

**综合实训报告**

**ELF文件解析器的设计与实现**

|  |  |
| --- | --- |
| **姓名：** | **詹少雄** |
| **学号：** | **2019308210202** |
| **班级：** | **计科2003** |
| **指导老师：** | **任继平 李小霞** |
|  |  |

**中国 武汉**

**二○二三年六月**

**2023.06**

目录

[1实训目的及内容 2](#_Toc138590940)

[1.1实训目的 2](#_Toc138590941)

[1.2实训内容 2](#_Toc138590942)

[1.3实训安排 4](#_Toc138590943)

[2理论基础 5](#_Toc138590944)

[2.1 ELF文件概述 5](#_Toc138590945)

[2.2 ELF文件作用 6](#_Toc138590946)

[2.3 ELF文件解析选项 8](#_Toc138590947)

[2.4 ELF选项-h的基础理论 9](#_Toc138590948)

[2.5 ELF选项-S的基础理论 11](#_Toc138590949)

[2.6 ELF选项-l的基础理论 16](#_Toc138590950)

[2.7 ELF选项-d的基础理论 18](#_Toc138590951)

[3系统设计 20](#_Toc138590952)

[3.1 -h选项文件头表的数据结构设计 20](#_Toc138590953)

[3.2 -S选项节区头表的数据结构设计 21](#_Toc138590954)

[3.3 -l选项程序头表的数据结构设计 22](#_Toc138590955)

[3.4 -d选项动态链接表的数据结构设计 23](#_Toc138590956)

[4系统实现 24](#_Toc138590957)

[4.1 -h选项文件头表的程序设计 24](#_Toc138590958)

[4.2 -S选项节区头表的程序设计 27](#_Toc138590959)

[4.3 -l选项程序头表的程序设计 30](#_Toc138590960)

[4.4 -d选项动态链接的程序设计 32](#_Toc138590961)

[5系统测试 35](#_Toc138590962)

[5.1测试用例设计 35](#_Toc138590963)

[5.2测试结果及分析 36](#_Toc138590964)

[6结论与体会 44](#_Toc138590965)

[6.1结论 44](#_Toc138590966)

[6.2个人体会 45](#_Toc138590967)

[7参考文献 46](#_Toc138590968)

[8 附录 47](#_Toc138590969)

# 1实训目的及内容

## 1.1实训目的

本次综合实训围绕构建ELF文件解析器进行展开，通过分析ELF文件结构来以及相关的基础知识来构建ELF文件解析器。

通过本实践课程的学习，要求学生能够针对可执行文件解析较为复杂的计算机相关工程问题，对可执行文件格式涉及的问题进行抽象、对可执行文件格式系统建模，并能根据实验方案搭建系统开发环境，以具体可执行文件为实验数据，能正确解析其格式，优化解析方案。通过解析可执行文件格式，有助于学生理解计算机语言与操作系统之间的二进制接口，其已构成系统性理解计算机体系的必要环节。为学生今后从事计算机工程设计和软硬件开发及科研活动、生产实践打下扎实的良好的实践基础。增强学生的工程实践能力、系统能力。拟达成实训目标有：

实训目标1：（知识目标）对ELF文件格式进行分析，对源语言和硬件平台的知识进行融会贯通，对支持软件和硬件方案进行比较分析，针对具体应用选择实现方案；

实训目标2：（能力目标）熟练基于C/C++语言编程工具及其他辅助工具的能力，合理搭建开发环境、系统研发与部署、能对真实的可执行文件格式数据进行正确分析；

实训目标3：（素质目标）采用三人一组，让每个学生在团队中承担个体、团队成员的角色，独立或合作开展工作，体现团队合作精神；

实训目标4：（素质目标）针对其相关基础知识，设计方案、研究方法、技术路线等问题与他人进行有效沟通和交流，对实施过程和结果，以口头答辩和实训报告的方式准确表达观点；

## 1.2实训内容

|  |  |  |  |
| --- | --- | --- | --- |
| **任务名称** | **参考学时** | **实训内容** | **实训要求** |
| 第一章 问题定位与分析 | 4 | （1）阅读本实训的指导书，了解实训目的，要求和内容  （2）阅读ELF文件格式分析和程序员的自我修养，结合源语言和硬件平台理解ELF主要成分的含义 | 1.理解ELF文件格式内容；  2.结合指导书和ELF文件格式进行项目需求分析；  3.小组项目分工； |
| 第二章 实验方案设计和系统建模 | 12 | （1）系统概要设计  （2）系统详细设计  （3）关键算法选择和设计 | 1.进行系统概要设计建模过程；  2.进行系统详细设计建模过程；  3.对问题解决所需要的核心算法进行分析和选择  4.小组成员通过论证，迭代修改确定最终的实验方案； |
| 第三章 系统开发 | 24 | （1）项目系统开发  （2）项目集成 | 1.熟练掌握和应用C/C++编程语言进行系统的研发；  2.使用核心算法实现问题的解决；  3.熟练运行集成工作进行项目集成； |
| 第四章 实验数据获取与分析 | 12 | （1）对ELF格式文件进行系统测试  （2）对任意的ELF格式文件作为实验数据进行分析  （3）项目报告撰写 | 1.选择合适的系统测试方法；  2.针对不同的ELF格式形式，如库文件，目标格式文件，可执行文件作为测试数据进行测试；  3.项目完善并提出优化方案；  4.小组合作进行项目报告撰写。 |
| 第五章 项目演示与答辩 | 4 | （1）提交设计报告和源程序  （2）小组答辩 | 1.公开答辩和成果展示；  2.根据答辩意见进行项目修改完善。 |

该项目包括五个主要任务。第一章是问题定位与分析，我们需要阅读指导书和相关资料，理解ELF文件格式并分析项目需求，进行小组分工。第二章是实验方案设计和系统建模，我们需要进行系统概要设计和详细设计，并选择和设计关键算法。第三章是系统开发，我们需要使用C/C++编程语言进行系统研发，并进行项目集成。第四章是实验数据获取与分析，我们需要对ELF格式文件进行系统测试和分析，撰写项目报告。第五章是项目演示与答辩，我们需要提交设计报告和源程序，并进行公开答辩和成果展示。本项目涵盖了从问题分析到系统开发、测试、报告撰写和最终演示的全过程，我们需要在小组合作中完成各项任务。

## 1.3实训安排

##### 1.3.1 任务分工

本次实训我们三个人一组共同实现了ELF文件解析器的功能，我们小组的分工如下：

* **詹少雄**（计科2003）

负责统筹团队任务，安排实训方案与讲解，并成功完成了-h、-S、-l和-d的ELF解析选项。在项目中展示了出色的组织能力和解析技术，为团队提供了方向和指导。

* **李绅**（计科2004）

负责实训方案的实行与讲解，并顺利完成了-n、-e、-r和-d的ELF解析选项。展现了良好的实施能力和解析技术，为团队提供了有关ELF文件的重要信息。

* **杜鹏**（计科2003）

负责实训方案的实行与讲解，并圆满完成了-s、-t、-g和-d的ELF解析选项。在项目中展现了优秀的编程能力和解析技术，为团队提供了强大的功能。

通过我们小组成员的紧密合作和各自的分工，我们成功地开发出了一个功能完善的ELF文件解析器。每个人在项目中发挥了自己的优势，共同推动了项目的进展。我们共同面对挑战，克服了遇到的困难，并取得了显著的成果。

##### 1.3.2 任务合作Git流

在本次项目中，我们采用了Github工作流作为我们的团队合作平台。Github是一个广泛使用的代码托管和协作平台，它提供了一系列功能和工具，使得团队成员可以方便地协同工作和管理项目。我们将项目代码托管到Github上。通过创建一个项目仓库，我们可以将我们的代码统一存放在一个地方，并与团队成员共享。这使得团队成员可以轻松地访问、查看和编辑代码。

Github提供了强大的版本控制功能。我们可以使用Git作为代码版本控制工具，记录和管理我们的代码修改历史。这使得团队成员可以轻松地查看和比较不同版本的代码，以及回滚到之前的版本。通过版本控制，我们可以更好地跟踪项目的进展，并确保代码的稳定性和一致性。Github还提供了问题跟踪和任务管理功能。我们可以使用Github的Issue功能来记录和分配项目中的问题和任务。团队成员可以通过创建Issue、分配责任人、添加标签和评论等方式，对问题和任务进行跟踪和讨论。这使得团队成员可以更加高效地协同工作，明确各自的工作职责，并及时解决项目中的问题。Github还支持代码审核和合并功能。团队成员可以通过创建Pull Request来将自己的代码提交给项目的主要负责人进行审核。主要负责人可以对代码进行评论、提出修改建议，并最终决定是否合并到主分支中。这种代码审核和合并机制有助于保证代码的质量和一致性，以及团队成员之间的知识分享和技术交流。

通过将项目打包开源并发布到Github网站，我们不仅可以方便地进行团队合作，还可以向其他开发者和用户展示我们的工作成果。其他开发者可以查看我们的代码、提出建议和改进意见，从而促进项目的进一步发展和改善。

我们的项目已开源至：<https://github.com/Jasaxion/LinuxELF_FileParse>

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图 1 Github开源社区图

# 2理论基础

## 2.1 ELF文件概述

ELF文件格式是一种常见的可执行文件和目标文件格式。

它可以细分为三类：

1. 可重定位文件（Relocatable Files）：包含了链接器所需的代码和数据信息。链接器可以根据这些信息将多个可重定位文件通过链接过程生成可执行文件或共享库。
2. 可执行文件（Executable Files）：包含了最终需要执行的程序。可执行文件中的信息用于指导操作系统生成进程映像，从而执行程序。
3. 共享库文件（Shared Object Files）：共享库中的代码和数据具有两个主要用途。首先，静态链接器（如GNU ld）可以利用共享库和可重定位文件生成最终的目标文件，无论是可执行文件还是新的共享库。其次，动态链接器（如GNU ld-linux.so）可以利用共享库和可执行文件生成最终的进程映像。

经过编译器和链接器的处理，目标文件（可执行文件或共享库）被转化为处理器可识别的二进制指令序列，这些指令描述了程序的行为。需要注意的是，有些程序的执行需要依靠解释器的帮助。

## 2.2 ELF文件作用

ELF文件在程序的连接和执行过程中扮演着重要的角色，因此可以从不同的角度来理解ELF格式的文件：

* 如果用于编译和链接（可重定位文件），编译器和链接器将把ELF文件视为节头表描述的节的集合，其中每个节都包含了程序中的特定信息，如代码、数据和符号表等。可重定位文件的主要目的是提供链接器所需的代码和数据信息，以便生成最终的可执行文件或共享库。此时，ELF文件中的程序头表是可选的，因为它主要用于加载执行阶段。
* 如果用于加载执行（可执行文件），加载器将把ELF文件看作是程序头表描述的段的集合。一个段可能包含多个节，这些节包含了在程序执行过程中需要的代码、数据和其他资源。程序头表描述了这些段在内存中的加载位置、大小和访问权限等信息，以便操作系统正确地将程序映射到内存并执行。与可重定位文件不同，此时ELF文件中的节头表是可选的，因为加载执行阶段更关注段的组织和映射。
* 如果是共享文件（共享库），ELF文件既包含了用于编译和链接的节头表，也包含了用于加载执行的程序头表。共享库既可以作为编译和链接的目标，也可以在程序加载和执行时被动态链接到内存中。

图2和图3展现了两种视图下的模块形式：

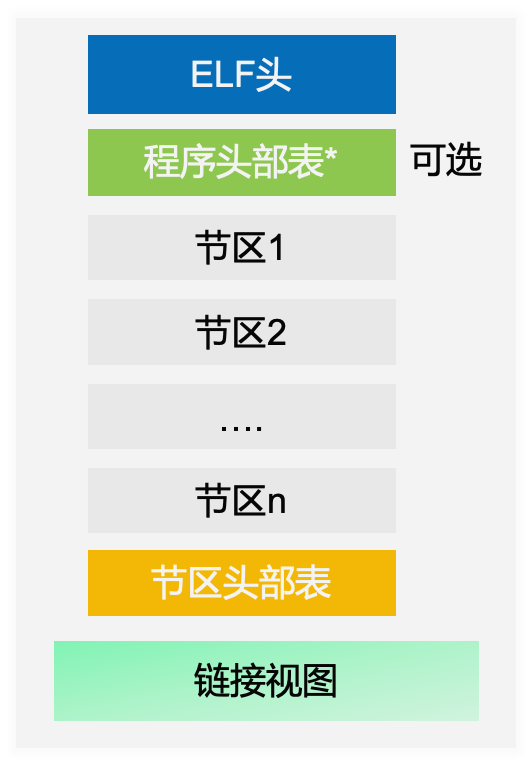


图 2 链接视图

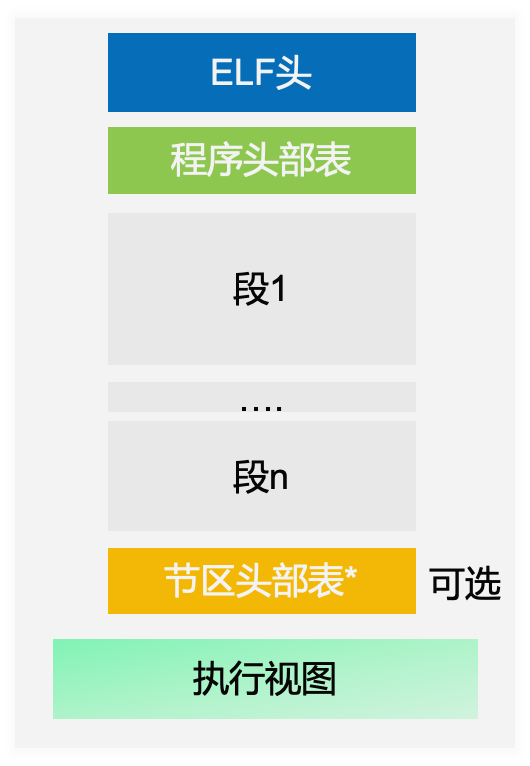


图 3 执行视图

从图3中可以看出，包含了一个ELF头部，它描绘了整个文件的组织结构。它还包括很多节区（section）。这些节有的是系统定义好的，有些是用户在文件在通过.section命令自定义的，链接器会将多个输入目标文件中的相同的节合并。节区部分包含链接视图的大量信息：指令、数据、符号表、重定位信息等等。除此之外，还包含程序头部表（可选）和节区 头部表，程序头部表，告诉系统如何创建进程映像。用来构造进程映像的目标文件必须具有程序头部表，可重定位文件不需要这个表。而节区头部表（Section Heade Table）包含了描述文件节区的信息，每个节区在表中都有一项，每一项给出诸如节区名称、节区大小这类信息。用于链接的目标文件必须包含节区头部表，其他目标文件可以有，也可以没有这个表。

需要注意地是：尽管图中显示的各个组成部分是有顺序的，实际上除了 ELF 头部表以外，其他节区和段都没有规定的顺序。

图4是以程序执行视图来看待的，与左边对应，多了一个段（segment）的概念，编译器在生成目标文件时，通常使用从零开始的相对地址，而在链接过程中，链接器从一个指定的地址开始，根据输入目标文件的顺序，以段（segment）为单位将它们拼装起来。其中每个段可以包括很多个节（section）。

## 2.3 ELF文件解析选项

-a , --all 显示全部信息,等价于 -h -l -S -s -r -d -V -A -I 。

-h , --file-header 显示 elf 文件开始的文件头信息.

-l , --program-headers , --segments 显示程序头（段头）信息(如果有的话)。

-S , --section-headers , --sections 显示节头信息(如果有的话)。

-g , --section-groups 显示节组信息(如果有的话)。

-t , --section-details 显示节的详细信息( -S 的)。

-s , --syms , --symbols 显示符号表段中的项（如果有的话）。

-e , --headers 显示全部头信息，等价于: -h -l -S

-n , --notes 显示 note 段（内核注释）的信息。

-r , --relocs 显示可重定位段的信息。

-u , --unwind 显示 unwind 段信息。当前只支持 IA64 ELF 的 unwind 段信息。

-d , --dynamic 显示动态段的信息。

-V , --version-info 显示版本段的信息。

-A , --arch-specific 显示 CPU 构架信息。

-D , --use-dynamic 使用动态段中的符号表显示符号，而不是使用符号段。

-x , --hex-dump= 以16进制方式显示指定段内内容。 number 指定段表中段的索引,或字符串指定文件中的段名。

-I , --histogram 显示符号的时候，显示 bucket list 长度的柱状图。

-v , --version 显示 readelf 的版本信息。

-H , --help 显示 readelf 所支持的命令行选项。

-W , --wide 宽行输出。

## 2.4 ELF选项-h的基础理论

##### 2.4.1 -h选项的成员参数

选项-h ： 显示ELF的文件头信息

-h 命令可以显示 文件的 ELF 文件头信息，包括文件类型、机器架构、入口地址、程序头表和节头表的偏移和数量等信息。

成员函数及其含义如下：

表 1 ELF-h选项的成员值表

|  |  |
| --- | --- |
| **成员** | **含义** |
| e\_ident | Magic: 7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00 |
|  | Class: ELF64 |
|  | Data: 2's complement, little endian |
|  | Version: 1(current) |
|  | OS/ABI: UNIX System V ABI |
|  | ABI Version: 0 |
| e\_type | Type: None (None) |
|  | ELF文件类型 |
| e\_machine | Machine: None |
|  | ELF文件的CPI平台属性 |
| e\_version | Version: 0x0 |
|  | ELF版本号。一般为常数1 |
| e\_entry | Entry point address: 0x0 |
|  | 入口地址，规定ELF程序的入口虚拟地址，操作系统在加载完该程序后从这个地址开始执行进程的指令。可重定位指令一般没有入口地址，则该值为0 |
| e\_phoff | Start of program headers: 0(bytes into file) |
| e\_shoff | Start of section headers: 0 (bytes into file) |
|  | Section Header Table 在文件中的偏移 |
| e\_word | Flags: 0x0 |
|  | ELF标志位，用来标识一些ELF文件平台相关的属性。 |
| e\_ehsize | Size of this header: 0 (bytes) |
|  | ELF Header本身的大小 |
| e\_phentsize | Size of program headers: 0 (bytes) |
| e\_phnum | Number of program headers: 0 |
| e\_shentsize | Size of section headers: 0 (bytes) |
|  | 单个Section Header大小 |
| e\_shnum | Number of section headers: 0 |
|  | Section Header的数量 |
| e\_shstrndx | Section header string table index: 0 |
|  | Section Header字符串表在Section Header Table中的索引 |

##### 2.4.2 Magic魔数

每种可执行文件的格式的开头几个字节都是很特殊的，特别是开头4个字节，通常被称为魔数（Magic Number）。通过对魔数的判断可以确定文件的格式和类型。如：ELF的可执行文件格式的头4个字节为0x7F、e、l、f；Java的可执行文件格式的头4个字节为c、a、f、e；如果被执行的是Shell脚本或perl、python等解释型语言的脚本，那么它的第一行往往是#!/bin/sh或#!/usr/bin/perl或#!/usr/bin/python，此时前两个字节#和!就构成了魔数，系统一旦判断到这两个字节，就对后面的字符串进行解析，以确定具体的解释程序路径。

##### 2.4.3 ELF文件类型

ELF文件主要有三种类型，可以通过ELF Header中的e\_type成员进行区分。

* 可重定位文件（Relocatable File）：ETL\_REL。一般为.o文件。可以被链接成可执行文件或共享目标文件。静态链接库属于可重定位文件。
* 可执行文件（Executable File）：ET\_EXEC。可以直接执行的程序。
* 共享目标文件（Shared Object File）：ET\_DYN，一般为.so文件，有两种情况可以使用。
  + 链接器将其与其他可重定位文件、共享目标文件链接成新的目标文件；
  + 动态链接器将其与其他共享目标文件、结合一个可执行文件，创建进程映像。

##### 2.4.4 机器类型

ELF文件格式被设计成可以在多个平台下使用，但这并不是表示同一个ELF文件可以在不同的平台下使用，而是表示不同平台下的ELF文件都遵循同一套ELF标准。e\_machine成员就表示该ELF文件的平台属性，

* EM\_M32：1 「AT&T WE 32100」
* EM\_SPARC：2 「SPARC」
* EM\_386: 3 「Intel x86」
* EM\_68K：4 「Motorola 680000」
* EM\_88K：5 「Motorola 88000」
* EM\_860：6 「Intel 80860」

## 2.5 ELF选项-S的基础理论

##### 2.5.1 选项- S的介绍

选项-S用于列出节的头信息

段（segment) 和 节（section)是有区别的。 节不是段。 段是程序执行的必要组成部分。 在每个段中会有代码或者数据被划分为不同的节。 而 节头表 则是对这些节的位置和大小的描述，主要是用于链接和调试。

因为节头表没有对程序的内存布局进行描述，对程序内存布局的描述的是 程序头表的任务。 所以节头表就是对程序头的补充。所以我们将“节头表”都填充为无用的值的话程序还是可以正常启动的。 虽然可以修改，但是随着版本的升级，保不准以后会使用。 就跟window平台上的最小PE一样，在xp下可以是100kb以下。win7下则对各个表的限制更严格了。所以需要100kb以上。 win10同理。 所以节头表以后可能会使用。

* **节头和节**

​ 如果二进制文件中缺少了 节头 ，并不意味着节是不存在的。只是没有办法通过节头来引用节了，对于调试器或者反编译（IDA)程序来说，参考的信息就变少了。

每一个节都保存了某种类型的代码和数据。数据可以是程序中的全局变量，也可以是连接器所需要的动态链接的信息。这点跟windows平台的 windowsPE文件格式设计很像。节头可以被抹除，默认的ELF文件是有节头的。如果节头被抹除，那么 objcopy objdump gdb IDA 等工具就可能无法使用。而节头表中的 .dynsym这样的节（记录了函数名和偏移地址，导入导出等符号）就无法分析。进而就增大了逆向的难度。

##### 2.5.2 选项- S的成员参数

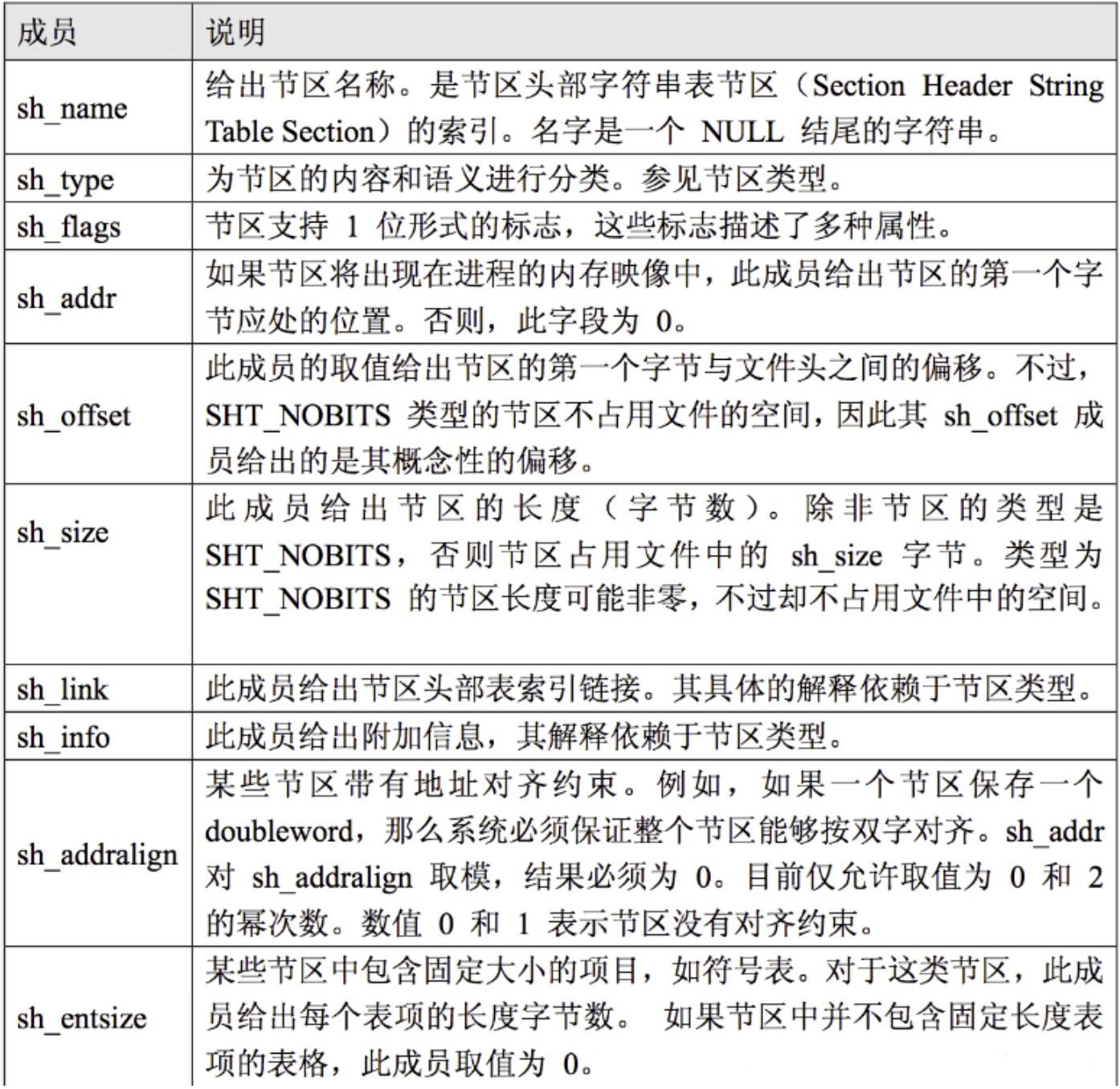


图 4 选项-S的成员参数列表图

sh\_name：0——无名称

sh\_type：SHT\_NULL——非活动

sh\_flags：0——无标志

此字段定义了一个节区中包含的内容是否可以修改，是否可以执行的信息。 如果一个标志位被设置，则该位取值为1. 定义的各位都设置为0

SHF\_WRITE：0x1

SHF\_ALLOC：0x2

SHF\_EXECINSTR：0x4 ——节区包含可执行的机器指令

SHF\_MASKPROC：0xF0000000

sh\_addr：0——无地址

sh\_offset：0——无文件偏移

sh\_size：0——无尺寸大小

sh\_link：SHN\_UNDEF——无链接信息

sh\_inf：0——无辅助信息

sh\_addralign：0——无对齐要求

sh\_entsize：0——无表项

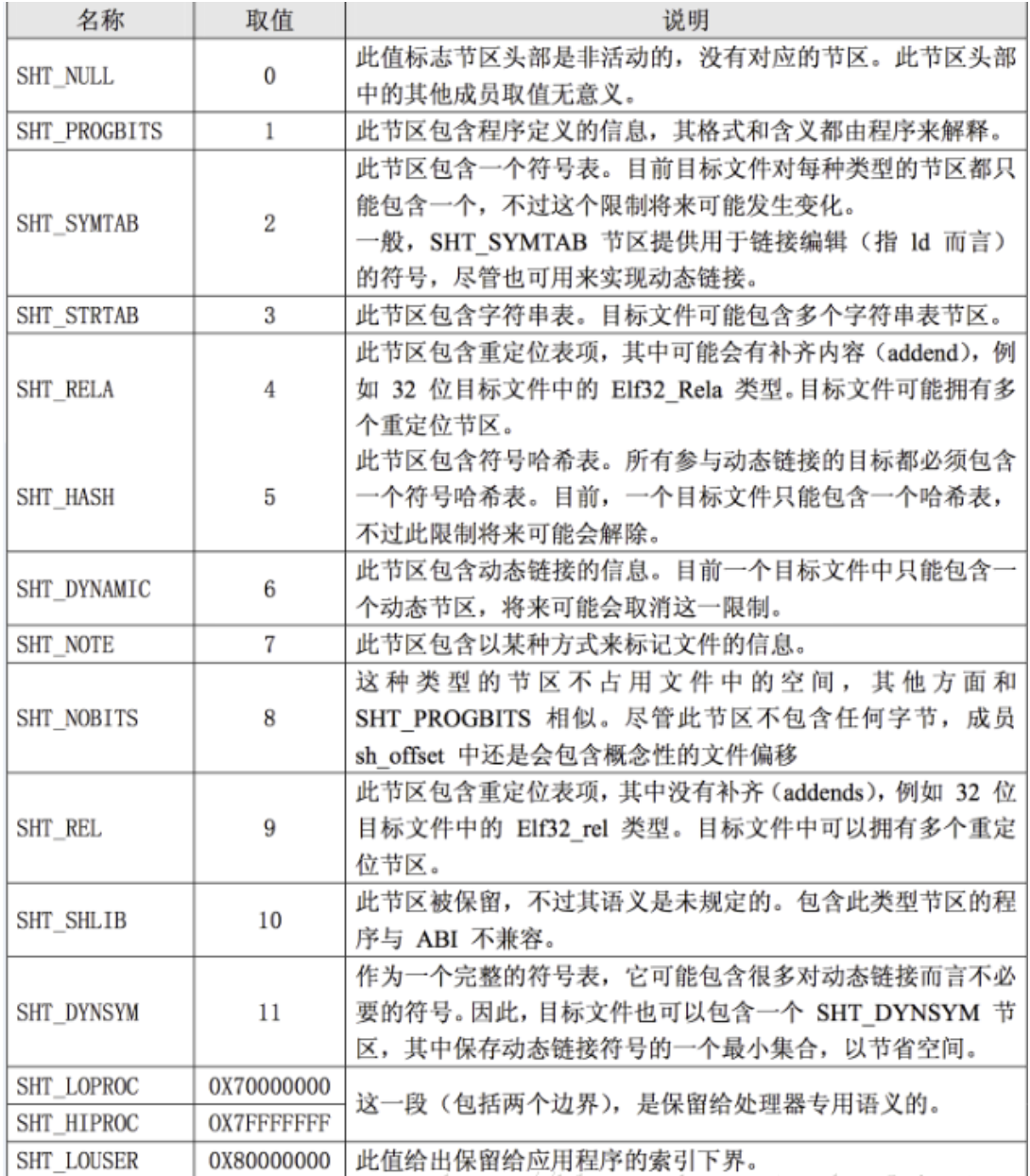


图 5 选项-S的取值列表图

##### 2.5.3 特殊节区

表 2特殊节区列表

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | **类型** | **属性** | **含义** |
| .bss | SHT NO BITS | SHF\_ALLOC SHF\_WRITE | 包含将出现在程序的内存映像中的为初始 化数据。根据定义，当程序开始执行，系统 将把这些数据初始化为0。此节区不占用文 件空间。 |
| .comment | SHT\_PROG BITS | (无) | 包含版本控制信息。 |
| .data | SHT PROG BITS | SHF\_ALLOC SHF\_WRITE | 这些节区包含初始化了的数据，将出现在程 序的内存映像中。 |
| .data l | SHT\_PROG BITS | SHF\_ALLOC |  |
| SHF WRITE |  |  |  |
| .debug | SHT\_PROG BITS | (无) | 此节区包含用于符号调试的信息。 |
| .dynamic | SHT DYNAMIC |  | 此节区包含动态链接信息。节区的属性将包 含SHF\_ALLOC位。是否SHF\_WRITE位 被设置取决于处理器。 |
| .dyn str | SHT\_STRTAB | SHF\_ALLOC | 此节区包含用于动态链接的字符串，大多数 情况下这些字符串代表了与符号表项相关 的名称。 |
| .dynsym | SHT DYNSYM | SHF ALLOC | 此节区包含了动态链接符号表。 |
| .fini | SHT\_PROG BITS | SHF\_ALLOC SHF\_EXEC INSTR | 此节区包含了可执行的指令，是进程终止代 码的一部分。程序正常退出时，系统将安排 执行这里的代码。 |
| ·got | SHT\_PROG BITS |  | 此节区包含全局偏移表。 |
| .hash | SHT\_HASH | SHF\_ALLOC | 此节区包含了一个符号哈希表。 |
| .in it | SHT\_PROG BITS | SHF\_ALLOC SHF\_EXEC INSTR | 此节区包含了可执行指令，是进程初始化代 码的一部分。当程序开始执行时，系统要在 开始调用主程序入口之前(通常指C语言 的main函数) 执行这些代码。 |
| .interp | SHT PROG BITS |  | 此节区包含程序解释器的路径名。如果程序包含一个可加载的段，段中包含此节区，那么节区的属性将包含SHF\_ALLOC位， 否则该位为0。 |
| .line | SHT\_PROG BITS | (无) | 此节区包含符号调试的行号信息，其中描述 了源程序与机器指令之间的对应关系。其内 容是未定义的。 |
| .note | SHT\_NOTE | (无) | 此节区中包含注释信息，有独立的格式。 |
| ·plt | SHT\_PROG BITS |  | 此节区包含过程链接表(procedure linkage |
| table) 。 |  |  |  |
| .relname | SHT\_REL |  | 这些节区中包含了重定位信息。如果文件中 包含可加载的段，段中有重定位内容，节区 的属性将包含SHF\_ALLOC位， 否则该位 置0。传统上name根据重定位所适用的节 区给定。例如 .text节区的重定位节区名字 将是：.rel.text或者.rela.text。 |
| .rela name | SHT RELA |  |  |
| .rodata | SHT PROG BITS | SHF ALLOC | 这些节区包含只读数据，这些数据通常参与 |
| .rodata l | SHT\_PROG BITS | SHF\_ALLOC | 进程映像的不可写段。 |
| .shstrtab | SHT STRTAB |  | 此节区包含节区名称。 |
| .strtab | SHT STRTAB |  | 此节区包含字符串，通常是代表与符号表项 相关的名称。如果文件拥有一个可加载的 段，段中包含符号串表，节区的属性将包含 SHF ALLOC位， 否则该位为0。 |
| .symtab | SHT\_SYMTAB |  | 此节区包含一个符号表。如果文件中包含一 个可加载的段，并且该段中包含符号表，那 么节区的属性中包含SHF\_ALLOC位， 否则 该位置为0。 |
| .text | SHT PROG BITS | SHF\_ALLOC SHF EXEC INSTR | 此节区包含程序的可执行指令 |

## 2.6 ELF选项-l的基础理论

##### 2.6.1 选项- l的介绍

ELF 程序头是对二进制文件中段的描述，是程序装载必须的一部分。

* 段（segment) 是在内核装载时被解析的。
  + 主要作用就是描述磁盘上可执行文件的内存布局以及如何映射到内存中。
  + 可以通过引用原始的ELF头中名为： e\_phoff(程序头表的偏移量)的偏移量来得到程序头表。

基本的几个程序段内容如下：

* **PT\_LOAD段**

p\_type描述了段的类型。 一个可执行文件至少要有一个PT\_LOAD类型的段。 这类程序头描述的是可装载的段，

也就是说，这种类型的段会被装载或者映射到内存中。

一般来说，一个动态链接的ELF可执行文件通常包含两个可装载的段。 段类型都为PT\_LOAD

一个是存放程序代码的text段

另一个是存放全局变量和动态链接信息的data段。

上面两个段则会根据p\_align的对齐值在内存中对齐。并且映射到内存中。一般来说，TEXT段也称为代码段，权限一般都是可读可执行的。 对应取值就是PF\_READ\_EXEC，data段一般就是读写权限。 可以修改p\_flags来让我们的程序权限增大。

* **PT\_PHDR段**

此段一般位于elf文件的第一个段。PT\_PHDR段保存了程序头表本身的位置和大小。 phdr表保存了所有的phdr对文件（以及内存镜像）中段的描述信息。

* **PT\_INTERP段**

PT\_INTERP：存放一个以null结尾的字符串位置和大小信息，是对解释器位置的描述；

* **PT\_DYNAMIC段**

动态段是动态链接可执行文件所特有的，包含了动态链接器所需要的一些信息，它包括以下内容

运行时需要链接的共享库列表

* 全局偏移表(GOT)
* 重定位条目相关信息
* **PT\_NOTE**

可以保存于特定供应商或者系统相关附加信息，这个段在程序运行时是不需要的，因为系统会假设可执行文件是本地的，这个段很容易被感染

##### 2.6.2 选项- l的信息解释

-l 选项用于显示ELF文件中的程序头表和节区头表信息，其主要作用有：

1. 显示程序头表信息。程序头表描述ELF文件各个段(代码段、数据段等)在文件中的布局信息。
2. 显示节区头表信息。节区头表描述ELF文件各个节区(代码节、数据节等)在文件中的布局信息。
3. 帮助分析ELF文件 segments和sections的组织结构。

程序头表显示如下信息：

1. p\_type：表示程序段的类型信息，标识了段的类型
   1. 主要类型包括PT\_LOAD，PT\_DYNAMIC，PT\_INFERP
      1. PT\_LOAD类型的段会在创建进程时加载到内存中
      2. PT\_INFERP类型的段包含了.interp节，该节提供了加载二进制文件的解释器的名称
      3. PT\_DYNAMIC包含了.dynamic节，该节告诉解释器如何解析二进制文件用于执行
2. p\_offset：表示分段文件的偏移信息
3. p\_vaddr：表示段段虚拟地址信息
4. p\_paddr：表示段物理地址信息
5. p\_filesz：文件中段的大小
6. p\_memsz：内存中段段大小
7. p\_flags：段的标志信息
   1. 指示了段在运行时的访问权限，有三种重要的类型：
      1. PF\_X（可执行），PF\_W（可写），PF\_R（可读）
8. p\_align：段、文件、内存对齐信息：指定了段所需的内存对齐方式（字节为单位）
   1. 提供了二进制文件的段视图，ELF包括零或多个节，实际上就是把这些节捆绑成单个块
   2. 段提供的可执行视图，只有二进制文件会用到

## 2.7 ELF选项-d的基础理论

readelf -d

--dynamic

附加参数-d用于显示动态节区.dynamic的信息。

动态节区表保存了动态链接器所需要的基本信息，比如依赖于哪些共享对象、动态链接符号表的位置、动态链接重定位表的位置、共享对象初始化代码的地址等.

* d\_tag：表明了动态表项的类型。以下是一些常见的类型:
  + DT\_SYMTAB：表示动态链接符号表的地址，d\_ptr为.dynsym的地址
  + DT\_STRTAB：表示动态链接字符串表地址，d\_ptr为.dynstr的地址
  + DT\_STRSZ：动态链接字符串表大小，d\_val为大小
  + DT\_NEED：依赖的共享对象文件，d\_ptr表示依赖的共享对象文件名
  + DT\_REL：动态链接重定位表位置
* d\_val or d\_ptr：是一个联合体，要么表示一个值，要么表示一个地址，具体的情况因动态表的类型不同而不同

链接过程主要包含了三个步骤：

1. 地址与空间分配（Address and Storage Allocation）
2. 符号解析（Symbol Resolution）
3. 重定位（Relocation）

* **静态链接**

事实上，静态链接的过程就是上文所描述的过程。在Linux中，静态链接器（static linker）ld以一组可重定位目标文件和命令行参数作为输入，生成一个完全链接的、可以加载和运行的可执行目标文件作为输出。输入的可重定位目标文件由各种不同的节组成，每一节都是一个连续的字节序列。

* **动态链接**

静态链接使得进行模块化开发，大大提供了程序的开发效率。随着，程序规模的扩大，静态链接的诸多缺点也逐渐暴露出来，如：浪费内存和磁盘空间、模块更新困难等。在静态链接中，C语言静态库是很典型的浪费空间的例子。关于模块更新，静态链接的程序有任何更新，都必须重新编译链接，用户则需要重新下载安装该程序。

解决空间浪费和更新困难最简单的方法便是将程序的模块相互分割开来，形成独立文件。简而言之，就是不对那些组成程序的目标文件进行链接，而是等到程序要运行时才进行链接。

* **动态链接的基本实现**

动态链接涉及运行时的链接以及多个文件的装载，必需要有操作系统的支持。因为动态链接的情况下，进程的虚拟地址空间的分布会比静态链接情况下更为复杂，还有一些存储管理、内存共享、进程线程等机制在动态链接下也会有一些微妙的变化。

目前，主流操作系统都支持动态链接。在Linux中，ELF动态链接文件被称为 动态共享对象（DSO，Dynamic Shared Objects），一般以.so为后缀；在Windows中，动态链接文件被称为 动态链接库（Dynamic Linking Library），一般以.dll为后缀。

在Linux中，常用的C语言库的运行库glibc，其动态链接形式的版本保留在 /lib目录下，文件名为 libc.so。整个系统只保留一份C语言动态链接文件libc.so，所有的C语言编写的、动态链接的程序都可以在运行时使用它。当程序被装载时，系统的动态链接器会将程序所需要的所有动态链接库装载到进程的地址空间，并将程序中所有未解析的符号绑定到相应的动态链接库中，并进行重定位。

**共享库**（shared library）是致力于解决静态库缺陷的一个现代创新产物。共享库是一个目标模块，在运行或加载时，可以加载到任意的内存地址，并和一个在内存中的程序链接起来。这个过程称为**动态链接**（dynamic linking），是由一个叫做**动态链接器**（dynamic linker）的程序来执行的。共享库也称为**共享目标**（shared object），在 Linux 系统中通常用 .so 后缀来表示。微软的操作系统大量地使用了共享库，它们称为 DLL（动态链接库）。

共享库是以两种不同的方式来“共享”的。首先，在任何给定的文件系统中，对于一个库只有一个. so 文件。所有引用该库的可执行目标文件共享这个 .so 文件中的代码和数据，而不是像静态库的内容那样被复制和嵌入到引用它们的可执行的文件中。其次，在内存中，一个共享库的 .text 节的一个副本可以被不同的正在运行的进程共享。

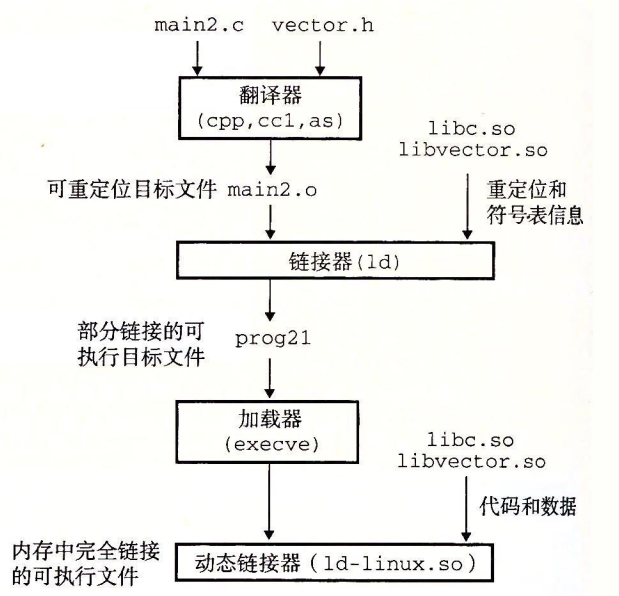


图 6动态链接共享库过程图

# 3系统设计

## 3.1 -h选项文件头表的数据结构设计

**我们主要以32位的数据结构作为主要实现方案。**

32位数据结构设计

typedef struct {

unsigned char e\_ident[16]; /\* ELF "magic数" \*/

unsigned char e\_type[2]; /\* 标识对象文件类型 \*/

unsigned char e\_machine[2]; /\* 指定所需的体系结构 \*/

unsigned char e\_version[4]; /\* 标识目标文件版本 \*/

unsigned char e\_entry[4]; /\* 入口点虚拟地址\*/

unsigned char e\_phoff[4]; /\* 程序头表文件偏移量 \*/

unsigned char e\_shoff[4]; /\* 节头表文件偏移量 \*/

unsigned char e\_flags[4]; /\* 特定于处理器的标志 \*/

unsigned char e\_ehsize[2]; /\* ELF头大小（以字节为单位） \*/

unsigned char e\_phentsize[2]; /\* 程序头表条目大小 \*/

unsigned char e\_phnum[2]; /\* 程序头表条目计数 \*/

unsigned char e\_shentsize[2]; /\* 节头表条目大小 \*/

unsigned char e\_shnum[2]; /\* 节头表项计数 \*/

unsigned char e\_shstrndx[2]; /\* 节头字符串表索引 \*/

} Elf32\_External\_Ehdr;

64位数据结构设计

/\*与Elf32\_External\_Ehdr 一致，不过适用于64位\*/

typedef struct {

unsigned char e\_ident[16]; /\* ELF "magic number" \*/

unsigned char e\_type[2]; /\* Identifies object file type \*/

unsigned char e\_machine[2]; /\* Specifies required architecture \*/

unsigned char e\_version[4]; /\* Identifies object file version \*/

unsigned char e\_entry[8]; /\* Entry point virtual address \*/

unsigned char e\_phoff[8]; /\* Program header table file offset \*/

unsigned char e\_shoff[8]; /\* Section header table file offset \*/

unsigned char e\_flags[4]; /\* Processor-specific flags \*/

unsigned char e\_ehsize[2]; /\* ELF header size in bytes \*/

unsigned char e\_phentsize[2]; /\* Program header table entry size \*/

unsigned char e\_phnum[2]; /\* Program header table entry count \*/

unsigned char e\_shentsize[2]; /\* Section header table entry size \*/

unsigned char e\_shnum[2]; /\* Section header table entry count \*/

unsigned char e\_shstrndx[2]; /\* Section header string table index \*/

} Elf64\_External\_Ehdr;

## -S选项节区头表的数据结构设计

**我们主要以32位的数据结构作为主要实现方案。**

32位数据结构设计

/\* 节区头表32位 \*/

typedef struct {

unsigned char sh\_name[4]; /\* 节名，字符串 tbl 中的索引 \*/

unsigned char sh\_type[4]; /\* 节头表的类型 \*/

unsigned char sh\_flags[4]; /\* 杂项节头表的属性 \*/

unsigned char sh\_addr[4]; /\* 执行时的节头虚拟地址\*/

unsigned char sh\_offset[4]; /\* 节头文件的偏移 \*/

unsigned char sh\_size[4]; /\* 节的大小（以字节为单位） \*/

unsigned char sh\_link[4]; /\* 另一节的索引\*/

unsigned char sh\_info[4]; /\* 附加节头信息 \*/

unsigned char sh\_addralign[4]; /\* 节头对齐 \*/

unsigned char sh\_entsize[4]; /\* 如果节头包含表的话条目大小 \*/

} Elf32\_External\_Shdr;

64位数据结构设计

/\* 节区头表64位 \*/

typedef struct {

unsigned char sh\_name[4]; /\* Section name, index in string tbl \*/

unsigned char sh\_type[4]; /\* Type of section \*/

unsigned char sh\_flags[8]; /\* Miscellaneous section attributes \*/

unsigned char sh\_addr[8]; /\* Section virtual addr at execution \*/

unsigned char sh\_offset[8]; /\* Section file offset \*/

unsigned char sh\_size[8]; /\* Size of section in bytes \*/

unsigned char sh\_link[4]; /\* Index of another section \*/

unsigned char sh\_info[4]; /\* Additional section information \*/

unsigned char sh\_addralign[8]; /\* Section alignment \*/

unsigned char sh\_entsize[8]; /\* Entry size if section holds table \*/

} Elf64\_External\_Shdr;

## 3.3 -l选项程序头表的数据结构设计

**我们主要以32位的数据结构作为主要实现方案。**

32位数据结构设计

/\* 程序头表 \*/

typedef struct {

unsigned char p\_type[4]; /\* 标识程序段类型 \*/

unsigned char p\_offset[4]; /\* 分段文件偏移 \*/

unsigned char p\_vaddr[4]; /\* 段虚拟地址 \*/

unsigned char p\_paddr[4]; /\* 段物理地址 \*/

unsigned char p\_filesz[4]; /\* 文件中的段大小 \*/

unsigned char p\_memsz[4]; /\* 内存中的段大小 \*/

unsigned char p\_flags[4]; /\* 段标志 \*/

unsigned char p\_align[4]; /\* 段对齐、文件和内存 \*/

} Elf32\_External\_Phdr;

64位数据结构设计

typedef struct {

unsigned char p\_type[4]; /\* 标识程序段类型 \*/

unsigned char p\_flags[4]; /\* 段标志 \*/

unsigned char p\_offset[8]; /\* 段文件偏移量 \*/

unsigned char p\_vaddr[8]; /\* 段虚拟地址 \*/

unsigned char p\_paddr[8]; /\* 段物理地址 \*/

unsigned char p\_filesz[8]; /\* 文件中的段大小 \*/

unsigned char p\_memsz[8]; /\* 内存中的段大小 \*/

unsigned char p\_align[8]; /\* 段对齐、文件和内存 \*/

} Elf64\_External\_Phdr;

## 3.4 -d选项动态链接表的数据结构设计

/\* 动态节区结构 \*/

/\*32位\*/

typedef struct {

unsigned char d\_tag[4]; /\* 条目标签值 \*/

union {

unsigned char d\_val[4];

unsigned char d\_ptr[4];

} d\_un;

} Elf32\_External\_Dyn;

/\*64位\*/

typedef struct {

unsigned char d\_tag[8]; /\* 条目标签值 \*/

union {

unsigned char d\_val[8];

unsigned char d\_ptr[8];

} d\_un;

} Elf64\_External\_Dyn;

# 4系统实现

## 4.1 -h选项文件头表的程序设计

图示

描述已自动生成

图 7 选项-h实现程序流程图

以上功能大致代码实现如下：

如果需要完整代码请查看附录或前往我们的Github开源地址进行下载

1. /\*读取文件头\*/

2. /\*头文件信息在Magic 数中\*/

3. int ELF\_process::process\_file\_header(void)

4. {

5. /\*判断是否Magic是否存在问题\*/

6. if ( elf\_header.e\_ident[EI\_MAG0] != ELFMAG0

7. || elf\_header.e\_ident[EI\_MAG1] != ELFMAG1

8. || elf\_header.e\_ident[EI\_MAG2] != ELFMAG2

9. || elf\_header.e\_ident[EI\_MAG3] != ELFMAG3)

10. {

11. printf("Not an ELF file - it has the wrong magic bytes at the start\n");

12. return 0;

13. }

14. /\*输出M相关参数\*/

15. printf("ELF Header:\n");

16. printf(" Magic: ");

17. for (int i = 0; i <EI\_NIDENT ; ++i)

18. printf ("%2.2x ", elf\_header.e\_ident[i]); /\*读取Magic 数\*/

19. printf("\n");

20. printf(" Class: %s\n",

21. get\_elf\_class(elf\_header.e\_ident[EI\_CLASS]));

22.

23. printf (" Data: %s\n",

24. get\_data\_encoding (elf\_header.e\_ident[EI\_DATA]));

25. const char \*str=elf\_header.e\_ident[EI\_VERSION] == EV\_CURRENT ?

26. "(current)" : (elf\_header.e\_ident[EI\_VERSION] != EV\_NONE ? "<unknown>" : "");

27. printf (" Version: %d %s\n",

28. elf\_header.e\_ident[EI\_VERSION],str);

29. printf (" OS/ABI: %s\n",

30. get\_osabi\_name (elf\_header.e\_ident[EI\_OSABI]));

31.

32. printf (" ABI Version: %d\n",

33. elf\_header.e\_ident[EI\_ABIVERSION]);

34.

35. printf (" Type: %s\n",

36. get\_file\_type (elf\_header.e\_type));

37.

38. printf (" Machine: %s\n",

39. get\_machine\_name (elf\_header.e\_machine));

40.

41. printf (" Version: 0x%lx\n",

42. (unsigned long) elf\_header.e\_version);

43.

44. printf (" Entry point address: 0x%x",elf\_header.e\_entry);

45.

46. printf ("\n Start of program headers: %d",elf\_header.e\_phoff);

47.

48. printf (" (bytes into file)\n Start of section headers: %d",elf\_header.e\_shoff);

49. printf (" (bytes into file)\n");

50.

51. printf (" Flags: 0x%lx\n",(unsigned long)elf\_header.e\_flags);

52.

53. printf (" Size of this header: %ld (bytes)\n",(long)elf\_header.e\_ehsize);

54.

55. printf (" Size of program headers: %ld (bytes)\n",(long)elf\_header.e\_phentsize);

56.

57. printf (" Number of program headers: %ld\n",(long)elf\_header.e\_phnum);

58.

59. printf (" Size of section headers: %ld (bytes)\n",

60. (long) elf\_header.e\_shentsize);

61.

62. printf (" Number of section headers: %ld\n",

63. (long) elf\_header.e\_shnum);

64.

65. if (section\_headers != NULL && elf\_header.e\_shnum == SHN\_UNDEF)

66. printf (" (%ld)", (long) section\_headers[0].sh\_size);

67.

68. printf (" Section header string table index: %ld\n",

69. (long) elf\_header.e\_shstrndx);

70.

71. return 1;

73. }

74.

## 4.2 -S选项节区头表的程序设计

图示

描述已自动生成

图 8选项-S实现程序流程图

以上功能大致代码实现如下：

如果需要完整代码请查看附录或前往我们的Github开源地址进行下载

1. //如果是-S或-e指令，显示节头信息和全部头信息

2. else if((option & (1<<2) ) || (option & (1<<6))) //-S || -e

3. {

4.

5. //打印列名

6. printf(" [Nr] Name Type Addr Off Size ES Flg Lk Inf Al\n");

7. //遍历节区头表的所有项，每一个项都对应一个节区

8. for (int i = 0; i < elf\_header.e\_shnum; i++, section++)

9. {

10. printf (" [%2u] ", i);

11.

12. //计算该节区名在shstrtab中的偏移地址

13. countC = flag\_shoff + section->sh\_name;

14.

15. //将文件指针移动到这个地方

16. fseek(file,countC,SEEK\_SET);

17. //名字字符串，长度为20，名字以'\0'结尾，所以多读一些没有关系

18. char string\_name[20];

19. //从文件中读取名字字符串

20. fread(string\_name,20,1,file);

21.

22. //判断节区名是不是"IA\_64",记录unwind节区的索引

23. if(!strcmp(string\_name,"IA\_64")) unwind\_idx=i;

24. //判断节区名和目标的节区名是否一致，相同的话记录目标节区名对应的索引，这个是给-x用的

25. if(!strcmp(string\_name,target\_section\_name)) target\_section\_idx=i;

26.

27. //打印输出节区名

28. printf("%-16s ",string\_name);

29.

30.

31. //打印输出节区类型

32. printf ( " %-15.15s ",

33. get\_section\_type\_name (section->sh\_type));

34.

35. //打印输出节区虚拟地址、文件中偏移地址、节区大小、节区条目大小

36. printf("%6.8lx",(unsigned long) section->sh\_addr);

37. printf ( " %6.6lx %6.6lx %2.2lx",

38. (unsigned long) section->sh\_offset,

39. (unsigned long) section->sh\_size,

40. (unsigned long) section->sh\_entsize);

41.

42. //如果节区有标志位那么就打印输出标志

43. if (section->sh\_flags)

44. printf (" %2.2x ", section->sh\_flags);

45. //否则用空格填充

46. else

47. printf("%4c",32);

48.

49. //打印输出sh\_link和sh\_info，这个因不同节区类型而异，最后输出对齐信息

50. printf ("%2u ", section->sh\_link);

51. printf ("%3u %3lu", section->sh\_info,

52. (unsigned long) section->sh\_addralign);

53.

54. //如果节区名是.dynamic动态链接信息表，那么需要记录节区的偏移地址和大小

55. if (strcmp(string\_name,".dynamic")==0)

56. {

57. dynamic\_addr = section->sh\_offset;

58. dynamic\_size = section->sh\_size;

59. }

60.

61. //如果节区名是.rel.dyn动态链接重定位表，那么需要记录节区的偏移地址和大小

62. if (strcmp(string\_name,".rel.dyn")==0)

63. {

64. rel\_dyn\_offset = section->sh\_offset;

65. rel\_dyn\_size = section->sh\_size;

66. }

67.

68. //如果节区名是.dynsym动态链接符号表，那么需要记录节区的偏移地址和大小

69. if(strcmp(string\_name,".dynsym")==0)

70. {

71. sym\_dyn\_offset = section->sh\_offset;

72. sym\_dyn\_size = section->sh\_size;

73. }

74.

75. //如果节区名是.dynstr动态链接字符表，那么需要记录节区的偏移地址和大小

76. if(strcmp(string\_name,".dynstr")==0)

77. {

78. str\_dyn\_offset = section->sh\_offset;

79. str\_dyn\_size = section->sh\_size;

80. }

81.

82. printf("\n");

83.

84. }

85. }

86.

## 4.3 -l选项程序头表的程序设计

图示

描述已自动生成

图 9选项-l实现程序流程图

以上功能大致代码实现如下：

如果需要完整代码请查看附录或前往我们的Github开源地址进行下载

1. int ELF\_process::process\_program\_headers(FILE \*file)

2. {

3.

4. Elf32\_Phdr\* segment;

5. unsigned long dynamic\_addr;

6. if(elf\_header.e\_phnum == 0)

7. {

8.

9. if(elf\_header.e\_phoff!=0)

10. {

11. printf ("possibly corrupt ELF header - it has a non-zero program"

12. " header offset, but no program headers");

13. }

14. else

15. {

16. printf ("\nThere are no program headers in this file.\n");

17. return 0;

18. }

19.

20. }

21. else

22. {

23. /\*打印相关的信息\*/

24. if(elf\_header.e\_phnum>1)

25. printf ("\nProgram Headers:\n");

26. else

27. printf ("\nProgram Header:\n");

28.

29. if(is\_32bit\_elf)

30. printf(" Type Offset VirtAddr PhysAddr FileSiz MemSiz Flg Align\n");

31. else

32. printf(" Type Offset VirtAddr PhysAddr FileSiz MemSiz Flg Align\n");

33.

34. }

35.

36. /\*获取程序段头表信息\*/

37. if (! get\_program\_headers (file))

38. return 0;

39.

40.

41. unsigned int i;

42. for (i = 0, segment = program\_headers;

43. i < elf\_header.e\_phnum;

44. i++, segment++)

45. {

46. printf (" %-14.14s ", get\_segment\_type (segment->p\_type));

47.

48. if(is\_32bit\_elf) /\*如果是32位的话，那么输出程序段的相关信息\*/

49. {

50. printf ("0x%6.6x ", (unsigned int) segment->p\_offset);

51. printf ("0x%8.8x ", (unsigned int) segment->p\_vaddr);

52. printf ("0x%8.8x ", (unsigned int) segment->p\_paddr);

53. printf ("0x%5.5x ", (unsigned int) segment->p\_filesz);

54. printf ("0x%5.5x ", (unsigned int) segment->p\_memsz);

55. printf ("%c%c%c ",

56. (segment->p\_flags & PF\_R ? 'R' : ' '),

57. (segment->p\_flags & PF\_W ? 'W' : ' '),

58. (segment->p\_flags & PF\_X ? 'E' : ' '));

59. printf ("%#x", (unsigned int) segment->p\_align);

60. }

61.

62. printf("\n");

63.

64. }

65.

66. return 0;

67. }

68.  

## 4.4 -d选项动态链接的程序设计

图示, 工程绘图

描述已自动生成

图 10选项-d实现程序流程图

以上功能大致代码实现如下：

如果需要完整代码请查看附录或前往我们的Github开源地址进行下载

1. int ELF\_process::process\_dynamic\_section(FILE \*file)

2. {

3. // 定义指向Elf32\_Dyn结构的指针entry

4. Elf32\_Dyn \* entry;

5.

6. if(dynamic\_addr) // 如果dynamic\_addr非空

7. {

8. // 打印动态节的偏移地址和条目数

9. printf ("\nDynamic section at offset 0x%x contains %u entries:\n",

10. dynamic\_addr, dynamic\_nent);

11. // 打印表头

12. printf (" Tag Type Name/Value\n");

13. }else{

14. // 文件中没有动态节

15. printf ("\nThere are no dynamic section in this file.\n");

16. return 0;

17. }

18. // 如果是32位ELF文件

19. if (is\_32bit\_elf)

20. {

21. // 调用get\_32bit\_dynamic\_section函数获取32位动态节

22. if (! get\_32bit\_dynamic\_section (file))

23. return 0;

24. }

25. // 如果是64位ELF文件，调用get\_64bit\_dynamic\_section函数获取64位动态节

26. else if (! get\_64bit\_dynamic\_section (file))

27. return 0;

28.

29. // 遍历动态节的每一条目

30. for (entry = dynamic\_section;

31. entry < dynamic\_section + dynamic\_nent;

32. entry++)

33. {

34. const char \* dtype; // 定义记录条目的动态类型的指针

35. // 输出空格

36. putchar (' ');

37. printf("0x%2.8x ",entry->d\_tag); // 打印条目的标签

38. dtype = get\_dynamic\_type(entry->d\_tag); // 获取条目的动态类型

39. // 打印动态类型

40. printf("(%s)%\*s",dtype,(int)(27-strlen(dtype))," ");

41.

42. // 根据条目的标签进行判断

43. switch (entry->d\_tag)

44. {

45. case DT\_FLAGS: // 如果标签是DT\_FLAGS

46. // 调用print\_dynamic\_flags函数打印动态标志

47. print\_dynamic\_flags (entry->d\_un.d\_val);

48. break;

49.

50. case DT\_AUXILIARY:

51. case DT\_FILTER:

52. case DT\_CONFIG:

53. case DT\_DEPAUDIT:

54. case DT\_AUDIT: // 如果标签是DT\_AUXILIARY、DT\_FILTER、DT\_CONFIG、DT\_DEPAUDIT或DT\_AUDIT

55. switch (entry->d\_tag) // 根据标签进行判断

56. {

57. case DT\_AUXILIARY:

58. printf ("Auxiliary library"); // 辅助库

59. break;

60.

61. case DT\_FILTER:

62. printf ("Filter library"); // 过滤器库

63. break;

64.

65. case DT\_CONFIG:

66. printf ("Configuration file"); // 配置文件

67. break;

68.

69. case DT\_DEPAUDIT:

70. printf ("Dependency audit library"); // 依赖审核库

71. break;

72.

73. case DT\_AUDIT:

74. printf ("Audit library"); // 审计库

75. break;

76. }

77. break;

78.

79. default:

80. printf("0x%x",entry->d\_un.d\_val); // 默认情况下打印条目的值

81. }

82.

83. printf("\n");

84. }

85. }

86.

# 5系统测试

## 5.1测试用例设计

对于-h，-S和-l指令设计的测试代码如下：

1. #include <iostream>

2.

3. using namespace std;

4.

5.

6. int main(){

7. int a = 1;

8. cout << "Hello Linux!!HZAU\n";

9. return 0;

10. }

11.

对于选项-d设计的测试代码如下

1. #include<stdio.h>

2. int cnt = 0;

3. int func(){

4. cnt++;

5. printf("%d\n",cnt);

6. }

7.

Main函数

1. extern void func();

2. extern int cnt;

3.

4. int main(){

5. func();

6. }

7.

## 5.2测试结果及分析

##### 5.2.1 选项- h的测试与样例解释

编译产生.so文件

g++ -o test-h.so test-h.cpp

使用./main test-h.so -h 查看头文件信息

文本

描述已自动生成

图 11 运行查看-h选项后的信息显示图

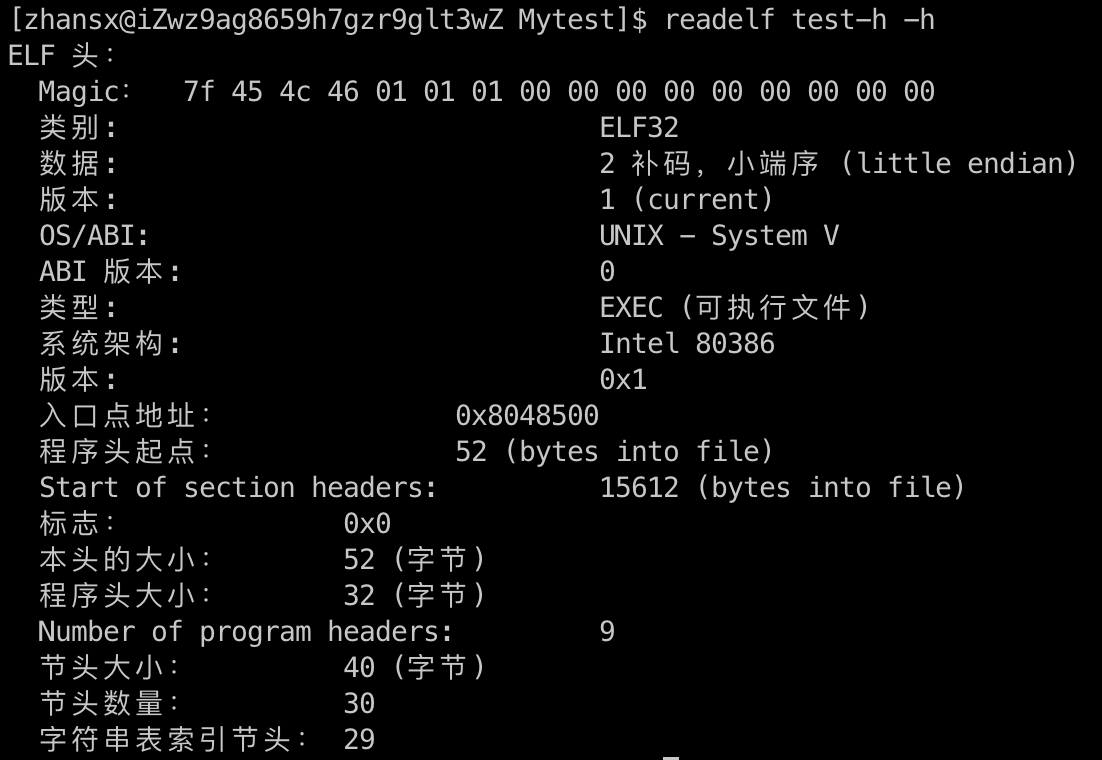


图 12运行readelf查看-h选项后的信息显示图

可以发现，我们的程序与ELF进行对比后，可以正确实现选项-h的内容。

对如上Magic魔数信息的解释：

* 第1个字节：0x7f 表示ELF标记
* 第2个字节：‘E’
* 第3个字节：‘L’
* 第4个字节：‘F’
* 第5个字节：ELF文件类型，也就是class
* 第6个字节：数据编码信息，字节序信息，大端序、小端序
* 第7个字节：ELF版本号：标识ELF Version, 该值等于EV\_CURRENT
* 第8个字节：OS信息
* 第9个字节：ABI 版本信息
* 第10~16个字节：填充位

##### 5.2.2 选项- S的测试与样例解释

首先我们查看文件头信息

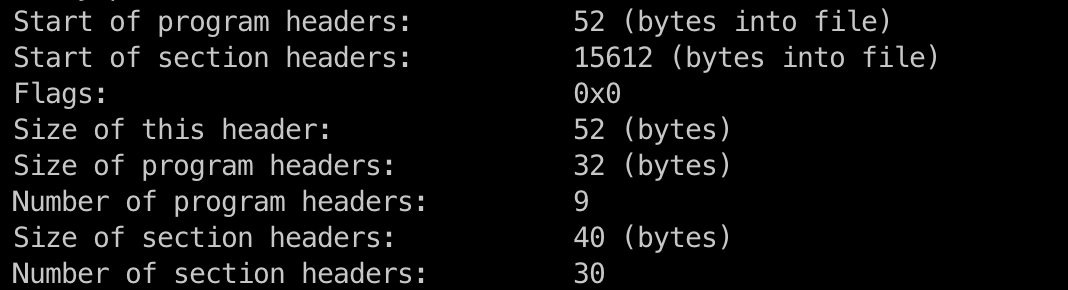


图 13 文件头信息(部分)图

从中可以发现节头表的开始偏移位置位15612字节，每个节头表的大小为40字节，一共有30个节点头表。

* 使用./main test-h.so -S 查看节信息，如下所示：

图片包含 文本

描述已自动生成

图 14 节区头表信息展示图

idex为0的位置：



图 15 索引为0位置的节区图

可以看到 index=0 的 Section Header，内容全部为0。（在某些情况下，它的某部分字段不为0，这些特殊情况当前先跳过） 这是一个非常特别的 Section Header，它的作用是表示 undefined 。它的 index（=0） 也有一个特别的名字，叫 SHN\_UNDEF。

使用hexdump查看索引为0的位置的物理地址信息

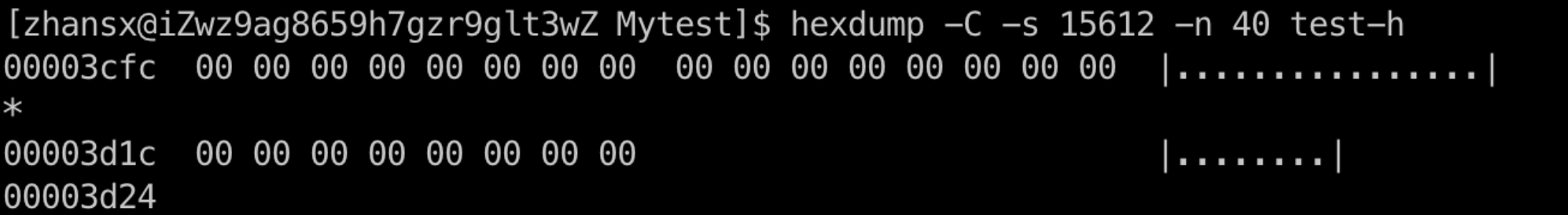


图 16 hexdump查看索引为0位置的物理信息图

那么程序的可执行段在哪个位置呢？答案就在.text节区

现在我们查看.text节区



其偏移地址为16132，长度为40

图形用户界面, 文本, 应用程序

描述已自动生成

图 17hexdump查看索引为.text节区的物理信息图

* 首先前4个字节表示的是sh\_name：

92 00 00 00

值为 90 00 00 00 + little endian = 0x92 = 146

* 接下来的4个字节表示sh\_type

01 00 00 00

值为：“01 00 00 00” + little endian = 0x1 对照表，1对应的类型是 SHT\_PROGBITS，表示这部分的信息，格式和意义完全由程序来定义。内容可以是已初始化的数据，未初始化的数据，comment 或者是程序代码等。

* 接下来的4个字节表示sh\_flag

06 00 00 00

值为：“06 00 00 00” + little endian = 0x6 = SHF\_ALLOC | SHF\_EXECINSTR => 这部分是可执行代码，进程运行时需要放置在内存中。 再对照回 Section Header 列表中 “.text” 那一行

[13] .text PROGBITS 08048500 000500 000245 00 AX 0 0 16

所以可以发现 “.text” 对应的就是 A (alloc), X (execute)。

* 接下来的4个字节表示sh\_addr

00 85 04 08

Section 存放于进程内存映像中的虚存地址，如果 Section 不需要出现在内存中，则为0。Relocatable file 的虚存地址都为0。Executable file 和 Shared object file 才会为有需要的 Section 计算虚存地址。 地址计算为 00 85 04 08 + little endian = 08 04 85 00

* 接下来的4个字节为section在文件中的字节偏移量

00 05 00 00

00 00 05 00 + little endian = 0x500 = 5 \* 16^3 = 20480

* 接下来4个字节表示sh\_size

表示 Section 在文件中占据的字节数。 类型为 NOBITS 的 Section，即使这个值不为0，它在文件中也不占据空间。".bss" Section 就是这个类型。bss 全称为 “block started by symbol”（更简单的记法是：Better Save Space），存放的是未初始化的数据，因为数据无初始值，所以只需要记录它在内存中占据的空间即可，在文件中不需要额外的存储。相反，".data" Section 存储的则是已经初始化的数据，所以需要在文件中记录下初始值，才能在进程内存映像中把这些值带进去。

45 02 00 00

45 02 00 00 + little endian = 00 00 02 45 = 2 \* 16^2 + 4 \* 15 + 5 = 577

* 紧接着的4个字节表示sh\_link

包含另外一个 Section Header 的 index，具体的含义取决于 Section 的类型

00 00 00 00

* 后面4个字节就表示sh\_info

包含了额外的信息，具体的含义取决于 Section 的类型。 需要把 sh\_type，sh\_link 和 sh\_info 联合在一起进行解析。 另外，当 sh\_flags=SHF\_INFO\_LINK 时，sh\_info 则表示另外一个 Section Header 的 index。

00 00 00 00

* 最后8个字节，分别表示sh\_addralign和sh\_entsize
* 前4个字节表示sh\_addralign 表示对齐约束。0或1表示无约束。sh\_addr % sh\_addralign 必须等于0

10 00 00 00

* 后4个字节表示sh\_entsize

有些 Section 会包含一组大小固定的记录，这时 sh\_entsize 就表示记录的大小，通过 sh\_size / sh\_entsize 就能得到记录的个数。如果 Section 没有包含这种类型的记录，则值为0。比如后面会看到的 “.shstrtab” Section，包含的是一组 string，但 string 的长度不一样，于是 sh\_entsize 的值就为0。

00 00 00 00

* 我们再来反复看一下.text节

[13] .text PROGBITS 08048500 000500 000245 00 AX 0 0 16

由此可以得出

1. offset = 0x500 = 20480
2. size = 0x0245 = 577
3. flag = AX => 进程运行期间占据内存 + 这部分是可执行的指令 => 可执行

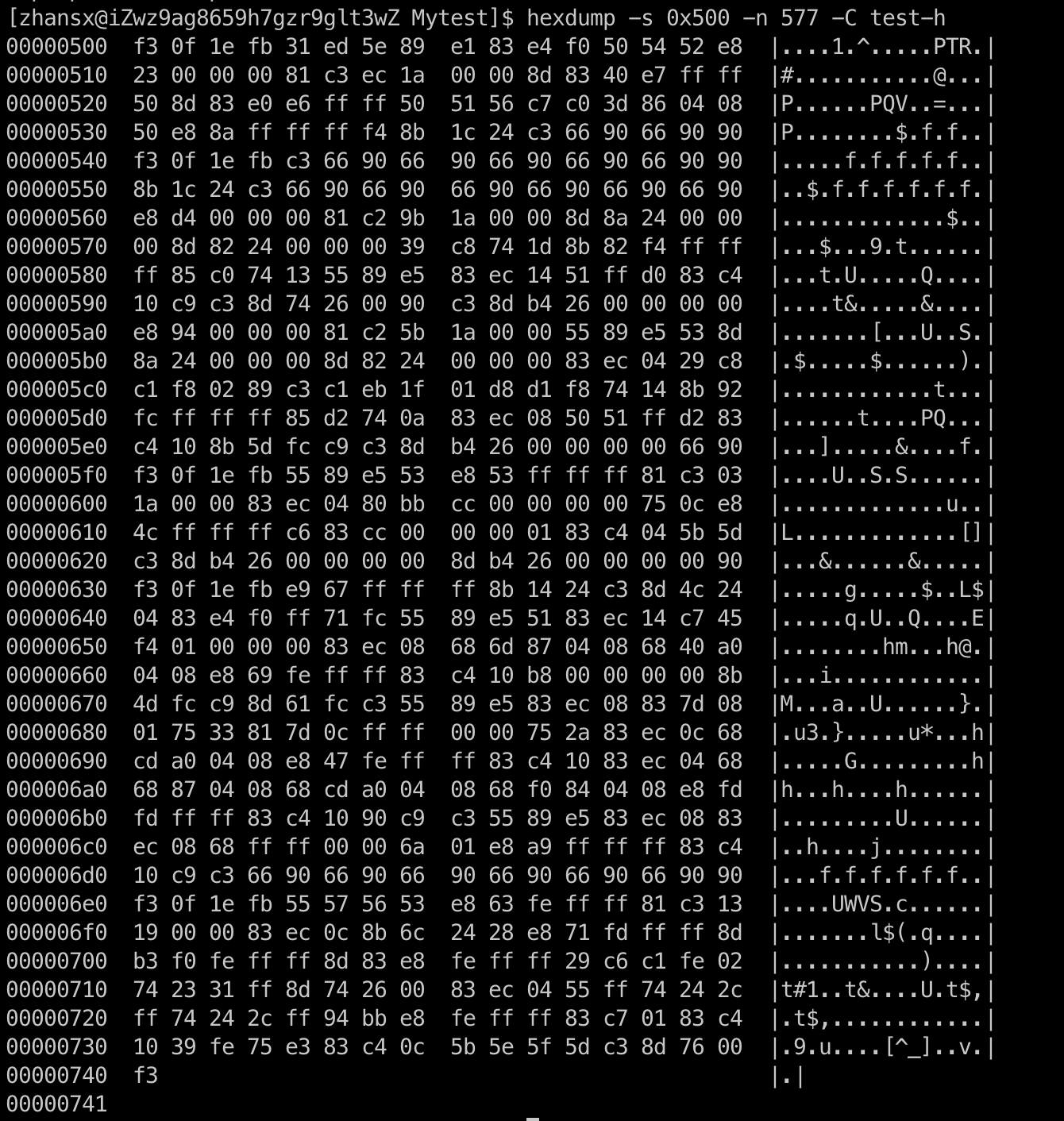


图 18 .text节区的可执行区在物理地址中的信息

可以使用objdump查看其中的内容，红框部分便是mian函数反编译后的结果

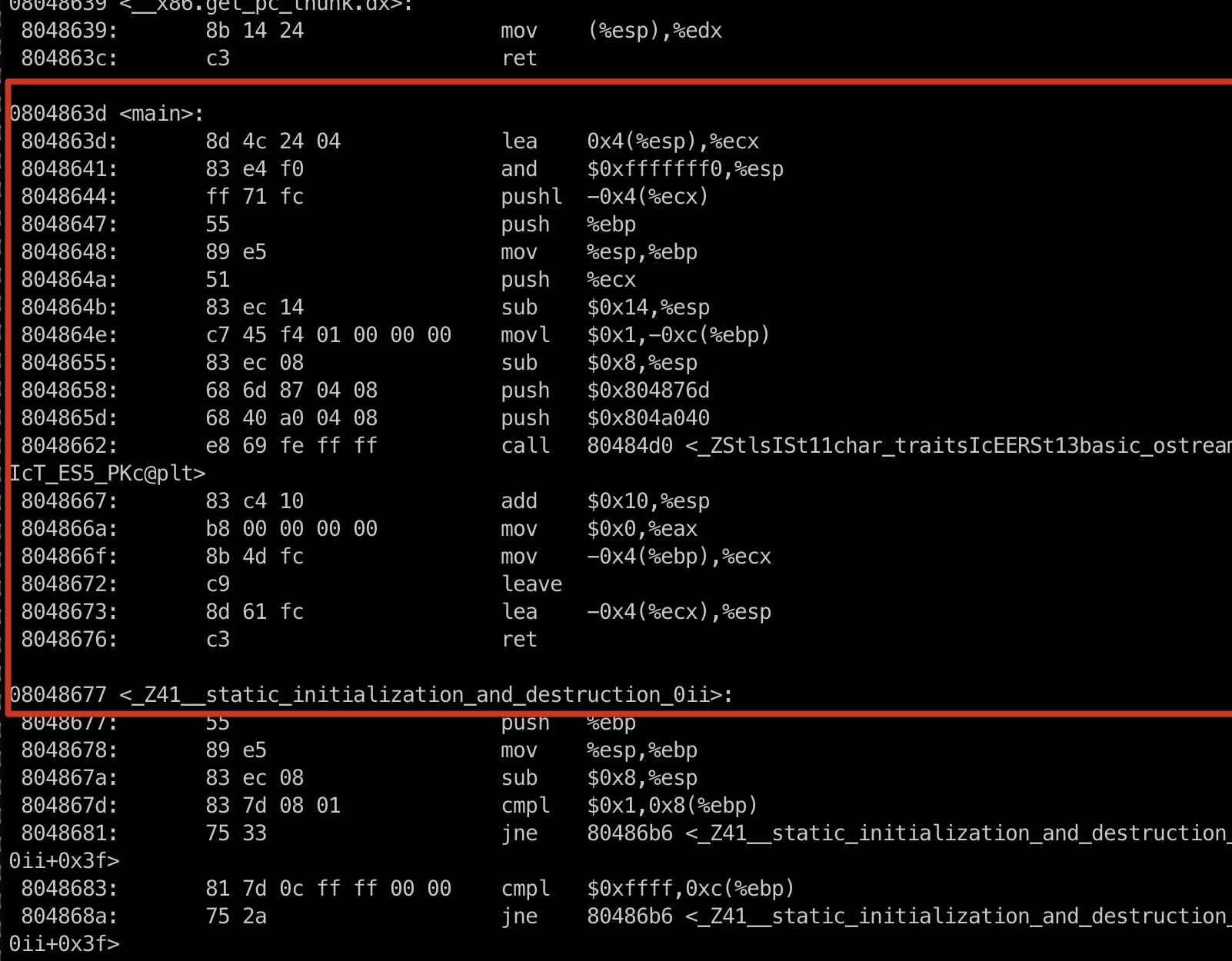


图 19 objdump反编译后的main函数代码图

* Section .rodata：这些节区包含只读数据，这些数据通常参与

[15] .rodata PROGBITS 08048760 000760 000020 00 A 0 0 4

由此可以得出

1. offset = 0x760
2. size = 0x20 = 32
3. flag = A => 进程运行期间占据内存 => 只读

这里的只读数据为输出内容

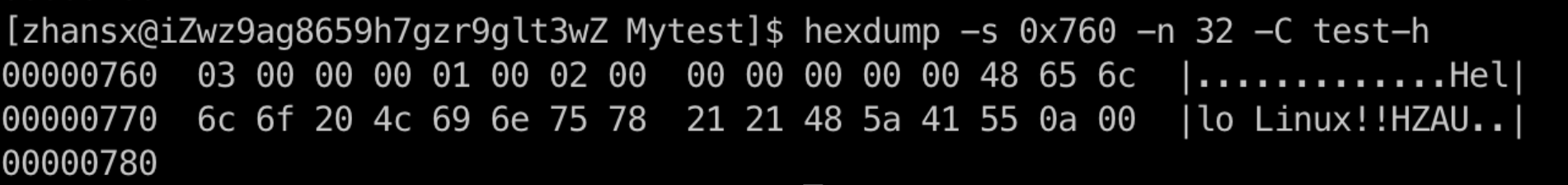


图 20.rodata节区物理地址信息图

结合代码可以发现，该部分存储的为

Cout << “Hello Linux!! HZAU”

的内容

* Section .comment：这个 Section 包含了版本控制信息。

[25] .comment PROGBITS 00000000 001024 00002d 01 MS 0 0 1

1. offset = 0x1024

2. size = 0x2d = 2\*16 + 14 = 46

3. flag = WA => 进程运行期间可写 + 进程运行期间占据内存 => 可读写

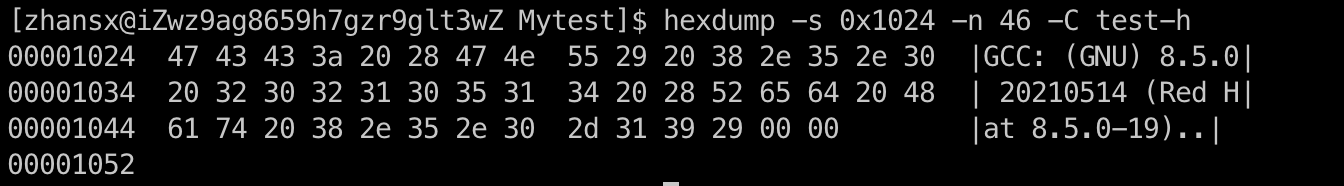


图 21.comment节区物理地址信息图

##### 5.2.3 选项- l的测试与样例解释

使用./main test-h -l 查看节区信息

文本

描述已自动生成

图 22程序头表信息展示图

* Flg标志的含义：
  + R:可读段
  + W:可写段
  + X:可执行段
* Align对齐方式的含义：
  + 段对齐,表示段在文件和内存中的对齐方式。常见的对齐方式有:
  + 0x1:1字节对齐
  + 0x2:2字节对齐
  + 0x4:4字节对齐
  + 0x8:8字节对齐
  + 0x10:16字节对齐
  + 更大的对齐数表示更严格的对齐方式。
  + 对齐方式会影响段在文件和内存中的起始地址,起始地址会是对齐数的整数倍。

如上可知，程序段的名字的内容如下：

1. PHDR:程序头表段，描述ELF文件中的程序头表段。
2. INTERP:程序解释器名,描述动态链接器的路径名。
3. LOAD:可加载段,描述可映射到内存中的段信息。

这里有两个LOAD段,第一个是只读段,第二个是读写段。

1. DYNAMIC:动态链接信息,描述动态链接信息。
2. NOTE:注释段,包含一些注释信息。
3. GNU\_EH\_FRAME:异常帧信息,包含堆栈中的异常处理信息。
4. GNU\_STACK:堆栈段,标记堆栈的可执行性。
5. GNU\_RELRO:只读数据段,标记的数据段中的只读部分。

##### 5.2.4 选项- d的测试与样例解释

我们先编写测试代码。要实现动态链接的方式，我们需要定义库函数，实现打印输出的功能，同时，这个库也使用外部库stdio的printf符号。lib.c代码如下：

1. #include<stdio.h>

2. int cnt = 0;

3. int func(){

4. cnt++;

5. printf("%d\n",cnt);

6. }

接下来对这段代码进行编译，使用-fPIC指令让其编译为位置无关的代码，作为动态链接库lib.so使用。

dp@ubuntu:~/Desktop/elf/share$ gcc -shared -fpic -o lib.so lib.c

然后我们编写主测试程序，这个程序引用这个动态链接库的cnt变量和func函数。main.c代码如下：

1. extern void func();

2. extern int cnt;

3.

4. int main(){

5. func();

6. }

然后进行编译为可执行文件，下面编译中使用库文件，不是为了将库中代码段和数据段合并入可执行文件，而仅仅只是传递符号表和重定位信息告诉可执行文件这里可以进行动态重定位。

dp@ubuntu:~/Desktop/elf/share$ gcc -m32 -o main main.c lib.so

最后进行执行，执行的时候需要修改环境变量，将当前目录下的动态链接文件添加到环境变量中去。

dp@ubuntu:~/Desktop/elf/share$ export LD\_LIBRARY\_PATH=$LD\_LIBRARY\_PATH:./

dp@ubuntu:~/Desktop/elf/share$ ./main

1

自此完成了测试程序的编写，上面的解释将基于这个测试程序。

# 6结论与体会

## 6.1结论

在本次项目中，我们设计并实现了一个ELF文件解析器，该解析器能够解析ELF格式的文件，我作为小组长，在进行小组实训项目策划的同时，在我的部分我实现了-h、-S、-l和-d指令的功能。

在项目设计中，我将ELF文件解析器划分为几个功能模块，每个模块负责处理特定的指令。首先是-h指令，它允许用户查看ELF文件的文件头信息。我实现了解析文件头的功能，提取出了文件的基本信息，如文件类型、入口地址、段表偏移等，并将这些信息以易读的方式展示出来。再来是-S指令，它用于显示ELF文件的节表。我通过解析节头表，将文件中的各个节的信息提取出来，并以表格的形式呈现给用户。用户可以查看节的名称、偏移地址、大小等重要信息，从而更好地了解ELF文件的结构。至于-l指令，它用于显示ELF文件的重定位信息。在实现这个功能时，我解析了重定位节和符号表，将重定位的目标符号和重定位类型提取出来，并展示给用户。这样用户可以查看ELF文件中的重定位信息，了解符号和地址之间的关系。最后是-d指令，它用于显示ELF文件的动态链接信息。我实现了解析动态节和动态符号表的功能，提取出动态链接库的名称、版本等重要信息，并展示给用户。通过这个功能，用户可以了解ELF文件的动态链接情况，以及与其他动态链接库的依赖关系。

## 6.2个人体会

“纸上谈来终觉浅，绝知此事要躬行”从理论到具体实现。首先我对ELF文件格式进行了深入的学习和理解。ELF文件是一种常见的可执行文件和目标文件格式，它包含了程序在连接和执行过程中所需的重要信息。通过学习ELF文件格式，我对文件结构、节、段、符号表等概念有了更清晰的认识。

通过本次实训实现这些功能，我的ELF文件解析器能够帮助用户更好地理解和分析ELF文件。用户可以通过指定相应的指令，查看文件头信息、节表、重定位信息和动态链接信息，从而深入了解ELF文件的结构和属性。通过实现不同指令的功能，我提高了自己的编程和算法设计能力。解析ELF文件涉及到复杂的数据结构和算法，例如解析节表、符号表和重定位表等。通过编写高效的解析代码，我不仅加深了对这些概念的理解，还提升了自己的编程技巧。

在项目的过程中，我遇到了一些挑战和困难。首先是理解和解析ELF文件格式的复杂性，需要仔细阅读规范和文档，并理解不同部分之间的关系。其次是设计和实现解析器的算法和数据结构，以便高效地解析和提取ELF文件的信息。我在这些方面花费了大量的时间和精力，进行了反复的学习和实践，最终成功地完成了解析器的设计和实现。

在团队协作方面，通过这个项目，我锻炼了团队合作和沟通能力。在项目中，我与团队成员进行了讨论和分工，确保每个人都能贡献自己的技能和专长。我们共同解决了一些技术难题，共享经验和知识，使项目得以顺利完成。与此同时，我们使用Git工作流，将工程项目进行开源共享，并且更加方便我们团队成员进行修改和溯源，采用Github工作流对于我们的项目来说具有重要意义。它提供了一个集中、协作和可追踪的平台，使得团队成员可以更加高效地合作，管理和追踪项目的进展，并与其他开发者进行交流和分享。通过这种方式，我们能够更好地组织和管理我们的项目，提高工作效率，以及促进项目的成功完成。

最后，我通过编写项目总结和报告的过程，通过进行PPT答辩以及撰写报告，进一步强化了自己的沟通和表达能力。通过将项目的设计和实现过程以及取得的成果进行详细的描述和总结，我不仅可以向他人清晰地展示我的工作，还可以反思和总结自己的经验和教训，以便在今后的项目中改进和提升。

总而言之，通过完成ELF文件解析器的设计和实现，我不仅实现了-h、-S、-l和-d指令的功能，还获得了深入理解ELF文件格式和程序链接的能力。同时，我也提高了编程和算法设计能力，锻炼了团队合作和沟通技巧，以及加强了自己的报告撰写以及表达能力。这个项目为我今后的学习和职业发展打下了坚实的基础，让我更加自信和有能力应对更复杂的编程任务和挑战。

**致谢：**

感谢任老师和李老师的指导和陪伴！老师辛苦了！

# 7参考文献

1. 陈逸鹤. 程序员的自我修养. 北京：清华大学出版社，2017. 40-168
2. ELF文件详解. 爱笑的林羽. <https://blog.csdn.net/qq_42875402/article/details/106963323>
3. （美）布赖恩特（Bryant,R.E.）. 深入理解计算机系统(原书第3版). 北京：机械工业出版社，2016. 70-280
4. ELF文件格式. By7e\_f@lc0n. <https://blog.csdn.net/m0_73644864/article/details/129899412>
5. 计算机那些事. 楚权的世界. http://chuquan.me/
6. elf-parser. marler8997,TheCodeArtistmarler8997. <https://github.com/TheCodeArtist/elf-parser>

# 8 附录

完整代码实现 ELF\_process.cpp

完整头文件可以前往我们的Github开源仓库进行下载：<https://github.com/Jasaxion/LinuxELF_FileParse>

1. #include <elf.h>

2. #include <cstring>

3. #include "ELF\_process.h"

4. #define file\_name "/home/hx/cProgram/Process/libhello-jni.so"

5. //将原始的小端字数据，转换为大端数据，与结构体对齐

6. #define BYTE\_GET(field) byte\_get\_little\_endian (field,sizeof(field))

7. static int is\_32bit\_elf;

8. Elf32\_Ehdr elf\_header;

9. Elf32\_Shdr\* section\_headers;

10. Elf32\_Phdr\* program\_headers;

11. Elf32\_Sym\* sym\_dyn;

12.

13. static unsigned int dynamic\_addr;

14. static unsigned int dynamic\_offset;

15. unsigned int dynamic\_strings;

16. unsigned int dynamic\_size;

17. static unsigned int rel\_nent;

18. static unsigned int rel\_dyn\_offset;

19. static unsigned int rel\_dyn\_size;

20. static unsigned int sym\_dyn\_offset;

21. static unsigned int sym\_dyn\_size;

22. static unsigned int str\_dyn\_offset;

23. static unsigned int str\_dyn\_size;

24. unsigned int sym\_nent;

25. Elf32\_Dyn\* dynamic\_section;

26.

27. int unwind\_idx,target\_section\_idx;

28.

29. static unsigned int dynamic\_nent;

30.

31. #define NT\_GNU\_PROPERTY\_TYPE\_0 5

32. #define SHT\_PARISC\_ANNOT 0x70000003

33. #define SHT\_PARISC\_SYMEXTN SHT\_LOPROC + 8

34. #define SHT\_PARISC\_STUBS SHT\_LOPROC + 9

35. #define SHT\_PARISC\_DLKM 0x70000004

36.

37. #define PT\_PARISC\_WEAKORDER 0x70000002

38. #define PT\_HP\_CORE\_UTSNAME (PT\_LOOS + 0x15)

39.

40. #define SHT\_IA\_64\_PRIORITY\_INIT (SHT\_LOPROC + 0x9000000)

41. #define SHT\_IA\_64\_VMS\_TRACE 0x60000000

42. #define SHT\_IA\_64\_VMS\_TIE\_SIGNATURES 0x60000001

43. #define SHT\_IA\_64\_VMS\_DEBUG 0x60000002

44. #define SHT\_IA\_64\_VMS\_DEBUG\_STR 0x60000003

45. #define SHT\_IA\_64\_VMS\_LINKAGES 0x60000004

46. #define SHT\_IA\_64\_VMS\_SYMBOL\_VECTOR 0x60000005

47. #define SHT\_IA\_64\_VMS\_FIXUP 0x60000006

48. #define SHT\_IA\_64\_LOPSREG (SHT\_LOPROC + 0x8000000)

49.

50.

51.

52. #define EM\_L1OM 180 /\* Intel L1OM \*/

53. #define EM\_K1OM 181 /\* Intel K1OM \*/

54. #define EM\_TI\_C6000 140 /\* Texas Instruments TMS320C6000 DSP family \*/

55. #define EM\_MSP430 105 /\* TI msp430 micro controller \*/

56.

57.

58. #define SHT\_ARM\_DEBUGOVERLAY 0x70000004 /\* Section holds overlay debug info. \*/

59. #define SHT\_ARM\_OVERLAYSECTION 0x70000005 /\* Section holds GDB and overlay integration info. \*/

60.

61. #define SHT\_X86\_64\_UNWIND 0x70000001 /\* unwind information \*/

62.

63.

64. #define SHT\_AARCH64\_ATTRIBUTES 0x70000003 /\* Section holds attributes. \*/

65.

66. #define SHT\_C6000\_UNWIND 0x70000001

67. #define SHT\_C6000\_PREEMPTMAP 0x70000002

68. #define SHT\_C6000\_ATTRIBUTES 0x70000003

69. #define SHT\_TI\_ICODE 0x7F000000

70. #define SHT\_TI\_XREF 0x7F000001

71. #define SHT\_TI\_HANDLER 0x7F000002

72. #define SHT\_TI\_INITINFO 0x7F000003

73. #define SHT\_TI\_PHATTRS 0x7F000004

74.

75.

76. #define SHT\_MSP430\_ATTRIBUTES 0x70000003 /\* Section holds ABI attributes. \*/

77. #define SHT\_MSP430\_SEC\_FLAGS 0x7f000005 /\* Holds TI compiler's section flags. \*/

78. #define SHT\_MSP430\_SYM\_ALIASES 0x7f000006 /\* Holds TI compiler's symbol aliases. \*/

79.

80.

81.

82. #define PT\_AARCH64\_ARCHEXT (PT\_LOPROC + 0)

83.

84. //按照小端方式对字进行转换读取，转换为大端方式

85. int byte\_get\_little\_endian (unsigned char \*field, int size)

86. {

87. //依据字的长度进行转换

88. switch (size)

89. {

90. case 1:

91. return \*field;

92. case 2:

93. return ((unsigned int)(field[0]))

94. | (((unsigned int)(field[1])) << 8);

95. case 3:

96. return ((unsigned long) (field[0]))

97. | (((unsigned long) (field[1])) << 8)

98. | (((unsigned long) (field[2])) << 16);

99.

100. case 4:

101. return ((unsigned long) (field[0]))

102. | (((unsigned long) (field[1])) << 8)

103. | (((unsigned long) (field[2])) << 16)

104. | (((unsigned long) (field[3])) << 24);

105. }

106.

107. }

108.

109. ELF\_process::ELF\_process()

110. {

111. printf("NO parameter\n");

112. }

113.

114. int ELF\_process::Process\_object(FILE \*file,int option,char \* target\_section\_name)

115. {

116.

117.

118. if (!get\_file\_header(file))

119. {

120. printf("get file header Failed");

121. return 0;

122. }

123.

124.

125. /\*\*\*\*\*\*\*\*\* start process \*\*\*\*\*\*\*\*\*\*\*/

126. if(option & (1<<0) || option & (1<<6) ) // -h -e

127. {

128. if (!process\_file\_header())

129. {

130. return 0;

131. }

132. }

133. if(!process\_section\_headers(file,option,target\_section\_name))

134. {

135. return 0;

136. }

137. if(option & (1<<3) ) //-g

138. {

139. process\_section\_group(file);

140. }

141. if(option & (1<<1) || option & (1<<6)) //-l -e

142. {

143. process\_program\_headers(file);

144. }

145.

146. if(option & (1<<7)) //-n

147. {

148. process\_note(file);

149. }

150.

151. if(option & (1<<11)) //-n

152. {

153. process\_version(file);

154. }

155.

156. if(option & (1<<10)) //-d

157. {

158. process\_dynamic\_section(file);

159. }

160. if(option & (1<<8)) //-r

161. {

162. process\_relocs(file);

163. }

164. if((option & (1<<13))||(option & (1<<2))) //-S -I

165. {

166. process\_symbol\_table(file,option);

167. }

168. if(option & (1<<9)) //-u

169. {

170. print\_unwind(file);

171. }

172. if(option & (1<<14)) //-x

173. {

174. if(target\_section\_name[0]>='0'&&target\_section\_name[0]<='9') target\_section\_idx=target\_section\_name[0]-'0';

175. print\_xout(file, target\_section\_idx);

176. }

177. }

178. //获取文件头信息的其他部分

179. //下面的代码为32位信息显示

180. //只支持32位的信息显示目前

181. int ELF\_process::get\_file\_header(FILE \*file)

182. {

183.

184. /\* 读取ELF信息，前16个字节，只有当读取成功了才往后面走 \*/

185. if (fread (elf\_header.e\_ident, EI\_NIDENT, 1, file) != 1)

186. return 0;

187.

188. /\* 目前只是实现了32位环境下的表示 \*/

189. is\_32bit\_elf = (elf\_header.e\_ident[EI\_CLASS] != ELFCLASS64);

190.

191. /\* 读取头部信息的其他部分 \*/

192. if (is\_32bit\_elf)

193. {

194.

195. Elf32\_External\_Ehdr ehdr32; //文件头信息的其他部分

196. //读取信息除了前16个字节，从后一个字节开始读取

197. if (fread (ehdr32.e\_type, sizeof (ehdr32) - EI\_NIDENT, 1, file) != 1)

198. return 0;

199. //读取对应部分的字节信息

200. elf\_header.e\_type = BYTE\_GET (ehdr32.e\_type);

201. elf\_header.e\_machine = BYTE\_GET (ehdr32.e\_machine);

202. elf\_header.e\_version = BYTE\_GET (ehdr32.e\_version);

203. elf\_header.e\_entry = BYTE\_GET (ehdr32.e\_entry);

204. elf\_header.e\_phoff = BYTE\_GET (ehdr32.e\_phoff);

205. elf\_header.e\_shoff = BYTE\_GET (ehdr32.e\_shoff);

206. elf\_header.e\_flags = BYTE\_GET (ehdr32.e\_flags);

207. elf\_header.e\_ehsize = BYTE\_GET (ehdr32.e\_ehsize);

208. elf\_header.e\_phentsize = BYTE\_GET (ehdr32.e\_phentsize);

209. elf\_header.e\_phnum = BYTE\_GET (ehdr32.e\_phnum);

210. elf\_header.e\_shentsize = BYTE\_GET (ehdr32.e\_shentsize);

211. elf\_header.e\_shnum = BYTE\_GET (ehdr32.e\_shnum);

212. elf\_header.e\_shstrndx = BYTE\_GET (ehdr32.e\_shstrndx);

213.

214.

215. {

216. if (is\_32bit\_elf)

217. get\_32bit\_section\_headers(file,1);

218. else

219. {

220. //64λ ...

221. }

222. }

223.

224. }

225. return 1;

226. }

227.

228. int ELF\_process::process\_version(FILE \*file){

229. // EV\_NONE 0 非法版本

230. // EV\_CURRENT 1 当前版本

231. if(elf\_header.e\_version==1){

232. return printf("readELF 0.1.1, build time 2021.9.10\n");

233. }

234. return printf("No version information found in this file.\n");

235. }

236.

237. //读取32位ELF文件的节区头表

238. int ELF\_process::get\_32bit\_section\_headers(FILE \*file, unsigned int num)

239. {

240. //file：ELF文件指针

241. //num：节区头表的项目数

242.

243. Elf32\_External\_Shdr \* shdrs;

244. Elf32\_Shdr\* internal;

245.

246. //利用elf头中的关于节头的信息，读取节头的数据，并强制转换为节头指针数据类型

247. //这里读取的shdrs是节头表数组的首地址

248. shdrs = (Elf32\_External\_Shdr \*) get\_data (NULL, file, elf\_header.e\_shoff,

249. elf\_header.e\_shentsize, num,

250. ("section headers"));

251. //如果节头数组为空，就表示读取失败了，所以直接返回

252. if (!shdrs)

253. return 0;

254.

255. //申请内存存放节头数组，之前的读取的节头数组是

256. section\_headers = (Elf32\_Shdr \*) cmalloc (num,sizeof (Elf32\_Shdr));

257.

258. //如果申请内存失败，返回内存溢出异常

259. if (section\_headers == NULL)

260. {

261. printf("Out of memory\n");

262. return 0;

263. }

264.

265. internal = section\_headers;

266.

267. //将从文件中读取的小端数据的节区头表数据转换为结构体的数据

268. //这里的转换有讲究的，因为我们读取使用的char[]数组读4个字节的，是不会进行转换的，会直接读取原始的小端数据

269. //这里需要将小端数据转换一下，变成正常的字数据

270. //那为什么不直接用uint\_32t?

271. //因为保存的ELF文件不一定都是我定义的Elf32Word类型，变个名字就失效了

272. for (int i = 0; i < num; i++, internal++)

273. {

274. internal->sh\_name = BYTE\_GET (shdrs[i].sh\_name);

275. internal->sh\_type = BYTE\_GET (shdrs[i].sh\_type);

276. internal->sh\_flags = BYTE\_GET (shdrs[i].sh\_flags);

277. internal->sh\_addr = BYTE\_GET (shdrs[i].sh\_addr);

278. internal->sh\_offset = BYTE\_GET (shdrs[i].sh\_offset);

279. internal->sh\_size = BYTE\_GET (shdrs[i].sh\_size);

280. internal->sh\_link = BYTE\_GET (shdrs[i].sh\_link);

281. internal->sh\_info = BYTE\_GET (shdrs[i].sh\_info);

282. internal->sh\_addralign = BYTE\_GET (shdrs[i].sh\_addralign);

283. internal->sh\_entsize = BYTE\_GET (shdrs[i].sh\_entsize);

284. }

285.

286. free (shdrs);

287.

288. return 1;

289. }

290.

291. //将硬盘中文件中的数据提取到内存中的变量

292. void \* ELF\_process::get\_data (void \* var, FILE \* file, long offset, size\_t size, size\_t nmemb,const char \* reason)

293. {

294. //var：存放数据的变量地址

295. //file：读取的文件

296. //offset：被读取的数据的偏移地址

297. //size：每个元素的大小

298. //nmemb：一共有多少个这样的元素

299. //reason：读取的原因，便于报错

300.

301.

302. //临时变量保存地址

303. void \* mvar;

304.

305. //如果每个元素的大小为0，或者有0个元素，那么读空

306. if (size == 0 || nmemb == 0)

307. return NULL;

308.

309. //将文件的读取指针移动到偏移地址处

310. if (fseek (file, offset, SEEK\_SET))

311. {

312. //error (\_("Unable to seek to 0x%lx for %s\n"),

313. // (unsigned long) archive\_file\_offset + offset, reason);

314. //若失败则返回读空

315. return NULL;

316. }

317.

318. mvar = var;

319. //判断用户的变量是不是为空，如果为空，那么需要申请空间

320. if (mvar == NULL)

321. {

322. /\* Check for overflow. \*/

323. //检查是否溢出，即将要读取的元素个数大于等于了地址空间全部存放这个元素时的最大个数

324. if (nmemb < (~(size\_t) 0 - 1) / size)

325. /\* + 1 so that we can '\0' terminate invalid string table sections. \*/

326. //如果没有溢出，那么就申请 元素大小\*元素个数+1 的内存空间

327. //+1是为了最后添加'/0'给字符串节区用

328. mvar = malloc (size \* nmemb + 1);

329.

330. //如果此时变量指针还是空的，说明没有成功申请到内存，所以返回读空

331. if (mvar == NULL)

332. {

333. //error (\_("Out of memory allocating 0x%lx bytes for %s\n"),

334. //(unsigned long)(size \* nmemb), reason);

335. return NULL;

336. }

337.

338. //申请成功的话，将最后一位（+1的那个字节）设置为'\0'字符串结束符

339. ((char \*) mvar)[size \* nmemb] = '\0';

340. }

341.

342. //从文件读取指针处读取nmemb个size大小的数据到mvar所指向的内存空间中

343. if (fread (mvar, size, nmemb, file) != nmemb)

344. {

345. //若实际读取的元素个数和想要读取的元素个数不一致，那么就异常

346. //error (\_("Unable to read in 0x%lx bytes of %s\n"),

347. // (unsigned long)(size \* nmemb), reason);

348. //如果两个指针所指向的地址不一样，那么就释放内存，避免内存泄漏

349. if (mvar != var)

350. free (mvar);

351. //返回读空

352. return NULL;

353. }

354.

355. //读取完毕，成功返回复制到内存中的数据

356. return mvar;

357. }

358.

359. //在内存中申请空间

360. void \*ELF\_process::cmalloc (size\_t nmemb, size\_t size)

361. {

362. /\* Check for overflow. \*/

363. //检查溢出，判断要申请的空间存放的元素个数 是否大于等于 假如全部装这个元素时能存放的最大元素个数

364. if (nmemb >= ~(size\_t) 0 / size)

365. return NULL;

366. //如果没有溢出，那么就申请 元素大小\*元素个数 的内存空间大小

367. else

368. return malloc (nmemb \* size);

369. }

370. /\*读取文件头\*/

371. /\*头文件信息在Magic 数中\*/

372. int ELF\_process::process\_file\_header(void)

373. {

374. /\*判断是否Magic是否存在问题\*/

375. if ( elf\_header.e\_ident[EI\_MAG0] != ELFMAG0

376. || elf\_header.e\_ident[EI\_MAG1] != ELFMAG1

377. || elf\_header.e\_ident[EI\_MAG2] != ELFMAG2

378. || elf\_header.e\_ident[EI\_MAG3] != ELFMAG3)

379. {

380. printf("Not an ELF file - it has the wrong magic bytes at the start\n");

381. return 0;

382. }

383. /\*输出M相关参数\*/

384. printf("ELF Header:\n");

385. printf(" Magic: ");

386. for (int i = 0; i <EI\_NIDENT ; ++i)

387. printf ("%2.2x ", elf\_header.e\_ident[i]); /\*读取Magic 数\*/

388. printf("\n");

389. printf(" Class: %s\n",

390. get\_elf\_class(elf\_header.e\_ident[EI\_CLASS]));

391.

392. printf (" Data: %s\n",

393. get\_data\_encoding (elf\_header.e\_ident[EI\_DATA]));

394. const char \*str=elf\_header.e\_ident[EI\_VERSION] == EV\_CURRENT ?

395. "(current)" : (elf\_header.e\_ident[EI\_VERSION] != EV\_NONE ? "<unknown>" : "");

396. printf (" Version: %d %s\n",

397. elf\_header.e\_ident[EI\_VERSION],str);

398. printf (" OS/ABI: %s\n",

399. get\_osabi\_name (elf\_header.e\_ident[EI\_OSABI]));

400.

401. printf (" ABI Version: %d\n",

402. elf\_header.e\_ident[EI\_ABIVERSION]);

403.

404. printf (" Type: %s\n",

405. get\_file\_type (elf\_header.e\_type));

406.

407. printf (" Machine: %s\n",

408. get\_machine\_name (elf\_header.e\_machine));

409.

410. printf (" Version: 0x%lx\n",

411. (unsigned long) elf\_header.e\_version);

412.

413. printf (" Entry point address: 0x%x",elf\_header.e\_entry);

414.

415. printf ("\n Start of program headers: %d",elf\_header.e\_phoff);

416.

417. printf (" (bytes into file)\n Start of section headers: %d",elf\_header.e\_shoff);

418. printf (" (bytes into file)\n");

419.

420. printf (" Flags: 0x%lx\n",(unsigned long)elf\_header.e\_flags);

421.

422. printf (" Size of this header: %ld (bytes)\n",(long)elf\_header.e\_ehsize);

423.

424. printf (" Size of program headers: %ld (bytes)\n",(long)elf\_header.e\_phentsize);

425.

426. printf (" Number of program headers: %ld\n",(long)elf\_header.e\_phnum);

427.

428. printf (" Size of section headers: %ld (bytes)\n",

429. (long) elf\_header.e\_shentsize);

430.

431. printf (" Number of section headers: %ld\n",

432. (long) elf\_header.e\_shnum);

433.

434. if (section\_headers != NULL && elf\_header.e\_shnum == SHN\_UNDEF)

435. printf (" (%ld)", (long) section\_headers[0].sh\_size);

436.

437. printf (" Section header string table index: %ld\n",

438. (long) elf\_header.e\_shstrndx);

439.

440. return 1;

441.

442. }

443.

444. /\*从magic数中，提取elf\_class信息\*/

445. const char \*ELF\_process::get\_elf\_class (unsigned int elf\_class)

446. {

447. static char buff[32];

448. /\*判断elf\_class处的字节信息\*/

449. switch (elf\_class)

450. {

451. case ELFCLASSNONE:

452. return ("none");

453. case ELFCLASS32:

454. return "ELF32";

455. case ELFCLASS64:

456. return "ELF64";

457. default:

458. snprintf (buff, sizeof (buff), ("<unknown: %x>"), elf\_class);

459. return buff;

460. }

461. }

462. /\*获取data的编码信息\*/

463. const char \*ELF\_process::get\_data\_encoding (unsigned int encoding)

464. {

465. static char buff[32];

466. /\*表示数据存储的方式，大端、小端\*/

467. switch (encoding)

468. {

469. case ELFDATANONE:

470. return ("none");

471. case ELFDATA2LSB:

472. return ("2's complement, little endian");

473. case ELFDATA2MSB:

474. return ("2's complement, big endian");

475. default:

476. snprintf (buff, sizeof (buff), ("<unknown: %x>"), encoding);

477. return buff;

478. }

479. }

480. const char \*ELF\_process::get\_osabi\_name (unsigned int osabi)

481. {

482.

483. static char buff[32];

484. switch (osabi)

485. {

486. case ELFOSABI\_NONE:

487. return "UNIX System V ABI";

488. case ELFOSABI\_HPUX:

489. return "HP-UX";

490. case ELFOSABI\_NETBSD:

491. return "NetBSD";

492. case ELFOSABI\_GNU:

493. return "Object uses GNU ELF extensions";

494. case ELFOSABI\_SOLARIS:

495. return "Sun Solaris";

496. case ELFOSABI\_AIX:

497. return "IBM AIX";

498. case ELFOSABI\_IRIX:

499. return "SGI Irix";

500. case ELFOSABI\_FREEBSD:

501. return "FreeBSD";

502. case ELFOSABI\_TRU64:

503. return "Compaq TRU64 UNIX";

504. case ELFOSABI\_MODESTO:

505. return "Novell Modesto";

506. case ELFOSABI\_OPENBSD:

507. return "OpenBSD";

508. case ELFOSABI\_ARM\_AEABI:

509. return "ARM EABI";

510. case ELFOSABI\_ARM:

511. return "ARM";

512. case ELFOSABI\_STANDALONE:

513. return "Standalone (embedded) application";

514. default:

515. break;

516. }

517.

518. snprintf (buff, sizeof (buff), ("<unknown: %x>"), osabi);

519. return buff;

520. }

521. /\*返回文件类型\*/

522.

523. const char \*ELF\_process::get\_file\_type(unsigned e\_type)

524. {

525.

526. static char buff[32];

527.

528. switch (e\_type)

529. {

530. case ET\_NONE:

531. return "NONE (None)";

532. case ET\_REL:

533. return "REL (Relocatable file)"; //重定向文件

534. case ET\_EXEC:

535. return "EXEC (Executable file)"; //执行文件

536. case ET\_DYN:

537. return "DYN (Shared object file)"; //共享文件

538. case ET\_CORE:

539. return "CORE (Core file)"; //核心文件

540.

541. default: //如果不是如上三种文件，那么返回具体的处理器信息或操作系统信息

542. if ((e\_type >= ET\_LOPROC) && (e\_type <= ET\_HIPROC))

543. snprintf(buff, sizeof(buff), ("Processor Specific: (%x)"), e\_type);

544. else if ((e\_type >= ET\_LOOS) && (e\_type <= ET\_HIOS))

545. snprintf(buff, sizeof(buff), ("OS Specific: (%x)"), e\_type);

546. else

547. snprintf(buff, sizeof(buff), ("<unknown>: %x"), e\_type);

548. return buff;

549.

550. }

551. }

552. /\*获取机器类型\*/

553. const char \*ELF\_process::get\_machine\_name(unsigned e\_machine)

554. {

555.

556. static char buff[64];

557.

558. switch (e\_machine)

559. {

560. case EM\_NONE:

561. return ("None");

562. case EM\_AARCH64:

563. return "AArch64";

564. case EM\_M32:

565. return "WE32100";

566. case EM\_SPARC:

567. return "Sparc";

568. case EM\_386:

569. return "Intel 80386";

570. case EM\_68K:

571. return "MC68000";

572. case EM\_88K:

573. return "MC88000";

574. case EM\_860:

575. return "Intel 80860";

576. case EM\_MIPS:

577. return "MIPS R3000";

578. case EM\_S370:

579. return "IBM System/370";

580. case EM\_MIPS\_RS3\_LE:

581. return "MIPS R4000 big-endian";

582. case EM\_PARISC:

583. return "HPPA";

584. case EM\_SPARC32PLUS:

585. return "Sparc v8+" ;

586. case EM\_960:

587. return "Intel 90860";

588. case EM\_PPC:

589. return "PowerPC";

590. case EM\_PPC64:

591. return "PowerPC64";

592. case EM\_FR20:

593. return "Fujitsu FR20";

594. case EM\_RH32:

595. return "TRW RH32";

596. case EM\_ARM:

597. return "ARM";

598. case EM\_SH:

599. return "Renesas / SuperH SH";

600. case EM\_SPARCV9:

601. return "Sparc v9";

602. case EM\_TRICORE:

603. return "Siemens Tricore";

604. case EM\_ARC:

605. return "ARC";

606. case EM\_H8\_300:

607. return "Renesas H8/300";

608. case EM\_H8\_300H:

609. return "Renesas H8/300H";

610. case EM\_H8S:

611. return "Renesas H8S";

612. case EM\_H8\_500:

613. return "Renesas H8/500";

614. case EM\_IA\_64:

615. return "Intel IA-64";

616. case EM\_MIPS\_X:

617. return "Stanford MIPS-X";

618. case EM\_COLDFIRE:

619. return "Motorola Coldfire";

620. case EM\_ALPHA:

621. return "Alpha";

622. case EM\_D10V:

623. return "d10v";

624. case EM\_D30V:

625. return "d30v";

626. case EM\_M32R:

627. return "Renesas M32R (formerly Mitsubishi M32r)";

628. case EM\_V800:

629. return "Renesas V850 (using RH850 ABI)";

630. case EM\_V850:

631. return "Renesas V850";

632. case EM\_MN10300:

633. return "mn10300";

634. case EM\_MN10200:

635. return "mn10200";

636. case EM\_FR30:

637. return "Fujitsu FR30";

638. case EM\_PJ:

639. return "picoJava";

640. case EM\_MMA:

641. return "Fujitsu Multimedia Accelerator";

642. case EM\_PCP:

643. return "Siemens PCP";

644. case EM\_NCPU:

645. return "Sony nCPU embedded RISC processor";

646. case EM\_NDR1:

647. return "Denso NDR1 microprocesspr";

648. case EM\_STARCORE:

649. return "Motorola Star\*Core processor";

650. case EM\_ME16:

651. return "Toyota ME16 processor";

652. case EM\_ST100:

653. return "STMicroelectronics ST100 processor";

654. case EM\_TINYJ:

655. return "Advanced Logic Corp. TinyJ embedded processor";

656. case EM\_PDSP:

657. return "Sony DSP processor";

658. case EM\_FX66:

659. return "Siemens FX66 microcontroller";

660. case EM\_ST9PLUS:

661. return "STMicroelectronics ST9+ 8/16 bit microcontroller";

662. case EM\_ST7:

663. return "STMicroelectronics ST7 8-bit microcontroller";

664. case EM\_68HC16:

665. return "Motorola MC68HC16 Microcontroller";

666. case EM\_68HC12:

667. return "Motorola MC68HC12 Microcontroller";

668. case EM\_68HC11:

669. return "Motorola MC68HC11 Microcontroller";

670. case EM\_68HC08:

671. return "Motorola MC68HC08 Microcontroller";

672. case EM\_68HC05:

673. return "Motorola MC68HC05 Microcontroller";

674. case EM\_SVX:

675. return "Silicon Graphics SVx";

676. case EM\_ST19:

677. return "STMicroelectronics ST19 8-bit microcontroller";

678. case EM\_VAX:

679. return "Digital VAX";

680. case EM\_AVR:

681. return "Atmel AVR 8-bit microcontroller";

682. case EM\_CRIS:

683. return "Axis Communications 32-bit embedded processor";

684. case EM\_JAVELIN:

685. return "Infineon Technologies 32-bit embedded cpu";

686. case EM\_FIREPATH:

687. return "Element 14 64-bit DSP processor";

688. case EM\_ZSP:

689. return "LSI Logic's 16-bit DSP processor";

690. case EM\_MMIX:

691. return "Donald Knuth's educational 64-bit processor";

692. case EM\_HUANY:

693. return "Harvard Universitys's machine-independent object format";

694. case EM\_PRISM:

695. return "Vitesse Prism";

696. case EM\_X86\_64:

697. return "Advanced Micro Devices X86-64";

698. case EM\_S390:

699. return "IBM S/390";

700. case EM\_OPENRISC:

701. case EM\_ARC\_A5:

702. return "ARC International ARCompact processor";

703. case EM\_XTENSA:

704. return "Tensilica Xtensa Processor";

705. case EM\_MICROBLAZE:

706. case EM\_TILEPRO:

707. return "Tilera TILEPro multicore architecture family";

708. case EM\_TILEGX:

709. return "Tilera TILE-Gx multicore architecture family";

710. default:

711. snprintf (buff, sizeof (buff), ("<unknown>: 0x%x"), e\_machine);

712. }

713.

714. return buff;

715.

716. }

717.

718. //解析和处理文件的节头表

719. int ELF\_process::process\_section\_headers(FILE \*file,int option,char \*target\_section\_name)

720. {

721. //file：文件指针

722. //option：解析的内容选项

723. //target\_section\_name：目标节区索引，这个只有当-x指令时生效

724.

725. Elf32\_Shdr \* section;

726. section = NULL;

727. char \* string\_table;

728.

729. unsigned int flag\_shoff;

730.

731. //依据ELF头判断节区头表的项目数，如果项目数为0那么存在异常

732. if (elf\_header.e\_shnum == 0)

733. {

734. //依据elf头中的节区表头偏移地址是不是0，如果是0，那么就说明不存在节区表头，有异常

735. if (elf\_header.e\_shoff!=0)

736. printf("possibly corrupt ELF file header - it has a non-zero section header offset, but no section headers\n");

737. //节区表头存在但是没有表项，就说明文件中没有节区

738. else

739. printf ("\nThere are no sections in this file.\n");

740. return 1;

741. }

742.

743. //如果指令为-t -S -e，那么就先打印出节头表的项目数量和节头表的偏移位置，

744. //这些指令分别是：显示节的详细信息、 显示节头信息、显示全部头信息

745. if((option & (1<<4))||(option & (1<<2) ) || (option & (1<<6)))

746. printf (" There are %d section headers, starting at offset 0x%lx:\n",elf\_header.e\_shnum, (unsigned long) elf\_header.e\_shoff);

747.

748. //如果是32位的文件

749. if (is\_32bit\_elf)

750. {

751. //读取32位的节区头表，依据elf头中的信息

752. if (! get\_32bit\_section\_headers (file, elf\_header.e\_shnum))

753. return 0;

754. }

755.

756. /\* Read in the string table, so that we have names to display. \*/

757. //找到shstrtab的位置

758. //先判断shstrtab的节区索引是不是未定义，然后判断是不是小于总节区数

759. if (elf\_header.e\_shstrndx != SHN\_UNDEF && elf\_header.e\_shstrndx < elf\_header.e\_shnum)

760. {

761. //获取shstrtab节区，位置是节区头的偏移地址加上对应的索引，即节区头表中的第e\_shstrndx个元素

762. section = section\_headers + elf\_header.e\_shstrndx;

763.

764. //保存shstrtab的偏移地址

765. flag\_shoff = section->sh\_offset;

766.

767. }

768.

769. //如果指令为-t -S -e，那么接下来打印节头信息

770. //这些指令分别是：显示节的详细信息、 显示节头信息、显示全部头信息

771. if((option & (1<<4))||(option & (1<<2) ) || (option & (1<<6)))

772. {

773. //如果节头表项个数大于1，那么单词用复数

774. if (elf\_header.e\_shnum > 1)

775. printf ("\nSection Headers:\n");

776. else

777. printf ("\nSection Header:\n");

778. }

779. section = section\_headers;

780. unsigned int countC;

781. //只做32位文件的分析

782. if (is\_32bit\_elf)

783. {

784. //如果是-t指令，显示节区的详细信息

785. if(option & (1<<4)) //-t

786. {

787. //打印列名

788. printf(" [Nr] Name\n Type Addr Off Size ES Flg Lk Inf Al\n Flags\n");

789. //遍历节区头表的所有项，每一个项都对应一个节区

790. for (int i = 0; i < elf\_header.e\_shnum; i++, section++)

791. {

792. printf (" [%2u] ", i);

793.

794. //计算该节区名在shstrtab中的偏移地址

795. countC = flag\_shoff + section->sh\_name;

796.

797. //将文件指针移动到这个地方

798. fseek(file,countC,SEEK\_SET);

799. //名字字符串，长度为20，名字以'\0'结尾，所以多读一些没有关系

800. char string\_name[20];

801. //从文件中读取名字字符串

802. fread(string\_name,20,1,file);

803.

804. //判断节区名是不是"IA\_64",记录unwind节区的索引

805. if(!strcmp(string\_name,"IA\_64")) unwind\_idx=i;

806. //判断节区名和目标的节区名是否一致，相同的话记录目标节区名对应的索引，这个是给-x用的

807. if(!strcmp(string\_name,target\_section\_name)) target\_section\_idx=i;

808.

809. //打印输出节区名

810. printf("%-16s \n",string\_name);

811.

812. //打印输出节区类型

813. printf("%-16s ",get\_section\_type\_name (section->sh\_type));

814.

815. //打印输出节区虚拟地址、文件中偏移地址、节区大小、节区条目大小

816. printf("%6.8lx",(unsigned long) section->sh\_addr);

817. printf ( " %6.6lx %6.6lx %2.2lx",

818. (unsigned long) section->sh\_offset,

819. (unsigned long) section->sh\_size,

820. (unsigned long) section->sh\_entsize);

821.

822. //如果节区有标志位那么就打印输出标志

823. if (section->sh\_flags)

824. printf (" %2.2x ", section->sh\_flags);

825. //否则用空格填充

826. else

827. printf("%4c",32);

828.

829. //打印输出sh\_link和sh\_info，这个因不同节区类型而异，最后输出对齐信息

830. printf ("%2u ", section->sh\_link);

831. printf ("%3u %3lu", section->sh\_info,

832. (unsigned long) section->sh\_addralign);

833.

834. //如果节区名是.dynamic动态链接信息表，那么需要记录节区的偏移地址和大小

835. if (strcmp(string\_name,".dynamic")==0)

836. {

837. dynamic\_addr = section->sh\_offset;

838. dynamic\_size = section->sh\_size;

839. }

840.

841. //如果节区名是.rel.dyn动态链接重定位表，那么需要记录节区的偏移地址和大小

842. if (strcmp(string\_name,".rel.dyn")==0)

843. {

844. rel\_dyn\_offset = section->sh\_offset;

845. rel\_dyn\_size = section->sh\_size;

846. }

847.

848. //如果节区名是.dynsym动态链接符号表，那么需要记录节区的偏移地址和大小

849. if(strcmp(string\_name,".dynsym")==0)

850. {

851. sym\_dyn\_offset = section->sh\_offset;

852. sym\_dyn\_size = section->sh\_size;

853. }

854.

855. //如果节区名是.dynstr动态链接字符表，那么需要记录节区的偏移地址和大小

856. if(strcmp(string\_name,".dynstr")==0)

857. {

858. str\_dyn\_offset = section->sh\_offset;

859. str\_dyn\_size = section->sh\_size;

860. }

861.

862. printf("\n");

863. //打印输出标志位

864. printf(" [%x]\n",section->sh\_flags);

865. }

866. }

867. //如果是-S或-e指令，显示节头信息和全部头信息

868. else if((option & (1<<2) ) || (option & (1<<6))) //-S || -e

869. {

870.

871. //打印列名

872. printf(" [Nr] Name Type Addr Off Size ES Flg Lk Inf Al\n");

873. //遍历节区头表的所有项，每一个项都对应一个节区

874. for (int i = 0; i < elf\_header.e\_shnum; i++, section++)

875. {

876. printf (" [%2u] ", i);

877.

878. //计算该节区名在shstrtab中的偏移地址

879. countC = flag\_shoff + section->sh\_name;

880.

881. //将文件指针移动到这个地方

882. fseek(file,countC,SEEK\_SET);

883. //名字字符串，长度为20，名字以'\0'结尾，所以多读一些没有关系

884. char string\_name[20];

885. //从文件中读取名字字符串

886. fread(string\_name,20,1,file);

887.

888. //判断节区名是不是"IA\_64",记录unwind节区的索引

889. if(!strcmp(string\_name,"IA\_64")) unwind\_idx=i;

890. //判断节区名和目标的节区名是否一致，相同的话记录目标节区名对应的索引，这个是给-x用的

891. if(!strcmp(string\_name,target\_section\_name)) target\_section\_idx=i;

892.

893. //打印输出节区名

894. printf("%-16s ",string\_name);

895.

896.

897. //打印输出节区类型

898. printf ( " %-15.15s ",

899. get\_section\_type\_name (section->sh\_type));

900.

901. //打印输出节区虚拟地址、文件中偏移地址、节区大小、节区条目大小

902. printf("%6.8lx",(unsigned long) section->sh\_addr);

903. printf ( " %6.6lx %6.6lx %2.2lx",

904. (unsigned long) section->sh\_offset,

905. (unsigned long) section->sh\_size,

906. (unsigned long) section->sh\_entsize);

907.

908. //如果节区有标志位那么就打印输出标志

909. if (section->sh\_flags)

910. printf (" %2.2x ", section->sh\_flags);

911. //否则用空格填充

912. else

913. printf("%4c",32);

914.

915. //打印输出sh\_link和sh\_info，这个因不同节区类型而异，最后输出对齐信息

916. printf ("%2u ", section->sh\_link);

917. printf ("%3u %3lu", section->sh\_info,

918. (unsigned long) section->sh\_addralign);

919.

920. //如果节区名是.dynamic动态链接信息表，那么需要记录节区的偏移地址和大小

921. if (strcmp(string\_name,".dynamic")==0)

922. {

923. dynamic\_addr = section->sh\_offset;

924. dynamic\_size = section->sh\_size;

925. }

926.

927. //如果节区名是.rel.dyn动态链接重定位表，那么需要记录节区的偏移地址和大小

928. if (strcmp(string\_name,".rel.dyn")==0)

929. {

930. rel\_dyn\_offset = section->sh\_offset;

931. rel\_dyn\_size = section->sh\_size;

932. }

933.

934. //如果节区名是.dynsym动态链接符号表，那么需要记录节区的偏移地址和大小

935. if(strcmp(string\_name,".dynsym")==0)

936. {

937. sym\_dyn\_offset = section->sh\_offset;

938. sym\_dyn\_size = section->sh\_size;

939. }

940.

941. //如果节区名是.dynstr动态链接字符表，那么需要记录节区的偏移地址和大小

942. if(strcmp(string\_name,".dynstr")==0)

943. {

944. str\_dyn\_offset = section->sh\_offset;

945. str\_dyn\_size = section->sh\_size;

946. }

947.

948. printf("\n");

949.

950. }

951. }

952. //如果是指令-x或-u，显示指定节区详细信息或.unwind节区详细信息

953. else if(option & (1<<14) || option & (1<<9))

954. {

955. //遍历节区头表的所有项，每一个项都对应一个节区

956. for (int i = 0; i < elf\_header.e\_shnum; i++, section++)

957. {

958. //计算该节区名在shstrtab中的偏移地址

959. countC = flag\_shoff + section->sh\_name;

960. //将文件指针移动到这个地方

961. fseek(file,countC,SEEK\_SET);

962. //名字字符串，长度为20，名字以'\0'结尾，所以多读一些没有关系

963. char string\_name[20];

964. //从文件中读取名字字符串

965. fread(string\_name,20,1,file);

966.

967. //判断节区名是不是"IA\_64",记录unwind节区的索引，这个是给-u用的

968. if(!strcmp(string\_name,"IA\_64")) unwind\_idx=i;

969. //判断节区名和目标的节区名是否一致，相同的话记录目标节区名对应的索引，这个是给-x用的

970. if(!strcmp(string\_name,target\_section\_name)) target\_section\_idx=i;

971. }

972. }

973. }

974.

975. //成功返回

976. return 1;

977. }

978. /\*获取节的类型名\*/

979. const char \*ELF\_process::get\_section\_type\_name(unsigned int sh\_type)

980. {

981.

982. static char buff[32];

983. switch (sh\_type)

984. {

985. case SHT\_NULL:

986. return "NULL";

987. case SHT\_PROGBITS:

988. return "PROGBITS";

989. case SHT\_SYMTAB:

990. return "SYMTAB";

991. case SHT\_STRTAB:

992. return "STRTAB";

993. case SHT\_RELA:

994. return "RELA";

995. case SHT\_HASH:

996. return "HASH";

997. case SHT\_DYNAMIC:

998. return "DYNAMIC";

999. case SHT\_NOTE:

1000. return "NOTE";

1001. case SHT\_NOBITS:

1002. return "NOBITS";

1003. case SHT\_REL:

1004. return "REL";

1005. case SHT\_SHLIB:

1006. return "SHLIB";

1007. case SHT\_DYNSYM:

1008. return "DYNSYM";

1009. case SHT\_INIT\_ARRAY:

1010. return "INIT\_ARRAY";

1011. case SHT\_FINI\_ARRAY:

1012. return "FINI\_ARRAY";

1013. case SHT\_PREINIT\_ARRAY:

1014. return "PREINIT\_ARRAY";

1015. case SHT\_GNU\_HASH:

1016. return "GNU\_HASH";

1017. case SHT\_GROUP:

1018. return "GROUP";

1019. case SHT\_SYMTAB\_SHNDX:

1020. return "SYMTAB SECTION INDICIES";

1021. case SHT\_GNU\_verdef:

1022. return "VERDEF";

1023. case SHT\_GNU\_verneed:

1024. return "VERNEED";

1025. case SHT\_GNU\_versym:

1026. return "VERSYM";

1027. case 0x6ffffff0:

1028. return "VERSYM";

1029. case 0x6ffffffc:

1030. return "VERDEF";

1031. case 0x7ffffffd:

1032. return "AUXILIARY";

1033. case 0x7fffffff:

1034. return "FILTER";

1035. case SHT\_GNU\_LIBLIST:

1036. return "GNU\_LIBLIST";

1037.

1038. default:

1039. if ((sh\_type >= SHT\_LOPROC) && (sh\_type <= SHT\_HIPROC))

1040. {

1041.

1042.

1043. const char \* result;

1044.

1045. switch (elf\_header.e\_machine)

1046. {

1047.

1048. case EM\_MIPS:

1049. case EM\_MIPS\_RS3\_LE:

1050. result = get\_mips\_section\_type\_name (sh\_type);

1051. break;

1052. case EM\_PARISC:

1053. result = get\_parisc\_section\_type\_name (sh\_type);

1054. break;

1055. case EM\_IA\_64:

1056. result = get\_ia64\_section\_type\_name (sh\_type);

1057. break;

1058. case EM\_X86\_64:

1059. case EM\_L1OM:

1060. case EM\_K1OM:

1061. result = get\_x86\_64\_section\_type\_name (sh\_type);

1062. break;

1063. case EM\_AARCH64:

1064. result = get\_aarch64\_section\_type\_name (sh\_type);

1065. break;

1066. case EM\_ARM:

1067. result = get\_arm\_section\_type\_name (sh\_type);

1068. break;

1069. case EM\_TI\_C6000:

1070. result = get\_tic6x\_section\_type\_name (sh\_type);

1071. break;

1072. case EM\_MSP430:

1073. result = get\_msp430x\_section\_type\_name (sh\_type);

1074. break;

1075. default:

1076. result = NULL;

1077. break;

1078.

1079. }

1080. if (result != NULL)

1081. return result;

1082. sprintf (buff, "LOPROC+%x", sh\_type - SHT\_LOPROC);

1083. }

1084. else if ((sh\_type >= SHT\_LOOS) && (sh\_type <= SHT\_HIOS))

1085. {

1086. const char \* result;

1087.

1088. switch (elf\_header.e\_machine)

1089. {

1090. case EM\_IA\_64:

1091. result = get\_ia64\_section\_type\_name (sh\_type);

1092. break;

1093. default:

1094. result = NULL;

1095. break;

1096. }

1097.

1098. if (result != NULL)

1099. return result;

1100.

1101. sprintf (buff, "LOOS+%x", sh\_type - SHT\_LOOS);

1102. }

1103. else if ((sh\_type >= SHT\_LOUSER) && (sh\_type <= SHT\_HIUSER))

1104. sprintf (buff, "LOUSER+%x", sh\_type - SHT\_LOUSER);

1105. else

1106. /\* This message is probably going to be displayed in a 15

1107. character wide field, so put the hex value first. \*/

1108. snprintf (buff, sizeof (buff), ("%08x: <unknown>"), sh\_type);

1109.

1110. return buff;

1111. }

1112. }

1113. /\*获取MIPS节类型名\*/

1114. const char \*ELF\_process::get\_mips\_section\_type\_name(unsigned int sh\_type)

1115. {

1116.

1117. switch (sh\_type)

1118. {

1119. case SHT\_MIPS\_LIBLIST:

1120. return "MIPS\_LIBLIST";

1121. case SHT\_MIPS\_MSYM:

1122. return "MIPS\_MSYM";

1123. case SHT\_MIPS\_CONFLICT:

1124. return "MIPS\_CONFLICT";

1125. case SHT\_MIPS\_GPTAB:

1126. return "MIPS\_GPTAB";

1127. case SHT\_MIPS\_UCODE:

1128. return "MIPS\_UCODE";

1129. case SHT\_MIPS\_DEBUG:

1130. return "MIPS\_DEBUG";

1131. case SHT\_MIPS\_REGINFO:

1132. return "MIPS\_REGINFO";

1133. case SHT\_MIPS\_PACKAGE:

1134. return "MIPS\_PACKAGE";

1135. case SHT\_MIPS\_PACKSYM:

1136. return "MIPS\_PACKSYM";

1137. case SHT\_MIPS\_RELD:

1138. return "MIPS\_RELD";

1139. case SHT\_MIPS\_IFACE:

1140. return "MIPS\_IFACE";

1141. case SHT\_MIPS\_CONTENT:

1142. return "MIPS\_CONTENT";

1143. case SHT\_MIPS\_OPTIONS:

1144. return "MIPS\_OPTIONS";

1145. case SHT\_MIPS\_SHDR:

1146. return "MIPS\_SHDR";

1147. case SHT\_MIPS\_FDESC:

1148. return "MIPS\_FDESC";

1149. case SHT\_MIPS\_EXTSYM:

1150. return "MIPS\_EXTSYM";

1151. case SHT\_MIPS\_DENSE:

1152. return "MIPS\_DENSE";

1153. case SHT\_MIPS\_PDESC:

1154. return "MIPS\_PDESC";

1155. case SHT\_MIPS\_LOCSYM:

1156. return "MIPS\_LOCSYM";

1157. case SHT\_MIPS\_AUXSYM:

1158. return "MIPS\_AUXSYM";

1159. case SHT\_MIPS\_OPTSYM:

1160. return "MIPS\_OPTSYM";

1161. case SHT\_MIPS\_LOCSTR:

1162. return "MIPS\_LOCSTR";

1163. case SHT\_MIPS\_LINE:

1164. return "MIPS\_LINE";

1165. case SHT\_MIPS\_RFDESC:

1166. return "MIPS\_RFDESC";

1167. case SHT\_MIPS\_DELTASYM:

1168. return "MIPS\_DELTASYM";

1169. case SHT\_MIPS\_DELTAINST:

1170. return "MIPS\_DELTAINST";

1171. case SHT\_MIPS\_DELTACLASS:

1172. return "MIPS\_DELTACLASS";

1173. case SHT\_MIPS\_DWARF:

1174. return "MIPS\_DWARF";

1175. case SHT\_MIPS\_DELTADECL:

1176. return "MIPS\_DELTADECL";

1177. case SHT\_MIPS\_SYMBOL\_LIB:

1178. return "MIPS\_SYMBOL\_LIB";

1179. case SHT\_MIPS\_EVENTS:

1180. return "MIPS\_EVENTS";

1181. case SHT\_MIPS\_TRANSLATE:

1182. return "MIPS\_TRANSLATE";

1183. case SHT\_MIPS\_PIXIE:

1184. return "MIPS\_PIXIE";

1185. case SHT\_MIPS\_XLATE:

1186. return "MIPS\_XLATE";

1187. case SHT\_MIPS\_XLATE\_DEBUG:

1188. return "MIPS\_XLATE\_DEBUG";

1189. case SHT\_MIPS\_WHIRL:

1190. return "MIPS\_WHIRL";

1191. case SHT\_MIPS\_EH\_REGION:

1192. return "MIPS\_EH\_REGION";

1193. case SHT\_MIPS\_XLATE\_OLD:

1194. return "MIPS\_XLATE\_OLD";

1195. case SHT\_MIPS\_PDR\_EXCEPTION:

1196. return "MIPS\_PDR\_EXCEPTION";

1197. default:

1198. break;

1199. }

1200. return NULL;

1201. }

1202. /\*获取PA-RISC类型名\*/

1203. const char \*ELF\_process::get\_parisc\_section\_type\_name(unsigned int sh\_type)

1204. {

1205.

1206.

1207. switch (sh\_type)

1208. {

1209. case SHT\_PARISC\_EXT:

1210. return "PARISC\_EXT";

1211. case SHT\_PARISC\_UNWIND:

1212. return "PARISC\_UNWIND";

1213. case SHT\_PARISC\_DOC:

1214. return "PARISC\_DOC";

1215. case SHT\_PARISC\_ANNOT:

1216. return "PARISC\_ANNOT";

1217. case SHT\_PARISC\_SYMEXTN:

1218. return "PARISC\_SYMEXTN";

1219. case SHT\_PARISC\_STUBS:

1220. return "PARISC\_STUBS";

1221. case SHT\_PARISC\_DLKM:

1222. return "PARISC\_DLKM";

1223. default:

1224. break;

1225. }

1226. return NULL;

1227. }

1228. /\*获取IA-64类型名\*/

1229. const char \*ELF\_process::get\_ia64\_section\_type\_name(unsigned int sh\_type)

1230. {

1231.

1232.

1233. /\* If the top 8 bits are 0x78 the next 8 are the os/abi ID. \*/

1234. if ((sh\_type & 0xFF000000) == SHT\_IA\_64\_LOPSREG)

1235. return get\_osabi\_name ((sh\_type & 0x00FF0000) >> 16);

1236.

1237. switch (sh\_type)

1238. {

1239. case SHT\_IA\_64\_EXT:

1240. return "IA\_64\_EXT";

1241. case SHT\_IA\_64\_UNWIND:

1242. return "IA\_64\_UNWIND";

1243. case SHT\_IA\_64\_PRIORITY\_INIT:

1244. return "IA\_64\_PRIORITY\_INIT";

1245. case SHT\_IA\_64\_VMS\_TRACE:

1246. return "VMS\_TRACE";

1247. case SHT\_IA\_64\_VMS\_TIE\_SIGNATURES:

1248. return "VMS\_TIE\_SIGNATURES";

1249. case SHT\_IA\_64\_VMS\_DEBUG:

1250. return "VMS\_DEBUG";

1251. case SHT\_IA\_64\_VMS\_DEBUG\_STR:

1252. return "VMS\_DEBUG\_STR";

1253. case SHT\_IA\_64\_VMS\_LINKAGES:

1254. return "VMS\_LINKAGES";

1255. case SHT\_IA\_64\_VMS\_SYMBOL\_VECTOR:

1256. return "VMS\_SYMBOL\_VECTOR";

1257. case SHT\_IA\_64\_VMS\_FIXUP:

1258. return "VMS\_FIXUP";

1259. default:

1260. break;

1261. }

1262. return NULL;

1263.

1264.

1265. }

1266. /\*获取 x86 64节类型名\*/

1267. const char \*ELF\_process::get\_x86\_64\_section\_type\_name(unsigned int sh\_type)

1268. {

1269.

1270.

1271. switch (sh\_type)

1272. {

1273. case SHT\_X86\_64\_UNWIND:

1274. return "X86\_64\_UNWIND";

1275. default:

1276. break;

1277. }

1278. return NULL;

1279.

1280. }

1281. /\*获取AArch64节类型名\*/

1282. const char \*ELF\_process::get\_aarch64\_section\_type\_name(unsigned int sh\_type)

1283. {

1284.

1285.

1286. switch (sh\_type)

1287. {

1288. case SHT\_AARCH64\_ATTRIBUTES:

1289. return "AARCH64\_ATTRIBUTES";

1290. default:

1291. break;

1292. }

1293. return NULL;

1294.

1295.

1296.

1297. }

1298. /\*获取ARM架构的节类型名\*/

1299. const char \*ELF\_process::get\_arm\_section\_type\_name(unsigned int sh\_type)

1300. {

1301.

1302. switch (sh\_type)

1303. {

1304. case SHT\_ARM\_EXIDX:

1305. return "ARM\_EXIDX";

1306. case SHT\_ARM\_PREEMPTMAP:

1307. return "ARM\_PREEMPTMAP";

1308. case SHT\_ARM\_ATTRIBUTES:

1309. return "ARM\_ATTRIBUTES";

1310. case SHT\_ARM\_DEBUGOVERLAY:

1311. return "ARM\_DEBUGOVERLAY";

1312. case SHT\_ARM\_OVERLAYSECTION:

1313. return "ARM\_OVERLAYSECTION";

1314. default:

1315. break;

1316. }

1317. return NULL;

1318. }

1319. /\*获取Tic6X架构的节类型名\*/

1320. const char \*ELF\_process::get\_tic6x\_section\_type\_name(unsigned int sh\_type)

1321. {

1322.

1323. switch (sh\_type)

1324. {

1325. case SHT\_C6000\_UNWIND:

1326. return "C6000\_UNWIND";

1327. case SHT\_C6000\_PREEMPTMAP:

1328. return "C6000\_PREEMPTMAP";

1329. case SHT\_C6000\_ATTRIBUTES:

1330. return "C6000\_ATTRIBUTES";

1331. case SHT\_TI\_ICODE:

1332. return "TI\_ICODE";

1333. case SHT\_TI\_XREF:

1334. return "TI\_XREF";

1335. case SHT\_TI\_HANDLER:

1336. return "TI\_HANDLER";

1337. case SHT\_TI\_INITINFO:

1338. return "TI\_INITINFO";

1339. case SHT\_TI\_PHATTRS:

1340. return "TI\_PHATTRS";

1341. default:

1342. break;

1343. }

1344. return NULL;

1345.

1346.

1347. }

1348. /\*获取MSP430x架构的节类型名\*/

1349. const char \*ELF\_process::get\_msp430x\_section\_type\_name(unsigned int sh\_type)

1350. {

1351.

1352. switch (sh\_type)

1353. {

1354. case SHT\_MSP430\_SEC\_FLAGS:

1355. return "MSP430\_SEC\_FLAGS";

1356. case SHT\_MSP430\_SYM\_ALIASES:

1357. return "MSP430\_SYM\_ALIASES";

1358. case SHT\_MSP430\_ATTRIBUTES:

1359. return "MSP430\_ATTRIBUTES";

1360. default:

1361. return NULL;

1362. }

1363. }

1364.

1365.

1366.

1367.

1368. /\*获取段段类型\*/

1369. const char \*ELF\_process::get\_segment\_type(unsigned int p\_type)

1370. {

1371.

1372. static char buff[32];

1373.

1374. switch (p\_type)

1375. {

1376. case PT\_NULL:

1377. return "NULL";

1378. case PT\_LOAD:

1379. return "LOAD";

1380. case PT\_DYNAMIC:

1381. return "DYNAMIC";

1382. case PT\_INTERP:

1383. return "INTERP";

1384. case PT\_NOTE:

1385. return "NOTE";

1386. case PT\_SHLIB:

1387. return "SHLIB";

1388. case PT\_PHDR:

1389. return "PHDR";

1390. case PT\_TLS:

1391. return "TLS";

1392.

1393. case PT\_GNU\_EH\_FRAME:

1394. return "GNU\_EH\_FRAME";

1395. case PT\_GNU\_STACK:

1396. return "GNU\_STACK";

1397. case PT\_GNU\_RELRO:

1398. return "GNU\_RELRO";

1399.

1400. default:

1401. if ((p\_type >= PT\_LOPROC) && (p\_type <= PT\_HIPROC))

1402. {

1403. const char \* result;

1404.

1405. switch (elf\_header.e\_machine)

1406. {

1407. case EM\_AARCH64:

1408. result = get\_aarch64\_segment\_type (p\_type);

1409. break;

1410. case EM\_ARM:

1411. result = get\_arm\_segment\_type (p\_type);

1412. break;

1413. case EM\_MIPS:

1414. case EM\_MIPS\_RS3\_LE:

1415. result = get\_mips\_segment\_type (p\_type);

1416. break;

1417. case EM\_PARISC:

1418. result = get\_parisc\_segment\_type (p\_type);

1419. break;

1420. case EM\_IA\_64:

1421. result = get\_ia64\_segment\_type (p\_type);

1422. break;

1423. case EM\_TI\_C6000:

1424. result = get\_tic6x\_segment\_type (p\_type);

1425. break;

1426. default:

1427. result = NULL;

1428. break;

1429. }

1430.

1431. if (result != NULL)

1432. return result;

1433.

1434. sprintf (buff, "LOPROC+%x", p\_type - PT\_LOPROC);

1435. }

1436. else if ((p\_type >= PT\_LOOS) && (p\_type <= PT\_HIOS))

1437. {

1438. const char \* result;

1439.

1440. switch (elf\_header.e\_machine)

1441. {

1442. case EM\_PARISC:

1443. result = get\_parisc\_segment\_type (p\_type);

1444. break;

1445. case EM\_IA\_64:

1446. result = get\_ia64\_segment\_type (p\_type);

1447. break;

1448. default:

1449. result = NULL;

1450. break;

1451. }

1452.

1453. if (result != NULL)

1454. return result;

1455.

1456. sprintf (buff, "LOOS+%x", p\_type - PT\_LOOS);

1457. }

1458. else

1459. snprintf (buff, sizeof (buff), ("<unknown>: %x"), p\_type);

1460.

1461. return buff;

1462. }

1463.

1464. }

1465.

1466. int ELF\_process::process\_section\_group(FILE \*file) {

1467. unsigned int flag=0;

1468. Elf32\_Shdr \* section;

1469. section = NULL;

1470. char \* string\_table;

1471. unsigned int flag\_shoff;

1472. /\* Read in the string table, so that we have names to display. \*/

1473. if (elf\_header.e\_shstrndx != SHN\_UNDEF

1474. && elf\_header.e\_shstrndx < elf\_header.e\_shnum)

1475. {

1476. section = section\_headers + elf\_header.e\_shstrndx;

1477.

1478. flag\_shoff = section->sh\_offset;

1479.

1480. }

1481. section = section\_headers;

1482. unsigned int countC;

1483. if (is\_32bit\_elf){

1484.

1485. for (int i = 0;

1486. i < elf\_header.e\_shnum;

1487. i++, section++)

1488. {

1489. if(section->sh\_type==SHT\_GROUP){

1490. if(!flag){

1491. printf(" [Nr] Name Type Addr Off Size ES Flg Lk Inf Al\n");

1492. flag=1;

1493. }

1494. printf (" [%2u] ", i);

1495.

1496. countC = flag\_shoff + section->sh\_name;

1497.

1498. fseek(file,countC,SEEK\_SET);

1499. char string\_name[20];

1500. fread(string\_name,20,1,file);

1501.

1502. printf("%-16s ",string\_name);

1503.

1504. printf ( " %-15.15s ",

1505. get\_section\_type\_name (section->sh\_type));

1506.

1507. printf("%6.8lx",(unsigned long) section->sh\_addr);

1508. printf ( " %6.6lx %6.6lx %2.2lx",

1509. (unsigned long) section->sh\_offset,

1510. (unsigned long) section->sh\_size,

1511. (unsigned long) section->sh\_entsize);

1512.

1513. if (section->sh\_flags)

1514. printf (" %2.2x ", section->sh\_flags);

1515. else

1516. printf("%4c",32);

1517.

1518. printf ("%2u ", section->sh\_link);

1519. printf ("%3u %3lu", section->sh\_info,

1520. (unsigned long) section->sh\_addralign);

1521. printf("\n");

1522. }

1523. }

1524. if(!flag){

1525. printf("There are no section group in this file.\n");

1526. return 0;

1527. }

1528. }

1529.

1530. return 1;

1531. }

1532.

1533.

1534. int ELF\_process::process\_program\_headers(FILE \*file)

1535. {

1536.

1537. Elf32\_Phdr\* segment;

1538. unsigned long dynamic\_addr;

1539. if(elf\_header.e\_phnum == 0)

1540. {

1541.

1542. if(elf\_header.e\_phoff!=0)

1543. {

1544. printf ("possibly corrupt ELF header - it has a non-zero program"

1545. " header offset, but no program headers");

1546. }

1547. else

1548. {

1549. printf ("\nThere are no program headers in this file.\n");

1550. return 0;

1551. }

1552.

1553. }

1554. else

1555. {

1556. /\*打印相关的信息\*/

1557. if(elf\_header.e\_phnum>1)

1558. printf ("\nProgram Headers:\n");

1559. else

1560. printf ("\nProgram Header:\n");

1561.

1562. if(is\_32bit\_elf)

1563. printf(" Type Offset VirtAddr PhysAddr FileSiz MemSiz Flg Align\n");

1564. else

1565. printf(" Type Offset VirtAddr PhysAddr FileSiz MemSiz Flg Align\n");

1566.

1567. }

1568.

1569. /\*获取程序段头表信息\*/

1570. if (! get\_program\_headers (file))

1571. return 0;

1572.

1573.

1574. unsigned int i;

1575. for (i = 0, segment = program\_headers;

1576. i < elf\_header.e\_phnum;

1577. i++, segment++)

1578. {

1579. printf (" %-14.14s ", get\_segment\_type (segment->p\_type));

1580.

1581. if(is\_32bit\_elf) /\*如果是32位的话，那么输出程序段的相关信息\*/

1582. {

1583. printf ("0x%6.6x ", (unsigned int) segment->p\_offset);

1584. printf ("0x%8.8x ", (unsigned int) segment->p\_vaddr);

1585. printf ("0x%8.8x ", (unsigned int) segment->p\_paddr);

1586. printf ("0x%5.5x ", (unsigned int) segment->p\_filesz);

1587. printf ("0x%5.5x ", (unsigned int) segment->p\_memsz);

1588. printf ("%c%c%c ",

1589. (segment->p\_flags & PF\_R ? 'R' : ' '),

1590. (segment->p\_flags & PF\_W ? 'W' : ' '),

1591. (segment->p\_flags & PF\_X ? 'E' : ' '));

1592. printf ("%#x", (unsigned int) segment->p\_align);

1593. }

1594.

1595. printf("\n");

1596.

1597. }

1598.

1599. return 0;

1600. }

1601.

1602. /\*获取aarch64程序段类型\*/

1603. const char \*ELF\_process::get\_aarch64\_segment\_type(unsigned long type)

1604. {

1605.

1606. switch (type)

1607. {

1608. case PT\_AARCH64\_ARCHEXT:

1609. return "AARCH64\_ARCHEXT";

1610. default:

1611. break;

1612. }

1613.

1614. return NULL;

1615.

1616. }

1617. /\*获取ARM程序段类型\*/

1618. const char \*ELF\_process::get\_arm\_segment\_type(unsigned long type)

1619. {

1620.

1621. switch (type)

1622. {

1623. case PT\_ARM\_EXIDX:

1624. return "EXIDX";

1625. default:

1626. break;

1627. }

1628.

1629. return NULL;

1630.

1631. }

1632. /\*获取MIPS程序段信息\*/

1633. const char \*ELF\_process::get\_mips\_segment\_type(unsigned long type)

1634. {

1635.

1636. switch (type)

1637. {

1638. case PT\_MIPS\_REGINFO:

1639. return "REGINFO";

1640. case PT\_MIPS\_RTPROC:

1641. return "RTPROC";

1642. case PT\_MIPS\_OPTIONS:

1643. return "OPTIONS";

1644. default:

1645. break;

1646. }

1647.

1648. return NULL;

1649. }

1650. /\*获取PA-RISC程序段信息\*/

1651. const char \*ELF\_process::get\_parisc\_segment\_type(unsigned long type)

1652. {

1653. switch (type)

1654. {

1655. case PT\_HP\_TLS:

1656. return "HP\_TLS";

1657. case PT\_HP\_CORE\_NONE:

1658. return "HP\_CORE\_NONE";

1659. case PT\_HP\_CORE\_VERSION:

1660. return "HP\_CORE\_VERSION";

1661. case PT\_HP\_CORE\_KERNEL:

1662. return "HP\_CORE\_KERNEL";

1663. case PT\_HP\_CORE\_COMM:

1664. return "HP\_CORE\_COMM";

1665. case PT\_HP\_CORE\_PROC:

1666. return "HP\_CORE\_PROC";

1667. case PT\_HP\_CORE\_LOADABLE:

1668. return "HP\_CORE\_LOADABLE";

1669. case PT\_HP\_CORE\_STACK:

1670. return "HP\_CORE\_STACK";

1671. case PT\_HP\_CORE\_SHM:

1672. return "HP\_CORE\_SHM";

1673. case PT\_HP\_CORE\_MMF:

1674. return "HP\_CORE\_MMF";

1675. case PT\_HP\_PARALLEL:

1676. return "HP\_PARALLEL";

1677. case PT\_HP\_FASTBIND:

1678. return "HP\_FASTBIND";

1679. case PT\_HP\_OPT\_ANNOT:

1680. return "HP\_OPT\_ANNOT";

1681. case PT\_HP\_HSL\_ANNOT:

1682. return "HP\_HSL\_ANNOT";

1683. case PT\_HP\_STACK:

1684. return "HP\_STACK";

1685. case PT\_HP\_CORE\_UTSNAME:

1686. return "HP\_CORE\_UTSNAME";

1687. case PT\_PARISC\_ARCHEXT:

1688. return "PARISC\_ARCHEXT";

1689. case PT\_PARISC\_UNWIND:

1690. return "PARISC\_UNWIND";

1691. case PT\_PARISC\_WEAKORDER:

1692. return "PARISC\_WEAKORDER";

1693. default:

1694. break;

1695. }

1696.

1697. return NULL;

1698.

1699.

1700. }

1701. /\*获取IA-64程序段信息\*/

1702. const char \*ELF\_process::get\_ia64\_segment\_type(unsigned long type)

1703. {

1704.

1705. switch (type)

1706. {

1707. case PT\_IA\_64\_ARCHEXT:

1708. return "IA\_64\_ARCHEXT";

1709. case PT\_IA\_64\_UNWIND:

1710. return "IA\_64\_UNWIND";

1711. case PT\_HP\_TLS:

1712. return "HP\_TLS";

1713. case PT\_IA\_64\_HP\_OPT\_ANOT:

1714. return "HP\_OPT\_ANNOT";

1715. case PT\_IA\_64\_HP\_HSL\_ANOT:

1716. return "HP\_HSL\_ANNOT";

1717. case PT\_IA\_64\_HP\_STACK:

1718. return "HP\_STACK";

1719. default:

1720. break;

1721. }

1722.

1723. return NULL;

1724. }

1725. #define PT\_C6000\_PHATTR 0x70000000

1726. /\*获取TIC6x程序段信息\*/

1727. const char \*ELF\_process::get\_tic6x\_segment\_type(unsigned long type)

1728. {

1729. switch (type)

1730. {

1731. case PT\_C6000\_PHATTR:

1732. return "C6000\_PHATTR";

1733. default:

1734. break;

1735. }

1736.

1737. return NULL;

1738.

1739.

1740. }

1741. /\*获取程序头表\*/

1742. int ELF\_process::get\_program\_headers(FILE \*file)

1743. {

1744.

1745. Elf32\_Phdr\* phdrs;

1746. Elf64\_Phdr\* phdrs64;

1747.

1748. /\* Check cache of prior read. \*/

1749. if (program\_headers != NULL)

1750. return 1;

1751.

1752. phdrs = (Elf32\_Phdr \*) cmalloc (elf\_header.e\_phnum,

1753. sizeof (Elf32\_Phdr));

1754. phdrs64 = (Elf64\_Phdr \*) cmalloc (elf\_header.e\_phnum,

1755. sizeof (Elf64\_Phdr));

1756. if (phdrs == NULL)

1757. {

1758. printf("Out of memory\n");

1759. return 0;

1760. }

1761. //获取32位程序头表

1762. if (is\_32bit\_elf

1763. ? get\_32bit\_program\_headers (file, phdrs)

1764. : get\_64bit\_program\_headers (file, phdrs64))

1765. {

1766. program\_headers = phdrs;

1767. return 1;

1768. }

1769.

1770. free (phdrs);

1771. free (phdrs64);

1772. return 0;

1773.

1774.

1775.

1776. }

1777. /\*获取32位程序头表\*/

1778. int ELF\_process::get\_32bit\_program\_headers(FILE \*file, Elf32\_Phdr \*pheaders)

1779. {

1780. /\*初始化结构体\*/

1781. Elf32\_External\_Phdr\* phdrs;

1782. Elf32\_External\_Phdr\* external;

1783. Elf32\_Phdr\* internal;

1784.

1785. unsigned int i;

1786. /\*从ELF文件头中读取程序段的相关信息\*/

1787. phdrs = (Elf32\_External\_Phdr \*) get\_data (NULL, file, elf\_header.e\_phoff,

1788. elf\_header.e\_phentsize,

1789. elf\_header.e\_phnum,

1790. ("program headers"));

1791.

1792. if (!phdrs)

1793. return 0;

1794.

1795. for (i = 0, internal = pheaders, external = phdrs;

1796. i < elf\_header.e\_phnum;

1797. i++, internal++, external++)

1798. {

1799.

1800. internal->p\_type = BYTE\_GET (external->p\_type);

1801. internal->p\_offset = BYTE\_GET (external->p\_offset);

1802. internal->p\_vaddr = BYTE\_GET (external->p\_vaddr);

1803. internal->p\_paddr = BYTE\_GET (external->p\_paddr);

1804. internal->p\_filesz = BYTE\_GET (external->p\_filesz);

1805. internal->p\_memsz = BYTE\_GET (external->p\_memsz);

1806. internal->p\_flags = BYTE\_GET (external->p\_flags);

1807. internal->p\_align = BYTE\_GET (external->p\_align);

1808. }

1809. free (phdrs);

1810.

1811. return 1;

1812. }

1813. /\*获取64位程序头表信息-暂未实现\*/

1814. int ELF\_process::get\_64bit\_program\_headers(FILE \*file, Elf64\_Phdr \*pheaders)

1815. {

1816.

1817.

1818. return 0;

1819. }

1820.

1821.

1822. int ELF\_process::process\_dynamic\_section(FILE \*file)

1823. {

1824.

1825. Elf32\_Dyn \* entry;

1826.

1827. if(dynamic\_addr)

1828. {

1829. printf ("\nDynamic section at offset 0x%x contains %u entries:\n",

1830. dynamic\_addr, dynamic\_nent);

1831. printf (" Tag Type Name/Value\n");

1832. }else{

1833. printf ("\nThere are no dynamic section in this file.\n");

1834. return 0;

1835. }

1836. if (is\_32bit\_elf)

1837. {

1838. if (! get\_32bit\_dynamic\_section (file))

1839. return 0;

1840. }

1841. else if (! get\_64bit\_dynamic\_section (file))

1842. return 0;

1843.

1844. for (entry = dynamic\_section;

1845. entry < dynamic\_section + dynamic\_nent;

1846. entry++)

1847. {

1848.

1849. const char \* dtype;

1850. putchar (' ');

1851. printf("0x%2.8x ",entry->d\_tag);

1852. dtype = get\_dynamic\_type(entry->d\_tag);

1853. printf("(%s)%\*s",dtype,(int)(27-strlen(dtype))," ");

1854.

1855.

1856. switch (entry->d\_tag)

1857. {

1858. case DT\_FLAGS:

1859. print\_dynamic\_flags (entry->d\_un.d\_val);

1860. break;

1861.

1862. case DT\_AUXILIARY:

1863. case DT\_FILTER:

1864. case DT\_CONFIG:

1865. case DT\_DEPAUDIT:

1866. case DT\_AUDIT:

1867. switch (entry->d\_tag)

1868. {

1869. case DT\_AUXILIARY:

1870. printf ("Auxiliary library");

1871. break;

1872.

1873. case DT\_FILTER:

1874. printf ("Filter library");

1875. break;

1876.

1877. case DT\_CONFIG:

1878. printf ("Configuration file");

1879. break;

1880.

1881. case DT\_DEPAUDIT:

1882. printf ("Dependency audit library");

1883. break;

1884.

1885. case DT\_AUDIT:

1886. printf ("Audit library");

1887. break;

1888. }

1889. break;

1890.

1891. default:

1892. printf("0x%x",entry->d\_un.d\_val);

1893. }

1894.

1895. printf("\n");

1896. }

1897.

1898.

1899. }

1900.

1901.

1902.

1903. int ELF\_process::get\_32bit\_dynamic\_section(FILE \*file)

1904. {

1905.

1906. Elf32\_External\_Dyn \* edyn = (Elf32\_External\_Dyn \*) malloc(dynamic\_size);

1907. Elf32\_External\_Dyn \* ext;

1908. Elf32\_Dyn \* entry;

1909.

1910. fseek(file,dynamic\_addr,SEEK\_SET);

1911. fread(edyn,dynamic\_size,1,file);

1912.

1913.

1914. if(edyn==NULL)

1915. return 0;

1916.

1917. for (ext = edyn, dynamic\_nent = 0;

1918. (char \*) ext < (char \*) edyn + dynamic\_size;

1919. ext++)

1920. {

1921. dynamic\_nent++;

1922. if (BYTE\_GET (ext->d\_tag) == DT\_NULL)

1923. break;

1924. }

1925.

1926. dynamic\_section = (Elf32\_Dyn \*) cmalloc (dynamic\_nent,

1927. sizeof (\* entry));

1928.

1929. if (dynamic\_section == NULL)

1930. {

1931. printf("Out of memory\n");

1932. free (edyn);

1933. return 0;

1934. }

1935.

1936.

1937. for (ext = edyn, entry = dynamic\_section;

1938. entry < dynamic\_section + dynamic\_nent;

1939. ext++, entry++)

1940. {

1941. entry->d\_tag = BYTE\_GET (ext->d\_tag);

1942. entry->d\_un.d\_val = BYTE\_GET (ext->d\_un.d\_val);

1943. }

1944.

1945. free(edyn);

1946.

1947. return 1;

1948.

1949.

1950. }

1951.

1952. int ELF\_process::get\_64bit\_dynamic\_section(FILE \*file)

1953. {

1954.

1955. return 0;

1956. }

1957.

1958. void ELF\_process::print\_dynamic\_flags(Elf32\_Word flags)

1959. {

1960.

1961. int first = 1;

1962.

1963. while (flags)

1964. {

1965. Elf32\_Word flag;

1966.

1967. flag = flags & - flags;

1968. flags &= ~ flag;

1969.

1970. if (first)

1971. first = 0;

1972. else

1973. putc (' ', stdout);

1974.

1975. switch (flag)

1976. {

1977. case DF\_ORIGIN:

1978. fputs ("ORIGIN", stdout);

1979. break;

1980. case DF\_SYMBOLIC:

1981. fputs ("SYMBOLIC", stdout);

1982. break;

1983. case DF\_TEXTREL:

1984. fputs ("TEXTREL", stdout);

1985. break;

1986. case DF\_BIND\_NOW:

1987. fputs ("BIND\_NOW", stdout);

1988. break;

1989. case DF\_STATIC\_TLS:

1990. fputs ("STATIC\_TLS", stdout);

1991. break;

1992. default:

1993. fputs (("unknown"), stdout);

1994. break;

1995. }

1996. }

1997.

1998. }

1999. #define DT\_FEATURE 0x6ffffdfc

2000. #define DT\_USED 0x7ffffffe

2001. const char \*ELF\_process::get\_dynamic\_type(unsigned long type)

2002. {

2003.

2004. static char buff[64];

2005.

2006. switch (type)

2007. {

2008.

2009. case DT\_NULL:

2010. return "NULL";

2011. case DT\_NEEDED:

2012. return "NEEDED";

2013. case DT\_PLTRELSZ:

2014. return "PLTRELSZ";

2015. case DT\_PLTGOT:

2016. return "PLTGOT";

2017. case DT\_HASH:

2018. return "HASH";

2019. case DT\_STRTAB:

2020. return "STRTAB";

2021. case DT\_SYMTAB:

2022. return "SYMTAB";

2023. case DT\_RELA:

2024. return "RELA";

2025. case DT\_RELASZ:

2026. return "RELASZ";

2027. case DT\_RELAENT:

2028. return "RELAENT";

2029. case DT\_STRSZ:

2030. return "STRSZ";

2031. case DT\_SYMENT:

2032. return "SYMENT";

2033. case DT\_INIT:

2034. return "INIT";

2035. case DT\_FINI:

2036. return "FINI";

2037. case DT\_SONAME:

2038. return "SONAME";

2039. case DT\_RPATH:

2040. return "RPATH";

2041. case DT\_SYMBOLIC:

2042. return "SYMBOLIC";

2043. case DT\_REL:

2044. return "REL";

2045. case DT\_RELSZ:

2046. return "RELSZ";

2047. case DT\_RELENT:

2048. return "RELENT";

2049. case DT\_PLTREL:

2050. return "PLTREL";

2051. case DT\_DEBUG:

2052. return "DEBUG";

2053. case DT\_TEXTREL:

2054. return "TEXTREL";

2055. case DT\_JMPREL:

2056. return "JMPREL";

2057. case DT\_BIND\_NOW:

2058. return "BIND\_NOW";

2059. case DT\_INIT\_ARRAY:

2060. return "INIT\_ARRAY";

2061. case DT\_FINI\_ARRAY:

2062. return "FINI\_ARRAY";

2063. case DT\_INIT\_ARRAYSZ:

2064. return "INIT\_ARRAYSZ";

2065. case DT\_FINI\_ARRAYSZ:

2066. return "FINI\_ARRAYSZ";

2067. case DT\_RUNPATH:

2068. return "RUNPATH";

2069. case DT\_FLAGS:

2070. return "FLAGS";

2071.

2072. case DT\_PREINIT\_ARRAY:

2073. return "PREINIT\_ARRAY";

2074. case DT\_PREINIT\_ARRAYSZ:

2075. return "PREINIT\_ARRAYSZ";

2076.

2077. case DT\_CHECKSUM:

2078. return "CHECKSUM";

2079. case DT\_PLTPADSZ:

2080. return "PLTPADSZ";

2081. case DT\_MOVEENT:

2082. return "MOVEENT";

2083. case DT\_MOVESZ:

2084. return "MOVESZ";

2085. case DT\_FEATURE:

2086. return "FEATURE";

2087. case DT\_POSFLAG\_1:

2088. return "POSFLAG\_1";

2089. case DT\_SYMINSZ:

2090. return "SYMINSZ";

2091. case DT\_SYMINENT:

2092. return "SYMINENT"; /\* aka VALRNGHI \*/

2093.

2094. case DT\_ADDRRNGLO:

2095. return "ADDRRNGLO";

2096. case DT\_CONFIG:

2097. return "CONFIG";

2098. case DT\_DEPAUDIT:

2099. return "DEPAUDIT";

2100. case DT\_AUDIT:

2101. return "AUDIT";

2102. case DT\_PLTPAD:

2103. return "PLTPAD";

2104. case DT\_MOVETAB:

2105. return "MOVETAB";

2106. case DT\_SYMINFO:

2107. return "SYMINFO"; /\* aka ADDRRNGHI \*/

2108.

2109. case DT\_VERSYM:

2110. return "VERSYM";

2111.

2112. case DT\_TLSDESC\_GOT:

2113. return "TLSDESC\_GOT";

2114. case DT\_TLSDESC\_PLT:

2115. return "TLSDESC\_PLT";

2116. case DT\_RELACOUNT:

2117. return "RELACOUNT";

2118. case DT\_RELCOUNT:

2119. return "RELCOUNT";

2120. case DT\_FLAGS\_1:

2121. return "FLAGS\_1";

2122. case DT\_VERDEF:

2123. return "VERDEF";

2124. case DT\_VERDEFNUM:

2125. return "VERDEFNUM";

2126. case DT\_VERNEED:

2127. return "VERNEED";

2128. case DT\_VERNEEDNUM:

2129. return "VERNEEDNUM";

2130.

2131. case DT\_AUXILIARY:

2132. return "AUXILIARY";

2133. case DT\_USED:

2134. return "USED";

2135. case DT\_FILTER:

2136. return "FILTER";

2137.

2138. case DT\_GNU\_PRELINKED:

2139. return "GNU\_PRELINKED";

2140. case DT\_GNU\_CONFLICT:

2141. return "GNU\_CONFLICT";

2142. case DT\_GNU\_CONFLICTSZ:

2143. return "GNU\_CONFLICTSZ";

2144. case DT\_GNU\_LIBLIST:

2145. return "GNU\_LIBLIST";

2146. case DT\_GNU\_LIBLISTSZ:

2147. return "GNU\_LIBLISTSZ";

2148. case DT\_GNU\_HASH:

2149. return "GNU\_HASH";

2150.

2151.

2152. }

2153.

2154. return NULL;

2155. }

2156.

2157. #define ARRAY\_SIZE(a) (sizeof (a) / sizeof ((a)[0]))

2158. #define FALSE 0

2159. #define TRUE 1

2160. #define UNKNOWN -1

2161. static struct

2162. {

2163. const char \* name;

2164. int reloc;

2165. int size;

2166. int rela;

2167. } dynamic\_relocations [] =

2168. {

2169. { "REL", DT\_REL, DT\_RELSZ, FALSE },

2170. { "RELA", DT\_RELA, DT\_RELASZ, TRUE },

2171. { "PLT", DT\_JMPREL, DT\_PLTRELSZ, UNKNOWN }

2172. };

2173. Elf32\_Rel\* elf32\_rel;

2174. int ELF\_process::process\_relocs(FILE \*file)

2175. {

2176.

2177. printf("\nrelocs:");

2178. Elf32\_Rel\* entry\_rel;

2179.

2180. if(is\_32bit\_elf)

2181. {

2182. get\_32bit\_rel(file,rel\_dyn\_offset);

2183. }

2184. else

2185. {

2186. //64λ...

2187. }

2188. printf (" \nat offset 0x%2.2x contains %u entries:\n",

2189. rel\_dyn\_offset, rel\_nent);

2190. printf (" Offset Info Type Sym. Value Sym. Name\n");

2191. for (entry\_rel = elf32\_rel;

2192. entry\_rel < elf32\_rel + rel\_nent;

2193. entry\_rel++)

2194. {

2195. printf("%10.8x ",entry\_rel->r\_offset);

2196. printf("%15.8x\n",entry\_rel->r\_info);

2197. }

2198.

2199.

2200. return 0;

2201. }

2202.

2203.

2204.

2205. void ELF\_process::get\_32bit\_rel(FILE \*pFILE, unsigned int offset)

2206. {

2207.

2208. Elf32\_External\_Rel\* rel= (Elf32\_External\_Rel \*) malloc(rel\_dyn\_size);

2209. Elf32\_External\_Rel\* ext;

2210. Elf32\_Rel\* relt;

2211.

2212. fseek(pFILE,offset,SEEK\_SET);

2213. fread(rel,rel\_dyn\_size,1,pFILE);

2214.

2215. if(rel==NULL)

2216. return;

2217.

2218. for (ext = rel, rel\_nent = 0;

2219. (char \*) ext < (char \*) rel + rel\_dyn\_size;

2220. ext++)

2221. {

2222. rel\_nent++;

2223. if (BYTE\_GET (rel->r\_offset) == DT\_NULL)

2224. break;

2225. }

2226.

2227. elf32\_rel = (Elf32\_Rel \*) cmalloc (dynamic\_nent,

2228. sizeof (\* relt));

2229.

2230.

2231. for (ext = rel, relt = elf32\_rel;

2232. relt < elf32\_rel + rel\_nent;

2233. ext++, relt++)

2234. {

2235. relt->r\_offset = BYTE\_GET (ext->r\_offset);

2236. relt->r\_info = BYTE\_GET (ext->r\_info);

2237. }

2238.

2239. free(rel);

2240.

2241. return;

2242. }

2243.

2244. //处理打印符号表

2245. void ELF\_process::process\_symbol\_table(FILE \*pFILE,int option)

2246. {

2247. Elf32\_Sym\* sym;

2248. /\*定义32位符号表\*/

2249. get\_32bit\_symbol(pFILE,option);

2250. unsigned int i;

2251. /\*判断option的第5位是否为1\*/

2252. if(option & (1<<5)) //-s

2253. {

2254. //打印列名

2255. printf("Num Value NdX other info Size Name\n");

2256. //遍历符号表中的每一个符号项

2257. for (i=0, sym = sym\_dyn; sym<sym\_dyn+sym\_nent; sym++,i++)

2258. {

2259. //打印符号在符号表中的索引

2260. printf("%2d: ",i);

2261. //打印符号的值，这个值因不同的符号类型而异

2262. printf("%2.8x ",sym->st\_value);

2263. //打印符号所在的节区的索引

2264. printf("%-2.2x",sym->st\_shndx);

2265. //打印符号的其他信息

2266. printf("%-12.2x ",sym->st\_other);

2267. //打印符号的类型和绑定方式，低4为为类型，高28位为绑定方式

2268. printf("%-12.2x ",sym->st\_info);

2269. //打印符号的大小

2270. printf("%-12.2x ",sym->st\_size);

2271. //调用函数使用st\_name符号名索引在strtab表中找到对应的符号名

2272. get\_32bit\_strdyn(pFILE,sym->st\_name);

2273. }

2274. }

2275. <<<<<<< HEAD

2276. //这个是打印统计信息的

2277. =======

2278. /\*判断option的第13位是否为1\*/

2279. >>>>>>> 9188e7c23a63c8f754a88ac11cc64a343182f39a

2280. if(option & (1<<13)) //-I

2281. {

2282. //输出列名和提示

2283. printf("\nbucket list:\n");

2284. printf("Num Size of total \n");

2285. int sum=0;

2286. //遍历符号表中的每一个符号

2287. for (i=0, sym = sym\_dyn; sym<sym\_dyn+sym\_nent; sym++,i++)

2288. {

2289. //统计全部符号占用的大小

2290. sum+=sym->st\_size;

2291. }

2292. //再次遍历符号表中的每一个符号

2293. for (i=0, sym = sym\_dyn; sym<sym\_dyn+sym\_nent; sym++,i++)

2294. {

2295. //输出每个符号占用的空间的比例

2296. printf("%3d: ",i);

2297. printf("%-12.2x ",sym->st\_size);

2298. printf(" %f \n",1.0\*(sym->st\_size)/sum);

2299. }

2300. }

2301. }

2302. //从文件中读取ELF32符号表

2303. void ELF\_process::get\_32bit\_symbol(FILE \*pFILE,int option)

2304. {

2305. //pFILE：文件

2306. //option：选项，附加参数

2307.

2308. //临时变量存储符号表

2309. Elf32\_External\_Sym\* exty = (Elf32\_External\_Sym \*) malloc(sym\_dyn\_size);

2310. Elf32\_External\_Sym\* ext;

2311. Elf32\_Sym\* symbool;

2312.

2313. //将文件读取指针移动至动态符号表偏移位置

2314. fseek(pFILE,sym\_dyn\_offset,SEEK\_SET);

2315. //读取符号表大小的数据到内存中

2316. fread(exty,sym\_dyn\_size,1,pFILE);

2317.

2318. //未读取到返回

2319. if (!exty)

2320. return;

2321. //遍历符号表，统计符号表项目数

2322. for (ext = exty, sym\_nent = 0;(char \*) ext < (char \*) exty + sym\_dyn\_size;ext++)

2323. {

2324. sym\_nent++;

2325. }

2326. if(option &(1<<5))

2327. printf ("\nSymbol tabel '.dynsym' contains %d entries\n",sym\_nent);

2328.

2329. //为动态符号表申请空间

2330. sym\_dyn = (Elf32\_Sym \*) cmalloc (sym\_nent,sizeof (\* exty));

2331.

2332. //遍历，赋值过去，这里是进行的大小端转换，可以参考之间的实验，结构体的问题才需要这样子做

2333. for (ext = exty, symbool = sym\_dyn ;symbool < sym\_dyn + sym\_nent;ext++, symbool++)

2334. {

2335. symbool->st\_name = BYTE\_GET(ext->st\_name);

2336. symbool->st\_info = BYTE\_GET(ext->st\_info);

2337. symbool->st\_other = BYTE\_GET(ext->st\_other);

2338. symbool->st\_shndx = BYTE\_GET(ext->st\_shndx);

2339. symbool->st\_size = BYTE\_GET(ext->st\_size);

2340. symbool->st\_value = BYTE\_GET(ext->st\_value);

2341. //printf("%2.2x ",sym\_dyn->st\_name);

2342. }

2343.

2344. //释放临时变量内存

2345. free(exty);

2346.

2347. return;

2348.

2349. }

2350.

2351. //查询符号名

2352. void ELF\_process::get\_32bit\_strdyn(FILE \*pFILE, Elf32\_Word name)

2353. {

2354. //pFILE：文件

2355. //name：符号名在符号名表中的索引

2356.

2357. //定义临时变量存放符号名

2358. unsigned char sym\_name[1024];

2359. //将文件的读取指针移动到符号名表的偏移地址处

2360. fseek(pFILE,(str\_dyn\_offset+name),SEEK\_SET);

2361. //将数据读入到临时变量中，

2362. //读取长度为1024是任意的，因此每个符号后面都跟着一个'/0'结束符

2363. fread(sym\_name,1024,1,pFILE);

2364. //输出符号名

2365. printf("%s\n",sym\_name);

2366. }

2367.

2368. void ELF\_process::print\_unwind(FILE \*file)

2369. {

2370.

2371. if(!strcmp(get\_machine\_name (elf\_header.e\_machine),"IA\_64"))

2372. {

2373. printf("\nThe decoding of unwind sections for machine type IA\_64 is waiting for perfection.\n");

2374. print\_xout(file, unwind\_idx);

2375. }

2376. else

2377. printf("\nThe decoding of unwind sections for machine type %s is not currently supported.\n",get\_machine\_name (elf\_header.e\_machine));

2378. }

2379.

2380. int ELF\_process::print\_xout(FILE \*pFILE, unsigned int offset)

2381. {

2382. if(offset>=elf\_header.e\_shnum){

2383. printf("no.[%d] section is not exist!!!\n",offset);

2384. return 0;

2385. }

2386. Elf32\_Shdr \*shdr=section\_headers+offset;

2387. //Elf32\_External\_Shdr \*ext;

2388. Elf32\_Shdr \* section;

2389. unsigned int flag\_shoff;

2390. section= section\_headers + elf\_header.e\_shstrndx;

2391. flag\_shoff = section->sh\_offset;

2392. if(!shdr){

2393. return 0;

2394. }

2395. unsigned int state=0;

2396. unsigned int addr=shdr->sh\_offset;

2397. unsigned int countC = flag\_shoff + shdr->sh\_name;

2398. char str[16]="";

2399. char data[1000];

2400. fseek(pFILE,countC,SEEK\_SET);

2401. char string\_name[20];

2402. fread(string\_name,20,1,pFILE);

2403. countC=shdr->sh\_offset;

2404. fseek(pFILE,countC,SEEK\_SET);

2405. fread(data,shdr->sh\_size,1,pFILE);

2406. printf("\nHex dump of section '%s':\n",string\_name);

2407. for(int i=0;i<shdr->sh\_size;i+=4)

2408. {

2409. if(state==0)

2410. {

2411. printf(" 0x%08x",addr);

2412. addr+=16;

2413. i-=4;

2414. }

2415. else{

2416. for(int j=0;j<4;j++)

2417. {

2418. printf("%02x",data[i+j]);

2419. str[(state-1)\*4+j]=data[i+j];

2420. }

2421. }

2422. if(state==4)

2423. {

2424. printf(" %d: %s\n",i+4,str);

2425. state=0;

2426. }

2427. else

2428. {

2429. state++;

2430. printf(" ");

2431. }

2432. }

2433. for(int i=0;i<(state==0?0:5-state);i++) printf(" ");

2434. if(state) printf("%s\n\n",str);

2435. return 1;

2436. }

2437.

2438.

2439.

2440.

2441. int ELF\_process::process\_note(FILE \*file) {

2442. int tag=false;

2443. Elf32\_Shdr \* shdr;

2444. Elf32\_Nhdr \* nhdr;

2445. int i;

2446. for(i=0,shdr=section\_headers;i < elf\_header.e\_shnum;i++,shdr++){

2447. if(shdr->sh\_type==SHT\_NOTE)

2448. {

2449. tag=true;

2450. get\_32bit\_nhdr(file,shdr->sh\_offset,shdr->sh\_size,nhdr);

2451. char \* n\_name=(char\*)nhdr+sizeof(Elf32\_Nhdr);

2452. printf("\nDisplaying notes found at file offset 0x%8x with the length 0x%8x\n",

2453. shdr->sh\_offset,shdr->sh\_size);

2454. printf(" Owner Data size Description\n");

2455. // printf(" %-18s0x%-10x%s\n",n\_name,nhdr->n\_descsz,note\_type\_map(nhdr->n\_type,n\_name));

2456. printf(" GNU 0x%-10x%s\n",nhdr->n\_descsz,note\_type\_map(nhdr->n\_type,n\_name));

2457. if(!strcmp(ELF\_NOTE\_GNU,n\_name)&&nhdr->n\_type==NT\_GNU\_BUILD\_ID)

2458. {

2459. char \* n\_desc=(char\*)(n\_name+nhdr->n\_namesz);

2460. printf(" Build ID: ");

2461. for(int j=0;j<nhdr->n\_descsz/sizeof(char);j++) printf("%x",(unsigned)(unsigned char)n\_desc[j]);

2462. printf("\n");

2463. }

2464. else if(!strcmp(ELF\_NOTE\_SOLARIS,n\_name)&&nhdr->n\_type==ELF\_NOTE\_PAGESIZE\_HINT)

2465. {

2466. int \* n\_desc=(int\*)(n\_name+nhdr->n\_namesz);

2467. printf(" Pagesize: 0x%x\n",\*n\_desc);

2468. }

2469. else if(!strcmp(ELF\_NOTE\_GNU,n\_name)&&nhdr->n\_type==NT\_GNU\_ABI\_TAG)

2470. {

2471. int \* n\_desc=(int\*)(n\_name+nhdr->n\_namesz);

2472. printf(" OS: %s, ABI: %d.%d.%d\n",

2473. get\_ABI\_tag(\*n\_desc)+12,

2474. \*(n\_desc+1),

2475. \*(n\_desc+2),

2476. \*(n\_desc+3)

2477. );

2478. }

2479. else if(!strcmp(ELF\_NOTE\_GNU,n\_name)&&nhdr->n\_type==NT\_GNU\_HWCAP)

2480. {

2481. int \* n\_desc=(int\*)(n\_name+nhdr->n\_namesz);

2482. int num=\*n\_desc;

2483. int mask=\*(n\_desc+1);

2484. n\_desc+=2;

2485. for(int j=0;j<num;j++)

2486. {

2487. char \* tmp=(char\*)n\_desc;

2488. printf(" %-30s%s\n",

2489. tmp+1,

2490. (1U << (\*tmp)) & mask?"enabled":"disabled"

2491. );

2492. n\_desc+=strlen(tmp);

2493. }

2494. }

2495. else if(!strcmp(ELF\_NOTE\_GNU,n\_name)&&nhdr->n\_type==NT\_GNU\_GOLD\_VERSION)

2496. {

2497. char \* n\_desc=(char\*)(n\_name+nhdr->n\_namesz);

2498. printf(" Version: %s\n",n\_desc);

2499. }

2500. else if(!strcmp(ELF\_NOTE\_GNU,n\_name)&&nhdr->n\_type==NT\_GNU\_PROPERTY\_TYPE\_0)

2501. {

2502. char \* n\_desc=(char\*)(n\_name+nhdr->n\_namesz);

2503. printf(" Properties: x86 feature: IBT, SHSTK\n");

2504. }

2505. }

2506. }

2507.

2508. return 0;

2509. }

2510.

2511. const char \* ELF\_process::note\_type\_map(unsigned int type, char \*name){

2512. static char buff[32];

2513. if(strcmp(name,ELF\_NOTE\_GNU)){

2514. if(type==ELF\_NOTE\_PAGESIZE\_HINT)

2515. return "ELF\_NOTE\_PAGESIZE\_HINT";

2516. }

2517. switch (type)

2518. {

2519. case NT\_GNU\_ABI\_TAG: return "NT\_GNU\_ABI\_TAG (ABI version tag)";

2520. case NT\_GNU\_HWCAP: return "NT\_GNU\_HWCAP";

2521. case NT\_GNU\_BUILD\_ID: return "NT\_GNU\_BUILD\_ID (unique build ID bitstring)";

2522. case NT\_GNU\_GOLD\_VERSION: return "NT\_GNU\_GOLD\_VERSION";

2523. case NT\_GNU\_PROPERTY\_TYPE\_0: return "NT\_GNU\_PROPERTY\_TYPE\_0";

2524.

2525. default:

2526. snprintf (buff, sizeof (buff), ("<unknown: %x>"), type);

2527. return buff;

2528. }

2529. }

2530.

2531.

2532.

2533. const char \* ELF\_process::get\_ABI\_tag(unsigned int n){

2534. switch(n)

2535. {

2536. case ELF\_NOTE\_OS\_LINUX:return "ELF\_NOTE\_OS\_LINUX";

2537. case ELF\_NOTE\_OS\_GNU:return "ELF\_NOTE\_OS\_GNU";

2538. case ELF\_NOTE\_OS\_SOLARIS2:return "ELF\_NOTE\_OS\_SOLARIS2";

2539. case ELF\_NOTE\_OS\_FREEBSD:return "ELF\_NOTE\_OS\_FREEBSD";

2540. default:return NULL;

2541. }

2542. }

2543. int ELF\_process::get\_32bit\_nhdr(FILE \*file,unsigned int offset,unsigned int size,Elf32\_Nhdr \*note){

2544. Elf32\_External\_Nhdr\* nhdr;

2545. Elf32\_External\_Nhdr\* external;

2546. Elf32\_Nhdr\* internal;

2547.

2548. nhdr = (Elf32\_External\_Nhdr\*) get\_data(NULL,file,offset,size,1,("note"));

2549.

2550. if(!nhdr)

2551. return 0;

2552.

2553. internal = note;

2554. external = nhdr;

2555. internal->n\_namesz = BYTE\_GET(external->n\_namesz);

2556. internal->n\_descsz = BYTE\_GET(external->n\_descsz);

2557. internal->n\_type = BYTE\_GET(external->n\_type);

2558. free(nhdr);

2559. return 1;

2560. }

2561.