CTF-数字取证合集

原创

why you learn hard? 于 2021-11-27 22:05:36 发布 2950 收藏 5
分类专栏： misc 文章标签： ctf 安全 web安全

本文链接：https://blog.csdn.net/hacker_zrq/article/details/121583888


misc 专栏收录该内容
16 篇文章 0 订阅
订阅专栏

本题来自moectf的easyForensics。

下面是题目链接：

https://masternoah.lanzoui.com/iFXVfsy5o3e

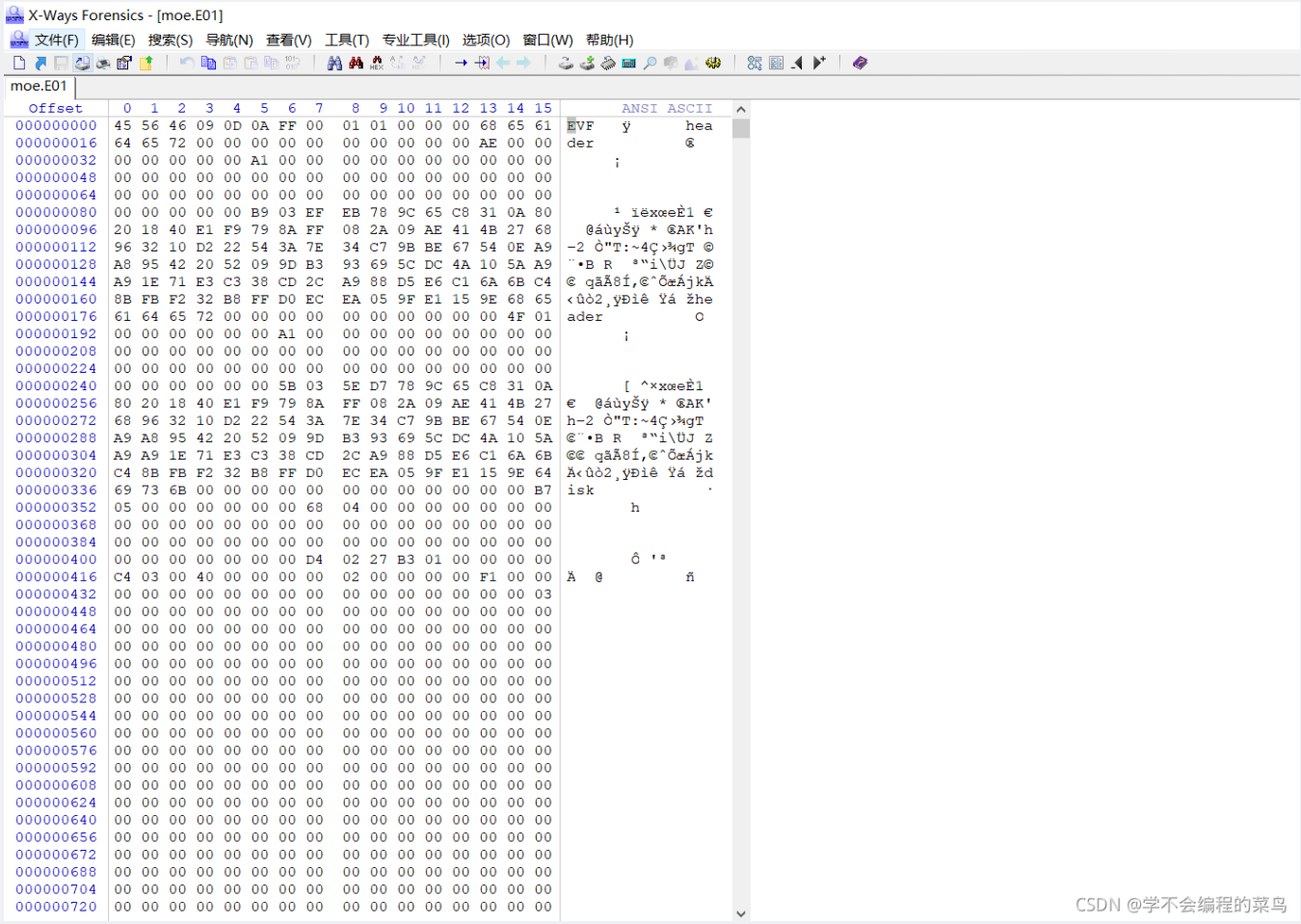
一、首先下载软件X-ways Forensics

我们可以了解一下e01文件的文件类型。参照下面这篇文章。一句话来讲就是e01就是一个计算机某一时刻全部操作的证据文件。

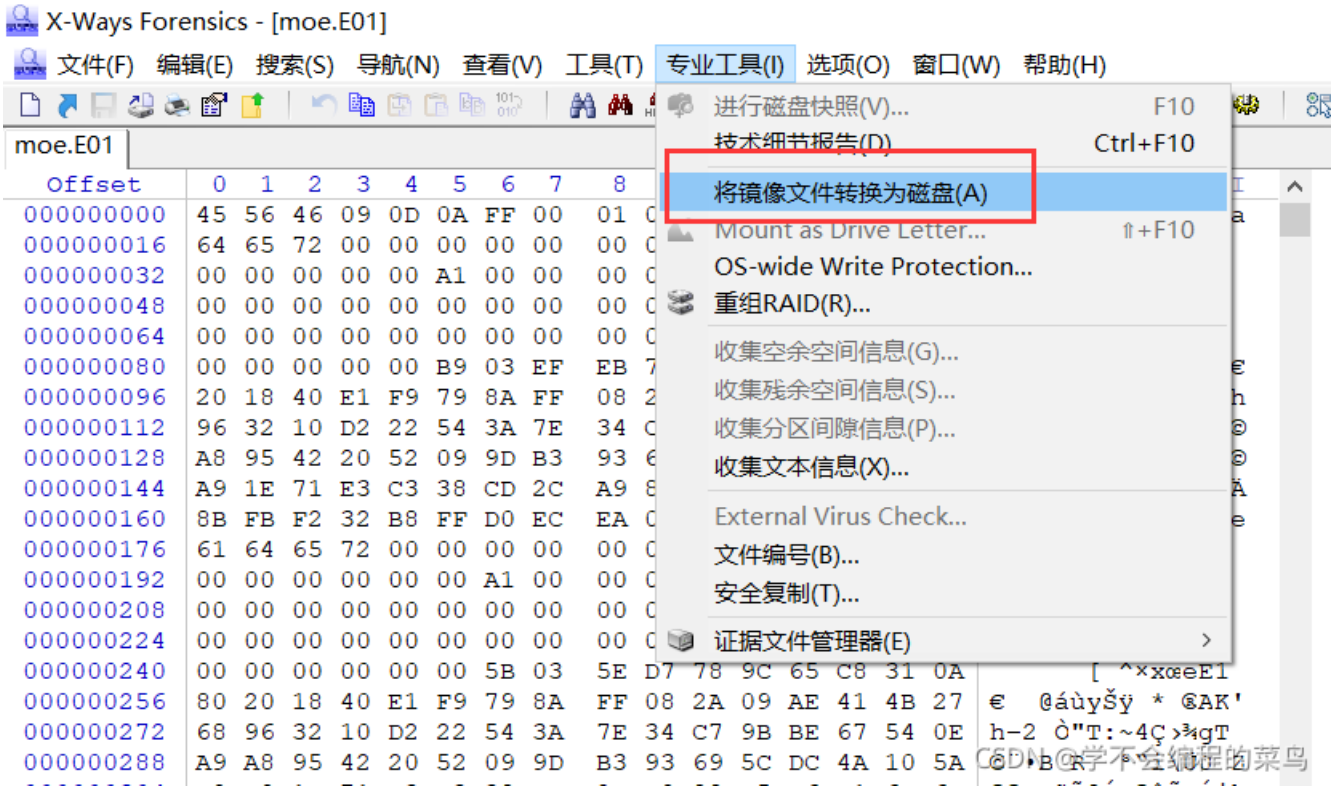
封装E01文件格式说明 — 磁盘映像取证 (forensicsware.com)

二、打开文件

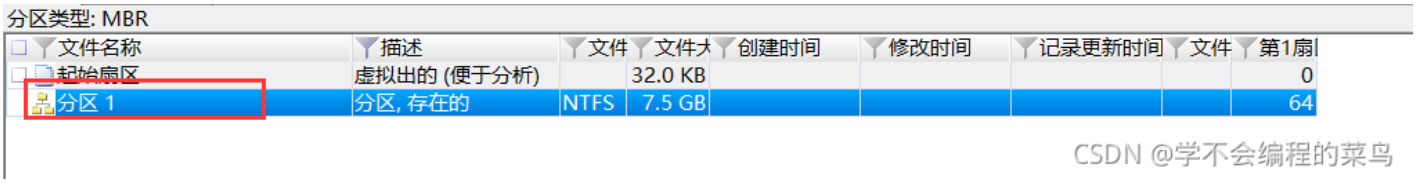
文件打开后是这个样子：

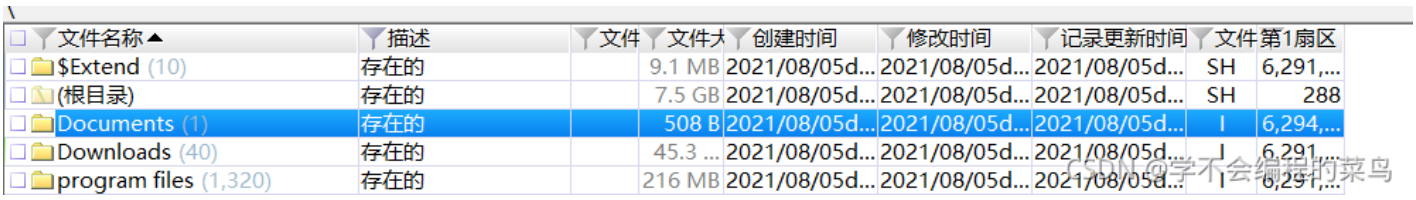


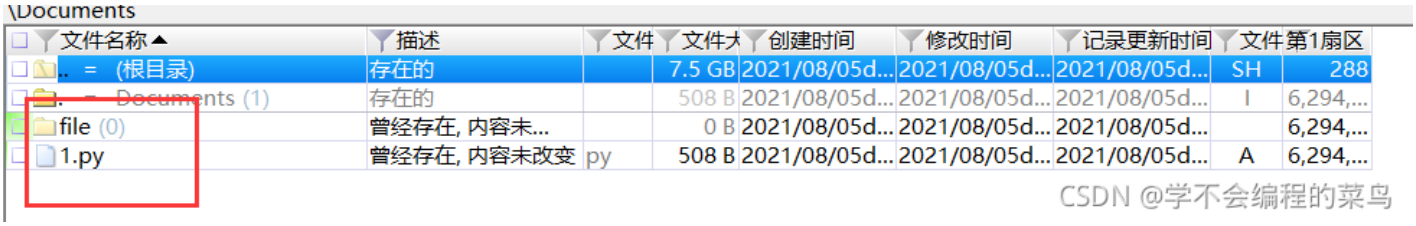
然后点击这个按钮，就可以看到解析好的证据：也就是我们保存的操作。



然后打开分区1，就可以看到嫌疑人一定时间段内的使用被取证电脑的工作状态。对这道题目来讲，Documents目录下就可以看到出题人删除的1.py文件。







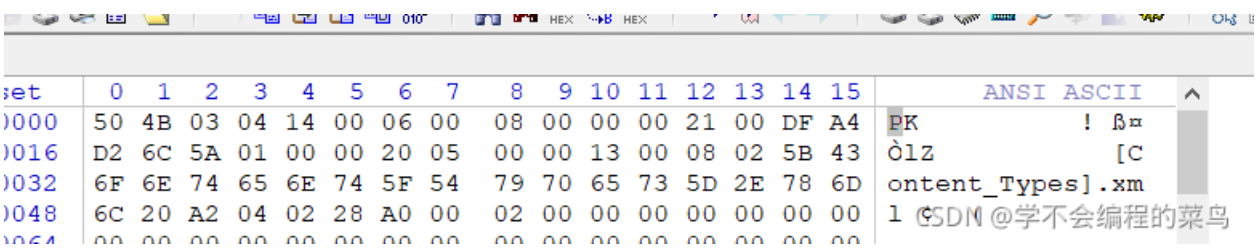
我们将该文件恢复到电脑上，然后就可以逆向工程。

```
from base64 import b64encode as be
import os
import re

with open("file.in", "rb") as fin:
    data = fin.read()

data = be(data).decode()
data = data.replace("/", "_")
data = re.findall(r'.{40}', data)

base = os.getcwd() + "\\file\\"
count = 1
for item in data:
    folder = str(count) + " " + item
    if count < 10:
        path = base + "00" + folder
    elif count <100:
        path = base + "0" + folder
    else:
        path = base + folder
    os.mkdir(path)
    count += 1
```

EXP如下：

```
import base64
import os

data = ""

for root,dirs,files in os.walk("./file/"):
    for dir in dirs:
        data += dir.split()[1]

data = data.replace("_", "/")

with open("file", "wb") as fout:
    fout.write(base64.b64decode(data))

#file_path：就是你想要的path(路径)
#os.walk(path)：就是在path路径下去遍历文件夹，就像是a = [b,c,d[]],walk获取到是就是b，c，d的名称
#root：就是获取当前目录路径，就是a
#dirs：就是获取当前路径下所有子目录，就是d
#files：  就是获取当前路径下所有非目录子文件，就是b，c
```

三、后面的操作就是把目录的名字提取出来，按照逆向工程解码。得到一个文件，但不知道是什么，这时候你就把他拖到winhex里面看看。



> docx_百度百科 (baidu.com)
>
> 是一个docx文件，这个可以查看百度百科。docx实际上就是一个压缩包，由许多xml文件组成。改后缀。

打开文档即可发现flag。

后续还有很多类型的取证，参见下面这个师傅的博客。

> (18条消息) CTF题记——取证小集合_m0re's blog-CSDN博客_ctf 取证