CDF BOOT CAMP
电子数据取证技术训练营

实验

取证基础/软件入门

目录

1 取证基础-软件入门

1.1 实验内容

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。取证软件可通过过滤来对所需要的文件进行快速查找。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。过滤是取证调查中非常有效的数据分析方法。而 X-Ways Forensics 和法证通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。

- 文件过滤：什么是过滤？怎么使用过滤
- 文件名和扩展名过滤：*.DOC, A*.DOC，?
- 文件类型库：对文件类型的定义，如图片类
- 文件类型描述：文件类型的创建软件,pst:OUTLOOK
- 排序：升序、降序
- 通过文件名过滤：常用办公文档、常用图片
- 通过文件类型过滤：所有邮件，所有图片
- 组合过滤：大于 1MB 的 PDF 文件，小于 4K 的文件等
- 保存过滤条件：所有大于 1KB,小于 100MB 的所有办公文档
- 修改文件类型库：
- 高级过滤条件：通过属性过滤，如$j 文件的过滤
- 排除和隐藏：路径中不包含 OFFICE 的文件；隐藏小于 4KB 的._文件。

1.2 实验目的

实际数据分析过程中，经常需要对某一个文件或某一类文件进行过滤，以便缩小范围，查找到我们所需要的准确数据，提高工作效率。例如，时间案件中，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。

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。

1.3 实训资源

C01-CCFC-Windows XP.e01

1.4 背景知识

1.4.1 X-Ways 软件概述

X-Ways Forensics，是基于 Winhex 的一个数据恢复和十六进制编辑器，是功能强大的电子数据取证分析工具。

图 1 X-Ways Forensics 套件

必学 X-Ways 的几个实在理由

- X-Ways 所出具的报告在国际范围具有法庭认可性；
- 界面永久不变，软件一经掌握，终生可以熟练使用；
- X-Ways 系列工具应用领域广泛：计算机法证据、E-discovery、数据恢复、底层数据处理以及 IT 安全等；
- X-Ways 可以提供自己独立的计算机法证培训以及课程，并出具 X-PERT 证书。

Winhex 与 X-Ways Forensics 的关系

Winhex 是 X-Ways 公司的 CEO Stefan 先生在学生时代写的一个十六进制编辑器，主要用于磁盘和内存十六进

制编辑，常被用于数据恢复和磁盘编辑，但其被忽略的法证功能更为强大。

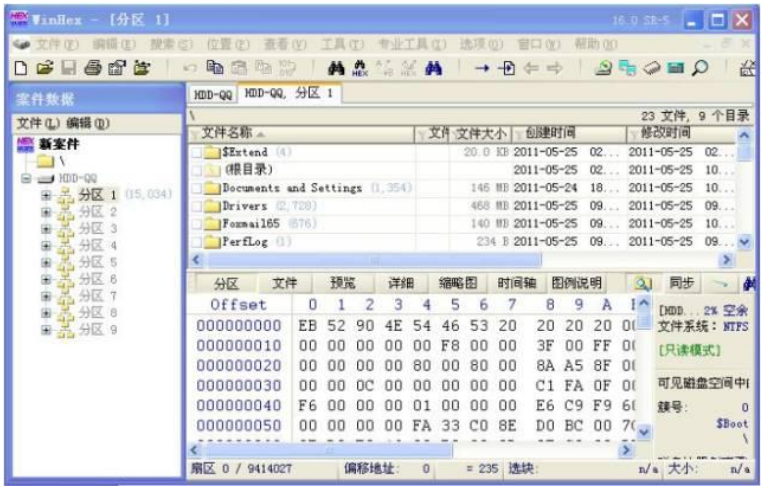

图 2 Winhex 界面

Winhex 功能主要有四个：

- 磁盘克隆、数据镜像
- RAM 内存编辑：对内存信息直接编辑，如调试内存、编译程序等；
- 文件分析：分析文件格式、判断文件类型，如使用 chkdsk 命令分析磁盘数据挽回丢簇数据从而判断数据格式；
- 擦除涉密磁盘：可对磁盘填充 0 或任意值，保证数据安全的最佳方式。

X-Ways Forensics 则是为计算机取证分析人员提供的一个功能强大的综合取证平台，与 Winhex 紧密结合，能够发现很多其他分析工具无法找到的数据和文件。

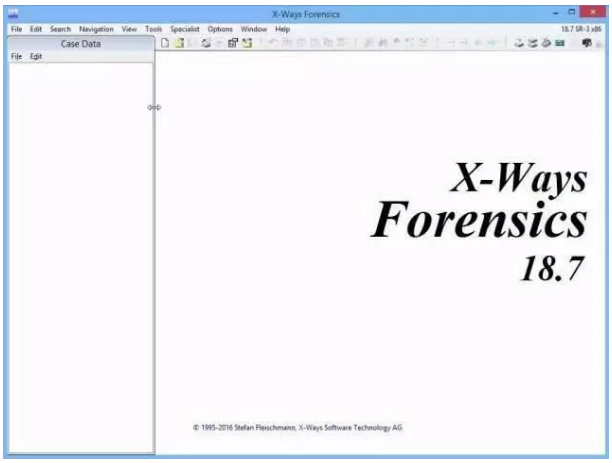

图 3 X-Ways Forensics 启动界面

X-Ways Forensics 与 Winhex 是包含关系，X-Ways 软件中含有 Winhex 工具，因此它具备 Winhex 所有的基本

功能，此外还有许多自己特有功能。X-Ways Forensics 和 Winhex 的主要区别如下图：

	代码	显示界面	下载安装	使用
Winhex	相同的代码基础	名称为Winhex	Winhex需要单独下载作为插件使用，且要放到X-Ways安装目录下	编辑磁盘、镜像
X-Ways		名称为X-Ways		只读模式严格写保护

图 4 软件区别

1.4.2 软件安装和升级

图 5 软件套件

安装

购买了 X-Ways Forensics 软件后，会包含软件和注册码（WinHex），USB 加密狗。需要提示一下，X-Ways Forensics 是免安装的。在这里要说一下后期软件升级的安装问题，早期的升级文件包，如下图所示。只需要下载最新的 xw-forensics.zip，替换原有文件即可。 viewer.zip 为 X-Ways Forensics 的 OutsideIn 查看器插件，定期也会有更新；Winhex-add-on.ZIP 现在已经不再提供。如果需要使用 Winhex，只需将 X-ways Forensics 主程序文件名，重命名为 WINHEX 即可。

图 6 升级文件

两种安装方法，自动和手动，具体使用哪种方法可根据用户习惯自由选择。

自动安装：X-Ways Forensics 软件可以通过 setup.exe 自动安装使用，你也可以选择复制到适当位置， 运

行 xw_forensics.zip 直接使用，通常来说这种方式更方便。19.6 版的 xw_forensics.zip 解压缩后，共包含图中显示的 74 个文件和 1 个目录。

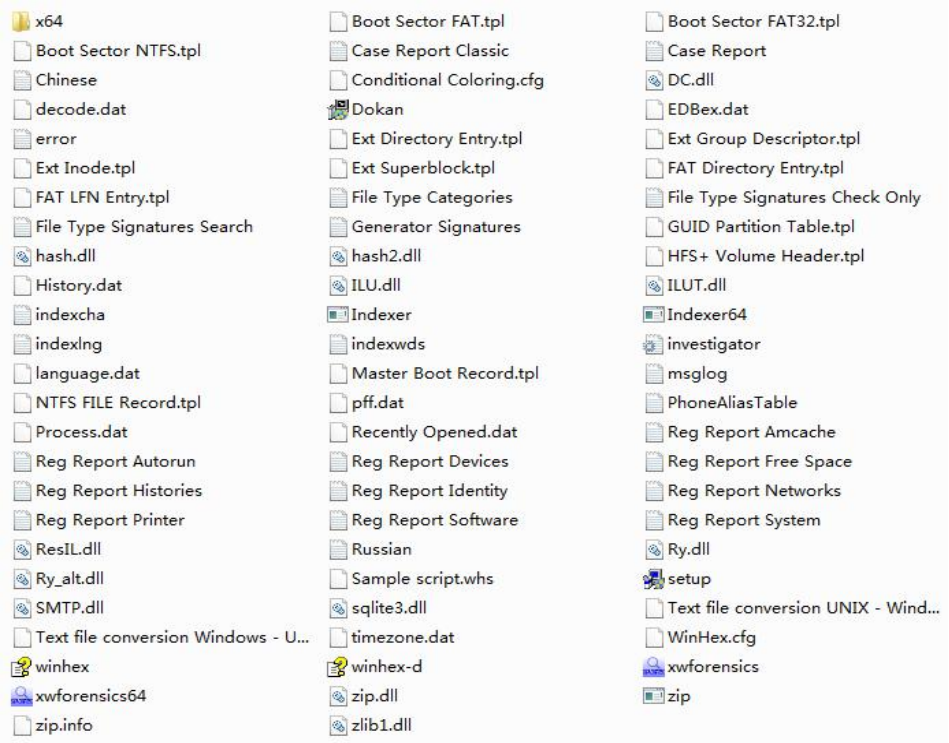

图 7 软件安装文件

手动安装的主要步骤和建议操作如下：

- 将 xw_forensics.zip 压缩文件解压缩，释放至同一个目录中，如：“C:\CDF\CDF-Winhex\19.8”目录下。
- 将 Viewer.zip 解压缩后复制到 xw_forensics.zip 所在目录下。如：复制至“C:\CDF\CDF-Winhex\19.8”目录下。
- 建立案件数据存储目录。

X-Ways Forensics 软件运行过程中，将会需要**保存临时文件、保存案件数据、保存哈希库、 保存磁盘镜像**等数据。为了使各种数据能够有规律地保存、并为将来快速找到所需数据，我们需要建立几个单独的目录用于保存相关数据。

保存有 X-Ways Forensics 软件临时文件和案例文件的分区将作为默认的数据输出路径，X-Ways Forensics **只会向该分区写入数据**。因此，在选择 X-Ways Forensics 软件使用分区时， 需要考虑好未来数据分析的实际情况。**建议选择容量较大，数据较少的分区；**或可以将镜像目录设置在其他磁盘或阵列中。

用户可以参照下图建立五个文件夹，分别用于保存**案例文件、哈希库、镜像文件、脚本和临时文件。**

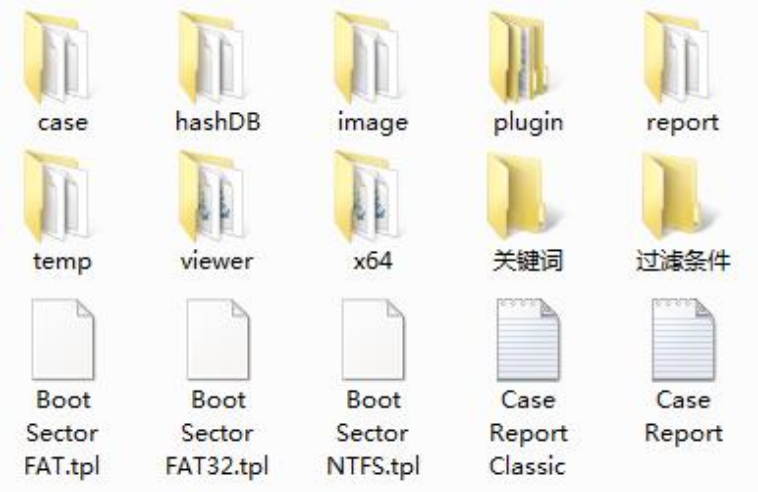

图 8 创建案例、镜像、临时目录

文件夹名称可自定义，但通常来说，为了保证案件数据、临时文件保存有序，也便于今后其他协同分析的调查员均保持相同的软件使用习惯，**建议所有用户都采用 case、image 和 temp 等相同的文件夹名称。**

随着不断的积累，大家可能会发现，有些关键词、过滤条件会在案件中经常使用，那么自己也可以建立“关键词”、“过滤条件”文件夹，保存自己特有的一些辅助数据。

对于拥有局域网络，或有大容量磁盘阵列的用户来说，也可以将这三个目录建立在共享磁盘中。这样，所有局域网中各独立计算机中的 X-way Forensics 都可以调用共享磁盘中的案例和磁盘镜像文件，有助于提高工作效率。（小窍门赶快 Get！）

1.4.3 软件配置

语言配置

运行 X-Ways Forensics 软件后，软件首次启动会弹出英文界面，显示 Winhex 版权信息提示。关闭 Winhex 帮助文件后，会看到 “General Options”(常规设置)窗口。

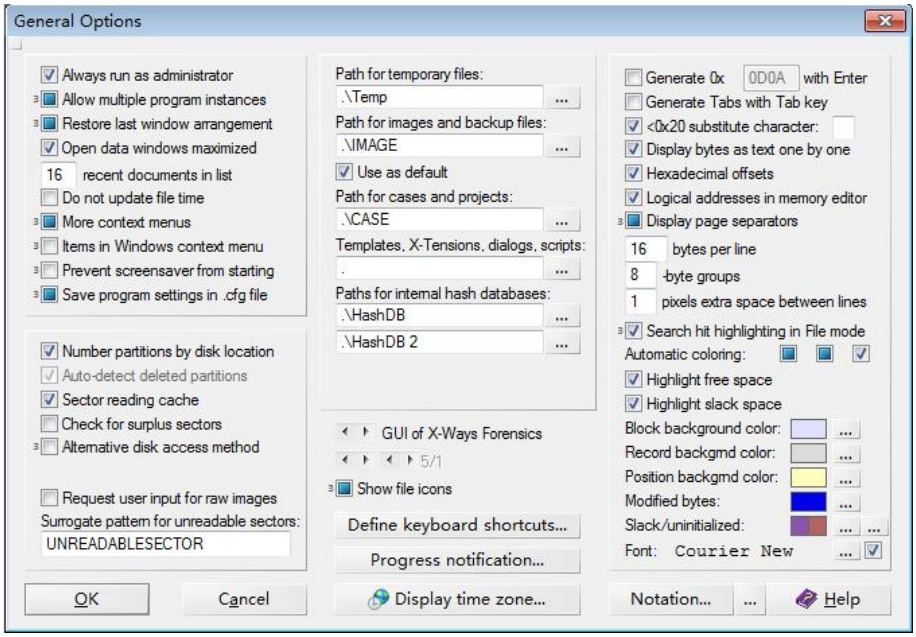

图 9 常规配置界面

要将软件设置成为中文界面，点击菜单中的 “Help”(帮助)。然后选择“Setup”(设置)，接着选择“中文”。

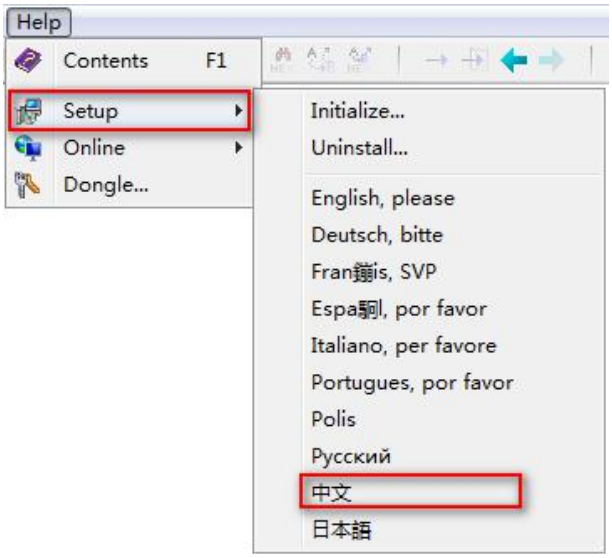

图 10 修改界面语言

常规设置：目的是为 X-way Forensics 和 Winhex **设置一个良好的运行环境，将个人操作习惯保存为固定设置。**其中，最主要就是**设置临时目录和案件保存目录，**以便用户能够从固定的、习惯的位置找到案件中产生的数据。

点击“选项”调用“常规设置”，或者直接按 F5 键，即可进入“常规设置”对话窗。

图 11 调用常规设置

常规设置窗口中，方框标记的区域是主要的设置内容。

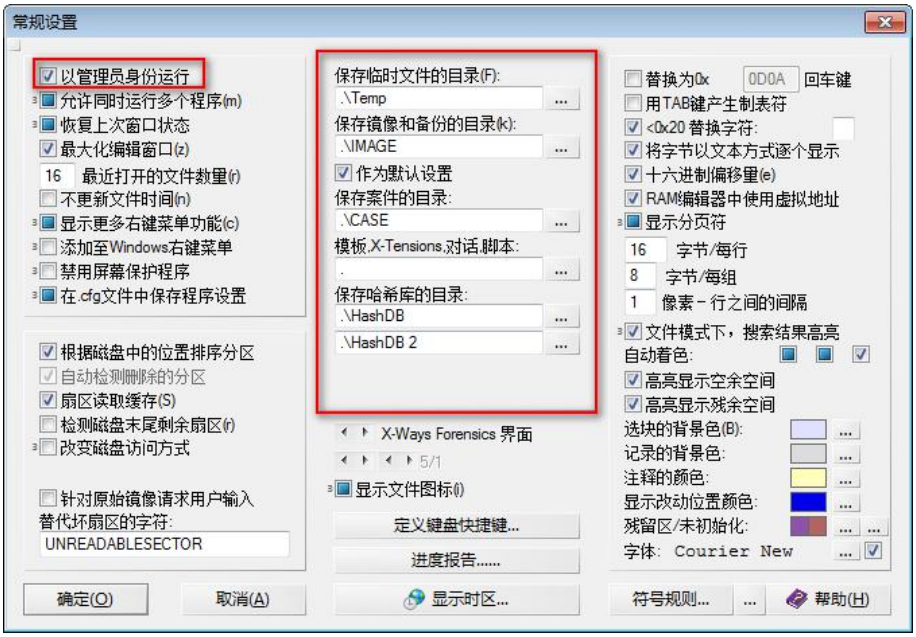

图 12 常规设置内容

保存临时文件的目录:用于保存分析过程中临时生成的数据。软件最初设置中默认将临时文件保存至“C:\Documents and Settings\用户名\Local Settings\Temp”。为便于管理临时文件，我们为其创建一个 temp 文件夹，可以设置为绝对路径 C:\CDF\CDF-Winhex\temp，也可像本例一样设置相对路径。见图 12。推荐使用相对路径。

保存镜像和备份文件的目录:软件默认设置中镜像文件和备份文件会被保存至“C:\Documents and Settings\用户名\Local Settings\Temp”。为将来方便地调用和管理镜像文件，我们为其新创建一个 image 文件夹，本例中路径为 .\image。

保存案件的目录:当前系统默认保存至 X-ways Forensics 当前目录下，本例 为 E:\xway 目录。由于将来创建的案件越来越多，将这些案例文件保存在当前目录下会造成 混乱、不利于查找，因此，我们为其新创建一个案例文件夹，本例为 .\case。

模板、X-tensions、对话脚本的目录:当前系统默认保存在至 X-ways Forensics 当前目录下。如果不需要脚本，则无需改变。

保存哈希库的目录:系统默认哈希库保存位置为 .\HashDB。此目录可由 X-ways Forensics 自动创建和管理，无需改变。

查看器设置：如果后续发现文件无法预览成功，则可能是因为：

1.查看器路径设置问题。参考下图设置即可。

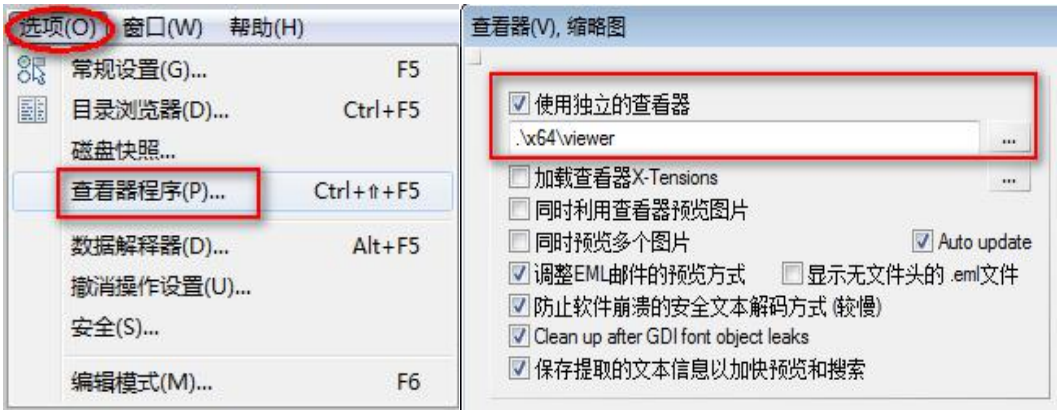

图 13　查看器设置

2.缺少 Visual C++ 2013 Package 。点击圆圈位置 19.6 Sr-X64，出现“关于”。查看 Visual C++ 2013 Package 之后，是否如图中所示。如果不是，请安装 Visual C++ 驱动。

图 14 查看“关于”

1.4.4 创建案件

创建新案件

利用 X-Ways Forensics 数据获取，或者进行数据分析，首先要创建一个新的案件。创建案件是为了将案件信息和需要分析的存储介质或者镜像文件加载到案例中。X-ways Forensics 软件本身不会使数据内容产生变化，但操作系统和应用程序则可能对新加入的设备造成数据修改。因此数据获取过程中，应注意使用硬件写保护设备。

创建案件，选择“案件数据”，然后点击“文件”，选择“创建新案件”。

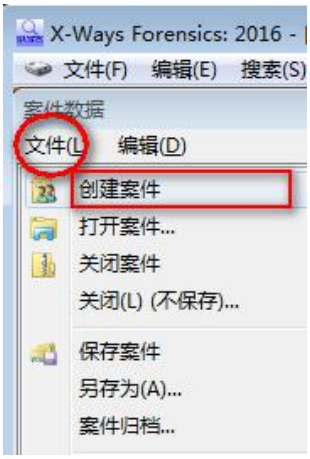

图 15 创建案件

图 16 创建案件，输入案件信息

在属性对话框中，可输入案件名称、案件描述、调查员、机构地址等辅助信息。案件名称可以根据需要设定一个便于记忆和区分的名字。

1. 案件名称需使用英文或数字，否则将来的日志和案件报告中无法出现软件窗口截图。

2. 调查员信息一经设置自动保存，后续创建案件可以自动调用，无需再次输入。

3. **X-ways Forensics 依据系统时钟自动生成案件创建日期。**为保障 X-Ways Forensics 在证据固定过程中记录的时间准确，且在日后数据分析过程中显示的时间正确，**请确保当前计算机系统时间设置无误，**并在显示时区中设置**正确的时区**信息。

4. 可以通过点击**“自动记录所有操作”**以启用或禁用自动日志功能。

5. **当前创建的案件目录将被默认为数据恢复、证据导出的保存目录。**如果需要将不同的案件中的证据文件导出到同一个目录下，可以禁用**“输出至缺省证据文件夹”**选项。

6. 可以根据案件情况**设置处理当前案件的代码页。**设定的代码页用于对案件中文件名称的支持，例如保存邮件时自动命名.eml 文件，解压缩 Zip 文件时将文件名自动转换为 Unicode。如果代码页设置错误，则文件名无法正常识别；如两个代码相同，不会对案件产生影响。如果代码页与当前 Windows 的代码页一致，则无需设置。

7. 创建案例还可以设置保护口令，但这并不是对案件数据进行加密，只是设置了一个打开权限。

1.4.5 视图模式

1. 磁盘模式

以分区、磁盘模式查看扇区数据。显示当前证据的具体信息，如文件系统、簇、扇区等。

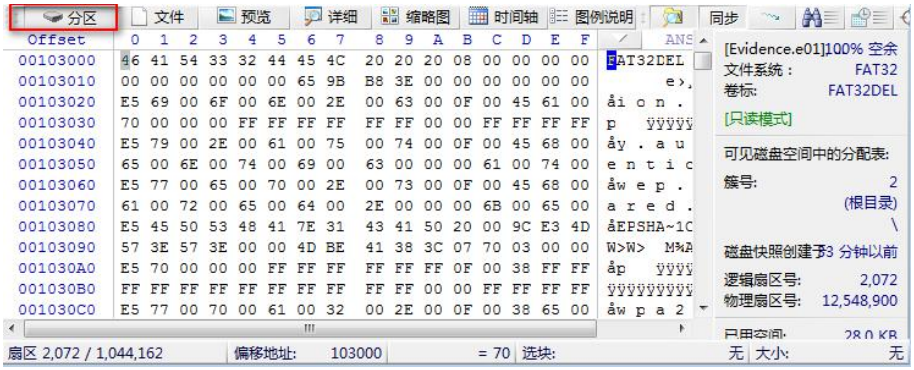

图 11 分区模式

2. 文件模式

查看所选文件的十六进制信息、对应的文本信息。显示关于文件的大小、时间等信息。

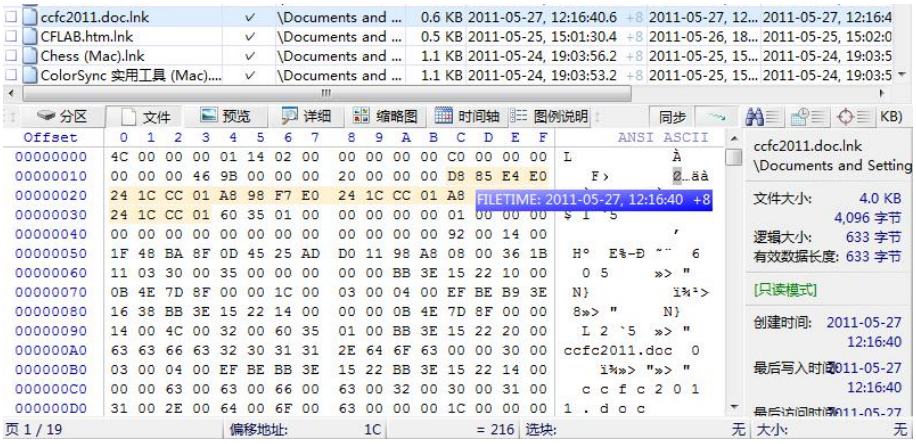

图 12 文件模式

3. 预览模式

利用 Outside In 技术查看文件内容。支持 300 多种文件格式预览。

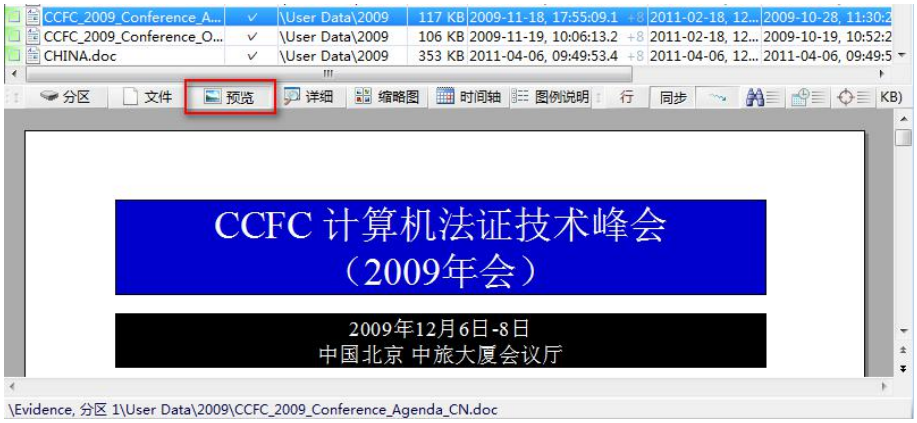

图 13 预览模式

4. 缩略图模式

以缩略图方式查看图片或视频抽帧图片。图中找到 Stefan。

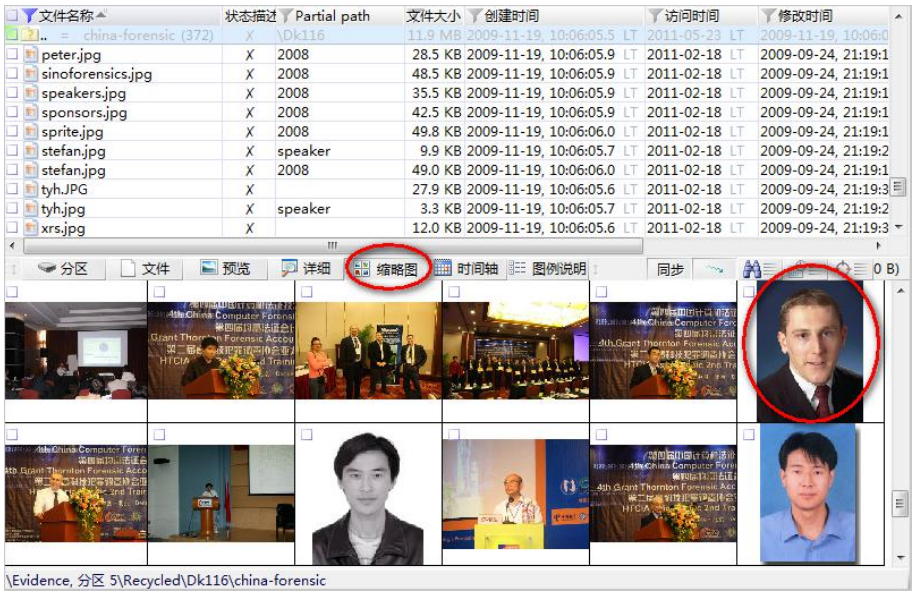

图 14 缩略图模式

5. 详细模式

查看文件的属性、元数据信息。如照片、Office、PDF 的内部时间、作者、版本等。

图 15 详细模式

1.4.6 目录浏览设置

浏览设置

这是 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。

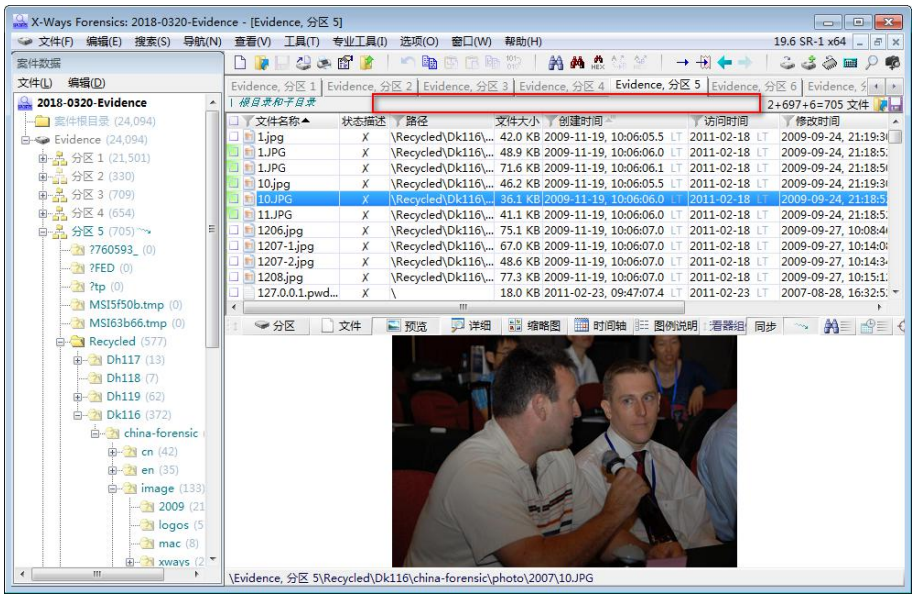

图 6 点击 TAB 信息栏 （看到 X-Ways 作者 Stefan 喽  ）

点击这个没有任何字的空白区域，就会弹出设置窗口，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。

图 7　设置目录列表的显示栏

1.5　实验步骤

1.5.1 X-Ways/ Winhex 软件设置和创建案件

X-Ways Forensics，是基于 Winhex 的一个数据恢复和十六进制编辑器，是功能强大的电子数据取证分析工具。

题目 1

在 64 位 Windows 10 中使用 X-Ways Forensics，应执行以下哪个版本的程序？

A：xwforensics64.exe

B：xwforensics.exe

C：winhex.exe

D：xwforensic64.bat

题目 2

当需要利用软件进行十六进制修改编辑等操作时，可以将 X-Ways Forensics 主程序变为 Winhex。你可以将程序更名为:

问题描述：多选题

A：winhex64.exe

B：myhex.exe

C：winhex.exe

D：mywinhex64.exe

题目 3

需要对磁盘底层数据操作时，应以管理员模式运行程序。如果不希望每次都点击程序选择“鼠标右键-以管理员身份运行”，应如何操作？

A：选项-安全-以管理员身份运行

B：选项-磁盘快照-以管理员身份运行

C：专业工具-常规设置-以管理员身份运行

D：选项-常规设置-以管理员身份运行

题目 4

默认状态下，X-Ways Forensics 会将程序运行过程中生成的临时文件保存在哪里？

问题描述：（本题目设定 C：为 Windows 和用户数据保存位置）

A：C:\Temp

B：C:\Users\用户名\AppData\Local\Temp

C：C:\Windows\AppData\Local\Temp

D：C:\X-Ways 安装目录\TEMP

题目 5

为使 X-Ways Forensics 管理好临时文件、案件、镜像和自定义的过滤条件，用户可自行创建一些文件夹将数据分类保存。一般应建立如下哪些目录？

问题描述：多选题

A：.\TEMP

B：.\IMAGE

C：.\CASE

D：.\过滤条件

题目 6

X-Ways Forensics 目录中，如果希望保存哈希库，用户可以：

A：自行创建一个目录用于保存哈希库

B：使用默认设置的 HashDB 目录，无需自行创建

C：修改目录名为 MD5 和 SHA

D：将目录修改为绝对路径

题目 7

如果需要切换 X-Ways Forensics 的语言界面为中文或英文，应如何操作？

A：重新安装软件

B：帮助-设置-初始化设置

C：帮助-设置-选择对应语言

D：删除 X-Ways 目录下的 WinHex.cfg 文件

题目 8

如果需要将 X-Ways Forensics 软件复位到初次使用时的缺省状态，应如何操作？

问题描述：多选题

A：重新启动软件

B：帮助-设置-初始化设置

C：删除*.prj 文件

D：删除 X-Ways 目录下的 WinHex.cfg 文件

题目 9

利用 X-Ways Forensics 查看一个 Word（*.doc）文件时，却无法预览到文件的内容，显示为乱码。这可能是什么原因？

问题描述：多选题

A：Word 文件有破损

B：没有安装 Viewer 查看器

C：没有设置好 Viewer 查看器路径

D：Word 文件是加密的

题目 10

在 X-Ways Forensics 目录中存在有 Viewer 目录，但却发现查看器无法正常工作。此时说明 Windows 系统可能缺少必要的运行环境。应该安装什么环境？

A：安装 Visual C++ 2013 Package

B：安装 .Net Framework

C：安装 Java

D：安装 Flash Player

题目 11

X-Ways Forensics 使用的查看器的具体名称为？

A：X-Ways Viewer

B：FTK Viewer

C：Oracle Outside In Viewer

D：Quick View Plus

题目 12

在 64 位 Windows 系统中，X-Ways Forensics 的独立的查看器设置路径可以是？

问题描述：多选题。设定软件目录盘符为 X，目录为：\x-ways 安装目录

A：.\x64\viewer

B：.\viewer

C：.

D：盘符:\x-ways 安装目录\x64\viewer

题目 13

如果希望 X-Ways Forensics 在 USB 磁盘中使用，并用于针对运行状态的计算机实施取证，则：临时文件、案件、镜像等路径应如何设置？

A：使用绝对路径

B：使用相对路径

C：设置路径为空

D：采用默认设置

题目 14

利用 X-Ways Fornsics 创建新案件时，为了保证后期案件报告中的链接图片、文档正常查看，案件名称最好设置为何种形式？

问题描述：多选题

A：默认名称

B：英文-数字

C：英文的日期、案件名称、介质编号

D：便于理解的中文案件名

题目 15

关于设置案件时区的描述，以下哪个是正确的？

A：应该设置为 UTC+8

B：应依据取证分析工作站 Windows 注册表中的正确时区

C：必须设置为 UTC 时间

D：应根据嫌疑人磁盘或镜像文件中操作系统的时区设置来调整 X-WAYS 的案件时区

题目 16

使用 X-Ways Forensics 进行数据分析过程中，采用以下哪种方法可以保存之前的案件分析结果？

问题描述：多选题

A：案件数据-文件-保存案件

B：软件会自动保存案件，无需另行保存

C：直接关闭案件

D：直接退出程序

题目 17

使用 X-Ways Forensics 查看下列哪种格式的文件时，必须使用第三方查看器？

问题描述：多选题

A：SQLite 数据库

B：二进制 Plist 文件

C：xml 格式 Plist 文件

D：TXT 文本文件

题目 18

关于自定义查看器，下列哪些描述是不准确的？

问题描述：多选题

A：第三方查看器，一定要保存在 X-ways Forensics 目录下

B：第三方查看器，一定需要无需安装的绿色软件，这样可以随 X-WAYS 目录一起拷贝到任何位置使用

C：如 WPS OFFICE 不是系统默认的.doc 文件编辑软件，如果希望用 WPS OFFICE 程序查看 doc 文件，应在自定义查看器中设置 WPS Office 的路径

D：第三方查看器，可以使用相对路径来调用可执行程序

1.5.2 X-Ways/ Winhex 软件基础操作

本章节练习配合案例 PART-C-Windows Forensics\C01-CCFC-Windows XP.e01。题目 20，分值 60。时间 30 分钟。 注意：本练习所得答案均在未进行磁盘快照状态下完成。如发现答案不符，请注意答题时磁盘快照状态，并进行更新磁盘快照操作。

题目 1

浏览递归练习：分区 1 下总计有多少个文件：

A：19497+2000+4=21501

B：20+0+4=24

题目 2

浏览递归练习：分区 2 下总计有多少个文件:

A：11+0+4=15

B：326+0+4=330

题目 3

浏览递归练习：分区 1 Windows 目录下，现有文件和和删除文件各有多少？

A：7416，1

B：7417，0

题目 4

浏览递归练习：分区 9 照片目录下，共有多少文件？

A：70

B：74

C：75

D：0

题目 5

浏览递归练习：所有分区（包含 1-9 和分区间隙）中共有多少文件？

A：24084

B：24094

C：25136

D：21299

题目 6

分区 9“元数据”目录下“This is a Microsoft word document with 4 embedded images.dot”文件中，包含几幅嵌入的图片？

问题描述：提示：可以利用 WPS Office 文件打开 DOT 文件查看内容

A：1

B：2

C：3

D：4

题目 7

分区 9“元数据”目录下“This is a Microsoft word document with 4 embedded images.dot”文件，查看 16 进制编码，文件的前 4 个 16 进制数值为：

A：FF D8 FF E0

B：D0 CF 11 E0

C：49 44 33 03

D：25 50 44 46

题目 8

分区 9“元数据”目录下“This is a Microsoft word document with 4 embedded images.dot”文件，查看该文件的创建时间和修改时间，下面描述正确的是？

问题描述：多选题

A：文件创建时间晚于修改时间

B：文件可能在本地被修改过

C：文件可能是本地创建的

D：文件可能是复制到本地的

题目 9

分区 9“元数据”目录下“This is a Microsoft word document with 4 embedded images.dot”文件，查看该文件的详细信息，下面描述正确的是？

问题描述：多选题

A：文件是 Word 97 格式模板

B：文件编辑时间总计 21 分钟

C：文件的作者是 BJBJ

D：文件真正创建时间为 2007/03/05 09:47:00 +8

题目 10

分区 9“元数据”目录下包含文件 DSC01409.JPG，对于该文件，下面描述正确的是？

问题描述：多选题

A：图片中显示文字 KD858N

B：拍摄设备为 Sony DSC-P72

C：拍照时间为 2005/04/06 14:17:30（LT）

D：文件大小为 579299 字节

题目 11

针对分区 9“元数据”目录，下面描述正确的是？

问题描述：多选题

A：目录中的 10 个文件大小总计为 8MB

B：10 个文件是同时拷贝过来的

C：目录是 2011 年 5 月 26 日 17:53:50（UTC+8）在本地创建的

D：有 1 个文件无法预览

题目 12

分区 9“个人文档”目录下文件总容量为？

A：2.1 MB

B：2100 KB

C：2 MB

D：2.2 MB

题目 13

分区 9 “个人文档” 目录下 ”home.doc“ 文件，该文件是：

A：Word 文档

B：加密文件

C：预览后，文件名显示为绿色

D：已破损

题目 14

分区 9 “个人文档” 目录下 ”峰会简版.BAK“ 文件，对该文件描述正确的是：

问题描述：多选题

A：BAK 扩展名，本意为备份文件

B：通过分析文件签名，这个文件的真实类型为 RAR

C：这可能是一个被故意修改了扩展名的文件

D：这个文件的真实类型是 DOC 文件

题目 15

查看分区 5 下的文件，有几个文件是 0 字节的？

A：1

B：3

C：5

D：7

题目 16

查看分区 5 下的所有文件，发现文件名显示为绿色的加密文件有几个？

问题描述：提示：使用用缩略图视图查看所有文件，并参考文件属性列

A：2

B：4

C：6

D：8

题目 17

查看分区 5 下的数据，文件属性同时包含隐含和系统的文件有几个？

问题描述：提示：归档属性：A，隐含属性：H，系统属性：S。 注意区分文件和目录

A：2

B：4

C：5

D：7

题目 18

查看分区 5 下的数据，显示“首簇无法发现”的文件有几个？

问题描述：提示：参考"描述"列

A：1

B：3

C：5

D：7

题目 19

查看分区 5 空余空间，偏移地址 080-084（十六进制）位置，看到的英文字符为？

问题描述：提示： 空余空间容量为 299MB，查看十六进制“文件”视图，十进制地址为 128-132

A：WUHAN

B：CHINA

C：SPRIT

D：FOREN

答案：示例

题目 1

在 64 位 Windows 10 中使用 X-Ways Forensics，应执行以下哪个版本的程序？

A：xwforensics64.exe B：xwforensics.exe C：winhex.exe D：xwforensic64.bat

解题思路：