看雪

SDC·2019

2019 安全开发者峰会

Security
Development
Conference

基于云数据的司法取证技术

程勋德　万兴科技

目录

content

司法取证现状，常见取证技术及问题

司法取证新趋势 – 云取证

- **JTAG**
  - 许多设备上没有JTAG端口
  - 全磁盘加密使JTAG完全无用
- **物理读取**
  - 兼容性有限
  - 数据伪造问题
  - 也有全磁盘数据加密问题
- **普通读写**
  - 兼容性较好
  - 需要绕过屏幕锁定
  - 需要Root权限读写数据

云数据取证优缺点

优点

- ✓ 用户无感知
- ✓ 实时证据
- ✓ 同时从多个设备获取数据
- ✓ 能够访问到已删除数据
- ✓ 设备密码
- ✓ 云采集甚至适用于锁定设备
- ✓ 系统范围内的敏感数据存储（密钥，密码等）
- ✓ 设备损坏，擦除或锁定也能访问
- ✓ 无需访问物理设备
- ✓ 云数据日趋丰富，备份，同步，云盘。

缺点

- 不同的平台（苹果、谷歌、微软）
- 需要凭据（密码或Token）
- 二步验证问题
- 没有公开接口
- 私有接口及内部数据保护机制经常变化

移动云的生态系统

iCloud

存储在云中的完整备份(包括删除信息)

实时与iCloud同步的多种数据类型

Google Cloud

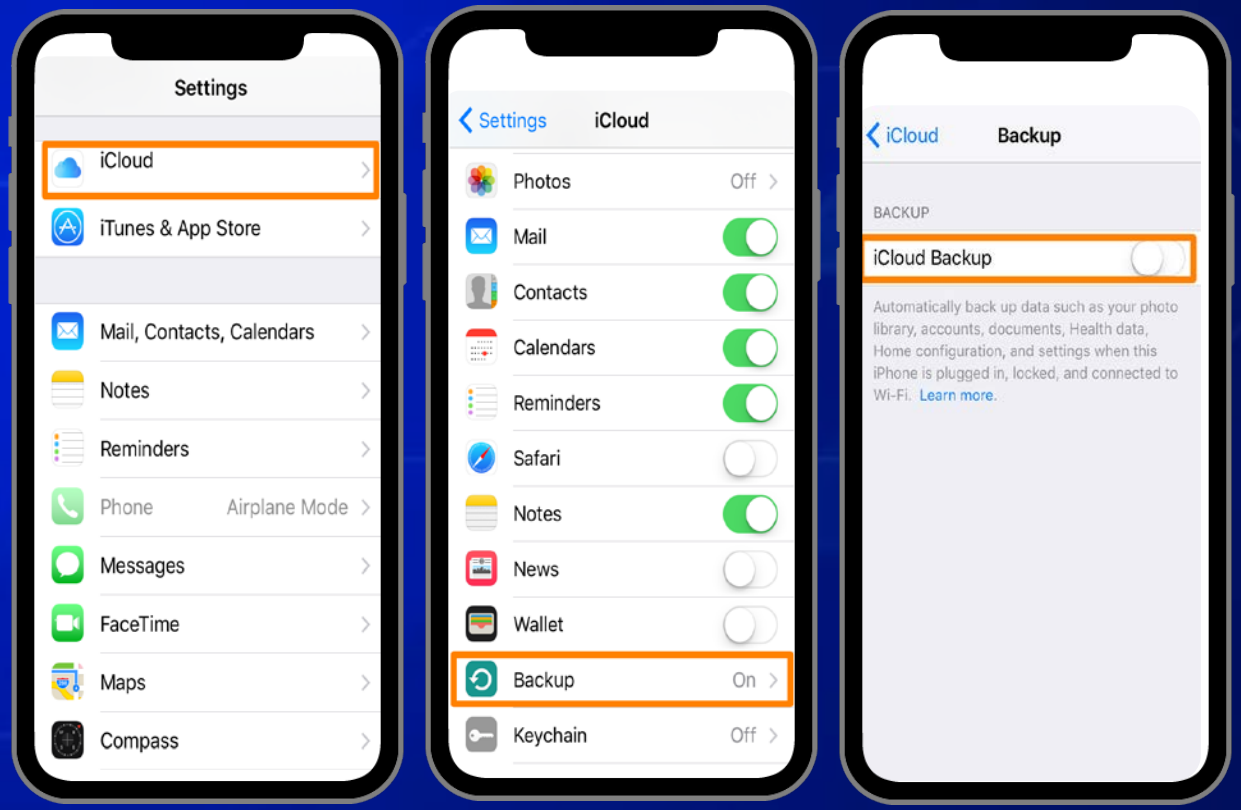
Google Cloud

Android备份几乎没用，但是...

谷歌账户包含大量同步数据

iCloud:备份

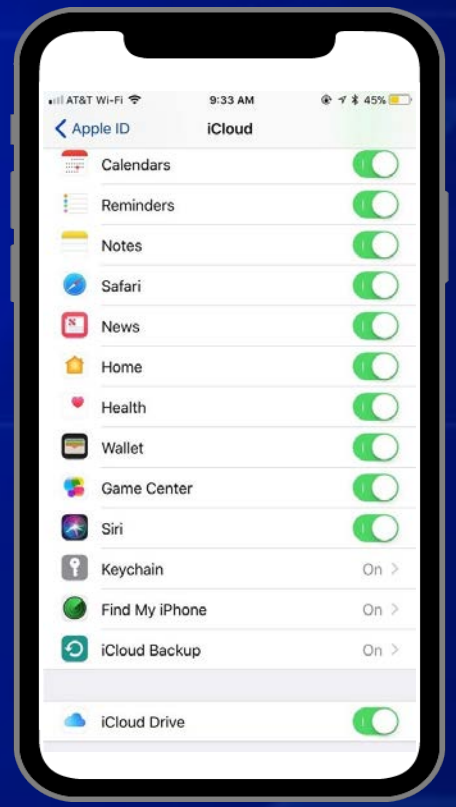
- 联系人和联系人收藏夹
- 消息(包括iMessage)
- 通话记录
- 应用数据
- 设备设置
- 相机胶卷（照片和视频） - 仅在没有iCloud照片库的情况下
- 购买（音乐，电影，电视，应用程序，书籍）
- 邮件帐户
- 网络设置（保存的Wi-Fi热点，VPN设置等）
- 配对蓝牙设备
- 脱机Web应用程序缓存/数据库
- Safari书签，Cookie，历史记录，离线数据
- 地理位置的历史和地点
- 密码（iCloud Keychain）
- 照片（iCloud照片库）
- 文档，备注，日历，查找我的手机等



使用iCloud控制面板无法下载完整数据(并且未同步到PC / Mac)，仍然可以使用适当的工具获得

iCloud:同步

- 日历、邮件、联系人
- 通话记录、备忘
- 健康数据、家庭、新闻、地图、Wi-Fi、iBooks
- 浏览历史，书签
- iOS 11.3:iMessage/短信息
- iCloud照片库：图片（EXIF可能包含位置）
- iCloud Keychain密码!
- 地图：我的地图，路线，已保存的地点，搜索
- Safari历史记录，所有同步设备上的打开选项卡，书签



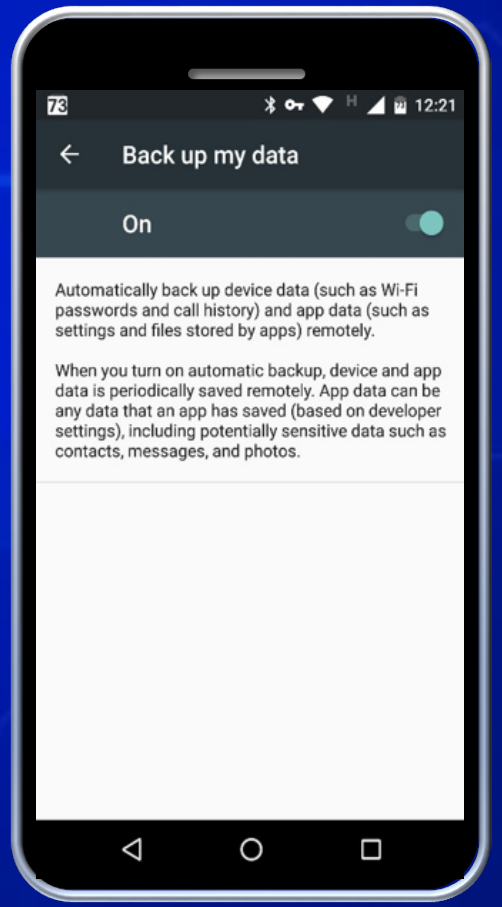
iCloud:结论

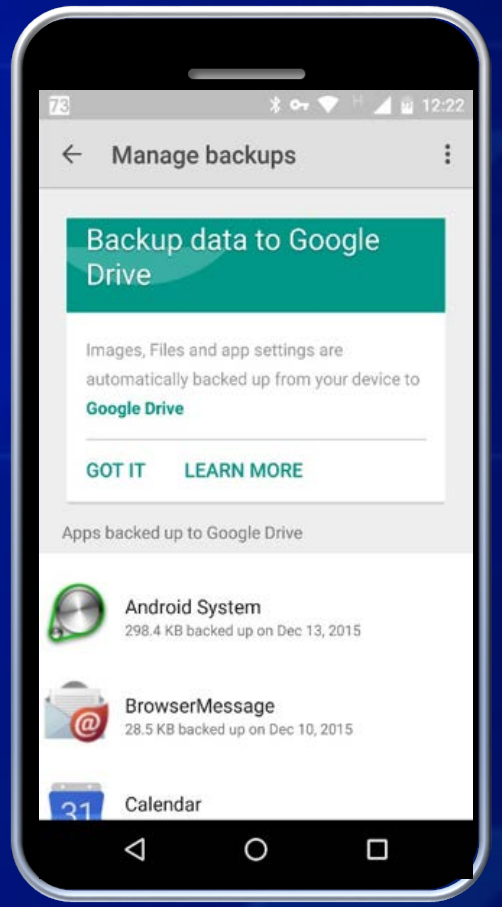
- 无需用户交互即可自动创建
- 备份包含大量数据
- 某些类型的数据实时同步
- 可以使用适当的工具进行采集
- 可以获取所有设备iPhone，iPad的数据，包括macOS X桌面

Google Cloud:备份

- Wi-Fi网络和密码
- 通过Google Play安装的应用
- 显示，语言，输入和其他设置
- 第三方应用设置和数据，

Android备份中的数据非常有限，亮点是同步...





Google Cloud:同步

- 联系人，日历
- 设备/浏览器和应用程序请求访问
- YouTube观看记录，搜索记录
- Location，历史位置记录
- 笔记，邮件
- 通话记录和短信（取决于Android版本）
- 专辑（照片/图片/视频）
- 环聊对话
- 手机中保存的WiFi

谷歌浏览器：搜索和浏览历史记录等等多达50种以上的数据

Google Cloud:结论

- Google Cloud备份中的数据非常有限
- Google帐户中的大量信息会实时同步

  可以获取浏览历史记录，YouTube历史记录，综合位置历史记录，邮件，备注，图片等。

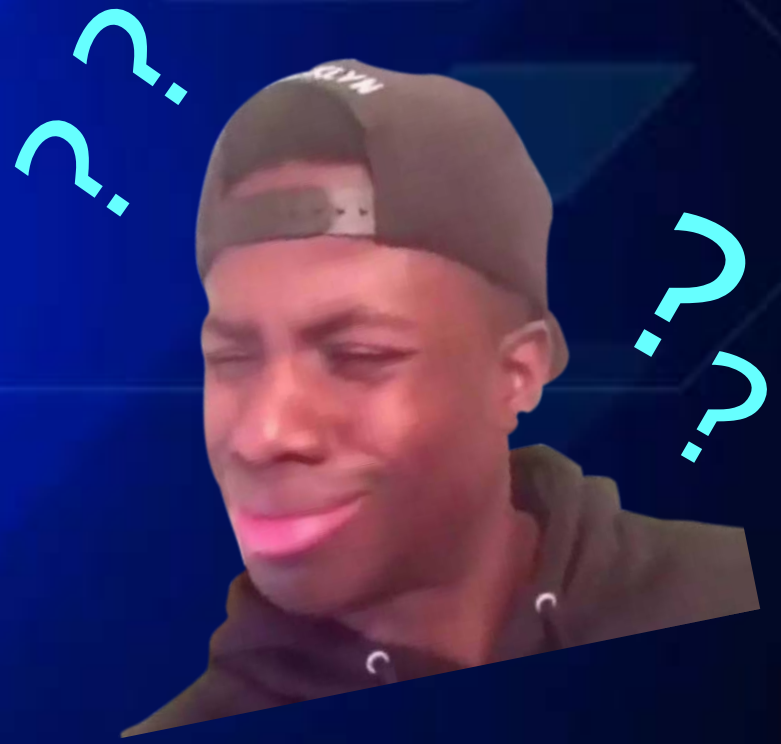
二步验证问题

- 保护对备份数据、Keychain的访问。
- 验证码发送到受信任的设备。
- 访问数据时发送电子邮件通知。

二步验证的解决方法： 使用来自设备、PC或Mac的历史应用Token

如何解决授权问题

- 社会工程学
- 浏览器缓存的密码
- 系统或应用程序保存的Token
- 提取macOS keychain
- 提取PC/macOS应用程序保存的Token
- 从本地iTunes备份中提取（带密码）



基于iCloud，Goole Cloud的典型应用

司法取证,数据恢复

司法取证

- 通过提取PC缓存中的Token或者macOS中的keychain
- 能够获取到用户无法感知甚至删除的很多数据。
- 还可以获得用户无法抵赖的时间相关数据。

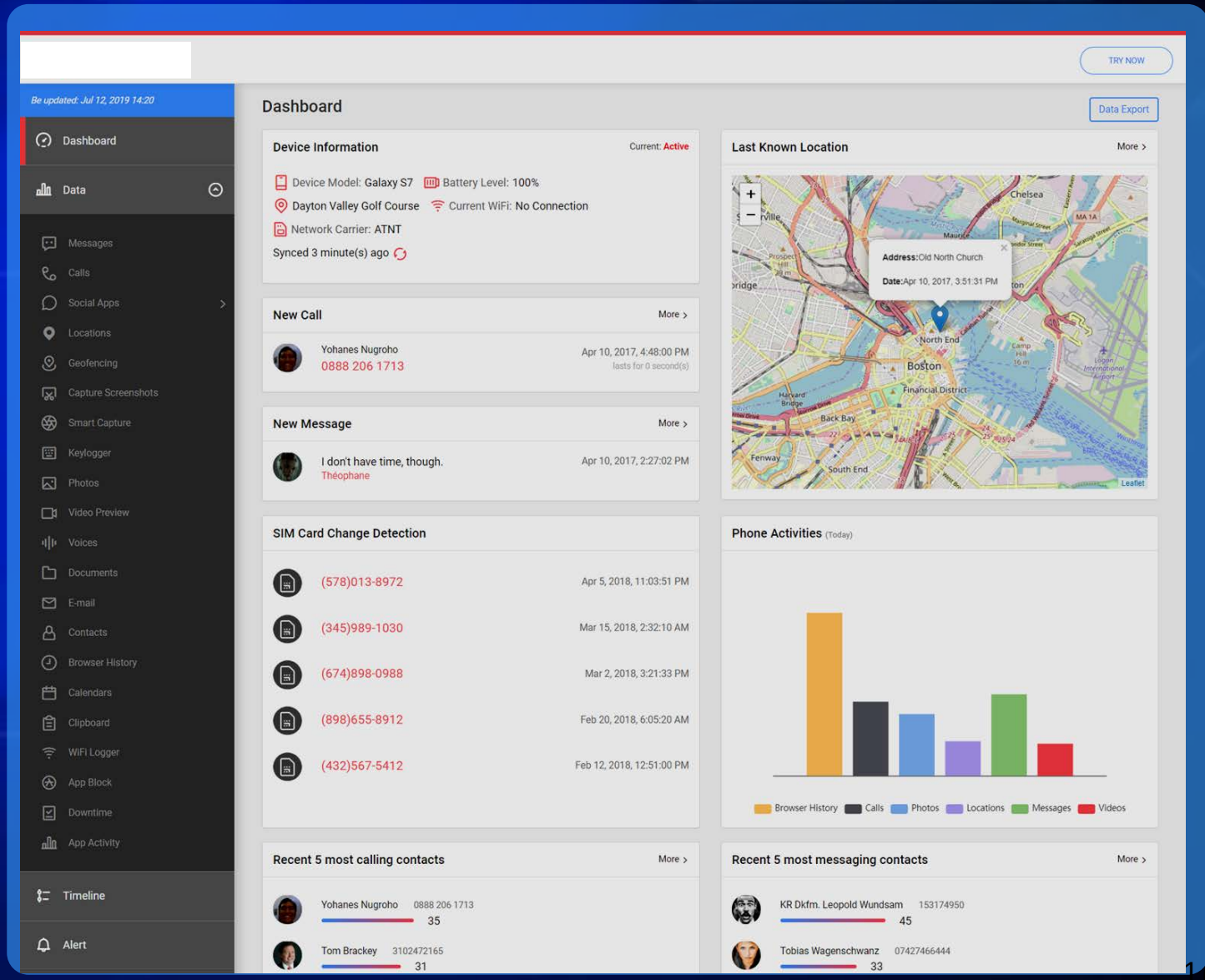
数据恢复

- 在用户授权的前提下，可以对iCloud或者Goolge Cloud备份进行分析，恢复删除的数据。
- 可以恢复联系人，通话记录，短信，邮件，照片，视频，社交应用聊天记录等等。

基于 Apple iCloud，Goole Cloud的典型应用

家长监控

- 通过Token能够获取用户的即时数据包括
  - 日历、邮件、联系人
  - 通话记录、备忘
  - 地图位置信息，Wi-Fi账号密码
  - 浏览历史，书签
  - 短信，照片(EXIF可能包含位置)
  - iCloud Keychain：密码
  - iOS 11.3:iMessage/短信息
  - 地图：我的收藏地图，路线，已保存的地点
  - 搜索记录，Safari历史记录，Chrome浏览记录。



实例讲解无密码获取iCloud数据

1. 提取系统登录密码(用户有一台PC或者Mac)

通过提取%WINDIR%目录下的SYSTEM SAM文件(Mac提取keychain文件)使用hashcat进行暴力枚举,提取用户密码,hashcat可以非常快速的枚举用户密码。

```
joen@ubuntu:~$ samdump2 SYSTEM SAM -o sam.hash
joen@ubuntu:~$
```

sam.hash (~/) - gedit

Open | Save

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:83c51742bc598fb6b24e30d140d8d65c:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

:83c51742bc598fb6b24e30d140d8d65c:::

Guess.Mask.....: ?1?1?1?1?1?1?1 [7]

```
Session.........: hashcat
Status..........: Running
Hash.Type.......: NTLM
Hash.Target.....: sam.hash
Time.Started.....: Fri Jul 05 15:49:06 2019 (31 secs)
Time.Estimated...: Fri Jul 05 15:54:54 2019 (5 mins, 17 secs)
Guess.Mask.....: ?1?1?1?1?1?1?1 [7]
Guess.Charset....: -1 ?l?u?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 10103.7 MH/s (7.69ms) @ Accel:128 Loops:64 Thr:1024 Vec:1
Recovered.....: 0/2 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 310614425600/3521614606208 (8.82%)
Rejected.....: 0/310614425600 (0.00%)
Restore.Point....: 79953920/916132832 (8.73%)
Restore.Sub.#1...: Salt:0 Amplifier:2432-2496 Iteration:0-64
Candidates.#1....: 2d4fTP5 -> heQdyU5
Hardware.Mon.#1..: Temp: 68c Fan: 47% Util: 89% Core:1949MHz Mem:3802MHz Bus:16

83c51742bc598fb6b24e30d140d8d65c:Luck019
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => |
```

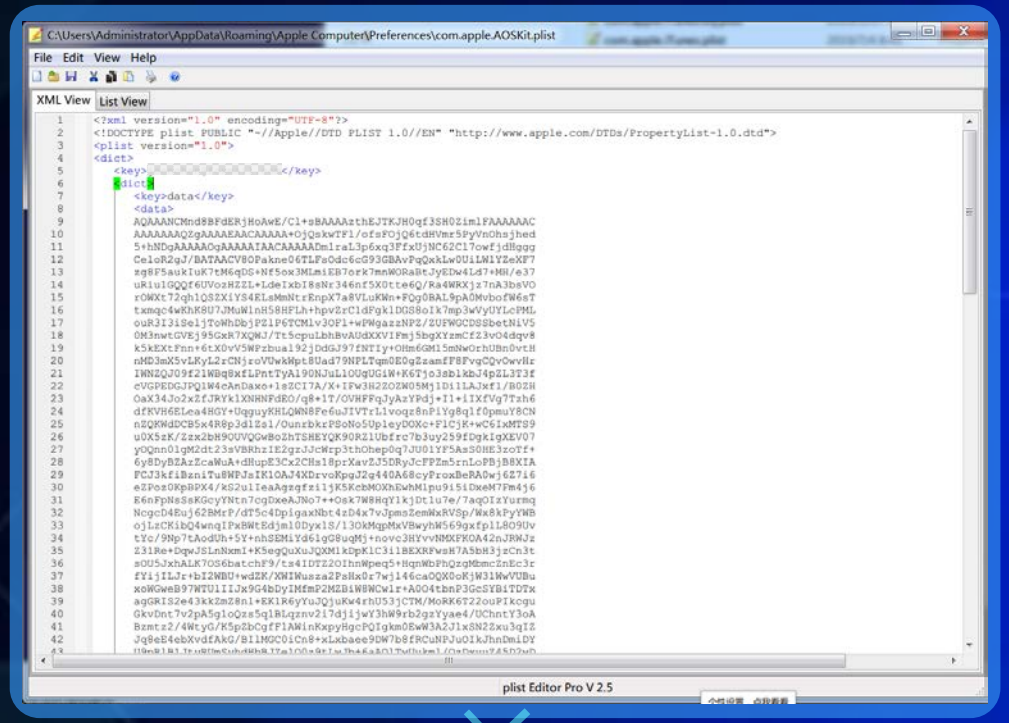
83c51742bc598fb6b24e30d140d8d65c:Luck019

icloud_token_2019-07-06 06/47/19 +0000.plist

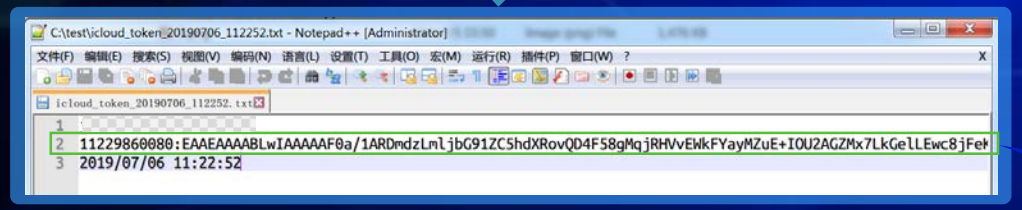
icloud_token_2019-07-06 06:47:19 +0000.plist 〉No Selection

Key	Type	Value
▼ Root	Dictionary	(5 items)
apple_id	String	huloves@foxmail.com
atex_version	String	1.4
auth_token_with_limitations	String	459067826:EAADAAAABLwIAAAAAF0CAsERDmdzLmljbG91ZC5hdXRovQAX9wZqVS4FDxKrNGNoroM+3o+AoBLbkj
ctoken	String	MDAwNjc2LTEwLTZmODQ3YTA2LTYzYzItNDM2Mi1iN2U0LTIwMzUzZjg0ODU2ZjoyNzNmYjQ0MDQ0YWQ2M2UzMW
date	String	2019-07-06 06:47:19 +0000

实例讲解无密码获取iCloud数据



提取出



2. 得到系统登录密码，通过算法提取mmeAuthToken

从用户安装的苹果系App中提取加密

mmeAuthToken，%appdata%\Apple Computer\Preferences\目录中提取com.apple.AOSKit.plist文件进行解密，解密算法和平台,登录用户相关，Win上面调用CryptUnprotectData解密出mmeAuthToken。

```
11229860080:EAAEAAAABLwIAAAAAF0a/1ARDmdzLmljbG91ZC5hdXRovQD4F58gMqjRHVvEWkFYayMZuE+IOU2AGZMx7LkGelLEwc8jFeK
```

实例讲解无密码获取iCloud数据

3、 得到mmeAuthToken之后就可以使用该Token，去请求iCloud服务Token，和账户信息。

```
<udid>96cc51b8fce3428493482ab19808d3a9ccb0ec2e</udid>
```

```
<key>protocolVersion</key>
<string>3</string>

<key>tokens</key>
<dict>
        <key>mmeAuthToken</key>
        <string>AQAAAABdIr0vWO7NX537KhjW6W0QhPiYvpZG1FQ=</string>

        <key>mmeFMFToken</key>
        <string>AQAAAABdIr0zYp3f9AUv0HYbpOCMxMV2TkG3H_0~</string>

        <key>mmeFMIPToken</key>
        <string>AQAAAABdIr0zZSL3zClnF-BFtOM06AwwMlILTnQ~</string>

        <key>mapsToken</key>
        <string>AQAAAABdIr0zqbega3zGlzV2WQup2c8ViTn0BUY~</string>

        <key>mmeFMFAppToken</key>
        <string>AQAAAABdIr0zbedsXNKaNSpybrSgxiDKQeltiOA~</string>

        <key>cloudKitToken</key>
        <string>ATS3_AQAAAABdIr0zc_k8psUYnvINHjmcJoAUUcY_7aM~</string>

</dict>

<key>appleAccountInfo</key>
<dict>
        <key>lastName</key>
        <string>itransfer</string>
```

<key>mmeAuthToken</key>

<key>cloudKitToken</key>

```
<BackupInfo>
  <DeviceInfo>
    <udid>96cc51b8fce3428493482ab19808d3a9ccb0ec2e</udid>
    <type>iPhone 8</type>
    <SnapshotInfo>
      <last_backup_time>2019-1-17 10:4:3</last_backup_time>
      <device_name>Boz的 iPhone</device_name>
      <size>1018384409</size>
      <os_version>12.1.2</os_version>
      <is_complete>1</is_complete>
    </SnapshotInfo>
    <SnapshotInfo>
      <last_backup_time>2019-1-21 2:4:42</last_backup_time>
      <device_name>Boz的 iPhone</device_name>
      <size>8284676</size>
      <os_version>12.1.2</os_version>
      <is_complete>1</is_complete>
    </SnapshotInfo>
  </DeviceInfo>
</BackupInfo>
```

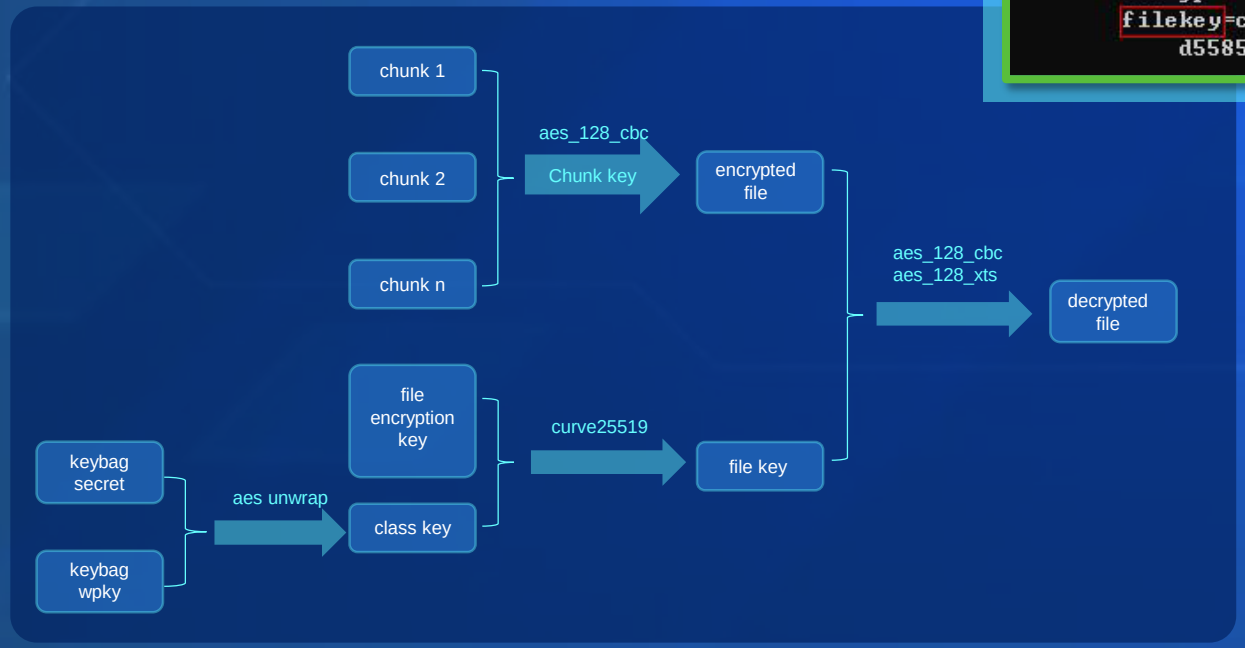
实例讲解无密码获取iCloud数据

4、通过iCloud服务Token和账户信息就可以获取用户数据。

iCloud 备份加密使用公开密钥算法中的椭圆曲线算法中的 Curve25519 曲线生成密钥。遵循 Diffie–Hellman 椭圆曲线密钥交换规则。

```
>>> FILE - F:A26D017D-19E3-448E-BCFA-0C6E4C5D5FBC:ZKSxMWoLqUdNLQOc7TGUVRIAAOY=:2278224:+Tv2
    * Keybag
        secret - 1c3bb179ae0dd6d614ff68f05ba3f56403676214df3887ba6a8030db3d61d64f
        wpky - de5fcb074bb1abefb70d320176df72be561feba8ac98f99bffb52bb330da502035d6d2a3a798a8b8
        classkey=aes_unwrap(secret, wpky) :
            b1e4205c39d68ed3a8550dcd68af164fa70ddebbd32c950348e7cd6412256ccd

    * File
        encryptionkey - 0638e9a7ddf1498b819f82fb7e20564e00000000000008467d0000000301010001 ...
        filekey=curve25519(classkey, encryptionkey) :
            d55856b4376f1ac96d2aa8be2ac8b1c661deb6be646a06d3...
```



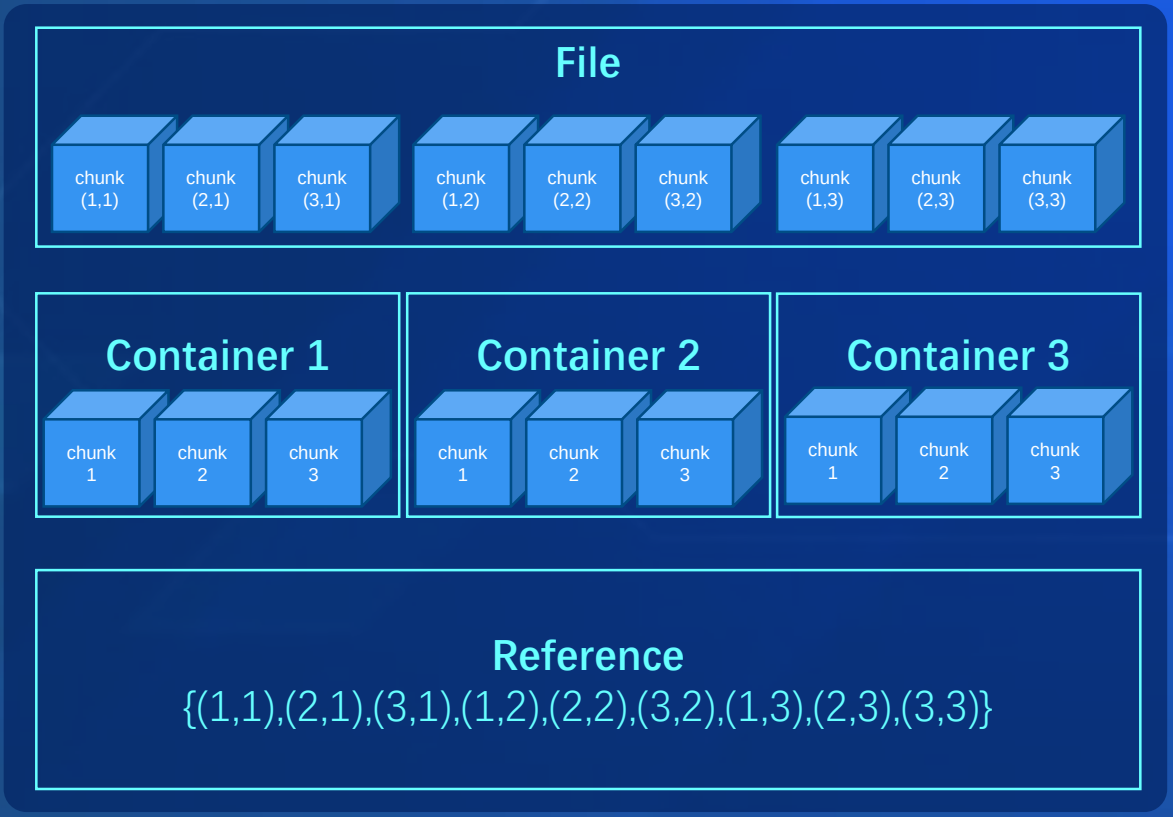

```
>>> FILE - F:A26D017D-19E3-448E-BCFA-0C6E4C5D5FBC:ZKSxMWoLqUdNLQOc7TGUVRIAAOY=:2278224:+Tv2
    * Keybag
        secret - 1c3bb179ae0dd6d614ff68f05ba3f56403676214df3887ba6a8030db3d61d64f
        wpky - de5fcb074bb1abefb70d320176df72be561feba8ac98f99bffb52bb330da502035d6d2a3a798a8b8
        classkey=aes_unwrap(secret, wpky) :
            b1e4205c39d68ed3a8550dcd68af164fa70ddebbd32c950348e7cd6412256ccd

    * File
        encryptionkey - 0638e9a7ddf1498b819f82fb7e20564e00000000000008467d0000000301010001 ...
        filekey=curve25519(classkey, encryptionkey) :
            d55856b4376f1ac96d2aa8be2ac8b1c661deb6be646a06d3...
```

实例讲解无密码获取iCloud数据

5、 文件组织信息。

用户在 iCloud 存储的每个文件都被分成若干个块，每一块使用 128 位密钥的 AES 加密算法进行加密，每个 128 位的密钥根据文件块的内容生成。

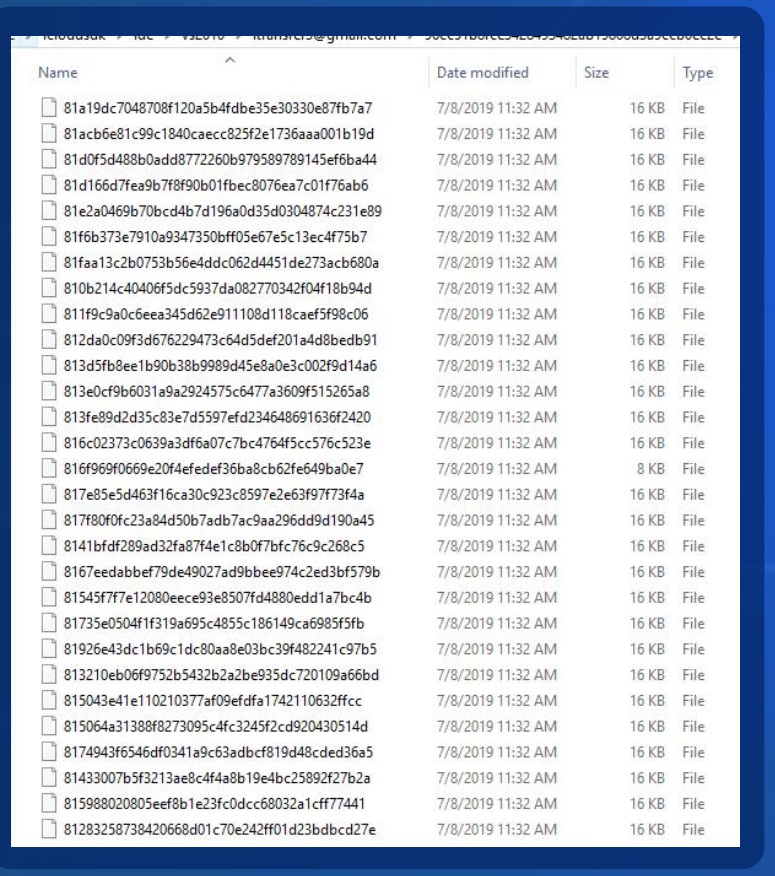



```
Container 0 (edge-007.hkhkg-2.icloud-content.com/eK_cwG0BaFtCICEA-Llx?x-client-request-id=d3af3d07-5a49-4343-842 ...)
    chunk 0 - 816c02373c0639a3df6a07c7bc4764f5cc576c523e
    chunk 1 - 812da0c09f3d676229473c64d5def201a4d8bedb91
    chunk 2 - 8167eedabbef79de49027ad9bbee974c2ed3bf579b
    chunk 3 - 816f969f0669e20f4efedef36ba8cb62fe649ba0e7
Container 1 (edge-007.hkhkg-2.icloud-content.com/U85o_4kBaIf3Q3MA-Lly?x-client-request-id=d3af3d07-5a49-4343-842 ...)
    chunk 0 - 813210eb06f9752b5432b2a2be935dc720109a66bd
    chunk 1 - 8141bfdf289ad32fa87f4e1c8b0f7bfc76c9c268c5
    chunk 2 - 810b214c40406f5dc5937da082770342f04f18b94d
    chunk 3 - 81926e43dc1b69c1dc80aa8e03bc39f482241c97b5
    chunk 4 - 81433007b5f3213ae8c4f4a8b19e4bc25892f27b2a
    chunk 5 - 815064a31388f8273095c4fc3245f2cd920430514d
    chunk 6 - 81735e0504f1f319a695c4855c186149ca6985f5fb
    chunk 7 - 81faa13c2b0753b56e4ddc062d4451de273acb680a
    chunk 8 - 81e2a0469b70bcd4b7d196a0d35d0304874c231e89
    chunk 9 - 81d0f5d488b0add8772260b979589789145ef6ba44
    chunk 10 - 817e85e5d463f16ca30c923c8597e2e63f97f73f4a
    chunk 11 - 813e0cf9b6031a9a2924575c6477a3609f515265a8
    chunk 12 - 815988020805eef8b1e23fc0dcc68032a1cff77441
    chunk 13 - 81acb6e81c99c1840caecc825f2e1736aaa001b19d
    chunk 14 - 815043e41e110210377af09efdfa1742110632ffcc
    chunk 15 - 81f6b373e7910a9347350bff05e67e5c13ec4f75b7
    chunk 16 - 811f9c9a0c6eea345d62e911108d118caef5f98c06
    chunk 17 - 8128325873842066 8d01c70e242ff01d23bdbcd27e
    chunk 18 - 813d5fb8ee1b90b38b9989d45e8a0e3c002f9d14a6
    chunk 19 - 81545f7f7e12080eece93e8507fd4880edd1a7bc4b
    chunk 20 - 81d166d7fea9b7f8f90b01fbec8076ea7c01f76ab6
    chunk 21 - 8174943f6546df0341a9c63adbcf819d48cded36a5
    chunk 22 - 817f80f0fc23a84d50b7adb7ac9aa296dd9d190a45
    chunk 23 - 813fe89d2d35c83e7d5597efd234648691636f2420
    chunk 24 - 81a19dc7048708f120a5b4fdbe35e30330e87fb7a7
Reference
[0,0] [0,1] [1,0] [2,0] [1,1] [2,1] [3,1] [4,1] [5,1] [6,1] [7,1]
[8,1] [9,1] [10,1] [11,1] [12,1] [13,1] [14,1] [15,1] [16,1] [17,1]
[18,1] [19,1] [20,1] [21,1] [22,1] [23,1] [24,1] [3,0]
```

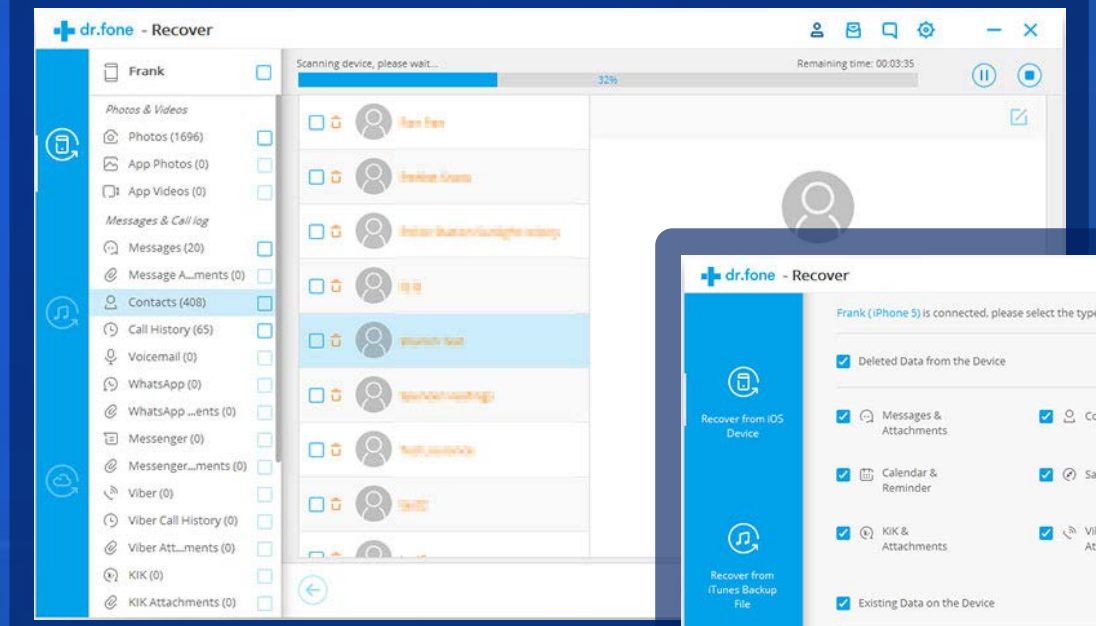
实例讲解无密码获取iCloud数据

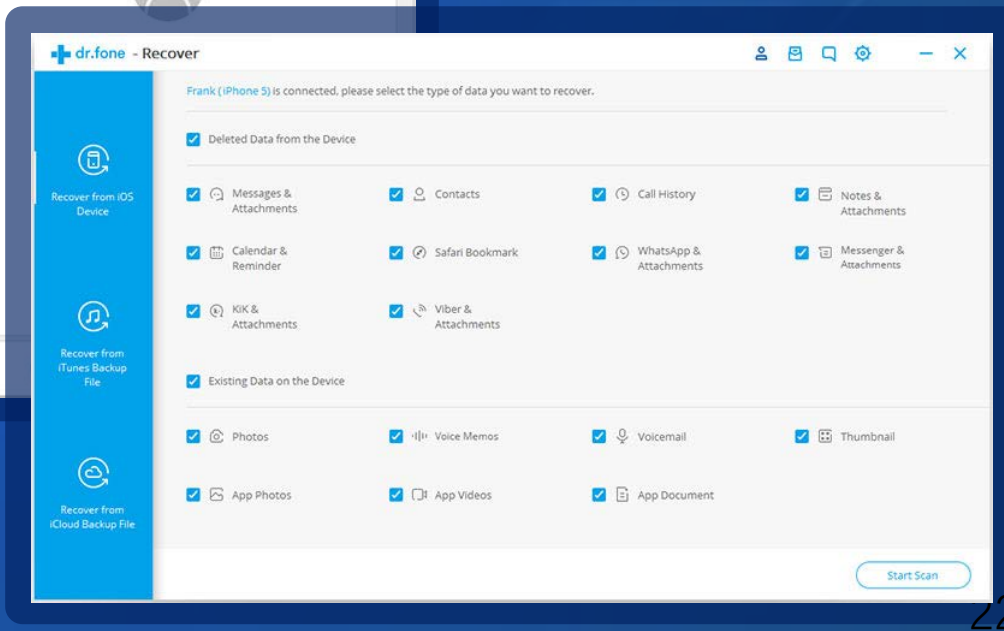
6、 最终文件

通过解析Container和chunk按照Reference组织得到最终的文件列表。



Name	Date modified	Size	Type
81a19dc7048708f120a5b4fdbe35e30330e87fb7a7	7/8/2019 11:32 AM	16 KB	File
81acb6e81c99c1840caecc825f2e1736aaa001b19d	7/8/2019 11:32 AM	16 KB	File
81d0f5d488b0add8772260b979589789145ef6ba44	7/8/2019 11:32 AM	16 KB	File
81d166d7fea9b7f8f90b01fbec8076ea7c01f76ab6	7/8/2019 11:32 AM	16 KB	File
81e2a0469b70bcd4b7d196a0d35d0304874c231e89	7/8/2019 11:32 AM	16 KB	File
81f6b373e7910a9347350bff05e67e5c13ec4f75b7	7/8/2019 11:32 AM	16 KB	File
81faa13c2b0753b56e4ddc062d4451de273acb680a	7/8/2019 11:32 AM	16 KB	File
810b214c40406f5dc5937da082770342f04f18b94d	7/8/2019 11:32 AM	16 KB	File
811f9c9a0c6eea345d62e911108d118caef5f98c06	7/8/2019 11:32 AM	16 KB	File
812da0c09f3d676229473c64d5def201a4d8bedb91	7/8/2019 11:32 AM	16 KB	File
813d5fb8ee1b90b38b9989d45e8a0e3c002f9d14a6	7/8/2019 11:32 AM	16 KB	File
813e0cf9b6031a9a2924575c6477a3609f515265a8	7/8/2019 11:32 AM	16 KB	File
813fe89d2d35c83e7d5597efd234648691636f2420	7/8/2019 11:32 AM	16 KB	File
816c02373c0639a3df6a07c7bc4764f5cc576c523e	7/8/2019 11:32 AM	16 KB	File
816f969f0669e20f4efedef36ba8cb62fe649ba0e7	7/8/2019 11:32 AM	8 KB	File
817e85e5d463f16ca30c923c8597e2e63f97f73f4a	7/8/2019 11:32 AM	16 KB	File
817f80f0fc23a84d50b7adb7ac9aa296dd9d190a45	7/8/2019 11:32 AM	16 KB	File
8141bfdf289ad32fa87f4e1c8b0f7bfc76c9c268c5	7/8/2019 11:32 AM	16 KB	File
8167eedabbef79de49027ad9bbee974c2ed3bf579b	7/8/2019 11:32 AM	16 KB	File
81545f7f7e12080eece93e8507fd4880edd1a7bc4b	7/8/2019 11:32 AM	16 KB	File
81735e0504f1f319a695c4855c186149ca6985f5fb	7/8/2019 11:32 AM	16 KB	File
81926e43dc1b69c1dc80aa8e03bc39f482241c97b5	7/8/2019 11:32 AM	16 KB	File
813210eb06f9752b5432b2a2be935dc720109a66bd	7/8/2019 11:32 AM	16 KB	File
815043e41e110210377af09efdfa1742110632ffcc	7/8/2019 11:32 AM	16 KB	File
815064a31388f8273095c4fc3245f2cd920430514d	7/8/2019 11:32 AM	16 KB	File
8174943f6546df0341a9c63adbcf819d48cded36a5	7/8/2019 11:32 AM	16 KB	File
81433007b5f3213ae8c4f4a8b19e4bc25892f27b2a	7/8/2019 11:32 AM	16 KB	File
815988020805eef8b1e23fc0dcc68032a1cff77441	7/8/2019 11:32 AM	16 KB	File
81283258738420668d01c70e242ff01d23bdbcd27e	7/8/2019 11:32 AM	16 KB	File





如何保护个人数据

- 关闭iCloud同步，Google Cloud同步
- 注意开启二步验证
- 不要在陌生电脑登录iCloud账号，Chrome账号

谢大家的聆听!

同时感谢公司的支持和彭重阳的协助

万兴科技