

360-804 Computer Forensics

Credit Points:	12.500
Level:	Graduate/Postgraduate
Dates & Locations:	2008, This subject commences in the following study period/s: Semester 1, - Taught on campus. Semester 2, - Taught on campus.
Time Commitment:	Total Time Commitment: Not available
Prerequisites:	None
Corequisites:	None
Recommended Background Knowledge:	None
Non Allowed Subjects:	None
Core Participation Requirements:	<p><p>For the purposes of considering request for Reasonable Adjustments under the Disability Standards for Education (Cwth 2005), and Student Support and Engagement Policy, academic requirements for this subject are articulated in the Subject Overview, Learning Outcomes, Assessment and Generic Skills sections of this entry.</p> <p>It is University policy to take all reasonable steps to minimise the impact of disability upon academic study, and reasonable adjustments will be made to enhance a student's participation in the University's programs. Students who feel their disability may impact on meeting the requirements of this subject are encouraged to discuss this matter with a Faculty Student Adviser and Student Equity and Disability Support: http://services.unimelb.edu.au/disability</p></p>
Subject Overview:	<p>This subject will enable an understanding of the practical and legal implications of the search, seizure and presentation of computer based evidence and computer forensic techniques that are employed at an electronic crime scene. It will include topics such as internet evidence and how to interpret mail and Usenet information. It will also provide valuable insight in to the management of an electronic crime scene.</p> <p>Topics to be covered include:-</p> <ul style="list-style-type: none"> # Digital Evidence; # Identification and analysis of software and hardware equipment affected; # Identification and recovery process of affected files /systems; # Identification of key components of affected computers including the re-creation of target computers, peripherals and files; # Tracking tools and techniques for email; # Network analysis and technology including abuses of networks and network evidence; # Gathering & monitoring network traffic and network based intrusion detection systems and understanding event logs.
Prescribed Texts:	None
Breadth Options:	This subject is not available as a breadth subject.
Fees Information:	Subject EFTSL, Level, Discipline & Census Date, http://enrolment.unimelb.edu.au/fees
Related Course(s):	Graduate Certificate in Digital Forensics