Course Approval Form

For approval of new courses and deletions or modifications to an existing course.
registrar.gmu.edu/facultystaff/curriculum

Action Requested:  
- [x] Create new course   
- [ ] Delete existing course   
- [ ] Modify existing course

Course Level:  
- x Undergraduate   
- [ ] Graduate

College/School:  
- VSE (Volgenau School of Engineering)

Submitted by:  
- Robert Osgood

Department:  
- ECE

Subject Code:  
- CFRS

Number:  
- 771

Effective Term:  
- Fall
- [x] Spring
- [ ] Summer
- Year 2014

Title:  
- Current
  - Banner (30 characters max including spaces)
- New
  - Digital Forensic Profiling

Credits:  
- [x] Fixed 3
- [ ] Variable

Repeat Status:  
- [x] Not Repeatable (NR)
- [ ] Repeatable within degree (RD)
- [ ] Repeatable within term (RT)

Grade Mode:  
- [x] Regular (A, B, C, etc.)
- [ ] Satisfactory/No Credit
- [ ] Special (A, B C, etc. +IP)

Schedule Type Code(s):  
- [x] Lecture (LEC)
- [x] Lab (LAB)
- [x] Recitation (RCT)
- [ ] Internship (INT)
- [ ] Seminar (SEM)
- [ ] Studio (STU)

Prerequisite(s):  
- CFRS 500, CFRS 661

Corequisite(s):  
- [ ]

Instructional Mode:  
- [x] 100% face-to-face
- [ ] Hybrid: ≤ 50% electronically delivered
- [ ] 100% electronically delivered

Special Instructions:  
- (list restrictions for major, college, or degree; hard-coding; etc.)

Are there equivalent course(s)?  
- [x] Yes
- [ ] No

If yes, please list

Catalog Copy for NEW Courses Only (Consult University Catalog for models)

Description:  
- Presents the application of criminal profiling to digital forensic evidence and cybercrime. Covers typologies of cyber criminals and reviews how the results of digital forensics can be used to profile individuals to better facilitate investigative interviews and prosecutions. Applies digital profiling to the identification of criminal behavior for insider threats and fraud.

Notes:  

Indicate number of contact hours:  
- [ ] Hours of Lecture or Seminar per week: 3
- [ ] Hours of Lab or Studio:

When Offered:  
- [x] Fall
- [x] Summer
- [x] Spring

Approval Signatures

Andre Manitius  
10/18/13
Department Approval

College/School Approval

If this course includes subject matter currently dealt with by any other units, the originating department must circulate this proposal for review by those units and obtain the necessary signatures prior to submission. Failure to do so will delay action on this proposal.

Unit Name  
- [ ]

Unit Approval Name  
- [ ]

Unit Approver’s Signature  
- [ ]

Date  
- [ ]

For Graduate Courses Only

Graduate Council Member  
- [ ]

Provost Office  
- [ ]

Graduate Council Approval Date  
- [ ]

For Registrar Office’s Use Only:  
Banner ____________________________  Catalog ____________________________

revised 2/2/10
SCHOOL PROPOSAL TO THE GRADUATE COUNCIL
BY
THE VOLGENAU SCHOOL OF ENGINEERING

1. CATALOG DESCRIPTION
   (a) CFRS 771 Digital Forensic Profiling
   (b) Prerequisites: CFRS 500 and CFRS 661
       Presents the application of criminal profiling to digital forensic evidence and cybercrime. Covers typologies of cyber criminals and reviews how the results of digital forensics can be used to profile individuals to better facilitate investigative interviews and prosecutions. Applies digital profiling to the identification of criminal behavior for insider threats and fraud.

2. JUSTIFICATION
   (a) Course Objectives:
       Through this course students will be able to articulate the various aspects of criminal profiling, including inductive and deductive profiles, modus operandi and signatures, and victimology. Students will be able to identify targets for digital forensic profiling, including mobile devices, log files, Internet activity, GPS devices, and non-traditional digital forensic sources. Students will exhibit an understanding of how digital evidence can provide behavioral clues that can be used in search warrants, interviews, and subsequent analyses. Students will demonstrate an understanding of how behavioral digital evidence can be used to show intent for prosecutorial purposes and combat current defense strategies. Students will be familiar with how to profile the different types of individuals that commit computer crime (and computer facilitated crime), including: Organized Crime, Digitally Facilitated Fraud, Digital Stalkers, Child Pornographers, Data Thieves, and Cyber espionage Actors.

   (b) Course Necessity:
       The course builds upon the introductory concepts of computer forensics and provides acquired knowledge and skills as how to digitally profile criminals.

   (c) Relationship to Existing Courses:
       This course builds on the courses CFRS 500 Introduction of Technologies of Forensic Value and CFRS 661 Digital Media Forensics, and this course specifically expands on the area of digital profiling.

3. APPROVAL HISTORY
   Department Date: October 18th, 2013
   IT&E Graduate Committee Date: 
   IT&E Dean Date: 

4. SCHEDULING
   The course will be offered every fall and spring semester, starting fall 2014 and every regular semester thereafter.

5. PROPOSED INSTRUCTORS
   Robert Osgood, Chad Steele, Jim Jones, and other suitably qualified faculty

6. COURSE OUTLINE
   (a) Week 1
       Introduction to Criminal Profiling
       Traditional profiling is covered, including an explanation of nomothetic and idiographic approaches. Statistical and case-based analysis is reviewed.

       Week 2
       Traditional Victimology, Criminal Motivation, MO, and Signature
       The choice of victim and the linkage to the behavior are reviewed. The concepts of modus operandi, signature, and ritual are compared and contrasted. Motive and intent are reviewed.

       Week 3
       Introduction to Digital Profiling
       The sources of digital information that can inform behavior are examined. Types of digital crime and associated behavioral characteristics are covered.

       Week 4
       Digital Victimology, Criminal Motivation, MO, and Signature
How digital criminals target victims, including researching, exploiting, and covering their actions will be covered. Specific digital artifacts that can be used to differentiate a modus operandi from a digital signature are reviewed.

**Week 5**

**Sources of Digital Profile Information/Constructing a Digital Profile**

Key digital locations where information can be behaviorally useful are reviewed, including email meta-data, browser history, and activity timelines. These are put together using a methodology that categorizes an offender on several axis including technical ability and countermeasures used.

**Week 6**

**Fraud and Identity Theft Patterns of Behavior**

Traditional criminal activity that is applied to the web is reviewed. Organized crime rings, focusing on recent attacks and convictions, are analyzed for behavioral commonality.

**Week 7**

**The Hacker Mindset**

Hacking, as hacktivism as well as for other means is covered. Individual hackers with diverse motives, ranging from Gary McKinnon to Aaron Swartz are profiled.

**Week 8**

**Online Child Exploitation**

Online predators, ranging from child pornographers to those who impersonate children are cataloged. The differing motives of each offender type are analyzed through the lens of digital evidence.

**Week 9**

**Virus Writers**

Viruses and worms are written for many different reasons – ranging from the Robert Tappan Morris worm to the Stuxnet virus. The different techniques and how victimology impacts their deployment are covered.

**Week 10**

**Cyber terrorists**

Cyberterrorism uses the techniques of all of the other types of cybercrime with the motivation of causing destabilization and terror for a particular group. Website mass defacements, denial of service attacks, and other damaging techniques are contrasted with for-profit and other motivators.

**Week 11**

**Using the Digital Profile in Search Warrants and Interviews**

The application of the behavioral cues identified above and the extraction of digital artifacts are employed to assist in developing probable cause for search warrants and for developing relevant themes in interviews.

**Week 12**

**The Insider Threat**

The insider threat includes the risk that an individual in an organization utilizes their access and/or knowledge to digitally exploit their employer. The various motives and countermeasures that can be employed (and those that are ineffective) for combating the psychological aspects of insider threat are reviewed.

**Week 13**

**Proving Intent and Combatting Defense Strategies**

The capstone lecture will be on bringing the information developed above to bear on proving intent in a court of law and on utilizing the profiles and digital evidence to combat various defense strategies.

**Week 14**

**Project Presentation**

Student presentations on the tool that they developed to assist in digital profiling efforts.

**Week 15**

**Final**

---

*(b) Required Reading and Reference Material*


Lanning, Kenneth V. "SEX OFFENDER CONTINUUM."


(c) Student Evaluation Criteria

Grades will be assessed on the following components:

- **Case Study** 30%
- **Tool Construction/Demo** 30%
- **Research Paper** 20%
- **Final Exam** 20%

**Case Study** - Each student is responsible for presenting a case study on a particular computer criminal. The case study should be approximately 30 minutes in length, and will be presented at the end of each class session (starting on week 3).

**Tool Development/Paper** - Each student will develop a tool and present a paper on that tool covering a specific area of interest in digital profiling. Tool design and selection is up to the student, as is the platform used. The tool may use a prototype interface or be text-based, and provide information useful in doing a digital profile. Students may work in groups of up to 4 students. Each student in the group will receive the same grade. Only one project/paper needs to be submitted per group. The tool must first be described and approved in a proposal (due week 3). The student (or group) must demonstrate the tool on the final two days of class in a 15 minute demonstration and submit their research paper.