



## 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.

|   |                               |
|---|-------------------------------|
| <b>Submitted by:</b>                                | <hr/> Felicia DiPrinzio <hr/> |
| <b>Membership Review Period:</b>                    | <hr/> NA <hr/>                |
| <b>Draft of Policy Reviewed by Board:</b>           | <hr/> August 17, 2024 <hr/>   |
| <b>Date of Policy Ratification by Board:</b>        | <hr/> October 7, 2024 <hr/>   |
| <b>Effective Date (30 days after ratification):</b> | <hr/> October 7, 2024 <hr/>   |
| <b>Final Version Identifier:</b>                    | <hr/> 1.0 <hr/>               |