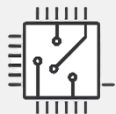## Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics

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?

Tools and procedures employed in digital and multimedia (D/MM) forensic examinations should be tested to establish confidence that the tool or procedure performs correctly, thereby reducing the risk of error.

This standard includes minimum requirements for testing (often referred to as validation or verification testing) for broad categories of commonly used forensic D/MM tools and procedures so forensic science service providers (FSSPs) can evaluate whether each performs as expected and understand the tool's limitations. Recommendations for documentation of testing results are also included to support the use of the tool.

WHY IS THIS STANDARD IMPORTANT? WHAT ARE ITS BENEFITS?

Adherence to this standard by FSSPs enhances the reliability, consistency, and quality of D/MM forensic analysis. It promotes confidence in the D/MM field, ultimately enhancing the overall effectiveness of D/MM forensic examinations.

Implementation of this standard will allow for compatibility among FSSPs. When tools are tested to the same standards, FSSPs can exchange, compare and verify the results of other tool testing. This facilitates effective collaboration, increased confidence and trust in tool findings, and, as a result, can strengthen the acceptance of D/MM evidence in court.

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

FSSPs can leverage this standard to understand the minimum recommended types of testing, the frequency of such testing, and who should perform the testing for different functional categories of D/MM tools.

The key elements of the standard are the specific minimum requirements, as well as recommendations, for distinct categories of tools to include, but not limited to:
- Critical forensic process tools, such as write blockers and radio isolation tools for data preservation, imaging tools for data acquisition, hashing tools to verify that data is unchanged, and wiping tools to sanitize and prepare storage media.
- Forensic analysis tools used to search, recover, and aggregate data to facilitate follow-on analysis.
- Multimedia tools used to display, capture, and/or enhance data from imagery, video, and audio sources, in both analog and digital formats.
- Administrative and auxiliary tools to manage and document the investigation and export relevant data.

Given the wide variability of software and hardware versions in which all of these tools must operate, the standard recognizes that it is not possible to ensure that a given tool will perform as expected in all situations. Therefore, organizations must balance the confidence gained by the level and frequency of testing with the resources used to perform that testing.