ISYS90005 e-Forensic Investigation

Credit Points:	12.50
Level:	9 (Graduate/Postgraduate)
Dates & Locations:	2010, Hawthorn This subject commences in the following study period/s: Semester 1, Hawthorn - Taught on campus. Semester 2, Hawthorn - Taught on campus. Intensive Mode
Time Commitment:	Contact Hours: 24 hours of face-to-face contact over an eight-week semester plus at least eight hours of pre-seminar reading Total Time Commitment: It is anticipated that students will need to allocate around 80 hours to undertake the assessable components of the subject to be completed in the three months encompassing the eight-week semester.
Prerequisites:	nil
Corequisites:	nil
Recommended Background Knowledge:	nil
Non Allowed Subjects:	nil
Core Participation Requirements:	For the purposes of considering requests for Reasonable Adjustments under the Disability Standards for Education (Cwth 2005), and Students Experiencing Academic Disadvantage Policy, academic requirements for this subject are articulated in the Subject Description, Subject Objectives, Generic Skills and Assessment Requirements of this entry. The University is dedicated to provide support to those with special requirements. Further details on the disability support scheme can be found at the Disability Liaison Unit website: http://www.services.unimelb.edu.au/disability/
Contact:	Melbourne Consulting and Custom Programs Level 3, 442 Auburn Rd Hawthorn VIC 3122 Phone: 9810 3148 Email: **mccp.enquiries@mccp.unimelb.edu.au (mailto:mccp.enquiries@mccp.unimelb.edu.au)**
Subject Overview:	The topics in this unit include: • 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; • Internet evidence e.g. how to interpret mail and Usenet information; • 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; • Management of an electronic crime scene, and • Understanding event logs.
Objectives:	**This course is no longer taking new enrolments. The last intake into this program was Semester 2, 2009.** Students who successfully complete this subject will have demonstrated 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.
Assessment:	Two written assignments and a practical exam totalling 6000 words.

Prescribed Texts:	nil
Recommended Texts:	Please refer to MCCP website.
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
Generic Skills:	n/a
Links to further information:	http://www.mccp.unimelb.edu.au/courses/award-courses/masters/e-forensics-enterprise-security
Related Course(s):	Master of e-Forensics and Enterprise Security