C1 A Study of Video Conferencing Software From an Authentication Perspective

Cole Whitecotton, MSc, National Center for Media Forensics, University of Colorado Denver, Denver, CO 80204; Gretchel Lomboy, MSc, Seattle Police Department - Video Unit, Seattle, WA 98134; James Zjalic, MSc, Verden Forensics, Edgbaston, England B15 1TH, UNITED KINGDOM*

Learning Overview: After attending this presentation, attendees will better understand the capabilities, specifications, file structures, and metadata pertaining to video conferencing software, which will aid authentication examinations of video captures relating to such.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing detailed authentication information for commonly used conference-recording software. This is a growing, impactful, and current area of concern.

As highlighted by the COVID-19 pandemic, video conferencing software has become an essential tool for maintaining communication between groups of people, whether that relates to a workplace environment or friends and family. It is common that these programs allow for recording of the video and audio streams, sometimes in multiple formats. Naturally, the recordings taken using conference software are also susceptible to the same issues as other digital recordings, namely the potential for manipulations. When performing authentication examinations, it is critical that examiners have an understanding of the capabilities of the purported capture device/software, as well as other factors such as the file structures of original and edited recordings made with said devices.[1] For instance, if a recording in a standalone audio format is purported to be an original capture using Microsoft® Teams, knowing that this platform only records video, regardless of whether a video or voice call is made, would support the proposition that the recording is not an original. In the majority of cases, the examiner would have to create and/or maintain a database of multiple exemplar recordings in order to determine these factors, which can be time consuming.[2] In cases where this is not possible as the identity of the capture device is not known, multiple exemplar recordings from a variety of video conferencing software are required in an attempt to identify or eliminate the source, which can be even more time consuming than the first scenario. To address this issue, a large-scale study of the following was performed that included: (1) capabilities of the most common video conferencing software on the market today, including Zoom®, Microsoft® Teams, and Skype® running on a variety of operating systems and devices, including Windows®, OSX®, Android™, and iOS®; (2) the specifications of the captured recordings from each of these software; (3) the file structure of recordings captured from each of these software; and (4) the Exchangeable Image File Format (EXIF) data fields and information captured from each of these devices.[3,4]

Reference(s):

1. Scientific Working Group on Digital Evidence (SWGDE), 2018 *Best Practices for Digital Forensic Video Analysis*, Version 1.0.
2. Grigoras, C. et al. 2012. *Analytical Framework for Digital Audio Authentication.* Audio Engineering Society (AES) 46th International Conference, Denver, CO. June 2012.
3. Wales, G. 2019. *Proposed Framework for Digital Video Authentication*. Thesis from the University of Colorado, Denver, USA.
4. Gloe, T. 2014. Forensic Analysis of Video File Formats. *Digital Investigation*, 11, pp. 568-576.

Video Authentication, Metadata, Video Conferencing

*Presenting Author