The International Association of Computer Investigative Specialists

Forensic Linux Examiner

Core Competencies

IACIS Forensic Linux Examiner (FLEX) Program

The FLEX 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 Forensic Linux Examiner (FLEX) Core Competencies
There are three competency areas addressed in the FLEX Program:

i. **General Linux**
ii. **Linux Forensic Artifacts**
iii. **Tools for Linux Forensic Analysis**

i. General Linux

a. Understanding of Linux fundamentals, which include how Linux works, system startup, disk management, package management and how to compile tools from source code.
b. Ability to identify Linux file attributes, file types, hard and soft links and user and group management.
c. Knowledge of the bash shell, how to customize the user environment to make it easier to use (aliases, functions, colors, fonts, etc.) and basic shell scripting

ii. Linux Forensic Artifacts

a. Understanding of system level artifacts.
b. Knowledge of user level artifacts.

iii. Tools for Linux Forensic Analysis

a. Familiarity with RAM acquisitions, file metadata extractions and disk image acquisitions.
b. Proficiency in the Command Line Interface (CLI) – to include file searching, text searching, image acquisition, file hashing, and log file analysis via Linux CLI tools.
c. Understanding of timeline analysis, networking and encryption and password cracking.

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