The International Association of Computer Investigative Specialists

---

Certified Mobile Device Examiner (ICMDE) Core Competencies

IACIS Certified Mobile Device Examiner (ICMDE) Program

The ICMDE core competencies described in this document are a binding set of competencies that guide both the training and certification programs to ensure that the skills and knowledge points delivered within the training program are also the same set of standards evaluated within the certification program.

IACIS Certified Mobile Device Examiner (ICMDE) Core Competencies

There are six competency areas addressed in the ICMDE Program:

i. **Evidence Handling and Identification**
ii. **Device Technology**
iii. **Examination Methodologies**
iv. **Database Architecture**
v. **Examination of iOS Devices**
vi. **Examination of Android Devices**

i. Evidence Handling and Identification

a. Demonstration of knowledge related to the importance of network isolation; its purpose, and options/methodologies available to ensure isolation.
b. Ability to accurately identify mobile devices and attached media including SIM and microSD cards.
c. Understand terminology common in mobile device forensics.
d. Demonstrate basic knowledge of mobile device security and proper handling during evidence collection.
e. Knowledge of best practice in handling and preserving of mobile devices.

ii. Mobile Device Technology

a. Demonstrate knowledge of the different types of mobile communication networks, such as CDMA, GSM, and iDEN.
b. Knowledge of the fundamental differences between traditional computer forensics and mobile device forensics.
c. Ability to identify the differences of a feature phone as compared to a smartphone.
d. Understanding of SIM card technology.

iii. Examination Methodologies

a. Understand the various device acquisition methodologies to include the advantages, disadvantages and challenges related to each method.
b. Knowledge of best practices for examination of mobile devices.
c. Knowledge of the differences between logical, file system, and physical extractions.
d. Knowledge of the concepts related to data extraction methodologies.

iv. Database Architecture

a. Knowledge of the methodologies for viewing and interpreting data stored in an SQLite database.
b. Understanding of SQLite databases, to include overall structure of the database, including the WAL, SHM, and blob files.
c. Be able to explain how records are stored and how deleted records are handled.
d. Ability to properly interpret date/time functions.

v. Examination of iOS Devices

a. Ability to identify current iOS partition schemes.
b. Ability to distinguish between different versions of iOS and the different models of devices running iOS.
c. Understand the challenges related to acquiring data from iOS devices, to include the acquisition of data from devices that are password protected.
d. Knowledge of the various types of iOS artifacts available and the relevance of these
e. Ability to interpret and examine third party applications.
f. Ability to examine iOS devices including related backup data.

vi. Examination of Android Devices

a. Ability to identify current Android partition scheme.
b. Ability to distinguish between different versions of Android operating systems.

c. Understand the major files and how they relate to an examination.
d. Knowledge of the various types of Android artifacts available and the relevance of these artifacts.
e. Understanding of the Android Developer Bridge (ADB) to include common commands.
f. Ability to interpret and examine third-party applications.
g. Ability to examine Android related data including backup data.

Submitted by:	Felicia DiPrinzio
Membership Review Period:	N/A
Draft of Policy Reviewed by Board:	February 13, 2024
Date of Policy Ratification by Board:	April 3, 2024
Effective Date:	April 4, 2024
Final Version Identifier:	1.1