# Compiler Optimization Notes

## Mac Radigan

## Compiler Optimization

## Variable Declaration

declared in base scope

```
// variable_stack_1.cc
2
      #include <stdio.h>
3
      int main(void) {
        int value;
        for(int k=0; k<10; ++k)</pre>
          value = k;
9
          fprintf(stdout, "value: %d\n", value);
10
11
        return 0;
12
13
    // *EOF*
```

```
./bin/variable_stack_1:
                              file format elf64-x86-64
2
    Disassembly of section .init:
    00000000004003b8 <_init>:
                                           $0x8,%rsp
     4003b8: 48 83 ec 08
                                    sub
      4003bc: 48 8b 05 1d 05 20 00 mov
                                             0x20051d(%rip),%rax
                                                                       # 6008e0 <_DYNAMIC+0x1d0>
9
      4003c3: 48 85 c0
                                      test %rax,%rax
     4003c6: 74 05
4003c8: e8 43 00 00 00
                                             4003cd <_init+0x15>
                                      jе
11
12
                                      callq 400410 <fprintf@plt+0x10>
      4003cd: 48 83 c4 08
                                      add
                                             $0x8,%rsp
13
      4003d1: c3
                                      retq
14
```

```
15
    Disassembly of section .plt:
16
17
    0000000004003e0 <__libc_start_main@plt-0x10>:
18
      4003e0: ff 35 0a 05 20 00
                                                                     # 6008f0 <_GLOBAL_OFFSET_TABLE_+0x8>
                                        pushq 0x20050a(%rip)
19
      4003e6:
                ff 25 0c 05 20 00
                                        jmpq
                                               *0x20050c(%rip)
                                                                      # 6008f8 <_GLOBAL_OFFSET_TABLE_+0x10>
20
      4003ec: Of 1f 40 00
21
                                        nopl
                                               0x0(\%rax)
22
    0000000004003f0 <__libc_start_main@plt>:
      4003f0: ff 25 0a 05 20 00
                                               *0x20050a(%rip)
24
                                        jmpq
                                                                      # 600900 <_GLOBAL_OFFSET_TABLE_+0x18>
      4003f6:
                68 00 00 00 00
25
                                        pushq $0x0
      4003fb: e9 e0 ff ff ff
                                        jmpq
                                               4003e0 <_init+0x28>
26
27
    0000000000400400 <fprintf@plt>:
                                               *0x200502(%rip)
      400400: ff 25 02 05 20 00
                                                                      # 600908 <_GLOBAL_OFFSET_TABLE_+0x20>
                                        jmpq
29
      400406:
                68 01 00 00 00
                                        pushq
                                               $0x1
30
31
      40040b:
               e9 d0 ff ff ff
                                        jmpq
                                               4003e0 <_init+0x28>
32
    Disassembly of section .plt.got:
34
    0000000000400410 <.plt.got>:
35
     400410: ff 25 ca 04 20 00
                                               *0x2004ca(%rip)
                                                                      # 6008e0 <_DYNAMIC+0x1d0>
36
                                        jmpq
      400416:
                66 90
                                        xchg
                                               %ax,%ax
37
38
    Disassembly of section .text:
39
40
    0000000000400420 <_start>:
41
                                               %ebp,%ebp
42
      400420: 31 ed
                                        xor
      400422:
                49 89 d1
                                        mov
                                               %rdx,%r9
43
      400425:
                5e
                                               %rsi
                                        pop
44
      400426:
                48 89 e2
                                               %rsp,%rdx
                                        mov
      400429: 48 83 e4 f0
                                               $0xfffffffffffffff,%rsp
46
                                        and
      40042d: 50
                                        push
47
      40042e:
                54
                                        push
                                               %rsp
48
      40042f:
                49 c7 c0 b0 05 40 00
                                               $0x4005b0,%r8
                                        mov
49
      400436:
                48 c7 c1 40 05 40 00
                                        mov
                                               $0x400540,%rcx
50
      40043d:
                48 c7 c7 f7 04 40 00
                                               $0x4004f7,%rdi
51
                                        mov
      400444:
                e8 a7 ff ff ff
                                        callq 4003f0 <__libc_start_main@plt>
      400449:
               f4
53
                                        hlt
      40044a:
               66 Of 1f 44 00 00
                                               0x0(%rax,%rax,1)
54
    000000000400450 <deregister_tm_clones>:
56
                                        push
      400450: 55
                                               %rbp
                                                $0x600920, %eax
      400451:
                b8 20 09 60 00
                                        mov
58
      400456:
                48 3d 20 09 60 00
                                                $0x600920, %rax
59
                                        cmp
      40045c: 48 89 e5
60
                                        mov
                                               %rsp,%rbp
      40045f:
                74 17
                                        jе
                                               400478 <deregister_tm_clones+0x28>
61
      400461:
               ъ8 00 00 00 00
                                        mov
                                               $0x0, %eax
62
      400466:
                48 85 c0
                                        test
                                               %rax.%rax
63
      400469:
                74 0d
                                                400478 <deregister_tm_clones+0x28>
                                        jе
64
      40046b:
               5d
65
                                        pop
                                               %rbp
      40046c:
                bf 20 09 60 00
                                               $0x600920, %edi
                                        mov
66
67
      400471:
               ff e0
                                        jmpq
                                               *%rax
      400473:
                Of 1f 44 00 00
                                               0x0(\%rax,\%rax,1)
                                        nopl
68
69
      400478:
                5d
                                        pop
      400479:
                c3
70
                                        reta
      40047a: 66 0f 1f 44 00 00
                                        nopw
                                               0x0(%rax,%rax,1)
```

2

```
72
     0000000000400480 <register_tm_clones>:
73
       400480: be 20 09 60 00
                                                $0x600920, %esi
74
                                        mov
       400485: 55
                                         push
                                                %rbp
75
                                                $0x600920,%rsi
       400486:
               48 81 ee 20 09 60 00
76
                                         sub
       40048d:
                48 89 e5
                                         mov
                                                %rsp,%rbp
77
       400490: 48 c1 fe 03
                                         sar
                                                $0x3, %rsi
       400494: 48 89 f0
                                                %rsi,%rax
79
                                         mov
       400497: 48 c1 e8 3f
                                                $0x3f, %rax
80
               48 01 c6
       40049b:
81
                                         add
                                                %rax,%rsi
       40049e:
                 48 d1 fe
82
                                         sar
                                                %rsi
       4004a1:
                74 15
                                         jе
                                                4004b8 <register_tm_clones+0x38>
83
       4004a3: b8 00 00 00 00
                                                $0x0, %eax
                                         mov
84
       4004a8: 48 85 c0
                                         test
                                                %rax,%rax
       4004ab:
                74 0b
                                         jе
                                                4004b8 <register_tm_clones+0x38>
86
       4004ad:
                 5d
                                         pop
                                                %rbp
87
88
       4004ae:
                bf 20 09 60 00
                                         mov
                                                $0x600920, %edi
       4004b3: ff e0
                                                *%rax
89
                                         jmpq
       4004b5:
               Of 1f 00
                                         nopl
                                                (%rax)
       4004b8:
                5d
                                                %rbp
91
                                         pop
       4004b9:
92
                                         retq
       4004ba: 66 0f 1f 44 00 00
                                                0x0(\%rax,\%rax,1)
93
                                         nopw
94
     0000000004004c0 <__do_global_dtors_aux>:
95
       4004c0: 80 3d 61 04 20 00 00
                                                $0x0,0x200461(%rip)
                                                                           # 600928 <completed.6981>
                                         cmpb
96
       4004c7:
                 75 17
                                                4004e0 <__do_global_dtors_aux+0x20>
97
                                         jne
       4004c9: 55
                                                %rbp
98
                                         push
       4004ca: 48 89 e5
                                                %rsp,%rbp
99
                                         mov
                                         callq 400450 <deregister_tm_clones>
       4004cd: e8 7e ff ff ff
       4004d2:
                c6 05 4f 04 20 00 01
                                         movb
                                                $0x1,0x20044f(%rip)
                                                                         # 600928 <completed.6981>
101
       4004d9: 5d
102
                                         pop
       4004da: c3
103
                                         retq
       4004db: Of 1f 44 00 00
                                                0x0(%rax,%rax,1)
                                         nopl
104
105
       4004e0: f3 c3
                                         repz retq
                 Of 1f 40 00
       4004e2:
                                         nopl
                                                0x0(%rax)
106
       4004e6: 66 2e 0f 1f 84 00 00
                                         nopw
                                                %cs:0x0(%rax,%rax,1)
107
       4004ed: 00 00 00
108
109
     0000000004004f0 <frame_dummy>:
110
       4004f0:
                                         push
                                                %rbp
111
       4004f1:
                                                %rsp,%rbp
112
                 48 89 e5
                                         mov
       4004f4:
                 5d
                                                %rbp
113
                                         pop
       4004f5:
                 eb 89
                                                400480 <register_tm_clones>
                                         jmp
115
     00000000004004f7 <main>:
116
117
       4004f7: 55
                                         push
                                                %rbp
                 48 89 e5
       4004f8:
                                                %rsp,%rbp
                                         mov
118
       4004fb:
                 48 83 ec 10
                                         sub
                                                $0x10, %rsp
       4004ff: c7 45 fc 00 00 00 00 400506: 83 7d fc 09
                                         movl
                                                $0x0,-0x4(%rbp)
120
                                                $0x9,-0x4(%rbp)
                                         cmpl
121
       40050a: 7f 28
                                                400534 <main+0x3d>
122
                                         jg
       40050c: 8b 45 fc
                                                -0x4(%rbp),%eax
                                         mov
123
124
       40050f: 89 45 f8
                                         mov
                                                %eax,-0x8(%rbp)
                                                0x200407(%rip),%rax
       400512:
                 48 8b 05 07 04 20 00
                                                                           # 600920 <__TMC_END__>
                                         mov
125
126
       400519:
                 8b 55 f8
                                                -0x8(%rbp), %edx
                                                $0x4005c4, %esi
       40051c:
                 be c4 05 40 00
127
                                         mov
       400521: 48 89 c7
                                         mov
                                                %rax,%rdi
128
```

3

```
400524:
                  ъ8 00 00 00 00
                                                   $0x0, %eax
                                            mov
129
                                                   400400 <fprintf@plt>
       400529:
                  e8 d2 fe ff ff
130
                                            callq
       40052e:
                  83 45 fc 01
                                            addl
                                                   $0x1,-0x4(%rbp)
131
       400532:
                  eb d2
                                            jmp
                                                   400506 <main+0xf>
132
       400534:
                  ъ8 00 00 00 00
                                                   $0x0, %eax
133
                                            mov
       400539:
                                            leaveq
134
       40053a:
135
                  c3
                                            retq
       40053b:
                  Of 1f 44 00 00
                                            nopl
                                                   0x0(\%rax,\%rax,1)
136
     0000000000400540 <__libc_csu_init>:
138
       400540:
                  41 57
                                            push
                                                   %r15
139
       400542:
                  41 56
                                                   %r14
140
                                            push
       400544:
                  41 89 ff
                                            mov
                                                   %edi,%r15d
141
       400547:
                  41 55
                                            push
                                                   %r13
142
       400549:
                  41 54
                                            push
                                                   %r12
143
       40054b:
                  4c 8d 25 ae 01 20 00
                                                   0x2001ae(%rip),%r12
                                                                                # 600700 <__frame_dummy_init_array_entry>
                                            lea
144
       400552:
                  55
                                            push
145
                                                   %rbp
       400553:
                  48 8d 2d ae 01 20 00
                                            lea
                                                   0x2001ae(%rip),%rbp
                                                                                # 600708 <__init_array_end>
146
       40055a:
                                                   %rbx
147
                  53
                                            push
       40055b:
                  49 89 f6
                                                   %rsi,%r14
                                            mov
148
       40055e:
                  49 89 d5
                                                   %rdx,%r13
149
                                            {\tt mov}
       400561:
                  4c 29 e5
                                                   %r12,%rbp
                                            sub
150
       400564:
                  48 83 ec 08
                                                   $0x8,%rsp
151
                                            sub
                  48 c1 fd 03
       400568:
                                                   $0x3,%rbp
152
                                            sar
                  e8 47 fe ff ff
       40056c:
                                            callq 4003b8 <_init>
153
       400571:
                  48 85 ed
                                            test
                                                   %rbp,%rbp
       400574:
                  74 20
                                                   400596 <__libc_csu_init+0x56>
                                            jе
155
       400576:
                  31 db
                                                   %ebx,%ebx
156
                                            xor
157
       400578:
                  Of 1f 84 00 00 00 00
                                            nopl
                                                   0x0(%rax,%rax,1)
       40057f:
158
                  4c 89 ea
       400580:
                                            mov
                                                   %r13,%rdx
                  4c 89 f6
       400583:
                                                   %r14,%rsi
                                            mov
160
161
       400586:
                  44 89 ff
                                                   %r15d,%edi
                  41 ff 14 dc
       400589:
                                                   *(%r12,%rbx,8)
162
                                            callq
       40058d:
                  48 83 c3 01
                                            add
                                                   $0x1,%rbx
163
       400591:
                  48 39 eb
164
                                            \mathtt{cmp}
                                                   %rbp,%rbx
       400594:
                  75 ea
                                                   400580 <__libc_csu_init+0x40>
                                            ine
165
       400596:
                  48 83 c4 08
                                            add
                                                   $0x8,%rsp
166
       40059a:
                  5b
                                                   %rbx
167
                                            pop
168
       40059b:
                  5d
                                            pop
                                                   %rbp
                  41 5c
       40059c:
                                                   %r12
169
                                            pop
       40059e:
                  41 5d
                                                   %r13
170
                                            pop
171
       4005a0:
                  41 5e
                                            pop
                                                   %r14
       4005a2:
                  41 5f
172
                                            pop
                                                   %r15
                                            retq
       4005a4:
                  сЗ
       4005a5:
                  90
174
                                            nop
       4005a6:
                  66 2e Of 1f 84 00 00
                                            nopw
                                                   %cs:0x0(%rax,%rax,1)
175
                  00 00 00
176
       4005ad:
177
178
     0000000004005b0 <__libc_csu_fini>:
       4005b0:
                 f3 c3
                                            repz retq
179
180
     Disassembly of section .fini:
181
182
     00000000004005b4 <_fini>:
183
                                                   $0x8,%rsp
       4005b4:
                  48 83 ec 08
                                            sub
184
       4005b8:
                  48 83 c4 08
                                                   $0x8,%rsp
```

```
4005bc: c3 retq
```

#### declared within statement block

```
// variable_stack_1.cc
      #include <stdio.h>
3
      int main(void) {
5
        for(int k=0; k<10; ++k)</pre>
6
           int value = k;
           fprintf(stdout, "value: %d\n", value);
9
10
        return 0;
11
12
    // *EOF*
14
                              file format elf64-x86-64
    ./bin/variable_stack_2:
2
```

```
Disassembly of section .init:
    00000000004003b8 <_init>:
7
      4003b8: 48 83 ec 08
                                      sub
                                             $0x8,%rsp
      4003bc: 48 8b 05 1d 05 20 00
                                             0x20051d(%rip),%rax
                                                                       # 6008e0 <_DYNAMIC+0x1d0>
                                      mov
9
      4003c3: 48 85 c0
                                      test
                                             %rax,%rax
10
      4003c6: 74 05
                                             4003cd <_init+0x15>
11
                                       jе
      4003c8:
               e8 43 00 00 00
                                      callq 400410 <fprintf@plt+0x10>
12
      4003cd: 48 83 c4 08
13
                                      add
                                             $0x8,%rsp
      4003d1: c3
                                      retq
14
    Disassembly of section .plt:
16
17
    0000000004003e0 <__libc_start_main@plt-0x10>:
18
                                      pushq 0x20050a(%rip)
      4003e0: ff 35 0a 05 20 00
                                                                  # 6008f0 <_GLOBAL_OFFSET_TABLE_+0x8>
19
20
      4003e6: ff 25 0c 05 20 00
                                      jmpq *0x20050c(%rip)
                                                                   # 6008f8 <_GLOBAL_OFFSET_TABLE_+0x10>
      4003ec: Of 1f 40 00
                                            0x0(%rax)
                                      nopl
21
    00000000004003f0 <__libc_start_main@plt>:
23
      4003f0: ff 25 0a 05 20 00
                                             *0x20050a(%rip)
                                                                   # 600900 <_GLOBAL_OFFSET_TABLE_+0x18>
                                      jmpq
24
      4003f6:
              68 00 00 00 00
25
                                      pushq $0x0
      4003fb:
             e9 e0 ff ff ff
                                             4003e0 <_init+0x28>
                                      jmpq
26
    0000000000400400 <fprintf@plt>:
28
      400400: ff 25 02 05 20 00
                                             *0x200502(%rip)
                                                                   # 600908 <_GLOBAL_OFFSET_TABLE_+0x20>
29
                                       jmpq
      400406: 68 01 00 00 00
                                      pushq $0x1
30
      40040b: e9 d0 ff ff ff
                                      jmpq 4003e0 <_init+0x28>
31
```

```
32
    Disassembly of section .plt.got:
33
34
    0000000000400410 <.plt.got>:
35
      400410: ff 25 ca 04 20 00
                                              *0x2004ca(%rip)
                                                                     # 6008e0 <_DYNAMIC+0x1d0>
36
                                        jmpq
      400416:
               66 90
                                        xchg
                                              %ax,%ax
37
38
    Disassembly of section .text:
39
40
    0000000000400420 <_start>:
41
               31 ed
                                               %ebp,%ebp
42
      400420:
                                        xor
      400422:
43
               49 89 d1
                                       mov
                                              %rdx,%r9
      400425: 5e
                                              %rsi
44
                                       pop
      400426: 48 89 e2
                                              %rsp,%rdx
      400429: 48 83 e4 f0
                                              $0xfffffffffffffff,%rsp
                                        and
46
      40042d:
               50
                                        push
                                               %rax
47
48
      40042e:
               54
                                        push
                                              %rsp
                                              $0x4005b0,%r8
      40042f:
               49 c7 c0 b0 05 40 00
                                       mov
49
      400436:
              48 c7 c1 40 05 40 00
                                       mov
                                               $0x400540,%rcx
      40043d:
               48 c7 c7 f7 04 40 00
                                              $0x4004f7,%rdi
                                       mov
51
      400444:
               e8 a7 ff ff ff
52
                                        callq 4003f0 <__libc_start_main@plt>
      400449: f4
53
                                       hlt
      40044a: 66 Of 1f 44 00 00
                                             0x0(%rax, %rax, 1)
                                       nopw
54
55
    000000000400450 <deregister_tm_clones>:
56
      400450:
57
                                              %rbp
      400451:
               ъ8 20 09 60 00
                                              $0x600920, %eax
58
                                       mov
      400456: 48 3d 20 09 60 00
                                              $0x600920, %rax
59
                                       cmp
      40045c: 48 89 e5
                                       mov
                                              %rsp,%rbp
      40045f:
               74 17
                                              400478 <deregister_tm_clones+0x28>
                                       jе
61
      400461:
               ъ8 00 00 00 00
                                       mov
                                               $0x0, %eax
      400466: 48 85 c0
63
                                       test
                                              %rax.%rax
      400469: 74 0d
                                               400478 <deregister_tm_clones+0x28>
                                       jе
64
65
      40046b: 5d
                                       pop
                                              %rbp
      40046c:
               bf 20 09 60 00
                                               $0x600920, %edi
                                       mov
66
      400471: ff e0
                                        jmpq
                                              *%rax
67
      400473: Of 1f 44 00 00
                                              0x0(%rax,%rax,1)
68
                                       nopl
      400478:
              5d
                                        pop
                                              %rbp
69
      400479:
70
               c3
                                        retq
      40047a:
               66 Of 1f 44 00 00
                                              0x0(%rax,%rax,1)
71
    000000000400480 <register_tm_clones>:
73
      400480: be 20 09 60 00
                                              $0x600920, %esi
      400485:
               55
                                        push
                                              %rbp
75
      400486:
               48 81 ee 20 09 60 00
                                               $0x600920,%rsi
76
                                        sub
      40048d: 48 89 e5
77
                                       mov
                                              %rsp,%rbp
      400490:
               48 c1 fe 03
                                              $0x3,%rsi
                                       sar
78
      400494:
               48 89 f0
                                       mov
                                              %rsi,%rax
      400497:
               48 c1 e8 3f
                                       shr
                                              $0x3f, %rax
80
      40049b:
               48 01 c6
                                       add
                                              %rax,%rsi
81
               48 d1 fe
82
      40049e:
                                       sar
                                              %rsi
      4004a1: 74 15
                                       jе
                                               4004b8 <register_tm_clones+0x38>
83
      4004a3: b8 00 00 00 00
                                       mov
                                              $0x0.%eax
      4004a8:
                48 85 c0
                                       test
                                              %rax.%rax
85
86
      4004ab:
                74 Ob
                                        jе
                                               4004b8 <register_tm_clones+0x38>
      4004ad:
                                               %rbp
               5d
87
                                        pop
      4004ae: bf 20 09 60 00
                                        mov
                                               $0x600920, %edi
```

6

```
4004b3:
                 ff e0
                                                 *%rax
89
                                          jmpq
       4004b5:
                 Of 1f 00
                                                 (%rax)
90
                                          nopl
       4004b8:
                 5d
                                                 %rbp
                                          pop
91
       4004b9:
                 сЗ
                                          retq
                 66 Of 1f 44 00 00
                                                 0x0(\%rax,\%rax,1)
       4004ba:
93
                                          nopw
     0000000004004c0 <__do_global_dtors_aux>:
95
                                                 $0x0,0x200461(%rip)
                                                                             # 600928 <completed.6981>
       4004c0:
                 80 3d 61 04 20 00 00
                                          cmpb
96
       4004c7:
                 75 17
                                                 4004e0 <__do_global_dtors_aux+0x20>
                                          jne
       4004c9:
                 55
                                          push
                                                 %rbp
98
       4004ca:
                 48 89 e5
                                                 %rsp,%rbp
       4004cd:
                 e8 7e ff ff ff
                                                 400450 <deregister_tm_clones>
100
                                          callq
                 c6 05 4f 04 20 00 01
                                                 $0x1,0x20044f(%rip) # 600928 <completed.6981>
       4004d2:
                                          movb
101
       4004d9:
                5d
                                          pop
                                                 %rbp
102
       4004da:
                 c3
                                          retq
103
       4004db:
                Of 1f 44 00 00
                                                 0x0(%rax,%rax,1)
                                          nopl
104
       4004e0:
                 f3 c3
105
                                          repz retq
       4004e2:
                 Of 1f 40 00
                                          nopl
                                                 0x0(%rax)
106
                 66 2e Of 1f 84 00 00
                                                 %cs:0x0(%rax,%rax,1)
107
       4004e6:
                                          nopw
       4004ed:
                 00 00 00
108
109
     00000000004004f0 <frame_dummy>:
110
       4004f0:
                 55
111
                                          push
                                                 %rbp
                 48 89 e5
       4004f1:
                                                 %rsp,%rbp
112
                                          mov
       4004f4:
                 5d
                                          pop
                                                 %rbp
113
       4004f5:
                 eb 89
                                          jmp
                                                 400480 <register_tm_clones>
115
     00000000004004f7 <main>:
116
117
       4004f7: 55
                                          push
                                                 %rbp
                 48 89 e5
                                                 %rsp,%rbp
       4004f8:
                                          mov
118
       4004fb:
                 48 83 ec 10
                                          sub
                                                 $0x10,%rsp
119
                 c7 45 fc 00 00 00 00
       4004ff:
                                          movl
                                                 $0x0,-0x4(%rbp)
120
       400506: 83 7d fc 09
                                          cmpl
                                                 $0x9,-0x4(%rbp)
       40050a: 7f 28
                                                 400534 <main+0x3d>
122
                                          jg
       40050c: 8b 45 fc
                                          mov
                                                 -0x4(%rbp),%eax
123
       40050f: 89 45 f8
                                                 %eax,-0x8(%rbp)
124
                                          mov
       400512:
                 48 8b 05 07 04 20 00
                                                 0x200407(%rip),%rax
                                                                             # 600920 <__TMC_END__>
                                          mov
125
       400519:
                 8b 55 f8
                                          mov
                                                 -0x8(%rbp),%edx
       40051c:
                 be c4 05 40 00
                                                 $0x4005c4, %esi
127
                                          mov
       400521:
                 48 89 c7
                                                 %rax,%rdi
       400524:
                 ъ8 00 00 00 00
                                                 $0x0,%eax
129
                                          mov
       400529:
                 e8 d2 fe ff ff
                                          callq 400400 <fprintf@plt>
130
                 83 45 fc 01
                                                 $0x1,-0x4(%rbp)
       40052e:
                                          addl
131
       400532:
                 eb d2
                                                 400506 <main+0xf>
132
                                          jmp
       400534:
                 ъ8 00 00 00 00
                                          mov
                                                 $0x0, %eax
       400539:
                 с9
                                          leaveq
134
       40053a:
                 сЗ
                                          retq
135
                 Of 1f 44 00 00
136
       40053b:
                                          nopl
                                                 0x0(\%rax,\%rax,1)
137
138
     0000000000400540 <__libc_csu_init>:
                41 57
                                          push
       400540:
                                                 %r15
139
       400542:
                 41 56
                                          push
                                                 %r14
140
                                                 %edi,%r15d
                 41 89 ff
       400544:
141
                                          mov
       400547:
                 41 55
                                          push
                                                 %r13
142
                                          push
       400549:
                 41 54
                                                 %r12
       40054b:
                 4c 8d 25 ae 01 20 00
                                          lea
                                                 0x2001ae(%rip),%r12
                                                                             # 600700 <__frame_dummy_init_array_entry>
144
       400552:
                                          push
```

```
400553:
                 48 8d 2d ae 01 20 00
                                                  0x2001ae(%rip),%rbp
                                                                              # 600708 <__init_array_end>
                                          lea
146
       40055a:
                                          push
147
                 53
                                                 %rbx
       40055b:
                 49 89 f6
                                                  %rsi,%r14
                                          mov
148
       40055e:
                 49 89 d5
                                                  %rdx,%r13
149
                                          mov
                 4c 29 e5
       400561:
                                                  %r12,%rbp
150
                                          sub
       400564:
                 48 83 ec 08
                                                  $0x8,%rsp
                                          sub
151
                 48 c1 fd 03
       400568:
                                                  $0x3,%rbp
152
                                          sar
       40056c:
                 e8 47 fe ff ff
                                          callq 4003b8 <_init>
153
       400571:
                 48 85 ed
                                          test
                                                  %rbp,%rbp
154
       400574:
                 74 20
                                                  400596 <__libc_csu_init+0x56>
                                          jе
155
       400576:
                 31 db
                                                  %ebx,%ebx
                                          xor
156
       400578:
                 Of 1f 84 00 00 00 00
                                          nopl 0x0(%rax,%rax,1)
157
       40057f:
                 00
158
       400580:
                 4c 89 ea
                                          mov
                                                  %r13,%rdx
159
       400583:
                 4c 89 f6
                                                  %r14,%rsi
                                          mov
160
       400586:
                 44 89 ff
                                                  %r15d,%edi
                                          mov
161
       400589:
                 41 ff 14 dc
                                          callq *(%r12,%rbx,8)
162
       40058d:
                 48 83 c3 01
                                          add
                                                  $0x1,%rbx
163
                 48 39 eb
164
       400591:
                                          \mathtt{cmp}
                                                  %rbp,%rbx
       400594:
                 75 ea
                                                  400580 <__libc_csu_init+0x40>
                                          jne
165
       400596:
                 48 83 c4 08
                                          {\tt add}
                                                  $0x8,%rsp
166
       40059a:
                 5b
                                                  %rbx
167
                                          pop
       40059b:
                 5d
168
                                          pop
                                                  %rbp
                 41 5c
       40059c:
                                                  %r12
169
                                          pop
       40059e:
                41 5d
                                                  %r13
                                          pop
170
       4005a0:
                 41 5e
                                          pop
                                                  %r14
       4005a2:
                 41 5f
                                                  %r15
172
                                          pop
       4005a4:
                 сЗ
173
                                          retq
174
       4005a5:
                 90
                                          nop
                 66 2e Of 1f 84 00 00
       4005a6:
                                          nopw
                                                 %cs:0x0(%rax,%rax,1)
175
       4005ad:
                 00 00 00
177
178
     0000000004005b0 <__libc_csu_fini>:
       4005b0: f3 c3
179
                                          repz retq
180
181
     Disassembly of section .fini:
182
     00000000004005b4 <_fini>:
183
       4005b4: 48 83 ec 08
                                                  $0x8,%rsp
                                           sub
184
185
       4005b8:
                  48 83 c4 08
                                           add
                                                  $0x8,%rsp
       4005bc:
                 сЗ
186
                                          retq
```

## implementation difference (side-by-side diff, no suppression)

```
00000000004003e0 <_libc_start_main@plt-0x10>:
# 4003e0: ff 35 0a 05 20 00 pus
4003e6: ff 25 0c 05 20 00 jmp
4003ec: 0f if 40 00 nopl 0x0(
                00000000004003e0 < libc start main@plt-0x10>:
                    4003e0: ff 35 0a 05 20 00
4003e6: ff 25 0c 05 20 00
                                                                                           pushq 0x20050a(%rip)
jmpq *0x20050c(%rip)
                                                                                                                                                                                                                                        pushq 0x20050a(%rip)
jmpq *0x20050c(%rip)
  18
19
                                                                                                                                                                                                                               00 jmpq * nopl 0x0(%rax)
                    4003ec: Of 1f 40 00
                                                                                                          0x0(%rax)
 20
                                                                                                          00000000004003f0 <_libc_start_main
4003f0: ff 25 0a 05 20 00
4003f6: 68 00 00 00 00
4003fb: e9 e0 ff ff ff
                                                                                           jmpq
                                                                                             pushq $0x0 40
impq 4003e0 <_init+0x28>
  23
 24
 25
26
27
                                                                                                                               0000000000400400 <fprintf@plt>:
                0000000000400400 <fprintf@plt>:
                                                                                                          400400: ff 25 02 05 20 00
400406: 68 01 00 00 00
40040b: e9 d0 ff ff ff
                                                                                            jmpq
 31
                Disassembly of section .plt.got:
                                                                                                                                    Disassembly of section .plt.got:
  32
33
                0000000000400410 <.plt.got>
                                                                                                                                     0000000000400410 <.plt.got>:
                                                                                                          *0x2004ca(%rip) 400410: ff 25 ca 04 20 00
%ax,%ax 400416: 66 90 xc
 34
                                                                                                                                                                                                                                                  jmpq *0x2004ca(%rip)
                    400410: ff 25 ca 04 20 00
400416: 66 90
                                                                                            jmpq
                                                                                                                                                                                                                                  xchg %ax,%ax
 35
                                                                                                        %ax,%ax
                Disassembly of section .text:
                                                                                                                                    Disassembly of section .text:
 38
 39
                0000000000400420 <_start>:
                                                                                                                           00000000000400420 < start>:
  \frac{40}{41}
\frac{42}{42}
                                                                                                          %ebp,%ebp
%rdx,%r9
                                                                                                                                      400420: 31 ed
400422: 49 89 d1
                                                                                                                                                                                                                                 mov %rsi
                                                                                                                                                                                                                     pop %rsi
mov %rsp,%rdx
and $
                     400425:
                                                                                            pop
mov
                                                                                                           %rsi
                                                                                                                                                 400425: 5e
                                                                                                         43
                     400426:
                                        48 89 e2
                                                                                                                                                                                                                                                                 $0xffffffffffffff0.%rs
                                                                                                                                                  40042e: 54 push Xrsp

40042f: 49 c7 c0 b0 05 40 00 mov

400436: 48 c7 c1 40 05 40 00 mov

400436: 48 c7 c7 f7 04 40 00 mov
  46
                    40042e: 54
                                                                                            push
                    40042f ·
                                         49 c7 c0 b0 05 40 00
                                                                                                                                                                                                                                                         $0x4005b0 %r8
                                                                                                                                                                                                                                                        $0x400540,%rcx
$0x4004f7,%rdi
                     40043d:
                                                                                                           $0x4004f7,%rdi
                                                                                            mov
 50
                    400444:
                                       e8 a7 ff ff ff
                                                                                            callq 4003f0 <__libc_start_ma
                                                                                                                                                                       400444: e8 a7 ff ff ff
                                                                                                                                                                                                                                              callq 4003f0 <__libc_start_ma
                                                                                                          400449: f4 hl
0x0(%rax,%rax,1) 40044a: 66 0f 1f 44 00 00
                     40044a: 66 Of 1f 44 00 00
                                                                                                                                                                                                                                          nopw 0x0(%rax,%rax,1)
                                                                                            nopw
  53
                                                                                                                                     0000000000400450 <deregister_tm_clones>:
                000000000400450 <deregister_tm_clones>:
                                                                                                                                                  400450: 55 push
400451: b8 20 09 60 00
  55
56
                                                                                                       %rbp
$0x600920,%eax
                                                                                                         %0x600920, %eax

$0x600920, %rax 4004b6: ...

%rsp, %rbp 40045c: 48 89 e5

400478 < deregister_tm_c 40045f: 74 17

$0x0, %eax 400466: 48 85 c0

**vax, %rax 400466: 48 85 c0
  57
                     400456:
                                         48 3d 20 09 60 00
                                                                                                                                                                                       48 3d 20 09 60 00
                                                                                                                                                                                                                                          cmp
                                                                                                                                                                                                                                                         $0x600920, %rax
                                                                                                                                                                                                                                                p $0x00002
%rsp,%rbp
ie 400478 <deregister_tm_c
                     40045c:
                                         48 89 e5
                    40045f:
400461:
                                                                                                                                                                                                                                                 je 40
$0x0,%eax
                                                                                                                                                                                                                       test %rax,%rax
                                                                                                         61
                     400466:
                                         48 85 c0
                                                                                            test
  62
63
64
                     400469:
                                         74 Od
                    40046b:
40046c:
                                        5d
bf 20 09 60 00
                                                                                                         65
                     400471:
                                        ff e0
                                                                                            jmpq
                     400473:
                                         Of 1f 44 00 00
                                                                                            pop
  68
                     400479:
                                                                                            retq
  69
                    40047a: 66 Of 1f 44 00 00
                                                                                                                                             70
71
72
                                                                                                                                            0000000000400480 <register_tm_clones>:
                0000000000400480 <register_tm_clones>:
                                                                                                          $0x600920,%esi
                    400480:
                                       be 20 09 60 00
                                                                                                                                                                                                                                           mov $0x600920, %esi
                                       55
48 81 ee 20 09 60 00
48 89 e5
                                                                                                         %rbp
$0x600920,%rsi
                                                                                            push
                                                                                                                                                                                                                         push %rbp
60 00 sub $0x600920,%rsi
                                                                                                          %rsp,%rbp
$0x3,%rsi
                                       48 c1 fe 03
  76
                     400490:
                                                                                                                                                                                                                                                 $0x3,%rsi
                                       48 89 f0
                                                                                                                                                                                                                                                 %rsi,%rax
                    400494:
                                                                                                           %rsi.%rax
                     400497:
                                                                                                           $0x3f,%rax
                                                                                                                                                                                                                                                 $0x3f,%rax
                                                                                                           $0x3f,%rax
%rax,%rsi
                                                                                                         \text{Vrax}, \text{Vrsi} \quad \quad
                                                                                                                                                                                                                                                 %rax,%rsi
                                        48 d1 fe
                     40049e:
                                                                                            sar
                                                                                                                                                                                                                     je 40
mov $0x0,%eax
test %rax,%rax
                                                                                                                                                                                                                                                           4004b8 <register_tm_clo
                     4004a1 ·
                                         74 15
                    4004a1:
4004a3:
4004a8:
                                        ъ8 00 00 00 00
                                                                                                                                                       48 85 c0
                                                                                            test
                     4004ab:
                                         74 Ob
                                                                                                                                                  m_clo 40
4004ad: 5d
                     4004ad:
  87
                     4004ъ3:
                                                                                            jmpq
                                                                                                           *%rax
(%rax)
  88
                     4004b5:
                                        Of 1f 00
                                                                                                          \( \frac{\text{k1a}}{\text{k7}} \) \( \frac{\text{k04b}}{\text{k04b}} \) \( \frac{\text{k1}}{\text{k04b}} \) \( \frac{\text{k1}}{\text{k1}} \) \( \frac{\text{k04b}}{\text{k1}} \) \( \frac{\text{k04b}}{\text{k1}} \) \( \frac{\text{k1}}{\text{k1}} \) \( \frac{\text{k1}}{\text{k1}
                     4004ъ8:
                    4004ba: 66 0f 1f 44 00 00
                                                                                            nopw
  92
                                                                                           00000000004004c0 <__do_global_dtors_aux>:
                    4004c0: 80 3d 61 04 20 00 00
 95
                    4004c7:
                                         75 17
  96
                     4004c9:
                    4004ca:
4004cd:
                                         c6 05 4f 04 20 00 01
 99
                     4004d2:
                     4004d9:
                                         c3
Of 1f 44 00 00
                     4004db:
102
103
                     4004e0:
                                         f3 c3
                                         0f 1f 40 00
```

```
4004ed: 00 00 00
106
                      4004ed: 00 00 00
                                                                                                                                                                                      00000000004004f0 <frame_dummy>:
                                                                                                                                                                                                                                                                                                       push %rbp
mov %rsp,%rbp
                                                                                                                             push %rbp
                                                                                                                                                                               4004f0: 55

4004f1: 48 89 e5

4004f4: 5d

gister_tm_clo 4004f5: eb 89
109
                            4004f0: 55
4004f1: 48 89 e5
                                                                                                                                                 %rsp,%rbp 400
%rbp 4004f4:
400480 <register_tm_clo
110
                                                                                                                                                                                                                                                                                                      pop %rbp jmp 400480 <register_tm_clo
                                                                                                                                | Most | 
                      000000000004004f7 <main>:
114
116
                                                       48 83 ec 10
c7 45 fc 00 00 00 00
83 7d fc 09
7f 28
117
                             4004fb:
                                                                                                                             sub
                             4004ff:
                            400506:
40050a:
120
                                                        8b 45 fc
121
                            40050c:
\frac{122}{123}
                            40050f:
400512:
                                                        89 45 f8
48 8b 05 07 04 20 00
124
                             400519:
                                                        8b 55 f8
                                                        be c4 05 40 00
125
                             40051c:
                            400521:
400524:
                                                                                                                             callq 400400 <fprintf@plt>
128
                            400529:
                                                        e8 d2 fe ff ff
                                                        83 45 fc 01
129
                            40052e:
                                                                                                                             addl
                            400532:
400534:
132
                            400539:
                                                       с9
                                                                                                                            leaveq
                                                                                                                             retq
133
                            40053a:
                                                     Of 1f 44 00 00
                      0000000000400540 < libc csu init>:
136
                                                                                                                                                                                                      00000400540 <__libc_csu_init>:
400540: 41 57
400542: 41 56
400544: 41 89 ff
400547: 41 55
400549: 41 54
                                                                                                                            push
137
                                                        41 57
                                                                                                                                                %r15
%r14
%edi,%r15d
%r13
%r12
                                                                                                                                                 138
139
                                                                                                                             push
                             400544:
140
                             400547:
                                                       41 55
                             400549:
                                                          4c 8d 25 ae 01 20 00
                                                                                                                           lea 0x2001ae(%rip),%r12 40054b: 4c 8d 2b ae 01 20 UU lea 0x2001ae(%rip),%rbp 400552: 55 push %rbp
lea 0x2001ae(%rip),%rbp 400553: 48 8d 2d ae 01 20 UU lea 0x2001ae(%rip),%rbp
push %rbx 40055a: 53 push %rbx
mov %rsi,%r14 40055b: 49 89 f6 mov %rdx, %r13
sub vx12,%rbp 400561: 4c 29 e5 sub %r12,%rbp
sub $0x8,%rsp 400564: 48 8d e0 8 sub $0x8,%rsp
sar $0x3,%rbp 400564: 48 8d e0 8 sub $0x8,%rsp
callq 400586 <init> 400566: e8 47 feff ff
extra 400586 <init 4005
143
                             400552:
                                                        48 8d 2d ae 01 20 00
144
                            400553:
                            40055a:
40055b:
147
                             40055e:
                                                        49 89 d5
                                                       4c 29 e5
48 83 ec 08
48 c1 fd 03
148
                             400561:
                            400564:
400568:
                                                        e8 47 fe ff ff
151
                             40056c:
152
153
154
155
                            400571:
400574:
400576:
                                                       48 85 ed
74 20
                                                        31 db
                             400578:
                                                       Of 1f 84 00 00 00 00
                                                                                                                            nop1 0xU(\(\alpha\)x,\(\alpha\)x,\(\alpha\)x,\(\alpha\)x 100

mov \(\alpha\)13,\(\alpha\)x mov \(\alpha\)14,\(\alpha\)x 10

mov \(\alpha\)15d,\(\alpha\)di

callq \(\alpha\)(\alpha\)1,\(\alpha\)t bx

cmp \(\alpha\)p,\(\alpha\)t bx
                            40057f:
400580:
400583:
                                                       00
4c 89 ea
                                                                                                                                                                                                                  400580: 4c 89 ea
400583: 4c 89 f6
400586: 44 89 ff
158
                                                        4c 89 f6
                                                                                                                                                                                                                                                                                                                                        %r14,%rsi
159
                            400586:
                                                        44 89 ff
                                                                                                                                                                                                                400586:
                                                                                                                                                                                                                                                                                                                    mov
                                                                                                                                                                                                                                                                                                                                        %r15d.%edi
                                                                                                                                                                                                                  400580: 44 69 11

400589: 41 ff 14 dc

40058d: 48 83 c3 01

400591: 48 39 eb
                                                                                                                                                                                                                                                                                                                  callq *(%r12,%rbx,8)
add $0x1,%rbx
cmp %rbp,%rbx
160
161
                            400589:
40058d:
                                                       41 ff 14 dc
48 83 c3 01
162
                            400591:
                                                        48 39 eb
                                                                                                                             cmp
                                                                                                                                                 %rbp,%rbx
                                                                                                                                                 400580 <_libc_csu_init 400594: 75 e
$0x8, %rsp 400596: 48 83 c4 08
%rbx 40059a: 5b
                                                      75 ea
48 83 c4 08
                                                                                                                                                                                                                                                                                                                    jne 40
add $0x8,%rsp
                             400594:
                                                                                                                                                                                                                                                                                                                                                               400580 <__libc_csu_init
                             400596
                                                                                                                                                                               400596: 48
40059a: 5b
40059b: 5d
40059c: 41 5c
                                                                                                                                                                                                                                                                                                        pop
pop
166
                            40059b:
                                                                                                                                                 %rbp
%r12
                                                                                                                                                                                                                                                                                                                             %rbp
%r12
167
                            40059c:
                                                       41 5c
168
169
                                                                                                                                                 %r13
%r14
                                                                                                                                                                                                                                                                                                                             %r13
%r14
                             40059e:
                                                                                                                                                                                                        40059e:
                                                                                                                                                                                                                                                                                                         pop
170
                            4005a2:
                                                       41 5f
                                                                                                                                                 %r15
                                                                                                                                                                                                        4005a2: 41 5f
                                                                                                                                                                                                                                                                                                                             %r15
171
                             4005a4 ·
                                                                                                                                                                                                        4005a4: c3
                                                                                                                                                                                           4005a5: 90 nop
rax,1) 4005a6: 66 2e 0f 1f 84 00 00
                                                     66 2e Of 1f 84 00 00
                                                                                                                                             %cs:0x0(%rax,%rax,1)
                                                                                                                                                                                                                                                                                                                         nopw %cs:0x0(%rax,%rax,1)
                             4005a6:
                                                                                                                                                                    4005ad: 00 00 00
174
                            4005ad: 00 00 00
175
                                                                                                                                                                        00000000004005b0 <__libc_csu_fini>:
                      00000000004005b0 <__libc_csu_fini>:
177
                            4005b0: f3 c3
                                                                                                                          repz retq
                                                                                                                                                                                                     4005b0: f3 c3
                                                                                                                                                                                                                                                                                                        repz retq
178
179
180
181
                      Disassembly of section .fini:
                                                                                                                                                                                    Disassembly of section .fini:
                      00000000004005b4 <_fini>:
                                                                                                                                                                         00000000004005b4 <_fini>:
                                                                                                                                                                               4005b4: 48 83 ec 08
4005b8: 48 83 c4 08
4005bc: c3
                           4005b4: 48 83 ec 08
4005b8: 48 83 c4 08
4005bc: c3
182
                                                                                                                            sub $0x8,%rsp
add $0x8,%rsp
                                                                                                                                                                                                                                                                                                                sub
                                                                                                                                                                                                                                                                                                                                        $0x8.%rsp
183
184
                                                                                                                                                                                                                                                                                                                   add
                                                                                                                            retq
185
                     == No Difference ==
```

## Memory Initialization

#### declared in .BSS segment

FINI

30

INIT\_ARRAY

```
// segments 1.cc
2
     #include <stdio.h>
     #include <string.h>
     #define N (1024)
     int value[N]; // .bss
8
9
     int main(void) {
10
       memset(&value, 'x', N);
11
       fprintf(stdout, "value: %d\n", value[0]);
12
       return 0;
13
     }
14
15
   // *EOF*
16
   ./bin/segments_1:
                    file format elf64-x86-64
2
   ./bin/segments_1
   architecture: i386:x86-64, flags 0x00000112:
   EXEC_P, HAS_SYMS, D_PAGED
   start address 0x0000000000400470
8
   Program Header:
     PHDR off 0x00000000000000000 vaddr 0x000000000400040 paddr 0x0000000000400040 align 2**3
9
10
         filesz 0x00000000000001c0 memsz 0x000000000001c0 flags r-x
    11
          filesz 0x0000000000000000 memsz 0x00000000000000 flags r-
12
     LOAD off 0x0000000000000000 vaddr 0x000000000400000 paddr 0x000000000400000 align 2**21
13
         filesz 0x000000000000074c memsz 0x0000000000074c flags r-x
14
     LOAD off 0x00000000000000750 vaddr 0x000000000600750 paddr 0x0000000000600750 align 2**21
         filesz 0x000000000000228 memsz 0x00000000001250 flags rw-
16
   17
         filesz 0x00000000000001d0 memsz 0x000000000001d0 flags rw-
18
      NOTE off 0x00000000000001c vaddr 0x00000000040021c paddr 0x00000000040021c align 2**2
19
         20
   21
22
         filesz 0x00000000000000034 memsz 0x000000000000034 flags r--
     STACK off 0x000000000000000 vaddr 0x0000000000000 paddr 0x0000000000000 align 2**4
23
          filesz 0x00000000000000000 memsz 0x000000000000000 flags rw-
25
   Dynamic Section:
26
27
    NEEDED
                    libc.so.6
    INIT
                     0x00000000004003f8
28
```

v 11

0x0000000000400604

0x0000000000600750

```
INIT_ARRAYSZ
                           0x0000000000000008
      FINI_ARRAY
                           0x0000000000600758
32
      FINI_ARRAYSZ
                           33
34
      HASH
                           0x0000000000400240
      STRTAB
                           0x000000000400300
35
      SYMTAB
                           0 \times 0000000000400270
      STRSZ
                           0x0000000000000004e
37
      SYMENT
                           0x000000000000018
38
      DEBUG
                           0x000000000000000
39
      PLTGOT
                           0x0000000000600938
40
      PLTRELSZ
                           0x000000000000048
41
                           0x0000000000000007
      PLTREL
42
      JMPREL
                           0х0000000004003b0
43
      R.F.T.A
44
                           0x0000000000400380
      RELASZ
                           45
      RELAENT
                           0x000000000000018
46
      VERNEED
                           0x0000000000400360
47
48
      VERNEEDNUM
                           0x0000000000000001
      VERSYM
                           0x000000000040034e
49
50
51
    Version References:
      required from libc.so.6:
52
        0x09691a75 0x00 02 GLIBC_2.2.5
53
54
    Sections:
55
                                                                    File off Algn
    Idx Name
                                VMA
                                                  LMA
56
                      Size
                                000000000400200 000000000400200
                                                                    00000200
      0 .interp
                      000001c
57
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
58
      1 .note.ABI-tag 00000020 00000000040021c 000000000040021c
                                                                    0000021c 2**2
59
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
                      0000002c 000000000400240 000000000400240
                                                                    00000240 2**3
61
      2 .hash
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
62
63
      3 .dynsym
                      00000090 000000000400270 000000000400270
                                                                    00000270 2**3
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
64
65
      4 .dynstr
                      0000004e 000000000400300 000000000400300
                                                                    00000300 2**0
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
66
67
      5 .gnu.version
                      000000c
                                00000000040034e 00000000040034e
                                                                    0000034e
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
68
      6 .gnu.version_r 00000020 000000000400360 0000000000400360
                                                                     00000360
69
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
70
      7 .rela.dyn
                      00000030 000000000400380 000000000400380
                                                                    00000380 2**3
71
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
72
      8 .rela.plt
                      00000048 0000000004003b0 0000000004003b0
                                                                    000003b0
                                                                             2**3
73
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
74
                      0000001a 0000000004003f8 0000000004003f8
      9 .init
                                                                    000003f8 2**2
75
                      CONTENTS, ALLOC, LOAD, READONLY, CODE
76
77
     10 .plt
                      00000040 \quad 000000000400420 \quad 000000000400420
                                                                    00000420
                                                                              2**4
                      CONTENTS, ALLOC, LOAD, READONLY, CODE
78
     11 .plt.got
                      00000008 \quad 000000000400460 \quad 0000000000400460
                                                                    00000460
79
                      CONTENTS, ALLOC, LOAD, READONLY, CODE
80
                                000000000400470 000000000400470
     12 .text
                      00000192
                                                                    00000470 2**4
81
82
                      CONTENTS, ALLOC, LOAD, READONLY, CODE
                      00000009 000000000400604 0000000000400604
     13 .fini
                                                                    00000604 2**2
83
                      CONTENTS, ALLOC, LOAD, READONLY, CODE
                      0000000f
                                000000000400610 000000000400610
                                                                    00000610 2**2
85
     14 .rodata
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
86
     15 .eh_frame_hdr 00000034 000000000400620 0000000000400620
                                                                    00000620
```

```
CONTENTS, ALLOC, LOAD, READONLY, DATA
88
                      000000f4 000000000400658 000000000400658
      16 .eh_frame
                                                                 00000658 2**3
89
                      CONTENTS, ALLOC, LOAD, READONLY, DATA
90
91
      17 .init_array
                      00000008 000000000600750 0000000000600750
                                                                 00000750 2**3
                      CONTENTS, ALLOC, LOAD, DATA
92
      18 .fini_array
                      00000008 0000000000600758
                                                0000000000600758
                                                                 00000758 2**3
93
                      CONTENTS, ALLOC, LOAD, DATA
94
                      000001d0
                               0000000000600760
                                                0000000000600760
                                                                 00000760
95
      19 .dynamic
                      CONTENTS, ALLOC, LOAD, DATA
96
      20 .got
                      00000008 \quad 000000000600930 \quad 000000000600930
                                                                 00000930
97
                      CONTENTS, ALLOC, LOAD, DATA
98
      21 .got.plt
                               000000000600938 000000000600938
                                                                 00000938 2**3
                      00000030
99
                      CONTENTS, ALLOC, LOAD, DATA
100
      22 .data
                      00000010 000000000600968 0000000000600968
                                                                 00000968 2**3
101
                      CONTENTS, ALLOC, LOAD, DATA
102
      23 .bss
                      00001020 \quad 000000000600980 \quad 000000000600980
                                                                 00000978 2**5
103
                      ALLOC
104
105
        .comment
                      00000029
                               00000978 2**0
                      CONTENTS, READONLY
106
      000009a1 2**0
107
                      CONTENTS, READONLY, DEBUGGING
108
      26 .debug_info
                      000009d1 2**0
109
                      CONTENTS, READONLY, DEBUGGING
110
      00000d22 2**0
111
                      CONTENTS, READONLY, DEBUGGING
112
                      28 .debug_line
                                                                 00000e1c 2**0
113
                      CONTENTS, READONLY, DEBUGGING
114
                      000002b8 00000000000000 000000000000000
                                                                 00000f0c 2**0
      29 .debug_str
115
                      CONTENTS, READONLY, DEBUGGING
116
     SYMBOL TABLE:
     0000000000400200 1
                                      0000000000000000
118
                            .interp
                                                                   .interp
     000000000040021c 1
                            .note.ABI-tag 0000000000000000
                                                                       .note.ABI-tag
119
120
     0000000000400240 1
                         d
                            .hash 0000000000000000
                                                               .hash
     0000000000400270 1
                                       0000000000000000
                         d
                            .dvnsvm
                                                                   .dynsym
121
     000000000400300 1
                            .dynstr
                                       0000000000000000
                                                                   .dynstr
                            .gnu.version 0000000000000000
     0000000000040034e 1
                                                                      .gnu.version
                         d
123
                            .gnu.version_r 00000000000000000
     0000000000400360 1
                                                                       .gnu.version_r
124
     0000000000400380 1
                            .rela.dyn 0000000000000000
                                                                   .rela.dyn
125
     00000000004003b0 1
                            .rela.plt 00000000000000000
                                                                   .rela.plt
126
                            .init 0000000000000000
127
     00000000004003f8 1
                                                                .init.
                                                               .plt
     0000000000400420 1
                            .plt
                                  0000000000000000
128
     0000000000400460 1
                                      000000000000000
                                                                   .plt.got
129
                            .plt.got
     0000000000400470 1
                            .text 0000000000000000
130
                                                               .text
     0000000000400604 1
                            .fini 0000000000000000
131
     0000000000400610 1
                            .rodata
                                      000000000000000
                                                                   .rodata
     0000000000400620 1
                            .eh_frame_hdr 0000000000000000
                                                                      .eh_frame_hdr
                         d
133
     000000000400658 1
                            .eh_frame 0000000000000000
                                                                   .eh_frame
                            .init_array
     0000000000600750 1
                                          0000000000000000
135
                                                                      .init arrav
     0000000000600758 1
                                          0000000000000000
                            .fini_array
                                                                       .fini_array
136
                                      0000000000000000
137
     0000000000600760 1
                            .dynamic
                                                                   .dynamic
     0000000000600930 1
                            .got 0000000000000000
138
                                                               .got
                                                                   .got.plt
139
     000000000600938 1
                         d
                            .got.plt
                                      0000000000000000
                            .data 0000000000000000
     0000000000600968 1
                                                                .data
140
141
     0000000000600980 1
                            .bss 0000000000000000
                            .comment 0000000000000000
     000000000000000000001
142
                         d
                                                                   .comment
143
     00000000000000000001
                            .debug_aranges 0000000000000000
                                                                       .debug_aranges
     00000000000000000001
                            .debug_info
                                          0000000000000000
                                                                       .debug_info
144
```

```
d .debug_abbrev 00000000000000000
     00000000000000000001
                                                                            .debug_abbrev
     000000000000000000001
                                             0000000000000000
                              .debug_line
                                                                            .debug_line
146
     000000000000000000001
                              .debug_str 00000000000000000
                                                                        .debug_str
147
     00000000000000000001
                           df *ABS* 000000000000000
                                                                    crtstuff.c
148
     00000000004004a0 1
                            F .text 0000000000000000
                                                                    deregister_tm_clones
149
     00000000004004d0 1
                            F .text 000000000000000
                                                                    register_tm_clones
     0000000000400510 1
                            F .text 000000000000000
                                                                    __do_global_dtors_aux
151
     0000000000600988 1
                                     0000000000000001
                                                                    completed.6981
152
                            0 .bss
     0000000000600758 1
                                             0000000000000000
                            0 .fini_array
                                                                            __do_global_dtors_aux_fini_array_entry
153
     0000000000400540 1
                            F .text 0000000000000000
154
     0000000000600750 1
                            0 .init_array
                                             0000000000000000
                                                                            __frame_dummy_init_array_entry
     00000000000000000001
                           df *ABS* 000000000000000
                                                                    segments_1.cc
156
     00000000000000000001
                           df *ABS* 000000000000000
                                                                    crtstuff.c
157
                           O .eh_frame 0000000000000000
                                                                        __FRAME_END__
158
     0000000000400748 1
                           df *ABS* 000000000000000
     00000000000000000001
159
     0000000000600758 1
                              .init_array
                                            0000000000000000
                                                                            __init_array_end
     0000000000600760 1
                            O .dynamic 000000000000000
                                                                        _DYNAMIC
161
     0000000000600750 1
                               .init_array
                                             0000000000000000
                                                                            __init_array_start
                              .eh_frame_hdr 0000000000000000
     0000000000400620 1
                                                                             _GNU_EH_FRAME_HDR
163
                            O .got.plt 000000000000000
     0000000000600938 1
                                                                        _GLOBAL_OFFSET_TABLE_
164
     0000000000400600 g
                            F .text 0000000000000002
                                                                    __libc_csu_fini
165
                                                                    _ITM_deregisterTMCloneTable
     000000000000000 w
                              *UND*
                                     0000000000000000
166
                                                                    stdout@GLIBC_2.2.5
     0000000000600980 g
                            0 .bss
                                     800000000000000
     0000000000600968 w
                              .data 00000000000000000
                                                                    data_start
168
     0000000000600978 g
                              .data 0000000000000000
                                                                    _edata
169
     0000000000400604 g
                                                                    _fini
                            F .fini 0000000000000000
170
                                                                    memset@@GLIBC_2.2.5
     0000000000000000
                            F *UND*
                                     0000000000000000
171
                                                                    __libc_start_main@@GLIBC_2.2.5
     0000000000000000
                            F *UND*
                                     0000000000000000
     0000000000600968 g
                              .data 0000000000000000
173
                                                                     data start
     00000000000000000
                            F *UND*
                                     0000000000000000
                                                                    fprintf@@GLIBC_2.2.5
                              *UND*
     W 000000000000000 W
                                     0000000000000000
                                                                    __gmon_start__
175
     00000000006009a0 g
                            0.bss
                                     000000000001000
                                                                    value
176
     0000000000600970 g
177
                            O .data 0000000000000000
                                                                    .hidden __dso_handle
     0000000000400610 g
                                         0000000000000004
                                                                        _IO_stdin_used
                            O .rodata
178
     0000000000400590 g
                            F .text 000000000000065
                                                                    __libc_csu_init
     00000000006019a0 g
                                                                    _end
                              .bss
                                     00000000000000000
180
     0000000000400470 g
                            F .text
                                     000000000000002a
                                                                    _start
181
     0000000000600978 g
                                                                    __bss_start
                                     0000000000000000
182
                              .bss
     0000000000400547 g
                            F .text 00000000000003e
                                                                    main
183
                                                                    .hidden __TMC_END__
     0000000000600978 g
                            _ITM_registerTMCloneTable
     w 000000000000000
                              *UND* 000000000000000
185
     00000000004003f8 g
                            F .init 0000000000000000
186
                                                                    init
```

#### declared in .DATA segment

187

```
1  // segments_2.cc
2
3  #include <stdio.h>
4
5  #define N (1024)
```

```
int value[N]; // .data
7
8
     int main(void) {
9
       value[0] = 0xdeadbeef;
10
       value[N] = Oxdeadbeef;
       fprintf(stdout, "value: %d\n", value[0]);
12
       return 0;
13
14
15
   // *E0F*
16
                     file format elf64-x86-64
   ./bin/segments_2:
   ./bin/segments_2
   architecture: i386:x86-64, flags 0x00000112:
4
5
   EXEC_P, HAS_SYMS, D_PAGED
   start address 0x0000000000400420
6
   Program Header:
      PHDR off
                0x0000000000000000000 vaddr 0x0000000000400040 paddr 0x000000000400040 align 2**3
9
          10
     11
          filesz 0x000000000000001c memsz 0x000000000000001c flags r--
      LOAD off 0x0000000000000000 vaddr 0x000000000400000 paddr 0x000000000400000 align 2**21
13
          14
      LOAD off 0x00000000000006f0 vaddr 0x0000000006f0 paddr 0x00000000006f0 align 2**21
15
          filesz 0x0000000000000220 memsz 0x00000000001250 flags rw-
16
    filesz 0x00000000000001d0 memsz 0x000000000001d0 flags rw-
18
      NOTE off 0x00000000000021c vaddr 0x00000000040021c paddr 0x000000000040021c align 2**2
19
          20
   EH_FRAME off 0x00000000000005c0 vaddr 0x0000000004005c0 paddr 0x00000000004005c0 align 2**2
21
          filesz 0x0000000000000034 memsz 0x000000000000034 flags r--
     STACK off 0x000000000000000 vaddr 0x000000000000 paddr 0x000000000000 align 2**4
23
          filesz 0x0000000000000000 memsz 0x00000000000000 flags rw-
24
25
   Dynamic Section:
26
     NEEDED
                      libc.so.6
     INIT
                      0x0000000004003b8
28
     FINI
                      0x00000000004005a4
30
     INIT ARRAY
                      0x00000000006006f0
     INIT_ARRAYSZ
                      0x0000000000000008
31
     FINI_ARRAY
                      0x0000000006006f8
32
     FINI_ARRAYSZ
                      0x0000000000000008
33
     HASH
                      0x0000000000400240
     STRTAB
                      0x00000000004002e0
35
     SYMTAB
                      0x0000000000400268
36
     STRSZ
                      0x0000000000000047
37
     SYMENT
                      0x000000000000018
38
     DEBUG
                      0x0000000000000000
39
     PLTGOT
                      0x0000000006008d8
40
     PLTRELSZ
                      PLTREL
                      0x00000000000000007
42
     JMPREL
                      0x000000000400388
43
```

44	RELA 0x00000000400358										
45				0000000000030							
46				0000000000018							
47	VE	RNEED	0x000	0000000400338							
48	VE	CRNEEDNUM	0x000	00000000001							
49	VE	RSYM	0x000	0000000400328							
50											
51	Version References:										
52	required from libc.so.6:										
53	0x09691a75 0x00 02 GLIBC_2.2.5										
54											
55	Sect	ions:									
56	Idx	Name	Size	VMA LMA	File off	Algn					
57	0	.interp	0000001c	000000000400200 000000000400200	00000200	2**0					
58		-	CONTENTS,	ALLOC, LOAD, READONLY, DATA							
59	1	.note.ABI-tag	00000020	00000000040021c 00000000040021c	0000021c	2**2					
60		· ·	CONTENTS,	ALLOC, LOAD, READONLY, DATA							
61	2	.hash	00000028	000000000400240 0000000000400240	00000240	2**3					
62			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
63	3	.dynsym	00000078	000000000400268 000000000400268	00000268	2**3					
64			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
65	4	.dynstr	00000047	0000000004002e0 0000000004002e0	000002e0	2**0					
66			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
67	5	.gnu.version	0000000a	000000000400328 000000000400328	00000328	2**1					
68			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
69	6	.gnu.version_	00000020	000000000400338 000000000400338	00000338	2**3					
70			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
71	7	.rela.dyn	00000030	000000000400358 000000000400358	00000358	2**3					
72			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
73	8	.rela.plt	00000030	000000000400388 000000000400388	00000388	2**3					
74			CONTENTS,	ALLOC, LOAD, READONLY, DATA							
75	9	.init	0000001a	0000000004003b8 0000000004003b8	000003ъ8	2**2					
76			CONTENTS,	ALLOC, LOAD, READONLY, CODE							
77	10	.plt	00000030	0000000004003e0 0000000004003e0	000003e0	2**4					
78			CONTENTS,	ALLOC, LOAD, READONLY, CODE							
79	11	.plt.got	8000000	000000000400410 000000000400410	00000410	2**3					
80			-	ALLOC, LOAD, READONLY, CODE							
81	12	.text	00000182	000000000400420 000000000400420	00000420	2**4					
82				ALLOC, LOAD, READONLY, CODE							
83	13	.fini	00000009	00000000004005a4 0000000004005a4	000005a4	2**2					
84			-	ALLOC, LOAD, READONLY, CODE							
85	14	.rodata	0000000f	0000000004005b0 0000000004005b0	000005b0	2**2					
86			-	ALLOC, LOAD, READONLY, DATA	000005 0	00					
87	15	.eh_frame_hdr		0000000004005c0 0000000004005c0	000005c0	2**2					
88	10	-1 f	•	ALLOC, LOAD, READONLY, DATA	00000540	Outsuts 2					
89	16	.eh_frame	000000f4	0000000004005f8 0000000004005f8	000005f8	2**3					
90	17	ini+		ALLOC, LOAD, READONLY, DATA	00000640	U**3					
91	17	.init_array	00000008	0000000006006f0 0000000006006f0	000006f0	2**3					
92	10	fini c	-	ALLOC, LOAD, DATA	00000648	U**3					
93	18	.fini_array	00000008	0000000006006f8 0000000006006f8	000006f8	2**3					
94	10	dunamia		ALLOC, LOAD, DATA 00000000000600700 000000000600700	00000700	0++3					
95	19	.dynamic	000001d0		00000700	2**3					
96	20	mot.	00000008	ALLOC, LOAD, DATA 000000000006008d0 0000000006008d0	000000840	2**3					
97	20	.got		ALLOC, LOAD, DATA	000008d0	∠ <b>∓</b> ∓∪					
98	21	.got.plt	00000028	00000000006008d8 0000000006008d8	000008d8	2**3					
99	21	.goc.prc		ALLOC, LOAD, DATA	JUUUUUU	20					
100			CONTENTO,	ndlov, bond, bair							

```
22 .data
                      00000010 000000000600900 000000000600900 00000900 2**3
                      CONTENTS, ALLOC, LOAD, DATA
102
      23 .bss
                      00001020 000000000600920 000000000600920
                                                                 00000910 2**5
103
                      ALLOC
104
                      00000910 2**0
      24 .comment
105
                      CONTENTS, READONLY
      00000939 2**0
107
                      CONTENTS, READONLY, DEBUGGING
108
                      00000969
      26 . debug_info
                                                                         2**0
109
                      CONTENTS, READONLY, DEBUGGING
110
      00000cba 2**0
111
                      CONTENTS, READONLY, DEBUGGING
112
      28 .debug_line
                      00000db4 2**0
113
                      CONTENTS, READONLY, DEBUGGING
114
                      000002b8 00000000000000 0000000000000 00000ea2 2**0
      29 .debug_str
115
                      CONTENTS, READONLY, DEBUGGING
116
     SYMBOL TABLE:
117
118
     0000000000400200 1
                            .interp
                                      000000000000000
                                                                   .interp
                            .note.ABI-tag 000000000000000
     000000000040021c 1
                                                                      .note.ABI-tag
119
                         d
     0000000000400240 1
                            .hash 0000000000000000
120
                                      0000000000000000
     0000000000400268 1
                            .dynsym
                                                                   .dynsym
121
     00000000004002e0 1
                            .dynstr
                                       000000000000000
                                                                   .dynstr
122
     000000000400328 1
                            .gnu.version 0000000000000000
                                                                       .gnu.version
123
     0000000000400338 1
                            .gnu.version_r 00000000000000000
                                                                       .gnu.version_r
124
     0000000000400358 1
                            .rela.dyn 0000000000000000
                                                                   .rela.dyn
     0000000000400388 1
                            .rela.plt 0000000000000000
126
                                                                   .rela.plt
                            .init 0000000000000000
     00000000004003b8 1
                                                               .init
127
                            .plt 0000000000000000
     00000000004003e0 1
                                                               .plt
     0000000000400410 1
                                      0000000000000000
129
                            .plt.got
                                                                   .plt.got
     000000000400420 1
                            .text 0000000000000000
                                                               .text
                            .fini 0000000000000000
     00000000004005a4 1
131
                                                               .fini
     00000000004005b0 1
                            .rodata
                                      000000000000000
                                                                   .rodata
132
133
     00000000004005c0 1
                         d
                            .eh_frame_hdr 0000000000000000
                                                                       .eh_frame_hdr
     00000000004005f8 1
                            .eh_frame 0000000000000000
                                                                   .eh frame
134
     00000000006006f0 1
                            .init_array
                                          0000000000000000
                                                                       .init_array
                            .fini_array
                                          000000000000000
     000000000006006f8 1
                         Ы
                                                                       .fini arrav
136
     0000000000600700 1
                            .dynamic
                                     0000000000000000
                                                                   .dynamic
137
                            .got 0000000000000000
     00000000006008d0 1
138
                                                               .got
     00000000006008d8 1
                            .got.plt 0000000000000000
                                                                   .got.plt
139
                            .data 00000000000000000
140
     0000000000600900 1
                                                               .data
     0000000000600920 1
                            .bss
                                  0000000000000000
                                                               .bss
141
     00000000000000000001
                            .comment
                                      0000000000000000
142
                                                                   .comment
     0000000000000000000001
                            .debug_aranges 00000000000000000
                                                                      .debug_aranges
143
     0000000000000000001
                            .debug_info
                                          000000000000000
                                                                      .debug_info
144
     0000000000000000001
                            .debug_abbrev 0000000000000000
                                                                       .debug_abbrev
     00000000000000000001
                         А
                            .debug_line
                                          0000000000000000
                                                                       .debug_line
146
     000000000000000000001
                            .debug_str 0000000000000000
                                                                   .debug_str
                         df *ABS* 000000000000000
     00000000000000000001
                                                               crtstuff.c
148
     0000000000400450 1
                          F .text 000000000000000
                                                               deregister_tm_clones
149
                          F .text 000000000000000
150
     0000000000400480 1
                                                               register_tm_clones
     00000000004004c0 1
                          F .text 0000000000000000
                                                               __do_global_dtors_aux
151
152
     0000000000600928 1
                          0 .bss
                                  0000000000000001
                                                               completed.6981
     00000000006006f8 1
                          O .fini_array
                                          0000000000000000
                                                                       __do_global_dtors_aux_fini_array_entry
153
     00000000004004f0 1
                          F .text 0000000000000000
     00000000006006f0 1
                          0 .init_array
                                          0000000000000000
155
                                                                       __frame_dummy_init_array_entry
                         df *ABS* 000000000000000
156
     00000000000000000001
                                                               segments_2.cc
                         df *ABS* 000000000000000
     00000000000000000001
                                                               crtstuff.c
157
```

```
00000000004006e8 1
                            0 .eh_frame 000000000000000
                                                                         __FRAME_END__
                            df *ABS* 000000000000000
     000000000000000000001
159
     00000000006006f8 1
                               .init_array
                                              0000000000000000
                                                                              _init_array_end
160
     0000000000600700 1
                             O .dvnamic
                                         0000000000000000
                                                                          DYNAMIC
161
     00000000006006f0 1
                                              0000000000000000
                                                                             __init_array_start
                               .init array
162
     0000000004005c0 1
                               .eh_frame_hdr 0000000000000000
                                                                              __GNU_EH_FRAME_HDR
     0000000000600848 1
                            O .got.plt
                                         0000000000000000
                                                                         _GLOBAL_OFFSET_TABLE_
164
                             F .text 0000000000000002
     00000000004005a0 g
165
                                                                      _libc_csu_fini
                                                                     _ITM_deregisterTMCloneTable
                               *UND*
                                      0000000000000000
     000000000000000 w
166
     0000000000600920 g
                             0 .bss
                                      800000000000000
                                                                     stdout@GLIBC_2.2.5
167
     0000000000600900 w
                               .data
                                      0000000000000000
                                                                     data_start
     0000000000600910 g
                                                                     _edata
                               .data
                                      0000000000000000
169
     00000000004005a4 g
                             F .fini
                                      000000000000000
                                                                     fini
170
                             F *UND*
                                                                     __libc_start_main@@GLIBC_2.2.5
171
     0000000000000000
                                      00000000000000000
     0000000000600900 g
                               .data
                                     0000000000000000
                                                                     __data_start
172
     0000000000000000
                             F *UND*
                                      0000000000000000
                                                                     fprintf@@GLIBC_2.2.5
     W 00000000000000000
                               *UND*
                                      0000000000000000
                                                                     __gmon_start__
174
     0000000000600940 g
                             0 .bss
                                      000000000001000
                                                                     value
     0000000000600908 g
                                     0000000000000000
                                                                     .hidden __dso_handle
                             O .data
176
     00000000004005b0 g
                             O .rodata
                                          0000000000000004
                                                                         _IO_stdin_used
177
                            F .text 000000000000065
     0000000000400530 g
                                                                     __libc_csu_init
178
     0000000000601940 g
                                      000000000000000
                                                                     _end
                               .bss
179
     0000000000400420 g
                             {\tt F} .text
                                      0000000000000002a
                                                                     _start
     0000000000600910 g
                                      0000000000000000
181
                               .bss
                                                                     __bss_start
     00000000004004f7 g
                             F .text
                                      0000000000000002a
182
     0000000000600910 g
                                      0000000000000000
                                                                     .hidden __TMC_END__
183
                             O .data
     w 000000000000000
                               *UND*
                                      0000000000000000
                                                                     _ITM_registerTMCloneTable
184
     00000000004003b8 g
                             F .init
                                     0000000000000000
                                                                     init
185
186
```

#### implementation difference (side-by-side diff, with suppression)

```
/bin/segments_1
                                                               | ./bin/segments_2
        start address 0x0000000000400470
                                                                        | start address 0x0000000000400420
                  filesz 0x0000000000000074c memsz 0x00000000000074c flags r-x
off 0x0000000000000750 vaddr 0x000000000000750 paddr 0x00
filesz 0x0000000000000228 memsz 0x00000000001250 flags rw-
                                                                                                       filesz 0x0000000000006c memsz 0x000000000006c flags r-x
LOAD off 0x0000000000006f0 vaddr 0x00000000006f0 paddr 0x00
filesz 0x000000000000220 memsz 0x00000000001250 flags rw-
         DYNAMIC off
                                                                                                   DYNAMIC off
                                                                                                                    0x000000000000000000 vaddr 0x0000000000600700 paddr 0x00
                           0x0000000000000760 vaddr 0x0000000000600760 paddr 0x00
        EH_FRAME off
INIT
                          0x0000000000000620 vaddr 0x0000000000400620
0x000000000004003f8 |
0x00000000000400604 |
                                                                               paddr 0x00
                                                                                                 | EH_FRAME off
                                                                                                                     0x00000000000005c0 vaddr 0x0000000004005c0 paddr 0x00
           FINI
                                                                                  FINI
                                                                                                           0x00000000004005a4
           TNTT ARRAY
                                   0x00000000000600750
                                                                                  TNIT ARRAY
                                                                                                           0x00000000006006f0
10
11
12
13
          FINI_ARRAY
STRTAB
                                    FINI_ARRAY
STRTAB
                                                                                                           0x0000000000400270
           SYMTAB
                                                                                  SYMTAB
                                                                                                           0x0000000000400268
14
           STRSZ
                                    0x0000000000000004e
                                                                                  STRSZ
                                                                                                           0x0000000000000047
15
16
17
          PLTGOT
PLTRELSZ
                                    0x0000000000600938
                                                                                  PLTGOT
                                                                                                           0×0000000000000848
           JMPREL
                                    0х00000000004003b0
                                                                                  JMPREL
                                                                                                           0x0000000000400388
18
19
20
21
           RELA
                                   0x0000000000400380
                                                                                  RELA
                                                                                                           0x0000000000400358
           VERNEED
                                    0x0000000000400360
                                                                                  VERNEED
                                                                                                           0×00000000000400338
                                                                                                           0x00000000000400328
                                    0x000000000040034e
                                                                                  VERSYM
           2 .hash
                             0000002c 000000000400240
                                                              0000000000400240
                                                                                    000002
                                                                                                    2 .hash
                                                                                                                       00000028
                                                                                                                                    0000000000400240
                                                                                                                                                        0000000000400240
                                                                                                                                                                              000002
                                                                                                       .dynsym
.dynstr
22
          3 .dynsym
4 .dynstr
                             00000090 0000000000400270
                                                              00000000000400270
                                                                                    000002
                                                                                                                       00000078
                                                                                                                                    00000000000400268
                                                                                                                                                         00000000000400268
                                                                                                                                                                              000002
             .gnu.version
                             0000000c
                                         000000000040034e
                                                               000000000040034e
                                                                                                        .gnu.version
                                                                                                                       0000000a
                                                                                                                                    0000000000400328
                                                                                                                                                         0000000000400328
                                                                                                                                                                               000003
                                                                                                        .gnu.version_r 00000020
.rela.dyn 00000030
.rela.plt 00000030
             .gnu.version_r 00000020
.rela.dyn 00000030
25
                                          0000000000400360
                                                                0000000000400360
                                                                                    00000
                                                                                                                                    0000000000400338
                                                                                                                                                          0000000000400338
                                                                                                                                                                               00000
                                         00000000000400380
                                                               00000000000400380
                                                                                    000003
                                                                                                                                    00000000000400358
                                                                                                                                                         00000000000400358
                                                                                                                                                                               000003
                              00000048
                                         00000000004003ь0
                                                                                                                                    0000000000400388
             .rela.plt
           9 .init
                              0000001a
                                         00000000004003f8
                                                               00000000004003f8
                                                                                    000003
                                                                                                        .init
                                                                                                                        0000001a
                                                                                                                                    00000000004003ъ8
                                                                                                                                                         00000000004003ъ8
                                                                                                                                                                               000003
29
          10 .plt
                              00000040
                                         0000000000400420
                                                               0000000000400420
                                                                                    000004
                                                                                                    10
                                                                                                        .plt
                                                                                                                        00000030
                                                                                                                                    00000000004003e0
                                                                                                                                                         00000000004003e0
                                                                                                                                                                               000003
         11 .plt.got
12 .text
                                                                                                        .plt.got
.text
30
                              80000000
                                          00000000000400460
                                                               00000000000400460
                                                                                    000004
                                                                                                                        00000008
                                                                                                                                    00000000000400410
                                                                                                                                                         00000000000400410
                                                                                                                                                                               000004
32
          13 .fini
                              00000009
                                         0000000000400604
                                                               0000000000400604
                                                                                    000006
                                                                                                    13 .fini
                                                                                                                        00000009
                                                                                                                                    00000000004005a4
                                                                                                                                                         00000000004005a4
                                                                                                                                                                              000005
33
          14 .rodata
                              0000000f
                                         00000000000400610
                                                               00000000000400610
                                                                                    000006
                                                                                                    14 .rodata
                                                                                                                        0000000f
                                                                                                                                    000000000004005b0
                                                                                                                                                         000000000004005b0
                                                                                                                                                                              000005
                             00000034
                                         0000000000400620
                                                                                                                       00000034
                                                                                                                                   00000000004005c0
                                                                                                                                                         00000000004005c0
```

35	16 .eh_frame		00000000400658 000006		000000f4 0000000004005f8	
36	17 .init_array		00000000600750 000007		00000008 00000000006006f	
37	18 .fini_array		000000000600758 000007		00000008 00000000006006f8	
38	19 .dynamic		000000000600760 000007		000001d0 00000000060070	
39 40	20 .got		000000000600930 000009 00000000600938 000009		00000008 00000000006008di 00000028 00000000006008di	
41	21 .got.plt 22 .data		000000000600938 000009		00000010 00000000000000000	
41	22 .data 23 .bss		000000000600980 000009		00001020 000000000000000920	
43	24 .comment		000000000000000000000000000000000000000		00000029 000000000000000000000000000000	
44	25 .debug_aranges		0000000000000000 00000	25 .debug_aranges		
45	26 .debug_info		0000000000000000 000009	26 .debug_info	00000351 0000000000000000	
46	27 .debug_abbrev		D00000 0000000000000000000000000000000	27 .debug_abbrev		
47	28 .debug_line		000000000000000 00000e	. 0=	000000ee 00000000000000000000000000000	
48	29 .debug_str		100000 0000000000000000000000000000000	29 .debug_str	000002ъ8 000000000000000	
49	0000000000400270	d .dynsym 000000000000	00000		d .dynsym 00000000000	
50	0000000000400300	l d .dynstr 000000000000	00000	00000000004002e0 1	d .dynstr 00000000000	00000
51	000000000040034e 3	d .gnu.version 00000000	00000000	000000000400328 ]	l d .gnu.version 000	000000000000
52	0000000000400360			000000000400338 1		
53	0000000000400380	l d .rela.dyn 000000000000	00000 I	0000000000400358 1	d .rela.dyn 000000000000	00000
54	00000000004003ъ0				d .rela.plt 00000000000	
55	00000000004003f8 1				d .init 0000000000000000	
56	0000000000400420	- ·p-· ·······			d .plt 0000000000000000	
57	0000000000400460				d .plt.got 00000000000	
58	0000000000400470				d .text 000000000000000	
59	0000000000400604				d .fini 00000000000000000000000000000000000	
60	00000000000400610	. a 1104404 0000000000		000000000000000000000000000000000000000	u 110uuuu 0000000000	
61 62	0000000000400620 1			0000000004005c0 1 00000000004005f8 1	<pre>d .eh_frame_hdr 0000 d .eh_frame 0000000000000</pre>	
63	000000000000000000000000000000000000000		000000000	000000000000000000000000000000000000		000000000000
64	0000000000000758		000000000	000000000000000000000000000000000000		000000000000
65	000000000000000000000000000000000000000				d .dynamic 00000000000	
66	000000000000000000000000000000000000000				d .got 000000000000000	
67	00000000000600938				d .got.plt 00000000000	
68	00000000000600968				d .data 00000000000000000	
69	0000000000600980	d .bss 00000000000000000	0 .bss	0000000000600920 1	d .bss 0000000000000000	0 .bss
70	00000000004004a0 1	F .text 00000000000000000000000000000000000	0 deregist	000000000400450 1	1 F .text 000000000000	00000 deregist
71	00000000004004d0 1	F .text 00000000000000000000000000000000000	0 register	000000000400480 1	F .text 00000000000000000000000000000000000	00000 register
72	0000000000400510			0000000004004c0		
73	0000000000600988			0000000000600928 1		
74	0000000000600758		00000000	00000000006006f8 ]		000000000000
75	0000000000400540			00000000004004f0 1		
76 77	000000000000000000000000000000000000000		000000000	00000000006006f0 1		000000000000
78	000000000000000000000000000000000000000			0000000000000000 1 00000000004006e8 1	<pre>df *ABS* 000000000000 0 .eh_frame 000000000000</pre>	
79	00000000000400748 1		000000000	000000000000000000000000000000000000		000000000000
80	000000000000758			000000000000000000000000000000000000000	0 .dynamic 000000000000	
81	000000000000000000000000000000000000000		000000000	00000000000000000100 1		000000000000
82	000000000000000000000000000000000000000			000000000000000000000000000000000000		
83	00000000000600938			000000000006008d8 1	0 .got.plt 00000000000	
84	0000000000400600 g			0000000004005a0 p		
85	00000000000000980 8	g 0.bss 000000000000000		0000000000600920	g 0.bss 00000000000	
86	0000000000600968			000000000600900		- · · · · - · · - · · · - · · · · · - ·
87	00000000000600978 g			0000000000600910 g		
88	0000000000400604 8			00000000004005a4 g	F .fini 00000000000000000000000000000000000	0 _fini
89	0000000000000000	F *UND* 000000000000000000000000000000000000		<		
90	00000000000600968 g			0000000000600900 g		
91 92	00000000000000000000000000000000000000			00000000000000000000000000000000000000	0 .bss 00000000000001000 g 0 .data 0000000000000	
93	000000000000000000000000000000000000000			000000000000000000000000000000000000		
93	0000000000400610 g			00000000004005b0 g   000000000400530 д		
95	00000000000400890 g			0000000000400830 g	.bss 00000000000000000000000000000000000	
96	000000000001940 8		- · · · · · · · · · · · · · · · · · · ·	00000000001940 g		
97	000000000000000000000000000000000000000			000000000000000000000000000000000000		
98	000000000000000000000000000000000000000			00000000004004f7 g	F .text 000000000000000	
99	00000000000000978			0000000000600910 g		
100	00000000004003f8			000000000004003ъ8 g	F .init 00000000000000000	
101						
102	== No Difference =					