盘点电子数据取证中的难点与瓶颈

白虹软件 陆琦 13817065810

顾名思义

- 获取证据
- 《刑礼论》晋 杨乂“或者取证於《春秋》，有意乎寻本以综末。”

舶来词

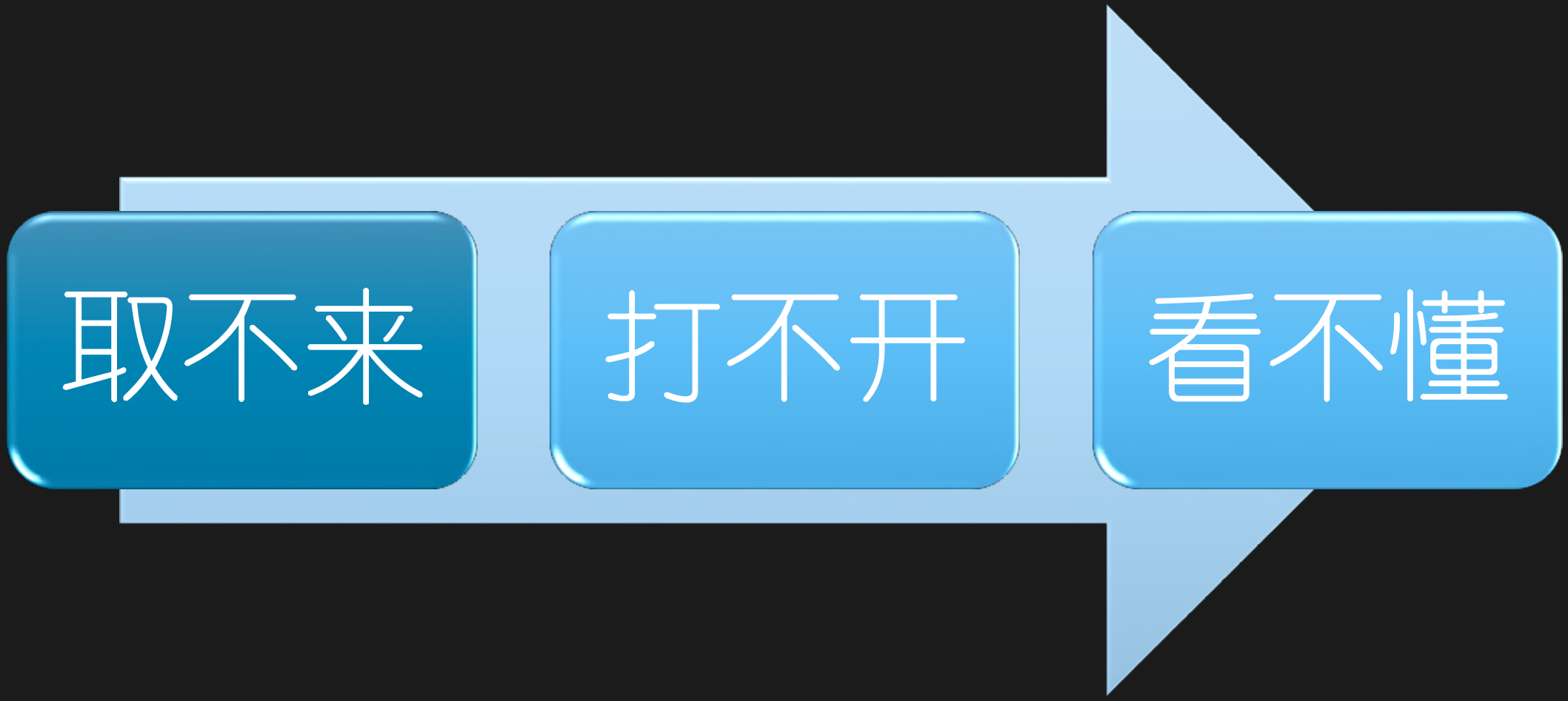
- *Forēnsis（Latin，Roman Times）*
- Forensic Science
- Computational forensics，Forensic accounting

司法解释

- 具有调查取证权的国家机关对于立案处理的案件,为查明案情、收集证据和查获违法行为人而依法定程序进行的专门活动和依法采取的有关强制措施。

什么是取证？

取证中的难点



取不来

现场数据取证

- 数据接口兼容问题
- 软硬件加密问题*
- 智能终端和可穿戴设备
- 数据在云端，终端是入口

远程证据固定

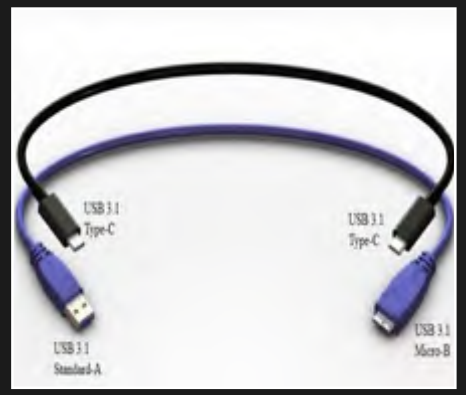
- 所见非所得
- 虚拟化与云服务
- 暗网

数据接口兼容问题

1、硬盘数据接口

- 机械硬盘：IDE、SATA、SAS、SCSI、光纤
- 固态硬盘：SATA、mSATA、NGFF（M.2）
- PCIE SSD

2、移动存储接口



USB1.1、USB2.0、USB3.0、USB3.1（micro、type-c）、OTG、雷口、IDE、SATA、并口、IEEE1394等

3、移动终端接口

- USB接口数据线：m-bus、f-bus、dku5、flash
- Com口

软硬件加密

硬件级

- 加密磁盘/优盘/闪存芯片
- 固件（BIOS、UEFI、EFI、Bootloader）
- 可信计算

软件级

- 加密卷口令（bitlocker、filevault、LUKS、FDE、TC……）
- 系统口令、软件登陆口令（数据库）
- OTP
- 防水墙（透明加密）

智能终端和可穿戴设备

- 锁屏
- 提权
- 芯片
- 异形

数据在云端，终端是入口

- 本地凭证
- 内存取证

打不开

- 随着软硬件技术的日益成熟，硬件设备越来越多、软件种类越来越多，即使获取了数据，往往也需要特定的硬件设备、特定的软件程序来对数据文件进行正确解析。
- 随着加密容器的使用越来越广泛，数据隐藏的方式将越来越丰富，打开容器获取内容的难度也会越来越大。
- 目前找不到一种很好的方法对取证数据文件进行自动化、高效率、低误差的数据清洗和挖掘方案。

怎么办？

没办法吗？

解决思路

- 掌握加密技术，理解解密原理。
- 灵活取证方式，开拓芯片取证。
- 创新工作模式，尝试多次取证。
- 重视无线取证，拓宽工作领域。

1、掌握加密技术 理解解密原理

- 软硬件暴力破解
- 优化解密策略
- 掌握加密机制，发现实现过程中的漏洞和断点

Eg：主流加密软件调研，掌握加密机制及加密容器特征。

2、灵活取证方式 开拓芯片取证

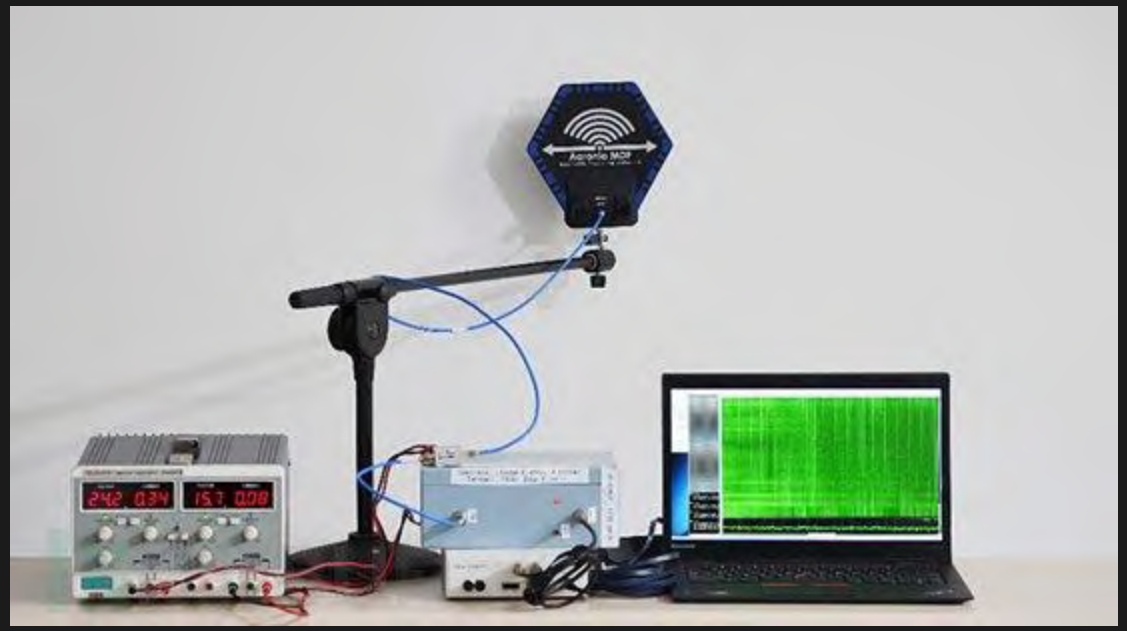
- 集成现场取证工具盘

- 研究内存取证技术、芯片取证技术等

3、创新工作模式 尝试多次取证

边信道

- 隔墙有耳



*邪恶女佣攻击（Evil Maid）

- 总体思路：通过物理接触，修改启动配置文件，实现内核映像劫持。
- 作用：应对TrueCrypt、Bitlocker、PGP等全盘加密技术。
- 多次取证模式。
- 趋势：可信计算。
- Eg：2009年10月，Joanna putkowska实现针对TrueCrypt的邪恶女佣攻击。

4、重视无线取证 拓宽工作领域

- 无线网络的覆盖范围越来越广，应用场合也越来越频繁。
- 智能终端的云服务，通往云存储的天梯。
- 题外话：量子计算

白虹软件 市场部
陆琦 13817065810