C33 iPhone® Video Metadata: What Can It Teach Us About a Recordings History?

James Zjalic, MSc, Birmingham, England B62 0EZ, UNITED KINGDOM; Jeff M. Smith, MS, National Center for Media Forensics, CU Denver, Denver, CO 80204; Cole Whitecotton, MS, UC Denver, Englewood, CO 80110; Catalin Grigoras, PhD, Denver, CO 80202*

Learning Overview: After attending this presentation, attendees will understand how video recordings made with Apple® iPhone® devices change based on both the method used to download the files and whether they have been edited within an Apple® device. These changes can provide vital information to inform us as to the recording's history.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating why all iPhone® multimedia should be considered with caution and by providing a methodology as to how to determine the history of a recording. This will specifically aid those who perform video authentications and, in a broader sense, reveal why exhibits should not be taken at face value as authentic without a consideration as to the history of the exhibit.

The need for research into this area became evident during a forensic examination of an Apple® iPhone® video recording that was found to have iOS® metadata that didn't relate to the phone it was extracted from. This led to the present research into iOS® video, from which previous work into the iOS® Voice Memos App is built upon.[1] With this research framework, video is captured in all available manipulation and sharing scenarios in order to examine the various states that video data can take in these situations.

Video imagery captured using mobile phones can form a large area of work conducted by forensic media experts and suffers from two key issues in terms of reliability. The first is that the data can easily be transmitted via text message or email and saved to a new device, masking its origin. The second is that the mobile phones themselves have features that allow for the editing of the data. Combining these two factors can complicate examinations, as the possibility can exist that the data was edited on another device, sent via email to the seized device, and saved.

Understanding the provenance of multimedia is essential for the chain of the custody and, specifically, to authentication examinations. Without knowing where an image, audio, or video recording first originated, the possibility can exist that the evidence will later be deemed inadmissible and any further work conducted (such as enhancements) will become worthless. In the case of this presentation, the analogous links in the chain of custody are the transmissions of emails between phones and computers. Research has shown that there is the potential that some of these links may be missed, and edited multimedia can easily go undetected and accepted at face value, even after authentication analysis. Attendees will come to understand why all multimedia data obtained from iPhones® should be treated with caution with regard to its provenance and how to best determine the history of the version provided.

The research that informs this presentation is part of a larger research project that will also see the investigation of the changes that occur in audio, images, and video when edited and sent via differing transmission channels, such as email, text message, and iMessage®.

Reference(s):

1. J. Smith, D. Lacey, B. Koenig, and C. Grigoras. Triage Approach for the Forensic Analysis of Apple iOS® Audio Files Recorded Using the "Voice Memos" App. In: *Audio Engineering Society Conference: 2017 AES International Conference on Audio Forensics*, 2017.

Video Authentication, Video Analysis, iPhone® Analysis