cellebrite
delivering mobile expertise

NOVEMBER, 2012

UFED Physical/Logical Analyzer 3.5
Release Notes

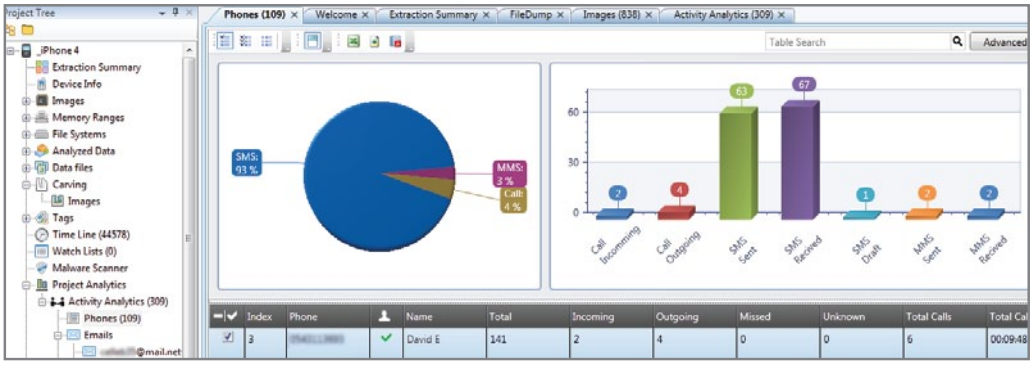
The Best Just Got Better!

Project Analytics

Establish better investigation leads by viewing statistics on communications and identifying relationship strengths via volume of events, as well as regular and irregular patterns. Statistics are generated by data types such as chats, calls, SMS and emails, from file system and physical extractions.
Results are presented in a graph and table view.

Quickly identify:

- Whom the device owner communicates with the most
- Preferred communication channels
- Communication directions - incoming and outgoing calls, SMS, MMS, emails, chat messages etc.



Industry First! Mobile Malware Detection

Malware detection allows UFED Physical Analyzer users to perform on-demand searches for viruses, spyware, Trojans and other malicious payloads in files extracted using physical or file system methods – applicable to ALL smartphones.

There's more:

- Ongoing malware signature updates
- UFED Physical Analyzer 3.5 is now integrated with award-winning security software – BitDefender
- Once infected files have been identified, a detailed list containing malware data, file name, path, size and other information is presented

Malware Type	Malware Information
Virus	Android.Trojan.Kmin.A
Virus	Android.Exploit.RATC.A
Virus	Android.Trojan.PjApps.B
Virus	Android.Trojan.BaseBridge.D
Virus	Android.Trojan.Geinimi.A
Virus	Android.Trojan.BaseBridge.B
Virus	Android.Trojan.Geinimi.B
Virus	Android.Trojan.Kmin.B
Virus	Android.Trojan.PjApps.A
Virus	Android.Exploit.Exploid.B
Virus	Android.Trojan.Kmin.A
Virus	Android.Trojan.Kmin.A
Virus	Android.Trojan.Geinimi.A

Vast Performance Improvements

Coping with the ever growing amount of data available in smartphones, Cellebrite has re-designed the UFED Physical Analyzer engine for much faster decoding, scrolling, sorting and searching among huge amounts of data – pictures, files etc.

Release Highlights

New Decoding

- **Exclusive – BlackBerry® messenger (groups, attachments and deleted data)**
- **Exclusive – Nokia BB5 – File system reconstruction and decoding of selected data**
- View Android application files
- New apps on iPhone, Android and BlackBerry
- Enhanced data types from phones with Chinese chipsets

and more…

UFED Physical/Logical Analyzer Features:

- Improved TomTom trip-log decryption process*
- Timeline graph
- Export locations to KML files
- Export emails to EML files
- Embedded text viewer
- Advanced filter improvements

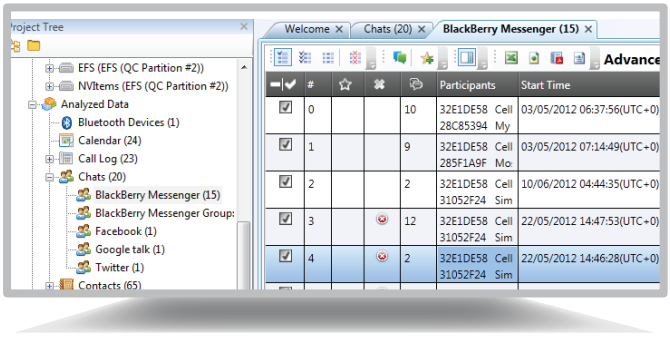
*Available within UFED Physical Analyzer only

UFED series

Enhanced Decoding within UFED Physical Analyzer

BlackBerry Messenger (BBM)

- Deleted messages and chats
- Message attachments
- Contact photos
- Groups: Contacts, chats and shared photos

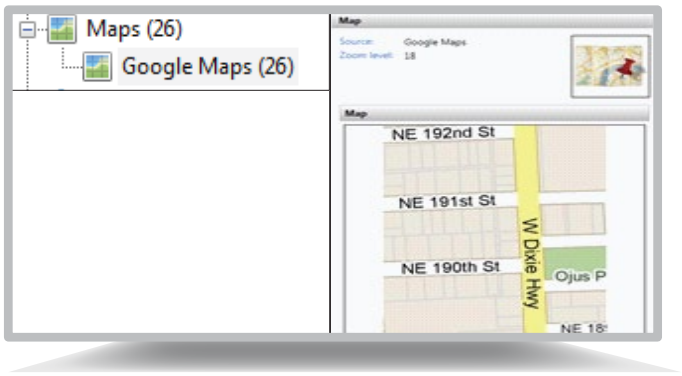


New Smartphone Apps Support

iPhone – Google Maps, Kik, Kakaotalk, QIP, Evernote, New Viber, ICQ, Mail.ru, VKontakte

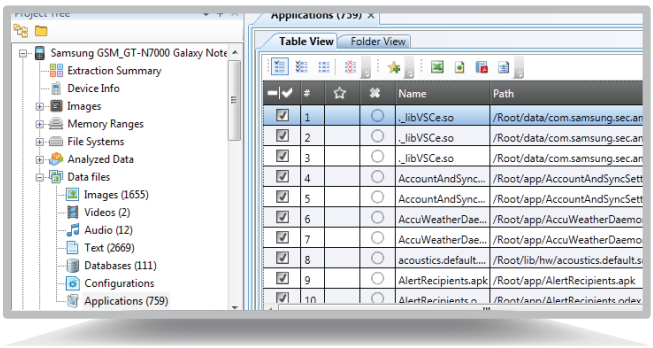
Android – Kik, Kakaotalk, QIP, Evernote, New Viber, ICQ, Mail.ru, VKontakte

BlackBerry – Facebook, Twitter, Google Talk (Gtalk), UberSocial



New Data File Type – Application

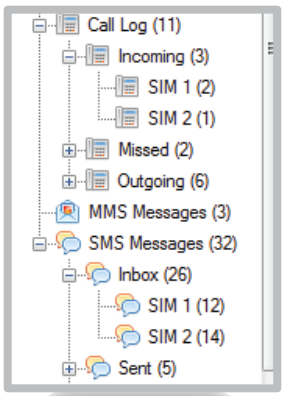
Application files such as executable files (*.exe), JAR files (Java ARchive), the Android application package file (APK) and more, are decoded and can now be found under data files – Applications category.



Phones Manufactured with Chinese Chipsets*

- **MTK chipsets**: Indication of the SIM slot used for incoming/outgoing SMS and calls
- **Spreadtrum chipsets**:
  - File system reconstruction
  - Phonebook, SMS, calls, Bluetooth devices and SIM slot (used for SMS and Calls)

*For UFED CHINEX users only



New Capabilities within UFED Physical Analyzer

- Decoding from selected Japanese devices
- WiFi passwords available in Android devices
- BlackBerry IPD PIN
- Samsung U-470 – SMS decoding
- LG CDMA devices UN-200 Saber, AN-200, UX-265, UX-210 – SMS and MMS decoding
- Motorola iDEN – Phonebook decoding from selected devices

©2012 Cellebrite Mobile Synchronization LTD, All Rights Reserved | Tel: +972 3 926 0900 | www.ufedseries.com | sales@cellebrite.com

TomTom Trip-log Decryption Improvements

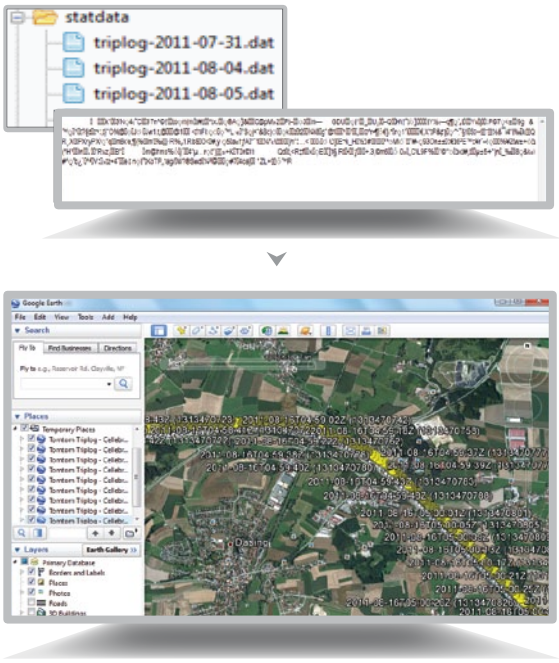
TomTom GPS's can record the device location in encrypted trip-log files. Cellebrite is the only vendor that enables the physical extraction of these files using UFED Touch/UFED Physical Analyzer.

UFED Physical Analyzer generates an XML report containing **selected and non-personal data** from the trip-log files which should be sent to Cellebrite support for decryption. The processing can take hours to days, depending on the amount of data and device model.

Once you have received the report from Cellebrite, it should be imported into the UFED Physical Analyzer to view locations' latitude, longitude and timestamps.

For additional analysis, filtered locations can be exported to a KML file and viewed using map applications such as Google Earth.

The TomTom trip-log decryption service is currently free of charge.



New Timeline Graph

Visualize events over time, view distances between events and see the number of events within a defined timespan. Events that occur in a close proximity are flagged in groups. View different time frames by scrolling forwards and backwards and adjust the level of detail displayed by zooming in and out. Timeline graph is available for both UFED Physical and Logical Analyzer users.

Export Locations to KML Reports

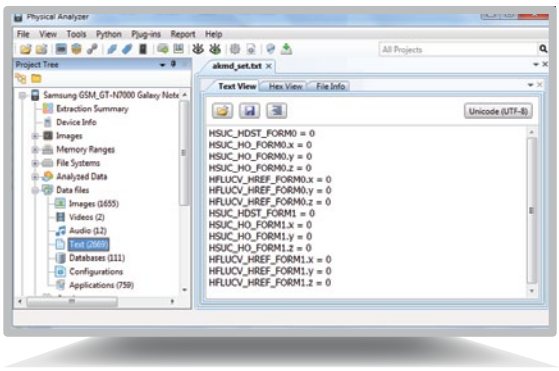
Export selected latitudes, longitudes, and timestamps to KML reports. These reports can be viewed on map applications - Google Earth or Google Maps.

Export Emails to EML Files

Export selected emails to EML format supported by many email and analysis applications. Each selected email is exported to a single report where the title of the email serves as the file subject.

Embedded Text Viewer

View text files including file information, content, and Hex, within UFED Physical Analyzer. No need for external tools.



©2012 Cellebrite Mobile Synchronization LTD, All Rights Reserved | Tel: +972 3 926 0900 | www.ufedseries.com | sales@cellebrite.com

Improved – Advanced Filters

Filter table information based on a variety of different fields – each field can contain multiple values. Available values within the search field are automatically generated: Calls, SMS, MMS and more.

UFED Applications Downloads & Upgrades

- UFED Physical Analyzer 3.5
- UFED Logical Analyzer 3.5
- UFED Reader 3.5

Has your UFED provided critical evidence for one of your cases? We want to hear about it.

Send us the case citation and relevant details, and we'll keep track of the cases for everyone's future reference.

Email us: sales@cellebrite.com

©2012 Cellebrite Mobile Synchronization LTD, All Rights Reserved | Tel: +972 3 926 0900 | www.ufedseries.com | sales@cellebrite.com