**实验1** 完成漏洞挖掘环境搭建及固件分析

**实验目的：**

* + 学会使用固件分析、模拟固件工具 [粘贴脚本截图和shell截图]
  + 掌握分析常见固件分格式
  + 掌握解析固件文件技巧

**实验题目：**

1. 完成Binwalk工具安装，通过分析固件获取隐藏在固件中的密钥(截图固件中的登陆密钥)。
2. 完成静态编译的ARM架构的Hello World程序，使用qemu-arm-static、模拟运行该程序。(截图打印个人学号- Hello \*学号\*)

1.binwalk分析

首先查看该固件包的基本信息如下

（1）LZMA 压缩数据:

偏移量 0x0 - 这个段以 LZMA 压缩数据开始，其中 properties: 0x5d 指明了 LZMA 数据流的属性。字典大小为 33554432 字节，未压缩大小为 4840000 字节。

描述 - 从描述来看，这可能是固件的主要部分，常见于引导或主操作系统的映像。

（2）SquashFS 文件系统:

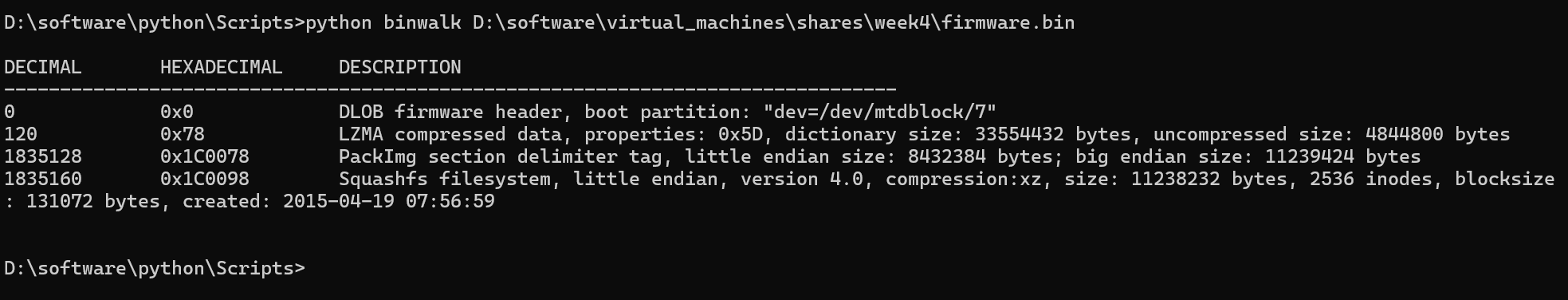
偏移量 0x1C000 - 这个段是一个 SquashFS 文件系统，该文件系统是为嵌入式系统设计的高度压缩的只读文件系统。

字典大小 131072 字节和其他参数如 block size: 131072 bytes, 2306 inodes 表示了文件系统的结构和大小。这通常用于存储应用程序和配置文件。

（3）时间戳:

文件系统的创建时间为 2015-09-17 16:56:59，这可能是固件最后一次更新或编译的时间。

基于以上信息，这个固件包含一个引导段（可能是操作系统或固件的一部分），后跟一个包含各种系统文件和应用程序的 SquashFS 文件系统。



接下来检测 ARM 架构

三个 ARM 指令集的函数序幕（function prologue），这通常是函数的开始部分。

（1）偏移量 0xB6AAE:

指示在该偏移处发现了 ARM 指令，具体是函数的开头（函数序幕）。这表明该部分可能是一个独立的函数或一段执行代码的起始。

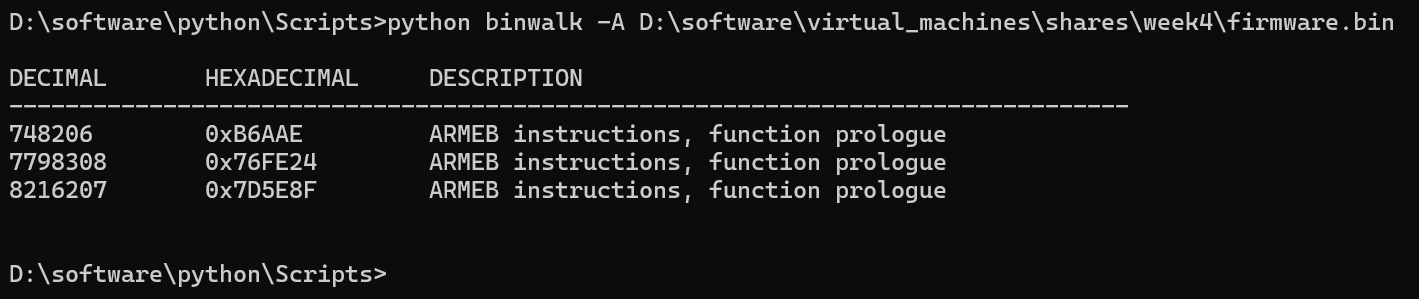
（2）偏移量 0x1F6E24:

同样，在这个地址也检测到了函数序幕，表明另一个可能的代码段或函数的起始。

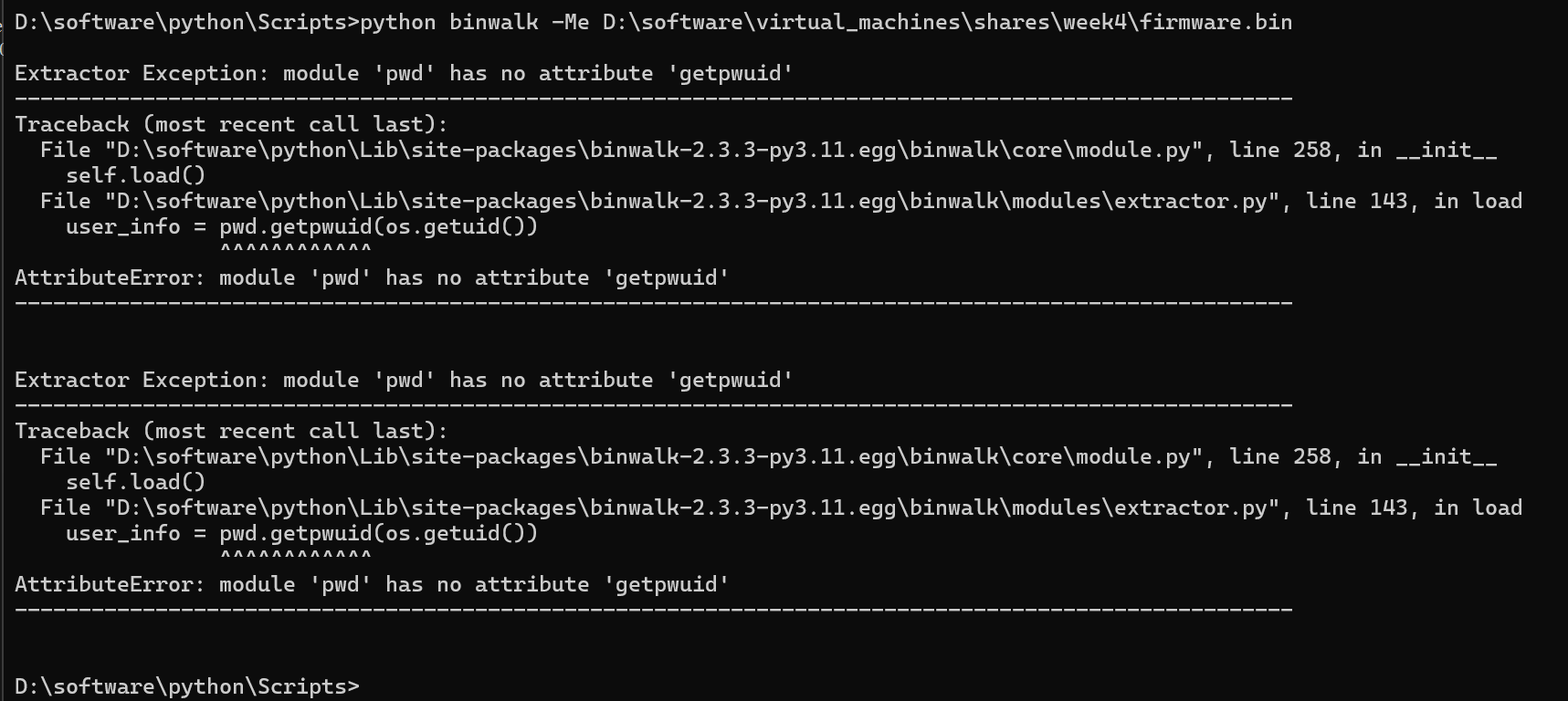
（3）偏移量 0x75DEF:

这是第三处函数序幕的位置，进一步确认了固件中包含多段可执行代码。

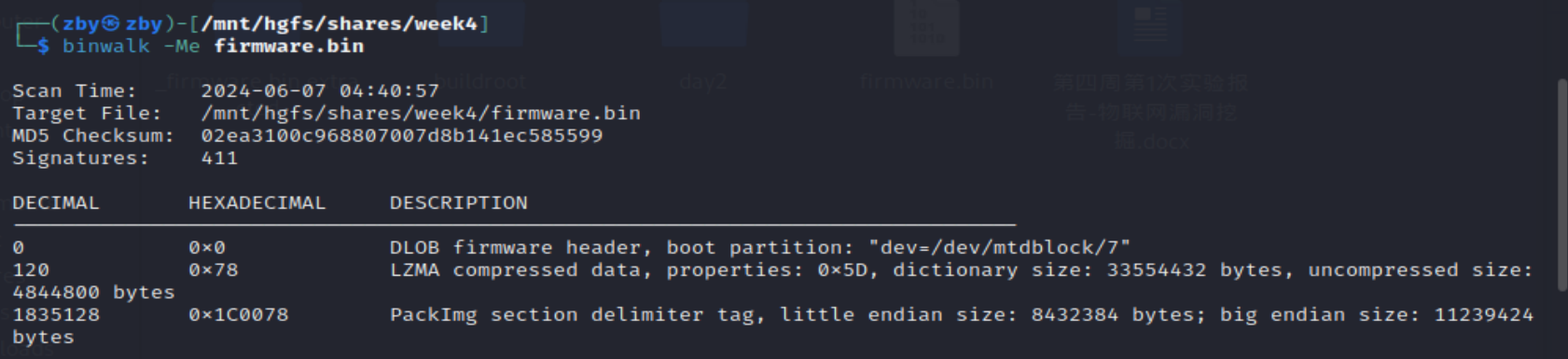
从这些信息可以看出，这个固件文件包含 ARM 处理器架构的可执行代码。这些代码可能是固件的主要逻辑部分，用于控制硬件或执行特定的操作任务。



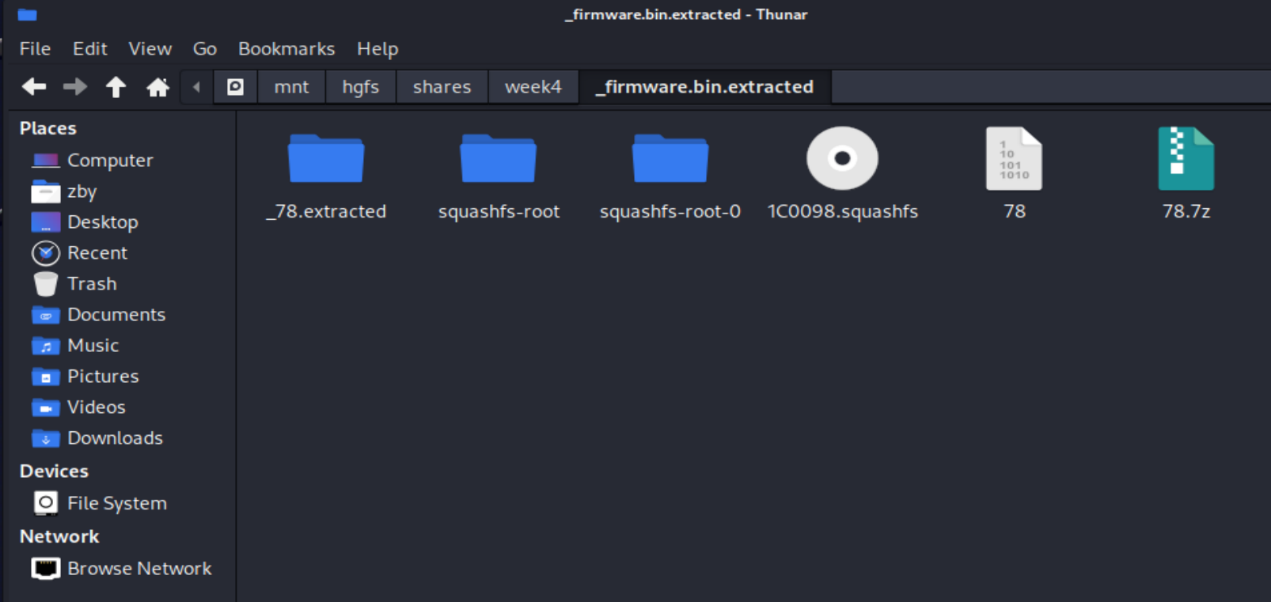
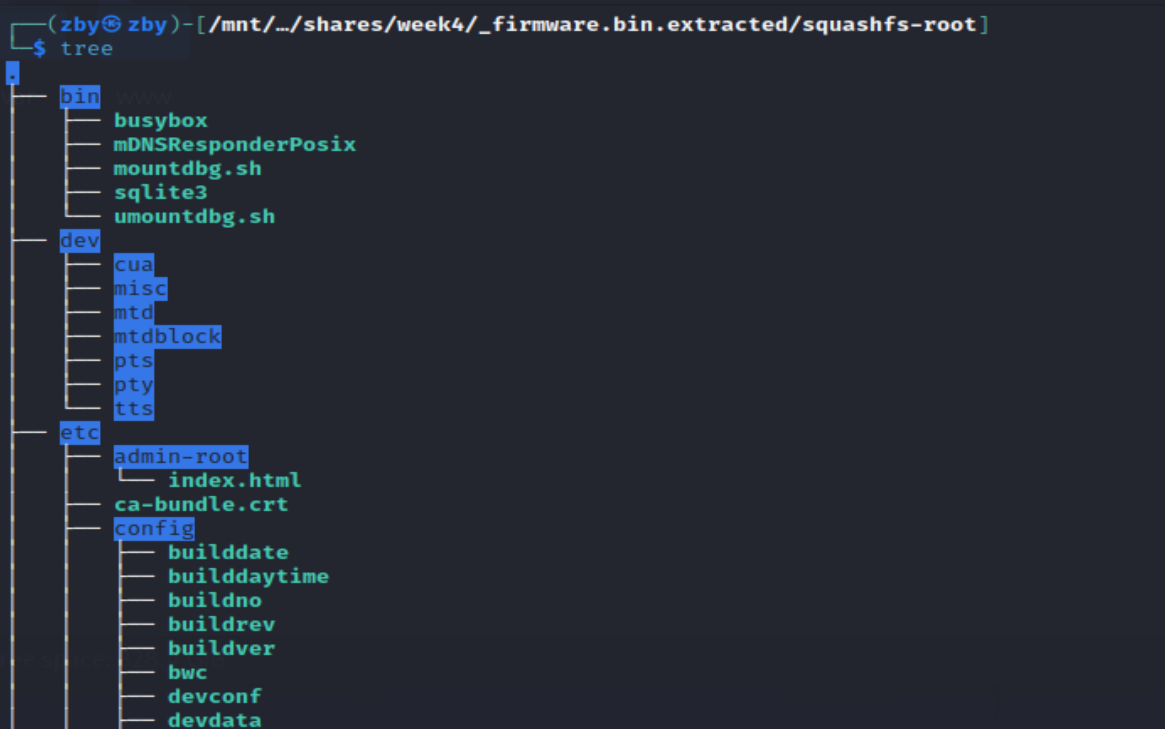
接下来根据magic签名的扫描结果对固件进行递归提取时出现报错，推测可能是windows系统的原因



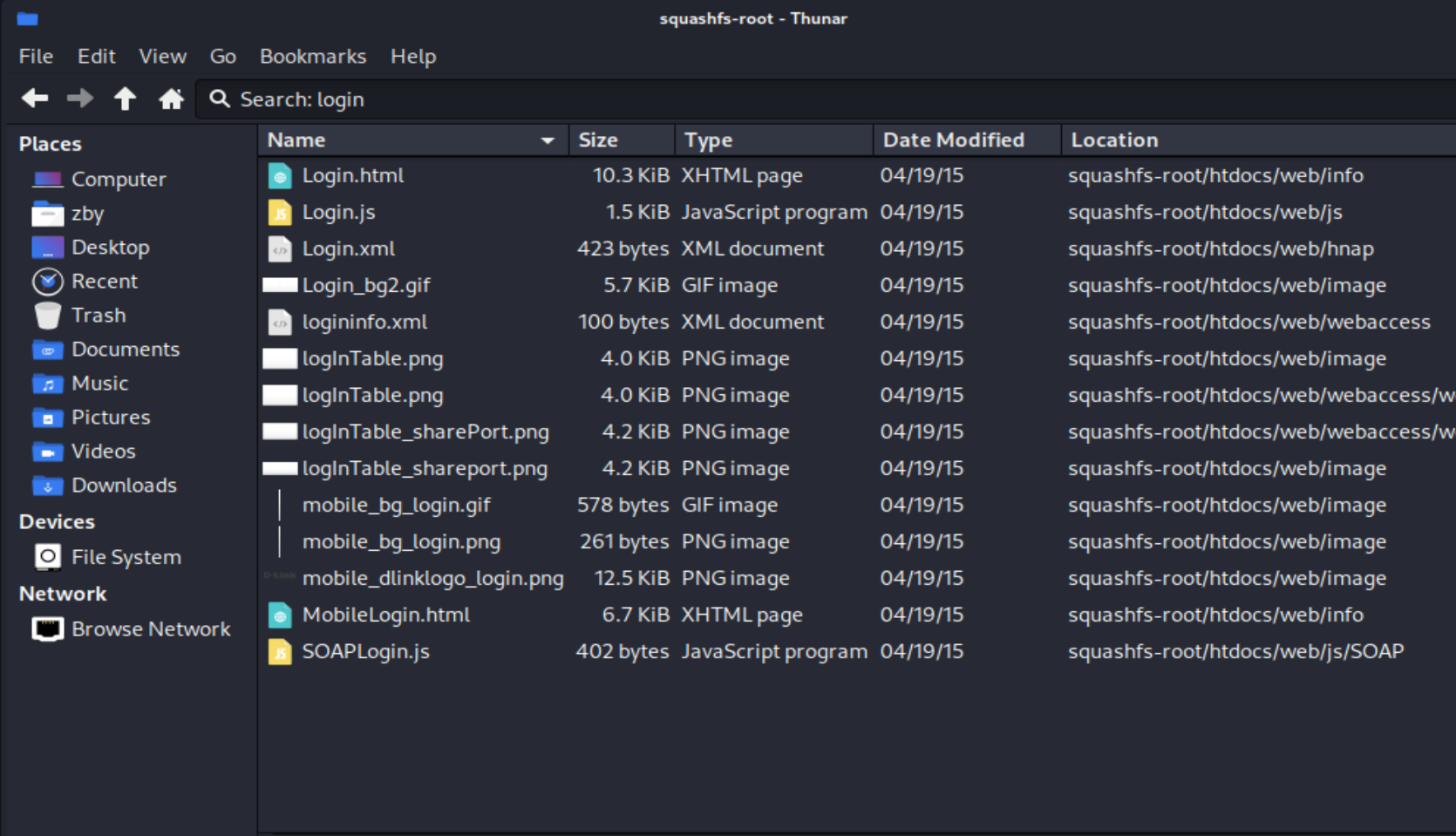
在kali虚拟机上重新执行该指令



可以成功获取到固件的根目录\_firmware.bin.extracted

进入到squashfs-root目录查看文件目录树结构如下所示  


在目录结构中查找login字段，找到logininfo.xml文件



将找到的文件打开后成功获取登陆密钥

