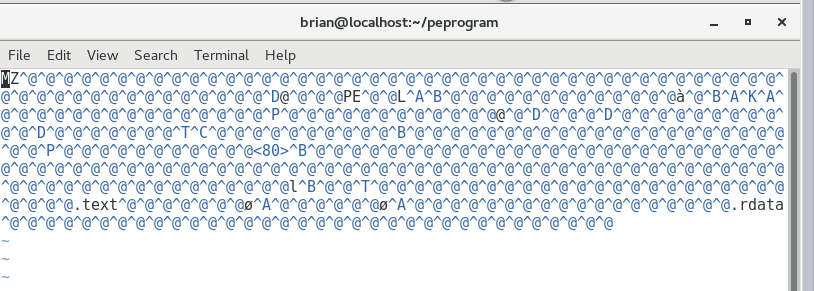
现在恢复PE头阶段：

设计思路

代码语言（Python）

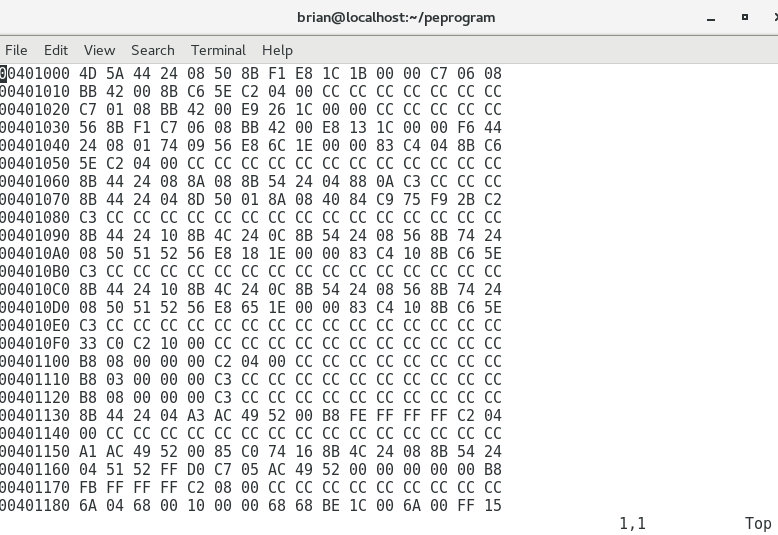
1. 自己用反编译软件写了一个拥有基本信息的PE Header（已由16进制转为ASCII），存在一个txt档案里



2. 写代码将数据集里每个恶意程序的.byte文件中已有的section将其转成ASCII（如上方的PE 头格式差不多）

补充信息：.byte文件里是包含virtual address，和每行以16进制形式表达的二进制代码、

（文件名：0A32eTdBKayjCWhZqDOQ.bytes）



问题：

1. 此文件是一个文本文件，所有的数据都是以ASCII来表示

我的想法：(未实现，在写代码转换的过程中遇到点问题，有些思路有些混乱)

1. 把它从ASCII转成真正以16进制表达二进制代码 {例如：“4D”变成 4D， 而不是4D变成34 （**即是说： 不是要文件里数据ASCII的16进制表达，而是要数据自己本身以16进制存在**）} (**这是我现在遇到的主要问题**)
2. 然后转成真正属于这个二进制代码的ASCII， 方便与步骤一的PE头进行拼接（Step 3）

3.完成以上将16进制表达的二进制代码转成ASCII之后，跟第一步的PE header 的ASCII拼接，再放进IDA pro进行反编译，输出EXE文件

相关代码存放位置： <https://github.com/brianchankobe/recoverPEheader.gi>t

\*\*\*以上思路有可能有问题，望能批评指出