November 29th 2014

Expert Data Forensics beefs up its capability in mobile data forensics

In the course of a legal proceeding, the recovery of data can make or break a case.

For years, data forensics experts have honed their craft in preserving, extracting and analyzing data from computers. It has become a sophisticated science.

Mobile data, however, is a different story.

"Conducting a data forensics investigation on mobile technology has not caught up with computer forensic technology," said *Expert Data Forensics'* Director of Case Management, Eliya Azoulay. "The source devices are not comparable. We are still burdened by the laborious task of decoding deleted artifacts from third party applications (Apps) for the purpose of recovering the data."

The gap in computer versus mobile data forensics prompted *Expert Data Forensics* to recently invest in Cellebrite™ as the company's latest addition to its forensic digital laboratory, thus closing the gap between computer and mobile data forensics.

Cellebrite's Universal Forensic Extraction Device (UFED), a high-end mobile forensics solution, extracts, decodes and analyzes actionable data from legacy and smartphones, handheld tablets and portable GPS devices. More than 30,000 UFED units have been deployed to law enforcement, police and security agencies in 100 countries.

Expert Data Forensics (EDF) Senior Digital Forensic Investigator Leon Mare said Cellebrite's UFED provides the most advanced analysis, decoding and reporting application in the mobile forensic industry. "It includes malware detection, enhanced decoding and reporting functions, project analytics, timeline graphs and exporting data capabilities."

Mare said having the Cellebrite™ product enhances EDF's capabilities in three areas: Data Verification, Data Preservation and Forensic Data Recovery.

He also said that through the usage of Cellebrite™ EDF increases its ability to assist attorneys in civil, corporate and criminal cases. Forensic data investigation can strengthen divorce and custody cases, help document employee behavior such as harassment and embezzlement, partnership disputes and can provide valuable evidence in criminal cases.

Azoulay said attorneys should be aware that "not all data recovery tools are forensically sound." "If you are using digital evidence or data extraction in court, make sure the data extraction tools used can be certified for authenticity," added Mare. "Your data extraction tools, as well as your extraction methodology, could be challenged. Its good practice in today's digital age for an attorney to advise their clients to forensically preserve digital evidence, you don't know how things will turn out. It's like insurance," he added.

Mare said an investment in a certified forensic examiner will save in the long run because the methodology and data presented by a certified forensic examiner is less likely to be challenged in court.

“We get way too many instances where digital device preservation and extraction is an after-thought. In a dispute situation it should become standard practice to have your client preserve their cell phones and digital devices; they may contain data helpful to them pre, post and during litigation. It’s a proactive approach that can literally help win a case,” he said.

Cellebrite™ uses three processes to extract data from mobile devices: extraction, decoding and analysis.

"When you extract raw data, a binary file which is a copy of the physical memory or the file system, you need to make it usable. That's what our decoding group is doing. If you look at different phones, Android or Nokia for example, you get different things. The entire decoding process is more complex because there is no one standard,” said Leeor Ben-Peretz, Cellebrite’s VP of mobile forensics products and business development. “It's a very complex process, and we started out with hundreds of types of file systems. We fiddle with different encryptions and compression levels, and in the end we give our end customer the information in an accessible form…”

Ben-Peretz said the third process is analytics.

"We are talking about gigabytes of information, almost infinite. For example, take a phone with 120,000 text messages, or go and browse through 30,000 pictures — it would take you forever to find your smoking gun. We developed analytics capabilities to use the time constants of an investigation to their fullest. It can find you a keyword in three extractions and get you relevant information in seconds for search a term like 'money'," he said.

The second element in the analytics phase is mapping.

Cellebrite™’s UFED can find out who is connected to who, how connected they are, what conversations they have had, and can scan multiple communication services — be it Facebook, Skype, text messages and calls — and gather that information a number of different devices.

"The mapping of connections shortens investigation times by using time limits. For example, if you don't want to screen 75,000 messages, but only the ones on 1 July, we are down to 3,000 messages. You apply a keyword watch list and we are down to 10 messages. You can map past events by graphs, vectors, hours, locations and communication cross references,” said Ben-Peretz.

EDF recognizes that Mobile Device Management (MDM) and security are key issues for the legal community as well as big business.

A recent survey by Tech Pro Research of IT leaders found that MDM and security are the top two issues IT professionals believe they will face over the next three years.

The poll found that 81 percent of firms are concerned about security with data breeches and cybercrime threats becoming more prevalent.

“As the majority of data on smartphones is now being transmitted by apps the difference between success and failure for an investigation will often be determined by the agility and adaptability of the forensic tools being employed to interact with them,” said Mare. “By bringing the best technology available to our clients, along with the years of experience gained, we can continue to be leaders in our industry,” he added.

Expert Data Forensics
888.355.3888
ExpertDataForensics.com
NVPILic#1498