# 数字取证技术(Digital Forensics Technology)笔记V

> 这部分内容涵盖了IOS系统取证技术,移动终端取证技术和电子数据取证环境的知识点.

#### 电子数据取证环境

☞**知识点**:台式计算机

- **硬盘种类**:通常使用机械硬盘(HDD)和固态硬盘(SSD).
- **接口类型**:SATA用于大多数HDD和SSD连接;较新的台式机可能支持NVMe接口,一般通过PCIe插槽直接连接至主板,提供更快的数据传输速度.

☞**知识点**:笔记本电脑

- **硬盘种类**:更常使用固态硬盘(SSD)因其抗震性能好;依然有使用2.5英寸的机械硬盘(HDD)的情况.
- **接口类型**:多数采用SATA接口,高性能笔记本电脑可能采用NVMe接口SSD.

☞**知识点**:苹果电脑(MacBook/iMac)

- **硬盘种类**:早期型号可能会有机械硬盘(HDD),但现代Apple设备多采用固态硬盘(SSD).
- **接口类型**:MacBook Air和MacBook Pro等新机型会使用专有的闪存存储或NVMe接口SSD,这些接口速度快.

☞**知识点**:苹果手机(iPhone)

- **硬盘种类**:iPhone使用内置非拆卸式的NAND闪存.
- **接口类型**:苹果设备通常通过Lightning或USB-C端口进行数据传输和充电,并采用专用的iOS系统存储文件.

☞**知识点**:安卓手机

- **硬盘种类**:安卓手机一般使用内置的NAND闪存,并且许多设备支持通过microSD卡扩展存储;
- **接口类型**:安卓手机多采用 microUSB 或 USB-C 端口进行数据传输和充电;文件系统更加开放,通常运行与Linux兼容的文件系统,如ext4;

#### IOS系统取证技术

☞**知识点**:时间戳查看:在MacOS中,文件和目录的时间戳信息包括创建时间(c时间),修改时间(m时间),元数据修改时间(md时间)和最后访问时间(a时间).可以使用终端应用程序并利用`ls -la`命令查看文件的详细信息,包括时间戳.也可以使用`stat`命令获取特定文件或目录的时间戳数据.

☞**知识点**:文件保险箱(FileVault)

- **FileVault**:MacOS提供的全盘加密功能称为FileVault,它使用XTS-AES-128加密与4096位秘钥链结合的加密技术.
- **加密解密**:FileVault加密通常在用户层有密码保护.要访问加密数据,取证专家可能需要用户的密码或恢复钥匙.在某些案件中,法律程序可能需要来获取这些信息.
- **取证注意点**:一旦有权访问,取证工具可以在启动到特殊外部驱动器或在保持系统未解锁的状态下,通过创建加密磁盘的物理镜像来提取数据.

☞**知识点**:数据提取

- **备份方法**:利用Time Machine等备份工具制作全盘备份可以作为数据提取的方式.取证专家可以分析这些备份,或直接从中恢复数据.
- **直接提取**:通常需使用专门的取证工具进行直接数据提取,如使用EnCase,FTK或MacQuisition等支持MacOS文件提取的取证工具.
- **逻辑提取**:逻辑提取常用于获取文件和文件系统数据,而不是制作完整的物理镜像.

**移动终端取证技术**

☞**知识点**:人工提取(Manual Extraction)

- **描述**:操作手机,手动获取信息.这可能包括浏览用户数据、短信、通话记录、应用程序数据等.
- **工具**:无需特定工具,但可能需要密码或用户锁定模式的绕过.
- **优点**:简单且不会损坏手机.
- **缺点**:提取数据的范围有限,取证人员可访问的数据量取决于用户权限和手机锁定状态.

☞**知识点**:逻辑提取(Logical Extraction)

- **描述**:使用专业软件通过USB等接口读取手机存储的逻辑信息.
- **工具**:Cellebrite UFED、Oxygen Forensics、XRY等.
- **优点**:相比人工提取可以获得更多的信息,且不需要物理改动设备.
- **缺点**:无法获取已删除或隐藏的数据,受设备保护状态影响较大.

☞**知识点**:JTAG/ISP方法

- **描述**:JTAG/ISP是直接操作手机硬件,通过测试点来获取存储在手机中的数据.
  - **JTAG**(Joint Test Action Group):通过设备上的测试接口,将手机置于特殊模式,直接读取内存数据.
  - **ISP**(In-System Programming):通过直接连接到手机主板上的内存芯片接口进行读取数据.
- **工具**:需要具有JTAG或ISP功能的设备和适当的训练.
- **优点**:能够绕开操作系统获取更深层次的数据.
- **缺点**:需要专业知识和工具,且可能破坏保修.

☞**知识点**:Chip-Off提取方法

- **描述**:物理移除手机上的内存芯片,然后使用特殊的读卡器或编程器提取数据.
- **工具**:芯片拆卸工具、电子显微镜、读卡器、热风枪等.
- **优点**:可以绕过所有软件锁定,直接读取内存数据.
- **缺点**:风险高,可能造成不可逆的损坏.

☞**知识点**:微读方法(Micro-reading / Microscopic Examination)

- **描述**:通过高级显微镜等设备进行芯片的微观结构分析,可能用于密码或加密破解(对NAND或NOR芯片存储层进行微观状态观察,并借助均衡磨损原理等固态介质存储理论进行数据还原).
- **工具**:电子显微镜、专业级实验室设备.
- **优点**:可以用于高难度的数据恢复,如焚毁、损坏的设备.
- **缺点**:需要高度专业的设备和技能,成本和时间消耗大.