

Press Release

New app streamlines digital evidence collection

SLO County investigators have a new tool which helps them keep up with changing technology when collecting digital evidence

San Luis Obispo, CA – January 1, 2019.

[Summary] SACRAMENTO BEE | INVESTIGATIONS – The Central Coast Cyber Forensics Lab (CCCFL), in collaboration with Cal Poly’s Digital Transformation Hub (powered by Amazon Web Services), has released a new mobile application that coaches crime scene investigators on how to collect digital evidence in a legally compliant way. Given the fast pace of technological change, the types of devices that the public uses change every day, making it hard for even seasoned crime scene investigators to properly collect key digital evidence with the confidence that it will be admissible in court. The Digital Evidence Expert mobile application changes that.

[Opportunity/problem] Until today, both new and experienced investigators had to collect digital evidence at crime scenes from a variety of unique and ever-changing technology devices in the field. This creates uncertainty for investigators, especially those new to the force, around how to collect digital evidence legally. Per U.S. Constitutional Law and State law (CalECPA – California Electronic Communications Privacy Act, SB 178), digital evidence is required to be collected in a compliant way to protect citizens’ rights. If digital evidence isn’t collected in a compliant way, it is inadmissible in court. Collecting a popular cell phone model without compromising the device is easy enough for an investigator who owns that same phone or has been trained to do so, but having to keep up with the wide array of other commercially available mobile devices can cause confusion to investigators unfamiliar with those devices. Investigators not only have to collect mobile devices, but they also must collect laptops, routers, servers, and a variety of other technologies that may contain evidence that could make or break the case.

[Approach/Solution] Collecting this evidence in a consistent and constitutionally compliant way throughout the law enforcement community is key to ensuring that a crime is fairly processed through the justice system. With the Digital Evidence Expert application, investigators can now access device specific, step-by-step instructions on how to properly collect digital evidence in the field. The investigator can provide the application with the make, model, type, current state of the device (open, unlocked, password protected, etc.) and the application will provide accurate and up-to-date collection advice, including a hotline to an on-call digital forensics expert to address complicated scenarios. This new capability provides the investigator with the confidence they need to move forward with the evidence collection process.

[Customer experience] *“When an investigator enters a crime scene they might see several different types of electronic devices that might hold key evidence related to the crime. That can be overwhelming even for seasoned investigators”, said a San Luis Obispo Sheriff’s Office Detective. “The investigator might see a laptop that is open and not password protected. If she’s new, there is a good chance that she has never dealt with this scenario before. Now she can pull out her phone and open the Digital Evidence Expert application. She can navigate to ‘laptop’ from the application menu, provide further details, and the application will show her exactly how to collect and preserve the machine without manipulating it. A video tutorial is also available to remove any doubt about the instructions. Once she completes the evidence collection and delivers it to her local station, it eventually becomes a part of the case file and is used to prosecute (or defend) the criminal. During the trial, when the Defense Attorney questions her about how she collected the evidence, she can confidently walk through the steps that she took, leaving no doubt to the judge and jury as to whether the evidence was properly collected. That certainty is huge and will have a meaningful impact on our justice system.” Said the Detective.*

[Customer quote] *“This new mobile application guides me in the collection and preservation of digital evidence.” Said Investigator Mendoza, “It walks me through the process of collecting different types of devices, from specific cell phone models to servers. Technology changes so much it can be hard to know how to handle the latest and greatest gadget. If it is a really complicated situation it connects me to an on-call expert so I can be certain that I am collecting the evidence in the right way. This tool helps me to do my job better and gives me confidence that the*

evidence I collect in the field will be admissible in court and that I will be able to provide that same level of confidence to the judge and jury."

FICTIONAL PRESS RELEASE

Customer FAQ (Front Line Officer)

Q: How is it going to help me do my job better?

A: The Digital Evidence Expert will provide me with support to properly collect and handle data collected from crime scenes, so that it is permissible in a court of law.

Q: Do I have to take a class?

A: No, the application is a self-taught program. It is easy to use and accessible.

Q: Are there privacy concerns? Do you track my location?

A: No, we are not tracking your location, but do we want to know which law enforcement agencies (LEA) are using the application through a one-time sign-in.

Q: Can I use this on my own phone? Do I have to use the application?

A: The application will be made available on iOS and Android platforms.

Q: Does it work offline?

A: The application will require an internet connection to be able to iterate through the California District Attorney Association's (CDA) database of evidence and search warrants.

Q: Does this report my evidence collection activity to my manager? To a statewide database?

A: The application does not track the user, it is meant to serve as an assistive technology. It collects a time stamped record of when an investigator collected data for their own personal use and reporting. It does not collect any other data.

Q: What is the benefit of using it?

A: LEA first responders will be better equipped to secure crime scene devices and will receive accurate guidance to properly collect and preserve digital evidence on those devices.

Q: Do I have to use this? What happens if I don't?

A: This application is meant to serve as an assistant to help ensure the proper collection and handling of evidence from a crime scene. It helps to assist the investigators in following legal compliance for evidence to be submitted in court.

Q: What happens if I follow the instructions and the evidence isn't admissible but it was the application's fault not mine?

A: The Digital Evidence Expert is a support tool and offers support for first responders, but the application and company do not claim responsibility for usage.

Q: Where do I get help? What if I have questions?

A: Contact the Central Coast Cyber Forensics Lab.

Q: How often is the application updated?

A: When significant iOS and Android updates are made available.

Stakeholder FAQ (Management, Staff, Community)

Q: What does it cost?

A: Costs are being currently evaluated and assessed to understand the cost of the application at scale throughout the state of California.

Q: Who maintains and controls the application?

A: A state entity is exploring the feasibility of developing hosting and maintaining this application as a state-wide shared services solution. Additionally, options are being explored with third parties to assess alternate delivery options.

Q: If I use the application, do I need to submit my digital evidence to the CCCFL's services?

A: No, there are no contractual or other obligations to utilize CCCFL services if you use this application.

Q: Is the application secure?

A: The application securely communicates between the cloud and the device using an encrypted connection. It also follows all best practices for secure application development within the cloud. If you would like to read more about cloud security, please visit Amazon Web Services (AWS) Cloud Security.

Q: Do I need to train my staff?

A: The application is meant to be as intuitive to use as possible. Additional training content will be developed and published online for ease of access and use.

Q: Where does the content come from?

A: Content provider options have been explored through a number of different public and private data sources, along with assessing ongoing support and updates to the data set themselves.

Q: How is data stored? Is it Criminal Justice Information Services (CJIS) compliant?

A: The application only stores procedure information and does not store information that would fall under CJIS compliance.

Q: Will there be personally identifiable information (PII) collected or stored?

A: No.

Q: How much time will it take to get familiar with it?

A: The application is designed to be as intuitive as possible. Based on user testing, it takes only a few minutes to get familiar with the application and use it to collect digital forensics.

Q: Will it be updated and current?

A: The intent is for the content to be as up-to-date and current as possible. This is one of the key value propositions of the application.

Q: Will this application collect data on evidence?

A: The application will only keep track of the fact that evidence was collected. It will not keep detailed information on what was collected or who it was collected on.

Q: Is data collected at all through this application?

A: It collects a time stamped record of when an investigator collected data for their own personal use and reporting. It does not collect any other data.

Q: Do you collect application usage?

A: Only a record of when an investigator collects evidence for their own personal use.

Q: How do I know if your application is being used by investigators? And by who?

A: We don't collect data-points on users in order to increase adoption rates. Any data in the application is self-reported by the investigator.

Q: How is the application distributed? Is it on public application stores? Is it only privately accessed?

A: This application would not be publicly distributed. It would be distributed privately to agencies that want to use the application.

Q: Is this application compatible with different types of phones? And devices?

A: It will be compatible with both iOS and Android devices.

Q: How is the application updated and maintained?

A: The application will be updated and maintained by the team that develops it.

Q: Who is going to fund this application?

A: Funding opportunities are currently being explored and assessed to account for both up-front costs to develop the application and long-term maintenance and support. Cost recovery options are also being explored to establish a sustainable economic model.