| LSC Use Only Proposal No:<br>LSC Action-Date: | UWUCC Use Only Proposal No: 11-124;<br>UWUCC Action-Date: App-4/3/12 Senate Action Date: App-5/01/12 |
|---|---|

**Curriculum Proposal Cover Sheet - University-Wide Undergraduate Curriculum Committee**

| Contact Person(s) Rose Shumba | Email Address shumba@iup.edu |
|---|---|
| Proposing Department/Unit Computer Science | Phone 7-3166 |

Check all appropriate lines and complete all information. Use a separate cover sheet for each course proposal and/or program proposal.

**1. Course Proposals (check all that apply)**

- [x] New Course
- [ ] Course Prefix Change
- [ ] Course Deletion
- [ ] Course Revision
- [ ] Course Number and/or Title Change
- [ ] Catalog Description Change

*Current* course prefix, number and full title: _____

*Proposed* course prefix, number and full title, if changing: COSC 429 Digital Forensics

**2. Liberal Studies Course Designations, as appropriate**

This course is also proposed as a Liberal Studies Course (please mark the appropriate categories below)

- [ ] Learning Skills
- [ ] Knowledge Area
- [ ] Global and Multicultural Awareness
- [ ] Writing Across the Curriculum (W Course)
- [ ] Liberal Studies Elective (please mark the designation(s) that applies – must meet at least one)
  - [ ] Global Citizenship
  - [ ] Information Literacy
  - [ ] Oral Communication
  - [ ] Quantitative Reasoning
  - [ ] Scientific Literacy
  - [ ] Technological Literacy

**3. Other Designations, as appropriate**

- [ ] Honors College Course
- [ ] Other: (e.g. Women's Studies, Pan African)

**4. Program Proposals**

- [ ] Catalog Description Change
- [ ] Program Revision
- [ ] Program Title Change
- [ ] New Track
- [ ] New Degree Program
- [ ] New Minor Program
- [ ] Liberal Studies Requirement Changes
- [ ] Other

*Current* program name: _____

*Proposed* program name, if changing: _____

| 5. Approvals | Signature | Date |
|---|---|---|
| Department Curriculum Committee Chair(s) | | 2/6/12 |
| Department Chairperson(s) | | 2/10/2012 |
| College Curriculum Committee Chair | | 3/7/12 |
| College Dean | | 3/12/12 |
| Director of Liberal Studies (as needed) | | |
| Director of Honors College (as needed) | | |
| Provost (as needed) | | |
| Additional signature (with title) as appropriate | | |
| UWUCC Co-Chairs | Gail S Sechrist | 4/3/12 |

Received
MAR 12 2012
Liberal Studies

**SAMPLE SYLLABUS OF RECORD**

**NEW Syllabus of Record**

## COSC 429: Digital Forensics

### I. Course Description

**COSC 429 Digital Forensics** 3c-0l-3cr

Prerequisites: COSC 110 or equivalent programming course, junior standing or permission of instructor.

Takes a detailed, hands-on approach to the use of computer technology in investigating computer crime. From network security breaches to child pornography, the common bridge is the demonstration that particular electronic media contains incriminating evidence. Using modern forensics tools and techniques, students learn how to conduct a structured investigation process to determine exactly what happened and who was responsible, and to perform this investigation in such a way that the results are useful in criminal proceedings. Real world case studies will be used to provide a better understanding of security issues. Unique forensics issues associated with various operating systems including Linux/Windows operating systems and associated applications are covered.

### II. Course Outcomes:

Upon completion of this course, students will be able to:

1. Explain digital forensics and investigations on digital media.
2. Identify relevant electronic evidence associated with various violations of specific laws, including, but not limited to, computer crimes.
3. Locate and recover relevant electronic evidence from digital media using a variety of tools.
4. Identify and articulate probable cause as necessary to obtain a warrant to search for electronic artifacts and recognize the limits of warrants.
5. Explain the principles and practice of ethics and law for computer forensics investigators.
6. Explain how to manage/conduct a computer crime investigation involving digital media.
7. Follow a documented investigation process.
8. Present the evidence and conclusions of an investigation in a report form.
9. Describe core computer science theory necessary to perform computer forensics.

### III. Course Outline

**1. Fundamentals of digital forensics** **3 hrs**

   a. Introduction to digital forensics
   b. Digital evidence and investigations
   c. Real life examples of computer crime
   d. Challenging aspects of digital forensics

2. **Computer crime investigation process** **3 hrs**
   a. The Investigation process
   b. Preparing a computer investigation
   c. Systematic approach to an investigation
   d. Procedures for corporate high-tech investigations
   e. Conducting an investigation

3. **Digital evidence acquisition.**
   a. Implications of related law **2 hrs**
      i. The 4th Amendment to the US Constitution and its application to computer/network search and seizure
      ii. The implications of the Electronic Communications and Privacy Act, the US Patriot Act, US Federal and State guidelines
      iii. Methods of ensuring chain of custody of evidence
   b. Processing crime and incident scenes **3 hrs**
      i. Rules for acquiring digital evidence.
      ii. Collecting evidence at private-sector incident scenes.
      iii. Steps in preparing for evidence search.
      iv. Performing a digital hash.
   c. Process of digital evidence acquisition **3 hrs**
      i. Procedures for digital evidence acquisition
      ii. Digital evidence storage formats
      iii. Acquisition tools
      iv. Validating data acquisitions
      v. RAID acquisition methods

**First Exam** **1 hr**

4. **Computer science theory behind computer forensics.**
   a. Windows and DOS file systems **4 hrs**
      i. Microsoft file structures
      ii. The structure of NTFS disks
      iii. Windows Registry
      iv. Microsoft and DOS startup tasks
      v. Forensics analysis in Windows
         1. Live response
         2. Response data analysis
   b. Linux boot processes and file systems **4 hrs**
      i. UNIX and Linux disk structures
      ii. UNIX and Linux boot processes.
      iii. Other disk structures.
      iv. Forensics analysis in Linux

5. **Methods for performing evidence examination.**
   a. Evidence examination procedure **4 hrs**
      i. Physical/logical extraction
      ii. Analysis of extracted data
      iii. Data hiding techniques

b. Recovering graphics files **4 hrs**
   i. Types of graphics file formats.
   ii. Types of data compression.
   iii. Locating and recovering graphics files.
   iv. Indentifying unknown file formats.
   v. Copyright issues with graphics.

**Second Exam** **1 hr**

c. E-mail Investigations **3 hrs**
   i. The role of e-mail in investigations
   ii. Client and server roles in e-mail
   iii. Tasks in investigating e-mail crimes and violations
   iv. The use of e-mail server logs
   v. Available e-mail computer forensics tools
d. Cell Phone and mobile device forensics **2 hrs**
   i. Basic concepts of mobile device forensics
   ii. Procedures for acquiring data from cell phones and mobile devices

**6. Evidence presentation**
a. Procedures for documenting and reporting **2 hrs**
b. Guidelines for writing reports.
c. Using forensics tools to generate reports

**7. Ethical issues for computer forensics.**
a. Expert Testimony in High-Tech Investigations **3 hrs**
b. Guidelines for giving testimony as a technical/scientific or expert witness.
c. Guidelines for testifying in court.
d. Guidelines for testifying in dispositions and hearings.
e. Procedures for preparing forensics evidence for testimony incident.

**Final Exam during the final exam week.**

---

**Total** **42 hrs**

**Final** **2 hrs**

## IV. Evaluation Methods

The final grade will be determined as follows:

| | |
|---|---|
| Three exams | **45%** |
| Projects | **15%** |
| Group project including final presentation | **40%** |

## V. Grading Scale

Grading Scale: A: ≥90% B: 80-89% C: 70-79% D: 60-69% F: <60%

## VI. Attendance Policy

The attendance policy will follow the guidelines as is given in the IUP Handbook.

## VII. Required textbooks, supplemental books and readings

Nelson B, Phillips A, Enfinger F, Steuart C, Guide to Computer Forensics and Investigations, 4th edition, Course Technology, 2010.

## VIII. Special resource requirements

None.

## IX. Bibliography


1. Altheide C., (2004), Forensic analysis of Windows Hosts using UNIX-based Tools, Digital Investigation (Sept), 197-212.
2. Cheng D., (2009), Freeware Forensics Tools for UNIX. Available at: http://www.securityfocus.com/infocus/1503
3. Collins A., (2003) CSI: Body of Evidence, Pocket Books. ISBN: 0743455827.
4. EC-Council, (2010), Computer Forensics: Hard Disk and Operating Systems, 1st Edition, ISBN-10: 1435483502, ISBN-13: 9781435483507, Course Technology.
5. EC-Council, (2010), Computer Forensics: Investigating Data and Image Files, 1st Edition, ISBN-10: 1435483510, Course Technology.
6. Harrison W., (2004), The Digital Detective: An introduction to Digital Forensics. In Advances in Computers, vol. 60, M. Zelkowitz, ed., Academic Press.
7. Jones K., (2008), Forensic Analysis of Internet Explorer Activity Files. Available at: http://umn.dl.sourceforge.net/sourceforge/sourceforge/odessa/IE_Cookie_File_Reconstruction.pdf
8. Leuenberger A., (2004), Win32 - Evidence Gathering. Available at: http://www.csnc.ch/static/download/misc/2004_win32_forensics_v1.1.pdf
9. Morris J., (2010) Forensics on the Windows Platform, Part One. Available at: http://www.securityfocus.com/infocus/1661
10. Nelson B., Phillips A., Enfinger F., Steuart C., (2010), Guide to Computer Forensics and Investigations, 3rd edition, Course Technology.
11. Prosecuting Computer Crimes, Computer Crime & Intellectual Property Section, United States Department of Justice. Available at http://www.cybercrime.gov/ccmanual/index.html
12. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, (2002). Available at http://www.usdoj.gov/criminal/cybercrime/searching.html
13. Stephen B., (2002) Windows Forensics - A Case Study: Part One, SecurityFocus InFocus Article. Available at: http://www.securityfocus.com/infocus/1653
14. Stephen B., (2003) Windows Forensics - A Case Study: Part Two, SecurityFocus InFocus Article. Available at: http://www.securityfocus.com/infocus/1672

15. Willassen S., (2007) Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Available at :http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf
16. Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., (2003), Computer Forensics Education. IEEE Security & Privacy (July/Aug.), 15-23.

**Course Analysis Questionnaire**

## A. Details of the Course

A1. This course is one of the controlled electives for Computer Science and Criminology majors, and MIS students that minor in Information Assurance. This course is not intended to be a Liberal Studies course.

A2. This course does not require changes in any other course in the department.

A3. This course has been previously offered two times as COSC481 in the spring of 2010 and spring 2011.

A4. This course is not dual listed.

A5. This course is not to be taken for variable credit.

A6. Similar courses are offered at the following institutions.

Portland State University: Digital Forensics
University of Alaska, Fairbanks: Digital Forensics
Eastern Washington University: Computer Forensics
University of Washington: Digital Forensics
Champlain College: Digital Forensics
Stroudsburg University: Introduction to Digital Forensics
Kutztown University: Computer Forensics.

A7. This course is highly recommended by the National Security Agency (NSA). The offering of this course will help towards the NSA reaccreditation process for the Institute of Information Assurance education. NSA has set up a working group on the standardization of the Digital Forensics curriculum. I am a member of that group.

## B. Interdisciplinary Implications

B1. This course will be taught by one instructor.

B2. The content of this course does not overlap with any other at the University.

B3. This course is not cross-listed.

## C. Implementation

C1. No new faculty member will be hired to teach this course. This course will be included in the normal rotation of upper-level electives for majors.

C2. Other resources:

1. Current space allocations are adequate to offer this course.
2. Special equipment needed for this course is already available in the Computer Science department.
3. Current laboratories are sufficient for this course.
4. Current library holdings are adequate.
5. The department has a new isolated information assurance lab, equipped with Encase software for teaching the course.

C3. No grant funds are necessary to provide supplementary materials.

C4. This course will be offered every other Spring semester.

C5. One section will be offered at a time.

C6. Up to 24 students can be accommodated in this class in which students do considerable amount of writing and capacity of the digital forensics lab.

C7. No professional society recommends enrollment limits or parameters for this course.

C8. This course does not involve the use of distance education.

**D. Miscellaneous**

No additional information is necessary.