05.PIC

List

PIC(Position Independent Code)

Description

- **해당 기술은 보호 기술은 아닙니다. PIE를 이해하기 전에 참고하기 위해 설명합니다.**
- **PIC(Position Independent Code)은 주기억 장치의 어딘가에 배치되어 절대 주소와 관계없이 모든 메모리 주소에서 수정없이 실행되는 기계 코드입니다.**
  - PIC는 일반적으로 공유 라이브러리에서 사용되며, 동일한 라이브러리 코드는 각 프로그램의 메모리 영역에 로드됩니다
  - 각 프로세서 들은 PIC를 서로 다른 주소에서 실행 할 수 있으며, 실행 시 재배치가 필요 없습니다.
  - 공유 라이브러리를 만들 때 -fPIC 옵션을 이용하여 소스를 컴파일 합니다.
- **Relocatable code**
  - Relocatable code는 말 그대로 재배치가 필요한 코드를 의미합니다.
  - 재배치 과정은 동적 링커에 의해 코드에 생성 된 label과 symbol의 주소를 수정하는 것입니다.

Example

Source code

Shared library - lazenca.c

```
#include <stdio.h>

void lazenca(int a){
        printf("Lazenca.0x%d\n",a);
}
```

Build

Build Command

```
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gcc -mcmodel=large -shared -o libNonPIC.so lazenca.c
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gcc -fPIC -shared -o libPIC.so lazenca.c
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gcc -fPIC -nostartfiles -shared -o libNoStartPIC.so
lazenca.c
```

Compare files(Non-PIC vs PIC vs NoStart) - Section Headers

- **다음과 같이 PIC가 적용되 파일과 적용되지 않은 파일이 다릅니다.**
  - PIC가 적용된 바이너리에는 ".rela.plt" 섹션이 추가 되어 있습니다.
  - PIC와 nostartfiles 옵션이 적용된 바이너리에는 ".rela.dyn", ".init", ".plt.got", ".fini", ".init_array", ".fini_array", ".jcr", ".got", ".data", ".bss" 섹션이 없습니다.

Check for Section Headers

Non-PIC	PIC	NoStartPIC
lazenca0x0@ubuntu:~/Documents /Definition/protection/PIC$ readelf -S libNonPIC.so There are 28 section headers, starting at offset 0x1850: Section Headers: [Nr] Name Type Address Offset Size EntSize Flags Link Info Align [0] NULL 0000000000000000 00000000 0000000000000000 0000000000000000 0 0 0 [1] .note.gnu.build-i NOTE 00000000000001c8 000001c8 0000000000000024 0000000000000000 A 0 0 4 [2] .gnu.hash GNU_HASH 00000000000001f0 000001f0 000000000000003c 0000000000000000 A 3 0 8 [3] .dynsym DYNSYM 0000000000000230 00000230 0000000000000150 0000000000000018 A 4 2 8 [4] .dynstr STRTAB 0000000000000380 00000380 00000000000000b2 0000000000000000 A 0 0 1 [5] .gnu.version VERSYM 0000000000000432 00000432 000000000000001c 0000000000000002 A 3 0 2 [6] .gnu.version_r VERNEED 0000000000000450 00000450 0000000000000020 0000000000000000 A 4 1 8 [7] .rela.dyn RELA 0000000000000470	lazenca0x0@ubuntu:~/Documents /Definition/protection/PIC$ readelf -S libPIC.so There are 29 section headers, starting at offset 0x1878: Section Headers: [Nr] Name Type Address Offset Size EntSize Flags Link Info Align [0] NULL 0000000000000000 00000000 0000000000000000 0000000000000000 0 0 0 [1] .note.gnu.build-i NOTE 00000000000001c8 000001c8 0000000000000024 0000000000000000 A 0 0 4 [2] .gnu.hash GNU_HASH 00000000000001f0 000001f0 000000000000003c 0000000000000000 A 3 0 8 [3] .dynsym DYNSYM 0000000000000230 00000230 0000000000000150 0000000000000018 A 4 2 8 [4] .dynstr STRTAB 0000000000000380 00000380 00000000000000b2 0000000000000000 A 0 0 1 [5] .gnu.version VERSYM 0000000000000432 00000432 000000000000001c 0000000000000002 A 3 0 2 [6] .gnu.version_r VERNEED 0000000000000450 00000450 0000000000000020 0000000000000000 A 4 1 8 [7] .rela.dyn RELA	lazenca0x0@ubuntu:~/Documents /Definition/protection/PIC$ readelf - S libNoStartPIC.so There are 19 section headers, starting at offset 0x13e8: Section Headers: [Nr] Name Type Address Offset Size EntSize Flags Link Info Align [0] NULL 0000000000000000 00000000 0000000000000000 0000000000000000 0 0 0 [1] .note.gnu.build-i NOTE 00000000000001c8 000001c8 0000000000000024 0000000000000000 A 0 0 4 [2] .gnu.hash GNU_HASH 00000000000001f0 000001f0 0000000000000034 0000000000000000 A 3 0 8 [3] .dynsym DYNSYM 0000000000000228 00000228 00000000000000a8 0000000000000018 A 4 2 8 [4] .dynstr STRTAB 00000000000002d0 000002d0 000000000000003e 0000000000000000 A 0 0 1 [5] .gnu.version VERSYM 000000000000030e 0000030e 000000000000000e 0000000000000002 A 3 0 2 [6] .gnu.version_r VERNEED 0000000000000320 00000320 0000000000000020 0000000000000000 A 4 1 8 [7] .rela.plt RELA 0000000000000340

```
00000470
       00000000000000f0
0000000000000018   A       3
0     8
  [ 8] .init
PROGBITS         0000000000000560
00000560
       000000000000001a
0000000000000000  AX       0
0     4
  [ 9] .plt
PROGBITS         0000000000000580
00000580
       0000000000000010
0000000000000010  AX       0
0     16
  [10] .plt.got
PROGBITS         0000000000000590
00000590
       0000000000000010
0000000000000000  AX       0
0     8
  [11] .text
PROGBITS         00000000000005a0
000005a0
       000000000000012e
0000000000000000  AX       0
0     16
  [12] .fini
PROGBITS         00000000000006d0
000006d0
       0000000000000009
0000000000000000  AX       0
0     4
  [13] .rodata
PROGBITS         00000000000006d9
000006d9
       000000000000000e
0000000000000000   A       0
0     1
  [14] .eh_frame_hdr
PROGBITS         00000000000006e8
000006e8
       000000000000001c
0000000000000000   A       0
0     4
  [15] .eh_frame
PROGBITS         0000000000000708
00000708
       0000000000000064
0000000000000000   A       0
0     8
  [16] .init_array
INIT_ARRAY       0000000000200e20
00000e20
       0000000000000008
0000000000000000  WA       0
0     8
  [17] .fini_array
FINI_ARRAY       0000000000200e28
00000e28
       0000000000000008
0000000000000000  WA       0
0     8
  [18] .jcr
PROGBITS         0000000000200e30
00000e30
       0000000000000008
0000000000000000  WA       0
0     8
  [19] .dynamic
DYNAMIC          0000000000200e38
00000e38
       00000000000001a0
0000000000000010  WA       4
0     8
  [20] .got
PROGBITS         0000000000200fd8
00000fd8
       0000000000000028
0000000000000008  WA       0
0     8
  [21] .got.plt
PROGBITS         0000000000201000
0000000000000470  00000470
       00000000000000c0
0000000000000018   A       3
0     8
  [ 8] .rela.plt
RELA
0000000000000530  00000530
       0000000000000018
0000000000000018  AI       3
22     8
  [ 9] .init
PROGBITS
0000000000000548  00000548
       000000000000001a
0000000000000000  AX       0
0     4
  [10] .plt
PROGBITS
0000000000000570  00000570
       0000000000000020
0000000000000010  AX       0
0     16
  [11] .plt.got
PROGBITS
0000000000000590  00000590
       0000000000000010
0000000000000000  AX       0
0     8
  [12] .text
PROGBITS
00000000000005a0  000005a0
       0000000000000124
0000000000000000  AX       0
0     16
  [13] .fini
PROGBITS
00000000000006c4  000006c4
       0000000000000009
0000000000000000  AX       0
0     4
  [14] .rodata
PROGBITS
00000000000006cd  000006cd
       000000000000000e
0000000000000000   A       0
0     1
  [15] .eh_frame_hdr
PROGBITS
00000000000006dc  000006dc
       000000000000001c
0000000000000000   A       0
0     4
  [16] .eh_frame
PROGBITS
00000000000006f8  000006f8
       0000000000000064
0000000000000000   A       0
0     8
  [17] .init_array
INIT_ARRAY
0000000000200e00  00000e00
       0000000000000008
0000000000000000  WA       0
0     8
  [18] .fini_array
FINI_ARRAY
0000000000200e08  00000e08
       0000000000000008
0000000000000000  WA       0
0     8
  [19] .jcr
PROGBITS
0000000000200e10  00000e10
       0000000000000008
0000000000000000  WA       0
0     8
  [20] .dynamic
DYNAMIC
0000000000200e18  00000e18
       00000000000001c0
0000000000000010  WA       4
0     8
  [21] .got
PROGBITS
00000340
       0000000000000018
0000000000000018  AI       3
14     8
  [ 8] .plt
PROGBITS         0000000000000360
00000360
       0000000000000020
0000000000000010  AX       0
0     16
  [ 9] .text
PROGBITS         0000000000000380
00000380
       0000000000000024
0000000000000000  AX       0
0     1
  [10] .rodata
PROGBITS         00000000000003a4
000003a4
       000000000000000e
0000000000000000   A       0
0     1
  [11] .eh_frame_hdr
PROGBITS         00000000000003b4
000003b4
       000000000000001c
0000000000000000   A       0
0     4
  [12] .eh_frame
PROGBITS         00000000000003d0
000003d0
       0000000000000060
0000000000000000   A       0
0     8
  [13] .dynamic
DYNAMIC          0000000000200ed0
00000ed0
       0000000000000130
0000000000000010  WA       4
0     8
  [14] .got.plt
PROGBITS         0000000000201000
00001000
       0000000000000020
0000000000000008  WA       0
0     8
  [15] .comment
PROGBITS         0000000000000000
00001020
       0000000000000034
0000000000000001  MS       0
0     1
  [16] .shstrtab
STRTAB           0000000000000000
00001339
       00000000000000af
0000000000000000           0
0     1
  [17] .symtab
SYMTAB           0000000000000000
00001058
       0000000000000270
0000000000000018          18
21     8
  [18] .strtab
STRTAB           0000000000000000
000012c8
       0000000000000071
0000000000000000           0
0     1
Key to Flags:
  W (write), A (alloc), X (execute),
M (merge), S (strings), l (large)
  I (info), L (link order), G
(group), T (TLS), E (exclude), x
(unknown)
  O (extra OS processing required) o
(OS specific), p (processor specific)
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
```

```
00001000
       0000000000000018
0000000000000008  WA       0
0     8
  [22] .data
PROGBITS         0000000000201018
00001018
       0000000000000008
0000000000000000  WA       0
0     8
  [23] .bss
NOBITS           0000000000201020
00001020
       0000000000000008
0000000000000000  WA       0
0     1
  [24] .comment
PROGBITS         0000000000000000
00001020
       0000000000000034
0000000000000001  MS       0
0     1
  [25] .shstrtab
STRTAB           0000000000000000
00001761
       00000000000000ec
0000000000000000           0
0     1
  [26] .symtab
SYMTAB           0000000000000000
00001058
       0000000000000540
0000000000000018          27
44     8
  [27] .strtab
STRTAB           0000000000000000
00001598
       00000000000001c9
0000000000000000           0
0     1
Key to Flags:
  W (write), A (alloc), X
(execute), M (merge), S (strings),
l (large)
  I (info), L (link order), G
(group), T (TLS), E (exclude), x
(unknown)
  O (extra OS processing required)
o (OS specific), p (processor
specific)
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
```

```
0000000000200fd8  00000fd8
       0000000000000028
0000000000000008  WA       0
0     8
  [22] .got.plt
PROGBITS
0000000000201000  00001000
       0000000000000020
0000000000000008  WA       0
0     8
  [23] .data
PROGBITS
0000000000201020  00001020
       0000000000000008
0000000000000000  WA       0
0     8
  [24] .bss
NOBITS
0000000000201028  00001028
       0000000000000008
0000000000000000  WA       0
0     1
  [25] .comment
PROGBITS
0000000000000000  00001028
       0000000000000034
0000000000000001  MS       0
0     1
  [26] .shstrtab
STRTAB
0000000000000000  00001781
       00000000000000f6
0000000000000000           0
0     1
  [27] .symtab
SYMTAB
0000000000000000  00001060
       0000000000000558
0000000000000018          28
45     8
  [28] .strtab
STRTAB
0000000000000000  000015b8
       00000000000001c9
0000000000000000           0
0     1
Key to Flags:
  W (write), A (alloc), X
(execute), M (merge), S
(strings), l (large)
  I (info), L (link order), G
(group), T (TLS), E (exclude), x
(unknown)
  O (extra OS processing
required) o (OS specific), p
(processor specific)
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
```

Compare files(Non-PIC vs PIC vs NoStart) - Dynamic section

- **다음과 같이 PIC가 적용되 파일과 적용되지 않은 파일이 다릅니다.**
  - PIC가 적용되지 않은 파일에는 TEXTREL 섹션이 존재하며, PLTRELSZ, PLTREL, JMPREL 섹션은 존재하지 않습니다.
  - PIC가 적용된 파일에는 PLTRELSZ, PLTREL, JMPREL 섹션이 존재하며, TEXTREL 섹션은 존재하지 않습니다.
  - PIC와 nostartfiles 옵션이 적용된 파일에는 PLTRELSZ, PLTREL, JMPREL 섹션이 존재하며, INIT, FINI, INIT_ARRAY, INIT_ARRAYSZ, FINI_ARRAY, FINI_ARRAYSZ, RELA, RELASZ, RELAENT, RELACOUNT 섹션은 존재하지 않습니다.

Check for Dynamic section

NonPIC

```
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
readelf -d libNonPIC.so

Dynamic section at offset 0xe38
contains 22 entries:
  Tag
Type                         Name
/Value
 0x0000000000000001
(NEEDED)             Shared
library: [libc.so.6]
 0x000000000000000c
(INIT)               0x560
 0x000000000000000d
(FINI)               0x6d0
 0x0000000000000019
(INIT_ARRAY)         0x200e20
 0x000000000000001b
(INIT_ARRAYSZ)       8 (bytes)
 0x000000000000001a
(FINI_ARRAY)         0x200e28
 0x000000000000001c
(FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5
(GNU_HASH)           0x1f0
 0x0000000000000005
(STRTAB)             0x380
 0x0000000000000006
(SYMTAB)             0x230
 0x000000000000000a
(STRSZ)              178 (bytes)
 0x000000000000000b
(SYMENT)             24 (bytes)
 0x0000000000000003
(PLTGOT)             0x201000
 0x0000000000000007
(RELA)               0x470
 0x0000000000000008
(RELASZ)             240 (bytes)
 0x0000000000000009
(RELAENT)            24 (bytes)
 0x0000000000000016
(TEXTREL)            0x0
 0x000000006fffffe
(VERNEED)            0x450
 0x000000006fffffff
(VERNEEDNUM)         1
 0x000000006ffffff0
(VERSYM)             0x432
 0x000000006ffffff9
(RELACOUNT)          4
 0x0000000000000000
(NULL)               0x0
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
```

PIC

```
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
readelf -d libPIC.so

Dynamic section at offset 0xe18
contains 24 entries:
  Tag
Type                         Name
/Value
 0x0000000000000001
(NEEDED)             Shared
library: [libc.so.6]
 0x000000000000000c
(INIT)               0x548
 0x000000000000000d
(FINI)               0x6c4
 0x0000000000000019
(INIT_ARRAY)         0x200e00
 0x000000000000001b
(INIT_ARRAYSZ)       8 (bytes)
 0x000000000000001a
(FINI_ARRAY)         0x200e08
 0x000000000000001c
(FINI_ARRAYSZ)       8 (bytes)
 0x000000006ffffef5
(GNU_HASH)           0x1f0
 0x0000000000000005
(STRTAB)             0x380
 0x0000000000000006
(SYMTAB)             0x230
 0x000000000000000a
(STRSZ)              178 (bytes)
 0x000000000000000b
(SYMENT)             24 (bytes)
 0x0000000000000003
(PLTGOT)             0x201000
 0x0000000000000002
(PLTRELSZ)           24 (bytes)
 0x0000000000000014
(PLTREL)             RELA
 0x0000000000000017
(JMPREL)             0x530
 0x0000000000000007
(RELA)               0x470
 0x0000000000000008
(RELASZ)             192 (bytes)
 0x0000000000000009
(RELAENT)            24 (bytes)
 0x000000006fffffe
(VERNEED)            0x450
 0x000000006fffffff
(VERNEEDNUM)         1
 0x000000006ffffff0
(VERSYM)             0x432
 0x000000006ffffff9
(RELACOUNT)          3
 0x0000000000000000
(NULL)               0x0
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
```

NoStartPIC

```
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$ readelf -
d libNoStartPIC.so

Dynamic section at offset 0xed0
contains 14 entries:
  Tag
Type                         Name
/Value
 0x0000000000000001
(NEEDED)             Shared library:
[libc.so.6]
 0x000000006ffffef5
(GNU_HASH)           0x1f0
 0x0000000000000005
(STRTAB)             0x2d0
 0x0000000000000006
(SYMTAB)             0x228
 0x000000000000000a
(STRSZ)              62 (bytes)
 0x000000000000000b
(SYMENT)             24 (bytes)
 0x0000000000000003
(PLTGOT)             0x201000
 0x0000000000000002
(PLTRELSZ)           24 (bytes)
 0x0000000000000014
(PLTREL)             RELA
 0x0000000000000017
(JMPREL)             0x340
 0x000000006fffffe
(VERNEED)            0x320
 0x000000006fffffff
(VERNEEDNUM)         1
 0x000000006ffffff0
(VERSYM)             0x30e
 0x0000000000000000
(NULL)               0x0
lazenca0x0@ubuntu:~/Documents
/Definition/protection/PIC$
```

- **여기서 중요한 내용은 또 있습니다. RELA, RELASZ, RELAENT, RELACOUNT 입니다.**
- **각 바이너리는 다음과 같은 재배치 정보를 포함하고 있습니다.**
  - PIC가 적용되지 않은 라이브러리의 경우 재배치가 필요합니다.
  - PIC가 적용된 라이브러리의 경우도 재배치가 필요합니다.
  - 하지만 -nostartfiles 옵션이 적용된 파일의 경우 재배치가 필요없습니다.

About relocation information included in the file

	NonPIC	PIC	NoStartPIC
RELA	0x470	0x470	X
RELASZ	240	192	X
RELAENT	24	24	X
RELACOUNT	4	3	X

해당 섹션들은 재배치와 관련된 섹션입니다.

- RELA : 상대주소 재배치 테이블 주소
- RELASZ : 상대주소 재배치 테이블 크기
- RELAENT : 상대 주소 재배치 엔트리 크기
- RELACOUNT : 재배치 횟수

Compare files(Non-PIC vs PIC) - Code

NonPIC

- **다음과 같이 PIC가 적용되지 않은 바이너리의 경우 함수를 호출 할 때 rdx 레지스터에 저장된 주소를 호출합니다.**

assembler code for function lazenca

```
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gdb -q ./libNonPIC.so
Reading symbols from ./libNonPIC.so...(no debugging symbols found)...done.
gdb-peda$ disassemble lazenca
Dump of assembler code for function lazenca:
   0x00000000000006a0 <+0>:     push   rbp
   0x00000000000006a1 <+1>:     mov    rbp,rsp
   0x00000000000006a4 <+4>:     sub    rsp,0x10
   0x00000000000006a8 <+8>:     mov    DWORD PTR [rbp-0x4],edi
   0x00000000000006ab <+11>:     mov    eax,DWORD PTR [rbp-0x4]
   0x00000000000006ae <+14>:     mov    esi,eax
   0x00000000000006b0 <+16>:     movabs rdi,0x6d9
   0x00000000000006ba <+26>:     mov    eax,0x0
   0x00000000000006bf <+31>:     movabs rdx,0x0
   0x00000000000006c9 <+41>:     call   rdx
   0x00000000000006cb <+43>:     nop
   0x00000000000006cc <+44>:     leave
   0x00000000000006cd <+45>:     ret
End of assembler dump.
gdb-peda$ info file
Symbols from "/home/lazenca0x0/Documents/Definition/protection/PIC/libNonPIC.so".
Local exec file:
        `/home/lazenca0x0/Documents/Definition/protection/PIC/libNonPIC.so', file type elf64-x86-64.
        Entry point: 0x5a0
        0x00000000000001c8 - 0x00000000000001ec is .note.gnu.build-id
        0x00000000000001f0 - 0x000000000000022c is .gnu.hash
        0x0000000000000230 - 0x0000000000000380 is .dynsym
        0x0000000000000380 - 0x0000000000000432 is .dynstr
        0x0000000000000432 - 0x000000000000044e is .gnu.version
        0x0000000000000450 - 0x0000000000000470 is .gnu.version_r
        0x0000000000000470 - 0x0000000000000560 is .rela.dyn
        0x0000000000000560 - 0x000000000000057a is .init
        0x0000000000000580 - 0x0000000000000590 is .plt
        0x0000000000000590 - 0x00000000000005a0 is .plt.got
        0x00000000000005a0 - 0x00000000000006ce is .text
        0x00000000000006d0 - 0x00000000000006d9 is .fini
        0x00000000000006d9 - 0x00000000000006e7 is .rodata
        0x00000000000006e8 - 0x0000000000000704 is .eh_frame_hdr
        0x0000000000000708 - 0x000000000000076c is .eh_frame
        0x0000000000200e20 - 0x0000000000200e28 is .init_array
        0x0000000000200e28 - 0x0000000000200e30 is .fini_array
        0x0000000000200e30 - 0x0000000000200e38 is .jcr
        0x0000000000200e38 - 0x0000000000200fd8 is .dynamic
        0x0000000000200fd8 - 0x0000000000201000 is .got
        0x0000000000201000 - 0x0000000000201018 is .got.plt
        0x0000000000201018 - 0x0000000000201020 is .data
        0x0000000000201020 - 0x0000000000201028 is .bss
gdb-peda$ x/s 0x6d9
0x6d9:        "Lazenca.0x%d\n"
gdb-peda$
```

- **다음과 같이 디버깅을 통해 함수 호출을 분석할 수 있습니다.**
  - main 함수는 lazenca 함수를 호출하기 위해 0x400570(lazenca@plt)영역을 호출합니다.
  - 0x400699 영역에 Break point를 설정 후 프로그램을 실행합니다.
    - lazenca 함수의 실제 주소가 0x601020영역에 재배치됩니다.
  - 공유 라이브러리가 프로그램에 로드되어 lazenca 함수를 Disassemble 할 수 있습니다.
  - rdx 레지스터에 0x7ffff78608000이 저장되고, 호출됩니다.
  - 0x7ffff7860800 영역은 "/lib/x86_64-linux-gnu/libc.so.6"의 .text 영역 입니다. (0x7ffff782a8b0 - 0x7ffff797dac4)

Function call analysis

```
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gdb -q ./test
Reading symbols from ./test...(no debugging symbols found)...done.
gdb-peda$ disassemble main
Dump of assembler code for function main:
   0x0000000000400686 <+0>:     push   rbp
```

```
   0x0000000000400687 <+1>:     mov    rbp,rsp
   0x000000000040068a <+4>:     mov    esi,0xa
   0x000000000040068f <+9>:     mov    edi,0xa
   0x0000000000400694 <+14>:     mov    eax,0x0
   0x0000000000400699 <+19>:     call   0x400570 <lazenca@plt>
   0x000000000040069e <+24>:     nop
   0x000000000040069f <+25>:     pop    rbp
   0x00000000004006a0 <+26>:     ret
End of assembler dump.
gdb-peda$ disassemble lazenca
Dump of assembler code for function lazenca@plt:
   0x0000000000400570 <+0>:     jmp    QWORD PTR [rip+0x200aaa]        # 0x601020
   0x0000000000400576 <+6>:     push   0x1
   0x000000000040057b <+11>:     jmp    0x400550
End of assembler dump.
gdb-peda$ b *0x0000000000400699
Breakpoint 1 at 0x400699
gdb-peda$ r
Starting program: /home/lazenca0x0/Documents/Definition/protection/PIC/test


Breakpoint 1, 0x0000000000400699 in main ()
gdb-peda$ disassemble lazenca
Dump of assembler code for function lazenca:
   0x00007ffff7bd56a0 <+0>:     push   rbp
   0x00007ffff7bd56a1 <+1>:     mov    rbp,rsp
   0x00007ffff7bd56a4 <+4>:     sub    rsp,0x10
   0x00007ffff7bd56a8 <+8>:     mov    DWORD PTR [rbp-0x4],edi
   0x00007ffff7bd56ab <+11>:     mov    eax,DWORD PTR [rbp-0x4]
   0x00007ffff7bd56ae <+14>:     mov    esi,eax
   0x00007ffff7bd56b0 <+16>:     movabs rdi,0x7ffff7bd56d9
   0x00007ffff7bd56ba <+26>:     mov    eax,0x0
   0x00007ffff7bd56bf <+31>:     movabs rdx,0x7ffff7860800
   0x00007ffff7bd56c9 <+41>:     call   rdx
   0x00007ffff7bd56cb <+43>:     nop
   0x00007ffff7bd56cc <+44>:     leave
   0x00007ffff7bd56cd <+45>:     ret
End of assembler dump.
gdb-peda$ x/i 0x7ffff7860800
   0x7ffff7860800 <__printf>:        sub    rsp,0xd8
gdb-peda$ info file
Symbols from "/home/lazenca0x0/Documents/Definition/protection/PIC/test".
Native process:
        Using the running image of child process 4525.
        While running this, GDB does not access memory from...
Local exec file:
        `/home/lazenca0x0/Documents/Definition/protection/PIC/test', file type elf64-x86-64.
        Entry point: 0x400590
        0x0000000000400238 - 0x0000000000400254 is .interp
        0x0000000000400254 - 0x0000000000400274 is .note.ABI-tag
        0x0000000000400274 - 0x0000000000400298 is .note.gnu.build-id
        0x0000000000400298 - 0x00000000004002d0 is .gnu.hash
        0x00000000004002d0 - 0x00000000004003f0 is .dynsym
        0x00000000004003f0 - 0x00000000004004ab is .dynstr
        0x00000000004004ac - 0x00000000004004c4 is .gnu.version
        0x00000000004004c8 - 0x00000000004004e8 is .gnu.version_r
        0x00000000004004e8 - 0x0000000000400500 is .rela.dyn
        0x0000000000400500 - 0x0000000000400530 is .rela.plt
        0x0000000000400530 - 0x000000000040054a is .init
        0x0000000000400550 - 0x0000000000400580 is .plt
        0x0000000000400580 - 0x0000000000400588 is .plt.got
        0x0000000000400590 - 0x0000000000400722 is .text
        0x0000000000400724 - 0x000000000040072d is .fini
        0x0000000000400730 - 0x0000000000400734 is .rodata
        0x0000000000400734 - 0x0000000000400768 is .eh_frame_hdr
        0x0000000000400768 - 0x000000000040085c is .eh_frame
        0x0000000000600e00 - 0x0000000000600e08 is .init_array
        0x0000000000600e08 - 0x0000000000600e10 is .fini_array
        0x0000000000600e10 - 0x0000000000600e18 is .jcr
        0x0000000000600e18 - 0x0000000000600ff8 is .dynamic
        0x0000000000600ff8 - 0x0000000000601000 is .got
```

```
        0x0000000000601000 - 0x0000000000601028 is .got.plt
        0x0000000000601028 - 0x0000000000601038 is .data
        0x0000000000601038 - 0x0000000000601040 is .bss
        0x00007ffff7dd71c8 - 0x00007ffff7dd71ec is .note.gnu.build-id in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd71f0 - 0x00007ffff7dd72b0 is .hash in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd72b0 - 0x00007ffff7dd7390 is .gnu.hash in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7390 - 0x00007ffff7dd7648 is .dynsym in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7648 - 0x00007ffff7dd77ef is .dynstr in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd77f0 - 0x00007ffff7dd782a is .gnu.version in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7830 - 0x00007ffff7dd78d4 is .gnu.version_d in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd78d8 - 0x00007ffff7dd79f8 is .rela.dyn in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd79f8 - 0x00007ffff7dd7a58 is .rela.plt in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7a60 - 0x00007ffff7dd7ab0 is .plt in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7ab0 - 0x00007ffff7dd7ab8 is .plt.got in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7ac0 - 0x00007ffff7df5810 is .text in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df5820 - 0x00007ffff7df98e0 is .rodata in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df98e0 - 0x00007ffff7df98e1 is .stapsdt.base in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df98e4 - 0x00007ffff7df9f20 is .eh_frame_hdr in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df9f20 - 0x00007ffff7dfc3b8 is .eh_frame in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffcbc0 - 0x00007ffff7ffce6c is .data.rel.ro in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffce70 - 0x00007ffff7ffcfe0 is .dynamic in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffcfe0 - 0x00007ffff7ffcff0 is .got in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffd000 - 0x00007ffff7ffd038 is .got.plt in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffd040 - 0x00007ffff7ffdfc0 is .data in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffdfc0 - 0x00007ffff7ffe168 is .bss in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffa120 - 0x00007ffff7ffa160 is .hash in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa160 - 0x00007ffff7ffa1a8 is .gnu.hash in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa1a8 - 0x00007ffff7ffa2b0 is .dynsym in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa2b0 - 0x00007ffff7ffa30e is .dynstr in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa30e - 0x00007ffff7ffa324 is .gnu.version in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa328 - 0x00007ffff7ffa360 is .gnu.version_d in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa360 - 0x00007ffff7ffa470 is .dynamic in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa470 - 0x00007ffff7ffa7f8 is .rodata in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa7f8 - 0x00007ffff7ffa834 is .note in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa834 - 0x00007ffff7ffa870 is .eh_frame_hdr in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa870 - 0x00007ffff7ffa998 is .eh_frame in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa9a0 - 0x00007ffff7ffaee9 is .text in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffaee9 - 0x00007ffff7ffaf1d is .altinstructions in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffaf1d - 0x00007ffff7ffaf29 is .altinstr_replacement in system-supplied DSO at
0x7ffff7ffa000
        0x00007ffff7bd51c8 - 0x00007ffff7bd51ec is .note.gnu.build-id in /home/lazenca0x0/Documents/Definition
/protection/PIC/libNonPIC.so
        0x00007ffff7bd51f0 - 0x00007ffff7bd522c is .gnu.hash in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7bd5230 - 0x00007ffff7bd5380 is .dynsym in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7bd5380 - 0x00007ffff7bd5432 is .dynstr in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7bd5432 - 0x00007ffff7bd544e is .gnu.version in /home/lazenca0x0/Documents/Definition
/protection/PIC/libNonPIC.so
        0x00007ffff7bd5450 - 0x00007ffff7bd5470 is .gnu.version_r in /home/lazenca0x0/Documents/Definition
/protection/PIC/libNonPIC.so
        0x00007ffff7bd5470 - 0x00007ffff7bd5560 is .rela.dyn in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7bd5560 - 0x00007ffff7bd557a is .init in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7bd5580 - 0x00007ffff7bd5590 is .plt in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7bd5590 - 0x00007ffff7bd55a0 is .plt.got in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7bd55a0 - 0x00007ffff7bd56ce is .text in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7bd56d0 - 0x00007ffff7bd56d9 is .fini in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7bd56d9 - 0x00007ffff7bd56e7 is .rodata in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7bd56e8 - 0x00007ffff7bd5704 is .eh_frame_hdr in /home/lazenca0x0/Documents/Definition
/protection/PIC/libNonPIC.so
        0x00007ffff7bd5708 - 0x00007ffff7bd576c is .eh_frame in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7dd5e20 - 0x00007ffff7dd5e28 is .init_array in /home/lazenca0x0/Documents/Definition
```

```
/protection/PIC/libNonPIC.so
        0x00007ffff7dd5e28 - 0x00007ffff7dd5e30 is .fini_array in /home/lazenca0x0/Documents/Definition
/protection/PIC/libNonPIC.so
        0x00007ffff7dd5e30 - 0x00007ffff7dd5e38 is .jcr in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7dd5e38 - 0x00007ffff7dd5fd8 is .dynamic in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7dd5fd8 - 0x00007ffff7dd6000 is .got in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7dd6000 - 0x00007ffff7dd6018 is .got.plt in /home/lazenca0x0/Documents/Definition/protection
/PIC/libNonPIC.so
        0x00007ffff7dd6018 - 0x00007ffff7dd6020 is .data in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff7dd6020 - 0x00007ffff7dd6028 is .bss in /home/lazenca0x0/Documents/Definition/protection/PIC
/libNonPIC.so
        0x00007ffff780b270 - 0x00007ffff780b294 is .note.gnu.build-id in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff780b294 - 0x00007ffff780b2b4 is .note.ABI-tag in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff780b2b8 - 0x00007ffff780ed80 is .gnu.hash in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff780ed80 - 0x00007ffff781bff8 is .dynsym in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff781bff8 - 0x00007ffff78219d7 is .dynstr in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff78219d8 - 0x00007ffff7822b62 is .gnu.version in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7822b68 - 0x00007ffff7822edc is .gnu.version_d in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7822ee0 - 0x00007ffff7822f10 is .gnu.version_r in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7822f10 - 0x00007ffff782a680 is .rela.dyn in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a680 - 0x00007ffff782a7b8 is .rela.plt in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a7c0 - 0x00007ffff782a8a0 is .plt in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a8a0 - 0x00007ffff782a8b0 is .plt.got in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a8b0 - 0x00007ffff797dac4 is .text in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff797dad0 - 0x00007ffff797ffed is __libc_freeres_fn in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff797fff0 - 0x00007ffff79802b2 is __libc_thread_freeres_fn in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79802c0 - 0x00007ffff79a1610 is .rodata in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a1610 - 0x00007ffff79a1611 is .stapsdt.base in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a1620 - 0x00007ffff79a163c is .interp in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a163c - 0x00007ffff79a6af8 is .eh_frame_hdr in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a6af8 - 0x00007ffff79c738c is .eh_frame in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79c738c - 0x00007ffff79c77cd is .gcc_except_table in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79c77d0 - 0x00007ffff79caad0 is .hash in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7c0 - 0x00007ffff7bcb7d0 is .tdata in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7d0 - 0x00007ffff7bcb838 is .tbss in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7d0 - 0x00007ffff7bcb7e0 is .init_array in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7e0 - 0x00007ffff7bcb8d8 is __libc_subfreeres in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb8d8 - 0x00007ffff7bcb8e0 is __libc_atexit in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb8e0 - 0x00007ffff7bcb900 is __libc_thread_subfreeres in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb900 - 0x00007ffff7bceba0 is .data.rel.ro in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bceba0 - 0x00007ffff7bced80 is .dynamic in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bced80 - 0x00007ffff7bceff0 is .got in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcf000 - 0x00007ffff7bcf080 is .got.plt in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcf080 - 0x00007ffff7bd0720 is .data in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bd0720 - 0x00007ffff7bd49a0 is .bss in /lib/x86_64-linux-gnu/libc.so.6
gdb-peda$
```

PIC

- 다음과 같이 PIC가 적용된 바이너리는 함수를 호출 할 때 .plt 영역의 해당 함수의 주소를 호출합니다.

assembler code for function lazenca

```
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gdb -q ./libNoStartPIC.so
Reading symbols from ./libNoStartPIC.so...(no debugging symbols found)...done.
gdb-peda$ disassemble lazenca
Dump of assembler code for function lazenca:
   0x0000000000000380 <+0>:     push   rbp
   0x0000000000000381 <+1>:     mov    rbp,rsp
   0x0000000000000384 <+4>:     sub    rsp,0x10
   0x0000000000000388 <+8>:     mov    DWORD PTR [rbp-0x4],edi
   0x000000000000038b <+11>:     mov    eax,DWORD PTR [rbp-0x4]
   0x000000000000038e <+14>:     mov    esi,eax
   0x0000000000000390 <+16>:     lea    rdi,[rip+0xd]        # 0x3a4
   0x0000000000000397 <+23>:     mov    eax,0x0
   0x000000000000039c <+28>:     call   0x370 <printf@plt>
   0x00000000000003a1 <+33>:     nop
   0x00000000000003a2 <+34>:     leave
   0x00000000000003a3 <+35>:     ret
End of assembler dump.
gdb-peda$ info file
Symbols from "/home/lazenca0x0/Documents/Definition/protection/PIC/libNoStartPIC.so".
Local exec file:
        `/home/lazenca0x0/Documents/Definition/protection/PIC/libNoStartPIC.so', file type elf64-x86-64.
        Entry point: 0x380
        0x00000000000001c8 - 0x00000000000001ec is .note.gnu.build-id
        0x00000000000001f0 - 0x0000000000000224 is .gnu.hash
        0x0000000000000228 - 0x00000000000002d0 is .dynsym
        0x00000000000002d0 - 0x000000000000030e is .dynstr
        0x000000000000030e - 0x000000000000031c is .gnu.version
        0x0000000000000320 - 0x0000000000000340 is .gnu.version_r
        0x0000000000000340 - 0x0000000000000358 is .rela.plt
        0x0000000000000360 - 0x0000000000000380 is .plt
        0x0000000000000380 - 0x00000000000003a4 is .text
        0x00000000000003a4 - 0x00000000000003b2 is .rodata
        0x00000000000003b4 - 0x00000000000003d0 is .eh_frame_hdr
        0x00000000000003d0 - 0x0000000000000430 is .eh_frame
        0x0000000000200ed0 - 0x0000000000201000 is .dynamic
        0x0000000000201000 - 0x0000000000201020 is .got.plt
gdb-peda$ x/s 0x3a4
0x3a4:        "Lazenca.0x%d\n"
gdb-peda$
```

- **다음과 같이 디버깅을 통해 함수 호출을 분석할 수 있습니다.**
  - main 함수는 lazenca 함수를 호출하기 위해 0x400570(lazenca@plt)영역을 호출합니다.
  - 0x400699 영역에 Break point를 설정 후 프로그램을 실행합니다.
    - lazenca 함수의 실제 주소가 0x601020영역에 재배치됩니다.
  - 공유 라이브러리가 프로그램에 로드되어 lazenca 함수를 Disassemble 할 수 있습니다.
  - lazenca 함수는 printf함수를 호출하기 위해 0x7ffff7bd5580 영역을 호출합니다.
  - 0x7ffff7bd5580 영역은 "/home/lazenca0x0/Documents/Definition/protection/PIC/libPIC.so"의 .plt 영역 입니다. (0x7ffff7bd5570 - 0x00007ffff7bd5590)

Function call analysis

```
lazenca0x0@ubuntu:~/Documents/Definition/protection/PIC$ gdb -q ./testPIC
Reading symbols from ./testPIC...(no debugging symbols found)...done.
gdb-peda$ disassemble main
Dump of assembler code for function main:
   0x0000000000400686 <+0>:     push   rbp
   0x0000000000400687 <+1>:     mov    rbp,rsp
   0x000000000040068a <+4>:     mov    esi,0xa
   0x000000000040068f <+9>:     mov    edi,0xa
   0x0000000000400694 <+14>:     mov    eax,0x0
   0x0000000000400699 <+19>:     call   0x400570 <lazenca@plt>
   0x000000000040069e <+24>:     nop
   0x000000000040069f <+25>:     pop    rbp
   0x00000000004006a0 <+26>:     ret
End of assembler dump.
```

```
gdb-peda$ disassemble lazenca
Dump of assembler code for function lazenca@plt:
   0x0000000000400570 <+0>:        jmp    QWORD PTR [rip+0x200aaa]        # 0x601020
   0x0000000000400576 <+6>:        push   0x1
   0x000000000040057b <+11>:        jmp    0x400550
End of assembler dump.
gdb-peda$ b *0x0000000000400699
Breakpoint 1 at 0x400699
gdb-peda$ r
Starting program: /home/lazenca0x0/Documents/Definition/protection/PIC/testPIC
Breakpoint 1, 0x0000000000400699 in main ()
gdb-peda$ disassemble lazenca
Dump of assembler code for function lazenca:
   0x00007ffff7bd56a0 <+0>:        push   rbp
   0x00007ffff7bd56a1 <+1>:        mov    rbp,rsp
   0x00007ffff7bd56a4 <+4>:        sub    rsp,0x10
   0x00007ffff7bd56a8 <+8>:        mov    DWORD PTR [rbp-0x4],edi
   0x00007ffff7bd56ab <+11>:        mov    eax,DWORD PTR [rbp-0x4]
   0x00007ffff7bd56ae <+14>:        mov    esi,eax
   0x00007ffff7bd56b0 <+16>:        lea    rdi,[rip+0x16]        # 0x7ffff7bd56cd
   0x00007ffff7bd56b7 <+23>:        mov    eax,0x0
   0x00007ffff7bd56bc <+28>:        call   0x7ffff7bd5580 <printf@plt>
   0x00007ffff7bd56c1 <+33>:        nop
   0x00007ffff7bd56c2 <+34>:        leave
   0x00007ffff7bd56c3 <+35>:        ret
End of assembler dump.
gdb-peda$ info file
Symbols from "/home/lazenca0x0/Documents/Definition/protection/PIC/testPIC".
Native process:
        Using the running image of child process 4632.
        While running this, GDB does not access memory from...
Local exec file:
        `/home/lazenca0x0/Documents/Definition/protection/PIC/testPIC', file type elf64-x86-64.
        Entry point: 0x400590
        0x0000000000400238 - 0x0000000000400254 is .interp
        0x0000000000400254 - 0x0000000000400274 is .note.ABI-tag
        0x0000000000400274 - 0x0000000000400298 is .note.gnu.build-id
        0x0000000000400298 - 0x00000000004002d0 is .gnu.hash
        0x00000000004002d0 - 0x00000000004003f0 is .dynsym
        0x00000000004003f0 - 0x00000000004004a8 is .dynstr
        0x00000000004004a8 - 0x00000000004004c0 is .gnu.version
        0x00000000004004c0 - 0x00000000004004e0 is .gnu.version_r
        0x00000000004004e0 - 0x00000000004004f8 is .rela.dyn
        0x00000000004004f8 - 0x0000000000400528 is .rela.plt
        0x0000000000400528 - 0x0000000000400542 is .init
        0x0000000000400550 - 0x0000000000400580 is .plt
        0x0000000000400580 - 0x0000000000400588 is .plt.got
        0x0000000000400590 - 0x0000000000400722 is .text
        0x0000000000400724 - 0x000000000040072d is .fini
        0x0000000000400730 - 0x0000000000400734 is .rodata
        0x0000000000400734 - 0x0000000000400768 is .eh_frame_hdr
        0x0000000000400768 - 0x000000000040085c is .eh_frame
        0x0000000000600e00 - 0x0000000000600e08 is .init_array
        0x0000000000600e08 - 0x0000000000600e10 is .fini_array
        0x0000000000600e10 - 0x0000000000600e18 is .jcr
        0x0000000000600e18 - 0x0000000000600ff8 is .dynamic
        0x0000000000600ff8 - 0x0000000000601000 is .got
        0x0000000000601000 - 0x0000000000601028 is .got.plt
        0x0000000000601028 - 0x0000000000601038 is .data
        0x0000000000601038 - 0x0000000000601040 is .bss
        0x00007ffff7dd71c8 - 0x00007ffff7dd71ec is .note.gnu.build-id in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd71f0 - 0x00007ffff7dd72b0 is .hash in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd72b0 - 0x00007ffff7dd7390 is .gnu.hash in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7390 - 0x00007ffff7dd7648 is .dynsym in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7648 - 0x00007ffff7dd77ef is .dynstr in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd77f0 - 0x00007ffff7dd782a is .gnu.version in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7830 - 0x00007ffff7dd78d4 is .gnu.version_d in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd78d8 - 0x00007ffff7dd79f8 is .rela.dyn in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd79f8 - 0x00007ffff7dd7a58 is .rela.plt in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7a60 - 0x00007ffff7dd7ab0 is .plt in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7dd7ab0 - 0x00007ffff7dd7ab8 is .plt.got in /lib64/ld-linux-x86-64.so.2
```

```
        0x00007ffff7dd7ac0 - 0x00007ffff7df5810 is .text in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df5820 - 0x00007ffff7df98e0 is .rodata in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df98e0 - 0x00007ffff7df98e1 is .stapsdt.base in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df98e4 - 0x00007ffff7df9f20 is .eh_frame_hdr in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7df9f20 - 0x00007ffff7dfc3b8 is .eh_frame in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffcbc0 - 0x00007ffff7ffce6c is .data.rel.ro in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffce70 - 0x00007ffff7ffcfe0 is .dynamic in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffcfe0 - 0x00007ffff7ffcff0 is .got in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffd000 - 0x00007ffff7ffd038 is .got.plt in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffd040 - 0x00007ffff7ffdfc0 is .data in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffdfc0 - 0x00007ffff7ffe168 is .bss in /lib64/ld-linux-x86-64.so.2
        0x00007ffff7ffa120 - 0x00007ffff7ffa160 is .hash in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa160 - 0x00007ffff7ffa1a8 is .gnu.hash in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa1a8 - 0x00007ffff7ffa2b0 is .dynsym in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa2b0 - 0x00007ffff7ffa30e is .dynstr in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa30e - 0x00007ffff7ffa324 is .gnu.version in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa328 - 0x00007ffff7ffa360 is .gnu.version_d in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa360 - 0x00007ffff7ffa470 is .dynamic in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa470 - 0x00007ffff7ffa7f8 is .rodata in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa7f8 - 0x00007ffff7ffa834 is .note in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa834 - 0x00007ffff7ffa870 is .eh_frame_hdr in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa870 - 0x00007ffff7ffa998 is .eh_frame in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffa9a0 - 0x00007ffff7ffaee9 is .text in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffaee9 - 0x00007ffff7ffaf1d is .altinstructions in system-supplied DSO at 0x7ffff7ffa000
        0x00007ffff7ffaf1d - 0x00007ffff7ffaf29 is .altinstr_replacement in system-supplied DSO at
0x7ffff7ffa000
        0x00007ffff7bd51c8 - 0x00007ffff7bd51ec is .note.gnu.build-id in /home/lazenca0x0/Documents/Definition
/protection/PIC/libPIC.so
        0x00007ffff7bd51f0 - 0x00007ffff7bd522c is .gnu.hash in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd5230 - 0x00007ffff7bd5380 is .dynsym in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd5380 - 0x00007ffff7bd5432 is .dynstr in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd5432 - 0x00007ffff7bd544e is .gnu.version in /home/lazenca0x0/Documents/Definition
/protection/PIC/libPIC.so
        0x00007ffff7bd5450 - 0x00007ffff7bd5470 is .gnu.version_r in /home/lazenca0x0/Documents/Definition
/protection/PIC/libPIC.so
        0x00007ffff7bd5470 - 0x00007ffff7bd5530 is .rela.dyn in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd5530 - 0x00007ffff7bd5548 is .rela.plt in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd5548 - 0x00007ffff7bd5562 is .init in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff7bd5570 - 0x00007ffff7bd5590 is .plt in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff7bd5590 - 0x00007ffff7bd55a0 is .plt.got in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd55a0 - 0x00007ffff7bd56c4 is .text in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff7bd56c4 - 0x00007ffff7bd56cd is .fini in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff7bd56cd - 0x00007ffff7bd56db is .rodata in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7bd56dc - 0x00007ffff7bd56f8 is .eh_frame_hdr in /home/lazenca0x0/Documents/Definition
/protection/PIC/libPIC.so
        0x00007ffff7bd56f8 - 0x00007ffff7bd575c is .eh_frame in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7dd5e00 - 0x00007ffff7dd5e08 is .init_array in /home/lazenca0x0/Documents/Definition
/protection/PIC/libPIC.so
        0x00007ffff7dd5e08 - 0x00007ffff7dd5e10 is .fini_array in /home/lazenca0x0/Documents/Definition
/protection/PIC/libPIC.so
        0x00007ffff7dd5e10 - 0x00007ffff7dd5e18 is .jcr in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff7dd5e18 - 0x00007ffff7dd5fd8 is .dynamic in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7dd5fd8 - 0x00007ffff7dd6000 is .got in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff7dd6000 - 0x00007ffff7dd6020 is .got.plt in /home/lazenca0x0/Documents/Definition/protection
/PIC/libPIC.so
        0x00007ffff7dd6020 - 0x00007ffff7dd6028 is .data in /home/lazenca0x0/Documents/Definition/protection/PIC
```

```
/libPIC.so
        0x00007ffff7dd6028 - 0x00007ffff7dd6030 is .bss in /home/lazenca0x0/Documents/Definition/protection/PIC
/libPIC.so
        0x00007ffff780b270 - 0x00007ffff780b294 is .note.gnu.build-id in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff780b294 - 0x00007ffff780b2b4 is .note.ABI-tag in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff780b2b8 - 0x00007ffff780ed80 is .gnu.hash in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff780ed80 - 0x00007ffff781bff8 is .dynsym in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff781bff8 - 0x00007ffff78219d7 is .dynstr in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff78219d8 - 0x00007ffff7822b62 is .gnu.version in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7822b68 - 0x00007ffff7822edc is .gnu.version_d in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7822ee0 - 0x00007ffff7822f10 is .gnu.version_r in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7822f10 - 0x00007ffff782a680 is .rela.dyn in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a680 - 0x00007ffff782a7b8 is .rela.plt in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a7c0 - 0x00007ffff782a8a0 is .plt in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a8a0 - 0x00007ffff782a8b0 is .plt.got in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff782a8b0 - 0x00007ffff797dac4 is .text in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff797dad0 - 0x00007ffff797ffed is __libc_freeres_fn in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff797fff0 - 0x00007ffff79802b2 is __libc_thread_freeres_fn in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79802c0 - 0x00007ffff79a1610 is .rodata in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a1610 - 0x00007ffff79a1611 is .stapsdt.base in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a1620 - 0x00007ffff79a163c is .interp in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a163c - 0x00007ffff79a6af8 is .eh_frame_hdr in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79a6af8 - 0x00007ffff79c738c is .eh_frame in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79c738c - 0x00007ffff79c77cd is .gcc_except_table in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff79c77d0 - 0x00007ffff79caad0 is .hash in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7c0 - 0x00007ffff7bcb7d0 is .tdata in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7d0 - 0x00007ffff7bcb838 is .tbss in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7d0 - 0x00007ffff7bcb7e0 is .init_array in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb7e0 - 0x00007ffff7bcb8d8 is __libc_subfreeres in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb8d8 - 0x00007ffff7bcb8e0 is __libc_atexit in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb8e0 - 0x00007ffff7bcb900 is __libc_thread_subfreeres in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcb900 - 0x00007ffff7bceba0 is .data.rel.ro in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bceba0 - 0x00007ffff7bced80 is .dynamic in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bced80 - 0x00007ffff7bceff0 is .got in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcf000 - 0x00007ffff7bcf080 is .got.plt in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bcf080 - 0x00007ffff7bd0720 is .data in /lib/x86_64-linux-gnu/libc.so.6
        0x00007ffff7bd0720 - 0x00007ffff7bd49a0 is .bss in /lib/x86_64-linux-gnu/libc.so.6
gdb-peda$
```

Related information

- N/a