电子证据标准体系研究

演讲人：郭弘

职务：上海辰星电子数据司法鉴定中心 主管

日期：2014年9月25日

上海辰星电子数据司法鉴定中心

- 中国最权威的电子数据鉴定机构之一。
- 电子物证领域第一家通过实验室认可和国家级资质认定认定的专业机构。
- 公安系统唯一通过CNAS组织的PTP评审的机构。

互联网发展与犯罪问题

排序	违法犯罪类型
1	网络诈骗
2	网络色情
3	网络传销
4	网络贩卖公民个人信息
5	网络钓鱼
6	网络赌博
7	网络黑客攻击
8	网络贩卖假冒伪劣产品
9	网络贩毒
10	网络非法集资

鉴定标准

2007年司法部颁布的《司法鉴定程序通则》第22条规定，“司法鉴定人进行鉴定应当依下列顺序遵守和采用该专业领域的技术标准和技术规范。”

国家

•国家标准和技术规范；

行业

•司法鉴定主管部门、司法鉴定行业组织或者相关行业主管部门制定的行业标准和技术规范；

自制

•该专业领域多数专家认可的技术标准和技术规范。不具备前款规定的技术标准和技术规范的，可以采用所属司法鉴定机构自行制定的有关技术规范。

电子数据取证标准体系

国际相关标准制定机构


ISC
2014


AMERICAN SOCIETY OF CRIME LABORATORY DIRECTORS
LABORATORY ACCREDITATION BOARD
LAB

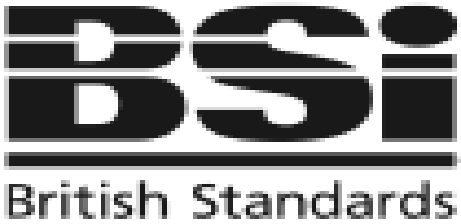

ISO
IEC


SCIENTIFIC WORKING GROUP FOR DIGITAL EVIDENCE
SWGDE


INTERNATIONAL
ORGANIZATION
ON COMPUTER
EVIDENCE

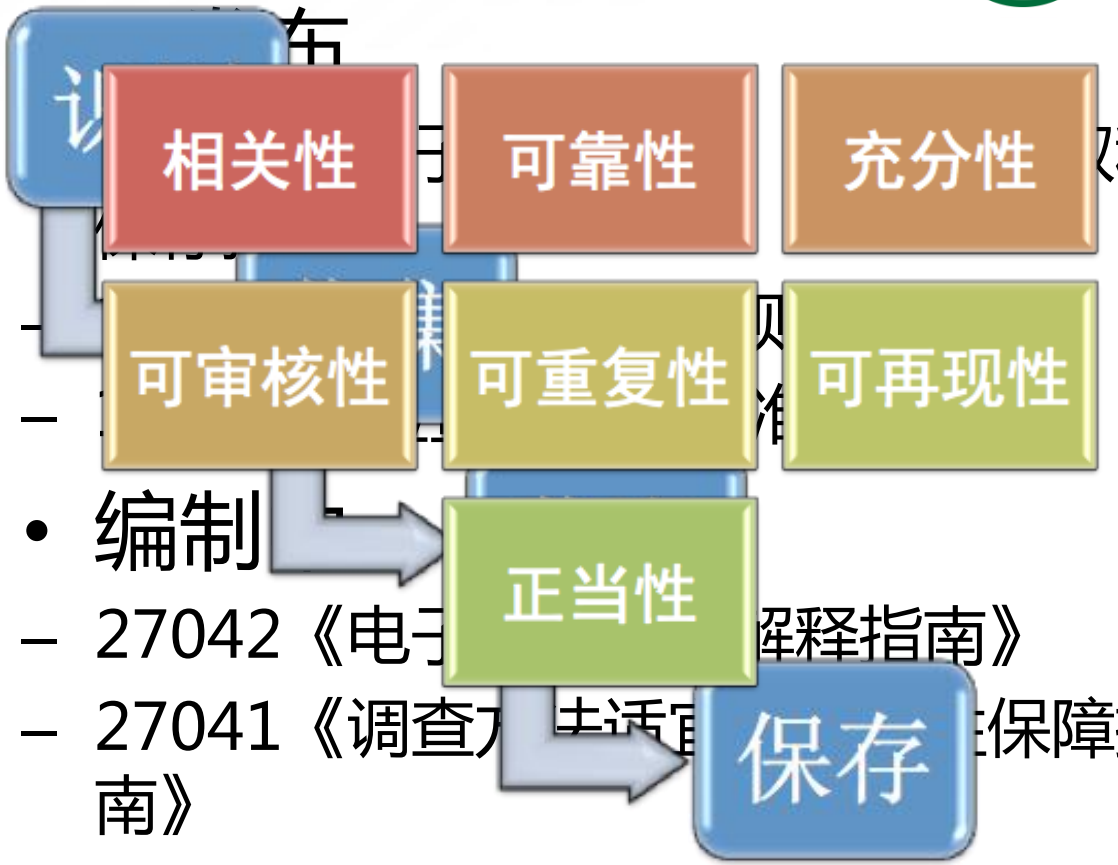

NIST


DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR


BSi
British Standards


ENGLAND, WALES & NORTHERN IRELAND
ACPO
ASSOCIATION OF CHIEF POLICE OFFICERS

ISO/IEC相关标准



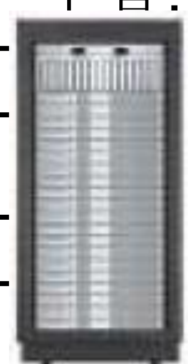
- 编制
  - 27042《电子[illegible]解释指南》
  - 27041《调查[illegible]保障指南》
  - 27043《调查原则和过程》

NIST相关标准

- SPECIAL PUBLICATIONS
  - …ERIES… …DA 取证
  - 既述和分… …取证指…
  - …, NIST… …机 取证
  - 既述和分… …响应事…
  - …, SP 8… …机 取证
  - …NIST… 《电子取证技术集成指南》
  - 工具：概述和分析》更新
  - …年，SP 8… …电话
  - …NIST… …动终端
  - …指南》… …》《移动
  - …参考资料… …计算取
  - …年，NIST… …取证指南
  - …挑战》

Collect software

Secure library



Compute file profiles

Reference Data Set (RDS)

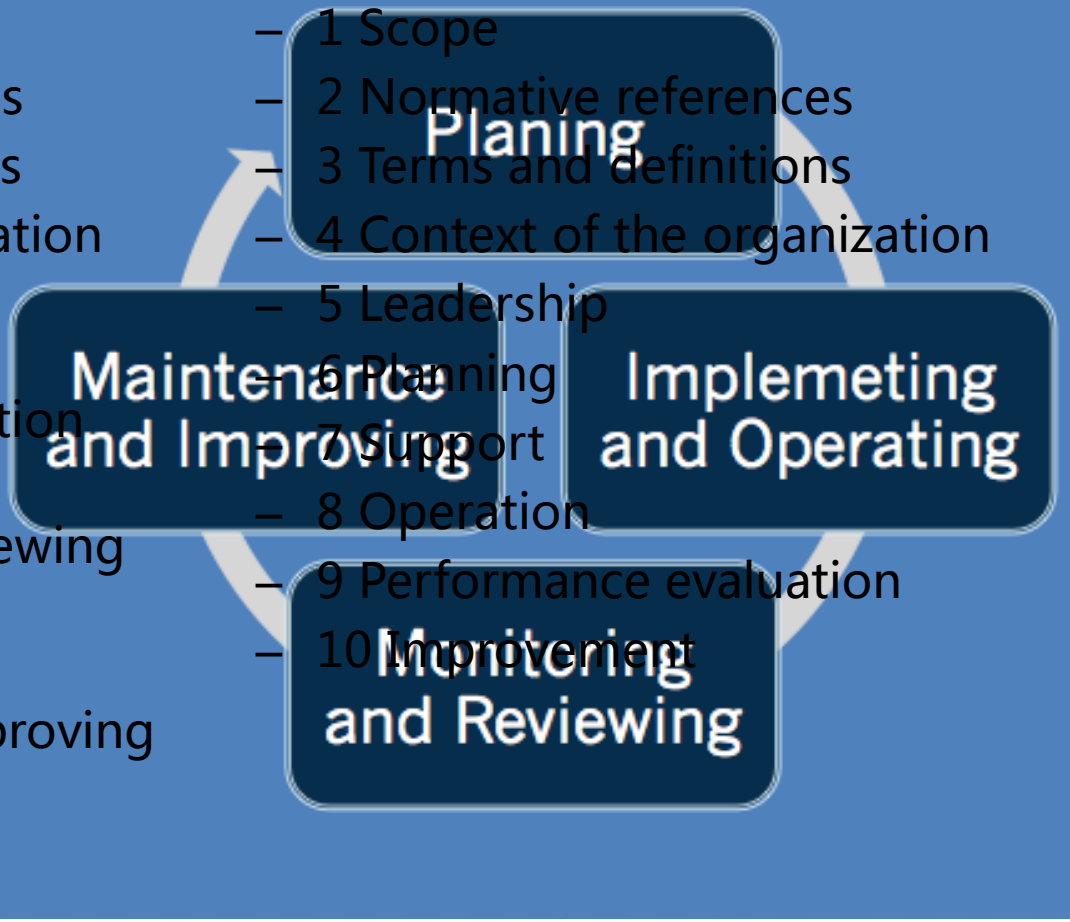
美国相关标准

- 美国司法部
  - 2001年, NCJ 187736 《计算机现场勘查指南》
  - 2007年, NCJ 210798 《互联网和计算机网络调查》
  - 2008年, NCJ 219941 《计算机现场勘查指南》第二版
  - 2009年, NCJ 227050 《计算机现场勘查参考资料》

英国相关标准

- 10008:2008
  - 1 Scope
  - 2 Normative references
  - 3 Terms and definitions
  - 4 Planning the information management system
  - 5 Implementing and operating the information management system
  - 6 Monitoring and reviewing the information management system
  - 7 Maintaining and improving the information management system

- 10008:2014
  - 1 Scope
  - 2 Normative references
  - 3 Terms and definitions
  - 4 Context of the organization
  - 5 Leadership
  - 6 Planning
  - 7 Support
  - 8 Operation
  - 9 Performance evaluation
  - 10 Improvement



IOCE Principles

- 英国高级警官协会(ACPO)

子证据实践指南》

uide for Computer Based Evidence

科学工作组(SWGDE)

子证据实践指南》

uide for Computer Based Evidence

http://www.swgde.org

- 1、必须应用标准的取证过程；
- 2、获取电子证据后，任何举措都不得改变证据；
- 3、接触原始证据的人员应该得到相关培训；
- 4、任何对电子证据进行获取、访问、存储或转移的活动必须有完整记录；
- 5、任何人持用电子证据时，必须对其在该证据上的任何操作活动负责；
- 6、任何负责获取、访问、存储或转移电子证据的机构须遵从上述原则。

中国国家标准

- GB/T 29360-2012 电子物证数据恢复检验规程
- GB/T 29361-2012 电子物证文件一致性检验规程
- GB/T 29362-2012 电子物证数据搜索检验规程

行业标准（1）

- 2008年发布
  - GA/T 754-2008 电子数据存储介质复制工具要求及检测方法
  - GA/T 755-2008 电子数据存储介质写保护设备检测方法
  - GA/T 756-2008 数字化设备证据数据发现提取固定方法
  - GA/T 757-2008 程序功能检验方法

行业标准（2）

- 2009年发布
  - GA/T 825-2009 电子物证数据搜索检验技术规范
  - GA/T 826-2009 电子物证数据恢复检验技术规范
  - GA/T 827-2009 电子物证文件一致性检验技术规范
  - GA/T 828-2009 电子物证软件功能检验技术规范
  - GA/T 829-2009 电子物证软件一致性检验技术规范
- 2013年发布
  - GA/T 1069-2013法庭科学电子物证手机检验技术规范
  - GA/T 1070-2013法庭科学计算机开关机时间检验技术规范
  - GA/T 1071-2013法庭科学电子物证Windows操作系统日志检验技术规范

行业标准（3）

- 2012年发布
  - GA/T 976-2012 电子数据法庭科学鉴定通用方法
  - GA/T 977-2012 取证与鉴定文书电子签名
  - GA/T 978-2012 网络游戏私服检验技术方法
- 2014年发布
  - GA/T 1770-2014 《移动终端取证检验方法》
  - GA/T 1771-2014 《芯片相似性比对检验方法》
  - GA/T 1772-2014 《电子邮件检验技术方法》
  - GA/T 1773-2014 《即时通讯记录检验技术方法》
  - GA/T 1774-2014 《电子证据数据现场获取通用方法》
  - GA/T 1775-2014 《软件相似性检验技术方法》
  - GA/T 1776-2014 《网页浏览器历史数据检验技术方法》

司法鉴定技术规范

- 2014年发布
  - SF/Z JD0400001-2014《电子数据司法鉴定通用实施规范》
  - SF/Z JD0401001-2014《电子数据复制设备鉴定实施规范》
  - SF/Z JD0402001-2014《电子邮件鉴定实施规范》
  - SF/Z JD0403001-2014《软件相似性检验实施规范》

其他相关技术规范

- 公安部
  - 《计算机犯罪现场勘验与电子证据检查规则》
  - 《公安机关电子数据鉴定规则》
- 最高人民检察院
  - 《人民检察院电子证据鉴定程序规则（试行）》
- 国家工商行政管理总局
  - 《关于工商行政管理机关电子数据证据取证工作的指导意见》
- 中华全国律师协会
  - 《律师办理电子数据证据业务操作指引》

实验室管理规范

- 国家认可委
  - CNAS-CL08:2013《司法鉴定/法庭科学机构能力认可准则》
  - CNAS-CL27：2014《司法鉴定/法庭科学机构能力认可准则在电子物证鉴定领域的应用说明》
  - CNAS-AL13《司法鉴定/法庭科学认可领域分类》
  - CNAS-AL14《司法鉴定/法庭科学认可领域仪器设备配置标准》
- 国家认监委
  - 《司法鉴定机构资质认定评审准则》

面临的挑战

Thanks!

guohong@stars.org.cn