cellebrite
delivering mobile expertise

UFED TOUCH

高性能设备之高性能解决方案

UFED Touch 是一套综合的移动取证解决方案，让调查人员能够有效地对移动设备数据做提取、解码和分析。UFED Touch 拥有直观的触控界面和一体式电池，旨在提高使用速度和可用性，增强便携性，从而轻松应用于现场和后台研究。

UFED Touch 提供旗舰版或逻辑版，配备配套的软件、外围设备和附件。

概览

UFED Touch 定义了移动取证领域的行业标准，为调查人员提供最先进的功能：

- 可对证据数据进行深层的物理提取、文件系统提取、密码提取和逻辑提取
- 全面支持最广泛的移动设备类型
- 专有的技术和引导程序确保取证有效性
- 全面的即开即用工具包——提供紧凑排列的多种转接头和4条主连接线，方便用户提取数据，并可在使用过程中充电
- 支持触摸屏操作，用户界面直观简洁
- 使用 HTML 报告查看器在屏幕上查看提取报告
- 短周期软件同步更新，兼容新上市的新款手机

解决方案版本

UFED Touch 提供旗舰版和逻辑版，标配版也提供配套的应用软件，能够进行深层解码、分析和报告。

旗舰版解决方案的功能包括：

- 绕过图形锁/密码/PIN 码对 Android 安卓设备进行物理提取和解码，支持机型包括 Samsung 三星 Galaxy S 系列、LG、HTC 和 Motorola 摩托罗拉等
- 对运行 OS 4.2 – 4.4.3 系统的 Android 安卓设备进行物理提取、文件系统提取和解码
- 对运行 OS 4 – 7 系统的 BlackBerry® 黑莓设备进行物理提取并独家解码：BBM 数据、应用程序、电子邮件和蓝牙等
- 可对 Apple 设备广泛提取和解码
- 对被锁的 Nokia BB5 设备进行物理提取和解码——提取部分设备密码
- 绕过、显示或禁用用户锁代码，自由访问被锁设备
- 对运行 OS 8.0 – 8.1 系统的 Windows Phone 设备进行物理提取
- 对任何 Windows Phone、HTC、Samsung 三星、华为和中兴手机进行文件系统提取
- 从设备闪存的未分配空间恢复更多已删除数据
- 对各种 JTAG 物理提取数据进行解码
- TomTom® 旅行日志解密，对其他便携式 GPS 设备进行数据提取
- 可解密 WhatsApp 加密历史数据库
- 丰富的解码功能：针对应用程序数据、密码、电子邮件、通话记录、短信、联系人、日历、媒体文件、位置信息等。
- UFED Physical Analyzer 提供全面的分析功能，包括时间轴、项目分析、恶意软件检测和监视列表
- 使用 UFED Physical Analyzer 生成简单易读的各种格式的报告
- 使用 UFED Physical Analyzer 的离线翻译解决方案处理提取数据中的外文内容

逻辑版解决方案的功能包括：

- 逻辑数据提取：应用程序数据、密码、IM(即时消息)、联系人、短信和彩信、电子邮件、日历、多媒体、通话记录、手机详细信息(IMEI/ESN)、ICCID 和 IMSI、SIM 位置信息(TMIS、MCC、MNC、LAC)
- 克隆 SIM 卡 ID，以便在分析过程中将手机与网络活动隔离开来
- 短周期软件同步更新，兼容新上市的新款手机

随时携带使用

UFED Touch 配备全包式标准型或加固型移动取证工具包，其中包含各种外围设备和附件。配备轻量型数据线、手机转接头、带嵌入式工作台的加固型携带箱、一体式超长续航电池和外接硬盘，让用户更快、更轻松、更高效地进行移动调查。

UFED CAMERA

UFED Camera 是一项证据收集工具，使调查人员可拍摄数据照片或直接从设备中屏幕截图，手动收集证据。

通过以下方式加快案件调查：

- 在数据无法提取时，拍摄有关设备的图像/视频作为证据
- 在 UFED 中添加图像类别和描述，以便生成报告

UFED Camera 是旗舰版解决方案的标准配置，在逻辑版解决方案中作为附加装置提供

Cellebrite 简介

Cellebrite 是一家全球领先企业，提供先进的移动取证解决方案。Cellebrite 通过 UFED Pro 和 UFED Field 系列为现场调查和后台研究提供灵活且经实战检验的创新型跨平台解决方案。

公司的 Universal Forensic Extraction Device (UFED) 综合解决方案旨在应对发掘现代移动设备中所存储的海量数据带来的挑战。UFED 系列能够对智能手机、传统和功能手机、便携式 GPS 设备、平板电脑、存储卡和中国芯片组手机等数以千计移动设备中的数据进行提取、解码、分析并生成报告。UFED 系列已部署于全球100多个国家，部署量超过30,000台，是执法、军事、情报、企业安全及电子发现领域取证专家的首选工具。

Cellebrite 成立于1999年。

UFED TOUCH

应用软件

- UFED Physical Analyzer*
- UFED Logical Analyzer
- UFED Reader
- UFED Phone Detective

硬件

- UFED Touch 设备
- 坚固的 UFED 保护箱
- 转接头和连接线
- 转接头和连接线管理工具
- UFED 电源
- 标准携带箱
- 加固型携带箱*
- 嵌入式工作台*
- UFED Touch 屏幕罩*
- 法拉第袋*
- UFED 外接硬盘*
- UFED 读卡器
  - 集成 SIM 卡适配器
  - SIM ID 克隆卡
  - 微型 SIM ID 克隆卡
  - 纳米 SIM ID 克隆卡
- 车载充电适配器
- UFED 电脑连接线
- 手机充电线
- USB 闪存驱动器
- 5V 至 6V 直流适配器
- 手机连接器清洁刷
- UFED Camera**

*仅加固版提供
**旗舰版提供

欲了解更多信息,请访问

www.cellebrite.com **sales@cellebrite.com**

cellebrite
delivering mobile expertise

cellebrite
delivering mobile expertise

UFED优势

随着移动设备数量的不断增多，移动设备数据的容量及复杂程度也与日俱增。快速及时地部署恰当的移动取证工具以快速提取数据从未变得如此重要。

Cellebrite值得信赖的技术可提供市面上最综合的移动取证提取与解码功能，支持来自所有领先智能手机平台的19,000多种设备文件，这些平台包括Android、iOS、BlackBerry®、Windows Phone、传统和功能手机、便携式GPS设备、平板电脑、内存卡和采用中国国产芯片组制造的手机。

Cellebrite独特的技术功能针对现场和研究室进行了优化，可从任何替代方案中脱颖而出。

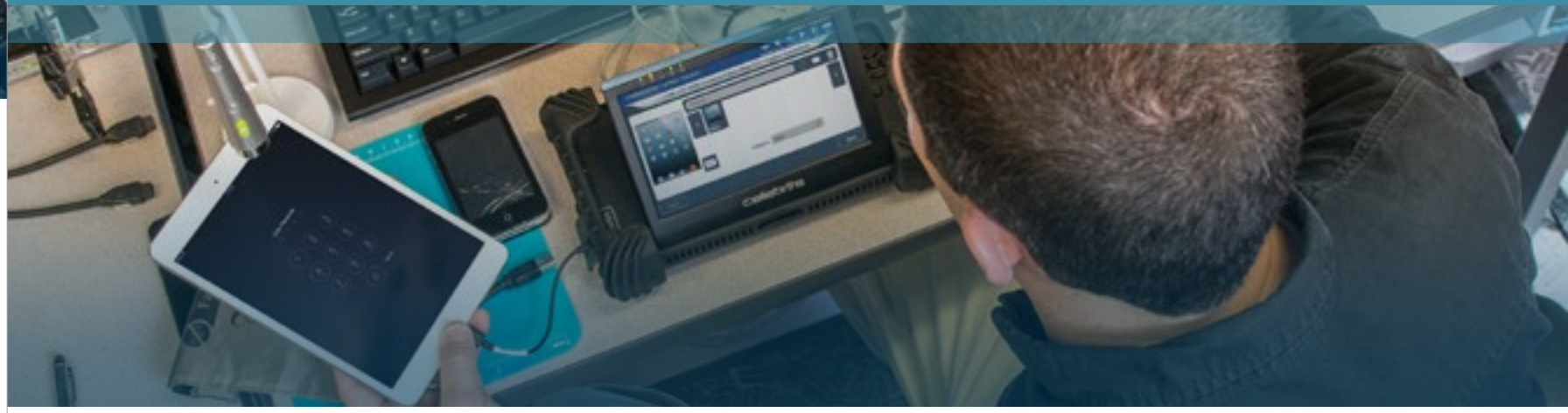
设备支持

- 每年约发布10个版本。
- 每个版本均新增上百种新支持的设备配置文件。
- 新版本经常增加针对新操作系统版本的支持。
- 所有的支持型号均经过Cellebrite检验。
  Cellebrite支持的设备列表并非基于其他来源，而是始终通过Cellebrite研发团队所开展的测试进行验证。

应用程序支持

- Cellebrite支持最广泛的应用程序，包括已删除数据。
- Cellebrite支持1,528个应用程序版本（iOS、Android、BlackBerry和Windows phone 8）。
- Cellebrite独特的解密解决方案支持 以下第三方应用程序：KeepSafe、微信、 Snapchat、Line、 TextSecure、 KakaoTalk、 TigerText、Facebook、Wickr和BBM。
- Cellebrite运用独特的雕复算法来恢复未分配空间的应用程序数据。

UFED提取优势



使用引导加载程序方法进行物理提取，可绕过设备锁

Cellebrite在业内首开先河，可在绕过各种移动设备的密码、通行码和格式锁的同时支持物理提取。该功能支持超过3200种不同的移动设备类型，包括800多种被受青睐的Android设备，如三星（包括预付费）、摩托罗拉、华为、LG、HTC、LG和三星智能手表、苹果、Windows Phone（诺基亚Lumia），等等。

Cellebrite独特的引导加载程序方法支持物理提取并具有设备锁绕过功能，可支持在三星Android设备上运行Android 5.x的最新电话固件。

UFED优势

独家的物理提取功能，可绕过密码，适用于三星Android设备（芯片集与型号），包括：

芯片组	型号
Samsung Android：Qualcomm MSM8674/ APQ8060	SM-N9009 Galaxy Note 3、SGH-T989 Galaxy S II、SGH-T989D Galaxy S II、SGH-i727 Galaxy S II Skyrocket
Samsung Android：Qualcomm Snapdragon 400 MSM8226 / 800 MSM8974 / 801 MSM8974 / 805 APQ8084	SM-G710 Galaxy Grand 2、SM-G7102 Galaxy Grand 2、SM-G7106 Galaxy Grand 2、GT-i9506 Galaxy S4、SM-N900V Galaxy Note 3、SM-P605V Galaxy Note 10.1、GT-i9506 Galaxy S4、SM-N900V Galaxy Note 3、SM-P605V Galaxy Note 10.1、SM-G870W Galaxy S5 Active、SM-G900P Galaxy S5、SM-G860P Galaxy S5 Sport、SM-N910V Galaxy Note 4、SM-N915P Galaxy Note Edge、SM-G901F Galaxy S5 Plus
Samsung Android：Samsung S3C64xx	GT-I5700 Galaxy Spica、SPH-M920 Transform、SCH-R880 Acclaim
Samsung Android：Samsung Exynos 5 Octa 5410	GT-i9500 Galaxy S4、SHV-E300S Galaxy S4、SHV-E300K Galaxy S4
Samsung Android：ST-Ericsson Novathor U8500	GT-i9070 Galaxy S Advance、GT-i8530 Galaxy Beam、GT-i9070 Galaxy S Advance
Samsung Android：TI OMAP4430 / OMAP4460	GT-P3100 Galaxy Tab 2 7.0、GT-P5100 Galaxy Tab 10.1、GT-P3110 Galaxy Tab 2 7.0、GT-i9250 Galaxy Nexus、SPH-L700 Galaxy Nexus、SCH-i515 Galaxy Nexus
Samsung Android：Broadcom 21553 /21654/28155/21664	GT-S5839i Galaxy Ace、GT-B5512 Galaxy Y Pro Duos、GT-S5360T Galaxy Y、GT-S7562C Galaxy Trend Duos、GT-S6790 Galaxy Fame Lite、SM-G350 Galaxy Core Plus、GT-S7580 Galaxy Trend Plus、GT-I9082 Galaxy Grand、GT-I9082i Galaxy Grand Duos、I9105P Galaxy S II Plus
Samsung Bada	GT-S5253 Wave 525、GT-S7250 Wave M、GT-S8530 Wave II
Samsung Android：QC8960	SHV-E400S Galaxy Golden、SM-S975L Galaxy S4,GT-I9158 Galaxy Mega、GT-i9230 Galaxy Golden、GT-i9235 Galaxy Golden、GT-i9508 Galaxy S4、GT-N7108D Galaxy Note II、SGH-i337M Galaxy S4、SCH-R530C Galaxy S III、SPH-L720T Galaxy S4、Samsung GT-I9152 Galaxy Mega 5.8、Samsung SCH-R890 Galaxy S4 Mini、Samsung SGH-M819N Galaxy Mega、Samsung GT-S5831i Galaxy Ace、Samsung GT-I9507V Galaxy S4、Samsung SPH-L520 Galaxy S4 Mini
Samsung Android：APQ8084	SM-N910V/P/T/F Galaxy Note 4、SM-N915V/P Galaxy Note Edge、SM-N910W8 Galaxy Note 4、SM-N9108V Galaxy Note 4、SM-G906L/S/K Galaxy S5

独家的物理提取功能，可绕过密码，适用于摩托罗拉Android设备，包括：

- Nvidia Tegra 2：MB867 Milestone X2、MB870 Droid X2、MB860 Atrix 4G。
- TI OMAP 3xxx (3410/3430/3440/3610/3620/3630)：MB526 Defy+、XT720 Milestone、A955 Droid 2。

独家的物理提取功能，可绕过密码，适用于诺基亚Lumia Windows Phone 8设备，包括：

- Lumia 520、820、822、920、928、1020。
  自2015年1月起，Cellebrite已经成为业内唯一一家支持对运行8.0和8.1操作系统的各种诺基亚Lumia Windows Phone设备进行物理提取和解码的厂商

可绕过密码对各种诺基亚BB5设备中进行物理提取，其中包括：

- 运行在以下设备上的RAPUv21芯片组：Asha 300 (RM-781)、Asha 302 (RM-813)、Asha 311 (RM-714)、700 Benji (RM-670)、603 (RM-779)

cellebrite
delivering mobile expertise

UFED优势

独家的物理提取功能，适用于已解锁（包括NAND和NOR存储）的BlackBerry黑莓7xxx/8xxx/9xxx设备，包括：

- 9930 Bold、9800 Torch和8330 Curve。

独家的BlackBerry黑莓解决方案：

- 对运行4-7系统版本的BlackBerry黑莓设备进行位对位解密与解码。
- BlackBerry 10文件系统提取，备份获取与解密，包括 Z10、Z30、Classic和Passport。

多种独特的临时Root权限解决方案，包括：

- 各种运行任何高达4.3版本的Android设备（包括已Root设备和和未Root设备）。
- 运行高达5.1.1版本的Android设备。

通过文件系统提取获取上锁应用程序数据

- 使用新的Android备份APK降级法，可通过文件系统提取方法从众多热门应用程序中提取数据，可获取众多应用程序的数据,包括WhatsApp、Facebook、Facebook Messenger、Line、Telegram等。
- Android备份法不再支持很多应用程序数据类型，但是，借助这个新功能，用户可以突破这种局限，让用户可获取关键的应用程序数据。

cellebrite
delivering mobile expertise

UFED优势

提取、禁用和重新启用用户锁功能

- UFED是唯一一种可禁用400多款领先Android设备图形锁和PIN锁的工具，让用户能开展任何类型的提取。这些设备包括三星Note 2、3、4、Galaxy Tab、Galaxy S5、Galaxy Mini； LG G3 & G4；以及Nexus 5。
- 禁用50多款已上锁LG Android设备上的用户锁，其中包括D820 Nexus 5。
- 针对运行iOS版本8.0至8.4.1的iPhone 4S、5和5C设备的iOS解锁功能。
- 重新启用数百款Android设备的用户锁。
- 针对45种摩托罗拉iDEN Android设备的独家密码提取功能，其中包括：i890、i836、i580、i876、i776、i855。

抽取和解码功能

增强对iOS和Android设备的逻辑提取——包括文件系统和应用程序数据。这一全面的功能让用户采用单一的增强型逻辑提取流程即可获得逻辑提取数据和文件系统提取数据。

诺基亚BB5设备物理提取、文件系统重建和解码

- Cellebrite支持绕过用户锁代码对众多诺基亚BB5设备进行位对位物理提取。使用Cellebrite的专有引导加载程序，对带USB连接的OneNAND存储芯片进行物理提取。
- 支持对这些设备进行文件系统重建和所选数据解码。
- 可对部分设备进行密码提取。

cellebrite
delivering mobile expertise

UFED解码优势

Cellebrite的UFED Physical Analyzer软件可为多种数据类型提供最先进的解码功能，如：已删除数据、应用程序、聊天、电邮、网页书签（收藏）、网页历史、SIM数据、Cookies、笔记、彩信、即时消息、蓝牙设备、位置、旅程、GPS定位、通话记录、短信、联系人、等等。

Android安卓

- 从完整的Flash图像揭示图案锁。
- 解码诸多已安装的第三方应用程序内容——消息、联系人、位置等。
- 针对未分配空间的应用程序数据进行先进雕复。

iOS

- 解码个人内容，包括：通话记录、语音邮件、联系人列表、位置、图像、视频文件、文字消息等。
- 解码诸多已安装的应用程序内容，如：Skype、WhatsApp、Viber、Fring、MotionX、AIM、TigerText、Facebook Messenger、Twitterrific、Textfree、Google+、Facebook、Foursquare、Waze等

BlackBerry黑莓

- BlackBerry 10文件系统提取、备份获取与解密。
- 对运行4-7系统版本的BlackBerry设备进行位对位解密与解码。
- 支持对BlackBerry 7xxx/8xxx/9xxx设备进行物理提取。

中国国产芯片组手机

对领先的中国芯片组（联发科、展讯等）手机进行解码。

Windows Phone

- 范围广泛的应用程序与JTAG解码。
- 针对未分配空间的应用程序数据进行先进雕复。

UFED优势

高级解码

高级验证工具

Cellebrite提供独特的高亮显示引擎，让用户能够查看已选文本的多个编码类型，并可查看各个已解码内容条目的确切位置。这样就能因验证目的在已分析数据和新提取数据之间进行轻松切换了。

离线地图

Cellebrite是业内唯一一家提供功能强大的离线地图解决方案的厂商，让用户能够可视化在解码过程中已经恢复的位置。该功能可通过UFED Physical Analyzer和UFED Logical Analyzer获得。

运行脚本与链

Cellebrite提供一种先进的开放式向导程序，让用户能够运行数百个脚本与链；可无比灵活地对UFED或第三方工具提取的取证图片进行解码。

JTAG解码

Cellebrite率先添加了JTAG解码功能。这是业内最灵活的解决方案，被开展JTAG提取的人士广泛采用。用户可从各种预付费用完即扔设备中解码数据，其中包括对JTAG提取物进行解码。

UFED用户锁代码恢复工具优势

UFED User Lock Code Recovery Tool提供针对上锁设备的解决方案。此工具支持Android和iOS操作系统，让用户能够访问上锁的设备，在屏幕上显示设备的用户锁代码。

UFED相机能检测出设备是否上锁，因此是解锁过程的一个关键组成部分。

支持的设备包括：

iPhone 4s、5、5c、5s、三星 Galaxy Note 3、三星 Galaxy S5、S4以及LG G3等。

UFED相机优势

图片

通过拍摄设备的图片或视频收集证据。

截图

捕获相片证据来验证结果，或在无法从设备提取数据时使用此功能。直接从iOS、Android和BlackBerry®设备捕获内部截图。

UFED恶意软件检测优势

Cellebrite率先在移动取证行业将恶意软件检测技术整合到UFED Physical Analyzer软件，查明被调查的设备是否与恶意软件有关联。

UFED Physical Analyzer软件用户可根据需要查找已提取文件中是否有病毒、间谍软件、木马病毒和其他恶意负载，以此作为物理或文件系统提取的一部分。用户还可根据需要更新恶意软件特征数据库，以确保最新的已知软件包含在自动搜索程序中。

UFED TOMTOM优势

专门解密TomTom行程日志，并从多种便携式GPS设备中提取各种数据。行程日志文件保留了完整行程的GPS信息和数千个位置，1至5秒即可分辨出（具体取决于TomTom设备及版本）。如果TomTom解码没有提供时间戳，Cellebrite的解密技术则可从行程日志文件中提取时间戳。TomTom解密与解码支持的设备包括Go 950、Go 930、Go 750和Go 510。

为最新TomTom设备提供解码支持。支持的内容类型包括联系人、通话及位置。TomTom解码支持Go 1000 Point Trading、4CQ01 Go 2505 Mm、4CT50、4CR52 Go Live 1015和4CS03 Go 2405等设备。

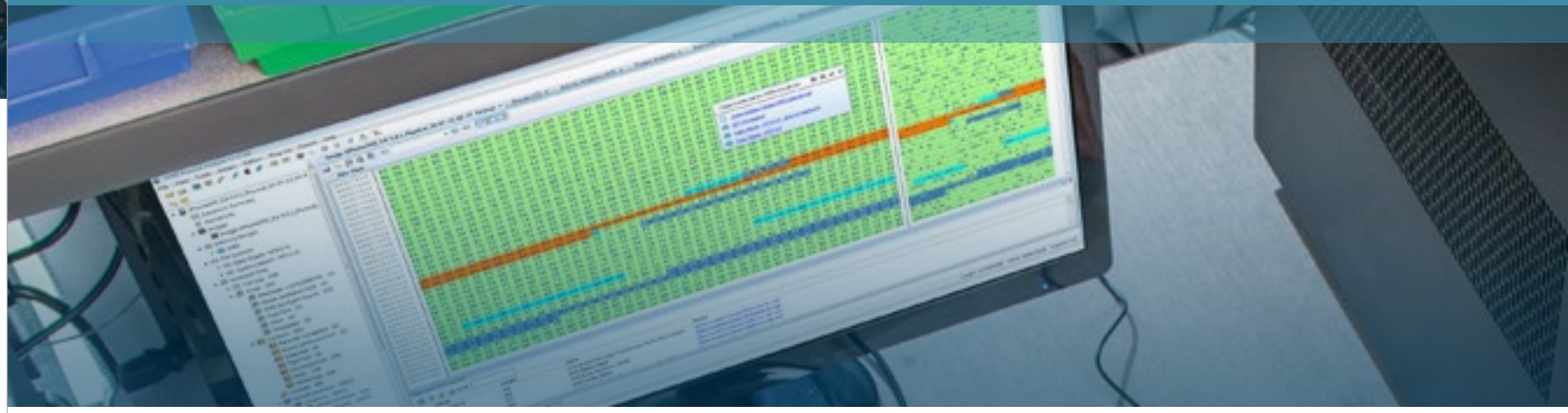
UFED专有引导加载程序优势

Cellebrite专有的只读引导加载程序支持合法有效的物理提取，并且专门为了读取设备的存储装置并将之发送给UFED系统而设计。

通过控制流程的每一个部分，Cellebrite就可确保引导加载不具有侵入性且设备上没有发生任何改变，进而让数据从取证上而言合法有效。该功能在专有的引导加载程序中提供，该程序支持物理提取，同时可绕过移动设备的锁，是不可替代的解决方案。对设备开展完整Root权限的第三方引导加载程序可能存在损坏设备数据的风险。

不同于第三方引导加载程序的是，Cellebrite的专有引导加载程序包含专门用于只读内存而非写入内存的编码，因此更加灵活、通用且可与各种设备兼容，从而让Cellebrite能比其他工具支持更多的设备。

UFED分析优势



分析和验证功能

- 在单一的统一报告中合并多种提取数据，进而开展综合分析和更高效调查。
- 原始文件源验证。利用原始文件源验证已解码的数据，无需使用其他移动取证工具进行验证。

UFED优势

取证调查人员面临这各种困难挑战，其中包括日益增多的大量新手机型号、固件、操作系统、加密和其他安全屏障。为帮助应对这些挑战，Cellebrite不断提供具有最新移动取证技术和最先进功能的创新型解决方案，以满足用户在关键调查方面的需求。

cellebrite
delivering mobile expertise