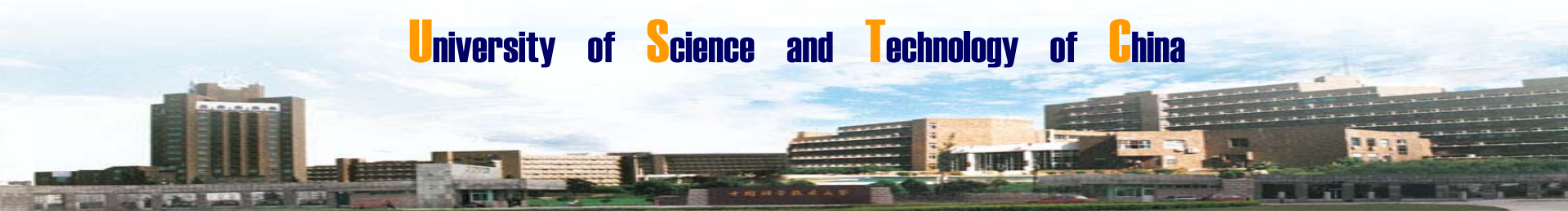
信息安全法律基础

主讲人： 庄连生

Email: *{lszhuang@ustc.edu.cn}*

Fall, 2009



专　题

数字取证

内容提要：

① 数字取证概述

② 数字取证技术

③ 数字取证方法

④ 数字取证工具

⑤ 数字取证规范

数字取证概述

- 电子证据是指以存储的电子化信息资料来证明案件真实情况的电子物品或者电子记录；
- 数字取证是指为了揭示与数字产品相关的犯罪或过失行为，以及由其他原因导致的使系统发生故障的现象，利用一切科学且合法的方法和工具，对以0/1二进制表示的数据电文进行识别、保存、收集、检查、分析和呈堂等活动过程。
- 数字取证分类：
  - ① 根据难易程度分类：一般取证、复杂取证；
  - ② 从取证时间角度出发：事后取证、事中取证；
  - ③ 从取证范围的角度出发：外部取证、内部取证；
  - ④ 从取证状态的角度出发：静态取证、动态取证；

数字取证概述

- 数字取证的特点：

① 技术性收集：主要是指在技术上对电子证据进行收集的手段、相应的技术要求和指标；主要涉及计算机科学的一些问题，要解决的是电子证据的固定、保全以及修复等一系列问题；目的是将电子证据以法定的证据形态或者法庭可以采纳的证据形式固定下来。

② 法律性收集：主要是指电子证据收集的法律程序上的要求，主要包括收集主体的要求、收集具体程序的要求以及其收集中和相关权利的冲突和协调。

数字取证概述

- 数字取证研究内容：

① 数字取证技术：指在计算机或其他数字设备取证的整个过程中，在相关理论的指导下，使用合法的、合理的、规范的技术或手段，以保证计算机或其他数字设备取证的正确进行，以及合理信服的结论的产生。

② 数字取证程序：指取证所遵循的原则、过程和步骤。

③ 数字取证法律：主要涉及对电子证据及取证过程的法律研究。

④ 数字取证工具：指计算机犯罪调查过程中使用的软件和硬件的集成，以满足复杂多变的现场勘查取证需要，实现符合法律程序要求的计算机犯罪调查过程，提供简单易用的数字取证与证据分析工具。

⑤ 数字取证规范：数字取证工作标准与规范、数字取证工具标准和规范。

数字取证概述

- 数字取证的发展趋势

① 取证领域不断扩大

② 取证工具向自动化和专业化方向发展

③ 取证技术融合越来越多的新技术和新理论

④ 取证工具向标准化方向发展

⑤ 取证方法向动态取证的方向发展

⑥ 取证法规需要进一步完善

⑦ 取证研究团体将由得到认可的科学团体来承担

⑧ 取证程序有待标准化和深入研究

⑨ 取证管辖地域的限制

数字取证技术

- 数字取证技术的研究范围：

① 证据识别：指对要进行调查的计算机上的数据以及与之相关的设备上的数据的判断、识别过程，在海量的数据中识别出哪些数据与要调查的案件相关。

② 证据保存：采用有效保存措施保护电子证据的完整性和真实性。

③ 证据收集：指取证人员在计算机犯罪现场提取或捕获与要调查案件相关的数据信息。

④ 证据检查：指对收集来的数据进行仔细检查，该类技术与证据发现和提取相关，但不涉及从证据中得出结论。

⑤ 证据分析：对收集的数据进行检查和分析，找出之间关系，或证明它们就是某攻击或犯罪的证据，以对法庭进行出示，对案件起到佐证的作用

⑥ 证据呈堂：对电子证据的分析解雇和评估报告进行归档处理，形成能够提供给法庭的电子证据。

数字取证技术

- 当代流行的取证技术：包括数据复原技术、数据监控技术、数据加解密技术、日志分析技术、对比搜索技术、数据挖掘技术、数据复制技术、数据呈堂技术、数据欺骗技术、扫描技术、数据截取技术、数据隐藏技术、数字签名和数字时间戳技术、攻击源追踪技术、数字摘要技术。

- 取证技术发展趋势：

① 应用领域更广泛

② 与安全理论紧密结合

③ 与其他技术的融合

数字取证方法

- 数字取证程序是数字取证工作中的重要环节，是指取证所遵循的原则、过程和步骤。它应具有知道行，其制定应确保具有法律效力和普遍适合原则。
- 数字取证原则是取证工作的标准要求，指导取证工作各个环节应达到的某种程度，符合某些标准。

数字取证方法

- 国外取证方法分析

① 事件响应方法：由**Mandia**等人提出，包括事前准备、事中检测、初始响应、制定响应策略、备份、调查、保护被测系统、网络监听、复原、跟踪等过程。

② 现场调查过程模型：由美国司法部提出，该模型包括准备、收集、检查、分析、报告等过程。

③ 取证抽象过程模型：由美国空军学院提出，包括识别、准备、方法策略、保存、收集、检查、分析、陈述、返还证据等过程。

④ 集成的数字调查过程模型：包括就绪期、配置期、物理犯罪现场调查期、数字犯罪现场调查期、审查期等过程。

⑤ 端到端的数字调查过程模型：分析独立事件、初次关联、事件规范化、事件去冗余、二次关联、时间链分析、构建证据链.

数字取证方法

- 国内数字取证方法分析

  ① 起步很晚，不够深入、集中在取证步骤和方法等细节；

  ② 中科院高能物理研究所许榕生研究员定义了一个数字取证步骤；

  ③ 中科院软件研究所丁丽萍等人从侦查角度探讨数字取证的步骤。

- 数字取证原则：

  ① 取证合法原则

  ② 实事求是原则

  ③ 技术优先原则

  ④ 保密原则

  ⑤ 固定保全原则

数字取证方法

- 数字取证的方法步骤：
  - ① 准备阶段：制订计划、培训人员、设置监控、技术准备、发现识别现场
  - ② 取证阶段：现场勘查、查找证据、收集证据、证据固定保全、审查证据、分析证据、给出分析结果并整理诉讼依据
  - ③ 整理阶段：证据集中保存、法律文书归档、取证工具回收保存、移交移送
- 现场勘查：现场保护、现场访问、实地勘察、现场搜查、现场分析、现场勘查记录、侦查实验、现场取证、数据恢复、发现和收集犯罪证据、了解判断犯罪嫌疑人的个体特点等

数字取证工具

- 数字取证工具的分类：

① 根据开发目的：专业取证工具和通用工具；

② 根据取证流程：证据识别工具、证据保存工具、证据收集工具、证据检查工具、证据分析工具和证据呈堂工具。

- 通用型证据识别类工具：

① 密码破译工具：**John the Ripper，AZPR、AOXPPR等**

② 数据恢复工具：诺顿工具集、**EasyRecovery等**

③ 文件浏览工具：**Quick View Plus、DataViz套件等**

④ 网络监控工具：**NetMonitor、netstat、route 等**

数字取证工具

- 通用型证据保存类工具
  - ① 磁盘擦除工具：**DiskScrub**等
  - ② 磁盘映像工具：**Safe Back**， **Snap DataArrest, DIBS PERU**等
  - ③ 反复擦除工具：诺顿工具
  - ④ 加密工具：**Password 2000, BestCrypt**，硬件加密狗等
- 通用型证据收集类工具：
  - ① 磁盘映像工具
  - ② 数据截取工具：**Sniffer,TCPDump**等
  - ③ 数据欺骗工具：**DTK**蜜罐工具，**BOF**蜜罐
  - ④ 硬盘拷贝工具

数字取证工具

- 通用型证据检查类工具

  ① 图片检查工具：**ThumbsPlus**

  ② 文本搜索工具：**DtSearch**

  ③ 磁盘分区检测工具：**FDISK、PartitionMagic、UltraEdit32等**

- 通用型证据分析类工具

  ① 数据挖掘类工具：**Net Threat Analyzer， IPfilter，Ethereal等**

  ② 日志分析工具：**AWStates，Logcheck等。**

- 通用型证据呈堂类工具：

  比较著名的有**NTI公司的NTIDOC软件**

数字取证工具

- 专用取证工具：
  - ① 基本上来自国外厂家
  - ② 比较著名的有**EnCase, TCT（The Coronor's Toolkit），ForensiX等**
  - ③ 取证勘查工具箱：**Forensic Air – Lite V**

- 国内数字取证工具：
  - ① 厦门美亚柏科公司的网警勘察箱
  - ② 北京天宇晶远移动介质取证箱、电子证据取证平台
  - ③ 上海金诺网络安全股份 有限公司的计算机犯罪取证勘查箱
  - ④ 北京久之峰科技有限公司：**930型涉密硬盘数据强力粉粹机**

数字取证规范

- 数字取证标准相关组织：
  - ① 国际计算机证据组织（IOCE）
  - ② 数字证据科学工作组（ SWGDE）

- 数字取证规范
  - ① 数字取证主体规范
  - ② 数字取证过程规范
  - ③ 数字取证程序规范
  - ④ 证据鉴定过程工作规范
  - ⑤ 数字取证工具标准

谢谢！

Q & A