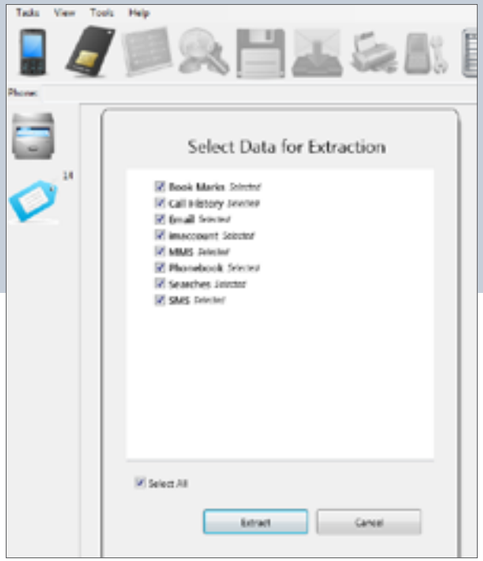
A White Paper from AccessData Group

The Future of Mobile E-Discovery

AccessData®

Contents

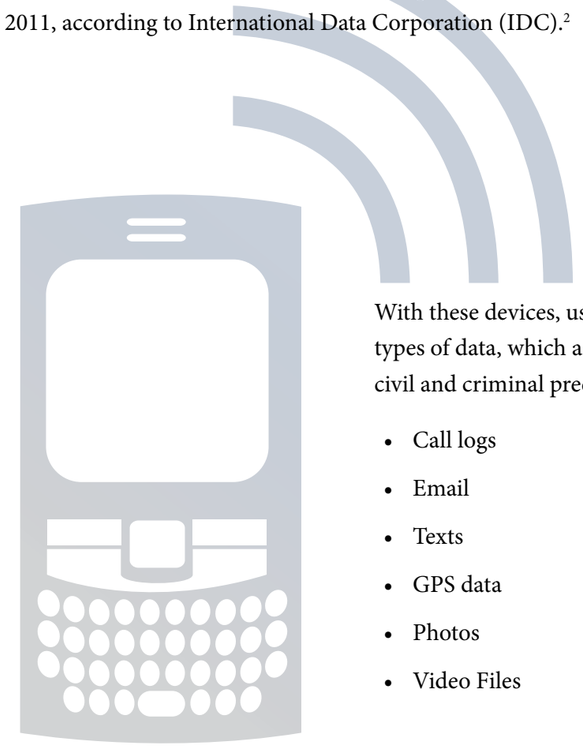


Parse options for Android >

In the business world, the use of mobile devices such as smartphones, cell phones and tablet devices is proliferating. This presents enormous challenges for attorneys who oversee electronic discovery (e-discovery) for organizations.

As of February 2012, 88% of American adults have a cell phone, 46% have a smartphone, 57% have a laptop, 19% have an ebook reader and 19% own a tablet, according to Mobify.[1]

Mobile devices are growing increasingly sophisticated, and the market shows no sign of slowing down. The worldwide smartphone market grew 54.7% year over year in the fourth quarter of 2011, according to International Data Corporation (IDC).[2]



With these devices, users are generating more and different types of data, which are all potentially responsive in both civil and criminal precedings, including:

- Call logs
- Email
- Texts
- GPS data
- Photos
- Video Files
- Voicemail
- Web browsing history
- Address Book
- Search History
- Calendar

[1] http://www.mobify.com/resources/mobile-device-ownership-statistics
[2] http://www.idc.com/getdoc.jsp?containerId=prUS23299912

Once, organizations involved in civil litigation could argue that it was too difficult to collect this type of information during discovery, and therefore, they did not have to worry about acquisition, review, processing and production. Today, though, litigants should not expect to be able to claim this much longer. There is simply too much potentially relevant information being generated and stored on mobile devices. Those in the law enforcement area have been successfully extracting and capturing mobile device data for several years, making it difficult for those involved with civil litigation to claim that it's impossible for them to do the same.

In-house counsel need to understand how the mobile device landscape is changing e-discovery, and what they will have to do in order to comply with changing expectations of the court in the future in order to avoid sanctions.

Mobile Discovery and Criminal Litigation

In criminal law, there is a longer tradition of mobile device forensics. In many instances, though, the technology has been overshadowed by issues around civil liberties, potential Fourth Amendment violations and how information is begin extracted and used.

For example, the Michigan State Police utilize mobile forensic devices that are capable of extracting information from smartphones in a matter of minutes. For several years now, the American Civil Liberties Union of Michigan has been filing freedom of information requests regarding the use and access of portable devices. In a series of dueling press releases in 2011, the ACLU accused the state police of using the technology to "quickly download data from cell phones without the owner of the cell phone knowing."[3]

[3] http://www.aclumich.org/issues/privacy-and-technology/2011-04/1542

In its own press release, the Michigan State Police (MSP) insisted that it only uses the devices when officers have a search warrant or the owner gives consent. "The MSP does not possess [data extraction devices] that can extract data without the officer actually possessing the owner's mobile device. The DEDs utilized by the MSP cannot obtain information from mobile devices without the mobile device owner knowing," the state police announced in a statement about the agency's official policy on the use of the devices.[4]

Last year, the national ACLU (American Civil Liberties Union), along with the New York Civil Liberties Union and the National Association of Criminal Defense Lawyers, brought a lawsuit challenging the U.S. Department of Homeland Security's policy of searching, copying and detaining travelers' laptops, cell phones and other electronic devices at the border.[5]

According to court filings in Abidor v. Napolitano, "This is a constitutional challenge to Department of Homeland Security (DHS) policies that authorize the suspicionless search of the contents of Americans' laptops, cell phones, cameras and other electronic devices at the international border. Between October 1, 2008 and June 2, 2010, over 6,500 people —nearly 3,000 of them U.S. citizens—were subjected to a search of their electronic devices as they crossed U.S. borders."

[4] http://www.michigan.gov/msp/0,1607,7-123-1586-254783--,00.html

[5] http://newsandinsight.thomsonreuters.com/Legal/legal_materials/court_filings/2010/10_-_october/abidor_v__napolitano/

Mobile Device Discovery within Corporations

Traditionally, corporations have been able to argue that discovery of this type of ESI is "unduly burdensome" for their own matters. However, since the technology has become so prevalent in criminal cases, corporate legal departments should not expect to be able to use this argument much longer.

While in-house attorneys can be less concerned about the Fourth Amendment implications of these types of forensic searches, they face unique complications when it comes to mobile device extraction for civil litigation, HR matters and regulatory issues.

Increasingly at many companies, the mobile device policy is basically "BYOD," or bring your own device. Employees may use their personal devices for work-related emails or to transfer files back and forth between work and home computers. Even when employees strictly use work-related devices for work-related purposes, mobile devices allow them to take data out of the office and off the network much more easily.

Companies have several options when it comes to controlling and containing the use of ESI on mobile devices, all of which have real or perceived drawbacks.

Issue Company-Owned Mobile Devices

Employers should make every effort to encourage their employees to keep their work-related files and communications off their personal devices, which will make discovery far more manageable. One way to do this?

Employers should make every effort to encourage their employees to keep their work-related files and communications off their personal devices.

Pay for the latest technologies. This is an expensive option, but it will help to ensure that employees aren't tempted to send a quick text to a colleague on their personal iPhone, which could then become part of the e-discovery process. It will also help IT and legal to control the number of apps that employees download, which can create even more challenges when retrieving potentially responsive ESI from mobile devices.

However, in many organizations, this may not be financially or procedurally feasible. Some employees may feel stifled or choose to use their own devices anyway without telling managers or supervisors.

Create Backup Policies

Companies can also develop strict policies that require employees to synchronize and backup their mobile devices on the organization's networks. Unfortunately, this can create ever-larger stores of data that could ultimately become discoverable. There may be changes to the metadata when location or time-specific files are downloaded from mobile devices, which can cause chain-of-custody issues down the road.

Most servers and some current discovery software are also not designed to capture texts, photos and other common files generated by mobile devices.

Embrace New Mobile Device Forensic Technologies

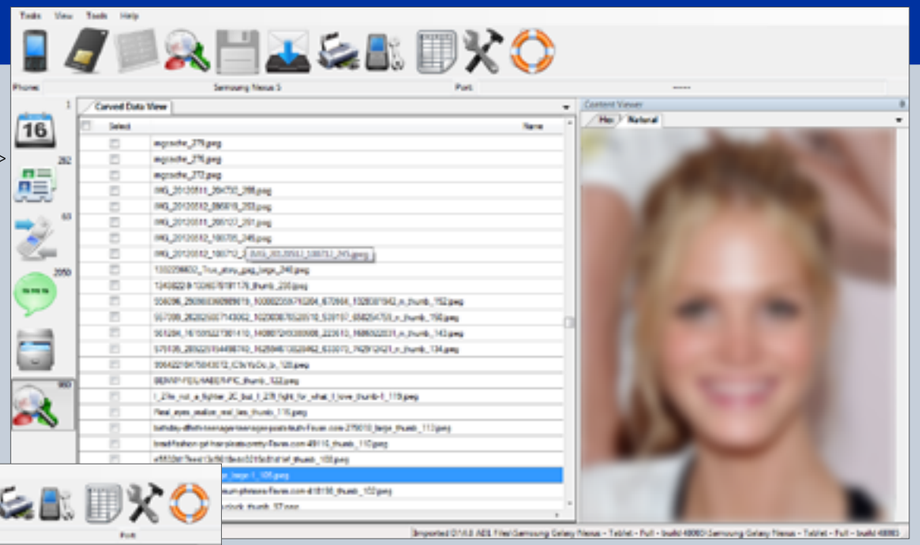
Adding mobile device forensics may also seem expensive, and many attorneys in corporate legal departments and law firms have voiced concerns that e-discovery vendors do not offer products and services that cover this area. Once they capture the data, the legal team must be able to review it. Even if the technology exists, legal teams must consider the costs and the amount of training involved in mastering it.

Increasingly sophisticated tablets and smartphones also have security features that could cause attorneys to be leery of new software. So they worry that this vast source of ESI is being overlooked, putting them at risk of sanctions.

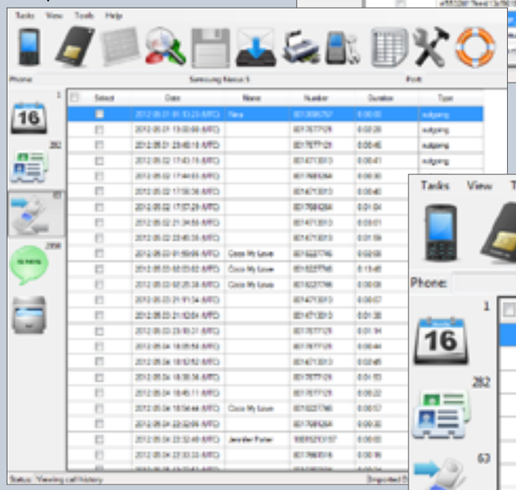
Fortunately, cost-effective, defensible, user-friendly solutions are now available that can capture ESI directly from mobile devices.

^ Options for data carving

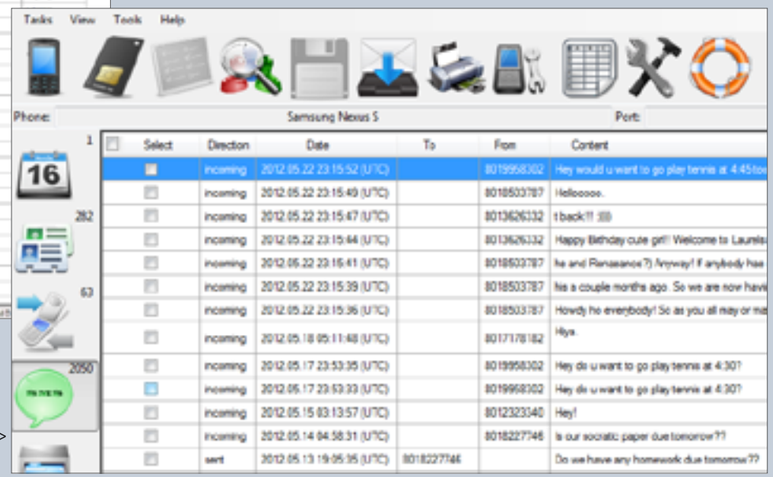
AccessData's MPE+ Forensic Technology



Carved data results >



Call history view
v



Retrieved SMS results >

AccessData has developed an extremely *simple*, *quick* and *affordable solution*: **MPE+**. Designed specifically to allow users to collect and view mobile data, MPE+ supports more than 3,500 mobile phones and smart devices, including iPhones®, iPads®, iPods®, Android™ and BlackBerry® devices.

MPE+ is a stand-alone mobile forensics software solution that provides legal teams with the broad capabilities of competing solutions at a fraction of the total cost of ownership. MPE+ can be purchased as a software-only solution, but it is also available preconfigured on a sleek touch-screen field tablet.

MPE+ is easy to use, with a graphical interface and data review organization that mimics the phone's own look and organization of data. Once data is collected, it can be reviewed within MPE+ or exported to the full range of AccessData's products, including AccessData eDiscovery, ECA or Summation Express & Pro, through an AD1 file. The use of the forensically sound AD1 container file ensures that the chain of custody is maintained throughout. This allows members of the legal team to either view the data independently or combined with other case data to allow for a more complete picture. It also smoothly integrates with AccessData's Forensic Toolkit (FTK) if analysis of more data sources is required for cellphone, laptop, iPad or other devices. For example, attorneys may need to review a custodian's laptop as well as his mobile phone, a process that AccessData's complete range of discovery products makes seamless.

MPE+ is also affordable and works quickly. With this technology, legal teams can acquire mobile device data in a matter of minutes. It retails for $3,000, as opposed to more expensive competitor solutions or truly expensive service provider options.

Among MPE+'s other features:

- It collects from a range of mobile devices and does a full forensic level capture, not just the active data. This means MPE+ can collect deleted items and all appropriate metadata as well.
- It can also be reviewed within the software. The system will correlate data with contacts in the phone, so that users can review files by custodian.
- It generates advanced reports to detail phone data, including call history, contacts, messages, photos, voice recordings, video files, calendar, tasks, notes and more.

Conclusion

The question is not if corporate legal departments will need to collect ESI from mobile devices, but when. Many departments are already faced with this requirement and pay by the GB or by the hour for service. Fortunately, this type of collection is no longer limited to the realm of forensic investigators or law enforcement. With AccessData's MPE+ technology, in-house counsel now have an easy and affordable way to make mobile device discovery a part of the routine e-discovery process.

AccessData Group has pioneered digital investigations and litigation support for more than twenty years and is the maker of the industry-standard computer forensics technology, FTK, as well as the leading legal review technology, Summation. AccessData provides a broad spectrum of stand-alone and enterprise-class solutions that enable digital investigations of any kind, including computer forensics, incident response, e-discovery, legal review, IP theft, compliance auditing and information assurance. More than 130,000 users in law enforcement, government agencies, corporations, consultancies, and law firms around the world rely on AccessData software solutions, as well as our premier hosted review and digital investigations services. AccessData Group is also a leading provider of digital forensics and litigation support training and certification, with our much sought after AccessData Certified Examiner® (ACE®) program and Summation certification program.

Come learn why our e-discovery solutions are consistently ranked among the "leaders" in analysts coverage of the market space, by visiting AccessData.com.

AccessData Group
384 South 400 West Suite 200
Lindon, UT 84042 USA
801.377.5410