Forensic

1. 内存镜像分析

volatility(Kali)

volatility imageinfo –f ${file} #查看镜像文件信息，主要是操作系统版本

volatility –p ${WinXPSP2x86} –f ${file} [plugin] #使用相关插件读取镜像内存信息

volatility –p WinXPSP2x86 –f ${file} pstree #查看pstree

volatility –p WinXPSP2x86 –f ${file} cmdline #查看进程启动时的命令，只包含命令和参数，不显示任何管道、重定向的信息

volatility –p WinXPSP2x86 –f ${file} cmdscan #从cmd/bash history中提取历史命令，显示命令行中完整的命令

volatility –p WinXPSP2x86 –f ${file} connscan #查看连接信息

volatility –p WinXPSP2x86 –f ${file} filescan #分析出加载进内存的所有文件及其物理偏移

volatility –p WinXPSP2x86 –f ${file} dumpfiles #dump出指定文件，-p参数指定进程号，同时dump出该进程对应的可执行文件和加载的所有文件；-o指定物理偏移，效果和-p类似；-Q指定物理偏移，用于dump非可执行文件。

volatility –p WinXPSP2x86 –f ${file} notepad

1. 磁盘镜像分析

AccessData FTK Imager

数据恢复

1. winhex

使用winhex打开磁盘镜像文件，可以根据文件类型进行数据恢复。

tools->Disk Tools->File Recovery by Type

