ELF1 7 Examples - 4 Library librel.so - ELF Study 1999

Young W. Lim

2020-03-20 Fri

Outline

1. Based on
2. Summary of relocation results for `librel.so`
   - TOC
   - 1. Reloc summary for `librel.so`
   - 2. Symbols and sections for `librel.so`
   - 3. Relocation listings for `librel.so`
3. Linking for `librel.so`
   - TOC
   - Linking the `.data` section for `librel.so`
   - Linking the `.text` section for `librel.so`
   - Undefined symbols in `librel.so`
4. Locating relocs and symbol references of `librel.so`
   - TOC
   - 1. Locating `.data` section relocs of `librel.so`
   - 2. Locating `.text` section relocs of `librel.so`
   - 3. Locating `.data` section symbol references of `librel.so`
   - 4. Locating `.text` section symbol references of `librel.so`

Based on

"Study of ELF loading and relocs", 1999
http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

Compling 32-bit program on 64-bit gcc

- `gcc -v`
- `gcc -m32 t.c`
- `sudo apt-get install gcc-multilib`
- `sudo apt-get install g++-multilib`
- `gcc-multilib`
- `g++-multilib`
- `gcc -m32`
- `objdump -m i386`
- `-Wl,-q`

TOC: Summary of relocation results for `librel.so`

1. Reloc summary for `librel.so`
2. Symbols and sections for `librel.so`

TOC: 1. librel.so shared object file relocs

- Relocation listing sections for a shared library
- Relocation table section for librel.so shared library
- Relocation listing section for librel.so shared library
- a) data section relocs of librel.so shared library
- b) text section relocs of librel.so shared library
- c) data section reloc listing of librel.so shared library
- d) text section reloc listing of librel.so shared library

Relocation listing sections for a shared library

- based on "Study of ELF loading and relocs"

.rel.bss	R_386_COPY	*non-PIC* reference of a global symbol
.rel.got	R_386_GLOB_DAT	*PIC* reference of a global symbol
.rel.plt	R_386_JUMP_SLOT	*PIC* reference of a function symbol

- from the results of `readelf -r`

.rel.dyn	R_386_GLOB_DAT	*PIC* reference of a global symbol
.rel.plt	R_386_JUMP_SLOT	*PIC* reference of a function symbol

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

Relocation table sections for librel.so shared library

- for librel.so

	-fno-pic	default	-fPIC
.plt	✓	✓	✓
.plt.got	✓	✓	✓
.got	✓	✓	✓
.got.plt	✓	✓	✓

```
readelf -t librel-fno-pic.so | grep -e .plt -e .got -e .rel
```

Relocation listing sections for librel.so shared library

- for librel.so

	-fno-pic	default	-fPIC
.rel.data			
.rel.text			
.rel.dyn	✓	✓	✓
.rel.plt			✓
.rel.got			

```
readelf -t librel-fno-pic.so | grep -e .plt -e .got -e .rel
```

a) data section relocs of librel.so shared library

- data section relocs of librel.so file
    - local data symbol reference (cLocal)
        - R_386_32 in .data → R_386_RELATIVE in .data (-fno-pic)
        - R_386_32 in .data.rel → R_386_RELATIVE in .data (default, -fPIC)
    - local function symbol reference (fLocal)
        - R_386_32 in .data → R_386_RELATIVE in .data (-fno-pic)
        - R_386_32 in .data.rel → R_386_RELATIVE in .data (default, -fPIC)
    - global data symbol reference (cPub)
        - R_386_32 in .data for all cases (-fno-pic, default, -fPIC)
    - global function symbol reference (fPub)
        - R_386_32 in .data for all cases (-fno-pic, default, -fPIC)

b) text section relocs of librel.so shared library

- text section relocs of librel.so file
  - local data symbol reference (cLocal)
    - when GOT is used (default, -fPIC)
      R_386_GOTOFF in .text is resolved
    - otherwise (-fno-pic)
      R_386_32 in .text → R_386_RELATIVE in .text
  - global data symbol reference (cPub)
    - when GOT is used (default, -fPIC)
      R_386_GOT32 in .text → R_386_GLOB_DAT in .got
    - otherwise (-fno-pic)
      R_386_32 in .text
  - global function symbol reference (fPub)
    - when PLT is used (-fPIC)
      R_386_PLT32 in .text → R_386_JUMP_SLOT in .got.plt
    - otherwise (-fno-pic, default)
      R_386_PC32 in .text

c) data section reloc listing of librel.so shared library

- data section related listing of .rel.dyn

symbol	-fno-pic	default	-fPIC
cLocal	R_386_RELATIVE in .data	R_386_RELATIVE in .data	R_386_RELATIVE in .data
fLocal	R_386_RELATIVE in .data	R_386_RELATIVE in .data	R_386_RELATIVE in .data
cPub	R_386_32 in .data	R_386_32 in .data	R_386_32 in .data
fPub	R_386_32 in .data	R_386_32 in .data	R_386_32 in .data

d) text section reloc listing of librel.so shared library

- text section related listing of .rel.dyn

	-fno-pic	default	-fPIC
cLocal	R_386_RELATIVE in .text	resolved in .text	resolved in .text
cPub	R_386_32 in .text	R_386_GLOB_DAT in .got	R_386_GLOB_DAT in .got
fPub	R_386_PC32 in .text	R_386_PC32 in .text	See .rel.plt

- text section related listing of .rel.plt

	-fno-pic	default	-fPIC
fPub	not applicable	not applicable	R_386_JUMP_SLOT in .got.plt

TOC: 2. Symbols and sections for `librel.so`

- -fno-pic case
  - (1.a) Symbol table in `librel.so` (-fno-pic)
  - (1.b) Section header in `librel.so` (-fno-pic)
  - (1.c) Symbol's section listing `librel.so` (-fno-pic)
  - (1.d) Zero value symbol listing `librel.so` (-fno-pic)
- default case
  - (2.a) Symbol table in `librel.so` (default)
  - (2.b) Section header in `librel.so` (default)
  - (2.c) Symbol's section listing `librel.so` (default)
  - (2.d) Zero value symbol listing `librel.so` (default)
- -fPIC case
  - (3.a) Symbol table in `librel.so` (-fPIC)
  - (3.b) Section header in `librel.so` (-fPIC)
  - (3.c) Symbol's section listing `librel.so` (-fPIC)
  - (3.d) Zero value symbol listing `librel.so` (-fPIC)

(1.a) Symbol table in librel.so (-fno-pic)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
     5: 000004bd    77 FUNC    GLOBAL DEFAULT    9 foo
     9: 000004ad     8 FUNC    GLOBAL DEFAULT    9 fPub
    10: 00002022     1 OBJECT  GLOBAL DEFAULT   19 cPub
    12: 00002010    16 OBJECT  GLOBAL DEFAULT   18 a

Symbol table '.symtab' contains 55 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
    30: 000004b5     8 FUNC    LOCAL  DEFAULT    9 fLocal
    31: 00002021     1 OBJECT  LOCAL  DEFAULT   19 cLocal
    44: 000004ad     8 FUNC    GLOBAL DEFAULT    9 fPub
    46: 00002022     1 OBJECT  GLOBAL DEFAULT   19 cPub
    50: 000004bd    77 FUNC    GLOBAL DEFAULT    9 foo
    53: 00002010    16 OBJECT  GLOBAL DEFAULT   18 a
```

(1.b) Section header in librel.so (-fno-pic)

```
readelf -S librel-fPIC.so

Section Headers:
[Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
[ 5] .rel.dyn          REL             000002e8 0002e8 000080 08   A  3   0  4
[ 7] .plt              PROGBITS        00000390 000390 000010 04  AX  0   0 16
[ 8] .plt.got          PROGBITS        000003a0 0003a0 000010 08  AX  0   0  8
[ 9] .text             PROGBITS        000003b0 0003b0 00015a 00  AX  0   0 16
[16] .got              PROGBITS        00001ff0 000ff0 000010 04  WA  0   0  4
[17] .got.plt          PROGBITS        00002000 001000 00000c 04  WA  0   0  4
[18] .data             PROGBITS        0000200c 00100c 000014 00  WA  0   0  4
[19] .bss              NOBITS          00002020 001020 000004 00  WA  0   0  1
[21] .symtab           SYMTAB          00000000 00104c 000370 10     22  42  4
```

(1.c) Symbol's section listing in librel.so (-fno-pic)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
     5: 000004bd [.text]   77 FUNC    GLOBAL DEFAULT    9 foo
     9: 000004ad [.text]    8 FUNC    GLOBAL DEFAULT    9 fPub
    10: 00002022 [.bss ]    1 OBJECT  GLOBAL DEFAULT   19 cPub
    12: 00002010 [.data]   16 OBJECT  GLOBAL DEFAULT   18 a

Symbol table '.symtab' contains 55 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
    30: 000004b5 [.text]    8 FUNC    LOCAL  DEFAULT    9 fLocal
    31: 00002021 [.bss ]    1 OBJECT  LOCAL  DEFAULT   19 cLocal
    44: 000004ad [.text]    8 FUNC    GLOBAL DEFAULT    9 fPub
    46: 00002022 [.bss ]    1 OBJECT  GLOBAL DEFAULT   19 cPub
    50: 000004bd [.text]   77 FUNC    GLOBAL DEFAULT    9 foo
    53: 00002010 [.data]   16 OBJECT  GLOBAL DEFAULT   18 a
```

(1.d) Zero value symbol listing in librel.so (-fno-pic)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
     2: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
     3: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
     4: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__

Symbol table '.symtab' contains 55 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
    20: 00000000     0 SECTION LOCAL  DEFAULT   20
    21: 00000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    29: 00000000     0 FILE    LOCAL  DEFAULT  ABS rel.c
    32: 00000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    34: 00000000     0 FILE    LOCAL  DEFAULT  ABS
    42: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
    45: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
    47: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
    54: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
```

(2.a) Symbol table in librel.so (default)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table ’.dynsym’ contains 14 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
     5: 000004c1    96 FUNC    GLOBAL DEFAULT    9 foo
     9: 0000049d    18 FUNC    GLOBAL DEFAULT    9 fPub
    10: 00002022     1 OBJECT  GLOBAL DEFAULT   19 cPub
    12: 00002010    16 OBJECT  GLOBAL DEFAULT   18 a

Symbol table ’.symtab’ contains 56 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
    30: 000004af    18 FUNC    LOCAL  DEFAULT    9 fLocal
    31: 00002021     1 OBJECT  LOCAL  DEFAULT   19 cLocal
    45: 0000049d    18 FUNC    GLOBAL DEFAULT    9 fPub
    47: 00002022     1 OBJECT  GLOBAL DEFAULT   19 cPub
    51: 000004c1    96 FUNC    GLOBAL DEFAULT    9 foo
    54: 00002010    16 OBJECT  GLOBAL DEFAULT   18 a
```

(2.b) Section header in librel.so (default)

```
readelf -S librel-fPIC.so

Section Headers:
[Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
[ 5] .rel.dyn          REL             000002e8 0002e8 000068 08   A  3   0  4
[ 6] .init             PROGBITS        00000350 000350 000023 00  AX  0   0  4
[ 7] .plt              PROGBITS        00000380 000380 000010 04  AX  0   0 16
[ 8] .plt.got          PROGBITS        00000390 000390 000010 08  AX  0   0  8
[ 9] .text             PROGBITS        000003a0 0003a0 000185 00  AX  0   0 16
[16] .got              PROGBITS        00001fec 000fec 000014 04  WA  0   0  4
[17] .got.plt          PROGBITS        00002000 001000 00000c 04  WA  0   0  4
[18] .data             PROGBITS        0000200c 00100c 000014 00  WA  0   0  4
[19] .bss              NOBITS          00002020 001020 000004 00  WA  0   0  1
[21] .symtab           SYMTAB          00000000 00104c 000380 10     22  43  4
```

(2.c) Symbol's section listing in librel.so (default)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
     5: 000004c1 [.text]    96 FUNC    GLOBAL DEFAULT    9 foo
     9: 0000049d [.text]    18 FUNC    GLOBAL DEFAULT    9 fPub
    10: 00002022 [.bss ]     1 OBJECT  GLOBAL DEFAULT   19 cPub
    12: 00002010 [.data]    16 OBJECT  GLOBAL DEFAULT   18 a

Symbol table '.symtab' contains 56 entries:
   Num:    Valor         Tam  Tipo    Unión  Vis      Nombre Ind
    30: 000004af [.text]   18 FUNC    LOCAL  DEFAULT    9 fLocal
    31: 00002021 [.bss ]    1 OBJECT  LOCAL  DEFAULT   19 cLocal
    45: 0000049d [.text]    18 FUNC    GLOBAL DEFAULT    9 fPub
    47: 00002022 [.bss ]    1 OBJECT  GLOBAL DEFAULT   19 cPub
    51: 000004c1 [.text]   96 FUNC    GLOBAL DEFAULT    9 foo
    54: 00002010 [.data]   16 OBJECT  GLOBAL DEFAULT   18 a
```

(2.d) Zero value symbol listing in librel.so (default)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
     2: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
     3: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
     4: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__

Symbol table '.symtab' contains 56 entries:
   Num:    Valor         Tam  Tipo    Unión  Vis      Nombre Ind
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
    20: 00000000     0 SECTION LOCAL  DEFAULT   20
    21: 00000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    29: 00000000     0 FILE    LOCAL  DEFAULT  ABS rel.c
    32: 00000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    34: 00000000     0 FILE    LOCAL  DEFAULT  ABS
    43: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
    46: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
    48: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
    55: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
```

(3.a) Symbol table in librel.so (-fPIC)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
     5: 000004d1   102 FUNC    GLOBAL DEFAULT   10 foo
     9: 000004ad    18 FUNC    GLOBAL DEFAULT   10 fPub
    10: 00002026     1 OBJECT  GLOBAL DEFAULT   20 cPub
    12: 00002014    16 OBJECT  GLOBAL DEFAULT   19 a

Symbol table '.symtab' contains 57 entries:
   Num:    Valor  Tam  Tipo    Unión  Vis      Nombre Ind
    31: 000004bf    18 FUNC    LOCAL  DEFAULT   10 fLocal
    32: 00002025     1 OBJECT  LOCAL  DEFAULT   20 cLocal
    46: 000004ad    18 FUNC    GLOBAL DEFAULT   10 fPub
    48: 00002026     1 OBJECT  GLOBAL DEFAULT   20 cPub
    52: 000004d1   102 FUNC    GLOBAL DEFAULT   10 foo
    55: 00002014    16 OBJECT  GLOBAL DEFAULT   19 a
```

(3.b) Section header in librel.so (-fPIC)

```
readelf -S librel-fPIC.so

Section Headers:
[Nr] Name              Type            Addr     Off    Size   ES Flg Lk Inf Al
[ 5] .rel.dyn          REL             000002e8 0002e8 000060 08   A  3   0  4
[ 6] .rel.plt          REL             00000348 000348 000008 08  AI  3  18  4
[ 8] .plt              PROGBITS        00000380 000380 000020 04  AX  0   0 16
[ 9] .plt.got          PROGBITS        000003a0 0003a0 000010 08  AX  0   0  8
[10] .text             PROGBITS        000003b0 0003b0 00018b 00  AX  0   0 16
[17] .got              PROGBITS        00001fec 000fec 000014 04  WA  0   0  4
[18] .got.plt          PROGBITS        00002000 001000 000010 04  WA  0   0  4
[19] .data             PROGBITS        00002010 001010 000014 00  WA  0   0  4
[20] .bss              NOBITS          00002024 001024 000004 00  WA  0   0  1
[22] .symtab           SYMTAB          00000000 001050 000390 10     23  44  4
```

(3.c) Symbol’s section listing in librel.so (-fPIC)

```
young@USys2:˜$ readelf -s librel-fPIC.so

Symbol table ’.dynsym’ contains 14 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
     5: 000004d1 [.text]   102 FUNC    GLOBAL DEFAULT   10 foo
     9: 000004ad [.text]    18 FUNC    GLOBAL DEFAULT   10 fPub
    10: 00002026 [.bss ]     1 OBJECT  GLOBAL DEFAULT   20 cPub
    12: 00002014 [.data]    16 OBJECT  GLOBAL DEFAULT   19 a

Symbol table ’.symtab’ contains 57 entries:
   Num:    Valor          Tam  Tipo    Unión  Vis      Nombre Ind
    31: 000004bf [.text]    18 FUNC    LOCAL  DEFAULT   10 fLocal
    32: 00002025 [.bss ]     1 OBJECT  LOCAL  DEFAULT   20 cLocal
    46: 000004ad [.text]    18 FUNC    GLOBAL DEFAULT   10 fPub
    48: 00002026 [.bss ]     1 OBJECT  GLOBAL DEFAULT   20 cPub
    52: 000004d1 [.text]   102 FUNC    GLOBAL DEFAULT   10 foo
    55: 00002014 [.data]    16 OBJECT  GLOBAL DEFAULT   19 a
```

(3.d) Zero value symbol listing in librel.so (-fPIC)

```
young@USys2:~$ readelf -s librel-fPIC.so

Symbol table '.dynsym' contains 14 entries:
   Num:    Valor          Tam  Tipo    Unión   Vis      Nombre Ind
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
     2: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
     3: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
     4: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__

Symbol table '.symtab' contains 57 entries:
   Num:    Valor          Tam  Tipo    Unión   Vis      Nombre Ind
     0: 00000000     0 NOTYPE  LOCAL  DEFAULT  UND
    21: 00000000     0 SECTION LOCAL  DEFAULT   21
    22: 00000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    30: 00000000     0 FILE    LOCAL  DEFAULT  ABS rel.c
    33: 00000000     0 FILE    LOCAL  DEFAULT  ABS crtstuff.c
    35: 00000000     0 FILE    LOCAL  DEFAULT  ABS
    44: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
    47: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
    49: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
    56: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
```

TOC: 3. Relocation listings for `librel.so`

- -fno-pic case
  - (1.a) Relocs of `librel.so` (-fno-pic)
  - (1.b) Reloc sections of `librel.so` (-fno-pic)
  - (1.c) Reloc Info field of `librel.so` (-fno-pic)
  - (1.d) Zero value symbols of `librel.so` (-fno-pic)
- default
  - (2.a) Relocs of `librel.so` (default)
  - (2.b) Reloc sections of `librel.so` (default)
  - (2.c) Reloc Info field of `librel.so` (default)
  - (2.d) Zero value symbols of `librel.so` (default)
- -fPIC case
  - (3.a) Relocs of `librel.so` (-fPIC)
  - (3.b) Reloc sections of `librel.so` (-fPIC)
  - (3.c) Reloc Info filed of `librel.so` (-fPIC)
  - (3.d) Zero value symbols of `librel.so` (-fPIC)

(1.a) Relocs of librel.so (-fno-pic)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 16 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
000004f3  [000000][08] R_386_RELATIVE
000004fc  [000000][08] R_386_RELATIVE
00001f30  [000000][08] R_386_RELATIVE
00001f34  [000000][08] R_386_RELATIVE
0000200c  [000000][08] R_386_RELATIVE
00002010  [000000][08] R_386_RELATIVE
00002014  [000000][08] R_386_RELATIVE
000004c5  [000009][02] R_386_PC32        000004ad   fPub
0000201c  [000009][01] R_386_32          000004ad   fPub
000004e0  [00000a][01] R_386_32          00002022   cPub
000004e9  [00000a][01] R_386_32          00002022   cPub
00002018  [00000a][01] R_386_32          00002022   cPub
00001ff0  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff4  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff8  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__
```

(1.b) Reloc sections of librel.so (-fno-pic)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 16 entries:
 Desplaz    Sec    Tipo            Val.Símbolo Nom. Símbolo
000004f3  [.text]  R_386_RELATIVE
000004fc  [.text]  R_386_RELATIVE
00001f30  [     ]  R_386_RELATIVE
00001f34  [     ]  R_386_RELATIVE
0000200c  [.data]  R_386_RELATIVE
00002010  [.data]  R_386_RELATIVE
00002014  [.data]  R_386_RELATIVE
000004c5  [.text]  R_386_PC32        000004ad   fPub
0000201c  [.data]  R_386_32          000004ad   fPub
000004e0  [.text]  R_386_32          00002022   cPub
000004e9  [.text]  R_386_32          00002022   cPub
00002018  [.data]  R_386_32          00002022   cPub
00001ff0  [.got ]  R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff4  [.got ]  R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff8  [.got ]  R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  [.got ]  R_386_GLOB_DAT    00000000   __gmon_start__
```

(1.c) Reloc Info field of librel.so (-fno-pic)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 16 entries:
 Desplaz   Info:3    Symbols             Info:1  Types
000004f3  [000000]                        [08] R_386_RELATIVE
000004fc  [000000]                        [08] R_386_RELATIVE
00001f30  [000000]                        [08] R_386_RELATIVE
00001f34  [000000]                        [08] R_386_RELATIVE
0000200c  [000000]                        [08] R_386_RELATIVE
00002010  [000000]                        [08] R_386_RELATIVE
00002014  [000000]                        [08] R_386_RELATIVE
000004c5  [000009] fPub                   [02] R_386_PC32        000004ad
0000201c  [000009] fPub                   [01] R_386_32          000004ad
000004e0  [00000a] cPub                   [01] R_386_32          00002022
000004e9  [00000a] cPub                   [01] R_386_32          00002022
00002018  [00000a] cPub                   [01] R_386_32          00002022
00001ff0  [000001] __cxa_finalize         [06] R_386_GLOB_DAT    00000000
00001ff4  [000002] _ITM_registerTMCloneTa [06] R_386_GLOB_DAT    00000000
00001ff8  [000003] _ITM_deregisterTMClone [06] R_386_GLOB_DAT    00000000
00001ffc  [000004] __gmon_start__         [06] R_386_GLOB_DAT    00000000
```

(1.d) Zero value symbols of librel.so (-fno-pic)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 16 entries:
 Desplaz     Info    Tipo            Val.Símbolo Nom. Símbolo
00001ff0  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize         [.got]
00001ff4  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa [.got]
00001ff8  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone [.got]
00001ffc  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__         [.got]
```

(2.a) Relocs of librel.so (default)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 13 entries:
 Desplaz     Info    Tipo            Val.Símbolo Nom. Símbolo
00001f2c  [000000][08] R_386_RELATIVE
00001f30  [000000][08] R_386_RELATIVE
0000200c  [000000][08] R_386_RELATIVE
00002010  [000000][08] R_386_RELATIVE
00002014  [000000][08] R_386_RELATIVE
000004d5  [000009][02] R_386_PC32        0000049d   fPub
0000201c  [000009][01] R_386_32          0000049d   fPub
00001fec  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff0  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff4  [00000a][06] R_386_GLOB_DAT    00002022   cPub
00002018  [00000a][01] R_386_32          00002022   cPub
00001ff8  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__
```

(2.b) Reloc sections of librel.so (default)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 13 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00001f2c  [      ] R_386_RELATIVE
00001f30  [      ] R_386_RELATIVE
0000200c  [.data] R_386_RELATIVE
00002010  [.data] R_386_RELATIVE
00002014  [.data] R_386_RELATIVE
000004d5  [.text] R_386_PC32        0000049d   fPub
0000201c  [.data] R_386_32          0000049d   fPub
00001fec  [.got ] R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff0  [.got ] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff4  [.got ] R_386_GLOB_DAT    00002022   cPub
00002018  [.data] R_386_32          00002022   cPub
00001ff8  [.got ] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  [.got ] R_386_GLOB_DAT    00000000   __gmon_start__
```

(2.c) Reloc Info field of librel.so (default)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 13 entries:
 Desplaz    Info:3     Symbols              Info:1  Types
00001f2c   [000000]                          [08] R_386_RELATIVE
00001f30   [000000]                          [08] R_386_RELATIVE
0000200c   [000000]                          [08] R_386_RELATIVE
00002010   [000000]                          [08] R_386_RELATIVE
00002014   [000000]                          [08] R_386_RELATIVE
000004d5   [000009] fPub                     [02] R_386_PC32        0000049d
0000201c   [000009] fPub                     [01] R_386_32          0000049d
00001fec   [000001] __cxa_finalize           [06] R_386_GLOB_DAT    00000000
00001ff0   [000002] _ITM_registerTMCloneTa  [06] R_386_GLOB_DAT    00000000
00001ff4   [00000a] cPub                     [06] R_386_GLOB_DAT    00002022
00002018   [00000a] cPub                     [01] R_386_32          00002022
00001ff8   [000003] _ITM_deregisterTMClone  [06] R_386_GLOB_DAT    00000000
00001ffc   [000004] __gmon_start__           [06] R_386_GLOB_DAT    00000000
```

(2.d) Zero value symbols of librel.so (default)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 13 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo

00001fec  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize         [.got]
00001ff0  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa [.got]
00001ff8  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone [.got]
00001ffc  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__         [.got]
```

(3.a) Relocs of librel.so (-fPIC)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 12 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00001f24  [000000][08] R_386_RELATIVE
00001f28  [000000][08] R_386_RELATIVE
00002010  [000000][08] R_386_RELATIVE
00002014  [000000][08] R_386_RELATIVE
00002018  [000000][08] R_386_RELATIVE
00001fec  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff0  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff4  [00000a][06] R_386_GLOB_DAT    00002026   cPub
0000201c  [00000a][01] R_386_32          00002026   cPub
00001ff8  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__
00002020  [000009][01] R_386_32          000004ad   fPub

La sección de reubicación '.rel.plt' at offset 0x348 contains 1 entry:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
0000200c  00000907 R_386_JUMP_SLOT   000004ad   fPub
```

(3.b) Reloc sections of librel.so (-fPIC)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 12 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00001f24  [      ] R_386_RELATIVE
00001f28  [      ] R_386_RELATIVE
00002010  [.data] R_386_RELATIVE
00002014  [.data] R_386_RELATIVE
00002018  [.data] R_386_RELATIVE
00001fec  [.got ] R_386_GLOB_DAT    00000000   __cxa_finalize
00001ff0  [.got ] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
00001ff4  [.got ] R_386_GLOB_DAT    00002026   cPub
0000201c  [.data] R_386_32          00002026   cPub
00001ff8  [.got ] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
00001ffc  [.got ] R_386_GLOB_DAT    00000000   __gmon_start__
00002020  [.data] R_386_32          000004ad   fPub

La sección de reubicación '.rel.plt' at offset 0x348 contains 1 entry:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
0000200c  00000907 R_386_JUMP_SLOT   000004ad   fPub
```

(3.c) Reloc Info field of librel.so (-fPIC)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 12 entries:
 Desplaz   Info:3    Symbols             Info:1  Types
00001f24  [000000]                        [08] R_386_RELATIVE
00001f28  [000000]                        [08] R_386_RELATIVE
00002010  [000000]                        [08] R_386_RELATIVE
00002014  [000000]                        [08] R_386_RELATIVE
00002018  [000000]                        [08] R_386_RELATIVE
00001fec  [000001] __cxa_finalize         [06] R_386_GLOB_DAT    00000000
00001ff0  [000002] _ITM_registerTMCloneTa [06] R_386_GLOB_DAT    00000000
00001ff4  [00000a] cPub                   [06] R_386_GLOB_DAT    00002026
0000201c  [00000a] cPub                   [01] R_386_32          00002026
00001ff8  [000003] _ITM_deregisterTMClone [06] R_386_GLOB_DAT    00000000
00001ffc  [000004] __gmon_start__         [06] R_386_GLOB_DAT    00000000
00002020  [000009] fPub                   [01] R_386_32          000004ad

La sección de reubicación '.rel.plt' at offset 0x348 contains 1 entry:
 Desplaz   Info:3    Symbols             Info:1  Types
0000200c  [000009] fPub                   [07] R_386_JUMP_SLOT   000004ad
```

(3.d) Zero value symbols of librel.so (-fPIC)

```
  readelf -r librel-fPIC.so

La sección de reubicación '.rel.dyn' at offset 0x2e8 contains 12 entries:
 Desplaz    Info    Tipo            Val.Símbolo Nom. Símbolo
00001fec  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize         [.got]
00001ff0  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa  [.got]
00001ff8  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone  [.got]
00001ffc  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__         [.got]

La sección de reubicación '.rel.plt' at offset 0x348 contains 1 entry:
 N/A
```

TOC: Linking for `librel.so`

- Linking the `.data` section for `librel.so`
- Linking the `.text` section for `librel.so`
- Undefined symbols in `librel.so`

TOC: linking the .data section

- resolving local symbol references cLocal, fLocal
- resolving global symbol references cPUb, fPub

```
_st a[] = { { &cLocal,  // 1                typedef struct {
              fLocal }, // 2                     char* p;
            { &cPub,    // 3                     char (*f)(int);
              fPub } }; // 4                  } _st;
```

resolving local symbol references : cLocal, fLocal (1)

- relocs for &cLocal and fLocal
  R_386_32 in .data (-fno-pic) or
  R_386_32 in .data.rel (default, -fPIC)
  → R_386_RELATIVE in .data

symbol	-fno-pic	default	-fPIC
&cLocal	R_386_RELATIVE in .data	R_386_RELATIVE in .data	R_386_RELATIVE in .data
fLocal	R_386_RELATIVE in .data	R_386_RELATIVE in .data	R_386_RELATIVE in .data

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving local symbol references : cLocal, fLocal (2)

- At the beginning of the run time,
  - &cLocal has R_386_RELATIVE reloc
  - fLocal has R_386_RELATIVE reloc
  - the reloc targets are &cLocal, fLocal
  - the offset is stored at the reloc target location
- the dynamic linker will
  - add the *base* (module) address to the *offset*
  - store the added result at the reloc target

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving global symbol references : cPub, fPub (1)

- relocs for &cPub and fPub are maintained
  until the dynamic linking
  R_386_32 in .data (-fno-pic) or
  R_386_32 in .data.rel (default, -fPIC)

symbol	-fno-pic	default	-fPIC
cPub	R_386_32 in .data	R_386_32 in .data	R_386_32 in .data
fPub	R_386_32 in .data	R_386_32 in .data	R_386_32 in .data

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving global symbol references : cPub, fPub (2)

- &cPub and fPub are marked as needing a full 32-bit address
  - these symbols are referenced by their name
  - R_386_32 relocs are generated full absolute addresses at compile time
  - R_386_32 relocs are maintained until dynamic linking

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

TOC: linking the `.text` section

- resolving function symbol definitions `foo`
- resolving function symbol references `fPub(a)`, `fLocal(a)`
- resolving global symbol references `&cPub`, `cPub`
- resolving local symbol references `&cLocal`, `cLocal`

- (1) resolving global symbol references (non-PIC)
- (2) resolving global symbol references (PIE)
- (3) resolving global symbol references (PIC)

```
int foo(int a) {          // 5             + cPub            // 9
  return fPub(a)          // 6             + (int) &cLocal   // 10
       + fLocal(a)        // 7             + cLocal;         // 11
       + (int) &cPub      // 8       }
```

resolving public function symbol definition : foo(int)

- foo(int a) reloc .text is fixed up fully,
  does no appear in the library librel.so

- the function foo(int) as a public symbol
  which is called externally (_outside_ of the library)

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving global function symbol references : fPub(a)

- the PIC reloc of a global function reference in .text section will cause the linker to add a PLT entry and a corresponding GOT entry
  - the reloc of fPub(a) is translated into a indirect call through the PLT entry
  - the GOT entry gets a R_386_JUMP_SLOT reloc using the symbol fPub

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving global data symbol references : cPub

- the PIC relocs of a global data symbol reference in .text section will cause the linker to add a GOT entry to hold them
- the relocs at &cPub (address) and cPub (data) will have an GOT entry to hold &cPub
    - the symbol value is an address of the symbol
- the GOT entry is marked with a R_386_GLOB_DAT reloc asking the dynamic linker for the full 32-bit absolute address

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving local function symbol references : fLocal(a)

- the reloc of a local function reference in .text section is converted into a direct call to the function
    - the reloc of fLocal(a) is converted into a direct call to fLocal()
    - because it can be fully resolved at the final linker stage

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

resolving local data symbol references : `cLocal`

- the relocs of local data symbol references in `.text` section are fully resolved at final link time
- the relocs at `&cLocal` (address) and `cLocal` (data) are not required

`http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html`

(1) resolving global symbol references (non-PIC)

- for a non-PIC
  - cPub reference in .text section has R_386_32 reloc

    ```
    [readelf -r]
    000004e0  00000a01 R_386_32          00002022   cPub
    000004e9  00000a01 R_386_32          00002022   cPub
    ```

  - fPub call in .text section has R_386_PC32 reloc

    ```
    [readelf -r]
    000004c5  00000902 R_386_PC32        000004ad   fPub
    ```

  - the dynamic linker will store at the reloc target
    the full 32-bit absolute and relative addresses

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

(2) resolving global symbol references (PIE)

- for a PIE (default)
  - cPub reference in .text section has R_386_GOT32 reloc
    → R_386_GLOB_DAT in .got

    ```
    [readelf -r]
    00001ff4  00000a06 R_386_GLOB_DAT    00002022   cPub
    ```
  - fPub call in .text section has R_386_PLT32 reloc
    → R_386_PC32 in .got

    ```
    [readelf -r]
    000004d5  00000902 R_386_PC32        0000049d   fPub
    ```
  - the PLT is not used
    because fPub is defined in the same module (rel.c)

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

(3) resolving global symbol references (PIC)

- for a PIC
  - cPub reference in .text section has R_386_GOT32 reloc
    → R_386_GLOB_DAT in .got

    ```
    [readelf -r]
    00001ff4  00000a06 R_386_GLOB_DAT    00002026   cPub
    ```

  - fPub call in .text section has R_386_PLT32 reloc
    → R_386_JUMP_SLOT in .got

    ```
    [readelf -r]
    0000200c  00000907 R_386_JUMP_SLOT   000004ad   fPub
    ```

http://netwinder.osuosl.org/users/p/patb/public_html/elf_relocs.html

TOC: Undefined symbols in `librel.so`

- Undefined symbols in a shared object
- A self-contained shared object
- Weak and strong symbols
- Undefined weak symbols in a shared object

Undefined symbols in a shared object

- when the link-editor is generating
  a shared object output file,
  undefined symbols are allowed to *remain*
  at the end of the link-edit

- then the shared object is able
  to import symbols from a dynamic executable
  that defines the shared object as a dependency

https://docs.oracle.com/cd/E19120-01/open.solaris/819-0690/chapter2-9/index.html

A self-contained shared object

- A self-contained shared object
  - all references to external symbols are *satisfied* by named dependencies
  - provides maximum *flexibility*
  - do not have to determine and establish dependencies

`https://docs.oracle.com/cd/E19120-01/open.solaris/819-0690/chapter2-9/index.html`

Weak and strong symbols

- Strong symbols
  - functions and initialized global variables
- Weak symbols
  - uninitialized global variables

```
// p1.c

int foo =5; // strong

p1 () {     // strong

}
```

```
// p2.c

int foo;     // weak

p2() {       // strong

}
```

https://www.quora.com/What-are-strong-and-weak-symbols-in-C

Undefined weak symbols in a shared object

- Weak symbol references that remain unresolved,
  do not result in a fatal error condition,
  no matter what output file type is being generated.

```
’.dynsym’ and ’.symtab’
     ?: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __cxa_finalize
     ?: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_registerTMCloneTable
     ?: 00000000     0 NOTYPE  WEAK   DEFAULT  UND _ITM_deregisterTMCloneTab
     ?: 00000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__

Relocs for undefined weak symbols
[.got]  [000001][06] R_386_GLOB_DAT    00000000   __cxa_finalize
[.got]  [000002][06] R_386_GLOB_DAT    00000000   _ITM_registerTMCloneTa
[.got]  [000003][06] R_386_GLOB_DAT    00000000   _ITM_deregisterTMClone
[.got]  [000004][06] R_386_GLOB_DAT    00000000   __gmon_start__
```

https://docs.oracle.com/cd/E19120-01/open.solaris/819-0690/chapter2-11/index.html

TOC: Locating relocs and symbol references of `librel.so`

- Locating `.data` section relocs of `librel.so`
- Locating `.text` section relocs of `librel.so`
- Locating `.data` section symbol references of `librel.so`
- Locating `.text` section symbol references of `librel.so`

TOC: Locating .data section relocs of librel.so

- Finding .data section relocs (-fno-pic) for librel.so
- Finding .data section relocs (default) for librel.so
- Finding .data section relocs (-fPIC) for librel.so
- Locating R_386_RELATIVE relocs in .data section (-fPIC)

```
_st a[] = { { &cLocal,  // 1                typedef struct {
              fLocal }, // 2                    char* p;
            { &cPub,    // 3                    char (*f)(int);
              fPub } }; // 4                  } _st;
```

Finding .data section relocs (no-PIC) for librel.so

```
[readelf -S]
  [18] .data             PROGBITS        0000200c 00100c 000014 00   WA  0   0  4
  Address: 0000200c Size: 000014 ---> [200c, 201f]

[readelf -s]
    12: 00002010    16 OBJECT  GLOBAL DEFAULT   18 a

[readelf -r]
0000200c  00000008 R_386_RELATIVE                                  ....  .data 0000200c
00002010  00000008 R_386_RELATIVE                                  ....  .data 0000200c (cLocal)
00002014  00000008 R_386_RELATIVE                                  ....  .data 0000200c (fLocal)
00002018  00000a01 R_386_32          00002022   cPub ....  .data 0000200c
0000201c  00000901 R_386_32          000004ad   fPub ....  .data 0000200c
```

Finding .data section relocs (default) for librel.so

```
[readelf -S]
  [18] .data             PROGBITS        0000200c 00100c 000014 00  WA  0   0  4
  Address: 0000200c Size: 000014 ---> [200c, 201f]

[readelf -s]
    12: 00002010    16 OBJECT  GLOBAL DEFAULT   18 a

[readelf -r]
0000200c  00000008 R_386_RELATIVE                        ....  .data 0000200c
00002010  00000008 R_386_RELATIVE                        ....  .data 0000200c (cLocal)
00002014  00000008 R_386_RELATIVE                        ....  .data 0000200c (fLocal)
00002018  00000a01 R_386_32         00002022   cPub ....  .data 0000200c
0000201c  00000901 R_386_32         0000049d   fPub ....  .data 0000200c
```

Finding .data section relocs (PIC) for librel.so

```
[readelf -S]
  [19] .data             PROGBITS         00002010 001010 000014 00   WA  0   0  4
  Address: 0000200c Size: 000014 ---> [2010, 2024]

[readelf -s]
    12: 00002014    16 OBJECT  GLOBAL DEFAULT   19 a

[readelf -r]
00002014 R_386_RELATIVE     *ABS* ... .data    00002010    (cLocal)
00002018 R_386_RELATIVE     *ABS* ... .data    00002010    (fLocal)
0000201c R_386_32           cPub .... .data    00002010
00002020 R_386_32           fPub .... .bss     00002024
```

Locating R_386_RELATIVE relocs in .data section (-fPIC)

- section address

```
[readelf -S]
.data   = 00002010
.bss    = 00002024
```

- symbol values

```
[readelf -s]
fLocal = 000004bf
cLocal = 00002025
a      = 00002014
```

- R_386_RELATIVE relocs

```
[readelf -r]
00002010  00000008 R_386_RELATIVE
00002014  00000008 R_386_RELATIVE              (cLocal)
00002018  00000008 R_386_RELATIVE              (fLocal)
```

- hexadumps of .data section

```
[objdump -s -j .got]
0x00002010 10200000 25200000 bf040000 00000000 . ..% ..........
0x00002020 00000000                            ....
```

TOC: Locating .text section relocs of librel.so -

- Finding .text section relocs of librel.so (-fno-PIC)
- Finding .text section relocs of librel.so (default)
- Finding .text section relocs of librel.so (-fPIC)
- Locating R_386_JUMP_SLOT relocs in .plt section (-fPIC)
- Locating R_386_GLOB_DAT relocs in .got section (-fPIC)

```
int foo(int a) {        // 5           + cPub            // 9
  return fPub(a)        // 6           + (int) &cLocal   // 10
       + fLocal(a)      // 7           + cLocal;         // 11
       + (int) &cPub    // 8      }
```

Finding .text section relocs (no-PIC) for librel.so

```
[readelf -S]
  [ 9] .text             PROGBITS        000003b0 0003b0 00015a 00   AX  0   0 16
  Address: 000003b0 Size: 00015a ---> [3b0, 509]

[readelf - r]
000004c5  00000902 R_386_PC32         000004ad   fPub ....  .text 000003b0
000004e0  00000a01 R_386_32           00002022   cPub ....  .text 000003b0
000004e9  00000a01 R_386_32           00002022   cPub ....  .text 000003b0
000004f3  00000008 R_386_RELATIVE                     ....  .text 000003b0
000004fc  00000008 R_386_RELATIVE                     ....  .text 000003b0
```

Finding .text section relocs (default) for librel.so

```
[readelf -S]
  [ 9] .text             PROGBITS        000003a0 0003a0 000185 00  AX  0   0 16
  Address: 000003a0 Size: 000185 ---> [3a0, 524]

  [16] .got              PROGBITS        00001fec 000fec 000014 04  WA  0   0  4
  Address: 00001fec Size: 000014 ---> [1fec, 1fff]

[readelf - r]
000004d5  00000902 R_386_PC32        0000049d   fPub ....  .text 000003a0
00001ff4  00000a06 R_386_GLOB_DAT    00002022   cPub ....  .got  00001fec
```

Finding .text section relocs (-flPPIC) for librel.so

```
[readelf -S]
  [10] .text             PROGBITS        000003b0 0003b0 00018b 00   AX  0   0 16
 Address: 000003b0 Size: 00018b ---> [3a0, 53a]

  [17] .got              PROGBITS        00001fec 000fec 000014 04   WA  0   0  4
  Address: 00001fec Size: 000014 ---> [1fec, 1fff]

  [18] .got.plt          PROGBITS        00002000 001000 000010 04   WA  0   0  4
  Address: 00002000 Size: 000010 ---> [2000, 200f]

[readelf - r]
00001ff4 R_386_GLOB_DAT    cPub .... .got     00001fec
0000200c R_386_JUMP_SLOT   fPub .... .got.plt 00002000
```

Locating R_386_JUMP_SLOT relocs in .plt section (-fPIC)

- .plt section address

```
[readelf -S]
.plt = 00000380
```

- symbol value

```
[readelf -s]
fPub   = 000004ad
```

- R_386_JUMP_SLOT relocs in .rel.dyn

```
[readelf -r]
0000200c  00000907 R_386_JUMP_SLOT   000004ad   fPub
```

- hexadumps of .got.plt section

```
[objdump -s -j .got.plt]
2000 2c1f0000 00000000 00000000 96030000  ,...............
---> 200c 00000396
```

- hexadumps of .plt section

```
[objdump -dr]
00000390 <fPub@plt>:
  390:   ff a3 0c 00 00 00       jmp    *0xc(%ebx)
  396:   68 00 00 00 00          push   $0x0
  39b:   e9 e0 ff ff ff          jmp    380 <.plt>
```

Locating R_386_GLOB_DAT relocs in .got section (-fPIC)

- .got section address

```
[readelf -S]
.got = 00001fec
```

- symbol value

```
[readelf -s]
cPub  = 00002026   ... in the same module
```

- R_386_GLOB_DAT relocs in .rel.dyn

```
[readelf -r]
00001ff4  00000a06 R_386_GLOB_DAT    00002026   cPub
```

- hexadumps of .got section

```
[objdump -s -j .got]
1fec 00000000 00000000[00000000] 00000000  ................
1ffc 00000000                             ....


---> 1ff4 00000000
```

TOC: Locating .data section symbol references of librel.so

- (a) referencing symbols in .data section in librel.so
- (b) disassemble .data section in librel.so
- (c) hexadump .data section in librel.so

```
_st a[] = { { &cLocal,  // 1              typedef struct {
              fLocal }, // 2                   char* p;
            { &cPub,    // 3                   char (*f)(int);
              fPub } }; // 4                 } _st;
```

(a) referencing symbols in .data section of librel.so

- .data section of librel.so with -fno-pic

```
0x00002010 00002021    cLocal  R_386_RELATIVE
0x00002014 000004b5    fLocal  R_386_RELATIVE
0x00002018 00000000    cPub    R_386_32
0x0000201c 00000000    fPub    R_386_32
```

- .data section of librel.so with default

```
0x00002010 00002021    cLocal  R_386_RELATIVE
0x00002014 000004af    fLocal  R_386_RELATIVE
0x00002018 00000000    cPub    R_386_32
0x0000201c 00000000    fPub    R_386_32
```

- .data section of librel.so with -fPIC

```
0x00002014 00002025    cLocal  R_386_RELATIVE
0x00002018 000004bf    fLocal  R_386_RELATIVE
0x0000201c 00000000    cPub    R_386_32
0x00002020 00000000    fPub    R_386_320
```

(b) Disassemble .data section in librel.so (-fPIC)

```
Desensamblado de la sección .data:

00002010 <__dso_handle>:
    2010:       10 20                   adc    %ah,(%eax)
        ...

00002014 <a>:
    2014:       25 20 00 00 bf          and    $0xbf000020,%eax
    2019:       04 00                   add    $0x0,%al
        ...
```

(c) Hexadump .data section in librel.so (-fPIC)

```
objdump -s -j .data librel-fPIC.so

librel-fPIC.so:     file format elf32-i386

Contents of section .data:
 2010 10200000 25200000 bf040000 00000000  . ..% ..........
 2020 00000000                             ....


readelf -x .data librel-fPIC.so

Hex dump of section '.data':
  0x00002010 10200000 25200000 bf040000 00000000 . ..% ..........
  0x00002020 00000000                            ....
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-

TOC: Locating .text section symbol references of librel.so

- (a) calling fPub in the .text section of librel.so
- (b) referencing cPub in the .text section of librel.so
- (c) hexadump .got section of librel.so
- (d) hexadump .plt section of librel.so
- (e) hexadump .plt.got section of librel.so
- (f) disassemble .plt section of librel.so
- (g) disassemble .plt.got section of librel.so
- Examining .got and .plt section

```
int foo(int a) {         // 5
  return fPub(a)         // 6
       + fLocal(a)       // 7
       + (int) &cPub     // 8
       + cPub            // 9
       + (int) &cLocal   // 10
       + cLocal;         // 11
}
```

(a) calling fPub in the .text section of librel.so

- librel.so with -fno-pic

```
4c4:  e8 fc ff ff ff          call   4c5 <foo+0x8> ; call func at 4c5
                                 ;   4c5 = 4bd + 8; fPub func ref location
                                 ;  -4 = fffffffc; offset (pc adjust)
                                 ;   000004ad <fPub>:
                                 ;   000004bd <foo>: ...
                                     4c5+4
```

- librel.so with default

```
4d4:  e8 fc ff ff ff          call   4d5 <foo+0x14> ; call func at 4d5
                                 ;   4d5 = 4c1 + 14; fPub func ref location
                                 ;  -4 = fffffffc; offset (pc adjust)
                                 ;   0000049d <fPub>:
                                 ;   000004c1 <foo>: ...
```

- librel.so with -fPIC (fPub : PLT)

```
4e7:  e8 a4 fe ff ff          call   390 <fPub@plt> ; call func at 390
                                 ;   4e8 = fPub func ref location
                                 ;  -15c = fffffea4; offset (4e8+4-15c=390)
                                 ;   00000390 <fPub@plt>:
                                 ;   000004ad <fPub>:
                                 ;   000004d1 <foo>: ...
```

(b) referencing cPub in the .text section of librel.so

- librel.so with -fno-pic

```
4e6:   0f b6 05 00 00 00 00     movzbl 0x0,%eax
                                      ; 4e9 = cPub symbol ref location
                                      ;   0 = offset (no pc adjust)
```

- librel.so with default (cPub : GOT)

```
4f8:   8b 83 f4 ff ff ff        mov    -0xc(%ebx),%eax
                                       ; 4fa = cPub symbol ref location
                                       ;  -c = offset (1fec-4+c=1ff4)
                                       ;  00001fec <.got>: ...
                                       ; same module reference (pc adjust)
```

- librel.so with -fPIC (cPub : GOT)

```
50e:   8b 83 f4 ff ff ff        mov    -0xc(%ebx),%eax
                                       ; 510 = cPub symbol ref location
                                       ;  -c = offset (1fec-4+c=1ff4)
                                       ;  00001fec <.got>: ...
                                       ; same module reference (pc adjust)
```

(c) Hexadump .got section in librel.so (-fPIC)

```
objdump -s -j .got librel-fPIC.so

Contents of section .got:
 1fec 00000000 00000000 00000000 00000000  ................
 1ffc 00000000                             ....
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

(d) Hexadump .plt section in librel.so (-fPIC)

```
objdump -s -j .plt librel-fPIC.so

librel-fPIC.so:     file format elf32-i386

Contents of section .plt:
 0380 ffb30400 0000ffa3 08000000 00000000  ................
 0390 ffa30c00 00006800 000000e9 e0ffffff  ......h.........
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

(e) Hexadump .plt.got section in librel.so (-fPIC)

```
objdump -s -j .plt.got librel-fPIC.so
```

```
Contents of section .plt.got:
 03a0 ffa3ecff ffff6690 ffa3fcff ffff6690  ......f.......f.
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

(f) Disassemble .plt section in librel.so (-fPIC)

```
objdump -dr librel-fPIC

00000380 <.plt>:
 380:    ff b3 04 00 00 00        pushl  0x4(%ebx)
 386:    ff a3 08 00 00 00        jmp    *0x8(%ebx)
 38c:    00 00                    add    %al,(%eax)
         ...

00000390 <fPub@plt>:
 390:    ff a3 0c 00 00 00        jmp    *0xc(%ebx)
 396:    68 00 00 00 00           push   $0x0
 39b:    e9 e0 ff ff ff           jmp    380 <.plt>
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

(g) Disassemble .plt.got section in librel.so (-fPIC)

```
objdump -dr librel-fPIC.so

000003a0 <__cxa_finalize@plt>:
 3a0:   ff a3 ec ff ff ff       jmp    *-0x14(%ebx)
 3a6:   66 90                   xchg   %ax,%ax

000003a8 <__gmon_start__@plt>:
 3a8:   ff a3 fc ff ff ff       jmp    *-0x4(%ebx)
 3ae:   66 90                   xchg   %ax,%ax
```

https://stackoverflow.com/questions/1685483/how-can-i-examine-contents-of-a-data-s

Examining .got and .plt section (-fPIC)

- hexadumps of .got section

```
00000000 ...                    ... at 1fec
00000000 ...                    ... at 1ff0
00000000 ...                    ... at 1ff4
00000000 ...                    ... at 1ff8
00000000 ...                    ... at 1ffc
```

- .plt section disassembly

```
00000380 <.plt>:
380:  ff b3 04 00 00 00       pushl  0x4(%ebx)
386:  ff a3 08 00 00 00       jmp    *0x8(%ebx)
38c:  00 00                   add    %al,(%eax)
      ...

00000390 <fPub@plt>:
390:  ff a3 0c 00 00 00       jmp    *0xc(%ebx)
396:  68 00 00 00 00          push   $0x0
39b:  e9 e0 ff ff ff          jmp    380 <.plt>
```