

## Introduction:

This is a ELF object file editor, which can analyze, edit any section in a 32-bit ELF object file. Also, part of disassembly mode is now available.

## How to install:

Make sure no file is missed, see file\_list.txt.

cd <location of file\_editor>

gcc ./file\_editor.c -o ./file\_editor.o

## Open a demo file:

cd <location of file\_editor.o>

./file\_editor.o <path of ELF 32 object file>

## Print everything in header:

Enter -555, then press <Enter>.

```
-555
e_ident: 7f 45 4c 46 2 0 3 0 1 0 0 0 c0 83 4 8
e_type: 2
e_machine: 3
e_version: 1
e_entry: 134513600
e_phoff: 0x34
e_shoff: 0x1860
e_flags: 0
e_ehsize: 52
e_phentsize: 32
e_phnum: 9
e_shentsize: 40
e_shnum: 31
e_shstrndx: 28
```

## Select a section:

Enter the corresponding section code, then press <Enter>.

Ex. Select .shstrtab section

```
.bss: fc
.comment: 101
.shstrtab: 11
.symtab: 1
.strtab: 9
Exit: -1
11
```

## Print everything in section header:

Enter I, then press <Enter>.

```
I
sh_name: 9
sh_type: 3
sh_flags: 0
sh_addr: 0
sh_offset: 14e0
sh_size: 276
sh_link: 0
sh_info: 0
sh_addraling: 1
sh_entsize: 0
```

### Print the whole <section>:

Enter P, then press <Enter>.

```
P
00000000      0063 7274 7374 7566 662e 6300 5f5f 4a43      .crtstuff.c.__JC
00000010      525f 4c49 5354 5f5f 0064 6572 6567 6973      R_LIST__deregis
00000020      7465 725f 746d 5f63 6c6f 6e65 7300 5f5f      ter_tm_clones.__
00000030      646f 5f67 6c6f 6261 6c5f 6474 6f72 735f      do_global_dtors_
00000040      6175 7800 636f 6d70 6c65 7465 642e 3732      aux.completed.72
00000050      3039 005f 5f64 6f5f 676c 6f62 616c 5f64      09.__do_global_d
00000060      746f 7273 5f61 7578 5f66 696e 695f 6172      tors_aux_fini_ar
00000070      7261 795f 656e 7472 7900 6672 616d 655f      ray_entry.frame_
00000080      6475 6d6d 7900 5f5f 6672 616d 655f 6475      dummy.__frame_du
00000090      6d6d 795f 696e 6974 5f61 7272 6179 5f65      mmy_init_array_e
000000A0      6e74 7279 006c 6f67 696e 2e63 005f 5f46      ntry.login.c.__F
000000B0      5241 4d45 5f45 4e44 5f5f 005f 5f4a 4352      RAME_END__.__JCR
000000C0      5f45 4e44 5f5f 005f 5f69 6e69 745f 6172      _END__.__init_ar
000000D0      7261 795f 656e 6400 5f44 594e 414d 4943      ray_end._DYNAMIC
```

### Print the whole <section> in disassembly mode:

Enter Z, then press <Enter>.

```
Z
00000000      31 ed                                XOR      Ev,Gv
00000002      5e                                POP      rSI/r14
00000003      89 e1                                MOV      Ev,Gv
00000005      83 e4 f0                            Grp1     Ev,Ib
00000008      50                                PUSH     rAX/r8
00000009      54                                PUSH     rSP/r12
0000000A      52                                PUSH     rDX/r10
0000000B      68 e0 85 04 08                    PUSH     Iz
00000010      68 80 85 04 08                    PUSH     Iz
00000015      51                                PUSH     rCX/r9
00000016      56                                PUSH     rSI/r14
00000017      68 bb 84 04 08                    PUSH     Iz
0000001C      e8 af ff ff ff                    CALL     Jz
00000021      f4                                HLT
00000022      66 90                            NOP
00000024      66 90                            NOP
```

### Find one-byte with value:

Enter F <Hex value>, then press <Enter>.

```
F 0c
location at 127
location at 153
location at 165
location at 17E
location at 190
location at 1D1
location at 1D8
location at 217
```

### Find two-byte with value(in big-endian):

Enter L <Hex value>, then press <Enter>.

```
L 0000
location at 50
location at 51
location at 52
location at 89
location at 8A
location at 8B
location at AC
location at AD
location at AE
location at E1
location at E2
location at E3
location at 10F
location at 110
location at 11B
```

### Edit two-byte with value and address(in big-endian):

Enter E <Hex value> <Hex address>, then press <Enter>.

```
00000200      7424 2c55
00000210      1039 f775
00000220      f3c3
```

```
E 3412 210
```

```
00000200      7424 2c55
00000210      1234 f775
00000220      f3c3
```

### Delete X bytes:

Enter D <Hex address> <X>, then press <Enter>.

```
00000200      7424 2c55
00000210      1234 f775
00000220      f3c3
```

```
D 210 2
```

```
00000200      7424 2c55
00000210      f775 e383
```

### Add one-byte:

Enter A <Hex value> <Hex address>, then press <Enter>.

```
00000200      7424 2c55
00000210      f775 e383
```

```
A 3910 210
```

```
00000200      7424 2c55
00000210      1039 f775
00000220      f3c3
```

**Save and Exit section:**

Enter Q, then press<Enter>.

**Exit section:**

Enter any letter else (ex.'r'), then press <Enter> .