SUMMER 2017 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss relevant case law on smartphones, evidentiary value in cases and the increasing security threat from mobile malware.

Smartphone Discovery Hits Prime Time

Our company has performed discovery on phones for over a decade (yes, even before the iPhone's debut in 2007). This past year, however, we've experienced a dramatic spike in demand for smartphone discovery – over 30% of our cases included smartphone data acquisition and analysis. Such a spike in demand may be unsurprising given that IDC, a global market research firm, forecasts shipments of smartphones will reach 1.53 billion units in 2017 and grow to 1.77 billion in 2021. These numbers mean that 20% of the world population owns a smartphone; roughly estimated using today's population of 7.5 billion. In other words, the demand for smartphone discovery has clearly hit prime time – but why? Multiple factors play a role, including not least that smartphone data is discoverable evidence and as such creates preservation and other discovery obligations for the party with custody and control of such smartphone data. It's also about what smartphone data illustrates (often more damningly than other evidence). Common items that may be extracted include SMS/MMS/iChat, Call Logs, Contacts, Calendar entries, Media Files/Pictures, Voicemail, Geotags/Locations Information/GPS, Notes, Web History, Cookies, Bookmarks and other relevant information, such as Email if the database is not encrypted. In about 80% of our cases, the attorneys or investigation teams are seeking active and deleted communications and contact history. For criminal matters, the digital evidence sought is generally broader.

Tips & Traps for Smartphone Discovery

Although smartphone discovery is useful in many types of cases, the majority of cases involve employment disputes. Smartphone discovery can be challenging from both a company policy perspective and from a technical perspective. Unlike traditional desktops and laptops where a computer forensics examiner may perform a targeted logical preservation, with smartphones the

entire device generally needs to be imaged prior to parsing content and communications into a readable form. For civil matters involving personal devices, it's important to obtain proper authorization before imaging devices. For smartphone devices, acquiring the proper PIN or passcode is essential prior to processing the device. If the device is a newer iPhone, and iTunes with the password is used, then one would require the iTunes' password in order to acquire the critical communication contents such as text messaging, call history log, and contacts. Some devices are configured to revert back to the factory settings (wiping all data) after a certain number of PIN attempts (e.g. 10 failed logins). Some devices may also have a microSD card that stores data (presently capable of holding up to 2TB), so it's critical to incorporate data from relevant storage into forensic exams.

Not all forensic imaging tools yield the same results. Furthermore, commercially available tools don't all enable the same quality of analysis. For example, all tools can typically perform a logical image, but sometimes only a limited amount of deleted items is produced with a logical image. If a physical image cannot be obtained because of technical issues, the next best option is a file system extraction (this is sometimes referred to as a "file system dump"). In other words, forensically imaging a smartphone can result in a spectrum of completeness (from less complete to more complete): logical imaging, file system extraction, and physical imaging. Physical imaging should always be the preferred method if the goal is to locate deleted data and the technology is commercially available for the specific source device. The devices must be imaged properly to enable proper discovery and searching of the smartphone data. Also, the imaging format is sometimes not interoperable among different analysis tools. That is to say, the data collection needs to happen with the same tool that will be used for the analysis.

Beyond SMS/MMS/iChat, email is sometimes available for parsing. Other types of communications potentially available for parsing from the smartphone include Facebook Messenger, GoChat, Instagram, Twitter, WeChat, WhatsApp, Skype, etc. Thousands of combinations of devices and operating systems currently exist, so which communications can be extracted will depend on the device, operating system, existing applications, and encryption (individual applications can enable encryption rendering certain databases unreadable). Most communications reside in SQLite databases. When existing tools cannot parse communications, it is possible to have custom scripting performed to attempt additional data extraction. The export options in most tools are PDF, CSV/Excel, HTML or XML. More advanced methods exist for obtaining data at a firmware-level that may not be available through forensic imaging of the device, including JTAG and chip-off. However, depending on the case, these extensive procedures may be cost prohibitive with a low probability of yielding fruitful results.

Although smartphone discovery has hit prime time, it's critical to use experienced professionals, such as Digital Mountain for proper and defensible smartphone data preservation, parsing, and processing. Performing proper analysis work involves using the best commercially available tools coupled with trained experts. For most smartphone cases, the analysis can be performed at a cost effective price. Due to the complexity of smartphones and the amount of evidence now being stored on the devices, smartphone examination as part of an overall digital evidence strategy is an important consideration for all investigatory matters, litigation, and regulatory compliance. Smartphones have now hit prime time and this trend is not reversing. Have you considered smartphone discovery as part of your case strategy?

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

Black Hat USA
Las Vegas, NV: July 22-27, 2017

ILTACON 2017 Annual Educational Conference
Las Vegas, NV: August 13-17, 2017

PFIC 2017 Cyber Symposium
Pittsburgh, PA: August 18, 2017

Today's General Counsel, "The Exchange" eDiscovery
Houston, TX: September 13-14, 2017

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) 2017 Midyear Meeting
San Diego, CA: September 18-19, 2017

Click here to see more upcoming events and links

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

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: