



C16 The Development of a Cleaning Protocol for Mobile Devices Contaminated With Controlled Substances

Rachel Valerio*, Marshall University, Huntington, WV 25701; Josh Brunty, MS, Marshall University, Huntington, WV 25701; Lauren L. Richards-Waugh, PhD, Marshall University Forensic Science Program, Huntington, WV 25701; Dale Mosley, West Virginia State Police Digital Forensics Unit, Huntington, WV 25701

Learning Overview: After attending this presentation, attendees will understand the dangers digital forensics analysts face with regard to drug exposure and will learn decontamination protocols that will protect analysts while allowing for digital data acquisition.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing protocols that support both the digital forensic analyst's safety and digital data acquisition when cleaning digital devices contaminated with controlled substances. The focus of this presentation is on the decontamination of mobile devices from various illegal and potentially dangerous drugs, such as heroin, cocaine, methamphetamine, and fentanyl/carfentanil. In addition, this presentation will recommend appropriate Personal Protective Equipment (PPE) that is vital to the safety of the digital analysts.

Digital evidence submitted with potentially undetected dangerous illicit substances has become a huge concern in the digital forensics community. While there are suggested protocols and best practices to collect liquid, structurally, and thermally damaged devices, there is little-to-no accepted protocol within the forensics community to effectively clean drug-contaminated devices that ensures both the safety of the analyst and a complete data acquisition from the mobile device.¹

A set of 60 Blackberry® 8330 Curves and Blackberry® 9330 Curve 3s were utilized for this research. Initial hash values and total size from file system and physical acquisitions were obtained using Cellebrite® UFED 4PC version 7.18.0.199 for all of the devices used. Both industrial and household cleaners were used as decontamination cleaners. The industrial cleaners tested include: Apple® Environmental® Meth Remover Parts 1 and 2, First Line Technology® FiberTect Polyester Pads/Wipes, First Line Technology® Dahlgren Decon 200mL Ready-to Use Configuration, and Intelgard® EasyDECON Parts 1 and 2. The household cleaners included Lysol® Fresh & Clean Multi-Surface Cleaner, Formula 409® Multi-Surface Cleaner, Alconox, Inc.® Liquinox 1232 Critical-Cleaning Liquid Detergent, Fiberlock Technologies® Shockwave-Concentrate, and Scrubbing Bubbles®. Each controlled substance was diluted in methanol and run on a Gas Chromatograph/Mass Spectrometer (GC/MS) equipped with a Restek® DB-5 column (30.0m x 250µm id x 0.25µm particle size) to obtain reference data. The devices were then systematically exposed to each drug, and the presence of the drug was confirmed using the GC/MS. Each cleaner was used to attempt to clean the controlled substance from the device to the point of no detection. Cleaning steps were repeated if the drug remained detectable.

Data acquisitions from each digital device were obtained both immediately after the cleaning process and one week after to simulate the environment of a working digital forensics laboratory. Advanced data extraction techniques such as chip-off or JTAG were attempted if a traditional cable acquisition was unsuccessful. The data acquired after cleaning was compared to the initial hash values and flash.bin file sizes. The success of each data acquisition was then used to create a list of recommended decontamination methods for digital devices contaminated with the tested controlled substances.

Reference(s):

¹. SWGDE Best Practices for Collection of Damaged Mobile Devices. *Scientific Working Group on Digital Evidence*, Version 1.1. 2019.

Damaged Devices, Controlled Substances, Cleaning Protocols