The International Association of Computer Investigative Specialists

_____

Advanced Mobile Device Forensics

Core Competencies

IACIS Advanced Mobile Device Forensics (AMDF) Program

The AMDF core competencies described in this document are a binding set of competencies that guide the training program to ensure that the skills and knowledge points are delivered within the training program.

IACIS Advanced Mobile Device Forensics (AMDF) Core Competencies
There are seven competency areas addressed in the AMDF Program:

   i.   **Advanced understanding of Android and iOS file systems**
  ii.   **Proficient in using commercial and open-source forensic tools**
 iii.   **In-depth parsing of third-party applications**
 iv.   **Expertise in advanced database and various types of data store analysis**
  v.   **Deep understanding of data stores**
 vi.   **Utilization of Python scripts for forensic examination**
vii.   **Proficiency in investigating Android malware**

   i.   **Advanced understanding of Android and iOS file systems**

      a. Comprehension of mobile operating systems, enabling a more thorough and efficient data retrieval and analysis.

  ii.   **Proficient in using commercial and open-source forensic tools**

      a. Ability to effectively use and switch between different commercial and open-source tools to enhance the investigation process.

 iii.   **In-depth parsing of third-party applications**

      a. Ability to dissect third-party applications on mobile devices to extract and analyze valuable data.

 iv.   **Expertise in advanced database and various types of data store analysis**

      a. Ability to analyze and extract valuable information from different database systems.
      b. Ability to identify and analyze different data structures found inside of SQLite databases on mobile devices.

v. Deep understanding of data stores

    a. Thorough comprehension of how and where data is stored, enabling more comprehensive data recovery and analysis.

    b. Data structures explored include but are not limited to: JSON, LevelDB, Plists/BPlists, Protobuf, Realm, SEGB, ABX & XML.

vi. Utilization of Python scripts for forensic examination

    a. Understanding of Python scripts to automate the extraction of valuable artifacts from smartphones.

    b. Ability to identify valuable strings within the script that are targeted to certain artifacts.

vii. Proficiency in investigating Android malware

    a. Familiarization in detecting, analyzing, and mitigating malware threats on Android devices.

Submitted by:	Felicia DiPrinzio
Membership Review Period:	NA
Draft of Policy Reviewed by Board:	August 17, 2024
Date of Policy Ratification by Board:	October 7, 2024
Effective Date *(30 days after ratification)*:	October 7, 2024
Final Version Identifier:	1.0