Best Practices for Chromebook Acquisition and Analysis

WHAT IS AN AAFS STANDARD FACTSHEET?

The AAFS produces clear, concise, and easy-to-understand factsheets to summarize the contents of technical and professional forensic science standards on the OSAC Registry. They are not intended to provide an interpretation for any portion of a published standard.

WHAT IS THE PURPOSE OF THIS STANDARD?

This standard provides guidance and recommendations for forensic science service providers (FSSPs), investigators, and organizations involved in the acquisition and analysis of Chromebook™ devices.

It addresses several recommended acquisition techniques while detailing the limitations that FSSPs must consider when employing these techniques. Analysis of derived data parsing tools and viewers used to analyze databases are also covered.

This standard is not intended to be employed as a training manual and does not provide specific operating procedures. It does not cover associated storage from the cloud and search warrant returns.

WHY IS THIS STANDARD IMPORTANT? WHAT ARE ITS BENEFITS?

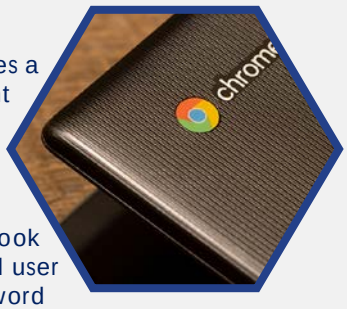
Since a successful forensic image of a Chromebook does not follow other laptop-style forensic acquisition practices and the number of validated acquisition tools is rather limited, this standard is important to ensure that FSSPs are aware of the specific challenges associated with Chromebook acquisition and analysis, as well as available best practice options.

This standard includes a recommended sequence of methods using processes that are designed to maintain the integrity of digital evidence. In addition, the standard details the potential artifacts that can be derived from the analysis of the Chromebook acquisition.

HOW IS THIS STANDARD USED, AND WHAT ARE THE KEY ELEMENTS?

This standard provides FSSPs with recommended methods and techniques to acquire and analyze data from Chromebook devices. FSSPs can also leverage the documented challenges associated with Chromebook acquisition and analysis to manage expectations regarding the data that can be acquired from Chromebooks.

The key elements of the standard related to acquisition are detailed methods and caveats for the physical acquisition of the device in developer mode as well as the logical backup acquisition using the *Daniel Dickerman Method (DDM),* which requires a username and password. The notes and caveats are lessons learned that will prevent FSSPs from inadvertently compromising or erasing data from Chromebook devices.



The key elements related to analysis are the recommended tools for parsing Chromebook data, multiple recommended viewers that can be used to analyze LevelDB database files, and a list of artifacts that can be derived from the Chromebook device. Given the large amount of user data stored in the cloud and that encrypted user data is stored in internal memory, without an associated Google account and password for the device, most recoverable user data will be encrypted.

American Academy of Forensic Sciences
aafs.org

This factsheet is made possible through the following financial assistance award 70NANB21H097 awarded to AAFS from U.S. Department of Commerce, National Institute of Standards and Technology