ACCESSDATA

CASE STUDY

The Northwest Ohio Technology Crimes Unit (NOTCU) task force was formed in 2011 to aid law enforcement in its investigation of digital crimes. Based in the Lima Police Department's training facility, NOTCU is designed to help law enforcement agencies process diverse technology-based evidence, ranging from evidence obtained from investigations of identity theft to investigations involving the sexual exploitation of children, to more traditional crimes.

Major case gets solved by the Northwest Ohio Technology Crimes Unit using Mobile Phone Examiner *Plus*® (MPE+®)

MPE+, No Longer the Validation Tool!

Sergeant Terry Sneary, a 23-year veteran of the Allen County Sheriff's Office, is a digital investigator currently assigned to the Northwest Ohio Technology Crimes Unit (NOTCU). For the past year, his primary duty within the Unit has been to conduct mobile device investigations.

In this capacity, Sgt. Sneary faces a significant backlog of cases due in part to the fact that law enforcement continually seizes more digital evidence across more devices year after year. As a result, Sgt. Sneary's job has become more difficult. Not because of workload, but due to the multitude of mobile forensic solutions on the market today coupled with the inability to keep up with advances in mobile device technology. Sgt. Sneary contends that most mobile forensic tools only provide a "push-button" solution that is capable of acquiring only a fraction of the potential evidence that can be contained on a device.

Considering that nearly every criminal investigation involves acquiring digital evidence in some form and that this evidence is increasingly acquired from mobile devices, Sgt. Sneary recognizes the need to have adequate mobile forensic tools at his disposal. Furthermore, in acquiring evidence that will withstand judicial scrutiny, Sgt. Sneary recognizes the importance of obtaining digital evidence in a manner that does not compromise or corrupt the integrity of the data.

> **"You cannot put dollars and cents on cases we process. The ability to take these criminals off the street for us is priceless."**
>
> —Sgt. Terry Sneary
> Digital Investigator, Northwest Ohio Technology Crimes Unit (NOTCU)

When Sgt. Sneary was first assigned to the NOTCU, a Cellebrite® UFED unit was purchased to address the increasing number of service requests to process smart devices in criminal cases. In 2013, the NOTCU purchased MPE+® as a validation tool in order to corroborate findings obtained from other forensic tools (in compliance with the National Institute of Standards and Technology [NIST], test results of acquired data must be repeatable and reproducible to be considered admissible as electronic evidence). However, due to the performance of MPE+ in the case presented below, MPE+ is now the primary tool utilized by the NOTCU in the processing of mobile devices.

Key Evidence Obtained With MPE+ Leads to the Conviction of Dangerous Child Predator

In a recent case involving the sexual exploitation of minors, Sgt. Sneary was tasked with processing a suspect's iPhone® 4, which was used both to communicate with the victims in this case, as well as store sexually explicit images of the victims.

From information gleaned from the victims and the suspect, Sgt. Sneary determined the suspect utilized the application textPlus to communicate with the victims. This application gave the suspect the ability to not only communicate with the victims but also appear as if the suspect was in a different state, thus lending credibility to the suspect's claims that he was a representative of a modeling agency. In this capacity, the suspect enticed minors to send sexually explicit images of themselves to the suspect in exchange for the promise of becoming famous.

Sgt. Sneary knew it was imperative to retrieve the messages sent via the textPlus application that were stored on the suspect's phone. However, in reviewing the data initially extracted by both Cellebrite UFED and MPE+, Sneary realized none of the text messages sent or received from textPlus were extracted as regular SMS/TEXT messages, making it impossible to properly display them on a report. "At that point I didn't think any of the tools, either Cellebrite or MPE+, were able to get those text messages from the textPlus application. In reality I was wrong. MPE+ was able to." Using MPE+ SQLBuilder, Sneary was able to extract the application's SQL database, and present the textPlus messages in a readable format for the jury to see.

Additionally, in processing the suspect's iPhone 4 with the Cellebrite UFED, Sgt. Sneary utilized MPE+ iLogical support for iOS® devices to validate the Cellebrite findings. By utilizing MPE+ iLogical support for iOS devices, Sgt. Sneary was able to carve 13,000 more images than were first extracted when the Cellebrite UFED tool was used. "It was almost double the amount of pictures we originally had," Sneary says. In reviewing the additional images extracted using MPE+ iLogical support for iOS devices, Sgt. Sneary recovered a deleted picture the suspect took of one of the minor victims. In the picture, the suspect's face was visible in the background of the image as a reflection in a mirror. This recovered picture as well as the textPlus messages recovered with MPE+ SQLBuilder would later be the key evidence presented at the suspect's trial, which refuted the suspects claim that he did not take the pictures nor communicate with the minor victims

The use of MPE+ SQLBuilder and iLogical support for iOS devices in this investigation provided overwhelming evidence of the suspect's guilt in the commission of numerous sex offenses involving multiple victims, and led to the jury returning a guilty verdict in less than an hour.

Sgt. Sneary concludes, "You cannot put dollars and cents on cases we process. The ability to take these criminals off the street for us is priceless." In the two biggest cases of his career to date, Sgt. Sneary has relied on MPE+ as the key solution in obtaining evidence needed to secure a conviction.

Conclusion

As outlined in Sgt. Sneary's case, the iLogical support for iOS devices built into MPE+ was able to extract more evidence from the device than the Cellebrite UFED. This evidence was critical in the conviction of a very dangerous child predator. Likewise, the MPE+ SQLBuilder allowed Sgt. Sneary to build a custom query against the textPlus application—which was not supported by the Cellebrite UFED—and recover the additional evidence needed to solidify the case and present it in a readable format in the court proceedings.

MPE+ SQLBuilder and iLogical support for iOS devices are just two of the many unique features built into MPE+ that will assist investigators in overcoming the challenges faced in today's mobile forensic investigations.

ACCESSDATA®

AccessData Group has pioneered digital forensics and e-discovery software development for more than 25 years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil e-discovery of any kind, including digital investigations, computer forensics, legal review, compliance, auditing and information assurance. More than 130,000 customers in law enforcement, government agencies, corporations and law firms around the world rely on AccessData® software solutions, and its premier digital investigations products and services. AccessData Group is also a leading provider of digital forensics training and certification, with its AccessData Certified Examiner® (ACE®) and Mobile Phone Examiner Certification AME programs. For more information, please go to www.accessdata.com.

©2015 AccessData Group, Inc. All Rights Reserved. AccessData, MPE+, Mobile Phone Examiner *Plus*, AccessData Certified Examiner and ACE are registered trademarks owned by AccessData in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners. 112015

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com

LEARN MORE

www.AccessData.com