电子数据取证实验

网络犯罪与网络安全

方便

快捷

高效

网络犯罪

电子数据是什么？

1991年第一届国际计算机调查专家会议（IACIS,USA）首次对计算机证据的定义

可以识别、恢复、提取、保存并形成报告使之成为法律证据的电子形式存储的信息

2013版《中华人民共和国刑事诉讼法》首次将“电子数据”列入证据类型

电子数据是什么？

第五章 证据	第五章 证据
第四十二条证明案件真实情况的一切事实，都是证据。 证据有下列七种： （一）物证、书证； （二）证人证言； （三）被害人陈述； （四）犯罪嫌疑人、被告人供述和辩解； （五）鉴定结论； （六）勘验、检查笔录； （七）视听资料。 以上证据必须经过查证属实，才能作为定案的根据。	**第四十八条** 可以用于证明案件事实的材料，都是证据。 证据包括： （一）物证； （二）书证； （三）证人证言； （四）被害人陈述； （五）犯罪嫌疑人、被告人供述和辩解； **（六）鉴定意见；** （七）勘验、检查、辨认、侦查实验等笔录； （八）视听资料、**电子数据。** 证据必须经过查证属实，才能作为定案的根据。

内容简介
INTRODUCTION

1 任务1 磁盘镜像和证据固定

2 任务2 判断文件类型

3 任务3 文件搜索

电子数据取证

International Organization on Computer Evidence，计算机取证国际组织

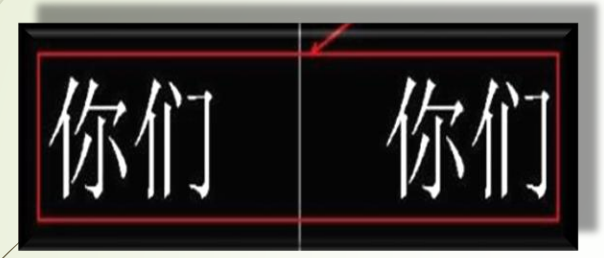
IOCE于2000年提出了电子数据取证的6条原则：

- 取证过程必须符合规定和标准；
- 获取电子证据前，不得改变证据的原始性；
- 接触原始证据的人员应该得到培训；
- 任何对电子证据的操作活动必须有完整的记录；
- 任何人必须对其在该证据上的任何操作活动负责；
- 任何负责操作电子证据的机构必须遵从上述原则

数据备份

不能再原始数据上进行操作！

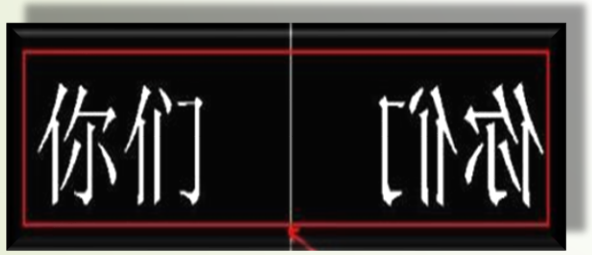
复制和镜像



复制

对象：文件

结果：数据相同，空间不同



镜像

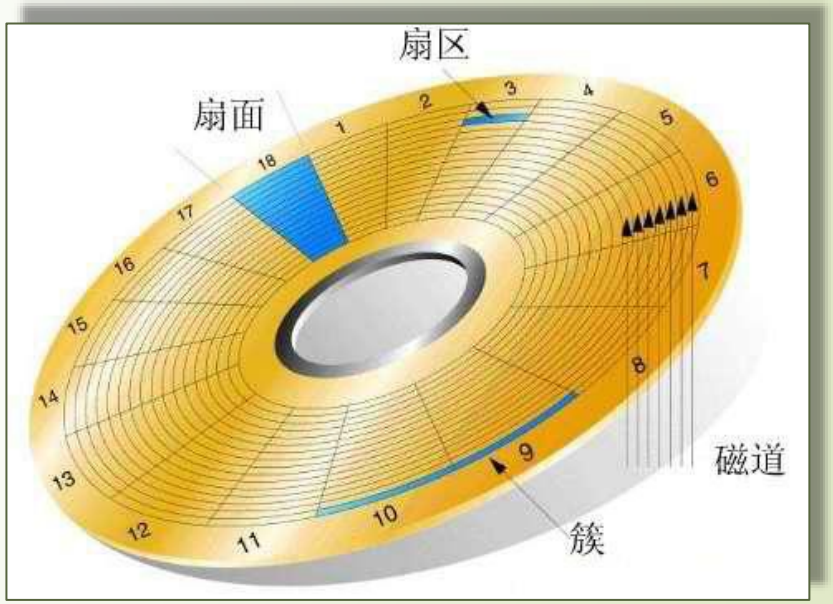
对象：硬盘

结果：数据相同，空间相同

复制和镜像

机械硬盘

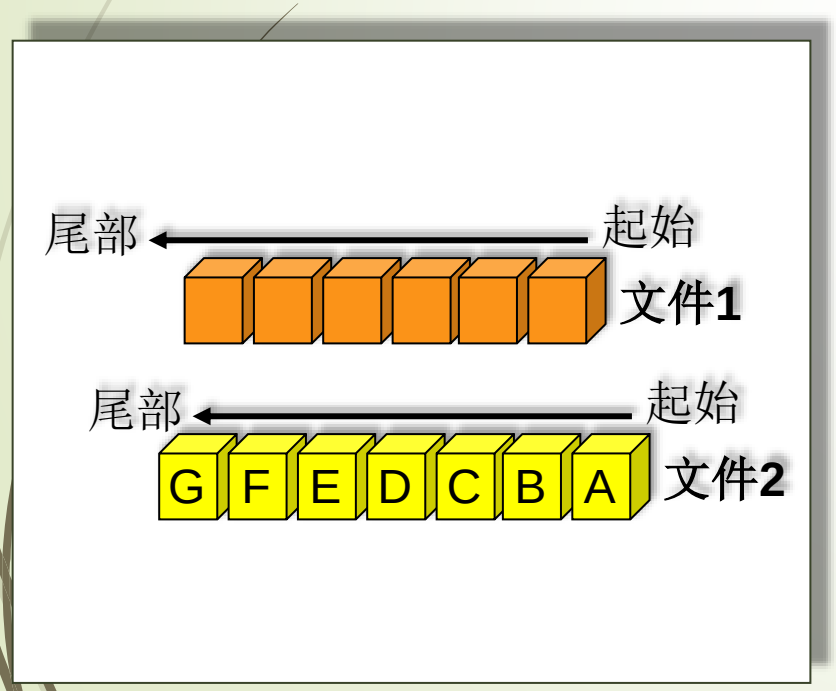
- 将磁道划分成若干段弧
- 每段弧成为一个**扇区**
- 扇区是硬盘的**最小**存储单元
- 每个扇区存储**512字节**数据
- 同一径向上扇区组成**扇面**

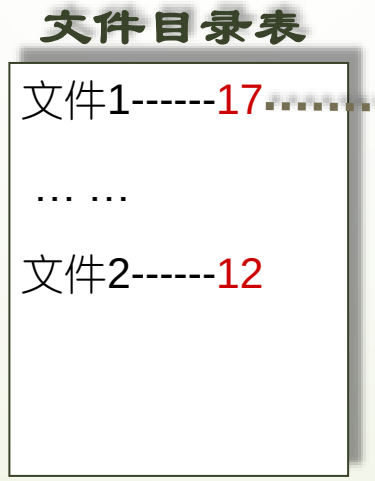


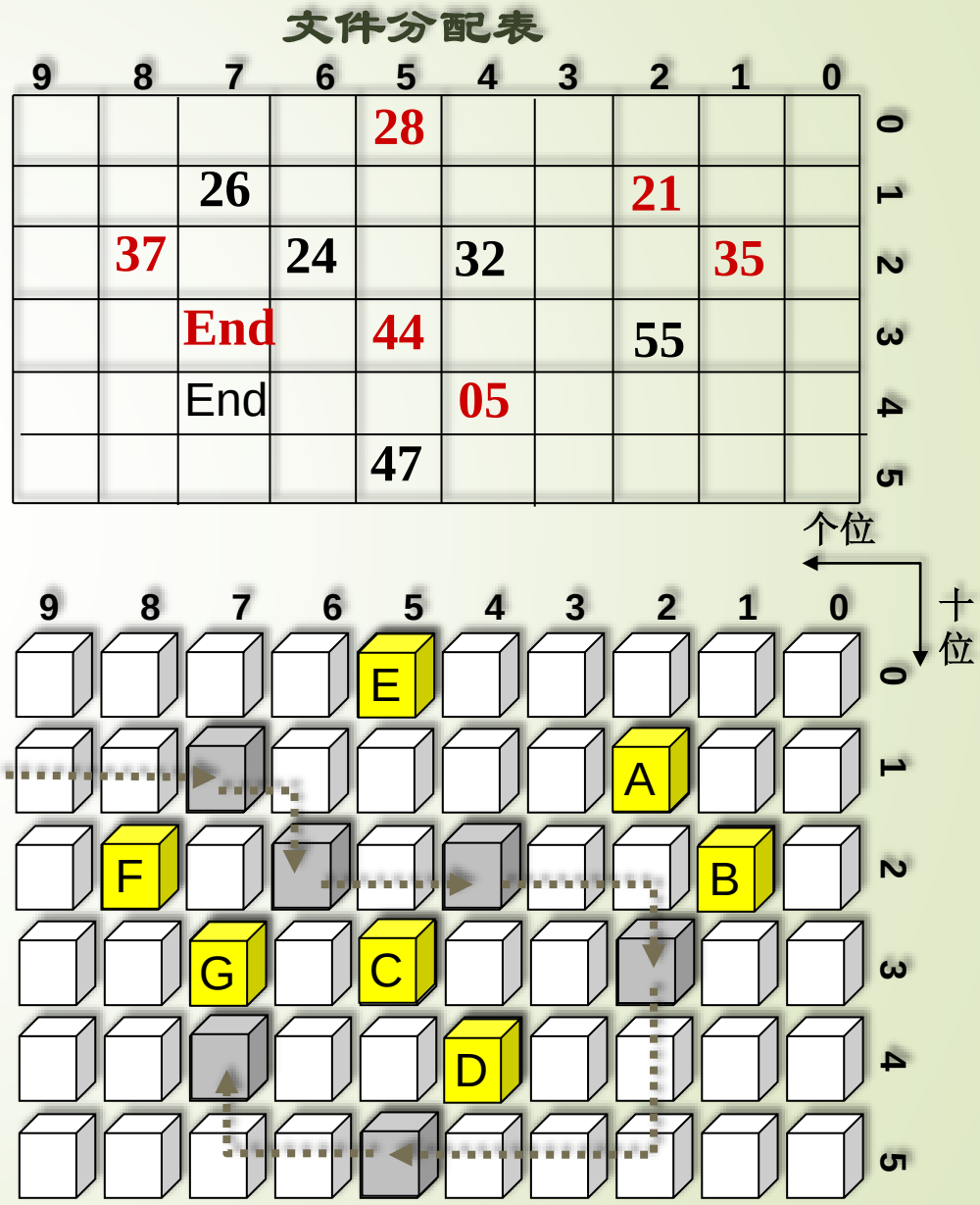
复制和镜像

FAT文件系统

链式存储结构

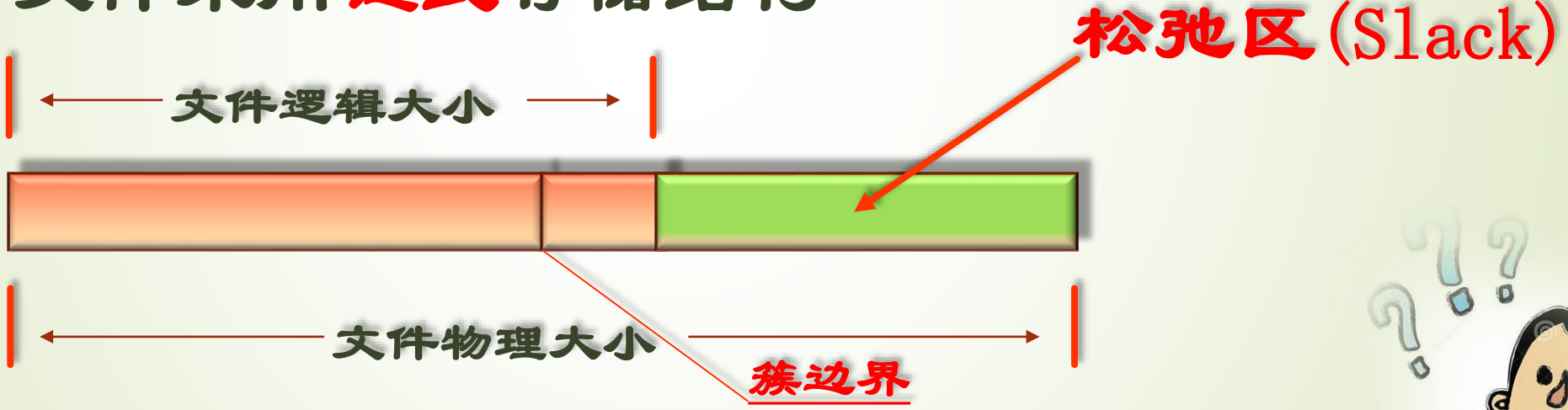






复制与镜像

- 以簇为基本处理单位
- 依据硬盘大小，一簇可能是1个或者多个扇区
- 文件采用链式存储结构



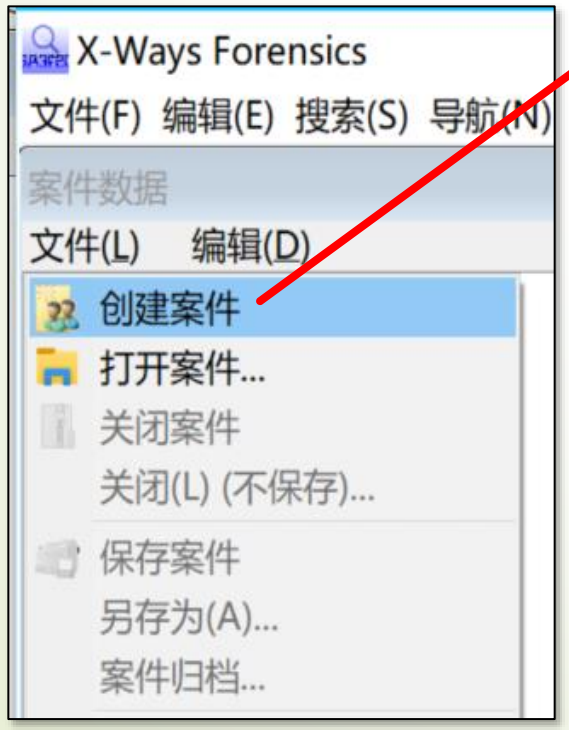
X-Ways Forensics

- 由德国X-ways出品的一个法证分析软件
- 用于计算机取证的综合的取证、分析软件，可在 Windows系列操作系统下运行，有32位和64位版。它事实上就是WinHex的法证授权版本，具有跟Winhex相同的界面和Winhex所有功能外的更多功能，并增加了文件预览等实用功能。

创建案件

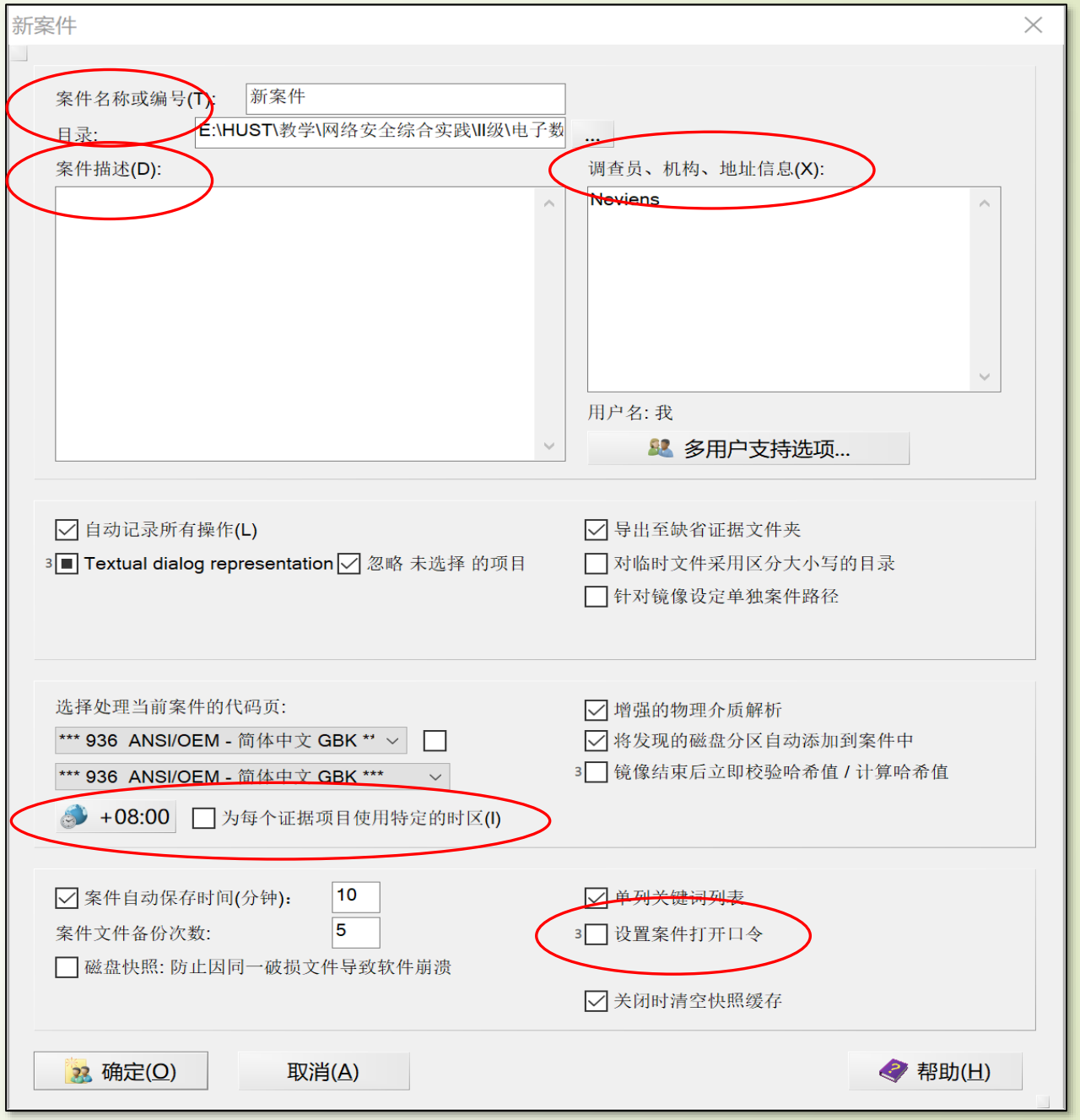
在X-Ways Forensics中创建一个案件

案件数据窗口点击文件菜单



创建案件

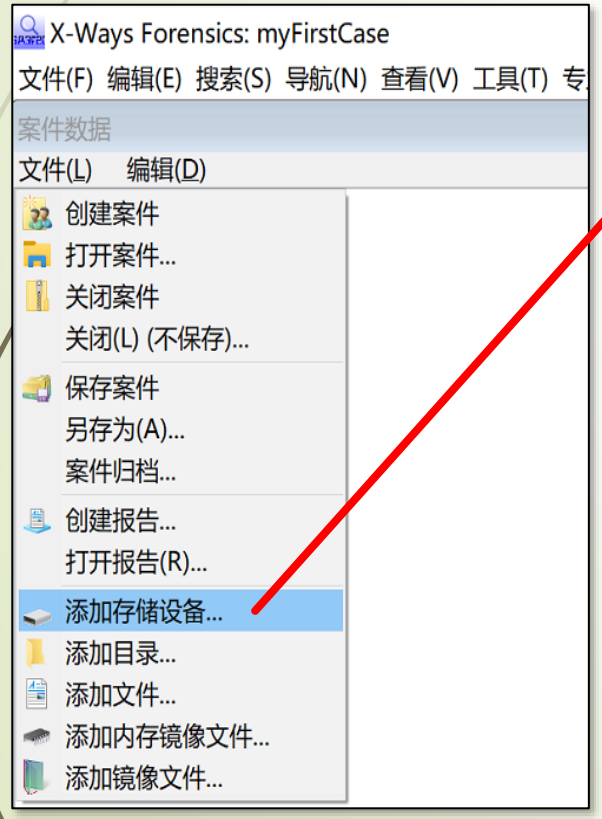
需要注意的几点

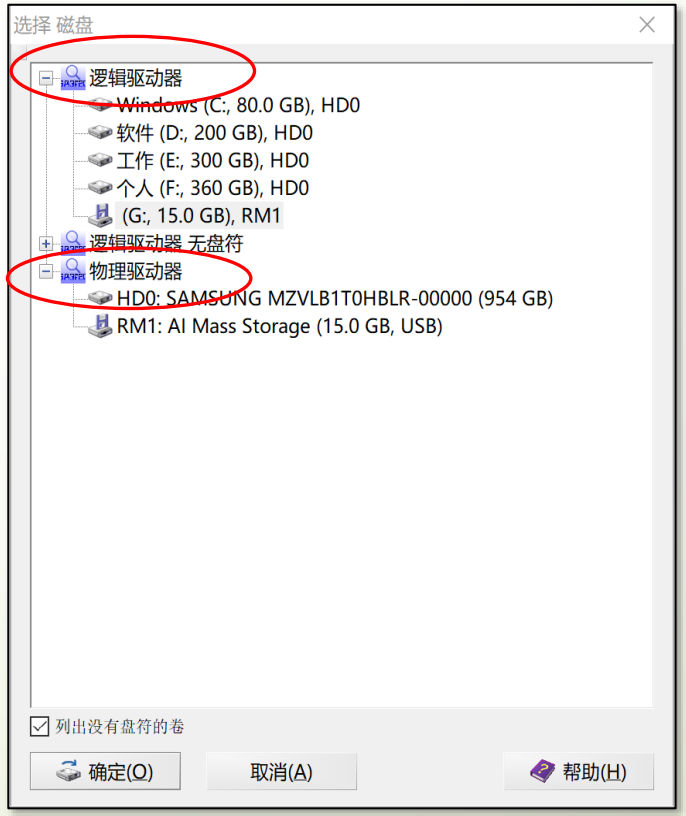


添加存储设备

向案件中添加需要获取/分析的目标

案件数据窗口点击文件-添加存储设备菜单





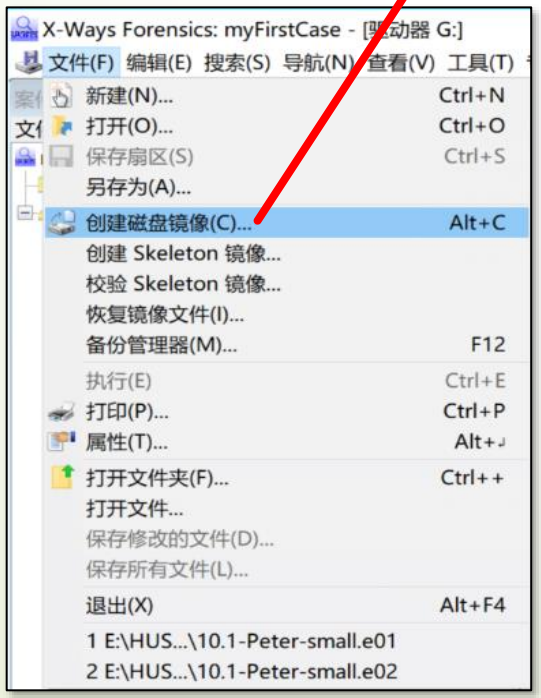
创建磁盘镜像

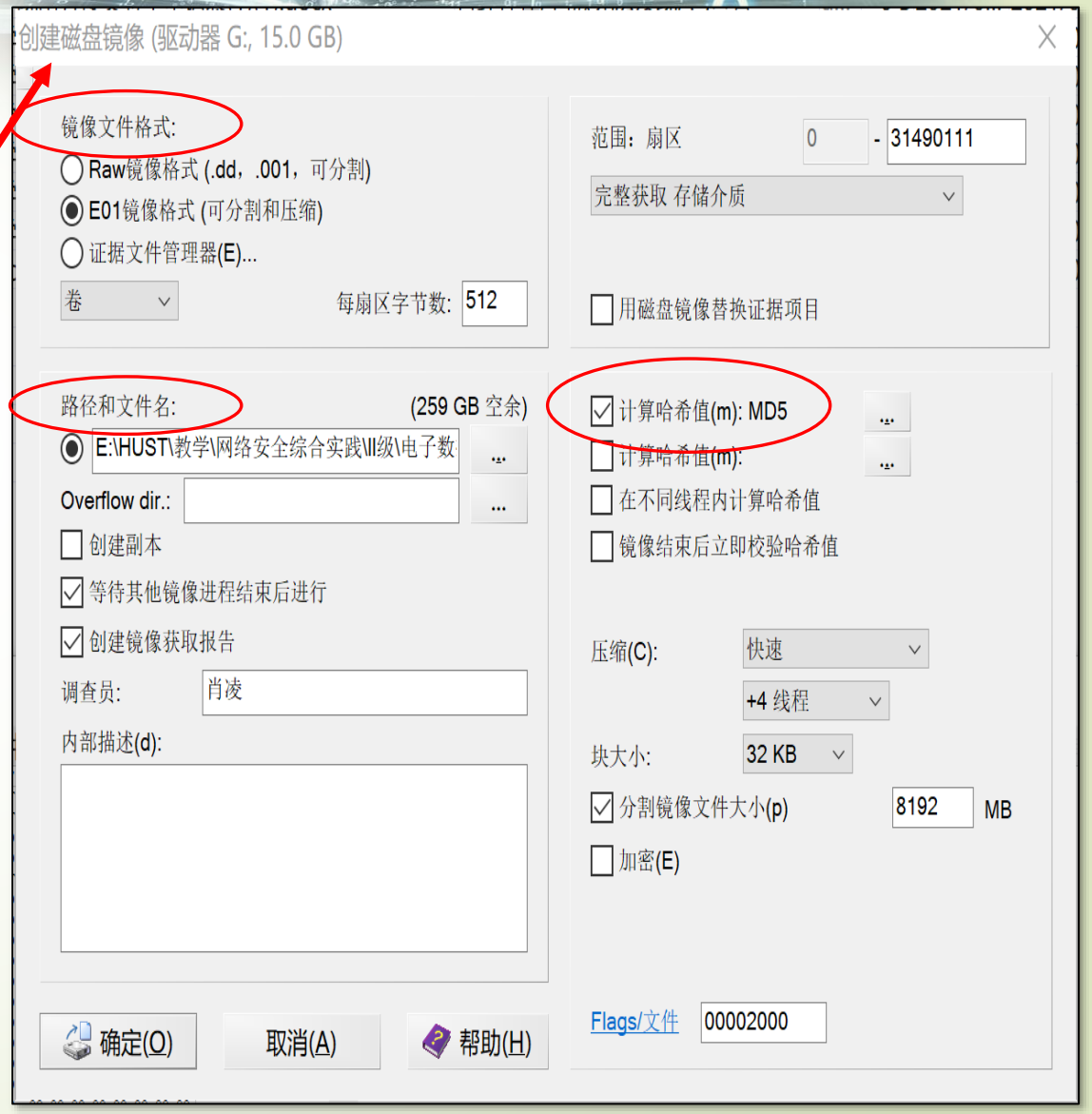
接下来创建自盘镜像

主窗口菜单点击

文件-创建磁盘

镜像菜单





获取数据报告

获取数据报告是获取证据的**重要依据**

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1-1

为你的U盘制作镜像。

1）在U盘上创建文本文件，该内容以“adcdefgh”，开头，其余内容随意且长度大于8个字节。将该文件以自己的姓名为文件名，扩展名为自己的学号。

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1中的U盘存储器，截图提交到学习通。

操作实验1-2

为你的U盘制作镜像。

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**。

内容简介
INTRODUCTION

1 任务1 磁盘镜像和证据固定

2 任务2 判断文件类型

3 任务3 文件搜索

文件名和扩展名

文件名：用户识别文件的**标志**

文件扩展名(Filename Extension)

- **早期**标识文件格式的一种机制
- 帮助系统识别用什么应用打开文件
- 对于文件而言**不**是必须的

扩展名可以人为设定或修改

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。

类别	文件类型	Magic数	起始偏移	结束偏移
Exe, dll	Windows可执行文件	"MZ"	0	2
	Linux可执行文件	"\x7F\x45\x4c\x46"	0	4
	Java类	"\xCA\xFE\xBA\xBE"	0	4
	Office2003, WPS	"\xD0\xCF\x11\xE0\xA1\xB1\x1A\xE1"	0	8
	Office2003, WPS	"WPS2001"	2	9
	Office2003, WPS	"\x64\x6f\x63\x50\x72\x6f\x70\x73"	30	38
	Office2007	"_Types\x5d\x2exml"	38	49

文件签名数据库

X-Ways Forensics有一个文件签名数据库，保存在文本文件中。

File Type Categories.txt	2021/6/9 4:03	文本文档	80 KB
File Type Signatures Check Only.txt	2020/7/20 18:09	文本文档	76 KB
File Type Signatures Search.txt	2021/6/9 1:21	文本文档	25 KB

	A	B	C	D	E	F	G	H
1	Descriptio	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 Phc	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	

文件签名数据库

	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	

文件类型（Description）：对某种类型文件的定义，长度为19字节；

文件扩展名（Extensions）：对所定义的文件类型的典型扩展名；

文件头签名（Header）：文件类型的唯一签名特征，最多支持16字节。

偏移量（Offset）：文件签名数据第一个字节相对文件的偏移地址；

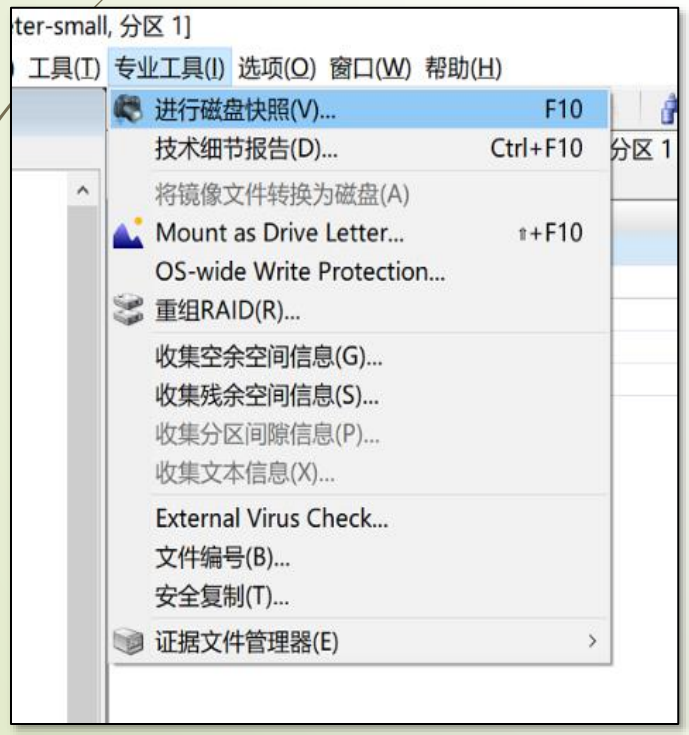
文件尾签名（Footer）：可选项，用于标记文件的结尾位置，最多支持8字节；

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

磁盘快照

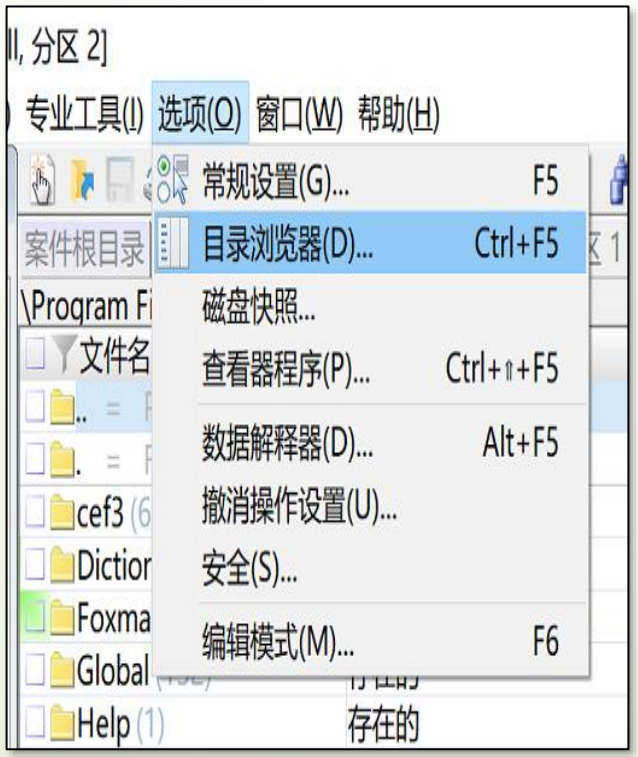
实际上是对磁盘中的数据进行分析的行为。

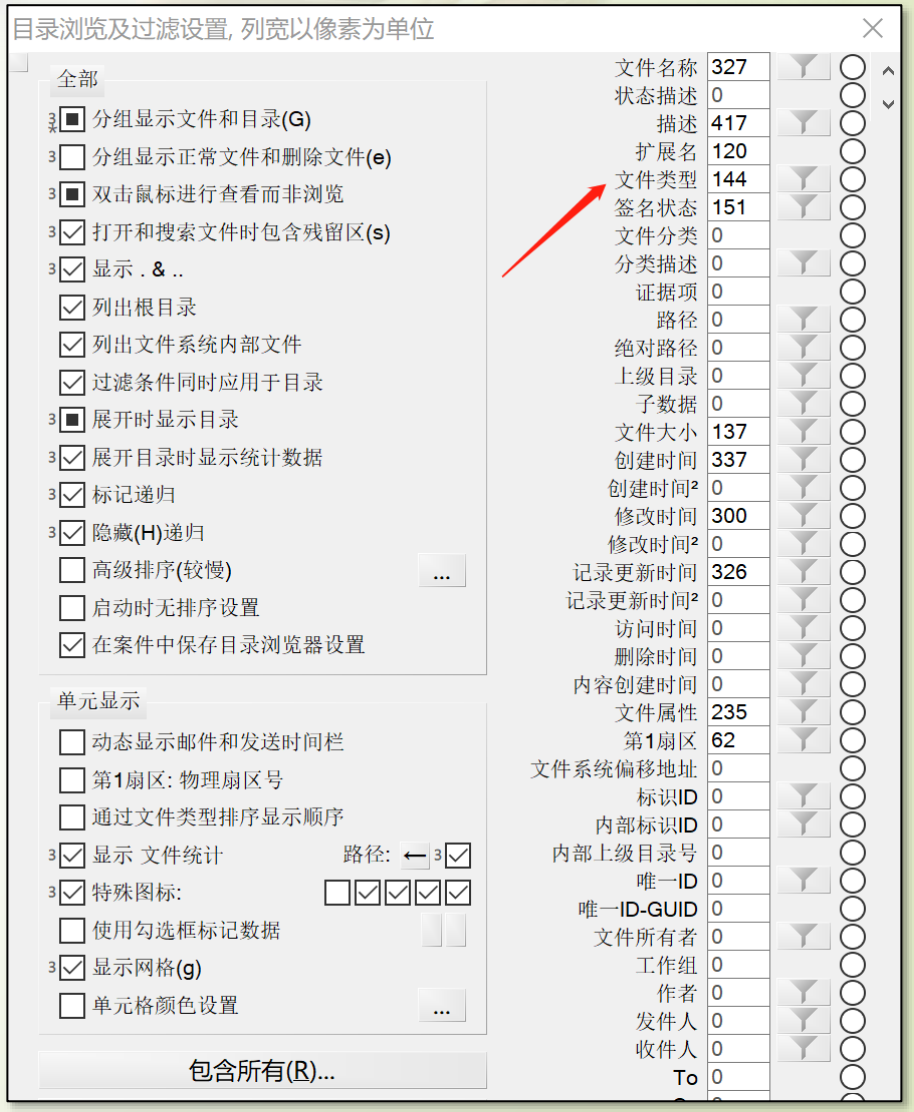
选中要进行快照的分区，点击主菜单中的专业工具-进行磁盘快照，打开进行磁盘快照对话框。



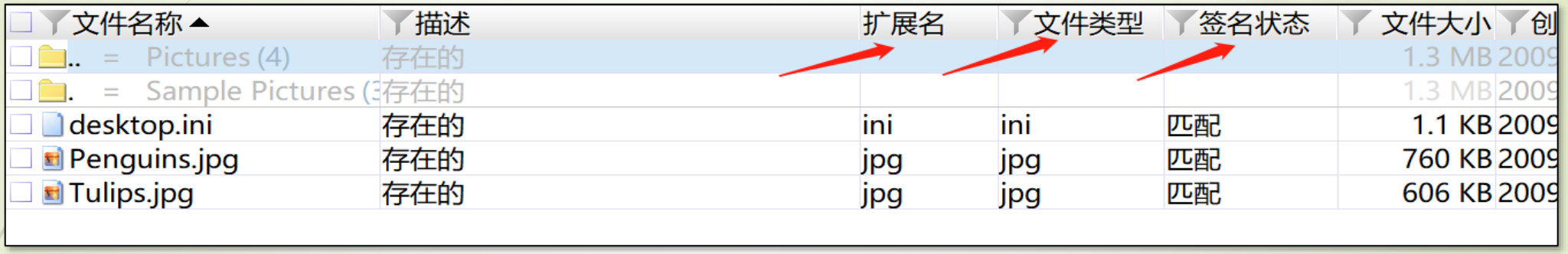
显示文件类型相关列

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。





显示文件类型相关列



文件名称	描述	扩展名	文件类型	签名状态	文件大小	创
.. = Pictures (4)	存在的				1.3 MB	2009
. = Sample Pictures (3	存在的				1.3 MB	2009
desktop.ini	存在的	ini	ini	匹配	1.1 KB	2009
Penguins.jpg	存在的	jpg	jpg	匹配	760 KB	2009
Tulips.jpg	存在的	jpg	jpg	匹配	606 KB	2009

文件的初始状态为“未验证”，经过比对文件签名，会出现以下的状态：

签名匹配：文件签名、扩展名和文件签名库匹配；

不在列表中：文件类型在文件签名库中不存在；

无关的：文件小于8字节；

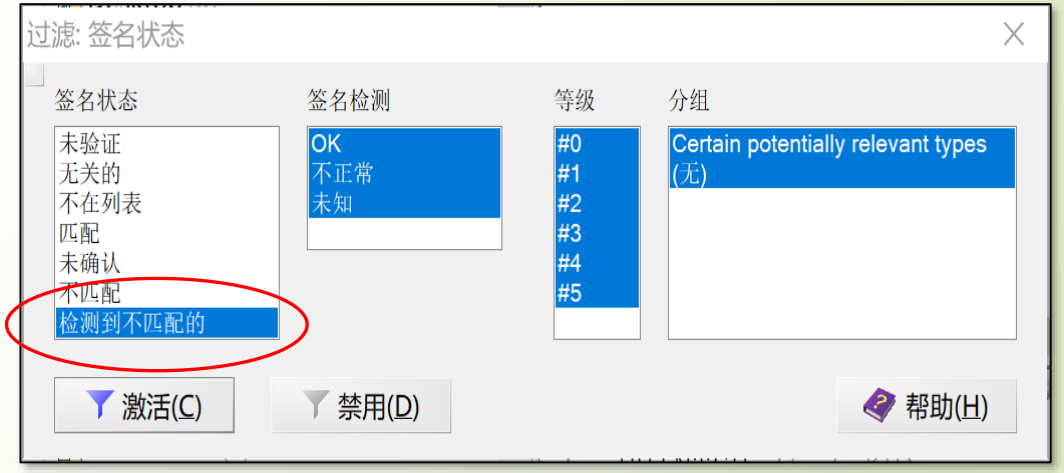
签名未校验：扩展名在数据库中被引用，但签名未知；

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；

未确认：扩展名在数据库中被引用，但是文件签名不匹配。

利用签名状态过滤

点击签名状态列左边的漏斗图标，打开过滤：签名状态对话框



操作实验2-1

在刚才创建的案件中去除添加的存储器，然后向案件添加U盘的镜像文件，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；

操作实验2-2

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盘中以自己姓名命名文件的文件类型、扩展名、签名状态等信息，提供截图到学习通；

操作实验2-3

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）**删除新添加的文件类型签名**，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**。

内容简介
INTRODUCTION

1. 任务1 磁盘镜像和证据固定
2. 任务2 判断文件类型
3. 任务3 文件搜索

文件搜索

文件过滤

文件属性

文件搜索

文件内容

影响搜索成功的因素

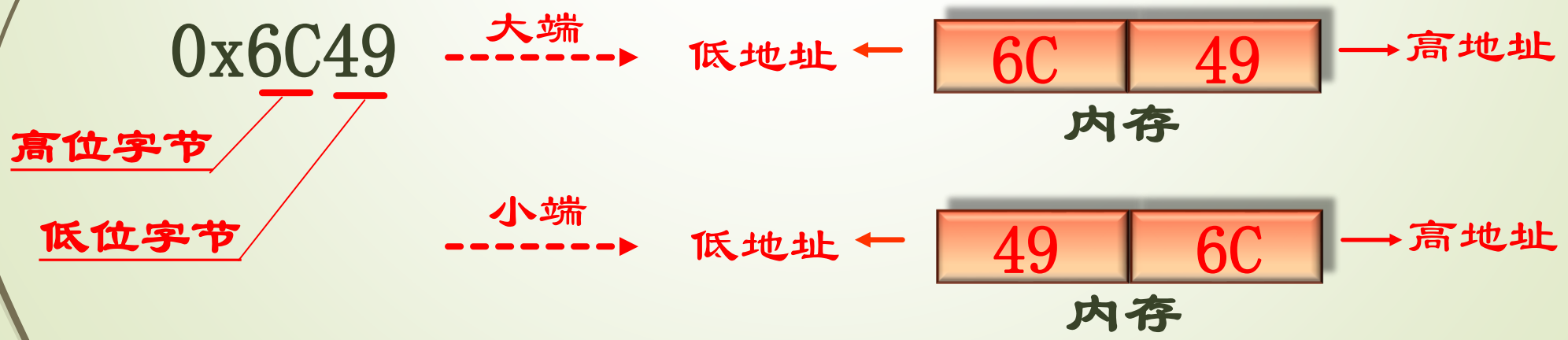
- 字节顺序
- 编码方式
- 搜索方法

文件搜索

字节顺序

计算机系统对多字节数据的表现方式

字节顺序	含义
大端字节序	word数据类型的高位字节放在内存中的低地址处
小端字节序	word数据类型的低位字节放在内存中的低地址处



文件搜索

编码&解码

问题背景

011101010

编码

解码

我爱我的祖国

文件搜索

编码-字符编码

计算机将二进制内码与字符对应起来的映射表

常用的字符编码集

- ASCII编码
- Unicode编码

文件搜索

编码-字符编码-ASCII编码

7位编码，忽略每个字节的最高位

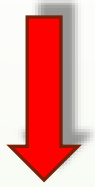
码值	字符	码值	字符	码值	字符	码值	字符	码值	字符
48	0	63	?	78	N	93	]	108	l
49	1	64	@	79	O	94	^	109	m
50	2	65	A	80	P	95	_	110	n
51	3	66	B	81	Q	96	`	111	o
52	4	67	C	82	R	97	a	112	p
53	5	68	D	83	S	98	b	113	q
54	6	69	E	84	T	99	c	114	r
55	7	70	F	85	U	100	d	115	s
56	8	71	G	86	V	101	e	116	t
57	9	72	H	87	W	102	f	117	u
58	:	73	I	88	X	103	g	118	v
59	;	74	J	89	Y	104	h	119	w
60	<	75	K	90	Z	105	i	120	x
61	=	76	L	91	[	106	j	121	y
62	>	77	M	92	\	107	k	122	z

文件搜索

编码-字符编码-Unicode编码

ISO和Unicode协会共同工作成果，为世界上所有的字符分配了一个唯一的Unicode编号

- 编号范围从0x000000-0x10FFFF，共110多万字符
- 仅定义了编号，没有定义编号如何存储和传输



Unicode字符集传输格式

文件搜索

编码-字符编码-Unicode编码

UTF(UCS Transformation Format)

UTF本质上是Unicode的具体实现方式

- UTF-32
- UTF-16
- UTF-8

使用4字节直接表示Unicode编号

文件搜索

编码-字符编码-Unicode编码

UTF-16

对Unicode编号再进行编码，以期节省空间

- 0x0-0xFFFF
  - 2字节
- 0xFFFF-0x10FFFF
  - 4字节

文件搜索

编码-字符编码-Unicode编码

UTF-16

Unicode 编号范围 （十六进制）	具体的 Unicode 编号 （二进制）	UTF-16 编码	编码后的 字节数
0000 0000 ~ 0000 FFFF	xxxxxxxx xxxxxxxx	xxxxxxxx xxxxxxxx	2
0001 0000---0010 FFFF	yyyy yyyy yyxx xxxx xxxx	110110yy yyyyyyyy 110111xx xxxxxxxx	4

文件搜索

编码-字符编码-Unicode编码

UTF-8

对Unicode编号再进行编码，以期节省空间

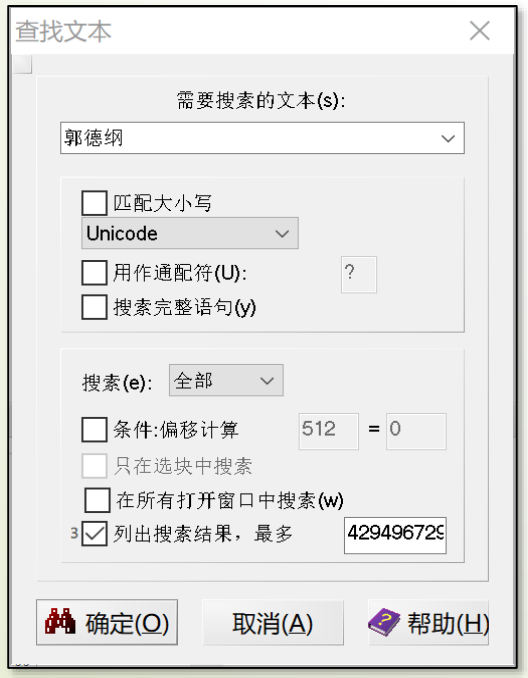
编号范围 （编号对应的十进制数）	二进制格式
0x00 - 0x7F (0 - 127)	0XXXXXXX
0x80 - 0x7FF (128 - 2047)	110XXXXX 10XXXXXX
0x800 - 0xFFFF (2048 - 65535)	1110XXXX 10XXXXXX 10XXXXXX
0x10000 - 0x10FFFF (65536以上)	11110XXX 10XXXXXX 10XXXXXX 10XXXXXX

- 更节省空间
- 兼容ASCII码

文件搜索

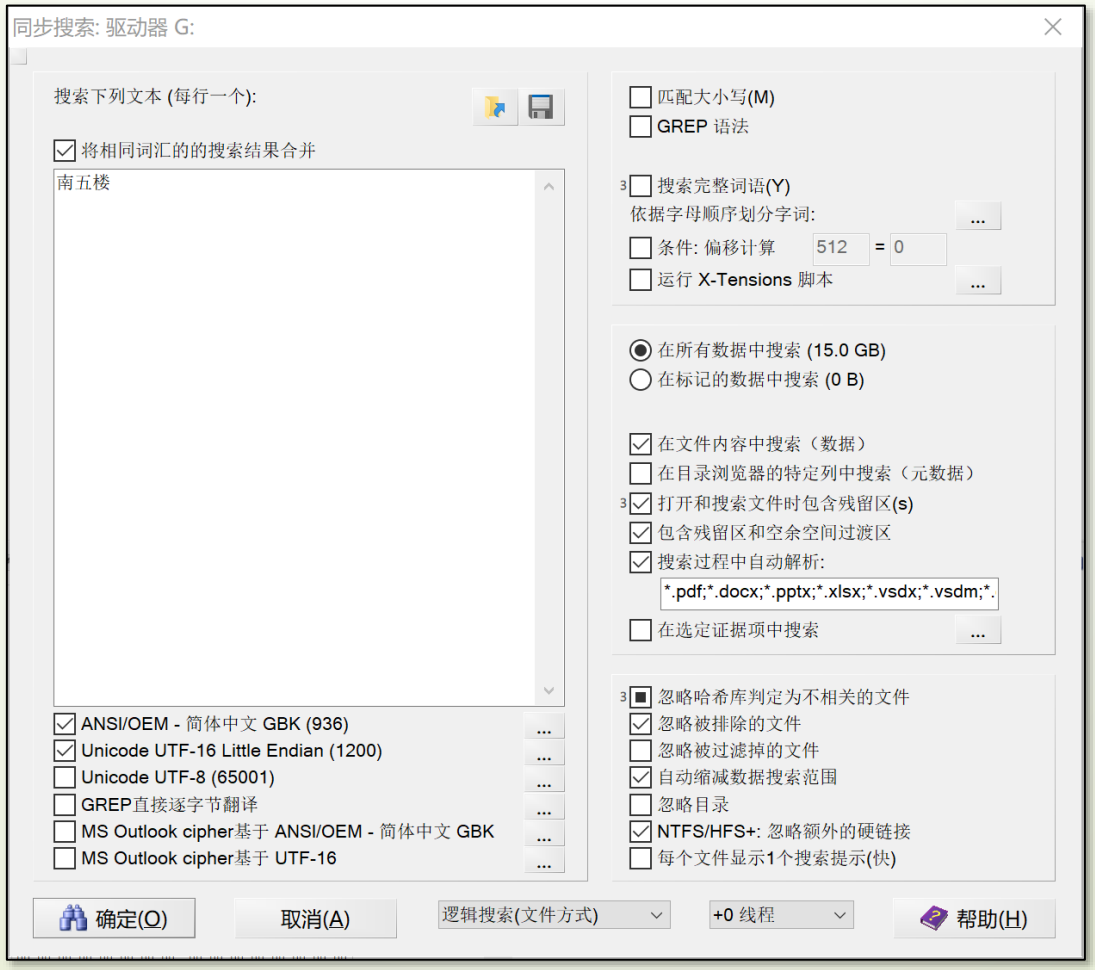
通过字符/特定表达式对数据查找、匹配、定位

- 字符串匹配　搜索目标是字符串
- 十六进制匹配 搜索目标非字符串



文件搜索

- 同步搜索　用户指定一个搜索关键词列表文件



文件搜索步骤

1. **选定搜索范围。**为了精确、快速的搜索，需要在搜索前决定搜索时的位置。
2. **输入关键词。**
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3-1

在实验1中创建的案件添加自己的逻辑分区C，并按要求进行搜索

1）在逻辑分区中搜索包含“华中科技大学”字符的word文档，你准备如何搜索呢？请将你的回答、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）

操作实验3-2

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）

操作实验3-3

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）