華中科技大學

“网络安全综合实验（II）”实验指导

题目：电子数据取证

1　电子数据取证

1.1　实验环境及要求

1.1.1　实验平台及说明

实验软件：X-Ways Forensics；

操作系统：windows；

参考资料：

1、X-Ways Forensics 在线帮助

2、课程群文件共享资料

3、其他在线文档资源。

学习通要求：实验过程中，请各位同学按照实验指导手册中红色文字部分（例如：【验证实验 1】）的要求进行实验操作，并在“学习通软件”上回答相关问题。

1.2　实验任务

本次实验主要了解电子数据取证的一些基础的知识原理，能够使用 X-Ways Forensics 工具软件对指定数据镜像进行基本的取证操作。

1.2.1　任务 1　磁盘镜像和证据固定

计算机证据国际组织（International Organization on Computer Evidence，IOCE）1998 年接受八国集团（G8）委托，负责制定国际计算机取证原则，并于 2000 年颁布了计算机取证的 6 条原则：

1、取证过程必须符合规定和标准；

2、获取电子证据前，不得改变证据的原始性；

3、接触原始证据的人员应该得到培训；

4、任何对电子证据的获取、访问、存储或转移的活动必须有完整的记录；

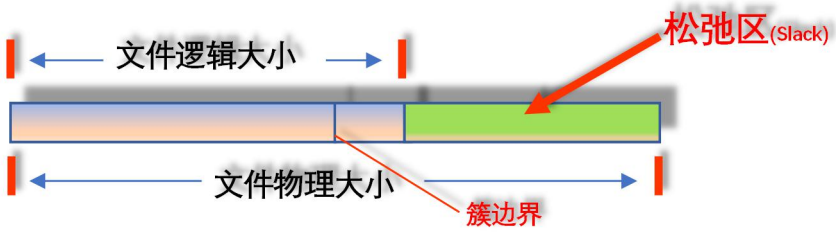
5、 任何人接触电子证据时，必须对其在该证据上的任何操作活动负责；

6、 任何负责获取、访问、存储或转移电子证据的机构必须遵从上述原则。

1. 知识回顾：复制和镜像

对于数据的任何操作，包括取证都会对数据产生影响，因此进行电子数据取证的不会对原始的电子数据进行操作。在进行电子数据取证之前，必须对数据进行备份。对电子数据进行备份通常由两种方式，复制和镜像。

我们知道，磁盘以扇区为单位进行数据的存取；文件系统以块或者簇为单位进行数据的存取，而根据存储空间的大小和系统配置，一个块或者簇往往是一个扇区甚至多个扇区。这就产生了所谓“松弛空间”的问题。



在进行数据复制时，不会将松弛区内的数据拷贝到新的存储空间；进行数据镜像时，对原始数据进行逐比特位进行复制，从而产生与原始数据完全一致的镜像数据，这样就会将松弛区的数据也拷贝到新的存储空间。从电子数据取证的角度，需要用镜像的方式对数据进行备份。

这是为什么呢？

因为松弛区内的数据也可能成为“证据”。

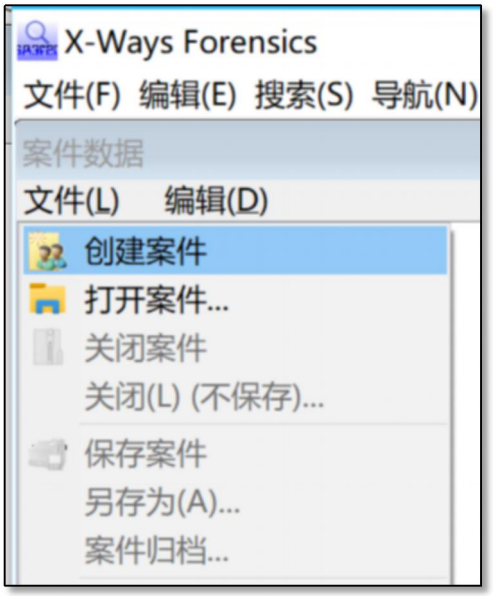
数据镜像时，除了原始的数据外还可以增加不同类型的信息对镜像文件进行增强，例如增加错误校验、数据哈希、不同性能的压缩算法等，这样就演化出来了一系列的新的镜像格式。目前比较典型的有 E01 格式磁盘镜像。

2. 创建案件

在 X-Ways Forensics 中进行电子数据取证，首先需要创建一个案件。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件中。

在案件数据窗口点击***文件***菜单，可以创建一个新的案件、打开现有的案件、关闭当前案件，自动创建案件报告等等各种操作。

选择案件数据窗口，点击***文件-创建案件***，会打开***新案件***对话框。进行相关设置后点击***确定***按钮，成功创建一个新的案件。



创建新案件有几点需要注意的地方。

1、 案件名称要使用英文和数字，否则将来的案例日志和案件报告中无法出现屏幕快照；

2、 案件描述，调查员、机构、地址信息将会用于自动生成案件报告，一般来说需要填写；

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，需要确保当前计算机系统时间设置无误，并且在显示时区中设置正确的时区信息。

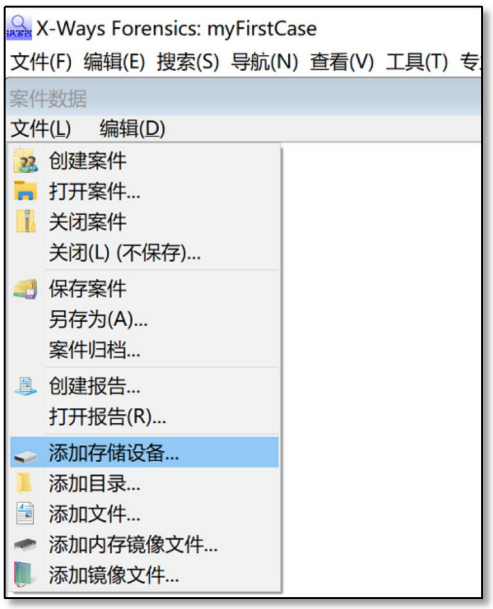
4、 创建案件可以设置口令保护，但这并不是对案件数据进行加密保护，只是设置了一个打开权限。

3. 添加存储设备

创建案件后，既可以添加所需要获取/分析的目标。

选择案件数据窗口，点击***文件-添加存储设备***，会打开***选择磁盘***对话框，选中你需要获取/分析的磁盘。可以将与当前计算机连接的计算机存储介质，例如硬盘、闪存卡、USB 存储设备、CD-ROM、DVD、磁盘镜像文件等等添加为获取/分析的目标。

如果需要获取/分析某个磁盘的完整数据，可以通过两种方式进行：逻辑驱动器或者物理驱动器。



4. 创建磁盘镜像

创建磁盘镜像，需要在磁盘查看方式下，选择主菜单中的***文件-创建磁盘镜像***，打开***创建磁盘镜像***对话框。

鉴于创建磁盘镜像时需要的时间比较长，建议各位同学对 U 盘进行重新分区和格式化，在 U 盘上创建一个较小的分区专门用于实验，这样在后续的操作中需要的时间会小很多，便于提高效率。（对 U 盘重新分区以及格式化的方法，参见附录 B）

在进行相关设置时，需要注意以下几个方面：

（1） 镜像文件格式：可以有两种选择，两种文件格式的特点不一致，执行镜像操作的速度也不太一样，镜像文件的大小也不一样，通常根据案件特点和需要进行选择；

（2） 路径和文件名：可以选择希望保存镜像文件的位置；

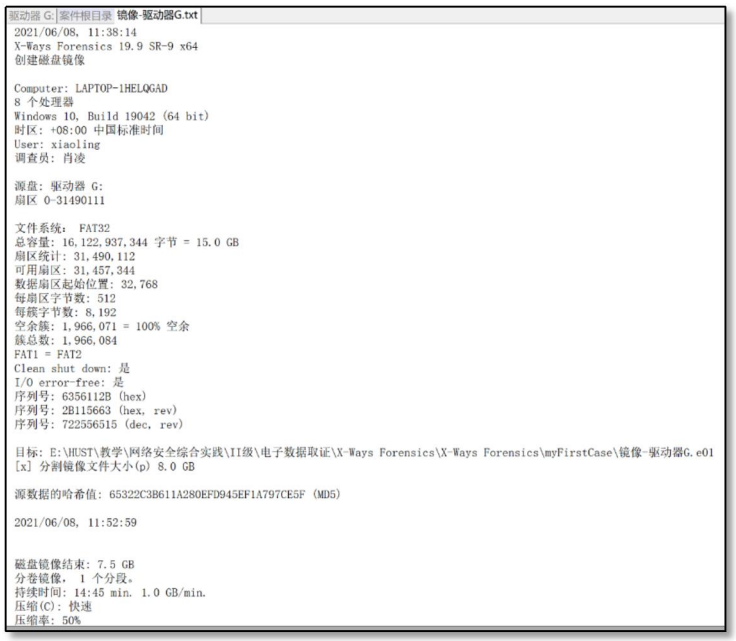
（3） 设定哈希算法级校验：电子数据取证过程中必须保证数据的真实、可靠，必须保证数据的可靠性。因此，对于镜像数据采用哈希值校验的方式来保证数的完整性。在制作镜像时可以设置其采用的具体哈希算法。由于需要逐扇区、逐比特的进行数据复制，因此数据进行磁盘镜像的速度会比较慢。

5. 数据获取报告

在数据镜像完成后，会产生一份数据获取报告。数据获取报告是获取证据的重要依据，里面会包括如获取时间、获取工具、存储介质参数、MD5、SHA 值等信息，需要妥善保存。一般来说，数据获取报告将会随着镜像数据一并刻录到光盘中。

如果是现场取证，应该在数据获取结束后，立即打印此报告，并由调查人员和第三方证

人签字确认。为保持证据链的连续性，对各种信息记录备案，并由调查和人员签字。



【操作实验 1】

在你的计算机上安装 X-Ways forensics 软件，创建一个案件对指定的存储设备制作镜像，并完成下列操作：

1）在 U 盘上创建几个文件。

2）在 X-Ways Forensics 中创建一个以自己的学号命名的案件，并向案件添加刚才的 U 盘存储器。

3）对该 U 盘存储器创建磁盘镜像，在镜像创建完成后将数据获取报告。

1.2.2 任务 2 判断文件类型

计算机中的信息浩如烟海，数据量太大，如何在如此众多的信息中一步一步的缩小调查人员需要关注的数据的范围，往往成为电子数据取证中的关键问题。能够准确地判断文件的类型，并通过文件类型对文件进行过滤，是一个不错的选择。

提到对于文件类型的判断，同学们第一个反应应该是根据文件名中的扩展名对文件类型进行判断，例如：我们都知道的 doc 扩展名表明该文件是一个 word 文档，ppt 扩展名表明该文件是一个 office 的演示文档。

但是，在一些特殊的情况下，这种判断方法却没有效果，甚至会误导取证。例如，有些文件没有扩展名，甚至为了不然别人轻易发现文件，可能故意更改扩展名，在这种情况下必须使用文件签名（File Signature）来对文件类型进行判断。

1．文件签名

大多数文件都具有一些独特的字节，这些字节仅仅在此文件格式中出现，我们称之为文件签名，或者为文件头特殊标识。这个标识可以是几个特殊的字符，也可以是几个十六进制字节。

幸运的是，文件签名与文件类型的对应关系保存在 X-ways Forensics 的文件签名数据库中（其文件名为 File Type Signature*.txt），虽然该数据库中已经包含了很多的文件签名，但是用户也可以编辑 File Type Signature Search.txt 文件加入自定义的文件签名或者更改相关的文件签名的内容。

File Type Signature Search.txt 文件中的数据分为六列：

（1） 文件类型（Description）：对某种类型文件的定义，长度为 19 字节；

（2） 文件扩展名（Extensions）：对所定义的文件类型的典型扩展名；

（3） 文件头签名（Header）：用于识别文件类型的唯一签名特征，可以是 ASCII 码或者十六进制数值。文件头签名最多支持 16 字节。

（4） 偏移量（Offset）：包含文件签名数据第一个字节相对文件第一个字节的偏移地址；

（5） 文件尾签名（Footer）：可选项，用于标记文件的结尾位置，可以是 ASCII 码或者十六进制数值，文件尾签名最多支持 8 个字节；

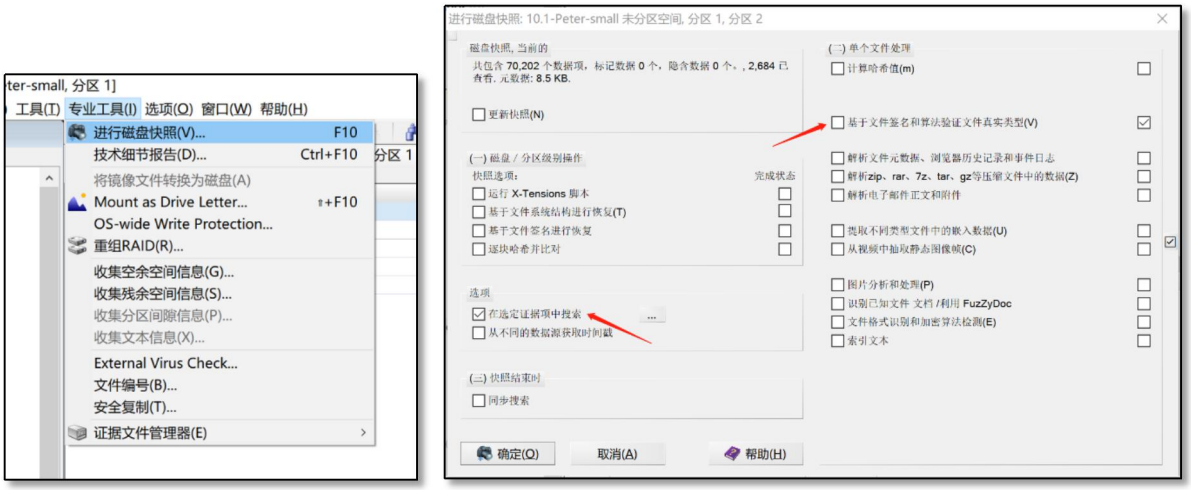
（6） 文件缺省字节数（Default in KB）：定义某类文件的默认大小，以 KB 为单位。在进行特定类型文件的恢复时非常有效。

使用 Excel 软件打开文件类型签名数据库文件，可以看到如下的信息。由于文件签名数据库文件是文本文件，数据之间只用分隔符隔开，按照 Excel 的文件导入向导提示的默认配置即可成功打开查看。

	A	B	C	D	E	F	G	H
1	Description	Extensions	Header	Offset	Footer	Default siz	Flags	
2	*** Pictures							
3	JPEG	JPG;jpeg;jpe;thm;n	\xFF\xD8\xFF[\xC0\xC4\xDB\xDD\xE0-\xE5\xE7\xE8\xEA-\xEE\xFE]	0	~1	2097152/3	e	
4	PNG	png	\x89PNG\x0D\x0A\x1A\x0A	0	~6		e	
5	GIF	gif	GIF8[79]a	0	~3	2097152/33554432		
6	Thumbcac	cmmm	CMMM..\x00\x00.[^\x00]	0	~84	2097152/5	GUb	
7	TIFF/NEF/(	tif;tiff;nef;cr2;dng;p	(\x49\x49\x2A\x00)|(\x4D\x4D\x00\x2A)	0	~5	25165824/268435456		
8	Bitmap	bmp;dib	BM.....\x00.\x00....[\x0C\x28\x38\x40\x6C\x7C]\x00\x00\x00	0	~4			
9	Paint Shop	psp;PsPImage;pfr	(Paint Shop Pro Im)|(~BK\x00)	0	~8	2097152	b	
10	Canon Rav	crw	HEAPCCDR	6		8200000	c	
11	Adobe Ph	PSD;pdd;p3m;p3r;	8BPS\x00\x01\x00\x00\x00\x00\x00\x00	0	~9	10485760	b	
12	Icon	ico	\x00\x00\x01\x00[\x01-\x15]\x00(\x10\x10|\x20\x20|\x30\x30|\x40\x40	0	~7	1024/1782	c	
13	Enhanced	emf	EMF\x00\x00\x01\x00	40	~18		e	
14	Artwork ca	ITC2;itc	\x00\x00\x01\x1Citch	0		802400	c	
15	Corel Phot	cpt	CPT[789]FILE[\x01-\x0F]\x00\x00\x00	0	~97	3145728/3	b	
16	Corel Drav	cdr;cdt	RIFF....CDR[3-G]vrsn\x02\x00\x00\x00	0	~33		bx	
17	Corel Bina	cmx	CMX1	8	~33			
18	Freehand (	fh3	FH31	0			c	
19	Freehand (	fh9;fh8;fh7;fh5	AGD[1-4]	0		600000	c	
20	Google Sk	SKP;skb	\xFF\xFE\xFF\x0ES\x00k\x00e\x00t\x00c\x00h\x00U\x00p\x00\x20\x00	0		4194304	b	
21	SketchUp (	SKP;skb	\xFF\xFE\xFF\x0ES\x00k\x00e\x00t\x00c\x00h\x00U\x00p\x00\x20\x00	0	\x9A\x99\x	4194304	b	
22	AutoCAD [	DWG;123d	AC10[01][0-5]\x00	0		5242880	c	
23	AutoCAD [	dwg;dwt	AC10(18|24|27)\x00	0	~98	5242880		
24	Drawing E	dxf	\x20{0,3}\x30(\x0D\x0A|\x0A|\x0D)SECTION	0	~99			
25	Encapsulat	eps;ai	\xC5\xD0\xD3\xC6	0	~70			
26	JPEG (Base	B64	/9j/4[\x0A\x0Da-zA-Z0-9\+/]{256}	0	~101		b	
27	PNG (Base	B64	iVBORw0[\x0A\x0Da-zA-Z0-9\+/]{256}	0	~101		b	
28	Sony RAW	arw	\x05\x00\x00\x00AW1\x2E	0		16882074	b	
29	Fuji Raw	raf	FUJIFILMCCD-RAW	0		9600000		
30	Minolta Di	mrw	\x00MRM	0		6900000	c	
31	WordPerfe	WPG1;wpg	\xFFWPC...\x00\x01\x16	0		600000	c	
32	The GIMP	xcf	gimp\x20xcf\x20(file|v001|v002|v003)	0	~95	1048576/1	b	
33	LuraWave	JP2;jpx;jpf;j2k	\x00\x00\x00\x0C\x6A\x50\x20\x20\x0D\x0A.....ftypjp2	0		5442880		
34	Xara X dra	XARA;xar;web	XARA\xA3\xA3\x0D	0		1200000		
35	High Dyna	hdr	\#\?RADIANCE\x0A	0		8400000	c	
36	Kodak Cin	cin	\x80\x2A\x5F\xD7\x00\x00\x08\x00\x00\x00\x04\x00\x00\x00\x04\x00	0				
37	Digital Pict	dpx	(SDPX|XPDS)\x00...V#\x2E	0		7635174	c	

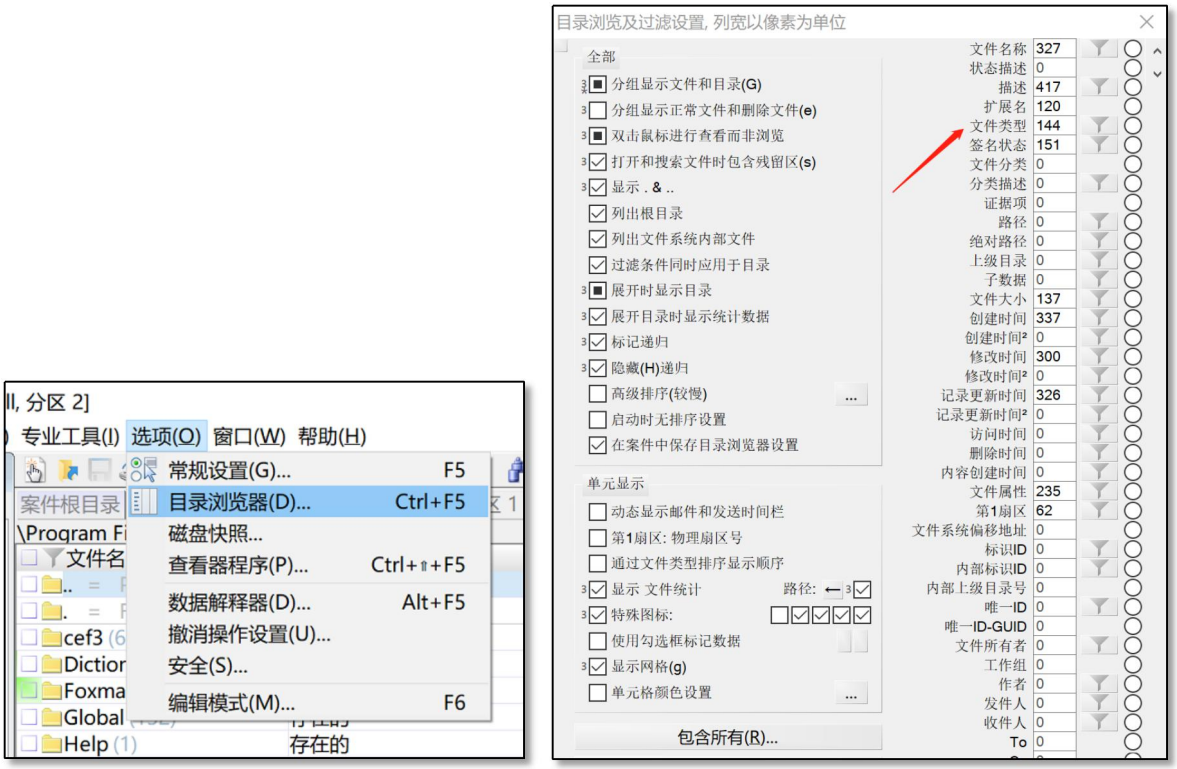
2. 进行磁盘快照

选中要进行快照的分区，点击主菜单中的***专业工具-进行磁盘快照***，打开***进行磁盘快照***对话框。选择***基于文件签名和算法验证文件真实类型***和***在选定证据项中搜索***选项后确定。工具开始对指定的分区进行快照过程。



3. 显示文件类型相关列

点击主菜单中的***选项-目录浏览器***，打开***目录浏览及过滤设置***对话框。将扩展名、文件类型、签名状态列宽度设置为大于 100 像素。在目录浏览窗口中将会多出三列。



文件的初始状态为“未验证”，经过比对文件签名库后，会出现以下的状态：

（1） 签名匹配：文件签名、扩展名和文件签名库匹配；

（2） 不在列表中：文件类型在文件签名库中不存在；

（3） 无关的：文件小于 8 字节；

（4） 签名未校验：扩展名在数据库中被引用，但签名未知；

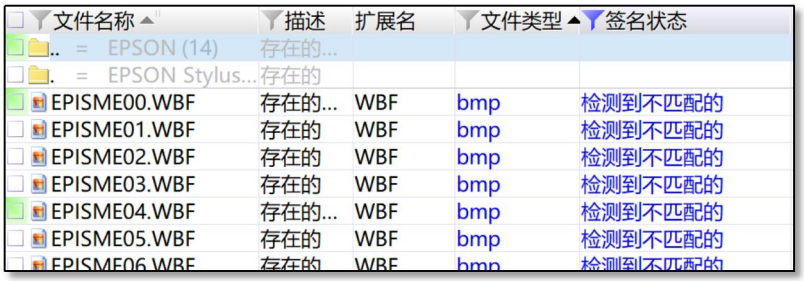
（5） 检测到不匹配的：文件签名在数据库中和某种文件类型匹配，但是扩展名另一种文件类型或者根本没有扩展名；

（6） 未确认：扩展名在数据库中被引用，但是文件签名不匹配。

4. 利用签名状态过滤

在电子数据取证实践中，一些被故意修改文件扩展名的文件往往需要重点关注，这个时候基于签名状态的过滤功能就非常方便了。

点击签名状态列左右的***漏斗***图标，打开***过滤：签名状态***对话框。在***签名***状态栏中选择***检测到不匹配的***后激活该过滤条件，分区中仅显示扩展名与文件类型不符合的文件了。这样有助于调查员将有限的精力集中到重点数据的分析上。



文件名称	描述	扩展名	文件类型	签名状态
.. = EPSON (14)	存在的...			
. = EPSON Stylus...	存在的			
EPISME00.WBF	存在的...	WBF	bmp	检测到不匹配的
EPISME01.WBF	存在的	WBF	bmp	检测到不匹配的
EPISME02.WBF	存在的	WBF	bmp	检测到不匹配的
EPISME03.WBF	存在的	WBF	bmp	检测到不匹配的
EPISME04.WBF	存在的...	WBF	bmp	检测到不匹配的
EPISME05.WBF	存在的	WBF	bmp	检测到不匹配的
EPISME06.WBF	存在的	WBF	bmp	检测到不匹配的

【操作实验 2】

向【操作实验 1】创建的案件中添加镜像文件 fileType.e01，然后执行下列操作。

1）进行相应的操作，使浏览目录中显示扩展名、文件类型、签名状态等列；

2）使用磁盘快照对指定存储器的文件类型进行分析，回答学习通上的问题“综合实践 II-取证-文件类型判断-2-1”；

3）在 X-Ways Forensics 的安装目录下找到 File Type Signature Search.txt 文件，并用 Excel 或者 WPS 的表格工具等能够支持查看和编辑带分隔符的文本文件的软件打开该文件，并在其中增加一行并保存，如下图所示。查看文件的文件类型、扩展名、签名状态等信息的变化；

353	XML fragm	xml	<\?xml ve	0	~15	8196/320(b
354	Comma sep	csv	\x22[\x22	0	~107	1024/104(GS
355	Windows. e	lsps	1SPS\xA6\	8	~106	4096 b
356	Bitlocker	bitlocker	\xFF\xFE\	0	~48	1500
357	BitTorrer	torrent	d(8:annou	0	ee	32768/655360
358	filetest	ftt	adcdefgh	0		
359						
360						

4）使用磁盘快照功能，查看文件的文件类型、扩展名、签名状态等信息的变化。回答

学习通上的问题“综合实践 II-取证-文件类型判断-2-2”和“综合实践 II-取证-文件类型判断-2-3”；

5）从文件“File Type Signature Search.txt”删除刚才添加的那一行数据并保存，再次执行磁盘快照功能，查看文件的文件类型、扩展名、签名状态等信息的变化，回答学习通上的问题“综合实践 II-取证-文件类型判断-2-4”

注意：多次使用文件快照时，在勾选***基于文件签名和算法验证文件真实类型选项***的同时需要勾选***重新校验选项，或者勾选重新进行磁盘快照。***

1.2.3 任务 3 搜索

搜索在面对海量的电子数据时对于取证的重要性是不言而喻的。针对电子数据取证的搜索，需要注意编码、字节序等诸多问题。

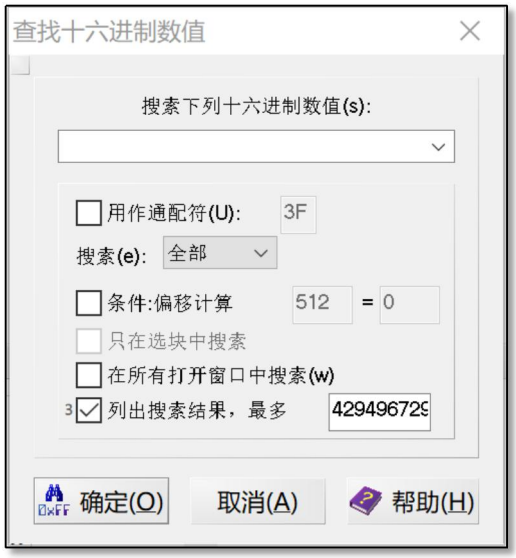
1. 搜索的基本方式

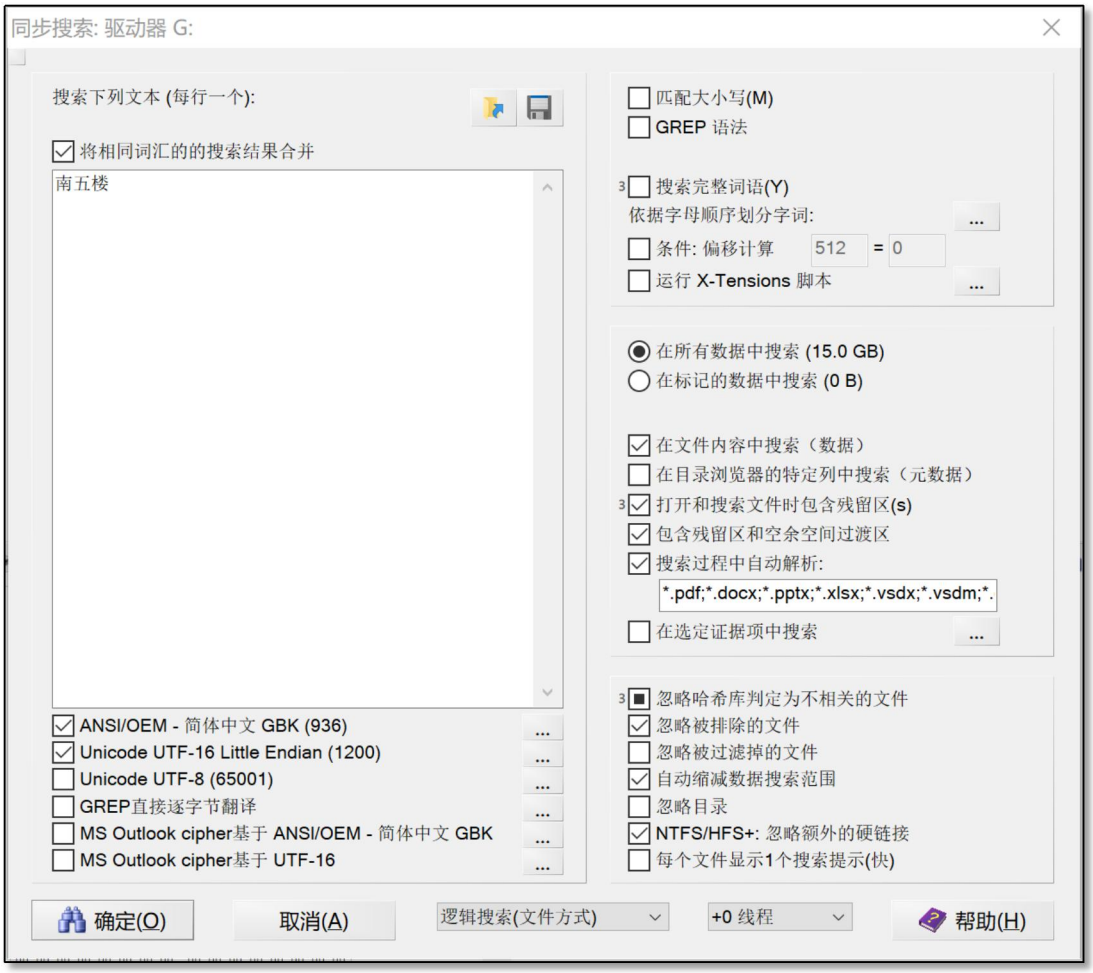
X-Ways Forensics 提供三种搜索方式：搜索文本、搜索十六进制数据和同步搜索。

（1） 搜索文本：在扇区或文件中查找指定的 ASCII 或 UNICODE 字符

（2） 搜索十六进制：在扇区或指定文件中搜索指定的十六进制数值

（3） 同步搜索：允许用户指定一个搜索关键词列表文件，每行设定一个搜索关键词。





2. 搜索的步骤

搜索的目的，是为了缩小调查人员需要调查的数据的范围，因此搜索的步骤也按照这一原则进行。

（1） **选定搜索范围。**是在某个分区中搜索，还是在整个硬盘中搜索；是在多个硬盘中同时搜索，还是在 1 个文件中搜索；是在现有的数据中搜索，还是在空余空间中搜索？为了精确、快速的搜索，需要在搜索前决定搜索时的位置。例如，可以先过滤出需要的文件，做好标记。选择“在选定证据项中搜索”，可以大大提高搜索效率。

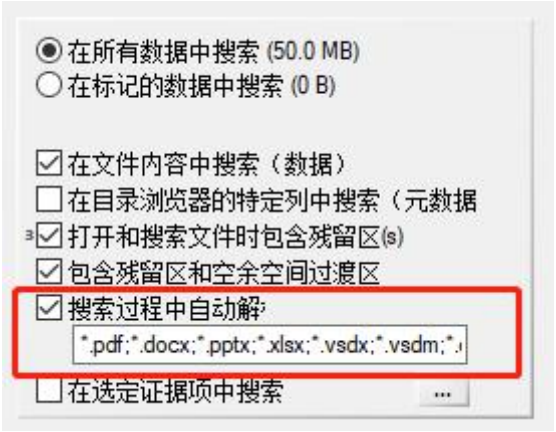
（2） **输入关键词。**可以依据案件的性质将经常使用的关键词积累并保存为关键词库。需要注意的时，设置关键词时需要选择编码方式。在这方面非英文关键词比英文要复杂的多；如果对 pdf 等文件中的数据进行搜索，需要选择“搜索过程中自动解析”才能进行搜索。

（3） **其它设置。**如果只需要发现包含有关键词的文件，可以设置“每个文件显示 1 个

搜索结果”，这样可以大大提高搜索的速度。

3. 格式搜索

在实际的案件侦破或者取证中，往往会对一些符合特定格式的数据进行搜索。例如，需要在分区中搜索包含特定数字的手机号码的文件，这就需要用到格式搜索。在进行格式搜索时，搜索的关键字位 GREP 表达式，同时必须勾选“同步搜索”对话框中的 ***GREP 语法***。同时需要注意，对于选项***搜索过程中自动解码***的文件类型的设置。



例如：138 开头的手机号码，其 GREP 表达式为：[1][3][8][0-9]{8}。

关于 GREP 语法，简单解释如下。

[1] [3458][0-9]{9} 其中：1 代表开头的第一位字符；

[3458] 代表紧跟 1 后面，可以是 3、4、5 或 8 中任一个数字；

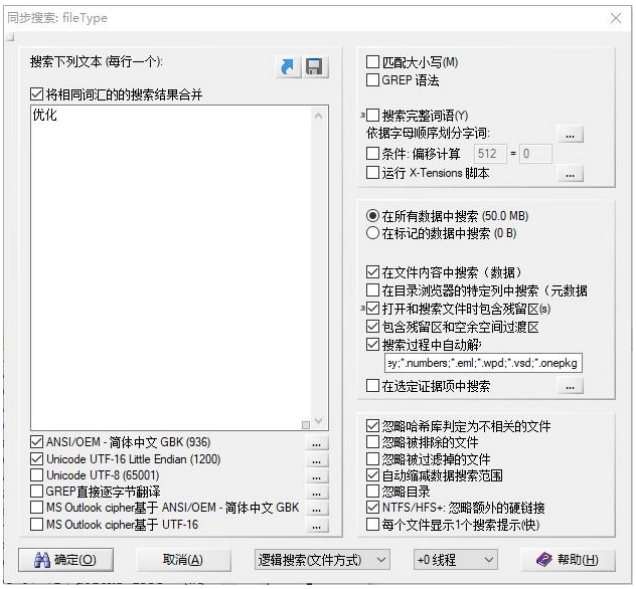
[0-9]代表 0-9 中的任何数字，可以是 0 或者 9；

{9}代表前面 0-9 中的数字，共有 9 位数。

【操作实验 3】

在【操作实验 2】的基础上，执行下列操作。

1）在磁盘镜像中搜索包含“优化”关键字的文件，采用如图所示的同步搜索参数配置，回答学习通问题“综合实践 II-取证-搜索-3-1”、“综合实践 II-取证-搜索-3-2”和“综合实践 II-取证-搜索-3-3”；



2） 在磁盘镜像中搜索包含以“189”开头的手机号码的文件，回答学习通问题“综合实践 II-取证-搜索-3-4”和“综合实践 II-取证-搜索-3-5”。

附录 A

X-Ways Forensics 软件介绍和安装

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。

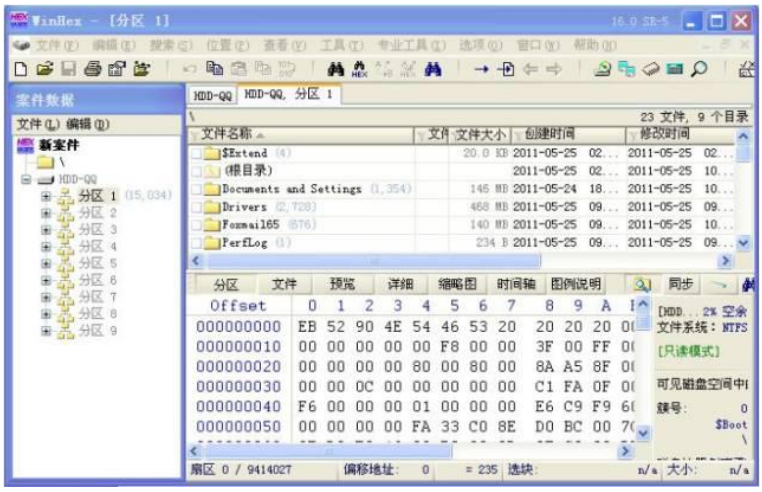


图 2 Winhex 界面

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。

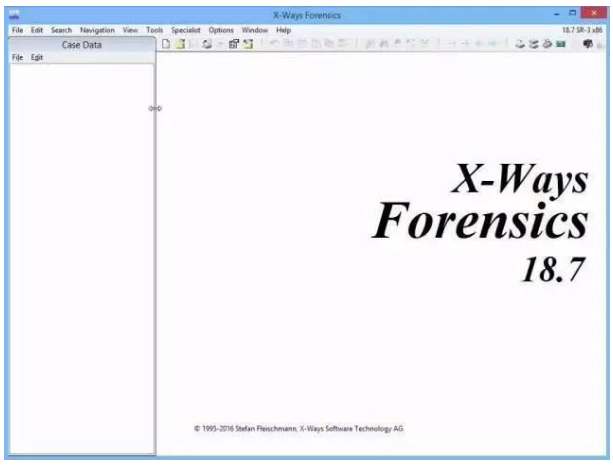


图 3 X-Ways Forensics 启动界面

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

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，直接使用。

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。**

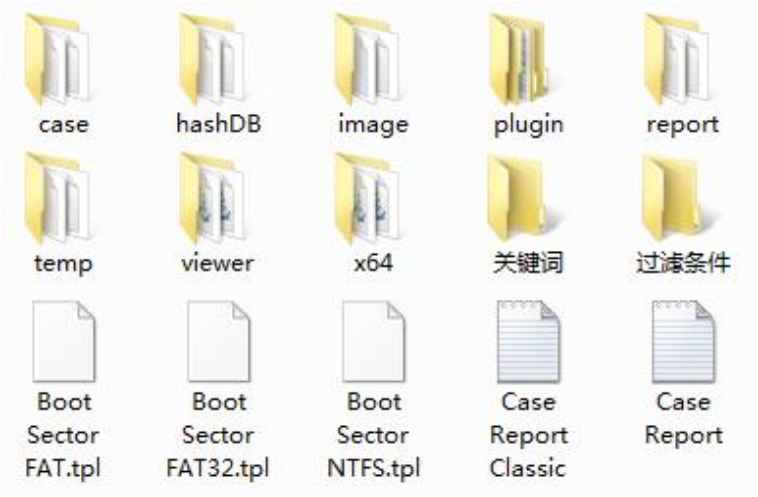


图 6 创建案例、镜像、临时目录

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。

提示：如果 X-Ways 或 Winhex 启动直接闪退，无法进入软件界面，找到程序目录下的 WINHEX.CFG 文件，将其删除，重新运行软件就可以正常运行。不过，启动后，软件被彻底复位，需要重新进行选项设置。具体方式参下述操作。

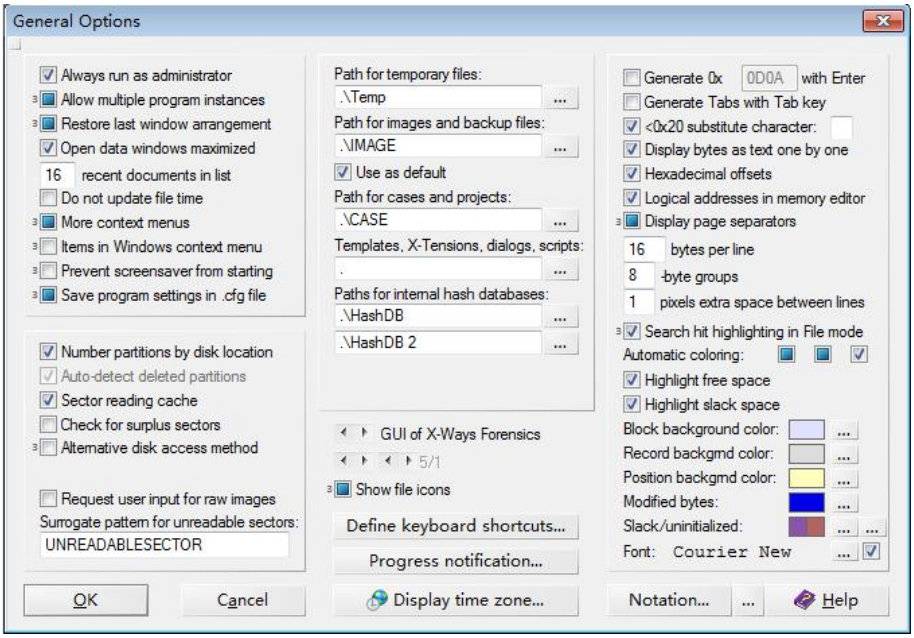


图 7 常规配置界面

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”。

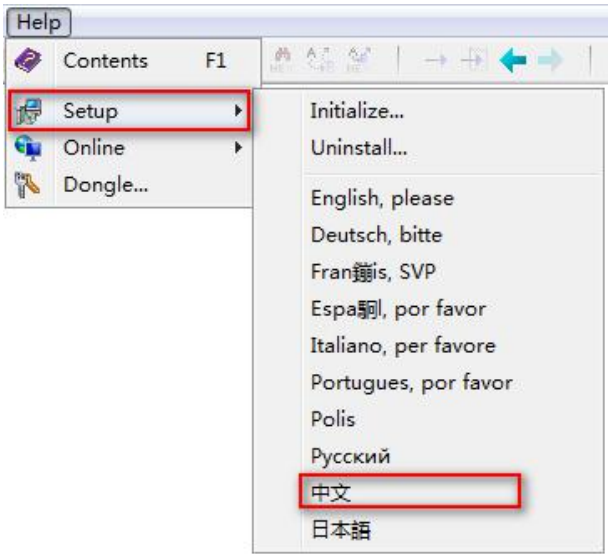


图 8 修改界面语言

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 9 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。

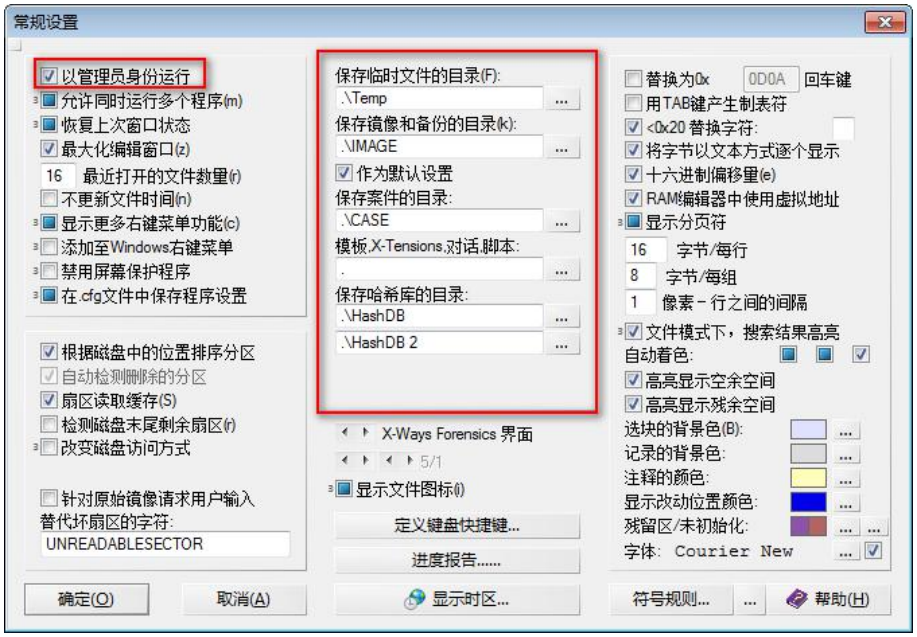


图 10 常规设置内容

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 10。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。

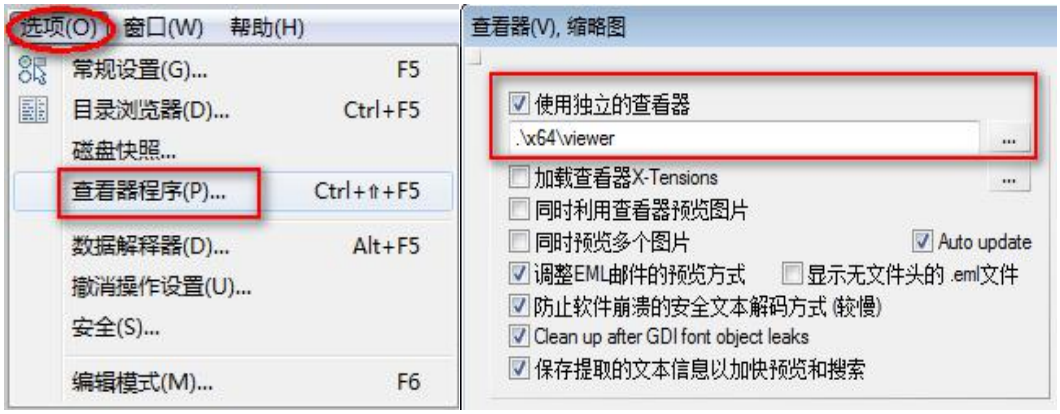


图 11　查看器设置

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 12 查看“关于”

附录 B

X-Ways Forensics 基本操作

1 X-Ways Forensics 界面布局

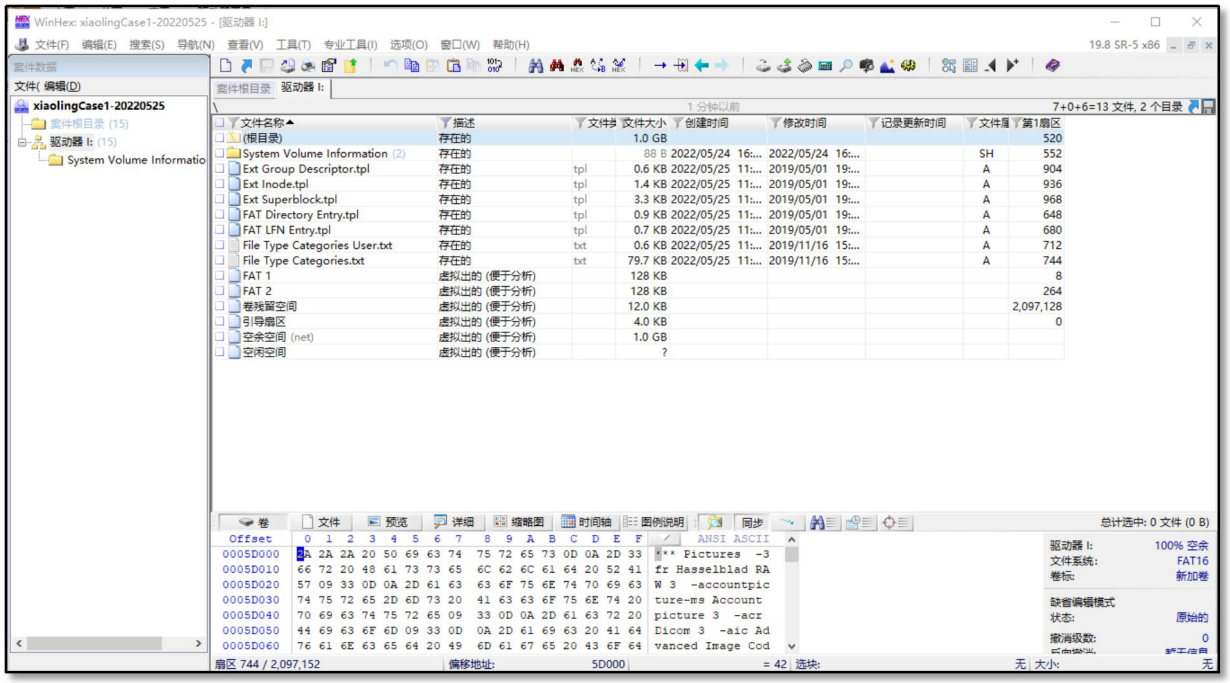


图 1 主界面布局

2 视图模式

2.1 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。

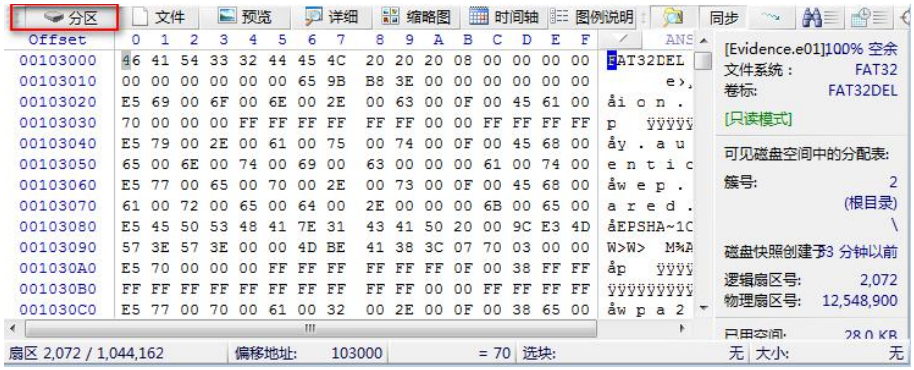


图 2 分区模式

2.2 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。

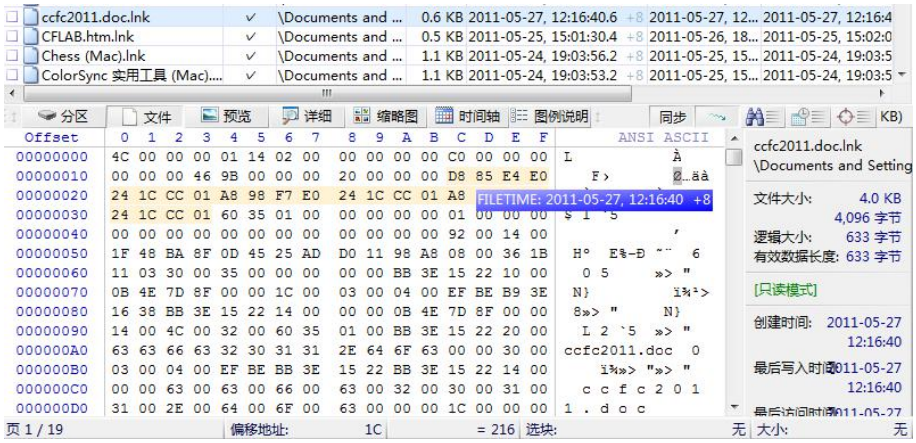


图 3 文件模式

2.3 预览模式

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

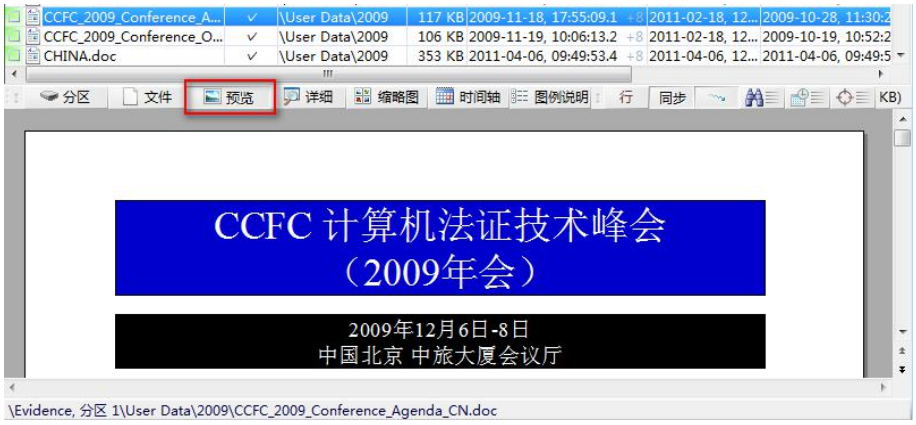


图 4 预览模式

2.4 缩略图模式

以缩略图方式查看图片或视频抽帧图片。图中可以发现 X-Ways Forensics 作者 Stefan。

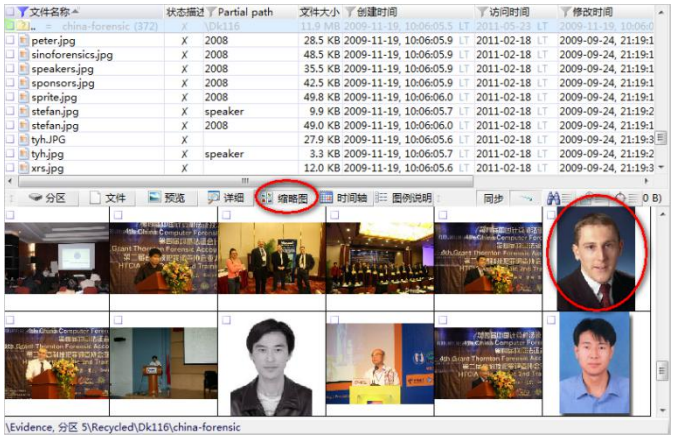


图 5 缩略图模式

2.5 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。

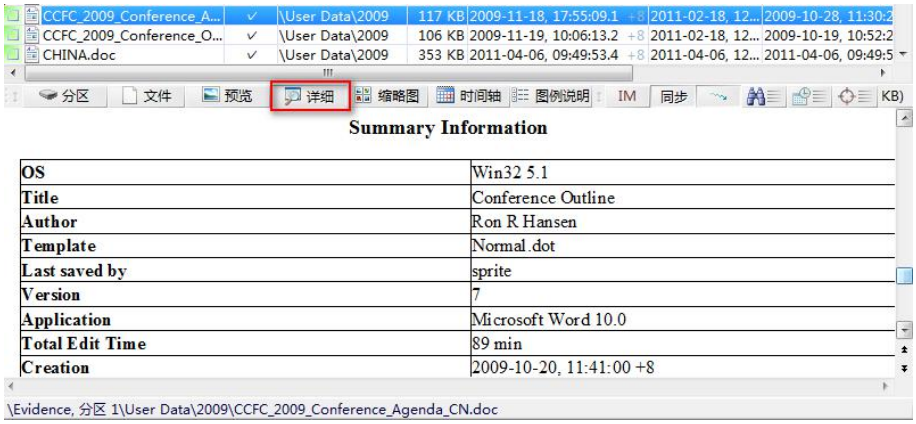


图 6 详细模式

2.7 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。

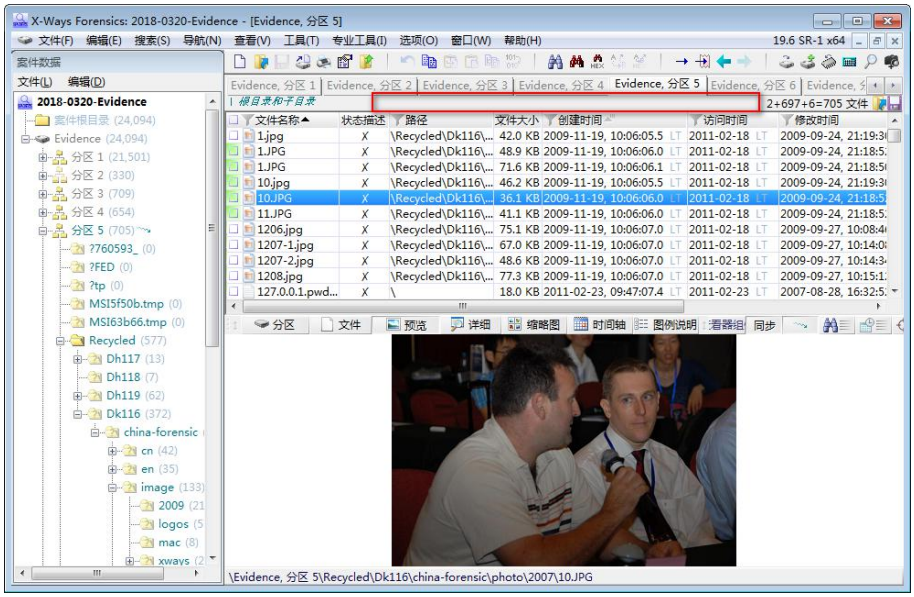


图 7 点击 TAB 信息栏 ，设置列

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 8　设置目录列表的显示栏

3 磁盘快照

什么是磁盘快照？

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 Forensics 提供了证据预处理功能，称为磁盘快照。

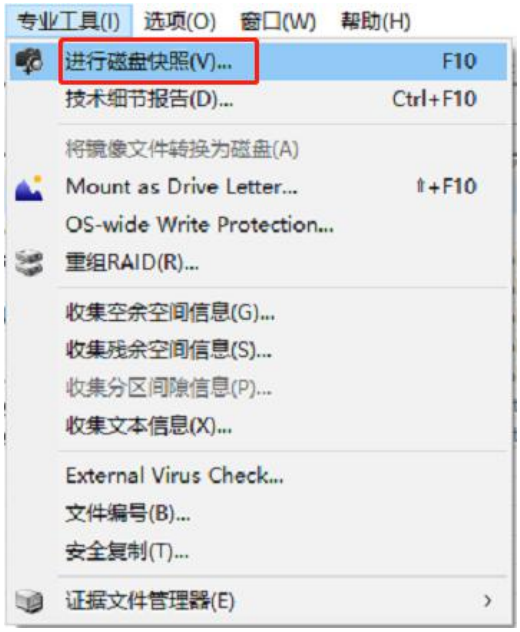


图 9　调用磁盘快照

磁盘快照功能包括：文件恢复、文件签名哈希、哈希校验、复合型文件提取、电子邮件内容提取等等。

更新快照：是重新进行磁盘快照，将之前的所有解析结果全部清除。如果经过很长时间解析了磁盘的所有数据之后，一定要慎重选择该功能。否则，你又要等待很长时间了。

在选定的证据中搜索：选择进行指定操作的证据项。

应用于所有文件和应用于所有标记的文件：如果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：可以提取所有的“ppt”中的图片，则可以先标记所有的“ppt”文件，在进行操作。

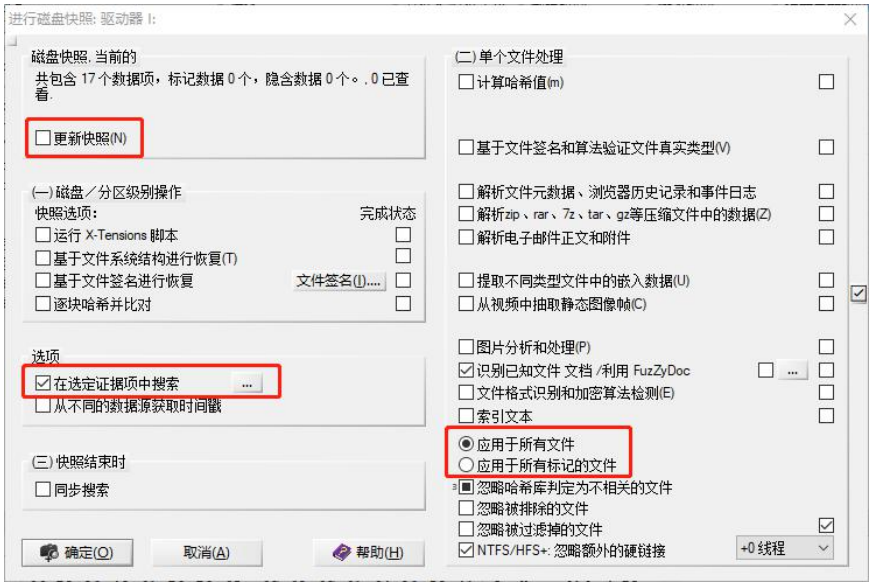


图 10　磁盘快照

附录 C

为 U 盘创建分区

因为磁盘镜像需要对磁盘的所有数据进行扫描，因此速度较慢。可以在 U 盘上创建一个较小的分区作为实验对象，实验仅对该分区进行操作，以提高实验效率。

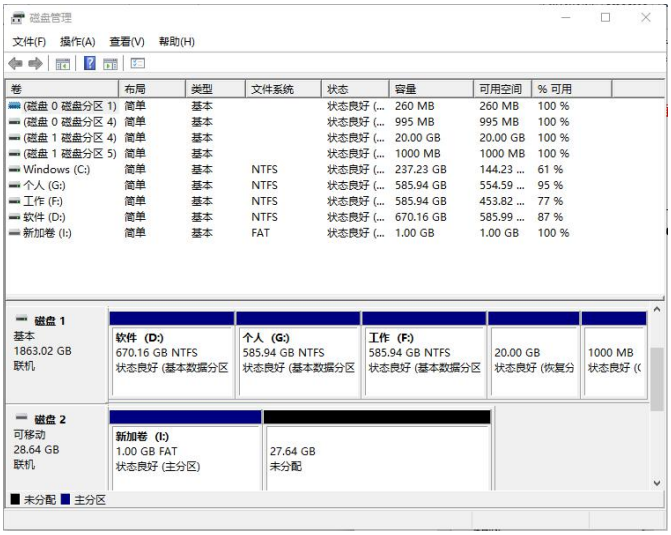
能够在 U 盘上创建分区的工具有很多，指导手册仅以 Win10 作为说明。使用其他工具对 U 盘创建分区，已相应工具的说明为准。

注意：创建分区可能删除 U 盘上所有的数据，请各位同学一定注意在操作前备份数据。

第一步：备份 U 盘原有数据

第二步：将需要创建分区的 U 盘插入计算机 USB 接口，打开 Windows 系统的磁盘管理器工具。

鼠标右键点击开始菜单，选择***磁盘管理（K）***，打开磁盘管理对话框。

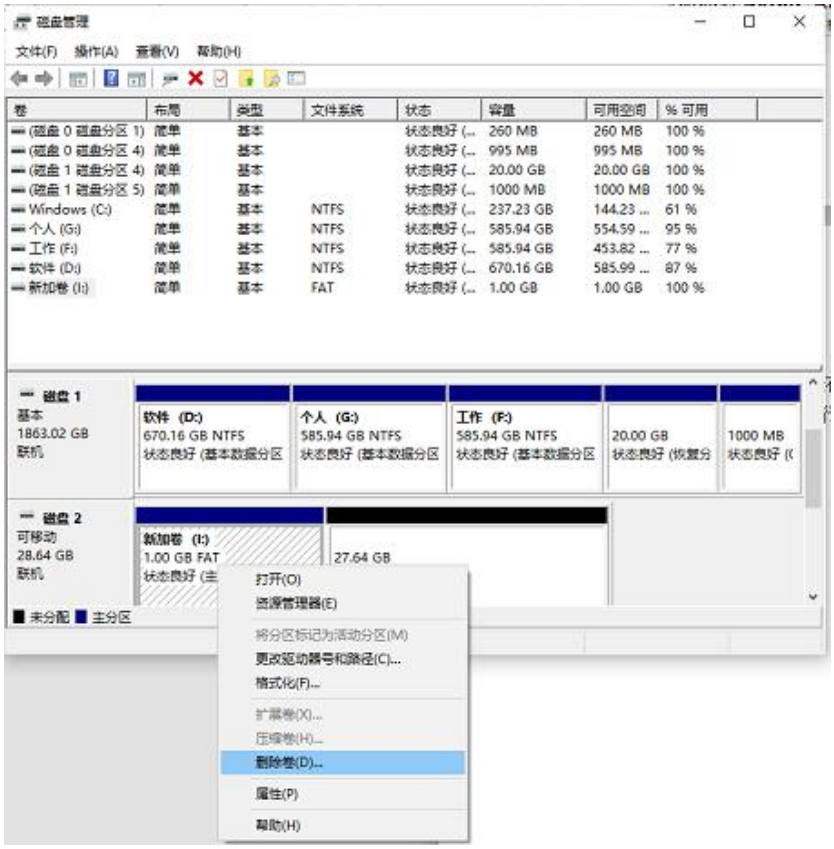


对于已经使用过的 U 盘，通常已经有了相应的分区结构。要创建新的分区，需要删除原有的分区，或者在“未分配”空间中进行。

第三步：删除原有分区

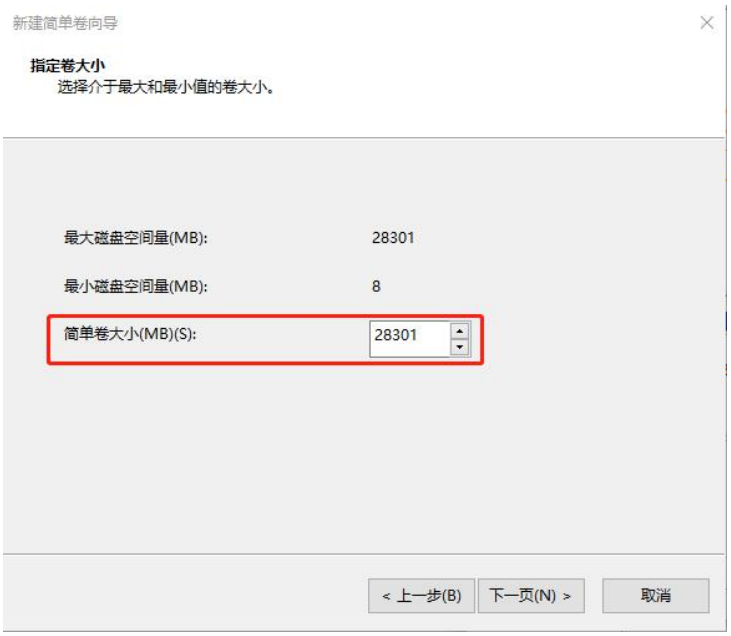
鼠标右键选中要删除的分区，点击***删除卷***。

注意：“删除卷”操作将删除改卷上所有的数据，各位同学一定注意在操作前备份数据。



第四步：创建新分区。

鼠标右键选中“未分配”空间，点击***新建简单卷***。最后会弹出创建分区的向导对话框。点击下一步，在“制定卷大小”对话框中选择需要创建的新卷的大小。



第五步：循环操作，为所有未分配空间创建分区。

未创建分区的空间是不能使用的，为了充分利用 U 盘空间，循环上述操作，为 U 盘中其他未分配的空间创建分区。