

**实验报告**

**实 验（四）**

题 目 LinkLab

链接

专 业 计算机专业

学　　 号 1190200501

班　　 级 1903002

学 生 林燕燕

指 导 教 师 郑贵滨

实 验 地 点 G709

实 验 日 期 2021.05.21

**计算机科学与技术学院**

**目 录**

[第1章 实验基本信息 - 3 -](#_Toc25154534)

[1.1 实验目的 - 3 -](#_Toc25154535)

[1.2 实验环境与工具 - 3 -](#_Toc25154536)

[1.2.1 硬件环境 - 3 -](#_Toc25154537)

[1.2.2 软件环境 - 3 -](#_Toc25154538)

[1.2.3 开发工具 - 3 -](#_Toc25154539)

[1.3 实验预习 - 3 -](#_Toc25154540)

[第2章 实验预习 - 4 -](#_Toc25154541)

[2.1 ELF文件格式解读 - 4 -](#_Toc25154542)

[2.2程序的内存映像结构 - 4 -](#_Toc25154543)

[2.3程序中符号的位置分析 - 5 -](#_Toc25154544)

[2.4程序运行过程分析 - 7 -](#_Toc25154545)

[第3章 各阶段的原理与方法 - 9 -](#_Toc25154546)

[3.1 阶段1的分析 - 9 -](#_Toc25154547)

[3.2 阶段2的分析 - 10 -](#_Toc25154548)

[3.3 阶段3的分析 - 13 -](#_Toc25154549)

[3.4 阶段4的分析 - 13 -](#_Toc25154550)

[3.5 阶段5的分析 - 13 -](#_Toc25154551)

[第4章 总结 - 14 -](#_Toc25154552)

[4.1 请总结本次实验的收获 - 14 -](#_Toc25154553)

[4.2 请给出对本次实验内容的建议 - 14 -](#_Toc25154554)

[参考文献 - 15 -](#_Toc25154555)

# 第1章 实验基本信息

## 1.1 实验目的

* 理解链接的作用与工作步骤
* 掌握ELF结构、符号解析与重定位的工作过程
* 熟练使用Linux工具完成ELF分析与修改

## 1.2 实验环境与工具

### 1.2.1 硬件环境

X64 CPU；1.6GHz；8G RAM；256G SSD Disk；1T HDD Disk

### 1.2.2 软件环境

Windows10 64位；Vmware 14pro；Ubuntu 20.04.2 LTS 64位

### 1.2.3 开发工具

Visual Studio Code 64位；vim/gpedit+gcc

## 1.3 实验预习

* 请按顺序写出ELF格式的可执行目标文件的各类信息。
* 请按照内存地址从低到高的顺序，写出Linux下X64内存映像。
* 请运行“LinkAddress -u 学号 姓名” 按地址顺序写出各符号的地址、空间。并按照Linux下X64内存映像结构，标出其所属各区。
* 请按顺序写出LinkAddress从开始执行到main前/后执行的子程序的名字。(gcc与objdump/GDB/EDB)

# 第2章 实验预习

## 2.1 ELF文件格式解读

请按顺序写出ELF格式的可执行目标文件的各类信息（5分）

|  |
| --- |
| ELF 头 |
| 段头部表 |
| .init |
| .text |
| .rodata |
| .data |
| .bss |
| .symtab |
| .debug |
| .line |
| .strtab |
| 节头部表 |

## 2.2程序的内存映像结构

请按照内存地址从低到高的顺序，写出Linux下X64内存映像（5分）

|  |
| --- |
| 内核内存 |
| 用户栈  （运行时 创建） |
| （栈-向下）  ...  （映射区域-向上） |
| 共享库的内存映射区域 |
| ...  （堆-向上） |
| 运行时堆  （由 malloc 创建） |
| 读/写段  （.data,.bss） |
| 只读代码段  （.init,.text,.rodata） |
| ... |

## 2.3程序中符号的位置分析

请运行“LinkAddress -u 学号 姓名” 按地址顺序写出各符号的地址，并按照Linux下X64内存映像标出其所属内存区段（5分）

|  |  |
| --- | --- |
| 所属 | 符号、地址、空间（从小到大） |
| 只读代码段  (.init , .text ,.rodata) | exit 0x7f84fd098bc0 140209157671872  printf 0x7f84fd0b3e10 140209157783056  malloc 0x7f84fd0ec260 140209158013536  free 0x7f84fd0ec850 140209158015056 |
| 读/写段  (.data , .bss) | show\_pointer 0x561bea048199 94677890269593  useless 0x561bea0481d0 94677890269648  main 0x561bea0481df 94677890269663  global 0x561bea04b02c 94677890281516  huge array 0x561bea04b040 94677890281536  big array 0x561c2a04b040 94678964023360 |
| 运行时堆 | p1 0x7f84ed04e010 140208888930320  p2 0x561c2c5a76b0 94679003199152  p3 0x7f84ed02d010 140208888795152  p4 0x7f84ad02c010 140207815049232  p5 0x7f842d02b010 140205667561488 |
| 用户栈  (运行时创建) | argc 0x7fffa503d2cc 140735961879244  local 0x7fffa503d2d0 140735961879248  argv 0x7fffa503d408 140735961879560  argv[0] 7fffa503f2dc  argv[1] 7fffa503f2ea  argv[2] 7fffa503f2ed  argv[3] 7fffa503f2f8  argv[0] 0x7fffa503f2dc 140735961887452  ./LinkAddress  argv[1] 0x7fffa503f2ea 140735961887466  -u  argv[2] 0x7fffa503f2ed 140735961887469  1190200501  argv[3] 0x7fffa503f2f8 140735961887480  林燕燕  env 0x7fffa503d430 140735961879600  env[0] \*env 0x7fffa503f302 140735961887490  SHELL=/bin/bash  env[1] \*env 0x7fffa503f312 140735961887506  SESSION\_MANAGER=local/ubuntu:@/tmp/.ICE-unix/1941,unix/ubuntu:/tmp/.ICE-unix/1941  env[2] \*env 0x7fffa503f364 140735961887588  QT\_ACCESSIBILITY=1  env[3] \*env 0x7fffa503f377 140735961887607  COLORTERM=truecolor  env[4] \*env 0x7fffa503f38b 140735961887627  XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg  env[5] \*env 0x7fffa503f3b8 140735961887672  XDG\_MENU\_PREFIX=gnome-  env[6] \*env 0x7fffa503f3cf 140735961887695  GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated  env[7] \*env 0x7fffa503f3fb 140735961887739  LANGUAGE=en\_US:en  env[8] \*env 0x7fffa503f40d 140735961887757  LC\_ADDRESS=zh\_CN.UTF-8  env[9] \*env 0x7fffa503f424 140735961887780  GNOME\_SHELL\_SESSION\_MODE=ubuntu  env[10] \*env 0x7fffa503f444 140735961887812  LC\_NAME=zh\_CN.UTF-8  env[11] \*env 0x7fffa503f458 140735961887832  SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh  env[12] \*env 0x7fffa503f481 140735961887873  XMODIFIERS=@im=ibus  env[13] \*env 0x7fffa503f495 140735961887893  DESKTOP\_SESSION=ubuntu  env[14] \*env 0x7fffa503f4ac 140735961887916  LC\_MONETARY=zh\_CN.UTF-8  env[15] \*env 0x7fffa503f4c4 140735961887940  SSH\_AGENT\_PID=1907  env[16] \*env 0x7fffa503f4d7 140735961887959  GTK\_MODULES=gail:atk-bridge  env[17] \*env 0x7fffa503f4f3 140735961887987  DBUS\_STARTER\_BUS\_TYPE=session  env[18] \*env 0x7fffa503f511 140735961888017  PWD=/mnt/hgfs/CSAPP/Lab/Lab05-linking-2021  env[19] \*env 0x7fffa503f53c 140735961888060  LOGNAME=lyy  env[20] \*env 0x7fffa503f548 140735961888072  XDG\_SESSION\_DESKTOP=ubuntu  env[21] \*env 0x7fffa503f563 140735961888099  XDG\_SESSION\_TYPE=x11  env[22] \*env 0x7fffa503f578 140735961888120  GPG\_AGENT\_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1  env[23] \*env 0x7fffa503f5ac 140735961888172  XAUTHORITY=/run/user/1000/gdm/Xauthority  env[24] \*env 0x7fffa503f5d5 140735961888213  WINDOWPATH=2  env[25] \*env 0x7fffa503f5e2 140735961888226  HOME=/home/lyy  env[26] \*env 0x7fffa503f5f1 140735961888241  USERNAME=lyy  env[27] \*env 0x7fffa503f5fe 140735961888254  IM\_CONFIG\_PHASE=1  env[28] \*env 0x7fffa503f610 140735961888272  LC\_PAPER=zh\_CN.UTF-8  env[29] \*env 0x7fffa503f625 140735961888293  LANG=en\_US.UTF-8  env[30] \*env 0x7fffa503f636 140735961888310  LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.zst=01;31:\*.tzst=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.wim=01;31:\*.swm=01;31:\*.dwm=01;31:\*.esd=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.mjpg=01;35:\*.mjpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:  env[31] \*env 0x7fffa503fc18 140735961889816  XDG\_CURRENT\_DESKTOP=ubuntu:GNOME  env[32] \*env 0x7fffa503fc39 140735961889849  VTE\_VERSION=6003  env[33] \*env 0x7fffa503fc4a 140735961889866  GNOME\_TERMINAL\_SCREEN=/org/gnome/Terminal/screen/081cd264\_5b2e\_4ca5\_b96a\_e0e65c376bcd  env[34] \*env 0x7fffa503fca0 140735961889952  INVOCATION\_ID=985fd6a32d9644eab0ac58b5b0825588  env[35] \*env 0x7fffa503fccf 140735961889999  MANAGERPID=1185  env[36] \*env 0x7fffa503fcdf 140735961890015  LESSCLOSE=/usr/bin/lesspipe %s %s  env[37] \*env 0x7fffa503fd01 140735961890049  XDG\_SESSION\_CLASS=user  env[38] \*env 0x7fffa503fd18 140735961890072  TERM=xterm-256color  env[39] \*env 0x7fffa503fd2c 140735961890092  LC\_IDENTIFICATION=zh\_CN.UTF-8  env[40] \*env 0x7fffa503fd4a 140735961890122  LESSOPEN=| /usr/bin/lesspipe %s  env[41] \*env 0x7fffa503fd6a 140735961890154  USER=lyy  env[42] \*env 0x7fffa503fd73 140735961890163  GNOME\_TERMINAL\_SERVICE=:1.95  env[43] \*env 0x7fffa503fd90 140735961890192  DISPLAY=:0  env[44] \*env 0x7fffa503fd9b 140735961890203  SHLVL=1  env[45] \*env 0x7fffa503fda3 140735961890211  LC\_TELEPHONE=zh\_CN.UTF-8  env[46] \*env 0x7fffa503fdbc 140735961890236  QT\_IM\_MODULE=ibus  env[47] \*env 0x7fffa503fdce 140735961890254  LC\_MEASUREMENT=zh\_CN.UTF-8  env[48] \*env 0x7fffa503fde9 140735961890281  DBUS\_STARTER\_ADDRESS=unix:path=/run/user/1000/bus,guid=854ae56f732a8aa6c55336b460adfe75  env[49] \*env 0x7fffa503fe41 140735961890369  PAPERSIZE=a4  env[50] \*env 0x7fffa503fe4e 140735961890382  XDG\_RUNTIME\_DIR=/run/user/1000  env[51] \*env 0x7fffa503fe6d 140735961890413  LC\_TIME=zh\_CN.UTF-8  env[52] \*env 0x7fffa503fe81 140735961890433  JOURNAL\_STREAM=8:47675  env[53] \*env 0x7fffa503fe98 140735961890456  XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop  env[54] \*env 0x7fffa503feed 140735961890541  PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin  env[55] \*env 0x7fffa503ff55 140735961890645  GDMSESSION=ubuntu  env[56] \*env 0x7fffa503ff67 140735961890663  DBUS\_SESSION\_BUS\_ADDRESS=unix:path=/run/user/1000/bus,guid=854ae56f732a8aa6c55336b460adfe75  env[57] \*env 0x7fffa503ffc3 140735961890755  LC\_NUMERIC=zh\_CN.UTF-8  env[58] \*env 0x7fffa503ffda 140735961890778  \_=./LinkAddress |

## 2.4程序运行过程分析

请按顺序写出LinkAddress从开始执行到main前/后执行的子程序的名字(使用gcc与objdump/GDB/EDB)（5分）

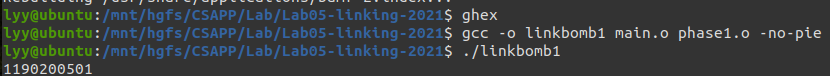
|  |  |
| --- | --- |
| 从开始执行到main前执行的子程序 | \_start ()  \_\_libc\_start\_main  \_\_GI\_\_\_cxa\_atexit  \_\_internal\_atexit  \_\_lll\_cas\_lock  \_\_new\_exitfn  \_\_libc\_start\_main  \_\_libc\_csu\_init ()  \_init ()  frame\_dummy ()  register\_tm\_clones ()  \_setjmp ()  \_\_sigsetjmp ()  \_\_sigjmp\_save |
| main后执行的子程序 | useless ()  show\_pointer ()  printf@plt ()  \_\_printf  \_\_vfprintf\_internal  \_\_find\_specmb  \*ABS\*+0xa4e10@plt ()  \_\_strchrnul\_avx2 ()  \_\_lll\_cas\_lock  IO\_validate\_vtable  \_IO\_new\_file\_xsputn  \*ABS\*+0xa27b0@plt ()  \_\_GI\_\_IO\_doallocbuf  \_\_GI\_\_IO\_file\_doallocate  \_\_GI\_\_IO\_file\_stat  \_\_GI\_\_\_fxstat  \_\_gnu\_dev\_major  malloc@plt  \_\_GI\_\_\_libc\_malloc  malloc\_hook\_ini  ptmalloc\_init ()  \_\_GI\_\_dl\_addr  \_dl\_find\_dso\_for\_object@plt ()  determine\_info |

# 第3章 各阶段的原理与方法

每阶段40分，phasex.o 20分，分析20分，总分不超过80分

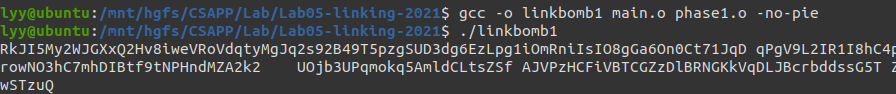
## 3.1 阶段1的分析

程序运行结果截图：

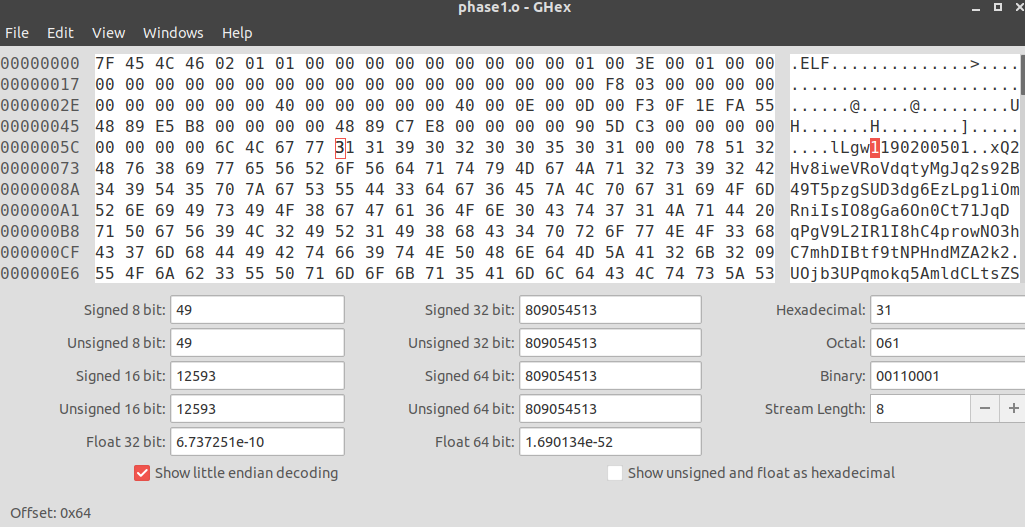


分析与设计的过程：

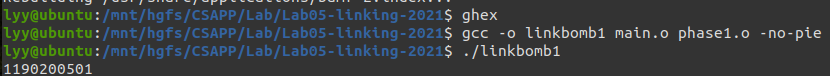
1. 将main.o和phase1.o链接编译运行，产生如下结果：



(2)再linux中使用GHex，查看"RkJI5......"位置，从首位修改为学号ASCII码值并在学号末尾加上00，即31 31 39 30 32 30 30 35 30 31 00，如下：

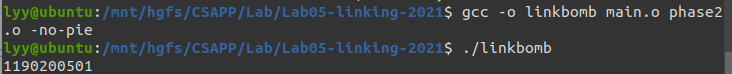


(3)重新连接编译运行得到结果：



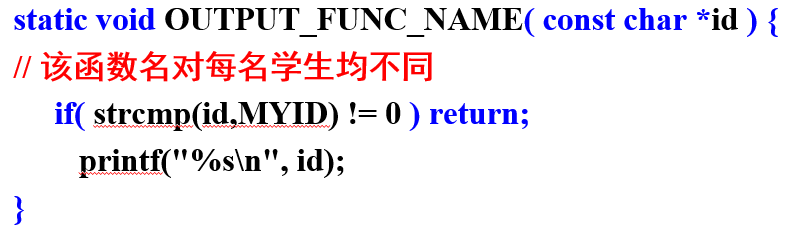
## 3.2 阶段2的分析

程序运行结果截图：

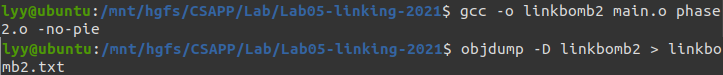


分析与设计的过程：

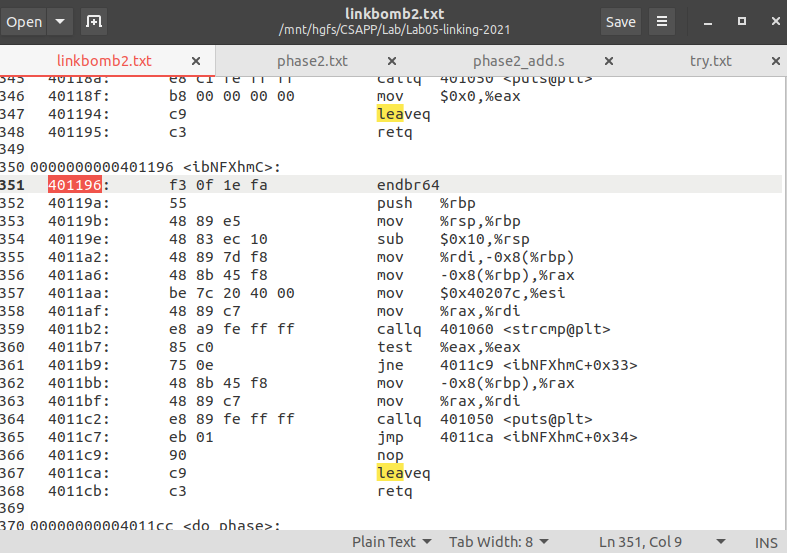
实验要求在do\_phase预留的存储位置加入代码，将学号传入如下示例函数，打印出学号。



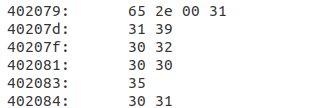
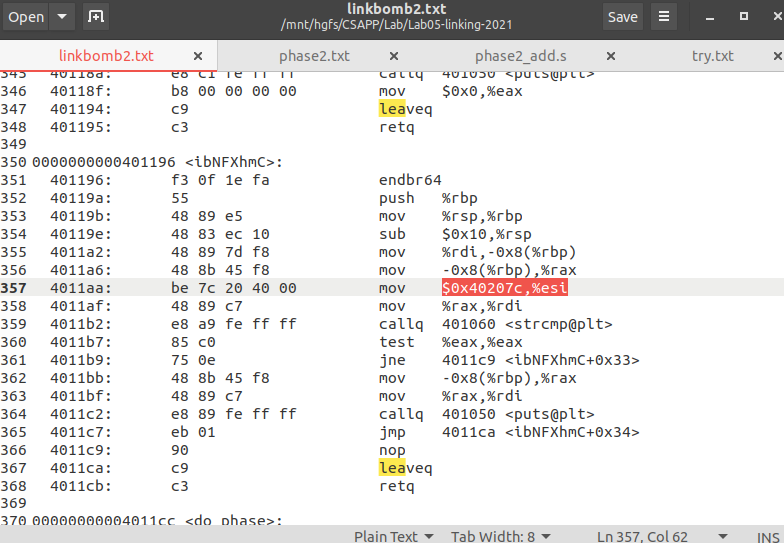
1、先将main.o和phase2.o进行链接生成linkbomb2，将linkbomb2反汇编，结果输出到linkbomb2.txt：



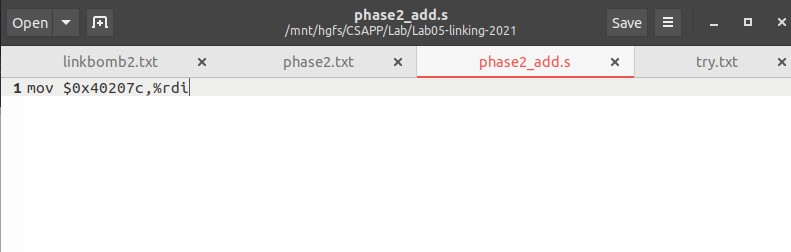
2、找到以下函数ibNFXhmC即为所需函数，记录地址为401196；



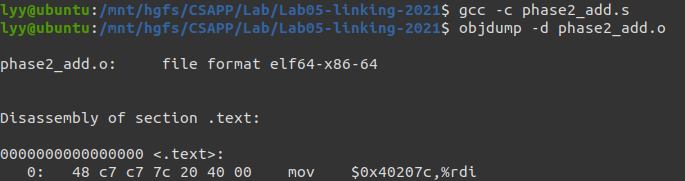
3、在ibNFXhmC函数中找到学号存储的地址为0x40207c



4、编写如下代码将学号存储地址传入%rdi，



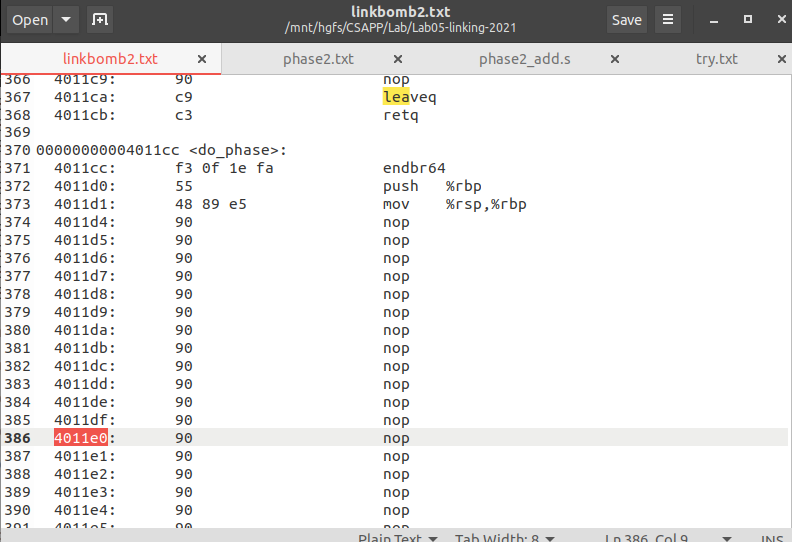
再汇编形成十六进制码：48 c7 c7 7c 20 40 00 共7个字节；



5、又有call指令相对寻址为5个字节，在do\_phase函数中从第一个nop开始留出7+5=12个字节存放mov和call指令，call指令的相对寻址为ibNFXhmC函数的地址减去留出12个字节后的地址，即为：

0x40207c - 0x4011e0 = ff ff ff b6

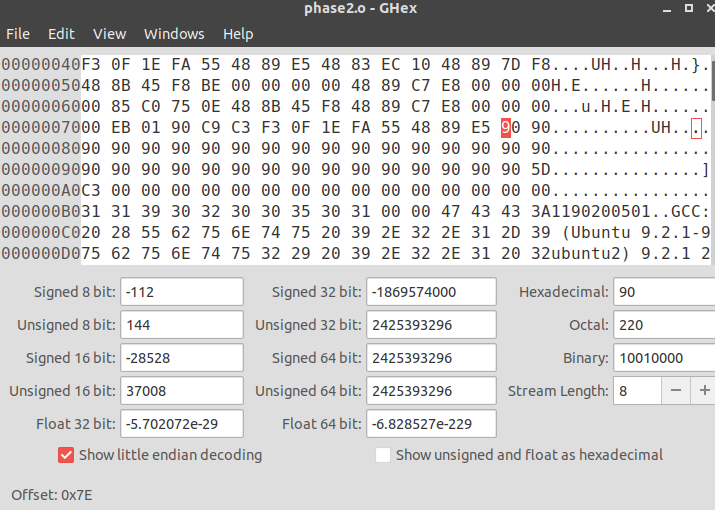
小端法表示，call指令六进制码为e8 b6 ff ff ff；



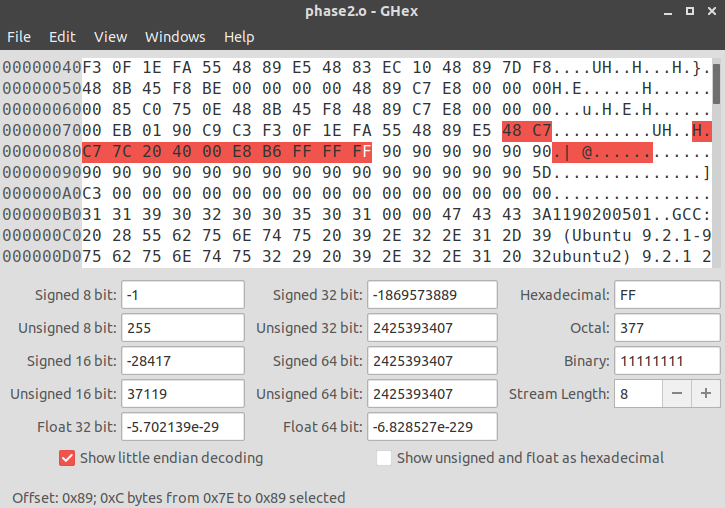
6、则需要加入do\_phase函数预留存储位置的十六进制码为：

48 c7 c7 7c 20 40 00 e8 b6 ff ff ff

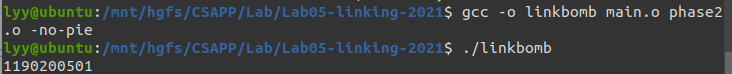
将phase2.o用GHex打开，找到预留位置：



将48 c7 c7 7c 20 40 00 e8 b6 ff ff ff替换如下：



7、重新连接main.o和phase2.o生成linkbomb，运行，输出学号如下：



## 3.3 阶段3的分析

程序运行结果截图：

分析与设计的过程：

## 3.4 阶段4的分析

程序运行结果截图：

分析与设计的过程：

## 3.5 阶段5的分析

程序运行结果截图：

分析与设计的过程：

# 第4章 总结

## 4.1 请总结本次实验的收获

学习了将多个.o 文件链接在一起运行；学会了 readelf 查看 elf 头文件。

## 4.2 请给出对本次实验内容的建议

注：本章为酌情加分项。

# 参考文献

[1] 林来兴. 空间控制技术[M]. 北京：中国宇航出版社，1992：25-42.

[2] 辛希孟. 信息技术与信息服务国际研讨会论文集：A集[C]. 北京：中国科学出版社，1999.

[3] 赵耀东. 新时代的工业工程师[M/OL]. 台北：天下文化出版社，1998 [1998-09-26]. http://www.ie.nthu.edu.tw/info/ie.newie.htm（Big5）.

[4] 谌颖. 空间交会控制理论与方法研究[D]. 哈尔滨：哈尔滨工业大学，1992：8-13.

[5] KANAMORI H. Shaking Without Quaking[J]. Science，1998，279（5359）：2063-2064.

[6] CHRISTINE M. Plant Physiology: Plant Biology in the Genome Era[J/OL]. Science，1998，281：331-332[1998-09-23]. http://www.sciencemag.org/cgi/ collection/anatmorp.