CHINA COMPUTER
FORENSICS CONFERENCE

现场勘验的难点与解决方案

晓光

第十四届CCFC计算机取证技术峰会

The 14th China Computer Forensic Conference

摘 要

了解规范，认识规范，遵守规范

各种现勘技术难点

- 计算机
- 手机
- 复印机
- 路由器
- 赌博机
- 远勘
- …

PART
ONE

了解规范，认识规范

了解规范

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》

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要求及检测方法》
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》
GA/T 825-2009 《电子物证数据搜索检验技术规范》（已废止）
GA/T 826-2009 《电子物证数据恢复检验技术规范》（已废止）
GA/T 827-2009 《电子物证文件一致性检验技术规范》（已废止）
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》
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[illegible]法》
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》
GA/T 1170-2014 《移动终端取证检验方法》
GA/T 1171-2014 《芯片相似性比对检验方法》
GA/T 1172-2014 《电子邮件检验技术方法》
GA/T 1173-2014 《即时通讯记录检验技术方法》
GA/T 1174-2014 《电子证据数据现场获取通用方法》
GA/T 1175-2014 《软件相似性检验技术方法》
GA/T 1176-2014 《网页浏览器历史数据检验技术方法》

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 《软件相似性鉴定实施规范》
SF/Z JD0400002-2015 《电子数据证据现场获取通用规范》
SF/Z JD0401002-2015 《手机电子数据提取操作规范》
SF/Z JD0402002-2015 《数据库数据真实性鉴定规范》
SF/Z JD0402003-2015 《即时通讯记录检验操作规范》
SF/Z JD0403002-2015 《破坏性程序检验操作规范》
SF/Z JD0403003-2015 《计算机系统用户操作行为检验规范》

[无标题]

数据安全与取证

认识规范


ICS 35.240.01
A 92

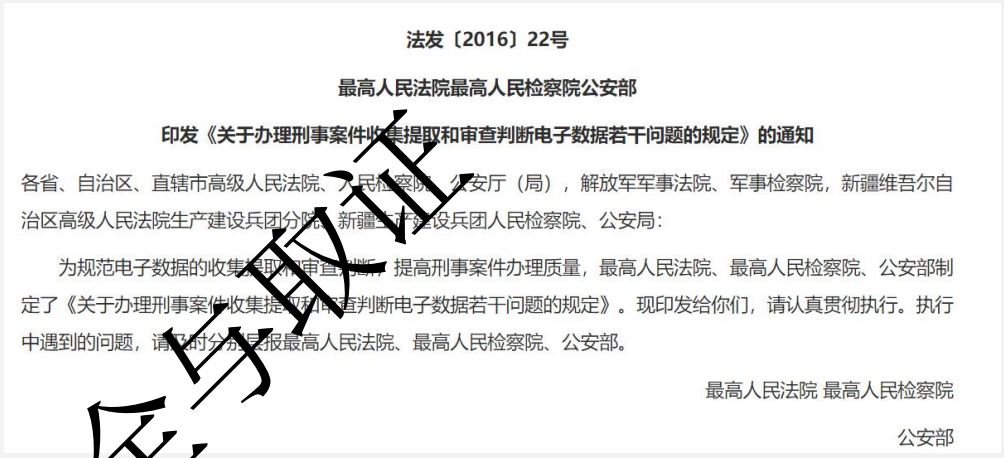
GA

中华人民共和国公共安全行业标准

GA/T 1174—2014

电子证据数据现场获取通用方法

General methods for capture of live electronic evidence data


法发〔2016〕22号

最高人民法院最高人民检察院公安部

印发《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》的通知

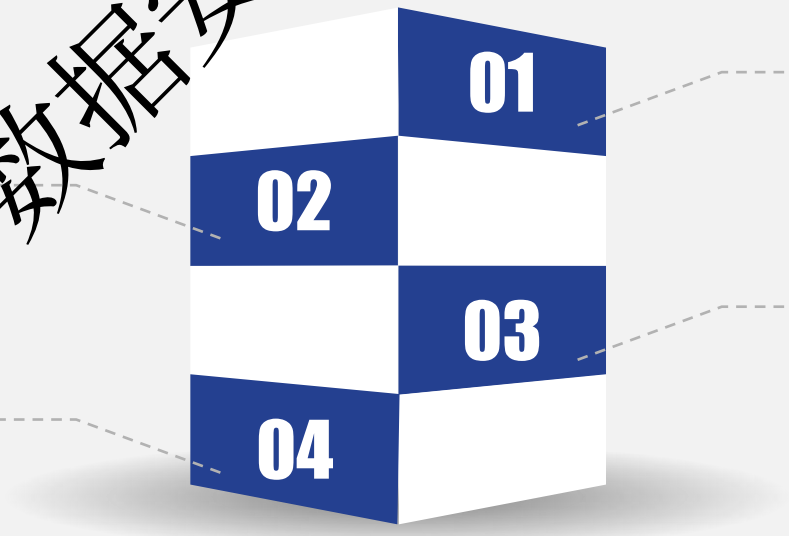
各省、自治区、直辖市高级人民法院、人民检察院、公安厅（局），解放军军事法院、军事检察院，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，最高人民法院、最高人民检察院、公安部制定了《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》。现印发给你们，请认真贯彻执行。执行中遇到的问题，请及时分别报最高人民法院、最高人民检察院、公安部。

最高人民法院 最高人民检察院

公安部

数据安全与取证



事前计划

事中记录

封存

其他细节

PART
TWO

数据安全与取证

遵守规范

不规范的例子

快播案

辩方就这四台服务器的查扣、保管和移交程序提出的质疑主要包括：

（1）海淀文委查扣服务器时“未对物证特征进行固定”。既没有记载内置硬盘的型号、数量、容量，也没有对扣押物品拍照。

（2）服务器被扣押期间的保管状况不明。自被海淀文委扣押到被公安机关调取的近五个月内，服务器历经文创公司——海淀文委——北京市版权局——文创公司——公安机关四次移转。且服务器由文创公司保管的期间，行政执法机关没有也不可能进行全程监督，服务器存在被偷换的可能。

（3）移交服务器的手续违法。海淀公安分局调取服务器时，制作的调取证据通知书上“2014”的“4”字是由打印的“5”字涂改而来。

（4）公安机关调取服务器后，依然没有登记服务器的特征、型号与内置硬盘的型号、数量、容量，也没有对扣押物品拍照。

（5）在公诉机关出示的不同份鉴定意见中，关于服务器内硬盘的数量及容量的表述存在不一致。

不只是规范

以验证，并出具相应检验报告书。

对于上述证据保全方式，本院认为，首先，上述证据保全方式在技术可信度上尚缺乏权威、有效的验证，不能当然排除整个过程存在数据被篡改的可能。其次，与公证机构的公证行为相比，鉴定机构对客观事实的保全和见证行为并不具有预设的证明力。在专利复审委员会口审时，经查证涉案网页内容均已灭失，而中证鉴定中心在出具鉴定报告时并未实际登陆互联网对网页内容予以查证的情况下，仅凭鉴定报告尚不足以认定铭轩公司主张其保存的网页的真实性。该鉴定报

数据安全与取证

PART
THREE

数据安全与取证

不同的现勘场景

常规现勘

- 获取现场情况
- 工具准备
  - 只读锁（原始性）
  - 证据存储设备
  - 锁屏绕过
  - 易失性数据提取
  - 不拆机镜像工具
  - 手机快速提取工具
  - 信号屏蔽
  - 网线、路由（端口转发）（网络抓包）
  - 螺丝刀、物证袋、硬盘保护箱
  - 封条、标签
  - 录像机、相机（VGA记录仪）
  - 笔、纸、打印机
  - 监控视频下载工具
  - 充电宝（防止手机关机）
  - 带电移机
  - 防静电手套
  - 恶意木马检测
- 人员分工
- 方案设计

计算机开机状态（提取易失性数据）

- 现场操作
  - 使用现场勘查工具小工具提取易失性数据
  - 提取内存

- 工具准备
  - 锁屏绕过工具
  - 易失性数据提取程序（Nirsoft、FastIR、cofee等）
  - 内存提取程序（dumpIt等）

计算机开机状态（提取易失性数据）

- Netstat ， traceroute，ifconfig，alias，df，mount，ps等命令的结果使用管道>来保存到证据存储盘
- Linux的内存提取（lime）
- Mac内存提取

计算机开机状态（在线提取）

- 现场不提取会有数据缺失后果
  - 正在连接远程
  - 已经登录的网盘、云服务器
  - 全盘加密、加密容器
  - 特殊的软件

- 不允许关机扣押（如：大型网站服务器）

计算机开机状态（在线提取）

- 现场操作
  - 运行在线提取工具
  - 固定远程的计算机
  - 固定网盘数据
  - 固定云服务器数据
  - 固定已解密的分区
- 工具准备
  - 远勘设备
  - 网络拷贝工具
  - 多通道高速拷贝工具

计算机关机状态

- 现场操作
  - 直接封存
  - 拷贝固定（HASH）
  - 不拆机镜像
  - BIOS时间记录
- 工具准备
  - 封条等
  - 拷贝机、只读锁
  - 不拆机镜像工具

伪基站

现场操作

- 观察
- 固定数据

工具准备

- 拷贝机
- 在线提取工具
- 拆机工具

手机

- 现场操作
  - 屏蔽（双层/干扰）
  - 飞行模式
  - 断开与计算机的连接
  - 收集帮助破解密码的信息
- 工具准备
  - 屏蔽袋
  - 快速提取工具

复印机


硬盘位置


正常文件
零数或删除文件
作业日志
作业日志
复印/打印
扫描
打印机
本地打印
网络打印
打印服务
发送/接收
传真
存储
开关机日志

复印机

现场操作

现场提取复印机数据

封存拷贝复印机数据

工具准备

复印机提取工具

拷贝机

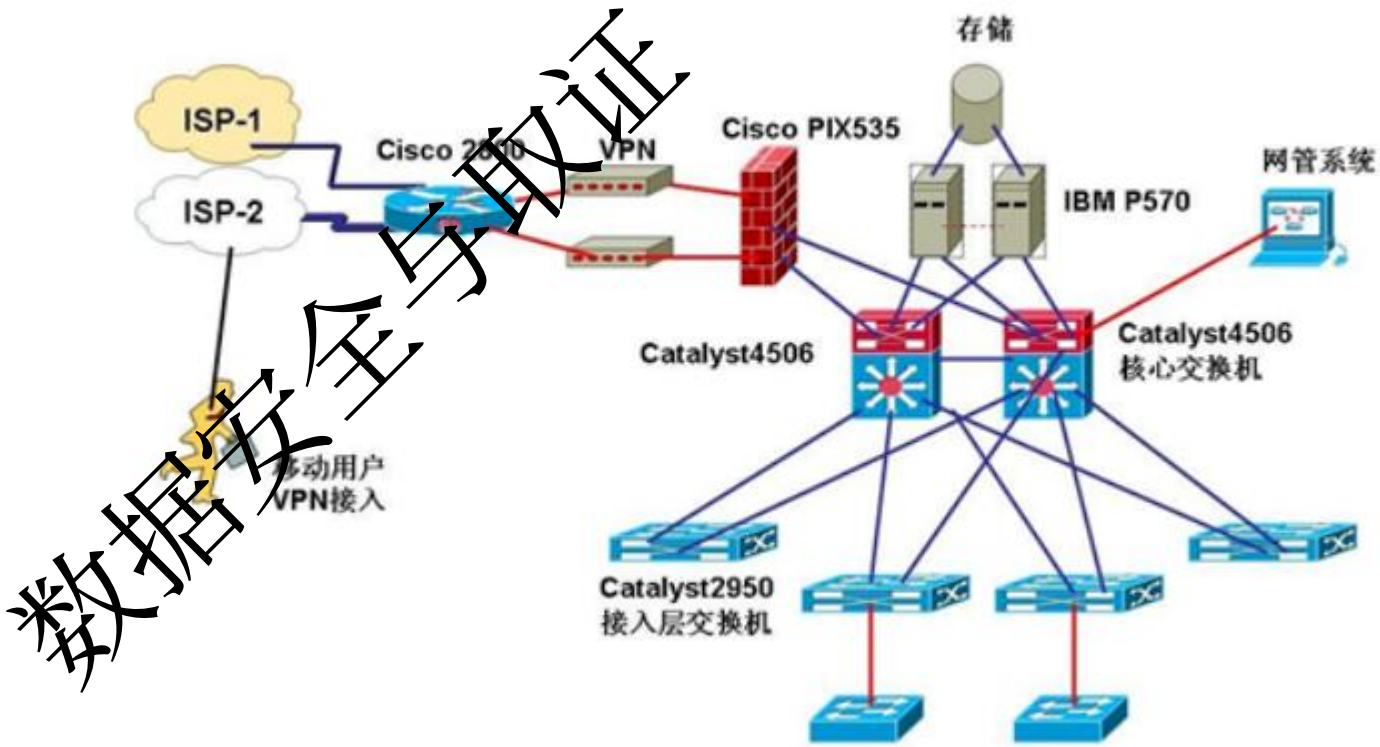
拆解工具

监控、行车记录仪

- 现场操作
  - 停止录制
  - 校对时间
  - 数据提取
  - 封存
- 工具准备
  - 视频提取专用设备
  - 拆机工具

网络入侵案件

- 现场操作
  - 抓包
  - 木马检测
  - 进程分析
  - 二进制分析
  - 提取相关数据
- 工具准备
  - 网络数据固定工具
  - 木马检测工具
  - 二进制分析工具
  - 网络拓扑分析工具



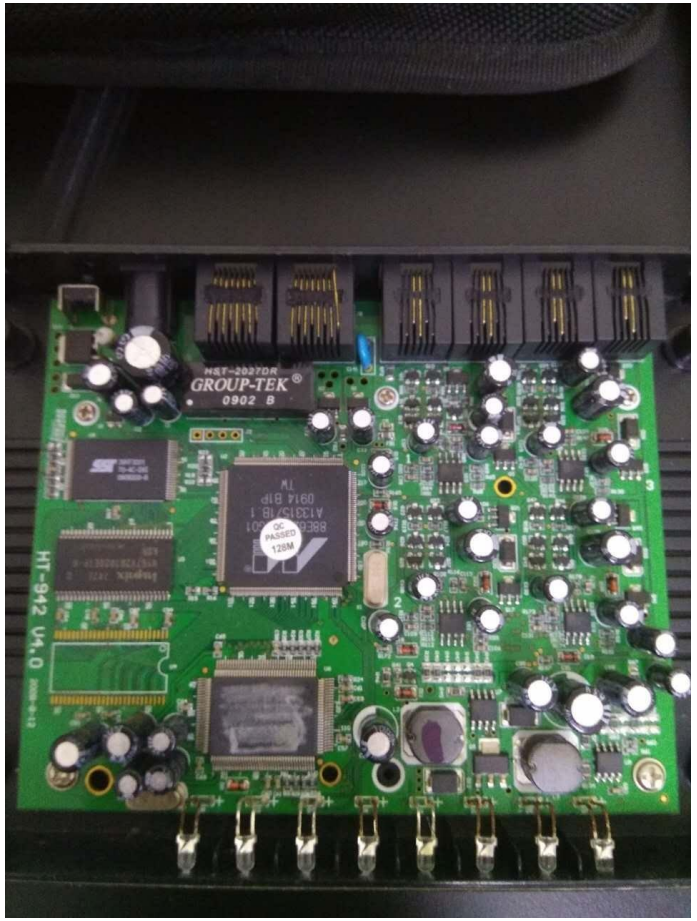
路由器

现场操作

- 下载日志
- 封存设备

工具准备

- 勘查工作站
- 封条



本页显示路由器的系统日志。用户可以分类、分级查看其中部分日志，并且可以保存日志内容或将日志内容通过邮件发送。

通过邮件定时发送日志功能： 未启用 邮件发送设置

选择要查看的日志类型： 全部 选择要查看的日志等级： ALL

索引	时间	类型	级别	日 志 内 容
205	Sep 23 13:34:49	DHCP	INFO	DHCPS:Send ACK to 192.168.1.102
204	Sep 23 13:34:49	DHCP	INFO	DHCPS:Recv REQUEST from 10:02:B5:54:A8:3F
203	Sep 23 13:00:45	DHCP	INFO	DHCPS:Send ACK to 192.168.1.103
202	Sep 23 13:00:45	DHCP	INFO	DHCPS:Recv REQUEST from 48:A1:95:40:BE:6E
201	Sep 23 12:47:32	DHCP	INFO	DHCPS:Send ACK to 192.168.1.100
200	Sep 23 12:47:32	DHCP	INFO	DHCPS:Recv REQUEST from 6C:19:C0:50:BB:81
199	Sep 23 12:34:48	DHCP	INFO	DHCPS:Send ACK to 192.168.1.102
198	Sep 23 12:34:48	DHCP	INFO	DHCPS:Recv REQUEST from 10:02:B5:54:A8:3F
197	Sep 23 11:58:04	DHCP	INFO	DHCPS:Send ACK to 192.168.1.103
196	Sep 23 11:58:04	DHCP	INFO	DHCPS:Recv REQUEST from 48:A1:95:40:BE:6E
195	Sep 23 11:45:31	DHCP	INFO	DHCPS:Send ACK to 192.168.1.100

完整提取各种设备

- 旧硬盘
- 私有云（Airport Time capsule、群晖）
- 各种物联网设备
- 小SD卡
- 小芯片（佩戴静电手环）
- U盘（各种形状）
- 密码记录本

- 附属设备：
  - 电源适配器
  - 读取设备及线缆
  - 特殊设备说明书

CFC
CHINA COMPUTER
FORENSICS CONFERENCE

数据安全与取证

特殊硬盘的处理

现场操作

- 需要原设备直接导出，
- 提取原盘回来重组，字节转换
- 故障盘及时断电


```
turbo on
Assign FileSize  GetSize
//ASSign Pagecount  ((FileSize%10) - 1)
ASSign Pagecount 10
goto 0
read MyVariable 512
Create "D:\copy512.img" 0
write MyVariable
{
    nextobj
    move 8
    read MyVariable 512
    nextobj
    write MyVariable
}[Pagecount]
save
MessageBox "完成"
turbo off
```

Surface的处理

- 难点
  - 安全启动
  - Bitlocker TPM加密

- 现场操作：
  - 使用Surface取证专业工具进行数据提取

- 工具准备
  - Surface取证专业工具

赌博机

现场操作：

封存赌博机

获取控制器、打码器

控制器

打码器

无人机

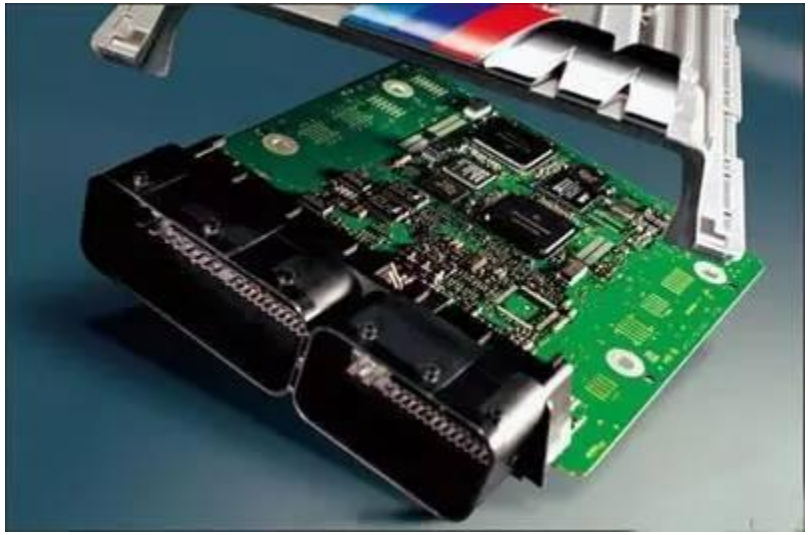
无人机的获取

- 信号干扰
- 武力抓取

无人机数据的提取

- 数据线
- 芯片

汽车

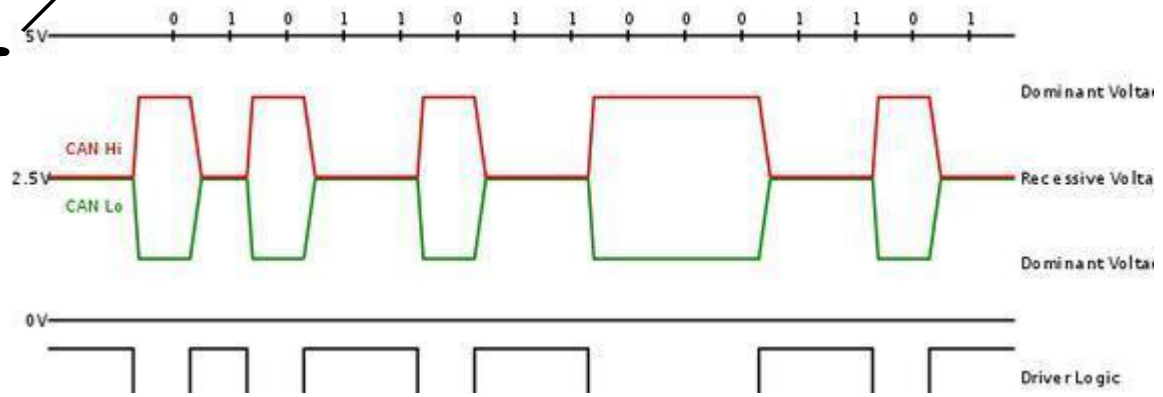


现场操作

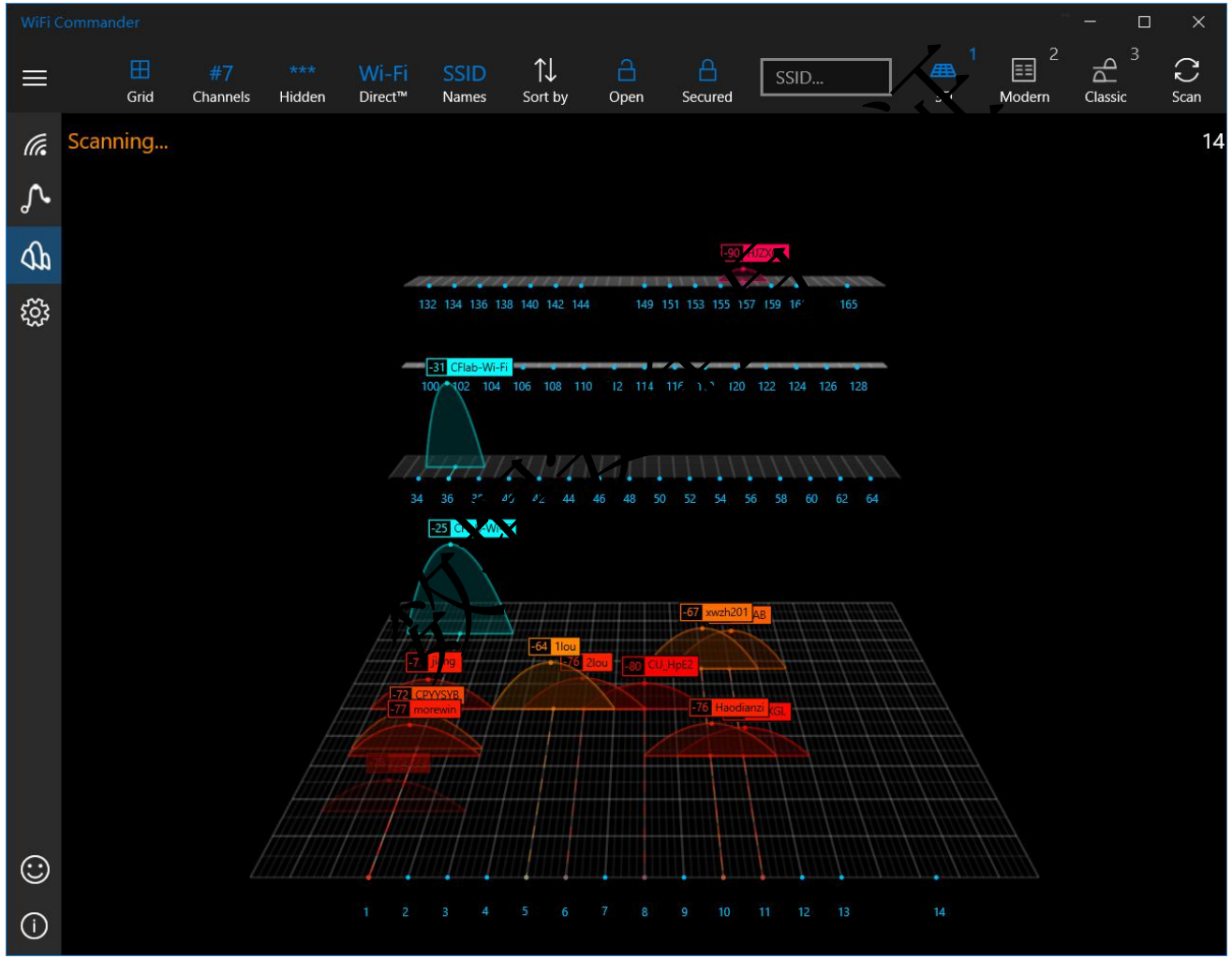
- 提取ECU数据
- 提取娱乐系统数据

工具准备

- 汽车取证设备



无线信号信息


WiFi Commander
Grid
#7
Channels
***
Hidden
Wi-Fi
Direct™
SSID
Names
Sort by
Open
Secured
SSID...
Modern
Classic
Scan
Scanning...
14
-31 CFlab-Wi-Fi
-67 xwzh201
-64 1lou
-76 2lou
-80 CU_Hpf2
-72 CPYYSYB
-77 morewin
-76 Haodianzi
1 2 3 4 5 6 7 8 9 10 11 12 13 14

远程勘验

- 操作：
  - 记录
  - 时间校对
  - 路由信息
  - 录像
  - 提取数据
- 工具
  - 远勘工具
  - 远程桌面
  - 网络环境

展望

全景相机

远程控制硬件

THANKS FOR YOUR WATCHING