George Mason University
Graduate Course Approval/Inventory Form

Please complete this form and attach a copy of the syllabus for new courses. Forward it as an email attachment to the Secretary of the Graduate Council. A printed copy of the form with signatures should be brought to the Graduate Council Meeting. Complete the Coordinator Form on page 2, if changes in this course will affect other units.

Please indicate: ___X__ NEW ____ MODIFY ______ DELETE

Local Unit: ECE/TCOM

Graduate Council Approval Date:

Course Abbreviation: TCOM

Course Number: 661

Full Course Title: Digital Media Forensics

Abbreviated Course Title (24 characters max.): Digital Media Forensics

Credit hours: 3.0

Program of Record: MS in Telecommunications

Repeatable for Credit? ___D=Yes, not within same term Up to hours

___T=Yes, within the same term Up to hours

__N__ N=Cannot be repeated for credit

Activity Code (please indicate): ___X_ Lecture (LEC) ___ Lab (LAB) ___ Recitation (RCT)

___ Studio (STU) ___ Internship (INT) ___ Independent Study (IND)

__ Seminar (SEM)

Catalog Credit Format 3.0: 3.0: 0

Course Level: GF(500-600) __X__ GA(700+)

Maximum Enrollment: 35

For NEW courses, first term to be offered: Spring 2005

Prerequisites or co-requisites: prerequisite courses TCOM 548 & TCOM 556, or TCOM 562; a working knowledge of computer operating systems (e.g. CS 471 or equivalent), or permission from instructor.

Catalog Description (35 words or less) Please use catalog format and attach a copy of the syllabus for new courses:

This course deals with the collection, preservation, and analysis of digital media such that this evidence can be successfully presented in a court of law (both civil and criminal). The relevant federal laws will be examined as well as private sector applications. The seizure, preservation, and analysis of digital media will be examined in this course.

For MODIFIED or DELETED courses as appropriate:

Last term offered: Previous Course Abbreviation: Previous number:

Description of modification:

APPROVAL SIGNATURES:

Submitted by: ___Jeremy Allnutt__________________ email: _jallnutt@gmu.edu__

Department/Program: ___ECE/MS in Telecommunications ___ Date: _Oct. 18th, 2004___

College Committee: ______________________________________ Date: __Oct. 21st, 2004___

Graduate Council Representative: __________________________________ Date: __________________
Approval from other units: Not Applicable

Please list those units outside of your own who may be affected by this new, modified, or deleted course. Each of these units must approve this change prior to its being submitted to the Graduate Council for approval.

<table>
<thead>
<tr>
<th>Unit:</th>
<th>Head of Unit’s Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Graduate Council approval: ___________________________ Date: __________

Graduate Council representative: _______________________ Date: __________

Provost Office representative: _________________________ Date: __________
SCHOOL PROPOSAL TO THE GRADUATE COUNCIL
BY
SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING

1. CATALOG DESCRIPTION
   (a) TCOM 661 Digital Media Forensics (3:3:0)
   (b) Prerequisites: TCOM 548 & TCOM 556 or TCOM 562; a working knowledge of computer operating systems (e.g. CS 471 or equivalent) or permission from instructor
   (c) Catalog Description:
       This course deals with the collection, preservation, and analysis of digital media such that this evidence can be successfully presented in a court of law (both civil and criminal). The relevant federal laws will be examined as well as private sector applications. The seizure, preservation, and analysis of digital media will be examined in this course.

2. JUSTIFICATION
   (a) Course Objectives:
       At the conclusion of this course, the student will have learned the laws, concepts, tools, and methodologies necessary to seize, preserve, analyze, and present digital media evidence in a court of law. The student will have an understanding of: the processes required for conducting digital media analysis; federal laws governing the seizure of digital evidence, software and hardware, file system structures, and steganography (digital watermarking).
   (b) Course Necessity:
       Computers permeate our lives and our lives are recorded on computers, however, most computer storage media are volatile and, as such, they can be changed and altered intentionally as well as unintentionally. Digital media forensics is a discipline whose goal is to preserve information (evidence) on digital media in such a way that this evidence can be successfully admitted into a court of law. In both the public and private sectors, digital media forensics is being applied to a broad range of issues to include: due diligence, intellectual property rights issues, and high technology as well as more mundane criminal matters.
   (c) Relationship to Existing Courses:
       This is a new course in the TCOM program that has been designed to provide a body of knowledge that is directly applicable to forensic activities in the telecommunications industry. It builds on other courses within the TCOM program (TCOM 548/556, and TCOM 562) with the goal of applying engineering skills to the field of computer forensics. This course will work hand in hand with two proposed new courses, TCOM 661, Network Forensics (that will be offered in alternating semesters) and TCOM 662, Network Security Issues, plus related course in INFS.

3. APPROVAL HISTORY
   ECE Department Date: October 18th, 2004
   IT&E Graduate Committee Date: October 21st, 2004
   IT&E Dean Date:

4. SCHEDULING
   Every spring semester, starting spring 2005 and every spring thereafter.
5. COURSE OUTLINE

(a) Syllabus

Week 1
Course overview: Introduction to the course and the concept of seizure and preservation of stored data

Week 2
Presentation of Federal Laws: Federal laws pertaining to the seizure of digital evidence, particularly in stored media

Week 3
Documentation requirements: Procedures for ensuring accurate documentation of the storage medium under investigation

Week 4
Operating System environments: WINTEL file system structures

Week 5
Operating System environments: UNIX/LINUX file system structure

Week 6
Storage media structure analysis (fixed)

Week 7
Storage media structure analysis (removable devices)

Week 8
Course review; Mid-term exam

Week 9
Write protection

Week 10
Imaging WINTEL

Week 11
Imaging UNIX/LINUX/Solaris

Week 12
Detailed storage investigations: Logical files, deleted files, slack space, free space, and unallocated space

Week 13
**RAID devices**

**Week 14**  
*Quality control:* Steganography; Commercial tools used in digital media forensics

**Week 15**  
Final exam

(b) **Required Reading and Reference Material:**


Reading assignments from the Web include the following sites:  
www.house.gov  
www.microsoft.com  
www.sun.com  
www.foundstone.com

(c) **Student Evaluation Criteria**

Mid-term: 35%

Project: 30%

Final: 35%