《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) | Windows、office、winhex、U盘 | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  了解数据恢复的原理  了解文件的相关知识  了解windows系统使用的磁盘管理机制  掌握数据恢复的操作方法 | | |

|  |  |
| --- | --- |
| 实验内容 | 实验1：随意创建一个小文件，并在将其删除后，将其再重新恢复。    首先创建一个doc文档，名称为1.doc，内容为“我是施阳溢”    随后，将其删除。如下图。      随后打开工具——winhex。对优盘进行扫描。  在扫描完成之后发现了一个疑似是我删除的同名文件（根据实验时文档修改的时间判断出是第一个）。如下图    随后右键将其复制到非U盘的分区中，避免把数据重新覆盖掉。Winhex提示如下。    随后回到桌面，的确找到了我们需要恢复的文件——1.doc  进行验证，得到确实是原来被删除的那个文件。    实验2：在文件登记项被覆盖的情况下，对被删除的doc文件的内容进行获取。  这个实验是假定在文件登记项被破坏了的情况下进行的，因此不能使用之前的办法。并且由于使用的办法是特征搜索，所以这次选择使用文字比较多一点的小文件来进行实验。  我使用了U盘中的2.doc，里面的内容就是我们学校的学生手册的部分内容。      随后将其删除掉。并且确认优盘里面已经没有了文件。    然后，使用winhex对优盘进行扫描。同时我们也利用我们知道2.doc里面的文本内容有“教室要保持整洁,课桌要整理干净并有序摆放,同时要关好门窗,关闭电源,检查教室安全情况。各区队应安排好教室安全卫生值日”这么一段话，所以另外在一个分区上新建一个doc文档，并且内容就是这个。    使用winhex打开这个我们新创建的文档，找到文本内容对应的Unicode编码，内容如下：    接下来复制这段十六进制值，再在优盘里面搜索。    但是出现了这个。    怀疑是自己选的这段话的十六进制值太大了，所以就只好弄少一点，果然是这样的问题，解决了这个问题之后就开始扫描    扫描结束后，自动跳转到了对应的区域。  可以看到这一段全都是十六进制数值，我们往上翻看，找到文件内容的开头。    很明显，就是0x0BB43BA00这里就是文件内容的开头了。  然后尽可能地往后翻，然后选定复制十六进制值，选择多了没有关系，最多就是后面有乱码。新建一个文本，内容随便加上点并且另存为Unicode编码(UTF-16 LE)格式。    然后用winhex打开这个文件，然后在FFFE后面复制上之前的十六进制，再保存。重新打开这个文件。    里面的内容就是我们之前删除的文件的内容了，但是这样做也会有一些缺点，就是没有办法确定哪里是结尾，很多时候会选少了或者选多了。这个时候尽可能多选一些，多出来的也不过是乱码，但是少了的话就会缺少内容。 |
| 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）  本次的实验操作难度不是很高，但是对于winhex的熟悉程度要求比之前的实验高一些。因为不是很方便可以模拟出文件登机项被覆盖的情况，向U盘里面写入尽可能多的东西才有可能会覆盖掉它，但是我没能成功尝试出来。 |
| 评分 |  |