ELF - GNU utilities

symbols

```
$ readelf -s a.out
Symbol table '.dynsym' contains 4 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__

Symbol table '.symtab' contains 24 entries:
   Num:    Value  Size Type    Bind   Vis      Ndx Name
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 FILE    LOCAL  DEFAULT  ABS a.c
     8: 00000000     4 OBJECT  LOCAL  DEFAULT    2 static_var
     9: 00000000     0 SECTION LOCAL  DEFAULT    9
    14: 00000020  1024 OBJECT  GLOBAL DEFAULT   24 global_uninit_array
    19: 00000000     5 FUNC    WEAK   DEFAULT    1 _extern_func
    20: 0000000a     5 FUNC    GLOBAL DEFAULT    1 global_func
```

dummy **UND**efined section

enclosing section number

dummy section for symbols with **ABS**olute value (untouched by linker)

value relative to enclosing section start address

Sections

```
$ readelf -S a.out
  ...
Section Headers:
  [Nr] Name              Type ...
  [ 0]                   NULL
  [ 1] .text             PROGBITS
  [ 2] .data             PROGBITS
       ...
  [ 5] .dynsym           DYNSYM
       ...
  [ 9] .rodata           PROGBITS
       ...
  [24] .bss              NOBITS
       ...
  [36] .symtab           SYMTAB
  [37] .strtab           STRTAB
```

segments (program headers)

```
$ readelf -l a.out
...
Program Headers:
  Type           Offset   VirtAddr   PhysAddr   FileSiz MemSiz  Flg Align
  PHDR           0x000034 0x08048034 0x08048034 0x000e0 0x000e0 R E 0x4
  INTERP         0x000114 0x08048114 0x08048114 0x00013 0x00013 R   0x1
      [Requesting program interpreter: /lib/ld-linux.so.2]
  LOAD           0x000000 0x08048000 0x08048000 0x00438 0x00438 R E 0x1000
                                  ...
 Section to Segment mapping:
  Segment Sections...
   00
   01     .interp
   02     .interp .note.ABI-tag .hash .gnu.hash .dynsym .dynstr .gnu.version .gnu.version_r
          .rel.dyn .rel.plt .init .plt .text .fini .rodata .eh_frame
                                  ...
```

offset in file

address in memory

unused

size in file

size in memory

no alignment constraints

Read

Execute

segment **#02** contains these sections

ELF - GNU utilities

demangle **C++** names

all symbols, even debugger-only

```
$ nm -Cola a.o
a.o:00000000 b .bss                a.c:11
                ...
a.o:00000000 W _extern_func        a.c:11
a.o:00000000 a a.c
a.o:00000000 R const_var           a.c:8
a.o:0000000a T global_func         a.c:15
a.o:00000004 C global_uninit_var
a.o:00000004 D global_var          a.c:3
a.o:00000005 t local_func          a.c:13
a.o:00000000 d static_var          a.c:1
```

appears in file ...

value

type

name

defined in source file ... (according to debug info)

- **A a** - value is **absolute** (untouched by linker)
- **B b** - uninitialized data (**BSS**)
- **C c** - **common** symbol (uninitialized, but can be bound to defined symbol with the same name)
- **D d** - initialized **data**
- **G g** - initialized data for small objects
- **N n** - debugging symbol
- **R r** - **read-only**
- **S s** - uninitialized data for **small** objects
- **T t** - code (**text**)
- **U u** - **undefined**
- **V v** - weak (defaulted to 0)
- **W w** - **weak** (default is system-specific)

GLOBAL

local

dump .**d**ynamic section

```
$ readelf -d a.out

Dynamic section at offset 0x44c contains 21 entries:
  Tag        Type         Name/Value
 0x00000001 (NEEDED)     Shared library: [libc.so.6]
 0x0000000c (INIT)       0x8048254
                        ...
```

```
$ ldd a.out
 linux-gate.so.1 =>  (0xb7f82000)
 libc.so.6 => /lib/tls/i686/cmov/libc.so.6 (0xb7e21000)
 /lib/ld-linux.so.2 (0xb7f83000)
```

library base address (usually randomized)

mapped into process' address space by Linux kernel; does not exist as a file on any filesystem

disassemble

```
$ objdump -d a.o
                ...
0000000f <main>:
   f: 8d 4c 24 04            lea    0x4(%esp),%ecx
  13: 83 e4 f0               and    $0xfffffff0,%esp
                ...
  27: c3                     ret
```