Computer and Network Forensics

INF 528 (3 Units)

USC Viterbi School of Engineering

Spring 2015

Description

According to the Internet Crimes Complaint Center Annual Report, in 2011, there were over 300,000 incidents reported to the organization, with a total of $485.3 million dollars directly lost. In a report released by Symantec, the total cost of cybercrime dollars (meaning direct theft, loss due to services disruption, and funds to prevent crime) in 2010 was $388 million, and 73% of adults in the US have experienced some sort of cybercrime in their lifetime. Perhaps more staggering is that because of the reluctance of many organizations to either not report or write off losses due to the impact on reputation, some experts place the cost of cybercrime at over one trillion dollars per year. These staggering figures would have this criminal category eclipse the international drug trade.

While measures in information protection can mitigate the risk to individuals and business, society is not yet at the point where understanding in the virtual domain has translated to preventative action; in essence, people don't yet realize that cyber security equates to the same guards, guns, and walls used to protect other valued resources. Because of this, crime will continue (and probably increase), and therefore it will be necessary for information security professionals to have the knowledge and skills to properly investigate and assist in the prosecution of cybercrime.

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 computer forensics. Topics include: the legal and ethical implications of computer forensics; forensic duplication and data recovery; steganography; network forensics; and tools and techniques for investigating computer intrusions.

This course is intended for first year graduate students with the following qualification: typically coming out of computer science, mathematics, computer engineering, or informatics; it is helpful to have a working understanding of number theory and some programming facility.

This class will be primary individual study, with weekly assigned readings, various homework assignments (laboratory exercises), two forensic cases, one midterm and one final.

Objectives

The nature of digital forensics lends itself to a more applied understanding and concept demonstration than some purely theoretically-based course. Therefore, students are expected to not only understand the principles involved in forensic analysis and investigation, but upon leaving the course, be able to apply these in practice. A summary outline of objectives includes:

- Demonstrate an understanding of the legal and ethical implications of computer forensics and investigations
- Demonstrate an understanding of evidence preservation and authentication
- Understand how to analyze an email header
- Understand how to capture network packets and analyze network traffic
- Understand how to analyze stenographic evidence
- Understand the basics of file systems
- Understand the specifics of FAT32 and NTFS file systems
- Understand how to perform a forensic analysis of a Windows XP and Windows 7 system
- Demonstrate how to draft a digital forensics report for the appropriate audience

Methods of Teaching

The primary teaching methods will be discussion, lecture, demonstrations, assignments, and full case investigations. Students are expected to perform directed self-learning outside of class which encompasses among other things a considerable amount of literature review. The students are expected to take an active role in the course. Students will attend lectures, participate in class assigned team projects, complete regular exams to reinforce the concepts taught and highlight weaknesses in grasp and presentation, complete assigned projects to apply and illustrate the concepts in an applied manner (through demonstrations or class projects).

Students will be given ten laboratory exercises that will require work outside of class to complete. There will be a series of steps that will be required to execute, an analysis of what was performed, and an explanation of the results. These laboratory exercise will be crucial to being able to complete the cases.

Students will be given two full cases to demonstrate their understanding of how to complete a forensics investigation. Students will be provided with the case background and imaged drive. After completing the investigation, students will be required to draft a forensic report appropriate for submission to a court of law, which will be graded appropriately. Each case will require approximately twenty hours to complete.

Instructor	Joseph Greenfield
Contacting the Instructor	joseph.greenfield@usc.edu
Office Hours	OHE 530F, TBA
Lab Assistants	TBA
Lecture/Lab	12:30 – 1:50 Tuesday & Thursday

Required Textbooks

The Basics of Digital Forensics. Sammons.
ISBN: 1597496618

Windows Forensic Analysis Toolkit, 4th Edition. Carvey.
ISBN: 0124171575

NOTE: The above two textbooks are available through USC's Safari Books license, along with many other valuable security and forensics textbooks. To access Safari Books, please visit http://proquest.safaribooksonline.com/
You must either be logged in through the USC Network or through the USC VPN http://itservices.usc.edu/vpn/

Recommended Textbooks (For This Course and the Future)

System Forensics, Investigation and Response. Easttom.
ISBN: 1284031055

Hacking Exposed: Computer Forensics, Second Edition. Davis, Philipp, and Cowen
ISBN: 0071626778

Incident Response & Computer Forensics, Third Edition. Luttgens, Pepe and Mandia.
ISBN: 0071798684

File System Forensic Analysis. Carrier
ISBN: 0321268172

Website

All course material will be on Blackboard (http://blackboard.usc.edu).

Grading

Grading will be based on percentages earned in assignments, cases, and exams. The following is the grade breakdown.

Lab Exercises (10)	40% (4% each)
Case Reports (2)	30% (15% each)
Midterm Exam	10%
Final Exam	20%
Total	100%

Grading Scale

The following shows the grading scale to be used to determine the letter grade.

94% and above	A
90% - 93%	A-
87% - 89%	B+
84% - 86%	B
80% - 83%	B-
77% - 79%	C+
74% - 76%	C
70% - 73%	C-
67% - 69%	D+
64% - 66%	D
60% - 63%	D-
60% and below	F

Policies

No make-up exams (except for documented medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule.

The labs will be posted on Blackboard under the "Assignments" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link.

Cases will be posted on Blackboard, and the forensic drive images will be distributed during class. Case reports must be submitted as a hard copy on or before the due date and time.

It is your responsibility to submit your assignments on or before the due date. Assignments turned in up to 24 hours late will have 20% of the total points deducted from the graded score. Assignments turned in between 24 and 48 hours late will have 50% of the total points deducted from the graded score. After 48 hours, submissions will not be accepted and will be recorded as a 0.

All labs must be submitted through blackboard. All cases must be turned in as a hard copy. Do not email the labs or cases to the TAs, graders or instructor.

Incomplete and Missing Grades

Excerpts for this section have been taken from the University Grading Handbook, located at http://www.usc.edu/dept/ARR/grades/gradinghandbook/index.html. Please see the link for more details on this and any other grading concerns.

A grade of Missing Grade (MG) "should only be assigned in unique or unusual situations… for those cases in which a student does not complete work for the course before the semester

ends. All missing grades must be resolved by the instructor through the Correction of Grade Process. One calendar year is allowed to resolve a MG. If an MG is not resolved [within] one year the grade is changed to [Unofficial Withdrawal] UW and will be calculated into the grade point average a zero grade points.
A grade of Incomplete (IN) "is assigned when work is no completed because of documented illness or other 'emergency' **occurring after the twelfth week** of the semester (or 12th week equivalency for any course scheduled for less than 15 weeks)."

Academic Integrity

The University, as an instrument of learning, is predicated on the existence of an environment of integrity. As members of the academic community, faculty, students, and administrative officials share the responsibility for maintaining this environment. Faculties have the primary responsibility for establishing and maintaining an atmosphere and attitude of academic integrity such that the enterprise may flourish in an open and honest way. Students share this responsibility for maintaining standards of academic performance and classroom behavior conducive to the learning process. Administrative officials are responsible for the establishment and maintenance of procedures to support and enforce those academic standards. Thus, the entire University community bears the responsibility for maintaining an environment of integrity and for taking appropriate action to sanction individuals involved in any violation. When there is a clear indication that such individuals are unwilling or unable to support these standards, they should not be allowed to remain in the University." (Faculty Handbook, 1994:20)

Academic dishonesty includes: (Faculty Handbook, 1994: 21-22)
Examination behavior – any use of external assistance during an examination shall be considered academically dishonest unless expressly permitted by the teacher.
Fabrication – any intentional falsification or invention of data or citation in an academic exercise will be considered a violation of academic integrity.
Plagiarism – the appropriation and subsequent passing off of another's ideas or words as one's own. If the words or ideas of another are used, acknowledgment of the original source must be made through recognized referencing practices.
Other Types of Academic Dishonesty – submitting a paper written by or obtained from another, using a paper or essay in more than one class without the teacher's express permission, obtaining a copy of an examination in advance without the knowledge and consent of the teacher, changing academic records outside of normal procedures and/or petitions, using another person to complete homework assignments or take-home exams without the knowledge or consent of the teacher.

The use of unauthorized material, communication with fellow students for course assignments, or during a mid-term examination, attempting to benefit from work of another student, past or present and similar behavior that defeats the intent of an assignment or mid-term examination, is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behavior resulting from the nervous tensions accompanying

examinations. Where a clear violation has occurred, however, the instructor may disqualify the student's work as unacceptable and assign a failing mark on the paper.

Students with Disabilities

Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to your course instructor (or TA) as early in the semester as possible. DSP is located in STU 301 and is open from 8:30am to 5:00pm, Monday through Friday. Website and contact information for DSP http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html (213) 740-0776 (Phone), (213) 740-6948 (TDD only), (213) 740-8216 (FAX) ability@usc.edu

Emergency Preparedness/Course Continuity in a Crisis

In case of emergency, when travel to campus is difficult, if not impossible, USC executive leadership will announce a digital way for instructors to teach students in their residence halls or homes using a combination of the Blackboard LMS (Learning Management System), teleconferencing, and other technologies. Instructors should be prepared to assign students a "Plan B" project that can be completed 'at a distance.' For additional information about maintaining your classes in an emergency, please access: http://cst.usc.edu/services/emergencyprep.html

Return of Course Assignments

Returned work, unclaimed by a student, will be discarded after one academic year. This work will not be available should a grade appeal be pursued following receipt of his/her grade.

Computer and Network Forensics
INF 528 (3 Units)

Course Outline

Note: Schedule subject to change

Week 1 – Introduction and Digital Forensic Process and Methodologies

- Course overview
- Understanding the need for computer forensics
- Defining computer forensics
- Digital Forensic Process
- Digital Forensic Methodologies

Reading

Sammons, Chapter 1

Week 2 – Digital Concepts and Magnetic Media

- Bits, Bytes, Numbering Schemes
- 2s complement binary notation
- Little vs. Big Endian
- Data Types
- Magnetic Media
- Cryptographic Hashes and Forensics

Reading

Sammons, Chapter 2

Assignment/Lab

Lab 1: Numeric conversions

Week 3 – Evidence Preservation

- Forensic hardware
- Hardware write/blockers
- Hard drive acquisitions
- Forensic Image Files
- Assessment , Acquisition and Authentication

Reading

Sammons, Chapters 3 & 4

Assignment/Lab

Lab 2: Hard drive acquisitions

Week 4 – Forensic Software Packages

- Overview of different software packages
- Open source vs. closed source

- EnCase Introduction

Reading

Carvey, Chapter 1

Assignment/Lab

Lab 3: EnCase Introduction

Week 5 – Windows Filesystems: FAT32

- Windows Volumes
- Master boot record analysis
- FAT32 volume boot record analysis
- Directory entry analysis
- Allocation table analysis

Reading

Instructor Handouts

Assignment/Lab

Lab 4: FAT32 Analysis

Week 6 – Windows Filesystems: NTFS

- NTFS volume boot record analysis
- Overview of NTFS structures
- MFT analysis
- MFT entry analysis
- Resident vs. non-resident data

Reading

Carvey, Chapter 4

Assignment/Lab

Lab 5: NTFS Analysis

Week 7 – Timeline and File Metadata Behaviors

- Analysis of windows timestamps
- Local time vs. UTC
- Filesystem timestamps versus embedded timestamps
- Timestamp manipulation
- Timestamp alteration when copying between volumes and filesystems

Reading

Carvey, Chapter 7

Assignment/Lab

Lab 6: Timestamps

Week 8 – Windows Forensic Techniques I

- Basic searches
- Deleted partition/volume analysis
- File signature analysis
- File hash analysis

- Recycle bin analysis
- Prefetch Files
- Windows XP system analysis

Reading

Sammons, Chapter 5

Assignment/Lab

Lab 7: Windows XP evidence collection

Case 1 Assigned

Week 9 – Forensic Reports and Legal Concerns

- Creating a forensic report
- Proper report writing
- Understanding your target audience

Reading

Sammons, Chapter 7; Carvey, Chapter 9

Week 10 – Midterm, Work On Case 1

Week 11 – Windows Forensic Techniques II and Internet/Email Analysis

- Regular-expression searches
- Registry analysis
- Internet cache analysis
- Email and email header analysis
- USBStor Analysis
- Windows 7 analysis

Reading

Sammons, Chapter 8; Carvey, Chapters 5 and 8

Assignment/Lab

Lab 8: Windows 7 evidence collection

Case 2 Assigned

Week 12 – Image Analysis and Steganography

- Image types
- Evidence hiding
- Steganography

Reading

Sammons, Chapter 6

Assignment/Lab

Lab 9: Steganography lab

Week 13 – Live System Acquisition and Partial Acquisitions

- Live system concerns
- Large server concerns
- Imaging speed and bandwidth

- RAM acquisitions and concerns

Reading

Instructor Handouts

Week 14 – Network Forensics Introductions

- Network forensic concerns
- Preservation of network traffic
- Network traffic packet analysis tools and techniques
- Incident response

Reading

Sammons, Chapter 9; Carvey, Chapters 2 & 6

Assignment/Lab

Lab 10: Network traffic capture and analysis

Week 15 – Conclusion

- Review for the final exam
- Conclusion to the course
- Future topics

Reading

Sammons, Chapter 11

Final Exam to Be Held According to the Schedule of Classes