Case Study

CRITICAL CASE EVIDENCE OFTEN HIDES IN CLOUD APPLICATION DATA

Gallatin, Tennessee Police Department Uses Google Location Data to Close Tough Cases

WHO

Gallatin Police Department, Gallatin, TN; LogicForce Consulting, Nashville, TN

WHAT

Cellebrite UFED Cloud Analyzer helped identify valuable cloud-based mobile data evidence quickly.

WHY

Cloud application data is becoming more critical to investigations. Having access to proven, forensically sound tools to access it quickly, accelerates investigations.

RESULTS

Cellebrite's UFED Cloud Analyzer helped investigators uncover critical location history data to solve several complex, high profile cases.

Mobile device evidence increasingly provides the critical insights that build credibility in criminal cases; to corroborate victims' statements, strengthen physical evidence and reveal otherwise hidden connections between people, places and things. Many times that evidence sits on cloud data servers, where it remains undetected or is accessed too late to be of any use. With Cellebrite's UFED Cloud Analyzer, Gallatin, Tenn. Investigators were able to locate and remotely collect this volatile data quickly - ultimately unlocking intelligence that helped close several big cases.

PRIVATE CLOUD DATA AND LOCATION DETAILS UNLOCK VALUABLE INTELLIGENCE

A former police detective, Jim KempVanEe, now Director of Digital Forensics for LogicForce Consulting, regularly assists the Gallatin Police Force in unlocking mobile device evidence in a wide variety of criminal investigations. As a department reserve officer, he understands firsthand the complexity of quickly obtaining mobile data from cloud data servers and the red tape involved in dealing with service providers to get it. Offering pro-bono services to the department from the LogicForce lab, he has been involved in several recent high-profile cases where accessing that data quickly made all the difference in their outcomes.

"The department brought me in on a case that involved a 12-year-old sexual assault victim who was heavily courted, through social media, by an adult male suspect," said KempVanEe. "The initial evidence we had, included the victim's statements and a single prowler call originating from the girl's house. We felt that if we could corroborate the victim's statements and prove our suspicion that the prowler call was the result of our suspect visiting the victim's home, the prosecutor would feel confident in moving forward with filing felony charges. Understanding the types of private cloud data sources we could obtain with UFED Cloud Analyzer, we requested and were granted an additional search warrant for the suspect's phone that covered the remote collection of social and cloud data. We used the tool to extract a year's worth of Google Location History in minutes, all while awaiting Google's response to our original warrant. With the data we extracted, we established that the suspect had been at the victim's home just prior to the prowler call as well as on several other occasions."

After more in-depth analysis, the Google Location History also revealed the suspect's path of travel, how long he was near the victim's house and the path he took after he departed. KempVanEe noted that the tool provided a lot more intelligence than they previously had, including documenting other extended visits the suspect had to the victim's home – several which directly corroborated the victim's statements.

> **"The remote collection of the suspect's location data greatly reduced the time this suspect remained free in our community. By leveraging the new technology utilized by Cloud Analyzer, my investigators were able to quickly corroborate our victim's statements and develop the probable cause we needed to arrest him for multiple felony sexual abuse charges."**
>
> ***— Chief Donald Bandy, Gallatin Police Department - Gallatin, Tennessee***

"Cloud data is challenging to get," he said. "Many times, investigators simply don't look beyond the evidence that might reside on a phone. Sometimes cloud data may not be sought at all due to the time it takes to write additional warrants and then wait for service providers' responses. Or, by the time we get the data back from the provider, it may no longer be actionable. The prosecutor was thrilled to have this data, because it provided credibility for the victim's statements. Up to that point it really came down to a matter of she-said, he-said. The tool gave us the information we needed in minutes instead of weeks or months. In fact, it took Google over a month to respond to our warrant for this same information."

SPEED CLOUD DATA EXTRACTIONS FROM ANYWHERE

As part of the UFED Pro Series, this exclusive and powerful investigative tool provides investigators with timely access, preservation and analysis of social media accounts. Within preapproved legal boundaries, it allows investigators to collect both existing cloud data and metadata without requiring the investigator to know or obtain account credentials. The tool has the ability to impersonate the user's phone and use the credentials stored within it to perform the remote collection. The data is then packaged in a forensically sound manner either in the field or the lab. Investigators and examiners can then search, filter and sort data to quickly identify the "Who? When? Where?" details to speed investigations from anywhere.

The tool gives investigators the ability to:

- Access private-user cloud data utilizing login information extracted from the mobile device or by using usernames and passwords provided by the subject, retrieved from personal files, contacts or via other discovery means
- Extract information from cloud data sources including Facebook, Twitter, Gmail, Dropbox and other data sources while logging and tracing the entire process to maintain data authenticity

- Extract detailed location information from a suspect's or victim's private Google Location History, stored on Google cloud servers, allowing investigators to track time stamped movements minute by minute
- Track and analyze a suspect's Facebook Likes and Events and Twitter posts and connections to get a better understanding of a suspect or victim's interests, relationships, opinions and daily activities
- Normalize disparate data into a unified format and dynamically visualize multiple data sources in Timeline, File Thumbnails, Contacts or Maps format for easier analysis

In our socially-driven world, it's not surprising that social media posts, as well as other private cloud data sources and location information, have the power to reveal critical evidence in criminal cases. The challenge for investigators is getting to that data quickly. Together with mobile device data, these sources often capture the details and critical connections investigators and prosecutors need to solve a wide variety of crimes. UFED Cloud Analyzer, the first tool of its kind, removes the technology roadblocks involved in getting data access from cloud service providers, reducing valuable time and cost to investigations.

HARNESSING CLOUD DATA TO FIND MISSING LINKS

KempVanEe has used UFED Cloud Analyzer in several other recent cases and said it increasingly makes sense to write warrants for mobile devices that extend to pulling in all known cloud data sources.

"The use of cloud storage has become so closely tied with many mobile devices that it functions as an extension of the device; for this reason, persons may have application data on cloud servers that are not present on the physical device," he said. "Cloud Analyzer is a game changer. The Google Location History data alone has changed the course of some big cases. The criminal element has always been an early adopter of technology; to be successful, investigators must be also."

Click here and learn more about UFED Cloud Analyzer.

ABOUT CELLEBRITE

Cellebrite is the world leader in delivering cutting–edge mobile forensic solutions. Cellebrite provides flexible, field–proven and innovative cross–platform solutions for lab and field via its UFED Pro and UFED Field Series.

The company's comprehensive Universal Forensic Extraction Device (UFED) is designed to meet the challenges of unveiling the massive amount of data stored in the modern mobile device. The UFED Series is able to extract, decode, analyze and report data from thousands of mobile devices, including, smartphones, legacy and feature phones, portable GPS devices, tablets, memory cards and phones manufactured with Chinese chipsets. With more than 30,000 units deployed across 100 countries, UFED Series is the primary choice for forensic specialists in law enforcement, military, intelligence, corporate security and eDiscovery.

Founded in 1999, Cellebrite is a subsidiary of the Sun Corporation, a publicly traded Japanese company (6736/JQ).

To learn more, visit
www.cellebrite.com

For more information contact sales