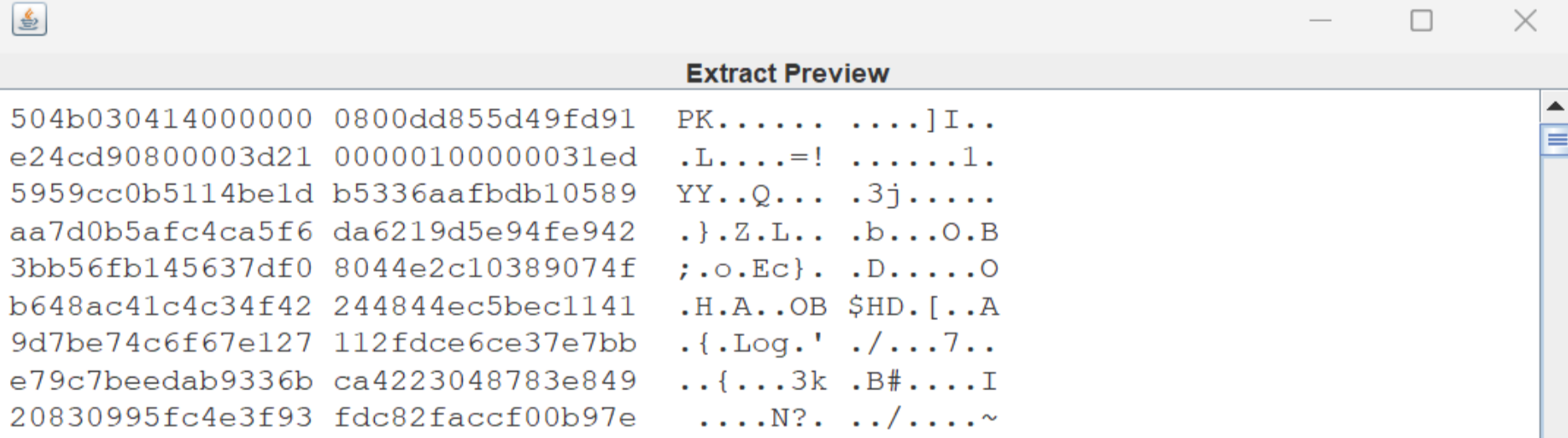
第二周周报

题目：

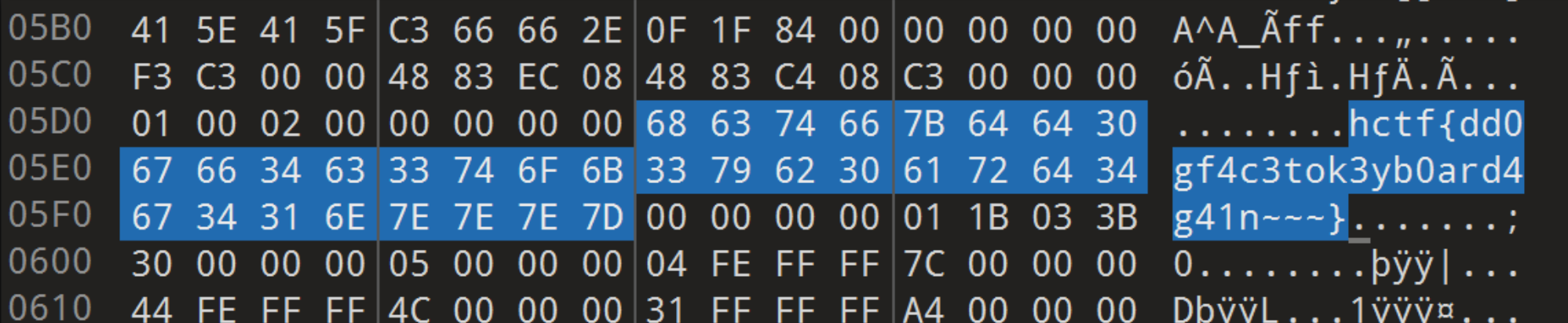
答案：flag{dd0gf4c3tok3yb0ard4g41n~}

解题过程：（难）

下载附件，得到一张.png图片

因为附件是一张图片，先放到StegSolve中，在Analyse（分析）选项卡，使用Data Extract（数据提取），可以看到有zip文件的标志。（通过）

由pk文件头可以看出隐写内容为zip文件，按save Bin键保存为zip文件。解压获得一个名为1的文件，可以通过添加.txt后缀或在010 Editor中查看文件。仔细找，找到flag。



题目：

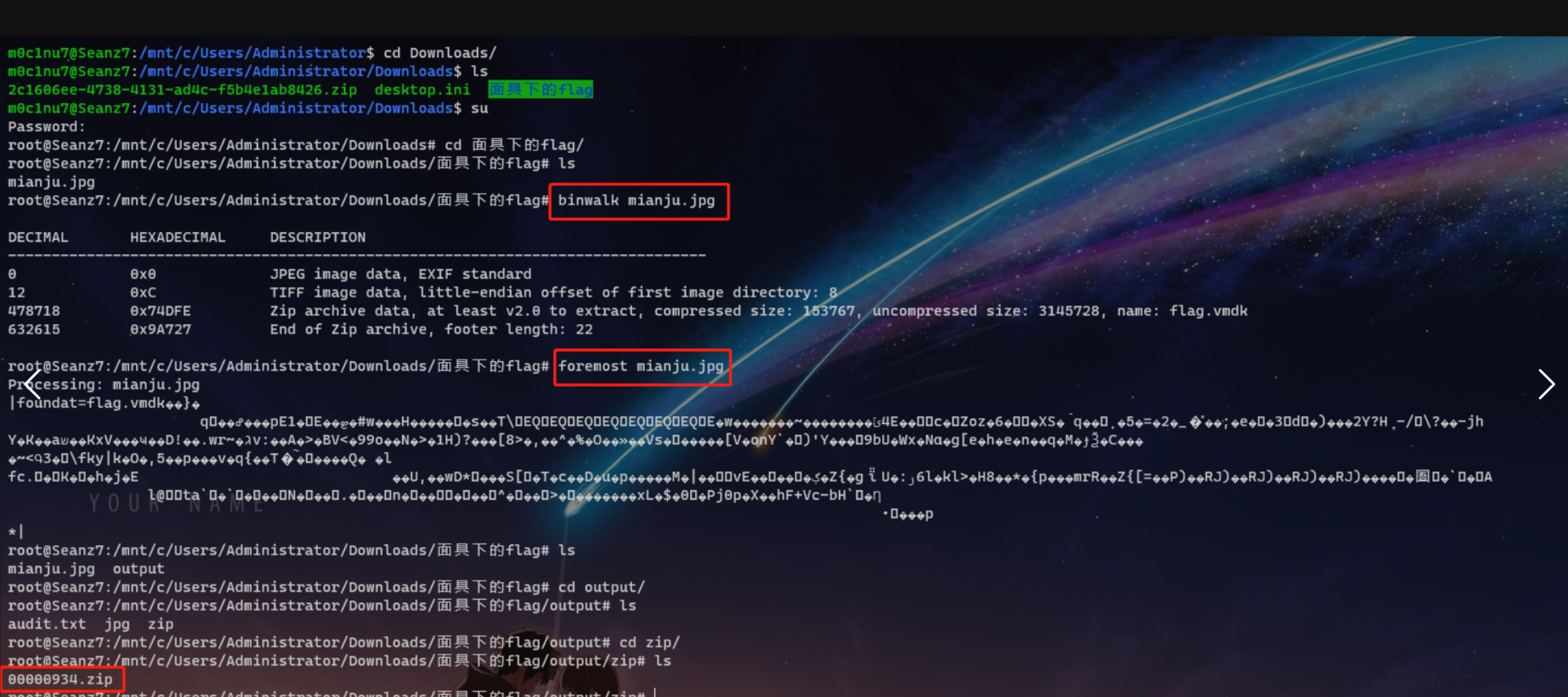
答案：flag{N7F5\_AD5\_i5\_funny!}

解题过程：（难）

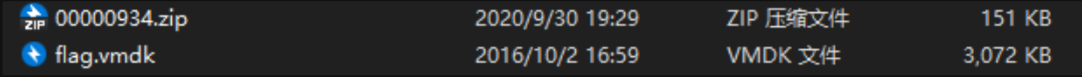
打开文件，是下图



用binwalk分析，发现有隐藏了zip，foremost分离得到一个压缩包



再进行zip伪加密，解压得到flag.vmdk



再可以用7z解压，得到flag

知识点：

Binwalk：Binwalk 是用于搜索给定二进制镜像文件以获取嵌入的文件和代码的工具。 具体来说，Binwalk是一个固件的分析工具，旨在协助研究人员对固件非分析，提取及逆向工程用处。简单易用，完全自动化脚本，并通过自定义签名，提取规则和插件模块，还重要一点的是可以轻松地扩展。

具体用法：binwalk【选项】文件名

参数介绍：

-B：不执行任何提取，只显示可能包含文件的偏移量。

-e：将所有提取文件保存到当前目录下的一个子目录中。

-M：尝试包含另一个已知格式（以逗号分隔的列表）。

-y：尝试所有提取操作/文件类型。

Foremost：Foremost 是一款常用于文件提取和数据恢复的工具

StegSolve：Stegsolve是一款图片隐写分析软件，支持常见的图片文件格式，可提取GIF文件中的帧。当两张jpg图片外观、大小、像素都基本相同时，可以考虑进行结合分析，即将两个文件的像素RGB值进行XOR、ADD、SUB等操作，看能否得到有用的信息。

功能介绍：

File Format:文件格式

Data Extract:数据提取

Steregram Solve:立体试图 左右控制偏移

Frame Browser:帧浏览器

Image Combiner:拼图 图片拼接