

Problem 1

Read-only code segment

```
1  LOAD  off   0x00000000  vaddr  0x08048000  paddr  0x08048000  align 2**12
2          filesz  0x00000448  memsz  0x00000448  flags  r-x
```

Read/write data segment

```
3  LOAD  off   0x00000448  vaddr  0x08049448  paddr  0x08049448  align 2**12
4          filesz  0x000000e8  memsz  0x00000104  flags  rw-
```

The segment header indicates that the data segment occupies 0x104 bytes in memory. However, only the first 0xe8 bytes of these come from the sections of the executable file. What causes this discrepancy?

Problem 2

Express the difference between the procedure of static link and the procedure of dynamic link (with shared library). You can draw a picture to show that.

Problem 3

- 1) Draw a Linux run-time memory image to show the location of GOT, PLT and shared library.
- 2) Express the function of PLT and GOT. And how to use them?
- 3) When the GOT is generated, and when the items of it are relocated?(Two situations: PIC Data References and PIC Function Calls)

Problem 4

Suppose we have **main.c** and a shared library **foo.so**. In main.c, we called a function "void flag()" which is in the **foo.so**.

Complete the following Codes in **main.c** to call the **flag()**.

```
#include <stdio.h>
#include <stdlib.h>
#include <dlfcn.h>
```

```
Int main()
{
    // Your codes here.

    flag();

    return 0;
}
```