Digital Evidence Collection Expert

Helping Investigators Gather Court Admissible Digital Evidence

April 2019

Challenge Sponsor: Central Coast Cyber Forensics Lab

Cloud Innovation Center Sponsor: CAL POLY | Digital Transformation Hub
Powered by AWS

Table of Contents

Introduction

In July 2018, California Polytechnic State University's Digital Transformation Hub (Cal Poly DxHub) embarked on the digital evidence collection Innovation Challenge, with a focus on how San Luis Obispo County law enforcement agencies could enhance and optimize their ability to collect, process, and analyze digital forensic evidence. During an Innovation Workshop with a diverse group of stakeholders, the DxHub applied Amazon's Working Backwards process to reach consensus on a customer obsessed solution. The solution prototyping scope was then defined in the Solutions Workshop. By January 2019, a clickable mobile application prototype was developed by seven Cal Poly students, Central Coast Cyber Forensics Lab (3CFL), California Cyber Institute (CCI), Amazon Web Services (AWS), and Cal Poly DxHub personnel.

Problem Statement

Initially, the 3CFL team was focused on how to provide a common platform to store and analyze digital forensics data for law enforcement county-wide. Upon diving deeper into the overall digital forensics landscape, discussions turned to the larger problem of inconsistent digital evidence collection practices by law enforcement agencies. 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. Additionally, state laws frequently change, requiring law enforcement agencies to comply with digital collection standards above and beyond constitutional protections. The issue of inconsistent digital evidence collection is compounded by the variety and evolution of device types (e.g. cell phones, storage devices, servers), makes, models, software updates, and collection considerations and requirements. This necessitates that digital evidence collection processes continuously advance with device technology. This multifactorial digital evidence collections process has resulted in a confusing landscape for law enforcement agencies. They need help discerning exactly how to properly collect a given piece of digital evidence to ensure it will be admissible in a court of law.

Innovation Workshop

An Innovation Workshop was held by the DxHub to guide digital forensics experts, investigators, and a former Assistant District Attorney through Amazon's Working Backwards process. During this process, the diverse team examined the pain points and needs of the customer (an investigator collecting digital evidence), and empathy mapped the following insights:

Customer (investigator's) Pain Points

- Revolving Door
- Lack of Standardization
- Boxed Thinking/ Compartmentalization
- Short Sightedness
- Being asked: "Why didn't you…(comply)"

Customer (investigator's) Needs

- Personal Satisfaction
- Collaboration
- Doing their job right
- Keeping up with technology
- Ability to answer: "Why didn't you…(comply)"

Ideas were generated by the team based on these insights and a wide variety of concepts emerged, ranging from data collection walkthrough tools, artificial intelligence enabled assistants (i.e. Alexa), field collection kits, and more. The team ultimately drove to consensus on defining a solution that included a mobile application that would guide an investigator step-by-step through the digital evidence collection process, specified by current policy and device type, make, model, and software. The application would also provide the ability to issue a record of data processing activities that an investigator could present to the court to validate steps taken when collecting digital evidence. The ideated solution was honed further in a Press Release/Frequently Asked Questions (PR/FAQ) document which is used to provide a foundation for the proceeding Solutions Workshop (Appendix 1).

Solutions Workshop

During the Solutions Workshop, the team reunited to define the technical implementation and scope of the application prototype. By creating a storyboard, the team was able to illustrate the customer experience and key customer benefit(s) from the application solution (Appendix 2). From this, a common customer experience theme emerged; the investigator should be able to simply identify different devices via pictures, and work down a decision tree to locate the correct digital evidence collection procedure. The prototype was scoped to a clickable User Experience Design/User Interface (UX/UI) mockup to gather feedback from investigators that collect digital evidence (Appendix 3).

With the help of seven students from Cal Poly, the prototype was built using the design tool Figma®. This tool allowed for quick iterations on the concept, without introducing the complexities of creating and managing working code. After multiple design reviews with 3CFL and investigators from San Luis Obispo County, a final prototype was completed. From there, multiple investigators with varying levels of technical skill tested the application prototype under a mock scenario. The test objective was to confirm that investigators could use the application to identify the correct digital evidence collection procedure from an unknown device. During prototype testing, user feedback was

gathered and the mock scenario test results were collected to establish prototype functionality. A conceptual architecture was then created to illustrate what the final product may look like if the prototype was developed into a production-ready application (Appendix 4).

Value Proposition

The Digital Evidence Expert mobile application's core value proposition is to provide simplicity, clarity, and confidence to investigators collecting digital evidence from a variety of device types, makes, models and software. The application's ability to standardize behavior around digital evidence collection also ensures that all collected evidence would be admissible in court. Providing the investigator with the right information at the right time, as well as a record of steps taken, would ensure consistency in digital evidence collection. The following feedback was collected from investigators that consulted on this challenge:

Q: Would you use this application to help collect digital evidence?
A: "100%"

Q: As a more advanced technical user, would you recommend this application to investigators?
A: "Yes absolutely. Even as an advanced investigator, this adds value for me."

Q: Do you think it provides value?
A: "It definitely would provide me with the confidence that I need to collect digital evidence correctly."

Conclusion

The Digital Evidence Expert mobile application has the potential to help investigators collect and secure digital evidence in a way that is admissible in court and ensures every citizen's right to data privacy. This Innovation Challenge demonstrated two key concepts: 1) solving a big problem requires starting with something small and actionable, and 2) that a solution does not need to be overly complex to provide significant user value.

Next Steps

Several statewide law enforcement agencies have indicated an interest in participating in a pilot program. This provides ample opportunity to take the solution into a realize value phase, with the potential for statewide scale out.

Special Thanks

Special thanks to the San Luis Obispo County District Attorney's Office, San Luis Obispo Sherriff's Office, Central Coast Cyber Forensics Lab, CA Cybersecurity Institute, and Cal Poly Students.

Appendix

Appendix 1

Press Release / FAQ. During the Innovation Workshop, a fictional Press Release is drafted as a mechanism to articulate the most promising idea discovered.

Appendix 2

Storyboard. A Working Backwards mechanism, used to articulate the customer experience and key customer benefit(s) of the application solution.

Appendix 3

User Experience Design/User Interface (UX/UI). A tool used to gain user feedback on the application prototype.

Appendix 4

Solutions Architecture. The process diagrams