OS_Assignment1

Assign	
Property	
tag	homework
姓名	周鹏宇
学号	2019K8009929039

请在一个 posix 兼容的环境(unix、linux、windows cmd、mac 等)编译执行附件小程序，并试着分析每个变量所属的段(section)，可以用 `objdump` 等进行验证。

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

char *myname="Chen Mingyu";
char gdata[128];
char bdata[16] = {1,2,3,4};
main() {
  char * ldata[16];
  char * ddata;

  ddata = malloc(16);
  printf("gdata: %llX\nbdata:%llX\nldata:%llx\nddata:%llx\n",
    gdata,bdata,ldata,ddata);
  free(ddata);
}
```

本回答基于MacOS系统的运行结果

▼ 全局变量

- `char *`类指针`myname`位于__DATA, __data中（同时存在于内存和可执行文件）
- `char`类型数组`gdata`位于__BBS, __commen中(仅存在于内存，不存在于可执行文件)
- `char`类型数组`bdata`位于__DATA, __data中（同时存在于内存和可执行文件）

▼ 局部变量

- 数组指针`ladta`和指针`ddata`位于栈中，运行时分配内存空间

▼ malloc

- 函数 `malloc` 申请的内存位于堆中，运行时通过库函数分配内存空间

▼ 字符串常量

`"Chen Mingyu"` 和 `"gdata: %llX\nbdata:%llX\nldata:%llx\nddata:%llx\n"` 均作为只读数据存在于__DATA, ___cstring中，同时存在于运行时内存和可执行文件中。

验证分析如下：

```
Sections:
Idx Name            Size     VMA              Type
  0 __text          000000a0 0000000100003e80 TEXT
  1 __stubs         00000018 0000000100003f20 TEXT
  2 __stub_helper   00000038 0000000100003f38 TEXT
  3 __cstring       0000003a 0000000100003f70 DATA
  4 __unwind_info   00000048 0000000100003fac DATA
  5 __got           00000010 0000000100004000 DATA
  6 __la_symbol_ptr 00000020 0000000100008000 DATA
  7 __data          00000030 0000000100008020 DATA
  8 __common        00000080 0000000100008050 BSS
```

```
Contents of section __text:
 100003e80 554889e5 4881ecb0 00000048 8b056e01  UH..H......H..n.
 100003e90 0000488b 00488945 f8bf1000 0000e889  ..H..H.E........
 100003ea0 00000048 8d35a641 0000488d 0d8f4100  ...H.5.A..H...A.
 100003eb0 00488d95 70ffffff 48898568 ffffff4c  .H..p...H..h...L
 100003ec0 8b8568ff ffff488d 3daf0000 00488995  ..h...H.=....H..
 100003ed0 60ffffff 4889ca48 8b8d60ff ffffb000  `...H..H..`.....
 100003ee0 e84d0000 00488bbd 68ffffff 89855cff  .M...H..h.....\.
 100003ef0 ffffe82f 00000048 8b0d0201 0000488b  .../...H......H.
 100003f00 09488b55 f84839d1 0f850b00 000031c0  .H.U.H9.......1.
 100003f10 4881c4b0 0000005d c3e80200 00000f0b  H......]........
Contents of section __stubs:
 100003f20 ff25da40 0000ff25 dc400000 ff25de40  .%.@...%.@...%.@
 100003f30 0000ff25 e0400000                    ...%.@..
Contents of section __stub_helper:
 100003f38 4c8d1de1 40000041 53ff25c1 00000090  L...@..AS.%.....
 100003f48 68000000 00e9e6ff ffff6818 000000e9  h.........h.....
 100003f58 dcffffff 68240000 00e9d2ff ffff6832  ....h$........h2
 100003f68 000000e9 c8ffffff                    ........
Contents of section __cstring:
 100003f70 4368656e 204d696e 67797500 67646174  Chen Mingyu.gdat
 100003f80 613a2025 6c6c580a 62646174 613a256c  a: %llX.bdata:%l
 100003f90 6c580a6c 64617461 3a256c6c 780a6464  lX.ldata:%llx.dd
 100003fa0 6174613a 256c6c78 0a00               ata:%llx..
Contents of section __unwind_info:
 100003fac 01000000 1c000000 00000000 1c000000  ................
 100003fbc 00000000 1c000000 02000000 803e0000  .............>..
 100003fcc 34000000 34000000 213f0000 00000000  4...4...!?......
 100003fdc 34000000 03000000 0c000100 10000100  4...............
 100003fec 00000000 00000001                    ........
```

```
Contents of section __got:
 100004000 00000000 00000000 00000000 00000000  ................
Contents of section __la_symbol_ptr:
 100008000 483f0000 01000000 523f0000 01000000  H?......R?......
 100008010 5c3f0000 01000000 663f0000 01000000  \?......f?......
Contents of section __data:
 100008020 00000000 00000000 00000000 00000000  ................
 100008030 703f0000 01000000 00000000 00000000  p?..............
 100008040 01020304 00000000 00000000 00000000  ................
Contents of section __common:
<skipping contents of bss section at [100008050, 1000080d0)>
```

其中

- `100003f70-100003f75` 处为 `"Chen Mingyu"`
- `100003f76-100003faa` 处为 `"gdata: %llX\nbdata:%llX\nldata:%llx\nddata:%llx\n"`
- `100008030-100008037` 为指针 `myname`
- `100008040-10000804f` 为数组 `bdata`