2.4 磁盘快照

为了实现数据的全面和自动化处理，提升工作效率，降低取证分析人员的工作量，X-Ways提供了证据预处理功能，称作磁盘快照。

本节重点学习掌握磁盘快照的基本功能，包括：文件恢复、文件签名恢复、哈希校验、复合型文件提取、电子邮件内容提取等。这是后续灵活进行数据恢复、搜索、签名比对的重要基础。

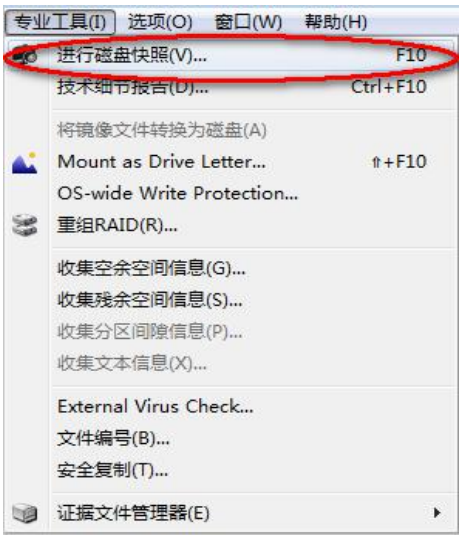

图 2-4-1 调用磁盘快照

更新快照：重新进行磁盘快照。会将之前所有的解析结果全部清除。对大容量硬盘的所有数据进行磁盘快照经常需要几个小时的解析时间，一定要慎重选择“更新快照”，否则有需要重新快照几个小时。

在选定的证据中搜索：选择进行指定操作的证据项。例如在一个分区中，还是在九个分区中，或是在三个硬盘中进行指定的快照操作。

应用于所有文件和**应用于所有标记的文件：**如果我们只想针对所选的一类文件操作，可以将这些数据进行标记，然后在标记的这几个文件中进行操作。例如，可以提取所有“PPT”中的图片。则先标记所有的PPT再进行操作。

图 2-4-2 磁盘快照选项

实验 2-22:依据文件签名恢复 DOC 文件

本实验配合案例文件：C:\CDF\2-取证基础\2.1-CCFC.e01。

场景：查找所有位置存在的 doc 类型文档，恢复出来的 Doc 格式文件数量。

1.进行磁盘快照，选择快照选项-基于文件签名进行恢复。

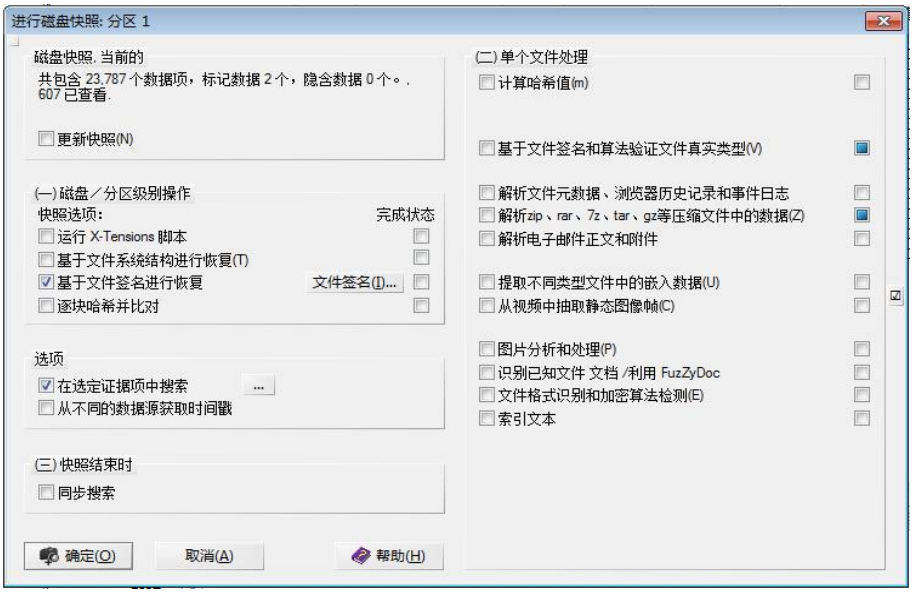

图 2-4-3 磁盘快照

2.选择恢复 Doc，设置文件名前缀“Recover_”

图 2-4-4 选择签名恢复的类型 doc

3.通过文件名过滤“Reovery*”过滤，共计找到 80 个文件。

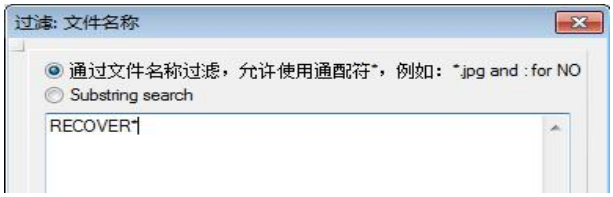

图 2-4-5 过滤所有恢复的文件

图 2-4-6 统计文件数量

实验 2-23:磁盘快照

配合案例文件：2.1-CCFC.e01，本节实验仅需针对分区 1 数据进行操作。

实验描述：XX 案件中需要对 doc 格式文件进行搜索。调查员对分区 1 进行了查找之后，总计发现有 20 多个 doc 为扩展名的文档。那么，分区中包含的 doc 格式文件只是这么多吗？

第一部分：

1、分区 1 中所有扩展名为 DOC 的文件数量：＿＿＿＿＿＋＿＿＿＿＿；（例：20+1）

2、分区 1 中所有文件类型为 DOC 的文件数量：＿＿＿＿＿＋＿＿＿＿＿；

3、选择磁盘快照-基于文件系统结构进行恢复，过滤所有真实类型为 DOC 的文件数量：

＿＿＿＿＿＋＿＿＿＿＿；

4、选择“磁盘快照”-“基于文件签名进行恢复”-(选择 Documents 中的 OLE2/MS Office)后，过滤所有文件类型为 DOC 的文件数量：＿＿＿＿＿＋＿＿＿＿＿；

5、选择“磁盘快照”-“解析电子邮件正文和附件”，过滤所有真实类型为 DOC 的文件数量：

＿＿＿＿＿＋＿＿＿＿＿；

6、选择磁盘快照-解析 ZIP、RAR 等压缩文件中的数据，过滤所有真实类型为 DOC 的文件数量：

＿＿＿＿＿＋＿＿＿＿＿；

第二部分：

基于第一部分操作后，继续实验并回答问题：

1、请选择“磁盘快照”-“更新快照”，将所有以解析的数据还原原始状态。

2、此时，重新过滤并分析分区 1 中所有真实类型为 DOC 的文件数量为：＿＿＿＿＿＋＿＿＿＿＿；

3、在磁盘快照中，同时勾选基于文件系统结构进行恢复、基于文件签名进行恢复(选择 Documents 中的 OLE2/MS Office)，鉴于文件签名和算法验证文件真实类型，解析电子邮件正文和附件，解析 ZIP、RAR 等压缩文件中的数据，开始进行磁盘快照，过滤所有真实类型为 DOC 的文件数量：＿＿＿＿＿＋＿＿＿＿＿；

实验 2-24：教训平台“2.4 磁盘快照”练习题

配合“C:\CDF\2-取证基础\2.2-FAT-Disk.E01”完成 10 道练习题。