The International Association of Computer Investigative Specialists

Cyber Incident Forensic Response

Core Competencies

IACIS Cyber Incident Forensic Response (CIFR) Program

The CIFR 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 Cyber Incident Forensic Response (CIFR) Core Competencies
There are eight competency areas addressed in the CIFR Program:

i. **Network Fundamentals**
ii. **Log Analysis**
iii. **Remote Drive Imaging**
iv. **Network Assessment**
v. **Windows Host Analysis**
vi. **Linux Host Analysis**
vii. **RAM Capture and Analysis Concepts**
viii. **Malware Analysis Concepts**

i. Network Fundamentals

a. Explain Internet protocols and Internet addressing fundamentals.
b. Understand the Open Systems Interconnection (OSI) Model.
c. Comprehend various networking protocols and their forensic relevance.
d. Understand fundamental concepts and principles of Windows domains.
e. Ability to give investigative considerations when conducting an investigation involving a network.

ii. Log Analysis

a. Understand network and host sources for log evidence.
b. Ability to recognize log formats and content, and anticipate the relevant log evidence related to each log type and source.
c. Identify different tools to collect and analyze log files.
d. Demonstrate the ability to use various software tools to perform log analysis.

iii. Remote Drive Imaging

a. Understanding of remote imaging processes
b. Ability to obtain drive images across a network.

iv. Network Assessment

a. Ability to perform network-based analysis.
b. Understanding of remotely analyzing hosts using host-based agents.

v. Windows Host Analysis

a. Understand the types of Windows artifacts resulting from malware infections and intrusions.
b. Ability to perform registry, event log and file system analysis for malware and intrusion artifacts.

vi. Linux Host Analysis

a. Understand the common Linux folder structures and settings.
b. Understand the types of Linux artifacts resulting from malware infections and intrusions.
c. Ability to perform analysis of Linux images for malware and intrusion artifacts.

vii. RAM Capture and Analysis Concepts

a. Understanding the methods for live memory acquisition and analysis.
b. Ability to conduct RAM analysis to Identify what processes were running on a Windows machine during the acquisition of memory.
c. Ability to conduct RAM analysis to Identify what network information is available in RAM and how to correlate connections to a running process.
d. Ability to conduct RAM analysis to locate and extract operating system files available in RAM.
e. Understanding of how to extract data from an acquired memory capture.

viii. Malware Analysis Concepts

a. Understand different types of malware and how they function.
b. Knowledge of malware analysis methods.
c. Understanding of dynamic malware analysis, including ability to execute Windows malware under controlled circumstances to obtain information on malware actions and capabilities.

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:	1.1