

手机取证的新问题和新发展

孙奕

CFE/EnCE/ACE

美亚柏科信息股份有限公司

2016-7-14

1 当前手机取证工作所面临的问题

3 新的解决方案

2 新问题的新对策

4 Q&A

目录

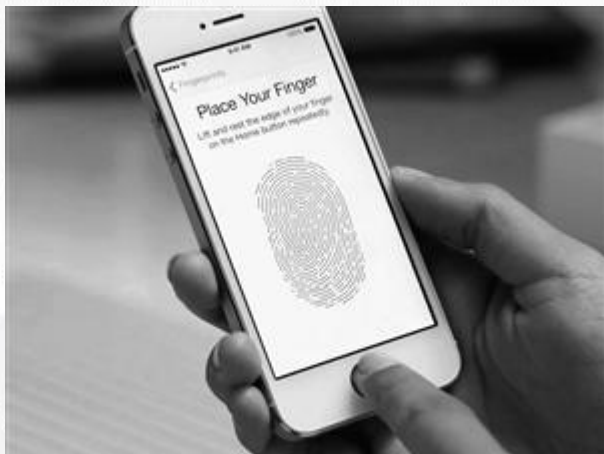
contents

“

这是最好的时代，也是最坏的时代.....

——狄更斯

”



安全意识

厂商与用户的安全意识不断提高，不断产生的新的保护措施和加密技术手段

容量倍增

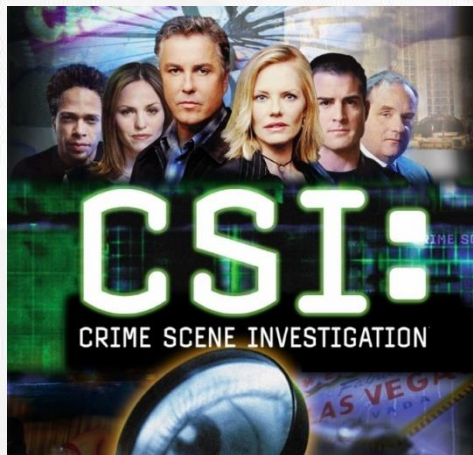
手机存储容量日益增大，取证平均耗时大大增加

手机App

移动应用快速更新，部分程序增加了反取证措施

工作模式转变

从“怎么取”逐渐转换为“怎么看”和“怎么用”



外行眼中的我们



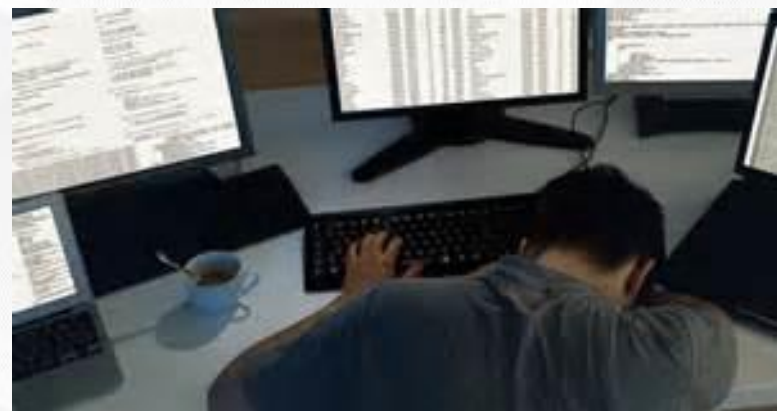
亲友眼中的我们



领导眼中的我们



我们想象中的自己



实际工作中的自己



iOS	Android
高版本有密码	有密码未开调试
iTunes备份加密	高版本root问题
应用程序数据加密	BL锁
删除文件恢复	应用程序备份限制
删除应用程序恢复	应用程序删除填充
损坏、被破坏手机的取证	
.....	

- ◎ 当前市场智能手机容量不断增加，目前主流机型起步容量基本都在16GB-32GB，64GB、128GB容量机型也屡见不鲜
- ◎ 应用程序，尤其是社交类应用程序使用频繁，本地数据量较大，在手机取证解析过程中占据了多数时间

■ 解决思路：

- 1. 目前智能手机应用程序数据主要采用备份方式完成，通过技术手段根据取证内容，选择性备份数据，从而缩短备份和解析时间。
- 2. 在应用程序解析部分引入多线程并行解析，充分利用计算机运算资源，提高解析效率。


- 通过排除多媒体文件备份的方式，iPhone手机备份时间大大缩短，实际测试中，最高速度提升54%
- 引入应用程序多线程解析后，解析速度也有所提升，其中IOS速度提升较为明显。

	单线程解析	多线程解析
iPhone 6 w/ iOS 8.4 JB	4分16秒	2分52秒
iPhone 5c w/ iOS 9.1	4分17秒	3分36秒
华为荣耀6 Android 4.4 root	6分38秒	6分04秒
小米4s Android 5.1.1	13分45秒	12分35秒

◎ Android 6.0版本下，目前微信无法通过备份方式获取导致微信提取结果为 0。

■ 解决思路：

- 1. 利用厂商自带备份工具，将手机数据备份，随后将厂商备份数据转换为可解析格式后，进行数据提取和分析。
- 2. 少数非原生Android 6.0手机，通过提取root权限方式取得应用程序数据。



中国移动 0K/s 19:38

证据列表 搜索结果

20160627

- HuaWeiAppBackup(167)
 - 手机信息(11)
 - 即时通讯(156)
 - 微信(156)
 - wxid_8qsnw9gtg6qz12-FL
 - 帐号资料(1)
 - 通讯录(23)
 - 聊天记录(115)
 - 公众号(94)
 - 好友列表(21)
 - 朋友圈(17)

Storage
ackupir
stemC:

2016-06-27_19-39-16

Android备

步骤1：选择备
App备份

步骤2：选择需
C:\Users

步骤3：选择转
C:\Users

进度：

设置

◎ Android 4.x以及5.x版本下，部分应用程序限制了自身的备份，如腾讯QQ、微信、WhatsApp等。

■ 解决思路：

- 1. 首先将手机中的应用程序替换为旧版本。
- 2. 通过支持备份的旧版本进行备份。
- 3. 取证完成后，替换为原始版本。

■ 潜在问题：证据有效性问题、系统安全机制问题、数据完整性问题

◎ Android 4.x以及5.x版本下，部分应用程序限制了自身的备份，如腾讯QQ、微信、WhatsApp等。

■ 解决思路：

- 1. 找到iOS设备使用者对应的计算机，将Lockdown文件拷贝并移动至取证计算机，以实现无密码建立信任关系。
- 2. 使用芯片替换的方法突破iOS的密码尝试次数限制，目前POC阶段。



Lockdown文件位置：

C:\ProgramData\Apple\Lockdown

1

• 吹下iPhone Flash芯片，并使用复制设备制作副本；

2

• 将副本使用测试架桥接至iPhone主板，开机；

3

• 穷举密码，5-10次为一轮；

4

• 如触发长时间锁定或触发数据抹除，则更换副本；

5

• 重复上述步骤，直至解锁。



新问题的新方法——Android高版本设置密码/无调试解决方案

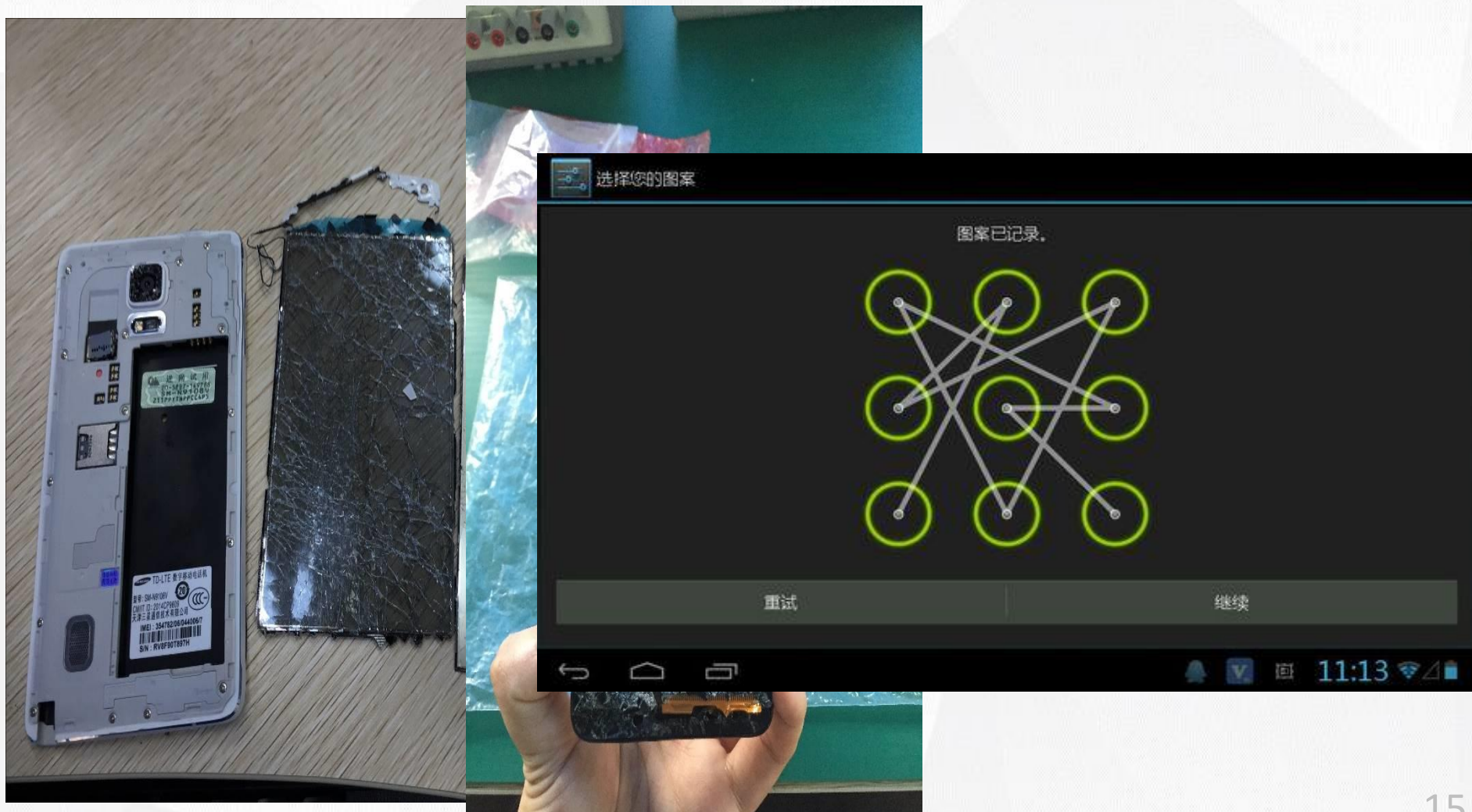
- ◎ 在Android 4.4以上，尤其是Android 5.x版本中，用户设置密码无法进入用户交互开始调试和允许调试。



■ 解决思路：

- 1. 在设备没有Bootloader锁定的情况下，通过刷入第三方Recovery程序实现备份（如TWRP）。
2. 针对有Bootloader锁定的，根据情况采用芯片级取证方案。

现有手机取证设备无法解决的问题



- ◎ 目前，手机芯片级解决方案主要适用于以下几种情况：
 1. 手机损坏，无法通过在线提取方式进行取证；
 2. Android手机设置密码，无法破解或者绕过的；
 3. 部分非智能手机无可用数据接口或通讯协议。



- ◎ 某单
将随



告，
居。

20160202 chipoff

证据

手机恢复

恢复结果概况 保存恢复结果 历史恢复记录

实体文件 应用程序 请输入文件名 高级搜索

全部结果 搜索结果

分类 目录 删除文件

- 所有结果(6989)
 - C:\Users\Admin\Desktop\
 - 图片(306)
 - 多媒体(432)
 - 网页(1)
 - 数据库文件(37)
 - 压缩文件(6)
 - 其他文件(1119)
 - 没有扩展(5088)

列表

<input type="checkbox"/>	序号	名称	恢复状态	创建时间	修改时间	访问时间
<input type="checkbox"/>	1	图片(306)				
<input type="checkbox"/>	2	多媒体(432)				
<input type="checkbox"/>	3	网页(1)				
<input type="checkbox"/>	4	数据库文件(37)				
<input type="checkbox"/>	5	压缩文件(6)				
<input type="checkbox"/>	6	其他文件(1119)				
<input type="checkbox"/>	7	没有扩展(5088)				

导出选中文件 导出选中列表

摘要 预览 文本 十六进制

深度恢复

检材信息：2016-02-02_16-57-44_User Area TJ.dd 8.00 GB 快速MD5：15F249417A9B7D053833FD39ADD2EF22 更多

新的解决方案：Android手机仿真取证 解决方案

- ◎ 当前安卓手机取证的短板：
 - 支付宝等应用程序，数据在本地缓存较少
 - 微信红包需联网查看
 - 损坏手机取证不直观
 - 部分恶意程序调查需要截图取证与通讯抓包

.....



取证结果Reader - 飞信案件

打开案件 搜索证据 通知消息过滤 合并删除数据 数据排重 生成证据报告 生成标签报告

证据列表 标签结果 搜索结果

请输入过滤内容

手机信息(4727)

即时通讯(13069)

腾讯QQ(2681)

- 2263823425-绝对可怜(147)
- 账号信息(1)
- 关联账号(2)
- 好友列表(29)
- 群列表(17)
- 群成员(640)
- 讨论组列表(47)
- 搜索记录(4)
- 聊天记录(737)
 - 好友聊天记录(30)
 - 群聊天记录(637)
 - 讨论组聊天记录(29)
 - 临时会话(37)
 - 系统消息(4)
- 2263823425-绝对可怜(删除)
- 2263823425-绝对可怜的小
- 2263823425-绝对可怜的小
- 2263823425-绝对可怜(轻聊)
- 2263823425-绝对可怜(轻聊)

103409254-淘宝天猫交流群(98)

105997680-安梦瑶(18)

166602666-彩虹桥VPN(64)

174415435-平面设计(60)

199409867-奔跑的小马驹(10)

250982193-绝对可怜的孩子(32)

263196146-Black Bob(1)

292526347(42)

313250377(36)

314868233-SUC.交流群(270)

90514669-扬帆淘宝特价购物005群

绝对可怜 (2263823425)

好像

2015-07-25 13:55:11

AI (1091550465)

这什么

2015-07-25 14:29:53

AI (1091550465)

【天上真的掉馅饼了哈~贝莉雅黛嘉文丽防晒霜~享受美丽~免费试用】淘口令¥AAAHHtLS¥..长按复制这条信息,打开手机淘宝即可看到..,注:请更新至最新版的手机淘宝哟!!

2015-07-31 18:24:52

AI (1091550465)

去申请啊,我们做活动送十瓶防晒霜

2015-07-31 18:25:09

加载中... (1321469927)

.....

2015-07-31 20:26:13

JC榕晨 (1991447323)

是不是哦

2015-08-01 20:34:12

当前页60条, 第1/1页

首页 上一页 下一页 尾页

◎ 路将越走越窄，日子会越来越难

Android 6.0原生设备，全盘加密

更多的BL锁定

App加密

App数据抹除、阅后即焚

云端存储

新兴系统（YunOS）

移动支付相关信息和安全保护

Q & A

手机取证的新问题和新发展



谢谢