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: 660

Full Course Title: Network Forensics

Abbreviated Course Title (24 characters max.): Network Forensics

Credit hours: 3.0  
Program of Record: MS in Telecommunications

Repeatable for Credit?  
___ D=Yes, not within same term  
___ T=Yes, within the same term  
___ 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: Fall 2005

Prerequisites or co-requisites: prerequisite course TCOM 509 and a working knowledge of a computer language

Catalog Description (35 words or less) Please use catalog format and attach a copy of the syllabus for new courses: Collection, preservation, and analysis of network generated digital evidence such that this evidence can be successfully presented in a court of law (both civil and criminal). Relevant federal laws will be examined as well as private sector applications. The capture/intercept of digital evidence, the analysis of audit trails, the recordation of running processes, and the reporting of such information will be examined.

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>
</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 660 Network Forensics (3:3:0)
   (b) Prerequisites: TCOM 509 and a working knowledge of computer programming
   (a) Catalog Description:
       This course deals with the collection, preservation, and analysis of network generated digital evidence 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 capture/intercept of digital evidence, the analysis of audit trails, the recordation of running processes, and the reporting of such information will be examined.

2. JUSTIFICATION
   (a) Course Objectives:
       At the conclusion of this course, the student will have learned the laws, concepts, tools, and methodologies necessary to collect, preserve, analyze, and present network digital evidence in a court of law. The student will be able to successfully analyze logs, decipher network traffic, and report this information in a suitable format.
   (b) Course Necessity:
       Since the explosion of the Internet with the World Wide Web, our increasingly internetwork-dependent society has been under attack by those who would subvert the Internet for political, economic, and/or personal gain. The field of network forensics represents how intercepted digital evidence is used to document, identify, and successfully prosecute those who would exploit computer networks. Viruses, trojans, worms, root kits, buffer overflows, and other malicious code permeate society, and network forensics provides the tools and techniques to determine and document what happened.
   (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 the needs of the telecommunications industry. It builds on other courses within the program (TCOM 501/502, TCOM 509, TCOM 548/556, and TCOM 562) with the goal of applying network-engineering skills to the field of network forensics. This course will work hand in hand with the new course TCOM 661 Digital Media Forensics that will be offered in alternating semesters. It will also be a complementary course to another new course, TCOM 662 Network Security Issues, and related courses 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 fall semester, starting fall 2004 and every fall thereafter.
   Proposed Instructors: Dr. Jeremy Allnutt, Mr. Robert Osgood, and other suitably qualified faculty.

5. COURSE OUTLINE
(a) Syllabus

**Week 1**
*Course overview:* Introduction to the course and review of TCP/IP and Ethernet and aspects required for network forensic analysis

**Week 2**
*Presentation of Federal Laws:* Federal laws pertaining to the interception of digital evidence will be presented as they pertain to network forensics

**Week 3**
*Intrusion methodologies:* network vulnerabilities and likely attack points will be presented

**Week 4**
*Network data collection devices.* The role routers, firewalls, intrusion detection systems, together with access control systems will be presented.

**Week 5**
*Log collection and analysis WINTEL:*

**Week 6**
*Log collection and analysis WINTEL (contd.):*

**Week 7**
*Course review;* Mid-term exam

**Week 8**
*Log collection and analysis Unix/Linux*

**Week 9**
*Log collection and analysis Unix/Linux (contd.)*

**Week 10**
*Using PERL to analyze log information*

**Week 11**
*Collection of online processes WINTEL*

**Week 12**
*Collection of online processes UNIX/LINUX*

**Week 13**
*Interception of digital evidence:* Techniques for the interception of digital evidence (Ethereal, Snoop, Etherpeek)

**Week 14**
*Writing computer forensics reports*

**Week 15**
Final exam

(b) Required Reading and Reference Material


Reading assignments from the Web include the following sites:
www.house.gov
www.cert.org
www.cisco.com
www.ethereal.com
www.perl.org
www.foundstone.com

Suggested supplementary material includes:

"PERL by Example",

(c) Student Evaluation Criteria

Mid-term: 35%

Project: 30%

Final: 35%