The International Association of Computer Investigative Specialists

RAM Capture and Analysis

Core Competencies

IACIS RAM Capture and Analysis (RCA) Program

The RCA 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 RAM Capture and Analysis (RCA) Core Competencies
There are four competency areas addressed in the RCA Program:

- **i. Lock Screen Concepts**
- **ii. Capturing RAM Concepts**
- **iii. Analyzing RAM Concepts**
- **iv. Encryption Concepts**

i. Lock Screen Concepts

a. Understand what occurs during bootup and the log in function of Windows Operating systems.
b. Knowledge of methods for bypassing the login screen on Windows 7, 8, 10 and 11 machines using open source hardware and software.
c. Ability to use open source hardware and software to dump RAM on a locked Windows 7, 10 and 11 machines.

ii. Capturing RAM Concepts

a. Understand methods for live memory acquisition and analysis.
b. Ability to conduct RAM captures on Windows, MAC and Linux machines using numerous commercial and open source tools.
c. Knowledge of performing RAM captures over a network.

iii. Analyzing RAM Concepts

a. Ability to conduct RAM analysis to identify what programs were running on a Windows machine during the acquisition of memory.
b. Ability to conduct RAM analysis to identify what local user files are saved during the acquisition of memory.
c. Ability to conduct RAM analysis to locate/extract passwords and encryption keys available in RAM.

iv. **Encryption Concepts**

a. Knowledge of different encryption programs how Windows saves the encryption keys.
b. Ability to manually pull TrueCrypt/VeraCrypt and BitLocker encryption keys out of RAM and open a forensic container using command line and forensic programs.
c. Knowledge of how to create targeted password lists to crack numerous password protected files (docx, pdf, xls, KeePass, SAM, etc) with open source tools.

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