AccessData®

Mobile Phone Examiner *Plus*® (MPE+®)

Take Control of your Investigations.

The only mobile forensic solution that enables you to adapt to ever-changing mobile device technology and address new challenges in real time.

Key Features

Supports 10,000+ mobile devices (with Chinese chipset device collection add-on VELOCITOR).

Physical extraction of Android™ devices, with password bypass capabilities.

Logical extraction of Android devices without the need to know the manufacture or model.

Logical extraction of "burner" Android devices utilizing dSOLO.

Physical extraction of iOS® devices.

Logical extraction of iOS devices without the need of iTunes**.**

30% faster than leading competitors in logical extraction of iOS and Android devices utilizing the iLogical and dLogical data collection capabilities

SQLBuilder allows examiners to parse the data of all applications containing a SQLite database. "ZeroDay applications" can be supported, allowing examiners to build and save their own scripts to extract and analyze application data.

pythonScripter provides users with the ability to build python scripts to parse anything from a mobile device with an easy-to-use interface. Unlike other solutions, MPE+ pythonScripter acts upon a copy of the evidence, not the original binary or evidence file.

Advanced Analytics with Graphical Data Visualization allows users to get a timeline view of device communication that can be customized to the year, month, day or hour; quickly filtering the relevant data.

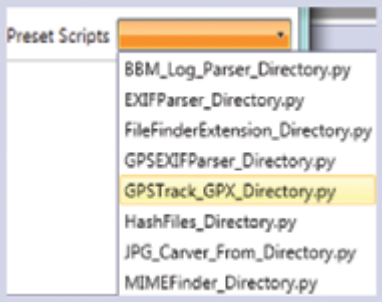
Output all the data or selected data in several different report formats with customizable reports.

Advanced Alert Manager gives the examiner the ability to import or create predefined words, phrases, numbers, etc and search the entire data set to help uncover key evidence in a matter of minutes. Alerts can be ran per case or for all collections; helping to triage large datasets for specific criteria.

MPE+ is the perfect choice for mobile forensics examiners looking to upgrade their capabilities.

Today, most crimes involve electronic evidence contained on mobile devices; quickly identifying this evidence is not only critical in resolving these crimes but also streamlines case processing to help reduce case backlogs. AccessData's Mobile Phone Examiner *Plus* (MPE+) provides you with the tools necessary to identify, collect and effectively uncover the key data other solutions miss. MPE+ supports even the most challenging mobile device profiles and offers the broad capabilities of high-priced tools at a fraction of the cost. Features advanced carving, deleted data recovery, application data extraction and analysis, SQLite database browsing, filtering options and more.

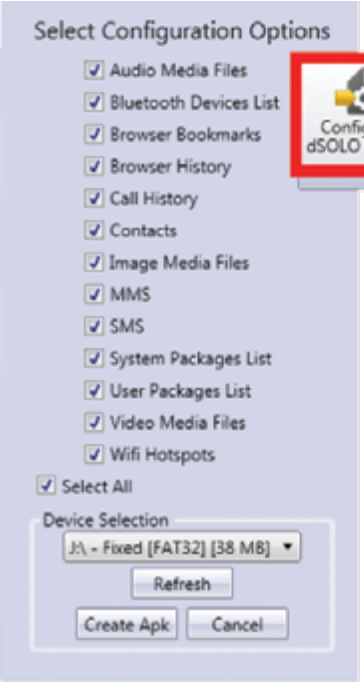
Mobile device technology is ever-changing. It's almost impossible to maintain the quality and efficiency of mobile forensic tools with such technology changing cycles so frequently.



Mobile technology is progressing at such a rapid rate, it's difficult for mobile forensic solutions to keep up. Most forensic tools require regular updates to keep pace with the volatility of mobile technologies and are often overwhelmed. Typically, forensic tools are antiquated technology at the time of their release since mobile device application updates are anything but routine. MPE+ overcomes all the variations of mobile devices—different hardware, OS versions, updates, etc.—by providing investigators with an easy-to-use yet comprehensive solution that works on today's technology and future variations without the need for constant software upgrades. The MPE+ pythonScripter allows the examiner to create, import or use pre-configured python scripts against data imported into the MPE+ solution. This allows MPE+ to support a near unlimited volume of devices, data types, application specific data and digital metadata.

>50% of the U.S. population uses smart devices. >95% use Mobile Device applications daily for communication purposes, social media, and financial transactions.

Law enforcement must be able to identify and examine all the apps that reside on a mobile device, and they must be able to extract the data associated with those apps. They need a mobile device forensics solution that's flexible enough to keep up with the fast-moving landscape of mobile apps and smart enough to uncover the hidden evidence those apps often hold. MPE+ is the only mobile forensic tool on the market that allows you to build simple SQL queries to extract hidden application data from all applications containing a SQLite database. Because of this capability, MPE+ can support most applications available—no need to wait for a software upgrade!



Mobile forensic investigators can no longer rely on "push button" mobile forensics tools that are unable to uncover ALL data available on mobile devices.

Research shows that only 5 to 10 percent of the entire corpus of user data is examined by typical mobile device forensics tools. This leaves as much as 95% of application data uncollected, and therefore unanalyzed. MPE+ not only acquires Android and iOS devices 30% faster than competitor tools but also uncovers more critical user data from these devices than any other tool on the market. It bypasses select Android and iOS device "locks" and performs advanced iOS acquisitions even when the iTunes® password is not known.

If you haven't encountered mobile malware yet, you will soon.

WORST CASE SCENARIO:

Mobile malware harms the integrity of evidence presented in a court of law.

BEST CASE SCENARIO:

Mobile malware introduces a delay in the investigation.

The rising tide of mobile malware is forcing forensics examiners to understand how to recognize and analyze it together with other evidence. Furthermore, the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes. MPE+ allows you to identify, analyze and document these threats without the need of built in signature based tools. With MPE+, you can mount a collected image and use any custom malware tool, as well as commercial anti-virus, to scan for threats.

A portable device can contain gigabytes of data. This increases the security risk for enterprises utilizing BYOD.

MPE+ helps enterprises address BYOD (Bring Your Own Device) risks by allowing them to collect data from employee's mobile devices when a threat is identified. It not only allows them to visualize and analyze contact and communication data, but can also identify elements that may have lead to a security breach (IP addresses accessed, Internet traffic, domains accessed, etc.). MPE+ transforms this big data into data intelligence to help pinpoint the meaningful information needed for data interpretation and incident remediation.

Support 95% of Chinese Devices by adding MPE+ VELOCITOR

In many cases, a mobile device may look like a mainstream smart device, but it is actually a cloned or counterfeit devices known as Shanzhai phones. In those instances, most mobile forensics solutions fall short, making it impossible to process critical data. MPE+ VELOCITOR is an MPE+ add-on hardware that enables the full flash data extraction from these devices, exposing critical evidence quickly without the need for a third-party tool or software.

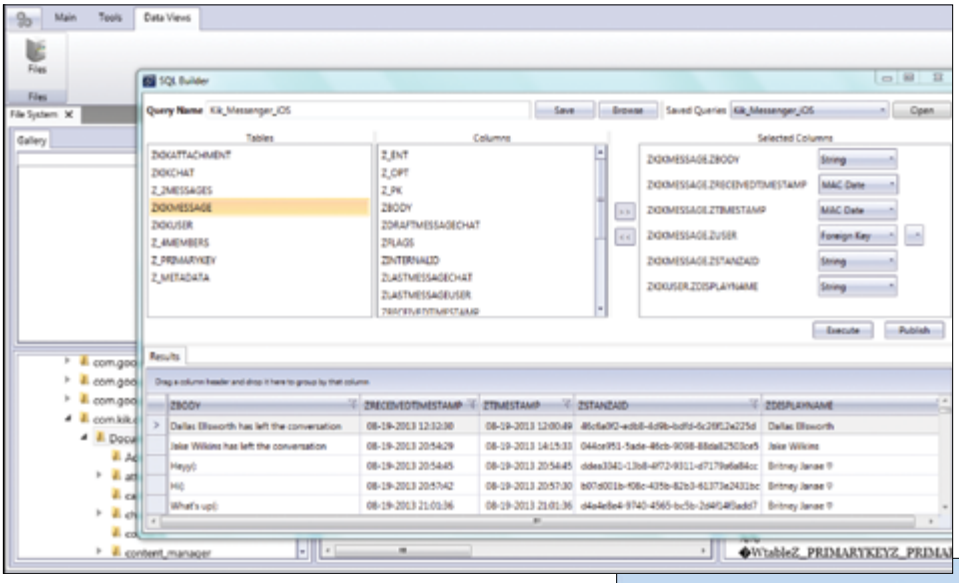
> First responders lack the clearance, tools and training to search a phone. MPE+ is a critical tool for us to manage our growing case load.
>
> **Detective Tyler Clarke, Lead Investigator, Reno Police Dept. Forensics Unit**

MPE+ nFIELD

A simpler, inexpensive solution for data collection in the field.

MPE+ nFIELD combines the powerful mobile device extraction capabilities of MPE+ with a simple user interface specifically ideal for non tech users. The wizard-driven interface allows you to forensically collect from mobile devices on-scene with practically zero training.

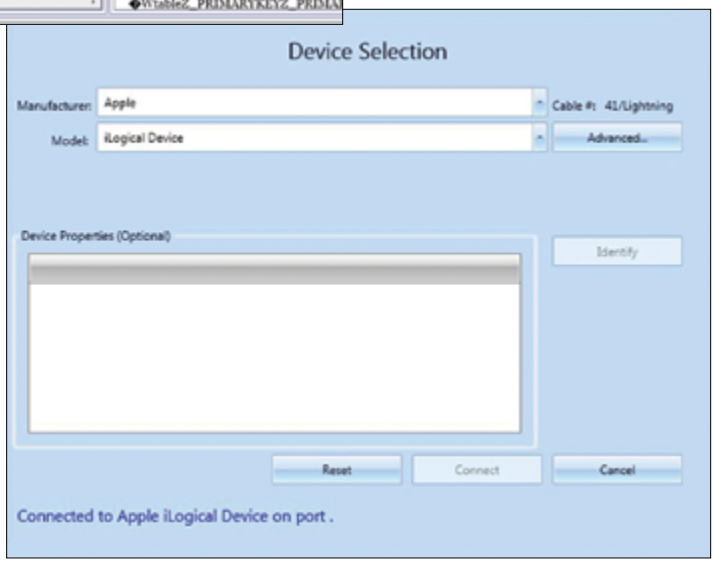
Build python scripts with pythonScripter to parse anything from a mobile device on an easy to use interface. This allows limitless support for any device. Unlike other solutions on the market, MPE+ pythonScripter acts upon a copy of the evidence, not the original binary or evidence file. This insures the MPE+ solution will not change or alter the original files, folders or any associated data.



Case Study: In processing a suspect's iPhone 4 with Cellebrite's UFED, Sgt. Sneary utilized MPE+'s iLogical support for iOS devices to validate findings by Cellebrite. By utilizing MPE+'s iLogical support for iOS devices, Sgt. Sneary was able to carve **13,000 more images** than what was first extracted when Cellebrite's UFED tool was used.

LEARN MORE

Fast logical extraction of iOS and Android devices utilizing iLogical and dLogical data collection capabilities.



MPE+
Mobile Phone Examiner *Plus*

LEARN MORE: www.AccessData.com

AccessData®

GLOBAL HEADQUARTERS
+1 801 377 5410
588 West 300 South
Lindon, Utah
USA

NORTH AMERICAN SALES
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

INTERNATIONAL SALES
+44 20 7010 7800
internationalsales@accessdata.com