B6 Recovering Deleted Evidence From Mobile Devices

Eoghan Casey, MA, 3014 Abell Avenue, Baltimore, MD 21218*

After attending this presentation, attendees will gain an understanding of how to recover deleted evidence from mobile devices and will learn how this evidence has been used in actual cases. Practitioners will learn about the forensic challenges and advantages associated with mobile devices. Researchers will learn about areas that require further exploration to advance the field of mobile device forensics.

This presentation will impact the forensic science community by expressing how the growing number of mobile devices can contain digital evidence, including cell phones, smart phones, and satellite navigation systems. Although some deleted data may be recoverable from these devices, the process can be technically difficult and physically destructive. This presentation presents various approaches to extracting and interpreting deleted data from non-volatile memory on mobile devices and discusses the forensic implications of each approach.

Mobile devices present significant forensic opportunities and challenges. Their ever-increasing prevalence, functionality, and storage capacity make them valuable sources of evidence. Evidence on these devices can include incriminating communications, illegal materials, location-based information, passwords, and other personal data. However, the complexity and variety of mobile devices make it difficult to develop standardized forensic methods for recovering deleted data from non-volatile memory of these systems. Current tools and techniques available to forensic practitioners and researchers for acquiring and examining data from embedded systems are limited to specific model devices and, under most circumstances, not all of the data can be retrieved due to proprietary hardware and software.

To ensure that important evidence on mobile devices is not overlooked, it is important for practitioners in digital forensics to be aware of the potential for recovering deleted data from mobile devices and how this evidence can be useful in an investigation. Digital forensic researchers also need to be aware of the unsolved challenges relating to extraction and interpretation of deleted data from non-volatile memory on mobile devices. This presentation covers various approaches to obtaining and analyzing deleted data from mobile devices, including file system examination and chip extraction. The forensic implications of each approach are discussed, and case examples and research are presented to demonstrate and emphasize key points.

Mobile Device Forensics, Cell Phone Forensics, Digital Evidence

 ** Presenting Author*