locate savefile
Savefile           = "hiew.sav"        v6. 00

;
;      Colors
;
ColorMain          = 0x1B              ; main color
ColorCurrent       = 0x71              ; current byte
ColorMark          = 0x5E              ; block color
ColorEdit          = 0x1E              ; file editing
ColorEditOut       = 0x1D              ; non-file editing
ColorError         = 0x4E              ; error messages
ColorMsg           = 0x2E              ; messages
ColorTitle        = 0x70              ; status bar
ColorKbNum         = 0x07              ; keys
ColorKb            = 0x30              ; key is active

```

```

Col orKbOff           = 0x37           ; key is inactive
Col orBar              = 0x02           ; progress indicator
Col orWi n            = 0x70           ; input dialog
Col orWi nBold         = 0x7F           ; - " - selected
Col orWi nInput        = 0x3F           ; - " - input field
Col orMenu             = 0x30           ; menu frame
Col orMenuText         = 0x31           ; - " - field
Col orMenuBold         = 0x0F           ; - " - text
Col orHelp             = 0x20           ; help frame
Col orHelpText         = 0x2E           ; - " - field
Col orHelpBold         = 0x0F           ; - " - text

```

; ---+--- End of Inifile ---+---

-----8<-----8<-----8<-----

++++ SAV file ++++++

If executed without any parameters, HIEW will look for SAV-file in the current directory (you can specify "Savefile=<locate\_savefile>" in INI-file or /SAV=<savefile> in the command line) and restore previously saved (Ctrl-F10) state.

++++ XLT file structure ++++++

```

typedef struct{
    BYTE  sign[ 9 ],           // "Hi ewXl at", 0
          unused[ 5 ],
          versionMajor,       // 0x05
          versionMinor;       // 0x40
}XLAT_HEADER;

typedef struct{
    BYTE  title[ 16 ],         // show in F8
          tableOut[ 256 ],     // for output
          tableIn[ 256 ],      // for input
          tableUpper[ 256 ];   // for search with ignore case
}XLAT;

```

Maximal count xlat-table is 15.

++++ Command line ++++++

```

Hiew [/SAV=<savefile>] [/INI=<inifile>] [/s]filemask ... [/s][filemask]

    /SAV=<savefile>           - location for savefile
    /INI=<inifile>            - location for inifile
    [/s] filemask ... [/s][filemask] - more files, include pattern

```

Option /s toggle search with subdirectories:  
hiew /s \*.dll \*.exe /s \*.txt -> search .dll and .exe with subdir and  
.txt only in current catalog

++++ History ++++++

```

5.03aa 3/10/95 - OS/2: DosSleep( 1L )
              - Unvisible cursor
5.10ee 22/12/95 - fix: invalid jump for Jc 7E/7F
              - fix: invalid opsize, if previons byte is 0x0F
              - save screencopy into file ( PrScr deleted )
              - chose symbol "linefeed" in INI-file

```

- for replace write full buffer ( was: 1 byte )
- for OS/2session get key with KbdCharIn ( was: getch() )
- delete DosSleep( 1 )
- 5. 11bb 24/01/96 - fix: call/jmp PWORD ptr
- 5. 13 01/02/96 - fix: marked text on 2-lines
- fix: crash scrolling Up, if upper code is
- 24 one-byte command (ex. NOP )
- fix: OS/2: trap on create file
- 5. 14 09/04/96 - fix: ( from 5. 13 ) double prefix 0x66
- fix: bad assembler with [EBP]
- for (Pg)Up looking symbol 0x0A
- added leading zero to all digit in decode
- pattern find with wildcards as in decode
- 5. 15 12/05/96 - fix: pattern find truncate line
- 5. 16 28/05/96 - fix: pattern find not found "mov ax,?"
- 5. 20 17/06/96 - NE-executable: Header & segment table
- 5. 21 27/06/96 - NE-executable: TransSegment call support
- 5. 22 01/07/96 - Fill block
- 5. 23 12/07/96 - NE-executable: Entry table support
- 5. 24 30/07/96 - fix: crash after replace in decode mode
- 5. 30 20/12/96 - Support LX-executable (header, object table, call/jmp)
- Named ordinals for NE- and LX-executable
- fix: invalid percent bar on long file
- fix: assemble relative jmp/call > 8000
- fix: Save hiew.sav before edit disabled write
- 5. 31 9/01/97 - Alt-0 in decode: show named ordinal toggle
- fix: incorrect far jump/call in exe-MZ (from 5. 30)
- 5. 40 29/01/97 - F4 in NE/LX header: goto on top NE(LX) image
- F8 in text: select translation table
- Alt-G: toggle Global/Local offset for NE(LX) files
- 5. 41 31/01/97 - choise "AutoCodeSize" in INI-file: automatic define
- size of code (32/16)
- Alt-R: Reload file
- fix: russian 'p'
- 5. 50 10/02/97 - support PE-executable (header, object table)
- choise "KbdFlush" in INI-file: flush keyboard buffer
- 5. 51 27/02/97 - jmp/call show as local
- imports name for PE from NT
- input (F5) local offset, if first symbol is '.'
- word "call"/"jmp" before system functions
- choise "ViewOffset" in INI-file
- 5. 52 4/03/97 - for localOffset patternSearch only in code segments
- ( NE/LX/PE )
- 5. 53 18/03/97 - choise "RunningOffsetMask" in INI-file
- fixed bug in HIEW.XLT: upcase table
- 5. 60 10/04/97 - option /s in command line
- fix: lost double prefix 66(67)
- fix: assemble relative jmp/call > 8000 bytes
- (fix in 5. 30 incorrect)
- fix: jmp/call with prefix 67
- 5. 61 2/06/97 - new releases of NEDUMP.EXE and LXDUMP.EXE (show
- named ordinals from hiew.ord)
- assembled "rep cmovsd" as F3 66 A3 ( was: 66 F3 A3 )
- on binary files 'line feed' define as CR/LF
- increase length of line in decode
- 5. 65 24/07/97 - added xor with string
- 5. 66 4/08/97 - fix: trap in Win'95 - losted free()
- 5. 67 14/01/98 - fix: bad translation for big get/put blocks
- 5. 70 13/03/98 - fix: text file with first 'NE'...
- calculator with parenthesis and priority (Alt-=)
- Pentium(R) Pro (dis)assembler (inc. floating and MMX)
- 5. 71 30/03/98 - showed import in delphi-exe
- 5. 80 7/04/98 - support LE-modules

		- new release of LXDUMP.EXE (support LE)
5.81	10/04/98	- bugfixed release of 5.80
5.82	28/04/98	- internal change
5.83	7/05/98	- fixed bug (5.70): crash on long string in Crypt
5.84	13/05/98	- Alt-9 restore last edit position
5.85	10/06/98	- fix: prtScr into exist file
		- F5 in FindInput: go last editing position
		- choise "XlatTableIndex" in ini-file
5.90	9/07/98	- File list
		- choise "FlistSort" in ini-file
		- choise "FlistSortReverse" in ini-file
		- choise "FlistShowHidden" in ini-file
		- choise "NextFileSaveOffset" in ini-file
		- parameter in command line "/SAV=<savefile>" (was: "/FS=" )
		- new parameter in command line "/INI=<inifile>"
		- fix: lose first empty line in text
5.91	17/08/98	- Alt-R in Filelist (reread)
		- fix: go image in MZ-header show
		- include DEXEM EXE - DualEXEcatableManipulator (NE/LX/LE)
		( replace stub, split old-exe & new-exe, ...)
5.92	21/09/98	- Alt-S in decode: toggle scancode step (byte/command)
		- timeslice under windows
		- modified import for PE
		- fix: empty filelist for mask
		- fix: restore current offset from .sav
6.00	19/10/98	- delete "ActionAfterWriteSavefile" in ini-file
		- delete "NextFileSaveOffset" ini ini-file
		- no more crypt, sorry...
		- support NLM module
		- history of files (Backspace, Tab)
		- history input (PgDown in edit input string)
		- Ctrl-* - mark all
		- choise "SaveFileAtExit" in ini-file
		- choise "ScanStep" in ini-file
		- choise "Savefile" in ini-file
		- choise "NextFileSaveState" in ini-file
		- DEXEM EXE v1.50 - know PE
6.01	9/12/98	- crypt return !
		- Info move at Ctrl-Alt
		- fix: trap for scanning PE with zeroed virtualSize
		in PE-section
6.02	26/01/99	- fix: no correct canonicalize for CD
		- no auto switch ascii/hex for input search string
		- scale in info
		- dos version compiled for 80286
6.03	3/03/99	- Decode: Alt-F7(Auto) moved to Alt-F9
		- Alt-F7 toggle of find direction
		- help moved to key F1
		- save find position for change mode
		- (OS/2 & KbdFlush=off) VideoUpdate if not pressed key
		- help moved to key F1
		- Dexem.exe v1.51
		- Lxdump.exe v2.02
6.04	26/03/99	- fix: jmp 0xFFFFFFFF do not show target
		- fix: divide by zero A%0 in calculator
		- fix: incorrect assemble Jxx in 32bit
		- fix: backward search with '0xFF 0xFF 0xFF... 0xFF' :-)
		- in 32bit mode show: 'mov SegReg, Reg16' (was: Reg32)
		- multiline asm-find with pattern in decode (first in 5.83)
		- synchronize toggle flag of find direction
		- safe next find with asm-pattern for next file
		- key '/' in decode - current offset at top
6.10	24/05/99	- multifile search/replace for argv* list

- for GetBlock select marked block from file history
- fix: in multiline assembler search
- 6.11 2/07/99 - fix: crash on filled big block
- 6.15 7/07/99 - SHAREWARE version

+++++ = YES = +++++

```
*****
*
*                               [Hi ew License Conditions]
*
*****
```

This ist Freeware.

Noncommercial distribution and/or use is permitted under the following terms: You may copy and distribute verbatim copies of the HIEW executable code and associated files; provide unmodified copies of the documentation as provided with the program.

Commercial distribution and/or use prohibited without written consent of Eugene Suslikov.

HIEW is provided "as is", without warranty of any kind, neither expressed nor implied. The author only guarantees that HIEW and the included tools occupy diskspace.

In no event will the author be liable to you for any damages, including lost profits, lost savings or other incidental or consequential damages arising out of the use of this program or the inability to use this program.

===== End of license conditions =====