Y26 Cost-Effective Robust Authentication and Environmental Monitoring of Forensic Evidence

Peter Gompper, San Francisco, CA*

Learning Overview: After attending this presentation, attendees will have learned about the weaknesses of existing forensic evidence containers as they relate to the detection of lost, counterfeit, or degraded material. Attendees will also have learned about the utility of the "last mile" problem when developing solutions to these problems, and why custody-chain tracking is unable to support solutions to such events. Finally, attendees will have learned about recent innovations in packaging and how they support reliability and efficient evidence processing.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by describing and elaborating on the necessity of secure unit-level evidence packaging as the optimal means of meeting guidelines. This presentation will also propose performance actions, including how best to: (1) detect an incursion across the surface boundary of an evidence package; (2) authenticate evidence using encryption; (3) register the environmental status of biological evidence; (4) support custody chain requirements (i.e., data regarding location, date, responsible contact, etc.); and (5) support inspection readiness efforts and performance initiatives for agencies unequipped with advanced evidence management systems.

From crime scene to presentation at court, forensic material evidence is at risk of careless handling, theft, counterfeiting, tampering, and environmental degradation. Such "triggering events" can become liability issues for law enforcement agencies, crime labs, courts, and communities dependent upon the credibility of criminal justice systems. Property and evidence managers attempt to mitigate against a wide variety of events by manual and semi-automated processes that focus on custody chain monitoring, tracking in-transit evidence, and controlling access to evidence rooms. The weakness of both manual and semi-automated systems is the lack of unit-level detection of an event. For instance, containers with unique identifiers—such as signature lines, barcodes, or adhered Radio Frequency Identification Devices (RFID) tags—can easily be broken, copied, replaced, or decrypted to thwart systems-level security. Without robust unit-level security, systems-level weaknesses leave evidence at risk, at any point along the custody chain.

To reliably and conveniently authenticate evidence without additional cost or burden to evidence handlers, an electronic Tamper-Evident Packaging (eTEP) was developed. The packaging acts as a one-time irreversible surface monitor capable of communicating to smart phones, electronic devices, and evidence management systems in the submission, handling, presentation, and disposition of items of evidence. Additionally, to support best practice in the maintenance and integrity of biological evidence, the eTEP laminate was designed to detect environmental changes (as outlined by the National Institute of Justice/National Institute of Standards and Technology (NIJ/NIST) Technical Working Group on Biological Evidence, NIST Interagency/Internal Report (NISTIR) 7928).

As a part of the National Science Foundation's I-Corps program, this presentation will outline the innovation to conference attendees and request feedback and insight regarding potential usability within varying agencies.

Evidence, Monitoring, Theft

*Presenting Author