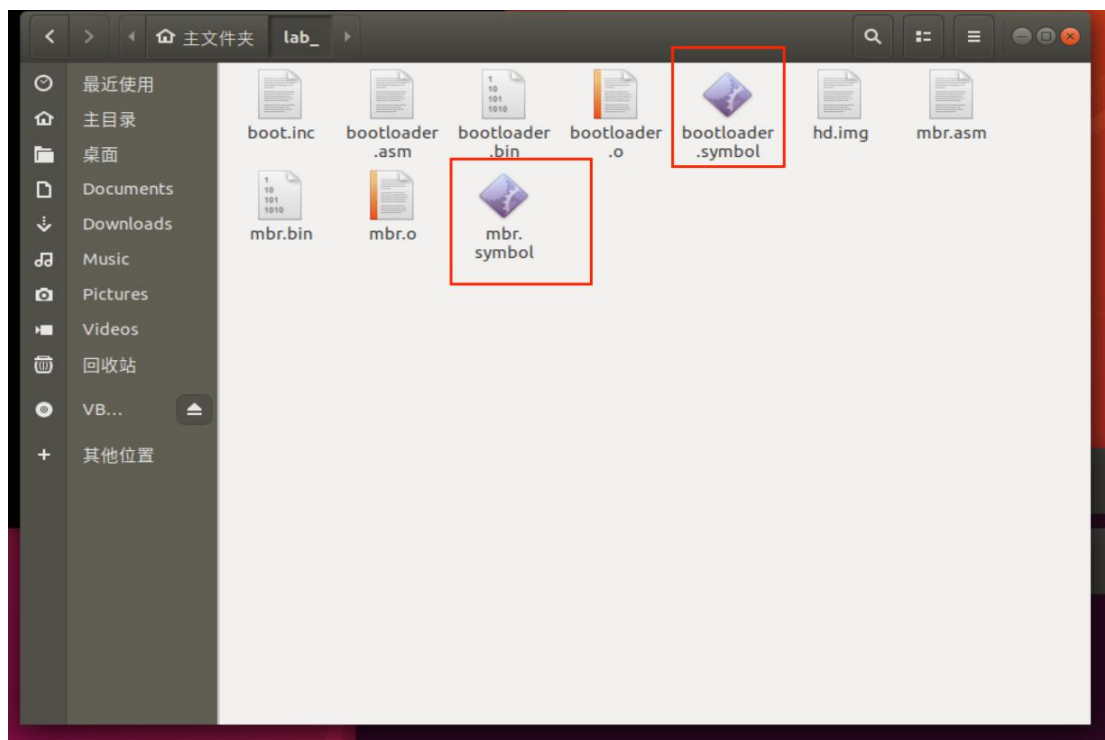


## 1. 生成符号表和img 文件

```
adria@adria-VirtualBox:~$ cd chap2
adria@adria-VirtualBox:~/chap2$ cd ..
adria@adria-VirtualBox:~$ cd lab_
adria@adria-VirtualBox:~/lab_$ touch bootloader.asm
adria@adria-VirtualBox:~/lab_$ touch mbr.asm
adria@adria-VirtualBox:~/lab_$ nasm -o mbr.o -g -f elf32 mbr.asm
adria@adria-VirtualBox:~/lab_$ nasm -o bootloader.o -g -f elf32 bootloader.asm
adria@adria-VirtualBox:~/lab_$ ld -o mbr.bin -melf_i386 -N mbr.o -Ttext 0x7c00 --oformat binary
ld: 警告: 无法找到项目符号 _start; 缺省为 0000000000007c00
adria@adria-VirtualBox:~/lab_$ ld -o bootloader.symbol -melf_i386 -N bootloader.o -Ttext 0x7e00 --oformat binary
ld: 警告: 无法找到项目符号 _start; 缺省为 0000000000007e00
adria@adria-VirtualBox:~/lab_$ ld -o bootloader.bin -melf_i386 -N bootloader.o -Ttext 0x7e00 --oformat binary
ld: 警告: 无法找到项目符号 _start; 缺省为 0000000000007e00
adria@adria-VirtualBox:~/lab_$ qemu-img create hd.img 10M
Formatting 'hd.img', fmt=raw size=10485760
adria@adria-VirtualBox:~/lab_$ dd if=bootloader.bin of=hd.img bs=512 count=1 seek=0 conv=notrunc
dd: 记录了1=0 的写入
dd: 记录了1=0 的写入
512 bytes copied, 0.00019907 s, 2.7 MB/s
adria@adria-VirtualBox:~/lab_$ dd if=bootloader.bin of=hd.img bs=512 count=5 seek=1 conv=notrunc
dd: 记录了5=1 的写入
dd: 记录了5=1 的写入
256 bytes copied, 0.00013131 s, 1.9 MB/s
adria@adria-VirtualBox:~/lab_$ qemu-system-i386 -s -S -hda hd.img -serial null -parallel stdio
WARNING: Image format was not specified for 'hd.img' and probing guessed raw.
Automatically detecting the format is dangerous for raw images, write operations on block 0 will be restricted.
Specify the 'raw' format explicitly to remove the restrictions.
```



## 2. gdb 调试

```
WARNING: Image format was not specified for 'hd.img' and probing guessed r-
Automatically detecting the format is dangerous for raw images, w
QEMU [Stopped]
Seabios (version 1.10.2-1ubuntu1)
[FXE (http://ipxe.org) 00:03:0 C300 PCI2.10 PnP P00-07F0B000-07EC0000 C300
Booting from Hard Disk...
adria@adria-VirtualBox: ~/lab_
License GPLv3: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type 'show copying'
and 'show warranty' for details.
This GDB was configured as 'x86_64-linux-gnu'.
Type 'show configuration' for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB Manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type 'help'.
Type 'apropos word' to search for commands related to 'word'.
(gdb) target remote:1234
Remote debugging using 1234
Warning: No executable has been specified and target does not support
determining executable automatically. Try using the 'file' command.
(gdb) b *0x7c00
Breakpoint 1 at 0x7c00
(gdb) c
Continuing.
Breakpoint 1, 0x00007c00 in ?? ()
(gdb)
```

第一个断点处

第一个断点(0x7c00)处的寄存器表

```
adria@adria-VirtualBox: ~/lab_
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
(gdb) b *0x7c00
Breakpoint 1 at 0x7c00
(gdb) c
Continuing.

Breakpoint 1, 0x00007c00 in ?? ()
(gdb) info registers
eax                0xaa55    43605
ecx                0x0        0
edx                0x80       128
ebx                0x0        0
esp                0x6f04     0x6f04
ebp                0x0        0x0
esi                0x0        0
edi                0x0        0
eip                0x7c00     0x7c00
eflags             0x202     [ IF ]
cs                 0x0        0
ss                 0x0        0
ds                 0x0        0
es                 0x0        0
fs                 0x0        0
gs                 0x0        0
(gdb)
```

此时的 gdb 状态

```
adria@adria-VirtualBox: ~/lab_
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

[ No Source Available ]

Remote Thread 1 In: L?? PC: 0x7c00
(gdb)
```

第二个断点(0x7e00)处的寄存器表

```
remote Thread 1 In:
(gdb) add-symbol-file mbr.symbol 0x7c00
add symbol table from file "mbr.symbol" at
.text_addr = 0x7c00
(y or n) y
Reading symbols from mbr.symbol...done.
(gdb) b *0x7e00
Breakpoint 2 at 0x7e00
(gdb) info registers
eax          0xaa55      43605
ecx          0x0         0
edx          0x80        128
ebx          0x0         0
esp          0x6f04      0x6f04
ebp          0x0         0x0
esi          0x0         0
edi          0x0         0
eip          0x7c00      0x7c00
eflags       0x202       [ IF ]
cs           0x0         0
ss           0x0         0
ds           0x0         0
es           0x0         0
fs           0x0         0
gs           0x0         0
(gdb)
```

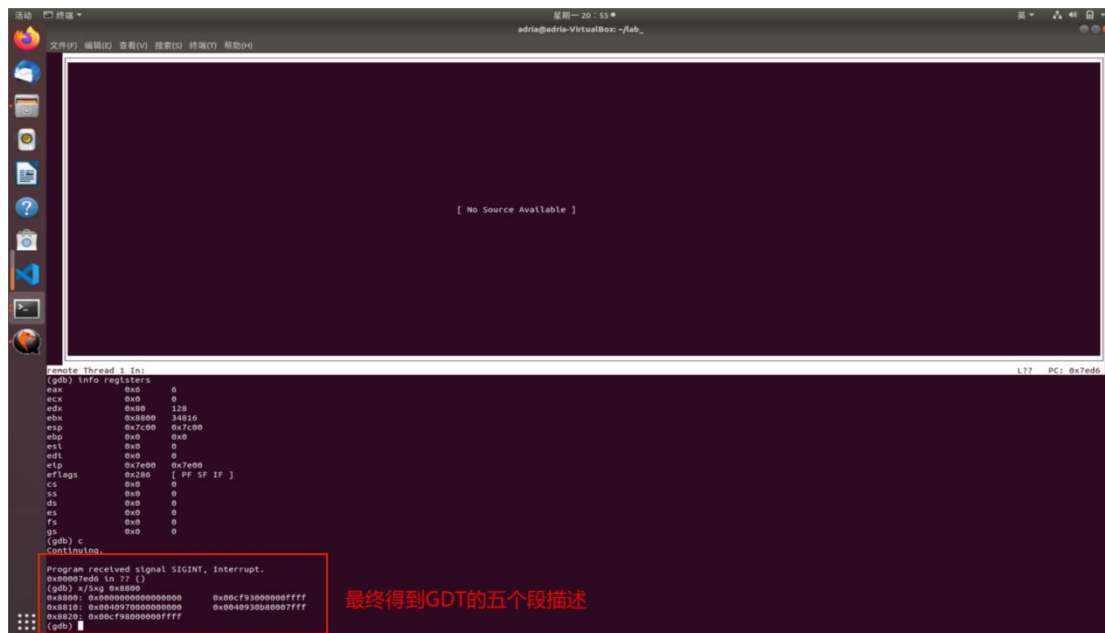
第二个断点处

第三个断点（protect\_mode\_begin）处的寄存器表

```
remote Thread 1 In:
gs          0x0         0
(gdb) b protect_mode_begin
Function "protect_mode_begin" not defined.
Make breakpoint pending on future shared library load? (y or [n]) y
Breakpoint 3 (protect_mode_begin) pending.
(gdb) c
Continuing.
Breakpoint 2, 0x00007e00 in ?? ()
(gdb) info registers
eax          0x6         6
ecx          0x0         0
edx          0x80        128
ebx          0x8800      34816
esp          0x7c00      0x7c00
ebp          0x0         0x0
esi          0x0         0
edi          0x0         0
eip          0x7e00      0x7e00
eflags       0x286       [ PF SF IF ]
cs           0x0         0
ss           0x0         0
ds           0x0         0
es           0x0         0
fs           0x0         0
gs           0x0         0
(gdb)
```

第三个断点处

最终 GDT 的五个段描述



最终 qemu 和 gdb 显示

