

# 哈尔滨工业大学

# 实验报告

## 实 验（四）

题 目 LinkLab

链接

专 业 计算机科学与技术

学 号 1170300520

班 级 1703005

学 生 郭子阳

指 导 教 师 吴 锐

实 验 地 点 G712

实 验 日 期 \_\_\_\_\_

计算机科学与技术学院

# 目 录

<b>第 1 章 实验基本信息 .....</b>	<b>- 3 -</b>
1.1 实验目的.....	- 3 -
1.2 实验环境与工具 .....	- 3 -
1.2.1 硬件环境.....	- 3 -
1.2.2 软件环境.....	- 3 -
1.2.3 开发工具 .....	- 3 -
1.3 实验预习.....	- 3 -
<b>第 2 章 实验预习 .....</b>	<b>- 4 -</b>
2.1 请按顺序写出 ELF 格式的可执行目标文件的各类信息（5 分） .....	- 4 -
2.2 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） .....	- 4 -
2.3 请运行“LINKADDRESS -U 学号 姓名”按地址循序写出各符号的地址、空间。 并按照 LINUX 下 X64 内存映像标出其所属各区。 .....	- 5 -
（5 分） .....	- 5 -
2.4 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)（5 分） .....	- 13 -
<b>第 3 章 各阶段的原理与方法.....</b>	<b>- 14 -</b>
3.1 阶段 1 的分析 .....	- 14 -
3.2 阶段 2 的分析 .....	- 14 -
3.3 阶段 3 的分析 .....	- 15 -
3.4 阶段 4 的分析 .....	- 15 -
3.5 阶段 5 的分析 .....	- 15 -
<b>第 4 章 总结.....</b>	<b>- 16 -</b>
4.1 请总结本次实验的收获 .....	- 16 -
4.2 请给出对本次实验内容的建议 .....	- 16 -
<b>参考文献.....</b>	<b>- 17 -</b>

## 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

Intel Core i7 6700HQ, 8GB RAM, 128GB SSD

#### 1.2.2 软件环境

Windows 10 专业版 64 位, Ubuntu 18.04.1 64 位

#### 1.2.3 开发工具

Codeblocks 17.12, gcc, cgdb, vscode

### 1.3 实验预习

上实验课前, 必须认真预习实验指导书 (PPT 或 PDF)

了解实验的目的、实验环境与软硬件工具、实验操作步骤, 复习与实验有关的理论知识。

请按顺序写出 ELF 格式的可执行目标文件的各类信息。

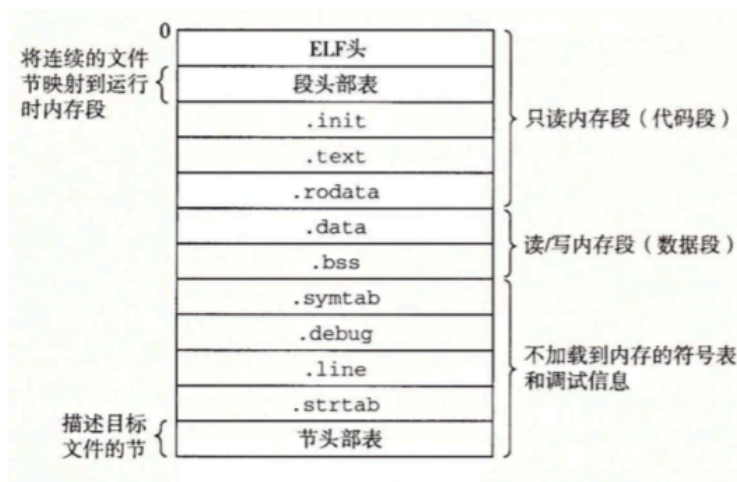
请按照内存地址从低到高的顺序, 写出 Linux 下 X64 内存映像。

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。

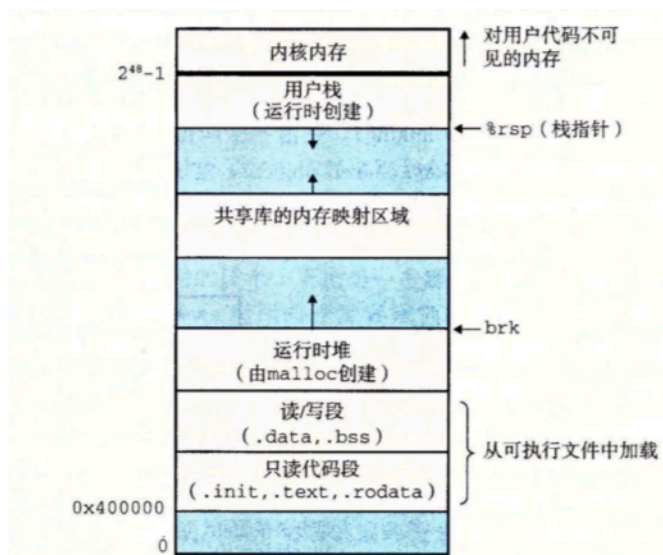
请按顺序写出 LinkAddress 从开始执行到 main 前/后执行的子程序的名字。(gcc 与 objdump/GDB/EDB)

## 第 2 章 实验预习

### 2.1 请按顺序写出 ELF 格式的可执行目标文件的各类信息 (5 分)



### 2.2 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)



2.3 请运行“LinkAddress -u 学号 姓名” 按地址循序写出各符号的地址、空间。并按照 Linux 下 X64 内存映像标出其所属各区。

(5 分)

env 0xffb8d8e8 4290304232

env[0] \*env 0xffb8f16e 4290310510

XDG\_SEAT=seat0

env[1] \*env 0xffb8f17d 4290310525

XDG\_SESSION\_ID=4

env[2] \*env 0xffb8f18e 4290310542

LC\_IDENTIFICATION=zh\_CN.UTF-8

env[3] \*env 0xffb8f1ac 4290310572

WINDOWPATH=2

env[4] \*env 0xffb8f1b9 4290310585

\_=/home/guoziyang/Desktop/outside/Desktop/lab5/./LinkAddr

env[5] \*env 0xffb8f1f3 4290310643

DISPLAY=:0

env[6] \*env 0xffb8f1fe 4290310654

DBUS\_STARTER\_ADDRESS=unix:path=/run/user/1000/bus, guid=6655975be02a4fd07ed702e55c0160b9

env[7] \*env 0xffb8f256 4290310742

COLORTERM=truecolor

env[8] \*env 0xffb8f26a 4290310762

GNOME\_TERMINAL\_SERVICE=:1.85

env[9] \*env 0xffb8f287 4290310791

GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated

env[10] \*env 0xffb8f2b3 4290310835

DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path

env[11] \*env 0xffb8f2e6 4290310886

LOGNAME=guoziyang

env[12] \*env 0xffb8f2f8 4290310904

TEXTDOMAIN=im-config

env[13] \*env 0xffb8f30d 4290310925

LC\_TIME=zh\_CN.UTF-8

env[14] \*env 0xffb8f321 4290310945

SHELL=/bin/zsh

env[15] \*env 0xffb8f330 4290310960

PAPERSIZE=a4

env[16] \*env 0xffb8f33d 4290310973

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

env[17] \*env 0xffb8f3a5 4290311077

LC\_NUMERIC=zh\_CN.UTF-8

env[18] \*env 0xffb8f3bc 4290311100

LC\_PAPER=zh\_CN.UTF-8

env[19] \*env 0xffb8f3d1 4290311121

IM\_CONFIG\_PHASE=2

env[20] \*env 0xffb8f3e3 4290311139

TEXTDOMAINDIR=/usr/share/locale/

env[21] \*env 0xffb8f404 4290311172

CLUTTER\_IM\_MODULE=xim

env[22] \*env 0xffb8f41a 4290311194

QT4\_IM\_MODULE=xim

env[23] \*env 0xffb8f42c 4290311212

INVOCATION\_ID=d51f7ca36c9f43f8ab1a34ae4b8d1227

env[24] \*env 0xffb8f45b 4290311259

XDG\_MENU\_PREFIX=gnome-

env[25] \*env 0xffb8f472 4290311282

GNOME\_SHELL\_SESSION\_MODE=ubuntu

env[26] \*env 0xffb8f492 4290311314

XAUTHORITY=/run/user/1000/gdm/Xauthority

env[27] \*env 0xffb8f4bb 4290311355

XDG\_SESSION\_DESKTOP=ubuntu

env[28] \*env 0xffb8f4d6 4290311382

GDMSESSION=ubuntu

env[29] \*env 0xffb8f4e8 4290311400

QT\_IM\_MODULE=ibus

env[30] \*env 0xffb8f4fa 4290311418

SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh

env[31] \*env 0xffb8f523 4290311459

LC\_MEASUREMENT=zh\_CN.UTF-8

env[32] \*env 0xffb8f53e 4290311486

LC\_ADDRESS=zh\_CN.UTF-8

env[33] \*env 0xffb8f555 4290311509

XMODIFIERS=@im=ibus

env[34] \*env 0xffb8f569 4290311529

XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg

env[35] \*env 0xffb8f596 4290311574

MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path

env[36] \*env 0xffb8f5cc 4290311628

USERNAME=guoziyang

env[37] \*env 0xffb8f5df 4290311647

DESKTOP\_SESSION=ubuntu

env[38] \*env 0xffb8f5f6 4290311670

XDG\_RUNTIME\_DIR=/run/user/1000

env[39] \*env 0xffb8f615 4290311701

GTK\_IM\_MODULE=ibus

env[40] \*env 0xffb8f628 4290311720

GTK\_MODULES=gail:atk-bridge

env[41] \*env 0xffb8f644 4290311748

USER=guoziyang

env[42] \*env 0xffb8f653 4290311763

PWD=/home/guoziyang/Desktop/outside/Desktop/lab5

env[43] \*env 0xffb8f684 4290311812

VTE\_VERSION=5202



env[44] \*env 0xffb8f695 4290311829

LC\_MONETARY=zh\_CN.UTF-8

env[45] \*env 0xffb8f6ad 4290311853

HOME=/home/guoziyang

env[46] \*env 0xffb8f6c2 4290311874

QT\_ACCESSIBILITY=1

env[47] \*env 0xffb8f6d5 4290311893

SSH\_AGENT\_PID=1417

env[48] \*env 0xffb8f6e8 4290311912

XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/local/share:/usr/share:/var/lib/napd/desktop

env[49] \*env 0xffb8f73b 4290311995

LANGUAGE=zh\_CN:en\_US:en

env[50] \*env 0xffb8f753 4290312019

MANAGERPID=1309

env[51] \*env 0xffb8f763 4290312035

LANG=zh\_CN.UTF-8

env[52] \*env 0xffb8f774 4290312052

LC\_NAME=zh\_CN.UTF-8

env[53] \*env 0xffb8f788 4290312072

GNOME\_TERMINAL\_SCREEN=/org/gnome/Terminal/screen/00b6b38f\_f475\_4f67\_92a5\_23cb893b481b

env[54] \*env 0xffb8f7de 4290312158

GPG\_AGENT\_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1

env[55] \*env 0xffb8f812 4290312210

SHLV=1

env[56] \*env 0xffb8f81a 4290312218

JOURNAL\_STREAM=9:42431

env[57] \*env 0xffb8f831 4290312241

DBUS\_STARTER\_BUS\_TYPE=session

env[58] \*env 0xffb8f84f 4290312271

XDG\_VTNR=2

env[59] \*env 0xffb8f85a 4290312282

TERM=xterm-256color

env[60] \*env 0xffb8f86e 4290312302

DBUS\_SESSION\_BUS\_ADDRESS=unix:path=/run/user/1000/bus, guid=6655975be02a4fd07ed702e55c0160b9

env[61] \*env 0xffb8f8ca 4290312394

XDG\_CURRENT\_DESKTOP=ubuntu:GNOME

env[62] \*env 0xffb8f8eb 4290312427

XDG\_SESSION\_TYPE=x11

env[63] \*env 0xffb8f900 4290312448

SESSION\_MANAGER=local/ubuntu:@/tmp/.ICE-unix/1839,unix/ubuntu:/tmp/.ICE-unix/1839

env[64] \*env 0xffb8f952 4290312530

LC\_TELEPHONE=zh\_CN.UTF-8

env[65] \*env 0xffb8f96b 4290312555

OLDPWD=/home/guoziyang/Desktop/outside/Desktop

env[66] \*env 0xffb8f99a 4290312602

ZSH=/home/guoziyang/.oh-my-zsh

env[67] \*env 0xffb8f9b9 4290312633

PAGER=less

env[68] \*env 0xffb8f9c4 4290312644

LESS=-R

env[69] \*env 0xffb8f9cc 4290312652

LC\_CTYPE=zh\_CN.UTF-8

env[70] \*env 0xffb8f9e1 4290312673

LSCOLORS=Gxfxcxdxbxegedabagacad

env[71] \*env 0xffb8fa01 4290312705

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:\*.lzh=01;31:\*.lma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=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:

big array 0x96613040 2522951744

huge array 0x56613040 1449209920

local 0xffb8d7ec 4290303980

global 0x56613024 1449209892

argc 0xffb8d840 4290304064

argv 0xffb8d8d4 4290304212

argv[0] ffb8f14b

argv[1] ffb8f156

argv[2] ffb8f159

argv[3] ffb8f164

argv[0] 0xffb8f14b 4290310475

./LinkAddr

argv[1] 0xffb8f156 4290310486

-u

argv[2] 0xffb8f159 4290310489

1170300520

argv[3] 0xffb8f164 4290310500

郭子阳

p1 0xe7dd9010 3890057232

p2 0x97b26570 2545050992

p3 0xe7db8010 3889922064

p4 0xa7db7010 2816176144

p5 (nil) 0

show\_pointer 0x566101bd 1449198013

useless 0x566101ef 1449198063

main 0x56610203 1449198083

exit 0xf7e0a3d0 4158694352

printf 0xf7e2b2d0 4158829264

malloc 0xf7e54c30 4158999600

free 0xf7e55250 4159001168

2. 4 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) (5 分)

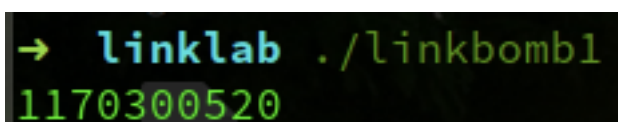
时间段	程序
Main函数执行前	Ld-2.27.so!_dl_start Ld-2.27.so!_dl_init Libc-2.27.so!_cxa_atexit Linkaddress!_init Linkaddress! _register_tm_clones Libc-2.27.so!_setjmp Libc2.27.so!__sigsetjmp Libc2.27.so!__sigjmpsave
Main函数执行之后	Linkaddress!puts@plt Linkaddress!useless@plt Linkaddress!showpointer@plt malloc Linkaddress!.plt Libc-2.27.so!exit

## 第 3 章 各阶段的原理与方法

每阶段 40 分，phases.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：



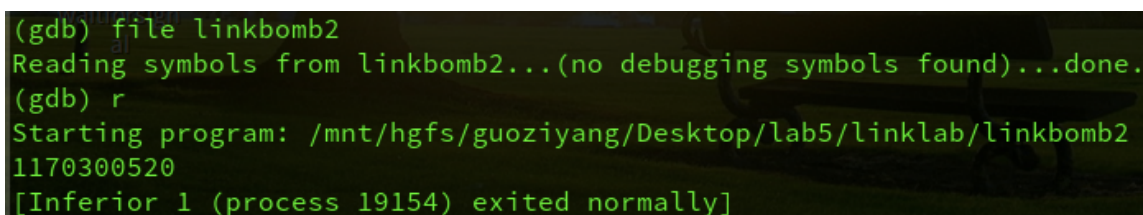
```
→ linklab ./linkbomb1
1170300520
```

分析与设计的过程：

用hexedit 把 phase 给打开之后，会发现第一次运行产生的字符串，找到字符串开头，从头开始把字符串修改为自己的学号即可

### 3.2 阶段 2 的分析

程序运行结果截图：



```
(gdb) file linkbomb2
Reading symbols from linkbomb2...(no debugging symbols found)...done.
(gdb) r
Starting program: /mnt/hgfs/guoziyang/Desktop/lab5/linklab/linkbomb2
1170300520
[Inferior 1 (process 19154) exited normally]
```

分析与设计的过程：

分析与设计的过程：

这里是 zctokQFQ 函数，我们想办法要做的就是让这个函数去被 do\_phase 这个函数调用，由于我们需要想办法 call 到这个函数上去，通过利用重定位算法进行计算，我们可以计算得到这个地址的相对偏移量，就可以直接 call 到这个函数上去。然后在把 nop 改成我们想要的代码就可以。

### 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

### 4.2 请给出对本次实验内容的建议

Phase2 无法在 terminal 直接运行



## 参考文献

### 为完成本次实验你翻阅的书籍与网站等

- [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>.