《电子证据分析》课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 实验名称 |  | 姓名 |  |
| 班级 |  | 学号 |  |
| 实验日期 |  | 指导老师 |  |
| 实验环境  (实验软硬件要求) | win10、cmd | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  *了解并且掌握win10的多数据流文件的相关原理，并且能够利用多数据流进行文件的隐藏和恢复* | | |

|  |  |
| --- | --- |
| 实验内容 | 已知在D盘中存在文件1.jpg和noname.docx两个文件，要想创建一个内容与1.jpg一样但是不被人看得到的文件，可以使用如下指令（宿主文件不一定需要docx，也可以是别的文件）  clipboard.png  然后可以发现里面并没有test.jpg，但是在使用如下指令时，可以看到原本的1.jpg的内容  clipboard.png  noname.docx:test.jpg的内容如下：  clipboard.png  而1.jpg则是这样的：  clipboard.png  要想找出这种藏起来的文件，可以使用dir命令  clipboard.png  可以看出修改时间变成了今天  另外使用dir /?可以查看所有的dir参数  clipboard.png  这里在对应的文件夹里使用dir /R  clipboard.png  这样就能看到了隐藏起来的文件了（这招只能在win10上实现）    另外还有别的办法，因为NTFS才支持多数据流，如果将这个文件复制到其他文件系统里面，就会无法隐藏，如果复制在FAT32中会复制失败，而且在粘贴的过程中会直接报错，提示粘贴过程中有文件是多数据流，如果强行粘贴会丢失。（亲测在linux的ext中没用可以直接复制成功）  复制到FAT32的U盘中：（使用的同学的截图，因为身边实在没有FAT32的设备了……）  f27ddf4c8f37d7abe8aead38dbe10f1.jpg  复制到kali成功了，没有任何提示：  clipboard.png |
| 实验总结 | （对本次实验涉及到的知识点的重难点归纳、实验心得、思考与建议） |
| 评分 |  |