ELF1 7 Examples - 9 Assembly Listings - ELF Study 1999

Young W. Lim

2020-01-28 Tue

Outline

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: Relocs background in shared object and executable files

- Relocs in a PIC shared object (.so) file
- Relocs in a non-PIC executable file
- PIC, PIE, and non-PIC executables

Example library code

```
typedef struct {
  char* p;
  char (*f)(int);
} _st;

char fPub(int a) {
  return a;
}

static char fLocal(int b) {
  return b;
}

char cPub;              // uninitialized
static char cLocal;     // uninitialized
```

```
_st a[] = { { &cLocal,  // 1
              fLocal }, // 2
            { &cPub,    // 3
              fPub } }; // 4

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

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

Example executable code

- the main function code

```
extern int fPub(int);
extern int cPub;

int main() {
  return fPub(123)   // 1
       + cPub;       // 2
}
```

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

Using a shared library

- creating a shared library

```
gcc -m32 -fPIC -c -g rel.c
gcc -m32 -shared rel.o -o librel.so
```

- linking with a shared library

```
gcc -m32 -c -g main.c
gcc -m32 main.o -Wl,-q -L/home/young/ -lrel -o run_dynamic
```

- run a dynamic executable

```
LD_LIBRARY_PATH=/home/young/ ./run_dynamic
```

https://renenyffenegger.ch/notes/development/languages/C-C-plus-plus/GCC/create-libraries/index

TOC: A. `rel.o` function listings

- (a) `-fno-pic` : `fPub` function listing in `rel.o`
- (b) `-fno-pic` : `fLocal` function listing in `rel.o`
- (c) `-fno-pic` : `foo` function listing in `rel.o` (1)
- (d) `-fno-pic` : `foo` function listing in `rel.o` (2)

(a) -fno-pic : fPub function listing in rel.o

```
00000000 <fPub>:
   0:   55                      push   %ebp
   1:   89 e5                   mov    %esp,%ebp
   3:   8b 45 08                mov    0x8(%ebp),%eax
   6:   5d                      pop    %ebp
   7:   c3                      ret
```

(b) -fno-pic : fLocal function listing in rel.o

```
00000008 <fLocal>:
   8:   55                      push   %ebp
   9:   89 e5                   mov    %esp,%ebp
   b:   8b 45 08                mov    0x8(%ebp),%eax
   e:   5d                      pop    %ebp
   f:   c3                      ret
```

(c) -fno-pic : foo function listing in rel.o (1)

```
00000010 <foo>:
  10:   55                      push   %ebp
  11:   89 e5                   mov    %esp,%ebp
  13:   53                      push   %ebx
  14:   ff 75 08                pushl  0x8(%ebp)
  17:   e8 fc ff ff ff          call   18 <foo+0x8>
                        18: R_386_PC32  fPub
  1c:   83 c4 04                add    $0x4,%esp
  1f:   0f be d8                movsbl %al,%ebx
  22:   ff 75 08                pushl  0x8(%ebp)
  25:   e8 de ff ff ff          call   8 <fLocal>
  2a:   83 c4 04                add    $0x4,%esp
  2d:   0f be c0                movsbl %al,%eax
  30:   01 d8                   add    %ebx,%eax
  32:   ba 00 00 00 00          mov    $0x0,%edx
                        33: R_386_32    cPub
```

(d) -fno-pic : foo function listing in rel.o (2)

```
37:   01 c2                      add    %eax,%edx
39:   0f b6 05 00 00 00 00       movzbl 0x0,%eax
                      3c: R_386_32    cPub
40:   0f be c0                   movsbl %al,%eax
43:   01 d0                      add    %edx,%eax
45:   ba 00 00 00 00             mov    $0x0,%edx
                      46: R_386_32    .bss
4a:   01 c2                      add    %eax,%edx
4c:   0f b6 05 00 00 00 00       movzbl 0x0,%eax
                      4f: R_386_32    .bss
53:   0f be c0                   movsbl %al,%eax
56:   01 d0                      add    %edx,%eax
58:   8b 5d fc                   mov    -0x4(%ebp),%ebx
5b:   c9                         leave
5c:   c3                         ret
```

TOC: B. librel.so function listings

(a) -fno-pic : fPub function listing in librel.so

```
000004ad <fPub>:
 4ad:   55                      push   %ebp
 4ae:   89 e5                   mov    %esp,%ebp
 4b0:   8b 45 08                mov    0x8(%ebp),%eax
 4b3:   5d                      pop    %ebp
 4b4:   c3                      ret
```

(b) -fno-pic : fLocal function listing in librel.so

```
000004b5 <fLocal>:
 4b5:   55                      push   %ebp
 4b6:   89 e5                   mov    %esp,%ebp
 4b8:   8b 45 08                mov    0x8(%ebp),%eax
 4bb:   5d                      pop    %ebp
 4bc:   c3                      ret
```

(c) -fno-pic : foo function listing in librel.so (1)

```
000004bd <foo>:
 4bd:   55                      push   %ebp
 4be:   89 e5                   mov    %esp,%ebp
 4c0:   53                      push   %ebx
 4c1:   ff 75 08                pushl  0x8(%ebp)
 4c4:   e8 fc ff ff ff          call   4c5 <foo+0x8>
 4c9:   83 c4 04                add    $0x4,%esp
 4cc:   0f be d8                movsbl %al,%ebx
 4cf:   ff 75 08                pushl  0x8(%ebp)
 4d2:   e8 de ff ff ff          call   4b5 <fLocal>
 4d7:   83 c4 04                add    $0x4,%esp
 4da:   0f be c0                movsbl %al,%eax
 4dd:   01 d8                   add    %ebx,%eax
 4df:   ba 00 00 00 00          mov    $0x0,%edx
```

(d) -fno-pic : foo function listing in librel.so (2)

```
4e4:   01 c2                   add    %eax,%edx
4e6:   0f b6 05 00 00 00 00    movzbl 0x0,%eax
4ed:   0f be c0                movsbl %al,%eax
4f0:   01 d0                   add    %edx,%eax
4f2:   ba 21 20 00 00          mov    $0x2021,%edx
4f7:   01 c2                   add    %eax,%edx
4f9:   0f b6 05 21 20 00 00    movzbl 0x2021,%eax
500:   0f be c0                movsbl %al,%eax
503:   01 d0                   add    %edx,%eax
505:   8b 5d fc                mov    -0x4(%ebp),%ebx
508:   c9                      leave
509:   c3                      ret
```

TOC: C. librel.so function listings

(a) -fno-pic : main function listing in main.o (1)

```
00000000 <main>:
   0:   8d 4c 24 04             lea    0x4(%esp),%ecx
   4:   83 e4 f0                and    $0xfffffff0,%esp
   7:   ff 71 fc                pushl  -0x4(%ecx)
   a:   55                      push   %ebp
   b:   89 e5                   mov    %esp,%ebp
   d:   51                      push   %ecx
   e:   83 ec 04                sub    $0x4,%esp
  11:   83 ec 0c                sub    $0xc,%esp
  14:   6a 7b                   push   $0x7b
  16:   e8 fc ff ff ff          call   17 <main+0x17>
                        17: R_386_PC32  fPub
```

(b) -fno-pic : main function listing in main.o (2)

```
1b:   83 c4 10                add    $0x10,%esp
1e:   89 c2                   mov    %eax,%edx
20:   a1 00 00 00 00          mov    0x0,%eax
                      21: R_386_32    cPub
25:   01 d0                   add    %edx,%eax
27:   8b 4d fc                mov    -0x4(%ebp),%ecx
2a:   c9                      leave
2b:   8d 61 fc                lea    -0x4(%ecx),%esp
2e:   c3                      ret
```

TOC: D. `run_dynamic` function listings

(a) -fno-pic : main function listing in run_dynamic (1)

```
000005fd <main>:
 5fd:   8d 4c 24 04             lea    0x4(%esp),%ecx
 601:   83 e4 f0                and    $0xfffffff0,%esp
 604:   ff 71 fc                pushl  -0x4(%ecx)
 607:   55                      push   %ebp
 608:   89 e5                   mov    %esp,%ebp
 60a:   51                      push   %ecx
 60b:   83 ec 04                sub    $0x4,%esp
 60e:   83 ec 0c                sub    $0xc,%esp
 611:   6a 7b                   push   $0x7b
 613:   e8 fc ff ff ff          call   614 <main+0x17>
                        614: R_386_PC32 fPub
```

(b) -fno-pic : main function listing in run_dynamic (2)

```
618:   83 c4 10                add    $0x10,%esp
61b:   89 c2                   mov    %eax,%edx
61d:   a1 00 00 00 00          mov    0x0,%eax
                      61e: R_386_32   cPub
622:   01 d0                   add    %edx,%eax
624:   8b 4d fc                mov    -0x4(%ebp),%ecx
627:   c9                      leave
628:   8d 61 fc                lea    -0x4(%ecx),%esp
62b:   c3                      ret
62c:   66 90                   xchg   %ax,%ax
62e:   66 90                   xchg   %ax,%ax
```

TOC: A. `rel.o` function listings

- (a) `default : fPub` function listing in `rel.o`
- (b) `default : fLocal` function listing in `rel.o`
- (c) `default : foo` function listing in `rel.o` (1)
- (d) `default : foo` function listing in `rel.o` (2)

(a) default : fPub function listing in rel.o

```
00000000 <fPub>:
   0:   55                      push   %ebp
   1:   89 e5                   mov    %esp,%ebp
   3:   e8 fc ff ff ff          call   4 <fPub+0x4>
                        4: R_386_PC32   __x86.get_pc_thunk.ax
   8:   05 01 00 00 00          add    $0x1,%eax
                        9: R_386_GOTPC  _GLOBAL_OFFSET_TABLE_
   d:   8b 45 08                mov    0x8(%ebp),%eax
  10:   5d                      pop    %ebp
  11:   c3                      ret
```

(b) default : fLocal function listing in rel.o

```
00000012 <fLocal>:
  12:   55                      push   %ebp
  13:   89 e5                   mov    %esp,%ebp
  15:   e8 fc ff ff ff          call   16 <fLocal+0x4>
                        16: R_386_PC32  __x86.get_pc_thunk.ax
  1a:   05 01 00 00 00          add    $0x1,%eax
                        1b: R_386_GOTPC _GLOBAL_OFFSET_TABLE_
  1f:   8b 45 08                mov    0x8(%ebp),%eax
  22:   5d                      pop    %ebp
  23:   c3                      ret
```

(c) default : foo function listing in rel.o (1)

```
00000024 <foo>:
  24:   55                      push   %ebp
  25:   89 e5                   mov    %esp,%ebp
  27:   56                      push   %esi
  28:   53                      push   %ebx
  29:   e8 fc ff ff ff          call   2a <foo+0x6>
                        2a: R_386_PC32  __x86.get_pc_thunk.bx
  2e:   81 c3 02 00 00 00       add    $0x2,%ebx
                        30: R_386_GOTPC _GLOBAL_OFFSET_TABLE_
  34:   ff 75 08                pushl  0x8(%ebp)
  37:   e8 fc ff ff ff          call   38 <foo+0x14>
                        38: R_386_PC32  fPub
  3c:   83 c4 04                add    $0x4,%esp
  3f:   0f be f0                movsbl %al,%esi
  42:   ff 75 08                pushl  0x8(%ebp)
  45:   e8 c8 ff ff ff          call   12 <fLocal>
  4a:   83 c4 04                add    $0x4,%esp
  4d:   0f be c0                movsbl %al,%eax
  50:   8d 14 06                lea    (%esi,%eax,1),%edx
  53:   8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                        55: R_386_GOT32X        cPub
```

(d) default : foo function listing in rel.o (2)

```
59:   01 c2                    add    %eax,%edx
5b:   8b 83 00 00 00 00        mov    0x0(%ebx),%eax
                      5d: R_386_GOT32X        cPub
61:   0f b6 00                 movzbl (%eax),%eax
64:   0f be c0                 movsbl %al,%eax
67:   01 c2                    add    %eax,%edx
69:   8d 83 00 00 00 00        lea    0x0(%ebx),%eax
                      6b: R_386_GOTOFF        .bss
6f:   01 c2                    add    %eax,%edx
71:   0f b6 83 00 00 00 00     movzbl 0x0(%ebx),%eax
                      74: R_386_GOTOFF        .bss
78:   0f be c0                 movsbl %al,%eax
7b:   01 d0                    add    %edx,%eax
7d:   8d 65 f8                 lea    -0x8(%ebp),%esp
80:   5b                       pop    %ebx
81:   5e                       pop    %esi
82:   5d                       pop    %ebp
83:   c3                       ret
```

TOC: B. `librel.so` function listings

- (a) `default` : `fPub` function listing in `librel.so`
- (b) `default` : `fLocal` function listing in `librel.so`
- (c) `default` : `foo` function listing in `librel.so` (1)
- (d) `default` : `foo` function listing in `librel.so` (2)

(a) default : fPub function listing in librel.so

```
0000049d <fPub>:
 49d:   55                      push   %ebp
 49e:   89 e5                   mov    %esp,%ebp
 4a0:   e8 7c 00 00 00          call   521 <__x86.get_pc_thunk.ax>
 4a5:   05 5b 1b 00 00          add    $0x1b5b,%eax
 4aa:   8b 45 08                mov    0x8(%ebp),%eax
 4ad:   5d                      pop    %ebp
 4ae:   c3                      ret
```

(b) default : fLocal function listing in librel.so

```
000004af <fLocal>:
 4af:   55                      push   %ebp
 4b0:   89 e5                   mov    %esp,%ebp
 4b2:   e8 6a 00 00 00          call   521 <__x86.get_pc_thunk.ax>
 4b7:   05 49 1b 00 00          add    $0x1b49,%eax
 4bc:   8b 45 08                mov    0x8(%ebp),%eax
 4bf:   5d                      pop    %ebp
 4c0:   c3                      ret
```

(c) default : foo function listing in librel.so (1)

```
000004c1 <foo>:
 4c1:   55                      push   %ebp
 4c2:   89 e5                   mov    %esp,%ebp
 4c4:   56                      push   %esi
 4c5:   53                      push   %ebx
 4c6:   e8 d5 fe ff ff          call   3a0 <__x86.get_pc_thunk.bx>
 4cb:   81 c3 35 1b 00 00       add    $0x1b35,%ebx
 4d1:   ff 75 08                pushl  0x8(%ebp)
 4d4:   e8 fc ff ff ff          call   4d5 <foo+0x14>
 4d9:   83 c4 04                add    $0x4,%esp
 4dc:   0f be f0                movsbl %al,%esi
 4df:   ff 75 08                pushl  0x8(%ebp)
 4e2:   e8 c8 ff ff ff          call   4af <fLocal>
 4e7:   83 c4 04                add    $0x4,%esp
 4ea:   0f be c0                movsbl %al,%eax
 4ed:   8d 14 06                lea    (%esi,%eax,1),%edx
 4f0:   8b 83 f4 ff ff ff       mov    -0xc(%ebx),%eax
```

(d) default : foo function listing in librel.so (2)

```
4f6:   01 c2                   add    %eax,%edx
4f8:   8b 83 f4 ff ff ff       mov    -0xc(%ebx),%eax
4fe:   0f b6 00                movzbl (%eax),%eax
501:   0f be c0                movsbl %al,%eax
504:   01 c2                   add    %eax,%edx
506:   8d 83 21 00 00 00       lea    0x21(%ebx),%eax
50c:   01 c2                   add    %eax,%edx
50e:   0f b6 83 21 00 00 00    movzbl 0x21(%ebx),%eax
515:   0f be c0                movsbl %al,%eax
518:   01 d0                   add    %edx,%eax
51a:   8d 65 f8                lea    -0x8(%ebp),%esp
51d:   5b                      pop    %ebx
51e:   5e                      pop    %esi
51f:   5d                      pop    %ebp
520:   c3                      ret
```

TOC: C. `librel.so` function listings

(a) default : main function listing in main.o (1)

```
00000000 <main>:
   0:   8d 4c 24 04             lea    0x4(%esp),%ecx
   4:   83 e4 f0                and    $0xfffffff0,%esp
   7:   ff 71 fc                pushl  -0x4(%ecx)
   a:   55                      push   %ebp
   b:   89 e5                   mov    %esp,%ebp
   d:   53                      push   %ebx
   e:   51                      push   %ecx
   f:   e8 fc ff ff ff          call   10 <main+0x10>
                        10: R_386_PC32  __x86.get_pc_thunk.bx
  14:   81 c3 02 00 00 00       add    $0x2,%ebx
                        16: R_386_GOTPC _GLOBAL_OFFSET_TABLE_
  1a:   83 ec 0c                sub    $0xc,%esp
  1d:   6a 7b                   push   $0x7b
  1f:   e8 fc ff ff ff          call   20 <main+0x20>
                        20: R_386_PLT32 fPub
```

(b) default : main function listing in main.o (2)

```
24:   83 c4 10                add    $0x10,%esp
27:   89 c2                   mov    %eax,%edx
29:   8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                      2b: R_386_GOT32X        cPub
2f:   8b 00                   mov    (%eax),%eax
31:   01 d0                   add    %edx,%eax
33:   8d 65 f8                lea    -0x8(%ebp),%esp
36:   59                      pop    %ecx
37:   5b                      pop    %ebx
38:   5d                      pop    %ebp
39:   8d 61 fc                lea    -0x4(%ecx),%esp
3c:   c3                      ret
```

TOC: D. `run_dynamic` function listings

(a) default : main function listing in run_dynamic.o (1)

```
000005dd <main>:
 5dd:   8d 4c 24 04             lea    0x4(%esp),%ecx
 5e1:   83 e4 f0                and    $0xfffffff0,%esp
 5e4:   ff 71 fc                pushl  -0x4(%ecx)
 5e7:   55                      push   %ebp
 5e8:   89 e5                   mov    %esp,%ebp
 5ea:   53                      push   %ebx
 5eb:   51                      push   %ecx
 5ec:   e8 ef fe ff ff          call   4e0 <__x86.get_pc_thunk.bx>
                        5ed: R_386_PC32 __x86.get_pc_thunk.bx
 5f1:   81 c3 e3 19 00 00       add    $0x19e3,%ebx
                        5f3: R_386_GOTPC        _GLOBAL_OFFSET_TABLE_
 5f7:   83 ec 0c                sub    $0xc,%esp
 5fa:   6a 7b                   push   $0x7b
 5fc:   e8 7f fe ff ff          call   480 <fPub@plt>
                        5fd: R_386_PLT32        fPub
```

(b) default : main function listing in run_dynamic.o (2)

```
601:   83 c4 10                add    $0x10,%esp
604:   89 c2                   mov    %eax,%edx
606:   8b 83 24 00 00 00       mov    0x24(%ebx),%eax
                       608: R_386_GOT32X       cPub
60c:   8b 00                   mov    (%eax),%eax
60e:   01 d0                   add    %edx,%eax
610:   8d 65 f8                lea    -0x8(%ebp),%esp
613:   59                      pop    %ecx
614:   5b                      pop    %ebx
615:   5d                      pop    %ebp
616:   8d 61 fc                lea    -0x4(%ecx),%esp
619:   c3                      ret
61a:   66 90                   xchg   %ax,%ax
61c:   66 90                   xchg   %ax,%ax
61e:   66 90                   xchg   %ax,%ax
```

TOC: A. `rel.o` function listings

- (a) `-fPIC` : `fPub` function listing in `rel.o`
- (b) `-fPIC` : `fLocal` function listing in `rel.o`
- (c) `-fPIC` : `foo` function listing in `rel.o` (1)
- (d) `-fPIC` : `foo` function listing in `rel.o` (2)

(a) -fPIC : fPub function listing in rel.o

```
00000000 <fPub>:
   0:   55                      push   %ebp
   1:   89 e5                   mov    %esp,%ebp
   3:   e8 fc ff ff ff          call   4 <fPub+0x4>
                        4: R_386_PC32   __x86.get_pc_thunk.ax
   8:   05 01 00 00 00          add    $0x1,%eax
                        9: R_386_GOTPC  _GLOBAL_OFFSET_TABLE_
   d:   8b 45 08                mov    0x8(%ebp),%eax
  10:   5d                      pop    %ebp
  11:   c3                      ret
```

(b) -fPIC : fLocal function listing in rel.o

```
00000012 <fLocal>:
  12:   55                      push   %ebp
  13:   89 e5                   mov    %esp,%ebp
  15:   e8 fc ff ff ff          call   16 <fLocal+0x4>
                        16: R_386_PC32  __x86.get_pc_thunk.ax
  1a:   05 01 00 00 00          add    $0x1,%eax
                        1b: R_386_GOTPC _GLOBAL_OFFSET_TABLE_
  1f:   8b 45 08                mov    0x8(%ebp),%eax
  22:   5d                      pop    %ebp
  23:   c3                      ret
```

(c) -fPIC : foo function listing in rel.o (1)

```
00000024 <foo>:
  24:   55                      push   %ebp
  25:   89 e5                   mov    %esp,%ebp
  27:   56                      push   %esi
  28:   53                      push   %ebx
  29:   e8 fc ff ff ff          call   2a <foo+0x6>
                        2a: R_386_PC32  __x86.get_pc_thunk.bx
  2e:   81 c3 02 00 00 00       add    $0x2,%ebx
                        30: R_386_GOTPC _GLOBAL_OFFSET_TABLE_
  34:   83 ec 0c                sub    $0xc,%esp
  37:   ff 75 08                pushl  0x8(%ebp)
  3a:   e8 fc ff ff ff          call   3b <foo+0x17>
                        3b: R_386_PLT32 fPub
  3f:   83 c4 10                add    $0x10,%esp
  42:   0f be f0                movsbl %al,%esi
  45:   83 ec 0c                sub    $0xc,%esp
  48:   ff 75 08                pushl  0x8(%ebp)
  4b:   e8 c2 ff ff ff          call   12 <fLocal>
  50:   83 c4 10                add    $0x10,%esp
  53:   0f be c0                movsbl %al,%eax
  56:   8d 14 06                lea    (%esi,%eax,1),%edx
  59:   8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                        5b: R_386_GOT32X        cPub
```

(d) -fPIC : foo function listing in rel.o (2)

```
5f:   01 c2                   add    %eax,%edx
61:   8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                    63: R_386_GOT32X        cPub
67:   0f b6 00                movzbl (%eax),%eax
6a:   0f be c0                movsbl %al,%eax
6d:   01 c2                   add    %eax,%edx
6f:   8d 83 00 00 00 00       lea    0x0(%ebx),%eax
                    71: R_386_GOTOFF        .bss
75:   01 c2                   add    %eax,%edx
77:   0f b6 83 00 00 00 00    movzbl 0x0(%ebx),%eax
                    7a: R_386_GOTOFF        .bss
7e:   0f be c0                movsbl %al,%eax
81:   01 d0                   add    %edx,%eax
83:   8d 65 f8                lea    -0x8(%ebp),%esp
86:   5b                      pop    %ebx
87:   5e                      pop    %esi
88:   5d                      pop    %ebp
89:   c3                      ret
```

TOC: B. librel.so function listings

- (a) -fPIC : fPub function listing in librel.so
- (b) -fPIC : fLocal function listing in librel.so
- (c) -fPIC : foo function listing in librel.so (1)
- (d) -fPIC : foo function listing in librel.so (2)

(a) -fPIC : fPub function listing in librel.so

```
000004ad <fPub>:
 4ad:   55                      push   %ebp
 4ae:   89 e5                   mov    %esp,%ebp
 4b0:   e8 82 00 00 00          call   537 <__x86.get_pc_thunk.ax>
 4b5:   05 4b 1b 00 00          add    $0x1b4b,%eax
 4ba:   8b 45 08                mov    0x8(%ebp),%eax
 4bd:   5d                      pop    %ebp
 4be:   c3                      ret
```

(b) -fPIC : fLocal function listing in librel.so

```
000004bf <fLocal>:
 4bf:   55                      push   %ebp
 4c0:   89 e5                   mov    %esp,%ebp
 4c2:   e8 70 00 00 00          call   537 <__x86.get_pc_thunk.ax>
 4c7:   05 39 1b 00 00          add    $0x1b39,%eax
 4cc:   8b 45 08                mov    0x8(%ebp),%eax
 4cf:   5d                      pop    %ebp
 4d0:   c3                      ret
```

(c) -fPIC : foo function listing in librel.so (1)

```
000004d1 <foo>:
 4d1:   55                      push   %ebp
 4d2:   89 e5                   mov    %esp,%ebp
 4d4:   56                      push   %esi
 4d5:   53                      push   %ebx
 4d6:   e8 d5 fe ff ff          call   3b0 <__x86.get_pc_thunk.bx>
 4db:   81 c3 25 1b 00 00       add    $0x1b25,%ebx
 4e1:   83 ec 0c                sub    $0xc,%esp
 4e4:   ff 75 08                pushl  0x8(%ebp)
 4e7:   e8 a4 fe ff ff          call   390 <fPub@plt>
 4ec:   83 c4 10                add    $0x10,%esp
 4ef:   0f be f0                movsbl %al,%esi
 4f2:   83 ec 0c                sub    $0xc,%esp
 4f5:   ff 75 08                pushl  0x8(%ebp)
 4f8:   e8 c2 ff ff ff          call   4bf <fLocal>
 4fd:   83 c4 10                add    $0x10,%esp
 500:   0f be c0                movsbl %al,%eax
 503:   8d 14 06                lea    (%esi,%eax,1),%edx
 506:   8b 83 f4 ff ff ff       mov    -0xc(%ebx),%eax
```

(d) -fPIC : foo function listing in librel.so (2)

```
50c:   01 c2                   add    %eax,%edx
50e:   8b 83 f4 ff ff ff       mov    -0xc(%ebx),%eax
514:   0f b6 00                movzbl (%eax),%eax
517:   0f be c0                movsbl %al,%eax
51a:   01 c2                   add    %eax,%edx
51c:   8d 83 25 00 00 00       lea    0x25(%ebx),%eax
522:   01 c2                   add    %eax,%edx
524:   0f b6 83 25 00 00 00    movzbl 0x25(%ebx),%eax
52b:   0f be c0                movsbl %al,%eax
52e:   01 d0                   add    %edx,%eax
530:   8d 65 f8                lea    -0x8(%ebp),%esp
533:   5b                      pop    %ebx
534:   5e                      pop    %esi
535:   5d                      pop    %ebp
536:   c3                      ret
```

TOC: C. `librel.so` function listings

(a) -fPIC : main function listing in main.o (1)

```
00000000 <main>:
   0:   8d 4c 24 04             lea    0x4(%esp),%ecx
   4:   83 e4 f0                and    $0xfffffff0,%esp
   7:   ff 71 fc                pushl  -0x4(%ecx)
   a:   55                      push   %ebp
   b:   89 e5                   mov    %esp,%ebp
   d:   53                      push   %ebx
   e:   51                      push   %ecx
   f:   e8 fc ff ff ff          call   10 <main+0x10>
                        10: R_386_PC32  __x86.get_pc_thunk.bx
  14:   81 c3 02 00 00 00       add    $0x2,%ebx
                        16: R_386_GOTPC _GLOBAL_OFFSET_TABLE_
  1a:   83 ec 0c                sub    $0xc,%esp
  1d:   6a 7b                   push   $0x7b
  1f:   e8 fc ff ff ff          call   20 <main+0x20>
                        20: R_386_PLT32 fPub
```

(b) -fPIC : main function listing in main.o (2)

```
24:    83 c4 10                add    $0x10,%esp
27:    89 c2                   mov    %eax,%edx
29:    8b 83 00 00 00 00       mov    0x0(%ebx),%eax
                       2b: R_386_GOT32X        cPub
2f:    8b 00                   mov    (%eax),%eax
31:    01 d0                   add    %edx,%eax
33:    8d 65 f8                lea    -0x8(%ebp),%esp
36:    59                      pop    %ecx
37:    5b                      pop    %ebx
38:    5d                      pop    %ebp
39:    8d 61 fc                lea    -0x4(%ecx),%esp
3c:    c3                      ret
```

TOC: D. `run_dynamic` function listings

(a) -fPIC : main function listing in run_dynamic.o (1)

```
000005dd <main>:
 5dd:   8d 4c 24 04             lea    0x4(%esp),%ecx
 5e1:   83 e4 f0                and    $0xfffffff0,%esp
 5e4:   ff 71 fc                pushl  -0x4(%ecx)
 5e7:   55                      push   %ebp
 5e8:   89 e5                   mov    %esp,%ebp
 5ea:   53                      push   %ebx
 5eb:   51                      push   %ecx
 5ec:   e8 ef fe ff ff          call   4e0 <__x86.get_pc_thunk.bx>
                        5ed: R_386_PC32 __x86.get_pc_thunk.bx
 5f1:   81 c3 e3 19 00 00       add    $0x19e3,%ebx
                        5f3: R_386_GOTPC        _GLOBAL_OFFSET_TABLE_
 5f7:   83 ec 0c                sub    $0xc,%esp
 5fa:   6a 7b                   push   $0x7b
 5fc:   e8 7f fe ff ff          call   480 <fPub@plt>
                        5fd: R_386_PLT32        fPub
```

(b) -fPIC : main function listing in run_dynamic.o (2)

```
601:   83 c4 10                add    $0x10,%esp
604:   89 c2                   mov    %eax,%edx
606:   8b 83 24 00 00 00       mov    0x24(%ebx),%eax
                       608: R_386_GOT32X       cPub
60c:   8b 00                   mov    (%eax),%eax
60e:   01 d0                   add    %edx,%eax
610:   8d 65 f8                lea    -0x8(%ebp),%esp
613:   59                      pop    %ecx
614:   5b                      pop    %ebx
615:   5d                      pop    %ebp
616:   8d 61 fc                lea    -0x4(%ecx),%esp
619:   c3                      ret
61a:   66 90                   xchg   %ax,%ax
61c:   66 90                   xchg   %ax,%ax
61e:   66 90                   xchg   %ax,%ax
```