SWGDE Best Practices Apple MacOS Forensic Acquisition

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 forensic imaging methodologies for Apple systems differ significantly from the traditional methods used on Windows-based or other systems. This is primarily due to the cohesive security-minded environment Apple has created with its products and limitations on publicly available technical data.

The purpose of this standard is to describe the best practices for the forensic acquisition of digital evidence from Apple macOS-based ("Mac") computers, specifically MacBook Pro, MacBook Air, Mac Mini, Mac Studio, iMac, and Mac Pro, that are equipped with the Intel based processors and the Apple Silicon processors (i.e., "M1", "M2").

Early Macs (i.e., pre-2006) with the PowerPC processors are beyond the scope of this standard.

WHY IS THIS STANDARD IMPORTANT? WHAT ARE ITS BENEFITS?

This standard outlines procedures that will maintain the integrity of digital evidence. It discusses the risks that examiners should understand when handling Intel and Apple Silicon based Macs.

The importance of understanding appropriate legal authority, communication between the examiner and the investigative team, and the need to consider the collection and preservation of other types of forensic evidence is covered.

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

This standard is for examiners qualified to acquire and handle digital evidence.

This standard may not be applicable to all circumstances (e.g., incident response or complex live acquisition scenarios), and it does not contain information regarding specific commercial forensic products; therefore, the standard acknowledges that, when warranted, an examiner may need to deviate from these best practices. When that occurs, the specifics of the situation and actions taken should be thoroughly documented to support the results obtained.

The main sections in this standard include:

- Information Specific to Forensic Collection of Mac/Apple Computers
- Training and Experience Considerations
- Image Format and Metadata Considerations
- Triage
- Pre-interaction Intelligence
- Start-up Commands
- Acquisition Process
- Logical Acquisition Considerations
- Documentation and Safe Handling of Digital Evidence

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