2.2 过滤与组合过滤

过滤，即按照设定的条件查找符合条件的数据。Winhex 和 Myhex 都具有强大的过滤功能，可以通过各种组合条件实现精确的数据查找。通俗来说，过滤的功能就像软件中的“漏斗”一样，把想要的东西留下来，将不要的东西筛走。通过过滤可以将复杂的操作简单化，快速找到自己想找的文件。

本节实验，重点学习文件过滤，快速找到所需要的文件类型。掌握过滤的操作方法、理解组合过滤。结合相关知识点，达到可以利用系统信息、文件属性快速找到所需文件的目的。

一、文件名过滤

文件扩展名，可以理解为一种软件特有的格式定义。通过扩展名，Windows 可以帮助我们搜索到这些相同扩展名的文件。对于文件，我们一般还会进行分类，例如：文档类、图片类、视频类、邮件类、压缩类等等。

每个文件都有一个名字，称为文件名，它由字母、数字或字符组成。文件名又可分割为主文件名和扩展文件名，就拿“数字取证.docx”为例，“数字取证”就是主文件名，主要说明文件的内容，docx 为扩展文件名，它主要说明文件的性质(在这里表示 word 文档)，中间的小数点为主文件名和扩展文件名的分隔符。在 DOS 下，文件名采用 8＋3 结构，即：最长 8 位的文件名，由小数点分隔后再跟上最长 3 位的后缀名，如：READ.ME、SETUP.EXE。

实验 2-5:指定文件名称过滤

本实验配合案例文件：C:\CDF\2-取证基础\2.1-CCFC.E01

通常，采用文件名进行过滤是最简单的方法。为了快速过滤某一类文件，或与某个字符相关的文件名或目录名称，Myhex 允许通过文件通配符 * 号或？配合过滤。当通配符位于文件名的最前面和最后面时，最多使用 2 个星号。

*.doc	查找所有扩展名是 doc 的文档
*.jpg	查找所有 JPG 图片
1.gif	查找文件名为 1.gif 的文件
峰会*.bak	文件名是中文峰会为起始字符，扩展名为 bak 的文档

查找所有 DOC 文档：点击“文件名称”右侧的灰色漏斗，输入过滤条件*.DOC，点击激

活即可。可同时过滤多个文档：可同时准确文件名为“index.dat”的文件。

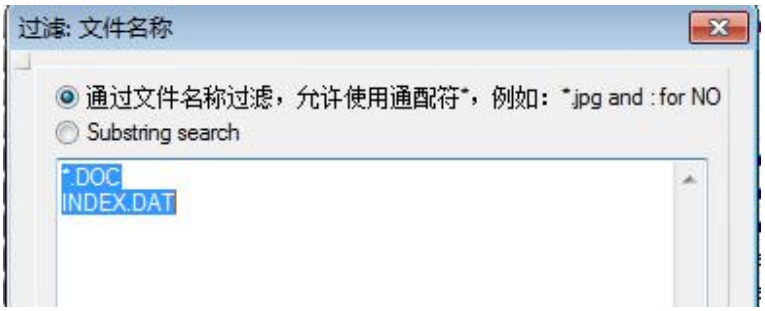

图 2-2-1 同时过滤多个文件名

应用上述过滤后的结果。当前分区中符合上述 2 个条件的所有文件都被显示出来。

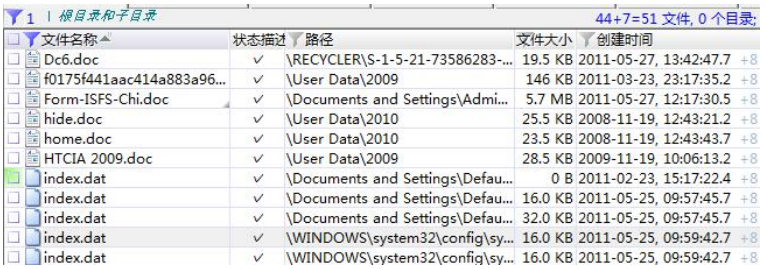

图 2-2-2 过滤结果

应用过滤之后，对任何目录操作都会自动应用此过滤。有时你可能会忘记了自己启用了过滤，会因为在当前目录下看不到文件而奇怪。其实，只要看到栏目上醒目的蓝色漏斗，就应该立刻想到，是因为启动了某个过滤条件而影响了文件的浏览。需要取消某个过滤条件，可调用目录浏览器过滤设置对话框，选择已经应用的过滤条件，点击“禁用”即可。也可单击两端的蓝色漏斗，直接取消所有过滤。

图 2-2-3 过滤条件被激活，没有发现过滤结果

实验 2-6：多分区中过滤多个文件

本实验配合案例文件 C:\CDF\2-取证基础\2.2-FAT-Disk.e01

1. 所有分区中，扩展名为 doc 和 docx 的所有文档总计_____个？

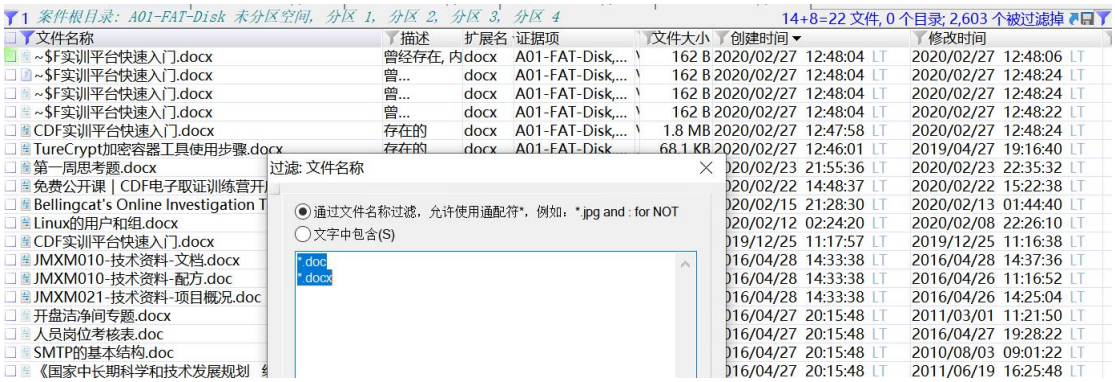

图 2-2-4 所有分区中过滤多个文件名

2. 查找分区 3 中，文件名为 1.png 的文件共有_____个？

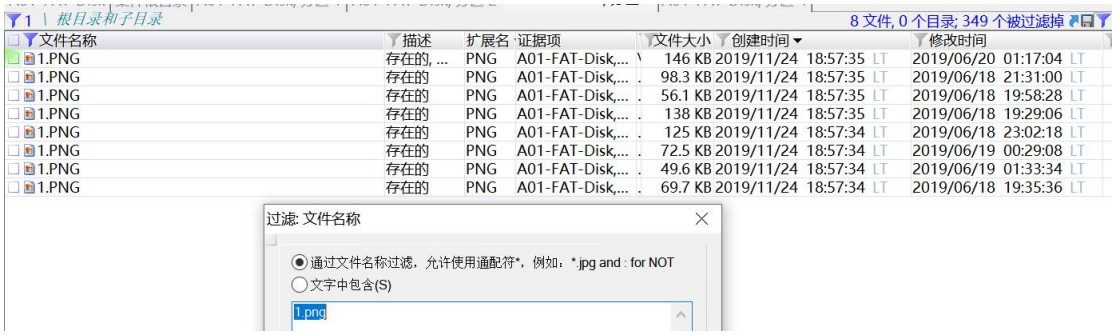

图 2-2-5 指定分区分区中过滤同名文件

3. 查找所有分区中，文件名以 1 为起始字符的文件数量为_____个。

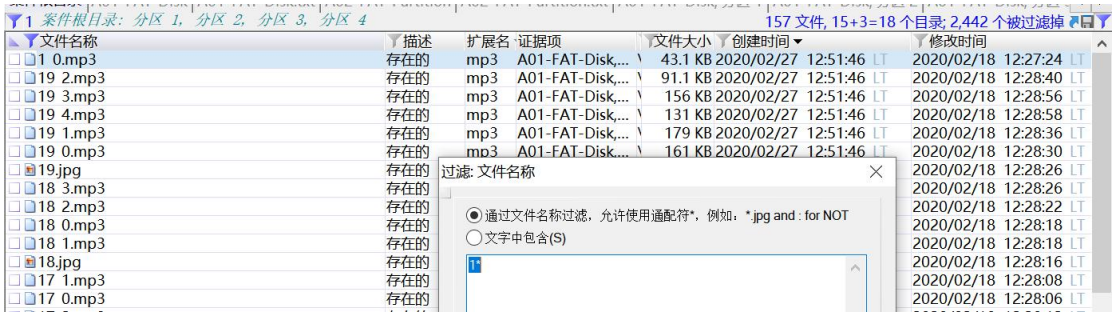

图 2-2-6 指定分区分区中过滤特定文件名

4. FTK 软件保存在分区_____？

图 2-2-7 指定分区分区中过滤特定软件名称

5. 所有分区中，文件名中包含“技术资料”四个字符的文件有_____个？

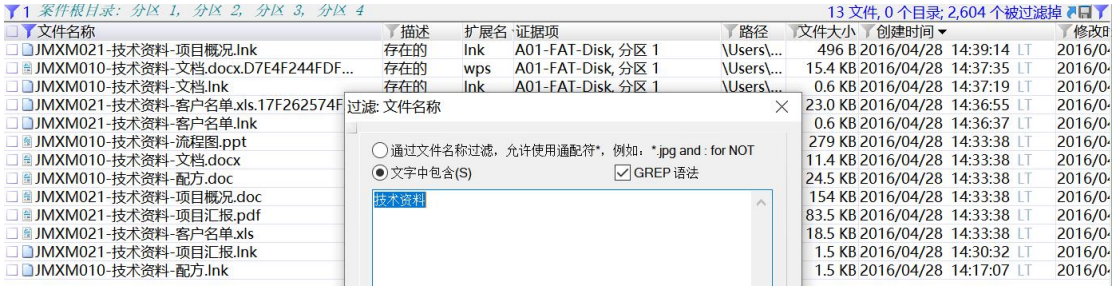

图 2-2-8 文件名之中包含特定字符

实验 2-7：教训平台“2.3 文件名称过滤”练习题

配合“C:\CDF\2-取证基础\2.1-CCFC.E01”完成 19 道练习题。

二、组合过滤

过滤可以通过文件名、文件类型、时间、大小、位置等方式，帮助我们更加快速地寻找到如“2016 年制作的大于 1GB 的视频”、“所有 2018 年复制到本地的 doc 文件”等等。组合过滤是取证调查中非常有效的数据分析方法。而 X-Ways Forensics 和鉴证大师采用相同的过滤机制，是所有取证软件中过滤最直接、效果最好的工具。而 X-Ways Forensics 支持大量的属性过滤，需要全面掌握才能发挥出过滤的优势，缩短分析时间。例如，在实际案件中，调查员经常需要快速过滤出当前案件中的 Office 文档、电子邮件，也可能会需要查找一个操作系统注册表文件或上网记录，或者要将案件中所有的图片查找出来。

1. 时间属性过滤

在“目录浏览及过滤设置”窗口中，所有带有漏斗的栏目都可以进行过滤操作。显示灰色漏斗的，表示未启用过滤选项；如果显示为蓝色漏斗的，表示当前已应用了过滤设置。

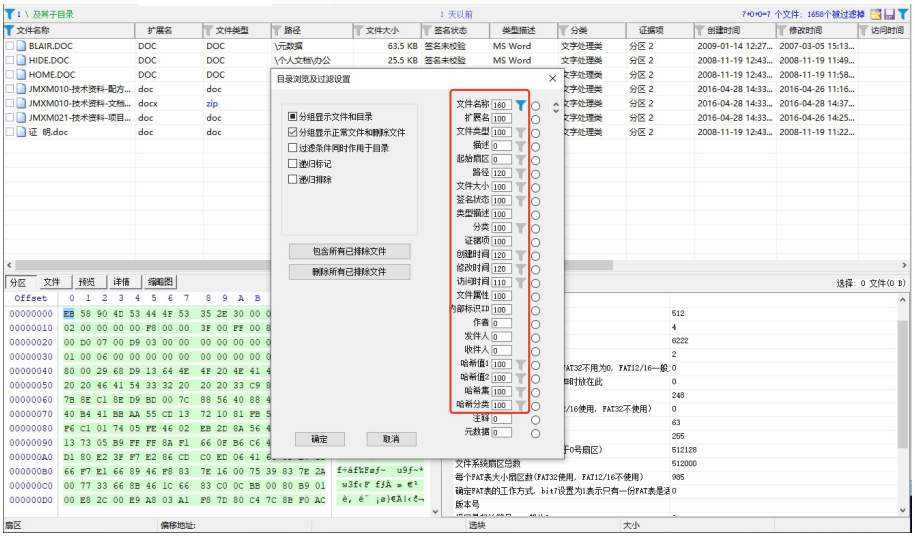

图 2-2-9 Myhex 中可进行过滤的列

例如：如果调查员想找到所有在 2008 年 11 月 19 日创建的文件，可以利用时间排序功能，将所有的文件全部按照升序或降序排列，然后找到创建时间是 2008 年 11 月 19 日的文件。但是，利用时间过滤则更加有效，可以直接将创建时间是 2008 年 11 月 19 日的所有文件显示出来，将不属于这个日期的文件隐藏掉。

可按照设定的文件分类，对不同类型的文件进行过滤。通过此过滤方式，可以容易地将办公文档、图形图像、压缩文件，

Windows 时间属性很多。后续章节会详细介绍创建时间、修改时间、访问时间、记录更新时间、删除时间、内部创建时间等。

创建时间：创建时间代表文件在一个位置生成的时间。

修改时间：文件被最后编辑、写入数据的时间。

访问时间文：件被访问的时间，是计算机系统本身对文件进行了某种操作的时间。最常见的行为是：文件打印、查看（打开并未保存）。此外病毒检测、文件备份、系统维护等操作都会改变文件访问时间。FAT 文件系统仅记录访问日期。NTFS 文件系统下的访问时间可以记录至秒。

记录更新时间：NTFS 文件系统 FILE 文件记录(FILE record)、Linux 文件系统索引节点(inode)中文件和目录的最后发生变化修改时间。这是文件系统数据结构中包含的数据时间信息。索引节点：在 Linux 文件系统下，每个存储设备或存储设备的分区被格式化为文件系统后，包含两部份，一部份是索引节点，另一部份是块区(Block)。块区是用来存储数据用的，

索引节点是用来存储数据的信息，包括文件大小、属性、归属的用户组、读写权限等。 索引节点为每个文件进行信息索引，所以就有了索引节点的数值。Linux 系统根据指令，能通过索引节点值快速地找到相对应的文件。

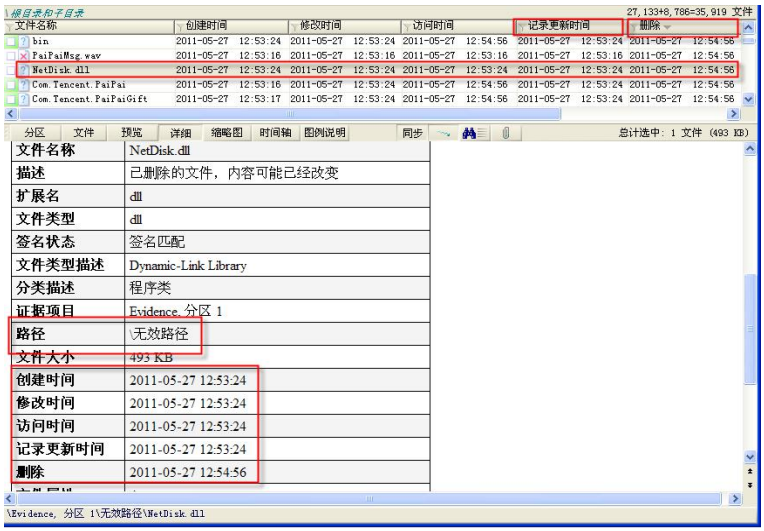

图 2-2-10 各种时间属性

删除时间：是一个最难判断的问题。我们很难从文件时间属性直接来判断某个文件到底是什么时候被删除的。因为文件系统并不直接记录文件的删除时间，某些 NTFS 元数据会记录删除时间，回收站可以记录某个文件是的删除时间。不同的取证分析工具对删除时间的认识和解析方法不同。X-Ways Forensics 中，可以显示 Linux 文件系统或 NTFS 文件系统（在对文件系统对$UsnJrnl:$J 文件解析后）某些目录和文件的删除时间。

内部创建时间文件元数据中记录的文件真正的创建时间。Microsoft Word 和 Excel，数码相机、手机拍摄的图片都包含有时间属性。内部创建时间通常不易被人为修改，也不会被文件系统自动修改。可以通过内部创建时间和其他时间属性一同分析判断用户行为。

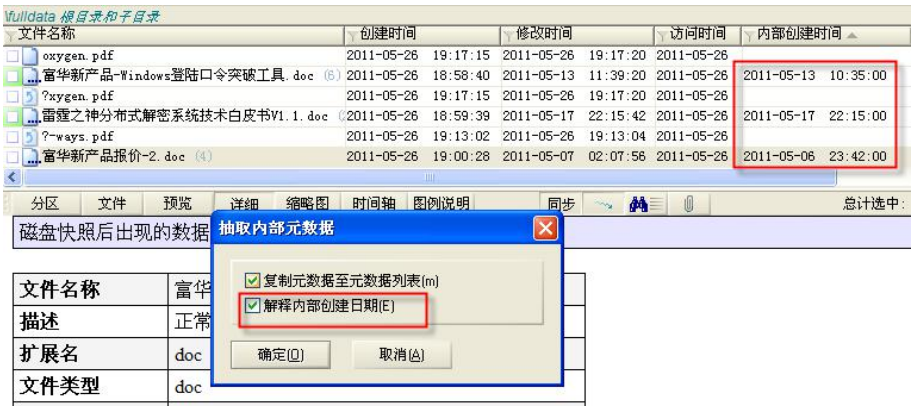

图 2-2-11 提取内部创建时间

此外，某些文件的元数据中还可能保存一些其他的时间信息，例如文件打印时间、图片的编辑时间、邮件的发送时间。

图 2-2-12 元数据中包含的打印时间