目录结束标识（End of Central Directory Record)

存在于整个归档包的结尾，用于标记压缩的目录数据的结束。每个压缩文件必须有且只有一个结束标识。

50 4B 05 06：目录结束标记

00 00：当前磁盘编号

00 00：目录区开始磁盘编号

01 00：本磁盘上纪录总数

01 00：目录区中纪录总数

59 00 00 00：目录区尺寸大小

3E 00 00 00：目录区对第一张磁盘的偏移量

00 00：ZIP 文件注释长度

1

2

3

4

5

6

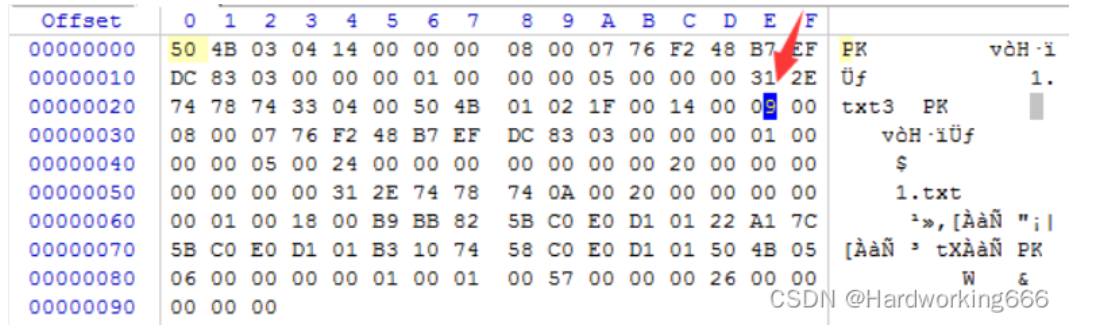
7

8

zip伪加密

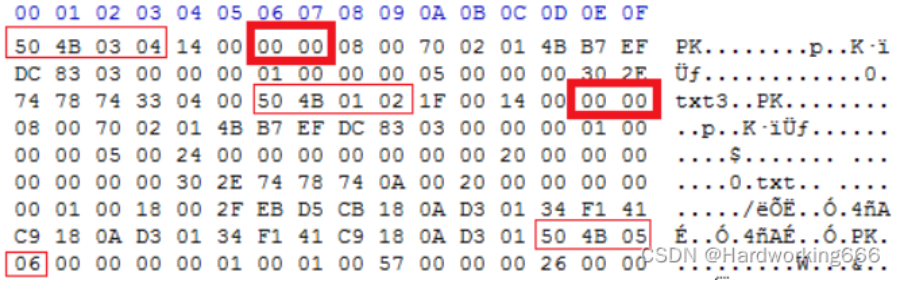
zip伪加密是在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩包。

如果把第二个加密标记位的00 00改为09 00，打开就会提示有密码：



其实改成09只是举的一个例子，只要末位是奇数，就代表加密，反之，末位是偶数代表未加密。

有时这里是01，也代表加密！不用更改！



识别真假加密

无加密

压缩源文件数据区的全局加密应当为00 00

且压缩源文件目录区的全局方式位标记应当为00 00

假加密

压缩源文件数据区的全局加密应当为00 00

且压缩源文件目录区的全局方式位标记应当为09 00

真加密

压缩源文件数据区的全局加密应当为09 00

且压缩源文件目录区的全局方式位标记应当为09 00

————————————————

1. 常用命令插件

volatility -f [image] --profile=[profile] [plugin]

volatility -f [对象] --profile=[操作系统] [插件参数]

在分析之前，需要先判断当前的镜像信息，分析出是哪个操作系统 命令imageinfo即可获取镜像信息。

Volatility -f xxx.vmem imageinfo

在查到操作系统后如果不确定可以使用以下命令查看

volatility - f xxx.vmem --profile= [操作系统] volshell

————————————————

❤可以先查看当前内存镜像中的用户printkey -K “SAM\Domains\Account\Users\Names”

volatility -f 1.vmem –profile=Win7SP1x64 printkey -K “SAM\Domains\Account\Users\Names”

❤查看用户名密码信息(密码是哈希值，需要john爆破) hashdump

volatility -f 1.vmem --profile=Win7SP1x64 hashdump

查看当前操作系统中的 password hash，例如 Windows 的 SAM 文件内容(mimikatz插件可以获取系统明文密码)

❤如果john爆破不出来，就使用 lasdmp 查看强密码 lsadmp

volatility -f 1.vmem --profile=Win7SP1x64 lsadump

❤查看进程pslist

volatility -f 1.vmem --profile=Win7SP1x64 pslist

pslist：该插件列举出系统进程，但它不能检测到隐藏或者解链的进程，psscan可以

❤查看已知进程pslist

volatility -f 1.vmem --profile=Win7SP1x64 pslist -p 2588

❤隐藏或解链的进程psscan

volatility -f 1.vmem --profile=Win7SP1x64 psscan

psscan：可以找到先前已终止(不活动)的进程以及被rootkit隐藏或解链的进程

❤查看服务 查询服务名称svcscan

volatility -f 1.vmem --profile=Win7SP1x64 svcscan

svcscan：扫描 Windows 的服务

❤查看浏览器历史记录,获取当前系统浏览器搜索过的关键词 iehistory

volatility -f 1.vmem --profile=Win7SP1x64 iehistory

❤查看网络连接 获取当前系统 ip netscan

volatility -f 1.vmem --profile=Win7SP1x64 netscan

有一些版本 这个命令是使用不了 这里我们就要使用（connscan,connections)

❤查看网络连接connscan

volatility -f 1.vmem --profile=Win7SP1x64 connscan

connscan：查看网络连接

❤查看网络连接connections

volatility -f 1.vmem --profile=Win7SP1x64 connections

connections：查看网络连接

❤查看命令行操作，显示cmd历史命令 cmdscan

volatility -f 1.vmem --profile=Win7SP1x64 cmdscan

cmdscan：可用于查看终端记录

❤查看进程命令行参数（具体一些可疑进程的参数指令）cmdline

volatility -f 1.vmem --profile=Win7SP1x64 cmdline

❤扫描所有的文件列表 filescan

volatility -f 1.vmem --profile=Win7SP1x64 filescan

（linux配合 grep 命令进行相关字符定向扫描，如：grep flag、grep -E ‘png|jpg|gif|zip|rar|7z|pdf|txt|doc’）

例

volatility -f 1.vmem --profile=Win7SP1x64 filescan grep "flag.txt"

cat system.txt|grep -i computername

❤查看文件内容dmpfiles

volatility -f 1.vmem --profile=Win7SP1x64 dumpfiles -Q 0xxxxxxxx -D ./

需要指定偏移量 -Q 和输出目录 -D

dumpfiles：导出某一文件(指定虚拟地址)

❤查看当前展示的notepad内容 notepad

volatility -f 1.vmem --profile=Win7SP1x64 notepad

查看当前展示的 notepad 文本（–profile=winxp啥的低版本可以，win7的不行，可以尝试使用editbox）

❤显示有关编辑控件（曾经编辑过的内容）的信息 editbox

volatility -f 1.vmem --profile=Win7SP1x64 editbox

editbox：显示有关编辑控件（曾经编辑过的内容）的信息 查看内存中记事本的内容

❤提取进程memdump

volatility -f 1.vmem --profile=Win7SP1x64 memdump -p xxx --dump-dir=./

memdump：提取出指定进程，常用foremost 来分离里面的文件

需要指定进程-p [pid] 和输出目录 -D

memdump -p 332 -D XX/

提取进程 -p 进程号 -D 当前输出路径（导出为332.dmp）

dump出来的进程文件，可以使用 foremost 来分离里面的文件，用 binwak -e 不推荐

strings -e l 2040.dmp | grep flag 查找flag

❤屏幕截图screenshot

volatility -f 1.vmem --profile=Win7SP1x64 screenshot --dump-dir=./

screenshot：保存基于GDI窗口的伪截屏

❤查看注册表配置单元hivelist

volatility -f 1.vmem --profile=Win7SP1x64 hivelist

hivelist: 列出所有的注册表项及其虚拟地址和物理地址

❤查看注册表键名hivedmp

volatility -f 1.vmem --profile=Win7SP1x64 hivedump -o 0xfffff8a001032410

❤查看注册表键值printkey

volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "ControlSet001\Control\ComputerName\ComputerName"

❤ 获取主机名 printkey

volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "ControlSet001\Control\ComputerName\ComputerName"

❤列出用户名 pringkey

volatility -f 1.vmem --profile=Win7SP1x64 printkey -K "SAM\Domains\Account\Users\Names"

❤查看运行程序相关的记录，比如最后一次更新时间，运行过的次数等。serassist

volatility -f 1.vmem --profile=Win7SP1x64 userassist

❤最大程序提取信息timeliner

volatility -f 1.vmem --profile=Win7SP1x64 timeliner

timeliner: 将所有操作系统事件以时间线的方式展开

❤查看剪贴板信息clipboard

volatility -f 1.vmem --profile=Win7SP1x64 clipboard

clipboard：查看剪贴板信息

❤显示关于计算机及其操作系统的详细配置信息（插件）systeminfo

volatility -f 1.vmem --profile=Win7SP1x64 systeminfo

systeminfo：显示关于计算机及其操作系统的详细配置信息（插件）

❤恢复被删除的文件mftparser

volatility -f 1.vmem --profile=Win7SP1x64 mftparser

mftparser：恢复被删除的文件

❤查看环境变量envars

volatility -f 1.vmem --profile=Win7SP1x64 envars

envars：查看环境变量

❤列出某一进程加载的所有dll文件dlllist

volatility -f 1.vmem --profile=Win7SP1x64 dlllist -p 2588

dlllist: 列出某一进程加载的所有dll文件

需要指定进程-p [pid]

❤程序版本信息 verinfo

volatility -f 1.vmem --profile=Win7SP1x64 verinfo

列出PE｜程序版本信息

❤产看进程树，可以轻松了解各进程之间的关系：父进程与子进程 pstree

volatility -f 2008.raw –profile=Win2008R2SP1x64 pstree

在进程中PPID比PID还大，那就可能这个进程有异常程序

❤从内存文件中找到异常程序植入到系统的开机自启痕迹 shimcache

volatility -f 2008.raw –profile=Win2008R2SP1x64 shimcache

七，内存取证的大致思路

首先确定镜像是何种操作系统的，命令imageinfo即可获取镜像信息。

需要获取的是计算机在这一时刻运行了哪些进程。

Volatility提供了众多的分析进程的命令，如pstree、pesscan、pslist……

filescan命令可以对打开的文件进行扫描。

命令dumpfile和memdump命令将相关数据导出，然后对导出的数据进行二进制分析。

简单说只要熟悉Volatility工具的常用命令，并能够对结合其他类型的知识（图片隐写、压缩包分析等）对提取出的文件进行分析，便可轻松解决。

但当然具体问题具体分析吗 但插件就上面的

