

Hexedit - Usage

What is hexedit?

Allows one to view and edit files in hexadecimal or in ASCII.

Usage: hexedit \$program-name

Use the keyboard arrows to move through the content of the file and modify it by simply typing the new desired bytes. The modified file can then be saved by using 'Ctrl+X' and typing 'y' for yes.

Example usages

Example 1

Assuming you have decided to edit the .dynamic section of an ELF file; Objdump -s yielded the following output:

```

Terminal - roee@roee-ORTEGE-Z930: ~/aes
File Edit View Terminal Tabs Help
roee@roee-ORTEGE... x roee@roee-ORTEGE... x roee@roee-ORTEGE... x roee@roee-ORTEGE... x roee@roee-ORTEGE... x
GNU nano 2.2.6 File: bla
400ca0 44000000 94000000 58ffffff 65000000 D.....X...e...
400cb0 00420e10 8f02450e 188e0345 0e208d04 .B...E...E. ..
400cc0 450e288c 05480e30 8606480e 3883074d E(..H.0..H.8..M
400cd0 0e406c0e 38410e30 410e2842 0e20420e .@l.8A.0A.(B. B.
400ce0 18420e10 420e0800 14000000 dc000000 .B..B.....
400cf0 80ffffff 02000000 00000000 00000000 .....
400d00 00000000 .....
Contents of section .init_array:
600df0 40084000 00000000 @.@.....
Contents of section .fini_array:
600df8 20084000 00000000 .@.....
Contents of section .jcr:
600e00 00000000 00000000 .....
Contents of section .dynamic:
600e08 01000000 00000000 01000000 .....
600e18 01000000 00000000 7a000000 .....Z.....
600e28 0f000000 00000000 c1000000 .....
600e38 0c000000 00000000 98064000 .....@.....
600e48 0d000000 00000000 740b4000 .....t.@.....
600e58 19000000 00000000 f00d6000 .....
600e68 1b000000 00000000 08000000 .....
600e78 1a000000 00000000 f80d6000 .....
600e88 1c000000 00000000 08000000 .....
600e98 f5feff6f 00000000 98024000 .....o.....@.....
600ea8 05000000 00000000 20044000 .....@.....
600eb8 06000000 00000000 b8024000 .....@.....
600ec8 0a000000 00000000 ea000000 .....
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```

Run hexedit by typing 'hexedit \$program' (\$program=your program) and find address of the .dynamic section. You'll see that you cannot find an offset of 600e08 within the file since the latter is a virtual address and all we care about is the **physical** (i.e. location on the disk). The actual offset you're looking for is 600e08-600000 = e08.

Therefore:

```

Terminal - roee@roee-PORTEGE-Z930: ~/aes
File Edit View Terminal Tabs Help
roee@roee-PORTEGE... x roee@roee-PORTEGE... x roee@roee-PORTEGE... x roee@roee-PORTEGE... x roee@roee-PORTEGE... x
00000C80 07 FD FF FF 75 01 00 00 00 41 0E 10 86 02 43 0D .....u....A....C.
00000C90 06 45 83 03 03 6B 01 0C 07 08 00 00 00 00 00 00 .E...k.....
00000CA0 44 00 00 00 94 00 00 00 58 FE FF FF 65 00 00 00 D.....X...e...
00000CB0 00 42 0E 10 8F 02 45 0E 18 8E 03 45 0E 20 8D 04 .B....E....E. ..
00000CC0 45 0E 28 8C 05 48 0E 30 86 06 48 0E 38 83 07 4D E.(..H.0..H.8..M
00000CD0 0E 40 6C 0E 38 41 0E 30 41 0E 28 42 0E 20 42 0E .@l.8A.0A.(B. B.
00000CE0 18 42 0E 10 42 0E 08 00 14 00 00 00 DC 00 00 00 .B..B.....
00000CF0 80 FE FF FF 02 00 00 00 00 00 00 00 00 00 00 00 .....
00000D00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000D90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000DA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000DB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000DC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000DD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000DE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000DF0 40 08 40 00 00 00 00 00 20 08 40 00 00 00 00 00 @.@. .@.
00000E00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 .....
00000E10 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 .....
00000E20 7A 00 00 00 00 00 00 00 0F 00 00 00 00 00 00 00 z.....
00000E30 C1 00 00 00 00 00 00 00 0C 00 00 00 00 00 00 00 .....
00000E40 98 06 40 00 00 00 00 00 0D 00 00 00 00 00 00 00 ..@.....
00000E50 74 0B 40 00 00 00 00 00 19 00 00 00 00 00 00 00 t.@.....
00000E60 F0 0D 60 00 00 00 00 00 1B 00 00 00 00 00 00 00 ..
-- gennnn --0xE08/0x232F-----

```

As can be seen, offset E08 (corresponds to virtual address 600e08) is marked with a blue frame.

Example 2

Assuming you have decided to manipulate a string located in the dynamic-string table. Using `readelf -d` (Or by inspecting the `.dynamic` section – remember, type ‘5’ points to the dynamic string table) it is possible to find out the address of the `.dynstr` section. Assuming the virtual address is `0x400420`, the offset within the file (physical offset) is `0x400420-0x400000=0x420`.

Therefore:

```

Terminal - roee@roee-ORTEGE-Z930: ~/aes
File Edit View Terminal Tabs Help
roee@roee-ORTEGE... x roee@roee-ORTEGE... x roee@roee-ORTEGE... x roee@roee-ORTEGE... x roee@roee-ORTEGE... x
00000340 00 00 00 00 00 00 00 00 84 00 00 00 12 00 00 00 .....
00000350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000360 28 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 (... .....
00000370 00 00 00 00 00 00 00 00 8A 00 00 00 12 00 00 00 .....
00000380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000390 65 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 e.....
000003A0 00 00 00 00 00 00 00 00 72 00 00 00 12 00 00 00 .....r.....
000003B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000003C0 37 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 7... .....
000003D0 00 00 00 00 00 00 00 00 4B 00 00 00 20 00 00 00 .....K... ..
000003E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000003F0 6C 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 l.....
00000400 00 00 00 00 00 00 00 00 85 00 00 00 12 00 00 00 .....
00000410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000420 00 6C 69 62 64 6C 2E 73 6F 2E 32 00 5F 49 54 4D .libdl.so.2. ITM
00000430 5F 64 65 72 65 67 69 73 74 65 72 54 4D 43 6C 6F _deregisterTMClo
00000440 6E 65 54 61 62 6C 65 00 5F 5F 67 6D 6F 6E 5F 73 neTable.__gmon_s
00000450 74 61 72 74 5F 5F 00 5F 4A 76 5F 52 65 67 69 73 tart__Jv_Regis
00000460 74 65 72 43 6C 61 73 73 65 73 00 5F 49 54 4D 5F terClasses. ITM
00000470 72 65 67 69 73 74 65 72 54 4D 43 6C 6F 6E 65 54 registerTMCloT
00000480 61 62 6C 65 00 72 6F 65 65 6C 65 6F 6E 6C 73 79 able.roeeleonlsy
00000490 6D 00 64 6C 63 6C 6F 73 65 00 6C 69 62 63 2E 73 m.dlclose.libc.s
000004A0 6F 2E 36 00 73 72 61 6E 64 00 74 69 6D 65 00 5F o.6.srand.time._
000004B0 5F 73 74 61 63 6B 5F 63 68 6B 5F 66 61 69 6C 00 _stack_chk_fail.
000004C0 70 75 74 63 68 61 72 00 70 72 69 6E 74 66 00 5F putchar.printf._
000004D0 5F 6C 69 62 63 5F 73 74 61 72 74 5F 6D 61 69 6E _libc_start_main
000004E0 00 24 4F 52 49 47 49 4E 2F 6D 79 2E 73 6F 66 69 .$ORIGIN/my.sofi
000004F0 6C 65 73 00 47 4C 49 42 43 5F 32 2E 32 2E 35 00 les.GLIBC_2.2.5.
00000500 47 4C 49 42 43 5F 32 2E 34 00 00 00 02 00 00 00 GLIBC_2.4.....
00000510 03 00 02 00 02 00 02 00 00 00 02 00 04 00 04 00 .....
00000520 00 00 00 00 04 00 02 00 01 00 01 00 01 00 00 00 .....
- ** gennnn --0x48D/0x232F-----

```

The start of the `.dynstr` section is marked with a red frame.

Changes that I have done are marked with a green frame (Manipulated the bytes to represent ‘roeeleon’ in ASCII).