

**CENTER FOR APPLIED INFORMATION TECHNOLOGY  
TOWSON UNIVERSITY**

**AIT 650:** Computer & Networks Forensics

**Credit Hours:** 3

**Prerequisite:** AIT 600, AIT 610, AIT 614 and Familiarity with Linux

**Course Description:** Traditional computer forensic analysis and network forensics are rapidly converging disciplines. And depending on one's objectives, incident response *can* be an active, real-time forensic analysis. At the very least, the process of incident response will have a significant impact on any later forensic analysis, so knowledge of all of these disciplines is important to the practitioner of any of the disciplines. This course is a core component of an Information Assurance curriculum.

**Learning Objectives:**

1. Provide a comprehensive overview of computer and network forensics in an Internet context.
2. Provide an introduction to computer and network forensics through a series of lectures/discussions and hands-on laboratory exercises.
3. Understand the fundamental operation of a set of forensic acquisition and analysis tools

**Suggested Textbook:**

1. Mandia, P., Pepe, *Incident Response & Computer Forensics*, 2<sup>nd</sup> edition, McGraw-Hill/Osbourne

**Other References/Journals:**

1. Conklin, W., et al., *Principle of Computer Security+ Beyond*, McGraw-Hill
2. Howard and LeBlanc, *Writing Secure Code*, 2<sup>nd</sup> edition, Microsoft Press, 2003
3. Phillips, A., Nelson, B., Enfinger, F., Steuart, C., *Guide to Computer Forensics and Investigations*, Thomson Course Technology