



# 取证这些年： 浅谈电子证据问题

戴士剑

中国政法大学 教授

## 目录

1. 电子数据是什么？
2. 电子取证是什么？
3. 电子数据何去何从？



## 第五章 证 据

### 第五十条

可以用于证明案件事实的材料，都是证据。

证据包括：

- (一) 物证；
- (二) 书证；
- (三) 证人证言；
- (四) 被害人陈述；
- (五) 犯罪嫌疑人、被告人供述和辩解；
- (六) 鉴定意见；
- (七) 勘验、检查、辨认、侦查实验等笔录；
- (八) 视听资料、**电子数据**。

证据必须经过查证属实，才能作为定案的根据。

### 第五十四条

人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。

行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、**电子数据等证据材料**，在刑事诉讼中可以作为证据使用。

对涉及国家秘密、商业秘密、个人隐私的证据，应当保密。凡是伪造证据、隐匿证据或者毁灭证据的，无论属于何方，必须受法律追究。

# 1. 电子数据是什么？

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

----对象

----工具

----线索（隐私、兴趣爱好等，马家爵杀人案）

----沟通工具（心理战、定位、与罪犯的交流渠道，清华北大爆炸案2003年）

----沉默的现场知情人（2012年）

### 第四十三条

辩护律师经证人或者其他有关单位和个人同意，可以向他们收集与本案有关的材料，也可以申请人民检察院、人民法院收集、调取证据，或者申请人民法院通知证人出庭作证。辩护律师经人民检察院或者人民法院许可，并且经被害人或者其近亲属、被害人提供的证人同意，可以向他们收集与本案有关的材料。

### 第一百五十八条

下列案件在本法第一百五十六条规定的期限届满不能侦查终结的，经省、自治区、直辖市人民检察院批准或者决定，可以延长二个月：（一）交通十分不便的边远地区的重大复杂案件；（二）重大的犯罪集团案件；（三）流窜作案的重大复杂案件；（四）犯罪涉及面广，取证困难的重大复杂案件。

### 第五十四条

人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、电子数据等证据材料，在刑事诉讼中可以作为证据使用。对涉及国家秘密、商业秘密、个人隐私的证据，应当保密。凡是伪造证据、隐匿证据或者毁灭证据的，无论属于何方，必须受法律追究。

### 第一百六十条

在侦查期间，发现犯罪嫌疑人另有重要罪行的，自发现之日起依照本法第一百五十六条的规定重新计算侦查羁押期限。犯罪嫌疑人不讲真实姓名、住址，身份不明的，应当对其身份进行调查，侦查羁押期限自查清其身份之日起计算，但是不得停止对其犯罪行为的侦查取证。对于犯罪事实清楚，证据确实、充分，确实无法查明其身份的，也可以按其自报的姓名起诉、审判。

◆关于办理刑事案件收集提取和审查判断电子数据若干问题的规定

◆两个证据规定

◆公安机关办理刑事案件电子数据取证规则

◆全国人民代表大会常务委员会关于司法鉴定管理问题的决定



**为了加强对鉴定人和鉴定机构的管理，适应司法机关和公民、组织进行诉讼的需要，保障诉讼活动的顺利进行，特作如下决定：**

一、司法鉴定是指在诉讼活动中鉴定人运用科学技术或者专门知识对诉讼涉及的专门性问题进行鉴别和判断并提供鉴定意见的活动。

十七、本决定下列用语的含义是：

- （一）法医类鉴定，包括法医病理鉴定、法医临床鉴定、法医精神病鉴定、法医物证鉴定和法医毒物鉴定。
- （二）物证类鉴定，包括文书鉴定、痕迹鉴定和微量鉴定。
- （三）声像资料鉴定，包括对录音带、录像带、磁盘、光盘、图片等载体上记录的声音、图像信息的真实性、完整性及其所反映的情况过程进行的鉴定和对记录的声音、图像中的语言、人体、物体作出种类或者同一认定。

十八、本决定自2005年10月1日起施行。

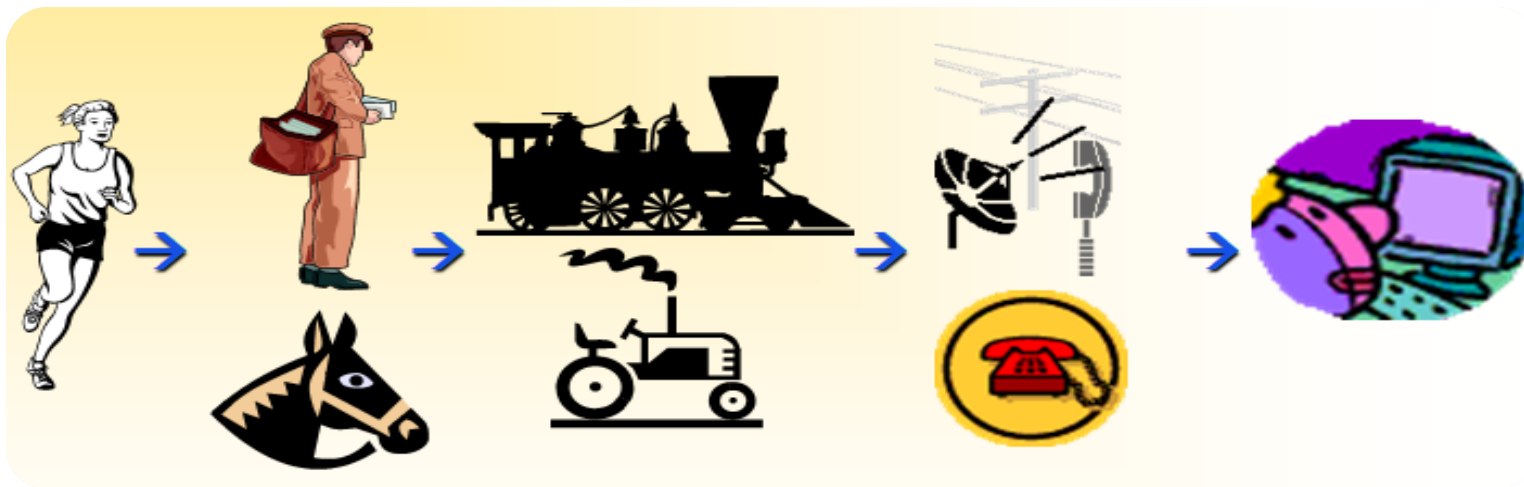
# 人类历史上已经经历了6次信息革命：

- 第一次信息革命是语言的产生。这次信息革命解决了信息分享问题。
- 第二次信息革命是文字的出现，解决了信息记录问题。
- 第三次信息革命是纸和印刷术的出现，解决了信息远距离传输的问题。
- 第四次信息革命是无线电的发明，解决了信息的远距离实时传输问题。
- 第五次信息革命是电视的出现，解决了远距离多媒体传输的问题。
- 第六次信息革命是互联网的出现，完成了信息双向和多向交互的传输。



### 3. 电子数据何去何从?

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE



神证时代

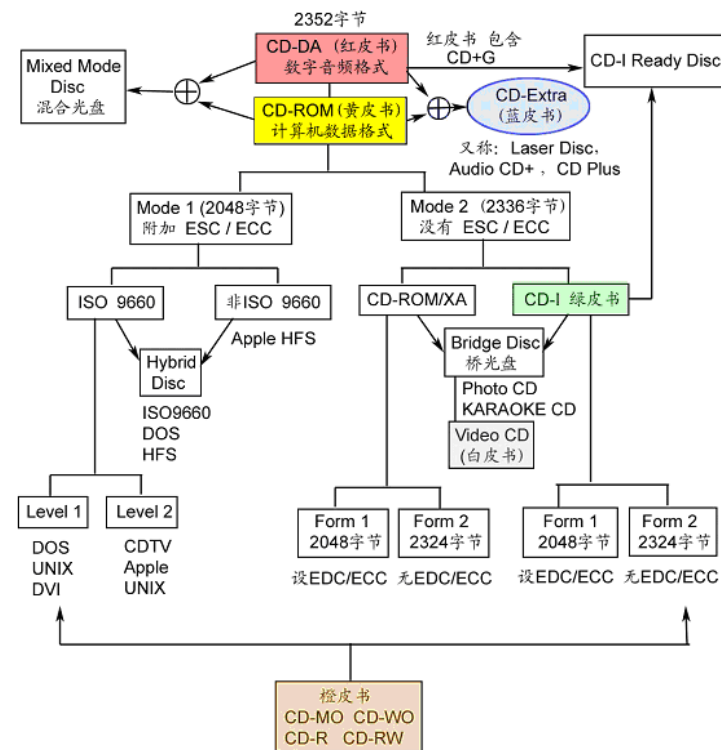
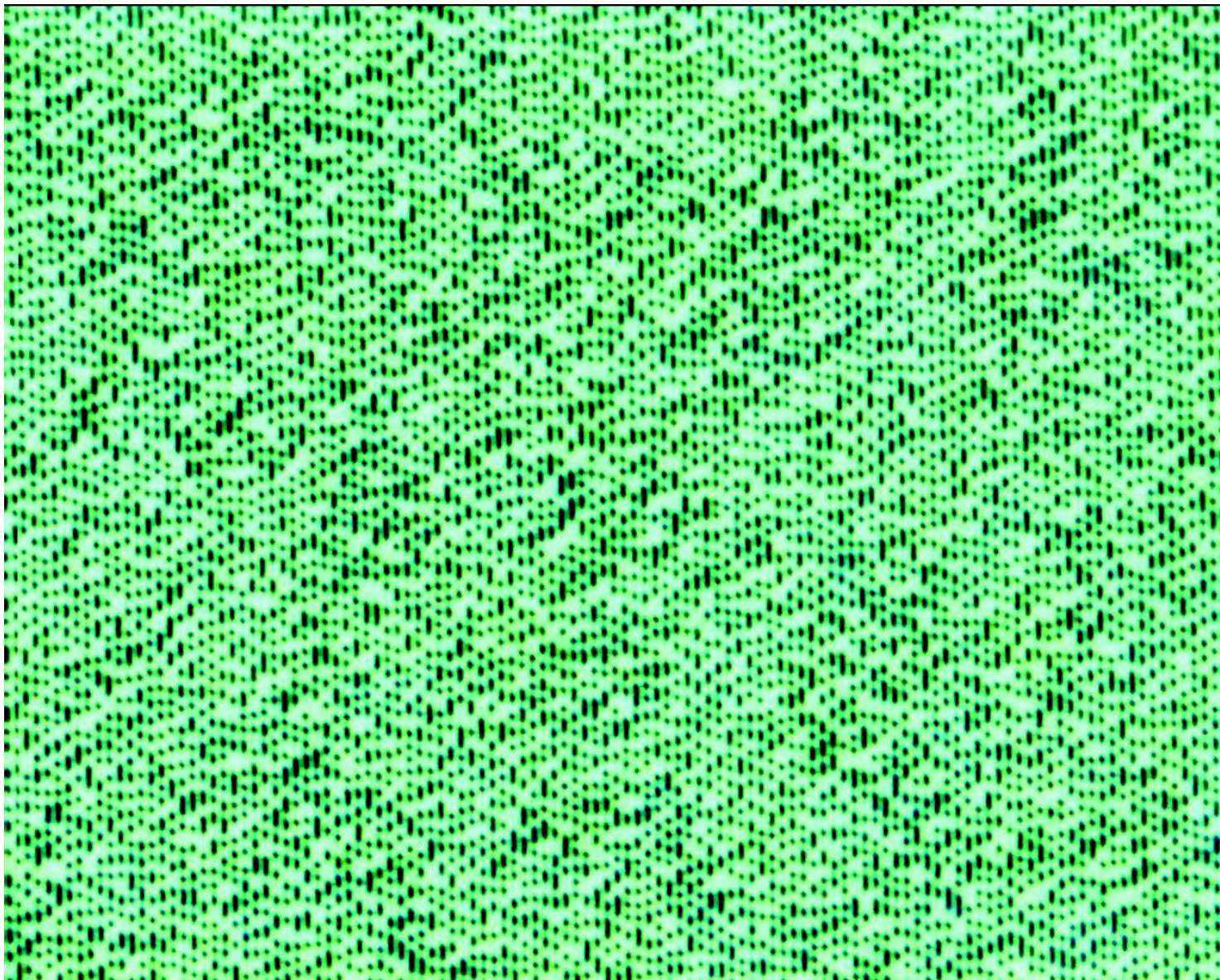
人证时代

物证时代

电子证据时代?

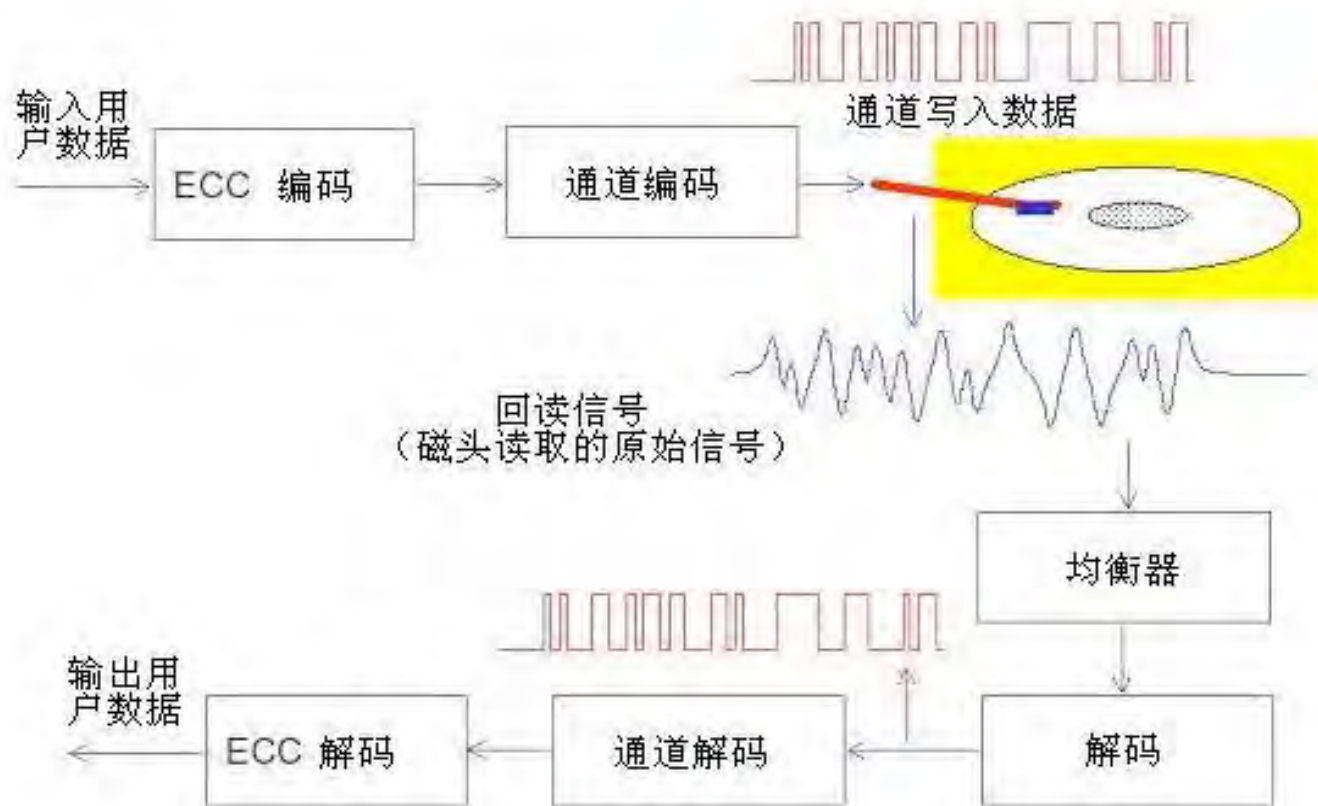


### 3. 电子数据何去何从?





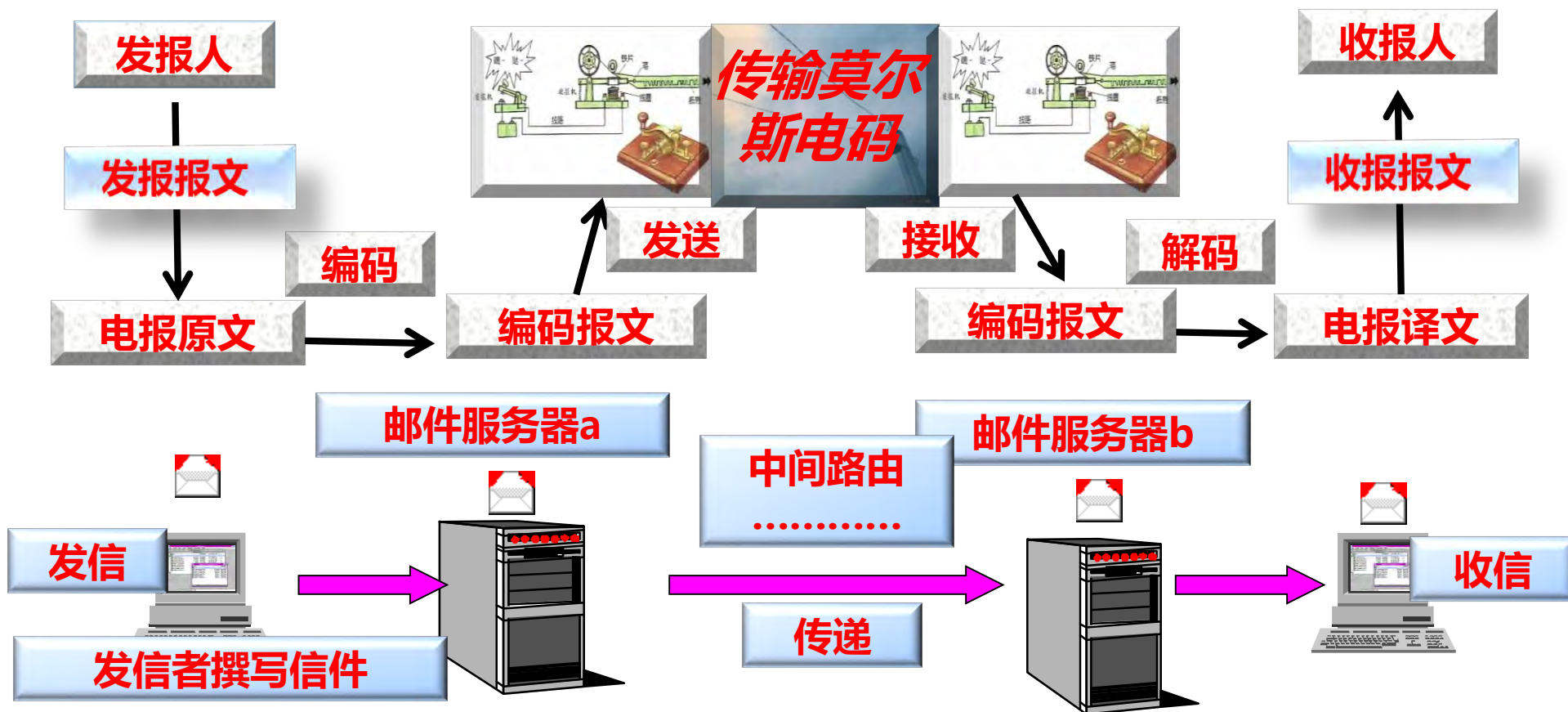
### 3. 电子数据何去何从？





# 3. 电子数据何去何从?

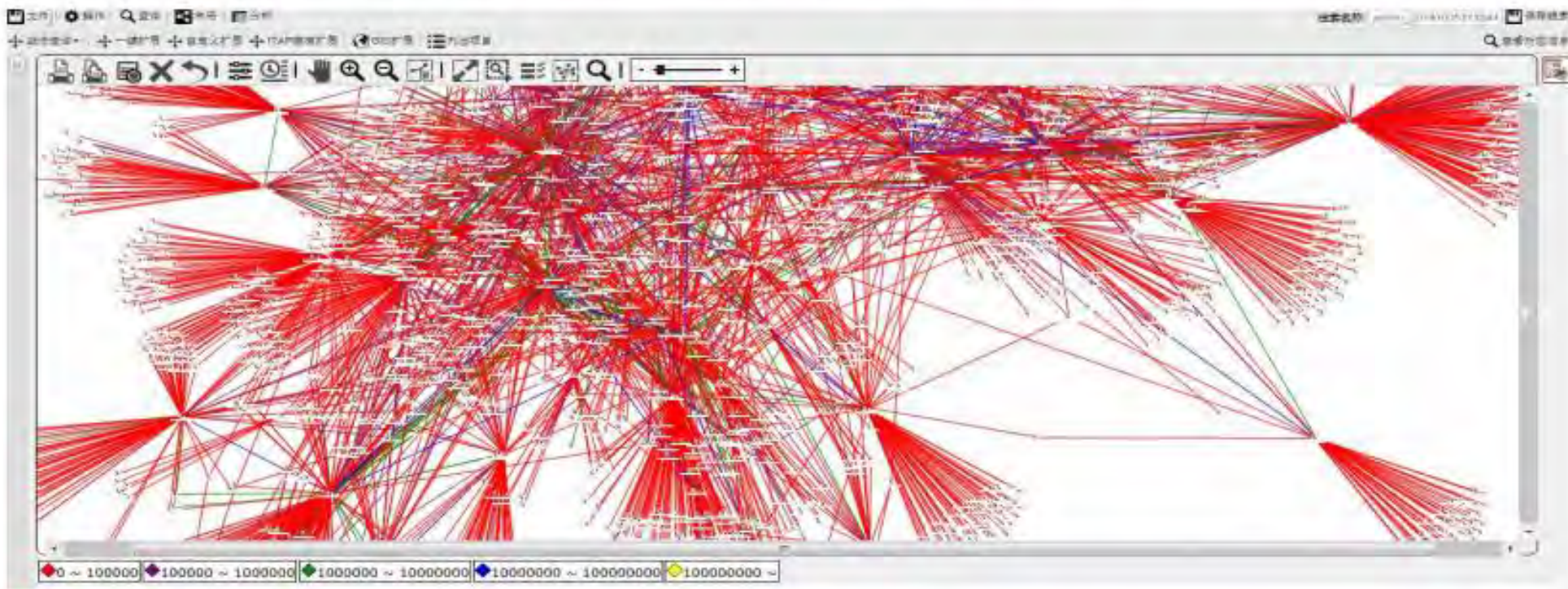
2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE





## 银行账户交易分析

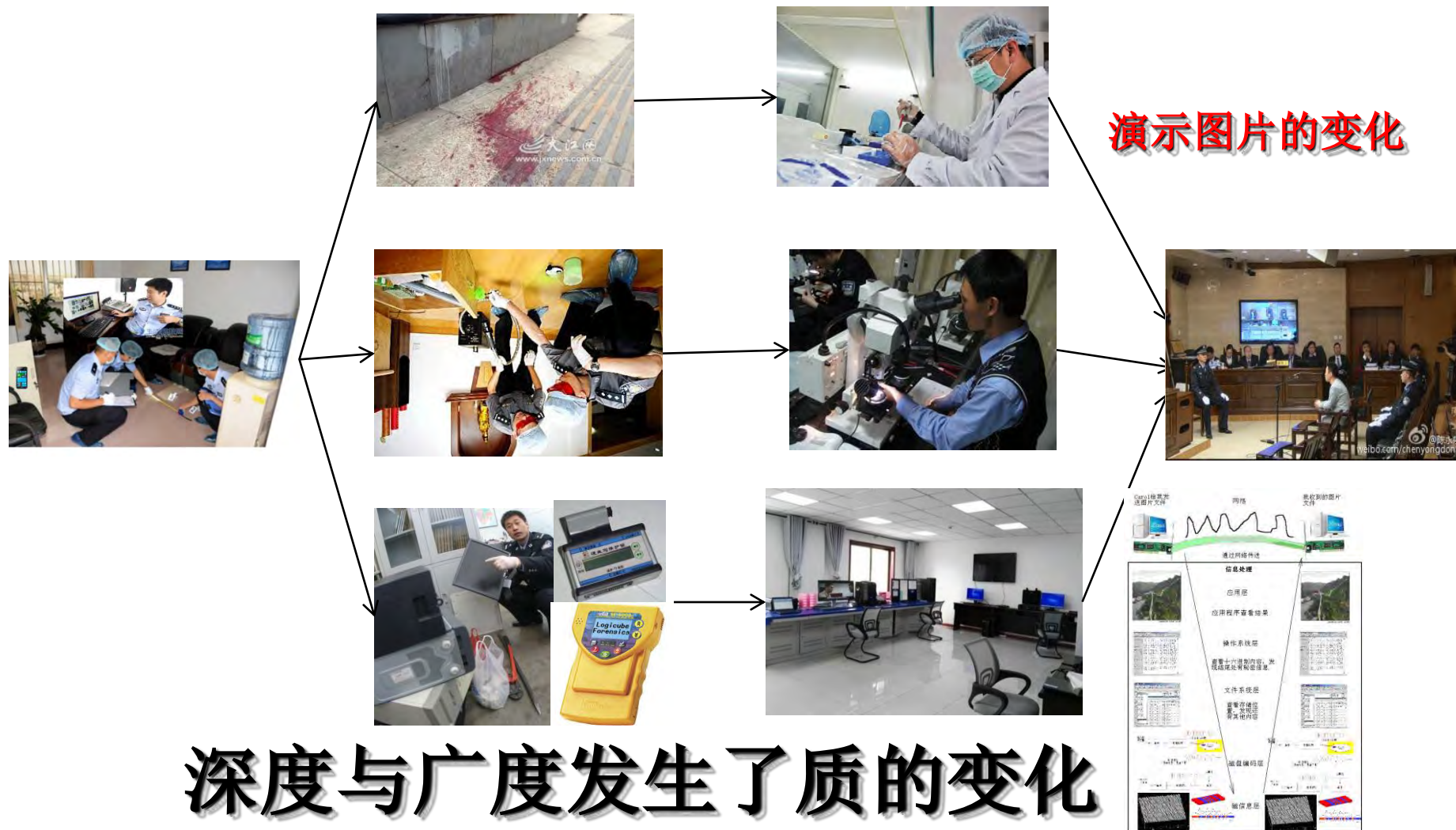
根据银行资金流水记录，图形化分析资金流水的走账，了解大额资金走向，快速锁定目标账号，并找出资金流向和交易结构，辅助领导进行正确决策分析。





# 3. 电子数据何去何从?

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE





# 3. 电子数据何去何从?

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

电子数据取证技能树

## CF 计算机取证

### 基础系列

#### CF101-电子数据取证入门与应用

- 取证基础知识
    - 电子数据取证发展史
      - 国内外电子取证发展
      - 行业应用
      - 法律法规
    - 电子数据取证流程与标准
      - 国内GA标准
      - ISO27000系列标准
      - 司法鉴定标准
    - 现场取证基本原则
      - 现场勘验规则
      - 电子证据收集与保全
  - 磁盘结构及文件系统
    - 取证相关概念
      - 磁盘结构(分区、扇区、簇)
      - 磁盘分区结构(MBR/EBR/VBR)
      - 文件结构(簇、未分配簇)
    - 文件系统工作原理
      - FAT文件系统
      - NTFS文件系统
      - exFAT文件系统
      - ext2/3/4文件系统
  - 电子数据证据固定与保全
    - 国际常用的证据文件格式及应用
      - 原始数据镜像(Raw/idd)
      - E01/Ex01证据文件
    - AFF证据文件
    - Smart证据文件
    - 取证引导系统盘
      - 常见取证引导系统盘
        - Paladdin
        - DEFT
        - KALI
        - WinFE
      - 取证引导系统盘制作
        - WinFE取证引导盘制作
        - Linux取证引导盘制作
    - 磁盘镜像制作
      - 写保护设备使用
      - 硬盘复制设备使用
      - 哈希计算原理与校验应用
- 时间格式与解析
  - 操作系统的时区设置
  - 常见文件的时间属性(MACE)的特性及数据解码
  - 文件附加属性(元数据)时间信息
- 文件分析
  - 签名分析原理及应用
  - 哈希计算原理与应用
  - 信息熵计算原理与应用
- 关键字搜索
  - 文字编码及应用
  - 常见关键词编码搜索
  - 十六进制搜索
  - 模糊搜索高级语法
  - 正则表达式
  - 特殊文件内容搜索(DOCX/XLSX/PPTX/PDF)
  - 索引技术及应用
- 常见应用取证分析
  - 浏览器取证基础
  - 电子邮件取证基础
  - 即时通讯取证基础

### 进阶系列

#### CF201-Windows取证

- 注册表取证
  - 注册表基础及应用
    - 系统注册表
    - 用户注册表
  - 删除注册表数据恢复与分析
  - 注册表分析工具应用
- 浏览器取证
  - 常见浏览器数据恢复与分析
  - URL地址编码与解码
  - 搜索引擎关键词提取与解码
- 电子邮件取证
  - 电子邮件客户端取证
    - Outlook
    - Foxmail
    - Windows Mail
    - ThunderBird
  - Webmail取证分析
- 系统痕迹分析
  - 最近访问文件(MRU)
  - 快捷方式分析(LNK)
  - ShellBags痕迹分析
  - 跳转痕迹分析(JumpList)
  - 卷影复制数据(VSC)
  - 回收站分析
  - 打印服务器文件
- 即时通讯取证
  - QQ、Skype通讯数据取证
  - Web即时通讯信息取证
- 应用程序痕迹取证
  - Prefetch
  - AmCache
  - UserAssist
- Windows事件日志分析
  - USB设备使用记录
  - 系统时间修改日志
  - 无线网络访问日志
  - 远程终端服务访问记录
  - 用户登录注销日志

#### CF202-Linux取证

- Linux系统发展史及应用简介
- Linux文件系统及磁盘(LVM/LVM2)
- Linux系统单用户模式及密码绕过
- Linux日志分析
  - Apache日志
  - FTP日志
  - 数据库日志
  - 邮件服务器日志
- Linux应用程序分析
- Linux入侵取证分析

### 高级系列

#### CF301-Windows高级取证

- 电子邮件取证
  - 电子邮件通讯原理
  - Mac OS操作系统版本
  - 电子邮件头分析
  - 电子邮件编码原理
    - Base64编码
    - Quoted-Printable编码
    - T2加密芯片
  - 残缺电子邮件、碎片正文及附件的恢复
- 数字时间取证
  - NTFS文件系统时间属性解码
  - 数据库时间解码
  - 应用程序存储数据时间解码
- 文件系统取证
  - 文件系统日志分析
    - SUSN.JRNL日志
    - SL logfile日志
  - PowerShell取证应用
    - PowerShell常用命令
    - 常用取证分析命令
    - 脚本编写

#### CF302-内存取证

- 物理内存工作机制及数据的价值
- 计算机物理内存结构
- 内存镜像提取工具及文件格式转化
  - DumpIt
  - Belkasoft RAMCapture
  - Magnet RAMCapturer
  - FTK Imager
  - Encase Imager
  - WinEn
  - LIME
- 物理内存镜像分析
  - 内存镜像中的数据提取与提取
    - 内存分析工具应用
      - Volatility工具
      - Rekall工具
      - 取证神探
    - 取证大师

#### CF303-服务器取证

- 服务器常用硬件
  - 软硬件RAID
  - 网络存储、光纤存储
- 服务器常用的操作系统及文件系统
  - Windows Server
  - Linux
  - Mac Server
- 服务器常见的应用系统
  - Web服务取证
    - Web服务器应用简介
    - Web服务器日志分析
  - 数据库取证
    - 数据库基本简介
      - MySQL
      - Microsoft SQL Server
      - Oracle
    - SQL语言基础与应用
    - 常用SQL语句
    - 数据库备份与导入导出
    - 数据库日志分析
    - 不同OS环境的数据库迁移与重建
- 电子邮件服务取证
  - 系统服务简介及应用
    - Microsoft Exchange
    - Lotus Domino
    - Sendmail
    - Magic Winmail
  - 电子邮件服务日志分析
    - POP3日志分析
    - SMTP日志分析
    - IMAP日志分析
    - HTTP访问日志分析
- 虚拟架构服务应用
  - Vmware ESXi
  - Microsoft HyperV
  - Linux KVM
- 网络云存储及应用取证
  - 常见云存储应用简介
  - 云存储数据源采集(远程勘验)
  - 计算机终端/手机终端云端数据采集

## MF 手机取证

### 基础系列

#### MF101-手机取证入门与应用

- 手机取证基础
  - 手机通讯原理
  - 基本概念(IMEI/IMSI/ICCID)
- 手机存储介质及工作机制
  - NOR Flash
  - NAND Flash
  - UFS
  - eMMC
  - 存储卡
  - SIM卡
  - SIM卡数据结构
  - SIM卡数据提取方法
- 非智能机数据提取方法
  - iOS取证分析
    - iOS系统简介及其安全机制
    - iOS数据提取与分析
      - 物理镜像
      - 逻辑提取
      - iTunes备份解析
      - LockDown信任密钥
      - iCloud云端数据获取
  - Android取证分析
    - Android系统简介及其安全机制
    - Android数据提取与分析
      - 物理镜像
      - 逻辑提取
      - Android备份
- 基于手机终端身份认证进行云端数据采集

### 高级系列

#### MF301-手机高级取证分析

- iOS系统常见数据的存储位置及手工解析
  - 设备信息提取与分析
  - 常见基础数据手工分析
  - 微信数据库加密机制与分析
  - QQ数据库分析
- Android系统常见数据的存储位置及手工解析
  - 设备信息提取与分析
  - 常见基础数据手工分析
  - 微信数据库加密机制与分析
  - QQ数据库分析
- 手机芯片数据获取
  - Chip-Off
  - JTAG
  - 阅读
- Android手机分析
  - Android系统Root
  - ADB命令行基础与应用
  - Android手机物理镜像获取
- iOS手机分析
  - iOS越狱
  - iTunes备份与加密
  - iCloud两步验证机制

## DR 数据恢复

- 逻辑删除数据恢复
  - 基于文件系统元数据信息的数据恢复
  - 删除文件恢复
    - 分区格式化恢复
    - 基于文件签名数据恢复技术
    - 连续存储文件恢复
    - 不连续存储文件恢复
  - 基于特征的分区分区搜索与恢复技术
  - 基于文件/数据结构的特征的数据恢复技术
    - JPEG图片恢复
    - NOR Flash
    - NAND Flash
    - UFS
    - eMMC
    - 存储卡
    - SIM卡
    - SIM卡数据结构
    - SIM卡数据提取方法
- RAID阵列重建技术
  - 硬件RAID阵列重建
    - RAID5
    - RAID6
  - 软件RAID阵列重建
    - Windows系统内置RAID阵列
    - Linux系统内置mdadm阵列
- 数据库删除数据恢复
  - Microsoft SQL Server
  - MySQL
  - Oracle
- 故障硬盘修复
  - 磁盘固件修复
    - PC-3000
    - ATOLA
  - 数据文件修复
    - JPEG图片重建
    - Office文档文件修复
    - 不完整数据恢复

## PR 信息加解密

- 信息加解密基本原理
  - 密码学基础
  - 信息加密/解密发展史
- 加密技术应用
  - 硬盘加密
    - ATA硬盘加密
      - 基于软件的磁盘加密
        - BitLocker
        - LUKS
        - FileVault
        - TrueCrypt/VeraCrypt
        - Symantec PGP/Endpoint Encryption
      - 基于硬件芯片的磁盘加密
        - TPM加密芯片
        - 苹果T2加密芯片
        - 移动硬盘专用加密芯片
    - 文件加密
      - 文件打开加密保护
      - 文件内容修改加密保护
      - 基于哈希算法的数据保护
      - 数据库加密技术
      - 信息隐藏技术
  - 密码恢复技术
    - 基于CPU计算资源
      - 单机
      - 分布式密码恢复
    - 基于GPU计算资源
      - CUDA
      - OpenCL
    - 基于FPGA计算资源
    - 基于ASIC计算资源
    - 基于彩虹表(Rainbow Table)
    - 基于加密应用漏洞或脆弱性
- 密码破解技巧
  - 密码使用规律研究
  - 密码字典应用与制作

## NF 网络取证

- TCP/IP网络协议基础
- OSI七层模型
- 网络设备类型及应用
  - 网络设备类型
    - 网络交换机
    - 路由器
  - 网络设备数据获取
    - Cisco路由配置信息 & 数据提取
    - 华为路由配置信息 & 数据提取
    - 交换机及路由器设备数据提取
- 无线通讯协议及应用
  - 通讯协议
    - Wi-Fi
    - 蓝牙
    - ZigBee
  - 无线路由设备取证
- 有线及无线网络数据抓包
- 网络数据包分析
  - 传输内容重组
  - 数据包分析工具应用
  - Wireshark

## 应急响应取证


- 计算机终端应急响应
  - 现场勘验
    - 电子数据证据保全
      - 全盘镜像或分区镜像
      - 不关机取证
    - 损失性数据提取与保全
      - 计算机物理内存提取
      - 屏幕镜像
      - 网络通讯数据保全
      - 网络实时抓包
    - 应急响应
      - 断网/保持联网
      - 阻止数据破坏
      - 追踪攻击者
    - 后处理取证分析
      - 删除数据恢复
      - 日志分析
      - 系统行为溯源分析
- 服务器终端应急响应
  - 现场勘验
    - 电子数据证据保全
      - 全盘镜像或分区镜像
      - 不关机取证
    - 损失性数据提取与保全
      - 计算机物理内存提取
      - 屏幕镜像
      - 网络通讯数据保全
      - 网络实时抓包
    - 应急响应
      - 断网/保持联网
      - 阻止数据破坏
      - 追踪攻击者
    - 后处理取证分析
      - 删除数据恢复
      - 日志分析
      - 系统行为溯源分析

□ 鉴定与案情的界限在哪里？

□ 技术侦查与侦查技术的界限在哪里？

□ 伪造、篡改是人的意图，不是机器的意图



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE