Computer Forensics

INF 528 (4 Units)

USC Viterbi School of Engineering

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. In 2013, according to Europol Serious & Organized Threat Assessment, the "Total Global Impact of CyberCrime [has risen to] US $3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined."

Due to the ease of access to tools and software, the low risk of perpetrating the crime and the internationally connected network called the Internet, cybercrime will continue. 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; 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.

This class will be primary individual study, with weekly assigned readings, various homework assignments (laboratory exercises), three 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 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 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, 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 lab exercises and case investigations).

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 three 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	TBA
Lab Assistants	TBA
Lecture/Lab	TBA

Required Textbooks

Windows Forensic Analysis Toolkit, 3rd Edition. Carvey.
ISBN: 1597497274
NOTE: The 3rd edition of the textbook covers Windows 7. The 4th edition covers Windows 8, and the 2nd edition covers Windows XP. I have all three and they have different material. For this course, you need the 3rd edition.

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

Recommended Textbooks (For This Course and the Future)

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

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 Desire2Learn (courses.uscden.net)

Grading

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

Lab Exercises (10)	30% (3% each) In the event of fewer labs during the semester, they will be weighted evenly to add up to 30% of your final grade
Case Reports (3)	45% (15% each) Case descriptions provided towards the end of the syllabus
Midterm Exam	10%
Final Exam	15%
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 25% 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.

Writing Skills

The goal of the Digital Forensics program at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. A significant portion of the digital forensics curriculum involves communicating what was discovered by writing professional quality digital forensic reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges and juries. It is expected that the reports will be written with correct spelling, grammar and language nuances of the American English language. A component of each report grade will be based on writing style, grammar and word choice. These reports must be accessible to technical and non-technical readers alike.

Please take care to review the Digital Forensic Report Writing Guidelines available on Desire2Learn. If you are not a native English speaker and writer, it is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional careers. Writing assistance is available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with University standards, plagiarism of any type will not be tolerated.

Computer Forensics
INF 528 (4 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

Phillip & Cowen, Chapter 1
Carvey, 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

Phillip & Cowen, Chapters 2 & 3

Assignment/Lab

Lab 1: Digital concepts review

Week 3 – Evidence Preservation, Forensic Software

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

Reading

Phillip & Cowen, Chapters 4 & 5

Assignment/Lab

Lab 2: Hard drive acquisitions

Week 4 – Windows Filesystems: FAT12, 16 & 32

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

Reading

Instructor Notes

Assignment/Lab

Lab 3: FAT32 Analysis

Week 5 – Windows Filesystems: NTFS

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

Reading

Instructor Handouts

Assignment/Lab

Lab 4: NTFS Analysis

Week 6 – Files, File Formats, Windows Artifacts I, Forensic Reports

- Deleted partition/volume analysis
- File signature analysis
- File hash analysis
- Recycle bin analysis
- Prefetch Files
- Windows XP system analysis
- Creating a forensic report
- Proper report writing
- Understanding your target audience

Reading

Phillip & Cowen, Chapters 6, 14 & 15
Carvey, Chapter 4
Instructor Handouts

Assignment/Lab

Lab 5: Files, Signature and Hash Analysis
Case 1 Assigned

Week 7 – Searching, GREP, MIDTERM

- Keyword Searches
- Limiting search scope
- Regular expressions and pattern matching basics

Reading

Instructor Notes

MIDTERM

Week 8 – Timeline Analysis, Timestamps, Steganography

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

Reading

Carvey, Chapter 7

Assignment/Lab

Lab 6: Timestamps

Week 9 – Windows Registry

- Windows Registry Basics
- Registry Hives, Keys
- Analysis of HKEY_LOCAL_MACHINE registry (SAM, SYSTEM and SOFTWARE hives)
- Analysis of HKEY_CURRENT_USER registry (ntuser.dat)

Reading

Carvey, Chapter 5

Assignment/Lab

Lab 7: Windows Registry Analysis

Case 2 Assigned

Week 10 – Tracking User Activity

- USB Device Analysis
- Prefetch/Superfetch
- LNK files and Jumplists
- UserAssist Registry Analysis

Reading

Phillip & Cowen, Chapter 12

Assignment/Lab

Lab 8: USB Device Analysis

Week 11 – Internet/Email Analysis

- Internet History, Bookmarks, Cookies and Cache Analysis
- Major browser artifacts
- Email client artifacts
- Analyzing Email Headers

Reading

Phillip & Cowen, Chapter 11

Assignment/Lab

Lab 9: Internet & Email Analysis

Week 12 – Servers, Solid State Hard Drives

- Servers
- RAID
- Server software
- Log Analysis
- Flash memory
- Solid State Hard Drives

Reading

Instructor Notes

Week 13 – Advanced Topics: BitTorrent Analysis

- Peer-to-Peer networks
- BitTorrent Protocol
- BitTorrent Forensic Artifacts

Reading

Instructor Notes

Case 3 Assigned

Week 14 – Memory Acquisitions and Analysis

- Issues with live memory capture
- Memory capture tools
- Memory capture analysis
- Malware analysis

Reading

Carvey, Chapters 2 & 6

Assignment/Lab

Lab 10: Memory Analysis Using Volatility

Week 15 – Conclusion

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

Final Exam to Be Held According to the Schedule of Classes

Case Scenarios

Case 1: Child Pornography Investigation

Background: You have been called to assist in the investigation of a Richard Bruin. Mr. Bruin has been accused by his roommate of having some contraband material on his computer. Mr. Bruin's roommate, Thomas Trojan, reported to the IT staff that he saw possible child pornography on Mr. Bruin's computer while Mr. Bruin was sitting in front of the computer. Since Mr. Trojan is an upstanding member of the community, his word is taken in the highest regard and seriousness, and Mr. Bruin's computer was confiscated, along with other removable media.

Goal: You have been given the suspect's hard disk for analysis. You are to determine if there is indeed contraband material on the hard disk. Additionally, if there is, you must determine if the suspect has been distributing the content, since the penalty is worse for distribution than for possession.

Note: The placeholder images for child pornography in this case appear similar to the image below:

Case 2: Student Misconduct

Background: You have been hired by the IT staff at the local college. Upon demonstrating a new security appliance, the appliance started reporting portscanning activity originating from a particular computer system. Upon investigation and cross-correlating the registered MAC address, it was determined that the computer system belongs to Alicia Houston. This student has a system on loan from the college for independent research. The college security policy states that any portscanning or other malicious activity must be fully investigated. The IT staff hired you to investigate this system.

The target of the portscanning appears to be a system belonging to Professor Biff Tannen of the Philosophy department. It appears as though Ms. Houston was a student of Prof. Tannen's in the Fall of 2015 in PHIL 230.

Both systems have been forensically imaged and provided to you for analysis. Professor Tannen's system is indicated as 02USC01 and Ms. Houston's system is 02USC02. Additionally, prior to shutdown, Professor Tannen's system had the RAM imaged using FTK imager to a network share, Y:\. You will be given this memory image at a later point for analysis.

Task: Determine if any suspicious activity was conducted by Ms. Houston. You have been given both systems to analyze, 02USC01 and 02USC02. Be sure to conduct a thorough investigation of both systems and be sure to indicate whichever artifacts and analysis involve one or both systems.

Task: Determine if any suspicious activity was conducted by Ms. Houston. You have been given both systems to analyze, 02USC01 and 02USC02. Be sure to conduct a thorough investigation of both systems and be sure to indicate whichever artifacts and analysis involve one or both systems.

Case 3: Content Piracy Investigation

Background: You are a new employee of the internal affairs and investigations division of Acme Inc. Your manager has been notified by the RIAA & MPAA that your network has been utilized for copyright infringement. After analyzing the network logs, your manager has determined that the traffic leads to one person, Neil Flannigan. Upon seizing his computer, your manager discovers that he has installed VMWare, which is against company policy. He creates an EnCase image from one of the Virtual Machines, and gives it to you for analysis.

Goal: Determine if Mr. Flannigan is engaging in content piracy through BitTorrent. Note any and all files used in the infringement, the method (program) used, and any other items of evidentiary value.