TCOM 4243: Information Technology Forensics
Spring Semester 2015

Sections:

TCOM 5243.001	M, 4:30 – 7:10	MSCS 310
TCOM 5243.801	M, 4:30 – 7:10	T-NCB 209
TCOM 5243.503	Distance, with recorded lectures	

Instructor: Dr. Jim Burkman
E-mail: jim.burkman@okstate.edu
Homepage: http:/oc.okstate.edu
Office: BUS 311C
Office hours: Monday 9-11 and 1-4, also by appointment
Phone: 744-5142
Club: http://isac.okstate.edu

Distance Learning Office: spearsdistance@okstate.edu
405-744-4048
Twitter: @spearsdistance

Textbooks: Required:

Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet, Eoghan Casey, ISBN 978-0123742681 (~ $40)

Recommended Reading:

Digital Forensics with Open Source Tools, First Edition, Cory Altheide, ISBN 978-1597495868 (~ $40)

The slides will follow the Casey book pretty closely. Given the density of the material I recommend buying the book and reading the assigned chapters before class. It's cheap, so get it and read it. The Altheide book is a great reference for open source forensics tools. I'll be using the Altheide book to look for both Short Assignments (SA) and PAATH assignments. PAATH (**P**lay **AT H**ome) assignments are ungraded hands-on projects for students who want to extend their technical strengths.

The OSU Spring Syllabus Attachment includes important dates, information, and resources to HELP YOU SUCCEED and is available at: http://goo.gl/U6Y8ir (Stillwater) and http://goo.gl/oBkDRN (Tulsa).

Course Description: Digital Forensic Analysis introduces students to both the technical and legal aspects of digital forensics and the investigation of fraud. Legal aspects covered are the Federal Rules of Evidence, the Federal Rules of Civil Procedure, and several federal acts and regulations that affect the practice of digital forensics. Students must approach their forensic investigation using a framework that incorporates these guidelines and laws. This framework will in turn guide them in creating an ethical code of conduct.

Students progressively incorporate skills learned in class to gather evidence using digital forensic tools and techniques. They are presented with diverse challenges during their investigation that they must overcome to produce the required evidence to support their hypothesis. Some of these challenges require the student to think and use digital forensic software in ways that may not seem intuitive or be found in a user manual. The overarching objectives for students are to have performed an investigation using digital forensic techniques that can stand up in a court of law, and also gain a broad understanding of the domain of digital forensic science.

This class will be a blended mix of lecture and self-guided hands-on labs. Be sure to check the D2L site often. This syllabus and the D2L site for this class will likely change in response to the progress of this class. I will make an effort to post course changes on D2L, and also bring them up in class. However, I'm prone to just saying things in class that you need to know, without further posting. More formally stated, the policies and schedule in this syllabus are subject to change at my discretion, upon notice in any form to the class. You are responsible for getting any downloads offered for upcoming classes from D2L. Handouts, assignments, slides, due dates, and other information will be posted on D2L.

Course Topics (Subject to Change)	
12-Jan	Intro/Overview of Field (Chapters 1 and 2)
19-Jan	**Martin Luther King Day – No Class**
26-Jan	Legal Aspects of Forensics (Chapters 3, 4 and 5)
2-Feb	Digital Investigations (Chapters 6, 7, 8 and 9)
9-Feb	Forensics Investigation Process (Chapters 16 and 22)
16-Feb	**Exam 1**
23-Feb	Threats (Chapter 14)
2-Mar	Intrusions (Chapter 13)
9-Mar	Computer Physiology (Chapter 15)
16-Mar	**Spring Break**
23-Mar	Tools and Resources
30-Mar	**Exam 2**
6-Apr	Digital Evidence - Windows (Chapter 17)
13-Apr	Digital Evidence - Linux (Chapters 18 and 19)
20-Apr	Network Forensics (Chapters 21, 23, 24 and 25)
27-Apr	Mobile Forensics (Chapter 20)

Learning Goals and Course Objectives:

Ethical Decision Making

Upon completion of this course the student should be able to:

Identify the ethical issues of various forms and degrees of criminal behavior in cyberspace

Identify the ethical responsibilities of Information Assurance professionals

Identify the different roles of law enforcement, politics, court decisions, corporate influence and consumer attitudes surrounding issues of digital forensics, search and seizure, chain of custody and the balance between privacy and lawful intrusion.

Business Knowledge and Competency

Upon completion of this course the student should be able to:

Demonstrate a basic knowledge of the vocabulary, processes, environment and practices of digital forensics in the context of the business environment.

Recognize interrelationships between digital forensic investigations and the other core business disciplines.

Recognize and appreciate the global differences and similarities in the application of digital forensics, particularly by contrasting the laws and policies of the US in comparison with the EU.

Technological Competence

Upon completion of this course the student should be able to:

Recognize, discuss and evaluate a variety of core digital forensics technical skills including (but not limited to): the use of commercial and open source digital forensic tools and applications, finding hidden or deleted data in Windows, Linux and Mac systems on diverse media (hard drives, SSD, USB, memory, etc), and applying those skills to computers, tablets, phones and other digital devices.

Recognize, discuss and evaluate a variety of core Information Assurance skills including (but not limited to): steganography; program and o/s security; legal and ethical issues of information assurance; and data safeguard duties and responsibilities in the corporate environment.

Disabled Students: According to the ADA, each student with a disability is responsible for notifying the University of his/her disability and requesting accommodations. If you think you have a qualified disability and need classroom accommodations, contact the office of Student Disability Services (SU 315). Please advise the instructor of your disability as soon as possible, to ensure timely implementation of appropriate accommodations. Faculty have an obligation to respond when they receive official notice of a disability from SDS but are under no obligation to provide retroactive accommodations. To receive services, you must submit appropriate documentation and complete an intake process during which the existence of a qualified disability is verified and reasonable accommodations are identified. Call 744-7116 v/t for more information.

Attendance: Attendance is not graded. This is a dense technical and lecture course taught once weekly. The only reasonable way to expect a good grade is to attend every class. You are solely responsible for any missed material/information if you miss class. Absent a verifiable emergency, there are no provisions for making up exams or homework (or early exams). If a makeup exam is necessary I will have you take it at the testing center, and they charge for the service ($15 or so). Makeup exams may be delivered in a format different than that provided at the regular testing time, to include different questions, question formats and delivery methods (online with a shorter time limit). The exams are based on my lectures, my slides, any outside videos or material that I may ask you to read/watch.

Participation: Class participation is an integral part of the class. It includes not only your ability to read assigned class materials and discuss them intelligently in class, but it also your ability to scan the environment and contribute scholarly information that you find. Stay up on current information security and digital forensics events.

Academic Conduct: Oklahoma State University is committed to the maintenance of the highest standards of integrity and ethical conduct of its members. This level of ethical behavior and integrity will be maintained in this course. Participating in a behavior that violates academic integrity (e.g., unauthorized collaboration, plagiarism, multiple submissions, cheating on examinations, fabricating information, helping another person cheat, unauthorized advance access to examinations, altering or destroying the work of others, and fraudulently altering academic records) will result in your being sanctioned. Violations may subject you to disciplinary action including the following: receiving a failing grade on an assignment, examination or course, receiving a notation of a violation of academic integrity on your transcript (F!), and being suspended from the University. You have the right to appeal the charge. Contact the Office of Academic Affairs, 101 Whitehurst, 405-744-5627, academicintegrity.okstate.edu.

Class Conduct: Arrive on time (especially important on test days), be awake, interact, ask questions, and be engaged in the class. Tame your cell phones.

Grading:

Exams	45%
Forensics Case (FC)	25%
Short Assignments (SA)	15%
Graduate Project	15%

There will be three equally weighted multiple choice exams. Exams will cover all readings, lectures, and all materials presented in class. They are collectively worth 40% of the course grade, or about 13.3% each.

The Forensics Case (FC) is a series of four assignments focused around a digital forensics examination. Each assignment will be considered part of an "investigation" you will perform over the course of the semester. You will use various techniques and digital forensic tools in each investigation. A portion of each assignment is a written narrative; the narrative portion of the homework is a brief synopsis of your actions and any noteworthy findings and/or artifacts of evidentiary value that support your case hypothesis. Since each assignment in the FC is linked in this common endeavor it is imperative you complete all the assignments. Each assignment in the case is worth 6.25% of the course grade (though the assignments do vary widely in terms of time and effort), for a total of 25%

There will be multiple Short Assignments (SA) given throughout the semester. These will all be weighted equally and collectively worth 15% of the course grade. Given *n* Short Assignments, each is worth (1/*n*)*15% of your course grade. By example, given 10 SA, each would be worth (1/10)*15 or 1.5% of your course grade. Conversely, with only 2 SA each would be worth 7.5% of your course grade.

Late FC assignments or SA will not be accepted.

Graduate Project:

You will be required to create a presentation packet that will include: a wiki style article, a written tutorial with screenshots, and a short demonstration video. The project will focus on a specific forensic tool or process that has not been covered or used in class. The wiki article will explain both the tool and the context within which it has value. The tutorial will walk a novice user through a use case from acquisition, installation, investigation and sufficiently legal write up. The video will be a 3-5 minute "teaser" showing the scenario where it would be used and actual use. Further information on the project will be provided later in the semester. Projects will be due to me in the D2L dropbox no later than Monday of finals week at noon. Late projects will not be accepted.

Exam Info:

Distance students (section 503) will have the following exam windows:

Exam 1	Feb 16 - 18
Exam 2	Mar 30 - 21, Apr 1
Exam 3	May 4 – May 6

At the time I wrote this syllabus, I think the final (Exam 3) for non-distant students is Thursday, May 7 from 6:00 – 7:50 pm in the regular classroom. Look at the schedule yourself. I've been known to get final exam dates wrong. The responsibility for being at the right final exam, at the right place and time, is yours alone.

A .pdf file of the Spring 2015 Final Exam schedule is available at http://goo.gl/O0veIU

Distance learning students (section .503) will be expected to follow regular procedures to establish a valid proctor with the Center for Executive and Professional Development. See the Enrollment Confirmation Email Memo on D2L for further information.

A course grade of 90% or better will result in a letter grade of A, 80-89% B, 70-79% C, 60-69% D, <60% F. **NOTE!** I reserve the right to uniformly move the class average up at the end of the semester. For example, if the course average is 70%, I will not move it to 68%, but I may move it to 72%. This is not a curving process, as all individual scores would move the same amount.

Software: Since you are enrolled in an MSIS class you will have access to our MSDNAA license. You should receive an email with information about this opportunity. Go to Login, click on the "I forgot my password", and provide your Okey email as your login name. Your password will be mailed to you. Note that this can take a few days to get set up at the start of the semester. My expectation is that all students in this class have access to a computer that can support VMware virtualization.