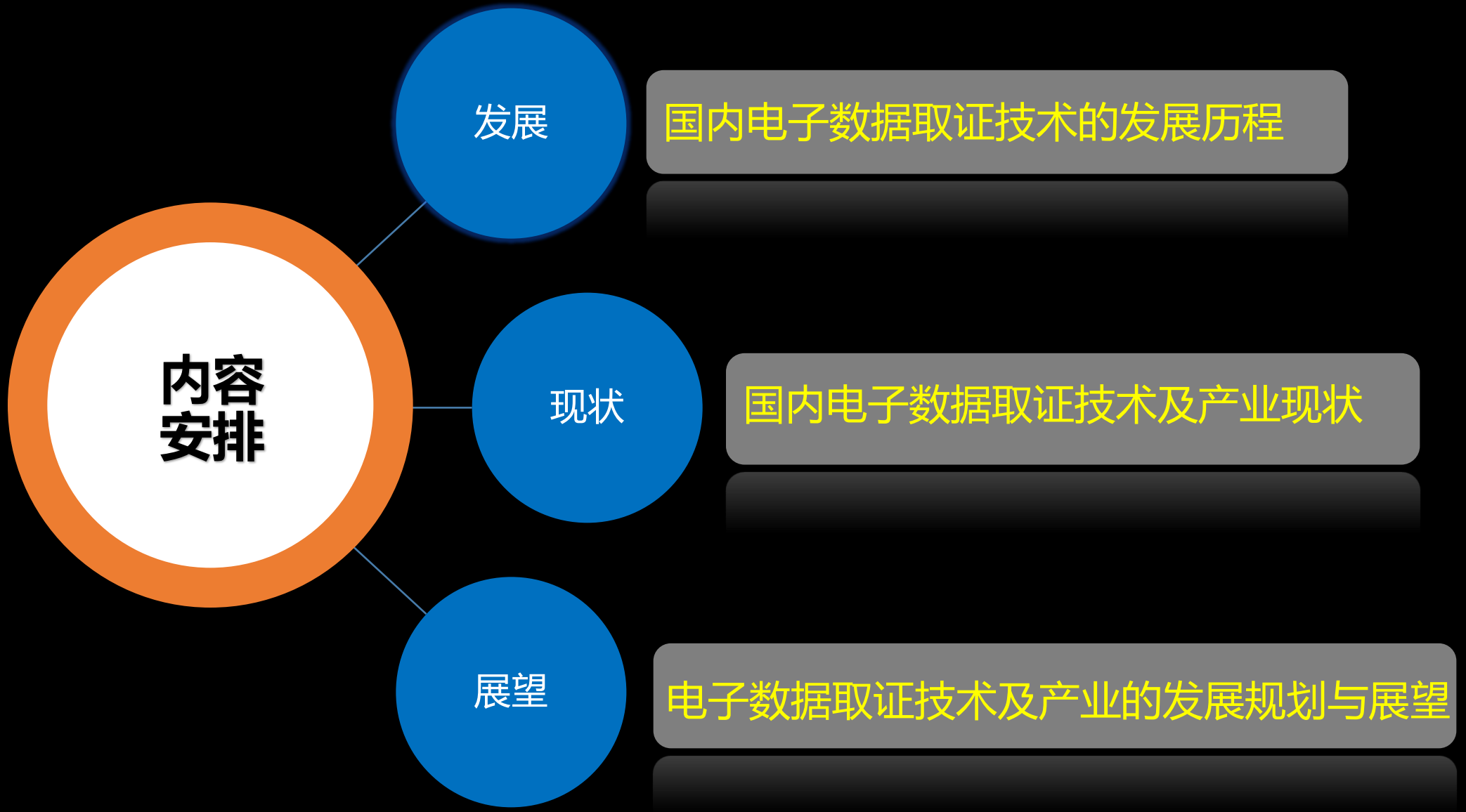
国内计算机取证发展历程与展望

美亚柏科信息股份有限公司

赵庸

2016.8.17


内容
安排
发展
国内电子数据取证技术的发展历程
现状
国内电子数据取证技术及产业现状
展望
电子数据取证技术及产业的发展规划与展望

Meiya Pico
美亚柏科

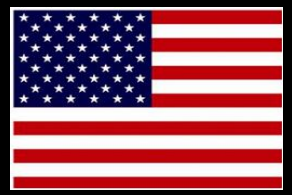
国内计算机取证的发展历程

Part 01

Meiya Pico
美亚柏科

国外计算机取证的发展

早在上世纪80年中期，计算机取证技术就已开始在执法部门和军队中使用。1999年，电子数据取证的商用工作开始出现，当时，EnCase这一开创性的取证工具，在国际计算机调查专家会议IACIS上第一次被介绍。



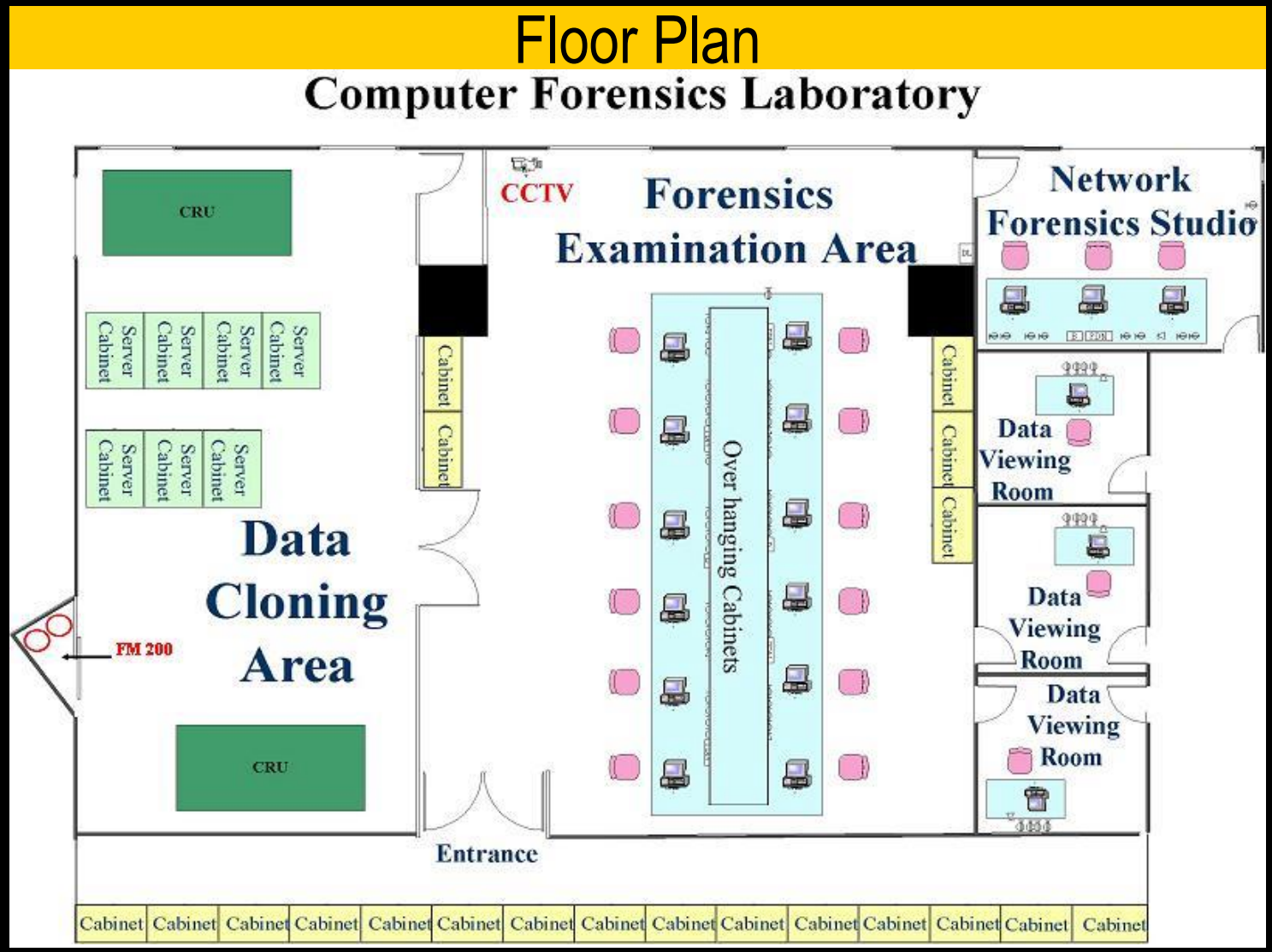
联邦调查局（FBI），司法部（NIJ），缉毒局（DEA）等多家执法部门，根据权限分别设立了电子数据取证的专门机构。

英国内政部设立有网络犯罪调查部门，其电子数据取证机构的特点是全部社会化。

2004年，国家警察厅建立了数据证据分析中心（Center of Digital Evidence Analysis）进行电子数据取证工作。

国内计算机取证的发展

香港警务处计算机取证实验室
（2001年）



香港警务处计算机取证实验室

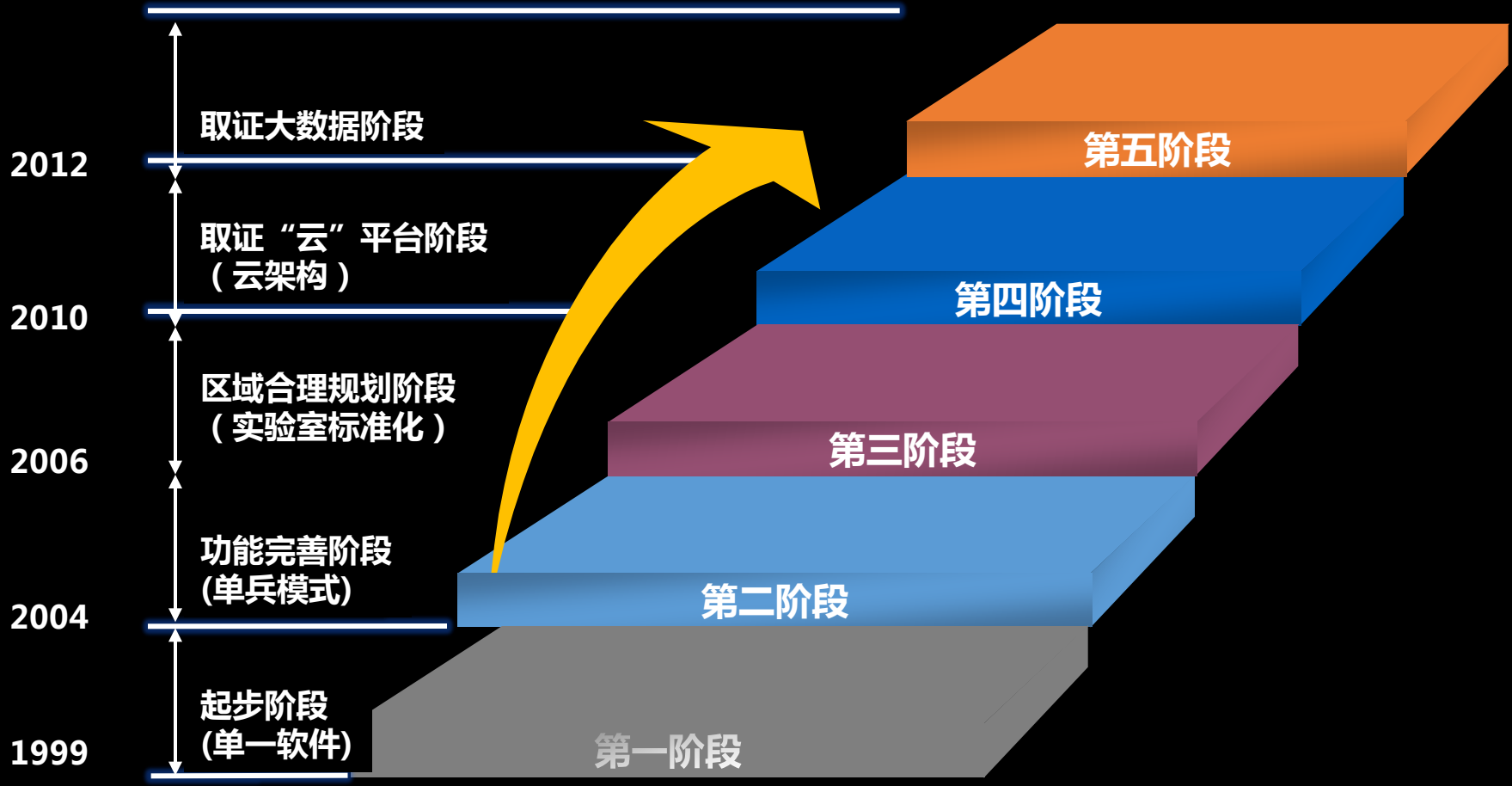
Data Cloning Area

Working Benches

Data Viewing Room

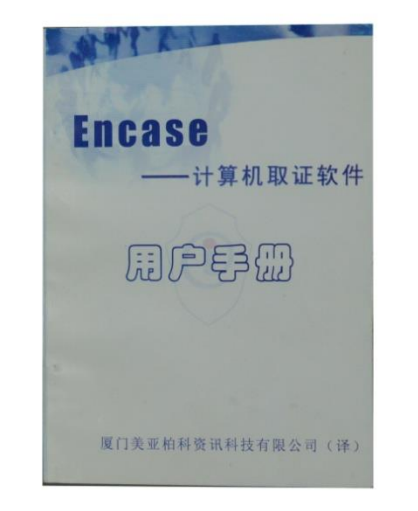
Network Forensics Studio

国内计算机取证的发展历程



第一阶段（起步）

- 1999年 第一款计算机取证工具EnCase诞生
- 2002年 国内首款“计算机取证勘查箱”诞生（美亚柏科）
  - 各类型只读接口
  - 美国Logicube SF500、ICS Solo2
  - Encase取证分析系统；



第二阶段（功能完善）

■功能完善阶段（2004、2005年）

- 摆脱原来的单兵工作模式；
- 开始出现角色的概念；
- 区域由“大单间”向“多分割”方向发展；
- 简单的访问权限控制初现；
- 无尘环境不具备。

第二阶段

该阶段计算机取证技术成功应用的典型案例

马加爵案件

马加爵熟练掌握网络 高科技成为缉捕其重要因素

http://www.sina.com.cn 2004年03月17日10:25 新华网

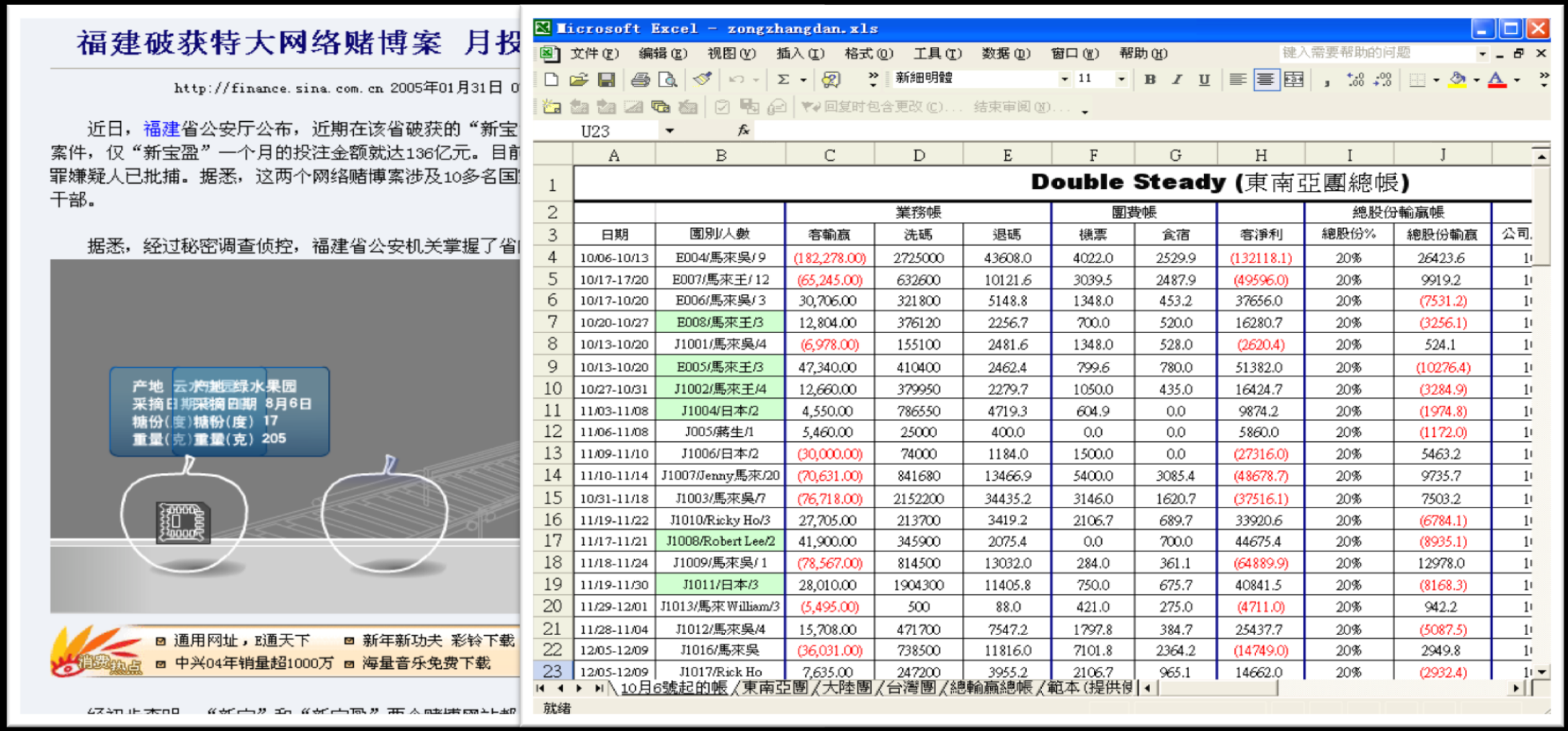
新华网海南频道三亚3月16日电（王英诚　赵叶苹）“此次能够成功缉捕国家A级通缉犯马加爵，一个重要的原因就是高科技手段在侦察过程中的出色运用。”谈及此次抓捕，三亚市公安局局长王少山难以掩饰心中的喜悦。

据悉，马加爵熟练掌握网络技术，经常在网上发布一些迷惑公安部门的信息。还常有网民以“马加爵”之网名在网上闲逛，干扰人们和办案人员的视线，以致数次因假消息而在全国范围内引起轩然大波。

据了解，公安部门在案发后运用计算机技术对马加爵曾经使用过的电脑进行了十分周密的分析。办案人员发现，马加爵在案发前后曾经大量浏览一些省、市的地理、人文情况。其中海南省是他网上浏览比较多的地区。他曾经关注过海南的旅游、出租屋、房地产以及交通等信息，其中三亚地区他犹为关心。公安部随即将这些信息通报海南省公安厅，海南省公安部门立刻针对这些情况制定了完整而周密的抓捕

第二阶段

该阶段计算机取证技术成功应用的典型案例



福建破获特大网络赌博案 月投

http://finance.sina.com.cn 2005年01月31日 0

近日，福建省公安厅公布，近期在该省破获的“新宝
案件，仅“新宝盈”一个月的投注金额就达136亿元。目前
罪嫌疑人已批捕。据悉，这两个网络赌博案涉及10多名国
干部。

据悉，经过秘密调查侦控，福建省公安机关掌握了省

产地 云南地区绿水果园
采摘日期 采摘日期 8月6日
糖份(度) 糖份(度) 17
重量(克) 重量(克) 205

消费热点
通用网址，E通天下
新年新功夫 彩铃下载
中兴04年销量超1000万
海量音乐免费下载

Microsoft Excel - zongzhangdan.xls

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 数据(D) 窗口(W) 帮助(H)

U23

	A	B	C	D	E	F	G	H	I	J
1	Double Steady (東南亞團總帳)									
2			業務帳			團費帳			總股份輸贏帳	
3	日期	團別/人數	客輸贏	洗碼	退碼	機票	食宿	客淨利	總股份%	總股份輸贏
4	10/06-10/13	E004/馬來吳/9	(182,278.00)	2725000	43608.0	4022.0	2529.9	(132118.1)	20%	26423.6
5	10/17-17/20	E007/馬來王/12	(65,245.00)	632600	10121.6	3039.5	2487.9	(49596.0)	20%	9919.2
6	10/17-10/20	E006/馬來吳/3	30,706.00	321800	5148.8	1348.0	453.2	37656.0	20%	(7531.2)
7	10/20-10/27	E008/馬來王/3	12,804.00	376120	2256.7	700.0	520.0	16280.7	20%	(3256.1)
8	10/13-10/20	J1001/馬來吳/4	(6,978.00)	155100	2481.6	1348.0	528.0	(2620.4)	20%	524.1
9	10/13-10/20	E005/馬來王/3	47,340.00	410400	2462.4	799.6	780.0	51382.0	20%	(10276.4)
10	10/27-10/31	J1002/馬來王/4	12,660.00	379950	2279.7	1050.0	435.0	16424.7	20%	(3284.9)
11	11/03-11/08	J1004/日本/2	4,550.00	786550	4719.3	604.9	0.0	9874.2	20%	(1974.8)
12	11/06-11/08	J005/蔣生/1	5,460.00	25000	400.0	0.0	0.0	5860.0	20%	(1172.0)
13	11/09-11/10	J1006/日本/2	(30,000.00)	74000	1184.0	1500.0	0.0	(27316.0)	20%	5463.2
14	11/10-11/14	J1007/Jenny馬來/20	(70,631.00)	841680	13466.9	5400.0	3085.4	(48678.7)	20%	9735.7
15	10/31-11/18	J1003/馬來吳/7	(76,718.00)	2152200	34435.2	3146.0	1620.7	(37516.1)	20%	7503.2
16	11/19-11/22	J1010/Ricky Ho/3	27,705.00	213700	3419.2	2106.7	689.7	33920.6	20%	(6784.1)
17	11/17-11/21	J1008/Robert Lee/2	41,900.00	345900	2075.4	0.0	700.0	44675.4	20%	(8935.1)
18	11/18-11/24	J1009/馬來吳/1	(78,567.00)	814500	13032.0	284.0	361.1	(64889.9)	20%	12978.0
19	11/19-11/30	J1011/日本/3	28,010.00	1904300	11405.8	750.0	675.7	40841.5	20%	(8168.3)
20	11/29-12/01	J1013/馬來William/3	(5,495.00)	500	88.0	421.0	275.0	(4711.0)	20%	942.2
21	11/28-11/04	J1012/馬來吳/4	15,708.00	471700	7547.2	1797.8	384.7	25437.7	20%	(5087.5)
22	12/05-12/09	J1016/馬來吳	(36,031.00)	738500	11816.0	7101.8	2364.2	(14749.0)	20%	2949.8
23	12/05-12/09	J1017/Rick Ho	7,635.00	247200	3955.2	2106.7	965.1	14662.0	20%	(2932.4)

10月6號起的帳 / 東南亞團 / 大陸團 / 台灣團 / 總輸贏總帳 / 範本 (提供

就緒

第二阶段（功能完善）

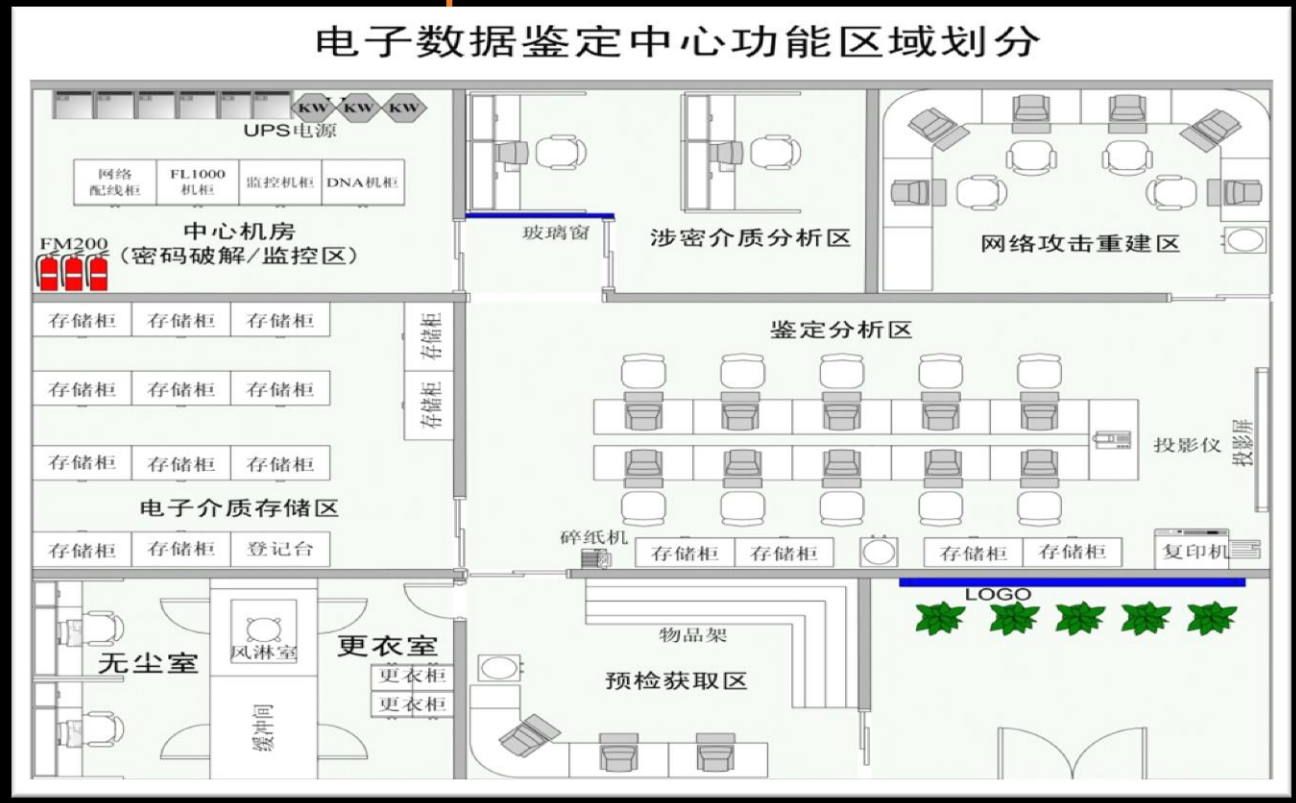
- 国内尝试研发取证设备及软件，国内外设备混用阶段
  - 硬件设备：
    - 分立设备（SF5000、SOLO II、DC8100/8200、勘查箱、大量只读锁）
    - 大量转接卡（IDE、SCSI）
    - 简单整合
  - 软件：
    - EnCase v4
    - FTK v2.0
    - DiskForen
    - PDA Seizure
    - DNA 2.0
    - AN 6

- 具有中国特色的“鉴定流程审计监管”概念产生

第三阶段（实验室阶段）

■规范化管理阶段（2006-2010年）

- 摆脱原来的流水工作模式；
- 开始逐步符合司法规范；
- 功能由“慎独”向“可控、可审”
- 角色丰富，管理
- 更趋于规范、严格。
- 无尘室被重视。



第三阶段（实验室阶段）

- 取证设备及软件
  - 硬件设备
    - 复制设备：SOLO III、DC8101、勘查箱
    - 只读设备：有机整合，形成桌面模块
    - 工作台专业化明显
    - 无尘工作台
    - 移动勘查取证综合平台：FL150/200
  - 软件
    - EnCase v5汉化
    - FTK v2
    - Cell Seizure/safemobile/DC-4500
    - DNA 2.3/Rainbow Table
    - AN 7
  - 案件管理系统成形

国内首个国家级计算机取证实验室

第三阶段（实验室阶段）

- 国产取证设备及软件逐渐丰富，功能逐渐完善，实验室开始大规模建设
  - 硬件设备：
    - 复制设备：TD1、SOLO IV、DC8200pro、勘查箱
    - 只读设备：DC8750pro功能强化和完善
    - 100级无尘工作室
    - 取证设备：FL-800、DC8000pro、FL200pro、仿真、破解、在线取证
  - 软件
    - EnCase v6
    - FTK v3
    - Device Seizure/safemobile/DC-4500a
    - DNA 3/ATT1000pro/Elcomsoft
    - AN 8
    - X-ways
    - 取证大师（FM2008）、SafeAnalyzer
  - 案件管理系统：加入检材管理、光盘归档刻录打印

实验室建设指导规范

NO.2 引用文件

GB 50016-2006 建筑设计防火设计规范；
GB 50015-2010 建筑给排水设计规范；
GB 50057-2010 建筑物防雷设计规范；
GB 50343-2012 建筑物电子信息系统防雷技术规范；
GB 50222-2001 建筑内部装修设计防火规范；
GB 50019-2002 采暖通风与空气调节设计规范；
GB 50311-2009 综合布线系统工程设计规范；
GB 50073-2001 洁净厂房设计规范；
GB。。。。。。

NO.6 建设要求

建筑装饰

环境要求
温湿度
电磁干扰
磁场
振动
洁净度
电气要求

建筑面积

按级别要求
位置选择
建筑结构
采光
高度
网络
消防
防雷

NO.7 建设标准

《公安机关网安部门电子物证检验鉴定实验室装备分级标准》

《公安机关网安部门电子物证检验鉴定实验室能力分级标准》

能力要求	数据固定	数据提取	远程提取	数据发现	数据解密	数据解码	数据分析	程序分析	实验室管理
国家级	√	√	√	√	√	√	√	√	√
一级	√	√	√	√	√	√	√	-	√
二级	√	√	-	√	√	-	√		√
三级	√	√		√			√		

NO.1 科学定义

实验室需有界定的术语和定义

NO.5 业务范围

损坏存储介质检验
数据恢复
数据搜索
文件一致性检验
软件功能性检验
软件一致性检验
时间属性检验
电子邮件检验
上网记录检验
即时通讯检验
日志检验
数据库检验

电子物证提取与固定
现场保全备份
易丢失数据提取
密码破解
手机检验

信息应用

手机信息关联分析
社交网络信息挖掘库分析

基础建设

手机样本库
硬盘录像机样本库
硬盘样本库

NO.3 建设分级

实验室建设需有分级：

国家级实验室	5名鉴定人
一级实验室	4名鉴定人
二级实验室	3名鉴定人
三级实验室	3名鉴定人

基本配置

场地要求	操作区	行政区
国家级	200	90
一级	160	60
二级	120	45
三级	独立	独立

NO.4 区域设置

第四阶段

- “云”阶段（2010年开始）
  - 全面提升技术手段和设备能力；
  - “绿色”超算；
  - 功能由“单中心”向“分布式”方向发展；
  - 远程协助、会诊、技术支持得以实现；
  - 数据关联查询分析；
  - 远程取证；
  - 邮件取证；
  - QQ群信息查询；
  - 取证GPS；
  - 网络舆情、热点分析；
  - 基础信息查询。

第四阶段

- 国产取证设备及软件全面替代国外产品，产品线丰富
  - 硬件设备：
    - 复制设备：第五代复制设备13G/min、支持SAS
    - 只读设备：DC8750pro超级只读模块
    - 100级无尘工作室
    - 取证设备：取证魔方、取证精灵、 FL800取证塔、破解（ ATT5000pro/极光II ）、在线取证
  - 软件
    - EnCase v6
    - FTK v3
    - Device Seizure/safemobile/DC-4500pro
    - DNA 3/ATT1000pro/Elcomsoft
    - AN 8
    - X-ways
    - 取证大师（网络版、标准版、现场版）、SafeAnalyzer
  - 实验室认可需求，案件管理系统：向认可靠近，加入预检功能

Meiya Pico
美亚柏科

国内电子数据取证技术及产业现状

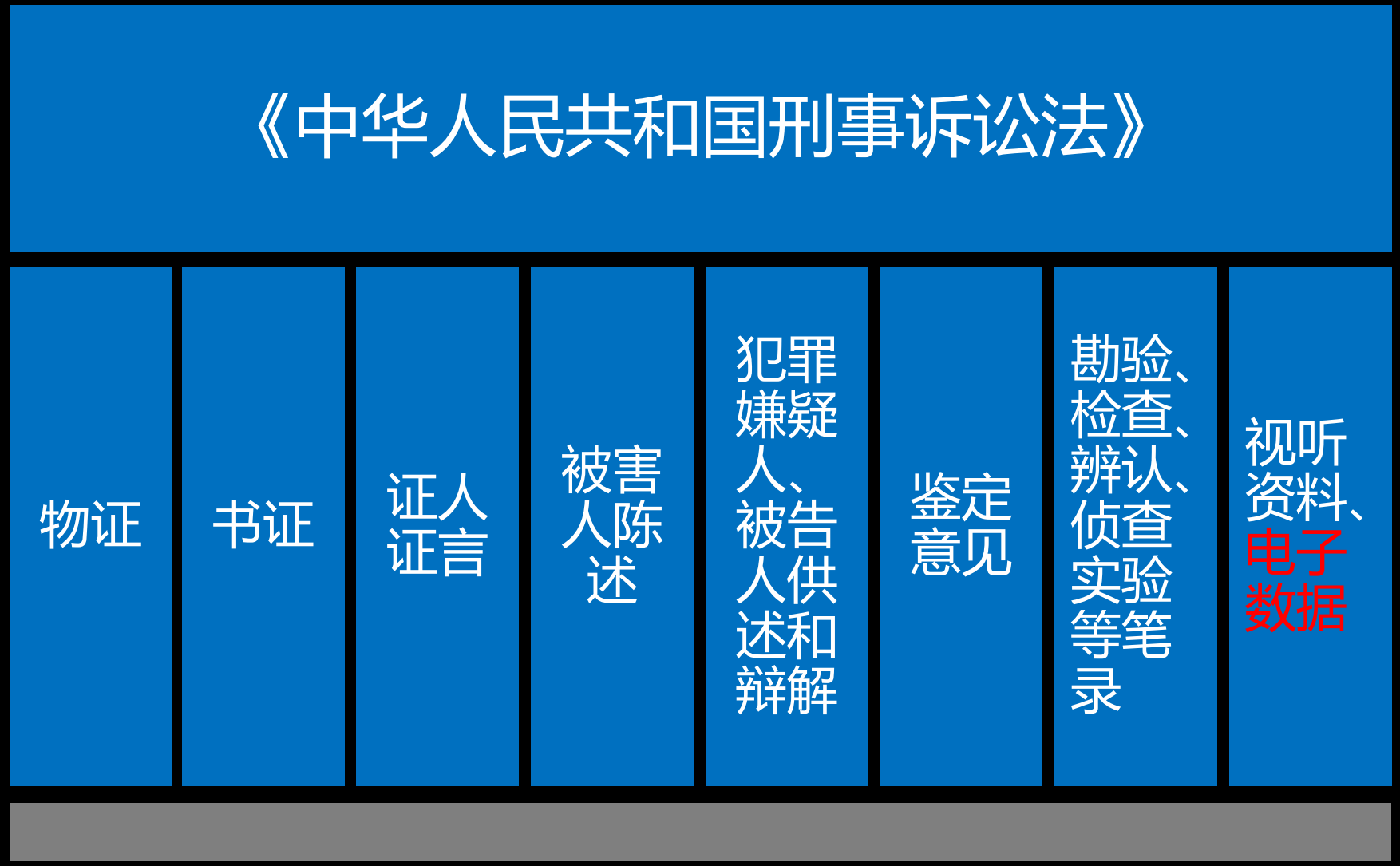
Part 02

Meiya Pico
美亚柏科

信息技术发展状况

- 信息技术和信息产业的迅速发展，对我国国民经济和社会发展的各个领域都产生了广泛而深远的影响。
- 互联网中心统计报告，截至2015年5月，我国网民规模达到6.68亿，手机网民5.94亿。
- 电子数据已成为司法机关获取破案线索和诉讼证据的重要来源。
- 因此，从法律、规范、应用等多个领域开始对计算机取证技术和应用做出了系统性的支持。

法律依据


《中华人民共和国刑事诉讼法》
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
鉴定意见
勘验、检查、辨认、侦查实验等笔录
视听资料、电子数据

规范文件

- 《GT/A 825-2009 电子物证数据搜索检验技术规范》
- 《GT/A 826-2009 电子物证数据恢复检验技术规范》
- 《GT/A 827-2009 电子物证文件一致性检验技术规范》
- 《GT/A 828-2009 电子物证软件功能检验技术规范》
- 《GT/A 829-2009 电子物证软件一致性检验技术规范》

应用领域

- 刑事案件的侦查取证和诉讼
- 民事案件的举证和诉讼
- 行政诉讼案件的举证和处理
- 企业内部调查

实验室认可

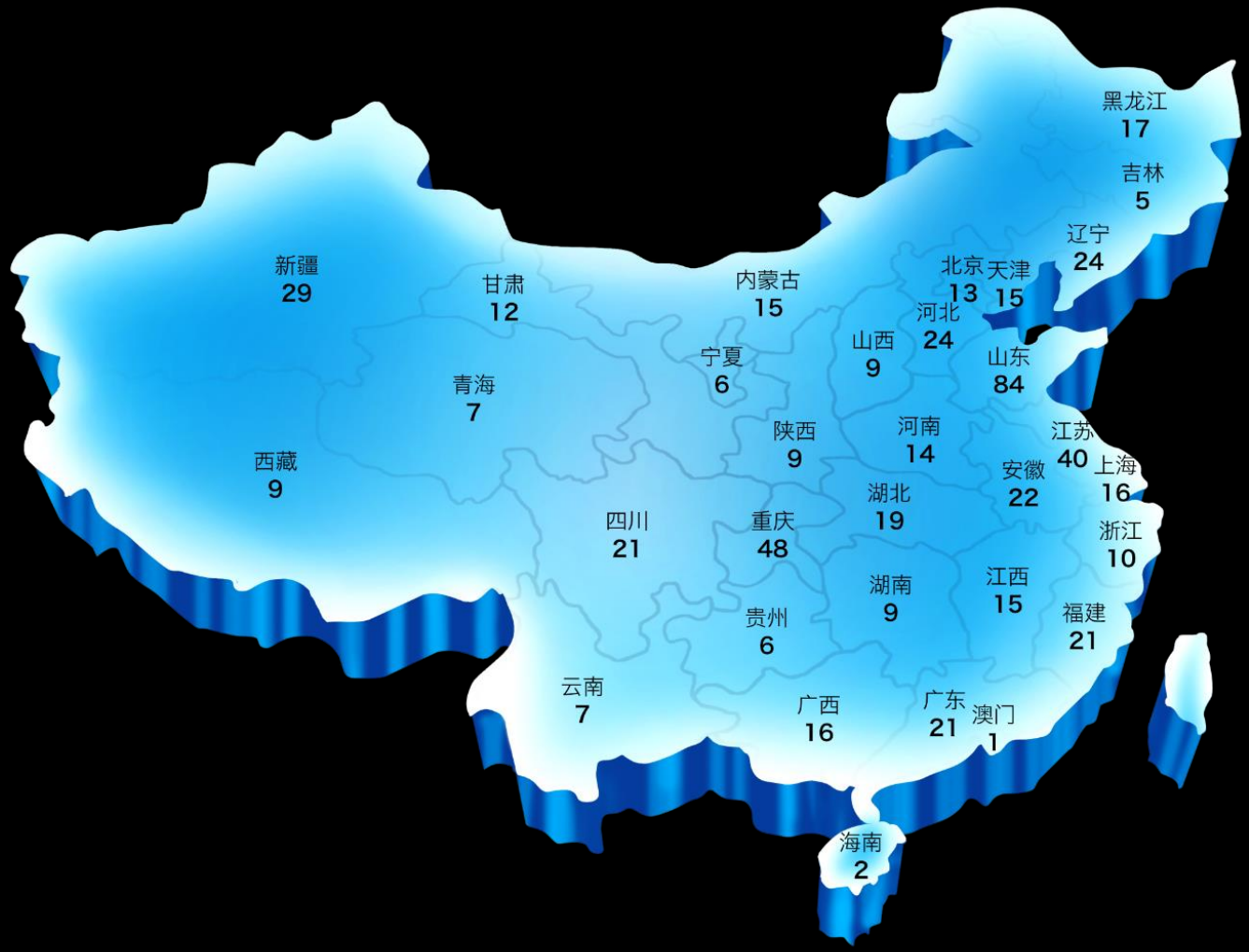
- 中国合格评定国家认可委员会（英文名称为：China National Accreditation Service for Conformity Assessment 英文缩写为：CNAS），是根据《中华人民共和国认证认可条例》的规定，由国家认证认可监督管理委员会批准设立并授权的唯一的国家认可机构，统一负责实施对认证机构、实验室和检查机构等相关机构的认可工作。
- 国家权威认可机构对实验室具备实施特定检测（如：司法鉴定、法庭科学）工作能力的一种正式承认。
- 提高了鉴定机构的管理水平与技术能力,其技术能力和所出数据均可得到国家以及全球一百多个其它国家/地区或认可机构所承认。


中国合格评定国家认可委员会
实验室认可证书
（No. CNAS L4709）
兹证明：
厦门市美亚柏科信息安全研究所有限公司
福建中证司法鉴定中心
福建省厦门市软件园二期观日路14号，361008
符合 ISO/IEC 17025：2005《检测和校准实验室能力的通用要求》（CNAS-CL01《检测和校准实验室能力认可准则》）的要求，具备承担本证书附件所列检测服务的能力，予以认可。
获认可的能力范围见标有相同认可注册号的证书附件，证书附件是本证书组成部分。
发证日期：2010-08-27
有效期至：2013-08-26
初次认可：2010-08-27
中国合格评定国家认可委员会授权人

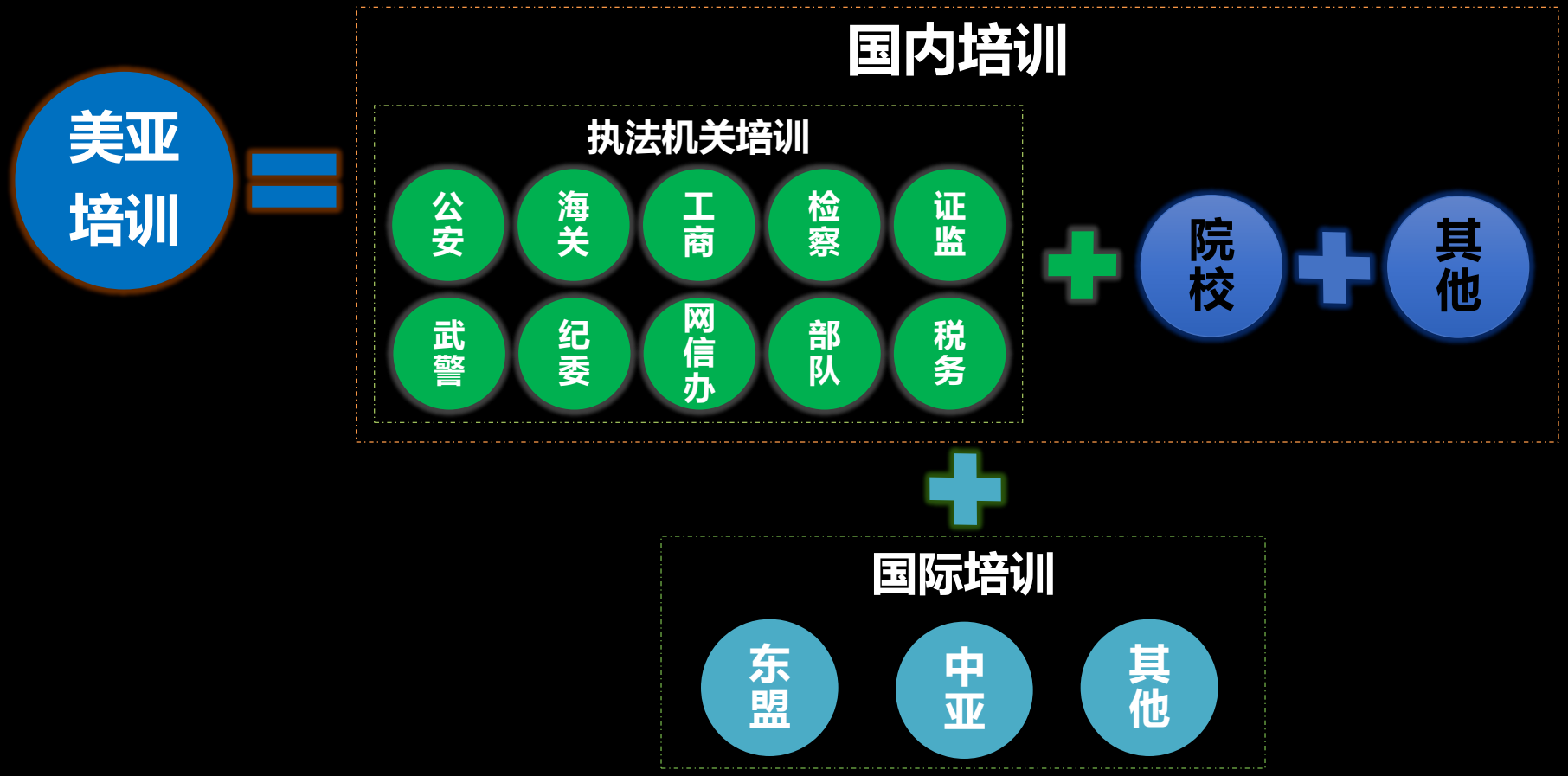
实验室建设情况

美亚柏科已在全国建设781个实验室 （截止2016年7月）

公检法：700个
工商：31个
院校：25个
其他：25个



取证技能培训



产业状况

- 产业定位：信息安全（或网络空间安全）相关领域。
- 产业规模：
  - 从业企业：100+家
  - 市场空间：11.3亿元
- 科研院所：20+家
- 市场培育：
  - 每年相关会议、论坛、峰会：10+个
  - 参会及游客：10000+人
- 中国电子学会计算机取证专家委员会是全国第一个专业委员会。（**丁丽萍**2004年筹组，2005年第一次会议，北京人民警察学院）

产业问题

1. 同质化问题：

门槛不高：没有准入制度，良莠不齐

基础不实：基础研究的投入普遍不足

创新乏力：抄袭、仿制阻碍创新动力

瓶颈阻碍：重点、难点问题突破很难

2. 产业规模：

- 从业企业：100+家
- 市场空间：11.3亿元

11.3 ÷ 100 = 0.113 （亿元）

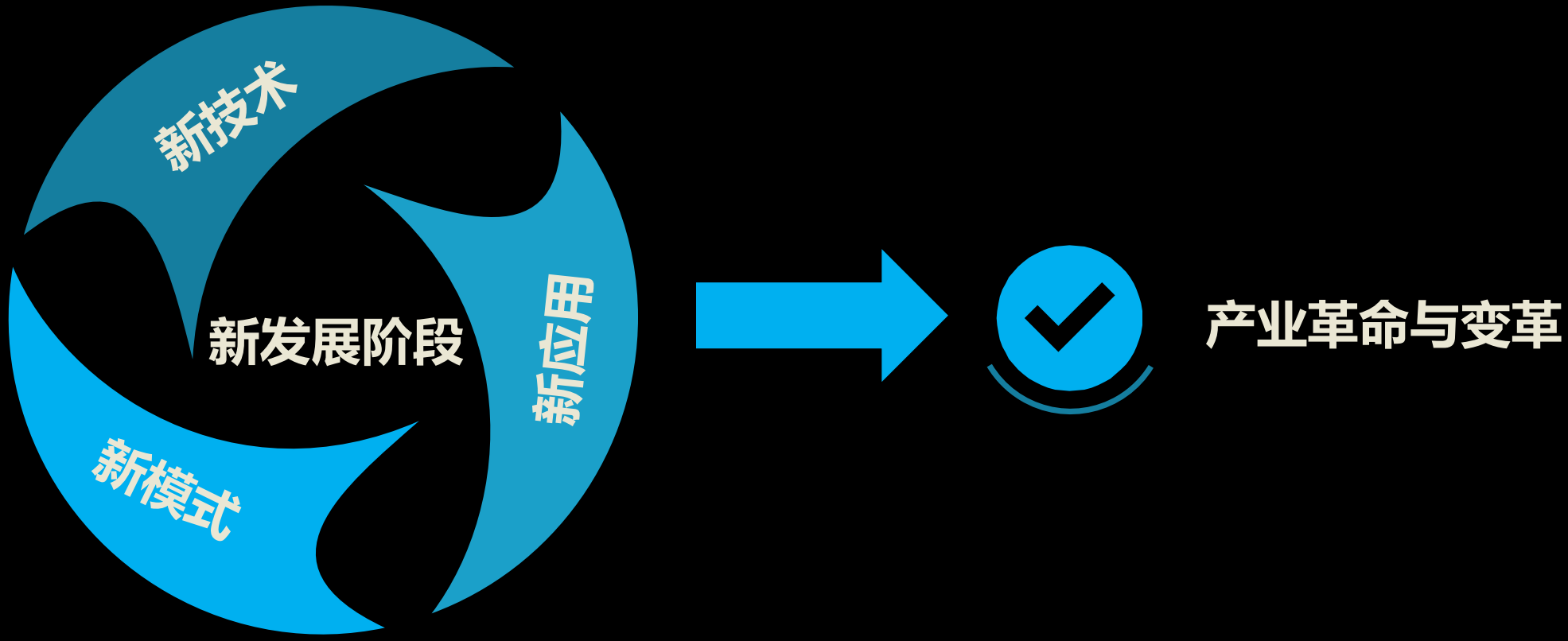
Meiya Pico
美亚柏科

电子数据取证技术及产业的发展规划与展望

Part 03

Meiya Pico
美亚柏科

新形势下的背景



市场规划

一、取证技术衍生出来的增值服务：

1、电子数据司法鉴定服务；

2、企业计算机取证与调查服务；

3、电子数据取证专家咨询服务；

4、信息保全与证据保全服务。

二、取证产品拓展新市场：

拓展新行业和领域；沿着国家“一带一路”战略指导，走向国际市场。

大数据背景下的计算机取证展望

发展展望

产品装备化、系统平台化

产品装备化，涵盖了取证全流程的装备化产品，服务于不同阶段的取证需求。系统平台化涵盖整合多渠道数据、规范业务标准、规范数据标准等工作，实现各种电子数据的纵向逐层汇聚，横向数据共享、协同工作的模式

数据分析智能化

人物的多维度刻画，运用图形可视化技术的数据可视化分析
大数据实战分析思维，未来的数据分析模式
语义分析技术，数据分析的人工智能

实验室建设标准化

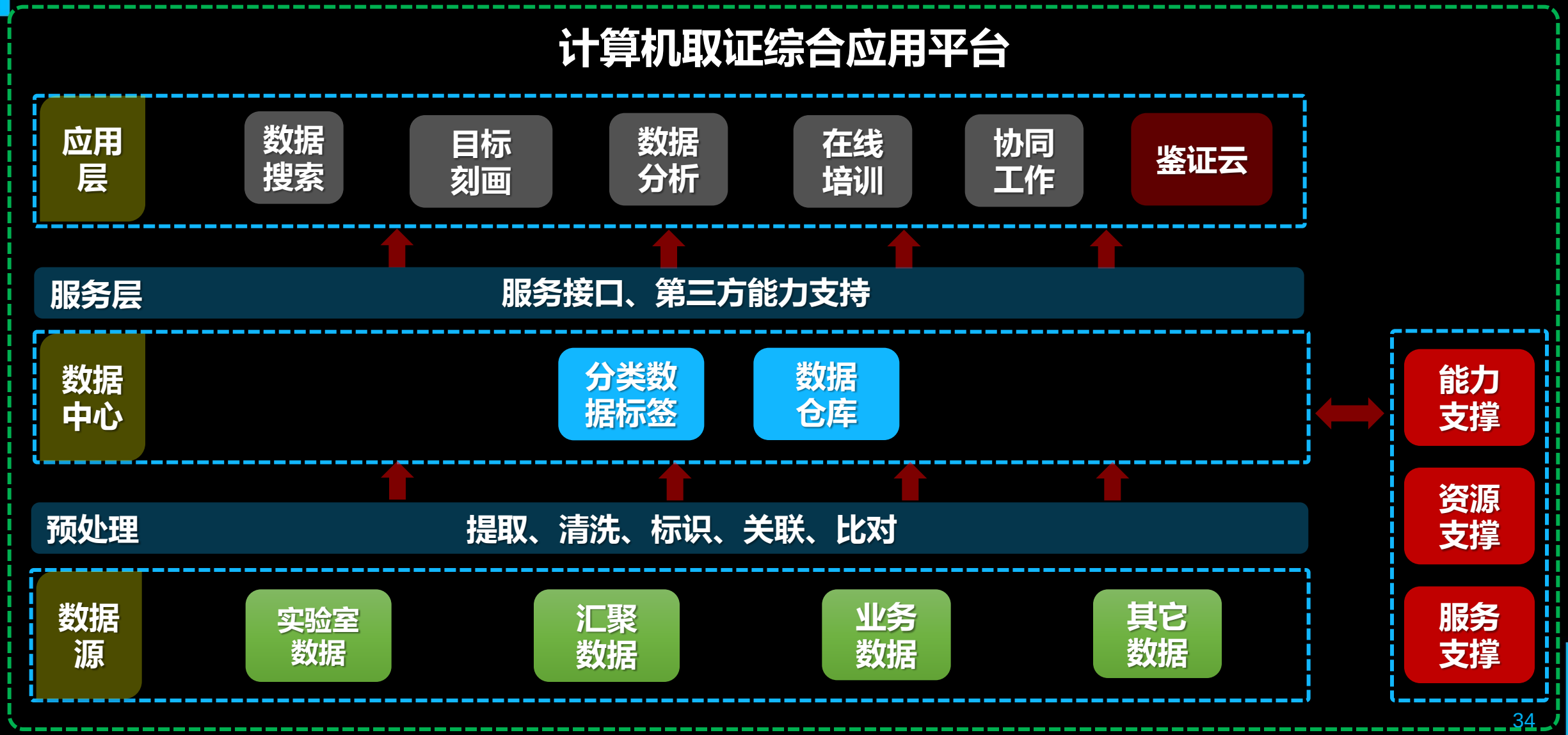
通过实验室建设标准化，实现电子数据鉴定技术、管理和法律的融合，使管理更加规范，结论更加严谨。包括管理物联化、实验室互联互通协同工作、差异化的行业标准、实验室认可认证资格认定。

更多新型电子设备的取证

物联网及智能设备取证：如车载设备、可穿戴设备、无人机等
芯片级取证
云环境下远程取证与存证技术
工业控制网络取证技术

取证大数据平台建立与应用

实验室大数据应用


计算机取证综合应用平台
应用层
数据搜索
目标刻画
数据分析
在线培训
协同工作
鉴证云
服务层
服务接口、第三方能力支持
数据中心
分类数据标签
数据仓库
预处理
提取、清洗、标识、关联、比对
数据源
实验室数据
汇聚数据
业务数据
其它数据
能力支撑
资源支撑
服务支撑

大数据展望


政府大数据开放
服务大众--关注民生及便民服务
网络空间大数据监管
服务行政执法部门--维护网络空间秩序
网络空间安全
服务司法机关--打击犯罪
促 进
能力延伸
保 障

THANKS

FOR YOUR TIME !

2016

Meiya Pico
美亚柏科