# 内存取证相关总结

## **Volatility的常见使用方法**

我们做MISC的时候，取证是一个不可避免的板块，这一篇首先讲一下内存取证，这是我们在做misc时的一个难点，在做内存取证的时候，volatility是我们必需要用到的一个工具，基本上绝大部分的题都是使用这个软件。

Volatility是一款开源内存取证框架，能够对导出的内存镜像进行分析，通过获取内核数据结构，使用插件获取内存的详细情况以及系统的运行状态。它时一个开源的软件，使用Python编写，易于和基于python的主机防御框架集成。

工具地址： https://github.com/volatilityfoundation/volatility

那么我们主要介绍一些它的常用使用命令：

****下载volatility****

apt-get install volatility

****imageinfo****

识别操作系统：

volatility -f example.raw imageinfo

****pslist/pstree/psscan****

扫描进程：

volatility -f example.raw --profile=Win7SP1x64 pslist #win7SP1x64为操作系统

****filescan****

扫描文件：

volatility -f example.raw --profile=Win7SP1x64 filescan | grep -E 'txt|png|jpg|gif|zip|rar|7z|pdf|doc'

volatility -f example.raw --profile=Win7SP1x64 filescan | grep TMP\_User #搜索指定文件夹下的文件

****Dumpfiles****

volatility -f wuliao.data --profile=Win7SP1x64 dumpfiles -Q 0x000000007f142f20 -D ./ -u

****dumpfile/memdump****

导出文件：

volatility -f example.raw --profile=Win7SP1x64 memdump -p [PID] -D ./ # -D ./ 导出到当前目录

or

volatility -f example.raw --profile=Win7SP1x64 dumpfiles -Q [Offset] -D ./

****提取系统的账号密码****

volatility -f win7.raw --profile=Win7SPIx64 hashdump

****查看网络通信连接****

volatility -f win7.raw --profile=Win7SPIx64 netscan |grep ESTABLISHED

****查看cmd历史记录****

volatility -f win7.raw --profile=Win7SPIx64 cmdscan

****分割dmp文件****

foremost 352.dmp

****找出注入的可执行代码或者DLL****

vol.py -f <镜像文件> --profile=[profile文件] malfind -p[pid]

**导出程序**

vol.py -f <镜像文件> --profile=[profile文件] prodump -p [pid1,pid2,..pidn] -D [目录]

**查看恶意的钩子**

vol.py -f <镜像文件> --profile=[profile文件] apihooks -p[pid]

****追踪****

vol.py -f <镜像文件> --profile=[profile文件] volshell -p[pid]

****检查恶意驱动程序****

vol.py -f <镜像文件> --profile=[profile文件] modules

****提取驱动程序****

vol.py -f <镜像文件> --profile=[profile文件] moddump -D [目录] --base [base地址]

****检查驱动内核回调****

vol.py -f <镜像文件> --profile=[profile文件] callbacks

****检查恶意注册表项****

vol.py -f <镜像文件> --profile=[profile文件] printkey

****查看服务****

vol.py -f <镜像文件> --profile=[profile文件] svcscan

## **依赖**

如果只是用Volatility本体的话，这些依赖是没必要装的，但是如果你想用某些插件，还是把以下这些必备的依赖包装上吧。因为插件也是这个软件的一大特点。

**Distorm3:**牛逼的反编译库

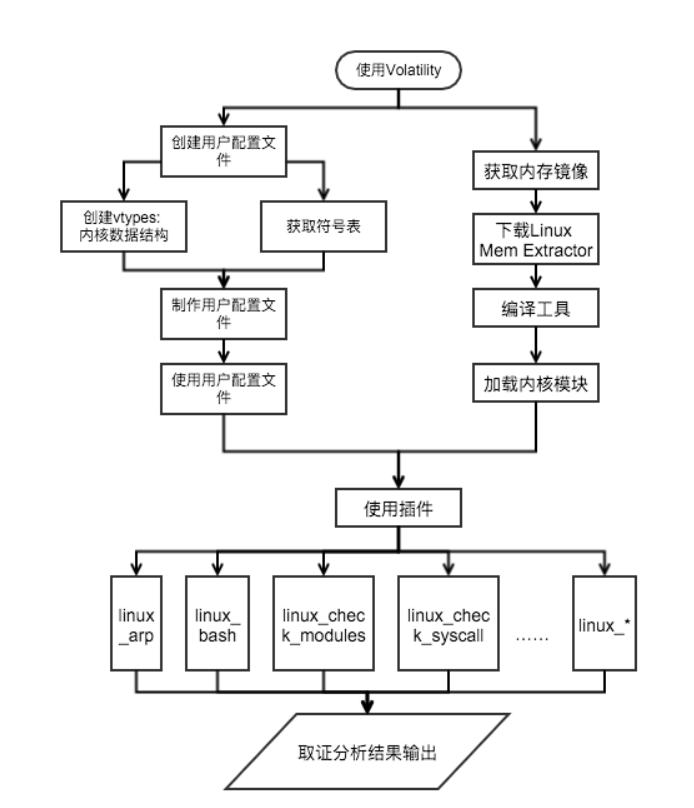
pip install distorm3

**Yara:**恶意软件分类工具

pip install yara

**PyCrypto:**加密工具集

pip install pycrypto

**PIL:**图片处理库

pip install pil

**OpenPyxl:**读写excel文件

pip install openpyxl

**ujson:**JSON解析

pip install ujson

## 创建用户配置文件

Volatility需要从用户配置文件中读取内核的相关信息，通过这些信息来定位内存中的关键信息并对其进行解析。因此我们需要获取用户配置文件，且这些配置文件需与你要分析的内核版本相匹配，其中包含了内核数据结构以及调试符号。

通常我们可以从[github](https://link.jianshu.com?t=https://github.com/volatilityfoundation/profiles" \t "_blank)上获取已经整理好的用户配置信息，当然我们也能够自己来编译。以下就是自己编译用户配置文件的过程。

**首先我们得装一些工具。**

dwarfdump&GCC/Make&KernelHeaders:调试文件导出工具、编译工具以及待分析系统内核头文件

sudo apt-get install dwarfdump build-essential linux-header-'uname -r'

**创建vtypes**

vtypes是内核数据结构，为创建该数据结构，我们需要检查我们的源码并针对我们要分析的系统内核编译module.c文件，这将会为我们生成一个名为module.dwarf文件，该文件包含了我们所需的内核调试信息。

具体可以这么做：

cd volatility/tools/linux

make

**获取符号表**

一般我们可以在/boot目录下找到该System.map文件。该文件包含系统的符号信息。

**制作用户配置文件**

随后对moudle.dwarf以及system.map文件打包成一个zip文件，随后将该zip文件放在volatility/plugins/overlays/linux下。

sudo zip volatility/volatility/plugins/overlays/linux/Ubuntu1404.zip volatility/tools/linux/module.dwarf /boot/System.map-'uname -r'

**使用用户配置文件**

随后就可以通过以下命令来查看用户配置文件的名字了。

python vol.py --info|grep Linux

这里面的LinuxUbuntu1404x64就是随后要用的配置文件名了，一般用在选项--profile之后。

**获取内存镜像**

Volatility并不会抓取内存，因此建议使用lime(Linux Mem Extractor)，从intel硬件或虚拟机上抓取内存，当然他也支持安卓系统内存抓取。

**下载内存抓取工具Lime**

git clone https://github.com/504ensicsLabs/LiME.git

**编译工具**

cd volatility/tools/linux

make

**加载内核模块**

sudo insmod lime-`uname -r`.ko "path=<outfile | tcp:<port>> format=<raw|padded|lime> [dio=<0|1>]"

其中 path参数可以为输出文件outfile，用于本地保存或tcp:<port>用于远程监听。format：raw是将所有系统RAM空间串联起来，padded是将非系统RAM空间以0填充，而lime则是将每段空间前填充固定大小的头部，该头部包含地址空间信息。dio则用于是否启用Direct IO。

我们则是：

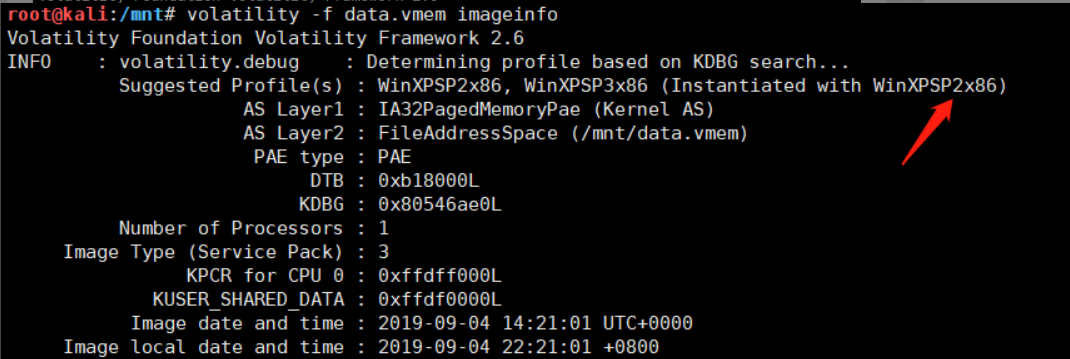
sudo insmod lime-`uname -r`.ko "path=/home/crazydog/ubuntu.lime format=lime"

PS：这一步会使得系统非常卡顿，大家使用时请不要使用在生产系统上防止对正常应用造成影响。

那么当我们在使用volatility时，我们通常做题的步骤为：

****第一步提取内容镜像信息****

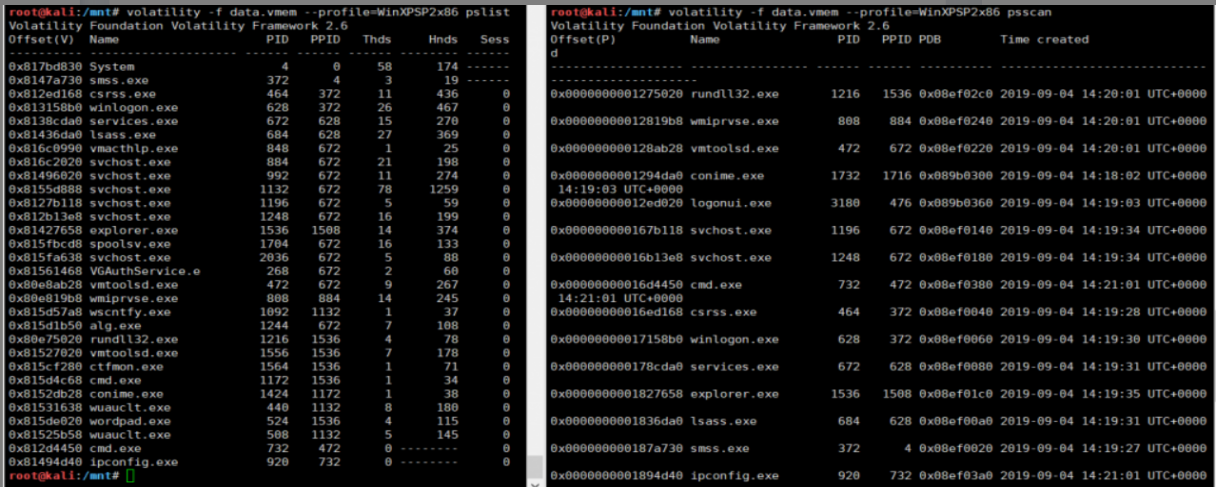
常用命令volatility -f <xxx.vmem>(或xx.raw) imageinfo

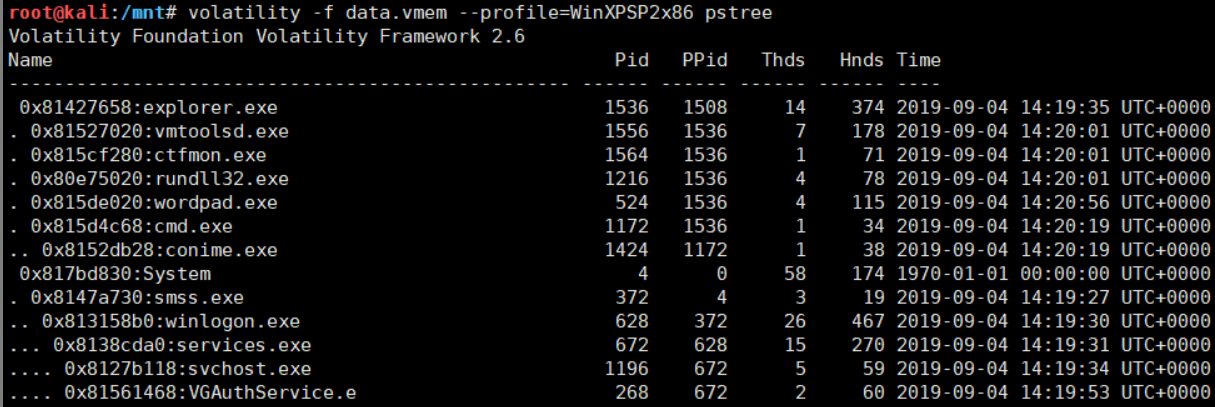


使用imageinfo插件获取到基本信息，特别是内存数据是什么操作系统下生成的，这点尤为重要 （如图的WinXPSP2x86） 因为在接下来每一步都要命令“–profile”指定操作系统的属性。

****第二步列取文件中曾使用的进程信息****

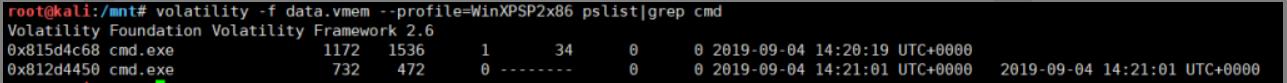
常用命令： pslist/pstree/psscan





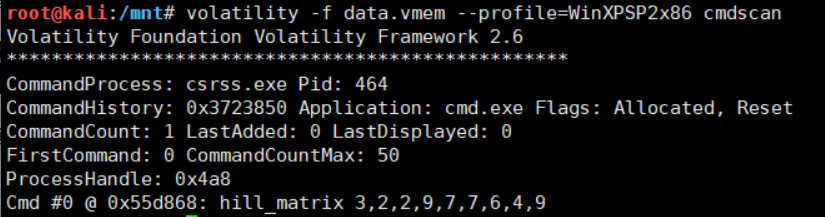
1）pslist无法显示隐藏/终止进程。  
2）解决这个问题的插件是psscan，这个插件输出的内容会比pslist多得多。（所以全面信息获取用psscan）  
3）pstree同样也是扫描进程的，但是是以进程树的形式出现的。

同时可以搭配grep命令进行对可疑进程(cmd.exe、notepad.exe等)的快速筛选

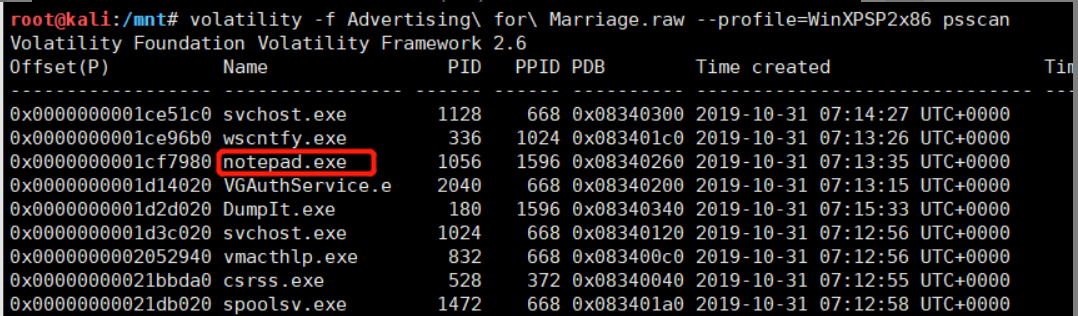


****第三步根据进程中使用的工具对应查看****

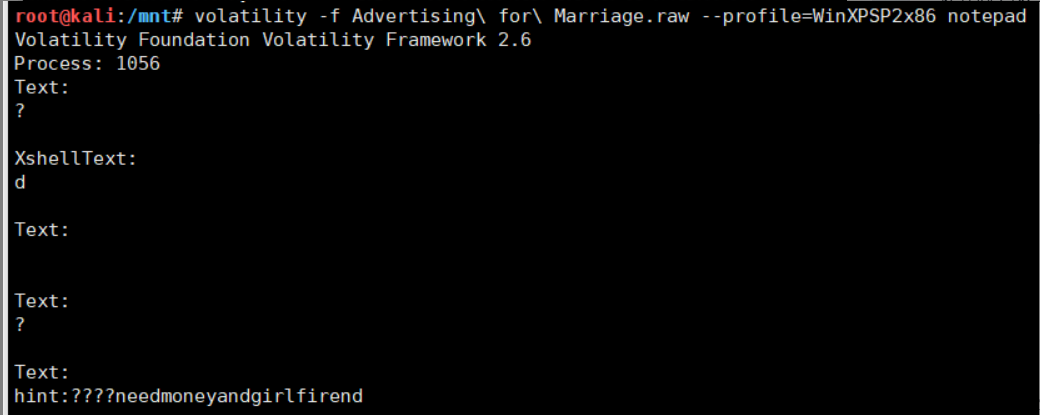
常用命令：cmdscan notepad



cmdscan 可以用来查看受害者系统上攻击者操作的最强大的命令之一，无论他们是否打开cmd.exe。简单地说，可以看到攻击者在命令提示符中键入的内容。



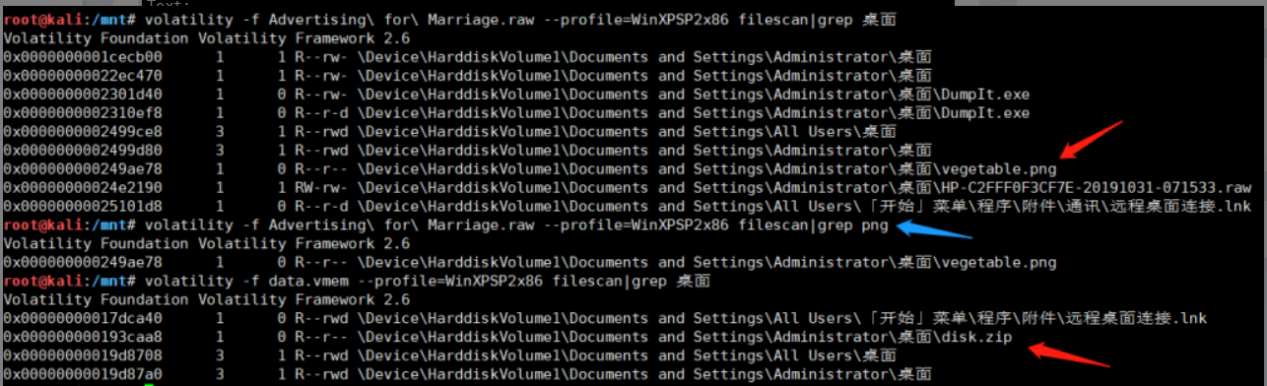
当进程中存在notepad.exe时，可用notepad插件查看文本中所写内容



****第四步文件探测****

常用命令：filescan

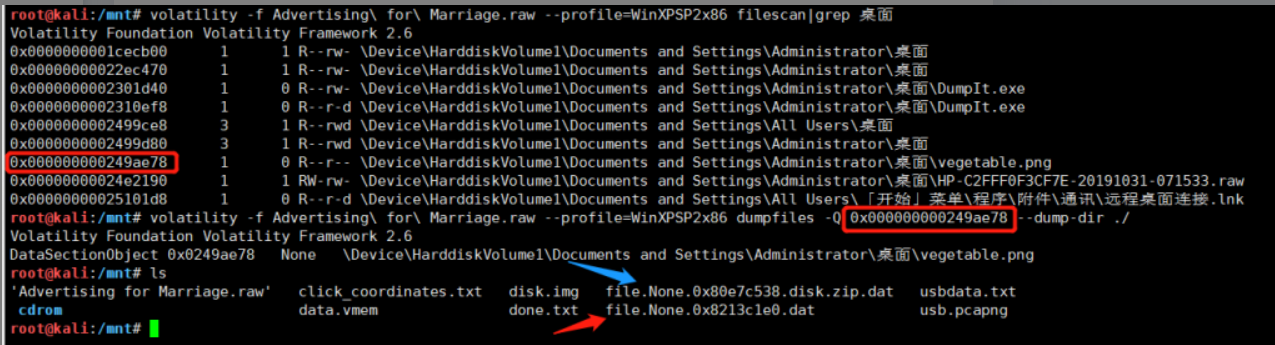
该命令通常结合grep命令对所需要文件进行筛选，以下我已在CTF中遇到的两道内存取证的文件隐藏做出结论：大概率搜索桌面即可。



****第五步提取文件****

常用命令：dumpfiles memdump

volatility -f [imgfile] –profile=[imgversion] dumpfiles -Q [file\_offset] –dump-dir [outdir]



注意红框所示需要对应，–dump-dir指定下载到本地的什么位置（这里是当前目录），注：下载下来的文件如果是普通文件（图片，文本）会直接以dat结尾，如果是压缩包，则会在前面加上一个.zip（蓝箭头所指）后续的使用修改为对应文件名及其后缀即可。

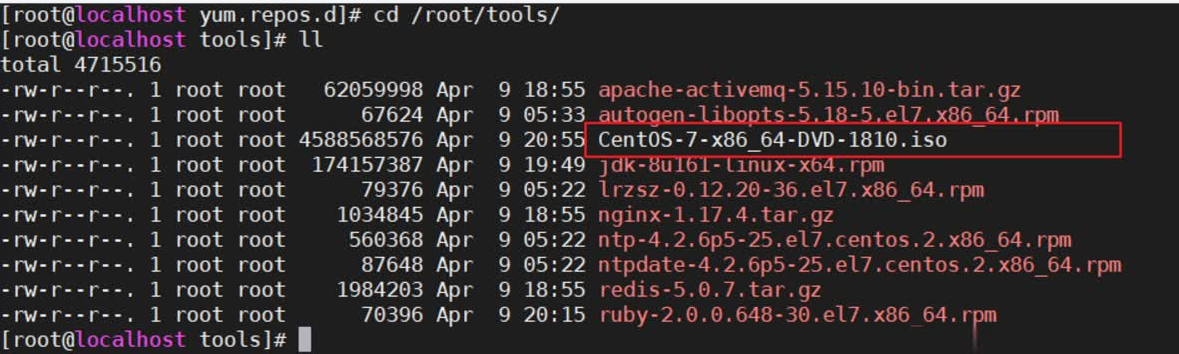
## **磁盘数据操作**

1、镜像挂载（镜像类别对应挂载方法及工具 例如linux mount挂载 veracrypt挂载.fat镜像等等）

Linux挂载镜像：

上传镜像文件到服务器

将需要挂载的源文件上传到服务器指定目录下

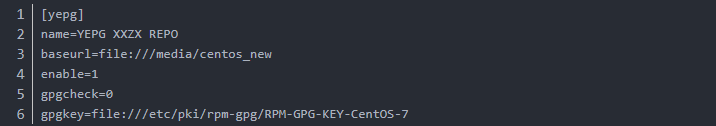


挂载源

mount ./CentOS-7-x86\_64-DVD-1810.iso /media/centos\_new/

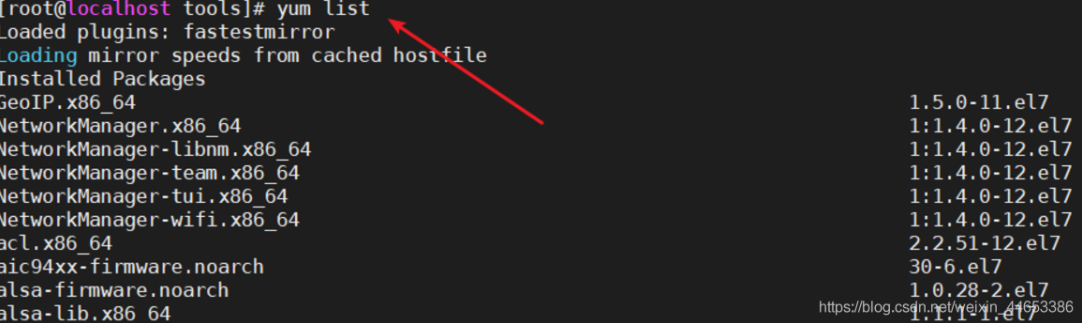
编辑配置文件

vi /etc/yum.repos.d/yepg.repo



测试

yum list



取消挂载

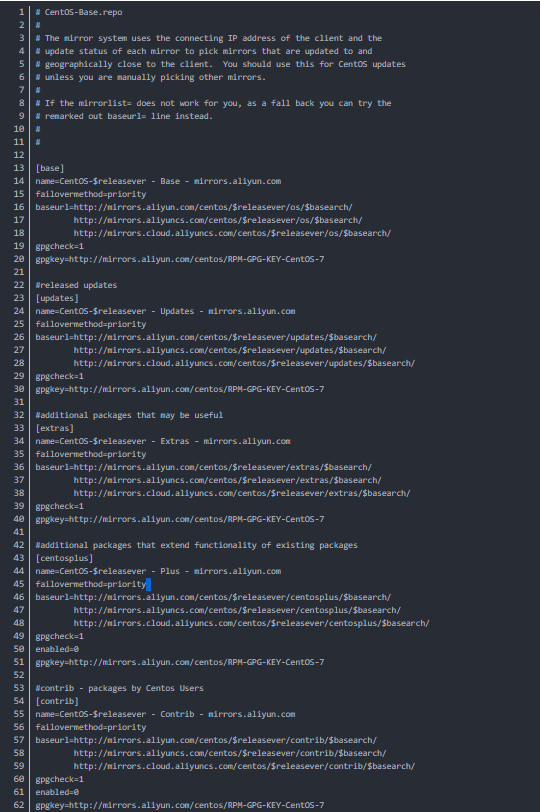
umount ./CentOS-7-x86\_64-DVD-1810.iso /media/centos\_new/

1

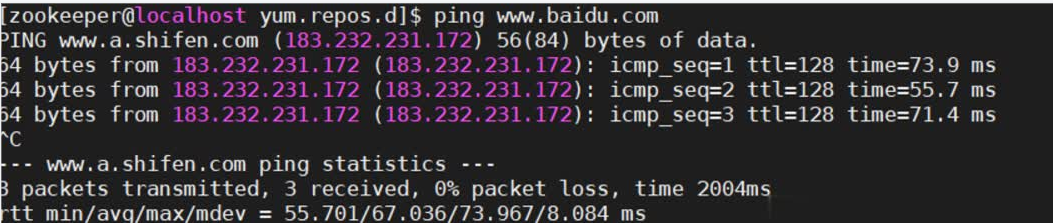
访问外部源

将本地的VMware Network Adapter VMnet8网卡设置成自动获取IP

将以下CentOS-Base.repo放到/etc/yum.repo/目录下



电脑连上WIFI，访问外网测试



问题及汇总

问题描述：

挂载源之后不能使用，需要设置这里为1

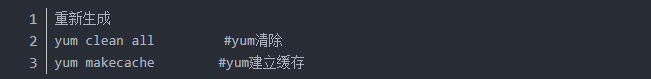
解决方案：



问题描述：

挂载源之后不能使用

解决方案：



**mount挂载**

首先，介绍一下挂接(mount)命令的使用方法，mount命令参数非常多，这里主要讲一下今天我们要用到的。

命令格式：mount [-t vfstype] [-o options] device dir

1、-t vfstype 指定文件系统的类型，通常不必指定，mount 会自动选择正确的类型。

光盘或光盘镜像：iso9660

DOS fat16文件系统：msdos

Windows 9x fat32文件系统：vfat

Windows NT ntfs文件系统：ntfs

Mount Windows文件网络共享：smbfs

UNIX(LINUX) 文件网络共享：nfs

2、-o options 主要用来描述设备或档案的挂接方式。

loop：用来把一个文件当成硬盘分区挂接上系统

ro：采用只读方式挂接设备

rw：采用读写方式挂接设备

iocharset：指定访问文件系统所用字符集

3、device 要挂接(mount)的设备。  
4、dir设备在系统上的挂接点(mount point)。

****挂接光盘镜像文件****

**1、从光盘制作光盘镜像文件。将光盘放入光驱，执行下面的命令。**

#cp /dev/cdrom /home/sunky/mydisk.iso 或

#dd if=/dev/cdrom of=/home/sunky/mydisk.iso

注：执行上面的任何一条命令都可将当前光驱里的光盘制作成光盘镜像文件/home/sunky/mydisk.iso

**2、将文件和目录制作成光盘镜像文件，执行下面的命令。**

#mkisofs -r -J -V mydisk -o /home/sunky/mydisk.iso /home/sunky/ mydir

注：这条命令将/home/sunky/mydir目录下所有的目录和文件制作成光盘镜像文件/home/sunky/mydisk.iso，光盘卷标为：mydisk

**3、光盘镜像文件的挂接(mount)**

#mkdir /mnt/vcdrom

注：建立一个目录用来作挂接点(mount point)

#mount -o loop -t iso9660 /home/sunky/mydisk.iso /mnt/vcdrom

注：使用/mnt/vcdrom就可以访问光盘镜像文件mydisk.iso里的所有文件了。

**挂接移动硬盘**

对[linux系统](https://www.linuxprobe.com/" \o "linux系统" \t "https://www.cnblogs.com/betterquan/p/_blank)而言，USB接口的移动硬盘是当作SCSI设备对待的。插入移动硬盘之前，应先用fdisk –l或more /proc/partitions查看系统的硬盘和硬盘分区情况。

[root at pldyrouter /]# fdisk -l

接好移动硬盘后，再用fdisk –l或more。  
/proc/partitions查看系统的硬盘和硬盘分区情况，应该可以发现多了一个SCSI硬盘/dev/sdc和它的两个磁盘分区/dev  
/sdc1、/dev/sdc2，其中/dev/sdc5是/dev/sdc2分区的逻辑分区，我们可以使用下面的命令挂接/dev/sdc1和  
/dev/sdc5。

#mkdir -p /mnt/usbhd1

#mkdir -p /mnt/usbhd2

注：建立目录用来作挂接点(mount point)

#mount -t ntfs /dev/sdc1 /mnt/usbhd1

#mount -t vfat /dev/sdc5 /mnt/usbhd2

注：对ntfs格式的磁盘分区应使用-t ntfs参数，对fat32格式的磁盘分区应使用-t vfat参数。若汉字文件名显示为乱码或不显示，可以使用下面的命令格式。

#mount -t ntfs -o iocharset=cp936 /dev/sdc1 /mnt/usbhd1

#mount -t vfat -o iocharset=cp936 /dev/sdc5 /mnt/usbhd2

linux系统下使用fdisk分区命令和mkfs文件系统创建命令可以将移动硬盘的分区制作成linux系统所特有的ext2、ext3格式。这样，在linux下使用就更方便了。使用下面的命令直接挂接即可。

#mount /dev/sdc1 /mnt/usbhd1

**挂接U盘**

和USB接口的移动硬盘一样对linux系统而言U盘也是当作SCSI设备对待的。使用方法和移动硬盘完全一样。插入U盘之前，应先用fdisk –l 或more /proc/partitions查看系统的硬盘和硬盘分区情况。

[root at pldyrouter root]# fdisk -l

插入U盘后，再用fdisk –l 或 more /proc/partitions查看系统的硬盘和硬盘分区情况。

[root at pldyrouter root]# fdisk -l

系统多了一个SCSI硬盘/dev/sdd和一个磁盘分区/dev/sdd1,/dev/sdd1就是我们要挂接的U盘。

#mkdir -p /mnt/usb

注：建立一个目录用来作挂接点(mount point)

#mount -t vfat /dev/sdd1 /mnt/usb

注：现在可以通过/mnt/usb来访问U盘了, 若汉字文件名显示为乱码或不显示，可以使用下面的命令。

#mount -t vfat -o iocharset=cp936 /dev/sdd1 /mnt/usb

**挂接Windows文件共享**

Windows网络共享的核心是SMB/CIFS，在linux下要挂接(mount)windows的磁盘共享，就必须安装和使用samba  
软件包。现在流行的linux发行版绝大多数已经包含了samba软件包，如果安装linux系统时未安装samba请首先安装samba。当然也可以到www.samba.org网站下载新的版本是3.0.10版。  
当windows系统共享设置好以后，就可以在linux客户端挂接(mount)了，具体操作如下：

# mkdir –p /mnt/samba

注：建立一个目录用来作挂接点(mount point)

# mount -t smbfs -o username=administrator,password=pldy123 //10.140.133.23/c$ /mnt/samba

注：administrator 和 pldy123 是ip地址为10.140.133.23 windows计算机的一个用户名和密码，c$是这台计算机的一个磁盘共享。  
如此就可以在linux系统上通过/mnt/samba来访问windows系统磁盘上的文件了。

**挂接UNIX系统NFS文件共享**

类似于windows的网络共享，UNIX(Linux)系统也有自己的网络共享，那就是NFS(网络文件系统)，下面我们就以SUN Solaris2.8和REDHAT as server 3 为例简单介绍一下在linux下如何mount nfs网络共享。  
在linux客户端挂接(mount)NFS磁盘共享之前，必须先配置好NFS服务端。

**1、linux系统NFS服务端配置方法如下：**

(1)修改 /etc/exports,增加共享目录

/export/home/sunky 10.140.133.23(rw)

/export/home/sunky1 \*(rw)

/export/home/sunky2 linux-client(rw)

注：/export/home/目录下的sunky、sunky1、sunky2是准备共享的目录，10.140.133.23、\*、  
**2、linux-client是被允许挂接此共享linux客户机的IP地址或主机名。如果要使用主机名linux-client必须在服务端主机**/etc/hosts文件里增加linux-client主机ip定义。格式如下：

10.140.133.23 linux-client

(2)启动与停止NFS服务

/etc/rc.d/init.d/portmap start (在REDHAT中PORTMAP是默认启动的)

/etc/rc.d/init.d/nfs start 启动NFS服务

/etc/rc.d/init.d/nfs stop 停止NFS服务

注：若修改/etc/export文件增加新的共享，应先停止NFS服务，再启动NFS服务方能使新增加的共享起作用。  
使用命令exportfs -rv也可以达到同样的效果。

**3、linux客户端挂接(mount)其他linux系统或UNIX系统的NFS共享**

# mkdir –p /mnt/nfs

注：建立一个目录用来作挂接点(mount point)

#mount -t nfs -o rw 10.140.133.9:/export/home/sunky /mnt/nfs

注：这里我们假设10.140.133.9是NFS服务端的主机IP地址，当然这里也可以使用主机名，但必须在本机/etc/hosts文件里增加服务端ip定义。/export/home/sunky为服务端共享的目录。  
如此就可以在linux客户端通过/mnt/nfs来访问其它linux系统或UNIX系统以NFS方式共享出来的文件了。  
以上操作在 redhat as server 3、redflag server4.1、suse server 9以及Solaris 7、Solaris 8、Solaris 9 for x86&sparc环境下测试通过。

**补充：**

linux加载光驱：  
（1）使用光驱前，要先mount一下：

＃mount /dev/cdrom /mnt/cdrom

然后您就可以进入/mnt/cdrom目录下读取光盘内容了。  
（2）当您想退出光盘时，须使用umout命令，否则光驱就会一直处于死锁状态：

＃umount /mnt/cdrom

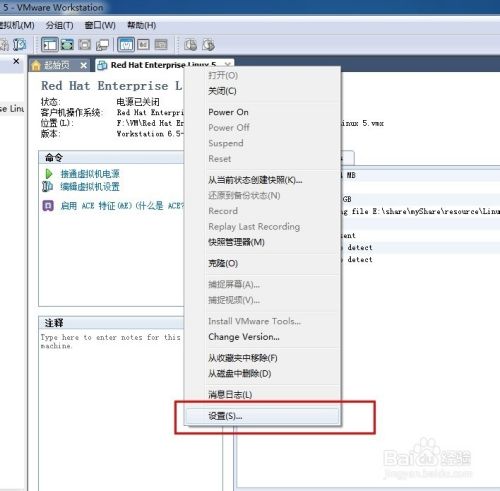
**对于vxm的镜像加密**

加密：虚拟机加密时对 VMware VMX 配置文件进行加密

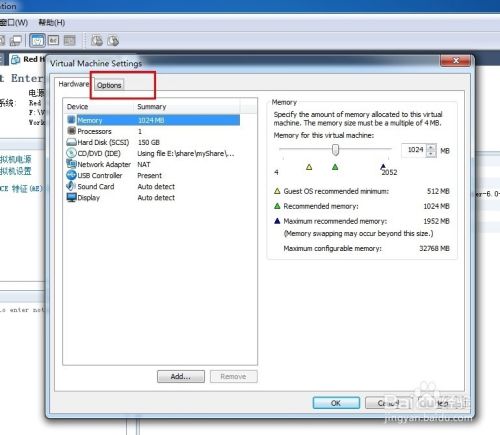
首先打开VMware.



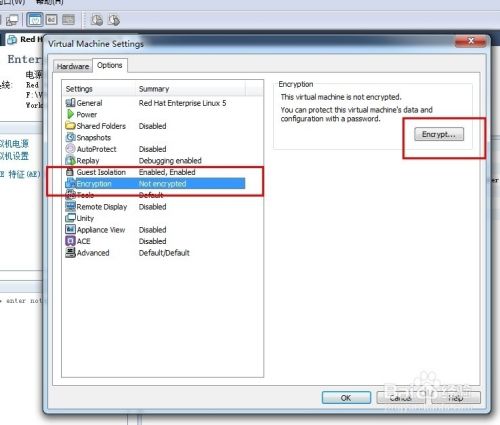
找到要加密的虚拟机系统.右击选择"设置"



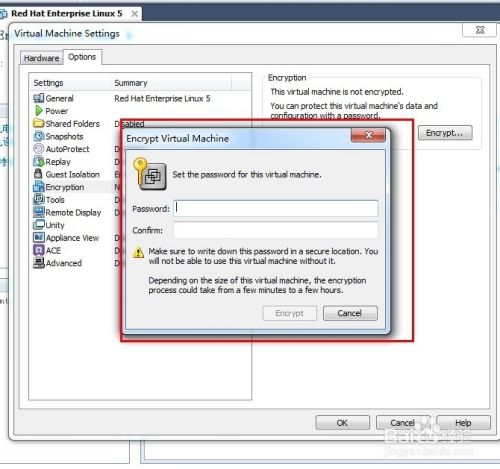
进入到"virtual machine settings"设置页面.点击"options"选项卡.

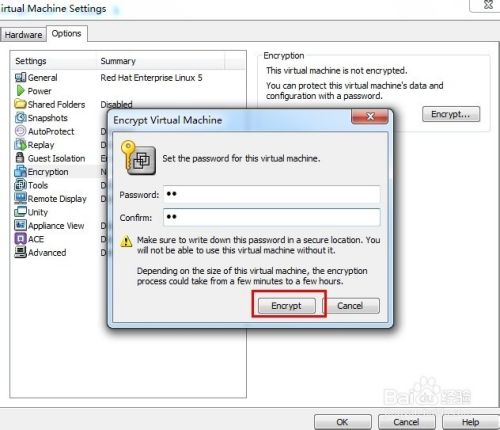


点击下面的""Encryption"选项.然后点击页面右侧的"Encrypt.."按钮



进入"Encrypt virtual Machine"页面.输入你要设置的密码,点击"Encrypt"即可.这样在启动你的系统就需要输入密码了.





解密的话需要用到GitHub的一个项目

工具附上：github.com/axcheron/pyvmx-cracker

题解附上，可供参考：https://www.anquanke.com/post/id/234503#h3-30

## **VeraCrypt识别**



VeraCrypt创建加密卷

首先，从VeraCrypt加密容器创建加密卷，如图2可知，创建加密数据有三种方式：

**1.创建文件型加密卷**：创建一个文件类型的虚拟加密盘，推荐入门用户使用；

**2.加密非系统分区/设备**：加密一个内部或者外部驱动器上的非系统分区（例如：U盘）。也可以创建一个隐藏的加密卷；

**3.加密系统分区或者整个系统所在硬盘**：加密Windows系统所在的分区/驱动器。加密后，任何人想要访问和使用此加密系统、读写此系统盘下的文件等，都需要每次在Windows启动前输入正确的密码。也可以选择创建一个隐形的操作系统。

**接下来将针对不同的加密类型展开识别研究**

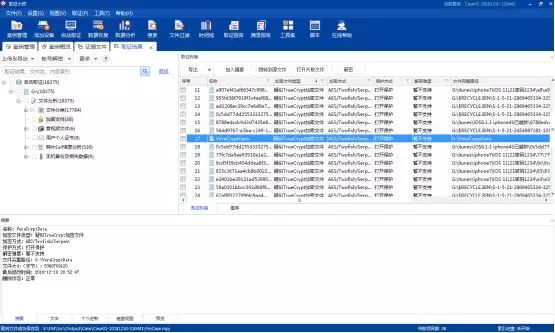
**1、文件型加密卷类型的识别**

对于文件型加密卷的识别可以从以下三个方面入手：

**（1）文件大小**，重点关注大文件（因为存储需要的空间大，加密文件相对会设置的比较大），大小必须被512整除；

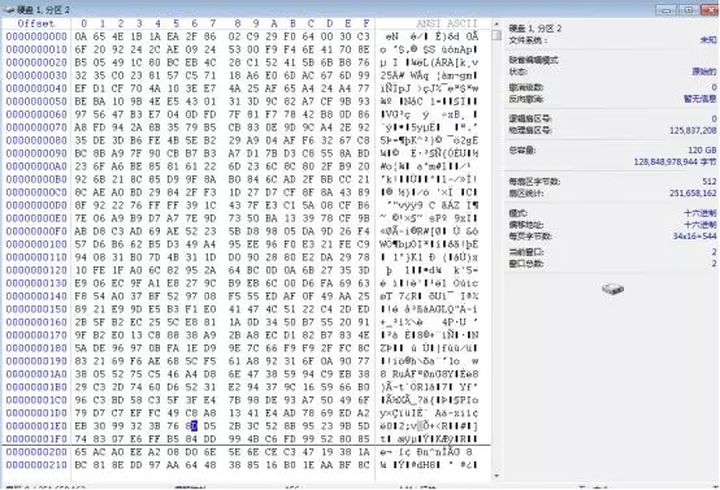
**（2）已知的文件签名校验**，通过对文件进行已知类型的相关特征进行比对；

**（3）信息熵（information entropy）**，通过上述两种方法检测后，再通过文件的信息熵值可以比较精确地识别出加密文件。

 取证大师加密容器自动识别结果

如图所示，当前取证大师已使用以上综合方法检测加密容器。

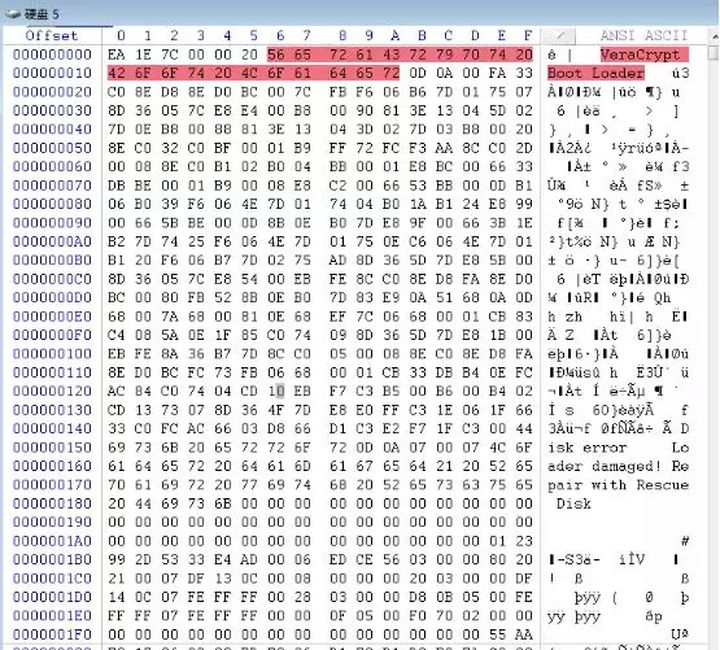
**2、加密非系统分区/设备的类型识别**

VeraCrypt加密非系统分区头部数据

通过对非系统分区数据研究如图4所示，可以看出分区内开头数据全部杂乱无章，且正常文件系统的特征全无，对此种类型，可以通过计算分区内数据的信息熵结合已知文件系统特征来识别。

**3、加密系统分区类型的识别**

对于加密系统分区或者加密整个系统盘类型：

 VeraCrypt加密系统分区头部数据

此类型的识别在三种加密中是属于比较容易识别类型。通过对加密数据硬盘开头512字节分析，可发现VeraCrypt系统分区加密后的数据会在头部生成一个相应的标识。观察头部是否有VeraCrypt Boot Loader标志，即可识别，如图5所示，此数据为一个系统分区加密的类型。

**4、隐藏类型的识别**

 VeraCrypt创建加密卷类型

如图所示，创建加密卷时，不管是文件类型、分区类型或者硬盘类型都有隐藏的类型可以选择创建。隐藏卷其实就是建立两层：外层是一个密码，内层又是一个密码。对于这个加密卷类型是在加密卷上再创建一个隐藏的加密卷，识别的难度更大，当前暂无可靠的方法可以直接检测，可通过其他数据的特征推算出是否有疑似隐藏卷。

比如，从文件修改的时间范围着手，因隐藏加密卷建立在外层加密卷之上，鉴于存储数据需求，外层的数据必定不能存储太多，太多会覆盖掉隐藏卷内容，导致隐藏卷无法正常使用。因外层加密卷文件用于伪装迷惑，故这些文件的修改时间变动较小，甚至外层加密卷的文件创建后可能不会进行修改。

## **取证方法**

从上述的类型研究可以发现，如果需要对VeraCrypt加密数据取证，必须要获得加密的密码或相关密钥。针对以上的加密类型，下面以取证大师为例，总结了如下相关取证方法：

对已获知是加密容器数据，用取证大师V6版本的镜像添加或直接用加密容器添加, 添加后，用TrueCrypt解密功能（取证大师的TrueCrypt解密功能支持对TrueCrypt与VeraCryp加密数据的解密）进行VeraCrypt加密数据解密。

添加后，取证大师可自动识别为加密容器。

之后，在案例视图加密容器节点右键点击TrueCrypt解密功能弹出解密对话框，再设置解密相关参数。

设置完成后，点击确定，解密后再进行相关数据取证。

**Fat文件详解**

FAT格式的文件系统，磁盘数据分为5部分：MBR区、DBR区、FAT区、DIR区和DATA区。

**MBR区**

MBR（Main Boot Record主引导扇区）,意即为主引导记录区,位于整个硬盘的0磁道0柱面1扇区。在总共512字节的主引导扇区中,MBR占用了446个字节（偏移0–偏移1BDH）,另外的64个字节（偏移1BEH–偏移1FDH）交给了DPT(Disk Partition Table硬盘分区表)（见下表）,最后两个字节”55,AA”（偏移1FEH- 偏移1FFH）是分区的结束标志。

主引导记录中包含了硬盘的一系列参数和一段引导程序。其中的硬盘引导程序的主要作用是检查分区表是否正确并且在系统硬件完成自检以后引导具有激活标志的分区上的操作系统,并将控制权交给启动程序。MBR是由分区程序（如Fdisk）所产生的,不依赖任何操作系统, 硬盘引导程序也可以改变,从而实现多系统共存。

**DBR区**

DBR（Dos Boot Record）是操作系统引导记录区的意思。它通常位于硬盘的0磁道1柱面1扇区,是操作系统可以直接访问的第一个扇区,它包括一个引导程序和一个被称为BPB（Bios Parameter Block）的本分区参数记录表。引导程序的主要任务是当MBR将系统控制权交给它时,判断本分区跟目录前两个文件是不是操作系统的引导文件（以DOS为例,即是Io.sys和Msdos.sys）。如果确定存在,就把其读入内存,并把控制权 交给该文件。BPB参数块记录着本分区的起始扇区、结束扇区、文件存储格式、硬盘介质描述符、根目录大小、FAT个数,分配单元的大小等重要参数。

**FAT区**

下面是FAT（File Allocation Table文件分配表）区。在此之前,我们来谈谈簇（cluster）的概念。文件占用磁盘空间时,基本单位不是字节而是簇。簇的大小与磁盘的规格有关,一般情况下,软盘每簇是1个扇区,硬盘每簇的扇区数与硬盘的总容量大小有关,可能是4、8、16、32、64……

我们知道,同一个文件的数据并不一定完整地存放在磁盘的一个连续的区域内,而往往会分成若干段,像一条链子一样存放。这种存储方式称为文件的链式存储。硬盘上的文件常常要进行创建、删除、增长、缩短等操作。这样操作做的越多,盘上的文件就可能被分得越零碎（每段至少是1簇）。但是,由于硬盘上保存着段与段之间的连接信息（即FAT）,操作系统在读取文件时,总是能够准确地找到各段的位置并正确读出。不过,这种以簇为单位的存储法也是有其缺陷的。这主要表现在对空间的利用上。每个文件的最后一簇都有可能有未被完全利用的空间（称为尾簇空间）。一般来说,当文件个数比较多时,平均每个文件要浪费半个簇的空间。

为了实现文件的链式存储,硬盘上必须准确地记录哪些簇已经被文件占用,还必须为每个已经占用的簇指明存储后继内容的下一个簇的簇号,对一个文件的最后一簇,则要指明本簇无后继簇。这些都是由FAT表来保存的,表中有很多表项,每项记录一个簇的信息。

由于FAT对于文件管理的重要性,所以FAT有一个备份,即在原FAT的后面再建一个同样的FAT。初形成的FAT中所有项都标明为”未占用”,但如果磁盘有局部损坏,那么格式化程序会检测出损坏的簇,在相应的项中标为”坏簇”,以后存文件时就不会再使用这个簇了。FAT的项数与硬盘上的总簇数相当,每一项占用的字节数也要与总簇数相适应,因为其中需要存放簇号。FAT的格式有多种,最为常见和为读者所熟悉的是FAT16和FAT32,其中FAT16是指文件分配表使用16位数字,由于16位分配表最多能管理65536（即2的16次方）个簇,也就是所规定的一个硬盘分区。

由于每个簇的存储空间最大只有32KB,所以在使用FAT16管理硬盘时,每个分区的最大存储容量只有（65536\*32 KB）即2048MB,也就是我们常说的2G。现在的硬盘容量是越来越大,由于FAT16对硬盘分区的容量限制,所以当硬盘容量超过2G之后,用户只能将硬盘划分成多个2G的分区后才能正常使用,为此微软公司从Windows 95 OSR2版本开始使用FAT32标准,即使用32位的文件分配表来管理硬盘文件,这样系统就能为文件分配多达4294967296（即2的32次方）个簇,所以在簇同样为32KB时每个分区容量最大可达65G以上。此外使用FAT32管理硬盘时,每个逻辑盘中的簇长度也比使用FAT16标准管理的同等容量逻辑盘小很多。由于文件存储在硬盘上占用的磁盘空间以簇为最小单位,所以某一文件即使只有几十个字节也必须占用整个簇,因此逻辑盘的簇单位容量越小越能合理利用存储空间。所以FAT32更适于大硬盘。

**DIR区（根目录区）**

DIR（Directory）是根目录区,紧接着第二FAT表（即备份的FAT表）之后,记录着根目录下每个文件（目录）的起始单元,文件的属性等。定位文件位置时,操作系统根据DIR中的起始单元,结合FAT表就可以知道文件在硬盘中的具体位置和大小了。

**数据（DATA）区**

数据区是真正意义上的数据存储的地方,位于DIR区之后,占据硬盘上的大部分数据空间。

对于FAT文件格式，制作一个2GB的FAT镜像就会有2GB大小，但由于只是一个空文件系统(其中并没有存储具体的文件)，其中有意义的只有前面一部分，包括引导记录以及FAT表所在的部分，所以实际上前20MB就能表示整个FAT文件系统了。

以制作1GB大小的udisk.bin文件为例，在Linux下两个命令搞定：

mkfs.vfat -n "Internal SD" -F 32 -C usbdisk.tmp 1048576

dd if=usbdisk.tmp of=udisk.img bs=1024 count=20480

其中：

-n "Internal SD" 是指定了卷标

1048576 是磁盘空间大小，单位是KB

dd这个命令的目的就是将前面20MB的内容抠出来。

Linux dd命令在扩增SWAP分区时的应用http://www.linuxidc.com/Linux/2015-03/114326.htm

Linux dd命令制作U盘系统启动盘http://www.linuxidc.com/Linux/2015-02/113585.htm

**数据恢复、数据解密（bitlocker解密等）**

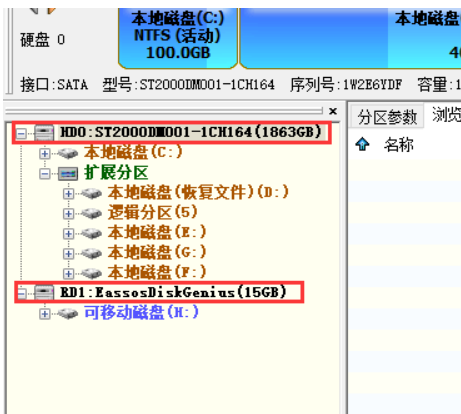
**diskgenius的使用**

当我们遇到一些关于数据恢复的问题时，diskgenius这款软件是我们的首选，使用此软件的原理如下：

## 一、DiskGenius能够恢复数据的前提条件

DiskGenius能够恢复数据的前提条件是：DiskGenius能够识别出你要恢复数据的存储硬件（硬盘、移动硬盘、U盘、存储卡等）。

比如下图：



在电脑上，运行DiskGenius，识别出的两个存储硬件，HD0是本机的硬盘，容量2T，上面有C、D、E等6个分区（有一个分区没有被分配盘符）；RD1是个U盘，容量只有15G，上面只有一个分区H。

如果一个存储设备，联接电脑后，不能被DiskGenius识别，在DiskGenius主界面左侧的窗口中不显示，那么，可以断定这个存储设备有了硬件故障，仅仅依靠软件已经不能恢复数据恢复，需要送到专业的数据恢复公司，做固件修复或开盘恢复。

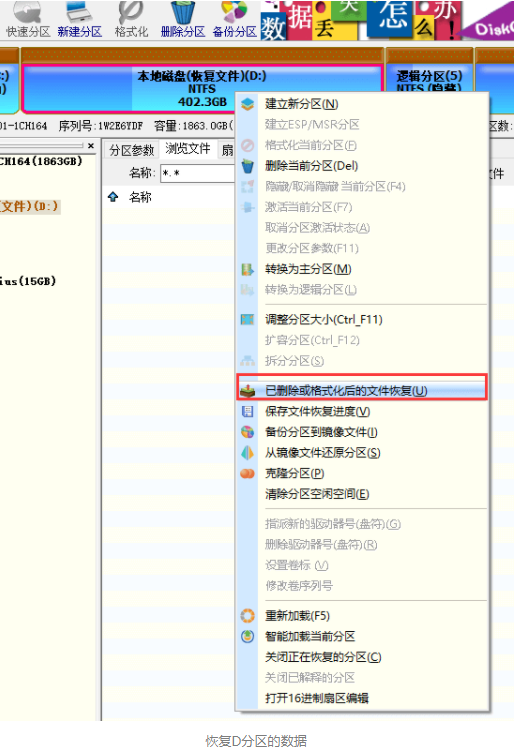
DiskGenius团队本身也提供这种服务，而且作为DiskGenius的开发商，自然技术上更加权威。有需要的用户，可以访问DiskGenius远程数据恢复服务，了解更多。

提示：

分区丢失并不是硬盘不能识别，通常情况下并不影响数据恢复。有时，用户的分区由于各种原因在DiskGenius中看不到了，这个没关系，并不是硬件问题，通常是文件系统的软件问题，仍然可以使用DiskGenius恢复丢失数据。

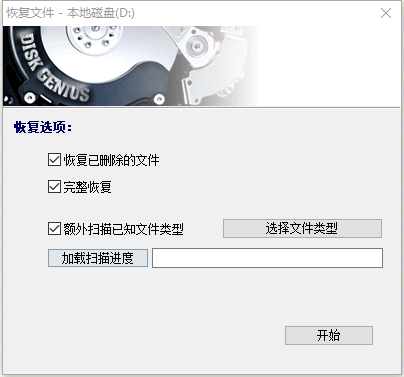
## 如何开始恢复数据

## 如果你能确定你要恢复的数据存在于哪个分区上，那么直接在DiskGenius主界面上方的硬盘分区图中，选中分区，点击鼠标右键，然后在弹出的快捷菜单中，选择菜单项“已删除或格式化后的文件恢复”，如下图所示：

如果你不能确定要恢复的数据在哪个分区中，更常见的情形是，原来的分区已经丢失了或者已经被新建的分区覆盖了，这些情况下，你需要在DiskGenius左侧主界面中，选择要恢复数据的存储设备，然后点击右键，同样在弹出的快捷菜单中，选择菜单项“已删除或格式化后的文件恢复”，如下图所示：

## 三、恢复选项

在上一步中，不管您是要恢复分区中的数据，还是要恢复整个硬盘中的数据，点击快捷菜单项“已删除或格式化后的文件恢复”后，都会弹出恢复选项窗口，如下图所示：



恢复选项窗口

可以看到，有“恢复已删除的文件”、“完整恢复”、“额外扫描已知文件类型”，三个选项（加载扫描进度稍后再讨论）。

这三个选项，其实是恢复数据时，扫描硬盘、分区等存储介质的三种方式。

****恢复已删除的文件****

非常快，缺点是适用于刚刚删除文件，还未写入新数据时的情形，其他情形下的恢复效果不好。

这种模式，只扫描分区文件系统的目录信息部分，一般10秒左右就能完成一个100G硬盘的扫描，因为只扫描分区文件系统的目录信息部分，所以只适用于简单的数据恢复情形。

****完整恢复****

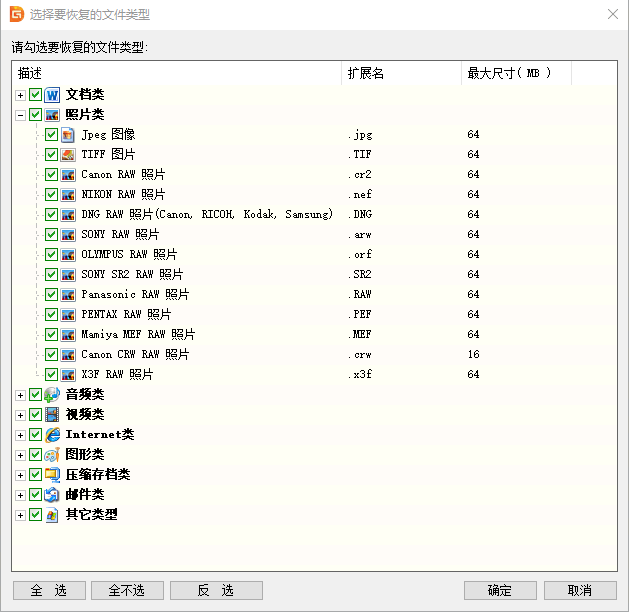
扫描速度慢，但恢复效果非常好，适合大多数情况下的数据恢复。

这种扫描方式，不仅扫描分区文件系统的目录信息部分，还要分析分区系统的数据部分，尽可能多的查找可能的有价值的数据信息，因此它的恢复效果非常好，只要数据没有被覆盖，成功恢复数据的希望非常大，相应的，这种扫描方式需要花费的时间，也要比仅仅扫描分区文件系统的目录信息部分-恢复已删除的文件扫描方式要多很多。

****额外扫描已知文件类型****

扫描速度慢，在硬盘及分区损坏程度比较大的情况，往往能取得较好的恢复效果。

这种扫描方式，有些数据恢复软件称之为万能恢复，其实就是从头至尾扫描分区或硬盘，匹配文件类型的文件头信息，这种扫描方式，对空间上一般是连续存储的存储介质（比如数码相机中的存储卡），恢复效果较好，对于普通的硬盘等存储介质，也很有意义，缺点一是恢复出来的文件，没有文件名及目录结构等信息，二是因为要对整个数据存储空间空间进行扫描，速度会比较慢，三是恢复大文件的效果要差些，因为大文件连续存储的概率要小一些。 勾选“额外扫描已知文件类型”选项后，点击右侧的“选择文件类型”按钮，可以在弹出的窗口中指定您要恢复的文件类型，如下图：



这里有几百个文件类型，基本上您常接触到的文件类型都在这里了，默认是全都勾选了，您可以只勾选需要恢复的文件类型，可以简化“所有类型”的恢复结果。

****选项建议****

默认情况下，这三个恢复选项都是勾选的（某些情况下，DiskGenius会自动屏蔽“恢复已删除的文件”选项的选择，即变灰，不能勾选，因为有的时候，这种扫描方式没有意义），大多数情况，这是最好的选择，建议您采用。

实际上，三个选项都被选择时，DiskGenius扫描数据的过程实际上是这样的：

1、用“恢复已删除的文件”模式，快速扫描一遍硬盘或分区；

2、前一遍的扫描结束后，同时执行“完整恢复”、“额外扫描已知文件类型”两种模式的扫描；

此外，DiskGenius恢复数据时，还有如下一些特色，稍后，我们会具体讲解：

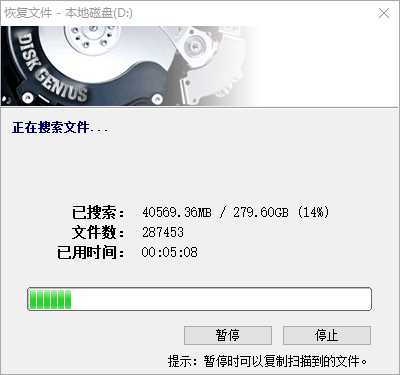
1、DiskGeniu的扫描结果是所见即所得的方式，即一边扫描，一边把扫描出来的文件、目录等信息显示出来，供用户参考；

2、用户可以随时暂停或停止扫描过程，然后查看当前的扫描结果，预览扫描的文件，以决定是否继续扫描；

3、用户需要时，还可以暂停扫描，保存扫描进度及结果，这样再次恢复数据时，可以直接读取扫描进度及结果，最大限度地节约了扫描的时间。

## 四、扫描

设置好恢复选项，点击“开始”按钮后，DiskGenius软件就开始扫描硬盘或分区中的数据了，首先会弹出一个扫描窗口，如下图：



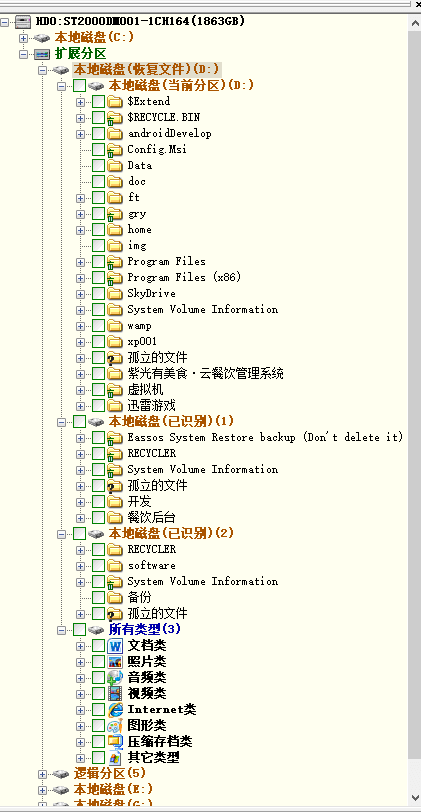
扫描窗口，可以随时暂停或停止扫描

扫描窗口中，“已搜索”表示已经搜索的存储空间大小及其占全部搜索空间的百分比；“文件数”表示已经搜索到的文件数量；“已用时间”表示已经扫描的时间。下面的进度条，图形化地表示搜索的进度。

最下面的两个按钮，“暂停”与“停止”。您可以暂停扫描，然后查看、预览已经扫描出的文件，如果需要恢复的文件已经全部找到并能正确预览，就可以停止扫描了；如果当前的扫描结果不满意，可以继续扫描。

## 五、查看扫描结果（一），目录结构

暂停扫描，查看扫描结果，您会发现，左侧的分区、目录树窗口，变成了下面这个样子：



扫描D分区的扫描结果

首先，D分区的名称，加上了恢复文件字样，表明现在正在扫描该分区，恢复数据。

然后，是一个一个被扫描出来的分区，通常第一个分区是该硬盘当前的正常分区，括号标明为当前分区；后面的几个分区是DiskGenius扫描出来的分区，括号标明为已识别。正常分区与已识别分区内都有目录层次结构，选择任何一个目录后，都能够在右侧的文件窗口中看到该目录下的文件列表信息。

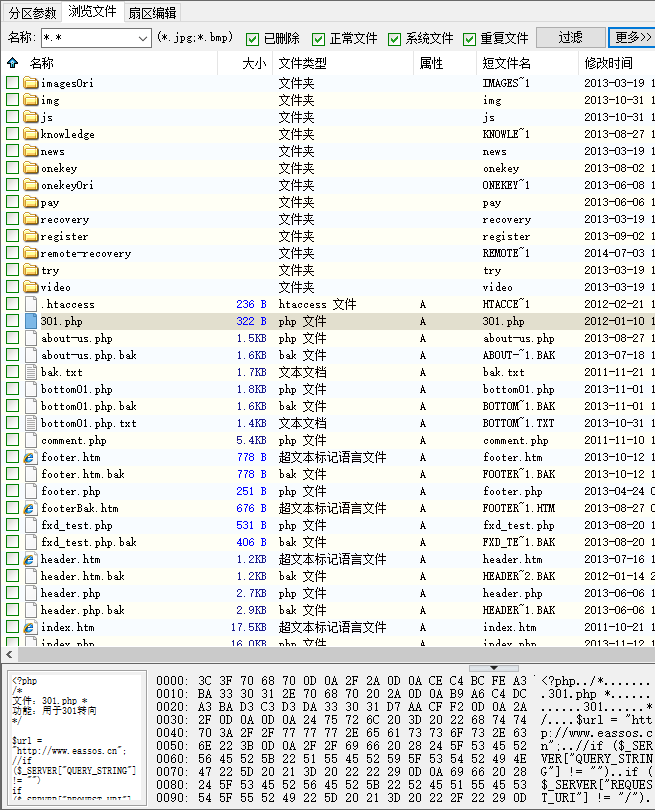
提示：

你有时会看到有些名称是“孤立的文件”的文件夹，文件夹图标上还有一个问号，这些文件夹里的文件，是所属文件夹信息已经丢失的文件。

最后，所有类型，是在恢复选项中，勾选了额外扫描已知文件类型后，按文件类型方式扫描出的文件。因为这种扫描方式，无法获取文件的名称及目录信息，所以选择某个文件类型，您会发现，在右侧文件窗口中显示的文件名称，都是顺序的数字名称。

## 六、查看扫描结果（二），筛选文件

暂停或停止扫描结果后，选择某个目录，一般右侧的文件窗口如下图：



如何在扫描结果中，筛选出自已需要恢复的文件呢？DiskGenius提供了如下的方法。

1、使用通配符，筛选特定名称或特定扩展名的文件，如下图：

IMG_259

2、控制是否显示正常文件等，缩小筛选范围，如下图：

IMG_260

3、根据文件大小，及创建修改访问时间，筛选文件

点击更多按钮，会出现文件大小及时间筛选项，如下图：

IMG_261

## 七、查看扫描结果（三），预览文件

当你在扫描结果中，发现了自己想要恢复的文件，怎么判断这个文件是否能够成功的恢复呢？这就需要使用文件预览功能，能够成功预览的文件，就百分之百的可以成功恢复出来。

另外，按文件类型方式，扫描出的文件，文件名信息已经丢失，要判断是否是需要恢复的文件，及能否成功恢复，就更需要使用文件预览的功能了。

DiskGenius的文件预览功能非常强大，文本、图片，office文档、pdf、音频、视频等常用的文件格式，都可以预览。

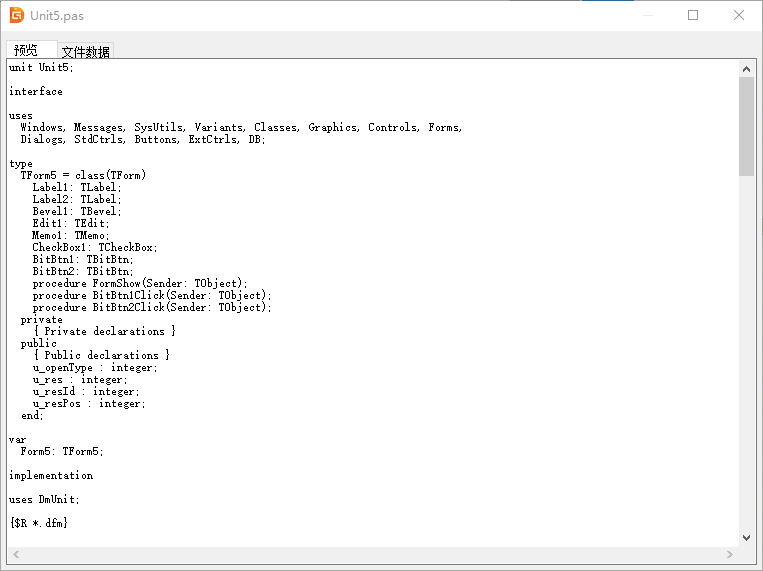
在浏览文件窗口中，选中一个文件后，通过下述三种方式，可以打开文件预览窗口，预览该文件。

1、双击该文件；

2、双击该文件在界面最下方的缩略图；

3、点击鼠标右键，在弹出的快捷菜单中，点击“预览”。

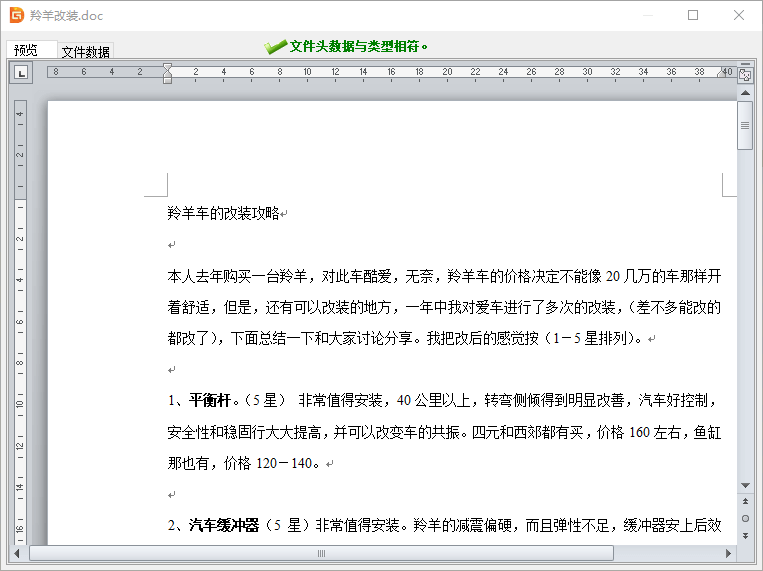
在预览窗口中，会显示该文件的内容，您可以查看文件内容是否正确，判断该文件是否可以被成功恢复出来，下面是几种文件格式的预览结果：



文本文件的预览结果



图片的预览结果，大于64k的图片会有水印



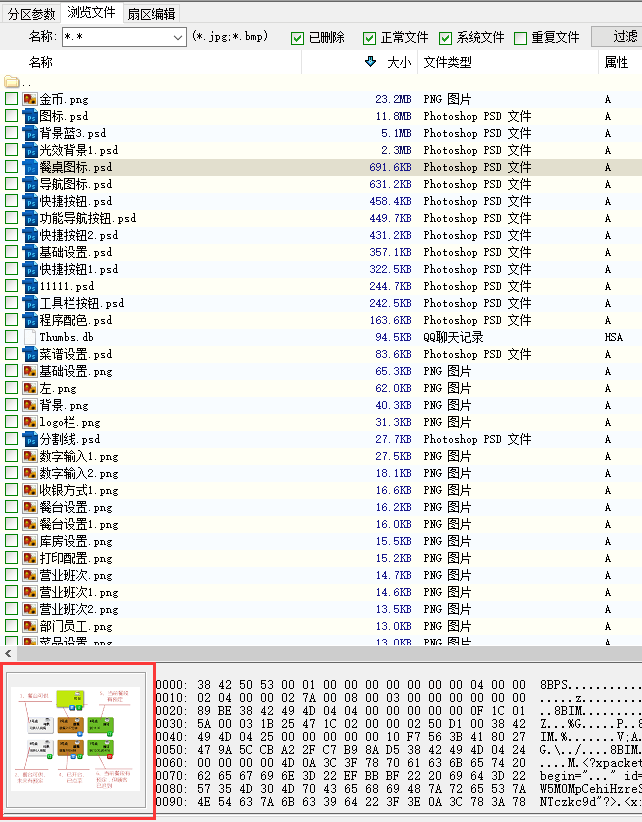
Word文档的预览结果



视频文件的预览，播放效果非常好！

提示：

在操作浏览文件窗口的过程中，您会发现，文本与图片文件，会在界面下方的缩略图中，自动显示出来，这样，在恢复文本文件与图片文件时，预览文件非常方便，如下图所示：

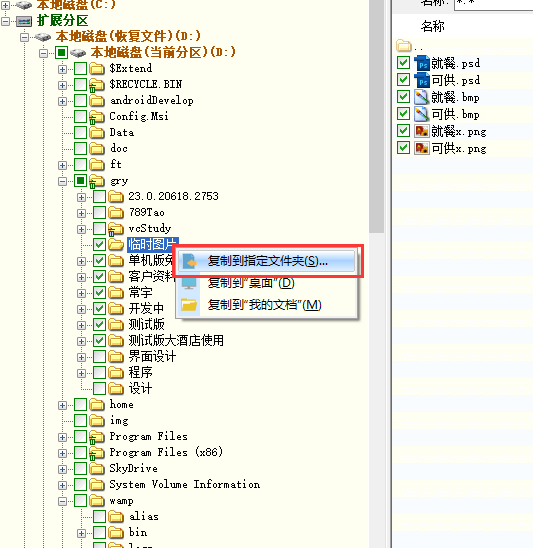


选择了文本或图片格式的文件时，缩略图窗口会自动显示该文件的内容

DiskGenius的文件预览功能，非常强大，又方便使用，能够帮助准确地判断出文件是否能够成功恢复，是执行数据恢复操作时，最有用的功能之一。

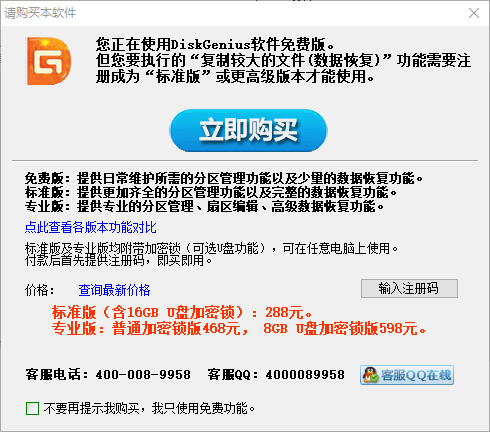
## 八、复制文件

DiskGenius完成扫描过程，或者用户对当前搜索结果已经满意，主动停止了扫描过程后，就可以在扫描结果中，选中要恢复的文件、目录等，然后点击鼠标右键，将其复制到指定的文件夹中，如下图：



选中文件或文件夹后，点击鼠标右键，将其复制到指定的文件夹，可以同时选取多个文件及文件夹

在之前的使用中，你会发现，DiskGenius免费版在使用上基本没有限制，但在这一步，如果使用的是免费版本的DiskGenius，那么软件会弹出如下的提示窗口，提醒你注册软件。



免费版的DiskGenius只能复制出小于64K的文件出来，所以通常情况下，要想恢复数据，你需要购买软件。

## 九、标准版与专业版的差别

1、专业版的数据恢复功能更强大，某些情况下，必须使用专业版才能恢复数据；

2、DiskGenius不仅仅是一款数据恢复软件，更是一款All In 的工具，分区管理、备份还原等方面的一些高级功能，也是只有专业版才支持；

3、由标准版升级的专业版，由于需要更换加密锁等问题，比较麻烦，需要花费额外的金钱与时间。

提示：

无论标准版还是专业版，用户购买后，DiskGenius后台都会立刻给用户发送一个注册码，用户使用这个注册码，可以立即在当前机器上激活使用；稍后，DiskGenius团队会给你快递一个加密锁，一般三四天你收到加密锁后，就可以在任意的电脑上使用DiskGenius的收费功能了。

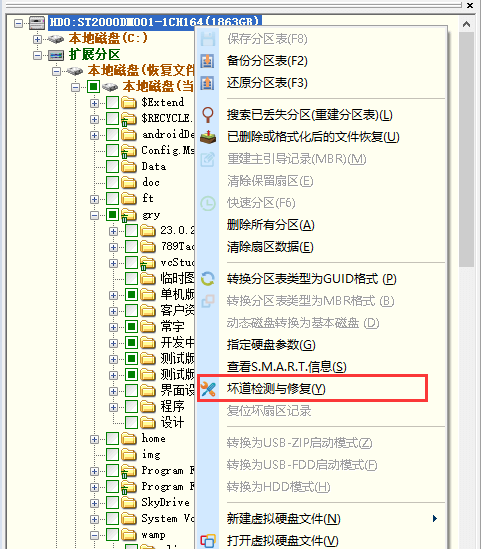
## 十、更多问题

最后，介绍一些在恢复数据时可能遇到的问题。

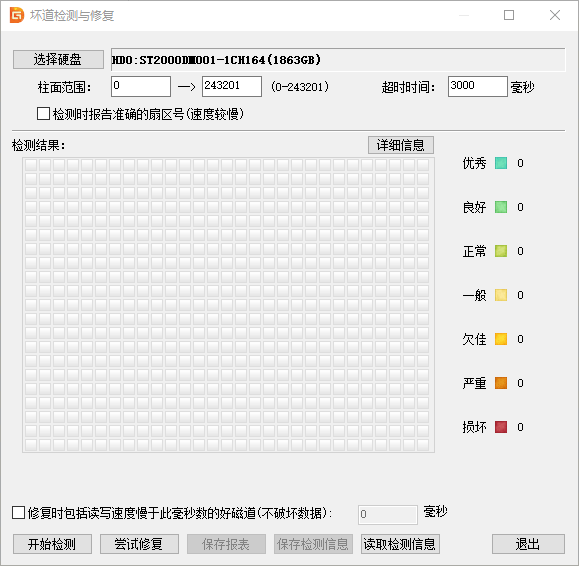
### 1、坏道对数据恢复的影响

如果DiskGenius扫描硬盘或分区时，速度非常慢，一般情况下都是因为硬盘有了坏道。遇到这种情况，可以先尝试多花些时间等待扫描结果，如果实在是太慢（比如卡在某个进度，几个小时也不动），建议停止扫描，把硬盘发给专业数据恢复公司去处理吧。

提示：使用DiskGenius可以检测硬盘的坏道情况，如下图所示，但若想恢复数据，千万不要用DiskGenius去修复坏道，会二次覆盖数据！



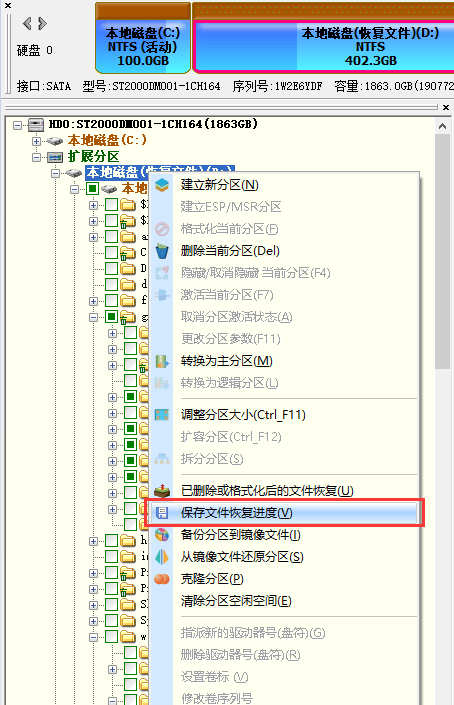
选中硬盘后，点击鼠标右键，快捷菜单中选择"坏道检测与修复"



在弹出的坏道检测与修复窗口中，可以检测硬盘坏道情况，也可以尝试修复坏道。切记的是数据恢复前不可以做尝试修复操作！

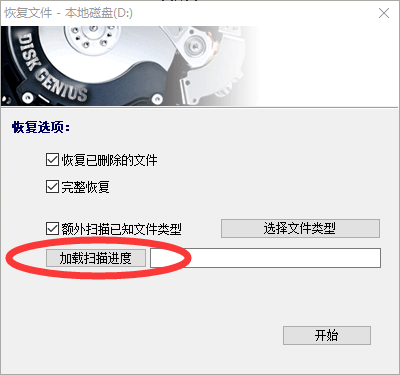
### 2、保存与读取文件恢复进度

有些时候，对硬盘、分区的扫描是比较耗费时间的。在扫描结果中，搜索与预览要恢复的文件，也需要花费时间。临时有事不能继续操作怎么办呢？DiskGenius提供了保存当前扫描进度结果的功能，如下图：



暂停、停止数据恢复扫描，或扫描过程自然结束后，右键点击恢复数据的分区或硬盘，可以保存文件恢复进度。

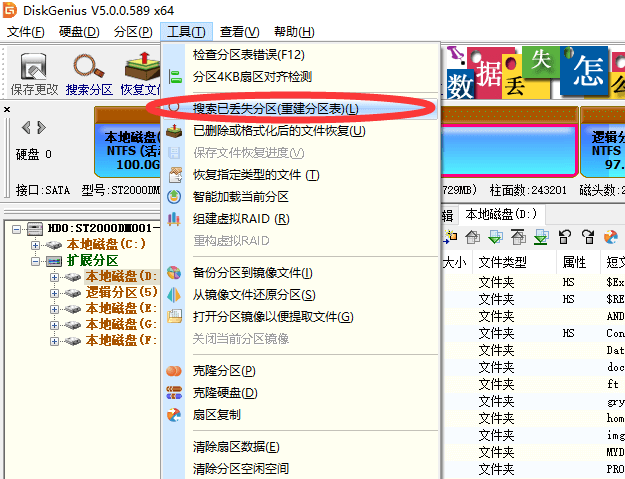
这样，下一次继续恢复同一个硬盘或分区的数据时，在恢复选项窗口中，可以直接调用保存的文件恢复进度，如下图：



点击“加载扫描进度”，可以直接导入上次扫描的文件恢复进度，不必再次扫描，极大地节省了数据恢复的时间。

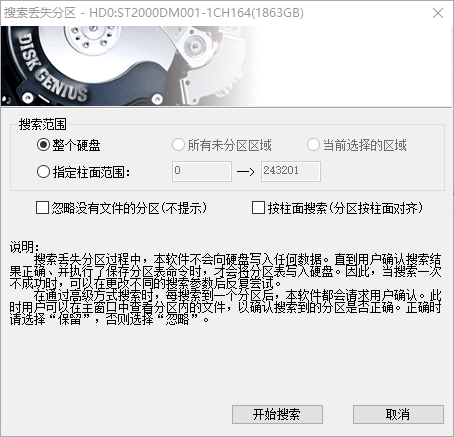
### 3、分区恢复

在使用DiskGenius的过程中，DiskGenius还有分区恢复的功能，如下图：



进入分区恢复操作

然后会弹出搜索已丢失分区的选项窗口，如下图：



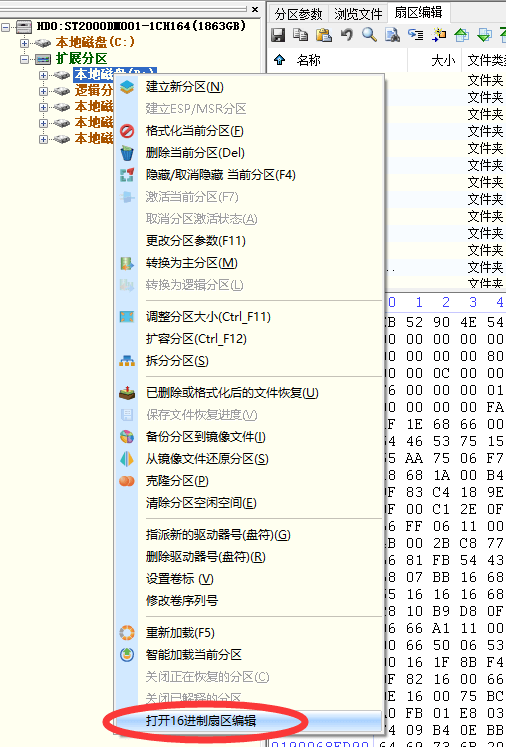
某些情况下，使用分区恢复功能非常方便，恢复速度极快，可以实现原盘恢复（不需要额外复制恢复出来的数据）等。

但分区恢复对用户的要求比较高，需要对原来的硬盘分区情况有一定的了解，涉及到系统分区的地方还要注意系统启动等问题，本文不做进一步的讨论，有兴趣的用户可以查看DiskGenius官网上的[在线帮助文档](https://www.diskgenius.cn/help/)。

### 4、手工数据恢复 – 扇区编辑

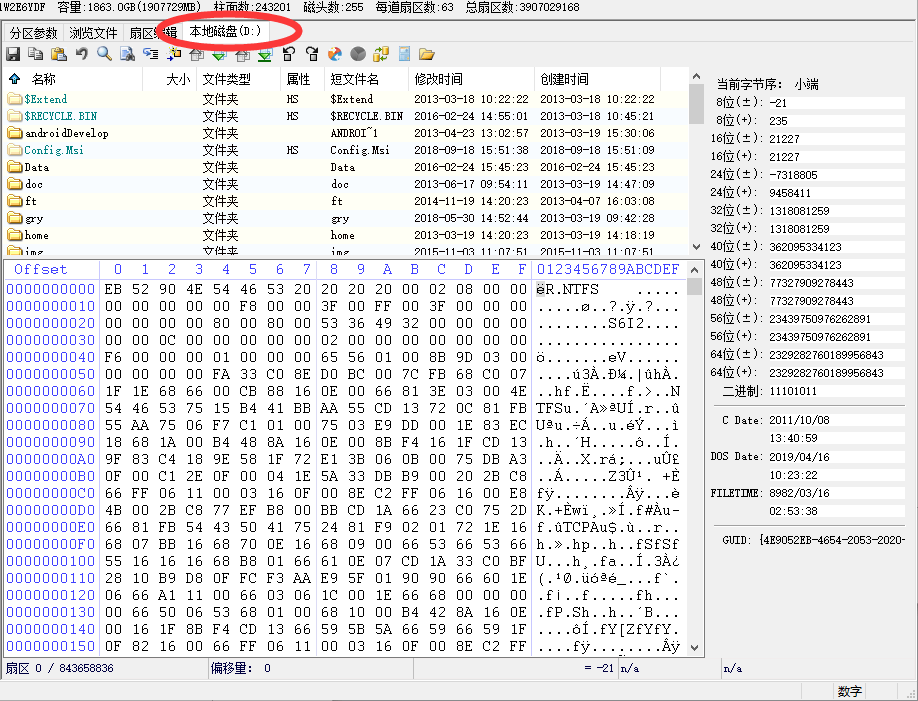
对于专业的数据恢复工程师来说，虽然DiskGenius软件本身的数据恢复功能已经足够强大，但某些情况下，直接修改硬盘中错误的参数及关键数据，有时更为方便。通常，做类似操作时，一般都是用WinHex这个工具软件，实际上，DiskGenius提供了扇区编辑功能，也可以直接修改硬盘中的数据，结合DiskGenius的分区管理等功能，使用上比WinHe更灵活，更方便。

选择硬盘或分区，点击鼠标右键，在快捷菜单中，选择“打开16进制扇区编辑”，如下图：



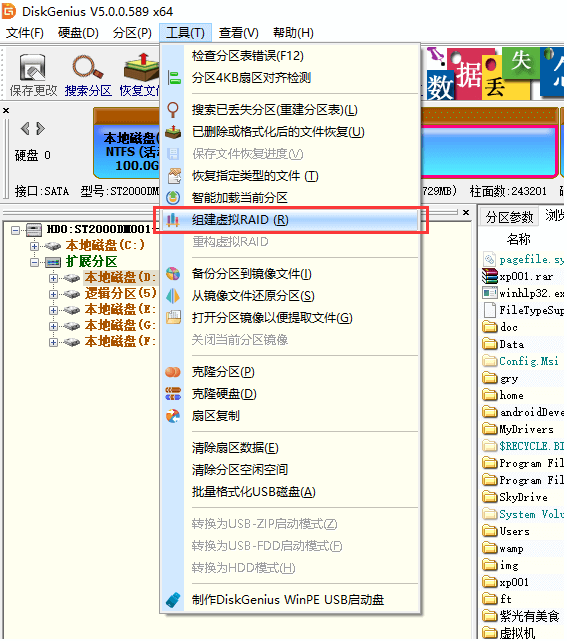
进入扇区编辑操作，直接编辑硬盘数据

相应的，右侧会出现该分区或硬盘的扇区编辑面板，如下图：

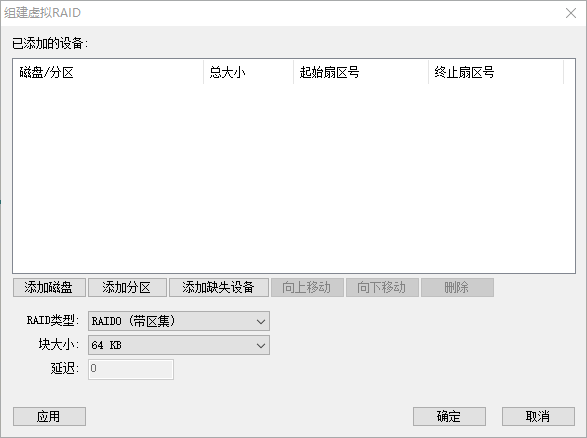
扇区编辑的界面与操作，同WinHex类似，功能上也大致相同，但结合DiskGenius的其它功能，使用上更加灵活、方便。

### 5、服务器RAID恢复

DiskGenius支持服务器Raid恢复，用户可以使用DiskGenius虚拟重组Raid，然后恢复数据，如下图：



主菜单，工具 – 组建虚拟RAID



用户可以添加硬盘，设置RAID类型等参数，组建虚拟RAID后恢复数据。

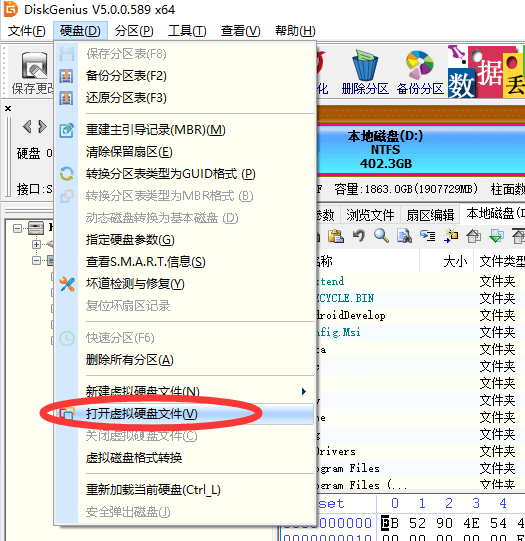
RAID恢复属于比较高级的操作，对RAID不熟悉的用户可以联系DiskGenius专家团队，远程指导RAID恢复。

### 6、虚拟机数据恢复

虚拟机的使用越来越多，怎么用DiskGenius恢复虚拟机的数据呢？你可能会想到，在虚拟机中安装DiskGenius，然后恢复数据…

但时这种方法不但比较麻烦，有时还容易出现其它问题。更有效的方法是，在真实的电脑中运行DiskGenius，然后加载虚拟机的虚拟硬盘文件，加载后就可以像恢复普通硬盘那样，恢复虚拟硬盘中的数据了，DiskGenius支持所有主流的虚拟硬盘格式。

加载虚拟硬盘的方法：主菜单，硬盘 – 打开虚拟硬盘文件，如下图：



加载虚拟硬盘后，就可以像普通硬盘一样恢复数据了

## **内存取证例题：**祥云杯2021层层取证

给出了磁盘镜像和内存镜像。

ftk imager打开disk image，全盘导出dd格式。

img转vdi，用virtualbox创建一个空的虚拟机，挂载vdi磁盘，可以启动。

"D:\Program Files\Oracle\VirtualBox\VBoxManage.exe" convertfromraw -format VDI test1.img test1v.vdi

efdd扫内存中的密钥。

Algorithm:'BitLocker' (incl. 'To Go') Volume Master KeyKey data (hex): 9dc9d924d0c693aa9ec9fb9b389e2f24c96c11c231a18ea9dbd3722a6440bb9f

volatility mimikatz读内存中的用户密码。

volatility -f memdump.mem --profile=win7SP1x64 mimikatzVolatility Foundation Volatility Framework 2.6Module User Domain Passwordwdigest XiaoMing PC xiaoming\_handsome

把efdd安装进虚拟机，用之前扫内存密钥生成的evk文件解密bitlocker分区。得到一个pcap文件。

recovery pin:549714-116633-006446-278597-176000-708532-618101-131406

找udp.stream eq 32找到rar。rar解压密码是与计算机开机密码相同。解压得到flag.docx文件。

docx密码是xiaoming1314，在桌面的便签下面。

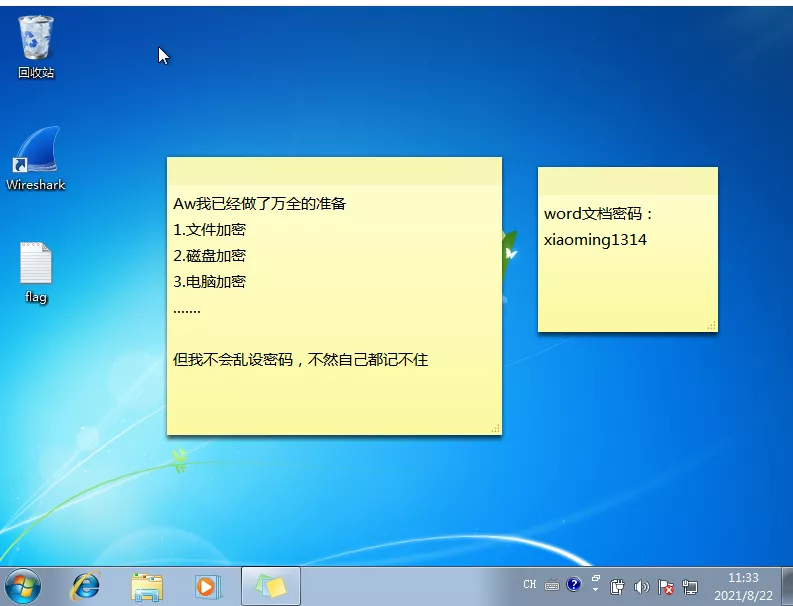


image-20210822113327725

### **ChieftainsSecret**

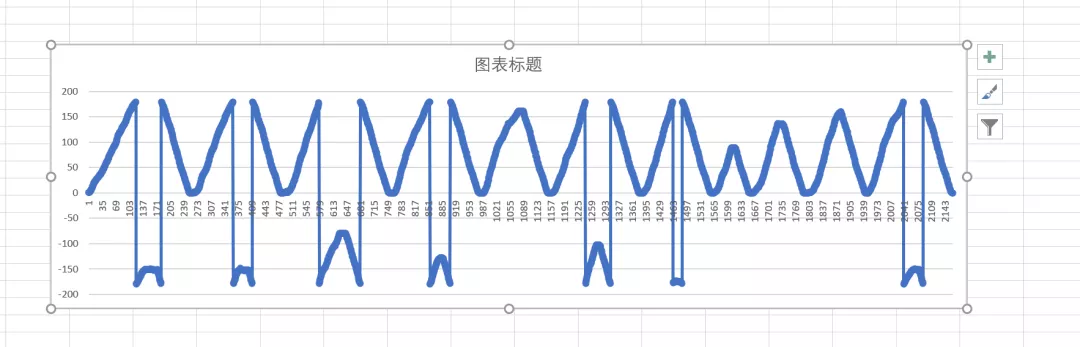
根据接线图，github找到TLE5xxx的库，根据datasheet，TLE5xxx是通用的。

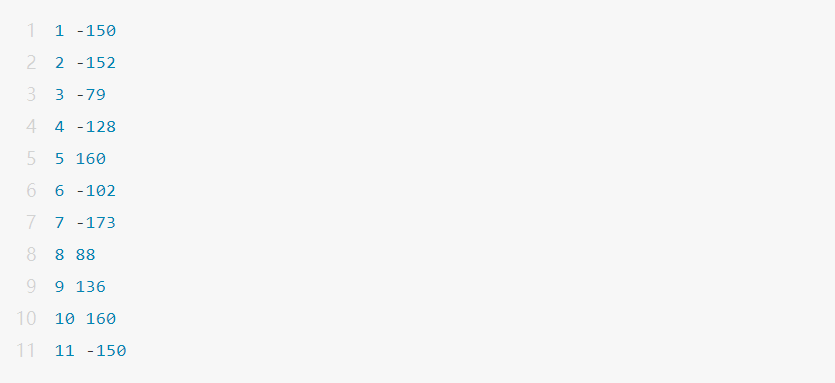
https://github.com/CreativeRobotics/TLE5009

借鉴其核心代码，将读数转换成角度，根据接线图确定PC0-3的引脚定义。

**#代码里有个clampS限制sin和cos的绝对值最大值为1，如果加上的话，能看到初始位置是45度，但是加上了输出的结果非常方，精度损失多到无法区分7和8。不加能看到正常的结果，但不滤波，看不出初始位置是45度。尝试修改库本身，在c++非arduino下运行，把数据手动喂给库，也有精度损失的问题。没有实际使用过CreativeRobotics/TLE5009这个库，不清楚是这个库本身的问题还是我的使用问题。**data = open("adc.csv").readlines()data = data[1:]  
var1s = []var2s = []var3s = []var4s = []  
for line in data: s = line.strip().split(",") var1s.append(s[0]) var2s.append(s[1]) var3s.append(s[2]) var4s.append(s[3])  
from math import atan2  
def clampS(var,limit): #constrain to the limit value if(var > limit): return limit; elif(var < -limit): return -limit; else: return var;  
#//var1=sin\_p#//var2=sin\_n#//var3=cos\_p#//var4=cos\_n  
sin\_p = var1ssin\_n = var2scos\_p = var3scos\_n = var4s  
sinScale=1.0;cosScale=1.0;TODEGREES=57.295779513082320876798154814105;  
for i in range(len(var1s)): sinP = float(sin\_p[i]); sinN = float(sin\_n[i]); cosP = float(cos\_p[i]); cosN = float(cos\_n[i]); sinD = sinP - sinN; cosD = cosP - cosN; sine = sinD\*sinScale; cosine = cosD\*cosScale; #sine = clampS(sine, 1.0); #cosine = clampS(cosine, 1.0); angle = atan2(sine, cosine); angleD=angle\*TODEGREES; print(angleD);

保存输出到csv，用excel打开，生成折线图进行分析。

image-20210822011530450

摘录其中11个点，用geogebra进行画图。  


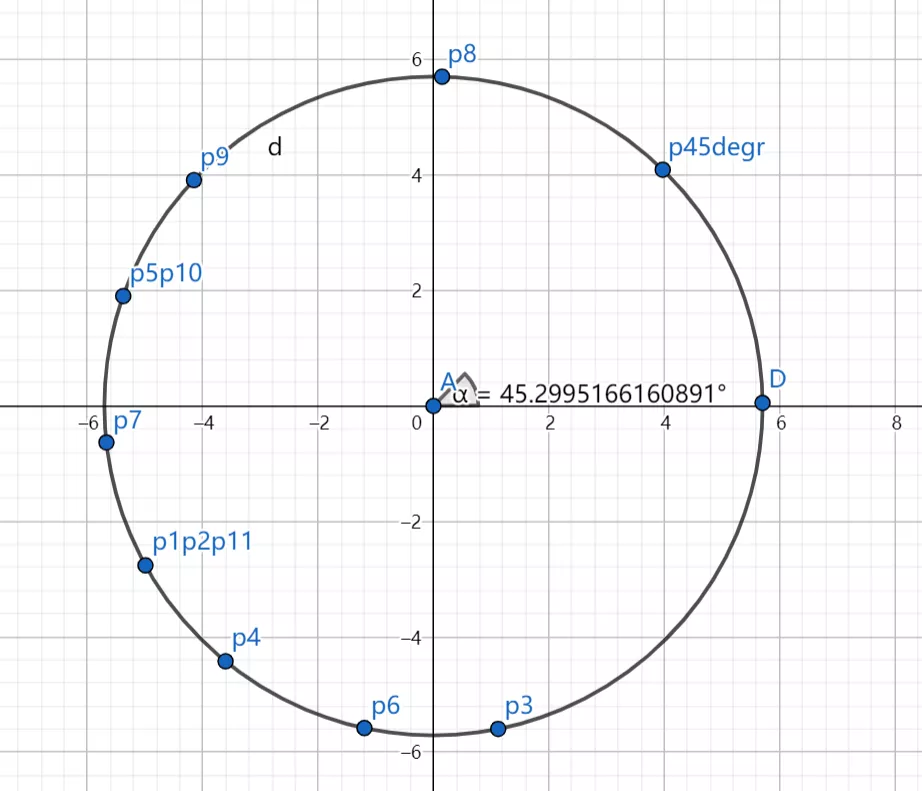


image-20210822012739766

将画图叠加到电话的图上，旋转~45度，读出flag。



image-20210822014908524

77085962457