The International Association of Computer Investigative Specialists

Collecting and Admitting Digital Evidence at Trial

Core Competencies

IACIS Collecting and Admitting Digital Evidence at Trial (CADET) Program

The CADET 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 Collecting and Admitting Digital Evidence at Trial (CADET) Core Competencies
There are six competency areas addressed in the CADET Program:

i. **Evaluating Digital Evidence**
ii. **Digital Forensic Fundamentals**
iii. **Constitutionally Sound Evidence Collection**
iv. **Digital Discovery Ethics**
v. **Presentation of Digital Evidence at Trial and Beyond**
vi. **Direct and Cross Examination of Digital Forensic Experts**

i. Evaluating Digital Evidence

a. Knowledge of the most common sources of digital evidence and what kinds of data they contain
b. Ability to identify lesser-known sources of potential evidence
c. Understanding of how digital evidence can be used in the investigation and trial of even non-computer-based offenses

ii. Digital Forensic Fundamentals

a. Familiarity with the basics of digital evidence extraction, including the imaging process and the various examination tools
b. Ability to navigate and understand digital forensic reports and how to work with digital forensic examiner to obtain relevant evidence and identify potential evidentiary hurdles

iii. Constitutionally Sound Evidence Collection

a. Knowledge of the general Fourth Amendment framework concerning the seizure and search of digital devices and data
b. Knowledge of the other methods for obtaining digital evidence, including court orders, administrative subpoenas, and subpoenas duces tecum

c. Ability to draft search warrant attachments and document requests to obtain relevant results while avoiding overbreadth challenges
d. Understanding the dangers of third-party notification and how to limit the risk of disclosure

iv. Digital Discovery Ethics

a. Knowledge of discovery obligations
b. Understanding of how to meet those obligations when dealing with digital evidence
c. Ability to navigate discovery involving personally identifying information, confidential or classified data, and contraband material
d. Ability to facilitate independent forensic examination by opposing expert

v. Presentation of Digital Evidence and Trial and Beyond

a. Knowledge of the rules of evidence related to digital evidence and ability to introduce digital evidence in compliance with those rules
b. Understanding of common defenses and challenges to digital evidence and how to overcome them
c. Ability to present digital forensic findings to grand and petit juries
d. Knowledge of the relevant sentencing guidelines and ability to use digital evidence to enhance or mitigate offense conduct

vi. Direct and Cross Examination of Digital Forensic Experts

a. Knowledge of digital forensic trainings, education, and certifications
b. Understanding the limits of digital forensics
c. Understanding of the requirements and process for certification as an expert witness under the rules of evidence and criminal procedure
d. Identifying how and when to use expert testimony
e. Ability to challenge opposing digital forensic examiner's expert qualifications, findings, and opinions

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