Forensic

1. 内存镜像分析

volatility(Kali)

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

