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 - PRESERVATION 101 FOR YOUR CASES

We spend much time and effort reviewing email and documents from corporate systems for electronic discovery. However, many times the key piece of communication may be overlooked on a smartphone (e.g. iPhone, Blackberry, Samsung Galaxy, etc.) where that "smoking gun" text communication may reside. Employees at corporations may use applications to text and for other purposes on phones. The most popular applications are supported for examination. There are so many permutations of smartphones and tablets your head may spin (Cellebrite has over 6,500 phones listed for their Logical product matrix alone). Unlike many corporations which systems are built upon Windows operating systems, smart phones have many more flavors of operating systems such as Android, iOS, Windows and Blackberry OS making interoperability of data preservation and analysis tools much more complex. As a result, specialized tools are needed that are more expensive to maintain since specific tools may work better at analyzing certain types of devices and applications. Although there are many specialized tools in the market, the mainstream ones as of this writing are Cellebrite, Oxygen, Susteen, XRY, Katana (Lantern) and Paraben. The quality of results can vary dramatically based on the tool and also the examiner's training. For example, manual decoding may sometimes be an option to make data not easily parsed by a tool available for review. Also, the depth of the imaging process available may be the difference causing variance in price quotes from the vendor community. There are 3 types of images to contemplate when having a phone preserved and analyzed:

1) Physical Image – this bypasses the phone's operating system and enables data to be preserved directly from the phone's internal flash memory which includes unallocated space and deleted data. This extraction option is not available on all devices and is a bit-by-bit copy of the entire flash memory of a mobile device. This includes access to usually inaccessible partitions of the device.

2) File System Dump – this extraction option relies on the operating system of the device and allows access to active data as well as data that may be recognized by the file system as deleted or hidden data.

3) Logical Image – this extraction option relies on the device's designated API (Application Programming Interface) and operating system and allows access to active data that is viewable. This is typically the quickest option, but does not provide access to deleted data.

The definitions are more important than the terms as many providers are using terminology that is not the same given the infancy of the market and the actual words used may morph over time. Also, a phone may be imaged in a proprietary format, so it may be only able to be analyzed by the tool that created the image versus portable across many tools for analysis. This article does not cover iTunes or iCloud backups. Relevant data may also be stored in these backup formats if the data on the device was an Apple smart device and a backup was actually performed.

Even if the phone is password-protected, our smartphone experts can often get the passcode when the passcode is not known. If the device cannot be accessed with these preliminary procedures due to password protection or being damaged, there are more advanced procedures that can be taken if proper authorization occurs such as Chip-off or JTAG. With JTAG (Joint Test Action Group), an examiner is relying on the firmware's interface to connect equipment to Test Access Ports (TAPs) on a device and instructing the processor to transfer the raw data stored on connected memory chips. This is highly specialized because the examiner may have to reverse engineer raw data into something usable for a case. Cellebrite is able to parse out some raw data dumps from JTAG and Chip-offs.

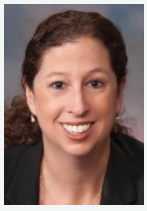
The Chip-off method, which is even more complex than JTAG, involves physically removing the flash memory chip from the phone and then acquiring the raw data using highly specialized equipment. It is cost prohibitive for the average case given the manual effort required and making the data user-friendly for a case. With Chip-off, the device is generally destroyed in this process.

This article is meant as a high level overview of the smart phone preservation process and as a result much detail was glazed over in our effort to provide an overview. Even though smartphones may be much more complex given the many flavors of the devices and tools used, for most cases the costs are actually less than processing data from a desktop or laptop and should be considered as part of the overall case planning process.

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

www.digitalmountain.com

Contact us today!

FOLLOW US AT: