

February 3, 2017

TO WHOM IT MAY CONCERN

This letter identifies Cellebrite as the sole developer and manufacturer of the Universal Forensic Extraction Device (UFED) Mobile Forensics solution. Cellebrite Inc., established in 1999 and based in Parsippany, NJ, is incorporated in the state of Delaware. Cellebrite Inc. supports customers and users in the US, Canada and Mexico.

The UFED is a mobile forensics extraction, decoding, and analysis tool that extracts logical, file system, and physical data from mobile devices (i.e., smartphones, cell phones, tablets, GPS units, SIM cards, memory cards, and USB devices), including live and deleted data, contacts, phone numbers, call logs, text messages, SMS messages, app data (social network and other), location data, pictures, videos, and voice messages.

UFED technology provides digital forensic lab examiners, investigators, field personnel, and first responders with the capability to collect, protect and act decisively on mobile device data with the speed and accuracy a situation demands. Our competitive advantages include:

- **Large, Established User Community.** Since 2007, Cellebrite has deployed more than 40,000 UFEDs in 100+ countries to support law enforcement, intelligence services, border patrols, military forces, public safety agencies and commercial organizations.
- **Industry's Broadest Device & App Support.** Cellebrite has established collaborative business relationships with original equipment manufacturers (OEMs) and wireless carriers worldwide. These global partners send us more than 100 new handsets per month - most prior to actual consumer market release. This allows Cellebrite Mobile Forensics to develop mobile forensics support for new devices prior to our competition. We retain more than 8,000 mobile phones at our company headquarters for ongoing innovation and support.
- **Forensically Sound Evidence Every Time.** Unlike competitors' "black box" third-party boot loaders, UFED uses custom-designed, read-only boot loaders, which ensure forensically sound file system and physical extractions
- **Technology and Research and Development (R&D) Leadership.** Cellebrite provides the mobile forensic industry's most comprehensive Android, Apple iOS, Blackberry, and Windows Mobile support. Cellebrite has a staff of 250+ engineers—the most of any mobile forensics solution provider. We are committed to investing in the ongoing R&D to innovate around customer and market needs.
- **Best-in Class Training Ensures a Repeatable, Reproducible Mobile Forensics Process.** Open to all user levels, from beginners to advanced, Cellebrite certification training provides hands-on experience with Cellebrite products and applications, delivering the tools and knowledge required for evidence collection data analysis, searching, and reporting.
- **Physical Extraction Using Bootloader Method with Lock Bypass.** Cellebrite supports physical extraction while bypassing passwords, passcodes, and pattern locks from more than 3,800 different device types, including Android (800+ devices from HTC, Huawei, LG, Motorola, and Samsung); Apple iOS; and Windows Phone (Nokia and Lumia).

UFED technology includes capabilities that are exclusive to Cellebrite and not available from any other company.

Exclusive Android Capabilities

- Decrypted physical extraction of data from Samsung Galaxy S6, Galaxy Note 5 and some Galaxy S7 devices
- Partial file system extraction while bypassing screen lock for 105 Android Samsung devices, including devices running on Android 6 OS
- Physical extraction while bypassing screen lock for 12 Samsung Galaxy S6, S6 Edge and Note 5, running on Android 6 OS

Cellebrite Inc., 7 Campus Drive, Suite 210, Parsippany, NJ 07054
Tel: (201) 848-8552 • Fax: (201) 848-9982 • www.cellebrite.com

Tax ID: 22-3770059 • DUNS: 033095568 • CAGE: 4C9Q7 • ORCA Registration Complete

- Physical extraction capability using bootloader method with lock bypass for Samsung Android devices, including Galaxy Note 4, Note Edge, S3, S4, and S5
- Built-in Android temporary root (granting extra permissions) for hundreds of Android devices
- Physical extraction while bypassing user lock on 140 LG devices, including the G3 and G4
- Bypass user screen lock for 137 Samsung devices, including the Galaxy S5, Tab, and Mini; and Galaxy Note 2, 3, and 4
- Bypass user screen lock for 17 LG devices, including the G5
- Physical extraction and decoding from 26 popular Motorola Android devices
- Bootloader-based physical extraction from 17 MTK Android devices
- UFED User Lock Recovery Tool (Android)

Exclusive Apple (iOS) capabilities

- Decrypted physical extraction of data from Apple iPhones 4S, 5, 5c
- iOS unlocking support for Apple devices running iOS 8.x (8.0-8.4.1), with no risk of a device wipe
- iOS unlocking support for iPhone 4s/5/5c running iOS 9.x (9.0-9.3.2), with no risk of a device wipe
- UFED User Lock Recovery Tool (iOS)

Exclusive Blackberry Capabilities

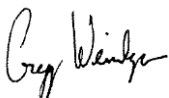
- BlackBerry 10 file system extraction, backup acquisition & decryption
- Physical extraction for unlocked BlackBerry 7xxx/8xxx/9xxx devices (including NAND and NOR memory)

Other Exclusive Capabilities

- Physical extraction with password bypass for Nokia Lumia Windows Phone 8 devices, including the Lumia 520, 820, 822, 920, 928, and 1020
- Physical extraction while bypassing user lock and decoding support for 3 Nokia 105 devices: RM-1133, RM-1134 and RM-1135
- Physical extraction while bypassing user lock and decoding support for 37 Huawei devices (Hisilicon)
- Physical extraction and decoding support for the latest TomTom devices, including the Go 1000 Point Trading and 4CQ01 Go 2505 Mm
- Wickr app decryption (Android)
- TigerText app decryption (iOS)
- Provide support matrix – what is supported using username and password / application token.
- Provide traces and changes document that describe what traces the extraction process might leave.
- Supports extracting a token from the subject device in addition to the user name and password option for several of data sources including: Facebook, WhatsApp, Twitter, Gmail, Google(Location History, My Activity, Photos, Chrome, Calendar, Contacts, Drive, Bookmarks, Tasks), Mail (IMAP), Dropbox, iCloud(App, Calendar, Contacts, Drive, Photos, OneDrive, Notes, Reminder, Location), Instagram, VK, Telegram

Please feel free to contact Cellebrite with any questions.

Sincerely,



Gregg Weinberger
Director, Sales Operations