PENLINK

Investigator Spotlight: An Expert Q&A Series

"Digital evidence is a time machine": A detective shares how his team uses PenLink to animate data and provide context

In each edition of PenLink's monthly Q&A series, we interview investigative experts to understand the impact of digital evidence in today's investigations. This month we sat down with ***Tim Spitzer, a detective with the Galesburg Police Department,*** *to talk about how investigations have changed with digital evidence. Detective Spitzer says digital evidence can be like a time machine, showing "where a person was, what they were doing, and sometimes even what was on their mind at the time of a crime."*

Q: How has the investigative process changed with technology?

A: It's changed drastically in the last few years. Three years ago, the most important focus at the scene of a crime was on witnesses, video, and fingerprints/DNA. Each of those types of evidence has strengths and weaknesses:

- Witnesses can have an impact, provided they are cooperative and reliable, but that's becoming more rare. Witnesses also have a human tendency to be contradictory, incorrect, and even off-putting in a court setting.
- Video evidence used to be the cream of the crop. It was usually the first thing judges and attorneys seemed to ask about in a case. A typical law enforcement phrase was, "If it didn't happen on video, it didn't happen." That statement was true even given a law enforcement witness account: if it wasn't corroborated with video, it was too risky for a prosecutor to try in court.
- Fingerprints and DNA obviously have their strengths in a case, and they provide that "crime TV" aspect in the courtroom that a jury expects. Their weakness is their lack of context.

Now, digital evidence is the new video and DNA. Of course, we still gather witnesses, video, and DNA at a scene if we can, but we make it a point to get accessible digital evidence. Accessibility is key. The difference between getting access to a powered mobile device and getting access to an unpowered one could be calculated in years. We treat a phone left at a crime scene as a confession written in ice: we want to secure it, keep it charged, and get the radio signals deactivated (i.e., airplane mode and Bluetooth off) as soon as possible. Without access to the device, acquisition and analysis aren't possible.

"There are cases we have cleared recently that would never have come close to an arrest, let alone a conviction, had it not been for digital evidence."

Tim Spitzer
Detective

The same goes for learning online account names. Three years ago, we wouldn't have asked for a suspect's email address; we used to ask for phone numbers, addresses, and nicknames.

Now, many criminals don't particularly live anywhere, and their phone numbers often change. However, when it comes to keeping the same online profile (and keeping all their followers/clients/contacts), they tend to be more reliable.

One would think criminals would avoid using mobile devices and social media when committing crimes, considering all the evidence captured by digital data. However, modern-day criminals use technology to enhance their criminal efforts. Dealing drugs is far easier when you can just exchange a couple of messages and send money through Cash App. Showing someone you have a gun to protect yourself is easy with a simple video or image. Getting information on a location, person, or business is often just a Google search away.

Q: What impact does digital evidence have on clearing your cases?

A: There are cases we have cleared recently that would never have come close to an arrest, let alone a conviction, had it not been for digital evidence. In the proper hands, accessing digital evidence (especially from mobile devices) is like using a time machine. With the right circumstances and access, you can figure out where a person was, what they were doing, and sometimes even what was on their mind at the time of a crime.

The most powerful impact of digital evidence is the objective truth it provides. A witness might have a different memory of an event; a video might not be at a high enough resolution to show what happened, or confirm the identity of the subjects in view; but digital evidence leaves little space for argument.

A defense attorney isn't going to ask me, "Are you sure my client Googled 'How do I get rid of a dead body'"? A defense attorney *can* ask, "Why are you so certain my client's phone was pinging off this tower in this direction?" but the answer is always going to be the same: because that's what the data indicates.

A jury has very little reason to doubt the motive of data—it has none. Attorneys love to paint pictures of witnesses' motives or the professional abilities of law enforcement officers, but they can't do the same with data. The data often speaks for itself, and it usually spells out G-U-I-L-T-Y.

Q: Research shows that investigators believe that digital evidence is more important than DNA evidence. How would you say this applies to your jurisdiction?

A: My agency has completely embraced the investigative results of digital evidence analysis, and have prioritized admitting it into the courtroom.

Digital evidence also comes with authentication letters, which are certifications from big tech companies allowing the data to be brought into a courtroom without a legal representative. DNA evidence, on the other hand, still requires a forensic scientist to be subpoenaed for testimony—and a forensic scientist can tell you whose DNA it is, but they can't necessarily tell you how it got there, or when.

Digital evidence often has all sorts of contextual supplemental data to go with it. For example, GPS might show a suspect's device at a crime scene, just like DNA could. But the digital evidence may also show the device arriving at the scene minutes before the crime, then departing shortly after. The digital evidence might also include phone calls, messages, and media indicating who the target was communicating

with before, during, and after the crime. Some of our "smart" criminals even use police-scanner apps on their mobile devices, or search for police-scanner apps on the internet around the time of their criminal activity. DNA doesn't show that kind of information.

Q: Has PenLink made your team more efficient?

A: The PenLink platform is a powerful tool when it comes to digital investigations, but it also doubles as mental-health medicine. If I had to decipher every bit of code in the millions of digital artifacts we come across, I would be the one going on a rampage! I have a theory that the people who developed PenLink did a study on what law enforcement complains about, and then developed software to solve those problems.

An obvious obstacle with digital evidence is the vast amount of it out there, and the time, knowledge, and patience needed to analyze it. Analyzing GPS data and tower data alone is a cumbersome process that takes unfathomable numbers of work hours. PenLink solved that problem for my unit. If you have a task that looks annoying and cumbersome, PenLink probably does it for you.

It used to be commonplace for us to worry about getting a guilty verdict, or even charges filed, on cases where we'd invested a lot of our time. Now we make guesses on how much prison time the offender is going to serve. Our community is benefiting from PenLink, and we have the stats to prove it.

Q: What's your favorite investigative tip?

A: My favorite tip would have to be importing XML files of our map data into PenLink. Traditionally, my investigations have involved mobile devices, such as iPhones. A full filesystem extraction from an iPhone will often involve cached location data from a device that may contain 40,000 GPS locations. Instead of checking thousands of GPS locations in the Axiom or Cellebrite file, I can export the data in XML format and autoload it into PenLink, which then recognizes the data as locations with timestamps.

I then usually start with data surrounding the timeframe of a crime, and create a map in PenLink. A quick animation of the data then provides me with a clear understanding of where that device was during the time of the crime, which tells me if I'm going in the right direction. It also tends to be the most powerful piece of evidence in the courtroom.

Q: As a user of PLX Connect, do you have a tip to share?

A: My agency is still in the early stages of using PLX Connect, but I can say that usernames and phone numbers can be the key to an investigation result. Often, a new name or phone number will show up in our jurisdiction. The new name might not mean anything to my agency at first glance, but when we find out via PLX Connect that the name means something to another agency, we can quickly draw the connection and learn more about our new suspect.

Q: How are the expectations for investigations evolving, and how are you preparing for those changes?

A: One of the issues with digital evidence is that it can actually be too effective—it can cause officers to get complacent, and attorneys to think that every case will be the same and barely even argue the evidence. One of our fears is that law enforcement could pick up a suspect's phone at

the scene, and do nothing else! But there are still times when we don't have digital evidence, or a device is not accessible. Sometimes an offender uses incompatible devices, or has major settings deactivated. Digital evidence greatly supplements standard police work, but it doesn't replace it.

Our biggest task in law enforcement is explaining to attorneys what the digital evidence means, and how strong the case is. But I've met with defense attorneys who have stated that they also appreciate the strong evidence. A lot of defense attorneys often chase down leads provided by their clients which they later find out are false, and I've been told that digital evidence can help the defense show their client how likely they are to lose, and to help them make the case for a reasonable plea agreement. So the strength of digital evidence can help our outcomes that way, too.

*Thank you to **Tim** and the entire **Galesburg Police Department** for their commitment to keeping their community safe—and to Tim especially, for his willingness to share his experiences with us.*

If you would like to participate in our Q&A series, please contact info@penlink.com. To learn more about PenLink and view additional resources, visit penlink.com.