'清空回收站'后依然在磁盘中被抓到证据！原因竟然是...

原创 队员编号012 酒仙桥六号部队 6月11日

这是 **酒仙桥六号部队** 的第 **16** 篇文章。

全文共计1871个字，预计阅读时长5分钟。

1 前言

当我们需要对计算机进行磁盘取证时往往会发现，该台电脑之前的操作人员已经将敏感文件删除进入回收站，并清空回收站或从回收站中彻底删除了这些文件，而这些文件很可能包含了重要的取证信息。

从原理上，删除只是在文件上作了删除标记，而真正的文件内容仍保存在磁盘的数据区中，并未得以删除。要等到以后的数据写入，把此数据区覆盖掉，这样才算是彻底把原来的数据删除。因此只要将整个磁盘进行分析，就有可能将已经彻底删除的文件恢复。

2 准备工作

目标系统：Win7SP1x86

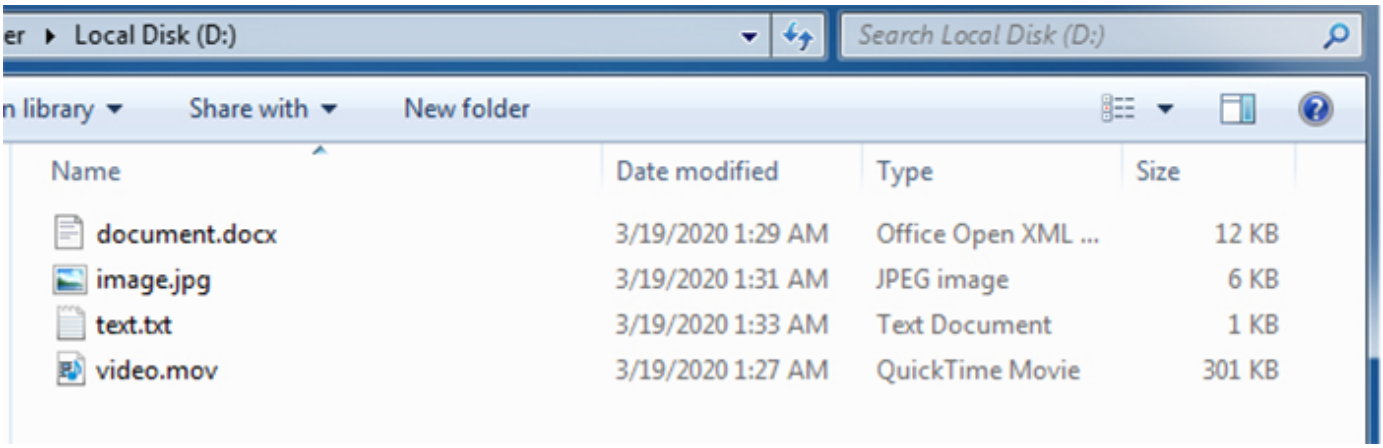
1、首先我们在 D 盘创建几个小图片、小视频、小文档：

image.jpg 、 video.mov 、 text.txt 、 document.docx 、 image_d.jpg 、 video_d.mov 、 text_d.txt、document_d.docx。

2、右键删除

image_d.jpg、video_d.mov、text_d.txt、document_d.docx，

之后 "清空回收站"。



3 创建磁盘镜像

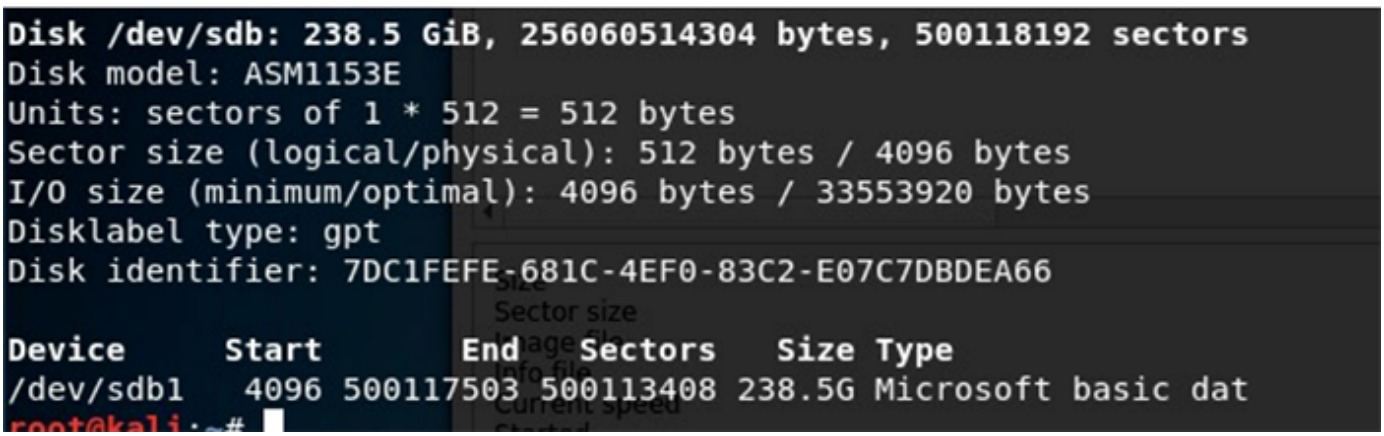
在进行磁盘取证时，为了尽量减少目标主机文件系统的变动，我们可以使用离线方式进行磁盘取证，将目标主机的磁盘创建镜像，放在移动磁盘中存储。

3.1 在 Kali 下创建磁盘镜像

3.3.1 启动到Live模式下

1、首先启动进入取证模式；

2、接入移动硬盘，fdisk -l 确定移动硬盘的设备名为/dev/sdb1；

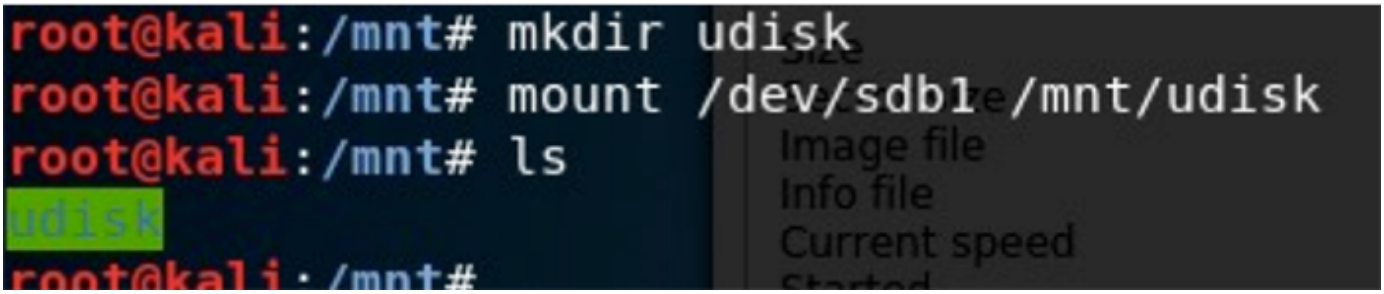


3、挂载移动硬盘。

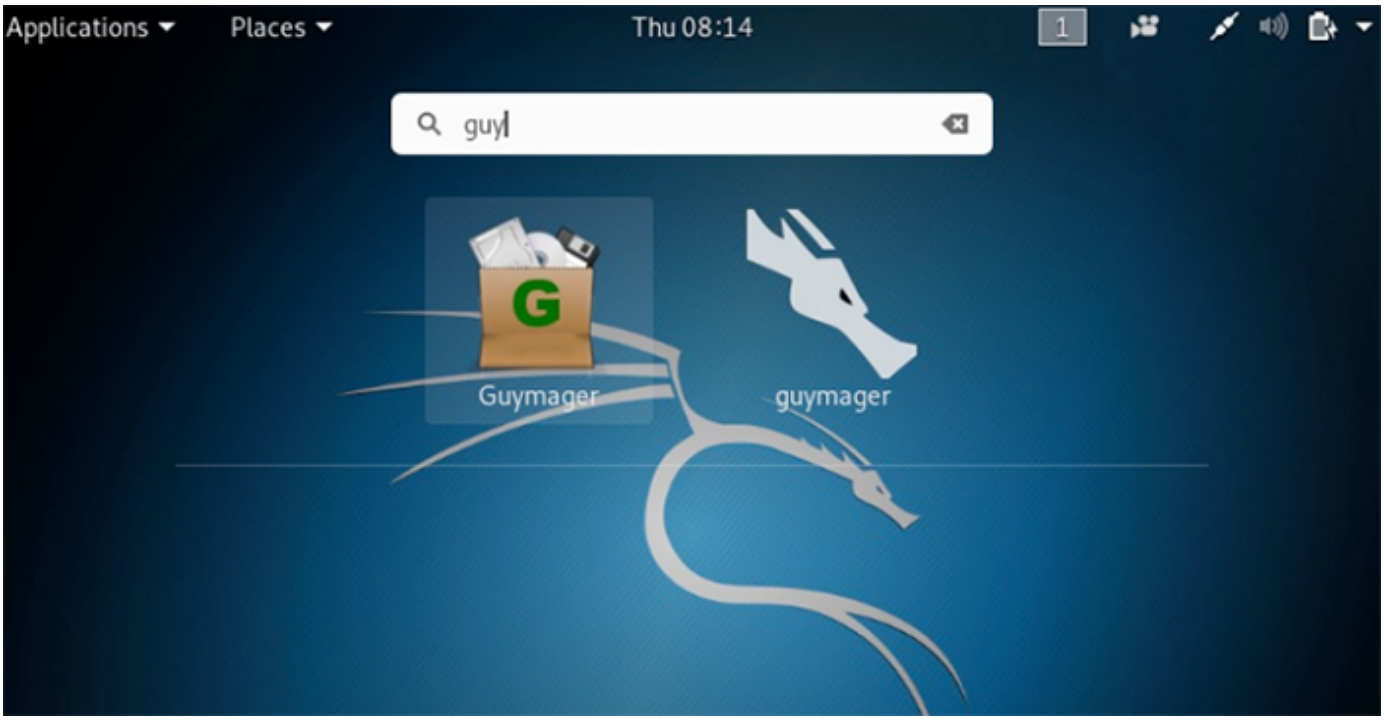
cd /mnt

mkdir udisk

mount /dev/sdb1 /mnt/udisk



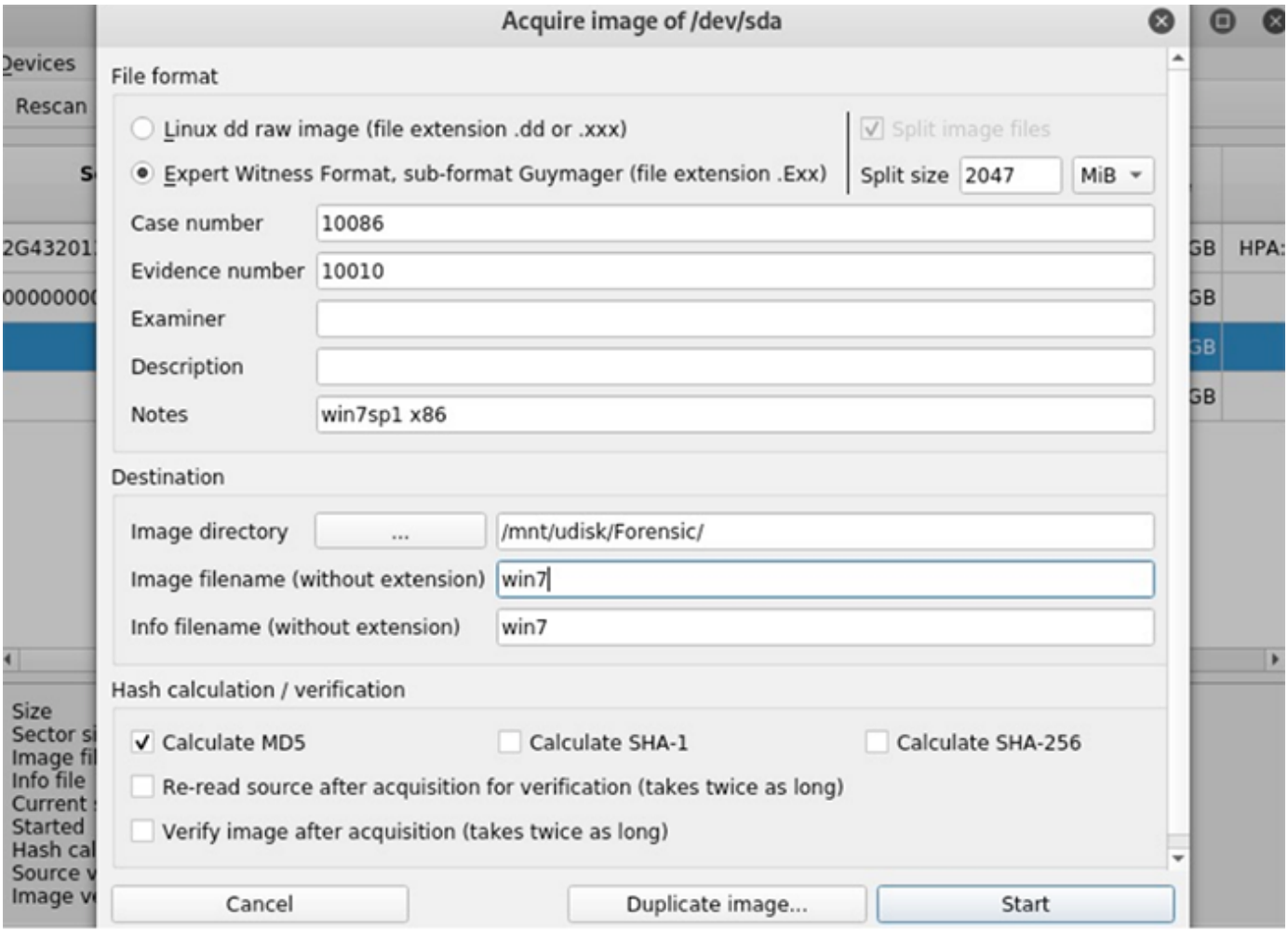
3.1.2 使用Guymager



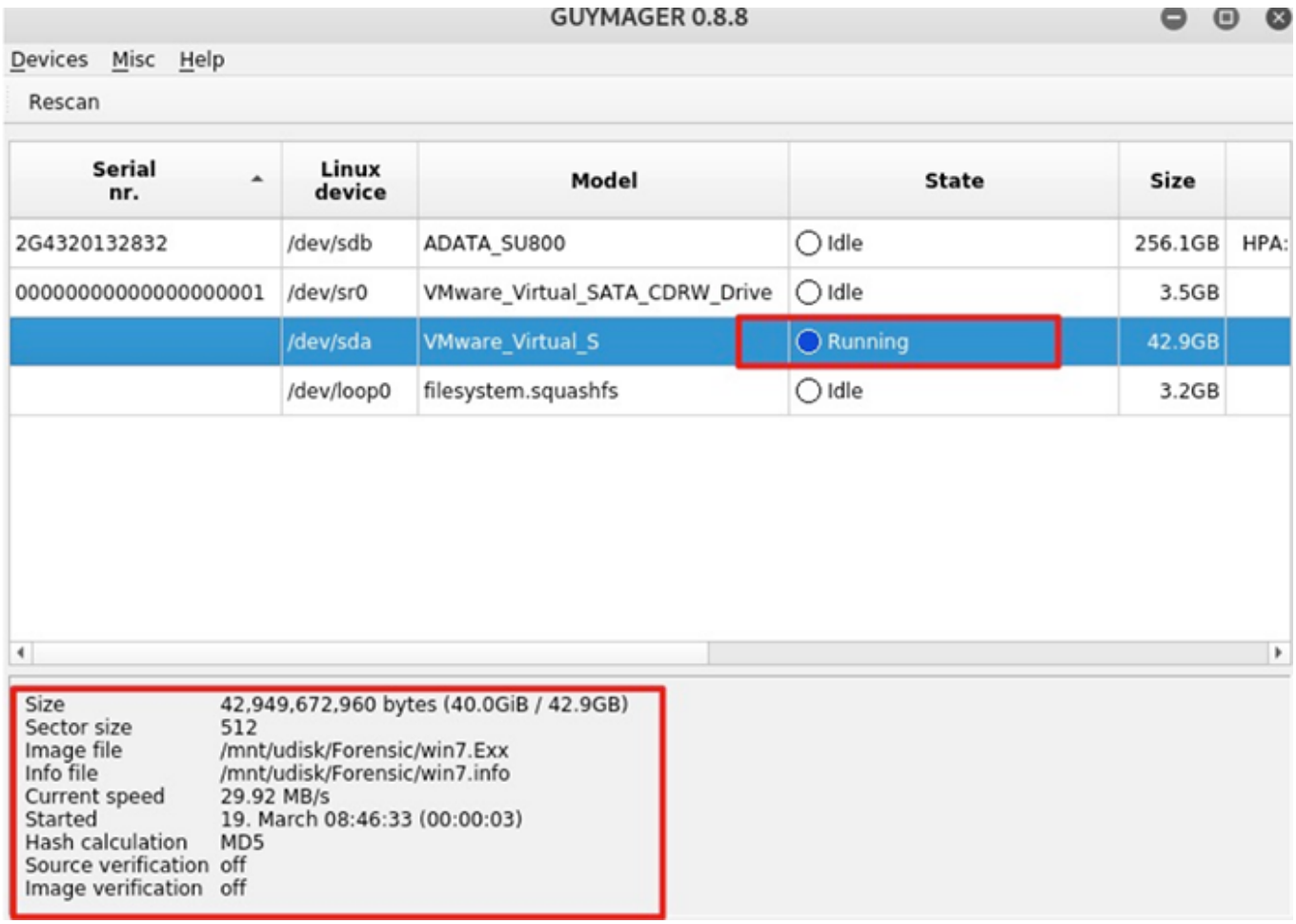
1、在目标硬盘上右键 Acquire image，

设置相关信息、保存路径、文件名，开始获取磁盘镜像。

下面的hash校验我勾掉了，是为了让速度更快一些。



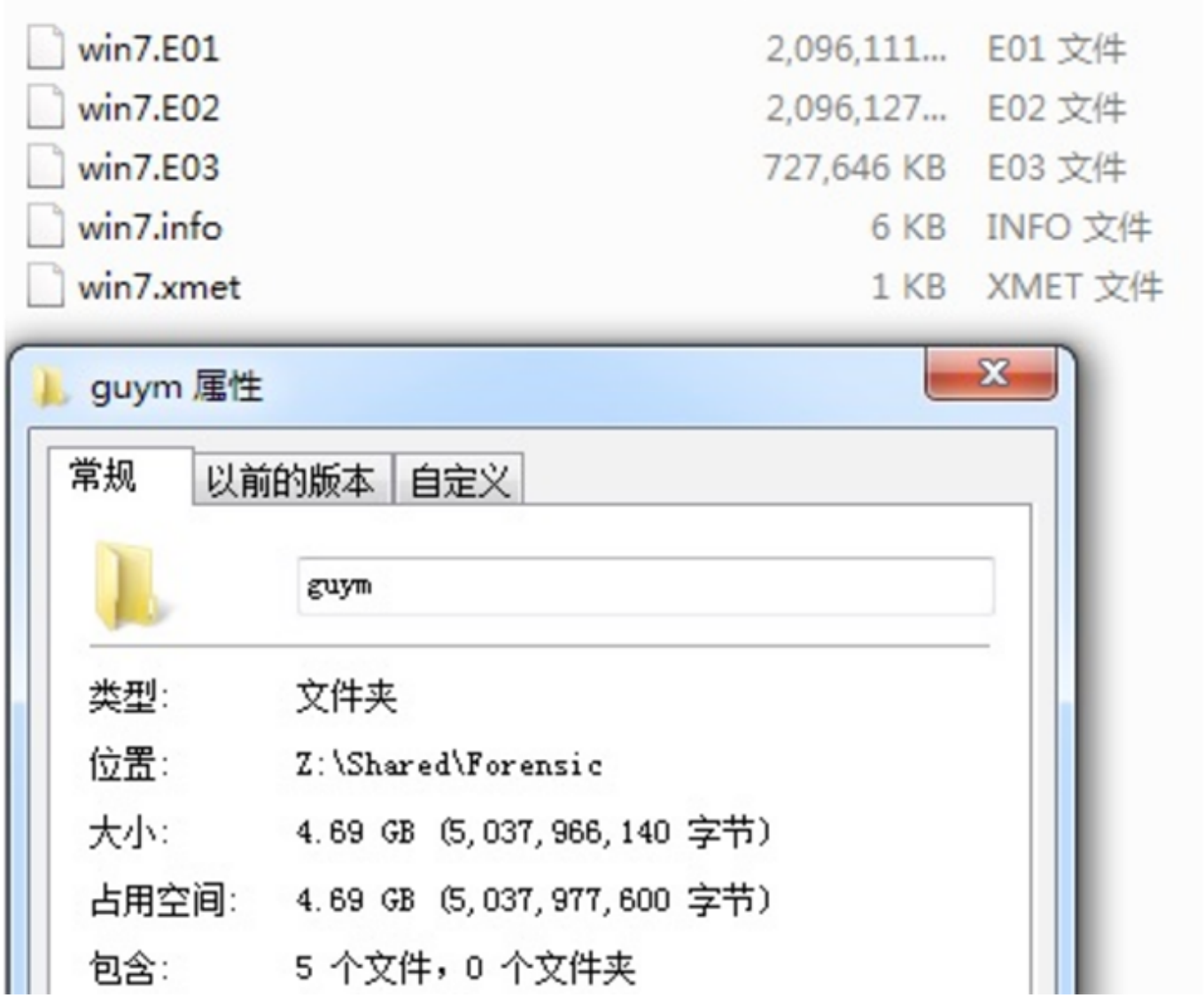
2、Start开始后，需要一段时间，由磁盘容量、速度与电脑性能决定。



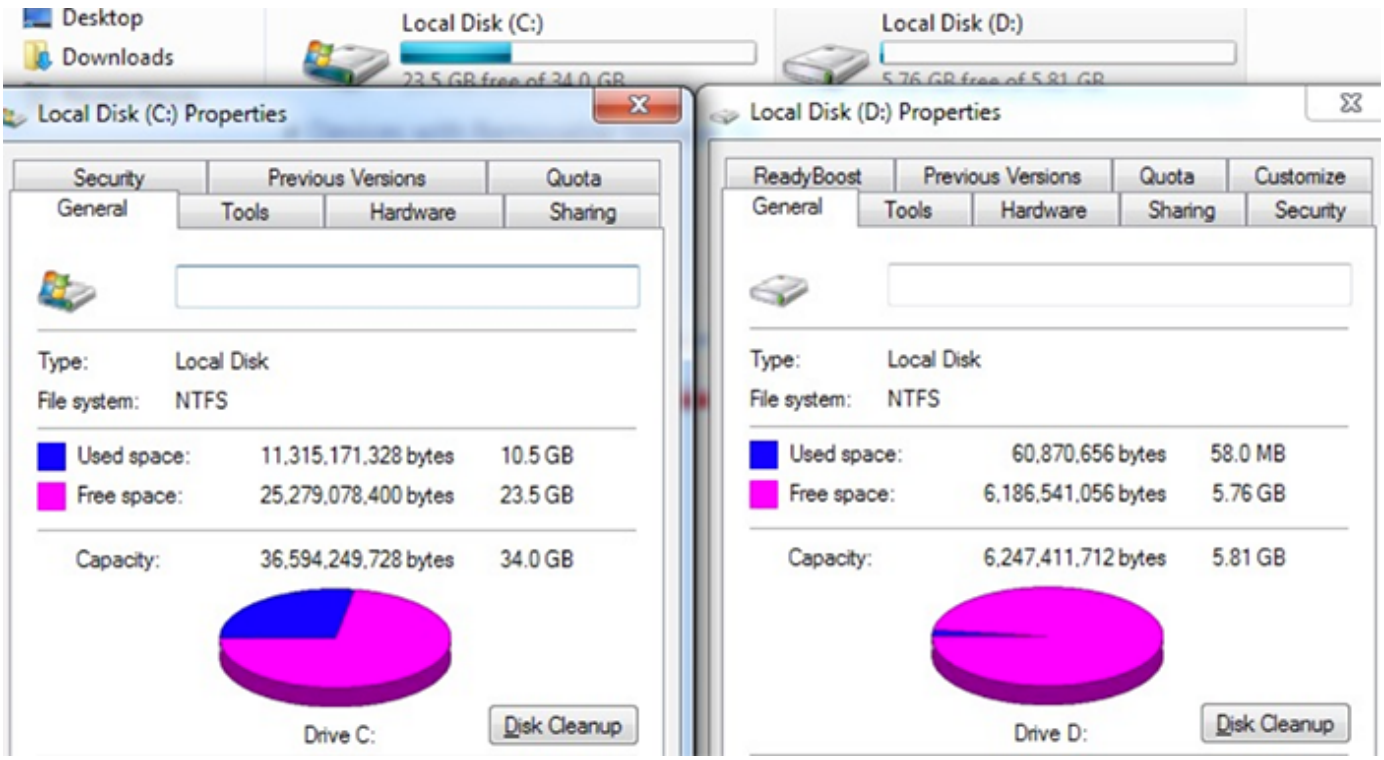
3、镜像制作完成。

Serial nr.	Linux device	Model	State	Size	
2G4320132832	/dev/sdb	ADATA_SU800	Idle	256.1GB	HPA:
00000000000000000001	/dev/sr0	VMware_Virtual_SATA_CDRW_Drive	Idle	3.5GB	
	/dev/sda	VMware_Virtual_S	Finished	42.9GB	
	/dev/loop0	filesystem.squashfs	Idle	3.2GB	

全磁盘镜像文件大小共4.7GB。



磁盘实际使用大小是这样的。



3.1.3 使用dd

1、fdisk -l 判断目标磁盘编号：

#if=指定需要制作映像设备，-of=指定保存的位置。

2、dd if=/dev/sda

of=/mnt/udisk/Forensic/dd/sda

```
root@kali:/mnt/udisk/Forensic/dd# dd if=/dev/sda of=/mnt/udisk/Forensic/dd/sda
^C2831068+0 records in
2831068+0 records out
1449506816 bytes (1.4 GB, 1.3 GiB) copied, 508.674 s, 2.8 MB/s

root@kali:/mnt/udisk/Forensic/dd# dd if=/dev/sda3 of=/mnt/udisk/Forensic/dd/sda3
^C1339327+0 records in
1339327+0 records out
685735424 bytes (686 MB, 654 MiB) copied, 231.578 s, 3.0 MB/s
```

dd速度非常慢，且在备份过程中没有任何进度提示，直接放弃换用增强版dd------dc3dd。

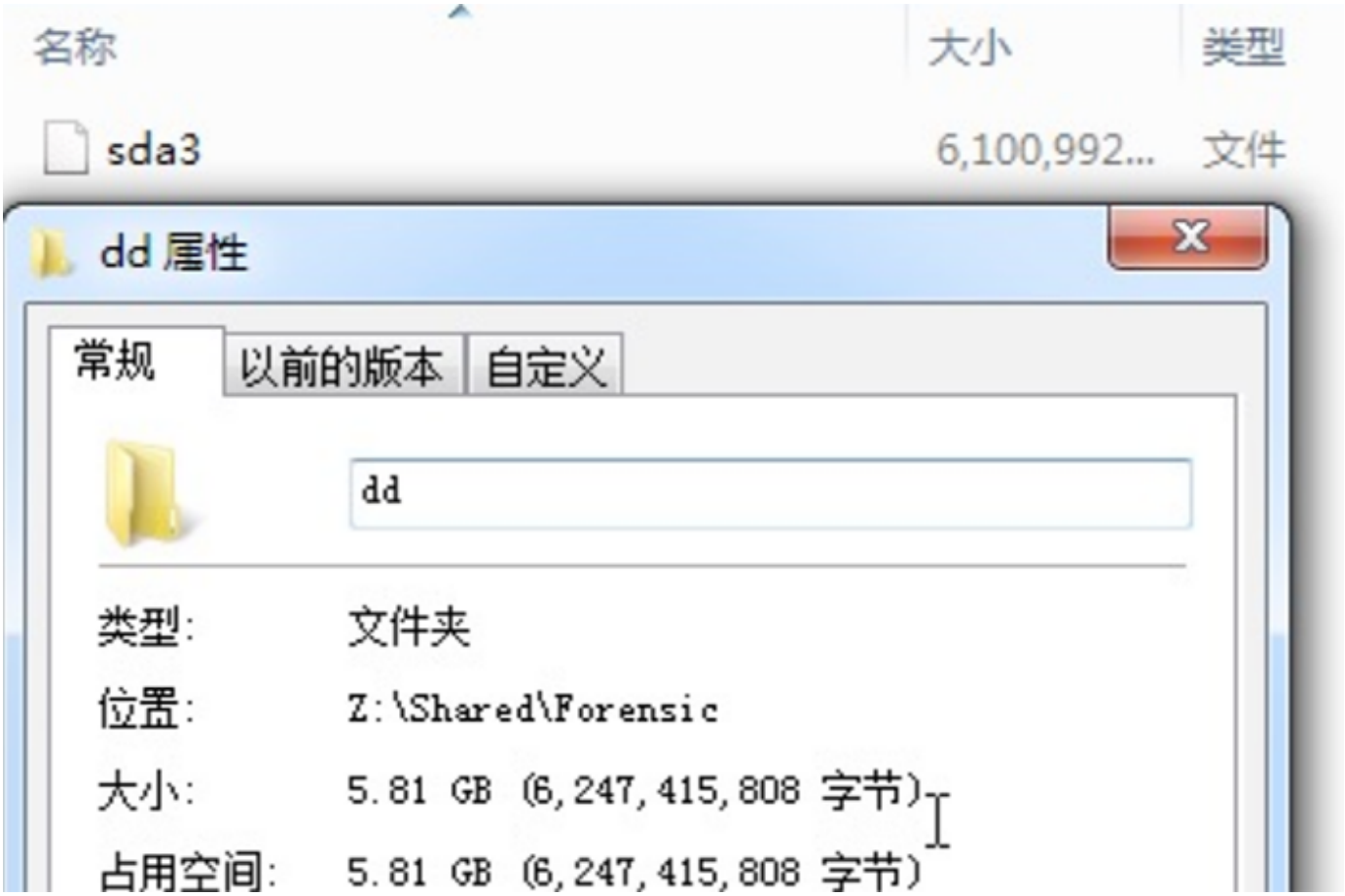
3.1.4 使用dc3dd

dc3dd和dd参数使用是一样的，它们一样是完整备份，对备份盘容量需求比较大，这里只备份sda3（D盘），可以看到备份了约6GB大小。

```
root@kali:/mnt/udisk/Forensic/dd# dc3dd if=/dev/sda3 of=/mnt/udisk/Forensic/dd/sda3

dc3dd 7.2.646 started at 2020-03-19 09:31:24 +0000
compiled options:
command line: dc3dd if=/dev/sda3 of=/mnt/udisk/Forensic/dd/sda3
device size: 12201984 sectors (probed),    6,247,415,808 bytes
sector size: 512 bytes (probed)
   130580480 bytes ( 125 M ) copied (  2% ),    4 s, 34 M/s
```

最终D盘分区镜像大小5.81GB。



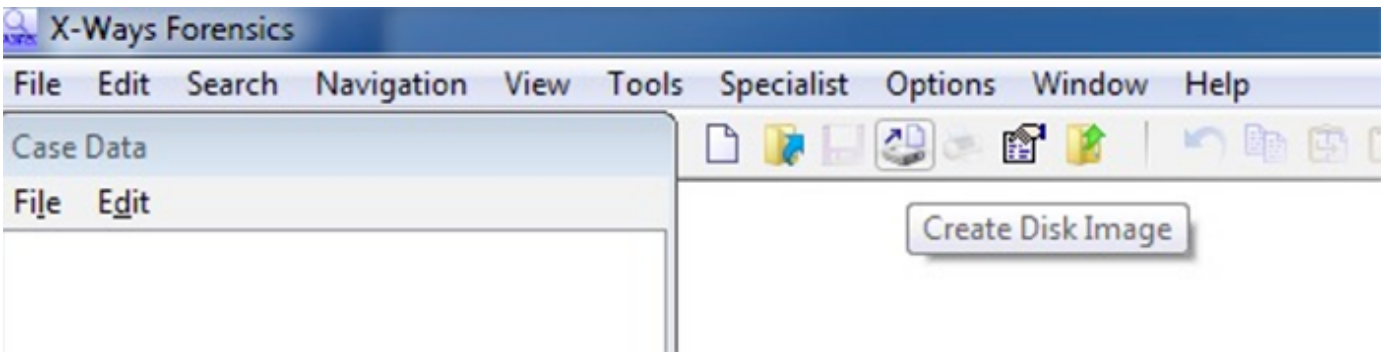
3.2 在 Windows 下创建磁盘镜像

在Windows下也最好使用Live系统如WindowsPE启动盘进行取证，但是由于这里没有现成的包含取证工具的启动盘，因此直接在系统里操作。取证工具、创建的磁盘镜像文件，都放在虚拟机的共享磁盘上，尽可能避免改变目标文件系统。

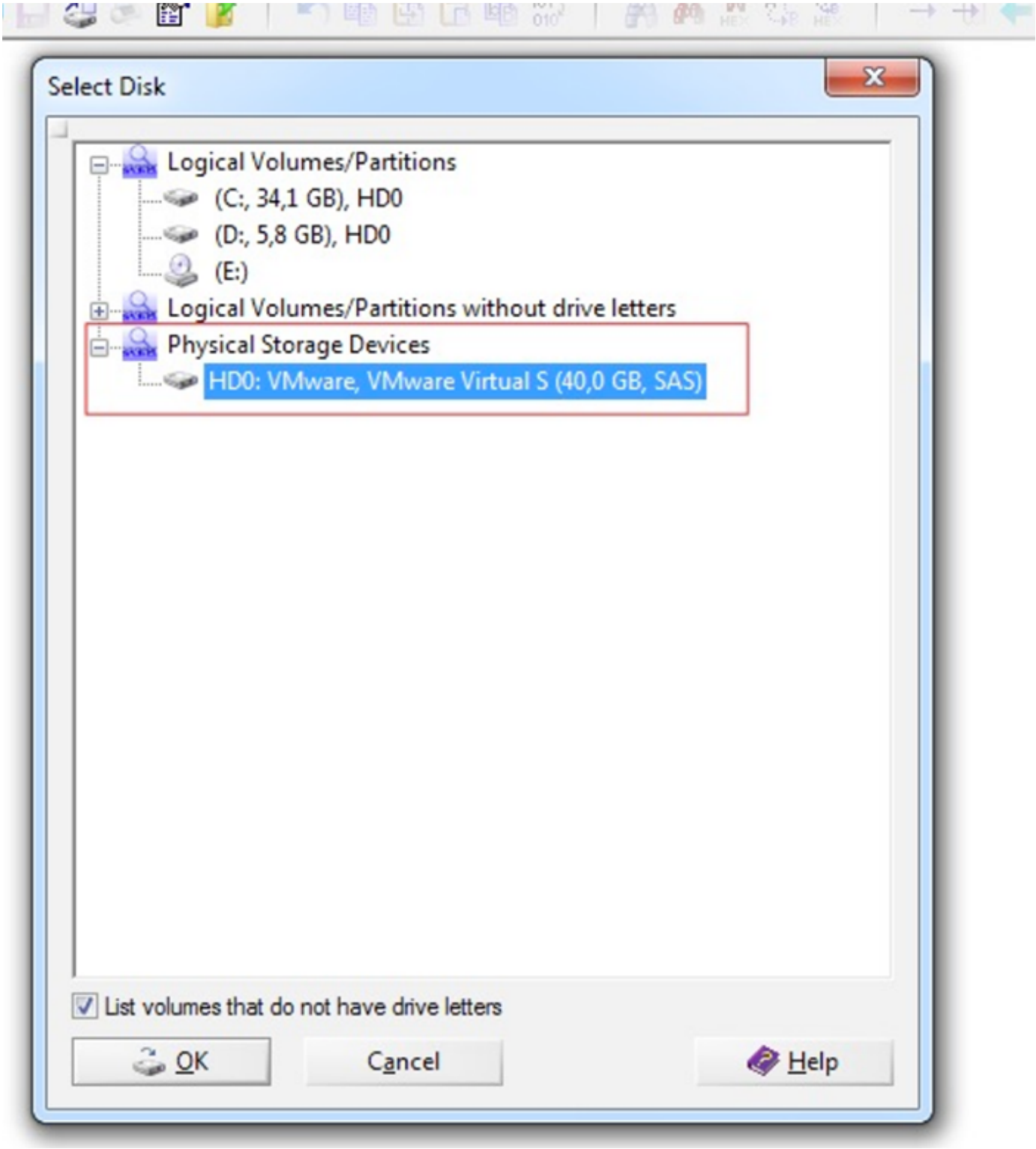
3.2.1 使用X-Ways Forensics

这个工具就是Winhex的取证加强版，因此界面几乎都一样。

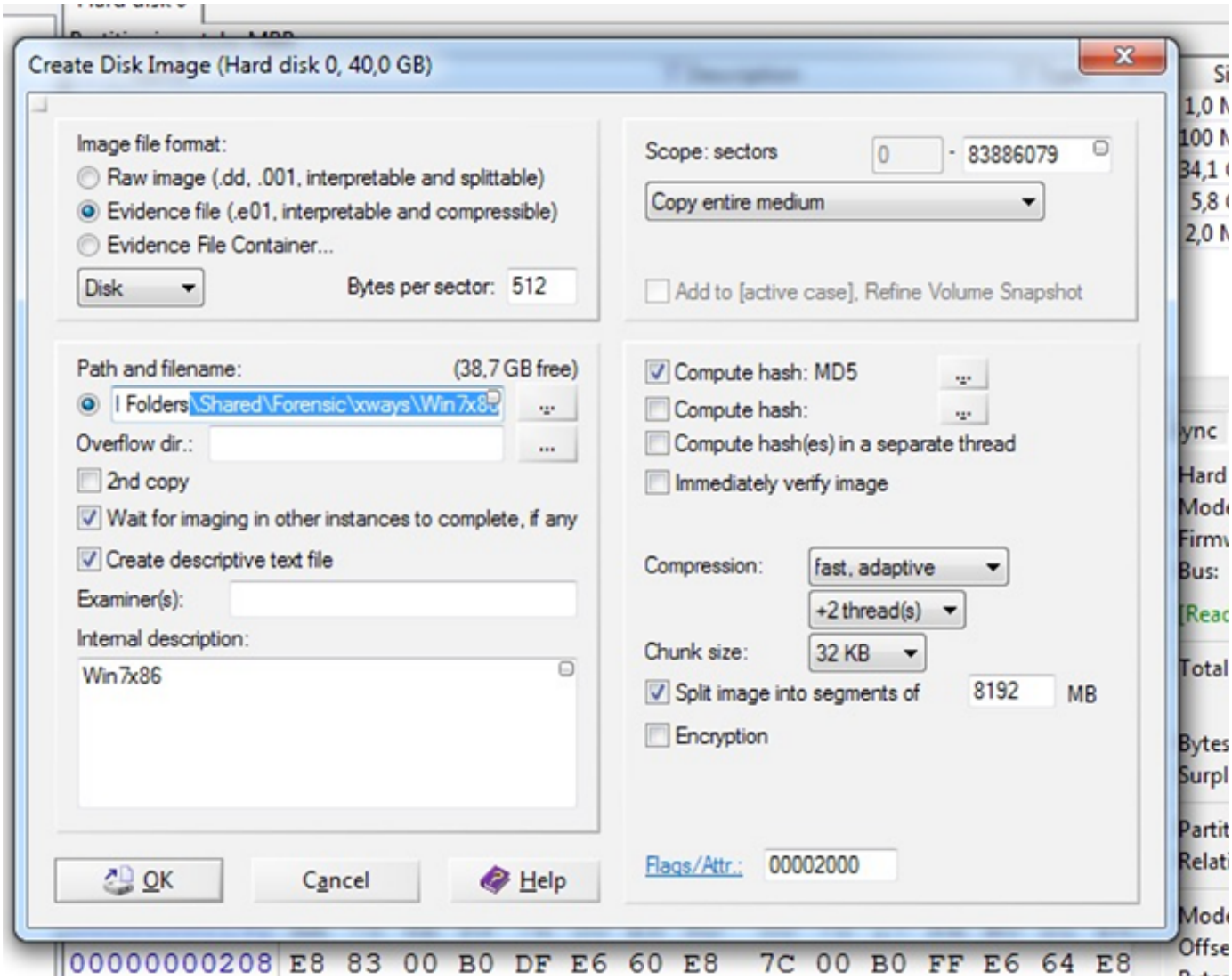
1、工具栏选择Create Disk Image。



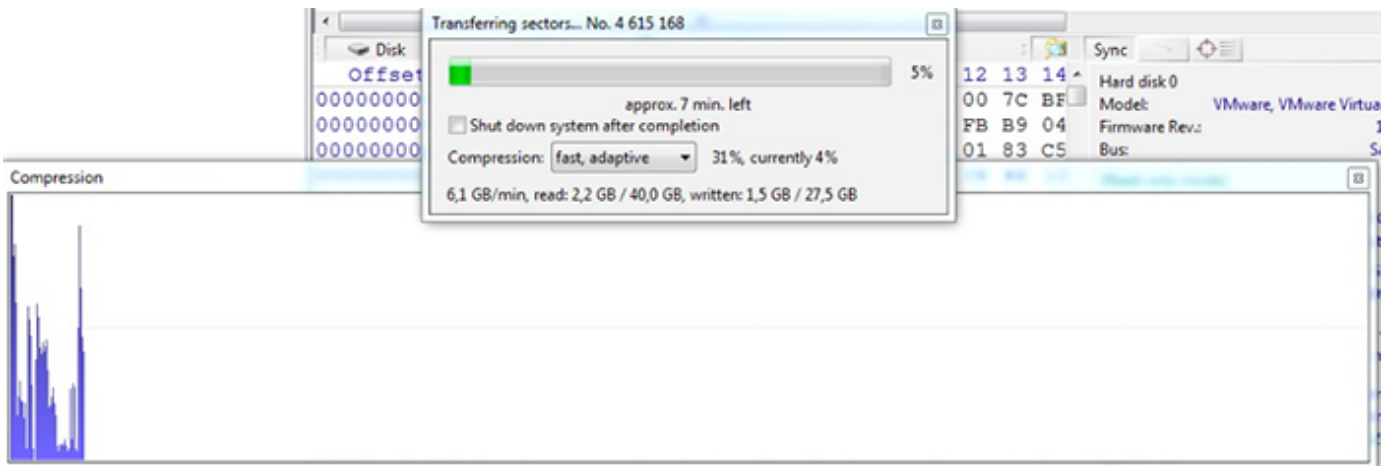
2、直接给整个磁盘创建镜像，创建分区镜像可以选择上边的。



3、选择好存储路径后点OK开始。



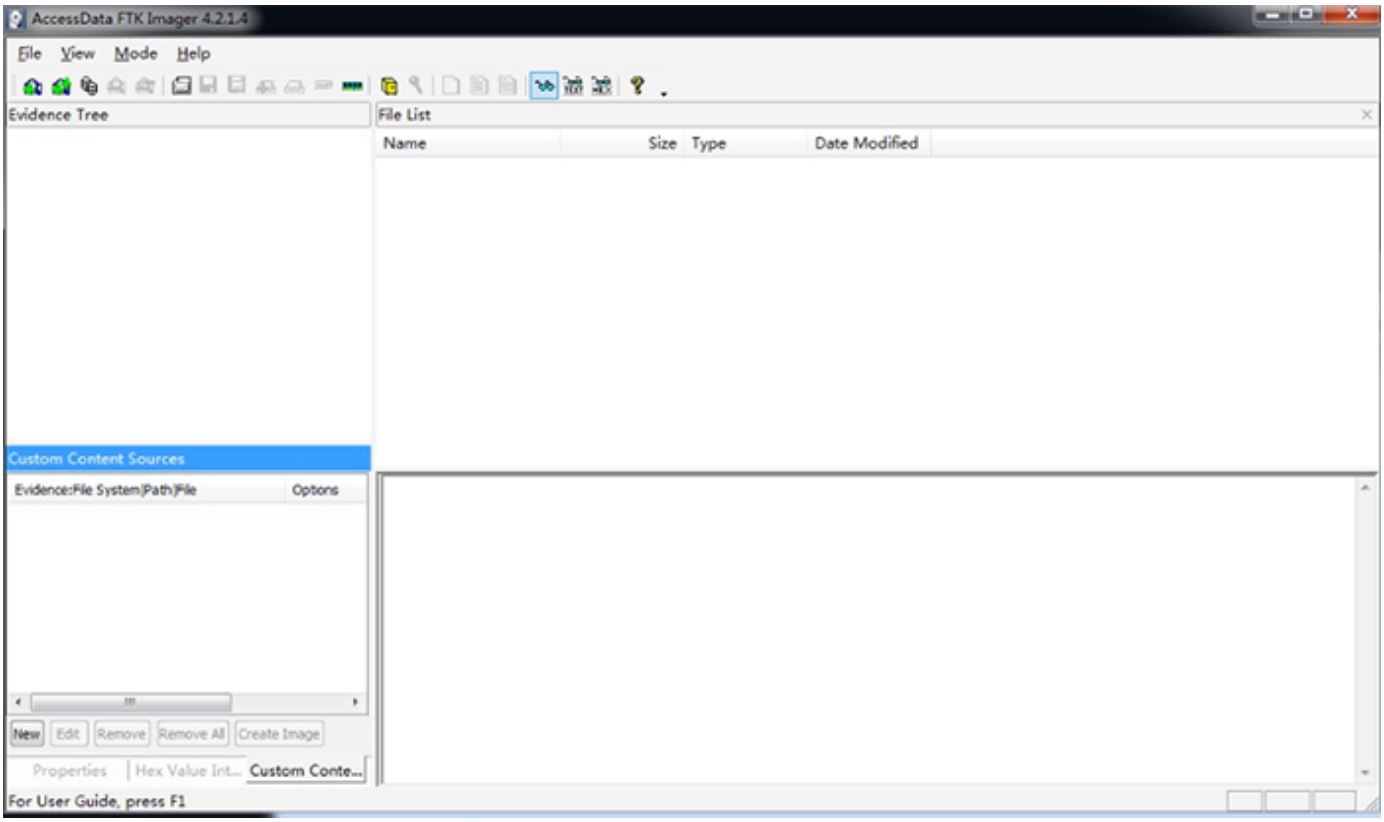
4、开始创建镜像，镜像备份的速度比dd真是快的太多了。



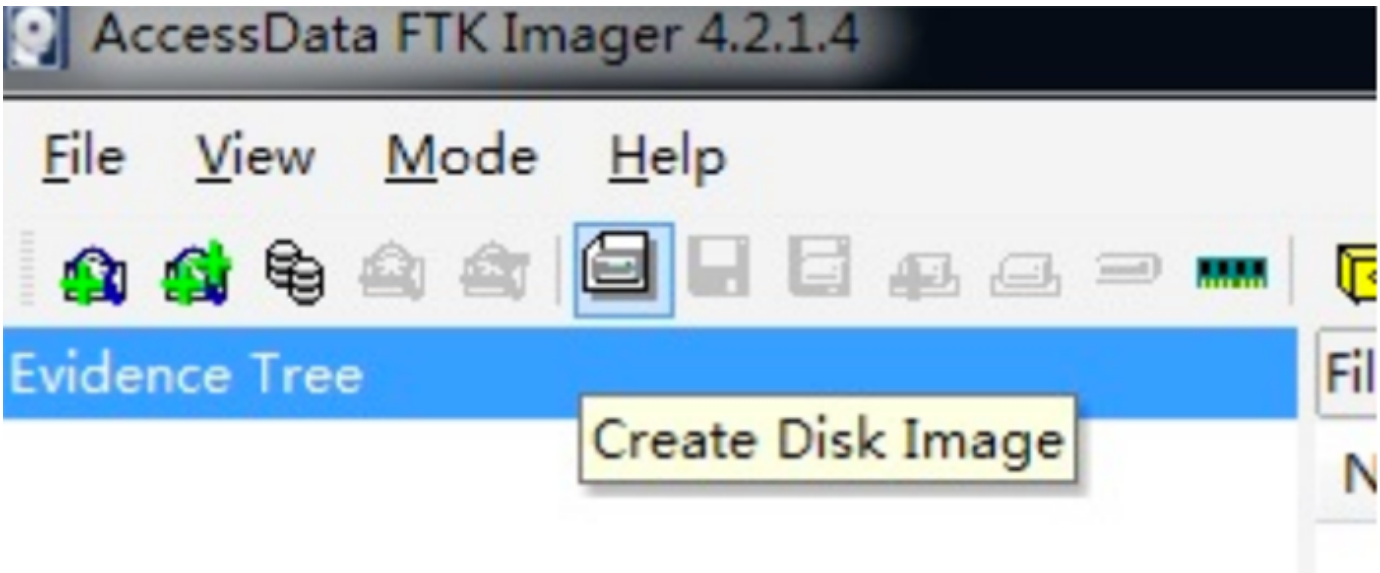
全盘备份5.8GB，要比guymager备份的文件容量多1GB，这个结果可能是受到了在线备份镜像的影响。

3.2.2 使用AccessData FTK Imager

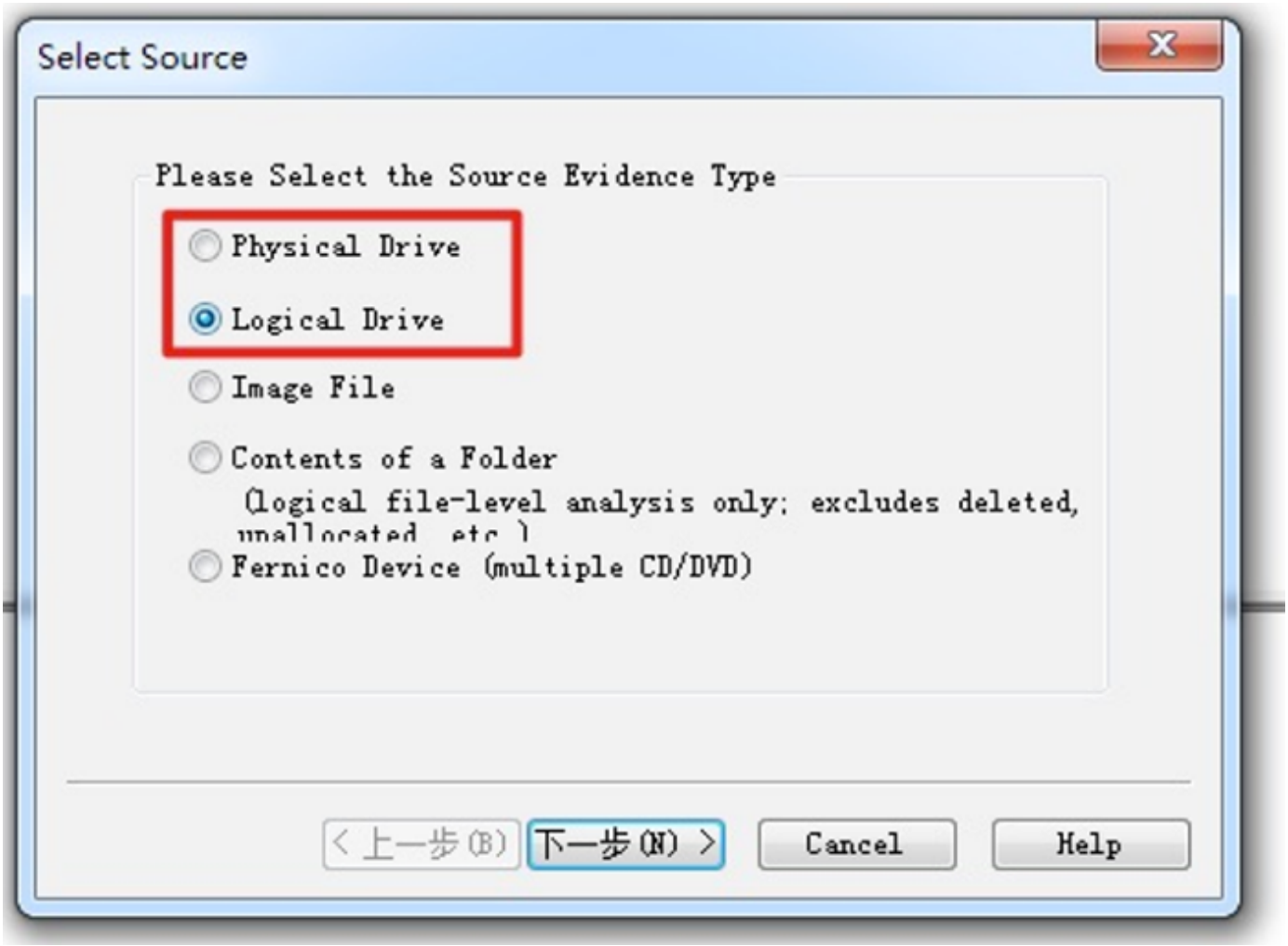
由于我找到的这个版本不支持32位系统，因此只能使用它在另外一台x64虚拟机做一个创建镜像的演示。（D盘环境存在相同的文件读写删除操作）

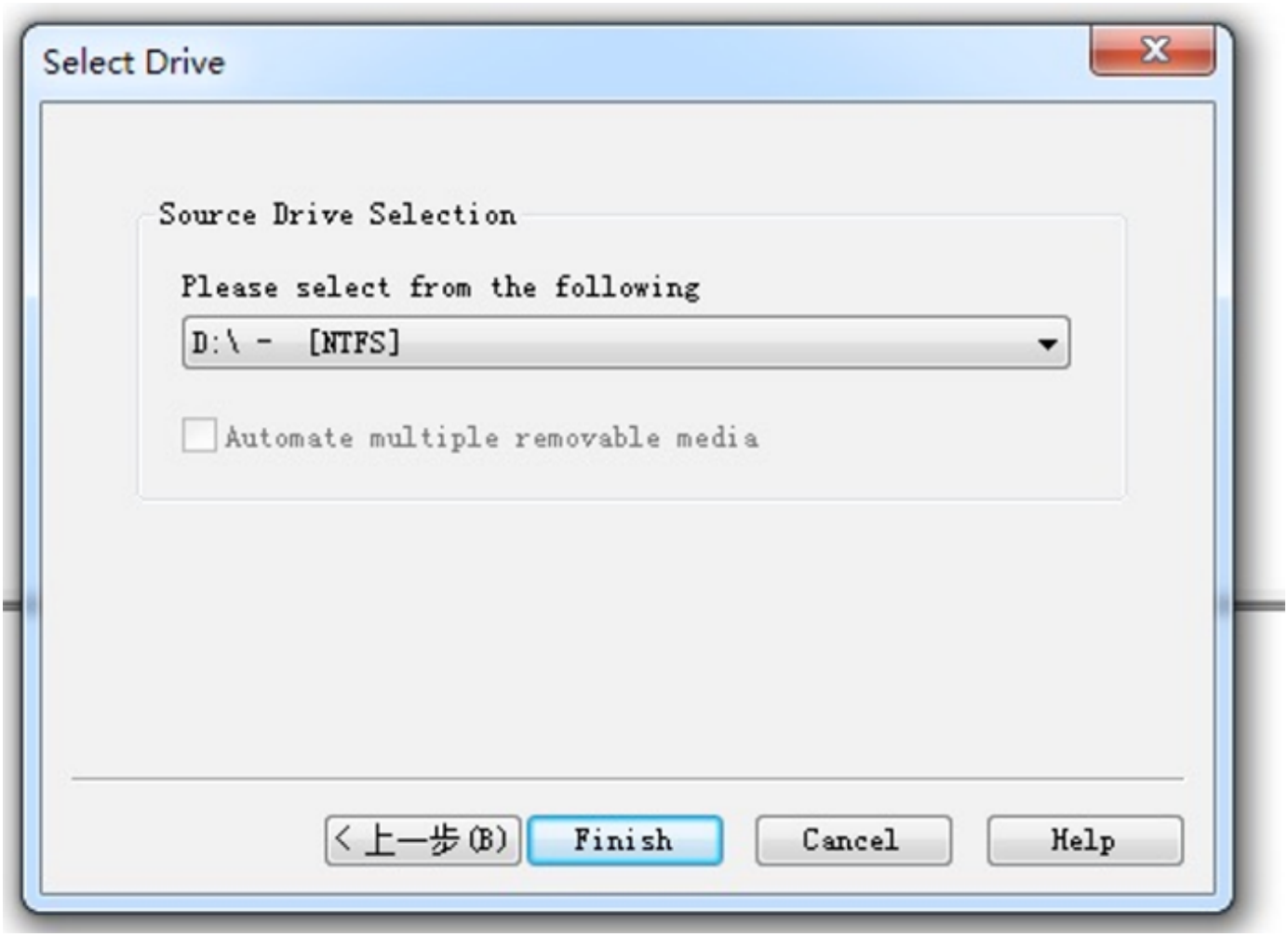


1、同样在工具栏选择Create Disk Image。

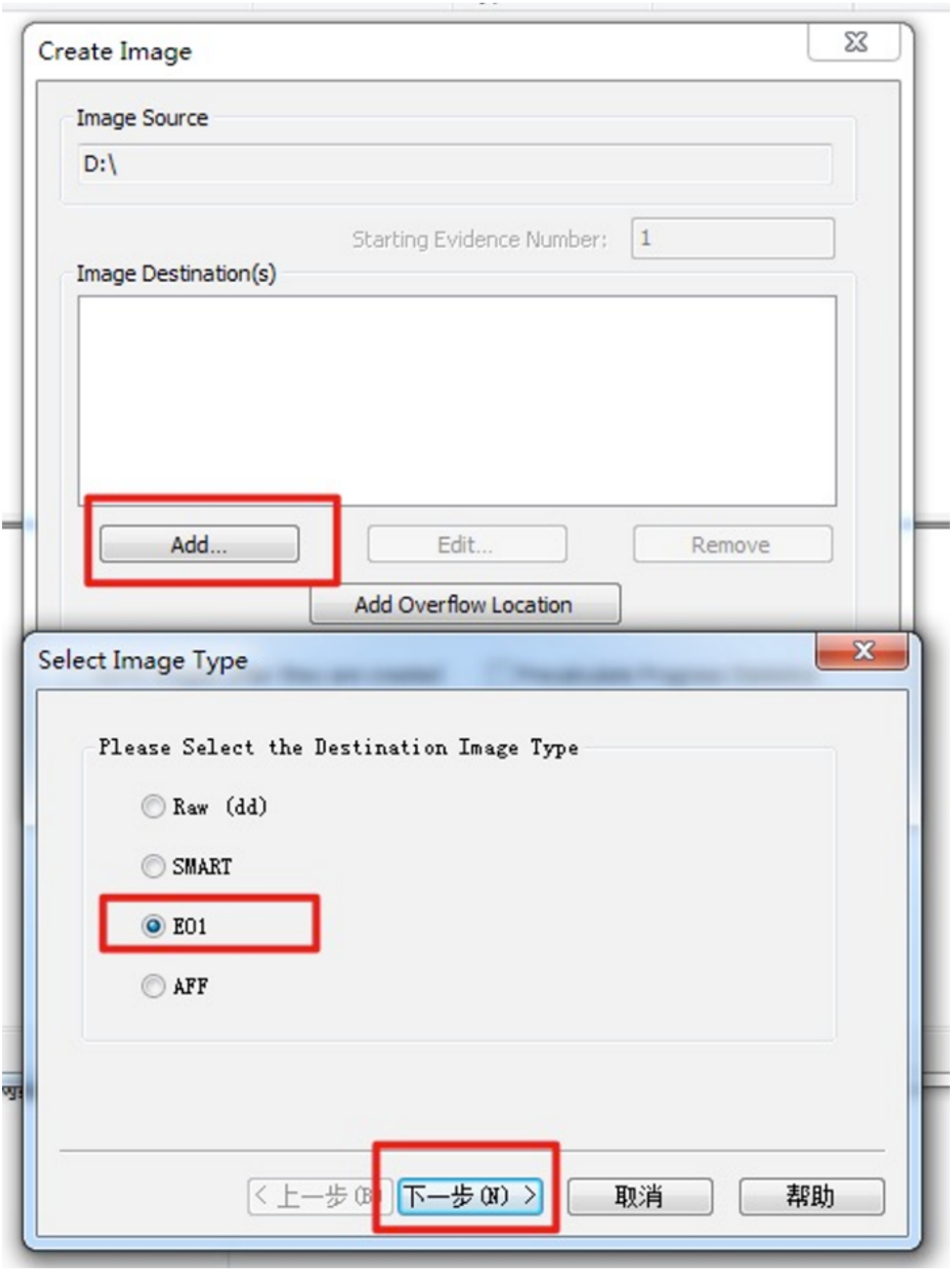


2、选择整个磁盘或分区，这里准备备份一个分区D盘。

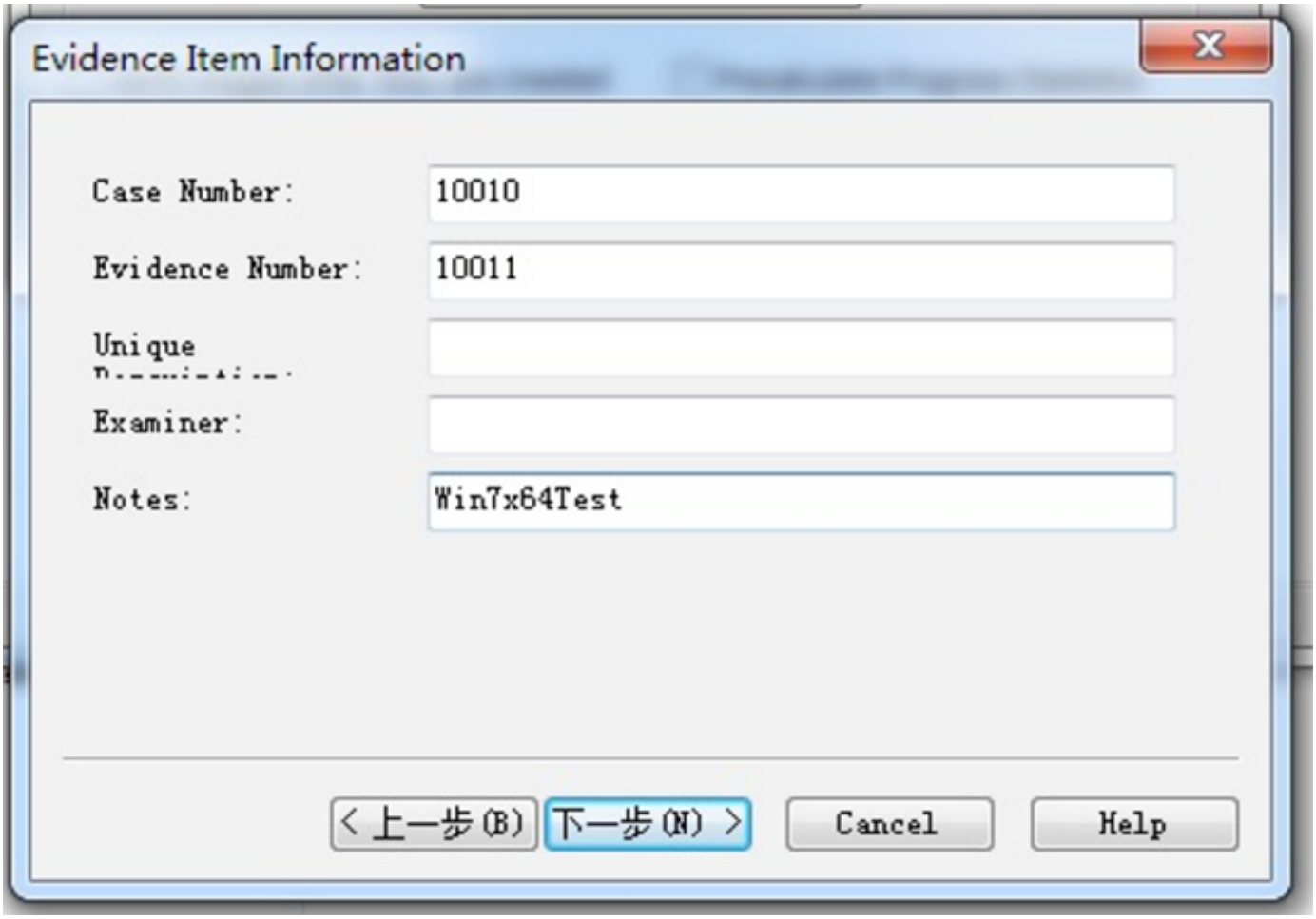

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted,
unallocated etc.)
Fernico Device (multiple CD/DVD)
< 上一步(B)
下一步(N) >
Cancel
Help


Select Drive
Source Drive Selection
Please select from the following
D:\ - [NTFS]
Automate multiple removable media
< 上一步(B)
Finish
Cancel
Help

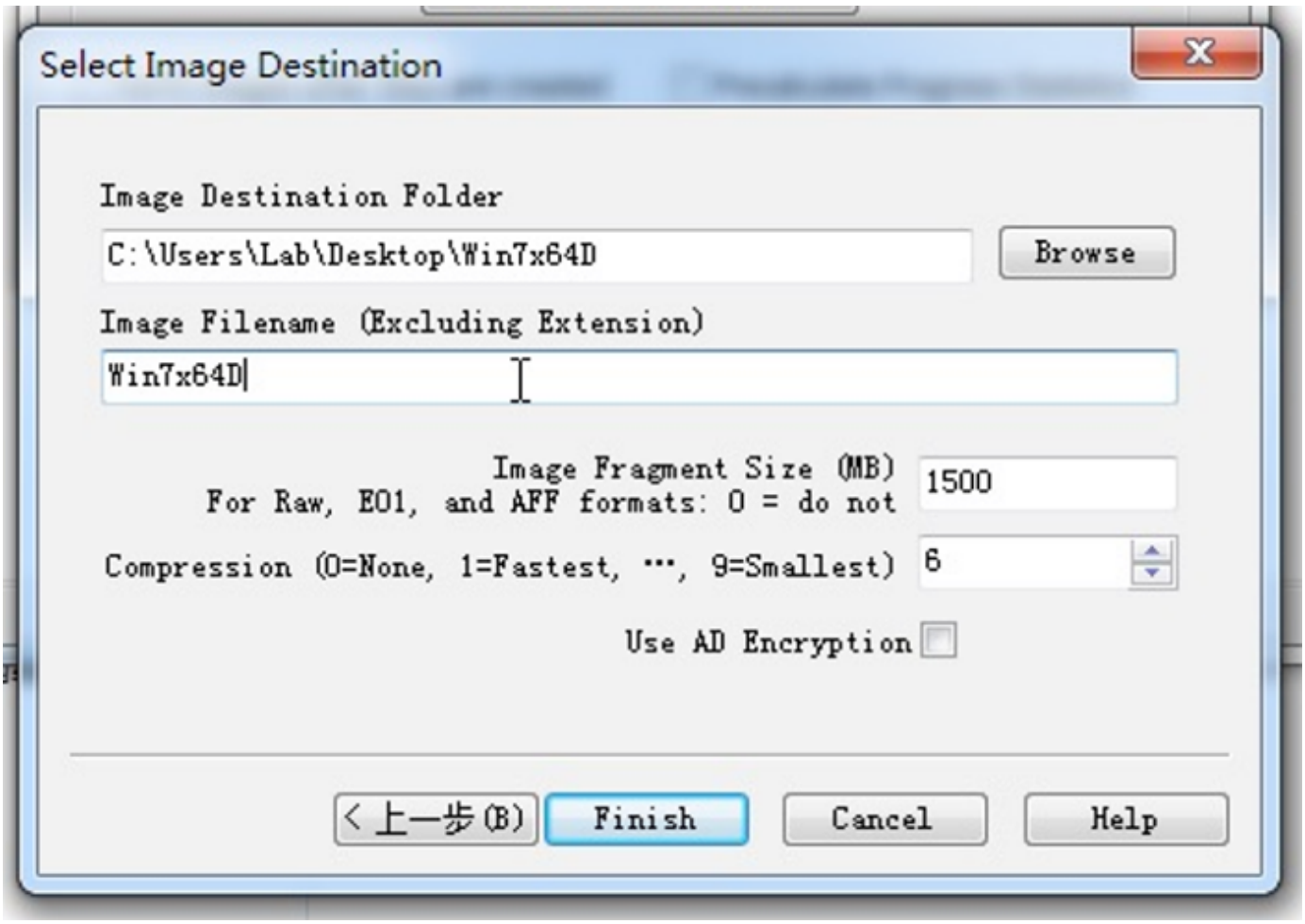
3、选择备份类型，这里不建议用Raw，那样就跟dd一样创建一个和磁盘大小一样的镜像，无视实际使用空间大小。

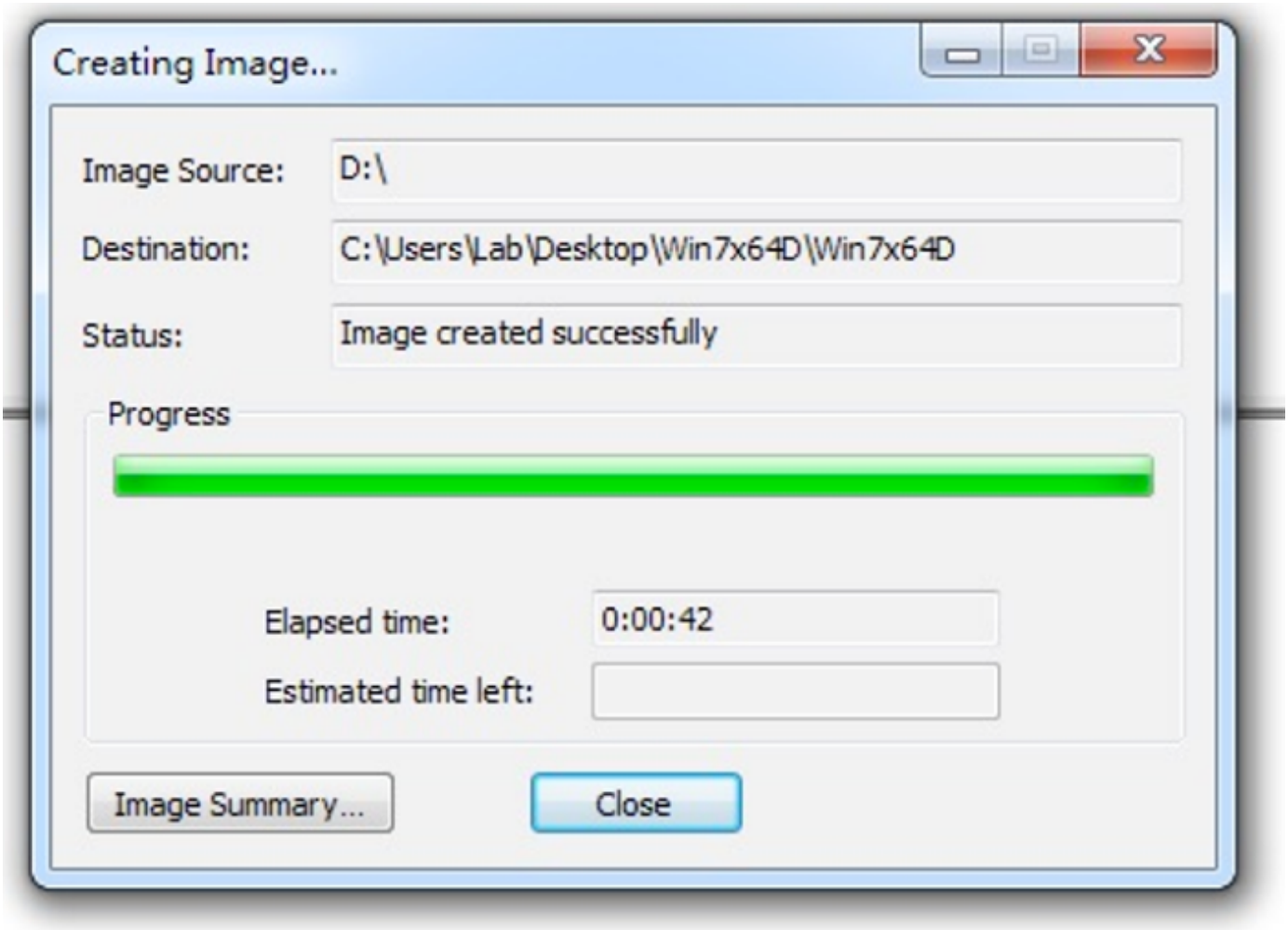


4、按需填写证据信息。

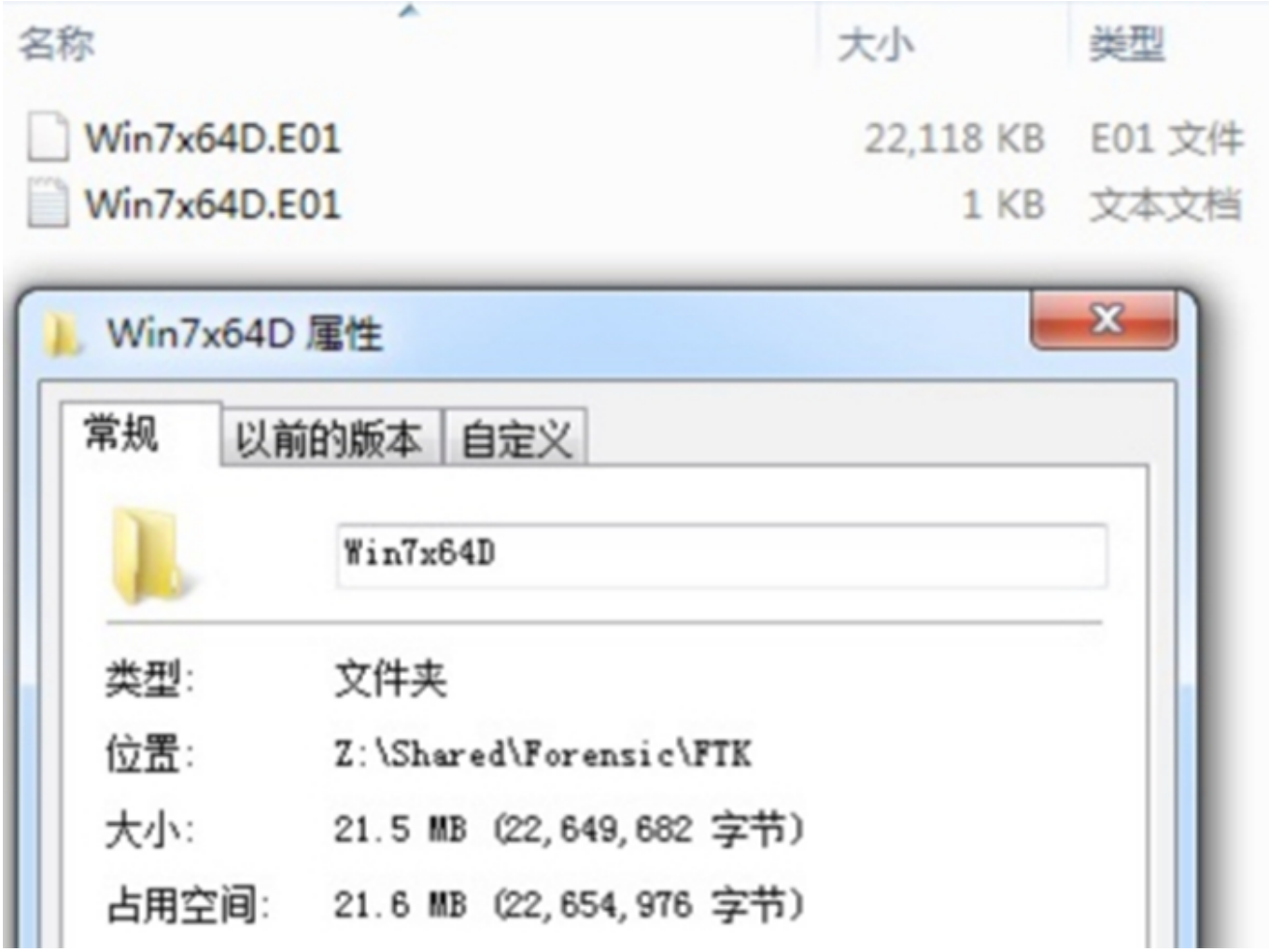


5、选择存储位置，之后开始创建镜像。





D盘镜像大小21.6MB（如果使用RAW格式，将会是10GB）。

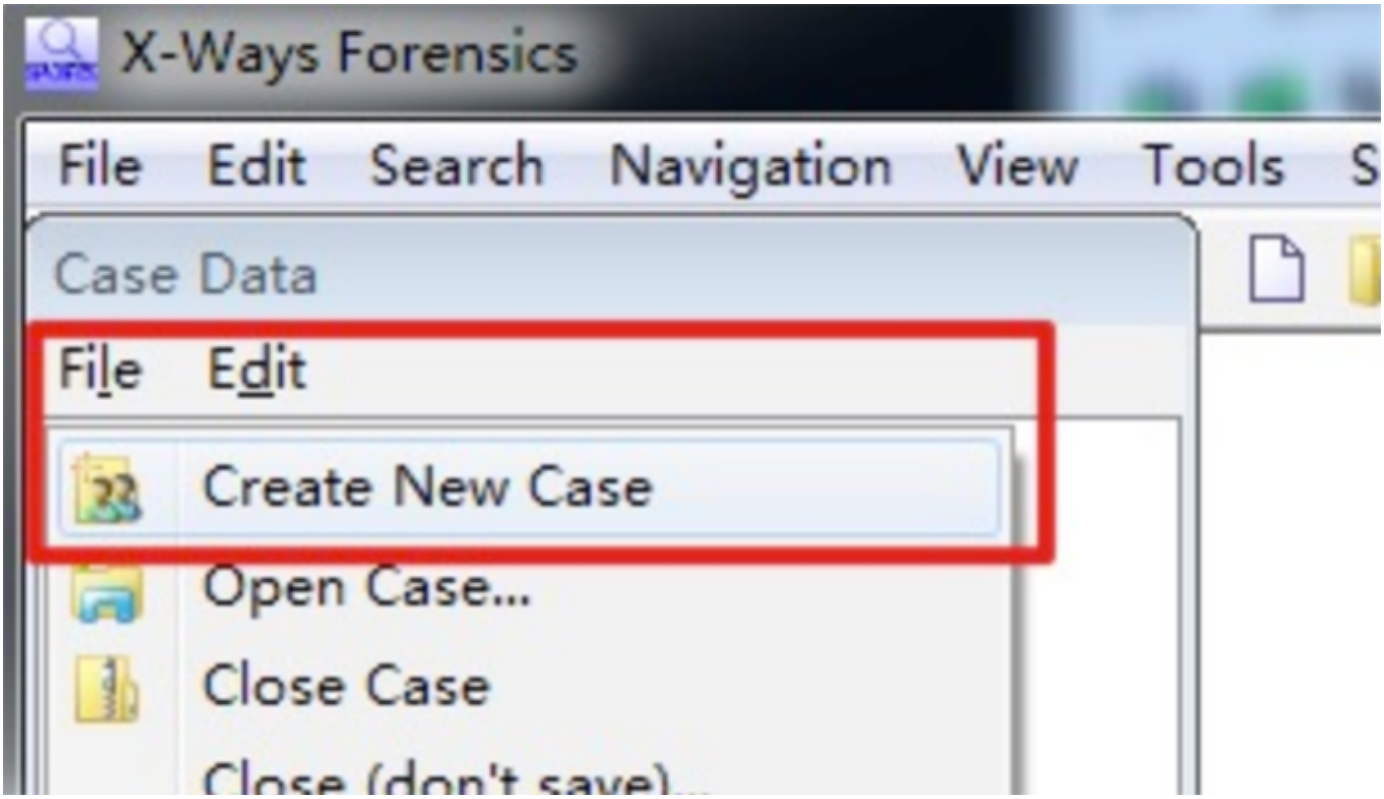


4 分析磁盘镜像

4.1 使用 X-Ways Forensics 分析证据

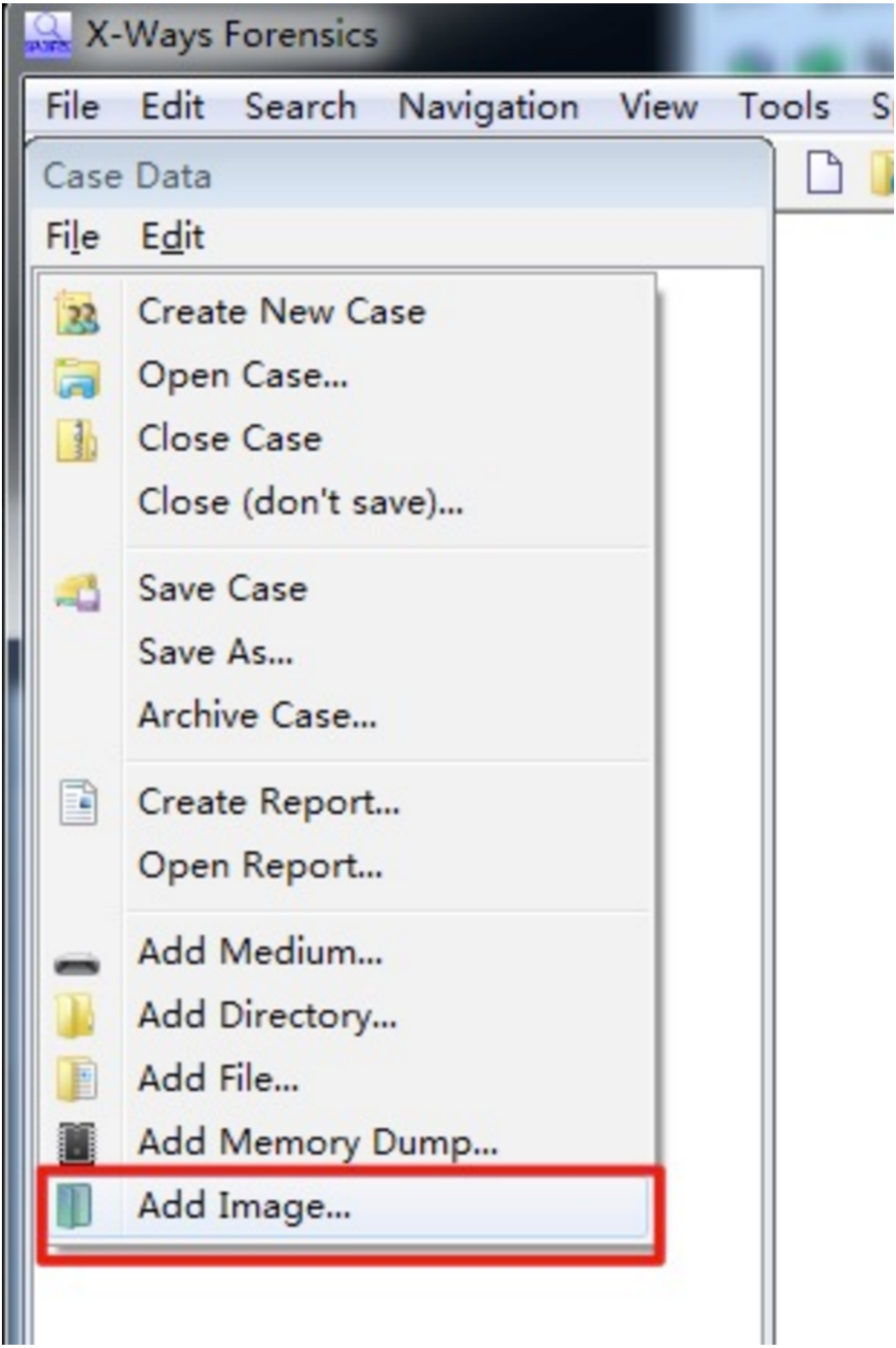
相较于FTK，X-Ways拥有更完善的案件、证据管理模式，可以保存案件后续再接着分析。

1、创建案件。

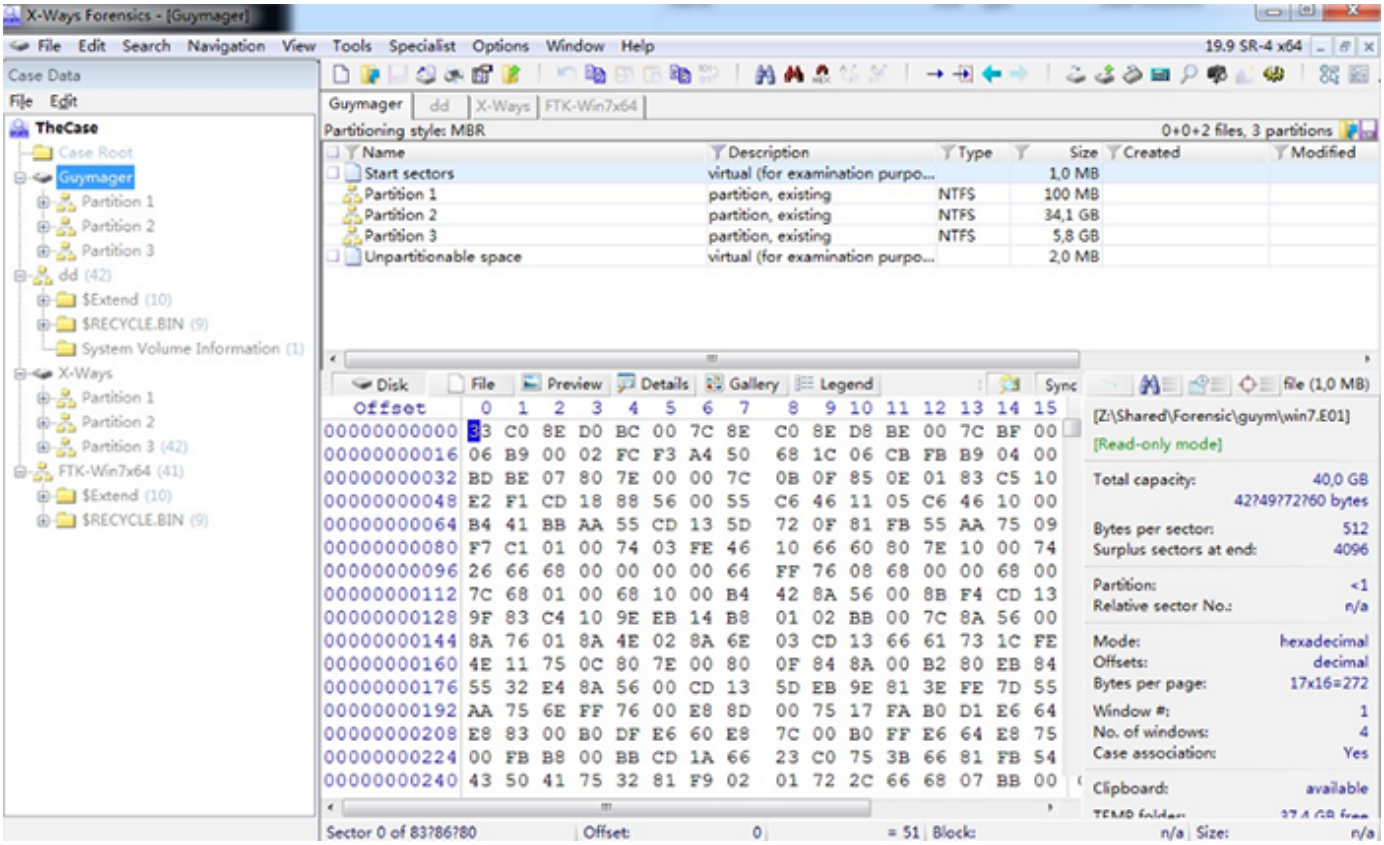


2、导入证据。

可以导入各类证据，这里选择镜像。

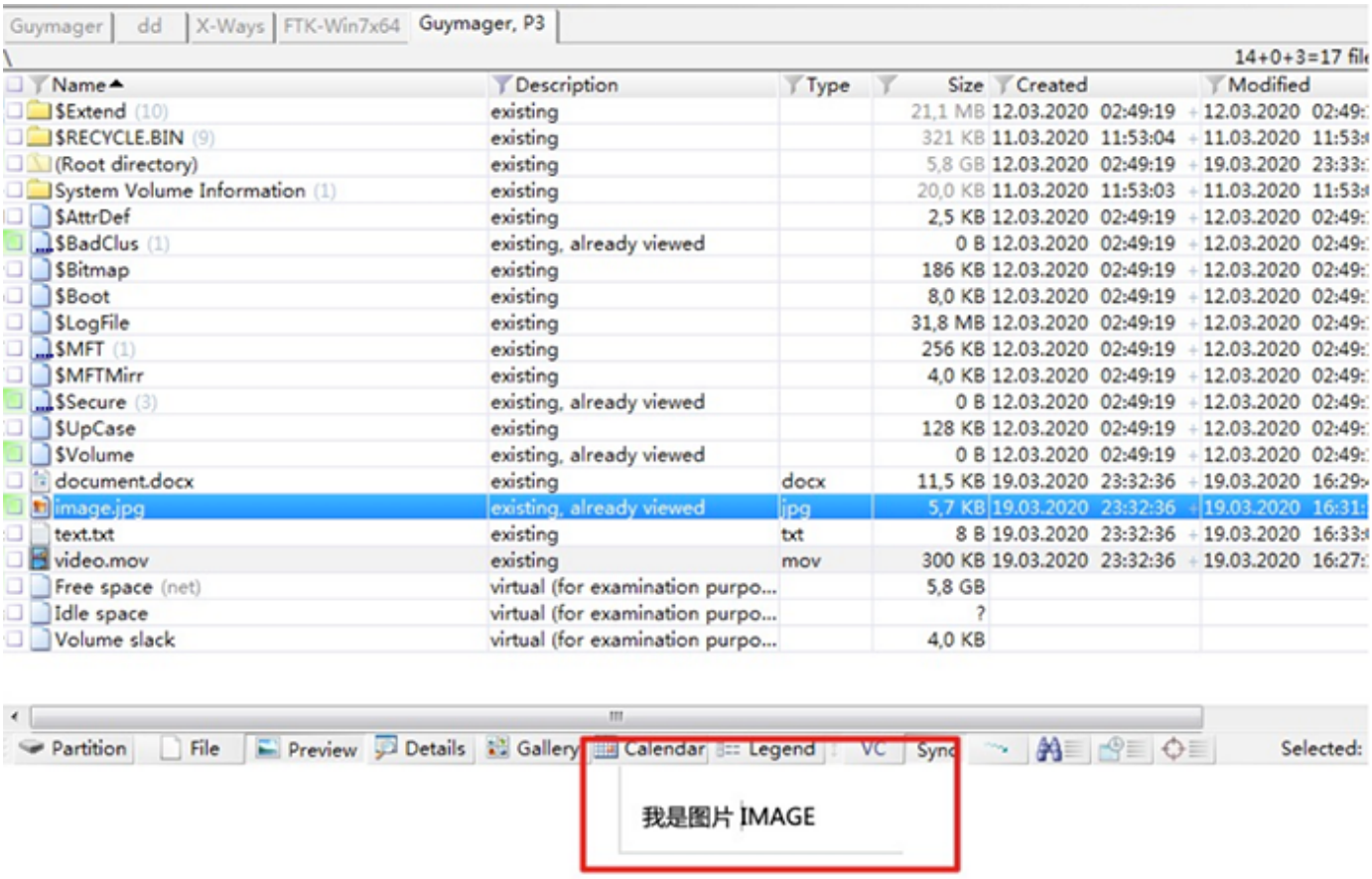

X-Ways Forensics
File Edit Search Navigation View Tools S
Case Data
File Edit
Create New Case
Open Case...
Close Case
Close (don't save)...
Save Case
Save As...
Archive Case...
Create Report...
Open Report...
Add Medium...
Add Directory...
Add File...
Add Memory Dump...
Add Image...

3、导入前面创建的4个镜像（包含两个全磁盘镜像、1个x86虚拟机的D盘、1个x64虚拟机的D盘）。



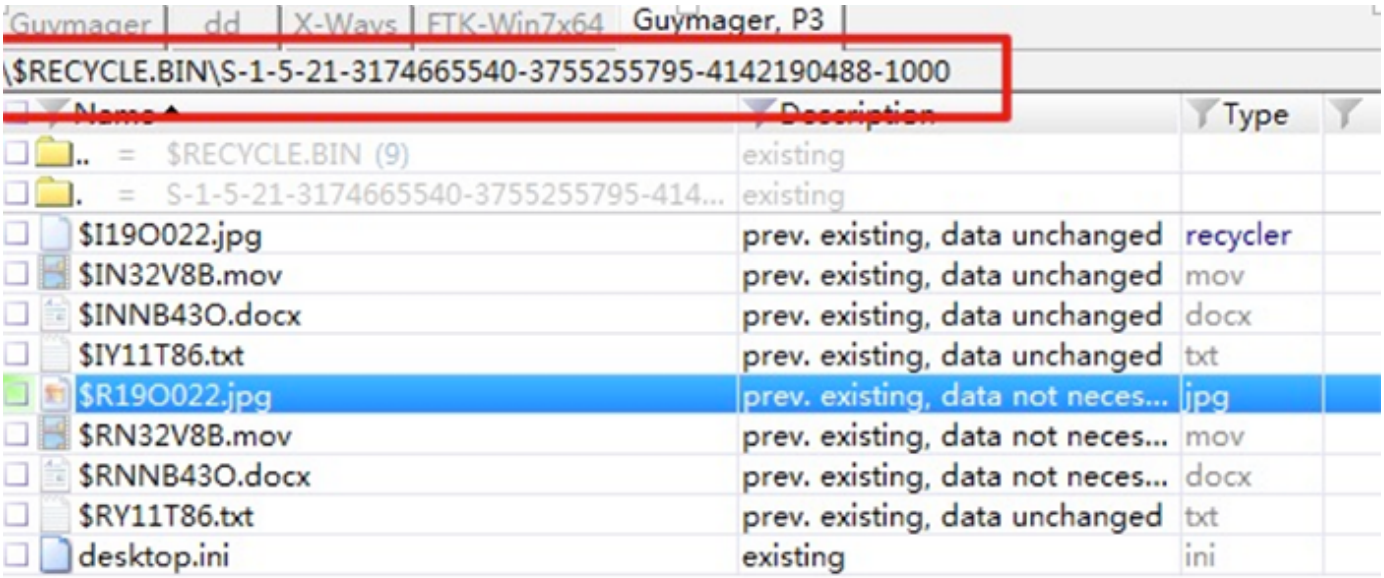
4、查看D盘里的文件 。

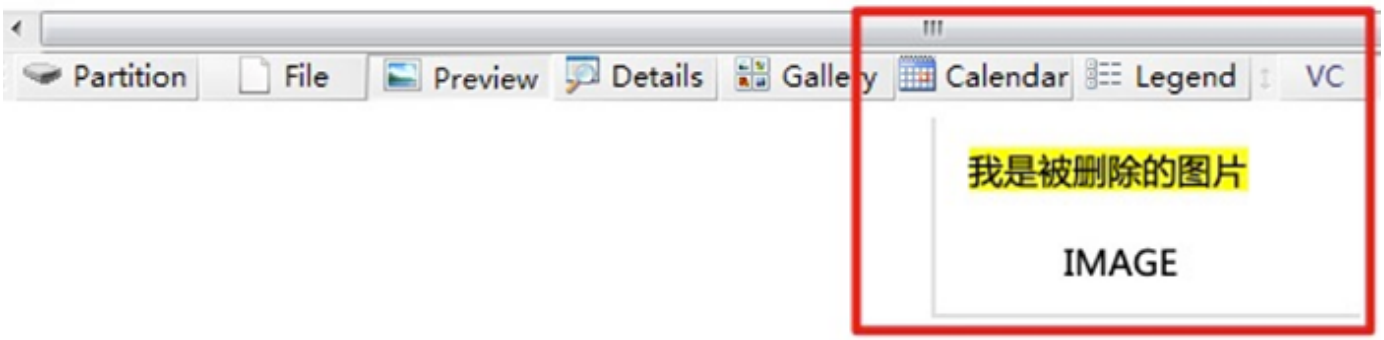
可以正常显示图片，但是这里没有看到被删除的文件（被删除的文件显示为半透明）。



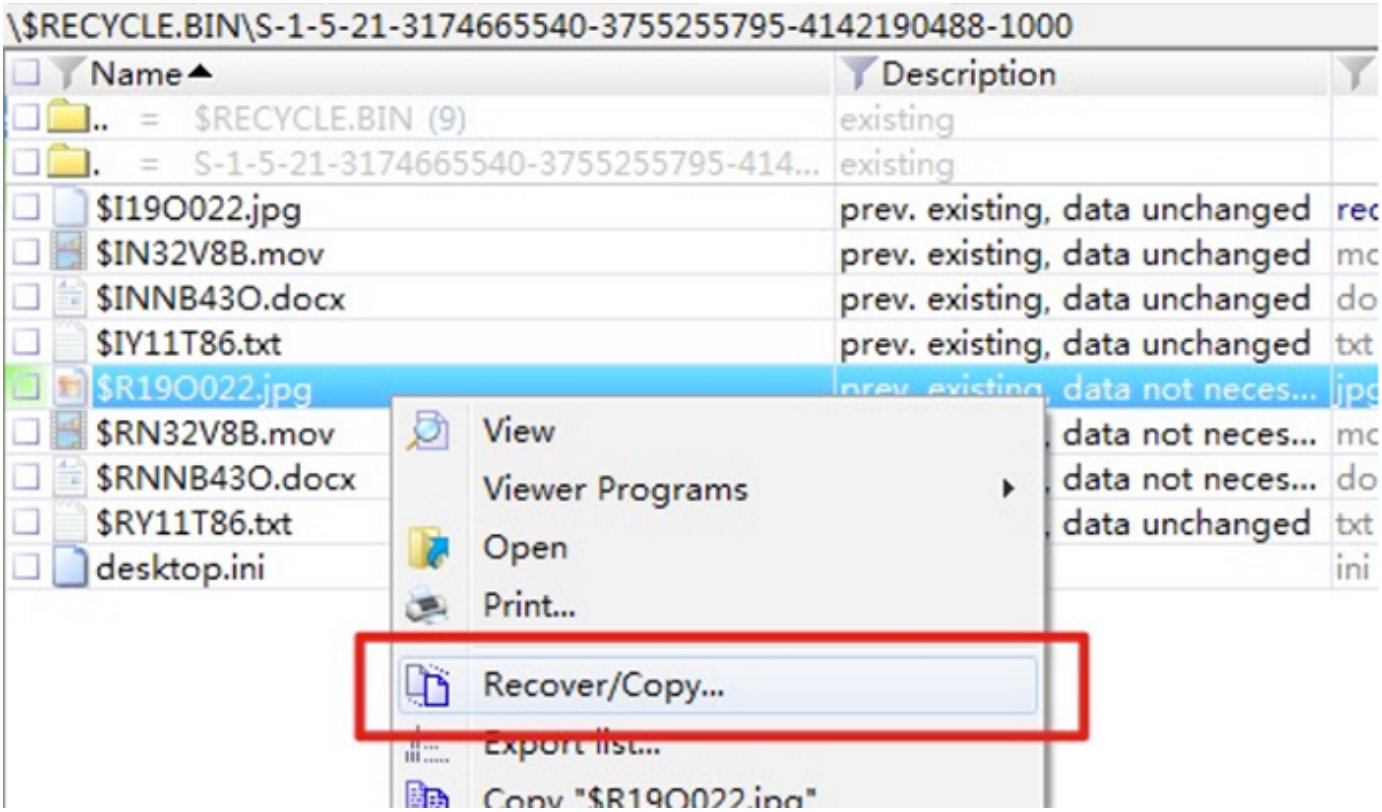
5、寻找被删除的文件。

由于删除时，是先del进入回收站，然后清空的，因此被删除的文件会在回收站的路径中。



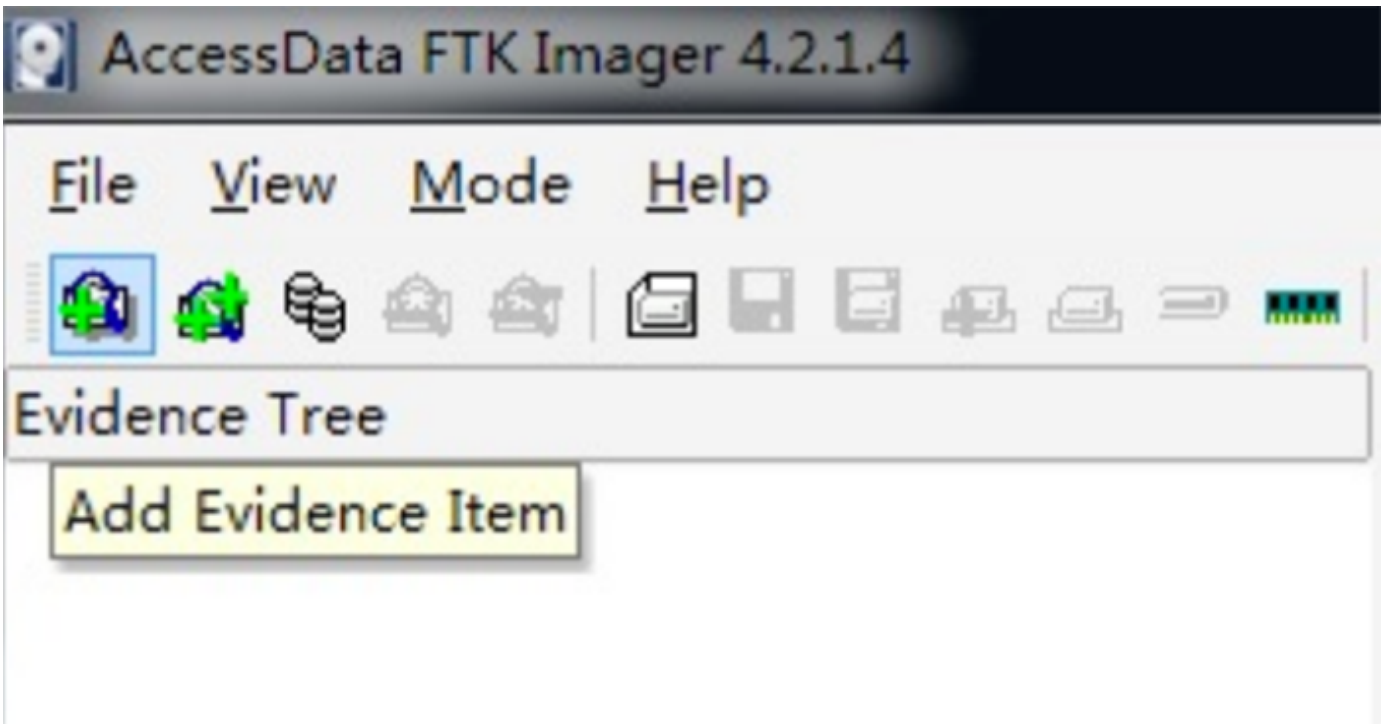


6、可以将镜像中有需要的文件恢复出来进一步分析。

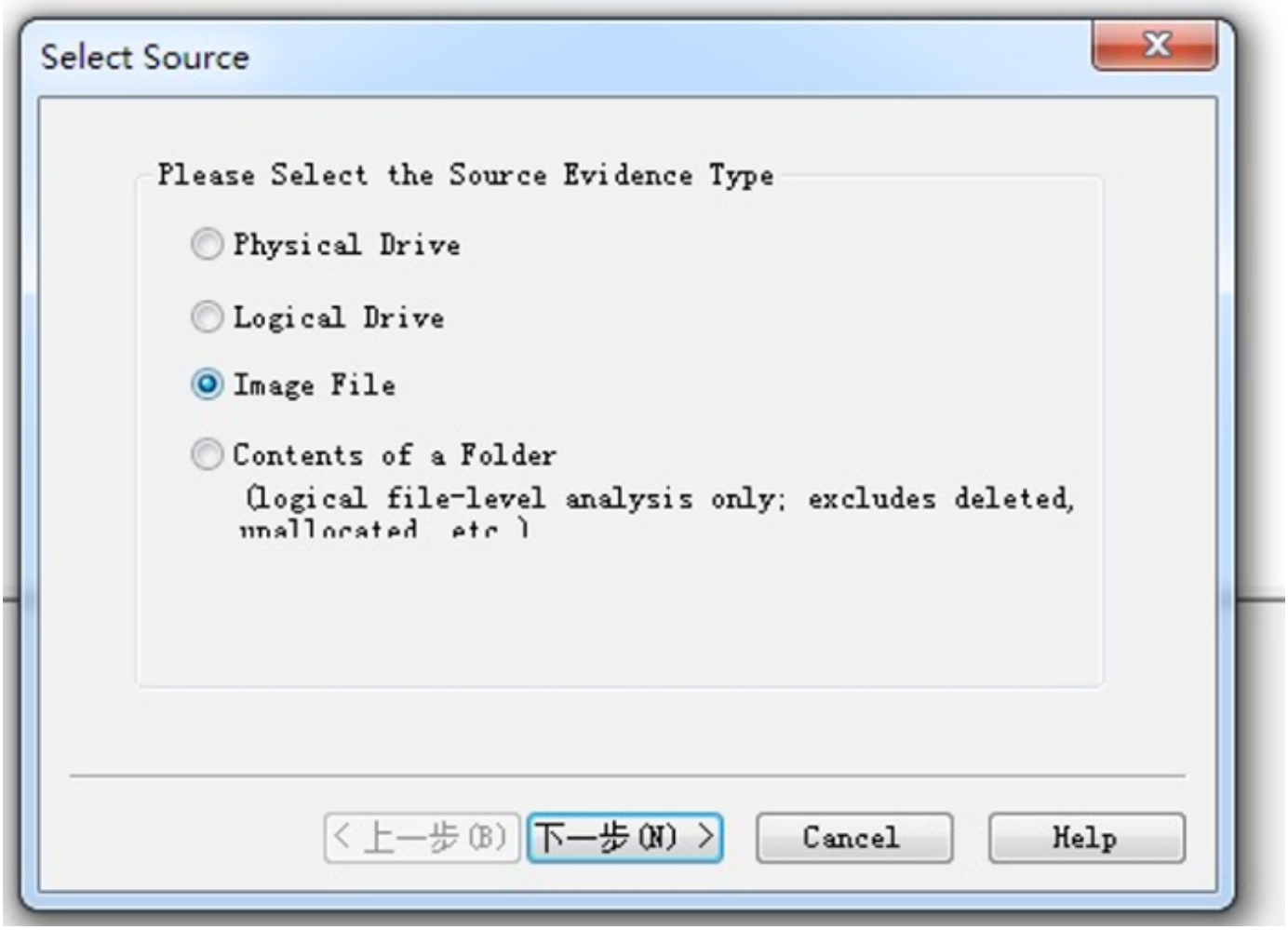


4.2 使用 AccessData FTK Imager 分析证据

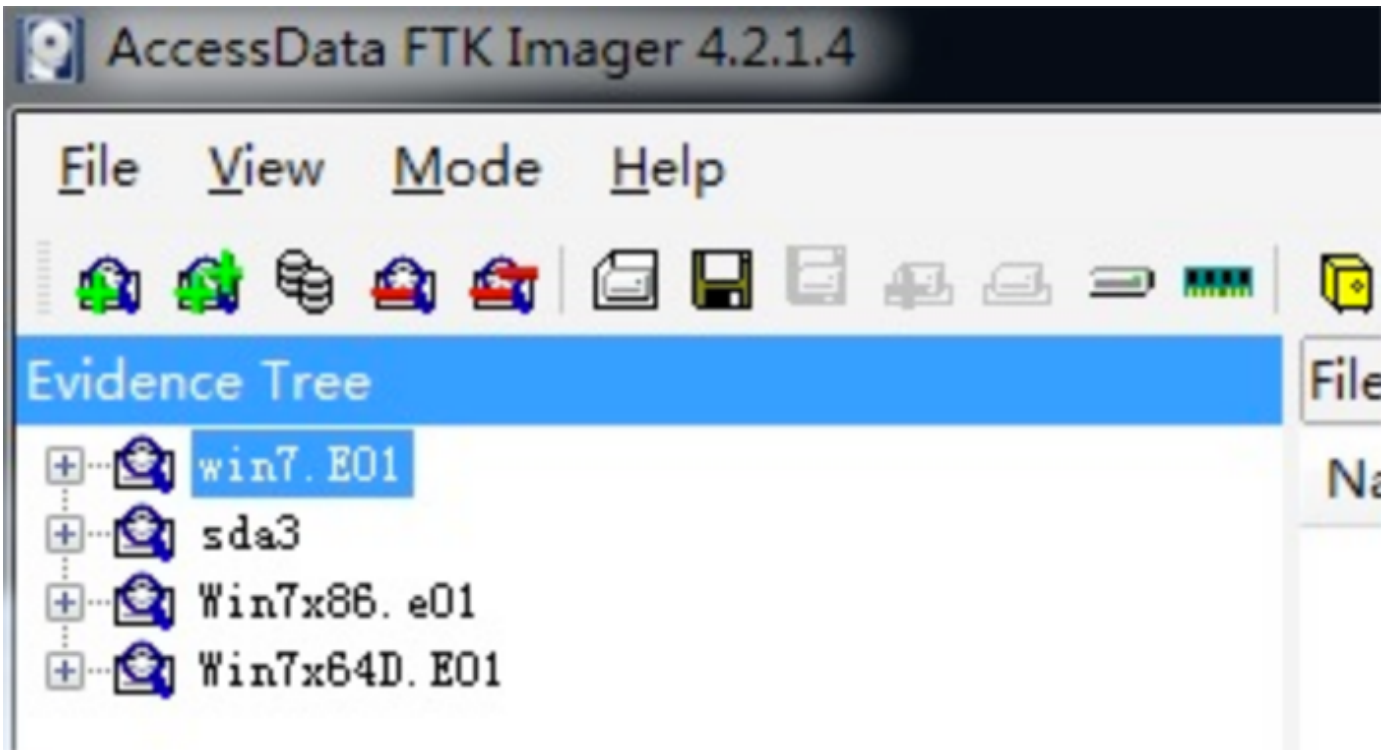
1、添加证据。



2、选择镜像文件，之后选择位置即可。

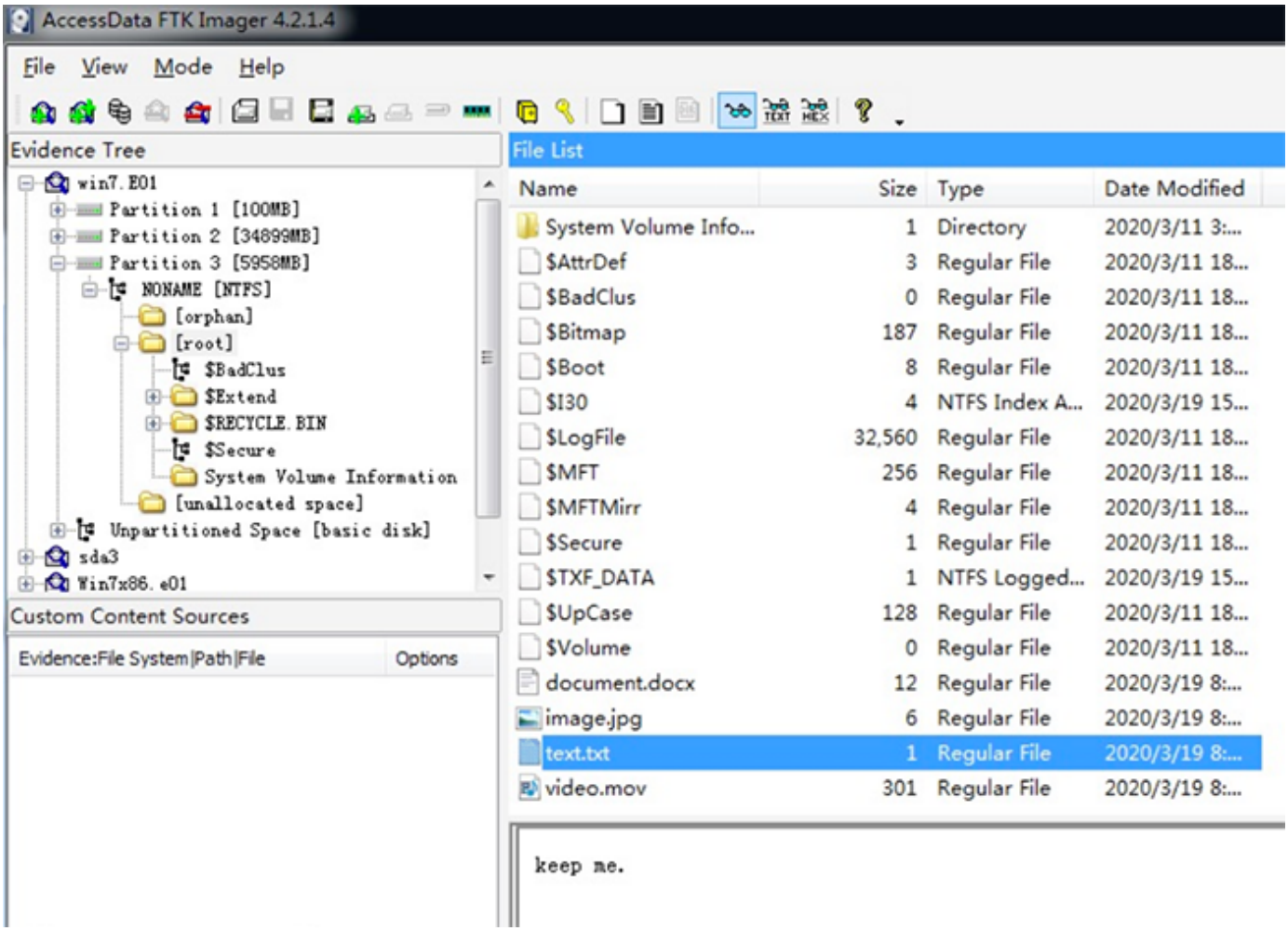


3、将4个镜像全部载入，这里不支持重命名。



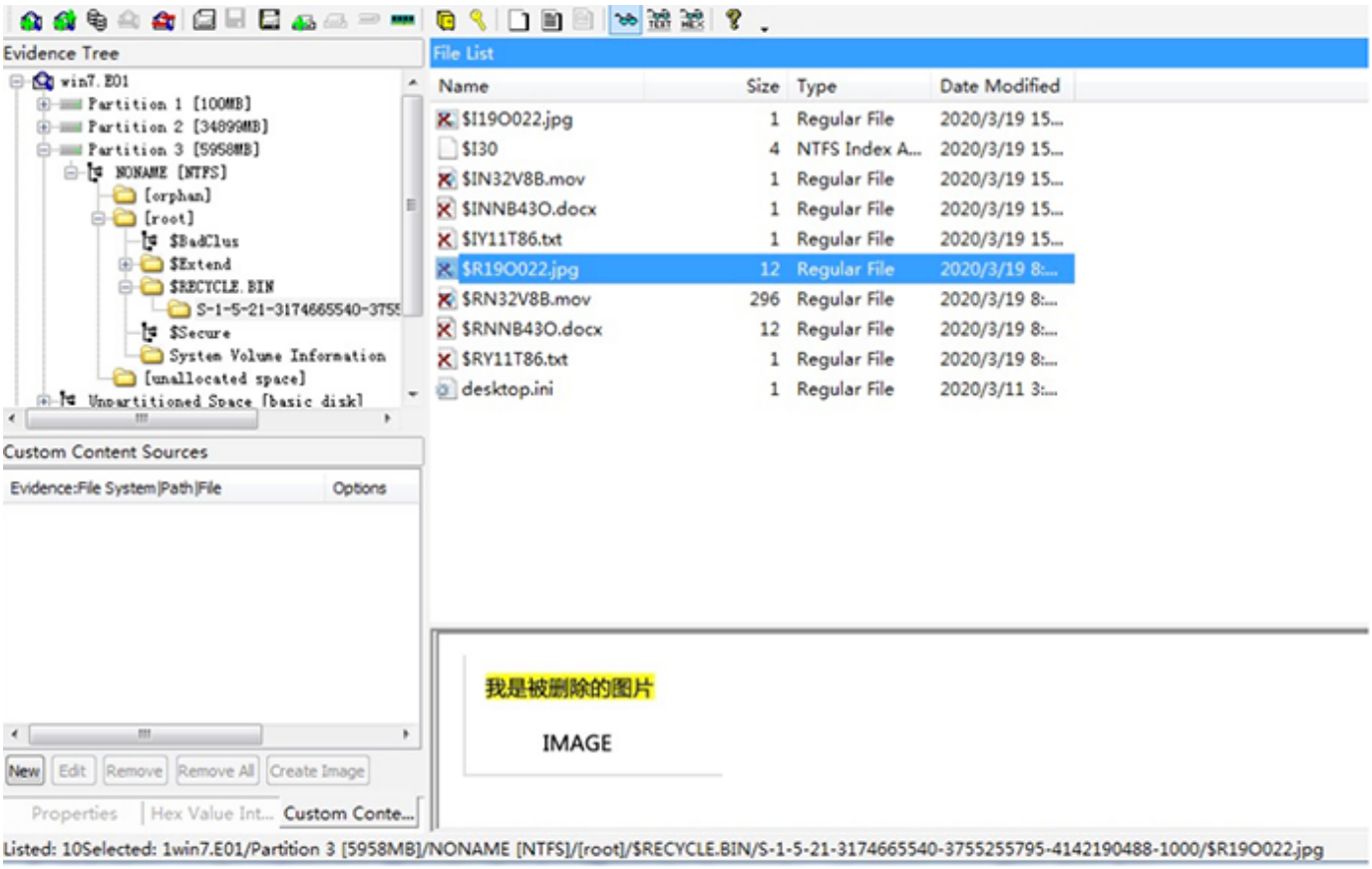
4、分析文件。

FTK同样可以直接预览txt、jpg



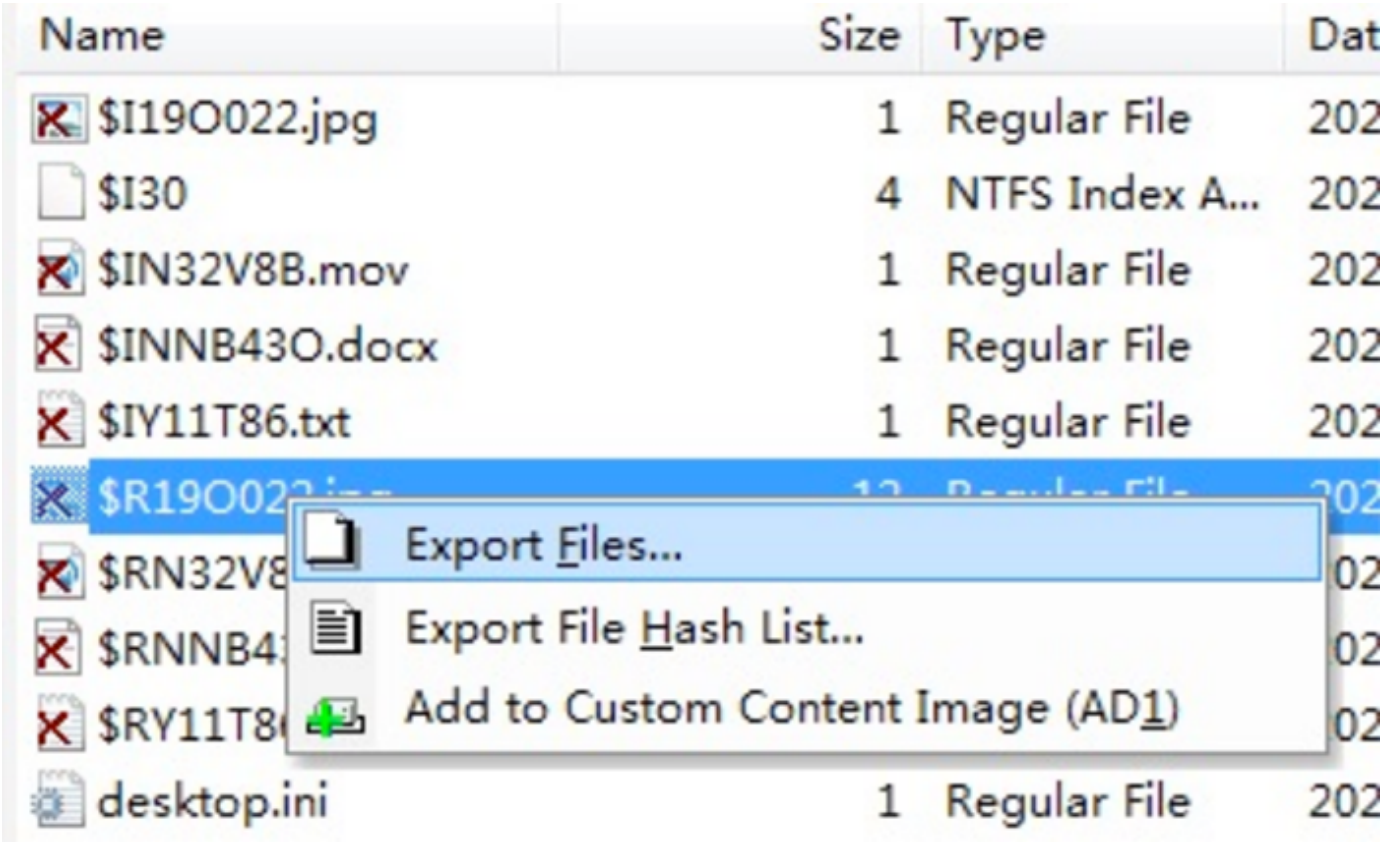
5、寻找被删除的文件。

同样到回收站目录下寻找被清空的文件，这里是使用红叉表示其被删除了。



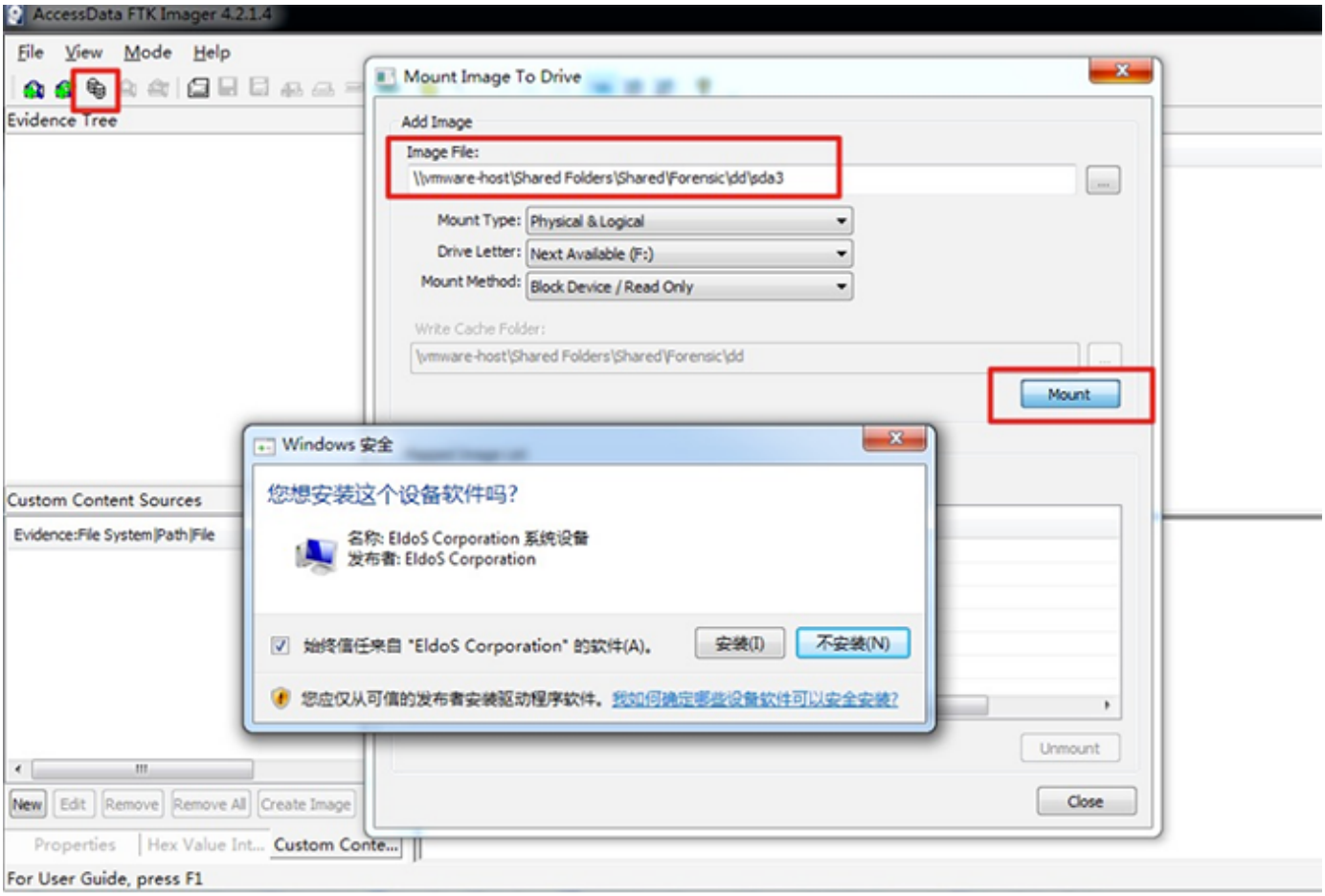
6、导出文件。

FTK同样可以导出镜像内的文件。



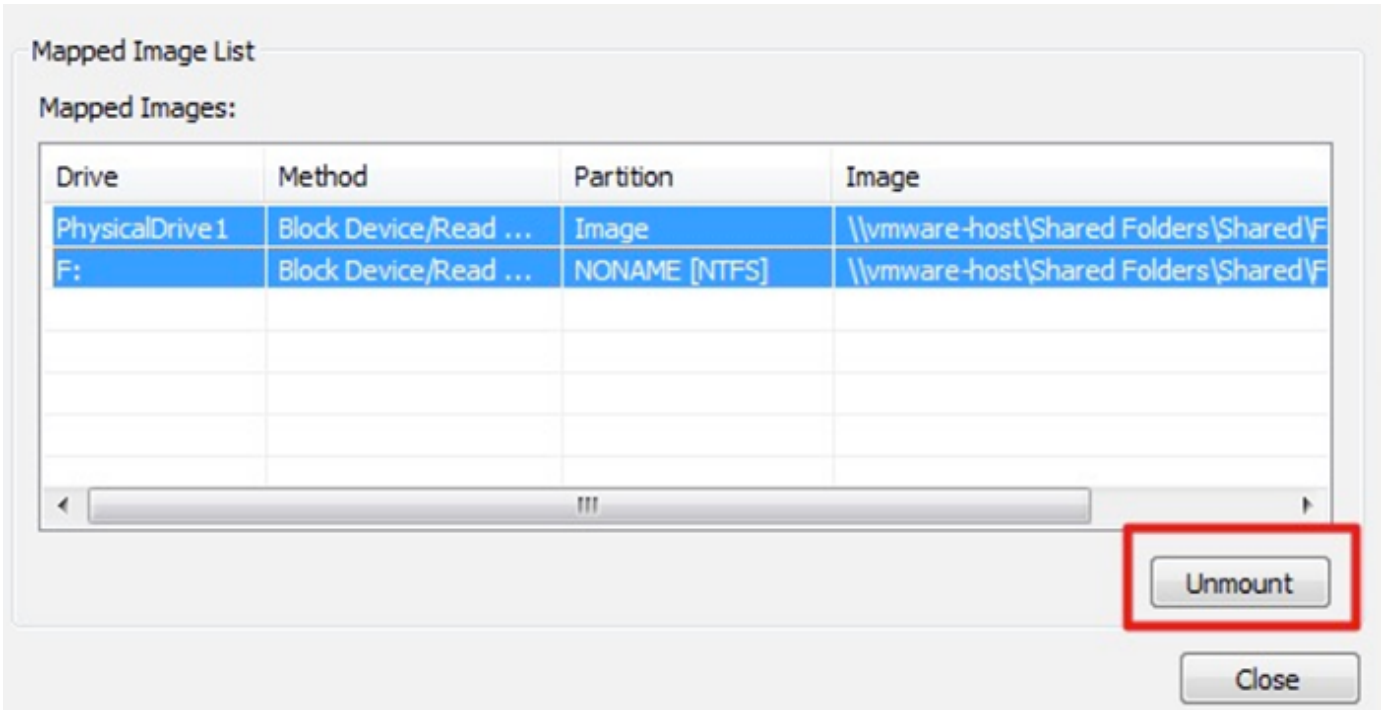
磁盘镜像挂载

1、FTK有个特殊功能，可以把磁盘镜像映射为一个虚拟磁盘。



2、这样就多了一个和win7x86主机里一样的分区。

3、不用的时候unmount即可。



5 快速提取镜像内的文件

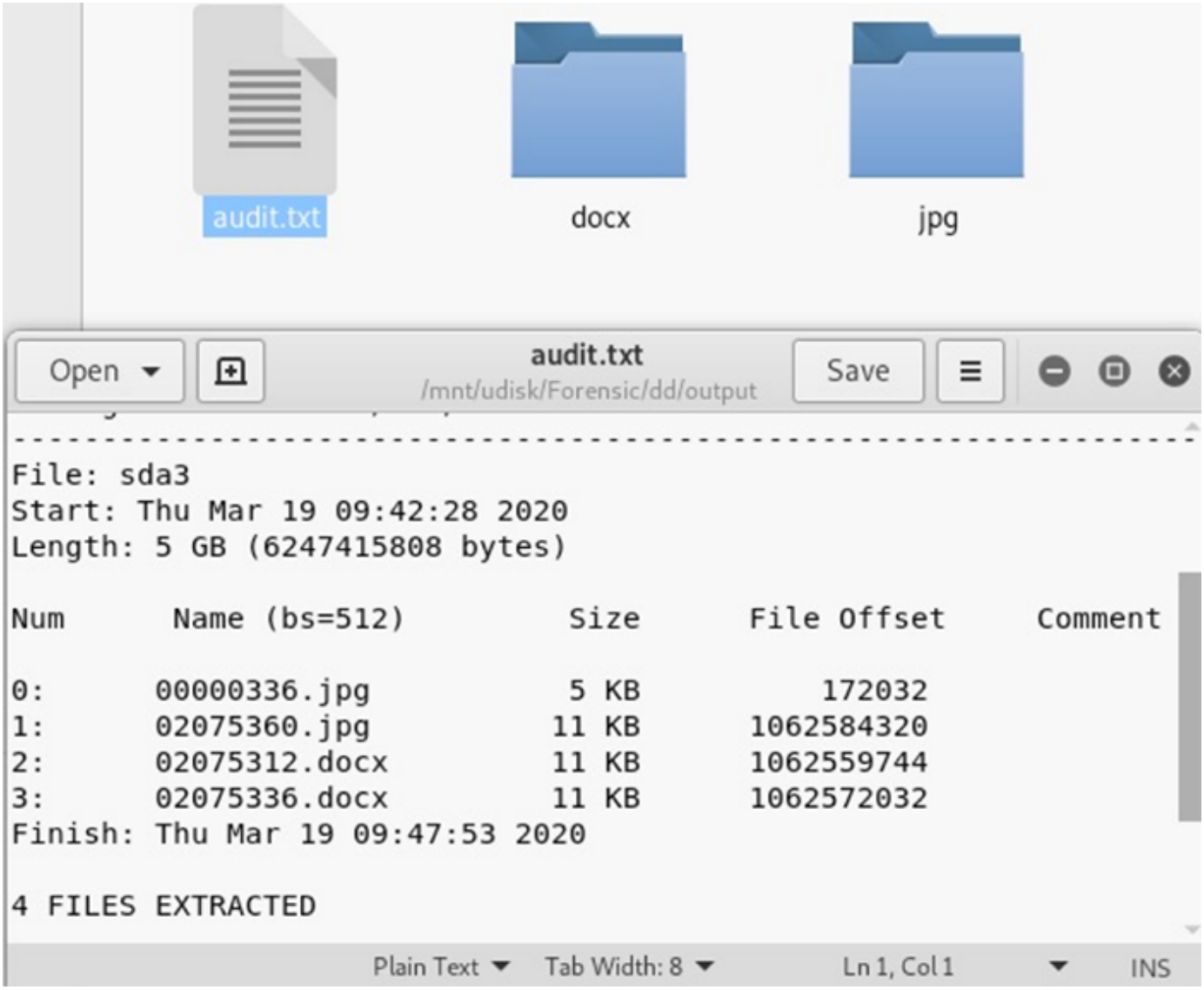
使用 foremost 提取磁盘映像里的文件。

```
foremost -t all -i sda3
```

-i 指定镜像文件
-t 指定文件类型
all 是所有支持的类型，具体支持的类型查看man。

运行结果：

经过测试，jpg、mov、txt、docx四种类型的文件，只能提取到docx和jpg两种格式的文件。


audit.txt
docx
jpg
Open
audit.txt
/mnt/udisk/Forensic/dd/output
Save
File: sda3
Start: Thu Mar 19 09:42:28 2020
Length: 5 GB (6247415808 bytes)
Num Name (bs=512) Size File Offset Comment
0: 00000336.jpg 5 KB 172032
1: 02075360.jpg 11 KB 1062584320
2: 02075312.docx 11 KB 1062559744
3: 02075336.docx 11 KB 1062572032
Finish: Thu Mar 19 09:47:53 2020
4 FILES EXTRACTED
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队