



WINTER 2015 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery and cybersecurity needs. A primary area of growth is digital evidence preservation and analysis from smartphones. With the explosion of Bring Your Own Device (BYOD), we chose to theme our Winter 2015 E-Newsletter on these topics.

SMARTPHONES - A POTENTIAL GOLDMINE FOR DIGITAL EVIDENCE

Smartphones such as the iPhone, Samsung Galaxy, HTC and other devices should be considered in the overall case planning process. Text messages (SMS/MMS), call logs, contacts, calendar items, pictures, video, voicemail, geotags/locations/GPS, Notes, Web history, cookies and bookmarks are examples of the types of data that can be extracted from smartphones. Much of the data within smartphones resides in SQLite databases and must be parsed into reports such as PDF, CSV, HTML and/or XML to be made viewable for attorneys or investigators to review. The positive is that these formats make digital evidence available for review.



The drawback is that extra data massaging is needed to get the data into a document review system and some of the linkage in the reports may be lost if this extra data processing happens. This issue does not exist with email or documents stored on a desktop or laptop. On smartphones, there may also be applications loaded with data not parsed out by the commercially available smartphone forensics tools. In the cases where such data may be relevant, additional tools may need to be used such as Magnet Forensics' Internet Evidence Finder, specialized Python parsing or additional custom scripting. Some examples of types of cases that smartphone data has been reviewed are as follows:

- 1) A corporation is suing a former employee for intellectual property theft. Key communication about its corporate trade secrets is communicated in a deleted text message from the custodian's iPhone to its primary competitor.
- 2) In an antitrust matter, a meeting between two fierce competitors is on the calendar of a key executive in-charge of pricing for a semiconductor company.
- 3) A teacher at a school district is having inappropriate sexual relations with a minor. Inappropriate videos and pictures of the minor are found on the device.
- 4) In a car accident where a red light was run, key evidence was located on a smartphone that the custodian was texting at the same time as the reported accident.

It is good practice to image phones of disgruntled and terminated employees if proper authorization exists, especially if you suspect the employee of intellectual property or trade secrets theft. Smartphones

may be more difficult to obtain access to data due to ownership rights of information and when an individual owns the device express authorization may have to be granted unless a subpoena or warrant is issued. Additional processing may need to be performed with the custodian for filtering or redacting records containing spousal communication, communication with minors, health care information or financial-related data. Many smartphones may contain co-mingled and business data. Some organizations seeking to better manage text messages from mobile device data proactively have archived corporate communications using technologies such as ArmorTex (through the acquisition of Uppidy), Smarsh and Sonian.

Corporations may also seek to proactively adopt Mobile Device Management (MDM) software to better manage its mobile devices. Examples of such technologies include AirWatch (purchased by VMware), AmTel MDM Dialogs Smartman Device Management (purchased by Sophos), Citrix's XenMobile, GDS Transnational's FancyFon, Fiberlink MaaS360, Good Technology, MobileIron and Symantec. These technologies allow corporate control of data coupled with security and is a separate topic in itself.

UPCOMING INDUSTRY EVENTS

March 2015

The Masters Conference, Managing the E-Discovery and Social Media Minefield: March 31

April 2015

RSA Conference: April 20-24

May 2015

CEIC 2015: May 18-21

[Click here to see more upcoming events and links](#)



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

Please update your records with our corporate headquarter's new address below as of November 1, 2014!

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

[Contact us today!](#)

www.digitalmountain.com

FOLLOW US AT:

