C6 The Development of Protocols for the Analysis of Mobile Devices That Have Been Submerged in Oil-Based, Flammable, and Clandestine Chemical Liquids

Nico Kresl, Huntington, WV 25704; Chelsey McPhillen*, Port Washington, OH 43837; HollyAnn D. Swann, BA, MUFIA, Huntington, WV 25701; Steven B. Watson, BA, VTO, Broomfield, CO 80021-8042; David Rathbone, VTO, Broomfield, CO 80021; Lauren L. Richards-Waugh, PhD, Marshall University Forensic Science Program, Huntington, WV 25701; Joshua L. Brunty, MS, Marshall University, Huntington, WV 25701; Catherine G. Rushton, EdD, Marshall University Forensic Science Program, Huntington, WV 25701*

Learning Overview: After attending this presentation, attendees will understand the protocols that were developed to aid in the handling of mobile devices that have been submerged in either oil-based, flammable, or clandestine chemical liquids.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing techniques to safely handle and acquire data from mobile devices that have been damaged with either oil-based, flammable, or clandestine chemical liquids.

Society has become inundated with a large variety of connected mobile devices used in the course of everyday life, and these devices become useful during forensic investigations. Mobile devices found in their original state or submerged in water-based liquids are examined by the guidelines established by the individual labs or their accrediting body. However, mobile devices that have been submerged in non-water-based liquids tend to be neglected in some laboratories due to not having the proper protocols and procedures in place to inform their examiners on safe and proper handling. These damage modalities, which tend to result in the mobile device being turned away, include, but are not limited to, oil-based liquids, flammable liquids, and clandestine chemical liquids. The overall goal of this project was to develop a protocol that can be used by the average digital forensic laboratory so potential items of high evidentiary value are not turned away due to a lack of knowledge in how to safely handle the device.

In conjunction with VTO Labs, Marshall University's Forensic Science Center endeavored to create protocols to demonstrate how mobile devices damaged with either oil-based, flammable, or clandestine chemical liquids should be handled to ensure the safety of the examiner and the data on the mobile device. The mobile devices were split into three equal groupings of devices and every device that could be imaged was imaged. Imaging was carried out via cable acquisition with Cellebrite®, UFED 4PC®, and SHA256 hash values were generated for each image. After imaging, the phones were submerged in their assigned liquid for a total of seven days before they were removed and neutralized, if necessary, before they were disassembled for the ultrasonic cleaning process. Ultrasonic cleaning was conducted using ElmaTec®, Clean A1®, and Clean S1® detergents with a modified manufacturing industry standard (IPC/JEDEC Standard 610) that VTO Labs had used in previous studies to great effect. Confirmation that the devices were cleaned of all remaining residue was conducted via Gas Chromatography/Mass Spectrometry (GC/MS) for the oil-based liquids and the flammable liquids using ASTM E2881-13e1 and ASTM E1618-14 methods, respectively. Confirmation that the devices submerged in clandestine chemical liquids was performed by using litmus paper to indicate a neutral pH value. If any cleaning methodology did not result in satisfactory results, additional cycles or pre-work steps were utilized to achieve the best result. To ensure the data remained intact after cleaning, the devices were reimaged using cable acquisition with a Cellebrite®, UFED 4PC®, or via chip-off methods. The SHA256 hash values generated after submersion and cleaning were compared with the SHA256 hash values generated prior to submersion.

The funding for this research was sponsored by the United States Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) via contract number HHSP233201700017C, which was awarded to VTO Labs.

Mobile Forensics, Damaged Devices, Device Cleaning