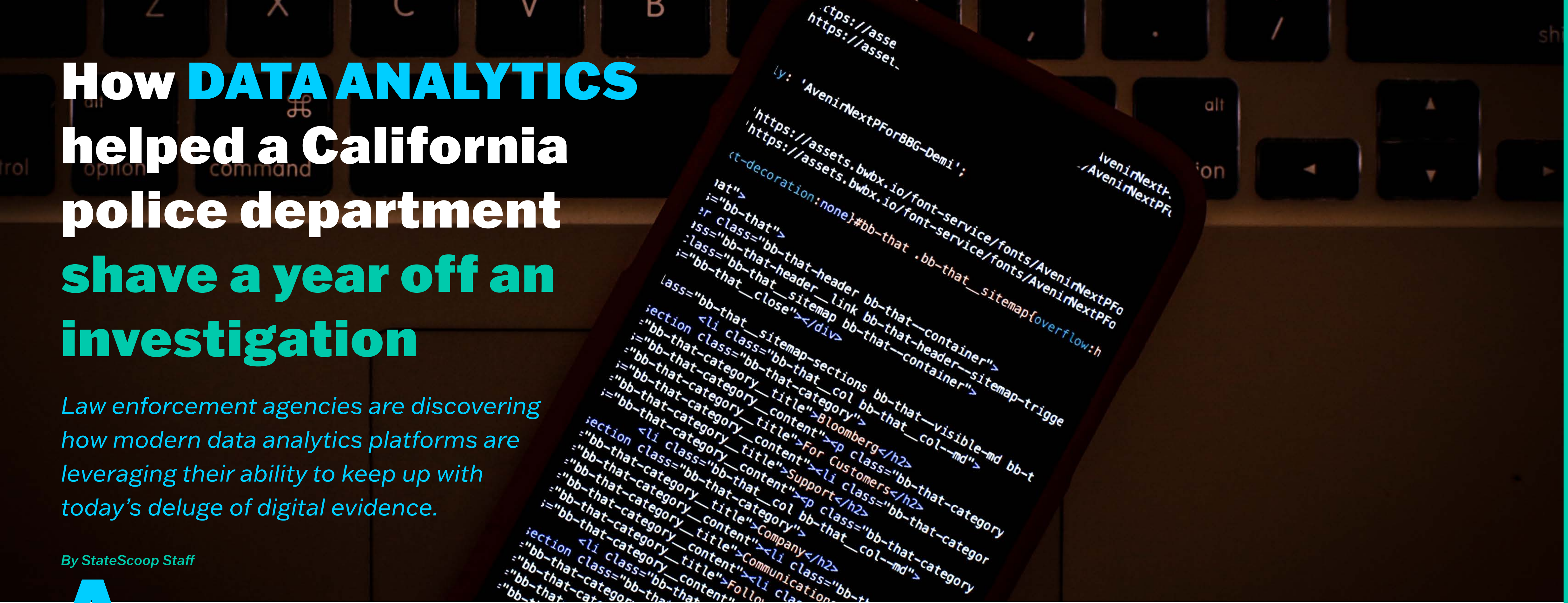


How DATA ANALYTICS helped a California police department shave a year off an investigation

Law enforcement agencies are discovering how modern data analytics platforms are leveraging their ability to keep up with today's deluge of digital evidence.

By StateScoop Staff

A detective, working on a homicide case in a California city last year, was bracing for the arduous investigative work ahead of him. Law enforcement agents had secured the cell phones of four suspects in the case. Now came the task of ingesting and analyzing terabytes of data and determining what clues the data might hold.

It can take days or weeks for most law enforcement agencies to properly process and analyze the digital breadcrumbs on a single smart phone. Stringing together clues from an individual's digital accounts and social media profiles — and making a case that can stand up in court — can take months or even years.

There are software tools capable of helping law enforcement agencies extract and assemble data from cell phones and computers. However, much of the data those tools can capture is encrypted or incomplete. And too often, agents still rely on spreadsheets to catalog potential clues — an approach data experts argue can no longer keep up with the scale, variability and velocity of today's digital forensics demands.

Nearly two-thirds (63%) of cases now include digital evidence as part of the investigation, according to the most recent Digital Intelligence Benchmark Report from Cellebrite. Yet, 96% of investigators and 47% of examiners feel they miss key evidence, in part because of the time and energy required to review digital data.

That made what happened next for that California detective (who wished to remain unnamed) all the more astonishing.

Shaving months off investigations

Paul Jeffery, a Splunk employee, happened to be working with officials at that city's police department to demonstrate the data-crunching capabilities of Splunk's data analytics platform.

Splunk's platform and applications are widely regarded in IT and cybersecurity circles worldwide. Thousands of U.S. public sector organizations use Splunk's security, IT and observability solutions, including:

- All three branches of the federal government and more than a dozen cabinet-level departments.
- All four branches of the U.S. military and multiple intelligence agencies.
- All 50 states.
- 48 out of the 50 largest U.S. cities and the majority of the largest U.S. counties.
- More than 900 higher education institutions.

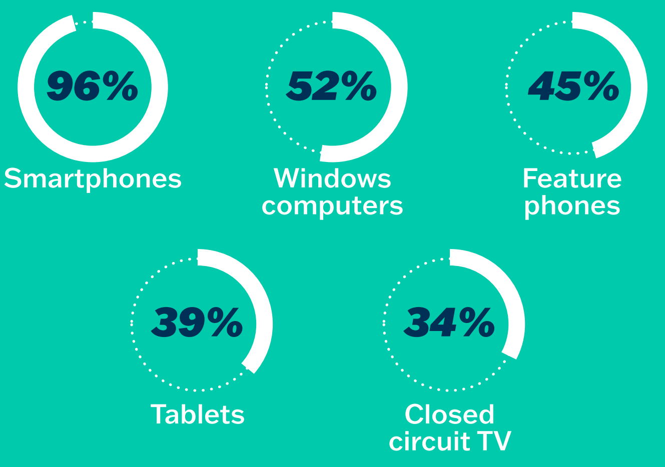
Jeffery began working with the detective and successfully extracted and assembled three terabytes of structured and unstructured data from the various devices and services associated with the case in a matter of hours.

"I asked the detective, 'What questions do you have?'" recalled Jeffery. "I would turn those questions into Splunk searches and the results into reports. We were just banging out searches and reports. The detective was completely blown away at the speed that we were able to create them. Then we exported a few of them and handed them over to the prosecution and defense attorneys to review," he said.

"I remember taking our first reports to the district attorney — documenting communications between the suspect and the victim. And his office immediately called back and said, 'What is this? How did you get this done so quickly?'"

Jeffery had to explain to skeptical attorneys how Splunk works. They are used to waiting days or weeks for answers to their questions, he said in an interview. "It's just their normal cadence. I was able to show them if they needed an enhancement to the report, or had questions about it, how I'm able to go into the platform, pivot in a matter of minutes, complete the requested changes and pull together an updated report."

Frequency of digital evidence appearing in investigations in 2021:



Biggest digital challenges:

56%	Inability to extract data from encrypted apps
54%	The amount of data that needs to be extracted
47%	Not getting enough data from the device"
36%	The volume of phones
36%	Inability to decode artifacts

Source: 2021 Digital Intelligence Benchmark Report

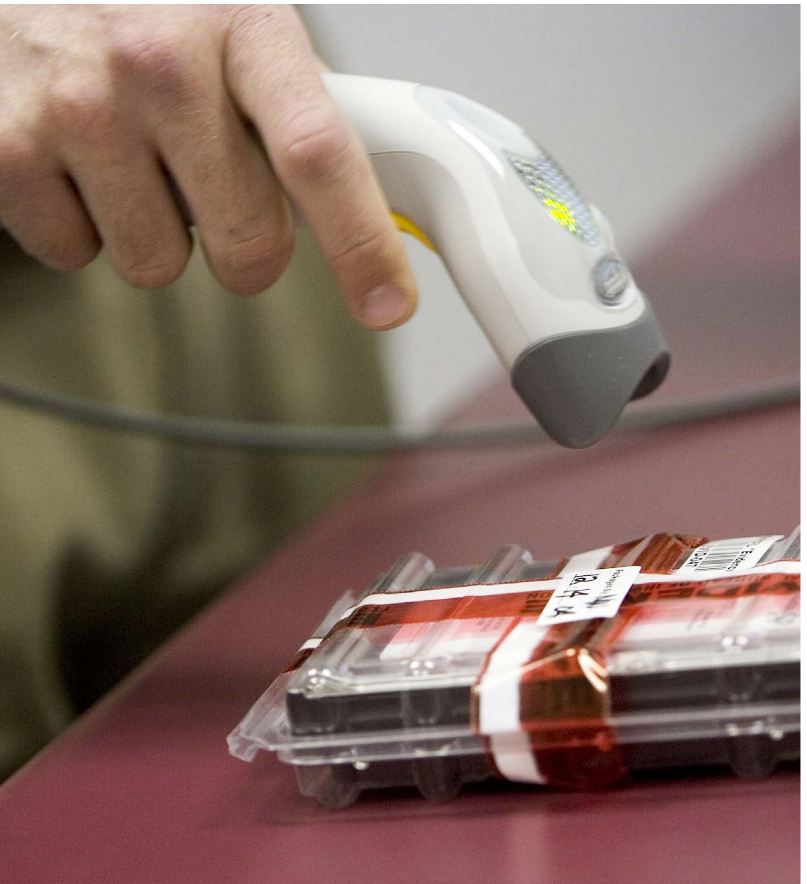
In the months since Jeffery first teamed up with the police department, he said, "I've been told by both the detective and the prosecution attorneys that using Splunk's platform and applications shaved 12 to 14 months off the investigation, which is massive. They were looking at a three-and-a-half-year gap between the crime and trial — and we knocked just over a year off of that. To them, it was unprecedented."

> ***"I remember taking our first reports to the district attorney — documenting communications between the suspect and the victim. And his office immediately called back and said, 'What is this? How did you get this done so quickly?'"***
>
> ***-Paul Jeffery, Splunk***

Fast-tracking investigations

Splunk's platform correlates data, performs advanced analytics on various data sources and applies built-in AI to quickly identify unusual behaviors or anomalies that point to criminal activities — helping law enforcement agencies move faster on a growing array of criminal investigations cases, including:

- **Paycheck Protection Program (PPP) loan fraud** — Where Splunk's solutions helped investigators identify scammers who illegally diverted and stole as much as $100 billion in federal aid intended to help millions who lost their jobs.
- **Civil discourse** — Where Splunk's platform and applications helped law enforcement investigators in the aftermath of 2021 civil unrest to review troves of data from disparate data sources and identify tens of thousands social media links involving hundreds of subjects. Splunk's solutions can also analyze data following events for discovery, cold cases, intelligence and investigative purposes.
- **Apprehending a child pornography ring** — Where Splunk's platform and applications helped the police department at Florida State University, working with federal investigators, assemble FSU internet logging data to track and ultimately apprehend students who were buying and selling child pornography on campus.



- **Human trafficking** — Where the Global Emancipation Network (GEN) and Splunk solutions teamed up to develop Minerva, an analytics platform that takes unstructured, siloed data from hundreds of sources to help identify and stop human trafficking operations. Through GEN and Splunk for Good, Minerva is free to national and international government and law enforcement agencies, NGOs, academia and the private sector. Additionally, GEN launched a program called Artemis, partnering with Accenture. Artemis helps hotels and massage businesses identify risks and vulnerabilities before a crime is committed.
- **Following the money on criminal activities** — Where Splunk's platform and applications are helping various state and local law enforcement agencies trace the digital fingerprints on financial and cryptocurrency transactions associated with everything from drug distribution to human trafficking, ransomware, elder abuse to fraud.

Because police departments typically rely on the technical support provided through state, county, and municipal IT departments, law enforcement officials often aren't aware of, or lack the wherewithal to use, Splunk's powerful analytical capabilities, according to Jeffery.

But that's changing, he said. Police chiefs are learning how Splunk's applications — which are available in cloud-based environments, including Amazon Web Services, or through managed service providers — eliminate the need to invest in additional IT equipment and licenses. The applications also offer the advantage of meeting numerous government-approved security standards from the start.

Leveraging crime analytics

Another area where Splunk's analytic solutions are proving especially useful to law enforcement officials is in helping them allocate resources more effectively, by better understanding changing neighborhood crime patterns and public safety issues.

Police chiefs juggle many competing priorities and risks. Every day, they face the chronic question, "Where should we send our officers today?" Part of that challenge lies not in a lack of crime and public safety data. Rather, it's making sense of an overwhelming amount of data.

Having a powerful data analytics platform, capable of managing any type of data to support daily operations is essential. Splunk's platform and applications help agencies cut across silos of operations and brings all relevant information in one place to offer holistic visibility to solve a variety of challenges across security, IT operations, and public safety programs. That includes the ability to:

- Address a wide and unpredictable range of threat, vulnerability, and risk elements.
- Improve effectiveness and resilience when called upon under emergency conditions.
- Increase operational efficiencies under routine conditions.
- Demonstrate responsible investment of taxpayer resources.
- Improve quality and performance, while leaning into future capabilities and needs.

Meanwhile, a growing community of police departments are beginning to share their crime dashboard models and programming updates with one another on GitHub, a popular hosting service for software developers, according to Jeffery. That's allowing police departments to adopt the digital analytics capabilities of other departments — in some cases around specific types of crimes — and ultimately improve their ability to allocate limited policing resources.

Addressing staffing and skills shortages

A third factor prompting police departments to consider using Splunk's platform and applications is the ability to address staffing and skills shortages, by automating a wider range of data processing and analytics tasks.

"Police departments, and many state and local law enforcement agencies, simply aren't fully prepared to handle 21st-century crimes, especially ones that involve copious amounts of data — not just by volume, but more importantly, the variability of data," observed Jeffery. That includes the growing number of cybercrimes that law enforcement agencies must respond to.

Even relatively advanced police departments are still trying to manage cases using CSV and Microsoft Excel files that are time-consuming to maintain and prone to errors, he said, adding. "It's almost akin to what you see in the movies, where detectives are pinning up clues on the wall and using yarn to connect their clues."

By being able to harness the power of automation built into Splunk's applications, law enforcement agents can process and analyze much larger volumes and varieties of data than in the past — and far more quickly.

Jeffery acknowledges that a sophisticated solution like Splunk requires a certain degree of training. However, the ability to dramatically accelerate investigations and improve operational decision-making using a tool as powerful as Splunk's platform is a game changer, he argued.

Thinking back to his work with the California detective and the challenges today's police departments now face, Jeffery also maintains that higher education institutions teaching criminal justice courses need to catch up with the times. They have to do a much better job moving future law enforcement professionals into the digital age, he said.

But police departments and law enforcement agencies also need to accelerate their embrace of today's modern data analytics platforms if they are to keep up with the deluge of digital evidence, he concluded.

***Learn more** about how Splunk's data analytics platform can help your law enforcement agency work faster and more productively.*

STATESCOOP | FEDSCOOP

splunk>