CCFC 2019

移动取证和云取证

Vladimir Katalov, ElcomSoft


为什么进行云取证？
账户秘密和令牌
Web和应用程序密码
消息(包括短信)
健康数据(Apple Health，谷歌Fit)
支付数据(Apple Pay)
通话记录
电子邮件和聊天
无线网络密码
文档、设置和数据库
网页浏览历史，标签，搜索
图片和视频
位置历史，路线和地点
Extract Data
DOWNLOADING...

苹果和iCloud

苹果公司收集、处理和存储个人信息

- iCloud 是苹果公司的云服务
- 苹果公司收集、存储和处理大量数据
- 在如何存储和保护不同类型的数据方面存在巨大的差异
- Physically, iCloud 服务器位于中国
- 苹果公司必须遵守中国司法管辖区法律实施的要求
- 然而…
- **苹果公司在向执法部门反馈信息时非常谨慎**

苹果和iCloud

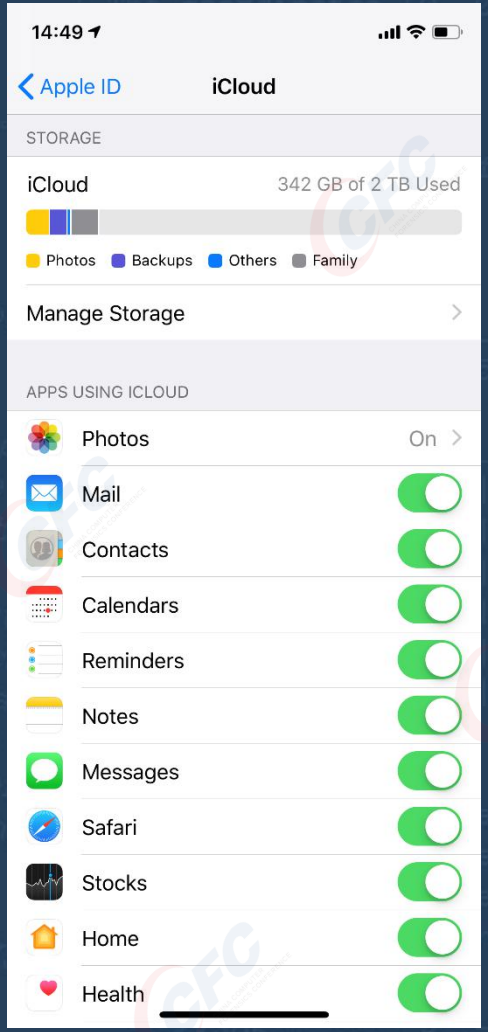
苹果 iCloud: 法律合规性和技术因素

- 虽然用户的数据存储在中国，但它是安全加密的
- 苹果公司仍然保留着加密密钥，并将其物理存储在加州Cupertino的美国数据中心
- **苹果公司在向执法部门反馈信息时非常谨慎**
- 为什么?
- 有些数据是用根本不存储的加密密钥来保护的
- 苹果公司在访问这类数据时涉及了技术限制
- 这并不完全正确

iCloud 数据

Checklist #1: iOS 设置

- 并不是所有的类别都被列出来了
  - 例如没有通话记录，邮件签名，黑名单，自校正字典
- 一些选项需要启用密钥链
  - 健康状态、消息
- “iCloud Drive”下的内容不明
  - 有些数据只能通过各自的应用程序访问，如WhatsApp和Viber 备份



iCloud 数据

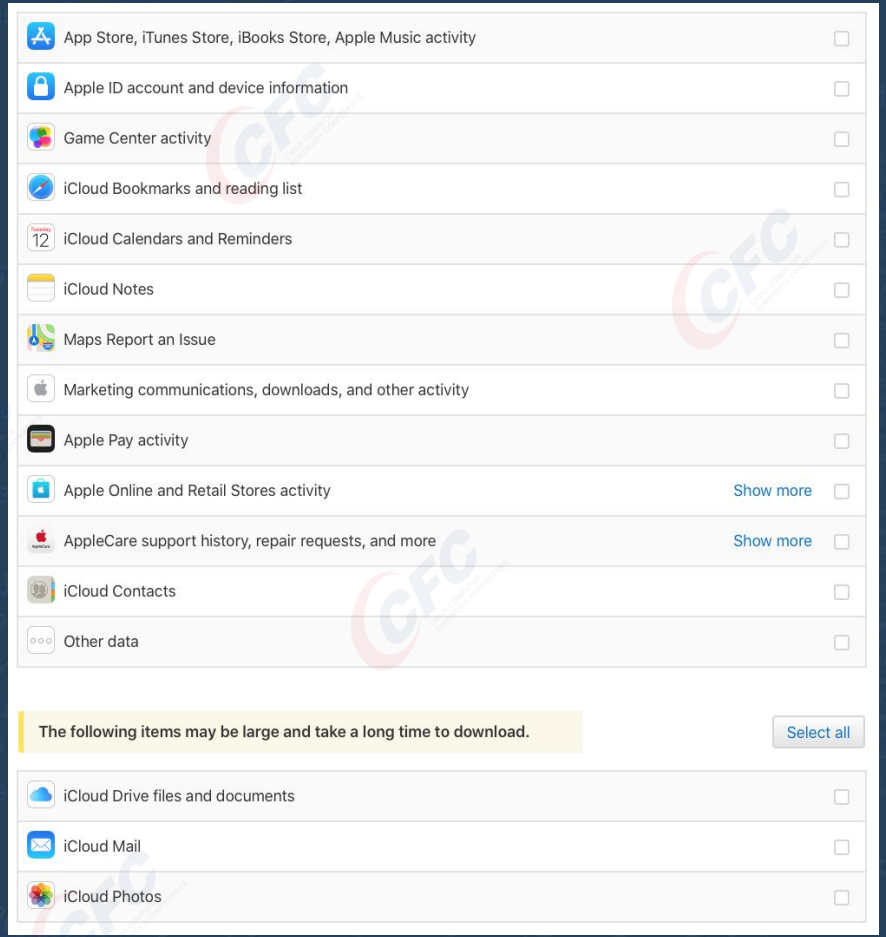
Checklist #2: icloud.com Web访问

- 只有基本的数据类别可以通过网络访问
- 立即通知帐户持有人(通过电子邮件)
- Web浏览器方法(令牌保存在cookie中)

iCloud 数据

Checklist #3: privacy.apple.com

- 目前只在欧洲、美国和其他很少的国家有售
- 准备数据大约需要一个星期
- 多种不同的数据格式(txt, csv, xml, json)
- 这里有一些苹果公司的“内部”数据(其他方式无法获得)
- 最有趣的是隐藏在*其他数据*之下



iCloud 安全

Checklist #4: 政府请求

- apple.com/legal/transparency/cn.html
- 苹果公司公开了政府请求的统计信息
- **中国政府请求（2018年7月- 12月）**

Requests for Customer Data

Request Type ⊕	Requests Received ⊕	Identifiers Specified in Requests ⊕	Requests where Data Provided ⊕	Percentage of Requests where Data Provided ⊕
Device	689	137,595	660	96%
Financial Identifier	95	471	83	87%
Account	42	7,154	41	98%
Emergency	0	-	0	-

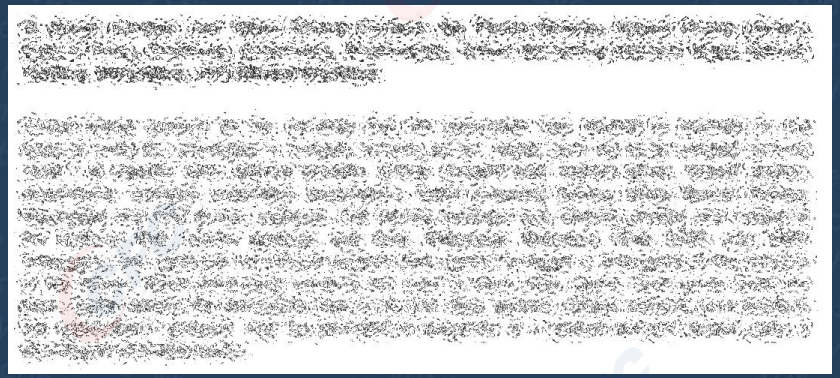
iCloud 安全

Checklist #4: 政府请求阐释

- 在6个月期间，只有689个设备请求
  - 设备请求意味着对与特定设备相关的客户数据的访问
  - 设备请求基于设备标识符，如Apple序列号、IMEI或MEID
- 然而，这些请求覆盖了大约137,595个苹果ID
- 200个不同的标识符被捆绑在一个请求中
- 苹果满足了96%的设备需求

iCloud 安全

Checklist #4: 政府请求



III. Information Available from Apple

A. Device Registration
B. Customer Service Records
C. iTunes
D. Apple Retail Store Transactions
E. Apple Online Store Purchases
F. Gift Cards
G. iCloud
H. Find My iPhone
I. Extracting Data from Passcode Locked iOS Devices
J. Other Available Device Information
K. Requests for Apple Retail Store CCTV Data
L. Game Center
M. iOS Device Activation
N. Sign-on Logs
O. My Apple ID and iForgot Logs
P. FaceTime
Q. iMessage

iCloud 安全

III. Information Available from Apple

iii. Email Content and Other iCloud Content. My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, Maps Search History, Messages, iOS Device Backups

iCloud stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include email, stored photos, documents, contacts, calendars, bookmarks, Safari browsing history, Maps Search History, Messages and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, Business Chat, SMS, and MMS messages and voicemail. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers. iCloud content, as it exists in the subscriber's account, may be provided in response to a search warrant issued upon a showing of probable cause.

Q. iMessage

iCloud 安全

Checklist #5: 分层保护

没有双重认证的帐户:

- iCloud备份
- 一些同步数据 (Safari历史和书签、联系人、笔记、语音备忘录等)
- 照片

- 你只需要输入苹果登录ID和密码

iCloud 安全

Checklist #5: 分层保护 – 2FA

具有双重身份验证的帐户:

- iCloud备份（附加保护）
- 一些同步数据（Safari历史和书签、联系人、笔记、语音备忘录等）
- 照片
- 苹果登录ID，密码，一次性代码;
- 存在着模式；2FA只是一个必要的先决条件

iCloud 安全

Checklist #5: 分层保护 – 2FA + 设备密码

设备屏幕锁定密码用于附加保护：

- 短信和苹果短信
- 健康活动(数据)
- 屏幕时间
- **用户密码(iCloud密钥链)**

- 苹果登录ID，密码，2FA代码和设备屏幕锁或系统密码(从任何登记的设备)需要访问
- 这些数据**无法**通过政府请求获得
- **不能**通过privacy.apple.com访问

iCloud 同步数据

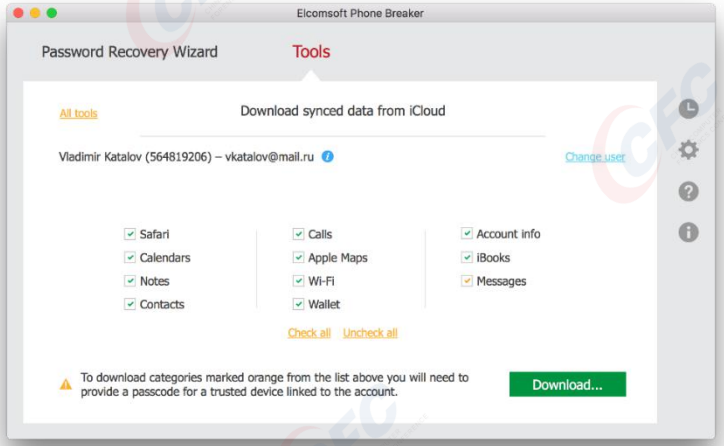
iCloud 同步数据

- 与使用设备备份相比，苹果同步越来越多的数据
- 备份：每个设备
- 同步数据：每个帐户，多个设备

iCloud 同步数据

同步是什么？

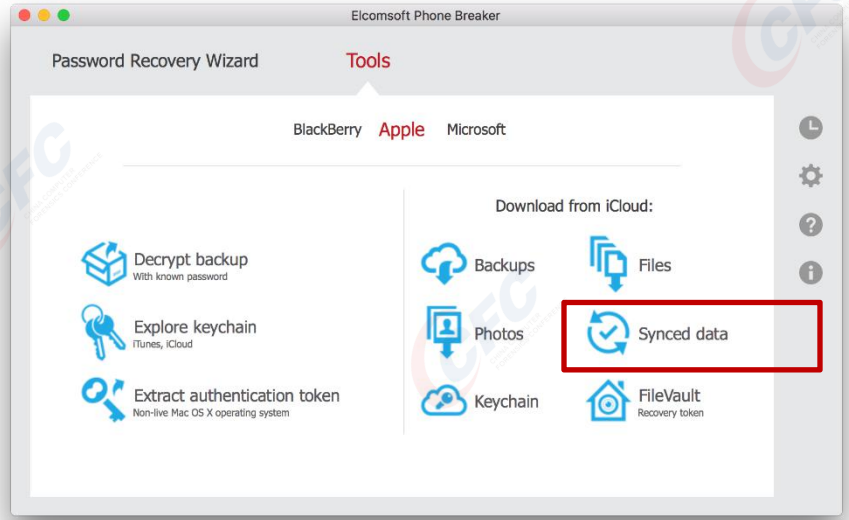
- iCloud邮件，日历，联系人
- Safari浏览历史和打开标签
- 语音备忘录
- 照片（如果iCloud照片库已启用）
- 钱包、地图
- 还有很多



iCloud 取证

提取同步数据

- 使用Elcomsoft Phone Breaker手机密码破解软件
- 需要Apple ID和密码
- 或者，可以使用身份验证令牌
- 苹果允许使用令牌访问同步数据



iCloud 备份

iCloud 有完整的备份

- App数（如果开发者允许备份）
- 照片（仅当iCloud照片库未启用时）
- 消息（如果iCloud消息未启用）
- 密码（密钥链）：“仅限本设备”
- 联系人、日历、笔记等。
- 有些应用程序在iCloud中保持单独的备份或同步数据

iCloud 备份

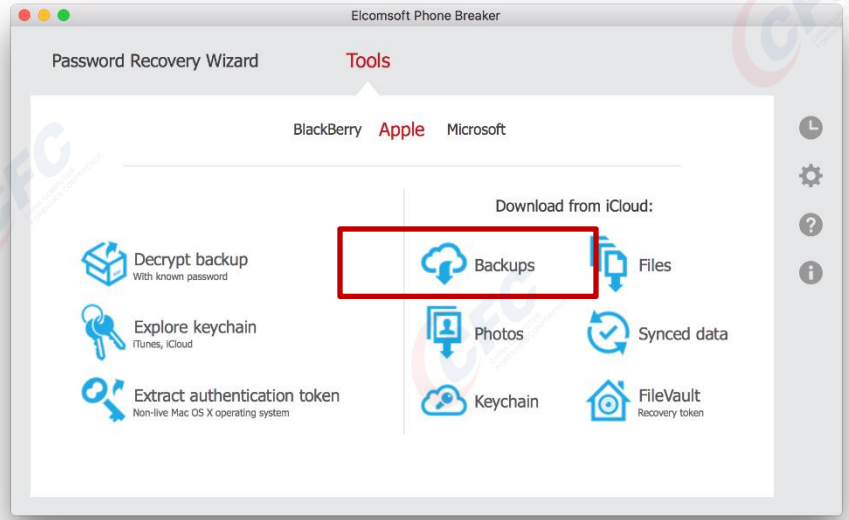
iCloud 备份: 现实情况

- **备份将以5GB的限额计数**
- **在现实生活中，许多用户没有备份(即使启用了备份)**
  - 因为他们的iCloud存储空间被用来存储图片和同步数据
  - 因为有一个应用程序想要备份它的整个数据集(>5GB)
  - 因为仍然有来自非常旧的设备的备份
  - 因为他们不注意，也不关心备份

iCloud 备份

提取 iCloud 备份

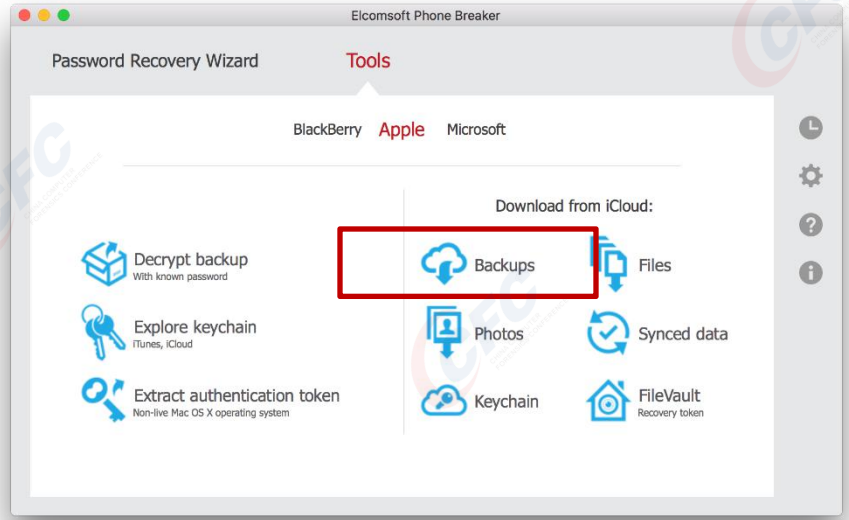
- 抱歉，您无法通过Web界面访问它们
- 选项 1: 新iPhone，从iCloud恢复，进行逻辑采集
- 选项 2: Elcomsoft Phone Breaker 手机密码破解软件



iCloud 备份

提取 iCloud 备份

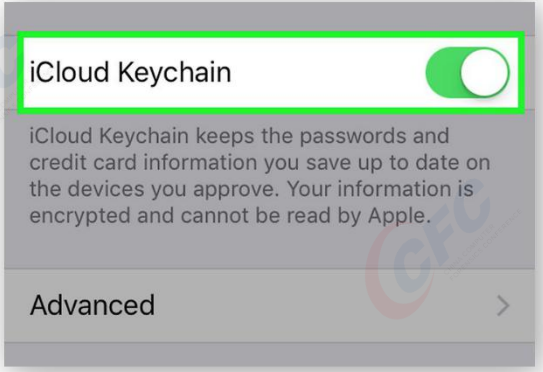
- 需要登录名和密码
- 需要2FA（如果启用），除非从可信的Mac中提取
- 备选方案:令牌（iOS 11.3.1+2FA之前版本）
- 有些项目使用“本设备专用”密钥加密，无法解密



iCloud: 密码

iCloud 密钥链

- 密码、令牌和支付信息通过iCloud同步
- 苹果不提供任何工具或API来访问iCloud密钥链(仅针对您特定于应用程序的数据)
- 几种不同的实现
  - 密码可以存储在iCloud中，也可以不存储在iCloud中

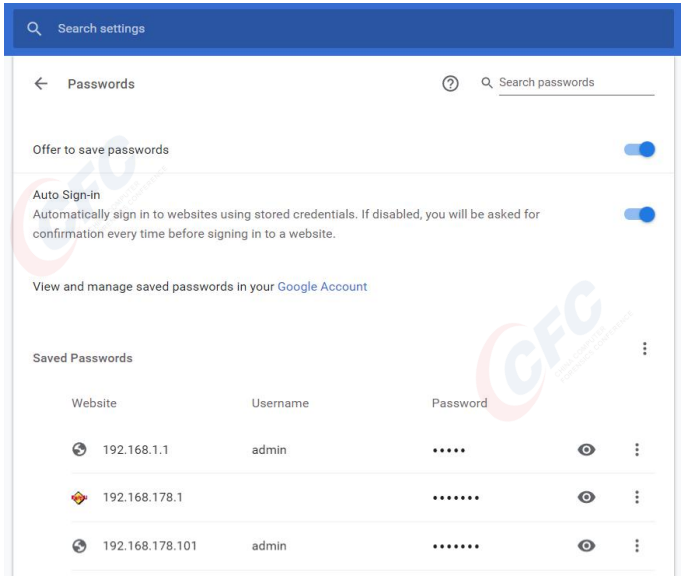


Google: 密码

提取 Chrome 密码

从用户的计算机中提取（如果已安装Chrome且用户已登录）

- 使用谷歌浏览器；登录 chrome://settings/passwords
  - 逐个访问
  - 没有出口
- 使用Elcomsoft Internet Password Breaker密码恢复软件
  - 即时访问
  - 导出到文本文件
  - 建立过滤后的密码字典



iCloud 消息

iCloud 中的消息

- iOS 11.4及更高版本可能会通过iCloud同步消息（iMessages，SMS）
- 类似于iCloud密钥链的保护
  - AES256 加密，需要密码
- 需要Apple ID, 密码和 2FA
  - 如果从受信任的Mac购买，则**不需要**2FA
- 需要来自已注册设备的密码或系统密码

位置

您的智能手机会追踪您的位置

- 精确
- 高效节能
- 除非明确禁用，否则会持续运行
- 即使被明确禁用有时也会运行
  https://www.bbc.com/news/technology-45183041
  https://www.macrumors.com/2018/08/13/google-location-history-disabled-still-stores-data/

位置

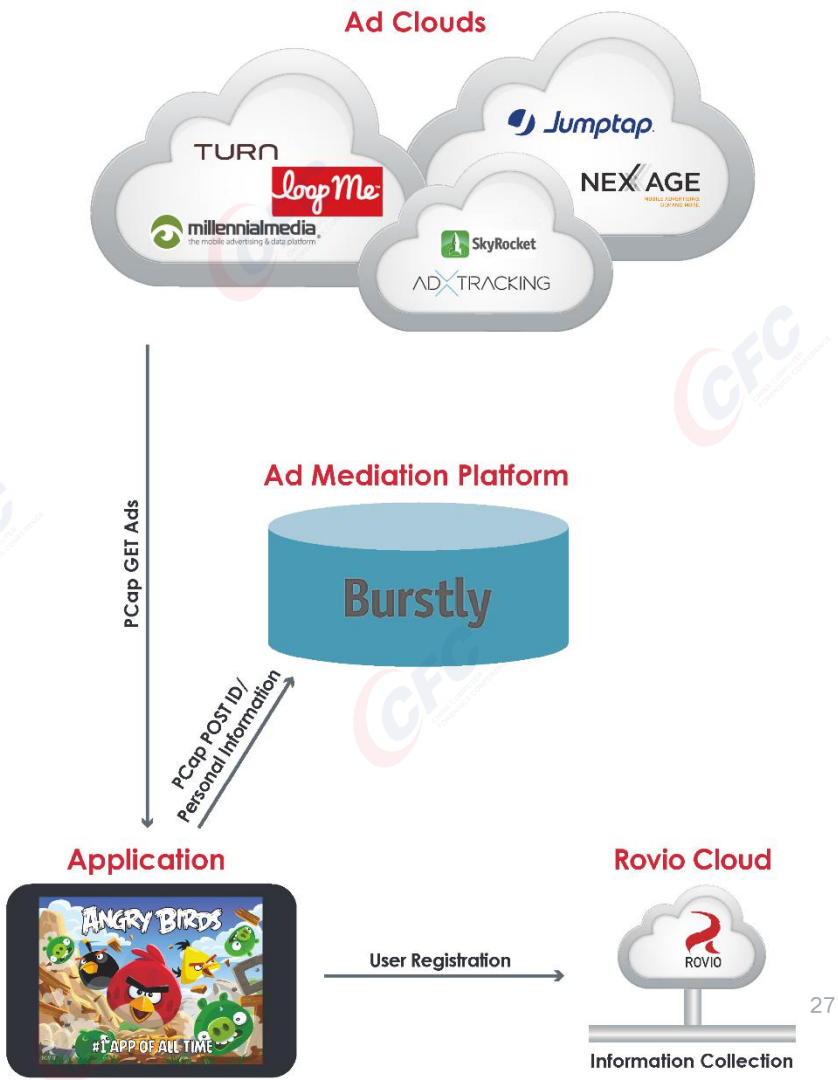
谁在追踪您的位置?

- Apple (iOS, macOS)
- 无数的第三方应用程序和服务
  - 即使记录位置的功能是被禁用的
  - 是的，有可能

位置

第三方应用程序的跟踪

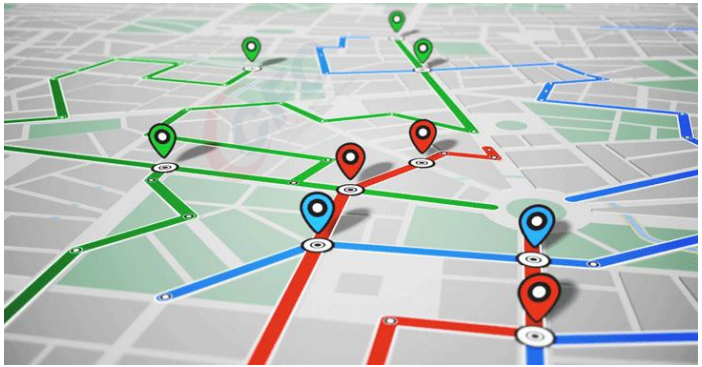
- **收集位置，联系人，电话使用方式等**
- 为了更好地为您服务：
  - 您真的以为该游戏是免费的吗？
- 出售您的数据：
  - 多个经纪人购买此类数据
  - 从各地收集的位置数据
  - 包括Wi-Fi网络和反向BSSID查找
  - 甚至使用IP地址作为位置数据的来源



位置

位置数据存储在哪里？

- 物理设备 (iOS, Android, Windows, macOS X, other systems)
- Apple iCloud
- 第三方云帐户
  - 社交网络
  - 健康与健身应用
  - 即时通讯工具
  - 约会应用
  - 打车应用
  - 旅游应用



位置

Apple 如何存储位置数据？

- 位置数据存储为：
  - 数据库记录
  - PLIST 值
  - JSON 值
  - 混合的 PLIST/JSON 结构作为数据库记录
  - 日志文件（纯文本）
- 存储在哪里？
  - 系统数据库（与服务/守护程序有关）
  - 内置应用数据
  - 临时/缓存数据
  - iCloud

位置

Apple 都收集什么？

- 收集的数据取决于来源和存储
- 这些项目始终存在：
  - **纬度**
  - **经度**
  - **时间戳**（主要为UNIX Epoch格式）
  - 我们可以看到没有时间戳的位置记录
  - 我们可以看到没有纬度/经度的位置名称/ ID

- 这些项目可额外提供：
  - **高度**
  - **准确度** – 测量的准确度（可以表示为具有给定半径的圆）
  - **置信度** – 系统对所述准确度的置信度
  - **最小/最大纬度和经度** – 另一种精度表示。可以用矩形面积来表示
  - **速度**
  - **航向** – 以度为单位表示转角
  - **结束日期**-设备离开原来位置的日期
  - **地址**-您的地址； 可以存储为字符串或多个项目

位置

路由

- 路由可以在设备或应用程序上被追踪
  - 可以考虑速度，航向，角度(磁罗盘)值
  - 路由被存储在设备上
- 在取证软件中，可以根据单个位置记录计算路由
  - 基于已记录的位置
  - 可以基于从多个来源(如地图、第三方应用、系统日志等)获得的位置记录来进行计算。

位置

iTunes备份：位置数据的来源

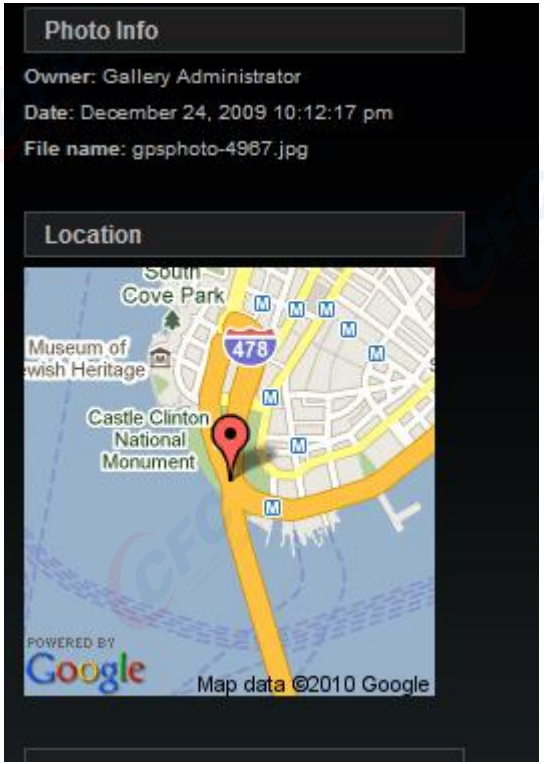
- *本地（iTunes）备份是主要的证据来源*
- *备份包含位置数据（没有存储在物理设备上的那么多）*

- Apple 地图
- 日历
- 媒体 (EXIF)
- 钱包
- 多个第三方应用程序数据和缓存
- 位置缓存
- 频繁/重要的地点
- 媒体文件分析期间缓存的位置
- Apple Pay 的地点

位置

媒体 (EXIF)

- Windows, macOS, iOS, Android
- Windows: 文件属性 > 详细信息 > GPS
- macOS: 更多信息 > 纬度和经度
- 第三方软件可以映射位置数据
- 取证软件提取EXIF标签，解析位置数据，建立路线



位置

钱包

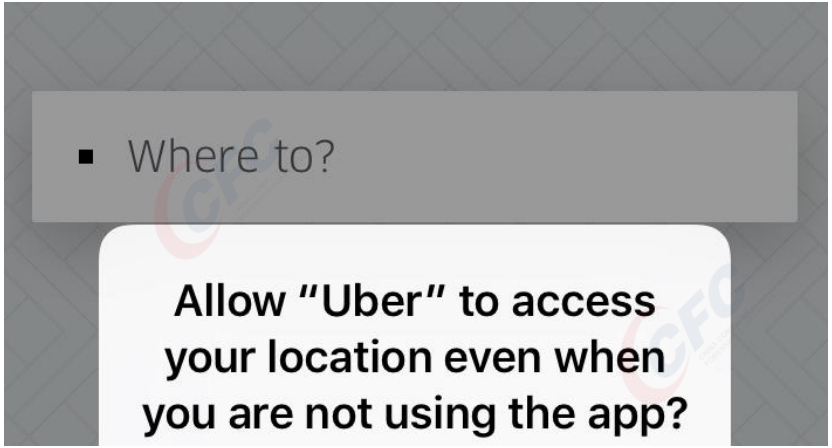
- 存储在文件夹中：
- /HomeDomain/Library/Passes/Cards
- /HomeDomain/Library/Passes/BadUbiquitousPasses
- 在.pkpass子文件夹中
- 寻找pass.json文件
- 有些包含位置信息


```
{
  "description": "SOURCE to DESTINATION",
  "formatVersion": 1,
  "organizationName": "The Airlines",
  "relevantDate": "2013-02-20T20:40:00+01:00",
  "boardingPass": {
    "transitType": "PKTransitTypeAir"
  },
  "locations": [
    {
      "latitude": 12.11334800,
      "longitude": 13.56972200,
      "relevantText": "AirportName1"
    },
    {
      "latitude": 80.45861100,
      "longitude": 80.10611100,
      "relevantText": "AirportName2"
    }
  ]
}
```

位置

第三方应用程序

- 多个第三方应用程序和游戏收集位置数据
  - 即使您不使用该应用程序
- 这些数据在iTunes备份中可能可用，也可能不可用
- 应用程序可能还会缓存数千个位置点
  - /private/var/mobile/Containers/Data/Application/<UUID>/Library/Caches/
  - *<UUID>: 此设备上的唯一的应用程序标识符*




```
{
  "jsonConformingObject":{
    "meta":{
      "location":{
        "course":-1,
        "city":"test",
        "speed":-1,
        "longitude":3.4,
        "gps_time_ms":1506351484216,
        "latitude":1.2,
        "horizontal_accuracy":65,
        "vertical_accuracy":10,
        "altitude":0.1
      }
    }
  }
}
```

位置

物理提取的其他专用位置数据

- 物理获取提取文件系统的完整镜像
- 获得对不在备份中的文件访问权
  - 系统日志、缓存和临时文件
  - 受保护的应用程序数据
  - 禁用备份的应用程序
- iCloud自动同步(如果在设置中启用iCloud同步)
  - 计划同步
  - 在设备重启
  - 账户变更时

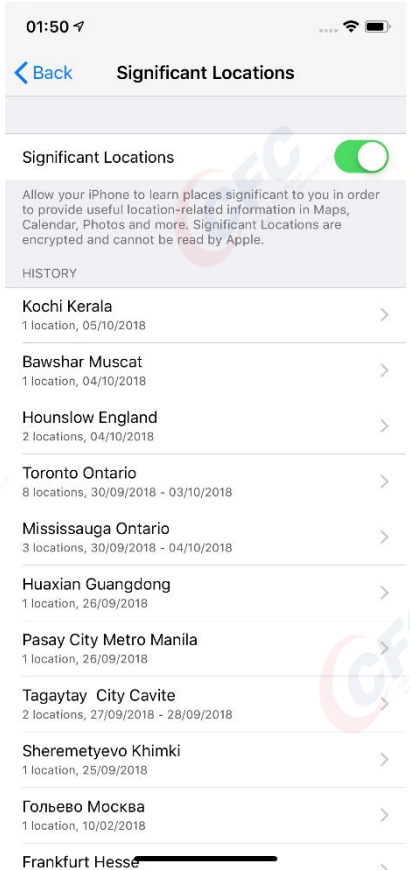
- 高速缓存 (3G/LTE, Wi-Fi)
- 频繁的/重要的位置
- 媒体文件分析缓存
- 第三方缓存
- Apple Pay 地点

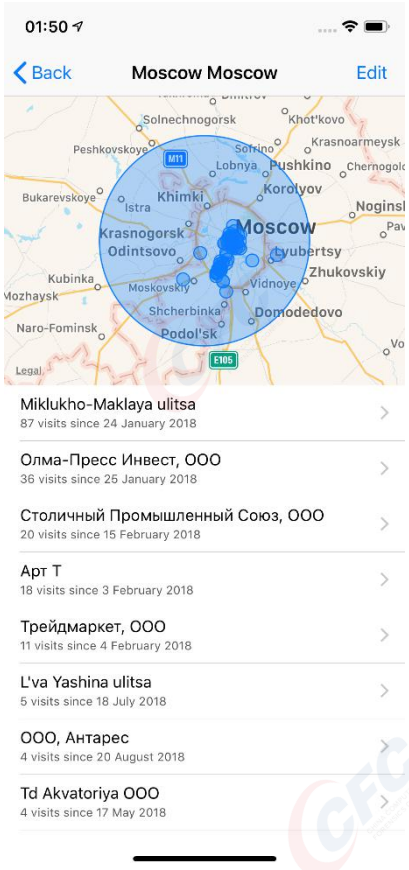
位置

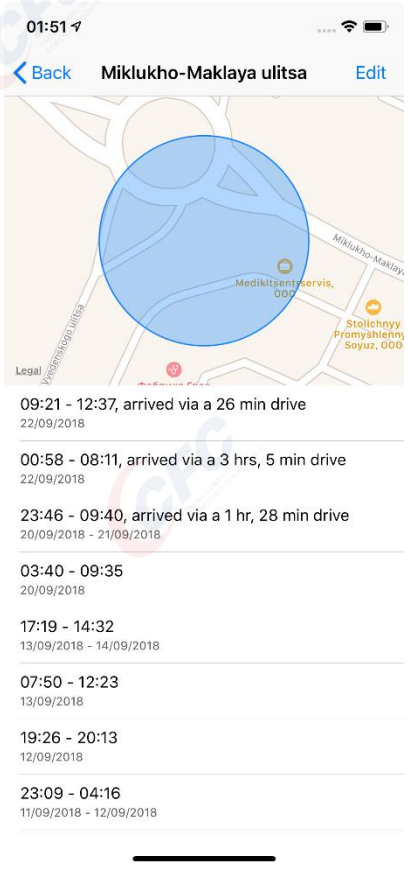
位置缓存（仅物理提取）

- 数据库：
  - /private/var/root/Library/Caches/locationd/cache_encryptedA.db
  - /private/var/root/Library/Caches/locationd/cache_encryptedB.db
  - /private/var/mobile/Library/Caches/com.apple.routined/cache_encryptedA.db
  - /private/var/mobile/Library/Caches/com.apple.routined/cache_encryptedB.db
- 表：
  - 纬度，经度，高度，时间戳，水平精度，垂直精度，速度，航向，置信度
  - 最小纬度，最小经度，最大纬度，最大经度

重要地点


01:50
Back
Significant Locations
Significant Locations
Allow your iPhone to learn places significant to you in order to provide useful location-related information in Maps, Calendar, Photos and more. Significant Locations are encrypted and cannot be read by Apple.
HISTORY
Kochi Kerala
1 location, 05/10/2018
Bawshar Muscat
1 location, 04/10/2018
Hounslow England
2 locations, 04/10/2018
Toronto Ontario
8 locations, 30/09/2018 - 03/10/2018
Mississauga Ontario
3 locations, 30/09/2018 - 04/10/2018
Huaxian Guangdong
1 location, 26/09/2018
Pasay City Metro Manila
1 location, 26/09/2018
Tagaytay City Cavite
2 locations, 27/09/2018 - 28/09/2018
Sheremetyevo Khimki
1 location, 25/09/2018
Гольево Москва
1 location, 10/02/2018
Frankfurt Hesse


01:50
Back
Moscow Moscow
Edit
Solnechnogorsk
Khot'kovo
Peshkovskoye
Krasnoarmeysk
Sofrino
Lobnya
Pushkino
Bukarevskoye
Khimki
Istra
Korolyov
Krasnogorsk
Odintsovo
Moscow
Lyubertsy
Zhukovskiy
Kubinka
Moskovskiy
Vidnoye
Shcherbinka
Domodedovo
Naro-Fominsk
Podol'sk
Legal
Miklukho-Maklaya ulitsa
87 visits since 24 January 2018
Олма-Пресс Инвест, ООО
36 visits since 25 January 2018
Столичный Промышленный Союз, ООО
20 visits since 15 February 2018
Арт Т
18 visits since 3 February 2018
Трейдмаркет, ООО
11 visits since 4 February 2018
L'va Yashina ulitsa
5 visits since 18 July 2018
ООО, Антарес
4 visits since 20 August 2018
Td Akvatoriya OOO
4 visits since 17 May 2018


01:51
Back
Miklukho-Maklaya ulitsa
Edit
Miklukho-Maklaya
Mediklitsentr servis, OOO
Stolichnyy Promyshlenny Soyuz, OOO
Legal
09:21 - 12:37, arrived via a 26 min drive
22/09/2018
00:58 - 08:11, arrived via a 3 hrs, 5 min drive
22/09/2018
23:46 - 09:40, arrived via a 1 hr, 28 min drive
20/09/2018 - 21/09/2018
03:40 - 09:35
20/09/2018
17:19 - 14:32
13/09/2018 - 14/09/2018
07:50 - 12:23
13/09/2018
19:26 - 20:13
12/09/2018
23:09 - 04:16
11/09/2018 - 12/09/2018

位置

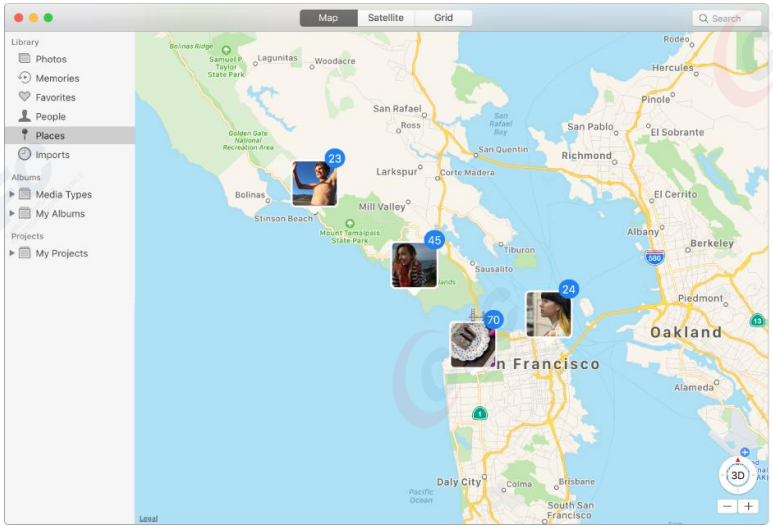
同步位置数据（iCloud）

- 系统应用通过iCloud的同步位置数据：
  - 苹果地图
  - 健康
  - 日历
  - 钱包
- 直接同步敏感位置数据：
  - 重要地点：直接的设备到设备的同步而已，绕过iCloud。
  - Wi-Fi连接
  - 反向BSSID查找可显示位置
  - 根据来源，可能不连接时间戳（仅第一次连接和最后一次断开连接）
  - 日志包含时间戳

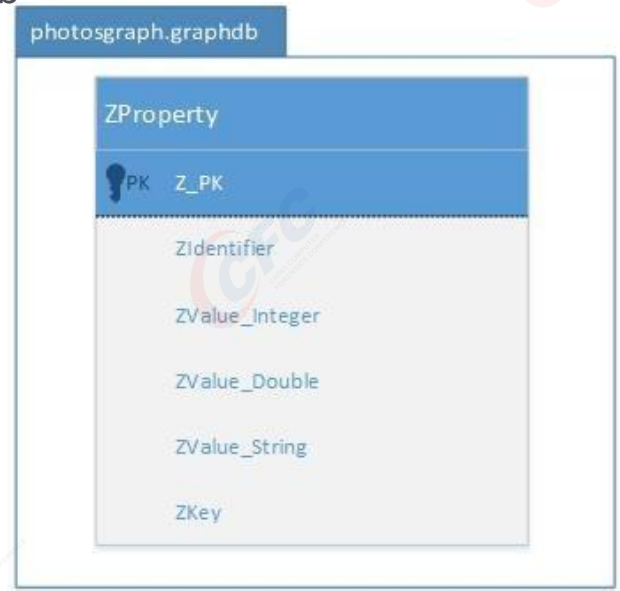
位置

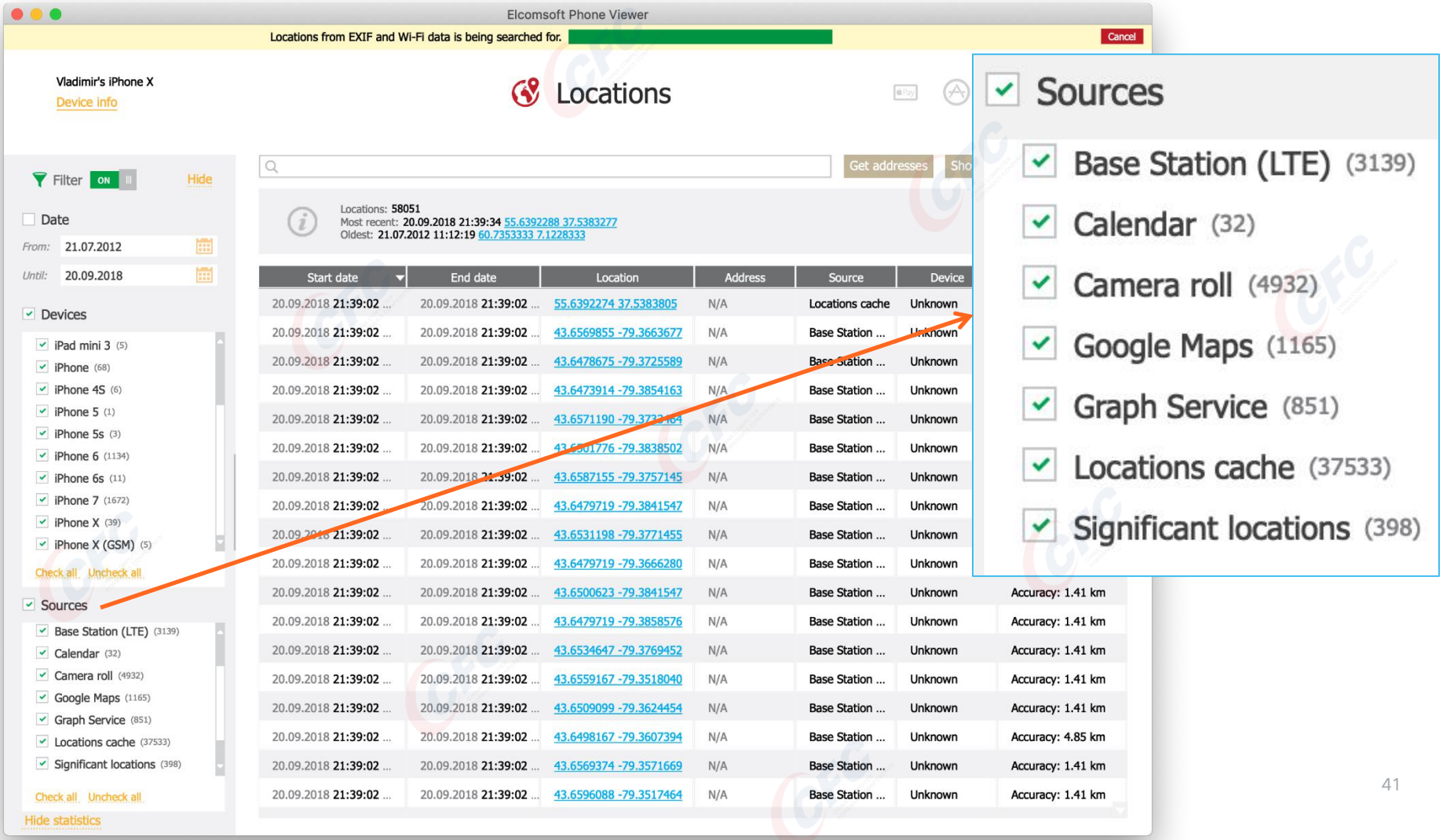
分析媒体文件时缓存的位置

- **照片分析过程**分析媒体文件；分配标签，发现面孔，提取EXIF等；
- **照片地图**提取的EXIF位置。



/private/var/mobile/Media/PhotoData/Caches/GraphService/PhotosGraph/photosgraph.graphdb




Elcomsoft Phone Viewer
Locations from EXIF and Wi-Fi data is being searched for.
Cancel
Vladimir's iPhone X
Device info
Locations
Filter ON
Hide
Date
From: 21.07.2012
Until: 20.09.2018
Devices
iPad mini 3 (5)
iPhone (68)
iPhone 4S (6)
iPhone 5 (1)
iPhone 5s (3)
iPhone 6 (1134)
iPhone 6s (11)
iPhone 7 (1672)
iPhone X (39)
iPhone X (GSM) (5)
Check all Uncheck all
Sources
Base Station (LTE) (3139)
Calendar (32)
Camera roll (4932)
Google Maps (1165)
Graph Service (851)
Locations cache (37533)
Significant locations (398)
Check all Uncheck all
Hide statistics
Get addresses
Locations: 58051
Most recent: 20.09.2018 21:39:34 55.6392288 37.5383277
Oldest: 21.07.2012 11:12:19 60.7353333 7.1228333
Start date
End date
Location
Address
Source
Device
20.09.2018 21:39:02 ... 55.6392274 37.5383805 N/A Locations cache Unknown
20.09.2018 21:39:02 ... 43.6569855 -79.3663677 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6478675 -79.3725589 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6473914 -79.3854163 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6571190 -79.3731464 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6501776 -79.3838502 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6587155 -79.3757145 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6479719 -79.3841547 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6531198 -79.3771455 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6479719 -79.3666280 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 43.6500623 -79.3841547 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 43.6479719 -79.3858576 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 43.6534647 -79.3769452 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 43.6559167 -79.3518040 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 43.6509099 -79.3624454 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 43.6498167 -79.3607394 N/A Base Station ... Unknown Accuracy: 4.85 km
20.09.2018 21:39:02 ... 43.6569374 -79.3571669 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 43.6596088 -79.3517464 N/A Base Station ... Unknown Accuracy: 1.41 km
Sources
Base Station (LTE) (3139)
Calendar (32)
Camera roll (4932)
Google Maps (1165)
Graph Service (851)
Locations cache (37533)
Significant locations (398)

iCloud 取证

iCloud 同步数据：特殊的类别

- iCloud 密钥链
- 健康数据
- 信息 (SMS 和 iMessage)
- 屏幕时间

  包括屏幕时间的密码

iCloud 取证

iCloud 同步数据：特殊的类别

- 加密和保护
- 需要访问的已注册设备的密码或系统密码

Apple Health

- **活动量** – 您的活动量
- **营养** – 饮食的分解
- **睡眠** – 您的睡眠习惯
- Mindfulness

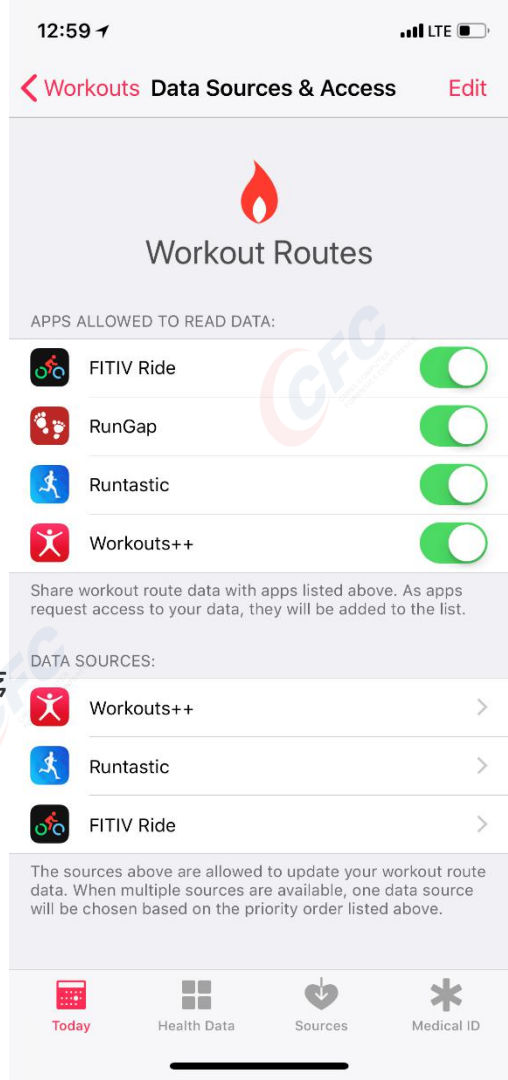
附加的数据类别

- **身体监测** – 身高和体重
- **健康记录** - CDA + 健康记录
- **心脏数据** – 血压、心率
- **生殖健康** – 性活动和月经周期yue'j
- **检查结果** – 各种医学测试结果（例如糖水平）
- **重要信息** – 血压，体温，心率，呼吸率
- **医疗 ID** – 基本医疗数据

Apple Health

Apple Health从哪里获取数据

- 从HealthKit设备（iPhone，Apple Watch，兼容的健身追踪器等）接收的数据
  - 自动数据提交
  - 脉搏，血压
  - 专注力，心脏和活动的数据
  - Apple Watch收集睡眠数据;无自动模式(可以使用第三方应用程序
- 第三方应用程序（Nike +，Strava，Workouts ++）
  - 支持所有数据类别
  - 每个数据类别都有一个“推荐”第三方应用程序列表，用于收集该类型的数据
  - 必须在“健康”>“源”中跟踪的类别中激活第三方应用



Apple Health

访问Apple Health数据

- 从健康类应用程序中导出（XML）
- 本地备份（仅加密）
- 文件系统获取（需要破解）
- GDPR请求
- 政府/ 执法部门请求
- 云提取

Apple Health

提取Apple Health数据：简单的方法

- Apple Health可以通过逻辑获取来获得
- **未加密的备份中没有Apple Health数据！**
  - 与密钥链不同，密钥链仍存在于未加密的备份中，并由硬件密钥保护
- 进行备份之前设置一个已知的密码
- 使用iTunes进行本地备份
- 解密备份，访问Apple Health数据
- 使用取证软件查看（或手动分析数据库）

Apple Health

提取Apple Health数据：复杂的方法

- Apple Health 可以通过文件系统获取
- **需要破解**
  - 目前，破解适用于从8到12.1.2的所有版本的iOS
- 破解，使用SSH（或取证软件）
- 获取TAR镜像
- 使用取证软件查看（或手动分析数据库）
- *仅当备份受密码保护时才需要*

Apple Health

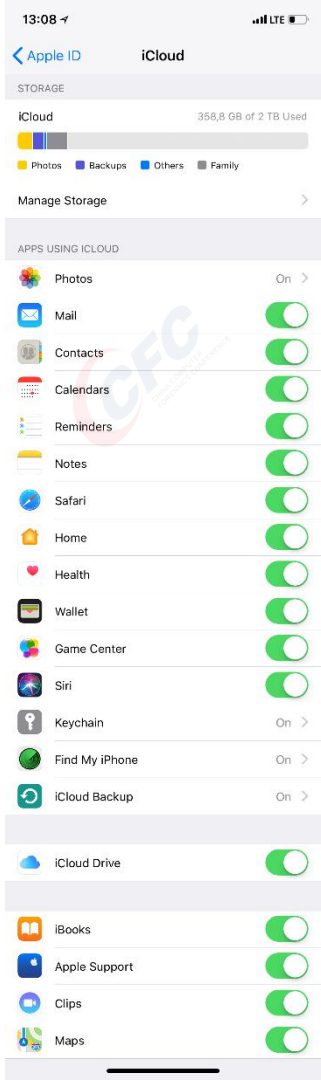
提取Apple Health数据：GDPR

- 欧盟用户可以通过请求GDPR来访问他们的健康数据
- 注册GDPR请求：privacy.apple.com
- 需要Apple ID, password, 2FA
- 需要7天才能收到数据
- 多种二进制和文本格式

Apple Health

Apple Health和云

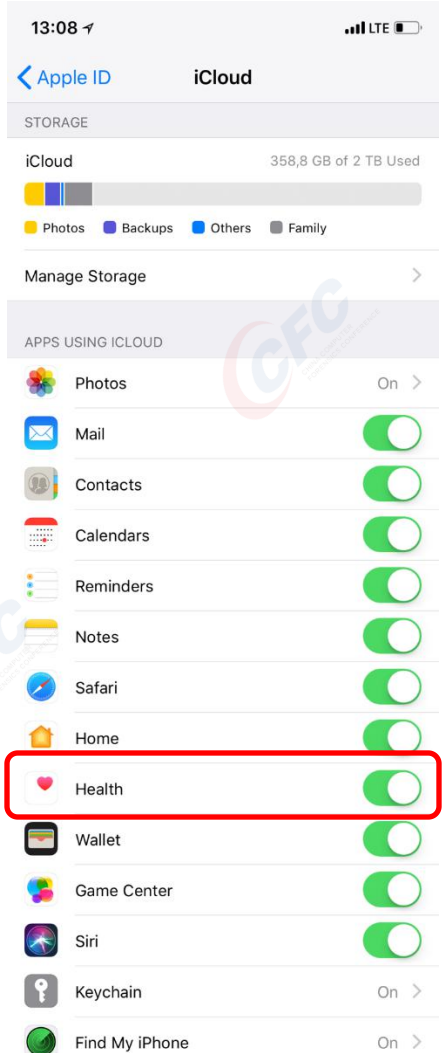
- 本机Apple Health数据与iCloud同步到所有已注册的设备
- 第三方应用程序通过HealthKit运行
- 某些第三方应用程序数据未与Apple Health共享
- 某些应用使用专有的云同步（Strava，Endomondo）
- 每个设备的**医疗ID**数据都是唯一的，并且**不会同步**
- **CDA记录**不同步（据我们所知）



Apple Health

Apple Health和 iCloud

- Apple Health数据可以从iCloud获得
- 与设备上可用的信息相比，可能包含更多的信息
- 从技术上讲，Apple Health属于“同步数据”，而不是“云备份”
  - 这显著提高了提取的可靠性
  - 与备份相比，iCloud令牌的过期失效规则更宽松



Apple Health

访问iCloud中的健康数据

我们可以下载同步数据，包括Apple Health

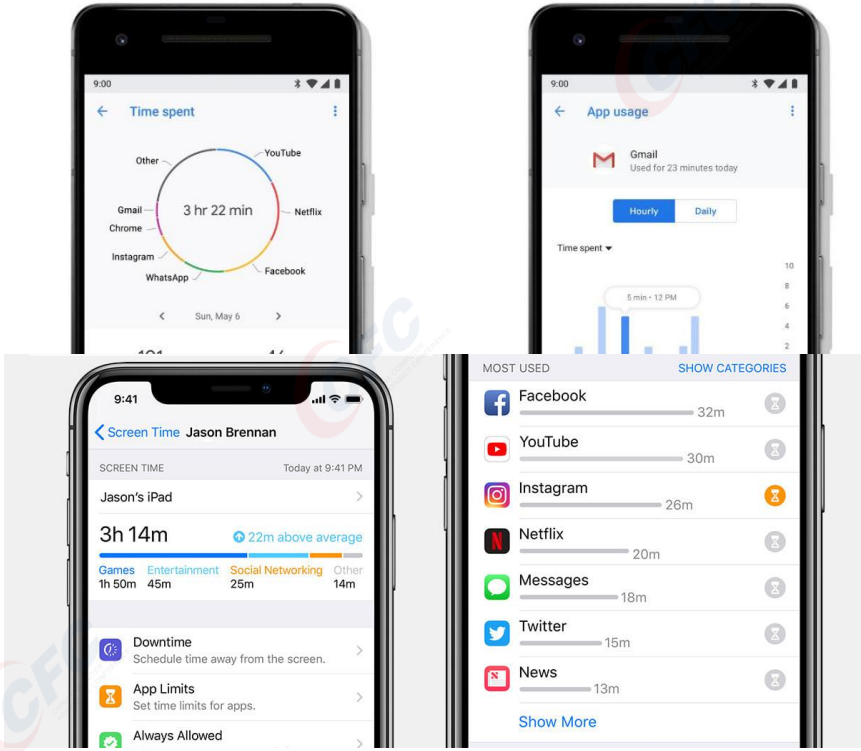
什么地方可能出错：

- 双因素身份验证可能是个问题
- 需要访问二级身份验证因子(除非使用身份验证令牌)
- 从ios12开始，健康数据可能会被加密(就像消息一样)

使用数据: Apple屏幕时间

您的智能手机更了解您的生活

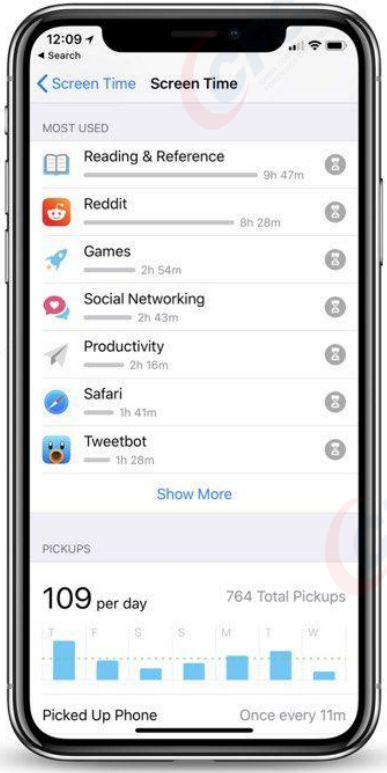
- Apple在iOS 13中引入了用户可访问的使用情况统计信息
- 详细说明应用程序使用情况和类别
- 在游戏，娱乐，社交网络和其他活动上花费的时间
- 每日，每小时和每周统计



屏幕时间

iOS 屏幕时间：统计数据

- 每日及每周报告
- 每个类别的统计信息和执行时间限制
- 按照每个应用程序跟踪
- 追踪您拿起手机的次数



屏幕时间

iOS 屏幕时间：限制条件

- 跟踪或限制在游戏，娱乐，社交网络，阅读以及其他活动上花费的时间
- 跟踪和限制单个应用
- 设置停机时间和应用程序限制
- 内容和隐私限制

屏幕时间

iOS 屏幕时间：密码

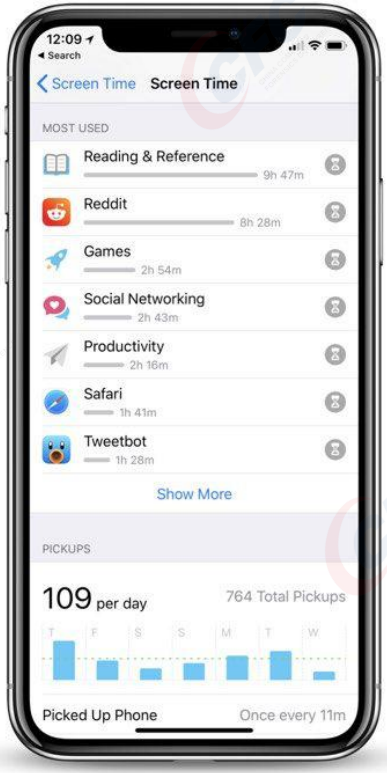
防沉迷屏幕时间的密码限制如下：

- 重置iTunes备份密码
- 使用受限制保护的设置
- 修改屏幕时间限制

屏幕时间

iOS 屏幕时间：统计数据

- 每日及每周报告
- 每个类别的统计信息和执行时间限制
- 按照每个应用程序跟踪
- 追踪您拿起手机的次数



屏幕时间

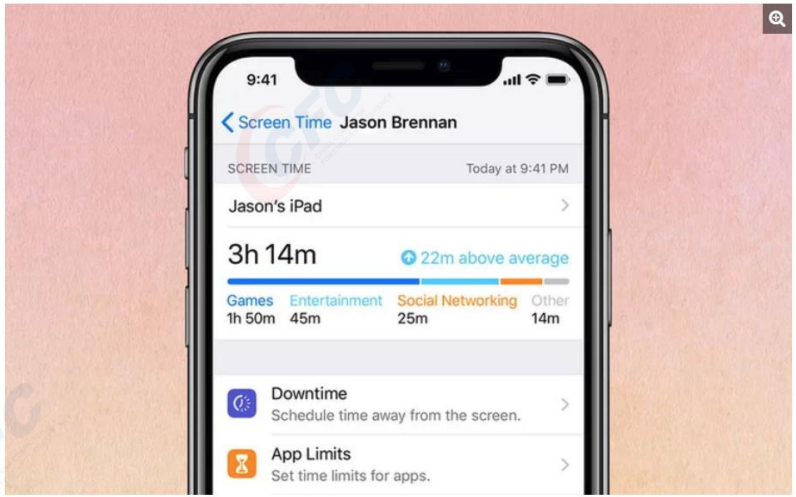
iOS 屏幕时间：iCloud同步

- 查看如何在多个设备上使用应用程序
- 通过iCloud同步停机时间和应用限制
- 限制自动应用于所有设备
- 使用情况数据同步到同一Apple ID上的所有设备
  - 这样您就不能欺骗系统
    - 除非您才7岁☺

7-Year-Old Hacks Apple's Screen Time Restrictions

by JESUS DIAZ Sep 26, 2018, 10:02 AM

Redditor PropellerGuy's 7-year-old son has cracked a way to bypass Screen Time, the new Apple iOS 12 feature that — among other things — is supposed to allow parents to set limitations to the time kids can spend in their tablets and phones.

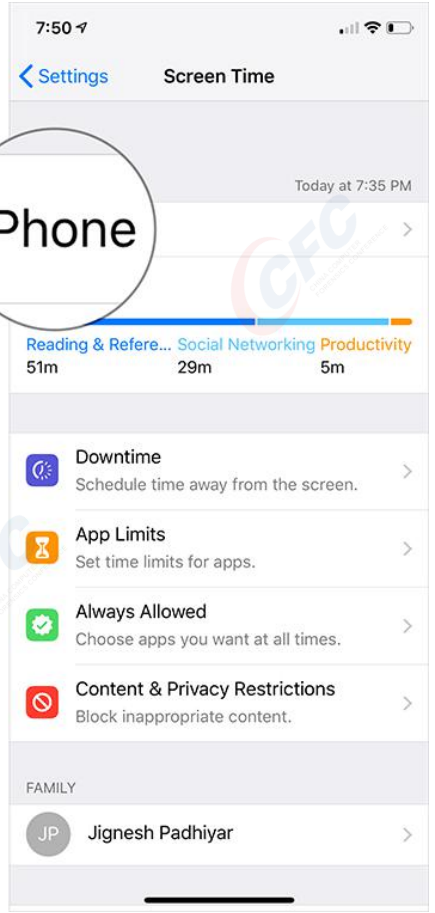


屏幕时间

提取屏幕时间密码

屏幕时间密码可以从以下位置提取：

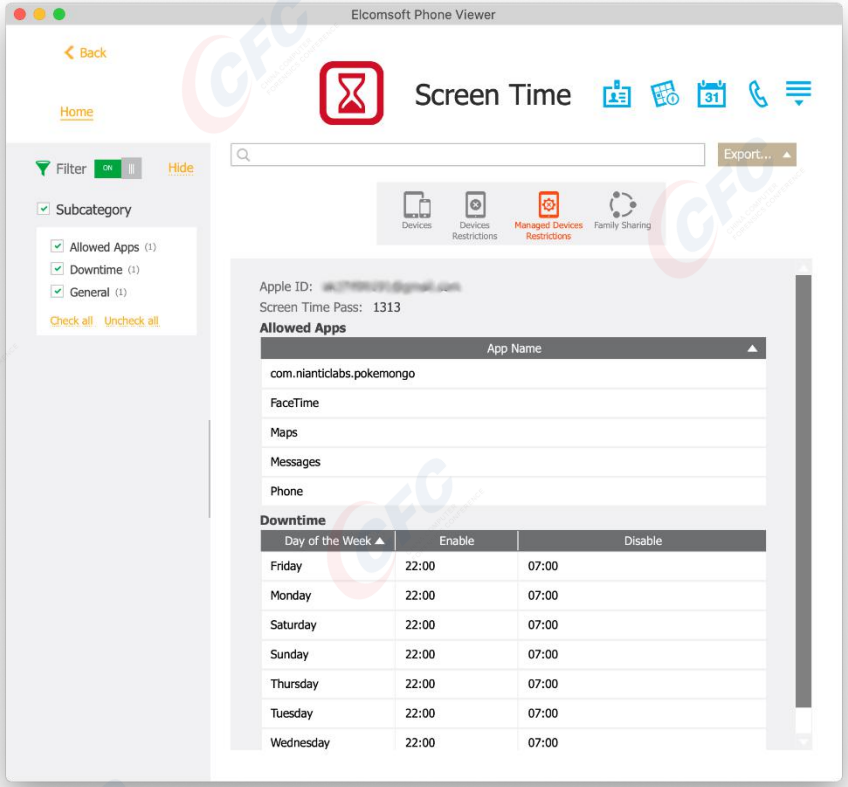
- iOS 12: 受密码保护的本地备份（必须知道密码）
- iOS 12: iCloud（需要Apple ID，密码，2FA，设备密码）
- iOS 13: 仅 iCloud（相同要求）



屏幕时间

屏幕时间密码: 获取工具

- Elcomsoft Phone Breaker 进行提取
- Elcomsoft Phone Viewer 进行查看



屏幕时间

iOS 屏幕时间：结论

- Apple 非常清楚您如何使用您的设备
- 他们将其存储在他们的服务器上:
- 统计数据和报告
  - 使用iCloud同步
- 宽松的强制性限制
  - 使用iCloud同步

屏幕时间

屏幕时间总结

- Apple屏幕时间
  - 每个应用程序和每个类别的统计
  - 每日及每周报告
  - iCloud同步到所有用户的设备
    - 包括使用情况和限制
  - 停机时间
  - 通知统计数据
  - 限制密码

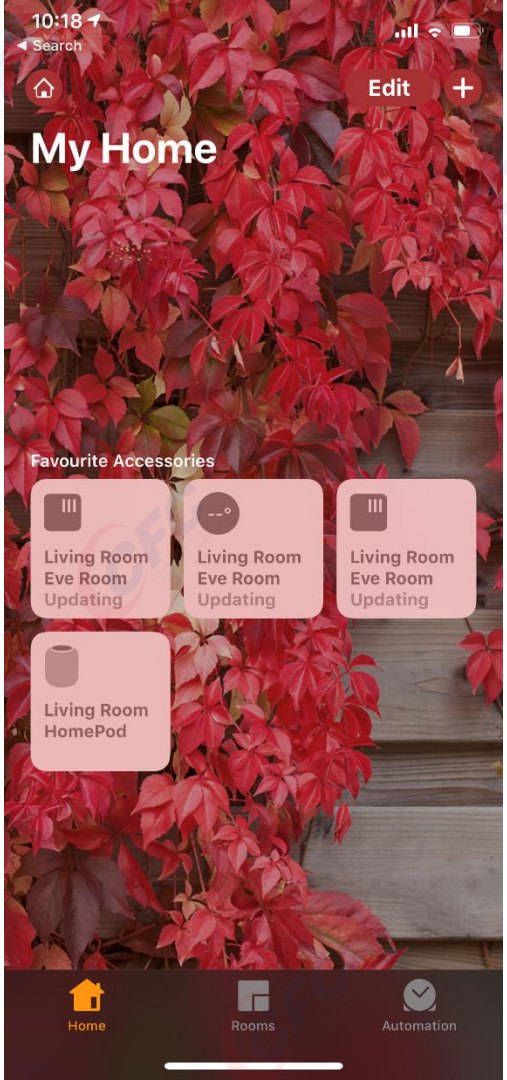
未来将会是…

iCloud: 接下来是什么?

iCloud中存在更多的同步数据

- 家庭数据（HomePod，各种传感器，灯光，恒温器等）
- 屏幕时间（应用使用情况；以前只能通过完整文件系统获取获得）
- 语音备忘
- 天气和股票

Remember Celebgate? ;)



智能手机取证

从哪里获得数据?

- 设备(本地备份)　　//经由逻辑获取
- 设备(云备份)　　//需要凭证!
- 设备(物理获取)　　//需要破解/root
- 设备数据与桌面同步
- 云(同步数据)　　//需要凭证!
- 云(位置服务，如Apple Find My) //需要凭证!
- 第三方[云]服务　　//需要凭证!

Apple 数据保护

iCloud 安全概览 (HT202303)

End-to-end encrypted data

End-to-end encryption provides the highest level of data security. Your data is protected with a key derived from information unique to your device, combined with your device passcode, which only you know. No one else can access or read this data.

These features and their data are transmitted and stored in iCloud using end-to-end encryption:

- Home data
- Health data
- iCloud Keychain (includes all of your saved accounts and passwords)
- Payment information
- Siri information
- Wi-Fi network information

To use end-to-end encryption, you must have two-factor authentication turned on for your Apple ID. To access your data on a new device, you might have to enter the passcode for an existing or former device.

Messages in iCloud also uses end-to-end encryption. If you have iCloud Backup turned on, your backup includes a copy of the key protecting your Messages. This ensures you can recover your Messages if you lose access to iCloud Keychain and your trusted devices. When you turn off iCloud Backup, a new key is generated on your device to protect future messages and isn't stored by Apple.

现实是：

- *家庭数据：尚未检查，但似乎没有*
- *健康状况：有，如果帐户中的所有设备都使用macOS 11.4 / iOS 12或更高版本*
- *iCloud 密钥链: 有*
- *支付信息：有*
- *Siri 信息：有*
- *Wi-Fi 网络信息：仅密码有*

尽管如此，大多数数据仍可以下载，并使用适当的凭据进行解密

Apple 和执法部门

Apple 如何满足执法部门请求

- 执法部门可以通过政府信息请求获取证据
- **整个过程是完全透明的**(在法律允许的范围内)
- 年度统计数据已公布，并向公众提供
- 指南：

  https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

Apple 和执法部门

执法部门请求如何发挥作用：

- 帐户保存请求，然后是帐户信息请求
- 所有请求都按照苹果的隐私政策处理（Apple’s privacy policy）
- 为满足政府的要求，苹果公司以专有格式提供信息
- 调查人员会收到加密的信息。 提供了解密密钥，但没有用于解密数据的工具
- 解密过程很复杂
- 许多专家使用第三方工具或服务，例如Kleopatra，GPG，Cellebrite或BlackBag

Apple 和执法部门

执法部门请求的利弊：

- 政府请求不需要用户的身份验证凭据
- 如果登录名和密码不可用，则政府请求可能是获取信息的唯一方法
- 除了身份认证证书，与内部云获取相比，政府请求有许多重大缺陷

Apple 和执法部门

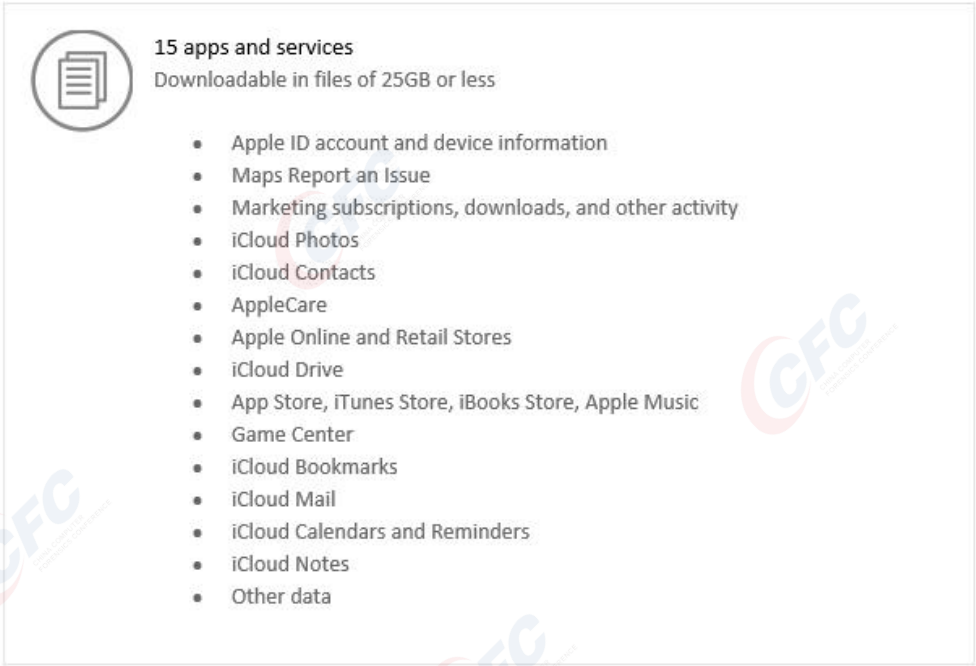
LE请求丑陋的一面

- 很多法律文书
- **帐户保留请求**必须在获取之前提交
- 这个过程很漫长
  - 长达两个月
- Apple 提供加密的二进制格式的数据
  - 提供了解密密钥，但没有解密工具
  - 第三方工具和服务增加了额外的成本和延迟
- Apple **不会**提供**健康数据**，**屏幕时间**，**消息**或**密码**（iCloud密钥链）
  - Apple公司未存储的具有其他加密密钥的其他加密

Apple 和 GDPR

什么是适用的呢…

- 所有主要数据都在那里
- 包括图片
- 浏览历史，文件，iCloud邮件
- 7天处理申请
- 提供在请求的第一天拍摄的快照



15 apps and services

Downloadable in files of 25GB or less

- Apple ID account and device information
- Maps Report an Issue
- Marketing subscriptions, downloads, and other activity
- iCloud Photos
- iCloud Contacts
- AppleCare
- Apple Online and Retail Stores
- iCloud Drive
- App Store, iTunes Store, iBooks Store, Apple Music
- Game Center
- iCloud Bookmarks
- iCloud Mail
- iCloud Calendars and Reminders
- iCloud Notes
- Other data

This process can take up to seven days. To ensure the security of your data, we use this time to verify that the request was made by you. We will notify you when your data is ready. You can check the status of your request at any time by visiting privacy.apple.com/account.

Apple 和 GDPR

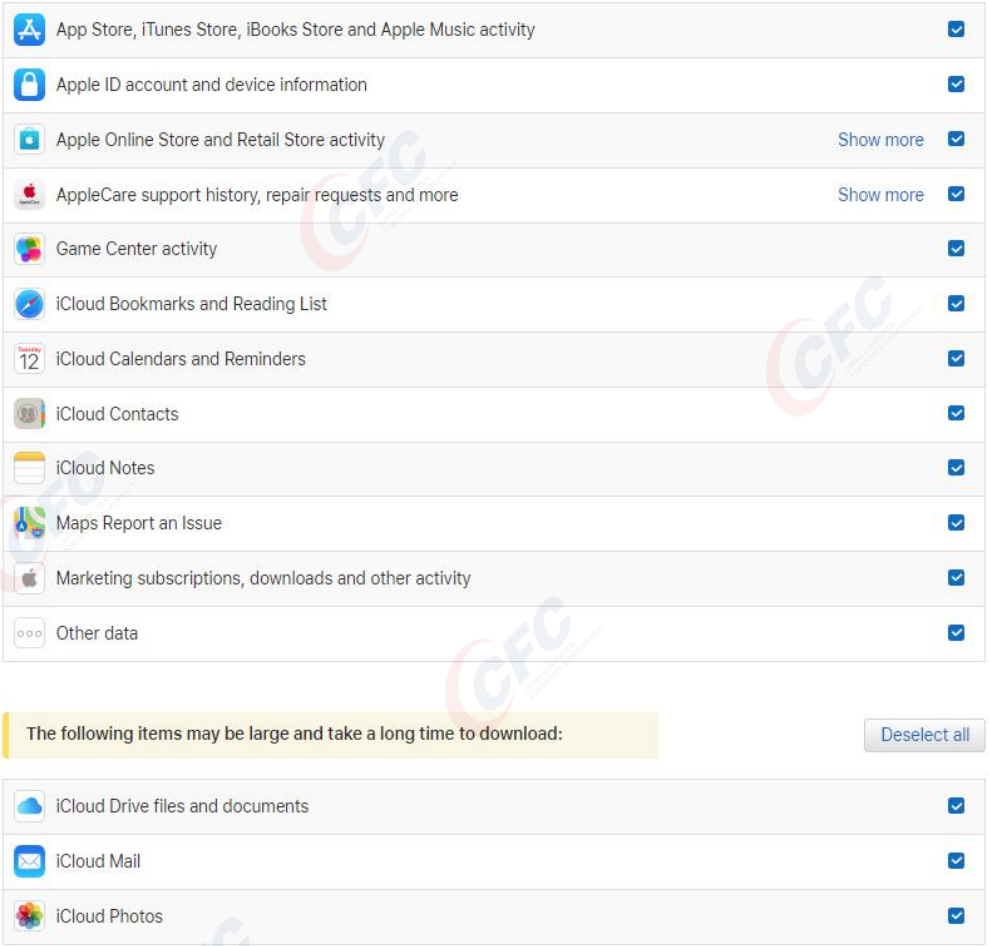
什么不是呢...

- **也不是对所有人都适用：在中国不适用**
- **有些东西不见了**
- **Apple Pay** – 从未与iCloud同步
- **防沉迷屏幕时间限制**
- **讯息** – 附加加密

  我们可以解密它
- **密码** – iCloud 密钥链有额外的加密

  我们可以解密它
- **健康数据** – 额外的加密, 需要密码

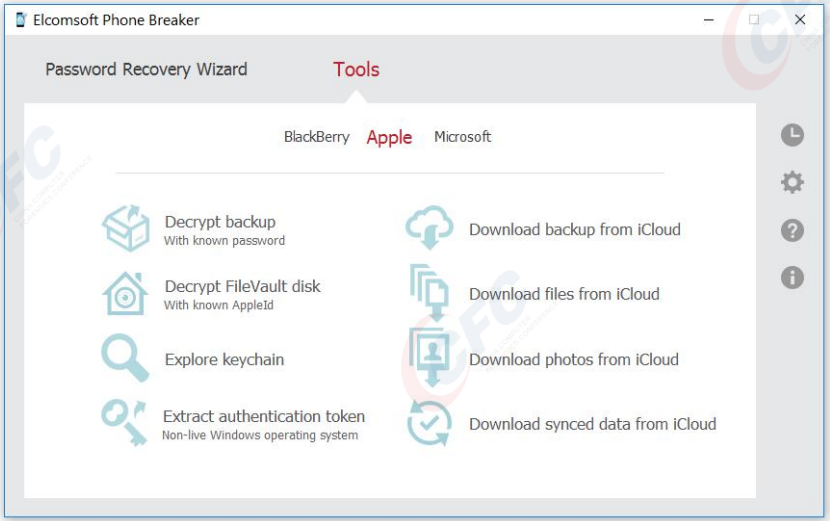
  我们可以解密它



Apple: 云的提取和备份

Elcomsoft Phone Breaker

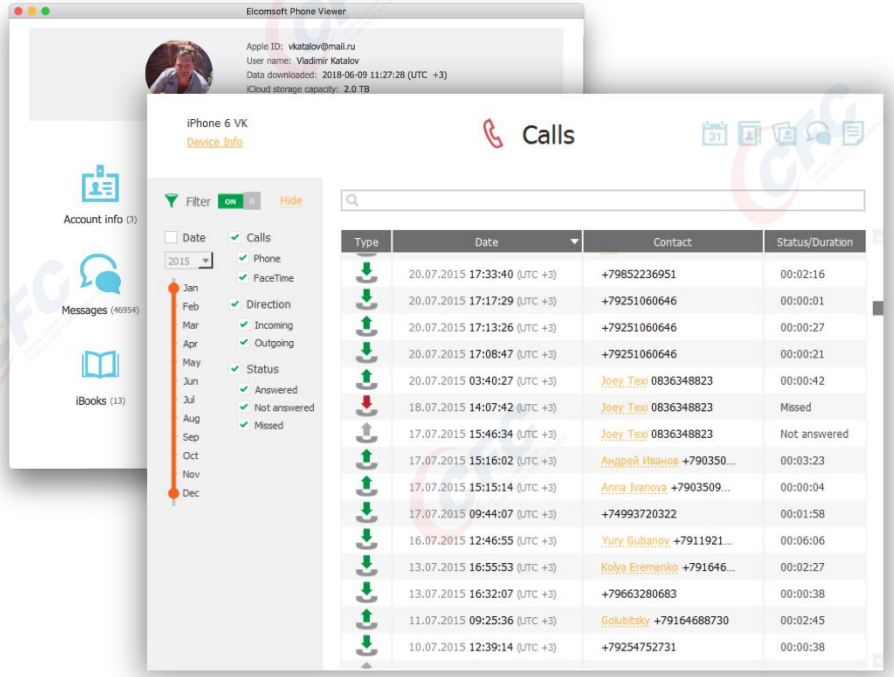
- **执行云提取和解密本地备份的单一工具**
- 密钥链提取和分析：查看和导出本地备份和iCloud密钥链中的密码
- 从iCloud中提取同步数据、备份和受保护的数据
- 包括未提供给执法部门或未通过隐私门户提供的信息



Apple: 分析数据

Elcomsoft Phone Viewer

- **一个用于查看本地和云备份、TAR映像的小型和轻量级工具**
- 比其他工具更容易使用
- 对于密钥链分析，使用Elcomsoft Phone Breaker



移动取证工具

本演示文稿中提到的工具

- Elcomsoft Phone Breaker
  通过离线和云备份获取； 破坏备份密码
- Elcomsoft Phone Viewer
  查看提取的磁盘映像、下载或解密的备份
- Elcomsoft Cloud Explorer
  从谷歌账户中提取和分析信息
- Elcomsoft Mobile Forensic Bundle
  包含以上所有内容以及70%的PC和Mac版本中的其他工具

智能手机隐私

Vladimir Katalov, ElcomSoft

Questions?