B13 Digital Media Players — Recent Research and a Cautionary Tale

Jessica Reust Smith, MFS, Stroz Friedberg, LLC, 1150 Connecticut Avenue Northwest, Suite 200, Washington DC, 20036; Thomas Owley, MD, 1747 West Roosevelt Road, Chicago, IL 60608; Edward Zawadzki, DO, 144 West 12th Street, New York, NY 10021; Soyna Owley, MD, 1500 Waters Place, 10011, Bronx, NY 10461; and Stephen B. Billick, MD, 11 East 68th Street, Suite 1B, New York, NY 10065-4955*

After attending this presentation, attendees will gain knowledge of recent research and analysis performed on digital media players, with a specific emphasis on Apple iPod™ devices and the analysis of metadata for generating timelines and determining user activity.

This presentation will impact the forensic community by serving as a cautionary tale and reminder about the challenges involved when preserving, storing, and analyzing devices as dynamic as digital media players.

Digital media players are fast becoming as ubiquitous as cell phones, and are turning up in increasing numbers in forensic investigations of both civil and criminal matters. A jogger is raped and her digital media player is missing. A suspect is arrested with a digital media player in his possession. What can examination of this device do to help determine the guilt or innocence of the suspect? An employee is accused of industrial espionage. A digital media player is turned over for examination. Could this device have been used in the commission of this crime? What evidence can be extracted from the digital media player to help build a timeline of the commission of the alleged offense?

Digital media players vary greatly both between and within manufacturers. For example, since the introduction of the Apple iPod™, only seven years ago, there have been 15 different hardware versions released. Even within each version there are differences resulting from firmware updates, file system formats, and syncing methods. All of these possible combinations result in unique behaviors that can impact the conclusions that can be drawn from forensic analysis. What happens when the battery dies while it is stored in your evidence room? What are the forensic consequences of playing a song or simply the passage of time? Can you verify the MD5 hash of your forensic duplicate with the original evidence if you allow it to sync with your forensic workstation?

When performing forensic tool/methodology testing and evaluation, your ability to duplicate the hardware, firmware, file system, and syncing environment can significantly impact your results. For this reason, relying on the published results of other forensic researchers without performing sufficient verification may not be wise. When building a timeline of the user activities it is important to have, among other things, an in-depth knowledge of both the file system on which the activity took place and the applications that are involved in the activity. Metadata that can be used in timeline generation is stored, both on the device and within the software application data store used for syncing (most frequently iTunes™). What are the implications on your forensic examination for a two year old device that has been sync'd with each new version of syncing software as they were released? Can you rely on the metadata for each digital media file to be consistent?

Attendees of this presentation will learn forensic examination techniques for extracting valuable evidence from digital media players, drawn from both applied research and actual investigations. This presentation will also show a forensic examiner what they can do to avoid some of the forensic pitfalls caused by the fast changing digital media player environment.

iPod, Timeline Generation, Metadata Analysis

 ** Presenting Author*