

初探ADS流文件隐写术

原创

知远同学 于 2020-07-11 15:54:13 发布 457 收藏

分类专栏: [电子数据取证](#) 文章标签: [电子取证办案](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_47401101/article/details/107286053

版权



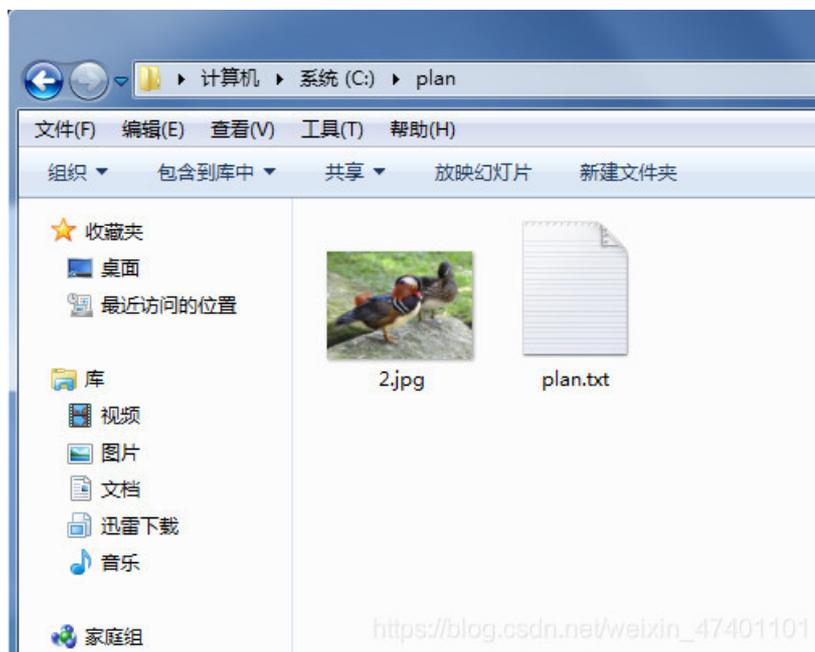
[电子数据取证 专栏收录该内容](#)

0 篇文章 0 订阅

订阅专栏

文件隐写技术分为很多种, 今天笔者给大家介绍一种依靠ADS流文件进行文件隐藏的技术, 原理在这里就不详细介绍了, 比较枯燥的内容就略过吧, 我们看看是如何实现的。

在电脑C盘, 文件名为“plan”的文件夹内有两个文件, 一个是文件名为“2.jpg”的图片文件, 一个是文件名为“plan.txt”的文本文件,



现在我们要把这个图片文件隐藏到文本文件中去。

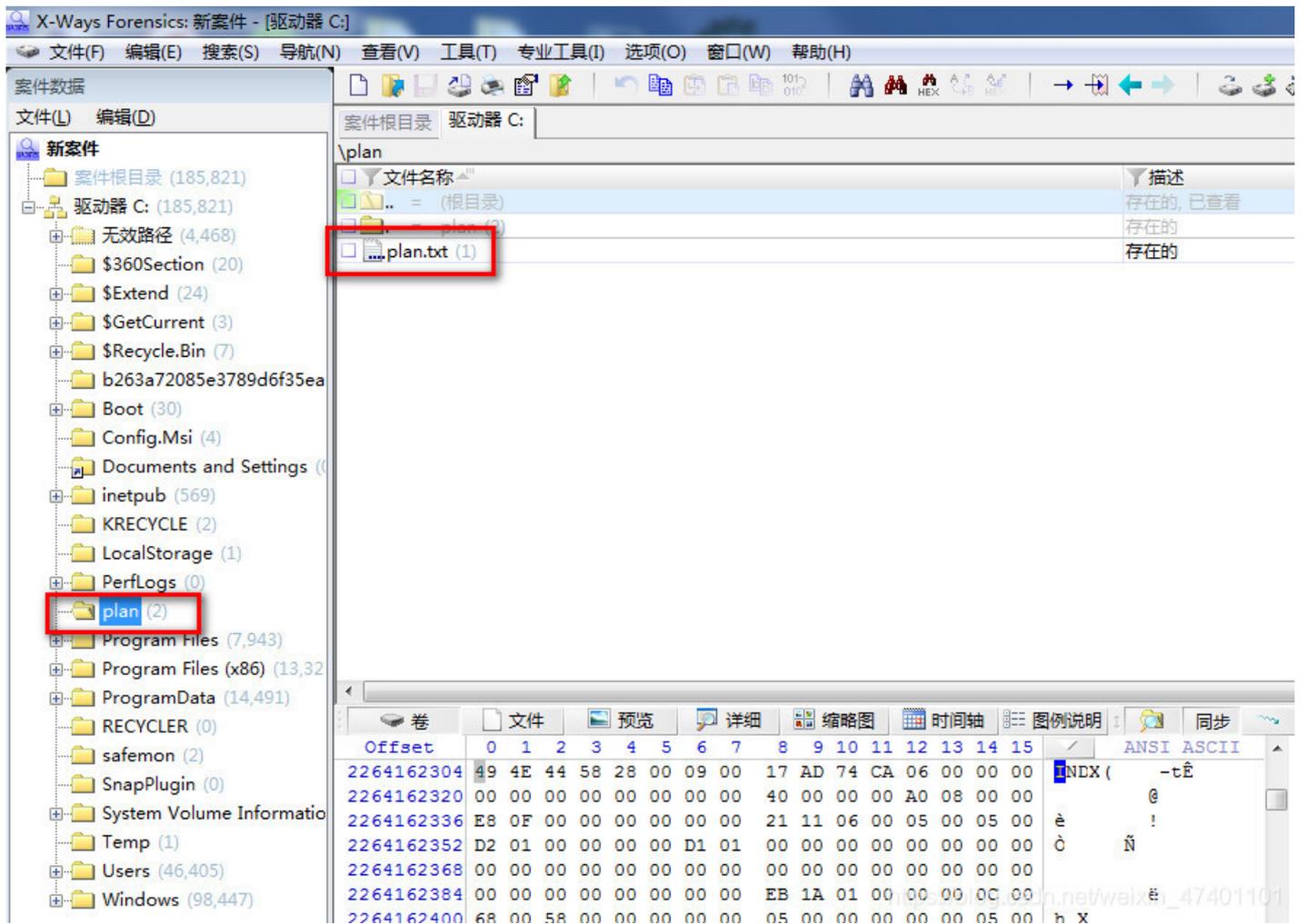
打开CMD, 通过命令将“2.JPG”隐藏到“plan.txt”文本文件中去:

关键命令为: `type 2.jpg > plan.txt`

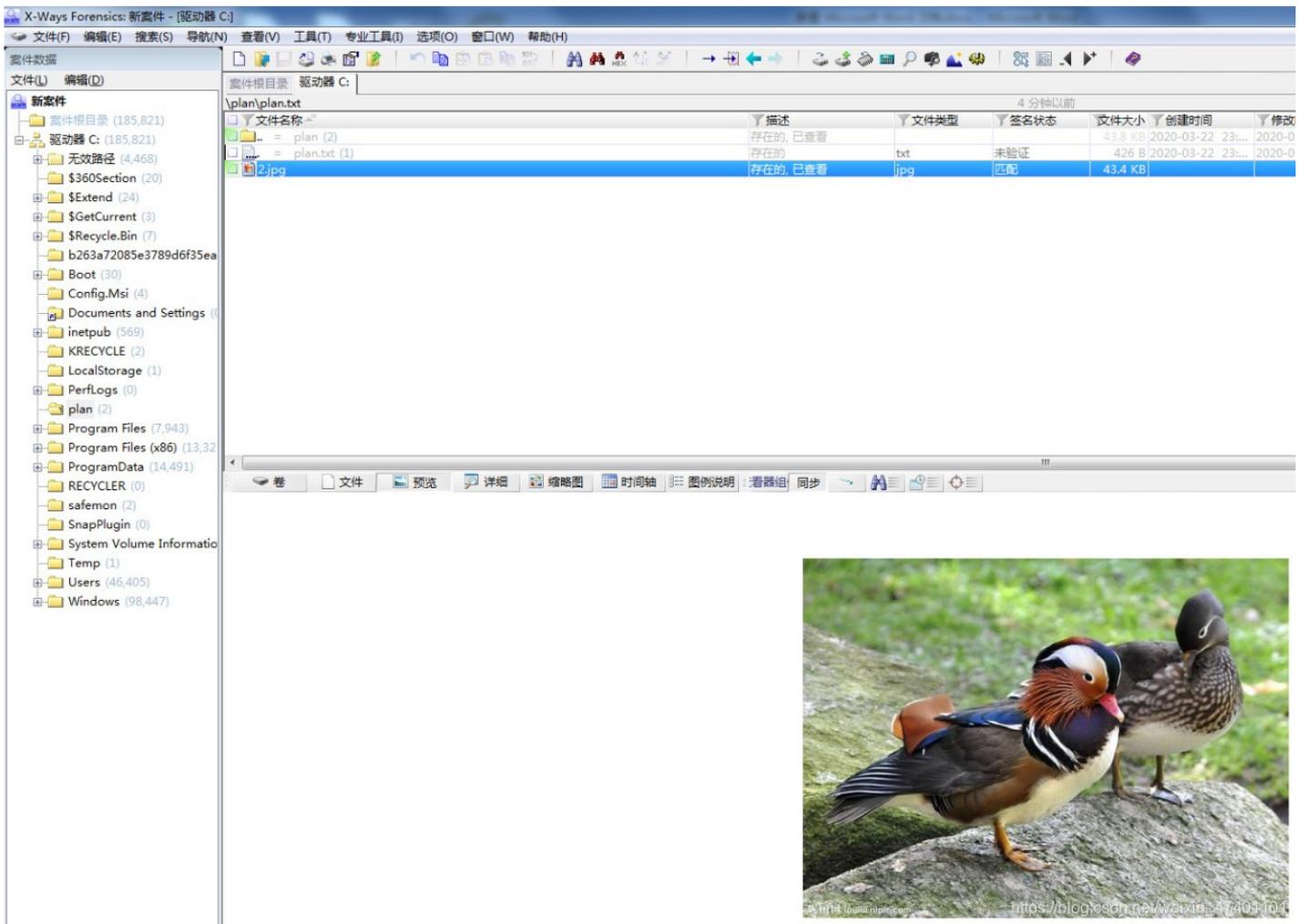
```
管理员: C:\Windows\system32\cmd.exe
C:\>\cd plan 1.进入C盘目录下的plan文件夹
C:\plan>dir
驱动器 C 中的卷是 系统
卷的序列号是 B019-EC3F 2.查看plan文件夹的目录
C:\plan 的目录
2020-03-22 23:25 <DIR> .
2020-03-22 23:25 <DIR> ..
2020-03-22 23:23          44,419 2.jpg
2020-03-22 23:21          426 plan.txt
                2 个文件          44,845 字节
                2 个目录 15,699,677,184 可用字节
C:\plan>type 2.jpg >plan.txt:2.jpg 3.通过命令将2.JPG图片文件隐藏到plan.txt
文本文件中
C:\plan>del 2.jpg
C:\plan>dir
驱动器 C 中的卷是 系统
卷的序列号是 B019-EC3F 4.删除2.JPG图片文件
C:\plan 的目录
2020-03-22 23:35 <DIR> .
2020-03-22 23:35 <DIR> ..
2020-03-22 23:34          426 plan.txt
                1 个文件          426 字节
                2 个目录 15,699,673,088 可用字节
C:\plan>
```

通过这样的操作，图片文件就隐藏到文本文档中去了，那么如何才能找到这个图片文件呢？

借助X-WAYS（一款国际电子数据取证软件），将电脑的C盘加载到软件中，选中“plan”文件夹后右侧可以看到“plan.txt”文本文件，在这个文件图标下方有三个点，表示这个文件有下级。



在“plan.txt”文件上右键浏览，就可以看到“2.jpg”文件了。



在很多时候，犯罪嫌疑人在发送邮件的时候，会将关键内容隐藏在其他文件内，也会把关键信息隐藏在其他文件内保存，侦查人员了解一些信息隐写技术，对于扩展侦查思路也是有帮助的，当嫌疑人的电脑中实在找不到需要的信息的时候，也要请分析人员对电脑中的ADS流文件进行分析一下了。



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)