《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) | Winehx、win10、windowsxp、U盘、记事本 | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  掌握windows回收站的原理和机制  学会将已经在windows回收站中被删除的文件或文件夹进行恢复，并且获取其原本的文件信息 | | |

|  |  |
| --- | --- |
| 实验内容 | 1. 在windowsXP环境中进行回收站已删除文件还原。   首先在任意地方创建一个文件，任意名命名，并且任意在文件内输入内容。内容和位置如下：      然后将这个文件送进回收站即可。如下图。    接下来，因为是删除的文件，所以将文件删除。    之后打开winhex，然后F9打开当时删除的文件对应所在的分区（实验的环境虚拟机只有一个分区）    进入到RECYCLER目录下去。看到如下内容，继续进入文件夹中。  施阳溢  我是施阳溢    然后就能看到被删除的文件了。    根据文件的创建时间、删除时间、访问时间可以直接确定，文件就是Dc2.txt  这里的第一个D表示被删除的”Deleted”，后面的c表示所属的分区，后面的数字就是流水号。  将其恢复到U盘中。如下：      并且在INF02中找到了对应的文件名。    本来因为这个文件名是中文没办法看出来，但是因为使用的是Unicode编码，所以我找了找教程，发现winhex可以直接看Unicode编码，所以才会和上面一样。     1. 在windows10环境中进行回收站已删除文件还原。   因为宿主机之前做过太多次和windows账户有关的实验，所以有非常多的账户，回收站很多……还是采用虚拟机的办法。  一样的，打开win10之后在桌面创建了一个txt文件  内容如下：    然后将其放入回收站。    随后删除。  打开winhex。然后使用F9，对C盘进行读取。（桌面默认都在C盘）    进入$Recycle.Bin文件夹中（“$”符号表示这个文件夹是隐藏的）    可以看到有两个文件夹，说明这个win10有两个账户。我删除的时候账户是1001    这里是win10和XP不一样的地方了。这里有两个文件。  前面的I表示是被删除的文件的信息，而后面的R表示的是被删除的文件的内容。    再将文件还原到U盘中：      可以看到，还原成功了。 |
| 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）  这次实验在C盘里面很难成功，不知道为什么C盘将文件删除之后很快文件就会消失，D盘就不会这么快速……靠手速在删除之后立马对C盘扫描也是可以的。 |
| 评分 |  |