

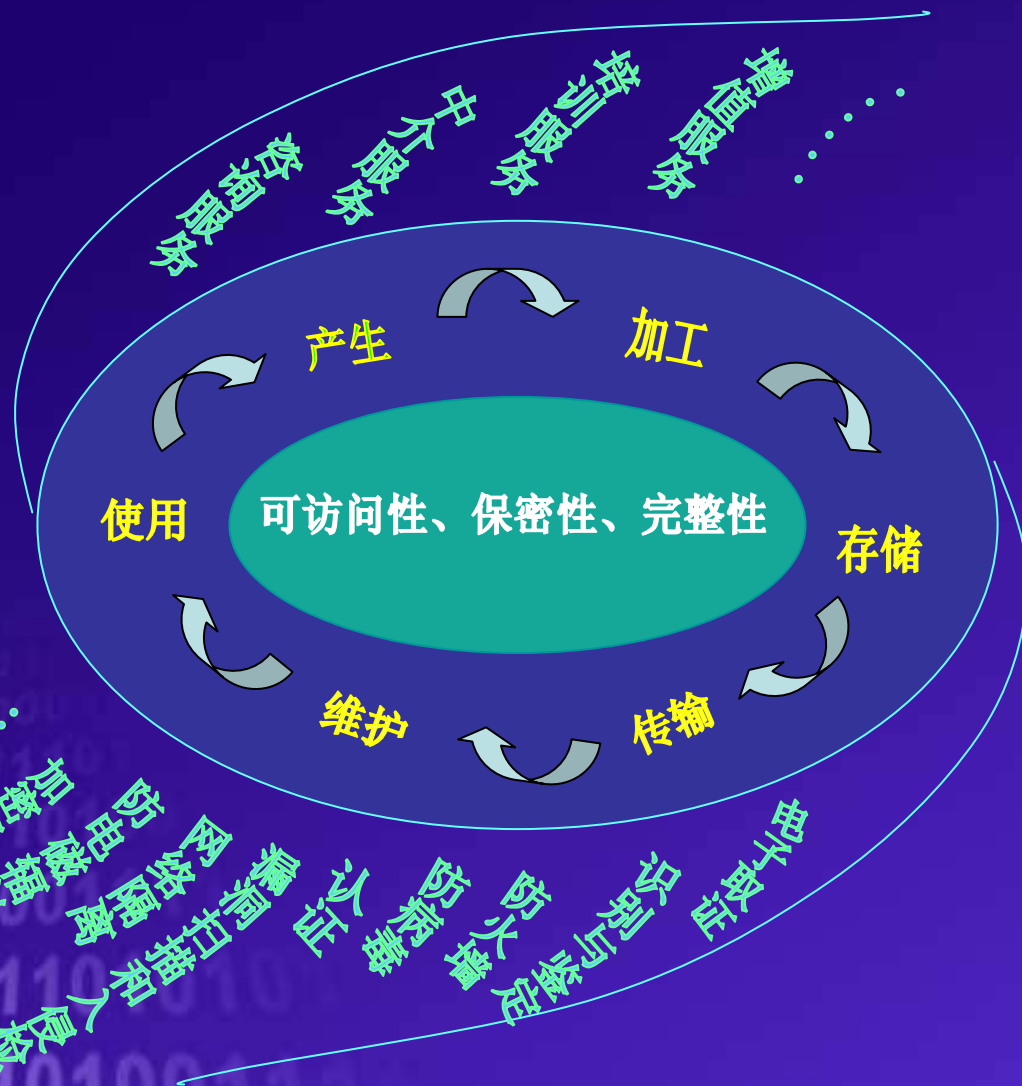
电子取证技术与法律的客观一致性

张喜平
2006.6

提纲

- 数据安全与电子取证
- 电子取证技术
- 电子取证技术与法律客观一致性
- 存在问题与发展趋势

数据安全



数据安全

- 数据安全涉及到数据的保密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability)、可控性 (Controllability)。综合起来说，就是要保障电子数据的有效性。
- **保密性**就是对抗对手的被动攻击，保证数据不泄漏给未经授权的人。**完整性**就是对抗对手主动攻击，防止数据被未经授权的篡改。**可用性**就是保证数据及数据系统确实为授权使用者所用。**可控性**就是对数据及数据系统实施安全监控。

电子证据

- 我国刑事诉讼法第42条规定，刑事诉讼中的七种是：物证、书证，证人证言，被害人陈述，犯罪嫌疑人、被告人供述和辩解，鉴定结论，勘验、检查笔录，视听资料
- 视听资料，是指以录音带、录像带、光盘、电脑和其他科学技术设备储存的音像或者电子信息证明案件事实的证据。
- 以二进制数字信号组成信息作为证明事实的证据(建议为一种独立的证据)

电子证据

- 分为静态数据、动态数据两种。
- 静态数据：硬盘和软盘、光盘、闪盘等存储设备的数据
- 动态数据：当前活动进程、网络连接状态、打开的文件、屏幕截图、物理内存和交换文件拷贝等关闭电源后就会消失的数据

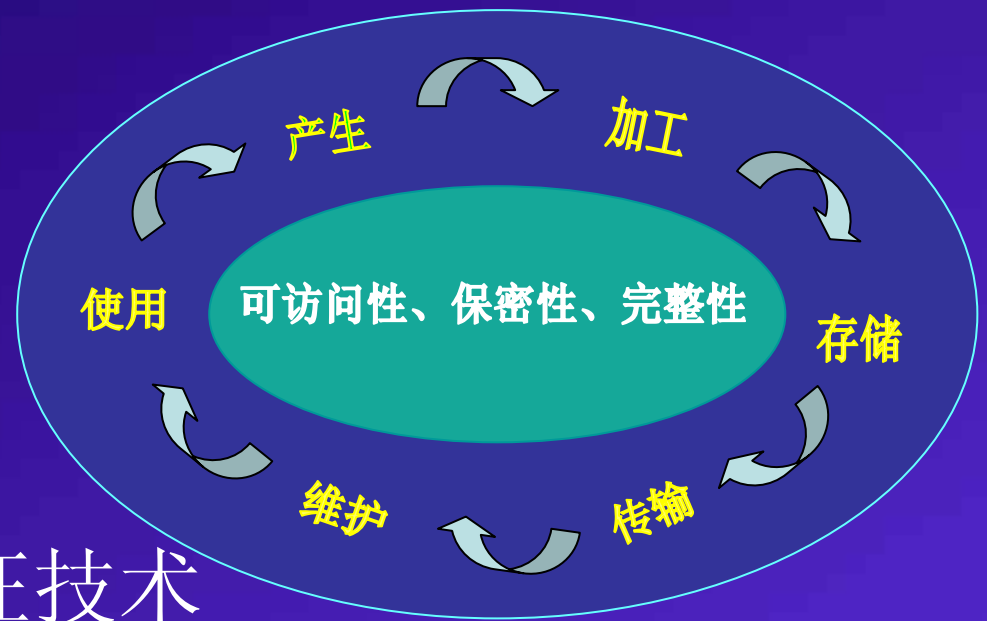
电子取证

- 就是利用电子技术、依法对电子证据进行保全、获取、分析、鉴定和提交的过程
- 是法学、刑事侦查学和计算机科学的交叉学科



电子取证技术

保全——获取——分析——鉴定——提交



- 基于单机的取证技术
- 基于网络的取证技术

电子取证技术——基于单机的取证技术

- 磁盘映像拷贝技术
- 数据恢复技术
- 加密解密技术
- 信息搜索与过滤技术
- 反向工程技术

电子取证技术——基于网络的取证技术

- 漏洞扫描与入侵检测技术
- 身份认证与审计技术
- 数据存储和备份技术
- 数据获取与还原技术
- 人工智能与数据挖掘技术
- 入侵追踪技术

电子取证技术与法律的客观一致性

- 问题

- 如何保证获取的电子数据及时准确？
- 如何保证获取的电子数据真实可靠？
- 如何保证获取的电子数据充分详实？
- 如何保证获取的电子数据不被篡改？
- 如何保证获取的电子数据不被添加？
- 如何保证获取的电子数据不被删除？
- 如何保证获取电子数据的行为合法？

电子取证技术与法律的客观一致性

- 怎样的电子证据可以被采用（可采性）
- 被采用的电子证据是否可以证明案件事实（证明力）



电子取证技术与法律的客观一致性

证据可采用的三个标准：客观性标准、关联性标准、合法性标准

- 客观性标准：客观存在的事物、客观存在的形式
- 关联性标准：与案件事实有联系
- 合法性标准：是指主体、形式和程序的合法

电子取证技术与法律的客观一致性

证明力的三个标准：真实性标准、充分性标准、完整性标准

- 真实性标准：明确电子证据真实可靠
- 充分性标准：电子证据足以证明待证事实
- 完整性标准：保证电子证据内容未经删改

电子取证技术与法律的客观一致性

- 如何通过电子取证技术实现电子证据可采性，保证电子证据的证明力
- 电子取证技术贯穿电子证据保全、获取、分析、鉴定和提交的始终
- 形成规范与标准

电子取证技术与法律的客观一致性

例：电子证据保全

- 不应改变原始磁盘
- 若原始磁盘没有错误，应创建原始磁盘的字节流副本或映像文件
- 若原始磁盘发生I/O 错误，应将遇到错误部分的内容替换为指定的数值
- 应以访问和阅读的形式记录I/O错误，包括错误的类型和位置
- 应通过一种或多种明确定义的接口访问硬盘

电子取证技术与法律的客观一致性

- 将数据复制到大于源盘的硬盘上，应标明目标盘中并非源盘拷贝的部分
- 若将数据复制到小于源盘的硬盘上，则应告知，截断副本，并记录相关的动作
- 不改变可疑计算机硬盘上的数据
- 不使用可疑计算机上的软件
- 尽量避免受可疑计算机上有害程序的影响
- 保存证据到可疑计算机以外的介质上

电子取证技术与法律的客观一致性

例：获取电子证据行为的合法性

- 证据的**主体**必须符合有关法律的规定（如：证人能力、取证资格、鉴定资格）
- 证据的**形式**必须符合有关法律的规定（如：刑事诉讼中鉴定结论和勘验检查笔录上必须由鉴定人员或勘验检查人员签名盖章）
- 证据的**提取方法和收集程序**必须符合法律的有关规定

电子取证技术与法律的客观一致性

例：获取电子证据的不合法行为

- 非法窃听和窃录
- 非法搜查和扣押等方式获得电子证据
- 非法软件收集的证据
- 非核证软件所获取的电子证据
- 具有其它重大违法情形的

存在问题与发展趋势——技术

电子反取证技术

- 数据加密技术
- 数据隐藏技术
- 数据擦除技术

存在问题与发展趋势——技术

- 向专业化、自动化发展，从而保证取证及时迅速，增强电子证据的可靠性
- 向规范化、标准化发展，从而保证取证详实充分，确保电子证据的完整性

存在问题与发展趋势——人才

- 需要一批专业的取证队伍
- 需要一批专业的鉴定专家



存在问题与发展趋势

- 电子取证技术反取证技术的对立统一
- 电子取证技术与法律客观性的对立统一



谢谢

10001100101011
10101010111101
01010111110101
101000001110101
100101010000101
1010101001011000
0101010000111101
1011110010001010
0001111100100111
1010001111110101
10111110010100111