Best Practices for Acquiring Online Content

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?

The purpose of this standard is to provide best practices and considerations for acquiring and preserving digital evidence from online content. This standard is focused on public-facing data including, but not limited to, websites, streaming services, and communication platforms but does not include searches conducted pursuant to a warrant or acquisition of data from cloud service providers. Refer to SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers.

Focused on acquisition, this standard does not address the identification or analysis of data acquired.

WHY IS THIS STANDARD IMPORTANT? WHAT ARE ITS BENEFITS?

Based upon the three basic principles that govern digital evidence - relevance, reliability, and sufficiency - this standard will limit material acquired to that which is relevant to the investigation, which contains information of value to the investigation or the particular incident, and for which there is a good reason for the information being acquired.

All processes mentioned in this standard should be auditable and repeatable so that the results of applying such processes should be reproducible.

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

This standard is directed at those needing to preserve internet content for future use in the context of legal, administrative, or similar proceedings, including forensic examiners, investigators, attorneys, etc. Those conducting such collections should have a working knowledge of basic information technology and foundational computer forensics principles.

This standard is tool agnostic; references to specific tools are for demonstrative purposes only. It is not intended as a step-by-step guide or source of legal advice.

Acquiring results can be limited by protected areas of a site, hidden URLs, dynamic content generated based on browser identity, or software limitations due to complex site design. For restricted access sites, this standard suggests considering alternative investigative tactics in accordance with agency policies.

The examiner selects the appropriate course of action based on the goal of the collection, available resources, and their knowledge and understanding of the circumstances. When doing so, the standard raises awareness of understanding appropriate legal authority, the risks of live access and collection tools on the integrity of the data, and content volatility.

American Academy of Forensic Sciences
aafs.org

This factsheet is made possible through the following financial assistance award 70NANB24H078 awarded to AAFS from U.S. Department of Commerce, National Institute of Standards and Technology