《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、Process Monitor、WeChat | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  *能够了解使用Process Monitor* | | |

|  |  |
| --- | --- |
| 实验内容 | 打开Process Monitor，使用过滤选项添加对微信以及写入文件操作的监视    打开微信，并且随意发送一张照片    在这时，监控的Process Monitor窗口内出现了微信大量对dat文件的写入操作，在根据我发送时间和显示的时间的比较，以及对于对应的目录的基本的猜测，我认为下面的这个dat文件就应该是微信的图片了。    因为之前的实验已经知道了微信会将图片与一个密钥异或之后保存为dat文件，所以还需要使用异或对文件进行还原。  使用上一次的实验的小程序将这个图片解开查看，判断自己的结论对不对。  解开以后就是这个，没有错了    同时在进行了多次的重复的实验后，我确定了微信就是将图片文件异或之后保存在了以下的目录里面。另外这些照片是按照了月份来分类到各个目录下面的  C:\Users\ROOT\Documents\WeChat Files\wxid\_fspsrj89m3xr11\FileStorage\Image    另外，对于微信隐藏的消息我也做了一点点的探究。但是因为能力问题没有办法进行验证操作……  下面就说明一下我的推测过程。  同样的，也是在Process Monitor内添加对微信这个进程的监视、同时添加上对文件写入操作的监视。如下图：    在点击确定之后，将监视框内现在的所有跳出的内容全部清空（直接ctrl+x或者点击选项的这个图标）等到暂时不会再有任何的无关消息出现之后。如下图：    直接在已经后台开启了的微信内输入一些文字，并且发送。  然后我就得到了下面的实验结果，我发现就在发送文字的一瞬间，下面的监视框里面就跳出来了许多的文件写入操作。    都是对C:\Users\ROOT\Documents\WeChat Files\wxid\_fspsrj89m3xr11\FileStorage\Msg 目录下的文件的操作，因为我发现对文件的修改操作都是对.db-wal文件动手的（最前面的那几个xlog是我因为写报告，clear以后又过了一点时间，又有了……）  我以为是信息就是在这个文件里面的。于是我直接用16进制文件，但是发现里面什么都没有（如下图）    事实上，我发现所有的db-wal文件都是0KB大小的  在网上进行查找后，了解到了这些db-wal文件都是临时文件，这是负责临时的写入的文件，找到的结果如下图：    参考网址：<https://blog.csdn.net/qq_35417527/article/details/113940408#:~:text=.db-wal%E6%96%87%E4%BB%B6wal%E6%84%8F%E6%80%9D%E6%98%AFwrite-ahead,log%EF%BC%8C%E9%A1%BE%E5%90%8D%E6%80%9D%E4%B9%89%E5%B0%B1%E6%98%AF%E4%BF%9D%E5%AD%98%E7%9A%84%E4%B8%80%E4%B8%AA%E6%97%A5%E5%BF%97%EF%BC%8C%E5%AF%B9%E4%BA%8E%E6%8F%90%E4%BA%A4%2F%E5%9B%9E%E6%BB%9A%E7%9B%AE%E7%9A%84%E5%BE%88%E6%9C%89%E7%94%A8%E3%80%82%20sqlite3.7%E4%B9%8B%E5%90%8E%E5%BC%80%E5%A7%8B%E6%8F%90%E4%BE%9B%E8%BF%99%E4%B8%AA%E5%8A%9F%E8%83%BD%EF%BC%8C%E5%BD%93%E4%B8%80%E4%B8%AA%E6%95%B0%E6%8D%AE%E5%BA%93%E9%87%87%E7%94%A8WAL%E6%A8%A1%E5%BC%8F%EF%BC%8C%E6%89%80%E6%9C%89%E8%BF%9E%E6%8E%A5%E6%95%B0%E6%8D%AE%E7%9A%84%E6%93%8D%E4%BD%9C%E9%83%BD%E5%BF%85%E9%A1%BB%E4%BD%BF%E7%94%A8WAL%EF%BC%8C%E7%84%B6%E5%90%8E%E5%9C%A8%E5%9C%A8%E6%95%B0%E6%8D%AE%E5%BA%93%E6%96%87%E4%BB%B6%E5%A4%B9%E4%B8%8B%E7%94%9F%E6%88%90%E4%B8%80%E4%B8%AA%E5%90%8E%E7%BC%80%E4%B8%BA.db-wal%E7%9A%84%E6%96%87%E4%BB%B6%E4%BF%9D%E5%AD%98%E6%93%8D%E4%BD%9C%E6%97%A5%E5%BF%97%E3%80%82>  在查看完之后，我大致明白了，文件的数据应该就是存放在了下面的这个文件里面：    但是因为是db文件，我上网查找的时候没有发现有很好的办法可以直接打开读取显示内容的……    这个软件没办法用……打不开db文件。  所以实验到这里就只好中止了。没办法敲定猜想了。只能猜测如此。 |
| 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）  主要本次实验主要让我们了解了Process Monitor的相关操作，并且老师也在上课的时候向我们展示了如何在虚拟机环境下使用该软件进行对病毒程序的跟踪，如何查看程序对于文件、注册表的修改。  心得：这个款开发工具的功能很强大，可以监控许多的进程的操作，并且还可以查看进程树。  思考：这款开发工具的确很强，可以监控到自己的电脑上的进程的所有操作，但是如果遇到有恶意进程将除了自己之外的进程都直接杀死，那这种工具是否还能有效果呢？  问题：关于后面的寻找微信信息存储的文件，我大致猜测是放在C:\Users\ROOT\Documents\WeChat Files\wxid\_fspsrj89m3xr11\Msg\Multi 里面的一个db文件里面的，但是没有办法验证，网上的办法也没有用。 |
| 评分 |  |