UNIVERSITY OF NEBRASKA AT OMAHA
COURSE SYLLABUS/DESCRIPTION

Department and Course Number	IASC 4380 (cross-listed as CSCI 4380)
Course Title	Computer and Network Forensics
Course Coordinator	Stephen Nugen
Total Credits	3
Date of Last Revision	August 31, 2012

1.0 Course Description

1.1 Overview of content and purpose of the course.

Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored on a computer. This course takes a technical, legal, and practical approach to the study and practice of incident response, computer forensics, and network forensics. Topics include legal and ethical implications, duplication and data recovery, steganography, network forensics, and tools and techniques for investigating computer intrusions. This course is intended as a second course in information assurance for undergraduate students as well as other qualified students. It is also intended as a foundation course for graduate digital forensics studies.

1.2 Prerequisites of the course

Introduction to information assurance (IASC 1100, CIST 3600, or instructor permission).
Computer networking (CSCI 3550 or ISQA 3400, or instructor permission).
Host security administration (IASC 3350, or IASC 3370, or instructor permission).

1.3 Overview of contents and purpose of the course

The Computer Forensics class is designed for the Information Assurance student to learn what actions are appropriate for preservation of evidence in case of intrusion or data theft. The topics covered include, but are not limited to:

- Core terms and principles of information assurance: Confidentiality, Integrity, Availability, Threats, Vulnerabilities, Types of Malware, Authorization, Access Control, Accountability, Identification, Authentication, Security Controls, and Defense in Depth.
- Computer networking topics: Media, Protocol Stacks, Protocol Encapsulation, ARP, IP addressing, IP routing, ICMP, DHCP, TCP Virtual Circuits, Network Address Translation, DNS, and HTTP.
- Operating system logging, file system organization, system-level filesystem calls and operations.

- Database operations and organization, security relative to externally facing database interfaces. Understand the context and motivation for incident response and computer/network forensics.
- Understand and demonstrate how to acquire and initially analyze volatile and persistent evidence from Windows and Unix host operating systems.
- Understand and partially demonstrate how to acquire and analyze network based evidence.
- Identify tradeoffs between different methods for evidence acquisition and analysis.
- Discover and explain errors in evidence acquisition and analysis.
- Demonstrate the ability for independent learning in this area by preparing, presenting, and defending a discussion on some aspect of computer/network forensics not covered by class lectures.

1.4 Unusual circumstances of the course.

None

2.0 Course Justification Information

2.1 Anticipated audience / demand.

This course is required for all Information Assurance undergraduates. It is anticipated that some CS and MIS undergraduates perusing an IA concentration in their major may also take this course as an elective.

2.2 How often the course will be offered and anticipated enrollment.

The anticipated schedule is to offer this class once yearly in the Spring semester. With the current IA enrollment for undergraduate at approximately 100 students, and ¼ nearing graduation at any time, we anticipate a typical class size of approximately 25 students.

2.3 If it is a significant change to an existing course please explain why it is needed

It is not a significant change to an existing course.

3.0 Objective Information

This course is not a part of the general education curriculum.

Here is a list of performance objectives stated in a student's perspective.

- Identify appropriate level of data breech in a computer system so that appropriate actions can be taken.

- Learn proper procedures for contacting authorities concerning data theft, as well as legal issues which might result.

- Identify and demonstrate an understanding of the risks associated with information flow between different security domains.

- Utilize forensics tools to analyze system logs, filesystem data, operating system performance, memory contents, and so on.

- Evaluate other security designs and implementations with respect to external requirements.

- Students will learn the principles of computer and network forensics illustrated by cases histories involving Windows hosts, Linux hosts, and network traffic. Students will apply, extend, and demonstrate that knowledge through hands-on laboratory assignments.

- The course will address the social and ethical issues related to the special role of computer and network forensics including legal obligations and the potential for ethical conflicts in the collection and analysis of sensitive data which may include individuals' private information, trade secrets, and banned content.

- Course discussions will include critiques of court cases where the expert testimony may have been incomplete.

4.0 Content and organization

		Contact hours
4.1	Context and a review of fundamentals.	4.0
	4.1.1 Context within Information Assurance	
	4.1.2 Motivations	
	4.1.3 Legal considerations	
	4.1.4 Process frameworks	
	4.1.5 Information encoding	
	4.1.6 Information hiding.	
4.2	Live Response for Windows Hosts.	10.0
	4.2.1 Incident response for Windows hosts.	
	4.2.2 Acquiring and handling live state (volatile) evidence from Windows hosts.	
	4.2.3 Initial analysis of volatile evidence.	
4.3	Network-Based Evidence.	7.0
	4.3.1 Options for the acquisition of network-based evidence.	
	4.3.2 Analysis of network-based evidence.	
	4.3.3 Analyzing the combination of network- and host-based evidence for stronger findings.	
4.4	Live Response for Unix/Linux Hosts.	7.0
	4.4.1 Incident response.	

4.4.2 Acquiring and handling live state (volatile) evidence.

4.5 Internet Forensics. 4.0

4.6 Offline Forensics.
4.6.1 Acquiring and safeguarding persistent evidence (e.g., host images) for Windows and Unix/Linux hosts. 7.0
4.6.2 Analyzing persistent evidence.

4.7 Student Project Presentations. 6.0

5.0 Teaching Methodology

5.1 Methods to be used

The primary teaching methods will be lecture, discussion, demonstrations, lab exercises, reading assignments, and a comprehensive project.

5.2 Student role in the course

Students will attend lectures and demonstrations, participate in discussions, complete and submit lab and other assignments, complete a comprehensive project, and complete required examinations.

6.0 Evaluation

6.1 Types of student projects

Students will complete assignments requiring additional study and short written responses to instructor-provided questions.

Students will complete small and medium laboratory assignments and projects with specified deliverables such as: Report of Findings. Most laboratory assignments will be due within one or two weeks of assignment. Some laboratory assignments will be started in-class. Laboratory assignments will generally require access to STEAL-1 outside of class.

Students will complete a comprehensive project that incorporates course content and independent study on some instructor-approved topic related to computer and/or network forensics.

Student performance will be evaluated through two examinations: Midterm Exam and a comprehensive Final Exam. Both of these exams will include a variety of question types to measure student understanding of the material.

6.2 Basis for determining the final grade

The final grade will be determined from the following weighted components.

Assignments and project	55%
Midterm Exam	20%
Final Exam	25%
	100%

6.3 Grading scale.

Points	Grade
97 – 100%	A+
93 – 96%	A
90 – 92%	A-
87 – 89%	B+
83 – 86%	B
80 – 82%	B-
77 – 79%	C+
73 – 76%	C
70 – 72%	C-
67 – 69%	D+
63 – 66%	D
60 – 62%	D-
0 – 59%	F

7.0 Resource Material

7.1 Textbooks and/or other required readings used in course

Carnegie-Mellon Software Engineering Institute: CERT Training and Education. (2005). *First Responders Guide to Computer Forensics*. Available from http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf

Microsoft. (2007). *Fundamental Computer Investigation Guide For Windows.* Available from http://www.microsoft.com/technet/security/guidance/disasterrecovery/computer_investigation/default.mspx.

National Institutes of Standards and Technology. (2006). *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response.*. Available from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Altheide, Cory, and Harlan A. Carvey. *Digital Forensics with Open Source Tools*. Burlington, MA: Syngress, 2011. Print.

Carvey, Harlan. *Windows Registry Forensics*. Amsterdam: Elsevier Syngress, 2011. Print.

Malin, Cameron H., Eoghan Casey, and James M. Aquilina. *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides*. Waltham, MA: Syngress, 2012. Print.

Nelson, Bill, Amelia Phillips, and Christopher Steuart. *Guide to Computer Forensics and Investigations*. Boston, MA: Course Technology Cengage Learning, 2010. Print.

7.2 Other suggested reading materials.

Additional materials and online resources will be identified for students at the beginning of the course and as the course progresses.

7.3 Other sources of information.

Anson, S. & Bunting, S. (2007). *Mastering Windows Network Forensics and Investigation*. Indianapolis, IN: Wiley Publishing, Inc.

Aquilina, J. M., Casey, E. & Malin, C. H. (2008). *Malware Forensics: Investigating and Analyzing Malicious Code*. Burlington, MA: Syngress Publishing, Inc.

Carrier, B. (2005). File *System Forensic Analysis (3rd ed.)*. Upper Saddle River, NJ: Pearson Education, Inc.

Carvey, H. (2007). *Windows Forensic Analysis: DVD Toolkit*. Burlington, MA: Syngress Publishing, Inc.

Davidoff, Sherri, and Jonathan Ham. *Network Forensics. ; Tracking Hackers Through Cyberspace.* N.p.: Prentice Hall PTR, 2012. Print.

Jones, R. (2006). *Digital Forensics: Using Digital Evidence to Solve Computer Crime (2nd ed.)*. Sebastopol, CA: O'Reilly Media, Inc.

Jones, K. J., Bejtlich, R. & Rose, C. W. (2006). *Real Digital Forensics: Computer Security and Incident Response (3rd ed.)*. Upper Saddle River, NJ: Pearson Education, Inc.

Pogue, C., Altheide, C. & Haverkos, T. (2008). *UNIX and Linux Forensic Analysis DVD Toolkit*. Burlington, MA: Syngress Publishing, Inc.

Sammons, John. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* Amsterdam: Elsevier/Syngress, 2012. Print.

Sanders, C. (2007). *Practical Packet Analysis: Using Wireshark to Solve Real World Network Problems*. San Francisco, CA: No Starch Press, Inc.

8.0 Oral and Written Communications

8.1 Accommodations statement

Accommodations are provided for students who are registered with Disability Services and make their requests sufficiently in advance. For more information, contact Disability Services (EAB 117, Phone: 554-2872, TTY: 554-3799) or go to the website: http://www.unomaha.edu/disability.

8.2 Other

All student submissions will be evaluated for technical content, application of principles, completeness, accuracy, and use of use of supporting materials.

Every student is required to develop a project with a written report, typically 10 pages. These projects are graded for scope, technical quality, and clarity of the communication (structure, grammar, and spelling).

Every student must prepare, deliver, and defend an oral presentation of their project to the entire class.

8.3 Author

Steve Nugen, with a dollop of Bill Mahoney

CHANGE HISTORY

Date	***Change***	***By whom***	***Comments***
02/12/2009	Revised ABET version	Nugen	Prerequisites changed.
8/31/12	Made to match CCMS and entered in.	Mahoney	