



# 第十四届CCFC计算机取证技术峰会

The 14th China Computer Forensic Conference



**报告主题:**

**电子证据的扩张**  
**Expansion of Digital Evidence**

**演 讲:**

**韩马剑**  
**河北省公安厅**

# 引言



- ◆ 电子数据证据正在从以内容数据为主的直接单一证据证明维度，向行为分析、主观心理刻画等多证据证明维度转变
- ◆ 电子数据证据正在从一个专业技术领域向全领域扩张

# 主要内容



1

2

3

4

**电子数据范围和能力的变化**

**电子证据的广度扩张**

**电子证据的维度扩张**

**机遇与挑战**



# PART ONE

**电子数据范围和能力的  
变化**

## 在法律层面电子数据的范围不断扩大

《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》

电子邮件、电子数据交换、网上聊天记录、博客、微博客、手机短信、电子签名、域名等

《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》

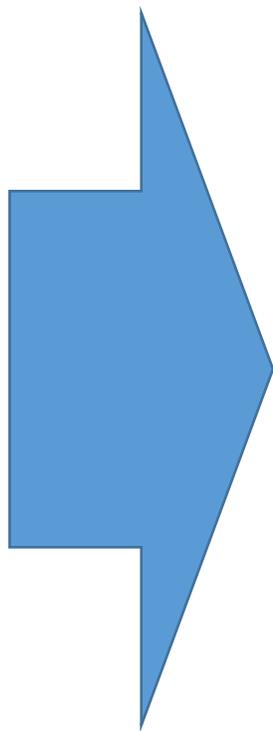
包括但不限于下列信息、电子文件：

- （一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；
- （二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；
- （三）用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；
- （四）文档、图片、音视频、数字证书、计算机程序等电子文件。

## 记录能力不断增强

- 通讯类信息
- 网上行为类信息
- 社会属性类信息

计算机、手机



- 人或器官的行为信息
- 场所环境信息
- 设备状态信息

智能家居、可穿戴  
设备、传感设备

# PART TWO

## 电子证据的广度扩张

# 电子证据的广度扩张



## 证据：

- 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**

**在法庭科学中，电子数据与物证、书证、视听资料的边界越来越模糊**

# 电子证据的广度扩张

## 电子数据证据正逐渐向物证、书证领域进行扩张



## 电子手写签名和印章

## 侦查实务中，不同案件对电子数据提出了更丰富的证据要求

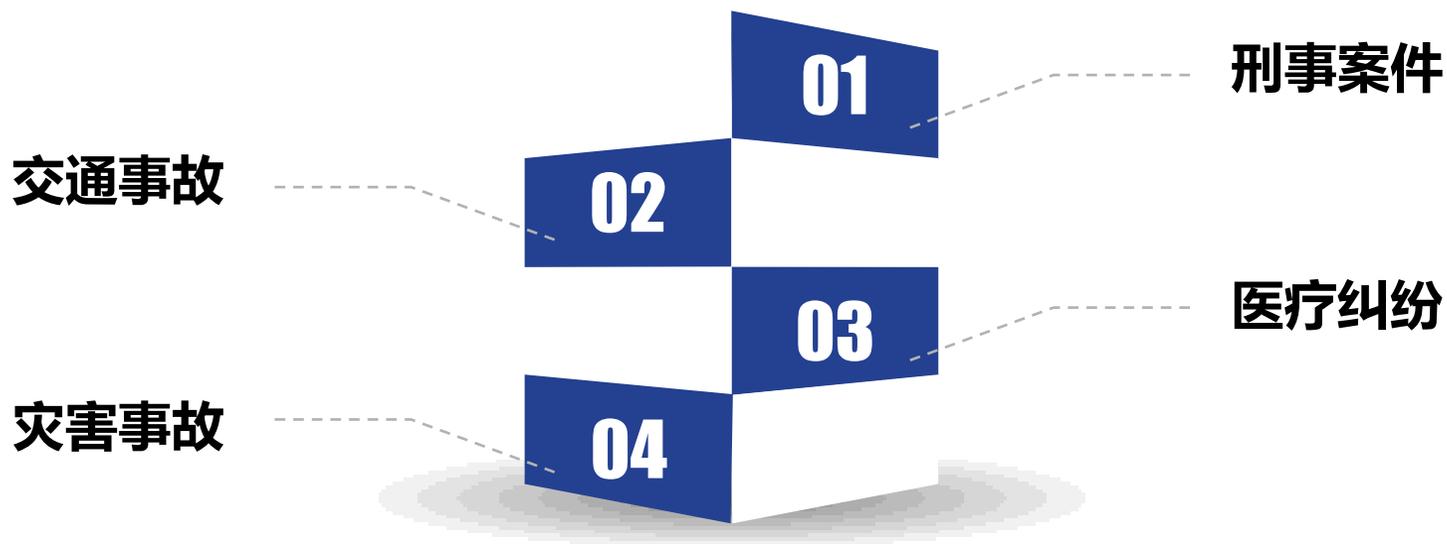
- **GPS轨迹、日志信息**
- **智能家居指令记录、日志信息**
- **软硬件运行状况记录**
- ... ..

# PART THREE

## 电子证据的维度扩张

# 电子证据的维度扩张

人们对电子证据的关注点已经不仅仅是电子数据内容的含义，而且更加关注电子数据所代表的人的行为、心理以及产生的后果。



# 电子证据在传统刑事案件现场勘查中的扩张

现在



痕迹物证



生物物证



微量物证



计算机手机信息内容

长期以来，我们大部分刑事案件现场勘查的重点是痕迹物证、生物物证、微量物证和在计算机、手机中存储的信息内容方面的证据为主。

# 电子证据在传统刑事案件现场勘查中的扩张

## 扩张之后



## 智能扫地机器人

# 电子证据在传统刑事案件现场勘查中的扩张



## 扩张之后



- 环境地图
- 运行路线
- 清扫记录
- 耗材状态

现场与APP记录是否吻合

房间物品摆放的变化

计划外的清扫事件

房间地面历史洁净程度

## 智能扫地机器人

# 电子证据在传统刑事案件现场勘查中的扩张

## 扩张之后



余额：180分钟

# 电子证据在传统刑事案件现场勘查中的扩张



## 扩张之后



➤ 指令记录

操作痕迹

➤ 运行记录

无法识别的指令

➤ 语音数据

历史语音、环境声音

智能音箱

# 电子证据在交通事故勘查和鉴定中的扩张

现在



现场及车辆痕迹物证



交通视频监控



目击证人



行车记录仪

来电或去电	通话时间	通话时长	通话号码
呼入电话	2017-03-24 21:08:15	25秒	1867
呼出电话	2017-03-23 19:34:15	0秒	1364
呼入电话	2017-03-23 18:05:20	62秒	155
呼出电话	2017-03-23 05:14:05	0秒	130
呼出电话	2017-03-22 16:56:04	30秒	186
呼出电话	2017-03-22 16:55:49	0秒	155
呼出电话	2017-03-21 18:45:30	0秒	159
呼入电话	2017-03-21 14:16:16	55秒	155
呼入电话	2017-03-21 14:02:44	127秒	184
呼入电话	2017-03-21 08:39:43	35秒	186
呼入电话	2017-03-21 08:37:43	23秒	186
呼出电话	2017-03-21 08:36:32	0秒	186
呼出电话	2017-03-21 08:29:55	0秒	186
呼出电话	2017-03-21 08:28:23	0秒	155

手机通话记录

# 电子证据在交通事故勘查和鉴定中的扩张

## 扩张之后



汽车大脑

ECU



车载影音系统



手机APP信息

## 汽车数据

# 电子证据在交通事故勘查和鉴定中的扩张

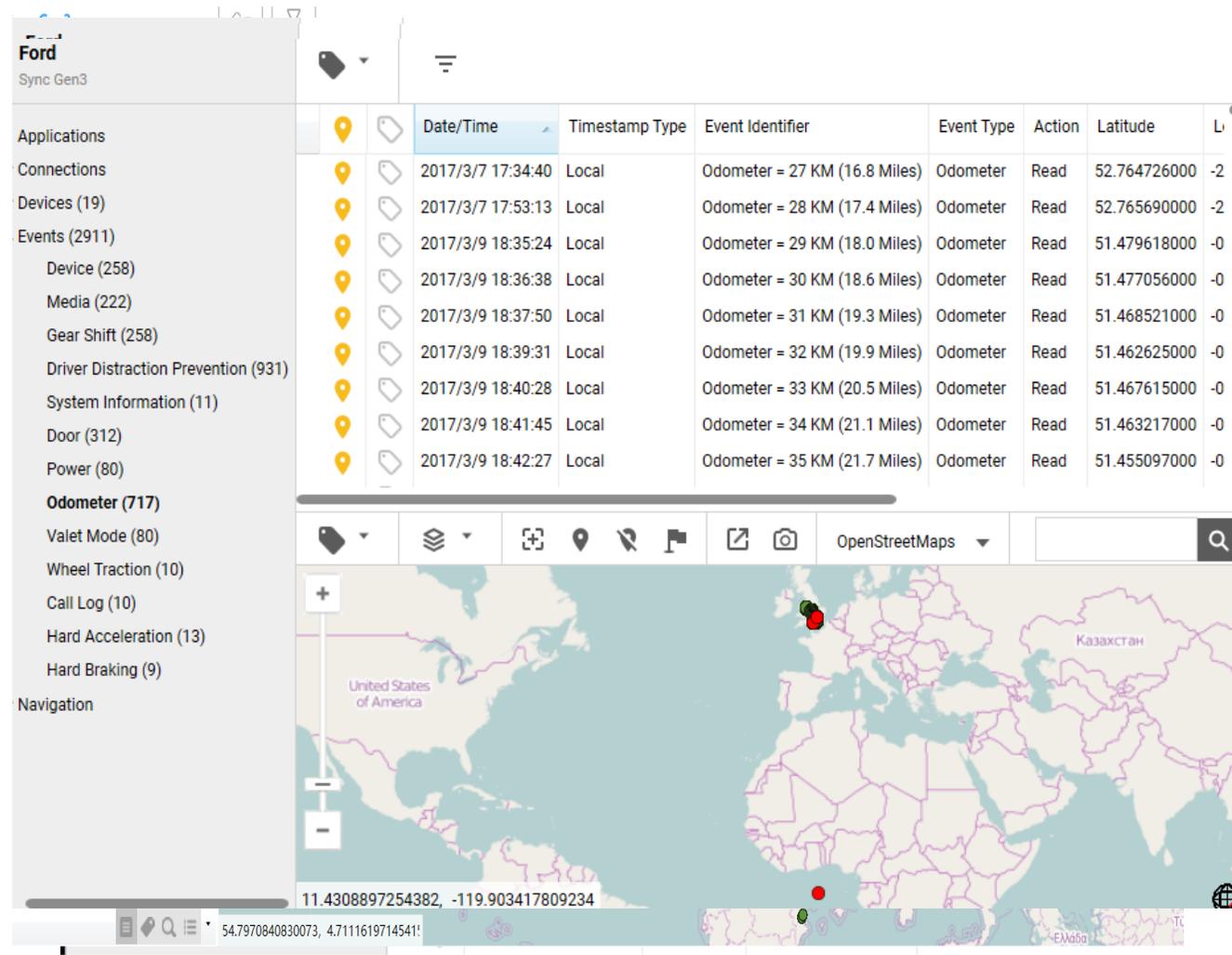
## 扩张之后



汽车大脑

ECU

- 车辆信息
- 电源开关记录
- 车门开关记录
- 急加速记录
- 急刹车记录
- 速度记录
- 里程记录



The screenshot shows a software interface for analyzing vehicle data. On the left, a sidebar lists various data categories for a 'Ford Sync Gen3' device, including Applications, Connections, Devices (19), Events (2911), and Navigation. The 'Events' section is expanded, showing a list of 10 events. The main area displays a table of these events, with columns for Date/Time, Timestamp Type, Event Identifier, Event Type, Action, and Latitude. Below the table is a map showing the geographic locations of the events, with a red pin indicating a specific location in the United States.

Date/Time	Timestamp Type	Event Identifier	Event Type	Action	Latitude
2017/3/7 17:34:40	Local	Odometer = 27 KM (16.8 Miles)	Odometer	Read	52.764726000
2017/3/7 17:53:13	Local	Odometer = 28 KM (17.4 Miles)	Odometer	Read	52.765690000
2017/3/9 18:35:24	Local	Odometer = 29 KM (18.0 Miles)	Odometer	Read	51.479618000
2017/3/9 18:36:38	Local	Odometer = 30 KM (18.6 Miles)	Odometer	Read	51.477056000
2017/3/9 18:37:50	Local	Odometer = 31 KM (19.3 Miles)	Odometer	Read	51.468521000
2017/3/9 18:39:31	Local	Odometer = 32 KM (19.9 Miles)	Odometer	Read	51.462625000
2017/3/9 18:40:28	Local	Odometer = 33 KM (20.5 Miles)	Odometer	Read	51.467615000
2017/3/9 18:41:45	Local	Odometer = 34 KM (21.1 Miles)	Odometer	Read	51.463217000
2017/3/9 18:42:27	Local	Odometer = 35 KM (21.7 Miles)	Odometer	Read	51.455097000

汽车数据

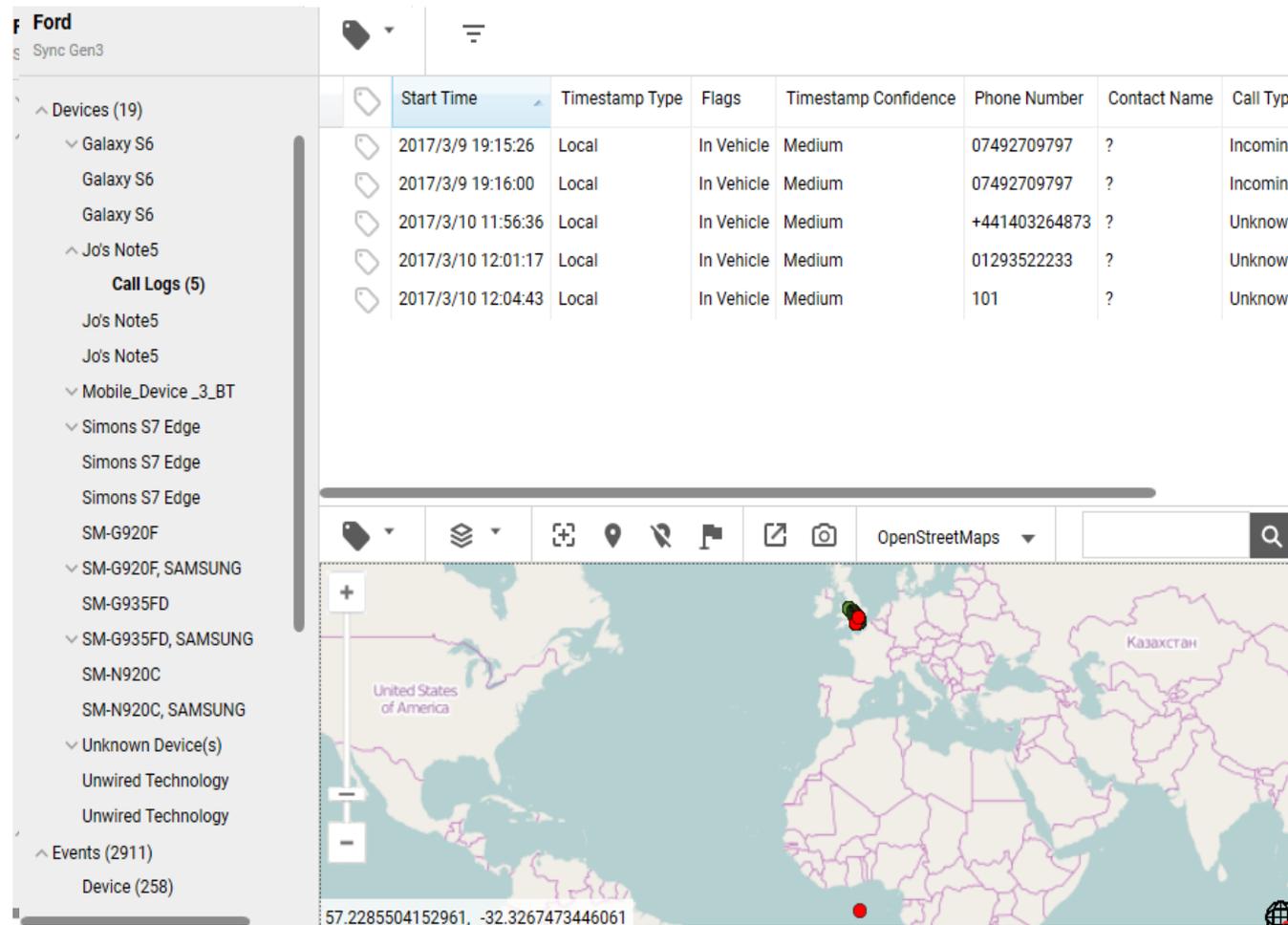
# 电子证据在交通事故勘查和鉴定中的扩张

## 扩张之后



车载影音系统

- 蓝牙连接记录
- 导航记录
- 车载通话记录
- 操作日志



**Ford**  
Sync Gen3

Devices (19)

- Galaxy S6
- Galaxy S6
- Galaxy S6
- Jo's Note5
- Call Logs (5)
- Jo's Note5
- Jo's Note5
- Mobile\_Device\_3\_BT
- Simons S7 Edge
- Simons S7 Edge
- Simons S7 Edge
- SM-G920F
- SM-G920F, SAMSUNG
- SM-G935FD
- SM-G935FD, SAMSUNG
- SM-N920C
- SM-N920C, SAMSUNG
- Unknown Device(s)
- Unwired Technology
- Unwired Technology

Events (2911)  
Device (258)

Start Time	Timestamp Type	Flags	Timestamp Confidence	Phone Number	Contact Name	Call Type
2017/3/9 19:15:26	Local	In Vehicle	Medium	07492709797	?	Incoming
2017/3/9 19:16:00	Local	In Vehicle	Medium	07492709797	?	Incoming
2017/3/10 11:56:36	Local	In Vehicle	Medium	+441403264873	?	Unknown
2017/3/10 12:01:17	Local	In Vehicle	Medium	01293522233	?	Unknown
2017/3/10 12:04:43	Local	In Vehicle	Medium	101	?	Unknown

OpenStreetMaps

57.2285504152961, -32.3267473446061

汽车数据

# 电子证据在交通事故勘查和鉴定中的扩张



## 扩张之后



**手机APP**

➤ **各种APP的登录、搜索、  
联络等记录**

**机主使用APP的时间和操作**

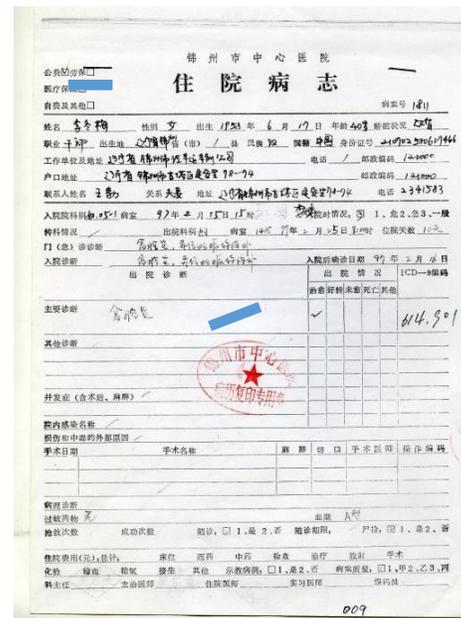
**汽车数据**

# 电子证据在医疗纠纷中的扩张

现在



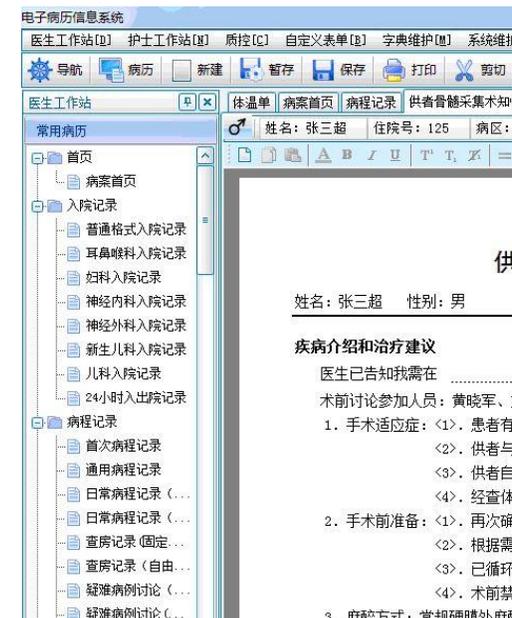
监控视频



郑州市中心医院  
住院病志

姓名: 李冬梅 性别: 女 出生: 1972年6月12日 年龄: 40岁 职业: 教师  
职业: 教师 工作单位: 郑州市教育局 身份证号: 410222197206121444  
工作单位: 郑州市教育局 电话: / 邮编: / 户口地址: 郑州市金水区东大街10-7号 邮政编码: 450002  
联系人姓名: 李冬梅 关系: 家属 地址: 郑州市金水区东大街10-7号 电话: 2341583

入院科别: 妇产科 入院日期: 97年2月15日 出院日期: 97年2月15日 住院天数: 1天  
入院原因: 产妇产前检查 入院时情况: 1. 胎位: 头位 2. 胎心: 140次/分 3. 宫高: 28cm 4. 腹围: 90cm  
主要诊断: 孕38周 胎位: 头位 胎心: 140次/分 宫高: 28cm 腹围: 90cm  
其他诊断: /  
并发症(含术后、麻醉): /  
院内感染名称: /  
手术日期: / 手术名称: / 手术部位: / 手术医师: / 操作医师: /  
病历记录: /  
病程记录: /  
首次病程记录: /  
通用病程记录: /  
日常病程记录: /  
查房记录(固定): /  
查房记录(自由): /  
疑难病例讨论: /  
009



电子病历信息系统

医生工作站 [X] 护士工作站 [X] 质控 [X] 自定义表单 [X] 字典维护 [X] 系统维护 [X]

导航 病历 新建 保存 打印 剪切

常用病历

- 首页
- 病案首页
- 入院记录
  - 普通格式入院记录
  - 耳鼻喉科入院记录
  - 妇科入院记录
  - 神经内科入院记录
  - 神经外科入院记录
  - 新生儿科入院记录
  - 儿科入院记录
- 24小时出院记录
- 病程记录
  - 首次病程记录
  - 通用病程记录
  - 日常病程记录
  - 日常病程记录
  - 查房记录(固定)
  - 查房记录(自由)
  - 疑难病例讨论
  - 疑难病例讨论

姓名: 张三超 住院号: 125 病区: /

疾病介绍和治疗建议

医生已告知我需在 .....

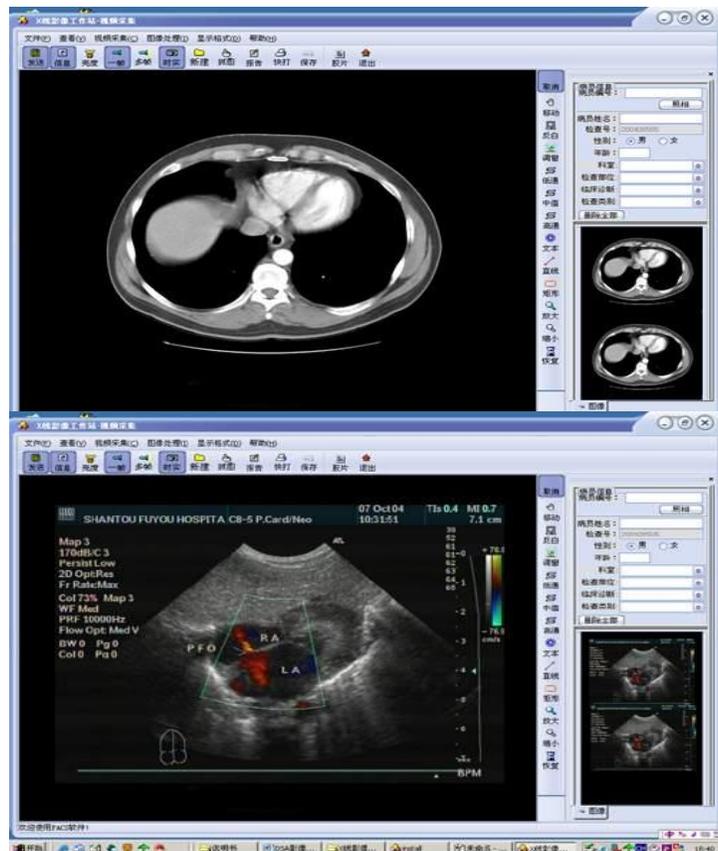
术前讨论参加人员: 黄晓军、刘

- 手术适应症: <1> 患者有接 <2> 供者与患 <3> 供者自愿 <4> 经遗体无
- 手术前准备: <1> 再次确认 <2> 根据需要 <3> 已循环采 <4> 术前禁食
- 麻醉方式: 常规硬膜外麻醉

病历

# 电子证据在医疗纠纷中的扩张

## 扩张之后



- 医疗设备信息
- 历史影像
- 影像设备参数

## 影像工作站数据

# 电子证据在医疗纠纷中的扩张

## 扩张之后



- 医疗设备信息
- 呼吸、监护等设备的日志数据
- 麻醉记录

**麻醉工作站数据**

# 电子证据在灾害事故中的扩张

现在



灾害事故现场勘查



现场电子设备

# 电子证据在灾害事故中的扩张

## 扩张之后



- 传感器记录的数据
- 后台或者云端记录的数据

**各种具有传感器和远程信息记录的设备**

# PART FOUR

## 机遇与挑战

# 挑战



- 识别
- 搜集
- 意识

人员

- 提取固定标准
- 分析鉴定标准

标准

- 提取固定
- 分析判断
- 量值溯源

技术

技术领域更加广泛，技术标准尚未建立，人员素质有待提升。

# 机遇



- **丰富的线索和证据**
- **侦查办案更加多元化**

**一切有电子数据的地方，都是侦查取证人员战斗的阵地。**

# 电子证据将成为未来的 **证据之王**

**CONTACT ME**



**邮箱: hbhanmajian@163.com**



THANKS FOR YOUR WATCHING