### Computer Forensics Fundamentals Course Template

<table>
<thead>
<tr>
<th>Discipline: Computer Science</th>
<th>Sub-discipline:</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Course Title:</td>
<td>Min. Units 3</td>
</tr>
<tr>
<td>Computer Forensics Fundamentals</td>
<td></td>
</tr>
</tbody>
</table>

**General Course Description:**
This course is an introduction to the methods used to properly conduct a computer forensics investigation beginning with a discussion of ethics, while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. Topics covered include an overview of computer forensics as a profession; the computer investigation process; understanding operating systems boot processes and disk structures; data acquisition and analysis; technical writing; and a review of familiar computer forensics tools. (Proposed Number: ITIS 165)

| Number: comp 122 | Suffix: |

**Required Prerequisites or Co-Requisites**: Prerequisite: None

**Advisories/Recommended Preparation**

**Course Content:**
1. Computer Forensics as a profession
2. Computing investigation processes
3. Microsoft operating systems, boot processes and disk structures
4. Macintosh and Linux operating systems, boot processes and disk structures
5. The investigator’s office
6. Current computer forensics tools
7. Digital evidence controls
8. Crime/incident scene processing
9. Data acquisition
10. Computing forensics analysis
11. Email investigations
12. Graphic image recovery
13. High tech reports
14. Expert witness overview

**Course Objectives:** *At the conclusion of this course, the student should be able to:*
1. Define computer forensics.
2. Summarize how to prepare for a computer investigation.
3. Summarize the certification requirements for computer forensics labs.
4. Measure the different ways for proper data acquisition.
5. Classify the rules for proper digital evidence handling.
6. Analyze how data is stored and managed by an operating system.
7. Analyze various computer forensics tools.
8. Validate the evidence during the analysis process.
9. Identify and reconstruct graphics files.
10. Describe the importance of network forensics.
11. Analyze email investigations.
12. Generate a forensic report.
14. Maintain a high level of ethical behavior in their work.

**Methods of Evaluation:** May include any or all of
Exams
Quizzes
Programming Projects
Discussions
Class Presentations

Sample Textbooks, Manuals, or Other Support Materials


FDRG Lead Signature:   Date:
[For Office Use Only] Internal Tracking Number