Forensic Computing Investigations and Electronic Evidence

The objectives of this module are to:

- Show the methodology of investigating cyber-crimes and the electronic evidence that they generate
- Describe ways of finding, recovering and analyzing electronic evidence from individual computers and from networks
- Explore legislation related to cyber-crime, including some substantive and procedural law provisions from US, Europe, UK and Greece
- Recommend procedural approaches to evidence gathering, to presenting evidence in court, and to making preparations for potential cyber-crime incidents.

Outline:

- Cyber Crimes
- Computer Vulnerabilities
- Deleted Data and Evidence Recovery
- The legal view of Cyber Crime
- Investigative Process
- Beyond the PC: Evidence Recovery from Networks & the Internet
- Beyond Keywords: Finding and Analyzing Electronic Evidence
- Beyond Cyber Crime legislation: Legal issues in Electronic Evidence Gathering
- Before and After an Investigation: Forensic Readiness and Experts in the Courtroom
- Future Challenges