C7 Google® Chromebook™: Evaluation of Forensic Methods for Data Extraction

Marcus Rogers, PhD, Purdue University, 401 N Grant Street, West Lafayette, IN 47907; and Yoshitaka Takase, MS*, National Police Agency of Japan /Purdue University, 401 N Grant Street, West Lafayette, IN 47907*

After attending this presentation, attendees will be more familiar with the various forensic methods for extracting data for Google® Chromebooks™. The pros and cons of each method will be discussed.

This presentation will impact the forensic science community by providing information on data storage locations of Google® Chromebooks™ and how evidence can be located and preserved.

The number of Chromebook™ unit shipments has increased in recent years and this increase is expected to continue; correspondingly, more devices could potentially become objects of forensic examinations in various cases. Computers using Google® Chrome™ OS are highly dependent on being connected to the internet. Therefore, they usually contain a relatively small on-board storage capacity; the users are required to use the Google® Drive cloud storage. These systems also use primarily web-based applications.

The current research focuses on understanding the data extraction methods for Chromebooks™ in a laboratory or on site. Three empirical studies were conducted (using a typical case scenario) that focused on settings information and files related to the Chromebook™ device. The first study's objective was to determine the different settings information each user could show on the screen; the users were a Guest user and a Google® account user who was registered as an owner. It was determined that the latter user could show more information. The second study's objective was to determine methods for extracting files from the limited internal storage. The methods tested included manual extraction, designated file extraction, logical extraction, and physical extraction. It was found that manual extraction and designated file extraction were the best methods. Last, the research looked at the preservation of metadata and file integrity as a result of the file extractions from: (1) local drive; (2) cloud drive; and, (3) attached storage media. The results indicated that the "Files application" was a practical method for copying the files to an external drive attached to the Chromebook™, as the modified dates were not altered; however, when using Windows® Explorer or forensic software, the time stamp was interpreted differently. The time difference was the same as the time-gap from Universal Time Coordinated (UTC) (1-hour-gap between standard time and daylight savings time). The research concluded that with Google® Chromebooks™, manual extraction (e.g., taking screenshots, pictures, or notes) maintains the metadata the best and should be considered as part of any standard operation procedure for conducting forensic examinations and analyses of these devices.

Chromebook™, Digital Forensics, Electronic Evidence

*Presenting Author