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】）的要求截图和回答问题，并将问题的答案提交至“学习通软件”。

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；

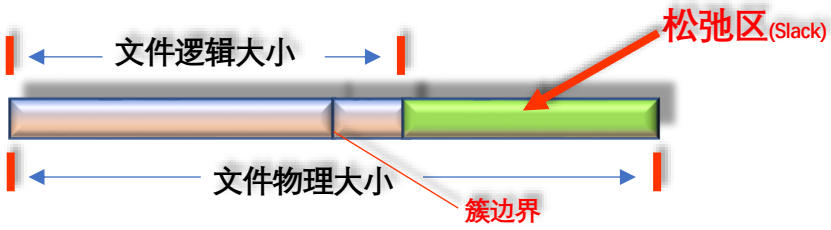
5、任何人接触电子证据时，必须对其在该证据上的任何操作活动负责；

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。

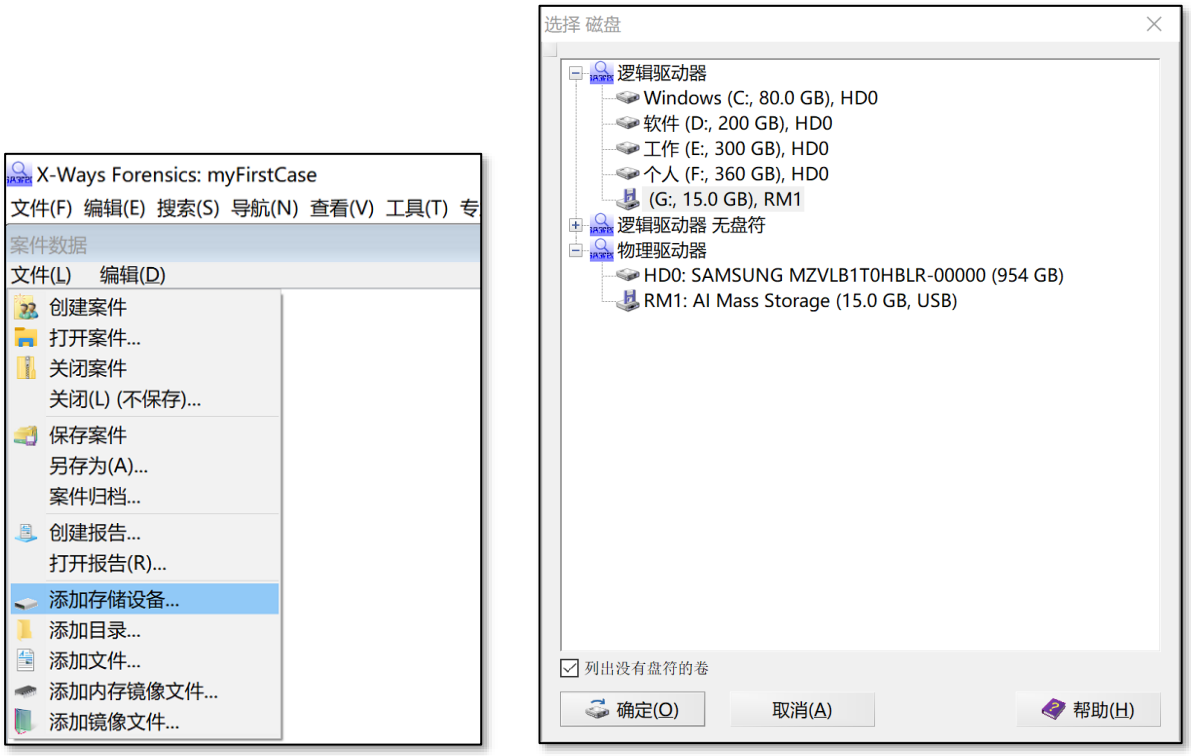
4、创建案件可以设置口令保护，但这并不是对案件数据进行加密保护，只是设置了一个打开权限。

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。

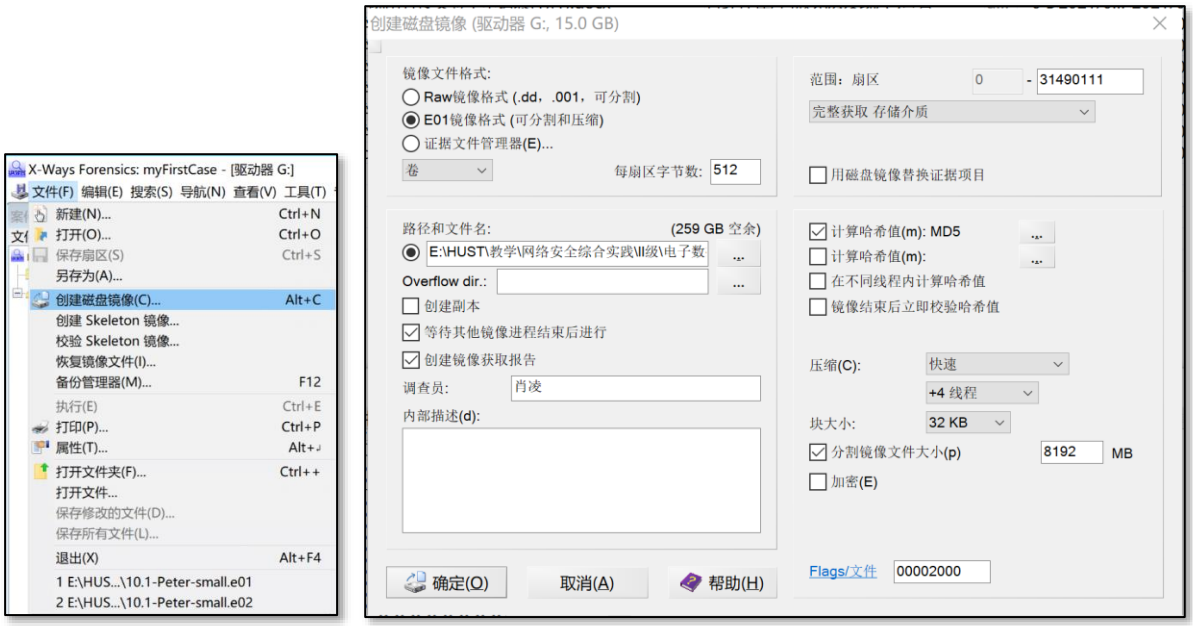
选择案件数据窗口，点击***文件-添加存储设备***，会打开***选择磁盘***对话框，选中你需要获取/分析的磁盘。可以将与当前计算机连接的计算机存储介质，例如硬盘、闪存卡、USB 存储设备、CD-ROM、DVD、磁盘镜像文件等等添加为获取/分析的目标。

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。



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；

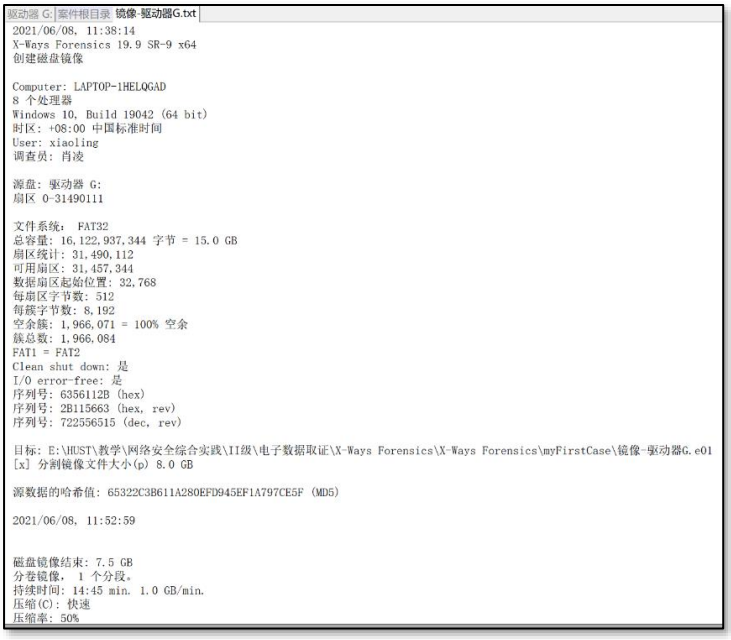
（2） 路径和文件名：可以选择希望保存镜像文件的位置；

（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。


驱动器 G | 案件根目录 镜像-驱动器G.txt

```
2021/06/08, 11:38:14
X-Ways Forensics 19.9 SR-9 x64
创建磁盘镜像

Computer: LAPTOP-1HELQGAD
8 个处理器
Windows 10, Build 19042 (64 bit)
时区: +08:00 中国标准时间
User: xiaoling
调查员: 肖凌

源盘: 驱动器 G:
扇区 0-31490111

文件系统: FAT32
总容量: 16,122,937,344 字节 = 15.0 GB
扇区统计: 31,490,112
可用扇区: 31,457,344
数据扇区起始位置: 32,768
每扇区字节数: 512
每簇字节数: 8,192
空余簇: 1,966,071 = 100% 空余
簇总数: 1,966,084
FAT1 = FAT2
Clean shut down: 是
I/O error-free: 是
序列号: 6356112B (hex)
序列号: 2B115663 (hex, rev)
序列号: 722556515 (dec, rev)

目标: E:\HUST\教学\网络安全综合实践\II级\电子数据取证\X-Ways Forensics\X-Ways Forensics\myFirstCase\镜像-驱动器G.e01
[x] 分割镜像文件大小(p) 8.0 GB

源数据的哈希值: 65322C3B611A280EFD945EF1A797CE5F (MD5)

2021/06/08, 11:52:59


磁盘镜像结束: 7.5 GB
分卷镜像, 1 个分段。
持续时间: 14:45 min. 1.0 GB/min.
压缩(C): 快速
压缩率: 50%
```

【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）在自己的 U 盘上创建一个文本文件，该文件开头的内容为“adcdefgh”，其余内容随意且长度大于 8 个字节。将该文件的文件名为自己的姓名，扩展名命名为自己的学号。

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，提交截图提交到学习通。

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截图提交到学习通。

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；

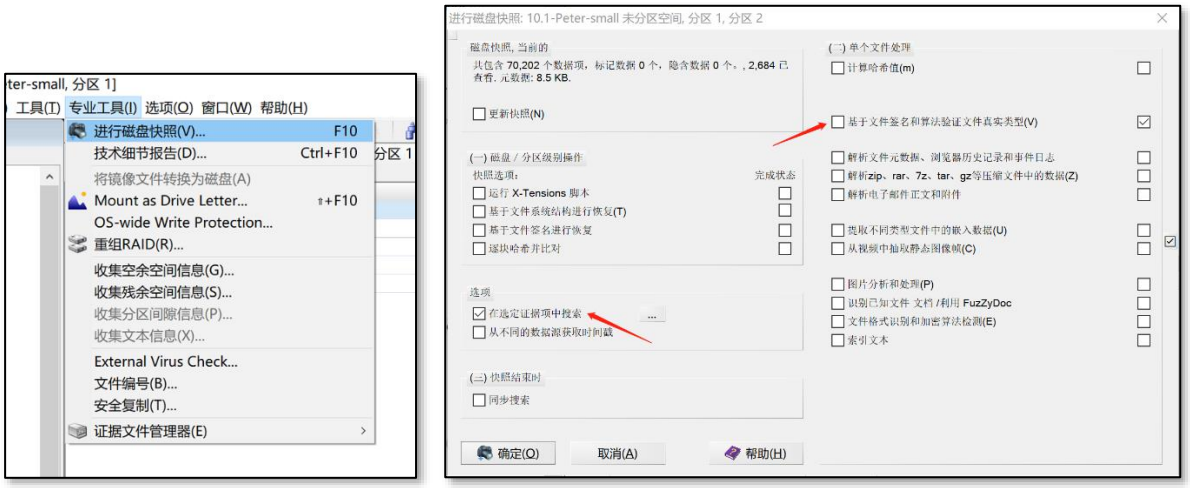
（6） 文件缺省字节数（Default in KB）：定义某类文件的默认大小，以 KB 为单位。在进行特定类型文件的恢复时非常有效。

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 的文件导入想到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;r	(\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\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 Binai	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	

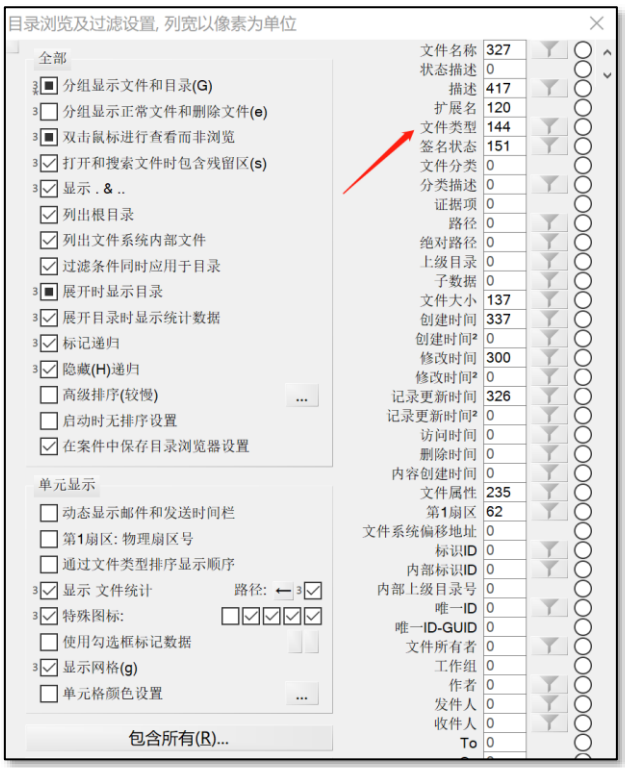
2. 进行磁盘快照

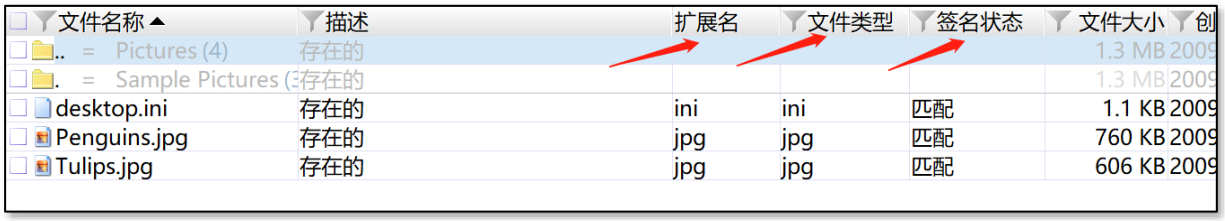
选中要进行快照的分区，点击主菜单中的***专业工具-进行磁盘快照***，打开***进行磁盘快照***对话框。选择***基于文件签名和算法验证文件真实类型***和***在选定证据项中搜索***选项后确定。工具开始对指定的分区进行快照过程。



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；

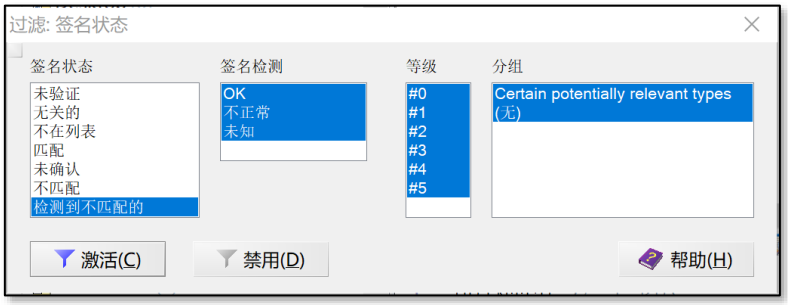
（5） 检测到不匹配的：文件签名在数据库中和某种文件类型匹配，但是扩展名另一种文件类型或者根本没有扩展名；

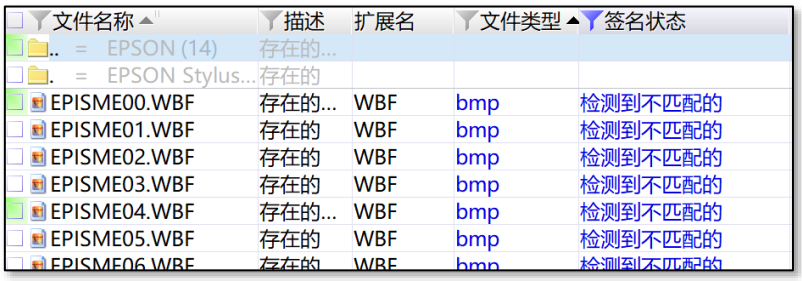
（6） 未确认：扩展名在数据库中被引用，但是文件签名不匹配。

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。





【操作实验 2】

在【操作实验 1】中创建的案件中去除添加的存储器，然后向案件添加【操作实验 1】中创建的镜像文件，执行下列操作。

1）在 X-Ways Forensics 的安装目录下找到 File Type Signature Search.txt 文件，并用 Excel 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，并在其中增加一种以自己学号为文件类型和扩展名，以“abcdefgh”为文件特征的文件类型签名，提供截图到学习通；

2）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，提供截图到学习通；

3）使用磁盘快照对指定存储器的文件类型进行分析，查看刚才在 U 盘中以自己姓名为文件名的文件的文件类型、扩展名、签名状态等信息，提供截图到学习通；

4）修改文件签名数据库中的文件头签名内容，再次使用文件快照对指定存储器进行分析，查看 3 中文件的文件类型、扩展名、签名状态等信息的变化，提供截图到学习通；

5）删除添加到文件签名数据库中新的文件类型签名，再次使用文件快照对指定存储器进行分析，查看 3 中文件的文件类型、扩展名、签名状态等信息的变化，提供截图到学习通。

注意：再次使用文件快照时，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。***

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。

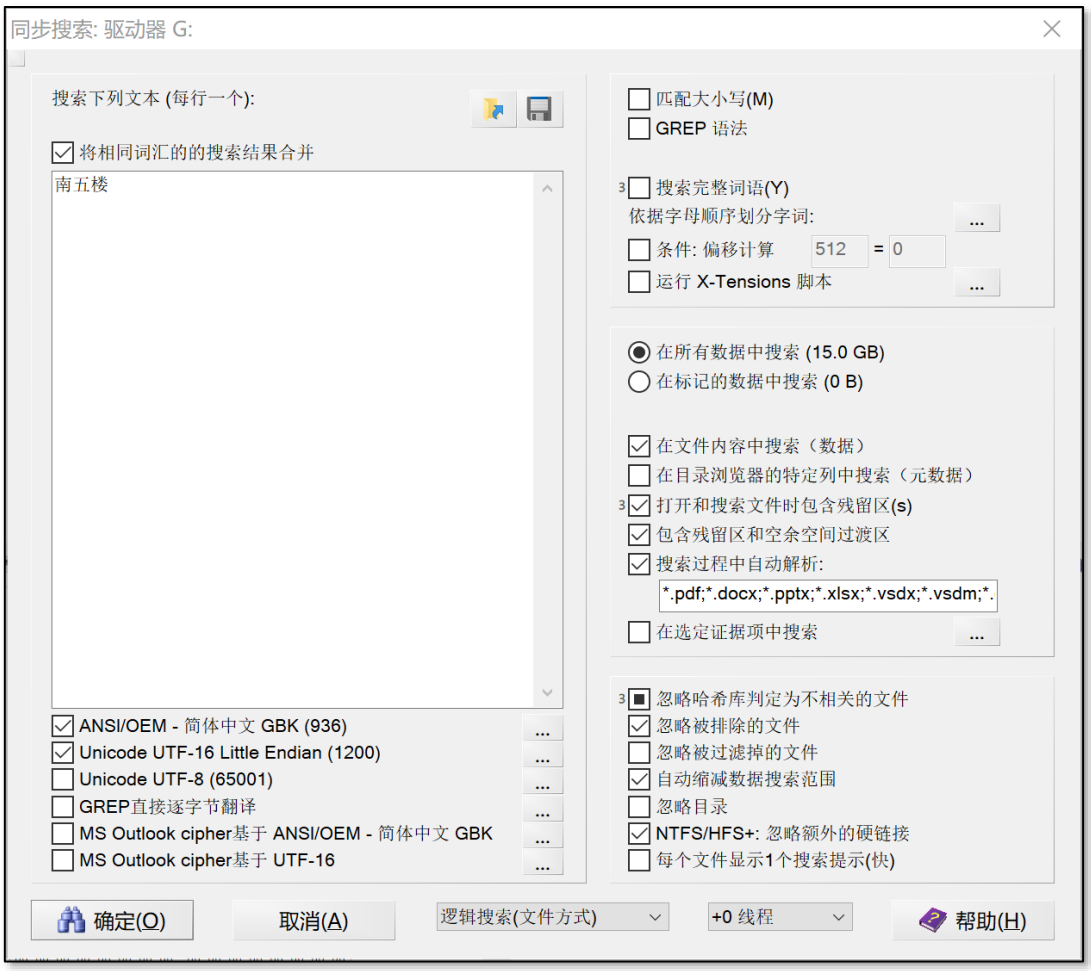
1. 搜索的基本方式

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；实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在编码方式。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。

【操作实验 3】

在【操作实验 1】中创建的案件中去除添加的镜像文件，然后向案件添加自己电脑的逻辑分区 C，执行下列操作。

1）在电脑的逻辑分区中搜索包含“华中科技大学”的 word 文档，你准备如何搜索呢？请将你的搜索设置窗口和搜索结果窗口截图并上传至学习通。（若你的电脑中没有符合条件的文件，请创建一个符合条件的文件

2）互联网残留的数据中，往往包含大量有价值的残留信息。例如，使用浏览器利用 Web 方式登录邮箱，收发邮件有时会在本地残留一些曾经打开过的网页邮件。如何能够方便的发现发现这些痕迹呢？请回答你的思路并将操作过程截图上传。（若你的电脑中没有进行过相关操作，请进行一次这样的邮件操作后在进行发现）

3）在实际的案件侦破或这取证中，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 GREP 语法了。如何在你的逻辑分区中搜索包含以“189”开头的手机号码的文件呢？请将你的搜索条件设置和搜索结果截图上传至学习通。（如果没有这样的文件，请创建一个）