《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（实验的环境虚拟机原本只有一个分区，后来我手动加了一个分区）      进入到RECYCLER目录下去。看到如下内容，继续进入文件夹中。    然后就能看到被删除的文件了。    可以看到，被删除的文件就是De2.txt一般来说不会只有一个文件被删除这么简单（也可能干脆一个都没有），这个时候需要根据文件的创建时间、删除时间、访问时间来确定。  另外，这里的第一个D表示被删除的”Deleted”，后面的e表示所属的分区就是e盘，后面的数字就是流水号。  将其恢复到U盘中。如下：      原本文件所属的路径和对应的文件名则需要到INF02中去查看了。    另外，原本因为这个文件名是中文没办法看出来，它使用的是Unicode编码，所以只需要将原本的ASCII改成UTF-16 LE就可以了。     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E盘里面创建了一个txt文件  内容如下：    然后将其放入回收站并且删除。    打开winhex。然后使用F9，对E盘进行读取。（要是只有一个分区的话就会很痛苦了……C盘回收站里的东西消失的非常快，需要拼手速）    进入$Recycle.Bin文件夹中（“$”符号表示这个文件夹是隐藏的）    进入到这个对应的文件夹里去。可以看到有以下内容：    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：      同样的，文件的原本名字和路径如下：    实验完成 |
| 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，另外的盘就不会这么快速……当然，靠手速在删除之后立马对C盘扫描也是可以的（基本上需要马上就去进行磁盘扫描），我认为这样的操作在现实中不具有可操作性…… |
| 评分 |  |