CDF BOOT CAMP
电子数据取证技术训练营

《电子数据取证实验》

第 2 章 取证基础

数字取证是法医学的重要分支，其包括对数字设备中发现的材料的恢复、调查、检查和分析，通常与移动设备和计算机犯罪有关。数字取证调查主要包括：计算机取证、网络取证、移动手机取证和 IOT 设备取证等方向，因此，数字取证也被认为是计算机科学技术的一个重要的分支。教材第二章从计算机科学的角度出发，结合数字取证中遇到的实际问题，来介绍一些基础的计算机科学知识。

配合教材涉及的取证基础知识，对应的实验课将学习通用取证分析工具基本使用方法，并学习文件过滤、组合过滤、文件浏览、内容预览、关键词搜索、文件签名的基础知识。

本章节包括 7 个实验模块，涉及 Winhex 软件设置和基础操作、文件名称过滤、组合过滤、文件签名和签名库、磁盘快照、关键词搜索等内容，都是取证分析中需要熟练掌握的内容。

2.1 取证软件基础操作

实验目的：学习 Winhex 和 Myhex 软件的使用方法，是后续实验模块的重要基础实验。

实验 2-1：启动 Winhex，创建案件，查看环境

本实验无需镜像文件。

1.启动 Winhex

2.参考图 2-15，点击“案件数据”-“文件”-“创建案件”

3.参考图 2-16，输入案件信息，案件名称命名为“2.2-FAT”

4.参考图 2-12，点击菜单“选项”-“常规设置”，查看并记录环境设置

5.参考图 2-13，点击菜单“选项”-“文件查看”，查看并记录查看器设置

6.参考图 2-10，点击菜单“帮助”-“设置”，切换菜单语言为中文、英文。

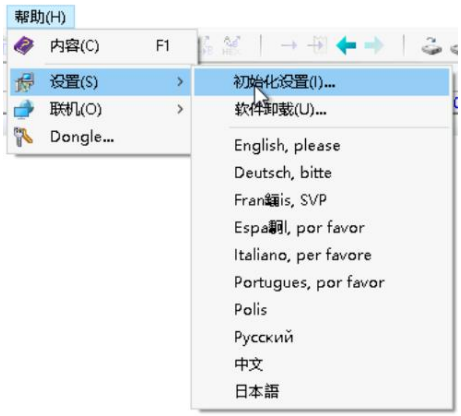

图 2-1-24 切换语言设置

练习：点击菜单“帮助”-“设置”-“初始化设置”。重新启动软件，还原至初始化设置之前相同的配置环境。

实验 2-2：加载镜像文件，查看磁盘和文件模式

本实验配合镜像文件：C:\CDF\2-取证基础\2.2-FAT-Disk.E01

实验步骤：

1.点击“案件数据”-“文件”-“添加镜像文件”

2.选择“C:\CDF\2-取证基础\2.2-FAT-Disk.E01”，点击“打开”

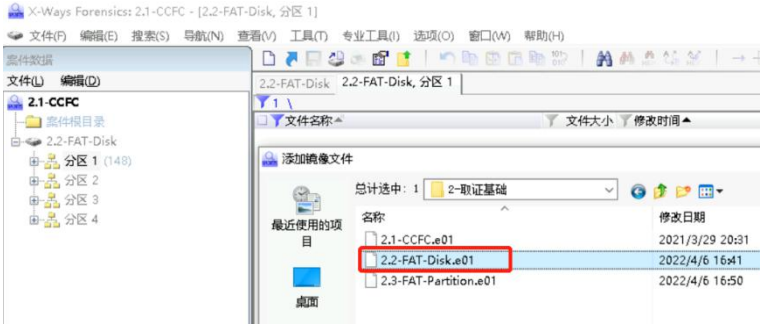

图 2-1-25 添加镜像文件

3.取消所有过滤条件。在文件名称位置或上方位置，如见到蓝色漏斗，表示当前启用了某些过滤条件。点击文件名称上方位置的蓝色漏斗，点击“是”禁用所有过滤条件。

图 2-1-26 禁用所有过滤

4.点击分区 1，找到“~$实训平台快速入门.docx”，162 字节，以“分区”视图模式查看文件内容。

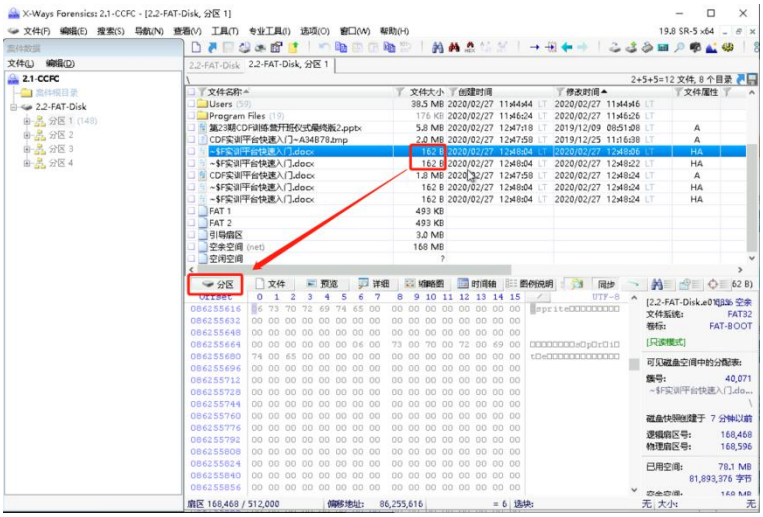

图 2-1-27 以分区视图模式查看

5.针对相同文件“~$实训平台快速入门.docx”，以“文件”模式查看文件内容。

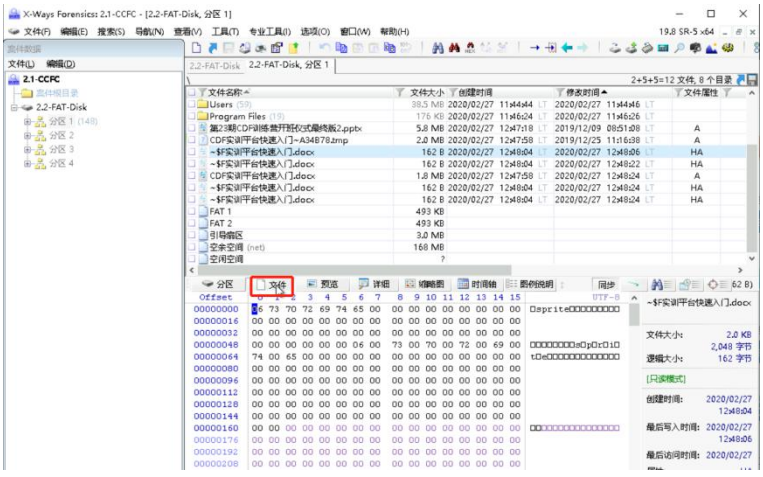

图 2-1-28 以文件视图模式查看

问题 1：为什么“分区”模式下十六进制数值为灰色？

问题 2：“文件”模式下被标记为紫色的数值应如果理解？

实验 2-3：“预览”和“详细”模式查看信息

本实验配合镜像文件：C:\CDF\2-取证基础\2.2-FAT-Disk.E01

实验步骤：

1.点击分区 1，找到“CDF 实训平台快速入门~A32B78.tmp”，2MB，以“详细”模式查看。

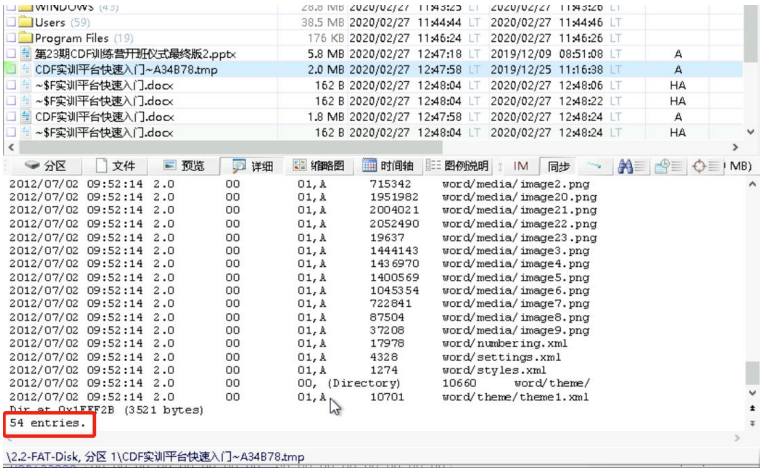

图 2-1-29

2. 针对相同文件，以“预览”模式查看文件内容。

图 2-1-30

问题 1：该文件元数据中，tmp 文件内共包含有 54 个数据项吗？

问题 2：这个 tmp 文件的真实类型是什么？

问题 3：记录这个 tmp 文件的前 8 个字节。

七、展开目录和文件

学习使用 X-ways Forensics，需要掌握几个必会的操作。掌握这些操作后，经过几天的反复练习，大家能够彻底掌握 Winhex、X-Way Forensics。本实验内容，将练习目录和文件管理、软件界面设置、文件浏览等基本操作。

本节实验使用镜像文件：C:\CDF\2-取证基础\2.1-CCFC.E01。

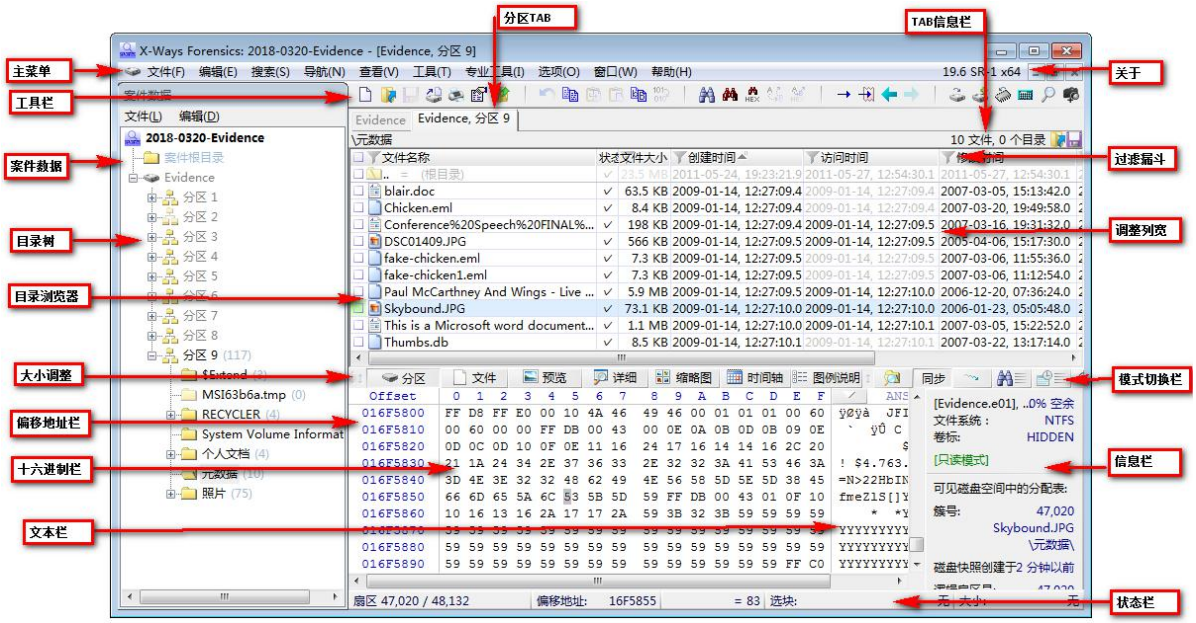

图 2-1-31 X-Ways Forensics 操作主界面

1、展开目录

X-Ways Forensics 中的目录需要层级展开，而且每一层都需要专门选择浏览，用户需根据需要选择指定分区来展开目录并浏览。

2、开所有证据项下的数据

在案件目录窗口**右键点击**案件根目录，并选择需要展开的分区；展开所有证据后，可以列出分区下的所有的文件。

应用场景：需要统计整个磁盘所有分区下有多少个文件？显示所有磁盘中的被删除文件？预览所有磁盘中的图片的缩略图？都需要使用这个操作。

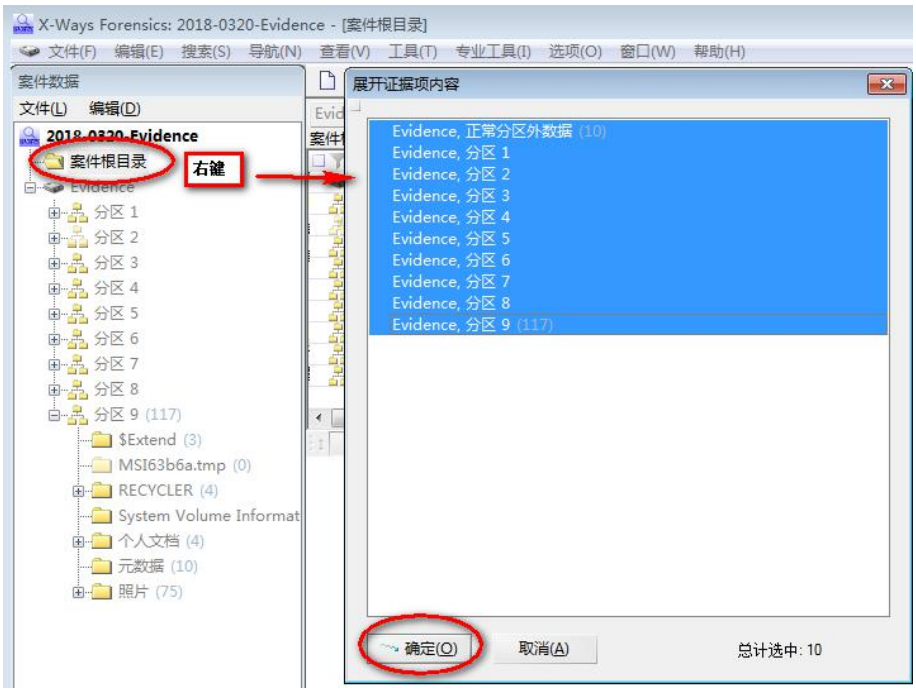

图 2-1-32　选择分区展开证据界面

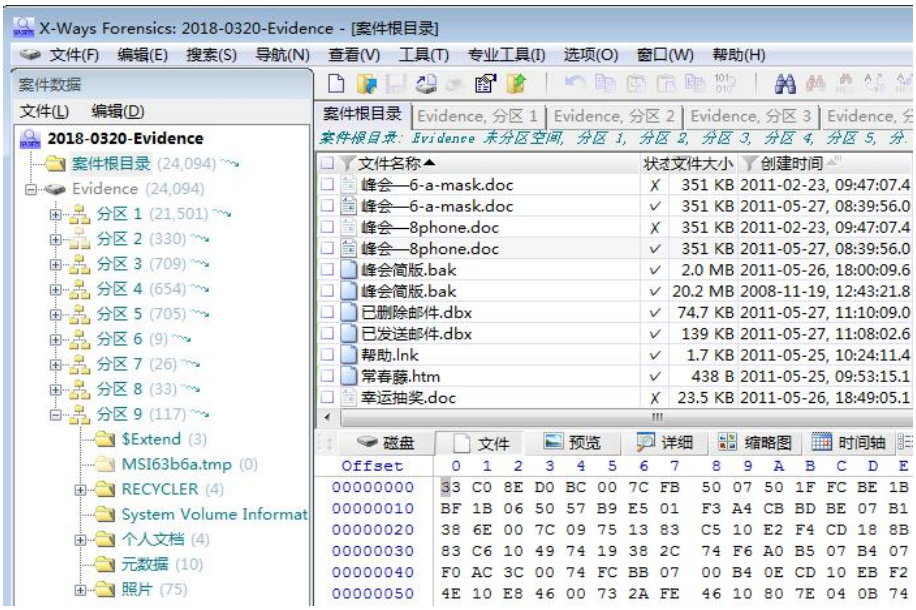

图 2-1-33 证据展开后的效果

3、展开某个分区

鼠标右键点击分区1，选择“浏览递归”，则能查看该分区内的所有文件。

应用场景：查找C盘中的所有注册表文件；C盘中的所有办公文件等。

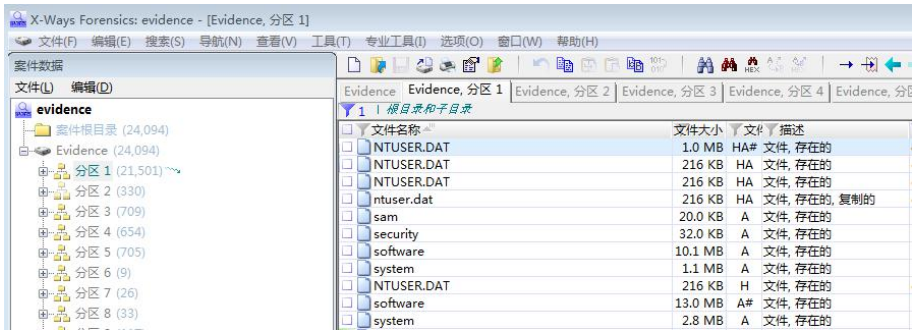

图 2-1-34　过滤分区 1 下注册表文件

右键点击某一个目录，可以显示该目录下的所有文件。

应用场景：查找C盘Document and Settings目录中的所有doc文件、Windows目录下的注册表文件。

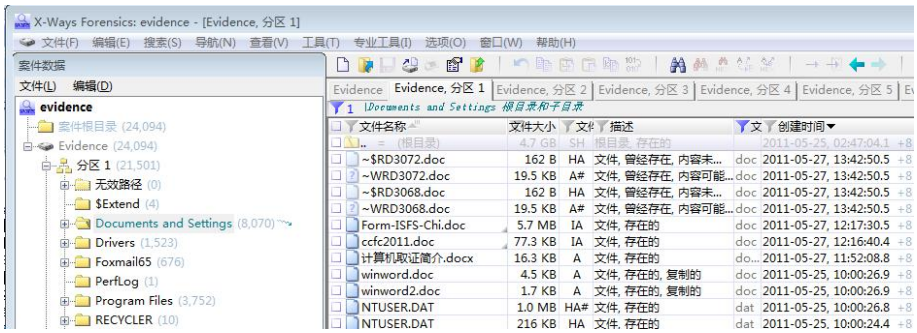

图 2-1-35　查看 Document and Settings 目录下的所有文件

4、设置需要的栏目和列表

浏览设置是 X-Ways 里面一个隐藏的快捷键，下图红色标记出的菜单栏空白区域，是一个通往设置显示列表的入口。

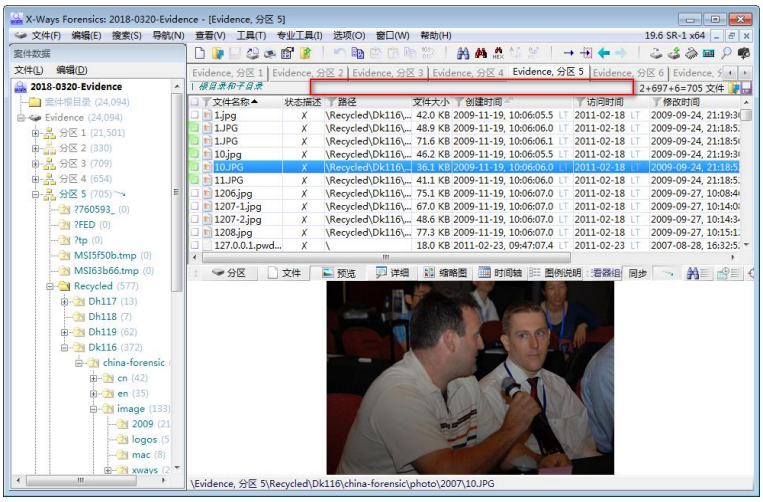

图 2-1-36　点击 TAB 信息栏 （看到 X-Ways 作者 Stefan，右一）

点击红色框区域会弹出设置窗口，选择需要显示在列表中的那一栏，使其后面的值不为零即可。数值表示显示的宽度，通常习惯设置成100。点击圆圈，可以通过箭头调整在列表栏的前后显示顺序。包含漏斗图标的列，都可以进行过滤。过滤操作，2.3节将全面练习过滤操作。

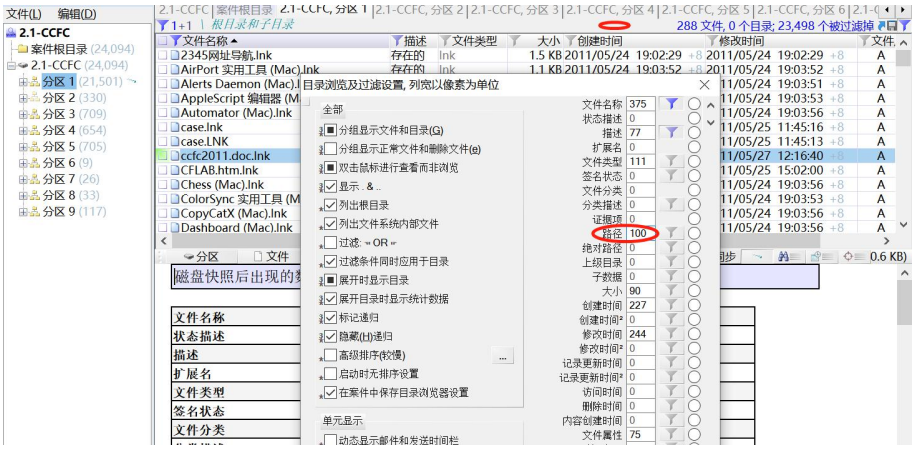

图 2-1-37　设置目录列表的显示栏

实验 2-4：教训平台“2.1 Winhex 软件基础操作”练习题

配合案例：C:\CDF\2-取证基础\2.1-CCFC.E01

要求：完成实验环境中的练习题。