# IACIS

**The International Association of Computer Investigative Specialists**

**IACIS Cyber Incident Forensic Response (CIFR) Core Competencies**

## IACIS Cyber Incident Forensic Response (CIFR) Program

The CIFR core competencies described in this document ensure that the skills and knowledge points are delivered within the training program.

## Cyber Incident Forensic Response Core Competencies

There are eight (8) 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 principals 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. Indentify 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. Gain knowledge of remote imaging processes
b. Practice obtaining drive images across a network.

**IV. Network Assessment**

a. Be able to perform network-based analysis.
b. Gain proficiency at remotely analysing hosts using host-based agents.

**V. Windows Host Analysis**

a. Understand the types of Windows artifacts resulting from malware infections and intrusions.
b. 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. Perform analysis of Linux images for malware and intrusion artifacts.

**VII. RAM Capture and Analysis Concepts**

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

**VIII. Malware Analysis Concepts**

a. Understand different types of malware and how they function.
b. Develop knowledge of malware analysis methods.
c. Gain experience with dynamic malware analysis, including execution of Windows malware under controlled circumstances to obtain information on malware actions and capabilities.