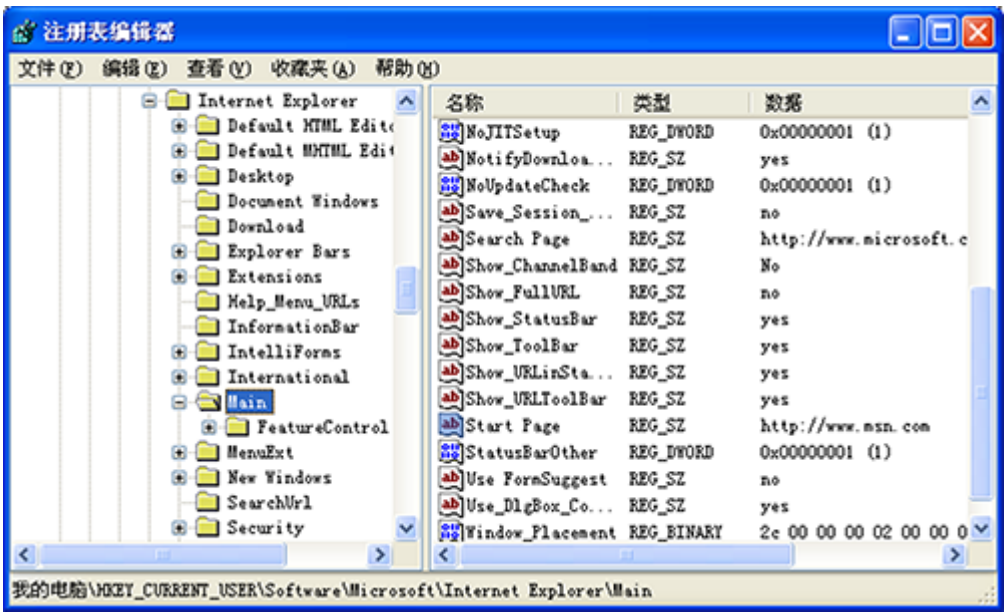
数字取证技术(Digital Forensics Technology)笔记III

Windows操作系统取证技术

👉**知识点(注册表的功能)**:Windows注册表是一个集中式分层数据库,每一个文件夹表示注册表中的项,项又包括子项和值项,项和子项的关系就像目录可以包含子目录一样.例子:查看用户的IE浏览器默认首页;

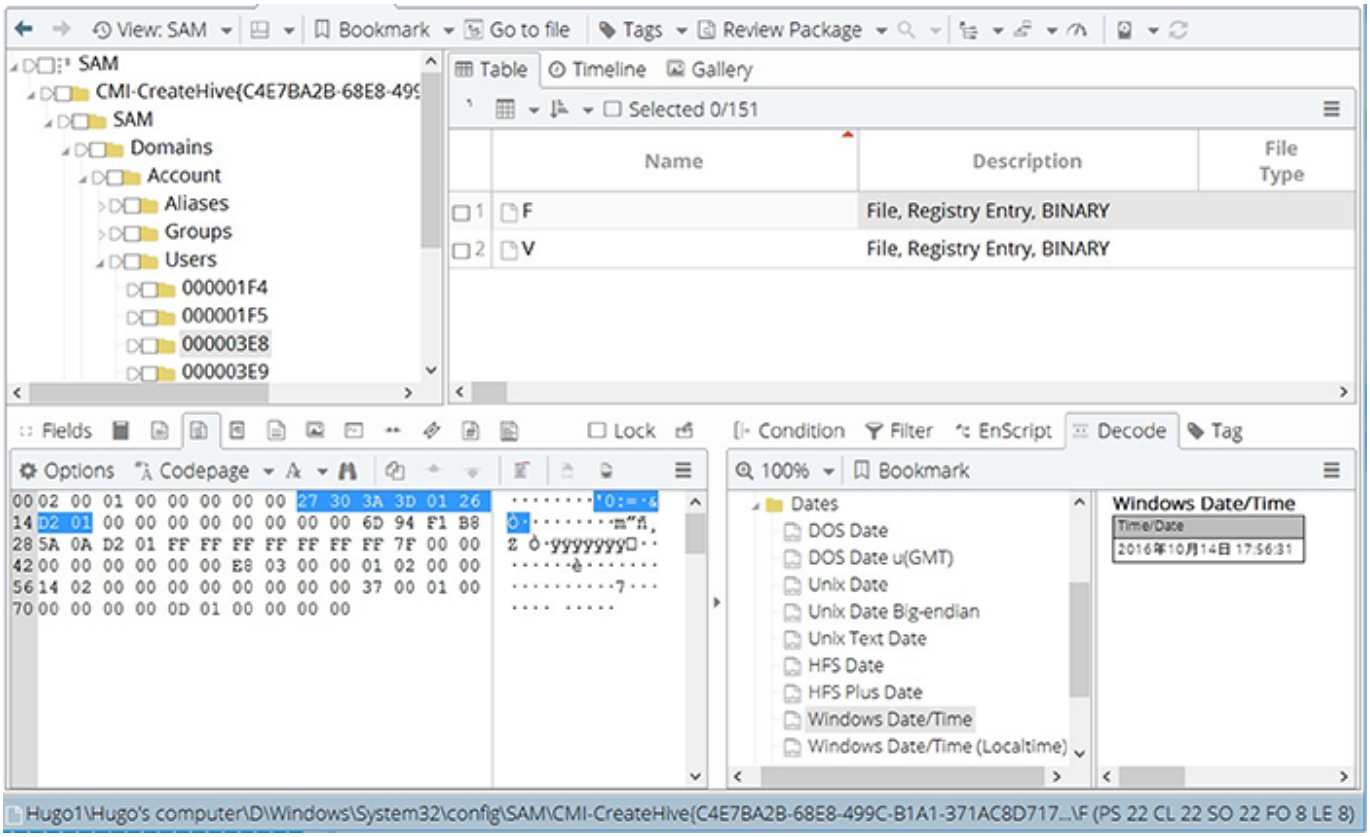


👉**知识点(Windows注册表核心文件)**:Windows注册表用于存储系统配置、用户设置和软件信息等.Windows系统中,注册表的核心由几个主要的文件组成,这些文件在系统中是隐藏的,存储在`%SystemRoot%\System32\config\`目录下.核心的注册表文件包括:

1. **SYSTEM**:存储了系统级的配置信息,如硬件设备、系统服务等.
2. **SOFTWARE**:包含了所有用户级软件和系统软件的设置.
3. **SAM**:存储了安全账户管理器信息,包括用户账户和安全描述符.
4. **SECURITY**:包含安全相关信息,例如安全策略和访问控制列表.

除了这些核心文件,还有一些其他重要的注册表文件:

- **DEFAULT**:包含了默认用户配置的注册表信息,适用于新用户的初始配置.
- **NTUSER.DAT**:位于每个用户的个人目录下(`%USERPROFILE%`),存储了特定用户的设置和配置.
- **USRCLASS.DAT**:存储了每个用户的类注册信息,也位于每个用户的个人目录下的`AppData\Local\Microsoft\Windows`目录中.



👉**知识点(Windows注册表的取证)**:主要的工具和技术:

1. **注册表编辑器(Registry Editor)**:Windows自带的注册表编辑器(regedit.exe)是最基本的工具之一.它允许用户浏览、编辑和导出注册表中的键值.虽然它主要用于系统管理和配置,但在取证工作中也可以用于快速查看注册表的内容.

2. **注册表取证工具**:如EnCase Forensic、Registry Recon、FTK Registry Viewer、X-Ways Forensics等.这些工具可以帮助分析人员以更有效的方式浏览、搜索、导出和分析注册表中的数据.提供了用户友好的界面和高级的分析功能,有助于取得更深入的证据.

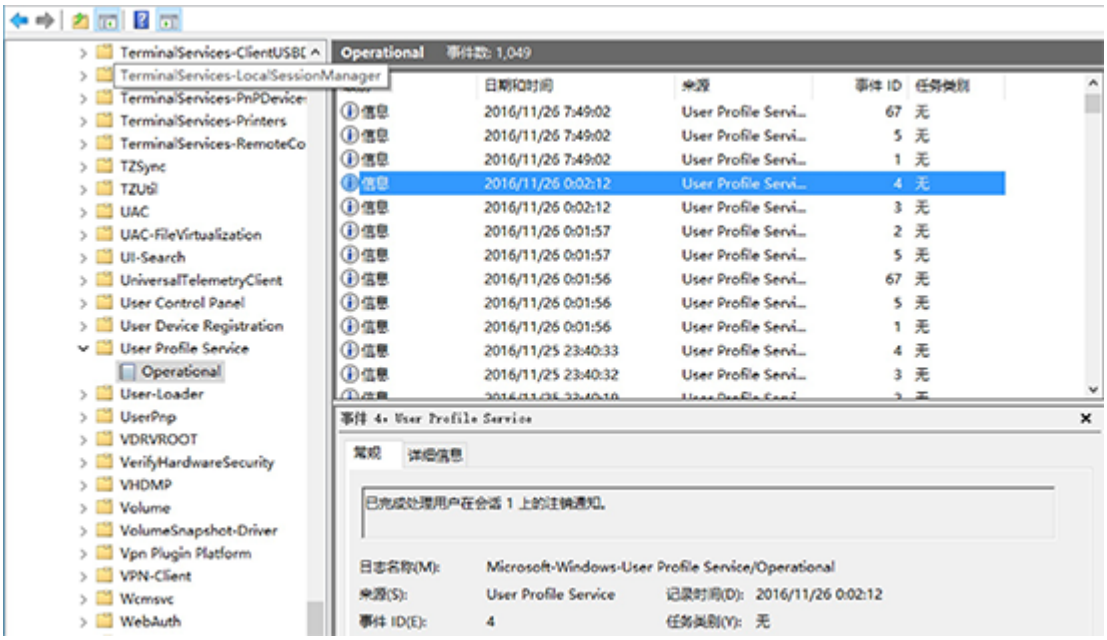
3. **取证镜像工具**:在进行注册表取证时,通常需要先获取系统的镜像.取证镜像工具如FTK Imager、EnCase、DD等可用于创建完整的磁盘镜像,包括注册表文件和其他系统文件,以确保数据的完整性和可靠性.

4. **数据恢复工具**:注册表文件可能已损坏或被删除.数据恢复工具如Recuva、R-Studio等可用于尝试恢复已删除或损坏的注册表文件,从而帮助还原重要的取证数据.

5. **静态和动态分析技术**:在进行注册表取证时,可以采用静态和动态分析技术.静态分析涉及对注册表文件的离线分析,而动态分析则涉及在运行时监视系统的注册表活动.这两种方法可以结合使用,以获取更全面的证据.

👉**知识点(Windows事件日志取证)**:Windows事件日志提供了丰富的数据,可用于取证分析,特别是在监测和记录用户行为,如登录、插拔移动设备以及修改系统时间等方面.主要工具和方法:

- **Event Viewer (事件查看器)**:Windows自带的Event Viewer是最基础的工具,允许用户查看和搜索本地计算机的事件日志.可以查看安全日志来跟踪用户登录和注销活动,系统日志和应用程序日志也可提供关于设备事件和系统时间更改的信息.
- **LogParser**:Microsoft提供的强大工具,能以SQL风格查询日志数据,非常适用于从大量日志数据中快速提取信息.可用于分析各种类型的日志文件,包括Windows事件日志.
- **Windows Sysinternals**:提供了一系列强大的工具,如Process Monitor,可以实时监控Windows进程和线程的活动,包括对事件日志的访问.
- **用户登录行为**:Windows用户登录/注销的事件日志中的事件ID 1到5;可查看登录尝试的详细信息,包括用户名、登录类型、登录时间和登录源.对这些事件进行监控和分析可以帮助识别未授权的登录尝试或其它可疑活动.
- **用户插拔移动设备行为**:事件ID 20001或20003(关于即插即用设备的事件)可用于跟踪USB设备的插拔活动.审计这些事件可以帮助识别潜在的数据泄露或非法访问尝试.
- **用户修改系统时间的行为**:事件ID 4616(系统时间被更改)记录了系统时间的更改.分析这类事件可以帮助确定是否有企图隐藏或伪造其他安全事件的行为.
- **用户无线网络接入的行为**:在WLAN-AutoConfig和NetworkProfile日志文件中有相关信息,事件ID 10001(网络接入/断开).



👉**知识点(磁盘与文件)**:磁盘存储和文件系统是计算机系统中核心的组成部分,它们负责管理和存储文件及目录的方式.不同的文件系统具有不同的特点、设计理念以及优缺点:

- FAT(File Allocation Table)

    - **特点**:FAT文件系统是最早广泛使用的文件系统之一,它简单且与多种操作系统兼容.文件存储在磁盘上时使用一个分配表来记录文件的位置.
    - **设计思维**:设计上追求简单和跨平台兼容性,易于实现和维护.适用于小容量存储设备,如早期的个人计算机和移动存储设备.
    - **优点**:兼容性好,几乎所有的操作系统都能识别和读写FAT文件系统.结构简单,易于实现,在嵌入式系统和小型设备中仍然非常流行.
    - **缺点**:不支持大文件(FAT32的单个文件最大限制为4GB)和大磁盘.没有内置的文件加密和安全控制机制.文件碎片整理比较频繁,随着使用时间的增加,性能可能下降.
- NTFS(New Technology File System):
    - **特点**:NTFS是由微软开发,用于替代FAT的更先进的文件系统,现在广泛用于Windows操作系统中.支持大文件和大容量存储,具有日志记录、文件权限和数据恢复功能.
    - **设计思维**:提供高性能和高可靠性,适合企业和专业环境.引入了元数据概念和更复杂的数据结构,以支持详细的文件安全权限和磁盘配额.
    - **优点**:支持文件压缩和加密.支持文件权限和安全设置,更适合企业级应用.系统出错时,恢复能力更强,支持事务日志处理.
    - **缺点**:相对FAT,NTFS复杂,消耗的系统资源也更多.在非Windows平台上的兼容性和支持较差.
- EFS(Encrypted File System)
    - **特点**:EFS不是一个独立的文件系统,而是构建在NTFS之上的一个功能,允许用户对文件进行加密.加密是透明的,即用户在访问文件时不需进行额外操作,系统自动加解密.
    - **设计思维**:设计上注重数据安全,目的是保护存储在硬盘上的敏感数据不被未授权访问.与NTFS紧密集成,保持文件系统的高效性和安全性.
    - **优点**:对用户透明,易于使用,提供强大的数据安全保护.结合NTFS的其他功能,如文件权限,为企业数据提供双重保障.
    - **缺点**:文件加密虽然提高了安全性,但一旦加密密钥丢失,数据将不可恢复.性能开销相对较大,特别是在大量文件加密和解密的情况下.

👉**知识点(Windows下的文件取证技术)**:Windows操作系统中的文件取证是一个重要的过程,涉及对文件系统内的数据进行详细分析,以获取法律和安全相关的证据.在Windows环境下,文档文件、图片文件、视频文件的取证尤为重要,因为这些类型的文件常常包含敏感或关键信息.下面介绍这些文件的取证技术及一些简单例子.

- **文档文件取证**:使用专门的取证工具,如FTK(Forensic Toolkit) 或 EnCase,这些工具可以帮助提取文档文件的元数据和内容,包括创建日期、修改日期、作者信息等.分析文档的内容和结构,查找隐藏信息或修改痕迹,如Word、Excel、PDF等文件中的修订记录和注释.例子:在一起骚扰起诉的调查中,取证分析人员使用FTK工具从疑犯电脑中恢复了删除的Word文档.通过分析这些文档的修订记录,确认了骚扰信件的起草和修改过程,为案件提供了关键证据.

- **图片文件取证**:图片文件的取证通常涉及分析图片的EXIF数据,这包括拍摄时间、设备信息、地理位置信息等.使用工具如PhotoRec进行恢复已删除的图片.分析图片内容,使用StegExpose等工具检测隐写术,即分析图片是否被用来隐藏其他文件或信息.例子:在一起涉密拍摄案件中,调查人员通过分析嫌疑人相机中的照片EXIF信息,确定了照片的拍摄时间和地点.与案发地点和时间的匹配加强了案件的证据链.

- **视频文件取证**:视频文件取证涉及提取视频文件的元数据,如编码信息、创建和修改时间等.使用视频分析软件,如Amped FIVE,可以进行视频内容的增强、格式转换、速度分析等,以辅助取证分析.检查视频文件是否经过编辑或篡改.例子:在一起交通事故责任争议中,通过对事故监控视频的分析,取证专家使用Amped FIVE软件调整了视频的清晰度和对比度,清晰地显示了事故发生时各车辆的位置和行驶状态,帮助法庭确定了责任方.

思考题

(♞思考) Windows事件日志取证中,用户登录事件对应"已收到用户在会话的登录通知","正常登录","完成处理用户在会话的登录通知","已收到用户在会话上的注销通知","已完成处理用户在会话上的注销通知"的 EventID 分别是几多?

答:分别是1,67,2,3,4;

(♞思考) 一家公司怀疑一个高级员工在离职前删除了重要文件.请描述如何利用Windows文件系统的日志和取证工具来确定此员工是否删除了文件,包括查找哪些日志记录.

答:使用Windows事件查看器(Event Viewer)检查安全日志,特别是关注事件ID 4663(一个对象的访问尝试)和 4656(受保护的对象的访问尝试).这些事件可以显示哪些文件被访问.查找事件ID 4660(删除对象),它记录了文件删除活动.利用文件系统日志分析工具,如 USN Journal Viewer,分析NTFS驱动器的USN日志,这可以帮助识别文件创建、修改和删除的时间线.考虑到文件可能被彻底删除,使用如Recuva或EnCase等数据恢复工具尝试恢复已删除的文件,以便进一步分析.