NOTE: This course is not designed for transfer credit.

Catalog Course Description:

This course will be a guide to computer forensics and investigation. It presents methods 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.

Entry Level Standards:

College level reading and math skills; keyboarding skills of at least 20 wpm; familiarity with the HPC architecture and related internetworking issues; problem solving and analytical skills also important.

Prerequisites:

HPC 1010 (NETW 2530) or consent of instructor

Textbook(s) and Other Reference Materials Basic to the Course:


I. Week/Unit/Topic Basis:

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Computer Forensics as a Profession</td>
</tr>
<tr>
<td>2</td>
<td>Computing Investigation Processes</td>
</tr>
<tr>
<td>3</td>
<td>Operating Systems, Boot Processes and Disk Structures</td>
</tr>
<tr>
<td>4</td>
<td>The Investigator’s Office</td>
</tr>
<tr>
<td>5</td>
<td>Current Computer Forensics Tools</td>
</tr>
<tr>
<td>6</td>
<td>Digital Evidence Controls</td>
</tr>
</tbody>
</table>
II. Course Objectives*

A. Develop a working understanding of the terminology and hardware devices associated with HPC computer forensics. I, II, III, II, V

B. Demonstrate basic fundamentals of HPC security investigation concepts. II

C. Demonstrate applied principles of managing security measures for investigating security problems. I, III

D. Exhibit a knowledge of current forensics tools as related to the HPC environment. I

E. Exhibit a knowledge of HPC operating systems and boot structure. IV, V

F. Develop an understanding of the methods to conduct computer investigations. II, IV

*Roman numerals after course objectives reference goals of the HPC program.

III. Instructional Processes*

Students will:

1. Use computer forensics security configuration utilities to perform practical tasks for investigating High Performance Computing operations. *Active Learning Strategy, Problem Solving and Decision Making Outcome, Technological Literacy Outcome, Information Literacy Outcome, Transitional Strategy*

2. Solve problems in computer forensics investigations within the HPC environment. *Information Literacy Outcome, Problem Solving and Decision Making Outcome*

3. Use professionally accepted investigative methods of using digital evidence control components. *Personal Development Outcome, Technological Literacy Outcome, Transitional Strategy*

4. Demonstrate knowledge concerning investigating computer crime incidents. *Information Literacy Outcome, Communication Outcome, Technological Literacy Outcome*
5. Use tools for infosecurity professionals and cyberforensics on the communications grid. 
*Information Literacy Outcome, Communication Outcome, Technological Literacy Outcome*

6. Practice elements of the work ethic such as punctuality, professionalism, dependability, cooperation, and contribution. *Personal Development Outcome*

*Strategies and outcomes listed after instructional processes reference Pellissippi State’s goals for strengthening general education knowledge and skills, connecting coursework to experiences beyond the classroom, and encouraging students to take active and responsible roles in the educational process.

IV. Expectations for Student Performance*:

Upon successful completion of this course, the student should be able to:

1. Use terminology associated with infosecurity as related to HPC architecture. A,B,D,E
2. Use cyber forensics security methodology to solve computer crimes. A,B,E, F
3. Generate audit trails and identify electronic tampering and misuse of lab systems. A,B,D,E,
4. Identify and resolve inappropriate use of HPC clusters. D
5. Gain proficiency in the examination and preservation of infosecurity evidence. C, D, F
6. Load and run software products as resources for identifying inappropriate cluster use. B,C,D,E
7. Transfer forensic audit procedures to protect corporate or educational assets. B,C, E, F
8. Produce documentation of successful infosecurity investigations. B, E

*Letters after performance expectations reference the course objectives listed above.

V. Evaluation:

A. Testing Procedures:

   Fourteen chapter exams each worth 100 points will be given. Pretests and post quizzes may be given. A group project will be required. Teamwork will count as 100 points.

B. Laboratory Expectations:

   Hands-on learning activities done individually and in teams will also serve as the basis for course evaluation.

C. Field Work:

   N/A

D. Other Evaluation Methods:

   Other assessment activities worth 100 points each will consist of special projects, research papers, team activities, essays, short answer documents, or other work assigned.

E. Grading Scale:

   90 - 100 % A
VI. Policies:

A. Attendance Policy:

Pellissippi State Technical Community College expects students to attend all scheduled required instructional activities. As a minimum, students in all courses MUST BE PRESENT for at least 75 percent of their scheduled class and laboratory meetings in order to receive credit for the course (Pellissippi State Catalog).