**The International Association of Computer Investigative Specialists**

**Mobile Device Forensics (MDF)**
**Core Competencies**

## Mobile Device Forensics (MDF) Program

IACIS prides itself on being the world's leading organization for computer forensics practitioners. In addition to providing the highest quality computer forensics training, IACIS strives to foster excellence in the field through its formal certification programs.

Computer forensics is the acquisition, authentication, reconstruction, examination, and analysis of data stored on electronic media. The IACIS Basic Computer Forensic Examiner (BCFE) Program and its accompanying certification program, the Certified Computer Forensic Examiner (CFCE), address each of these key tasks and measure one's ability to perform these key tasks in accordance with established standards.

Like the BCFE Program, the IACIS Mobile Device Forensics (MDF) Program and its accompanying certification Program, the Certified Mobile Device Examiner (CMDE) Program, expand on the foundational concepts of the computer forensic examination process by exploring forensically critical features of Mobile Devices.

The MDF 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. The IACIS Standards Committee monitors both programs to ensure each adheres to strict guidelines of the established certification competencies.

The IACIS Basic Computer Forensic Examiner (BCFE) course is a strongly recommended prerequisite for enrollment in the Mobile Device Examiner course. There are no required prerequisites.

**Mobile Device Forensics Core Competencies**

There are six competency areas addressed in the MDF Program:

I. **Evidence Handling and Identification**
II. **Mobile 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.
c. Understand terminology common in mobile device forensics.

**II. Mobile Device Technology**

a. Understand the manner in which a cellular device communicates over a network; CDMA vs TDMA/GSM.
b. Knowledge of the fundamental differences between traditional computer forensics and mobile device forensics.
c. Understand the basic concepts of flash technology.
d. Understand the distinction between a feature phone as compared to a smart phone.
e. 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 systems and physical extraction.
d. Knowledge of the concepts related to JTAG related methodologies.
e. Knowledge of the concepts related to Chip Off/ISP related methodologies.

**IV. Database Architecture**

a. Understanding of SQLite databases to include; overall structure of the database and the WAL and SHM files.
b. Be able to explain how records are stored and how deleted records are handled.
c. Be familiar with functions such as vacuuming, joins and arrays.
d. Knowledge of methodologies for viewing and interpreting data stored in a SQLite database.

**V. Examination of iOS devices**

a. Be able to distinguish between different versions of iOS and different models of devices running iOS.
b. Understand the challenges related to acquiring data from iOS devices, to include the acquisition of data from devices that are password protected.
c. Knowledge of the various types of iOS artifacts available and the relevance of these artifacts.
d. Ability to examine iOS related backup data.

**VI. Examination of Android Devices**

a. Be able to distinguish between different versions of Android operating systems.
b. Understand the major files and how they relate to an examination.
c. Knowledge of the various types of Android artifacts available and the relevance of these artifacts.
d. Understanding of the Android Developer Bridge (ADB) to include common commands.
e. Ability to examine Android related backup data.